McAfee®

VirusScan® Plus 2007

AntiVirus, Firewall & AntiSpyware

Table des matières

CHAPITRE 1

Introduction

McAfee VirusScan Plus Suite protège votre ordinateur et vos fichiers contre les virus, les logiciels espions et les pirates. Naviguez sur le Web et téléchargez des fichiers en toute sécurité et confiance, car McAfee vous offre une protection fiable, toujours active et toujours à jour. Grâce à McAfee, bénéficiez d'une protection fiable qui permet de bloquer automatiquement les menaces et les pirates informatiques pour assurer le bon fonctionnement et la sécurité de votre ordinateur. McAfee permet également de consulter en toute simplicité l'état de sécurité de votre ordinateur, de rechercher des virus et des logiciels espions, et de vérifier que vos produits sont à jour grâce au nouveau McAfee SecurityCenter. En outre, avec votre abonnement, vous recevrez automatiquement les mises à jour et les logiciels McAfee les plus récents.

VirusScan Plus comprend les programmes suivants :

- SecurityCenter
- VirusScan
- Personal Firewall
- Network Manager
- EasyNetwork (licence 3 utilisateurs uniquement)
- SiteAdvisor

CHAPITRE 2

McAfee SecurityCenter

McAfee SecurityCenter est un environnement convivial que les utilisateurs de McAfee peuvent utiliser pour lancer, gérer et configurer leurs abonnements de sécurité.

Il est également une source d'informations sur les alertes de virus, les produits, l'assistance et l'abonnement. En un seul clic, SecurityCenter permet d'accéder aux outils et aux informations du site Web de McAfee.

Contenu de ce chapitre

Caractéristiques

McAfee SecurityCenter vous offre les nouvelles fonctions et avantages suivants :

Niveau de protection redéfini

Consultez facilement le niveau de sécurité de votre ordinateur, vérifiez la présence de mises à jour et réglez les problèmes de sécurité potentiels.

Mises à jour et mises à niveau permanentes

Installez automatiquement les mises à jour quotidiennes. Lorsqu'une nouvelle version d'un logiciel McAfee est disponible, vous l'obtenez automatiquement sans frais pendant toute la durée de votre abonnement. Vous bénéficiez ainsi d'une protection à jour en permanence.

Alertes en temps réel

Les alertes de sécurité vous avertissent des nouvelles épidémies virales et des menaces de sécurité, tout en vous fournissant des possibilités de réponse pour supprimer, neutraliser ou mieux connaître la menace.

Une protection pratique

Plusieurs options de renouvellement permettent de maintenir à jour votre protection McAfee.

Outils de performances

Supprimez les fichiers inutilisés, défragmentez les fichiers utilisés et utilisez l'option de restauration du système pour maintenir le niveau de performances optimal de votre ordinateur.

Une Aide en ligne concrète

Bénéficiez du support des experts McAfee en matière de sécurité informatique, par chat sur Internet, par e-mail ou par téléphone.

Protection de la navigation

S'il est installé, le plug-in de navigateur McAfee SiteAdvisor vous aide à vous protéger contre les logiciels espions, spams, virus et e-mails frauduleux en établissant une classification des sites Web que vous consultez ou qui apparaissent dans les résultats des recherches que vous effectuez sur le Web. Vous pouvez afficher des évaluations de sécurité détaillées illustrant la manière dont un site a été testé en termes de pratiques d'e-mail, de téléchargement, d'affiliations en ligne et d'interventions non sollicitées telles que les fenêtres instantanées et les cookies tiers traceurs.

CHAPITRE 3

Utilisation de SecurityCenter

Vous pouvez lancer SecurityCenter depuis le bureau Windows ou la zone de notification Windows située à l'extrême droite de la barre des tâches (pour ce faire, utilisez l'icône McAfee SecurityCenter).

Une fois SecurityCenter ouvert, vous pouvez visualiser l'état de sécurité de votre ordinateur dans le volet Accueil et accéder rapidement à des tâches courantes, notamment aux opérations de mise à jour et d'analyse (si McAfee VirusScan est installé) :

En-tête

Aide

Affiche le fichier d'aide du programme.

Colonne de gauche

Mise à jour

Met à jour votre produit pour protéger votre ordinateur contre les dernières menaces.

Analyse

Permet d'effectuer une analyse manuelle de votre ordinateur (si McAfee VirusScan est installé).

Tâches courantes

Exécute des tâches courantes comme revenir au volet Accueil, afficher les événements récents, mettre à jour votre ordinateur et gérer votre réseau informatique (si l'ordinateur utilisé dispose des droits appropriés). Si McAfee Data Backup est installé, vous pouvez également sauvegarder vos données.

Composants installés

Permet de connaître les services de sécurité de votre ordinateur.

Volet principal

Etat de protection

Affiche le niveau général de protection informatique dans la section **Suis-je protégé**. Au-dessous de celle-ci, vous pouvez consulter l'état de chaque catégorie et type de protection.

SecurityCenter - Informations

Permet de connaître le moment de la dernière mise à jour de votre ordinateur, celui de l'expiration de votre abonnement et celui de la dernière analyse (si McAfee VirusScan est installé).

Contenu de ce chapitre

Signification des icônes SecurityCenter

Les icônes SecurityCenter s'affichent dans la zone de notification Windows située à l'extrême droite de la barre des tâches. Utilisez-les pour voir si votre ordinateur est totalement protégé, visualiser l'état d'une analyse en cours (si McAfee VirusScan est installé), rechercher des mises à jour, afficher les événements récents, mettre à jour votre ordinateur et obtenir de l'aide sur le site Web de McAfee.

Ouverture de SecurityCenter et utilisation des fonctionnalités supplémentaires

Lorsque SecurityCenter est en cours d'exécution, l'icône M de SecurityCenter s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches.

Pour ouvrir SecurityCenter ou utiliser des fonctionnalités supplémentaires :

- Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, puis cliquez sur l'une des options suivantes :
  - Ouvrir SecurityCenter
  - Mises à jour
  - Liens rapides

    Le sous-menu contient des liens vers les sections suivantes Accueil, Afficher les événements récents, Gérer un réseau, Mettre à jour l'ordinateur et Sauvegarde des données (si ces fonctionnalités sont installées).
  - Vérifier l'abonnement

    (Cet élément apparaît lorsque l'abonnement à au moins un produit a expiré.)
  - Centre de mise à niveau
  - Service clientèle

Vérification de votre état de protection

Si votre ordinateur n'est pas totalement protégé, l'icône d'état de protection s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches. Cette icône peut être rouge ou jaune selon l'état de protection.

Pour vérifier votre état de protection :

- Cliquez sur l'icône d'état de protection pour ouvrir SecurityCenter et corriger les éventuels problèmes.

Vérification de l'état de vos mises à jour.

Si vous recherchez des mises à jour, l'icône Mises à jour  s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches.

Pour vérifier l'état des mises à jour :

- Pointez sur l'icône Mises à jour pour afficher l'état de vos mises à jour sous forme d'info-bulle.

Explications sur l'état de protection

L'état de protection générale de votre ordinateur apparaît dans la section **Suis-je protégé** de SecurityCenter.

L'état de protection vous indique si votre ordinateur est totalement protégé contre les dernières menaces de sécurité ou s'il existe des problèmes nécessitant une attention particulière et comment les résoudre. Si un problème affecte plusieurs catégories de protection, sa résolution peut permettre à celles-ci de retrouver un état de protection totale.

Les critères pris en compte pour déterminer votre état de protection comprennent notamment les menaces de sécurité externes, les produits de sécurité installés sur votre ordinateur, les produits d'accès à Internet, ainsi que la configuration de ces produits de sécurité et d'accès à Internet.

Par défaut, si les fonctionnalités Protection antispam ou Blocage de contenu ne sont pas installées, ces problèmes de protection mineurs sont automatiquement ignorés et ne sont pas consignés dans l'état de protection générale de votre ordinateur. Toutefois, lorsqu'un problème de protection est suivi d'un lien **Ignorer**, vous pouvez choisir d'ignorer le problème en question si vous êtes sûr de ne pas vouloir le résoudre.

Suis-je protégé ?

Dans la section **Suis-je protégé** de SecurityCenter, consultez le niveau général de protection de votre ordinateur :

- **Oui** apparaît si votre ordinateur est totalement protégé (vert).
- **Non** apparaît si votre ordinateur est partiellement protégé (jaune) ou s'il n'est pas protégé du tout (rouge).

Pour résoudre la plupart des problèmes de protection automatiquement, cliquez sur **Corriger** en regard de l'état de protection. Toutefois, si certains problèmes persistent et nécessitent une réponse de votre part, cliquez sur le lien suivant le problème en question pour effectuer l'action suggérée.

Explications sur les catégories et les types de protection

Dans la section **Suis-je protégé** de SecurityCenter, vous pouvez consulter l'état des catégories et types de protection suivants :

- Ordinateur et fichiers
- Réseau et Internet
- E-mails et messages instantanés
- Contrôle parental

Les types de protection affichés dans SecurityCenter dépendent des produits installés. Par exemple, si McAfee Data Backup est installé, le type de protection de l'état du PC apparaît.

Les catégories qui ne présentent pas de problèmes de protection ont l'état vert. Si vous cliquez sur une catégorie verte, la liste des types de protection activés s'affiche sur la droite, suivie de la liste des problèmes ignorés. Si aucun problème n'a été relevé, une information sur les virus s'affiche à la place. Vous pouvez également cliquer sur **Configurer** pour modifier les options sélectionnées pour cette catégorie.

Si tous les types de protection d'une catégorie ont l'état vert, la catégorie est elle aussi définie sur l'état vert. De même, si toutes les catégories de protection ont l'état vert, l'état de protection générale de votre ordinateur est lui aussi défini sur l'état vert.

Si une catégorie de protection a l'état jaune ou rouge, vous pouvez régler les problèmes de protection en les résolvant ou en les ignorant afin d'obtenir l'état vert.

Explications sur la protection des ordinateurs et des fichiers

Cette catégorie de protection comprend les types de protection suivants.

- **Protection antivirus** : l'analyse en temps réel protège votre ordinateur contre les virus, vers, chevaux de Troie, scripts suspects, attaques hybrides et autres menaces. Le système analyse automatiquement les fichiers et essaie de les nettoyer (y compris les fichiers compressés au format .exe, le secteur d'amorçage, la mémoire et les fichiers critiques) lorsque vous ou votre ordinateur y accédez.
- **Protection contre les logiciels espions** : cette fonction détecte, bloque et éradique rapidement les logiciels espions, les logiciels publicitaires et autres programmes potentiellement indésirables qui accèdent à vos données personnelles et les transmettent sans votre autorisation.
- **SystemGuards** : cette fonction détecte les modifications intervenant sur votre ordinateur et vous alerte. Vous pouvez alors examiner les modifications et décider de les autoriser ou non.
- **Protection Windows** : cette protection indique l'état des mises à jour de Windows sur votre ordinateur. Si McAfee VirusScan est installé, la protection contre le débordement de la mémoire tampon est également disponible.

L'un des facteurs déterminants du niveau de protection de l'ordinateur et des fichiers est les menaces virales externes. Par exemple, si un virus se déclare, votre logiciel antivirus vous protège-t-il contre ce virus ? Parmi les autres facteurs figurent notamment la configuration de votre logiciel antivirus et la fréquence des mises à jour de celui-ci avec les derniers fichiers de signatures afin de protéger votre ordinateur contre les dernières menaces de sécurité.

Ouverture du volet de configuration de l'ordinateur et des fichiers

Si aucun problème n'a été relevé pour **l'ordinateur et les fichiers**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration de l'ordinateur et des fichiers :

1. Dans le volet Accueil, cliquez sur l'option relative à l'**ordinateur** et **aux fichiers**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Explications sur la protection Internet et réseau

Cette catégorie de protection comprend les types de protection suivants.

- **Protection par pare-feu** : cette fonction protège votre ordinateur contre les intrusions et contre le trafic réseau indésirable. Elle vous permet de gérer les connexions Internet entrantes et sortantes.
- **Protection sans fil** : la protection sans fil empêche toute intrusion et interception de données sur votre réseau domestique sans fil. Toutefois, si vous êtes connecté à un réseau sans fil externe, cette protection varie en fonction du niveau de sécurité de ce dernier.
- **Protection de la navigation sur le Web** : la fonction de protection de navigation Web masque les publicités, les fenêtres instantanées et les pixels invisibles sur votre ordinateur.
- **Protection antiphishing** : la protection antiphishing permet de bloquer les sites Web frauduleux qui vous invitent à donner des informations personnelles grâce à des liens hypertexte dans les e-mails et les messages instantanés, les fenêtres instantanées et d'autres sources.
- **Protection des informations personnelles** : la protection des informations personnelles permet de bloquer la diffusion d'informations sensibles ou confidentielles sur Internet.

Ouverture du volet de configuration Internet et réseau

Si aucun problème n'a été relevé pour **Internet et le réseau**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration Internet et réseau :

1. Dans le volet Accueil, cliquez sur l'option relative à **Internet et au réseau**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Explications sur la protection des e-mails et des messages instantanés

Cette catégorie de protection comprend les types de protection suivants.

- **Protection des e-mails** : la fonction de protection des e-mails analyse et essaie automatiquement de nettoyer les virus, les logiciels espions et autres menaces potentielles contenus dans vos messages et pièces jointes entrants et sortants.
- **Protection antispam** : la protection antispam vous aide à bloquer l'accès des messages indésirables à votre boîte de réception.
- **Protection de la messagerie instantanée** : la fonction de protection de la messagerie instantanée analyse et essaie automatiquement de nettoyer les virus, les logiciels espions et autres menaces potentielles contenus dans vos messages et pièces jointes entrants et sortants. Elle empêche également les clients de messagerie instantanée d'échanger du contenu indésirable ou des informations personnelles sur Internet.
- **Protection de la navigation** : s'il est installé, le plug-in de navigateur McAfee SiteAdvisor vous aide à vous protéger contre les logiciels espions, spams, virus et e-mails frauduleux en définissant une classification des sites Web que vous visitez ou qui apparaissent dans les résultats de recherches que vous effectuez sur le Web. Vous pouvez afficher des évaluations de sécurité détaillées illustrant la manière dont un site a été testé en termes de pratiques d'e-mail, de téléchargement, d'affiliations en ligne et d'interventions non sollicitées telles que les fenêtres instantanées et les cookies tiers traceurs.

Ouverture du volet de configuration des e-mails et des messages instantanés

Si aucun problème n'a été relevé pour les **e-mails et les messages instantanés**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration des e-mails et messages instantanés :

1. Dans le volet Accueil, cliquez sur l'option des **e-mails et messages instantanés**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Explications sur la protection par contrôle parental

Cette catégorie de protection comprend les types de protection suivants.

- **Protection par contrôle parental** : le blocage de contenu empêche les utilisateurs de visualiser du contenu Internet indésirable en bloquant l'accès aux sites Web potentiellement dangereux. L'activité et l'utilisation d'Internet que font les utilisateurs peuvent aussi être surveillées et limitées.

Ouverture du volet de configuration Contrôle parental

Si aucun problème n'a été relevé sous **Contrôle parental**, vous pouvez ouvrir le volet de configuration à partir du volet d'information.

Pour ouvrir le volet de configuration Contrôle parental :

1. Dans le volet Accueil, cliquez sur **Contrôle parental**.
2. Dans le volet de droite, cliquez sur **Configurer**.

Résolution des problèmes de protection

La plupart des problèmes de protection rencontrés par les utilisateurs peuvent être résolus automatiquement. Toutefois, si un ou plusieurs problèmes persistent, il est indispensable de les résoudre.

Résolution automatique des problèmes de protection

La plupart des problèmes de protection rencontrés par les utilisateurs peuvent être résolus automatiquement.

Pour résoudre automatiquement les problèmes de protection :

- Cliquez sur **Corriger** en regard de l'état de protection.

Résolution manuelle des problèmes de protection

Si certains problèmes ne peuvent pas être résolus automatiquement, cliquez sur le lien suivant le problème en question pour effectuer l'action suggérée.

Pour résoudre manuellement les problèmes de protection :

- Effectuez l'une des opérations suivantes.
  - Si l'analyse complète de votre ordinateur n'a pas été exécutée depuis au moins 30 jours, cliquez sur l'option **Analyser** située à gauche de l'état de protection principal pour effectuer une analyse manuelle (cette option est disponible si McAfee VirusScan est installé).
  - Si vos fichiers de signatures (DAT) sont dépassés, cliquez sur le lien **Mettre à jour** situé à gauche de l'état de protection principal pour mettre à jour votre protection.
  - Si un programme n'est pas installé, cliquez sur **Bénéficiez d'une protection complète** pour l'installer.
  - Si certains composants d'un programme sont manquants, réinstallez-le.
  - Si un programme doit être enregistré pour bénéficier d'une protection complète, cliquez sur **M'enregistrer maintenant**. Cet élément apparaît si l'abonnement à un ou plusieurs programmes a expiré.
  - Dans ce cas, cliquez sur **Vérifiez votre abonnement maintenant** pour vérifier l'état de votre compte. Cet élément apparaît si l'abonnement à un ou plusieurs programmes a expiré.

Affichage des informations sur SecurityCenter

En bas du volet Etat de protection, la section SecurityCenter - Informations vous permet d'accéder aux options de SecurityCenter et vous indique la dernière mise à jour, la dernière analyse (si McAfee VirusScan est installé) et des informations sur l'expiration de l'abonnement à vos produits McAfee.

Ouverture du volet de configuration SecurityCenter

Pour votre commodité, vous pouvez ouvrir le volet de configuration SecurityCenter pour modifier les options définies depuis le volet Accueil.

Pour ouvrir le volet de configuration SecurityCenter :

- Dans le volet Accueil, sous **SecurityCenter - Informations**, cliquez sur **Configurer**.

Affichage des informations sur les produits installés

Vous pouvez afficher la liste des produits installés avec le numéro de version de chaque produit et la date de la dernière mise à jour.

Pour consulter les informations de produits McAfee :

- Dans le volet Accueil, sous **SecurityCenter - Informations**, cliquez sur **Afficher les détails** pour ouvrir la fenêtre des informations sur le produit.

Utilisation du Menu avancé

A la première ouverture de SecurityCenter, le Menu de base apparaît dans la colonne de gauche. Si vous êtes un utilisateur expérimenté, vous pouvez cliquer sur **Menu avancé** pour afficher à la place un menu de commandes plus détaillé. Pour votre commodité, le dernier menu utilisé sera affiché à la prochaine ouverture de SecurityCenter.

La page Menu avancé comprend les éléments suivants :

- Particuliers
- Journaux et rapports (comprend la liste des événements les plus récents et des journaux par type relatifs aux 30, 60 et 90 derniers jours)
- Configurer
- Restaurer
- Outils

CHAPITRE 4

Configuration des options de SecurityCenter

SecurityCenter vous permet de consulter l'état de protection générale de votre ordinateur, de créer des comptes utilisateur McAfee, d'installer automatiquement les dernières mises à jour du produit, et d'être averti automatiquement par des alertes et des signaux sonores en cas d'attaques générales de virus, de menaces et de mises à jour de produits.

Dans le volet Configuration de SecurityCenter, vous pouvez modifier les options SecurityCenter définies pour les fonctions suivantes :

- Etat de protection
- Utilisateurs
- Mises à jour automatiques
- Alertes

Contenu de ce chapitre

Configuration de l'état de protection

L'état de protection générale de votre ordinateur apparaît dans la section **Suis-je protégé** de SecurityCenter.

L'état de protection vous indique si votre ordinateur est totalement protégé contre les dernières menaces de sécurité ou s'il existe des problèmes nécessitant une attention particulière et comment les résoudre.

Par défaut, si les fonctionnalités Protection antispam ou Blocage de contenu ne sont pas installées, ces problèmes de protection mineurs sont automatiquement ignorés et ne sont pas consignés dans l'état de protection générale de votre ordinateur. Toutefois, lorsqu'un problème de protection est suivi d'un lien **Ignorer**, vous pouvez choisir d'ignorer le problème en question si vous êtes sûr de ne pas vouloir le résoudre. Si vous décidez par la suite de régler un problème précédemment ignoré, vous pourrez l'inclure dans l'état de protection de l'ordinateur afin que celui-ci soit contrôlé.

Configuration des problèmes ignorés

Vous pouvez inclure ou exclure des problèmes de l'état de protection générale de votre ordinateur. Lorsqu'un problème de protection est suivi d'un lien **Ignorer**, vous pouvez choisir d'ignorer le problème en question si vous êtes sûr de ne pas vouloir le résoudre. Si vous décidez par la suite de régler un problème précédemment ignoré, vous pourrez l'inclure dans l'état de protection de l'ordinateur afin que celui-ci soit contrôlé.

Pour configurer les problèmes ignorés :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Etat de protection** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Effectuez l'une des opérations suivantes dans le volet Problèmes ignorés :
   - Pour ne plus ignorer certains problèmes dans l'état de protection, désactivez les cases à cocher correspondantes.
   - Pour exclure des problèmes de l'état de protection, activez les cases à cocher correspondantes.
4. Cliquez sur **OK**.

Configuration des options utilisateur

Si vous exécutez des programmes McAfee qui nécessitent des autorisations utilisateur, celles-ci correspondent par défaut aux comptes utilisateur Windows de cet ordinateur. Pour faciliter la gestion des utilisateurs de ces programmes, vous pouvez changer de compte utilisateur McAfee à tout moment.

Dans ce cas, les noms d'utilisateur et autorisations de votre programme de contrôle parental sont importés automatiquement. Toutefois, lors du premier changement de compte utilisateur, vous devez créer un compte administrateur. Vous pouvez ensuite commencer à créer et à configurer d'autres comptes utilisateur McAfee.

Passage aux comptes utilisateur McAfee

Par défaut, vous utilisez les comptes utilisateur de Windows. Toutefois, pour utiliser des comptes utilisateur McAfee, il n'est pas nécessaire de créer des comptes utilisateur supplémentaires sous Windows.

Pour basculer vers les comptes utilisateur McAfee :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Utilisateurs** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Pour utiliser les comptes utilisateur McAfee, cliquez sur **Basculer**.

Si vous basculez vers les comptes utilisateur McAfee pour la première fois, vous devez créer un compte administrateur (page 23).

Création d'un compte administrateur

Lors du premier changement de compte utilisateur McAfee, vous êtes invité à créer un compte administrateur.

Pour créer un compte administrateur :

1. Entrez un mot de passe dans la zone **Mot de passe**, puis entrez-le à nouveau dans la zone **Confirmer le mot de passe**.
2. Sélectionnez une question permettant de récupérer le mot de passe dans la liste, puis entrez la réponse à celle-ci dans la zone **Réponse**.
3. Cliquez sur **Appliquer**.

   Lorsque vous avez terminé, le type de compte utilisateur est mis à jour (le cas échéant) avec les noms d'utilisateur et

autorisations existants de votre programme de contrôle parental. Si vous configurez des comptes utilisateur pour la première fois, le volet Gérer les utilisateurs s'affiche.

Configuration des options utilisateur

Dans ce cas, les noms d'utilisateur et autorisations de votre programme de contrôle parental sont importés automatiquement. Toutefois, lors du premier changement de compte utilisateur, vous devez créer un compte administrateur. Vous pouvez ensuite commencer à créer et à configurer d'autres comptes utilisateur McAfee.

Pour configurer des options utilisateur :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Utilisateurs** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sous **Comptes utilisateur**, cliquez sur **Ajouter**.
4. Entrez le nom d'utilisateur dans la zone **Nom d'utilisateur**.
5. Entrez un mot de passe dans la zone **Mot de passe**, puis entrez-le à nouveau dans la zone **Confirmer le mot de passe**.
6. Sélectionnez la case **Utilisateur au démarrage** si vous voulez que ce nouvel utilisateur se connecte automatiquement au démarrage de SecurityCenter.
7. Sous **Type de compte utilisateur**, sélectionnez un type de compte pour l'utilisateur voulu, puis cliquez sur **Créer**.

   Remarque : vous devez ensuite configurer les paramètres d'utilisateur limité sous Contrôle parental.

8. Pour changer le mot de passe d'un utilisateur, la connexion automatique ou le type de compte, sélectionnez un nom d'utilisateur dans la liste, puis cliquez sur **Modifier**.
9. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Récupération du mot de passe administrateur

Si vous oubliez le mot de passe administrateur, vous pouvez le récupérer.

Pour récupérer le mot de passe administrateur :

1. Cliquez à l'aide du bouton droit de la souris sur l'icône M de SecurityCenter, puis cliquez sur **Changer d'utilisateur**.
2. Dans la liste **Nom d'utilisateur**, sélectionnez **Administrateur** et cliquez sur **Mot de passe oublié**.
3. Entrez la réponse à la question secrète que vous avez sélectionnée lors de la création de votre compte administrateur.
4. Cliquez sur **Valider**.

   Votre mot de passe d'administrateur s'affiche.

Modification du mot de passe administrateur

Si vous ne vous souvenez pas du mot de passe administrateur ou si vous pensez que sa confidentialité a pu être compromise, vous pouvez le modifier.

Pour modifier le mot de passe administrateur :

1. Cliquez à l'aide du bouton droit de la souris sur l'icône M de SecurityCenter, puis cliquez sur **Changer d'utilisateur**.
2. Dans la liste **Nom d'utilisateur**, sélectionnez **Administrateur** et cliquez sur **Changer le mot de passe**.
3. Entrez votre mot de passe dans la zone **Ancien mot de passe**.
4. Entrez un nouveau mot de passe dans la zone **Mot de passe**, puis entrez-le à nouveau dans la zone **Confirmer le mot de passe**.
5. Cliquez sur **OK**.

Configuration des options de mise jour

SecurityCenter est configuré pour vérifier automatiquement toutes les quatre heures les mises à jour de tous vos services McAfee lorsque vous êtes connecté à Internet et pour installer automatiquement les dernières mises à jour du produit. Toutefois, vous pouvez à tout moment rechercher manuellement les mises à jour grâce à l'icône SecurityCenter de la zone de notification située à l'extrême droite de la barre des tâches.

Recherche automatique de mises à jour

SecurityCenter recherche automatiquement les mises à jour toutes les quatre heures lorsque vous êtes connecté à Internet. Cependant, vous pouvez configurer SecurityCenter de manière à recevoir une notification avant le téléchargement ou l'installation automatique des mises à jour.

Pour rechercher des mises à jour automatiquement :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'état **Des mises à jour automatiques sont activées** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sélectionnez l'une des options suivantes dans le volet Options de mise à jour :
   - Installer les mises à jour automatiquement et m'avertir quand le produit est mis à jour (recommandé) (page 27)
   - Télécharger automatiquement les mises à jour et m'avertir de la possibilité de les installer (page 28)
   - M'avertir avant de télécharger une mise à jour (page 28)
4. Cliquez sur **OK**.

Remarque : pour une protection maximale, il est préférable que SecurityCenter recherche et installe automatiquement les mises à jour. Toutefois, si vous souhaitez uniquement mettre à jour vos services de sécurité manuellement, vous pouvez désactiver la mise à jour automatique (page 29).

Téléchargement et installation automatiques de mises à jour

Si vous sélectionnez **Installer automatiquement les mises à jour de mes services et m'avertir de l'opération une fois terminée (recommandé)** dans les options de mise à jour, SecurityCenter télécharge et installe automatiquement les mises à jour.

Téléchargement automatique de mises à jour

Si vous sélectionnez **Télécharger les mises à jour automatiquement et m'avertir quand elles sont prêtes à être installées** dans la boîte de dialogue Options de mise à jour, SecurityCenter télécharge automatiquement les mises à jour et vous avertit dès qu'une mise à jour est prête à être installée. Vous pouvez choisir d'installer la mise à jour ou de la reporter (page 29).

Pour installer une mise à jour téléchargée automatiquement :

1. Cliquez sur **Mettre à jour mes produits maintenant**, puis sur **OK**.

   Si vous y êtes invité, vous devez vous connecter au site Web pour vérifier votre abonnement avant que le téléchargement ne puisse démarrer.

2. Une fois votre abonnement vérifié, cliquez sur **Mettre à jour** dans le volet Mises à jour afin de télécharger et d'installer la mise à jour. Si votre abonnement est arrivé à expiration, cliquez sur **Renouveler mon abonnement** dans le message d'alerte et suivez les indications.

Remarque : dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Enregistrez votre travail et fermez tous les programmes avant de redémarrer.

Notification avant téléchargement de mises à jour

Si vous sélectionnez **M'avertir avant de télécharger une mise à jour** dans la boîte de dialogue Options de mise à jour, SecurityCenter vous avertit avant de télécharger les mises à jour. Vous pouvez alors choisir de télécharger et d'installer la mise à jour de vos services de sécurité afin d'éliminer toute menace d'attaque.

Pour télécharger et installer une mise à jour :

1. Sélectionnez **Mettre à jour mes produits maintenant**, puis sur **OK**.

2. Connectez-vous au site Web si vous y êtes invité.

   La mise à jour est automatiquement téléchargée.

3. Cliquez sur **OK** une fois l'installation de la mise à jour terminée.

Remarque : dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Enregistrez votre travail et fermez tous les programmes avant de redémarrer.

Désactivation de la mise à jour automatique

Pour une protection maximale, il est préférable que SecurityCenter recherche et installe automatiquement les mises à jour. Toutefois, si vous souhaitez procéder uniquement à la mise à jour manuelle de vos services de sécurité, vous pouvez désactiver la mise à jour automatique.

Remarque : n'oubliez pas de rechercher manuellement les mises à jour (page 30) au moins une fois par semaine. Si vous ne recherchez pas de mises à jour, votre ordinateur n'est pas protégé par les dernières mises à jour de sécurité.

Pour désactiver la mise à jour automatique :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'état **Des mises à jour automatiques sont activées** pour ouvrir le volet correspondant.
3. Cliquez sur **Inactif**.
4. Cliquez sur **Oui** pour confirmer les modifications.

   L'état est mis à jour dans l'en-tête.

Si vous n'avez pas recherché manuellement les mises à jour au bout de sept jours, une alerte vous rappelle de le faire.

Report des mises à jour

Si vous êtes trop occupé pour mettre à jour vos services de sécurité lorsque l'alerte apparaît, vous pouvez choisir d'être rappelé ultérieurement ou ignorer l'alerte.

Pour reporter une mise à jour :

- Effectuez l'une des opérations suivantes.
  - Sélectionnez **Me le rappeler ultérieurement**, puis cliquez sur **OK**.
  - Sélectionnez **Fermer cette alerte**, puis cliquez sur **OK** pour fermer l'alerte sans rien faire d'autre.

Recherche manuelle de mises à jour

SecurityCenter est configuré pour rechercher automatiquement des mises à jour toutes les quatre heures lorsque vous êtes connecté à Internet et pour installer les dernières mises à jour du produit. Toutefois, vous pouvez à tout moment rechercher manuellement les mises à jour grâce à l'icône SecurityCenter de la zone de notification Windows située à l'extrême droite de la barre des tâches.

Remarque : pour une protection maximale, il est préférable que SecurityCenter recherche et installe automatiquement les mises à jour. Toutefois, si vous souhaitez uniquement mettre à jour vos services de sécurité manuellement, vous pouvez désactiver la mise à jour automatique (page 29).

Pour rechercher des mises à jour manuellement :

1. Assurez-vous que votre ordinateur est bien connecté à Internet.
2. Cliquez avec le bouton droit de la souris sur l'icône M de SecurityCenter dans la zone de notification Windows située à l'extrême droite de la barre des tâches, puis cliquez sur **Mises à jour**.

   Pendant que SecurityCenter recherche des mises à jour, vous pouvez continuer à travailler avec cette application.

   Pour plus de facilité, une icône animée s'affiche dans la zone de notification Windows située à l'extrême droite de la barre des tâches. Une fois que SecurityCenter a terminé, cette icône disparaît automatiquement.
3. Si vous y êtes invité, connectez-vous au site Web pour vérifier l'état de votre abonnement.

