symantec™

Norton™ Personal Firewall 2003

Guide de l'utilisateur

Guide de l'utilisateur – Norton™ Personal Firewall

Documentation version 6.0

Référence : 10029049-FR

Copyright

Marques

Imprimé en Irlande.

10 9 8 7 6 5 4 3 2 1

Table des matières

Chapitre 4 Bases de Norton Personal Firewall

Chapitre 5 Mises à jour avec LiveUpdate

Annexe C Risques et menaces liés à Internet

Réponse aux urgences

1

En cas d'urgence, reportez-vous à cette section pour trouver la solution à votre problème.

Si vous pensez que votre ordinateur fait l'objet d'une attaque

Si l'ordinateur répond de manière anormale et que vous avez déterminé qu'il ne s'agit pas d'un virus ou d'un fichier corrompu, vous faites peut-être l'objet d'une attaque.

Si vous soupçonnez une attaque de pirate, déconnectez immédiatement l'ordinateur d'Internet. Si vous n'avez pas encore installé Norton Personal Firewall, installez-le maintenant.

Si vous avez installé Norton Personal Firewall, vous pouvez utiliser ses outils de sécurité pour bloquer l'attaque, rechercher l'attaquant et éviter les attaques à l'avenir.

Pour bloquer et analyser une attaque

1. Ouvrez Norton Personal Firewall.
2. Cliquez sur **Bloquer le trafic**.
   Cela bloque immédiatement toute communication entrante et sortante avec les autres ordinateurs.
3. Si vous utilisez Security Monitor, cliquez sur **Security Center**.
4. Dans Security Center, cliquez sur **Statistiques**.
5. Cliquez sur **Détails de l'attaquant**.
   Votre navigateur ouvre la page Web Visual Tracking.

Se reporter à "Arrêt d'une communication Internet avec la fonction Bloquer le trafic" à la page 45.

6 Visual Tracking permet d'identifier l'adresse IP de l'ordinateur utilisé par l'attaquant.
Vous pouvez vous servir de cette information pour signaler l'attaque au FAI propriétaire de l'adresse.

Se reporter à "Identification de la source de communications" à la page 44.

7 Pour bloquer toute connexion future de cette adresse IP, ajoutez l'ordinateur à votre zone Restreints.

Se reporter à "Ajout d'un ordinateur bloqué à la zone Restreints" à la page 97.

Si vous pensez qu'un pirate a déjà investi l'ordinateur, installez Norton Personal Firewall, puis consultez l'adresse http://security.symantec.com où sont disponibles des outils permettant de réparer et d'éradiquer toute menace qu'un pirate aurait pu placer sur l'ordinateur.

Restauration après incident

Quand vous avez résolu le problème, vous pouvez installer Norton Personal Firewall et procéder aux activités suivantes :

Action	Description
Installation de Norton Personal Firewall.	Norton Personal Firewall peut protéger votre ordinateur contre toute attaque ultérieure. Se reporter à "Installation de Norton Personal Firewall" à la page 17.
Mise à jour de la protection.	Une fois l'installation effectuée, exécutez LiveUpdate pour vérifier que vous disposez des protections les plus récentes. Se reporter à "Mises à jour avec LiveUpdate" à la page 57.
Configuration du pare-feu.	L'installation par défaut de Norton Personal Firewall doit fournir une protection suffisante aux utilisateurs, mais il est possible de personnaliser la protection en définissant les paramètres du pare-feu. Se reporter à "Personnalisation de la protection du pare-feu" à la page 78.
Consultation régulière des journaux et des statistiques.	Norton Personal Firewall conserve des rapports complets de toutes les opérations entreprises pour protéger l'ordinateur. Consultez régulièrement ces journaux pour identifier les problèmes potentiels. Se reporter à "Contrôle de Norton Personal Firewall" à la page 115.

Prévention des problèmes ultérieurs

Norton Personal Firewall peut protéger votre ordinateur contre la plupart des attaques par Internet.

Pour préparer votre ordinateur aux situations d'urgence

- Tenez-vous informé sur les risques relatifs à la sécurité en visitant le *site Web* de Symantec Security Response (securityresponse.symantec.com).
- Actualisez votre *navigateur*. Les éditeurs de logiciels publient de nouvelles versions pour remédier aux vulnérabilités de leurs navigateurs.
- Utilisez intelligemment les *mots de passe*. Pour protéger les données importantes, utilisez des mots de passe complexes composés de majuscules, de minuscules, de chiffres et de symboles. N'utilisez pas le même mot de passe en plusieurs endroits.
- N'exécutez pas un logiciel si vous ne faites pas confiance à son éditeur et à la source qui vous l'a fourni.
- N'ouvrez une pièce jointe de *courrier électronique* que si vous l'attendiez et que vous faites confiance à son expéditeur.
- Soyez prudent lorsque vous décidez de transmettre des informations personnelles. Bien souvent, les sites demandent des informations dont ils n'ont pas besoin.
- Consultez la politique de confidentialité des sites auxquels vous envisagez d'envoyer des informations.
- Indiquez aux enfants de ne jamais révéler d'informations personnelles sur des messageries instantanées.
- Sauvegardez régulièrement vos fichiers et conservez à portée de main une copie des dernières sauvegardes.

A propos de Norton Personal Firewall

2

Norton Personal Firewall protège les ordinateurs contre les attaques Internet, protège la confidentialité de vos informations et accélère la navigation sur le Web en éliminant les publicités.

Nouveautés de Norton Personal Firewall 2003

Norton Personal Firewall 2003 inclut à présent :

- Security Monitor
  Vous assure un accès rapide aux outils de Norton Personal Firewall les plus utilisés.
- Visual Tracking
  Identifie la source des attaques et d'autres communications Internet.
- Protection par mot de passe
  Renforce la protection des options de Norton Personal Firewall.
- Blocage du trafic
  Permet d'empêcher immédiatement d'autres ordinateurs de communiquer avec le vôtre.
- Assistant Alerte
  Vous permet de comprendre les alertes et les problèmes de sécurité éventuels.
- Afficheur du journal
  Cette version améliorée permet de voir toutes les actions entreprises par Norton Personal Firewall pour protéger votre ordinateur

- Confidentialité
  Cette version améliorée bloque les informations confidentielles envoyées dans les courriers électroniques et les programmes de messagerie instantanée.

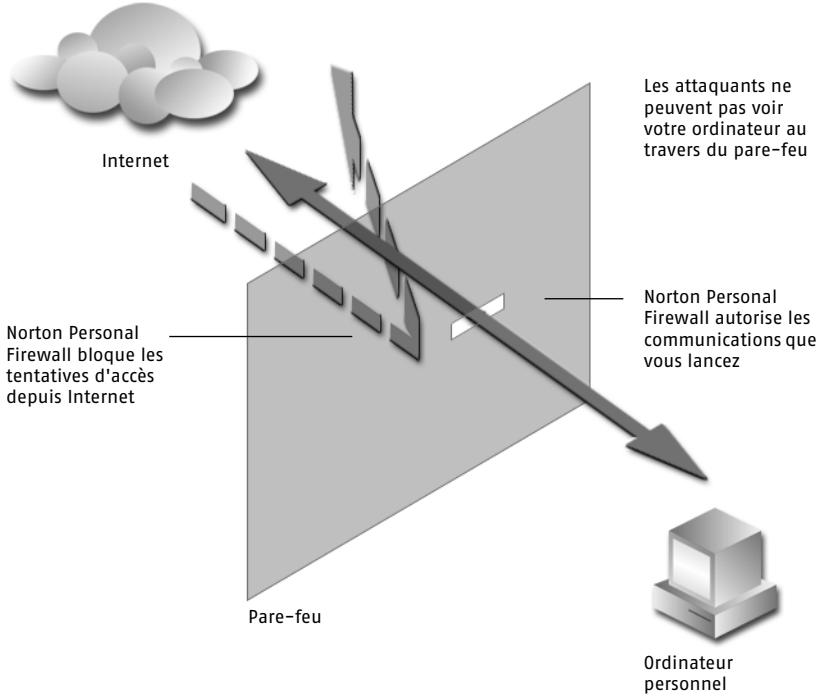
Fonctionnalités de Norton Personal Firewall

Norton Personal Firewall comprend plusieurs outils de sécurité qui contribuent à protéger votre ordinateur. Vous pouvez accéder rapidement à tous les outils de Norton Personal Firewall depuis Security Monitor.

La sécurité sur Internet peut s'avérer une question complexe. Norton Personal Firewall inclut désormais l'assistant Alerte, qui aide à comprendre les questions de sécurité, suggère des méthodes de résolution des problèmes et propose des conseils pour éviter les problèmes de sécurité.

A propos de Norton Personal Firewall

Norton Personal Firewall constitue une barrière de protection entre votre ordinateur et Internet. Un *pare-feu* interdit aux utilisateurs non autorisés d'accéder aux ordinateurs privés et aux réseaux connectés à Internet.



Norton Personal Firewall inclut des fonctionnalités qui interdisent l'accès non autorisé à votre ordinateur quand vous êtes sur Internet, détectent les attaques éventuelles, protègent vos informations personnelles et bloquent les publicités Internet pour accélérer votre navigation.

Fonctionnalités de Norton Personal Firewall

Détection d'intrusion	La fonction de Détection d'intrusion contribue à protéger votre ordinateur contre les attaques Internet en analysant chaque information qui entre sur votre ordinateur et en sort. Si elle identifie une attaque éventuelle, la Détection d'intrusion vous prévient et bloque automatiquement la connexion à l'origine de l'attaque. Se reporter à "Protection contre les tentatives d'intrusion" à la page 75.
Confidentialité	La fonction de Confidentialité propose différents niveaux de contrôle sur le type d'informations que les utilisateurs peuvent envoyer par le Web, le courrier électronique et les programmes de messagerie instantanée. Vous pouvez également contrôler la manière dont la fonction Confidentialité réagit lorsque des sites Web tentent de configurer et d'utiliser des cookies ou d'obtenir des informations sur votre navigateur. Se reporter à "Protection de votre confidentialité" à la page 99.
Blocage des publicités	Le Blocage des publicités accélère votre navigation sur le Web en éliminant les bannières publicitaires et autres contenus importuns ou lents à charger. Norton Personal Firewall bloque également les publicités créées avec Macromedia Flash et empêche les sites d'ouvrir des fenêtres de publicité déroulantes. Se reporter à "Blocage des publicités sur Internet" à la page 107.

Installation de Norton Personal Firewall

3

Avant d'installer Norton Personal Firewall, prenez le temps de vérifier la configuration requise décrite dans ce chapitre.

Configuration système requise

Pour utiliser Norton Personal Firewall, l'un des systèmes d'exploitation Windows suivants doit être installé sur l'ordinateur :

- Windows 98, 98SE
- Windows Me
- Windows 2000 Professional
- Windows XP Professional ou Windows XP Home Edition

Windows 95 et NT, les versions serveur de Windows 2000/XP et Windows XP version 64 bits ne sont pas pris en charge.

L'ordinateur doit également répondre aux spécifications suivantes.

Système d'exploitation	Configuration requise
Windows 98/ 98SE/Me	■ Processeur Intel Pentium (ou compatible) à 150 MHz ou supérieur ■ 48 Mo de RAM (64 Mo recommandés) ■ 25 Mo d'espace disque ■ Internet Explorer 5.01 ou ultérieur (5.5 recommandé) ■ Lecteur de CD-ROM ou de DVD-ROM
Windows 2000 Professional	■ Processeur Intel Pentium (ou compatible) à 150 MHz ou supérieur ■ 48 Mo de RAM (64 Mo recommandés) ■ 25 Mo d'espace disque ■ Internet Explorer 5.01 ou ultérieur (5.5 recommandé) ■ Lecteur de CD-ROM ou de DVD-ROM
Windows XP Professional ou Home Edition	■ Processeur Intel Pentium II (ou compatible) à 300 MHz ou supérieur ■ 48 Mo de RAM (64 Mo recommandés) ■ 25 Mo d'espace disque ■ Internet Explorer 5.01 ou ultérieur (5.5 recommandé) ■ Lecteur de CD-ROM ou de DVD-ROM

Clients de messagerie pris en charge

Norton Personal Firewall peut analyser les courriers électroniques pour rechercher des informations confidentielles dans tout client de messagerie compatible POP3, notamment :

- Microsoft® Outlook® Express 4.0/5.X
- Microsoft Outlook 97/98/2000/XP
- Netscape® Messenger 4.X, Netscape Mail 6.0
- Eudora® Light 3.0, Eudora Pro 4.0, Eudora 5.0

L'analyse du courrier électronique ne prend pas en charge les clients de messagerie suivants :

- Clients IMAP
- Clients AOL

- POP3 avec SSL (Secure Socket Layer)
- Courrier électronique Web comme Hotmail et Yahoo!
- Messagerie Lotus Notes

Clients de messagerie instantanée pris en charge

- AOL Instant Messenger, version 4.3 ou ultérieure
- MSN Instant Messenger, version 3.6 ou ultérieure
- Windows Messenger, version 4.0 ou ultérieure

Avant l'installation

Avant d'installer Norton Personal Firewall, préparez l'ordinateur.

Préparation de l'ordinateur

Se reporter à "Si vous devez désinstaller Norton Personal Firewall" à la page 32.

Si vous disposez d'une ancienne version de Norton Personal Firewall, la nouvelle version vous propose de la remplacer.

Avant d'installer Norton Personal Firewall, fermez tous les programmes Windows ouverts. D'autres programmes en cours d'exécution risqueraient d'entrer en conflit lors de l'installation et de diminuer la protection.

Si vous utilisez Windows XP

Windows XP inclut un *pare-feu* pouvant entrer en conflit avec les fonctions de protection de Norton Personal Firewall. Il est donc nécessaire de désactiver le pare-feu de Windows XP avant d'installer Norton Personal Firewall.

Pour désactiver le pare-feu de Windows XP

1. Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Panneau de configuration** > **Connexions réseau**.
2. Si vous avez créé plus d'une connexion modem ou réseau, sélectionnez la connexion active.
3. Cliquez sur **Tâches de réseau**.
4. Cliquez sur **Modifier les paramètres pour cette connexion**.
5. Dans la section Pare-feu pour la connexion Internet de l'onglet Avancés, désélectionnez l'option **Protéger mon ordinateur et le réseau en limitant l'accès à cet ordinateur depuis Internet**.

6 Cliquez sur **OK** pour fermer la fenêtre des paramètres.

7 Cliquez sur **OK** pour fermer la fenêtre Tâches de réseau.

Installation de Norton Personal Firewall

Installez Norton Personal Firewall depuis le Norton Personal Firewall CD. Installez un exemplaire de Norton Personal Firewall sur chaque ordinateur à protéger.

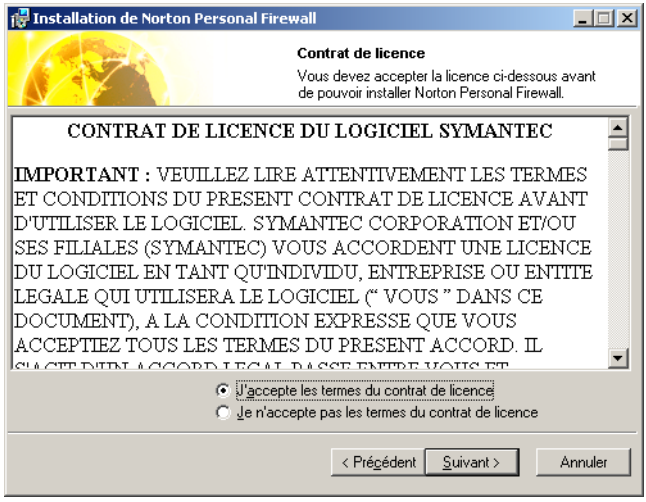
Pour installer Norton Personal Firewall

1 Insérez le Norton Personal Firewall CD dans le lecteur.

Se reporter à "Si l'écran d'ouverture n'apparaît pas" à la page 22.

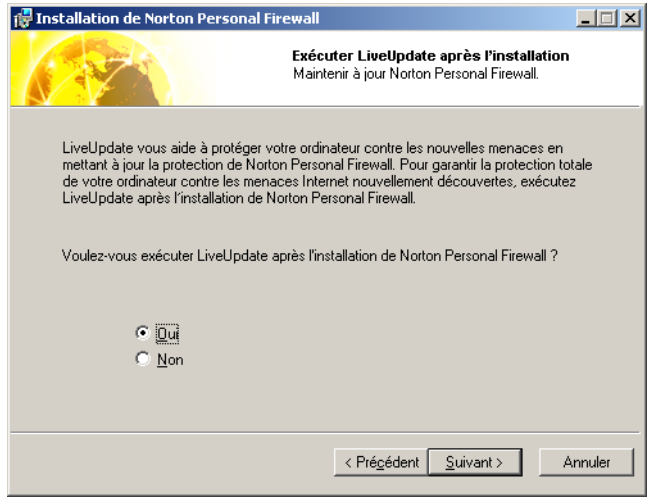
2 Dans la fenêtre du CD Norton Personal Firewall, cliquez sur **Installer Norton Personal Firewall**.
Si l'ordinateur n'est pas configuré pour exécuter automatiquement un CD, vous devez ouvrir le CD vous-même.
La première fenêtre d'installation vous rappelle de fermer tous les autres programmes Windows.

3 Cliquez sur **Suivant**.



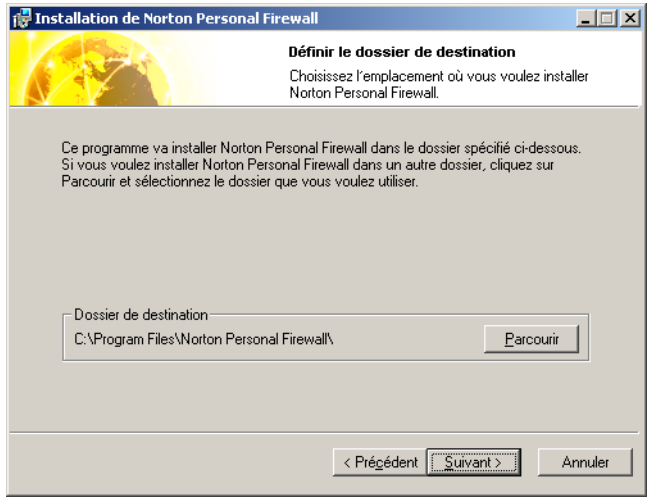
4 Lisez l'accord de licence et cliquez sur **J'accepte les termes du contrat de licence**.
Si vous n'acceptez pas les termes de l'accord, vous ne pourrez pas poursuivre l'installation.

5 Cliquez sur **Suivant**.



6 Dans la fenêtre Exécuter LiveUpdate après l'installation, décidez si vous souhaitez exécuter LiveUpdate à la fin de l'installation.

7 Cliquez sur **Suivant**.

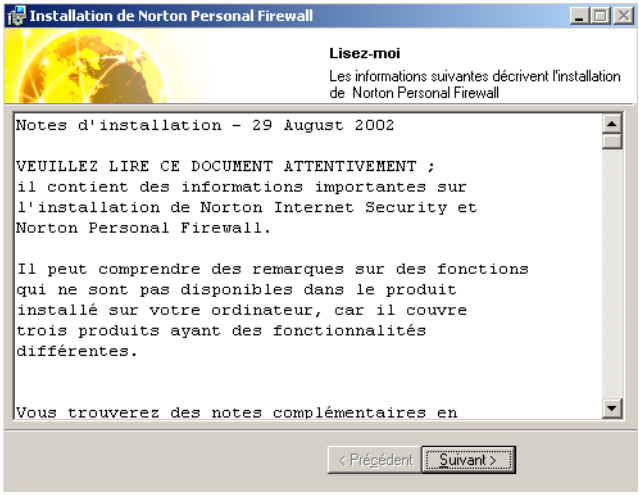


8 Cliquez sur **Parcourir** pour sélectionner le dossier dans lequel vous souhaitez installer Norton Personal Firewall, s'il s'agit d'un autre emplacement que celui par défaut.

9 Cliquez sur **Suivant**.

Se reporter à "Enregistrement du logiciel" à la page 23.

10 Cliquez sur **Suivant** pour commencer l'installation de Norton Personal Firewall.
Une fois Norton Personal Firewall installé, l'assistant Enregistrement apparaît.



11 Lisez le texte du fichier LisezMoi, puis cliquez sur **Suivant**.

12 Cliquez sur **Terminer** pour quitter l'installation.

Si l'écran d'ouverture n'apparaît pas

Il peut arriver que le lecteur de CD de l'ordinateur ne lance pas automatiquement le CD.

Pour démarrer l'installation depuis le CD Norton Personal Firewall

1 Sur votre bureau, cliquez deux fois sur **Poste de travail**.

2 Dans la boîte de dialogue Poste de travail, cliquez deux fois sur l'icône représentant le lecteur de CD.

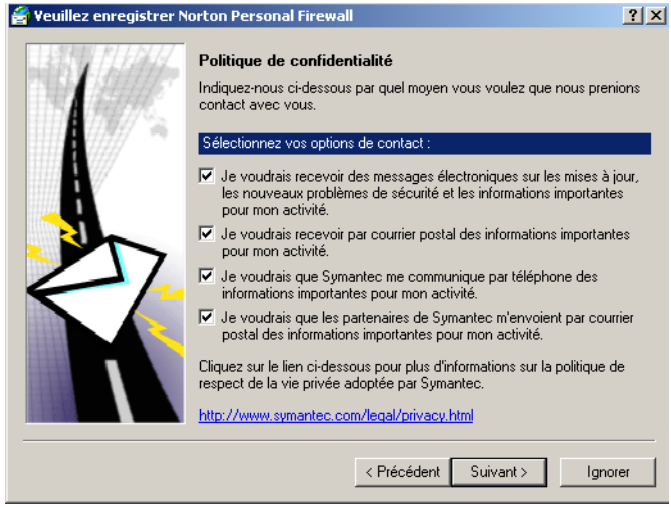
3 Dans la liste de fichiers, cliquez deux fois sur **Cdstart.exe**.

Enregistrement du logiciel

Utilisez l'assistant Enregistrement pour enregistrer votre logiciel en ligne. Si vous sautez l'enregistrement en ligne, vous pourrez l'effectuer ultérieurement avec l'option Enregistrement du menu Aide.

Pour enregistrer votre logiciel

1 Dans la première fenêtre d'enregistrement, sélectionnez le pays depuis lequel vous vous enregistrez et celui où vous vivez (s'il est différent), puis cliquez sur **Suivant**.



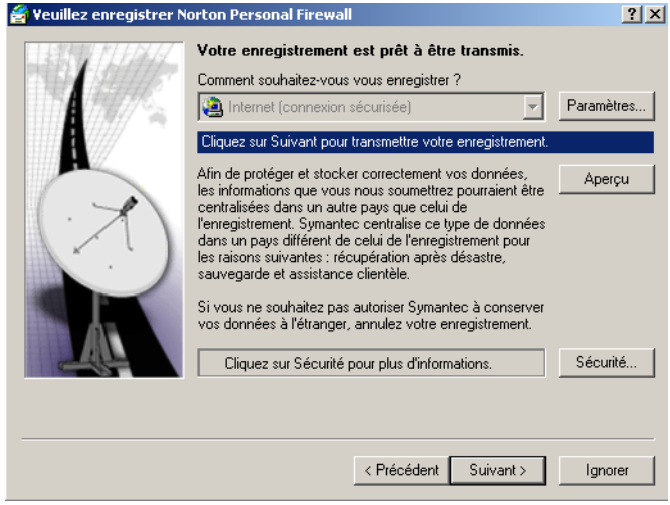
2 Si vous souhaitez obtenir des informations de Symantec sur Norton Personal Firewall, sélectionnez la méthode par laquelle vous voulez recevoir ces informations et cliquez sur **Suivant**.

3 Indiquez votre nom et cliquez sur **Suivant**.

4 Indiquez votre adresse et cliquez sur **Suivant**.

5 Effectuez l'une des opérations suivantes :

- Répondez au questionnaire afin d'aider Symantec à améliorer ses produits et services, puis cliquez sur **Suivant**.
- Sautez l'enquête en cliquant sur **Suivant**.



6 Choisissez l'enregistrement de Norton Personal Firewall par Internet ou par courrier.
Pour vous enregistrer par courrier, l'ordinateur doit être connecté à une imprimante que l'assistant Enregistrement utilisera pour imprimer le formulaire. Pour vous enregistrer par Internet, vous devez être connecté à Internet.

7 Cliquez sur **Suivant**.

8 Pour obtenir une copie de vos informations d'inscription pour référence ultérieure, effectuez l'une des opérations suivantes :

- Notez le numéro de série.
- Cliquez sur **Imprimer**.

9 Cliquez sur **Suivant**.

10 Choisissez si vous voulez utiliser votre profil existant pour l'enregistrement ultérieur d'un produit Symantec ou tapez les informations dans le cadre de l'enregistrement.

11 Cliquez sur **Terminer**.

Après l'installation

Une fois Norton Personal Firewall installé, une boîte de dialogue apparaît et vous donne la possibilité de redémarrer immédiatement l'ordinateur. Lorsque l'ordinateur a redémarré, l'assistant Sécurité apparaît et indique la marche à suivre pour configurer Norton Personal Firewall.

Redémarrage de l'ordinateur

Après l'installation, un message vous demande de redémarrer l'ordinateur pour que les modifications prennent effet.

Pour redémarrer l'ordinateur

❖ Dans la boîte de dialogue Informations du programme d'installation, cliquez sur **Oui**.
La configuration de Norton Personal Firewall n'est pas terminée tant que l'ordinateur n'a pas redémarré.

Utilisation de l'assistant Sécurité

L'assistant Sécurité vous aide à configurer rapidement votre protection Norton Personal Firewall. L'assistant Sécurité se divise en quatre catégories :

- Réseau personnel
- Contrôle des programmes
- Confidentialité
- Protection par mot de passe

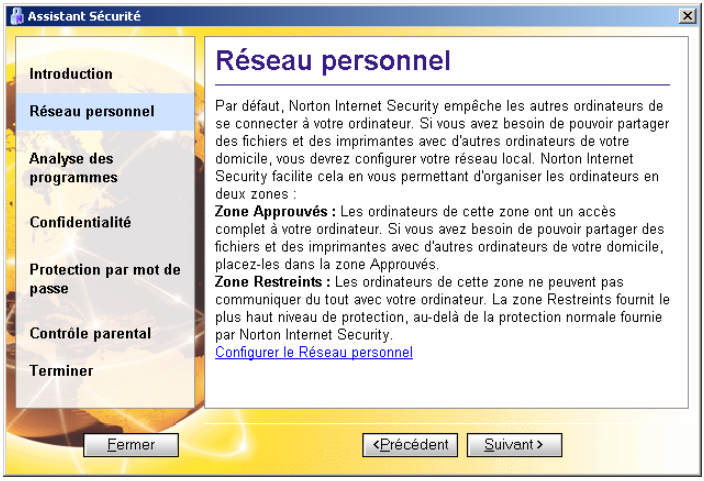
Configuration du Réseau personnel

Se reporter à "Connexion à un réseau" à la page 65.

Utilisez le Réseau personnel pour identifier les ordinateurs que vous savez inoffensifs et ceux dont vous souhaitez limiter l'accès à votre ordinateur. L'assistant de Contrôle de zone peut configurer automatiquement votre *réseau* et ajouter des ordinateurs à la zone Approuvés.

