ESET Smart Security 4

Guide de l'utilisateur

(versions 4.2 et supérieures)

Microsoft® Windows® 7 / Vista / XP / 2000 / 2003 / 2008

ESET Smart Security 4

Service client Monde : www.eset.eu/support
Service client Amérique du Nord : www.eset.com/support

REV.20100225-015

Sommaire

1. ESET Smart Security 4 4

1.1 Nouveautés 4
1.2 Configuration minimale requise 5

2. Installation 6

2.1 Installation typique 6
2.2 Installation personnalisée 7
2.3 Utilisation des paramètres d'origine 9
2.4 Entrée d'un nom d'utilisateur et d'un mot de passe 9
2.5 Analyse d'ordinateur à la demande 9

3. Guide du débutant 10

3.1 Présentation de l'interface utilisateur : les modes 10
3.1.1 Contrôle du fonctionnement du système 10
3.1.2 Que faire lorsque le programme ne fonctionne pas correctement 11
3.2 Configuration des mises à jour 11
3.3 Configuration de zone de confiance 11
3.4 Configuration du serveur proxy 12
3.5 Protection des paramètres 12

4. Utilisation d'ESET Smart Security 13

4.1 Protection antivirus et anti-logiciels espions 13
4.1.1 Protection en temps réel du système de fichiers 13
4.1.1.1 Configuration du contrôle 13
4.1.1.1.1 Supports à analyser 13
4.1.1.1.2 Analyser quand (Analyse déclenchée par un événement) 13
4.1.1.1.3 Autres paramètres ThreatSense pour les fichiers nouveaux et modifiés 13
4.1.1.1.4 Configuration avancée 13
4.1.1.2 Niveaux de nettoyage 13
4.1.1.3 Quand faut-il modifier la configuration la protection en temps réel 14
4.1.1.4 Vérification de la protection en temps réel 14
4.1.1.5 Que faire si la protection en temps réel ne fonctionne pas 14
4.1.2 Le système de prévention d'intrusiosns HIPS 14
4.1.3 Protection du client de messagerie 14
4.1.3.1 Contrôle POP3 14
4.1.3.1.1 Compatibilité 15
4.1.3.2 Intégration aux clients de messagerie 15
4.1.3.2.1 Ajout d'une étiquette au corps d'un courrier 15
4.1.3.3 Suppression d'infiltrations 16
4.1.4 Protection de l'accès Web 16
4.1.4.1 HTTP, HTTPs 16
4.1.4.1.1 Gestion d'adresse 16
4.1.4.1.2 Navigateurs Web 16
4.1.5 Analyse de l'ordinateur 17
4.1.5.1 Type d'analyse 17
4.1.5.1.1 Analyse standard 17
4.1.5.1.2 Analyse personnalisée 17
4.1.5.2 Cibles à analyser 17
4.1.5.3 Profils d'analyse 18
4.1.6 Filtrage des protocoles 18

4.1.6.1 SSL ... 18
4.1.6.1.1 Certificats approuvés ... 19
4.1.6.1.2 Certificats exclus ... 19
4.1.7 Configuration du moteur ThreatSense ... 19
4.1.7.1 Configuration des objets ... 19
4.1.7.2 Options ... 19
4.1.7.3 Nettoyage ... 20
4.1.7.4 Extensions ... 20
4.1.7.5 Limites ... 20
4.1.7.6 Autre ... 21
4.1.8 Une infiltration est détectée ... 21
4.2 Pare-feu personnel ... 21
4.2.1 Modes de filtrage ... 21
4.2.2 Profils ... 22
4.2.2.1 Gestion des profils ... 22
4.2.3 Bloquer tout le trafic réseau : déconnecter le réseau ... 22
4.2.4 Désactiver le filtrage : autoriser tout le trafic ... 22
4.2.5 Configuration et utilisation des règles ... 23
4.2.5.1 Création de nouvelles règles ... 23
4.2.5.2 Modification des règles ... 24
4.2.6 Configuration des zones ... 24
4.2.6.1 Authentification réseau ... 24
4.2.6.1.1 Authentification de zone – Configuration du client ... 24
4.2.6.1.2 Authentification de zone – Configuration du serveur ... 25
4.2.7 Établissement d'une connexion – détection ... 25
4.2.8 Journalisation ... 26
4.3 Protection contre le courrier indésirable ... 26
4.3.1 Auto-apprentissage du courrier indésirable ... 27
4.3.1.1 Ajout d'adresses à la liste blanche ... 27
4.3.1.2 Marquage de messages comme courrier indésirable ... 27
4.4 Mise à jour du programme ... 27
4.4.1 Configuration des mises à jour ... 27
4.4.1.1 Profils de mise à jour ... 28
4.4.1.2 Configuration avancée des mises à jour ... 28
4.4.1.2.1 Mode de mise à jour ... 28
4.4.1.2.2 Serveur proxy ... 29
4.4.1.2.3 Connexion au réseau local ... 29
4.4.1.2.4 Création de copies de mises à jour : miroir ... 30
4.4.1.2.4.1 Mise à jour à partir du miroir ... 30
4.4.1.2.4.2 Résolution des problèmes de miroir de mise à jour ... 31
4.4.2 Comment créer des tâches de mise à jour ... 31
4.5 Planificateur ... 31
4.5.1 Pourquoi planifier des tâches ... 31
4.5.2 Création de nouvelles tâches ... 32
4.6 Quarantaine ... 32
4.6.1 Mise de fichiers en quarantaine ... 32
4.6.2 Restaurer depuis la quarantaine ... 32
4.6.3 Soumission de fichiers de quarantaine ... 32
4.7 Fichiers journaux ... 33
4.7.1 Maintenance des journaux ... 33
4.8 Interface utilisateur ... 34
4.8.1 Alertes et notifications ... 34
4.9 ThreatSense.Net ... 35
4.9.1 Fichiers suspects ... 35
4.9.2 Statistiques ... 36
4.9.3 Soumission ... 36
4.10 Administration à distance ... 36
4.11 Licence ... 37

5. Utilisateur chevronné ... 38

5.1 Configuration du serveur proxy ... 38
5.2 Importer/exporter des paramètres ... 38
5.2.1 Exporter les paramètres ... 38
5.2.2 Importer des paramètres ... 38
5.3 Ligne de commande ... 38
5.4 ESET SysInspector ... 39
5.4.1 Interface utilisateur et utilisation de l'application ... 39
5.4.1.1 Contrôles du programme ... 40
5.4.1.2 Navigation dans ESET SysInspector ... 40
5.4.1.3 Comparer ... 41
5.4.1.4 SysInspector comme composant d'ESET Smart Security 4 ... 41
5.4.1.5 Script de service ... 42
5.4.1.5.1 Génération de scripts de service ... 42
5.4.1.5.2 Structure du script de service ... 42
5.4.1.5.3 Comment exécuter les scripts de service ... 43
5.5 ESET SysRescue ... 43
5.5.1 Configuration requise ... 43
5.5.2 Comment créer un CD de sauvetage ... 44
5.5.2.1 Dossiers ... 44
5.5.2.2 Antivirus ESET ... 44
5.5.2.3 Avancé ... 44
5.5.2.4 Périphérique USB d'amorçage ... 44
5.5.2.5 Graver ... 44
5.5.3 Utilisation d'ESET SysRescue ... 45
5.5.3.1 Utilisation d'ESET SysRescue ... 45

6. Glossaire ... 46

6.1 Types d'infiltrations ... 46
6.1.1 Virus ... 46
6.1.2 Vers ... 46
6.1.3 Chevaux de Troie ... 46
6.1.4 Rootkits ... 46
6.1.5 Logiciels publicitaires ... 47
6.1.6 Logiciels espions ... 47
6.1.7 Applications potentiellement dangereuses ... 47
6.1.8 Applications potentiellement indésirables ... 47
6.2 Types d'attaques distantes ... 47
6.2.1 Attaques DoS ... 47
6.2.2 Empoisonnement DNS ... 47
6.2.3 Attaques de vers ... 47
6.2.4 Balayage de ports ... 48
6.2.5 Désynchronisation TCP ... 48
6.2.6 Relais SMB ... 48
6.2.7 Attaques par protocole ICMP ... 48
6.3 Courrier électronique ... 48
6.3.1 Publicités ... 48
6.3.2 Canulars (hoax) ... 49
6.3.3 Hameçonnage ... 49
6.3.4 Reconnaissance des courriers indésirables ... 49
6.3.4.1 Règles ... 49
6.3.4.2 Filtre bayésien ... 49
6.3.4.3 Liste blanche ... 50
6.3.4.4 Liste noire ... 50
6.3.4.5 Contrôle côté serveur ... 50

1. ESET Smart Security 4

ESET Smart Security 4 est le premier représentant d'une nouvelle approche de sécurité informatique véritablement intégrée. Il s'appuie sur le programme ESET NOD32 Antivirus, dont la rapidité et la précision sont garanties par la dernière version du moteur d'analyse ThreatSense® combiné à un pare-feu personnel et à des modules de blocage du courrier indésirable sur mesure. Le résultat est un système intelligent et constamment en alerte pour protéger votre ordinateur des attaques et des programmes malveillants.

ESET Smart Security n'est pas un simple assemblage de divers produits, comme le propose d'autres fournisseurs. C'est le résultat d'un effort de longue haleine pour tenter d'allier protection maximale et encombrement minimal. Des technologies avancées basées sur l'intelligence artificielle sont capables de faire barrage de manière proactive à la pénétration de virus, de logiciels espions, de chevaux de Troie, de vers, de logiciels publicitaires, de rootkits et autres attaques provenant d'Internet, sans réduire les performances ni perturber votre ordinateur.

1.1 Nouveautés

Nos experts ont su faire valoir leur expérience en dotant le programme ESET Smart Security d'une architecture entièrement nouvelle qui garantit une protection maximale avec une configuration système minimale. Cette solution de sécurité puissante comporte des modules aux options avancées. La liste ci-dessous vous offre un bref aperçu de ces modules.

- **Antivirus et anti-logiciels espions**

Ce module est élaboré à partir du moteur d'analyse de ThreatSense®, utilisé pour la première fois sur le système primé NOD32 Antivirus. Le système ThreatSense® est optimisé et amélioré dans la nouvelle architecture d'ESET Smart Security.

Fonction	Description
Nettoyage amélioré	Le système antivirus nettoie et supprime désormais la plupart des infiltrations détectées sans intervention de l'utilisateur.
Mode d'analyse en arrière-plan	L'analyse de l'ordinateur peut être lancée en arrière-plan sans réduire les performances.
Fichiers de mise à jour de taille réduite	Grâce aux processus d'optimisation du noyau, la taille des fichiers de mise à jour est réduite par rapport à la version 2.7. En outre, la protection des fichiers de mise à jour contre les dommages a été améliorée.
Protection des clients de messagerie les plus populaires	Il est désormais possible d'analyser les messages entrants non seulement de Microsoft Outlook, mais aussi d'Outlook Express, de Windows Live Mail et de Mozilla Thunderbird.
Autres améliorations mineures	– Accès direct aux systèmes de fichiers pour une vitesse et un débit élevés. – Accès bloqué aux fichiers infectés. – Optimisation du Centre de sécurité Windows, Vista inclus.

- **Pare-feu personnel**

Le pare-feu personnel contrôle tout le trafic entre un ordinateur protégé et d'autres ordinateurs sur le réseau. Vous trouverez ci-dessous la description des fonctions avancées du pare-feu personnel ESET.

Fonction	Description
Profils	Les profils permettent de contrôler le comportement du pare-feu personnel ESET Smart Security. Les profils, avec différentes règles attribuées, permettent aux utilisateurs de modifier facilement le comportement du pare-feu personnel.
Authentification de zone	Permet aux utilisateurs d'identifier le réseau auquel ils se connectent et de définir une action (basculement de profil de pare-feu et blocage de la communication avec la zone, par exemple) en fonction de ces informations.
Analyse des communications sur une couche inférieure du réseau	L'analyse des communications réseau sur la couche liaison de données permet au pare-feu personnel de bloquer des attaques qui seraient sinon indétectables.
Prise en charge IPv6	Le pare-feu personnel ESET affiche les adresses IPv6 et permet aux utilisateurs de créer des règles pour ces adresses.
Contrôle des fichiers exécutables	Contrôle des modifications apportées aux fichiers exécutables afin de venir à bout des infections. Il est possible d'autoriser la modification d'applications signées.
Analyse de fichiers intégrée à HTTP(s) et POP3(s)	Analyse de fichiers intégrée aux protocoles d'application HTTP(s) et POP3(s). Les utilisateurs sont protégés lorsqu'ils naviguent sur Internet ou téléchargent des messages électroniques.
Système de détection des intrusions	Possibilité de reconnaître le type d'une communication sur le réseau et des d'attaques sur le réseau, avec option permettant d'interdire automatiquement ces communications.
Mode interactif, basé sur des règles personnalisées, d'apprentissage, automatique et automatique avec exceptions	Les utilisateurs peuvent choisir l'exécution automatique des actions du pare-feu personnel ou définir des règles de manière interactive. Les communications en mode basé sur des règles personnalisées sont traitées selon des règles prédéfinies par l'utilisateur ou l'administrateur du réseau. Le mode d'apprentissage crée et enregistre automatiquement les règles et convient pour la configuration initiale du pare-feu personnel.
Remplace le pare-feu intégré de Windows	Remplaçant le pare-feu intégré de Windows, il interagit également avec le Centre de sécurité Windows de manière à surveiller l'état de la sécurité. L'installation d'ESET Smart Security désactive par défaut le pare-feu Windows.

- **Antispam**

ESET Antispam filtre les messages non sollicités et accroît ainsi la sécurité et le confort des communications électroniques.

Fonction	Description
Système de notation des messages entrants	Tous les messages entrants se voient assigner une note allant de 0 (le message n'est pas du courrier indésirable) à 100 (le message est du courrier indésirable) et sont transférés, selon le résultat, dans le dossier des courriers indésirables ou dans un dossier personnalisé créé par l'utilisateur. Parallèlement, il est possible d'analyser les messages entrants.
Prise en charge de plusieurs techniques d'analyse	– Analyse de Bayes. – Analyse basée sur des règles. – Vérification globale de la base de données d'empreintes.
Intégration totale avec les clients de messagerie	La protection contre le courrier indésirable est actuellement disponible pour les utilisateurs de clients Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird.
Possibilité de sélection manuelle des spams	Option permettant de sélectionner ou de désélectionner manuellement les courriers identifiés comme étant du courrier indésirable.

- **Autres**

Fonction	Description
ESET SysRescue	ESET SysRescue permet à un utilisateur de créer un support CD/DVD/USB amorçable contenant ESET Smart Security, pouvant s'exécuter indépendamment du système d'exploitation. Il convient parfaitement pour débarrasser le système d'infiltrations difficiles à éliminer.
ESET SysInspector	L'application ESET SysInspector, qui inspecte complètement l'ordinateur, est désormais directement intégrée dans ESET Smart Security. Si vous contactez notre service client à l'aide de l'option Aide et assistance > Demande d'assistance du service client (recommandé), vous pouvez inclure un instantané d'état ESET SysInspector de votre ordinateur.
Protection des documents	La protection des documents analyse les documents Microsoft Office avant leur ouverture, ainsi que les fichiers téléchargés automatiquement par Internet Explorer, tels que des éléments Microsoft ActiveX.
Autodéfense	La nouvelle technologie d'autodéfense protège les composants d'ESET Smart Security de toute désactivation par des logiciels malveillants.
Interface utilisateur	L'interface utilisateur peut désormais fonctionner en mode non graphique, ce qui permet un contrôle d'ESET Smart Security par le clavier. La compatibilité accrue avec une application de lecture plein écran permet aux utilisateurs malvoyants de contrôler le programme plus efficacement.

1.2 Configuration minimale requise

Pour assurer le bon fonctionnement d'ESET Smart Security et ESET Smart Security Business Edition, la configuration matérielle et logicielle minimale requise est la suivante :

ESET Smart Security :

Windows 2000, XP	400 MHz 32 bits/64 bits (x86/x64) 128 Mo de RAM de mémoire système 130 Mo d'espace disponible Super VGA (800 × 600)
Windows 7, Vista	1 GHz 32 bits/64 bits (x86/x64) 512 Mo de RAM de mémoire système 130 Mo d'espace disponible Super VGA (800 × 600)

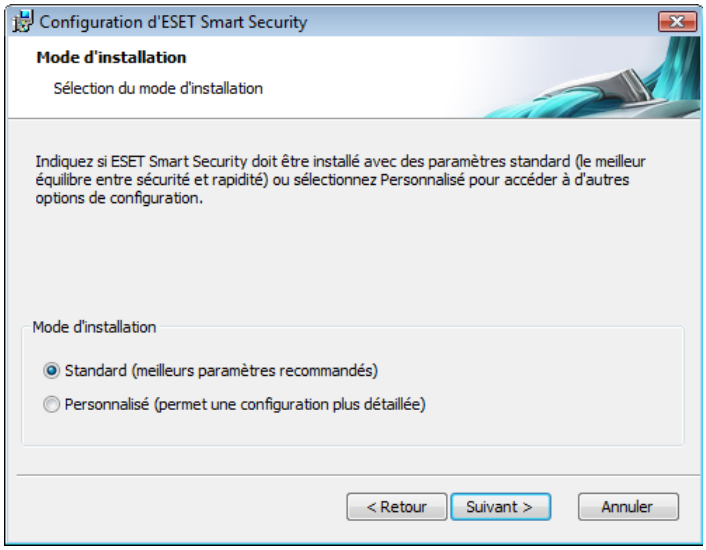
ESET Smart Security Business Edition :

Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32 bits/64 bits (x86/x64) 128 Mo de RAM de mémoire système 130 Mo d'espace disponible Super VGA (800 × 600)
Windows 7, Vista, Windows Server 2008	1 GHz 32 bits/64 bits (x86/x64) 512 Mo de RAM de mémoire système 130 Mo d'espace disponible Super VGA (800 × 600)

2. Installation

Après l'achat, le programme d'installation d'ESET Smart Security peut être téléchargé à partir du site web d'ESET. Il se présente sous la forme d'un module ess_nt**_***.msi (ESET Smart Security) ou essbe_nt**_***.msi (ESET Smart Security Business Edition). Lancez le programme d'installation ; l'Assistant Installation vous guidera dans les opérations de configuration de base. Deux types d'installation sont disponibles, avec différents niveaux de détails de configuration :

1. Installation typique
2. Installation personnalisée



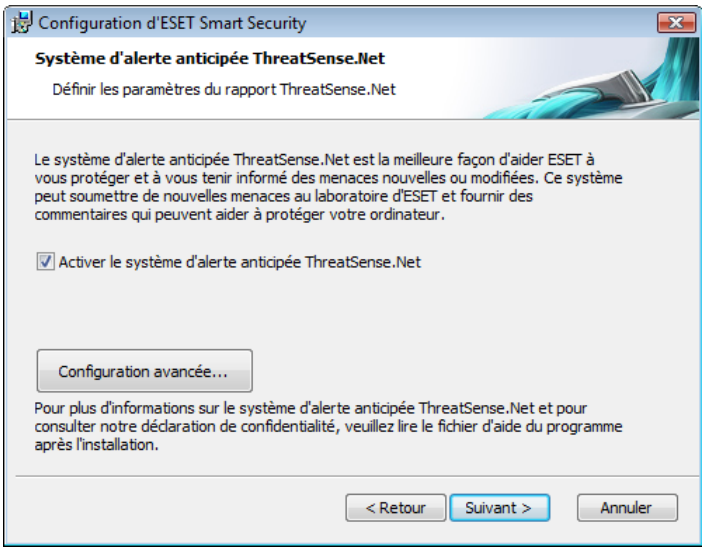
2.1 Installation typique

Une installation typique est recommandée aux utilisateurs qui souhaitent installer ESET Smart Security avec ses paramètres par défaut. Les paramètres par défaut du programme fournissent le niveau maximal de protection, une configuration appréciée par les utilisateurs qui ne veulent pas entrer dans le paramétrage détaillé.

La première étape (très importante) est la saisie d'un nom d'utilisateur et d'un mot de passe pour la mise à jour automatique du programme. Cette mise à jour joue un rôle important dans le maintien d'une protection constante du système.

Entrez dans les champs correspondants, votre **Nom d'utilisateur** et **Mot de passe**, c.-à-d. les données d'authentification reçues après l'achat ou l'enregistrement du produit. Si vos nom d'utilisateur et mot de passe ne sont pas disponibles, sélectionnez l'option **Définir les paramètres de mise à jour ultérieurement**. Les données d'authentification peuvent être introduites plus tard, directement à partir du programme.

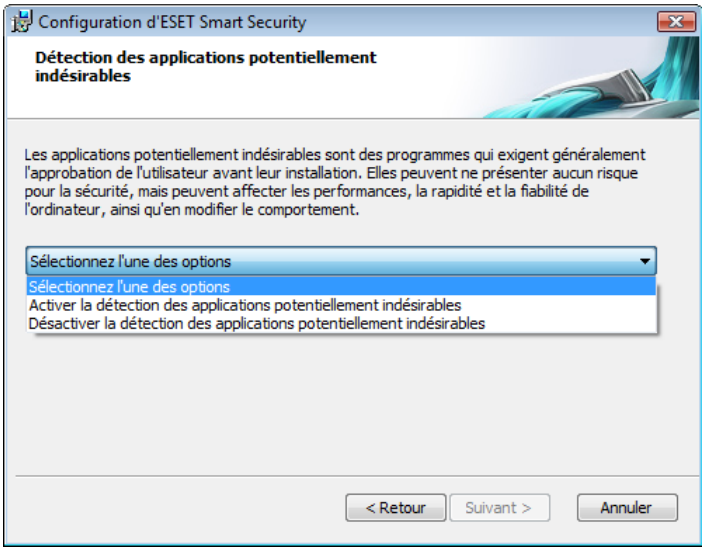
L'étape suivante de l'installation est la configuration du système d'avertissement anticipé ThreatSense.Net. Le système d'alerte anticipée ThreatSense.Net contribue à garantir qu'ESET est immédiatement et continuellement informé des nouvelles infiltrations dans le but de protéger ses clients. Le système permet la soumission de nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées puis ajoutées à la base de signatures de virus.



Par défaut, la case à cocher **Activer le système d'alerte anticipé ThreatSense.Net** est sélectionnée, activant cette fonction. Cliquez sur **Configuration avancée...** pour modifier les paramètres détaillés de soumission de fichiers suspects.

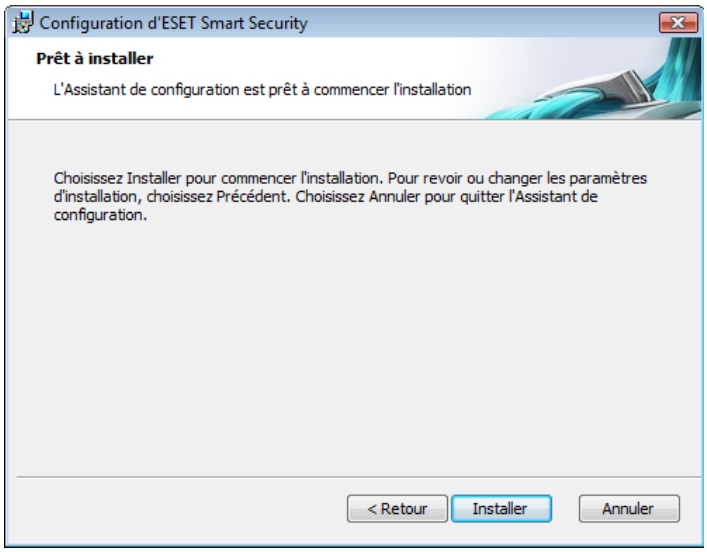
L'étape suivante de l'installation est la configuration de la **Détection des applications potentiellement indésirables**. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent d'une certaine manière affecter le comportement du système d'exploitation.

Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement.



Activez l'option **Activer la détection d'applications potentiellement indésirables** pour permettre à ESET Smart Security de détecter ce type de menace (recommandé).

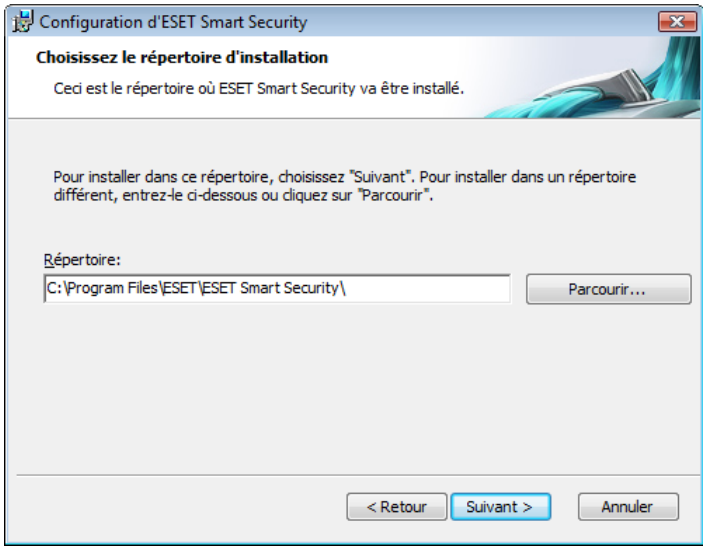
La dernière étape de l'installation typique est la confirmation de l'installation en cliquant sur le bouton **Installer**.



2.2 Installation personnalisée

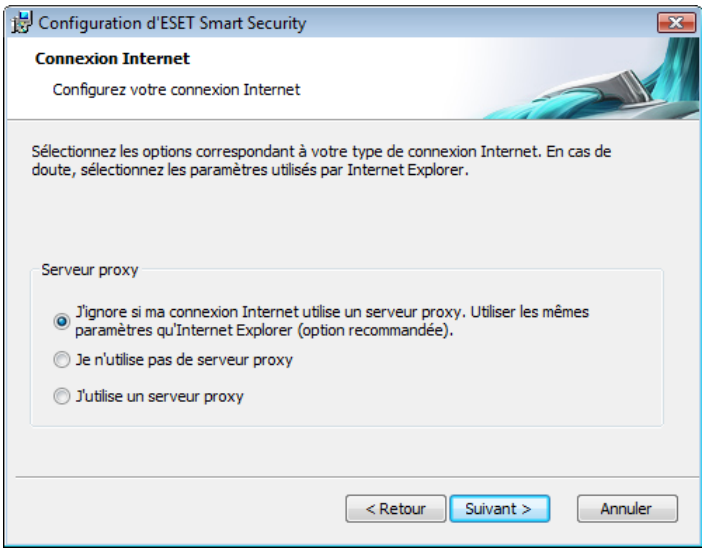
L'installation **Personnalisée** est destinée à des utilisateurs qui ont une certaine expérience de l'optimisation de programmes, et qui veulent modifier les paramètres avancés pendant l'installation.

La première étape est le choix de l'emplacement du dossier d'installation. Par défaut, le programme s'installe dans C:\Program Files\ESET\ESET Smart Security\. Cliquez sur **Parcourir...** pour changer d'emplacement (déconseillé).

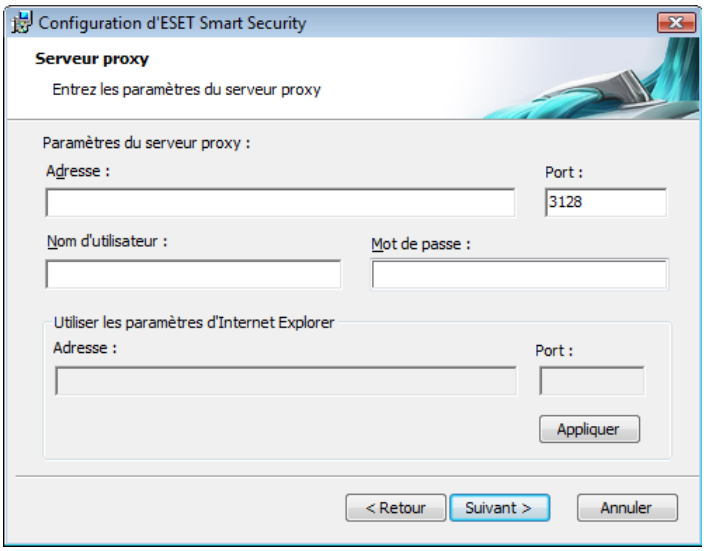


Ensuite, **entrez votre nom d'utilisateur et votre mot de passe**. Cette étape est la même que dans l'Installation typique (voir page 5).

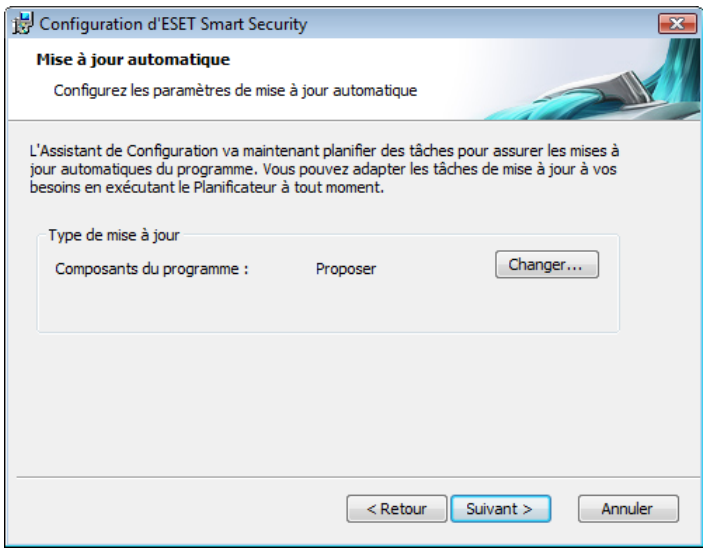
Après la saisie de votre nom d'utilisateur et de votre mot de passe, cliquez sur **Suivant** pour **Configurer votre connexion Internet**.



Si vous utilisez un serveur proxy, il doit être correctement configuré pour que les mises à jour des signatures de virus fonctionnent correctement. Si vous n'êtes pas sûr d'utiliser un serveur proxy pour la connexion à Internet, gardez le réglage par défaut **Je ne sais pas si ma connexion Internet utilise un serveur proxy. Utilisez les mêmes paramètres qu'Internet Explorer** , puis cliquez sur **Suivant**. Si vous n'utilisez pas de serveur proxy, sélectionnez l'option correspondante.

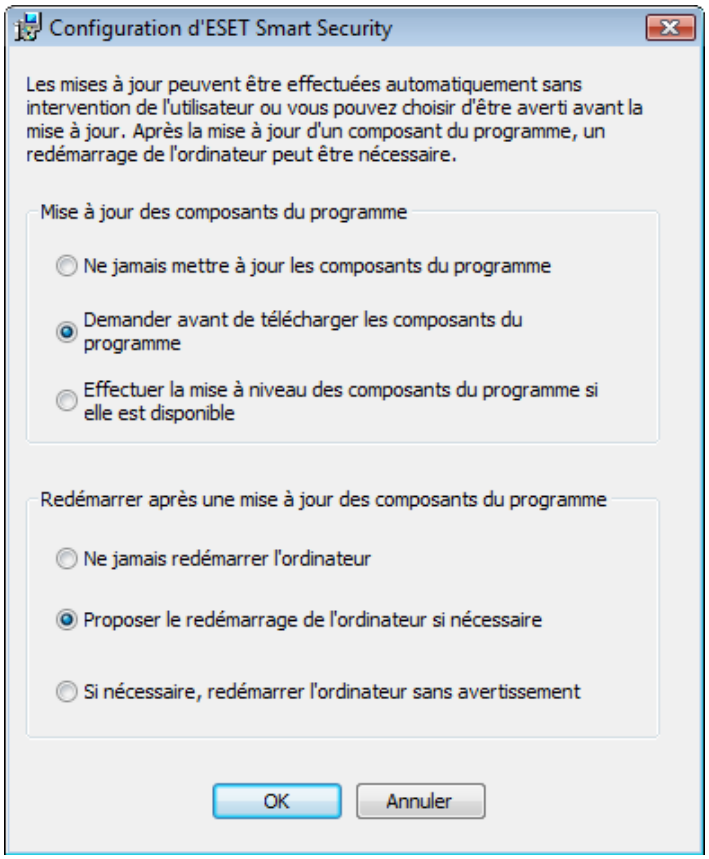


Pour configurer vos paramètres de serveur proxy, sélectionnez **J'utilise un serveur proxy** et cliquez sur **Suivant**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse.** Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, un nom d'utilisateur et un mot de passe valides y donnant accès doivent être entrés. Les paramètres du serveur proxy peuvent être copiés depuis Internet Explorer. Pour ce faire, cliquez sur le bouton **Appliquer**, puis confirmez la sélection.



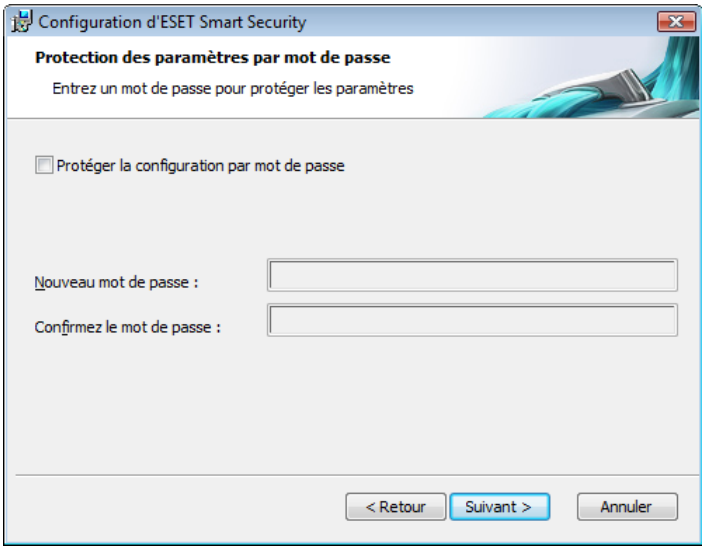
Cliquez sur **Suivant** pour continuer vers la fenêtre **Configurer les paramètres de mise à jour automatique** . Cette étape permet de spécifier la façon dont seront traitées les mises à jour automatiques des composants du programme sur votre système. Cliquez sur **Changer** pour accéder aux paramètres avancés.

