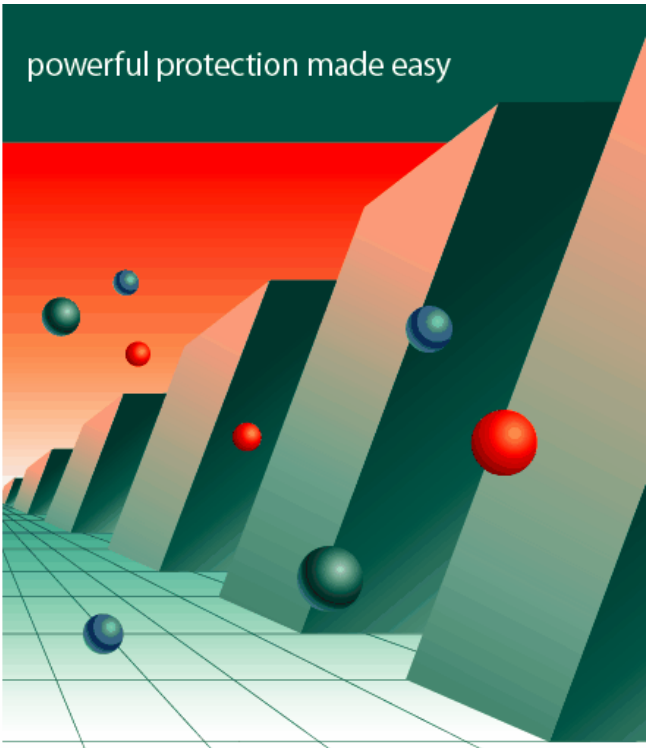
KASPERSKY LABS



EASY-TO-USE
SYSTEM PROTECTING STORED DATA

ADVANCED
TECHNOLOGIES AGAINST ALL TYPES OF HACKER ATTACKS

COMPLETE
CONTROL OVER INTRUSION ATTEMPTS

UNIQUE
SELF-LEARNING ABILITY

COMPREHENSIVE
DATA PACKET FILTRATION

CONTINUOUS
CONTROL OVER APPLICATION ACTIVITY

FREE
ROUND-THE-CLOCK TECHNICAL SUPPORT

Kaspersky Anti-Hacker

personal firewall

www.kaspersky.com

KASPERSKY lab

Kaspersky Anti-Hacker

GUIDE DE L'UTILISATEUR

KASPERSKY ANTI-HACKER

Guide de l'utilisateur

http://www.kaspersky.com/fr/

Date de révision : Septembre 2003

Sommaire

CHAPITRE 1. KASPERSKY ANTI-HACKER

1.1. Introduction

Qu'est-ce que Kaspersky Anti-Hacker ?

Kaspersky Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus provenant d'un réseau local adjacent ou de l'Internet.

Kaspersky Anti-Hacker:

- Surveille l'activité réseau via protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte n'importe quelle action suspecte des applications, vous en informe et si nécessaire, bloque l'accès de cette application au réseau. Cette solution permet de protéger vos données confidentielles de votre machine. Par exemple, si un cheval de Troie tente de transmettre des données vers l'extérieur, Kaspersky Anti-Hacker bloque l'accès à Internet du logiciel malveillant.

- Rend très difficile la détection de votre ordinateur depuis l'extérieur grâce à la technologie SmartStealth™. Les hackers ne trouvant pas de cible visible, toutes leurs tentatives de pénétrer dans votre ordinateur sont vouées à l'échec. En outre, cette technique évite les attaques DoS (Refus de service) quel que soit leur type. Par ailleurs, lorsque vous travaillerez sur le Web sous ce mode, vous ne percevrez aucune contrepartie négative : le logiciel garantit la transparence et l'accès normal aux données.

- Bloque les attaques les plus fréquentes des hackers à l'aide de filtres permanents du trafic sortant ou entrant, et en informe l'utilisateur.

- Surveille les tentatives d'analyse des ports qui précèdent habituellement d'autres attaques, et interdit toute communication ultérieure avec la machine attaquante.

- Permet l'examen de la liste des connexions établies, des ports ouverts et des applications réseau en exécution et, le cas échéant, d'interrompre les connexions non souhaitées.

- Sécurise votre machine contre les attaques des hackers, sans configuration spéciale des paramètres logiciels. Le logiciel propose une administration simplifiée par cinq niveaux de sécurité disponibles: *Bloquer tout, Haut, Moyen, Bas, Autoriser tout.* Par défaut, le logiciel utilise le niveau *Moyen* : ceci vous permet de vous familiariser avec les configurations du système de sécurité proposées automatiquement en fonction de vos réponses à divers événements.

- Offre une grande flexibilité dans la configuration du système de sécurité. Vous pouvez en particulier définir un filtre logiciel des opérations réseau souhaitées, et configurer le système de détection contre les intrusions.

- Permet l'enregistrement de certains événements réseau liés à la sécurité dans des registres à usages divers. Si besoin, vous pouvez définir le niveau de détail des registres du journal.

Le logiciel peut être utilisé comme un produit séparé, ou intégré dans un ensemble de plusieurs solutions **Kaspersky Lab**.

Attention ! Kaspersky Anti-Hacker ne protège pas votre ordinateur contre les virus ou les logiciels malveillants susceptibles de détruire ou d'endommager vos données. Pour cela, nous vous conseillons d'utiliser Kaspersky Anti-Virus Personal.

1.2. Nouveautés de la version 1.5

Nouvelles fonctions de la version 1.5.

Voici les nouveautés de la nouvelle version du logiciel :

- Prise en charge des modems ADSL ;

- Prise en charge complète du **mode invisible** (des tests ont été passés sur **www.pcflank.com**) ;

- Détection de nouvelles attaques réseau : **SmbDie**, **Helkern** et **Lovesan** ;

- Définition de plages de numéros de ports dans les règles de filtrage des paquets et d'application ;

- Facilité accrue de configuration juste après l'installation, sans réduire en aucune façon le niveau de sécurité de l'ordinateur : par défaut, les connexions sur le réseau sont autorisées pour les applications les plus fréquemment utilisées, strictement en fonction de leur type ;

- Interface graphique améliorée comprenant : la prise en charge du style XP sous Windows XP ; le redimensionnement des listes de contrôle de règles ; la possibilité d'utiliser la touche **<Ins>** pour ajouter un nouvelle règle.

1.3. Kit de distribution

Contenu du kit de distribution. Contrat de licence. Carte d'inscription.

1.3.1. Contenu du kit de distribution

Le kit de distribution contient :

- Une enveloppe fermée avec le CD d'installation contenant les fichiers du produit ;

- Ce guide de l'utilisateur ;

- Une disquette de clé, ou un fichier de clé sur le CD d'installation ;

- Le contrat de licence.

Avant d'ouvrir l'enveloppe avec le CD, assurez-vous de lire soigneusement le contrat de licence.

1.3.2. Contrat de licence

Le contrat de licence (CL) est un contrat légal établi entre vous (à titre personnel ou en représentation de votre société) et le fabricant (Kaspersky Labs Ltd.), qui spécifie les conditions d'utilisation du produit antivirus que vous avez acheté.

Assurez-vous de lire toutes les clauses du CL !

Si vous n'acceptez pas les termes du contrat de licence, Kaspersky Labs ne vous cède pas de licence sur le progiciel et vous devez retourner le produit non utilisé à votre revendeur Kaspersky Anti-Virus pour un remboursement complet, après vous être assuré que l'enveloppe contenant le CD (ou les disquettes) est bien fermée.

Le fait d'ouvrir l'enveloppe signifie que vous acceptez toutes les clauses du CL.

1.4. Contenu de la documentation

Aspects traités par la documentation

La documentation décrit la procédure d'installation, de personnalisation et d'administration de Kaspersky Anti-Hacker.

La documentation est composée des chapitres suivants :

Chapitre	**Sommaire**
Kaspersky Anti-Hacker	Qu'est-ce que Kaspersky Anti-Hacker? Composants du kit de distribution et informations sur cette documentation.
Installation et suppression du logiciel	Spécifications système. Installation du logiciel.
Premiers pas	Comment démarrer avec le logiciel. Exemple de configuration du système de sécurité.
Kaspersky Anti-Hacker : Blocage des attaques de hackers	Principes de fonctionnement du progiciel. Fonctions et tâches principales assurées par l'application.
Exécution du logiciel	Environnement d'écran et interaction avec les éléments de l'application principale.
Activation et définition des paramètres du système de sécurité	Comment activer le système de sécurité. Définition des paramètres de sécurité : règles pour applications et filtrage de datagrammes.

Chapitre	Sommaire
Supervision de l'activité	Examen des journaux : attaques réseau, activité des applications et filtrage de paquets. Affichage de la liste des applications actives, des ports ouverts et des connexions établies.
Annexe A. Kaspersky Labs Ltd.	À propos de Kaspersky Labs Ltd. Informations de contact.
Annexe B. Index	Glossaire des termes utilisés dans la documentation.
Annexe C. Questions fréquentes	Réponses aux questions fréquentes.

1.5. Conventions

Conventions utilisées dans cet ouvrage

Cet ouvrage utilise plusieurs conventions pour mettre en relief les différentes parties de la documentation.

Convention	Usage
Texte gras	Titres de menus, commandes, titres de fenêtres, éléments de boîtes de dialogue, etc.
 Note.	Information complémentaire, remarques.
 Attention !	Informations essentielles.

Convention	Usage
Pour démarrer l'application, suivez les étapes ci-après 1. Étape 1. 2. …	Actions à suivre.
Tâche	Exemple de tâche qu'un utilisateur doit accomplir pendant l'utilisation de l'application.
Solution	Solution à la tâche.

1.6. Assistance aux utilisateurs inscrits

Services offerts par Kaspersky Labs aux utilisateurs inscrits

Kaspersky Labs propose un large évantail de services à ses utilisateurs inscrits leur permettant d'utiliser plus efficacement Kaspersky Anti-Hacker.

Si vous vous inscrivez et achetez une souscription, vous recevrez les services suivants pour toute la période de votre inscription :

- Nouvelles versions du logiciel, fournies gratuitement ;
- Assistance téléphonique et par courrier électronique sur l'installation, la configuration et l'utilisation du logiciel ;
- Informations sur les nouveaux produits et les nouveaux virus d'ordinateurs (pour les abonnés au bulletin de Kaspersky Labs).

Kaspersky Labs ne fournit pas d'informations concernant l'administration ou l'utilisation de votre système d'exploitation ou d'autres technologies.

CHAPITRE 2. INSTALLATION ET SUPPRESSION DU LOGICIEL

2.1. Spécifications matérielles et logicielles

Spécifications système requises pour exécuter l'application

Pour exécuter Kaspersky Anti-Hacker, votre système doit répondre aux spécifications suivantes :

- Système d'exploitation préinstallé Microsoft Windows version 95 OSR2/98/ME/NT 4.0/2000/XP ;
- Pour installer sous Microsoft Windows NT 4.0/2000/XP, vous devez posséder des privilèges administrateur ;
- Protocole TCP/IP opérationnel ;
- Réseau local (Ethernet) ou connexion téléphonique.

Cette version du logiciel ne prise pas en charge des modems ADSL sous Windows ME

- Microsoft Internet Explorer (version minimum 5.0 , 5.5 (SP 2); version supérieure conseillée)
- Au moins 50 Mo d'espace libre pour les fichiers d'application, plus de l'espace pour les journaux de l'application
- Pour opérer sous Windows® 95 OSR2/98/Me/NT 4.0, vous devez avoir :
    - Intel Pentium® 133MHz ou supérieur sous Windows 98 or Windows NT 4.0 ;

- Intel Pentium® 150MHz ou supérieur sous Windows 95 OSR2/Me ;
- 32 Mo de RAM ;
- **Service Pack v. 6.0 ou supérieur préinstallé sous Windows NT 4.0 Workstation** ;

- pour opérer sous Windows 2000, vous devez avoir :
  - Intel Pentium® 133MHz ou supérieur ;
  - 64 Mo de RAM ;
- Pour opérer sous Windows XP, vous devez avoir :
  - Intel Pentium® 300MHz ou supérieur ;
  - 128 Mo de RAM.

2.2. Installation

Installation pas à pas. Assistant d'installation

Lancez l'application Setup.exe dans le CD pour démarrer le programme d'installation. L'assistant d'installation procède par dialogues. Chaque dialogue de l'assistant contient un certain nombre de boutons permettant de contrôler le déroulement de l'installation. Les principaux boutons sont :

- Ok : confirme les actions ;
- Annuler : annule la ou les opérations ;
- Suivant : se déplace à l'étape suivante ;
- Précédent : se déplace à l'étape précédente.

Avant d'installer Kaspersky Anti-Hacker assurez-vous de quitter toutes les applications ouvertes sur votre ordinateur.

Etape 1. Lecture des informations générales

La première boîte de dialogue de l'assistant d'installation (Figure 1. Première boîte de dialogue de l'assistant d'installation) contient des informations générales sur le progiciel Kaspersky Anti-Hacker.

Etape 2. Lecture du contrat de licence

La boîte de dialogue **Contrat de licence** (Figure 2. Boîte de dialogue **Contrat de licence**) contient le texte de l'accord. Lisez son contenu attentivement puis cliquez sur **Oui** si vous acceptez les termes du contrat de licence. Dans le cas contraire, cliquez sur **Non** pour annuler l'installation.

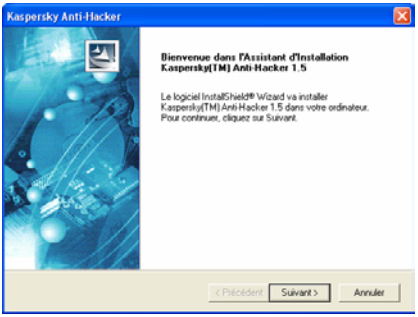


Figure 1. Première boîte de dialogue de l'assistant d'installation

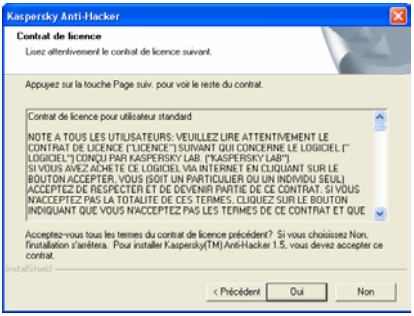


Figure 2. Boîte de dialogue **Contrat de licence**

Etape 3. Saisie des informations utilisateur

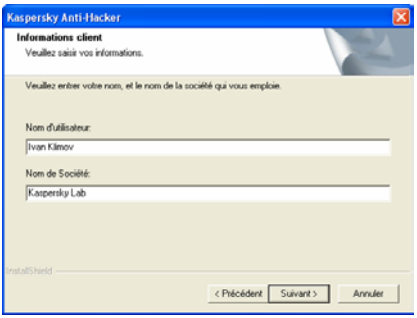


Figure 3. Boîte de dialogue **Informations client**

Indiquez les informations utilisateur dans la boîte de dialogue **Informations client** (Figure 3. Boîte de dialogue **Informations client**). Indiquez vos données dans les zones **Nom** et **Société**. Par défaut, le contenu de ces zones est extrait des informations du Registre de Windows.

Etape 4. Sélection du dossier d'installation de l'application

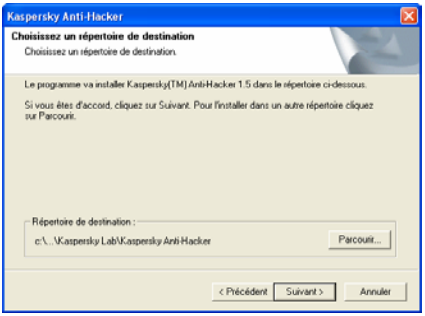


Figure 4. Boîte de dialogue **Choisissez un répertoire de destination**

Dans la boîte de dialogue **Choisissez un répertoire de destination** (Figure 4. Boîte de dialogue **Choisissez un répertoire de destination**), sélectionnez le dossier d'installation des composants de l'application pour installer les composants de Kaspersky Anti-Hacker. Le dossier doit être précisé dans le champ **Répertoire de destination**. Pour ce faire, cliquez sur **Parcourir** et indiquez le chemin d'accès du dossier dans la boîte de dialogue standard **Choix d'un dossier**.

Etape 5. Choix du nom du groupe d'applications du menu Démarrer\Programmes

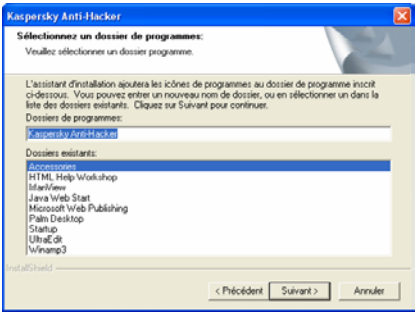


Figure 5. Boîte de dialogue **Sélectionnez un dossier de programmes**

Indiquez le nom du dossier dans la boîte de dialogue **Sélectionnez un dossier de programmes** (Figure 5. Boîte de dialogue **Sélectionnez un dossier de programmes**) correspondant au menu standard **Programmes** affichant l'icône de Kaspersky Anti-Hacker. Cliquez sur **Suivant**.

Etape 6. Définition des chemins d'accès aux fichiers de clé*

Dans la boîte de dialogue **Fichier de clé** (Figure 6. Boîte de dialogue **Fichier de clé**), vous devez définir le nom et le chemin d'accès du fichier de clé (avec extension *.key).

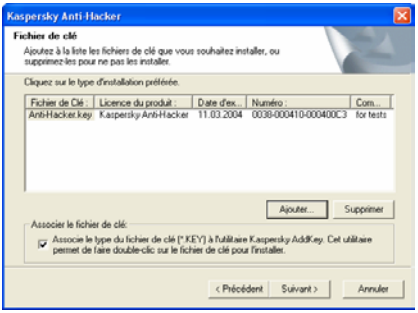


Figure 6. Boîte de dialogue **Fichier de clé**

S'il se trouve dans le dossier d'installation, le nom du fichier est affiché dans la liste des fichiers de clé à installer.

Si le fichier de clé se trouve dans un dossier différent, cliquez sur **Ajouter** et indiquez son nom et chemin d'accès dans la boîte de dialogue standard **Fichier de clé**. Si nécessaire, l'application peut utiliser plusieurs fichiers de clé en même temps.

Nous vous conseillons de cocher la case **Associer le fichier de clé**. Ce faisant, vous pourrez installer de nouveaux fichiers de clé par un double-clic sur leurs noms. Si vous ne cochez pas la case, vous devrez copier un fichier de clé dans le dossier des fichiers partagés avant de pouvoir l'installer.

Ce fichier est votre clé d'accès personnelle. Il contient toutes les données à usage interne essentielles pour que *Kaspersky Anti-Hacker* puisse exécuter toutes ses fonctions :

- L'information du revendeur de la version (société, adresses, numéros de téléphone) ;
- L'information du service technique (son nom et son adresse) ;
- Date de publication du produit ;
- Nom et numéro de la licence ;
- La période de validité de la licence.