Pour configurer le Réseau personnel

1 Dans l'Itinéraire de l'assistant Sécurité, cliquez sur **Réseau personnel**.



2 Dans le volet Réseau personnel, cliquez sur **Configuration du Réseau personnel**.

3 Dans l'Assistant de Contrôle de zone, cliquez sur **Suivant**.

4 Suivez les instructions affichées pour configurer le réseau.

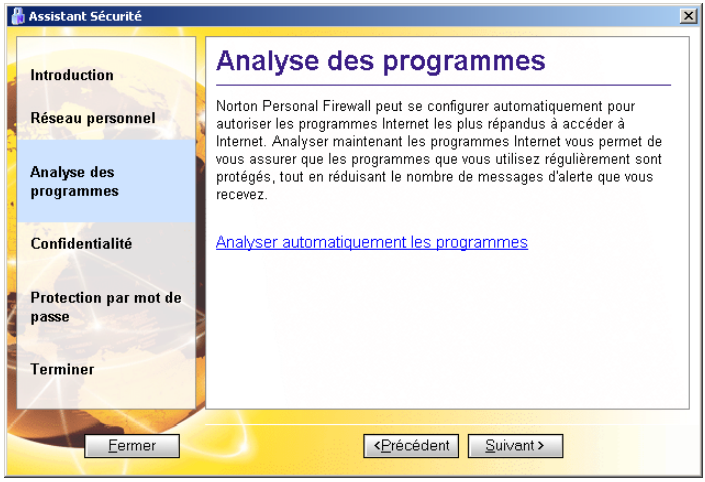
Configuration du Contrôle des programmes

Se reporter à "Recherche des applications utilisant Internet" à la page 84.

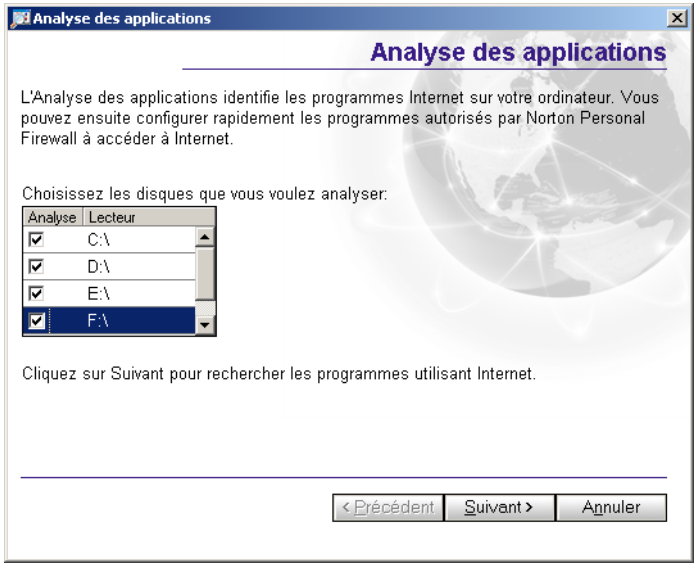
Norton Personal Firewall peut analyser votre ordinateur pour rechercher les applications capables d'accéder à Internet et créer des règles d'accès. Quand l'analyse est terminée, vous pouvez utiliser ses résultats pour déterminer quelles applications doivent accéder à Internet et, si nécessaire, ajuster leurs règles d'accès.

Pour configurer le Contrôle des programmes

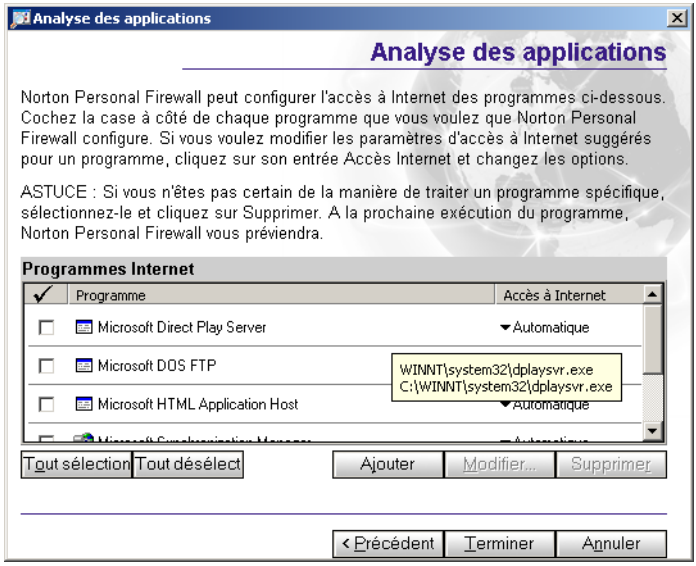
1 Dans l'Itinéraire de l'assistant Sécurité, cliquez sur **Analyse des applications**.



2 Sur le volet Analyse des applications, cliquez sur **Analyser les programmes automatiquement**.



3 Dans la fenêtre Analyse des applications, cliquez sur **Suivant** pour lancer l'analyse.
Lorsque l'analyse est terminée, toutes les applications qui se connectent à Internet sont indiquées.



4 Pour autoriser une application à accéder à Internet, cochez la case en regard de son nom.

5 Pour modifier la règle d'accès à Internet ou la catégorie d'une application, sélectionnez le paramètre souhaité dans la liste déroulante Accès à Internet ou Catégorie.

6 Cliquez sur **Terminer** lorsque vous avez fini.

Configuration de la Confidentialité

Se reporter à "Identification des informations confidentielles à protéger" à la page 100.

La fonction Confidentialité permet d'établir la liste des informations qui doivent bénéficier d'une protection supplémentaire. Le Contrôle de confidentialité empêche alors les utilisateurs d'envoyer des informations sur des *sites Web*, dans des *courriers électroniques*, dans des pièces jointes Microsoft Office files ou dans des programmes de messagerie instantanée.

Pour configurer le Contrôle de la confidentialité

1 Dans l'Itinéraire de l'Assistant Sécurité, cliquez sur **Confidentialité**.

2 Dans la fenêtre Confidentialité, cliquez sur **Ajouter des informations confidentielles à protéger**.

3 Dans la boîte de dialogue Ajouter des informations confidentielles, sélectionnez une catégorie dans la zone Type d'informations à protéger.

4 Dans le champ Nom descriptif, indiquez pour mémoire la raison pour laquelle vous souhaitez protéger ces données.

5 Dans le champ Informations à protéger, tapez les cinq ou sic derniers caractères de l'information dont vous souhaitez empêcher la transmission sur des connexions Internet non sécurisées.
En indiquant seulement des informations partielles, vous évitez que des individus malhonnêtes accédant à votre ordinateur ne dérobe des informations complètes.

6 Cliquez sur **OK**.

Cliquez sur Protection par mot de passe

Se reporter à "Utilisation de Security Monitor" à la page 38.

Pour une sécurité optimale, il est recommandé d'exiger un *mot de passe* avant toute modification des paramètres de Norton Personal Firewall. Cela vous garantit que seul des personnes de confiance pourront désactiver la protection, le *pare-feu* et la Détection d'intrusion ou apporter des modifications aux options de Norton Personal Firewall.

Pour protéger les options de Norton Personal Firewall avec un mot de passe

1 Dans l'Itinéraire de l'assistant Sécurité, cliquez sur **Protection par mot de passe**.

2 Dans le volet Protection par mot de passe, cliquez sur **Activer la protection par mot de passe**.

3 Dans les champs Mot de passe et Confirmation du mot de passe, saisissez un mot de passe.

4 Cliquez sur **OK**.

Si Norton SystemWorks est installé

Si Norton SystemWorks est installé sur votre ordinateur quand vous installez Norton Personal Firewall, le programme d'installation ajoute un onglet Norton Personal Firewall à la fenêtre principale de Norton SystemWorks et un onglet a Norton SystemWorks à Security Center.

Pour installer Norton Personal Firewall depuis Norton SystemWorks

1 Ouvrez Norton SystemWorks.

2 Sur l'onglet Norton Personal Firewall, cliquez sur **Lancer Norton Personal Firewall**.

Pour ouvrir Norton SystemWorks depuis Norton Personal Firewall

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre Norton SystemWorks 2002, cliquez sur **Lancer Norton SystemWorks**.

Si vous devez désinstaller Norton Personal Firewall

Si vous avez besoin de supprimer Norton Personal Firewall de l'ordinateur, ouvrez le menu Démarrer de Windows et utilisez l'option Désinstallation de Norton Personal Firewall.

Au cours de la désinstallation, Windows peut indiquer qu'il effectue l'installation d'un logiciel. Il s'agit d'un message général du programme d'installation de Microsoft, dont vous pouvez ne pas tenir compte.

Pour désinstaller Norton Personal Firewall

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Norton Personal Firewall** > **Désinstaller Norton Personal Firewall**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Autres programmes** > **Norton Personal Firewall** > **Désinstallation de Norton Personal Firewall**.
2. Cliquez sur **Suivant**.
3. Dans la boîte de dialogue Informations du programme d'installation, cliquez sur **Oui** pour redémarrer l'ordinateur.

Si aucun autre produit Symantec ne se trouve sur l'ordinateur, vous devez également désinstaller LiveReg et LiveUpdate.

Pour désinstaller LiveReg et LiveUpdate

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Panneau de configuration**.
2. Dans le Panneau de configuration, cliquez deux fois sur **Ajout/ Suppression de programmes**.

3. Dans la liste des programmes actuellement installés, sélectionnez **LiveReg**.
4. Effectuez l'une des opérations suivantes :
   - Sous Windows 2000/Me, cliquez sur **Modifier/Supprimer**.
   - Sous Windows 98, cliquez sur **Ajouter/Supprimer**.
   - Dans Windows XP, cliquez sur **Supprimer**.
5. Cliquez sur **Oui** pour confirmer la désinstallation du produit.
6. Pour désinstaller LiveUpdate, répétez les étapes 1 à 5 en sélectionnant LiveUpdate à l'étape 3.

Bases de Norton Personal Firewall

4

Après son installation, Norton Personal Firewall protège automatiquement l'ordinateur sur lequel il est installé. Vous n'avez pas besoin de lancer le programme pour activer la protection.

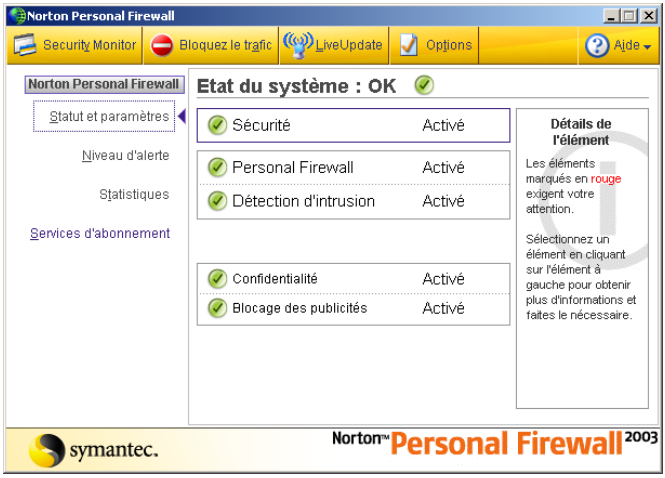
Accès à Norton Personal Firewall

Lancez Norton Personal Firewall afin de modifier les paramètres de protection ou de contrôler ses activités.

Pour accéder à Norton Personal Firewall

- Effectuez l'une des opérations suivantes :
  - Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Norton Personal Firewall** > **Norton Personal Firewall**.
  - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer**> **Autres programmes** > **Norton Personal Firewall** > **Norton Personal Firewall**.

- Sur le Bureau de Windows, cliquez deux fois sur **Norton Personal Firewall**.



Accès à Norton Personal Firewall depuis la barre d'état système

Norton Personal Firewall ajoute une icône à la barre d'état système de Windows. Sur la plupart des ordinateurs, la barre d'état est située à l'extrême droite de la barre des tâches de Windows en bas de l'écran. Cliquez sur cette icône pour ouvrir un menu qui contient les outils de Norton Personal Firewall fréquemment utilisés.

Pour utiliser le menu de la barre d'état système de Norton Personal Firewall

1. Dans la barre d'état système, cliquez avec le bouton droit sur l'icône de Norton Personal Firewall.
2. Dans le menu qui apparaît, sélectionnez un élément. Les éléments du menu sont les suivants :

Norton Personal Firewall	Ouvre une fenêtre Norton Personal Firewall.
Pour masquer/ afficher AlertTracker	Affiche ou masque Alert Tracker. Se reporter à "Utilisation d'Alert Tracker" à la page 41.

Bloquer le trafic	Arrête immédiatement toutes les informations entrantes et sortantes. Se reporter à "Arrêt d'une communication Internet avec la fonction Bloquer le trafic" à la page 45.
A propos de Norton Personal Firewall	Affiche des informations détaillées sur les composants de Norton Personal Firewall.
LiveUpdate	Met à jour votre protection. Se reporter à "Mises à jour avec LiveUpdate" à la page 57.
Aide	Affiche l'aide en ligne de Norton Personal Firewall. Se reporter à "Utilisation de l'aide en ligne" à la page 50.
Désactiver	Désactive toutes les fonctions de protection de Norton Personal Firewall. Se reporter à "Désactivation temporaire de Norton Personal Firewall" à la page 49.

Se reporter à "A propos des paramètres globaux" à la page 48.

Utilisez les options de Norton Personal Firewall pour ajouter d'autres outils au menu.

Utilisation de Norton Personal Firewall

Norton Personal Firewall fonctionne en arrière-plan, ce qui vous donne la possibilité d'agir sur le programme uniquement lorsqu'il vous avertit d'une nouvelle *connexion* réseau ou d'un problème potentiel. Vous pouvez choisir d'afficher le nouveau Security Monitor ou la fenêtre standard de Security Center, de répondre aux problèmes de sécurité et de contrôler le nombre d'*alertes* que vous recevez ainsi que la manière dont le programme résout les problèmes de sécurité potentiels.

Accès aux fonctions de protection de Norton Personal Firewall

Les paramètres par défaut de Norton Personal Firewall offrent une méthode sûre, automatique et efficace pour protéger votre ordinateur. Si vous voulez modifier ou personnaliser votre protection, vous pouvez accéder à tous les outils de Norton Personal Firewall depuis la fenêtre Statut et paramètres.

Pour modifier les paramètres de fonctions individuelles

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, effectuez l'une des opérations suivantes :
   - Cliquez deux fois sur une fonction que vous souhaitez personnaliser.
   - Sélectionnez une fonction, puis dans l'angle inférieur droit de la fenêtre, cliquez sur **Personnaliser**.
3. Configurez la fonction.
4. Lorsque que vous avez terminé les modifications, cliquez sur **OK**.

Utilisation de Security Monitor

Security Monitor rassemble les outils de Norton Personal Firewall les plus utilisés dans une fenêtre compacte. Lorsque vous êtes en ligne, placez la fenêtre de Security Monitor dans une partie inutilisée de l'écran. Ceci vous permet de surveiller votre *connexion*, d'afficher des informations sur les événements de sécurité et de personnaliser votre protection sans nécessiter beaucoup d'espace à l'écran.

A son démarrage, Norton Personal Firewall lance Security Center. Vous pouvez ensuite basculer dans la fenêtre de Security Monitor.

Pour afficher la fenêtre de Security Monitor

- Dans l'angle supérieur gauche de la fenêtre Security Center, cliquez sur **Security Monitor**.

Pour afficher la fenêtre Security Center

- Dans l'angle supérieur gauche de la fenêtre Security Monitor, cliquez sur **Security Center**.

Sélection d'une tâche avec Security Monitor

Utilisez le menu Sélectionner une tâche de Security Monitor pour exécuter rapidement les tâches courantes de Norton Personal Firewall. Le menu Sélectionner une tâche inclut les éléments suivants :

Tâche	Plus d'informations
Test de la sécurité	Se reporter à "Vérification de la vulnérabilité de l'ordinateur aux attaques" à la page 43.
Modification d'informations personnelles	Se reporter à "Protection de votre confidentialité" à la page 99.
Affichage de la visionneuse du journal	Se reporter à "Affichage des journaux de Norton Personal Firewall" à la page 120.
Exécution de LiveUpdate	Se reporter à "Mises à jour avec LiveUpdate" à la page 57.
Exécution de l'analyse de programme	Se reporter à "Recherche des applications utilisant Internet" à la page 84.
Configuration du réseau personnel	Se reporter à "Organisation des ordinateurs en zones de réseau" à la page 67.

Réponse aux alertes de Norton Personal Firewall

Norton Personal Firewall surveille les communications entrantes et sortantes et vous avertit lorsqu'une activité quelconque risque de compromettre votre sécurité.

Lorsqu'une *alerte* se produit, lisez le message avant de prendre une décision. Identifiez le type d'alerte et le niveau de menace. Quand vous avez évalué les risques, faites un choix.

Prenez le temps nécessaire avant de prendre votre décision. Tant que l'alerte est active, votre ordinateur est à l'abri des attaques.

Norton Personal Firewall vous permet de choisir une action appropriée en présélectionnant l'action recommandée s'il en existe une. Norton Personal Firewall ne peut pas suggérer d'actions recommandées pour toutes les alertes.

Informations complémentaires avec l'Assistant Alerte

Chaque alerte Norton Personal Firewall inclut un lien vers l'Assistant Alerte. L'Assistant Alerte comprend des informations personnalisées sur chaque alerte, notamment :

- Le type d'alerte
- Le niveau de menace
- La communication qui a déclenché cette alerte
- Ce que ces types d'alerte indiquent
- Le moyen de réduire le nombre de ces alertes

Pour utiliser l'Assistant Alerte

1. Dans une fenêtre d'alerte quelconque, cliquez sur le bouton Assistant Alerte.
2. Dans la fenêtre Assistant Alerte, examinez les informations sur cette alerte.
3. Pour répondre à l'alerte, fermez l'Assistant Alerte.

Réglage du niveau d'alerte

Le curseur du niveau d'alerte vous permet de contrôler la quantité d'informations que Norton Personal Firewall consigne dans des *journaux*, ainsi que le nombre d'alertes qu'il affiche.

Les options sont les suivantes :

Niveau d'alerte	Informations fournies	Messages Alert Tracker	Alertes de sécurité	Vous informe quand...
Minimum	Evénements Internet critiques	Aucun	Consigné, non affiché	Les règles de contrôle de programme sont créées automatiquement. Des analyses de port sont exécutées. Des informations confidentielles sont bloquées. Un programme de cheval de Troie d'accès distant est rencontré.

Niveau d'alerte	Informations fournies	Messages Alert Tracker	Alertes de sécurité	Vous informe quand...
Moyen	Evénements Internet importants	Certains	Consigné, non affiché	Mêmes notifications que pour Minimum, plus : ■ Programmes accédant à Internet.
Haut	Evénements Internet importants et activités de programme complètes	Nombre élevé	Consigné et affiché	Mêmes notifications que pour Moyen, plus : ■ Les ports inutilisés sont bloqués. ■ Les cookies et les contenus sont bloqués.

Pour régler le niveau d'alerte

1 Ouvrez Norton Personal Firewall.

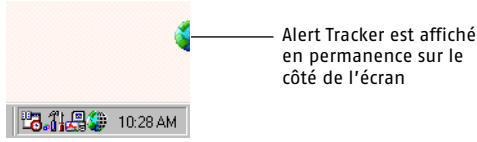
2 Dans Security Center, cliquez sur **Niveau d'alerte**.

3 Déplacez le curseur pour sélectionner un niveau d'alerte.

Utilisation d'Alert Tracker

De nombreux événements Internet surveillés par Norton Personal Firewall ne justifient pas le déclenchement d'une alerte. Alert Tracker fournit une méthode simple pour surveiller ces événements de sécurité moins importants.

Alert Tracker affiche les mêmes informations que celles qui apparaissent dans le champ Evénement de sécurité de Security Monitor. Ceci vous permet de surveiller la sécurité de votre ordinateur sans avoir à laisser Security Monitor visible en permanence. Alert Tracker fournit également une méthode rapide pour supprimer les publicités sur des *pages Web*.



Si vous choisissez de l'afficher, Alert Tracker s'ancre à l'un ou l'autre des côtés de l'écran principal. Lorsqu'un événement de sécurité survient, Alert Tracker affiche un message pendant quelques secondes, puis reprend sa place sur le côté de l'écran. Si vous n'avez pas pu voir un message Alert Tracker, vous pouvez consulter la liste des messages récents.

Les messages Alert Tracker sont affichés pendant quelques secondes

Alert Tracker comporte également la Corbeille publicitaire, qui fait partie de la fonction Blocage des publicités de Norton Personal Firewall.

Se reporter à "Utilisation de la Corbeille publicitaire" à la page 111.

Pour afficher ou masquer Alert Tracker

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Général, effectuez l'une des opérations suivantes :
   - Cochez l'option **Afficher Alert Tracker** pour afficher Alert Tracker.
   - Désélectionnez l'option **Afficher Alert Tracker** pour masquer Alert Tracker.
4. Cliquez sur **OK**.

Pour consulter les messages récents d'Alert Tracker

1. Sur le Bureau de Windows, cliquez deux fois sur Alert Tracker.
2. A droite du premier message, cliquez sur la flèche si elle apparaît.
3. Cliquez deux fois sur une entrée pour ouvrir la visionneuse du journal.

Se reporter à "Affichage des statistiques détaillées" à la page 118.

Pour déplacer Alert Tracker

- Faites glisser l'hémisphère vers le côté de l'écran sur lequel vous voulez le placer.

Pour afficher ou masquer Alert Tracker dans le menu de la barre d'état système

- Dans la barre d'état système de Windows, cliquez avec le bouton droit sur l'icône du Norton Personal Firewall, puis effectuez l'une des opérations suivantes :
  - Cliquez sur **Masquer Alert Tracker** pour masquer Alert Tracker.
  - Cliquez sur **Afficher Alert Tracker** pour afficher Alert Tracker.

Si vous masquez Alert Tracker, aucune notification ne sera affichée lorsque l'ordinateur se connectera à un *réseau*. Les informations relatives à la *connexion* seront toujours présentes dans les *journaux*.

Vérification de la vulnérabilité de l'ordinateur aux attaques

Utilisez Security Check pour vérifier la vulnérabilité de votre ordinateur face aux intrusions. Le lien Security Check dans Norton Personal Firewall vous connecte au *site Web* de Symantec, qui vous permet de rechercher les vulnérabilités et d'obtenir des informations détaillées sur les analyses de Security Check.

Vous devez être connecté à Internet pour vérifier la vulnérabilité de votre ordinateur.

Pour vérifier la vulnérabilité de l'ordinateur aux attaques

1. Ouvrez Norton Personal Firewall.
2. Effectuez l'une des opérations suivantes :
   - Dans Security Center, cliquez sur **Sécurité**, puis sur **Contrôler la sécurité**.
   - Dans le menu Sélectionner une tâche Security Monitor, cliquez sur **Tester la sécurité**.
3. Dans la page Web Security Check, cliquez sur **Analyse des risques en matière de sécurité**.
4. Pour plus d'informations sur les tests de Security Check, cliquez sur **A propos de l'analyse des risques en matière de sécurité**.

Lorsque l'analyse est terminée, la page de résultats répertorie toutes les zones contrôlées, ainsi que votre niveau de vulnérabilité dans chacune. Pour chaque zone à risque, vous pouvez obtenir davantage de détails sur le problème et la manière de le résoudre.

Pour obtenir davantage d'informations sur une zone à risque

- Dans la page des résultats, cliquez sur **Afficher les détails** à côté du nom de l'analyse.

Identification de la source de communications

Visual Tracking vous aide à en savoir plus sur les ordinateurs qui tentent de se connecter à votre ordinateur. Grâce à Visual Tracking, vous pouvez identifier l'emplacement de l'*adressee IP* utilisée et des informations de contact sur le propriétaire de l'adresse. Vous pouvez utiliser ces informations pour déterminer l'origine d'une attaque et vous informer sur les tentatives d'intrusion.

Vous pouvez suivre les *tentatives de connexion* à partir de trois emplacements dans Norton Personal Firewall :

- Statistiques
- Visionneuse du journal
- AutoBlock

Pour suivre une tentative de connexion depuis les statistiques

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez sur **Statistiques**.
3. Cliquez sur **Détails de l'attaquant**.
   Votre navigateur ouvre la page Web Visual Tracking.

Pour suivre une tentative de connexion depuis la visionneuse du journal

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez sur **Statistiques**.
3. Cliquez sur **Afficher le journal**.
4. Dans la colonne gauche de la fenêtre de la visionneuse du journal, sous Sécurité Internet, cliquez sur **Connexion**.
5. Dans la colonne droite de la fenêtre de la visionneuse du journal, sélectionnez la connexion que vous souhaitez suivre.

6 En bas de la fenêtre de la visionneuse du journal, cliquez sur l'adresse IP ou le nom de l'ordinateur.
Votre navigateur ouvre la page Web Visual Tracking.

Pour suivre une tentative de connexion depuis AutoBlock

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.

3 Dans la section AutoBlock de la fenêtre Détection d'intrusion, sélectionnez une connexion que vous souhaitez suivre.

4 Cliquez sur **Détails de l'attaquant**.
Votre navigateur ouvre la page Web Visual Tracking.

Lorsque Visual Tracking est terminé, il affiche une représentation visuelle de l'origine de cette communication et des informations de contact concernant le propriétaire de l'adresse IP.

Arrêt d'une communication Internet avec la fonction Bloquer le trafic

Les fenêtres Security Center et Security Monitor comportent un bouton Bloquer le trafic qui vous permet d'interrompre immédiatement une communication entre votre ordinateur et un autre. Ce bouton peut être pratique pour limiter les dommages éventuels sur votre ordinateur en cas d'attaque, si un *cheval de Troie* envoie des informations confidentielles à votre insu ou si vous autorisez par mégarde une personne peu fiable à accéder aux fichiers stockés sur votre ordinateur.

Lorsque cette option est active, Norton Personal Firewall bloque toutes les communications entrantes et sortantes. De l'extérieur, votre ordinateur semble totalement déconnecté d'Internet.

Si vous voulez bloquer tout le trafic entrant et sortant, la fonction Bloquer le trafic est plus efficace que le fait d'utiliser simplement votre logiciel Internet pour vous déconnecter. La plupart des programmes Internet étant capables de se connecter automatiquement sans aucune intervention de l'utilisateur, un programme malveillant pourrait se reconnecter en votre absence.

La fonction Bloquer le trafic est sensée servir de mesure temporaire pendant que vous résolvez un problème de sécurité. Si vous redémarrez l'ordinateur, Norton Personal Firewall autorise automatiquement toutes les communications entrantes et sortantes. Pour continuer à bloquer le trafic, cliquez sur le bouton Bloquer le trafic dans Security Center ou Security Monitor.

Pour éviter les attaques pendant la résolution d'un problème de sécurité

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre Security Center ou Security Monitor, cliquez sur **Bloquer le trafic**.
3. Utilisez les outils Norton Personal Firewall pour résoudre le problème de sécurité.
4. Une fois le problème résolu, cliquez sur **Autoriser le trafic**.

Personnalisation de Norton Personal Firewall

Les paramètres par défaut de Norton Personal Firewall offrent une protection appropriée à la majorité des utilisateurs. Si vous devez effectuer des modifications, utilisez le menu Options pour accéder aux options Norton Personal Firewall. Les options vous permettent de contrôler des paramètres plus avancés.

Si vous utilisez Windows 2000/XP, et que vous ne disposez pas des droits d'accès administrateur local, vous ne pouvez pas modifier les options Norton Personal Firewall.

Pour personnaliser Norton Personal Firewall

1. Ouvrez Norton Personal Firewall.
2. En haut de la fenêtre de Security Center, cliquez sur **Options**.
3. Sélectionnez l'onglet sur lequel vous souhaitez modifier des options.

A propos des options générales

Les options générales vous permettent de contrôler le moment d'exécution de Norton Personal Firewall, de protéger les paramètres du programme par un *mot de passe* et de sélectionner les éléments visuels à afficher.

A propos des options générales

Se reporter à "Mises à jour avec LiveUpdate" à la page 57.

Les options LiveUpdate vous permettent d'activer et de désactiver la fonction LiveUpdate automatique, qui recherche automatiquement les mises à jour de Norton Personal Firewall lorsque vous vous connectez à Internet. Pour une sécurité optimale, laissez cette option sélectionnée.

