

Norton Personal Firewall™ - Guide de l'utilisateur

Norton™

2002
Personal Firewall



07-30-00467-FR

Guide de l'utilisateur

Norton Personal Firewall™ 2002

Le logiciel décrit dans ce manuel est fourni aux termes d'un accord de licence et ne peut être utilisé que conformément à ces termes.

Documentation version 4.0

PN: 07-30-00467-FR

Copyright

Copyright © 2001 Symantec Corporation

Tous droits réservés.

Toute documentation technique fournie par Symantec Corporation est soumise à copyright et reste la propriété de Symantec Corporation.

LIMITATION DE GARANTIE. La documentation technique vous est fournie TELLE QUELLE et Symantec Corporation n'offre aucune garantie quant à son exactitude ou son utilisation. Toute utilisation de la documentation technique et des informations qu'elle contient se fait sous la responsabilité de l'utilisateur. La documentation peut inclure des erreurs techniques ou typographiques, ou autres imprécisions. Symantec se réserve le droit d'apporter des modifications sans préavis.

Aucune partie de cette documentation ne peut être copiée sans l'accord écrit préalable de Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, Etats-Unis.

Bibliothèque de modèles standard

Ce produit utilise la Bibliothèque de modèles standard, bibliothèque C++ de classes de conteneurs, algorithmes et itérations.

Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc.

L'autorisation d'utiliser, de copier, de modifier, de distribuer et de vendre ce logiciel et sa documentation pour quelque fin que ce soit est par la présente accordée gratuitement sous réserve que le copyright ci-dessus apparaisse sur tous les exemplaires et que ce copyright et cette autorisation figurent dans la documentation. Silicon Graphics ne donne aucune garantie quant à l'adaptabilité du présent logiciel à quelque fin que ce soit. Le logiciel est fourni « tel quel » sans garantie expresse ni implicite.

Copyright © 1994. Hewlett-Packard Company

L'autorisation d'utiliser, de copier, de modifier, de distribuer et de vendre ce logiciel et sa documentation pour quelque fin que ce soit est par la présente accordée gratuitement sous réserve que le copyright ci-dessus apparaisse sur tous les exemplaires et que ce copyright et cette autorisation figurent dans la documentation. Hewlett-Packard Company ne donne aucune garantie quant à l'adaptabilité du présent logiciel à quelque fin que ce soit. Le logiciel est fourni « tel quel » sans garantie expresse ni implicite.

Marques

Symantec, le logo Symantec, Norton, Norton Internet Security, Norton Personal Firewall, Norton SystemWorks, Emergency Disk, LiveUpdate, Norton AntiVirus, Norton Utilities et Rescue Disk sont des marques commerciales de Symantec Corporation.

Windows est une marque déposée de Microsoft Corporation. AOL et CompuServe sont des marques déposées de America Online, Inc. Prodigy Internet est une appellation commerciale de Prodigy. Pentium est une marque déposée d'Intel Corporation.

Tous les autres noms de produit cités peuvent être des marques commerciales ou déposées de leurs détenteurs respectifs et sont reconnus comme tels.

Imprimé en Irlande.

10 9 8 7 6 5 4 3 2 1

Comment réduire au minimum les risques d'Internet

Installation de Norton Personal Firewall.

Pour plus d'informations, consultez la section « [Installation de Norton Personal Firewall](#) » à la page 15.

Exécuter LiveUpdate toutes les semaines pour maintenir la protection à jour

Pour plus d'informations, consultez la section « [Mise en route de Norton Personal Firewall](#) » à la page 27.

Identifier les informations confidentielles à sauvegarder

Pour plus d'informations, consultez la section « [Protection des informations confidentielles](#) » à la page 41.

Répondre correctement aux alertes de Norton Personal Firewall

Pour plus d'informations, consultez la section « [Répondre aux alertes de Norton Personal Firewall](#) » à la page 47.

Personnaliser la protection par firewall

Pour plus d'informations, consultez la section « [Personnalisation de la protection par firewall](#) » à la page 59.

Maintenir la protection de Norton Personal Firewall activée

Pour plus d'informations, consultez la section « [Personnalisation de la protection par firewall](#) » à la page 59.

T A B L E D E S M A T I È R E S

Comment réduire au minimum les risques d'Internet

Chapitre 1 Présentation de Norton Personal Firewall

Interdiction des accès non autorisés	11
Protection des informations personnelles	13
Assistance en ligne	13
Conseils d'utilisation sécurisée d'un ordinateur	14

Chapitre 2 Installation de Norton Personal Firewall

Configuration requise	15
Windows 98 et Me	15
Windows NT 4.0 Workstation	16
Windows 2000 Professional Workstation	16
Windows XP Professional ou Windows XP Home Edition	16
Avant l'installation	16
Installation	17
Si l'écran d'accueil ne s'affiche pas	20
Enregistrement du logiciel	21
Après l'installation	22
Redémarrage de l'ordinateur	22
Utilisation de l'Assistant Informations	22
Utilisation de l'Assistant Sécurité	23
Si Norton SystemWorks est installé	24
Si vous devez désinstaller Norton Personal Firewall	24

Chapitre 3 Mise en route de Norton Personal Firewall

Lancement de Norton Personal Firewall	27
Désactivation temporaire de Norton Personal Firewall	28
Désactivation d'une fonction de protection	29
Actualisation avec LiveUpdate	29
A propos des mises à jour de programme	29
A propos des mises à jour de protection	30
Informations sur l'abonnement	30
Mises à jour du programme et de la protection	30
Comment trouver de l'aide dans Norton Personal Firewall	31
Aide en ligne complète	31
Aide sur les fenêtres et les boîtes de dialogue	31
Aide Qu'est-ce que c'est ? sur les boutons et les autres contrôles	31
Fichier Lisezmoi et notes de version	32

Utilisation de l'Assistant Sécurité	33
Firewall personnel	33
Confidentialité	34
Contrôle des applications	36
Contrôle de zone Internet	37
Etat Internet	38
Alert Tracker	38
LiveUpdate	38
Vérification de l'état de la sécurité	39

Chapitre 4 Protection des informations confidentielles

Définition du niveau de confidentialité	42
Définition des informations confidentielles à bloquer	42
Paramétrage des options de confidentialité	43
Modification du paramétrage de la fonction	
Informations confidentielles	44
Modification du paramétrage de la fonction	
Blocage des cookies	44
Activation de la confidentialité de navigation	45
Activation des connexions Web sécurisées	45
Blocage des connexions Web sécurisées	46

Chapitre 5 Répondre aux alertes de Norton Personal Firewall

Réponse aux alertes de sécurité	48
Réponse aux alertes de contrôle d'accès à Internet	50
Réponse aux alertes Java et ActiveX	52
Réponse aux alertes de cookie	53
Réponse aux alertes de confidentialité	54
Utilisation d'Alert Tracker	55
Ouverture d'Alert Tracker	55
Consultation des messages récents d'Alert Tracker	56
Déplacement d'Alert Tracker	56
Masquer Alert Tracker	56
Paramétrage du niveau de détail des informations	56
Définition du niveau de détail des informations	57

Chapitre 6 Personnalisation de la protection par firewall

Définition du niveau de sécurité	60
Définition de paramètres de sécurité personnalisés	61
Contrôle des applications qui accèdent à Internet	64
Analyse des applications pour déterminer	
celles utilisant Internet	65

Activation du contrôle automatique d'accès à Internet	65
Réponse aux alertes de contrôle d'accès à Internet	65
Ajout d'une application au contrôle d'accès à Internet	66
Modification des paramètres du contrôle d'accès à Internet	66
Modification des paramètres applicables à l'ensemble du système	67
Protection d'un réseau domestique avec le contrôle de zone Internet	67
Ajout d'ordinateurs aux zones	68
Ajout d'ordinateurs du réseau domestique à la zone Approuvés	68
Utilisation de la protection contre les intrusions pour arrêter les attaques	70
Détection des tentatives d'analyse des ports	70
Activation du blocage automatique	70
Déblocage d'un ordinateur bloqué	71
Exclusion d'activités spécifiques d'AutoBlock	71
Ajout d'un ordinateur bloqué à la zone Restreints	72
Identification d'ordinateurs dans Norton Personal Firewall	72
Définition d'ordinateurs individuels	73
Identification d'une série d'ordinateurs	73
Identification d'ordinateurs à l'aide d'une adresse réseau	74

Chapitre 7 Contrôle des événements de Norton Personal Firewall

Vérification de l'état courant	75
Vérification de l'état du firewall personnel	76
Vérification de l'état de la confidentialité	76

Chapitre 8 Configuration de Norton Personal Firewall pour des situations courantes

Utilisation de Norton Personal Firewall avec une connexion par modem	77
Utilisation de Norton Personal Firewall avec une connexion haut débit	77
Résolution des problèmes rencontrés avec les connexions haut débit	78
Utilisation de Norton Personal Firewall avec des jeux faisant intervenir plusieurs joueurs	79
Accord de l'accès à Internet à un jeu multi-joueurs	79
Placement d'autres joueurs dans la zone Approuvés	79

Utilisation de Norton Personal Firewall dans un réseau domestique	80
Activation du partage de fichiers et d'imprimantes	80
Partage de connexion Internet	81
Utilisation de Norton Personal Firewall avec un routeur câble/DSL	81
Utilisation de Norton Personal Firewall avec un réseau d'entreprise	82
Activation du partage de fichiers et d'imprimantes	82
Logiciels d'administration sur les réseaux d'entreprise	82
Utilisation de Norton Personal Firewall avec un serveur proxy	83
Déterminer si Norton Personal Firewall est compatible avec votre serveur proxy	83
Déterminer le port à surveiller pour les communications HTTP	83
Définition des ports à surveiller pour les communications HTTP	84
Exécution d'un serveur Web avec Norton Personal Firewall	84
Exécution d'un serveur FTP avec Norton Personal Firewall	85
Utilisation de Norton Personal Firewall avec DHCP	85
Utilisation de Norton Personal Firewall avec pcAnywhere	86
Utilisation de Norton Personal Firewall avec un réseau virtuel (VPN)	86

Chapitre 9 Dépannage

Résolution des problèmes de Norton Personal Firewall	87
Quel est le problème lié à ce site Web ?	87
Pourquoi ne puis-je pas publier des informations en ligne ?	89
Pourquoi Norton Personal Firewall ne m'envoie-t-il pas d'avertissement avant d'autoriser des applications à accéder à Internet ?	89
Pourquoi mon réseau local ne fonctionne-t-il plus ?	90
Pourquoi ne puis-je pas utiliser une imprimante partagée ?	90
Comment un site Web peut-il accéder aux informations sur mon navigateur ?	90

Annexe A A propos d'Internet

Transmission des informations sur Internet	92
TCP/IP	93
UDP	94
ICMP	94
IGMP	94
Les informations du Web sont stockées sur Internet	95
Demande d'une page	95
Parties d'un URL	96
Ports identifiant des applications sur un serveur	97
Identification des ordinateurs sur Internet	99

Annexe B Risques et menaces liés à Internet

Risques liés aux pirates	101
Déroulement d'une attaque de pirate	102
Risques liés à des contenus actifs	105
Risques liés à la confidentialité	105
Envoi d'informations confidentielles	106
Bons et mauvais cookies	106
Suivi de l'utilisation d'Internet	107
Risques liés aux chevaux de Troie et aux virus	108
Probabilité de subir une attaque	109

Glossaire

Index

Solutions de service et de support de Symantec

Présentation de Norton Personal Firewall

Des millions d'ordinateurs se connectent à Internet et leur nombre ne cesse d'augmenter. Lorsque vous accédez à Internet, vous avez la possibilité de vous connecter à tous ces ordinateurs qui peuvent, à leur tour se connecter au vôtre. Des connexions non protégées à Internet peuvent exposer votre ordinateur aux attaques de pirates et à d'autres menaces.

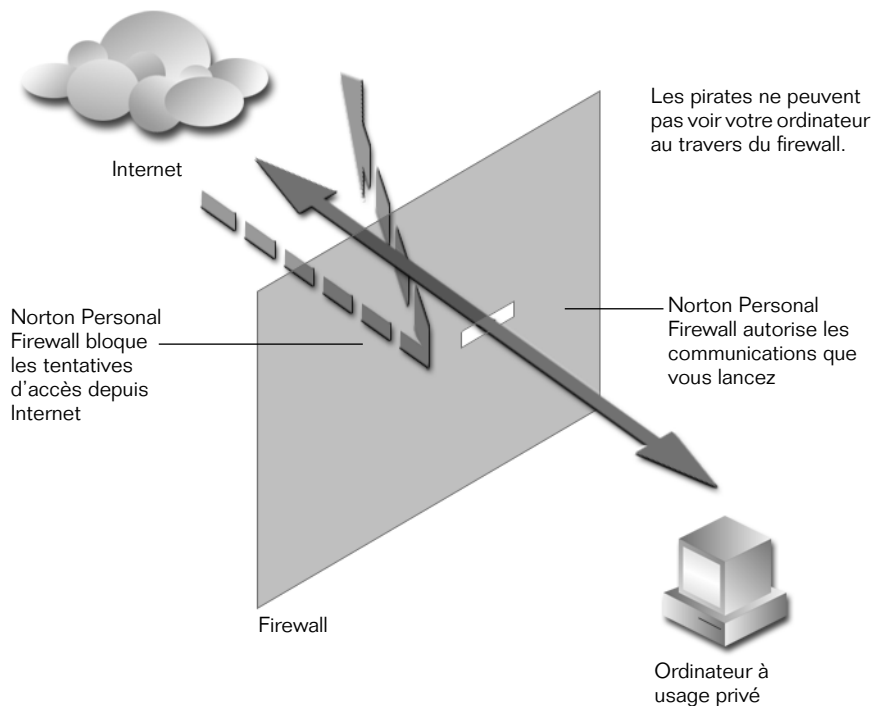
Norton Personal Firewall comporte plusieurs composants qui collaborent pour vous protéger des dangers d'Internet et rendre la navigation plus agréable :

- blocage des accès non autorisés à votre ordinateur quand vous êtes sur Internet ;
- protection des informations personnelles.

Interdiction des accès non autorisés

Norton Personal Firewall constitue une barrière de protection entre votre ordinateur et Internet. Les *firewalls* interdisent les échanges non autorisés avec un ordinateur ou un réseau. Ils interdisent également aux utilisateurs d'Internet non autorisés d'accéder aux ordinateurs et aux réseaux privés connectés à Internet.

Norton Personal Firewall utilise des règles pour déterminer si les connexions doivent être autorisées ou bloquées. Vous pouvez modifier ces règles et autoriser ou bloquer l'accès des applications à Internet.



Norton Personal Firewall sélectionne automatiquement la meilleure méthode pour protéger de nombreuses applications. Quand une application inconnue de Norton Personal Firewall tente de communiquer sur Internet, un message vous prévient et vous aide à décider si l'application est habilitée à accéder à Internet.

Les contrôles ActiveX et les *applets Java* sont des applications exécutées dans le navigateur. La plupart d'entre elles sont utiles, mais certaines sont dangereuses. Norton Personal Firewall peut empêcher l'exécution des contrôles ActiveX et des applets Java à votre insu et vous permet de sélectionner les sites sur lesquels ces applications peuvent être exécutées.

Protection des informations personnelles

Vous préférez sans doute que les informations confidentielles, comme vos numéros de carte de crédit ou votre numéro de téléphone personnel, ne soient pas envoyées non codées sur Internet. Norton Privacy Control interdit l'envoi d'informations confidentielles à des sites Web non sécurisés ou par l'intermédiaire de programmes de messagerie instantanée.

Les *cookies* sont de petits fichiers enregistrés sur l'ordinateur et utilisés par les sites Web pour suivre vos visites. Norton Personal Firewall peut bloquer les cookies et intercepter les autres données que le navigateur fournit normalement aux sites, comme l'adresse du dernier site Web visité et votre type de navigateur.

Assistance en ligne

Norton Personal Firewall comporte une assistance en ligne complète.

- L'Assistant Sécurité vous présente Norton Personal Firewall et vous aide à sélectionner le paramétrage approprié pour optimiser votre protection. Après avoir installé Norton Personal Firewall et redémarré l'ordinateur, l'assistant Sécurité apparaît. Cet assistant peut à tout moment fournir des informations sur le fonctionnement de Norton Personal Firewall et modifier les paramètres sélectionnés.
- L'aide en ligne est une source d'informations précieuse sur Norton Personal Firewall. Elle est composée d'un sommaire, d'un index détaillé et d'un système de recherche en texte intégral, qui facilite l'accès aux informations.
- Dans la plupart des fenêtres et des boîtes de dialogue, les options Plus d'infos ou Aide offrent des informations contextuelles sur Norton Personal Firewall.
- L'aide « Qu'est-ce que c'est ? » fournit une brève explication sur un composant d'une fenêtre ou d'une boîte de dialogue.

Conseils d'utilisation sécurisée d'un ordinateur

Norton Personal Firewall réunit de nombreux outils permettant de limiter les risques encourus sur Internet. Vous pouvez également prendre les précautions suivantes :

- Maintenez votre navigateur à jour. Les éditeurs de logiciels diffusent régulièrement des versions actualisées dans lesquelles les failles de la version précédente ont été corrigées.
- 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 à 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 annexe de courrier électronique que si vous attendiez la pièce jointe et si vous faites confiance à son expéditeur.
- Veillez à ne pas fournir d'informations personnelles quand cela n'est pas justifié. 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.

Pour plus d'informations, consultez la section « [Risques et menaces liés à Internet](#) » à la page 101.

Installation de Norton Personal Firewall

Avant d'installer Norton Personal Firewall, prenez le temps d'examiner les spécifications système indiquées dans ce chapitre.

Configuration requise

Pour utiliser Norton Personal Firewall, l'ordinateur doit fonctionner sous l'un des systèmes d'exploitation Windows suivants :

- Windows 98, 98SE
- Windows Me
- Système d'exploitation Windows NT v4.0 Workstation avec Service Pack 6 ou supérieur
- Windows 2000 Professional Workstation
- Windows XP Professional ou Windows XP Home Edition

L'ordinateur doit également posséder la configuration requise minimale suivante :

Windows 98 et Me

- Processeur Intel Pentium à 150 MHz
- 32 Mo de RAM
- 20 Mo d'espace disque
- Internet Explorer 4.01 avec Service Pack 1 ou version ultérieure
- Lecteur de CD-ROM ou de DVD-ROM
- Support Internet de Microsoft Windows

Windows NT 4.0 Workstation

- Service Pack 6a ou ultérieur
- Processeur Intel Pentium à 150 MHz
- 48 Mo de RAM
- 20 Mo d'espace disque
- Internet Explorer 4.01 avec Service Pack 1 ou version ultérieure
- Lecteur de CD-ROM ou de DVD-ROM
- Support Internet de Microsoft Windows

Windows 2000 Professional Workstation

- Processeur Intel Pentium à 150 MHz
- 48 Mo de RAM
- 20 Mo d'espace disque
- Internet Explorer 4.01 avec Service Pack 1 ou version ultérieure
- Lecteur de CD-ROM ou de DVD-ROM
- Support Internet de Microsoft Windows

Windows XP Professional ou Windows XP Home Edition

- Processeur Intel Pentium à 300 MHz ou supérieur
- 64 Mo de RAM
- 20 Mo d'espace disque
- Internet Explorer 4.01 avec Service Pack 1 ou version ultérieure
- Lecteur de CD-ROM ou de DVD-ROM
- Support Internet de Microsoft Windows

Avant l'installation

Si des versions antérieures de Norton Personal Firewall ou des programmes antivirus sont présents sur l'ordinateur, désinstallez-les avant d'installer cette version de Norton Personal Firewall. Pour plus d'informations, consultez la section « [Si vous devez désinstaller Norton Personal Firewall](#) » à la page 24.

Pour désinstaller d'autres programmes de firewall, consultez la documentation fournie avec le programme.

Vous devez également quitter tous les autres programmes Windows avant d'installer Norton Personal Firewall.

Si vous utilisez Windows XP, désactivez le firewall XP.

Installation

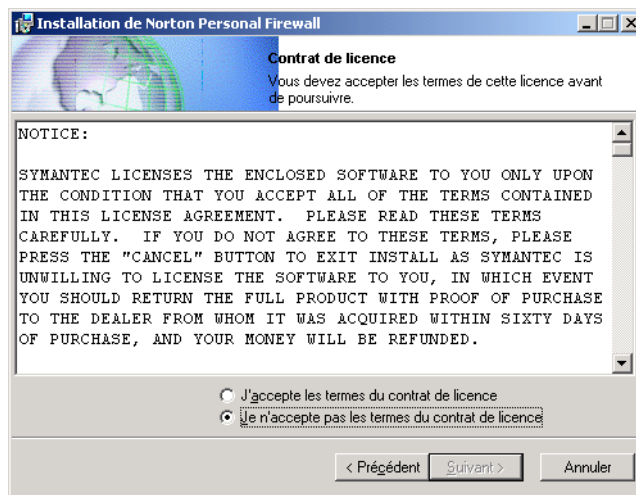
Installez Norton Personal Firewall depuis le CD Norton Personal Firewall.

Pour installer Norton Personal Firewall

- 1 Insérez le CD Norton Personal Firewall dans le lecteur de CD-ROM.
- 2 Dans la fenêtre du CD Norton Personal Firewall, cliquez sur **Installer Norton Personal Firewall**.

Si l'ordinateur n'est pas configuré pour ouvrir automatiquement un CD, vous devez l'ouvrir vous-même. Pour plus d'informations, consultez la section « Si l'écran d'accueil ne s'affiche pas » à la page 20.

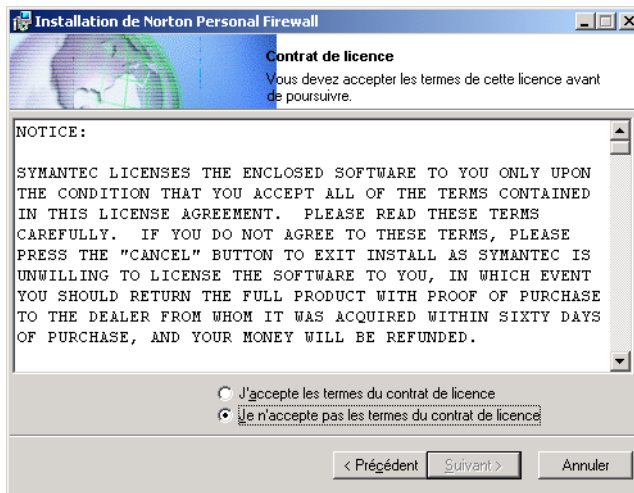
- 3 La première fenêtre d'installation vous rappelle de fermer tous les autres programmes Windows. Cliquez sur **Suivant**.