Remarque : dans certains cas, vous serez invité à redémarrer votre ordinateur pour terminer la mise à jour. Enregistrez votre travail et fermez tous les programmes avant de redémarrer.

Configuration des options d'alerte

SecurityCenter utilise des alertes et des sons pour vous avertir automatiquement des attaques générales de virus, des menaces et des mises à jour produit. Vous pouvez cependant configurer SecurityCenter pour afficher uniquement les alertes à traiter immédiatement.

Configuration des options d’alerte

SecurityCenter utilise des alertes et des sons pour vous avertir automatiquement des attaques générales de virus, des menaces et des mises à jour produit. Vous pouvez cependant configurer SecurityCenter pour afficher uniquement les alertes à traiter immédiatement.

Pour configurer les options d'alerte :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Alertes** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sélectionnez l'une des options suivantes dans le volet Options d’alerte :
   - **M'avertir en cas d'attaque générale d'un virus ou de menace**
   - **Afficher les alertes d'information en mode jeu**
   - **Emettre un son en cas d’alerte**
   - **Afficher l'écran d'accueil de McAfee au démarrage de Windows**
4. Cliquez sur **OK**.

Remarque : pour désactiver les alertes d'information, cochez la case **Ne plus afficher cette alerte**. Vous pourrez les réactiver ultérieurement à partir du volet Alertes d'information.

Configuration des alertes d'information

Les alertes d'information ne nécessitent pas un traitement immédiat. Si vous désactivez les alertes de d'information depuis l'alerte, vous pourrez les réactiver ultérieurement à partir du volet Alertes d'information.

Pour configurer les alertes d'information :

1. Sous **SecurityCenter - Informations**, cliquez sur **Configurer**.
2. Cliquez sur la flèche en regard de l'option **Alertes** pour ouvrir le volet correspondant, puis sur **Options avancées**.
3. Sous **Configuration de SecurityCenter**, cliquez sur **Alertes d'information**.
4. Décochez la case **Masquer les alertes de type Informations**, puis décochez dans la liste les cases correspondant aux alertes que vous souhaitez afficher.
5. Cliquez sur **OK**.

CHAPITRE 5

Exécution de tâches courantes

Vous pouvez exécuter des tâches courantes comme revenir au volet Accueil, afficher les événements récents, gérer votre réseau informatique (si l'ordinateur dispose des droits appropriés) et mettre à jour votre ordinateur. Si McAfee Data Backup est installé, vous pouvez également sauvegarder vos données.

Contenu de ce chapitre

Exécution de tâches courantes

Vous pouvez exécuter des tâches courantes comme revenir au volet Accueil, afficher les événements récents, mettre à jour votre ordinateur, gérer votre réseau informatique (si l'ordinateur dispose des droits appropriés) et sauvegarder vos données (si McAfee Data Backup est installé).

Pour exécuter des tâches courantes :

- Sous **Tâches courantes** dans le Menu de base, sélectionnez l'une des options suivantes :
  - Pour revenir au volet Accueil, cliquez sur **Accueil**.
  - Pour afficher les événements récents détectés par votre logiciel de sécurité, cliquez sur **Evénements récents**.
  - Pour supprimer des fichiers inutilisés, défragmenter vos données et rétablir les paramètres précédents de votre ordinateur, cliquez sur **Mettre à jour l'ordinateur**.
  - Pour gérer votre réseau informatique, cliquez sur **Gérer un réseau** à partir d'un ordinateur disposant des droits de gestion sur ce réseau.

    Network Manager surveille les vulnérabilités des ordinateurs de votre réseau en matière de sécurité pour vous permettre d'identifier facilement les problèmes de sécurité réseau.
  - Pour créer des copies de sauvegarde de vos fichiers, cliquez sur **Sauvegarde des données** si McAfee Data Backup est installé.

La fonction de sauvegarde automatique enregistre des copies de vos fichiers les plus précieux à tout moment, les chiffre et les stocke sur CD/DVD, clé USB ou disque externe réseau.

Conseil : pour votre commodité, vous pouvez effectuer des tâches courantes depuis deux autres emplacements (sous **Accueil** dans le Menu avancé et sous le menu **QuickLinks** accessible à partir de l'icône M de SecurityCenter située à l'extrême droite de la barre des tâches). Vous pouvez également consulter la liste des événements récents et des journaux complets par type sous **Journaux et rapports**, à partir du Menu avancé.

Affichage des événements récents

Les événements récents sont consignés lorsque des modifications sont apportées à votre ordinateur (par exemple, lorsqu'un type de protection est activé ou désactivé, qu'une menace potentielle est supprimée ou qu'une tentative de connexion Internet est bloquée). Vous pouvez afficher les 20 événements les plus récents et les informations sur ceux-ci.

Consultez le fichier d'aide du produit correspondant pour obtenir des informations détaillées sur ces événements.

Pour afficher les événements récents :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Afficher les événements récents**.

   Tous les événements récents apparaissent dans la liste, accompagnés de la date et d'une description générale de celui-ci.

2. Sous **Evénements récents**, sélectionnez un événement pour afficher des informations complémentaires dans le volet Détails.

   La liste des actions disponibles apparaît sous **Je souhaite**.

3. Pour afficher une liste d'événements plus complète, cliquez sur **Afficher le journal**.

Mise à jour automatique de votre ordinateur

Pour libérer un espace précieux sur votre disque dur et optimiser les performances de votre ordinateur, vous pouvez planifier à intervalles réguliers l'exécution de tâches avec QuickClean ou le défragmenteur de disque. Le programme exécute notamment les tâches telles que la suppression, le broyage et la défragmentation des fichiers et dossiers.

Pour mettre à jour automatiquement les données de votre ordinateur :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Tâches planifiées**, cliquez sur **Démarrer**.
3. Dans la liste des opérations, sélectionnez **QuickClean** ou **défragmenteur de disque**.
4. Effectuez l'une des opérations suivantes.
   - Pour modifier une tâche existante, sélectionnez-la puis cliquez sur **Modifier**. Suivez les instructions à l'écran.
   - Pour créer une tâche, entrez un nom dans la zone **Nom de la tâche**, puis cliquez sur **Créer**. Suivez les instructions à l'écran.
   - Pour supprimer une tâche, sélectionnez-la et cliquez sur **Supprimer**.
5. Sous **Récapitulatif de la tâche**, consultez le moment de la dernière exécution, celui de la prochaine exécution et l'état de la tâche.

Mise à jour manuelle de votre ordinateur

Vous pouvez exécuter des tâches de maintenance manuelles pour supprimer des fichiers inutilisés, défragmenter vos données ou rétablir les paramètres précédents de votre ordinateur.

Pour mettre à jour manuellement les données de votre ordinateur :

- Effectuez l'une des opérations suivantes.
  - Pour utiliser QuickClean, cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, cliquez sur **Mettre à jour l'ordinateur**, puis sur **Démarrer**.
  - Pour utiliser le défragmenteur de disque, cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, cliquez sur **Mettre à jour l'ordinateur**, puis sur **Analyser**.
  - Pour restaurer le système, dans le Menu avancé, cliquez sur **Outils**, **Restauration du système**, puis sur **Démarrer**.

Suppression de fichiers et de dossiers inutilisés

QuickClean permet de libérer un espace précieux sur votre disque dur et d'optimiser les performances de votre ordinateur.

Pour supprimer des fichiers et des dossiers inutilisés :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **QuickClean**, cliquez sur **Démarrer**.
3. Suivez les instructions à l'écran.

Défragmentation de fichiers et dossiers

La fragmentation des fichiers se produit lors de la suppression et de la création des fichiers et des dossiers. Généralement sans gravité, cette fragmentation ralentit les accès au disque et diminue les performances générales de l'ordinateur.

Utilisez la défragmentation pour réécrire des parties d'un fichier sur des secteurs contigus d'un disque dur afin d'augmenter la vitesse d'accès aux données et la récupération de celles-ci.

Pour défragmenter des fichiers et des dossiers :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Mettre à jour l'ordinateur**.
2. Sous **Défragmenteur de disque**, cliquez sur **Analyse**.
3. Suivez les instructions à l'écran.

Restauration des paramètres précédents de votre ordinateur

Les points de restauration sont des « instantanés » de votre ordinateur enregistrés périodiquement par Windows et en cas d'événement significatif (par exemple, l'installation d'un programme ou d'un pilote). Toutefois, vous pouvez également créer et nommer à tout moment vos propres points de restauration.

Utilisez les points de restauration pour annuler des modifications importantes apportées aux paramètres de votre ordinateur et rétablir les paramètres précédents.

Pour rétablir les paramètres précédents de votre ordinateur :

1. Dans le menu Avancé, cliquez sur **Outils**, puis sur **Restauration du système**.
2. Sous **Restauration du système**, cliquez sur **Démarrer**.
3. Suivez les instructions à l'écran.

Gestion de votre réseau

Si votre ordinateur dispose des droits de gestion sur le réseau, Network Manager surveille les vulnérabilités des ordinateurs de votre réseau en matière de sécurité pour vous permettre d'identifier facilement les problèmes de sécurité.

Si l'état de protection de votre ordinateur n'est pas surveillé sur ce réseau, cet ordinateur ne fait pas partie du réseau ou il est défini comme membre non géré de celui-ci. Consultez le fichier d'aide sur Network Manager pour plus d'informations.

Pour gérer votre réseau :

1. Cliquez avec le bouton droit de la souris sur l'icône principale SecurityCenter, pointez sur **QuickLinks**, puis cliquez sur **Gérer un réseau**.
2. Cliquez sur l'icône représentant cet ordinateur sur la carte du réseau.
3. Sous **Je souhaite**, cliquez sur **Surveiller cet ordinateur**.

Plus d'informations sur les virus

Utilisez la bibliothèque d'informations sur les virus et Virus Map pour effectuer les opérations suivantes :

- Obtenez des informations sur les derniers virus, canulars par e-mail et autres menaces.
- Bénéficiez d'outils de suppressions de virus gratuits pour réparer votre ordinateur.
- Obtenez une vue aérienne en temps réel de la carte des ordinateurs infectés par les derniers virus dans le monde.

Pour plus d'informations sur les virus :

1. Dans le menu Avancé, cliquez sur **Outils**, puis sur **Informations sur les virus**.
2. Effectuez l'une des opérations suivantes :
   - Recherchez les virus à l'aide de la bibliothèque d'informations sur les virus de McAfee.
   - Recherchez les virus à l'aide de World Virus Map sur le site Web de McAfee.

CHAPITRE 6

McAfee QuickClean

Lorsque vous surfez sur Internet, votre ordinateur accumule rapidement des fichiers encombrants. Avec QuickClean, protégez votre confidentialité et débarrassez-vous de l'encombrement inutile engendré par Internet et les e-mails. QuickClean identifie et supprime les fichiers qui s'accumulent au cours de la navigation sur Internet, tels que les cookies, les e-mails, les téléchargements et les historiques, autant de fichiers de données qui contiennent des informations personnelles vous concernant. Il protège votre confidentialité en permettant la suppression sécurisée de ces informations sensibles.

QuickClean supprime également les programmes indésirables. Indiquez les fichiers à supprimer et éliminez l'encombrement tout en préservant les informations essentielles.

Contenu de ce chapitre

Présentation des fonctions de QuickClean

Cette section décrit les fonctions de QuickClean.

Fonctions

QuickClean offre un ensemble d'outils efficaces et faciles à utiliser qui suppriment en toute sécurité les éléments inutiles de votre ordinateur. Vous pouvez ainsi libérer un espace disque précieux et optimiser les performances de votre ordinateur.

CHAPITRE 7

Nettoyage de votre ordinateur

QuickClean vous permet de vraiment supprimer des fichiers et des dossiers.

Lorsque vous naviguez sur Internet, votre navigateur copie chaque page Internet et ses graphiques dans un dossier cache du disque dur. Il peut ainsi charger rapidement une page sur laquelle vous retournez. La mise en cache des fichiers est utile si vous consultez souvent les mêmes pages Internet et que leur contenu ne change que rarement. Mais, la plupart du temps, les fichiers mis en cache sont inutiles et peuvent donc être supprimés.

Les nettoyeurs suivants vous permettent de supprimer divers éléments.

- Nettoyeur de la Corbeille : nettoie la Corbeille de Windows.
- Nettoyeur de fichiers temporaires : supprime les fichiers stockés dans des dossiers temporaires.
- Nettoyeur de raccourcis : supprime les raccourcis inutilisables et les raccourcis non associés à un programme.
- Nettoyeur de fragments de fichiers perdus : supprime de l'ordinateur les fragments de fichier perdus.
- Nettoyeur de registre : supprime du registre Windows les informations correspondant à des programmes désormais inexistants.
- Nettoyeur du cache : supprime les fichiers mis en cache qui s'accumulent lorsque vous naviguez sur Internet. Ils sont généralement stockés sous forme de fichiers Internet temporaires.
- Nettoyeur de cookies : supprime les cookies. Ils sont généralement stockés sous forme de fichiers Internet temporaires.
  Les cookies sont de petits fichiers que votre navigateur Internet stocke sur l'ordinateur à la demande d'un serveur Web. Chaque fois que vous affichez une page à partir du serveur Web, le navigateur renvoie le cookie au serveur. Ces cookies peuvent jouer le rôle d'étiquette, ce qui permet au serveur Web de savoir quelles pages vous consultez et à quelle fréquence.
- Nettoyeur de l'historique du navigateur : supprime l'historique de votre navigateur.

- Nettoyeur d'e-mails Outlook Express et Outlook (éléments supprimés et envoyés) : supprime les e-mails des dossiers Outlook Envoyé et Supprimé.
- Nettoyeur récemment utilisé : supprime les éléments récemment utilisés stockés sur votre ordinateur, tels que les documents Microsoft Office.
- Nettoyeur de plug-ins et de contrôles ActiveX : supprime les plug-ins et les contrôles ActiveX.
  ActiveX est une technologie utilisée pour implémenter des contrôles dans un programme. Un contrôle ActiveX permet, par exemple, d'ajouter un bouton à l'interface d'un programme. La plupart de ces contrôles sont inoffensifs ; cependant, des personnes mal intentionnées utilisent la technologie ActiveX pour récupérer des informations sur votre ordinateur.
  Les plug-ins sont de petits programmes qui s'intègrent à des applications plus importantes pour offrir une fonctionnalité supplémentaire. Grâce aux plug-ins, le navigateur Web peut exécuter des fichiers incorporés à des documents HTML, dans des formats qu'il ne reconnaîtrait pas normalement (par exemple, fichiers vidéo, audio et d'animation).
- Nettoyeur de points de restauration du système : supprime les anciens points de restauration du système de votre ordinateur.

Contenu de ce chapitre

Utilisation de QuickClean

Cette section présente l'utilisation de QuickClean.

Nettoyage de votre ordinateur

Vous pouvez supprimer les fichiers et dossiers inutilisés, libérer de l'espace disque et améliorer le fonctionnement de votre ordinateur.

Pour nettoyer votre ordinateur :

1. dans le menu Avancé, cliquez sur **Outils**.
2. Cliquez sur **Gérer l'ordinateur**, puis sur **Démarrer** sous **McAfee QuickClean**.
3. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** pour utiliser les nettoyeurs par défaut de la liste.
   - Sélectionnez ou désactivez les nettoyeurs appropriés, puis cliquez sur **Suivant.** Pour le Nettoyeur récemment utilisé, vous pouvez cliquer sur **Propriétés** pour éliminer les programmes dont vous ne souhaitez pas nettoyer les listes.
   - Cliquez sur **Paramètres par défaut** pour rétablir les nettoyeurs par défaut, puis cliquez sur **Suivant.**
4. Lorsque l'analyse est terminée, cliquez sur **Suivant** pour confirmer la suppression des fichiers. Vous pouvez développer cette liste pour voir les fichiers qui seront nettoyés et leur emplacement.
5. Cliquez sur **Suivant**.
6. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Suivant** si vous acceptez l'option par défaut **Non, je souhaite supprimer les fichiers à l'aide de la fonction Windows standard**.
   - Cliquez sur **Oui, je souhaite procéder à la suppression sécurisée de mes fichiers à l'aide de Shredder** et spécifiez le nombre de passages. Les fichiers supprimés à l'aide de Shredder ne peuvent pas être récupérés.
7. Cliquez sur **Terminer**.
8. Sous **Résumé QuickClean**, consultez le nombre de fichiers de registre supprimés et le volume d'espace disque récupéré après le nettoyage du disque et la suppression des éléments générés par Internet.

CHAPITRE 8

McAfee Shredder

Vous pouvez récupérer les fichiers supprimés sur votre ordinateur, même après avoir vidé la Corbeille. Lorsque vous supprimez un fichier, Windows marque cet espace sur votre lecteur de disque comme inutilisé, mais le fichier est toujours là. Avec des outils d'expertise informatique judiciaire, il est possible de récupérer des déclarations d'impôt, des CV ou d'autres documents que vous avez supprimés. Shredder protège votre confidentialité en supprimant en toute sécurité et de manière définitive les fichiers indésirables.

Pour supprimer un fichier définitivement, vous devez écraser le fichier existant plusieurs fois avec de nouvelles données. Microsoft® Windows ne supprime pas les fichiers de manière définitive parce que cette opération serait très lente. Le fait de broyer un document n'empêche pas sa récupération, car certains programmes créent des copies cachées temporaires des documents ouverts. Si vous ne broyez que les documents visibles dans l'Explorateur Windows®, il se peut qu'il existe encore des copies temporaires de ces documents.

Remarque : les fichiers broyés ne sont pas sauvegardés. Il est impossible de restaurer des fichiers effacés par Shredder.

Contenu de ce chapitre

Présentation des fonctions de Shredder

Cette section décrit les fonctions de Shredder.

Fonctionnalités

Shredder vous permet d'effacer le contenu de la Corbeille, les fichiers Internet temporaires, l'historique des sites Web, les fichiers, les dossiers et les disques.

CHAPITRE 9

Effacement des fichiers indésirables avec Shredder

Shredder protège votre confidentialité en supprimant en toute sécurité et de manière définitive les fichiers indésirables tels que le contenu de la Corbeille, les fichiers Internet temporaires et l'historique des sites Web. Vous pouvez sélectionner les fichiers et les dossiers à broyer, ou naviguer jusqu'à leur emplacement.

Contenu de ce chapitre

Utilisation de Shredder

Cette section vous explique comment utiliser Shredder.

Broyage des fichiers, des dossiers et des disques.

Des fichiers peuvent résider sur votre ordinateur, même après que vous ayez vidé la Corbeille. Cependant, lorsque vous broyez des fichiers, vos données sont définitivement supprimées et les pirates informatiques ne peuvent plus y accéder.

Pour broyer des fichiers, des dossiers et des disques :

1. Dans le menu Avancé, cliquez sur **Outils**, puis sur **Shredder**.
2. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Effacer des fichiers et des dossiers** pour broyer des fichiers et des dossiers.
   - Cliquez sur **Effacer un disque entier** pour broyer des disques.
3. Sélectionnez l'un des niveaux de broyage suivants :
   - **Rapide** : broie 1 fois les éléments sélectionnés.
   - **Complet** : broie 7 fois les éléments sélectionnés.
   - **Personnalisé** : broie jusqu'à 10 fois les éléments sélectionnés. Un nombre élevé de broyages augmente le niveau de sécurité de suppression des fichiers.
4. Cliquez sur **Suivant**.
5. Effectuez l'une des opérations suivantes :
   - Si vous broyez des fichiers, cliquez sur **Contenu de la Corbeille**, **Fichiers Internet temporaires** ou **Historique des sites Web** dans la liste **Sélectionnez le(s) fichier(s) à broyer**. Si vous broyez un disque, sélectionnez le disque.
   - Cliquez sur **Parcourir**, naviguez jusqu'aux fichiers que vous voulez broyer, puis sélectionnez-les.
   - Saisissez le chemin d'accès aux fichiers que vous voulez broyer dans la liste **Sélectionnez le(s) fichier(s) à broyer**.
6. Cliquez sur **Suivant**.
7. Cliquez sur **Terminer** pour terminer l'opération.
8. Cliquez sur **Terminé**.

CHAPITRE 10

McAfee Network Manager

McAfee® Network Manager présente sous forme graphique les ordinateurs et les autres composants de votre réseau. Vous pouvez utiliser Network Manager pour surveiller à distance l'état de protection de chaque ordinateur géré de votre réseau, mais aussi pour corriger à distance les points faibles de la sécurité de ces ordinateurs gérés.

Avant de commencer à utiliser Network Manager, nous vous conseillons de vous familiariser avec ses fonctionnalités les plus utilisées. Pour plus de détails sur la configuration et l'utilisation de ces fonctionnalités, consultez l'aide de Network Manager.

Contenu de ce chapitre

Fonctionnalités

Network Manager propose les fonctionnalités suivantes :

Carte graphique du réseau

La carte du réseau de Network Manager est une représentation graphique du niveau de sécurité des ordinateurs et des composants de votre réseau domestique. Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), la carte du réseau identifie ces changements. Vous pouvez actualiser la carte du réseau, renommer le réseau, ou encore afficher ou masquer des composants de la carte du réseau. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Gestion à distance

Utilisez la carte du réseau de Network Manager pour gérer le niveau de sécurité des ordinateurs qui constituent votre réseau domestique. Vous pouvez inviter un ordinateur à s'affilier au réseau géré, surveiller le niveau de protection des ordinateurs gérés et régler les problèmes connus de failles de sécurité du réseau à partir d'un ordinateur distant.

Présentation des icônes de Network Manager

Le tableau suivant décrit les icônes les plus utilisées sur la carte du réseau Network Manager.

Icône	Description
	Représente un ordinateur géré connecté au réseau
	Représente un ordinateur géré non connecté au réseau
	Représente un ordinateur non géré sur lequel McAfee Security 2007 est installé
	Représente un ordinateur non géré non connecté au réseau
	Représente un ordinateur connecté au réseau sur lequel McAfee Security 2007 n'est pas installé ou un matériel inconnu sur le réseau
	Représente un ordinateur non connecté au réseau sur lequel McAfee Security 2007 n'est pas installé ou un matériel inconnu non connecté au réseau
	Signifie que l'élément correspondant est protégé et connecté
	Signifie que l'élément correspondant nécessite votre attention
	Signifie que l'élément correspondant nécessite votre attention et qu'il est déconnecté
	Représente un routeur personnel sans fil
	Représente un routeur personnel standard
	Représente Internet en mode connexion
	Représente Internet en mode déconnexion

CHAPITRE 11

Configuration d'un réseau géré

Pour configurer un réseau géré, vous triez les éléments de la carte de votre réseau et vous ajoutez des membres (des ordinateurs) au réseau.

Contenu de ce chapitre

Utilisation de la carte du réseau

Chaque fois que vous connectez un ordinateur au réseau, Network Manager analyse l'état du réseau afin de déterminer ses membres (gérés ou non), les attributs du routeur et l'état Internet. Si aucun membre n'est trouvé, Network Manager suppose que l'ordinateur actuellement connecté est le premier du réseau et en fait automatiquement un membre géré avec des autorisations d'administration. Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de McAfee Security 2007. Vous pouvez modifier le nom du réseau à tout moment.

Lorsque vous modifiez votre réseau (lorsque vous ajoutez un ordinateur, par exemple), vous pouvez personnaliser la carte du réseau. Ainsi, vous pouvez actualiser la carte du réseau, renommer le réseau et afficher/masquer des composants de la carte. Vous pouvez également afficher les détails associés aux composants de la carte du réseau.

Accéder à la carte du réseau

Pour accéder à une carte de votre réseau, lancez Network Manager depuis la liste des tâches communes de SecurityCenter. La carte du réseau propose une représentation graphique des ordinateurs et des autres composants de votre réseau.

Pour accéder à la carte du réseau :

- Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**.
  La carte du réseau apparaît dans le panneau de droite.

Remarque : pour afficher la carte du réseau, vous devez commencer par autoriser les autres ordinateurs du réseau au premier accès à la carte.

Actualiser la carte du réseau

Vous pouvez actualiser la carte du réseau à tout moment, lorsqu'un nouvel ordinateur est affilié au réseau géré par exemple.

Pour actualiser la carte du réseau :

1. Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**.
   La carte du réseau apparaît dans le panneau de droite.
2. Cliquez sur **Actualiser la carte du réseau** sous **Je souhaite**.

Remarque : le lien **Actualiser la carte du réseau** n'est disponible que si aucun élément n'est sélectionné sur la carte du réseau. Pour désélectionner un élément, cliquez sur l'élément sélectionné ou sur une zone vide de la carte du réseau.

Attribution d'un nouveau nom au réseau

Par défaut, le nom du réseau inclut le nom du groupe de travail ou du domaine du premier ordinateur qui se connecte au réseau équipé de McAfee Security 2007. Si ce nom ne vous convient pas, vous pouvez le modifier.

Pour renommer le réseau :

1. Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**.
   La carte du réseau apparaît dans le panneau de droite.
2. Cliquez sur **Renommer le réseau** sous **Je souhaite**.
3. Saisissez le nom de votre ami dans le champ **Renommer le réseau**.
4. Cliquez sur **OK**.

Remarque : le lien **Renommer le réseau** n'est disponible que si aucun élément n'est sélectionné sur la carte du réseau. Pour désélectionner un élément, cliquez sur l'élément sélectionné ou sur une zone vide de la carte du réseau.

Afficher ou masquer des éléments de la carte du réseau

Par défaut, les ordinateurs et les autres composants de votre réseau apparaissent sur la carte du réseau. Si vous avez masqué des éléments, vous pouvez les réafficher à tout moment. Seuls les éléments non gérés peuvent être masqués. Les ordinateurs gérés ne peuvent pas être masqués.

Pour...	Dans le menu de base ou le menu avancé, cliquez sur **Gérer un réseau**, puis...
Masquer un élément de la carte du réseau	Cliquez sur un élément de la carte du réseau, puis sur **Masquer cet élément** sous **Je souhaite**. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.
Afficher des éléments masqués de la carte du réseau	Sous **Je souhaite**, cliquez sur **Afficher les éléments masqués**.

Afficher les détails d'un élément

Sélectionnez un composant de votre réseau dans la carte du réseau pour afficher des informations détaillées concernant ce composant. Ces informations comprennent le nom du composant, l'état de sa protection et d'autres informations nécessaires pour gérer le composant.

Pour afficher les détails d'un élément :

1. Cliquez sur l'icône d'un élément sur la carte du réseau.
2. Sous **Détails**, affichez des informations sur l'objet.

Affiliation au réseau géré

Pour qu'un ordinateur puisse être géré à distance ou qu'il reçoive les autorisations nécessaires pour gérer d'autres ordinateurs à distance sur le réseau, il doit devenir membre autorisé du réseau. L'appartenance au réseau est accordée aux nouveaux ordinateurs par ceux qui sont déjà membres du réseau et qui possèdent des autorisations d'administration. Pour garantir que seuls les ordinateurs autorisés s'affilient au réseau, les utilisateurs des ordinateurs qui accordent les autorisations et ceux qui s'affilient au réseau doivent s'authentifier mutuellement.

Lorsqu'un ordinateur s'affilie au réseau, il est invité à indiquer l'état de sa protection McAfee aux autres ordinateurs du réseau. Si un ordinateur accepte d'afficher l'état de sa protection, il devient un membre *géré* du réseau. Si un ordinateur refuse d'afficher l'état de sa protection, il devient un membre *non géré* du réseau. Les membres non gérés du réseau sont généralement des invités qui souhaitent accéder à d'autres fonctionnalités du réseau (partage de fichiers ou d'impression, par exemple).

Remarque : après vous être affilié, si d'autres programmes réseau McAfee sont installés (McAfee Wireless Network Security ou EasyNetwork, par exemple), l'ordinateur est également reconnu comme étant un ordinateur géré pour ces programmes. Le niveau d'autorisation affecté à un ordinateur dans Network Manager s'applique à tous les programmes réseau McAfee. Pour obtenir des informations sur la signification des autorisations de type Invité, Complet ou Administration dans un autre programme réseau McAfee, reportez-vous à sa documentation.

Affiliation à un réseau géré

Lorsque vous êtes invité à vous affilier à un réseau géré, vous pouvez accepter ou refuser l'invitation. Vous pouvez également déterminer si vous voulez que cet ordinateur et les autres ordinateurs du réseau surveillent mutuellement leurs paramètres de sécurité (pour savoir par exemple si les services de protection antivirus d'un ordinateur sont à jour).

Pour s'affilier à un réseau géré :

1. Dans la boîte de dialogue d'invitation, cochez la case **Autoriser cet ordinateur et d'autres ordinateurs à surveiller les paramètres de sécurité les uns les autres** pour autoriser les autres ordinateurs du réseau géré à surveiller les paramètres de sécurité.
2. Cliquez sur l'option d'**affiliation**.
   Lorsque vous acceptez l'invitation, deux cartes à jouer s'affichent.
3. Vérifiez que ces cartes sont identiques à celles affichées sur l'ordinateur qui vous a invité à vous affilier au réseau géré.
4. Cliquez sur **Confirmer**.

Remarque : si l'ordinateur qui vous a invité à vous affilier au réseau géré n'affiche pas les mêmes cartes que celles de la boîte de dialogue de confirmation de la sécurité, le réseau géré est victime d'une faille de sécurité. Le fait de vous affilier au réseau risque de compromettre la sécurité de votre ordinateur. Par conséquent, nous vous conseillons de cliquer sur **Refuser** dans la boîte de dialogue de confirmation de la sécurité.

Inviter un ordinateur à s'affilier au réseau géré

Si un ordinateur est ajouté au réseau géré ou si un autre ordinateur non géré est déjà présent sur le réseau, vous pouvez inviter cet ordinateur à s'affilier au réseau géré. Seuls les ordinateurs avec des autorisations d'administration sur le réseau peuvent en inviter d'autres à s'y affilier. Lorsque vous envoyez l'invitation, vous spécifiez également le niveau d'autorisation que vous affectez à cet ordinateur.

Pour inviter un ordinateur à s'affilier au réseau géré :

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Surveiller cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue d'invitation à l'affiliation au réseau géré, cliquez sur l'une des options suivantes :
   - **Accorder l'accès à un invité**
     Permet à l'ordinateur d'accéder au réseau.

- **Accorder un accès complet à toutes les applications du réseau géré**
  Permet à l'ordinateur d'accéder au réseau, comme pour l'accès Invité.
- **Accorder un accès administratif à toutes les applications du réseau géré**
  Permet à l'ordinateur d'accéder au réseau avec des autorisations d'administration. L'ordinateur a par ailleurs la possibilité d'accorder un accès aux autres ordinateurs qui veulent s'affilier au réseau.

4 Cliquez sur **Inviter**.
Une invitation à s'affilier au réseau géré est envoyée à l'ordinateur. Lorsque l'ordinateur accepte l'invitation, deux cartes à jouer s'affichent.

5 Vérifiez que ces cartes sont identiques à celles affichées sur l'ordinateur que vous avez invité à s'affilier au réseau.

6 Cliquez sur **Autoriser l'accès**.

Remarque : si l'ordinateur que vous avez invité à s'affilier au réseau géré n'affiche pas les mêmes cartes que celles de la boîte de dialogue de confirmation de la sécurité, le réseau géré est victime d'une faille de sécurité. Le fait d'autoriser l'ordinateur à s'affilier au réseau risque de compromettre la sécurité des autres ordinateurs. Par conséquent, nous vous conseillons de cliquer sur **Refuser l'accès** dans la boîte de dialogue de confirmation de la sécurité.

Ne plus approuver les ordinateurs du réseau

Si vous avez accepté par erreur de faire confiance aux autres ordinateurs du réseau, vous pouvez arrêter de leur faire confiance.

Pour arrêter de faire confiance aux ordinateurs du réseau :

- Cliquez sur **Arrêter de faire confiance aux ordinateurs du réseau** sous **Je souhaite**.