Vous pouvez sélectionner les composants Norton Personal Firewall que LiveUpdate automatique doit surveiller. Vous pouvez également indiquer à LiveUpdate automatique de mettre à jour les composants en arrière-plan ou de vous avertir lorsque des mises à jour sont disponibles.

A propos des options du pare-feu

Les options du pare-feu vous permettent d'activer des fonctions de protection avancées et de personnaliser les ports utilisés par votre ordinateur pour afficher les *pages Web*. La plupart des utilisateurs n'ont pas besoin de modifier ces paramètres.

A propos des options des contenus Web

Les options des contenus Web vous permettent de contrôler comment Norton Personal Firewall gère les contenus interactifs en ligne, les publicités et les intrusions de confidentialité éventuelles. Ces options sont classées en trois onglets.

A propos des paramètres globaux

Les paramètres globaux vous permettent de contrôler les actions par défaut que Norton Personal Firewall entreprend lorsque des sites Web tentent d'obtenir des informations sur votre *navigateur* ou d'utiliser des image animées, des scripts Java et autres *contenus actifs*.

A propos des paramètres utilisateur

Les paramètres utilisateurs vous permettent de personnaliser le blocage des *cookies*, des fenêtres déroulantes ainsi que les paramètres *ActiveX* et *Java* pour des sites individuels.

A propos des paramètres du blocage des publicités

Se reporter à "Utilisation des chaînes de texte pour identifier les publicités à bloquer ou à autoriser" à la page 112.

Les paramètres du blocage des publicités vous permettent de spécifier les *bannières publicitaires* individuelles ou les groupes d'images publicitaires que vous souhaitez interdire ou autoriser sur des sites spécifiques.

A propos des options de messagerie

Les options de *messagerie* vous permettent de contrôler la manière dont Norton Personal Firewall vous avertir quand il recherche dans les messages électroniques des informations confidentielles.

Options de protection par mot de passe

Vous pouvez protéger les options de Norton Personal Firewall par un *mot de passe*. Ainsi, seules les personnes fiables sont à même de modifier vos options.

Pour protéger les options de Norton Personal Firewall par un mot de passe

1. Ouvrez Norton Personal Firewall.
2. En haut de la fenêtre de Norton Personal Firewall, cliquez sur **Options > Sécurité Internet**.
3. Sur l'onglet Général, cochez **Activer la protection par mot de passe**.
4. Tapez un mot de passe dans les zones de texte Mot de passe et Confirmation du mot de passe.
5. Cliquez sur **OK**.

Réinitialisation du mot de passe des options

Si vous oubliez le mot de passe de vos options, vous pouvez le redéfinir.

Pour redéfinir le mot de passe des options Norton Personal Firewall

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Norton Personal Firewall** > **Désinstallation de Norton Personal Firewall**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Autres programmes** > **Norton Personal Firewall** > **Désinstallation de Norton Personal Firewall**.
2. Dans la fenêtre Suppression d'application, cliquez sur **Réinitialiser le mot de passe**.
3. Dans la zone de texte Réinitialiser la clé de mot de passe de la boîte de dialogue de réinitialisation du mot de passe, tapez la clé correspondante qui apparaît au-dessus de la zone de texte.
   La clé de réinitialisation du mot de passe est sensible à la casse.
4. Tapez un nouveau mot de passe dans les zones de texte Nouveau mot de passe et Confirmer le nouveau mot de passe.
5. Cliquez sur **OK**.
6. Dans la fenêtre Suppression d'application, cliquez sur **Annuler**.
7. Dans l'alerte Norton Personal Firewall, cliquez sur **Quitter**.
8. Dans l'alerte Installation annulée, cliquez sur **OK**.

Désactivation temporaire de Norton Personal Firewall

Il peut y avoir des cas où vous souhaiterez désactiver temporairement Norton Personal Firewall ou l'une de ses fonctionnalités. Par exemple, vous pouvez souhaiter afficher des publicités en ligne ou vérifier si Norton Personal Firewall empêche l'affichage d'une *page Web*.

La désactivation de Norton Personal Firewall désactive également l'ensemble des fonctionnalités individuelles.

Pour désactiver temporairement Norton Personal Firewall

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez sur **Sécurité**.
3. Sur le côté droit de l'écran, cliquez sur **Désactiver**.

Norton Personal Firewall est automatiquement réactivé au prochain démarrage de l'ordinateur.

Vous pouvez également désactiver des fonctions de sécurité individuelles. Par exemple, vous pouvez vérifier si Personal Firewall entrave le bon fonctionnement d'un programme.

Pour désactiver une fonction de protection

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, sélectionnez la fonction à désactiver.
3. Sur le côté droit de l'écran, cliquez sur **Désactiver**.

Pour plus d'informations

Norton Personal Firewall fournit sur le *Web* des termes de glossaire, une aide en ligne, ce guide de l'utilisateur au format PDF, des didacticiels ainsi que des liens vers la base de connaissances du *site Web* de Symantec.

Recherche des termes de glossaire

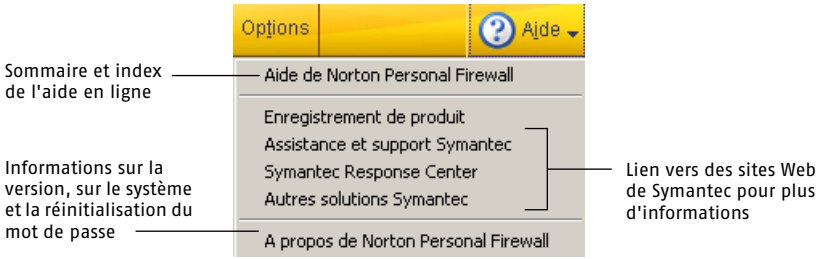
Les termes techniques indiqués en italiques dans le guide de l'utilisateur sont définis dans le glossaire disponible dans le fichier PDF du guide et dans l'aide. A ces deux emplacements, le fait de cliquer sur un terme vous donne sa définition.

Utilisation de l'aide en ligne

L'aide est en permanence disponible dans Norton Personal Firewall. Des boutons d'aide ou des liens vers des informations complémentaires fournissent des détails spécifiques à la tâche que vous effectuez. Le menu Aide vous offre un guide exhaustif pour toutes les fonctionnalités de produit et les tâches que vous pouvez effectuer.

Pour accéder à l'aide

1 En haut de la fenêtre Security Center, cliquez sur **Aide**.



2 Dans le menu principal de l'aide, cliquez sur **Aide Norton Personal Firewall**.

3 Dans le volet gauche de la fenêtre d'aide, sélectionnez l'un des onglets suivants :

- Sommaire : Affiche l'aide par rubrique.
- Index : Affiche les rubriques d'aide par mot clé et par ordre alphabétique.
- Rechercher : Ouvre un champ de recherche qui vous permet de saisir un mot ou une phrase.

Aide sur les fenêtres et les boîtes de dialogue

L'aide sur les fenêtres et les boîtes de dialogue fournit des informations sur le programme Norton Personal Firewall. Ce type d'aide est contextuel : l'aide affichée concerne la boîte de dialogue ou la fenêtre utilisée.

Pour accéder à l'aide sur les fenêtres et les boîtes de dialogue

❖ Effectuez l'une des opérations suivantes :

- Cliquez sur le lien **Plus d'infos** s'il est disponible.
- Dans la boîte de dialogue, cliquez sur **Aide**.

Fichier LisezMoi et notes de version

Le fichier LisezMoi contient des informations sur des questions d'installation et de compatibilité. Les notes de version contiennent des conseils techniques et des informations sur des modifications du produit intervenues après l'impression du présent manuel. Elles sont installées sur votre disque dur au même emplacement que les fichiers de Norton Personal Firewall.

Pour consulter le fichier LisezMoi

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer > Programmes > Norton Personal Firewall > Support produit> LisezMoi.txt**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer > Autres programmes > Norton Personal Firewall > Support produit > LisezMoi.txt**.

   Le fichier s'ouvre dans le Bloc-notes.
2. Une fois que vous avez fini de lire le fichier, fermez le traitement de texte.

Les notes de version sont également accessibles depuis le menu Démarrer.

Pour lire les notes de version

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer > Programmes > Norton Personal Firewall > Support produit > Norton Personal Firewall Notes de version**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer > Autres programmes > Norton Personal Firewall > Support produit > Norton Personal Firewall Notes de version**.

   Le fichier s'ouvre dans le Bloc-notes.
2. Une fois que vous avez fini de lire le fichier, fermez le traitement de texte.

Accès à la version PDF du guide de l'utilisateur

Ce guide de l'utilisateur est fourni sur le CD Norton Personal Firewall au format PDF. Pour pouvoir lire le PDF, vous devez installer Adobe Acrobat Reader sur l'ordinateur.

Pour installer Adobe Acrobat Reader

1. Insérez le CD Norton Personal Firewall dans le lecteur de CD-ROM.
2. Cliquez sur **Parcourir le CD**.
3. Cliquez deux fois sur le dossier **Manual**.
4. Cliquez deux fois sur le dossier **Acrobat**.
5. Cliquez deux fois sur **ar500enu.exe**.
6. Suivez les instructions affichées pour sélectionner un dossier de destination pour Adobe Acrobat Reader et terminer l'installation.

Une fois Adobe Acrobat Reader installé, vous pouvez lire le fichier PDF depuis le CD.

Pour lire la version PDF du guide de l'utilisateur depuis le CD

1. Insérez le CD Norton Personal Firewall dans le lecteur de CD-ROM.
2. Cliquez sur **Parcourir le CD**.
3. Cliquez deux fois sur le dossier **Manual**.
4. Cliquez deux fois sur **NPF2003.pdf**.

Vous pouvez également copier le guide de l'utilisateur sur le disque dur et le lire depuis ce disque. Nécessite environ 2,25 Mo d'espace disque.

Pour lire le guide de l'utilisateur depuis le disque dur

1. Accédez à l'emplacement où vous avez copié le fichier PDF.
2. Cliquez deux fois sur **NPF2003.pdf**.

A propos de Norton Personal Firewall sur le Web

Le site Web de Symantec fournit des informations complètes sur Norton Personal Firewall. Il existe différents moyens d'accéder au site Web de Symantec.

Pour accéder au site Web Symantec à partir de la fenêtre principale de Norton Personal Firewall

1. Cliquez sur **Aide**.
2. Sélectionnez l'une des options suivantes :
   - Site Web de support technique : vous amène à la page de support technique du site Web de Symantec, où vous pouvez rechercher des solutions à des problèmes spécifiques, mettre à jour la protection antivirus et lire les dernières informations sur les technologies antivirus.
   - Visitez le site Web de Symantec : vous amène à la page d'accueil du site Web de Symantec, qui vous permet d'obtenir des informations sur tous les produits Symantec.

Vous pouvez également accéder au site Web de Symantec par l'intermédiaire de votre navigateur Internet.

Pour accéder au site Web de Symantec depuis le navigateur

- Tapez l'adresse du site Web de Symantec, www.symantec.fr.

Exploration des didacticiels en ligne

Symantec fournit des didacticiels en ligne que vous pouvez utiliser pour examiner de nombreuses tâches courantes effectuées par Norton Personal Firewall.

Pour explorer les démos en ligne

1. Accédez avec le navigateur à http:http://www.symantec.com/region/fr/techsupp/tutorials.html
2. tutorials.htmlSur la page Web des démos, sélectionnez le produit et la version pour lesquels vous souhaitez un didacticiel.
3. Cliquez sur **Continuer**.
4. Dans la liste des démos disponibles pour votre produit, sélectionnez celui que vous souhaitez examiner.

Inscription au bulletin d'informations de Symantec Security Response

Symantec publie chaque mois un bulletin d'informations électronique gratuit axé sur les besoins des clients de la sécurité Internet. Ce bulletin traite des dernières technologies antivirus produites par Symantec Security Response, des virus courants, des tendances en termes de travaux sur les virus, des avertissements d'épidémies de virus, et des versions de définitions de virus spécifiques.

Pour vous inscrire au bulletin d'informations de Symantec Security Response

1. Accédez avec votre navigateur à securityresponse.symantec.com
2. Sur la page Web de Security Response, défilez jusqu'à la zone de référence, puis cliquez sur **Newsletter**.
3. Sur la page Web du bulletin d'informations de Security Response, sélectionnez la langue dans laquelle vous souhaitez recevoir le bulletin.
4. Sur la page Web d'inscription, tapez les informations demandées, puis cliquez sur **S'abonner**.

Mises à jour avec LiveUpdate

5

Les produits Symantec ont besoin d'informations à jour pour protéger l'ordinateur des nouvelles menaces virales. Symantec met ces informations à votre disposition par l'intermédiaire de LiveUpdate. LiveUpdate utilise votre connexion Internet pour obtenir des mises à jour de programme et de définitions de virus pour l'ordinateur.

Lorsque vous utilisez LiveUpdate, vous ne payez que les frais d'accès à Internet habituels.

Si vous utilisez Norton Personal Firewall sous Windows 2000 ou Windows XP, vous devez posséder des droits d’accès administrateur pour exécuter LiveUpdate.

A propos des mises à jour de programme

Les mises à jour de programme sont des améliorations mineures apportées au produit installé. Elles diffèrent des mises à jour de produit, qui installent une nouvelle version d'un produit entier. Les mises à jour de programme dotées d'un programme d'installation intégré qui remplace le logiciel existant sont appelées "correctifs". Les correctifs sont généralement créés pour augmenter la compatibilité du système d'exploitation ou du matériel, pour résoudre un problème de performances ou pour corriger une erreur.

La fonction LiveUpdate automatise l’obtention et l'installation des mises à jour de programme. Il recherche et obtient les fichiers sur un site Internet, les installe, puis supprime les fichiers superflus de l'ordinateur.

A propos des mises à jour de la protection antivirus

Les mises à jour de protection sont des fichiers disponibles par abonnement auprès de Symantec et destinés à actualiser vos produits Symantec sur base de la technologie antivirus la plus récente. Les mises à jour de protection reçues dépendent des produits que vous utilisez.

Norton AntiVirus, Norton SystemWorks	Les utilisateurs de Norton AntiVirus et de Norton SystemWorks reçoivent des mises à jour du service des définitions de virus, qui donnent accès aux dernières signatures de virus et autres technologies Symantec.
Norton Internet Security	En plus du service de définition des virus, les utilisateurs de Norton Internet Security reçoivent des mises à jour de protection pour le service de filtrage Web, le service de détection des intrusions et l'alerte concernant le courrier non désiré. Les mises à jour du service de filtrage Web donnent accès aux listes d'adresses et de catégories de sites les plus récentes pour identifier les contenus Web contestables. Les mises à jour du service de détection des intrusions donne accès aux règles de firewall prédéfinies les plus récentes et aux listes d'applications accédant à Internet. Ces listes permettent d'identifier les tentatives d'accès non autorisés à votre ordinateur. Les mises à jour d'alertes de courrier non désiré donnent accès aux définitions les plus récentes et aux listes actualisées de caractéristiques de courrier non désiré. Ces listes permettent d'identifier les e-mails non désirés.
Norton Personal Firewall	Les utilisateurs de Norton Personal Firewall reçoivent des mises à jour du service de détection des intrusions pour les règles de firewall prédéfinies les plus récentes et les listes d'applications accédant à Internet.

Informations sur l'abonnement

Se reporter à "Politique d'abonnement" à la page 167.

Votre produit Symantec comprend un abonnement limité sans frais vous permettant de bénéficier de mises à jour de protection correspondant aux services d'abonnement utilisés par votre produit. Lorsque cet abonnement est sur le point d'expirer, un message vous rappelle de le renouveler.

Si vous ne renouvelez pas votre abonnement, vous pouvez continuer à utiliser LiveUpdate pour obtenir des mises à jour de programme. Cependant, vous ne pourrez plus récupérer les mises à jour de la protection antivirus et vous ne serez plus protégé contre les nouvelles menaces découvertes.

Quand mettre à jour ?

Exécutez LiveUpdate aussitôt après l'installation du produit. Une fois vos fichiers actualisés, exécutez régulièrement LiveUpdate pour obtenir des mises à jour. Par exemple, pour maintenir la protection antivirus à jour, utilisez LiveUpdate une fois par semaine ou chaque fois que de nouveaux virus sont découverts. Les mises à jour des programmes sont mises à disposition suivant les besoins.

Demander une alerte de mise à jour

Pour vous assurer que les mises à jour de protection sont actualisées, vous pouvez demander à être informé par e-mail à chaque épidémie de virus ou à chaque nouvelle menace à la sécurité d'Internet. Le message d'alerte décrit la menace, fournit des instructions de détection et de suppression et vous donne des informations pour la sécurité de votre ordinateur. Vous devez toujours exécuter LiveUpdate après réception d'une de ces alertes.

Pour demander une alerte de mise à jour

1. A l'aide de votre navigateur, accédez à http://securityresponse.symantec.com/avcenter
2. Faites défiler jusqu'au bas de la page Web Security Response, puis cliquez sur **Symantec security response - Free Subscription - Click here!**.
3. Dans la page Web Abonnement aux alertes concernant la sécurité, complétez le formulaire d'abonnement.
4. Cliquez sur **Send me free Security Alerts!**

Si vous exécutez LiveUpdate sur un réseau interne

Si vous exécutez LiveUpdate sur un ordinateur connecté à un réseau protégé par un pare-feu de société, votre administrateur de réseau pourra installer un serveur LiveUpdate interne sur le réseau. LiveUpdate doit trouver automatiquement cet emplacement.

Si vous éprouvez des problèmes de connexion à un serveur LiveUpdate interne, contactez votre administrateur de réseau.

Si vous ne pouvez pas utiliser LiveUpdate

Lorsque de nouvelles mises à jour sont disponibles, Symantec les place sur son site Web. Si vous ne pouvez pas exécuter LiveUpdate, vous pouvez obtenir de nouvelles mises à jour à partir du site Web de Symantec.

Votre abonnement doit être valide pour que vous puissiez obtenir de nouvelles mises à jour de protection à partir du site Web de Symantec.

Pour obtenir des mises à jour à partir du site Web de Symantec

1. Visitez le site Symantec Security Response : http://securityresponse.symantec.com
2. Suivez les liens pour obtenir le type de mise à jour nécessaire.

Obtenir des mises à jour à l'aide de LiveUpdate

LiveUpdate vérifie les mises à jour de tous les produits Symantec installés sur votre ordinateur.

Si vous utilisez AOL, CompuServe ou Prodigy, connectez-vous à Internet avant d'exécuter LiveUpdate.

Pour obtenir des mises à jour à l'aide de LiveUpdate

1. Ouvrez le produit Symantec.
2. En haut de la fenêtre, cliquez sur **LiveUpdate**.
   Un avertissement vous signalera peut-être que votre abonnement a expiré. Suivez les instructions affichées pour le renouveler.
3. Dans la fenêtre LiveUpdate, cliquez sur **Suivant** pour détecter les mises à jour.

4 Si des mises à jour sont proposées, cliquez sur **Suivant** pour les télécharger et les installer.

5 Quand l'installation est terminée, cliquez sur **Terminer**.

Certaines mises à jour ne prendront effet qu'après le redémarrage de l'ordinateur.

Paramétrez LiveUpdate pour opérer en mode interactif ou en mode express

LiveUpdate s'exécute en mode interactif ou en mode express. En mode interactif (option par défaut), LiveUpdate télécharge une liste de mises à jour disponible pour vos produits Symantec pris en charge par la technologie LiveUpdate. Vous pouvez alors choisir les mises à jour que vous voulez installer. En mode express, LiveUpdate installe automatiquement toutes les mises à jour de vos produits Symantec.

Pour paramétrer LiveUpdate pour opérer en mode interactif ou en mode express.

1 Ouvrez le produit Symantec.

2 En haut de la fenêtre, cliquez sur **LiveUpdate**.

3 Dans l'écran de bienvenue de LiveUpdate, cliquez sur **Configure**.

4 Dans l'onglet Général de la boîte de dialogue Configuration de LiveUpdate, choisissez **Mode interactif** ou **Mode express**.

5 Si vous avez choisi le Mode express, sélectionnez la manière de vérifier les mises à jour :

- Pour avoir la possibilité d'annuler la mise à jour, sélectionnez **Je veux appuyer sur le bouton Démarrer pour exécuter LiveUpdate**.
- Pour que les mises à jour soient installées automatiquement à chaque démarrage de LiveUpdate, sélectionnez **Je veux que LiveUpdate démarre automatiquement**.

6 Cliquez sur **OK**.

Désactiver le mode express

Après avoir paramétré LiveUpdate pour s'exécuter en mode express, vous ne pouvez plus accéder à la boîte de dialogue Configuration de LiveUpdate directement à partir de LiveUpdate. Vous devez utiliser le panneau de configuration de Symantec LiveUpdate.

Pour désactiver le mode express

1. Dans la barre des tâches Windows, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration**.
2. Dans la fenêtre Panneau de configuration, double-cliquez sur **Symantec LiveUpdate**.
3. Dans l'onglet Général de la boîte de dialogue Configuration de LiveUpdate, choisissez **Mode interactif**.
4. Cliquez sur **OK**.

Exécution automatique de LiveUpdate

Vous pouvez demander à LiveUpdate de contrôler automatiquement les mises à jour de programme de protection, selon le programme paramétré, en activant des sessions LiveUpdate automatiques. Vous devez poursuivre l'exécution de LiveUpdate manuellement pour recevoir des mises à jour de produit.

Les sessions LiveUpdate automatiques vérifient une connexion Internet toutes les cinq minutes, jusqu'à ce qu'elle réponde et, par la suite, toutes les quatre heures. Si votre routeur RNIS est paramétré pour se connecter automatiquement à votre fournisseur d'accès Internet, de nombreuses connexions seront effectuées et chacune pourra occasionner des frais téléphoniques. Pour éviter cela, configurez le routeur RNIS de manière à désactiver la connexion automatique au fournisseur d'accès ou désactivez les sessions automatiques LiveUpdate dans les options Norton Personal Firewall.

Pour activer les sessions LiveUpdate automatiques

1. Lancer Norton Personal Firewall
2. En haut de la fenêtre principale de Norton Personal Firewall, cliquez sur **Options**.

Si vous définissez un mot de passe pour les options, Norton Personal Firewall vous demande de saisir le mot de passe avant de continuer.

3 Dans la boîte de dialogue Options de Norton Personal Firewall, cliquez sur l'onglet **LiveUpdate**.

4 Dans le volet LiveUpdate, cochez la case **Activer une session LiveUpdate automatique**.

5 Si vous voulez être prévenu lorsque des mises à jour sont disponibles, cochez **Me prévenir lorsque des mises à jour Norton Personal Firewall sont disponibles**.

6 Sélectionnez les mises à jour à vérifier par la session LiveUpdate automatique.

7 Pour chaque type de mise à jour que vous voulez demander à la session LiveUpdate automatique de vérifier, définissez la façon dont ces mises à jour doivent être appliquées en sélectionnant une des options suivantes :

Mettre à jour automatiquement ma protection	LiveUpdate recherche et installe les mises à jour de la protection antivirus sans vous consulter. LiveUpdate affiche une alerte lorsqu'une mise à jour de protection a été téléchargée. Vous devez toutefois exécuter LiveUpdate de temps en temps afin de rechercher les mises à jour de programme.
Me prévenir	LiveUpdate recherche les mises à jour des définitions de virus et vous demande si vous souhaitez les installer.

8 Cliquez sur **OK**.

Pour supprimer les sessions LiveUpdate automatiques programmées, désactivez l'option de sessions LiveUpdate automatiques.

Pour désactiver les sessions LiveUpdate automatiques

1 Lancer Norton Personal Firewall

2 En haut de la fenêtre principale de Norton Personal Firewall, cliquez sur **Options**.

Si vous définissez un mot de passe pour les options, Norton Personal Firewall vous demande de saisir le mot de passe avant de continuer.

3 Dans la boîte de dialogue Options de Norton Personal Firewall, cliquez sur l'onglet **LiveUpdate**.

4 Dans le volet LiveUpdate, désactivez l'option **Activer une session LiveUpdate automatique**.

5 Cliquez sur **OK**.

Contrôle de l'accès aux ordinateurs protégés

6

Norton Personal Firewall peut être configuré pour répondre à vos besoins dans de nombreuses situations. Vous pouvez utiliser le programme pour contrôler l'accès de votre ordinateur à la fois aux ordinateurs locaux et par l'intermédiaire d'Internet. Vous pouvez également contrôler les modalités d'accès des utilisateurs extérieurs à votre ordinateur.

Contrôle de l'utilisation de votre ordinateur

Norton Personal Firewall contrôle toutes les *connexions*, y compris celles entre les ordinateurs de votre domicile. Après l'installation, il peut être nécessaire d'ajuster quelques paramètres afin de partager des fichiers, des imprimantes et d'autres ressources avec d'autres ordinateurs.

Connexion à un réseau

Chaque fois que vous utilisez le partage de fichiers de Windows pour échanger des fichiers, que vous imprimez sur une imprimante partagée ou que vous vous connectez à Internet avec un *modem* ou une connexion à haut débit, votre ordinateur se connecte à un *réseau* composé d'autres ordinateurs. En tant que membre d'un réseau, votre ordinateur est vulnérable aux attaques. Norton Personal Firewall surveille automatiquement l'ensemble des connexions réseau afin de garantir la sécurité de l'ordinateur.

En temps normal, votre ordinateur se connecte à un réseau à la suite d'une action de votre part. Une connexion inattendue peut indiquer qu'un programme nuisible tente d'envoyer des informations sur Internet. Certaines cartes réseau sans fil analysent automatiquement tout réseau à leur portée et s'y connectent. Si vous vous déplacez avec un ordinateur portable équipé d'une telle carte, vous constaterez peut-être qu'il se connecte à des réseaux sans fil dans les aéroports et autres lieux publics.

Se reporter à "Contrôle de Norton Personal Firewall" à la page 115.

Dès qu'une connexion réseau est établie, Norton Personal Firewall en commence automatiquement la surveillance. Il n'est pas nécessaire d'effectuer des modifications pour être protégé. Norton Personal Firewall vous avertit de la nouvelle connexion et l'enregistre dans le *journal des connexions*.

Activation du partage de fichiers et d'imprimantes

Le réseau Microsoft permet de partager des fichiers et des imprimantes. Par défaut, Norton Personal Firewall empêche tout ordinateur d'accéder à ces *services* sur un ordinateur protégé.

Pour partager des fichiers et donner accès à des imprimantes sur votre *réseau* local, vous devez activer le partage de fichiers et d'imprimantes. Si vous activez ces fonctionnalités sur votre réseau local, elles restent protégées des internautes malintentionnés.

Avant d'activer le partage de fichiers et d'imprimantes sur votre réseau local, assurez-vous que chaque ressource partagée est protégée par un *mot de passe* sécurisé. Pour plus d'informations sur la sécurisation des ressources partagées, consultez le fichier Aide de Windows dans le menu Démarrer.

Pour activer le partage de fichiers et d'imprimantes

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur Personal firewall.
3. Dans la fenêtre Personal firewall, cliquez sur **Règles générales** sur l'onglet Avancé.
4. Dans la fenêtre Règles générales, sélectionnez l'entrée pour le partage de fichiers ou d'imprimantes Windows.
5. Cliquez sur **Modifier**.
6. Sur l'onglet Action de la boîte de dialogue Modifier une règle, cliquez sur **Autoriser l'accès à Internet**.

7 Cliquez sur **OK**.

8 Dans la boîte de dialogue Règles générales, cliquez sur **OK**.

9 Dans la fenêtre Firewall avancé, cliquez sur **OK**.

Organisation des ordinateurs en zones de réseau

Norton Personal Firewall vous permet d'organiser les ordinateurs de votre réseau personnel et sur Internet en deux zones : Approuvés et Restreints.