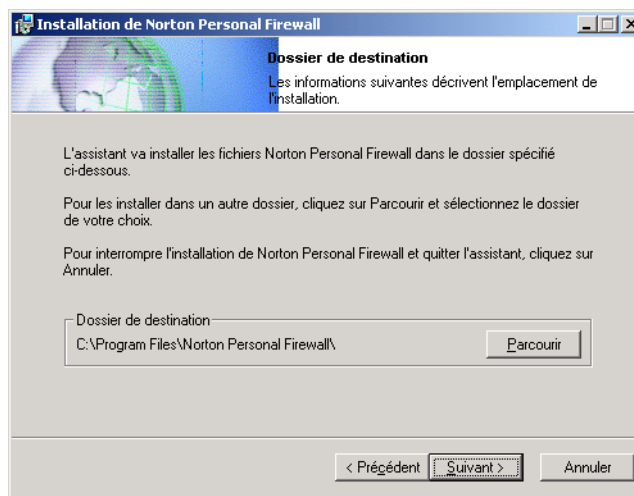
- 4 Dans la fenêtre Accord de licence, cliquez sur **J'accepte les termes de l'accord de licence**.

Si vous refusez, vous ne pouvez pas poursuivre l'installation.

- 5 Cliquez sur **Suivant**.

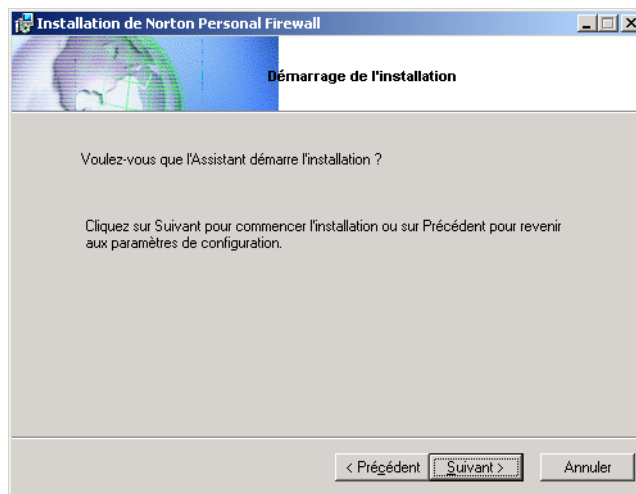


- 6 LiveUpdate actualise votre exemplaire de Norton Personal Firewall avec les dernières mises à jour de programme et de protection. Décidez si vous souhaitez ou non exécuter LiveUpdate à la fin de l'installation.
- 7 Cliquez sur **Suivant**.

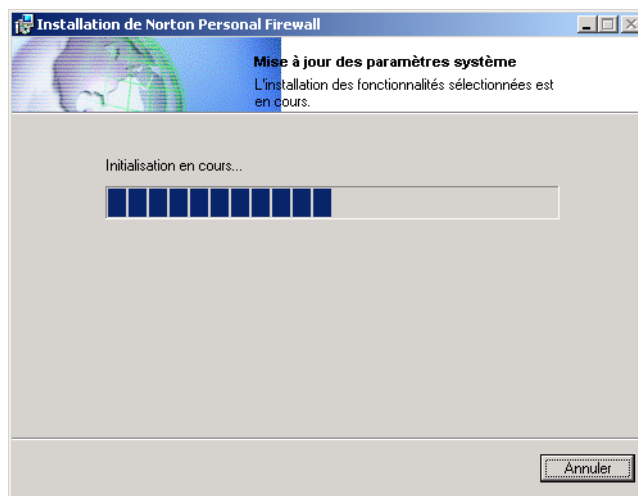


- 8 Cliquez sur **Parcourir** pour sélectionner le dossier dans lequel vous souhaitez installer Norton Personal Firewall, si ce n'est pas l'emplacement par défaut.

9 Cliquez sur **Suivant**.



10 Cliquez sur **Suivant** pour commencer l'installation de Norton Personal Firewall.



Après avoir installé Norton Personal Firewall, l'Assistant Enregistrement apparaît pour vous permettre d'enregistrer le logiciel. Pour plus d'informations, consultez la section « [Enregistrement du logiciel](#) » à la page 21.

Si vous avez choisi d'exécuter LiveUpdate après l'installation, il s'exécute après l'enregistrement.

- 11 Quand LiveUpdate est terminé, cliquez sur **Terminer**.
- 12 Parcourez le texte Lisezmoi, puis cliquez sur **Suivant**.



- 13 Cliquez sur **Terminer** pour quitter l'installation.

Si l'écran d'accueil ne s'affiche pas

Il arrive parfois que le lecteur de CD-ROM d'un ordinateur ne démarre pas automatiquement un 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 votre lecteur de CD-ROM.
- 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 n'effectuez pas l'enregistrement en ligne, vous pouvez le faire 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 Tapez votre nom et indiquez si vous souhaitez enregistrer Norton Personal Firewall en votre nom ou pour votre société, puis cliquez sur **Suivant**.
- 4 Tapez 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 le questionnaire en cliquant sur **Suivant**.
- 6 Choisissez si vous voulez enregistrer Norton Personal Firewall par Internet ou par courrier.
 - Pour vous enregistrer par courrier, vous devez connecter l'ordinateur à une imprimante l'Assistant Enregistrement utilisera pour imprimer le formulaire.
 - Pour vous enregistrer par Internet, connectez-vous à Internet.
- 7 Cliquez sur **Suivant**.

Si vous avez soumis le formulaire par Internet, l'Assistant Enregistrement affiche le numéro de série correspondant à votre produit.
- 8 Notez le numéro de série ou cliquez sur **Imprimer** afin d'avoir un exemplaire des informations d'enregistrement pour référence ultérieure.
- 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

Si vous devez redémarrer l'ordinateur après l'installation de Norton Personal Firewall, une invite vous propose de le faire immédiatement. Après le redémarrage ou, si l'ordinateur n'a pas besoin d'être redémarré, une fois l'installation terminée, l'Assistant Informations apparaît. Après avoir terminé cet assistant, l'Assistant Sécurité apparaît pour vous guider tout au long de la configuration de Norton Personal Firewall.

Remarque : si vous avez acheté l'ordinateur avec Norton Personal Firewall déjà installé, l'Assistant Informations apparaît au premier démarrage de l'ordinateur. Vous devez accepter l'accord de licence qui apparaît dans l'Assistant Informations pour pouvoir activer Norton Personal Firewall.

Redémarrage de l'ordinateur

Après l'installation, vous pouvez recevoir un message vous indiquant que l'ordinateur doit être redémarré pour que les mises à jour prennent effet.

Pour redémarrer l'ordinateur

- Dans la boîte de dialogue Informations du programme d'installation, cliquez sur **Oui**.
Si vous cliquez sur Non, la configuration de Norton Personal Firewall ne sera terminée qu'au redémarrage de l'ordinateur.

Utilisation de l'Assistant Informations

Cet assistant vous donne des informations sur le service d'abonnement de Symantec.

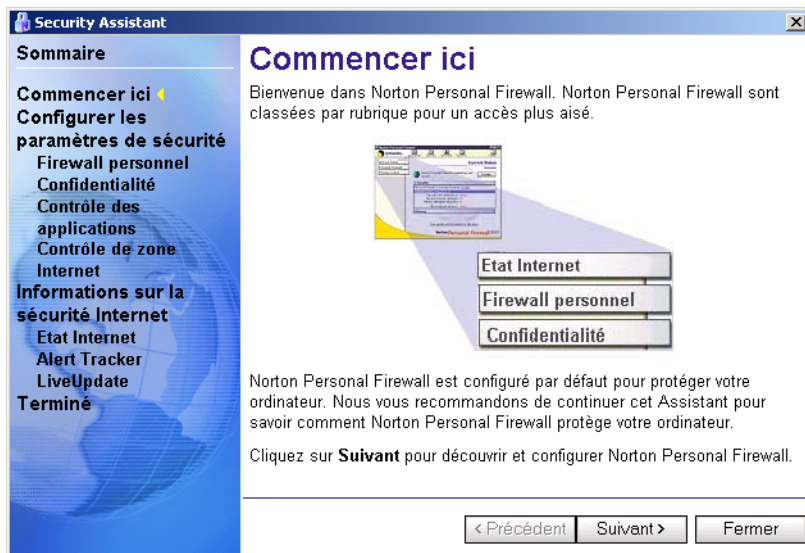
Pour utiliser l'Assistant Informations

- 1 Sur l'écran de bienvenue, cliquez sur **Suivant**.
Si vous avez acheté l'ordinateur avec Norton Personal Firewall déjà installé, vous devez accepter l'accord de licence pour pouvoir utiliser Norton Personal Firewall. Vous pouvez ensuite enregistrer votre logiciel.
- 2 Cliquez sur **J'accepte l'accord de licence**, puis cliquez sur **Suivant**.
L'Assistant Enregistrement apparaît pour vous permettre d'enregistrer le logiciel en ligne. Pour plus d'informations, consultez la section « [Enregistrement du logiciel](#) » à la page 21.
Après l'enregistrement, des informations sur votre abonnement sont affichées.

- 3 Examinez les informations du service d'abonnement, puis cliquez sur **Suivant**.
Si vous avez acheté l'ordinateur avec Norton Personal Firewall déjà installé, le fichier Lisezmoi apparaît.
- 4 Parcourez le fichier Lisezmoi, puis cliquez sur **Suivant**.
- 5 Sur le dernier écran de l'Assistant Informations, cliquez sur **Terminer**.

Utilisation de l'Assistant Sécurité

L'Assistant Sécurité démarre automatiquement après l'Assistant Enregistrement. Vous pouvez l'utiliser pour examiner et, le cas échéant, modifier la configuration de Norton Personal Firewall pour votre ordinateur.



Remarque : Il est recommandé d'utiliser les paramètres par défaut pour Norton Personal Firewall. Si vous pensez que des modifications doivent être apportées après avoir utilisé Norton Personal Firewall pendant un certain temps, vous pouvez vous servir de l'Assistant Sécurité pour effectuer ces modifications. Pour plus d'informations, consultez la section « Utilisation de l'Assistant Sécurité » à la page 33.

Pour utiliser l'Assistant Sécurité

- Au bas de chaque écran, cliquez sur **Suivant** pour faire défiler l'Assistant Sécurité et examiner tous les paramètres.
- Dans l'itinéraire situé dans la partie gauche de la fenêtre Assistant de Sécurité, cliquez sur le nom d'une fonction pour en examiner les paramètres.
- Cliquez sur **Fermer** pour fermer l'Assistant Sécurité.

Si Norton SystemWorks est installé

Si Norton SystemWorks est installé sur votre ordinateur quand vous installez Norton Personal Firewall, un message vous demande, après l'Assistant Informations, si vous souhaitez intégrer Norton Personal Firewall à Norton SystemWorks. Si vous cliquez sur Oui, il se produit ce qui suit :

- Un onglet Norton Personal Firewall apparaît dans la fenêtre principale de Norton SystemWorks. Toutes les fonctionnalités de Norton Personal Firewall apparaissent quand vous cliquez sur l'onglet.
- Norton Personal Firewall apparaît sous forme d'outil dans Norton Tray Manager.
- Si vous tentez d'ouvrir Norton Personal Firewall, Norton SystemWorks s'ouvre à la place.

Si vous devez désinstaller Norton Personal Firewall

Si vous avez besoin de supprimer Norton Personal Firewall de votre ordinateur, utilisez l'option Ajout/Suppression de programmes du Panneau de configuration Windows.

Remarque : au cours de la désinstallation, Windows peut indiquer qu'il installe le logiciel. Il s'agit d'un message général du programme d'installation Microsoft que vous pouvez ignorer.

Pour désinstaller Norton Personal Firewall

- 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 **Norton Personal Firewall**.
- 4 Effectuez l'une des opérations suivantes :
 - Dans Windows 2000 ou Windows Me, cliquez sur **Modifier/Supprimer**.
 - Dans Windows 98 ou Windows NT, cliquez sur **Ajouter/Supprimer**.
 - Dans Windows XP, cliquez sur **Supprimer**.
- 5 Cliquez sur **Oui** pour confirmer la désinstallation du produit.

Si vous n'avez pas d'autres produits Symantec sur l'ordinateur, désinstallez également LiveReg et LiveUpdate. Répétez les étapes 1 à 5 deux fois, d'abord en sélectionnant LiveReg à l'étape 3 pour désinstaller LiveReg, puis en sélectionnant LiveUpdate à l'étape 3 pour désinstaller LiveUpdate.

Mise en route de Norton Personal Firewall

Norton Personal Firewall est lancé automatiquement au démarrage de l'ordinateur. Vous n'avez pas besoin d'ouvrir cette application pour être protégé.

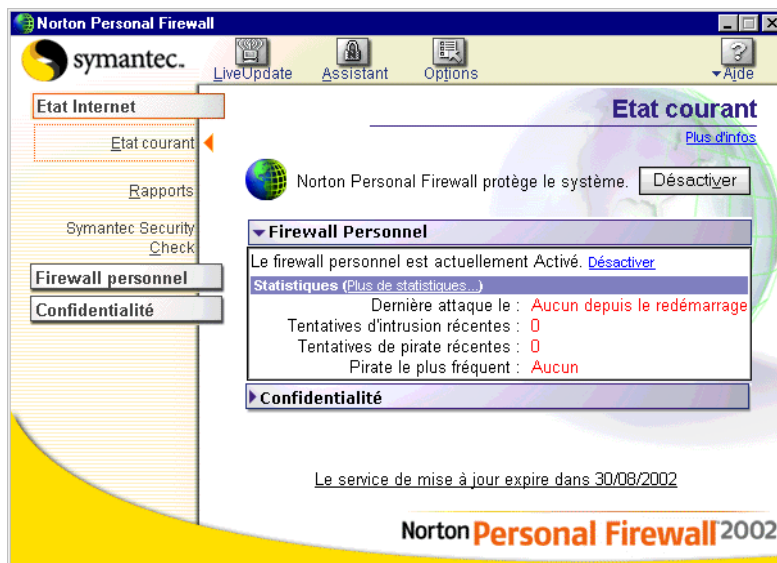
Lancement de Norton Personal Firewall

Ouvrez Norton Personal Firewall si vous souhaitez modifier les paramètres de protection ou surveiller les activités du programme.

Pour démarrer Norton Personal Firewall

- Effectuez l'une des opérations suivantes :
 - Dans la zone de notification de la barre des tâches de Windows, cliquez deux fois sur **Norton Personal Firewall**.
 - 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**.

La fenêtre principale de Norton Personal Firewall apparaît.



Désactivation temporaire de Norton Personal Firewall

Dans certains cas, il peut se révéler nécessaire de suspendre temporairement l'exécution d'une fonction de protection ou du programme tout entier. Par exemple, vous pouvez vérifier si Norton Personal Firewall interdit l'affichage correct d'une page Web. Norton Personal Firewall permet de désactiver des fonctions sans modifier le paramétrage.

Pour désactiver temporairement Norton Personal Firewall

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Etat Internet > Etat courant**.
- 2 Dans la fenêtre Etat courant, cliquez sur **Désactiver**.

Vous pouvez également désactiver Norton Personal Firewall en cliquant avec le bouton droit sur l'icône Norton Personal Firewall dans la zone notification de la barre des tâches de Windows et en choisissant Désactiver.

Norton Personal Firewall est réactivé quand vous choisissez Activer ou lors du démarrage suivant de l'ordinateur.

Désactivation d'une fonction de protection

Vous pouvez désactiver une fonction de protection. Par exemple, vous pouvez vérifier si le firewall personnel entrave le bon fonctionnement d'une application.

Pour désactiver une fonction de protection

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Etat Internet > Etat courant**.
- 2 Dans la fenêtre Etat courant, cliquez sur la fonction à désactiver pour faire apparaître sa fenêtre d'état.
- 3 Dans la fenêtre d'état de la fonction, cliquez sur **Désactiver**.

La fonction est réactivée quand vous choisissez Activer ou lors du démarrage suivant de l'ordinateur.

Actualisation avec LiveUpdate

Les produits Symantec ont besoin des dernières informations disponibles pour protéger l'ordinateur contre les nouvelles menaces. Symantec met ces informations à votre disposition par l'intermédiaire de LiveUpdate. LiveUpdate accède à Internet pour actualiser votre protection Internet et antivirus.

Les frais de connexion Internet habituels sont à votre charge quand vous utilisez LiveUpdate.

A propos des mises à jour de programme

Les mises à jour de programme sont des améliorations mineures des produits installés. Elles diffèrent des mises à niveau, qui sont de nouvelles versions de produits complets. Les mises à jour de programme qui comportent un installateur pour remplacer des fragments de logiciel existant sont également appelées correctifs. Les correctifs sont généralement destinés à étendre les possibilités du système d'exploitation ou la compatibilité du matériel, résoudre un problème de performance ou résoudre une bogue.

LiveUpdate automatise la procédure de téléchargement et d'installation des mises à jour du programme. Il vous évite de localiser et télécharger les fichiers sur un site Internet, de les installer et de supprimer les fichiers superflus du disque.

A propos des mises à jour de protection

Le service de protection contre les intrusions fournit un accès aux règles de firewall prédéfinies les plus récentes et aux listes d'applications accédant à Internet. Ces listes sont utilisées pour identifier les accès non autorisés à votre ordinateur. Norton Personal Firewall utilise les mises à jour disponibles auprès du service de protection contre les intrusions pour détecter les menaces les plus récentes présentes sur Internet.

Informations sur l'abonnement

Votre produit Symantec inclut un abonnement gratuit, limité dans le temps, pour les mises à jour de protection portant sur les services utilisés par votre produit. Lorsque cet abonnement est sur le point d'expirer, un message vous rappelle de le renouveler. Pour plus d'informations, consultez la section « Solutions de service et de support de Symantec » à la page 133.

Si vous ne renouvelez pas l'abonnement, vous pouvez toujours utiliser LiveUpdate pour recevoir les mises à jour du programme. Par contre, vous ne pouvez plus récupérer les mises à jour de la protection et vous n'êtes pas protégé contre les nouvelles menaces

Mises à jour du programme et de la protection

Utilisez régulièrement LiveUpdate pour obtenir des mises à jour du programme et de la protection.

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

Pour obtenir des mises à jour avec LiveUpdate

- 1 Ouvrez votre produit Symantec.
- 2 En haut de la fenêtre, cliquez sur **LiveUpdate**.
Un message peut vous signaler que votre abonnement est arrivé à expiration. Suivez les instructions affichées pour le renouveler.
- 3 Cliquez sur **Suivant** pour rechercher 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**.

Comment trouver de l'aide dans Norton Personal Firewall

Il existe quatre types d'aide en ligne :

- Aide en ligne complète
- des instructions détaillées sur les fenêtres et les boîtes de dialogue ;
- aide « Qu'est-ce que c'est ? » sur les boutons et les autres contrôles
- fichier Lisezmoi et notes de version

Aide en ligne complète

L'aide en ligne contient les informations du présent manuel.

Pour afficher l'aide en ligne

- 1 En haut de la fenêtre Norton Personal Firewall, cliquez sur **Aide**.
- 2 Cliquez sur **Aide Norton Personal Firewall**.

Aide sur les fenêtres et les boîtes de dialogue

L'aide sur 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 consulter l'aide sur une fenêtre ou une boîte 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**.

Aide Qu'est-ce que c'est ? sur les boutons et les autres contrôles

L'aide « Qu'est-ce que c'est ? » propose la définition des composants d'une fenêtre ou d'une boîte de dialogue.

Pour afficher l'aide Qu'est-ce que c'est ?

- Cliquez avec le bouton droit à l'endroit où vous avez besoin d'aide dans une fenêtre ou une boîte de dialogue et choisissez **Qu'est-ce que c'est ?**

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 endroit que les fichiers de Norton Personal Firewall.

Pour lire 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 Fermez le programme de traitement de texte quand vous avez fini de lire le fichier.

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 Fermez le programme de traitement de texte quand vous avez fini de lire le fichier.

Utilisation de l'Assistant Sécurité

Cet assistant peut à tout moment fournir des informations sur le fonctionnement de Norton Personal Firewall et modifier les paramètres sélectionnés.

Pour utiliser l'Assistant Sécurité

- 1 En haut de la fenêtre Norton Personal Firewall, cliquez sur **Assistant**.
- 2 Au bas de chaque écran, cliquez sur **Suivant** pour faire défiler l'Assistant Sécurité.
- 3 Cliquez sur **Fermer** pour fermer l'Assistant Sécurité.

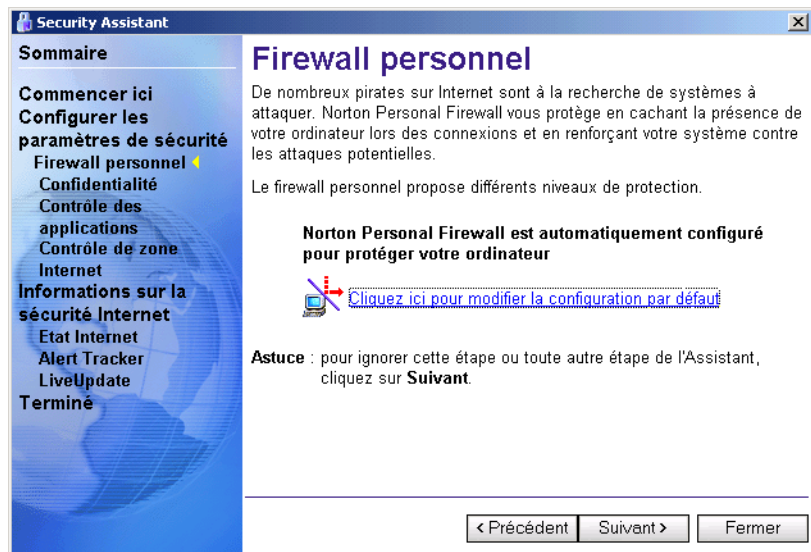
Les sections suivantes décrivent le rôle de chaque volet.

Firewall personnel

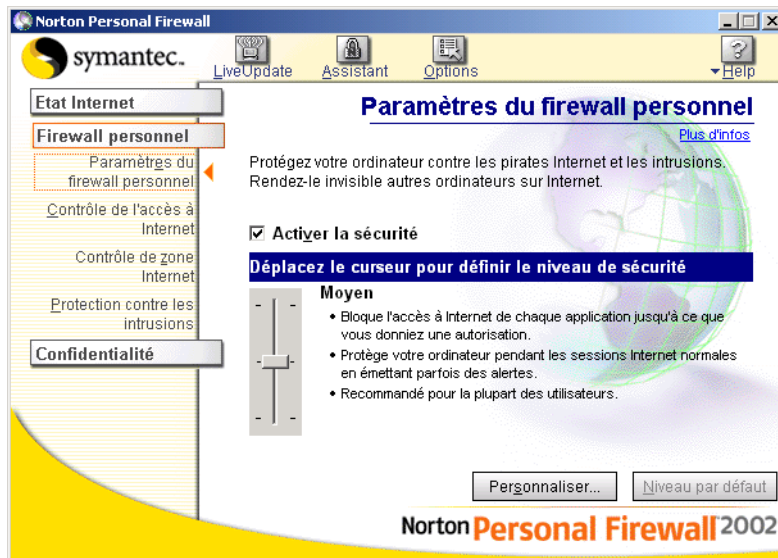
Le Firewall personnel protège votre ordinateur contre les accès non autorisés pendant que vous êtes connecté à Internet. Vous pouvez choisir d'activer ou de désactiver le Firewall personnel. S'il est activé (paramètre par défaut), vous pouvez également choisir le niveau de protection assuré.

Pour activer le Firewall personnel

- 1 Dans l'Itinéraire de l'Assistant Sécurité, cliquez sur **Firewall personnel**.



