



# AVG Internet Security 2012

## Manuel de l'utilisateur

### Révision du document 2012.20 (3/29/2012)

Copyright AVG Technologies CZ, s.r.o. Tous droits réservés.

Toutes les autres marques commerciales appartiennent à leurs détenteurs respectifs.

Ce produit utilise l'algorithme MD5 Message-Digest de RSA Data Security, Inc., Copyright (C) 1991-2, RSA Data Security, Inc. Créé en 1991.

Ce produit utilise un code provenant de la bibliothèque C-SaCzech, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Ce produit utilise la bibliothèque de compression zlib, Copyright (c) 1995-2002 Jean-loup Gailly et Mark Adler.

Ce produit utilise la bibliothèque de compression libbzip2, Copyright (c) 1996-2002 Julian R. Seward.



## Table des matières

<b>1. Introduction</b>	<b>7</b>
<b>2. Pré-requis à l'installation d'AVG</b>	<b>8</b>
2.1 Systèmes d'exploitation pris en charge	8
2.2 Configuration matérielle minimale et recommandée	8
<b>3. Processus d'installation d'AVG</b>	<b>9</b>
3.1 Bienvenue : Sélection de la langue	9
3.2 Bienvenue : Contrat de licence	10
3.3 Activer la licence	11
3.4 Sélectionner le type d'installation	12
3.5 Options personnalisées	14
3.6 Installer la Barre d'outils de sécurité AVG	15
3.7 Progression de l'installation	16
3.8 Installation réussie	17
<b>4. Opérations à effectuer après l'installation</b>	<b>18</b>
4.1 Enregistrement du produit	18
4.2 Accès à l'interface utilisateur	18
4.3 Analyse complète	18
4.4 Test Eicar	18
4.5 Configuration AVG par défaut	19
<b>5. Interface utilisateur AVG</b>	<b>20</b>
5.1 Menu système	21
5.1.1 Fichier	21
5.1.2 Composants	21
5.1.3 Historique	21
5.1.4 Outils	21
5.1.5 Aide	21
5.1.6 Support	21
5.2 Informations sur l'état de la sécurité	28
5.3 Liens d'accès rapide	29
5.4 Présentation des composants	30
5.5 Icône de la barre d'état	32
5.6 AVG Advisor	34
5.7 Gadget AVG	34



<b>6. Composants AVG</b>	<b>37</b>
6.1 Anti-Virus	37
6.1.1 Moteur d'analyse	37
6.1.2 Protection résidente	37
6.1.3 Protection Anti-spyware	37
6.1.4 Interface de l'Anti-Virus	37
6.1.5 Détections du Bouclier résident	37
6.2 LinkScanner	43
6.2.1 Interface de LinkScanner	43
6.2.2 Détections par Search-Shield	43
6.2.3 Détections de Surf-Shield	43
6.2.4 Détection du Bouclier résident	43
6.3 Protection e-mail	49
6.3.1 Scanner e-mail	49
6.3.2 Anti-spam	49
6.3.3 Interface du composant Protection e-mail	49
6.3.4 Détections du scanner e-mail	49
6.4 Pare-Feu	53
6.4.1 Principes de fonctionnement du pare-feu	53
6.4.2 Profils de pare-feu	53
6.4.3 Interface du Pare-feu	53
6.5 Anti-Rootkit	57
6.5.1 Interface de l'Anti-Rootkit	57
6.6 System Tools	59
6.6.1 Processus	59
6.6.2 Connexions réseau	59
6.6.3 Démarrage automatique	59
6.6.4 Extensions du navigateur	59
6.6.5 Visualiseur LSP	59
6.7 PC Analyzer	65
6.8 Identity Protection	67
6.8.1 Interface d'Identity Protection	67
6.9 Administration à distance	69
<b>7. Mes applications</b>	<b>70</b>
7.1 AVG Family Safety	70
7.2 AVG LiveKive	71
7.3 AVG Mobilation	71



7.4 AVG PC Tuneup.....	72
<b>8. AVG Security Toolbar.....</b>	<b>74</b>
<b>9. AVG Do Not Track.....</b>	<b>76</b>
9.1 AVG Do Not Track.....	77
9.2 Informations sur les processus de suivi.....	78
9.3 Bloquer les processus de suivi.....	79
9.4 Paramètres AVG Do Not Track.....	79
<b>10. Paramètres avancés d'AVG.....</b>	<b>82</b>
10.1 Affichage.....	82
10.2 Sons .....	86
10.3 Désactiver provisoirement la protection AVG.....	87
10.4 Anti-Virus.....	88
10.4.1 Bouclier résident.....	88
10.4.2 Serveur de cache.....	88
10.5 Protection e-mail.....	94
10.5.1 Scanner e-mail.....	94
10.5.2 Anti-spam .....	94
10.6 LinkScanner.....	113
10.6.1 Paramètres LinkScanner.....	113
10.6.2 Bouclier Web.....	113
10.7 Analyses.....	116
10.7.1 Analyse complète.....	116
10.7.2 Analyse contextuelle.....	116
10.7.3 Analyse zones sélectionnées.....	116
10.7.4 Analyse des périphériques amovibles.....	116
10.8 Programmations.....	122
10.8.1 Analyse programmée.....	122
10.8.2 Programmation de la mise à jour des définitions.....	122
10.8.3 Programmation de la mise à jour du programme.....	122
10.8.4 Programmation de la mise à jour de l'anti-spam.....	122
10.9 Mise à jour.....	133
10.9.1 Proxy.....	133
10.9.2 Numérotation.....	133
10.9.3 URL.....	133
10.9.4 Gérer.....	133
10.10 Anti-Rootkit.....	139



10.10.1 Exceptions .....	139
10.11 Identity Protection .....	141
10.11.1 Paramètres d'Identity Protection .....	141
10.11.2 Liste des éléments autorisés .....	141
10.12 Programmes potentiellement dangereux .....	145
10.13 Quarantaine .....	148
10.14 Programme d'amélioration des produits .....	148
10.15 Ignorer les erreurs .....	151
10.16 Advisor – Réseaux connus .....	152
<b>11. Paramètres du Pare-feu .....</b>	<b>153</b>
11.1 Généralités .....	153
11.2 Sécurité .....	154
11.3 Profils de zones et d'adaptateurs .....	155
11.4 IDS .....	157
11.5 Journaux .....	159
11.6 Profils .....	160
11.6.1 Informations sur le profil .....	160
11.6.2 Réseaux définis .....	160
11.6.3 Applications .....	160
11.6.4 Services système .....	160
<b>12. Analyse AVG .....</b>	<b>171</b>
12.1 Interface d'analyse .....	171
12.2 Analyses prédéfinies .....	172
12.2.1 Analyse complète .....	172
12.2.2 Analyse zones sélectionnées .....	172
12.3 Analyse contextuelle .....	181
12.4 Analyse depuis la ligne de commande .....	181
12.4.1 Paramètres d'analyse CMD .....	181
12.5 Programmation de l'analyse .....	184
12.5.1 Paramètres de la programmation .....	184
12.5.2 Comment faire l'analyse .....	184
12.5.3 Objets à analyser .....	184
12.6 Résultats d'analyse .....	194
12.7 Détails des résultats d'analyse .....	195
12.7.1 Onglet Résultats d'analyse .....	195
12.7.2 Onglet Infections .....	195
12.7.3 Onglet Spywares .....	195



12.7.4 Onglet Avertissements.....	195
12.7.5 Onglet Rootkits.....	195
12.7.6 Onglet Informations.....	195
12.8 Quarantaine.....	202
<b>13. Mises à jour d'AVG.....</b>	<b>205</b>
13.1 Exécution de mises à jour.....	205
13.2 Progression de la mise à jour.....	205
13.3 Niveaux de la mise à jour.....	206
<b>14. Journal des évènements.....</b>	<b>208</b>
<b>15. FAQ et assistance technique.....</b>	<b>210</b>



## 1. Introduction

Ce manuel de l'utilisateur constitue la documentation complète du produit **AVG Internet Security 2012**.

**AVG Internet Security 2012** offre plusieurs niveaux de protection pour toutes vos activités en ligne. Vous n'aurez plus à redouter l'usurpation d'identité, les virus ou les sites malveillants. La technologie AVG Protective Cloud et le réseau de protection de la communauté AVG sont inclus. Ce qui veut dire que nous collectons les informations les plus récentes et les partageons avec la communauté afin de nous assurer que chacun reçoit la meilleure protection:

- Achetez et effectuez vos transactions bancaires en toute sécurité grâce aux composants AVG Pare-feu, Anti-Spam et Identity Protection
- Communiquez en toute sécurité sur les réseaux sociaux grâce à AVG Social Networking Protection
- Naviguez et faites des recherches en toute sérénité sous la protection en temps réel d'AVG LinkScanner



## 2. Pré-requis à l'installation d'AVG

### 2.1. Systèmes d'exploitation pris en charge

AVG Internet Security 2012 sert à protéger les postes de travail fonctionnant avec les systèmes d'exploitation suivants :

- Windows XP Edition familiale SP2
- Windows XP Professionnel SP2
- Windows XP Professionnel x64 SP1
- Windows Vista (x86 et x64, toutes éditions confondues)
- Windows 7 (x86 et x64, toutes éditions confondues)

(et éventuellement les service packs de versions ultérieures pour certains systèmes d'exploitation)

**Remarque :** le composant [Identity Protection](#) n'est pas pris en charge par Windows XP x64. Sur ce système d'exploitation, vous pouvez installer AVG Internet Security 2012 sans le composant Identity Protection.

### 2.2. Configuration matérielle minimale et recommandée

Configuration matérielle minimale pour **AVG Internet Security 2012** :

- Processeur Intel Pentium 1,5 GHz
- 512 Mo libres de RAM
- 1000 Mo d'espace disque dur (pour l'installation)

Configuration matérielle recommandée pour **AVG Internet Security 2012** :

- Processeur Intel Pentium 1,8 GHz
- 512 Mo libres de RAM
- 1550 Mo d'espace disque dur (pour l'installation)



### 3. Processus d'installation d'AVG

#### Où trouver le fichier d'installation ?

Pour installer **AVG Internet Security 2012** sur l'ordinateur, vous devez posséder le fichier d'installation le plus récent. Pour être sûr d'installer la dernière version d'**AVG Internet Security 2012**, il est recommandé de vous rendre sur le site Web d'AVG (<http://www.avg.com/>) pour télécharger le fichier d'installation. La section **Centre de support / Téléchargement** contient une présentation structurée des fichiers d'installation de chaque édition d'AVG.

Si vous ne savez pas quels fichiers télécharger et installer, utilisez le service **Sélection du produit** au bas de la page Web. Une fois vous aurez répondu à trois questions simples, il vous sera indiqué quels fichiers vous sont nécessaires. Cliquez sur **Continuer** pour accéder à la liste complète de fichiers téléchargeables, personnalisée pour vos besoins.

#### A quoi ressemble le processus d'installation ?

Après avoir téléchargé le fichier d'installation et l'avoir enregistré sur le disque dur, lancez le processus d'installation, qui consiste en une séquence de boîtes de dialogue simples et faciles à comprendre. Chaque boîte de dialogue décrit brièvement ce qu'il faut faire à chaque étape du processus d'installation. Ces fenêtres sont expliquées en détail ci-dessous.

#### 3.1. Bienvenue : Sélection de la langue

Le processus d'installation commence par la boîte de dialogue **Bienvenue dans l'Assistant d'installation d'AVG** :



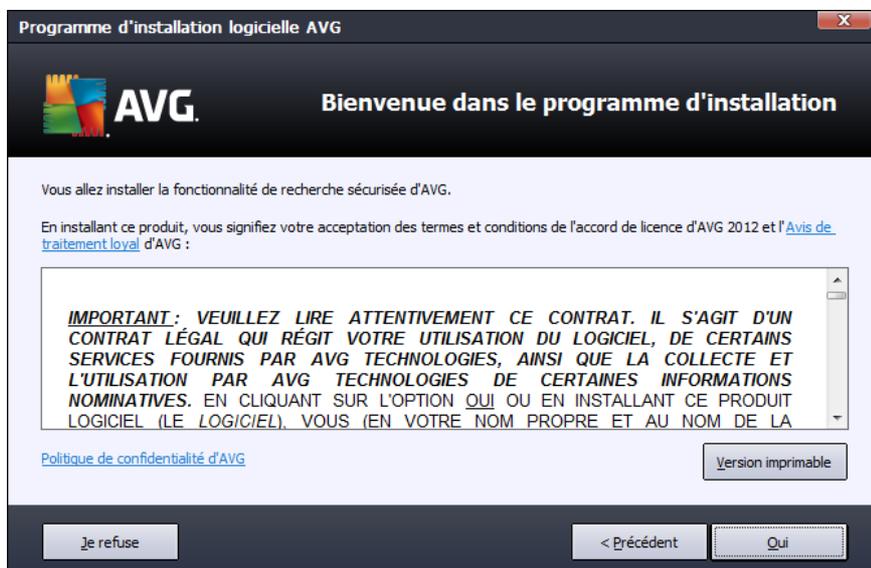
A ce stade, vous pouvez choisir la langue à utiliser pour le processus d'installation. Dans l'angle droit de la boîte de dialogue, cliquez sur le menu déroulant pour afficher les langues. Choisissez-en une. Le processus d'installation se poursuivra dans cette langue.



**Attention : A ce stade, vous choisissez seulement la langue du processus installation. L'application AVG Internet Security 2012 sera installée dans la langue choisie, mais aussi en anglais, dont l'installation est automatique. Toutefois, il est possible d'ajouter d'autres langues et d'utiliser AVG Internet Security 2012 dans l'une d'elles. Vous serez invité à confirmer l'ensemble des langues sélectionnées dans l'une des boîtes de dialogue de configuration [Options personnalisées](#).**

### 3.2. Bienvenue : Contrat de licence

A l'étape suivante, la boîte de dialogue **Bienvenue dans l'Assistant d'installation d'AVG** contient le texte intégral du Contrat de licence AVG :



Veillez lire attentivement l'intégralité du texte. Pour indiquer que vous avez lu, compris et accepté l'accord, cliquez sur le bouton **Oui**. Si vous n'acceptez pas les termes de la licence, cliquez sur le bouton **Je refuse** ; le processus d'installation prendra fin immédiatement.

#### Politique de confidentialité d'AVG

Outre le Contrat de licence, la boîte de dialogue de configuration donne l'occasion d'en savoir plus sur la Politique de confidentialité d'AVG. Dans l'angle inférieur gauche, vous trouverez le lien **Politique de confidentialité d'AVG**. Cliquez sur ce lien pour accéder au site Web d'AVG (<http://www.avg.com/>) et prendre connaissance de l'ensemble des principes de la Politique de confidentialité d'AVG Technologies.

#### Boutons de commande

La première boîte de dialogue de configuration contient uniquement deux boutons :

- **Version imprimable** : Cliquez sur ce bouton pour imprimer l'intégralité du texte du Contrat



de licence AVG.

- **Je refuse** : Cliquez sur ce bouton pour refuser le contrat de licence. Dans ce cas, le processus de configuration s'arrête immédiatement. **AVG Internet Security 2012** ne sera pas installé !
- **Précédent** – cliquez sur ce bouton pour retourner à l'étape de configuration précédente.
- **J'accepte** : Cliquez sur ce bouton pour confirmer que vous avez lu, compris et accepté le contrat de licence. L'installation se poursuit alors et la boîte de dialogue suivante s'ouvre.

### 3.3. Activer la licence

Dans la boîte de dialogue visant à **activer votre licence AVG**, indiquez votre numéro de licence dans le champ prévu à cet effet:

Programme d'installation logicielle AVG

**AVG** Activer la licence

Numéro de licence :

Exemple : IQNP6-9BCA8-PUQU2-A5HCK-GP338L-93OCB

Si vous avez acheté le logiciel AVG 2012 en ligne, vous recevrez le numéro de licence par e-mail. Pour éviter toute erreur de frappe, nous vous recommandons de copier-coller le numéro reçu par e-mail, dans l'écran actuel.

Si vous avez acheté le logiciel auprès d'un détaillant, vous trouverez le numéro de licence sur la carte d'enregistrement du produit incluse dans le coffret. Prenez soin de copier le numéro tel qu'il figure sur la carte.

Annuler < Précédent Suivant >

#### Où trouver le numéro de licence

Le numéro d'achat se trouve dans le coffret du CD-ROM contenant le programme **AVG Internet Security 2012**. Le numéro de licence figure dans l'e-mail de confirmation que vous avez reçu après avoir acheté le produit **par Internet**. Vous devez saisir le numéro tel qu'il apparaît. Si le numéro de licence est disponible au format électronique (*par exemple, dans un mail*), il est recommandé de l'insérer à l'aide de la méthode copier-coller.

#### Comment utiliser la méthode copier-coller

La méthode **copier-coller** permet d'entrer le numéro de licence du produit **AVG Internet Security 2012** sans faire d'erreurs. Pour ce faire, procédez comme suit :



- Ouvrez le courrier contenant votre numéro de licence.
- Cliquez sur le premier caractère du numéro de licence et faites glisser la souris tout en maintenant le bouton appuyé jusqu'au dernier caractère, puis relâchez le bouton. Le numéro devrait être sélectionné (il apparaît sur fond bleu).
- Maintenez la touche **Ctrl** enfoncée, puis appuyez sur la touche **C**. Le numéro est copié.
- Cliquez pour positionner le curseur à l'endroit voulu (où vous voulez copier le numéro).
- Maintenez la touche **Ctrl** enfoncée, puis appuyez sur la touche **V**. Le numéro est collé à l'emplacement choisi.

### Boutons de commande

Comme pour la plupart des boîtes de dialogue de configuration, trois boutons de commande sont disponibles :

- **Annuler** – cliquez sur ce bouton pour quitter immédiatement le processus. **AVG Internet Security 2012** ne sera pas installé !
- **Précédent** – cliquez sur ce bouton pour retourner à l'étape de configuration précédente.
- **Suivant** – cliquez sur ce bouton pour poursuivre l'installation et avancer d'une étape.

### 3.4. Sélectionner le type d'installation

La boîte de dialogue **Sélectionner le type d'installation** propose deux modes d'installation : **Installation rapide** et **Installation personnalisée** :





## Installation rapide

Dans la majorité des cas, il est recommandé d'opter pour l'**Installation rapide**, qui installe automatiquement **AVG Internet Security 2012** selon les paramètres prédéfinis par l'éditeur du logiciel, notamment le [Gadget AVG](#). Cette configuration allie un maximum de sécurité et une utilisation optimale des ressources. Par la suite, vous aurez toujours la possibilité de modifier la configuration directement dans l'application **AVG Internet Security 2012**.

Dans cette option, vous pouvez observer deux cases précochées et il est fortement recommandé de les laisser activées :

- **Je souhaite définir AVG Secure Search comme mon moteur de recherche par défaut** – laissez cette option activée pour confirmer que vous souhaitez utiliser le moteur de recherche AVG Secure Search qui fonctionne en étroite collaboration avec le composant [Link Scanner](#) pour vous garantir une sécurité maximale en ligne.
- **Je souhaite installer la Barre d'outils de sécurité AVG** – laissez cette option activée pour installer la [Barre d'outils de sécurité AVG](#) qui maintient un niveau de sécurité élevé lorsque vous surfez sur Internet.

Cliquez sur le bouton **Suivant** pour passer à la boîte de dialogue suivante [Installer la Barre d'outils de sécurité AVG](#).

## Installation personnalisée

L'**Installation personnalisée** est exclusivement réservée aux utilisateurs expérimentés qui ont une raison valable d'installer **AVG Internet Security 2012** selon des paramètres non standard. Cela leur permet d'adapter le programme à une configuration système spécifique.

Si vous sélectionnez cette option, une nouvelle section intitulée **Dossier de destination** s'affiche dans la boîte de dialogue. Vous devez ici indiquer l'emplacement dans lequel **AVG Internet Security 2012** doit être installé. Par défaut, **AVG Internet Security 2012** est installé dans le dossier contenant les fichiers programme sur le lecteur C:, comme indiqué dans la zone de texte de la boîte de dialogue. Si vous optez pour un autre emplacement, cliquez sur le bouton **Parcourir** pour consulter l'organisation du lecteur, puis sélectionnez le dossier souhaité. Pour rétablir la destination prédéfinie par défaut par l'éditeur du logiciel, cliquez sur le bouton **Par défaut**.

Après la sélection de cette option, cliquez sur le bouton **Suivant** pour ouvrir la boîte de dialogue [Options personnalisées](#).

## Boutons de commande

Comme pour la plupart des boîtes de dialogue de configuration, trois boutons de commande sont disponibles :

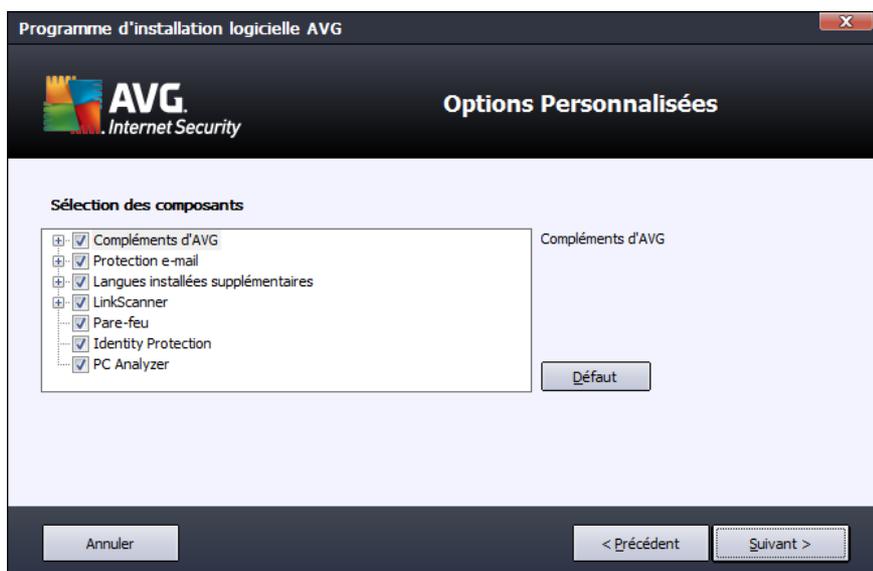
- **Annuler** – cliquez sur ce bouton pour quitter immédiatement le processus. **AVG Internet Security 2012** ne sera pas installé !



- **Précédent** – cliquez sur ce bouton pour retourner à l'étape de configuration précédente.
- **Suivant** – cliquez sur ce bouton pour poursuivre l'installation et avancer d'une étape.

### 3.5. Options personnalisées

La boîte de dialogue **Options personnalisées** permet de configurer des paramètres d'installation détaillés :



La section **Sélection des composants** présente tous les composants d'**AVG Internet Security 2012** pouvant être installés. Si les paramètres par défaut ne vous satisfont pas, vous pouvez supprimer ou ajouter des composants spécifiques.

**Notez que vous pouvez seulement choisir des composants inclus dans l'Édition AVG dont vous avez acquis les droits.**

Mettez en surbrillance un élément de la liste **Sélection des composants** : une brève description du composant correspondant s'affiche à droite de la section. Pour plus d'informations sur le rôle de chacun des composants, consultez le chapitre [Présentation des composants](#) de la présente documentation. Pour rétablir la configuration prédéfinie par défaut par l'éditeur du logiciel, cliquez sur le bouton **prévu à cet effet**.

#### Boutons de commande

Comme pour la plupart des boîtes de dialogue de configuration, trois boutons de commande sont disponibles :

- **Annuler** – cliquez sur ce bouton pour quitter immédiatement le processus. **AVG Internet Security 2012** ne sera pas installé !
- **Précédent** – cliquez sur ce bouton pour retourner à l'étape de configuration précédente.



- **Suivant** – cliquez sur ce bouton pour poursuivre l'installation et avancer d'une étape.

### 3.6. Installer la Barre d'outils de sécurité AVG



La boîte de dialogue **Barre d'outils de sécurité AVG** offre le choix entre installer ou ne pas installer la fonctionnalité **Barre de sécurité AVG**. Si vous ne modifiez pas les paramètres par défaut, ce composant sera installé automatiquement dans votre navigateur Internet (*seuls Microsoft Internet Explorer v. 6.0 ou version supérieure et Mozilla Firefox v. 3.0 ou version supérieure sont actuellement pris en charge*) afin de garantir une protection complète sur Internet.

Vous pouvez également choisir *AVG Secure Search (powered by Google)* comme moteur par défaut. Dans ce dernier cas, laissez la case correspondante cochée.

#### Boutons de commande

Comme pour la plupart des boîtes de dialogue de configuration, trois boutons de commande sont disponibles :

- **Annuler** – cliquez sur ce bouton pour quitter immédiatement le processus. **AVG Internet Security 2012** ne sera pas installé !
- **Précédent** – cliquez sur ce bouton pour retourner à l'étape de configuration précédente.
- **Suivant** – cliquez sur ce bouton pour poursuivre l'installation et avancer d'une étape.



### 3.7. Progression de l'installation

La boîte de dialogue *Progression de l'installation* montre la progression du processus d'installation et ne requiert aucune intervention de votre part :



Une fois que l'installation est terminée, vous accédez automatiquement à la boîte de dialogue suivante.

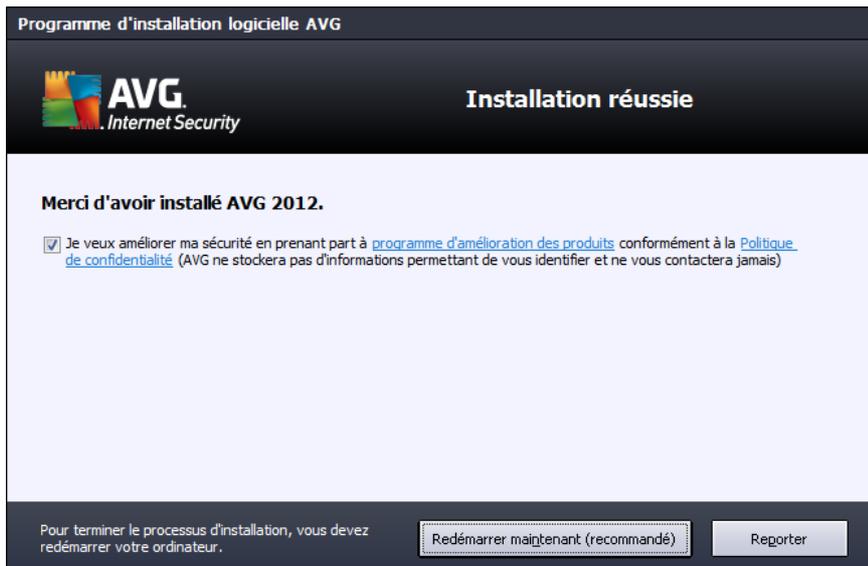
#### Boutons de commande

Cette boîte de dialogue comporte un seul bouton de commande : **Annuler**. Il ne doit être utilisé que pour arrêter le processus d'installation. Notez que dans ce cas, **AVG Internet Security 2012** ne sera pas installé !



### 3.8. Installation réussie

La boîte de dialogue **Installation réussie** confirme que le programme **AVG Internet Security 2012** est bien installé et configuré:



#### Programme d'amélioration des produits

Cette boîte de dialogue permet de choisir de participer ou non au Programme d'amélioration des produits (*pour en savoir plus, voir le chapitre [Paramètres avancés d'AVG / Programme d'amélioration des produits](#)*) qui recueille de façon anonyme des informations sur les menaces détectées, dans le but d'améliorer le niveau de sécurité global d'Internet. Si vous acceptez cette déclaration, ne décochez pas l'option **J'accepte de participer à la sécurité Web d'AVG 2012 et au Programme d'amélioration des produits ...** (*elle est cochée par défaut*).

#### Redémarrage de l'ordinateur

Pour terminer le processus d'installation, vous devez redémarrer l'ordinateur. Sélectionnez (**Redémarrer maintenant**) ou différer le redémarrage (**Reporter**).



## 4. Opérations à effectuer après l'installation

### 4.1. Enregistrement du produit

Une fois l'installation d'**AVG Internet Security 2012** terminée, enregistrez votre produit en ligne sur le site Web d'AVG (<http://www.avg.com/>). Après l'enregistrement, vous bénéficierez de tous les avantages associés à votre compte utilisateur AVG et aurez accès à la lettre d'informations d'AVG ainsi qu'aux autres services réservés exclusivement aux utilisateurs enregistrés.

Le moyen le plus simple d'enregistrer le produit consiste à le faire directement dans l'interface d'utilisateur d'**AVG Internet Security 2012**. Dans le menu principal, sélectionnez [Aide/Enregistrer maintenant](#). La page d'**enregistrement** du site Web d'AVG (<http://www.avg.com/>) s'ouvre. Suivez l'instruction fournie dans cette page.

### 4.2. Accès à l'interface utilisateur

La [boîte de dialogue principale d'AVG](#) est accessible de plusieurs façons :

- double-cliquez sur l'[icône de la barre d'état système AVG](#)
- double-cliquez sur l'icône AVG située sur le Bureau
- à partir du menu **Démarrer / Tous les programmes / AVG 2012**

### 4.3. Analyse complète

Le risque de contamination de l'ordinateur par un virus avant l'installation d'**AVG Internet Security 2012** ne doit pas être écarté. C'est pour cette raison qu'il est recommandé d'exécuter une [analyse complète](#) afin de s'assurer qu'aucune infection ne s'est déclarée dans votre ordinateur. La première analyse peut prendre un peu de temps (*environ une heure*) mais il est recommandé de la lancer pour vous assurer que votre ordinateur n'a pas été compromis par une menace. Pour obtenir des instructions sur l'exécution d'une [Analyse complète](#), consultez le chapitre [Analyse AVG](#).

### 4.4. Test Eicar

Pour confirmer qu'**AVG Internet Security 2012** est bien installé, réalisez un test EICAR.

Cette méthode standard et parfaitement sûre sert à tester le fonctionnement de l'anti-virus en introduisant un pseudo-virus ne contenant aucun fragment de code viral et ne présentant absolument aucun danger. La plupart des produits réagissent comme s'il s'agissait d'un véritable virus (*en lui donnant un nom significatif du type « EICAR-AV-Test »*). Vous pouvez télécharger le test Eicar à partir du site Web Eicar à l'adresse [www.eicar.com](http://www.eicar.com) où vous trouverez toutes les informations nécessaires.

Essayez de télécharger le fichier **eicar.com** et enregistrez-le sur votre disque dur local. Dès que vous confirmez le téléchargement du fichier test, le [Bouclier Web](#) (*qui appartient au composant [Link Scanner](#)*) va afficher un avertissement. Ce message du Bouclier Web indique qu'AVG est installé correctement sur votre ordinateur.



A partir du site Web <http://www.eicar.com>, vous pouvez aussi télécharger la version compacte du « virus » EICAR (sous la forme *eicar\_com.zip*, par exemple). [Le Bouclier Web](#) permet de télécharger ce fichier et de l'enregistrer sur votre disque local, mais le [Bouclier résident](#) (au sein du composant [Anti-Virus](#)) détecte le « virus » au moment où vous décompressez ce fichier.

**Si AVG n'identifie pas le fichier test Eicar comme un virus, il est recommandé de vérifier de nouveau la configuration du programme.**

#### 4.5. Configuration AVG par défaut

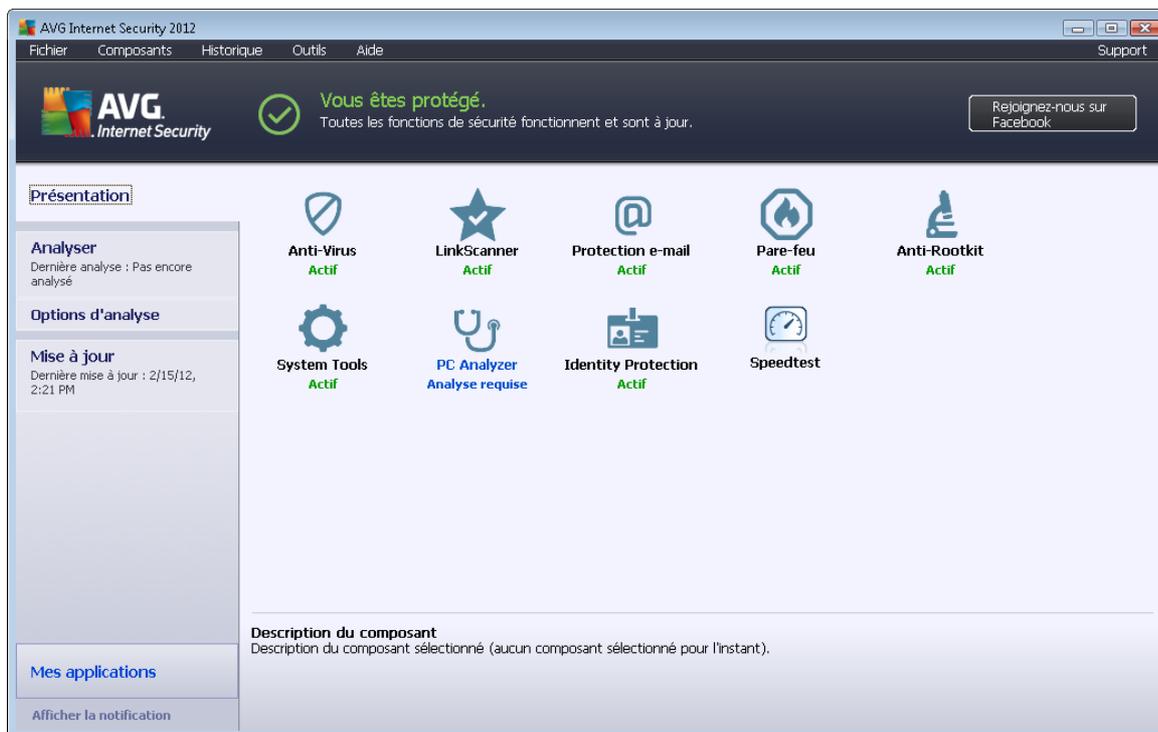
La configuration par défaut (c'est-à-dire la manière dont l'application est paramétrée à l'issue de l'installation) d'AVG Internet Security 2012 est définie par l'éditeur du logiciel de sorte que les composants et les fonctions délivrent leurs performances optimales.

***Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté.***

Il est possible d'apporter certaines corrections mineures aux paramètres des [composants AVG](#), directement dans l'interface utilisateur du composant concerné. Si vous voulez modifier la configuration d'AVG pour mieux l'adapter à vos besoins, accédez aux [paramètres avancés d'AVG](#) : cliquez sur le menu **Outils/Paramètres avancés** et modifiez la configuration AVG dans la boîte de dialogue [Paramètres avancés d'AVG](#) qui s'affiche.

## 5. Interface utilisateur AVG

La fenêtre principale du programme **AVG Internet Security 2012** s'affiche :



La fenêtre principale comprend plusieurs parties :

- **Menu système** (barre de menus en haut de la fenêtre) : ce système de navigation standard donne accès à l'ensemble des composants, des services et des fonctions d'**AVG Internet Security 2012**. [Détails >>](#)
- **Informations sur l'état de la sécurité** (partie supérieure de la fenêtre) : donne des informations sur l'état actuel du programme **AVG Internet Security 2012** – [détails >>](#)
- Λε βουτων **Rejoignez-nous sur Facebook** (angle supérieur droit de la fenêtre) vous permet de rejoindre la [communauté AVG sur Facebook](#). Toutefois, ce bouton n'apparaît que lorsque tous les composants sont totalement opérationnels et fonctionnent correctement (pour plus de détails sur la manière de reconnaître l'état des composants AVG, consultez le chapitre [Informations sur l'état de la sécurité](#))
- **Liens d'accès rapide** (partie gauche de la fenêtre) : ces liens permettent d'accéder rapidement aux tâches les plus importantes et les plus courantes d'**AVG Internet Security 2012**- [détails >>](#)
- **Mes applications** (partie inférieure gauche de la fenêtre) : présente une vue d'ensemble des applications disponibles dans **AVG Internet Security 2012** : [LiveKive](#), [Family Safety](#) et [PC Tuneup](#)
- **Présentation des composants** (partie centrale de la fenêtre) : présentation générale de



tous les composants **AVG Internet Security 2012** installés - [détails >>](#)

- **Icône d'état**  (coin inférieur droit de l'écran, sur la barre d'état système) : elle indique l'état actuel du programme **AVG Internet Security 2012** - [détails >>](#)
- **Gadget AVG** (Volet Windows pour Windows Vista/7) : permet un accès rapide aux analyses et mises à jour **AVG Internet Security 2012** – [détails >>](#)

## 5.1. Menu système

Le **menu système** est le système de navigation standard propre à toutes les applications Windows. Il se présente sous la forme d'une barre horizontale en haut de la fenêtre principale du programme **AVG Internet Security 2012**. Servez-vous du menu système pour accéder aux composants, fonctions et services AVG de votre choix.

Le menu système inclut cinq sections principales :

### 5.1.1. Fichier

- **Quitter**  – ferme l'interface utilisateur d'**AVG Internet Security 2012**. L'application AVG continue néanmoins de s'exécuter en arrière-plan de sorte que l'ordinateur reste protégé !

### 5.1.2. Composants

L'option [Composants](#) du menu système contient des liens qui renvoient vers tous les composants AVG installés et ouvrent la boîte de dialogue par défaut associée dans l'interface utilisateur :

- **Présentation du système** – ouvre l'interface utilisateur par défaut et affiche [une présentation générale de tous les composants installés et leur état](#)
- **Le composant Anti-Virus** détecte les virus, spywares, vers, chevaux de Troie, fichiers exécutables ou bibliothèques indésirables sur votre système ; il vous protège également des adwares malveillants - [détails >>](#)
- **Le composant LinkScanner** vous protège des attaques Internet pendant que vous effectuez des recherches ou surfez sur Internet – [détails >>](#)
- **Le composant Protection e-mail** analyse vos messages entrants pour y détecter les messages indésirables et bloquer les virus, attaques par hameçonnage ou autres menaces – [détails >>](#)
- **Le composant Pare-feu** contrôle toutes les communications sur chaque port réseau, vous protégeant des attaques malveillantes et bloquant toutes les tentatives d'intrusion - [détails >>](#)
- **Le composant Anti-Rootkit** recherche les rootkits dangereux dissimulés dans les applications, les pilotes ou les bibliothèques – [détails >>](#)
- **Le composant System Tools** décrit de manière détaillée l'environnement AVG et le système d'exploitation – [détails >>](#)
- **PC Analyzer** renseigne sur l'état de l'ordinateur – [détails >>](#)



- **Identity Protection** est constamment en veille et protège vos données numériques contre les menaces nouvelles et inconnues – [détails >>](#)
- **L'outil Administration à distance** n'apparaît que dans les Editions Business d'AVG si vous avez précisé, au cours de l'[installation](#), que vous vouliez installer ce composant

### 5.1.3. Historique

- [Résultats des analyses](#) – affiche l'interface d'analyse AVG et ouvre notamment la boîte de dialogue [Résultats d'analyse](#)
- [Détection du Bouclier résident](#) – ouvre la boîte de dialogue contenant une vue générale des menaces détectées par le [Bouclier résident](#)
- [Détection du Scanner e-mail](#) – ouvre la boîte de dialogue des pièces jointes détectées comme dangereuses par le composant [Protection e-mail](#)
- [Objets trouvés par Bouclier Web](#) – ouvre la boîte de dialogue contenant une vue générale des menaces détectées par le service [Bouclier Web](#) du composant [LinkScanner](#)
- [Quarantaine](#) – ouvre l'interface de la zone de confinement ([Quarantaine](#)) dans laquelle AVG place les infections détectées qui n'ont pu, pour une raison quelconque, être réparées automatiquement. À l'intérieur de cette quarantaine, les fichiers infectés sont isolés. L'intégrité de la sécurité de l'ordinateur est donc garantie et les fichiers infectés sont stockés en vue d'une éventuelle réparation future
- [Journal de l'historique des événements](#) – ouvre l'interface de l'historique des événements présentant toutes les actions consignées du programme **AVG Internet Security 2012**.
- [Journal du pare-feu](#) – ouvre l'interface de configuration du pare-feu à l'onglet [Journaux](#) qui présente une vue générale des actions du pare-feu

### 5.1.4. Outils

- [Analyse de l'ordinateur](#) – lance une analyse complète de l'ordinateur.
- [Analyser le dossier sélectionné...](#) – ouvre l'[Interface d'analyse AVG](#) et permet de spécifier, au sein de l'arborescence de l'ordinateur, les fichiers et les dossiers à analyser.
- **Analyser le fichier...** – permet de lancer sur demande l'analyse d'un fichier sélectionné. Cliquez sur cette option pour ouvrir une nouvelle fenêtre contenant l'arborescence de votre disque. Sélectionnez le fichier souhaité et confirmez le lancement de l'analyse.
- [Mise à jour](#) – lance automatiquement le processus de mise à jour d'**AVG Internet Security 2012**.
- **Mise à jour depuis le répertoire** – effectue la mise à jour à l'aide de fichiers situés dans le dossier spécifié de votre disque local. Notez que cette option n'est recommandée qu'en cas d'urgence, c'est-à-dire si vous ne disposez d'aucune connexion Internet (*si, par exemple, l'ordinateur est infecté et déconnecté d'Internet ou s'il est relié à un réseau sans accès à Internet, etc.*). Dans la nouvelle fenêtre qui apparaît, sélectionnez le dossier dans lequel vous avez placé le fichier de mise à jour et lancez la procédure de mise à jour.



- [Paramètres avancés](#) – ouvre la boîte de dialogue [Paramètres avancés d'AVG](#) qui permet de modifier la configuration d'AVG Internet Security 2012 . En général, il est recommandé de conserver les paramètres par défaut de l'application tels qu'ils ont été définis par l'éditeur du logiciel.
- [Paramètres du Pare-feu](#) – ouvre une boîte de dialogue autonome permettant de définir la configuration avancée du composant [Pare-feu](#).

### 5.1.5. Aide

- **Sommaire** – ouvre les fichiers d'aide du programme AVG
- **Obtenir de l'aide** – affiche le site Web d'AVG (<http://www.avg.com/>) à la page du Centre de Support Clients
- **Site Internet AVG** – ouvre le site Web d'AVG (<http://www.avg.com/>)
- **A propos des virus et des menaces** – ouvre l'[Encyclopédie des virus en ligne](#), dans laquelle vous obtenez des informations détaillées sur le virus identifié
- **Réactiver** – ouvre la boîte de dialogue **Activer AVG** avec les données que vous avez saisies dans la boîte de dialogue [Personnaliser AVG](#) au cours du [processus d'installation](#). Dans cette boîte de dialogue, vous indiquez votre numéro de licence en lieu et place de la référence d'achat (*le numéro indiqué lors de l'installation d'AVG*) ou de votre ancien numéro (*si vous installez une mise à niveau du produit AVG, par exemple*).
- **Enregistrer maintenant** – renvoie à la page d'enregistrement du site Web d'AVG (<http://www.avg.com/>). Complétez le formulaire d'enregistrement ; seuls les clients ayant dûment enregistré leur produit AVG peuvent bénéficier de l'assistance technique gratuite.

**Remarque :** *si vous utilisez une version d'évaluation d'AVG Internet Security 2012, les deux dernières options sont remplacées par **Acheter et Activer**, ce qui vous permet de vous procurer de suite la version complète du programme. Si le programme **AVG Internet Security 2012** est installé à l'aide d'un numéro d'achat, vous avez alors le choix entre les options **Enregistrer et Activer**.*

- **A propos d'AVG** – ouvre la boîte de dialogue **Informations** comportant six onglets, où sont précisés le nom du programme, la version du programme, la version de la base de données virale, des informations système, le contrat de licence et des informations de contact d' **AVG Technologies CZ**.

### 5.1.6. Support

Le lien **Support** ouvre une boîte de dialogue **Informations** contenant toutes sortes d'informations utiles pour obtenir de l'aide. Vous y trouverez des données de base, relatives à l'application AVG installée (*version de l'application / de la base de données*), les informations de licence et une liste de liens d'accès rapide au support.

La boîte de dialogue **Informations** comporte six onglets :



L'onglet **Version** comporte trois sections :



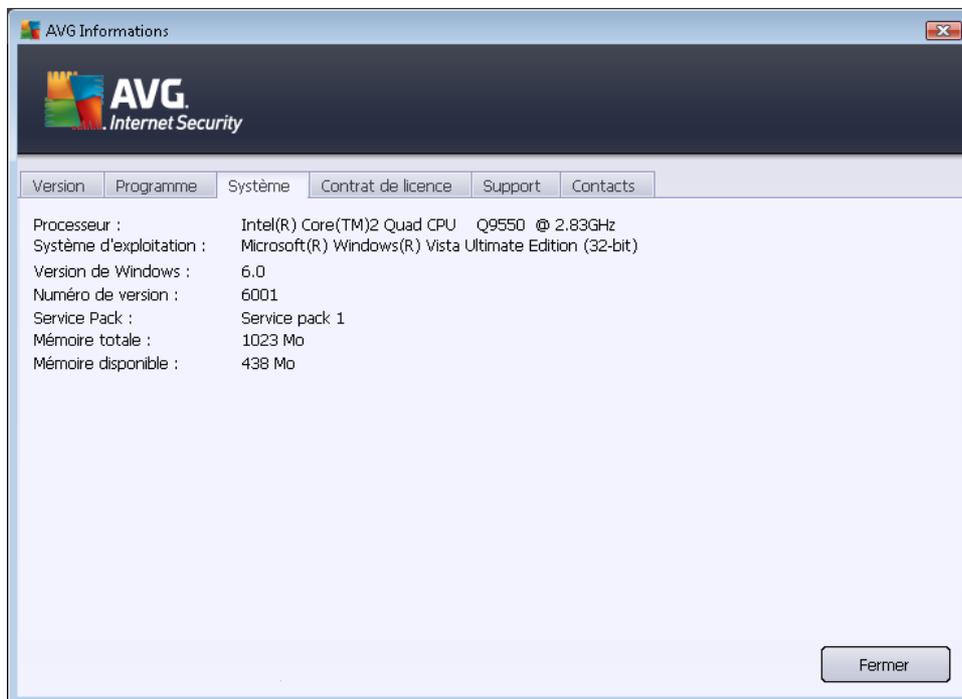
- **Informations de support**- Fournit des informations sur les versions d'**AVG Internet Security 2012**, de la base de données virale, de la base de données [Anti-Spam](#) et de [LinkScanner](#).
- **User Information** (Informations sur l'utilisateur) – Fournit des informations sur l'utilisateur et la société propriétaires de la licence.
- **Informations de licence** – Fournit des informations sur la licence (*nom du produit, type de licence, numéro de licence, date d'expiration et nombre de postes*). Cette section contient également le lien **Enregistrer** qui permet d'enregistrer le produit **AVG Internet Security 2012** en ligne et de bénéficier de l'[Assistance technique AVG](#) complète. De même, le lien **Réenregistrer** permet d'ouvrir la boîte de dialogue **Activer AVG** et de saisir le numéro de licence dans le champ prévu à cet effet à la place du numéro d'achat (*utilisé pour l'AVG Internet Security 2012 installation*) ou de remplacer le numéro de licence actuel par un autre (*par exemple, pour migrer une version supérieure d'AVG*).



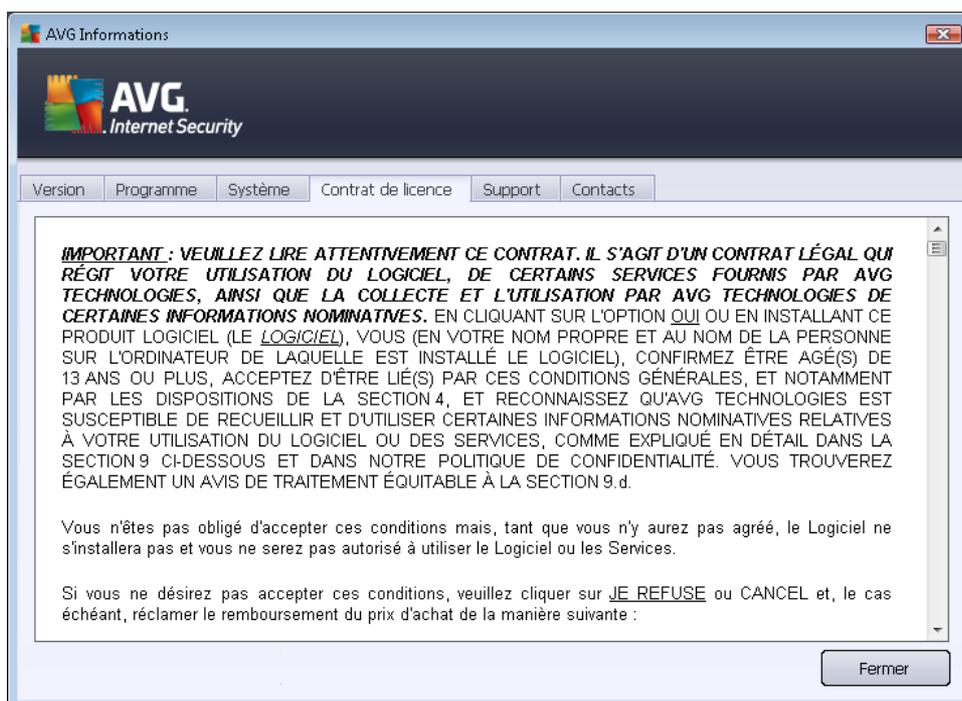
L'onglet **Programme** contient des informations sur la version d'**AVG Internet Security 2012** et les codes tiers utilisés dans le produit.



L'onglet **Système** répertorie les paramètres de votre système d'exploitation (*type de processeur, système d'exploitation et version, numéro de version, services packs utilisés, mémoire totale et mémoire disponible*).



L'onglet **Contrat de licence** contient le texte intégral du contrat de licence qui vous lie à AVG Technologies.



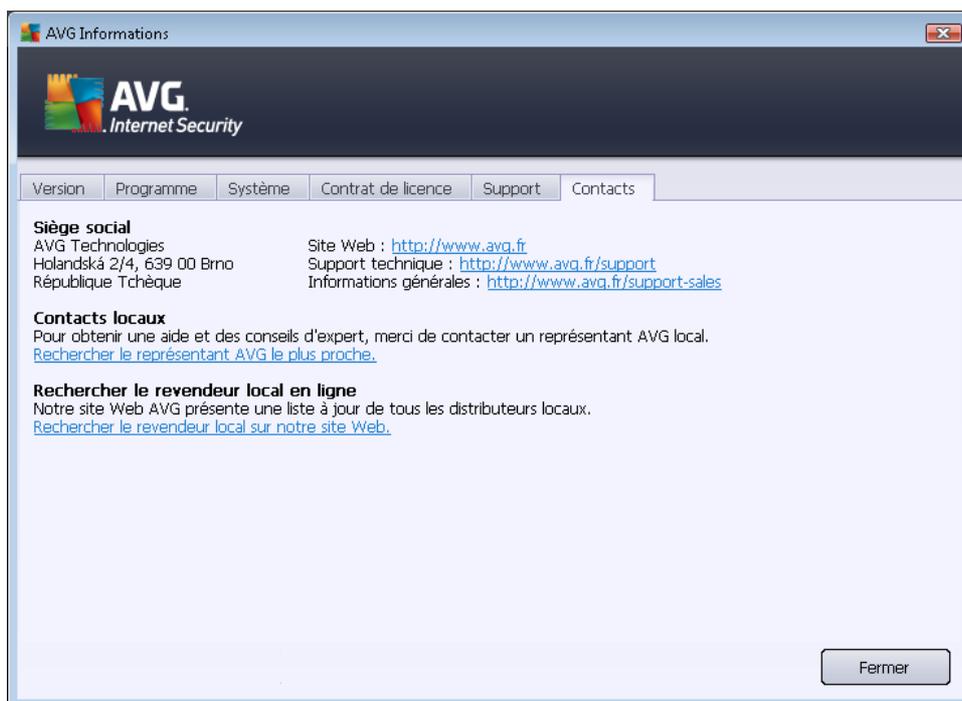


L'onglet **Support** indique les différents moyens de contacter le support clients. En outre, il contient des liens vers le site Web d'AVG (<http://www.avg.com/>), les forums d'AVG, les FAQ, etc. De plus, vous y trouverez les informations à fournir à l'équipe de support clients lorsque vous la contactez.





L'onglet **Contacts** fournit la liste de tous les contacts à AVG Technologies ainsi que les contacts des représentants et revendeurs locaux AVG :



## 5.2. Informations sur l'état de la sécurité

La section **Informations sur l'état de la sécurité** figure dans la partie supérieure de la fenêtre principale d'**AVG Internet Security 2012**. Vous y trouverez des informations sur l'état actuel de la sécurité du programme **AVG Internet Security 2012**. Les icônes illustrées ont la signification suivante :



– L'icône verte indique que le programme **AVG Internet Security 2012 est complètement opérationnel**. Votre système est totalement protégé et à jour ; tous les composants installés fonctionnent convenablement.



– L'icône jaune signale **qu'un ou plusieurs composants ne sont pas correctement configurés**, il est conseillé d'examiner leurs propriétés ou paramètres. Aucun problème critique n'est à signaler dans le programme **AVG Internet Security 2012** ; vous avez sans doute choisi de désactiver certains composants. Vous êtes toujours protégé ! Certains paramètres d'un composant réclament toutefois votre attention. Son nom est indiqué dans la section d'**informations sur l'état de la sécurité**.

L'icône jaune s'affiche également si vous décidez, pour une raison quelconque, d'ignorer les erreurs d'un composant. L'option **Ignorer l'état du composant** est disponible dans le menu



contextuel (qui s'ouvre à l'aide du bouton droit de la souris) qui s'affiche au-dessus de l'icône du composant concerné dans la fenêtre de [présentation des composants](#) de la boîte de dialogue principale d'**AVG Internet Security 2012**. Sélectionnez cette option pour indiquer que vous avez constaté que le composant comporte une erreur, mais que vous souhaitez conserver la configuration d'**AVG Internet Security 2012** en l'état et ne plus être avisé de l'erreur par l'[icône de la barre d'état](#). Vous pouvez être amené à utiliser cette option dans certaines situations, mais il est vivement conseillé de désactiver l'option **Ignorer l'état du composant**, dès que possible.

L'icône jaune peut également s'afficher si votre **AVG Internet Security 2012** nécessite un redémarrage de votre ordinateur (**Redémarrage nécessaire**). Tenez compte de cet avertissement et redémarrez votre ordinateur en cliquant sur le bouton **Redémarrer maintenant**.



– L'icône orange indique que l'état d'**AVG Internet Security 2012 est critique** ! Un ou plusieurs composants ne fonctionnent pas convenablement : **AVG Internet Security 2012** n'est plus en mesure d'assurer la protection de l'ordinateur. Veuillez immédiatement vous porter sur le problème signalé. Si vous ne pouvez pas le résoudre, contactez l'équipe du [support technique AVG](#).

**Si AVG Internet Security 2012 n'est pas configuré de manière optimale, un nouveau bouton, Corriger (ou Tout corriger si le problème implique plusieurs composants), apparaît près des informations relatives au statut de la sécurité. Cliquez sur le bouton pour lancer le processus automatique de vérification et de configuration du programme. C'est un moyen simple d'optimiser les performances d'AVG Internet Security 2012 et d'établir un niveau de sécurité maximal !**

Il est vivement conseillé de ne pas ignorer les informations sur l'état de la sécurité et, en cas de problème indiqué, de rechercher immédiatement une solution. A défaut, vous risquez de mettre en péril la sécurité de votre système.

**Remarque :** vous pouvez à tout moment obtenir des informations sur l'état du programme **AVG Internet Security 2012** en consultant l'[icône de la barre d'état système](#).

### 5.3. Liens d'accès rapide

**Les liens d'accès rapide** se trouvent sur le côté gauche de l'[interface utilisateur](#) d'**AVG Internet Security 2012**. Ils permettent d'accéder instantanément aux fonctions de l'application les plus importantes et les plus utilisées, comme l'analyse et la mise à jour. Ils sont disponibles dans chaque boîte de dialogue de l'interface utilisateur.



Au plan graphique, les **liens d'accès rapide** sont répartis en trois sections :

- **Analyser** : par défaut, ce bouton affiche les informations de la dernière analyse (*c'est-à-dire, le type et la date d'exécution de l'analyse*). Cliquez sur le bouton **Analyser** pour exécuter de nouveau la même analyse. Pour lancer une autre analyse, cliquez sur le lien **Options d'analyse**. Cette action ouvre l'[interface d'analyse d'AVG](#) qui permet d'exécuter ou de programmer des analyses ou d'en modifier les paramètres. (*Pour en savoir plus, consultez le chapitre [Analyse AVG](#)*)
- **Options d'analyse** : ce lien permet de passer de la boîte de dialogue d'AVG ouverte à la fenêtre par défaut, qui [présente tous les composants installés](#). (*Pour en savoir plus, consultez le chapitre [Présentation des composants](#)*)
- **Mise à jour** : ce lien indique la date et l'heure de la dernière [mise à jour](#). Cliquez sur le bouton pour exécuter immédiatement le processus de mise à jour et en suivre la progression. (*Pour en savoir plus, consultez le chapitre [Mises à jour AVG](#)*)

**Les liens d'accès rapide** sont accessibles en permanence dans l'[interface utilisateur d'AVG](#). Lorsque vous cliquez sur un lien d'accès rapide (analyse ou mise à jour), l'application ouvre une nouvelle boîte de dialogue, mais les liens d'accès rapides restent disponibles. En outre, le processus en cours est décrit graphiquement dans la navigation, pour permettre de surveiller la totalité des processus qui s'exécutent dans **AVG Internet Security 2012** à cet instant.

## 5.4. Présentation des composants

### Sections Présentation des composants

La section **Présentation des composants** figure dans la partie centrale de l'[interface utilisateur d'AVG Internet Security 2012](#). La section comprend deux parties :

- **Présentation des composants installés** présente sous forme de volets graphique tous les composants installés. Chaque panneau est identifié par l'icône du composant et fournit des informations sur l'état actuel de ce dernier (actif ou inactif).
- **La description** du composant figure dans la partie inférieure de cette boîte de dialogue. Elle consiste en une explication succincte des principales fonctionnalités du composant. Elle fournit également des informations sur l'état actuel du composant sélectionné.



## Liste des composants installés

Dans **AVG Internet Security 2012**, le panneau de **présentation des composants** contient des renseignements sur les composants suivants :

- **Le composant Anti-Virus** détecte les virus, spywares, vers, chevaux de Troie, fichiers exécutables ou bibliothèques indésirables sur votre système ; il vous protège également des adwares malveillants - [détails >>](#)
- **Le composant LinkScanner** vous protège des attaques dès que vous effectuez des recherches ou naviguez sur Internet – [détails >>](#)
- **Le composant Protection e-mail** analyse vos messages entrants pour y détecter les messages indésirables et bloquer les virus, les attaques par phishing ou autres menaces – [détails >>](#)
- **Le composant Pare-feu** contrôle toutes les communications sur chaque port réseau, vous protégeant des attaques malveillantes et bloquant toutes les tentatives d'intrusion - [détails >>](#)
- **Le composant Anti-Rootkit** recherche les rootkits dangereux dissimulés dans les applications, les pilotes ou les bibliothèques – [détails >>](#)
- **System Tools** décrit de manière détaillée l'environnement AVG et le système d'exploitation – [détails >>](#)
- **PC Analyzer** renseigne sur l'état de l'ordinateur – [détails >>](#)
- **Identity Protection** est constamment en veille et protège vos données numériques contre les menaces nouvelles et inconnues – [détails >>](#)
- **L'outil Administration à distance** n'apparaît que dans les Editions Business d'AVG si vous avez précisé, au cours de l'[installation](#), que vous vouliez installer ce composant

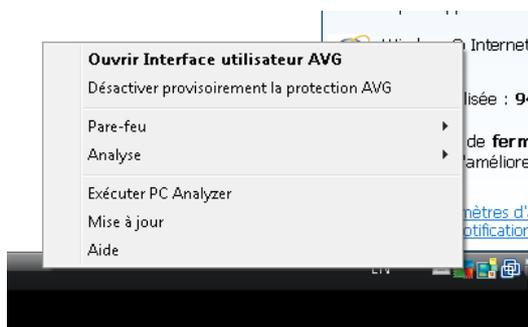
## Actions accessibles

- **Cliquer sur l'icône d'un composant** permet de le mettre en surbrillance dans la vue générale des composants. Par ailleurs, la fonctionnalité de base du composant est décrite en bas de l'[interface utilisateur](#).
- **Cliquer une fois sur l'icône d'un composant** a pour effet d'ouvrir la propre interface du composant présentant une liste de données statistiques.
- **Cliquez avec le bouton droit sur l'icône d'un composant** pour dérouler un menu contextuel comportant plusieurs options :
  - **Ouvrir** – Cliquer sur cette option a pour effet d'ouvrir la boîte de dialogue du composant (*comme lorsque vous cliquez une fois sur l'icône du composant*).

- **Ignorer l'état du composant** – Sélectionnez cette option pour indiquer que vous avez noté l'[état incorrect du composant](#), mais que vous souhaitez conserver la configuration AVG en l'état et ne plus être avisé de l'erreur par l'[icône de la barre d'état système](#).
- **Paramètres avancés ...** - Cette option ne s'applique qu'à certains composants, à savoir ceux qui offrent la possibilité de configurer des [paramètres avancés](#).

## 5.5. Icône de la barre d'état

L'**icône de barre d'état d'AVG** (dans la barre des tâches Windows, coin inférieur droit de l'écran) indique l'état actuel d'**AVG Internet Security 2012**. Elle est toujours visible dans la barre d'état, que l'[interface utilisateur](#) d'**AVG Internet Security 2012** soit ouverte ou fermée.



### Affichages de l'icône de barre d'état d'AVG

-  En couleurs complètes sans éléments additionnels, l'icône indique que tous les composants d'**AVG Internet Security 2012** sont actifs et pleinement opérationnels. Toutefois, l'icône peut prendre cette apparence alors qu'un des composants n'est pas pleinement opérationnel, parce que l'utilisateur a choisi d'[en ignorer l'état](#). (En confirmant ce choix (*ignorer l'état du composant*), vous indiquez que vous savez que le [composant comporte une erreur](#) mais que, pour une raison ou une autre, vous ne voulez ni la corriger ni en être averti.)
-  Un point d'exclamation sur l'icône indique qu'un composant (*voire plusieurs*) comporte une [erreur](#). Prêtez attention à ce type d'avertissement à chaque fois et tentez de corriger le problème de configuration incorrecte d'un composant. Pour modifier la configuration d'un composant, double-cliquez sur l'icône de la barre d'état afin d'ouvrir l'[interface utilisateur de l'application](#). Pour identifier les composants comportant une [erreur](#), consultez la section [infos de sécurité](#).
-  L'icône de la barre d'état peut également comporter un rayon lumineux clignotant en rotation. Ce type d'image signale qu'un processus de mise à jour est en cours.
-  En revanche, une flèche sur l'icône signifie que des analyses **AVG Internet Security 2012** sont en cours.



## Informations de l'icône de barre d'état d'AVG

En outre, l'**icône de barre d'état d'AVG** vous informe des activités en cours dans **AVG Internet Security 2012**, mais aussi des éventuels changements d'état de l'application (*exécution automatique d'une analyse ou d'une mise à jour programmée, Changement de profil du pare-feu, changement d'état d'un composant, apparition d'une erreur, etc.*). Ces informations s'affichent dans une fenêtre de l'icône de la barre d'état :



## Actions exécutables via l'icône de barre d'état d'AVG

L'**icône de barre d'état d'AVG** peut également servir de lien d'accès rapide à l'[interface utilisateur](#) d'**AVG Internet Security 2012**. Pour cela, il suffit d'y double-cliquer. Lorsque vous cliquez avec le bouton droit sur l'icône, un menu contextuel affiche brièvement les options suivantes :

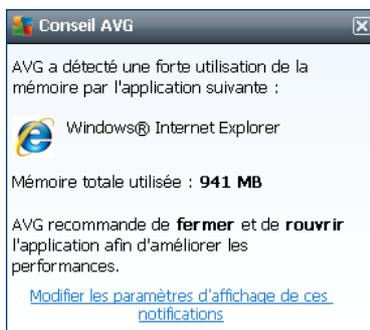
- **Ouvrir Interface utilisateur AVG** – affiche l'[interface utilisateur](#) d'**AVG Internet Security 2012**.
- **Désactiver provisoirement la protection AVG** – cette option vous permet de désactiver entièrement la protection offerte par le programme **AVG Internet Security 2012**. Rappelez-vous que vous ne devez utiliser cette option qu'en cas d'absolue nécessité ! Dans la plupart des cas, il n'est pas nécessaire de désactiver **AVG Internet Security 2012** avant d'installer un nouveau logiciel ou pilote, même si l'assistant d'installation ou le logiciel vous indique d'arrêter tous les programmes et applications s'exécutant sur le système et qui pourraient créer des interruptions inopinées lors du processus d'installation. Si vous êtes amené à désactiver provisoirement **AVG Internet Security 2012**, vous devez le réactiver dès la fin de vos opérations. Si vous êtes connecté à Internet ou à un réseau alors que l'anti-virus est désactivé, l'ordinateur est particulièrement vulnérable.
- **Pare-feu** – ouvre le menu contextuel des options de configuration du [Pare-feu](#) permettant de modifier les paramètres principaux : [Etat du Pare-feu](#) (*Activer Pare-feu/Désactiver Pare-feu/ Mode d'urgence*), [Activer le Mode jeu](#) et [Profils du Pare-feu](#).
- **Analyses** – ouvre le menu contextuel des [Analyses prédéfinies](#) (*Analyse complète et Analyse zones sélectionnées*) qui permet de sélectionner et de lancer immédiatement l'analyse souhaitée.
- **Analyses en cours d'exécution...** - cette option n'est visible que si une analyse est en cours sur l'ordinateur. Vous êtes libre de définir la priorité de ce type d'analyse, de l'interrompre ou de la suspendre. Les options suivantes sont disponibles : *Définir la priorité pour toutes les analyses, Suspendre toutes les analyses ou Arrêter toutes les analyses*.
- **Exécuter PC Analyzer** – lance le composant [PC Analyzer](#).
- **Mise à jour** – lance une [mise à jour](#) immédiate.



- **Aide** – ouvre la première page du fichier d'aide.

## 5.6. AVG Advisor

**AVG Advisor** est une fonction performante qui contrôle en permanence tous les processus s'exécutant sur votre ordinateur afin de détecter les éventuels problèmes et propose des conseils sur la manière d'éviter le problème. **AVG Advisor** s'affiche sous la forme d'une fenêtre contextuelle au dessus de la barre d'état système.



**AVG Advisor** peut s'afficher dans les situations suivantes :

- votre navigateur Internet manque de mémoire ce qui peut ralentir votre travail (*AVG Advisor ne prend en charge que les navigateurs Internet Explorer, Chrome, Firefox, Opera, et Safari*);
- un processus s'exécutant sur votre ordinateur consomme une quantité de mémoire trop importante et affecte les performances de votre ordinateur ;
- votre ordinateur est sur le point de se connecter automatiquement à un réseau WiFi inconnu.

Dans de tels cas de figure, **AVG Advisor** vous signale le problème qui risque de se produire et indique le nom et l'icône du processus ou de l'application à l'origine du conflit. **AVG Advisor** vous suggère également les mesures à prendre pour éviter ce problème.

## 5.7. Gadget AVG

**Le gadget AVG** s'affiche sur le Bureau de Windows (*Volet Windows*). Cette application n'est compatible qu'avec les systèmes d'exploitation Windows Vista et Windows 7. **Le gadget AVG** donne immédiatement accès aux fonctionnalités les plus importantes du programme **AVG Internet Security 2012**, c'est-à-dire aux fonctions d'[analyse](#) et de [mise à jour](#) :



### Accès rapide à l'analyse et à la mise à jour

Le cas échéant, le **gadget AVG** vous permet de lancer immédiatement une analyse ou une mise à jour :

- **Analyser** – Cliquez sur le lien **Analyser** pour lancer directement l'[analyse complète de l'ordinateur](#). Vous pouvez observer la progression d'une analyse dans l'interface utilisateur du gadget. Une brève présentation de statistiques indique le nombre d'objets analysés, de menaces détectées et de menaces réparées. Il est possible de suspendre  ou d'interrompre  l'analyse en cours. Pour des informations détaillées concernant les résultats d'analyse, consultez la boîte de dialogue standard [Résultats d'analyse](#) que vous pouvez ouvrir directement depuis l'option **Afficher les détails** (les résultats d'analyse correspondants s'affichent sous le volet gadget AVG).



- **Mise à jour** – cliquez sur le lien **Mise à jour** pour lancer directement la mise à jour d'**AVG Internet Security 2012** à partir du gadget :



### Accès aux réseaux sociaux

Le **gadget AVG** fournit également un lien rapide pour vous connecter rapidement aux principaux



réseaux sociaux. Utilisez le bouton correspondant pour vous connecter aux communautés AVG dans Twitter, Facebook ou LinkedIn :

- **Lien Twitter**  – Ouvre une nouvelle interface du **Gadget AVG** qui présente les derniers posts d'AVG publiés sur Twitter. Suivez le lien **Afficher tous les posts d'AVG sur Twitter** pour ouvrir votre navigateur Internet dans une nouvelle fenêtre et vous serez redirigé vers le site Web Twitter et notamment à la page consacrée aux actualités de la société AVG :



- **Lien Facebook**  - ouvre le site Web Facebook dans votre navigateur Internet, à la page **Communauté AVG**.
- **LinkedIn**  - cette option n'est disponible qu'au sein d'une installation en réseau (*c'est-à-dire, si vous avez installé AVG à l'aide d'une licence relative à une édition AVG Business*). Elle ouvre votre navigateur Internet au niveau du site **AVG SMB Community** appartenant au réseau social LinkedIn.

### Autres fonctionnalités accessibles via le gadget

- **PC Analyzer**  - Ouvre l'interface utilisateur dans le composant [PC Analyzer](#) et démarre immédiatement l'analyse.
- **Zone de recherche** - insérez un nouveau mot clé et obtenez immédiatement les résultats de recherche dans la nouvelle fenêtre qui s'ouvre, dans votre navigateur Web par défaut.



## 6. Composants AVG

### 6.1. Anti-Virus

Le composant **Anti-Virus** représente la pièce maîtresse de votre programme **AVG Internet Security 2012** et regroupe plusieurs fonctionnalités de base de votre programme de sécurité :

- [Moteur d'analyse](#)
- [Protection résidente](#)
- [Protection Anti-spyware](#)

#### 6.1.1. Moteur d'analyse

Le moteur d'analyse, qui constitue l'élément central du composant **Anti-Virus**, analyse tous les fichiers et activités connexes (*ouverture/fermeture, etc.*) afin de déceler la présence de virus connus. Tout virus détecté sera bloqué, puis supprimé ou mis en [Quarantaine](#).

**Caractéristique importante de la protection AVG Internet Security 2012 : aucun virus connu ne peut s'exécuter sur l'ordinateur !**

#### Méthodes de détection

La plupart des anti-virus font également appel à la méthode heuristique en utilisant les caractéristiques des virus, appelées également signatures des virus, pour analyser les fichiers. En d'autres termes, l'analyse anti-virus est en mesure de filtrer un virus inconnu si ce nouveau virus porte certaines caractéristiques de virus existants. Le composant **Anti-Virus** utilise les méthodes de détection suivantes :

- *Analyse* – recherche d'une chaîne de caractères typique d'un virus donné
- *Analyse heuristique* – émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel
- *Détection générique* – détection des instructions caractéristiques d'un virus ou d'un groupe de virus donné

Aucune technologie n'est infaillible. C'est pourquoi le composant **Anti-Virus** combine plusieurs technologies pour repérer ou identifier un virus et garantir la protection de votre ordinateur : **AVG Internet Security 2012** est également en mesure d'analyser et de détecter des exécutables ou bibliothèques DLL qui peuvent se révéler dangereux pour le système. Ce type de menaces porte le nom de programmes potentiellement dangereux (*différents types de spywares, d'adwares, etc.*). Par ailleurs, **AVG Internet Security 2012** analyse la base de registre de votre système afin de rechercher toute entrée suspecte, les fichiers Internet temporaires ou des cookies. Il vous permet de traiter les éléments à risque de la même manière que les infections.

**AVG Internet Security 2012 assure une protection non-stop de votre ordinateur !**



### 6.1.2. Protection résidente

**AVG Internet Security 2012** assure une protection permanente sous forme de protection résidente. Le composant **Anti-Virus** analyse chaque fichier (*avec certaines extensions ou sans extension du tout*) ouvert, enregistré ou copié. Il protège les zones système de l'ordinateur et les supports amovibles (*disque flash, etc.*). S'il détecte un virus dans un fichier, il interrompt l'opération en cours et ne donne donc pas la possibilité au virus de s'activer. Normalement, ce processus passe inaperçu, car la protection résidente s'exécute "en arrière-plan". Vous n'êtes informé que si une menace est détectée et, entre-temps, **Anti-Virus** en bloque l'activation et la supprime.