Si vous avez plusieurs ordinateurs chez vous, vous les ajouterez probablement à votre zone Approuvés. N'ajoutez d'ordinateurs externes à cette zone que s'il s'agit d'utilisateurs de confiance qui disposent d'un logiciel de pare-feu installé.

L'assistant de contrôle de zone permet d'organiser rapidement les ordinateurs dans les zones. Vous pouvez aussi répartir les ordinateurs manuellement.

Pour ouvrir l'assistant de contrôle de zone depuis Security Center

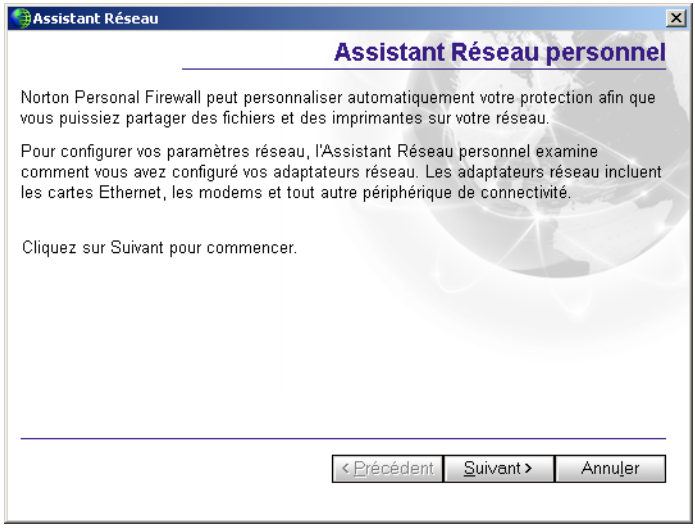
1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur Personal firewall.

3 Dans la fenêtre Personal firewall, cliquez sur l'onglet **Réseau personnel**.

Pour ouvrir l'Assistant de contrôle de zone depuis Security Monitor

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Sélectionner une tâche de Security Monitor, sélectionnez **Configurer un réseau personnel**.



Pour organiser des ordinateurs en zones ave l'Assistant de contrôle de zone

1. Dans l'Assistant de contrôle de zone, cliquez sur **Suivant**.
2. Dans la liste obtenue, cochez les adaptateurs réseau que vous souhaitez que Norton Personal Firewall configure automatiquement et ajoute à la zone Approuvés.
3. Cliquez sur **Suivant**.
4. Cliquez sur **Terminer** pour fermer l'assistant.

Pour ajouter manuellement des ordinateurs aux zones

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur Personal firewall.
3. Dans la fenêtre Personal firewall, sur l'onglet Réseau personnel, sélectionnez la zone à laquelle vous voulez ajouter un ordinateur.
4. Cliquez sur **Ajouter**.

Se reporter à "Identification des ordinateurs dans Norton Personal Firewall" à la page 69.

5 Utilisez la fenêtre Indiquer les ordinateurs pour identifier l'ordinateur.

6 Quand vous avez fini d'ajouter des ordinateurs, cliquez sur **OK**.

Pour supprimer des ordinateurs des zones

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur Personal firewall.

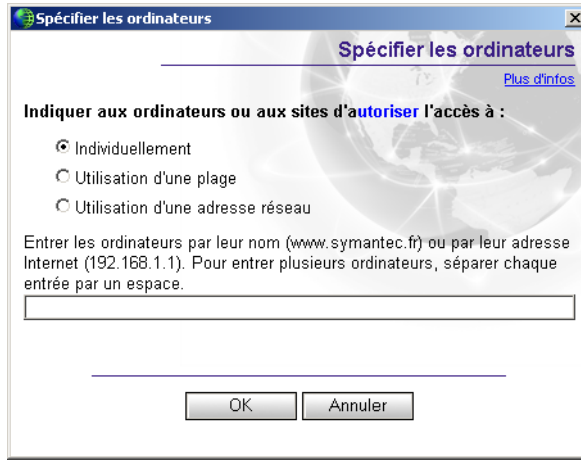
3 Sélectionnez l'ordinateur que vous souhaitez supprimer.

4 Cliquez sur **Supprimer**.

5 Quand vous avez fini de supprimer des ordinateurs, cliquez sur **OK**.

Identification des ordinateurs dans Norton Personal Firewall

Vous devez identifier les ordinateurs dans Norton Personal Firewall pour configurer manuellement les zones du réseau, les règles de filtrage et d'autres fonctions de protection. Dans ce cas, la boîte de dialogue Indiquer les ordinateurs apparaît.



Cette boîte de dialogue permet d'identifier des ordinateurs de trois façons. Dans tous les cas, vous pouvez indiquer des *adresses IP*.

Recherche de l'adresse IP d'un ordinateur

Deux méthodes permettent de trouver l'adresse IP d'un ordinateur : Sur les ordinateurs Windows 98/Me, vous pouvez utiliser Winipcfg pour trouver l'adresse IP d'un ordinateur. Sur les ordinateurs Windows 2000/XP, vous pouvez utiliser Ipconfig pour trouver l'adresse IP d'un ordinateur.

Pour rechercher une adresse IP avec Winipcfg

1. Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Exécuter**.
2. Dans la boîte de dialogue Exécuter, tapez **winipcfg**
3. Cliquez sur **OK**.
4. Sélectionnez un adaptateur réseau.
5. Notez l'adresse IP.

Pour rechercher une adresse IP avec Ipconfig

1. Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Exécuter**.
2. Dans la boîte de dialogue Exécuter, tapez **cmd**.
3. Cliquez sur **OK**.
4. A l'invite de commande, tapez **ipconfig**.
5. Cliquez sur **OK**.
6. Notez l'adresse IP.

Spécification d'un ordinateur individuel

Le nom de l'ordinateur peut être une adresse IP, une *URL* comme service.symantec.com ou un nom de réseau Microsoft comme Mojave. Vous pouvez trouver le nom des ordinateurs du réseau local dans le Voisinage réseau ou dans les Favoris réseau Windows.

Si le protocole TCP/IP n'est pas associé au Client pour les réseaux Microsoft dans les propriétés réseau Windows, vous devez utiliser des adresses IP au lieu de noms pour désigner les ordinateurs du réseau local.

Pour spécifier un ordinateur individuel

1. Dans la boîte de dialogue Indiquer les ordinateurs, cliquez sur **Individuellement**.
2. Tapez le nom ou l'adresse IP de l'ordinateur.
3. Cliquez sur **OK**.

Spécification d'une série d'ordinateurs

Vous pouvez identifier une plage d'ordinateurs en indiquant l'adresse IP de départ (plus petit nombre) et celle de fin (plus grand nombre). Tous les ordinateurs compris dans la plage d'adresses IP sont inclus.

Dans la plupart des cas, les trois premiers nombres sur les quatre qui composent une adresse IP sont identiques.

Pour spécifier une plage d'ordinateurs

1. Dans la boîte de dialogue Indiquer les ordinateurs, cliquez sur **A l'aide d'une plage**.
2. Dans le champ Adresse Internet de départ, tapez l'adresse IP de départ (plus petit nombre).
3. Dans le champ Adresse Internet de fin, tapez l'adresse IP de fin (plus grand nombre).
4. Cliquez sur **OK**.

Spécification d'ordinateurs avec une adresse réseau

Vous pouvez identifier tous les ordinateurs d'un même *sous-réseau* en spécifiant une adresse IP et un masque de sous-réseau. L'adresse IP spécifiée peut être n'importe quelle adresse du sous-réseau identifié.

Pour spécifier des ordinateurs avec une adresse réseau

1. Dans la fenêtre Indiquer les ordinateurs, cliquez sur **A l'aide d'une adresse réseau**.
2. Dans le champ Adresse réseau, tapez l'adresse IP de l'un des ordinateurs du sous-réseau.
3. Dans le champ Masque de sous-réseau, tapez le masque de sous-réseau.
   Le masque de sous-réseau est presque toujours 255.255.255.0.
4. Cliquez sur **OK**.

Si vous utilisez le protocole DHCP

Si votre *FAI* utilise un serveur *DHCP* (dynamic host control protocol) pour fournir des adresses IP aux ordinateurs des utilisateurs, soyez prudent lorsque vous tapez les adresses IP.

Au lieu d'identifier un ordinateur avec une seule adresse IP, qui peut changer à tout moment, indiquez une adresse réseau en utilisant une adresse IP de base et un masque de sous-réseau. Fournissez des valeurs couvrant la plage d'adresses qui peuvent être attribuées à l'ordinateur.

Contrôle de l'accès des utilisateurs à Internet

Norton Personal Firewall prend en charge la plupart des méthodes de *connexion* à Internet sans nécessiter de configuration supplémentaire.

Si vous accédez à Internet via un routeur câble ou DSL

Norton Personal Firewall fonctionne derrière un *routeur* câble ou DSL et renforce la protection assurée par le routeur. Dans certains cas, il peut être utile de réduire la protection fournie par le routeur pour pouvoir utiliser des applications telles que NetMeeting ou Microsoft Messenger. Norton Personal Firewall propose également des fonctions qui peuvent ne pas être disponibles avec les routeurs câble et DSL, comme le Contrôle de confidentialité.

Si des ordinateurs multiples partagent une même connexion à Internet

Norton Personal Firewall fonctionne avec la plupart des programmes de partage de connexion à Internet. Pour protéger votre réseau des nombreuses attaques extérieures, installez Norton Personal Firewall sur l'ordinateur passerelle. Pour une protection optimale contre les *chevaux de Troie* ou autres applications qui initient des *connexions sortantes*, installez Norton Personal Firewall sur tous les ordinateurs qui partagent la connexion.

Contrôle de l'accès des utilisateurs extérieurs à votre réseau

Norton Personal Firewall peut protéger les ordinateurs tout en autorisant des utilisateurs externes à accéder aux serveurs de votre *réseau*. Pour exécuter des *serveurs* sur des ordinateurs protégés, vous devrez probablement créer des règles de filtrage permettant aux utilisateurs extérieurs de se connecter à certains ports. Pour une sécurité optimale, ne créez ces règles que sur les ordinateurs qui exécutent vos serveurs.

Si vous exécutez Symantec pcAnywhere

Se reporter à "Modification d'une règle de filtrage existante" à la page 92.

Vous ne devriez pas rencontrer de problèmes avec Symantec pcAnywhere utilisé comme client ou Elève avec Norton Personal Firewall. Pour bénéficier d'une protection maximale si vous utilisez un Elève pcAnywhere, modifiez la règle pour limiter son utilisation aux seuls ordinateurs que vous utilisez avec l'Elève. Cette précaution, combinée aux *mots de passe* de Symantec pcAnywhere, offre un niveau de protection optimal.

Si vous exécutez un réseau privé virtuel

Norton Personal Firewall fonctionne avec les réseaux privés virtuels (VPN) suivants :

- Nortel
- VPNRemote
- PGP
- SecureRemote

Avec la plupart des VPN, vous ne pouvez pas voir Internet ou d'autres ordinateurs du réseau local quand le client VPN est actif. Vous ne pouvez voir que ce qui est disponible par l'intermédiaire du serveur VPN auquel vous êtes connecté.

Protection contre les tentatives d'intrusion

7

Les attaques issues d'Internet exploitent la manière dont les ordinateurs transfèrent les données. Norton Personal Firewall protège votre ordinateur en surveillant les informations entrantes et sortantes, et en bloquant toute tentative d'attaque.

Protection offerte par Norton Personal Firewall contre les attaques de réseau

Norton Personal Firewall est doté de trois outils de protection contre les tentatives d'intrusion, les contenus Web malveillants et les *chevaux de Troie* :

- Norton Personal Firewall
  Contrôle toutes les communications Internet et crée un bouclier qui bloque ou limite les tentatives pour accéder aux informations de votre ordinateur.
- Détection d'intrusion
  Analyse toutes les informations entrantes et sortantes pour rechercher des modèles de données caractéristiques d'une attaque.
- Visual Tracking
  Identifie l'ordinateur à l'origine de l'attaque.

Surveillance des communications par Norton Personal Firewall

Lorsque Norton Personal Firewall est actif, il surveille les communications entre votre ordinateur et d'autres ordinateurs sur Internet. Il protège également votre ordinateur contre les problèmes de sécurité courants :

Tentatives de connexion anormales	Vous avertit de toute tentative de connexion provenant d'autres ordinateurs et des tentatives d'applications de votre ordinateur de se connecter à d'autres ordinateurs.
Chevaux de Troie	Vous avertit quand votre ordinateur rencontre des programmes malveillants qui prennent l'apparence d'applications utiles.
Infractions à la sécurité et à la confidentialité issues de contenus Web malveillants	Surveille l'ensemble des applets Java et contrôles ActiveX, et permet de choisir de les exécuter ou de les bloquer.
Analyses de port	Masque les ports inactifs de votre ordinateur et détecte les analyses de port.
Intrusions	Détecte et bloque les transmissions malveillantes et les tentatives d'attaque émanant d'utilisateurs externes.

Se reporter à "Personnalisation de la protection du pare-feu" à la page 78.

Vous pouvez contrôler le niveau de protection offert par Norton Personal Firewall à l'aide du curseur de niveau de sécurité. Vous pouvez également configurer la réaction de Norton Personal Firewall à des tentatives de connexions incorrectes, des chevaux de Troie et des contenus Web malveillants.

Détection d'intrusion et analyse des communications

La Détection d'intrusion analyse chaque *paquet* entrant ou sortant de votre ordinateur pour vérifier la présence de signatures d'attaque. Une signature d'attaque est un groupe de données qui identifie une tentative de piratage visant à exploiter une faille connue d'un système d'exploitation ou d'une application.

Norton Personal Firewall protège votre ordinateur contre les attaques les plus fréquente, notamment celles-ci :

Bonk	Attaque de la pile TCP/IP Microsoft capable de bloquer l'ordinateur cible.
RDS_Shell	Utilisation du composant RDS (Remote Data Services, services de données distants) de Microsoft Data Access Components permettant à un pirate d'exécuter des commandes à distance avec les privilèges système.
WinNuke	Utilisation de NetBIOS pour bloquer les ordinateurs exécutant l'un des anciens systèmes d'exploitation Windows.

Comme les attaques peuvent se répartir sur plusieurs paquets, la détection d'intrusion examine les paquets de deux manières différentes. D'une part, elle analyse chaque paquet individuellement pour rechercher les modèles de données caractéristiques d'une attaque. D'autre part, elle surveille les paquets sous forme de flux de données afin d'identifier les attaques réparties sur plusieurs paquets.

Si les informations correspondent à une attaque connue, la Détection d'intrusion rejette automatiquement le paquet et interrompt la *connexion* avec l'ordinateur à l'origine de l'envoi des données. L'ordinateur est ainsi protégé contre toutes les attaques possibles.

Vous pouvez modifier la façon dont la Détection d'intrusion répond aux attaques en excluant de la surveillance certaines signatures d'attaque et en activant/désactivant la fonction AutoBlock, qui bloque automatiquement toute communication issue de l'ordinateur à l'origine d'une attaque. L'exclusion du blocage de certains comportements de réseau vous permet de continuer à travailler, même lorsque votre ordinateur subit une attaque.

Parallèlement à la protection qu'il vous offre contre les attaques, Norton Personal Firewall surveille toutes les informations que votre ordinateur envoie à d'autres ordinateurs. Cela permet de s'assurer que votre ordinateur ne peut pas servir à attaquer d'autres utilisateurs ni être exploité par des programmes *zombies*. Si Norton Personal Firewall détecte que votre ordinateur envoie des informations caractéristiques d'une attaque, il bloque immédiatement la connexion et vous avertit du problème potentiel.

Pour réduire le nombre d'avertissements, Norton Personal Firewall surveille uniquement les attaques visant les ports que votre ordinateur utilise. Si un pirate tente de se connecter à votre ordinateur par l'intermédiaire d'un port inactif ou d'un port bloqué par le pare-feu, Norton Personal Firewall ne vous en avertit pas car il n'y a aucun risque d'intrusion.

Norton Personal Firewall ne surveille pas les intrusions des ordinateurs figurant dans la zone Approuvés. La Détection d'intrusion analyse néanmoins les informations que vous leur envoyez pour vérifier l'existence de zombies ou d'autres attaques de contrôle à distance.

Se reporter à "Mises à jour avec LiveUpdate" à la page 57.

Pour détecter et bloquer les activités de réseau douteuses, la Détection d'intrusion s'appuie sur une vaste liste de signatures d'attaque. Veillez à ce que la liste des signatures d'attaque reste à jour en exécutant régulièrement LiveUpdate.

Visual Tracking et le repérage d'attaquants

Se reporter à "Identification de la source de communications" à la page 44.

Norton Personal Firewall inclut à présent Visual Tracking, qui vous permet d'obtenir des informations sur l'adresse IP à l'origine d'une connexion particulière. Il peut ainsi vous aider à identifier un attaquant.

Personnalisation de la protection du pare-feu

Les paramètres par défaut du Firewall personnel offrent une protection appropriée à la majorité des utilisateurs. Si la protection par défaut ne convient pas, vous pouvez la personnaliser avec le curseur du niveau de sécurité pour sélectionner des niveaux de sécurité prédéfinis ou modifier des paramètres individuels.

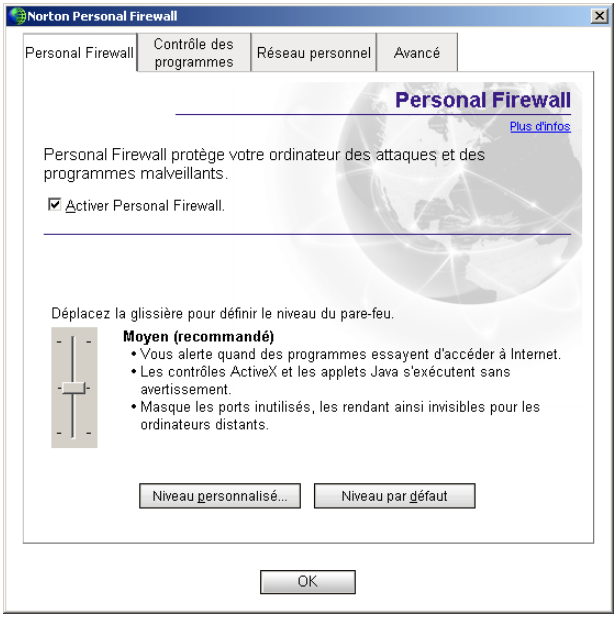
Modification du niveau de sécurité

Le curseur du niveau de sécurité permet de sélectionner un niveau de sécurité Bas, Moyen ou Elevé. Le niveau de protection varie en fonction de la position du curseur. Le curseur n'affecte pas la protection assurée par la Détection d'intrusion.

Pour modifier le niveau de sécurité

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur Personal firewall.



3 Placez le curseur sur un niveau de sécurité. Les options sont les suivantes :

Elevé	Le pare-feu bloque toute transmission jusqu'à votre autorisation. Si vous avez effectué une Analyse des applications, vous ne devriez pas être interrompu souvent par des alertes du Contrôle des programmes. Se reporter à "Activation du Contrôle des programmes automatique" à la page 83. Un avertissement s'affiche lors de la détection d'un contrôle ActiveX ou d'une applet Java. Les ports inutilisés ne répondent pas aux demandes de connexion. Les ordinateurs externes ne les voient plus.

Moyen (recommandé)	Le pare-feu bloque toute transmission jusqu'à votre autorisation. Si vous avez effectué une Analyse des applications, vous ne devriez pas être interrompu souvent par des alertes du Contrôle des programmes. Les contrôles ActiveX et les applets Java s'exécutent sans avertissement. Les ports inutilisés ne répondent pas aux demandes de connexion. Les ordinateurs externes ne les voient plus.
Bas	Le pare-feu bloque les tentatives de connexion émanant des chevaux de Troie. Les contrôles ActiveX et les applets Java s'exécutent sans avertissement.

Modification de paramètres de sécurité individuels

Si le paramétrage offert par l'option Niveau de sécurité ne vous convient pas, vous pouvez modifier le niveau de protection de Norton Personal Firewall, des *applets Java* et des *contrôles ActiveX*. La modification d'un paramètre individuel remplace le Niveau de sécurité, mais n'a aucun impact sur les autres paramètres de sécurité.

Pour modifier des paramètres de sécurité individuels

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur Personal firewall.
3. Cliquez sur **Niveau personnalisé**.

4 Effectuez une ou plusieurs des opérations suivantes :

- Dans le menu Personal firewall, sélectionnez un niveau. Les options sont les suivantes :

Maximum	Bloque toutes les communications que vous n'autorisez pas expressément. Vous devez définir des règles de filtrage pour toutes les applications qui nécessitent un accès à Internet.
Moyen	Bloque de nombreux ports utilisés par des applications dangereuses. Cependant, ce réglage peut également bloquer les programmes utiles qui utilisent les mêmes ports.
Aucun	Désactive Norton Personal Firewall et autorise toutes les communications Internet.

- Sélectionnez le niveau de sécurité souhaité pour les applets Java et les contrôles ActiveX. Les options sont les suivantes :

Maximum	Empêche le navigateur d'exécuter des applets Java ou des contrôles ActiveX sur Internet. Cette option est la plus sûre, mais aussi la moins pratique. Certains sites Web risquent de ne pas fonctionner correctement lorsqu'elle est active.
Moyen	Vous interroge en cas de présence d'une applet Java ou d'un contrôle ActiveX. Vous pouvez ainsi, selon les cas, accepter ou bloquer les applets et les contrôles. Il peut être fastidieux d'intervenir chaque fois que vous rencontrez une applet Java ou un contrôle ActiveX, mais cette méthode permet de choisir d'en exécuter certains.
Aucun	Autorise l'exécution de toutes les applets Java et de tous les contrôles ActiveX.

- Pour être averti chaque fois que des programmes inconnus accèdent à Internet, cochez l'option **Activer les alertes de contrôle d'accès**.
- Pour être averti quand un ordinateur distant tente de se connecter à un port inutilisé de votre ordinateur, cochez l'option **Alerter en cas d'accès à des ports inutilisés**.

5 Cliquez sur **OK**.

Réinitialisation des options de sécurité sur les valeurs par défaut

La configuration d'un niveau de sécurité personnalisé désactive le curseur Sécurité. Le curseur indique le niveau de sécurité sur lequel le vôtre est basé, mais vous ne pouvez pas utiliser le curseur pour modifier vos paramètres. Pour utiliser le curseur Sécurité pour choisir l'un des niveaux prédéfinis, vous devez réinitialiser le niveau de sécurité.

Pour réinitialiser les paramètres de sécurité sur les valeurs par défaut

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Personal firewall.**
3. Cliquez sur **Niveau personnalisé**.

Se reporter à "Modification du niveau de sécurité" à la page 78.

Votre niveau de sécurité est réinitialisé sur le niveau moyen. Utilisez le curseur Sécurité pour choisir l'un des autres niveaux de sécurité prédéfinis.

Personnalisation des règles de filtrage

Les règles de filtrage déterminent la façon dont Norton Personal Firewall protège votre ordinateur contre les transmissions entrantes, les applications et les *chevaux de Troie* malveillants. Le pare-feu utilise ces règles pour vérifier automatiquement toutes les données entrantes ou sortantes de votre ordinateur.

Traitement des règles de filtrage

Lorsqu'un ordinateur tente de se connecter à votre ordinateur ou vice versa, Norton Personal Firewall compare le type de *connexion* à la liste des règles de filtrage.

Les règles de filtrage sont traitées dans un ordre défini en fonction de leur type. Les règles système sont traitées d'abord, suivies des règles d'application puis de celles applicables aux chevaux de Troie.

Lorsqu'une règle de blocage ou d'autorisation s'applique, les autres règles ne sont pas prises en compte. Autrement dit, les autres règles pertinentes pour ce type de communication sont ignorées si elles apparaissent à la suite de la première règle applicable.

Si aucune règle ne correspond, la communication est bloquée. Selon le niveau de rapport demandé, une alerte peut apparaître.

Création de règles de filtrage

Norton Personal Firewall inclut le Contrôle des programmes, qui crée automatiquement les règles de filtrage au fur et à mesure que vous utilisez Internet.

Vous pouvez créer des règles de filtrage avec le Contrôle des programmes de quatre manières différentes :

Activer le Contrôle automatique des programmes	Configure automatiquement l'accès à Internet des applications connues à leur premier lancement. Il s'agit de la méthode de configuration de règles la plus rapide.
Utiliser l'Analyse des applications	Détecte et configure simultanément toutes les applications Internet d'un ordinateur.
Ajouter manuellement des programmes	Gère avec précision la liste des applications pouvant accéder à Internet.
Répondre aux alertes	Norton Personal Firewall avertit les utilisateurs lorsqu'une application tente d'accéder à Internet pour la première fois. Les utilisateurs peuvent alors décider d'autoriser l'application à accéder à Internet ou de le lui interdire.

Activation du Contrôle des programmes automatique

Lorsque le Contrôle automatique des programmes est activé, Norton Personal Firewall crée automatiquement des règles de filtrage la première fois qu'une application connue est exécutée. Le Contrôle automatique des programmes ne configure l'accès à Internet que pour les versions des applications que Symantec a identifiées comme sans danger.

Si une application inconnue ou une version inconnue d'une application connue tente d'accéder à Internet, Norton Personal Firewall en avertit l'utilisateur. L'utilisateur peut alors décider d'autoriser l'application à accéder à Internet ou de le lui interdire.

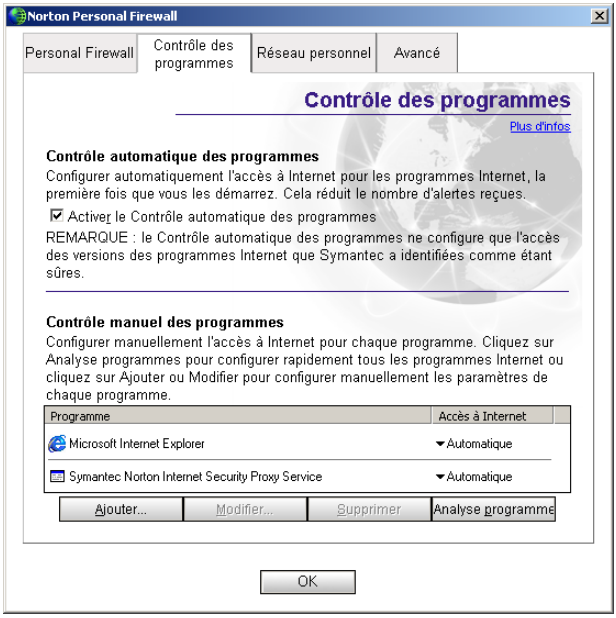
Se reporter à "Mises à jour avec LiveUpdate" à la page 57.

Symantec actualise en permanence la liste des applications reconnues. Exécutez régulièrement LiveUpdate pour tenir à jour votre liste.

Pour activer le Contrôle automatique des programmes

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur **Personal firewall.**



3 Dans la fenêtre de Personal Firewall, cliquez sur **Activer le Contrôle automatique des programmes** sur l'onglet Contrôle des programmes.

4 Cliquez sur **OK**.

Recherche des applications utilisant Internet

L'Analyse des applications est la méthode la plus rapide pour configurer le Firewall personnel. Norton Personal Firewall recherche les applications de l'ordinateur qu'il reconnaît et propose des paramètres appropriés pour chaque application.

Vous pouvez rechercher les programmes accédant à Internet depuis Security Center ou Security Monitor.

Pour rechercher les applications utilisant Internet depuis Security Center

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Personal firewall.**
3. Dans la fenêtre Personal firewall, cliquez sur **Analyse programme** sur l'onglet Contrôle des programmes.
4. Sélectionnez le ou les disques de l'ordinateur à analyser.
5. Cliquez sur **OK**.
6. Dans la fenêtre Analyse des applications, effectuez l'une des opérations suivantes :
   - Cochez les applications à ajouter à la liste du Contrôle des programmes.
   - Pour ajouter simultanément toutes les applications Internet, cliquez sur **Tout sélect.**
7. Cliquez sur **Terminer**.
8. Cliquez sur **OK**.