- 2 Cliquez sur **Cliquez ici pour modifier la configuration prédéfinie.**



- 3 Cochez l'option **Activer la sécurité.**

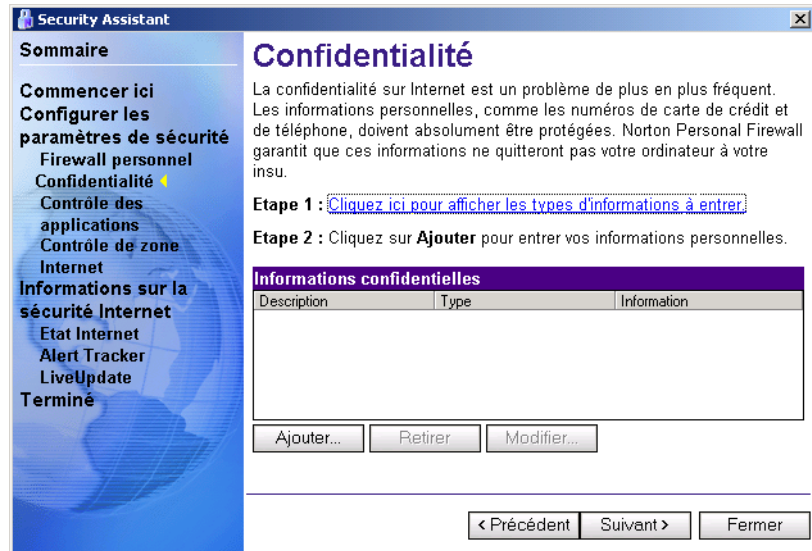
Pour plus d'informations, consultez la section « Définition du niveau de sécurité » à la page 60.

Confidentialité

La fonction de confidentialité vous permet de définir les informations confidentielles, stockées sur votre ordinateur, qui doivent bénéficier d'une protection supplémentaire. Les informations de cette liste ne peuvent être transmises aux sites Web qui n'utilisent pas de communications sécurisées et cryptées et leur envoi est interdit avec des programmes de messagerie instantanée.

Pour ajouter des informations confidentielles à bloquer

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



- 2 Dans le volet Confidentialité, cliquez sur **Ajouter**.
- 3 Dans la boîte de dialogue Ajout d'informations confidentielles, sélectionnez une catégorie dans la liste déroulante 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 informations dont vous souhaitez empêcher la transmission par l'intermédiaire de connexions Internet non sécurisées.
- 6 Cliquez sur **OK**.

Pour plus d'informations, consultez la section « Définition des informations confidentielles à bloquer » à la page 42.

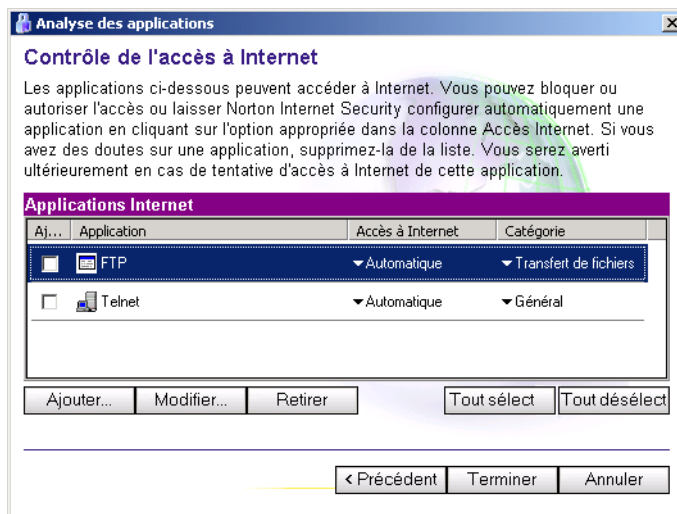
Contrôle des applications

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 de filtrage.

Pour analyser les applications utilisant Internet

- 1 Dans l'itinéraire de l'Assistant Sécurité, cliquez sur **Contrôle des applications**.
- 2 Dans le volet Contrôle des applications, cliquez sur **Cliquez ici pour analyser les applications Internet**.
- 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.



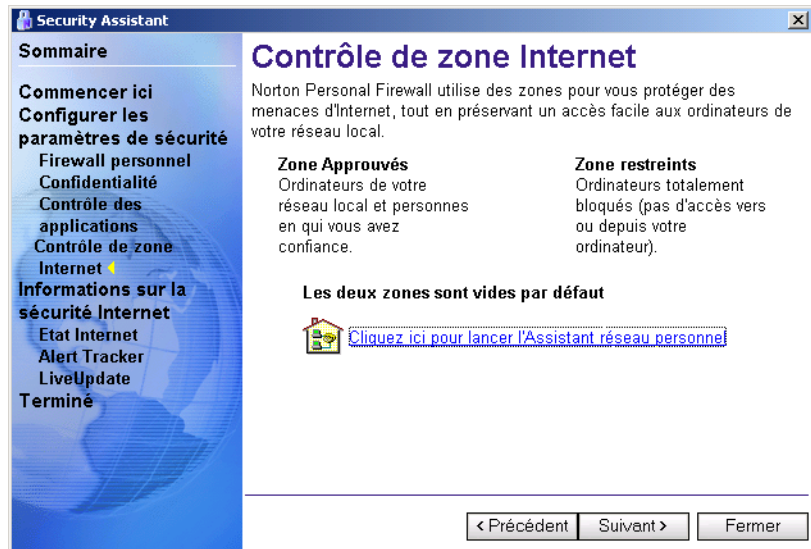
- 4 Pour autoriser une application à accéder à Internet, cochez la case à gauche de son nom.
- 5 Pour modifier la règle d'accès ou la catégorie d'une application, sélectionnez le paramètre souhaité dans la liste appropriée.
- 6 Cliquez sur **Terminer** lorsque vous avez fini.

Contrôle de zone Internet

Le contrôle de zone Internet permet d'identifier les ordinateurs que vous savez inoffensifs et ceux dont vous souhaitez limiter l'accès à votre ordinateur. Le contrôle de zone peut configurer automatiquement votre réseau et ajouter à la zone Approuvés les ordinateurs qu'il contient.

Pour utiliser le contrôle de zone depuis l'Assistant Sécurité

- 1 Dans l'Itinéraire de l'Assistant Sécurité, cliquez sur **Zone Internet**.



- 2 Dans le volet Contrôle de zone Internet, cliquez sur **Cliquez ici pour lancer l'Assistant Contrôle de zone**.
- 3 Suivez les instructions affichées à l'écran.

Pour plus d'informations, consultez la section « Protection d'un réseau domestique avec le contrôle de zone Internet » à la page 67.

Etat Internet

Norton Personal Firewall contrôle les activités qui interviennent sur votre ordinateur quand vous êtes connecté à Internet. Vous pouvez vous informer sur cette activité avec l'Etat Internet.

Pour vérifier l'état d'Internet

- 1 Dans l'Itinéraire de l'Assistant Sécurité, cliquez sur **Etat Internet**.
- 2 Pour consulter l'état actuel, cliquez sur **Etat courant**.

Pour plus d'informations, consultez la section « [Contrôle des événements de Norton Personal Firewall](#) » à la page 75.

- 3 Pour modifier la quantité d'informations affichées par l'état courant, cliquez sur **Rapports**.

Pour plus d'informations, consultez la section « [Paramétrage du niveau de détail des informations](#) » à la page 56.

Alert Tracker

Alert Tracker est affiché sous la forme d'un hémisphère, sur le côté de l'écran. En cas d'événement donnant lieu à un rapport de Norton Personal Firewall, Alert Tracker affiche brièvement un message pour vous informer. Pour plus d'informations, consultez la section « [Utilisation d'Alert Tracker](#) » à la page 55.

LiveUpdate

LiveUpdate vous permet de recevoir des mises à jour de votre programme et de votre protection. Pour plus d'informations, consultez la section « [Actualisation avec LiveUpdate](#) » à la page 29.

Vérification de l'état de la sécurité

Utilisez Security Check pour vérifier la vulnérabilité de votre ordinateur face aux intrusions. Le lien Security Check de Norton Personal Firewall vous connecte au site Web de Symantec. Vous y obtiendrez des informations détaillées sur ce que recherche Security Check et vous pourrez lancer l'analyse.

Pour exécuter Security Check

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Etat Internet > Security Check**.
- 2 Dans la fenêtre Security Check, cliquez sur **Rechercher les vulnérabilités**.
Votre navigateur ouvre la page Web Symantec Security Check.
- 3 Pour en savoir plus sur le rôle de Security Check, cliquez sur **A propos de la recherche des vulnérabilités**.
- 4 Pour exécuter l'analyse, cliquez sur **Rechercher les vulnérabilités**.

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

Pour obtenir davantage d'informations sur une zone analysée

- Dans la page des résultats, cliquez sur **Afficher les détails** à côté du nom de l'analyse
Si la zone présente un risque, les détails contiennent des suggestions pour résoudre le problème.

Protection des informations confidentielles

Les ordinateurs et les sites Web recueillent des informations personnelles pendant que vous naviguez sur Internet. Les fonctions de sécurité d'un ordinateur ne protègent pas toujours vos informations personnelles. Norton Privacy Control permet de protéger votre vie privée contre divers types d'intrusion.

La fonction Confidentialité vérifie que vous n'envoyez pas par inadvertance des informations confidentielles non codées sur Internet, comme les numéros de carte de crédit.

Les sites Web font appel à des *cookies* pour suivre vos visites. La plupart des sites les utilisent pour mémoriser vos préférences. Cependant, certains sites s'en servent pour suivre vos habitudes de navigation. Norton Personal Firewall offre plusieurs niveaux de contrôle sur les cookies.

Votre navigateur fournit peut-être plus d'informations que vous ne le souhaiteriez aux sites que vous visitez. Par exemple, la plupart des navigateurs révèlent aux sites Web l'adresse du dernier site visité. Privacy Control interdit au navigateur de fournir ce type d'information.

Définition du niveau de confidentialité

Le curseur de niveau de confidentialité permet de sélectionner un niveau de confidentialité faible, moyen ou élevé.

Paramètre	Description
Elevé	Toutes les informations personnelles sont bloquées sur Internet. Une alerte apparaît chaque fois qu'un cookie est intercepté.
Moyen (conseillé)	Une alerte apparaît si des informations confidentielles sont saisies dans un formulaire Web ou une messagerie instantanée. Dissimule vos parcours aux sites Web. Les cookies ne sont pas bloqués.
Faible	Les informations confidentielles ne sont pas bloquées. Les cookies ne sont pas bloqués. Dissimule vos parcours aux sites Web.

Pour définir le niveau de confidentialité

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Placez le curseur **Niveau de confidentialité** sur le niveau de votre choix.

Définition des informations confidentielles à bloquer

De nombreux sites Web demandent des informations personnelles et portent atteinte à votre vie privée ou pourraient permettre à quelqu'un de vous nuire. Par ailleurs, les informations transmises par messagerie instantanée ne sont pas sécurisées.

Pour plus d'informations, consultez la section « [Activation des connexions Web sécurisées](#) » à la page 45.

Norton Personal Firewall permet de créer une liste d'informations confidentielles à censurer dans tous les échanges non sécurisés sur Internet.

Pour ajouter des informations confidentielles à bloquer

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Infos 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 déroulante 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 par l'intermédiaire de connexions Internet non sécurisées.

Conseils pour la saisie des informations confidentielles

Norton Personal Firewall bloque les informations personnelles telles que vous les avez saisies. Il est donc préférable de taper une partie seulement des numéros à protéger. Par exemple, un numéro de téléphone peut être saisi sous la forme 01-02-03-04-05, 0102030405 ou 01 02 03 04 05, voire dans plusieurs champs. Quel que soit le format, les quatre derniers chiffres sont toujours groupés. Vous serez donc mieux protégé si vous tapez les quatre derniers chiffres au lieu du numéro entier.

La saisie d'informations partielles présente deux avantages. D'abord, vous évitez de saisir votre numéro de carte de crédit entier avec le risque que quelqu'un n'en prenne connaissance. Deuxièmement, Norton Personal Firewall pourra bloquer vos informations personnelles sur les sites sur lesquels les numéros de carte de crédit sont découpés en plusieurs champs.

Paramétrage des options de confidentialité

Vous pouvez modifier le paramétrage des fonctions Informations confidentielles, Blocage des cookies, Confidentialité de navigation et Connexions sécurisées si le niveau de confidentialité ne vous convient pas.

Modification du paramétrage de la fonction Informations confidentielles

La fonction Informations confidentielles comporte trois options :

- 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'une messagerie instantanée.
- Aucun : ne bloque pas les informations confidentielles.

Pour modifier le paramétrage de la fonction Informations confidentielles

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Personnaliser**.
- 3 Sélectionnez un paramètre de la fonction Informations confidentielles.

Modification du paramétrage de la fonction Blocage des cookies

Les cookies sont de petits fichiers que le navigateur enregistre sur l'ordinateur. Certains sites Web s'en servent pour enregistrer des informations destinées à simplifier la navigation.

Les cookies qui enregistrent des informations personnelles peuvent porter atteinte à votre vie privée en permettant à des tiers d'accéder à ces informations sans votre autorisation. En effet, ils peuvent contenir suffisamment d'informations pour dévoiler vos habitudes de navigation ou divulguer vos mots de passe et vos noms d'ouverture de session.

Lorsqu'un site Web demande un cookie à votre ordinateur, Norton Personal Firewall vérifie si vous avez choisi d'autoriser les cookies, de les bloquer ou d'utiliser la fonction Alerte cookie pour déterminer l'action à exécuter.

La fonction Blocage des cookies comporte trois paramètres :

- Maximum : bloque tous les cookies.
- Moyen : vous prévient chaque fois qu'un cookie est intercepté.
- Aucun : autorise les cookies.

Pour modifier les paramètres de blocage des cookies

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Personnaliser**.
- 3 Sélectionnez un paramètre de blocage des cookies.

Activation de la confidentialité de navigation

La fonction Confidentialité de navigation empêche les sites Web d'identifier le navigateur que vous utilisez et de déterminer le dernier site Web visité.

Pour activer la confidentialité de navigation

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Personnaliser**.
- 3 Dans la boîte de dialogue Personnalisation de la confidentialité, cochez la case **Activer la confidentialité de navigation**.

Activation des connexions Web sécurisées

Lorsque vous visitez un site Web sécurisé, le navigateur établit automatiquement une connexion cryptée avec ce site. Les informations transmises par l'intermédiaire des connexions sécurisées ne sont pas détectées par le firewall car elles sont cryptées. Le terme *cryptage* signifie que les informations sont codées à l'aide d'une formule mathématique qui brouille les données et les rend illisibles.

Pour activer les connexions Web sécurisées

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Personnaliser**.
- 3 Dans la boîte de dialogue Personnalisation de la confidentialité, cochez la case **Activer la sécurisation des connexions (https)**.

Blocage des connexions Web sécurisées

Pour vous assurer qu'aucune information confidentielle ne peut être transmise sur une connexion Web sécurisée, vous pouvez bloquer toutes les connexions sécurisées.

Pour bloquer les connexions Web sécurisées

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Personnaliser**.
- 3 Dans la boîte de dialogue Personnalisation de la confidentialité, désélectionnez la case **Activer la sécurisation des connexions (https)**.

Répondre aux alertes de Norton Personal Firewall

Norton Personal Firewall surveille les communications en provenance et à destination de votre ordinateur et vous prévient si une activité risque d'en compromettre la sécurité.

The screenshot shows a dialog box titled "Norton Personal Firewall" with the following content:

- Type d'alerte:** Alerte ActiveX
- Description du problème qui a déclenché l'alerte:** Une page Web venant de www.msn.fr contient un contrôle ActiveX. Vous devez autoriser ou bloquer ce contrôle pour terminer le chargement de la page.
- Evaluation du risque:** Niveau de menace Risque moyen
- Réponses proposées pour l'alerte:**
 - Autoriser ce contrôle ActiveX
 - Bloquer ce contrôle ActiveX
- Rendre ce choix permanent:** Autoriser le paramétrage par défaut pour ce site Web et ne plus me demander.

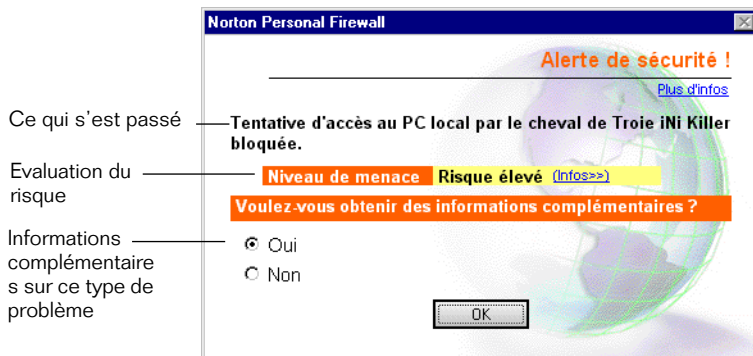
Lorsqu'une alerte apparaît, lisez le message avant de prendre une décision. Identifiez le type d'alerte et le niveau de risque. Quand vous avez évalué les risques, faites un choix.

Les alertes des types suivants apparaissent dans Norton Personal Firewall :

- Alertes de sécurité
- alertes de contrôle de l'accès à Internet
- alertes ActiveX
- alertes Java
- alertes de cookie
- alertes de confidentialité

Réponse aux alertes de sécurité

Les alertes de sécurité apparaissent lorsque quelqu'un tente d'accéder à votre ordinateur. Il peut s'agir d'un pirate ou d'un utilisateur de votre réseau.



La plupart des alertes de sécurité activent la fonction AutoBlock, qui interdit à l'ordinateur à l'origine de la tentative de connexion de communiquer avec votre ordinateur pendant 30 minutes. Ainsi, les assaillants ne peuvent pas tenter diverses attaques pour accéder à votre ordinateur.

Pour plus d'informations, consultez la section « [Utilisation de la protection contre les intrusions pour arrêter les attaques](#) » à la page 70.

Vérifiez que l'alerte correspond à une attaque réelle et non à une tentative légitime d'accès à l'ordinateur. Si la tentative est légitime, utilisez le contrôle d'accès à Internet pour autoriser le type de connexion décrit dans l'alerte.

Pour plus d'informations, consultez la section « [Ajout d'ordinateurs aux zones](#) » à la page 68.

Pour plus d'informations, consultez la section « [Ajout d'une application au contrôle d'accès à Internet](#) » à la page 66.

Ne partez pas du principe que toutes les alertes de sécurité signalent une tentative de piratage de l'ordinateur. De nombreux événements plus ou moins bénins peuvent déclencher des alertes de sécurité sur Internet. Les questions suivantes peuvent vous aider à déterminer si une alerte de sécurité signale une attaque réelle ou une activité normale sur Internet :

- La tentative de connexion émane-t-elle d'un ordinateur inconnu ?
- L'alerte de sécurité signale-t-elle une activité manifestement menaçante ? L'accès à un simple port fermé n'est pas aussi dangereux que l'analyse de tous les ports.
- Cette tentative fait-elle partie d'une série d'actions menaçantes émanant d'un même ordinateur ?

Si vous ne pouvez pas répondre oui à toutes ces questions, vous ne faites probablement pas l'objet d'une attaque. Toutefois, vous avez peut-être détecté un pirate analysant plusieurs ordinateurs à la recherche de failles éventuelles. Si Norton Personal Firewall est activé, votre ordinateur ne semblera pas vulnérable au pirate. En fait, le pirate ne s'apercevra peut-être même pas de son existence.

Pour plus d'informations, consultez la section « [Risques et menaces liés à Internet](#) » à la page 101.

Pour répondre à une alerte de sécurité

- 1 Dans la fenêtre Alertes de sécurité, cliquez sur **Infos** pour lire des informations sur l'événement.
- 2 Cliquez sur **Oui** pour obtenir des informations complémentaires sur ce type d'incident.
- 3 S'il apparaît que Norton Personal Firewall bloque une activité acceptable, modifiez les paramètres de protection ou de rapport du firewall.

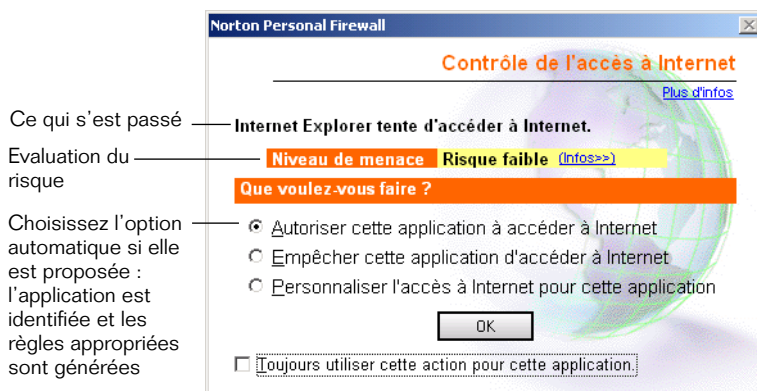
Pour plus d'informations, consultez la section « [Personnalisation de la protection par firewall](#) » à la page 59.

Pour plus d'informations, consultez la section « [Paramétrage du niveau de détail des informations](#) » à la page 56.

- 4 Cliquez sur **OK** pour faire disparaître l'incident.

Réponse aux alertes de contrôle d'accès à Internet

Les alertes Contrôle d'accès à Internet apparaissent lorsque Norton Personal Firewall nécessite votre intervention concernant une application qui tente d'accéder à Internet depuis l'ordinateur.



Vous pouvez réduire le nombre d'alertes de contrôle d'accès à Internet en lançant une analyse des applications ou en activant la fonction de contrôle automatique d'accès à Internet. Lorsque cette option est activée, Norton Personal Firewall crée des règles pour les applications reconnues sans interrompre votre travail.

Pour plus d'informations, consultez la section « [Analyse des applications pour déterminer celles utilisant Internet](#) » à la page 65.

Pour plus d'informations, consultez la section « [Activation du contrôle automatique d'accès à Internet](#) » à la page 65.

Pour répondre à une alerte de contrôle d'accès à Internet

- 1 Dans la fenêtre Contrôle d'accès à Internet, cliquez sur **Infos** pour lire des informations sur l'événement.
- 2 Effectuez l'une des opérations suivantes :
 - Cliquez sur **Configurer automatiquement l'accès à Internet** quand il est disponible.

Norton Personal Firewall identifie l'application et dispose des règles d'accès appropriées dans sa base de données. Il est recommandé de sélectionner cette option chaque fois que possible.
 - Choisissez l'option **Autoriser cette application à accéder à Internet** pour accorder à l'application un accès Internet complet.

Cette option, moins sûre que l'option automatique, convient pour de nombreuses applications non reconnues par Norton Personal Firewall. Si vous connaissez l'application et la considérez comme sûre, utilisez cette option.
 - Choisissez **Empêcher cette application d'accéder à Internet** pour interdire à l'application d'accéder à Internet.

Cette option est conseillée si vous ne reconnaissez pas l'application et si le risque est élevé.
 - Choisissez **Personnaliser l'accès à Internet pour cette application** pour créer des règles encadrant l'accès de l'application à Internet.