***La protection résidente est chargée dans la mémoire de votre ordinateur au démarrage. Il est essentiel qu'elle reste activée en permanence !***

### 6.1.3. Protection Anti-spyware

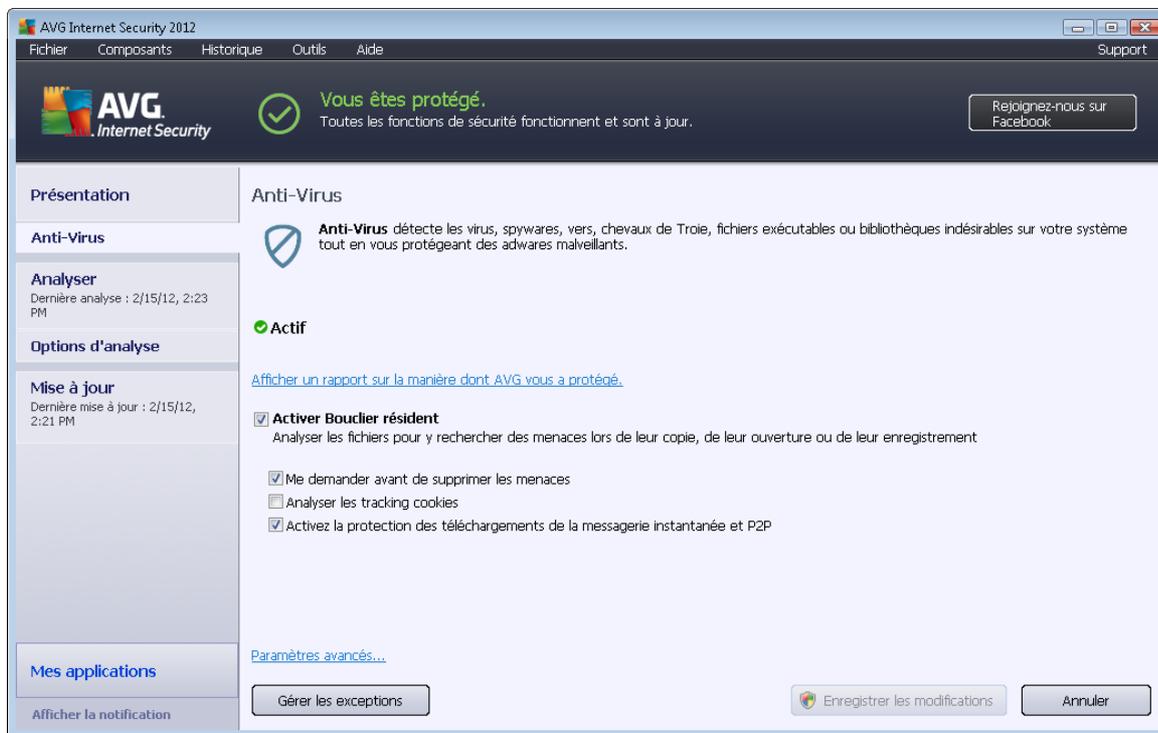
Le composant **Anti-Spyware** est constitué d'une base de données permettant d'identifier les types de définition de spywares connus. Les experts en spywares d'AVG s'efforcent d'identifier et de décrire les modèles de spywares les plus récents et ce, dès leur apparition, puis ajoutent des définitions appropriées dans la base de données. Grâce au processus de mise à jour, ces nouvelles définitions sont téléchargées sur votre ordinateur de sorte que vous bénéficiez d'une protection fiable contre les derniers codes de ce type. Le composant **Anti-Spyware** vous permet d'analyser la totalité de votre ordinateur à la recherche de programmes malicieux et des spywares. Il se charge également de détecter les codes malicieux inactifs ou en sommeil (ceux qui ont été téléchargés, mais non activés).

#### Qu'est-ce qu'un spyware ?

Le terme spyware désigne généralement un code malicieux et plus précisément un logiciel qui collecte des informations sur l'ordinateur d'un utilisateur, à l'insu de celui-ci. Certains spywares installés volontairement peuvent contenir des informations à caractère publicitaire, des pop-ups ou d'autres types de logiciels déplaisants. Actuellement, les sites Web au contenu potentiellement dangereux sont les sources d'infection les plus courantes. D'autres vecteurs comme la diffusion par mail ou la transmission de vers et de virus prédominent également. La protection la plus importante consiste à définir un système d'analyse en arrière-plan, activé en permanence (tel que le composant **Anti-Spyware**) agissant comme un bouclier résident afin d'analyser les applications exécutées en arrière-plan.

### 6.1.4. Interface de l'Anti-Virus

L'interface du composant **Anti-Virus** comporte une description succincte des fonctionnalités du composant, des informations sur l'état actuel du composant (*Actif*), ainsi que les options de configuration de base du composant :



## Options de configuration

Cette boîte de dialogue contient quelques options de configuration de base disponibles dans le composant **Anti-Virus**. Une brève description de ces dernières est fournie ci-dessous :

- **Consultez un rapport en ligne pour savoir comment AVG vous protège** – Le lien vous redirige vers une page du site Web d'AVG (<http://www.avg.com/>). Sur cette page, vous trouverez une présentation statistique détaillée de toute l'activité d'**AVG Internet Security 2012** sur votre ordinateur au cours d'une période donnée et depuis le début.
- **Activer le Bouclier résident** – Cette option permet d'activer ou de désactiver facilement la protection résidente. Le composant Bouclier résident analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés. Lorsqu'un virus ou tout autre type de menace est détecté, vous en êtes averti immédiatement. La fonctionnalité est activée par défaut et il est recommandé de la laisser ainsi ! Si la protection résidente est activée, vous pouvez établir plus précisément la manière dont les infections détectées sont traitées :
  - **Me demander avant de supprimer les menaces** - Laissez l'option cochée pour confirmer que vous souhaitez être consulté lorsqu'une menace est détectée, avant qu'elle ne soit déplacée et mise en [Quarantaine](#). Cette option n'a pas d'impact sur le niveau de la sécurité, mais reflète uniquement les préférences de l'utilisateur.
  - **Analyser les tracking cookies** – Indépendamment du réglage des options précédentes, vous pouvez décider d'analyser ou non les tracking cookies. (les cookies sont des portions de texte envoyées par un serveur à un navigateur Web et renvoyées en l'état par le navigateur chaque fois que ce dernier accède au serveur.



Les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs telles que leurs préférences en matière de site ou le contenu de leur panier d'achat électronique.) Dans certaines circonstances, vous pouvez activer cette option pour appliquer le niveau de sécurité le plus élevé. Notez que cette option est désactivée par défaut.

- **Activer la protection des téléchargements de messagerie instantanée et P2P** - Cochez cette case si vous souhaitez vérifier que la communication par messagerie instantanée (ICQ, MSN Messenger, etc.) est exempte de virus.
- **Paramètres avancés...** – Cliquez sur le lien pour être redirigé vers la boîte de dialogue correspondante dans les [Paramètres avancés](#) d'AVG Internet Security 2012. Vous pouvez modifier la configuration du composant de manière approfondie à partir de cette dernière. Cependant, notez que la configuration par défaut de tous les composants est définie de sorte qu'AVG Internet Security 2012 fournisse une performance optimale et une sécurité maximale. A moins que vous n'ayez une bonne raison de le faire, il est recommandé de préserver cette configuration par défaut !

### Boutons de commande

Dans cette boîte de dialogue, vous pouvez utiliser les boutons de commande suivants :

- **Gérer les exceptions** – Ce bouton permet d'ouvrir une nouvelle boîte de dialogue intitulée **Bouclier résident – Exceptions**. Vous pouvez également accéder à la configuration des exceptions pour l'analyse du Bouclier résident à partir du menu principal en suivant la séquence [Paramètres avancés / Anti-Virus / Bouclier résident / Exceptions](#) (pour obtenir une description détaillée, consultez le chapitre correspondant). Dans cette boîte de dialogue, vous pouvez indiquer les fichiers et les dossiers qui doivent être exclus de l'analyse du Bouclier résident. Il est vivement recommandé de n'exclure aucun fichier, sauf en cas d'absolue nécessité ! Cette boîte de dialogue présente les boutons de fonction suivantes :
  - **Ajouter un chemin** – ce bouton permet de spécifier un répertoire ou des répertoires que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local.
  - **Ajouter un fichier** – Ce bouton permet de spécifier les fichiers que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local.
  - **Modifier** – Ce bouton permet de modifier le chemin d'accès à un fichier ou dossier sélectionné.
  - **Supprimer** – ce bouton permet de supprimer le chemin d'accès à un objet sélectionné dans la liste.
  - **Modifier la liste** – permet de modifier l'ensemble de la liste des exceptions définies dans une nouvelle boîte de dialogue qui fonctionne comme un éditeur de texte standard.

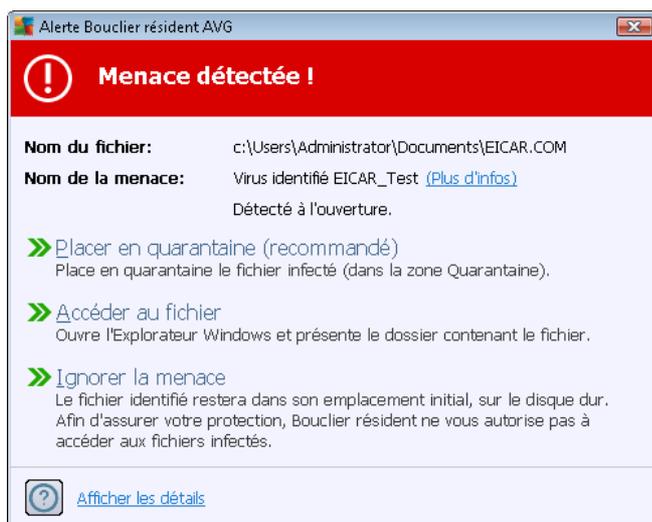


- **Appliquer** - Ce bouton permet d'enregistrer toutes les modifications apportées à la configuration du composant dans cette boîte de dialogue et de revenir à l'[interface utilisateur](#) principale d'**AVG Internet Security 2012** (*vue d'ensemble des composants*).
- **Annuler** – Ce bouton permet d'annuler toutes les modifications des paramètres du composant entrées dans cette boîte de dialogue. Aucune modification ne sera enregistrée. Vous allez revenir à l'[interface utilisateur](#) principale d'**AVG Internet Security 2012** (*vue d'ensemble des composants*).

### 6.1.5. Détections du Bouclier résident

#### Menace détectée !

**Le composant Bouclier résident** analyse les fichiers lorsqu'ils sont copiés, ouverts ou enregistrés. Lorsqu'un virus ou tout autre type de menace est détecté, vous êtes averti immédiatement via la boîte de dialogue suivante :



Dans cette fenêtre d'avertissement, vous trouverez des informations sur le fichier qui a été détecté et défini comme étant infecté (*Nom du fichier*), le nom de l'infection reconnue (*Nom de la menace*) ainsi qu'un lien renvoyant à l'[Encyclopédie des virus](#) contenant de plus amples détails sur l'infection, le cas échéant (*Plus d'infos*).

Ensuite, vous devez décider de la mesure à prendre tout de suite. Plusieurs autres options sont disponibles. **Notez que, dans certaines conditions (type de fichier infecté et emplacement du fichier), certaines de ces options ne sont pas actives !**

- **Réparer** – ce bouton ne s'affiche que si une solution permettant de traiter l'infection décelée existe. Dans ce cas, elle élimine l'infection et rétablit l'état initial du fichier. Si le fichier lui-même est un virus, cette fonction le supprime (*en plaçant le fichier dans la zone [Quarantaine](#)*)
- **Placer en quarantaine (recommandé)** - le virus sera placé dans la [Quarantaine](#)



- **Accéder au fichier** - cette option vous redirige vers l'emplacement d'origine de l'objet suspect (*ouvre une nouvelle fenêtre de Windows Explorer*)
- **Ignorer la menace** - nous vous recommandons fortement de ne PAS utiliser cette option sauf si vous avez une très bonne raison de le faire !

**Remarque:** Il peut arriver que la taille de l'objet détecté dépasse les limites d'espace de la Quarantaine. En pareil cas, un message d'avertissement s'affiche et vous en informe. Notez, toutefois, que la taille de la quarantaine est modifiable. Elle est définie sous la forme d'un pourcentage ajustable de la taille de votre disque dur. Pour augmenter la taille de la zone de quarantaine, ouvrez la boîte de dialogue [Quarantaine](#) dans [Paramètres avancés AVG](#), via l'option *Limiter la taille de la quarantaine*.

Dans la section inférieure de la boîte de dialogue, vous trouverez le lien **Afficher les détails**. Cliquez dessus pour ouvrir la fenêtre contenant des informations détaillées sur le processus en cours lorsque l'infection a été détectée et sur l'identification du processus.

## Présentation des détections du Bouclier résident

Vous trouverez des informations sur la présentation des menaces détectées par le [Bouclier résident](#) dans la boîte de dialogue **Détection par le Bouclier résident** accessible par la barre de menus [Historique / Détection du Bouclier résident](#) :

Infection	Objet	Résultat	Date de la détection	Type d'objet	Processus
Virus identifié EICAR...	c:\Users\Administrator\...	Infecté	2/15/2012, 2:25:09 PM	fichier	C:\Wind

La **détection du Bouclier résident** répertorie les objets détectés par le [Bouclier résident](#) comme étant dangereux, puis réparés ou déplacés en [quarantaine](#). Les informations suivantes accompagnent chaque objet détecté :



- **Infection** – description (et éventuellement le nom) de l'objet détecté
- **Objet** – emplacement de l'objet
- **Résultat** – action effectuée sur l'objet détecté
- **Date de la détection** – date et heure auxquelles l'objet a été détecté
- **Type d'objet** – type de l'objet détecté
- **Processus** – action réalisée pour solliciter l'objet potentiellement dangereux en vue de sa détection

Dans la partie inférieure de la boîte de dialogue, sous la liste, vous trouverez des informations sur le nombre total d'objets détectés répertoriés ci-dessus. Par ailleurs, vous êtes libre d'exporter la liste complète des objets détectés dans un fichier (**Exporter la liste dans le fichier**) et de supprimer toutes les entrées des objets détectés (**Vider la liste**). Le bouton **Actualiser la liste** permet de rafraîchir la liste des menaces détectées par le **Bouclier résident**. Le bouton **Précédent** permet de retourner à la [boîte de dialogue principale d'AVG](#) par défaut (*présentation des composants*).

## 6.2. LinkScanner

**LinkScanner** est conçu pour lutter contre les menaces d'un jour sans cesse plus nombreuses ; ces dernières disparaissent dès le lendemain de leur apparition sur Internet. Ces menaces peuvent infiltrer n'importe quel type de site Web, des sites gouvernementaux aux sites des PME en passant par ceux de marques bien connues. Elles ne s'attardent rarement plus de 24 heures sur un site. Pour vous protéger, le **LinkScanner** analyse les pages Web indiquées par les liens de la page que vous consultez et vérifie qu'elles sont sûres au moment crucial, c'est-à-dire lorsque vous êtes sur le point de cliquer sur un lien.

**LinkScanner n'est pas conçu pour la protection des plateformes serveur !**

La technologie **LinkScanner** repose essentiellement sur deux fonctions :

- [Search-Shield](#) contient une liste de sites Web (*adresses URL*) connus pour leur dangerosité. Lors de vos recherches sur Google, Yahoo! Lors d'une recherche sur JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, et Seznam, tous les résultats de recherche sont comparés à cette liste, puis une icône rendant un verdict sur la sécurité s'affiche (*sur Yahoo!, seules les icônes indiquant que le site Web est piraté s'affichent*).
- [Surf-Shield](#) analyse le contenu des sites Web que vous visitez, quelle que soit leur adresse. Même si [Search-Shield](#) ne détecte pas un site Web donné (*par exemple lorsqu'un nouveau site malveillant est créé ou lorsqu'un site officiel est contaminé*), [Surf-Shield](#) le détecte et le bloque si vous essayez d'y accéder.
- [Le Bouclier Web](#) vous protège en temps réel lorsque vous naviguez sur Internet. Il analyse le contenu des pages Web visitées et les fichiers qu'elles contiennent avant leur affichage dans le navigateur ou leur téléchargement. [Le Bouclier Web](#) détecte les virus et les spywares contenus dans la page que vous êtes sur le point de visiter et en arrête immédiatement le téléchargement. Ainsi, aucune menace ne touche votre ordinateur.

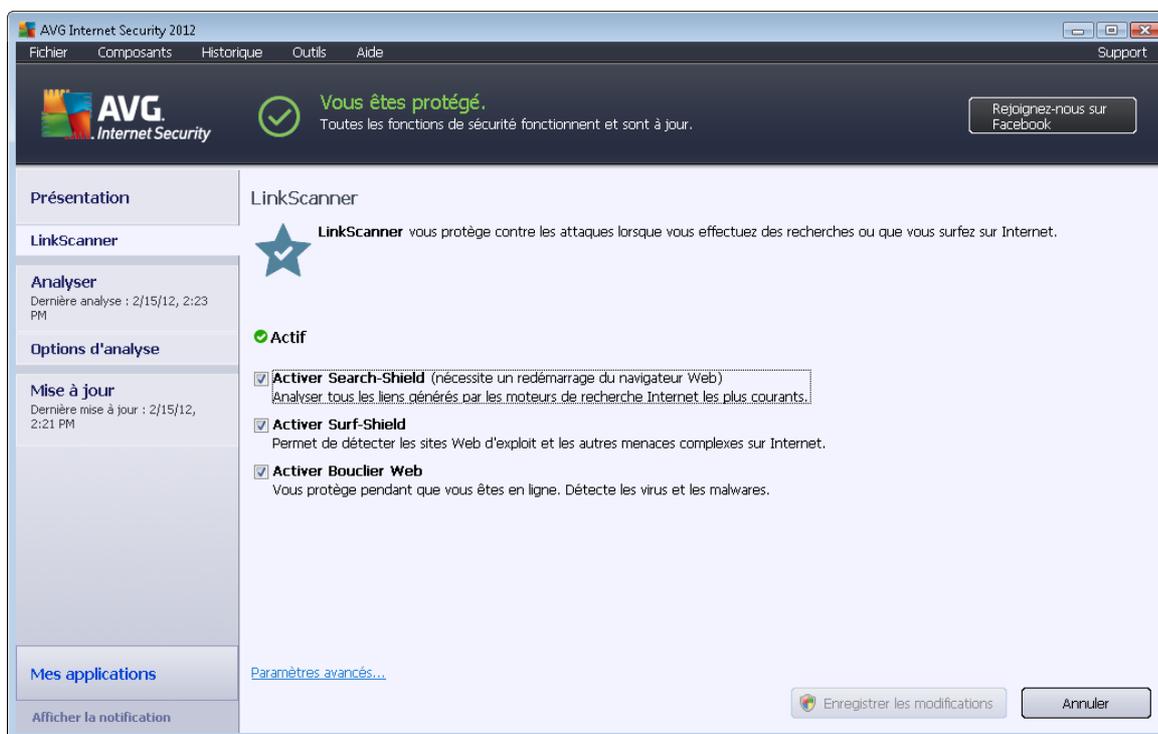


- **AVG Accelerator** permet une lecture vidéo en ligne plus fluide et facilite les téléchargements supplémentaires. Lorsque le processus d'accélération vidéo est en cours, une fenêtre contextuelle de la barre d'état vous en informe.



### 6.2.1. Interface de LinkScanner

La boîte de dialogue principale du composant [LinkScanner](#) décrit brièvement le fonctionnement du composant et indique son état actuel (*Actif*) :



Des options de configuration de base sont disponibles au bas de la boîte de dialogue :

- **Activer [Search-Shield](#)** (*option activée par défaut*) : ne désélectionnez cette case que si vous avez une bonne raison de désactiver la fonction Search Shield.
- **Activer [Surf-Shield](#)** (*option activée par défaut*) : protection active (*en temps réel*) contre les sites hébergeant des exploits, lorsque vous tentez d'y accéder. Les connexions à des sites malveillants et leur contenu piégé sont bloqués au moment où l'utilisateur demande à y accéder via un navigateur Web (*ou toute autre application qui utilise le protocole HTTP*).
- **Activer le [Bouclier Web](#)** (*option activée par défaut*) : analyse en temps réel des pages Web que vous êtes sur le point de consulter en vue de détecter d'éventuels virus ou spywares. Lorsqu'une infection est détectée, le téléchargement est interrompu avant que la



menace n'atteigne votre ordinateur.

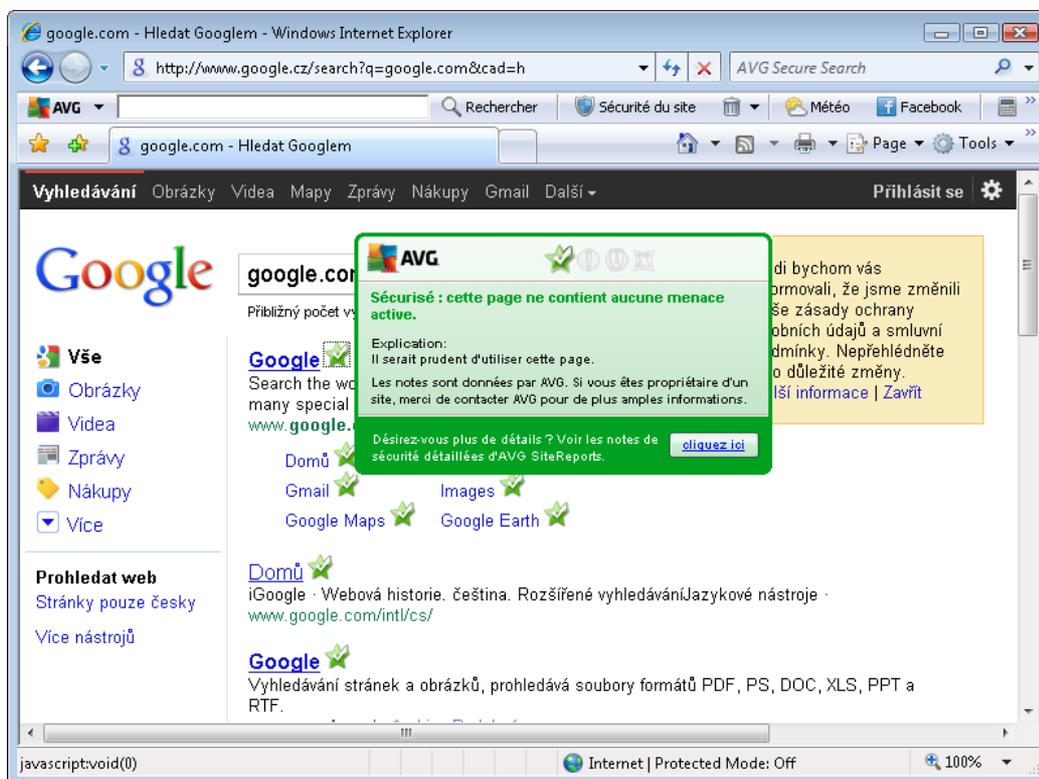
### 6.2.2. Détections par Search-Shield

Lorsque vous naviguez sur Internet en ayant pris soin d'activer **Search-Shield**, une vérification s'effectue sur tous les résultats de recherche retournés par la plupart des moteurs de recherche comme *Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg et SlashDot*) sont examinés pour voir s'ils contiennent des liens dangereux ou suspects. Grâce à cette vérification de ces liens et au signalement des mauvais liens, [LinkScanner](#) signale les liens dangereux ou suspects avant que vous ne les ouvriez. Vous naviguez ainsi en toute sécurité uniquement dans des sites Web sécurisés.

Lorsqu'un lien proposé dans une page de résultats de recherche fait l'objet d'une évaluation, une icône particulière apparaît pour indiquer qu'une vérification du lien est en cours. Lorsque l'évaluation du risque est terminée, l'icône d'information correspondante s'affiche :

-  La page associée au lien est exempte de virus.
-  La page associée ne contient pas de menaces, mais paraît néanmoins suspecte (*son origine comme son objet n'est pas explicite. Il est par conséquent préférable de ne pas l'utiliser pour les achats électroniques, etc.*).
-  La page associée au lien n'est pas fiable ou contient des liens menant à des pages dont les résultats d'analyse sont positifs ou dont le code est suspect, même s'il n'est pas directement lié pour le moment à des menaces.
-  La page liée contient des menaces actives ! Pour votre propre sécurité, vous n'êtes pas autorisé à visiter la page.
-  La page associée n'étant pas accessible, elle ne peut pas faire l'objet d'une analyse.

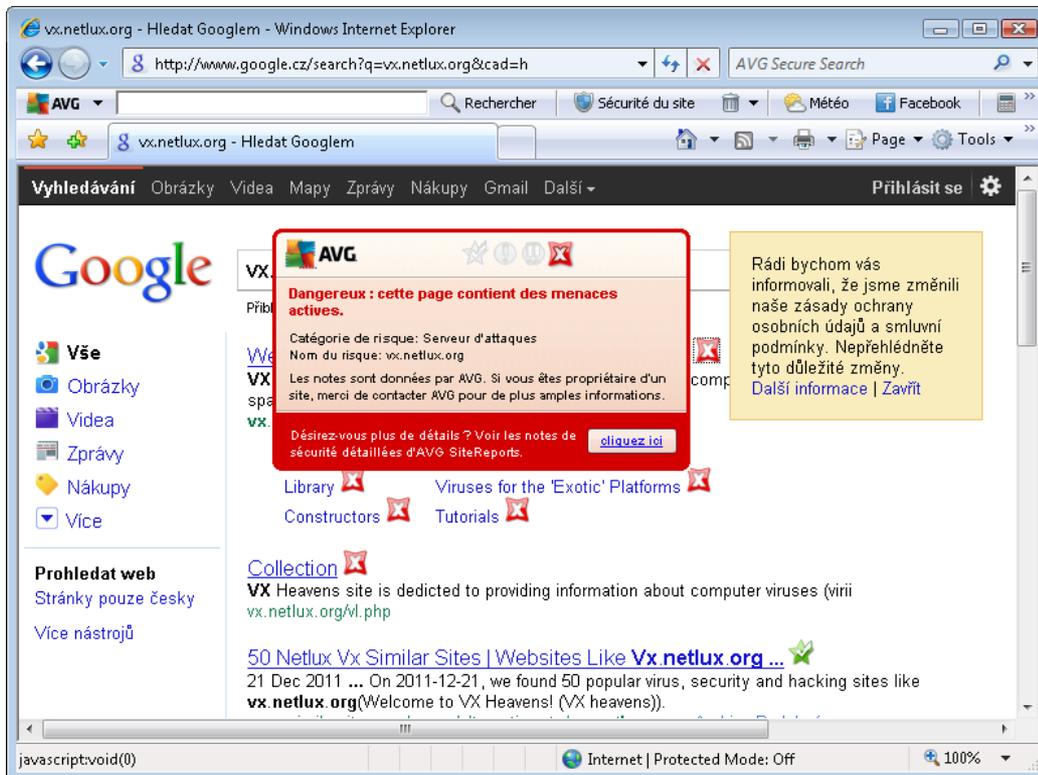
Le fait de placer le pointeur sur une icône d'évaluation permet d'obtenir des informations sur le lien en question. Les informations contiennent des détails supplémentaires sur la menace (*le cas échéant*):



### 6.2.3. Détections de Surf-Shield

Cette protection puissante bloque le contenu malveillant de toute page Web que vous êtes sur le point d'afficher et empêche son téléchargement sur l'ordinateur. Lorsque cette fonction est activée, cliquer sur un lien ou saisir une adresse URL menant à un site dangereux, bloque automatiquement l'ouverture de la page Web correspondante prévenant toute infection. Il est important de garder en mémoire que les pages Web contenant des exploits peuvent infecter votre ordinateur au détour d'une simple visite du site incriminé. Pour cette raison, quand vous demandez à consulter une page Web dangereuse contenant des exploits et d'autres menaces sérieuses, [LinkScanner](#) n'autorisera pas votre navigateur à l'afficher.

Si vous rencontrez un site Web malveillant, [LinkScanner](#) vous le signalera dans votre navigateur Web en affichant un écran comparable à celui-ci :



**L'accès à un tel site Web s'effectue à vos risques et périls et est fortement déconseillé !**

#### 6.2.4. Détection du Bouclier résident

**Le Bouclier Web** analyse le contenu des pages Web visitées (et les fichiers qu'elles contiennent) avant qu'elles ne s'affichent dans le navigateur ou ne soient téléchargées sur l'ordinateur. Vous serez immédiatement informé grâce à la boîte de dialogue suivante si une menace est détectée :



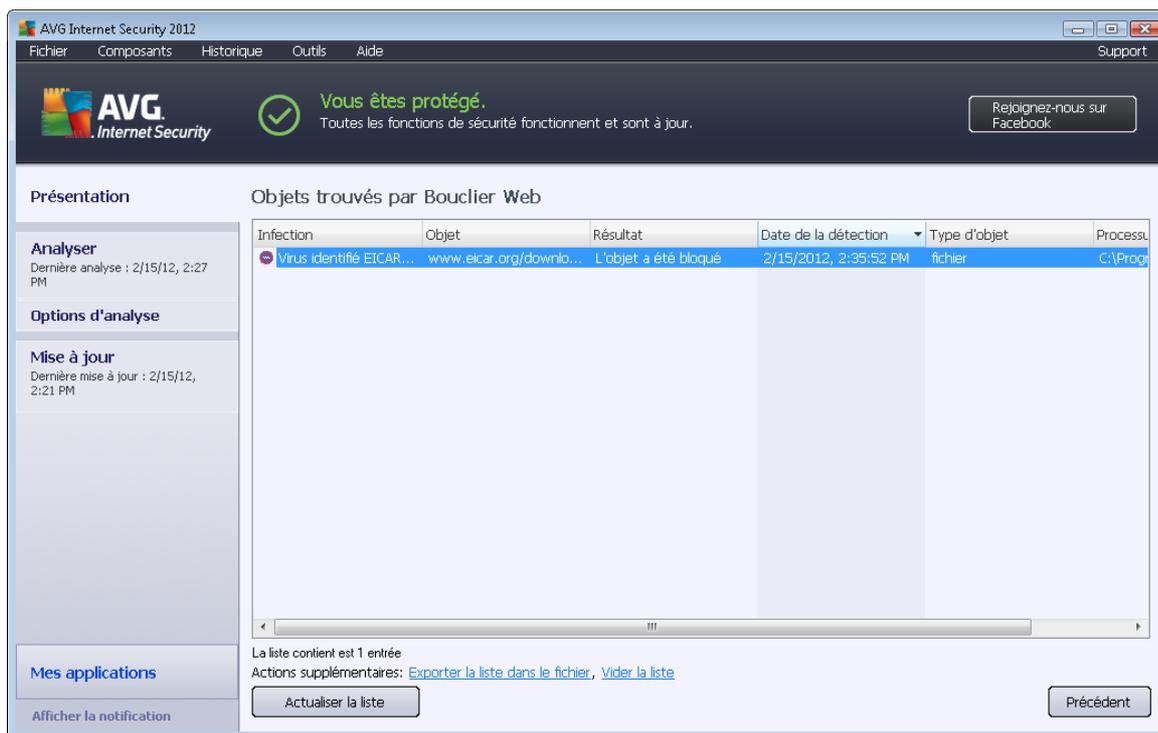
Dans cette boîte de dialogue d'avertissement, vous trouverez des informations sur le fichier qui a été détecté et défini comme infecté (*Nom du fichier*), le nom de l'infection reconnue (*Nom de la menace*) ainsi qu'un lien renvoyant à l'[Encyclopédie des virus](#) contenant de plus amples détails sur l'infection (*le cas échéant*). Cette boîte de dialogue présente les boutons de fonction suivantes :

- **Afficher les détails** – cliquez sur le bouton **Afficher les détails** pour ouvrir une fenêtre contenant des informations détaillées sur le processus en cours lorsque l'infection a été détectée et l'identification du processus.



- **Fermer** - cliquez sur le bouton pour fermer la boîte de dialogue.

La page Web suspecte ne sera pas ouverte et la détection de la menace sera consignée dans la liste des **Objets trouvés par Bouclier Web** (cette vue générale des menaces détectées est accessible via le menu système [Historique / Objets trouvés par Bouclier Web](#)).



Les informations suivantes accompagnent chaque objet détecté :

- **Infection** – description (et éventuellement le nom) de l'objet détecté.
- **Objet** – source de l'objet (page Web)
- **Résultat** – action effectuée sur l'objet détecté
- **Date de la détection** – date et heure auxquelles la menace a été détectée et bloquée
- **Type d'objet** – type de l'objet détecté
- **Processus** – action réalisée pour solliciter l'objet potentiellement dangereux en vue de sa détection

Dans la partie inférieure de la boîte de dialogue, sous la liste, vous trouverez des informations sur le nombre total d'objets détectés répertoriés ci-dessus. Par ailleurs, vous êtes libre d'exporter la liste complète des objets détectés dans un fichier (**Exporter la liste dans le fichier**) et de supprimer toutes les entrées des objets détectés (**Vider la liste**).



## Boutons de commande

- **Actualiser la liste** – permet de rafraîchir la liste des menaces détectées par le **Bouclier résident**
- **Précédent** – permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*présentation des composants*).

## 6.3. Protection e-mail

Le courrier électronique figure parmi les sources les plus courantes d'infection par virus ou Cheval de Troie. Les techniques d'hameçonnage (ou phishing) et d'envoi de messages non sollicités en masse (spam) rendent la messagerie encore plus vulnérable. Les comptes gratuits de messagerie offrent un risque élevé de réception de messages électroniques malveillants, *d'autant qu'ils utilisent rarement une technologie anti-spam*) et qu'ils sont très prisés des particuliers. Par ailleurs, en consultant des sites inconnus depuis leur domicile et en fournissant leurs données personnelles (*adresse e-mail, par exemple*) dans des formulaires en ligne, ces usagers contribuent à augmenter les risques d'attaque par e-mail. Les sociétés utilisent généralement des comptes de messagerie à usage professionnel et appliquent des filtres anti-spam et autres moyens pour réduire ce risque.

Le composant **Protection e-mail** assure l'analyse de chaque e-mail envoyé ou reçu. Lorsqu'un virus est détecté dans un message, il est immédiatement mis en [Quarantaine](#). Le composant permet également de filtrer les pièces jointes et d'ajouter un texte de certification aux messages dépourvus d'infection. **Protection e-mail** comporte deux fonctions principales :

- [Scanner e-mail](#)
- [Anti-Spam](#)

### 6.3.1. Scanner e-mail

**Le Scanner e-mail** analyse automatiquement les messages entrants et sortants. Vous pouvez l'utiliser avec les clients de messagerie qui ne possèdent pas leurs propres plug-ins AVG (*mais il peut également être utilisé pour lire les mails des clients de messagerie qu'AVG prend en charge au moyen d'un plug-in donné, par exemple Microsoft Outlook, The Bat et Mozilla Thunderbird*). Il est principalement destiné aux applications de messagerie telles que Outlook Express, Thunderbird, Incredimail, etc.

Lors de l'[installation](#) d'AVG, des serveurs sont automatiquement créés pour assurer la vérification des messages, l'un pour les messages entrants, l'autre pour les messages sortants. Grâce à ces deux serveurs, les messages sont vérifiés automatiquement sur les ports 110 et 25 (*ports standard affectés à l'envoi/la réception de messages*).

**Le Scanner e-mail personnel** fonctionne comme une interface entre le client de messagerie et les serveurs de messagerie sur Internet.

- **Message entrant** : lorsque vous recevez un message du serveur, le composant **Scanner e-mail** vérifie s'il ne contient pas de virus, supprime les pièces jointes infectées (le cas échéant) et ajoute la certification. Lorsque des virus sont détectés, ils sont immédiatement placés en [Quarantaine](#). Le message est ensuite transmis au client de messagerie.



- **Message sortant** : un message est envoyé du client de messagerie au scanner e-mail. Ce dernier vérifie que le message et ses pièces jointes ne contiennent pas de virus. Ensuite, il l'envoie au serveur SMTP (*l'analyse des messages sortants est désactivée par défaut et peut-être configurée de façon manuelle*).

**Scanner e-mail n'est pas conçu pour les plateformes serveur !**

## 6.3.2. Anti-spam

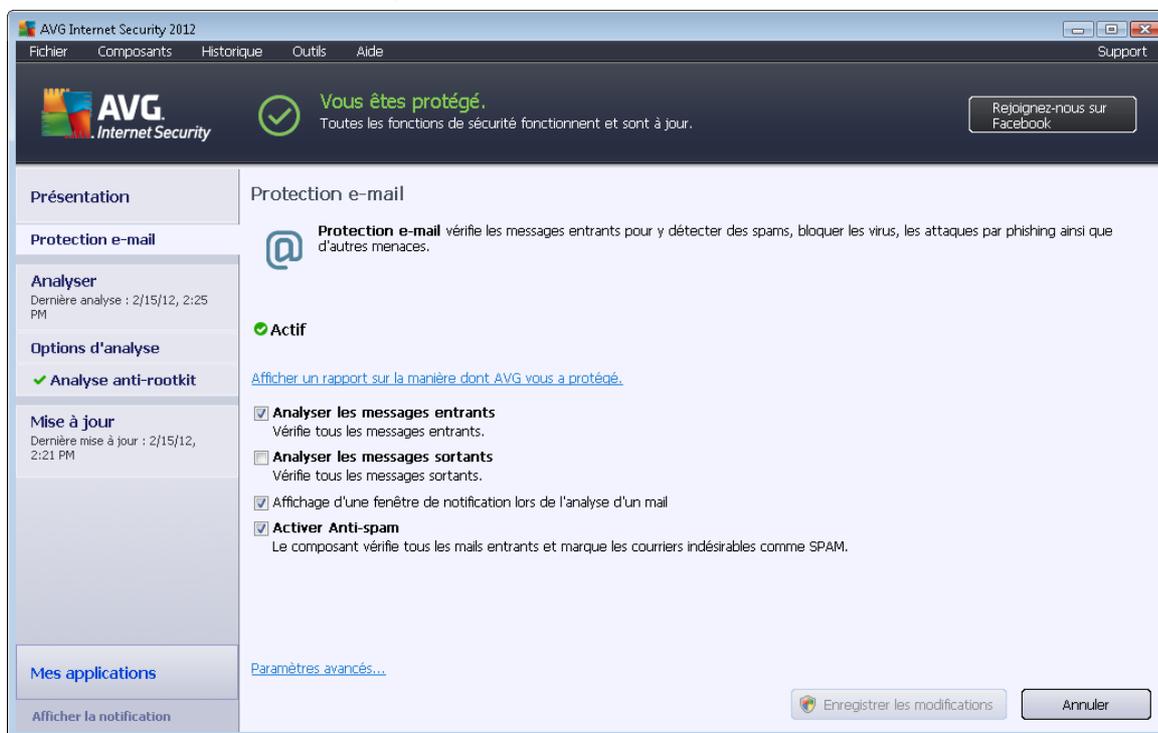
### Comment fonctionne le composant Anti-Spam ?

**Le composant Anti-Spam** vérifie tous les messages entrants et marque les courriers indésirables comme étant du SPAM. **Anti-Spam** est capable de modifier l'objet du message (*identifié comme du spam*) en ajoutant une chaîne spéciale. Il est ensuite très facile de filtrer vos messages dans votre client de messagerie. **Le composant Anti-Spam** utilise plusieurs méthodes d'analyse pour traiter chaque message afin d'offrir un niveau de protection maximal contre les messages indésirables. Pour détecter les messages indésirables, le composant **Anti-Spam** exploite une base de données régulièrement mise à jour. Vous pouvez également faire appel à des [serveurs RBL](#) (*bases de données publiques répertoriant les adresses électroniques d'expéditeurs de spam connus*) et ajouter manuellement des adresses électroniques à votre [liste blanche](#) (*pour ne jamais les considérer comme du spam*) et à votre [liste noire](#) (*pour systématiquement les considérer comme du spam*).

### Qu'est-ce que le spam ?

Le terme « spam » désigne un message indésirable ; il s'agit généralement d'un produit ou d'un service à caractère publicitaire envoyé en masse à de nombreuses adresses électroniques ayant pour conséquence d'encombrer les boîtes aux lettres des destinataires. Il faut distinguer le spam des autres messages commerciaux légitimes que les consommateurs consentent à recevoir. Non seulement le spam peut être gênant, mais il est également à l'origine d'escroqueries, de virus ou de contenu pouvant heurter la sensibilité de certaines personnes.

### 6.3.3. Interface du composant Protection e-mail



La boîte de dialogue du composant **Protection e-mail** décrit de façon concise la fonctionnalité du composant et signale son état actuel (*Actif*). Cliquez sur le lien **Consultez un rapport en ligne pour savoir comment AVG vous a protégé** pour parcourir des statistiques détaillées sur les activités d'AVG Internet Security 2012 et les détections sur une page dédiée du site Web d'AVG à l'adresse : (<http://www.avg.com/>).

#### Paramètres standard de Protection e-mail

Dans la boîte de dialogue **Protection e-mail**, vous pouvez modifier certaines options de base de la fonctionnalité du composant :

- **Analyser les messages entrants** (*Activé par défaut*) - Cochez cette case pour analyser tous les courriers adressés à votre compte.
- **Analyser les messages sortants** (*Désactivé par défaut*) - Cochez cette case pour analyser tous les courriers envoyés depuis votre compte.
- **Affichage d'une fenêtre de notification lors de l'analyse d'un mail** (*Activé par défaut*) - Cochez cette case pour qu'une info-bulle de notification s'affiche au-dessus de l'icône **AVG dans la barre d'état système** au cours de l'analyse du message par le composant e-mail.
- **Activer Anti-Spam** (*activé par défaut*) - Cochez cette case pour que tout votre courrier entrant soit filtré pour y détecter du courrier indésirable.



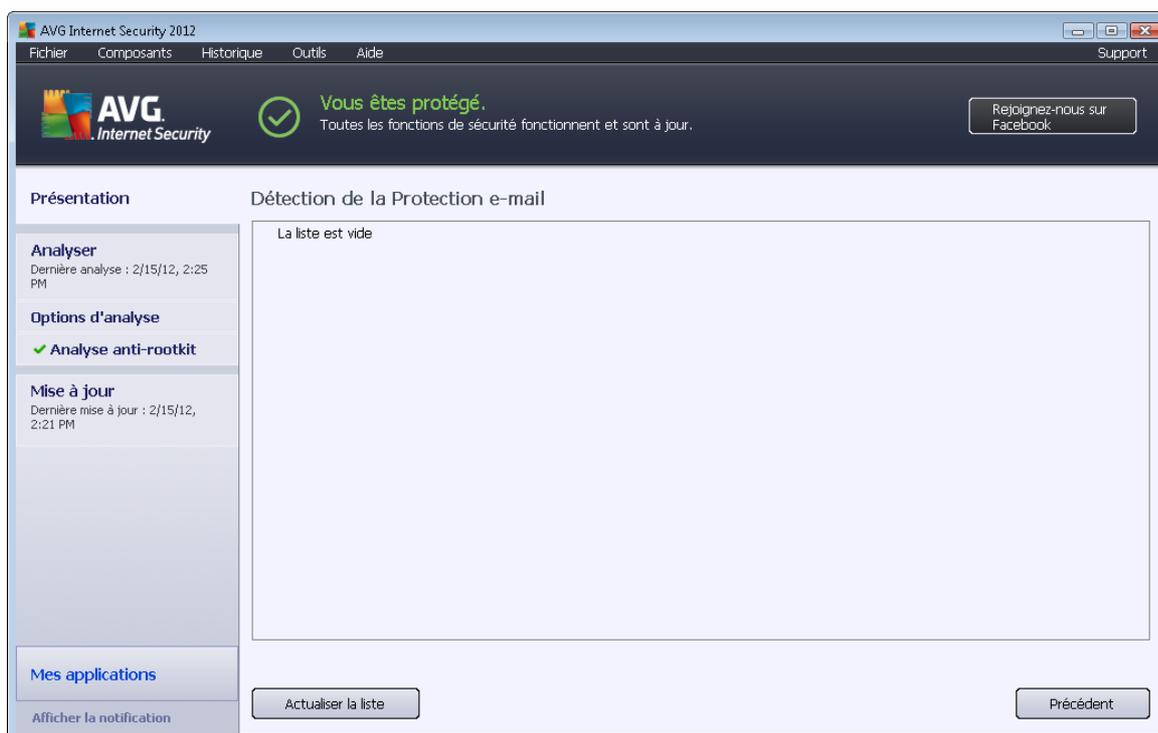
**L'éditeur du logiciel a configuré tous les composants AVG de manière à assurer des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous devez modifier la configuration d'AVG, sélectionnez le menu Outils / Paramètres avancés et modifiez la configuration d'AVG dans la boîte de dialogue [Paramètres avancés d'AVG](#) qui apparaît.**

### Boutons de commande

Les boutons de commande disponibles dans l'interface de **Protection e-mail** sont :

- **Enregistrer les modifications** – cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue
- **Annuler** : cliquez sur ce bouton pour revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*présentation des composants*).

### 6.3.4. Détections du scanner e-mail



Dans la boîte de dialogue **Détection du Scanner E-mail** (accessible par le menu *Historique / Détection du Scanner E-mail*), vous accédez à la liste de tous les éléments détectés par le composant [Protection e-mail](#). Les informations suivantes accompagnent chaque objet détecté :

- **Infection** – description (et éventuellement le nom) de l'objet détecté
- **Objet** – emplacement de l'objet



- **Résultat** – action effectuée sur l'objet détecté
- **Date de la détection** – date et heure auxquelles l'objet suspect a été détecté
- **Type d'objet** – type de l'objet détecté

Dans la partie inférieure de la boîte de dialogue, sous la liste, vous trouverez des informations sur le nombre total d'objets détectés répertoriés ci-dessus. Par ailleurs, vous êtes libre d'exporter la liste complète des objets détectés dans un fichier (**Exporter la liste dans le fichier**) et de supprimer toutes les entrées des objets détectés (**Vider la liste**).

### Boutons de commande

Les boutons de commande disponibles dans l'interface de **Détection du Scanner e-mail** sont :

- **Actualiser la liste** – Met à jour la liste des menaces détectées.
- **Précédent** – Revient à la boîte de dialogue précédente.

## 6.4. Pare-Feu

**Un pare-feu** est un système prévu pour appliquer des règles de contrôle d'accès entre plusieurs réseaux en bloquant/autorisant le trafic. Le composant **Pare-feu** dispose d'un jeu de règles destiné à protéger le réseau interne contre les attaques venant de l'extérieur (*généralement d'Internet*) et contrôle l'ensemble du trafic au niveau de chaque port réseau. Les communications sont évaluées en fonction de règles définies et sont ensuite autorisées ou interdites. Si le **pare-feu** détecte une tentative d'intrusion, il « bloque » l'opération de manière à empêcher l'intrus d'accéder à votre ordinateur.

**Le pare-feu** est configuré pour autoriser ou bloquer la communication interne ou externe (dans les deux sens, entrante ou sortante) passant par les ports définis et pour les applications définies. Par exemple, le pare-feu peut être configuré pour autoriser uniquement la transmission de données entrantes et sortantes transitant par Microsoft Internet Explorer. Toute tentative pour transmettre des données par un autre navigateur sera bloquée.

**Le pare-feu** empêche que des informations qui permettraient de vous identifier personnellement soient envoyées sans votre accord. Il régit la manière dont votre ordinateur échange des données avec les autres ordinateurs, que ce soit sur Internet ou dans un réseau local. Au sein d'une entreprise, le **pare-feu** permet de contrecarrer les attaques initiées par des utilisateurs internes travaillant sur d'autres ordinateurs reliés au réseau.

**Les ordinateurs qui ne sont pas protégés par le pare-feu deviennent une cible facile pour les pirates informatiques et le vol de données.**

**Recommandation** : en règle générale, il est déconseillé d'utiliser plusieurs pare-feu sur un même ordinateur. La sécurité de l'ordinateur n'est pas améliorée par l'installation de plusieurs pare-feux. Il est plus probable que des conflits se produisent entre deux applications. Nous vous conseillons donc de n'utiliser qu'un seul pare-feu sur votre ordinateur et de désactiver tous les autres pare-feu afin d'éviter des conflits entre AVG et ces programmes, ainsi que d'autres problèmes.



### 6.4.1. Principes de fonctionnement du pare-feu

Dans **AVG Internet Security 2012**, le **Pare-feu** contrôle tout le trafic passant par chaque port réseau de votre ordinateur. En fonction des règles définies, le **Pare-feu** évalue les applications en cours d'exécution sur votre ordinateur (*et qui cherchent à se connecter à Internet/au réseau local*) ou les applications qui essaient de se connecter à votre ordinateur depuis l'extérieur. Pour chacune de ces applications, le **Pare-feu** autorise ou interdit les communications transitant sur les ports réseau. Par défaut, si l'application est inconnue (*c'est-à-dire, aucune règle de pare-feu n'est définie*), le **Pare-feu** vous demandera si vous voulez autoriser ou bloquer la tentative de communication.

***Le Pare-feu AVG n'est pas conçu pour les plateformes serveur !***

#### Actions possibles du Pare-feu AVG :

- Autoriser ou bloquer automatiquement les tentatives de communication des [applications](#) connues ou demander votre confirmation
- Utiliser des [profils](#) complets avec des règles prédéfinies en fonction de vos besoins
- [Changer automatiquement de profil](#) lors de la connexion à différents réseaux ou de l'utilisation de divers adaptateurs réseau

### 6.4.2. Profils de pare-feu

Le [pare-feu](#) vous permet de définir des règles de sécurité spécifiques suivant si l'ordinateur est situé dans un domaine, s'il est autonome ou s'il s'agit d'un ordinateur portable. Chacune de ces options appelle un niveau de protection différent, géré par un profil particulier. En d'autres termes, un profil de [Pare-feu](#) est une configuration spécifique du composant [Pare-feu](#). Vous pouvez utiliser plusieurs configurations prédéfinies de ce type.

#### Profils disponibles

- **Autoriser tout** - un profil système de [Pare-feu](#) prédéfini par l'éditeur, qui est toujours présent. Lorsque ce profil est activé, toutes les communications réseau sont autorisées et aucune règle de sécurité n'est appliquée, de la même manière que si la protection du [Pare-feu](#) était désactivée (toutes les applications sont autorisées, mais les paquets sont toujours vérifiés – pour désactiver complètement tout filtrage, vous devez désactiver le Pare-feu). Ce profil système ne peut pas être dupliqué, ni supprimé et ses paramètres ne peuvent pas être modifiés.
- **Bloquer tout** – un profil système de [Pare-feu](#) prédéfini par l'éditeur, qui est toujours présent. Lorsque ce profil est activé, toutes les communications réseau sont bloquées et l'ordinateur ne peut ni accéder à d'autres réseaux ni recevoir des communications provenant de l'extérieur. Ce profil système ne peut pas être dupliqué, ni supprimé et ses paramètres ne peuvent pas être modifiés.
- **Les profils personnalisés** vous permettent de tirer parti du changement automatique de profils, qui peut être particulièrement utile si vous vous connectez fréquemment à divers réseaux (*par exemple, avec un ordinateur portable*). Profils générés automatiquement après



l'installation d'**AVG Internet Security 2012** et couvrant tous les besoins individuels des règles de [Pare-feu](#). Vous avez le choix entre les options suivantes :

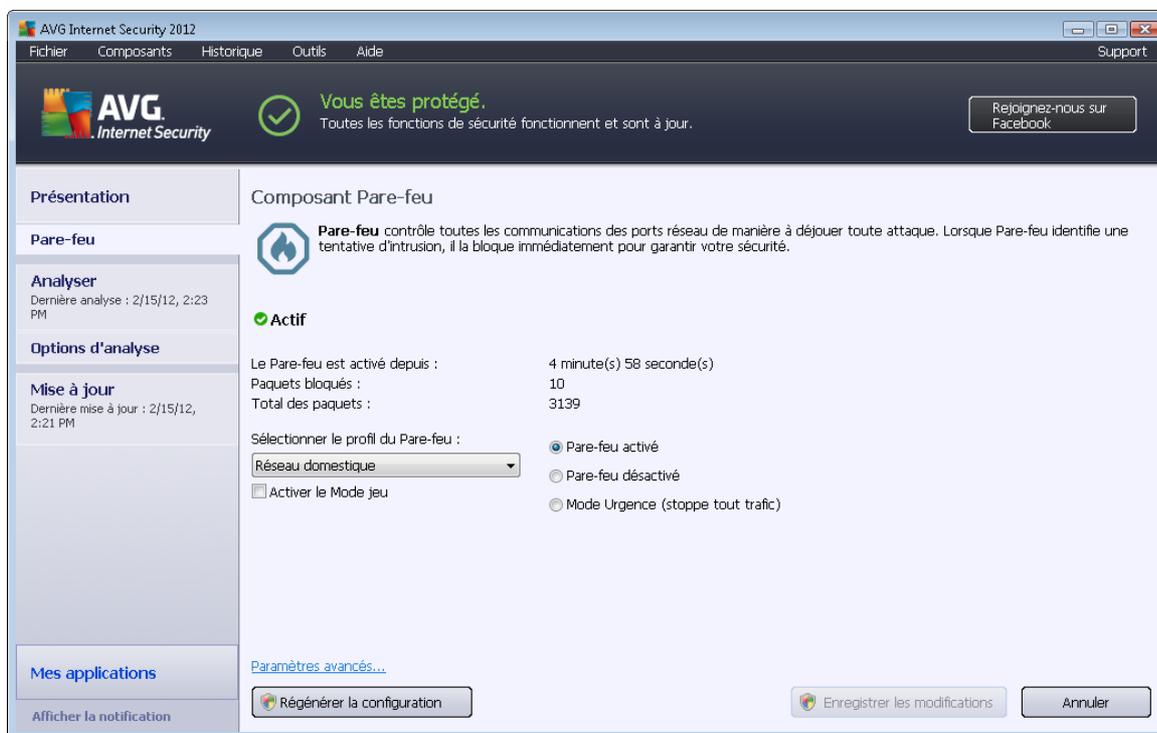
- **Directement connecté à Internet** – adapté à un usage familial sur un ordinateur de bureau ou un portable connecté à Internet, sans protection supplémentaire. Cette option est également recommandée lorsque vous connectez votre ordinateur portable à des réseaux inconnus et sans doute non sécurisés (*par exemple les cyber cafés, chambres d'hôtel, etc.*). Les règles strictes du profil [Pare-feu](#) permettent de vérifier que l'ordinateur est bien protégé.
- **Ordinateur inclus dans un réseau** – Convient pour les ordinateurs appartenant à un réseau local, d'habitude à l'école ou au bureau. En principe, le réseau est professionnellement géré et protégé par des dispositifs supplémentaires, d'où un niveau de sécurité plus faible que dans les cas susmentionnés, avec notamment l'autorisation de l'accès aux dossiers partagés, aux unités de disque, etc.
- **Réseau domestique** – Convient pour les ordinateurs appartenant à un réseau de petite taille, généralement à la maison ou dans une petite entreprise. En général, ce type de réseau est dépourvu d'administrateur "central" et ne comprend que quelques ordinateurs interconnectés qui partagent souvent une imprimante, un scanner ou un périphérique similaire, que les règles de [pare-feu](#) doivent inclure.

### Changement de profil

L'utilitaire Changement de profil permet au [Pare-feu](#) de changer automatiquement de profil lorsqu'il détecte une activité sur un adaptateur réseau ou lorsque vous êtes connecté sur un certain type de réseau. Si aucun profil n'a été assigné à une zone de réseau, à la prochaine connexion à cette zone, une boîte de dialogue du [Pare-feu](#) vous invitera à lui attribuer un profil. Vous pouvez assigner des profils à toutes les interfaces réseau ou à toutes les zones de réseau et définir des paramètres complémentaires dans la boîte de dialogue [Profils adaptateurs et réseaux](#), où vous pouvez aussi désactiver cette fonctionnalité si vous ne désirez pas l'utiliser. *Dans ce cas, quel que soit le type de la connexion, le profil par défaut sera utilisé.*

Les utilisateurs d'un ordinateur portable, par exemple, trouveront très pratique cette fonctionnalité, car ils utilisent plusieurs interfaces réseau pour se connecter (WiFi, Ethernet, etc.). Si vous possédez un ordinateur de bureau et n'utilisez qu'un seul type de connexion (*par exemple, une connexion câblée à Internet*), vous n'avez pas besoin de vous soucier du basculement de profil, car vous ne l'utiliserez probablement jamais.

### 6.4.3. Interface du Pare-feu



La principale boîte de dialogue intitulée **Composant Pare-feu** fournit des informations de base sur la fonctionnalité du composant, son état (*Actif*), ainsi qu'un bref aperçu des statistiques le concernant :

- **Le pare-feu est activé depuis** – temps écoulé depuis le dernier démarrage du [Pare-feu](#)
- **Paquets bloqués** - nombre de paquets bloqués par rapport au nombre total de paquets vérifiés
- **Total des paquets** – nombre total de paquets vérifiés au cours de l'[exécution du](#) Pare-feu

#### Paramètres de base

- **Sélectionner le profil du Pare-feu** – dans le menu déroulant, sélectionnez l'un des profils définis (*pour une description détaillée de chaque profil et l'utilisation qui en est conseillée, consultez le chapitre [Profils du Pare-feu](#)*)
- **Activer le mode jeu** – cochez cette case pour faire en sorte que lorsque vous exécutez des applications en mode plein écran (*jeux, présentations, films, etc.*), le [pare-feu](#) n'affiche pas de boîtes de dialogue vous demandant d'autoriser ou de bloquer les communications avec des applications inconnues. Si une application inconnue tente de communiquer par le réseau pendant ce temps, le [pare-feu](#) autorise ou bloque automatiquement la tentative selon les paramètres définis dans le profil actif. **Remarque** : En mode jeu, toutes les tâches programmées (analyses, mises à jour) sont reportées jusqu'à la fermeture de l'application.



- En outre, dans cette section de configuration initiale, vous pouvez sélectionner une option possible sur trois pour définir l'état en cours du composant [Pare-feu](#) :
  - **Pare-feu activé (par défaut)** - sélectionnez cette option pour autoriser la communication avec les applications dont le jeu de règles est "Autorisé" dans le profil [de Pare-feu](#) sélectionné.
  - **Pare-feu désactivé** – cette option désactive intégralement le [Pare-feu](#) : l'ensemble du trafic réseau est autorisé sans aucune vérification.
  - **Mode Urgence (bloque tout le trafic Internet)** – cette option vise à bloquer l'ensemble du trafic sur chaque port réseau ; [le Pare-feu](#) fonctionne, mais tout trafic réseau est stoppé.

**Remarque :** *l'éditeur du logiciel a configuré tous les composants AVG Internet Security 2012 de manière à assurer des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Tout changement de ces paramètres doit être réalisé par un utilisateur expérimenté. Si vous êtes amené à modifier la configuration du Pare-feu, cliquez sur l'élément de menu **Outils / Paramètres du Pare-feu** et modifiez la configuration du Pare-feu dans la boîte de dialogue [Paramètres avancés d'AVG](#) qui apparaît.*

### Boutons de commande

- **Régénérer la configuration** – cliquez sur ce bouton pour remplacer la configuration du [Pare-feu](#) et rétablir la configuration par défaut selon la détection automatique.
- **Enregistrer les modifications** – cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue.
- **Annuler** : cliquez sur ce bouton pour revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*présentation des composants*).

## 6.5. Anti-Rootkit

**Le composant Anti-Rootkit** est un outil spécialisé dans la détection et la suppression des rootkits. Ces derniers sont des programmes et technologies de camouflage destinés à masquer la présence de logiciels malveillants sur l'ordinateur. **Anti-Rootkit** peut détecter des rootkits selon un ensemble de règles prédéfinies. Notez que tous les rootkits sont détectés (*pas seulement ceux qui sont infectés*). Si **Anti-Rootkit** détecte un rootkit, cela ne veut pas forcément dire que ce dernier est infecté. Certains rootkits peuvent être utilisés comme pilotes ou faire partie d'applications correctes.

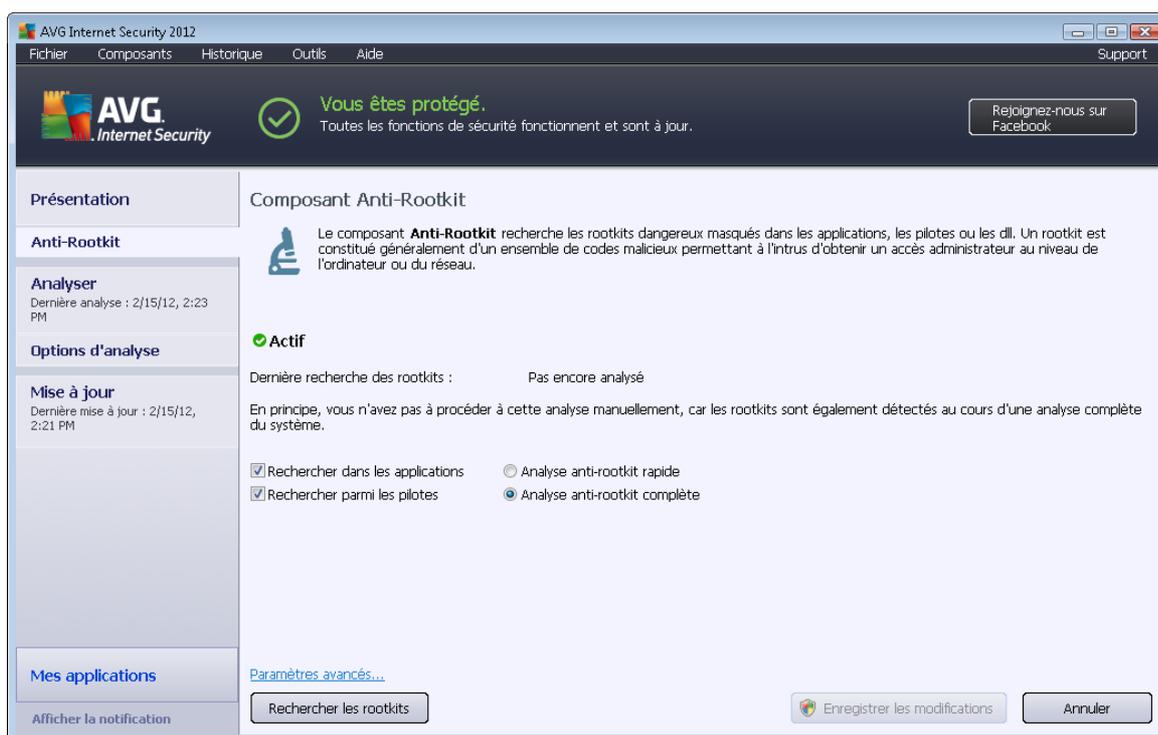
### Qu'est-ce qu'un rootkit ?

Un rootkit est un programme conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. Un accès matériel est rarement nécessaire car un rootkit est prévu pour s'introduire dans le système d'exploitation exécuté sur le matériel. En règle générale, les rootkits dissimulent leur présence dans le système en dupant ou en contournant les mécanismes de sécurité standard du système d'exploitation. Souvent, ils prennent la forme de



chevaux de Troie et font croire aux utilisateurs que leur exécution est sans danger pour leurs ordinateurs. Pour parvenir à ce résultat, différentes techniques sont employées : dissimulation de processus aux programmes de contrôle ou masquage de fichiers ou de données système, au système d'exploitation.

### 6.5.1. Interface de l'Anti-Rootkit



La boîte de dialogue **Anti-Rootkit** décrit brièvement le fonctionnement du composant, indique son état actuel (*Actif*) et fournit des informations sur la dernière analyse **Anti-Rootkit** effectuée (*Dernière recherche des rootkits : la recherche de rootkits est un processus par défaut s'exécutant dans le cadre de l'Analyse complète de l'ordinateur*). La boîte de dialogue **Anti-Rootkit** inclut également un lien [Outils/Paramètres avancés](#). Ce lien permet d'être redirigé vers l'environnement de la configuration avancée du composant **Anti-Rootkit**.

**L'éditeur du logiciel a configuré tous les composants AVG de manière à assurer des performances optimales. Aussi est-il recommandé de ne pas modifier la configuration AVG sans motif valable. Toute modification de ces paramètres doit être réalisée par un utilisateur expérimenté.**

#### Paramètres de base du composant Anti-Rootkit

Dans la partie inférieure de la boîte de dialogue, vous pouvez configurer certaines fonctionnalités de base de la détection rootkits. Cochez tout d'abord les cases permettant d'indiquer les objets à analyser :

- **Rechercher dans les applications**



- **Rechercher parmi les pilotes**

Vous pouvez ensuite choisir le mode d'analyse des rootkits :

- **Analyse anti-rootkit rapide** – Analyser tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows* )
- **Analyse anti-rootkit complète** – Analyser tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows généralement* ), ainsi que tous les disques locaux (*y compris le disque flash, mais pas les lecteurs de disquettes ou de CD-ROM*).

### Boutons de commande

- **Rechercher les rootkits** – Comme l'analyse anti-rootkit ne fait pas partie de l'[analyse complète de l'ordinateur](#), vous devez l'exécuter directement depuis l'interface **Anti-Rootkit** à l'aide de ce bouton.
- **Enregistrer les modifications** – Cliquez sur ce bouton pour enregistrer toutes les modifications réalisées dans cette interface et pour revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*vue d'ensemble des composants*).
- **Annuler** – Cliquez sur ce bouton pour revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*vue d'ensemble des composants*) sans enregistrer les modifications que vous avez effectuées.

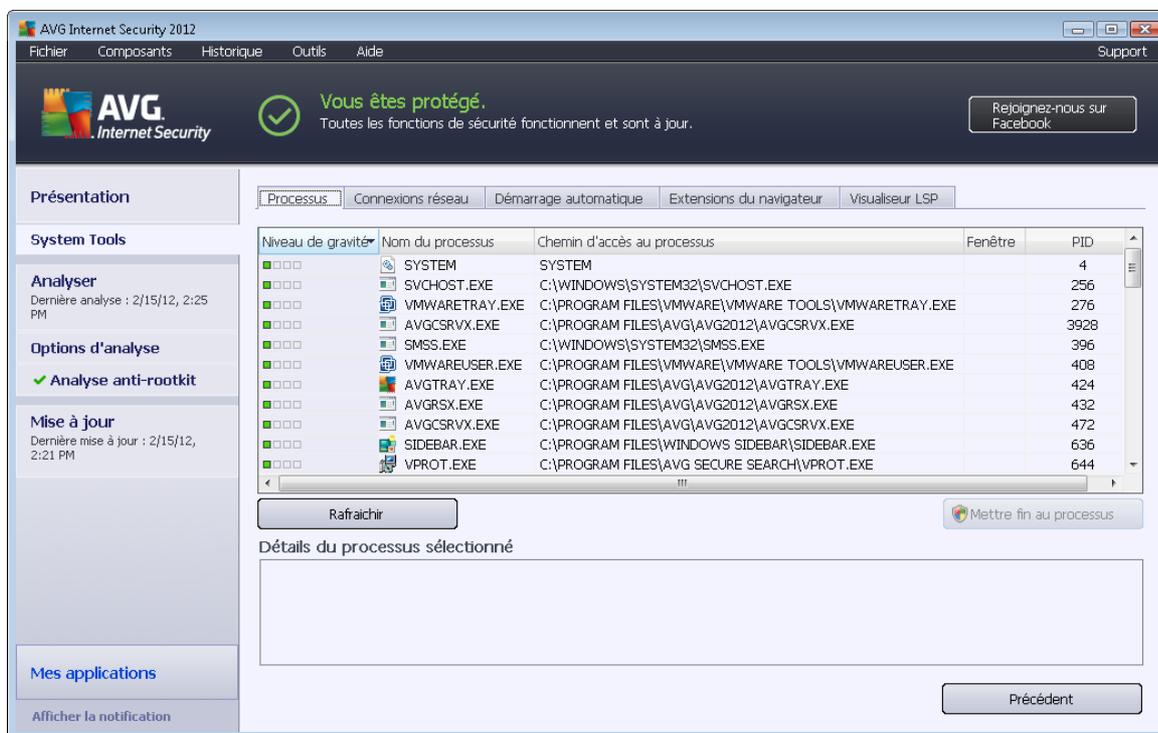
## 6.6. System Tools

**System Tools** désignent les outils offrant une vue détaillée de l'environnement **AVG Internet Security 2012** et du système d'exploitation. Le composant présente :

- [Processus](#) – liste des processus (*applications en cours d'exécution*) actifs sur votre ordinateur
- [Connexions réseau](#) – liste des connexions actives
- [Démarrage automatique](#) – liste des applications qui s'exécutent au démarrage de Windows
- [Extensions du navigateur](#) – liste des plug-ins (*applications*) installés dans votre navigateur Internet
- [Visualiseur LSP](#) – liste des fournisseurs *LSP* (Layered Service Providers)

**Certaines vues sont modifiables, mais notez que cette possibilité ne doit être réservée qu'aux utilisateurs très expérimentés !**

## 6.6.1. Processus



La boîte de dialogue **Processus** indique les processus, (*c'est-à-dire les applications*) actuellement actives sur l'ordinateur. La liste est constituée de plusieurs colonnes :

- **Niveau de gravité** – identification graphique de la gravité du processus en cours sur quatre niveaux allant du moins dangereux (■□□□) au plus grave (■□□■)
- **Nom du processus** – nom du processus en cours
- **Chemin d'accès au processus** – chemin d'accès physique menant à un processus actif
- **Fenêtre** – indique, le cas échéant, le nom de la fenêtre de l'application
- **PID** – numéro d'identification du processus propre à Windows permettant d'identifier de manière unique un processus interne

### Boutons de commande

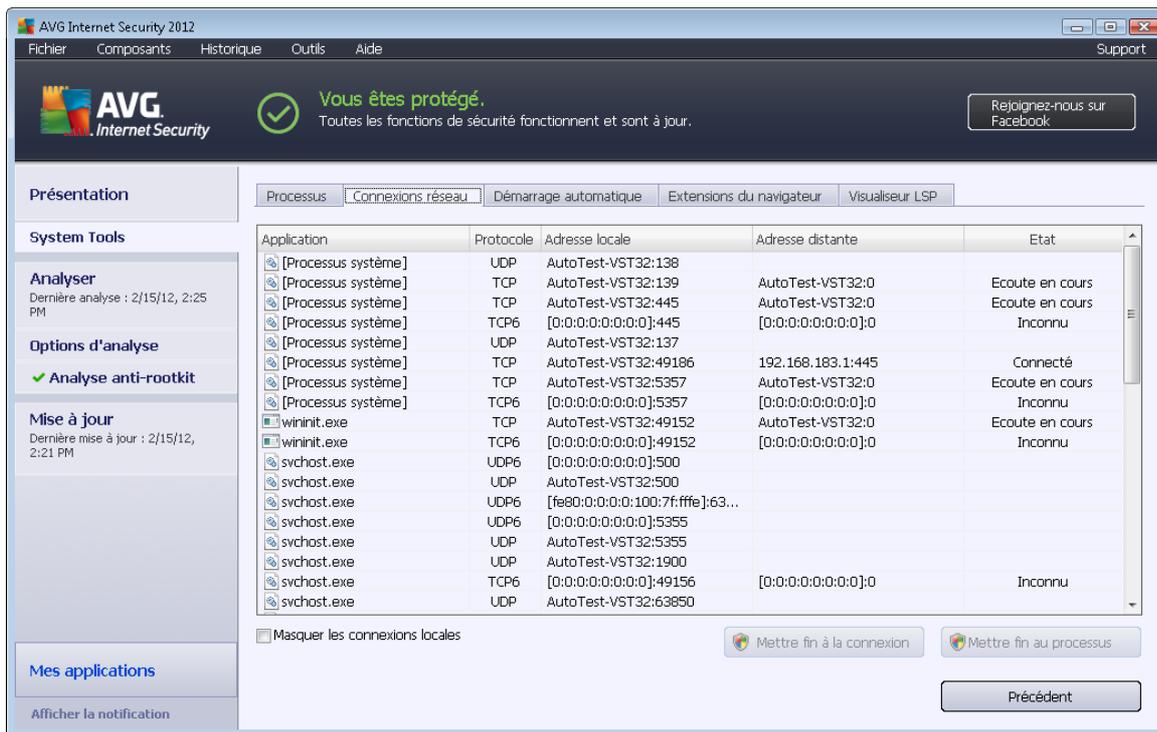
Les boutons de commande disponibles dans l'onglet **Processus** sont les suivants :

- **Actualiser** – met à jour la liste des processus en fonction de l'état actuel
- **Mettre fin au processus** - Vous pouvez sélectionner une ou plusieurs applications et les arrêter en cliquant sur ce bouton. ***nous vous recommandons vivement de n'arrêter aucune application à moins d'être absolument certain qu'elle représente une menace***

**véritable !**

- **Précédent** – permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (présentation des composants).

## 6.6.2. Connexions réseau



The screenshot shows the 'Connexions réseau' (Network Connections) window in AVG Internet Security 2012. The window displays a table of active network connections with the following columns: Application, Protocole, Adresse locale, Adresse distante, and Etat.