Si vous ne voulez pas que les composants du programme soient mis à jour, sélectionnez **Ne jamais mettre à jour les composants du programme**. L'option **Demander avant de télécharger les composants de programme** affiche une fenêtre de confirmation pour télécharger les composants du programme. Pour activer la mise à jour automatique des composants du programme sans confirmation, sélectionnez l'option **Effectuer la mise à niveau des composants du programme si elle est disponible**.



REMARQUE : Le redémarrage du système est généralement nécessaire après la mise à jour des composants du programme. L'option recommandée est : **Si nécessaire, redémarrer l'ordinateur sans avertissement**.

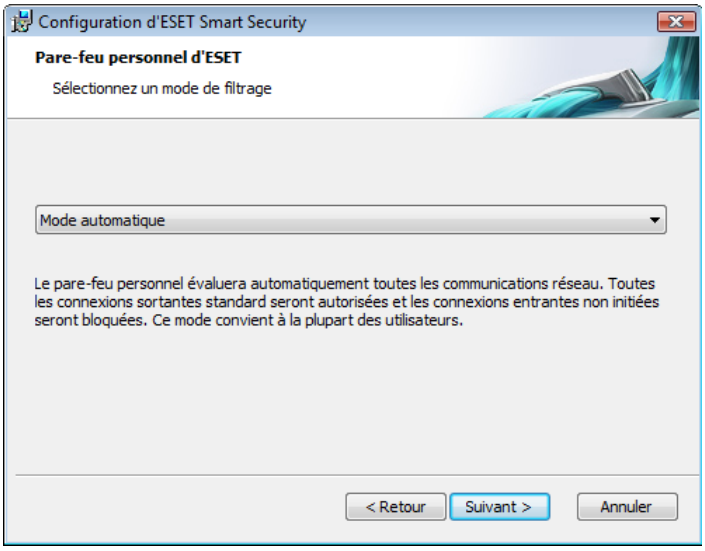
L'étape suivante de l'installation est la saisie d'un mot de passe pour protéger les paramètres. Choisissez un mot de passe pour protéger le programme. Tapez de nouveau le mot de passe pour le confirmer.



Les étapes **Configuration du système d'alerte anticipé ThreatSense.Net** et **Détection des applications potentiellement indésirables** sont les mêmes que dans l'Installation typique et ne sont pas reprises ici (voir page 5).

La dernière étape de l'installation personnalisée est le choix du mode de filtrage du pare-feu personnel ESET. Cinq modes sont disponibles :

- Automatique
- Mode automatique avec exceptions (règles définies par l'utilisateur)
- Interactif
- Basé sur des règles
- Apprentissage



Le mode **Automatique** est recommandé pour la majorité des utilisateurs. Toutes les connexions standard sortantes sont autorisées (analysées automatiquement selon les critères prédéfinis) et les connexions entrantes non sollicitées sont automatiquement bloquées.

Mode automatique avec exceptions (règles définies par l'utilisateur). En plus du mode automatique, il permet d'ajouter des règles personnalisées.

Le mode **Interactif** ne convient qu'aux utilisateurs chevronnés. Les communications sont gérées par des règles définies par l'utilisateur. En l'absence de règle définie pour une communication donnée, le programme demande à l'utilisateur d'autoriser ou de refuser la communication.

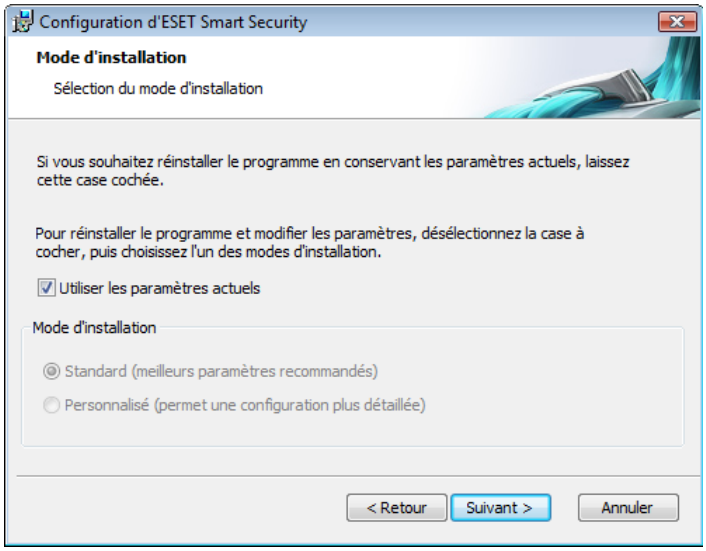
Le mode **Basé sur des règles** évalue les communications sur la base des règles prédéfinies créées par l'administrateur. En l'absence de règle disponible, la connexion est automatiquement bloquée et l'utilisateur ne voit aucun message d'avertissement. Nous recommandons de ne sélectionner le mode basé sur des règles que si vous comptez, en tant qu'administrateur, configurer les communications réseau.

Mode d'apprentissage : crée et enregistre automatiquement les règles et convient pour la configuration initiale du pare-feu personnel. Aucune intervention de l'utilisateur n'est requise, car ESET Smart Security enregistre les règles conformément aux paramètres prédéfinis. Le mode d'apprentissage n'étant pas sécurisé, il est recommandé de ne l'utiliser que jusqu'à ce que toutes les règles aient été créées pour les communications requises.

La dernière étape affiche une fenêtre demandant votre accord pour l'installation.

2.3 Utilisation des paramètres d'origine

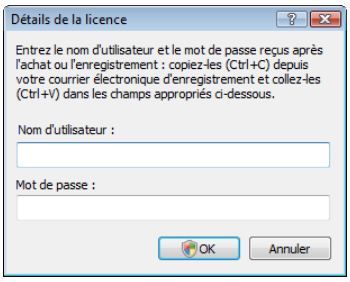
Si vous réinstallez ESET Smart Security, l'option **Utiliser les paramètres actuels** s'affiche. Sélectionnez cette option pour transférer les paramètres de configuration de l'installation d'origine vers la nouvelle installation.



2.4 Entrée d'un nom d'utilisateur et d'un mot de passe

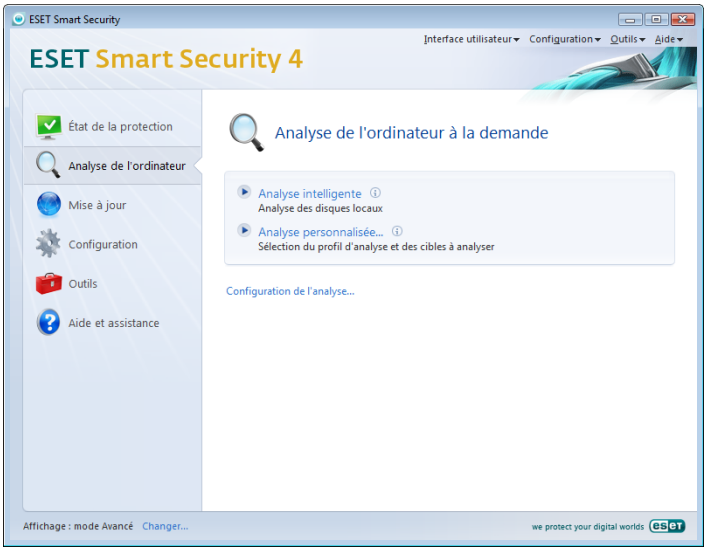
Le programme doit être mis à jour automatiquement pour assurer un fonctionnement optimal. Ce n'est possible que si le nom d'utilisateur et le mot de passe corrects sont entrés dans la configuration des mises à jour.

Si vous n'avez pas entré votre nom d'utilisateur et votre mot de passe lors de l'installation, vous pouvez le faire maintenant. Dans la fenêtre principale du programme, cliquez sur **Mettre à jour**, puis sur **Nom d'utilisateur et mot de passe...** Entrez les données reçues avec la licence du produit dans la fenêtre **Détails de la licence**.



2.5 Analyse d'ordinateur à la demande

Après l'installation d'ESET Smart Security, il y a lieu de procéder à une analyse de l'ordinateur à la recherche de codes malveillants. Pour lancer rapidement une analyse, sélectionnez **Analyse de l'ordinateur** dans le menu principal, puis sélectionnez **Analyse standard** dans la fenêtre principale du programme. Pour plus d'informations sur les options d'analyse de l'ordinateur, consultez le chapitre « Analyse de l'ordinateur ».



3. Guide du débutant

Ce chapitre donne un premier aperçu d'ESET Smart Security et de ses paramètres de base.

3.1 Présentation de l'interface utilisateur : les modes

La fenêtre principale d'ESET Smart Security est divisée en deux principales sections. La colonne de gauche donne accès à un -menu principal convivial. La fenêtre principale du programme, à droite, sert essentiellement à afficher des informations sur l'option sélectionnée dans le menu principal.

Voici une description des boutons disponibles dans le menu principal :

État de la protection : fournit, sous une -forme conviviale, des informations concernant l'état de la protection d'ESET Smart Security. Si le mode avancé est activé, l'état de tous les modules de protection est affiché. Cliquez sur un module pour voir son état actuel.

Analyse de l'ordinateur : cette option permet de configurer et de lancer l'Analyse de l'ordinateur à la demande.

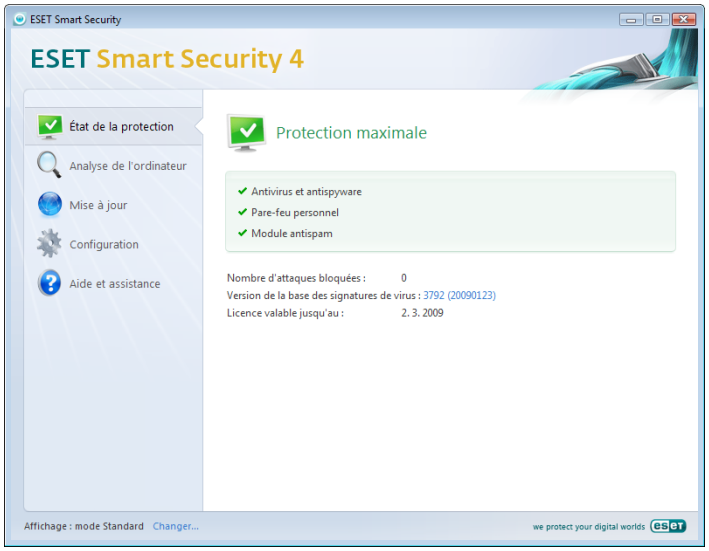
Mise à jour : sélectionnez cette option pour accéder au module de mise à jour qui gère les mises à jour de la base de signatures de virus.

Configuration : cette option permet d'ajuster le niveau de sécurité de votre ordinateur. Si le mode Avancé est activé, les sous-menus Protection antivirus et anti-logiciels espions, Pare-feu personnel et Blocage du courrier indésirable apparaissent.

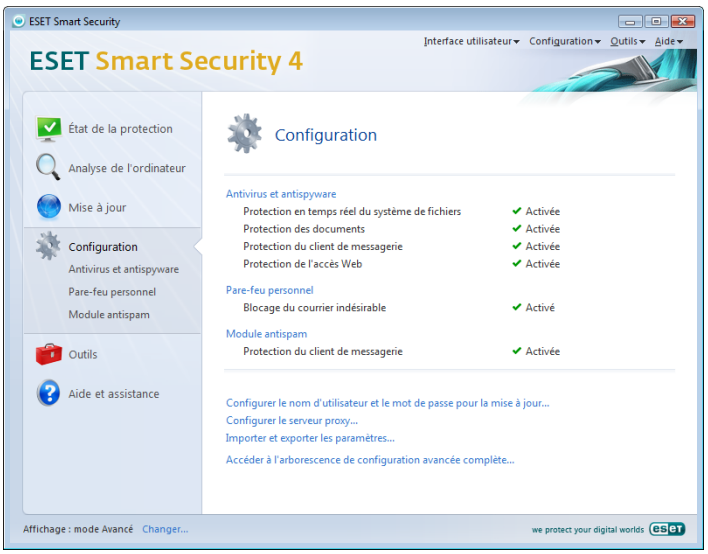
Outils : cette option est disponible uniquement en mode avancé. Elle permet d'accéder aux fonctions Fichiers journaux, Quarantaine et Planificateur.

Aide et assistance : sélectionnez cette option pour accéder aux fichiers d'aide, à la base de connaissances ESET, au site Web d'ESET et à une demande d'assistance du service client.

L'interface utilisateur d'ESET Smart Security permet également de basculer entre les modes standard et avancé. Pour basculer entre les modes, utilisez le lien **Affichage** situé dans l'angle inférieur gauche de la fenêtre principale d'ESET Smart Security. Cliquez sur ce bouton pour sélectionner le mode d'affichage souhaité.



Le mode Standard donne accès aux fonctionnalités nécessaires aux opérations ordinaires. Il n'affiche aucune option avancée.

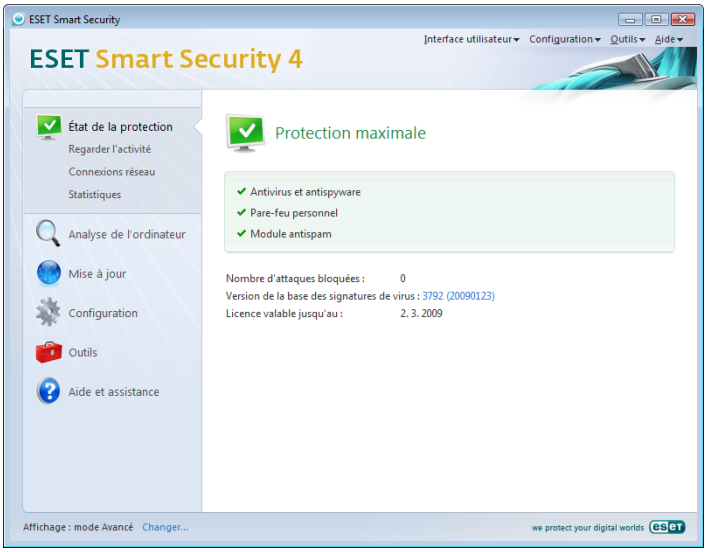


Le passage au mode avancé ajoute l'option **Outils** dans le menu principal. L'option Outils permet d'accéder au Planificateur et à la Quarantaine et de consulter les fichiers journaux d'ESET Smart Security.

REMARQUE : Toutes les instructions qui suivent dans ce guide seront effectuées en mode avancé.

3.1.1 Contrôle du fonctionnement du système

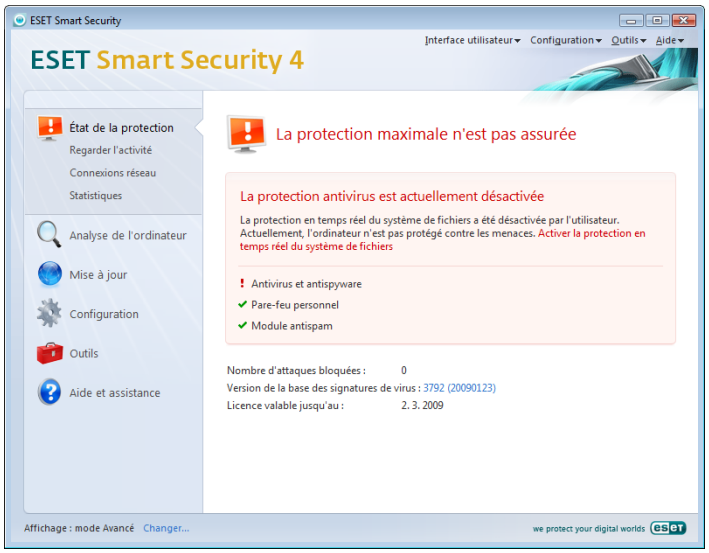
Pour afficher l'**État de la protection**, cliquez sur cette option en haut du menu principal. Un résumé de l'état de fonctionnement d'ESET Smart Security s'affiche dans la partie droite de la fenêtre, ainsi qu'un sous-menu avec trois options : **Antivirus et anti-logiciels espions**, **Pare-feu personnel** et **Blocage du courrier indésirable**. Sélectionnez une de ces options pour afficher les informations détaillées sur le module de protection correspondant.



Une marque verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange et des informations supplémentaires sur module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état des différents modules, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.

3.1.2 Que faire lorsque le programme ne fonctionne pas correctement

Si ESET détecte un problème dans l'un des ses modules de protection, il le signale dans la fenêtre **État de la protection**. Une solution potentielle au problème y est également proposée.

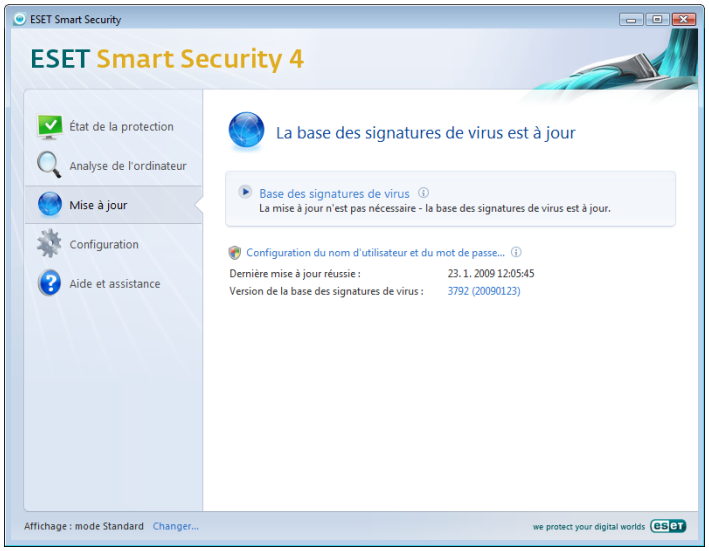


S'il est impossible de résoudre le problème au moyen de la liste des problèmes connus et résolus, cliquez sur **Aide et assistance** pour accéder aux fichiers d'aide ou effectuer une recherche dans la base de connaissances. Si vous ne trouvez toujours pas de solution, vous pouvez soumettre une demande de support à l'Assistance à la clientèle d'ESET. Sur la base de ce feedback, nos spécialistes peuvent rapidement répondre à vos questions et vous conseiller efficacement une solution.

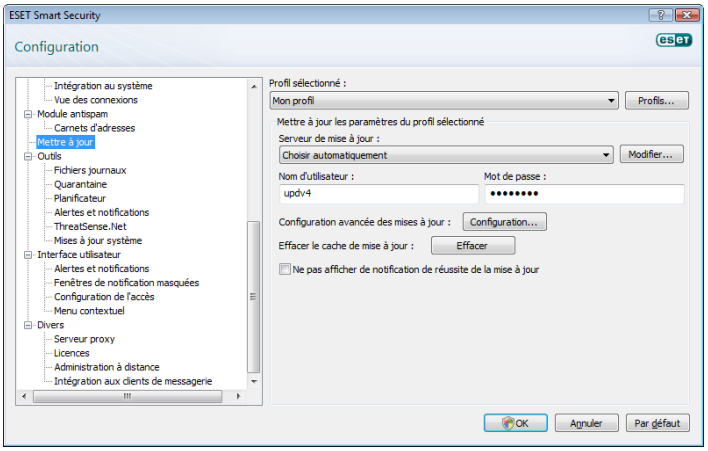
3.2 Configuration des mises à jour

La mise à jour de la base de signatures de virus et celle des composants du programme sont des parties importantes pour assurer une protection totale contre les attaques des codes malveillants. Soyez donc particulièrement attentif à leur configuration et à leur fonctionnement. Dans le menu principal, sélectionnez **Mettre à jour**, puis cliquez sur **Mettre à jour la base des signatures de virus** dans la fenêtre principale du programme pour vérifier instantanément la disponibilité d'une mise à jour plus récente de la base de données. **Nom d'utilisateur et mot de passe...** affiche une boîte de dialogue permettant d'entrer le nom d'utilisateur et le mot de passe reçus à l'achat du logiciel.

Si le nom d'utilisateur et le mot de passe ont été entrés lors de l'installation d'ESET Smart Security, vous ne serez pas invité à les réintroduire à ce stade.



La fenêtre **Configuration avancée** (pour y accéder, appuyez sur F5) contient d'autres options avancées pour la mises à jour. L'option du menu déroulant **Serveur de mise à jour** doit être configurée sur **Choisir automatiquement**. Pour configurer des options avancées de mise à jour telles que le mode de mise à jour, l'accès au serveur proxy, l'accès aux mises à jour sur un serveur local et la création de copies de signatures de virus (ESET Smart Security Business Edition), cliquez sur le bouton **Configuration...**.



3.3 Configuration de zone de confiance

La configuration d'une zone fiable est une étape importante dans la protection de votre ordinateur dans un environnement de réseau. Vous pouvez autoriser d'autres utilisateurs à accéder à votre ordinateur en configurant la zone Fiable de manière à autoriser le partage. Cliquez sur **Configuration > Pare-feu personnel > Modifier le mode de protection de votre ordinateur sur le réseau...** Une fenêtre s'affiche, vous permettant de configurer les paramètres de votre mode de protection de l'ordinateur dans le réseau ou la zone actuelle.

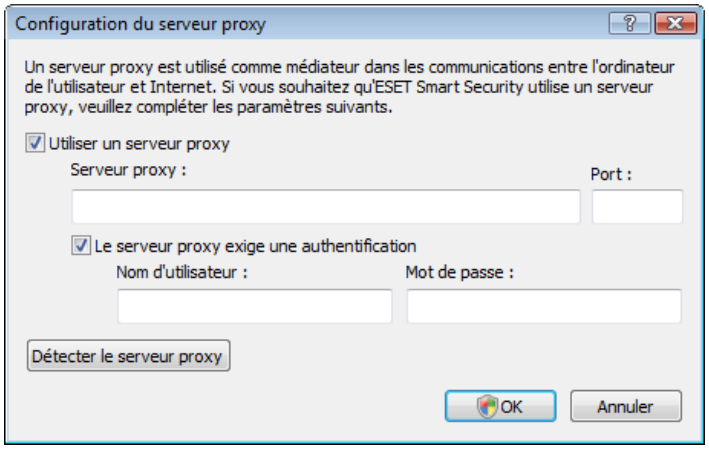
La détection de zones fiables s'effectue après l'installation d'ESET Smart Security et chaque fois que l'ordinateur est connecté à un nouveau réseau. Dans la plupart des cas, il n'est donc pas nécessaire de définir la zone Fiable. Par défaut, une boîte de dialogue s'ouvre à la détection d'une nouvelle zone afin de permettre d'en définir le niveau de protection.

Avertissement ! Une configuration incorrecte de la zone fiable peut poser un risque pour la sécurité de votre ordinateur.

REMARQUE : Par défaut, les postes de travail d'une zone Fiable ont l'autorisation d'accès aux fichiers et imprimantes partagés, la communication RPC entrante est activée et le partage de bureau à distance est également disponible.

3.4 Configuration du serveur proxy

Si vous travaillez sur un système avec ESET Smart Security et utilisez un serveur proxy pour la connexion à Internet, ce dernier doit être spécifié dans la Configuration avancée (F5). Pour accéder à la fenêtre de configuration **Serveur proxy**, dans l'arborescence Configuration avancée, cliquez sur **Divers > Serveur proxy**. Sélectionnez la case à cocher **Utiliser un serveur proxy** et entrez l'adresse IP et le port du serveur proxy, ainsi que des données d'authentification.



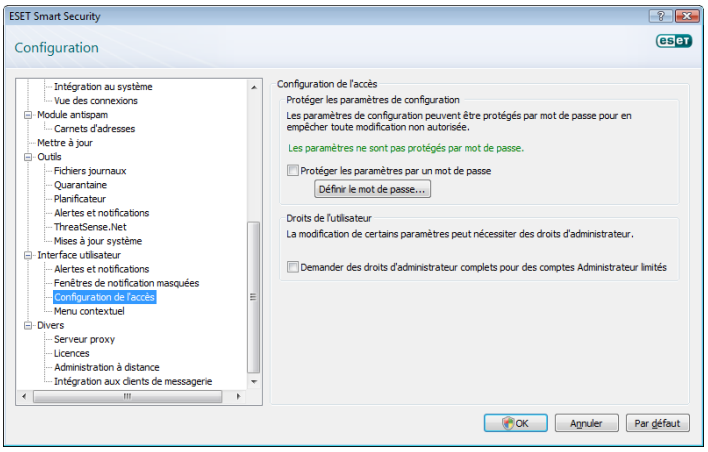
Si ces informations ne sont pas disponibles, vous pouvez tenter une détection automatique des paramètres de serveur proxy pour ESET Smart Security en cliquant sur le bouton **Détecter le serveur proxy**.

REMARQUE : Les options du serveur proxy peuvent varier selon les profils de mise à jour. Si c'est le cas, configurez le serveur proxy dans la configuration avancée des mises à jour.

3.5 Protection des paramètres

Les paramètres ESET Smart Security peuvent être très importants vis-à-vis de la stratégie de sécurité de votre organisation. Des modifications non autorisées pourraient mettre en danger la stabilité et la protection de votre système. Pour protéger par mot de passe les paramètres de configuration, partez du menu principal, puis cliquez sur **Configuration > Accéder à l'arborescence de la configuration avancée complète... > Interface utilisateur > Protection des paramètres** et cliquez sur le bouton **Entrer le mot de passe...**.

Entrez un mot de passe, confirmez-le en le tapant de nouveau, puis cliquez sur **OK**. Ce mot de passe sera requis pour toute modification future des paramètres ESET Smart Security.



4. Utilisation d'ESET Smart Security

4.1 Protection antivirus et anti-logiciels espions

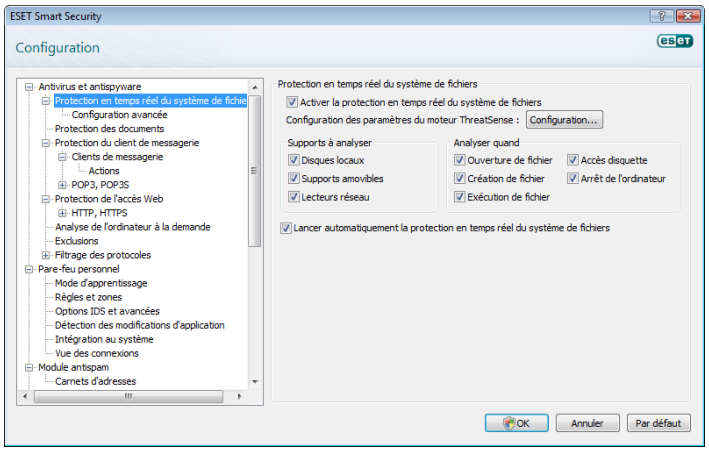
La protection antivirus vous prémunit des attaques contre le système en contrôlant les échanges de fichiers et de courrier et les communications Internet. Si une menace comportant du code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant dans un premier temps, puis en nettoyant, en supprimant ou en mettant en quarantaine l'objet infecté.

4.1.1 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Elle analyse tous les fichiers à la recherche de code malveillant lors de leur ouverture, de leur création ou de leur exécution sur l'ordinateur. La protection en temps réel du système de fichiers est lancée au démarrage du système.

4.1.1.1 Configuration du contrôle

La protection en temps réel du système de fichiers vérifie touts les types de supports et le contrôle est déclenché par différents événements. Le contrôle utilise les méthodes de détection de la technologie ThreatSense (décrites sous Configuration des paramètres du moteur ThreatSense). Le contrôle peut être différent pour les fichiers nouveaux et les fichiers existants. Pour les fichiers nouvellement créés, il est possible d'appliquer un niveau de contrôle plus approfondi.



4.1.1.1.1 Supports à analyser

Par défaut, tous les types de supports sont analysés à la recherche de menaces potentielles.

Disques locaux : Contrôle tous les disques durs du système

Supports amovibles : disquettes, périphériques de stockage USB, etc.

Lecteurs réseau : analyse toutes les unités mappées

il est recommandé de conserver les paramètres par défaut et de ne les modifier que dans des cas spécifiques, comme lorsque l'analyse de certains supports ralentit sensiblement les transferts de données.

4.1.1.1.2 Analyser quand (Analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés lorsqu'ils sont ouverts, exécutés ou créés. Il est recommandé de conserver les paramètres par défaut, qui offrent le niveau maximal de protection en temps réel pour votre ordinateur.

L'option **Accès disquette** contrôle le secteur d'amorçage des disquettes lors de l'accès au lecteur. L'option **Arrêt de l'ordinateur** contrôle les secteurs d'amorçage du disque dur lors de l'arrêt de l'ordinateur. Bien que les virus d'amorçage soient rares de nos jours, il est recommandé de laisser ces options activées, car le risque existe toujours d'une infection par un virus d'amorçage provenant d'autres sources.

4.1.1.1.3 Autres paramètres ThreatSense pour les fichiers nouveaux et modifiés

La probabilité d'infection des nouveaux fichiers est comparativement supérieure à celle des fichiers existants. C'est pourquoi le programme vérifie ces fichiers avec des paramètres d'analyse supplémentaires. Outre les méthodes d'analyse habituelles basées sur les signatures, l'heuristique avancée utilisée améliore sensiblement les taux de détection. En plus des fichiers nouvellement créés, l'analyse inclut les fichiers auto-extractibles (SFX) et les fichiers exécutables compressés par un compresseur d'exécutables (interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et contrôlées indépendamment de leur taille réelle. Désactivez l'option ***Paramètres d'analyse d'archive par défaut*** pour modifier les paramètres d'analyse d'archive.

4.1.1.1.4 Configuration avancée

Pour exercer un impact minimal sur le système lorsque la protection en temps réel est activée, les fichiers qui ont déjà été analysés ne le sont plus tant qu'il ne sont pas modifiés. Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus. Ce comportement se configure à l'aide de l'option **Analyse optimalisée**. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque fois qu'on y accède.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse ininterrompue. Dans des cas particuliers (p. ex. en cas de conflit avec un autre analyseur en temps réel), il est possible d'arrêter la protection en temps réel en désactivant l'option **Lancement automatique de la protection en temps réel du système de fichiers**.

Par défaut, l'heuristique avancée n'est pas utilisée lors de l'exécution de fichiers. Toutefois, dans certains cas, il peut être utile d'activer cette option (en sélectionnant **Heuristique avancée à l'exécution du fichier**). Notez que l'heuristique avancée peut ralentir l'exécution de certains programmes en raison de la charge système accrue.

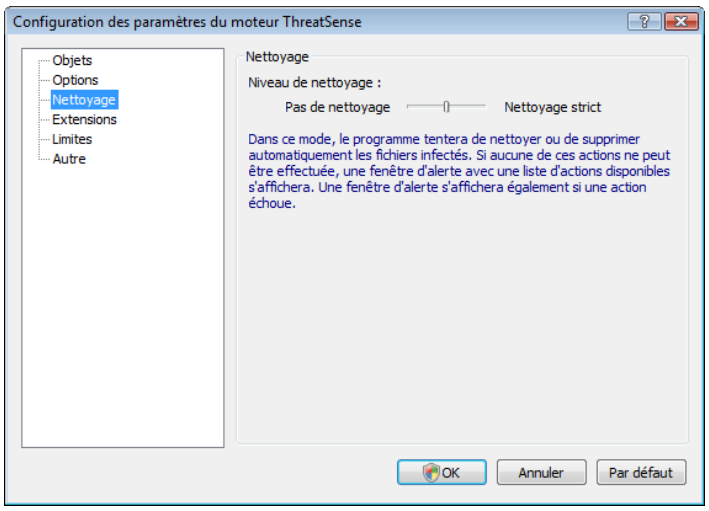
4.1.1.2 Niveaux de nettoyage

La protection en temps réel offre trois niveaux de nettoyage (pour y accéder, cliquez sur le bouton **Configuration...** dans la section **Protection en temps réel du système de fichiers**, puis cliquez sur la branche **Nettoyage**).

- Le premier niveau affiche une fenêtre d'avertissement qui propose des options pour chaque infiltration détectée. L'utilisateur doit choisir une action individuelle pour chaque infiltration. Ce niveau est conçu pour les utilisateurs chevronnés qui savent que faire en cas d'infiltration.

- Le niveau par défaut choisit et exécute automatiquement une action prédéfinie (selon le type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par un message d'information affiché dans l'angle inférieur droit de l'écran. Cependant, aucune action automatique n'est exécutée si l'infiltration se trouve dans une archive contenant aussi des fichiers sains ou s'il n'y a pas d'action prédéfinie pour les objets infectés.

- Le troisième niveau est le plus « agressif » : tous les fichiers infectés sont nettoyés. Ce niveau pouvant éventuellement entraîner la perte de fichiers valides, il n'est recommandé que dans des situations spécifiques.



4.1.1.3 Quand faut-il modifier la configuration la protection en temps réel

La protection en temps réel est le composant le plus essentiel de la sécurisation du système. Il faut donc être attentif lors de la modification de ces paramètres. Il est recommandé de ne changer ces paramètres que dans des cas spécifiques. Cela se justifie, par exemple, en présence d'un conflit avec une autre application ou l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation d'ESET Smart Security, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur le bouton **Par défaut** situé en bas à droite de la fenêtre **Protection en temps réel du système de fichiers** (**Configuration avancée > Protection contre les virus et les logiciels espions > Protection en temps réel du système de fichiers**).

4.1.1.4 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et détecte les virus, utilisez un fichier de test d'eicar.com. Ce fichier de test est un fichier spécial inoffensif détectable par tous les programmes antivirus. Le fichier a été créé par la société EICAR (European Institute for Computer Antivirus Research) pour tester la fonctionnalité des programmes antivirus. Le fichier eicar.com est téléchargeable depuis http://www.eicar.org/download/eicar.com.

REMARQUE : Avant d'effectuer une vérification de la protection en temps réel, il faut désactiver le pare-feu. Si le pare-feu est activé, il détectera le fichier et empêchera le téléchargement des fichiers de test.