Choisissez cette option si vous comprenez comment l'application accède à Internet et souhaitez créer des règles particulières pour en contrôler l'accès. Le choix de cette option entraîne le démarrage de l'Assistant Ajouter une règle.

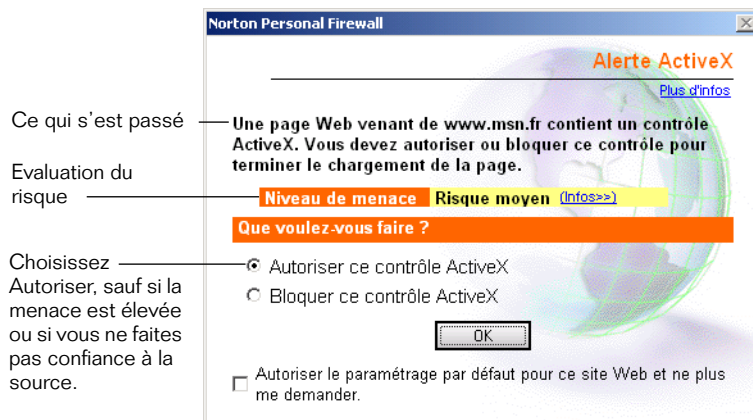
Réponse aux alertes Java et ActiveX

Les applets Java et les contrôles ActiveX sont des composants de page Web dont l'action dépasse l'affichage de texte et d'images. Ces composants sont souvent utilisés pour afficher des menus contextuels ou des cotations boursières.

Les alertes ActiveX et Java apparaissent lorsque le niveau de sécurité a la valeur Maximum, ou lorsque les options Protection contre les applets Java ou Protection contre les contrôles ActiveX ont la valeur Moyen et qu'une applet Java ou qu'un contrôle ActiveX est intercepté.

Pour plus d'informations, consultez la section « Définition du niveau de sécurité » à la page 60.

Pour plus d'informations, consultez la section « Définition des niveaux de sécurité pour les applets Java et les contrôles ActiveX » à la page 62.



Pour répondre à une alerte Java ou Active X

- 1 Dans la fenêtre Alerte Java ou Alerte ActiveX, cliquez sur **Infos** pour lire des informations sur l'événement.
- 2 Effectuez l'une des opérations suivantes :
 - Choisissez **Autoriser ce contrôle ActiveX / cette applet Java** pour autoriser l'exécution de l'élément concerné.
 - Choisissez **Bloquer ce contrôle ActiveX / cette applet Java** pour interdire l'exécution de l'élément concerné.

Cette option est la plus sûre ; cependant, la page Web pourrait ne pas s'afficher ou fonctionner correctement. Si vous choisissez Bloquer et si la page Web ne s'affiche pas ou ne fonctionne pas correctement, cliquez sur le bouton Actualiser du navigateur et choisissez Autoriser.

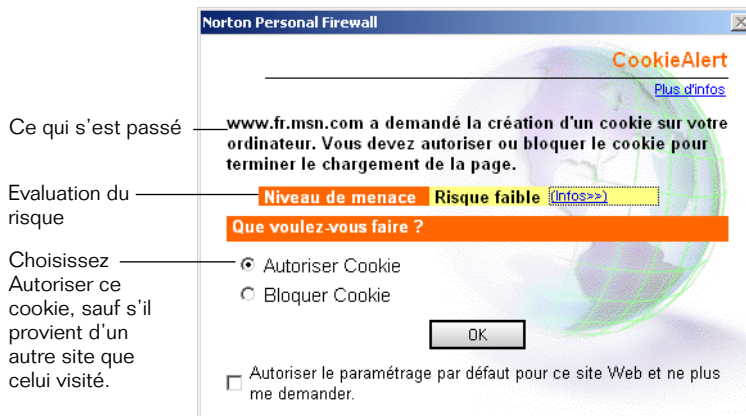
Réponse aux alertes de cookie

Les cookies sont de petits fichiers enregistrés sur l'ordinateur et utilisés par les sites Web pour suivre les visiteurs.

Les alertes de cookie apparaissent lorsque le niveau de confidentialité a la valeur Maximum, ou lorsque l'option Blocage des cookies a la valeur Moyen et qu'un cookie est intercepté.

Pour plus d'informations, consultez la section « Définition du niveau de confidentialité » à la page 42.

Pour plus d'informations, consultez la section « Modification du paramétrage de la fonction Blocage des cookies » à la page 44.



Il est conseillé de ne pas bloquer les cookies, car ils sont fréquemment utilisés et ne constituent pas un grand risque. Les cookies posent cependant des risques réels pour votre vie privée.

Pour plus d'informations, consultez la section « Risques et menaces liés à Internet » à la page 101.

Pour bloquer tous les cookies et ne pas voir d'alerte, attribuez au paramètre Blocage des cookies la valeur Maximum : cookies bloqués.

Pour répondre à une alerte de cookie

- 1 Dans la fenêtre Alerte cookie, cliquez sur **Infos** pour lire des informations sur l'événement.
- 2 Effectuez l'une des opérations suivantes :
 - Cliquez sur **Autoriser ce cookie** pour autoriser la création ou la lecture du cookie.

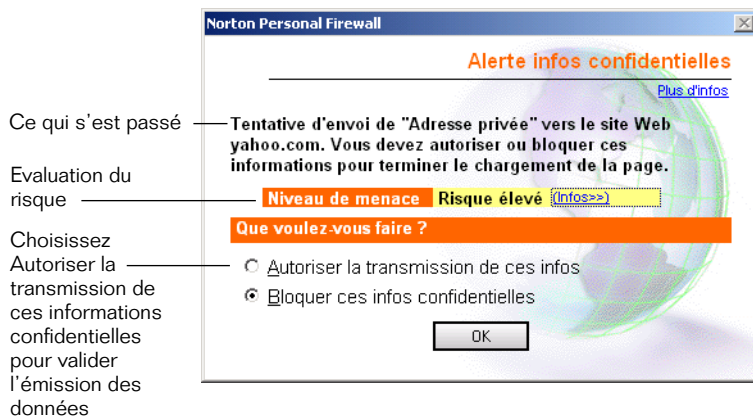
Les cookies originaires du site Web visité sont en général sans danger et peuvent être nécessaires au bon fonctionnement des pages Web.

- Cliquez sur **Bloquer ce cookie** pour interdire la création ou la lecture du cookie.

Lorsque vous bloquez les cookies de certaines pages, des alertes de cookie risquent de s'afficher à plusieurs reprises. Les cookies issus d'autres sites Web que celui visité sont en général exploités pour suivre votre utilisation d'Internet. Vous pouvez généralement les bloquer sans incidence sur le fonctionnement du site visité.

Réponse aux alertes de confidentialité

Les alertes de confidentialité apparaissent si vous essayez d'envoyer des informations protégées à un site Web n'utilisant pas de communications chiffrées et sécurisées ou par l'intermédiaire d'un programme de messagerie instantanée.



L'alerte précise les informations que vous tentez d'envoyer ainsi que le site Web auquel elles sont destinées.

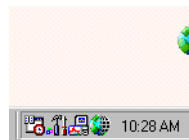
Pour répondre aux alertes de confidentialité

- 1 Dans la fenêtre Alerte informations confidentielles, cliquez sur **Infos** pour lire des informations sur l'événement.
- 2 Effectuez l'une des opérations suivantes :
 - Cliquez sur **Autoriser la transmission de ces informations confidentielles** pour envoyer les informations.
Par exemple, sélectionnez cette option si vous essayez de passer une commande.
 - Cliquez sur **Empêcher la transmission de ces informations confidentielles** pour interdire l'envoi des informations.

Il est possible que Norton Personal Firewall considère comme confidentielles des informations qui ne le sont pas. Par exemple, vous pourriez indiquer le numéro de téléphone d'un magasin dont les quatre derniers chiffres correspondent à ceux de votre numéro de carte de crédit. Dans ce cas, vous pouvez autoriser l'envoi des informations.

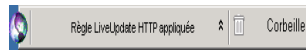
Utilisation d'Alert Tracker

Alert Tracker vous tient informé sur les actions de Norton Personal Firewall.



Alert Tracker est affiché en permanence sur le côté de l'écran

Quand survient un événement dont Norton Personal Firewall veut vous informer, mais qui ne justifie pas d'interrompre votre travail, Alert Tracker affiche un message pendant quelques secondes, puis retourne sur le côté de l'écran.



Les messages Alert Tracker sont affichés pendant quelques secondes

Ouverture d'Alert Tracker

Vous pouvez ouvrir Alert Tracker pour consulter les derniers messages et accéder à la Corbeille.

Pour ouvrir Alert Tracker

- Sur le Bureau de Windows, cliquez deux fois sur **Alert Tracker**.

Consultation des messages récents d'Alert Tracker

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 vers le haut si elle apparaît.
- 3 Cliquez sur un message pour consulter le journal des événements.

Déplacement d'Alert Tracker

Alert Tracker peut s'ancrer des deux côtés de l'écran principal.

Pour déplacer Alert Tracker

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

Masquer Alert Tracker

Vous pouvez masquer Alert Tracker si vous ne voulez pas qu'il apparaisse à l'écran.

Pour masquer Alert Tracker

- Dans la zone de notification de la barre des tâches de Windows, cliquez avec le bouton droit sur l'icône Norton Personal Firewall et choisissez **Masquer Alert Tracker**.

Paramétrage du niveau de détail des informations

Vous pouvez définir le niveau de détail des informations affichées dans Alert Tracker et le nombre d'alertes de sécurité qui apparaissent.

Définition du niveau de détail des informations

Le curseur de niveau de détail des informations permet de sélectionner un niveau de détail minimum, moyen ou maximum. Le niveau de précision varie en fonction de la position du curseur.

Paramètre	Description
Elevé	<p>Fournit des informations très complètes sur les activités de Norton Personal Firewall. Tous les messages Alert Tracker sont affichés.</p> <p>Signale les applications qui accèdent à Internet et les alertes de sécurité.</p>
Moyen (conseillé)	<p>Fournit des informations sur les événements Internet importants. Un nombre moyen de messages Alert Tracker est affiché.</p> <p>Signale les alertes de sécurité et les événements relatifs au contrôle automatique de l'accès à Internet.</p>
Faible	<p>Fournit des informations sur les événements Internet graves.</p> <p>Signale les alertes de sécurité et les événements relatifs au contrôle automatique de l'accès à Internet.</p>

Pour définir le niveau de détail

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Etat Internet > Rapport**.
- 2 Placez le curseur un niveau de détail.

Personnalisation de la protection par firewall

Norton Personal Firewall protège votre ordinateur des tentatives d'accès non autorisées. Il bloque les attaques provenant d'autres ordinateurs et contrôle l'accès des applications du système à Internet.

Le firewall offre quatre types de protection :

- Norton Personal Firewall comporte un paramètre général Niveau de sécurité qui effectue toutes les modifications nécessaires dans l'ensemble du programme.
- La fonction Contrôle de l'accès à Internet définit les règles d'accès pour les applications installées sur l'ordinateur.
- Le contrôle de zone Internet permet d'accéder aux ordinateurs approuvés et de bloquer complètement les ordinateurs restreints.
- La fonction de protection contre les intrusions surveille d'éventuelles attaques de pirates contre l'ordinateur et les empêche d'y accéder.

Définition du niveau de sécurité

Le système de niveau de sécurité permet de paramétrer l'ensemble de Norton Personal Firewall conformément au niveau de protection souhaité. Il modifie les paramètres de firewall et les règles concernant les applets Java et les contrôles ActiveX. Il définit également la réponse des ports inutilisés aux tentatives d'accès.

Le curseur permet de sélectionner le niveau de sécurité faible, moyen ou élevé. Le niveau de protection varie en fonction de la position du curseur.

Paramètre	Description
Elevé	<p>Le firewall est en position Elevé et 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 d'accès à Internet.</p> <p>Le blocage des contrôles ActiveX et des applets Java est en position Moyen, et demande votre autorisation chaque fois que l'un d'entre eux doit être exécuté.</p> <p>Les ports inutilisés ne répondent pas aux tentatives de connexion. Les ordinateurs externes ne les voient plus.</p>
Moyen (conseillé)	<p>Le firewall est en position Elevé et 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 d'accès à Internet.</p> <p>La sécurité des contrôles ActiveX et des applets Java est en position Aucun et aucune autorisation n'est demandée avant leur exécution.</p> <p>Les ports inutilisés ne répondent pas aux tentatives de connexion. Les ordinateurs externes ne les voient plus.</p>
Faible	<p>Le firewall est en position Moyen et bloque les applications malveillantes connues, comme les chevaux de Troie.</p> <p>La sécurité des contrôles ActiveX et des applets Java est en position Aucun et aucune autorisation n'est demandée avant leur exécution.</p>

Pour plus d'informations, consultez la section « [Analyse des applications pour déterminer celles utilisant Internet](#) » à la page 65.

Pour définir le niveau de sécurité

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Paramètres du firewall personnel**.
- 2 Placez le curseur sur un niveau de sécurité.

Définition de paramètres de sécurité personnalisés

Si le paramétrage offert par l'option Niveau de sécurité ne vous convient pas, vous pouvez modifier le niveau de protection du firewall, des applets Java et des contrôles ActiveX.

Modification des paramètres de firewall personnel

Le firewall surveille les communications entre votre poste et d'autres ordinateurs sur Internet. Il contrôle les tentatives de connexion provenant d'autres ordinateurs et les essais effectués par les applications de votre ordinateur pour se connecter à d'autres ordinateurs.

Norton Personal Firewall a trois paramètres :

Paramètre	Description
Elevé	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. Si vous avez effectué une analyse des applications, vous ne devriez pas être interrompu souvent par des alertes d'accès à Internet.
Moyen	Bloque de nombreux ports utilisés par des applications dangereuses. Cependant, ce réglage peut également bloquer les applications utiles qui font appel aux mêmes ports.
Aucun	Désactive le firewall et autorise toutes les communications Internet.

Pour plus d'informations, consultez la section « [Analyse des applications pour déterminer celles utilisant Internet](#) » à la page 65.

Pour modifier les paramètres de firewall personnel

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Paramètres du firewall personnel**.
- 2 Cliquez sur **Personnaliser**.
- 3 Sélectionnez un paramètre de firewall personnel.

Définition des niveaux de sécurité pour les applets Java et les contrôles ActiveX

Les applets Java et les contrôles ActiveX permettent de rendre les sites Web plus interactifs. De nombreux sites Web utilisent des contrôles ActiveX et des applets Java pour afficher les données et fonctionner correctement. La plupart de ces programmes sont sûrs et ne présentent aucune menace pour votre ordinateur ou vos données.

Toutefois, n'oubliez pas que les contrôles ActiveX peuvent avoir un accès total à vos données, selon leur mode de programmation. Par exemple, ils peuvent copier des données du disque dur et les transmettre via Internet pendant que vous êtes connecté. Ils peuvent également supprimer des fichiers, intercepter des messages, récupérer des mots de passe ou recueillir des numéros de compte bancaire et d'autres données importantes.

La seule manière d'empêcher l'exécution de programmes malveillants sur l'ordinateur consiste à interdire leur téléchargement. Cependant, le blocage de toutes les applets Java et de tous les contrôles ActiveX empêche de nombreux sites Web de s'afficher ou de s'exécuter correctement.

Dans la boîte de dialogue Personnalisation de la sécurité, vous disposez de trois options pour la protection contre les applets Java et les contrôles ActiveX :

Paramètre	Description
Elevé	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 utilisant ces contrôles ne fonctionnent pas correctement lorsqu'elle est activée.
Moyen	Demande si vous voulez charger une applet Java ou 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 ceux que vous voulez exécuter.
Aucun	Autorise l'exécution de toutes les applets Java et de tous les contrôles ActiveX.

Pour définir les niveaux de sécurité pour les applets Java et les contrôles ActiveX

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Paramètres du firewall personnel**.
- 2 Cliquez sur **Personnaliser**.
- 3 Sélectionnez les paramètres Protection contre les applets Java et Protection contre les contrôles ActiveX appropriés.

Activation des alertes de contrôle d'accès à Internet

Les alertes de contrôle d'accès à Internet permettent à l'utilisateur de contrôler les connexions d'une application à Internet quand il n'existe pas de règle de filtrage applicable. Lors d'une tentative de connexion, une alerte de contrôle d'accès à Internet apparaît et permet d'autoriser ou de bloquer l'accès de l'application à Internet.

Désactivez cette option si vous souhaitez bloquer l'accès à Internet de certaines applications lorsqu'aucune règle de filtrage n'est applicable.

Pour activer les alertes de contrôle d'accès à Internet

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Paramètres du firewall personnel**.
- 2 Cliquez sur **Personnaliser**.
- 3 Sélectionnez l'option **Activer les alertes de contrôle d'accès**.

Activation des alertes pour les ports inutilisés

Norton Personal Firewall interdit l'accès aux ports inutilisés de l'ordinateur.

Par exemple, si quelqu'un tente de se connecter à votre ordinateur en utilisant Symantec pcAnywhere alors qu'aucun Elève pcAnywhere n'est lancé, aucune réponse n'est envoyée suite à la tentative de connexion ; ainsi, l'ordinateur distant n'obtient aucune information sur votre poste.

Des alertes apparaissent quand un ordinateur tente d'accéder à un port inutilisé de votre ordinateur. Ces alertes sont pratiques pour résoudre des problèmes lorsque vous configurez des logiciels et des fonctions évolués, comme le partage d'une connexion Internet. Désactivez-les pour éviter l'affichage d'alertes concernant des tentatives de connexion inoffensives.

Pour activer des alertes pour les ports inutilisés

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Paramètres du firewall personnel**.
- 2 Cliquez sur **Personnaliser**.
- 3 Sélectionnez l'option **Alerte en cas d'accès de ports inutilisés**.

Contrôle des applications qui accèdent à Internet

Les applications se connectent à Internet pour diverses raisons. Un navigateur Web se connecte à Internet pour permettre la consultation de pages Web. LiveUpdate accède à Internet pour actualiser votre protection Internet et antivirus. Microsoft NetMeeting se connecte à Internet pour permettre d'organiser des téléconférences.

Ces applications ont des besoins différents en matière d'accès à Internet. Certaines, comme LiveUpdate, ont des besoins simples. D'autres, comme Internet Explorer, ont des besoins plus complexes.

La fonction Contrôle de l'accès à Internet gère la liste des applications de l'ordinateur qui accèdent à Internet. Cette liste enregistre les besoins des applications et précise si l'accès Internet leur est accordé ou refusé.

Il existe plusieurs moyens d'ajouter des applications à la liste du contrôle de l'accès à Internet :

- Analyser les applications pour déterminer celles utilisant Internet : toutes les applications Internet sont détectées et configurées en même temps.
Pour plus d'informations, consultez la section « [Analyse des applications pour déterminer celles utilisant Internet](#) » à la page 65.
- Activer le contrôle automatique de l'accès à Internet : permet de configurer automatiquement l'accès Internet des applications connues à leur premier lancement.
Pour plus d'informations, consultez la section « [Activation du contrôle automatique d'accès à Internet](#) » à la page 65.
- Répondre aux alertes : Norton Personal Firewall vous prévient la première fois qu'une de ces applications tente de se connecter à Internet. Vous pouvez lui interdire ou lui autoriser l'accès. Si l'application est reconnue, Norton Personal Firewall vous invite à utiliser l'option de configuration automatique.
Pour plus d'informations, consultez la section « [Réponse aux alertes de contrôle d'accès à Internet](#) » à la page 50.
- Ajouter des applications une par une : vous pouvez ajouter des applications à la liste de l'écran Contrôle de l'accès à Internet.
Pour plus d'informations, consultez la section « [Ajout d'une application au contrôle d'accès à Internet](#) » à la page 66.

Analyse des applications pour déterminer celles utilisant Internet

L'analyse des applications est le moyen le plus rapide de paramétrer le contrôle d'accès à Internet pour tous vos logiciels. Norton Personal Firewall analyse les applications de l'ordinateur et vous permet de choisir un paramétrage pour chacune d'entre elles.

Pour analyser les applications utilisant Internet

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Contrôle d'accès à Internet**.
- 2 Cliquez sur **Configurer**, puis sur **Analyse des applications**.
- 3 Suivez les instructions affichées à l'écran.

Activation du contrôle automatique d'accès à Internet

Lorsque le contrôle automatique d'accès à Internet est activé, Norton Personal Firewall crée automatiquement une règle de firewall la première fois qu'une application pour laquelle il a une signature numérique (empreinte) est exécutée.

N'activez pas cette option si vous préférez être prévenu lorsqu'une nouvelle application tente d'accéder à Internet.

Veillez à exécuter LiveUpdate chaque semaine pour actualiser votre programme et votre protection.

Pour activer le contrôle automatique de l'accès à Internet

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Contrôle d'accès à Internet**.
- 2 Cliquez sur **Configurer** et sélectionnez **Activer le Contrôle automatique d'accès à Internet**.

Réponse aux alertes de contrôle d'accès à Internet

Si le contrôle automatique d'accès à Internet n'est pas activé ou si Norton Personal Firewall détecte une application inconnue tentant d'accéder à Internet, une alerte de Contrôle d'accès à Internet apparaît.

Si l'option Configurer automatiquement l'accès à Internet figure dans l'alerte, Norton Personal Firewall reconnaît l'application et peut configurer son accès correctement.

Si l'option n'apparaît pas, l'application n'est pas reconnue par Norton Personal Firewall et vous devez choisir d'autoriser ou de bloquer son accès à Internet. Vérifiez le niveau de menace avant de décider.

Si l'option Configurer automatiquement l'accès à Internet figure dans l'alerte, Norton Personal Firewall reconnaît l'application mais n'attend pas la tentative de communication dans le cadre du fonctionnement normal de l'application.

Pour plus d'informations, consultez la section « [Réponse aux alertes de contrôle d'accès à Internet](#) » à la page 50.

Ajout d'une application au contrôle d'accès à Internet

Vous pouvez ajouter manuellement des applications à la liste de l'écran Contrôle d'accès à Internet. Utilisez cette méthode si une de vos applications a des besoins particuliers en matière d'accès à Internet et si vous comprenez le fonctionnement des règles de filtrage.

Pour ajouter une application au contrôle d'accès à Internet

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Contrôle d'accès à Internet**.
- 2 Cliquez sur **Ajouter**.
- 3 Sélectionnez le fichier exécutable de l'application.
- 4 Cliquez sur **Ouvrir**.
- 5 Dans la fenêtre Contrôle d'accès à Internet, suivez les instructions affichées à l'écran.

Modification des paramètres du contrôle d'accès à Internet

Vous pouvez modifier le paramétrage du contrôle d'accès à Internet pour des applications. Vous pouvez, par exemple, permettre l'accès à une application bloquée jusqu'ici.

Pour modifier les paramètres du contrôle d'accès à Internet

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Contrôle d'accès à Internet**.
- 2 Sous Accès Internet, sélectionnez l'entrée correspondant à l'application à modifier.
- 3 Dans le menu déroulant, choisissez un autre paramètre.

Modification des paramètres applicables à l'ensemble du système

Les paramètres applicables à l'ensemble du système offrent une protection plus générale que ceux applicables à une seule application. Par exemple, la protection contre les tentatives d'accès utilisant les fonctions de réseau Microsoft est définie dans les paramètres applicables à l'ensemble du système.