Application	Protocole	Adresse locale	Adresse distante	Etat
[Processus système]	UDP	AutoTest-VST32:138		
[Processus système]	TCP	AutoTest-VST32:139	AutoTest-VST32:0	Ecoute en cours
[Processus système]	TCP	AutoTest-VST32:445	AutoTest-VST32:0	Ecoute en cours
[Processus système]	TCP6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	Inconnu
[Processus système]	UDP	AutoTest-VST32:137		
[Processus système]	TCP	AutoTest-VST32:49186	192.168.183.1:445	Connecté
[Processus système]	TCP	AutoTest-VST32:5357	AutoTest-VST32:0	Ecoute en cours
[Processus système]	TCP6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	Inconnu
wininit.exe	TCP	AutoTest-VST32:49152	AutoTest-VST32:0	Ecoute en cours
wininit.exe	TCP6	[0:0:0:0:0:0:0:0]:49152	[0:0:0:0:0:0:0:0]:0	Inconnu
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:500		
svchost.exe	UDP	AutoTest-VST32:500		
svchost.exe	UDP6	[fe80:0:0:0:0:100:7f:ffe]:63...		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:5355		
svchost.exe	UDP	AutoTest-VST32:5355		
svchost.exe	UDP	AutoTest-VST32:1900		
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49156	[0:0:0:0:0:0:0:0]:0	Inconnu
svchost.exe	UDP	AutoTest-VST32:63850		

La boîte de dialogue **Connexions réseau** dresse la liste des connexions actives. Voici les différentes colonnes affichées :

- **Application** – nom de l'application liée à la connexion (*sauf pour Windows 2000 pour lequel les informations ne sont pas disponibles*)
- **Protocole** – type de protocole de transmission utilisé par la connexion :
  - TCP – protocole utilisé avec Internet Protocol (IP) pour communiquer des informations par Internet.
  - UDP – protocole pouvant remplacer le protocole TCP
- **Adresse locale** – adresse IP de l'ordinateur local et numéro de port utilisé
- **Adresse distante** – adresse IP de l'ordinateur distant et numéro de port auquel il est relié. Si possible, il spécifie également le nom d'hôte de l'ordinateur distant.
- **Etat** – indique l'état actuel le plus probable *Connecté, Le serveur doit s'arrêter, Ecouter, Fermeture active terminée, Fermeture passive, Fermeture active*)



Pour répertorier seulement les connexions externes, cochez la case **Masquer les connexions locales** qui figure dans la partie inférieure de la boîte de dialogue, sous la liste.

### Boutons de commande

L'onglet **Connexions réseau** comporte les boutons de commande suivants :

- **Mettre fin à la connexion** – ferme une ou plusieurs connexions sélectionnées dans la liste
- **Mettre fin au processus** – ferme une ou plusieurs applications associées aux connexions sélectionnées dans la liste
- **Précédent** – permet de revenir à la boîte de dialogue principale d'AVG par défaut (présentation des composants).

**Parfois, il n'est possible d'arrêter que les applications actuellement connectées ! Nous vous recommandons vivement de n'arrêter aucune connexion à moins d'être absolument certain qu'elle représente une véritable menace.**

### 6.6.3. Démarrage automatique

The screenshot shows the 'Démarrage automatique' (Automatic Start) tab in the AVG Internet Security 2012 interface. It displays a table with three columns: 'Nom' (Name), 'Localisation' (Location), and 'Chemin d'accès' (Access Path). The table lists various system and application components that are configured to start automatically with Windows.

Nom	Localisation	Chemin d'accès
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-20\Software\Micr...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
Sidebar	\REGISTRY\USER\S-1-5-20\Software\Micr...	%ProgramFiles%\Windows Sidebar\Sidebar...
yProt	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\AVG Secure Search\yprot...
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-19\Software\Micr...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
C:\Windows\system32\mshta.exe "%1" ...	\REGISTRY\MACHINE\SOFTWARE\Classes...	C:\Windows\system32\mshta.exe "%1" %*
SilkTest Agent	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Automation\startagent.bat"
AVG_TRAY	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\AVG\AVG2012\avgtray.exe"
VMware User Process	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
Sidebar	\REGISTRY\USER\S-1-5-21-2323238519-...	C:\Program Files\Windows Sidebar\sidebar.e...
SHELL	\INI\system.ini\BOOT\SHELL	SYS:Microsoft\Windows NT\CurrentVersion...
VMware Tools	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
hffsrsv	\REGISTRY\MACHINE\SOFTWARE\Microso...	c:\windows\hffext\hffsrsv.exe
Adobe Reader Speed Launcher	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\Adobe\Reader 8.0\Reade...
Sidebar	\REGISTRY\USER\S-1-5-19\Software\Micr...	%ProgramFiles%\Windows Sidebar\Sidebar...
AppInit_DLLs	\REGISTRY\MACHINE\SOFTWARE\Microso...	qaphooks.dll

La boîte de dialogue de **démarrage automatique** indique toutes les applications qui sont exécutées lors du démarrage système de Windows. Très souvent, des applications malveillantes se greffent sur l'entrée de la base de registre de démarrage.



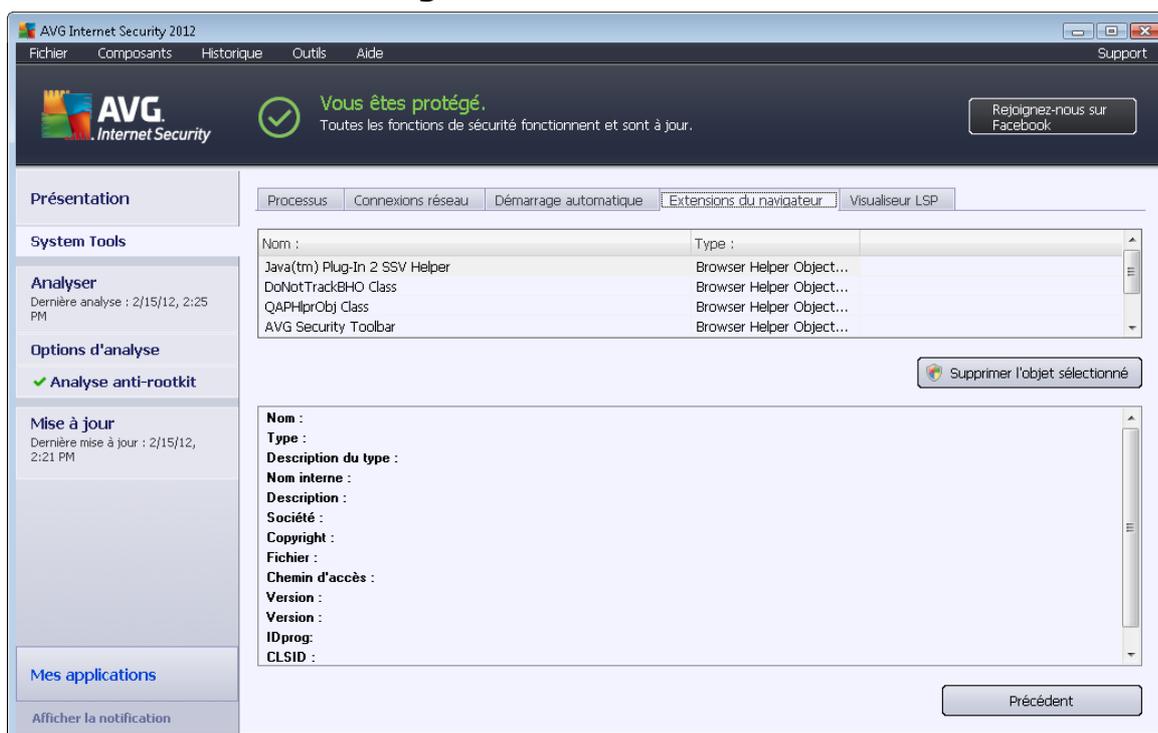
## Boutons de commande

Les boutons de commande disponibles dans l'onglet **Démarrage automatique** sont les suivants :

- **Supprimer l'objet sélectionné** – Ce bouton vous permet de supprimer un ou plusieurs éléments sélectionnés.
- **Retour** – Revenir à la [principale boîte de dialogue d'AVG](#) par défaut (*vue d'ensemble des composants*).

**Nous vous recommandons vivement de n'enlever aucune application de la liste à moins d'être absolument certain qu'elle représente une menace véritable !**

## 6.6.4. Extensions du navigateur



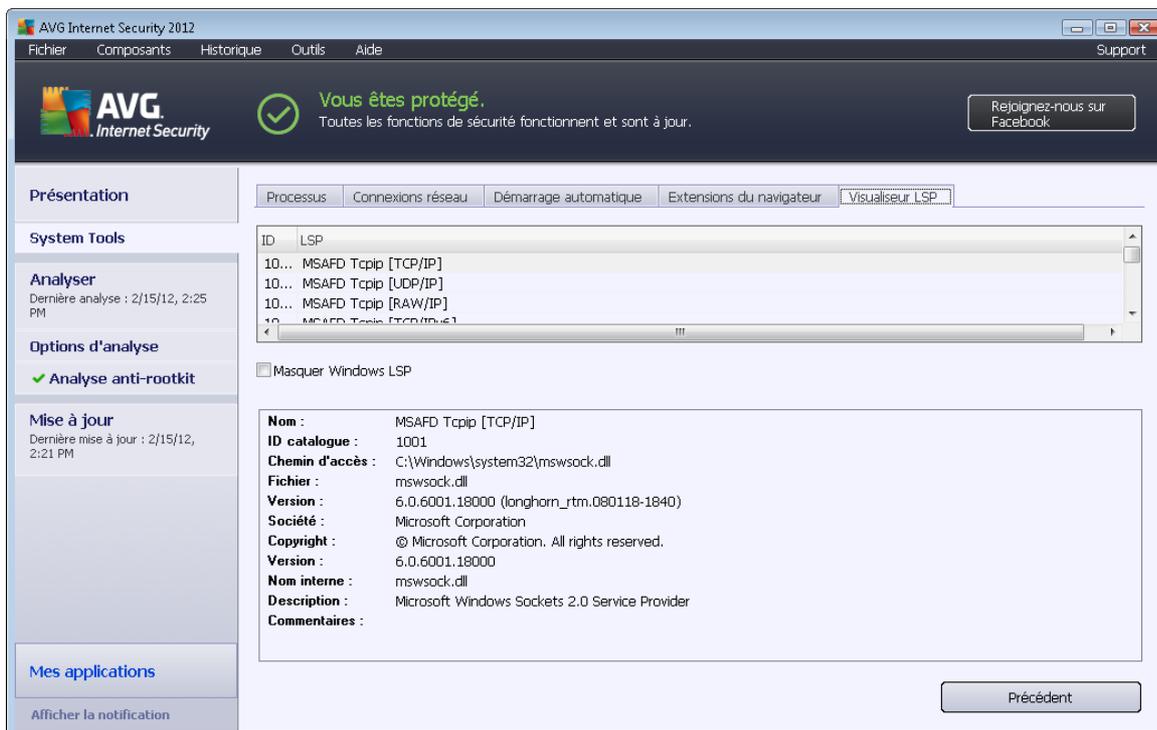
La boîte de dialogue **Extensions du navigateur** contient la liste des plug-ins (*ou applications*) qui sont installés dans votre navigateur Internet. La liste est constituée des plug-ins d'applications standard, ainsi que des programmes potentiellement malveillants. Cliquez sur un objet figurant dans la liste pour obtenir plus d'informations sur le plug-in sélectionné s'affichant dans la section inférieure de la boîte de dialogue.

## Boutons de commande

Les boutons de commande disponibles dans l'onglet **Extensions du navigateur** sont les suivants :

- **Supprimer l'objet sélectionné** – supprime le plug-in mis en surbrillance dans la liste.  
*Nous vous recommandons vivement de ne supprimer aucun plug-in dans la liste sauf si vous êtes absolument certain qu'il représente une menace véritable !*
- **Retour** – revenir à la [principale boîte de dialogue d'AVG](#) par défaut (vue d'ensemble des composants).

## 6.6.5. Visualiseur LSP



La boîte de dialogue **Visualiseur LSP** dresse la liste des fournisseurs de service de connexion (ou fournisseurs LSP).

Un **fournisseur de service de connexion** est un pilote système lié aux services réseau du système d'exploitation Windows. Il a accès à toutes les données qui entrent et sortent de l'ordinateur et peut éventuellement les modifier. En l'absence de certains fournisseurs LSP, Windows ne sera pas en mesure d'établir la connexion avec d'autres ordinateurs ou avec Internet. Cependant, notez que des applications de type malwares peuvent s'installer sous forme de LSP et ainsi avoir accès à toutes les données transmises par l'ordinateur. En conséquence, l'examen minutieux de la liste permet de repérer les menaces LSP potentielles.

Dans certaines conditions, il est également possible de réparer certains LSP dont le lien est interrompu (*notamment si un fichier est supprimé alors que les entrées correspondantes dans la base de registre sont conservées en l'état*). Un nouveau bouton permettant de résoudre ce genre de problème s'affiche dès lors qu'un LSP réparable est détecté.

### Boutons de commande

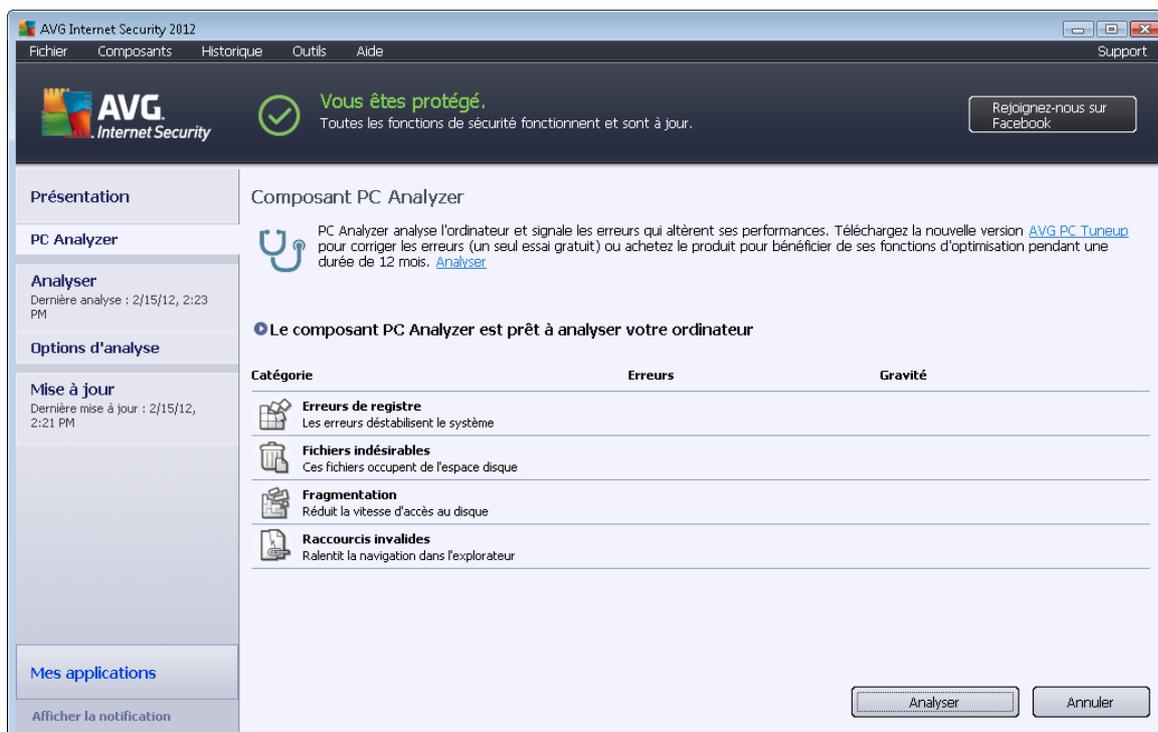


L'onglet **Visualiseur LSP** comporte les boutons de commande suivants :

- **Masquer Windows LSP** – pour ajouter Windows LSP à la liste, désactivez cette option.
- **Précédent** – permet de revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*présentation des composants*).

## 6.7. PC Analyzer

Le composant **PC Analyzer** est en mesure de détecter des défaillances système sur l'ordinateur et d'afficher une présentation claire des éléments à l'origine de la diminution des performances générales de l'ordinateur. Dans l'interface utilisateur du composant, vous pouvez observer un graphique comptant quatre lignes se rapportant aux catégories correspondantes : erreurs de registre, fichiers inutiles, fragmentation et raccourcis corrompus :



- **Erreurs de registre** : indique le nombre d'erreurs dans le Registre Windows. Nous vous déconseillons d'essayer de réparer le registre vous-même, car c'est une tâche qui nécessite des connaissances avancées.
- **Fichiers indésirables** : indique le nombre de fichiers probablement inutiles. Généralement, il s'agit de nombreux types de fichiers temporaires et des fichiers qui se trouvent dans la Corbeille.
- **Fragmentation** : calcule le pourcentage de l'espace du disque dur qui a été fragmenté, c'est-à-dire utilisé sur une longue durée, de sorte que plusieurs fichiers se trouvent éparpillés en différents endroits du disque physique. Un outil de défragmentation permet de remédier à ce gaspillage.



- **Raccourcis corrompus** : indique les raccourcis qui ne fonctionnent plus, mènent à des emplacements inexistant, etc.

Pour lancer l'analyse du système, cliquez sur le bouton **Analyser**. Vous serez en mesure de suivre la progression de l'analyse et d'examiner ses résultats dans le graphique qui apparaîtra :

The screenshot shows the AVG Internet Security 2012 interface. At the top, it says "Vous êtes protégé." and "Toutes les fonctions de sécurité fonctionnent et sont à jour." Below this, the "Composant PC Analyzer" section is active. It states "PC Analyzer a terminé l'analyse". A table displays the results of the analysis:

Catégorie	Erreurs	Gravité
<b>Erreurs de registre</b> Les erreurs déstabilisent le système	137 erreurs détectées <a href="#">Détails...</a>	
<b>Fichiers indésirables</b> Ces fichiers occupent de l'espace disque	293 erreurs détectées <a href="#">Détails...</a>	
<b>Fragmentation</b> Réduit la vitesse d'accès au disque	Fragmenté à 11% <a href="#">Détails...</a>	
<b>Raccourcis invalides</b> Ralentit la navigation dans l'explorateur	14 erreurs détectées <a href="#">Détails...</a>	

At the bottom of the results table, there are two buttons: "Réparer maintenant" and "Annuler".

Les résultats indiquent le nombre et le type de défaillances système détectées (**Erreurs**) selon les catégories évaluées. Les résultats d'analyse se présentent également sous la forme d'un graphique (axe de la colonne **Gravité**).

### Boutons de commande

- **Analyser** (à l'écran avant le début de l'analyse) - ce bouton permet de lancer une analyse immédiate de l'ordinateur
- **Réparer maintenant** (apparaît à la fin de l'analyse) - ce bouton permet d'accéder à la page du site Web d'AVG (<http://www.avg.com/>) qui fournit des informations détaillées et à jour sur le composant **PC Analyzer**
- **Annuler** – cliquez sur ce bouton pour arrêter l'analyse en cours ou pour revenir à l'écran par défaut de la [boîte de dialogue principale d'AVG](#) (présentation des composants) une fois l'analyse terminée



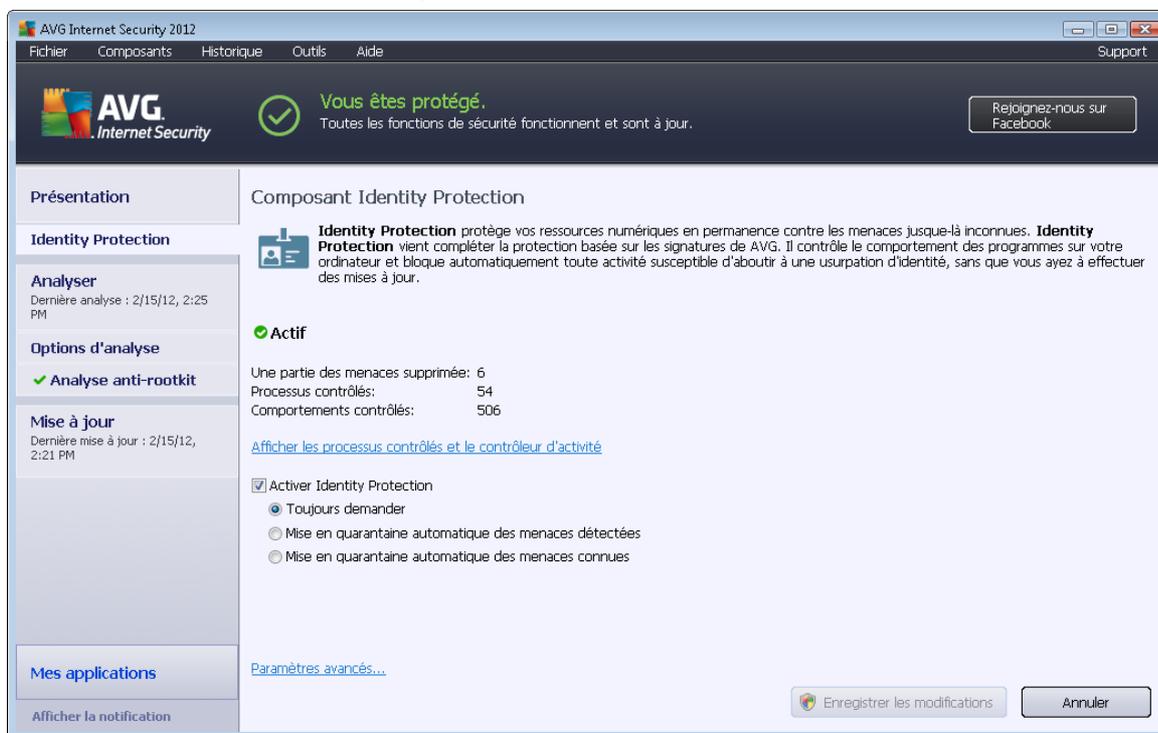
## 6.8. Identity Protection

**Identity Protection** est un composant Anti-malware qui vous protège contre tout type de programmes malveillants (*spywares, bots, usurpation d'identité, etc.*) à l'aide de technologies d'analyse du comportement. Ce programme vous assure une protection de type zero-day, contre les nouveaux virus. **Identity Protection** est une application conçue pour empêcher les usurpateurs d'identité de voler vos mots de passe, coordonnées bancaires, numéros de carte de crédit et autres ressources numériques personnelles au moyen de toutes sortes de logiciels malicieux (*programmes malveillants*) qui menacent votre ordinateur. Il vérifie que tous les programmes exécutés sur votre ordinateur ou sur le réseau partagé fonctionnent correctement. **Identity Protection** détecte et bloque de façon permanente les comportements suspects et protège votre ordinateur contre tous les nouveaux contenus malveillants.

**Identity Protection** assure la protection en temps réel de votre ordinateur contre les menaces nouvelles et inconnues. Il contrôle l'ensemble des processus (*même ceux cachés*) et plus de 285 comportements afin de déterminer si une activité malveillante est en cours sur votre système. Ainsi, il peut identifier des menaces non décrites dans la base de données virale. Lorsqu'un code inconnu s'introduit dans votre ordinateur, il est automatiquement analysé afin de vérifier s'il a un comportement malveillant, puis suivi. Si le fichier s'avère malveillant, **Identity Protection** place le code en [Quarantaine](#) et annule les modifications apportées au système (*injections de code, modifications de registre, ouverture de ports, etc.*). Vous n'avez pas besoin d'exécuter une analyse pour vous protéger. Cette technologie est proactive. Elle ne nécessite que de rares mises à jour et est toujours en mode de surveillance.

**Identity Protection est une protection complémentaire à associer au composant [Anti-Virus](#). Nous vous conseillons vivement d'installer les deux composants pour une protection complète de votre PC !**

## 6.8.1. Interface d'Identity Protection



La boîte de dialogue **Identity Protection** présente brièvement la fonctionnalité du composant, son état (*Actif*) et quelques données statistiques :

- **Menaces supprimées** : Indique le nombre d'applications détectées comme programmes malveillants et supprimées
- **Processus contrôlés** – nombre d'applications actives contrôlées par IDP
- **Comportements contrôlés** – nombre d'actions spécifiques en cours au sein des applications contrôlées

Vous trouverez au-dessous le lien [Afficher les processus contrôlés et le contrôleur d'activité](#) qui affiche l'interface utilisateur du composant [System Tools](#). Ce dernier présente de manière détaillée tous les processus sous surveillance.

### Paramètres de base du composant Identity Protection

Au bas de la boîte de dialogue, vous pouvez modifier certaines fonctions élémentaires du composant :

- **Activer Identity Protection** – (*option activée par défaut*) : cochez cette option pour activer le composant IDP et accéder à d'autres options de modification.

Dans certains cas, **Identity Protection** peut signaler qu'un fichier inoffensif est suspect ou



dangereux. Comme **Identity Protection** détecte les menaces sur la base de leur comportement, ce type de problème survient généralement lorsqu'un programme tente d'enregistrer les pressions de touches du clavier ou d'installer d'autres programmes, ou encore lorsqu'un nouveau pilote est installé sur l'ordinateur. En conséquence, vous devez sélectionner une des options suivantes pour spécifier le comportement du composant **Identity Protection** en cas de détection d'une activité suspecte :

- **Toujours demander** - si une application est identifiée comme malveillante, le programme vous invite à la bloquer (*cette option est activée par défaut et il est recommandé de ne pas modifier ce paramètre sauf absolue nécessité*)
- **Mise en quarantaine automatique des menaces détectées** - toutes les applications détectées comme des programmes malveillants sont automatiquement bloquées
- **Mise en quarantaine automatique des menaces connues** - toutes les applications dont vous êtes certain qu'elles seront détectées comme des programmes malveillants sont automatiquement bloquées
- **Paramètres avancés...** – cliquez sur le lien pour être redirigé vers la boîte de dialogue correspondante dans les [Paramètres avancés](#) d'**AVG Internet Security 2012**. Vous pouvez modifier la configuration du composant de manière approfondie à partir de cette dernière. Cependant, notez que la configuration par défaut de tous les composants est définie de sorte qu'**AVG Internet Security 2012** fournisse une performance optimale et une sécurité maximale. A moins que vous n'ayez une bonne raison de le faire, il est recommandé de préserver cette configuration par défaut !

## Boutons de commande

Les boutons de commande disponibles dans l'interface **Identity Protection** sont :

- **Enregistrer les modifications** : Cliquez sur ce bouton pour enregistrer et appliquer les modifications apportées dans cette boîte de dialogue
- **Annuler** : Cliquez sur ce bouton pour revenir à la [boîte de dialogue principale d'AVG](#) par défaut (*présentation des composants*)

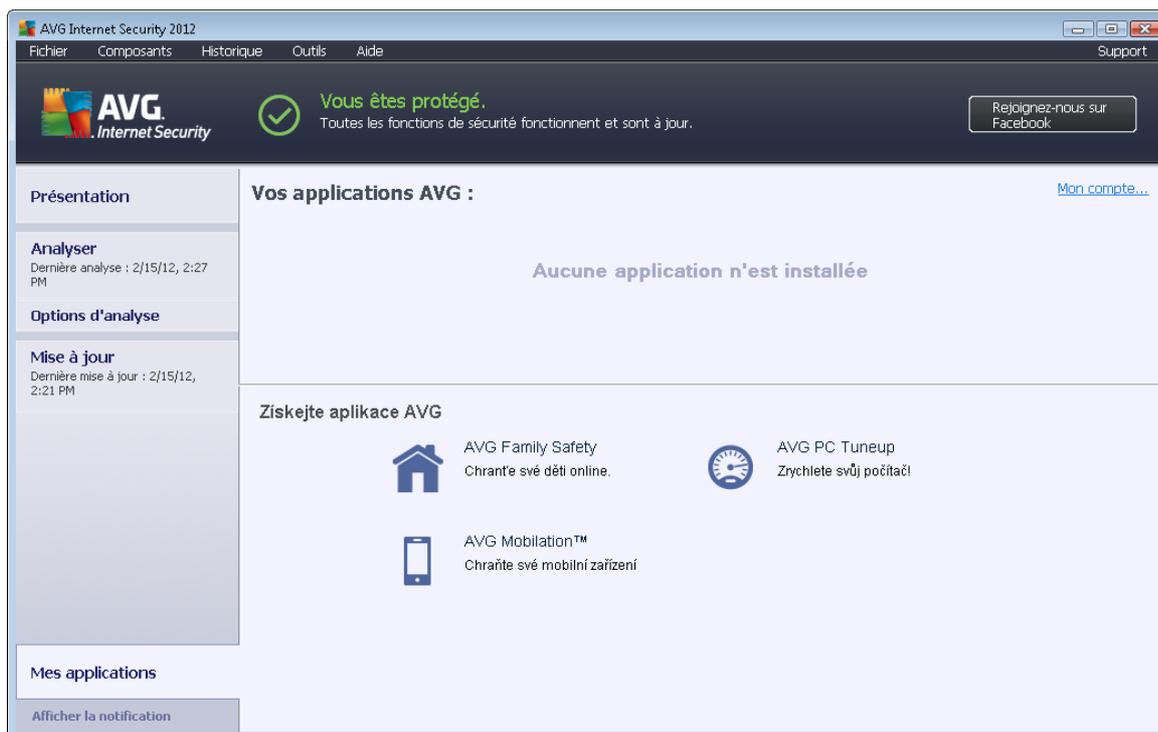
## 6.9. Administration à distance

Le composant **Administration à distance** ne s'affiche dans l'interface utilisateur d'**AVG Internet Security 2012** que si vous installez l'édition professionnelle (Business Edition) de votre produit (*pour plus d'informations sur la licence utilisée pour l'installation, sélectionnez l'onglet [Version](#) de la boîte de dialogue [Informations](#), sous le menu principal [Support](#)*). Pour obtenir une description détaillée des options et de la fonctionnalité du composant dans le système AVG, reportez-vous à la documentation spécifique consacrée à ce sujet. Cette documentation est téléchargeable à partir du site Web d'AVG (<http://www.avg.com/>), section **Centre de support / Téléchargement / Documentation**.



## 7. Mes applications

La boîte de dialogue **Mes Applications** (accessible via le bouton *Mes Applications* de la boîte de dialogue principale d'AVG) contient une présentation des applications autonomes d'AVG déjà installées sur votre ordinateur ou prêtes à être installées, selon vos besoins :



La boîte de dialogue se compose de deux sections :

- **Vos applications AVG** – contient une vue d'ensemble de toutes les applications autonomes d'AVG déjà installées sur votre ordinateur ;
- **Obtenir des applications AVG** – contient une présentation des applications autonomes d'AVG qui pourraient vous intéresser. Ces applications sont prêtes à être installées. L'offre change de manière dynamique selon votre licence, votre emplacement et selon d'autres critères. Pour plus d'informations sur ces applications, veuillez consulter le site Web d'AVG (<http://www.avg.com/>).

Vous trouverez ci-après une brève présentation de toutes les applications disponibles ainsi qu'une courte explication de leurs fonctionnalités :

### 7.1. AVG Family Safety

**AVG Family Safety** protège vos enfants des sites Web inappropriés, du contenu multimédia et des recherches en ligne sur du contenu non approprié. Il produit également des rapports sur leurs activités en ligne. **AVG Family Safety utilise la technologie de frappe de touche pour suivre les activités de vos enfants dans les espaces de discussion et sur les sites de réseaux sociaux.** S'il identifie des mots, des phrases ou des expressions habituellement utilisées pour persécuter les



enfants sur Internet, il vous en informera immédiatement par SMS ou par e-mail. Vous pouvez définir le niveau de protection souhaité en fonction de chacun de vos enfants et les surveiller individuellement grâce à des identifiants uniques.

***Pour en savoir plus, rendez-vous sur la page Web d'AVG dédiée, à partir de laquelle vous pouvez télécharger le composant. Pour ce faire, vous pouvez cliquer sur le lien AVG Family Safety de la boîte de dialogue [Mes applications](#).***

## **7.2. AVG LiveKive**

**LiveKive** est une application de sauvegarde de données en ligne sur des serveurs sécurisés. **AVG LiveKive** sauvegarde automatiquement tous vos fichiers, photos et musiques dans un lieu sûr, ce qui vous permet de les partager avec votre famille et vos amis et d'y accéder à partir de n'importe quel périphérique Web et en particulier des iPhones ou appareils Android. **AVG LiveKive** comporte les fonctions suivantes :

- Mesure de sécurité visant à remédier à la corruption éventuelle de l'ordinateur et/ou du disque dur
- Accès à vos données à partir d'un périphérique connecté à Internet
- Organisation facile
- Partage avec toute personne que vous autorisez

***Pour en savoir plus, rendez-vous sur la page Web d'AVG dédiée, à partir de laquelle vous pouvez télécharger le composant. Pour ce faire, vous pouvez cliquer sur le lien AVG LiveKive de la boîte de dialogue [Mes applications](#).***

## **7.3. AVG Mobilation**

**AVG Mobilation** protège votre téléphone portable contre les virus et les programmes malveillants et vous permet de suivre à distance votre Smartphone en cas de perte. **AVG Mobilation** comprend les fonctions suivantes :

- **File Scanner** analyse la sécurité des fichiers placés dans différents emplacements de stockage ;
- **Task Killer** permet d'interrompre une application si le fonctionnement de l'appareil ralentit ou se bloque ;
- **App Locker** vous permet de verrouiller une ou plusieurs applications et de les protéger par mot de passe contre leur utilisation frauduleuse ;
- **Tuneup** rassemble divers paramètres système (*jauge de batterie, utilisation du stockage, taille et emplacement des installations d'applications, etc.*) dans une vue centralisée pour vous aider à contrôler les performances du système ;
- **App Backup** vous permet de sauvegarder des applications sur votre carte SD et de les restaurer ultérieurement ;



- *la fonction Spam and Scam* vous permet de marquer des messages SMS comme spams et de signaler des sites Web comme des escroqueries ;
- *la suppression de vos données personnelles* à distance en cas de vol de votre téléphone portable ;
- *la navigation Web sécurisée* vous offre une surveillance en temps réel des pages Web que vous consultez.

***Pour en savoir plus, rendez-vous sur la page Web d'AVG dédiée, à partir de laquelle vous pouvez télécharger le composant. Pour ce faire, vous pouvez cliquer sur le lien AVG Mobilation de la boîte de dialogue [Mes applications](#).***

## **7.4. AVG PC Tuneup**

L'application **AVG PC Tuneup** est un outil avancé d'analyse approfondie et de correction du système permettant d'améliorer la vitesse et la performance globale de votre ordinateur.

**AVG PC Tuneup** comporte les fonctions suivantes :

- Disk Cleaner – Supprime les fichiers indésirables qui ralentissent l'ordinateur.
- Disk Defrag – Défragmente les disques durs et optimise les fichiers système.
- Registry Cleaner – Répare les erreurs du registre en vue d'améliorer la stabilité du PC.
- Registry Defrag – Comprime le registre et élimine les interstices, consommateurs de mémoire.
- Disk Doctor – Recherche et corrige les secteurs défectueux, les clusters perdus et les erreurs de répertoire.
- Internet Optimizer – Adapte les paramètres génériques à une connexion Internet spécifique.
- Track Eraser – Supprime l'historique de vos activités sur l'ordinateur et sur Internet.
- Disk Wiper – Efface l'espace libre des disques durs, afin d'éviter toute récupération de données sensibles.
- File Shredder – Efface et rend irrécupérables les fichiers d'un disque ou d'une clé USB.
- File Recovery – Récupère les fichiers supprimés accidentellement d'un disque, d'une clé USB ou d'un appareil photo.
- Duplicate File Finder – Aide à rechercher et à supprimer les doublons qui occupent inutilement de l'espace disque.
- Service Manager – Désactive les services inutiles qui ralentissent l'ordinateur.



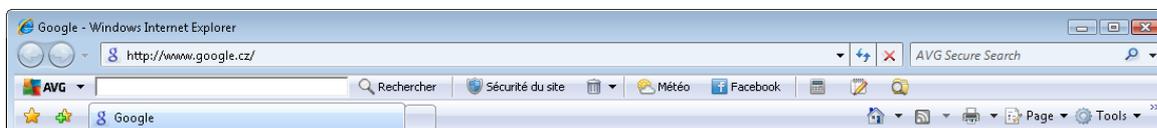
- Startup Manager – Permet à l'utilisateur de gérer les programmes qui se lancent automatiquement au démarrage de Windows.
- Uninstall Manager – Désinstalle entièrement les logiciels devenus inutiles.
- Tweak Manager – Permet à l'utilisateur de paramétrer des centaines de paramètres masqués de Windows.
- Task Manager – Répertorie les processus en cours, les services et les fichiers verrouillés.
- Disk Explorer – Affiche les fichiers qui occupent le plus d'espace sur l'ordinateur.
- System Information – Fournit des informations détaillées sur le matériel et les logiciels installés.

***Pour en savoir plus, rendez-vous sur la page Web d'AVG dédiée, à partir de laquelle vous pouvez télécharger le composant. Pour ce faire, vous pouvez cliquer sur le lien AVG PC Tuneup de la boîte de dialogue [Mes applications](#).***



## 8. AVG Security Toolbar

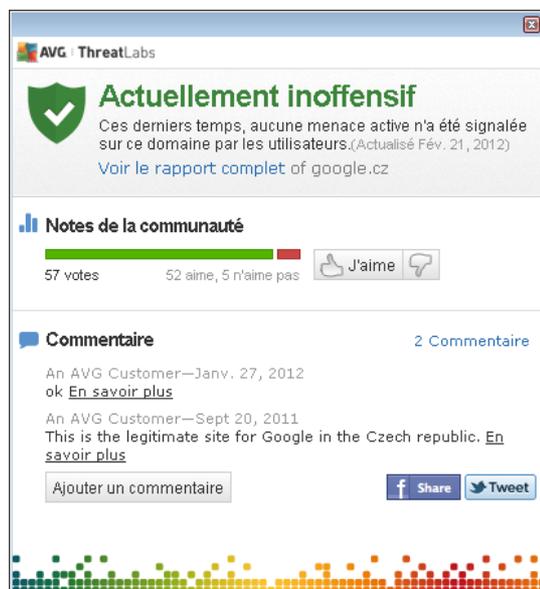
La **barre d'outils de sécurité AVG** est un outil qui fonctionne en étroite collaboration avec le composant [LinkScanner](#), afin de maintenir un niveau de sécurité élevé lorsque vous surfez sur Internet. Dans **AVG Internet Security 2012**, l'installation de la **Barre d'outils de sécurité AVG** est facultative ; au cours du [processus d'installation](#), vous avez été invité à décider d'installer ou non ce composant. La **Barre d'outils de sécurité AVG** est disponible directement dans votre navigateur Internet. Pour l'instant, les navigateurs suivants sont pris en charge : Internet Explorer (*version 6.0 et ultérieure*) et/ou Mozilla Firefox (*version 3.0 et ultérieure*). Aucun autre navigateur n'est pris en charge : *si vous utilisez un navigateur autre qu'Internet Explorer (par exemple, Avant Browser), ce dernier peut fonctionner de manière inattendue*.



La **barre d'outils de sécurité AVG** comprend les éléments suivants :

- **Le logo AVG** avec son menu déroulant :
  - **Utiliser AVG Secure Search** - Permet d'effectuer des recherches directement dans la **Barre d'outils de sécurité AVG** à l'aide du moteur **AVG Secure Search**. Tous les résultats des recherches sont vérifiés en permanence par le service [Search-Shield](#), de sorte que vous puissiez vous sentir en toute sécurité en ligne.
  - **Niveau de menace actuel** - Ouvre la page Web des laboratoires de virus donnant une représentation graphique du niveau de menace actuel sur le Web.
  - **AVG Threat Labs** – Ouvre la page du site Web d'**AVG Threat Lab** (à l'adresse <http://www.avgthreatlabs.com>) sur laquelle vous pouvez trouver des informations sur la sécurité de divers sites Web et le niveau de menace actuel en ligne.
  - **Aide de la barre d'outils** - Ouvre l'aide en ligne portant sur toutes les fonctionnalités de la **Barre d'outils de sécurité AVG**.
  - **Envoyer le feedback sur le produit** - Ouvre une page Web contenant un formulaire que vous pouvez remplir pour nous dire ce que vous pensez de la **Barre d'outils de sécurité AVG**.
  - **A propos de...** - Ouvre une nouvelle fenêtre contenant des informations sur la version de la **Barre d'outils de sécurité AVG** actuellement installée.
- **Champ de recherche** - Effectuez vos recherches sur Internet à l'aide de la **Barre d'outils de sécurité AVG** qui vous garantit sécurité et confort, puisque tous les résultats de recherche affichés sont sûrs à cent pour cent. Entrez un mot clé ou une expression dans le champ de recherche et cliquez sur le bouton **Rechercher** (ou appuyez sur la touche **Entrée**). Tous les résultats de recherche sont vérifiés en permanence par le service [Search-Shield](#) (dans le composant [LinkScanner](#)).
- **Sécurité du site** – Ce bouton ouvre une nouvelle boîte de dialogue indiquant des informations sur le niveau de menace actuel (*Actuellement inoffensif*) de la page que vous consultez. Ce bref

aperçu peut être étendu pour afficher dans la fenêtre du navigateur toutes les informations de toutes les activités de sécurité liées à la page (*Voir le rapport complet*) :



- **Supprimer** – Le bouton "corbeille" dispose d'un menu déroulant dans lequel vous pouvez sélectionner les informations de navigation à effacer, comme l'historique, les téléchargements, les formulaires en ligne, ou supprimer immédiatement tout votre historique de recherche.
- **Météo** – Ce bouton ouvre une boîte de dialogue qui vous fournit des informations sur le temps qu'il fait là où vous vous trouvez ainsi que les prévisions pour les deux jours à venir. Ces informations sont régulièrement mises à jour toutes les 3-6 heures. Dans cette boîte de dialogue, vous pouvez modifier le lieu manuellement et décider si la température doit s'afficher en Celsius ou en Fahrenheit.



- **Facebook** – Ce bouton vous permet de vous connecter directement au réseau social [Facebook](#) depuis la **Barre d'outils de sécurité AVG**.
- Boutons de raccourci pour accéder rapidement aux applications suivantes : **Calculatrice**, **Bloc-notes**, **Explorateur Windows**.



## 9. AVG Do Not Track

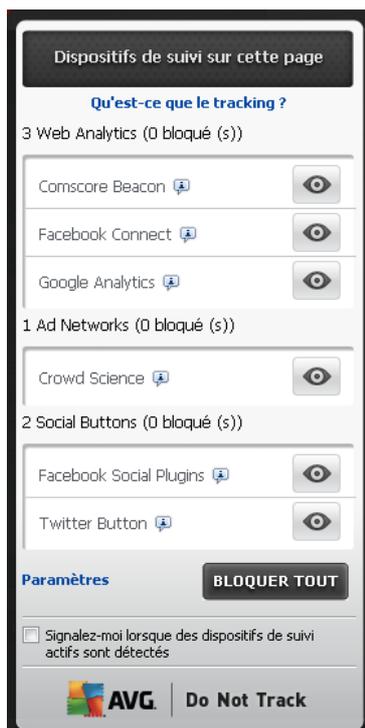
**AVG Do Not Track** vous aide à identifier les sites Web qui collectent des données relatives à vos activités en ligne. Une icône dans votre navigateur indique les sites Web ou les réseaux publicitaires qui collectent des données relatives à vos activités et vous donne le choix d'activer ou de désactiver cette collecte.

- **AVG Do Not Track** vous fournit des informations supplémentaires sur la politique de confidentialité de chaque service ainsi qu'un lien direct pour se désinscrire du service, le cas échéant.
- En outre, **AVG Do Not Track** prend en charge le [protocole W3C DNT](#) pour informer automatiquement les sites que vous ne souhaitez pas être suivi. Cette notification est activée par défaut mais peut être modifiée à tout moment.
- **AVG Do Not Track** est fourni selon les [termes et conditions](#) suivants.
- **La fonctionnalité AVG Do Not Track** est activée par défaut mais peut être facilement désactivée à tout moment. Des instructions sont disponibles dans l'article de la FAQ [Désactivation de la fonctionnalité AVG Do Not Track](#).
- Pour plus d'informations sur **AVG Do Not Track**, visitez notre [site Web](#).

Actuellement, la fonctionnalité **AVG Do Not Track** est uniquement prise en charge par les navigateurs suivants : Mozilla Firefox, Chrome et Internet Explorer. *(Dans Internet Explorer, l'icône AVG Do Not Track est située sur la droite de la barre de commandes. En cas de problème d'affichage de l'icône AVG Do Not Track en utilisant les paramètres par défaut du navigateur, veuillez vérifier que vous avez activé la barre de commandes. Si vous ne voyez toujours pas l'icône, faites glisser la barre de commandes sur la gauche pour afficher tous les boutons et icônes disponibles dans cette barre d'outils.)*

## 9.1. AVG Do Not Track

Quand vous êtes en ligne, **AVG Do Not Track vous prévient dès qu'une activité de collecte de données a été détectée.** La boîte de dialogue suivante s'affiche :



Tous les services de collecte de données sont classés par nom dans la présentation **Dispositifs de suivi sur cette page**. **Il existe trois types d'activités de collecte de données reconnus par AVG Do Not Track :**

- **Web Analytics** (par défaut : autorisé) : services utilisés pour améliorer les performances et l'expérience du site Web correspondant. Dans cette catégorie, vous pouvez trouver des services tels que Google Analytics, Omniture ou Yahoo Analytics. Nous recommandons de ne pas bloquer les services d'analyses Web, car le site Web pourrait ne pas fonctionner comme prévu.
- **Social buttons** (par défaut : autorisé) : éléments conçus pour améliorer le réseautage social. Les boutons sociaux sont insérés par des réseaux sociaux sur le site que vous visitez. Ils peuvent collecter des données relatives à votre activité en ligne lorsque vous êtes connecté. Voici quelques exemples de boutons sociaux : plug-ins sociaux Facebook, bouton Twitter, Google +1.
- **Ad Networks** (par défaut : bloqué pour certains) : services qui collectent ou partagent directement ou indirectement des données relatives à votre activité en ligne sur plusieurs sites pour vous proposer des publicités personnalisées, contrairement aux publicités basées sur le contenu. Ils sont déterminés en fonction de la politique de confidentialité disponible sur le site Web de chaque réseau publicitaire. Certains d'entre eux sont bloqués par défaut.



**Remarque :** en fonction des services en cours d'exécution en arrière-plan sur le site Web, plusieurs des trois sections décrites ci-dessus peuvent ne pas apparaître dans la boîte de dialogue AVG Do Not Track.

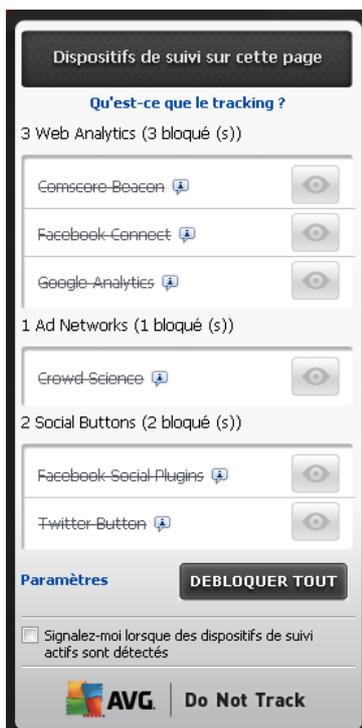
La boîte de dialogue contient également deux hyperliens :

- **Qu'est-ce que le tracking ?** - cliquez sur ce lien dans la section supérieure de la boîte de dialogue pour être redirigé vers la page Web dédiée fournissant des explications détaillées sur les principes de fonctionnement du tracking, et une description des types de tracking spécifiques.
- **Paramètres** - cliquez sur ce lien dans la section inférieure de la boîte de dialogue pour être redirigé vers la page Web dédiée sur laquelle vous pourrez configurer spécifiquement les différents paramètres d'**AVG Do Not Track** (voir le chapitre sur les [paramètres d'AVG Do Not Track](#) pour plus d'informations)

## 9.2. Informations sur les processus de suivi

La liste des services de collecte de données fournit uniquement le nom du service en question. Pour bien choisir quel service autoriser ou bloquer, il vous faut davantage d'informations. Passez votre souris sur l'élément de la liste concerné. Une info-bulle apparaît et fournit des données détaillées sur le service. Vous saurez s'il collecte vos données personnelles ou d'autres données disponibles, si elles sont partagées avec des tiers et si elles sont archivées pour une éventuelle utilisation future.

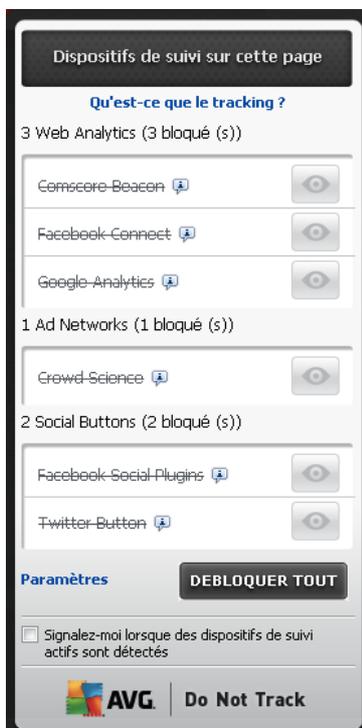
Dans la partie inférieure de l'info-bulle, vous pouvez voir le lien **Politique de confidentialité** qui vous redirige vers le site Web dédié à la politique de confidentialité du service détecté en question.



### 9.3. Bloquer les processus de suivi

Dans les listes de tous les Ad Networks, de tous les Social Buttons et de toutes les analyses Web, vous pouvez désormais spécifier quels services de suivi doivent être bloqués. Deux possibilités s'offrent à vous :

- **Bloquer tout** - Cliquez sur ce bouton situé dans la partie inférieure de la boîte de dialogue pour indiquer que vous ne souhaitez aucune activité de collecte de données. (*Cependant, veuillez noter que cette action peut endommager la fonctionnalité sur la page Web où le service est en cours.*)
-  – Si vous ne souhaitez pas bloquer immédiatement les services détectés, vous pouvez indiquer si le service doit être bloqué ou autorisé de manière individuelle. Vous pouvez autoriser l'exécution de certains systèmes détectés (*par exemple analyses Web*) : ceux de ce type utilisent les données collectées pour l'optimisation de leur propre site afin d'améliorer l'environnement Internet pour tous les utilisateurs. Toutefois, vous pouvez simultanément bloquer les activités de collecte de données de tous les processus classés comme Ad Networks. Cliquez simplement sur  l'icône en regard du service pour bloquer la collecte de données (*le nom du processus sera alors barré*) ou pour l'autoriser à nouveau.



### 9.4. Paramètres AVG Do Not Track

La boîte de dialogue **AVG Do Not Track** ne propose qu'une seule option de configuration : dans la partie inférieure, vous pouvez voir la case à cocher **Signaler la détection de dispositifs de suivi actifs**. Par défaut, elle est désactivée. Cochez la case pour confirmer que vous souhaitez être averti



à chaque fois que vous consultez une page Web contenant un nouveau service de collecte de données qui n'a pas encore été bloqué. Lorsqu'elle est cochée, si **AVG Do Not Track** détecte un nouveau service de collecte de données sur une page que vous êtes en train de consulter, la boîte de dialogue vous le signalant apparaît à l'écran. Si elle n'est pas cochée, vous remarquez simplement la détection d'un service par **le passage de vert à jaune** de l'icône **AVG Do Not Track** (située dans la barre de commandes de votre navigateur).

Toutefois, dans la partie inférieure de la boîte de dialogue **AVG Do Not Track**, vous pouvez trouver le lien **Paramètres**. **Cliquez sur le lien pour être redirigé vers une page Web où vous pouvez indiquer vos Options AVG Do Not Track** détaillées :

### Options AVG Do Not Track

#### Informez-moi

Durée de notification  secondes

Position de la notification

- Signaler la détection de dispositifs de suivi actifs
- Informer les sites Web que je ne souhaite pas être suivi (en utilisant [l'en-tête http Do Not Track](#))

#### Bloquer les éléments suivants

<input checked="" type="checkbox"/>	24/7 Real Media	Ad Networks
<input checked="" type="checkbox"/>	33Across	Ad Networks
<input checked="" type="checkbox"/>	[x+1]	Ad Networks
<input checked="" type="checkbox"/>	Accelerator Media	Ad Networks
<input checked="" type="checkbox"/>	AddtoAny	Ad Networks
<input checked="" type="checkbox"/>	Adition	Ad Networks
<input checked="" type="checkbox"/>	AdReady	Ad Networks
<input checked="" type="checkbox"/>	Aggregate Knowledge	Ad Networks
<input checked="" type="checkbox"/>	Baynote Observer	Ad Networks
<input checked="" type="checkbox"/>	Bizo	Ad Networks

Bloquer tout

Autoriser tout

Paramètres par défaut

Annuler

Enregistrer

- **Position de la notification** (*En haut à droite par défaut*) - Ouvrez la liste déroulante pour indiquer la position sur l'écran où vous souhaitez voir apparaître la boîte de dialogue
- **Afficher la notification pour** (*10 par défaut*) - Dans ce champ, vous pouvez définir la durée (*en secondes*) d'affichage à l'écran de la notification **AVG Do Not Track**. **La valeur peut être comprise entre 0 et 60 secondes** (si vous la réglez sur 0, la notification ne s'affichera pas).
- **Signaler la détection de dispositifs de suivi actifs** (*par défaut : désactivé*) - Cochez la case pour confirmer que vous souhaitez être averti à chaque fois que vous consultez une



page Web contenant un nouveau service de collecte de données qui n'a pas encore été bloqué. Lorsqu'elle est cochée, si **AVG Do Not Track** détecte un nouveau service de collecte de données sur une page que vous êtes en train de consulter, la boîte de dialogue vous le signalant apparaît à l'écran. Si elle n'est pas cochée, vous remarquez simplement la détection d'un service par **le passage de vert à jaune de l'icône** AVG Do Not Track (située dans la barre de commandes de votre navigateur).

- **Informez les sites Web que je ne souhaite pas être suivi** (par défaut : activé) - Laissez cette option cochée pour confirmer que vous souhaitez que **AVG Do Not Track** informe le fournisseur du service de collecte de données détecté que vous ne souhaitez pas faire l'objet d'un suivi.
- **Bloquer les éléments suivants** (par défaut : tous les services de collecte de données sont autorisés) – Dans cette section, vous pouvez voir une liste des services de collecte de données connus qui peuvent être classés comme Ad Networks. Par défaut, **AVG Do Not Track** bloque certains Ad Networks automatiquement et vous laisse choisir si vous souhaitez bloquer ou autoriser les autres. Pour ce faire, cliquez sur le bouton **Bloquer tout** en bas de la liste.

Les boutons de contrôle disponibles sur la page **Options AVG Do Not Track** sont les suivants :

- **Tout bloquer** : cliquez pour bloquer immédiatement tous les services répertoriés dans la boîte de dialogue ci-dessus qui sont classés comme Ad Networks ;
- **Autoriser tout** : cliquez pour débloquer immédiatement tous les services répertoriés dans la boîte de dialogue ci-dessus qui sont classés comme Ad Networks ;
- **Par défaut** : cliquez pour annuler tous vos paramètres personnalisés et pour rétablir la configuration par défaut ;
- **Enregistrer** : cliquez pour appliquer et enregistrer votre configuration ;
- **Annuler** : cliquez pour annuler tous les paramètres que vous avez indiqués.

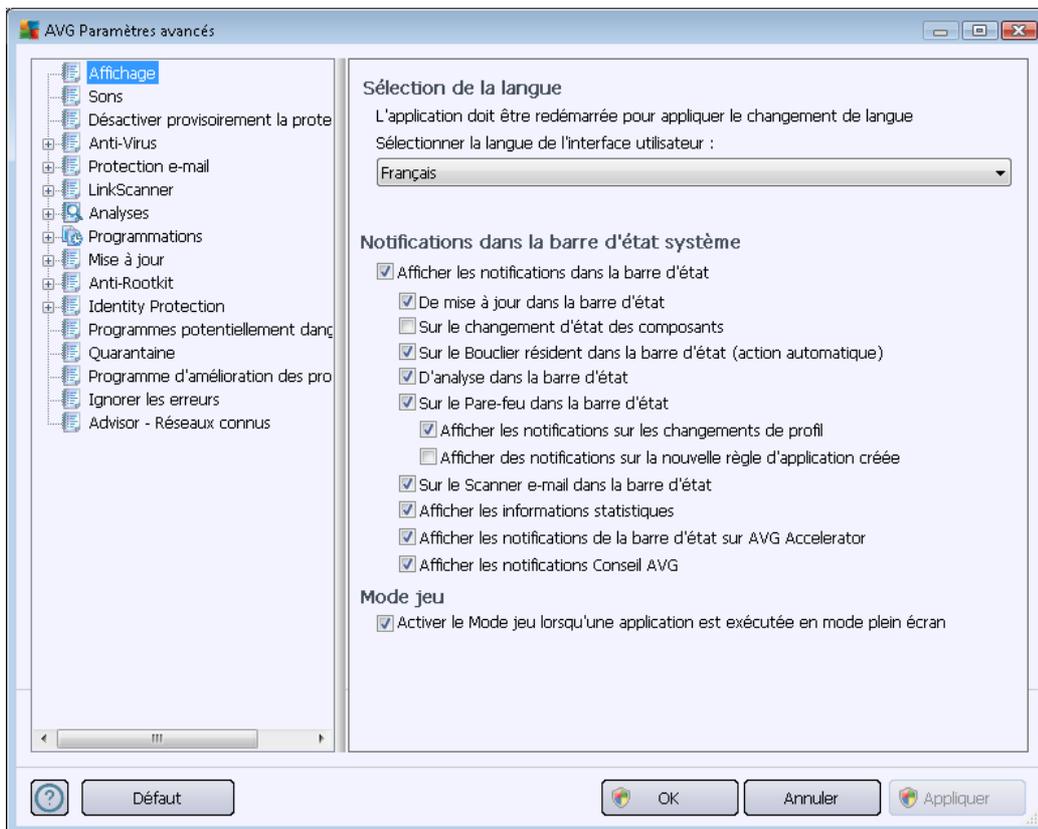


## 10. Paramètres avancés d'AVG

La boîte de dialogue de configuration avancée d'**AVG Internet Security 2012** a pour effet d'ouvrir une nouvelle fenêtre intitulée **Paramètres avancés d'AVG**. Cette fenêtre se compose de deux parties : la partie gauche présente une arborescence qui permet d'accéder aux options de configuration du programme. Sélectionnez le composant dont vous voulez modifier la configuration (*ou celle d'une partie spécifique*) pour ouvrir la boîte de dialogue correspondante dans la partie droite de la fenêtre.

### 10.1. Affichage

Le premier élément de l'arborescence de navigation, **Affichage**, porte sur les paramètres généraux de l'**interface utilisateur** d'[AVG Internet Security 2012](#) et sur des options essentielles du comportement de l'application :



#### Sélection de la langue

Dans la section **Sélection de la langue**, vous pouvez sélectionner la langue de votre choix dans le menu déroulant. La langue sélectionnée sera valable pour tous les composants de l'**interface utilisateur** de **AVG Internet Security 2012**. Le menu déroulant ne propose que les langues que vous avez sélectionnées au cours du [processus d'installation](#) (voir chapitre [Options personnalisées](#)) en plus de l'anglais (*l'anglais étant toujours installé par défaut*). Pour terminer le passage d'**AVG Internet Security 2012** vers une autre langue, il faut redémarrer l'application. Pour résoudre ce problème, procédez comme suit :



- Dans le menu déroulant, sélectionnez la langue dans laquelle vous voulez utiliser l'application
- Confirmez votre sélection en appuyant sur le bouton **Appliquer** (angle inférieur droit de la boîte de dialogue)
- Cliquez sur le bouton **OK** pour confirmer.
- Une nouvelle boîte de dialogue vous informe que pour modifier la langue de l'application, vous devez redémarrer votre **AVG Internet Security 2012**
- Appuyez sur le bouton **Redémarrer l'application maintenant** pour confirmer le redémarrage du programme, puis patientez jusqu'à ce que le changement de langue soit effectif :



### Notifications dans la barre d'état système

Dans cette section, vous pouvez supprimer l'affichage de notifications dans la barre d'état indiquant l'état de l'application **AVG Internet Security 2012**. Par défaut, l'affichage des notifications dans la barre d'état est autorisé. Il est fortement recommandé de conserver cette configuration ! Les notifications système fournissent des informations sur le lancement de l'analyse ou du processus de mise à jour, ou sur la modification du statut d'un composant **AVG Internet Security 2012**. Il est vivement conseillé de ne pas ignorer ces notifications !

Cependant, si pour une raison quelconque vous préférez ne pas recevoir ce type d'information ou si vous ne voulez recevoir que certaines notifications (*liées à un composant AVG Internet Security 2012 spécifique*), vous pouvez définir et préciser vos préférences en cochant/décochant les options suivantes :

- **Afficher les notifications dans la barre d'état** (*activé par défaut*) - Par défaut, toutes les notifications s'affichent. Décochez cette option pour désactiver complètement l'affichage de toutes les notifications dans la barre d'état. Lorsqu'elle est active, vous pouvez sélectionner les notifications qui doivent s'afficher :
  - **Afficher des notifications dans la barre d'état système concernant la [mise à jour](#)** (*activé par défaut*) - Indiquez s'il faut afficher les informations sur le lancement, la progression et la fin du processus de mise à jour d'**AVG Internet Security 2012**.
  - **Afficher les notifications concernant le changement d'état des composants** (*désactivé par défaut*) – indiquez s'il faut afficher des informations sur l'activité/ arrêt d'activité des composants ou les problèmes éventuels. Lorsque cette option signale un état d'anomalie dans un composant, elle a la même fonction d'information que l'[icône dans la barre d'état système](#) signalant un problème lié à un composant **AVG Internet Security 2012**.



- **Afficher les notifications sur le [Bouclier résident](#) dans la barre d'état (action automatique) (activé par défaut)** – Indiquez s'il faut afficher ou supprimer les informations sur les processus d'enregistrement, de copie et d'ouverture de fichier ( cette configuration est applicable seulement si l'option [Réparer automatiquement](#) du Bouclier résident est activée).
- **Afficher des notifications dans la barre d'état système concernant l'[analyse](#) (activé par défaut)** - indiquez s'il faut afficher les informations sur le lancement automatique de l'analyse programmée, sa progression et ses résultats.
- **Afficher les notifications sur le [Pare-feu](#) dans la barre d'état (activé par défaut)** - Décidez si les informations concernant les processus et le statut du [Pare-feu](#) (par exemple, les avertissements sur l'activation/la désactivation d'un composant, les éventuels goulets d'étranglement, etc.) doivent être affichées. Deux autres options spécifiques sont disponibles dans cet élément (pour une description détaillée de chacune d'entre elles, consultez le chapitre [Pare-feu](#) de ce document) :
  - **Afficher les notifications sur les changements de profil (activé par défaut)** – Vous informe des changements automatiques de profil du [Pare-feu](#).
  - **Afficher les notifications sur les règles de nouvelle application créées (désactivé par défaut)** – Vous informe de la création automatique de règles de [Pare-feu](#) pour de nouvelles applications sur la base d'une liste sûre.
- **Afficher les notifications sur le [Scanner e-mail](#) dans la barre d'état (activé par défaut)** – Indiquez s'il faut afficher les informations sur l'analyse de tous les messages entrants et sortants.
- **Afficher les informations statistiques (activé par défaut)** – Laissez l'option cochée pour permettre l'affichage régulier d'informations statistiques dans la barre des tâches .
- **Afficher les notifications sur AVG Accelerator dans la barre d'état (activé par défaut)** - Décidez si les informations sur les activités d'**AVG Accelerator** doivent être affichées. **AVG Accelerator** est un service qui permet une lecture vidéo en ligne plus fluide et qui facilite les téléchargements supplémentaires.
- **Afficher les notifications d'AVG Advice sur les performances (activé par défaut)** - **AVG Advice** examine les performances des navigateurs Internet pris en charge (*Internet Explorer, Chrome, Firefox, Opera et Safari*) et vous informe lorsqu'un navigateur dépasse la quantité de mémoire recommandée. Dans pareil cas, cela peut avoir pour effet de ralentir considérablement les performances de votre ordinateur et il est conseillé de redémarrer le navigateur Internet afin d'accélérer les processus. Laissez l'élément **Afficher les notifications d'AVG Advice sur les performances** activé pour recevoir cette information.

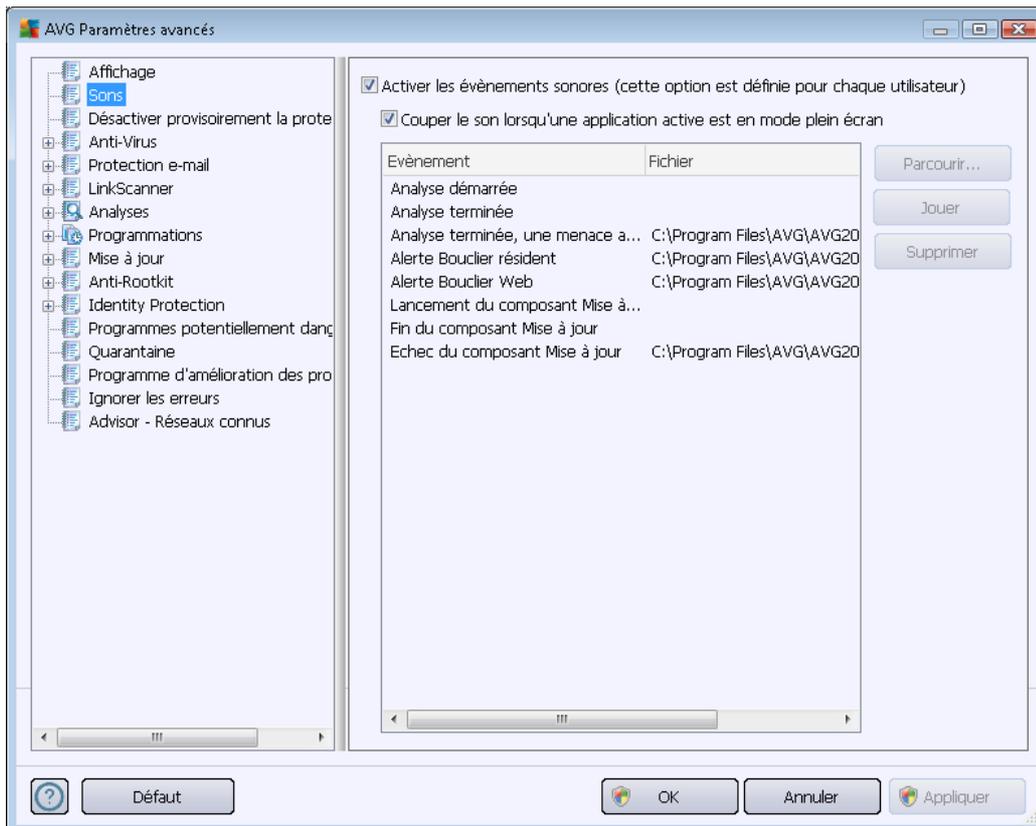


## Mode jeu

Cette fonction est conçue pour des applications plein écran pour lesquelles les éventuelles notifications d'information AVG (*qui s'affichent après le démarrage d'une analyse programmée*) seraient perturbantes (*elles risquent de réduire l'application ou de corrompre les images*). Pour éviter ce type de problème, il est recommandé de cocher la case **Activer le mode jeu lorsqu'une application est exécutée en mode plein écran** (paramètre par défaut).

## 10.2. Sons

La boîte de dialogue **Sons** vous permet d'indiquer si vous souhaitez ou non qu'une notification sonore vous signale certaines actions d'**AVG Internet Security 2012**.



Ces paramètres concernent uniquement l'utilisateur actuel. Autrement dit, chaque utilisateur de l'ordinateur peut définir ses propres paramètres audio. Pour autoriser les notifications sonores, cochez l'option **Activer les événements sonores** (*option activée par défaut*) pour activer la liste d'actions correspondantes. Par ailleurs, vous pouvez activer l'option **Couper le son lorsqu'une application active est en mode plein écran** afin de supprimer les notifications sonores susceptibles de vous déranger (*voir aussi la section Mode jeu du chapitre [Paramètres avancés/Affichage](#) de ce document*).

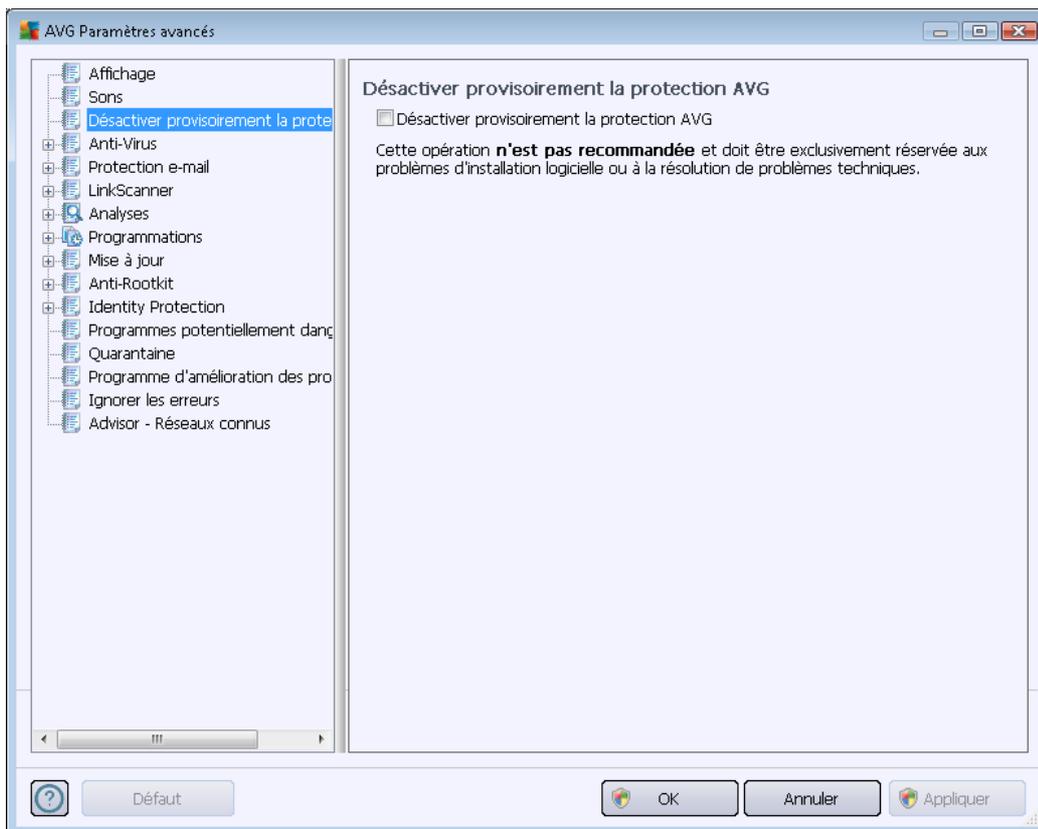
### Boutons de commande

- **Parcourir** – Après avoir sélectionné un évènement dans la liste, cliquez sur le bouton **Parcourir** pour rechercher dans votre disque le fichier audio à lui associer. (*Notez que seuls les sons \*.wav sont pris en charge pour l'instant !*)
- **Jouer** – Pour écouter le son sélectionné, mettez en surbrillance l'évènement dans la liste, puis cliquez sur le bouton **Jouer**.
- **Supprimer** – Cliquez sur ce bouton pour supprimer le son associé à un évènement.

### 10.3. Désactiver provisoirement la protection AVG

Dans la boîte de dialogue **Désactiver provisoirement la protection AVG**, vous avez la possibilité de désactiver entièrement la protection offerte par le programme **AVG Internet Security 2012**.

**Rappelez-vous que vous ne devez utiliser cette option qu'en cas d'absolue nécessité !**



Dans la plupart des cas, **il est déconseillé** de désactiver **AVG Internet Security 2012** avant d'installer un nouveau logiciel ou pilote, même si l'assistant d'installation ou le logiciel vous suggère d'arrêter d'abord tous les programmes et applications s'exécutant sur le système et qui pourraient créer des interruptions inopinées lors du processus d'installation. En cas de problème lors de l'installation, commencez par [désactiver la protection résidente](#) (*Activer le Bouclier résident*). Si vous êtes amené à désactiver **AVG Internet Security 2012**, vous devez le réactiver dès la fin de vos opérations. Si vous êtes connecté à Internet ou à un réseau alors que l'antivirus est désactivé, l'ordinateur est particulièrement vulnérable.

#### Désactivation de la protection AVG

- Cochez la case **Désactiver provisoirement la protection AVG**, puis cliquez sur **Appliquer** pour confirmer votre choix
- Dans la nouvelle boîte de dialogue **Désactiver provisoirement la protection AVG**, indiquez la durée de la désactivation d'**AVG Internet Security 2012**. Par défaut, la



protection est désactivée pendant 10 minutes, ce qui vous laisse suffisamment de temps pour effectuer les manipulations courantes (l'installation d'un nouveau logiciel, par exemple). Notez que le délai maximum pouvant être défini est de 15 minutes et ne peut pas être remplacé par une autre valeur pour des raisons de sécurité. A la fin de la durée spécifiée, tous les composants désactivés sont automatiquement réactivés.