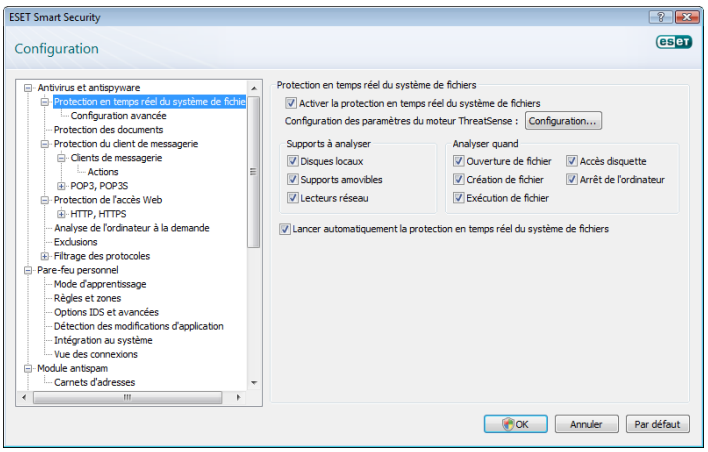
4.1.1.5 Que faire si la protection en temps réel ne fonctionne pas

Dans le chapitre suivant, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée

Si la protection en temps réel a été désactivée par mégarde par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, accédez à **Configuration > Antivirus et anti-logiciels espions**, puis cliquez sur **Activer** dans la section **Protection en temps réel du système de fichiers** de la fenêtre principale du programme.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement dû au fait que l'option **Lancement automatique de la protection en temps réel du système de fichiers** est désactivée. Pour activer cette option, accédez à **Configuration avancée** (F5), puis cliquez sur **Protection en temps réel du système de fichiers** dans l'arborescence Configuration avancée. Dans la section **Configuration avancée** dans le bas de la fenêtre, assurez-vous que la case à cocher **Lancement automatique de la protection en temps réel du système de fichiers** est activée.



Si la protection en temps réel ne détecte et ne nettoie pas les infiltrations

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux boucliers de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si l'option **Lancement automatique de la protection en temps réel du système de fichiers** est activée), le problème peut provenir de conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes du service clientèle ESET.

4.1.2 Le système de prévention d'intrusiosns HIPS

Le système de prévention d'intrusiosns HIPS protège votre système des malwares ou de toute autre activité non-désirée visant à réduire la sécurité de votre ordinateur. Il utilise une détection comportementale avancée couplée aux capacités de détection d'un filtrage réseau pour surveiller les processus en cours, les fichiers et les clefs de registre pour bloquer et prévenir toute tentative d'attaque.

4.1.3 Protection du client de messagerie

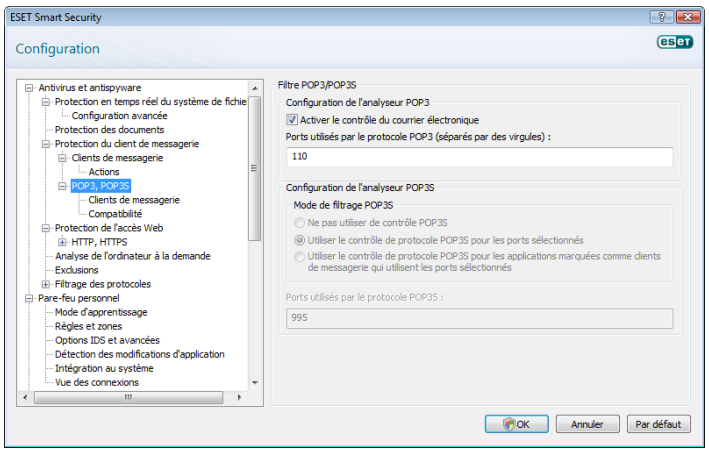
La protection du courrier offre le contrôle de la communication par courrier électronique effectuée via le protocole POP3. Utilisant l'extension pour Microsoft Outlook, ESET Smart Security assure le contrôle de toutes les communications impliquant le client de messagerie (POP3, MAPI, IMAP, HTTP). Lors de l'examen des messages entrants, le programme utilise toutes les méthodes d'analyse avancées offertes par le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants a lieu avant même la comparaison avec la base des signatures de virus. L'analyse des communications via le protocole POP3 est indépendante du client de messagerie utilisé.

4.1.3.1 Contrôle POP3

Le protocole POP3 est le protocole le plus répandu pour la réception de messages dans un client de messagerie. ESET Smart Security assure la protection de ce protocole quel que soit le client de messagerie utilisé.

Le module qui assure ce contrôle est automatiquement lancé au démarrage du système d'exploitation et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé ; le contrôle POP3 s'effectue automatiquement sans qu'il faille reconfigurer le client de messagerie. Par défaut, toute communication sur le port 110 est analysée, mais d'autres ports de communication peuvent être ajoutés si nécessaire. Les numéros de ports doivent être séparés par des virgules.

Les communications chiffrées ne sont pas contrôlées.



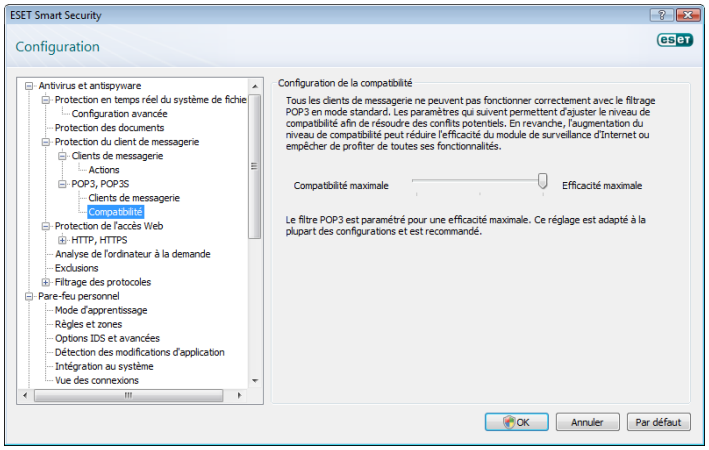
4.1.3.1.1 Compatibilité

Certains programmes de messagerie peuvent avoir des problèmes de filtrage POP3 (p. ex. si vous recevez des messages sur une connexion Internet lente, la vérification peut entraîner des dépassements de délai). Dans ce cas, essayez de modifiez la façon dont le contrôle est effectué. Une diminution du niveau de contrôle peut accélérer le processus de nettoyage. Pour modifier le niveau de contrôle du filtrage POP3, accédez à **Antivirus et anti-logiciels espions > Protection du courrier > POP3 > Compatibilité**.

Si vous activez l'option **Efficacité maximale**, les infiltrations sont supprimées des messages infectés et des informations concernant l'infiltration sont insérées au début de l'objet initial du message (les options **Supprimer** ou **Nettoyer** doivent être activées, ou le niveau de nettoyage **Strict** ou **Par défaut** doit être activé)

Le niveau **Compatibilité moyenne** modifie la façon dont les messages sont reçus. Les messages sont progressivement envoyés au client de messagerie ; une fois la dernière partie du message transférée, le message est analysé à la recherche d'infiltrations. Cependant, ce niveau de contrôle augmente le risque d'infection. Le niveau de nettoyage et la gestion des « étiquettes » (notes d'alerte ajoutées à l'objet et au corps des messages) sont identiques à ceux utilisés avec le paramètre d'efficacité maximale.

Avec la **Compatibilité maximale**, l'utilisateur est averti par l'affichage d'une fenêtre qui signale la réception d'un message infecté. Aucune information concernant les fichiers infectés n'est ajoutée à l'objet ni au corps des messages et les infiltrations ne sont pas automatiquement supprimées. Il incombe à l'utilisateur de supprimer les infiltrations à partir de son client de messagerie.

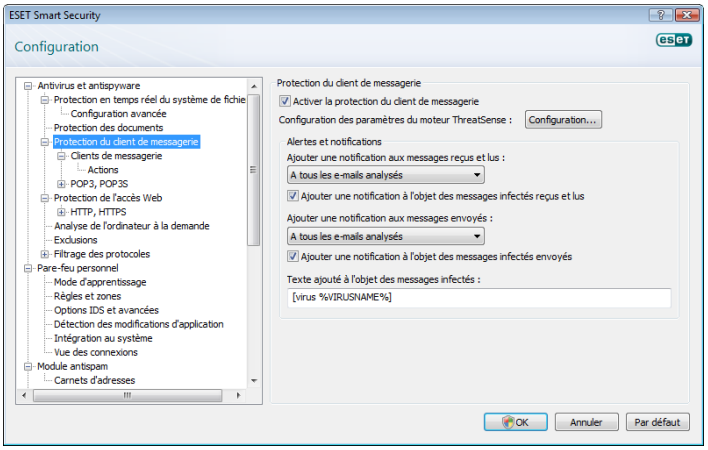


4.1.3.2 Intégration aux clients de messagerie

L'intégration d'ESET Smart Security aux clients de messagerie augmente le niveau de protection active contre le code malveillant dans les messages électroniques. Si votre client de messagerie est pris en charge, cette intégration peut être activée dans ESET Smart Security. Lorsque l'intégration est activée, la barre d'outils ESET Smart Security Antispam est insérée directement dans le client de messagerie, contribuant ainsi à une protection plus efficace du courrier. Les paramètres d'intégration sont accessibles dans **Configuration > Accéder à l'arborescence de la configuration avancée complète... > Divers > Intégration aux clients de messagerie**. Cette boîte de dialogue permet à l'utilisateur d'activer l'intégration aux clients de messagerie pris en charge. Les clients de messagerie actuellement pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird.

Activez l'option ***Désactiver la vérification au changement de contenu de la boîte aux lettres*** si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie. Une telle situation peut se présenter lors du téléchargement de messages à partir de Kerio Outlook Connector.

La protection du courrier s'active en sélectionnant la case correspondante dans **Configuration avancée (F5) > Antivirus et anti-logiciels espions > Protection du courrier**.



4.1.3.2.1 Ajout d'une étiquette au corps d'un courrier

Chaque message contrôlé par ESET Smart Security peut être marqué par l'ajout d'une mention (une « étiquette ») à l'objet ou au corps du message. Cette fonction augmente le niveau de crédibilité pour le destinataire et, en cas de détection d'une infiltration, fournit de précieuses informations sur le niveau de menace d'un message/expéditeur donné.

Les options de cette fonction sont accessibles dans **Configuration avancée > Antivirus et anti-logiciels espions > Protection du client de messagerie**. Le programme peut **Ajouter une notification aux messages reçus et lus**, ainsi qu'**Ajouter une notification aux messages envoyés**. L'utilisateur peut aussi décider si des notifications doivent être ajoutées à tous les messages, uniquement aux messages infectés ou à aucun message. ESET Smart Security permet aussi d'ajouter des notifications à l'objet initial des messages infectés. Pour ce faire, sélectionnez les options **Ajouter une note à l'objet des messages infectés reçus et lus** et **Ajouter une note à l'objet des messages infectés envoyés.**

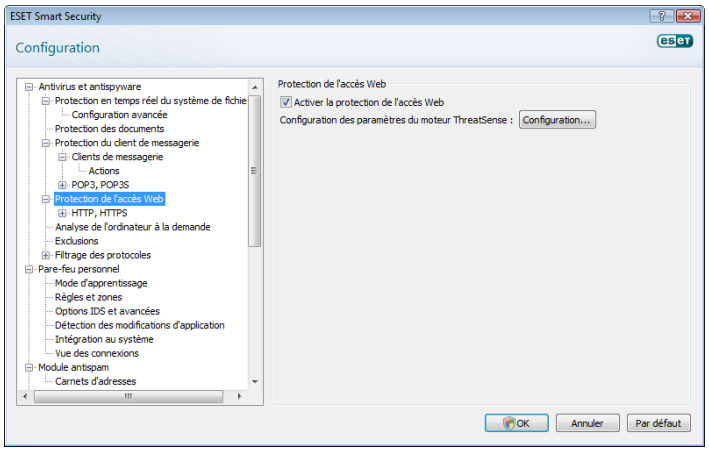
Le contenu de ces notes peut être modifié dans le champ Modèle et ajouté à l'objet des messages infectés. Les modifications en question permettent d'automatiser le filtrage des messages infectés, en permettant de définir un filtre (si votre client de messagerie le permet) qui place dans un dossier distinct les messages ayant un objet spécifique.

4.1.3.3 Suppression d'infiltrations

En cas de réception d'un message infecté, une fenêtre d'alerte s'affiche. Cette fenêtre indique le nom de l'expéditeur, son message et le nom de l'infiltration. Dans partie inférieure de la fenêtre, les options **Nettoyer**, **Supprimer** ou **Laisser** sont disponibles pour l'objet détecté. Dans la plupart des cas, nous recommandons de sélectionner **Nettoyer** ou **Supprimer**. Dans les situations particulières où vous souhaitez vraiment recevoir le fichier infecté, sélectionnez **Laisser**. Si le niveau **Nettoyage strict** est activé, une fenêtre d'information sans options s'affiche.

4.1.4 Protection de l'accès Web

La connexion Internet est une fonctionnalité standard dans un ordinateur personnel. Malheureusement, elle est devenue le principal moyen de transfert de codes malveillants. C'est pour cela qu'il est essentiel d'examiner attentivement de la protection de l'accès Web. Il est fortement recommandé de sélectionner l'option **Activer la protection de l'accès Web**. Cette option se trouve dans **Configuration avancée (F5) > Antivirus et anti-logiciels espions > Protection de l'accès Web**.



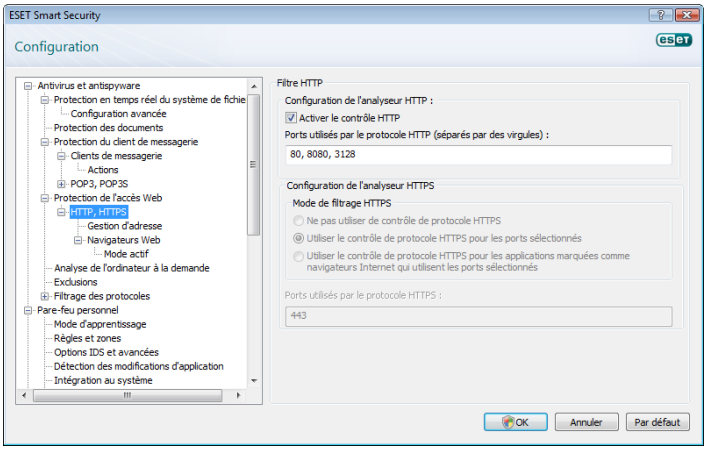
4.1.4.1 HTTP, HTTPs

La protection de l'accès Web opère par surveillance des communication entre les navigateurs Internet et des serveurs distants, conformément aux règles des protocoles HTTP et HTTPs. Par défaut, ESET Smart Security est configuré pour utiliser les normes de la plupart des navigateurs Internet. Toutefois, vous pouvez modifier les options de configuration de l'analyseur HTTP dans la section Protection de l'accès Web > HTTP, HTTPs. Dans la fenêtre principale du filtre HTTP, vous pouvez activer ou désactiver l'option **Activer le contrôle HTTP**. Vous pouvez également définir les numéros de port utilisés pour la communication HTTP. Par défaut, les numéros de ports 80, 8080 et 3128 sont prédéfinis. Le contrôle HTTPs peut être effectué dans les modes suivants :

Ne pas utiliser de contrôle de protocole HTTPS
Les communications chiffrées ne sont pas vérifiées.

Utiliser le contrôle de protocole HTTPS pour les ports sélectionnés
Le contrôle HTTPs n'a lieu que pour les ports définis dans Ports utilisés par le protocole HTTP.

Utiliser le contrôle de protocole HTTPS pour les applications marquées comme navigateurs Internet qui utilisent les ports sélectionnés
Le contrôle n'a lieu que pour les applications spécifiées dans la section navigateurs et qui utilisent les ports définis dans ***Ports utilisés par le protocole HTTP***.

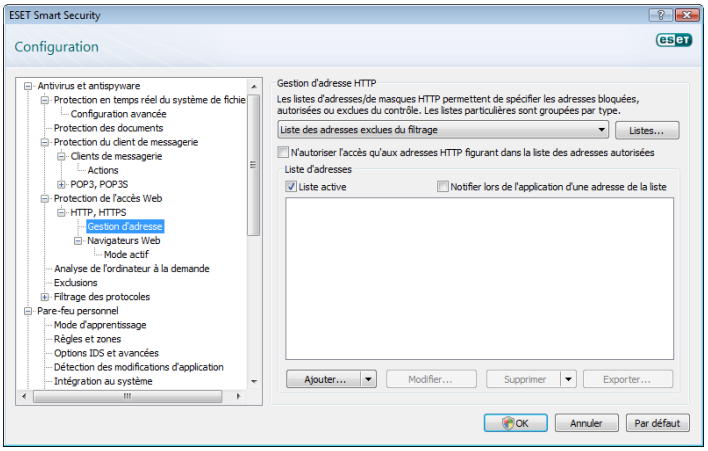


4.1.4.1.1 Gestion d'adresse

Cette section permet de spécifier des adresses HTTP à bloquer, autoriser ou exclure de la vérification.

Les boutons **Ajouter, Modifier, Supprimer** et **Exporter** permettent de gérer les listes d'adresses. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web figurant dans la liste des adresses exclues sont accessibles sans aucune analyse de code malveillant. Si vous activez l'option ***N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées***, seules les adresses figurant dans la liste des adresses autorisées sont accessibles, tandis que toutes les autres adresses HTTP sont bloquées.

Dans toutes les listes, vous pouvez utiliser les symboles spéciaux * (astérisque) et ? (point d'interrogation). L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère individuel. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et fiables. De même, il faut veiller à employer correctement les symboles * et ? dans cette liste. Pour activer une liste, activez l'option ***Liste active***. Pour être informé lors de l'entrée d'une adresse de la liste actuelle, activez l'option ***Notifier lors de l'application d'une adresse de la liste***.

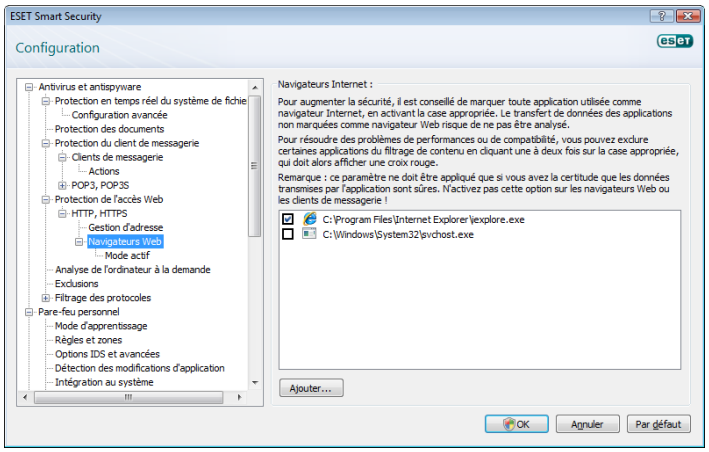


4.1.4.1.2 Navigateurs Web

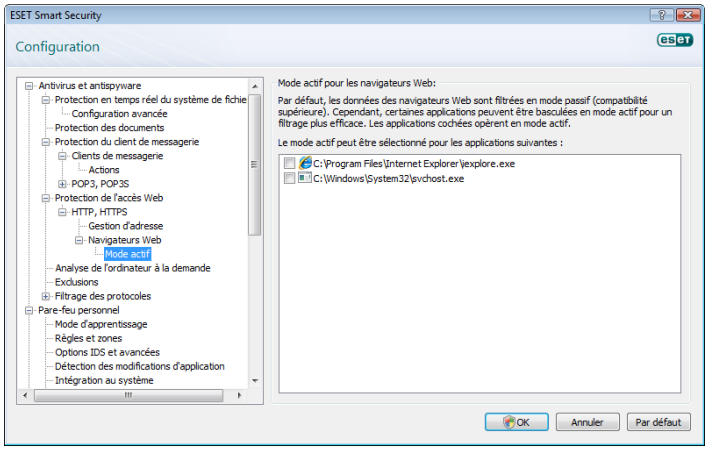
ESET Smart Security contient une fonction **Navigateurs Web** qui permet de définir si une application donnée est un navigateur ou non. Si une application est marquée par l'utilisateur comme étant un navigateur, toutes les communications provenant de cette application sont contrôlées, quels que soient les numéros de ports impliqués dans la communication.

La fonction Navigateurs Web complète la fonction de contrôle HTTP, laquelle ne s'applique qu'à des ports prédéfinis. Or, de nombreux services Internet utilisent des numéros de ports qui changent de manière dynamique ou sont inconnus. Pour prendre cela en compte,

la fonction Navigateurs Web permet de contrôler les communications sur les ports indépendamment des paramètres de connexion.



La liste des applications désignées comme navigateurs est accessible directement à partir du sous-menu **Navigateurs Web** de la branche **HTTP**. Cette section contient également le sous-menu **Mode actif**, qui définit le mode de contrôle des navigateurs Internet. L'intérêt du **Mode actif** est que les données transférées sont examinées dans leur ensemble. S'il n'est pas activé, la communication des applications est contrôlée progressivement, par lots. La vérification des données est alors moins efficace, mais la compatibilité avec les applications répertoriées est meilleure. Si le Mode actif ne pose pas de problèmes, nous recommandons de l'activer en sélectionnant la case à cocher en regard de l'application voulue.



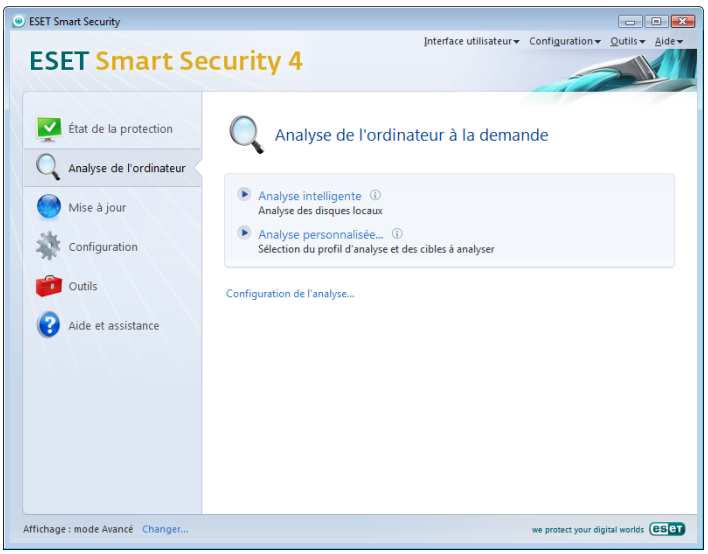
4.1.5 Analyse de l'ordinateur

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez une analyse à la demande pour rechercher d'éventuelles infiltrations. Par souci de sécurité, il est essentiel que l'ordinateur soit analysé non seulement en cas de soupçon d'infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Une analyse régulière assure la détection d'infiltrations non détectées par l'analyseur en temps réel lors de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base de signatures de virus est obsolète.

Nous recommandons d'exécuter une analyse à la demande au moins une ou deux fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils > Planificateur**.

4.1.5.1 Type d'analyse

Deux types sont disponibles. L'**Analyse standard** analyse rapidement le système sans exiger de configuration supplémentaire des paramètres d'analyse. L'**Analyse personnalisée**... permet à l'utilisateur de sélectionner un des profils d'analyse prédéfinis, ainsi que de choisir des objets d'analyse dans l'arborescence.



4.1.5.1.1 Analyse standard

L'analyse standard est une méthode conviviale qui permet à l'utilisateur de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de sa part. Les principaux avantages sont la facilité d'utilisation et l'absence de configuration détaillée de l'analyse. L'analyse standard vérifie tous les fichiers sur les lecteurs locaux et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur la valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage (page 18).

Le profil d'analyse standard est conçu pour les utilisateurs qui souhaitent analyser rapidement et facilement leurs ordinateurs. Il offre une solution d'analyse et de nettoyage efficace sans exiger une configuration détaillée.

4.1.5.1.2 Analyse personnalisée

L'analyse personnalisée est une solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'avantage de l'analyse personnalisée est la possibilité de configurer les paramètres de manière détaillée. Les configurations peuvent être enregistrées dans des profils d'analyse définis par l'utilisateur, utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner les cibles à analyser, utilisez le menu déroulant de la fonction de ciblage rapide ou sélectionnez des cibles dans l'arborescence des périphériques de l'ordinateur. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration... > Nettoyage**. Si vous souhaitez uniquement une analyse du système, sans action supplémentaire, activez la case à cocher **Analyse sans nettoyage**.

L'exécution d'analyses en mode Personnalisé convient pour des utilisateurs chevronnés ayant déjà utilisé des programmes antivirus.

4.1.5.2 Cibles à analyser

Le menu déroulant Cibles à analyser permet de sélectionner les fichiers, dossiers et périphériques (disques) à soumettre à l'analyse antivirus.

Les paramètres d'analyse rapide permettent de sélectionner les cibles suivantes :

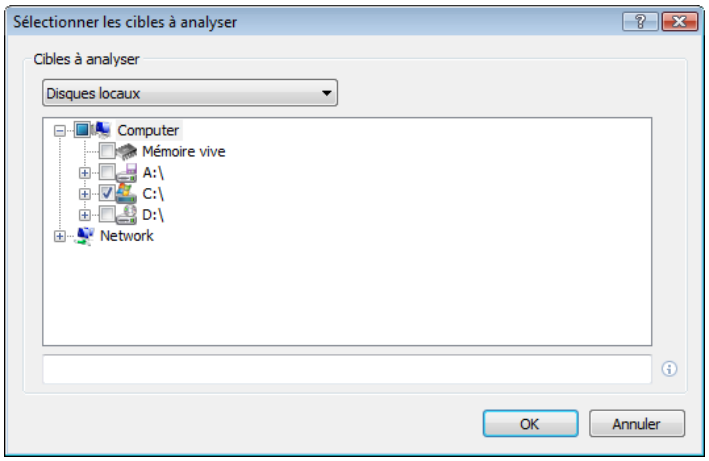
Par paramètres de profil : contrôle les cibles spécifiées dans le profil sélectionné.

Supports amovibles : disquettes, périphériques de stockage USB, CD/DVD.

Disques locaux : contrôle tous les disques durs du système.

Lecteurs réseau : analyse toutes les unités mappées.

Aucune sélection : annule toutes les sélections.



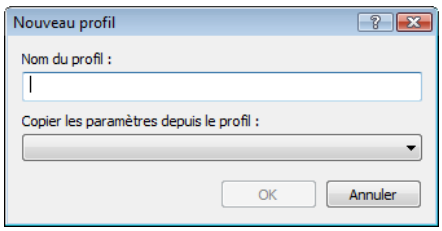
Une cible d'analyse peut aussi être spécifiée plus précisément en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans l'arborescence des périphériques de l'ordinateur.

4.1.5.3 Profils d'analyse

Vos paramètres d'analyse préférés peuvent être enregistrés dans des profils. L'avantage de créer des profils d'analyse est que vous pouvez les réutiliser pour des analyses futures. Il est recommandé de créer autant de profils (avec différentes cibles, méthodes et autres paramètres d'analyse) que vous en utilisez régulièrement.

Pour créer un profil utilisable pour des analyses futures, choisissez **Configuration avancée** (F5) **> Analyse- d'ordinateur à la demande**. Cliquez sur le bouton **Profils...** à droite de l'écran pour afficher la liste des profils d'analyse existants et l'option permettant d'en créer d'autres. La rubrique **Configuration des paramètres du moteur ThreatSense** ci-dessous décrit chacun des paramètres d'analyses configurables. Elle vous aidera à créer un profil d'analyse adapté à vos besoins.

Exemple :
Imaginez que vous vouliez créer votre propre profil d'analyse et que la configuration associée au profil **Smart scan** vous convienne en partie. Vous ne souhaitez cependant pas analyser les fichiers exécutables compressés par un compresseur d'exécutables ni les applications potentiellement dangereuses et voulez appliquer un **Nettoyage strict**. Dans la fenêtre **Profils de configuration**, cliquez sur le bouton**Ajouter...**. Entrez le nom du nouveau profil dans le champ **Nom du profil**, puis sélectionnez **Smart scan** dans le menu déroulant **Copier les paramètres depuis le profil**. Adaptez ensuite les autres paramètres à vos besoins.



4.1.6 Filtrage des protocoles

La protection antivirus pour les protocoles d'application POP3 et HTTP est assurée par le moteur d'analyse ThreatSense, qui intègre toutes les techniques d'analyse avancées des logiciels malveillants. Le contrôle fonctionne automatiquement indépendamment du navigateur Internet ou du client de messagerie utilisé. Les options suivantes sont disponibles pour le filtrage de protocole (si l'option **Activer le filtrage de protocole d'application** est activée :

Ports HTTP et POP3 : limite l'analyse des communications pour connaître les ports HTTP et POP3.

Applications marquées comme navigateurs Internet et clients de messagerie : activez cette option pour ne filtrer que les communications d'application marquées comme étant des navigateurs (Protection de l'accès Web > HTTP, HTTPS > Navigateurs Web) et des clients de messagerie (Protection du client de messagerie > POP3, POP3S > Clients de messagerie).

Ports et applications marqués comme navigateurs Internet ou clients de messagerie : tant les ports que les navigateurs font l'objet d'une détection des logiciels malveillants.

Remarque :
À partir de Windows Vista Service Pack 1 et de Windows Server 2008, un nouveau filtrage des communications est utilisé. Par conséquent, la section Filtrage des protocoles est indisponible.

4.1.6.1 SSL

ESET Smart Security 4 permet de contrôler les protocoles encapsulés dans le protocole SSL. Vous pouvez utiliser divers modes d'analyse pour les communications SSL protégées utilisant des certificats approuvés, inconnus ou exclus du contrôle des communications SSL protégées.

Toujours analyser le protocole SSL (les certificats exclus et fiables resteront valides) : activez cette option pour analyser toutes les communications SSL protégées, à l'exception de celles qui le sont par des certificats exclus du contrôle. Si une nouvelle communication utilisant un certificat signé inconnu est établie, l'utilisateur n'en est pas informé et la communication est filtrée automatiquement. Lorsque l'utilisateur accède à un serveur à l'aide d'un certificat non approuvé marqué par lui comme approuvé (ajouté à la liste des certificats approuvés), la communication avec le serveur est autorisée et le contenu du canal de communication est filtré.

Interroger sur les sites non visités (certificats inconnus) : si vous accédez à un nouveau site protégé par SSL (avec un certificat inconnu), une boîte de dialogue vous permettant de sélectionner une action s'affiche. Ce mode permet de créer une liste de certificats SSL qui seront exclus de l'analyse.

Ne pas analyser le protocole SSL : si cette option est activée, le programme n'analyse pas les communications SSL.

S'il est impossible de vérifier le certificat à l'aide du magasin d'Autorités de certification racine de confiance

Interroger sur la validité de la certification : invite l'utilisateur à choisir une action à exécuter.

Bloquer toute communication utilisant le certificat : met fin à la connexion au site utilisant le certificat.

Si le certificat est invalide ou endommagé

Interroger sur la validité du certificat : invite l'utilisateur à choisir une action à exécuter.

Bloquer toute communication utilisant le certificat : met fin à la connexion au site utilisant le certificat.

4.1.6.1.1 Certificats approuvés

Outre le magasin d'Autorités de certification de racine de confiance intégré, dans lequel ESET Smart Security 4 conserve le certificat approuvé, vous pouvez créer une liste personnalisée de certificats, accessible dans **Configuration** (F5) **> Filtrage de protocole > SSL > Certificats approuvés**.

4.1.6.1.2 Certificats exclus

La section Certificats exclus contient des certificats considérés comme sûrs. Le programme ne vérifie pas le contenu de communications chiffrées à l'aide de certificats dans cette liste. Il est recommandé de n'installer que les certificats Web dont la sécurité est garantie et pour lesquels aucun filtrage du contenu n'est nécessaire.

4.1.7 Configuration du moteur ThreatSense

ThreatSense est une technologie qui comprend des méthodes de détection de menaces complexes. Cette technologie est proactive : elle fournit également une protection durant les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Le moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, maximisant ainsi l'efficacité et le taux de détection. Cette technologie élimine avec succès les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

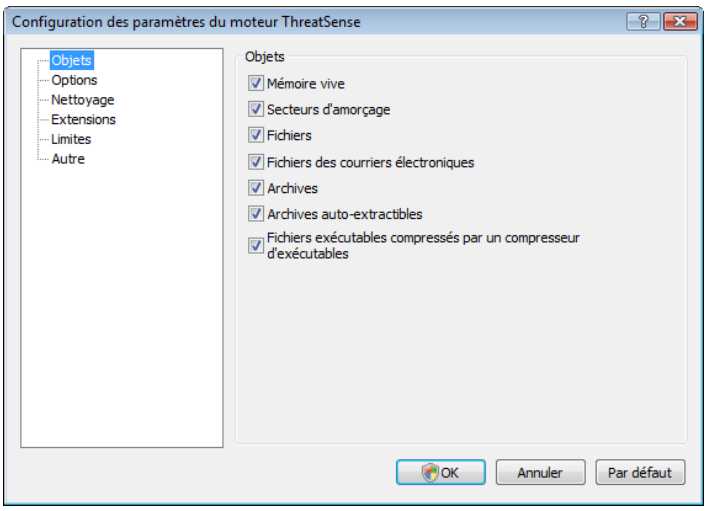
Pour ouvrir la fenêtre de configuration, cliquez sur **Configurer...** situé dans n'importe quelle fenêtre de configuration de module qui utilise la technologie ThreatSense (voir ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. Sachant cela, ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Contrôle des fichiers de démarrage du système
- Protection du courrier
- Protection de l'accès Web
- Analyse d'ordinateur à la demande

Les paramètres ThreatSense sont très optimisés pour chaque module et leur modification peut affecter significativement le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les Fichiers exécutables compressés par un compresseur d'exécutables ou pour autoriser l'heuristique avancée dans la protection en temps réel du système de fichiers, vous risquez de dégrader les performances du système (normalement, seuls les nouveaux fichiers créés sont analysés par ces méthodes). Il est donc recommandé de laisser les paramètres par défaut de ThreatSense inchangés pour tous les modules à l'exception du module Analyse de l'ordinateur.

4.1.7.1 Configuration des objets

La section **Objets** permet de définir les composants de l'ordinateur et fichiers à analyser.



Mémoire vive : détecte les menaces qui portent sur la mémoire vive du système.

Secteurs d'amorçage : analyse les secteurs d'amorçage à la recherche de virus dans l'enregistrement d'amorçage principal.

Fichiers : analyse tous les types de fichiers courants (programmes, images, musiques, vidéos, bases de données, etc.).

Fichiers de messages : analyse les fichiers spéciaux contenant les messages électroniques.

Archives : analyse les fichiers compactés dans des archives (.rar, .zip, .arj, .tar, etc.).