Les paramètres applicables à l'ensemble du système constituent une série de règles utilisées par le firewall pour autoriser ou interdire diverses activités. Vous pouvez modifier ces règles ou en ajouter d'autres ; cependant, sans une bonne compréhension de leur rôle, vous risquez de compromettre votre protection.

Pour modifier les paramètres applicables à l'ensemble du système

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Contrôle d'accès à Internet**.
- 2 Cliquez sur **Configurer** et sélectionnez **Paramètres applicables à l'ensemble du système**.

Protection d'un réseau domestique avec le contrôle de zone Internet

Le contrôle de zone Internet permet d'identifier facilement les ordinateurs que vous savez inoffensifs et ceux dont vous souhaitez limiter l'accès à votre ordinateur. Deux cas de figure peuvent se présenter : approuvés et restreints.

Les ordinateurs placés dans la zone Approuvés ne sont pas surveillés par Norton Personal Firewall. Ils bénéficient d'un accès total à votre ordinateur, comme si Norton Personal Firewall n'était pas installé. Utilisez cette zone pour les ordinateurs du réseau local avec lesquels vous avez besoin de partager des fichiers et des imprimantes.

Si un ordinateur de la zone Approuvés est attaqué et si un pirate en prend le contrôle, votre poste est menacé.

Les ordinateurs placés dans la zone Restreints ne peuvent pas du tout accéder au vôtre. Ajoutez à cette zone les ordinateurs qui essaient de vous attaquer. La zone Restreints fournit un niveau de protection supérieur à la protection normale assurée par Norton Personal Firewall. Vous ne pouvez pas échanger d'informations avec les ordinateurs de cette zone.

Ajout d'ordinateurs aux zones

Ajoutez à la zone Approuvés les ordinateurs que vous considérez comme non dangereux. Ajoutez à la zone Restreints ceux que vous voulez bloquer complètement.

Pour ajouter des ordinateurs à une zone

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Contrôle de zone Internet**.
- 2 Sélectionnez la zone à laquelle vous voulez ajouter un ordinateur.
- 3 Cliquez sur **Ajouter**.

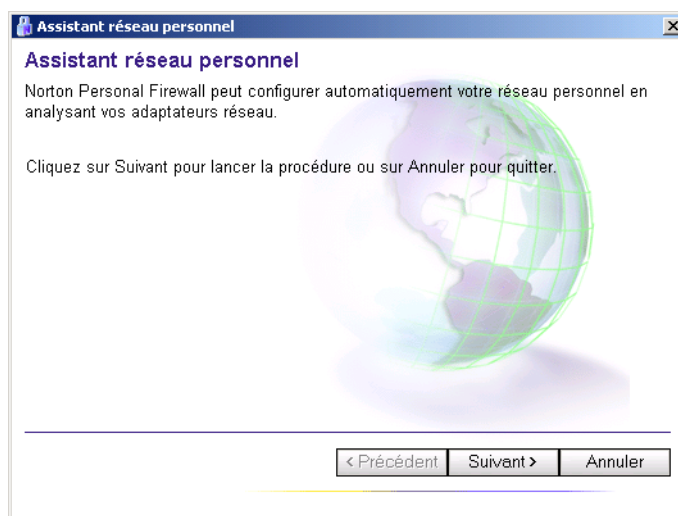
Vous pouvez ajouter un ou plusieurs ordinateurs. Pour plus d'informations, consultez la section « [Identification d'ordinateurs dans Norton Personal Firewall](#) » à la page 72.

Ajout d'ordinateurs du réseau domestique à la zone Approuvés

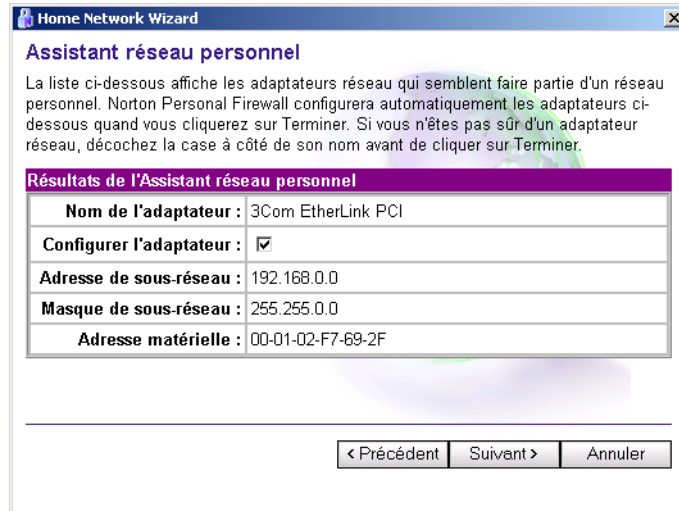
Le contrôle de zone Internet est le moyen le plus simple d'identifier les ordinateurs du réseau domestique avec lesquels vous voulez partager des fichiers ou des imprimantes.

Pour ajouter des ordinateurs du réseau domestique à la zone Approuvés

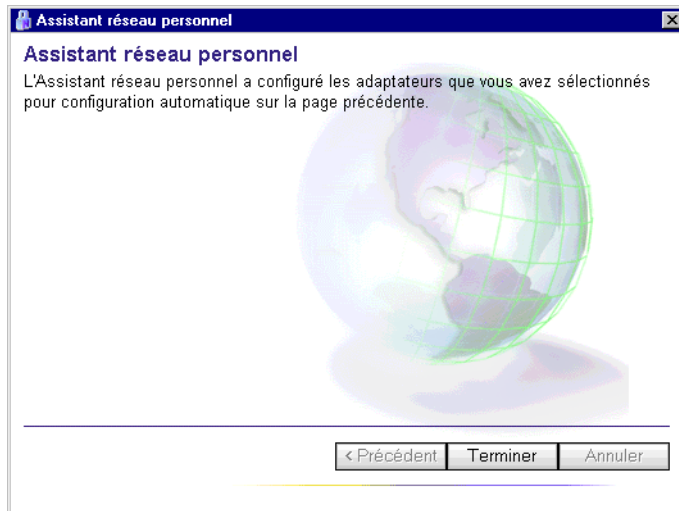
- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Contrôle de zone Internet**.
- 2 Dans le volet Contrôle de zone Internet, cliquez sur **Assistant**.



- 3 Cliquez sur **Suivant** pour lancer l'assistant.



- 4 Dans la liste résultante, cochez les adaptateurs réseau que vous souhaitez configurer automatiquement et ajouter à la zone Approuvés.
- 5 Cliquez sur **Suivant**.



- 6 Cliquez sur **Terminer** pour fermer l'assistant.

Utilisation de la protection contre les intrusions pour arrêter les attaques

La fonction de protection contre les intrusions arrête les attaques des pirates lorsqu'elles se produisent. Norton Personal Firewall surveille les communications avec Internet pour identifier les signes qui trahissent une attaque. Si un ordinateur tente, par exemple, de se connecter à une série de ports sur votre ordinateur, la fonction de protection contre les intrusions considère cette tentative comme une analyse de ports, qui est une pratique courante chez les pirates informatiques.

La protection contre les intrusions détecte également les tentatives de connexion à des ports utilisés par les chevaux de Troie d'accès à distance.

Pour plus d'informations, consultez la section « [Risques et menaces liés à Internet](#) » à la page 101.

Vous pouvez consulter et contrôler les réactions aux attaques dans la fenêtre Protection contre les intrusions.

Détection des tentatives d'analyse des ports

Pour être prévenu quand Norton Personal Firewall détecte une analyse des ports ou une autre attaque, sélectionnez l'option Détecter les tentatives d'analyse de port.

Pour activer l'option Détecter les tentatives d'analyse de port

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Protection contre les intrusions**.
- 2 Cochez l'option **Détecter les tentatives d'analyse de port**.

Activation du blocage automatique

Lorsqu'une attaque est détectée, Norton Personal Firewall vous prévient et bloque toutes les communications en provenance de l'ordinateur distant pendant 30 minutes. Ce blocage automatique des communications est appelé AutoBlock.

La fonction AutoBlock permet d'arrêter toute communication émanant de l'ordinateur distant pendant 30 minutes. En revanche, elle ne vous empêche pas de contacter cet ordinateur.

Les ordinateurs des zones Approuvés et Restreints ne sont pas concernés par le blocage automatique. Les ordinateurs de la zone Approuvés ne sont jamais bloqués, tandis que ceux de la zone Restreints le sont en permanence.

Pour activer la fonction AutoBlock

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Protection contre les intrusions**.
- 2 Sélectionnez l'option **Activer AutoBlock**.

Déblocage d'un ordinateur bloqué

Dans certains cas, Norton Personal Firewall peut considérer une activité normale comme une attaque. Si vous ne parvenez pas à communiquer avec un ordinateur avec lequel vous devriez pouvoir communiquer, vérifiez si ce dernier se trouve dans la liste Ordinateurs actuellement bloqués par AutoBlock.

Si un ordinateur auquel vous voulez accéder apparaît dans la liste Ordinateurs actuellement bloqués par AutoBlock, débloquent-le.

Pour débloquent un ordinateur bloqué

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Protection contre les intrusions**.
- 2 Sélectionnez l'adresse IP de l'ordinateur à débloquent.
- 3 Cliquez sur **Débloquent**.

Exclusion d'activités spécifiques d'AutoBlock

Certaines activités normales sur Internet seront considérées comme des attaques par Norton Personal Firewall à plusieurs reprises. Par exemple, certains fournisseurs d'accès Internet analysent les ports des ordinateurs clients afin de vérifier qu'ils respectent leurs accords de niveau de service.

Pour éviter que certaines activités normales n'interrompent les connexions Internet, vous pouvez exclure certains ordinateurs du champ d'application de la fonction AutoBlock.

Pour exclure des activités d'AutoBlock

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Protection contre les intrusions**.
- 2 Cliquez sur **Exclusions**.
- 3 Dans la liste des ordinateurs actuellement bloqués, sélectionnez l'adresse IP à exclure.
- 4 Cliquez sur **Exclure**.

Ajout d'un ordinateur bloqué à la zone Restreints

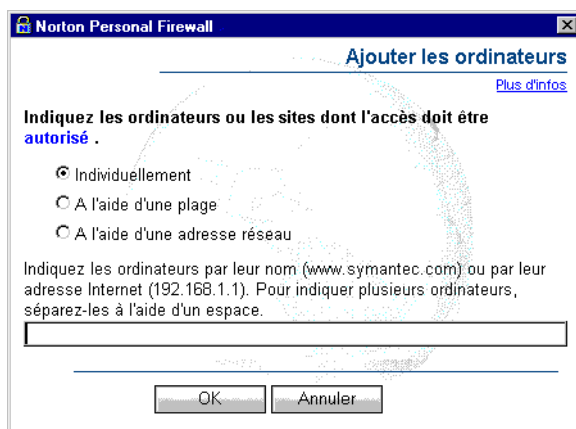
Vous pouvez ajouter un ordinateur bloqué à la zone Restreints pour l'empêcher en permanence d'accéder à votre ordinateur. Les ordinateurs ajoutés à la zone Restreints n'apparaissent plus dans la liste des ordinateurs bloqués.

Pour ajouter un ordinateur bloqué à la zone Restreints

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Protection contre les intrusions**.
- 2 Dans la liste des ordinateurs actuellement bloqués par AutoBlock, sélectionnez celui à ajouter à la liste des ordinateurs exclus et cliquez sur **Restreindre**.

Identification d'ordinateurs dans Norton Personal Firewall

Dans Norton Personal Firewall, plusieurs fonctions nécessitent d'identifier des ordinateurs. La boîte de dialogue Indiquer les ordinateurs apparaît à chaque fois.



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

Pour plus d'informations, consultez la section « A propos d'Internet » à la page 91.

Définition d'ordinateurs individuels

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. Par exemple : 206.204.52.71.

Le nom de l'ordinateur peut être une URL (Uniform Resource Locator) comme « service.symantec.com » ou un nom de réseau Microsoft, comme « Mojave ». Le nom des ordinateurs du réseau local est indiqué dans le Voisinage réseau ou dans les Favoris réseau.

Remarque : si le protocole TCP/IP n'est pas associé à Client pour les réseaux Microsoft dans la fenêtre Propriétés du réseau de Windows, vous devez utiliser des adresses IP au lieu de noms pour désigner les ordinateurs du réseau local.

Pour identifier un ordinateur individuel

- 1 Dans la fenêtre Indiquer les ordinateurs, cliquez sur **Individuellement**.
- 2 Tapez le nom ou l'adresse IP de l'ordinateur.

Identification d'une série d'ordinateurs

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

Dans la plupart des cas, les trois premiers nombres des adresses IP sont identiques.

Pour identifier une série d'ordinateurs

- 1 Dans la fenêtre 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 (le plus petit nombre).
- 3 Dans le champ Adresse Internet de fin, tapez l'adresse IP de fin (le plus grand nombre).

Identification d'ordinateurs à l'aide d'une adresse réseau

Vous pouvez identifier tous les ordinateurs d'un sous-réseau en indiquant une adresse IP et un masque de sous-réseau.

L'adresse IP indiquée doit faire partie du sous-réseau identifié. Le masque de sous-réseau prend presque toujours la valeur 255.255.255.0.

Pour plus d'informations, consultez la section « [Identification des ordinateurs sur Internet](#) » à la page 99.

Pour identifier des ordinateurs à l'aide d'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.

Contrôle des événements de Norton Personal Firewall

Norton Personal Firewall fournit des informations sur ses activités.

- La fenêtre Etat courant comporte plusieurs groupes de compteurs qui vous renseignent sur les activités de navigation et de filtrage en cours.
- Le journal des événements enregistre les actions effectuées par Norton Personal Firewall ainsi que vos activités Internet.
- La fenêtre Statistiques contient les statistiques de l'activité du réseau et des actions effectuées par Norton Personal Firewall.

Vérification de l'état courant

La fenêtre Etat courant est un instantané de l'état de Norton Personal Firewall. Elle fournit des informations sur les éléments suivants :

- Firewall personnel
- Confidentialité

Vérification de l'état du firewall personnel

L'état du firewall personnel fournit des informations sur les attaques récentes subies par votre ordinateur (heure de la dernière attaque et adresse IP de l'ordinateur qui en était à l'origine).

Le firewall personnel est actuellement Activé. Désactiver	
Statistiques (Plus de statistiques...)	
Dernière attaque le : 13/08/2001 17:03:28	
Tentatives d'intrusion récentes :	6
Tentatives de pirate récentes :	1
Pirate le plus fréquent :	165.10.2.1

Pour vérifier l'état du firewall personnel

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Etat Internet > Etat courant**.
- 2 Cliquez sur **Firewall personnel**.

Vérification de l'état de la confidentialité

L'état de la confidentialité indique le nombre de cookies bloqués ou autorisés et le nombre de fois où des informations confidentielles ont été émises ou interceptées.

La fonction de confidentialité est actuellement Activé. Désactiver	
Statistiques (Plus de statistiques...)	
	Bloquée Autorisée
Cookies récents :	Inactif Inactif
Sites ayant créé des cookies récemment :	Inactif Inactif
Sites Web demandant le plus de cookies :	Inactif Inactif
Infos confidentielles bloquées récemment :	0 Aucune

Pour vérifier l'état de la confidentialité

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Etat Internet > Etat courant**.
- 2 Cliquez sur **Confidentialité**.

Configuration de Norton Personal Firewall pour des situations courantes

Norton Personal Firewall peut être configuré pour répondre à vos besoins dans de nombreuses situations. Cette section décrit le paramétrage qui convient à diverses situations courantes.

Utilisation de Norton Personal Firewall avec une connexion par modem

Dès son installation, Norton Personal Firewall est configuré pour protéger les ordinateurs connectés à Internet par l'intermédiaire d'un modem.

Utilisation de Norton Personal Firewall avec une connexion haut débit

Dès son installation, Norton Personal Firewall est configuré pour protéger les ordinateurs connectés à Internet par l'intermédiaire d'un système haut débit (modem câble ou service ADSL).

Le plus important pour être protégé des dangers d'Internet est de ne pas désactiver Norton Personal Firewall. La plupart des connexions haut débit étant actives en permanence, votre ordinateur peut être attaqué à tout moment.

Résolution des problèmes rencontrés avec les connexions haut débit

Voici des problèmes fréquemment rencontrés avec les connexions haut débit :

- Nom NetBIOS obligatoire.
- Analyse régulière de l'ordinateur par le FAI.

Nom NetBIOS obligatoire

Certains systèmes câblés nécessitent que le nom NetBIOS de l'ordinateur soit visible. Le nom NetBIOS est visible, alors que les fichiers et les dossiers de l'ordinateur sont cachés.

Pour rendre visible le nom NetBIOS

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Contrôle d'accès à Internet**.
- 2 Cliquez sur **Configurer** et sélectionnez **Paramètres applicables à l'ensemble du système**.
- 3 Dans la boîte de dialogue, sélectionnez Nom NetBIOS entrant par défaut et cliquez sur **Modifier**.
- 4 Sur l'onglet Action de la boîte de dialogue Modifier, cliquez sur **Autoriser l'accès à Internet**.
- 5 Cliquez sur **OK**.
- 6 Dans la boîte de dialogue Paramètres applicables à l'ensemble du système, cliquez sur **OK**.

Analyse régulière de l'ordinateur par le FAI

Certains systèmes haut débit 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 FAI.

Si cette situation se présente, procédez comme suit pour d'autoriser ces analyses.

Pour autoriser les analyses de port par le FAI

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Protection contre les intrusions**.
- 2 Dans la fenêtre Protection contre les intrusions, cliquez sur **Exclusions**.
- 3 Dans la boîte de dialogue Exclusions, sélectionnez le FAI actuellement bloqué et cliquez sur **Exclure**.
- 4 Cliquez sur **OK**.

Utilisation de Norton Personal Firewall avec des jeux faisant intervenir plusieurs joueurs

Certains jeux faisant intervenir plusieurs joueurs nécessitent un accès spécial à Internet. Si vous rencontrez des problèmes avec un jeu, accordez-lui une autorisation d'accès totale à Internet. Si cette solution ne fonctionne pas, placez temporairement les ordinateurs des autres joueurs dans la zone Approuvés.

Accord de l'accès à Internet à un jeu multi-joueurs

La première étape consiste à donner au jeu l'autorisation d'accéder à Internet.

Pour donner à un jeu multi-joueurs l'autorisation d'accéder à Internet

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Contrôle d'accès à Internet**.
- 2 Cliquez sur **Ajouter**.
- 3 Sélectionnez le fichier exécutable de l'application et cliquez sur **Ouvrir**.
- 4 Dans la fenêtre Contrôle de l'accès à Internet, choisissez **Permettre à <application> d'accéder à Internet**.
- 5 Cliquez sur **OK**.

Remarque : si l'application est déjà répertoriée, cliquez sur l'entrée sous Accès à Internet et choisissez Tout autoriser.

Placement d'autres joueurs dans la zone Approuvés

Si le problème n'est pas résolu en autorisant l'application de jeu à accéder à Internet, placez l'ordinateur des autres joueurs dans la zone Approuvés.

Pour placer d'autres joueurs dans la zone Approuvés

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Contrôle de zone Internet**.
- 2 Dans l'onglet Restreint, cliquez sur **Ajouter**.
- 3 Tapez l'adresse IP des autres joueurs.

Utilisation de Norton Personal Firewall dans un réseau domestique

Norton Personal Firewall vous protège des dangers d'Internet tout en permettant une utilisation complète du réseau local.

Pour votre sécurité, Norton Personal Firewall empêche toute activité réseau lorsqu'il est installé. Cette protection est destinée à empêcher d'autres personnes de se connecter à votre ordinateur par l'intermédiaire d'Internet à l'aide des fonctions Réseau Microsoft.

Activation du partage de fichiers et d'imprimantes

Le réseau Microsoft permet de partager des fichiers et des imprimantes. Vous pouvez activer ces fonctions sur le réseau local, tout en les protégeant d'Internet.

Pour activer le partage de fichiers et d'imprimantes

- 1 Ouvrez l'Explorateur Windows.
- 2 Développez le **Voisinage réseau** ou les **Favoris réseau** pour afficher le nom des ordinateurs du réseau local.
- 3 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Contrôle de zone Internet**.
- 4 Dans l'onglet Restreint, cliquez sur **Ajouter**.
- 5 Ajoutez chaque ordinateur local à la zone Approuvés.

Pour plus d'informations, consultez la section « [Ajout d'ordinateurs aux zones](#) » à la page 68.

Vous pouvez également débloquer le partage de fichiers et d'imprimantes en utilisant les Paramètres applicables à l'ensemble du système.

Pour activer le partage de fichiers et d'imprimantes

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel > Contrôle d'accès à Internet**.
- 2 Cliquez sur **Configurer** et sélectionnez **Paramètres applicables à l'ensemble du système**.
- 3 Dans la boîte de dialogue Paramètres applicables à l'ensemble du système, sélectionnez l'entrée pour le partage de fichiers ou d'imprimantes Windows et cliquez sur **Modifier**.
- 4 Sur l'onglet Action de la boîte de dialogue Modifier, cliquez sur **Autoriser l'accès à Internet**.
- 5 Cliquez sur **OK**.
- 6 Dans la boîte de dialogue Paramètres applicables à l'ensemble du système, cliquez sur **OK**.

Partage de connexion Internet

Norton Personal Firewall fonctionne avec le partage de connexion Internet.

Pour obtenir une protection maximale, installez Norton Personal Firewall sur tous les ordinateurs en réseau. L'installation de Norton Personal Firewall sur l'ordinateur passerelle protège le réseau de la plupart des attaques extérieures ; le réseau n'est cependant pas protégé contre les chevaux de Troie ou d'autres problèmes si le logiciel n'est pas installé sur chaque poste.

Utilisation de Norton Personal Firewall avec un routeur câble/DSL

Norton Personal Firewall fonctionne derrière un routeur câble ou ADSL afin de renforcer la protection fournie par le routeur. Dans certains cas, vous pouvez réduire la protection fournie par le routeur afin d'utiliser des applications telles que NetMeeting ou Microsoft Messenger.

Norton Personal Firewall offre des fonctions qui peuvent ne pas être disponibles sur les routeurs câble ou DSL (protection des informations confidentielles, par exemple).

Utilisation de Norton Personal Firewall avec un réseau d'entreprise

Si vous utilisez votre ordinateur dans le cadre familial et professionnel, vous serez peut-être amené à combiner Norton Personal Firewall avec un firewall d'entreprise.

Activation du partage de fichiers et d'imprimantes

Si vous ne souhaitez pas désactiver Norton Personal Firewall, vous pouvez activer le partage de fichiers et d'imprimantes de sorte que l'ordinateur fonctionne sur le réseau de l'entreprise.

Pour activer le partage de fichiers et d'imprimantes

- 1 Ouvrez l'Explorateur Windows.
- 2 Développez le **Voisinage réseau** ou les **Favoris réseau** pour afficher le nom des ordinateurs du réseau local.
- 3 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Firewall personnel** > **Contrôle de zone Internet**.
- 4 Dans l'onglet Restreint, cliquez sur **Ajouter**.
- 5 Ajoutez chaque ordinateur local à la zone Approuvés.

Pour plus d'informations, consultez la section « [Ajout d'ordinateurs aux zones](#) » à la page 68.