Etape 7. Copie des fichiers sur le disque

Lisez l'information sur l'installation dans la boîte de dialogue **Copie des fichiers** (Figure 7. Boîte de dialogue **Copie des fichiers**). Pour modifier des paramètres, vous devez revenir en arrière jusqu'à l'étape de l'assistant correspondante, en cliquant sur le bouton **Précédent**. Si les informations d'installation sont correctes, cliquez sur **Suivant**. Le logiciel démarre la copie des fichiers sur le disque. Le déroulement de l'opération est reflété par la barre de progression dans la boîte de dialogue **État de l'installation** (Figure 8. Boîte de dialogue **État de l'installation**).

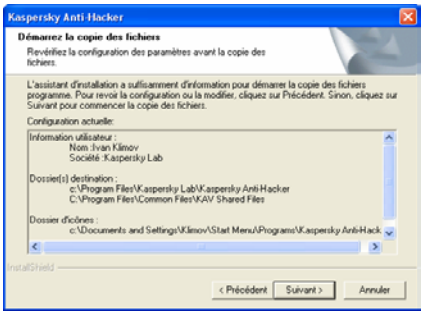


Figure 7. Boîte de dialogue **Copie des fichiers**

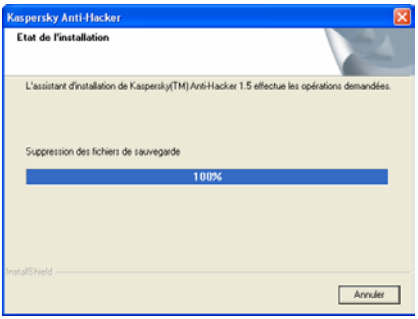


Figure 8. Boîte de dialogue **État de l'installation**

Etape 8. Fin de l'installation

Une fois terminée l'installation du progiciel Kaspersky Anti-Hacker la boîte de dialogue **Installation du programme terminée** est affichée sur l'écran (Figure 9. Boîte de dialogue **Installation du programme terminée**).

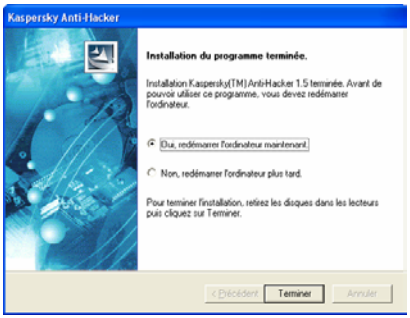


Figure 9. Boîte de dialogue **Installation du programme terminée**

Pour terminer correctement l'installation, vous devez redémarrer votre ordinateur. Sélectionnez **Oui, redémarrer l'ordinateur maintenant** pour redémarrer directement votre système, ou bien **Non, redémarrer l'ordinateur plus tard** pour remettre le redémarrage à plus tard. Pour terminer l'opération, cliquez sur **Terminer**.

2.3. Suppression de l'application

Suppression de l'application de votre ordinateur

Pour supprimer Kaspersky Anti-Hacker procédez comme suit :

1. Dans la barre des tâches du bureau de Windows, cliquez sur **Démarrer** et choisissez **Programmes**.

2. Sélectionnez le groupe correspondant à votre installation de Kaspersky Anti-Hacker. Par défaut, le nom du groupe d'applications est **Kaspersky Anti-Hacker**, à moins d'en avoir choisi un autre lors de l'installation. Puis sélectionnez **Désinstallation de Kaspersky Anti-Hacker**.

3. Si vous devez désinstaller Kaspersky Anti-Hacker, cliquez sur **Oui** dans le dialogue de confirmation. Si vous changez d'avis, annulez la désinstallation en cliquant sur **Non**.

Pour ajouter ou supprimer l'application, cliquez sur l'icône **Ajout ou suppression de programmes** dans le **Panneau de contrôle**.

CHAPITRE 3. PREMIERS PAS

Comment démarrer avec le logiciel.
Exemple de configuration du
système de sécurité

Aussitôt après l'installation du programme et le redémarrage de votre ordinateur, le système de sécurité est activé. En pratique, à ce moment précis, Kaspersky Anti-Hacker se trouve déjà en train de surveiller les tentatives attaques contre votre machine ou d'établissement de connexion de vos applications via un réseau local ou Internet.

Après avoir ouvert une session de travail, vous pouvez commencer à travailler comme d'habitude. S'il n'existe aucune connexion réseau active, la présence du système de sécurité de votre machine est signalée simplement par l'icône dans la barre d'état système. Si vous cliquez sur l'icône, la fenêtre principale de l'application s'affiche à l'écran. Cette fenêtre vous permet d'examiner les informations sur le niveau de sécurité courant , et le cas échéant, de le modifier (pour de plus amples détails sur la fenêtre principale de l'application, reportez-vous au sous-chapitre 5.3 à la page 29). Le niveau **Moyen** est activé par défaut. Ce niveau permet de configurer votre système de sécurité par dialogues interposés. Dans la plupart des cas, vous n'aurez pas à configurer vous-même votre système : par défaut, les connexions sur le réseau sont autorisées pour les applications les plus fréquemment utilisées, strictement en fonction de leur type. Cependant, vous devrez parfois configurer manuellement votre système de sécurité. Prenons comme modèle l'exemple ci-dessous.

Tâche : Supposons que votre ordinateur est connecté à Internet ; vous lancez Microsoft Internet Explorer et entrez www.kaspersky.com dans le champ adresse. Le message suivant s'affiche à l'écran : **Créer une règle pour IEXPLORER.EXE** (Figure 10. Fenêtre interactive du système de sécurité).

Dans la partie supérieure de la boîte de dialogue sont affichés l'icône de l'application concernée, son nom (ici, Microsoft Internet Explorer), l'adresse du site www.kaspersky.com**,** et le port utilisé pour établir la connexion. Pour examiner d'autres détails sur l'application, cliquez simplement sur le lien souligné (Figure 11. Informations obtenues sur la connexion).

La connexion réseau demandée ne sera pas établie avant d'avoir choisi comment gérer l'activité de cette application. Pour ce faire, vous devez répondre au message sur l'écran.

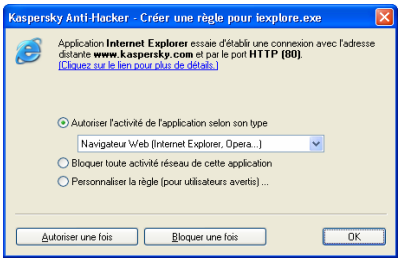


Figure 10. Fenêtre interactive du système de sécurité

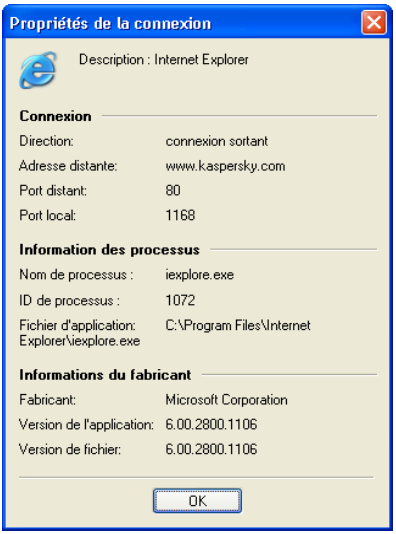


Figure 11. Informations obtenues sur la connexion

Procédez comme suit :

1. Activez l'option **Autoriser l'activité de cette application selon son type** et choisissez **Navigateur Web (IE, Netscape...)** dans la liste déroulante ;

2. Cliquez sur **Ok**.

Après cela, Kaspersky Anti-Hacker permettra à l'application Microsoft Internet Explorer d'établir la connexion. En outre, l'application sera autorisée à établir n'importe quelle autre connexion conforme à son type.

Vous aurez certainement remarqué les trois options offertes par la boîte de dialogue **Créer une règle pour IEXPLORER.EXE** :

- **Autoriser l'activité de cette application selon son type** (l'option choisie dans l'exemple précédent). Cette option ne permet que les communications réseau compatibles avec la catégorie d'application spécifiée. Sélectionnez la catégorie souhaitée dans la liste déroulante. Vous pouvez autoriser l'application à effectuer toutes les activités en sélectionnant **Autoriser tout** dans la liste déroulante.

- **Bloquer toute activité réseau de cette application**. Cette option empêche l'application spécifiée de réaliser tout type d'activité sur le réseau, y compris l'opération décrite.

- **Personnaliser la règle**. Cette option permet de spécifier les opérations autorisées pour l'application. Activez cette option puis cliquez sur Ok pour afficher la fenêtre de l'assistant de règles. L'assistant de règles permet de définir les conditions d'autorisation d'une opération (pour de plus amples détails sur l'assistant de règles, reportez-vous au sous-chapitre 6.3.2 à la page 50).

Si vous ne savez pas quelle option choisir, sélectionnez **Autoriser une fois** ou **Bloquer une fois** en bas de la boîte de dialogue. Vous pourrez ensuite observer le comportement de l'application et décider l'option souhaitée.

Si vous fermez la fenêtre interactive en cliquant sur  dans l'angle supérieur droit, l'opération en question sera bloquée pour cette fois.

Cette procédure par dialogues interposés vous permet donc de configurer de manière appropriée le système de sécurité de votre ordinateur.

Pour examiner la liste des règles définies, sélectionnez **Règles d'application** dans le menu **Service**, ou cliquez sur  dans la barre d'outils de la fenêtre principale.

Nous vous conseillons d'utiliser le mode de sécurité **Moyen** pendent les premières semaines, après avoir installé le logiciel. Le logiciel pourra ainsi configurer automatiquement la sécurité du système en fonction de vos réponses à plusieurs événements. Créez les règles permettant les opérations réseau standard.

Après une période d'apprentissage, vous pouvez basculer au niveau de sécurité **Haut**, et sécuriser votre ordinateur contre tout événement réseau non autorisé ou contre toute attaque de hackers. Gardez toutefois à l'esprit que les nouvelles applications que vous installez seront par défaut interdites d'accès au réseau local et à Internet. Pour informer Kaspersky Anti-Hacker de ces nouvelles applications, vous devrez basculer de nouveau à **Moyen** ou définir manuellement les règles appropriées pour ces applications.

CHAPITRE 4. KASPERSKY ANTI-HACKER : BLOCAGE DES ATTAQUES DE HACKERS

4.1. Principes de fonctionnement de Kaspersky Anti-Hacker

Comment procède Kaspersky Anti-Hacker ? Règles d'application. Règles de filtrage de paquets. Détection contre les intrusions.

Kaspersky Anti-Hacker sécurise votre ordinateur contre les attaques provenant du réseau et protège vos données confidentielles. Pour ce faire, Kaspersky Anti-Hacker surveille toutes les opérations réseau sur votre ordinateur. Il existe deux formes de procéder sur le réseau :

- Au niveau des applications (opérations de haut niveau). Dans ce niveau, Kaspersky Anti-Hacker analyse l'activité des applications réseau, y compris des navigateurs Web, des programmes de messagerie, de transfert de fichiers et autres.

- Au niveau des paquets (opérations de bas niveau). Avec ce niveau, Kaspersky Anti-Hacker analyse les paquets de données envoyés ou reçus par votre carte réseau ou votre modem.

Vous utilisez Kaspersky Anti-Hacker pour créer des règles spéciales de filtrage pour les opérations réseau. Un certain filtrage est effectué automatiquement par le système de détection contre les intrusions, qui est capable de détecter des analyses de ports, des attaques DoS, etc., et de bloquer l'assaillant. En outre, vous pouvez définir vos propres règles de filtrage pour renforcer la protection de votre machine.

Pour chaque type d'opération réseau, Kaspersky Anti-Hacker gère des listes séparées de règles.

- *Règles d'application*. Vous sélectionnez ici l'application souhaitée et autorisez les activités compatibles avec son type. Si besoin, vous pouvez définir un nombre quelconque de règles pour chaque application. Si une activité sur le réseau ne satisfaisant pas les conditions de la règle est détectée sur votre machine, le programme vous en informe et vous permet de bloquer toute action non souhaitée (avec le niveau **Moyen** activé). Pour définir la règle la plus simple possible pour une application donnée, sélectionnez simplement son type dans la liste déroulante (pour de plus amples détails reportez-vous au sous-chapitre 6.3.2.1 à la page 50). Pour définir une règle plus complexe, spécifiez les services et les adresses distantes qui seront autorisés pour cette application.

- *Les règles de filtrage de paquets* autorisent ou bloquent les paquets réseau envoyés ou reçus par votre machine. Ces règles examinent l'en-tête du paquet (protocole utilisé, numéro de port, adresse IP, etc.) puis prennent des décisions en fonction de ces données. Ces règles s'appliquent à toutes les applications réseau fonctionnant sur votre machine. Si vous créez par exemple une règle pour bloquer une certaine adresse IP, toutes les communications réseau avec cette adresse seront interdites.

La priorité des règles de filtrage de paquets est plus haute que celle des règles d'application, autrement dit, ces règles sont exécutées en premier lieu. Par exemple, si vous créez une règle pour bloquer tous les paquets entrants et sortants, l'exécution de cette règle annule l'application d'autres règles associées aux applications.

4.2. Niveaux de sécurité

Quels sont les niveaux de sécurité de sécurité pris en charge par Kaspersky Anti-Hacker ?

Le logiciel propose au choix les niveaux de sécurité suivants :

- Autoriser tout : désactive le système de sécurité de votre machine. Quand ce niveau de sécurité est sélectionné, toute activité sur le réseau de votre machine est autorisée.

- Bas : permet l'activité sur le réseau de toutes les applications, sauf de celles explicitement interdites par des règles d'application définies par l'utilisateur.

- Moyen : vous informe de tous les événements du réseau en rapport avec vos applications et vous permet de configurer votre système de sécurité

pour un rendement optimum. Si une application réseau sur votre ordinateur tente de connecter avec le réseau local ou Internet, le mode interactif sera activé. Les détails des applications et des opérations réseau seront affichés sur votre écran. En fonction de ces données, le logiciel vous offre le choix : autoriser ou bloquer pour cette fois l'événement, bloquer complètement l'activité de cette application, autoriser l'activité de l'application en fonction de son type, ou définir des paramètres de communication réseau supplémentaires. En fonction de votre réponse, le logiciel crée une règle pour cette application qui sera par la suite appliquée de manière automatique.

- Haut : interdit l'activité sur le réseau de toutes les applications, sauf de celles explicitement autorisées par des règles d'application définies par l'utilisateur. Lorsque ce niveau de sécurité est activé, la fenêtre interactive du logiciel n'est pas affichée, et toutes les tentatives d'établissement de connexions non définies par des règles utilisateur sont bloquées.

Rappelez-vous que toutes les applications installées après avoir activé ce niveau de sécurité sont par défaut interdites d'accès à Internet ou au réseau local.

- Bloquer tout : désactive toute communication de votre ordinateur avec Internet ou un réseau local. Ce niveau équivaut à la situation où votre ordinateur se trouve physiquement déconnecté, et toutes les tentatives d'établissement de connexions via Internet ou le réseau local sont bloqués.

Lorsque vous activez les niveaux **Haut**, **Moyen** ou **Bas** , vous pouvez activer la sécurité supplémentaire **Mode invisible** (reportez-vous au sous-chapitre 5.6 à la page 34). Ce mode n'autorise que les activités pour lesquelles vous avez pris l'initiative. Tous les autres types d'activités (accès depuis l'extérieur dans votre machine, interrogation de celle-ci à l'aide de l'utilitaire ping, etc.) sont interdits, à moins d'être explicitement autorisés par les règles utilisateur.

En pratique, cela veut dire que l'ordinateur devient « invisible » de l'extérieur. Les hackers perdent leur cible de vue et toutes leurs tentatives de pénétrer dans votre ordinateur sont vouées à l'échec. En outre, cette technique évite les attaques DoS (Refus de service) quel que soit leur type.

Par ailleurs, lorsque vous travaillerez sur le Web sous ce mode, vous ne percevrez aucune contrepartie négative : Kaspersky Anti-Hacker autorise l'activité sur le réseau lorsque l'initiative provient de votre machine.

Attention ! Le système de détection contre les intrusions est activé pour tous les niveaux de sécurité à l'exception de **Autoriser tout**. Mais vous pouvez si nécessaire le désactiver manuellement (reportez-vous au sous-chapitre 6.5.1 à la page 67).

4.3. Paramètres conseillés

Comment sélectionner le niveau de sécurité approprié et définir des règles pour des situations différentes ?

Quels composants de Kaspersky Anti-Hacker utiliser, et quel niveau de sécurité choisir ? La réponse dépend de la tâche que vous souhaitez accomplir.

Tâche 1. Comment protéger vos données contre des attaques de l'extérieur par Internet ?

Les deux méthodes suivantes sont principalement utilisées par les hackers pour dérober ou endommager les données d'un utilisateur via Internet : pénétration dans un ordinateur cible en profitant de défaillances logicielles de l'ordinateur, et infection d'un ordinateur cible à l'aide d'un cheval de Troie.

Si vous apprenez qu'il existe une défaillance dans une application installée dans votre machine, assurez-vous de créer une règle de blocage pour cette application. Nous vous conseillons de créer une règle de blocage complexe (reportez-vous au sous-chapitre 6.3.2.1 à la page 50) afin de prendre en compte cette défaillance.

Supposons que votre ordinateur est infecté par un cheval de Troie à travers une disquette ou par un message électronique, et que le programme malveillant tente de transmettre certaines données via Internet. Kaspersky Anti-Hacker sécurise facilement vos données en bloquant cette opération (niveau **Haut**), ou en vous informant de manière appropriée (niveau **Moyen**).

Attention ! Kaspersky Anti-Hacker ne protège pas votre ordinateur contre les virus ou les logiciels malveillants.

Par exemple, un cheval de Troie peut utiliser le logiciel de messagerie standard de votre ordinateur pour transférer ailleurs vos données confidentielles. Dans cette situation, Kaspersky Anti-Hacker ne sera pas en mesure d'empêcher ses agissements. En outre, si votre ordinateur est infecté par un virus ou un programme malveillant, vos données pourront être simplement détruites et votre ordinateur devenir une source de virus. Dans ce cas, Kaspersky Anti-Hacker ne peut que prévenir partiellement des conséquences de l'infection. Pour protéger efficacement votre système contre les virus et les programmes malveillants, nous vous conseillons d'utiliser un logiciel antivirus personnel comme Kaspersky Anti-Virus Personal, combiné avec Kaspersky Anti-Hacker. Nous vous conseillons également la création de règles d'application, afin que les applications de l'ordinateur n'exécutent que les activités strictement prévues par leur type. Il est également conseillé d'utiliser la liste des règles d'application pour affecter ces types d'activités aux applications strictement associées aux opérations autorisées. Vous réduirez ainsi au minimum le risque d'opérations réseau non autorisées dans votre machine.