Remarque : le lien **Arrêter de faire confiance aux ordinateurs du réseau** n'est disponible que si aucun autre ordinateur géré ne s'est affilié au réseau.

CHAPITRE 12

Gestion à distance du réseau

Une fois que vous avez configuré votre réseau géré, vous pouvez utiliser Network Manager pour gérer à distance les ordinateurs et les autres composants de votre réseau. Vous pouvez surveiller l'état et les niveaux de permission des ordinateurs et des autres composants, mais aussi corriger les problèmes de vulnérabilités, le tout à distance.

Contenu de ce chapitre

Surveillance de l'état et des autorisations

Un réseau géré comporte deux types de membres : des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection McAfee, contrairement aux membres non gérés. Les membres non gérés sont généralement des invités qui souhaitent accéder à d'autres fonctionnalités du réseau (partage de fichiers ou d'impression, par exemple). Un ordinateur non géré peut être invité à devenir géré à tout moment par un autre ordinateur géré du réseau. De même, un ordinateur géré peut devenir non géré à tout moment.

Des autorisations de type Administration, Complet ou Invité sont associées aux ordinateurs gérés. Les autorisations de type Administration permettent à l'ordinateur géré de gérer l'état de protection de tous les autres ordinateurs gérés du réseau, mais aussi d'accorder une appartenance aux autres ordinateurs du réseau. Les autorisations de type Complet et Invité ne permettent que l'accès au réseau. Vous pouvez modifier le niveau d'autorisation d'un ordinateur à tout moment.

Un réseau géré comporte également du matériel gérable via Network Manager (des routeurs, par exemple). Vous pouvez aussi configurer et modifier les propriétés d'affichage d'un matériel sur la carte du réseau.

Surveillance de l'état de protection d'un ordinateur

Si l'état de protection d'un ordinateur n'est pas surveillé sur le réseau (parce que l'ordinateur n'est pas membre du réseau ou parce qu'il est membre non géré), vous pouvez demander sa surveillance.

Pour surveiller l'état de protection d'un ordinateur :

1. Cliquez sur l'icône d'un ordinateur non géré sur la carte du réseau.
2. Cliquez sur **Surveiller cet ordinateur** sous **Je souhaite**.

Arrêt de la surveillance de l'état de protection d'un ordinateur

Vous pouvez arrêter de surveiller l'état de protection d'un ordinateur de votre réseau. L'ordinateur devient alors non géré.

Pour arrêter de surveiller l'état de protection d'un ordinateur :

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Arrêter de surveiller cet ordinateur** sous **Je souhaite**.
3. Cliquez sur **Oui** dans la boîte de dialogue de confirmation.

Modification des autorisations d'un ordinateur géré

Vous pouvez modifier les autorisations d'un ordinateur géré à tout moment. Ainsi, vous pouvez choisir les ordinateurs qui vont surveiller l'état de protection (paramètres de sécurité) des autres ordinateurs du réseau.

Pour modifier les autorisations d'un ordinateur géré :

1. Cliquez sur l'icône d'un ordinateur géré sur la carte du réseau.
2. Cliquez sur **Modifier les autorisations de cet ordinateur** sous **Je souhaite**.
3. Dans la boîte de dialogue de modification des autorisations, sélectionnez ou désélectionnez la case à cocher afin de déterminer si cet ordinateur et les autres ordinateurs du réseau géré peuvent surveiller mutuellement l'état de leur protection.
4. Cliquez sur **OK**.

Gestion d'un matériel

Pour gérer un matériel, accédez à sa page Web d'administration depuis Network Manager.

Pour gérer un matériel :

1. Cliquez sur l'icône d'un matériel sur la carte du réseau.
2. Cliquez sur **Gérer ce matériel** sous **Je souhaite**.
   Un navigateur Web s'ouvre pour afficher la page Web d'administration du matériel.
3. Dans votre navigateur Web, fournissez vos informations de connexion, puis configurez les paramètres de sécurité du matériel.

Remarque : si le matériel est un point d'accès ou un routeur sans fil protégé par Wireless Network Security, vous devez utiliser Wireless Network Security pour en configurer les paramètres de sécurité.

Modification des paramètres d'affichage d'un matériel

Lorsque vous modifiez les paramètres d'affichage d'un matériel, vous pouvez le renommer sur la carte du réseau et spécifier s'il s'agit d'un routeur sans fil.

Pour modifier les paramètres d'affichage d'un matériel :

1. Cliquez sur l'icône d'un matériel sur la carte du réseau.
2. Cliquez sur **Modifier les propriétés du matériel** sous **Je souhaite**.
3. Pour spécifier le nom d'affichage du matériel, saisissez un nom dans la zone **Nom**.
4. Pour spécifier le type de matériel, cliquez sur un des éléments suivants :
   - **Routeur**
     Représente un routeur personnel standard.
   - **Routeur sans fil**
     Représente un routeur personnel sans fil.
5. Cliquez sur **OK**.

Réparation des failles de sécurité

Les ordinateurs gérés avec des autorisations de type Administration peuvent surveiller l'état de protection McAfee des autres ordinateurs gérés du réseau, mais aussi corriger à distance toute défaillance détectée en matière de sécurité. Ainsi, si l'état de protection McAfee d'un ordinateur géré indique que VirusScan est désactivé, un autre ordinateur géré avec des autorisations de type Administration peut activer VirusScan à distance pour *corriger* ce problème.

Lorsque vous corrigez à distance des défaillances en matière de sécurité, Network Manager répare automatiquement la plupart des problèmes rencontrés. Dans certains cas, une intervention manuelle directement sur l'ordinateur peut être nécessaire. Dans ce cas, Network Manager corrige tous les problèmes qui peuvent être réglés à distance, puis vous invite à corriger les problèmes restants. Connectez-vous alors à SecurityCenter sur l'ordinateur vulnérable et suivez les recommandations fournies. Dans certains cas, vous êtes invité à installer McAfee Security 2007 sur les ordinateurs du réseau.

Réparation automatique des failles de sécurité

Network Manager permet de corriger automatiquement la plupart des problèmes de sécurité sur les ordinateurs gérés distants. Par exemple, si VirusScan est désactivé sur un ordinateur distant, vous pouvez utiliser Network Manager pour le réactiver automatiquement.

Pour réparer les problèmes de sécurité :

1. Cliquez sur l'icône d'un élément sur la carte du réseau.
2. Sous **Détails**, affichez l'état de protection de l'élément.
3. Cliquez sur **Réparer les failles de sécurité** sous **Je souhaite**.
4. Une fois les problèmes de sécurité réglés, cliquez sur **OK**.

Remarque : bien que Network Manager corrige automatiquement la plupart des failles de sécurité, il peut parfois être nécessaire de lancer SecurityCenter sur l'ordinateur vulnérable et de suivre les recommandations fournies.

Installation de McAfee Security sur les ordinateurs distants

Si des ordinateurs de votre réseau n'exécutent pas McAfee Security 2007, l'état de leur sécurité ne peut pas être surveillé à distance. Pour surveiller ces ordinateurs à distance, vous devez installer McAfee Security 2007 sur chacun d'entre eux.

Pour installer McAfee Security sur un ordinateur distant :

1. Dans un navigateur de l'ordinateur distant, rendez-vous sur http://download.mcafee.com/us/.
2. Suivez les instructions à l'écran pour installer McAfee Security 2007 sur l'ordinateur.

CHAPITRE 13

McAfee VirusScan

VirusScan offre une protection anti-virus et anti-logiciels espions complète, fiable et à jour. Géré par notre moteur d'analyse McAfee à la pointe de la technologie, VirusScan protège votre ordinateur contre les virus, vers, chevaux de Troie, scripts suspects, rootkits, débordements de tampon, attaques hybrides, logiciels espions, programmes potentiellement indésirables et autres menaces.

Contenu de ce chapitre

Caractéristiques

Cette version de VirusScan offre les fonctions suivantes :

Une protection anti-virus

L'analyse en temps réel analyse les fichiers lorsque vous ou votre ordinateur y accédez.

Analyse

Une recherche des virus et autres menaces sur les disques durs et les disquettes, ainsi que dans les fichiers et dossiers individuels. Vous avez également la possibilité de cliquer sur un objet avec le bouton droit de la souris pour l'analyser.

Une détection des logiciels espions et publicitaires

VirusScan identifie et supprime les logiciels espions et publicitaires ainsi que tous les programmes susceptibles de compromettre la confidentialité de vos informations ou de ralentir votre ordinateur.

Mises à jour automatiques

Les mises à jour automatiques vous protègent contre les dernières menaces informatiques, identifiées ou non.

Analyse rapide en arrière-plan

Des analyses discrètes et rapides identifient et détruisent virus, chevaux de Troie, vers, logiciels espions et publicitaires, numéroteurs ainsi que toute autre menace sans interrompre votre activité.

Alertes de sécurité en temps réel

Les alertes de sécurité vous avertissent des nouvelles épidémies virales et des menaces de sécurité, tout en vous fournissant des possibilités de réponse pour supprimer, neutraliser ou mieux connaître la menace.

Détection et nettoyage à de multiples points d'entrée

VirusScan surveille et neutralise les menaces aux principaux points d'entrée de votre ordinateur : e-mails, pièces jointes contenues dans les messages instantanés et fichiers Internet téléchargés.

Surveillance des e-mails contre les activités de type ver

WormStopper™ empêche les chevaux de Troie d'envoyer par e-mail des vers à d'autres ordinateurs, et affiche une invite avant que des programmes e-mails inconnus n'envoient des messages e-mails à d'autres ordinateurs.

Surveillance des scripts contre les activités de type ver

ScriptStopper™ empêche des scripts connus et nocifs de s'exécuter sur votre ordinateur.

McAfee X-ray for Windows

McAfee X-ray détecte et détruit les rootkits et autres programmes qui se cachent de Windows.

Protection contre les débordements de tampon

La protection contre les débordements de tampon vous protège de ce type d'attaque. Les débordements de tampon se produisent lorsque des programmes ou des processus suspects tentent de stocker dans un tampon (zone de stockage temporaire des données) une quantité de données plus importante que votre ordinateur ne peut en contenir, ce qui endommage ou écrase les données valides des tampons adjacents.

McAfee SystemGuards

SystemGuards surveille certains comportements de votre ordinateur pouvant révéler la présence de virus et de logiciels espions ou l'activité d'un pirate.

CHAPITRE 14

Gestion de la protection anti-virus

Vous pouvez gérer la protection en temps réel contre les virus, les logiciels espions et les scripts, ainsi que les SystemGuards. Vous pouvez par exemple désactiver l'analyse ou définir ce que vous souhaitez analyser.

Seuls les utilisateurs disposant de droits d'accès administrateur sont habilités à modifier les options avancées.

Contenu de ce chapitre

Utilisation de la protection anti-virus

Une fois la protection anti-virus (analyse en temps réel) activée, elle surveille constamment votre ordinateur à la recherche d'une activité virale. L'analyse en temps réel analyse les fichiers à chaque fois que vous ou votre ordinateur y accédez. Lorsque la protection anti-virus détecte un fichier infecté, elle tente de le nettoyer ou de supprimer l'infection. Si un fichier ne peut être ni nettoyé ni supprimé, une alerte vous en avertit afin que vous preniez d'autres mesures.

Rubriques connexes

- Mieux comprendre les alertes de sécurité (page 103)

Désactivation de la protection anti-virus

Si vous désactivez la protection anti-virus, votre ordinateur ne sera pas surveillé en permanence à la recherche d'une activité virale. Si vous devez arrêter la protection anti-virus, assurez-vous que vous n'êtes pas connecté à Internet.

Remarque : la désactivation de la protection anti-virus entraîne également la désactivation de la protection en temps réel de la messagerie, de la messagerie instantanée et contre les logiciels espions.

Pour désactiver la protection anti-virus :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection anti-virus**, cliquez sur **Désactivé**.
4. Dans la boîte de dialogue de confirmation, effectuez l'une des actions suivantes :
   - Pour relancer la protection anti-virus après un certain temps, cochez la case **Réactivation de l'analyse en temps réel après**, puis sélectionnez une durée dans le menu.
   - Pour empêcher la protection anti-virus de redémarrer après un certain temps, désélectionnez la case **Réactivation de la protection anti-virus après**

5 Cliquez sur **OK**.

Si la protection en temps réel est configurée pour être lancée automatiquement au démarrage de Windows, votre ordinateur est protégé lorsque vous le redémarrez.

Rubriques connexes

- Configuration de la protection en temps réel (page 74)

Activation de la protection anti-virus

La protection anti-virus surveille votre ordinateur en permanence à la recherche d'une activité virale.

Pour activer la protection anti-virus :

1 Dans le menu Avancé, cliquez sur **Configurer**.

2 Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.

3 Sous **Protection anti-virus**, cliquez sur **Activé**.

Configuration de la protection en temps réel

Vous avez la possibilité de modifier la protection anti-virus en temps réel. Vous pouvez par exemple choisir de n'analyser que les fichiers programme et documents ou de désactiver l'analyse en temps réel au démarrage de Windows (non recommandé).

Configuration de la protection en temps réel

Vous avez la possibilité de modifier la protection anti-virus en temps réel. Vous pouvez par exemple choisir de n'analyser que les fichiers programme et documents ou de désactiver l'analyse en temps réel au démarrage de Windows (non recommandé).

Pour configurer la protection en temps réel :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection anti-virus**, cliquez sur **Avancé**.
4. Sélectionnez ou désélectionnez les cases à cocher suivantes :
   - **Détecter les virus inconnus en utilisant des techniques heuristiques** : les fichiers sont comparés aux signatures de virus déjà connus afin de détecter les signes de virus non identifiés. Bien qu'effectuant l'analyse la plus complète, cette option est généralement plus lente qu'une analyse normale.
   - **Analyser les lecteurs de disquettes à l'arrêt du système** : votre lecteur de disquettes est analysé lorsque vous arrêtez votre ordinateur.
   - **Rechercher les logiciels espions et les programmes potentiellement indésirables** : les logiciels espions et publicitaires, ainsi que tout autre programme susceptible de collecter et de transmettre des données sans votre autorisation, sont détectés et supprimés.
   - **Rechercher et supprimer les cookies de suivi** : les cookies susceptibles de collecter et transmettre des données sans votre autorisation sont détectés et supprimés. Un cookie identifie un utilisateur lorsqu'il visite une page Web.
   - **Analyser les lecteurs réseau** : les lecteurs connectés à votre réseau sont analysés.
   - **Activer la protection contre le débordement de tampon** : si une activité de débordement de tampon est détectée, elle est bloquée et vous en êtes averti.
   - **Commencer l'analyse en temps réel au démarrage de Windows (recommandé)** : la protection en temps réel est activée à chaque démarrage de votre ordinateur, même si vous la désactivez pour une session.

5 Selon le cas, cliquez sur l'un des boutons suivants :

- **Tous les fichiers (recommandé)** : tous les types de fichier utilisés par votre ordinateur sont analysés. Cette option fournit l'analyse la plus complète.
- **Fichiers programme et documents uniquement** : seuls les fichiers programme et les documents sont analysés.

6 Cliquez sur **OK**.

Utilisation de la protection contre les logiciels espions

La protection contre les logiciels espions supprime les logiciels espions et publicitaires ainsi que tout programme potentiellement indésirable qui collecte et transmet des informations sans votre autorisation.

Désactiver la protection contre les logiciels espions

Si vous désactivez la protection contre les logiciels espions, les programmes potentiellement indésirables qui collectent et transmettent des informations sans votre autorisation ne seront pas détectés.

Pour désactiver la protection contre les logiciels espions :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection contre les logiciels espions**, cliquez sur **Désactivé**.

Activation de la protection contre les logiciels espions

La protection contre les logiciels espions supprime les logiciels espions et publicitaires ainsi que tout programme potentiellement indésirable qui collecte et transmet des informations sans votre autorisation.

Pour activer la protection contre les logiciels espions :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection contre les logiciels espions**, cliquez sur **Activé**.

Utilisation de SystemGuards

Les SystemGuards détectent les modifications potentiellement non autorisées apportées à votre ordinateur et vous en avertissent. Vous pouvez ensuite vérifier ces modifications et décider de les autoriser ou non.

Les SystemGuards sont classés de la manière suivante :

SystemGuards Progamme

Les SystemGuards Programme détectent les modifications apportées à vos fichiers de démarrage, extensions et fichiers de configuration.

SystemGuards Windows

Les SystemGuards Windows détectent les modifications apportées aux services, certificats et fichiers de configuration Windows.

SystemGuards Navigateur

Les SystemGuards Navigateur détectent les modifications apportées aux paramètres d'Internet Explorer, y compris aux attributs et aux paramètres de sécurité du navigateur.

Désactivation des SystemGuards

Si vous désactivez les SystemGuards, les modifications potentiellement non autorisées apportées à votre ordinateur ne seront pas détectées.

Pour désactiver tous les SystemGuards :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection SystemGuard**, cliquez sur **Désactivé**.

Activer les SystemGuards

Les SystemGuards détectent les modifications potentiellement non autorisées apportées à votre ordinateur et vous en avertissent.

Pour activer les SystemGuards :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection SystemGuard**, cliquez sur **Activé**.

Configuration des SystemGuards

Vous pouvez modifier les SystemGuards. Pour toute modification détectée, vous pouvez décider d'en être averti et d'archiver l'événement, de vous contenter d'archiver l'événement ou de désactiver le SystemGuard.

Configuration des SystemGuards

Vous pouvez modifier les SystemGuards. Pour toute modification détectée, vous pouvez décider d'en être averti et d'archiver l'événement, de vous contenter d'archiver l'événement ou de désactiver le SystemGuard.

Pour configurer les SystemGuards :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection SystemGuard**, cliquez sur **Avancé**.
4. Dans la liste des SystemGuards, cliquez sur une catégorie pour afficher une liste des SystemGuards associés et de leurs statuts.
5. Cliquez sur le nom d'un SystemGuard.
6. Sous **Détails**, affichez les informations relatives au SystemGuard.
7. Sous **Je souhaite**, effectuez l'une des actions suivantes :
   - Cliquez sur **Afficher les alertes** si vous souhaitez être averti lorsqu'une modification est apportée et que l'événement est archivé.
   - Cliquez sur **Archivage simple des modifications** si vous ne souhaitez pas qu'une action soit entreprise lorsqu'une modification est détectée. La modification est uniquement archivée.
   - Cliquez sur **Désactiver ce SystemGuard** pour arrêter le SystemGuard. Vous n'êtes pas averti des modifications qui sont apportées et l'événement n'est pas archivé.
8. Cliquez sur **OK**.

Mieux comprendre les SystemGuards

Les SystemGuards détectent les modifications potentiellement non autorisées apportées à votre ordinateur et vous en avertissent. Vous pouvez ensuite vérifier ces modifications et décider de les autoriser ou non.

Les SystemGuards sont classés de la manière suivante :

SystemGuards Progamme

Les SystemGuards Programme détectent les modifications apportées à vos fichiers de démarrage, extensions et fichiers de configuration.

SystemGuards Windows

Les SystemGuards Windows détectent les modifications apportées aux services, certificats et fichiers de configuration Windows.

SystemGuards Navigateur

Les SystemGuards Navigateur détectent les modifications apportées aux paramètres d'Internet Explorer, y compris aux attributs et aux paramètres de sécurité du navigateur.

Informations relatives aux SystemGuards Programme

Les SystemGuards Programme détectent les objets suivants.

Installations ActiveX

Les SystemGuards Programme détectent les programmes ActiveX téléchargés via Internet Explorer. Les programmes ActiveX sont téléchargés depuis des sites Web et stockés sur votre ordinateur dans C:\Windows\Downloaded Program Files ou C:\Windows\Temp\Temporary Internet Files. Ils sont également répertoriés dans le registre en fonction de leur CLSID (longue chaîne de chiffres entre crochets).

Internet Explorer utilise de nombreux programmes ActiveX légitimes. Si vous avez des doutes quant à un programme ActiveX, vous pouvez le supprimer sans endommager votre ordinateur. Si vous avez besoin de ce programme ultérieurement, Internet Explorer le téléchargera au prochain accès à un site Web demandeur.

Éléments de démarrage

Les SystemGuards Programme surveillent les modifications apportées à vos clés et dossiers de registre de démarrage. Les clés de registre de démarrage situées dans le registre Windows et les dossiers de démarrage situés dans le menu Démarrer enregistrent les chemins des programmes sur votre ordinateur. Les programmes répertoriés à ces emplacements sont chargés au démarrage de Windows. Les logiciels espions ou autres programmes potentiellement indésirables essaient souvent de se charger au démarrage de Windows.

Shell Execute Hooks de Windows

Les SystemGuards Programme surveillent les modifications apportées à la liste des programmes qui se chargent dans explorer.exe. Shell Execute Hook est un programme qui se charge dans le shell explorer.exe de Windows. Il reçoit toutes les commandes d'exécution utilisées sur un ordinateur. Tout programme chargé dans le shell explorer.exe peut réaliser une tâche supplémentaire avant le lancement réel d'un autre programme. Les logiciels espions ou autres programmes potentiellement indésirables peuvent utiliser Shell Execute Hook pour empêcher des programmes de sécurité de fonctionner.

Shell Service Object Delay Load

Les SystemGuards Programme détectent les modifications apportées aux fichiers répertoriés dans le Shell Service Object Delay Load. Ces fichiers sont chargés par explorer.exe au démarrage de votre ordinateur. Etant donné qu'explorer.exe est le shell de votre ordinateur, il démarre toujours en chargeant les fichiers sous cette clé. Ces fichiers sont chargés au début du processus de démarrage avant toute intervention humaine.

Informations relatives aux SystemGuards Windows

Les SystemGuards Windows détectent les objets suivants.

Gestionnaires de menus contextuels

Les SystemGuards Windows empêchent toute modification non autorisée des menus contextuels de Windows. Ces menus permettent de cliquer avec le bouton droit de la souris sur un fichier et d'effectuer des actions spécifiques adaptées à ce fichier.

DLL AppInit

Les SystemGuards Windows empêchent les modifications ou ajouts non autorisés aux DLL AppInit (de démarrage d'application) de Windows : la valeur de registre AppInit_DLLs contient une liste des fichiers chargés au chargement de user32.dll. Les fichiers répertoriés dans la valeur Applnit_DLLs sont chargés au début du processus de démarrage de Windows, permettant ainsi à un .DLL potentiellement dangereux de se cacher avant toute intervention de l'utilisateur.

Fichier Hosts Windows

Les SystemGuards Windows surveillent les modifications apportées au fichier Hosts de votre ordinateur : votre fichier Hosts est utilisé pour rediriger certains noms de domaines vers des adresses IP spécifiques. Par exemple, lorsque vous visitez le site www.example.com, votre navigateur vérifie le fichier Hosts, trouve une entrée pour example.com et pointe vers l'adresse IP de ce domaine. Certains logiciels espions essaient de modifier votre fichier Hosts pour rediriger votre navigateur vers un autre site ou empêcher votre logiciel de se mettre à jour correctement.

Shell Winlogon

Les SystemGuards Windows surveillent le shell Winlogon. Ce shell est chargé lorsqu'un utilisateur se connecte à Windows. Le shell est l'interface utilisateur principale utilisée pour gérer Windows. En général, il s'agit de l'Explorateur Windows (explorer.exe). Cependant, le shell de Windows peut facilement être modifié de manière à pointer vers un autre programme. Le cas échéant, un programme autre que le shell de Windows est lancé à chaque connexion d'un utilisateur.

Clé UserInit de Winlogon

Les SystemGuards Windows surveillent les modifications apportées à vos paramètres utilisateur de connexion à Windows. La clé HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit définit le programme lancé après connexion d'un utilisateur à Windows. Le programme par défaut rétablit votre profil, la police de caractères, les couleurs et autres paramètres de votre nom d'utilisateur. Des logiciels espions ainsi que d'autres programmes potentiellement indésirables peuvent tenter de se lancer en s'ajoutant à cette clé.

Protocoles Windows

Les SystemGuards Windows surveillent les modifications effectuées au niveau des protocoles réseau. Certains logiciels espions ou d'autres programmes potentiellement indésirables prennent le contrôle de certains moyens utilisés par votre ordinateur pour envoyer et recevoir des informations. Cette opération est effectuée via les filtres et les gestionnaires de protocoles Windows.

Fournisseurs de services en couche (Layered Service Providers ou LSP) Winsock

Les SystemGuards Windows surveillent les fournisseurs de services en couche (LSP), qui pourraient intercepter vos données sur le réseau et les modifier ou les rediriger. Les LSP légitimes comprennent le logiciel de contrôle parental, les firewalls et les autres programmes de sécurité. Les logiciels espions peuvent utiliser des LSP pour surveiller votre activité Internet et modifier vos données. Afin d'éviter une réinstallation du système d'exploitation, utilisez les programmes McAfee pour supprimer automatiquement les logiciels espions et les LSP douteux.

Commandes Open Shell Windows

Les SystemGuards Windows empêchent toute modification de vos commandes Open Shell Windows (explorer.exe). Les commandes Open Shell Windows permettent l'exécution d'un programme spécifique à chaque fois qu'un certain type de fichier est exécuté. Par exemple, un ver peut essayer de s'exécuter à chaque fois qu'une application .exe est exécutée.

Gestionnaire de tâches programmées

Les SystemGuards Windows surveillent la clé de registre SharedTaskScheduler qui contient une liste de programmes qui s'exécutent au démarrage de Windows. Certains logiciels espions ou autres programmes potentiellement indésirables modifient cette clé et s'ajoutent à la liste sans votre autorisation.

Windows Messenger Service

Les SystemGuards Windows surveillent Windows Messenger Service, une fonction non documentée de Windows Messenger qui permet aux utilisateurs d'envoyer des messages instantanés. Certains logiciels espions ou d'autres programmes potentiellement indésirables tentent d'activer le service et envoient des publicités non sollicitées. Ce service peut en outre être exploité par le biais d'une vulnérabilité connue pour exécuter du code à distance.

Fichier Windows Win.ini

Le fichier win.ini est un fichier texte qui fournit une liste de programmes à exécuter au lancement de Windows. La syntaxe applicable au chargement de ces programmes figure dans le fichier utilisé pour la prise en charge des versions antérieures de Windows. La plupart des programmes n'utilisent pas le fichier sin.ini pour ce chargement. Cependant, certains logiciels espions ou d'autres programmes potentiellement indésirables sont conçus pour tirer profit de cette syntaxe et se charger au démarrage de Windows.

Informations concernant les SystemGuards Navigateur

Les SystemGuards Navigateur détectent les objets suivants.

Browser Helper Objects (BHO)

Les SystemGuards Navigateur surveillent les ajouts apportés à vos Browser Helper Objects (BHO). Les BHO sont des programmes qui agissent comme des plug-ins Internet Explorer. Les logiciels espions et les pirates de navigateur utilisent souvent des BHO pour afficher des publicités ou suivre vos habitudes de navigation. Les BHO sont également utilisés par de nombreux programmes légitimes tels que les barres d'outils de recherche courantes.

Barres Internet Explorer

Les SystemGuards Navigateur surveillent les modifications apportées à votre liste de programmes de barres Internet Explorer. Une barre d'explorateur est similaire aux panneaux Rechercher/Favoris/Historique d'Internet Explorer (IE) ou de l'Explorateur Windows.

Plug-ins Internet Explorer

Les SystemGuards Navigateur empêchent les logiciels espions d'installer des plug-ins Internet Explorer. Les plug-ins Internet Explorer sont des programmes additionnels chargés au lancement d'Internet Explorer. Le logiciel espion utilise souvent des plug-ins Internet Explorer pour afficher des publicités ou suivre vos habitudes de navigation. Les plug-ins légitimes ajoutent une fonctionnalité à Internet Explorer.

ShellBrowser Internet Explorer

Les SystemGuards Navigateur surveillent les modifications apportées à votre instance de ShellBrowser Internet Explorer. Le ShellBrowser Internet Explorer contient des informations et des paramètres concernant une instance d'Internet Explorer. Si ces paramètres sont modifiés ou si un nouveau ShellBrowser est ajouté, ce ShellBrowser peut prendre le contrôle complet d'Internet Explorer, en ajoutant des fonctions telles que des barres d'outils, des menus et des boutons.

WebBrowser Internet Explorer

Les SystemGuards Navigateur surveillent les modifications apportées à votre instance de WebBrowser Internet Explorer. Le WebBrowser Internet Explorer contient des informations et des paramètres concernant une instance d'Internet Explorer. Si ces paramètres sont modifiés ou si un nouveau WebBrowser est ajouté, ce WebBrowser peut prendre le contrôle complet d'Internet Explorer en ajoutant des fonctions telles que des barres d'outils, des menus et des boutons.

URL Search Hooks Internet Explorer

Les SystemGuards Navigateur surveillent les modifications apportées à URL Search Hook Internet Explorer. URL Search Hook est utilisé lorsque vous entrez une adresse dans le champ d'adresse du navigateur sans protocole tel que http:// ou ftp://. Lorsque vous entrez ce type d'adresse, le navigateur peut utiliser URL Search Hook pour trouver sur Internet l'adresse entrée.

URL Internet Explorer

Surveillent les modifications apportées à vos URL prédéfinies dans Internet Explorer. Ainsi, les logiciels espions ou autres programmes potentiellement indésirables ne peuvent pas modifier vos paramètres de navigateur sans votre autorisation.

Restrictions Internet Explorer

Surveillent les restrictions Internet Explorer, qui permettent à l'administrateur d'un ordinateur d'empêcher un utilisateur de modifier la page d'accueil ou d'autres options d'Internet Explorer. Ces options n'apparaissent que si votre administrateur les a définies.

Zones de sécurité Internet Explorer

Les SystemGuards Navigateur surveillent les zones de sécurité d'Internet Explorer. Internet Explorer propose quatre zones de sécurité prédéfinies : Internet, l'intranet local, les sites autorisés et les sites restreints. Chaque zone de sécurité dispose de ses propres paramètres de sécurité prédéfinis ou personnalisés. Ces zones constituent l'une des cibles des logiciels espions ou autres programmes potentiellement indésirables puisqu'en diminuant le niveau de sécurité ils peuvent déjouer les alertes de sécurité et agir sans être détectés.

Sites de confiance d'Internet Explorer

Les SystemGuards Navigateur surveillent les sites de confiance d'Internet Explorer. La liste des sites de confiance est un répertoire des sites Web que vous considérez sûrs. Certains logiciels espions ou autres programmes potentiellement indésirables ciblent cette liste car elle leur fournit une méthode pour autoriser des sites suspects sans que vous en soyez informé.

Stratégie Internet Explorer

Les SystemGuards Navigateur surveillent les stratégies Internet Explorer. Ces paramètres sont généralement modifiés par les administrateurs système, mais des logiciels espions peuvent également les exploiter. Ces modifications peuvent empêcher de définir une autre Page d'accueil ou masquer des onglets de la boîte de dialogue Options Internet du menu Outils.

Utilisation de l'analyse de scripts

Un script peut créer, copier ou supprimer des fichiers. Il peut également ouvrir votre registre Windows.

L'analyse de scripts empêche automatiquement des scripts connus et nocifs de s'exécuter sur votre ordinateur.

Désactivation de l'analyse de scripts

Si vous désactivez l'analyse de scripts, les exécutions de scripts suspects ne seront pas détectées.

Pour désactiver l'analyse de scripts :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection des analyses de scripts**, cliquez sur **Désactivé**.

Activer l'analyse de scripts

L'analyse de scripts vous avertit si l'exécution d'un script entraîne la création/copie/suppression de fichiers ou l'ouverture de votre registre Windows.

Pour activer l'analyse de scripts:

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection des analyses de scripts**, cliquez sur **Activé**.

Utilisation de la protection de la messagerie

La protection de la messagerie détecte et bloque les menaces contenues dans les messages et pièces jointes entrants (POP3) et sortants (SMTP), qui incluent les virus, les chevaux de Troie, les vers, les logiciels espions et de publicité, ainsi que toute autre menace.