Archives auto-extractibles : analyse les fichiers contenus dans des fichiers d'archive auto-extractibles, généralement présentés avec une extension .exe.

Fichiers exécutables compressés par un compresseur d'exécutables : ces fichiers (à la différence des types d'archives standard) se décompactent en mémoire, comme les compacteurs statiques standard (UPX, yoda, ASPack, FGS, etc.).

4.1.7.2 Options

La section Options permet de sélectionner les méthodes à utiliser lors de la recherche d'infiltrations sur le système. Les options suivantes sont disponibles :

Signatures : l'option Signatures permet de détecter et identifier de manière précise et fiable toute infiltration par son nom grâce aux signatures de virus.

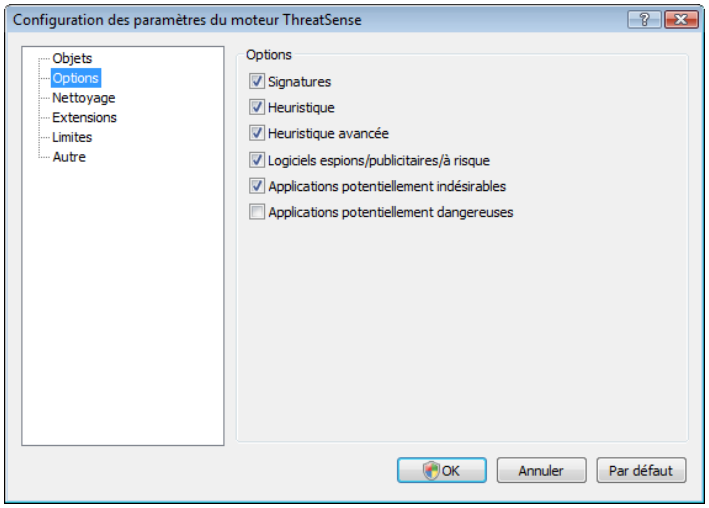
Heuristique : l'heuristique est un algorithme qui analyse l'activité (malveillante) des programmes. Le principal avantage de la détection heuristique est la possibilité de détecter de nouveaux logiciels malveillants qui n'existaient pas précédemment ou ne figuraient pas dans la liste des virus connus (base des signatures de virus).

Heuristique avancée : cette option utilise un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. L'heuristique avancée augmente sensiblement l'intelligence de détection du programme.

Logiciels espions/publicitaires/à risque : cette catégorie couvre les logiciels qui collectent diverses informations confidentielles sur les utilisateurs sans leur consentement informé. Elle inclut également les logiciels qui affichent des publicités.

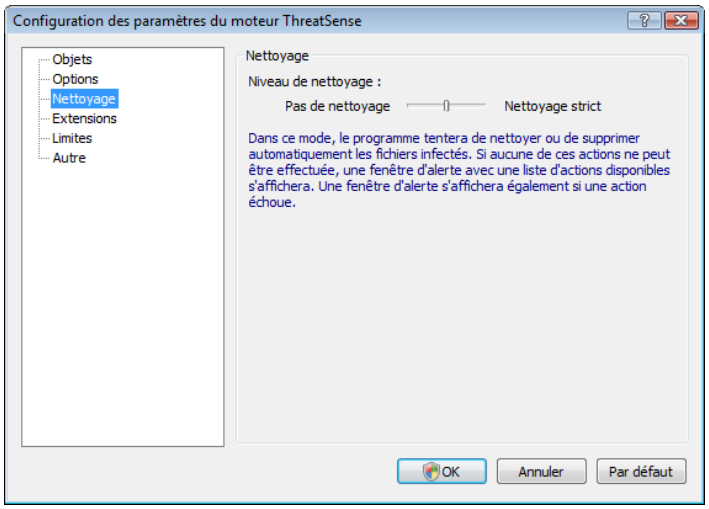
Applications potentiellement dangereuses : cette classification couvre les logiciels commerciaux légitimes. Elle inclut des programmes tels que des outils d'accès à distance, raison pour laquelle cette option est désactivée par défaut.

Applications potentiellement indésirables : ces applications ne sont pas nécessairement malveillantes par destination, mais peuvent altérer les performances de votre ordinateur. Leur installation requiert généralement un consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Les changements les plus significatifs concernent les fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'utilisation accrue des ressources système, des changements dans les résultats de recherche et la communication avec des serveurs distants.



4.1.7.3 Nettoyage

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Trois niveaux de nettoyage sont possibles :



Ne pas nettoyer
Les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche alors une fenêtre d'avertissement et laisse l'utilisateur choisir une action.

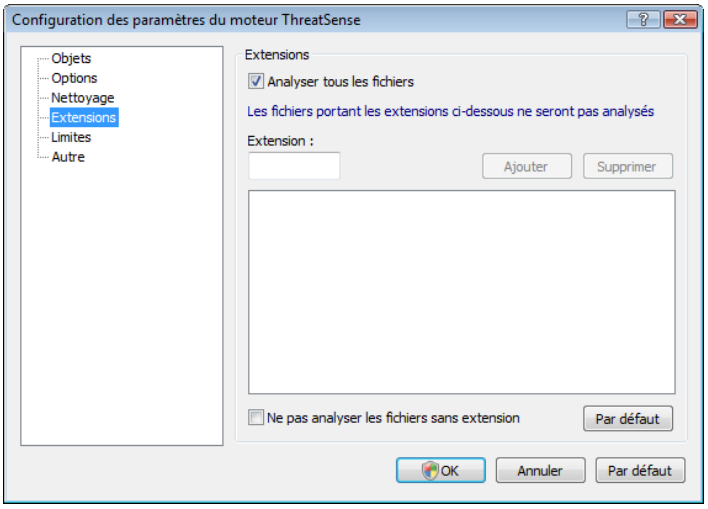
Niveau par défaut
Le programme tente de nettoyer ou supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose un choix d'actions de suivi. Ce choix s'affiche également si une action prédéfinie ne peut être exécutée.

Nettoyage strict
Le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, une fenêtre d'avertissement s'affiche avec une proposition d'action utilisateur.

Avertissement :
dans le mode Défaut, le fichier d'archive n'est entièrement supprimé que si tous les fichiers qu'il contient sont infectés. S'il contient aussi des fichiers légitimes, il n'est pas supprimé. Si un fichier d'archive infecté est détecté dans le mode Nettoyage strict, le fichier entier est supprimé, même s'il contient aussi des fichiers intacts.

4.1.7.4 Extensions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense permet de définir les types de fichiers à analyser.



Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. N'importe quelle extension peut être ajoutée à la liste des fichiers exclus de l'analyse. Si l'option **Analyser tous les fichiers** est désactivée, la liste change et affiche toutes les extensions de fichiers actuellement analysées. Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des fichiers portant certaines extensions.

Pour activer l'analyse de fichiers sans extension, activez l'option **Analyser les fichiers sans extension**.

L'exclusion de fichiers de l'analyse peut être utile lorsque certains types de fichiers provoquent un fonctionnement incorrect du programme utilisant ces extensions. Par exemple, il peut être judicieux d'exclure les extensions .edb, .eml et .tmp si vous utilisez le serveur MS Exchange.

4.1.7.5 Limites

La section Limites permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

Taille d'objet maximale (octets)
Définit la taille maximale des objets à analyser. Le module antivirus donné n'analyse alors que des objets d'une taille inférieure à celle spécifiée. Il n'est pas recommandé de modifier la valeur par défaut et il n'y a généralement aucune raison de le faire. Cette option ne devrait être modifiée que par des utilisateurs chevronnés ayant des raisons spécifiques d'exclure de l'analyse des objets de plus grande taille.

Durée d'analyse maximale pour l'objet (s)
Spécifie la valeur de temps maximale pour l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit finie ou non.

Niveau d'imbrication des archives
Spécifie la profondeur maximale d'analyse des archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive reste non vérifiée.

Taille maximale de fichier dans l'archive (octets)
Cette option permet de spécifier la taille maximale (après extraction) des fichiers à analyser dans les archives. Si l'analyse d'une archive prend fin prématurément pour cette raison, l'archive reste non vérifiée.

4.1.7.6 Autre

Analyser les flux de données alternatifs
Les flux de données alternatifs (ADS) utilisés par le système de fichiers NTFS sont des associations de fichiers et dossiers qui sont invisibles pour les techniques ordinaires de détection. Nombre d'infiltrations tentent d'éviter la détection en se faisant passer pour des flux de données alternatifs.

Exécuter les analyses en arrière-plan avec une priorité faible
Toute séquence d'analyse consomme une certaine quantité de ressources système. Si vous utilisez des programmes qui exigent beaucoup de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Journaliser tous les objets
Si cette option est activée, le journal montrera tous les fichiers analysés, même ceux qui ne sont pas infectés.

Conserver la date et l'heure du dernier accès
Activez cette option pour conserver l'heure d'accès d'origine des fichiers analysés au lieu de la mettre à jour (p. ex., pour l'utiliser avec des systèmes de sauvegarde de données).

L'optimisation intelligente est
L'optimisation intelligente est conçue pour simplifier l'analyse de votre système. Une fois activée, cette option accroit la vitesse d'analyse, sans diminuer ou nuire à la sécurité de votre système

Faire défiler le journal de l'analyse
Cette option permet d'activer ou de désactiver le défilement du journal. Si cette option est sélectionnée, les informations défilent vers le haut dans la fenêtre d'affichage.

Afficher la notification de fin d'analyse dans une fenêtre séparée
Ouvre une fenêtre indépendante contenant des informations sur les résultats d'analyse.

4.1.8 Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

- Ouvrez ESET Smart Security et cliquez sur **Analyse de l'ordinateur**
- Cliquez sur **Analyse standard** (pour plus d'informations, reportez-vous à la section Analyse standard).
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

Pour donner un exemple général de la façon dont les infiltrations sont traitées dans ESET Smart Security, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. Le programme tente de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'avertissement. Généralement, les options **Nettoyer**, **Supprimer** et **Laisser** sont disponibles. Il n'est pas recommandé de sélectionner **Laisser**, car les fichiers infectés seraient conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et a été détecté par erreur.

Nettoyage et suppression
Utilisez le nettoyage si un fichier sain a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, tentez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il sera supprimé.

Si un fichier infecté est « verrouillé » ou utilisé par un processus du système, il n'est généralement supprimé qu'après avoir été déverrouillé (généralement, après un redémarrage du système).

Suppression de fichiers dans des archives
En mode de nettoyage Défaut, l'archive entière n'est supprimée que si elle ne contient que des fichiers infectés et pas de fichiers sains. Autrement dit, les archives ne sont pas supprimées si elles contiennent aussi des fichiers sains. Cependant, soyez prudent si vous choisissez un nettoyage strict : en mode de Nettoyage strict, l'archive sera supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

4.2 Pare-feu personnel

Le pare-feu personnel contrôle tout le trafic réseau entrant et sortant du système. En fonction des règles de filtrage spécifiées, les différentes connexions réseau sont autorisées ou refusées. Le pare-feu fournit une protection contre les attaques en provenance d'ordinateurs distants et permet de bloquer certains services. Il fournit également une protection antivirus pour les protocoles HTTP et POP3. Cette fonctionnalité représente un élément important de la sécurité d'un ordinateur.

4.2.1 Modes de filtrage

Le pare-feu personnel d'ESET Smart Security comprend cinq modes de filtrage. Le comportement du pare-feu change en fonction du mode sélectionné. Les modes de filtrage ont également une incidence sur le niveau d'interaction de l'utilisateur.

Le filtrage peut être réalisé dans l'un des cinq modes suivants :

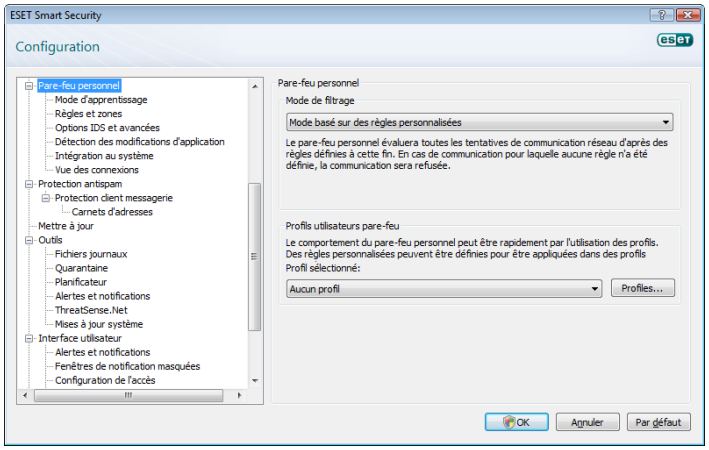
Mode automatique : c'est le mode par défaut. Il convient aux utilisateurs qui préfèrent un usage simple et pratique du pare-feu, sans nécessité de définir des règles. Le mode automatique autorise tout trafic sortant du système et bloque toutes les nouvelles connexions en provenance du côté distant.

Mode automatique avec exceptions (règles définies par l'utilisateur) : outre les fonctions du mode automatique, il permet d'ajouter des règles personnalisées.

Mode interactif : permet de personnaliser la configuration du pare-feu personnel. Lorsqu'une communication est détectée et qu'aucune règle n'est associée à cette communication, une boîte de dialogue s'affiche pour signaler une connexion inconnue. Cette boîte de dialogue permet d'autoriser ou de refuser la communication, cette décision pouvant être mémorisée comme nouvelle règle pour le pare-feu personnel. Si vous choisissez de créer une règle à ce moment, toutes les connexions futures de ce type seront autorisées ou refusées conformément à la règle.

Mode basé sur des règles personnalisées : bloque toute connexion ne faisant pas l'objet d'une règle spécifique l'autorisant. Ce mode permet aux utilisateurs expérimentés de définir des règles qui n'autorisent que des connexions souhaitées et sûres. Toute autre connexion non spécifiée sera bloquée par le pare-feu personnel.

Mode d'apprentissage : crée et enregistre automatiquement les règles et convient pour la configuration initiale du pare-feu personnel. Aucune intervention de l'utilisateur n'est requise, car ESET Smart Security enregistre les règles conformément aux paramètres prédéfinis. Le mode d'apprentissage n'étant pas sécurisé, il est recommandé de ne l'utiliser que jusqu'à ce que toutes les règles aient été créées pour les communications requises.



4.2.2 Profils

Les profils permettent de contrôler le comportement du pare-feu personnel ESET Smart Security. Lorsque vous créez ou modifiez une règle de pare-feu personnel, vous pouvez l'attribuer à un profil spécifique ou l'appliquer à tous les profils. Lorsque vous sélectionnez un profil, seules les règles globales (sans aucun profil indiqué) et les règles attribuées à ce profil sont appliquées. Vous pouvez créer plusieurs profils avec différentes règles attribuées afin de modifier facilement le comportement du pare-feu personnel.

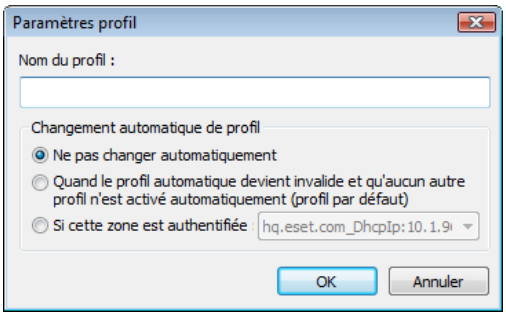
4.2.2.1 Gestion des profils

Cliquez sur le bouton **Profils...** (reportez-vous à la figure de la section 4.2.1, « Modes de filtrage ») pour ouvrir la fenêtre **Profils pare-feu**, dans laquelle vous pouvez **ajouter**, **modifier** et **supprimer** des profils. Notez que pour **modifier** ou **supprimer** un profil, ce dernier ne doit pas être sélectionné dans le menu déroulant **Profil sélectionné**. Lorsque vous ajoutez ou modifiez un profil, vous pouvez également définir les conditions de son déclenchement. Les possibilités suivantes sont disponibles :

Ne pas changer automatiquement : le déclencheur automatique est désactivé (le profil doit être activé manuellement).

Quand le profil automatique devient invalide et qu'aucun autre profil n'est activé automatiquement (profil par défaut) : lorsque le profil automatique devient incorrect (si l'ordinateur est connecté à un réseau non fiable, reportez-vous à la section 4.2.6.1, « Authentification réseau ») et qu'aucun autre profil n'est activé à la place (l'ordinateur n'est pas connecté à un autre réseau fiable), le pare-feu personnel bascule vers ce profil. Un seul profil peut utiliser ce déclencheur.

Si cette zone est authentifiée : ce profil est déclenché lors de l'authentification de la zone spécifiée (reportez-vous à la section 4.2.6.1, « Authentification réseau »).



Lorsque le pare-feu personnel bascule vers un autre profil, une notification apparaît dans l'angle inférieur droit, à côté de l'horloge système.

4.2.3 Bloquer tout le trafic réseau : déconnecter le réseau

La seule option permettant de bloquer tout le trafic réseau est **Bloquer tout le trafic réseau : déconnecter le réseau**. Toute communication entrante et sortante est bloquée par le pare-feu personnel sans aucun message d'avertissement. N'utiliser cette option qu'en cas de soupçon de risques critiques de sécurité qui nécessitent la déconnexion du système du réseau.

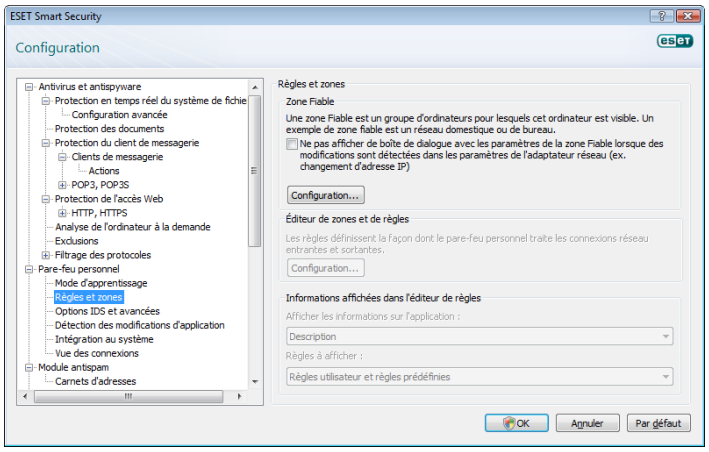
4.2.4 Désactiver le filtrage : autoriser tout le trafic

L'option Désactiver le filtrage est à l'opposé du blocage de l'intégralité du trafic réseau. Si cette option est activée, toutes les options de filtrage du pare-feu personnel sont désactivées et toutes les connexions entrantes et sortantes sont autorisées. C'est comme si le pare-feu n'existait pas.

4.2.5 Configuration et utilisation des règles

Les règles représentent un ensemble de conditions utilisées pour tester de façon significative toutes les connexions réseau ainsi que toutes les actions affectées à ces conditions. Dans le pare-feu personnel, vous pouvez choisir l'action à exécuter si une connexion définie par une règle est établie.

Pour accéder à la configuration des règles de filtrage, accédez à **Configuration avancée** (F5) > **Pare-feu personnel** > **Règles et zones**. Pour afficher la configuration actuelle, cliquez sur **Configuration...** dans la section **Éditeur de zones et de règles** (si le pare-feu personnel est configuré sur **Mode automatique**, ces paramètres ne sont pas disponibles).



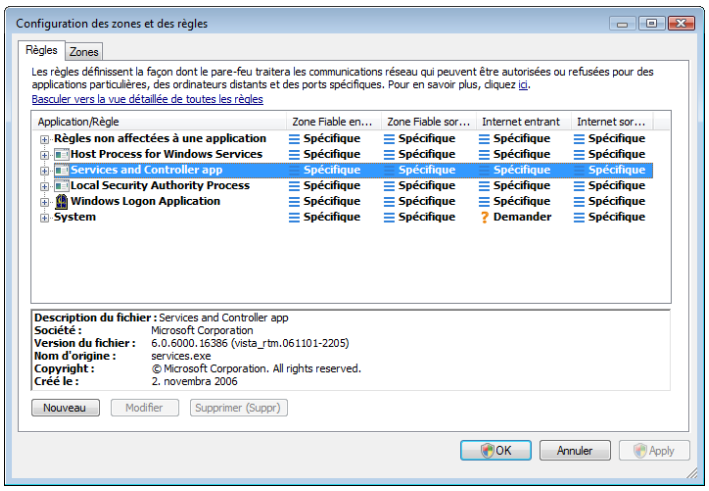
Un aperçu des règles ou des zones est affiché dans la fenêtre **Configuration des zones et des règles** (en fonction de l'onglet sélectionné). La fenêtre est divisée en deux sections. La section supérieure donne un aperçu résumé de chaque règle. La section inférieure affiche les détails de la règle sélectionnée dans la section supérieure. Dans la partie inférieure figurent les boutons **Nouveau**, **Modifier** et **Supprimer (Suppr)**, qui permettent à l'utilisateur de configurer les règles.

Les connexions peuvent être divisées en connexions entrantes et sortantes. Les connexions entrantes sont initiées par un ordinateur distant qui tente d'établir une connexion avec le système local. Les connexions sortantes fonctionnent dans le sens opposé : le côté local contacte l'ordinateur distant.

Si une nouvelle communication inconnue est détectée, il faut décider prudemment s'il faut l'autoriser ou la rejeter. Les connexions non sollicitées, non sûres ou inconnues posent un risque de sécurité au système. Si une telle connexion est établie, il est recommandé de faire très attention au côté distant et aux applications qui tentent de se connecter à votre ordinateur. Beaucoup d'infiltrations essaient d'obtenir et d'envoyer des données personnelles ou de télécharger d'autres applications malveillantes aux postes de travail hôtes. Le pare-feu personnel permet à l'utilisateur de détecter et mettre fin à de telles connexions.

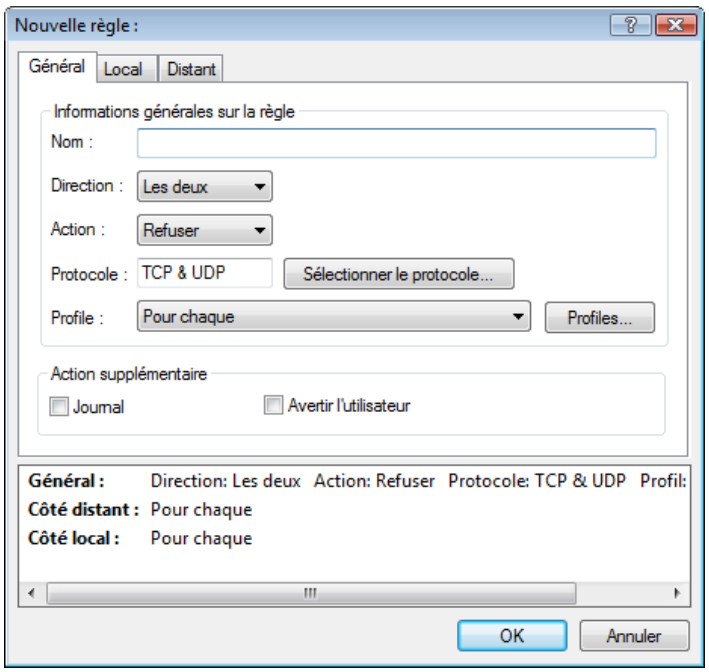
4.2.5.1 Création de nouvelles règles

Une nouvelle règle doit être créée à chaque installation de nouvelle application qui accède au réseau ou en cas de modification de connexion existante (côté distant, numéro de port, etc.).



Pour ajouter une nouvelle règle, vérifiez que l'onglet Règles est sélectionné. Cliquez sur le bouton Nouveau dans la fenêtre Configuration des zones et des règles. La boîte de dialogue qui s'ouvre permet de spécifier une nouvelle règle. La partie supérieure de la fenêtre contient trois onglets :

- **Général** : spécifiez le nom d'une règle, le sens de la connexion, l'action, le protocole et le profil dans lequel la règle s'applique.
- **Distant** : cet onglet comprend des informations concernant le port distant (plage de ports). Il vous permet également de définir la liste des adresses IP ou zones distantes pour la règle en question.
- **Local** : affiche des informations sur le côté local de la connexion, notamment le numéro du port local ou la plage des ports, ainsi que le nom de l'application communicante.



Un bon exemple d'ajout de nouvelle règle est d'autoriser le navigateur Internet à accéder au réseau. Dans ce cas, les informations suivantes doivent êtres fournies :

- Dans l'onglet **Général**, activez les communications sortantes via le protocole TCP & UDP.
- Dans l'onglet **Local**, ajoutez le processus représentant le navigateur (pour Internet Explorer, iexplore.exe).
- Dans l'onglet **Distant**, activez le port numéro 80 pour n'autoriser que les activités de navigation Internet standard.

4.2.5.2 Modification des règles

Pour modifier une règle existante, cliquez sur le bouton **Modifier**. Tous les paramètres (reportez-vous à la section 4.2.5.1, « Création de nouvelles règles » pour accéder aux descriptions) peuvent être modifiés.

Une modification s'impose chaque fois qu'un paramètre de contrôle change. Dans ce cas, la règle ne remplit pas les conditions et les actions spécifiées ne peuvent pas être appliquées. Enfin, la connexion donnée risque d'être refusée et cela peut engendrer des problèmes de fonctionnement de l'application en question. Un exemple est le changement d'adresse ou le numéro de port du côté distant.

4.2.6 Configuration des zones

Dans la fenêtre **Configuration de la zone**, vous pouvez indiquer le nom de la zone, la description, la liste des adresses réseau et l'authentification de la zone (reportez-vous à la section 4.2.6.1.1, « Authentification de zone – Configuration du client »).

Une zone représente un groupe d'adresses réseau formant un groupe logique. Chaque adresse d'un groupe donné se voit attribuer les mêmes règles définies de manière centralisée au niveau du groupe. La zone Fiable est un exemple de groupe. La zone Fiable représente un groupe d'adresses réseau totalement fiables et qui ne sont d'aucune manière bloquées par le pare-feu personnel.

Ces zones peuvent être configurées au moyen de l'onglet **Zones** de la fenêtre **Configuration des zones et des règles** ; vous y accédez en cliquant sur le bouton **Nouveau**. Saisissez le **nom** et la **description** de la zone, puis ajoutez une adresse IP distante en cliquant sur le bouton **Ajouter une adresse IPv4**.

4.2.6.1 Authentification réseau

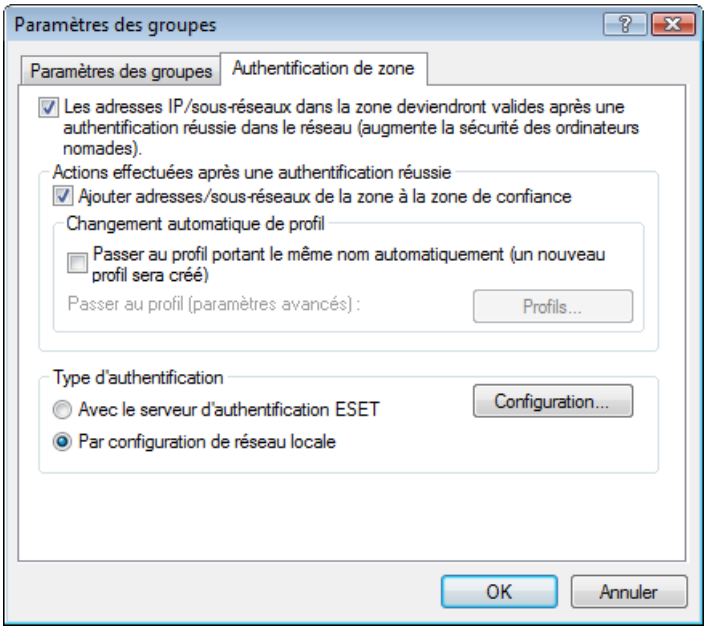
La zone Fiable est identifiée par l'adresse IP locale de l'adaptateur réseau. Les ordinateurs portables se connectent souvent à des réseaux avec des adresses IP semblables à celle du réseau fiable. Si les paramètres de zone Fiable ne sont pas basculés automatiquement sur **Protection stricte**, le pare-feu personnel continue à utiliser le mode **Autoriser le partage**.

Pour éviter ce type de situation, l'authentification de zone recherche un serveur spécifique sur le réseau et utilise le chiffrement asymétrique (algorithme RSA) pour authentifier le serveur. L'authentification est répétée pour chaque réseau auquel votre ordinateur se connecte.

4.2.6.1.1 Authentification de zone – Configuration du client

Dans la fenêtre **Configuration des zones et des règles**, créez une zone à l'aide du nom de la zone authentifiée par le serveur. Cliquez ensuite sur **Ajouter une adresse IPv4** et sélectionnez l'option Sous-réseau pour ajouter un masque de sous-réseau contenant le serveur d'authentification.

Cliquez sur l'onglet **Authentification de zone** et sélectionnez l'option **Les adresses IP/sous-réseaux de la zone deviendront valides après une authentification réussie du serveur dans le réseau**. Une fois cette option sélectionnée, la zone devient non valide si l'authentification n'aboutit pas. Pour sélectionner un profil de pare-feu personnel après l'authentification réussie d'une zone, cliquez sur le bouton **Profils...** Si vous sélectionnez l'option **Ajouter adresses/sous-réseaux de la zone à la zone de confiance**, les adresses/sous-réseaux de la zone sont ajoutés à la zone Fiable après l'authentification (recommandé).



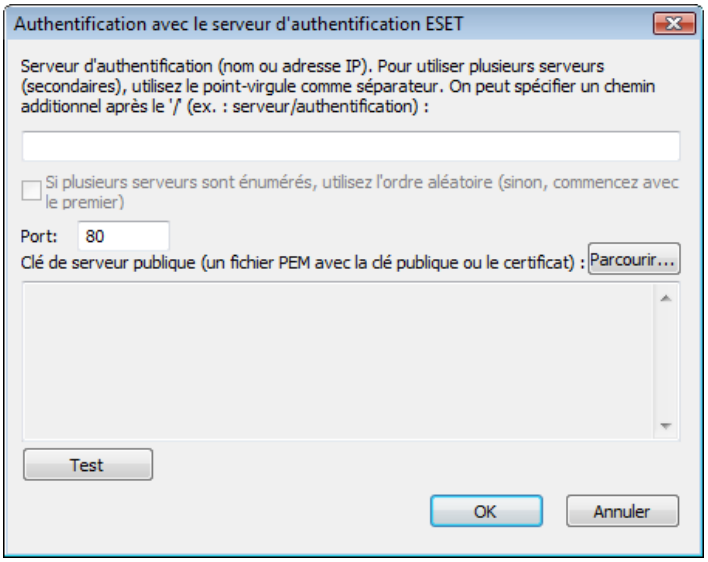
Les trois types d'authentification suivants sont disponibles :

1) Avec le serveur d'authentification ESET

Cliquez sur **Configuration...** et indiquez un nom de serveur, un port d'écoute du serveur et une clé publique qui correspond à la clé privée du serveur (reportez-vous à la section 4.2.6.1.2, « Authentification de zone – Configuration du serveur »). Le nom du serveur peut être saisi sous la forme d'une adresse IP, ou d'un nom DNS ou NetBios. Le nom du serveur peut être suivi d'un chemin indiquant l'emplacement de la clé sur le serveur (par exemple nom_serveur/répertoire1/répertoire2/authentification). Saisissez plusieurs serveurs, séparés par des points-virgules ; ils seront utilisés si le premier serveur n'est pas disponible.

La clé publique peut être un fichier de l'un des types suivants :

- Clé publique chiffrée PEM (.pem) : cette clé peut être générée à l'aide d'ESET Authentication Server (reportez-vous à la section 4.2.6.1.2, « Authentification de zone – Configuration du serveur »).
- Clé publique chiffrée
- Certificat de clé publique (.crt)



Pour tester vos paramètres, cliquez sur le bouton **Test**. Si l'authentification aboutit, le message *Authentification de serveur réussie* apparaît. Si l'authentification n'est pas configurée correctement, l'un des messages d'erreur suivants apparaît :

SAuthentification de serveur échouée. Le temps maximum pour l'authentification s'est écoulé.
Le serveur d'authentification est inaccessible. Vérifiez le nom du serveur/l'adresse IP et/ou les paramètres de pare-feu personnel du client, ainsi que la partie serveur.

Une erreur s'est produite lors de la communication avec le serveur.
Le serveur d'authentification n'est pas en cours d'exécution. Démarrez le service du serveur d'authentification (reportez-vous à la section 4.2.6.1.2, « Authentification de zone – Configuration du serveur »).

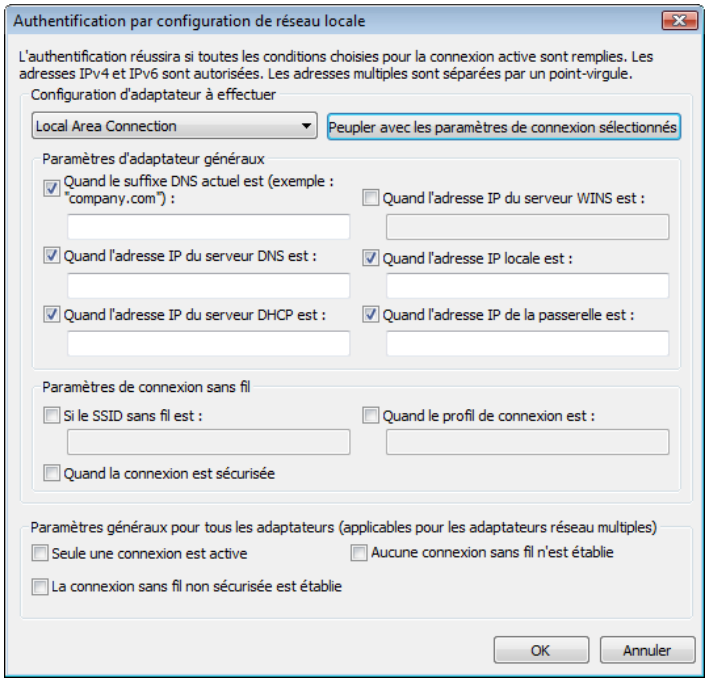
Le nom de la zone d'authentification ne correspond pas à la zone de serveur.
Le nom de la zone configurée ne correspond pas à la zone du serveur d'authentification. Examinez les deux zones et vérifiez que les noms sont identiques.