Vous pouvez également débloquer le partage de fichiers et d'imprimantes. Pour plus d'informations, consultez la section « [Pour activer le partage de fichiers et d'imprimantes](#) » à la page 81.

Logiciels d'administration sur les réseaux d'entreprise

Les logiciels d'administration utilisés sur certains réseaux d'entreprise peuvent provoquer des alertes Norton Personal Firewall. Si des alertes inhabituelles surviennent lors de l'utilisation d'un réseau d'entreprise, désactivez Norton Personal Firewall ou consultez l'administrateur du réseau.

Utilisation de Norton Personal Firewall avec un serveur proxy

Norton Personal Firewall fonctionne avec la plupart des serveurs proxy. Vous pouvez toutefois être amené à modifier certains paramètres afin de bénéficier d'une protection totale.

Déterminer si Norton Personal Firewall est compatible avec votre serveur proxy

La première étape est de vérifier si Norton Personal Firewall fonctionne avec votre serveur proxy.

Pour savoir si Norton Personal Firewall est compatible avec votre serveur proxy

- 1 En haut de la fenêtre de Norton Personal Firewall, choisissez **Options**.
- 2 Cliquez sur **Afficher les statistiques**.
- 3 Dans la catégorie Web, consultez le compteur Octets traités.
- 4 Utilisez un navigateur pour vous connecter à un site Web.

Si Norton Personal Firewall effectue un filtrage, le compteur Octets traités de la fenêtre Statistiques augmente quand vous chargez des pages Web. Si le compteur Octets traités reste à 0, Norton Personal Firewall ne contrôle probablement pas le port utilisé par le serveur proxy.

Déterminer le port à surveiller pour les communications HTTP

Si Norton Personal Firewall ne fonctionne pas avec votre serveur proxy, vérifiez le port que ce dernier utilise pour les communications HTTP.

Pour connaître le port à surveiller pour les communications HTTP

- 1 Utilisez un navigateur pour vous connecter à un site Web.
- 2 En haut de la fenêtre de Norton Personal Firewall, choisissez **Options**.
- 3 Cliquez sur **Afficher le journal**.
- 4 Sur l'onglet Connexions, examinez les informations dans la colonne Distant.
Un numéro de port figure à la suite de l'adresse IP du site chargé. Il s'agit du port utilisé pour accéder au serveur proxy en vue d'établir la connexion au Web.
- 5 Notez le numéro du port.

Définition des ports à surveiller pour les communications HTTP

Votre ordinateur peut se connecter à Internet par l'intermédiaire d'un serveur proxy, auquel cas toutes les communications HTTP transitent par le port affecté à ce serveur.

Pour définir les ports à surveiller pour les communications HTTP

- 1 En haut de la fenêtre de Norton Personal Firewall, choisissez **Options**.
- 2 Cliquez sur **Options avancées**.
- 3 Sur l'onglet Autre, effectuez l'une des opérations suivantes :
 - Cliquez sur **Ajouter**, puis tapez le numéro du port à surveiller pour les communications HTTP pour ajouter un port à la Liste des ports HTTP.
 - Cliquez sur le numéro du port dans la liste des ports HTTP, puis cliquez sur **Supprimer** pour supprimer un port de la liste.

Exécution d'un serveur Web avec Norton Personal Firewall

S'il est correctement configuré, Norton Personal Firewall ne vous empêchera pas d'exécuter un serveur Web.

Pour permettre à un serveur Web de fonctionner derrière Norton Personal Firewall, vous devez créer une règle autorisant les connexions TCP entrantes sur le port 80.

Pour configurer Norton Personal Firewall pour un serveur Web

- 1 Consultez le site Web en tapant l'adresse IP dans la barre d'adresses du navigateur.
Norton Personal Firewall affiche une alerte Contrôle de l'accès à Internet.
- 2 Dans la boîte de dialogue de l'alerte, cliquez sur **Configurer l'accès à Internet automatiquement**.

Exécution d'un serveur FTP avec Norton Personal Firewall

Pour permettre à un serveur FTP de s'exécuter derrière Norton Personal Firewall, vous devez créer les règles suivantes :

- une règle permettant les connexions TCP entrantes sur le port 21 ;
- une règle permettant les connexions TCP sortantes sur le port 22 ;
- une règle permettant les connexions TCP entrantes sur les ports 1024 à 5000.

Pour configurer Norton Personal Firewall pour un serveur FTP

- 1 Affichez le site FTP en tapant l'adresse **FTP://** suivie de l'adresse IP du serveur FTP dans la barre d'adresses du navigateur.

Norton Personal Firewall affiche une alerte Contrôle de l'accès à Internet.

- 2 Dans la boîte de dialogue de l'alerte, cliquez sur **Configurer l'accès à Internet pour cette application**.

Pour plus d'informations, consultez la section « [Réponse aux alertes de contrôle d'accès à Internet](#) » à la page 50.

Utilisation de Norton Personal Firewall avec DHCP

Si l'adresse IP de votre ordinateur est fixée par un serveur DHCP qui fournit une adresse IP différente à chaque fois, soyez prudent lorsque vous tapez les adresses locales dans les règles.

Au lieu de taper une seule adresse IP, qui peut changer à tout moment, tapez une adresse réseau à l'aide d'une adresse IP de base et d'un masque de sous-réseau. Tapez des valeurs couvrant une plage d'adresses qui peuvent être attribuées à l'ordinateur.

Pour plus d'informations, consultez la section « [Identification d'ordinateurs dans Norton Personal Firewall](#) » à la page 72.

Utilisation de Norton Personal Firewall avec pcAnywhere

Vous ne devriez pas rencontrer de problèmes avec pcAnywhere utilisé comme client ou hôte et Norton Personal Firewall. La première fois que vous l'exécutez, ou au cours de l'analyse des applications, Norton Personal Firewall identifie pcAnywhere et crée automatiquement des règles d'accès Internet.

Pour bénéficier d'une protection maximale, modifiez la règle pour limiter son utilisation aux seuls ordinateurs que vous utilisez avec l'hôte pcAnywhere. Cette précaution, combinée aux mots de passe pcAnywhere, offre un niveau de protection optimal.

Utilisation de Norton Personal Firewall avec un réseau virtuel (VPN)

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

- Nortel
- VPNRemote
- PGP
- SecureRemote

Avec la plupart des réseaux privés virtuels, vous ne pouvez pas voir Internet ou les autres ordinateurs du réseau local lorsque le client VPN est actif. Vous pouvez uniquement voir les ordinateurs disponibles par l'intermédiaire du serveur VPN auquel vous êtes connecté.



Dépannage

Cette section permet de résoudre de nombreux problèmes courants. Si vous ne trouvez pas la solution à votre problème dans cette section, reportez-vous aux autres sections de ce document.

Pour plus d'informations, consultez la section « [Configuration de Norton Personal Firewall pour des situations courantes](#) » à la page 77.

Résolution des problèmes de Norton Personal Firewall

Vous trouverez ci-après des solutions à des problèmes qui peuvent survenir dans Norton Personal Firewall.

Quel est le problème lié à ce site Web ?

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

Pour déterminer si Norton Personal Firewall bloque l'accès à un site Web, désactivez-le et essayez à nouveau de vous connecter à ce site. Gardez à l'esprit que lorsque vous désactivez Norton Personal Firewall, vous désactivez également sa protection, notamment en ce qui concerne le blocage de l'envoi d'informations personnelles et la réception d'informations inappropriées.

Pour plus d'informations, consultez la section « [Désactivation temporaire de Norton Personal Firewall](#) » à la page 28.

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

Il peut s'agir d'un blocage des cookies.

De nombreux sites Web nécessitent, pour s'afficher correctement, que les cookies soient activés sur l'ordinateur. Si le blocage des cookies est activé et que la page Web est vide, désactivez le blocage des cookies et essayez de nouveau d'afficher la page.

Pour désactiver le blocage des cookies

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Personnaliser**.
- 3 Choisissez l'option Moyen ou Aucun dans la liste **Blocage des cookies**.

Si le problème est résolu, vous pouvez envisager de définir des paramètres spécifiques au site afin d'autoriser les cookies en provenance de ce site.

Il peut s'agir d'une règle de firewall.

Une règle de firewall peut bloquer le site Web. Si c'est le cas, vous verrez probablement un message indiquant que la connexion n'a pu être établie. Vous pouvez afficher les règles de firewall qui ont été configurées et déterminer si l'une d'entre elles bloque le site.

Il peut s'agir d'un 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.

Pour plus d'informations, consultez la section « [Définition des niveaux de sécurité pour les applets Java et les contrôles ActiveX](#) » à la page 62.

Si le problème est résolu, vous pouvez envisager de définir des paramètres spécifiques au site afin d'autoriser les contrôles ActiveX ou les applets Java en provenance de ce site.

Il peut s'agir d'un blocage des scripts.

Certains sites Web utilisent du code JavaScript dans leurs contrôles de navigation et à d'autres endroits. Si Norton Personal Firewall bloque les scripts JavaScript ou VBScript, ces sites Web peuvent ne plus fonctionner correctement.

Pour débloquer les scripts JavaScript ou VBScript

- 1 En haut de la fenêtre de Norton Personal Firewall, choisissez **Options**.
- 2 Cliquez sur **Options avancées**.
- 3 Sur l'onglet Navigation, cliquez sur l'onglet **Contenus actifs**.
- 4 Dans la liste des sites Web, effectuez l'une des opérations suivantes :
 - Sélectionnez le site Web à modifier.
 - Cliquez sur **(Par défaut)** pour modifier tous les sites Web non référencés.
- 5 Dans la zone Scripts, sélectionnez l'option **Autoriser l'exécution de tous les scripts**.

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

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

Pour vérifier les informations dans la liste Informations confidentielles

- 1 Dans la partie gauche de la fenêtre Norton Personal Firewall, cliquez sur **Confidentialité**.
- 2 Cliquez sur **Infos confidentielles**.

Cette action a pour effet d'ouvrir la liste des informations dont la transmission à Internet est bloquée.

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

Si le contrôle automatique d'accès à Internet est activé, Norton Personal Firewall crée des règles pour les applications reconnues, sans vous envoyer d'avertissement. Vous pouvez désactiver le contrôle automatique d'accès à Internet.

Pour plus d'informations, consultez la section « [Activation du contrôle automatique d'accès à Internet](#) » à la page 65.

Pour plus d'informations, consultez la section « [Paramétrage du niveau de détail des informations](#) » à la page 56.

Pourquoi mon réseau local ne fonctionne-t-il plus ?

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

Pour autoriser l'utilisation du réseau local, notamment le partage de fichiers et d'imprimantes, placez les ordinateurs du réseau dans la zone approuvée ou débloquez l'accès avec les Paramètres applicables à l'ensemble du système.

Pour plus d'informations, consultez la section « [Ajout d'ordinateurs du réseau domestique à la zone Approuvés](#) » à la page 68.

Pour plus d'informations, consultez la section « [Utilisation de Norton Personal Firewall dans un réseau domestique](#) » à la page 80.

Pourquoi ne puis-je pas utiliser une imprimante partagée ?

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

Pour autoriser l'utilisation du réseau local, incluant notamment le partage d'imprimantes, placez les ordinateurs du réseau dans la zone approuvée.

Pour plus d'informations, consultez la section « [Ajout d'ordinateurs du réseau domestique à la zone Approuvés](#) » à la page 68.

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

Les paramètres Confidentialité de navigation empêchent le navigateur de transmettre des informations sur lui-même. Toutefois, certains sites de diagnostic sur Internet peuvent accéder aux informations sur le navigateur, même si le paramètre Confidentialité de navigation a été activé pour les bloquer.

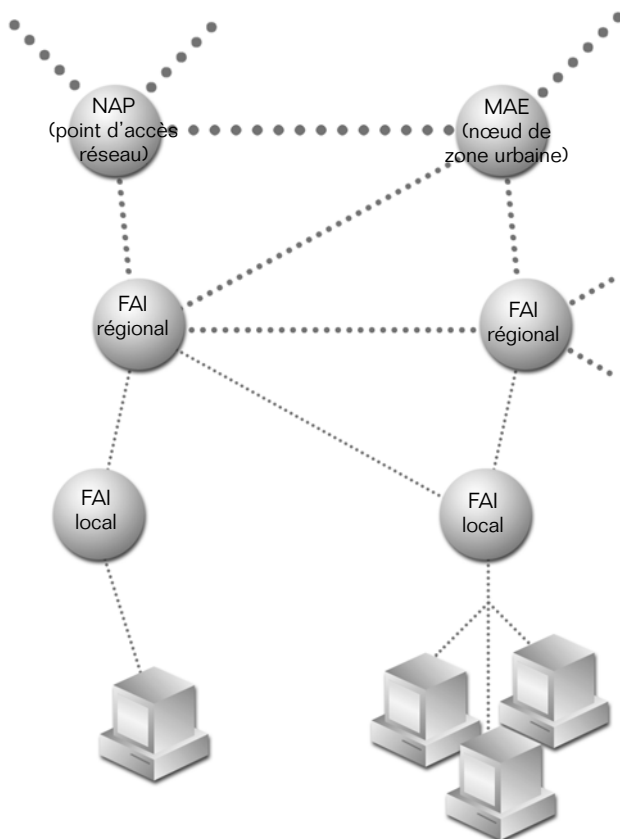
- Si vous n'avez pas bloqué les applets Java, les contrôles ActiveX ou les scripts, il est possible que le site utilise l'une de ces méthodes pour lire ces informations.

Pour plus d'informations, consultez la section « [Définition des niveaux de sécurité pour les applets Java et les contrôles ActiveX](#) » à la page 62.

- Parfois, lorsque des serveurs Web n'accèdent pas aux informations sur le navigateur, ils n'utilisent que 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

Internet est l'interconnexion de millions d'ordinateurs à travers le monde. Il comprend tous les ordinateurs et 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. Des échanges, appelés NAP (Network Access Point - point d'accès réseau) et MAE (Metropolitan Area Exchanges - nœud de zone urbaine) interviennent sur ces axes. Il existe également des « autoroutes régionales », fournies par de grands FAI et des « rues » établies par des FAI locaux.

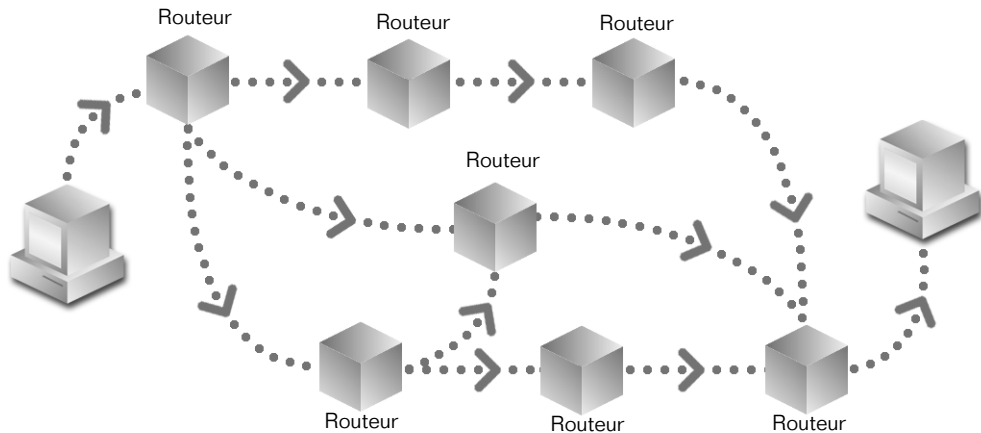
Tout comme un système de routes et d'autoroutes, Internet fournit plusieurs itinéraires pour aller d'un point à un autre. Si une partie d'Internet est encombrée ou endommagée, les informations sont redirigées sur un autre itinéraire.

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 ensemble. 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 l'adresse 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 leurs destinations. Chaque paquet peut suivre un itinéraire différent sur Internet et peut être divisé 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.



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.

TCP/IP

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

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 et la retransmission des paquets perdus.

Du point de l'importance pour la navigation sur Internet, UDP occupe le deuxième rang après TCP.

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 délais et pour faciliter le dépannage.

Norton Personal Firewall accepte normalement certains 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.

IGMP

Le protocole IGMP (Internet Group Membership Protocol) permet d'établir des appartenances à des groupes de multidiffusion. 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 Personal Firewall vous permet néanmoins de le bloquer totalement. Vous pouvez le bloquer si aucune de vos applications ne nécessite IGMP. Si vous avez des problèmes de réception d'informations de multidiffusion, par exemple de séquences vidéo ou de présentations PowerPoint, vérifiez que le protocole IGMP n'est pas bloqué.

Les informations du Web sont stockées 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.com` est un URL.

Chaque URL correspond à l'adresse IP de l'ordinateur qui stocke la page Web. Les URL sont utilisés car ils sont plus faciles à mémoriser que les adresses IP.

Avant de demander une page, votre navigateur demande à un serveur DNS (Domain Name 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 a une adresse IP distincte.

Demande d'une page

Une fois que le navigateur dispose de l'adresse IP, il établit une *connexion* 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 récents utilisent le protocole HTTP 1.1 (Hypertext Transfer Protocol version 1.1) et établissent des connexions pouvant transmettre plusieurs fichiers et rester ouvertes pour plusieurs pages.

Parties d'un URL

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

<code>http://</code>	<i>Protocole d'application</i> utilisé pour établir la connexion. Le protocole le plus couramment utilisé pour naviguer sur le Web est <code>http</code> . Si vous n'indiquez pas de protocole d'application, votre navigateur utilise par défaut le protocole <code>http</code> . Les autres protocoles couramment utilisés incluent <code>ftp</code> et <code>gopher</code> .
<code>.com</code>	<i>Domaine racine</i> ou <i>domaine de premier niveau</i> . Il existe plusieurs domaines racine courants, notamment <code>.com</code> , <code>.net</code> , <code>.edu</code> , <code>.org</code> , <code>.mil</code> et <code>.gov</code> . Il existe également des domaines racine de deux lettres pour la plupart des pays, par exemple, <code>.fr</code> pour la France, <code>.ca</code> pour le Canada et <code>.uk</code> pour le Royaume-Uni.
<code>symantec.com</code>	<i>Domaine</i> . 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.
<code>www.symantec.com</code>	<i>Hôte</i> . Site Web spécifique avec lequel le navigateur communique. Il s'agit également du nom pour lequel le serveur DNS fournit l'adresse IP.
<code>securitycheck</code>	<i>Dossier</i> ou répertoire qui contient le fichier à afficher.
<code>index.html</code>	<i>Nom du fichier</i> à afficher.

Une URL spécifique, *localhost*, identifie votre ordinateur pour lui-même. Si vous disposez d'un serveur Web sur votre ordinateur, vous pouvez taper `http://localhost` pour afficher votre page Web. L'adresse IP qui correspond à `localhost` est `127.0.0.1`.

Ports identifiant des applications sur un serveur

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

Les termes *serveur* et *service* sont souvent synonymes. Par exemple, un serveur Web fournit le service HTTP, et on dit souvent qu'un ordinateur exécute le service *Finger*.

Les ports sont numérotés de 1 à 65535. Les ports 1 à 1023 sont dits *Ports connus* et sont les ports par défaut pour de nombreuses applications Internet.

Les *ports* sont une partie rarement affichée de l'URL. 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.

Ports connus

Voici quelques-uns des ports connus les plus courants :

Port par défaut	Nom de service	Application
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
80	http	Protocole HTTP (Hypertext Transfer Protocol)
110	pop3	Protocole 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	nbssession	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 (Secure HTTP)

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 tenter de les identifier individuellement. Les *masques de sous-réseau* permettent d'identifier un groupe d'ordinateurs liés, par exemple ceux de votre réseau local.

Un masque de sous-réseau standard se présente comme suit : 255.255.255.0. Dans la forme la plus simple, chaque 255 indique des parties de l'adresse IP qui sont les mêmes pour tous les ordinateurs du sous-réseau, alors que les 0 indiquent les parties de l'adresse IP qui sont différentes.

Les masques de sous-réseau sont toujours utilisés en conjonction avec une adresse IP de base.

Par exemple :

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. 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 Personal Firewall vous protège contre les risques majeurs liés à Internet. Ces risques incluent la menace d'une attaque de pirate, le code malveillant dans un contenu actif, l'exposition à un contenu inopportun, la divulgation d'informations privées et la contamination par des virus provenant de fichiers infectés.

Risques liés aux pirates

A l'origine, le terme de *hacker* faisait référence à quelqu'un capable de résoudre des problèmes informatiques et d'écrire des programmes rapidement et élégamment. La signification de ce terme a toutefois changé et désigne une personne qui utilise ses connaissances en informatique à des fins illicites. Le mot *hacker* ayant au départ une connotation positive, certains utilisent le terme *cracker* avec une connotation péjorative. Dans ce guide, le terme de pirate a sa signification normale, sans connotation positive.

D'autres mots anglais sont couramment employés pour désigner les pirates, comme *script-kiddies*, *wannabes*, *packet monkeys* et *cyberpunks*. Ils s'appliquent tous à des pirates en herbe qui utilisent des applications écrites par des pirates plus avancée 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 élargit son accès à 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 de messagerie 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. La plupart de ces ressources sont licites, comme InterNic, organisation qui gère la base de données Whois répertoriant tous les noms de domaine enregistrés. Il existe également des outils intégrés, comme Sam Spade qui fournit plus de 20 outils différents pour rechercher et analyser des informations Internet.

Ces outils permettent aux pirates d'en apprendre beaucoup sur une cible potentielle. Avec un nom de domaine, il est facile d'utiliser la base de données Whois pour rechercher 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 d'autres informations. Il est plus facile d'appeler une société en se faisant passer pour un administrateur réseau et de demander un mot de passe que d'attaquer directement le réseau.

Si un pirate n'a pas de cible précise, de nombreux outils permettent d'analyser Internet afin de 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. Les réponses indiquent au pirate qu'un ordinateur existe aux adresses IP correspondantes. Lorsque Norton Personal Firewall est en cours d'exécution, votre ordinateur est masqué et ne peut être atteint par des 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 complète, 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 Personal Firewall 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, la fonctionnalité de réseau Microsoft est activée afin que les personnes sur le réseau puissent s'y connecter.

La fonction de réseau NetBIOS de Microsoft utilise trois des ports connus. Ces ports sont utilisés pour établir des connexions entre des ordinateurs sur 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 sur Internet. Norton Personal Firewall 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 Personal Firewall continue à vous protéger contre les risques liés à Internet tout en vous permettant d'utiliser votre réseau local.

Pour plus d'informations, consultez la section « [Ports connus](#) » à la page 98.

Pour plus d'informations, consultez la section « [Utilisation de Norton Personal Firewall dans un réseau domestique](#) » à la page 80.

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 des ordinateurs équipés de Windows 95, Windows 98 ou Windows 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 des ordinateurs équipés de Windows NT ou de Windows 2000, le pirate va tenter d'obtenir des droits administratifs sur l'ordinateur. La clé pour obtenir ces droits est généralement un mot de passe. Au lieu d'essayer de deviner le mot de passe, le pirate peut télécharger le fichier de mots de passe et l'analyser.

Une autre tactique consiste à placer un programme de *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 le faire fonctionner, il peut totalement contrôler l'ordinateur.