Désactivation de la protection de la messagerie

Si vous désactivez la protection de la messagerie, les menaces potentielles contenues dans les messages et pièces jointes entrants (POP3) ou sortants (SMTP) ne seront plus détectées.

Pour désactiver la protection de la messagerie :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.
3. Sous **Protection de la messagerie**, cliquez sur **Désactivé**.

Activation de la protection de la messagerie

La protection de la messagerie détecte les menaces contenues dans les messages et pièces jointes entrants (POP3) et sortants (SMTP).

Pour activer la protection de la messagerie :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.
3. Sous **Protection de la messagerie**, cliquez sur **Activé**.

Configuration de la protection de la messagerie

Les options de protection des e-mails vous permettent d'analyser les messages entrants et sortants et de détecter la présence de vers éventuels. Les vers se reproduisent et consomment les ressources du système, ce qui ralentit les performances ou interrompt les tâches. Les vers peuvent envoyer des copies d'eux-mêmes par l'intermédiaire d'e-mails. Ils peuvent par exemple tenter de transférer des e-mails à des contacts de votre carnet d'adresses.

Configuration de la protection de la messagerie

Les options de protection des e-mails vous permettent d'analyser les messages entrants et sortants et de détecter la présence de vers éventuels.

Pour configurer la protection de la messagerie :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.
3. Sous **Protection de la messagerie**, cliquez sur **Avancé**.
4. Sélectionnez ou désélectionnez les cases à cocher suivantes :
   - **Analyse des messages e-mails entrants** : les messages entrants (POP3) sont analysés pour rechercher des menaces potentielles.
   - **Analyse des messages e-mails sortants** : les messages sortants (SMTP) sont analysés pour rechercher des menaces potentielles.
   - **Activation de WormStopper** : WormStopper bloque les vers des e-mails.
5. Cliquez sur **OK**.

Utilisation de la protection de la messagerie instantanée

La protection de la messagerie instantanée détecte les menaces contenues dans les pièces jointes des messages instantanés entrants.

Désactivation de la protection de la messagerie instantanée

Si vous désactivez la protection de la messagerie instantanée, les menaces contenues dans les pièces jointes des messages instantanés entrants ne seront pas détectées.

Pour désactiver la protection de la messagerie instantanée :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.
3. Sous **Protection de la messagerie instantanée**, cliquez sur **Désactivé**.

Activation de la protection de la messagerie instantanée

La protection de la messagerie instantanée détecte les menaces contenues dans les pièces jointes des messages instantanés entrants.

Pour activer la protection de la messagerie instantanée :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **E-mail & IM**.
3. Sous **Protection de la messagerie instantanée**, cliquez sur **Activé**.

CHAPITRE 15

Analyse manuelle de votre ordinateur

Vous pouvez rechercher des virus et d'autres menaces sur les disques durs et les disquettes, ainsi que dans les fichiers et dossiers individuels. Quand VirusScan détecte un fichier suspect, il tente automatiquement de le nettoyer, sauf s'il s'agit d'un programme potentiellement indésirable. Si VirusScan ne parvient pas à nettoyer le fichier, vous pouvez le mettre en quarantaine ou le supprimer.

Contenu de ce chapitre

Analyse manuelle

Vous pouvez effectuer une analyse manuelle à tout moment. Par exemple, si vous venez d'installer VirusScan, vous pouvez effectuer une analyse pour vous assurer que votre ordinateur n'est pas infecté par un virus ou exposé à d'autres menaces. Si vous avez désactivé l'analyse en temps réel, vous pouvez également effectuer une analyse pour vous assurer que votre ordinateur est toujours sécurisé.

Analyse avec utilisation de vos paramètres manuels d'analyse

Ce type d'analyse utilise les paramètres manuels d'analyse que vous avez définis. VirusScan analyse les fichiers internes compressés (.zip, .cab, etc) mais comptabilise un fichier compressé comme un fichier. De plus, le nombre de fichiers analysés peut varier si vous avez supprimé vos fichiers Internet temporaires depuis votre dernière analyse.

Pour effectuer une analyse avec vos paramètres manuels d'analyse :

1. Dans le menu de base, cliquez sur **Analyser**. Une fois l'analyse terminée, un récapitulatif affiche le nombre d'objets analysés et détectés, le nombre d'objets nettoyés, ainsi que la date de votre dernière analyse.
2. Cliquez sur **Terminer**.

Rubriques connexes

- Configuration des analyses manuelles (page 94)

Analyse sans utilisation de vos paramètres manuels d'analyse

Ce type d'analyse n'utilise pas les paramètres manuels d'analyse que vous avez définis. VirusScan analyse les fichiers internes compressés (.zip, .cab, etc) mais comptabilise un fichier compressé comme un fichier. De plus, le nombre de fichiers analysés peut varier si vous avez supprimé vos fichiers Internet temporaires depuis votre dernière analyse.

Pour effectuer une analyse sans utiliser vos paramètres manuels d'analyse :

1. Dans le menu Avancé, cliquez sur **Accueil**.
2. Dans la fenêtre d'accueil, cliquez sur **Analyser**.
3. Sous **Emplacements à analyser**, cochez les cases en regard des fichiers, des dossiers et des lecteurs que vous souhaitez analyser.
4. Sous **Options**, cochez les cases en regard du ou des types de fichier que vous souhaitez analyser.
5. Cliquez sur **Analyser maintenant**. Une fois l'analyse terminée, un récapitulatif affiche le nombre d'objets analysés et détectés, le nombre d'objets nettoyés, ainsi que la date de votre dernière analyse.
6. Cliquez sur **Terminer**.

Remarque : ces options ne sont pas sauvegardées.

Analyse dans l'Explorateur Windows

Vous pouvez analyser les virus et autres menaces dans d'autres fichiers, dossiers ou lecteurs dans l'Explorateur Windows.

Pour analyser des fichiers dans l'Explorateur Windows :

1. Ouvrez l'Explorateur Windows.
2. Cliquez avec le bouton droit de la souris sur le fichier, le dossier ou le lecteur à analyser, puis cliquez sur **Analyser**. Toutes les options d'analyse par défaut sont sélectionnées afin d'offrir une analyse complète.

Configuration des analyses manuelles

Lorsque vous effectuez une analyse manuelle ou programmée, vous pouvez définir le type de fichier à analyser, les emplacements de l'analyse ainsi que le moment de l'analyse.

Configuration du type de fichier à analyser.

Vous pouvez configurer le type de fichier à analyser.

Pour configurer le type de fichier à analyser :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection anti-virus**, cliquez sur **Avancé**.
4. Dans la fenêtre Protection anti-virus, cliquez sur **Analyse manuelle**.
5. Cochez ou décochez les cases suivantes :
   - **Détecter les virus inconnus en utilisant des techniques heuristiques** : les fichiers sont comparés aux signatures de virus déjà connus afin de détecter les signes de virus non identifiés. Bien qu'effectuant l'analyse la plus complète, cette option est généralement plus lente qu'une analyse normale.
   - **Analyse des fichiers .zip et autres fichiers d'archive** : détecte et supprime les virus dans les fichiers .zip et autres fichiers d'archive. Parfois, les créateurs de virus placent des virus dans un fichier .zip, puis insèrent ce fichier .zip dans un autre fichier .zip afin de déjouer les analyseurs antivirus.
   - **Rechercher les logiciels espions et les programmes potentiellement indésirables** : les logiciels espions et publicitaires, ainsi que tout autre programme susceptible de collecter et de transmettre des données sans votre autorisation, sont détectés et supprimés.
   - **Rechercher et supprimer les cookies de suivi** : les cookies susceptibles de collecter et transmettre des données sans votre autorisation sont détectés et supprimés. Un cookie identifie un utilisateur lorsqu'il visite une page Web.
   - **Rechercher les rootkits et autres programmes furtifs** : détecte et supprime tous les rootkits et les autres programmes qui se cachent de Windows.
6. Selon le cas, cliquez sur l'un des boutons suivants :
   - **Tous les fichiers (recommandé)** : tous les types de fichier utilisés par votre ordinateur sont analysés. Cette option fournit l'analyse la plus complète.

- **Fichiers programme et documents uniquement** : seuls les fichiers programme et les documents sont analysés.

7 Cliquez sur **OK**.

Configuration des emplacements à analyser

Vous pouvez configurer les emplacements à analyser pour les analyses manuelles ou programmées.

Pour configurer les emplacements à analyser :

1 Dans le menu Avancé, cliquez sur **Configurer**.

2 Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.

3 Sous **Protection anti-virus**, cliquez sur **Avancé**.

4 Dans la fenêtre Protection anti-virus, cliquez sur **Analyse manuelle**.

5 Sous **Emplacements par défaut à analyser**, sélectionnez les fichiers, dossiers et lecteurs que vous souhaitez analyser.

Afin d'effectuer l'analyse la plus complète possible, assurez-vous que **Fichiers critiques** est sélectionné.

6 Cliquez sur **OK**.

Programmer des analyses

Vous pouvez programmer des analyses afin d'effectuer une recherche complète d'éventuels virus et autres menaces sur votre ordinateur à intervalles définis.

Pour programmer une analyse :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection anti-virus**, cliquez sur **Avancé**.
4. Dans la fenêtre Protection anti-virus, cliquez sur **Analyse programmée**.
5. Vérifiez que l'option **Activer l'analyse programmée** est bien sélectionnée.
6. Cochez la case en regard du jour de la semaine où l'analyse doit être effectuée.
7. Cliquez dans la liste des heures de début afin de définir une heure de début d'analyse.
8. Cliquez sur **OK**.

Conseil : pour utiliser le programme par défaut, cliquez sur **Réinitialiser.**

CHAPITRE 16

Administration de VirusScan

Vous pouvez supprimer des éléments des listes approuvées, gérer des programmes, cookies et fichiers placés en quarantaine, afficher des événements et des fichiers journaux et signaler une activité douteuse à McAfee.

Contenu de ce chapitre

Gestion des listes approuvées

Lorsque vous autorisez un SystemGuard, un programme, un débordement de tampon ou un programme e-mail, l'élément est ajouté à une liste approuvée et n'est plus détecté par la suite.

Si vous autorisez un programme par erreur ou si vous souhaitez à nouveau qu'il soit détecté, vous devez le supprimer de cette liste.

Gestion des listes approuvées.

Lorsque vous autorisez un SystemGuard, un programme, un débordement de tampon ou un programme e-mail, l'élément est ajouté à une liste approuvée et n'est plus détecté par la suite.

Si vous autorisez un programme par erreur ou si vous souhaitez à nouveau qu'il soit détecté, vous devez le supprimer de cette liste.

Pour supprimer des éléments des listes approuvées :

1. Dans le menu Avancé, cliquez sur **Configurer**.
2. Dans la fenêtre de configuration, cliquez sur **Ordinateur & Fichiers**.
3. Sous **Protection anti-virus**, cliquez sur **Avancé**.
4. Dans la fenêtre Protection anti-virus, cliquez sur **Listes approuvées**.
5. Dans la liste, sélectionnez un SystemGuard, un programme, un débordement tampon ou un programme e-mail autorisé pour afficher ses objets et leur statut autorisé.
6. Sous **Détails**, affichez les informations relatives à l'objet.
7. Sous **Je souhaite**, cliquez sur une action.
8. Cliquez sur **OK**.

Gestion des programmes, cookies et fichiers placés en quarantaine

Les programmes, cookies et fichiers placés en quarantaine peuvent être restaurés, supprimés ou envoyés chez McAfee pour analyse.

Restauration des programmes, cookies et fichiers placés en quarantaine

Si nécessaire, vous pouvez restaurer des programmes, cookies et fichiers qui ont été placés en quarantaine.

Pour restaurer des programmes, cookies et fichiers placés en quarantaine :

1. Dans le menu Avancé, cliquez sur **Restaurer**.
2. Dans la fenêtre Restaurer, cliquez sur **Programmes et cookies** ou **Fichiers** selon le cas.
3. Sélectionnez les programmes, cookies ou fichiers placés en quarantaine que vous souhaitez restaurer.
4. Pour plus d'informations sur le virus en quarantaine, cliquez sur le nom sous lequel il a été détecté sous **Détails**. La biblliothèque d'informations sur les virus s'affiche avec la description du virus.
5. Sous **Je souhaite**, cliquez sur **Restaurer**.

Suppression des programmes, cookies et fichiers placés en quarantaine

Si nécessaire, vous pouvez supprimer des programmes, cookies et fichiers placés en quarantaine.

Pour supprimer des programmes, cookies et fichiers placés en quarantaine :

1. Dans le menu Avancé, cliquez sur **Restaurer**.
2. Dans la fenêtre Restaurer, cliquez sur **Programmes et cookies** ou **Fichiers** selon le cas.
3. Sélectionnez les programmes, cookies ou fichiers placés en quarantaine que vous souhaitez restaurer.
4. Pour plus d'informations sur le virus placé en quarantaine, cliquez sur le nom sous lequel il a été détecté sous **Détails**. La biblliothèque d'informations sur les virus s'affiche avec la description du virus.
5. Sous **Je souhaite**, cliquez sur **Supprimer**.

Envoi des programmes, cookies et fichiers en quarantaine à McAfee

Vous pouvez envoyer des programmes, cookies et fichiers placés en quarantaine à McAfee pour analyse.

Remarque : si le fichier en quarantaine que vous envoyez dépasse une certaine taille, il peut être rejeté. La plupart du temps, cette situation ne se produit pas.

Pour envoyer des programmes ou fichiers placés en quarantaine à McAfee :

1. Dans le menu Avancé, cliquez sur **Restaurer**.
2. Dans la fenêtre Restaurer, cliquez sur **Programmes et cookies** ou **Fichiers** selon le cas.
3. Sélectionnez les programmes, cookies ou fichiers placés en quarantaine que vous souhaitez envoyer à McAfee.
4. Pour plus d'informations sur le virus placé en quarantaine, cliquez sur le nom sous lequel il a été détecté sous **Détails**. La biblliothèque d'informations sur les virus s'affiche avec la description du virus.
5. Sous **Je souhaite**, cliquez sur **Envoyer à McAfee**.

Affichage des événements récents et des journaux

Les événements récents et les fichiers journaux affichent les événements relatifs à tous les produits McAfee installés.

Sous Evénements récents, vous pouvez afficher les 30 derniers événements significatifs survenus sur votre ordinateur. Vous pouvez restaurer des programmes bloqués, réactiver l'analyse en temps réel et autoriser des débordements de tampon.

Vous pouvez également afficher des fichiers journaux qui enregistrent tous les événements survenus au cours des 30 derniers jours.

Afficher les événements

Sous Evénements récents, vous pouvez afficher les 30 derniers événements significatifs survenus sur votre ordinateur. Vous pouvez restaurer des programmes bloqués, réactiver l'analyse en temps réel et autoriser des débordements de tampon.

Pour afficher des événements :

1. Dans le menu Avancé, cliquez sur **Rapports et journaux**.
2. Dans la fenêtre Rapports et journaux, cliquez sur **Evénements récents**.
3. Sélectionnez l'événement à afficher.
4. Sous **Détails**, affichez les informations relatives à l'événement.
5. Sous **Je souhaite**, cliquez sur une action.

Afficher les journaux

Les journaux enregistrent tous les événements survenus au cours des 30 derniers jours.

Pour afficher les journaux :

1. Dans le menu Avancé, cliquez sur **Rapports et journaux**.
2. Dans la fenêtre Rapports et journaux, cliquez sur **Evénements récents**.
3. Dans la fenêtre Evénements récents, cliquez sur **Afficher le journal**.
4. Sélectionnez le type de fichier journal à afficher, puis sélectionnez un fichier journal.
5. Sous **Détails**, affichez les informations relatives au fichier journal.

Communication automatique d'informations anonymes

Vous pouvez envoyer anonymement à McAfee des informations concernant un virus, un programme potentiellement indésirable ou le suivi d'un pirate. Cette option n'est disponible qu'au cours de l'installation.

Aucune information d'identification personnelle n'est recueillie.

Signaler à McAfee

Vous pouvez envoyer à McAfee des informations concernant un virus, un programme potentiellement indésirable et le suivi d'un pirate. Cette option n'est disponible qu'au cours de l'installation.

Pour signaler automatiquement des informations anonymes :

1. Pendant l'installation de VirusScan, acceptez le paramètre par défaut suivant : **Soumettre informations anonymes**.
2. Cliquez sur **Suivant**.

Mieux comprendre les alertes de sécurité

Si l'analyse en temps réel détecte une menace, une alerte s'affiche. Pour la plupart des virus, des chevaux de Troie, des scripts et des vers, l'analyse en temps réel tente automatiquement de nettoyer le fichier et vous avertit. Pour les programmes potentiellement indésirables et les SystemGuards, l'analyse en temps réel détecte le fichier ou la modification et vous avertit. Pour les débordements de tampon, le suivi de cookies et l'activité de scripts, l'analyse en temps réel bloque automatiquement l'activité et vous avertit au moyen d'une alerte.

Ces alertes peuvent être classées en trois catégories principales.

- Alerte rouge
- Alerte jaune
- Alerte verte

Vous pouvez alors choisir le mode de gestion des fichiers détectés, des e-mails détectés, des scripts suspects, des vers potentiels, des programmes potentiellement indésirables, des SystemGuards ou des débordements de tampon.

Gestion des alertes

McAfee utilise un ensemble d'alertes pour vous aider à gérer la sécurité de votre système. Ces alertes peuvent être classées en trois catégories principales.

- Alerte rouge
- Alerte jaune
- Alerte verte

Alerte rouge

Une alerte rouge nécessite une réponse de votre part. Il arrive que McAfee ne soit pas en mesure de déterminer la réponse automatique à apporter à une activité particulière. Dans ces cas-là, l'alerte rouge décrit l'activité en question et vous fournit une ou plusieurs options à sélectionner.

Alerte jaune

Une alerte jaune constitue une indication non critique qui nécessite généralement une réponse de votre part. L'alerte jaune décrit l'activité en question et vous fournit une ou plusieurs options à sélectionner.

Alerte verte

Dans la plupart des cas, les alertes vertes fournissent des informations de base concernant un événement et ne requièrent aucune réponse.

Configuration des options d'alerte

Si vous choisissez de ne plus afficher une alerte puis que vous changez d'avis, vous pouvez revenir sur votre décision et configurer cette alerte pour qu'elle s'affiche à nouveau. Pour plus d'informations sur la configuration des options d'alerte, consultez la documentation de SecurityCenter.

CHAPITRE 17

Aide complémentaire

Cette rubrique décrit les questions fréquemment posées et les scénarios de dépannage.

Contenu de ce chapitre

Questions fréquemment posées

Cette section regroupe les réponses aux questions les plus fréquemment posées.

Une menace a été détectée, que dois-je faire ?

McAfee utilise un système d'alertes pour vous aider à gérer la sécurité de votre système. Ces alertes peuvent être classées en trois catégories principales.

- Alerte rouge
- Alerte jaune
- Alerte verte

Vous pouvez alors choisir le mode de gestion des fichiers détectés, des e-mails détectés, des scripts suspects, des vers potentiels, des programmes potentiellement indésirables, des SystemGuards ou des débordements de tampon.

Pour obtenir plus d'informations sur la gestion des alertes spécifiques, consultez la bibliothèque d'informations sur les virus sur le site : http://us.mcafee.com/virusInfo/default.asp.

Rubriques connexes

- Mieux comprendre les alertes de sécurité (page 103)

Puis-je utiliser VirusScan avec les navigateurs Netscape, Firefox et Opera ?

Vous pouvez utiliser Netscape, Firefox et Opera comme navigateur Internet par défaut, mais Microsoft Internet Explorer 6.0 ou une version ultérieure doit être installé sur votre ordinateur.

Dois-je être connecté à Internet pour effectuer une analyse ?

Vous n'avez pas besoin d'être connecté à Internet pour lancer une analyse, mais vous devez vous connecter au moins une fois par semaine pour recevoir les mises à jour McAfee.

VirusScan analyse-t-il les pièces jointes aux e-mails ?

Si l'analyse en temps réel et la protection de la messagerie sont activées, toutes les pièces jointes sont analysées à l'arrivée de l'e-mail.

VirusScan analyse-t-il les fichiers compressés (.zip) ?

VirusScan analyse les fichiers compressés (.zip) et autres fichiers d'archive.

Pourquoi des erreurs se produisent-elles lors de l'analyse d'e-mails sortants ?

Lors de l'analyse d'e-mails sortants, les erreurs suivantes peuvent se produire :

- Erreur de protocole Le serveur de messagerie a refusé un e-mail.
  Si une erreur de protocole ou une erreur système se produit, les e-mails restants de la session sont traités et envoyés au serveur.
- Erreur de connexion Une connexion au serveur de messagerie a été interrompue.
  En cas d'erreur de connexion, vérifiez que votre ordinateur est connecté à Internet, puis réessayez d'envoyer le message depuis la liste des éléments **Envoyés** de votre programme de messagerie.
- Erreur système. Un échec dans le traitement d'un fichier ou une autre erreur système s'est produite.
- Erreur de connexion SMTP cryptée. Une connexion SMTP cryptée de votre programme e-mail a été détectée.
  Si la connexion SMTP est cryptée, vous pouvez désactiver le cryptage dans votre programme de messagerie pour permettre l'analyse de vos e-mails.

Si des délais d'expiration apparaissent lors de l'envoi d'e-mails, désactivez l'analyse des e-mails sortants ou le cryptage de la connexion SMTP dans votre programme de messagerie.

Rubriques connexes

- Configuration de la protection de la messagerie (page 89)

Dépannage

Cette rubrique fournit de l'aide pour résoudre les problèmes d'ordre général que vous êtes susceptible de rencontrer.

Impossible de nettoyer ou de supprimer un virus

Pour certains virus, vous devez nettoyer manuellement votre ordinateur. Essayez de redémarrer votre ordinateur, puis de relancer l'analyse.

Si le logiciel ne parvient pas à nettoyer ou à supprimer un virus, consultez la bibliothèque d'informations sur les virus à l'adresse suivante : http://us.mcafee.com/virusInfo/default.asp.

Si vous avez besoin d'aide, consultez le service clientèle de McAfee via le site Web de McAfee.

Remarque : il est impossible de nettoyer les virus de CD-ROM, de DVD et de disquettes protégées en écriture.

Après redémarrage, un élément ne peut toujours pas être supprimé

Après analyse et suppression des éléments, certaines situations nécessitent que vous redémarriez votre ordinateur.

Si l'élément n'est pas supprimé après redémarrage de votre ordinateur, envoyez le fichier à McAfee.

Remarque : il est impossible de nettoyer les virus de CD-ROM, de DVD et de disquettes protégées en écriture.

Rubriques connexes

- Gestion des programmes, cookies et fichiers placés en quarantaine (page 99)

Certains composants sont manquants ou corrompus

Certaines situations peuvent entraîner une installation incorrecte de VirusScan.

- Votre ordinateur ne dispose pas d'un espace disque ou d'une mémoire suffisante. Vérifiez que la configuration système de votre ordinateur est compatible avec l'exécution du logiciel.
- Votre navigateur Internet n'est pas correctement configuré.
- Votre connexion à Internet est défectueuse. Vérifiez votre connexion ou tentez de vous reconnecter ultérieurement.
- Certains fichiers sont manquants ou l'installation a échoué.

La meilleure solution est de résoudre ces problèmes potentiels, puis de réinstaller VirusScan.

CHAPITRE 18

McAfee Personal Firewall

Personal Firewall 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.

Contenu de ce chapitre

Caractéristiques

Personal Firewall offre une protection complète en entrée et en sortie, et autorise automatiquement les applications connues. Il aide également à bloquer les logiciels espions, les chevaux de Troie et les enregistreurs de frappe. Firewall vous aide à vous défendre contre les violations et les attaques des pirates, surveille l'activité Internet et du réseau, vous prévient en cas d'événements malveillants ou suspects, fournit des informations détaillées sur le trafic Internet et complète votre protection antivirus.

Niveaux de protection standard et personnalisés

Protégez-vous des intrusions et des activités suspectes grâce aux paramètres de protection par défaut de Firewall ou personnalisez Firewall selon vos propres besoins en matière de sécurité.

Recommandations en temps réel

Vous pouvez recevoir des recommandations, de manière dynamique, pour vous aider à déterminer si vous devez autoriser l'accès de certains programmes à Internet ou si vous pouvez faire confiance au trafic réseau.

Gestion intelligente de l'accès des programmes

Gérez l'accès à Internet des programmes, via un système d'alertes et de journaux d'événements, ou configurez des autorisations d'accès pour des programmes spécifiques dans le volet Autorisations des programmes de Firewall.

Protection de vos séances de jeu

Empêchez les alertes concernant les tentatives d'intrusion et les activités suspectes de vous distraire au cours de vos séances de jeu en plein écran et configurez Firewall de manière à ce que les alertes s'affichent à la fin du jeu.

Protection au démarrage de l'ordinateur

Avant que Windows s'ouvre, Firewall protège votre ordinateur des tentatives d'intrusion, des programmes indésirables et du trafic réseau.

Contrôle du port de service système

Les ports de service système peuvent ouvrir une porte dérobée sur votre ordinateur. Firewall permet de créer et de gérer les ports de service système ouverts et fermés requis par certains programmes.

Gestion des connexions informatiques

Autorisez et bloquez les connexions à distance et les adresses IP qui peuvent se connecter à votre ordinateur.

Intégration des informations de HackerWatch

HackerWatch est un concentrateur d'informations de sécurité qui enregistre les schémas de piratage et d'intrusion généraux, et fournit des informations récentes sur les programmes installés sur votre ordinateur. Vous pouvez afficher des statistiques globales sur les événements de sécurité et sur les ports Internet.

Verrouillage du firewall

Bloquez instantanément tout le trafic réseau entrant et sortant entre votre ordinateur et Internet.

Rétablissement des paramètres de Firewall

Rétablissez instantanément les paramètres de protection d'origine de Firewall. Si Personal Firewall a un fonctionnement inadapté que vous ne parvenez pas à modifier, vous pouvez rétablir les paramètres par défaut de Firewall.

Détection avancée des chevaux de Troie

Personal Firewall associe la gestion des connexions des applications à une base de données améliorée afin de détecter et de bloquer les applications potentiellement nuisibles, telles que les chevaux de Troie, et de les empêcher d'accéder à Internet pour transmettre vos données personnelles.

Consignation des événements

Indiquez si vous souhaitez activer ou désactiver la consignation des événements et, lorsque cette fonction est activée, les types d'événements à consigner. La consignation des événements permet de visualiser les événements entrants et sortants qui se sont produits récemment. Vous pouvez également visualiser les événements d'intrusion détectés.

Surveillance du trafic Internet

Consultez des cartes graphiques faciles à lire indiquant la source des attaques malveillantes ainsi que le trafic mondial. Obtenez également des informations détaillées sur le propriétaire, ainsi que des données géographiques sur les adresses IP émettrices. Vous pouvez en outre analyser le trafic entrant et sortant, et surveiller la bande passante et l'activité des programmes.

Prévention des intrusions

Bloquez toute intrusion de menace Internet potentielle pour protéger votre confidentialité. Grâce à cette fonctionnalité de type heuristique, McAfee apporte un troisième niveau de protection en bloquant les éléments qui présentent des symptômes d'attaques ou des caractéristiques de tentatives de piratage.

Analyse du trafic améliorée

Analysez aussi bien le trafic Internet entrant et sortant que les connexions des programmes, y compris ceux qui écoutent activement les connexions ouvertes. Vous saurez ainsi quels sont les programmes vulnérables et vous pourrez prendre les mesures nécessaires.

Démarrage de Firewall

Dès que vous installez Firewall, votre ordinateur est protégé contre les intrusions et contre le trafic réseau indésirable. De plus, vous êtes prêt à traiter les alertes et à gérer les accès Internet entrants et sortants des programmes connus et inconnus. Les recommandations intelligentes et le niveau de sécurité Standard sont activés automatiquement.

Vous pouvez désactiver Firewall depuis le volet Internet & Configuration réseau mais, dans ce cas, votre ordinateur n'est plus protégé contre les intrusions et le trafic réseau indésirable, et vous ne pouvez plus gérer efficacement les connexions Internet entrantes et sortantes. La désactivation de la protection par pare-feu doit être provisoire et exceptionnelle. Vous pouvez aussi activer Firewall depuis le volet Internet & Configuration réseau.

Firewall désactive automatiquement le pare-feu Windows® pour devenir le pare-feu par défaut.

Remarque : pour configurer Firewall, ouvrez le volet Internet et Configuration réseau.

Activation de la protection par Firewall

La protection par Firewall défend votre ordinateur contre les intrusions et contre le trafic réseau indésirable. Elle vous aide à gérer les connexions Internet entrantes et sortantes.

Pour activer la protection par Firewall :

1. Dans le volet McAfee SecurityCenter, effectuez l'une des opérations suivantes.
   - Cliquez sur **Internet & Réseau**, puis sur **Configurer**.
   - Cliquez sur **Menu avancé**, puis sur **Configurer** dans le volet **Accueil**, et pointez ensuite sur **Internet & Réseau**.
2. Dans le volet **Internet & Configuration réseau**, sous **Protection par Firewall**, cliquez sur **Activer**.

Désactivation de la protection par Firewall

Si vous désactivez la protection par Firewall, votre ordinateur est exposé aux intrusions et au trafic réseau indésirable. Sans protection par Firewall activée, vous ne pouvez plus gérer les connexions Internet entrantes et sortantes.

Pour désactiver la protection par Firewall :

1. Dans le volet McAfee SecurityCenter, effectuez l'une des opérations suivantes.
   - Cliquez sur **Internet & Réseau**, puis sur **Configurer**.
   - Cliquez sur **Menu avancé**, puis sur **Configurer** dans le volet **Accueil**, et pointez ensuite sur **Internet & Réseau**.
2. Dans le volet **Internet & Configuration réseau**, sous **Protection par Firewall**, cliquez sur **Désactiver**.

Utilisation des alertes

Firewall utilise un ensemble d'alertes pour vous aider à gérer votre sécurité. Ces alertes peuvent être classées en quatre catégories principales.

- Alerte : cheval de Troie bloqué
- Alerte rouge
- Alerte jaune
- Alerte verte

Les alertes peuvent aussi contenir les informations nécessaires pour aider l'utilisateur à décider comment traiter les alertes ou à s'informer sur les programmes exécutés sur son ordinateur.

A propos des alertes

Le pare-feu dispose de quatre types d'alertes de base. De même, certaines alertes incluent des informations qui vous aideront à en savoir plus ou à obtenir des informations sur les programmes qui s'exécutent sur votre ordinateur.

Alerte : cheval de Troie bloqué

Un cheval de Troie semble être un programme légitime. Toutefois, il peut interrompre, endommager ou permettre un accès non autorisé à votre ordinateur. Une alerte relative à un cheval de Troie s'affiche si le pare-feu détecte, puis bloque, un cheval de Troie sur votre ordinateur et vous recommande d'effectuer une recherche d'autres menaces éventuelles. Cette alerte peut se produire à tous les niveaux de sécurité, excepté au niveau Ouvert ou lorsque les recommandations intelligentes sont désactivées.

Alerte rouge

Le type d'alerte le plus courant est l'alerte rouge, qui nécessite généralement une réponse de votre part. Le pare-feu ne parvenant pas, dans certains cas, à déterminer automatiquement les actions relatives à l'activité d'un programme ou d'un événement réseau, l'alerte décrit dans un premier temps l'activité du programme ou l'événement réseau en question, puis propose une ou plusieurs options auxquelles vous devez répondre. Si les recommandations intelligentes sont activées, des programmes sont ajoutés dans le volet Autorisations de programme.