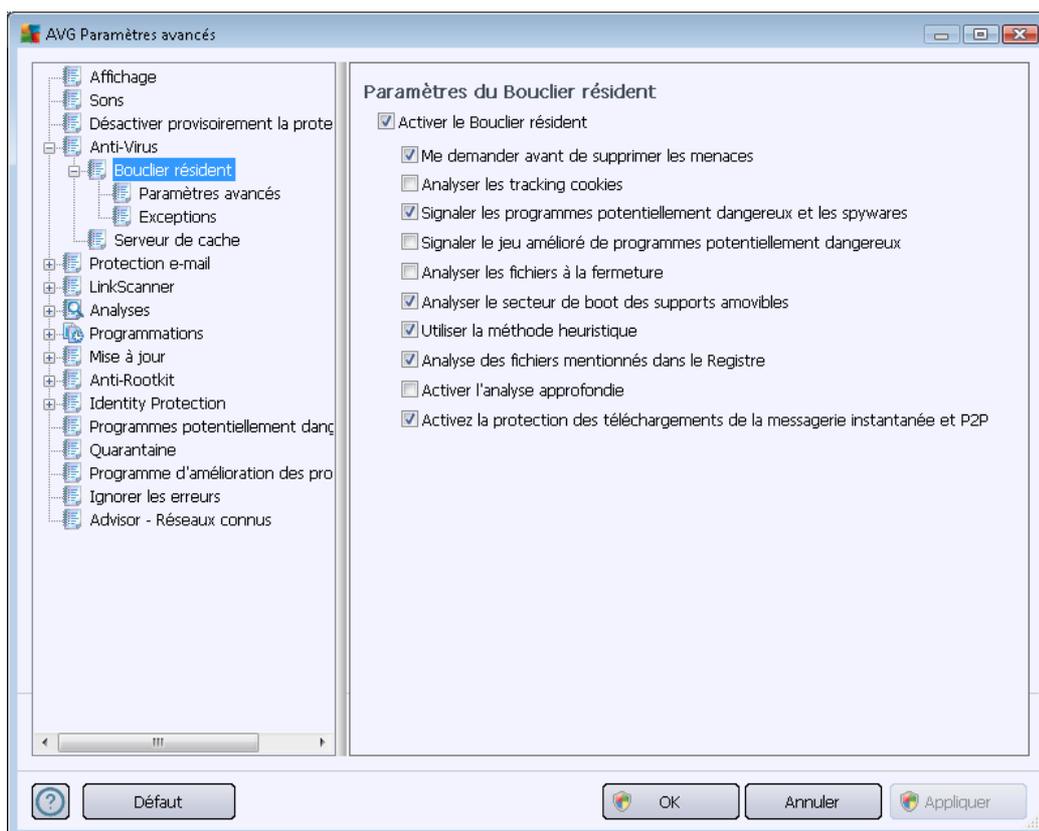


#### 10.4. Anti-Virus

Le composant **Anti-Virus** protège en permanence votre ordinateur de tous les types de virus et spywares connus (*y compris des programmes malveillants dits dormants et inactifs, c'est-à-dire téléchargés mais pas encore activés*).

### 10.4.1. Bouclier résident

Le Bouclier résident protège en temps réel les fichiers et les dossiers contre les virus, les spywares et autres codes malicieux.



Dans la boîte de dialogue **Paramètres du Bouclier résident**, il est possible d'activer ou de désactiver la protection résidente en cochant ou en désélectionnant la case **Activer le Bouclier résident** (cette option est activée par défaut). En outre, vous pouvez sélectionner les options de protection résidente à activer :

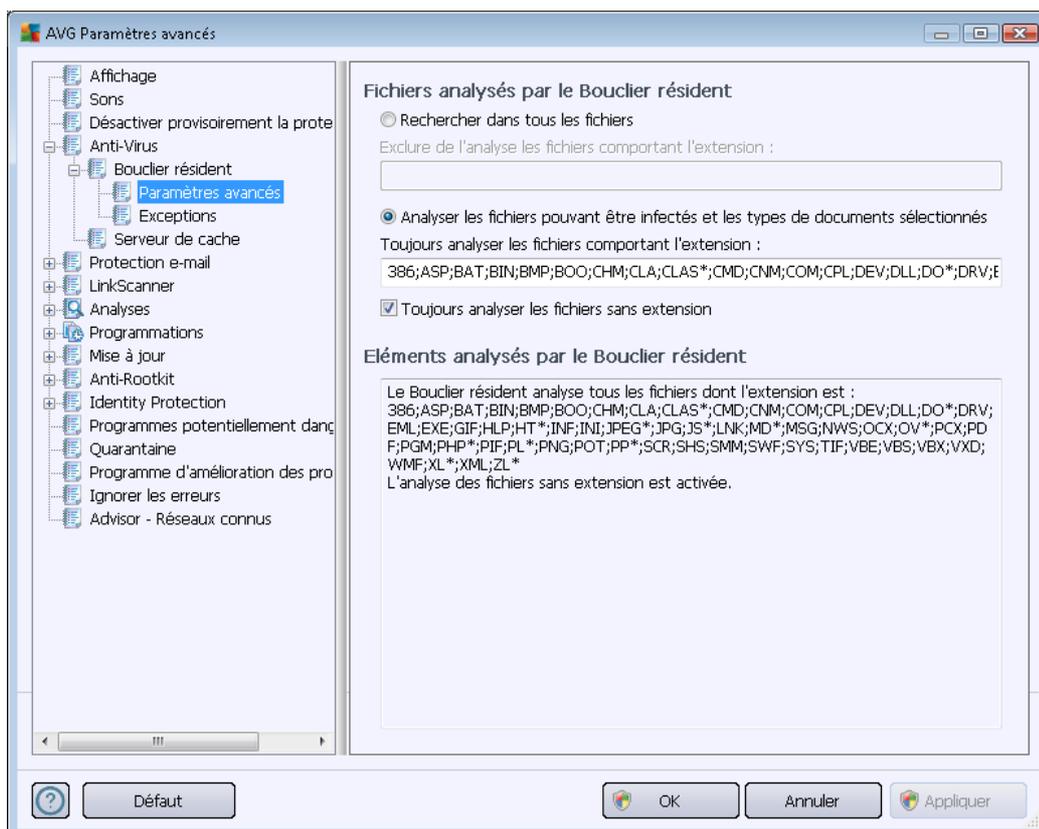
- **Me demander avant de supprimer les menaces** (activée par défaut) : cochez cette case pour vous assurer que le Bouclier résident n'exécutera aucune action automatiquement. Il affichera plutôt une boîte de dialogue décrivant la menace identifiée, vous permettant de décider de l'action à effectuer. Si vous n'avez pas coché la case, **AVG Internet Security 2012** réparera automatiquement l'infection et, si ce n'est pas possible, l'objet sera mis en [quarantaine](#).
- **Analyser les tracking cookies** (option désactivée par défaut) : ce paramètre définit les cookies à détecter au cours de l'analyse. (Les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs telles que leurs préférences en matière de site ou encore le contenu de leur panier d'achat électronique.)
- **Signaler les programmes potentiellement dangereux et les spywares** (option activée par défaut) : cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. [Les spywares](#) désignent une catégorie de codes suspects : même



s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre ordinateur.

- **Signaler le jeu amélioré de programmes potentiellement dangereux** (*option désactivée par défaut*) : permet de détecter le jeu étendu des [spywares](#) qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisés à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.
- **Analyser les fichiers à la fermeture** (*option désactivée par défaut*) : ce type d'analyse garantit qu'AVG vérifie les objets actifs (par exemple, les applications, les documents...) à leur ouverture et à leur fermeture. Cette fonction contribue à protéger l'ordinateur contre certains types de virus sophistiqués.
- **Analyser le secteur de boot des supports amovibles** – (*option activée par défaut*)
- **Utiliser la méthode heuristique** (*option activée par défaut*) : [l'analyse heuristique](#) est un moyen de détection (*émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*).
- **Analyse des fichiers mentionnés dans le Registre** (*option activée par défaut*) : ce paramètre indique qu'AVG analyse les fichiers exécutables ajoutés au registre de démarrage pour éviter l'exécution d'une infection connue au démarrage suivant de l'ordinateur.
- **Activer l'analyse approfondie** (*option désactivée par défaut*) : dans certains cas (*urgence*), vous pouvez cocher cette case afin d'activer les algorithmes les plus rigoureux qui examineront au peigne fin tous les objets représentant de près ou de loin une menace. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Activer la protection de Messagerie Instantanée et des téléchargements P2P** (*option activée par défaut*) : cochez cette option pour vérifier que les communications via la messagerie instantanée (*par exemple, ICQ, MSN Messenger, ...*) et les téléchargements P2P ne sont pas infectés par des virus.

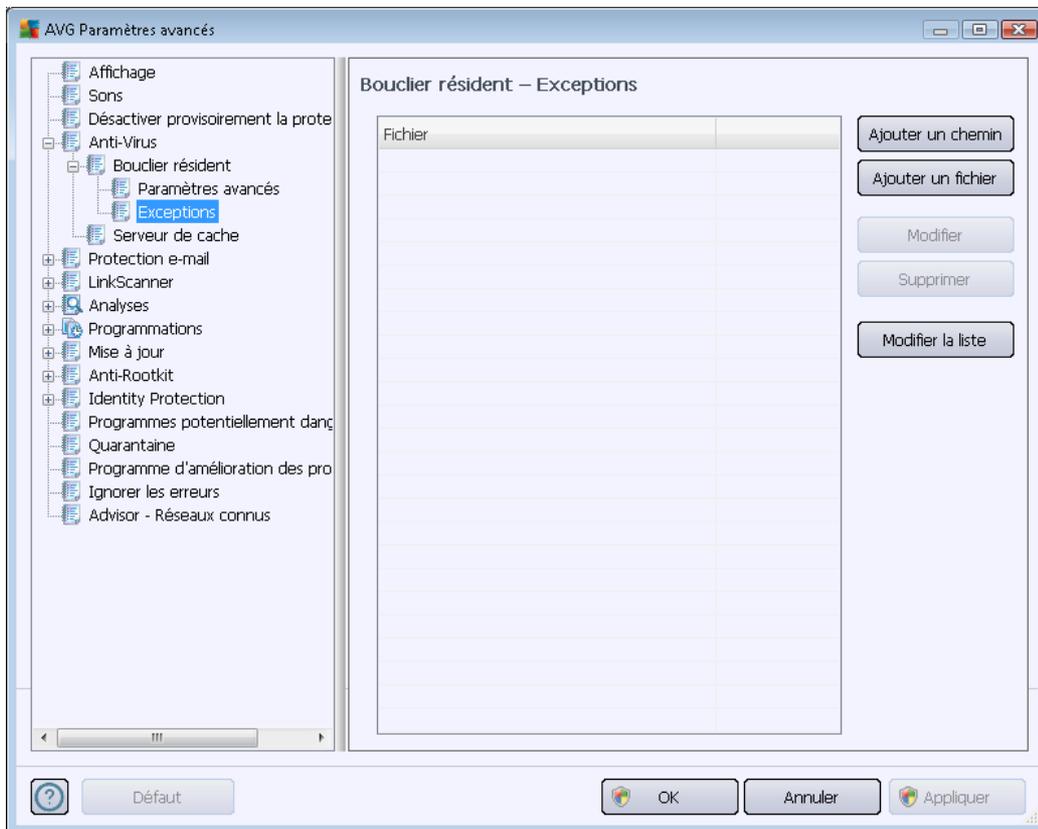
Dans la boîte de dialogue **Fichiers analysés par le Bouclier résident**, il est possible de spécifier les fichiers à analyser (*en fonction de leurs extensions*) :



Cochez la case correspondante pour décider si vous voulez **Rechercher dans tous les fichiers** ou **Analyser les fichiers pouvant être infectés et les types de documents sélectionnés**. Si vous choisissez cette dernière option, vous pouvez également définir une liste d'extensions indiquant les fichiers qui doivent être exclus de l'analyse, ainsi qu'une liste d'extensions définissant les fichiers devant absolument être analysés.

Cochez la case **Toujours analyser les fichiers sans extension** (*activée par défaut*) pour vous assurer que les fichiers sans extension et dont le format est inconnu sont également analysés par le Bouclier Résident. Nous vous recommandons de garder activée cette fonction, car les fichiers dépourvus d'extension sont suspects.

La section en dessous appelée **Eléments analysés par le Bouclier résident** récapitule les paramètres actuels et donne des informations détaillées sur les éléments examinés par le **Bouclier résident**.



La boîte de dialogue **Bouclier résident – Eléments exclus** offre la possibilité de définir les dossiers à exclure de l'analyse effectuée par le **Bouclier résident**.

**Il est vivement recommandé de n'exclure aucun fichier, sauf en cas d'absolue nécessité !**

### Boutons de commande

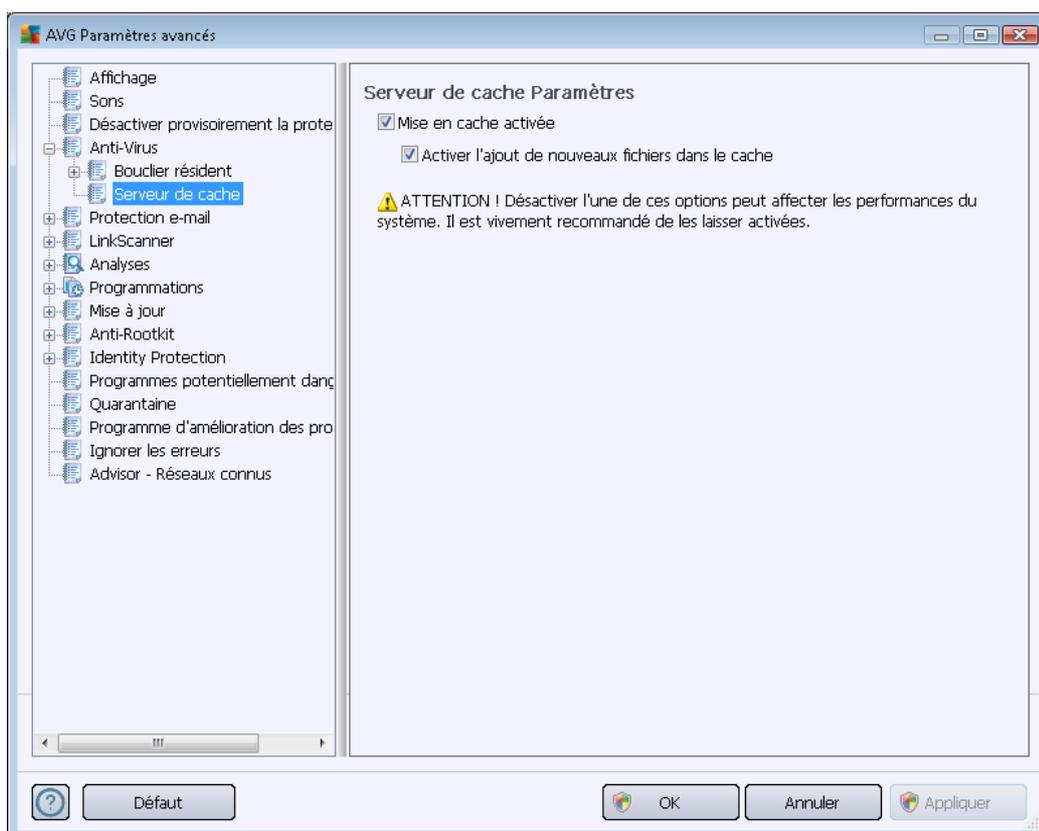
Cette boîte de dialogue présente les boutons de fonction suivantes :

- **Ajouter un chemin** – ce bouton permet de spécifier un répertoire ou des répertoires que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- **Ajouter un fichier** – ce bouton permet de spécifier les fichiers que vous souhaitez exclure de l'analyse en les sélectionnant un à un dans l'arborescence de navigation du disque local
- **Modifier** – ce bouton permet de modifier le chemin d'accès à un fichier ou dossier sélectionné
- **Supprimer** – ce bouton permet de supprimer le chemin d'accès à un objet sélectionné dans la liste

- **Modifier la liste** – permet de modifier l'ensemble de la liste des exceptions définies dans une nouvelle boîte de dialogue qui fonctionne comme un éditeur de texte standard

### 10.4.2. Serveur de cache

La boîte de dialogue **Paramètres du serveur de cache** porte sur le processus de serveur de cache, qui est conçu pour accélérer tous les types d'analyse par **AVG Internet Security 2012** :



Le serveur de cache recueille et conserve les informations relatives aux fichiers fiables (*un fichier est considéré comme fiable s'il comporte une signature numérique provenant d'une source fiable*). Par la suite, ces fichiers sont automatiquement considérés comme étant fiables et ne sont pas analysés de nouveau ; ils sont donc ignorés lors des analyses.

La boîte de dialogue **Paramètres du serveur de cache** comporte les options de configuration suivantes :

- **Mise en cache activée** (*option activée par défaut*) – désélectionnez la case pour désactiver le **serveur de cache** et videz la mémoire de mise en cache. Notez que l'analyse risque de durer plus longtemps et que les performances de l'ordinateur risquent d'être diminuées étant donné que chaque fichier en cours d'utilisation fera d'abord l'objet d'une analyse anti-virale et anti-spyware préalable.
- **Activer l'ajout de nouveaux fichiers dans le cache** (*option activée par défaut*) – désélectionnez la case pour mettre fin à l'ajout de fichiers dans la mémoire cache. Tout



fichier déjà mis en cache sera conservé et utilisé jusqu'à ce que la mise en cache soit complètement désactivée ou jusqu'à la prochaine mise à jour de la base de données virale.

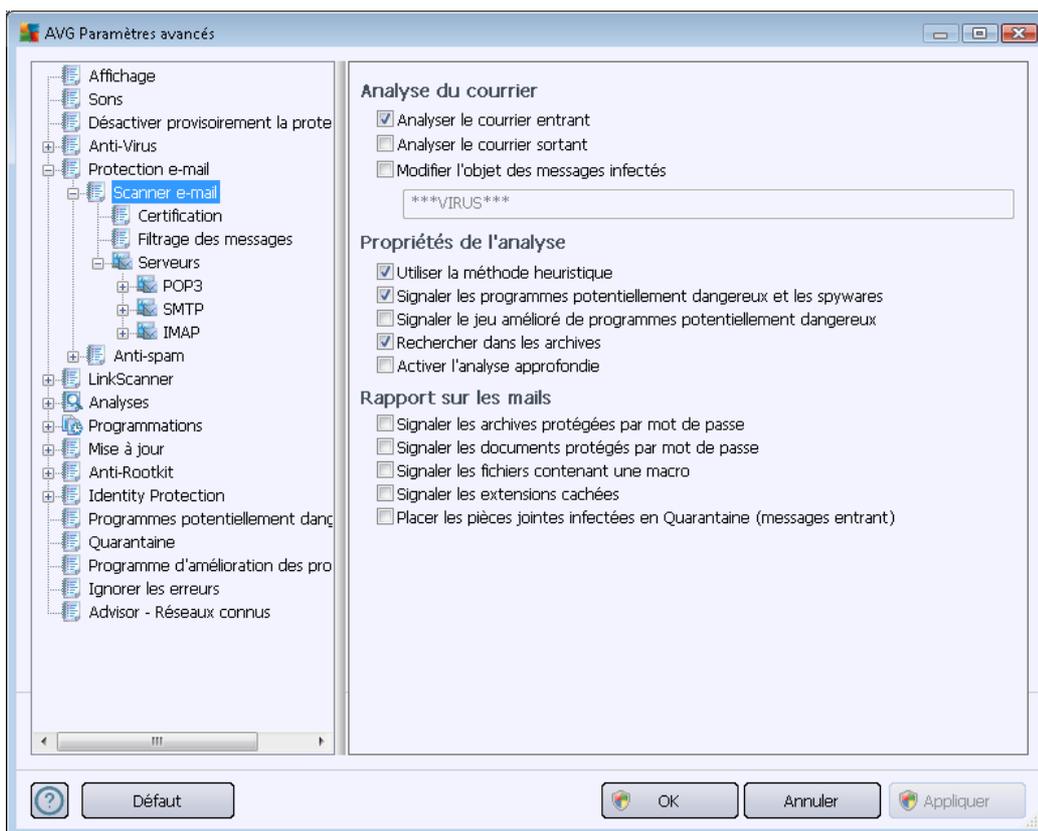
***A moins que vous n'ayez une très bonne raison de désactiver le serveur de cache, nous vous conseillons fortement de conserver les paramètres par défaut et de laisser les deux options activées ! Si vous ne le faites pas, vous risqueriez de subir une baisse de la vitesse et des performances du système.***

## 10.5. Protection e-mail

Dans la section **Protection e-mail**, vous pouvez modifier de manière approfondie la configuration des composants [E-mail Scanner](#) et [Anti-Spam](#) :

### 10.5.1. Scanner e-mail

La boîte de dialogue **Scanner e-mail** comporte trois parties :



#### Analyse du courrier

Dans cette section, vous définissez la configuration standard des messages entrants et/ou sortants :

- **Analyser le courrier entrant** (option activée par défaut) – cette option permet d'activer ou de désactiver l'analyse des e-mails remis à votre client de messagerie



- **Analyser le courrier sortant** (*option désactivée par défaut*) – cette option permet d'activer ou de désactiver l'analyse des e-mails envoyés par votre compte
- **Modifier l'objet des messages infectés** (*option désactivée par défaut*) – si vous voulez être averti que le message est infecté, cochez cette case et indiquez le texte à afficher dans le champ prévu à cet effet. Ce texte sera alors inséré dans l'objet de chaque mail infecté, pour une identification et un filtrage plus faciles. Nous vous recommandons de conserver la valeur par défaut : **\*\*\*VIRUS\*\*\***.

### Propriétés de l'analyse

Dans cette section, vous choisissez les modalités de l'analyse des messages :

- **Utiliser la méthode heuristique** (*option activée par défaut*) – cochez cette option pour appliquer la méthode heuristique à l'analyse des messages. Lorsque cette option est active, vous pouvez filtrer les pièces jointes, non seulement selon leur extension, mais aussi selon leur contenu. Le filtrage peut être défini dans la boîte de dialogue [Filtrage des messages](#).
- **Signaler les programmes potentiellement dangereux et les spywares** (*option activée par défaut*) : cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. [Les spywares](#) désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre ordinateur.
- **Signaler le jeu amélioré de programmes potentiellement dangereux** – (*option désactivée par défaut*) : permet de détecter le jeu étendu des [spywares](#) qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.
- **Rechercher dans les archives** (*option activée par défaut*) – cochez la case pour analyser le contenu des archives jointes aux messages.
- **Activer l'analyse approfondie** (*option désactivée par défaut*) – dans certains cas (*exemple : suspicion de présence d'un virus ou d'un exploit sur l'ordinateur*) vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.

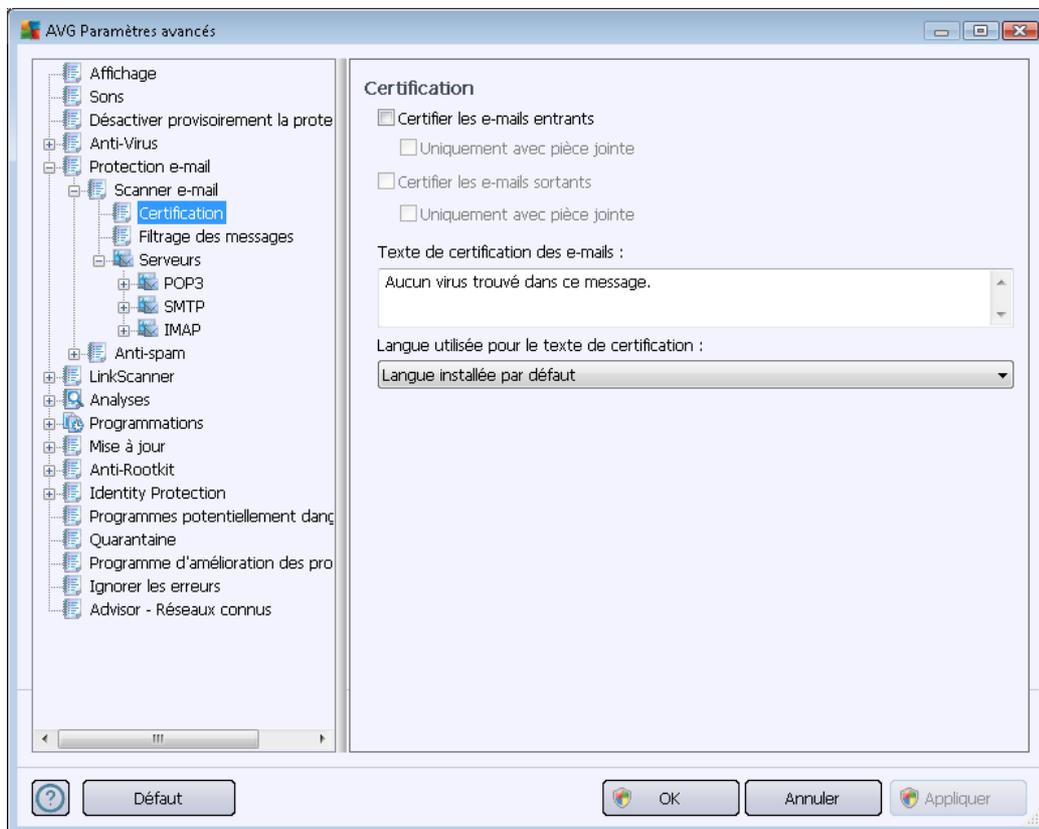
### Signalisation des pièces jointes

Dans cette section, vous pouvez définir des rapports supplémentaires sur les fichiers potentiellement dangereux ou suspects. Notez qu'aucun avertissement ne sera affiché, seul un texte de certification sera ajouté à la fin du message et tous les rapports associés seront recensés dans la boîte de dialogue [Détection du scanner e-mail](#).



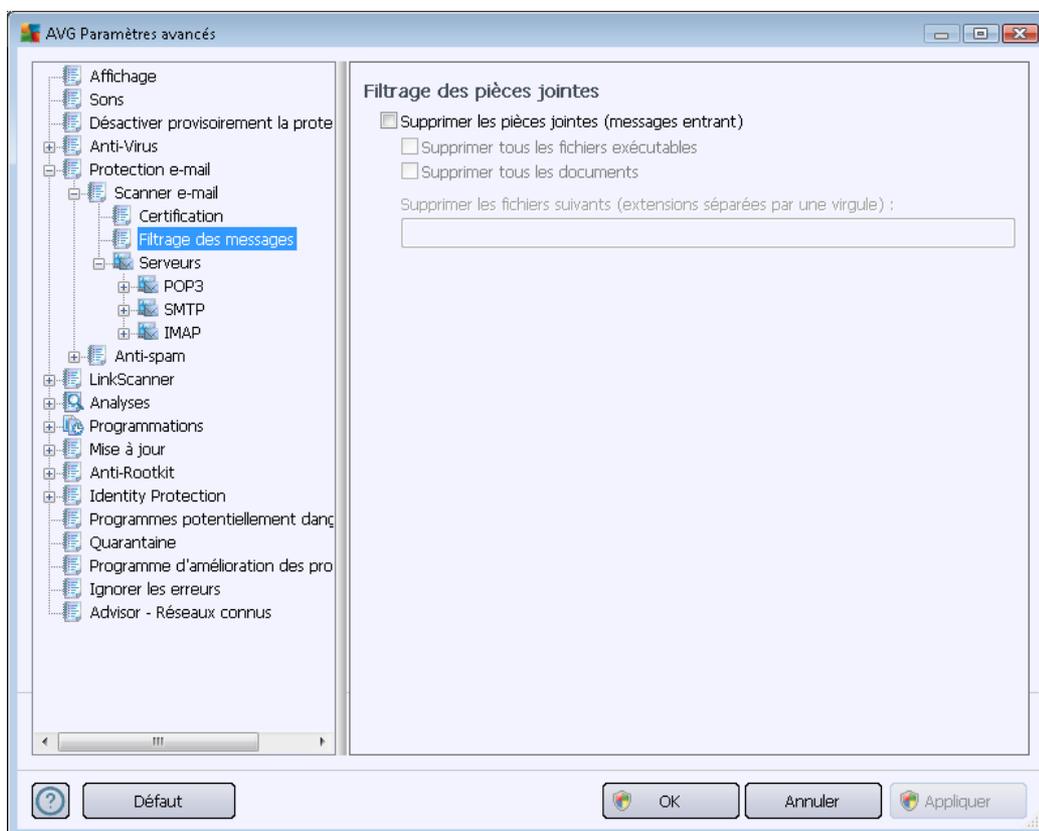
- **Signaler les archives protégées par mot de passe** – archives (ZIP, RAR, etc.) qui sont protégées par mot de passe et qui, à ce titre, ne peuvent pas faire l'objet d'une recherche de virus. Cochez cette case pour les signaler comme étant potentiellement dangereuses.
- **Signaler les documents protégés par mot de passe** – les documents protégés par mot de passe ne peuvent pas faire l'objet d'une recherche de virus. Cochez cette case pour les signaler comme étant potentiellement dangereux.
- **Signaler les fichiers contenant une macro** – Une macro est une séquence prédéfinie d'étapes destinées à faciliter certaines tâches pour l'utilisateur (*les macros MS Word en sont un exemple bien connu*). A ce titre, une macro peut contenir des instructions potentiellement dangereuses. Vous pouvez cocher cette case pour garantir que les fichiers contenant des macros seront signalés comme suspects.
- **Signaler les extensions cachées** : masquer les extensions qui peuvent présenter un fichier exécutable suspect "objet.txt.exe" sous la forme d'un fichier texte "objet.txt" inoffensif. Cochez cette case pour signaler ces fichiers comme étant potentiellement dangereux.
- **Placer les pièces jointes signalées dans Quarantaine** – indiquez si vous voulez être averti par e-mail lorsque l'analyse d'un e-mail révèle la présence d'une archive protégée par mot de passe, d'un document protégé par mot de passe, d'une macro contenant un fichier et/ou d'un fichier dont l'extension est masquée. En l'occurrence, définissez si l'objet détecté doit être placé en [quarantaine](#).

Dans la boîte de dialogue **Certification**, vous pouvez cocher des cases spécifiques pour décider si vous voulez certifier vos messages entrants (**Certifier les messages entrants**) et/ou vos messages sortants (**Certifier les messages sortants**). Pour chacune de ces options, vous pouvez en outre définir le paramètre **Avec pièces jointes uniquement** afin que la certification ne concerne que les messages électroniques comportant une pièce jointe :



Par défaut, le texte de certification consiste en un message simple indiquant qu'*Aucun virus n'a été détecté dans ce message*. Cependant, il est possible de développer ou de modifier cette information en fonction de vos besoins : rédigez le texte de certification de votre choix dans le champ **Texte de certification des messages électroniques**. Dans la section **Langue utilisée pour le texte de certification des messages électroniques**, vous pouvez en outre définir la langue dans laquelle la partie automatiquement générée de la certification (*Aucun virus n'a été détecté dans ce message*) doit être affichée.

**Remarque :** Retenez que seul le texte par défaut sera affiché dans la langue choisie, mais votre texte personnalisé ne sera pas traduit automatiquement !



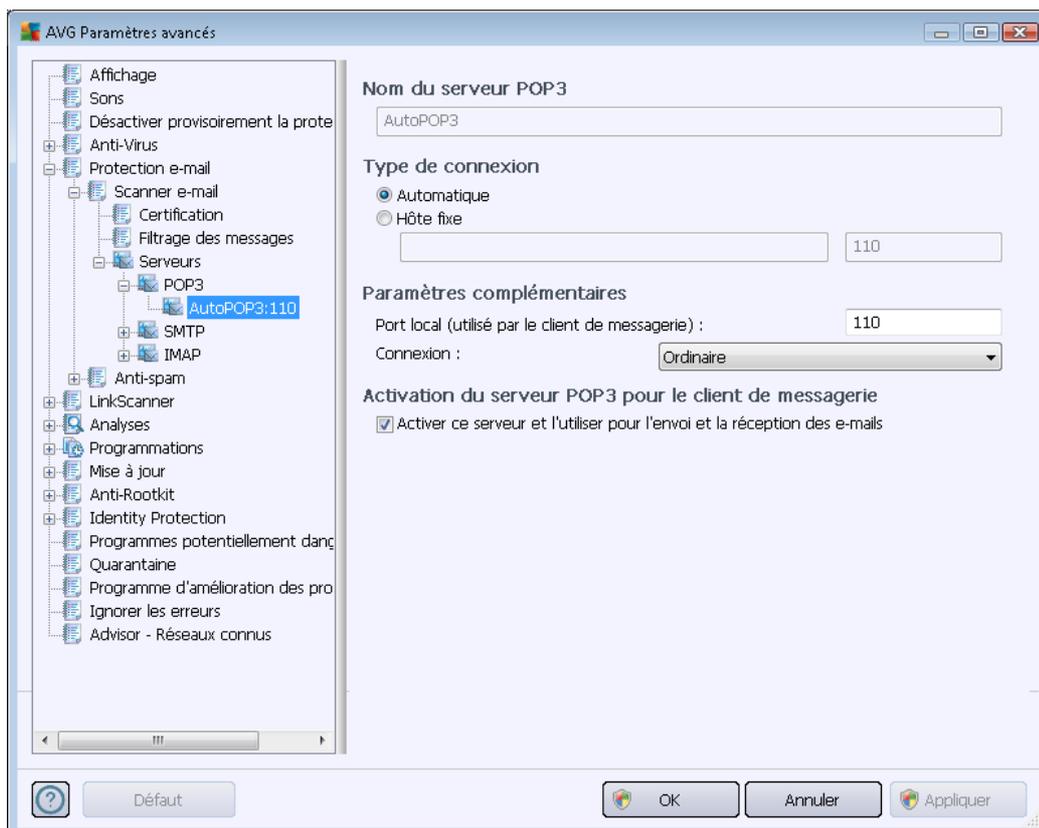
La boîte de dialogue **Filtrage des pièces jointes** est destinée à vous aider à définir les paramètres de l'analyse des pièces jointes aux mails. Par défaut, l'option **Supprimer les pièces jointes** est désactivée. Si vous décidez de l'activer, toutes les pièces jointes signalées comme infectées ou potentiellement dangereuses sont automatiquement supprimées. Pour définir explicitement les types de pièces jointes à supprimer, sélectionnez l'option correspondante :

- **Supprimer tous les fichiers exécutables** – tous les fichiers \*.exe seront supprimés
- **Supprimer tous les documents** - tous les fichiers \*.doc, \*.docx, \*.xls, \*.xlsx seront supprimés
- **Supprimer les fichiers comportant les extensions suivantes séparées par une virgule** – indiquez toutes les extensions de fichier correspondant aux fichiers à supprimer

La section **Serveurs** permet de modifier les paramètres des serveurs du [Scanner e-mail](#) servers.

- [Serveur POP3](#)
- [Serveur SMTP](#)
- [Serveur IMAP](#)

De même, vous pouvez définir un nouveau serveur pour le courrier entrant ou sortant à l'aide du bouton **Ajouter un nouveau serveur**.

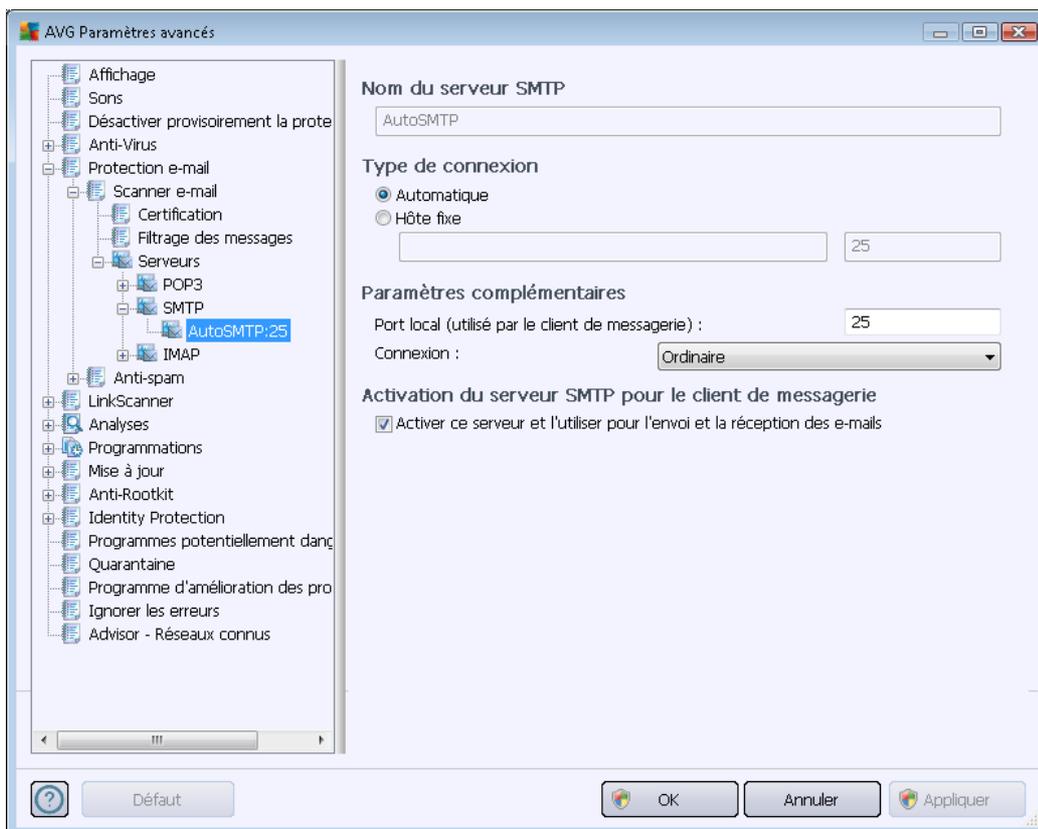


Dans cette boîte de dialogue (*accessible depuis la commande **Serveurs / POP3***), vous configurez un nouveau serveur **Scanner e-mail** à l'aide du protocole POP3 pour les messages entrants :

- **Nom du serveur POP3** – dans ce champ, vous pouvez spécifier le nom des serveurs récemment ajoutés (*pour ajouter un serveur POP3, cliquez avec le bouton droit sur l'option POP3 du menu de navigation gauche*). Dans le cas d'un serveur créé automatiquement (serveur "AutoPOP3"), ce champ est désactivé.
- **Type de connexion** – définissez la méthode de sélection du serveur de messagerie pour les mails entrants.
  - **Automatique** - la connexion est établie automatiquement selon les paramètres du client de messagerie.
  - **Hôte fixe** – Dans ce cas, le programme utilise toujours le serveur spécifié dans ce champ. Veuillez indiquer l'adresse ou le nom de votre serveur de messagerie. Le nom de connexion reste inchangé. En guise de nom, vous pouvez utiliser un nom de domaine (*pop.acme.com, par exemple*) ainsi qu'une adresse IP (*123.45.67.89, par exemple*). Si le serveur de messagerie fait appel à un port non standard, il est possible de spécifier ce port à la suite du nom du serveur en séparant ces éléments

par le signe deux-points (*pop.acme.com:8200, par exemple*). Le port standard des communications POP3 est le port 110.

- **Paramètres complémentaires** – se rapporte à des paramètres plus détaillés :
  - **Port local** – indique le port sur lequel transitent les communications provenant de l'application de messagerie. Dans votre programme de messagerie, vous devez alors indiquer que ce port fait office de port de communication POP3.
  - **Connexion** – dans la liste déroulante, vous pouvez spécifier le type de connexion à utiliser (*Ordinaire/SSL/SSL par défaut*). Si vous optez pour une connexion SSL, les données sont envoyées sous forme cryptée, sans risquer d'être analysées ou contrôlées par une tierce partie. Cette fonction également n'est disponible que si elle est prise en charge par le serveur de messagerie de destination.
- **Activation du serveur POP3 pour le client de messagerie** – cochez/désélectionnez cette case pour activer ou désactiver le serveur POP3 spécifié



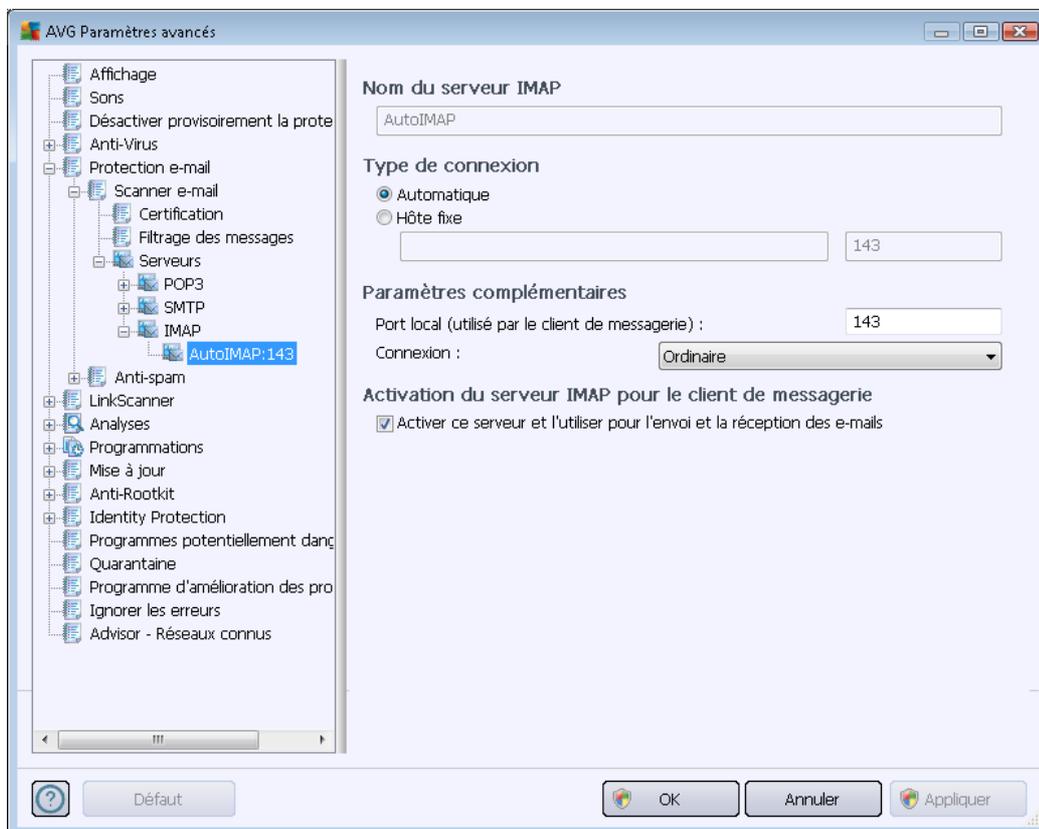
Dans cette boîte de dialogue (*ouverte grâce à la commande **Serveurs / SMTP***), vous configurez un nouveau serveur [Scanner e-mail](#) à l'aide du protocole SMTP pour les messages sortants :

- **Nom du serveur SMTP** – dans ce champ, vous pouvez spécifier le nom des serveurs récemment ajoutés (*pour ajouter un serveur SMTP, cliquez avec le bouton droit sur l'option*



SMTP du menu de navigation gauche). Dans le cas d'un serveur créé automatiquement (serveur "AutoSMTP"), ce champ est désactivé.

- **Type de connexion** – définissez la méthode de sélection du serveur de messagerie pour les mails sortants :
  - **Automatique** – la connexion est établie automatiquement selon les paramètres du client de messagerie
  - **Hôte fixe** – dans ce cas, le programme utilise toujours le serveur spécifié dans ce champ. Veuillez indiquer l'adresse ou le nom de votre serveur de messagerie. En guise de nom, vous pouvez utiliser un nom de domaine (*smtp.acme.com, par exemple*) ainsi qu'une adresse IP (*123.45.67.89, par exemple*). Si le serveur de messagerie fait appel à un port non standard, il est possible de saisir ce port à la suite du nom du serveur en séparant ces éléments par le signe deux-points (*smtp.acme.com:8200, par exemple*). Le port standard des communications SMTP est le port 25.
- **Paramètres complémentaires** – se rapporte à des paramètres plus détaillés :
  - **Port local** – indique le port sur lequel transitent les communications provenant de l'application de messagerie. Dans votre programme de messagerie, vous devez alors indiquer que ce port fait office de port de communication SMTP.
  - **Connexion** – dans la liste déroulante, vous pouvez spécifier le type de connexion à utiliser (*Ordinaire/SSL/SSL par défaut*). Si vous optez pour une connexion SSL, les données sont envoyées sous forme cryptée, sans risque d'être contrôlées ou surveillées par une tierce partie. Cette fonction n'est disponible que si elle est prise en charge par le serveur de messagerie de destination.
- **Activation du serveur SMTP pour le client de messagerie** – cochez/désélectionnez cette case pour activer ou désactiver le serveur SMTP spécifié ci-dessus

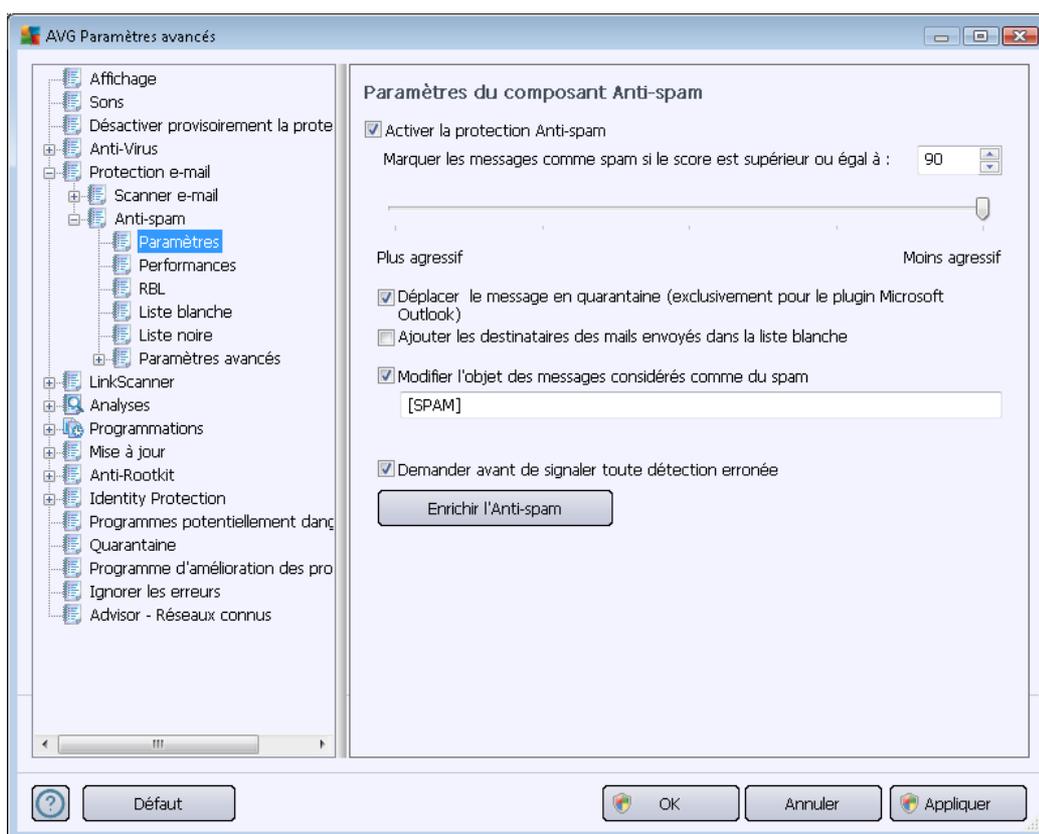


Dans cette boîte de dialogue (ouverte grâce à la commande **Serveurs / IMAP**), vous configurez un nouveau serveur **Scanner e-mail** à l'aide du protocole IMAP pour les messages sortants :

- **Nom du serveur IMAP** – dans ce champ, vous pouvez spécifier le nom des serveurs récemment ajoutés (*pour ajouter un serveur IMAP, cliquez avec le bouton droit sur l'option IMAP du menu de navigation gauche*). Dans le cas d'un serveur créé automatiquement (serveur "AutoIMAP"), ce champ est désactivé.
- **Type de connexion** – définissez la méthode de sélection du serveur de messagerie pour les mails sortants :
  - **Automatique** – la connexion est établie automatiquement selon les paramètres du client de messagerie
  - **Hôte fixe** – dans ce cas, le programme utilise toujours le serveur spécifié dans ce champ. Veuillez indiquer l'adresse ou le nom de votre serveur de messagerie. En guise de nom, vous pouvez utiliser un nom de domaine (*smtp.acme.com, par exemple*) ainsi qu'une adresse IP (*123.45.67.89, par exemple*). Si le serveur de messagerie fait appel à un port non standard, il est possible de saisir ce port à la suite du nom du serveur en séparant ces éléments par le signe deux-points (*imap.acme.com:8200, par exemple*). Le port standard des communications IMAP est le port 143.

- **Paramètres complémentaires** – se rapporte à des paramètres plus détaillés :
  - **Port local** – indique le port sur lequel transitent les communications provenant de l'application de messagerie. Vous devez alors indiquer, dans votre programme de messagerie, que ce port sert pour les communications IMAP.
  - **Connexion** – dans la liste déroulante, vous pouvez spécifier le type de connexion à utiliser (*Ordinaire/SSL/SSL par défaut*). Si vous optez pour une connexion SSL, les données sont envoyées sous forme cryptée, sans risque d'être contrôlées ou surveillées par une tierce partie. Cette fonction n'est disponible que si elle est prise en charge par le serveur de messagerie de destination.
- **Activation du serveur IMAP pour le client de messagerie** – cochez/décochez cette case pour activer ou désactiver le serveur IMAP spécifié ci-dessus

### 10.5.2. Anti-spam



Dans la boîte de dialogue **Paramètres de base anti-spam**, désélectionnez la case **Activer la protection anti-spam** pour autoriser/interdire l'analyse anti-spam dans les communications par e-mail. Cette option est activée par défaut et comme toujours, il est recommandé de garder la configuration par défaut et de ne la changer qu'en cas d'absolue nécessité

Vous pouvez ensuite sélectionner également des mesures de contrôle plus ou moins strictes en



matière de spam. Le composant **Anti-Spam** attribue à chaque message un score (*déterminant la présence de SPAM*) éventuel, en recourant à plusieurs techniques d'analyse dynamiques. Pour régler le paramètre **Marquer les messages comme spams si le score est supérieur à**, saisissez le score qui convient ou faites glisser le curseur vers la gauche ou vers la droite (*seules les valeurs entre 50 et 90 sont acceptées*).

Il est généralement recommandé de choisir un seuil compris entre 50 et 90 et en cas de doute de le fixer à 90. Voici l'effet obtenu selon le score que vous définissez :

- **Valeur 80-90** – les messages susceptibles d'être du spam sont identifiés par le filtre. Il est possible toutefois que certains messages valides soient détectés à tort comme du spam.
- **Valeur 60-79** – ce type de configuration est particulièrement strict. Tous les messages susceptibles d'être du spam sont identifiés par le filtre. Il est fort probable que certains messages anodins soient également rejetés.
- **Valeur 50-59** – ce type de configuration est très restrictif. Les messages qui ne sont pas du spam ont autant de chances d'être rejetés que ceux qui en sont vraiment. Ce seuil n'est pas recommandé dans des conditions normales d'utilisation.

Dans la boîte de dialogue **Paramètres anti-spam**, vous pouvez aussi définir la façon dont les messages indésirables doivent être traités :

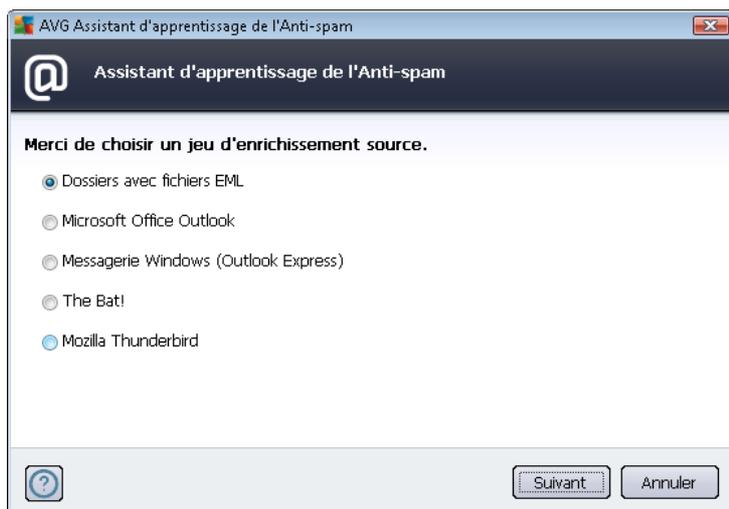
- **Mettre le message en quarantaine** (*exclusivement pour le plugin Microsoft Outlook*) – cochez cette case pour que tous les messages détectés comme du courrier indésirable soient automatiquement transférés dans le dossier des messages indésirables de votre client de messagerie MS Outlook. Cette fonction n'est actuellement pas prise en charge par d'autres clients de messagerie.
- **Ajouter les destinataires des messages envoyés dans la [liste blanche](#)** – cochez cette case pour confirmer que tous les destinataires des messages envoyés sont fiables et que tous les messages provenant de ces comptes e-mail peuvent être transmis.
- **Modifier l'objet des messages considérés comme du courrier indésirable** – cochez cette case pour signaler tous les messages détectés comme du courrier indésirable à l'aide d'un mot ou d'un caractère particulier dans l'objet du message. Le texte souhaité doit être saisi dans la zone de texte activée.
- **Demander avant de signaler toute détection erronée** – option activée si, au cours de l'[installation](#), vous avez accepté de participer au [Programme d'amélioration des produits](#). En pareil cas, vous avez autorisé le signalement des menaces détectées à AVG. La procédure de signalement est entièrement automatisée. Toutefois, vous pouvez cocher cette case pour confirmer que vous voulez être interrogé avant qu'un spam détecté soit signalé à AVG afin de vous assurer que le message en question a bien lieu d'être classé dans la catégorie du spam.

### Boutons de commande

Le bouton **Enrichir l'Anti-spam** lance l'[assistant d'enrichissement de l'anti-spam](#), décrit de façon détaillée dans le [paragraphe suivant](#).



La première boîte de dialogue de l'**Assistant d'enrichissement de l'anti-spam** vous invite à sélectionner la source des messages que vous souhaitez utiliser pour l'enrichissement. En général, vous utiliserez des mails signalés par erreur comme spam ou des messages indésirables qui n'ont pas été reconnus comme spam.



Plusieurs choix sont proposés :

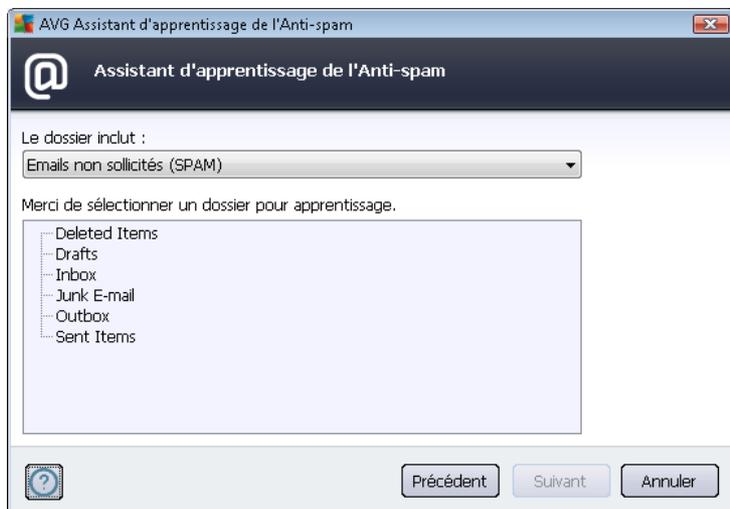
- **Un client de messagerie spécifique** – si vous utilisez un des clients répertoriés (*MS Outlook, Outlook Express, The Bat!*), sélectionnez l'option correspondante
- **Dossiers avec fichiers EML** – si vous utilisez un autre programme de messagerie, commencez par enregistrer les messages dans un dossier spécifique (*au format .eml*) ou assurez-vous que vous connaissez l'emplacement des dossiers dans lesquels sont stockés les messages du client de messagerie. Sélectionnez ensuite l'option **Dossiers avec fichiers EML**, qui permet de spécifier le dossier désiré à l'étape suivante

Pour faciliter et accélérer le processus d'enrichissement, il est judicieux de trier préalablement les mails dans les dossiers de façon à ne conserver que les messages pertinents (messages sollicités ou indésirables). Cela n'est toutefois pas absolument nécessaire car vous pourrez filtrer les messages par la suite.

Sélectionnez l'option qui convient, puis cliquez sur le bouton **Suivant** pour continuer l'assistant.

La boîte de dialogue qui s'affiche à cette étape dépend de votre précédente sélection.

### **Dossiers avec fichiers EML**



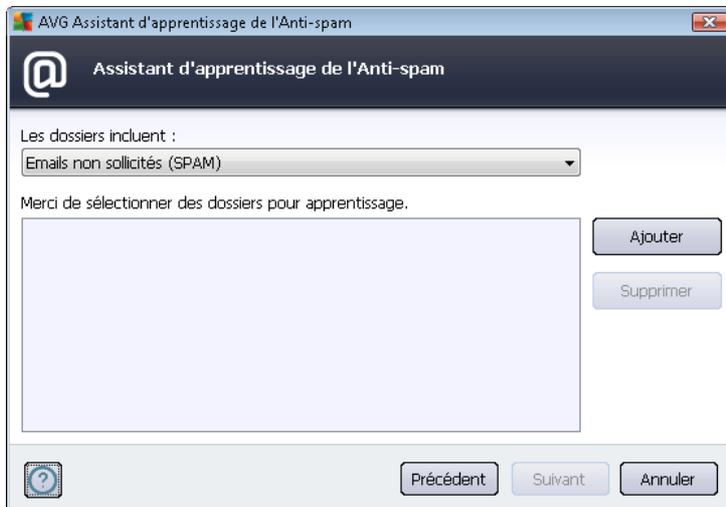
Dans cette boîte de dialogue, sélectionnez le dossier contenant les messages à utiliser pour la procédure d'enrichissement. Cliquez sur le bouton **Ajouter** pour localiser le dossier contenant les fichiers .eml (*messages e-mail enregistrés*). Le dossier sélectionné apparaît dans la boîte de dialogue.

Dans la liste déroulante **Les dossiers incluent**, choisissez l'une des deux options pour préciser si le dossier sélectionné contient des messages sollicités (*HAM*) ou des messages indésirables (*SPAM*). Notez que vous aurez la possibilité de filtrer les messages à l'étape suivante. Il n'est donc pas indispensable que le dossier contienne exclusivement des messages pertinents pour l'enrichissement de la base de données anti-spam. Vous pouvez également enlever de la liste les dossiers qui ne vous intéressent pas en cliquant sur le bouton **Supprimer**.

Une fois fait, cliquez sur **Suivant** et passez aux [options de filtrage des messages](#).

### Client de messagerie spécifique

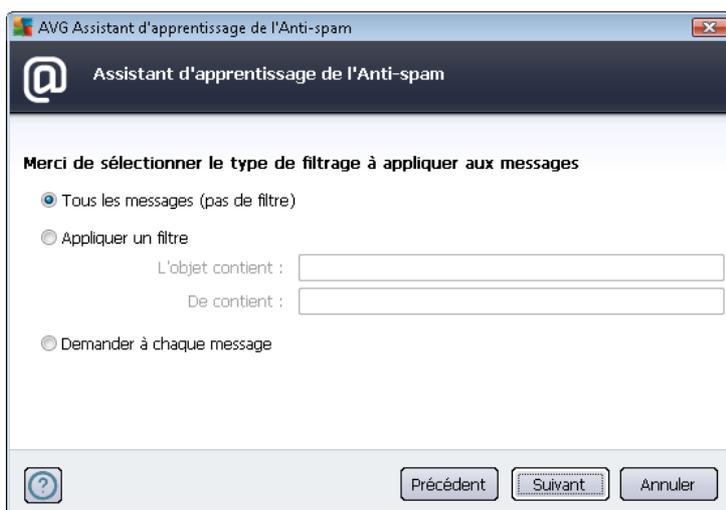
Lorsque vous avez choisi une option, une nouvelle boîte de dialogue apparaît.



**Remarque :** si vous avez opté pour Microsoft Office Outlook, vous devrez d'abord sélectionner le profil MS Office Outlook.

Dans la liste déroulante **Les dossiers incluent**, choisissez l'une des deux options pour préciser si le dossier sélectionné contient des messages sollicités (*HAM*) ou des messages indésirables (*SPAM*). Notez que vous aurez la possibilité de filtrer les messages à l'étape suivante. Il n'est donc pas indispensable que le dossier contienne exclusivement des messages pertinents pour l'enrichissement de la base de données anti-spam. L'arborescence du client de messagerie sélectionné figure déjà dans la partie centrale de la boîte de dialogue. Identifiez le dossier souhaité dans l'arborescence, et mettez-le en surbrillance à l'aide de la souris.

Cliquez ensuite sur **Suivant** et passez aux [options de filtrage des messages](#).



Dans cette boîte de dialogue, vous pouvez définir le filtrage des messages.

- **Tous les messages (sans filtrage)** – si vous êtes certain que le dossier sélectionné

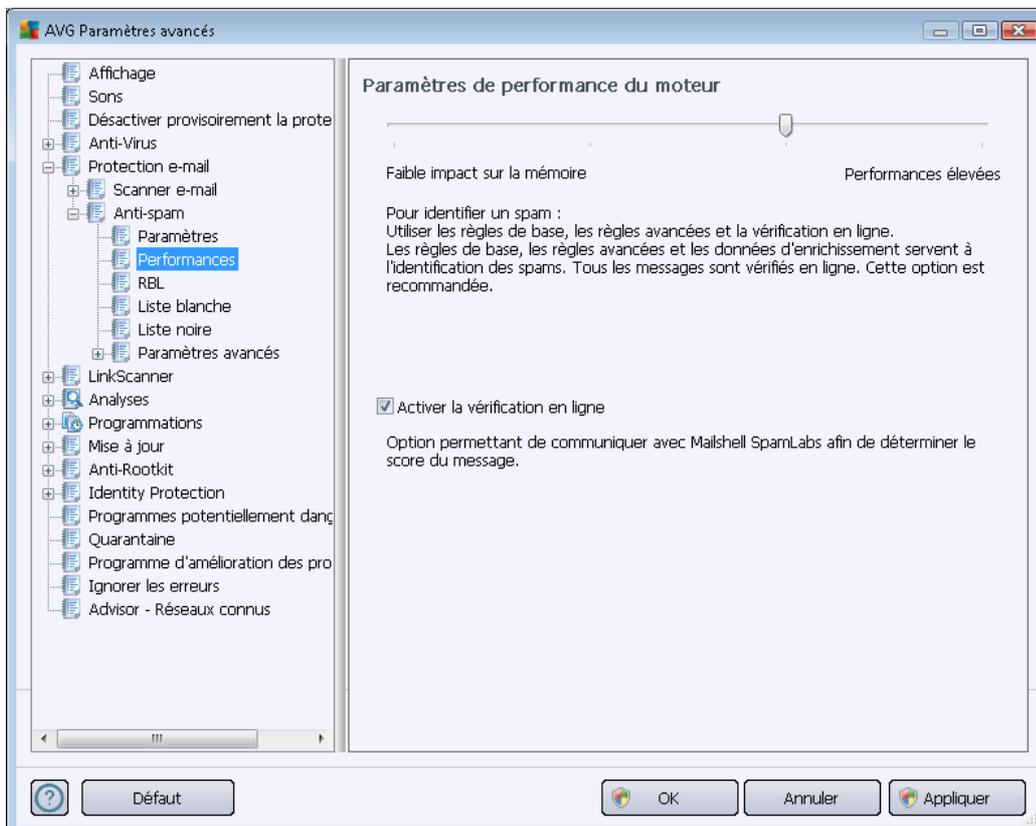


contient uniquement les messages que vous souhaitez utiliser pour l'enrichissement, sélectionnez l'option **Tous les messages (sans filtrage)**.

- **Utiliser le filtre** – pour un filtrage avancé, sélectionnez l'option **Utiliser le filtre**. Vous pouvez spécifier un mot (*nom*), une partie d'un mot ou une phrase à rechercher dans l'objet des messages et/ou dans le champ de l'expéditeur. Tous les messages correspondant exactement aux critères saisis seront utilisés pour l'enrichissement, sans autre demande de confirmation. Lorsque vous renseignez les deux zones de texte, les adresses qui correspondent à une seule des conditions sont aussi utilisées !
- **Demander à chaque message** – si vous avez des doutes quant aux messages contenus dans le dossier et que vous souhaitez que l'assistant vous invite à vous prononcer sur chaque message (*afin que vous puissiez déterminer s'il faut ou non l'utiliser dans l'enrichissement*), sélectionnez l'option **Demander à chaque message**.

Une fois l'option adéquate sélectionnée, cliquez sur **Suivant**. La boîte de dialogue suivante, fournie à titre d'information uniquement, indique que l'assistant est prêt à traiter les messages. Pour commencer l'enrichissement, cliquez de nouveau sur le bouton **Suivant**. L'enrichissement est déclenché et fonctionne selon les paramètres sélectionnés.

La boîte de dialogue **Paramètres de performance du moteur** (associée à l'entrée **Performances de l'arborescence de navigation de gauche**) présente les paramètres de performances du composant **Anti-Spam** :





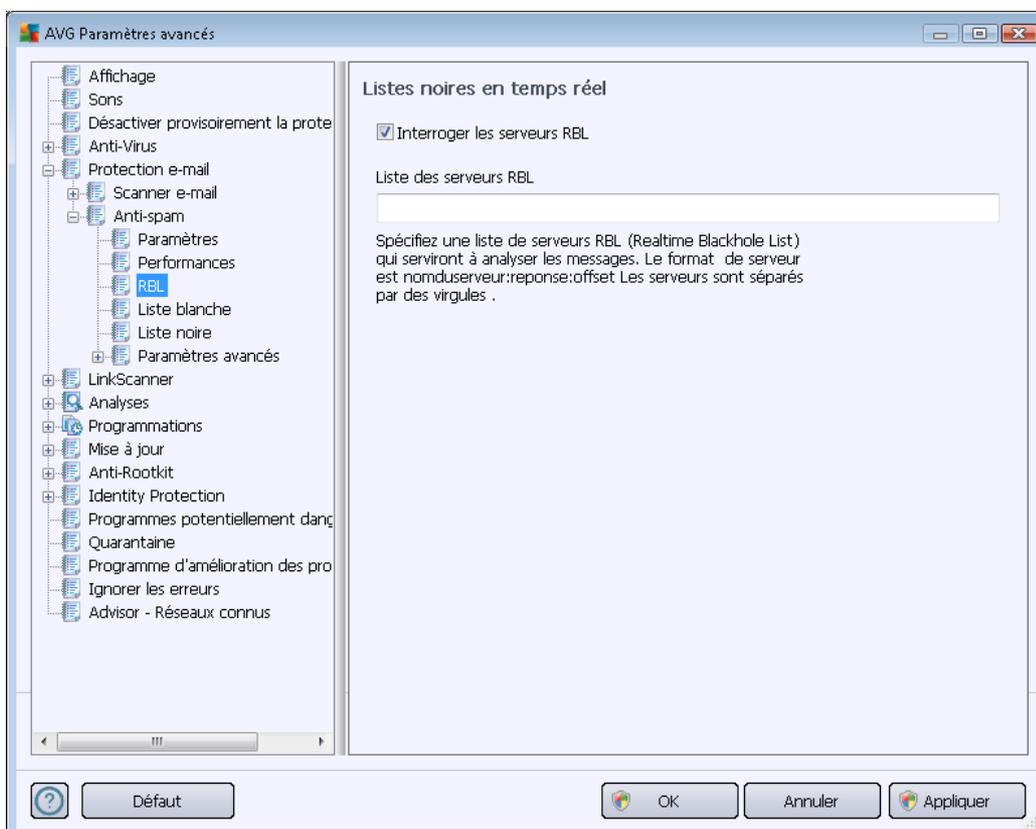
En faisant glisser le curseur vers la gauche ou la droite, vous faites varier le niveau de performances de l'analyse du mode **Faible impact sur la mémoire** au mode **Performances élevées**.

- **Faible impact sur la mémoire** – Pendant le processus d'analyse destiné à identifier le spam, aucune règle n'est appliquée. Seules les données d'enrichissement sont utilisées pour l'identification de spam. Ce mode ne convient pas pour une utilisation standard, sauf si votre ordinateur est peu véloce.
- **Performances élevées** - Ce mode exige une quantité de mémoire importante. Durant l'analyse destinée à identifier le spam, les fonctions suivantes seront utilisées : règles et cache de base de données de spam, règles standard et avancées, adresses IP et bases de données de l'expéditeur de spam.

L'option **Activer la vérification en ligne** est sélectionnée par défaut. Cette configuration produit une détection plus précise du spam grâce à la communication avec les serveurs [Mailshell](#). En effet, les données analysées sont comparées aux bases de données en ligne [Mailshell](#).

**Il est généralement recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité. Tout changement de configuration ne doit être réalisé que par un utilisateur expérimenté.**

L'option **RBL** ouvre la boîte de dialogue **Realtime Blackhole Lists**, qui permet d'activer/désactiver la fonction **Interroger les serveurs RBL**.



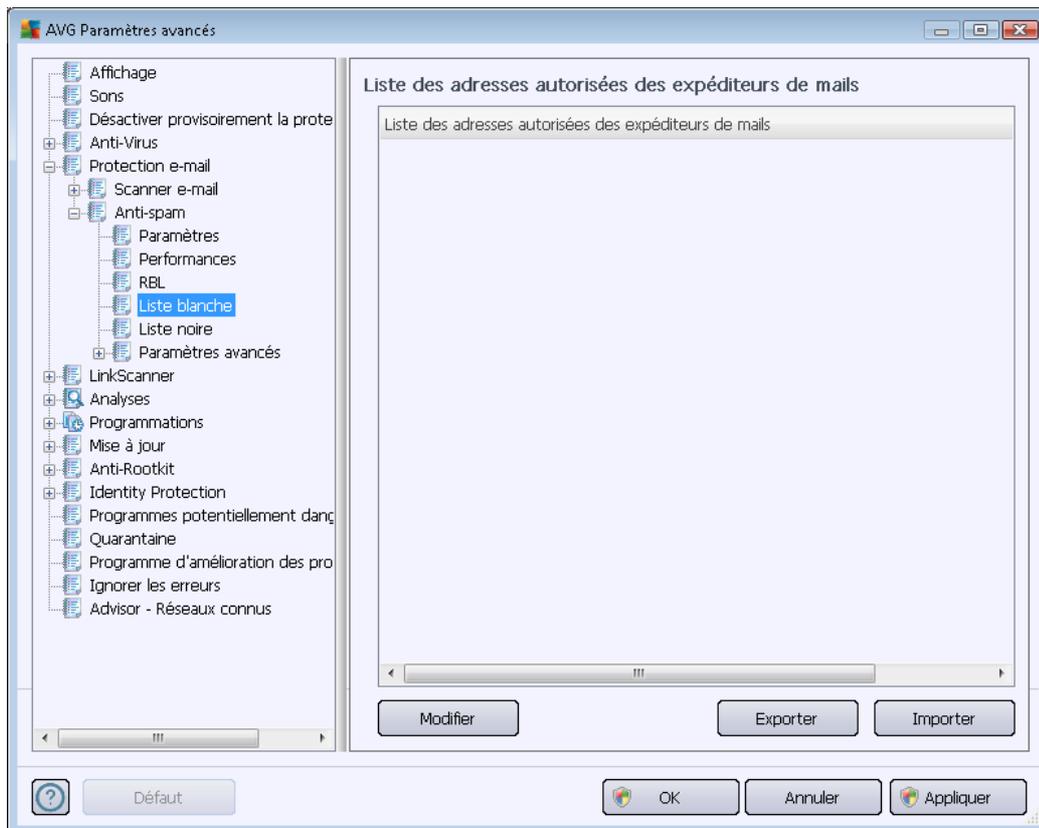


Le serveur RBL (*Realtime Blackhole List*) est un serveur DNS doté d'une base de données étendue d'expéditeurs connus de spam. Lorsque cette fonction est activée, tous les mails sont vérifiés par rapport à la base de données du serveur RBL et sont signalés comme du spam dès lors qu'ils sont identiques à une entrée de la base de données. Les bases de données des serveurs RBL contiennent les signatures de spam les plus actuelles afin de fournir une détection anti-spam la plus exacte et la meilleure qui soit. Cette fonction est particulièrement utile pour les utilisateurs qui reçoivent de gros volumes de spam qui ne sont ordinairement pas détectés par le moteur [anti-spam](#).

La zone de texte **Liste des serveurs RBL** permet de définir les emplacements des serveurs RBL à interroger. (*Veillez noter que l'activation de cette fonction peut, sur certains systèmes et configurations, ralentir la réception des messages, car chacun d'entre eux est vérifié à la lumière de la base de données des serveurs RBL*).

**Notez qu'aucune donnée personnelle n'est transmise au serveur.**

L'entrée **Liste blanche** ouvre la boîte de dialogue **Liste des adresses autorisées des expéditeurs de mails** contenant la liste globale des adresses électroniques d'expéditeurs et des noms de domaine approuvés dont les messages ne seront jamais considérés comme du courrier indésirable.