Pour rechercher les applications utilisant Internet depuis Security Monitor

1. Ouvrez Norton Personal Firewall.
2. Dans le menu Sélectionner une tâche de Security Monitor, sélectionnez **Exécuter l'analyse des programmes**.
3. Sélectionnez le ou les disques de l'ordinateur à analyser.
4. Cliquez sur **OK**.
5. Dans la fenêtre Analyse des applications, effectuez l'une des opérations suivantes :
   - Cochez les applications à ajouter à la liste du Contrôle des programmes.
   - Pour ajouter simultanément toutes les applications Internet, cliquez sur **Tout sélect.**
6. Cliquez sur **Terminer**.

Ajout manuel d'un programme au Contrôle des programmes

Se reporter à "Personnalisation de la protection du pare-feu" à la page 78.

Les utilisateurs peuvent ajouter des applications au Contrôle des programmes pour contrôler étroitement leur accès à Internet. Cette opération remplace tout paramétrage effectué par le Contrôle automatique des programmes.

Pour ajouter manuellement un programme au Contrôle des programmes

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Personal firewall.**
3. Dans la fenêtre Personal firewall, cliquez sur **Ajouter** sur l'onglet Contrôle des programmes.
4. Sélectionnez le fichier exécutable de l'application.
   Le nom des fichiers exécutables se termine généralement par .exe.
5. Cliquez sur **Ouvrir**.
6. Dans l'alerte du Contrôle d'accès à Internet, sélectionnez le niveau d'accès à accorder au programme. Les options sont les suivantes :

Configurer l'accès à Internet automatiquement (recommandé)	Utilise les paramètres de Norton Personal Firewall par défaut pour l'application.
Autoriser	Autorise toutes les tentatives d'accès de ce programme.
Bloquer	Refuse toutes les tentatives d'accès de ce programme.
Configurer automatiquement l'accès à Internet	Permet de créer des règles contrôlant l'accès à Internet de cette application.

7. Pour évaluer les risques qu'une application peut poser à votre ordinateur, cliquez sur **Détails**.
8. Cliquez sur **OK**.

Modification des paramètres du Contrôle des programmes

Après vous être familiarisé avec Norton Personal Firewall, vous souhaiterez peut-être modifier les paramètres d'accès des applications. Cette opération remplace tout paramétrage effectué par le Contrôle automatique des programmes.

Pour modifier les paramètres du Contrôle des programmes

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Personal firewall.**
3. Dans la fenêtre Personal firewall, cliquez sur le programme à modifier sur l'onglet Contrôle des programmes.
4. Cliquez sur **Modifier**.
5. Dans l'alerte du Contrôle d'accès à Internet, sélectionnez le niveau d'accès à accorder au programme. Les options sont les suivantes :

Configurer automatiquement l'accès à Internet	Utilise les paramètres de Norton Personal Firewall par défaut pour l'application.
Autoriser cette application à accéder à Internet	Autorise toutes les tentatives d'accès de ce programme.
Empêcher cette application d'accéder à Internet	Refuse toutes les tentatives d'accès de ce programme.
Personnaliser l'accès à Internet pour cette application	Permet de créer des règles contrôlant l'accès à Internet de cette application.

6. Cliquez sur **OK**.

Ajout manuel d'une règle de pare-feu

Norton Personal Firewall crée automatiquement la plupart des règles de filtrage nécessaires, mais vous pouvez être amené à en ajouter en fonction de vos besoins. Ne créez des règles de filtrage que si vous êtes un utilisateur expérimenté d'Internet.

Vous pouvez personnaliser trois ensembles de règles de filtrage :

- Règles générales
- Règles de cheval de Troie
- Règles d'application

Pour ajouter une règle générale

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Personal firewall.**
3. Dans la fenêtre Personal firewall, cliquez sur **Règles générales** sur l'onglet Avancé.
4. Suivez les instructions affichées à l'écran.
   Se reporter à "Ecriture d'une règle de filtrage" à la page 89.

Pour ajouter une règle de cheval de Troie

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Personal firewall.**
3. Dans la fenêtre Personal firewall, cliquez sur **Règles cheval de Troie** sur l'onglet Avancé.
4. Suivez les instructions affichées à l'écran.
   Se reporter à "Ecriture d'une règle de filtrage" à la page 89.

Pour ajouter une règle d'application

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Personal firewall.**
3. Dans la fenêtre Personal firewall, cliquez sur **Ajouter** sur l'onglet Contrôle des programmes.

4 Dans la fenêtre Sélection de programme, choisissez le fichier exécutable d'une application.
Le nom des fichiers exécutables se termine généralement par .exe.

5 Dans l'alerte du contrôle d'accès à Internet, sélectionnez **Créer une règle de filtrage** dans le menu Que dois-je faire ?

6 Suivez les instructions affichées à l'écran.
Se reporter à "Ecriture d'une règle de filtrage" à la page 89.

Ecriture d'une règle de filtrage

Norton Personal Firewall vous guide pour créer vos propres règles de filtrage.

Pour écrire une règle de filtrage

1 Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, cliquez sur **Ajouter**.

2 Dans la fenêtre Ajouter une règle, sélectionnez l'action souhaitée pour cette règle. Les options sont les suivantes :

Autoriser l'accès à Internet	Autorise les communications du type indiqué.
Bloquer l'accès à Internet	Interdit les communications du type indiqué.
Contrôler à l'accès à Internet	Actualise l'onglet Pare-feu du journal des événements ou affiche un message à chaque communication du type indiqué. Cette opération permet de constater la fréquence d'utilisation de cette règle de filtrage. Pour surveiller une connexion autorisée, vous devez créer à la fois une règle de surveillance et une règle d'autorisation. La règle de surveillance doit précéder la règle d'autorisation.

3 Cliquez sur **Suivant**.

4 Sélectionnez le type de connexion que la règle doit surveiller. Les options sont les suivantes :

Connexions à d'autres ordinateurs	La règle s'applique aux connexions sortantes (de votre ordinateur vers un autre ordinateur).
Connexions en provenance d'autres ordinateurs	La règle s'applique aux connexions entrantes (d'un ordinateur distant vers votre ordinateur).
Connexions à destination et en provenance d'autres ordinateurs	La règle s'applique aux connexions entrantes et sortantes.

5 Cliquez sur **Suivant**.

6 Sélectionnez les ordinateurs que la règle doit surveiller. Les options sont les suivantes :

Ordinateur quelconque	La règle s'applique à tous les ordinateurs.
Uniquement les ordinateurs identifiés ci-dessous	La règle ne s'applique qu'aux ordinateurs, sites et domaines répertoriés.
Adaptateurs	La règle s'applique à un adaptateur réseau particulier de votre ordinateur. Ce paramètre permet de personnaliser des règles de filtrage pour chaque adresse IP de votre ordinateur. Si, par exemple, l'ordinateur est connecté à un réseau personnel et à Internet, vous pouvez définir une règle qui autorise le partage de fichiers au sein du réseau personnel et une autre qui l'interdise sur Internet.

7 Cliquez sur **Suivant**.

8 Sélectionnez les protocoles que la règle doit surveiller. Les options sont les suivantes :

TCP	La règle s'applique aux communications TCP (Transport Control Protocol).
UDP	La règle s'applique aux communications UDP (User Datagram Protocol).

TCP et UDP	La règle s'applique à la fois aux communications TCP et UDP.
ICMP	La règle s'applique aux communications ICMP (Internet Control Message Protocol). Cette option n'est disponible que pour ajouter ou modifier une règle générale.

9 Sélectionnez les ports que la règle doit surveiller. Les options sont les suivantes :

Tous les types de communications (tous les ports)	La règle s'applique aux communications utilisant n'importe quel port.
Uniquement les types de communications ou les ports mentionnés ci-dessous	La règle s'applique aux ports répertoriés. Vous pouvez ajouter des ports à la liste ou en supprimer.

10 Cliquez sur **Suivant**.

11 Choisissez si et comment Norton Personal Firewall doit suivre cette règle. Les options sont les suivantes :

Pas de suivi de la règle	Aucune trace des actions de la règle n'est conservée.
Créer une entrée de fichier journal	Une entrée est ajoutée au journal des événements du pare-feu lorsqu'un événement de communication réseau correspond à la règle.
Envoyer un message Alert Tracker	Un message Alert Tracker apparaît lorsqu'une communication réseau correspond à la règle.
Afficher une alerte de sécurité	Une boîte de dialogue d'alerte de sécurité apparaît lorsqu'une communication réseau correspond à la règle.

12 Cliquez sur **Suivant**.

13 Dans la zone de texte **Comment voulez-vous appeler cette règle ?** , tapez un nom pour la règle.

14 Cliquez sur **Suivant**.

15 Vérifiez les paramètres de la nouvelle règle et cliquez sur **Terminer**.

16 Quand vous avez fini d'ajouter des règles, cliquez sur **OK**.

Modification d'une règle de filtrage existante

Vous pouvez modifier les règles de filtrage qui ne fonctionnent pas comme vous le souhaitez.

Pour modifier une règle de filtrage existante

1 Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, cliquez sur **Ajouter**.

2 Sélectionnez la règle à modifier.

3 Cliquez sur **Modifier**.

Se reporter à "Ecriture d'une règle de filtrage" à la page 89.

4 Suivez les instructions affichées à l'écran pour modifier la règle.

5 Quand vous avez fini de modifier des règles, cliquez sur **OK**.

Modification de l'ordre des règles de filtrage

Se reporter à "Traitement des règles de filtrage" à la page 82.

Norton Personal Firewall traite chaque liste de règles de filtrage du début à la fin. Vous pouvez déterminer comment Norton Personal Firewall traite les règles de filtrage en modifiant l'ordre de celles-ci.

Pour modifier l'ordre d'une règle de filtrage

1 Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, sélectionnez la règle que vous souhaitez déplacer.

2 Effectuez l'une des opérations suivantes :

- Pour que Norton Personal Firewall traite cette règle avant la règle située au-dessus, cliquez sur **Vers le haut**.
- Pour que Norton Personal Firewall traite cette règle après la règle située au-dessous, cliquez sur **Vers le bas**.

3 Quand vous avez fini de déplacer des règles, cliquez sur **OK**.

Désactivation temporaire d'une règle de filtrage

Vous pouvez désactiver temporairement une règle de filtrage si vous devez accorder un accès spécifique à un ordinateur ou un programme.

Pour désactiver temporairement une règle de filtrage

- Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, sélectionnez la règle que vous souhaitez désactiver.

Pensez à réactiver la règle quand vous avez fini de travailler avec le programme ou l'ordinateur qui nécessitait la modification.

Suppression d'une règle de filtrage

Supprimez les règles de filtrage dont vous n'avez plus besoin.

Pour supprimer une règle de filtrage

1. Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, cliquez sur **Ajouter**.
2. Sélectionnez la règle à supprimer.
3. Cliquez sur **Supprimer**.
4. Quand vous avez fini de supprimer des règles, cliquez sur **OK**.

Réinitialisation des paramètres par défaut des règles de filtrage

La réinitialisation des règles de filtrage ramène le pare-feu à ses paramètres par défaut et supprime toute modification apportée aux règles.

N'utilisez cette procédure qu'en cas d'urgence. Avant de réinitialiser vos règles de filtrage, essayez de supprimer les règles modifiées récemment.

Pour réinitialiser les paramètres par défaut des règles de filtrage

1. Fermez toutes les fenêtres de Norton Personal Firewall.
2. Dans l'Explorateur Windows, cliquez deux fois sur **Poste de travail**.
3. Cliquez deux fois sur le disque dur sur lequel vous avez installé Norton Personal Firewall.
   Dans la plupart des cas, il s'agit du disque C.

4 Ouvrez **Program Files** > **Fichiers communs** > **Symantec Shared**.

5 Faites glisser **firewall.rul** sur la Corbeille.

Le pare-feu reviendra à ses paramètres par défaut la prochaine fois que vous exécuterez Norton Personal Firewall.

Personnalisation de la Détection d'intrusion

Les paramètres par défaut de la Détection d'intrusion offrent une protection appropriée à la majorité des utilisateurs. Vous pouvez personnaliser la Détection d'intrusion, en excluant certaines activités de réseau de la surveillance, en activant ou en désactivant AutoBlock et en limitant les ordinateurs bloqués.

Exclusion d'activités de réseau de la surveillance

Certaines activités de réseau inoffensives peuvent ressembler à des signatures d'attaque Norton Personal Firewall. Si vous recevez de nombreux avertissements relatifs à des attaques potentielles déclenchés par des comportements inoffensifs, vous pouvez créer une exclusion pour la signature d'attaque correspondante.

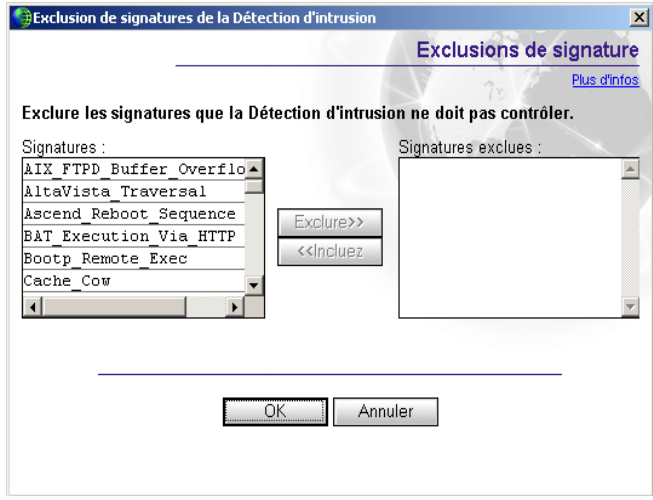
Chaque exclusion rend l'ordinateur un peu plus vulnérable aux attaques. Soyez très sélectif dans votre choix des attaques à exclure. N'excluez que les activités qui sont toujours inoffensives.

Pour exclure des signatures d'attaque de la surveillance

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.

3 Dans la fenêtre Détection d'intrusion, cliquez sur **Signatures**.



4 Dans la liste Signatures, sélectionnez la signature d'attaque à exclure.

5 Cliquez sur **Exclure**.

6 Quand vous avez fini d'exclure des signatures, cliquez sur **OK**.

Si vous avez exclu des signatures d'attaque que vous voulez surveiller de nouveau, vous pouvez les inclure dans la liste de signatures actives.

Pour inclure des signatures d'attaque

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.

3 Dans la fenêtre Détection d'intrusion, cliquez sur **Signatures**.

4 Dans la liste Signatures exclues, sélectionnez la signature d'attaque à surveiller.

5 Cliquez sur **Inclure**.

6 Quand vous avez fini d'inclure des signatures, cliquez sur **OK**.

Activation ou désactivation d'AutoBlock

Lorsque Norton Personal Firewall détecte une attaque, il bloque automatiquement la *connexion* pour garantir la sécurité de l'ordinateur. Le programme peut également activer la fonction AutoBlock, qui bloque automatiquement toutes les communications entrantes issues de l'ordinateur attaquant pendant une période de temps donnée, même lorsqu'elles ne correspondent pas à une signature d'attaque.

Par défaut, la fonction AutoBlock interrompt toutes les communications émanant de l'ordinateur malveillant pendant 30 minutes.

Pour activer ou désactiver AutoBlock

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la fenêtre Détection d'intrusion, cochez ou décochez la case **Activer AutoBlock**.

Déblocage d'ordinateurs

Si un ordinateur auquel vous voulez accéder apparaît dans la liste des ordinateurs actuellement bloqués par AutoBlock, débloquez-le. Si, à la suite d'une modification des paramètres de protection, vous souhaitez réinitialiser la liste AutoBlock, vous pouvez simultanément lever l'interdiction de tous les ordinateurs de la liste AutoBlock.

Pour débloquer les ordinateurs actuellement bloqués par AutoBlock

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la fenêtre Détection d'intrusion, effectuez l'une des opérations suivantes :
   - Pour débloquer un ordinateur, sélectionnez son adresse IP, puis cliquez sur **Débloquer**.
   - Pour débloquer tous les ordinateurs figurant dans la liste AutoBlock, cliquez sur **Tout débloquer**.

Exclusion d'ordinateurs d'AutoBlock

Si un ordinateur auquel vous voulez accéder est systématiquement placé dans la liste d'AutoBlock, vous pouvez l'exclure du blocage AutoBlock.

Pour exclure certains ordinateurs d'AutoBlock

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la fenêtre Détection d'intrusion, cliquez sur **Adresse IP**.
4. Effectuez l'une des opérations suivantes :
   - Dans la liste Actuellement bloqués, sélectionnez une adresse IP bloquée et cliquez sur **Exclure**.
   - Cliquez sur **Ajouter**, puis tapez le nom de l'ordinateur, son adresse IP, son identification réseau ou une plage d'adresses IP incluant l'ordinateur à exclure.
5. Quand vous avez fini d'exclure des adresses IP, cliquez sur **OK**.

Ajout d'un ordinateur bloqué à la zone Restreints

Vous pouvez ajouter un ordinateur bloqué à la zone Restreints pour l'empêcher en permanence d'accéder à votre ordinateur. Les ordinateurs ajoutés à la zone Restreints ne figurent pas dans la liste des ordinateurs bloqués car Norton Personal Firewall rejette automatiquement toutes les *tentatives de connexion* qu'ils effectuent.

Pour ajouter un ordinateur bloqué à la zone Restreints

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la liste des ordinateurs actuellement bloqués par AutoBlock, sélectionnez celui à ajouter à la liste Restreints.
4. Cliquez sur **Restreindre**.
5. Quand vous avez fini de restreindre des ordinateurs, cliquez sur **OK**.

Protection de votre confidentialité

8

Chaque fois que vous naviguez sur Internet, les ordinateurs et les *sites Web* collectent des informations à votre sujet. Certaines de ces informations proviennent de formulaires que vous remplissez et des choix que vous effectuez sur des pages. D'autres renseignements sont issus de votre *navigateur*, qui fournit automatiquement des informations sur la dernière page Web visitée et le type d'ordinateur utilisé.

Des utilisateurs malintentionnés peuvent également recueillir des informations confidentielles à votre insu Chaque fois que vous envoyez des informations par l'intermédiaire d'Internet, les données passent par un certain nombre d'ordinateurs avant d'atteindre leur destination. Lors de la transmission, des tiers peuvent intercepter ces informations.

Les ordinateurs comportent des fonctions de sécurité de base, mais celles-ci risquent de ne pas être suffisantes pour protéger vos informations confidentielles. Le Contrôle de confidentialité vous aide à protéger vos données personnelles en assurant différents niveaux de contrôle sur les *cookies* et les informations que votre navigateur envoie aux sites Web.

Le Contrôle de confidentialité permet également de vous assurer que les utilisateurs n'envoient pas par inadvertance des informations confidentielles non codées sur Internet, comme des numéros de carte de crédit.

Identification des informations confidentielles à protéger

Sur de nombreux *sites Web*, vous êtes invité à indiquer votre nom, votre *adresse électronique* et d'autres informations confidentielles. Bien que vous puissiez généralement fournir ces informations en toute confiance aux sites renommés, des sites malveillants peuvent utiliser ces informations pour porter atteinte à votre vie privée. Des personnes peuvent également intercepter des informations envoyées par l'intermédiaire du Web, de la messagerie électronique ou des programmes de messagerie instantanée.

Le Contrôle de confidentialité permet d'établir la liste des informations qui doivent rester confidentielles. Si des utilisateurs tentent d'envoyer des informations confidentielles sur Internet, Norton Personal Firewall les avertit du risque encouru par rapport à la sécurité ou bloque la *connexion*.

Confidentialité et SSL

Certains sites Web et serveurs de messagerie utilisent des connexions SSL (Secure Socket Layer) pour chiffre les connexions entre votre ordinateur et le serveur. Le Contrôle de confidentialité ne peut pas bloquer les informations confidentielles transmises sur des connexions SSL. Toutefois comme les informations sont chiffrées, le destinataire du courrier électronique sera seul à pouvoir le lire.

Ajout d'informations confidentielles

Vous devez ajouter les informations à protéger à la liste Informations confidentielles de Norton Personal Firewall.

Pour ajouter des informations confidentielles

1. Démarrez Norton Personal Firewall.
2. Effectuez l'une des opérations suivantes :
   - Dans Security Center, cliquez deux fois sur **Confidentialité**, puis sur **Informations confidentielles**.
   - Dans le menu Sélectionner une tâche de Security Monitor, sélectionnez **Modifier les informations confidentielles**.
3. Dans la boîte de dialogue Informations confidentielles, cliquez sur **Ajouter**.

4 Dans la boîte de dialogue Ajout d'informations confidentielles, sélectionnez une catégorie dans la liste Type d'informations à protéger.

5 Dans le champ Nom descriptif, indiquez pour mémoire la raison pour laquelle vous souhaitez protéger ces données.

6 Dans le champ Informations à protéger, tapez les informations dont vous souhaitez empêcher la transmission sur des connexions Internet non sécurisées.

7 Dans le champ Protéger ces informations confidentielles pour, sélectionnez les programmes Internet dans lesquels le Contrôle de la confidentialité doit bloquer ces informations :

- Web
- Messagerie instantanée
- Courrier électronique

8 Cliquez sur **OK**.

Modification ou suppression d'informations confidentielles

Vous pouvez modifier ou supprimer des informations confidentielles à tout moment.

Pour modifier ou supprimer des informations confidentielles

1 Démarrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur **Confidentialité**.

3 Dans la fenêtre e volet Confidentialité, cliquez sur **Informations confidentielles**.

4 Sélectionnez les informations confidentielles à modifier ou à supprimer.

5 Sélectionnez l'une des options suivantes :

- Modifier
- Supprimer

6 Cliquez sur **OK**.

Personnalisation de la confidentialité

Le Contrôle de confidentialité protège quatre zones :

Informations confidentielles	Bloque des chaînes de texte spécifiques à ne pas envoyer sur Internet.
Blocage des cookies	Empêche les sites Web de récupérer des informations personnelles stockées dans des fichiers de cookies.
Confidentialité de navigation	Protège les informations relatives à vos habitudes de navigation.
Connexions sécurisées	Empêche les utilisateurs d'établir des connexions sécurisées vers des sites marchands et d'autres sites Web.

Il existe deux façons de définir les paramètres de confidentialité :

- Définir le niveau de confidentialité
  Utilisez le curseur du volet principal Confidentialité pour sélectionner des niveaux de sécurité prédéfinis.
- Régler des paramètres de confidentialité individuels
  Personnalisez votre protection en réglant des paramètres manuellement.

Définition du niveau de confidentialité

Norton Personal Firewall propose des niveaux de sécurité prédéfinis permettant de paramétrer plusieurs options de confidentialité à la fois. Le curseur de niveau de confidentialité permet de sélectionner une protection minimale, moyenne ou maximale.

Pour définir le niveau de confidentialité

1. Démarrez Norton Personal Firewall.
2. Cliquez deux fois sur **Confidentialité**.

3 Placez le curseur sur le niveau de confidentialité souhaité. Les options sont les suivantes :

Haut	Toutes les informations confidentielles sont bloquées et une alerte s'affiche à chaque cookie rencontré.
Moyen (recommandé)	Une alerte apparaît si des informations confidentielles sont saisies dans un formulaire Web ou une messagerie instantanée. Dissimule votre navigation aux sites Web. Les cookies ne sont pas bloqués.
Bas	Les informations confidentielles ne sont pas bloquées. Les cookies ne sont pas bloqués. Dissimule votre navigation aux sites Web.

4 Cliquez sur **OK**.

Réglage de paramètres de confidentialité individuels

Vous pouvez modifier les paramètres pour les options Informations confidentielles, Blocage des cookies, Confidentialité de navigation et Connexions sécurisées si le niveau de confidentialité ne vous convient pas. Par exemple, vous pouvez bloquer toute tentative d'envoi d'informations confidentielles, tout en autorisant des sites Web à personnaliser leurs pages en utilisant les informations de votre navigateur.

Modification du paramètre Informations confidentielles

Modifiez le paramètre Informations confidentielles pour contrôler la façon dont Norton Personal Firewall traite les tentatives d'envoi sur Internet d'informations figurant dans la liste Informations confidentielles.

Pour modifier le paramètre Informations confidentielles

1 Démarrez Norton Personal Firewall.

2 Cliquez deux fois sur **Confidentialité**.

3 Cliquez sur **Niveau personnalisé**.

4 Sélectionnez un paramètre pour Informations confidentielles. Les options sont les suivantes :

Maximum	Bloque toutes les informations confidentielles.
Moyen	Vous avertit quand vous tentez de transmettre des informations confidentielles à un site Web non sécurisé ou par l'intermédiaire d'un programme de messagerie instantanée.
Aucun	Ne bloque pas les informations confidentielles.

5 Cliquez sur **OK**.

Modification du paramètre Blocage des cookies

De nombreux sites Web stockent les informations collectées dans des *cookies* placés sur votre disque dur. Lorsque vous retournez sur un site qui a installé un cookie sur votre ordinateur, le serveur Web ouvre le cookie et le lit.

La plupart des cookies sont inoffensifs. Les sites les utilisent pour personnaliser les pages Web, mémoriser vos choix sur le site et proposer des pages optimisées pour votre ordinateur. Cependant, les sites peuvent également utiliser des cookies pour effectuer le suivi de l'usage que vous faites d'Internet et de vos habitudes de navigation.

Modifiez le paramètre Blocage des cookies pour contrôler la façon dont Norton Personal Firewall gère les sites qui tentent de placer des cookies sur votre ordinateur.

Pour modifier le paramètre Blocage des cookies

1 Démarrez Norton Personal Firewall.

2 Cliquez deux fois sur **Confidentialité**.

3 Cliquez sur **Niveau personnalisé**.

4 Sélectionnez un paramètre pour Blocage des cookies. Trois options sont disponibles :

Maximum	Bloque tous les cookies.
Moyen	Vous prévient chaque fois qu'un cookie est rencontré.
Aucun	Autorise les cookies.

5 Cliquez sur **OK**.

Activation ou désactivation de la Confidentialité de navigation

La Confidentialité de navigation empêche les sites Web d'identifier le type de *navigateur* que vous utilisez, le dernier site Web visité en dernier et d'autres informations concernant vos habitudes de navigation. Certains sites Web basés sur JavaScript risquent de ne pas fonctionner correctement s'ils ne peuvent pas identifier le type de navigateur utilisé.

Pour activer ou désactiver la Confidentialité de navigation

1. Démarrez Norton Personal Firewall.
2. Cliquez deux fois sur **Confidentialité**.
3. Cliquez sur **Niveau personnalisé**.
4. Dans la boîte de dialogue Personnalisation de la confidentialité, cochez ou décochez la case **Activer la confidentialité de navigation**.
5. Cliquez sur **OK**.

Activation ou désactivation des connexions Web sécurisées

Lorsque vous visitez un site Web sécurisé, le navigateur établit automatiquement une *connexion* chiffrée avec ce site. Par défaut, Norton Personal Firewall permet à tous les comptes d'utiliser des connexions sécurisées. Si vous souhaitez éviter que les utilisateurs n'envoient pas d'informations confidentielles vers des sites Web sécurisés, désactivez les connexions Web sécurisées.

Si vous désactivez les connexions Web sécurisées, votre navigateur ne chiffrera plus aucune information envoyée. Désactivez les connexions Web sécurisées uniquement si vous protégez vos informations confidentielles.

Pour activer ou désactiver les connexions Web sécurisées

1. Démarrez Norton Personal Firewall.
2. Cliquez deux fois sur **Confidentialité**.
3. Cliquez sur **Niveau personnalisé**.
4. Dans la boîte de dialogue Personnalisation de la confidentialité, cochez ou décochez la case **Activer les connexions sécurisées (https)**.
5. Cliquez sur **OK**.