D'autres chevaux de Troie peuvent enregistrer toutes les séquences de touches afin de capturer les mots de passe et d'autres données stratégiques. Norton Personal Firewall 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 ne pouvez pas agir pour l'arrêter.

Sous Windows NT et Windows 2000, les pirates tentent de désactiver les fonctions d'audit et de modifier ou d'effacer les journaux d'événements. Sur tout ordinateur, le pirate peut cacher des fichiers afin de les avoir à disposition lors de visites ultérieures. Dans des cas extrêmes, le 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 considérés comme des *contenus actifs* car ils peuvent faire plus qu'afficher du texte ou des 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 ces certificats numériques pose un certain nombre de problèmes. Certains contrôles ne sont pas accompagnés de certificats et certains certificats fournissent très peu d'informations sur les fonctions du contrôle.

Java a été conçu à l'origine pour être sûr lors d'une exécution dans un navigateur. Le *sandbox* Java a été conçu pour éviter que des applets Java ne puissent sortir du navigateur et endommager l'ordinateur. Toutefois, les pirates et les experts en sécurité trouvent sans cesse des moyens de contourner les protections Java et de détourner les fonctionnalités Java de l'utilisation prévue par leurs développeurs.

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 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 des sites Web des informations sur l'utilisation que vous faites de votre ordinateur, sans votre autorisation.

Envoi d'informations confidentielles

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

Bons et mauvais cookies

Les cookies sont des messages envoyés à votre navigateur par un site Web qui sont stockés sous la forme de petits fichiers sur votre ordinateur. Ils sont souvent utilisés par des sites Web pour assurer le suivi de vos visites. Dans la plupart des cas, le fichier de cookie ne contient pas d'informations personnelles et stocke uniquement un identificateur qui permet de vous identifier auprès d'un site Web.

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 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 directement du site 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 effectuer le suivi de votre utilisation du Web sur une large gamme de sites.

Blocage des cookies

Norton Personal Firewall 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 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 Personal Firewall peut également bloquer ou autoriser les cookies issus de domaines ou de sites Web spécifiques.

Suivi de l'utilisation d'Internet

Lorsque vous utilisez Internet, la plupart des navigateurs transmettent plusieurs bits d'informations que vous jugez peut-être confidentielles. Un élément généralement transmis par votre navigateur aux sites Web est l'URL de la page dont vous provenez. Ces informations sont utilisées par certains sites Web pour vous aider à visiter le site, mais elles peuvent également servir à identifier le site Web dont vous arrivez. En d'autres termes, elles peuvent être utilisées pour suivre votre utilisation du Web. Norton Personal Firewall bloque ces informations.

Votre navigateur envoie également des informations sur lui-même et sur le système d'exploitation utilisé. Norton Personal Firewall 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 à un site Web. On a découvert que plusieurs programmes dont la fonction est de vous aider à télécharger et à installer des fichiers, donnent des informations sur vos activités sur Internet. Norton Personal Firewall préserve votre vie privée en bloquant 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. De plus, le risque ne se limite pas aux virus, il est également constitué par les chevaux de Troie, les *vers* et les *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 document reçu par courrier électronique.

Un cheval de Troie est un programme qui ne se duplique pas, mais qui provoque des dommages ou menace la sécurité de l'ordinateur. Généralement, il vous est envoyé par courrier électronique par une personne, mais ne s'envoie pas automatiquement. 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 implanté secrètement qui sommeille sur un ordinateur. Il se réveille ultérieurement, lors d'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 Personal Firewall 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. Quelle est la probabilité que votre ordinateur personnel fasse l'objet d'une attaque ?

La probabilité qu'un pirate isole votre ordinateur en particulier parmi tous ceux connectés à Internet est certainement très faible. Toutefois, des pirates néophytes employant des outils permettant de sélectionner des cibles peuvent analyser relativement fréquemment votre ordinateur à la recherche de failles. Plus les failles sont nombreuses, plus votre ordinateur devient tentant pour le pirate.

Les outils permettant de trouver des cibles vulnérables sont capables d'analyser de très grands groupes d'ordinateurs sur Internet. Le pirate doit simplement indiquer une plage d'adresses IP et cliquer sur OK. 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 Personal Firewall vous protège contre ces analyses en rendant votre ordinateur pratiquement invisible. Votre ordinateur ne répond pas à la plupart des requêtes envoyées par ces programmes d'analyse. Votre ordinateur présente ainsi très peu de failles (ou même aucune) au pirate et devient ainsi une mauvaise cible.

G L O S S A I R E

Ce glossaire fournit la définition de termes Internet couramment utilisés.

ActiveX, contrôles	Programmes conçus pour fonctionner sur Internet. Comme les contrôles ActiveX ne s'exécutent pas dans un environnement restreint (à la différence des applets Java), ils peuvent être utilisés pour prendre le contrôle d'un ordinateur. Les pirates peuvent exploiter cette fonctionnalité pour dérober ou détruire des données ou des logiciels du système.
adresse réseau	Partie d'une adresse IP commune à tous les ordinateurs d'un réseau ou sous-réseau spécifique.
analyse de port	Tentative d'accès à un ordinateur par recherche des ports ouverts. Tentative généralement effectuée 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. Ils peuvent cependant être également utilisés à des fins malveillantes, par exemple pour dérober des mots de passe.
bannière publicitaire	Graphique publicitaire qui apparaît en haut d'une page Web et qui contient souvent un lien vers le site Web de publicité.

- cache** Emplacement du disque dur où des données sont stockées en vue de leur réutilisation. Un cache de navigateur Web stocke des pages Web et des fichiers (des graphiques, par exemple) à mesure que vous les visualisez. Les pages Web que vous visitez fréquemment ou que vous avez déjà visualisées sont ainsi affichées plus rapidement, car le navigateur les ouvre à partir de votre disque dur, et non du Web.
- champ URL source** Informations incluses dans une demande de données, qui indiquent à un serveur le site affiché lors de l'émission de la demande. Les champs URL source permettent aux serveurs Web de déterminer les emplacements que vous avez visités sur Internet.
- Lorsque vous choisissez de bloquer les champs URL source, les informations concernant la page en cours de consultation ne sont pas transmises. Lorsque le navigateur se connecte à un nouveau serveur Web, tout se passe comme si vous veniez de taper l'URL dans le navigateur ou de la sélectionner parmi vos signets.
- cheval de Troie** Programme qui se fait passer pour un programme licite et qui peut causer des dommages à un ordinateur.
- Un cheval de Troie ne se duplique pas, mais endommage ou menace la sécurité de l'ordinateur. Généralement, il vous est envoyé par courrier électronique par une personne, mais ne s'envoie pas automatiquement. Un cheval de Troie peut arriver déguisé sous la forme d'un logiciel 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 aux pirates des capacités de contrôle à distance.

communication entrante	Tentative d'un ordinateur externe visant à 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 un ordinateur pour établir une connexion avec un ordinateur distant. La connexion peut être utilisée pour envoyer des données vers ou depuis l'ordinateur.
connexion	Méthode d'échange de données qui permet un transfert fiable entre deux ordinateurs.
connexion entrante	Connexion établie par un ordinateur distant avec votre ordinateur.
Contenus actifs	Contenu d'une page Web qui fait l'objet de mises à jour régulières ou qui se modifie en réponse à une action de l'utilisateur. Il peut s'agir, par exemple, de cartes météo ou de cotations boursières. Les contenus actifs sont mis en œuvre par l'intermédiaire de contrôles ActiveX, de scripts VB, de scripts Java et d'applets Java dans le code HTML qui définit la page.
cookie	Informations stockées par des serveurs Web sur votre ordinateur, en vue de les récupérer lors de votre connexion suivante au site. 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. Les cookies sont souvent utilisés pour stocker les éléments que vous placez dans votre « panier » sur un site marchand. Toutefois, ils peuvent également être utilisés pour déterminer quand vous visitez un site et quelles pages vous affichez. Ces informations peuvent ensuite être transmises à d'autres serveurs Web, par exemple des serveurs de publicité.

courrier électronique	Courrier électronique. Méthode d'échange de messages et de fichiers avec d'autres personnes par l'intermédiaire des réseaux informatiques. Le protocole SMTP (Simple Mail Transfer Protocol) est couramment utilisé pour envoyer des messages électroniques. Les protocoles courants 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 des courriers électroniques.
cracker	Personne qui effectue des tentatives d'accès non autorisé sur des ordinateurs dans le but de rassembler des informations sur ces ordinateurs ou de les endommager.
cyberpunk	Personne qui effectue des tentatives d'accès non autorisé sur des ordinateurs dans le but de rassembler des informations sur ces ordinateurs ou de les endommager. Ce type de pirate utilise généralement des applications écrites par d'autres pour attaquer des ordinateurs sur Internet.
DHCP	Dynamic Host Configuration Protocol. Le protocole DHCP attribue automatiquement une adresse IP temporaire à chaque périphérique du réseau.
DNS	Domain Name System. Système d'attribution de noms hiérarchique qui établit les relations entre les noms de domaine (comme www.symantec.com) et les adresses IP correspondantes (comme 206.204.212.71).
domaine	Sur Internet, adresse commune d'une société ou d'une organisation (comme symantec.com), 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 emplacement géographique de l'adresse (par exemple .fr pour la France, .ca pour le Canada ou .uk pour le Royaume-Uni).
écho	Opération consistant à retransmettre immédiatement à la source chaque caractère reçu par un ordinateur et à fournir ainsi un accusé de réception. Les protocoles TCP et UDP utilisent le port 7 à cet effet.
empreinte digitale	Signature numérique cryptée servant à identifier une version d'application spécifique. Utilisée par le contrôle automatique d'accès à Internet pour garantir de ne créer de règles que pour les applications connues.
finger	Dans certains systèmes d'exploitation, commande qui demande des informations de compte d'utilisateur réseau.
firewall	Système de sécurité qui utilise des règles pour bloquer ou autoriser des connexions et des transmissions de données entre votre ordinateur et Internet.
fragment	Paquet IP qui peut être divisé en deux parties (ou fragments) ou davantage. 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.
FSI	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 sites Web.

FTP	File Transfer Protocol. Protocole standard pour la copie de fichiers à destination et en provenance d'ordinateurs distants sur des réseaux TCP/IP, comme Internet. Le protocole FTP utilise les ports 20 et 21. Il est largement utilisé pour télécharger des programmes ou d'autres fichiers sur un ordinateur à partir d'autres serveurs. Il permet également de charger des fichiers de page Web sur votre propre site Web.
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.
HTTP	HyperText Transfer Protocol. Ensemble de règles permettant de demander des pages à un serveur Web et de transmettre des pages (notamment du texte, des images, des fichiers son et vidéo et d'autres fichiers multimédia) au navigateur Web à l'origine de la demande. HTTP est le protocole d'application le plus répandu sur le World Wide Web. Il utilise le port TCP 80.
HTTPS	HyperText Transfer Protocol Secure. Variante du protocole HTTP qui utilise le cryptage pour une transmission sécurisée des données. Il utilise le port TCP 443.
ICMP	Internet Control Message Protocol. Protocole utilisé sur Internet pour signaler les erreurs, fournir des conseils de routage limité et des services de bas niveau simples sur les réseaux TCP/IP. Certains outils de dépannage IP, comme Ping et Traceroute, utilisent le protocole ICMP.

identification	Service qui fournit des informations sur les utilisateurs à un autre système. Egalement connu sous le nom IDENT, Authentication ou AUTH. Certains serveurs de messagerie, serveurs de groupes de discussion et serveurs IRC utilisent ce service pour vérifier votre identité avant d'autoriser votre accès. Le service d'identification utilise le port TCP 113.
IGMP	Internet Group Membership Protocol. Protocole utilisé pour établir des appartenances à des groupes de multidiffusion.
Internet	Ensemble de réseaux et de passerelles (y compris ARPANET et NSFnet) qui utilisent la suite de protocoles TCP/IP et fonctionnent comme un réseau virtuel collectif unique.
intranet	Réseau interne à une organisation qui utilise les protocoles TCP/IP et d'autres technologies Internet. Il peut inclure plusieurs réseaux locaux (LAN) reliés entre eux, mais aussi des lignes spécialisées d'un réseau étendu (WAN). La fonction d'un intranet est de permettre le partage des informations et des ressources informatiques d'une entreprise entre tous ses employés.
IP	Internet Protocol. Protocole dominant utilisé pour transmettre des données d'un ordinateur à un autre sur Internet. Le protocole IP achemine les paquets vers les destinations appropriées.
IP, adresse	Adresse Internet Protocol. Adresse numérique sur 32 bits attribuée aux hôtes qui utilisent le protocole TCP/IP. L'adresse de chaque hôte doit être unique sur le réseau. Les adresses IP se présentent généralement sous la forme de quatre nombres décimaux, compris entre 0 et 255 et séparés par des points. Par exemple 206.204.52.71.

JavaScript	Langage de création de script similaire à Java, mais offrant moins de fonctionnalités. Le code JavaScript peut être inclus dans des pages Web pour ajouter une interactivité et d'autres fonctionnalités.
journal	Liste d'événements relatifs à l'activité du réseau.
local	Terme qui fait référence à votre ordinateur (par opposition à un ordinateur distant).
masque d'adresse	Technique utilisée pour sélectionner une partie d'une adresse Internet afin de créer une adresse de sous-réseau. Les masques sont souvent utilisés pour identifier une plage d'adresses.
masque de sous-réseau	Code, sous forme d'adresse IP, utilisé par les ordinateurs pour déterminer les parties d'une adresse IP qui identifient le sous-réseau (c'est-à-dire les parties communes à tous les ordinateurs du sous-réseau) et les parties qui identifient un ordinateur spécifique de ce sous-réseau.
masquer	Donner l'impression qu'un élément n'existe pas. Ne pas répondre aux demandes d'informations.
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 afin de s'identifier auprès d'un réseau ou d'un programme. Les mots de passe les plus sûrs sont les mots de passe difficiles à deviner ou introuvables 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 en adresses Internet IP des adresses IP utilisées sur un intranet ou un réseau local. Cette méthode permet le partage d'une adresse Internet IP entre plusieurs ordinateurs. De plus, elle permet de masquer les adresses IP des ordinateurs du réseau. La fonction de partage des connexions Internet (ICS - Internet Connection Sharing) incluse avec les versions récentes de Windows utilise la conversion NAT.

Navigateur Web

Application qui facilite la navigation sur Internet en fournissant une interface utilisateur graphique. L'utilisateur dispose de menus, d'icônes ou de boutons et n'est pas contraint d'assimiler des commandes compliquées. Egalement appelé client Web.

Parmi les navigateurs les plus utilisés, citons Microsoft Internet Explorer et Netscape Navigator.

NetBEUI

NetBIOS Extended User Interface. Mise en œuvre du protocole de transport NetBIOS disponible avec le Client pour les réseaux Microsoft. Protocole réseau qui permet à des ordinateurs de communiquer au sein d'un réseau local.

NetBIOS

Network Basic Input Output System. Spécification d'interface pour les réseaux locaux qui est utilisée avec le Client pour les réseaux Microsoft et d'autres systèmes d'exploitation réseau. Les applications utilisent NetBIOS pour les communications client/serveur ou point à point en vue du partage de fichiers et d'imprimantes. Ce protocole peut être transporté par TCP et UDP.

NNTP

Network News Transfer Protocol. Protocole utilisé par les serveurs de groupes de discussion et les lecteurs de groupes de discussion pour la gestion des messages publiés dans les groupes de discussion Usenet. NNTP utilise le port 119.

nom d'hôte	Nom qui identifie un ordinateur sur un réseau. Par exemple, <code>www.symantec.com</code> est le nom d'hôte du site Web de Symantec. Les noms d'hôte sont traduits en adresses IP par le serveur DNS.
nom de domaine	Situe une organisation ou une autre entité sur Internet. Par exemple, le nom de domaine <code>www.symantec.com</code> représente l'adresse Internet d'un nom de domaine, où <code>symantec.com</code> désigne le domaine et <code>www</code> le serveur hôte. La chaîne <code>www.symantec.com</code> constitue un nom de domaine complet.
NTP	Network Time Protocol. Protocole utilisé pour les services qui fournissent l'heure. NTP utilise le port 123.
numéro de port	Canal de communication logique devant être 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, HTTP utilise le port 80), mais ces numéros restent configurables. Les numéros de port sont toujours ajoutés aux adresses IP lors de l'établissement des connexions aux ordinateurs hôtes, mais la plupart des applications ne les affichent pas.
packet monkey	Personne qui effectue des tentatives d'accès non autorisé sur des ordinateurs dans le but de rassembler des informations sur ces ordinateurs ou de les endommager. Ce type de pirate utilise généralement des applications écrites par d'autres pour attaquer des ordinateurs sur Internet.
page Web	Document unique sur le World Wide Web qui est défini par une adresse unique ou URL. Une page Web peut contenir du texte, des liens hypertexte et des graphiques.

paquet	<p>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.</p> <p>Lorsqu'un fichier quelconque (message électronique, fichier HTML ou GIF, demande d'URL, etc.) est transmis d'un endroit à un autre sur Internet, la couche TCP (Transmission Control Protocol) de TCP/IP divise le fichier en morceaux (paquets). Chaque paquet contient l'adresse Internet de destination. Les divers paquets constituant un fichier peuvent suivre des itinéraires différents sur Internet ; une fois qu'ils sont tous arrivés, ils sont réassemblés par la couche TCP côté réception pour reconstituer le fichier d'origine.</p>
paquet entrant	Paquet de données qui arrive sur votre ordinateur en provenance d'un ordinateur distant ou d'un réseau.
partage de fichiers et d'imprimantes pour les réseaux Microsoft	Service qui permet le partage de fichiers et d'imprimantes par l'intermédiaire d'une connexion réseau. Le partage de fichiers et d'imprimantes pour les réseaux Microsoft utilise les ports UDP 137 et 138 et le port TCP 139. Si vous bloquez le port TCP 139, aucune ressource partagée n'est autorisée.
ping	Abréviation de « Packet Internet Groper ». Fonction qui teste les communications entre deux ordinateurs en envoyant une demande et en recevant une réponse.
pirate	Personne qui effectue des tentatives d'accès non autorisé sur des ordinateurs dans le but de rassembler des informations sur ces ordinateurs ou de les endommager.
POP3	Post Office Protocol, version 3. Protocole utilisé pour transmettre les messages électroniques. POP3 utilise le port TCP 110.

port	<p>Identification utilisateur de transport utilisée par un programme client pour indiquer un programme serveur particulier sur un ordinateur. Egalement appelé service.</p> <p>Les applications de plus haut niveau qui utilisent TCP/IP, notamment le protocole Web HTTP, ont des numéros de port prédéfinis. Pour les autres processus applicatifs, les numéros de port sont 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.</p>
port serveur « non à l'écoute »	<p>Port auquel aucun service n'est lié. Lorsqu'un service (programme serveur) démarre, il se rattache à un numéro de port défini qu'il utilise ensuite pour communiquer avec le réseau.</p>
ports connus	<p>Ports compris dans la plage numérique 0 à 1 023, associés à des applications selon les conventions Internet.</p>
PPP	<p>Point-to-Point Protocol. Méthode de connexion à Internet par liaison à distance.</p>
protocole	<p>Ensemble de règles pour communiquer sur un réseau. Les deux extrémités doivent reconnaître et respecter le même protocole.</p> <p>Les communications Internet reposent sur plusieurs protocoles, notamment :</p> <p>TCP (Transmission Control Protocol) : ensemble de règles pour l'échange de messages avec d'autres points Internet au niveau paquet d'informations.</p> <p>IP (Internet Protocol) : ensemble de règles pour l'envoi et la réception de messages au niveau adresse Internet.</p> <p>HTTP, FTP et autres protocoles de couche application : règles utilisées par des applications, comme des navigateurs Web, des programmes de transfert de fichiers et des programmes de messagerie.</p>

protocole avec connexion	Protocole, comme TCP, qui nécessite une connexion avant de transmettre des paquets d'informations.
protocole sans connexion	Protocole, comme UDP, qui envoie une transmission à une adresse de destination sur un réseau sans établir de connexion.
proxy	Mécanisme qui permet à un système d'agir au nom d'un autre système pour répondre aux demandes des protocoles. Les applications de sécurité des firewalls utilisent des services proxy pour protéger le réseau sécurisé vis-à-vis des utilisateurs d'Internet.
règle de firewall	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 de commutation par paquets	Réseau d'ordinateurs (comme Internet) qui transmet des fichiers en les scindant en unités plus petites (paquets) et en acheminant chaque paquet par l'itinéraire disponible le plus avantageux de la source à la destination, les paquets étant relayés en chemin par des ordinateurs. Les divers paquets constituant un fichier peuvent suivre des itinéraires différents et arriver à la destination à des heures différentes et dans le désordre. Les protocoles réseau (comme TCP/IP) réassemblent les paquets afin de reconstituer le fichier à la réception.
résolution de noms	Processus par lequel un nom de domaine est associé à l'adresse IP correspondante.
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.

script kiddie	Personne qui effectue des tentatives d'accès non autorisé sur des ordinateurs dans le but de rassembler des informations sur ces ordinateurs ou de les endommager. Ce type de pirate utilise généralement des applications écrites par d'autres pour attaquer des ordinateurs sur Internet.
serveur DNS	Serveur Domain Name System. Ordinateur qui stocke une base de données de noms de domaine et les adresses IP correspondantes. Lorsqu'un ordinateur envoie un nom de domaine à un serveur DNS, ce dernier lui renvoie l'adresse IP correspondant à ce domaine.
serveur proxy	<p>Serveur qui joue un rôle d'intermédiaire entre l'utilisateur d'un poste de travail et Internet pour permettre à l'entreprise d'assurer la sécurité, le contrôle administratif et la gestion de la mémoire cache. Un serveur proxy est associé à un serveur passerelle (ou fait partie de ce dernier) qui sépare le réseau de l'entreprise du réseau externe et à un serveur firewall qui protège le réseau de l'entreprise contre les intrusions extérieures.</p> <p>Un serveur proxy reçoit d'un utilisateur une demande de connexion à un service Internet (demande de page Web, par exemple). Si le serveur proxy est également un serveur de cache, il peut utiliser sa mémoire cache, où se trouvent des pages Web téléchargées antérieurement, pour fournir la page demandée sans transmettre la demande à Internet. Si la page demandée n'est pas stockée dans la mémoire cache, le serveur proxy utilise l'une de ses propres adresses IP pour demander la page au serveur situé sur Internet. Lorsque la page demandée est renvoyée, le serveur proxy fait le lien avec la demande d'origine et transmet la page à l'utilisateur.</p> <p>L'utilisateur a l'impression que toutes les demandes à Internet et les réponses renvoyées sont directement liées au serveur Internet destinataire. Vous devez définir l'adresse IP du proxy en tant qu'option de configuration dans le navigateur ou un autre programme de protocole.</p>

serveur Web	Ordinateur sur lequel sont stockées des pages Web accessibles à d'autres internautes à l'aide d'un navigateur Web. Egalement le logiciel qui permet à l'utilisateur d'accéder à ces pages Web.
service	Protocoles permettant à un ordinateur d'accéder à un type de données stockées sur un autre ordinateur. Nombre d'ordinateurs hôtes connectés à Internet offrent des services. Par exemple, les serveurs HTTP utilisent le protocole HTTP (HyperText Transfer Protocol) pour fournir le service World Wide Web ; les serveurs FTP offrent des services FTP (File Transfer Protocol) ; les serveurs SMTP utilisent le protocole SMTP (Simple Mail Transport Protocol) pour échanger des messages électroniques ; les serveurs POP utilisent le protocole POP (Post Office Protocol) pour échanger des messages électroniques. <i>Voir aussi port.</i>
site Web	Groupe de pages Web gérées par une même société, organisation ou personne. Un site Web peut comprendre du texte, des images, des fichiers audio et vidéo et des liens hypertexte vers d'autres pages Web.
SMTP	Simple Mail Transfer Protocol. Protocole TCP/IP qui régit l'émission et la réception des messages électroniques. SMTP est l'un des services de messagerie électronique les plus répandus. Il utilise le port TCP 25.
sneakernet	Méthode permettant de déplacer des données entre des ordinateurs qui ne sont pas connectés par un réseau. Un utilisateur copie des données sur un support de stockage amovible (par exemple une disquette) qu'il apporte physiquement à un autre ordinateur.
socket	Identificateur d'un service spécifique, sur un ordinateur spécifique. Un socket est constitué de l'adresse IP de l'ordinateur suivi du signe deux-points et du numéro de port.