Authentification de serveur échouée. Adresse de serveur non trouvée dans la liste d'adresses pour la zone donnée.
L'adresse IP de l'ordinateur qui exécute le serveur d'authentification est en dehors de la plage d'adresses IP définie pour la configuration actuelle de la zone.

Authentification de serveur échouée. Une clé publique non valide a probablement été entrée.
Vérifiez que la clé publique indiquée correspond à la clé privée du serveur. Vérifiez également que le fichier de clé publique n'est pas endommagé.

2) Par configuration de réseau locale

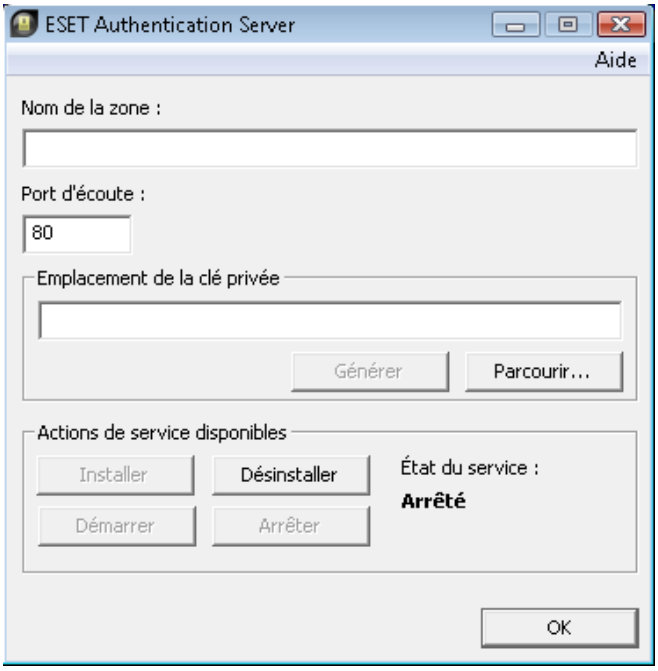
L'authentification est effectuée en fonction des paramètres d'un adaptateur réseau local. L'authentification aboutit si tous les paramètres sélectionnés pour la connexion active sont corrects.



4.2.6.1.2 Authentification de zone – Configuration du serveur

Le processus d'authentification peut être exécuté par tout ordinateur/serveur connecté au réseau et qui doit être authentifié. L'application ESET Authentication Server doit être installée sur un ordinateur/serveur qui est toujours accessible pour l'authentification dès qu'un client tente de se connecter au réseau. Le fichier d'installation de l'application ESET Authentication Server est téléchargeable depuis le site Web d'ESET.

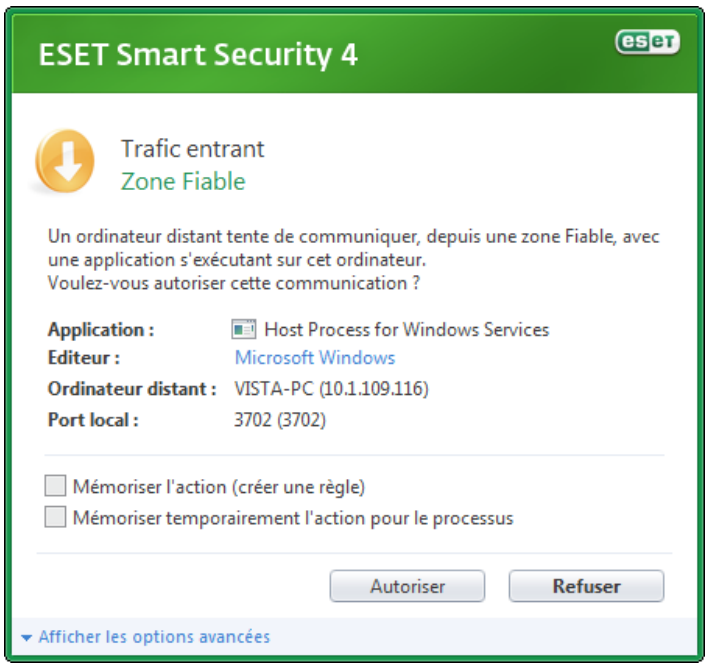
Après l'installation de l'application ESET Authentication Server, une boîte de dialogue apparaît (vous pouvez accéder à l'application à tout moment en choisissant **Démarrer > Programmes > ESET > ESET Authentication Server > ESET Authentication Server**).



Pour configurer le serveur d'authentification, saisissez le nom de la zone d'authentification, le port d'écoute du serveur (il s'agit par défaut du port 80), ainsi que l'emplacement de stockage de la paire de clés publique et privée. Générez ensuite les clés publique et privée qui seront utilisées dans le processus d'authentification. La clé privée reste définie sur le serveur, tandis que la clé publique doit être importée sur le côté client, dans la section Authentification de zone, lors de la configuration de la zone au cours de la configuration du pare-feu.

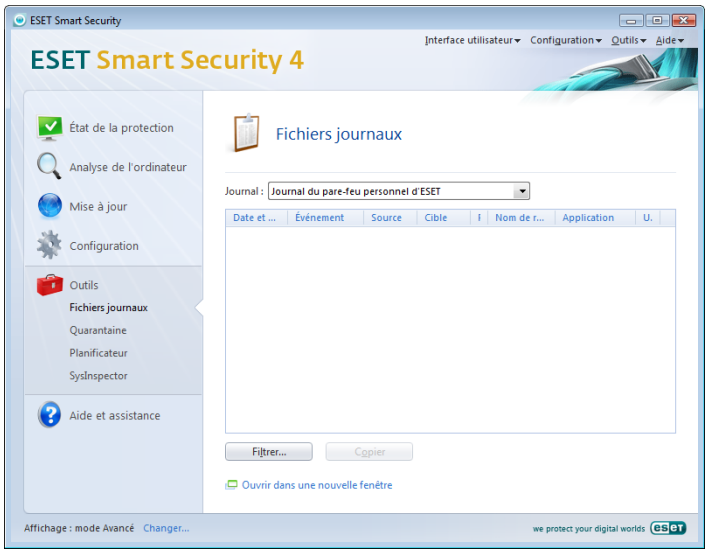
4.2.7 Établissement d'une connexion – détection

Le pare-feu personnel détecte toute nouvelle connexion au réseau. Le mode pare-feu actif détermine les actions à exécuter pour la nouvelle règle. Le pare-feu personnel exécutera les actions prédéfinies sans intervention de l'utilisateur lorsque le mode Automatique ou Basé sur des règles personnalisées est actif. Le mode interactif affiche une fenêtre d'information qui signale la détection d'une nouvelle connexion réseau, complétée d'informations détaillées sur la connexion. Vous pouvez choisir d'autoriser la connexion ou de la refuser (bloquer). Si vous autorisez toujours la même connexion dans la boîte de dialogue, il est recommandé de créer une nouvelle règle pour la connexion. Pour ce faire, sélectionnez l'option **Mémoriser l'action** (créer une règle) et sauvegardez l'action en tant que nouvelle règle pour le pare-feu personnel. Si le pare-feu personnel reconnaît la même connexion plus tard, il appliquera la règle existante.



Il faut être très attentif lors de la création de nouvelles règles et n'autoriser que les connexions sûres. Si toutes les connexions sont autorisées, le pare-feu personnel n'a aucune raison d'exister. Voici les paramètres importants pour les connexions :

- **Côté distant :** n'autorisez que les connexions aux adresses fiables et connues
- **Application locale :** il n'est pas conseillé d'établir des connexions à des applications et processus inconnus
- **Numéro de port :** les communications via les ports communs (par exemple le port numéro 80 pour le trafic réseau) doivent être autorisées dans des circonstances normales.



Pour proliférer, les infiltrations aux ordinateurs utilisent souvent des connexions masquées et Internet pour infecter les systèmes distants. Si les règles sont correctement configurées, le pare-feu personnel devient un important outil de protection contre diverses attaques des codes malveillants.

4.2.8 Journalisation

Le pare-feu personnel intégré dans ESET Smart Security enregistre tous les événements importants dans un journal, accessible directement à partir du menu principal. Cliquez sur **Outils > Fichiers journaux**, puis sélectionnez **Journal du pare-feu personnel ESET** dans le menu déroulant **Journal**.

Les fichiers journaux doivent faire l'objet d'une attention particulière car ils sont un outil inestimable pour la détection des erreurs et la révélation des intrusions dans le système. Le journal du pare-feu personnel d'ESET contient les données suivantes :

- la date et l'heure de l'événement
- le nom de l'événement
- la source
- l'adresse réseau cible
- le protocole de communication réseau
- la règle appliquée ou le nom du ver s'il est identifié
- l'application concernée
- l'utilisateur

Une analyse approfondie de ces données peut contribuer à détecter les tentatives qui risquent de compromettre la sécurité du système. Beaucoup d'autres facteurs peuvent vous informer sur les risques potentiels de sécurité et vous aider à minimiser leur effet : trop de connexions en provenance de sites inconnus, plusieurs tentatives d'établissement de connexions, communications issues d'applications inconnues ou utilisation de numéros de ports inhabituels

4.3 Protection contre le courrier indésirable

De nos jours, le courrier non sollicité, ou indésirable, constitue l'un des plus grands problèmes liés à la communication électronique. Il représente jusqu'à 80 % de toutes les communications par messagerie électronique. La protection contre le courrier indésirable sert à vous prémunir de ce problème. En combinant plusieurs principes très efficaces, le module Blocage du courrier indésirable garantit un meilleur filtrage.

Un principe important dans la détection de spam est la possibilité de reconnaître le courrier non sollicité d'après des listes prédéfinies d'adresses fiables (liste blanche) et de courrier indésirable (liste noire). Toutes les adresses de votre client de messagerie sont automatiquement ajoutées à la liste blanche, ainsi que toutes les autres adresses que vous désignez comme sûres.

La principale méthode utilisée pour détecter du courrier indésirable est l'analyse des propriétés des messages. Les messages reçus sont analysés selon des critères de blocage du courrier indésirable de base (définitions de messages, heuristique statistique, algorithmes de reconnaissance et d'autres méthodes uniques) et l'indice qui en résulte détermine si un message est du courrier indésirable ou non.

Le filtre bayésien est également utilisé dans le filtrage du courrier indésirable. En marquant les messages comme *courrier indésirable* et *non-courrier indésirable*, l'utilisateur crée une base de données de mots utilisés dans ces catégories respectives. Plus la base de données est étoffée, plus les résultats sont précis.

Une combinaison des méthodes ci-dessus permet d'obtenir un taux élevé de détections de courrier indésirable.

ESET Smart Security prend en charge la protection contre le courrier indésirable pour Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird.

4.3.1 Auto-apprentissage du courrier indésirable

L'auto-apprentissage du courrier indésirable est lié au filtre bayésien évoqué plus haut. L'importance des différents mots varie au cours de processus d'apprentissage consistant à marquer des messages individuels comme du courrier indésirable ou non. De même, plus nombreux sont les messages classifiés (comme courrier indésirable ou non), plus précis sont les résultats obtenus avec le filtre bayésien.

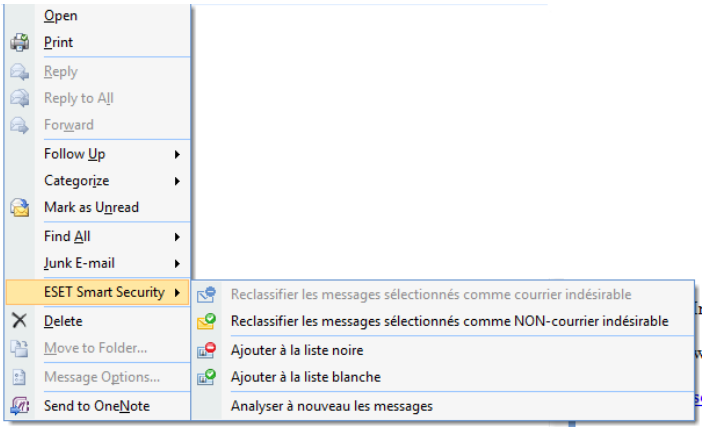
Ajoutez des adresses connues à la liste blanche pour éviter que les messages provenant de ces adresses soient classifiés comme courrier indésirable.

4.3.1.1 Ajout d'adresses à la liste blanche

Les adresses électroniques des personnes avec lesquelles vous échangez fréquemment du courrier peuvent être ajoutées à la liste des adresses « sûres » (Liste blanche). Aucun message provenant d'une adresse de la liste blanche n'est jamais classifié comme du courrier indésirable. Pour ajouter une adresse à la liste blanche, cliquez avec le bouton droit sur le message et sélectionnez « **Ajouter à la liste blanche** » dans l'option du menu contextuel « ESET Smart Security » ou sélectionnez « **Adresse fiable** » dans la barre d'outils ESS dans le haut de votre programme de messagerie. Ce processus s'applique de la même façon aux adresses de courrier indésirable. Si une adresse figure dans la liste noire, tous les messages provenant de cette adresse sont classifiés comme du courrier indésirable.

4.3.1.2 Marquage de messages comme courrier indésirable

Tout message affiché dans votre client de messagerie peut être marqué comme du courrier indésirable. Pour ce faire, utilisez le menu contextuel (clic droit) et cliquez sur **ESET Smart Security > Reclasser les messages sélectionnés comme courrier indésirable**) ou cliquez sur **Courrier indésirable** dans la barre d'outils ESET Smart Security Antispam située dans votre client de messagerie.



Les messages reclassés sont automatiquement déplacés vers le dossier SPAM, mais l'adresse de l'expéditeur n'est pas ajoutée à la liste noire. De même, les messages peuvent être marqués comme « non-courrier indésirable ». Si des messages du dossier **Junk E-mail** sont classés comme non-courrier indésirable, ils sont déplacés vers leur dossier d'origine. Lorsqu'un message est marqué comme courrier indésirable, l'adresse de l'expéditeur n'est pas automatiquement ajoutée à la liste blanche.

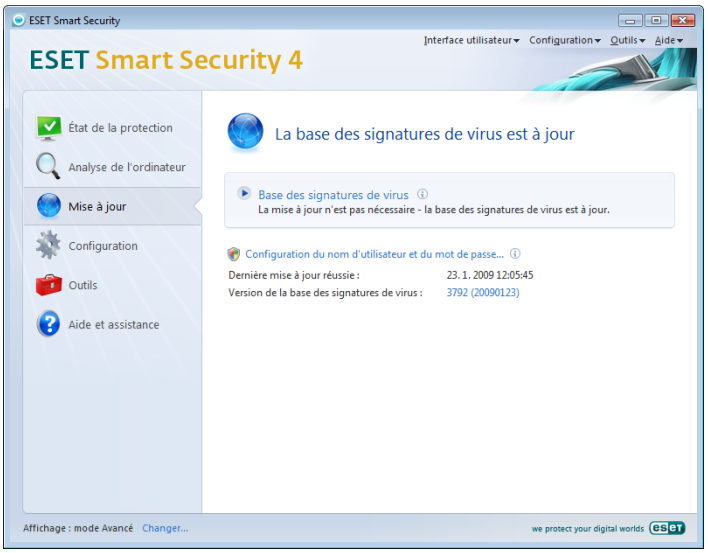
4.4 Mise à jour du programme

La mise à jour régulière du système est le fondement de base pour garantir le niveau de sécurité maximum fourni par ESET Smart Security. Le module de mise à jour assure que le programme est toujours à jour. Cela se fait de deux manières : en mettant à jour la base de signatures de virus et en mettant à jour toutes les composantes installées du système.

Les informations concernant l'état de la mise à jour actuelle s'obtiennent en cliquant sur **Mise à jour**, y compris la version actuelle de la base de signatures de virus et la nécessité ou non d'une mise à jour. En outre, l'option permettant d'activer le processus de mise à jour immédiate devient disponible (**Mettre à jour la base de signatures de virus**), ainsi que des options de base pour la configuration des mises à jour, telles que le nom d'utilisateur et mot de passe pour l'accès aux serveurs de mise à jour d'ESET.

La fenêtre d'information contient également la date et l'heure de la dernière mise à jour réussie, et le numéro de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui permet de voir toutes les signatures ajoutées dans cette mise à jour.

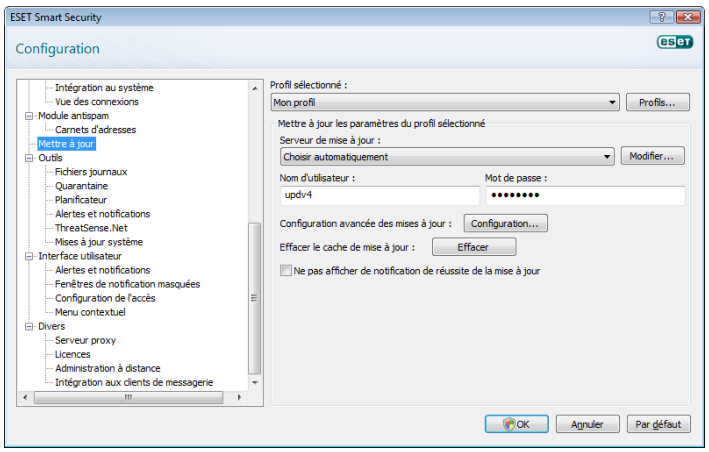
Utilisez le lien **Enregistrement** pour ouvrir le formulaire permettant d'enregistrer votre nouvelle licence auprès d'ESET afin de recevoir vos données d'authentification par courrier électronique.



REMARQUE : Le nom d'utilisateur et le mot de passe sont fournis par ESET après l'achat d'ESET Smart Security.

4.4.1 Configuration des mises à jour

La section de la configuration des mises à jour permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour et les données d'authentification donnant accès à ces serveurs. Par défaut, le champ **Serveur de mise à jour** est configuré sur **Choisir automatiquement**. Ce paramètre garantit que les fichiers de mise à jour seront téléchargés à partir du serveur ESET avec une charge de trafic minimale pour le réseau. Les options de configuration des mises à jour sont disponibles dans Options de configuration avancées (F5), sous **Mise à jour**.



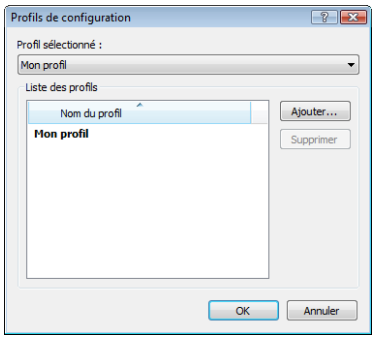
La liste des serveurs de mise à jour actuellement existants est accessible via le menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**.

L'authentification d'accès aux serveurs de mise à jour se fait par le **Nom d'utilisateur** et le **mot de passe** qui ont été générés et envoyés à l'utilisateur par ESET après l'achat de licence du produit.

4.4.1.1 Profils de mise à jour

L'utilisateur peut créer des profils de mise à jour qu'il utilise avec les tâches de mise à jour en fonction de la configuration de mise à jour. Les propriétés des connexions Internet étant variables, la création de différents profils de mise à jour devient particulièrement utile pour les utilisateurs mobiles. En modifiant la tâche de mise à jour, les utilisateurs mobiles peuvent spécifier un profil alternatif lorsque la mise à jour n'est pas possible à l'aide de la configuration spécifiée dans **Mon Profil**.

Le menu déroulant **Profil sélectionné** affiche le profil actuellement sélectionné. Par défaut, cette entrée est configurée sur l'option **Mon profil**. Pour créer un nouveau profil, cliquez sur le bouton **Profils** puis sur le bouton **Ajouter** et entrez votre **Nom de profil**. Lors de création d'un nouveau profil, il est possible de copier les paramètres d'un profil existant en le sélectionnant dans le menu déroulant **Copier les paramètres depuis le profil**.



Dans le profil, vous pouvez spécifier le serveur de mises à jour auquel le programme se connectera pour télécharger les mises à jour ; tout serveur de la liste des serveurs disponibles peut être utilisé, et un nouveau peut être ajouté. La liste des serveurs de mise à jour existants est accessible via le menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**.

4.4.1.2 Configuration avancée des mises à jour

Pour voir la section **Configuration avancée des mises à jour**, cliquez sur le bouton **Configuration...**. Les options de Configuration avancée des mises à jour comprennent la configuration du **Mode de mise à jour, Proxy HTTP, Réseau local** et **Miroir**.

4.4.1.2.1 Mode de mise à jour

L'onglet **Mode de mise à jour** contient les options concernant la mise à jour des composants du programme.

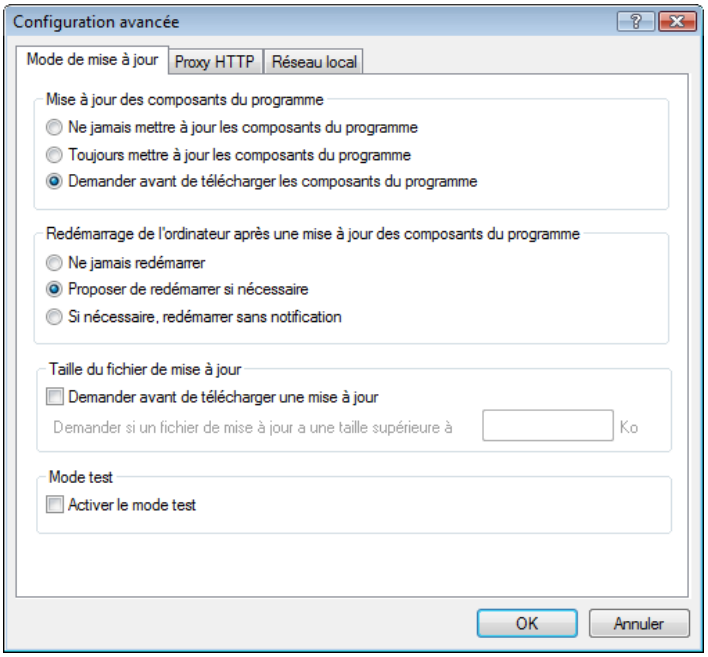
Dans la section **Mise à jour des composants du programme**, trois options sont disponibles :

- **Ne jamais mettre à jour les composants du programme**
- **Toujours mettre à jour les composants du programme**
- **Demander avant de télécharger les composants du programme**

La sélection de l'option **Ne jamais mettre à jour les composants du programme** garantit qu'après la publication par ESET d'une nouvelle mise à jour d'un composant du programme, ce dernier ne sera pas téléchargé et aucune mise à jour n'aura lieu sur le poste de travail en question. L'option **Toujours mettre à jour les composants du programme** signifie que les mises à jour des composants du programme seront effectuées chaque fois qu'une nouvelle version est disponible dans les serveurs de mise à jour d'ESET et que les composants du programme seront au même niveau que la version téléchargée.

Sélectionnez la troisième option, **Demander avant de télécharger des composants de programme** pour vous assurer que le programme demandera à l'utilisateur une confirmation avant de télécharger les mises à jour des composants du programme. Dans ce cas apparaît une boîte de dialogue contenant des informations concernant les mises à jour disponibles des composants du programme et une option pour les accepter ou les refuser. En cas de confirmation, les mises à jour sont téléchargées et les nouveaux composants du programme sont installés.

L'option par défaut de mise à jour des composants du programme est **Demander avant de télécharger les composants du programme**.



Après l'installation de mises à jour de composants du programme, il faut redémarrer le système afin d'obtenir la pleine fonctionnalité de tous les modules. La section **Redémarrer après une mise à jour des composants du programme** permet à l'utilisateur de choisir l'une des trois options suivantes :

- **Ne jamais redémarrer**
- **Proposer le redémarrage de l'ordinateur si nécessaire**
- **Si nécessaire, redémarrer l'ordinateur sans avertissement**

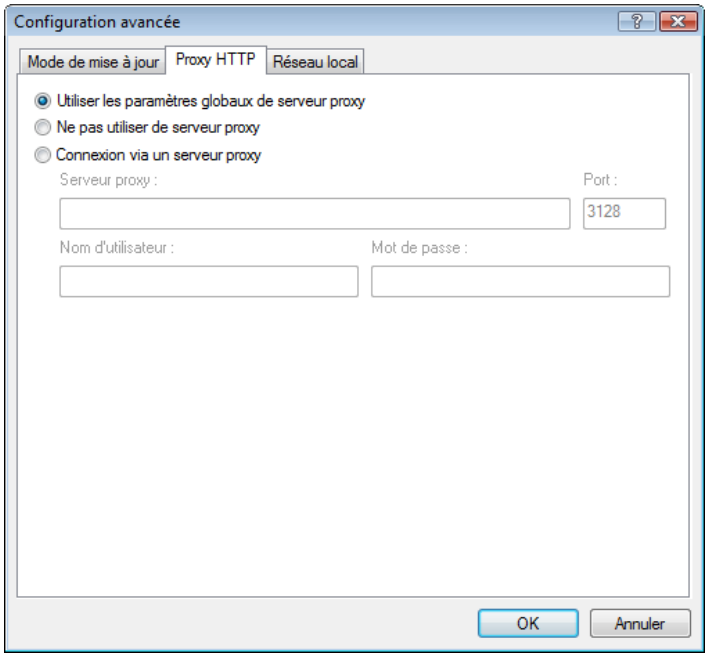
L'option par défaut de redémarrage est **Proposer le redémarrage de l'ordinateur si nécessaire**. La sélection des options les plus appropriées pour les mises à jour des composants du programme de l'onglet **Mode de mise à jour** dépend de chaque poste de travail, puisque c'est sur ces postes que les paramètres vont êtres appliqués. Notez qu'il existe des différences entre les postes de travail et les serveurs. P. ex., le redémarrage d'un serveur automatiquement après une mise à jour du programme peut causer de sérieux dommages.

4.4.1.2.2 Serveur proxy

Pour accéder aux options du serveur proxy pour un profil de mise à jour donné : Cliquez sur **Mise à jour** dans l'arborescence de configuration avancée (F5), puis cliquez sur le bouton **Configuration...** à droite de **Configuration avancée des mises à jour.** Cliquez sur l'onglet **Proxy HTTP** et sélectionnez une des trois options suivantes :

- **Utiliser les paramètres globaux de serveur proxy**
- **Ne pas utiliser de serveur proxy**
- **Connexion via un serveur proxy** (connexion définie par Propriétés de la connexion)

L'option **Utiliser les paramètres globaux de serveur proxy** utilise toutes les options de configuration du serveur proxy déjà spécifiées dans la branche **Divers > Serveur proxy** de l'arborescence de la configuration avancée.



Sélectionnez l'option **Ne pas utiliser de serveur proxy** pour définir explicitement qu'aucun serveur proxy ne sera utilisé pour la mise à jour d'ESET Smart Security.

L'option **Connexion via un serveur proxy** doit être choisie si la mise à jour d'ESET Smart Security utilise un serveur proxy et que celui-ci diffère du serveur proxy spécifié dans les paramètres globaux (**Divers > Serveur proxy**). Si c'est le cas, les paramètres doivent être spécifiés ici : l'adresse du **Serveur proxy**, le **Port** de communication et, si nécessaire, le **Nom d'utilisateur** et le **Mot de passe** du serveur proxy.

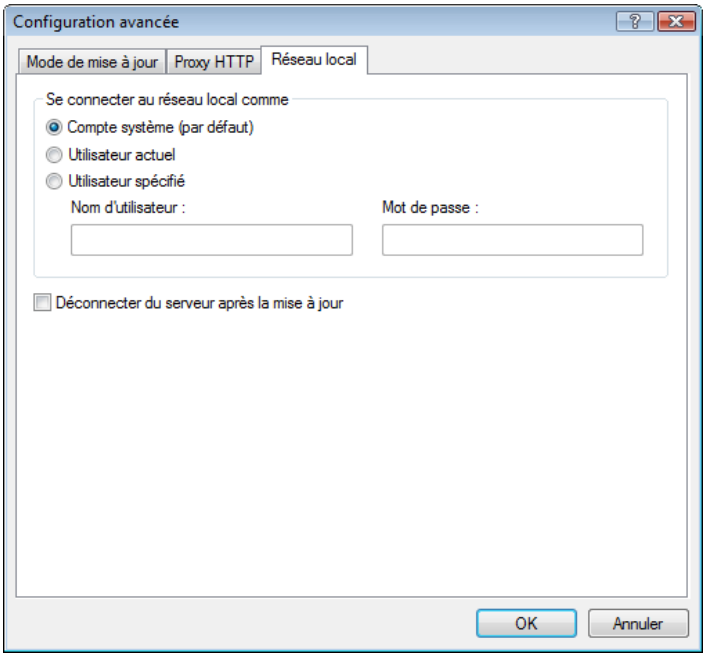
Cette option doit également être sélectionnée si les paramètres du serveur proxy ne sont pas définis globalement, mais qu'ESET Smart Security doit se connecter à un serveur proxy pour les mises à jour.

L'option par défaut pour le serveur proxy est **Utiliser les paramètres globaux de serveur proxy**.

4.4.1.2.3 Connexion au réseau local

Lors de mise à jour depuis un serveur local sous le système d'exploitation NT, une authentification est par défaut exigée pour chaque connexion réseau. Dans la plupart des cas, un compte système local n'a pas suffisamment de droits pour accéder au dossier miroir (contenant des copies des fichiers de mise à jour). Dans ce cas, entrez un nom d'utilisateur et un mot de passe dans la section de configuration des mises à jour ou spécifiez un compte existant avec lequel le programme peut accéder au serveur de mise à jour (Miroir).

Pour configurer ce compte, cliquez sur l'onglet **Réseau local**. La section **Se connecter au réseau comme** offre les options **Compte système (par défaut)**, **Utilisateur actuel** et **Utilisateur spécifié**.



Sélectionnez l'option **Compte système** pour utiliser le compte système pour l'authentification. Normalement, aucun processus d'authentification n'a lieu si des données d'authentification ne sont pas fournies dans la section principale de configuration des mises à jour.

Pour s'assurer que le programme s'autorise à utiliser le compte de l'utilisateur actuellement connecté, sélectionnez **Utilisateur actuel**. L'inconvénient de cette solution est que le programme est dans l'impossibilité de se connecter au serveur de mise à jour si aucun utilisateur n'est actuellement connecté.

Sélectionnez **Utilisateur spécifié** si vous voulez que le programme utilise un compte utilisateur spécifié pour l'authentification.

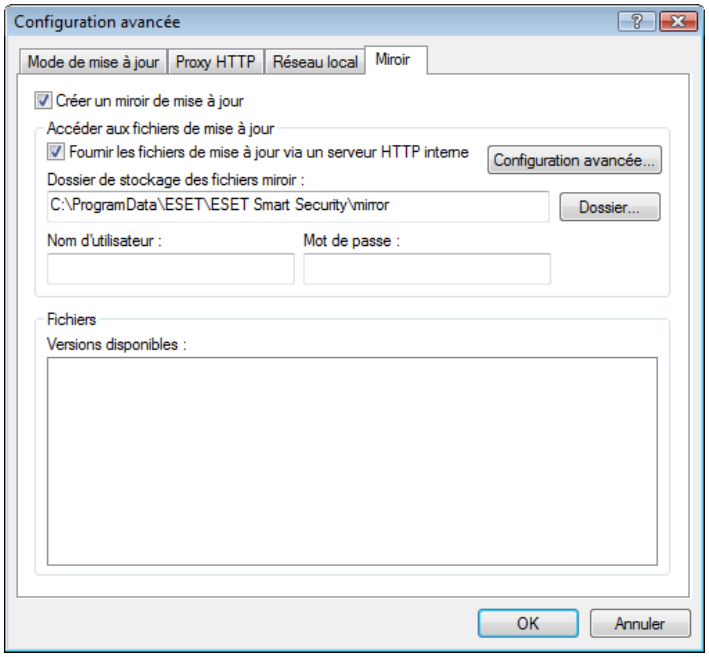
L'option par défaut pour une connexion au réseau local est **Compte système**.

Avertissement :
Si l'une des options **Utilisateur actuel** ou **Utilisateur spécifié** est activée, une erreur peut se produire en cas de changement de l'identité du programme pour l'utilisateur souhaité. C'est pour cela que nous recommandons d'entrer les données d'authentification du réseau local dans la section de configuration des mises à jour. Dans cette section de configuration des mises à jour, les données d'authentification doivent être entrées comme suit : nom_de_domaine\utilisateur (dans le cas d'un groupe de travail, entrez nom_de_groupe_de_travail\utilisateur) et le mot de passe de l'utilisateur. La mise à jour de la version HTTP du serveur local n'exige aucune authentification.

4.4.1.2.4 Création de copies de mises à jour : miroir

ESET Smart Security Business Edition permet de créer des copies des fichiers de mises à jour, qui peuvent être utilisées pour la mise à jour d'autres postes de travail du réseau. La mise à jour de postes de travail à partir d'un miroir optimise l'équilibre de la charge réseau et libère les bandes passantes des connexions Internet.

Les options de configuration du serveur miroir local sont accessibles (après l'ajout d'une clé de licence valide dans le gestionnaire de licences situé dans la section de configuration avancée d'ESET Smart Security Business Edition) dans la section **Configuration avancée des mises à jour** (pour accéder à cette section, appuyez sur F5 et cliquez sur **Mise à jour** dans l'arborescence de la configuration avancée. Cliquez sur le bouton **Configuration...** à côté de **Configuration avancée des mises à jour**, puis sélectionnez l'onglet **Miroir**).



La première étape de configuration du miroir consiste à sélectionner la case à cocher **Créer un miroir de mise à jour**. Cette option active d'autres options de configuration du miroir, telles que la manière d'accéder aux fichiers de mise à jour et le chemin des fichiers miroir.

Les méthodes d'activation du miroir sont décrites en détail dans le chapitre suivant « Différentes méthodes d'accès au miroir ». Pour le moment, notez qu'il existe deux méthodes différentes d'accès au miroir : le dossier miroir des fichiers de mise à jour peut être considéré comme un dossier réseau partagé, ou le miroir peut être considéré comme un serveur HTTP.

Le dossier dédié aux fichiers de mise à jour du miroir peut être défini dans la section **Dossier de stockage des fichiers miroir**. Cliquez sur **Dossier...** pour au dossier souhaité sur l'ordinateur local ou à un dossier réseau partagé. Si une autorisation pour le dossier spécifié est requise, les données d'authentification doivent être entrées dans les champs **Nom d'utilisateur** et **Mot de passe**. Le Nom d'utilisateur et le Mot de passe doivent être entrés sous le format *Domaine/Utilisateur* ou *Workgroup/Utilisateur*. N'oubliez pas de fournir les mots de passe correspondants.