Supposons que vous observez que votre ordinateur est constamment attaqué par certaine machine distante.

Tâche 2. Comment bloquer des attaques provenant de certaines adresses Internet ?

Vous pouvez interdire à votre ordinateur toute communication avec certaines adresses distantes en configurant des règles de filtrage de paquets appropriées. Par exemple, la Figure 12. Règle de blocage des communications avec une adresse suspecte vous montre la règle de blocage des communications avec l'adresse 111.111.111.111.

Pour éviter ce genre de situation, il est conseillé de laisser le système de détection contre les intrusions activé.

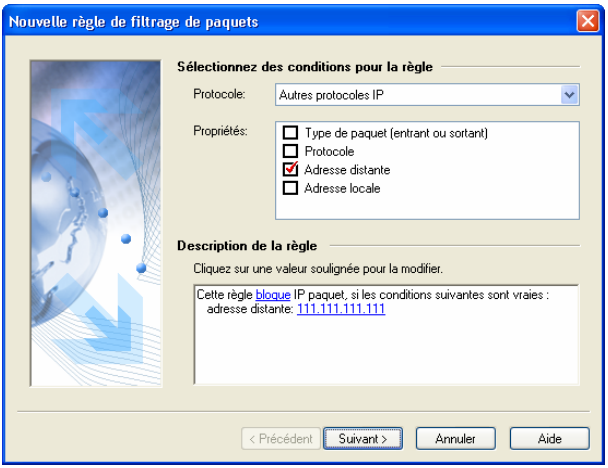


Figure 12. Règle de blocage des communications avec une adresse suspecte

Vous pouvez par exemple utiliser Kaspersky Anti-Hacker pour bloquer l'affichage de bannières sur les pages Web. Pour ce faire, créez une règle de filtrage de paquets pour bloquer les communications avec les sites Web qui les transmettent habituellement (par exemple, **linkexchange.ru**).

Supposons que vous craignez une attaque provenant du réseau local ou que vous souhaitez sécuriser vos données personnelles contre le vol.

Tâche 3. Surveillance des opérations sur le réseau local

L'ordinateur communique avec un réseau local au niveau du système d'exploitation. Par conséquent, il n'est pas toujours possible, d'identifier l'application concernée. Dans ce cas, la sécurisation de vos données passe par la création appropriée d'une règle de filtrage par paquets.

Pour simplifier la configuration du système de sécurité, Kaspersky Anti-Hacker préinstalle certaines règles de filtrage de paquets pour permettre les communications à travers le réseau local. Le réseau local est autorisé par défaut. Vous pouvez cependant redéfinir ces règles de filtrage, afin de bloquer complètement l'accès au réseau local, ou au contraire de le réserver à certains postes uniquement.

CHAPITRE 5. EXÉCUTION DU LOGICIEL

Comment démarrer l'application ? La fenêtre principale de l'application avec ses éléments. Quitter le logiciel.

5.1. Démarrage du logiciel

Kaspersky Anti-Hacker commence à protéger votre ordinateur aussitôt après l'ouverture d'une session de travail. Si vous quittez le logiciel, vous pouvez le lancer à nouveau manuellement.

Pour lancer Kaspersky Anti-Hacker, procédez comme suit :

1. Dans la barre des tâches du bureau de Windows, cliquez sur **Démarrer** et choisissez **Programmes**.

2. Sélectionnez le groupe correspondant à votre installation de Kaspersky Anti-Hacker. Par défaut, le nom du groupe d'applications est **Kaspersky Anti-Hacker**, à moins d'en avoir choisi un autre lors de l'installation. Sélectionnez ensuite **Kaspersky Anti-Hacker**.

3. Cliquez sur l'icône dans la barre d'état système avec le bouton gauche de la souris, ou encore, cliquez avec le bouton droit sur l'icône et sélectionnez **Ouvrir Kaspersky Anti-Hacker...** dans le menu présenté à l'écran.

La fenêtre principale de Kaspersky Anti-Hacker s'affiche à l'écran (reportez-vous au sous-chapitre 5.3 à la page 29).

Vous pouvez également lancer le logiciel directement à partir de son répertoire. Ouvrez l'explorateur de Windows et cherchez le répertoire de Kaspersky Anti-Hacker (le chemin d'accès par défaut est **C:\Program Files\Kaspersky Labs\Kaspersky Anti-Hacker**). Double-cliquez sur le fichier ***KAVPF.exe*** situé sous ce répertoire.

5.2. Menu Système

Icône dans la barre d'état système.
Menu Système.

Après son démarrage, le logiciel affiche l'icône  dans la barre d'état système.

Cliquez sur cette icône avec le bouton droit pour afficher le menu Système (Figure 13. Menu Système). Le menu Système contient les commandes suivantes :

Tableau 1

Menu →commandes	**Usage** (Cette commande...)
Ouvrir Kaspersky Anti-Hacker...	affiche la fenêtre principale de l'application.
Niveau de sécurité	bascule vers un autre niveau de sécurité : **Bloquer tout**, **Haut**, **Moyen**, **Bas**, **Autoriser tout**. Pour de plus amples détails sur les niveaux de sécurité, reportez-vous au sous-chapitre 4.2 à la page 22.
À propos de Kaspersky Anti-Hacker...	Affiche les détails du logiciel et des informations sur les clés utilisées.
Quitter	Décharge le logiciel de la mémoire de l'ordinateur.

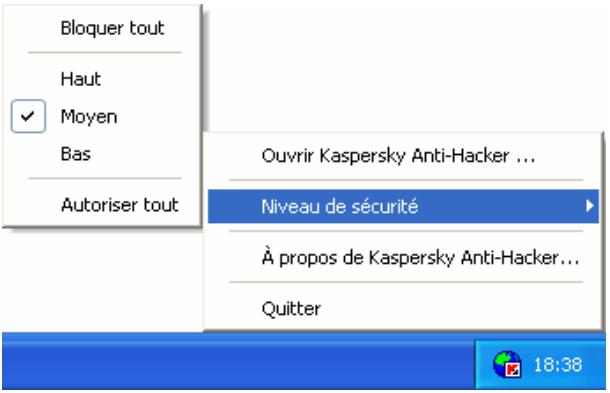


Figure 13. Menu Système

5.3. Fenêtre principale

Au démarrage de l'application, la fenêtre principale s'affiche à l'écran (Figure 14. La fenêtre principale de **Kaspersky Anti-Hacker**). La fenêtre principale de Kaspersky Anti-Hacker permet de sélectionner le niveau de sécurité, d'examiner l'état courant de votre système de sécurité, de modifier les paramètres de filtrage de paquets et d'examiner ou de configurer les journaux historiques.

Figure 14. La fenêtre principale de **Kaspersky Anti-Hacker**

La fenêtre principale de Kaspersky Anti-Hacker est composée des éléments suivants :

- Le menu ;
- La barre d'outils ;
- L'espace de travail ;
- La barre d'état.

5.4. Menus

Sur la partie supérieure de la fenêtre principale figure une *barre de menus*. Vous pouvez la faire glisser à l'aide de votre souris et la placer n'importe où à l'intérieur ou à l'extérieur de la fenêtre principale.

Certaines commandes de menu peuvent également être activées à l'aide des boutons correspondants de la barre d'outils. Pour de plus amples détails sur les fonctions associées aux boutons de la barre d'outils et aux commandes de menus, reportez-vous au sous-chapitre 5.5 à la page 32.

Tableau 2

Menu →commande	**Usage** (Cette commande...)
Service ⟶ Règles d'application	Affiche la fenêtre de règles d'application.
Service ⟶ Règles de filtrage de paquets	Ouvre la boîte de dialogue Règles de filtrage de paquets.

Menu →commande	**Usage** (Cette commande...)
Service ⟶ Niveau de sécurité	Sélectionne le niveau de sécurité nécessaire : • Bloquer tout • Haut • Moyen • Bas • Autoriser tout Vous pouvez également sélectionner le niveau de sécurité souhaité à l'aide des options présentes dans l'espace de travail. Pour de plus amples détails, reportez-vous au sous-chapitre 4.2 à la page 22.
Service⟶ Paramètres	Affiche une fenêtre permettant de configurer les journaux historiques de sécurité, le démarrage du système de sécurité et les paramètres de détection des attaques.
Service ⟶ Quitter	Décharge le logiciel de la mémoire de l'ordinateur.
Affichage ⟶ Barres d'outils	Permet de choisir parmi les options d'interface suivantes : • Barre d'outils Standard : affiche ou masque la barre d'outils Standard • Personnaliser : affiche une boîte de dialogue permettant de personnaliser l'interface graphique du logiciel
Affichage ⟶ Barre d'état	Affiche ou masque la barre d'état.

Menu →commande	**Usage** (Cette commande...)
Affichage ⟶ Journaux	Affiche la fenêtre du journal pour : • **Sécurité** • Activité des applications • Filtrage de paquets
Affichage ⟶ Afficher	Affiche des boîtes d'information avec les détails du système. • Applications actives : répertorie les applications réseau en exécution • Ports ouverts : répertorie les ports ouverts de votre machine; • Connexions établies : la liste des connexions établies.
Aide ⟶ À propos de Kaspersky Anti-Hacker...	Affiche les détails du logiciel et des informations sur les clés utilisées.
Aide ⟶ Kaspersky Anti-Hacker sur le Web	Ouvre la page Web officielle de Kaspersky Labs
Aide ⟶ Rubriques de l'aide...	Affiche les rubriques de l'aide.

5.5. Barre d'outils

La barre d'outils du logiciel se trouve sous la barre de menus. Si besoin, vous pouvez la faire glisser à l'aide de votre souris et la placer n'importe où à l'intérieur ou à l'extérieur de la fenêtre principale.

La *barre d'outils* contient des boutons. En cliquant sur les outils, il est possible de lancer plusieurs commandes. Vous pouvez également masquer ou afficher la barre d'outils en sélectionnant la commande **Standard** du sous-menu **Barres d'outils** du menu **Affichage**. Vous pouvez enfin ajouter ou supprimer des boutons de la barre d'outils (reportez-vous au sous-chapitre 5.10 à la page 36).

Tableau 3

Bouton	**Menu → Commande**	**Usage** (Ce bouton...)
	Service ⟶ Niveau de sécurité	Sélectionne le niveau de sécurité nécessaire : • Bloquer tout • Haut • Moyen • Bas • Autoriser tout Pour de plus amples détails, reportez-vous au sous-chapitre 4.2 à la page 22.
	Service ⟶ Règles d'application	Affiche la fenêtre de règles d'application.
	Service ⟶ Règles de filtrage de paquets	Ouvre la boîte de dialogue Règles de filtrage de paquets.
	Affichage ⟶ Journaux ⟶ Sécurité	Affiche la fenêtre du journal Sécurité.
	Affichage ⟶ Afficher ⟶ Applications actives	Répertorie les applications réseau en exécution.
	Affichage ⟶ Afficher ⟶ Ports ouverts	Répertorie les ports ouverts de votre machine.
	Affichage ⟶ Afficher ⟶ Connexions établies	Affiche la liste des connexions établies.

Bouton	Menu → Commande	Usage (Ce bouton...)
	Service⟶ Paramètres	Affiche une fenêtre permettant de configurer les journaux historiques de sécurité, le démarrage du système de sécurité et les paramètres de détection des attaques.
	Aide ⟶ Rubriques de l'aide...	Affiche les rubriques de l'aide.

5.6. Espace de travail

L'espace de travail de la fenêtre principale contient une *échelle de sécurité* et des informations sur l'état courant de votre système de sécurité.

L'échelle de sécurité vous permet de sélectionner l'un des niveaux de sécurité suivants :

- **Bloquer tout**
- **Haut**
- **Moyen**
- **Bas**
- **Autoriser tout**

Vous pouvez basculer vers un autre niveau de sécurité en faisant glisser le curseur le long de l'échelle. Une description détaillée du niveau de sécurité associé apparaît sur la droite du curseur (pour de plus amples détails reportez-vous au sous-chapitre 4.2 à la page 22) et les nouveaux paramètres sont appliqués immédiatement.

Lorsque vous activez les niveaux **Haut**, **Moyen** ou **Bas** , vous pouvez activer la sécurité supplémentaire **Mode invisible** (reportez-vous au sous-chapitre 4.2 à la page 22).

En dessous de l'échelle figurent des détails sur la dernière attaque de hackers détectée par le logiciel. Les informations indiquent la date et l'heure, le type et l'adresse de l'ordinateur source de l'attaque.

5.7. Barre d'état

Sur la partie inférieure de la fenêtre principale figure la *barre d'état.* Elle affiche des astuces sur l'élément actuellement sélectionné dans la fenêtre principale. Vous pouvez également masquer ou afficher la barre en sélectionnant la commande **Barre d'état** du menu **Affichage**.

5.8. Menu contextuel

Les menus contextuels permettent d'exécuter des commandes associées à une boîte de dialogue en particulier.

Pour afficher le menu contextuel de la boîte de dialogue, cliquez à l'intérieur avec le bouton droit de la souris.

5.9. Assistant de règles

L'assistant permettant la création ou l'édition des règles utilisateur est composé de nombreuses boîtes de dialogue. Chaque boîte de dialogue contient un certain nombre de boutons permettant de contrôler la création ou la modification des règles. Ces boutons sont :

- **Terminé** : applique les paramètres définis et crée la règle.
- **Annuler** : annule la procédure.
- **Suivant >** : passe à l'étape suivante de l'assistant.
- **< Précédent** : revient à l'étape précédente de l'assistant.
- Aide : affiche les rubriques de l'aide.

5.10. Modification et enregistrement des paramètres de l'interface

*Pour modifier les paramètres de l'interface, sélectionnez **Personnaliser** dans le sous-menu **Barres d'outils** du menu **Affichage**.*

La boîte de dialogue **Personnaliser** s'affiche à l'écran (Figure 15. Boîte de dialogue **Personnaliser**).

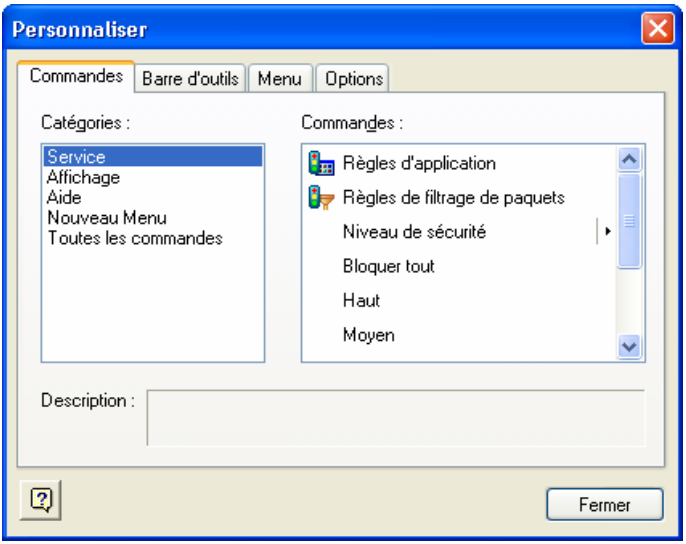


Figure 15. Boîte de dialogue **Personnaliser**

Pour modifier l'interface, nous vous conseillons d'organiser votre écran pour que la boîte de dialogue **Personnaliser** ne recouvre pas la barre de menus et la barre d'outils de la fenêtre principale.

Utilisez l'onglet **Commandes** pour modifier la présentation des menus et barres d'outils de la fenêtre principale. Pour ajouter une nouvelle commande, faites glisser la commande souhaitée dans la liste vers la barre de menus ou vers la barre d'outils. Pour supprimer une commande de la barre de menus ou de la barre d'outils, faites-la glisser en dehors de la fenêtre principale.

Les onglets **Barre d'outils** et **Menu** permettent de rétablir l'apparence originale de votre barre d'outils et de vos menus, respectivement.

L'onglet **Options** permet d'activer ou désactiver les info-bulles des boutons de la barre d'outils, de choisir leur taille et de définir la présentation de votre barre de menus.

Si besoin, vous pouvez modifier les titres des commandes de menu et des boutons, afficher les boutons sous forme d'image, ou de texte.

Pour modifier le titre ou les autres propriétés d'une commande ou d'un bouton, procédez comme suit :

1. Ouvrez la boîte de dialogue **Personnaliser** et sélectionnez la commande (ou le bouton) souhaitée dans la fenêtre principale.

2. Cliquez avec le bouton droit de la souris. Sélectionnez la commande souhaitée dans le menu contextuel à l'écran :

    - **Supprimer** : supprime le bouton ou la commande de menu sélectionné(e).

    - **Apparence des boutons** : permet de modifier le libellé. Une boîte de dialogue avec le même libellé s'affiche à l'écran. Modifiez le libellé du bouton ou de la commande de menu dans le champ **Texte du bouton** (Figure 16. Modification des propriétés de commandes). Cliquez sur **Ok**.

    - **Image** : affiche le bouton ou la commande de menu sous forme d'image.

    - **Texte** : affiche le bouton ou la commande de menu sous forme de texte.

    - **Image et texte** : affiche la commande de menu ou le bouton avec une image et du texte.

    - **Commencer un groupe :** insère un séparateur juste avant la commande de menu (ou le bouton) sélectionnée.

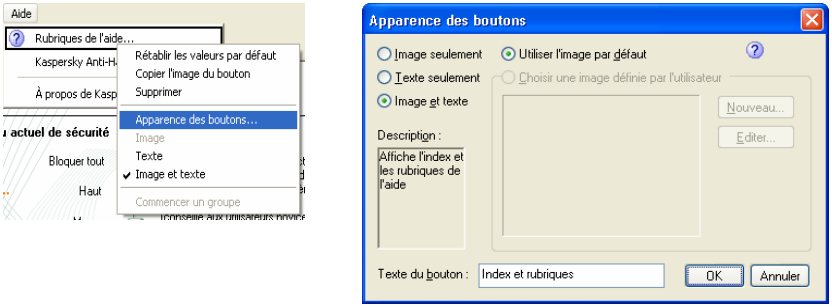


Figure 16. Modification des propriétés de commandes

Les paramètres de la nouvelle interface sont enregistrés automatiquement et appliqués immédiatement après les modifications. Ces modifications seront conservées pour toutes les sessions ultérieures avec l'application.

5.11. Quitter l'application

Pour décharger l'application de la mémoire de l'ordinateur, sélectionnez **Quitter** dans le menu système ou dans le menu **Service** de la fenêtre principale. Vous pouvez également fermer la fenêtre principale en cliquant sur dans l'angle supérieur droit de la fenêtre.

Cependant, si la case **Afficher l'icône de l'application dans la barre d'état système** est cochée, le logiciel n'est pas déchargé de la mémoire de l'ordinateur lorsque vous fermez la fenêtre principale de l'application. Cette case est cochée par défaut, mais vous pouvez la désactiver le cas échéant (reportez-vous au sous-chapitre 6.1.1 à la page 39). En plaçant l'icône dans la barre d'état système, le logiciel signale sa présence dans la mémoire de l'ordinateur.