Les descriptions d'alertes suivantes sont les plus courantes :

- **Le programme demande l'accès Internet** : le pare-feu détecte un programme qui tente d'accéder à Internet.
- **Le programme a été modifié** : le pare-feu détecte qu'un programme a été modifié d'une manière ou d'une autre : ce peut être le résultat d'une mise à jour en ligne.
- **Programme bloqué** : le pare-feu bloque un programme parce que celui-ci figure dans le volet Autorisations de programme.

Selon vos paramètres et l'activité des programmes ou les événements réseau qui se produisent, les options suivantes sont les plus courantes :

- **Autoriser l'accès** : autorise un programme qui se trouve sur votre ordinateur à accéder à Internet. La règle est ajoutée à la page Autorisations de programme.
- **Accorder l'accès une fois** : autorise un programme qui se trouve sur votre ordinateur à accéder temporairement à Internet. Par exemple, l'installation d'un nouveau programme peut nécessiter un accès unique à Internet.
- **Bloquer l'accès** : empêche un programme d'accéder à Internet.
- **Accorder l'accès sortant uniquement** : autorise uniquement une connexion Internet sortante. Ces alertes apparaissent généralement lorsque les niveaux de sécurité Elevé et Furtif sont définis.
- **Autoriser ce réseau** : autorise le trafic entrant et sortant provenant d'un réseau. Le réseau est ajouté à la section Adresses IP autorisées.
- **Ne pas autoriser ce réseau à ce moment** : bloque le trafic entrant et sortant provenant d'un réseau.

Alerte jaune

L'alerte jaune est une notification non critique vous informant qu'un événement réseau a été détecté par le pare-feu. Par exemple, l'alerte **Nouveau réseau détecté** s'affiche lors de la première exécution du pare-feu ou lorsqu'un ordinateur sur lequel le pare-feu est installé est connecté à un nouveau réseau. Vous pouvez choisir d'autoriser ou non le réseau. Si vous l'autorisez, le pare-feu autorise le trafic émanant de tout ordinateur se trouvant sur le réseau et l'adresse de celui-ci est ajoutée à la liste Adresses IP autorisées.

Alerte verte

Dans la plupart des cas, les alertes vertes fournissent des informations de base concernant un événement et ne requièrent aucune réponse. Ces alertes apparaissent généralement lorsque les niveaux de sécurité Standard, Elevé, Furtif et Bloqué sont définis. Ces alertes sont les suivantes :

- **Le programme a été modifié** : vous informe qu'un programme auquel vous avez précédemment autorisé l'accès à Internet a été modifié. Vous pouvez choisir de bloquer le programme ; toutefois, si vous ne répondez pas, l'alerte disparaît de votre bureau et le programme peut continuer d'accéder à Internet.
- **Programme autorisé à accéder à Internet** : vous informe qu'un programme a été autorisé à accéder à Internet. Vous pouvez choisir de bloquer le programme ; toutefois, si vous ne répondez pas, l'alerte disparaît et le programme peut continuer d'accéder à Internet.

Assistance utilisateur

Les alertes du pare-feu contiennent généralement des informations complémentaires pour vous aider à gérer la sécurité de votre ordinateur, comme par exemple :

- **En savoir plus sur ce programme** : ouvre le site Web de sécurité de McAfee pour vous permettre d'obtenir des informations sur un programme que le pare-feu a détecté sur votre ordinateur.
- **Informer McAfee de ce programme** : envoie à McAfee des informations sur un fichier inconnu que le pare-feu a détecté sur votre ordinateur.
- **McAfee vous recommande de** : affiche des informations concernant le traitement des alertes. Par exemple, une alerte peut vous recommander d'autoriser l'accès à Internet d'un programme.

Gestion des alertes de type Informations

Le pare-feu vous permet d'afficher ou de masquer les alertes de type Informations qui sont générées lors de certains événements.

Afficher des alertes durant une session de jeu

Par défaut, le pare-feu empêche les alertes de type Information de s'afficher durant vos parties de jeu en plein écran. Vous pouvez toutefois configurer le pare-feu pour afficher les alertes d'information durant les sessions de jeu si le pare-feu détecte des tentatives d'intrusion ou des activités suspectes.

Pour afficher les alertes d'information durant les sessions de jeu :

1. Dans le volet Tâches courantes, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans le volet Configuration de SecurityCenter, cliquez sur **Alertes**.
4. Cliquez sur **Avancé**.
5. Dans le volet **Options d'alerte**, sélectionnez **Afficher les alertes d'information en mode jeu**.

Masquer les alertes de type Informations

Les alertes d'information vous informent d'événements ne nécessitant pas un traitement immédiat.

Pour masquer les alertes de type Informations :

1. Dans le volet Tâches courantes, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans le volet Configuration de SecurityCenter, cliquez sur **Alertes**.
4. Cliquez sur **Avancé**.
5. Dans le volet **Configuration de SecurityCenter**, cliquez sur **Alertes d'information**.
6. Dans le volet **Alertes d'information**, vous pouvez soit :
   - Sélectionner un type d'alerte à masquer.
   - Sélectionner **Masquer les alertes de type Informations** pour masquer toutes les alertes de type Informations.

7 Cliquez sur **OK**.

CHAPITRE 19

Configuration de la protection Firewall

Firewall offre diverses méthodes pour gérer votre sécurité et pour personnaliser la manière dont vous souhaitez réagir aux événements et alertes de sécurité.

Lorsque vous installez Firewall pour la première fois, le niveau de protection Standard est activé. Ce paramétrage est satisfaisant dans la plupart des cas. Cependant, Firewall propose d'autres niveaux, du plus restrictif au plus permissif.

Firewall vous donne en outre la possibilité de recevoir des recommandations concernant les alertes et l'accès à Internet des programmes.

Contenu de ce chapitre

Gestion des niveaux de sécurité de Firewall

Vous pouvez configurer les niveaux de sécurité de façon à déterminer le degré selon lequel vous souhaitez gérer les alertes et y réagir lorsque Firewall détecte un trafic réseau et des connexions Internet entrantes et sortantes indésirables. Par défaut, le niveau de sécurité Standard est activé.

Lorsque le niveau de sécurité Standard est configuré et que les recommandations intelligentes sont activées, des alertes rouges proposent des options pour autoriser ou interdire l'accès aux programmes inconnus ou modifiés. Lorsque des programmes connus sont détectés, des alertes vertes apparaissent à titre informatif et l'accès à ces programmes est automatique. Lorsqu'un programme bénéficie d'une autorisation d'accès, il peut créer des connexions sortantes et être à l'écoute des connexions entrantes non sollicitées.

D'une manière générale, plus un niveau de sécurité est restrictif (Furtif et Elevé), plus le nombre d'options et d'alertes affichées, et donc le nombre d'interventions de votre part, est important.

Firewall utilise six niveaux de sécurité. Du plus restrictif au plus permissif, ces niveaux sont les suivants :

- **Verrouillage** : bloque toutes les connexions Internet.
- **Furtif** : bloque toutes les connexions Internet entrantes.
- **Elevé** : des alertes vous invitent à indiquer si vous autorisez les connexions Internet entrantes ou sortantes demandées.
- **Standard** : des alertes vous avertissent lorsqu'un programme inconnu ou nouveau demande à accéder à Internet.
- **Faible** : autorise toutes les connexions Internet entrantes et sortantes et les ajoute automatiquement au volet Autorisations de programme.
- **Ouvert** : autorise toutes les connexions Internet entrantes et sortantes.

Firewall vous permet également de rétablir immédiatement le niveau de sécurité Standard depuis le volet Restaurer les paramètres de protection par défaut du pare-feu.

Activation du niveau de sécurité Verrouillage

Lorsque vous activez le niveau de sécurité Verrouillage du pare-feu, vous bloquez toutes les connexions réseau entrantes et sortantes, y compris l'accès aux sites Web, aux e-mails et aux mises à jour de sécurité. Cette opération équivaut à vous déconnecter d'Internet. Vous pouvez utiliser ce paramètre pour bloquer des ports que vous avez configurés comme ouverts dans le volet Services système. Pendant le verrouillage, des alertes peuvent continuer à vous inviter à bloquer les programmes.

Pour activer le niveau de sécurité Verrouillage du pare-feu :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Verrouillage**.
3. Cliquez sur **OK**.

Activation du niveau de sécurité Furtif

Lorsque vous activez le niveau de sécurité Furtif du pare-feu, vous bloquez toutes les connexions réseau entrantes à l'exception des ports ouverts. Ce paramètre masque totalement la présence de votre ordinateur sur Internet. Lorsque le niveau de sécurité Furtif est activé, le pare-feu vous avertit lorsque de nouveaux programmes tentent d'effectuer une connexion Internet sortante ou reçoivent une demande de connexion entrante. Les programmes bloqués et ajoutés s'affichent dans le volet Autorisations de programme.

Pour activer le niveau de sécurité Furtif du pare-feu :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Furtif**.
3. Cliquez sur **OK**.

Activation du niveau de sécurité Elevé

Lorsque le niveau de sécurité Elevé est activé, le pare-feu vous avertit lorsque de nouveaux programmes tentent d'effectuer une connexion Internet sortante ou reçoivent une demande de connexion entrante. Les programmes bloqués et ajoutés s'affichent dans le volet Autorisations de programme. Lorsque le niveau de sécurité Elevé est activé, un programme ne demande que le type d'accès dont il a besoin à ce moment précis (accès uniquement sortant, par exemple), que vous pouvez alors autoriser ou interdire. Ultérieurement, si le programme demande une connexion à la fois entrante et sortante, vous pouvez lui accorder un accès complet depuis le volet Autorisations de programme.

Pour activer le niveau de sécurité Elevé du pare-feu :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Elevé**.
3. Cliquez sur **OK**.

Activation du niveau de sécurité Standard

Standard correspond au niveau de sécurité par défaut et recommandé.

Lorsque le niveau de sécurité Standard est activé, le Firewall surveille les connexions entrantes et sortantes. Il vous avertit lorsque de nouveaux programmes tentent d'accéder à Internet. Les programmes bloqués et ajoutés s'affichent dans le volet Autorisations de programme.

Pour activer le niveau de sécurité Standard du Firewall :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Standard**.
3. Cliquez sur **OK**.

Activation du niveau de sécurité Faible

Lorsque vous définissez le niveau de sécurité du pare-feu sur Faible, vous autorisez toutes les connexions réseau entrantes et sortantes. Le pare-feu autorise automatiquement l'accès à tous les programmes et ajoute ceux-ci à la liste des programmes autorisés dans le volet Autorisations de programme.

Pour activer le niveau de sécurité Faible du pare-feu :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Faible**.
3. Cliquez sur **OK**.

Configuration des recommandations intelligentes pour les alertes

Vous pouvez configurer le Firewall pour inclure, exclure ou afficher les recommandations sous forme d'alertes relatives aux programmes qui tentent d'accéder à Internet.

Les recommandations intelligentes vous aident à savoir comment traiter une alerte. Lorsque les recommandations intelligentes sont activées (et que le niveau de sécurité standard est activé), le Firewall autorise ou bloque automatiquement les programmes connus. Il vous avertit s'il détecte un programme non reconnu ou potentiellement dangereux et vous indique la conduite à tenir.

Lorsque les recommandations intelligentes sont désactivées, le Firewall n'autorise pas et ne bloque pas automatiquement l'accès à Internet et ne vous indique pas non plus la conduite à tenir.

Si le Firewall est configuré pour afficher uniquement des recommandations intelligentes, une alerte vous invite à autoriser ou interdire l'accès et vous indique la conduite à tenir.

Activation des recommandations intelligentes

Les recommandations intelligentes vous aident à décider comment traiter les alertes. Lorsque les recommandations intelligentes sont activées, le pare-feu autorise ou bloque automatiquement les programmes et vous avertit s'il détecte un programme non reconnu ou potentiellement dangereux.

Pour activer les recommandations intelligentes :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, sous **Recommandations intelligentes**, sélectionnez **Activer les recommandations intelligentes**.
3. Cliquez sur **OK**.

Désactivation des recommandations intelligentes

Lorsque vous désactivez les recommandations intelligentes, les alertes ne proposent plus d'assistance sur le traitement des alertes ni la gestion d'accès des programmes. Si les recommandations intelligentes sont désactivées, le pare-feu continue à autoriser et à bloquer les programmes et vous avertit s'il détecte un programme non reconnu ou potentiellement dangereux. Et, s'il détecte un nouveau programme suspect ou connu comme étant une menace possible, Firewall bloque automatiquement l'accès à Internet du programme.

Pour désactiver les recommandations intelligentes :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, sous **Recommandations intelligentes**, sélectionnez **Désactiver les recommandations intelligentes**.
3. Cliquez sur **OK**.

Affichage des recommandations intelligentes uniquement

L'affichage des recommandations intelligentes vous aide à décider comment traiter les alertes concernant les programmes non reconnus et potentiellement dangereux. Lorsque l'option Recommandations intelligentes a pour valeur **Afficher uniquement**, les informations concernant le traitement des alertes sont affichées mais, à la différence de l'option **Activer les recommandations intelligentes**, les recommandations affichées ne sont pas automatiquement appliquées et l'accès des programmes n'est pas automatiquement autorisé ou bloqué. A la place, les alertes fournissent des recommandations pour vous aider à déterminer s'il convient d'autoriser ou de bloquer les programmes.

Pour afficher les recommandations intelligentes uniquement :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, sous **Recommandations intelligentes**, sélectionnez **Afficher uniquement**.
3. Cliquez sur **OK**.

Optimisation de la sécurité du Firewall

La sécurité de votre ordinateur peut être mise en péril de différentes manières. Par exemple, certains programmes peuvent tenter de se connecter à Internet avant le lancement de Windows®. En outre, des utilisateurs expérimentés peuvent envoyer une requête ping à votre ordinateur pour savoir s'il est connecté à un réseau. Le Firewall vous protège contre ces deux types d'intrusions en permettant d'activer la protection au démarrage et de bloquer les requêtes ping ICMP. Le premier paramètre interdit aux programmes d'accéder à Internet au démarrage de Windows, et le second bloque les requêtes ping grâce auxquelles d'autres utilisateurs peuvent détecter votre ordinateur sur un réseau.

Les paramètres d'installation standard incluent la détection automatique des tentatives d'intrusion les plus courantes, comme les attaques par déni de service ou l'utilisation des failles. L'utilisation des paramètres d'installation standard garantit une protection contre les attaques et les accès indésirables. Toutefois, vous pouvez désactiver la détection automatique de certains types d'attaques ou d'accès dans le volet Détection des intrusions.

Protection de votre ordinateur au démarrage

Le pare-feu vous permet de protéger votre ordinateur au démarrage de Windows. La protection au démarrage bloque l'accès à Internet de tous les nouveaux programmes pour lesquels l'accès à Internet n'a pas été préalablement autorisé. Après le lancement du pare-feu, des alertes appropriées s'affichent pour les programmes ayant demandé l'accès à Internet au démarrage ; vous pouvez alors autoriser ou bloquer l'accès de chaque programme. Pour pouvoir utiliser cette option, votre niveau de sécurité ne doit pas être défini sur Ouvert ou sur Verrouillage.

Pour protéger votre ordinateur au démarrage :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, sous Paramètres de sécurité, sélectionnez **Activer la protection au démarrage**.
3. Cliquez sur **OK**.

Remarque : les connexions et les intrusions bloquées ne sont pas consignées lorsque la protection au démarrage est activée.

Configuration des paramètres de requête ping

Les utilisateurs d'ordinateurs peuvent utiliser un utilitaire Ping (permettant d'envoyer et de recevoir des messages ICMP Echo Request (requêtes d'écho ICMP)) afin de déterminer si un ordinateur donné est connecté au réseau. Vous pouvez configurer votre pare-feu pour autoriser ou empêcher les utilisateurs d'ordinateurs d'envoyer des requêtes ping à votre ordinateur.

Pour configurer les paramètres de requêtes ping ICMP :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, sous **Paramètres de sécurité**, effectuez l'une des actions suivantes :
   - Sélectionnez **Autoriser les requêtes ping ICMP** pour autoriser la détection de votre ordinateur sur le réseau à l'aide de requêtes ping.
   - Décochez la case **Autoriser les requêtes ping ICMP** pour empêcher la détection de votre ordinateur sur le réseau à l'aide de requêtes ping.
3. Cliquez sur **OK**.

Configuration de la détection des intrusions

Le système de détection d'intrusion IDS contrôle les paquets de données afin de déceler les transferts de données ou les méthodes de transfert suspects. IDS analyse le trafic et les paquets de données afin de déterminer les schémas de trafic utilisés par les pirates. Par exemple, si 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. Firewall compare les paquets à une base de données de signatures et, s'ils s'avèrent suspects ou dangereux, il les supprime de l'ordinateur en cause et, éventuellement, consigne l'événement.

Les paramètres d'installation standard incluent la détection automatique des tentatives d'intrusion les plus courantes, comme les attaques par déni de service ou l'utilisation des failles. L'utilisation des paramètres d'installation standard garantit une protection contre les attaques et les accès indésirables. Toutefois, vous pouvez désactiver la détection automatique de certains types d'attaques ou d'accès dans le volet Détection des intrusions.

Pour configurer la détection des intrusions :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Détection des intrusions**.
3. Sous **Détecter les tentatives d'intrusion**, effectuez l'une des actions suivantes :
   - Sélectionnez un nom pour détecter automatiquement l'attaque ou effectuer une analyse.
   - Désélectionnez un nom pour désactiver la détection ou l'analyse automatique.
4. Cliquez sur **OK.**

Configurer les paramètres relatifs à l'état de la protection par pare-feu

SecurityCenter effectue le suivi des problèmes liés à l'état de protection générale de votre ordinateur. Vous pouvez cependant configurer le pare-feu pour ignorer les problèmes spécifiques à votre ordinateur qui sont susceptibles d'affecter votre état de protection. Vous pouvez configurer SecurityCenter pour ignorer le fait que le pare-feu est configuré sur le niveau de sécurité Ouvert, que le service de pare-feu ne fonctionne pas et qu'aucun pare-feu en sortie n'est installé sur votre ordinateur.

Pour configurer les paramètres relatifs à l'état de la protection par pare-feu :

1. Dans le volet Tâches courantes, cliquez sur **Menu Avancé**.
2. Cliquez sur **Configurer**.
3. Dans le volet Configuration de SecurityCenter, cliquez sur **Alertes**.
4. Cliquez sur **Avancé**.
5. Dans le volet Tâches courantes, cliquez sur **Menu avancé**.
6. Cliquez sur **Configurer**.
7. Dans le volet Configuration de SecurityCenter, cliquez sur **Etat de protection**.
8. Cliquez sur Options avancées.
9. Dans le volet Problèmes ignorés, sélectionnez une ou plusieurs des options suivantes :
   - **Le pare-feu est configuré sur le niveau de sécurité Ouvert.**
   - **Le service de pare-feu ne fonctionne pas.**
   - **Le pare-feu en sortie n'est pas installé sur votre ordinateur.**
10. Cliquez sur **OK**.

Verrouillage et restauration du pare-feu

Le verrouillage est utile pour gérer les urgences liées à l'ordinateur, lorsqu'il est nécessaire de bloquer tout trafic pour isoler et résoudre un problème sur son ordinateur, ou en cas d'incertitude, pour déterminer comment gérer l'accès d'un programme à Internet.

Verrouillage instantané du pare-feu

Le verrouillage du pare-feu bloque instantanément tout le trafic réseau entrant et sortant entre votre ordinateur et Internet. Il empêche toutes les connexions à distance d'accéder à votre ordinateur et tous les programmes s'exécutant sur votre ordinateur d'accéder à Internet.

Pour verrouiller instantanément le pare-feu et bloquer tout le trafic réseau :

1. Dans les volets Page d'accueil ou Tâches courantes, lorsque l'option **De base** ou **Menu avancé** est activée, cliquez sur **Verrouiller le pare-feu**.
2. Dans le volet Verrouiller le pare-feu, cliquez sur **Verrouillage**.
3. Dans la boîte de dialogue, cliquez sur **Oui** pour confirmer que vous souhaitez bloquer instantanément l'ensemble du trafic entrant et sortant.

Déverrouillage instantané du pare-feu

Le verrouillage du pare-feu bloque instantanément tout le trafic réseau entrant et sortant entre votre ordinateur et Internet. Il empêche toutes les connexions à distance d'accéder à votre ordinateur et tous les programmes s'exécutant sur votre ordinateur d'accéder à Internet. Vous pourrez par la suite le déverrouiller pour autoriser le trafic réseau.

Pour déverrouiller instantanément le pare-feu et autoriser le trafic réseau :

1. Dans les volets Page d'accueil ou Tâches courantes, lorsque l'option **De base** ou **Menu avancé** est activée, cliquez sur **Verrouiller le pare-feu**.
2. Dans le volet Verrouillage activé, cliquez sur **Déverrouiller**.
3. Dans la boîte de dialogue, cliquez sur **Oui** pour confirmer que vous souhaitez déverrouiller le pare-feu et autoriser le trafic réseau.

Restaurer les paramètres du pare-feu

Vous pouvez restaurer rapidement les paramètres de protection définis à l'origine pour le pare-feu. Cela définit le niveau de sécurité sur standard, active les recommandations intelligentes, redéfinit les adresses IP autorisées et interdites et supprime tous les programmes figurant dans le volet Autorisations de programme.

Pour restaurer les paramètres d'origine du pare-feu :

1. Dans les volets Page d'accueil ou Tâches courantes, lorsque l'option **De base** ou **Menu avancé** est activée, cliquez sur **Restaurer les paramètres par défaut du pare-feu**.
2. Dans le volet Restaurer les paramètres de protection par défaut du pare-feu, cliquez sur **Paramètres par défaut**.
3. Dans la boîte de dialogue Restaurer les paramètres de protection par défaut du pare-feu, cliquez sur **Oui** pour confirmer que vous souhaitez rétablir les paramètres par défaut.

Activation du niveau de sécurité Ouvert

Lorsque vous activez le niveau de sécurité Ouvert du pare-feu, vous autorisez toutes les connexions réseau entrantes et sortantes. Pour autoriser l'accès à des programmes précédemment bloqués, utilisez le volet Autorisations de programme.

Pour activer le niveau de sécurité Ouvert du pare-feu :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Niveau de sécurité, faites glisser le curseur jusqu'à ce que le niveau actuel affiché soit **Ouvert**.
3. Cliquez sur **OK**.

Remarque : lorsque le niveau de sécurité du pare-feu est configuré sur **Ouvert**, l'accès aux programmes précédemment bloqués est toujours interdit. Pour éviter cet inconvénient, vous pouvez définir la règle du programme sur **Accès total**.

CHAPITRE 20

Gestion des programmes et des autorisations

Le pare-feu vous permet de gérer et de créer des autorisations d'accès pour les programmes (nouveaux et existants) nécessitant des accès Internet entrants et sortants. Le pare-feu vous permet d'accorder aux programmes un accès total ou sortant uniquement. Vous pouvez également bloquer l'accès des programmes.

Contenu de ce chapitre

Autorisation de l'accès à Internet des programmes

Certains programmes, comme les navigateurs Internet, doivent accéder à Internet pour fonctionner correctement.

Le pare-feu vous permet d'utiliser la page Autorisations de programme pour :

- Autoriser l'accès des programmes
- Autoriser l'accès sortant uniquement des programmes
- Bloquer l'accès des programmes

Vous pouvez également autoriser un accès complet ou un accès sortant uniquement depuis le journal des événements sortants ou des événements récents.

Autorisation de l'accès total d'un programme

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Personal Firewall comprend une liste de programmes automatiquement autorisés à accéder à Internet. Vous pouvez toutefois modifier ces autorisations.

Pour accorder à un programme un accès total à Internet :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
3. Sous **Autorisations de programme**, sélectionnez un programme défini sur **Bloqué** ou sur **Accès sortant uniquement**.
4. Sous **Action**, cliquez sur **Accorder l'accès total**.
5. Cliquez sur **OK**.

Autorisation de l'accès total d'un nouveau programme

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Le Firewall comprend une liste de programmes configurés pour avoir automatiquement un accès total à Internet. Vous pouvez toutefois ajouter des programmes et modifier leurs autorisations.

Pour accorder à un nouveau programme un accès total à Internet :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet **Firewall**, cliquez sur **Autorisations de programme**.
3. Sous **Autorisations de programme**, cliquez sur **Ajouter un programme autorisé**.
4. Dans la boîte de dialogue d'**ajout de programmes**, recherchez et sélectionnez le programme voulu.
5. Cliquez sur **Ouvrir**.
6. Cliquez sur **OK**.

   Le programme récemment ajouté apparaît sous **Autorisations de programme**.

Remarque : vous pouvez modifier les autorisations définies pour un programme récemment ajouté comme vous le feriez pour un autre programme, en sélectionnant le programme voulu puis en cliquant sur **Accorder l'accès sortant uniquement** ou sur **Bloquer l'accès** sous **Action**.

Accorder un accès total depuis le journal des événements récents

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Vous pouvez sélectionner un programme dans le journal des événements récents et lui accorder un accès Internet total.

Pour accorder un accès total à un programme depuis le journal des événements récents :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous Evénements récents, sélectionnez une description de l'événement, puis cliquez sur **Accorder l'accès total**.
3. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer que vous souhaitez accorder un accès total au programme.

Rubriques connexes

- Afficher les événements sortants (page 168)

Autorisation d'un accès total depuis le journal des événements sortants

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Vous pouvez sélectionner un programme dans le journal des événements sortants et lui accorder un accès total à Internet.

Pour accorder à un programme un accès total à Internet dans le journal des événements sortants :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Sélectionnez **Internet et réseau**, puis **Evénements sortants**.
4. Dans le volet Evénements sortants, sélectionnez une adresse IP source, puis cliquez sur **Autoriser l'accès**.
5. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer que vous souhaitez accorder au programme un accès total à Internet.

Rubriques connexes

- Afficher les événements sortants (page 168)

Autorisation de l'accès sortant uniquement des programmes

Certains programmes se trouvant sur votre ordinateur nécessitent uniquement un accès sortant à Internet. Le pare-feu vous permet d'accorder aux programmes un accès sortant uniquement à Internet.

Autorisation de l'accès sortant uniquement d'un programme

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Personal Firewall comprend une liste de programmes automatiquement autorisés à accéder à Internet. Vous pouvez toutefois modifier ces autorisations.

Pour accorder un accès sortant uniquement à un programme :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
3. Sous **Autorisations de programme**, sélectionnez un programme défini sur **Bloqué** ou sur **Accès total**.
4. Sous **Action**, cliquez sur **Accorder l'accès sortant uniquement**.
5. Cliquez sur **OK**.

Accorder un accès sortant uniquement depuis le journal des événements récents

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Vous pouvez sélectionner un programme dans le journal des événements récents et lui accorder un accès Internet uniquement sortant.

Pour accorder un accès uniquement sortant à un programme depuis le journal des événements récents :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous Evénements récents, sélectionnez une description de l'événement, puis cliquez sur **Accorder l'accès sortant uniquement**.
3. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer que vous souhaitez accorder au programme un accès sortant uniquement.

Rubriques connexes

- Afficher les événements sortants (page 168)

Autorisation d'un accès sortant uniquement depuis le journal des événements sortants

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Vous pouvez sélectionner un programme dans le journal des événements sortants et lui accorder un accès Internet uniquement sortant.

Pour accorder un accès uniquement sortant à un programme depuis le journal des événements sortants :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Sélectionnez **Internet et réseau**, puis **Evénements sortants**.
4. Dans le volet Evénements sortants, sélectionnez une adresse IP source, puis cliquez sur **Accorder l'accès sortant uniquement**.
5. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer que vous souhaitez accorder au programme un accès sortant uniquement.

Rubriques connexes

- Afficher les événements sortants (page 168)

Blocage de l'accès Internet des programmes

Le pare-feu vous permet d'empêcher les programmes d'accéder à Internet. Assurez-vous que le blocage de l'accès d'un programme n'interrompe pas votre connexion réseau ou un autre programme devant accéder à Internet pour pouvoir fonctionner correctement.

Blocage de l'accès d'un programme

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Personal Firewall comprend une liste de programmes automatiquement autorisés à accéder à Internet. Vous pouvez toutefois bloquer ces autorisations.

Pour bloquer l'accès à Internet d'un programme :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
3. Sous **Autorisations de programme**, sélectionnez un programme défini sur **Accès total** ou sur **Accès sortant uniquement**.
4. Sous **Action**, cliquez sur **Bloquer l'accès**.
5. Cliquez sur **OK**.

Blocage de l'accès d'un nouveau programme

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Personal Firewall comprend une liste de programmes configurés pour avoir automatiquement un accès total à Internet. Vous pouvez toutefois ajouter des programmes, puis bloquer leur accès à Internet.

Pour bloquer l'accès à Internet d'un nouveau programme :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Firewall, cliquez sur **Autorisations de programme**.
3. Sous **Autorisations de programme**, cliquez sur **Ajouter un programme bloqué**.
4. Dans la boîte de dialogue d'**ajout de programmes**, recherchez et sélectionnez le programme voulu.
5. Cliquez sur **Ouvrir**.
6. Cliquez sur **OK**.

   Le programme récemment ajouté apparaît sous **Autorisations de programme**.

Remarque : vous pouvez modifier les autorisations définies pour un programme récemment ajouté comme vous le feriez pour un autre programme, en sélectionnant le programme voulu puis en cliquant sur **Accorder l'accès sortant uniquement** ou sur **Accorder l'accès total** sous **Action**.

Bloquer l'accès depuis le journal des événements récents

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Cependant, vous pouvez également choisir de bloquer l'accès des programmes à Internet depuis le journal des événements récents.

Pour bloquer l'accès d'un programme depuis le journal des événements récents :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous Evénements récents, sélectionnez une description de l'événement, puis cliquez sur **Bloquer l'accès**.
3. Dans la boîte de dialogue Autorisations de programme, cliquez sur **Oui** pour confirmer que vous souhaitez bloquer l'accès au programme.

Rubriques connexes

- Afficher les événements sortants (page 168)

Suppression des autorisations d'accès de certains programmes

Avant de retirer l'autorisation d'accès d'un programme, assurez-vous que cela n'affecte pas le fonctionnement de votre ordinateur ou de votre connexion réseau.

Suppression des autorisations d'un programme

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Personal Firewall comprend une liste de programmes configurés pour avoir automatiquement un accès total à Internet ; vous pouvez toutefois retirer des programmes ayant été ajoutés automatiquement ou manuellement.

Pour retirer l'autorisation définie pour un nouveau programme :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Autorisations de programme**.
3. Sous **Autorisations de programme**, sélectionnez un programme.
4. Sous **Action**, cliquez sur **Annuler l'autorisation de programme**.
5. Cliquez sur **OK**.

   Le programme est supprimé du volet Autorisations de programme.

Remarque : le pare-feu vous empêche de modifier certains programmes (les actions sont alors désactivées ou apparaissent en grisé).

En savoir plus sur les programmes

Si vous n'êtes pas sûr de savoir quelles autorisations définir pour un programme, vous pouvez obtenir des informations sur le programme concerné sur le site Web HackerWatch de McAfee

Obtention d'informations sur un programme

De nombreux programmes se trouvant sur votre ordinateur nécessitent un accès entrant et sortant à Internet. Personal Firewall comprend une liste de programmes automatiquement autorisés à accéder à Internet ; vous pouvez toutefois modifier ces autorisations.

Le pare-feu peut vous aider à décider si vous autorisez ou si vous bloquez l'accès à Internet d'un programme. Assurez-vous que vous êtes bien connecté à Internet afin que votre navigateur se connecte bien au site Web HackerWatch de McAfee, où vous trouverez des informations à jour sur les programmes, les conditions d'accès à Internet et les menaces potentielles en termes de sécurité.

Pour obtenir des informations sur un programme :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Autorisations de programme**.
3. Sous **Autorisations de programme**, sélectionnez un programme.
4. Sous **Action**, cliquez sur **Plus d'informations**.