Lors de la configuration détaillée du miroir, l'utilisateur peut également spécifier les différentes langues des copies de mises à jour à télécharger. La configuration de la langue de version est accessible dans la section **Fichiers > Versions disponibles**.

4.4.1.2.4.1 Mise à jour à partir du miroir

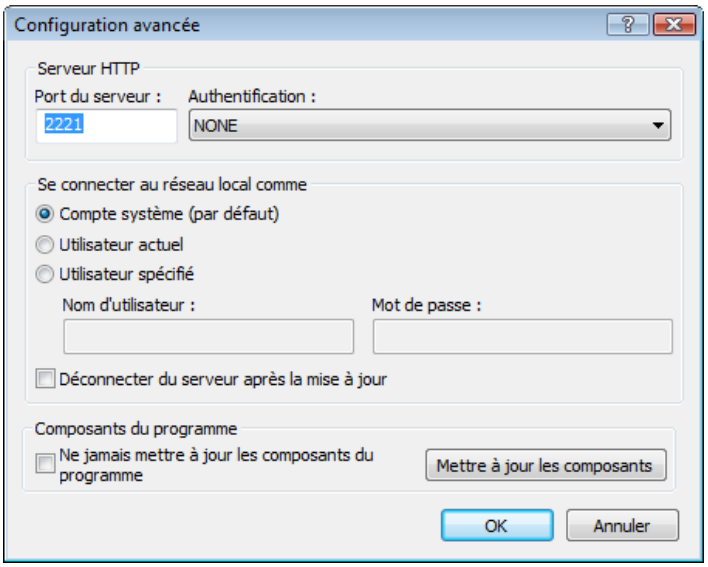
Deux méthodes différentes permettent d'accéder au miroir : le dossier miroir des fichiers de mise à jour peut être considéré comme un dossier réseau partagé, ou le miroir peut être considéré comme un serveur HTTP.

Accès au miroir au moyen de serveur HTTP interne

C'est la configuration par défaut, spécifiée dans la configuration prédéfinie du programme. Pour permettre l'accès au miroir via le serveur HTTP, choisissez **Configuration avancée des mises à jour** (onglet **Miroir**), puis activez l'option **Créer un miroir de mise à jour**.

Dans la section **Configuration avancée** de l'onglet **Miroir**, vous pouvez spécifier le **Port du serveur** d'écoute du serveur HTTP ainsi que le type d'**Authentification** utilisée par le serveur HTTP. Par défaut, le port de serveur défini est **2221**. L'option **Authentification** définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options suivantes sont disponibles : **NONE, Basic** et **NTLM**. Sélectionnez **Basic** pour utiliser le codage base64 avec l'authentification de base du nom d'utilisateur et mot de passe. L'option **NTLM** fournit un codage utilisant une méthode de codage fiable. L'utilisateur créé sur le poste de travail partageant les fichiers de mise à jour sera utilisé pour l'authentification. L'option par défaut est **NONE**. Elle autorise l'accès aux fichiers des mises à jour sans exiger d'authentification.

Avertissement :
L'accès aux fichiers des mises à jour au moyen du serveur HTTP exige que le dossier miroir doit être sur le même ordinateur que l'instance ESET Smart Security qui l'a créé.



Une fois la configuration du miroir terminée, ajoutez aux postes de travail un nouveau serveur de mise à jour dans le format **http://adresse_IP_de_votre_serveur:2221**. Pour ce faire, exécutez les étapes suivantes :

- Ouvrez **Configuration avancée d'ESET Smart Security**, puis cliquez sur la branche **Mise à jour**.
- Cliquez sur **Modifier...** à droite du menu déroulant **Serveur de mise à jour**, puis ajoutez un nouveau serveur au format suivant : http://adresse_IP_de_votre_serveur:2221
- dans la liste des serveurs de mise à jour, sélectionnez le serveur nouvellement ajouté

Accès au miroir via le partage des systèmes

Un dossier partagé doit d'abord être créé sur un lecteur local ou réseau. Lors de la création du dossier pour le miroir, il est nécessaire d'octroyer le droit d'écriture à l'utilisateur qui va sauvegarder les fichiers dans le dossier et le droit de lecture aux utilisateurs qui vont utiliser le dossier miroir pour la mise à jour d'ESET Smart Security.

Configurez ensuite l'accès au miroir dans la section **Configuration avancée des mises à jour** (onglet **Miroir**) en désactivant l'option **Fournir les fichiers de mise à jour via un serveur HTTP interne**. Cette option est activée par défaut lors de l'installation du programme.

Si le dossier partagé se trouve sur un autre ordinateur du réseau, une authentification est nécessaire pour accéder à l'autre ordinateur. Pour spécifier les données d'authentification, accédez à la configuration avancée dans ESET Smart Security (F5) et cliquez sur la branche **Mise à jour**. Cliquez sur le bouton **Configuration...**, puis cliquez sur l'onglet **Réseau local**. Ce paramètre est le même que celui de la mise à jour, comme décrit dans le chapitre « Se connecter au réseau local ».

Une fois la configuration du miroir terminée, continuez avec les stations de travail en spécifiant \\UNC\CHEMIN comme serveur de mise à jour. Voici comment réaliser cette opération :

- ouvrez la configuration avancée dans ESET Smart Security et cliquez sur **Mise à jour**
- cliquez sur **Modifier...** en regard de Serveur de mise à jour et ajoutez un nouveau serveur dans le format \\UNC\CHEMIN.
- dans la liste des serveurs de mise à jour, sélectionnez le serveur nouvellement ajouté

REMARQUE :
Pour un fonctionnement correct, le chemin du dossier miroir doit être spécifié comme un chemin UNC. Les mises à jour à partir de lecteurs mappés peuvent ne pas fonctionner.

4.4.1.2.4.2 Résolution des problèmes de miroir de mise à jour

Différents types de problèmes peuvent se produire selon la méthode d'accès au dossier miroir. Dans la plupart des cas, les problèmes lors d'une mise à jour depuis un serveur miroir sont dus à une ou plusieurs des causes suivantes : une mauvaise spécification des options du dossier miroir, des données d'authentification incorrectes pour l'accès au dossier miroir, une mauvaise configuration des postes de travail qui cherchent à télécharger des fichiers de mise à jour du miroir ou une combinaison des raisons citées précédemment. Nous donnons ici un aperçu des problèmes les plus fréquents qui peuvent se produire lors d'une mise à jour depuis le miroir :

- **ESET Smart Security signale une erreur de connexion au serveur miroir :** probablement causée par une spécification incorrecte du serveur de mise à jour (chemin réseau du dossier miroir) à partir duquel les postes de travail locaux téléchargent les mises à jour. Pour vérifier le dossier, cliquez sur le menu **Démarrer** de Windows, cliquez sur **Exécuter**, entrez le nom du dossier et cliquez sur **OK**. Le contenu du dossier doit s'afficher.
- **ESET Smart Security exige un nom d'utilisateur et un mot de passe :** probablement causée par l'entrée dans la section mise à jour de données d'authentification incorrectes (Nom d'utilisateur et Mot de passe). Le Nom d'utilisateur et le Mot de passe donnent accès au serveur de mise à jour, à partir duquel le programme se télécharge. Assurez-vous que les données d'authentification sont correctes et entrées dans le bon format. Par exemple, *Domaine/Nom d'utilisateur* ou *Workgroup/Nom d'utilisateur*, en plus des mots de passe correspondants. Si le serveur miroir est accessible à « Tous », cela ne veut pas dire que tout utilisateur est autorisé à y accéder. « Tous » ne veut pas dire tout utilisateur non autorisé, cela veut tout simplement dire que le dossier est accessible à tous les utilisateurs du domaine. Par conséquent, si le dossier est accessible à « Tous », un nom d'utilisateur du domaine et un mot de passe sont toujours nécessaires et doivent être entrés dans la configuration des mises à jour.
- **ESET Smart Security signale une erreur de connexion au serveur miroir :** le port de communication défini pour l'accès au miroir via HTTP est bloqué.

4.4.2 Comment créer des tâches de mise à jour

Les mises à jour peuvent être déclenchées manuellement en cliquant sur **Mettre à jour la base des signatures de virus** dans la fenêtre d'information affichée après avoir cliqué sur **Mise à jour** dans le menu principal.

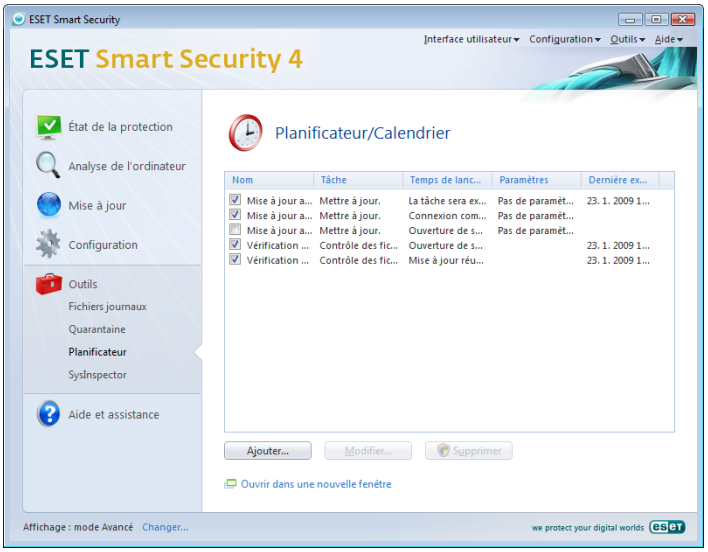
Les mises à jour peuvent également être réalisées par des tâches planifiées : pour configurer une tâche planifiée, cliquez sur **Outils > Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET Smart Security :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**

Chacune des tâches de mise à jour susmentionnées peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, consulter le chapitre « Planificateur ».

4.5 Planificateur

Le planificateur est disponible lorsque l'option Mode Avancé est activée dans ESET Smart Security. Le **Planificateur** se trouve dans le menu principale d'ESET Smart Security sous **Outils**. Il contient un résumé de toutes les tâches planifiées avec leurs propriétés de configuration telles que la date prédéfinie, l'heure et le profil d'analyse utilisé.



Par défaut, les tâches planifiées suivantes s'affichent dans le **Planificateur** :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification automatique des fichiers de démarrage**
- **Vérification automatique des fichiers de démarrage après la mise à jour réussie de la base des signatures de virus**

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche, puis cliquez sur **Modifier...**, ou sélectionnez la tâche à modifier, puis cliquez sur le bouton **Modifier...**.

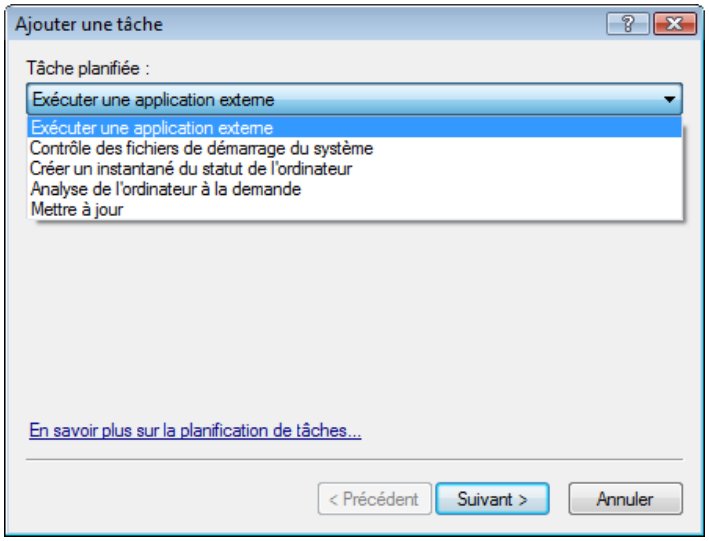
4.5.1 Pourquoi planifier des tâches

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés de ces tâches comprennent des informations telles que la date et l'heure ainsi que des profils spécifiques à utiliser pendant l'exécution de ces tâches.

4.5.2 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le Planificateur, cliquez sur le bouton **Ajouter...** ou cliquez avec le bouton droit et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe**
- **Maintenance des journaux**
- **Contrôle des fichiers de démarrage du système**
- **Analyse d'ordinateur à la demande**
- **Mise à jour**



Puisque les tâches **Analyse de l'ordinateur à la demande** et **Mise à jour** sont les tâches planifiées les plus utilisées, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mise à jour**. Cliquez sur **Suivant**, puis entrez le nom de la tâche dans le champ **Nom de la tâche**. Sélectionnez la fréquence de la tâche. Les options suivantes sont disponibles : **Une fois, Plusieurs fois, Quotidiennement**, **Chaque semaine** et **Déclenchée par un événement**. Selon la fréquence sélectionnée, vous serez invité à choisir différents paramètres de mise à jour. On peut définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **Attendre le prochain moment planifié**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini immédiatement à l'aide de la zone de liste déroulante **Intervalle de la tâche**).

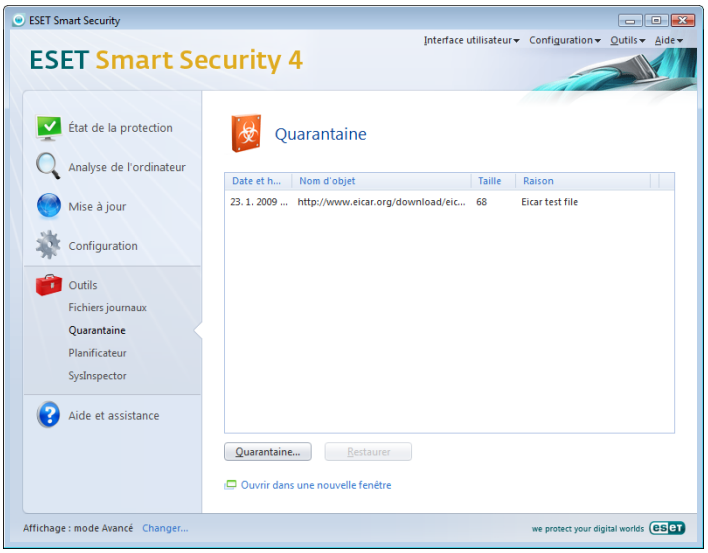
La prochaine étape affiche un résumé concernant la tâche planifiée courante ; l'option **Exécuter la tâche avec des paramètres spécifiques** doit être automatiquement activée. Cliquez sur le bouton **Terminer**.

Une boîte de dialogue s'ouvre pour permettre de choisir le profil à utiliser avec la tâche planifiée. Vous pouvez spécifier ici un profil primaire et un secondaire qui sera utilisé si la tâche ne peut s'exécuter en utilisant le profil primaire. Confirmez en cliquant sur **OK** dans la fenêtre **Profils de mise à jour**. La nouvelle tâche planifiée sera ajoutée à la liste des tâches planifiées.

4.6 Quarantaine

La principale fonction de la quarantaine est le stockage en toute sécurité des fichiers infectés. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont erronément détectés par ESET Smart Security.

L'utilisateur peut placer en quarantaine n'importe quel fichier. C'est conseillé si un fichier se comporte de façon suspecte mais n'a pas été détecté par l'analyseur antivirus. Les fichiers de la quarantaine peuvent être soumis pour analyse au laboratoire d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans une table qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (**ajouté par l'utilisateur...**) et le nombre de menaces (ex. s'il s'agit d'une archive contenant plusieurs infiltrations).

4.6.1 Mise de fichiers en quarantaine

Le programme déplace automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine...**. Dans ce cas, le fichier d'origine n'est pas supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin ; cliquez avec le bouton droit dans la fenêtre de quarantaine, puis sélectionnez **Ajouter...**.

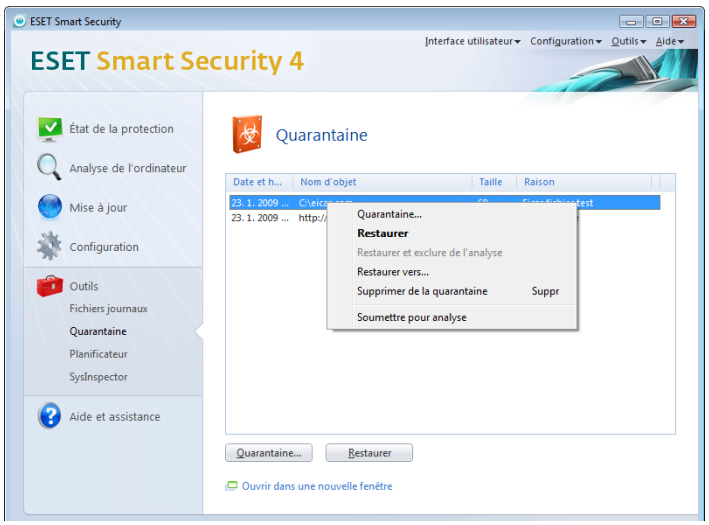
4.6.2 Restaurer depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Pour ce faire, utilisez la fonctionnalité **Restaurer** du menu contextuel après avoir cliqué avec le bouton droit sur un fichier dans la fenêtre de quarantaine. Le menu contextuel offre également l'option **Restaurer vers**, qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

REMARQUE :
Si le programme place en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au service client d'ESET.

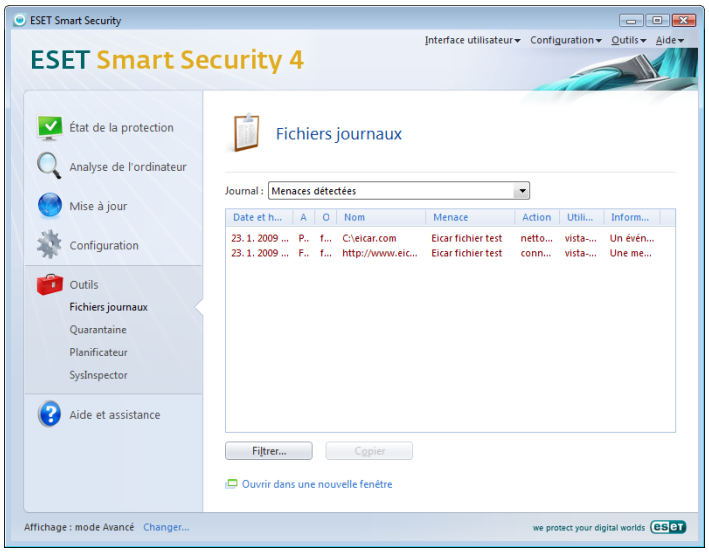
4.6.3 Soumission de fichiers de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré infecté par erreur (ex. par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire d'ESET. Pour soumettre un fichier de la quarantaine, cliquez dessus avec le bouton droit, puis, dans le menu contextuel, sélectionnez **Soumettre pour analyse**.



4.7 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres actifs de verbosité. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET Smart Security ainsi que d'archiver les journaux.



Les fichiers journaux sont accessibles à partir de la fenêtre principale d'ESET Smart Security en cliquant sur **Outils > Fichiers journaux**. Sélectionnez le type de journal souhaité à l'aide du menu déroulant **Journal** en haut de la fenêtre. Les journaux suivants sont disponibles :

1. **Menaces détectées :** cette option permet de consulter toutes les informations concernant les événements liés à la détection d'infiltrations.

2. **Événements :** cette option permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par ESET Smart Security sont enregistrées dans les journaux des événements.

3. **Analyse de l'ordinateur à la demande :** les résultats de toutes les analyses effectuées sont affichés dans cette fenêtre. Double-cliquez sur n'importe quelle entrée pour afficher les détails de l'analyse à la demande correspondante.

4. **Journal du pare-feu personnel ESET :** contient des enregistrements de tous les faits détectés par le pare-feu personnel. L'analyse du journal du pare-feu peut permettre de détecter à temps des tentatives d'intrusion sur le système et ainsi permettre de bloquer les accès non autorisés.

L'information affichée dans chaque section peut être directement copiée dans le Presse-papiers, il suffit de sélectionner l'entrée souhaitée puis de cliquer sur **Copier**. Vous pouvez sélectionner plusieurs entrées à l'aide des touches Ctrl et Maj.

4.7.1 Maintenance des journaux

La configuration de la consignation d'ESET Smart Security est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration > Accéder à l'arborescence de configuration avancée complète... > Outils > Fichiers journaux**. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

- **Supprimer automatiquement les entrées :** les entrées de journal vieilles de plus que le nombre de jours spécifiés seront automatiquement supprimées.

- **Optimiser automatiquement les fichiers journaux :** permet la défragmentation automatique des fichiers journaux si le pourcentage d'enregistrements inutilisés a été dépassé.

- **Verbosité minimale des journaux :** spécifie le niveau minimum de verbosité des journaux. Options disponibles :

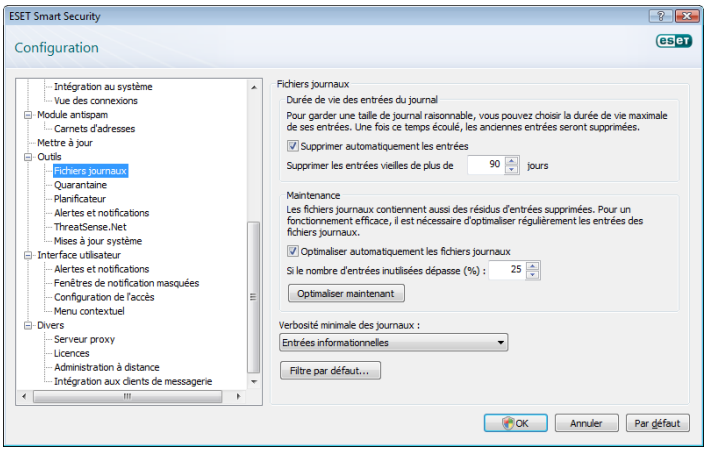
  – **Erreurs critiques :** consigne uniquement les erreurs critiques (erreurs produites au lancement de la Protection antivirus, Pare-feu personnel, etc.)

  – **Erreurs :** seuls les messages « Erreur de téléchargement de fichier » et les erreurs critiques sont consignés.

  – **Avertissements :** enregistre toutes les erreurs critiques et les messages d'avertissement.

  – **Entrées informatives :** consigne tous les messages d'information, y compris les mises à jour réussies et toutes les entrées citées ci-dessus.

  – **Entrées de diagnostic :** consigne toutes les informations nécessaires pour un réglage détaillé du programme ainsi que tous les enregistrements cités ci-dessus.



4.8 Interface utilisateur

La configuration de l'interface utilisateur d'ESET Smart Security peut être modifiée de manière à pouvoir ajuster l'environnement de travail selon vos besoins. Ces options de configuration sont accessibles dans la branche **Interface utilisateur** de l'arborescence de la configuration avancée ESET Smart Security.

La section **Éléments de l'interface utilisateur** permet de basculer vers le mode avancé. Le mode Avancé affiche des paramètres détaillés et des commandes supplémentaires pour ESET Smart Security.

L'option **Interface utilisateur graphique** doit être désactivée si les éléments graphiques ralentissent les performances de l'ordinateur ou causent d'autres problèmes. L'interface utilisateur graphique devra peut-être aussi être désactivée pour les utilisateurs malvoyants, car elle peut créer un conflit avec les applications spéciales utilisées pour la lecture de textes affichés à l'écran.

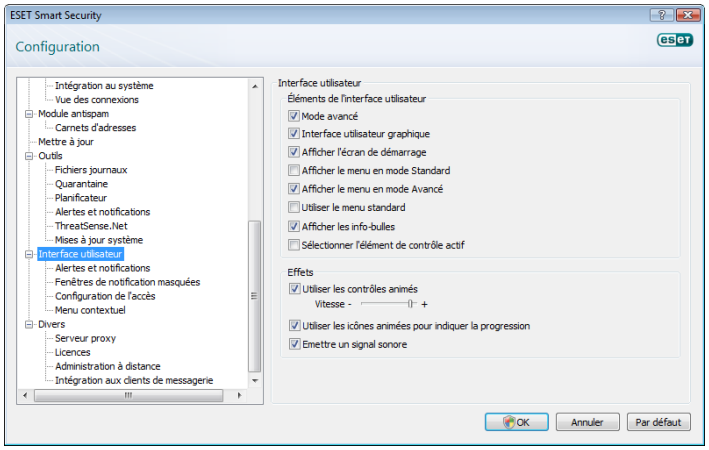
Pour désactiver l'écran de démarrage d'ESET Smart Security, désactivez l'option **Afficher l'écran de démarrage**.

En haut de la fenêtre principale d'ESET Smart Security, se trouve un menu standard qui peut être activé ou désactivé en fonction de l'option **Utiliser le menu standard**.

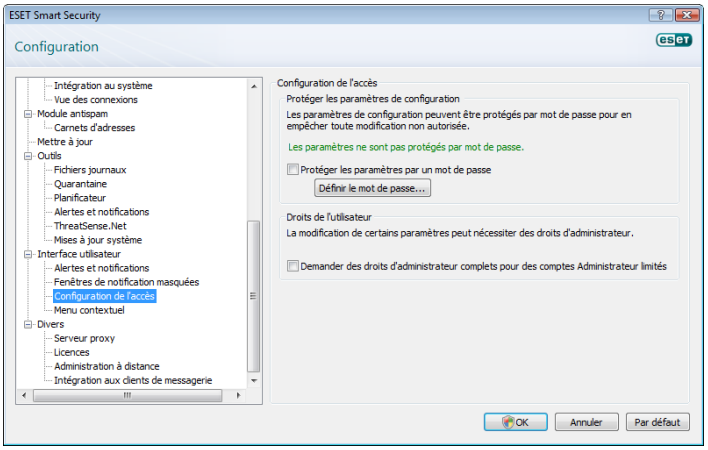
Si l'option **Afficher les info-bulles** est activée, une petite description de toute option sera affichée si le curseur est placé au-dessus de l'option. L'option **Sélectionner l'élément de contrôle actif** oblige le système à mettre en surbrillance tout élément qui se trouve sous la zone active du curseur de la souris. L'élément en surbrillance sera activé d'un clic de souris.

Pour augmenter ou diminuer la vitesse des effets animés, sélectionnez l'option **Contrôles animés** et déplacez le curseur **Vitesse** vers la gauche ou la droite.

Pour permettre l'utilisation d'icônes animées affichant la progression de diverses opérations, sélectionnez la case à cocher **Icônes animées...**. Si vous souhaitez que le programme émette un avertissement lorsqu'un événement important se produit, sélectionnez l'option **Signal sonore**.



Les fonctions de l'**Interface utilisateur** comprennent aussi une option de protection par mot de passe des paramètres de configuration d'ESET Smart Security. Cette option se trouve dans le sous-menu **Protection des paramètres**, sous **Interface utilisateur**. Il est essentiel que le programme soit correctement configuré pour garantir le maximum de sécurité au système. Tout changement non autorisé peut faire perdre des données importantes. Pour définir un mot de passe pour protéger les paramètres de la configuration, cliquez sur **Entrer un mot de passe...**.



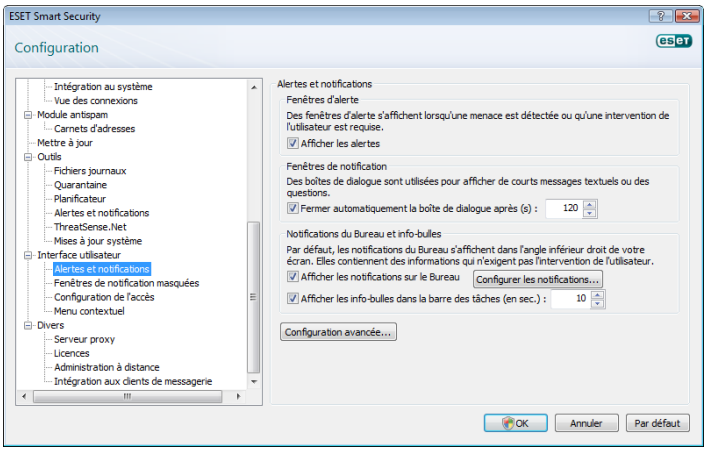
4.8.1 Alertes et notifications

La section **Configurer les alertes et notifications** sous **Interface utilisateur** permet de configurer le mode de traitement des alertes de menace et des notifications système par ESET Smart Security 4.

La première option est **Afficher les alertes**. Lorsqu'elle est désactivée, aucune fenêtre d'alerte ne s'affiche, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons à la majorité des utilisateurs de garder l'option par défaut (activée).

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez l'option **Fermer automatiquement la boîte de dialogue après (s)**. Si les fenêtres d'alerte ne sont pas fermées manuellement par l'utilisateur, elles le sont automatiquement une fois que le laps de temps spécifié est écoulé.

Les notifications sur le bureau et les info-bulles sont des moyens d'information uniquement et n'exigent aucune interaction avec l'utilisateur. Elles s'affichent dans la barre d'état système dans l'angle inférieur droit de l'écran. Pour activer l'affichage des notifications sur le bureau, sélectionnez l'option **Afficher les notifications sur le bureau**. D'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) peuvent être modifiées en cliquant sur le bouton **Configurer les notifications...**. Pour prévisualiser le comportement des notifications, cliquez sur le bouton **Aperçu**. Pour configurer la durée d'affichage des info-bulles, utilisez l'option **Afficher les info-bulles dans la barre des tâches (en sec.)**.



Cliquez sur **Configuration avancée...** pour accéder aux options de configuration supplémentaires **Alertes et notifications** dont **Afficher uniquement les notifications exigeant une intervention de l'utilisateur**. Cette option permet d'activer/désactiver l'affichage des alertes et des notifications qui n'exigent aucune intervention de l'utilisateur. Sélectionnez N'afficher que les notifications nécessitant une interaction de l'utilisateur lors de l'exécution d'applications en mode plein écran pour supprimer toutes les notifications non interactives. Le menu déroulant Verbosité minimale des événements à afficher permet de sélectionner le niveau de gravité de départ des alertes et notifications à afficher.

La dernière fonctionnalité de cette section est la spécification d'adresses de notification dans un environnement multi-utilisateurs. Le champ **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** permet de définir quel utilisateur recevra les notifications importantes d'ESET Smart Security 4. Normalement, il doit s'agir d'un administrateur système ou réseau. Cette option est particulièrement utile pour les serveurs de terminaux, pour autant que toutes les notifications système soient envoyées à l'administrateur.

4.9 ThreatSense.Net

Le système d'avertissement anticipé ThreatSense.Net est un outil qui maintient ESET immédiatement et continuellement informée des nouvelles infiltrations. Le système d'alerte anticipé bidirectionnel n'a qu'un seul objectif : améliorer la protections que nous vous offrons. Le meilleur moyen d'être sûr de voir les nouvelles menaces dès qu'elles apparaissent est d'être en contact permanent avec le plus grand nombre de nos clients et de les utiliser comme des éclaireurs de menaces. Deux options sont possibles :

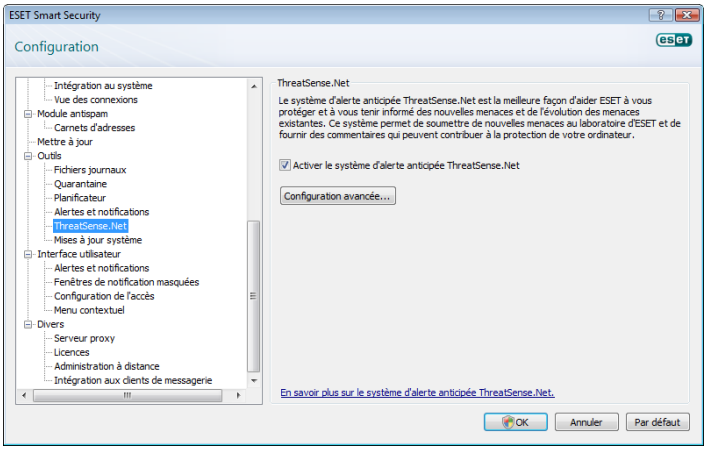
1. Vous pouvez décider de ne pas activer le système d'avertissement anticipé ThreatSense.Net. Vous ne perdez rien de la fonctionnalité du logiciel et vous aurez toujours la meilleure protection que nous offrons.

2. Vous pouvez configurer le système d'avertissement anticipé pour envoyer des informations anonymes concernant de nouvelles menaces où le code menaçant se trouve dans un seul fichier. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET améliore ses capacités à détecter les menaces. Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations concernant de nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin du fichier, le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de celui-ci. Certaines de ces informations peuvent comprendre des données particulières à votre ordinateur, telles que le chemin de dossier, etc.

Bien qu'il y ait une probabilité de divulgation de certaines informations relatives à vous ou à votre ordinateur, ici dans le laboratoire d'ESET, ces informations ne seront pas utilisées à AUCUNE autre fin autre que celle de nous aider à répondre immédiatement aux menaces.

Par défaut, ESET Smart Security est configuré pour demander avant de soumettre les fichiers suspects pour une analyse détaillée au laboratoire d'ESET. Notez que les fichiers avec les extensions .doc ou .xls sont toujours exclus, même si une menace a été détectée dans de tels fichiers. Vous pouvez ajouter d'autres extensions à la liste d'exclusion, dont vous ou votre organisation souhaitez éviter l'envoi.

La configuration de ThreatSense.Net est accessible depuis la configuration avancée complète, dans **Outils > ThreatSense.Net**. Sélectionnez la case à cocher **Activer le système d'alerte anticipé ThreatSense.Net**. Cela vous permettra de l'activer. Ensuite, cliquez sur le bouton **Configuration avancée...**.

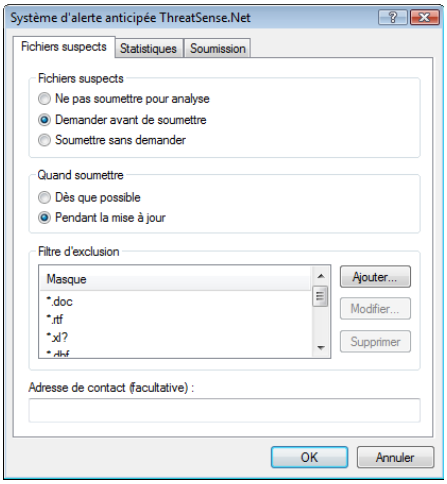


4.9.1 Fichiers suspects

L'onglet **Fichiers suspects** permet de configurer la manière dont les menaces sont soumises pour analyse au laboratoire d'ESET.