Blocage des publicités sur Internet

9

De nombreux sites Web utilisent des techniques agressives pour attirer l'attention sur les publicités présentes sur leurs pages. Certains utilisent des publicités de grande taille et voyantes, tandis que d'autres font appel à des fenêtres qui apparaissent lorsque vous visitez ou quittez le site. Outre l'augmentation du délai d'affichage des pages Web, certaines publicités contiennent des contenus inconvenants, provoquent des conflits logiciels ou utilisent des astuces *HTML* pour ouvrir des fenêtres de *navigateur* supplémentaires.

Le Blocage des publicités permet d'éviter ces problèmes. Lorsque le Blocage des publicités est actif, Norton Personal Firewall supprime de manière transparente les éléments suivants :

- Bannières publicitaires
- Publicités déroulantes
- Publicités "Flash" Macromedia

Fonctionnement du Blocage des publicités

Norton Personal Firewall détecte et bloque les publicités selon deux critères : leurs dimensions et leur emplacement.

Blocage d'après les dimensions

La plupart des publicistes en ligne utilisent une ou plusieurs dimension standard pour leurs publicités. Norton Personal Firewall est désormais capable de bloquer les images, les animations Flash et d'autres éléments *HTML* dont les dimensions sont celles des publicités courantes.

Blocage d'après l'emplacement

Chaque fichier sur Internet possède une adresse ou *URL* unique. Lorsqu'une page Web s'affiche, l'ordinateur se connecte à une URL et affiche le fichier stocké à cet emplacement. Si la page pointe vers des images, des fichiers audio ou d'autres contenus multimédia, votre *navigateur* affiche les fichiers en tant qu'éléments de la page.

Lorsque vous consultez une page Web contenant une *bannière publicitaire*, les instructions d'affichage de la page peuvent inclure les options suivantes :

<p>Bienvenue chez Ajax<img src="http://www.ajax.com/nifty_images/image7.gif">

Le navigateur affiche le texte "Bienvenue chez Ajax". Il se connecte ensuite à www.ajax.com et demande un fichier appelé /belles_images/image7.gif. (Le suffixe .gif indique qu'il s'agit d'un fichier de format GIF (Graphics Interchange Format), c'est à dire un format commun de fichier image.) L'ordinateur à l'adresse www.ajax.com envoie le fichier au navigateur qui affiche l'image.

Si le Blocage des publicités est activé lorsque vous vous connectez à un site Web, Norton Personal Firewall analyse les pages Web et compare leur contenu à deux listes :

Se reporter à "Mises à jour avec LiveUpdate" à la page 57.

- Une liste par défaut de publicités bloquées automatiquement par Norton Personal Firewall. Utilisez LiveUpdate pour actualiser régulièrement la liste des publicités bloquées.
- Une liste que vous créez en interceptant des publicités spécifiques. Vous pouvez enrichir et modifier cette liste.

Si la page contient des fichiers issus d'un *domaine* bloqué, Norton Personal Firewall supprime le lien et télécharge le reste de la page.

Activation et désactivation du Blocage des publicités

Norton Personal Firewall recherche les adresses des publicités à bloquer pendant le téléchargement de la page Web par le *navigateur*. S'il détecte des adresses figurant dans la liste des publicités à intercepter, les informations correspondantes sont bloquées pour qu'elles ne s'affichent pas dans le navigateur. Le reste de la page Web demeure inchangé et vous pouvez le consulter sans publicités.

Pour activer ou désactiver le Blocage des publicités

1 Ouvrez Norton Personal Firewall.

2 Cliquez deux fois sur **Blocage des publicités**.

3 Cochez ou décochez la case **Activer le blocage des publicités**.

4 Cliquez sur **OK**.

Activation/désactivation du Blocage des fenêtres déroulantes

Les publicités déroulantes sont des fenêtres secondaires que les sites Web ouvrent lorsque vous visitez ou quittez le site. Ces fenêtres apparaissent devant ("pop-up") ou derrière ("pop-under") la fenêtre en cours.

Lorsque le Blocage des fenêtres déroulantes est actif, Norton Personal Firewall bloque automatiquement le code de programmation que les sites Web utilisent pour ouvrir des fenêtres secondaires à votre insu. Les sites qui ouvrent des fenêtres secondaires lorsque vous cliquez sur un lien ou effectuez d'autres actions ne sont pas affectés.

Pour activer ou désactiver le Blocage des fenêtres déroulantes

1. Ouvrez Norton Personal Firewall.
2. Cliquez deux fois sur **Blocage des publicités**.
3. Cochez ou décochez la case **Activer le blocage des fenêtres déroulantes**.
4. Cliquez sur **OK**.

Activation ou désactivation du Blocage Flash

Lorsque le Blocage des publicités est actif, Norton Personal Firewall bloque automatiquement toutes les animations Flash qui ont les dimensions des publicités courantes. Norton Personal Firewall peut également bloquer tous les contenus Flash. Cette option est utile si votre connexion est lente ou si vous n'êtes pas intéressé par l'affichage d'animations Flash.

Vous pouvez demander à Norton Personal Firewall de bloquer toutes les animations Flash ou de ne les bloquer que sur certains sites Web.

Pour activer ou désactiver le Blocage Flash

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Contenu Web, cliquez sur l'onglet **Paramètres globaux**.
4. Dans la liste des sites Web, effectuez l'une des opérations suivantes :
   - Pour modifier les paramètres Flash de tous les sites, cliquez sur **(Par défaut)**.
   - Pour modifier les paramètres Flash d'un site de la liste, cliquez sur le nom du site.
   - Pour modifier les paramètres Flash d'un site absent de la liste, cliquez sur **Ajouter** et tapez l'adresse du site dans la boîte de dialogue Nouveau site/domaine.
5. Dans la section Animation Flash, sélectionnez l'une des options suivantes :
   - Bloquer
   - Autoriser
6. Cliquez sur **OK**.

Certains sites Web utilisent Flash pour créer des barres d'outils de navigation. Le Blocage Flash peut rendre ces sites inexploitables.

Utilisation de la Corbeille publicitaire

En utilisant Internet, vous vous rendrez compte que certaines publicités ne font pas partie de la liste de Blocage des publicités par défaut de Norton Personal Firewall. Vous pouvez utiliser la Corbeille publicitaire pour les ajouter à votre liste personnelle de publicités bloquées.

Pour utiliser la Corbeille publicitaire

1. Lancez votre navigateur Web et affichez la page qui contient la publicité à bloquer.
2. Ouvrez Norton Personal Firewall.
3. Dans Security Center, cliquez deux fois sur **Blocage des publicités**.
4. Blocage des publicités, vérifiez que Activer le blocage des publicités est coché.
5. Cliquez sur **Ouvrir la Corbeille publicitaire**.
   La fenêtre Corbeille publicitaire apparaît.
6. Disposez les fenêtres de manière à voir à la fois la publicité et la fenêtre de la Corbeille, puis effectuez l'une des opérations suivantes :
   - Si vous utilisez Microsoft Internet Explorer, faites glisser la publicité importune du site Web vers la boîte de dialogue Blocage des publicités.
   - Si vous utilisez Netscape, cliquez sur la publicité avec le bouton droit de la souris puis cliquez sur **Copier l'adresse de l'image**. Dans la Corbeille publicitaire, cliquez sur **Coller**.
     L'adresse de la publicité apparaît dans la zone Informations sur la publicité de la boîte de dialogue Corbeille publicitaire.
7. Sélectionnez l'une des options suivantes :
   - Ajouter : Bloquer cette adresse.
   - Modifier : Modifier l'entrée avant de l'ajouter à la liste de Blocage des publicités.
     Par exemple, si l'adresse de la publicité est http://www.publicites.org/irritantes/pubs/numeroun.gif, vous pouvez la changer pour l'adresse http://www.publicites.org/irritantes/pubs pour bloquer tout le contenu du répertoire "pubs".
8. Cliquez sur **OK**.

Utilisation des chaînes de texte pour identifier les publicités à bloquer ou à autoriser

Vous pouvez spécifier que Norton Personal Firewall affiche des publicités spécifiques en créant une liste de chaînes de texte identifiant des bannières publicitaires individuelles. Les chaînes de Blocage des publicités sont des sections d'adresses *HTML*. Si une partie de l'adresse d'un fichier correspond à la chaîne de texte, Norton Personal Firewall bloque automatiquement le fichier.

Norton Personal Firewall propose une liste prédéfinie (Par défaut) de Blocage des publicités utilisée pour déterminer les images à bloquer lors de l'affichage de pages Web.

Lorsque le Blocage des publicités est activé, toutes les pages Web sont analysées pour repérer les chaînes HTML définies dans la liste (Par défaut). Norton Personal Firewall recherche les chaînes bloquées dans les balises HTML utilisées pour représenter les images et les publicités. Les structures HTML qui contiennent des chaînes en correspondance sont supprimées par Norton Personal Firewall avant que la page ne soit affichée dans le navigateur Web.

Veillez à ne pas insérer de chaînes trop génériques dans la liste de blocage (Par défaut). Par exemple, il ne serait pas judicieux de bloquer la chaîne www car presque toutes les *URL* contiennent www. Une chaîne telle que www.slowads est plus efficace car elle bloque uniquement les graphiques du *domaine* slowads sans affecter les autres sites.

Identification des chaînes de Blocage des publicités

La manière dont vous définissez les chaînes de Blocage des publicités détermine la rigueur avec laquelle Norton Personal Firewall filtre les données.

Si vous ajoutez par exemple la chaîne ajax.com à la liste de blocage (Par défaut), toutes les pages du domaine ajax.com sont bloquées. En vous montrant plus précis, par exemple en ajoutant la chaîne "belles_images/image7.gif" à la liste de blocage spécifique au site www.ajax.com, seule cette image est bloquée.

Un site peut devenir inutilisable si toutes ses images sont bloquées. Un bon compromis consiste à bloquer seulement les répertoires contenant des publicités. Par exemple, si www.ajax.com stocke ses publicités sous /nifty_images/ et ses images de navigation sous /useful_images/, il est possible de bloquer www.ajax.com/nifty_images/ sans limiter l'utilisation du site.

Vous pouvez également créer des chaînes d'autorisation qui permettent aux sites Web d'afficher les images correspondant à la chaîne. Ceci vous permet de neutraliser l'effet de blocage d'une chaîne dans la liste de blocage (Par défaut) pour des sites individuels. Les règles d'autorisation sont prioritaires par rapport aux règles de blocage sur tous les sites.

Ajout d'une chaîne de Blocage des publicités

Vous pouvez ajouter des chaînes à la liste de Blocage des publicités pour tous les sites ou des sites spécifiques.

Pour ajouter une chaîne de Blocage des publicités

1. Ouvrez Norton Personal Firewall.
2. En haut de la fenêtre Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Contenu Web, sur l'onglet Blocage des publicités, faites l'une des opérations suivantes :
   - Pour bloquer une chaîne sur tous les sites Web, cliquez sur **(Par défaut)**.
   - Pour bloquer une chaîne sur un site Web de la liste, sélectionnez le nom du site.
   - Pour bloquer une chaîne sur un site Web absent de la liste, cliquez sur **Ajouter un site** et tapez l'adresse du site dans la boîte de dialogue Nouveau site/domaine.
4. Sur l'onglet Blocage des publicités, cliquez sur **Ajouter**.
5. Dans la boîte de dialogue Ajouter une nouvelle chaîne HTML, sélectionnez l'action à effectuer. Les options sont les suivantes :

Bloquer	Bloque les publicités correspondant à la chaîne.
Autoriser	Accepte les publicités correspondant à la chaîne.

6. Saisissez une chaîne HTML à bloquer ou à autoriser.
7. Cliquez sur **OK**.

Modification ou suppression d'une chaîne de Blocage des publicités

S'il apparaît qu'une chaîne de Blocage des publicités devient trop restrictive, pas assez vaste ou inadaptée, vous pouvez la modifier ou la supprimer.

Pour modifier ou supprimer une chaîne de Blocage des publicités

1. Ouvrez Norton Personal Firewall.
2. En haut de la fenêtre Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Blocage des publicités de l'onglet Contenu Web, effectuez l'une des opérations suivantes :
   - Pour modifier ou supprimer une chaîne de la liste (Par défaut), cliquez sur **(Par défaut)**.
   - Pour modifier ou supprimer une chaîne d'un site spécifique, sélectionnez le nom du site.
4. Dans la liste des chaînes HTML, sélectionnez celle à modifier.
5. Effectuez l'une des opérations suivantes :
   - Pour modifier une chaîne, cliquez sur **Modifier** et saisissez vos modifications.
   - Pour supprimer une chaîne, cliquez sur **Supprimer**.
6. Cliquez sur **OK**.

Contrôle de Norton Personal Firewall

10

Norton Personal Firewall tient des enregistrements de toutes les connexions Internet entrantes et sortantes et de toutes les actions exécutées par le programme pour protéger votre ordinateur. Consultez périodiquement ces informations afin d'identifier les problèmes éventuels.

Quatre sources d'informations sur Norton Personal Firewall sont disponibles :

Fenêtre Statut et paramètres	Informations de base sur les fonctions de protection actives.
Fenêtre Statistiques	Informations récentes relatives au pare-feu et aux activités de blocage de contenu.
Fenêtre Statistiques détaillées	Statistiques détaillées sur l'activité du réseau et les actions exécutées par Norton Personal Firewall.
Journal des événements	Activités des utilisateurs sur Internet et actions exécutées par Norton Personal Firewall.

Lorsque vous examinez les informations consignées, recherchez :

- les attaques récentes dans la fenêtre Paramètres d'état
- les refus d'accès multiples, particulièrement ceux correspondant à une même *address IP*
- les séries de *numéros de port* émanant de la même adresse IP, indiquant éventuellement un *sondage de ports*
- une activité réseau excessive due à des programmes inconnus.

Les tentatives d'accès refusées sont normales si elles sont aléatoires, c'est-à-dire si elles ne proviennent pas de la même adresse IP et si elles ne concernent pas une séquence de numéros de port. Vous pouvez également constater des tentatives d'accès consignées en raison d'une activité sur votre ordinateur, comme la connexion à un serveur FTP ou l'envoi de *courrier électronique*.

L'une des situations énoncées ci-dessus peut indiquer une attaque.

Fenêtre Statut et paramètres

La fenêtre Statut et paramètres fournit un cliché de la protection de votre ordinateur. Vous pouvez vérifier rapidement les fonctions de protection actives, identifier les trous de sécurité et personnaliser Norton Personal Firewall.

Pour afficher la fenêtre Statut et paramètres

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez sur **Statut et paramètres**.
3. Pour modifier des paramètres, cliquez deux fois sur une fonction de protection.

Affichage de la fenêtre Statistiques

La fenêtre Statistiques fournit un instantané de l'activité *réseau* de votre ordinateur depuis le dernier démarrage de Windows. Ces informations permettent d'identifier les tentatives d'attaques en cours et de vérifier comment les paramètres de Confidentialité et de Contrôle parental influent sur la protection de votre ordinateur.

La fenêtre Statistiques fournit des informations sur :

Pare-feu personnel	Toutes les attaques récentes sur cet ordinateur, notamment l'heure de la dernière attaque et l'adresse de l'ordinateur à l'origine de l'attaque.
Blocage de contenu en ligne	Nombre de cookies, publicités Web et messages spam bloqués et nombre de fois où les informations confidentielles ont été bloquées
Contrôle parental	Sites Web et applications bloqués

Pour afficher la fenêtre Statistiques

1 Ouvrez Norton Personal Firewall.

2 Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.

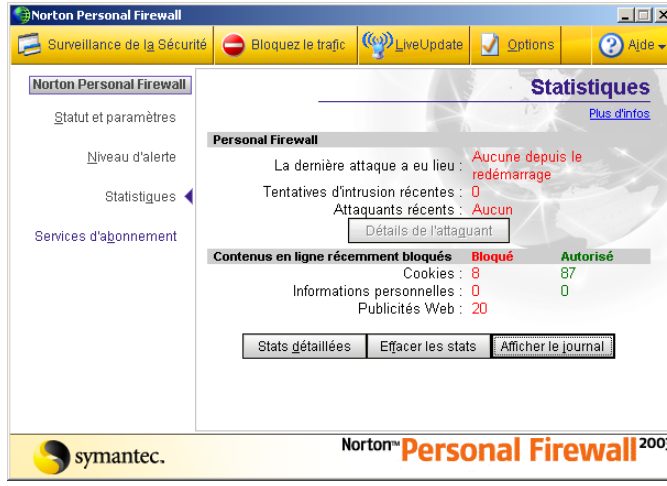
Réinitialisation des informations de la fenêtre Statistiques

Norton Personal Firewall efface automatiquement toutes les informations de la fenêtre Statistiques quand vous redémarrez Windows. Vous pouvez également effacer les statistiques manuellement. Cette opération peut s'avérer utile pour déterminer l'incidence sur les statistiques d'une modification de la configuration.

Pour réinitialiser les informations de la fenêtre Statistiques

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez sur **Statistiques**.



3 Dans la fenêtre Statistiques, cliquez sur **Effacer les statistiques**.

Affichage des statistiques détaillées

Outre les statistiques globales de la fenêtre Statistiques, Norton Personal Firewall tient à jour des compteurs réseau en temps réel qui suivent l'usage d'Internet par les utilisateurs et toute action exécutée par Norton Personal Firewall.

Les statistiques détaillées fournissent les informations suivantes.

Réseau	Octets TCP et UDP envoyés et reçus, nombre de connexions réseau ouvertes et nombre le plus élevé de connexions réseau ouvertes simultanément depuis le démarrage du programme
Navigation	Graphiques, cookies et demandes d'informations sur le navigateur bloqués, nombre d'octets et de paquets traités, et nombre de connexions HTTP
Images Web/ bannières publicitaires bloquées	Taille approximative des graphiques bloqués et gain de temps réalisé en ne chargeant pas les graphiques bloqués
Filtrage des connexions TCP	Nombre de connexions TCP bloquées et autorisées
Filtrage des datagrammes UDP	Nombre de connexions UDP bloquées et autorisées
Règles de filtrage	Toutes les règles définies pour le pare-feu et informations sur le nombre de tentatives de communication bloquées, autorisées ou ne correspondant pas aux règles de filtrage
Connexions réseau	Informations relatives aux connexions courantes, notamment l'application utilisant la connexion, le protocole utilisé et l'adresse ou le nom des ordinateurs connectés
Dernières 60 secondes	Nombre de connexion réseau et HTTP ainsi que la vitesse de chaque type de connexion

Pour afficher les statistiques détaillées

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.

Réinitialisation des statistiques détaillées

Réinitialisez les compteurs afin d'effacer toutes les statistiques et de recommencer à les enregistrer. Cette opération peut s'avérer utile pour déterminer l'incidence sur les statistiques d'une modification de la configuration.

Pour réinitialiser les compteurs

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans le menu Affichage, choisissez **Réinitialiser les valeurs**.

Définition des statistiques affichées dans la fenêtre Statistiques détaillées

Les utilisateurs peuvent afficher toutes les statistiques détaillées à la fois ou seulement certaines catégories.

Pour définir les statistiques affichées dans la fenêtre Statistiques détaillées

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans la fenêtre Statistiques détaillées, cliquez sur **Options** dans le menu Affichage.
5. Dans la fenêtre Options sur les statistiques de Norton Personal Firewall, sélectionnez une ou plusieurs catégories de statistiques à afficher.
6. Cliquez sur **OK**.

Affichage des journaux de Norton Personal Firewall

Norton Personal Firewall consigne des informations sur les sites Web visités par les utilisateurs, les actions du pare-feu et toute alerte déclenchée. Les *journaux* incluent des détails sur une partie de l'activité rapportée dans la fenêtre Statistiques.

Les journaux sont organisés en neuf onglets.

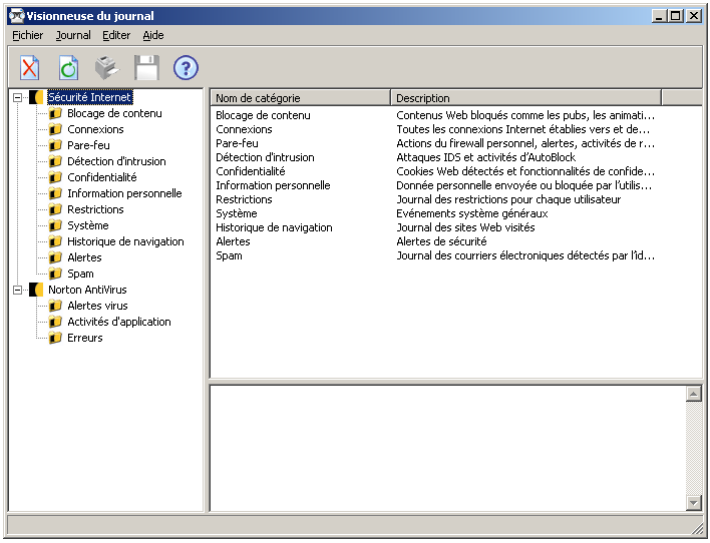
Blocage de contenu	Détails sur les publicités, les images, les applets Java et les contrôles ActiveX bloqués par Norton Personal Firewall.
Connexions	Historique de toutes les connexions réseau TCP/IP établies avec cet ordinateur et indiquant la date et l'heure de la connexion, l'adresse de l'ordinateur auquel vous vous êtes connecté, le service ou le numéro de port utilisé, la quantité d'informations transférée et la durée totale de la connexion.
Pare-feu	Communications interceptées par le pare-feu, incluant les règles appliquées, les alertes affichées, les ports inutilisés bloqués et les événements AutoBlock.
Détection d'intrusion	Etat de la détection d'intrusion (active ou inactive), signatures d'attaques contrôlées et nombre d'intrusions bloquées.
Confidentialité	Cookies bloqués, notamment le nom du cookie et du site Web qui a demandé le cookie.
Informations confidentielles	Historique de toutes les informations confidentielles protégées envoyées sur Internet.
Système	Erreurs système graves, état courant du filtrage IP, si le programme connecté a démarré en tant que service Windows, programmes utilisant trop de ressources ou ne fonctionnant pas dans des conditions optimales.
Historique de navigation	URL visitées par l'ordinateur, fournissant un historique de l'activité Web.
Alertes	Toutes les activités d'alerte déclenchées par d'éventuelles attaques sur votre ordinateur.

Affichage des journaux

Affichez les journaux Norton Personal Firewall depuis la fenêtre Statistiques.

Pour afficher les journaux

1. Ouvrez Norton Personal Firewall.
2. Effectuez l'une des opérations suivantes :
   - Dans Security Center, cliquez sur **Statistiques** > **Afficher les journaux** .
   - Dans Security Monitor, cliquez sur **Afficher le journal** dans le menu Sélectionner une tâche.



3. Dans la fenêtre Afficheur du journal, sélectionnez le journal à consulter.
4. Quand vous avez terminé, cliquez sur un autre journal ou cliquez sur **OK** pour fermer l'Afficheur.

Actualisation des journaux

Les journaux sont automatiquement actualisés lorsque vous passez de l'un à l'autre. Pour afficher les événements *réseau* qui se sont produits depuis que vous avez commencé à consulter l'Afficheur, vous pouvez actualiser manuellement tous les journaux ou des journaux individuels.

Pour actualiser tous les journaux à la fois

- Dans l'Afficheur, cliquez avec le bouton droit de la souris sur **Norton Personal Firewall**, puis cliquez sur **Actualiser toutes les catégories**.

Pour actualiser un journal individuel

- Dans l'Afficheur du journal, cliquez avec le bouton droit de la souris sur le journal à actualiser, puis cliquez sur **Actualiser la catégorie**.

Purge des journaux

Si vous utilisez Internet de façon intense ou si d'autres ordinateurs se connectent régulièrement au vôtre, vos fichiers journaux peuvent contenir des informations sur des centaines de *connexions*. Ce facteur risque de compliquer l'identification d'activités spécifiques ou l'évaluation de l'impact de toute modification apportée aux paramètres de Norton Personal Firewall.

Purgez les journaux afin de supprimer les informations sur d'anciennes connexions. Cette opération permet de constater la façon dont les changements de paramètres affectent votre protection. Vous pouvez purger un seul journal ou tous les journaux à la fois.

Pour supprimer un seul journal

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur du journal, cliquez avec le bouton droit de la souris sur le journal à purger, puis cliquez sur **Purger la catégorie**.

Pour purger tous les journaux à la fois

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur, cliquez avec le bouton droit de la souris sur **Norton Personal Firewall**, puis cliquez sur **Purger toutes les catégories**.

Modification de la taille des journaux

Norton Personal Firewall stocke les informations de chaque journal dans un fichier distinct. Vous pouvez modifier la taille de ces fichiers afin de contrôler l'espace disque qu'ils occupent. Lorsque les fichiers atteignent leur taille maximale, les nouveaux événements remplacent les plus anciens.

Par défaut, la taille des fichiers journaux est de 64 Ko à 512 Ko. Pour que les informations couvrent une période plus longue, augmentez la taille du journal. Si vous avez besoin de libérer de l'espace sur le disque dur, réduisez cette taille. Le changement de taille d'un fichier journal efface toutes les informations qu'il contient.

Pour modifier la taille d'un journal

1. Ouvrez Norton Personal Firewall.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur, cliquez avec le bouton droit de la souris sur un journal, puis cliquez sur **Changer la taille du fichier journal**.
   La boîte de dialogue Taille de fichier journal affiche la taille actuelle du journal.
5. Dans la boîte de dialogue Taille de fichier journal, sélectionnez une nouvelle taille de fichier.
6. Cliquez sur **OK**.

Dépannage de Norton Personal Firewall

A

Les informations de ce chapitre vous permettent de résoudre les problèmes les plus courants. Si vous ne trouvez pas ici la solution au problème, vous trouverez sur le site Web de Symantec une véritable mine d'informations. Vous y trouverez des mises à jour, des correctifs, des didacticiels en ligne, des articles de base de connaissances et des outils de suppression de virus.

Pour explorer le site Web de support technique Symantec

1. Accédez au site www.symantec.fr/frsupport/.
2. Sur la page Web Service et support, cliquez sur la catégorie d'utilisateur dont vous faites partie.
3. Sur la page d'accueil, cliquez sur le lien vers les informations qui vous intéressent.

Si vous ne trouvez pas ce que vous cherchez avec les liens, lancez une recherche sur le site.

Pour explorer le site Web de support technique Symantec

1. Du côté gauche d'une fenêtre du site Symantec, cliquez sur **Chercher**.
2. Tapez un mot ou une phrase correspondant aux informations que vous cherchez. Suivez ces consignes pour rechercher des informations sur le site de Symantec :
   - Tapez un terme unique en minuscules pour trouver toutes les correspondances du terme, y compris les correspondances partielles. Par exemple, tapez install pour trouver les articles contenant le terme installe, installation, installer, etc.

- Tapez plusieurs termes pour trouver toutes les occurrences de n'importe quel terme. Par exemple, tapez définitions virus pour trouver les articles contenant définitions, virus ou les deux termes.
- Tapez une phrase entre guillemets pour trouver les articles contenant la phrase exacte.
- Utilisez le signe plus (+) devant tous les termes de recherche pour trouver les articles contenant tous les termes. Par exemple, tapez +Internet +Security pour trouver les articles contenant les deux termes.
- Pour rechercher une correspondance exacte, tapez les termes recherchés en majuscules.
- Pour rechercher des phrases multiples, encadrez chacune avec des guillemets et séparez-les avec des virgules. Par exemple, "achat de produits", "MAC", "Norton SystemWorks" recherche les trois phrases et trouve tous les articles contenant l'une des trois.

3 Sélectionnez la zone du site Web sur laquelle vous voulez mener la recherche.

4 Cliquez sur **Chercher**.

Dépannage des problèmes de Norton Personal Firewall

Consultez l'onglet Sommaire pour des solutions aux problèmes éventuels de Norton Personal Firewall

Quel est le problème avec ce site Web ?