Obtenir des informations sur un programme depuis le journal des événements sortants

Personal Firewall vous permet d'obtenir des informations sur les programmes figurant dans le journal des événements sortants.

Avant de tenter d'obtenir des informations sur un programme, vérifiez que vous disposez bien d'une connexion Internet et d'un navigateur Internet.

Pour obtenir des informations sur un programme depuis le journal des événements sortants :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Sélectionnez **Internet et réseau**, puis **Evénements sortants**.
4. Dans le volet Evénements sortants, sélectionnez une adresse IP source, puis cliquez sur **Plus d'informations**.

   Vous pouvez afficher des informations concernant le programme sur le site Web HackerWatch. HackerWatch fournit des informations actualisées sur les programmes, les conditions d'accès à Internet et les menaces contre la sécurité.

Rubriques connexes

- Afficher les événements sortants (page 168)

CHAPITRE 21

Gestion des services système

Certaines applications, notamment les programmes de serveur Web ou de partage de fichiers, doivent pouvoir accepter les connexions non sollicitées d'autres ordinateurs via les ports de service système désignés. En général, Firewall ferme ces ports de service système car ils constituent la source la plus probable de menaces pour la sécurité de votre système. Cependant, pour que les demandes de connexion émises par des ordinateurs distants puissent être acceptées, il est nécessaire que les ports de service système soient ouverts.

La liste suivante présente les ports standard pour les services les plus courants.

- Ports 20-21 de protocole de transfert de fichiers (FTP)
- Port 143 de serveur de messagerie (IMAP)
- Port 110 de serveur de messagerie (POP3)
- Port 25 de serveur de messagerie (SMTP)
- Port 445 de Microsoft Directory Server (MSFT DS)
- Port 1433 de Microsoft SQL Server (MSFT SQL)
- Port 3389 d'assistance à distance/de Terminal Server (RDP)
- Port 135 d'appel de procédure à distance (RPC)
- Port 443 de serveur Web sécurisé (HTTPS)
- Port 5000 Universal Plug and Play (UPNP)
- Port 80 de serveur Web (HTTP)
- Ports 137-139 de partage de fichiers Windows (NETBIOS)

Contenu de ce chapitre

Configuration des ports de service système

Pour autoriser un accès distant à un service de votre ordinateur, vous devez spécifier ce service ainsi que le port associé à ouvrir. Sélectionnez un service et un port uniquement si vous êtes sûr que celui-ci doit être ouvert. Il est rarement nécessaire d'ouvrir un port.

Autoriser l'accès à un port de service système existant

Dans le volet Services système, vous pouvez ouvrir ou fermer un port existant afin d'autoriser ou d'interdire l'accès distant à un service réseau de votre ordinateur. Un port ouvert de service système peut rendre votre ordinateur vulnérable aux menaces Internet. Par conséquent, n'ouvrez un port que si c'est vraiment indispensable.

Pour autoriser l'accès à un port de service système :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Services système**.
3. Sous **Port ouvert de service système**, sélectionnez un service système pour ouvrir un port.
4. Cliquez sur **OK**.

Blocage de l'accès à un port de service système

Dans le volet Services système, vous pouvez ouvrir ou fermer un port existant afin d'autoriser ou d'interdire l'accès distant à un service réseau de votre ordinateur. Un port ouvert de service système peut rendre votre ordinateur vulnérable aux menaces Internet. Par conséquent, n'ouvrez un port que si c'est vraiment indispensable.

Pour bloquer l'accès à un port de service système :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Services système**.
3. Sous **Port ouvert de service système**, décochez un service système pour fermer un port.
4. Cliquez sur **OK**.

Configurer un nouveau port de service système

Dans le volet Services système, vous pouvez ajouter un nouveau port de service système que vous pourrez ensuite ouvrir ou fermer afin d'autoriser ou d'interdire l'accès distant à un service réseau de votre ordinateur. Un port ouvert de service système peut rendre votre ordinateur vulnérable aux menaces Internet. Par conséquent, ouvrez un port uniquement si cela est indispensable.

Pour créer et configurer un nouveau port de service système :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Services système**.
3. Cliquez sur **Ajouter**.
4. Sous **Ajouter une configuration de port**, spécifiez les paramètres suivants :
   - Nom du programme
   - Ports TCP/IP entrants
   - Ports TCP/IP sortants
   - Ports UDP entrants
   - Ports UDP sortants
5. Eventuellement, décrivez la nouvelle configuration.
6. Cliquez sur **OK**.

   Le port de service système que vous venez de configurer apparaît sous **Port ouvert de service système**.

Modification d'un port de service système

Un port ouvert et fermé autorise et interdit l'accès à un service réseau de votre ordinateur. Dans le volet Services système, vous pouvez modifier les informations entrantes et sortantes relatives à un port existant. Si vous saisissez les informations du port de manière erronée, le service système échouera.

Pour modifier un port de service système :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Services système**.
3. Sélectionnez un service système et cliquez sur **Modifier**.
4. Sous **Ajouter une configuration de port**, spécifiez les paramètres suivants :
   - Nom du programme

- Ports TCP/IP entrants
- Ports TCP/IP sortants
- Ports UDP entrants
- Ports UDP sortants

5 Eventuellement, décrivez la configuration modifiée.

6 Cliquez sur **OK**.

Le port de service système dont vous venez de modifier la configuration apparaît sous **Port ouvert de service système**.

Suppression d'un port de service système

Un port ouvert ou fermé autorise ou interdit l'accès à un service réseau sur votre ordinateur. Dans le volet Services système, vous pouvez supprimer un port existant et le service système associé. Une fois qu'un port et un service système sont supprimés du volet Services système, les ordinateurs distants ne peuvent plus accéder au service réseau sur votre ordinateur.

Pour supprimer un port de service système :

1 Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.

2 Dans le volet Pare-feu, cliquez sur **Services système**.

3 Sélectionnez un service système, puis cliquez sur **Supprimer**.

4 Dans la boîte de dialogue **Services système**, cliquez sur **Oui** pour confirmer que vous souhaitez supprimer le service système.

Le port du service système n'apparaît plus dans le volet Services système.

CHAPITRE 22

Gestion des connexions informatiques

Vous pouvez configurer le pare-feu pour gérer des connexions distantes à votre ordinateur en créant des règles basées sur des adresses IP (Internet Protocol) et associées à des ordinateurs distants. Les ordinateurs associés à des adresses IP autorisées sont considérés comme fiables pour se connecter à votre ordinateur, et vous pouvez interdire aux IP inconnues, suspectes ou non fiables de se connecter à celui-ci.

Lorsque vous autorisez une connexion, assurez-vous que l'ordinateur que vous autorisez n'est pas infecté. Si celui-ci est infecté par un ver ou un autre mécanisme, votre ordinateur sera exposé au même risque. En outre, McAfee recommande que les ordinateurs que vous autorisez soient également protégés par un firewall et par un antivirus à jour. Le pare-feu ne consigne pas le trafic et ne génère aucune alerte pour les adresses de la liste Adresses IP autorisées.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Contenu de ce chapitre

Fiabilité des connexions informatiques

Vous pouvez ajouter, modifier ou supprimer des adresses IP fiables dans le volet Adresses IP autorisées et interdites, sous **Adresses IP autorisées**.

La liste **Adresses IP autorisées** du volet Adresses IP autorisées et interdites permet d'autoriser tout le trafic provenant d'un ordinateur donné à accéder à votre ordinateur. Firewall ne consigne pas le trafic et ne génère aucune alerte pour les adresses qui figurent dans la liste **Adresses IP autorisées**.

Le pare-feu autorise toutes les adresses IP vérifiées de cette liste et permet toujours au trafic provenant d'une adresse IP fiable de franchir le pare-feu, quels que soient les ports concernés. Le pare-feu ne consigne aucun événement provenant des adresses IP autorisées. L'activité entre l'ordinateur associé à une adresse IP fiable et votre ordinateur n'est pas filtrée ou analysée par le pare-feu.

Lorsque vous autorisez une connexion, assurez-vous que l'ordinateur que vous autorisez n'est pas infecté. Si celui-ci est infecté par un ver ou un autre mécanisme, votre ordinateur sera exposé au même risque. En outre, McAfee recommande que les ordinateurs que vous autorisez soient également protégés par un firewall et par un antivirus à jour.

Ajout d'une connexion fiable à un ordinateur

Vous pouvez utiliser le pare-feu pour ajouter une connexion fiable à un ordinateur et l'adresse IP qui lui est associée.

La liste **Adresses IP autorisées** du volet Adresses IP autorisées et interdites permet d'autoriser tout le trafic provenant d'un ordinateur donné à accéder à votre ordinateur. Firewall ne consigne pas le trafic et ne génère aucune alerte pour les adresses qui figurent dans la liste **Adresses IP autorisées**.

Les ordinateurs associés à des adresses IP autorisées peuvent toujours se connecter à votre ordinateur. Avant d'ajouter, de modifier ou de supprimer une adresse IP autorisée, assurez-vous qu'il s'agit bien de l'adresse IP sécurisée.

Pour ajouter une connexion fiable à un ordinateur :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
3. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP autorisées**.
4. Cliquez sur **Ajouter**.
5. Sous **Ajouter une règle d'adresse IP autorisée**, vous pouvez soit :
   - Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.
   - Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.
6. Le cas échéant, sélectionnez **La règle expire dans**, puis entrez le nombre de jours où la règle doit être appliquée.
7. Eventuellement, entrez une description de cette règle.
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue Ajouter une règle d'adresse IP autorisée, cliquez sur **Oui** pour confirmer que vous souhaitez ajouter la connexion fiable à un ordinateur.

   L'adresse IP récemment ajoutée apparaît sous **Adresses IP autorisées**.

Ajouter un ordinateur autorisé depuis le journal des événements entrants

Vous pouvez ajouter la connexion d'un ordinateur autorisé et l'adresse IP associée depuis le journal des événements entrants.

Les ordinateurs associés à des adresses IP autorisées peuvent toujours se connecter à votre ordinateur. Avant d'ajouter, de modifier ou de supprimer une adresse IP autorisée, assurez-vous qu'il s'agit bien de l'adresse IP sécurisée.

Pour ajouter la connexion d'un ordinateur autorisé depuis le journal des événements entrants :

1. Vérifiez que l'onglet du menu Avancé est activé. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Internet et réseau**, puis sur **Evénements entrants**.
4. Dans le volet Evénements entrants, sélectionnez une adresse IP source, puis cliquez sur **Autoriser cette adresse**.
5. Dans la boîte de dialogue Ajouter une règle d'adresse IP autorisée, cliquez sur **Oui** pour confirmer que vous autorisez l'adresse IP.

   L'adresse IP récemment ajoutée apparaît sous **Adresses IP autorisées**.

Rubriques connexes

- Consignation des événements (page 166)

Modification d'une connexion fiable à un ordinateur

Vous pouvez utiliser le pare-feu pour modifier une connexion fiable à un ordinateur et l'adresse IP qui lui est associée.

Les ordinateurs associés à des adresses IP autorisées peuvent toujours se connecter à votre ordinateur. Avant d'ajouter, de modifier ou de supprimer une adresse IP autorisée, assurez-vous qu'il s'agit bien de l'adresse IP sécurisée.

Pour modifier une connexion fiable à un ordinateur :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
3. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP autorisées**.
4. Sélectionnez une adresse IP, puis cliquez sur **Modifier**.
5. Sous **Ajouter une règle d'adresse IP autorisée**, vous pouvez soit :
   - Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.
   - Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.
6. Le cas échéant, cochez la case **La règle expire dans**, puis entrez le nombre de jours pendant lesquels la règle doit être appliquée.
7. Eventuellement, entrez une description de cette règle.
8. Cliquez sur **OK**.

   L'adresse IP modifiée apparaît sous **Adresses IP autorisées**.

Suppression d'une connexion fiable à un ordinateur

Vous pouvez utiliser le pare-feu pour supprimer une connexion fiable à un ordinateur et l'adresse IP qui lui est associée.

Les ordinateurs associés à des adresses IP autorisées peuvent toujours se connecter à votre ordinateur. Avant d'ajouter, de modifier ou de supprimer une adresse IP autorisée, assurez-vous qu'il s'agit bien de l'adresse IP sécurisée.

Pour supprimer une connexion fiable à un ordinateur :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
3. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP autorisées**.
4. Sélectionnez une adresse IP, puis cliquez sur **Supprimer**.
5. Dans la boîte de dialogue **Adresses IP autorisées et interdites**, cliquez sur **Oui** pour confirmer que vous souhaitez supprimer l'adresse IP fiable figurant dans la liste **Adresses IP autorisées**

Interdiction de connexions informatiques

Vous pouvez ajouter, modifier ou supprimer des adresses IP fiables dans le volet Adresses IP autorisées et interdites, sous **Adresses IP interdites**.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Ajout d'une connexion interdite à un ordinateur

Vous pouvez utiliser le pare-feu pour ajouter une connexion interdite à un ordinateur et l'adresse IP qui lui est associée.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Pour ajouter une connexion interdite à un ordinateur :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
3. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP interdites**.
4. Cliquez sur **Ajouter**.
5. Sous Ajouter une règle d'adresse IP interdite, vous pouvez soit :
   - Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.
   - Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.
6. Le cas échéant, cochez la case **La règle expire dans**, puis entrez le nombre de jours pendant lesquels la règle doit être appliquée.
7. Eventuellement, entrez une description de cette règle.
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue **Ajouter une règle d'adresse IP interdite**, cliquez sur **Oui** pour confirmer que vous souhaitez ajouter la connexion interdite à un ordinateur.

   L'adresse IP récemment ajoutée apparaît sous **Adresses IP interdites**.

Modification d'une connexion interdite à un ordinateur

Vous pouvez utiliser le pare-feu pour modifier une connexion interdite à un ordinateur et l'adresse IP qui lui est associée.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Pour modifier une connexion interdite à un ordinateur :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
3. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP interdites**.
4. Sélectionnez une adresse IP, puis cliquez sur **Modifier**.
5. Sous **Ajouter une règle d'adresse IP autorisée**, vous pouvez soit :
   - Sélectionner **Une seule adresse IP**, puis entrer l'adresse IP voulue.
   - Sélectionner un **Intervalle d'adresses IP**, puis entrer les adresses IP de début et de fin dans les champs **De l'adresse IP** et **A l'adresse IP**.
6. Le cas échéant, cochez la case **La règle expire dans**, puis entrez le nombre de jours pendant lesquels la règle doit être appliquée.
7. Eventuellement, entrez une description de cette règle.

   Cliquez sur **OK**. L'adresse IP modifiée apparaît sous **Adresses IP interdites**.

Suppression d'une connexion interdite à un ordinateur

Vous pouvez utiliser le pare-feu pour supprimer une connexion interdite à un ordinateur et l'adresse IP qui lui est associée.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Pour supprimer une connexion interdite à un ordinateur :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Adresses IP autorisées et interdites**.
3. Dans le volet Adresses IP autorisées et interdites, sélectionnez **Adresses IP interdites**.
4. Sélectionnez une adresse IP, puis cliquez sur **Supprimer**.
5. Dans la boîte de dialogue **Adresses IP autorisées et interdites**, cliquez sur **Oui** pour confirmer que vous souhaitez supprimer l'adresse IP figurant dans la liste **Adresses IP interdites**

Interdiction d'un ordinateur depuis le journal des événements entrants

Vous pouvez interdire la connexion d'un ordinateur et l'adresse IP associée dans le journal des événements entrants.

Les adresses IP figurant dans le journal des événements entrants sont bloquées. Par conséquent, l'interdiction d'une adresse ne vous apporte aucune protection supplémentaire, sauf si votre ordinateur utilise des ports délibérément ouverts ou comporte un programme autorisé à accéder à Internet.

Ajoutez une adresse IP à votre liste **Adresses IP interdites** uniquement si un ou plusieurs ports sont délibérément ouverts et que vous avez de bonnes raisons pour souhaiter empêcher cette adresse d'accéder aux ports ouverts.

Vous pouvez utiliser la page Événements entrants, qui répertorie les adresses IP de l'ensemble du trafic Internet entrant, pour interdire une adresse IP que vous suspectez être la source d'activités Internet suspectes ou indésirables.

Pour interdire la connexion d'un ordinateur autorisé dans le journal des événements entrants :

1. Vérifiez que l'onglet du menu Avancé est activé. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Internet et réseau**, puis sur **Evénements entrants**.
4. Dans le volet Evénements entrants, sélectionnez une adresse IP source, puis cliquez sur **Interdire cette adresse**.
5. Dans la boîte de dialogue **Ajouter une règle d'adresse IP interdite**, cliquez sur **Oui** pour confirmer que vous souhaitez interdire l'adresse IP.

   L'adresse IP récemment ajoutée apparaît sous **Adresses IP interdites**.

Rubriques connexes

- Consignation des événements (page 166)

Interdiction d'un ordinateur depuis le journal des événements de détection des intrusions

Vous pouvez interdire la connexion d'un ordinateur et l'adresse IP associée depuis le journal des événements de détection des intrusions.

Vous pouvez faire en sorte que les ordinateurs associés à des adresses IP inconnues, suspectes ou non fiables ne puissent pas se connecter à votre ordinateur.

Firewall bloquant tout le trafic indésirable, l'interdiction d'une adresse IP n'est en règle générale pas nécessaire. Vous ne devez interdire une adresse IP que si vous êtes certain que cette connexion Internet représente une menace. Assurez-vous de ne bloquer aucune adresse IP importante, comme votre serveur DNS ou DHCP, ou d'autres serveurs de votre fournisseur d'accès Internet. En fonction des paramètres de sécurité définis sur votre ordinateur, Firewall peut vous prévenir s'il détecte un événement provenant d'une adresse IP interdite.

Pour interdire la connexion d'un ordinateur depuis le journal des événements de détection des intrusions :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Internet et réseau**, puis sur **Evénements de détection des intrusions**.
4. Dans le volet Evénements de détection des intrusions, sélectionnez une adresse IP source, puis cliquez sur **Interdire cette adresse**.
5. Dans la boîte de dialogue **Ajouter une règle d'adresse IP interdite**, cliquez sur **Oui** pour confirmer que vous souhaitez interdire l'adresse IP.

   L'adresse IP récemment ajoutée apparaît sous **Adresses IP interdites**.

Rubriques connexes

- Consignation des événements (page 166)

CHAPITRE 23

Consignation, surveillance et analyse

Firewall fournit des informations abondantes et faciles à consulter concernant la consignation, la surveillance et l'analyse des événements et du trafic Internet. Mieux vous comprendrez le trafic et les événements Internet, mieux vous pourrez gérer vos connexions Internet.

Contenu de ce chapitre

Consignation des événements

Le pare-feu vous permet de spécifier si vous souhaitez activer ou désactiver la consignation des événements et, lorsque cette fonction est activée, les types d'événements à consigner. La consignation des événements vous permet de visualiser les événements entrants et sortants qui se sont produits récemment. Vous pouvez également visualiser les événements d'intrusion détectés.

Configuration des paramètres du journal d'événements

Pour suivre les événements et l'activité du pare-feu, vous pouvez spécifier et configurer les types d'événement devant s'afficher.

Pour configurer la consignation des événements :

1. Dans le volet Internet & Configuration réseau, cliquez sur **Avancé**.
2. Dans le volet Pare-feu, cliquez sur **Paramètres du journal d'événements**.
3. Dans le volet Paramètres du journal d'événements, effectuez l'une des actions suivantes :
   - Sélectionnez **Consigner l'événement** pour activer la consignation des événements.
   - Sélectionnez **Ne pas consigner l'événement** pour désactiver la consignation des événements.
4. Sous **Paramètres du journal d'événements**, spécifiez les types d'événement à consigner. Les types d'événement sont les suivants :
   - Requêtes ping ICMP
   - Trafic en provenance des adresses IP interdites
   - Evénements sur des ports de service système
   - Evénements sur des ports inconnus
   - Evénements de détection des intrusions (IDS)
5. Pour empêcher la consignation sur des ports spécifiques, sélectionnez **Ne pas consigner les événements sur les ports suivants**, puis entrez des numéros de port séparés par des virgules ou bien des plages de ports en les séparant par des tirets. Exemple : `137-139, 445, 400-5000`.
6. Cliquez sur **OK**.

Affichage des événements récents

Si la consignation est activée, vous pouvez afficher les événements récents. Le volet Evénements récents présente la date et la description de l'événement. Il affiche uniquement l'activité des programmes dont l'accès à Internet est explicitement bloqué.

Pour afficher les événements récents de Firewall :

- Dans **Menu avancé**, sous le volet Tâches courantes, cliquez sur **Rapports & Journaux** ou **Afficher les événements récents**. Vous pouvez également cliquer sur **Afficher les événements récents** sous le volet Tâches courantes du Menu de base.

Affichage des événements entrants

Si la consignation est activée, vous pouvez afficher et trier les événements entrants.

Le journal des événements entrants comprend les catégories d'information suivantes :

- Date et heure
- Adresse IP source
- Nom d'hôte
- Type d'information et d'événement

Pour afficher les événements entrants de votre pare-feu :

1. Vérifiez que l'onglet du menu Avancé est activé. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Internet et réseau**, puis sur **Evénements entrants**.

Remarque : depuis le journal des événements entrants, vous pouvez autoriser, interdire et suivre une adresse IP.

Rubriques connexes

- Ajout d'un ordinateur autorisé depuis le journal des événements entrants (page 156)
- Interdiction d'un ordinateur depuis le journal des événements entrants (page 163)
- Suivi d'un ordinateur depuis le journal des événements entrants (page 173)

Affichage des événements sortants

Si la consignation est activée, vous pouvez afficher les événements sortants. Les événements sortants comprennent le nom du programme à l'origine d'une tentative d'accès sortant, la date et l'heure de l'événement et l'emplacement du programme sur votre ordinateur.

Pour afficher les événements sortants de votre pare-feu :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Sélectionnez **Internet et réseau**, puis **Evénements sortants**.

Remarque : vous pouvez accorder un accès total ou un accès uniquement sortant dans le journal des événements sortants. Vous pouvez également trouver des informations supplémentaires concernant le programme.

Rubriques connexes

- Octroi d'un accès total depuis le journal des événements sortants (page 140)
- Octroi d'un accès uniquement sortant depuis le journal des événements sortants (page 142)
- Accès aux informations d'un programme depuis le journal des événements sortants (page 148)

Affichage des événements de détection des intrusions

Si la consignation est activée, vous pouvez afficher les événements entrants. Les événements de détection d'intrusion indiquent la date et l'heure de l'événement ainsi que l'adresse IP source et le nom d'hôte associés. Le journal décrit en outre le type d'événement.

Pour afficher les événements de détection des intrusions :

1. Dans le volet Tâches courantes, cliquez sur **Rapports & Journaux**.
2. Sous Evénements récents, cliquez sur **Afficher le journal**.
3. Cliquez sur **Internet & Réseau**, puis sur **Evénements de détection des intrusions**.

Remarque : depuis le journal des événements de détection des intrusions, vous pouvez interdire et suivre une adresse IP.

Rubriques connexes

- Interdiction d'un ordinateur depuis le journal des événements de détection des intrusions (page 164)
- Suivi d'un ordinateur depuis le journal des événements de détection des intrusions (page 174)

Utilisation des statistiques

Firewall utilise HackerWatch, le site Web de sécurité de McAfee, pour obtenir et vous fournir des statistiques relatives aux événements de sécurité et à l'activité des ports sur l'ensemble d'Internet.

Afficher les statistiques générales des événements de sécurité

HackerWatch surveille les événements de sécurité Internet survenant dans le monde entier et vous permet d'en prendre connaissance sur SecurityCenter. Les informations recueillies concernent des incidents enregistrés par HackerWatch au cours des dernières 24 heures, et des 7 et 30 derniers jours.

Pour consulter les statistiques générales de sécurité :

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **HackerWatch**.
3. Consultez les statistiques des événements de sécurité sous **Suivi des événements**.

Consulter l'activité générale des ports Internet

HackerWatch surveille les événements de sécurité Internet survenant dans le monde entier et vous permet d'en prendre connaissance sur SecurityCenter. Les informations affichées concernent notamment les principaux ports pour lesquels des événements ont été communiqués à HackerWatch au cours des sept derniers jours. En général, les informations affichées concernent les ports HTTP, TCP et UDP.

Pour consulter l'activité générale des ports dans le monde :

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **HackerWatch**.
3. Consultez les événements des principaux ports sous **Activité récente des ports**.

Suivi du trafic Internet

Firewall propose plusieurs options pour suivre le trafic Internet. Ces options vous permettent de suivre géographiquement un ordinateur en réseau, d'obtenir des informations relatives au domaine et au réseau et de retrouver des ordinateurs à partir de journaux Evénements entrants et Evénements de détection des intrusions.

Suivre géographiquement un ordinateur en réseau

Vous pouvez utiliser le traceur visuel pour localiser géographiquement un ordinateur qui se connecte ou tente de se connecter au vôtre, et ce, en utilisant son nom ou son adresse IP. Le traceur visuel vous permet également d'accéder aux informations relatives au réseau et à l'enregistrement de l'ordinateur. Lorsque vous exécutez le traceur visuel, une carte du monde s'affiche et indique l'itinéraire le plus probable des données entre l'ordinateur source et le vôtre.

Pour localiser géographiquement un ordinateur :

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Traceur visuel**.
3. Saisissez l'adresse IP de l'ordinateur et cliquez sur **Rechercher**.
4. Sous **Traceur visuel**, sélectionnez **Vue de la carte**.

Remarque : vous ne pouvez pas effectuer le traçage d'événements sur une adresse IP en boucle, privée ou non valide.

Obtenir des informations concernant l'enregistrement d'un ordinateur

Le traceur visuel vous permet d'extraire de SecurityCenter des informations relatives à l'enregistrement d'un ordinateur. Il s'agit notamment du nom de domaine de celui-ci, des nom et adresse de l'abonné et du contact administratif.

Pour obtenir des informations relatives au domaine d'un ordinateur :

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Traceur visuel**.
3. Saisissez l'adresse IP de l'ordinateur, puis cliquez sur **Rechercher**.
4. Sous **Traceur visuel**, sélectionnez **Vue de l'abonné**.

Obtention d'informations concernant le réseau d'un ordinateur

Le traceur visuel vous permet d'extraire de SecurityCenter des informations relatives au réseau d'un ordinateur. Il s'agit notamment d'indications sur le réseau de domiciliation du domaine.

Pour obtenir des informations relatives au réseau d'un ordinateur :

1. Vérifiez que l'onglet Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Traceur visuel**.
3. Saisissez l'adresse IP de l'ordinateur, puis cliquez sur **Rechercher**.
4. Sous **Traceur visuel**, sélectionnez **Vue du réseau**.

Suivi d'un ordinateur depuis le journal des événements entrants

Dans le volet Evénements entrants, vous pouvez suivre une adresse IP figurant dans le journal des événements entrants.

Pour suivre l'adresse IP d'un ordinateur depuis le journal des événements entrants :

1. Vérifiez que l'onglet du menu Avancé est activé. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Internet et réseau**, puis sur **Evénements entrants**.
4. Dans le volet Evénements entrants, sélectionnez une adresse IP source, puis cliquez sur **Tracer cette adresse**.
5. Dans le volet Traceur visuel, effectuez l'une des actions suivantes :
   - **Vue de la carte** : localisez géographiquement un ordinateur à l'aide de l'adresse IP sélectionnée.
   - **Vue de l'abonné** : localisez les informations de domaine au moyen de l'adresse IP sélectionnée.
   - **Vue du réseau** : localisez les informations de réseau au moyen de l'adresse IP sélectionnée.
6. Lorsque vous avez fini, cliquez sur **Terminé**.

Rubriques connexes

- Suivi du trafic Internet (page 171)
- Afficher les événements entrants (page 167)

Suivre un ordinateur depuis le journal des événements de détection des intrusions

Dans le volet Evénements de détection des intrusions, vous pouvez suivre une adresse IP figurant dans le journal des événements de détection des intrusions.

Pour suivre l'adresse IP d'un ordinateur depuis le journal des événements de détection des intrusions :

1. Dans le volet Tâches courantes, cliquez sur **Rapports et journaux**.
2. Sous **Evénements récents**, cliquez sur **Afficher le journal**.
3. Cliquez sur **Internet et réseau**, puis sur **Evénements de détection des intrusions**.Dans le volet Evénements de détection des intrusions, sélectionnez une adresse IP source, puis cliquez sur **Tracer cette adresse**.
4. Dans le volet Traceur visuel, effectuez l'une des actions suivantes :
   - **Vue de la carte** : localisez géographiquement un ordinateur à l'aide de l'adresse IP sélectionnée.
   - **Vue de l'abonné** : localisez les informations de domaine au moyen de l'adresse IP sélectionnée.
   - **Vue du réseau** : localisez les informations de réseau au moyen de l'adresse IP sélectionnée.
5. Lorsque vous avez fini, cliquez sur **Terminé**.

Rubriques connexes

- Suivi du trafic Internet (page 171)
- Consignation, surveillance et analyse (page 165)

Suivi d'une adresse IP surveillée

Vous pouvez suivre une adresse IP surveillée afin d'obtenir une vue géographique indiquant l'itinéraire le plus probable des données entre l'ordinateur source et le vôtre. De plus, vous pouvez obtenir des informations d'enregistrement et de réseau concernant l'adresse IP.

Pour surveiller l'utilisation de la bande passante par les programmes :

1. Vérifiez que le Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Moniteur de trafic**.
3. Sous **Moniteur de trafic**, cliquez sur **Programmes actifs**.
4. Sélectionnez un programme, puis l'adresse IP apparaissant sous le nom du programme.
5. Sous **Activité du programme**, cliquez sur **Tracer cette adresse IP**.
6. Sous **Traceur visuel**, vous pouvez voir une carte indiquant l'itinéraire le plus probable des données entre l'ordinateur source et le vôtre. De plus, vous pouvez obtenir des informations d'enregistrement et de réseau concernant l'adresse IP.

Remarque : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Traceur visuel**.

Rubriques connexes

- Surveillance du trafic Internet (page 176)

Surveillance du trafic Internet

Firewall fournit diverses méthodes pour surveiller votre trafic Internet, et notamment :

- **Graphique d'analyse du trafic** : présente le trafic Internet entrant et sortant récent.
- **Graphique d'utilisation du trafic** : indique le pourcentage de bande passante utilisé par les programmes les plus actifs au cours des dernières 24 heures.
- **Programmes actifs** : indique les programmes qui utilisent actuellement le plus de connexions réseau sur votre ordinateur, ainsi que les adresses IP auxquelles ils accèdent.

A propos du graphique d'analyse du trafic

Le graphique Analyse du trafic est une représentation graphique et numérique du trafic Internet entrant et sortant. De plus, le Moniteur de trafic indique les programmes qui utilisent le plus grand nombre de connexions réseau sur votre ordinateur, ainsi que les adresses IP auxquelles ils accèdent.

Le volet Analyse du trafic présente le trafic Internet entrant et sortant récent, ainsi que les débits de transfert actuels, moyens et maximum. Vous pouvez également consulter le volume du trafic, y compris le volume depuis que vous avez démarré Firewall et le trafic total du mois en cours et du mois précédent.

Le volet Analyse du trafic présente l'activité Internet en temps réel de votre ordinateur, y compris le volume et le débit du trafic Internet entrant et sortant récent de votre ordinateur, ainsi que la vitesse de connexion et le nombre total d'octets transférés sur Internet.

La ligne verte continue représente le débit de transfert actuel du trafic entrant. La ligne pointillée verte représente le débit de transfert moyen du trafic entrant. Si le débit actuel et le débit moyen sont identiques, la ligne pointillée ne figure pas sur le graphique. La ligne continue reflète alors les débits moyen et actuel.

La ligne continue rouge représente le débit actuel du trafic sortant. La ligne pointillée rouge représente le débit moyen du trafic sortant. Si le débit actuel et le débit moyen sont identiques, la ligne pointillée ne figure pas sur le graphique. La ligne continue reflète alors les débits moyen et actuel.