CHAPITRE 6. ACTIVATION ET DÉFINITION DES PARAMÈTRES DU SYSTÈME DE SÉCURITÉ

6.1. Activation du système de sécurité et sélection du niveau de sécurité

Comment activer la sécurité de l'ordinateur avec Kaspersky Anti-Hacker ? Comment sélectionner le niveau de sécurité nécessaire ?

6.1.1. Activation du système de sécurité

Votre système de sécurité est activé aussitôt après l'installation de Kaspersky Anti-Hacker et le redémarrage de l'ordinateur. Après son démarrage, le logiciel affiche l'icône  dans la barre d'état système. Par défaut, le logiciel applique le niveau **Moyen** et si une application de votre ordinateur tente de connecter avec le réseau local ou Internet, le mode interactif est activé. Le détail des applications et des opérations réseau est présenté à l'écran. En fonction de ces données, le logiciel vous offre le choix : autoriser ou bloquer pour cette fois l'événement, bloquer complètement toute activité de l'application, autoriser l'activité de l'application en fonction de son type, ou définir une règle complexe pour cet événement. En fonction de votre réponse, le logiciel crée une règle pour cette application qui sera par la suite appliquée de manière automatique.

Kaspersky Anti-Hacker commence à protéger votre ordinateur aussitôt après l'ouverture d'une session de travail. Vous pouvez cependant paramétrer le logiciel pour que la sécurité soit activée juste après le démarrage du système d'exploitation Windows.

Pour lancer et activer Kaspersky Anti-Hacker immédiatement après le démarrage du système d'exploitation, procédez comme suit :

1. Sélectionnez **Paramètres** dans le menu **Service**.

2. Dans l'onglet **Général** de la boîte de dialogue **Paramètres** (Figure 17. Boîte de dialogue **Paramètres**), cochez la case **Activer le système de sécurité au démarrage**. Dans ce cas, le logiciel est lancé avec les paramètres utilisateur immédiatement après le démarrage du système d'exploitation, mais la journalisation restera cependant désactivée. Si le logiciel utilise le niveau **Moyen**, toutes les communications réseau seront automatiquement autorisées jusqu'à ce que vous ouvriez une session sur le poste de travail, parce que la fenêtre interactive ne peut pas être affichée sans la présence d'un utilisateur dans le système. Dans l'intervalle, les niveaux **Bas** ou **Autoriser tout**, autoriseront les communications réseau inconnues, tandis que les autres niveaux sécurité les bloqueront.

Supposons que votre ordinateur est connecté à un réseau local et que vous activez le logiciel pour qu'il lance le système de sécurité juste après le démarrage du système d'exploitation. Par ailleurs, vous avez bloqué tout le trafic du réseau avec le niveau de sécurité **Bloquer tout**, ou avec une règle de filtrage de paquets applicable pour tous les niveaux de sécurité (à l'exception du niveau **Autoriser tout**). Dans ce cas, vous attendrez plus longtemps que d'habitude avant de vous connecter au système, et une fois connecté, vous découvrirez que le réseau local n'est pas disponible.

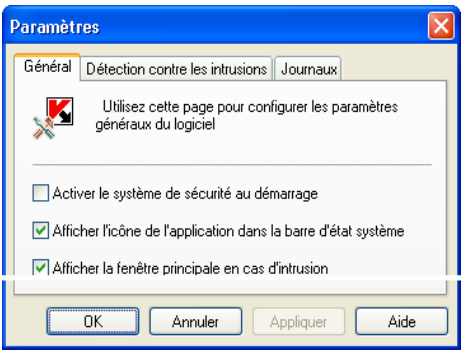


Figure 17. Boîte de dialogue **Paramètres**

Vous pouvez modifier l'affectation du bouton dans l'angle supérieur droit de la fenêtre principale. Par défaut, ce bouton permet de réduire la fenêtre principale à une icône dans la barre d'état système, en conservant le logiciel dans la mémoire de l'ordinateur.

Pour modifier l'affectation du bouton pour qu'il décharge le logiciel de la mémoire de l'ordinateur lors de la fermeture de la fenêtre principale, procédez comme suit :

1. Sélectionnez **Paramètres** dans le menu **Service**.

2. Dans l'onglet **Général** de la boîte de dialogue **Paramètres** (Figure 17. Boîte de dialogue **Paramètres**) annulez la coche de la case **Afficher l'icône de l'application dans la barre d'état système**.

Par défaut, si le logiciel détecte une attaque contre votre machine, la fenêtre principale s'ouvre en affichant un message associé.

Pour désactiver l'affichage de la fenêtre principale chaque fois qu'une intrusion est détectée, procédez comme suit :

1. Sélectionnez **Paramètres** dans le menu **Service**.

2. Dans l'onglet **Général** de la boîte de dialogue **Paramètres** (Figure 17. Boîte de dialogue **Paramètres**) annulez la coche de la case **Afficher la fenêtre principale en cas d'intrusion**.

6.1.2. Sélection du niveau de sécurité

Vous pouvez modifier le niveau de sécurité en faisant glisser le curseur le long de l'échelle dans la fenêtre principale de l'application, ou en sélectionnant la commande **Niveau de sécurité** dans le menu **Service**. Vous pouvez également sélectionner la commande correspondante du menu Système.

Vous pouvez basculer vers l'un des niveaux de sécurité suivants :

- **Bloquer tout**
- **Haut**
- **Moyen**
- **Bas**
- **Autoriser tout**

Lorsque l'un des niveaux **Haut**, **Moyen** ou **Bas** est activé, vous pouvez en plus cocher la case correspondante au mode de sécurité **invisible**.

Les niveaux de sécurité sont appliqués aussitôt après leur sélection par l'utilisateur.

Pour de plus amples détails sur les niveaux de sécurité disponibles, reportez-vous au sous-chapitre 4.2 à la page 22.

6.1.3. Avertissement d'événement réseau

Si vous cochez la case **Afficher l'avertissement** après avoir créé une règle (reportez-vous au sous-chapitre 6.3.2.3 à la page 59, et au sous-chapitre 6.4.2.2 à la page 66), le logiciel affichera le message associé à chaque exécution de la règle (Figure 18. Exemple d'avertissement de Kaspersky Anti-Hacker).

Reportez-vous à la Figure 18. Exemple d'avertissement de Kaspersky Anti-Hacker pour un exemple de message présenté lors de l'application de la règle de filtrage de paquets appropriée. Le message donne la description des adresses distante et locale associées ainsi que les ports utilisés.

Vous pouvez examiner la règle de filtrage correspondante en cliquant sur le lien.

Vous pouvez également désactiver les avertissements ultérieurs pour ce même événement. Pour ce faire, cochez la case **Ne pas afficher cet avertissement**.

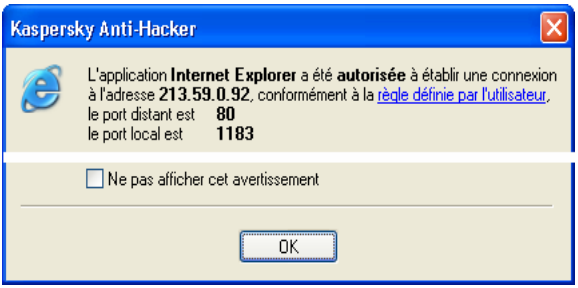


Figure 18. Exemple d'avertissement de Kaspersky Anti-Hacker

Lors de la création d'une règle, cochez la case **Enregistrer l'événement** si vous souhaitez enregistrer l'évènement correspondant.

6.1.4. Fenêtre interactive (niveau de sécurité Moyen)

La fenêtre interactive (Figure 19. Exemple de fenêtre interactive) est affichée chaque fois que le logiciel détecte un événement inconnu et que le mode de sécurité **Moyen** est sélectionné.

Sur la partie supérieure de la boîte de dialogue figure le nom de l'application qui demande la connexion avec une machine distante, ainsi que l'adresse et les numéros de port de cette machine. Vous pouvez si besoin obtenir des détails sur la connexion demandée en cliquant sur le lien **...détails**.

Pour autoriser ou bloquer cette opération concrète, cliquez sur **Autoriser une fois** ou **Bloquer une fois**, respectivement.

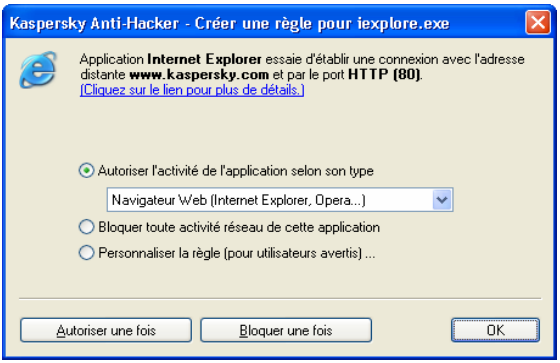


Figure 19. Exemple de fenêtre interactive

Si vous fermez la fenêtre interactive en cliquant sur ☒ dans l'angle supérieur droit, l'opération en question sera bloquée pour cette fois.

Pour définir une règle permettant de contrôler par la suite les événements générés par cette application, choisissez l'une des actions répertoriées et cliquez sur **Ok**. Ce faisant, la nouvelle règle sera ajoutée à votre liste de règles d'application.

- Autoriser l'activité de cette application selon son type. Cette action autorise uniquement les communications réseau compatibles avec la catégorie d'application spécifiée. Sélectionnez le type souhaité dans la liste déroulante (pour de plus amples détails, reportez-vous au sous-chapitre 6.3.2.1 à la page 50).

- Désactiver toute activité réseau de l'application. Cette action empêche l'application spécifiée de réaliser tout type d'activité sur le réseau, y compris l'opération décrite.

- Personnaliser la règle... – Cette action permet de spécifier les opérations autorisées pour l'application. Si vous choisissez cette option puis cliquez sur Ok, la boîte de dialogue de l'assistant de règles s'affiche à l'écran (pour de plus amples détails sur l'assistant, reportez-vous au sous-chapitre 6.3.2 à la page 50).

Si vous créez une règle qui ne correspond pas à l'événement décrit, le message correspondant s'affiche à l'écran (Figure 20. La règle que vous avez créée ne correspond pas à l'événement courant). Vous pouvez ensuite cliquer sur **Oui** pour ajouter la nouvelle règle à la liste, ou sur **Non**, en cas d'erreur. Dans les deux cas, l'application vous invite à sélectionner une autre option dans la liste de la fenêtre interactive.

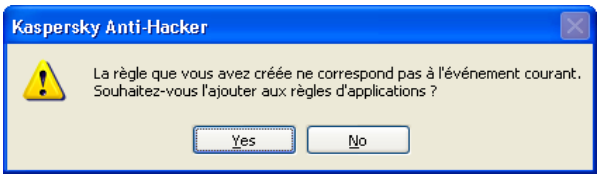


Figure 20. La règle que vous avez créée ne correspond pas à l'événement courant

Remarque : si de nombreux logiciels dans votre ordinateur tentent d'effectuer pendant une courte période de temps des opérations réseau non prévues par les règles utilisateur, il se forme une *queue de requêtes* de création de règles. Ces requêtes afficheront à tour de rôle la fenêtre interactive. Vous devez alors définir la réponse du logiciel aux actions de la première des applications, puis à celles de la seconde, et ainsi de suite. Toutes les applications de la queue resteront en attente de votre décision.

6.1.5. Avertissement de remplacement d'un module exécutable

Kaspersky Anti-Hacker protège vos applications réseau contre les tentatives non autorisées de remplacement de ses propres fichiers exécutables originaux. Lorsqu'une tentative de remplacement est détectée, Kaspersky Anti-Hacker affiche l'avertissement approprié (Figure 21. Avertissement de remplacement d'un module exécutable).

Vous avez le choix parmi les options suivantes :

- Bloquer toute activité ultérieure de l'application : toute opération réseau ultérieure est bloquée pour cette application. La règle de blocage appropriée sera ajoutée en début de liste et toutes les autres règles d'application seront désactivées. Nous vous conseillons de lancer votre logiciel antivirus afin d'analyser la présence d'un virus dans cette application, de la récupérer depuis un copie de sauvegarde ou de la réinstaller directement. Ensuite, supprimez la règle de blocage, puis réactivez les autres règles dans la liste des règles d'application. Si Kaspersky Anti-Hacker affiche à nouveau le message indiquant que le module exécutable a été remplacé, choisissez l'option ci-dessous.

- Je suis au courant de la modification du fichier ; je continue de faire confiance à l'application : toutes les règles utilisateur disponibles pour l'application seront également valables pour le fichier modifié.

Cliquez sur **Ok**.

Figure 21. Avertissement de remplacement d'un module exécutable

6.2. Comment réagit l'application en cas d'attaque ?

Qu'arrive-t-il lorsqu'une attaque externe est détectée par le système de sécurité ?

Lorsque le système de sécurité détecte une attaque de hacker contre votre machine, il affiche la fenêtre principale de l'application (si la case **Afficher la fenêtre principale en cas d'intrusion** est cochée. Reportez-vous au sous-chapitre 6.1.1 à la page 39). Dans cette éventualité, assurez-vous de lire soigneusement les détails sur l'attaque au bas de la fenêtre ; le logiciel indique la date, l'heure et le type d'attaque (Figure 24. La première boîte de dialogue de l'assistant de règles d'application).

Une telle attaque est bloquée. Le logiciel bloque également la machine de l'assaillant pendant la durée définie dans les paramètres (reportez-vous au sous-chapitre 6.5 à la page 67).

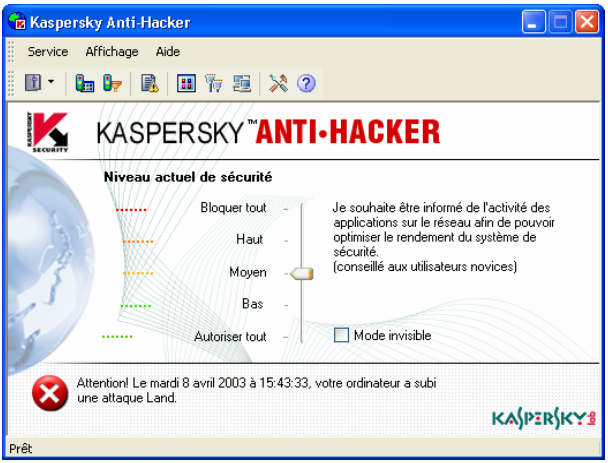


Figure 22. Exemple de message de détection d'attaque

Supposons que vous observez que votre ordinateur est constamment attaqué par une certaine machine distante. Vous pouvez interdire à votre ordinateur toute communication avec certaines adresses distantes en configurant des règles de filtrage de paquets appropriées (reportez-vous au sous-chapitre 6.4 à la page 60).

En cas d'attaques fréquentes en provenance d'une certaine adresse distante, nous vous conseillons de basculer vers le niveau de sécurité **Bloquer tout** et d'en informer votre administrateur système ou votre fournisseur Internet.

6.3. Personnalisation des règles d'application

Comment créer une règle d'application ? L'assistant de règles d'application

6.3.1. Utilisation de la liste de règles

Pour afficher la liste des règles d'application sur votre écran,

Sélectionnez **Règles d'application** dans le menu **Service**.

La boîte de dialogue **Règles d'application** s'affiche à l'écran (Figure 23. Boîte de dialogue **Règles d'application**).

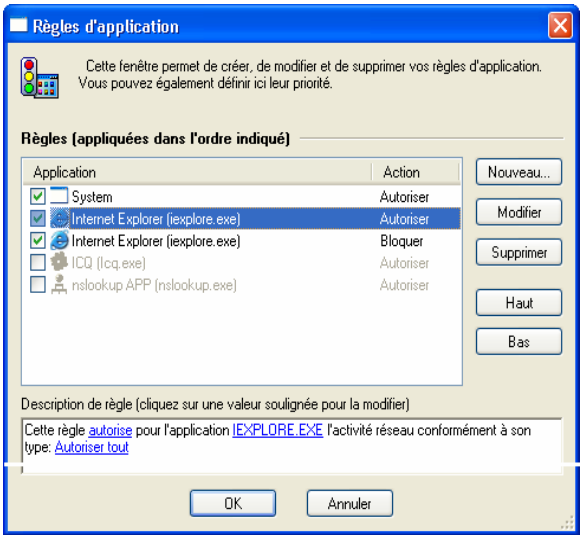


Figure 23. Boîte de dialogue **Règles d'application**

Dans la partie supérieure de la boîte de dialogue se trouve la liste des règles d'application. La colonne **Application** contient les icônes et les noms des applications associées ainsi qu'une case permettant d'activer ou de désactiver

les règles. La colonne **Action** contient les détails des actions effectuées par la règle correspondante : **Autoriser** pour les règles permettant certains événements, et **Bloquer** pour celles qui au contraire les bloquent.

Les règles sont classées en fonction de leur priorité. La règle en début de liste sera appliquée la première, et uniquement alors, le logiciel appliquera la seconde, et ainsi de suite. Si une application tente d'exécuter une opération réseau, le logiciel parcours la liste au complet à la recherche d'une règle correspondant à ce type d'opération. Si aucune règle correspondante n'est reconnue, l'action par défaut est alors appliquée (reportez-vous au sous-chapitre 4.2 à la page 22). Par conséquent, si vous souhaitez bloquer certaines opérations uniquement pour une application, vous devez créer deux règles : la première règle spécifiera que cette application pourra exécuter, tandis que la seconde bloquera toutes les autres opérations. En outre, la première règle doit figurer avant la seconde dans la liste des règles. En procédant ainsi, lorsque votre application tentera d'exécuter une opération autorisée, Kaspersky Anti-Hacker retrouvera la règle qui l'y autorise au cours de sa recherche dans la liste des règles. Si l'opération n'est pas désirée, Kaspersky Anti-Hacker appliquera en revanche la seconde règle, qui bloque toutes les opérations de cette application.

Par exemple, la Figure 23. Boîte de dialogue **Règles d'application**, la troisième règle d'application bloque l'accès Internet de l'application Internet Explorer, mais la seconde l'autorise à communiquer par Internet en utilisant le protocole HTTP. Dans la mesure où la seconde règle possède une priorité plus élevée que la troisième, Internet Explorer est autorisé à communiquer avec des serveurs HTTP distants (et uniquement avec eux).

Rappelez-vous que seules les règles dont les cases sont cochées sont exécutées. Par exemple, dans la Figure 23. Boîte de dialogue **Règles d'application** les cases des quatrième et cinquième règles ne sont pas cochées.

Pour activer ou désactiver une règle d'application,

Activez ou désactivez la case correspondante dans la liste des règles d'application.