Norton Personal Firewall peut bloquer certains éléments d'un site Web et empêcher l'affichage correct des données dans le navigateur Web. Dans certains cas, l'accès au site est impossible.

Se reporter à "Désactivation temporaire de Norton Personal Firewall" à la page 49.

Si vous devez voir le site, désactivez Norton Personal Firewall et réessayez d'accéder au site Web. Rappelez-vous que quand vous désactivez Norton Personal Firewall, votre ordinateur est vulnérable aux attaques par Internet.

Si vous ne parvenez toujours pas à vous connecter au site Web avec Norton Personal Firewall désactivé, il se peut que le problème soit lié à Internet ou à votre *fournisseur d'accès Internet*.

Problème	Solution
Il peut s'agir du Blocage des cookies	De nombreux sites Web nécessitent pour s'afficher correctement que les cookies soient activés sur l'ordinateur. Se reporter à "Modification du paramètre Blocage des cookies" à la page 104.
Il peut s'agir d'une règle de filtrage.	Une règle de filtrage peut bloquer le site Web. Si c'est le cas, vous verrez probablement un message indiquant que la connexion n'a pu être établie. Se reporter à "Personnalisation de la protection du pare-feu" à la page 78.
Il peut s'agir du Blocage des publicités	Le blocage de publicités sur Internet empêche parfois un site Web tout entier de s'afficher dans votre navigateur. Se reporter à "Blocage des publicités sur Internet" à la page 107.
Il peut s'agir du Blocage ActiveX ou Java.	Certains sites Web n'affichent que des contrôles ActiveX ou des applets Java. Si vous les bloquez, aucun élément ne sera affiché sur ces sites. Se reporter à "Modification de paramètres de sécurité individuels" à la page 80.
Il peut s'agir du Blocage Flash	Certains sites Web utilisent Macromedia Flash pour créer des pages d'accueil interactives. Si vous bloquez Flash, aucun élément ne sera affiché sur ces sites. Se reporter à "Activation ou désactivation du Blocage Flash" à la page 110.

Pourquoi ne puis-je pas publier des informations en ligne ?

Se reporter à "Identification des informations confidentielles à protéger" à la page 100.

Si vous ne parvenez pas à publier des informations sur un site Web, vérifiez si la fonction Confidentialité bloque ces informations. Vérifiez dans la liste Informations confidentielles de la fenêtre Confidentialité si les données que vous souhaitez saisir sont bloquées.

Pourquoi un courrier électronique que j'ai envoyé n'est-il jamais arrivé ?

Si vous choisissez de bloquer un *courrier électronique* contenant des informations confidentielles, Norton Personal Firewall supprime immédiatement le message. Votre programme de messagerie indiquera que le courrier a été envoyé mais le destinataire ne le recevra pas.

Si votre programme de messagerie enregistre le courrier sortant, vous pouvez ouvrir le dossier Eléments envoyés, modifier le message et l'envoyer.

Pourquoi Norton Personal Firewall ne m'envoie-t-il pas d'avertissement avant d'autoriser des applications à accéder à Internet ?

Se reporter à "Activation du Contrôle des programmes automatique" à la page 83.

Si le Contrôle automatique des programmes est activé, Norton Personal Firewall crée des règles pour les applications reconnues sans vous en avertir.

Pourquoi ne puis-je pas imprimer vers une imprimante partagée ou me connecter à un ordinateur du réseau local ?

Norton Personal Firewall bloque l'utilisation du réseau Microsoft afin d'éviter une connexion à votre ordinateur depuis Internet.

Se reporter à "Organisation des ordinateurs en zones de réseau" à la page 67.

Pour autoriser l'utilisation du réseau local, notamment le partage de fichiers et d'imprimantes, placez les ordinateurs du réseau dans la zone Approuvés.

Pourquoi ne puis-je pas me connecter à Internet par l'intermédiaire d'un modem câble ?

Si votre réseau accède à Internet au moyen d'une *connexion* par câble, vous aurez peut-être besoin de rendre visible le nom NetBIOS de votre ordinateur. Le nom NetBIOS est visible, mais les fichiers et les dossiers de l'ordinateur restent cachés.

Pour rendre visible le nom NetBIOS

1. Ouvrez Norton Personal Firewall.
2. Dans Security Center, cliquez deux fois sur **Firewall personnel**.

3 Dans la fenêtre Firewall personnel, cliquez sur **Règles générales** sur l'onglet Avancé.

4 Dans la boîte de dialogue Règles générales, cliquez sur **Nom NetBIOS entrant par défaut**.

5 Cliquez sur **Modifier**.

6 Sur l'onglet Action de la boîte de dialogue Modifier une règle, cliquez sur **Autoriser l'accès à Internet**.

7 Cliquez sur **OK**.

8 Dans la boîte de dialogue Règles générales, cliquez sur **OK**.

9 Dans la fenêtre Firewall personnel, cliquez sur **OK**.

Certains fournisseurs de services Internet analysent les ports sur les ordinateurs des utilisateurs afin de s'assurer qu'ils respectent les accords de niveau de service. Norton Personal Firewall peut considérer cette opération comme une *analyse de port* malveillante et interrompre les communications avec le système câble. Si c'est le cas, vous devrez laisser votre opérateur exécuter des analyses de port.

Pour autoriser les analyses de port du FAI

1 Ouvrez Norton Personal Firewall.

2 Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.

3 Dans la fenêtre Détection d'intrusion, cliquez sur **Adresse IP**.

4 Dans la boîte de dialogue Exclusions, sélectionnez l'adresse IP utilisée par votre FAI pour les analyses de port.
Renseignez-vous auprès de votre FAI pour connaître l'adresse IP utilisée.

5 Cliquez sur **Exclure**.

6 Cliquez sur **OK**.

Comment un site Web peut-il accéder aux informations sur mon navigateur ?

Les paramètres de Confidentialité de navigation empêchent le navigateur de transmettre des informations le concernant. Toutefois, certains sites de diagnostic sur Internet peuvent accéder aux informations sur le navigateur, même si les paramètres de Confidentialité de navigation sont activés pour les bloquer.

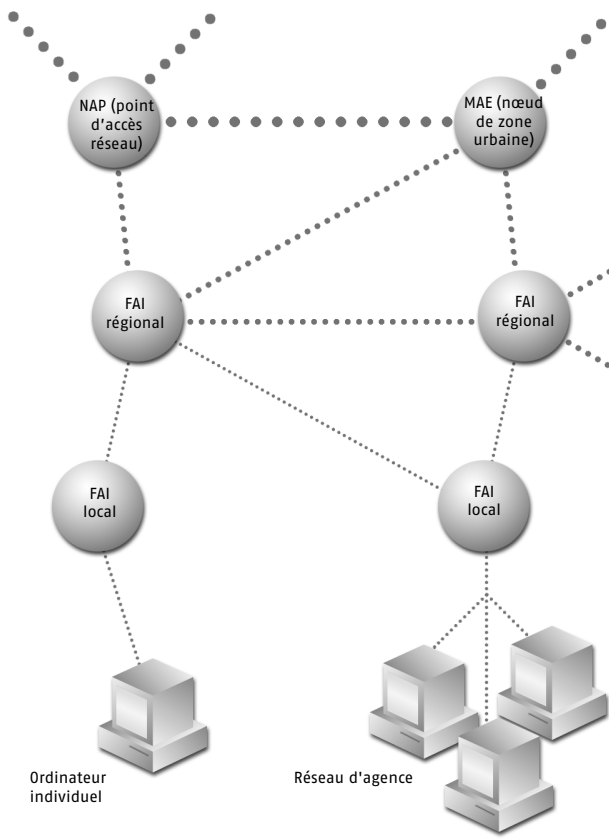
Si vous avez bloqué les *applets Java*, les *contrôles ActiveX* ou les scripts, il est possible que le site utilise l'une de ces méthodes pour lire ces informations. Parfois, lorsque des serveurs Web n'accèdent pas aux informations sur le navigateur, ils utilisent les dernières informations reçues. Dans ce cas, vous pourrez voir les informations de la dernière personne qui a visité le site.

A propos d'Internet

B

Internet est l'interconnexion de millions d'ordinateurs à travers le monde. Il se compose de tous les ordinateurs et de toutes les connexions qui permettent à un ordinateur sur Internet de communiquer avec tout autre ordinateur sur Internet.

Internet peut se comparer à un système de routes et d'autoroutes. Les grands axes d'Internet constituent l'infrastructure et véhiculent de gros volumes d'informations sur de longues distances. Sur ces axes, il y a des interconnexions, appelés NAP (Network Access Point - point d'accès réseau) et des MAE (Metropolitan Area Exchanges - nœud de zone urbaine). Il existe également des "autoroutes régionales", fournies par de grands FAI et des "rues" fournies par des FAI locaux.



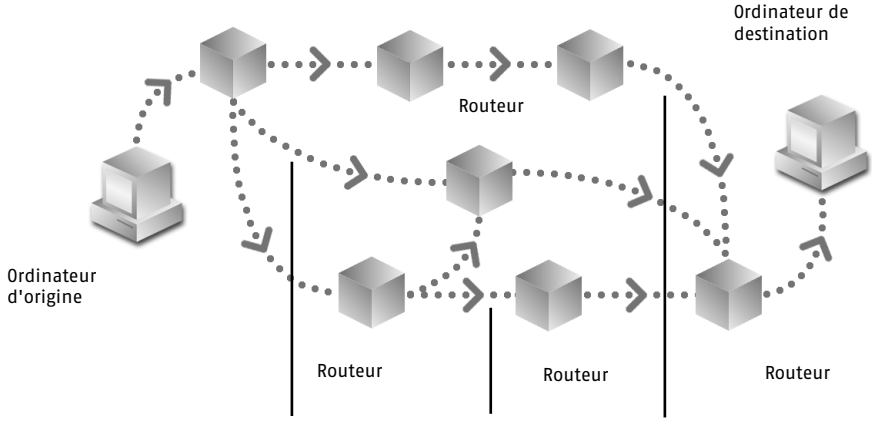
Tout comme un système de routes et d'autoroutes, Internet fournit plusieurs itinéraires pour aller d'un point à un autre. Si une partie d'Internet est encombrée ou endommagée, les informations sont redirigées.

Transmission des informations sur Internet

Toutes les informations envoyées sur Internet sont transmises à l'aide d'un protocole appelé *TCP/IP*. Comme tous les ordinateurs sur Internet comprennent ce protocole, ils peuvent tous communiquer entre eux. TCP et IP sont des parties distinctes de ce protocole.

Internet est un *réseau de commutation par paquets*. Chaque communication est divisée en *paquets* par le protocole TCP (Transmission Control Protocol). Chaque paquet contient les adresses des ordinateurs d'origine et de destination, ainsi que les informations à communiquer.

Le protocole *IP (Internet Protocol)* est chargé de l'acheminement des paquets vers leur destination. Chaque paquet peut suivre un itinéraire différent sur Internet et être subdivisé en *fragments*. Les paquets traversent Internet, en se déplaçant d'un *routeur* à un autre. Les routeurs consultent l'adresse de destination et transmettent le paquet au routeur suivant. IP ne garantit toutefois pas la livraison de chaque paquet.



Itinéraires qu'un paquet ou des fragments de paquet peuvent suivre

Sur l'ordinateur de destination, le protocole TCP réunit les paquets afin de reconstituer la communication complète. Il peut avoir à réorganiser les paquets s'ils ne sont pas arrivés dans l'ordre ainsi qu'à reconstruire les paquets fragmentés. Le protocole TCP demande également la retransmission des paquets manquants.

Le terme TCP/IP est souvent utilisé pour faire référence à un groupe de protocoles utilisés sur Internet, incluant UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) et IGMP (Internet Group Membership Protocol).

A propos du protocole UDP

Le protocole UDP (User Datagram Protocol) est utilisé dans les cas où la fiabilité de TCP n'est pas nécessaire, comme la diffusion d'images vidéo sur plusieurs ordinateurs simultanément. Le protocole UDP n'assure pas la correction des erreurs ni la retransmission des paquets perdus. Du point de l'importance pour la navigation sur Internet, UDP occupe le deuxième rang après TCP.

A propos du protocole ICMP

Les paquets ICMP (Internet Control Message Protocol) contiennent des informations sur les erreurs et des informations de contrôle. Ils sont utilisés pour signaler les erreurs réseau, la congestion du réseau et les dépassements de délai ainsi que pour faciliter le dépannage.

Norton Internet Security accepte normalement les paquets ICMP entrants qui fournissent des informations et présentent un risque minimal. Vous pouvez créer des règles pour bloquer tout ou partie des paquets ICMP.

A propos du protocole IGMP

Le protocole IGMP (Internet Group Membership Protocol) sert à établir des appartenances à des groupes de multidiffusion, séries d'ordinateurs recevant des messages simultanés d'un seul ordinateur. En général, le protocole IGMP sert à diffuser de la vidéo et d'autres données multimédia sur Internet. Votre ordinateur indique à un routeur proche qu'il désire recevoir les messages adressés à un groupe de multidiffusion spécifique.

Le protocole IGMP ne présente pas de risque de sécurité majeur, mais Norton Internet Security vous permet néanmoins de le bloquer totalement. Vous pouvez le bloquer si aucun de vos programmes ne nécessite IGMP. Si vous avez des problèmes de réception d'informations de multidiffusion, par exemples des films ou des présentations PowerPoint, vérifiez que le protocole IGMP n'est pas bloqué.

Stockage des informations du Web sur Internet

Les informations du Web sont stockées sous forme de pages, chacune ayant un nom unique appelé *URL (Uniform Resource Locator)*.

Lorsque vous tapez une adresse Web dans la barre d'adresse du navigateur ou que vous cliquez sur un lien du navigateur Web pour afficher un nouveau site Web, vous fournissez au navigateur l'URL de la page à afficher. Par exemple, www.symantec.fr est une URL standard.

Chaque URL se rattache à l'adresse IP de l'ordinateur qui stocke la page Web. Les URL sont utilisées car elles sont plus faciles à mémoriser que des adresses IP.

Avant de demander une page, votre navigateur demande à un *serveur DNS (Domain Naming System)* l'adresse IP du site Web. Les adresses IP sont des nombres sur 32 bits qui se présentent sous la forme de quatre nombres décimaux, compris entre 0 et 255 et séparés par des points : 206.204.104.148. Chaque ordinateur sur Internet possède une adresse IP distincte.

Demande d'une page

Quand le navigateur dispose de l'adresse IP, il établit une *connexion* TCP au serveur Web et demande la page. Chaque page affichée nécessite une nouvelle connexion au serveur Web. En fait, la plupart des pages nécessitent plusieurs connexions, car chaque graphique (ainsi que de nombreux autres éléments de page) nécessitent une connexion distincte.

Une fois la page chargée, toutes les connexions sont abandonnées. Le processus se répète pour chaque page du site, bien que le navigateur garde en mémoire son adresse IP. Certains sites Web récentes utilisent le protocole HTTP 1.1 (HyperText Transfer Protocol version 1.1), capable d'établir une seule connexion pour transmettre plusieurs fichiers et rester ouverte pour plusieurs pages.

Présentation des URL

Une URL standard se présente comme suit : http://www.symantec.com/securitycheck/index.html. Etant donné que vous pouvez souhaiter bloquer certaines parties seulement d'un *domaine*, vous devez connaître la composition d'une URL.

http://	Protocole de programme utilisé pour établir la connexion. Le protocole le plus utilisé pour naviguer sur le Web est HTTP (HyperText Transfer Protocol). Si vous n'indiquez pas de protocole de programme, votre navigateur utilise http par défaut. FTP (File Transfer Protocol) et gopher sont d'autres protocoles souvent utilisés.
.com	Domaine racine ou domaine de premier niveau. Il existe plusieurs domaines racine courants, notamment .com, .net, .edu, .org, .mil et .gov. Il existe également des domaines racine de deux lettres pour la plupart des pays, par exemple .fr pour la France, .ca pour le Canada et .uk pour le Royaume-Uni.
symantec.com	Domaine. Il s'agit du domaine avec lequel le navigateur établit une connexion. Un domaine correspond souvent à une seule société ou organisation qui peut disposer de plusieurs sites Web sur Internet.
www.symantec.com	Hôte. C'est le site Web spécifique avec lequel le navigateur communique. C'est également le nom pour lequel le serveur DNS fournit une adresse IP.
securitycheck	Dossier ou répertoire qui contient le fichier à afficher.
index.html	Nom du fichier à afficher.

Une URL spécifique, localhost, identifie votre ordinateur vis-à-vis de lui-même. Si votre ordinateur est équipé d'un logiciel de serveur Web, saisissez http://localhost pour afficher votre page Web. L'adresse IP correspondant à localhost est 127.0.0.1.

Identification des programmes sur les serveurs par les ports

Les *ports*, également appelés *sockets*, indiquent l'emplacement de programmes ou de serveurs spécifiques de l'ordinateur distant avec lequel vous essayez d'établir une communication. Il est ainsi possible d'exécuter plusieurs programmes Internet simultanément sur un même ordinateur. Par exemple, de nombreux ordinateurs connectés à Internet exécutent à la fois des serveurs Web et FTP. Le serveur Web utilise le port 80, alors que le serveur FTP utilise le port 21.

Les ports sont numérotés de 1 à 65535. Les ports 1 à 1 023 sont dits "ports connus" et sont utilisés par défaut pour de nombreux programmes Internet.

Les ports font partie des *URL*, mais sont rarement affichés. Le *numéro de port* suit le nom de l'hôte et un signe deux-points. Par exemple :

http://www.symantec.com:80/securitycheck/index.html

Les ports les plus utilisés étant standard, leur numéro est rarement affiché. Les navigateurs Web, par exemple, utilisent pratiquement toujours le port 80. Il n'est donc pas nécessaire de l'indiquer, à moins d'utiliser un port différent.

Les termes serveur et *service* sont utilisés de manière pratiquement interchangeable. Par exemple, un serveur Web fournit le service HTTP, et on dit généralement qu'un ordinateur exécute le service *Finger*.

Ports connus

Voici quelques-uns des ports connus les plus courants.

Port par défaut	Nom du service	Programme
20	ftp-data	Données FTP (File Transfer Protocol)
21	ftp	Contrôle FTP (File Transfer Protocol)
23	telnet	Gestionnaire de terminal Telnet
25	smtp	Protocole SMTP (Simple Mail Transfer Protocol)
53	domaine	Recherche DNS (Domain Naming System)
79	finger	Finger

Port par défaut	Nom du service	Programme
80	http	Protocole HTTP (HyperText Transfer Protocol)
110	pop3	POP3 (Post Office Protocol 3)
113	auth	Service d'authentification d'identité
119	nntp	Protocole NNTP (Network News Transfer Protocol)
137	nbname	Nom NetBIOS (réseau Microsoft)
138	nbdatagram	Datagramme NetBIOS (réseau Microsoft)
139	nbsession	Session NetBIOS (réseau Microsoft)
143	imap	Protocole IMAP (Internet Message Access Protocol)
194	irc	Protocole IRC (Internet Relay Chat)
389	ldap	Protocole LDAP (Lightweight Directory Access Protocol)
443	https	Protocole HTTPS (HTTP sécurisé)

Identification des ordinateurs sur Internet

Des millions d'ordinateurs sont connectés à Internet. Lorsque vous essayez d'identifier des ordinateurs, il est plus simple de travailler avec des groupes d'ordinateurs plutôt que de les identifier individuellement. Les masques de *sous-réseau* permettent d'identifier un groupe d'ordinateurs apparentés, par exemple ceux de votre réseau local.

Un masque de sous-réseau standard se présente comme suit : 255.255.255.0. Les nombres 255 indiquent les parties de l'adresse IP identiques pour tous les ordinateurs du sous-réseau, alors que le 0 indique une partie différente de l'adresse IP.

Les masques de sous-réseau sont toujours utilisés en conjonction avec une adresse IP de base. L'adresse IP de base est une adresse IP qui, lorsqu'elle est traitée avec le masque de sous-réseau, peut indiquer toutes les adresses IP d'un sous-réseau.

Exemple d'adresse IP de base/paire de sous-réseau :

Adresse IP de base : 10.0.0.1

Masque de sous-réseau : 255.255.255.0

Dans cet exemple, la plage d'adresses IP identifiée par l'adresse IP de base et le masque de sous-réseau est comprise entre 10.0.0.1 et 10.0.0.255. Le masque de sous-réseau le plus utilisé est le masque 255.255.255.0 car il identifie un groupe d'adresses IP relativement petit, jusqu'à 254 ordinateurs. Il est généralement utilisé pour de très petits groupes d'ordinateurs, par exemple des groupes de deux ordinateurs seulement.

Risques et menaces liés à Internet

Norton Internet Security vous protège contre les risques majeurs liés à Internet. Ces risques incluent des menaces telles qu'une intrusion dans votre réseau, un code malveillant dans un *contenu actif*, l'exposition à un contenu inopportun, la divulgation d'informations confidentielles et la contamination par des virus provenant de fichiers infectés.

Risques liés aux pirates

A l'origine, les *hackers* étaient des personnes capables de résoudre des problèmes informatiques complexes et d'écrire des programmes rapidement. La signification de ce terme a toutefois changé et désigne aujourd'hui un "pirate" qui utilise ses connaissances en informatique à des fins illicites. Le mot hacker ayant au départ une connotation positive, on utilise parfois le terme *cracker* comme forme péjorative. Dans le présent document, le terme "pirate" correspond à cette connotation péjorative.

D'autres termes anglais désignent les pirates, comme script-kiddies, wannabes et packet monkeys. Ils s'appliquent tous à des pirates en herbe qui utilisent des applications écrites par des pirates plus expérimentés pour attaquer des ordinateurs sur Internet.

Déroulement d'une attaque de pirate

La plupart des attaques de pirate se déroulent de la manière suivante :

- Collecte d'informations
  Le pirate rassemble le maximum d'informations sur votre ordinateur. Il tente ensuite de trouver des failles, sans que vous sachiez que votre ordinateur subit une attaque.
- Accès initial
  Le pirate exploite une faille décelée pendant la collecte d'informations et établit un point d'entrée dans votre ordinateur.
- Escalade des droits
  Le pirate gagne l'accès à davantage de programmes et de *services* sur votre ordinateur.
- Effacement des traces :
  le pirate masque ou supprime toute trace de sa visite, en laissant parfois une porte ouverte pour une future intrusion.

Collecte d'informations

La première étape de la collecte d'informations consiste à définir une cible. Un pirate peut choisir une personne ou une société à attaquer ou rechercher sur Internet une cible non protégée qui sera facile à attaquer. La quantité d'informations disponibles à votre propos sur Internet est directement proportionnelle à votre présence sur le Web. Si vous avez un nom de *domaine* et un site Web, une plus grande quantité d'informations est à la portée de tout le monde que si vous ne disposez que d'une *adresse électronique*.

Si un pirate a choisi une cible spécifique, comme une société ou une organisation, de nombreuses ressources sur Internet lui permettent de collecter des informations. Grâce à Internet, un pirate peut en apprendre beaucoup sur une cible potentielle. Avec un nom de domaine, il est facile de trouver le nom et l'adresse du propriétaire, ainsi que le nom et le numéro de téléphone des contacts administratifs et techniques. Ces informations ne peuvent généralement pas être utilisées directement pour attaquer un réseau ou un ordinateur, mais peuvent servir à rassembler plus informations.

Si un pirate n'a pas de cible précise, de nombreux outils permettent d'analyser Internet pour rechercher des cibles potentielles. L'analyse la plus simple consiste à utiliser la commande "ping", qui permet d'analyser rapidement des milliers d'ordinateurs. Le pirate utilise un programme pour lancer des "ping" à des ordinateurs dans des plages définies d'adresses IP. Une réponse indique au pirate qu'un ordinateur est connecté et utilise l'adresse IP correspondante. Lorsque Norton Internet Security est en cours d'exécution, votre ordinateur est masqué aux analyses ping car il ne répond pas. Le pirate ne peut donc pas déterminer qu'un ordinateur se trouve à votre adresse IP avec une simple commande ping.

Les *analyses de port* permettent une analyse plus approfondie, généralement effectuée sur un seul ordinateur. Une analyse de port peut indiquer à un pirate les services en cours d'exécution, comme HTTP et FTP. Chaque service en cours d'exécution fournit un point d'entrée potentiel au pirate. Sur des ordinateurs non protégés, les ports non utilisés répondent qu'ils sont fermés, indiquant ainsi au pirate qu'un ordinateur existe à cette adresse IP. Norton Internet Security ne répond pas aux analyses de ports non utilisés, en les *masquant*.

Accès initial

Le moyen le plus facile pour un pirate d'accéder à un ordinateur Windows consiste à utiliser la fonctionnalité de réseau Microsoft. Sur de nombreux ordinateurs, le réseau Microsoft est activé afin que les utilisateurs du réseau puissent s'y connecter.

La fonction de réseau NetBIOS de Microsoft utilise trois des ports les plus connus. Ces ports sont utilisés pour établir des *connexions* entre des ordinateurs d'un réseau Microsoft. En fait, ils indiquent normalement le nom de l'ordinateur sur le réseau local. C'est l'effet recherché sur votre réseau, mais pas du tout sur Internet. Norton Internet Security est configuré par défaut pour bloquer ces ports et éviter ainsi qu'une personne sur Internet ne puisse se connecter à votre ordinateur à l'aide de la fonctionnalité de réseau Microsoft. Si votre ordinateur est connecté à un réseau local ainsi qu'à Internet, vous devez modifier certains paramètres pour permettre les communications avec les autres ordinateurs du réseau. Norton Internet Security continue à vous protéger contre les risques liés à Internet tout en vous permettant d'utiliser votre réseau local.

Escalade des droits

Une fois qu'un pirate est connecté à votre ordinateur, son objectif suivant consiste à augmenter le plus possible son contrôle. Les étapes impliquées et les résultats obtenus varient en fonction de la version de Windows installée sur l'ordinateur cible.

Sur les ordinateurs équipés de Windows 95/98/Me, un pirate n'a pas besoin d'augmenter son contrôle une fois qu'il a accès à l'ordinateur. Il détient un contrôle total sur l'ordinateur. Heureusement, ces versions de Windows ne possèdent pas de nombreuses fonctions de contrôle à distance et sont donc relativement faciles à protéger.

Sur les ordinateurs équipés de Windows NT/2000/XP, le pirate va tenter d'obtenir des droits d'administrateur sur l'ordinateur. La clé pour obtenir ces droits est généralement un *mot de passe*. Un pirate peut télécharger votre fichier de mots de passe et le décoder.

Une autre tactique consiste à placer un *cheval de Troie* sur votre ordinateur. Si un pirate parvient à placer un programme comme Back Orifice, Subseven ou NetBus sur votre ordinateur et à l'exécuter, il peut prendre le contrôle total de l'ordinateur.

D'autres chevaux de Troie peuvent enregistrer le texte tapé au clavier afin de capturer les mots de passe et d'autres données stratégiques. Norton Internet Security et Norton AntiVirus fournissent deux niveaux de protection contre les chevaux de Troie. Norton AntiVirus vous protège contre l'exécution accidentelle de ces programmes. Norton Internet Security bloque les ports que les chevaux de Troie d'accès à distance utilisent pour communiquer sur Internet.

Effacement des traces

Lorsqu'un pirate a gagné un maximum de contrôle sur un ordinateur, il cherche ensuite à effacer les preuves. Tant que vous n'êtes pas conscient qu'un pirate a investi votre ordinateur, vous n'agissez pas pour l'arrêter.

Dans le cas d'ordinateurs fonctionnant sous Windows 2000/XP, les pirates tentent de désactiver les fonctions d'audit et de modifier ou d'effacer le *journal* des événements. Sur tout ordinateur, un pirate peut cacher des fichiers afin de les avoir à disposition lors de visites ultérieures. Dans des cas extrêmes, un pirate peut formater le disque dur d'un ordinateur attaqué afin d'éviter d'être identifié.