Dans l'interface d'édition, vous avez la possibilité d'établir la liste des expéditeurs qui ne vous enverront pas de messages indésirables (spam). De la même manière, vous pouvez dresser une liste de noms de domaine complets (*avgfrance.com*, par exemple) dont vous avez la certitude qu'ils ne diffusent pas de messages indésirables. Lorsque vous disposez d'une liste d'expéditeurs et ou de



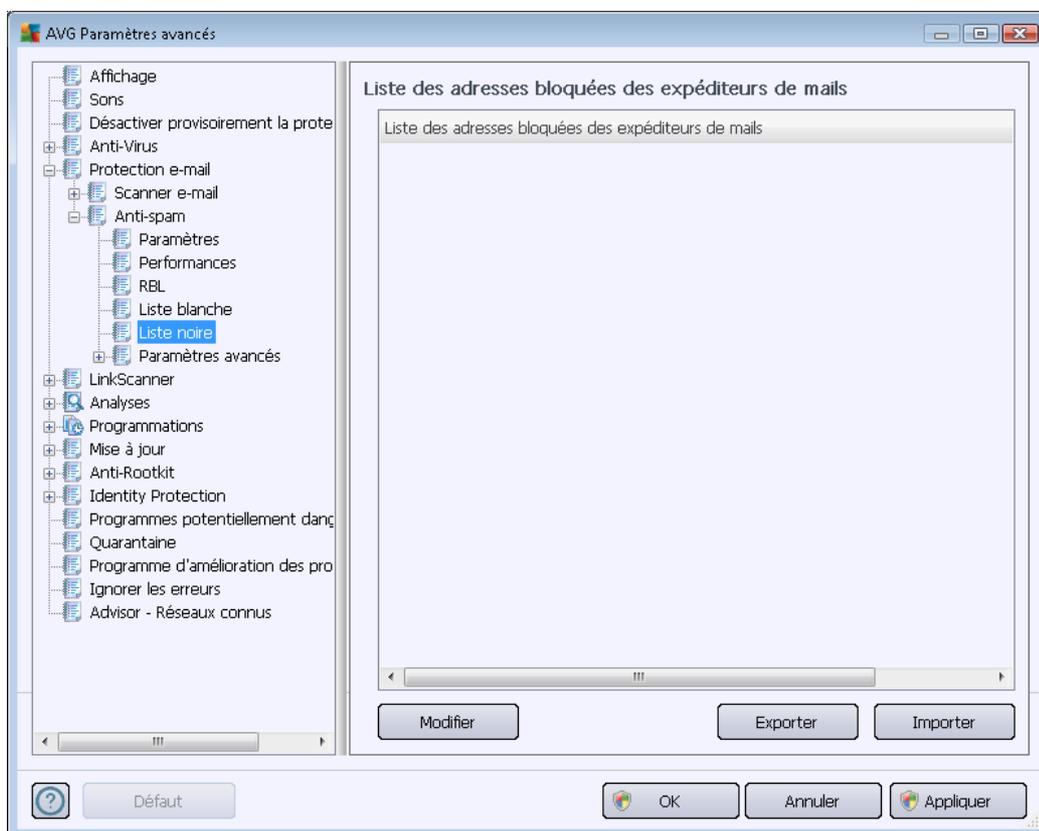
noms de domaines, il ne vous reste plus qu'à l'incorporer selon l'une des méthodes suivantes : saisissez directement chaque adresse ou importez la liste entière.

### Boutons de commande

Vous avez accès aux boutons de fonctions suivants :

- **Modifier** – cliquez sur ce bouton pour ouvrir une boîte de dialogue permettant de définir manuellement une liste d'adresses (*la méthode copier-coller convient également*). Insérez une entrée (*expéditeur, nom de domaine*) par ligne.
- **Exporter** – si vous désirez exporter les enregistrements pour une raison quelconque, cliquez sur ce bouton. Tous les enregistrements seront conservés au format texte brut.
- **Importer** – si vous avez déjà préparé un fichier texte d'adresses électroniques/de noms de domaines, cliquez simplement sur ce bouton pour l'importer. Le contenu du fichier doit inclure un seul élément par ligne (*adresse, nom de domaine*).

L'entrée **Liste noire** ouvre une boîte de dialogue contenant la liste globale des adresses d'expéditeurs et des noms de domaine bloqués dont les messages seront systématiquement considérés comme du spam.





Dans l'interface d'édition, vous avez la possibilité d'établir la liste des expéditeurs que vous jugez enclins à vous envoyer des messages indésirables (*spam*). De même, vous pouvez dresser une liste de noms de domaines complets (*sociétédespam.com*, par exemple) dont vous avez reçu ou pensez recevoir du courrier indésirable. Tous les mails des adresses ou domaines répertoriés seront alors identifiés comme du spam. Lorsque vous disposez d'une liste d'expéditeurs et ou de noms de domaines, il ne vous reste plus qu'à l'incorporer selon l'une des méthodes suivantes : saisissez directement chaque adresse ou importez la liste entière.

### **Boutons de commande**

Vous avez accès aux boutons de fonctions suivants :

- **Modifier** – cliquez sur ce bouton pour ouvrir une boîte de dialogue permettant de définir manuellement une liste d'adresses (*la méthode copier-coller convient également*). Insérez une entrée (*expéditeur, nom de domaine*) par ligne.
- **Exporter** – si vous désirez exporter les enregistrements pour une raison quelconque, cliquez sur ce bouton. Tous les enregistrements seront conservés au format texte brut.
- **Importer** – si vous avez déjà préparé un fichier texte d'adresses électroniques/de noms de domaines, cliquez simplement sur ce bouton pour l'importer.

***La catégorie Paramètres avancés contient les options de configuration détaillées du composant Anti-Spam. Ces paramètres sont destinés uniquement aux utilisateurs expérimentés et plus particulièrement aux administrateurs réseau, qui doivent paramétrer plus finement la protection anti-spam et garantir la protection la plus complète des serveurs de messagerie. Pour cette raison, aucune aide supplémentaire n'est fournie au sein des boîtes de dialogue. Néanmoins, l'interface utilisateur affiche une brève description de chaque option associée.***

***Nous vous conseillons vivement de ne pas modifier ces paramètres, à moins de maîtriser complètement les paramètres avancés de Spamcatcher (MailShell Inc.). Toute modification incorrecte risque de dégrader les performances ou de provoquer un dysfonctionnement du composant.***

Si vous pensez devoir modifier la configuration [Anti-Spam](#) à un niveau très avancé, conformez-vous aux instructions fournies dans l'interface utilisateur. Généralement, vous trouverez dans chaque boîte de dialogue une seule fonction spécifique que vous pouvez ajuster. Sa description figure toujours dans la boîte de dialogue elle-même :

- **Cache** - signature, réputation du domaine, réputation légitime
- **Enrichissement** - nombre maximum de mots à entrer, seuil d'apprentissage automatique, pondération
- **Filtrage** - liste des langues, liste des pays, adresses IP approuvées, adresses IP bloquées, pays bloqués, caractères bloqués, expéditeurs usurpés

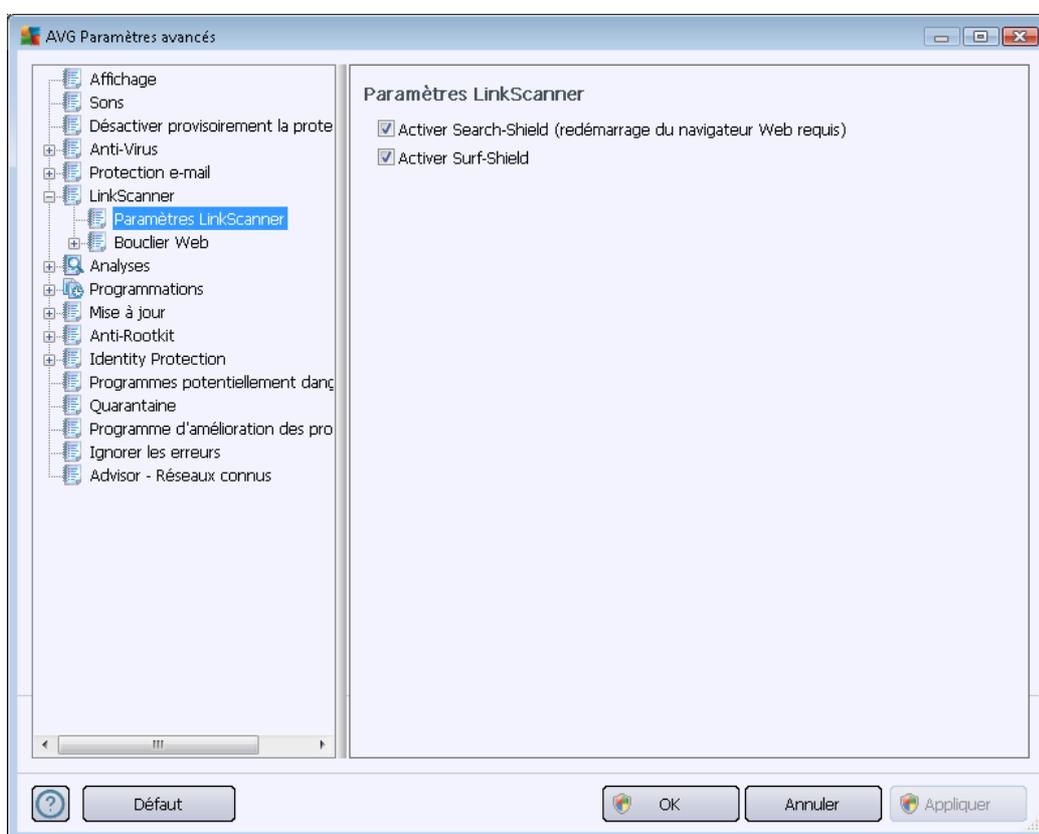


- **RBL** – serveurs RBL, résultats multiples, seuil, délai, IP max.
- **Connexion Internet** - délai, serveur proxy, authentification du proxy

## 10.6. LinkScanner

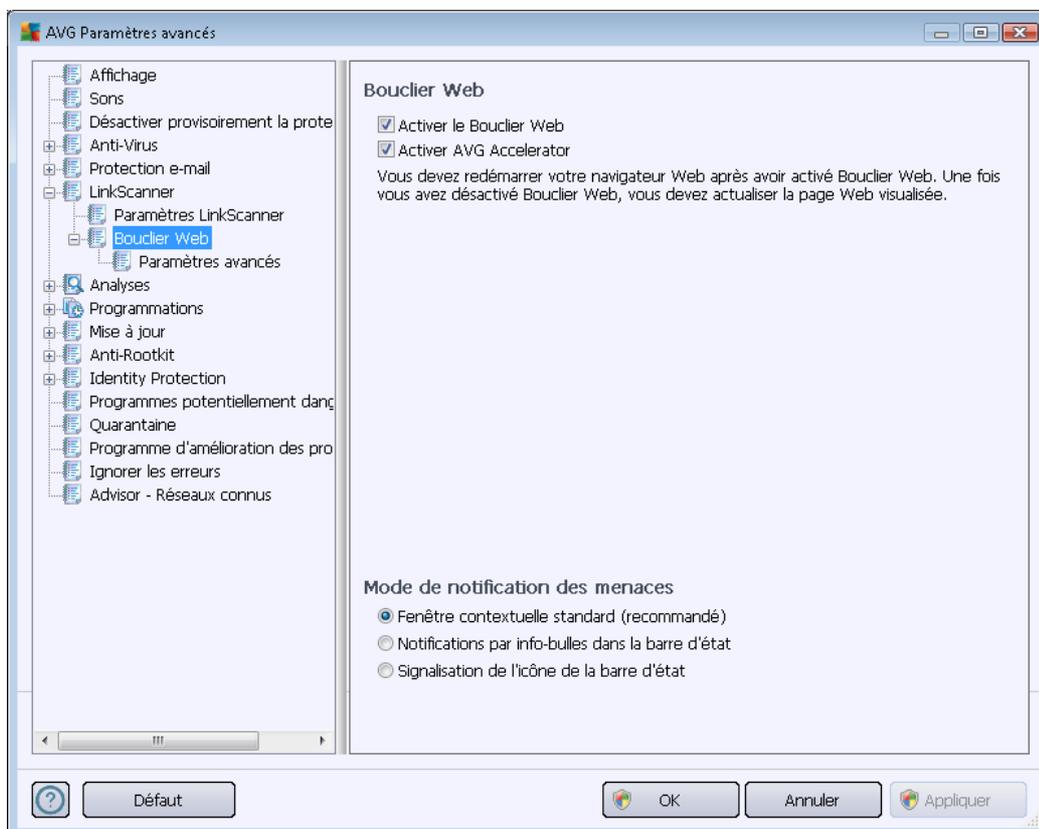
### 10.6.1. Paramètres LinkScanner

La boîte de dialogue des **Paramètres du LinkScanner** permet d'activer ou de désactiver les fonctions essentielles du composant **LinkScanner** :



- **Activer Search-Shield** – (*paramètre activé par défaut*): icônes de notification portant sur les recherches effectuées dans Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg ou SlashDot après vérification préalable du contenu des sites renvoyés par le moteur de recherche.
- **Activer Surf-Shield** : (*option activée par défaut*) : protection active (*en temps réel*) contre les sites hébergeant des exploits, lorsque vous y accédez. Les connexions à des sites malveillants et leur contenu piégé sont bloqués au moment où l'utilisateur demande à y accéder via un navigateur Web (*ou toute autre application qui utilise le protocole HTTP*).

## 10.6.2. Bouclier Web

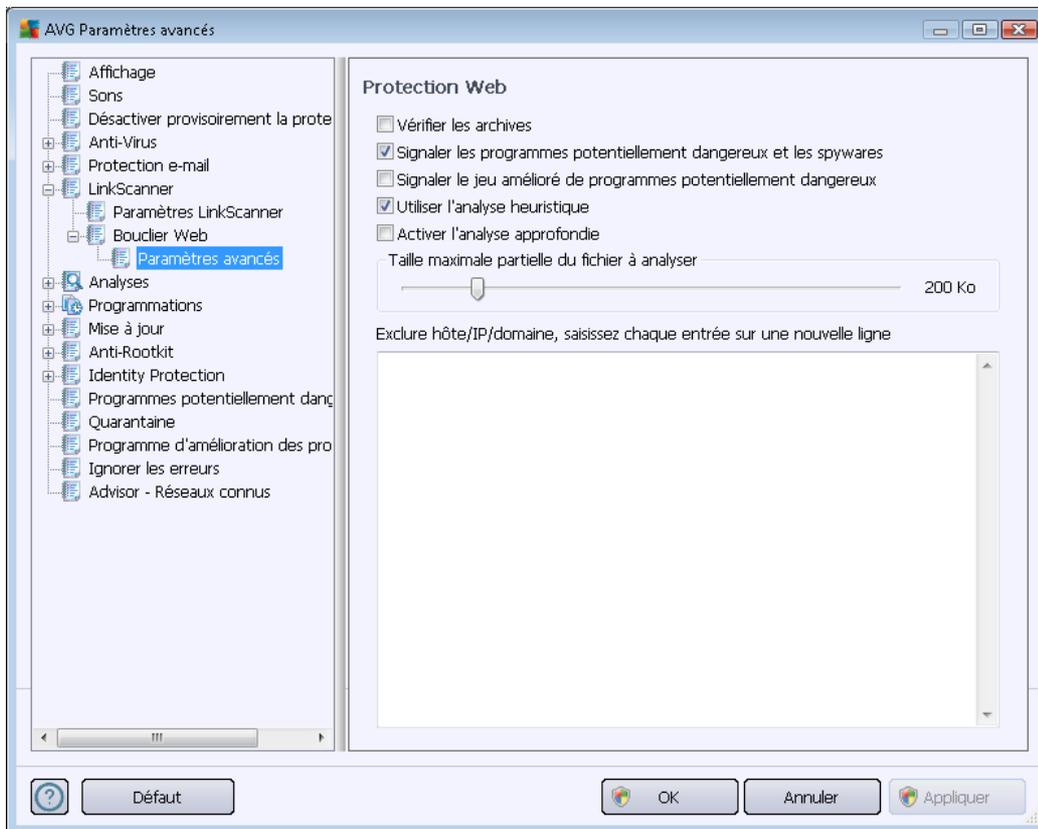


La boîte de dialogue **Bouclier Web** comporte les options suivantes :

- **Activer le Bouclier Web** (*option activée par défaut*) – Active/désactive l'ensemble du service **Bouclier Web**. Pour accéder à d'autres paramètres avancés du **Bouclier Web**, ouvrez la boîte de dialogue suivante, [Protection Web](#).
- **Activer AVG Accelerator** (*option activée par défaut*) - Active/désactive le service **AVG Accelerator** qui favorise une lecture vidéo en ligne plus fluide et facilite les téléchargements supplémentaires.

### Mode de notification des menaces

Au bas de la boîte de dialogue, sélectionnez le mode de notification des menaces détectées : boîte de dialogue contextuelle standard, info-bulle dans la barre d'état ou infos contenues dans l'icône de la barre d'état.



La boîte de dialogue **Protection Web** vous permet de modifier à votre convenance la configuration du composant chargé de l'analyse du contenu des sites Web. L'interface d'édition propose plusieurs options de configuration élémentaires, décrites ci-après :

- **Activer la Protection Web** – cette option confirme que le **Bouclier Web** doit analyser le contenu des pages Web. Si elle est activée (*par défaut*), vous pouvez activer/désactiver les options suivantes :
  - **Vérifier les archives** (option désactivée par défaut) : analyse le contenu des archives éventuelles contenues dans la page Web à afficher.
  - **Signaler les programmes potentiellement dangereux et les spywares** (option activée par défaut) : cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. [Les spywares](#) désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre ordinateur.
  - **Signaler le jeu amélioré de programmes potentiellement dangereux** (option désactivée par défaut) : permet de détecter le jeu étendu des [spywares](#) qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins



malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- **Utiliser l'analyse heuristique** (*option activée par défaut*) : analyse le contenu de la page à afficher en appliquant la [méthode heuristique](#) (*l'émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel*).
- **Activer l'analyse approfondie** (*option désactivée par défaut*) – dans certains cas (*suspicion d'une infection de l'ordinateur*), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Taille maximale des fichiers à analyser** – si les fichiers inclus figurent dans la page affichée, vous pouvez également analyser leur contenu avant même qu'ils ne soient téléchargés sur votre ordinateur. Notez cependant que l'analyse de fichiers volumineux peut prendre du temps et ralentir considérablement le téléchargement des pages Web. Utilisez le curseur pour fixer la taille de fichier maximale à faire analyser par le **Bouclier Web**. Même si le fichier téléchargé est plus volumineux que la taille maximale spécifiée, et ne peut donc pas être analysé, vous restez protégé : si le fichier est infecté, le **Bouclier résident** le détecte immédiatement.
- **Exclure hôte/IP/domaine** – dans la zone de texte, saisissez le nom exact d'un serveur (*hôte, adresse IP, adresse IP avec masque ou URL*) ou un domaine qui ne doit pas faire l'objet d'une analyse par le **Bouclier Web**. En conséquence, n'excluez que les hôtes dont vous pouvez affirmer qu'ils ne fourniront jamais un contenu Web dangereux.

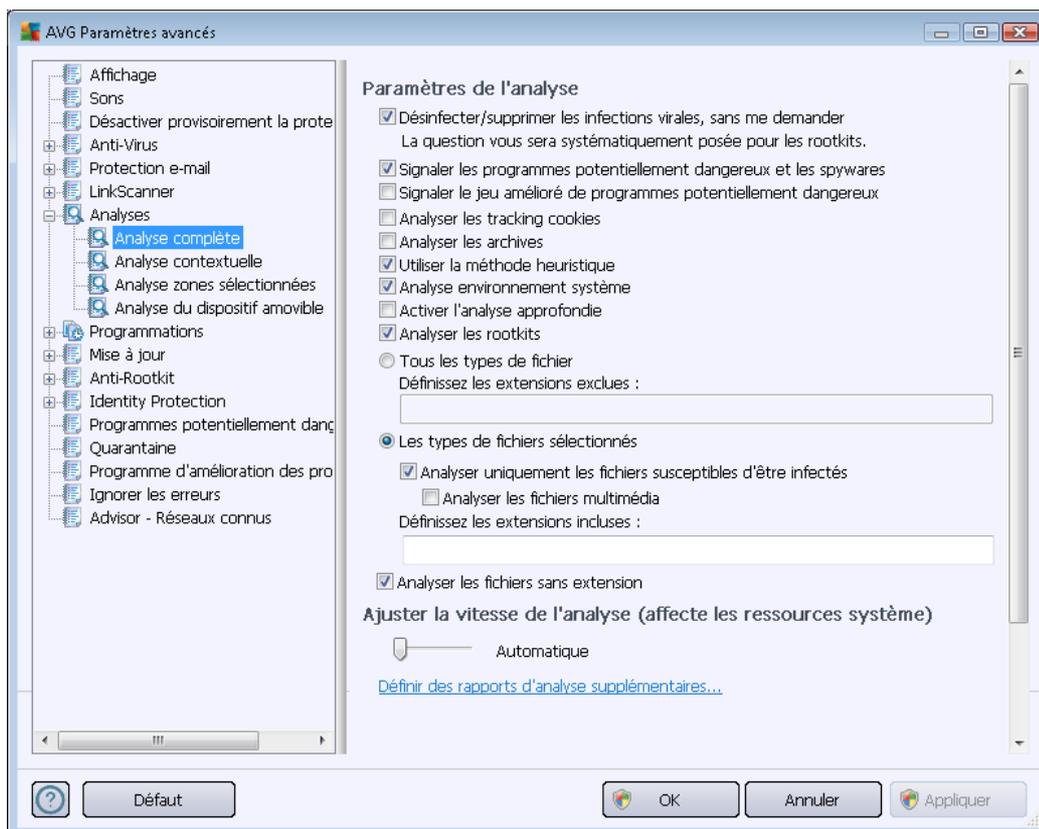
## 10.7. Analyses

Les paramètres d'analyse avancés sont répartis en quatre catégories selon le type d'analyse spécifique tel qu'il a été défini par l'éditeur du logiciel :

- **Analyse complète** - analyse standard prédéfinie appliquée à l'ensemble des fichiers contenus dans l'ordinateur
- **Analyse contextuelle** : analyse spécifique d'un objet directement sélectionné dans l'environnement de l'Explorateur Windows
- **Analyse zones sélectionnées** – analyse standard prédéfinie appliquée aux zones spécifiées de l'ordinateur
- **Analyse du dispositif amovible** : analyse spécifique des périphériques amovibles connectés à votre ordinateur

### 10.7.1. Analyse complète

L'option **Analyse complète** permet de modifier les paramètres d'une analyse prédéfinie par l'éditeur du logiciel, [Analyse complète](#).



#### Paramètres de l'analyse

La section **Paramètres de l'analyse** présente la liste de paramètres d'analyse susceptibles d'être activés ou désactivés :

- **Réparer/supprimer les infections sans me demander** (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en [quarantaine](#).
- **Signaler les programmes potentiellement dangereux et les spywares** (option activée par défaut) : cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.



- **Signaler le jeu amélioré de programmes potentiellement dangereux** (option désactivée par défaut) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisés à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.
- **Analyser les tracking cookies** (option désactivée par défaut) : ce paramètre du composant [Anti-Spyware](#) définit les cookies qui pourront être détectés au cours de l'analyse (les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique).
- **Analyser les archives** (option désactivée par défaut) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des archives (archives ZIP, RAR, par exemple).
- **Utiliser la méthode heuristique** (option activée par défaut) : l'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyse environnement système** (option activée par défaut) : l'analyse vérifie les fichiers système de l'ordinateur.
- **Activer l'analyse approfondie** (option désactivée par défaut) – dans certains cas (suspicion d'une infection de l'ordinateur), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Analyser les rootkits** (activée par défaut) : l'analyse [Anti-Rootkit](#) recherche les éventuels rootkits présents sur votre ordinateur, c'est-à-dire les programmes et technologies destinés à masquer l'activité de programmes malveillants sur l'ordinateur. Si un rootkit est détecté, cela ne veut pas forcément dire que votre ordinateur est infecté. Dans certains cas, des pilotes spécifiques ou des sections d'applications régulières peuvent être considérés, à tort, comme des rootkits.

Ensuite, vous pouvez choisir d'analyser

- **Tous les types de fichier** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers à ne pas analyser (séparées par des virgules) ;
- **Les types de fichiers sélectionnés** – vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables), y compris les fichiers multimédia (vidéo, audio – si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet



d'une analyse.

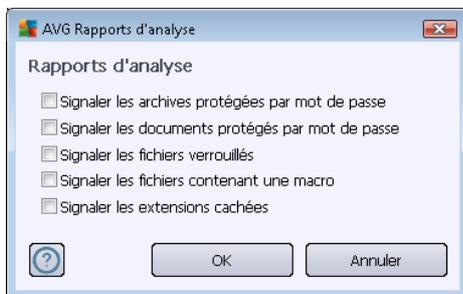
- Vous pouvez également choisir l'option **Analyser les fichiers sans extension** – cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

### Ajuster la vitesse de l'analyse

Dans la section **Ajuster la vitesse de l'analyse**, il est possible de régler la vitesse d'analyse en fonction des ressources système. Par défaut, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit la durée de l'analyse, mais sollicite fortement les ressources système et ralentit considérablement les autres activités de l'ordinateur (*cette option convient lorsque l'ordinateur est allumé, mais que personne n'y travaille*). Inversement, vous pouvez réduire l'utilisation des ressources système en augmentant la durée de l'analyse.

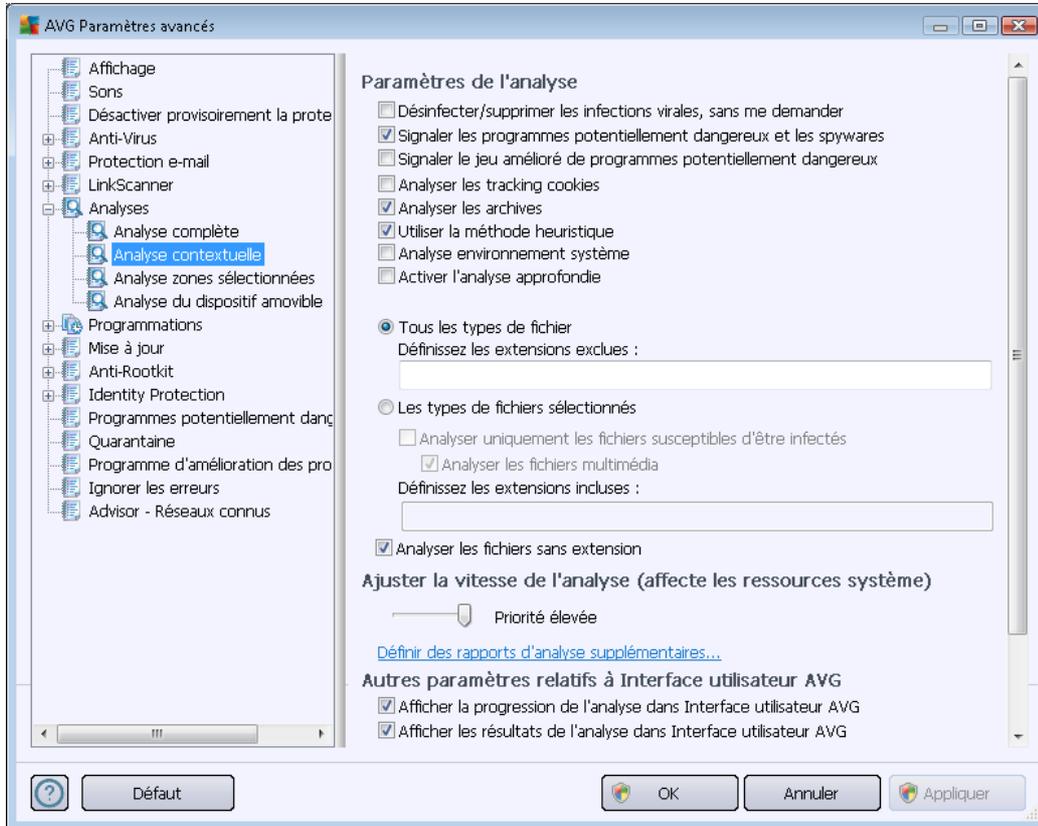
### Définir des rapports d'analyse supplémentaires...

Cliquez sur le lien **Définir des rapports d'analyse supplémentaires** pour ouvrir la boîte de dialogue **Rapports d'analyse** dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



### 10.7.2. Analyse contextuelle

Similaire à l'option précédente [Analyse complète](#), l'option **Analyse contextuelle** propose plusieurs options permettant d'adapter les analyses prédéfinies par l'éditeur du logiciel. La configuration actuelle s'applique à [l'analyse d'objets spécifiques exécutée directement dans l'Explorateur Windows](#) (*extension des menus*), voir le chapitre [Analyse dans l'Explorateur Windows](#) :



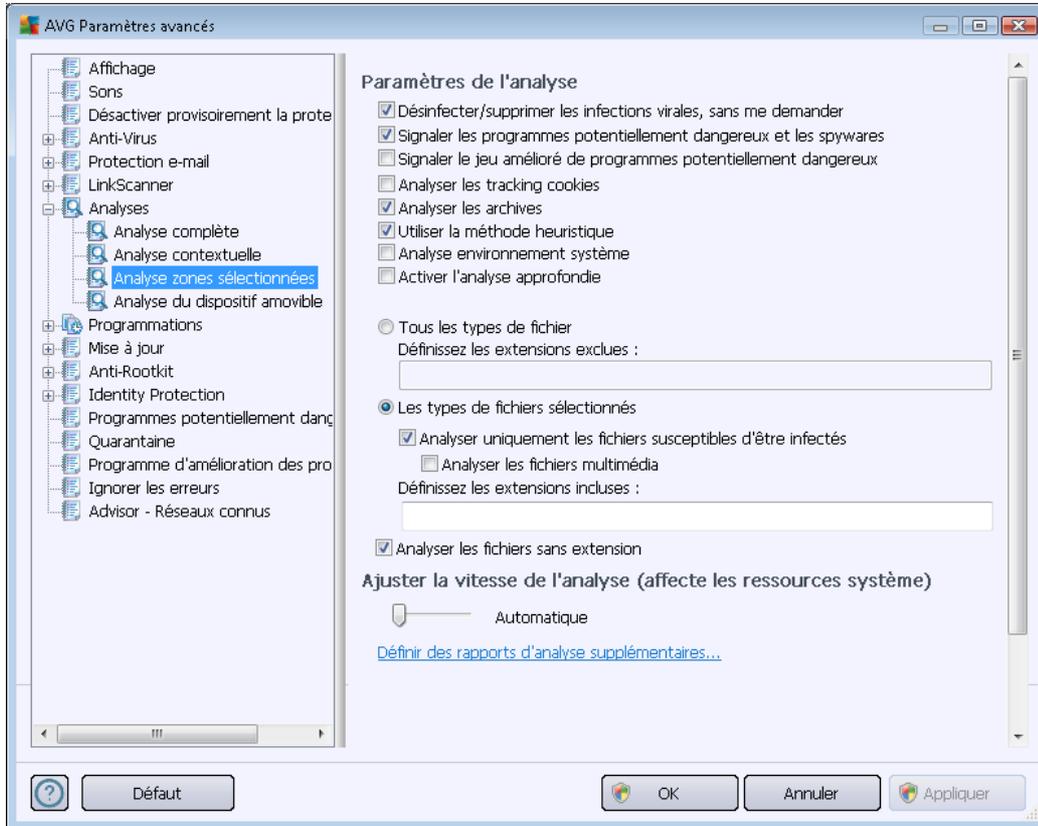
La liste des paramètres correspond à celle proposée pour l'[analyse complète](#). Cependant, les paramètres par défaut diffèrent (*par exemple, l'analyse complète par défaut ne vérifie pas les archives, mais analyse l'environnement système à l'inverse de l'analyse contextuelle*).

**Remarque :** pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre [Paramètres avancés d'AVG / Analyses / Analyse complète](#).

Comme la boîte de dialogue [Analyse complète](#), celle de l'**analyse contextuelle** inclut la section **Autres paramètres relatifs à l'interface utilisateur AVG**, dans laquelle vous indiquez si vous voulez que la progression de l'analyse et ses résultats soient accessibles à partir de l'interface utilisateur AVG. Vous pouvez aussi définir que les résultats d'analyse n'apparaissent qu'en cas d'infection détectée.

### 10.7.3. Analyse zones sélectionnées

L'interface d'édition de l'**analyse zones sélectionnées** est identique à celle de l'[analyse complète](#). Les options de configuration sont les mêmes, à ceci près que les paramètres par défaut sont plus stricts pour l'[analyse complète](#).

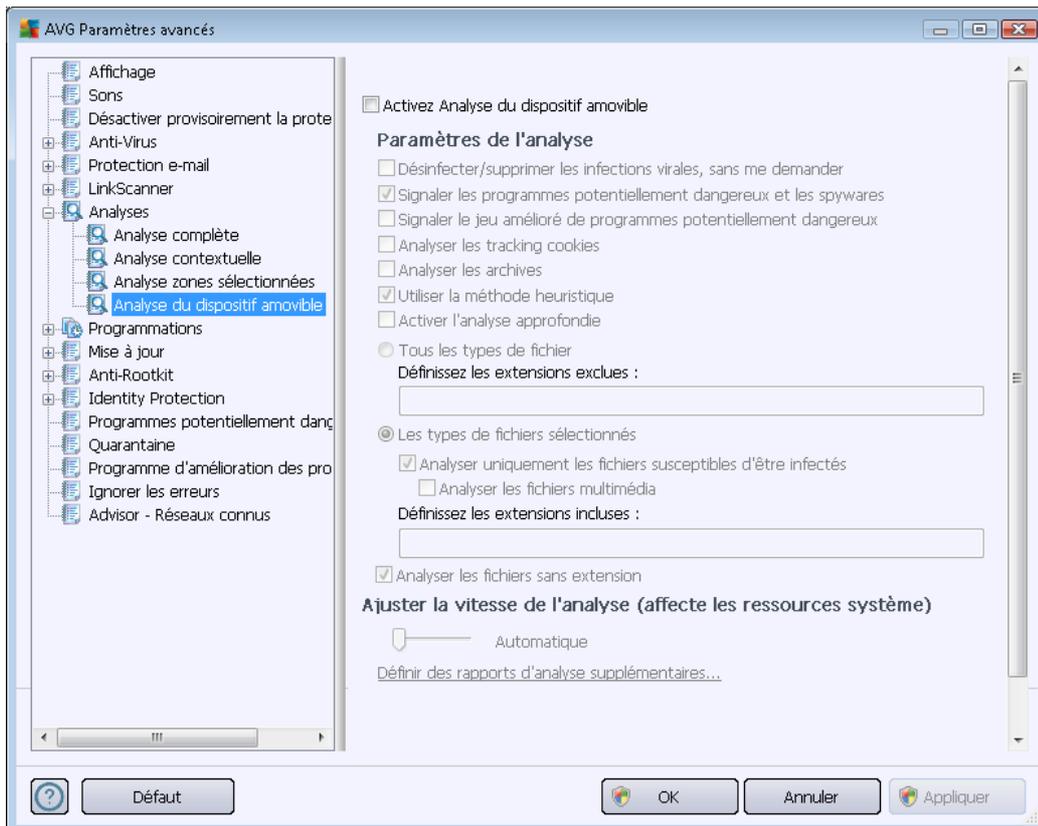


Tous les paramètres définis dans cette boîte de dialogue de configuration s'appliquent uniquement aux zones sélectionnées pour analyse dans le cadre de l'option [Analyse zones sélectionnées](#).

**Remarque :** pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre [Paramètres avancés d'AVG / Analyses / Analyse complète](#).

#### 10.7.4. Analyse des périphériques amovibles

L'interface de configuration de l'*analyse du dispositif amovible* ressemble beaucoup à celle intitulée [Analyse complète](#) :



L'*Analyse des périphériques amovibles* est lancée automatiquement chaque fois que vous connectez un périphérique amovible à l'ordinateur. Par défaut, cette fonctionnalité est désactivée. Cependant, il est primordial d'analyser les périphériques amovibles, car ils constituent l'une des sources d'infection majeurs. Pour que cette analyse soit activée et s'effectue automatiquement en cas de besoin, cochez la case **Activer l'analyse des périphériques amovibles**.

**Remarque** : pour obtenir la description des paramètres qui vous intéressent, consultez le chapitre [Paramètres avancés d'AVG / Analyses / Analyser complète](#).

#### 10.8. Programmations

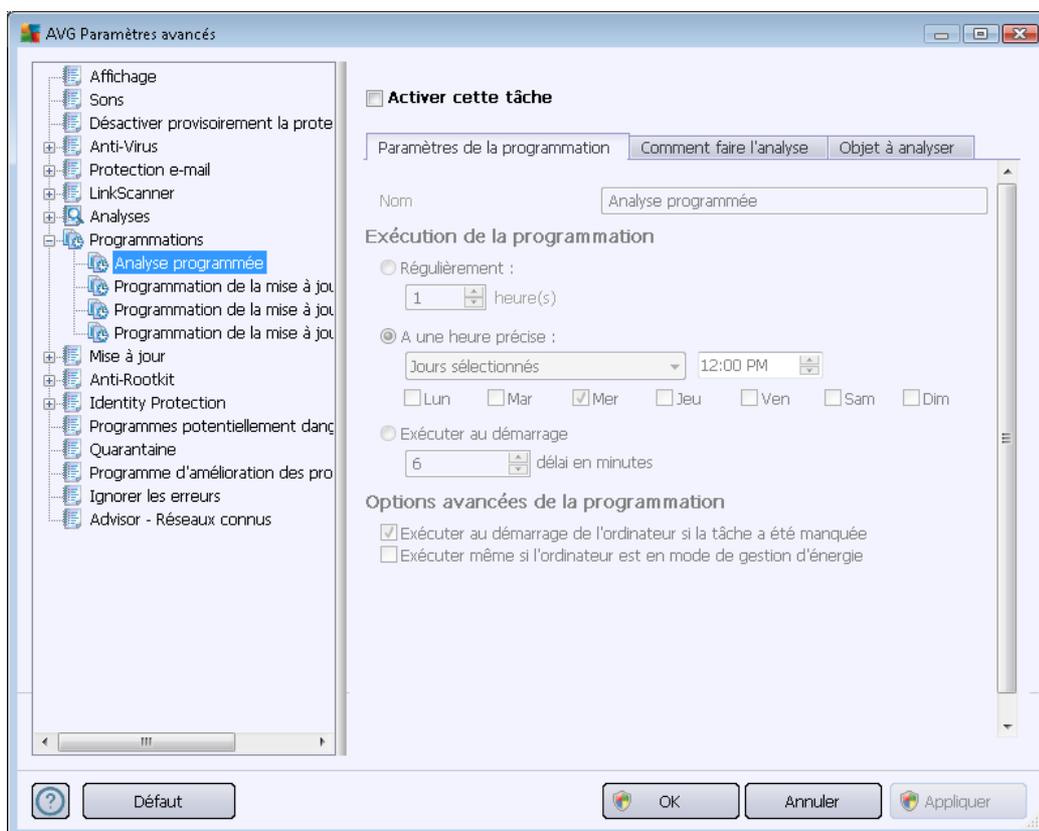
Dans l'entrée **Programmations**, vous êtes libre de modifier les paramètres par défaut des éléments suivants :

- [Analyse programmée](#)
- [Programmation de la mise à jour des définitions](#)
- [Programmation de la mise à jour du programme](#)

- [Programmation des mises à jour de l'Anti-Spam](#)

### 10.8.1. Analyse programmée

Les paramètres de l'analyse programmée peuvent être modifiés (ou une nouvelle analyse peut être programmée) depuis les trois onglets : Dans chaque onglet, vous pouvez cocher/décocher la case **Activer cette tâche** pour désactiver temporairement l'analyse programmée et la réactiver au moment opportun:



Dans la zone de texte **Nom** (option désactivée pour toutes les programmations par défaut), le nom est attribué à cette programmation par le fournisseur du programme. Pour les programmations nouvellement ajoutées (vous pouvez ajouter une nouvelle programmation en cliquant avec le bouton droit de la souris sur l'élément **Programmation de l'analyse** situé à gauche de l'arborescence de navigation), vous pouvez spécifier votre propre nom. Dans ce cas, la zone de texte est ouverte et vous pouvez y apporter des modifications. Veillez à utiliser toujours des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite.

**Exemple :** il n'est pas judicieux d'appeler l'analyse "Nouvelle analyse" ou "Mon analyse", car ces noms ne font pas référence au champ réel de l'analyse. A l'inverse, "Analyse environnement système" est un nom descriptif précis. Il est également nécessaire de spécifier dans le nom de l'analyse si l'analyse concerne l'ensemble de l'ordinateur ou une sélection de fichiers ou de dossiers. Notez que les analyses personnalisées sont toujours basées sur l'[Analyse zones sélectionnés](#).



Dans cette boîte de dialogue, vous définissez plus précisément les paramètres de l'analyse :

### Exécution de la programmation

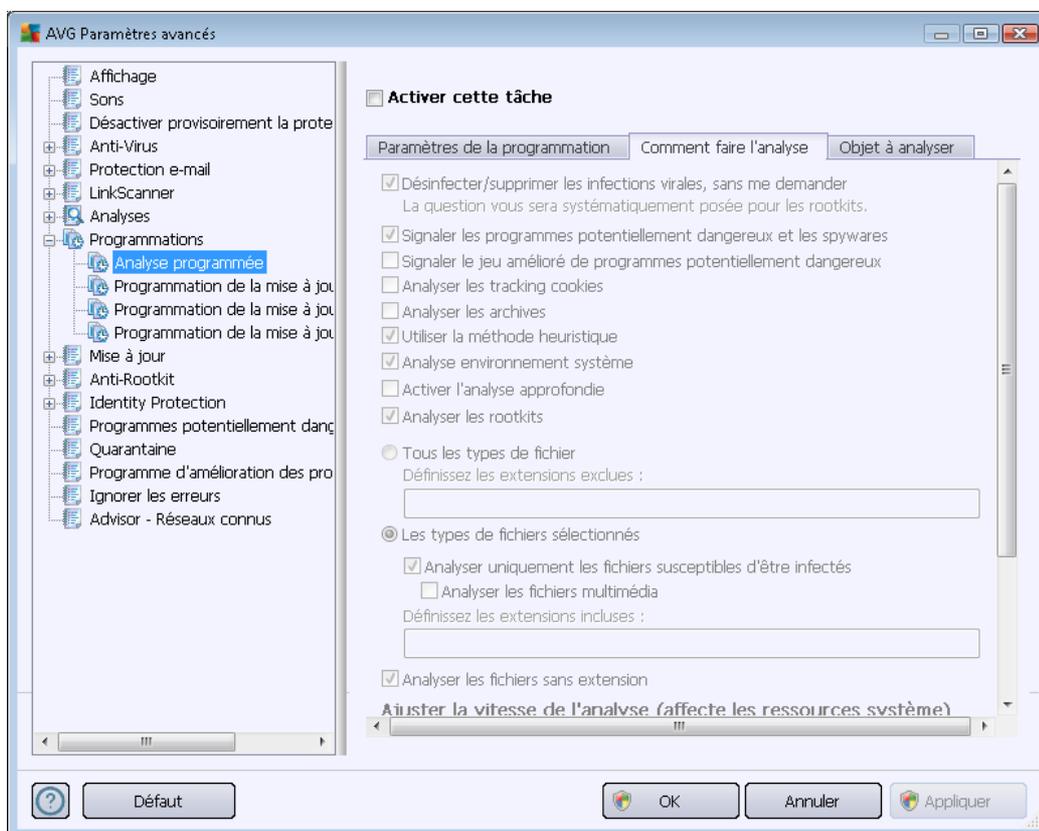
Ici, spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. La périodicité de l'analyse peut être programmée à des intervalles réguliers (**Régulièrement**), à une date et à une heure précises (**A une heure précise**) ou encore être associée à un événement (**Exécuter au démarrage**).

### Options avancées de la programmation

Cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension. Lorsque l'analyse programmée est exécutée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une fenêtre contextuelle de l'[icône dans la barre d'état système AVG](#) :



Une nouvelle [icône de la barre d'état système AVG](#) s'affiche alors (en couleurs clignotantes) et signale qu'une analyse programmée est en cours. Cliquez avec le bouton droit de la souris sur l'icône AVG de l'analyse en cours : un menu contextuel s'affiche dans lequel vous choisissez d'interrompre momentanément ou définitivement l'analyse et pouvez également modifier la priorité de l'analyse en cours d'exécution.



Dans l'onglet **Comment faire l'analyse**, vous trouverez la liste des paramètres d'analyse qui peuvent être activés ou désactivés. Par défaut, la plupart des paramètres sont activés et appliqués lors de l'analyse. **Il est vivement conseillé de ne pas modifier la configuration prédéfinie sans motif valable :**

- **Réparer/supprimer les infections sans me demander (activée par défaut) :** lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en [quarantaine](#).
- **Signaler les programmes potentiellement dangereux et les spywares (option activée par défaut) :** cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.
- **Signaler le jeu amélioré de programmes potentiellement dangereux (option désactivée par défaut) :** permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisés à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ;



c'est pourquoi elle est désactivée par défaut.

- **Analyser les tracking cookies** (option désactivée par défaut) : ce paramètre du composant [Anti-Spyware](#) définit que les cookies devront être détectés au cours de l'analyse (les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique).
- **Analyser les archives** (option désactivée par défaut) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des formats d'archives (archives ZIP, RAR, par exemple).
- **Utiliser la méthode heuristique** (option activée par défaut) : l'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyse environnement système** (option activée par défaut) : l'analyse vérifie les fichiers système de l'ordinateur.
- **Activer l'analyse approfondie** (option désactivée par défaut) : dans certains cas (suspicion d'une infection de l'ordinateur), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse pointus qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles d'être infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Analyser les rootkits** (activée par défaut) : l'analyse [Anti-Rootkit](#) recherche les éventuels rootkits présents sur votre ordinateur, c'est-à-dire les programmes et technologies destinés à masquer l'activité de programmes malveillants sur l'ordinateur. Si un rootkit est détecté, cela ne veut pas forcément dire que votre ordinateur est infecté. Dans certains cas, des pilotes spécifiques ou des sections d'applications régulières peuvent être considérés, à tort, comme des rootkits.

Ensuite, vous pouvez choisir d'analyser

- **Tous les types de fichier** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers à ne pas analyser (séparées par des virgules) ;
- **Types de fichiers sélectionnés** – vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables), y compris les fichiers multimédia (vidéo, audio – si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
- Vous pouvez également choisir l'option **Analyser les fichiers sans extension** – cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.

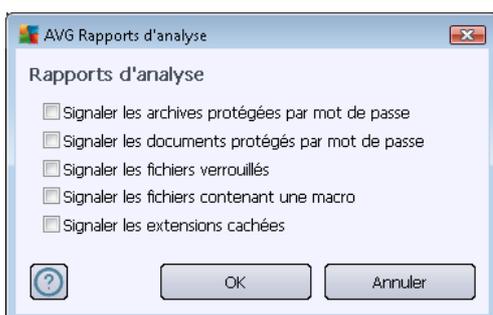


### Ajuster la vitesse de l'analyse

Dans la section **Ajuster la vitesse de l'analyse**, il est possible de régler la vitesse d'analyse en fonction des ressources système. Par défaut, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. Cette configuration permet d'accélérer l'analyse : elle réduit la durée de l'analyse, mais sollicite fortement les ressources système et ralentit considérablement les autres activités de l'ordinateur (*cette option convient lorsque l'ordinateur est allumé, mais que personne n'y travaille*). Inversement, vous pouvez réduire l'utilisation des ressources système en augmentant la durée de l'analyse.

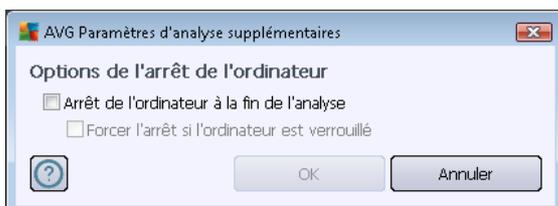
### Définir des rapports d'analyse supplémentaires

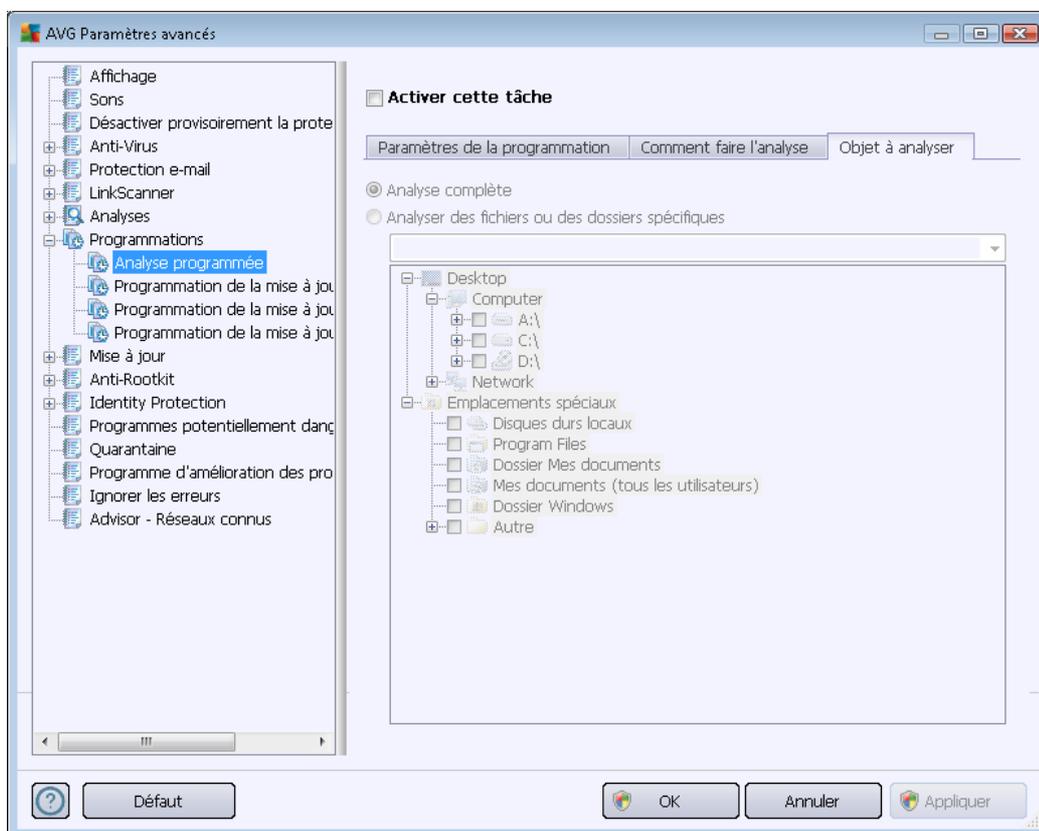
Cliquez sur le lien **Définir des rapports d'analyse supplémentaires** pour ouvrir la boîte de dialogue **Rapports d'analyse** dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



### Paramètres d'analyse supplémentaires

Cliquez sur **Paramètres d'analyse supplémentaires** pour ouvrir la boîte de dialogue **Options de l'arrêt de l'ordinateur** dans laquelle vous indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option **Arrêt de l'ordinateur à la fin de l'analyse** est activée, l'option **Forcer l'arrêt si l'ordinateur est verrouillé** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.

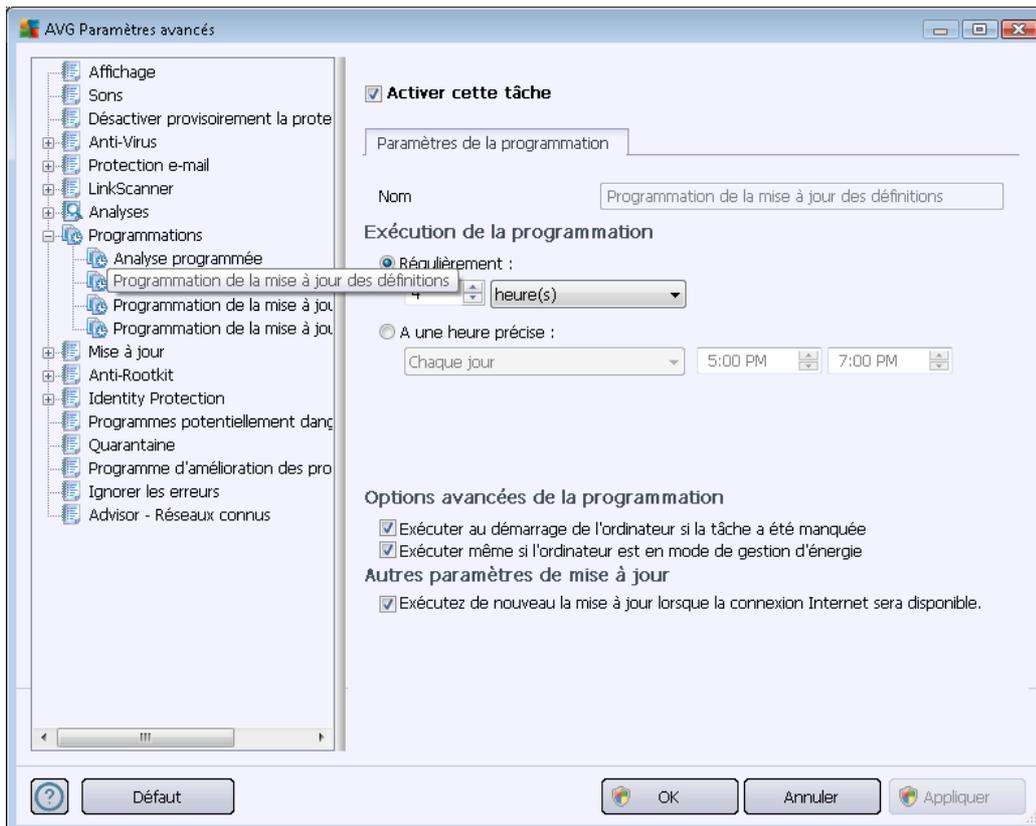




Sous l'onglet **Objet à analyser**, indiquez si vous voulez programmer l'[analyse complète](#) ou l'[analyse des zones sélectionnées](#). Si vous optez pour la deuxième solution, la structure de l'arborescence affichée dans la partie inférieure de la boîte de dialogue devient active et permet de définir les dossiers qui vous intéressent.

## 10.8.2. Programmation de la mise à jour des définitions

En cas de **nécessité absolue**, désélectionnez la case **Activer cette tâche** pour désactiver provisoirement la mise à jour programmée des définitions et la réactiver au moment opportun :



Cette boîte de dialogue permet d'affiner la programmation de la mise à jour des définitions. Dans la zone de texte **Nom** (désactivée pour toutes les programmations par défaut), le nom est attribué à cette programmation par le fournisseur du programme.

### Exécution de la programmation

Dans cette section, spécifiez la périodicité de l'exécution de la nouvelle mise à jour programmée des définitions. Il est possible de répéter le lancement de la mise à jour après un laps de temps donné (**Régulièrement**) ou d'en définir la date et l'heure précises (**A une heure précise**).

### Options avancées de la programmation

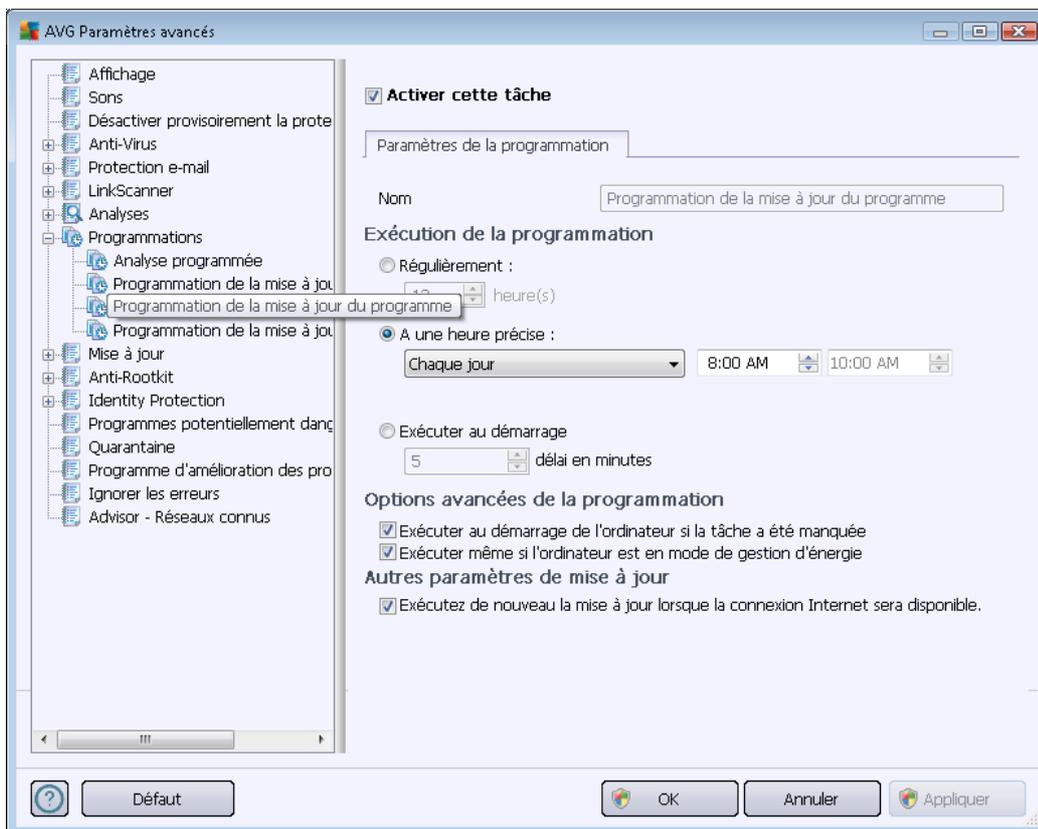
Cette section permet de définir dans quelles conditions la mise à jour des définitions doit ou ne doit pas être exécutée si l'ordinateur est hors tension ou en mode d'économie d'énergie.

## Autres paramètres de mise à jour

Enfin, cochez l'option **Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la mise à jour, le processus est relancé dès le rétablissement de la connexion Internet. Lorsque la mise à jour programmée est exécutée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une [icône dans la barre d'état système AVG](#) (à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue [Paramètres avancés/Affichage](#)).

### 10.8.3. Programmation de la mise à jour du programme

En cas de **nécessité absolue**, décochez la case **Activer cette tâche** pour désactiver temporairement la mise à jour programmée de l'application et la réactiver au moment opportun:



Dans la zone de texte **Nom** (non modifiable pour toutes les programmations par défaut), le nom est attribué par l'éditeur du programme.

## Exécution de la programmation

Ici, spécifiez l'intervalle entre chaque exécution de la mise à jour de l'application programmée. Il est possible de répéter l'exécution de la mise à jour après un laps de temps donné (**Régulièrement**), d'en définir la date et l'heure précises (**A une heure précise**) ou encore de définir l'évènement auquel



sera associé le lancement de la mise à jour (*Suivant une action*).

### Options avancées de la programmation

Cette section permet de définir dans quelles conditions la mise à jour de l'application doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

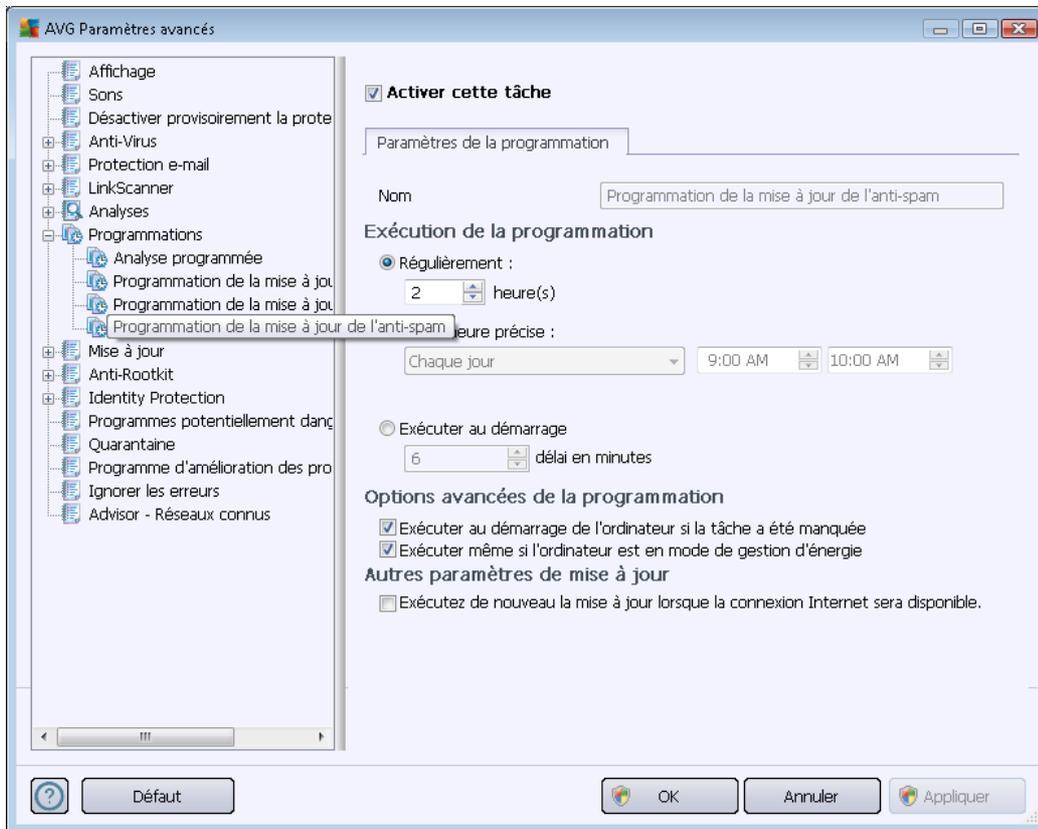
### Autres paramètres de mise à jour

Cochez l'option **Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la mise à jour, le processus est relancé dès le rétablissement de la connexion Internet. Lorsque la mise à jour programmée est lancée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une [icône dans la barre d'état système AVG](#) (à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue [Paramètres avancés/Affichage](#)).

**Remarque :** si une mise à jour planifiée du programme coïncide avec une analyse programmée, le processus de mise à jour a priorité sur l'analyse qui est interrompue.

### 10.8.4. Programmation de la mise à jour de l'anti-spam

En cas de nécessité absolue, décochez la case **Activer cette tâche** pour désactiver temporairement la mise à jour [programmée du composant](#) Anti-Spam et la réactiver au moment opportun :



Dans la boîte de dialogue correspondante, vous spécifiez en détail le programme de mise à jour : Dans la zone de texte **Nom** (désactivée pour toutes les programmations par défaut), le nom est attribué à cette programmation par le fournisseur du programme.

### Exécution de la programmation

Ici, spécifiez la fréquence de mise à jour du composant [Anti-Spam](#). Il est possible de répéter le lancement de la mise à jour [anti-spam](#) après un laps de temps donné (**Régulièrement**), de définir une heure et une date précises (**A une heure précise**) ou encore de définir un évènement auquel sera associé le lancement de la mise à jour (**Suivant une action**).

### Options avancées de la programmation

Cette section permet de définir dans quelles conditions la mise à jour [anti-spam](#) doit ou ne doit pas être exécutée si l'ordinateur est hors tension ou en mode d'économie d'énergie.

### Autres paramètres de mise à jour

Cochez l'option **Exécuter de nouveau la mise à jour lorsque la connexion Internet sera disponible** pour vous assurer qu'en cas d'interruption de la connexion Internet et d'échec de la [mise](#)

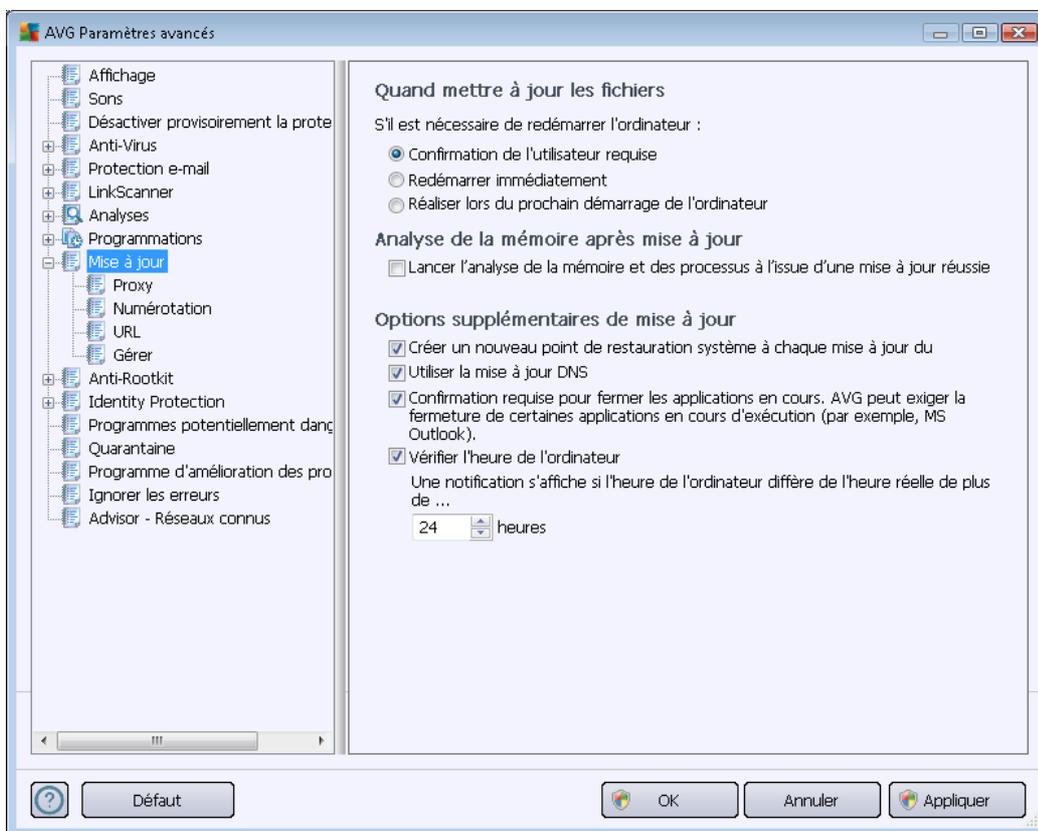


à jour d'Anti-Spam, le processus est relancé dès le rétablissement de la connexion Internet.

Lorsque l'analyse programmée est lancée à l'heure spécifiée, une fenêtre vous en informe par le biais d'une [icône dans la barre d'état système AVG](#) (à condition que vous ayez conservé la configuration par défaut de la boîte de dialogue [Paramètres avancés/Affichage](#)).

## 10.9. Mise à jour

L'élément de navigation **Mise à jour** ouvre une nouvelle boîte de dialogue dans laquelle vous spécifiez les paramètres généraux de la [mise à jour du programme AVG](#) :



### Quand mettre à jour les fichiers

Dans cette section, vous pouvez choisir une des trois solutions alternatives si le processus de mise à jour nécessite un redémarrage de l'ordinateur. Vous pouvez programmer la finalisation de la mise à jour pour le prochain redémarrage de l'ordinateur ou la lancer immédiatement:

- **Confirmation de l'utilisateur requise (par défaut)** - un message vous invite à approuver le redémarrage nécessaire pour finaliser le processus de [mise à jour](#)
- **Redémarrer immédiatement** – l'ordinateur redémarre automatiquement à l'issue du processus de [mise à jour](#), votre accord n'est pas recherché



- **Réaliser lors du prochain démarrage de l'ordinateur** - la finalisation du processus de [mise à jour](#) est reportée au prochain démarrage de l'ordinateur. Retenez que cette option n'est recommandée que si vous êtes sûr de redémarrer votre ordinateur souvent, au moins une fois par jour !

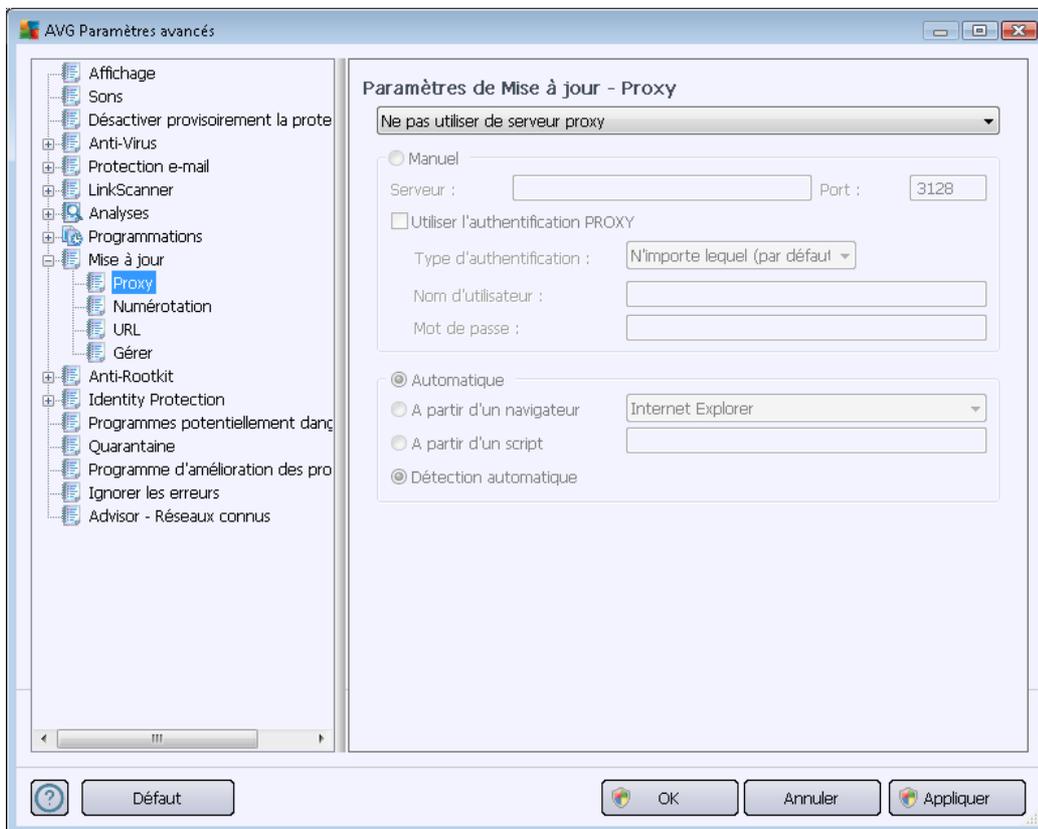
### Analyse de la mémoire après mise à jour

Cochez cette case pour indiquer que vous voulez exécuter une nouvelle analyse de la mémoire après chaque mise à jour achevée avec succès. La dernière mise à jour téléchargée peut contenir de nouvelles définitions de virus et celles-ci peuvent être analysées automatiquement.

### Options supplémentaires de mise à jour

- **Créer un nouveau point de restauration après chaque nouvelle mise à jour du programme** : un point de restauration est créé avant le lancement d'une mise à jour du programme AVG. En cas d'échec de la mise à jour et de blocage de votre système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est accessible via Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système. Option réservée aux utilisateurs expérimentés. Laissez cette case cochée si vous voulez utiliser cette fonctionnalité.
- **Utiliser la mise à jour DNS (option activée par défaut)** – lorsque cette option est cochée et que la mise à jour est lancée, **AVG Internet Security 2012** recherche les informations portant sur la base de données virale et le programme les plus récents, sur le serveur DNS. Seuls les fichiers de mise à jour indispensables requis sont téléchargés et appliqués. De cette manière, le nombre total de données est réduit au minimum et l'opération de mise à jour est plus rapide.
- **Confirmation requise pour fermer les applications en cours (option activée par défaut)** : cette option permet de vous assurer qu'aucune application actuellement en cours d'exécution ne sera fermée sans votre autorisation, si cette opération est requise pour la finalisation du processus de mise à jour.
- **Vérifier l'heure de l'ordinateur** : cochez cette case si vous voulez être informé lorsque l'écart entre l'heure de l'ordinateur et l'heure réelle est plus grand que le nombre d'heures spécifié.

### 10.9.1. Proxy



Un serveur proxy est un serveur ou un service autonome s'exécutant sur un PC dans le but de garantir une connexion sécurisée à Internet. En fonction des règles de réseau spécifiées, vous pouvez accéder à Internet directement, via le serveur proxy ou en combinant les deux possibilités. Dans la première zone (liste déroulante) de la boîte de dialogue **Paramètres de mise à jour – Proxy**, vous êtes amené à choisir parmi les options suivantes :

- **Utiliser un serveur proxy**
- **Ne pas utiliser de serveur proxy** – paramètres par défaut
- **Utiliser un serveur proxy. En cas d'échec, se connecter en direct**

Si vous sélectionnez une option faisant appel au serveur proxy, vous devez spécifier des données supplémentaires. Les paramètres du serveur peuvent être configurés manuellement ou automatiquement.

#### Configuration manuelle

Si vous choisissez la configuration manuelle (cochez la case *Manuel pour activer la section correspondante dans la boîte de dialogue*), spécifiez les éléments suivants :



- **Serveur** – indiquez l'adresse IP ou le nom du serveur
- **Port** – spécifiez le numéro du port donnant accès à Internet (*par défaut, le port 3128*) – *en cas de doute, prenez contact avec l'administrateur du réseau*

Il est aussi possible de définir des règles spécifiques à chaque utilisateur pour le serveur proxy. Si votre serveur proxy est configuré de cette manière, cochez l'option **Utiliser l'authentification PROXY** pour vous assurer que votre nom d'utilisateur et votre mot de passe sont valides pour établir une connexion à Internet via le serveur proxy.