À droite de la liste de règles se trouvent les boutons suivants :

- Nouveau... – permet de créer une nouvelle règle. Si vous cliquez sur ce bouton, la boîte de dialogue de l'assistant de règles d'application s'affiche à l'écran.

- Modifier : permet de modifier la règle sélectionnée. Si vous cliquez sur ce bouton, la boîte de dialogue de l'assistant de règles d'application s'affiche à l'écran.

- Supprimer : supprime la règle sélectionnée de la liste.
- Haut : déplace la règle sélectionnée une ligne vers le haut, ce qui augmente sa priorité.
- Bas : déplace la règle sélectionnée une ligne vers le bas, ce qui diminue sa priorité.

Pour modifier une règle sélectionnée dans la liste, vous pouvez également utiliser la touche **<ENTRÉE>** ou double-cliquer sur la règle. Pour supprimer cette règle, utilisez la touche **<SUPPR>**. Enfin, pour ajouter une nouvelle règle, utilisez la touche **<INS>**.

Vous pouvez également modifier la liste à partir du menu contextuel, qui comprend les commandes suivantes :

- Modifier : permet de modifier la règle sélectionnée.
- Supprimer : supprime la règle sélectionnée de la liste.
- Dupliquer la règle : crée une copie de la règle sélectionnée. La copie sera placée juste après la règle sélectionnée.

En dessous de la liste, la section **Description de la règle** contient les détails de la règle sélectionnée dans la section supérieure. Comme la même section se retrouve dans les dialogues de l'assistant de règles, nous allons en parler ici avec un peu plus de détail.

La description de la règle contient du texte en noir qui n'est pas modifiable, et du texte en bleu qu'il faut remplacer par les valeurs appropriées. Lorsque certains paramètres sont présentés en gras, cela veut dire que leur valeur est essentielle pour la règle.

Pour saisir ou modifier la valeur requise dans la description de la règle,

1. Cliquez sur le lien souligné approprié dans la section **Description de la règle**.
2. Dans la boîte de dialogue qui s'affiche à l'écran, sélectionnez la valeur souhaitée (pour de plus amples détails, reportez-vous aux sous-chapitres suivants).

Sur la partie inférieure de la boîte de dialogue **Règles d'application** se trouvent les boutons suivants :

- Ok : referme la boîte de dialogue et enregistre les modifications apportées.

- Annuler : referme la boîte de dialogue sans enregistrer les modifications.

Toutes les modifications apportées à la liste sont appliquées immédiatement après leur enregistrement.

6.3.2. Ajout d'une nouvelle règle

Pour lancer l'assistant de règles d'application:

Cliquez sur **Nouveau...** dans la boîte de dialogue **Règles d'application** (Figure 23. Boîte de dialogue **Règles d'application**).

6.3.2.1. Étape 1. Personnalisation de la règle

Lorsque vous lancez l'assistant, une boîte de dialogue comme celle de la Figure Figure 24. La première boîte de dialogue de l'assistant de règles d'application s'affiche à l'écran.

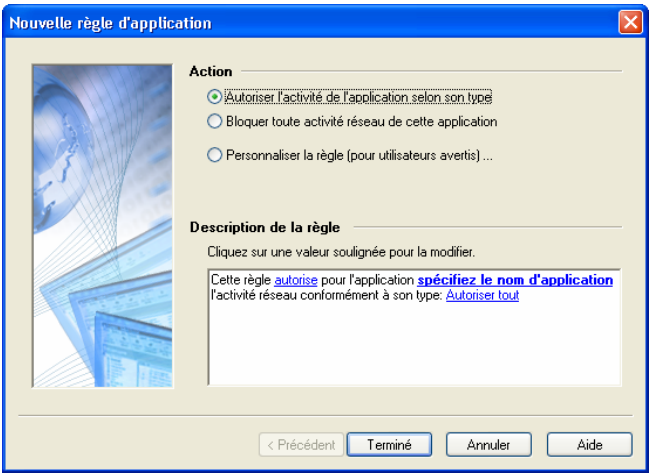
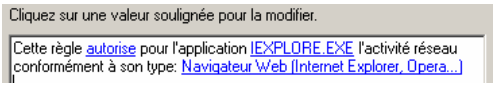
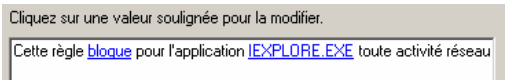
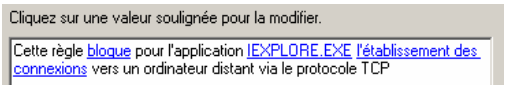


Figure 24. La première boîte de dialogue de l'assistant de règles d'application

La liste **Action** vous donne le choix entre les trois options suivantes :

Action	Description de la règle
• **Autoriser l'activité de l'application selon son type.**	
• **Désactiver toute activité réseau de l'application.**	
• **Personnaliser la règle.**	

Si vous sélectionnez **Personnaliser la règle**, la boîte de dialogue suivante de l'assistant peut vous suggérer de définir des paramètres supplémentaires.

- Type d'application Internet (client ou serveur)
- Protocole
- Adresse distante
- Port distant
- Port local

Pour créer une règle autorisant l'activité de l'application selon son type:

1. Sélectionnez **Autoriser l'activité de l'application selon son type** dans la liste d'options de la section **Action**.

2. Cliquez sur le lien **spécifiez le nom d'application** dans la section **Description de la règle**. Spécifiez le nom de l'application requise dans la boîte de dialogue **Spécifier le type d'application** sur l'écran.

3. Définissez le type d'application en cliquant sur le lien approprié dans la section **Description de la règle**. La valeur par défaut est **Autoriser tout** ce qui n'impose aucune limitation aux privilèges de l'application. Pour modifier cette valeur, cliquez sur l'application et sélectionnez une autre valeur dans la liste déroulante de la boîte de dialogue **Spécifier le type d'application** (Figure 25. Sélection du type d'application). Cliquez ensuite sur **Ok**.

- Navigateur Web : pour Internet Explorer, Netscape Navigator et d'autres navigateurs Web. Autorise les communications via les protocoles HTTP, HTTPS, FTP et les serveurs proxy.

- Transfert de fichiers : pour des logiciels comme Reget, Gozilla et similaires. Autorise les communications via les protocoles HTTP, HTTPS, FTP, TFTP et les serveurs proxy standard.

- Messagerie : pour MS Outlook, MS Outlook Express, the Bat et autres logiciels de messagerie. Autorise les communications via les protocoles SMTP, NNTP, POP3, IMAP4.

- News : pour les logiciels Forte Agent et autres. Autorise les communications via les protocoles SMTP et NNTP.

- Messagerie instantanée : pour des logiciels de chat comme ICQ, AIM et d'autres. Autorise les communications via le serveur proxy standard ainsi que les connexions directes ordinateur à ordinateur.

- Internet Relay Chat : pour des logiciels comme mIRC et similaires. Autorise l'authentification standard de l'utilisateur sur des réseaux IRC et l'accès aux ports des serveur IRC.

- Télé-réunions d'affaires : pour MS NetMeeting et autres logiciels semblables. Autorise les communications via les protocoles HTTP et HTTPS et les serveurs proxy standard. Cette catégorie prend également en charge les communications avec le réseau local (LDAP et autres).

- Administration à distance : pour Telnet, etc. Autorise les communications via les protocoles Telnet et SSH.

- Synchronisation de l'heure : pour des logiciels comme Timehook et similaires. Autorise les connexions aux serveurs de date et heure.

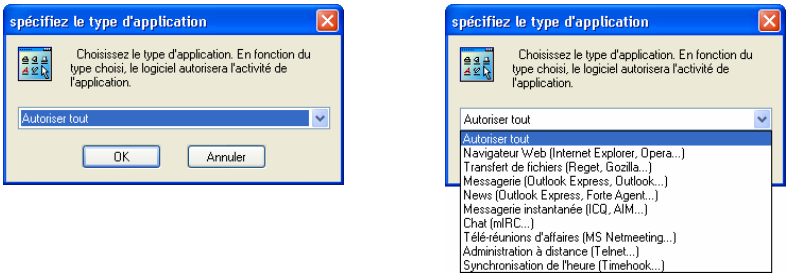


Figure 25. Sélection du type d'application

Pour bloquer toutes communications de l'application avec le réseau,

1. Sélectionnez **Désactiver toute activité de l'application** dans la liste des options de la section **Action**.

2. Cliquez sur le lien **spécifiez le nom d'application** dans la section **Description de la règle**. Spécifiez le nom de l'application requise dans la boîte de dialogue **Spécifier le type d'application** sur l'écran.

Si les paramètres précédents ne vous permettent pas de créer la règle souhaitée (si par exemple vous souhaitez autoriser les communications avec une adresse IP déterminée), vous pouvez configurer une règle plus complexe.

Pour configurer une règle complexe, procédez comme suit :

1. Sélectionnez **Personnaliser la règle** dans la liste d'options de la section **Action**.

2. Cliquez sur le lien **spécifiez le nom d'application** dans la section **Description de la règle**. Spécifiez le nom de l'application requise dans la boîte de dialogue **Spécifier le type d'application** sur l'écran.

3. Cliquez sur le lien **Autoriser tout** dans la section **Description de la règle**. Sélectionnez l'action souhaitée dans la liste d'options de la boîte de dialogue **Spécifier une action** (Figure 26. Sélection de l'action) puis cliquez sur **Ok** :

    - **Bloquer tout**
    - **Autoriser tout**

4. Sélectionnez l'activité de l'application à surveiller et contrôler à l'aide de cette règle ; établissement (par défaut) ou réception de connexion. Pour modifier l'activité par défaut, cliquez sur le lien **l'établissement de connexions** dans la section **Description de la règle**. Sélectionnez l'option **Réception d'une connexion réseau entrante depuis une machine distante** dans la boîte de dialogue **Sélectionner le type d'activité de l'application** (Figure 27. Sélection du type d'activité de l'application) puis cliquez sur **Ok**.

Après avoir choisi toutes les options dans la première étape de l'assistant, cliquez sur **Suivant >**.

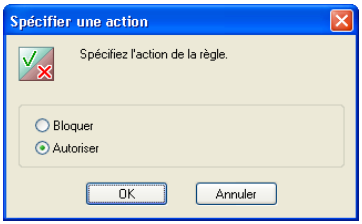


Figure 26. Sélection de l'action

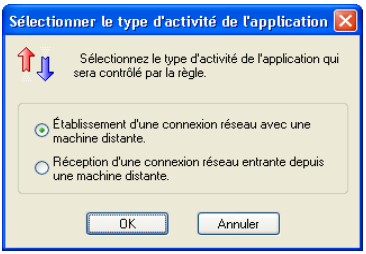


Figure 27. Sélection du type d'activité de l'application

Si vous cliquez sur **Suivant >** mais n'avez pas sélectionné d'application, un message vous invitant à le faire s'affiche à l'écran.

6.3.2.2. Étape 2. Conditions de la règle

L'assistant des conditions de la règle s'affiche à l'écran si vous avez sélectionné **Personnaliser la règle** à la première étape de l'assistant.

Dans cet assistant, vous spécifiez le protocole, l'adresse de la machine distante et les ports utilisés.

La liste déroulante **Protocole :** de cette boîte de dialogue contient les protocoles prédéterminés suivants ainsi que les numéros de ports correspondants :

- HTTP
- IMAP
- SMTP
- NNTP
- POP3
- DNS

Si vous souhaitez définir un autre numéro de port, sélectionnez l'une des entrées de la liste déroulante suivante :

- **Autre protocole sur TCP** : pour des services utilisant le protocole TCP
- **Autre protocole sur UDP** : pour des services utilisant le protocole UDP

La liste **Paramètres** contient des paramètres supplémentaires, et son contenu dépend directement du protocole choisi dans la liste déroulante précédente.

Adresse distante : l'adresse de l'ordinateur distant associé à la communication. Pour définir l'adresse, cliquez sur le lien **spécifiez l'adresse** correspondant dans la section **Description de la règle**. Pour spécifier plus d'une adresse, maintenez enfoncée la touche **<CTRL>** puis cliquez sur le lien. Pour de plus amples détails, reportez-vous au sous-chapitre 6.3.2.2.1 à la page 56.

Port distant : le numéro de port distant. Pour spécifier le port, cliquez sur le lien **spécifiez le port** dans la section **Description de la règle**. Pour spécifier plus d'un port, maintenez enfoncée la touche **<CTRL>** puis cliquez sur le lien. Pour de plus amples détails, reportez-vous au sous-chapitre 6.3.2.2.2 à la page 58.

Port local : le numéro de port local. Pour spécifier le port, cliquez sur le lien **spécifiez le port** dans la section **Description de la règle**. Pour spécifier plus d'un port, maintenez enfoncée la touche **<CTRL>** puis cliquez sur le lien. Pour de plus amples détails, reportez-vous au sous-chapitre 6.3.2.2.2 à la page 58.

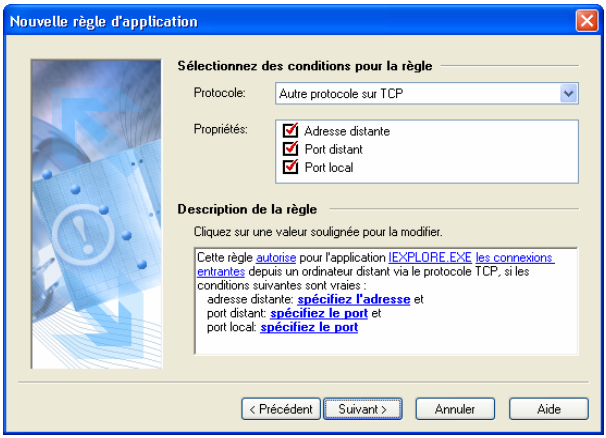


Figure 28. Définition des conditions de la règle

6.3.2.2.1. Définition de l'adresse ou de la plage d'adresses

Pour définir les adresses souhaitées, vous devez utiliser deux boîtes de dialogue.

La boîte de dialogue **Spécifier une adresse ou plage d'adresses** (Figure 29. Boîte de dialogue **Spécifier une adresse ou plage d'adresses**) apparaît lorsque vous maintenez enfoncée la touche **<CTRL>** et cliquez sur le lien **spécifiez l'adresse** à la seconde étape de l'assistant de règles.

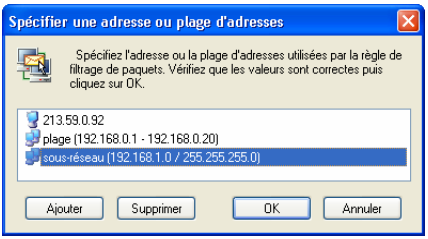


Figure 29. Boîte de dialogue **Spécifier une adresse ou plage d'adresses**

Utilisez ici les boutons **Ajouter** et **Supprimer** pour ajouter le nombre souhaité d'adresses ou de plages d'adresses d'ordinateurs, des adresses de sous-réseau. Une fois la configuration de la liste d'adresses terminée, cliquez sur **Ok** et retournez à la boîte de dialogue de l'assistant de règles.

Lorsque vous cliquez sur **Ajouter** dans la boîte de dialogue **Spécifier une adresse ou plage d'adresses**, la boîte de dialogue **Spécifier une adresse** (Figure 30. Boîte de dialogue **Spécifier une adresse** avec l'option **Adresse d'ordinateur.**) s'affiche à l'écran. La même boîte de dialogue apparaît lorsque vous cliquez sur le lien **spécifiez l'adresse** du second assistant de règles, sans enfoncer la touche **<CTRL>**.

La boîte de dialogue **Spécifier une adresse** permet de spécifier l'adresse, la plage d'adresses ou l'adresse de sous-réseau utilisée dans la règle (Figure 30. Boîte de dialogue **Spécifier une adresse** avec l'option **Adresse d'ordinateur.**).

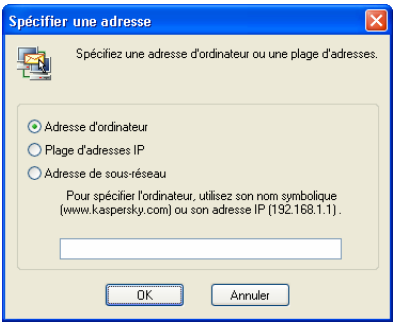


Figure 30. Boîte de dialogue **Spécifier une adresse** avec l'option **Adresse d'ordinateur**.

Vous avez le choix parmi les options suivantes :

- Adresse d'ordinateur : désignez l'ordinateur d'après son adresse symbolique (www.kaspersky.com) ou son adresse IP (192.168.1.1).
- Plage d'adresses IP : spécifiez la plage d'adresses dans les champs Commence par : et **Termine par :** (Figure 31. Boîte de dialogue **Spécifier une adresse** avec l'option Plage d'adresses IP).
- Adresse de sous-réseau : spécifiez l'adresse de sous-réseau dans le champ Adresse de sous-réseau : et le cas échéant, le masque de sous-réseau dans le champ Masque de sous-réseau : (Figure 32. Boîte de dialogue **Spécifier une adresse** avec l'option Adresse de sous-réseau).

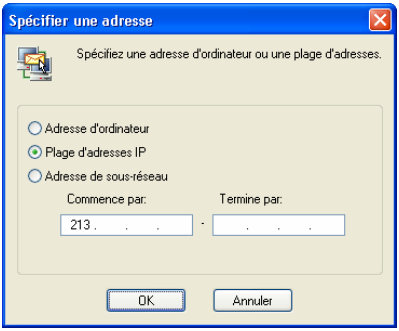


Figure 31. Boîte de dialogue **Spécifier une adresse** avec l'option **Plage d'adresses IP**

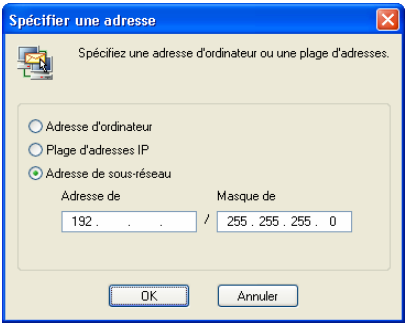


Figure 32. Boîte de dialogue **Spécifier une adresse** avec l'option **Adresse de sous-réseau**

Après avoir indiqué l'adresse requise, cliquez sur **Ok**.

6.3.2.2.2. Définition d'un port ou d'une plage de ports

Deux boîtes de dialogue permettent de définir le numéro ou les numéros de ports souhaités.

La boîte de dialogue **Port** apparaît lorsque vous maintenez enfoncée la touche **<CTRL>** et cliquez sur le lien **spécifiez le port** à la seconde étape de l'assistant de règles.

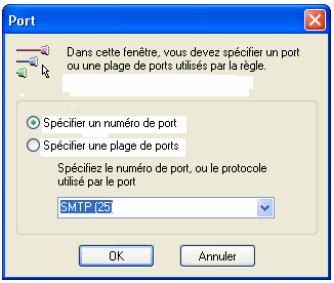


Figure 33. Boîte de dialogue **Port**

Utilisez ici les boutons **Ajouter** et **Supprimer** pour ajouter le nombre souhaité de ports ou de plages de ports de l'ordinateur. Une fois la configuration de la liste de ports terminée, cliquez sur **Ok** pour retourner à la boîte de dialogue de l'assistant de règles.