Risques liés à des contenus actifs

Les *contrôles ActiveX* et les *applets Java* sont désignés *contenus actifs* parce qu'ils vont au-delà du simple affichage de texte ou de graphiques. La plupart des contenus actifs ne sont pas dangereux. Ils sont couramment utilisés pour afficher des menus contextuels et le cours actualisé de valeurs boursières, par exemple.

Les contrôles ActiveX et les applets Java sont supposés être sûrs pour être exécutés dans votre navigateur. ActiveX utilise un système de certificats numériques qui vous permet de décider si vous souhaitez exécuter un contrôle ActiveX. Les certificats numériques se présentent sous la forme de boîtes de dialogue qui vous demandent si vous souhaitez installer et exécuter un contrôle qui apparaît lorsque vous naviguez sur le Web.

L'utilisation de certificats numériques pose plusieurs problèmes. Certains contrôles ne sont pas accompagnés de certificats et certains certificats fournissent très peu d'informations sur les fonctions du contrôle.

Le sandbox ("bac à sable") Java a été conçu pour empêcher les applets Java d'accéder à des informations en dehors du navigateur et de faire quoi que ce soit qui risque d'endommager l'ordinateur. Toutefois, les *pirates* trouvent sans cesse des moyens de contourner les protections Java et d'utiliser les fonctionnalités de Java de façon non prévue par leurs développeurs.

Norton Internet Security contrôle les contenus actifs et peut les bloquer tous ou vous avertir chaque fois qu'il rencontre un contenu actif. La fonction de protection automatique de Norton AntiVirus détecte les contrôles ActiveX et les applets Java dangereux et empêche leur exécution.

Norton Personal Firewall contrôle les contenus actifs et peut les bloquer tous ou vous avertir chaque fois qu'il rencontre un contenu actif.

Risques liés à des activités et des contenus inadaptés

Internet offre un trésor d'informations aisément accessible à tous. Certains sujets ne conviennent toutefois pas à tous les publics. Par exemple, la plupart des gens estiment que les sites consacrés à la pornographie ou à la violence sont inadaptés aux enfants. Vous pouvez également souhaiter restreindre l'accès à d'autres types de contenus.

Blocage de catégories de sites et de groupes de discussion

Norton Internet Security vous permet de sélectionner les sites Web et les groupes de discussion auxquels les utilisateurs auront accès depuis cet ordinateur. Comme il peut être nécessaire d'attribuer différents niveaux d'accès à différents publics, Norton Internet Security permet de bloquer des contenus spécifiques pour chaque utilisateur.

Restriction d'accès aux applications

Certaines applications Internet peuvent également être inappropriées sur votre ordinateur. Vous pouvez, par exemple, ne pas souhaiter que vos enfants utilisent des applications de discussion en direct. Vous pouvez également vouloir restreindre l'utilisation des programmes de transfert de fichiers. Vous réduirez ainsi le risque d'introduire dans votre ordinateur ou votre réseau des virus, des vers, des zombies, des *chevaux de Troie* et autre code dangereux.

Norton Internet Security permet de sélectionner les catégories de programmes qui auront accès à Internet. Il tient à jour la liste de programmes, de sorte que votre protection reste actualisée, même en cas de sortie de nouveaux programmes. Vous pouvez également ajouter des applications personnalisées et contrôler leur utilisation.

Risques liés à la confidentialité

Internet présente un certain nombre de risques en matière de confidentialité. Certains sites collectent et enregistrent des informations personnelles, comme les numéros de carte de crédit. D'autres suivent l'utilisation que vous faites d'Internet. Certaines applications envoient à votre insu à des sites Web des informations sur l'utilisation que vous faites de votre ordinateur.

Envoi d'informations confidentielles

Vous ne souhaitez certainement pas que des données confidentielles comme votre numéro de carte de crédit ou votre numéro de téléphone personnel, circulent pas en clair sur Internet. Le Contrôle de confidentialité empêche la saisie d'informations confidentielles sur les sites Web qui n'utilisent pas des communications sécurisées et chiffrées, et leur envoi avec des programmes de messagerie instantanée.

Si vous voulez éviter l'envoi de données confidentielles sur Internet, Norton Internet Security peut interdire l'accès des utilisateurs aux sites sécurisés qui risquent de demander des informations personnelles.

Les cookies

Les *cookies* sont des messages envoyés à votre navigateur par un site Web et stockés sous la forme de petits fichiers sur votre ordinateur. Ils sont souvent utilisés par des sites Web pour le suivi de vos visites. Dans la plupart des cas, les cookies ne contiennent aucune information personnelle, mais plutôt des informations permettant aux sites Web de vous identifier.

Bons cookies

Dans leur forme la plus inoffensive, les cookies cessent d'exister lorsque vous fermez votre navigateur. Ce type de cookie est principalement utilisé pour rappeler des choix effectués lors de la consultation d'un site Web.

De nombreux sites laissent des cookies sur votre ordinateur de manière à pouvoir vous identifier lors de votre visite suivante sur le même site. Ces cookies vous identifient de manière à utiliser les options que vous aviez sélectionnées auparavant. Si vous fréquentez un site qui garde en mémoire les valeurs mobilières dont vous souhaitez effectuer le suivi, par exemple, il est probable que ce site utilise ce type de cookie.

Mauvais cookies

Dans l'une de leurs formes malveillantes, les cookies d'un site Web peuvent suivre vos visites sur un autre site Web. Par exemple, la plupart des publicités que vous voyez sur des sites Web ne proviennent pas des sites que vous visitez, mais de sites qui fournissent des publicités à de nombreux autres sites. Lorsque le site de publicité affiche la publicité, il a accès aux cookies de votre ordinateur. Le site de publicité peut ainsi surveiller votre utilisation du Web sur une large gamme de sites et établir un profil.

Blocage des cookies

Norton Internet Security peut bloquer tous les cookies ou vous informer de toutes les demandes de cookie. Si vous bloquez tous les cookies, des fonctionnalités ne seront plus disponibles dans de nombreux sites Web. Par exemple, vous ne pourrez plus effectuer d'achats dans certains magasins en ligne sur Internet. Si vous choisissez d'être informé chaque fois qu'un site Web essaye de créer un cookie, vous serez en mesure d'étudier chaque demande et de bloquer celles qui ne proviennent pas du site que vous visitez. Norton Internet Security peut également bloquer ou autoriser les cookies issus de *domaines* ou de sites Web spécifiques.

Suivi de l'utilisation d'Internet

La plupart des navigateurs transmettent des informations que vous pouvez considérer comme confidentielles. Un élément généralement transmis par votre navigateur aux sites Web est l'*URL* de la page dont vous provenez. Cette information est utilisée par certains sites Web pour vous aider à visiter le site, mais elle peut également servir à surveiller vos habitudes de navigation sur le Web. Norton Internet Security bloque ce genre d'informations.

Votre navigateur envoie également des informations sur lui-même et sur le système d'exploitation utilisé. Norton Internet Security peut bloquer ces informations, mais elles sont généralement utilisées par les sites Web pour fournir les pages Web correspondant à votre navigateur.

Un risque potentiellement plus grand en matière de confidentialité est constitué par les programmes que vous installez sur votre ordinateur et qui, à votre insu, transmettent des informations aux sites Web. Plusieurs programmes dont la fonction est de vous aider à télécharger et à installer des fichiers, transmettent des informations sur vos activités sur Internet. Norton Internet Security préserve votre vie privée en vous prévenant de ces communications.

Risques liés aux chevaux de Troie et aux virus

De nos jours, avec de si nombreux ordinateurs connectés à des réseaux et à Internet, les virus peuvent se propager bien plus rapidement qu'à l'époque où les fichiers étaient transmis d'un ordinateur à un autre à l'aide de disquettes. En outre, le risque ne se limite plus aux virus, mais s'est élargi aux *chevaux de Troie*, vers et zombies.

Un virus est un programme ou un code qui se duplique en s'associant à un autre programme, un secteur d'amorçage, un secteur de partition ou un document qui prend en charge des macros. Si de nombreux virus ne font que se dupliquer, d'autres causent des dommages. Un virus peut arriver dans un *courrier électronique*.

Un cheval de Troie est un programme qui ne se duplique pas, mais qui endommage ou menace la sécurité de l'ordinateur. En principe, il vous est envoyé par courrier électronique par une personne, mais ne s'envoie pas de lui-même. Un cheval de Troie peut arriver déguisé sous la forme d'un utilitaire. Certains chevaux de Troie ont des effets malveillants sur l'ordinateur sur lequel ils sont exécutés, alors que d'autres, comme Back Orifice, fournissent des fonctionnalités de contrôle à distance aux *pirates*.

Un ver est un programme qui crée des copies de lui-même, par exemple d'un disque à un autre ou par courrier électronique. Il peut provoquer des dommages ou menacer la sécurité de l'ordinateur. Un ver peut arriver sous forme de pièce jointe d'un courrier électronique dont le sujet semble intéressant.

Un zombie est un programme installé secrètement qui sommeille sur un ordinateur. Il se réveille ultérieurement, pour contribuer à une attaque collective sur un autre ordinateur. Les programmes zombie ne causent normalement pas de dommages sur l'ordinateur sur lequel ils résident et servent à attaquer d'autres ordinateurs. Un zombie peut arriver sous forme de pièce jointe à un courrier électronique.

Norton AntiVirus vous protège contre la réception et l'exécution de virus, chevaux de Troie, vers et zombies. Il analyse les courriers électroniques lors de leur réception et vérifie les fichiers lors de leur ouverture, apportant ainsi deux niveaux de protection.

Norton Internet Security garantit que les chevaux de Troie ne communiquent pas sur Internet. Vous êtes ainsi protégé des pirates qui utilisent des chevaux de Troie.

Probabilité de subir une attaque

Internet présente de nombreux risques. Quelles sont vos chances d'être victime d'une attaque ? La probabilité qu'un pirate choisisse votre ordinateur en particulier parmi tous ceux connectés à Internet est certainement très faible. Cependant, avec la généralisation des programmes d'analyse de ports et autres outils de détection utilisés par les pirates, les analyses de failles dont votre ordinateur peut faire l'objet sont relativement fréquentes. Plus les failles sont nombreuses, plus votre ordinateur devient tentant pour les pirates.

Les outils permettant de trouver des cibles sont capables d'analyser de très grands groupes d'ordinateurs sur Internet. Le pirate doit simplement indiquer une plage d'adresses IP à analyser. Le programme vérifie chaque adresse IP afin de déterminer la présence éventuelle d'un ordinateur. Si un ordinateur est trouvé, une série de tests est lancée pour déceler des failles, comme la fonctionnalité de réseau Microsoft activée pour Internet. Le pirate revient ensuite consulter une liste d'ordinateurs, avec leurs failles.

Norton Internet Security vous protège contre ces analyses en rendant votre ordinateur invisible. Votre ordinateur ne répond pas à la plupart des requêtes envoyées par ces programmes d'analyse. Puisqu'il ne présente aucune faille au pirate, votre ordinateur devient ainsi une mauvaise cible, le rendant inintéressant pour une attaque.

Glossaire

Ce glossaire fournit la définition de termes Internet couramment utilisés.

adresse IP (adresse Internet Protocol) Identificateur numérique sur 32 bits qui identifie un ordinateur sur Internet.Les adresses IP se présentent généralement sous la forme de quatre groupes de nombres, compris entre 0 et 255 et séparés par des points. Par exemple, 206.204.52.71.

adresse réseau Partie d'une adresse IP commune à tous les ordinateurs d'un réseau ou sous-réseau spécifique.

alerte Boîte de dialogue qui apparaît dans une interface utilisateur graphique (GUI) afin de signaler une erreur ou pour fournir un avertissement.

analyse de port Tentative d'accès à un ordinateur par recherche des ports ouverts.Généralement effectué par un programme automatisé qui envoie une demande à chaque port d'une adresse IP et attend les réponses pouvant révéler une vulnérabilité.

applet Java Petit programme qui s'exécute dans un environnement restreint géré par votre navigateur.La plupart des applets Java servent à ajouter des effets multimédia, une interactivité ou d'autres fonctionnalités à une page Web, mais peuvent également être utilisées à des fins malveillantes, par exemple pour dérober des mots de passe.

bannière publicitaire Graphique publicitaire, souvent animé, qui apparaît en haut d'une page Web et peut contenir un lien vers le site Web à l'origine de la publicité.

cheval de Troie Programme destructeur souvent conçu pour endommager un ordinateur, bien que déguisé en application utile ou intéressante.

communication entrante Tentative d'un ordinateur externe d'établir une connexion avec votre ordinateur. La connexion peut être utilisée pour envoyer des données vers ou depuis l'ordinateur.

communication sortante Tentative effectuée par votre ordinateur pour établir une connexion avec un ordinateur distant.La connexion peut être utilisée pour envoyer des données vers ou depuis votre ordinateur.

connexion Méthode d'échange de données qui permet un transfert fiable entre deux ordinateurs.

contenu actif Matériau d'une page Web qui change dans le temps ou en réponse à une action de l'utilisateur. Les contenus actifs sont mis en œuvre par l'intermédiaire de contrôles ActiveX, de scripts Visual Basic, de scripts Java et d'applets Java dans le code HTML qui définit la page.

contrôle ActiveX Programme qui s'exécute dans un navigateur utilisant la technologie Microsoft pour ajouter des animations à une page Web, de l'audio et de la vidéo en continu, des films, etc.Lorsque vous visitez une page Web contenant un contrôle ActiveX, celui-ci est téléchargé dynamiquement et enregistré sur votre disque dur. Contrairement aux applets Java, les contrôles ActiveX ne s'exécutent pas dans un environnement restreint et peuvent potentiellement prendre le contrôle de votre ordinateur.

cookie Petit fichier de données que certains sites Web placent sur votre disque dur lors de l'affichage d'une page Web.Les serveurs Web peuvent utiliser des cookies pour stocker vos informations personnelles et vos préférences, afin de vous éviter d'avoir à les indiquer de nouveau lors de votre visite suivante.

courrier électronique ("e-mail") Méthode d'échange de messages et de fichiers avec d'autres personnes par l'intermédiaire de réseaux d'ordinateurs.SMTP (Simple Mail Transfer Protocol) est un protocole répandu pour envoyer des courriers électroniques. Les protocoles couramment utilisés pour la réception de messages sont POP3 (Post Office Protocol 3) et IMAP4 (Internet Message Access Protocol 4). Les services de messagerie Web utilisent le protocole HTTP (HyperText Transfer Protocol) pour l'envoi et la réception de courriers électroniques.

cracker Personne qui "craque" du code, pas obligatoirement pour des raisons malveillantes. Terme parfois utilisé pour faire référence à un pirate mal intentionné.

délai limite Période prédéterminée pendant laquelle une tâche donnée doit être exécutée. Si la valeur du délai est atteinte avant ou pendant l'exécution de la tâche, cette dernière est annulée.

DHCP (Dynamic Host Configuration Protocol) Protocole TCP/IP qui attribue automatiquement une adresse IP temporaire à chaque périphérique d'un réseau.

DNS (Domain Naming System) Système d'attribution de noms hiérarchique qui convertit les noms de domaine (comme www.symantec.com) en adresses IP (comme 206.204.212.71).

domaine Adresse commune d'une société ou d'une organisation (comme symantec.com) sur Internet, qui peut représenter plusieurs hôtes.

domaine de niveau supérieur Dernière partie d'un nom de domaine, qui identifie le type d'entité titulaire de l'adresse (comme .com pour des entreprises ou .edu pour les institutions du secteur de l'éducation) ou l'emplacement géographique de l'adresse (par exemple .fr pour la France, .ca pour le Canada ou .uk pour le Royaume-Uni).

FAI (fournisseur d'accès à Internet) Société qui fournit un accès à Internet à des particuliers et à des entreprises.La plupart des FAI offrent d'autres services de connectivité Internet, comme l'hébergement de site Web.

finger Dans certains systèmes d'exploitation, commande qui demande des informations de compte d'utilisateur réseau.

fragment Paquet IP qui a été divisé en deux ou plusieurs parties (ou fragments).Lorsque la taille d'un paquet IP dépasse la taille de trame maximale d'un réseau qu'il traverse, le paquet doit être divisé en paquets (fragments) plus petits.

furtif Donner l'impression de ne pas exister en ne répondant pas aux demandes d'informations.

HTML (Hypertext Markup Language) Langage standard des documents sur le World Wide Web. Les codes insérés dans un fichier texte indiquent au navigateur Web comment afficher le texte et les images d'une page Web sur l'écran de l'utilisateur et définissent des liens hypertexte entre les documents.

IP (Internet Protocol) Protocole dominant utilisé pour transmettre des données d'un ordinateur à un autre sur Internet. IP achemine les paquets vers les destinations appropriées.

JavaScript Langage de script similaire à Java, mais offrant moins de capacités. Le code JavaScript peut être inclus dans des pages Web pour ajouter une interactivité et d'autres fonctionnalités.

journal Enregistrement des actions et des événements qui se produisent sur un ordinateur de bureau ou un ordinateur de poche.

local Terme qui fait référence à votre ordinateur, par opposition à un ordinateur distant.

menace Circonstance, événement ou personne pouvant potentiellement porter atteinte à un système par destruction, divulgation, modification de données et/ou refus de service.

modem Dispositif de modulation (conversion en données analogiques) et démodulation (conversion de données analogiques) de données numériques en vue de leur transmission sur une ligne téléphonique.Inclut également les périphériques d'interface destinés aux connexions numériques sur Internet, comme les périphériques RNIS, câble et DSL.

mot de passe Séquence de caractères saisie par les utilisateurs pour de s'identifier auprès d'un réseau ou d'un programme. Les mots de passe les plus sûrs sont difficiles à deviner ou à trouver dans un dictionnaire et qui sont constitués d'une combinaison de lettres majuscules et minuscules, de chiffres et de symboles.

NAT (Network Address Translation) Méthode de conversion des adresses IP utilisées sur un intranet ou un réseau local en adresses Internet IP.Cette méthode permet de partager une adresse IP Internet entre plusieurs ordinateurs. De plus, elle permet de masquer les adresses IP des ordinateurs du réseau vis-à-vis de l'extérieur.

navigateur Application qui facilite la navigation sur Internet en fournissant une interface utilisateur graphique. L'utilisateur dispose de menus, d'icônes et de boutons qui lui évitent d'assimiler des commandes complexes. Egalement appelé client Web.

numéro de port Canal de communication logique utilisé par une application TCP/IP spécifique. Des numéros de port uniques sont associés à chaque application. Par convention, certains protocoles utilisent un numéro de port connu (par exemple, le protocole HTTP utilise le port 80), mais ces numéros restent configurables.

page Web Document unique sur le World Wide Web (WWW) identifié par une URL unique. Une page Web peut contenir du texte, des liens hypertexte et des graphiques.

paquet Unité de données acheminée entre une source et une destination sur Internet. Outre les données transmises, un paquet contient des informations qui permettent aux ordinateurs d'un réseau de déterminer s'ils doivent le recevoir.

pare-feu Système de sécurité qui utilise des règles pour bloquer ou autoriser des connexions et des transmissions de données entre votre ordinateur et Internet.

pirate Personne qui tente d'accéder à des ordinateurs sans autorisation dans le but de détourner les informations de ces ordinateurs ou de les endommager.

pop3 (Post Office Protocol 3) Protocole de courrier électronique servant à récupérer du courrier depuis un serveur distant sur une connexion Internet.

port Identification d'utilisateur de transport utilisée par un programme client pour spécifier un programme serveur particulier sur un ordinateur. Egalement appelé service.

Certaines applications ont des ports aux numéros préaffectés. D'autres ont des numéros de port affectés dynamiquement lors de chaque connexion. Lorsqu'un service (programme serveur) démarre, il se rattache au numéro de port qui lui a été associé. Lorsqu'un programme client veut utiliser ce serveur, il doit également demander à se rattacher à ce numéro de port.

proxy Mécanisme qui permet à un système d'agir au nom d'un autre système pour répondre aux demandes des protocoles. Les programmes de sécurité des pare-feu utilisent des services proxy pour protéger le réseau sécurisé des utilisateurs d'Internet.

règle de filtrage Ensemble de paramètres qui définit un type de paquet de données ou de communication réseau et indique la marche à suivre (autorisation ou blocage) vis-à-vis de cet élément.

réseau Ensemble d'ordinateurs et de périphériques associés reliés ensemble pour partager des informations et du matériel entre des utilisateurs.

réseau de commutation par paquets Réseau d'ordinateurs (comme Internet) qui transmet des fichiers en les scindant en paquets et en acheminant chaque paquet par l'itinéraire disponible le plus avantageux entre la source et la destination.

routeur Périphérique d'un réseau qui relie les ordinateurs ou les réseaux interconnectés. Un routeur reçoit des paquets et les transmet à leur destination selon l'itinéraire le plus avantageux.

serveur Ordinateur de contrôle d'un réseau local, qui contrôle l'accès des logiciels aux postes de travail, imprimantes et autres composants du réseau.

serveur DNS (serveur Domain Naming System) Ordinateur qui stocke une base de données de noms de domaine avec les adresses IP correspondantes.Lorsqu'un ordinateur envoie un nom de domaine à un serveur DNS, ce dernier lui renvoie l'adresse IP correspondant au domaine.

service Protocoles permettant à un ordinateur d'accéder à un type de données stockées sur un autre ordinateur. De nombreux ordinateurs hôtes connectés à Internet offrent des services. Ainsi, les serveurs HTTP utilisent Hypertext Transfer Protocol pour fournir un service World Wide Web et les serveurs FTP offrent des services File Transfer Protocol. *Voir aussi* port.

site Web Groupe de pages Web gérées par une même société, organisation ou personne.Un site Web peut inclure du texte, des images, des fichiers audio et vidéo et des liens hypertexte vers d'autres pages Web.

socket Identificateur d'un service spécifique, sur un ordinateur spécifique. Un socket est constitué de l'adresse IP de l'ordinateur suivie du signe deux points et du numéro de port.

sous-réseau Réseau local appartenant à un intranet plus important ou à Internet.

système d'exploitation	Programme qui relie les fonctionnalités des matériels et logiciels informatiques à des périphériques d'entrée/sortie tels que des disques, des claviers et des souris.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Gamme standard de protocoles utilisée pour communiquer avec les périphériques Internet.
télécharger	Transférer des données entre deux ordinateurs, généralement sur un modem ou un réseau. Se réfère en général à l'action de transférer un fichier depuis Internet, un système BBS ou un service en ligne vers son ordinateur.
tentative de connexion	Demande par le transfert de données de l'établissement d'une connexion.
URL (Uniform Resource Locator)	Adresse globale des documents et d'autres ressources sur le World Wide Web, et convention que les navigateurs Web utilisent pour localiser les fichiers et d'autres services distants.
World Wide Web (WWW)	Ensemble de documents hypertexte stockés sur des serveurs Web dans le monde entier. Egalement appelé WWW ou simplement Web. Le Web permet un accès universel à une vaste collection de documents stockés au format HTML sous forme de pages Web.

Index

B

C

D

E

F

G

I

J

L

M

N

O

P

R

S

T

U

V

W

Z

Solutions de service et de support EMEA

Service Clientèle - vous aide pour les questions non techniques telles que les commandes, les mises à jour, les échanges et les remises.

Support technique - vous aide pour les questions techniques telles que l'installation, la configuration ou le dépannage des produits Symantec.

Les systèmes de support technique et de service clientèle varient en fonction des pays. Pour vous renseigner sur les offres de service dans votre région, visitez le site Web approprié.

Si ce produit vous a été fourni lors de l'achat de votre ordinateur, le fabricant du système prend la responsabilité du support, sauf indication contraire.

Service Clientèle

Le site de support Web vous indique comment :

- localiser des revendeurs et des consultants dans votre région ;
- remplacer des CD défectueux et des manuels ;
- mettre à jour l'enregistrement de votre produit ;
- vous informer sur les commandes, les retours et les remises ;
- accéder à la Foire aux questions (FAQ) du service Clientèle ;
- adresser une question à un agent du Service Clientèle ;
- obtenir des informations une documentation produit ou un logiciel d'essai.

Pour les commandes de mises à jour produit, consultez les informations correspondant à votre région.

Royaume-Uni, Irlande :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/eedocid/199991585523

Allemagne, Autriche et Suisse :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/gdocid/20000531114300925

France, Belgique, Luxembourg :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/fdocid/20000530164002925

Pays-Bas, Belgique :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/ddocid/20000531114633925

Italie :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/idocid/20001114142714925

Espagne :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/sdocid/20000531113344925

Suède, Norvège, Danemark, Finlande :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/swdocid/20000531113940925

Autres pays :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/eedocid/199991585523

Support technique

Symantec propose deux options de support technique pour vous aider à installer, configurer ou dépanner des produits Symantec.

Service et support en ligne

Connectez-vous au site Web de service et de support Symantec pour votre région. Spécifiez un type d'utilisateur puis sélectionnez votre produit et sa version pour :

- accéder aux rubriques d'actualité ;
- consulter la base de connaissances ;
- suivre des didacticiels en ligne ;
- vous informer sur les options de contact ;
- adresser une question à un agent du support technique en ligne.

Support téléphonique

Des services de support payants par téléphone sont accessibles à tous les utilisateurs enregistrés. Visitez le site de support de votre pays pour obtenir des informations de contact.

Prise en charge des anciennes versions et des versions abandonnées

Lorsque Symantec annonce qu'un produit n'est plus commercialisé, le support téléphonique est assuré pendant 60 jours suivant cette annonce. Certaines informations techniques restent cependant disponibles sur le site de support Symantec.

Politique d'abonnement

Si votre produit Symantec inclut une protection antivirus, un pare-feu (firewall) ou une protection de contenu de site, vous pouvez avoir droit à des mises à jour via LiveUpdate. La durée de l'abonnement dépend de votre produit Symantec.

Quand l’abonnement initial expire, vous devez le renouveler pour continuer à actualiser votre protection. Ces mises à jour limitent votre vulnérabilité aux attaques.

Lorsque vous exécutez LiveUpdate vers la fin de votre abonnement, un message vous rappelle de vous réabonner pour un coût réduit. Suivez simplement les instructions affichées à l'écran.

Pour d'autres informations, visitez le site Web de service et de support Symantec pour votre région.

Bureaux service et support

Europe, Moyen Orient et Afrique

Service Clientèle de Symantec
Postbus 1029
3600 BA Maarssen
Pays-Bas
http://www.symantec.com/region/reg_eu/

Sites Web de service et de support

Europe/Anglais :
http://www.symantec.com/eusupport

Allemagne, Autriche et Suisse :
http://www.symantec.de/desupport/

France :
http://www.symantec.fr/frsupport/

Pays-Bas :
http://www.symantec.nl/nlsupport/

Italie :
http://www.symantec.it/itsupport/

Espagne :
http://www.symantec.com/region/mx/techsupp/index.html

Suède :
http://www.symantec.com/region/se/techsupp/index.html

Norvège :
http://www.symantec.com/region/no/techsupp/index.html

Danemark :
http://www.symantec.com/region/dk/techsupp/index.html

Finlande :
http://www.symantec.com/region/fi/techsupp/index.html

Pologne :
http://www.symantec.com/region/pl/techsupp/index.html

République tchèque :
http://www.symantec.com/region/cz/techsupp/index.html

République slovaque :
http://www.symantec.com/region/cz/techsupp/index.html

Russie :
http://www.symantec.com/region/ru/techsupp/index.html

Hongrie :
http://www.symantec.com/region/hu/techsupp/index.html

Pour les solutions de service et de support dans d'autres pays, visitez le site suivant et sélectionnez votre région.

http://www.symantec.com/globalsites.html

Tous les efforts ont été fournis pour garantir la précision de ces informations. Celles-ci peuvent toutefois faire l'objet de modifications sans préavis. Symantec Corporation se réserve le droit d'apporter de telles modifications sans avertissement préalable.