Rubriques connexes

- Analyser le trafic entrant et sortant (page 177)

Analyse du trafic entrant et sortant

Le graphique Analyse du trafic est une représentation graphique et numérique du trafic Internet entrant et sortant. De plus, le Moniteur de trafic indique les programmes qui utilisent le plus grand nombre de connexions réseau sur votre ordinateur, ainsi que les adresses IP auxquelles ils accèdent.

Pour analyser le trafic entrant et sortant :

1. Vérifiez que le Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Moniteur de trafic**.
3. Sous **Moniteur de trafic**, cliquez sur **Analyse du trafic**.

Conseil : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Analyse du trafic**.

Rubriques connexes

- A propos du graphique d'analyse du trafic (page 176)

Surveillance de la bande passante utilisée par les programmes

Vous pouvez afficher le graphique à secteurs, qui présente le pourcentage approximatif de bande passante utilisé par les programmes les plus actifs sur votre ordinateur au cours des dernières vingt-quatre heures. Ce graphique à secteurs représente visuellement les quantités relatives de bande passante utilisées par les programmes.

Pour surveiller l'utilisation de la bande passante par les programmes :

1. Vérifiez que le Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Moniteur de trafic**.
3. Sous **Moniteur de trafic**, cliquez sur **Utilisation du trafic**.

Conseil : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Utilisation du trafic**.

Surveillance de l'activité des programmes

Vous pouvez afficher l'activité entrante et sortante des programmes, y compris les connexions et ports des ordinateurs distants.

Pour surveiller l'utilisation de la bande passante par les programmes :

1. Vérifiez que le Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **Moniteur de trafic**.
3. Sous **Moniteur de trafic**, cliquez sur **Programmes actifs**.
4. Vous pouvez afficher les informations suivantes :
   - Graphique d'activité du programme : sélectionnez le programme dont vous souhaitez afficher le graphique d'activité.
   - Connexion à l'écoute : sélectionnez un élément sous le nom du programme.
   - Connexion de l'ordinateur : sélectionnez une adresse IP sous le nom du programme, le processus système ou le service.

Remarque : pour consulter les statistiques les plus récentes, cliquez sur **Actualiser** sous **Programmes actifs**.

CHAPITRE 24

Obtention d'informations sur la sécurité Internet

Firewall utilise HackerWatch, le site Web de sécurité de McAfee, pour fournir des informations actualisées concernant les programmes et l'activité générale d'Internet. HackerWatch fournit également un didacticiel HTML concernant Firewall.

Contenu de ce chapitre

Lancement du didacticiel HackerWatch

Pour en savoir plus sur Firewall, vous pouvez accéder au didacticiel HackerWatch depuis SecurityCenter.

Pour lancer le didacticiel HackerWatch :

1. Vérifiez que le Menu avancé est activé, puis cliquez sur **Outils**.
2. Dans le volet Outils, cliquez sur **HackerWatch**.
3. Sous **Ressources HackerWatch**, cliquez sur **Afficher le didacticiel**.

CHAPITRE 25

McAfee EasyNetwork

McAfee® EasyNetwork sécurise le partage des fichiers, simplifie les transferts de fichiers et automatise le partage d'imprimantes entre les ordinateurs de votre réseau domestique.

Avant de commencer à utiliser EasyNetwork, nous vous conseillons de vous familiariser avec ses principales fonctionnalités. Pour plus de détails sur la configuration et l'utilisation de ces fonctionnalités, consultez l'aide de EasyNetwork.

Contenu de ce chapitre

Caractéristiques

EasyNetwork propose les fonctionnalités suivantes :

Partage de fichiers

Grâce à EasyNetwork, il est facile de partager des fichiers depuis votre ordinateur vers d'autres ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs affiliés au réseau géré (c'est-à-dire ceux qui ont un accès complet ou administratif) peuvent partager des fichiers ou accéder à des fichiers partagés par d'autres ordinateurs affiliés.

Transfert de fichiers

Vous pouvez envoyer des fichiers à d'autres ordinateurs qui sont affiliés au réseau géré. Lorsque vous recevez un fichier, il apparaît dans votre boîte de réception EasyNetwork. La boîte de réception est un emplacement de stockage temporaire pour tous les fichiers que vous envoyez à d'autres ordinateurs sur le réseau.

Partage d'imprimantes automatique

Lorsque vous vous affiliez au réseau géré, EasyNetwork partage automatiquement toutes les imprimantes locales reliées à votre ordinateur, et utilise le nom actuel de l'imprimante comme nom d'imprimante partagée. L'application détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de configurer et d'utiliser ces imprimantes.

CHAPITRE 26

Configuration de EasyNetwork

Pour pouvoir utiliser les fonctionnalités de EasyNetwork, vous devez d'abord lancer le programme et vous affilier au réseau géré. Vous pourrez ensuite quitter le réseau à tout moment.

Contenu de ce chapitre

Lancement de l'application EasyNetwork

Par défaut, le système vous invite à lancer EasyNetwork immédiatement après l'installation, mais vous pouvez également lancer l'application ultérieurement.

Lancement de l'application EasyNetwork

Par défaut, le système vous invite à lancer EasyNetwork immédiatement après l'installation, mais vous pouvez également lancer l'application ultérieurement.

Pour lancer EasyNetwork :

- Dans le menu **Démarrer**, pointez le curseur de la souris sur **Tous les programmes**, puis sur **McAfee** et cliquez sur **McAfee EasyNetwork**.

Conseil : si vous avez demandé que des icônes de l'application soient créées pour le bureau et la zone de lancement rapide lors de l'installation, vous pouvez également double-cliquer sur l'icône McAfee EasyNetwork du bureau ou cliquer sur l'icône McAfee EasyNetwork de la zone de notification située à droite de la barre des tâches pour lancer EasyNetwork.

Affiliation à un réseau géré

Lorsque vous installez SecurityCenter, un agent réseau est installé sur votre ordinateur et s'exécute en arrière-plan. Dans le cas de EasyNetwork, l'agent réseau est chargé de détecter une connexion réseau valide, de détecter des imprimantes locales à partager et de surveiller l'état du réseau.

Si aucun autre ordinateur exécutant cet agent réseau n'est détecté sur le réseau auquel vous êtes actuellement connecté, vous êtes automatiquement affilié à ce réseau et êtes invité à indiquer si le réseau est fiable. Dans la mesure où votre ordinateur est le premier à être affilié au réseau, son nom est intégré à celui du réseau. Toutefois, vous pouvez modifier le nom du réseau à tout moment.

Lorsqu'un ordinateur se connecte au réseau, une demande d'affiliation est envoyée à tous les autres ordinateurs présents sur le réseau. La demande peut être accordée par tout ordinateur du réseau possédant des droits d'administration. Celui-ci peut également définir le niveau d'autorisation du nouvel ordinateur affilié au réseau : invité (possibilité de transférer des fichiers uniquement) ou accès complet ou d'administration (possibilité de transférer des fichiers et de les partager), par exemple. Avec EasyNetwork, les ordinateurs possédant des droits d'administration peuvent autoriser l'accès d'autres ordinateurs et gérer leurs autorisations (c'est-à-dire favoriser ou empêcher l'accès des ordinateurs) ; les ordinateurs bénéficiant d'un accès complet ne peuvent pas effectuer ces tâches administratives. Un contrôle de sécurité est effectué avant d'autoriser l'accès à l'ordinateur.

Remarque : après vous être connecté, si d'autres programmes réseau McAfee sont installés (McAfee Wireless Network Security ou Network Manager, par exemple), l'ordinateur est également reconnu comme étant un ordinateur géré pour ces programmes. Le niveau d'autorisation affecté à un ordinateur s'applique à tous les programmes réseau McAfee. Pour obtenir des informations sur la signification des autorisations de type Invité, Complet ou Administration dans un autre programme réseau McAfee, reportez-vous à sa documentation.

Affiliation au réseau

Lorsqu'un ordinateur se connecte à un réseau fiable pour la première fois après l'installation de EasyNetwork, un message d'invite s'affiche, vous proposant de vous affilier au réseau géré. Si vous acceptez, une demande est envoyée à tous les ordinateurs du réseau ayant des droits d'administration. Cette demande doit être accordée pour que l'ordinateur puisse partager des imprimantes ou des fichiers, ou encore envoyer et copier des fichiers sur le réseau. Si l'ordinateur est le premier à s'affilier au réseau, des autorisations de type Administration lui sont automatiquement attribuées.

Pour s'affilier au réseau :

1. Dans la fenêtre Fichiers partagés, cliquez sur **Oui, je souhaite me connecter à ce réseau maintenant**. Lorsqu'un ordinateur du réseau qui possède des droits d'administration vous accorde l'accès, un message s'affiche, vous demandant si vous souhaitez autoriser cet ordinateur et les autres ordinateurs présents sur le réseau à gérer les paramètres de sécurité les uns des autres.
2. Si vous souhaitez accorder cette autorisation, cliquez sur **Oui**. Dans le cas contraire, cliquez sur **Non**.
3. Vérifiez que l'ordinateur qui a autorisé l'accès affiche les cartes à jouer suivantes dans la boîte de dialogue de confirmation de sécurité, puis cliquez sur **Confirmer**.

Remarque : si ce n'est pas le cas, cela signifie que le réseau géré est victime d'une faille de sécurité. Le fait de vous affilier au réseau risque de compromettre la sécurité de votre ordinateur. Par conséquent, nous vous conseillons de cliquer sur **Refuser** dans la boîte de dialogue de confirmation de la sécurité.

Autorisation d'accès au réseau

Lorsqu'un ordinateur demande à être affilié au réseau géré, un message est envoyé aux autres ordinateurs du réseau possédant des droits d'administration. Le premier ordinateur à répondre au message devient l'administrateur de droits d'accès. L'administrateur de droits d'accès doit définir le type d'accès à accorder à l'ordinateur : invité, complet ou administratif.

Pour accorder l'accès au réseau :

1. Lors de l'alerte, cochez l'une des cases suivantes :
   - **Autoriser l'accès à un invité** : en tant qu'invité, l'utilisateur est autorisé à envoyer des fichiers à d'autres ordinateurs, mais pas à partager des fichiers.

- **Accorder un accès complet à toutes les applications du réseau géré** : ce niveau d'autorisation permet à l'utilisateur d'envoyer et de partager des fichiers.
- **Accorder un accès administratif à toutes les applications du réseau géré** : ce niveau d'autorisation permet à l'utilisateur d'envoyer et de partager des fichiers, d'accorder l'accès à d'autres ordinateurs et de modifier les niveaux d'autorisation des autres ordinateurs.

2 Cliquez sur **Autoriser l'accès**.

3 Vérifiez que l'ordinateur affiche les cartes à jouer suivantes dans la boîte de dialogue de confirmation de sécurité, puis cliquez sur **Confirmer**.

Remarque : si ce n'est pas le cas, cela signifie que le réseau géré est victime d'une faille de sécurité. Le fait d'autoriser l'accès de cet ordinateur au réseau risque de compromettre la sécurité de votre ordinateur. Par conséquent, nous vous conseillons de cliquer sur **Refuser** dans la boîte de dialogue de confirmation de sécurité.

Attribution d'un nouveau nom au réseau

Par défaut, le nom du réseau inclut celui du premier ordinateur à s'être affilié. Toutefois, vous pouvez modifier ce nom à tout moment. Lorsque vous modifiez le nom du réseau, vous modifiez la description du réseau affichée dans EasyNetwork.

Pour renommer le réseau :

1. Dans le menu **Options**, cliquez sur **Configurer**.
2. Dans la boîte de dialogue Configurer, saisissez le nom du réseau dans la zone **Nom du réseau**.
3. Cliquez sur **OK**.

Comment quitter un réseau géré

Si vous vous affiliez à un réseau géré et si vous décidez par la suite que vous ne souhaitez plus en faire partie, vous pouvez quitter le réseau. Une fois que vous avez annulé votre affiliation, vous pouvez revenir en arrière à tout moment. En revanche, vous devrez à nouveau demander une autorisation d'affiliation et effectuer le contrôle de sécurité. Pour plus d'informations, reportez-vous à Affiliation à un réseau géré (page 185).

Comment quitter un réseau géré

Vous pouvez quitter un réseau géré auquel vous êtes affilié.

Pour quitter un réseau géré :

1. Dans le menu **Outils**, cliquez sur **Quitter le réseau**.
2. Dans la boîte de dialogue Quitter le réseau, sélectionnez le nom du réseau que vous souhaitez quitter.
3. Cliquez sur **Quitter le réseau**.

CHAPITRE 27

Partage et envoi des fichiers

Grâce à EasyNetwork, il est facile de partager et d'envoyer des fichiers depuis votre ordinateur vers d'autres ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs affiliés au réseau géré (c'est-à-dire ceux qui ont un accès complet ou administratif) peuvent partager des fichiers ou accéder à des fichiers partagés par d'autres ordinateurs affiliés.

Contenu de ce chapitre

Partage de fichiers

Grâce à EasyNetwork, il est facile de partager des fichiers depuis votre ordinateur vers d'autres ordinateurs du réseau. Lorsque vous partagez des fichiers, vous donnez aux autres ordinateurs un accès en lecture seule à ces fichiers. Seuls les ordinateurs affiliés au réseau géré (c'est-à-dire ceux qui ont un accès complet ou administratif) peuvent partager des fichiers ou accéder à des fichiers partagés par d'autres ordinateurs affiliés. Lorsque vous partagez un dossier, vous partagez tous les fichiers contenus dans ce dossier et ses sous-dossiers. En revanche, les fichiers qui sont ajoutés au dossier par la suite ne sont pas automatiquement partagés. Si un fichier ou un dossier partagé est supprimé, il est automatiquement supprimé de la fenêtre Fichiers partagés. Vous pouvez mettre fin au partage de fichiers à tout moment.

Vous avez deux moyens d'accéder à un fichier partagé : en ouvrant le fichier directement à partir de EasyNetwork ou en copiant le fichier sur votre ordinateur et en l'ouvrant. Si la liste de vos fichiers partagés est trop longue, vous pouvez effectuer une recherche du/des fichier(s) partagé(s) au(x)quel(s) vous souhaitez accéder.

Remarque : les autres ordinateurs ne peuvent pas utiliser l'Explorateur Windows pour accéder aux fichiers partagés à l'aide de EasyNetwork. Le partage des fichiers EasyNetwork s'effectue via des connexions sécurisées.

Partage d'un fichier

Lorsque vous partagez un fichier, il est automatiquement mis à la disposition de tous les autres ordinateurs affiliés ayant un accès complet ou administratif au réseau géré.

Pour partager un fichier :

1. Dans l'Explorateur Windows, recherchez le fichier que vous souhaitez partager.
2. Faites glisser le fichier depuis son emplacement dans l'Explorateur Windows vers la fenêtre Fichiers partagés de EasyNetwork.

Conseil : pour partager un fichier, vous pouvez également cliquer sur **Partager les fichiers** dans le menu **Outils**. Dans la boîte de dialogue Partager, recherchez le dossier contenant le fichier que vous souhaitez partager, sélectionnez-le, puis cliquez sur **Partager**.

Fin de partage d'un fichier

Si vous partagez un fichier sur le réseau géré, vous pouvez mettre fin au partage à tout moment. Lorsque vous cessez de partager un fichier, les autres ordinateurs affiliés au réseau géré ne peuvent plus y accéder.

Pour mettre fin au partage d'un fichier :

1. Dans le menu **Outils**, cliquez sur **Arrêter de partager des fichiers**.
2. Dans la boîte de dialogue Arrêter de partager des fichiers, sélectionnez le fichier que vous ne souhaitez plus partager.
3. Cliquez sur **Ne pas partager**.

Copie d'un fichier partagé

Vous pouvez copier des fichiers partagés depuis n'importe quel ordinateur du réseau géré sur votre ordinateur. De cette façon, si l'ordinateur cesse de partager le fichier, vous en avez une copie à disposition.

Pour copier un fichier :

- Faites glisser le fichier depuis la fenêtre Fichiers partagés dans EasyNetwork vers un emplacement de l'Explorateur Windows ou vers le bureau Windows.

Conseil : pour copier un fichier partagé, vous pouvez également sélectionner le fichier dans EasyNetwork puis cliquer sur **Copier dans** dans le menu **Outils**. Dans la boîte de dialogue Copier dans le dossier, recherchez le dossier où vous souhaitez copier le fichier, sélectionnez-le et cliquez sur **Enregistrer**.

Recherche d'un fichier partagé

Vous pouvez rechercher un fichier qui a été partagé par vous-même ou par un autre ordinateur affilié au réseau. Au fur et à mesure que vous entrez vos critères de recherche, EasyNetwork affiche automatiquement les résultats correspondants dans la fenêtre Fichiers partagés.

Pour rechercher un fichier partagé :

1. Dans la fenêtre Fichiers partagés, cliquez sur **Rechercher**.
2. Cliquez sur l'une des options suivantes dans la liste **Contient** :
   - **Contient tous les mots** : la recherche porte sur les noms de fichiers ou de chemins qui contiennent tous les mots que vous spécifiez dans la liste **Nom de fichier ou de chemin**, quel que soit l'ordre des mots.

- **Contient certains mots** : la recherche porte sur les noms de fichiers ou de chemins qui contiennent au moins l'un des mots spécifiés dans la liste **Nom de fichier ou de chemin**.
- **Contient l'expression exacte** : la recherche porte sur les noms de fichiers ou de chemins qui contiennent l'expression exacte spécifiée dans la liste **Nom de fichier ou de chemin**.

3 Saisissez une partie ou la totalité du nom de fichier ou de chemin dans la liste **Nom de fichier ou de chemin**.

4 Cliquez sur l'un des types de fichiers suivants dans la liste **Type** :

- **Tous** : la recherche porte sur tous les types de fichiers partagés.
- **Document** : la recherche porte sur tous les documents partagés.
- **Image** : la recherche porte sur tous les fichiers image partagés.
- **Vidéo** : la recherche porte sur tous les fichiers vidéo partagés.
- **Audio** : la recherche porte sur tous les fichiers audio partagés.

5 Dans les listes **De** et **A**, cliquez sur les dates correspondant à la plage de dates au cours de laquelle le fichier a été créé.

Envoi de fichiers à d'autres ordinateurs

Vous pouvez envoyer des fichiers à d'autres ordinateurs qui sont affiliés au réseau géré. Avant d'envoyer un fichier, EasyNetwork confirme que l'ordinateur qui reçoit le fichier dispose d'un espace disque suffisant.

Lorsque vous recevez un fichier, il apparaît dans votre boîte de réception EasyNetwork. La boîte de réception est un emplacement de stockage temporaire pour tous les fichiers que vous envoyez à d'autres ordinateurs sur le réseau. Si votre application EasyNetwork est ouverte lorsque vous recevez un fichier, celui-ci apparaît instantanément dans votre boîte de réception ; sinon, un message s'affiche dans la zone de notification située à droite de la barre des tâches Windows. Si vous ne souhaitez pas recevoir de messages de notification, vous pouvez les désactiver. Si un fichier portant le même nom existe déjà dans la boîte de réception, le nouveau fichier est renommé avec un suffixe numérique. Les fichiers restent dans votre boîte de réception jusqu'à ce que vous les acceptiez (c'est-à-dire jusqu'à ce que vous les copiiez sur votre ordinateur).

Envoi d'un fichier à un autre ordinateur

Vous pouvez envoyer un fichier directement à un autre ordinateur présent sur le réseau géré sans pour autant le partager. Pour que l'utilisateur de l'ordinateur cible puisse voir le fichier, celui-ci doit être enregistré en local. Pour plus d'informations, reportez-vous à Acceptation d'un fichier provenant d'un autre ordinateur (page 196).

Pour envoyer un fichier à un autre ordinateur :

1. Dans l'Explorateur Windows, recherchez le fichier que vous souhaitez envoyer.
2. Faites glisser le fichier depuis son emplacement dans l'Explorateur Windows vers l'icône d'ordinateur actif de EasyNetwork.

Conseil : pour envoyer plusieurs fichiers à un ordinateur, appuyez sur Ctrl tout en sélectionnant les fichiers. Pour envoyer des fichiers, vous pouvez également cliquer sur **Envoyer** dans le menu **Outils**, sélectionner les fichiers puis cliquer sur **Envoyer**.

Acceptation d'un fichier provenant d'un autre ordinateur

Si un autre ordinateur du réseau géré vous envoie un fichier, vous devez l'accepter (en l'enregistrant dans un dossier de votre ordinateur). Si l'application EasyNetwork n'est pas ouverte ou au premier plan lorsque votre ordinateur reçoit un fichier, vous recevez un message de notification dans la zone située à droite de la barre des tâches. Cliquez sur ce message pour ouvrir EasyNetwork et accéder au fichier.

Pour recevoir un fichier d'un autre ordinateur :

- Cliquez sur **Reçu**, puis faites glisser le fichier de votre boîte de réception EasyNetwork vers un des dossiers de l'Explorateur Windows.

Conseil : pour recevoir un fichier d'un autre ordinateur, vous pouvez également sélectionner le fichier dans EasyNetwork puis cliquer sur **Accepter** dans le menu **Outils**. Dans la boîte de dialogue Accepter dans le dossier, recherchez le dossier où vous souhaitez enregistrer les fichiers, sélectionnez-le et cliquez sur **Enregistrer**.

Réception d'une notification lors de l'envoi d'un fichier

Vous pouvez recevoir une notification lorsqu'un autre ordinateur du réseau géré vous envoie un fichier. Si EasyNetwork n'est pas ouvert ou au premier plan sur votre bureau, un message de notification apparaît dans la zone située à droite de la barre des tâches Windows.

Pour recevoir une notification lors de l'envoi d'un fichier :

1. Dans le menu **Options**, cliquez sur **Configurer**.
2. Dans la boîte de dialogue Configurer, cochez la case **M'avertir lorsqu'un autre ordinateur m'envoie des fichiers**.
3. Cliquez sur **OK**.

CHAPITRE 28

Partage d'imprimantes

Lorsque vous vous affiliez à un réseau géré, EasyNetwork partage automatiquement toutes les imprimantes locales reliées à votre ordinateur. L'application détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de configurer et d'utiliser ces imprimantes.

Contenu de ce chapitre

Utilisation d'imprimantes partagées

Lorsque vous vous affiliez au réseau géré, EasyNetwork partage automatiquement toutes les imprimantes locales reliées à votre ordinateur, et utilise le nom actuel de l'imprimante comme nom d'imprimante partagée. L'application détecte également les imprimantes partagées par d'autres ordinateurs sur votre réseau et permet de configurer et d'utiliser ces imprimantes. Si vous avez configuré un pilote d'imprimante de manière à imprimer via un serveur d'impression du réseau (un serveur d'impression USB sans fil, par exemple), EasyNetwork considère qu'il s'agit d'une imprimante locale et la partage automatiquement sur le réseau. Vous pouvez également mettre fin au partage d'une imprimante à tout moment.

EasyNetwork détecte également les imprimantes partagées par tous les autres ordinateurs du réseau. Si l'application détecte une imprimante distante qui n'est pas encore connectée à votre ordinateur, le lien **Imprimantes réseau disponibles** apparaît dans la fenêtre Fichiers partagés lorsque vous ouvrez EasyNetwork pour la première fois. Vous pouvez ainsi installer des imprimantes disponibles ou désinstaller des imprimantes qui sont déjà connectées à votre ordinateur. Cela permet également d'actualiser la liste des imprimantes détectées sur le réseau.

Si vous n'êtes pas encore affilié au réseau géré mais si vous y êtes connecté, vous pouvez accéder aux imprimantes partagées depuis le panneau de commande Windows standard de l'imprimante.

Fin de partage d'une imprimante

Vous pouvez mettre fin au partage d'une imprimante à tout moment. Les ordinateurs affiliés sur lesquels l'imprimante est installée ne pourront plus imprimer dessus.

Pour mettre fin au partage d'une imprimante :

1. Dans le menu **Outils**, cliquez sur **Imprimantes**.
2. Dans la boîte de dialogue Gérer les imprimantes réseau, cliquez sur le nom de l'imprimante que vous ne souhaitez plus partager.
3. Cliquez sur **Ne pas partager**.

Installation d'une imprimante réseau disponible

En tant que membre du réseau géré, vous pouvez accéder aux imprimantes partagées sur le réseau. Pour cela, vous devez installer le pilote utilisé par l'imprimante. Si le propriétaire de l'imprimante cesse de la partager une fois que vous avez installé le pilote, vous ne pouvez plus imprimer sur cette imprimante.

Pour installer une imprimante réseau disponible :

1. Dans le menu **Outils**, cliquez sur **Imprimantes**.
2. Dans la boîte de dialogue Imprimantes réseau disponibles, cliquez sur le nom d'une imprimante.
3. Cliquez sur **Installer**.

CHAPITRE 29

Référence

Le glossaire répertorie et définit les termes de sécurité les plus utilisés dans les produits McAfee.

"A propos de McAfee" fournit des informations juridiques relatives à McAfee Corporation.

Glossaire

8

802.11

Ensemble de normes IEEE utilisées dans le cadre de la technologie des réseaux locaux sans fil. 802.11 qualifie une interface par liaison radio entre un client sans fil et une station de base ou entre deux clients sans fil. Les diverses spécifications de 802.11 comprennent 802.11a, une norme pour les réseaux allant jusqu'à 54 Mbits/s dans la bande des 5 GHz, 802.11b, une norme pour les réseaux allant jusqu'à 11 Mbits/s dans la bande des 2,4 GHz, 802.11g, une norme pour les réseaux allant jusqu'à 54 Mbits/s dans la bande des 2,4 GHz et 802.11i, une série de normes de sécurité pour tous les réseaux Ethernet sans fil.

802.11a

Extension de 802.11 qui s'applique aux réseaux locaux sans fil et envoie des données à un débit pouvant atteindre 54 Mbits/s dans la bande des 5 GHz. Même si le débit de transmission est plus rapide que celui du 802.11b, la distance couverte est inférieure.

802.11b

Extension du 802.11 qui s'applique aux réseaux locaux sans fil et assure une transmission à 11 Mbits/s dans la bande des 2,4 GHz. 802.11b est actuellement considéré comme la norme pour la communication sans fil.

802.11g

Extension du 802.11 qui s'applique aux réseaux locaux sans fil et assure une transmission pouvant atteindre 54 Mbits/s dans la bande des 2,4 GHz.

802.1x

Non compatible avec Wireless Home Network Security. Norme IEEE destinée à l'authentification sur les réseaux avec et sans fil, plus souvent utilisée avec les réseaux 802.11 sans fil. Cette norme assure une authentification performante et mutuelle entre un client et un serveur d'authentification. En outre, 802.1x peut fournir des clés WEP dynamiques par utilisateur et par session, en supprimant la charge administrative et les risques de sécurité liés aux clés WEP statiques.

A

adaptateur sans fil

Elément contenant le circuit qui permet à un ordinateur ou à un autre périphérique de communiquer avec un routeur sans fil (de se connecter à un réseau sans fil). Les adaptateurs sans fil peuvent être intégrés dans le circuit principal d'un matériel ou constituer un élément séparé à insérer dans un périphérique par le biais du port approprié.

adresse IP

Le numéro de protocole Internet (IP), ou adresse IP, est un numéro unique comportant quatre parties séparées par des points (par exemple, 63.227.89.66). Chaque ordinateur relié à Internet, depuis le serveur le plus important jusqu'au portable connecté via un téléphone cellulaire, possède un numéro IP unique. Tous les ordinateurs ne possèdent pas de nom de domaine, mais tous ont une adresse IP.

Voici quelques types d'adresses IP inhabituels :

- 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 de bouclage : ces adresses sont utilisées pour des tests. Le trafic envoyé vers ce bloc d'adresses IP retourne directement au périphérique ayant généré le paquet. Il ne quitte donc jamais le périphérique et sert essentiellement à des tests matériels et logiciels. Le bloc d'adresses IP en boucle est 127.x.x.x.

Adresse IP nulle : il s'agit d'une adresse non valide. Elle apparaît lorsque l'adresse IP du trafic était vierge. De toute évidence, cela est anormal et 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, incluant notamment des instructions spécifiques à cette application. Toute adresse commençant par 0 (0.x.x.x) est une adresse nulle. Par exemple, 0.0.0.0 est une adresse IP nulle.

adresse MAC (Media Access Control)

Adresse de bas niveau affectée au périphérique physique qui accède au réseau.

analyse des images

Empêche l'affichage des images potentiellement inappropriées. Les images sont bloquées pour tous les utilisateurs, à l'exception du groupe d'âge adulte.

analyse en temps réel

Analyse des fichiers à la recherche de virus ou d'autres activités lorsque vous ou votre ordinateur y accédez.

archivage complet

Archiver un jeu complet de données en fonction des types des fichiers de surveillance et des emplacements que vous avez déjà configurés.

archivage rapide

Archivage des seuls fichiers de surveillance modifiés depuis le dernier archivage complet ou rapide.

archive

Copie locale de vos fichiers de surveillance sur CD, DVD, lecteur USB, disque dur externe ou disque réseau.

archive

Copie locale de vos fichiers de surveillance sur CD, DVD, lecteur USB, disque dur externe ou disque réseau.

attaque en force

Aussi appelé craquage en force ; méthode par tâtonnement utilisée par les applications pour décoder des données chiffrées, comme des mots de passe, en employant une méthode exhaustive (en utilisant la force) plutôt qu'avec des stratégies intellectuelles. Tout comme un criminel pourrait entrer dans un coffre-fort en testant de nombreuses combinaisons possibles, une application de craquage en force passe par toutes les combinaisons possibles de caractères autorisés, les unes à la suite des autres. Ces méthodes en force sont jugées infaillibles mais longues.

attaque par dictionnaire

Ces attaques testent une série de mots dans une liste pour obtenir le mot de passe d'une personne. Les attaquants ne tentent pas manuellement toutes les combinaisons : ils disposent d'outils qui essaient d'identifier automatiquement le mot de passe.

attaque par immixtion

Ici, l'attaquant intercepte les messages dans un échange de clé publique, puis les retransmet, en substituant sa propre clé publique par celle demandée, de sorte que les deux parties aient toujours l'impression de communiquer directement entre elles. L'attaquant utilise un programme qui semble être le serveur pour le client et le client pour le serveur. L'attaque peut être simplement utilisée pour obtenir l'accès aux messages ou permettre à l'attaquant de les modifier avant de les retransmettre. Le terme anglais (man-in-the-middle, l'homme au milieu) est issu du jeu de ballon dans lequel des personnes tentent de s'envoyer la balle tandis qu'une autre, située entre deux, tente de l'intercepter.

authentification

Processus d'identification d'une personne, généralement basé sur un nom d'utilisateur et un mot de passe. L'authentification permet de s'assurer que la personne est bien celle qu'elle prétend être mais n'apporte aucune information sur ses droits d'accès.

B

bande passante

Quantité de données pouvant être transmise sur une période donnée. Pour les périphériques numériques, la bande passante est généralement exprimée en bits par seconde (bits/s) ou en octets par seconde. Pour les périphériques analogiques, la bande passante est exprimée en cycles par seconde ou en Hertz (Hz).

bibliothèque

Zone de stockage en ligne des fichiers publiés par les utilisateurs de Data Backup. La bibliothèque est un site Web sur Internet, accessible à toute personne disposant d'un accès Internet.