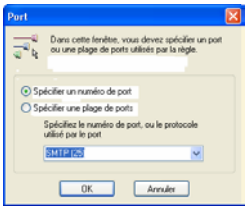
Lorsque vous cliquez sur **Ajouter** dans la boîte de dialogue **Spécifiez un port ou une plage de ports**, la boîte de dialogue **Port** (Figure 30. Boîte de dialogue **Spécifier une adresse** avec l'option **Adresse d'ordinateur.**) s'affiche à l'écran. La même boîte de dialogue apparaît lorsque vous cliquez sur le lien **spécifiez le port** du second assistant de règles, sans enfoncer la touche **<CTRL>**.

La boîte de dialogue **Port** permet de spécifier le numéro ou la plage de numéros de port dans la règle (1. Boîte de dialogue Port).

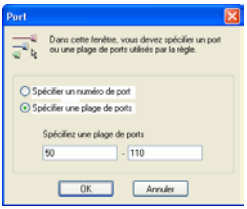
Vous avez le choix parmi les deux options suivantes :

- **Spécifier un numéro de port** : sélectionnez l'une des valeurs prédéfinies dans la liste déroulante ou entrez le numéro de port à l'aide du clavier.

- **Spécifier une plage de ports** : spécifiez la plage de ports en indiquant le premier port dans la première zone de texte, puis le dernier port dans la seconde (2. Définition de la plage de numéros de ports).



1. Boîte de dialogue Port



2. Définition de la plage de numéros de ports

Après avoir indiqué le numéro ou les numéros de ports, cliquez sur **Ok**.

6.3.2.3. Étape 3. Actions supplémentaires

La troisième étape de l'assistant permet d'ajouter des actions supplémentaires pour la règle. La boîte de dialogue contient deux cases à cocher : **Enregistrer l'événement** : si cette case est cochée, les événements détectés sont enregistrés, et si la case **Afficher l'avertissement** est cochée, le message correspondant est affiché (Figure 18. Exemple d'avertissement de Kaspersky Anti-Hacker).

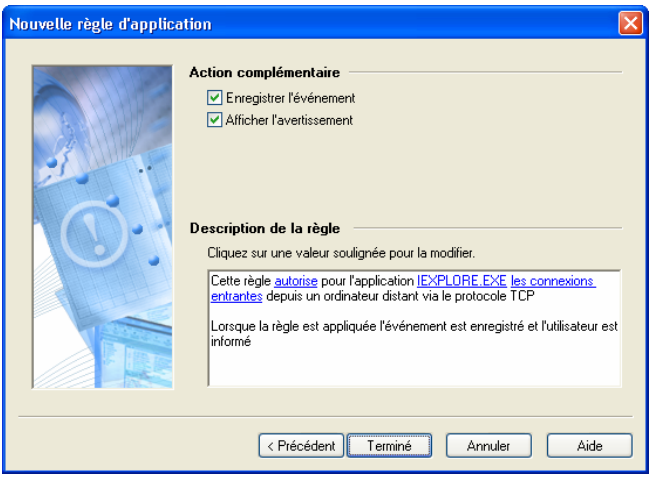


Figure 34. Actions supplémentaires pour la règle

6.4. Personnalisation des règles de filtrage de paquets

Comment créer une règle de filtrage de paquets ? L'assistant de règles de filtrage de paquets

6.4.1. Utilisation de la liste de règles

La gestion de la liste des règles de filtrage de paquets ressemble beaucoup à celle de la liste des règles d'application.

Pour afficher la liste des règles de filtrage de paquets à l'écran,

sélectionnez **Règles de filtrage de paquets** dans le menu **Service**.

La boîte de dialogue **Règles de filtrage de paquets** s'affiche à l'écran (Figure 35. Boîte de dialogue **Règles de filtrage de paquets**).

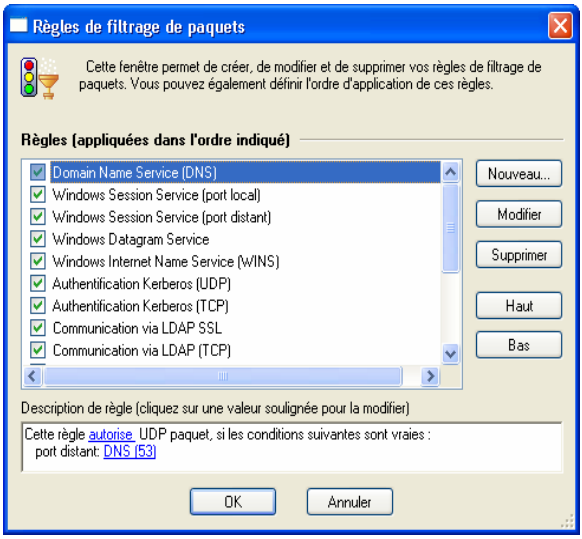


Figure 35. Boîte de dialogue **Règles de filtrage de paquets**

La partie supérieure de la boîte de dialogue contient la liste des règles de filtrage de paquets. Des cases à cocher en face de chaque règle permettent d'activer ou de désactiver ces dernières.

Les règles sont classées en fonction de leur priorité ; la règle en début de liste sera appliquée la première, et uniquement alors, le logiciel appliquera la seconde, et ainsi de suite. Rappelez-vous que seules les règles dont les cases sont cochées sont exécutées.

Pour activer ou désactiver une règle de filtrage de paquets,

activez ou désactivez la case correspondante dans la liste des règles de filtrage de paquets.

À droite de la liste de règles se trouvent les boutons suivants :

- Nouveau... – permet de créer une nouvelle règle. Si vous cliquez sur ce bouton, la boîte de dialogue de l'assistant de règles de filtrage de paquets s'affiche à l'écran.

- Modifier : permet de modifier la règle sélectionnée. Si vous cliquez sur ce bouton, la boîte de dialogue de l'assistant de règles de filtrage de paquets s'affiche à l'écran.

- Supprimer : supprime la règle sélectionnée de la liste.

- Haut : déplace la règle sélectionnée une ligne vers le haut, ce qui augmente sa priorité.

- Bas : déplace la règle sélectionnée une ligne vers le bas, ce qui diminue sa priorité.

Pour modifier une règle sélectionnée dans la liste, vous pouvez également utiliser la touche **<ENTRÉE>** ou double-cliquer sur la règle. Pour supprimer cette règle, utilisez la touche **<SUPPR>**. Enfin, pour ajouter une nouvelle règle, utilisez la touche **<INS>**.

Vous pouvez également modifier la liste à partir du menu contextuel, qui comprend les commandes suivantes :

- Modifier : permet de modifier la règle sélectionnée ;

- Supprimer : supprime la règle sélectionnée de la liste ;

- Dupliquer la règle : crée une copie de la règle sélectionnée. La copie sera placée juste après la règle sélectionnée.

En dessous de la liste, la section **Description de la règle** contient les détails de la règle sélectionnée dans la section supérieure. Comme la même section se retrouve dans les dialogues de l'assistant de règles, nous allons en parler ici avec un peu plus de détail.

La description de la règle contient du texte en noir qui n'est pas modifiable, et du texte en bleu qu'il faut remplacer par les valeurs appropriées. Lorsque certains paramètres sont présentés en gras, cela veut dire que leur valeur est essentielle pour la règle.

Pour saisir ou modifier la valeur requise dans la description de la règle,

1. Cliquez sur le lien souligné approprié dans la section **Description de la règle**.

2. Dans la boîte de dialogue qui s'affiche à l'écran, sélectionnez la valeur souhaitée (pour de plus amples détails, reportez-vous aux sous-chapitres suivants).

Sur la partie supérieure de la boîte de dialogue **Règles de filtrage de paquets** se trouvent les boutons suivants :

- Ok : referme la boîte de dialogue et enregistre les modifications apportées.

- Annuler : referme la boîte de dialogue sans enregistrer les modifications.

Toutes les modifications apportées à la liste sont appliquées immédiatement après leur enregistrement.

Les règles de filtrage de paquets ont une priorité plus haute que les règles d'application et sont par conséquent exécutées en premier.

6.4.2. Ajout d'une nouvelle règle

La gestion de l'assistant des règles de filtrage de paquets ressemble beaucoup à celle de l'assistant des règles d'application. Il ne compte cependant qu'avec deux boîtes de dialogue.

6.4.2.1. Étape 1. Conditions de la règle

La première étape de l'assistant de règles vous permet de spécifier :

- Le protocole utilisé (TCP, UDP, ICMP, autres protocoles IP) ;
- L'adresse de destination du paquet ;
- La direction du trafic (sortant, entrant) ;
- Les paramètres liés au protocole (les ports pour les protocoles TCP et UDP, les types de message pour le protocole ICMP, le numéro de protocole pour les autres protocoles IP) ;
- L'action (autoriser/bloquer).

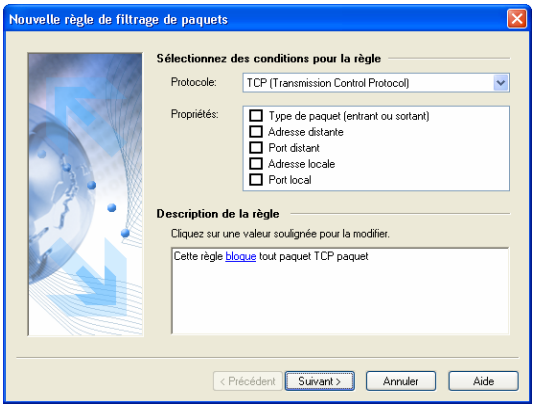


Figure 36. Première boîte de dialogue de l'assistant de règles de filtrage de paquets

Pour configurer une règle de filtrage de paquets, procédez comme suit :

1. Sélectionnez le protocole filtré dans la liste déroulante **Protocole**. Les valeurs disponibles sont **TCP (Transmission Control Protocol)**, **UDP (User Datagram Protocol)**, **ICMP (Internet Control Message Protocol)**, et **Autres protocoles IP**. La valeur par défaut est **TCP**.

2. Cochez les cases suivantes dans la section **Propriétés**:

Type de paquet (entrant ou sortant) : la direction du trafic. Par défaut, la case n'est pas cochée pour filtrer le trafic entrant et sortant à la fois.

Si vous souhaitez contrôler uniquement le trafic entrant ou le trafic sortant, cochez cette case et spécifiez le type de paquet souhaité dans la section **Description de la règle**. Pour saisir la valeur souhaitée, cliquez sur le lien **type de paquet**, sélectionnez une option dans la boîte de dialogue **Spécifier la direction du paquet**, puis cliquez sur **Ok**.

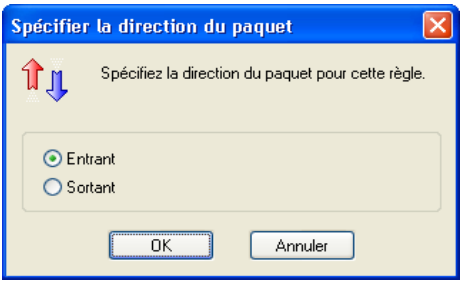


Figure 37. Boîte de dialogue **Spécifier la direction du paquet**

3. Certaines cases de la section **Propriétés** dépendent du protocole choisi.

   - Pour les protocoles TCP et UDP, spécifiez le **Port distant** et le **Port local**.
   - Pour le protocole ICMP, spécifiez le **Type de message ICMP**.
   - Pour d'autres protocoles sur IP, vous pouvez spécifier le **Protocole**.

   Adresse distante : l'adresse de la machine distante (pour tous les protocoles).

   Adresse locale : l'adresse de la machine locale (pour tous les protocoles).

   Pour définir l'adresse, cliquez sur le lien **spécifiez l'adresse** correspondant dans la section **Description de la règle**. Pour spécifier plus d'une adresse, maintenez enfoncée la touche **<CTRL>** puis cliquez sur le lien. Pour de plus amples détails, reportez-vous au sous-chapitre 6.3.2.2.1 à la page 56.

   Port distant : le numéro de port distant (pour les protocoles TCP et UDP).

   Port local : le numéro de port local (pour les protocoles TCP et UDP).

Pour spécifier le port, cliquez sur le lien **spécifiez le port** correspondant dans la section **Description de la règle**. Pour de plus amples détails, reportez-vous au sous-chapitre 6.3.2.2.2 à la page 58.

Type de message ICMP : le type de message ICMP (protocole ICMP uniquement). Pour spécifier le type de message, cliquez sur le lien **spécifiez le type de message ICMP** correspondant dans la section **Description de la règle** et sélectionnez la valeur souhaitée dans la liste déroulante de la boîte de dialogue **Spécifier le type de message ICMP** (Figure 38. Boîte de dialogue **Spécifier le type de message ICMP**), puis cliquez sur **Ok**.

- Echo request (demande d'écho)
- Echo reply (réponse à demande d'écho)
- Trace route (TTL exceed - sans réponse)
- Réseau inaccessible
- Hôte inaccessible
- Protocole inaccessible
- Port inaccessible
- Redirection vers hôte
- Redirection vers réseau
- Redirection vers TOS (type de service) et réseau
- Redirection vers TOS (type de service) et hôte.

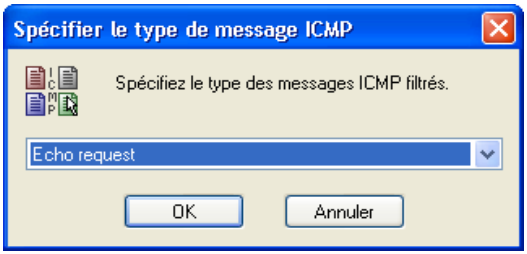


Figure 38. Boîte de dialogue **Spécifier le type de message ICMP**

Protocole : le nom ou numéro du protocole (pour protocoles IP uniquement). Si la case n'est pas cochée, l'application contrôle tous les protocoles IP. Pour spécifier un nom ou numéro de protocole, cliquez sur le lien et spécifiez le protocole dans la section **Description de la règle** puis sélectionnez la valeur souhaitée dans la liste déroulante de la boîte de dialogue **Spécifier le protocole** (Figure 39. Boîte de dialogue **Spécifier un protocole**) puis cliquez sur **Ok**. La liste des protocoles disponibles indique les numéros de protocole entre parenthèses.

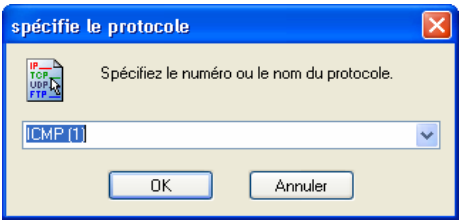


Figure 39. Boîte de dialogue **Spécifier un protocole**

- IGMP,RGMP(2)
- GGP(3)
- IP encapsulé (4)
- TCP(6)
- IGRP(9)
- UDP(17)
- GRE(47)
- ESP(50)
- AH(51)
- IP chiffré(53)

4. Indiquez l'action qui sera appliquée aux paquets vérifiant les conditions définies ci-dessus - bloquer ou autoriser. Par défaut, l'option **Bloquer** est sélectionnée. Pour modifier la valeur, cliquez sur le lien correspondant dans la section **Description de la règle** , sélectionnez la valeur souhaitée dans la boîte de dialogue **Spécifier une action** , puis cliquez sur **Ok** (Figure 40. Boîte de dialogue **Spécifier une action**).

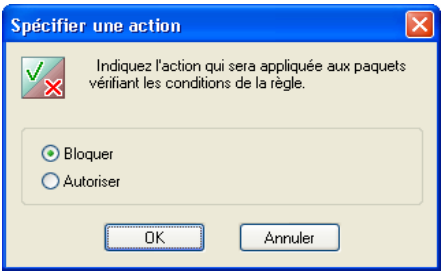


Figure 40. Boîte de dialogue **Spécifier une action**

6.4.2.2. Étape 2. Nom de la règle et actions supplémentaires

Vous devez spécifier le nom de la règle de filtrage de paquets dans le champ **Nom de la règle** dans la seconde boîte de dialogue de l'assistant. Le logiciel propose un nom par défaut comme par exemple, Règle de filtrage [numéro de règle]. Il est cependant conseillé d'indiquer un nom descriptif qui vous aidera à identifier la règle dans la liste.

Vous pouvez également activer des actions supplémentaires pour la règle. L'assistant contient deux cases à cocher : **Enregistrer l'événement** : si cette case est cochée, les événements détectés sont enregistrés, et si la case **Afficher l'avertissement** est cochée, le message correspondant est affiché(Figure 18. Exemple d'avertissement de Kaspersky Anti-Hacker).

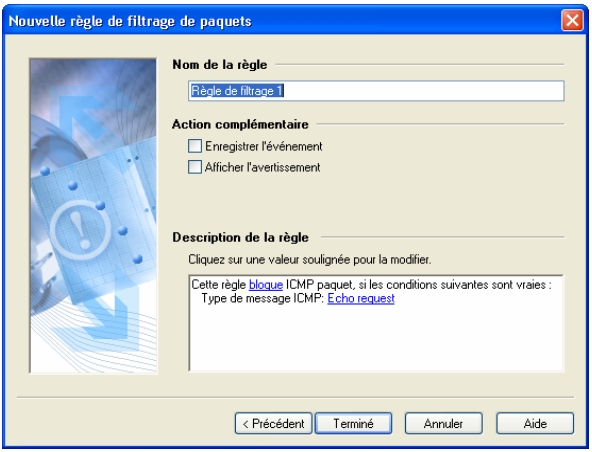


Figure 41. Définition du nom de la règle et des actions supplémentaires

6.5. Détection contre les intrusions

Comment configurer le système de détection contre les intrusions pour un rendement optimal ?

6.5.1. Paramètres du détecteur d'intrusions

Pour afficher les paramètres du détecteur d'intrusions,

sélectionnez **Paramètres** dans le menu **Service** et cliquez sur l'onglet **Détection contre les intrusions** (Figure 42. Onglet **Détection contre les intrusions** de la boîte de dialogue **Paramètres**).

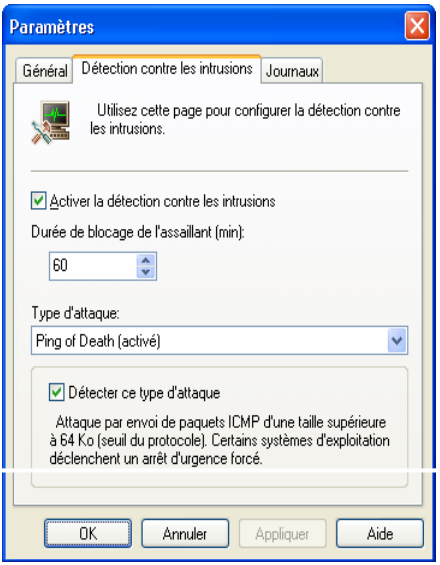


Figure 42. Onglet **Détection contre les intrusions** de la boîte de dialogue **Paramètres**

Il est recommandé de laisser toujours cochée la case **Activer la détection contre les intrusions** dans l'onglet **Détection contre les intrusions**. Cette case vous permet d'activer ou de désactiver la détection contre les intrusions extérieures dans votre machine.