Si vous avez trouvé un fichier suspect, vous pouvez le soumettre pour analyse à notre laboratoire. S'il s'avère que ces fichiers sont des applications malveillantes, ils seront ajoutés à la prochaine mise à jour de la base des signatures de virus.

La soumission de fichiers peut être configurée pour qu'elle soit automatique sans poser de question. Si cette option est sélectionnée, les fichiers suspects seront envoyés en arrière-plan. Si vous voulez connaître les fichiers envoyés pour analyse et confirmer leur soumission, sélectionnez l'option **Demander avant de soumettre**.



Si vous ne voulez soumettre aucun fichiers, sélectionnez l'option **Ne pas soumettre pour analyse**. Notez que la soumission des fichiers pour analyse n'affecte pas les informations statistiques de soumission à ESET. Les informations statistiques sont configurées dans une section qui leur est propre et qui est décrite dans le chapitre suivant.

Quand soumettre
Les fichiers suspects seront envoyés pour analyse aux laboratoires d'ESET dès que possible. Cela est recommandé lorsqu'une connexion Internet permanente est disponible et que les fichiers suspects peuvent être livrés très rapidement. L'autre option est de livrer les fichiers suspects **Pendant la mise à jour**. Si cette option est activée, les fichiers suspects sont collectés et téléchargés, pendant la mise à jour, sur les serveurs du système d'alerte anticipée.

Filtre d'exclusion
Tous les fichiers ne sont pas soumis pour analyse. Le filtre d'exclusion permet d'exclure certains fichiers/dossiers de la soumission. Par exemple, il est utile d'exclure des fichiers qui peuvent comporter des informations confidentielles potentielles, tels que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (Microsoft Office, OpenOffice). La liste des fichiers exclus peut être étendue à votre gré.

Adresse e-mail de contact
L'adresse de contact envoyée avec les fichiers suspects à ESET et peut être utilisée pour vous contacter si des informations complémentaires sur les fichiers soumis sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

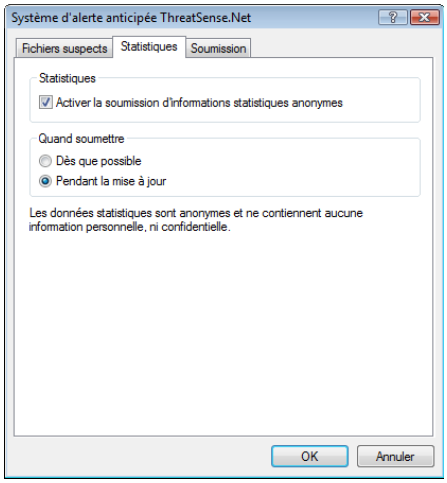
4.9.2 Statistiques

Le système d'avertissement anticipé ThreatSense.Net collecte sur votre ordinateur des informations anonymes concernant de nouvelles menaces détectées. Ces informations peuvent inclure le nom de l'infiltration, la date et l'heure de détection, la version d'ESET Smart Security ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont normalement fournies au serveur d'ESET une ou deux fois par jour.

Voici un exemple d'informations statistiques envoyées :

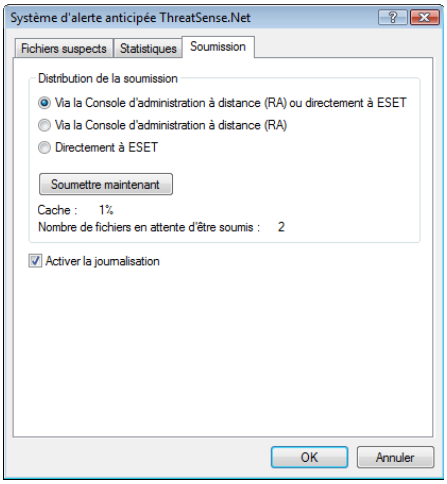
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Quand soumettre
Dans la section **Quand soumettre**, vous pouvez définir le moment de l'envoi des informations statistiques. Si vous choisissez d'envoyer **Dès que possible**, les informations statistiques seront envoyées immédiatement après leur création. Ce choix convient si une connexion Internet est disponible en permanence. Si l'option **Pendant la mise à jour** est sélectionnée, les informations statistiques seront conservées puis envoyées simultanément pendant la prochaine mise à jour.



4.9.3 Soumission

Cette section permet de choisir si les fichiers et les informations statistiques seront soumis à l'aide de la console d'administration à distance ou directement à ESET. Pour s'assurer que les fichiers suspects et les informations statistiques seront livrés à ESET, sélectionnez l'option **Via la Console d'administration à distance (RA) ou directement à ESET**. Si cette option est sélectionnée, les fichiers et les informations statistiques seront soumis à l'aide de tout moyen disponible. La soumission de fichiers suspects au moyen de l'Administrateur Distant livre les fichiers et les informations statistiques au serveur d'administration à distance, qui assure leur acheminement vers le laboratoire d'ESET. Si l'option **Directement à ESET** est sélectionnée, tous les fichiers suspects et les informations statistiques seront livrés directement par le programme au laboratoire d'ESET.



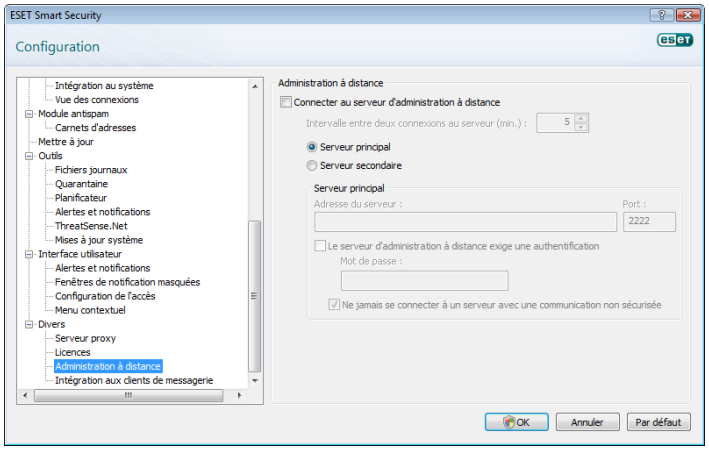
Si des fichiers sont en attente de soumission, le bouton **Soumettre maintenant** sera activé dans cette fenêtre de configuration. Cliquez sur ce bouton pour soumettre immédiatement les fichiers et les informations statistiques.

Sélectionnez la case à cocher **Activer la journalisation** pour consigner la soumission des fichiers et des informations statistiques. Dans ce cas, après chaque soumission de fichier suspect ou d'informations statistiques, une entrée est créée dans le journal des événements.

4.10 Administration à distance

L'administration à distance est un outil très puissant pour maintenir une politique de sécurité et avoir une vue d'ensemble de la gestion de la sécurité globale du réseau. Elle est particulièrement utile pour les grands réseaux. L'administration à distance ne fait pas qu'augmenter le niveau de sécurité, mais offre une administration d'utilisation simple d'ESET Smart Security sur les postes de travail client.

Les options de configuration de l'administration à distance sont accessibles à partir de la fenêtre principale d'ESET Smart Security. Cliquez sur **Configuration > Accéder à l'arborescence de configuration avancée complète... > Divers > Administration à distance**.



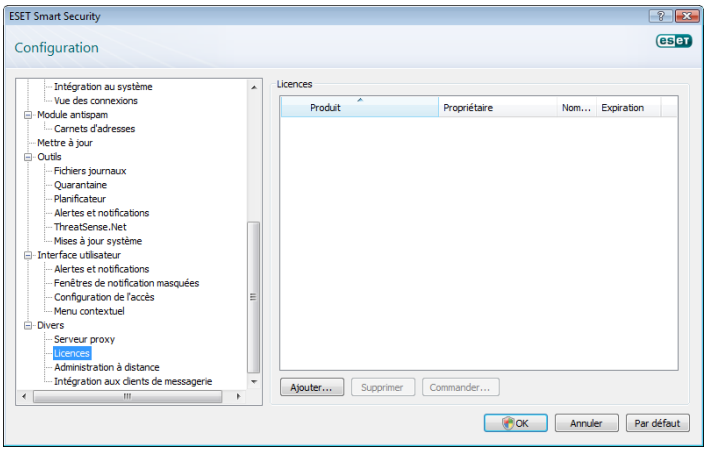
La fenêtre de configuration permet d'activer le mode Administration à distance en sélectionnant d'abord la case à cocher **Connecter au Serveur d'Administration à Distance**. Vous pouvez alors accéder aux autres options décrites ci-dessous :

- **Adresse du serveur :** adresse réseau du serveur d'administration à distance.
- **Port :** ce champ contient le port du serveur prédéfini utilisé pour la connexion. Il est recommandé de laisser le paramètre de port prédéfini sur 2222.
- **Intervalle entre deux connexions au serveur (min.) :** spécifie la fréquence à laquelle ESET Smart Security se connecte au serveur ERA pour envoyer les données. Autrement dit, les informations sont envoyées aux intervalles définis ici. Si la valeur est 0, les informations sont envoyées toutes les 5 secondes.
- **Le serveur d'administration à distance exige une authentification :** permet d'entrer un mot de passe pour la connexion au serveur d'administration à distance.

Cliquez sur **OK** pour confirmer les modifications et appliquer les paramètres. ESET Smart Security utilisera ces paramètres pour se connecter au serveur distant.

4.11 Licence

La branche **Licence** permet de gérer les clés de licence ESET Smart Security et d'autres produits ESET tels que l'Administrateur Distant ESET, ESET NOD32 pour Microsoft Exchange etc. Après l'achat, les clés de licence sont envoyées avec le Nom d'utilisateur et le Mot de passe. Pour **Ajouter/Supprimer** une clé de licence, cliquez sur le bouton correspondant dans la fenêtre du gestionnaire de licences. Le gestionnaire de licences est accessible à partir de l'arborescence de configuration avancée sous **Divers > Licences.**



Une clé de licence est un fichier texte contenant des informations concernant le produit acheté : son propriétaire, le nombre de licences et la date d'expiration.

La fenêtre du gestionnaire de licences permet à l'utilisateur de charger et de voir le contenu de la clé de licence à l'aide du bouton **Ajouter...** ; les informations contenues seront affichées dans la fenêtre du gestionnaire. Pour supprimer des clés de licence de la liste, cliquez sur **Supprimer**.

Si une clé de licence est expirée et que vous êtes intéressé par le renouvellement de l'achat, cliquez sur le bouton **Commander...** ; vous serez redirigé vers le site Web du magasin en ligne.

5. Utilisateur chevronné

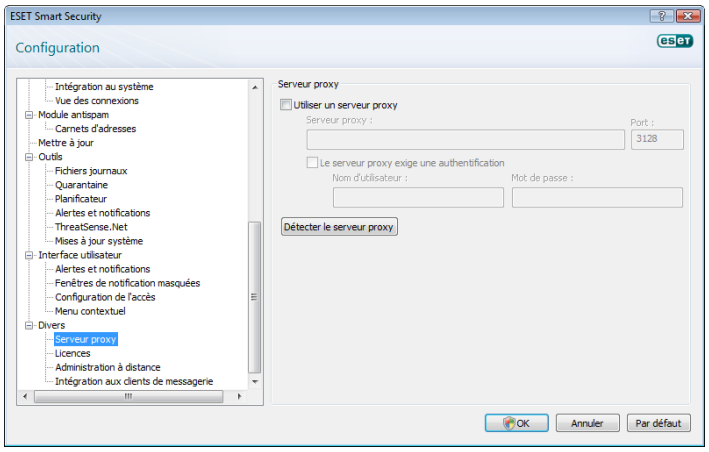
Ce chapitre décrit des fonctions d'ESET Smart Security qui peuvent être utiles aux utilisateurs chevronnés. Les options de configuration de ces fonctions sont accessibles uniquement en mode avancé. Pour basculer vers le mode avancé, cliquez sur **Basculer en mode Avancé** en bas à gauche de la fenêtre principale du programme ou appuyez sur CTRL + M sur le clavier.

5.1 Configuration du serveur proxy

Dans ESET Smart Security, la configuration du serveur proxy est disponible en deux endroits différents de l'arborescence de la configuration avancée.

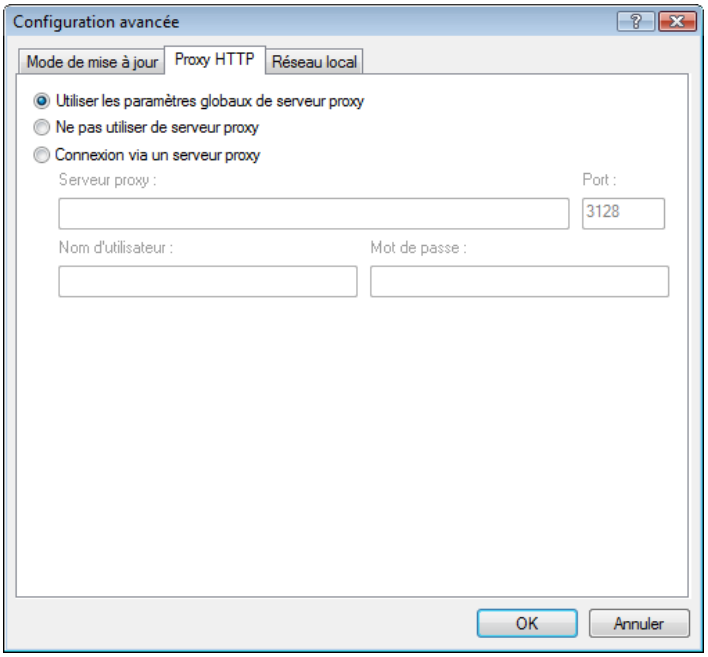
Premièrement, les paramètres de serveur proxy peuvent être configurés sous **Divers > Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour tout ESET Smart Security. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, sélectionnez la case à cocher **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy** ainsi que le numéro de **Port** de ce serveur proxy.



Si la communication avec le serveur proxy exige une authentification, sélectionnez la case à cocher **Le serveur proxy exige une authentification** et entrez un **Nom d'utilisateur** et un **Mot de passe** valides dans les champs correspondants. Cliquez sur le bouton **Détecter le serveur proxy** pour détecter et insérer automatiquement les paramètres du serveur proxy. Les paramètres spécifiés dans Internet Explorer sont alors copiés. Notez que cette fonction ne récupère pas les données d'authentification (Nom d'utilisateur et Mot de passe), qui doivent être fournies par l'utilisateur.

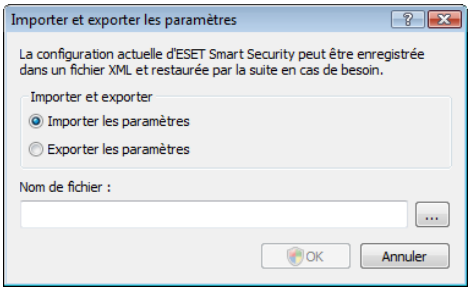
Les paramètres de serveur proxy peuvent aussi être définis dans la branche **Configuration avancée des mises à jour** de l'arborescence de la configuration avancée. Cette configuration s'applique au profil de mise à jour concerné et est recommandée pour les ordinateurs portables, qui reçoivent souvent les mises à jour des signatures de virus de différents endroits. Pour plus d'informations sur cette configuration, voir la Section 4.4, « Mise à jour du système ».



5.2 Importer/exporter des paramètres

L'exportation et l'importation de la configuration ESET Smart Security actuelle sont disponibles en mode Avancé sous **Configuration**.

Les deux fonctions utilisent le format de fichier .xml. Elles sont utiles si vous devez sauvegarder la configuration ESET Smart Security actuelle pour la réutiliser plus tard (quelle que soit la raison). La fonction d'exportation sera également appréciée par ceux qui souhaitent utiliser leur configuration ESET Smart Security favorite sur plusieurs systèmes : il leur suffit d'importer leur fichier .xml.



5.2.1 Exporter les paramètres

L'exportation de la configuration est très facile. Si vous souhaitez enregistrer la configuration ESET Smart Security actuelle, cliquez sur **Configuration > Importer et exporter les paramètres...**. Sélectionnez l'option **Exporter les paramètres** et entrez le nom du fichier de configuration. Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur où enregistrer le fichier de configuration.

5.2.2 Importer des paramètres

La procédure d'importation d'une configuration est très semblable. De nouveau, sélectionnez **Importer et exporter les paramètres**, puis sélectionnez l'option **Importer les paramètres**. Cliquez sur le bouton **...** et localisez le fichier de configuration à importer.

5.3 Ligne de commande

Il est possible de lancer le module antivirus ESET Smart Security par l'intermédiaire de la ligne de commande ; manuellement (avec la commande « ecls ») ou au moyen d'un fichier de traitement par lots (« bat »).

Les paramètres et commutateurs suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande à partir de la ligne de commande :

Options générales :

– help	afficher l'aide et quitter
– version	afficher les informations de la version et quitter
– base dir = FOLDER	charger les modules à partir du DOSSIER
– quar dir = FOLDER	DOSSIER quarantaine
– aind	afficher l'indicateur d'activité

Cibles :

– files	analyser les fichiers (valeur par défaut)
– no files	ne pas analyser les fichiers
– boots	analyser les secteurs d'amorçage (valeur par défaut)
– no boots	ne pas analyser les secteurs d'amorçage
– arch	analyser les archives (valeur par défaut)
– no arch	ne pas analyser les archives
– max archive level = LEVEL	NIVEAU d'imbrication maximum d'archives
– scan timeout = LIMIT	analyser les archives pendant un maximum de LIMITE secondes. Si la durée d'analyse atteint cette limite, l'analyse de l'archive est arrêtée et se poursuit sur le fichier suivant
– max arch size=SIZE	analyser uniquement la TAILLE des premiers octets des archives (valeur par défaut 0 = illimité)
– mail	analyser les fichiers de courriers électroniques
– no mail	ne pas analyser les fichiers de courriers électroniques
– sfx	analyser les archives auto-extractibles
– no sfx	ne pas analyser les archives auto-extractibles
– rtp	analyser les fichiers exécutables compressés
– no rtp	ne pas analyser les fichiers exécutables compressés
– exclude = FOLDER	exclure le DOSSIER de l'analyse
– subdir	analyser les sous-dossiers (valeur par défaut)
– no subdir	ne pas analyser les sous-dossiers
– max subdir level = LEVEL	NIVEAU d'imbrication maximum de sous-dossiers (valeur par défaut 0 = illimité)
– symlink	suivre les liens symboliques (valeur par défaut)
– no symlink	ignorer les liens symboliques
– ext remove = EXTENSIONS	
– ext exclude = EXTENSIONS	exclure de l'analyse les EXTENSIONS délimitées par deux-points

Méthodes :

– adware	rechercher les logiciels espions/publicitaires/à risque
– no adware	ne pas rechercher les logiciels espions/publicitaires/à risque
– unsafe	rechercher les applications potentiellement dangereuses
– no unsafe	ne pas rechercher les applications potentiellement dangereuses
– unwanted	rechercher les applications potentiellement indésirables
– no unwanted	ne pas rechercher les applications potentiellement indésirables
– pattern	utiliser les signatures
– no pattern	ne pas utiliser les signatures
– heur	activer l'heuristique
– no heur	désactiver l'heuristique
– adv heur	activer l'heuristique avancée
– no adv heur	désactiver l'heuristique avancée

Nettoyage :

– action = ACTION	appliquer l'ACTION aux objets infectés. Actions disponibles : none, clean, prompt (aucune, nettoyer, demander)
– quarantine	copier les fichiers infectés en quarantaine (complète ACTION)
– no quarantine	ne pas copier les fichiers infectés en quarantaine

Journaux :

– log file=FILE FICHIER	consigner les résultats dans le
– log rewrite	écraser le fichier de résultats (valeur par défaut - ajouter)
– log all	consigner également les fichiers sains
– no log all	ne pas consigner les fichiers nettoyés (valeur par défaut)

Différents codes sortie d'analyse :

0 – aucune menace détectée
1 – menace détectée mais pas nettoyée
10 – certains fichiers infectés sont restés
101 – erreur d'archive
102 – erreur d'accès
103 – erreur interne

REMARQUE : un code sortie supérieur à 100 signale un fichier non analysé, qui peut donc être infecté.

5.4 ESET SysInspector

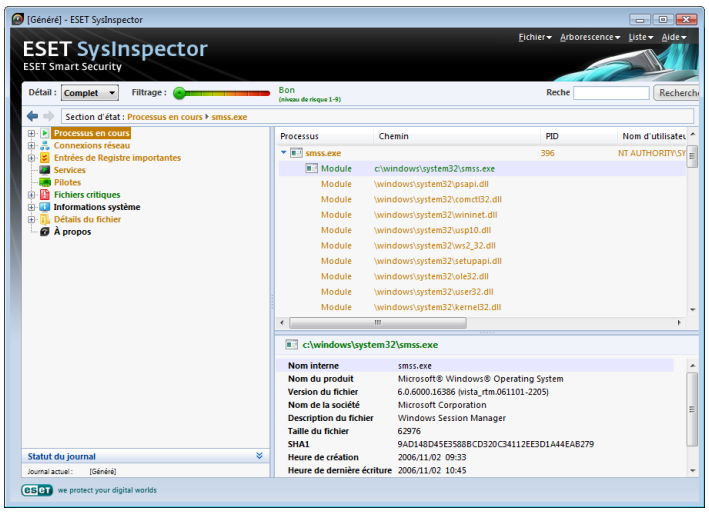
ESET SysInspector est une application qui inspecte complètement l'ordinateur et affiche les données collectées de façon exhaustive. Des information telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

SysInspector existe en deux variantes dans le portefeuille d'ESET. Vous pouvez télécharger l'application portable (SysInspector.exe) gratuitement à partir du site Web d'ESET. La variante intégrée est incluse dans ESET Smart Security 4. Pour ouvrir la section SysInspector, activez le mode d'affichage Avancé dans l'angle inférieur gauche, puis cliquez sur **Outils > SysInspector**. Les deux variantes sont identiques par leur fonction et offrent les mêmes contrôles du programme. La seule différence réside dans la manière dont les résultats sont gérés. L'application portable permet d'exporter un instantané système dans un fichier XML et de l'enregistrer sur votre disque. C'est également possible dans le SysInspector intégré. En outre, vous pouvez commodément stocker vos instantanés système directement dans **ESET Smart Security 4 > Outils > SysInspector** (pour plus d'informations, consultez la rubrique 5.4.1.4 Intégration de SysInspector dans ESS).

Patientez pendant qu'ESET SysInspector analyse votre ordinateur. Cela peut prendre entre 10 secondes et plusieurs minutes en fonction de la configuration du matériel, du système d'exploitation et du nombre d'applications installées sur l'ordinateur.

5.4.1 Interface utilisateur et utilisation de l'application

Pour simplifier l'utilisation, la fenêtre principale est divisée en quatre sections ; les Contrôles du programme situés dans le haut de la fenêtre principale, la fenêtre Navigation à gauche, la fenêtre Description à droite au centre et la fenêtre Détails à droite au bas de la fenêtre principale.



5.4.1.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponibles dans ESET SysInspector

Fichier
En cliquant ici, vous pouvez enregistrer l'état de votre rapport actuel à des fins d'investigation ultérieure ou ouvrir un rapport enregistré précédemment. Si vous voulez publier le rapport, il est recommandé de le générer comme « approprié pour envoi ». Sous cette forme, le rapport omet les informations sensibles.

Remarque : *Vous pouvez ouvrir des rapports d'ESET SysInspector précédemment stockés en les glissant-déplaçant simplement vers la fenêtre principale.*

Arborescence
Permet de développer ou de fermer tous les nœuds.

Liste
Contient des fonctions permettant de faciliter la navigation dans le programme, ainsi que d'autres telles que la recherche d'informations en ligne.

Important : *Les éléments en surbrillance de couleur rouge sont inconnus. C'est pourquoi le programme les marque comme potentiellement dangereux. Si un élément s'affiche en rouge, cela ne signifie pas forcément que vous pouvez supprimer le fichier. Avant de supprimer des fichiers, assurez-vous qu'ils sont vraiment dangereux ou inutiles.*

Aide
Contient des informations sur l'application et ses fonctions.

Détail
Détermine les informations affichées dans d'autres sections de la fenêtre principale, et utilise donc le programme. En mode *de base*, vous avez accès aux informations utilisées pour trouver des solutions à des problèmes courants de votre système. En mode *Moyen*, le programme affiche des détails moins utilisés, tandis qu'en mode *Complet*, ESET SysInspector affiche toutes les informations nécessaires pour résoudre des problèmes très spécifiques.

Filtrage des éléments
Convient parfaitement pour rechercher des fichiers suspects ou des entrées de Registre dans votre système. En réglant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Si le curseur est positionné tout à fait à gauche (Niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, le programme filtre tous les éléments présentant un risque inférieur au niveau de risque actuel, et n'affiche que ceux qui sont plus suspects que le niveau affiché. Lorsque le curseur est positionné tout à fait à droite, le programme n'affiche que les éléments nuisibles connus.

Tous les éléments s'inscrivant dans la plage de risques de 6 à 9 peuvent constituer un risque pour la sécurité. Si vous n'utilisez pas certaines des solutions de sécurité d'ESET, nous vous recommandons d'analyser votre système avec l'analyseur en ligne ESET après que le programme a trouvé un tel élément. L'analyseur en ligne ESET est un service gratuit accessible à l'adresse URL http://www.eset.eu/online-scanner.

Remarque : *Vous pouvez rapidement déterminer le niveau de risque d'un élément en comparant sa couleur à celle du curseur Niveau de risque.*

Rechercher
La fonction Rechercher permet de trouver rapidement un élément spécifique à l'aide de son nom ou d'une partie de celui-ci. Les résultats de la demande de recherche s'affichent dans la fenêtre Description.

Retour
En cliquant sur la flèche Précédent ou Suivant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description.

Section d'état
Affiche le nœud actuel dans la fenêtre Navigation.

5.4.1.2 Navigation dans ESET SysInspector

ESET SysInspector divise plusieurs types d'informations en plusieurs sections de base appelées nœuds. Si des détails supplémentaires sont disponibles, vous pouvez les afficher en développant chaque nœud en sous-nœuds. Pour ouvrir ou réduire un nœud, double-cliquez sur son nom, cliquez sur ⊞ ou ⊟, ou cliquez à côté de son nom. Tandis que vous parcourez l'arborescence des nœuds et sous-nœuds dans la fenêtre Navigation, il se peut que vous découvriez des détails pour chaque nœud affiché dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, il se peut que des détails supplémentaires sur chaque élément s'affichent dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et les informations correspondantes dans les fenêtres Description et Détails.

Processus en cours
Ce nœud contient des informations sur les applications et processus en cours d'exécution lors de la génération du rapport. Il se peut que la fenêtre Description affiche des détails supplémentaires pour chaque processus, tels que les bibliothèques dynamiques utilisées et leur emplacement dans le système, le nom du fournisseur de l'application, le niveau de risque du fichier, etc.

La fenêtre Détails contient des informations supplémentaires sur les éléments sélectionnés dans la fenêtre Description, telles que la taille du fichier ou son hachage.

Remarque : *Un système d'exploitation comprend plusieurs composants noyaux importants fonctionnant 24 h. sur 24/7 j. sur 7 et assurant des fonctions de base et vitales pour d'autres applications utilisateur. Dans certains cas, de tels processus s'affichent dans l'outil ESET SysInspector avec le chemin d'accès du fichier commençant par \??\. Ces symboles permettent une optimisation de ces processus avant leur lancement ; ils sont sûrs pour le système et, comme tels, corrects.*

Connexions réseau
La fenêtre Description contient la liste des processus et applications communiquant sur le réseau à l'aide du protocole sélectionné dans la fenêtre Navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également contrôler le DNS attribuant les adresses IP assignées.

La fenêtre Détails contient des informations supplémentaires sur les éléments sélectionnés dans la fenêtre Description, telles que la taille du fichier ou son hachage.

Entrées de Registre importantes
Contient la liste des entrées de Registre sélectionnées qui sont souvent liées à divers problèmes dans le système, telles que celles spécifiant les programmes à lancer au démarrage, des Objets application d'assistance du navigateur (BHO), etc.

Il se peut que la fenêtre Description indique les fichiers liés à des entrées de Registre spécifiques. La fenêtre Détails peut également présenter des détails supplémentaires.

Services
La fenêtre Description contient la liste des fichiers enregistrés en tant que Services Windows. Vous pouvez contrôler la manière dont le démarrage du service est paramétré, ainsi que des détails spécifiques du fichier dans la fenêtre Détails.

Pilotes
Liste des pilotes installés dans le système.

Fichiers critiques
La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

Informations système
Contient des informations détaillées sur le matériel et les logiciels, ainsi que des informations sur les variables d'environnement et les droits de l'utilisateur définis.

Détails du fichier
Liste des fichiers et fichiers système importants dans le dossier Program Files. Des informations spécifiques sur les fichiers figurent dans les fenêtres Description et Détails.

A propos
Informations sur ESET SysInspector.

5.4.1.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité produit un ensemble d'éléments non communs aux deux journaux. Elle convient si vous voulez conserver une trace des modifications apportées dans le système. Vous pouvez, par exemple, détecter l'activité d'un code malveillant.

Une fois lancée, l'application crée un journal qui s'affiche dans une nouvelle fenêtre. Accédez à **Fichier** -> **Enregistrer le journal** pour enregistrer un journal dans un fichier. Vous pouvez ensuite ouvrir et afficher les fichiers journaux. Pour ouvrir un journal existant, utilisez le menu **Fichier** -> **Ouvrir le journal**. Dans la fenêtre principale du programme, ESET SysInspector affiche toujours un seul journal à la fois.

Si vous comparez deux journaux, le principe est que vous comparez un journal actuellement actif à un autre enregistré dans un fichier. Pour comparer des journaux, utilisez l'option **Fichier** -> **Comparer les journaux**, puis cliquez sur **Sélectionner un fichier**. Le journal sélectionné sera comparé au journal actif dans les fenêtres principales du programme. Je journal obtenu, dit comparatif, n'indiquera que les différences entre ces deux journaux.

Remarque : *Si vous comparez deux fichiers journaux, sélectionnez Fichier -> Enregistrer le journal, puis enregistrez au format ZIP ; les deux fichiers sont enregistrés. Si vous ouvrez ensuite un tel fichier, les journaux qu'il contient sont automatiquement comparés.*

À côté des éléments affichés, SysInspector affiche des symboles identifiant les différences entre les journaux comparés. Les éléments marqués du signe ▬ ne figurent que dans le journal actif et sont absents du journal comparatif ouvert. En revanche, les éléments marqués du signe ✚ ne figurent que dans le journal ouvert et sont absents du journal actif.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

✚ nouvelle valeur, absente du journal précédent.

la section de l'arborescence contient de nouvelles valeurs.

▬ valeur supprimée, présente uniquement dans le journal précédent.

la section de l'arborescence contient des valeurs supprimées.

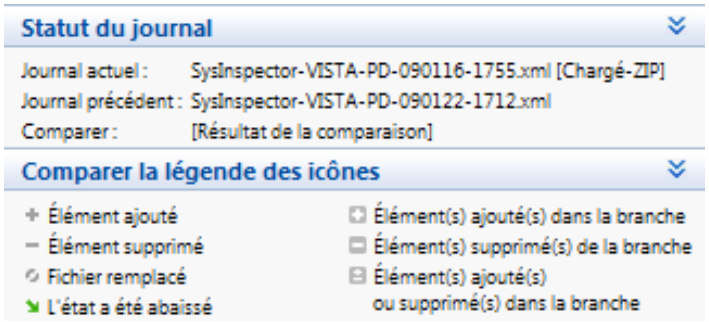
la valeur/le fichier a été modifié.

la section de l'arborescence contient des valeurs/des fichiers supprimés.

Le niveau de risque a baissé ; il était supérieur dans le journal précédent.

Le niveau de risque a augmenté ; il était inférieur dans le journal précédent.

La section d'explication dans l'angle inférieur gauche décrit tous les symboles et affiche les noms des journaux comparés.



Tout journal comparatif peut être enregistré dans un fichier, puis ouvert ultérieurement.

Exemple :
générez et enregistrez un journal consignant des informations originales sur le système dans un fichier nommé précédent.xml. Une fois les modifications apportées au système, ouvrez SysInspector et laissez-le générer un nouveau journal. Enregistrez-le dans un fichier nommé actuel.xml.

Pour suivre les différences entre ces deux journaux, accédez à **Fichier** -> **Comparer les journaux**. Le programme crée un journal comparatif montrant les différences entre les journaux.

Vous pouvez obtenir le même résultat en utilisant l'option de ligne de commande suivante :

SysIsnpector.exe actuel.xml précédent.xml

5.4.1.4 SysInspector comme composant d'ESET Smart Security 4

Pour ouvrir la section SysInspector dans ESET Smart Security 4, cliquez sur **Outils > SysInspector**. Le système de gestion dans la fenêtre de SysInspector est similaire à celui des journaux d'analyse ou des tâches planifiées de l'ordinateur. Toutes les opérations relatives aux instantanés (créer, afficher, comparer, supprimer et exporter) sont accessibles en un ou deux clics.

La fenêtre de SysInspector contient des informations de base sur les instantanés créés, telles que l'heure de création, un bref commentaire, le nom de leur auteur et leur état.

Pour **comparer, ajouter** ou **supprimer** des instantanés, utilisez les boutons correspondants situés sous la liste des instantanés dans la fenêtre de SysInspector. Ces options sont également disponibles dans le menu contextuel. Pour afficher l'instantané système sélectionné, utilisez l'option **Affichage** du menu contextuel. Pour exporter l'instantané sélectionné dans un fichier, cliquez dessus avec le bouton droit, puis sélectionnez **Exporter...**. Voici une description détaillée des options disponibles :

Comparer : permet de comparer deux journaux existants. Cette option convient pour suivre les différences entre le journal actuel et un journal plus ancien. Pour qu'elle fonctionne, vous devez sélectionner deux instantanés à comparer.

Ajouter : crée un enregistrement. Au préalable, vous devez entrer un bref commentaire sur l'enregistrement. Pour suivre la progression de la création de l'instantané (en cours de génération) exprimée en pour cent, consultez la colonne État. Tous les instantanés générés présentent l'état Créé.

Supprimer : supprime des entrées de la liste.