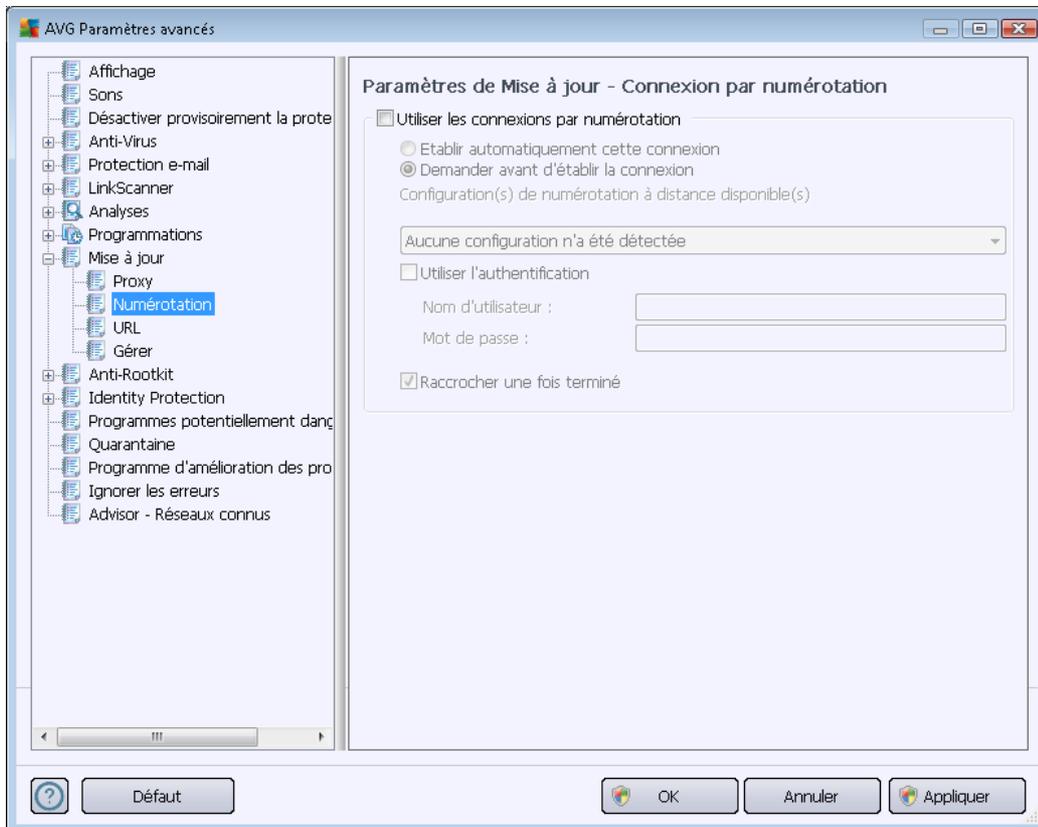
### Configuration automatique

Si vous optez pour la configuration automatique (*cochez la case **Automatique** pour activer la section correspondante dans la boîte de dialogue*), puis spécifiez le type de configuration proxy désiré :

- **A partir du navigateur** - la configuration sera lue depuis votre navigateur Internet par défaut
- **A partir d'un script** – la configuration sera lue à partir d'un script téléchargé avec la fonction renvoyant l'adresse du proxy
- **Détection automatique** – la configuration sera détectée automatiquement à partir du serveur proxy

### 10.9.2. Numérotation

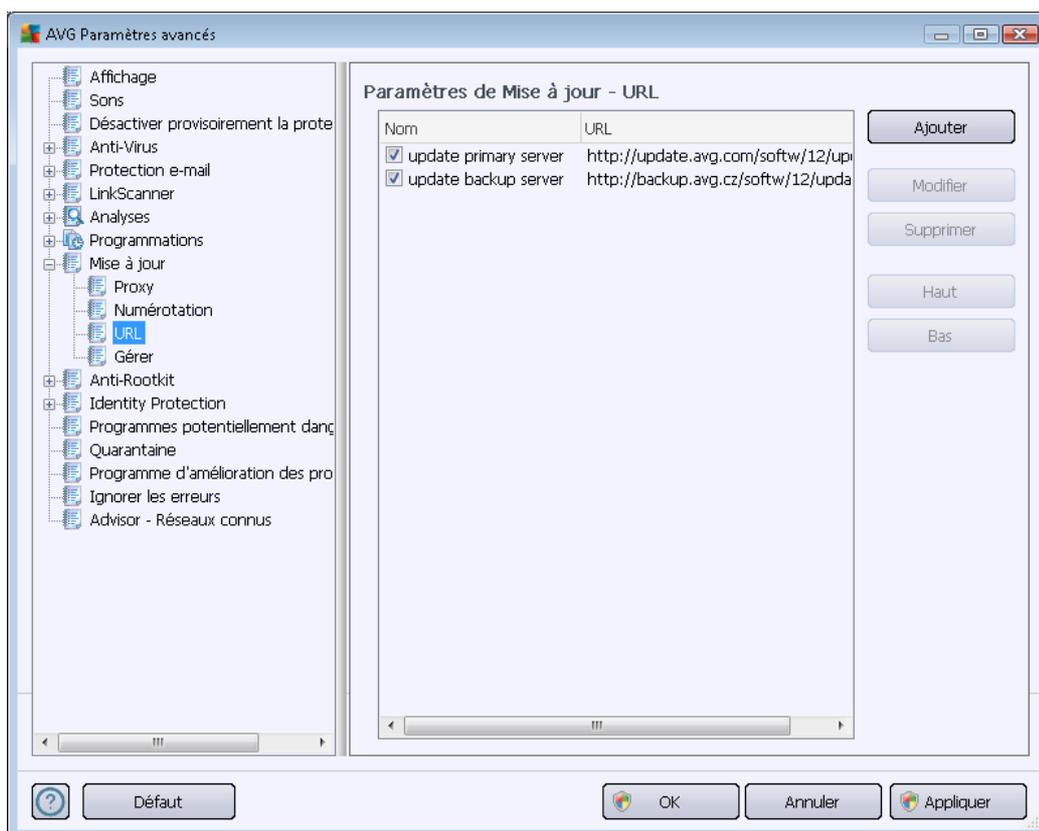
Tous les paramètres facultatifs de la boîte de dialogue **Paramètres de mise à jour – Connexion par numérotation** se rapportent à la connexion par numérotation à Internet. Les champs de cette boîte de dialogue sont activés à condition de cocher l'option **Utiliser les connexions par numérotation**:



Précisez si vous souhaitez vous connecter automatiquement à Internet (***Etablir cette connexion automatiquement***) ou confirmer manuellement la connexion (***Demander avant d'établir la connexion***). En cas de connexion automatique, vous devez indiquer si la connexion doit prendre fin après la mise à jour (***Raccrocher une fois terminé***).

### 10.9.3. URL

La boîte de dialogue **URL** contient une liste d'adresses Internet à partir desquelles il est possible de télécharger les fichiers de mise à jour :



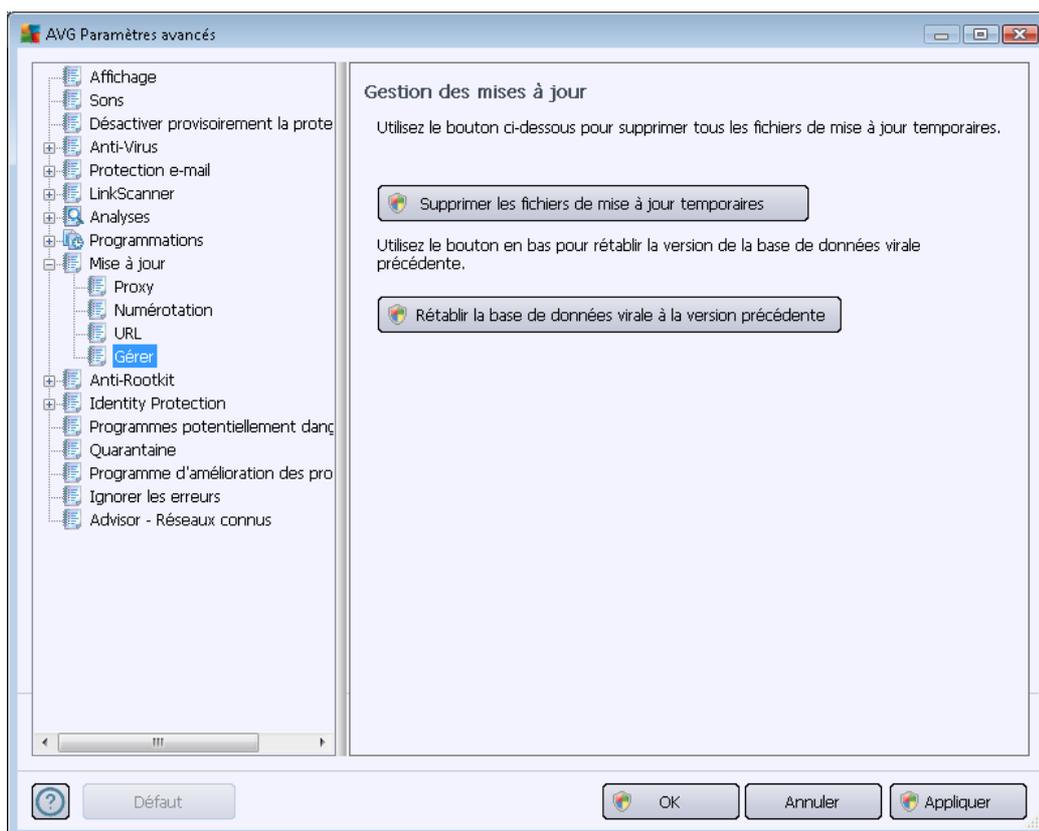
#### Boutons de commande

Vous pouvez redéfinir le contenu de cette liste à l'aide des boutons de fonction suivants :

- **Ajouter** – ouvre une boîte de dialogue permettant de spécifier une nouvelle adresse URL
- **Modifier** - ouvre une boîte de dialogue permettant de modifier les paramètres de l'URL sélectionnée
- **Supprimer** – retire l'URL sélectionnée de la liste
- **Haut** – déplace l'URL sélectionnée d'un rang vers le haut dans la liste
- **Bas** – déplace l'URL sélectionnée d'un rang vers le bas dans la liste

#### 10.9.4. Gérer

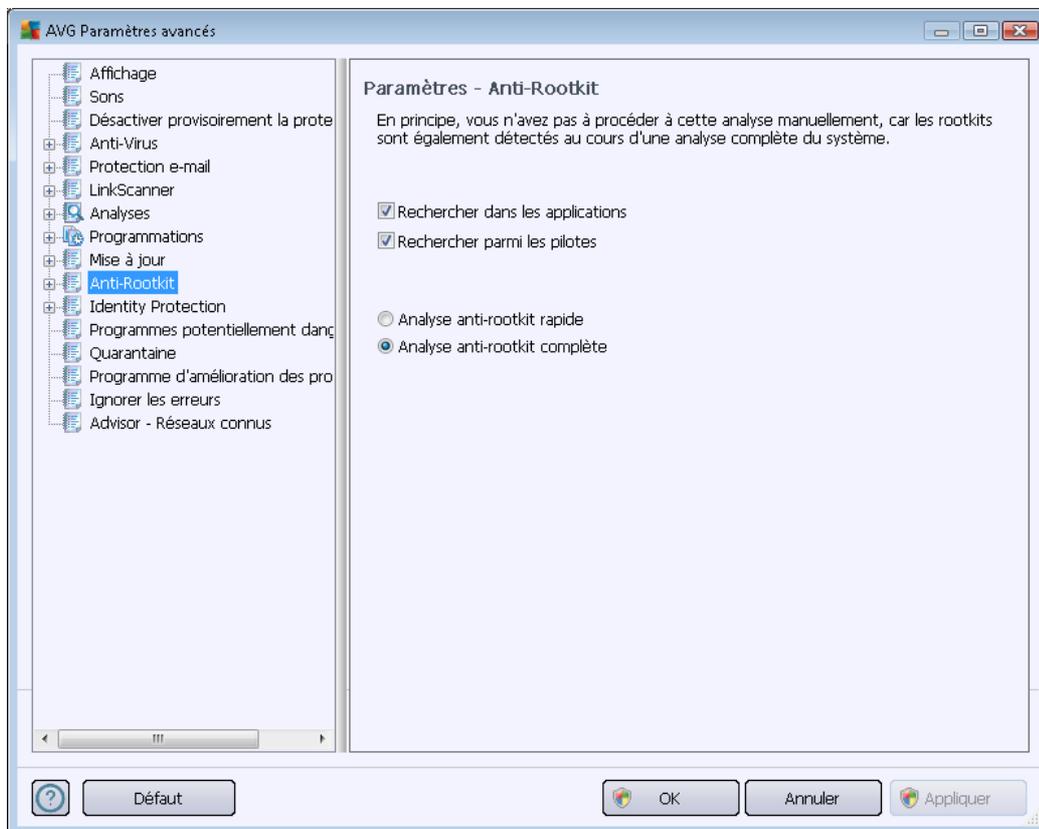
La boîte de dialogue **Gestion des mises à jour** comporte deux options accessibles via deux boutons :



- **Supprimer les fichiers de mise à jour temporaires** - cliquez sur ce bouton pour supprimer tous les fichiers redondants de votre disque dur (*par défaut, ces fichiers sont conservés pendant 30 jours*)
- **Revenir à la version précédente de la base virale** – cliquez sur ce bouton pour supprimer la dernière version de la base virale de votre disque dur et revenir à la version précédente enregistrée (*la nouvelle version de la base de données sera incluse dans la mise à jour suivante*)

#### 10.10. Anti-Rootkit

Dans la boîte de dialogue **Paramètres Anti-Rootkit**, vous pouvez modifier la configuration du composant [Anti-Rootkit](#) et certains paramètres de l'analyse anti-rootkit. L'analyse anti-rootkit est un processus par défaut inclus dans l'[Analyse complète de l'ordinateur](#) :



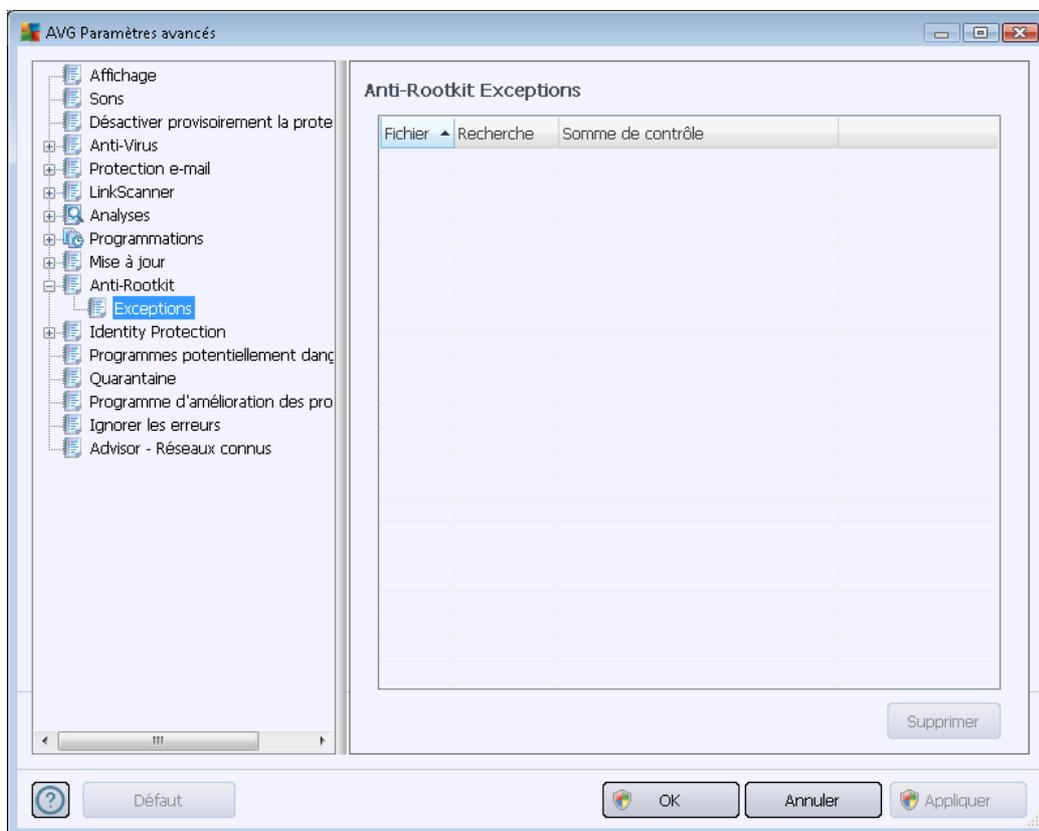
Modifier l'ensemble des fonctions du composant [Anti-Rootkit](#) comme indiqué dans cette boîte de dialogue est également possible directement depuis [l'interface du composant Anti-Rootkit](#).

**Rechercher dans les applications** et **Rechercher parmi les pilotes** vous permettent de préciser en détails les éléments à inclure dans l'analyse Anti-Rootkit. Ces paramètres sont destinés à des utilisateurs chevronnés ; nous vous recommandons de conserver toutes les options actives. Vous pouvez ensuite choisir le mode d'analyse des rootkits :

- **Analyse anti-rootkit rapide** – analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows* )
- **Analyse anti-rootkit complète** – analyse tous les processus en cours d'exécution, les pilotes chargés et le dossier système (*c:\Windows généralement* ), ainsi que tous les disques locaux (*y compris le disque flash, mais pas les lecteurs de disquettes ou de CD-ROM*)

### 10.10.1. Exceptions

Dans la boîte de dialogue **Exceptions Anti-Rootkit**, vous pouvez définir les fichiers spécifiques (*par exemple, certains pilotes qui peuvent être détectés à tort comme étant des rootkits*) qui doivent être exclus de cette analyse :

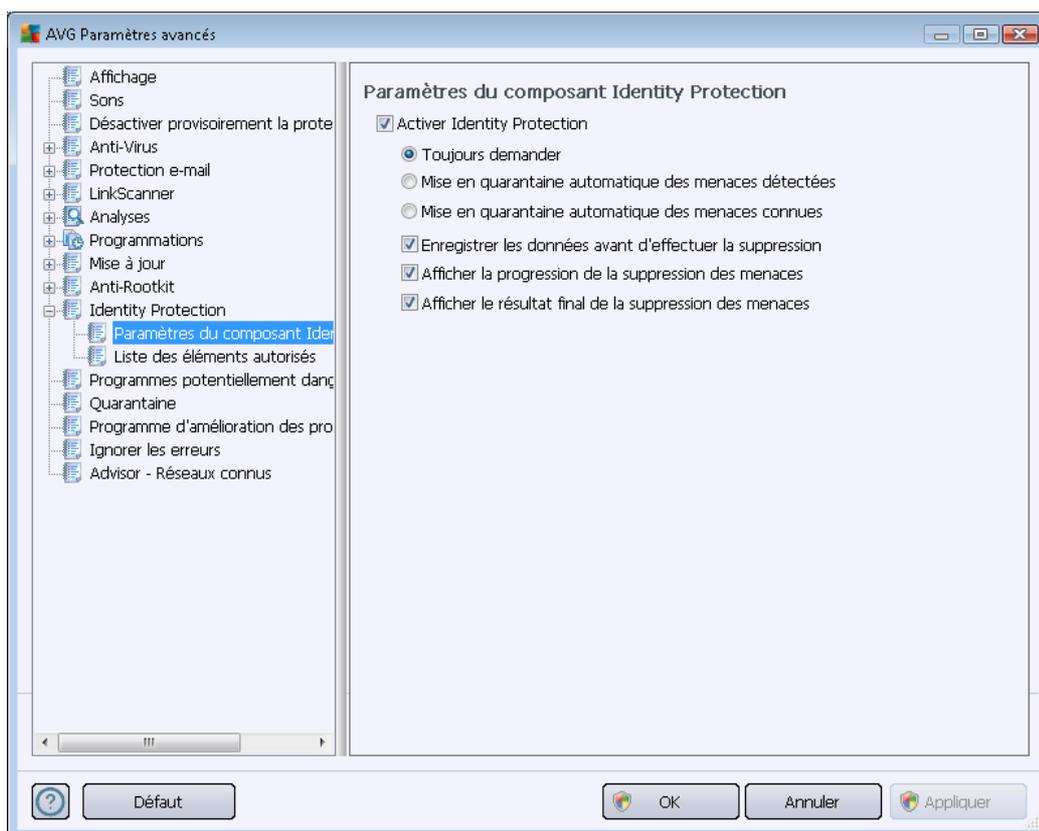


## 10.11. Identity Protection

**Identity Protection** est un composant Anti-malware qui vous protège contre tout type de programme malveillant (*spywares*, *bots*, *usurpation d'identité*, etc.) à l'aide de technologies d'analyse du comportement. Ce programme vous assure une protection de type zero-day contre les nouveaux virus (pour une description détaillée des fonctions du composant, consultez le chapitre [Identity Protection](#)).

### 10.11.1. Paramètres d'Identity Protection

La boîte de dialogue des **paramètres du composant Identity Protection** permet d'activer ou de désactiver les fonctions essentielles du composant [Identity Protection](#) :



**Activer Identity Protection** (option activée par défaut) – désélectionnez cette case pour désactiver le composant [Identity Protection](#).

**Nous recommandons vivement de ne pas le faire, sauf en cas d'absolue nécessité.**

Si le composant [Identity Protection](#) est activé, vous pouvez indiquer l'opération à effectuer lorsqu'une menace est détectée :

- **Toujours demander** (option activée par défaut) - vous avez la possibilité de conserver les paramètres par défaut. Dans ce cas, lorsqu'une menace est détectée, vous êtes invité à confirmer si elle doit être mise en quarantaine pour s'assurer que les applications à exécuter ne sont pas supprimées.
- **Mise en quarantaine automatique des menaces détectées** – cochez cette case pour indiquer que vous voulez placer immédiatement en quarantaine toutes les menaces détectées dans le composant [Quarantaine](#). Vous avez la possibilité de conserver les paramètres par défaut. Dans ce cas, lorsqu'une menace est détectée, vous êtes invité à confirmer si elle doit être mise en quarantaine pour s'assurer que les applications à exécuter ne sont pas supprimées.



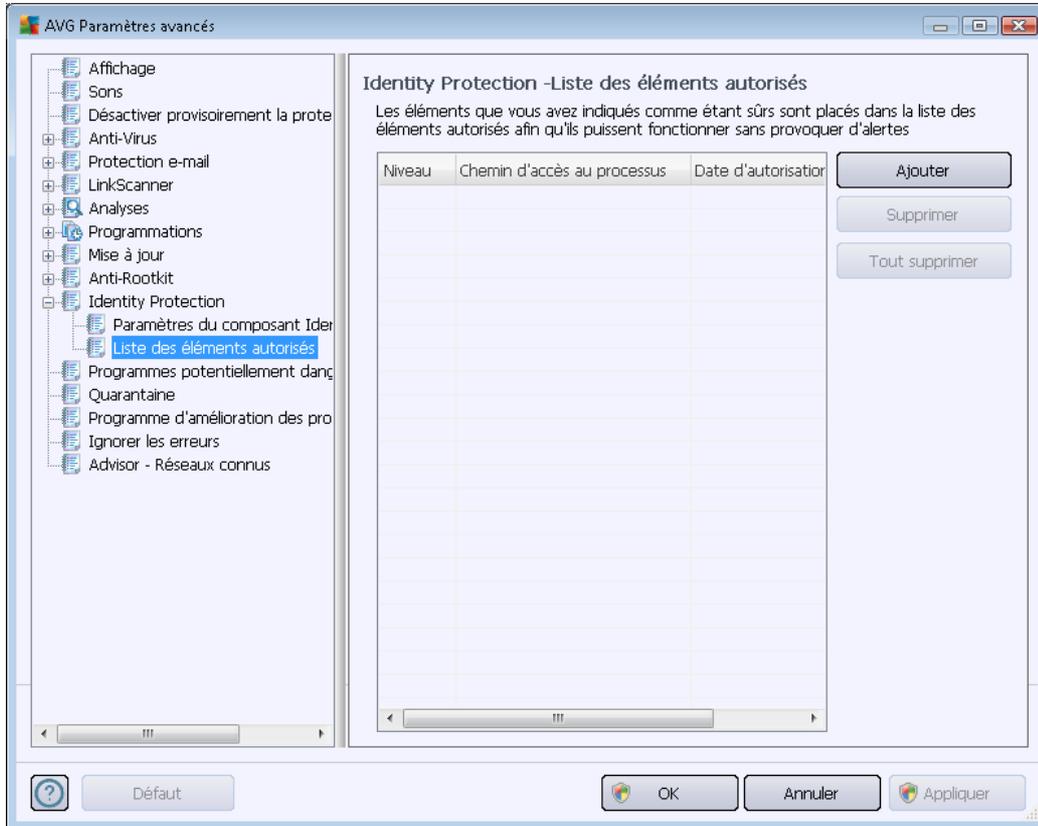
- **Mise en quarantaine automatique des menaces connues** – laissez cette option activée si vous voulez que toutes les applications identifiées comme potentiellement malveillantes soient immédiatement confinées dans [Quarantaine](#).

Par ailleurs, vous pouvez choisir d'autres options pour utiliser éventuellement d'autres options [Identity Protection](#) :

- **Enregistrer les données avant d'effectuer la suppression** – (option activée par défaut) – laissez cette case cochée si vous souhaitez être averti lorsque la quarantaine d'une application détectée comme potentiellement malveillante est levée. Au cas où vous seriez en train de travailler sur l'application, vous devez enregistrer votre travail pour ne pas le perdre. Par défaut, la case est activée et il est recommandé de ne pas modifier ce paramètre.
- **Afficher la progression de la suppression des menaces** - (option activée par défaut) – lorsqu'un programme potentiellement dangereux est détecté, cet élément (activé) permet d'afficher une nouvelle boîte de dialogue indiquant la progression de la mise en quarantaine du programme malveillant.
- **Afficher les détails finaux de la suppression des menaces** - (option activée par défaut) – lorsque cette option est activée, **Identity Protection** affiche des informations détaillées sur chaque objet mis en quarantaine (*niveau de gravité, emplacement, etc.*).

### 10.11.2. Liste des éléments autorisés

Si, dans la boîte de dialogue **Paramètres d'Identity Protection**, vous avez choisi de ne pas activer l'élément **Mise en quarantaine automatique des fichiers détectés**, à chaque fois qu'un programme malveillant potentiellement dangereux est détecté, vous êtes invité à confirmer s'il doit être supprimé. Si vous décidez de définir l'application suspecte comme étant sécurisée (*en vous basant sur son comportement*) et confirmez qu'elle doit être maintenue sur votre ordinateur, celle-ci est ajoutée à la **liste des éléments autorisés d'Identity Protection** et n'est plus signalée comme élément potentiellement dangereux :



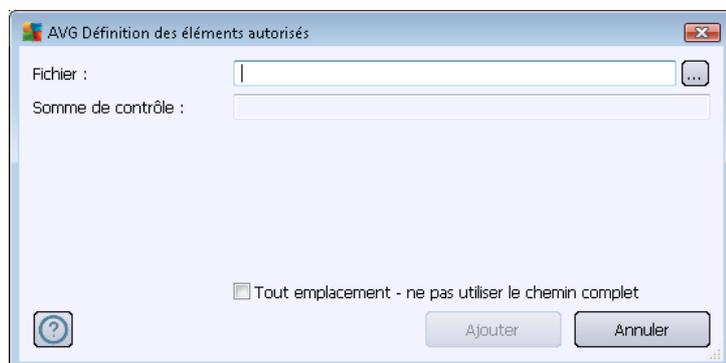
La **liste des éléments autorisée d'Identity Protection** fournit les informations suivantes sur chaque processus :

- **Niveau** – représentation graphique de la gravité du processus en cours sur quatre niveaux allant du moins dangereux (■□□□) au plus grave (■□■□)
- **Chemin d'accès au processus** - chemin d'accès à l'emplacement du fichier exécutable du (*processus*) d'application
- **Date d'autorisation** – date à laquelle l'application a été définie comme étant sécurisée

### Boutons de commande

Les boutons de commande disponibles dans la **Liste des éléments autorisés d'Identity Protection** sont :

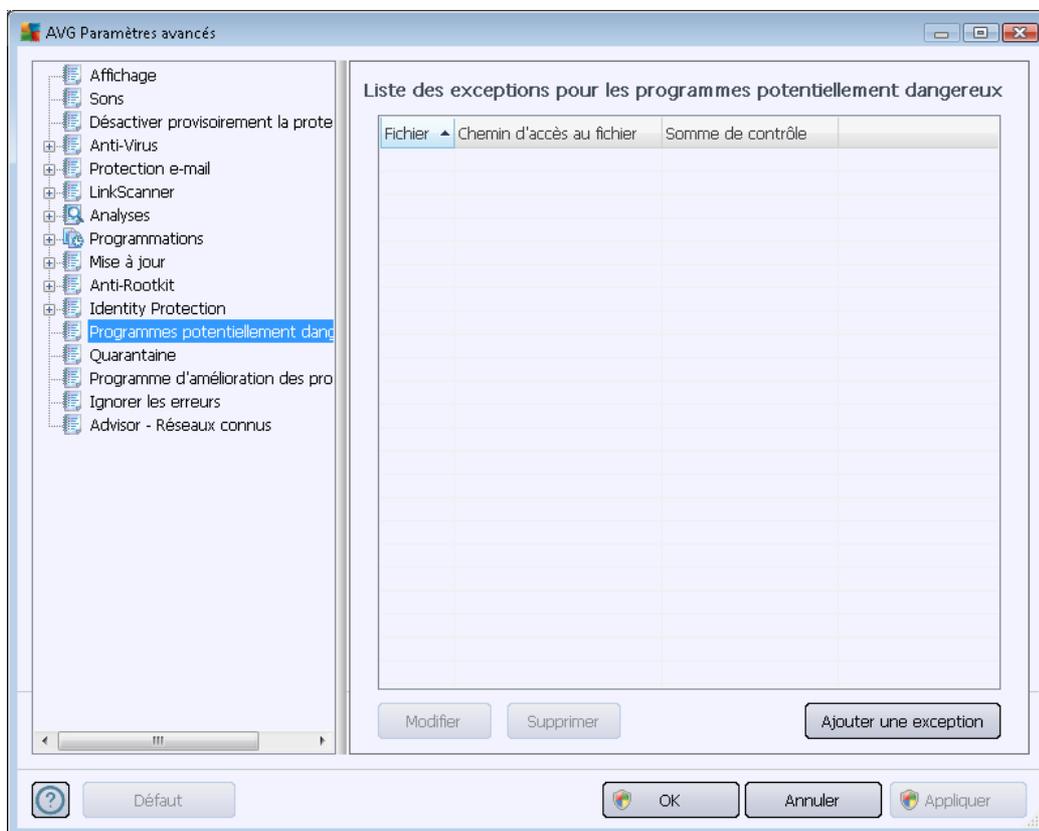
- **Ajouter** - cliquez sur ce bouton pour ajouter un élément à la liste autorisée. La boîte de dialogue suivante s'affiche :



- **Fichier** – spécifiez le chemin d'accès complet du fichier (*de l'application*) à considérer comme étant une exception
  - **Somme de contrôle** – affiche la « signature » unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.
  - **Tout emplacement – ne pas utiliser le chemin complet** – si vous souhaitez définir le fichier comme étant une exception pour un emplacement spécifique, ne cochez pas cette case.
- **Supprimer** - cliquez sur ce bouton pour supprimer l'application sélectionnée de la liste.
  - **Supprimer tout** - cliquez sur ce bouton pour supprimer toutes les applications répertoriées.

## 10.12. Programmes potentiellement dangereux

**AVG Internet Security 2012** est en mesure d'analyser et de détecter des exécutables ou bibliothèques DLL qui peuvent s'avérer malveillants pour le système. Dans certains cas, il est possible que l'utilisateur souhaite conserver certains programmes considérés comme potentiellement dangereux sur l'ordinateur (ceux installés volontairement, par exemple). Certains programmes, et notamment ceux fournis gratuitement, font partie de la famille des adwares. **AVG Internet Security 2012** peut détecter et signaler ces adwares au nombre des *programmes potentiellement dangereux*. Si vous souhaitez malgré tout le conserver sur votre ordinateur, il suffit de le définir comme une exception de programme potentiellement dangereux :



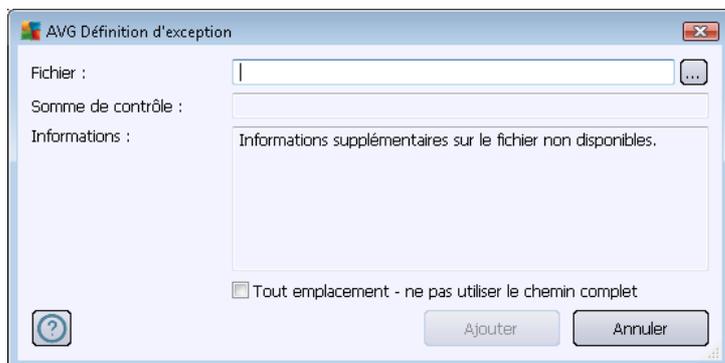
La boîte de dialogue **Liste des exceptions pour les programmes potentiellement dangereux** dresse la liste des exceptions déjà définies et actuellement valides par rapport aux programmes indésirables. Vous pouvez modifier la liste, supprimer des éléments existants ou ajouter une nouvelle exception. Vous trouverez les informations suivantes dans la liste de chaque exception :

- **Fichier** - indique le nom exact de l'application correspondante
- **Chemin d'accès au fichier** - indique le chemin d'accès à l'emplacement de l'application
- **Somme de contrôle** – affiche la signature unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.

### Boutons de commande

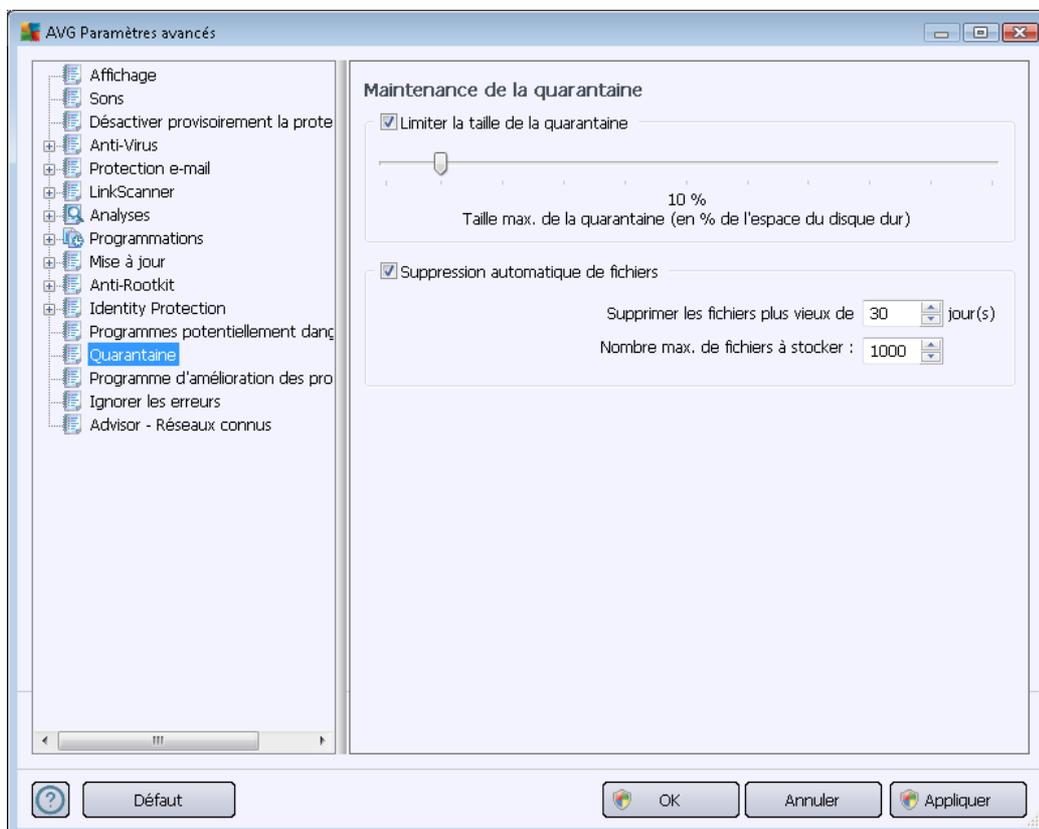
- **Modifier** - ouvre une boîte de dialogue d'édition (*identique à la boîte de dialogue permettant de définir une nouvelle exception, voir ci-dessus*) d'une exception déjà définie dans laquelle vous modifiez les paramètres de l'exception
- **Supprimer** - supprime l'élément sélectionné de la liste des exceptions
- **Ajouter une exception** – ouvre une boîte de dialogue dans laquelle vous définissez les

paramètres de l'exception à créer :



- **Fichier** – spécifiez le chemin d'accès complet du fichier à identifier comme étant une exception
- **Somme de contrôle** – affiche la "signature" unique du fichier choisi. Il s'agit d'une chaîne de caractères générée automatiquement, qui permet à AVG de distinguer sans risque d'erreur ce fichier parmi tous les autres. La somme de contrôle est générée et affichée une fois le fichier ajouté.
- **Informations** – affiche des informations supplémentaires sur le fichier (*licence, version, etc.*)
- **Tout emplacement – ne pas utiliser le chemin complet** – si vous souhaitez définir ce fichier comme une exception uniquement pour un emplacement spécifique, veillez à ne pas cocher cette case. Si la case est cochée, le fichier mentionné est défini en tant qu'exception, indifféremment de son emplacement (*vous devez malgré tout indiquer le chemin d'accès complet du fichier ; le fichier servira alors d'exemple unique au cas où le système comporte deux fichiers portant le même nom*).

## 10.13. Quarantaine



La boîte de dialogue **Maintenance de la quarantaine** permet de définir plusieurs paramètres liés à l'administration des objets stockés dans le module [Quarantaine](#) :

- **Limiter la taille de la quarantaine** – utilisez le curseur pour ajuster la taille de la [quarantaine](#). La taille est indiquée par rapport à la taille de votre disque local.
- **Suppression automatique de fichiers** – dans cette section, définissez la durée maximale de conservation des objets en [quarantaine](#) (**Supprimer les fichiers plus vieux de ... jour (s)**) ainsi que le nombre maximal de fichiers à conserver en [quarantaine](#) (**Nombre max. de fichiers à stocker**).

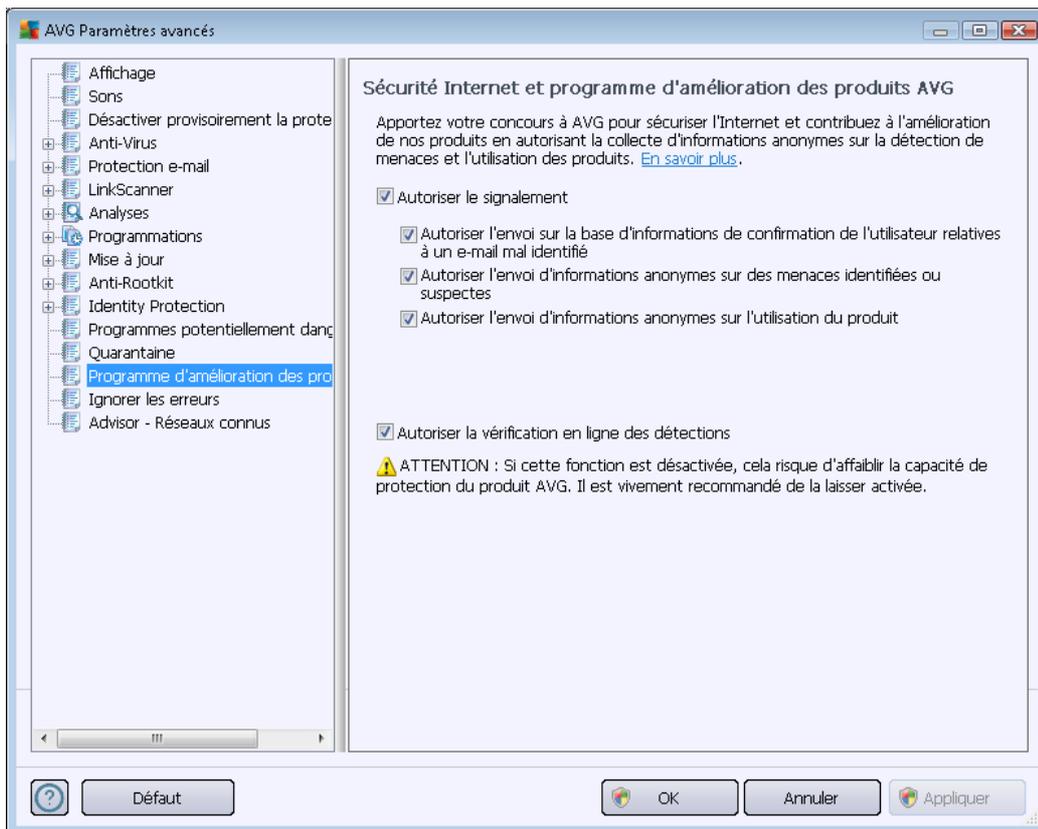
## 10.14. Programme d'amélioration des produits

La boîte de dialogue **Sécurité Internet et programme d'amélioration des produits AVG** vous invite à contribuer à l'amélioration des produits AVG et à une plus grande sécurité sur Internet. Cochez l'option **Autoriser le signalement** pour transmettre les menaces détectées aux laboratoires d'AVG. Ainsi, nous pourrions recueillir les dernières informations sur les nouvelles menaces signalées par les internautes du monde entier et, en retour, fournir à tous une meilleure protection en ligne.

**La création de rapports est assurée automatiquement. Il n'en résulte aucune gêne pour les utilisateurs. Notez par ailleurs qu'aucune donnée personnelle n'est incluse dans ces rapports.**



Le signalement des menaces détectées est facultatif. Cependant, nous vous demandons de ne pas désactiver cette option. Elle nous permet d'améliorer votre protection et celle des autres utilisateurs d'AVG.



Les options de configuration suivantes sont disponibles dans la boîte de dialogue :

- **Autoriser le signalement (activée par défaut)** - cochez cette case si vous souhaitez nous aider à améliorer davantage **AVG Internet Security 2012**. Ainsi, toutes les menaces seront signalées à AVG. Ce faisant, nous pourrions recueillir les dernières informations sur les nouvelles menaces signalées par les internautes du monde entier et, en retour, fournir à tous une meilleure protection en ligne. La création de rapports est assurée automatiquement. Il n'en résulte aucune gêne pour les utilisateurs. Notez par ailleurs qu'aucune donnée personnelle n'est incluse dans ces rapports.
  - **Autoriser l'envoi sur la base d'informations de confirmation de l'utilisateur, relatives à un e-mail mal identifié (activée par défaut)** – envoyez des informations sur des messages assimilés, par erreur, à du spam, ou sur du spam non détecté par le composant [Anti-Spam](#). Vous serez amené à confirmer l'envoi de ce genre d'informations.
  - **Autoriser l'envoi d'informations anonymes sur des menaces identifiées ou suspectes (activée par défaut)** – cette option permet d'envoyer des informations sur un code suspect ou dangereux ou un type de comportement (*il peut s'agir d'un virus, d'un spyware ou d'une page Web malveillante*) détecté sur l'ordinateur.



- **Autoriser l'envoi d'informations anonymes sur l'utilisation du produit (activée par défaut)** – cette option permet d'envoyer des données statistiques sur l'utilisation de l'application, comme le nombre de détections, les analyses exécutées, les mises à jour réussies ou non, etc.
- **Autoriser la vérification en ligne des détections (activée par défaut)** - les menaces détectées seront examinées pour en exclure les faux positifs.

### Menaces les plus répandues

De nos jours, les simples virus représentent une infime partie des menaces. Les auteurs de codes malveillants et de sites Web piégés sont à la pointe de l'innovation et de nouveaux types de menaces ne cessent de voir le jour principalement sur Internet. Voici les plus courants :

- **Un virus** est un code malveillant qui se multiplie et se propage souvent en passant inaperçu jusqu'à ce qu'il ait accompli son action. Certains virus constituent une menace non négligeable : ils suppriment ou modifient intentionnellement des fichiers sur leur passage. D'autres ont une action relativement moins nocive comme jouer un air de musique. Toutefois, tous les virus sont dangereux en raison de leur capacité de multiplication et de propagation, qui leur permet d'occuper intégralement l'espace mémoire d'un ordinateur en quelques instants et de provoquer une défaillance générale du système.
- **Un ver** est une sous-catégorie de virus qui, contrairement à ce dernier, n'a pas besoin d'un objet porteur et peut se propager tout seul à d'autres ordinateurs, généralement dans un e-mail, et provoquer une surcharge des serveurs de messagerie et des systèmes réseau.
- **Un spyware** se définit généralement comme une catégorie de malwares (*logiciels malveillants comportant des virus*) qui comprend des programmes (généralement des chevaux de Troie), conçus pour subtiliser des informations personnelles, des mots de passe, des numéros de carte de crédit ; ou pour infiltrer des ordinateurs et permettre aux intrus d'en prendre le contrôle à distance sans l'autorisation et à l'insu de leur propriétaire.
- **Les programmes potentiellement dangereux** forment une catégorie de codes espions qui ne sont pas nécessairement dangereux. Un adware est un exemple spécifique de programme potentiellement dangereux. Ce logiciel est spécifiquement conçu pour diffuser des publicités, généralement dans des fenêtres contextuelles intempestives, mais non malveillantes.
- **Par ailleurs, les tracking cookies** peuvent être considérés comme en faisant partie car ces petits fichiers, stockés dans le navigateur Web et envoyés automatiquement au site Web "parent" lors de votre visite suivante, peuvent contenir des données comme votre historique de navigation et d'autres informations comparables.
- **Un exploit** est un programme malveillant qui exploite une faille du système d'exploitation, du navigateur Internet ou d'un autre programme essentiel.
- **Une opération de phishing** consiste à tenter d'acquérir des informations confidentielles en se faisant passer pour une société connue et fiable. En règle générale, les victimes potentielles sont harcelées par des messages leur demandant de mettre à jour leurs coordonnées bancaires. Pour ce faire, elles sont invitées à suivre un lien qui les mène

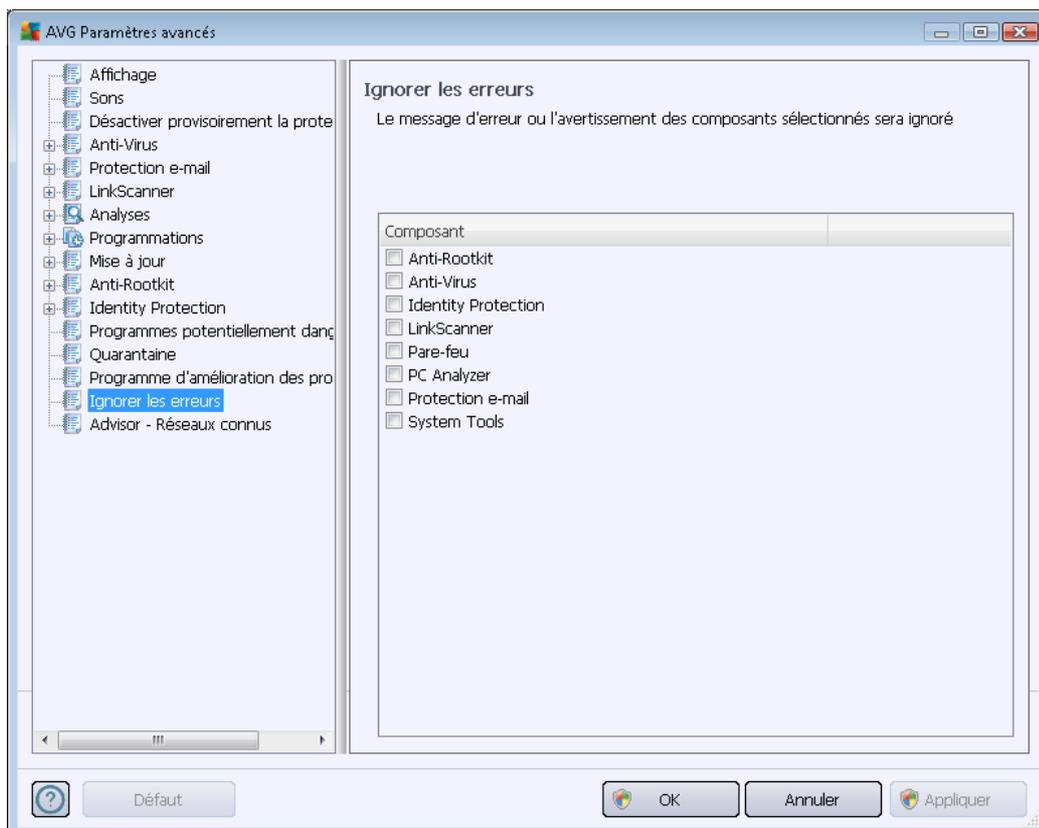
jusqu'à un site bancaire fictif.

- **Le canular (hoax) est un mail envoyé en masse contenant des informations dangereuses, alarmistes ou simplement dénuées d'intérêt.** La plupart de ces menaces utilisent des mails de type canular pour se propager.
- **Les sites Web malveillants** opèrent en installant des programmes malveillants sur votre ordinateur. Les sites piratés font de même, à ceci près que ce sont des sites Web légitimes qui ont été contaminés par des visiteurs.

**AVG Internet Security 2012 comporte des composants spécialement conçus pour vous protéger de ces différents types de menaces. Pour une brève description de ces composants, consultez le chapitre [Présentation des composants](#).**

## 10.15. Ignorer les erreurs

Dans la boîte de dialogue **Ignorer les erreurs**, vous pouvez cocher les composants dont vous ne souhaitez pas connaître l'état :



Par défaut, aucun composant n'est sélectionné dans cette liste. Dans ce cas, si l'état d'un des composants est incorrect, vous en serez immédiatement informé par le biais des éléments suivants :

- [icône de la barre d'état système](#) – si tous les composants d'AVG fonctionnent



correctement, l'icône apparaît en quatre couleurs ; cependant, si une erreur se produit l'icône apparaît avec un point d'exclamation de couleur jaune,

- Description du problème existant dans la section relative à l'[état de sécurité](#) de la fenêtre principale d'AVG.

Il peut arriver que pour une raison particulière, vous soyez amené à désactiver provisoirement un composant (*cela n'est pas recommandé ; vous devez toujours veiller à maintenir les composants activés et appliquer la configuration par défaut*). Dans ce cas, l'icône dans la barre d'état système signale automatiquement une erreur au niveau du composant. Toutefois, il est impropre de parler d'erreur alors que vous avez délibérément provoqué la situation à l'origine du problème et que vous êtes conscient du risque potentiel. Parallèlement, dès qu'elle apparaît en couleurs pastels, l'icône ne peut plus signaler toute autre erreur susceptible d'apparaître par la suite.

Aussi, dans la boîte de dialogue ci-dessus, sélectionnez les composants qui risquent de présenter une erreur (*composants désactivés*) dont vous voulez ignorer l'état. Une option similaire, *Ignorer l'état du composant*, est également disponible pour certains composants dans la [présentation des composants de la fenêtre principale d'AVG](#).

## 10.16. Advisor – Réseaux connus

L'outil [AVG Advisor](#) comprend une fonction surveillant les réseaux auxquels vous vous connectez. Lorsqu'un nouveau réseau est disponible (*portant un nom réseau déjà utilisé, ce qui peut prêter à confusion*), il vous en informe et vous recommande de vérifier la sécurité de ce réseau. Si vous décidez que ce nouveau réseau est sécurisé, vous pouvez également l'enregistrer dans cette liste. [AVG Advisor](#) mémorise alors les attributs uniques de ce réseau (*en particulier l'adresse MAC*) et n'affichera plus la notification de ce réseau.

Depuis cette boîte de dialogue, vous pouvez vérifier quels réseaux vous avez précédemment enregistrés comme des réseaux connus. Vous pouvez supprimer des entrées individuelles en cliquant sur le bouton **Supprimer**. Le réseau correspondant sera alors à nouveau considéré comme inconnu et potentiellement non sûr.

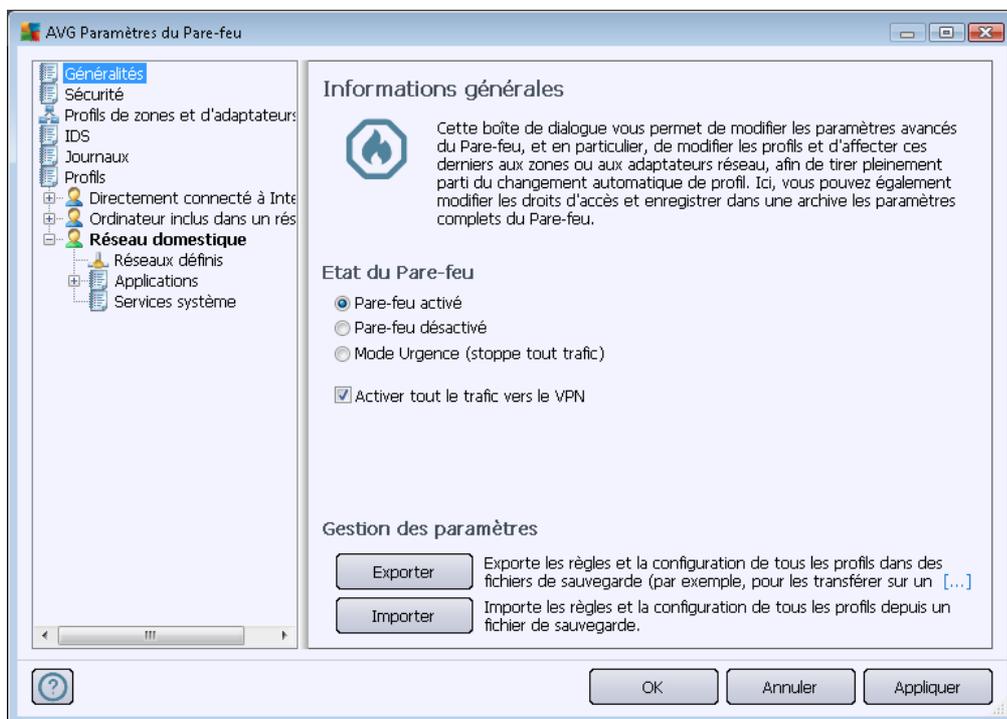
## 11. Paramètres du Pare-feu

La configuration du [Pare-feu](#) s'affiche au sein d'une nouvelle fenêtre à partir de laquelle vous accédez à plusieurs boîtes de dialogue et configurez les paramètres avancés du composant.

**Toutefois, l'éditeur du logiciel a configuré tous les composants d'AVG Internet Security 2012 de manière à en optimiser les performances. Il est déconseillé de modifier la configuration par défaut du composant sans motif valable. Toute modification de ces paramètres doit être uniquement réalisée par un utilisateur expérimenté !**

### 11.1. Généralités

La boîte de dialogue **Informations générales** comprend deux sections :



#### Etat du Pare-feu

Dans cette section, vous pouvez modifier l'état du [Pare-feu](#) à votre gré :

- **Pare-feu activé** – sélectionnez cette option pour autoriser la communication avec les applications dont le jeu de règles est « Autorisé » dans le profil de [Pare-feu sélectionné](#).
- **Pare-feu désactivé** – cette option désactive intégralement le [Pare-feu](#) : l'ensemble du trafic réseau est autorisé sans aucune vérification.
- **Mode Urgence (bloque tout le trafic Internet)** - cette option vise à bloquer l'ensemble du trafic sur chaque port réseau ; le [Pare-feu](#) fonctionne, mais tout trafic réseau est stoppé.



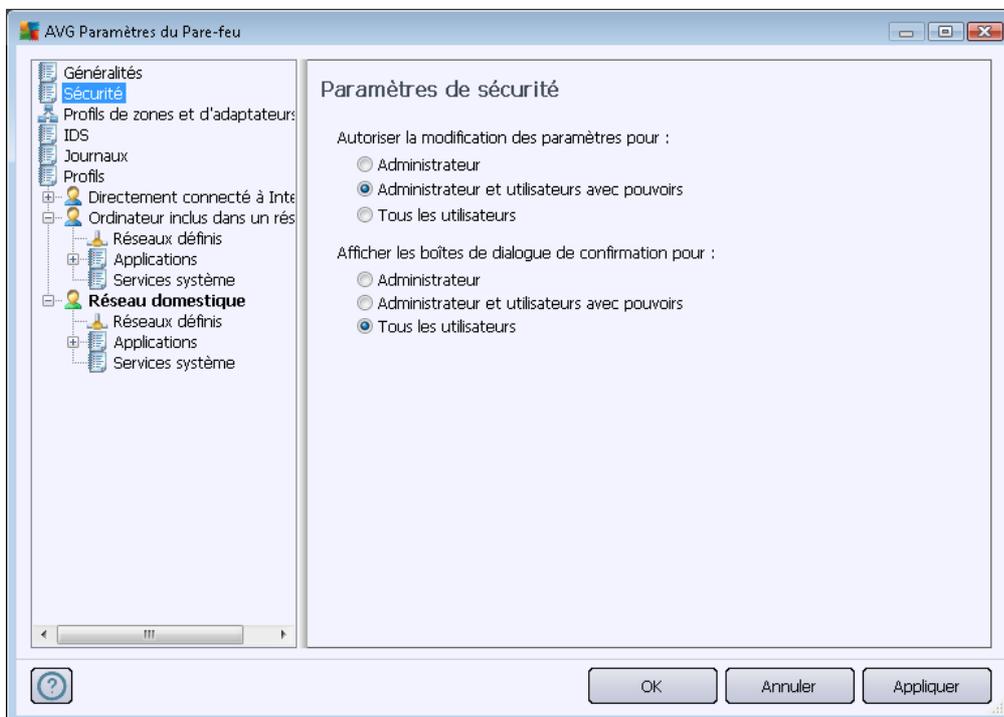
- **Activer tout le trafic vers le VPN (activé par défaut)** – si vous utilisez une connexion VPN (Réseau privé virtuel), par exemple pour vous connecter à votre bureau depuis votre domicile, nous vous recommandons de cocher cette case. **Le Pare-feu AVG** va automatiquement rechercher les adaptateurs de votre réseau pour identifier ceux utilisés pour la connexion VPN et permettre à toutes les applications de se connecter au réseau cible (ne s'applique qu'aux applications pour lesquelles aucune règle spécifique n'est définie par le Pare-feu). Sur un système standard doté d'adaptateurs réseau ordinaires, cette étape simple devrait vous éviter d'avoir à configurer une règle spécifique pour chaque application que vous voulez utiliser sur le VPN.

**Remarque:** pour activer la connexion VPN, il faut autoriser la communication avec les protocoles système suivants: GRE, ESP, L2TP, PPTP. Vous pouvez le faire dans la boîte de dialogue [Services système](#).

## Généralités

Dans la section **Gestion des paramètres**, vous avez la possibilité d'**exporter** et d'**importer** la configuration du [Pare-feu](#), à savoir d'exporter les règles et paramètres définis pour le [Pare-feu](#) dans les fichiers de sauvegarde ou, à l'inverse, en importer le contenu entier depuis un fichier de sauvegarde.

## 11.2. Sécurité



Dans la boîte de dialogue **Paramètres de sécurité**, vous pouvez définir les règles générales du comportement du [Pare-feu](#) et ce, indépendamment du profil sélectionné :



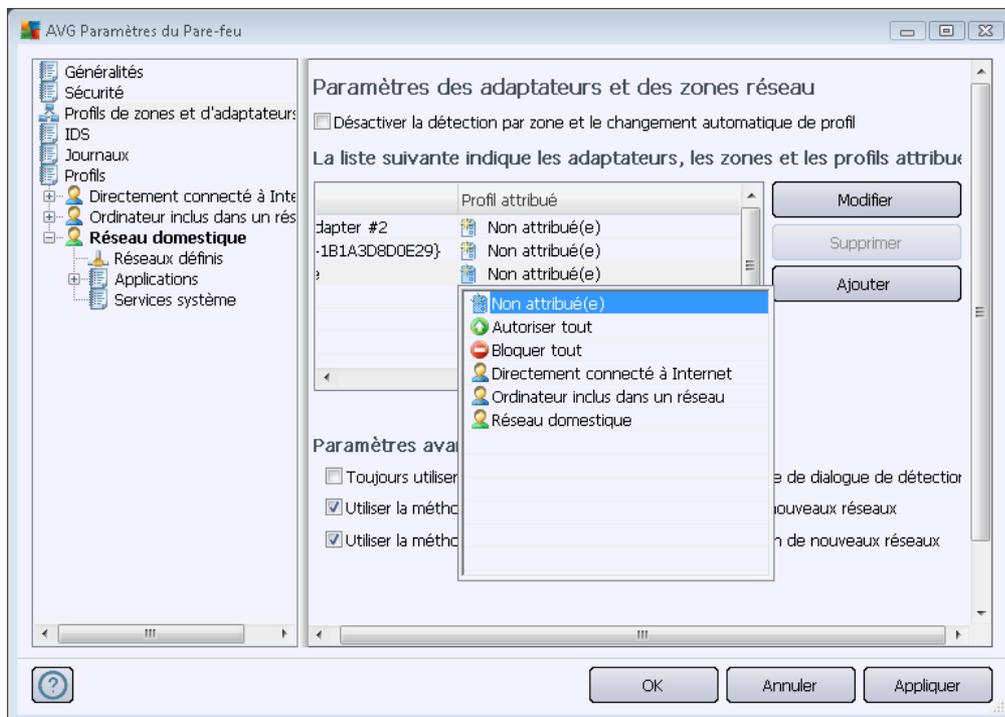
- **Autoriser la modification des paramètres pour** – spécifiez les personnes habilitées à adapter la configuration du [Pare-feu](#).
- **Afficher les boîtes de dialogue de confirmation pour** – spécifier les personnes auxquelles présenter les demandes de confirmation (*boîtes de dialogue sollicitant la décision de l'utilisateur dans les situations où aucune règle définie du [Pare-feu](#) n'est applicable*).

Pour ces deux options, il est possible d'attribuer l'autorisation spécifique à l'un des groupes utilisateurs suivants :

- **Administrateur** – l'administrateur bénéficie d'un contrôle total sur le PC et a le droit d'affecter les utilisateurs à des groupes jouissant de droits spécifiques.
- **Administrateur et Utilisateurs avec pouvoirs** – l'administrateur a le droit d'affecter chaque utilisateur à un groupe spécifique (*Utilisateurs avec pouvoirs*) et de définir les droits des membres du groupe.
- **Tous les utilisateurs** – ensemble des autres utilisateurs n'appartenant à aucun groupe particulier.

### 11.3. Profils de zones et d'adaptateurs

La boîte de dialogue **Paramètres des adaptateurs et des zones réseau** permet de modifier les paramètres liés à l'attribution de profils définis à des adaptateurs déterminés, ainsi que la référence des réseaux correspondants :



- **Désactiver la détection par zone et le changement automatique de profil (désactivé par défaut)** - Un profil défini peut être affecté à chaque type d'interface réseau, c'est-à-dire à chaque zone. Si vous ne voulez pas définir de profils, le profil courant sera utilisé. Si vous décidez de différencier des profils et de les attribuer à des adaptateurs et à des zones spécifiques puis, pour une raison quelconque, souhaitez désactiver temporairement ce dispositif, il suffit de cocher l'option **Désactiver la détection par zone et le changement automatique de profil**.
- **La liste suivante indique les adaptateurs, les zones et les profils attribués** – Cette liste présente les adaptateurs et les zones détectés. Un profil spécifique peut être attribué à chacun d'eux à partir du menu des profils définis. Pour ouvrir ce menu, cliquez avec le bouton gauche sur l'élément correspondant dans la liste des adaptateurs (*dans la colonne Profil affecté*), puis sélectionnez le profil dans le menu contextuel.

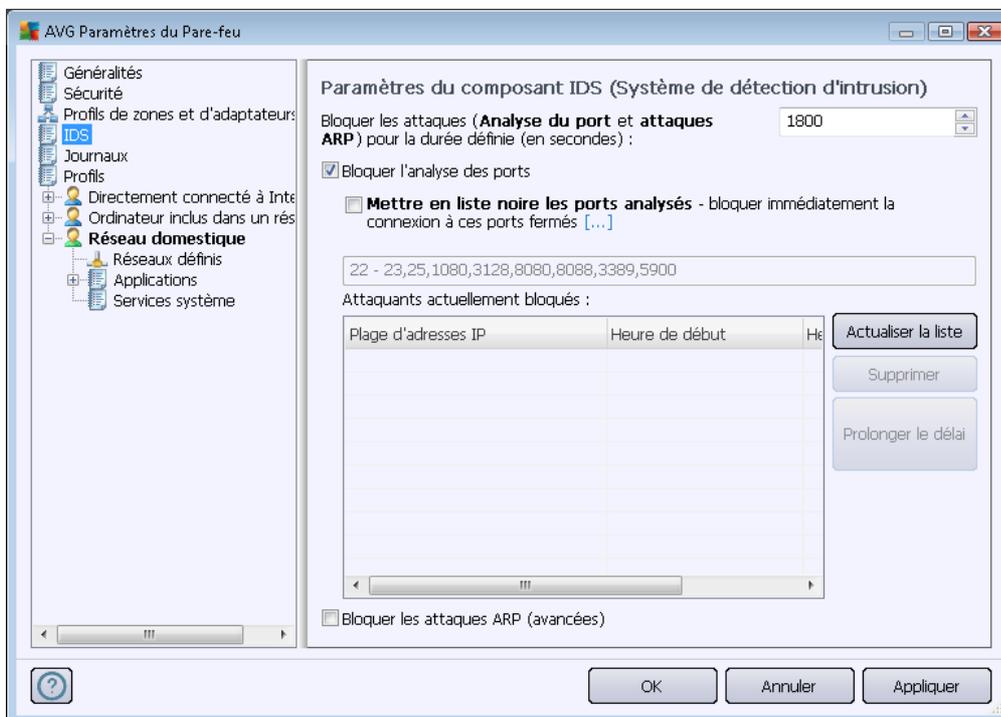
### Paramètres avancés

- **Toujours utiliser le profil par défaut et ne pas afficher la boîte de dialogue de détection d'un nouveau réseau** : quand l'ordinateur se connecte à un nouveau réseau, le [Pare-feu](#) le signale et affiche une boîte de dialogue dans laquelle vous pouvez définir un type de connexion réseau et lui affecter un [Profil de pare-feu](#). Si vous ne souhaitez pas voir cette boîte de dialogue s'afficher, cochez cette case.
- **Utiliser la méthode heuristique d'AVG pour la détection de nouveaux réseaux** - Permet de collecter des informations sur un réseau récemment détecté grâce au mécanisme propre à AVG (*cependant, cette option n'est disponible que pour le système d'exploitation VISTA, ou versions supérieures*).

- **Utiliser la méthode heuristique de Microsoft pour la détection de nouveaux réseaux** - Permet de récupérer des informations sur un réseau récemment détecté par le service Windows (*cette option est disponible pour Windows Vista ou versions supérieures*).

## 11.4. IDS

Le composant Intrusion Detection System (système de détection d'intrusion) est une fonctionnalité d'analyse des comportements spécialement conçue pour identifier et bloquer les tentatives de communication suspectes sur des ports spécifiques de votre ordinateur. Vous pouvez configurer les paramètres IDS dans la boîte de dialogue **Paramètres du composant IDS (Intrusion Detection System, système de détection d'intrusion)**.



La boîte de dialogue **Paramètres du composant IDS (Intrusion Detection System, système de détection d'intrusion)** présente les options de configuration suivantes :

- **Bloquer (analyse de ports et attaques ARP) les attaques pour une durée définie :** Permet de définir le temps (en secondes) durant lequel un port doit être bloqué, chaque fois qu'une tentative de communication suspecte y est détectée. Par défaut, ce laps de temps est fixé à 1 800 secondes (30 minutes).
- **Bloquer l'analyse des ports (activée par défaut) :** Cochez cette case pour bloquer les tentatives de communication entrante sur tous les ports TCP et UDP. Pour ce type de connexion, cinq tentatives sont autorisées, la sixième est bloquée. L'option est activée par défaut et il est recommandé de ne pas la désactiver. Si vous laissez l'option **Bloquer l'analyse des ports** activée, des options de configuration détaillée sont disponibles (*sinon, l'option suivante est désactivée*) :

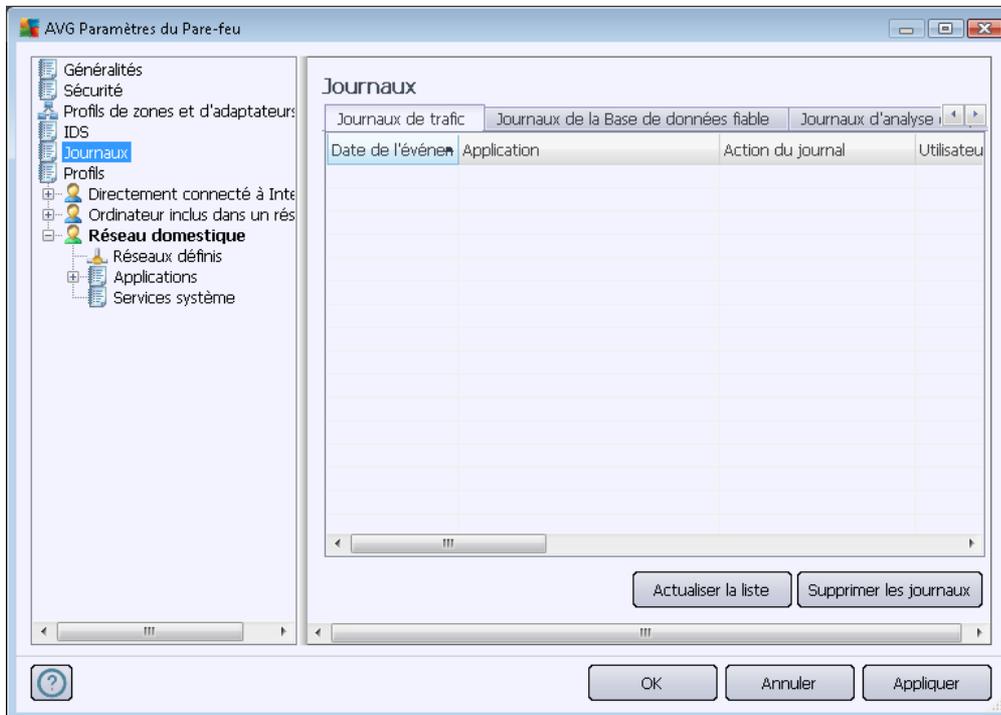


- **Mettre en liste noire les ports analysés** : Cochez cette case pour bloquer immédiatement toute tentative de communication sur les ports indiqués dans la zone de texte ci-dessous. Les ports individuels ou les plages de ports doivent être séparés par des virgules. Une liste prédéfinie de ports recommandés est disponible, si vous souhaitez utiliser cette fonctionnalité.
- Attaquants actuellement bloqués : Cette section répertorie les tentatives de communication bloquées par le [Pare-feu](#). L'historique complet des tentatives bloquées peut être consulté dans la boîte de dialogue [Journaux](#), (onglet *Journaux d'analyse des ports*).
- **Bloquer les attaques ARP (avancé) (désactivée par défaut)** : Cochez cette option pour activer le blocage de certains types de tentatives de communication au sein d'un réseau local que le composant **IDS** a signalé comme étant potentiellement dangereuses. Le délai fixé dans la zone **Bloquer les attaques pour la durée définie prend alors effet**. Nous recommandons l'utilisation de cette fonctionnalité uniquement aux utilisateurs expérimentés, maîtrisant le type et le niveau de risque de leur réseau local.

### Boutons de commande

- **Actualiser la liste** – cliquez sur le bouton pour mettre à jour la liste (*pour inclure toute tentative bloquée récemment*)
- **Supprimer** – cliquez sur ce bouton pour annuler le blocage sélectionné
- **Prolonger le délai** – cette option permet de prolonger la période pendant laquelle une tentative donnée est bloquée. Une nouvelle boîte de dialogue avec des options supplémentaires s'ouvre afin de vous permettre de définir une heure et une date spécifiques ou une durée illimitée.

## 11.5. Journaux



La boîte de dialogue **Journaux** permet de passer en revue l'ensemble des actions et des événements du **Pare-feu** qui ont été enregistrés ainsi que la description détaillée des paramètres associés (*date de l'évènement, nom de l'application, action du journal correspondante, nom d'utilisateur, PID, direction du trafic, type de protocole, numéros des ports locaux et distants, etc.*) sur quatre onglets :

- **Journaux de trafic** - cet onglet fournit des informations sur l'activité de toutes les applications qui ont essayé de se connecter au réseau.
- **Journaux de la base de données fiable** - la *Base de données fiable* désigne les informations entrées dans la base de données interne d'AVG relatives aux applications certifiées et fiables pouvant toujours être autorisées à communiquer en ligne. Lorsqu'une nouvelle application tente pour la première fois de se connecter au réseau (*c'est-à-dire, lorsque aucune règle de pare-feu n'a encore été spécifiée pour cette application*), vous devez déterminer si la communication réseau doit être autorisée pour l'application correspondante. AVG recherche d'abord la *Base de données fiable*. Si l'application est répertoriée, elle sera automatiquement autorisée à accéder au réseau. Uniquement après cette opération, s'il n'existe aucune information relative à l'application disponible dans la base de données, vous serez invité à indiquer, dans une nouvelle fenêtre, si l'application doit être autorisée à accéder au réseau.
- **Journaux d'analyse des ports** – fournit de toutes les activités [Intrusion Detection System](#).
- **Journaux ARP** – enregistrement d'informations relatives au blocage de certains types de tentatives de communication au sein d'un réseau local (option [Bloquer les attaques ARP](#)) détectées par le système [Intrusion Detection System](#) comme présentant un risque

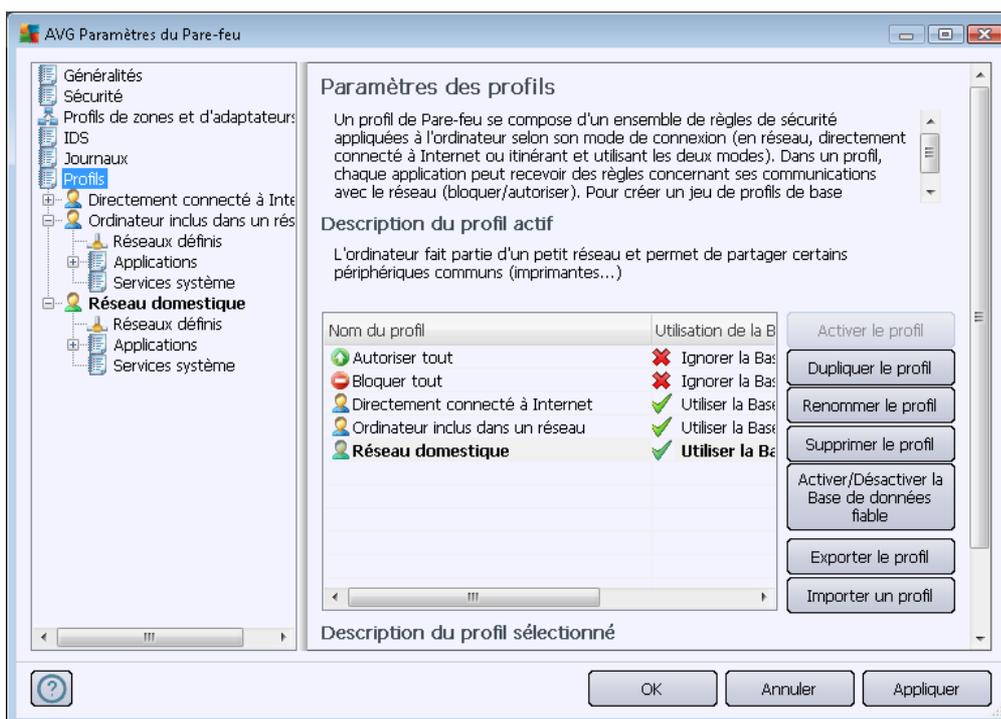
potentiel.