Sous la case à cocher, le champ **Durée de blocage de l'assaillant (min.)** permet de préciser la durée pendant laquelle la machine de l'assaillant sera bloquée, au cas où l'adresse distante pourrait être identifiée. Ce paramètre s'applique à tous les types d'attaques.

Si vous modifiez le paramètre **Durée de blocage de l'assaillant**, il s'appliquera à toutes les attaques ultérieures dès que vous aurez cliqué sur **Ok** ou sur **Appliquer** dans la boîte de dialogue **Paramètres**. La durée de blocage des ordinateurs déjà bloqués en raison d'une attaque précédente n'est pas modifiée.

Le groupe de champs situés dans la partie inférieure de l'onglet varie selon le type d'attaque sélectionné dans la liste **Type d'attaque**.

Cochez la case **Détecter ce type d'attaque** si vous souhaitez que le logiciel détecte ce type d'attaques. Sous cette case sont présentés des détails sur l'attaque qui vous seront utiles si vous n'êtes pas sûr de votre décision.

6.5.2. Liste des attaques détectées

Kaspersky Anti-Hacker est capable de détecter les attaques par refus de service (*SYN Flood, UDP Flood, ICMP Flood*), *les attaques Ping of death, Land, Helkern et SmbDie*, ainsi que les tentatives d'exploration des ports, annonçant habituellement une attaque plus sérieuse :

- ***Ping of death** (Ping de la mort)*. Ce type d'attaque procède par envoi de paquets ICMP d'une taille supérieure à 64 Ko (valeur de seuil) vers votre ordinateur. Certains systèmes d'exploitation déclenchent un arrêt d'urgence forcé.

- *Land*. Ce type d'attaque envoie vers votre ordinateur des requêtes de connexion récursives (l'ordre étant donné de se connecter avec soi-même). Une boucle infinie est enclenchée à chaque tentative d'auto-connexion. Il se produit une surcharge du processeur qui augmente sérieusement le risque d'un arrêt d'urgence.

- *Analyse de ports TCP*. Procède par détection de ports TCP ouverts sur votre ordinateur. Cette recherche des points faibles d'un ordinateur annonce généralement d'autres attaques plus dangereuses. Définissez les paramètres suivants pour ce type d'attaque : **Nombre de ports :** – le nombre de ports que la machine distante tente d'ouvrir et **Durée (sec):** – le temps investi.

- *Analyse de ports UDP*. Cette attaque procède par détection de ports UDP ouverts sur votre ordinateur. L'attaque est détectée grâce au nombre de paquets UDP transmis vers différents ports de l'ordinateur ports pendant une certaine période de temps. Cette recherche des points faibles d'un ordinateur annonce généralement d'autres attaques plus dangereuses. Définissez les paramètres suivants pour ce type d'attaque : **Nombre de ports :** – le nombre de ports que la machine distante tente d'ouvrir et **Durée (sec):** – le temps investi.

- *SYN Flood*. Ce type d'attaque procède par l'envoi d'une fausse pétition de connexion vers votre ordinateur. Le système réserve un certain nombre de ressources lors de chaque demande de connexion, et l'ordinateur cesse de répondre aux demandes d'autres sources. Définissez les paramètres suivants pour ce type d'attaque : **Nombre de connexions :** – le nombre de connexions que la machine distante tente d'établir et **Durée (sec):** – le temps investi.

- *UDP Flood.* Ce type d'attaque procède par envoi de paquets UDP spéciaux vers votre ordinateur. Ces paquets sont retransmis à l'infini entre les machines attaquées. Cette attaque force de cette manière la mobilisation de ressources importantes et provoque une surcharge du

lien de communications. Définissez les paramètres suivants pour ce type d'attaque : Nombre de paquets UDP : – le nombre de paquets UDP entrants, et **Durée (sec):** – le temps investi.

- *ICMP Flood.* Ce type d'attaque procède par l'envoi de paquets ICMP paquets vers votre ordinateur. Ceci provoque une surcharge du processeur, la machine attaquée devant répondre à chacun des paquets. Définissez les paramètres suivants pour ce type d'attaque : **Nombre de paquets ICMP :** – le nombre de paquets ICMP entrants, et **Durée (sec):** – le temps investi.

- ***Helkern*** Cette attaque procède par envoi de paquets UDP spéciaux, capables d'exécuter du code malveillant, vers l'ordinateur qui en est victime. L'attaque se traduit par un ralentissement de la connexion Internet.

- ***SmbDie*** Cette tente d'établir une connexion SMB. Lorsque l'attaque réussit, un paquet spécial faisant déborder le buffer système est transmis à l'ordinateur victime qui en est victime. L'utilisateur est alors obligé de redémarrer le système d'exploitation. Les systèmes d'exploitation Windows 2k/XP/NT sont susceptibles de subir ce type d'attaques.

- L'attaque de ***Lovesan*** essaie de détecter une faille dans le service DCOM RPC des systèmes d'exploitation Windows NT 4.0/NT 4.0 Terminal Services Edition/2000/XP/Server (tm) 2003 de votre ordinateur. Lorsque cette faille est détectée, le programme malfaisant, permettant d'effectuer n'importe quelle manipulation sur votre machine, vous est transmis.

CHAPITRE 7. SUPERVISION DE L'ACTIVITÉ

7.1. Affichage de l'état courant

Affichage de la liste des applications actives, des ports ouverts et des connexions établies

L'exécution de toutes les applications réseau fonctionnant sur votre machine est surveillée en permanence et les événements correspondants sont enregistrés par Kaspersky Anti-Hacker. Vous pouvez examiner les statistiques d'activité réseau suivantes :

- **Applications actives**. Les opérations réseau sont triées en fonction des applications associée. Pour chaque application de votre machine, vous pouvez examiner les ports et connexions contrôlées par cette application.
- **Connexions établies**. Affiche toutes les connexions entrantes et sortantes, les adresses et les numéros de ports d'ordinateur distants.
- **Ports ouverts**. Affiche tous les ports ouverts sur votre machine.

7.1.1. Applications actives

Pour examiner la liste des applications réseau active actuellement,

sélectionnez **Applications actives** dans le sous-menu **Afficher** du menu **Affichage** (Figure 43. Boîte de dialogue **Applications réseau actives**). Vous pouvez également cliquer sur  dans la barre d'outils.

La boîte de dialogue **Applications réseau actives** s'affiche à l'écran.

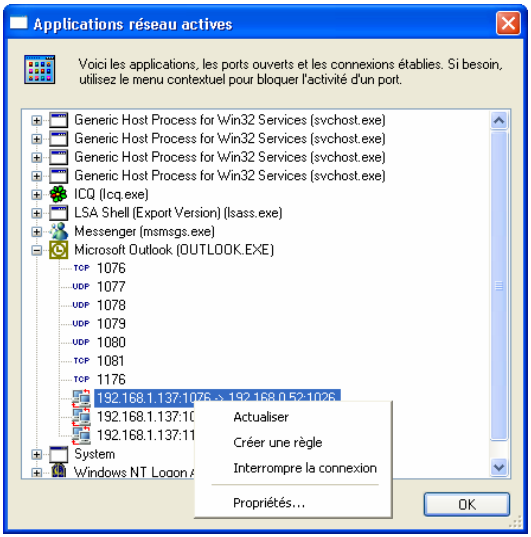


Figure 43. Boîte de dialogue **Applications réseau actives**

Cette boîte de dialogue permet d'examiner la liste des applications actives et des ressources qu'elles utilisent sur le réseau. Les noms d'application sont triés par ordre alphabétique, pour simplifier la navigation dans la liste. À côté du nom de chaque application apparaît l'icône de l'application.

En développant l'arborescence de l'application, vous affichez la liste des ports ouverts sur votre machine et les connexions établies par l'application. Les indicateurs sont les suivants :

- Les ports ouverts sont signalés par les icônes TCP ou UDP, selon le type du port. À droite de chacun des ports figure son numéro.

- Les connexions établies sont signalées par l'icône  si c'est votre machine qui les a établies, ou par l'icône  , si elles proviennent de l'extérieur Les paramètres de connexion sont décrits à droite de l'icône : `<adresse source>:<port source>` → `<adresse destination>:<port destination>`

La liste des applications réseau actives est mise à jour automatiquement deux fois par seconde.

La liste possède un menu contextuel qui comprend les commandes suivantes :

- Actualiser : met à jour la liste des applications actives à la demande de l'utilisateur.

- Créer une règle : permet de créer une règle sur le port sélectionné ou en fonction de la connexion. Le logiciel lance l'assistant de règles d'application et saisit automatiquement les détails du port sélectionné ou de la connexion dans les champs appropriés.

- Interrompre la connexion : interrompt la connexion sélectionnée dans la liste (cette commande n'est disponible que si une connexion est sélectionnée dans la liste).

Attention ! Si vous forcez l'interruption d'une connexion, l'application associée peut cesser de fonctionner correctement.

- Propriétés : affiche des détails supplémentaires sur l'élément sélectionné dans la liste (Figure 44. Boîte de dialogue Propriétés de l'application), connexion (Figure 46. Boîte de dialogue Propriétés de la connexion) ou port (Figure 48. Boîte de dialogue **Propriétés du port**).

La liste peut afficher plus d'une chaîne pour la même application. Autrement dit, lorsque plus d'une copie ou instance de cette application aura été lancée. Si vous développez les arborescences de chaque instance de l'application, différentes listes de ports ouverts ou connexions établies peuvent apparaître.

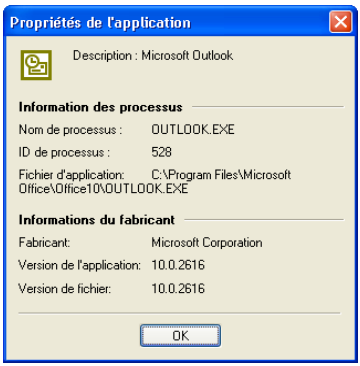


Figure 44. Boîte de dialogue **Propriétés de l'application**

La boîte de dialogue **Propriétés de l'application** contient la section Informations sur l'application avec les éléments suivants :

- Nom d'application : le nom du fichier exécutable ;

- ID d'application : identifiant de l'application ;

- Fichier d'application : chemin d'accès complet au fichier exécutable.

Sous la section **Informations sur l'application**, une autre section appelée **Informations du fabricant** contient les éléments suivants :

- Fabricant : nom du fabricant ;
- Version de l'application : version du logiciel ;
- Version de fichier : la version du fichier exécutable.

7.1.2. Connexions établies

Pour examiner la liste des connexions réseau établies actuellement,

Sélectionnez **Connexions établies** dans le sous-menu **Afficher** du menu **Affichage** (Figure 45. Boîte de dialogue **Connexions établies**). Vous pouvez également cliquer sur  dans la barre d'outils.

La boîte de dialogue **Connexions établies** s'affiche à l'écran.

Chaque ligne donne des détails sur une unique connexion établie. Ces connexions sont signalées par l'icône  si c'est votre machine qui les a établies, ou par l'icône  , si elles proviennent de l'extérieur

La liste contient également les détails de connexion suivants :

- Adresse distante : l'adresse et le port d'une machine distante avec laquelle une connexion est établie ;
- Port local : l'adresse et le port votre ordinateur ;
- Application : l'application qui a établi cette connexion.

Vous pouvez trier la liste par l'un des titres décrits précédemment.

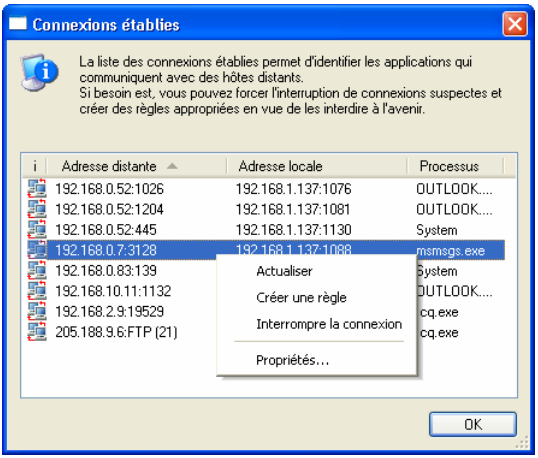


Figure 45. Boîte de dialogue **Connexions établies**

La liste des connexions établies est mise à jour automatiquement deux fois par seconde.

Si besoin, vous pouvez forcer l'interruption de connexions suspectes et créer des règles appropriées en vue de les interdire à l'avenir. Pour ce faire, utilisez les commandes appropriées du menu contextuel de la boîte de dialogue :

- Actualiser : met à jour la liste des applications actives à la demande de l'utilisateur.

- Créer une règle : permet de créer une règle en fonction de la connexion sélectionnée. Le logiciel lance l'assistant de règles d'application et saisit automatiquement les détails de la connexion dans les champs appropriés.

- Interrompre la connexion : interrompt la connexion sélectionnée dans la liste.

Attention ! Si vous forcez l'interruption d'une connexion, l'application associée peut cesser de fonctionner correctement.

- Propriétés : affiche des détails supplémentaires sur la connexion sélectionnée dans la liste (Figure 46. Boîte de dialogue Propriétés de la connexion).

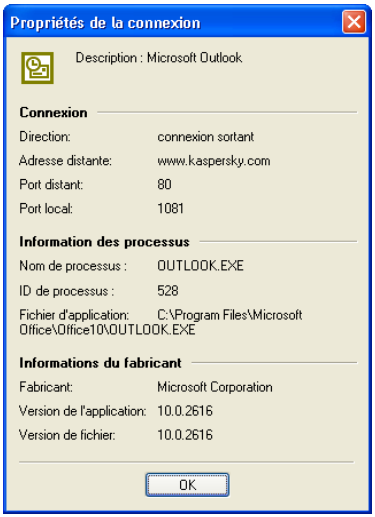


Figure 46. Boîte de dialogue **Propriétés de la connexion**

La section **Connexion** de la boîte de dialogue **Propriétés de la connexion** contient les éléments suivants :

- Direction : le type de connexion, sortant ou entrant ;
- Adresse distante : le nom symbolique ou l'adresse IP de la machine distante ;
- Port distant : le numéro de port distant ;
- Port local : le numéro de port local.

Sous la section **Connexion** figurent les sections **Informations sur l'application** et **Informations du fabricant** (reportez-vous au sous-chapitre 7.1.1 à la page 71).

7.1.3. Ports ouverts

Pour examiner la liste des ports ouverts actuellement,

Sélectionnez **Ports ouverts** dans le sous-menu **Afficher** du menu **Affichage** (Figure 47. Boîte de dialogue **Ports ouverts**). Vous pouvez également cliquer sur dans la barre d'outils.

La boîte de dialogue **Ports ouverts** s'affiche à l'écran.

Chaque ligne donne des détails sur un port ouvert unique. Les ports ouverts sont signalés par les icônes **TCP** ou **UDP**, selon le type du port.

La liste contient également les détails du port suivant :

- Port local : le numéro de port local ;
- Application : application associée ;
- Emplacement d'application : chemin d'accès complet au fichier exécutable.

Vous pouvez trier la liste par l'un des titres décrits précédemment.

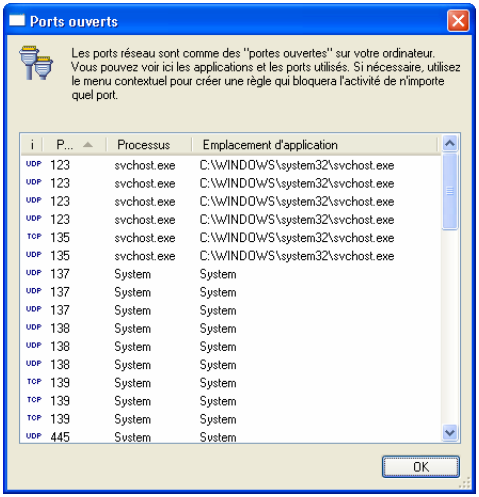


Figure 47. Boîte de dialogue **Ports ouverts**

La liste des connexions établies est mise à jour automatiquement deux fois par seconde.

Si besoin, vous pouvez créer une règle pour bloquer la connexion sur le port sélectionné. Pour ce faire, utilisez les commandes appropriées du menu contextuel de la boîte de dialogue :

- Actualiser : met à jour la liste des ports ouverts à la demande de l'utilisateur.

- Créer une règle : permet de créer une règle sur le port sélectionné. Le logiciel lance l'assistant de règles d'application et saisit automatiquement détails du port sélectionné dans les champs appropriés.

- Propriétés : affiche des détails supplémentaires sur le port sélectionné dans la liste (Figure 48. Boîte de dialogue **Propriétés du port**).

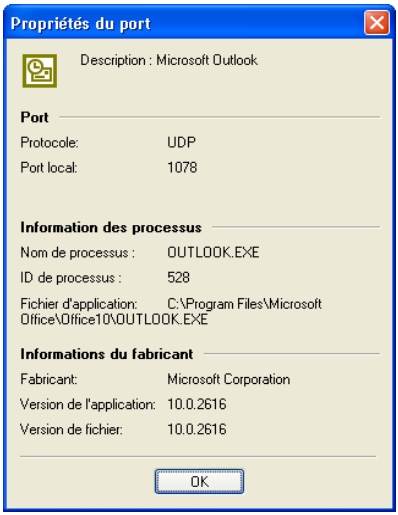


Figure 48. Boîte de dialogue **Propriétés du port**

La section **Port** de la boîte de dialogue **Propriétés du port** contient les éléments suivants :

- Protocole : le nom du protocole utilisé ;

- Port local : le numéro de port local.

Sous la section **Port** figurent les sections **Informations sur l'application** et **Informations du fabricant** (reportez-vous au sous-chapitre 7.1.1 à la page 71).

7.2. Utilisation des journaux

Affichage de la fenêtre Journaux.
Organisation de la fenêtre Journaux.
Sélection du type de journal.
Enregistrement du journal dans un fichier

Les événements du réseau qui se produisent dans votre machine sont surveillés et enregistrés dans des *journaux*. Chaque type d'événement est enregistré dans différents journaux :

- Le journal Sécurité contient les détails des dernières attaques de votre machine (reportez-vous au sous-chapitre 6.5 à la page 67).
- Le journal Activité des applications contient des détails sur les événements spécifiquement journalisés par l'assistant de règles d'application (reportez-vous au sous-chapitre 6.3.2.3 à la page 59).
- Le journal Filtrage de paquets contient des détails sur les événements spécifiquement journalisés par l'assistant de règles de filtrage de paquets (reportez-vous au sous-chapitre 6.4.2.2 à la page 66).