sous-réseau	Réseau local faisant partie d'un intranet plus important ou d'Internet.
TCP	<p>Transmission Control Protocol. Protocole de transport standard sur Internet fournissant un service en continu fiable en duplex intégral. Le logiciel de mise en œuvre de TCP réside normalement dans le système d'exploitation et utilise le protocole IP pour transmettre les informations sur Internet.</p> <p>Parmi les applications et services TCP, on peut citer FTP, l'exploration du Web, la messagerie électronique et IRC.</p>
TCP/IP	<p>Transport Control Protocol/Internet Protocol. Fait généralement référence à la suite de protocoles Internet qui comprend TCP et IP, mais aussi plusieurs autres protocoles utilisés par les ordinateurs pour communiquer entre eux. TCP/IP est le protocole standard utilisé sur Internet. Il peut également servir de protocole de communication dans les intranets et les extranets.</p> <p>TCP/IP est un programme à deux couches. La couche supérieure, TCP (Transmission Control Protocol), gère la décomposition d'un message ou d'un fichier en plusieurs petits paquets transmis sur Internet à une autre couche TCP où ils sont regroupés pour restituer le message d'origine. La couche inférieure, IP (Internet Protocol), gère les informations d'adressage de chaque paquet en vue d'assurer son acheminement vers la destination correcte.</p>
Telnet	Service TCP qui prend en charge les ouvertures de session à distance (généralement vers des systèmes UNIX). Ce service permet d'ouvrir une session sur un ordinateur distant, en tant qu'utilisateur ordinaire disposant de tous les privilèges qui vous ont été accordés vis-à-vis des différentes applications et données stockées sur l'ordinateur. Telnet utilise le port 23.

tentative de connexion	Transfert de données qui demande l'établissement d'une connexion.
UDP	User Datagram Protocol. Protocole sans connexion qui agit au niveau de la couche de transport afin de fournir des fonctionnalités similaires à celle du protocole TCP, mais avec une fiabilité moindre. UDP utilise IP pour envoyer ses paquets, mais n'établit pas de connexion avant l'envoi et ne vérifie pas que les paquets ont bien été reçus. La radio sur Internet et les autres supports de transmission en continu utilisent souvent le protocole UDP en raison des charges moindres.
URL	Uniform Resource Locator. Adresse globale des documents et d'autres ressources sur le World Wide Web. La première partie de l'URL indique le protocole à utiliser et la seconde définit l'adresse IP ou le nom de domaine où se trouve la ressource. Dans l'exemple d'URL <code>http://www.symantec.com/index.html</code> , <code>http</code> représente le protocole, <code>www.symantec.com</code> le nom de domaine et <code>index.html</code> le document.
ver	Programme qui crée des copies de lui-même, par exemple d'un disque à un autre, ou qui s'envoie lui-même par courrier électronique. Il peut provoquer des dommages ou menacer la sécurité de l'ordinateur. Un ver peut arriver sous forme d'annexe de courrier électronique.
virus	Programme conçu pour se répliquer et se propager, généralement à l'insu de l'utilisateur. Un virus 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, un grand nombre causent aussi de sérieux dommages. Un virus peut arriver dans un document reçu par courrier électronique.

vulnérabilité	Brèche par laquelle une attaque ou des dommages peuvent survenir.
wannabe	Personne qui effectue des tentatives d'accès non autorisé sur des ordinateurs dans le but de rassembler des informations sur ces ordinateurs ou de les endommager. Ce type de pirate utilise généralement des applications écrites par d'autres pour attaquer des ordinateurs sur Internet.
World Wide Web	Ensemble de documents hypertexte stockés sur des serveurs HTTP dans le monde entier. Egaleme nt 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.
zombie	Programme implanté secrètement qui sommeille sur un ordinateur. Il se réveille ultérieurement, lors d'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 d'annexe de courrier électronique.

I N D E X

A

Accès à Internet, contrôle 63-66, 89
 alertes 50
ActiveX, contrôles 12, 52, 62, 88, 105
Aide 13, 31-32
aide "Qu'est-ce que c'est ?" 31
Aide en ligne 13, 31-32
Alert Tracker, définition 38
Alertes
 accès à Internet, contrôle 50, 65
 ActiveX 52
 cookie 53
 firewall personnel 63
 informations confidentielles 54
 Java 52
 présentation 47
 Protection contre les intrusions 70
 sécurité 48
Alertes de sécurité 48
Analyse
 ports 78, 103
 applications Internet 65
AOL 30
Applets Java 12, 52, 62, 88, 105
Applications, accès à Internet. *Voir* applications Internet
Approuvés, zone 68
Assistant Informations
 exécution 22
 fonctions 22
 mode d'emploi 22
Assistant Sécurité 13
 Alert Tracker, volet 38
 après l'installation 23
 Contrôle de zone Internet 37
 Contrôle des applications 36
 Contrôle parental 34
 Etat Internet 38
 Firewall personnel 33
 navigation 33
 ouverture 33
 volet LiveUpdate 38
Attaques 102-104, 109
attaques 70-72
AutoBlock 48, 70

B

Barre d'état système, icône 27
Blocage
 ActiveX, contrôles 52
 adresse de messagerie 45
 applets Java 52
 cookies 44, 54, 88, 106
 informations confidentielles 13, 42-43, 55, 89, 106
 informations sur le navigateur 90
 Internet, applications 51
 ordinateurs 70
 programmes. *Voir* applications Internet
Bureau, icône 27

C

Carte de crédit, numéros 43
Chevaux de Troie, programmes 108
CompuServe 30
Confidentialité 13, 41-46, 89, 106
 configuration 34
 état 76
 niveaux 42
 Paramètres 43
 risques 105-107
Confidentielles, informations 13, 42-44, 54, 89, 106
Configuration requise 15
Connexion Internet, partage 81
Connexions haut débit 77-78, 81
Contenus actifs 105
 Voir aussi contrôles ActiveX, applets Java
Contrôle de zone Internet 67-69
 configuration 37
Contrôle des applications 36
Cookies 13, 44, 53, 76, 88, 106
Courrier électronique 14
Cryptage 45, 46

D

Désactivation temporaire de Norton Personal Firewall 28-29
Désinstallation
 autres programmes de firewall 16
 copies antérieures de Norton Personal Firewall 16
 Norton Personal Firewall 24
Détail des informations, niveau 57
DHCP (Dynamic Host Configuration Protocol), serveurs 85
DNS (Domain Naming System) 95
Domestiques, réseaux 80, 90
DSL, connexions 77-78, 81
Dynamic Host Configuration Protocol (DHCP), serveurs 85

E

Enregistrement du logiciel 21
Entreprise, firewalls 82
Etat
 Confidentialité 76
 Firewall personnel 76

F

Fichier Lisezmoi 32
Fichiers, partage 80, 82
Firewall personnel
 alertes 63
 configuration 33
 état 76
 paramètres de sécurité 60-62
 présentation 11, 59
Firewalls
 Voir aussi Firewall personnel
 entreprise 82
 présentation 11
Fonctions, résumé 11

I

ICMP (Internet Control Message Protocol) 93
Icône dans la zone de notification 27
IGMP (Internet Group Membership Protocol) 93
Imprimantes, partage 80, 82, 90
Informations confidentielles 13, 42-44, 54, 106
informations confidentielles 89

Informations sur le navigateur 90
Informations sur les activités Internet 38
Internet
 présentation 91-93, 95
Internet Control Message Protocol (ICMP) 93
Internet Group Membership Protocol (IGMP) 93
Internet, applications 50, 65
IP, adresses 73

J

JavaScript 88
Jeux 79

L

Lancement de Norton Personal Firewall 27
LiveUpdate 29
localhost 96

M

Masqués, ports 63, 103
Messages, affichage 55
Modem câble, connexions 77-78, 81
Modem, connexions 77
Modification 44
Multi-joueurs, jeux 79

N

Navigateur
 confidentialité 45
 informations 90
NetBIOS 78
Norton Personal Firewall. *Voir* Firewall personnel
Norton Privacy Control. *Voir* Confidentialité
Norton SystemWorks, installation avec 24
Numéro de série 21

O

Ordinateurs
 ajout aux zones 68
 blocage 70
 définition 72-74
 noms 73
 spécifications 15

P

- Paramètres
 - confidentialité 43
 - Firewall personnel 60-??
 - firewall personnel ??-62
- Partage de fichiers et d'imprimantes 80, 82, 90
- pcAnywhere 86
- Ping, analyses 103
- Pirates 101-104
- Ports 97-98
 - analyse 78, 103
 - dissimulation 63
- Problèmes
 - affichage d'un site Web 87-89
 - envoi d'informations aux sites Web 89
 - impression 90
 - informations sur le navigateur 90
 - réseau 90
- Prodigy Internet 30
- Produit, numéro de série 21
- Programmes, accès à Internet. *Voir* applications Internet
- Protection contre les intrusions 70-72
- Proxy, serveurs 83

R

- Règles de firewall
 - applicables à l'ensemble du système 67
 - problèmes 88
 - pour serveurs FTP 85
 - pour les serveurs Web 84
- Réseau privé virtuel (VPN) 86
- Réseaux 80, 90
- Risques 108
 - chevaux de Troie 108
 - confidentialité 105-107
 - contenus actifs 105
 - pirates 101-104
 - virus 108
- Routeurs 81

S

- Scripts 88
- Sécurisés, sites Web 45, 46
- Sécurité
 - attaques 70-72, 102-104, 109
 - niveaux 60-62
- Serveurs FTP 85
- Serveurs Web 84
- Service de protection contre les intrusions 30
- Sites Web, problèmes d'affichage 87-89
- Sockets 97
- Sous-réseau, masques 74, 99
- Suppression de Norton Personal Firewall de votre ordinateur 24
- Systèmes d'exploitation 15
- Systèmes d'exploitation Windows 15

T

- TCP/IP 92-94

U

- UDP (User Datagram Protocol) 93
- Uniform Resource Locator (URL) 73, 95, 96
- URL (Uniform Resource Locator) 73, 95, 96
- User Datagram Protocol (UDP) 93

V

- VBscript 88
- Vers 108
- VPN (réseau privé virtuel) 86

Z

- Zombies 108
- Zone de notification, icône 27
- Zones 67-69

Solutions de service et de support de Symantec

Symantec a pour vocation de fournir un excellent service dans le monde entier. Nous avons pour but de vous fournir une assistance professionnelle dans l'utilisation de nos logiciels et de nos services, quel que soit l'endroit où vous vous trouvez.

Les solutions de support technique et de Service Clientèle varient selon les pays. Si vous avez des questions sur les services décrits ci-dessous, reportez-vous à la section « Numéros de contact » à la fin de ce chapitre.

Si ce produit vous a été fourni par le fabricant de votre ordinateur, nous vous recommandons de le contacter pour toute assistance.

Enregistrement de votre produit Symantec

Le fait d'enregistrer votre produit Symantec vous permet d'accéder au support technique, au remplacement des supports et des manuels et bien d'autres services. Vous pouvez le faire de différentes façons :

- Lors de la procédure d'installation (si le logiciel Symantec vous le permet).
- En remplissant le formulaire d'enregistrement en ligne de Symantec depuis le site suivant :
 - **Canadien**
http://www.symantec.com/region/can/fr/custserv/cs_register.html
 - **Français**
<http://www.symantec.com/region/fr/techsupp/registration.html>
- Si une carte d'enregistrement est fournie avec votre produit, remplissez-la et postez-la à l'adresse indiquée ci-après.

Mise à jour des définitions de virus

Si votre logiciel inclut la fonctionnalité LiveUpdate, vous pouvez cliquer sur le bouton LiveUpdate pour télécharger et installer les définitions de virus de façon automatique. Vous pouvez également vous procurer les dernières définitions par Internet à l'adresse suivante :

<http://securityresponse.symantec.com>

Voici la procédure à suivre pour mettre vos définitions de virus à jour :

- Cliquez sur le lien Norton AntiVirus dans la section Updates.
- Cliquez sur Download Virus Definition Updates en haut de la page.
- Sélectionnez votre langue.
- Sélectionnez le nom de votre produit.
- Cliquez sur le bouton Download Updates.
- Sélectionnez le nom de fichier correspondant à votre produit.
- Vous pouvez exécuter le programme à partir de son emplacement courant ou le sauvegarder sur votre disque pour l'exécuter ultérieurement. Si vous choisissez de le sauvegarder, sélectionnez l'emplacement de votre disque dur où vous souhaitez télécharger le fichier
- A la fin du téléchargement, sélectionnez le fichier dans l'Explorateur Windows et cliquez deux fois sur son icône.

Lorsque la procédure de mise à jour automatique est terminée, vous bénéficiez des définitions de virus les plus récentes.

Renouvellement de l'abonnement aux définitions de virus

Votre achat de Norton AntiVirus vous donne droit à un an de téléchargement des définitions de virus par Internet, un service entièrement gratuit. A l'issue de cette première année, vous pouvez acheter un abonnement sur le site Web de Symantec pour un coût modique. Veuillez vous reporter à la section « Numéros de contact » dans les pages qui suivent pour connaître le site Web correspondant à votre pays de résidence. Après vous être connecté à ce site, allez dans la Boutique Symantec et choisissez Virus Update Subscription (Abonnement aux définitions de virus). Vous avez la possibilité de payer par carte bancaire (MasterCard ou VISA).

Pour de plus amples informations sur le renouvellement de votre abonnement, visitez le site :

■ **Canadien**

http://www.symantec.com/region/can/fr/techsupp/navsub_fr.html

■ **Français**

http://www.symantec.com/region/fr/techsupp/virus_subscriptions.html

Anciennes versions de produits Norton

Si vous possédez un produit Norton 2000, le bouton LiveAdvisor de la barre de menus de ce produit sera supprimé lors de l'installation d'un produit Norton 2001. LiveAdvisor étant une méthode d'envoi d'informations que nous n'utilisons plus, cette suppression n'aura aucune incidence sur les fonctionnalités dont vous disposez.

Comme nous vous l'avions indiqué dans les derniers messages LiveAdvisor, Symantec vous propose désormais de trouver les informations auparavant transmises par LiveAdvisor sur les sites suivants :

Sites Web de Symantec :

Symantec Security Response (anciennement SARC)

<http://securityresponse.symantec.com>

Sites internationaux :

■ **Europe**

(langue anglaise) :

www.symantec.com/eusupport/

■ **France :**

www.symantec.fr/frsupport/

Bulletins d'informations sur vos produits :

Etats-Unis/Angleterre (en anglais):

<http://www.symantec.com/techsupp/bulletin/index.html>

Français:

<http://www.symantec.com/region/fr/techsupp/bulletin/index.html>

Service Clientèle et support technique

Symantec offre une gamme complète d'options de support technique et généraliste afin de vous permettre d'optimiser vos investissements logiciels. Un support technique gratuit est disponible sur les sites Web d'assistance de Symantec, ainsi que par le système d'envoi de fax sur demande.

Support téléphonique

Symantec propose un support téléphonique payant pour les produits grand public. Les clients peuvent acheter une assistance « à la demande » auprès d'un technicien de support.

N'hésitez pas à contacter votre Service Clientèle Symantec pour toute information concernant les options d'assistance offertes par Symantec (voir la section « Numéros de contact » dans les pages qui suivent).

Prise en charge des anciennes versions et des versions abandonnées

Lorsqu'une nouvelle version d'un logiciel est commercialisée, les utilisateurs enregistrés reçoivent des informations de mise à jour. La version précédente continue de faire l'objet d'un support téléphonique pendant une période limitée après le début de la commercialisation de la nouvelle version. Des informations techniques pourront toujours être disponibles sur le site Web de Symantec et le système automatisé d'informations par télécopie.

Lorsque Symantec annonce l'abandon de la commercialisation ou de la vente d'un produit, le support téléphonique est arrêté 60 jours plus tard. Les produits abandonnés ne sont pris en charge que par l'intermédiaire de notre système automatisé d'informations par télécopie ou de documentations déposées sur le site Web de Symantec.

Service Clientèle

Le Service Clientèle de Symantec peut répondre à vos questions non techniques. Vous pouvez l'appeler pour :

- obtenir des informations générales sur un produit (fonctionnalités, prix, disponibilité de versions traduites, adresses de revendeurs, etc.) ;
- savoir comment déterminer la version de votre logiciel ;
- connaître la disponibilité d'une nouvelle version ou d'une mise à jour ;
- savoir comment mettre votre logiciel à jour ;
- demander de la documentation produit ou un logiciel d'essai ;
- remplacer des éléments manquants ou défectueux (disquettes, manuels, etc.) de vos produits;
- mettre à jour vos informations d'enregistrement de produits en cas de changement de nom ou d'adresse ;
- renouveler votre abonnement aux mises à jours des définitions de Norton AntiVirus ou Norton Internet Security;
- obtenir des informations sur les solutions de support technique de Symantec ;

Toutes les informations sur notre service Clientèle sont disponibles en ligne sur notre site Web dédié et par téléphone auprès du Service Clientèle Symantec. Consultez la section « Numéros de contact » à la fin de ce chapitre pour obtenir le numéro et l'adresse Internet du Service Clientèle le plus proche.

Numéros de contact

Si vous habitez le Canada, vous pouvez contacter le service Clientèle aux numéros suivants :

800 561-0820 ou 800 441-7234

Vous pouvez également visiter le service Clientèle en ligne à l'adresse :

<http://www.symantec.com/region/can/fr/custserv/cust1.html>

ou adresser votre correspondance à l'adresse postale suivante :

Symantec Canada

Attention: Service Clientèle
895, Don Mills Road
500-2 Park Center
Toronto, Ontario M3C 1W3
Canada

Sites Web du service technique de Symantec

- **Europe (langue anglaise) :** www.symantec.com/eusupport/
- **Canada :** www.symantec.com/region/can/fr/index.html
- **France :** www.symantec.fr/frsupport/
- **Site FTP de Symantec :** [ftp.symantec.com](ftp://ftp.symantec.com)
(Notes techniques et correctifs logiciels)

A partir des sites Web du service de support Symantec, vous pouvez effectuer des recherches dans la base de connaissances du support technique, consulter les informations produits, envoyer votre question à l'un des groupes de discussion, entre autres. Utilisez l'Assistant de dépannage pour trouver rapidement l'information recherchée.

Support technique de Symantec

Symantec propose un support technique GRATUIT sur son site Web de service clientèle et de support technique. Le support technique par téléphone est en revanche payant.

Utilitaires	Numéros locaux (autres pays : voir « Support produits Desktop »)
Norton SystemWorks Norton CleanSweep Norton Utilities pour Win95, NT, MAC Norton Commander Win95/NT Norton Ghost (version grand public) Norton Internet Security Norton Personal Firewall	Royaume-Uni : + (44) 20 7744 0061 France : + (33) 1 64 53 80 73 Allemagne : + (49) 69 6641 0371 Pays-Bas : + (31) 71 408 3958

Utilitaires	Numéros locaux (autres pays : voir « Support produits Desktop »)
-------------	--

Remarque : les utilitaires absents de la liste ci-dessus ne sont pris en charge que par site WEB.

AntiVirus	Numéros locaux (autres pays : voir « Support produits Desktop »)
Norton AntiVirus Windows/Macintosh	Royaume-Uni : + (44) 20 7616 5813 France : + (33) 1 64 53 80 63 Allemagne : + (49) 69 6641 0353 Pays-Bas : + (31) 71 408 3952

Solutions de productivité à distance	Numéros locaux (autres pays : voir « Support produits Desktop »)
DelrinaFax/Winfax pcAnywhere pour 95/NT	Royaume-Uni : + (44) 20 7616 5803 France : + (33) 1 64 53 80 60 Allemagne : + (49) 69 6641 0350 Pays-Bas : + (31) 71 408 3951

Support produits Desktop, autres pays

Autriche : + 43 (1) 501375023	Norvège : + 47 23053330
Belgique : + 32 (2) 7131701	Pologne : + 0 800 3111269
Danemark : + 45 35 445720	Afrique du Sud : + (27) 11 7849856
Finlande : + 358 (9) 22 930417	Espagne : + (34) 91 6625255
Irlande : + 353 (1) 6011901	Suède : + (46) 8 7355024
Israël : + 1 800 9453805	Suisse : + (41) 1 2121847
Italie : + (39) 02 45281052	Turquie : +(90) 212 213 42 65

Système de télécopie à la demande

Notre système de télécopie à la demande guidé par menus permet de recevoir de la documentation. En appelant le numéro approprié indiqué ci-dessous, vous serez guidé à travers diverses options que vous activez à l'aide de votre clavier téléphonique. Les informations que vous aurez choisies vous seront automatiquement envoyées par télécopie.

Belgique	+ (32) 2 7131710
Canada	+1 (541) 984 2490
France	+ (33) 1 64 53 80 52
Luxembourg	+ (352) 29 84 795022
Suisse	+ (41) 1 2126267

Service Clientèle de Symantec

Fournit des informations et des conseils non techniques en plusieurs langues.

Belgique	+ (32) 2 7131700
Canada	800 561-0820 ou 800 441-7234
France	+ (33) 1 64 53 80 50
Luxembourg	+ (352) 29 84 79 50 20
Suisse	+ (41) 1 2126262
Autres pays (Service en langue anglaise uniquement)	+ (353) 1 811 8032

Service Clientèle de Symantec : adresses pour la correspondance

Symantec Ltd
Customer Service Centre
Europe, Middle East and Africa (EMEA)
PO Box 5689
Dublin 15
Irlande

Canada

Symantec Corporation
Service Clientèle
895 Don Mills Road
500 - 2 Park Center
Toronto, ON
M3C 1W3

Afrique du Sud

Symantec SA (Pty) Ltd
PO Box 1998
Gallo Manor, Sandton
2052 Afrique du Sud

Tous les efforts ont été faits pour garantir l'exactitude des informations fournies dans ce document. Ces informations peuvent toutefois faire l'objet de modifications sans préavis. Symantec Corporation se réserve le droit d'apporter de telles modifications sans avertissement préalable.