### Boutons de commande

- **Actualiser la liste** - il est possible de réorganiser les paramètres enregistrés dans le journal en fonction de l'attribut choisi : par ordre chronologique (*dates*) ou alphabétique (*autres colonnes*). Pour cela, il suffit de cliquer sur l'en-tête de colonne qui convient. Cliquez sur le bouton **Actualiser la liste** pour mettre à jour les informations affichées.
- **Supprimer les journaux** – supprime toutes les entrées du tableau.

## 11.6. Profils

La boîte de dialogue **Paramètres des profils** inclut la liste de tous les profils disponibles:



Il est impossible de modifier les profils système (*Autoriser tout*, *Bloquer tout*). En revanche, tous les [profils](#) personnalisés (*Directement connecté à Internet*, *Ordinateur inclus dans un réseau*, *Réseau domestique*) peuvent être modifiés directement dans cette boîte de dialogue à l'aide des boutons de commande suivants :

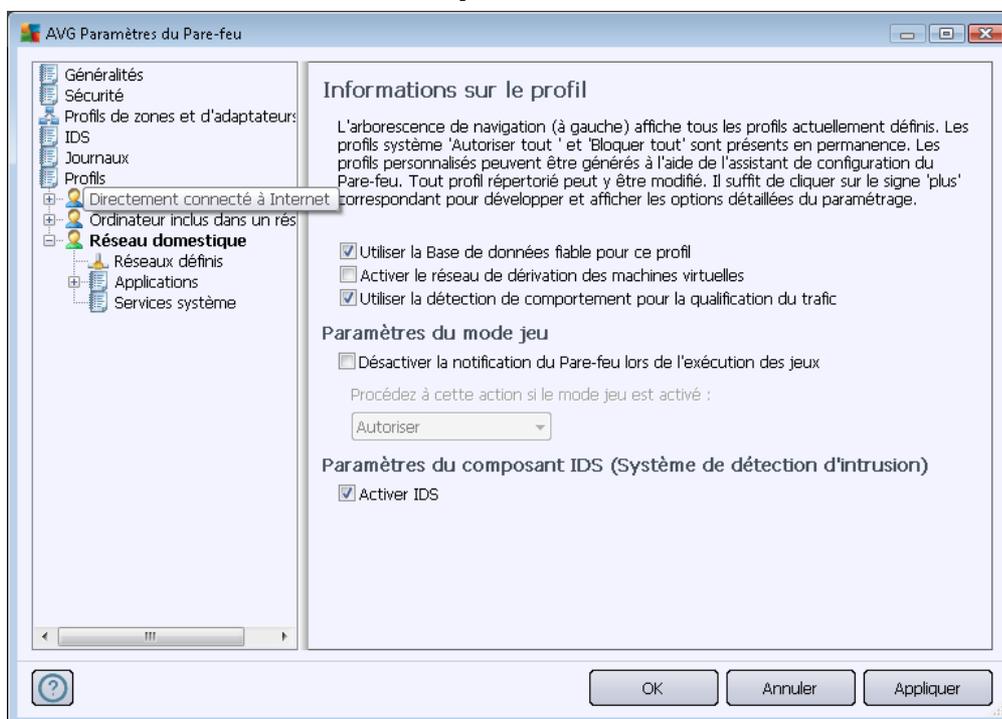
- **Activer le profil** – ce bouton définit le profil sélectionné comme étant actif. La configuration de ce profil sera alors utilisée par le [Pare-feu](#) pour contrôler le trafic réseau.
- **Dupliquer le profil**- génère une copie conforme du profil sélectionné ; vous pouvez ensuite modifier la copie et la renommer pour obtenir un nouveau profil.

- **Renommer le profil** – permet d'attribuer un nouveau nom au profil sélectionné.
- **Supprimer le profil** – retire le profil sélectionné de la liste.
- **Activer/Désactiver la Base de données fiable** - pour le profil sélectionné, vous pouvez décider d'utiliser les informations de la *Base de données fiable* (la *Base de données fiable* désigne les données contenues dans la base de données interne d'AVG relatives aux applications fiables et certifiées pouvant toujours être autorisées à communiquer en ligne.).
- **Exporter le profil** – enregistre la configuration du profil sélectionné dans un fichier en vue d'une utilisation ultérieure.
- **Importer un profil** - configure les paramètres du profil sélectionné en fonction des données exportées depuis le fichier de configuration de sauvegarde.

Dans la partie inférieure de la boîte de dialogue, vous trouverez la description du profil actuellement sélectionné dans la liste.

L'arborescence de navigation située à gauche diffère selon le nombre de profils définis qui figurent dans la liste au sein de la boîte de dialogue **Profil**. Chaque profil défini correspond à une branche spécifique placée sous l'entrée **Profil**. Il est possible de modifier les profils dans les boîtes de dialogue suivantes (*identiques pour tous les profils*) :

### 11.6.1. Informations sur le profil



La boîte de dialogue **Informations sur le profil** est la première d'une série de boîtes de dialogue permettant de modifier les paramètres de configuration des profils. A chaque boîte de dialogue correspond un profil.



- **Utiliser la base de données fiable pour ce profil** (option activée par défaut) – cochez cette option pour activer la *base de données fiable* (, c'est-à-dire la base de données interne de collecte d'informations AVG relatives aux applications fiables et certifiées communiquant en ligne. Aucune règle n'a encore été spécifiée pour l'application correspondante. Vous devez déterminer s'il faut autoriser cette application à accéder au réseau. AVG a d'abord effectué une recherche dans la base de données fiable. Si l'application est répertoriée, elle sera considérée comme sécurisée et sera autorisée à communiquer sur le réseau. Sinon, vous serez invité à indiquer si l'application doit être autorisée à communiquer sur le réseau pour le profil approprié.
- **Activer le réseau de dérivation des machines virtuelles** (option désactivée par défaut) – cochez cette case pour permettre aux machines virtuelles VMware de se connecter directement au réseau.
- **Utiliser la détection de comportement pour la qualification du trafic** (option activée par défaut) – cochez cette case pour permettre au [Pare-feu](#) d'utiliser la fonctionnalité [Identity Protection](#) lors de l'évaluation d'une application. [Identity Protection](#) identifie tout comportement suspect de l'application, mais aussi indique si elle est fiable et peut être autorisée à communiquer en ligne.

### Paramètres du mode jeu

La section **Paramètres du mode jeu** permet d'autoriser (et de le confirmer en cochant la case associée) l'affichage de messages d'information du [Pare-feu](#) pendant l'exécution des applications en mode plein écran (*généralement des jeux, mais aussi toute autre application exécutée en plein écran comme les présentations PowerPoint*).

Si vous cochez la case **Désactiver les notifications du Pare-feu lors de l'exécution de jeux**, sélectionnez dans la liste déroulante l'action souhaitée lorsqu'une nouvelle application sans règle définie tente de communiquer sur le réseau (*ces applications vous invitent habituellement à répondre à une question dans une boîte de dialogue*). Toutes ces applications peuvent être autorisées ou bloquées.

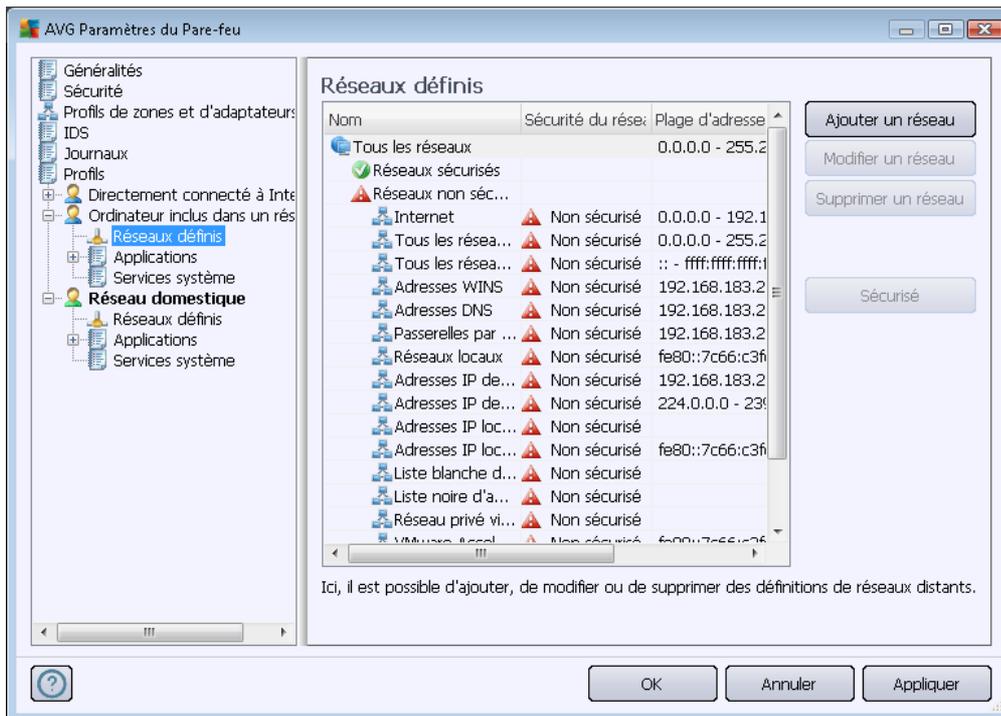
En mode jeu, toutes les tâches programmées (*analyses, mises à jour*) sont reportées jusqu'à la fermeture de l'application.

### Paramètres du composant IDS (Intrusion Detection System, système de détection d'intrusion)

Cochez la case **Activer IDS** pour activer une fonction d'analyse comportementale spécialisée conçue pour identifier et bloquer toute communication suspecte sur certains ports de l'ordinateur (*pour en savoir plus à ce sujet, consultez le chapitre consacré au [système de détection d'intrusion](#) de cette documentation*).

### 11.6.2. Réseaux définis

La boîte de dialogue **Réseaux définis** dresse la liste de tous les réseaux auxquels est relié l'ordinateur.

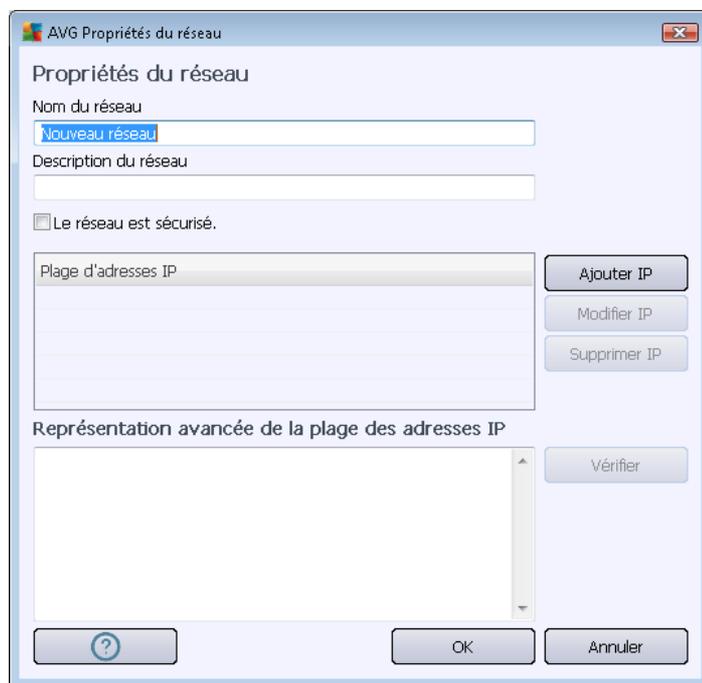


La liste fournit les informations suivantes sur chaque réseau détecté :

- **Réseaux** - Fournit la liste des réseaux auxquels l'ordinateur est relié.
- **Sécurité du réseau** – Par défaut, tous les réseaux sont considérés comme non sécurisés. Déclarez un réseau comme sécurisé seulement si vous êtes certain qu'il est fiable (*pour cela, cochez la case correspondante dans la liste et choisissez la commande Sécurisé dans le menu contextuel*). Tous les réseaux associés seront inclus dans le groupe des réseaux utilisés par l'application pour communiquer en appliquant le jeu de règles défini pour la valeur [Autoriser la connexion sécurisée](#).
- **Plage d'adresses IP** - Chaque réseau est automatiquement détecté et spécifié sous la forme d'une plage d'adresses IP.

#### Boutons de commande

- **Ajouter un réseau** - Ouvre la boîte de dialogue **Propriétés du réseau** dans laquelle vous ajustez les paramètres du réseau nouvellement défini :

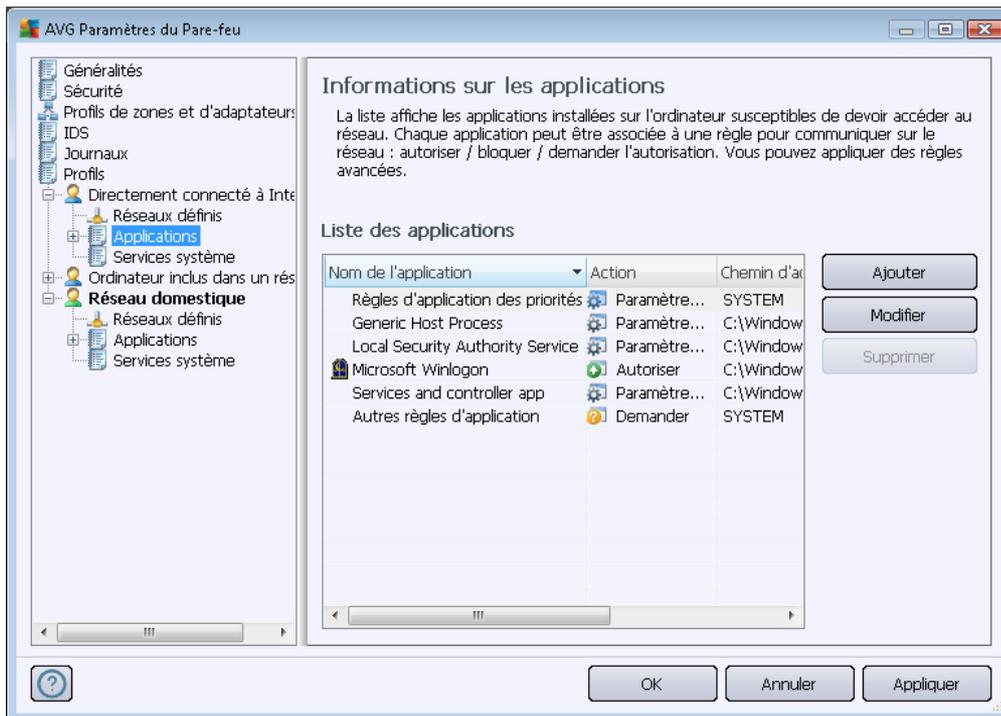


Dans cette boîte de dialogue, précisez le nom du réseau (champ **Nom du réseau**), décrivez-le dans le champ **Description du réseau**, puis indiquez s'il s'agit d'un réseau sécurisé. Le nouveau réseau peut être défini manuellement dans une boîte de dialogue distincte après avoir cliqué sur le bouton **Ajouter IP** (ou **Modifier IP** / **Supprimer IP**). Dans cette boîte de dialogue, vous spécifiez le réseau en indiquant une plage d'adresses IP ou un masque réseau. Pour un réseau étendu à intégrer au réseau actuel que vous venez de définir, vous pouvez utiliser l'option **Représentation avancée de la plage des adresses IP** : saisissez la liste intégrale des réseaux dans le champ de texte prévu à cet effet (*tous les formats standards sont pris en charge*), puis cliquez sur le bouton **Vérifier** pour vous assurer que le format est effectivement reconnu. Cliquez ensuite sur **OK** pour valider et enregistrer les données.

- **Modifier un réseau** – ouvre la boîte de dialogue **Propriétés du réseau** (voir ci-dessus) dans laquelle vous pouvez modifier les paramètres d'un réseau déjà défini (*la boîte de dialogue est identique à la boîte de dialogue d'insertion d'un nouveau réseau, décrite au paragraphe précédent*).
- **Supprimer un réseau** – Ce bouton retire la référence du réseau sélectionné de la liste des réseaux.
- **Le réseau est sécurisé** – Par défaut, tous les réseaux sont considérés comme non sécurisés. Déclarez un réseau comme sécurisé seulement si vous êtes certain qu'il est fiable (*et inversement, si le réseau est jugé sécurisé, le bouton qui s'affiche est Marqué comme non sécurisé*).

### 11.6.3. Applications

La boîte de dialogue d'information **Applications** indique toutes les applications installées qui pourraient être amenées à communiquer sur le réseau et les icônes affectées à l'action assignée :



Les applications figurant dans la **Liste des applications** sont celles qui ont été détectées sur l'ordinateur (et leurs actions respectives). Les types d'action suivants peuvent être utilisés :

-  - Autoriser les communications pour tous les réseaux
-  - Autoriser les communications uniquement pour les réseaux définis comme Sécurisé
-  - Bloquer les communications
-  - Afficher la boîte de dialogue appelant une décision de l'utilisateur (l'utilisateur devra décider s'il autorise ou bloque la communication lorsque l'application tente de se connecter au réseau)
-  - Définition des paramètres avancés

**Notez que seules les applications déjà installées ont pu être détectées. Par conséquent, si vous installez une nouvelle application après la recherche, vous aurez à définir des règles de pare-feu associées. Par défaut, lorsque la nouvelle application tente de se connecter sur le réseau pour la première fois, le pare-feu crée automatiquement une règle en fonction de la base de données fiable ou vous invite à autoriser ou à bloquer les communications. Dans ce dernier cas, vous pouvez configurer votre réponse comme règle permanente (qui sera alors répertoriée dans cette boîte de dialogue).**



Pour toute nouvelle application, vous pouvez aussi définir une règle immédiatement dans cette boîte de dialogue : cliquez simplement sur **Ajouter** et fournissez les détails nécessaires sur l'application.

Outre les applications, la liste contient aussi deux fonctions particulières :

- **Règles d'application des priorités** (*en haut de la liste*) sont des règles préférentielles, qui sont toujours appliquées avant toute autre règle de n'importe quelle application.
- **Autres règles d'applications** (*au bas de la liste*) sont utilisées en dernière instance lorsqu'aucune règle d'application spécifique ne s'applique (par exemple, pour une application inconnue et non définie). Sélectionnez l'action à déclencher lorsqu'une telle application tente de communiquer sur le réseau :
  - *Bloquer* : la communication sera toujours bloquée.
  - *Autoriser* : la communication sera autorisée sur n'importe quel réseau.
  - *Demander* : vous serez invité à décider si la communication doit être autorisée ou bloquée.

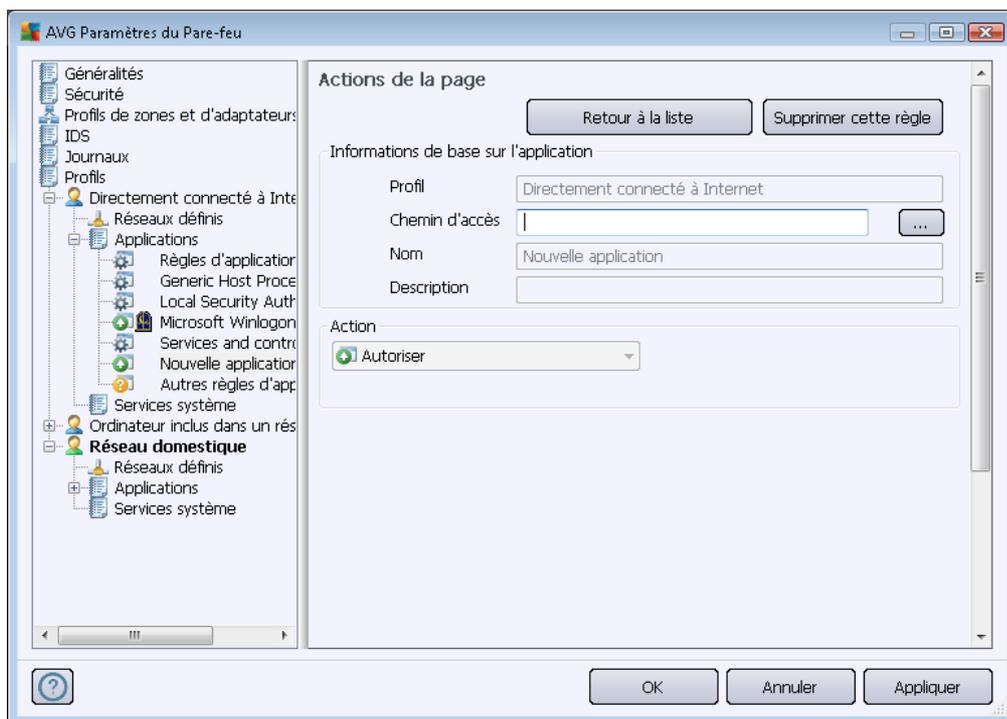
***Ces fonctions ont des options de paramétrage différentes de celles des applications courantes et ne s'adressent qu'à des utilisateurs expérimentés. Nous vous conseillons vivement de ne pas modifier ces paramètres !***

### **Boutons de commande**

La liste peut être modifiée à l'aide des boutons suivants :

- **Ajouter** – Ouvre une boîte de dialogue [Actions de la page](#) vide visant à définir de nouvelles règles d'application.
- **Modifier** - Ouvre la même boîte de dialogue [Actions de la page](#) renseignée selon les données fournies lors de la modification d'un ensemble de règles d'une application.
- **Supprimer** - Retire l'application sélectionnée de la liste.

Cette **boîte de dialogue** vous permet de définir précisément les paramètres des applications :



### Boutons de commande

Deux boutons de commande figurent dans la partie supérieure de la boîte de dialogue :

- **Retour à la liste** - Ce bouton permet d'afficher la présentation de l'ensemble des règles d'application définies.
- **Supprimer la règle** – Ce bouton permet de supprimer la règle d'application actuellement affichée. **Notez que cette action ne peut pas être annulée !**

### Informations de base sur l'application

Dans cette section, vous devez indiquer le **nom** de l'application et donner éventuellement une **description** (*commentaire bref pour votre usage personnel*). Dans le champ **Chemin**, saisissez le chemin d'accès complet à l'application (*le fichier exécutable*) sur le disque. Vous pouvez aussi identifier l'application facilement dans l'arborescence en cliquant sur le bouton "...".

### Action sur l'application

Dans le menu déroulant, sélectionnez la règle de **pare-feu** de l'application et précisez l'action que doit effectuer le **pare-feu** lorsque l'application tente de se connecter au réseau).

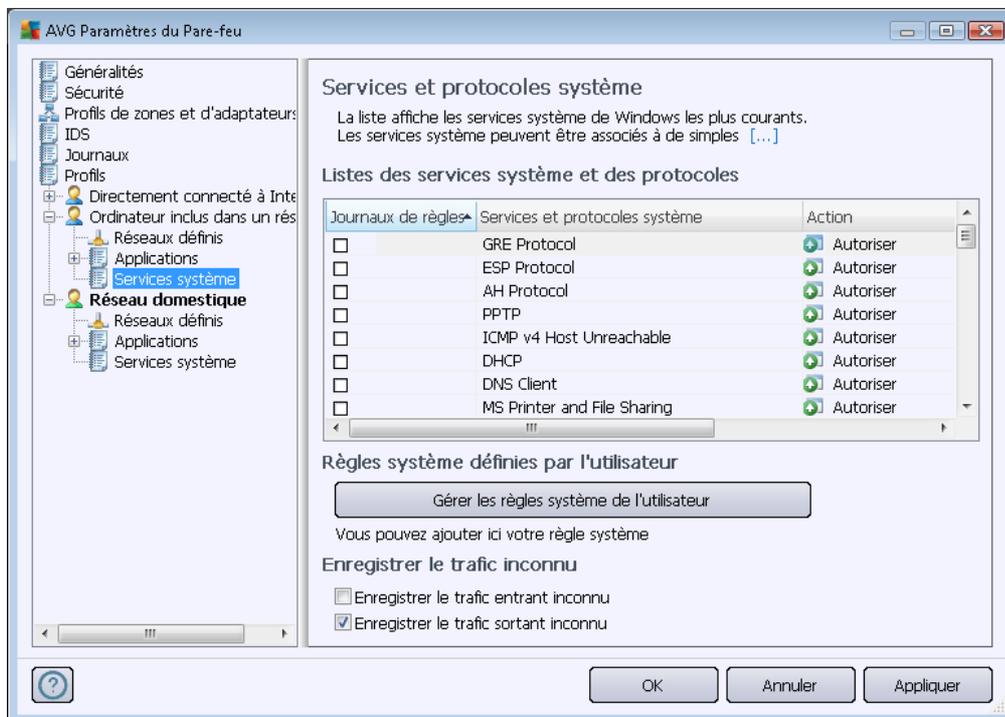


-  **Autoriser tout** – Permet à l'application de communiquer sur tous les réseaux définis et avec les adaptateurs, sans limitation.
-  **Autoriser la connexion sécurisée** – Permet à l'application de communiquer uniquement sur les réseaux définis comme fiables (*sécurisés*).
-  **Bloquer** – Interdit automatiquement la communication : l'application n'est autorisée à se connecter à aucun réseau.
-  **Demander** - Ouvre une boîte de dialogue où vous pouvez choisir de bloquer ou d'autoriser la tentative de communication en cours.
-  **Paramètres avancés** – Affiche des options de configuration supplémentaires dans la partie inférieure de la boîte de dialogue dans la section **Règles détaillées de l'application**. Les règles détaillées sont appliquées en fonction de leur rang dans la liste. Le classement se modifie à l'aide des fonctions **Haut** et **Bas**. Après avoir cliqué sur une règle donnée de la liste, la présentation de ses détails s'affichent dans la partie inférieure de la boîte de dialogue. Il est possible de modifier une valeur soulignée de couleur bleue en cliquant dans la boîte de dialogue correspondante. Pour supprimer la règle en surbrillance, cliquez simplement sur **Supprimer**. Pour définir une nouvelle règle, utilisez le bouton **Ajouter** pour ouvrir la boîte de dialogue de **modification des détails de la règle** qui permet de spécifier tous les détails nécessaires.

#### 11.6.4. Services système

**La modification de la boîte de dialogue Services et protocoles système est réservée EXCLUSIVEMENT AUX UTILISATEURS EXPERIMENTES !**

La boîte de dialogue **Services et protocoles système** répertorie tous les services système et les protocoles standard qui pourraient être amenés à communiquer sur le réseau:



## Listes des services système et des protocoles

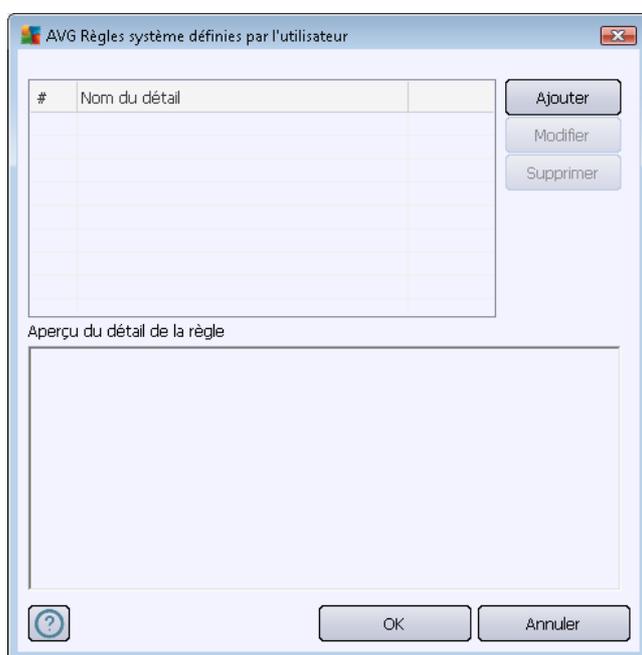
Le tableau comporte les colonnes suivantes :

- **Journaux de règles** – cette colonne permet d'activer l'enregistrement de l'application de chaque règle dans les [journaux](#).
- **Services et protocoles système** – cette colonne affiche le nom du service système correspondant.
- **Action** – cette colonne affiche une icône pour l'action associée :
  - Autoriser les communications pour tous les réseaux
  - Autoriser les communications uniquement pour les réseaux définis comme Sécurisé
  - Bloquer les communications
- **Nom** – cette colonne indique le réseau spécifique auquel la règle s'applique.

Pour modifier les paramètres d'un élément figurant dans la liste (y compris les actions assignées), cliquez avec le bouton droit de la souris sur l'élément, puis sélectionnez **Modifier**. **Toutefois, la modification d'une règle système ne doit être effectuée que par des utilisateurs expérimentés. Il est fortement recommandé de ne pas modifier la règle système.**

### Règles système définies par l'utilisateur

Pour ouvrir une nouvelle boîte de dialogue permettant de définir votre propre règle du service système (voir illustration ci-dessous), cliquez sur le bouton **Gérer les règles système de l'utilisateur**. La partie supérieure de la boîte de dialogue **Règles système définies par l'utilisateur** présente tous les détails de la règle système actuellement modifiée, la partie inférieure porte sur le détail sélectionné. Les règles système définies par l'utilisateur peuvent être modifiées, ajoutées ou supprimées à l'aide du bouton prévu à cet effet. En revanche, seule la modification est autorisée pour les détails des règles définies par l'éditeur:



**Notez que ces paramètres avancés s'adressent essentiellement aux administrateurs réseau qui maîtrisent parfaitement le processus de configuration du Pare-feu. Si vous ne connaissez pas les types de protocoles de communication, les numéros de port réseau, les définitions d'adresse IP, etc., ne modifiez pas ces paramètres. S'il est nécessaire de modifier la configuration, consultez l'aide pour obtenir des informations détaillées.**

### Enregistrer le trafic inconnu

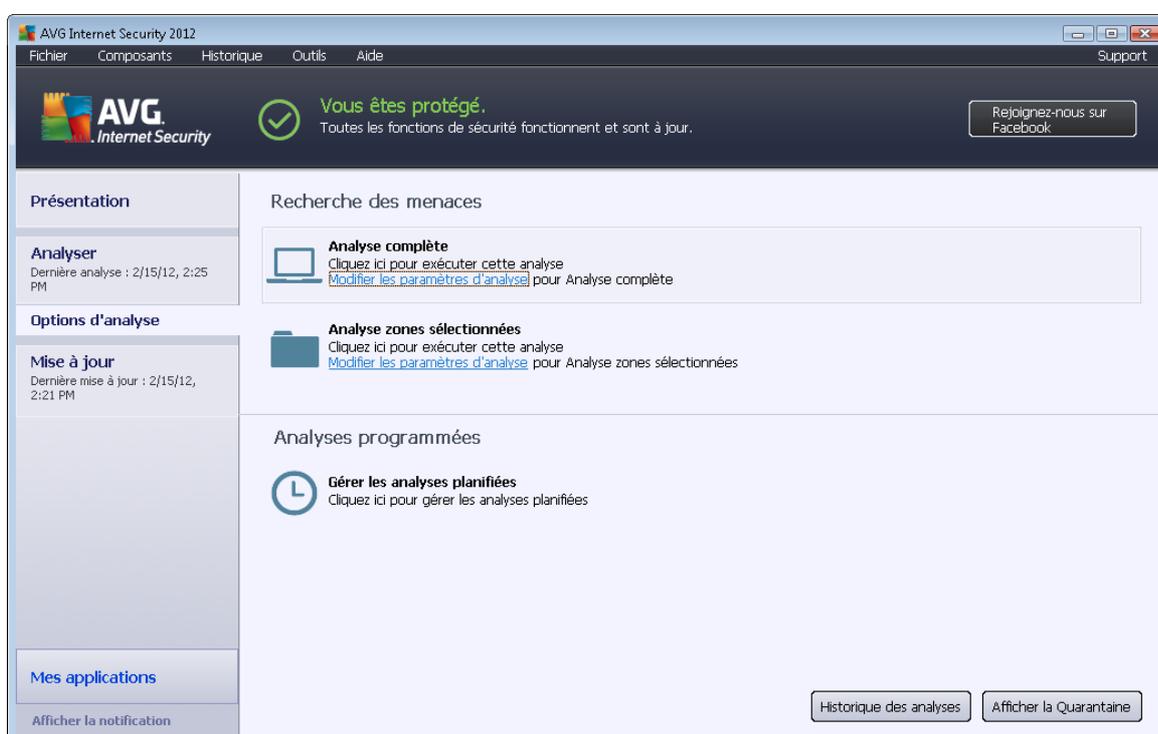
- **Enregistrer le trafic entrant inconnu** (option désactivée par défaut) – cochez cette case pour consigner dans les [Journaux](#) chaque tentative de connexion à votre ordinateur provenant d'un élément extérieur inconnu.
- **Enregistrer le trafic entrant inconnu** (option désactivée par défaut) – cochez cette case pour consigner dans les [Journaux](#) chaque tentative de connexion à votre ordinateur provenant d'un élément extérieur inconnu.



## 12. Analyse AVG

Par défaut, **AVG Internet Security 2012** n'exécute aucune analyse, car après l'analyse l'initiale, vous êtes parfaitement protégé par les composants résidents d'**AVG Internet Security 2012** qui reste toujours sur leur garde et ne laissent pas le moindre code malicieux s'insinuer dans l'ordinateur. Bien entendu, vous pouvez [programmer une analyse](#) à exécuter à intervalle régulier ou exécuter manuellement une analyse à la demande quand bon vous semble.

### 12.1. Interface d'analyse



L'interface d'analyse AVG est accessible via **Options d'analyse** ([lien d'accès rapide](#)). Cliquez sur ce lien pour accéder à la boîte de dialogue **Recherche des menaces**. Dans cette boîte de dialogue, vous trouverez les éléments suivants :

- présentation des [analyses prédéfinies](#) – trois types d'analyse (définis par l'éditeur du logiciel) sont prêts à l'emploi sur demande ou par programmation :
  - [Analyse complète](#)
  - [Analyse zones sélectionnées](#)
- [Programmation des analyses](#) – dans cette section, vous pouvez définir de nouvelles analyses et planifier d'autres programmations selon vos besoins.

#### Boutons de commande



Les boutons de commande disponibles au sein de l'interface d'analyse sont les suivants :

- **Historique des analyses** - affiche la boîte de dialogue [Résultats des analyses](#) relatant l'historique complet des analyses
- **Afficher la Quarantaine** - ouvre une nouvelle boîte de dialogue intitulée [Quarantaine](#) – espace dans lequel les infections sont confinées

## 12.2. Analyses prédéfinies

Parmi les principales fonctions d'**AVG Internet Security 2012**, citons l'analyse à la demande. Ce type d'analyse est prévu pour analyser différentes zones de l'ordinateur en cas de doute concernant la présence éventuelle de virus. Il est vivement recommandé d'effectuer fréquemment de telles analyses même si vous pensez qu'aucun virus ne s'est introduit dans votre système.

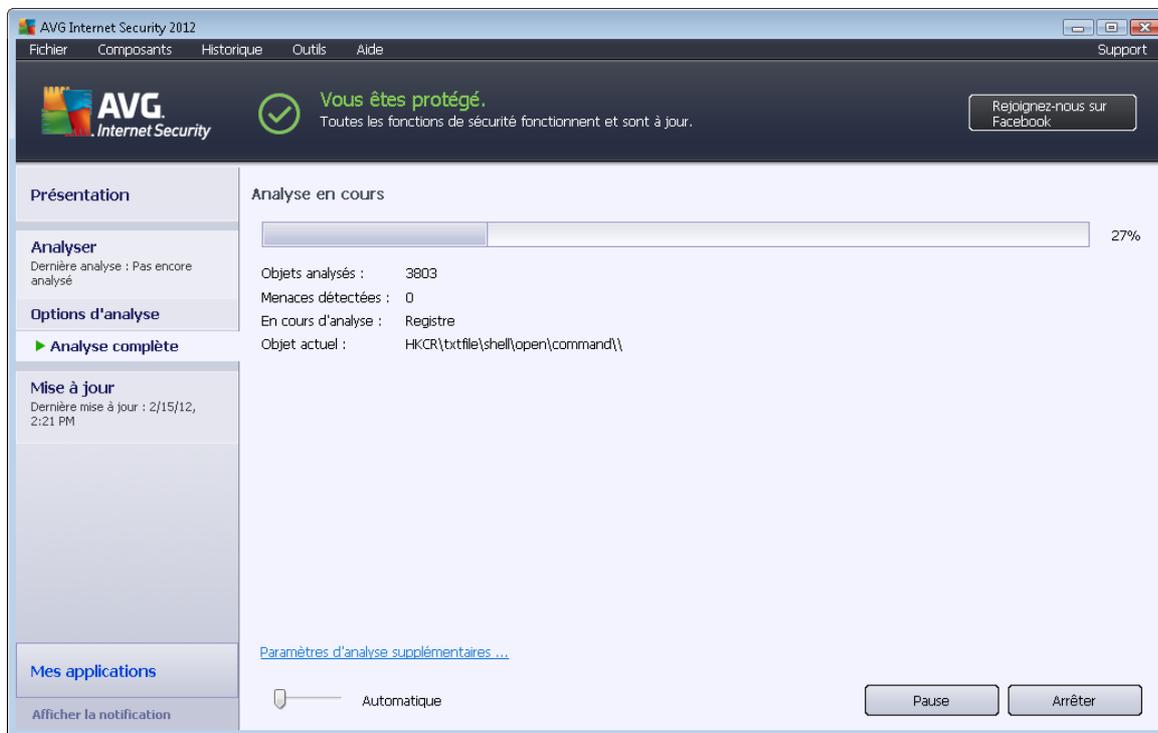
Dans **AVG Internet Security 2012**, vous trouverez les types d'analyses prédéfinies par l'éditeur du logiciel :

### 12.2.1. Analyse complète

L'**analyse complète** vérifie l'absence d'infection ainsi que la présence éventuelle de programmes potentiellement dangereux dans tous les fichiers de l'ordinateur. Cette analyse examine les disques durs de l'ordinateur, détecte et répare tout virus ou retire l'infection en la confinant dans la zone de [quarantaine](#). L'analyse de l'ordinateur doit être exécutée sur un poste de travail au moins une fois par semaine.

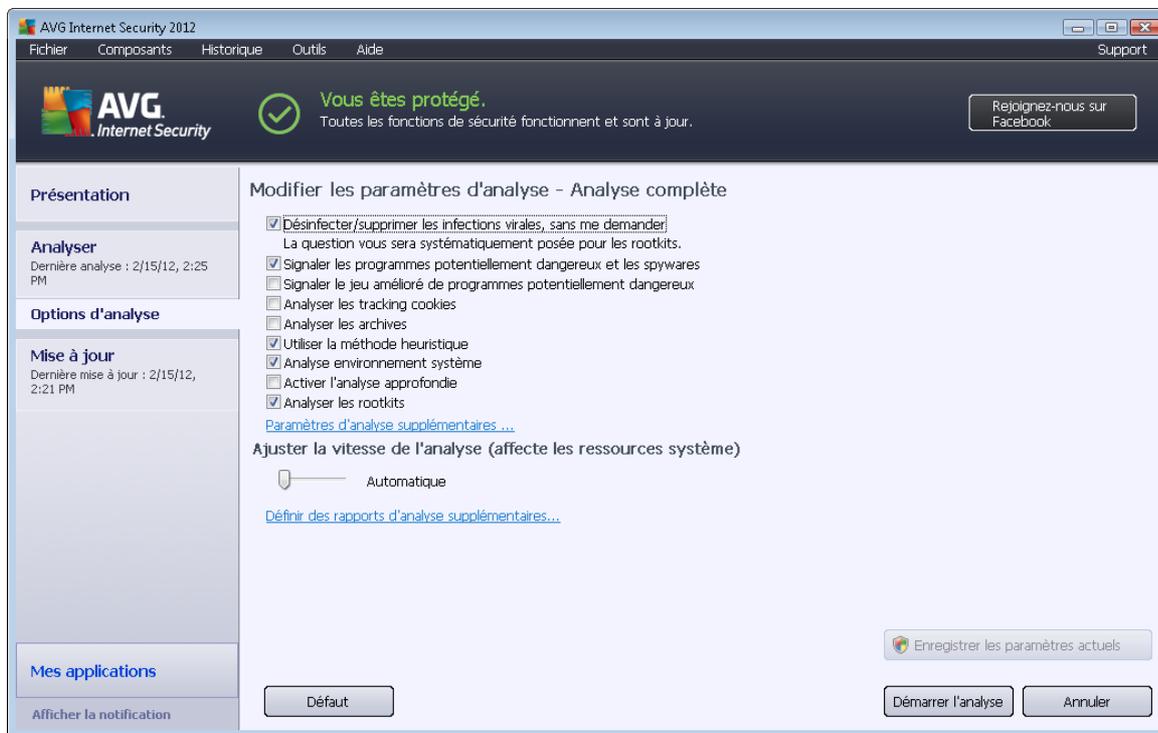
#### Lancement de l'analyse

L'**analyse complète** peut être lancée directement de l'[interface d'analyse](#) en cliquant sur l'icône d'analyse. Pour ce type d'analyse, il n'est pas nécessaire de configurer d'autres paramètres spécifiques. L'analyse démarre immédiatement dans la boîte de dialogue **Analyse en cours** (voir la *capture d'écran*). L'analyse peut être interrompue provisoirement (**Interrompre**) ou annulée (**Arrêter**) si nécessaire.



## Modification de la configuration de l'analyse

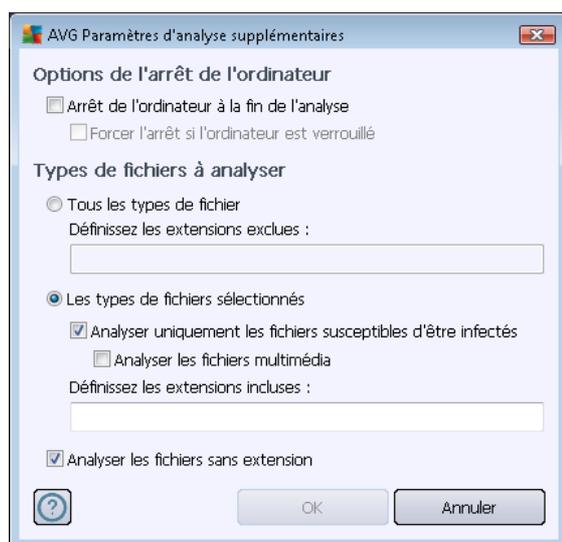
Vous avez la possibilité d'ajuster les paramètres prédéfinis par défaut de l'option **Analyse complète**. Cliquez sur le lien **Modifier les paramètres d'analyse** pour ouvrir la boîte de dialogue **Modifier les paramètres d'analyse de l'analyse complète** (accessible par l'[interface d'analyse](#) en activant le lien [Modifier les paramètres d'analyse du module Analyse complète](#)). **Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.**



- **Paramètres d'analyse** – dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins :
  - **Réparer/supprimer les infections sans me demander** (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en [quarantaine](#).
  - **Signaler les programmes potentiellement dangereux et les spywares** (option activée par défaut) : cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.
  - **Signaler le jeu amélioré de programmes potentiellement dangereux** – (option désactivée par défaut) : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisées à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.
  - **Analyser les tracking cookies** (option désactivée par défaut) : ce paramètre du composant [Anti-Spyware](#) définit les cookies qui pourront être détectés au cours de l'analyse (les cookies HTTP servent à authentifier, à suivre et à gérer certaines

informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique).

- **Analyser les archives** (option désactivée par défaut) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des archives (archives ZIP, RAR, par exemple).
  - **Utiliser la méthode heuristique** (option activée par défaut) : l'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
  - **Analyser l'environnement système** (option activée par défaut) : l'analyse vérifie également les zones système de votre ordinateur.
  - **Activer l'analyse approfondie** (option désactivée par défaut) – dans certains cas (suspicion d'une infection de l'ordinateur), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus qui analyseront jusqu'aux zones de l'ordinateur les moins susceptibles d'être infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
  - **Analyser les rootkits** (activée par défaut) : l'analyse [Anti-Rootkit](#) recherche les éventuels rootkits présents sur votre ordinateur, c'est-à-dire les programmes et technologies destinés à masquer l'activité de programmes malveillants sur l'ordinateur. Si un rootkit est détecté, cela ne veut pas forcément dire que votre ordinateur est infecté. Dans certains cas, des pilotes spécifiques ou des sections d'applications régulières peuvent être considérés, à tort, comme des rootkits.
- **Paramètres d'analyse supplémentaires** – ce lien ouvre une nouvelle boîte de dialogue **Paramètres d'analyse supplémentaires** permettant de spécifier les paramètres suivants :



- **Options de l'arrêt de l'ordinateur** – indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option **Arrêt de l'ordinateur à**



**la fin de l'analyse** est activée, l'option **Forcer l'arrêt si l'ordinateur est verrouillé** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.

- **Types de fichier à analyser** : en outre, vous pouvez choisir les éléments à analyser :
  - **Tous les types de fichier** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers à ne pas analyser (séparées par des virgules) ;
  - **Les types de fichiers sélectionnés** – vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio – si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
  - Vous pouvez également choisir l'option **Analyser les fichiers sans extension** – cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.
- **Ajuster la vitesse de l'analyse** – le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).
- **Définir des rapports d'analyse supplémentaires** – ce lien ouvre une nouvelle boîte de dialogue **Rapports d'analyse**, dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



**Avertissement** : ces paramètres d'analyse sont identiques à ceux d'une nouvelle analyse, comme indiqué dans le chapitre [Analyse AVG / Programmation de l'analyse / Comment faire l'analyse](#). Si vous décidez de modifier la configuration par défaut de l'**Analyse complète**, vous avez la possibilité d'enregistrer ces nouveaux paramètres en tant que configuration par défaut et de les appliquer à toute analyse complète de l'ordinateur.



### 12.2.2. Analyse zones sélectionnées

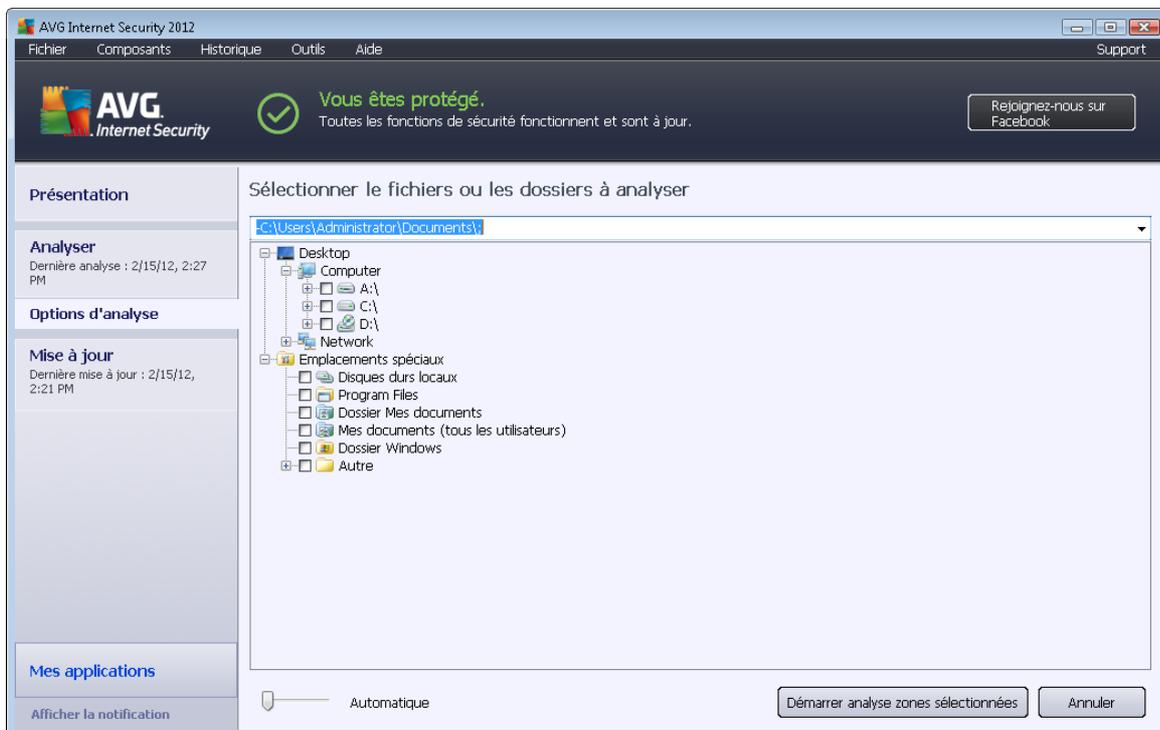
**Analyse zones sélectionnées** – analyse seulement les zones de l'ordinateur que vous avez sélectionnées en vue d'une analyse (*dossiers, disque durs, disquettes, CD, etc.*). Le déroulement de l'analyse en cas de détection virale, ainsi que la solution appliquée, est le même que pour une analyse complète de l'ordinateur : [tout virus détecté est réparé ou déplacé en quarantaine](#). L'Analyse zones sélectionnées permet de configurer vos propres analyses et de les programmer en fonction de vos besoins.

#### Lancement de l'analyse

L'**Analyse zones sélectionnées** peut être lancée directement depuis l'[interface d'analyse](#) en cliquant sur l'icône correspondante. La boîte de dialogue **Sélectionner les fichiers ou les dossiers à examiner** s'ouvre. Dans l'arborescence de votre ordinateur, sélectionnez les dossiers que vous souhaitez analyser. Le chemin d'accès à chaque dossier sélectionné est généré automatiquement et apparaît dans la zone de texte située dans la partie supérieure de la boîte de dialogue.

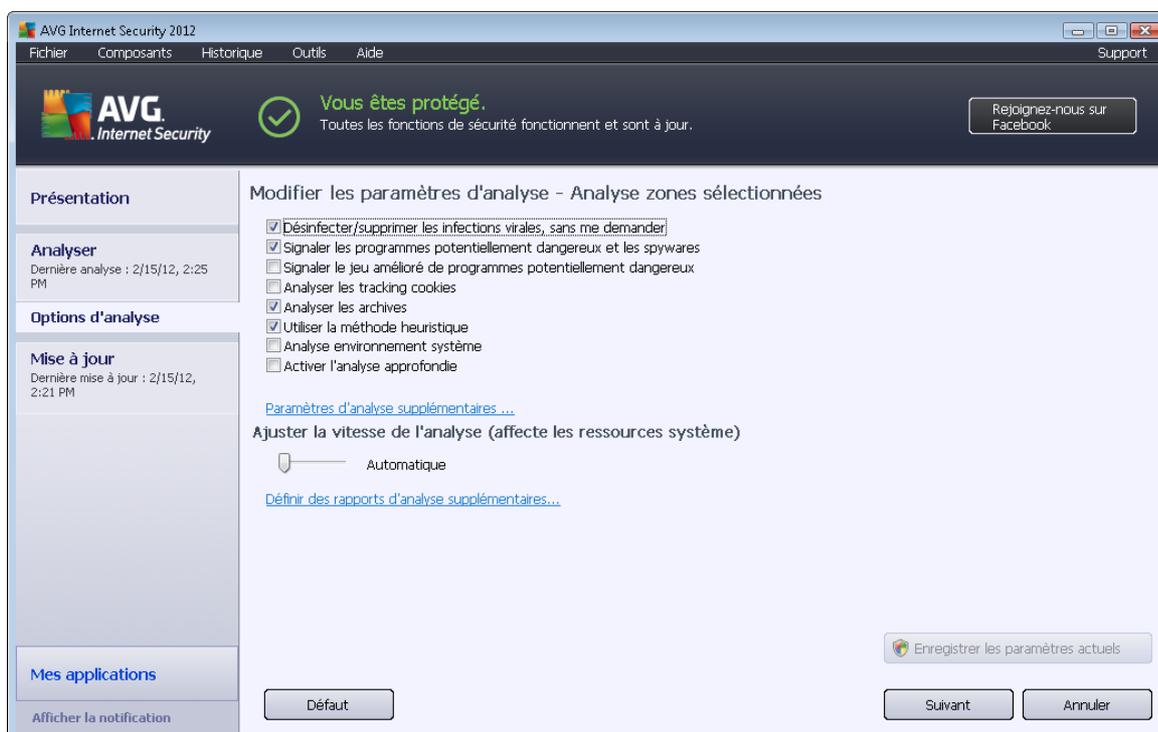
Il est aussi possible d'analyser un dossier spécifique et d'exclure tous ses sous-dossiers du processus. Pour ce faire, il suffit d'insérer le signe moins "-" avant le chemin d'accès généré automatiquement (*voir la capture d'écran*). Pour exclure un dossier complet de l'analyse, utilisez le paramètre « ! ».

Pour lancer l'analyse, cliquez sur le bouton **Démarrer l'analyse** ; le processus est fondamentalement identique à celui de l'[analyse complète](#) de l'ordinateur.



## Modification de la configuration de l'analyse

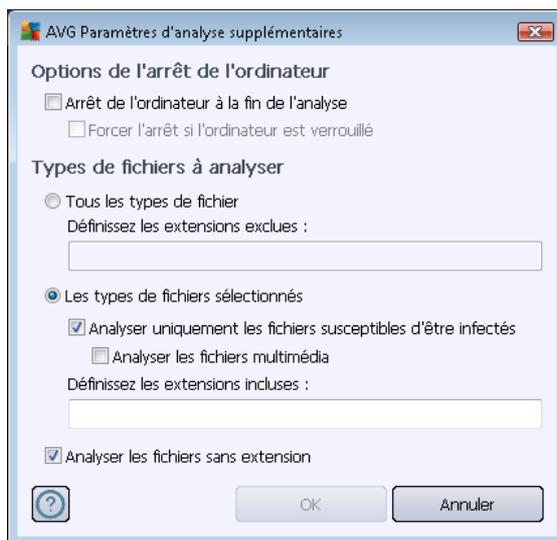
Vous pouvez modifier les paramètres prédéfinis par défaut de l'option **Analyser des fichiers ou des dossiers spécifiques**. Activez le lien **Modifier les paramètres d'analyse** pour accéder à la boîte de dialogue **Modifier les paramètres d'analyse – Analyse de fichiers ou dossiers spécifiques**. **Il est recommandé de conserver les paramètres par défaut et de ne les modifier qu'en cas d'absolue nécessité.**



- **Paramètres d'analyse** – dans la liste des paramètres d'analyse, vous pouvez activer/désactiver des paramètres spécifiques en fonction de vos besoins :
  - **Réparer/supprimer les infections sans me demander** (option activée par défaut) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, dans la mesure du possible. S'il est impossible de réparer automatiquement le fichier infecté, il sera placé en [quarantaine](#).
  - **Signaler les programmes potentiellement dangereux et les spywares** (option activée par défaut) : cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.
  - **Signaler le jeu amélioré de programmes potentiellement dangereux** (option désactivée par défaut) : permet de détecter le jeu étendu des spywares qui ne

posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisés à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.

- **Analyser les tracking cookies** (option désactivée par défaut) : ce paramètre du composant [Anti-Spyware](#) définit les cookies qui pourront être détectés au cours de l'analyse (les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique).
  - **Analyser les archives** (option désactivée par défaut) : ce paramètre indique que l'analyse examine tous les fichiers même ceux stockés dans des d'archives (archives ZIP, RAR, par exemple).
  - **Utiliser la méthode heuristique** (option activée par défaut) : l'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
  - **Analyse environnement système** (option désactivée par défaut) : l'analyse vérifie les fichiers système de l'ordinateur.
  - **Activer l'analyse approfondie** (option désactivée par défaut) : dans certains cas (suspicion d'une infection de l'ordinateur), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même, s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Paramètres d'analyse supplémentaires** – ce lien ouvre une nouvelle boîte de dialogue **Paramètres d'analyse supplémentaires** permettant de spécifier les paramètres suivants :



- **Options de l'arrêt de l'ordinateur** – indiquez si l'ordinateur doit être arrêté

automatiquement à la fin du processus d'analyse. Si l'option **Arrêt de l'ordinateur à la fin de l'analyse** est activée, l'option **Forcer l'arrêt si l'ordinateur est verrouillé** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.

- **Types de fichiers à analyser** – Ensuite, vous pouvez choisir d'analyser :
  - **Tous les types de fichier** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers à ne pas analyser (séparées par des virgules) ;
  - **Types de fichier sélectionnés** – vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio – si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
  - Vous pouvez également choisir l'option **Analyser les fichiers sans extension** – cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.
- **Priorité du processus d'analyse** – le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).
- **Définir des rapports d'analyse supplémentaires** – ce lien ouvre la boîte de dialogue **Rapports d'analyse** où vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :



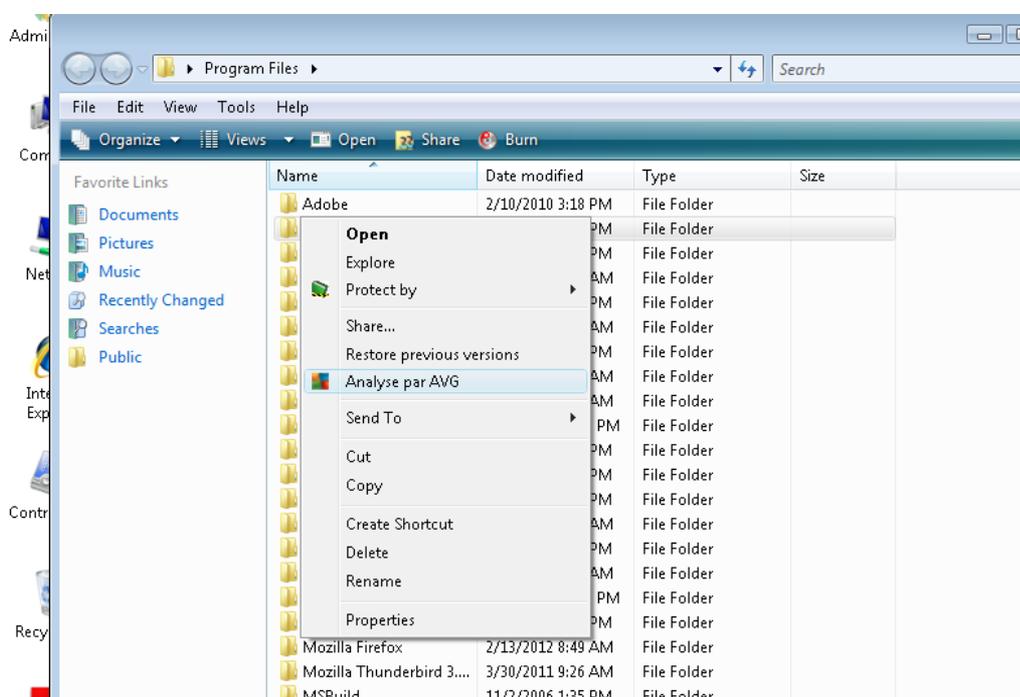
**Avertissement :** ces paramètres d'analyse sont identiques à ceux d'une nouvelle analyse, comme indiqué dans le chapitre [Analyse AVG / Programmation de l'analyse / Comment faire l'analyse](#). Si vous décidez de modifier la configuration **Analyse zones sélectionnées** par défaut, vous pouvez enregistrer les paramètres modifiés en tant que configuration par défaut et les appliquer aux analyses ultérieures de fichiers ou de dossiers spécifiques. De plus, cette configuration sera utilisée



comme modèle des nouvelles analyses programmées ([toutes les analyses personnalisées basées sur la configuration actuelle de l'analyse des fichiers ou dossiers spécifiques](#)).

### 12.3. Analyse contextuelle

Outre les analyses prédéfinies exécutées sur l'ensemble ou des zones sélectionnées de l'ordinateur, **AVG Internet Security 2012** offre la possibilité d'examiner rapidement l'objet de votre choix dans l'environnement de l'Explorateur Windows. Si vous désirez ouvrir un fichier inconnu dont le contenu est incertain, vous pouvez le vérifier à la demande. Procédez comme suit :



- Dans l'Explorateur Windows, mettez le fichier (*ou le dossier*) en surbrillance
- Cliquez avec le bouton droit de la souris sur l'objet pour afficher le menu contextuel
- Choisissez la commande **Analyse par AVG** pour faire analyser le fichier par **AVG Internet Security 2012**

### 12.4. Analyse depuis la ligne de commande

Dans **AVG Internet Security 2012**, il est possible de lancer l'analyse depuis la ligne de commande. Vous apprécierez cette possibilité sur les serveurs, par exemple, ou lors de la création d'un script de commandes qui doit s'exécuter automatiquement après l'initialisation de l'ordinateur. La plupart des paramètres proposés dans l'interface utilisateur graphique sont disponibles à partir de la ligne de commande.

Pour lancer l'analyse AVG en ligne de commande, exécutez la commande suivante depuis le dossier où AVG est installé :



- **avgscanx** pour un système d'exploitation 32 bits
- **avgscana** pour un système d'exploitation 64 bits

### Syntaxe de la commande

La syntaxe de la commande est la suivante :

- **avgscanx /paramètre...** par exemple, **avgscanx /comp** pour l'analyse complète de l'ordinateur
- **avgscanx /paramètre /paramètre** si plusieurs paramètres sont précisés, les entrer à la suite, séparés par un espace et une barre oblique
- si un paramètre requiert la saisie de valeurs spécifiques (par exemple, le paramètre **/scan** requiert de savoir quelles zones de votre ordinateur ont été sélectionnées afin d'être analysées et vous devez indiquer un chemin exact vers la section sélectionnée), il faut séparer les valeurs éventuelles par un point-virgule, par exemple : **avgscanx /scan=C:\;D:\**

### Paramètres d'analyse

Pour afficher la liste complète des paramètres disponibles, tapez la commande concernée ainsi que le paramètre **/?** ou **/HELP** (ex : **avgscanx /?**). Le seul paramètre obligatoire est **/SCAN** pour lequel il est nécessaire de spécifier les zones de l'ordinateur à analyser. Pour une description détaillée des options, voir la [liste des paramètres de ligne de commande](#).

Pour exécuter l'analyse, appuyez sur **Entrée**. Pendant l'analyse, vous pouvez arrêter le processus en appuyant sur **Ctrl+C** ou **Ctrl+Pause**.

### Analyse CMD lancée depuis l'interface d'analyse

Lorsque vous démarrez l'ordinateur en mode sans échec, il est également possible de faire appel à la ligne de commande à partir de l'interface utilisateur graphique. L'analyse à proprement parler sera lancée à partir de la ligne de commande, la boîte de dialogue **Editeur de ligne de commande** permet seulement de préciser la plupart des paramètres d'analyse dans l'interface graphique plus conviviale.

Etant donné que cette boîte de dialogue n'est accessible qu'en mode sans échec, consultez le fichier d'aide accessible à partir de cette boîte de dialogue si vous avez besoin de renseignements supplémentaires.

#### 12.4.1. Paramètres d'analyse CMD

Vous trouverez ci-après la liste de tous les paramètres disponibles pour lancer une analyse depuis la ligne de commande :

- **/SCAN** [Analyse zones sélectionnées](#) /SCAN=chemin;chemin (ex. : /



SCAN=C:\;D:\)

- **/COMP** [Analyse complète de l'ordinateur](#)
- **/HEUR** Utiliser l'[analyse heuristique](#)
- **/EXCLUDE** Fichiers ou chemin exclus de l'analyse
- **/@** Fichier de commande /nom du fichier/
- **/EXT** Analyser ces extensions /par exemple EXT=EXE,DLL/
- **/NOEXT** Ne pas analyser ces extensions /par exemple NOEXT=JPG/
- **/ARC** Analyser les archives
- **/CLEAN** Nettoyer automatiquement
- **/TRASH** Mettre les fichiers en [Quarantaine](#)
- **/QT** Analyse rapide
- **/LOG** Générer un fichier contenant le résultat de l'analyse
- **/MACROW** Signaler les macros
- **/PWDW** Signaler les fichiers protégés par un mot de passe
- **/ARCBOMBSW** Signaler les bombes d'archives (archives recompressées)
- **/IGNLOCKED** Ignorer les fichiers verrouillés
- **/REPORT** Reporter dans le fichier /nom du fichier/
- **/REPAPPEND** Inclure dans le fichier de rapport
- **/REPOK** Avertir l'utilisateur des fichiers non infectés
- **/NOBREAK** Ne pas autoriser CTRL-PAUSE pour arrêter
- **/BOOT** Activer la vérification MBR/BOOT
- **/PROC** Analyser les processus actifs
- **/PUP** Signaler les "[programmes potentiellement dangereux](#)
- **/PUPEXT** Signaler un jeu amélioré de [programmes potentiellement dangereux](#)
- **/REG** Analyser la base de registre



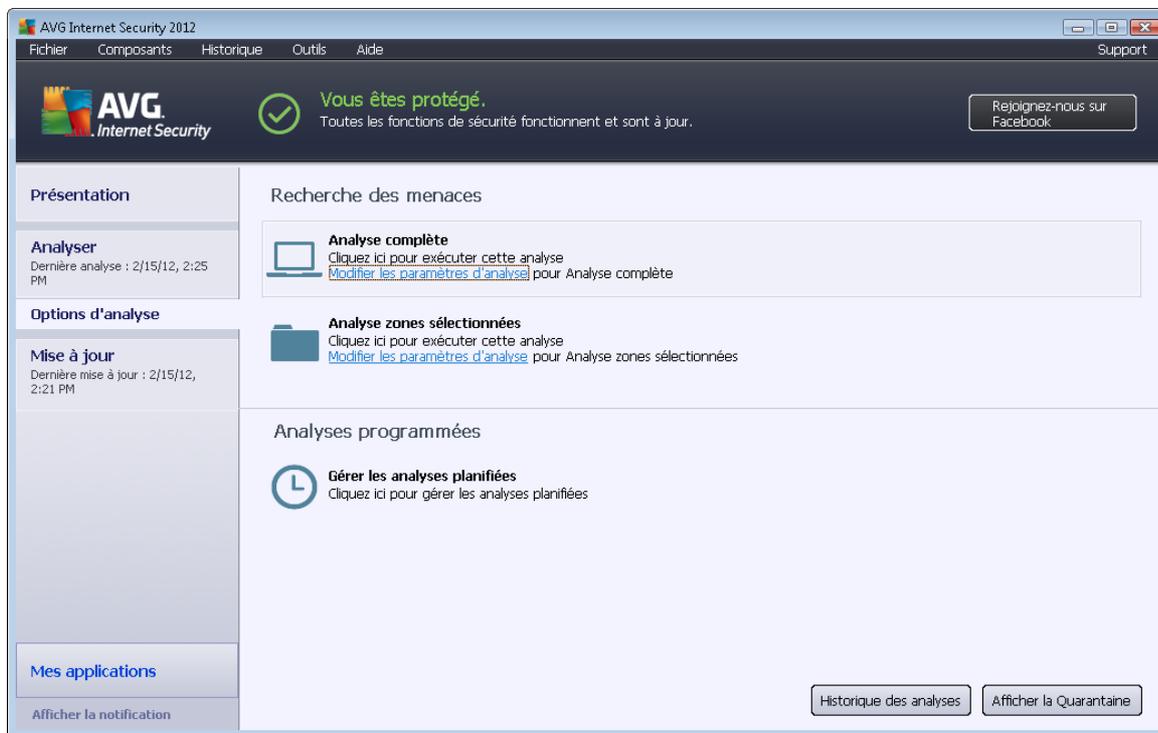
- **/COO** Analyser les cookies
- **/?** Affichage de l'aide sur un sujet
- **/HELP** Affichage de la rubrique d'aide en rapport avec l'élément actuellement sélectionné ou affiché
- **/PRIORITY** Définir la priorité de l'analyse /Faible, Auto, Elevée/ ([voir Paramètres avancés / Analyses](#))
- **/SHUTDOWN** Arrêt de l'ordinateur à la fin de l'analyse
- **/FORCESHUTDOWN** Forcer l'arrêt de l'ordinateur à la fin de l'analyse
- **/ADS** Analyser les flux de données alternatifs (*NTFS uniquement*)
- **/HIDDEN** Signaler des fichiers dont l'extension est masquée
- **/INFECTABLEONLY** Analyser uniquement les fichiers qui, d'après leur extension, sont susceptibles d'être infectés
- **/THOROUGHSCAN** Exécuter une analyse approfondie
- **/CLOUDCHECK** Vérifier les fausses détections
- **/ARCBOMBSW** Signaler les fichiers archives recompressés

## 12.5. Programmation de l'analyse

Avec **AVG Internet Security 2012**, vous pouvez effectuer une analyse à la demande (par exemple, lorsque vous soupçonnez qu'un virus s'est infiltré dans l'ordinateur) ou selon un programme prévu. Il est vivement recommandé d'exécuter des analyses planifiées. Vous serez ainsi assuré que votre ordinateur sera protégé de tout risque d'infection et vous n'aurez plus à vous soucier de la gestion des analyses.

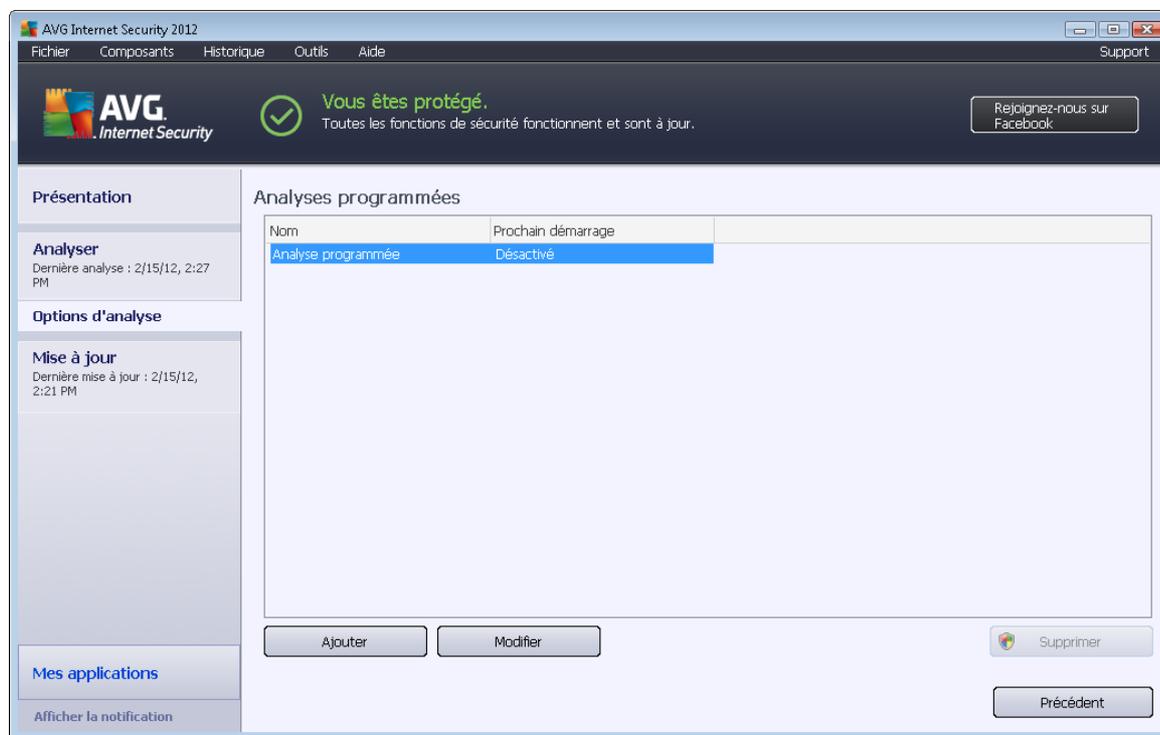
Il est possible d'effectuer une [analyse complète](#) régulièrement, c'est-à-dire une fois par semaine au moins. Si possible, faites aussi une analyse complète l'ordinateur une fois par jour, comme configuré par défaut dans la programmation de l'analyse. Si l'ordinateur est toujours allumé, vous pouvez programmer l'analyse en dehors de vos heures de travail. Si l'ordinateur est parfois éteint, programmez une analyse [au démarrage de l'ordinateur lorsqu'elle n'a pas pu être effectuée](#).