Tous les journaux peuvent être examinés et configurés à partir d'une même fenêtre (*la fenêtre **Journaux***).

Utilisez cette fenêtre pour limiter la taille des journaux, pour les effacer au redémarrage du logiciel ou pour conserver les résultats de plusieurs sessions (reportez-vous au sous-chapitre 7.2.4 à la page 84).

Vous pouvez si besoin nettoyer les journaux à tout moment.

Vous pouvez également les enregistrer dans des fichiers sur disque.

7.2.1. Affichage de la fenêtre Journaux

*Pour afficher la fenêtre **Journaux**,*

sélectionnez le type de journal dans le sous-menu **Journaux** du menu **Affichage**.

La fenêtre **Journaux** s'affiche à l'écran (Figure 49. L'onglet **Sécurité**).

7.2.2. Organisation de la fenêtre Journaux

La fenêtre Journaux contient les trois éléments suivants :

- Menus
- Tableau de rapports
- Onglets permettant de basculer entre les différents types de journaux.

7.2.2.1. Menus

Sur la partie supérieure de la fenêtre Journaux se trouve la *barre de menus*.

Tableau 4

Menu →commandes	**Usage** (Cette commande...)
Fichier ⟶ Enregistrer dans un fichier	Enregistre le journal actif dans un fichier
Aide ⟶ Rubriques de l'aide...	Affiche les rubriques de l'aide
Aide ⟶ Kaspersky Anti-Hacker sur le Web	Ouvre la page Web officielle de Kaspersky Labs
Aide ⟶ À propos de Kaspersky Anti-Hacker	Présente les détails du logiciel et des renseignements sur les clés utilisées

7.2.2.2. Tableau de rapports

Le tableau des rapports présente les informations enregistrées dans le type de journal sélectionné. Pour examiner son contenu, utilisez la barre de défilement sur la droite.

Le tableau de rapports possède un menu contextuel contenant par défaut les deux commandes suivantes, complétées éventuellement en fonction du type de journal :

- Effacer le journal : efface le journal sélectionné.
- Défilement automatique du journal : affiche toujours le dernier événement enregistré à la fin du rapport.
- **Ne pas enregistrer cet événement** : désactive l'enregistrement ultérieur de l'événement sélectionné. Cette commande est disponible pour tous les journaux, sauf pour le journal des attaques de hackers.
- Créer une règle : permet de créer une règle en fonction de l'événement sélectionné. La nouvelle règle est placée au début de la liste, avec la priorité la plus haute.

7.2.2.3. Onglets

Les onglets suivants au bas de la fenêtre **Journaux** permettent de basculer entre les différents types de journaux :

- Sécurité
- Activité des applications
- Filtrage de paquets

7.2.3. Sélection du journal

7.2.3.1. Journal Sécurité

Le journal **Sécurité** permet d'examiner la liste de toutes les attaques détectées sur votre machine (reportez-vous au sous-chapitre 6.5 à la page 67).

*Pour afficher le journal **Sécurité**,*

sélectionnez **Sécurité** dans le sous-menu **Journaux** du menu **Affichage**.

La fenêtre **Journaux** avec l'onglet **Sécurité** activé s'affiche à l'écran (Figure 49. L'onglet **Sécurité**). Le journal contient les informations suivantes :

- Date et heure : la date et l'heure où votre ordinateur a subi une attaque.
- **Description d'événement** : type d'attaque et adresse de l'assaillant, si identifiée.

Il est possible de trier la liste des événements par date et heure.

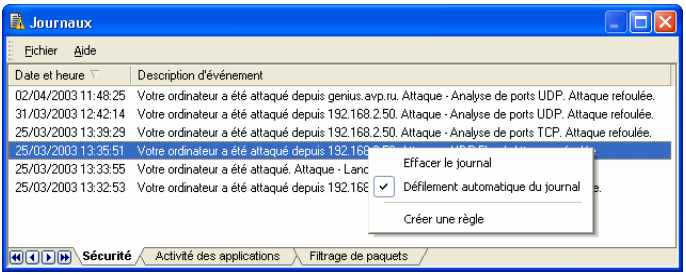


Figure 49. L'onglet **Sécurité**

7.2.3.2. Activité des applications

Le journal **Activité des applications** permet d'examiner les détails des applications lorsque l'option de journalisation est activée dans l'assistant de règles d'application (reportez-vous au sous-chapitre 6.3.2.3 à la page 59).

*Pour afficher le journal **Activité des applications**,*

sélectionnez **Activité des applications** dans le sous-menu **Journaux** du menu **Affichage**.

La fenêtre **Journaux** avec l'onglet **Activité des applications** s'affiche à l'écran (Figure 50. L'onglet du journal **Activité des applications**). Le journal contient les informations suivantes :

- Date et heure : la date et l'heure de l'événement ;
- Application : nom de l'application associée et chemin d'accès complet à son fichier exécutable ;
- Description d'activité : les détails de l'activité ;

- Adresse locale : l'adresse locale ;
- Adresse distante : l'adresse distante.

Il est possible de trier la liste des événements par date et heure.

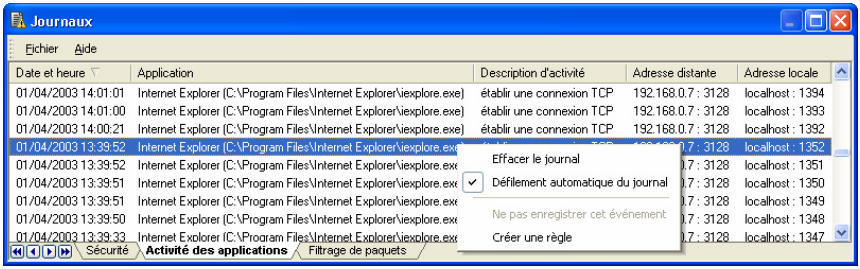


Figure 50. L'onglet du journal **Activité des applications**

7.2.3.3. Filtrage de paquets

Le journal **Filtrage de paquets** permet d'examiner les détails des événements liés au filtrage de paquets lorsque l'option de journalisation est activée dans l'assistant de règles de filtrage de paquets (reportez-vous au sous-chapitre 6.4.2.2 à la page 66).

*Pour afficher le journal **Filtrage de paquets**,*

sélectionnez **Filtrage de paquets** dans le sous-menu **Journaux** du menu **Affichage**.

La fenêtre **Journaux** avec l'onglet **Filtrage de paquets** s'affiche à l'écran (Figure 51. Onglet du journal **Filtrage de paquets**). Le journal contient les informations suivantes :

- Date et heure : la date et l'heure de l'événement ;
- Direction : le type de paquet : entrant ou sortant ;
- Protocole : le nom du protocole ;
- Adresse locale : l'adresse locale ;
- Adresse distante : l'adresse distante ;

- Règle utilisée : le nom de la règle utilisée.

Les entrées en noir correspondent aux paquets autorisés, et les entrées en rouge, aux paquets bloqués.

Il est possible de trier la liste des événements par date et heure.

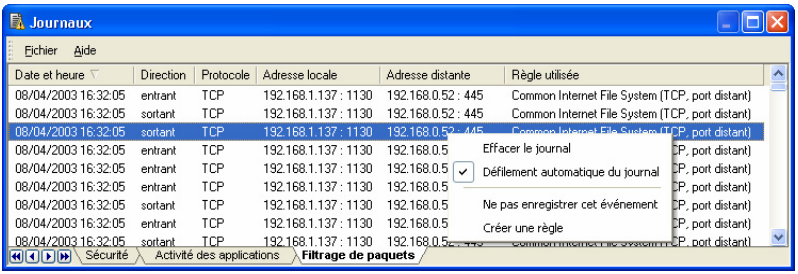


Figure 51. Onglet du journal **Filtrage de paquets**

7.2.4. Définition des paramètres du journal

Pour définir les paramètres du journal,

sélectionnez **Paramètres** dans le menu **Service** et cliquez sur l'onglet **Journaux** (Figure 52. Boîte de dialogue **Paramètres,** avec l'onglet **Journaux** activé).

Définissez des valeurs pour les deux options suivantes :

Effacer le journal au démarrage du logiciel : si la case est cochée, les journaux sont effacés au démarrage du logiciel.

Limiter la taille du journal à (Ko) : si la case est cochée, la taille du fichier peut être limitée. Spécifiez la taille maximum du fichier journal dans le champ inférieur. Lorsque la taille du journal atteint son maximum, chaque fois qu'une nouvelle entrée est ajoutée au journal, le logiciel supprime la plus ancienne.

Remarque : les cases à cocher précédentes permettent de définir la taille d'UN SEUL fichier journal. Lorsque vous calculez l'espace disque nécessaire pour une exécution normale du logiciel, tenez compte du fait que cette quantité peut être multipliée par trois.

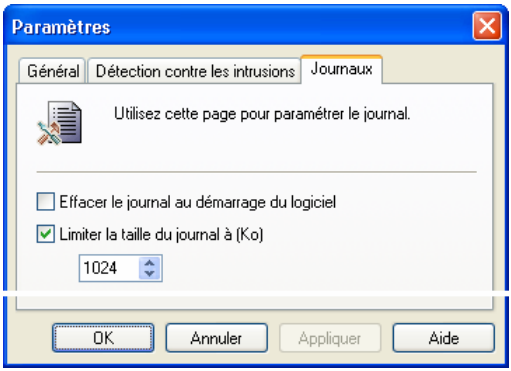


Figure 52. Boîte de dialogue **Paramètres**, avec l'onglet **Journaux** activé

7.2.5. Enregistrement du journal dans un fichier

*Pour enregistrer sur disque le journal sélectionné dans la fenêtre **Journaux**,*

Sélectionnez **Enregistrer dans un fichier** dans le menu **Fichier**. Spécifiez le nom de fichier dans la boîte de dialogue à l'écran. Le journal sera enregistré au format de texte simple.

ANNEXE A.
KASPERSKY LABS LTD.

À propos de Kaspersky Labs

Kaspersky Labs est un groupe international de capital privé de sociétés spécialistes en développement logiciel, avec sièges à Moscou (Russie), et des délégations officielles au Royaume-Uni, aux États-Unis d'Amérique, en Chine, en France et en Pologne. Fondée en 1997, Kaspersky Labs concentre ses efforts sur le développement, le marketing et la distribution de technologies de pointe dans les domaines de la sécurité des technologies de l'information et des logiciels pour ordinateurs.

Kaspersky Labs est un leader reconnu dans le monde de la sécurité des données et des technologies antivirales. Cette société a été la première à développer de nombreuses caractéristiques qui font aujourd'hui partie de tous les systèmes de protection antivirale modernes : une base antivirale externe composée de modules spécialisés incorporés, l'analyse à l'intérieur de fichiers d'archives et compressés, la protection antivirale intégrée pour Linux, etc. En plus des antivirus, Kaspersky Labs développe des produits de sécurité générale pour les données. Notre gamme de produits comprend actuellement Kaspersky™ Inspector et Kaspersky™ WEB Inspector, avec des possibilités uniques pour les utilisateurs de contrôler complètement toute altération non-autorisée du système des fichiers et du contenu d'un serveur Web.

De nouveaux produits en cours de développement sont Kaspersky™ Personal Firewall pour la protection globale contre les attaques des hackers, et Kaspersky™ Anti-Spam pour contrôler dans l'entreprise l'abus de messages entrants (« spam ») et l'utilisation non autorisée de la messagerie. En développement permanent depuis 1989, le produit principal de Kaspersky Labs appelé Kaspersky™ Anti-Virus (plus connu sous le nom de AVP), est régulièrement cité par de nombreuses publications de la presse informatique et par des centres chercheurs comme le meilleur produit antiviral présent sur le marché.

Kaspersky™ utilise toutes les méthodes éprouvées de protection antivirale : analyseurs antivirus, intercepteurs de virus résidents « au vol », contrôleurs d'intégrité et les verrouilleurs de comportement. Kaspersky™ prend en charge tous les systèmes d'exploitation et les logiciels les plus répandus. Il offre une solide défense contre les virus sur les passerelles de messagerie (MS Exchange Server, Lotus Notes/ Domino, Sendmail, Qmail, Postfix et Exim), les pare-feu et les sites Web. Tous les produits de Kaspersky Anti-Virus utilisent des bases des données propres référençant plus de 60 000 virus connus et autres types de codes malveillants. Le produit est également complété par une technologie

heuristique unique, capable de prévoir même des menaces futures : l'analyseur de code heuristique intégré peut détecter jusqu'à 92 % des virus inconnus tandis que l'inhibiteur de comportement pour MS Office 2000, unique au monde, garantit une protection à 100 % contre tous les virus de macro.

A.1. Autres produits de Kaspersky Lab

Kaspersky® Anti-Virus Lite

Le logiciel antivirus le plus facile à utiliser de Kaspersky Lab est conçu pour protéger des ordinateurs à usage personnel sous Windows 95/98/Me, Windows 2000/NT Workstation, Windows XP.

Kaspersky® Anti-Virus Lite comprend:

- **un analyseur antivirus** qui vérifie de manière exhaustive le contenu de tous les lecteurs locaux et partagés à la demande de l'utilisateur ;
- **un moniteur antivirus** qui vérifie automatiquement et en temps réel tous les fichiers utilisés ;
- un **analyseur de bases de données** de messagerie MS Outlook Express, capable de détecter des virus à la demande.

Kaspersky® Anti-Virus Personal/Personal Pro

Le paquet logiciel est conçu pour offrir une protection antivirale intégrale des ordinateurs personnels sous système d'exploitation Windows 95/98/ME, Windows 2000/NT ou Windows XP, des applications bureautiques MS Office 2000 et des logiciels de messagerie Outlook et Outlook Express. Kaspersky® Anti-Virus Personal/Personal Pro contient un programme pour récupérer quotidiennement des mises à jour par Internet. Il s'agit d'un module intégré de gestion et d'automatisation de votre protection antivirale. Le système exclusif d'analyse heuristique de seconde génération parvient à neutraliser efficacement les virus inconnus. L'interface ergonomique et d'utilisation facile vous permet de modifier rapidement les paramètres du logiciel et de travailler commodément avec lui.

Kaspersky® Anti-Virus Personal contient :

- **un analyseur antivirus** qui vérifie de manière exhaustive le contenu de tous les lecteurs locaux et partagés à la demande de l'utilisateur ;

- **un moniteur antivirus** qui vérifie automatiquement et en temps réel tous les fichiers utilisés ;

- **un filtre de messages électroniques** qui vérifie automatiquement en arrière-plan la présence de virus dans tous les messages entrants et sortants ;

- **le centre de contrôle** et la programmation du démarrage automatique de Kaspersky Anti-Virus vous permet de gérer le logiciel de manière centralisée, et de transmettre automatiquement des notifications sur les attaques de virus à travers le réseau.

Kaspersky® Anti-Virus Personal Pro contient les composants ci-dessus, et en plus :

- **un contrôleur d'intégrité** qui suit à la trace les modifications du contenu de votre disque dur, et vous permet de récupérer complètement les fichiers modifiés et les secteurs de démarrage sur simple demande ;

- **un bloqueur de comportements** qui garantit une protection à 100% contre les virus de macro destructifs.

Kaspersky® Security pour PDA

Le logiciel Kaspersky® Security pour PDA protège de manière fiable contre les virus les données conservées dans un PDA sous système d'exploitation Palm OS ou Windows CE, ainsi que toute information transférée à partir d'un PC ou une carte d'expansion, les fichiers ROM et les bases de données. Le logiciel combine de manière efficace un bouquet d'outils antivirus :

- **un analyseur antivirus** qui vérifie de manière exhaustive le contenu de toutes les données conservées (à la fois sur le PDA et sur n'importe laquelle des cartes d'expansion) à la demande de l'utilisateur ;

- **un intercepteur de virus** des données synchronisées par l'outil HotSync™ ou des portables.

Kaspersky® Security pour PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés. Il prend en charge l'accès chiffré aux périphériques et il est capable de chiffrer toutes les données écrites sur des périphériques ou des cartes mémoire.

Kaspersky® Anti-Virus Business Optimal

Ce paquet logiciel est conçu pour offrir une protection intégrale des données des réseaux d'entreprise de petite et moyenne taille.

Kaspersky® Anti-Virus Business Optimal offre une protection antivirale intégrale de :

- postes de travail sous Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux ;
- serveurs de fichiers et d'application sous Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi, OpenBSD ;
- passerelles de messagerie MS Exchange Server 5.5/2000, Lotus Notes/Domino, Sendmail, Postfix, Qmail, Exim.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

Ce paquet logiciel est conçu pour offrir une protection intégrale des données des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Le produit est parfaitement intégrable dans votre réseau d'entreprise, quels que soient les logiciels et matériels d'autres fabricants que vous utilisez. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite contient une protection antivirale intégrale de :

- postes de travail sous Windows 95/98/ME, Windows NT/2000 Workstation, Windows XP, Linux, OS/2 ;
- serveurs de fichiers et d'application sous Windows NT/2000 Server, Linux, Solaris, Novell NetWare, FreeBSD, BSDi; OpenBSD ;
- passerelles de messagerie MS Exchange Server 5.5/2000, Lotus Notes/Domino, Sendmail, Postfix, Exim, Qmail ;
- pare-feu compatible CVP ;
- serveurs Web ;
- ordinateurs de poche (PDA) sous Palm OS.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux de petite et moyenne taille contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages de texte, à l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection uniques de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux de messagerie entrants à la recherche d'objets identifiés en tant que spam. Le logiciel prend en charge tous les systèmes de messagerie existants sur le réseau client, et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des base de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

A.2. Informations de contact

Si vous avez des questions, des commentaires ou des suggestions, adressez-vous à nos revendeurs ou directement à Kaspersky Labs . Nous serons heureux de vous conseiller sur tous nos produits par téléphone ou par courrier électronique. Toutes vos recommandations et suggestions feront l'objet d'une étude et prises en considération.

Support technique	Pour toute information d'ordre technique, visitez : **http://www.kaspersky.com/fr/buyoffline.asp**
Information générale	WWW : **http://www.kaspersky.com/fr/** **http://www.viruslist.com** E-mail : **sales@kaspersky.com**

ANNEXE B. INDEX

ANNEXE C. QUESTIONS FRÉQUENTES

Pendant l'exécution d'une tâche, votre ordinateur a affiché une erreur et vous souhaitez savoir si celle-ci provient du fonctionnement de Kaspersky Anti-Hacker.

Sélectionnez provisoirement le niveau de sécurité **Autoriser tout** ou déchargez Kaspersky Anti-Hacker de la mémoire de l'ordinateur. Vérifiez si la situation a changé. Si la même erreur réapparaît, elle n'est pas provoquée par Kaspersky Anti-Hacker. Si votre ordinateur n'affiche plus l'erreur, contactez le département d'assistance technique de Kaspersky Labs (Technical Support Department).