C

carte du réseau

Dans Network Manager, il s'agit d'une représentation graphique des ordinateurs et des autres composants de votre réseau domestique.

cartes adaptateur sans fil PCI

Carte permettant de connecter un ordinateur de bureau à un réseau. La carte se branche dans un connecteur d'extension PCI de l'ordinateur.

cartes adaptateur sans fil USB

Cartes qui fournissent une interface série Plug and Play évolutive. Cette interface assure une connexion sans fil standard, à faible coût, pour des périphériques tels que des claviers, des souris, des manettes de jeu, des imprimantes, des scanners, des périphériques de stockage et des Webcams.

certifié Wi-Fi

Tous les produits testés et approuvés comme des produits certifiés Wi-Fi (une marque déposée) par la Wi-Fi Alliance sont certifiés compatibles les uns avec les autres, même s'ils proviennent de différents fabricants. Un utilisateur disposant d'un produit certifié Wi-Fi peut utiliser n'importe quelle marque de point d'accès avec toute autre marque de matériel client également certifié. Toutefois, d'ordinaire, tout produit Wi-Fi utilisant la même fréquence radio (par exemple 2,4 GHz pour 802.11b ou 11g, 5 GHz pour 802.11a) fonctionne avec n'importe quel autre, même s'il n'est pas certifié Wi-Fi.

cheval de Troie

Programmes qui prétendent être des applications inoffensives. Les chevaux de Troie ne sont pas des virus, car ils ne se répliquent pas, mais ils sont tout aussi ravageurs.

chiffrement

Processus de transformation de données, de texte en code, qui les obscurcit pour les rendre illisibles par les personnes ne sachant pas les déchiffrer.

clé

Série de lettres ou de chiffres utilisée par deux périphériques pour authentifier une communication. Les deux doivent disposer de la clé. Voir aussi WEP, WPA, WPA2, WPA-PSK et WPA2- PSK.

client

Application qui s'exécute sur un ordinateur personnel ou une station de travail et qui s'appuie sur un serveur pour certaines de ses opérations. Un client de messagerie, par exemple, est une application qui permet d'envoyer et de recevoir des courriers électroniques.

client de messagerie

Compte de messagerie électronique. Par exemple, Microsoft Outlook ou Eudora.

compression

Processus permettant de compresser des données (fichiers) dans un format qui réduit l'espace nécessaire pour les stocker ou les transmettre.

compte de messagerie standard

La plupart des particuliers utilisent ce type de compte. Voir aussi compte POP3.

compte MAPI

Acronyme de Messaging Application Programming Interface. Spécification d'interface de Microsoft permettant à différentes applications de messagerie et de groupes de travail (messagerie électronique, messagerie vocale, télécopie...) de fonctionner sur un seul client, comme le client Exchange. Par conséquent, les entreprises exploitent généralement le système MAPI si elles utilisent Microsoft™ Exchange Server. Toutefois, de nombreuses personnes continuent à utiliser Microsoft Outlook pour gérer leurs e-mails personnels.

compte MSN

Acronyme de Microsoft Network. Service en ligne et portail Internet. Il s'agit d'un compte basé sur le Web.

compte POP3

Acronyme de Post Office Protocol 3. La plupart des particuliers utilisent ce type de compte. Il s'agit de la version actuelle de la norme Post Office Protocol, généralement utilisée sur les réseaux TCP/IP. Aussi appelée compte de messagerie standard.

contrôle parental

Paramètres permettant de configurer la classification du contenu. Celle-ci restreint l'affichage des sites Web et du contenu, ainsi que les limites horaires. En d'autres termes, elle gère la période et la durée de connexion à Internet. Selon la tranche d'âge et les mots-clés associés, Parental Controls permet globalement de restreindre, d'accorder ou de bloquer l'accès à certains sites Web.

cookie

Sur le Web, bloc de données qu'un serveur Web stocke sur un système client. Lorsqu'un utilisateur revient sur le même site Web, le navigateur renvoie une copie du cookie au serveur. Les cookies servent à identifier des utilisateurs, demander au serveur d'envoyer une version personnalisée de la page Web demandée, soumettre des informations de compte à l'utilisateur et réaliser d'autres tâches administratives.

Ils permettent au site Web de se souvenir de vous et de connaître le nombre de visiteurs, les dates de consultation et les pages consultées. Les cookies peuvent également aider une entreprise à personnaliser son site Web pour vous. De nombreux sites Web vous demandent d'entrer un nom d'utilisateur et un mot de passe avant de vous donner accès à certaines pages et envoient un cookie à votre ordinateur pour que vous n'ayez pas à vous connecter à chaque fois. Cependant, les cookies peuvent être utilisés à des fins malveillantes. Les agences de publicité en ligne utilisent souvent des cookies pour identifier les sites que vous consultez le plus souvent, puis placent des publicités sur vos sites Web favoris. N'acceptez que les cookies des sites auxquels vous faites confiance.

Bien que les cookies constituent une source d'informations pour des entreprises honnêtes, ils peuvent également constituer une source d'informations pour les pirates informatiques. De nombreux sites disposant de boutiques virtuelles enregistrent les numéros de carte de crédit et d'autres informations personnelles dans des cookies pour simplifier les achats de leurs clients. Malheureusement, des bogues de sécurité peuvent survenir et permettre à des pirates informatiques d'accéder aux informations des cookies stockés sur les ordinateurs des clients.

D

débordement de la mémoire tampon

Les débordements de tampon se produisent lorsque des programmes ou des processus suspects tentent de stocker dans un tampon (zone de stockage temporaire des données) une quantité de données plus importante que votre ordinateur ne peut en contenir, ce qui endommage ou écrase les données valides des tampons adjacents.

déni de service

Sur Internet, incident au cours duquel un utilisateur ou une entreprise est privé des services d'une ressource dont il s'attendait à disposer. Généralement, la perte de service réside dans l'indisponibilité d'un service réseau en particulier, comme la messagerie électronique, ou la perte temporaire de toutes les connexions et de tous les services du réseau. Dans le pire des cas, par exemple, un site Web auquel accèdent des millions de personnes peut, à l'occasion, être obligé de cesser ses opérations de manière temporaire. Une attaque de déni de service peut également détruire la programmation et les fichiers d'un système informatique. Même si elle est généralement intentionnelle et malveillante, une attaque de déni de service peut quelquefois survenir accidentellement. Une attaque de déni de service est un type de violation de la sécurité d'un système informatique qui n'entraîne généralement pas le vol d'informations ni une baisse de la sécurité. Ces attaques peuvent toutefois coûter beaucoup d'argent et de temps à la victime, qui peut être un particulier ou une société.

disque dur externe

Disque dur conservé en dehors du boîtier de l'ordinateur.

DNS

Acronyme de Domain Name System. Système hiérarchique par lequel les hôtes sur Internet possèdent des adresses de nom de domaine (comme bluestem.prairienet.org) et des adresses IP (comme 192.17.3.4). L'adresse du nom de domaine sert aux utilisateurs humains et elle est automatiquement traduite en adresse IP numérique, qui sert au logiciel de routage des paquets. Les noms DNS sont composés d'un domaine de niveau supérieur (.com, .org, .net...), d'un domaine de niveau secondaire (nom du site d'une entreprise, d'un organisme ou d'une personne) et, parfois, d'un ou de plusieurs sous-domaines (serveurs placés dans un domaine de niveau secondaire). Voir aussi serveur DNS et adresse IP.

domaine

Adresse d'une connexion réseau qui identifie le propriétaire de cette adresse dans un format hiérarchique : serveur.organisation.type. Par exemple, www.whitehouse.gov identifie le serveur Web de la Maison blanche, qui fait partie du gouvernement des Etats-Unis.

E

e-mail

Courrier, messages électroniques envoyés via Internet ou sur le réseau local ou étendu d'une entreprise. Les virus et chevaux de Troie sont de plus en plus transmis par les pièces jointes aux courriers électroniques sous la forme de fichiers EXE (exécutables) ou VBS (scripts Visual Basic).

emplacement de surveillance accrue

Dossier (et ses sous-dossiers) de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement de surveillance accrue, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier ou ses sous-dossiers.

emplacements de surveillance de premier niveau

Dossier de votre ordinateur dont les changements sont surveillés par Data Backup. Si vous définissez un emplacement surveillé de premier niveau, Data Backup sauvegarde les types de fichiers de surveillance dans ce dossier, mais n'inclut pas ses sous-dossiers.

emplacements surveillés

Dossiers surveillés par Data Backup sur votre ordinateur.

en-tête

Informations ajoutées à la partie du message au cours de son cycle de vie. L'en-tête indique au logiciel Internet comment livrer votre message et où envoyer les réponses ; il lui fournit un numéro d'identification unique, ainsi que d'autres informations administratives. Exemples de champs d'en-tête : A, De, Cc, Date, Objet, ID du message et Reçu.

ESS (jeu de service étendu)

Ensemble de deux réseaux ou plus formant un même sous-réseau.

É

événements

événements provenant de 0.0.0.0

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

L'autre situation se présente lorsque la source IP 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. Il est important de se souvenir que Firewall bloque la tentative.

événements provenant de 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.

Quel que soit l'ordinateur que vous utilisez, 127.0.0.1 fera toujours référence à votre ordinateur local. 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/.

Cependant, Firewall autorise le trafic émanant de ces programmes ; par conséquent, si vous détectez des événements provenant de l'adresse IP 127.0.0.1, celle-ci est sans doute usurpée ou fausse. Les paquets usurpés indiquent généralement un utilisateur à la recherche d'un cheval de Troie. Il est important de se souvenir que Firewall bloque la tentative. A l'évidence, il sera inutile de signaler les événements provenant de l'adresse 127.0.0.01.

Ceci dit, certains programmes, notamment Netscape version 6.2 ou ultérieure, requièrent l'ajout de 127.0.0.1 à la liste **Adresses IP autorisées**. Ces composants du programme communiquent entre eux de telle manière que 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 de127.0.0.1 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 Firewall, puis regardez si cela résout le problème.

Si cela résout le problème, vous devrez faire un choix : 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 type de trafic malveillant.

événements provenant d'ordinateurs de votre réseau local

Pour la plupart des paramètres de réseaux locaux d'entreprise, vous pouvez autoriser tous les ordinateurs de votre réseau local.

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 accorderez ainsi votre confiance à 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 indiquent généralement qu'un utilisateur recherche un cheval de Troie. Il est important de se souvenir que Firewall bloque la tentative.

Les adresses IP privées étant différentes des adresses IP sur Internet, il est inutile de signaler ces événements.

fenêtres instantanées

Petites fenêtres qui apparaissent au-dessus d'autres fenêtres plus grandes, sur l'écran de l'ordinateur. Les fenêtres instantanées servent souvent à afficher des publicités dans les navigateurs Web. McAfee bloque les fenêtres instantanées chargées automatiquement lors de l'ouverture d'une page Web dans le navigateur et non celles qui apparaissent lorsque vous cliquez sur un lien.

groupes d'évaluation de contenu

Groupes d'âge auxquels appartient un utilisateur. Le contenu est évalué (à savoir qu'il est mis à disposition ou bloqué) en fonction du groupe auquel appartient l'utilisateur. Les groupes d'évaluation du contenu incluent : les jeunes enfants, les enfants, les pré-adolescents, les adolescents et les adultes.

Internet

Ensemble d'un grand nombre de réseaux interconnectés qui utilisent le protocole TCP/IP pour localiser et transférer des données. Initialement, il s'agissait d'une liaison entre des ordinateurs d'universités (à la fin des années 1960 et au début des années 1970) financée par le Ministère de la Défense des Etats-Unis et appelée ARPANET. Aujourd'hui, Internet est un réseau mondial qui regroupe près de 100 000 réseaux indépendants.

intranet

Réseau privé, généralement interne à une entreprise, de fonctionnement similaire à celui d'Internet. Désormais, les entreprises et les universités autorisent couramment des employés ou des étudiants travaillant en dehors des locaux à se connecter à leur intranet depuis un ordinateur autonome. Les Firewalls, ainsi que les procédures et les mots de passe de connexion, sont conçus pour en sécuriser l'accès.

itinérance

Capacité à se déplacer d'une zone de couverture d'un point d'accès à une autre, sans interruption du service, ni perte de connexion.

lecteur réseau

Disque ou lecteur de bande relié à un serveur sur un réseau partagé par plusieurs utilisateurs. Les lecteurs réseau sont quelquefois appelés lecteurs distants.

liste d'autorisation

Liste de sites Web auquel l'accès est autorisé car ils ne sont pas considérés comme frauduleux.

liste de blocage

Liste de sites Web considérés malveillants. Un site Web peut être placé sur une liste de blocage du fait d'une opération frauduleuse ou parce qu'il exploite une vulnérabilité du navigateur pour envoyer des programmes potentiellement indésirables à l'utilisateur.

MAC (Media Access Control ou Message Authenticator Code)

Pour le premier, voir adresse MAC. Le deuxième est un code servant à identifier un message donné (par exemple, un message RADIUS). Le code représente généralement un hachage cryptographique efficace du contenu du message, comprenant une valeur unique pour se prémunir contre les répétitions.

mot de passe

Code (généralement alphanumérique) qui permet d'accéder à votre ordinateur, à un programme ou à un site Web spécifique.

mot-clé

Mot pouvant être affecté à un fichier sauvegardé pour établir une relation ou une connexion avec d'autres fichiers auxquels le même mot-clé a été affecté. Les mots-clé facilitent la recherche des fichiers publiés sur Internet.

navigateur

Programme client qui utilise le protocole HTTP (Hypertext Transfer Protocol) pour adresser des requêtes aux serveurs Web sur Internet. Il affiche le contenu Internet sous forme graphique, afin de le rendre compréhensible par l'utilisateur.

NIC (Network Interface Card)

Carte qui se branche sur un ordinateur portable ou un autre périphérique pour le relier au réseau local.

noeud

Ordinateur unique relié à un réseau.

pare-feu

Système conçu pour empêcher les accès non autorisés à un réseau privé ou à partir de ce dernier. Les pare-feux peuvent être mis en oeuvre dans des configurations matérielles ou logicielles, ou une combinaison des deux. Ils sont fréquemment utilisés pour empêcher les utilisateurs non autorisés d'accéder à des réseaux privés connectés à Internet, en particulier des intranets. Tous les messages entrant ou sortant de l'intranet passent par le pare-feu. Celui-ci étudie chaque message et bloque ceux qui ne répondent pas aux critères de sécurité spécifiés. Un pare-feu est considéré comme une première ligne de défense pour protéger les informations privées. Les données peuvent être chiffrées pour plus de sécurité.

partage

Opération permettant aux destinataires des courriers électroniques d'accéder à certains fichiers sauvegardés pendant une certaine période. Lorsque vous partagez un fichier, vous en envoyez la copie sauvegardée aux destinataires que vous choisissez. Ces derniers reçoivent un courrier électronique de Data Backup leur signalant que des fichiers ont été partagés avec eux. Le courrier comporte également un lien vers ces fichiers partagés.

passerelle intégrée

Dispositif qui associe les fonctions d'un point d'accès, d'un routeur et d'un pare-feu. Certains peuvent aussi comporter des améliorations de sécurité et des fonctions de pont.

Password Vault

Zone de stockage sécurisée des mots de passe personnels. Ainsi, vous êtes assuré que personne ne peut accéder à vos mots de passe (pas même un administrateur système ou McAfee).

phishing

(Prononcer "fishing"). Arnaque visant à voler des informations précieuses, comme les numéros de carte de crédit et de sécurité sociale, les ID utilisateur et les mots de passe. Un courrier électronique, paraissant officiel, est envoyé aux victimes potentielles en leur faisant croire qu'il provient de leur FAI, de leur banque ou de leur magasin. Les courriers peuvent être envoyés à des personnes apparaissant sur certaines listes ou sur n'importe laquelle et supposent qu'une certaine partie des destinataires auront réellement un compte dans cet organisme.

pixels invisibles

Petits fichiers graphiques pouvant s'insérer dans vos pages HTML et permettant à une source non autorisée de placer des cookies sur votre ordinateur. Ces cookies peuvent ensuite transmettre des informations à la source non autorisée. Les pixels invisibles sont aussi appelés balises Web, GIF transparents ou GIF invisibles.

point d'accès

Périphérique réseau permettant aux clients 802.11 de se connecter à un réseau local. Les points d'accès prolongent la gamme de service physique pour un utilisateur sans fil. Quelquefois appelé routeur sans fil.

point d'accès non fiable

Point d'accès dont une société n'autorise pas le fonctionnement. Bien souvent, les points d'accès non fiables ne se conforment pas aux stratégies de sécurité d'un réseau local sans fil. Ils autorisent une interface ouverte et non sécurisée à accéder au réseau de l'entreprise depuis l'extérieur de la structure physiquement contrôlée.

Dans un réseau local sans fil correctement sécurisé, les points d'accès non fiables sont plus dévastateurs que les utilisateurs malveillants. En effet, si des mécanismes efficaces d'authentification sont installés, les utilisateurs non autorisés qui tentent d'accéder à un réseau local sans fil ne parviendront pas à atteindre les ressources précieuses de l'entreprise. Des problèmes majeurs apparaissent toutefois lorsqu'un employé ou un pirate se connecte à un point d'accès non fiable. Le point d'accès autorise quasiment tous les périphériques équipés du 802.11 du réseau de l'entreprise à entrer. Ceci les rapproche dangereusement des ressources essentielles.

point d'accès sans fil

Emplacement géographique spécifique dans lequel un point d'accès assure des services de réseau large bande sans fil public aux visiteurs itinérants, grâce à un réseau sans fil. Les points d'accès sans fil sont souvent situés dans des lieux très fréquentés comme les aéroports, les gares ferroviaires, les bibliothèques, les marinas, les centres de conférence et les hôtels. Ils présentent généralement une plage de fonctionnement assez courte.

port

Endroit par lequel les informations entrent dans un ordinateur ou en sortent. Par exemple, un modem analogique traditionnel se connecte à un port série. Les numéros de port des communications TCP/IP sont des valeurs virtuelles qui permettent de séparer les données qui transitent dans des flux spécifiques à chaque application. Les ports sont attribués à des protocoles standard tels que SMTP ou HTTP pour permettre aux programmes de savoir sur quel port établir des connexions. Le port de destination des paquets TCP indique l'application ou le serveur recherchés.

PPPoE

Acronyme de Point-to-Point Protocol Over Ethernet. Utilisé par de nombreux fournisseurs de services DSL, le PPPoE accepte les couches de protocole et l'authentification généralement utilisées en PPP et permet l'établissement d'une connexion en point à point dans l'architecture généralement multipoint d'Ethernet.

programme potentiellement indésirable

Programmes comprenant les logiciels espions et publicitaires et les autres programmes qui accèdent à vos données personnelles et les transmettent sans votre autorisation.

protocole

Format accepté pour transmettre des données entre deux périphériques. Du point de vue de l'utilisateur, la seule chose à savoir sur les protocoles réside dans le fait que leur ordinateur ou leur périphérique doit accepter le protocole adéquat pour communiquer avec d'autres ordinateurs. Le protocole peut être mis en place dans le matériel ou dans le logiciel.

proxy

Ordinateur (ou logiciel s'exécutant sur cet ordinateur) qui agit comme une barrière entre un réseau et Internet en présentant une adresse réseau unique aux sites externes. Le proxy joue le rôle d'intermédiaire pour l'ensemble des ordinateurs internes afin de protéger les identités réseau tout en fournissant un accès à Internet. Voir aussi serveur proxy.

publier

Mettre à disposition du public, sur Internet, un fichier sauvegardé.

quarantaine

Mise à l'écart des fichiers suspects détectés. L'utilisateur peut alors entreprendre l'action appropriée.

RADIUS (Remote Access Dial-In User Service)

Protocole assurant l'authentification des utilisateurs, généralement dans le contexte d'un accès distant. Initialement défini pour être utilisé avec des serveurs d'accès distant à commutation, le protocole sert maintenant dans divers environnements d'authentification, notamment l'authentification 802.1x d'un secret partagé de l'utilisateur d'un WLAN.

référentiel de sauvegarde en ligne

Emplacement sur le serveur en ligne pour stocker les fichiers de surveillance après leur sauvegarde.

réseau

Connexion de plusieurs ordinateurs.

réseau géré

Un réseau domestique comporte deux types de membres : des membres gérés et des membres non gérés. Les membres gérés autorisent les autres ordinateurs du réseau à surveiller l'état de leur protection McAfee, contrairement aux membres non gérés.

réseau local (LAN)

Réseau d'ordinateurs qui s'étend sur une zone relativement petite. La plupart des réseaux locaux sont limités à un seul bâtiment ou groupe de bâtiments. Un réseau local peut toutefois être relié à d'autres, quelle que soit la distance, par le téléphone et les ondes radio. Un système de réseaux locaux reliés de cette manière est appelé réseau étendu (WAN). La plupart des réseaux locaux relient des stations de travail et des ordinateurs, généralement par des concentrateurs ou des commutateurs simples. Chaque noeud (ordinateur) d'un réseau local possède sa propre unité centrale grâce à laquelle il exécute des programmes, mais il peut aussi accéder aux données et aux périphériques (comme les imprimantes) n'importe où sur le réseau. Ainsi, de nombreux utilisateurs peuvent partager des périphériques onéreux, comme des imprimantes laser, ou des données. Les utilisateurs peuvent aussi utiliser le réseau local pour communiquer entre eux, par exemple pour envoyer des messages électroniques ou discuter en direct.

réseau local sans fil (WLAN)

Voir aussi réseau local. Réseau local utilisant un support sans fil pour sa connexion. Un réseau local sans fil utilise des ondes radio hautes fréquences à la place des fils pour communiquer d'un noeud à un autre.

restauration

Récupération d'une copie d'un fichier à partir du référentiel de sauvegarde en ligne ou d'une archive.

routeur

Périphérique réseau qui transmet les paquets d'un réseau à un autre. Selon les tables de routage internes, les routeurs lisent chaque paquet entrant et décident ou non de le transmettre. L'interface à laquelle sont envoyés les paquets sortants du routeur peut être déterminée par une combinaison des adresses source et cible, ainsi que par les conditions actuelles du trafic, comme la charge, les coûts de la ligne et les lignes endommagées. Quelquefois appelé point d'accès.

sauvegarde

Copie des fichiers de surveillance sur un serveur sécurisé en ligne.

script

Elément capable de créer, copier ou supprimer des fichiers. Il peut également ouvrir votre registre Windows.

secret partagé

Voir aussi RADIUS. Protection des parties sensibles des messages RADIUS. Ce secret partagé est un mot de passe partagé entre l'authentificateur et le serveur d'authentification, de manière sécurisée.

serveur

Ordinateur ou logiciel qui fournit des services spécifiques aux logiciels exécutés sur d'autres ordinateurs. Le "serveur de messagerie" de votre FAI est un logiciel qui gère tous les messages entrants et sortants pour l'ensemble de ses utilisateurs. Un serveur sur un réseau local est un système matériel qui constitue le noeud principal du réseau. Il peut également exécuter des logiciels fournissant des services ou des données spécifiques à l'ensemble des ordinateurs clients qui y sont reliés, ou leur offrir d'autres fonctionnalités.

serveur DNS

Version abrégée de serveur de Domain Name System. Ordinateur capable de répondre à des requêtes de DNS. Le serveur DNS conserve une base de données d'ordinateurs hôtes et de leurs adresses IP correspondantes. Si on lui présente le nom apex.com, par exemple, le serveur DNS renvoie l'adresse IP de la société Apex imaginaire. Aussi appelé : serveur de nommage. Voir aussi DNS et adresse IP.

serveur proxy

Composant de Firewall qui gère le trafic Internet vers et depuis un réseau local (LAN). L'utilisation d'un serveur proxy améliore les performances par deux aspects : d'une part, il fournit des données fréquemment demandées, telles qu'une page Web et, d'autre part, il filtre les demandes et ignore celles que le propriétaire considère comme inappropriées (par exemple, les demandes d'accès non autorisées à des fichiers propriétaires).

serveur SMTP

Acronyme de Simple Mail Transfer Protocol. Protocole TCP/IP permettant de transmettre des messages d'un ordinateur à un autre sur un réseau. Ce protocole sert à router les courriers électroniques sur Internet.

SSID (Service Set Identifier)

Nom réseau pour les périphériques d'un sous-système d'un réseau local sans fil. Il s'agit d'une chaîne longue de 32 caractères en texte clair, ajoutée au début de chaque paquet de réseau local sans fil. Le SSID différentie entre eux les réseaux locaux sans fil pour que tous les utilisateurs puissent fournir le même SSID et accéder à un point d'accès donné. Un SSID refuse l'accès à tout périphérique client ne possédant pas de SSID. Par défaut toutefois, un point d'accès diffuse son SSID dans sa balise. Et même si la diffusion du SSID est désactivée, un pirate peut le détecter via une opération de reniflage.

SSL (Secure Sockets Layer)

Protocole développé par Netscape pour transmettre des documents privés sur Internet. SSL utilise une clé publique pour chiffrer des données transférées sur une connexion SSL. Netscape Navigator et Internet Explorer utilisent et acceptent tous deux le SSL et de nombreux sites Web utilisent le protocole pour obtenir des informations confidentielles sur l'utilisateur comme son numéro de carte de crédit. Par convention, les URL nécessitant une connexion SSL commencent par https au lieu de http.

synchroniser

Résoudre les incohérences entre des fichiers sauvegardés et ceux stockés sur votre ordinateur local. La synchronisation des fichiers a lieu lorsque la version du fichier dans le référentiel de sauvegarde en ligne est plus récente que la version du fichier sur d'autres ordinateurs. La synchronisation met à jour la copie du fichier sur l'ordinateur avec la version du fichier se trouvant dans le référentiel de sauvegarde en ligne.

SystemGuard

Les SystemGuards détectent les modifications non autorisées apportées à votre ordinateur et vous en avertissent.

texte brut

Message non chiffré.

texte chiffré

Données qui ont été chiffrées. Le texte chiffré est illisible tant qu'il n'a pas été converti en texte brut (déchiffré) à l'aide d'une clé.

TKIP (Temporal Key Integrity Protocol)

Méthode de réparation rapide pour surmonter les faiblesses inhérentes à la sécurité WEP, notamment pour la réutilisation des clés de chiffrement. TKIP modifie les clés temporaires tous les 10 000 paquets, pour offrir une méthode de distribution dynamique qui améliore considérablement la sécurité du réseau. Le processus TKIP (sécurité) démarre par une clé temporaire à 128 bits partagée entre les clients et les points d'accès. Il associe la clé temporaire à l'adresse MAC (celle de la machine cliente), puis ajoute un vecteur d'initialisation de 16 octets relativement large pour produire la clé qui chiffre les données. Cette procédure permet de s'assurer que chaque station utilise des flux de clé différents pour chiffrer les données. TKIP utilise le RC4 pour procéder au chiffrement. Le WEP utilise aussi le RC4.

types de fichiers de surveillance

Types de fichiers (par exemple, .doc, .xls, etc.) que Data Backup sauvegarde ou archive dans les emplacements surveillés.

URL

Localisateur de ressources universel. L'URL est le format standard d'adresse Internet.

usurpation d'adresse IP

Action de falsifier les adresses IP dans un paquet IP. Ceci est utilisé dans de nombreux types d'attaques, notamment la prise de contrôle des sessions, et sert souvent à falsifier les en-têtes des courriers électroniques de spam pour empêcher leur traçage.

ver

Virus qui se propage automatiquement et qui se fixe dans la mémoire active et peut utiliser les e-mails pour envoyer des copies de lui-même. Les vers reproduisent et consomment les ressources du système, ce qui ralentit les performances ou interrompt les tâches.

VPN (Virtual Private Network)

Réseau conçu pour utiliser les câbles publics afin de réunir des noeuds. Il existe par exemple plusieurs systèmes permettant de créer des réseaux en passant par Internet comme support du transport des données. Ces systèmes utilisent le chiffrement et d'autres mécanismes de sécurité pour s'assurer que seuls les utilisateurs autorisés aient accès au réseau et que les données ne puissent pas être interceptées.

wardriver

Interpolateurs munis d'ordinateurs portables, de logiciels spéciaux et de matériel improvisé, qui passent par les villes, les banlieues et les parcs d'activité pour intercepter le trafic d'un réseau local sans fil.

WEP (Wired Equivalent Privacy)

Protocole de chiffrement et d'authentification défini dans le cadre de la norme 802.11. Les premières versions sont basées sur des chiffrements RC4 et présentent des faiblesses considérables. WEP tente d'apporter un minimum de sécurité en chiffrant les données sur des ondes radio pour qu'elles soient protégées lors de leur transfert d'un point d'extrémité à un autre. On a toutefois découvert que WEP n'est pas aussi sûr qu'on le pensait.

Wi-Fi (Wireless Fidelity)

Terme générique utilisé pour désigner tout type de réseau 802.11, qu'il s'agisse de 802.11b, 802.11a, double bande, etc. Le terme est utilisé par la Wi-Fi Alliance.

Wi-Fi Alliance

Organisation constituée des principaux fournisseurs d'équipements et logiciels sans fil, avec pour mission de (1) certifier tous les produits basés sur 802.11 à des fins de compatibilité et (2) promouvoir le terme Wi-Fi comme marque internationale sur tous les marchés, pour tous les produits de réseaux locaux sans fil basés sur du 802.11. L'organisation agit comme un consortium, un laboratoire de test et un centre d'informations pour les fournisseurs qui veulent promouvoir la compatibilité et la croissance du marché.

Même si tous les produits 802.11a/b/g sont appelés Wi-Fi, seuls ceux qui ont réussi le test de Wi-Fi Alliance sont autorisés à se qualifier de certifiés Wi-Fi (une marque déposée). Les produits qui réussissent le test doivent avoir un sceau d'identification sur leurs emballages indiquant qu'ils sont certifiés Wi-Fi et précisant la bande de fréquence radio utilisée. Ce groupe était anciennement connu sous le nom WECA (Wireless Ethernet Compatibility Alliance) mais a changé de nom en octobre 2002 pour mieux représenter la marque Wi-Fi qu'il souhaitait créer.

WPA (Wi-Fi Protected Access)

Norme de spécification qui augmente fortement le niveau de protection des données et le contrôle d'accès des systèmes de réseau local sans fil actuels et futurs. Conçu pour fonctionner sur le matériel existant sous la forme d'une mise à niveau du logiciel, le WPA est issu de la norme IEEE 802.11i avec laquelle il est compatible. Lorsqu'il est correctement installé, il offre aux utilisateurs d'un réseau local sans fil un niveau de certitude élevé sur le fait que leurs données sont protégées et que seuls les utilisateurs autorisés à utiliser le réseau y auront accès.

WPA-PSK

Mode WPA spécial, conçu pour les utilisateurs à domicile qui n'ont pas besoin de la sécurité nécessaire aux entreprises et n'ont pas accès à des serveurs d'authentification. Avec ce mode, l'utilisateur à domicile entre manuellement le mot de passe de départ pour activer l'accès Wi-Fi protégé en mode clé pré-partagée et doit régulièrement modifier le mot de passe sur chaque ordinateur sans fil et point d'accès. Voir aussi WPA2-PSK et TKIP.

WPA2

Voir aussi WPA. Mise à jour de la norme de sécurité WPA, basée sur la norme 802.11i IEEE.

WPA2-PSK

Voir aussi WPA-PSK et WPA2. Norme similaire à WPA-PSK, basée sur la norme WPA2. Cette norme établit, parmi ses fonctions générales, que les périphériques acceptent souvent plusieurs modes de chiffrement (comme AES, TKIP) simultanément, tandis que les plus anciens n'acceptaient généralement qu'un mode de chiffrement à la fois (tous les clients devaient utiliser le même mode de chiffrement).

A propos de McAfee

McAfee, Inc., leader mondial en gestion des risques de sécurité et prévention des intrusions et dont le siège social est basé à Santa Clara, Californie, propose des solutions et services proactifs et éprouvés de sécurisation des systèmes et réseaux dans le monde entier. Avec son expérience de la sécurité et son engagement à l'innovation sans égal, McAfee offre aux particuliers, aux entreprises, au secteur public et aux prestataires de service la capacité de bloquer les attaques, de prévenir les perturbations et d'assurer et d'améliorer régulièrement leur sécurité.

Copyright

Index

B

C

D

E

F

G

I

L

M

N

O

T

U

V

W