Pour créer de nouvelles programmations d'analyse, consultez l'[interface d'analyse AVG](#), dans la section du bas, **Analyses programmées** :



## Analyses programmées

Cliquez sur l'icône située dans la section **Analyses programmées** pour ouvrir une nouvelle boîte de dialogue **Analyses programmées** présentant une liste de toutes les analyses programmées actuellement :

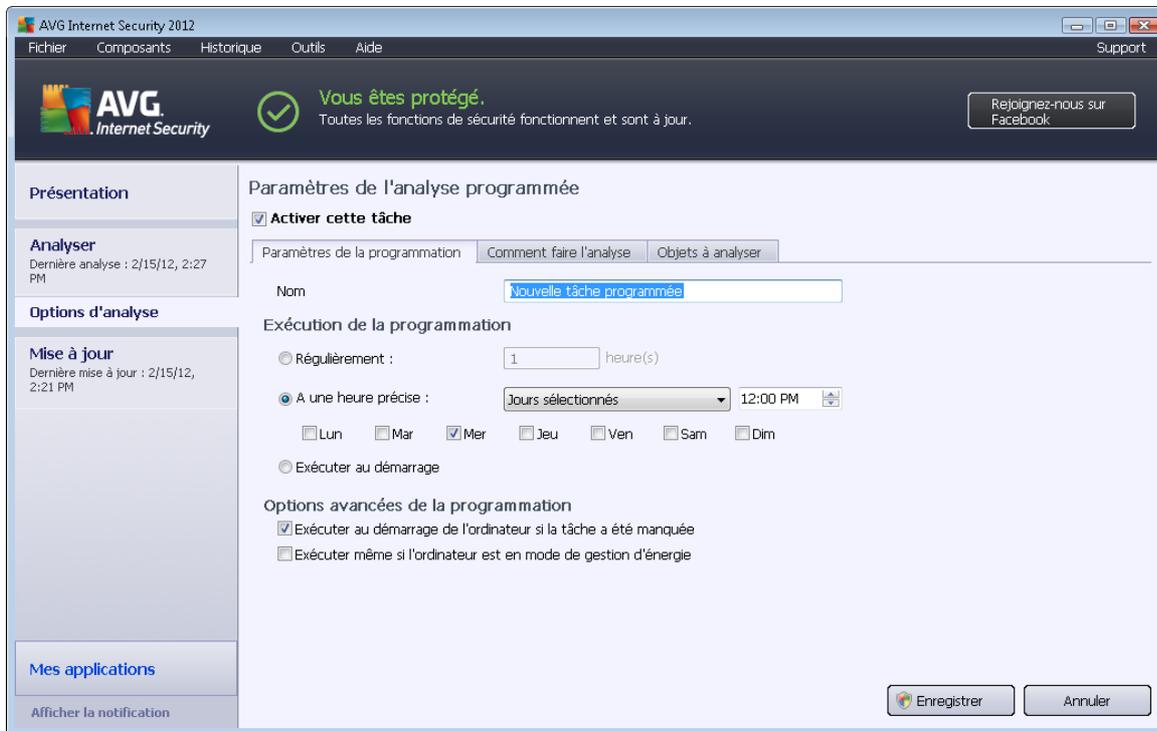


Vous pouvez modifier / ajouter des analyses à l'aide des boutons de commande suivants :

- **Ajouter** – le bouton ouvre la boîte de dialogue **Paramètres de l'analyse programmée**, onglet [Paramètres de la programmation](#). Dans cette boîte de dialogue, définissez les paramètres de la nouvelle analyse.
- **Modifier** – ce bouton n'est actif que si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Dans ce cas, le bouton est accessible ; il suffit de cliquer dessus pour accéder à la boîte de dialogue **Paramètres de l'analyse programmée**, onglet [Paramètres de la programmation](#). Les paramètres de l'analyse sélectionnée sont pré-renseignés et peuvent être modifiés.
- **Supprimer** – ce bouton est actif si vous avez déjà sélectionné une analyse existante dans la liste des analyses programmées. Cette analyse peut ensuite être supprimée de la liste en cliquant sur ce bouton. Notez néanmoins que vous ne pouvez supprimer que vos propres analyses. Les analyses de type **Programmation de l'analyse complète de l'ordinateur** prédéfinies par défaut ne peuvent jamais être supprimées.
- **Précédent** – permet de revenir à l'[interface d'analyse d'AVG](#)

### 12.5.1. Paramètres de la programmation

Pour programmer une nouvelle analyse et définir son exécution régulière, ouvrez la boîte de dialogue **Paramètres de l'analyse programmée** (cliquez sur le bouton **Ajouter une analyse programmée** situé dans la boîte de dialogue **Analyses programmées**). Cette boîte de dialogue comporte trois onglets : **Paramètres de la programmation** (voir l'illustration ci-dessous. Il s'agit de l'onglet qui s'affiche par défaut et de façon automatique à l'ouverture de la boîte de dialogue), [Comment faire l'analyse](#) et [Objets à analyser](#).



Dans l'onglet **Paramètres de la programmation**, vous pouvez cocher/désélectionner la case **Activer cette tâche** pour désactiver temporairement l'analyse programmée et le réactiver au moment opportun.

Donnez ensuite un nom à l'analyse que vous voulez créer et programmer. Saisissez le nom dans la zone de texte en regard de l'option **Nom**. Veillez à utiliser des noms courts, descriptifs et appropriés pour distinguer facilement les différentes analyses par la suite.

**Exemple :** il n'est pas judicieux d'appeler l'analyse "Nouvelle analyse" ou "Mon analyse", car ces noms ne font pas référence au champ réel de l'analyse. A l'inverse, "Analyse environnement système" est un nom descriptif précis. Il est également nécessaire de spécifier dans le nom de l'analyse si l'analyse concerne l'ensemble de l'ordinateur ou une sélection de fichiers ou de dossiers. Notez que les analyses personnalisées sont toujours basées sur l'[Analyse zones sélectionnés](#).

Dans cette boîte de dialogue, vous définissez plus précisément les paramètres de l'analyse :

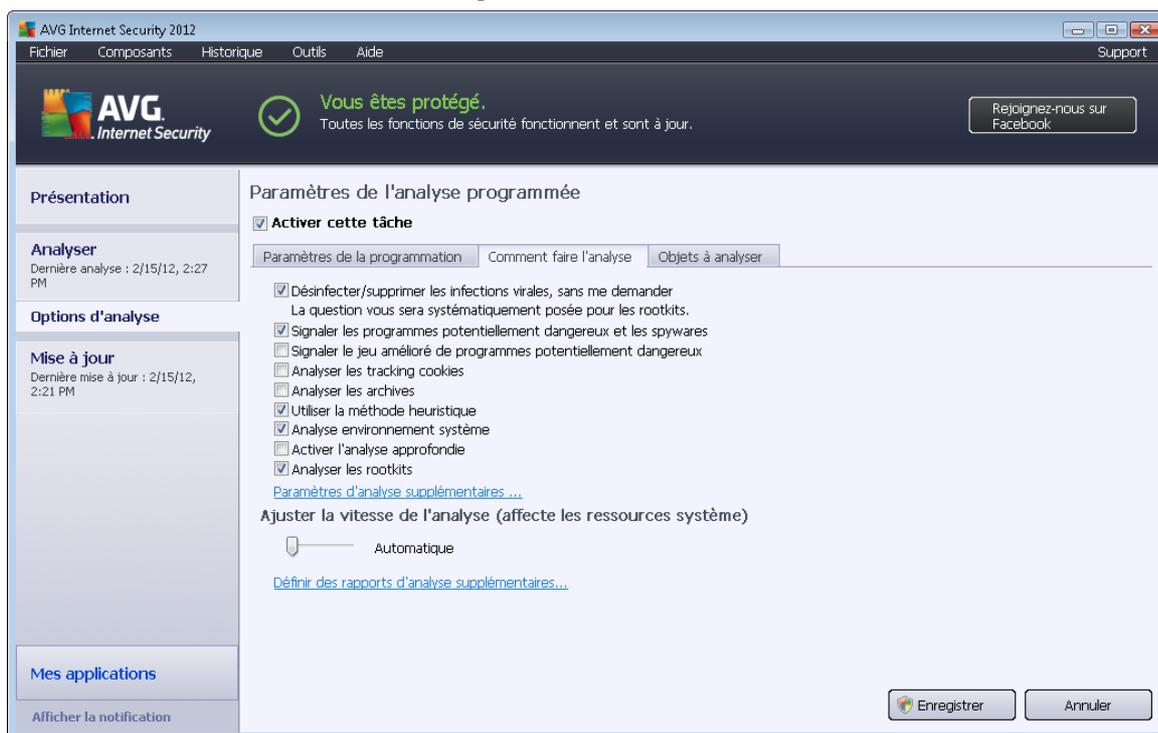
- **Exécution de la programmation** - spécifiez l'intervalle entre chaque exécution de la nouvelle analyse. Il est possible de répéter le lancement de l'analyse après un laps de temps donné (**Régulièrement**), d'en définir la date et l'heure précises (**A une heure précise**) ou encore d'indiquer l'évènement auquel sera associé le lancement de l'analyse (**Suivant une action**).
- **Options avancées de la programmation** – cette section permet de définir dans quelles conditions l'analyse doit ou ne doit pas être exécutée si l'ordinateur est en mode d'économie d'énergie ou hors tension.

## Boutons de commande de la boîte de dialogue Paramètres de l'analyse programmée

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue **Paramètres de l'analyse programmée** (*Paramètres de la programmation*, [Comment faire l'analyse](#) et [Objets à analyser](#)). Ils ont la même fonction :

- **Enregistrer** – enregistre toutes les modifications entrées sous l'onglet en cours ou un autre onglet de cette boîte de dialogue et affiche la [boîte de dialogue par défaut de l'interface d'analyse AVG](#). Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.
- **Annuler** – annule toutes les modifications entrées sous l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la [boîte de dialogue par défaut de l'interface d'analyse AVG](#).

### 12.5.2. Comment faire l'analyse



Dans l'onglet **Comment faire l'analyse**, vous trouverez la liste des paramètres d'analyse qui peuvent être activés ou désactivés. Par défaut, la plupart des paramètres sont activés et appliqués lors de l'analyse. Aussi est-il recommandé de ne pas modifier la configuration prédéfinie d'AVG sans motif valable.

- **Réparer/supprimer les infections sans me demander** (*option activée par défaut*) : lorsqu'un virus est détecté au cours de l'analyse, il est réparé automatiquement, dans la mesure du possible. Si la désinfection automatique du fichier n'est pas possible (ou si cette option est désactivée), un message de détection de virus s'affiche. Il vous appartient alors

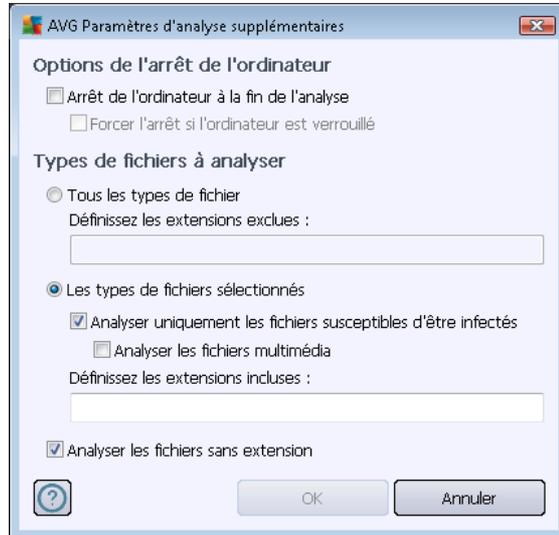


de déterminer le traitement à appliquer à l'infection. L'action recommandée consiste à confiner le fichier infecté en [quarantaine](#).

- **Signaler les programmes potentiellement dangereux et les spywares (activé par défaut)** : Cochez cette case pour activer le moteur [Anti-spyware](#) et rechercher les spywares et les virus. Les spywares désignent une catégorie de codes suspects : même s'ils représentent généralement un risque pour la sécurité, certains de ces programmes peuvent être installés intentionnellement par l'utilisateur. Nous vous recommandons de laisser cette fonction activée car elle augmente de manière significative la sécurité de votre système.
- **Signaler le jeu amélioré de programmes potentiellement dangereux (option désactivée par défaut)** : permet de détecter le jeu étendu des spywares qui ne posent aucun problème et sont sans danger dès lors qu'ils sont achetés directement auprès de leur éditeur, mais qui peuvent ensuite être utilisés à des fins malveillantes. Il s'agit d'une mesure de sécurité supplémentaire. Cependant, elle peut bloquer des programmes légitimes de l'ordinateur ; c'est pourquoi elle est désactivée par défaut.
- **Analyser les tracking cookies (option désactivée par défaut)** : ce paramètre du composant [Anti-Spyware](#) indique que les cookies devront être détectés au cours de l'analyse (les cookies HTTP servent à authentifier, à suivre et à gérer certaines informations sur les utilisateurs comme leurs préférences en matière de navigation ou le contenu de leur panier d'achat électronique).
- **Analyser les archives (option désactivée par défaut)** : ce paramètre indique que l'analyse doit examiner tous les fichiers, même ceux comprimés dans certains types d'archives (archives ZIP ou RAR, par exemple).
- **Utiliser la méthode heuristique (option activée par défaut)** : l'analyse heuristique (émulation dynamique des instructions de l'objet analysé dans un environnement informatique virtuel) est l'une des méthodes employées pour détecter des virus pendant l'analyse.
- **Analyse environnement système (option activée par défaut)** : l'analyse vérifie les fichiers système de l'ordinateur.
- **Activer l'analyse approfondie (option désactivée par défaut)** – dans certains cas (suspicion d'une infection de l'ordinateur), vous pouvez cocher cette option pour exécuter des algorithmes d'analyse très pointus même s'il est peu probable que certaines zones de l'ordinateur soient infectées. Gardez à l'esprit que cette méthode prend énormément de temps.
- **Analyser les rootkits (activée par défaut)** : l'analyse [Anti-Rootkit](#) recherche les éventuels rootkits présents sur votre ordinateur, c'est-à-dire les programmes et technologies destinés à cacher l'activité de programmes malveillants sur l'ordinateur. Si un rootkit est détecté, cela ne veut pas forcément dire que votre ordinateur est infecté. Dans certains cas, des pilotes spécifiques ou des sections d'applications régulières peuvent être considérés, à tort, comme des rootkits.

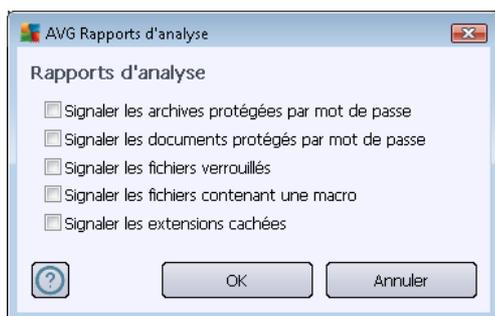
Ensuite, vous pouvez modifier les paramètres de l'analyse en procédant comme suit :

- **Paramètres d'analyse supplémentaires** – ce lien ouvre une nouvelle boîte de dialogue **Paramètres d'analyse supplémentaires** permettant de spécifier les paramètres suivants :



- **Options de l'arrêt de l'ordinateur** – indiquez si l'ordinateur doit être arrêté automatiquement à la fin du processus d'analyse. Si l'option **Arrêt de l'ordinateur à la fin de l'analyse** est activée, l'option **Forcer l'arrêt si l'ordinateur est verrouillé** devient disponible et permet d'arrêter l'ordinateur même s'il est verrouillé.
- **Types de fichier à analyser** : en outre, vous pouvez choisir les éléments à analyser :
  - **Tous les types de fichier** avec la possibilité de définir les éléments à exclure de l'analyse en répertoriant les extensions de fichiers à ne pas analyser (séparées par des virgules) ;
  - **Les types de fichiers sélectionnés** – vous pouvez choisir d'analyser uniquement les fichiers susceptibles d'être infectés (*les fichiers qui ne peuvent faire l'objet d'une infection ne sont pas analysés ; il s'agit par exemple de fichiers en texte brut ou de certains types de fichier non exécutables*), y compris les fichiers multimédia (*vidéo, audio – si vous ne sélectionnez pas cette option, la durée de l'analyse sera considérablement réduite, car ce sont souvent de gros fichiers qui sont rarement infectés par un virus*). En fonction des extensions, vous pouvez également spécifier les fichiers qui doivent toujours faire l'objet d'une analyse.
  - Vous pouvez également choisir l'option **Analyser les fichiers sans extension** – cette option est activée par défaut et il est recommandé de la conserver et de ne la modifier qu'en cas d'absolue nécessité. Les fichiers sans extension sont relativement suspects et doivent toujours faire l'objet d'une analyse.
- **Ajuster la vitesse de l'analyse** – le curseur vous permet de modifier la priorité du processus d'analyse. Par défaut, cette option est réglée sur le niveau *automatique* d'utilisation des ressources. Vous pouvez aussi choisir le processus d'analyse lent, qui réduit la charge sur les ressources système (*cette option est pratique quand vous devez travailler sur l'ordinateur sans avoir à vous soucier de la durée de l'analyse*) ; ou rapide, qui utilise plus de ressources système (*convient notamment lorsque vous quittez temporairement votre poste de travail*).

- **Définir des rapports d'analyse supplémentaires** – ce lien ouvre une nouvelle boîte de dialogue **Rapports d'analyse**, dans laquelle vous pouvez sélectionner les types de résultats que vous souhaitez obtenir :

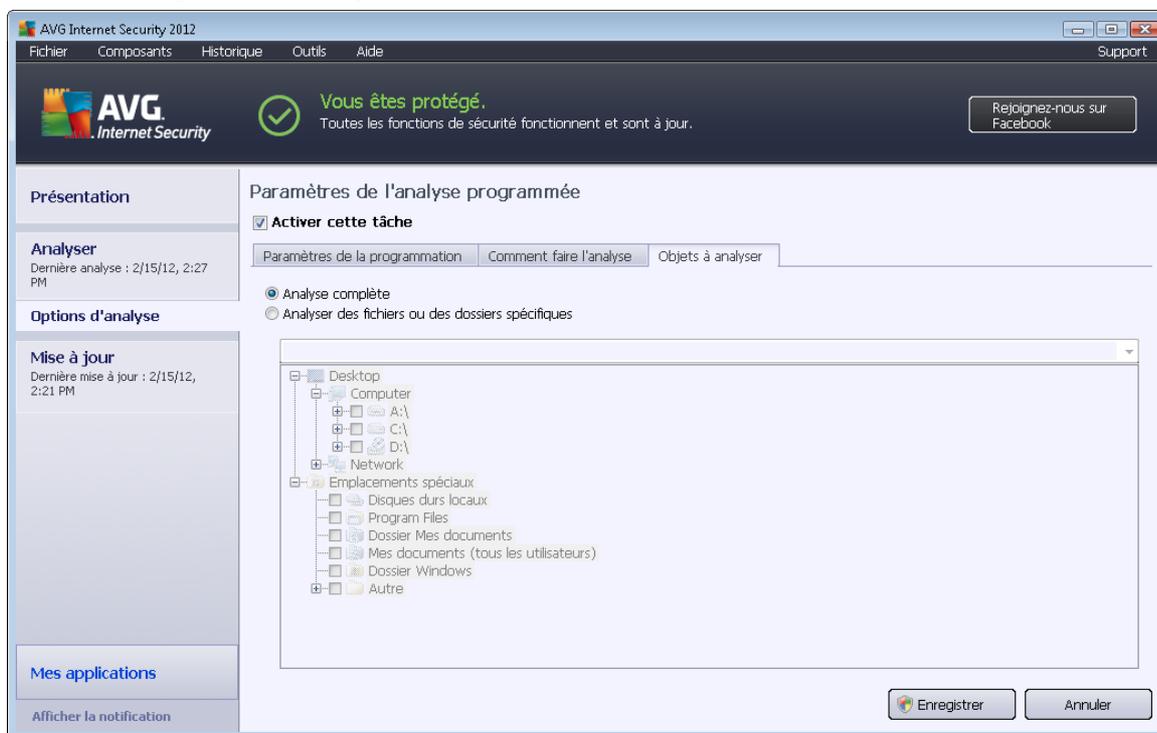


### Boutons de commande

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue **Paramètres de l'analyse programmée** ([Paramètres de la programmation](#), [Comment faire l'analyse](#) et [Objets à analyser](#)). Ils ont la même fonction :

- **Enregistrer** – enregistre toutes les modifications entrées sous l'onglet en cours ou un autre onglet de cette boîte de dialogue et affiche la [boîte de dialogue par défaut de l'interface d'analyse AVG](#). Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.
- **Annuler** – annule toutes les modifications entrées sous l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la [boîte de dialogue par défaut de l'interface d'analyse AVG](#).

### 12.5.3. Objets à analyser



Sous l'onglet **Objet à analyser**, indiquez si vous voulez programmer l'[analyse complète](#) ou l'[analyse des zones sélectionnées](#).

Si vous préférez l'analyse des zones sélectionnées, cela a pour effet d'activer, dans la partie inférieure de la boîte de dialogue, l'arborescence. Vous pouvez alors sélectionner les dossiers à analyser (*développez les catégories en cliquant sur le signe plus pour voir le dossier souhaité*). Vous pouvez sélectionner plusieurs dossiers en sélectionnant leur case respective. Les dossiers sélectionnés apparaîtront dans la zone de texte en haut de la boîte de dialogue et le menu déroulant conservera l'historique des analyses sélectionnées pour une utilisation ultérieure. *Autre solution, vous pouvez aussi saisir manuellement le chemin complet du dossier souhaité (si vous spécifiez plusieurs chemins, séparez-les par un point-virgule sans espace)*.

Dans l'arborescence, vous noterez également la présence d'une entrée **Emplacements spéciaux**. Voici la liste des emplacements qui seront analysés lorsque la case associée est cochée :

- **Disques durs locaux** - tous les disques durs de l'ordinateur
- **Program Files**
  - C:\Program Files\
  - dans la version 64 bits C:\Program Files (x86)
- **Dossier Mes documents**



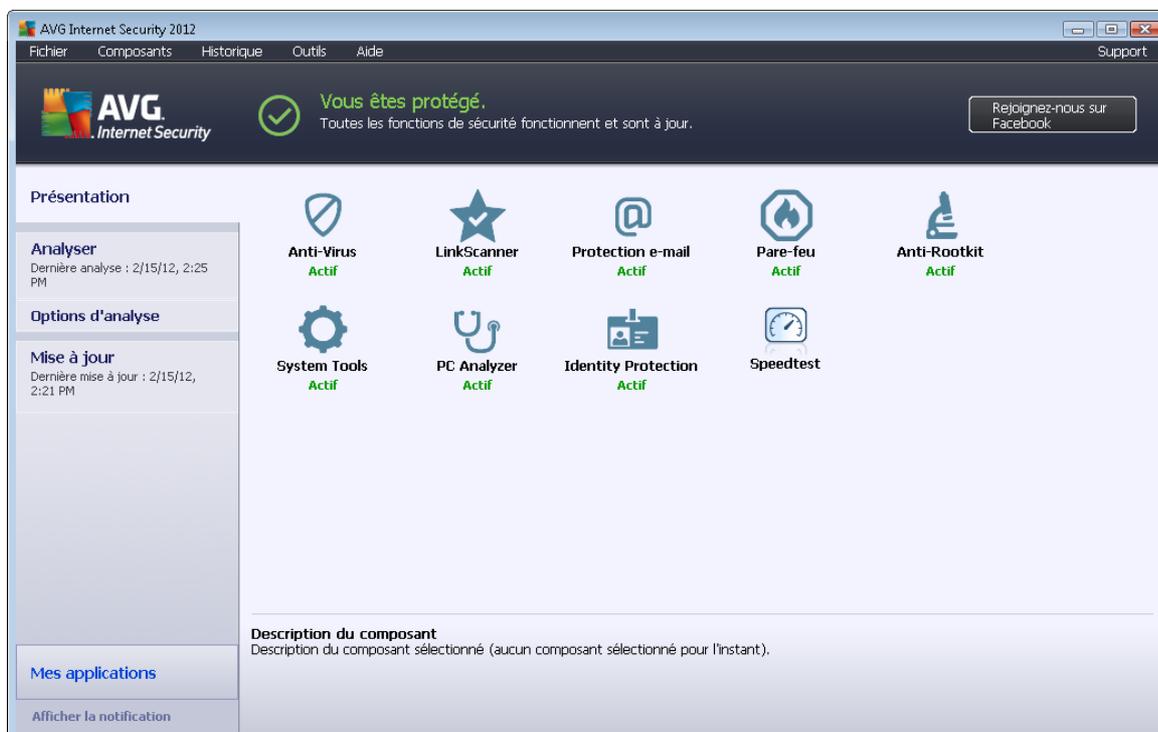
- *Win XP* : C:\Documents and Settings\Utilisateur\Mes Documents\
- *Windows Vista/7* : C:\Utilisateurs\utilisateur\Documents\
- **Documents partagés**
  - *Win XP* : C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7* : C:\Utilisateurs\Public\Documents\
- **Dossier Windows** – C:\Windows\
- **Autre**
  - *Lecteur système* – le disque dur sur lequel le système d'exploitation est installé (en général, il s'agit de C:)
  - *Dossier système* – C:\Windows\System32\
  - *Dossier Fichiers temporaires* – C:\Documents and Settings\User\Local\ (*Windows XP*) ou C:\Utilisateurs\utilisateur\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Fichiers Internet temporaires* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) ou C:\Utilisateurs\utilisateur\AppData\Local\Microsoft\Windows\Temporary Internet Files\ (*Windows Vista/7*)

### Boutons de commande

Deux boutons de commande figurent sur les trois onglets de la boîte de dialogue **Paramètres de l'analyse programmée** ([Paramètres de la programmation](#), [Comment faire l'analyse](#) et [Objets à analyser](#)) :

- **Enregistrer** – enregistre toutes les modifications entrées sous l'onglet en cours ou un autre onglet de cette boîte de dialogue et affiche la [boîte de dialogue par défaut de l'interface d'analyse AVG](#). Par conséquent, si vous voulez configurer les paramètres d'analyse répartis sous tous les onglets, cliquez sur ce bouton uniquement après avoir défini tous vos choix.
- **Annuler** – annule toutes les modifications entrées sous l'onglet actif ou un autre onglet de cette boîte de dialogue et affiche la [boîte de dialogue par défaut de l'interface d'analyse AVG](#).

## 12.6. Résultats d'analyse



La boîte de dialogue **Résultats d'analyse** est accessible depuis l'[interface d'analyse AVG](#) via le bouton **Historique / Résultats des analyses**. Elle contient la liste de toutes les analyses précédemment exécutées ainsi que les informations suivantes sur les résultats :

- **Nom** – désignation de l'analyse ; il s'agit soit du nom d'une [analyse prédéfinie](#), soit d'un nom que vous avez attribué à une [analyse personnalisée](#). Chaque nom inclut une icône indiquant le résultat de l'analyse :

 – une icône de couleur verte signale l'absence d'infection

 – une icône de couleur bleue indique l'absence d'infection, mais la suppression automatique d'un objet infecté

 – une icône de couleur rouge vous alerte sur la présence d'une infection qui a été détectée lors de l'analyse et qui n'a pas pu être traitée.

Les icônes sont entières ou brisées – l'icône entière représente une analyse exécutée et correctement terminée ; l'icône brisée désigne une analyse annulée ou interrompue.

**Remarque** : pour plus d'informations sur une analyse, consultez la boîte de dialogue [Résultats des analyses](#), par le biais du bouton *Voir les détails* (partie inférieure de la boîte de dialogue).

- **Heure de début** – date et heure d'exécution de l'analyse



- **Heure de fin** - date et heure de fin de l'analyse
- **Objets analysés** – nombre d'objets qui ont été vérifiés
- **Infections** – nombre d'infections détectées / supprimées
- **Spywares** - nombre de spywares détectés / supprimés
- **Avertissements** – nombre d'[objets suspects](#)
- **Rootkits** – nombre de [rootkits](#)
- **Informations sur le journal d'analyse** - informations sur le déroulement de l'analyse et sur les résultats (finalisation ou interruption du processus)

### Boutons de commande

Les boutons de contrôle de la boîte de dialogue **Résultats d'analyse** sont les suivants :

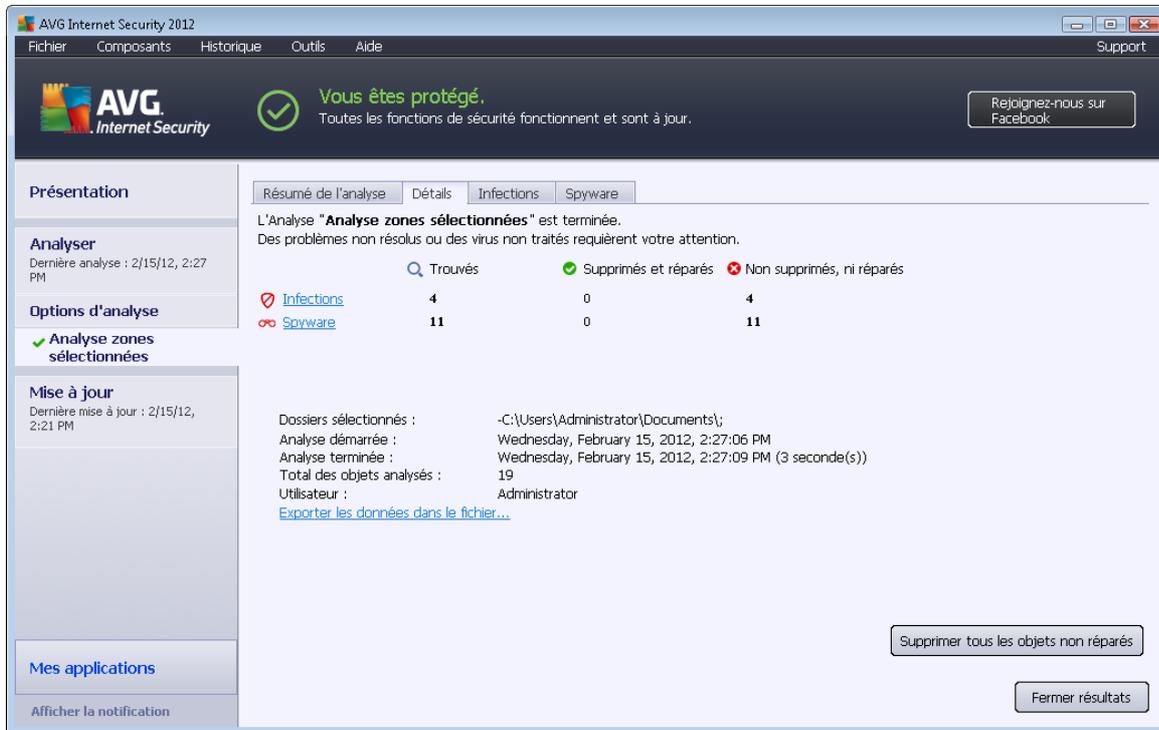
- **Voir les détails** - cliquez sur ce bouton pour ouvrir la boîte de dialogue [Résultats des analyses](#) et examiner les détails de l'analyse sélectionnée
- **Supprimer résultat** - cliquez sur ce bouton pour supprimer l'élément sélectionné de la présentation des résultats d'analyse
- **Précédent** – permet de revenir à la boîte de dialogue par défaut de l'[interface d'analyse AVG](#)

## 12.7. Détails des résultats d'analyse

Si, dans la boîte de dialogue [Résultats d'analyse](#), une analyse donnée est sélectionnée, cliquer sur le bouton **Voir les détails** a pour effet d'afficher la boîte de dialogue **Résultats des analyses** fournissant des détails sur la progression et le résultat de cette analyse. La boîte de dialogue est subdivisée en plusieurs onglets :

- [Résultats d'analyse](#) – l'onglet est toujours affiché et délivre des informations statistiques sur le déroulement de l'analyse
- [Infections](#) – l'onglet s'affiche seulement en cas d'infection virale, détectée lors de l'analyse
- [Spyware](#) – l'onglet s'affiche seulement si un spyware a été trouvé lors de l'analyse
- [Avertissements](#) – l'onglet s'affiche si l'analyse détecte des cookies, par exemple
- [Rootkits](#) – l'onglet s'affiche seulement si un rootkit a été trouvé lors de l'analyse
- [Informations](#) – l'onglet s'affiche seulement si certaines menaces potentielles ont été détectées et ne peuvent pas être rangées dans une des catégories mentionnées. Un message d'avertissement lié à l'objet trouvé s'affiche également. Vous trouverez également des informations sur des objets que l'analyse n'a pas réussi à traiter (*comme des archives protégées par mot de passe*).

### 12.7.1. Onglet Résultats d'analyse



AVG Internet Security 2012

Fichier Composants Historique Outils Aide Support

**AVG Internet Security**  **Vous êtes protégé.**  
Toutes les fonctions de sécurité fonctionnent et sont à jour. [Rejoignez-nous sur Facebook](#)

**Présentation**

**Analyser**  
Dernière analyse : 2/15/12, 2:27 PM

**Options d'analyse**

**Analyse zones sélectionnées**

**Mise à jour**  
Dernière mise à jour : 2/15/12, 2:21 PM

**Mes applications**  
[Afficher la notification](#)

Résumé de l'analyse | Détails | Infections | Spyware

L'Analyse "**Analyse zones sélectionnées**" est terminée.  
Des problèmes non résolus ou des virus non traités requièrent votre attention.

	Trouvés	Supprimés et réparés	Non supprimés, ni réparés
 Infections	4	0	4
 Spyware	11	0	11

Dossiers sélectionnés : -C:\Users\Administrator\Documents\  
Analyse démarrée : Wednesday, February 15, 2012, 2:27:06 PM  
Analyse terminée : Wednesday, February 15, 2012, 2:27:09 PM (3 seconde(s))  
Total des objets analysés : 19  
Utilisateur : Administrator  
[Exporter les données dans le fichier...](#)

[Supprimer tous les objets non réparés](#)

[Fermer résultats](#)

Sur la page de l'onglet **Résultats des analyses**, vous trouverez des statistiques détaillées portant sur :

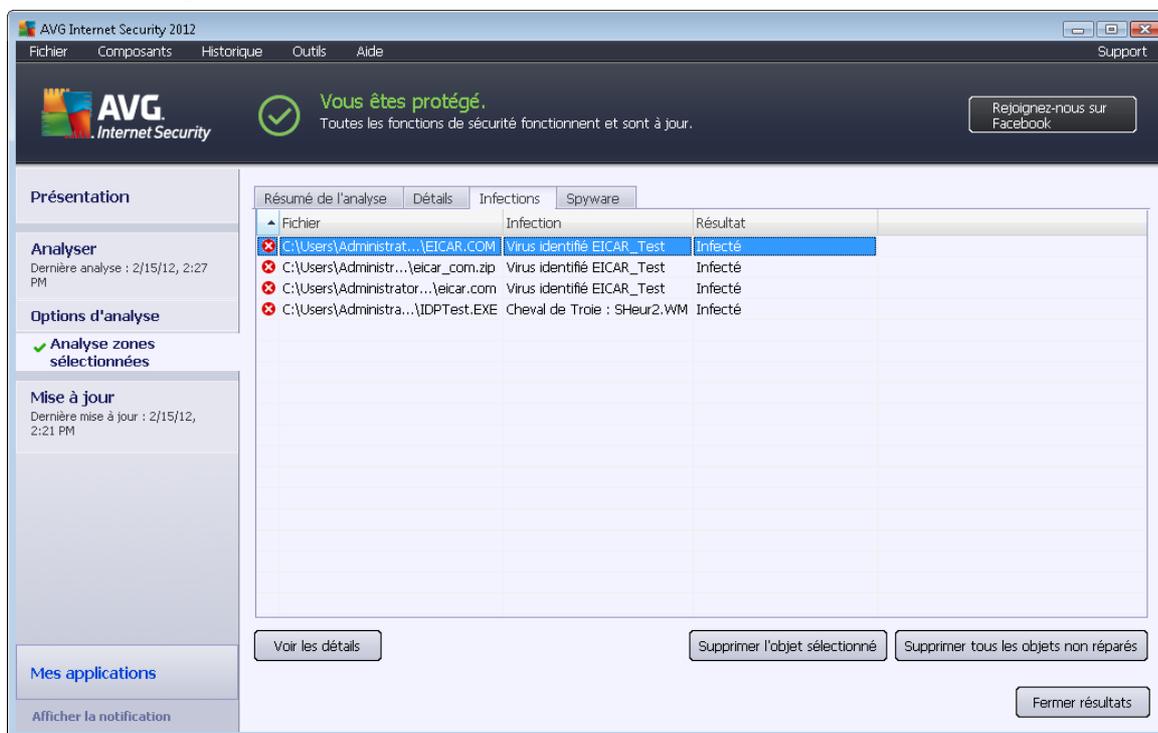
- les infections / spywares détectés
- les infections / spywares supprimés
- le nombre d'infections / de spywares qui n'ont pu être supprimés ou réparés

De plus, l'onglet signale la date et l'heure exactes du début de l'analyse, le nombre total d'objets analysés, la durée de l'analyse et le nombre d'erreurs qui se sont produites au cours de l'analyse.

#### Boutons de commande

Cette boîte de dialogue comporte un seul bouton de commande. Le bouton **Fermer résultats**, qui vous renvoie à la boîte de dialogue [Résultats d'analyse](#).

## 12.7.2. Onglet Infections



L'onglet **Infections** apparaît dans la boîte de dialogue **Résultats des analyses** seulement si une infection virale est identifiée au cours de l'analyse. L'onglet comporte trois parties contenant les informations suivantes :

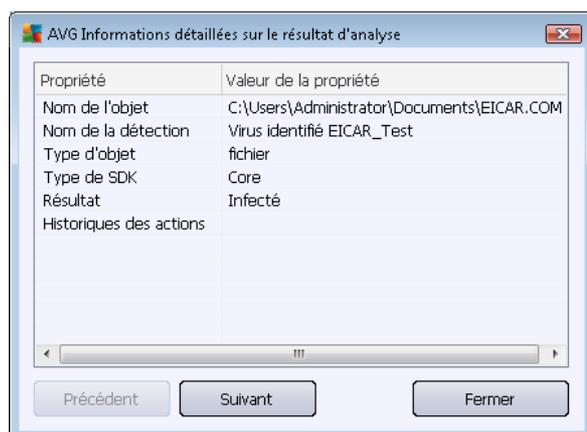
- **Fichier** – chemin complet vers l'emplacement d'origine de l'objet infecté
- **Infections** - nom du virus détecté (*pour plus de détails sur un virus particulier, consultez l'[Encyclopédie des virus](#) en ligne*)
- **Résultat** – indique l'état actuel de l'objet infecté détecté :
  - **Infecté** - l'objet infecté détecté a été laissé à son emplacement d'origine (*si, par exemple, vous avez [désactivé l'option de réparation automatique](#) pour une analyse spécifique*)
  - **Réparé** - l'objet infecté détecté a été réparé et conservé à son emplacement d'origine
  - **Placé en quarantaine** - l'objet infecté a été déplacé en [Quarantaine](#)
  - **Supprimé** - l'objet infecté a été supprimé
  - **Ajouté aux exceptions PUP** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue [Exceptions PUP](#) des paramètres avancés*)

- **Fichier verrouillé** – non vérifié - l'objet considéré est verrouillé, AVG ne peut donc pas l'analyser
- **Objet potentiellement dangereux** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (*il contient par exemple des macros*) ; cette information est fournie à titre d'avertissement uniquement
- **Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

### Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

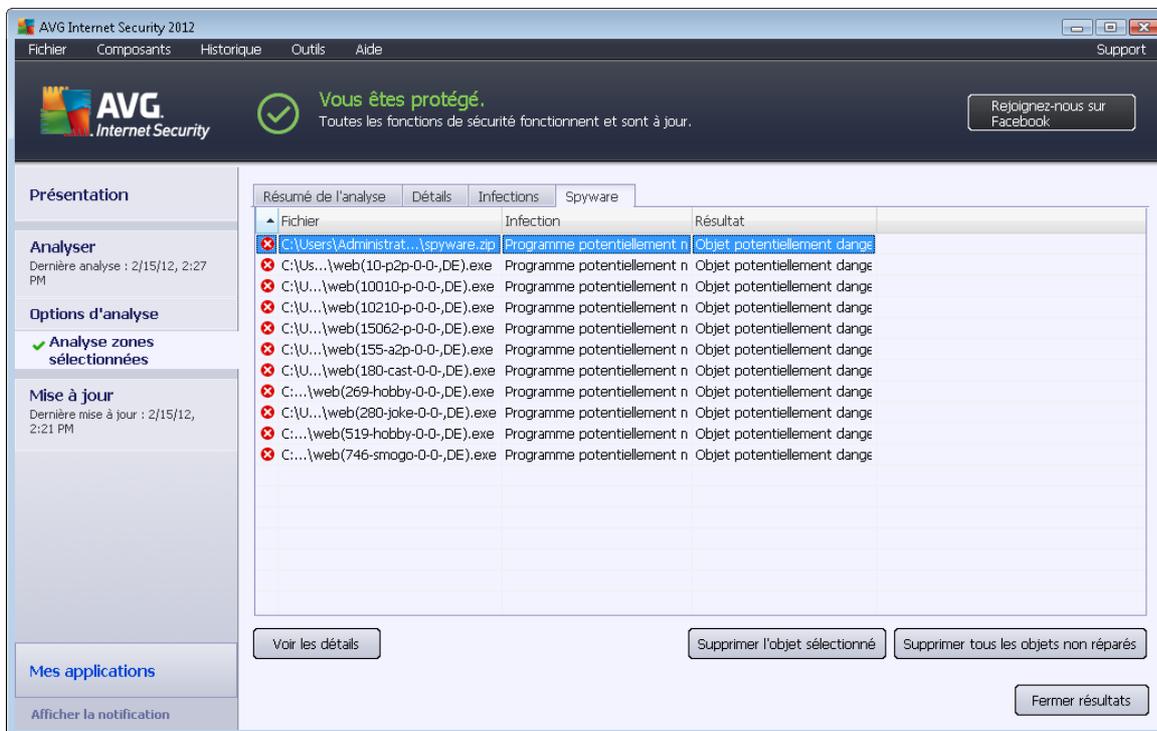
- **Voir les détails** - le bouton ouvre la boîte de dialogue des **informations détaillées sur l'objet** :



Dans cette boîte de dialogue, vous trouverez des informations détaillées sur l'objet infectieux détecté (*ex : nom et emplacement de l'objet infecté, type d'objet, type SDK, résultat de la détection et historique des actions liées à l'objet détecté*). Les boutons **Précédent** et **Suivant** vous donnent accès aux informations sur des résultats spécifiques. Le bouton **Fermer** permet de quitter la boîte de dialogue.

- **Supprimer l'objet sélectionné** – servez-vous de ce bouton pour mettre les objets trouvés en [quarantaine](#)
- **Supprimer tous les objets non réparés** – ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en [quarantaine](#)
- **Fermer résultats** - met fin aux informations détaillées et renvoie la boîte de dialogue [Résultats d'analyse](#)

### 12.7.3. Onglet Spywares



AVG Internet Security 2012

Fichier Composants Historique Outils Aide Support

**AVG** Internet Security

 **Vous êtes protégé.**  
Toutes les fonctions de sécurité fonctionnent et sont à jour.

Rejoignez-nous sur Facebook

Présentation

Analyser  
Dernière analyse : 2/15/12, 2:27 PM

Options d'analyse  
✓ Analyse zones sélectionnées

Mise à jour  
Dernière mise à jour : 2/15/12, 2:21 PM

Mes applications  
Afficher la notification

Résumé de l'analyse Détails Infections Spyware

Fichier	Infection	Résultat
C:\Users\Administrat...\spyware.zip	Programme potentiellement n	Objet potentiellement dange
C:\Us...\web(10-p2p-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:\U...\web(10010-p-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:\U...\web(10210-p-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:\U...\web(15062-p-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:\U...\web(155-a2p-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:\U...\web(180-cast-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:...web(269-hobby-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:\U...\web(280-joke-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:...web(519-hobby-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange
C:...web(746-smogo-0-0-,DE).exe	Programme potentiellement n	Objet potentiellement dange

Voir les détails

Supprimer l'objet sélectionné

Supprimer tous les objets non réparés

Fermer résultats

L'onglet **Spyware** apparaît dans la boîte de dialogue **Résultats des analyses** seulement si un spyware a été détecté au cours de l'analyse. L'onglet comporte trois parties contenant les informations suivantes :

- **Fichier** – chemin complet vers l'emplacement d'origine de l'objet infecté
- **Infections** – nom du spyware détecté (*pour en savoir plus sur un virus particulier, consultez l'[Encyclopédie des virus](#) en ligne*)
- **Résultat** – indique l'état actuel de l'objet infecté détecté :
  - **Infecté** – l'objet infecté détecté a été laissé à son emplacement d'origine (*si, par exemple, vous avez [désactivé l'option de réparation automatique](#) pour une analyse spécifique*)
  - **Réparé** - l'objet infecté détecté a été réparé et conservé à son emplacement d'origine
  - **Placé en quarantaine** – l'objet infecté a été mis en [Quarantaine](#)
  - **Supprimé** - l'objet infecté a été supprimé
  - **Ajouté aux exceptions PUP** - l'objet détecté est considéré comme une exception et est inclus dans la liste des exceptions PUP (*liste configurée dans la boîte de dialogue [Exceptions PUP](#) des paramètres avancés*)
  - **Fichier verrouillé – non vérifié** - l'objet considéré est verrouillé, AVG ne peut donc

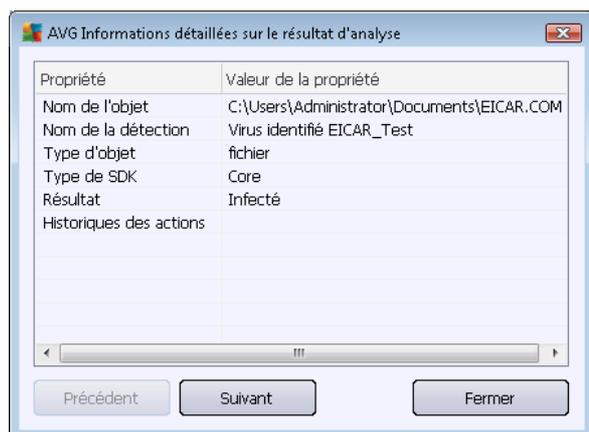
pas l'analyser

- **Objet potentiellement dangereux** - l'objet est considéré comme potentiellement dangereux, mais n'est pas infecté (il contient par exemple des macros) ; cette information est fournie à titre d'avertissement uniquement
- **Un redémarrage de l'ordinateur est nécessaire pour terminer l'opération** - l'objet infecté ne peut pas être supprimé ; pour ce faire, il faut redémarrer l'ordinateur

### Boutons de commande

Cette boîte de dialogue compte trois boutons de commande :

- **Voir les détails** - le bouton ouvre la boîte de dialogue des **informations détaillées sur l'objet** :



Dans cette boîte de dialogue, vous trouverez des informations détaillées sur l'objet infectieux détecté (ex : *nom et emplacement de l'objet infecté, type d'objet, type SDK, résultat de la détection et historique des actions liées à l'objet détecté*). Les boutons **Précédent** et **Suivant** vous donnent accès aux informations sur des résultats spécifiques. Le bouton **Fermer** permet de quitter la boîte de dialogue.

- **Supprimer l'objet sélectionné** – servez-vous de ce bouton pour mettre les objets trouvés en [quarantaine](#)
- **Supprimer tous les objets non réparés** – ce bouton supprime tous les objets trouvés qui ne peuvent être désinfectés, ni placés en [quarantaine](#)
- **Fermer résultats** – met fin aux informations détaillées et ouvre la boîte de dialogue [Résultats d'analyse](#)

#### 12.7.4. Onglet Avertissements

L'onglet **Avertissements** affiche des informations sur les objets "suspects" (*généralement des fichiers*) trouvés au cours de l'analyse. Lorsqu'ils sont détectés par le Bouclier résident, l'accès à ces fichiers est bloqué. Voici des exemples types de ce genre d'objets : fichiers masqués, cookies,



clés de registre suspectes, documents protégés par un mot de passe, archives, etc. De tels fichiers ne présentent pas de menace directe pour l'ordinateur ou sa sécurité. Les informations relatives à ces fichiers sont généralement utiles lorsque la présence d'adwares ou de spywares est décelée dans votre ordinateur. Si les résultats d'analyse ne contiennent que des avertissements détectés par **AVG Internet Security 2012**, aucune action de votre part n'est nécessaire.

Cette rubrique décrit brièvement les exemples les plus courants de tels objets :

- **Fichiers masqués** - Les fichiers masqués sont, par défaut, non visibles et certains virus ou autres menaces peuvent empêcher leur détection en stockant leurs fichiers avec cet attribut. Si **AVG Internet Security 2012** signale un fichier masqué que vous soupçonnez d'être dangereux, vous pouvez le confiner en [Quarantaine](#).
- **Cookies** – Les cookies sont des fichiers texte bruts utilisés par les sites Web pour stocker des informations propres à l'utilisateur. Elles permettent ultérieurement de charger un contenu personnalisé d'un site Web, de saisir automatiquement le nom d'utilisateur, etc.
- **Clés de registre suspectes** - Certains programmes malveillants stockent leurs informations dans la base de registre de Windows. De cette manière, elles sont chargées au démarrage ou peuvent s'immiscer dans le système d'exploitation.

### 12.7.5. Onglet Rootkits

L'onglet **Rootkits** affiche des informations sur les rootkits détectés au cours de l'analyse anti-rootkit comprise dans l'[Analyse complète de l'ordinateur](#).

Un [rootkit](#) est un programme conçu pour prendre le contrôle du système, sans l'autorisation de son propriétaire et de son administrateur légitime. Un accès matériel est rarement nécessaire car un rootkit est prévu pour s'introduire dans le système d'exploitation exécuté sur le matériel. En règle générale, les rootkits dissimulent leur présence dans le système en dupant ou en contournant les mécanismes de sécurité standard du système d'exploitation. Souvent, ils prennent la forme de chevaux de Troie et font croire aux utilisateurs que leur exécution est sans danger pour leurs ordinateurs. Pour parvenir à ce résultat, différentes techniques sont employées : dissimulation de processus aux programmes de contrôle ou masquage de fichiers ou de données système, au système d'exploitation.

La structure de cet onglet est quasiment la même que celle de l'[onglet Infections](#) ou de l'[onglet Spyware](#).

### 12.7.6. Onglet Informations

L'onglet **Informations** contient des renseignements sur des "objets trouvés" qui ne peuvent pas être classés dans les catégories infections, spywares, etc. Il est impossible de les qualifier de dangereux de manière formelle, mais ils réclament malgré tout votre attention. L'analyse **AVG Internet Security 2012** peut détecter des fichiers qui ne sont pas infectés, mais seulement suspects. Ces fichiers sont signalés par le biais d'un [avertissement](#) ou d'une information.

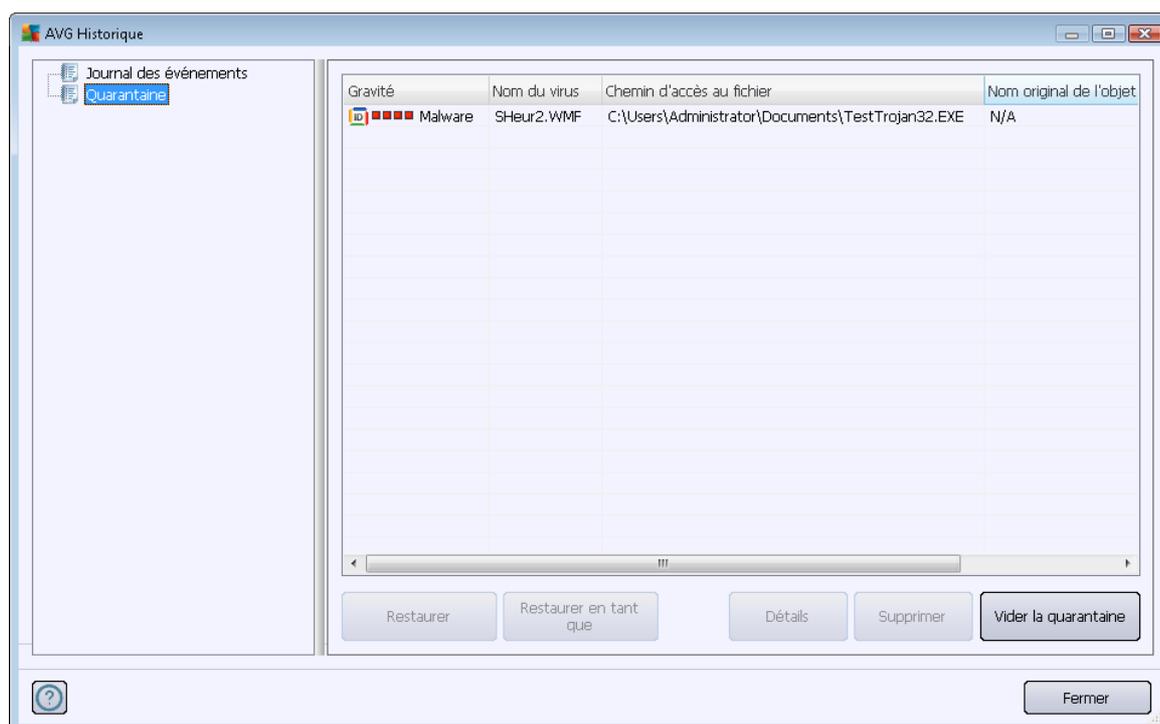
Les raisons suivantes peuvent expliquer la gravité des **informations** :

- **Mode de compression** - Le fichier a été compressé avec l'un des systèmes de compression les moins connus, peut-être dans le but d'en empêcher l'analyse par AVG. Cependant, il n'est pas dit qu'un tel résultat indique que ce fichier contienne un virus.



- **Mode de compression récursif** – Semblable au précédent, mais moins fréquent parmi les logiciels les plus connus. Ces fichiers sont malicieux et leur suppression ou envoi à AVG pour analyse doit être envisagé.
- **Archive ou document protégé par mot de passe** - Les fichiers protégés par mot de passe ne peuvent pas être analysés par **AVG Internet Security 2012** (ou par d'autres programmes anti-malwares).
- **Document contenant des macros** – Le document signalé contient des macros potentiellement dangereuses.
- **Extension cachée** – Les fichiers munis d'une extension cachée peuvent apparaître comme des images alors qu'en réalité ce sont des fichiers exécutables (exemple : *image.jpg.exe*). Par défaut, la deuxième extension n'est pas visible sur Windows et **AVG Internet Security 2012** signale ce genre de fichiers afin d'en empêcher l'ouverture accidentelle.
- **Chemin d'accès au fichier incorrect** - Si un fichier système important est exécuté à partir d'un chemin d'accès autre que celui par défaut (exemple : *winlogon.exe* exécuté à partir d'un dossier autre que Windows), signale cette contradiction.**AVG Internet Security 2012** Dans certains cas, les virus utilisent des noms de processus système standards afin de se dissimuler au système.
- **Fichier verrouillé** - Le fichier signalé est verrouillé et, de ce fait, **AVG Internet Security 2012** ne peut pas l'analyser. En général, il s'agit d'un fichier qui est constamment utilisé par le système (par exemple, un fichier d'échange).

## 12.8. Quarantaine





La **quarantaine** offre un environnement parfaitement sûr pour la manipulation des objets infectés ou susceptibles de l'être, détectés au cours des analyses AVG. Lorsqu'un objet infecté est repéré par l'analyse et qu'AVG n'est pas en mesure de le réparer automatiquement, un message vous invite à indiquer la mesure à prendre. Il est recommandé de placer l'objet en **Quarantaine** afin de le traiter ultérieurement. Le principal objet de la **quarantaine** consiste à conserver en lieu sûr et durant un laps de temps défini, tout fichier supprimé lors de l'analyse au cas où vous auriez besoin de ces fichiers ultérieurement. Si l'absence du fichier entraîne des problèmes, envoyez-nous le fichier pour analyse ou restaurez-le à son emplacement d'origine.

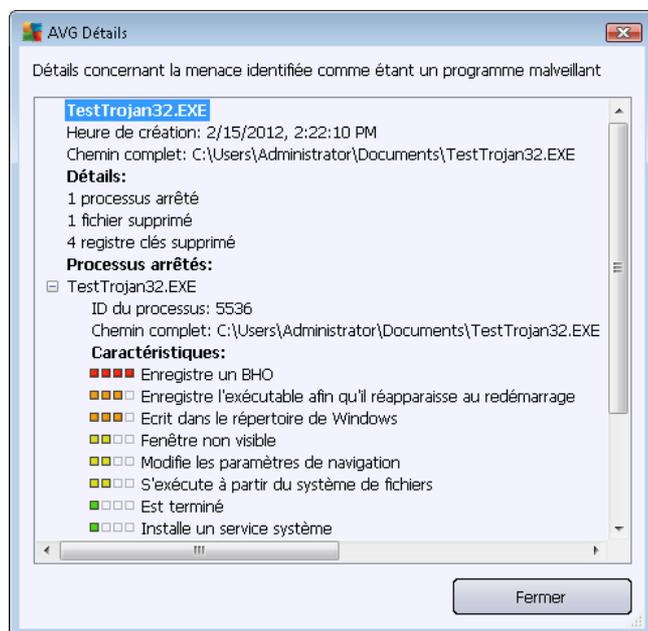
L'interface **Quarantaine** s'affiche dans une fenêtre différente et présente des informations générales sur les objets infectés et mis en quarantaine :

- **Gravité** – si vous choisissez d'installer le composant [Identity Protection](#) dans **AVG Internet Security 2012**, les objets trouvés sont classés (indication visuelle) selon une échelle à quatre niveaux allant de sécurisé (■□□□) jusqu'à très dangereux (■□□■). Vous avez également accès à des informations sur le type d'infection (*en fonction de leur niveau d'infection ; tous les objets reportés sont infectés ou le sont potentiellement*)
- **Nom du virus** – spécifie le nom de l'infection décelée conformément à l'[Encyclopédie des virus](#) (*disponible en ligne*)
- **Chemin d'accès au fichier** – chemin d'accès menant à l'origine du fichier infectieux
- **Nom original de l'objet** – tous les objets détectés figurant dans la liste portent un nom standard attribué par AVG au cours du processus d'analyse. Si le nom initial de l'objet est connu (*telle qu'une pièce jointe qui ne correspond pas au contenu véritable de la pièce jointe*), il sera indiqué dans cette colonne.
- **Date de l'enregistrement** – date et heure à laquelle le fichier a été trouvé et placé en quarantaine

### Boutons de commande

Les boutons de commande suivants sont accessibles depuis l'interface **Quarantaine** :

- **Restaurer** - rétablit le fichier infecté à sa place d'origine, sur le disque
- **Restaurer en tant que** - transfère le fichier infecté dans le dossier sélectionné
- **Détails** – ce bouton s'applique seulement aux menaces détectées par [Identity Protection](#). Après avoir activé le bouton, une présentation synthétique des détails des menaces s'affiche (*fichiers/processus affectés, caractéristiques du processus, etc.*). Notez que pour tous les éléments détectés autrement que par IDP, ce bouton est grisé et inactif.



- **Supprimer** – supprime définitivement le fichier infecté de la **Quarantaine**
- **Vider la quarantaine** – Vider intégralement le contenu de la **Quarantaine**. Lorsque vous supprimez des fichiers de la **quarantaine**, **ils sont définitivement effacés du disque dur** (ils ne sont pas mis dans la Corbeille).



## 13. Mises à jour d'AVG

Aucun logiciel de sécurité ne peut garantir une protection fiable contre la diversité des menaces, à moins d'une mise à jour régulière. Les auteurs de virus sont toujours à l'affût de nouvelles failles des logiciels ou des systèmes d'exploitation. Chaque jour apparaissent de nouveaux virus, malwares et attaques de pirates. C'est pour cette raison que les éditeurs de logiciels ne cessent de diffuser des mises à jour et des correctifs de sécurité visant à combler les vulnérabilités identifiées.

Au regard de toutes les menaces informatiques apparues récemment et de la vitesse à laquelle elles se propagent, il est absolument essentiel de mettre **AVG Internet Security 2012** à jour régulièrement. La meilleure solution est de conserver les paramètres par défaut du programme en ce qui concerne les mises à jour automatiques. Notez que si la base virale de votre programme **AVG Internet Security 2012** n'est pas à jour, ce dernier ne sera pas en mesure de détecter les menaces les plus récentes !

***C'est pourquoi il est essentiel de mettre régulièrement à jour votre produit AVG ! Les mises à jours de définitions de virus fondamentales doivent être exécutées quotidiennement si possible. Les mises à jour du programme, moins urgentes, peuvent se faire sur une base hebdomadaire.***

### 13.1. Exécution de mises à jour

Afin d'optimiser la sécurité, **AVG Internet Security 2012** est programmé par défaut pour rechercher de nouvelles mises à jour toutes les quatre heures. Les mises à jour d'AVG n'étant pas publiées selon un calendrier fixe, mais plutôt en réaction au nombre et à la gravité des nouvelles menaces, il est très important d'effectuer cette vérification pour garantir la mise à jour permanente de votre base de données virale AVG.

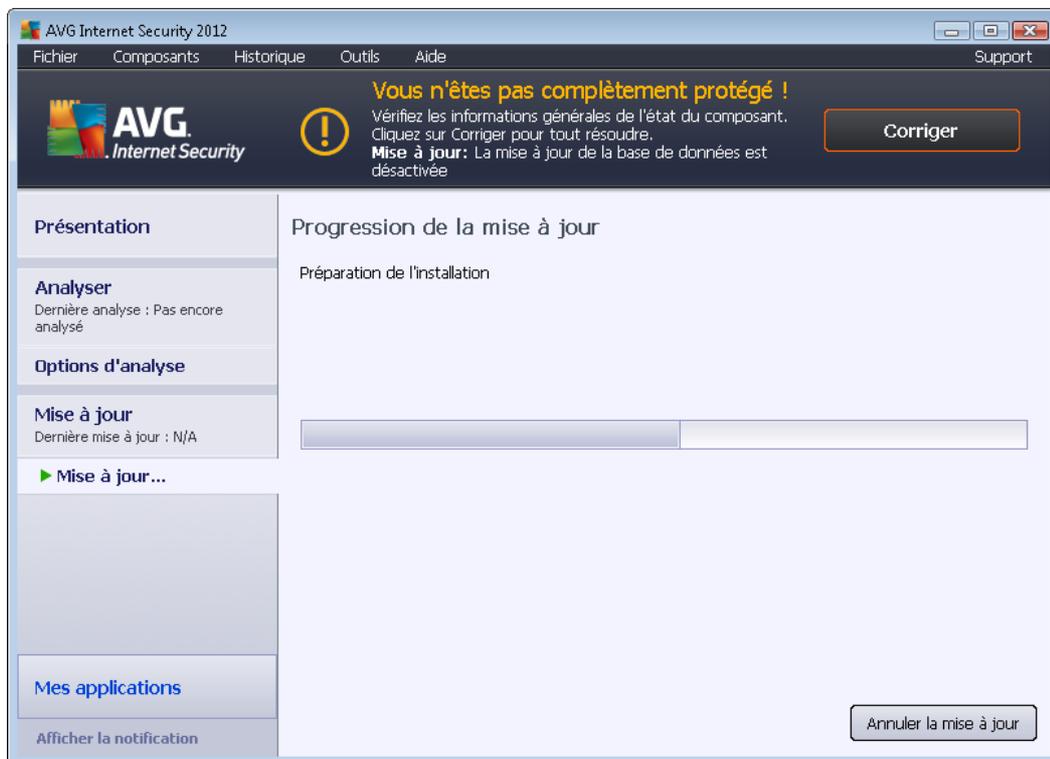
Si vous souhaitez réduire le nombre de mises à jour, vous pouvez définir vos propres paramètres d'exécution de ce type d'opération. Toutefois, il est fortement recommandé d'exécuter au moins une mise à jour par jour ! Pour modifier la configuration, ouvrez les boîtes de dialogue de la section [Paramètres avancés/Programmations](#) suivantes :

- [Programmation de la mise à jour des définitions](#)
- [Programmation de la mise à jour du programme](#)
- [Programmation des mises à jour de l'Anti-Spam](#)

Pour rechercher immédiatement de nouvelles mises à jour, cliquez sur le lien d'accès rapide [Mise à jour](#) de l'interface utilisateur principale. Ce lien est constamment disponible, quelle que soit la boîte de dialogue ouverte dans l'[interface utilisateur](#).

### 13.2. Progression de la mise à jour

Lorsque vous lancez la mise à jour, AVG vérifie en premier lieu si de nouveaux fichiers de mise à jour sont disponibles. Dans l'affirmative, **AVG Internet Security 2012** lance leur téléchargement et exécute le processus qui effectue la mise à jour. Au cours du processus de mise à jour, l'interface de **Mise à jour** s'affiche. Elle permet d'observer le déroulement de la procédure sous forme graphique et présente des données statistiques pertinentes (*taille du fichier de mise à jour, données reçues, vitesse du téléchargement, temps écoulé, etc.*) :



**Remarque :** avant chaque exécution de la mise à jour du programme AVG, un point de restauration est créé. En cas d'échec de la mise à jour et de blocage du système d'exploitation, vous avez alors la possibilité de restaurer le système d'exploitation tel qu'il était configuré à partir de ce point. Cette option est disponible via le menu Windows : Démarrer / Tous les programmes / Accessoires / Outils système / Restauration du système. Option destinée aux utilisateurs expérimentés seulement !

### 13.3. Niveaux de la mise à jour

AVG Internet Security 2012 permet de choisir parmi deux niveaux de mise à jour :

- **La mise à jour des définitions** inclut les modifications nécessaires à une protection efficace contre les virus, le spam et les programmes malveillants. En règle générale, cette action ne s'applique pas au code. Seule la base de données de définition est concernée. Il est conseillé d'effectuer cette mise à jour dès qu'elle est disponible.
- **La mise à jour du programme** contient diverses modifications, corrections et améliorations.

En [programmant une mise à jour](#), il est possible de définir des paramètres spécifiques pour les deux niveaux de mise à jour :

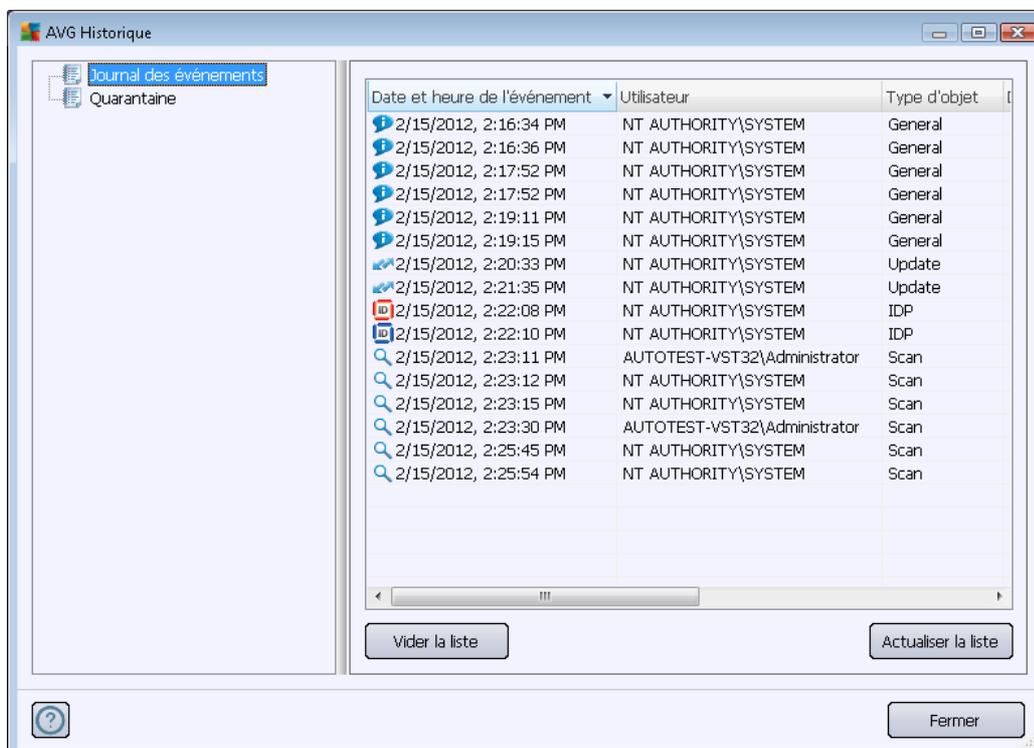
- [Programmation de la mise à jour des définitions](#)
- [Programmation de la mise à jour du programme](#)

**Remarque :** si une mise à jour planifiée du programme coïncide avec une analyse programmée, le



*processus de mise à jour a priorité sur l'analyse qui est interrompue.*

## 14. Journal des évènements



La boîte de dialogue **Journal de l'historique des évènements** est accessible par la [barre de menus](#), menu **Historique**, puis **Journal de l'historique des évènements**. Dans cette boîte de dialogue, vous trouverez un résumé des évènements les plus importants survenus pendant l'exécution du programme **AVG Internet Security 2012**. La commande **Journal de l'historique des évènements** enregistre les types d'évènements suivants :

- Informations au sujet des mises à jour de l'application AVG
- Informations sur l'heure de début, de fin ou d'interruption de l'analyse (*y compris pour les analyses effectuées automatiquement*)
- Informations sur les évènements liés à la détection des virus (*par le [Bouclier résident](#) ou résultant de l'[analyse](#)*) avec indication de l'emplacement des occurrences
- Autres évènements importants

Pour chaque évènement, les informations suivantes s'affichent :

- **Date et heure de l'évènement** donne la date et l'heure exactes de l'évènement
- **Utilisateur** indique le nom de l'utilisateur actuellement connecté au moment de l'occurrence de l'évènement
- **Source** fournit des informations sur le composant source ou une autre partie du système AVG qui a déclenché l'évènement



- **Description de l'évènement** donne un bref résumé de ce qui s'est réellement passé

#### **Boutons de commande**

- **Vider la liste** permet de supprimer toutes les entrées de la liste des évènements
- **Actualiser la liste** permet de mettre à jour toutes les entrées de la liste des évènements



## 15. FAQ et assistance technique

Si vous rencontrez des difficultés d'ordre commercial ou technique avec votre application **AVG Internet Security 2012**, il existe plusieurs méthodes pour obtenir de l'aide. Choisissez l'une de ces trois options :

- **Obtenir de l'aide** : Vous pouvez accéder à la page dédiée du support clients du site Web d'AVG directement à partir de l'application AVG (<http://www.avg.com/>). Sélectionnez la commande du menu principal **Aide / Obtenir de l'aide** pour être redirigé vers le site Web d'AVG contenant toutes les solutions de support disponibles. Suivez les instructions fournies sur la page Web pour poursuivre la procédure.
- **Support (lien du menu principal)** : Le menu de l'application AVG (*dans la partie supérieure de l'interface utilisateur principale*) comporte un lien **Support** qui permet d'ouvrir une nouvelle boîte de dialogue contenant toutes les informations dont vous pourriez avoir besoin pour rechercher de l'aide. Vous y trouverez des données de base relatives à l'application AVG installée (*version de l'application / de la base de données*), les informations de licence et une liste de liens d'accès rapide au support:



- **Résolution des problèmes dans le fichier d'aide** : Une nouvelle section **Résolution des problèmes** est disponible directement dans le fichier d'aide inclus dans **AVG Internet Security 2012** (*pour ouvrir le fichier d'aide, appuyez sur la touche F1 à partir de n'importe quelle boîte de dialogue de l'application*). Cette section fournit la liste des situations les plus courantes que peut rencontrer un utilisateur lorsqu'il recherche une aide professionnelle pour résoudre un problème technique. Cliquez sur la situation qui décrit le mieux votre problème afin d'obtenir des instructions détaillées sur la manière de le résoudre.
- **Site Web du Centre de support d'AVG** : Vous pouvez également rechercher la solution à



votre problème sur le site Web d'AVG (<http://www.avg.com/>). Dans la section **Centre de support**, vous trouverez une vue d'ensemble structurée des groupes thématiques abordant aussi bien les questions liées à l'achat que celles de nature technique.

- **Foire aux questions** : Sur le site Web d'AVG (<http://www.avg.com/>), vous trouverez également une section distincte et bien élaborée regroupant les questions fréquemment posées. Cette section est accessible via l'option de menu **Centre de support / FAQ**. Encore une fois, les questions sont clairement réparties dans différentes catégories : achats, sujets techniques et virus.
- **A propos des virus et des menaces** : Un chapitre spécifique du site Web d'AVG (<http://www.avg.com/>) est dédié aux problèmes liés aux virus (*la page Web est accessible à partir du menu principal via l'option Aide / A propos des virus et des menaces*). Dans le menu, sélectionnez **Centre de support / A propos des virus et des menaces** pour accéder à une page fournissant une vue d'ensemble structurée d'informations liées aux menaces sur Internet. Vous y trouverez également des instructions sur la manière de supprimer les virus et spyware et des conseils sur la manière de rester protégé.
- **Forum de discussion** : Vous pouvez également utiliser le forum de discussion des utilisateurs d'AVG à l'adresse : <http://forums.avg.com>.