Afficher : affiche l'instantané sélectionné. Vous pouvez également double-cliquer sur l'entrée sélectionnée.

Exporter... : enregistre l'entrée sélectionnée dans un fichier XML (ainsi que dans une version compressée).

5.4.1.5 Script de service

Le script de service est un outil qui a une incidence directe sur le système d'exploitation et sur les applications installées. Il permet aux utilisateurs d'exécuter des scripts qui suppriment les composants problématiques du système, notamment les virus, les restes de virus, les fichiers bloqués, les enregistrements de virus dans le registre, etc. Le script est stocké dans un fichier texte généré à partir d'un fichier .xml préexistant. Les données du fichier script .txt sont classées simplement pour des raisons pratiques. Le script présente à l'origine un comportement neutre. En d'autres termes, il n'a pas d'impact sur le système dans sa forme d'origine. L'utilisateur doit modifier le script pour que ce dernier ait un effet.

Avertissement :
Cet outil est destiné aux utilisateurs expérimentés. Une utilisation inadaptée de cet outil peut endommager les programmes ou le système d'exploitation.

5.4.1.5.1 Génération de scripts de service

Pour générer un script, cliquez avec le bouton droit sur un élément de l'arborescence (dans le volet de gauche) de la fenêtre principale SysInspector. Dans le menu contextuel, sélectionnez l'option **Exporter toutes les sections dans un script de suppression** ou **Exporter les sections sélectionnées dans un script de suppression**.

5.4.1.5.2 Structure du script de service

La première ligne de l'en-tête du script contient des informations sur la version du moteur (« ev » pour « Engine version »), de l'interface utilisateur graphique (« gv » pour « GUI version ») et du journal (« lv » pour « Log version »). Vous pouvez utiliser ces données pour effectuer le suivi des modifications éventuelles du fichier .xml qui génère le script afin d'éviter toute incohérence au cours de l'exécution. Cette partie du script ne doit pas être modifiée.

Le reste du fichier est divisé en sections dans lesquelles les éléments peuvent être modifiés (indique ceux qui seront traités par le script). Vous marquez les éléments à traiter en remplaçant le caractère « - » situé devant un élément par le caractère « + ». Les sections du script sont séparées par une ligne vide. Chaque section a un numéro et un titre.

01) Running processes (Processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution sur le système. Chaque processus est identifié par son chemin UNC et par son code de hachage CRC16 entre astérisques (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, le processus module32.exe a été sélectionné (il est identifié par le caractère « + »). Il s'arrêtera lors de l'exécution du script.

02) Loaded modules (Modules chargés)

Cette section répertorie les modules système utilisés.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbekhb.dll est marqué d'un caractère « + ». Lorsqu'il est exécuté, le script reconnaît les processus à l'aide de ce module spécifique et met fin à ces processus.

03) TCP connections (Connexions TCP)

Cette section comporte des informations concernant les connexions TCP existantes.

Example:

```
03) TCP connections:

- Active connection: 127.0.0.1:30606 ->
127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 ->
127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 ->
127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe
Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Lorsqu'il s'exécute, le script localise le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

04) UDP endpoints (Extrémités UDP)

Cette section comporte des informations concernant les extrémités UDP existantes.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsqu'il s'exécute, le script isole le propriétaire du socket au niveau des extrémités UDP marquées et arrête le socket.

05) DNS server entries (Entrées du serveur DNS)

Cette section comporte des informations concernant la configuration du serveur DNS.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées sont supprimées lors de l'exécution du script.

06) Important registry entries (Entrées de Registre importantes)

Cette section comporte des informations concernant les entrées de Registre importantes.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\
Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées sont supprimées, réduites à des valeurs de 0 octet ou réinitialisées sur les valeurs par défaut lors de l'exécution du script. L'action à appliquer sur une entrée particulière dépend de la catégorie d'entrée et de la valeur de clé du Registre spécifique.

07) Services (Services)

Cette section répertorie les services enregistrés dans le système.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\
windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path:
c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path:
c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Les services marqués et les services dépendants sont arrêtés et désinstallés lors de l'exécution du script.

08) Drivers (Pilotes)

Cette section répertorie les pilotes installés.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\
system32\drivers\acpi.sys, state: Running, startup:
Boot
- Name: ADI UAA Function Driver for High Definition
Audio Service, exe path: c:\windows\system32\drivers\
adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés sont désenregistrés du système et supprimés.

09) Critical files (Fichiers critiques)

Cette section comporte des informations sur les fichiers essentiels au fonctionnement correct du système d'exploitation.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]

* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]

* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés sont supprimés ou réinitialisés sur leurs valeurs d'origine.

5.4.1.5.3 Comment exécuter les scripts de service

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale SysInspector en sélectionnant l'option **Exécuter le script de service** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ?** Une fois que vous avez confirmé votre sélection, un autre avertissement peut apparaître. Il vous informe que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour exécuter le script.

La boîte de dialogue qui apparaît confirme l'exécution du script.

Si le script n'a pu être traité qu'en partie, le message suivant apparaît : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Sélectionnez **Oui** pour afficher le rapport d'erreurs répertoriant les opérations qui n'ont pas été exécutées.

Votre script n'a pas été reconnu comme étant valable et ne sera pas exécuté si le message suivant apparaît : **Y a-t-il des problèmes de cohérence dans le script (en-tête endommagé, titre de section endommagée, ligne vide manquante entre les sections, etc.) ?** Vous pouvez soit rouvrir le fichier de script et corriger les erreurs, soit créer un nouveau script de service.

5.5 ESET SysRescue

ESET Recovery CD (ERCD) est un utilitaire permettant de créer un disque d'amorçage contenant ESET Smart Security 4 (ESS). Le principal avantage d'ESET Recovery CD est le fait qu'ESS s'exécute indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et au système de fichiers entier. il est ainsi possible de supprimer des infiltrations dont la suppression est normalement impossible, par exemple, quand le système d'exploitation est en cours d'exécution, etc.

5.5.1 Configuration requise

ESET SysRescue (ESR) opère dans l'Environnement de préinstallation Microsoft Windows (Windows PE) version 2.x, qui est basé sur Windows Vista. Windows PE faisant partie du Kit d'installation automatisée (Windows AIK) gratuit, pour pouvoir créer un ESR,

Windows AIK doit être préalablement installé. En raison de la prise en charge de la version 32 bits de Windows PE, ESR ne peut être créé que dans la version 32 bits d'ESS/ENA. ESR prend en charge Windows AIK 1.1 et les versions postérieures. ESR est disponible dans ESS/ENA 4.0 et les versions postérieures.

5.5.2 Comment créer un CD de sauvetage

Si la configuration minimale requise pour la création d'un CD ESET SysRescue (ESR) est disponible, cette tâche est facile à exécuter. Pour lancer l'Assistant ESR, cliquez sur **Démarrer > Programmes > ESET > ESET Smart Security 4 > ESET SysRescue**.

Tout d'abord, l'Assistant vérifie la présence de Windows AIK et d'un périphérique adapté pour la création d'un support d'amorçage.

À l'étape suivante, sélectionnez le support cible pour ESR. Outre les supports CD/DVD/USB, vous pouvez enregistrer ESR dans un fichier ISO. Ensuite, vous pouvez graver l'image ISO sur un CD/DVD, ou l'utiliser d'une autre manière (p. ex., dans un environnement virtuel tel que VmWare ou Virtualbox).

Une fois tous les paramètres spécifiés, un aperçu de la compilation s'affiche à la dernière étape de l'Assistant ESET SysRescue. Vérifiez les paramètres, puis lancez la compilation. Les options disponibles sont les suivantes :

Dossiers
ESET Antivirus
Avancé
Périphérique USB d'amorçage
Gravure

5.5.2.1 Dossiers

Le dossier temporaire est un répertoire de travail pour les fichiers requis durant la compilation d'ESET SysRescue.

Un dossier est un dossier dans lequel le fichier ISO obtenu est enregistré une fois la compilation terminée.

La liste sous cet onglet présente tous les lecteurs réseau locaux et mappés ainsi que l'espace libre disponible. Si certains de ces dossiers se trouvent sur un lecteur dont l'espace libre est insuffisant, il est recommandé de sélectionner un autre lecteur disposant de davantage d'espace libre disponible. Sinon, la compilation peut se terminer prématurément en raison de l'insuffisance d'espace disque libre.

Applications externes
Permet de spécifier des programmes supplémentaires qui seront exécutés ou installés après l'amorçage d'un support SysRescue.

Applications externes : permet l'ajout d'un programme externe à la compilation SysRescue.

Dossier sélectionné : dossier dans lequel se trouvent des programmes à ajouter au disque SysRescue.

5.5.2.2 Antivirus ESET

Pour créer un CD ESET SysRescue, vous pouvez sélectionner deux sources de fichiers ESET que le compilateur doit utiliser.

Dossier ESS : fichiers figurant déjà dans le dossier dans lequel le produit ESET est installé sur l'ordinateur.

Fichier MSI : les fichiers du programme d'installation de MSI sont utilisés.

Profil : vous pouvez utiliser l'une des deux sources suivantes de nom d'utilisateur et de mot de passe :

ESS Installé : le nom d'utilisateur et le mot de passe sont copiés à partir de la version installée d'ESET Smart Security 4 ou d'ESET NOD32.

De l'utilisateur : le nom d'utilisateur et le mot de passe entrés dans les zones de texte correspondantes sont utilisés.

Remarque : *ESET Smart Security 4 ou ESET NOD32 Antivirus présent sur le CD ESET SysRescue est mis à jour à partir d'Internet ou de la solution de sécurité ESET installée sur l'ordinateur sur lequel le CD est exécuté.*

5.5.2.3 Avancé

L'onglet **Avancé** permet d'optimiser le CD ESET SysRescue pour la taille de la mémoire de votre ordinateur. Sélectionnez **512 Mo et plus** pour écrire le contenu du CD dans la mémoire vive (RAM). Si vous sélectionnez **Moins de 512 Mo**, le CD de récupération fera l'objet d'un accès permanent lors de l'exécution de WinPE.

Pilotes externes : dans cette section, vous pouvez insérer des pilotes pour votre matériel spécifique (généralement une carte réseau). Bien que WinPE soit basé sur Windows Vista SP1, qui prend en charge un vaste éventail de composants matériels, il arrive que certains composants ne soient pas reconnus et que vous deviez ajouter le pilote manuellement. Il y a deux manières d'introduire le pilote dans la compilation ESET SysRescue : manuellement (bouton **Ajouter**) et automatiquement (bouton **Aut.Search**). En cas d'introduction manuelle, vous devez sélectionner le chemin d'accès du fichier .inf correspondant (le fichier *.sys applicable doit également être présent dans ce dossier). En cas d'introduction automatique, le pilote est trouvé automatiquement dans le système d'exploitation de l'ordinateur. Nous recommandons de n'utiliser l'introduction automatique que si SysRescue est utilisé sur un ordinateur disposant de la même carte réseau que celle équipant celui sur lequel SysRescue est créé. Durant la création d'ESET SysRescue, le pilote est introduit dans la compilation, de façon à ce que l'utilisateur ne doive pas le rechercher ensuite.

5.5.2.4 Périphérique USB d'amorçage

Si vous avez sélectionné un périphérique USB comme support cible, vous pouvez sélectionner l'un des supports USB disponibles sous l'onglet Périphérique USB d'amorçage (s'il y a d'autres périphériques USB).

Avertissement : *Le périphérique USB sera formaté durant le processus de création d'ESET SysRescue, ce qui signifie que toutes les données figurant sur le périphérique seront supprimées.*

5.5.2.5 Graver

Si vous avez sélectionné CD/DVD comme support cible, vous pouvez spécifier des paramètres de gravure supplémentaires sous l'onglet Graver.

Supprimer fichier ISO : activez cette option pour supprimer les fichiers ISO après la création du CD ESET Rescue.

Suppression activée : permet de sélectionner un effacement rapide et un effacement complet.

Graveur : sélectionnez le lecteur à utiliser pour la gravure.

Avertissement : *Il s'agit de l'option par défaut. En cas d'utilisation d'un CD/DVD réinscriptible, toutes les données qu'il contient sont effacées.*

La section Support contient des informations sur le support inséré dans le périphérique CD/DVD.

Vitesse de gravure : sélectionnez la vitesse souhaitée dans le menu déroulant. Pour sélectionner la vitesse de gravure, vous devez tenir compte des capacités du graveur et du type de CD/DVD utilisé.

5.5.3 Utilisation d'ESET SysRescue

Pour utiliser efficacement les supports de sauvetage CD/DVD/USB, vous devez veiller à ce que l'ordinateur démarre à partir des supports d'amorçage d'ESET SysRescue. Vous pouvez modifier la priorité d'amorçage dans le BIOS. Vous pouvez également appeler le menu d'amorçage au démarrage de l'ordinateur (généralement à l'aide de l'une des touches F9 à F12) en fonction de la version de la carte mère ou du BIOS.

Une fois l'amorçage terminé, ESS/ENA démarre. Comme ESET SysRescue n'est utilisé que dans des situations spécifiques, certains modules de protection et fonctionnalités de programme présents d'ordinaire dans ESS/ENA ne sont pas nécessaires ; leur liste est limitée à l'analyse, à la mise à jour et à certaines sections de la configuration de l'ordinateur. La capacité de mise à jour des bases des signatures de virus est la fonctionnalité la plus importante d'ESET SysRescue. il est recommandé de mettre à jour le programme avant de démarrer une analyse de l'ordinateur.

5.5.3.1 Utilisation d'ESET SysRescue

Supposons que des ordinateurs du réseau aient été infectés par un virus modifiant des fichiers exécutables (EXE). ESS/ENA est capable de nettoyer tous les fichiers infectés à l'exception d'explorer.exe, qu'il est impossible de nettoyer, même en mode sans échec.

Cela est dû au fait qu'explorer.exe, processus Windows essentiel, est également lancé en mode sans échec. ESS/ENA ne peut appliquer aucune action au fichier qui reste donc infecté.

Dans un tel scénario, vous pouvez utiliser ESET SysRescue pour résoudre le problème. ESET SysRescue ne requiert pas de composant du système d'exploitation hôte. Il peut ainsi traiter (nettoyer, supprimer) tout fichier figurant sur le disque.

6. Glossaire

6.1 Types d'infiltrations

Une infiltration est un morceau de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur ou de l'endommager.

6.1.1 Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques, parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne comme ceci : après exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur exécute ou ouvre lui-même (accidentellement ou délibérément) le programme malveillant.

L'activité et la sévérité des virus varient. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres en revanche ne causent pas de réels dommages : ils ne servent qu'à ennuyer l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que les virus sont (par rapport aux chevaux de Troie et aux logiciels espions) de plus en plus rares, parce qu'ils ne sont pas commercialement très attrayants pour les auteurs de programmes malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend aujourd'hui à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer les fichiers infectés à leur état original, c'est-à-dire de les nettoyer à l'aide d'un programme anti-virus.

Dans la catégorie des virus, on peut citer : OneHalf, Tenga et Yankee Doodle.

6.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence de base entre un virus et un ver est que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage).

Les vers prolifèrent par le biais de courriers électroniques ou de paquets sur le réseau. Ils peuvent ainsi être catégorisés de deux manières :

- **Courriers électroniques :** qui se distribuent eux-mêmes dans les adresses de messagerie trouvées sur la liste de contacts d'un utilisateur ;
- **Réseau :** exploitant les failles de sécurité de diverses applications.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois même en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rendent plus dangereux que les autres types de programmes malveillants comme les virus.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. De par sa nature il est qualifié pour servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés parce qu'ils contiennent probablement du code malicieux.

Parmi les vers les plus connus, on peut citer : Lovsan/Blaster, Stration/Warezov, Bagle et Netsky.

6.1.3 Chevaux de Troie

Dans le passé, les chevaux de Troie ont été définis comme une catégorie d'infiltrations dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Il est cependant important de remarquer que cette définition s'applique aux anciens chevaux de Troie. Aujourd'hui, il ne leur est plus utile de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. « Cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories. Les plus connues sont :

- downloader : programme malveillant qui est en mesure de télécharger d'autres infiltrations sur l'Internet.
- dropper : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- backdoor : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- keylogger (keystroke logger) : programme qui enregistre chaque touche sur laquelle tape l'utilisateur avant d'envoyer les informations aux pirates.
- dialer : programme destiné à se connecter aux numéros à revenus partagés. Il est presque impossible qu'un utilisateur remarque qu'une nouvelle connexion a été créée. Les dialers ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Les chevaux de Troie prennent généralement la forme de fichiers exécutables avec l'extension .exe. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer car il contient sans doute du code malveillant.

Parmi les chevaux de Troie les plus connus, on peut citer : NetBus, Trojandownloader.Small.ZL, Slapper

6.1.4 Rootkits

Les rootkits sont des programmes malveillants qui procurent aux pirates un accès illimité à un système tout en dissimulant leur présence. Après avoir accédé au système (généralement en exploitant une faille), les rootkits utilisent des fonctions du système d'exploitation pour se protéger des logiciels antivirus : ils dissimulent des processus, des fichiers et des données de la base de registre Windows. Pour cette raison, il est presque impossible de les détecter à l'aide des techniques de test ordinaires.

Souvenez-vous donc que pour se protéger des rootkits, il existe deux niveaux de détection :

1. Lorsqu'ils essaient d'accéder au système. Ils ne sont pas encore installés et donc inactifs. La plupart des antivirus sont en mesure d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement les fichiers comme infectés).
2. Lorsqu'ils sont inaccessibles aux tests habituels. Les utilisateurs du système anti-virus ESET bénéficient de la technologie Anti-Stealth qui permet de détecter et d'éliminer les rootkits en activité.

6.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités tombent donc dans cette catégorie. Souvent, les logiciels publicitaires ouvrent automatiquement une nouvelle fenêtre contextuelle contenant de la publicité dans un navigateur Internet ou modifient la page de démarrage de ce dernier. Ils sont généralement associés à des programmes gratuits et permettent à leurs créateurs de couvrir les frais de développement de leurs applications (souvent utiles).

En soi, les logiciels publicitaires ne sont pas dangereux ; tout au plus dérangent-ils les utilisateurs par l'affichage de publicités. Le danger tient dans le fait qu'ils peuvent aussi avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertiront en effet qu'ils installent en plus un programme publicitaire. Souvent, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire. Cependant, certains programmes refuseront de s'installer sans leur logiciel publicitaire ou verront leurs fonctionnalités limitées. Bref, les logiciels publicitaires accèdent souvent au système d'une manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, mieux vaux jouer la sécurité.

Si un fichier est identifié comme logiciel publicitaire sur votre ordinateur, il est recommandé de le supprimer car il contient sans doute du code malveillant.

6.1.6 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Elles utilisent des fonctions de traçage pour envoyer diverses données statistiques telles qu'une liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou une liste de touches de frappe enregistrées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne seront pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte en banque, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme afin de les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes anti-logiciel espion alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est identifié comme logiciel espion sur votre ordinateur, il est recommandé de le supprimer car il contient sans doute du code malveillant.

6.1.7 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. C'est pourquoi ESET a créé cette catégorie spéciale. Nos clients ont maintenant la possibilité de choisir si le système antivirus doit ou non détecter ce type de menaces.

Les applications potentiellement risquées rentrent dans une classification utilisée pour les logiciels légitimement commerciaux. Cette classification comprend les programmes d'accès à distance, les applications de crackage des mots de passe, ou les keyloggers (programmes qui enregistrent chaque frappe sur le clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous l'ayez installée), consultez votre administrateur réseau et supprimez l'application.

6.1.8 Applications potentiellement indésirables

Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Leur installation requiert généralement un consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Les changements les plus significatifs sont :

- de nouvelles fenêtres que vous n'avez jamais vues s'ouvrent
- des processus cachés sont activés et exécutés
- l'utilisation des ressources système est plus importante
- les résultats de recherche sont modifiés
- l'application communique avec des serveurs distants

6.2 Types d'attaques distantes

Il existe diverses techniques permettant à des pirates de mettre en péril des systèmes distants. Elles se divisent en plusieurs catégories.

6.2.1 Attaques DoS

L'attaque DoS, ou attaque par déni de service (Denial of Service), est une tentative de rendre les ressources d'un ordinateur ou d'un réseau indisponibles pour ses utilisateurs. La communication entre les utilisateurs affectés est obstruée et ne peut plus continuer normalement. Les ordinateurs qui ont subi une attaque DoS doivent généralement redémarrer pour fonctionner correctement.

Le plus souvent, les cibles sont des serveurs Web et l'objectif est de les rendre inutilisables pendant un certain temps.

6.2.2 Empoisonnement DNS

Avec la méthode d'empoisonnement DNS (Domain Name Server), les pirates tentent de faire croire au serveur DNS de tout ordinateur que les fausses données qui leur sont transmises sont légitimes et authentiques. Ces fausses informations sont ensuite mises en cache pendant un certain temps, permettant aux agresseurs de réécrire les réponses DNS des adresses IP. De cette manière, les utilisateurs qui tentent d'accéder à des sites internet téléchargeront des virus ou des vers au lieu du contenu original de ces sites.

6.2.3 Attaques de vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. Les vers de réseau exploitent les failles de sécurité de diverses applications. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois même en quelques minutes.

La plupart des attaques de ver (Sasser, SqlSlammer) peuvent être évitées en utilisant les paramètres de sécurité par défaut du pare-feu ou en bloquant les ports non protégés et non utilisés. Il est également essentiel de mettre à jour votre système d'exploitation avec les correctifs de sécurité les plus récents.

6.2.4 Balayage de ports

Le balayage de ports permet de contrôler si les ports de certains ordinateurs sont ouverts sur un hôte de réseau. Le logiciel utilisé à cette fin s'appelle le scanneur de port.

Le port d'un ordinateur est un point virtuel qui traite les données entrantes et sortantes. C'est un point crucial pour la sécurité. Sur un réseau de grande taille, les informations collectées par le scanneur de ports peuvent permettre d'identifier les failles potentielles. Cette utilisation est bien sûr tout à fait légale.

D'un autre côté, le balayage de ports est souvent utilisé par les pirates qui tentent de compromettre la sécurité. Ils envoient d'abord des paquets à chaque port. En fonction du type de réponse, il est possible de déterminer quels ports sont utilisés. Si le balayage lui-même ne cause aucun dommage, cette activité peut révéler les failles potentielles et permettre aux pirates de prendre le contrôle d'ordinateurs distants.

Nous conseillons aux administrateurs du réseau de bloquer tous les ports non utilisés et de protéger ceux qui sont utilisés des accès non autorisés.

6.2.5 Désynchronisation TCP

La désynchronisation TCP est une technique utilisée pour les détournements de session TCP (TCP Hijacking). Elle est déclenchée par un processus dans lequel le numéro séquentiel de paquets entrants diffère du numéro attendu. Les paquets dont le numéro séquentiel est différent de celui attendu sont rejetés (ou enregistrés dans la mémoire tampon, s'ils sont présents dans la fenêtre de communication active).

Lorsqu'il y a désynchronisation, les deux extrémités de la communication rejettent les paquets reçus. C'est ici que les pirates peuvent intervenir à distance pour infiltrer et fournir des paquets dont le numéro séquentiel est correct. Les pirates peuvent même manipuler la communication à l'aide de leurs commandes ou la modifier d'une autre manière.

Les détournements de session TCP visent à interrompre les communications serveur-client ou les communications poste à poste. De nombreuses attaques peuvent être évitées par l'authentification de chaque segment TCP. Il est également conseillé d'utiliser les configurations recommandées pour vos périphériques réseau.

6.2.6 Relais SMB

SMBRelay et SMBRelay2 sont des programmes spéciaux permettant de mener une attaque contre des ordinateurs distants. Les programmes tirent parti du protocole de partage de fichiers SMB (Server Message Block) situé sur NetBIOS. Lorsqu'un utilisateur partage des dossiers ou répertoires sur un réseau local, il y a de grandes chances qu'il utilise ce protocole de partage de fichiers.

Au cours des communications sur le réseau local, les empreintes numériques des mots de passe sont échangées.

SMBRelay reçoit une connexion sur les ports UDP 139 et 445, relaie les paquets échangés par le client et le serveur, et les modifie. Après connexion et authentification, le client est déconnecté. SMBRelay crée une nouvelle adresse virtuelle IP, à laquelle il est possible d'accéder à l'aide de la commande « net use \\192.168.1.1 ». L'adresse peut ensuite être utilisée par n'importe quelle fonction de réseau de Windows. SMBRelay relaie les communications du protocole SMB, sauf la négociation et l'authentification. Les pirates peuvent utiliser l'adresse IP tant que l'ordinateur client est connecté.

SMBRelay2 fonctionne selon le même principe que SMBRelay, si ce n'est qu'il utilise les noms NetBIOS plutôt que les adresses IP. Tous deux peuvent mener des attaques dites de « l'homme du milieu » (man-in-the-middle). Ces attaques permettent à des pirates de lire, d'insérer des données et de modifier à distance les messages échangés entre deux points de communication sans être remarqué. Les ordinateurs exposés à ce type d'attaque arrêtent souvent de répondre ou redémarrent de manière impromptue.

Pour éviter de telles attaques, nous vous recommandons d'utiliser des mots de passe ou des clés d'authentification.

6.2.7 Attaques par protocole ICMP

L'ICMP (Internet Control Message Protocol) est un protocole Internet très utilisé. Il est surtout utilisé par les ordinateurs en réseau pour envoyer différents messages d'erreur.

Les attaquants distants tentent d'exploiter la faiblesse du protocole ICMP. Le protocole ICMP est conçu pour les communications à sens unique n'exigeant pas d'authentification. Cela permet aux attaquants distants de déclencher ce qu'on appelle les attaques DoS (Denial of Service (déni de service)), ou des attaques qui permettent différents accès non autorisés aux paquets entrants et sortants.

Le Ping Flood (inonder par flux de ping), l'ICMP_ECHO flood et le smurf sont des exemples typiques d'attaques ICMP. Les ordinateurs exposés aux attaques ICMP sont considérablement ralentis (cela est valable pour toutes les applications qui utilisent Internet) et ont des problèmes de connexion Internet.

6.3 Courrier électronique

Le courrier électronique est une forme de communication moderne qui offre beaucoup d'avantages. Il est flexible, rapide et direct. Le courrier électronique a joué un rôle crucial dans l'expansion d'Internet au début des années 90.

Malheureusement, le grand anonymat des courriers électroniques et Internet a laissé libre champ à beaucoup d'activités illégales telles que le spamming (c'est le fait d'exposer volontairement un grand nombre de personnes à un message indésirable). En gros, les courriers indésirables comprennent les publicités indésirables, les canulars (hoax) et les logiciels malveillants. Les désagréments et le danger pour l'utilisateur ont augmenté tout simplement par le fait que l'envoi de tels messages ne coûte rien, et que les auteurs des courriers indésirables disposent de nombreux outils et sources pour acquérir de nouvelles adresses de messagerie. En plus, le volume et la variété des courriers indésirables ne facilite pas la règlementation. Plus vous utilisez votre adresse de messagerie, plus vous augmentez la possibilité de vous retrouver dans une base de données de moteur de courrier indésirable. Quelques conseils pour la prévention :

- Ne publiez pas votre adresse de messagerie sur Internet, si possible.
- Ne donnez votre adresse de messagerie qu'à des personnes fiables.
- N'utilisez pas des pseudonymes communs, si possible : lorsque les pseudonymes sont compliqués, la probabilité de les traquer devient faible.
- Ne répondez pas aux courriers indésirables qui sont déjà arrivés dans votre boîte à lettre.
- Faites attention lorsque vous remplissez des formulaires Internet : soyez particulièrement attentif aux cases à cocher du type « Oui, je voudrais recevoir des informations concernant ....dans ma boîte à lettre ».
- Utilisez des adresses de messagerie « spécialisées » : p. ex., une pour votre travail, une pour communiquer avec vos amis, etc.
- Changez vos adresses de messagerie de temps en temps.
- Utilisez une solution de blocage du courrier indésirable.

6.3.1 Publicités

La publicité via Internet est une des formes de publicité les plus en vogue. La publicité par e-mail utilise le courrier électronique comme moyen de contact. Ses principaux avantages pour le marketing sont ses coûts nuls, le caractère très direct et la grande efficacité ; qui

plus est, les messages sont transmis quasi immédiatement. Nombre d'entreprises utilisent des outils de marketing par e-mail pour communiquer de manière efficace avec leurs clients et prospects.

Ce mode de publicité est légitime, car l'utilisateur pourrait être intéressé par la réception d'informations commerciales sur certains produits. Mais le fait est que de nombreuses entreprises envoient en masse des messages commerciaux non sollicités. La publicité par e-mail dépasse alors les limites et devient du courrier indésirable.

La quantité de messages publicitaires non sollicités est devenue un réel problème, car elle ne montre aucun signe d'accalmie. Les auteurs de messages non sollicités tentent naturellement de déguiser le courrier indésirable en messages légitimes. D'autre part, des publicités légitimes distribuées en grandes quantités peuvent provoquer des réactions négatives.

6.3.2 Canulars (hoax)

Un houx est message propagé à travers Internet. Il est envoyé généralement avec le courrier et parfois par des outils de communication tels que ICQ et Skype. Le message est souvent une blague ou une légende urbaine.

Les virus Hoax essaient de provoquer chez les destinataires de la peur, de l'incertitude et du doute, les amenant à croire qu'ils ont un « virus indétectable » en train de supprimer tous les fichiers et de récupérer les mots de passe, ou d'effectuer une activité nuisible sur leur système.

Quelques hoax sont conçus pour provoquer chez les autres des troubles émotionnels. Les destinataires sont généralement invités à réacheminer de tels messages à tous leurs contacts, et c'est ce qui perpétue le cycle de vie des hoax. Même les téléphones portables ont leurs hoax, les « pleas for help » (appels à l'aide), messages émanant de personnes qui vous proposent de vous envoyer de l'argent de l'étranger, etc. Dans la plupart des cas, il est impossible de déterminer l'intention de leur créateur.

En principe, si un message vous demande de le réacheminer à toutes vos connaissances, il se pourrait très bien être un hoax. Sur Internet, il y a beaucoup de sites spécialisés qui peuvent vérifier si un courrier est légitime ou pas. Faites une recherche sur Internet sur tout message suspecté d'être un hoax avant de le réacheminer.

6.3.3 Hameçonnage

Le terme d'hameçonnage (phishing en anglais) désigne une activité frauduleuse utilisant des techniques de piratage psychologique qui consistent à manipuler les utilisateurs pour obtenir des informations confidentielles. Son but est d'accéder à des données sensibles, telles que numéros de comptes bancaires, codes secrets, etc.

La technique consiste généralement à envoyer un message électronique en se faisant passer pour une personne ou une entreprise digne de confiance (institution financière, compagnie d'assurance). Le message peut sembler très authentique et contenir des graphiques et contenus qui proviennent véritablement de la source dont il se réclame. On vous demande d'entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe. Toutes ces données, si elles sont soumises, peuvent facilement être volées et utilisées à des fins illégales.

Notez que les banques, compagnies d'assurance et autres sociétés légales ne demandent jamais de noms d'utilisateur et de mots de passe dans un message non sollicité.

6.3.4 Reconnaissance des courriers indésirables

Généralement peu d'indicateurs contribuent à identifier les courriers indésirables (messages non sollicités) dans une boîte à lettres. Si un message remplit au moins l'un des critères suivants, il s'agit probablement d'un courrier indésirable.

- l'adresse de l'expéditeur n'est pas sur la liste de vos contacts
- on vous offre une grande somme d'argent, mais vous devez en fournir une petite somme avant
- on vous demande d'entrer, sous divers prétextes (vérification de données, opérations financières), certaines de vos données personnelles : numéros de compte en banque ou noms d'utilisateur et mots de passe.
- le message est écrit en langue étrangère
- on vous demande d'acheter un produit qui ne vous intéresse pas. Si vous décidez d'acheter quand même, vérifiez que l'expéditeur du message est un vendeur sérieux (consultez le fabricant original du produit).
- Certains mots sont mal écrits pour pouvoir passer à travers le filtre du courrier indésirable. Par exemple « vaigra » au lieu de « viagra », etc.

6.3.4.1 Règles

Dans le contexte des solutions de blocage du courrier indésirable et des clients de messagerie, les règles sont des outils permettant de manipuler les fonctions de messagerie. Elles se composent de deux parties logiques :

1. la condition (par exemple, un message entrant provenant d'une certaine adresse) ;
2. l'action (par exemple, la suppression du message ou son déplacement vers un dossier spécifique).

Le nombre de règles et leurs combinaisons varient en fonction de la solution de blocage du courrier indésirable. Ces règles servent de protection contre les courriers indésirables (messages non sollicités). Exemples caractéristiques :

- 1. condition : un message entrant contient des mots habituellement utilisés dans des courriers indésirables ;
  2. action : supprimer le message;
- 1. condition : un message entrant contient une pièce jointe comportant l'extension .exe ;
  2. action : supprimer la pièce jointe et livrer le message dans la boîte aux lettres.
- 1. condition : un message entrant arrive de votre employeur ;
  2. action : déplacer le message dans le dossier « Travail ».

Nous vous recommandons d'utiliser une combinaison de règles des programmes de blocage du courrier indésirable afin de faciliter l'administration et mieux filtrer les courriers indésirables (messages non sollicités).

6.3.4.2 Filtre bayésien

Le filtrage bayésien est une méthode très efficace de filtrage des messages, utilisée par la plupart des produits de blocage di courrier indésirable. Il permet d'identifier les messages non sollicités avec un haut degré de précision. Le filtre bayésien peut s'adapter à chaque utilisateur.

Le principe est le suivant : il y a d'abord une phase d'apprentissage. L'utilisateur doit désigner un nombre suffisant de messages entrants comme étant des messages légitimes ou du courrier indésirable (normalement 200/200). Le filtre analyse les deux catégories et apprend, par exemple, que le courrier indésirable contient généralement des mots tels que « rolex » ou « viagra », tandis que les messages légitimes sont envoyés par des parents ou à partir d'adresses de la liste de contacts de l'utilisateur. Si un grand nombre de messages sont traités, le filtre bayésien peut affecter un certain « indice de courrier indésirable » à chaque message et déterminer s'il s'agit ou non de courrier indésirable.

Le principal avantage est sa souplesse. Par exemple, si un utilisateur est biologiste, tous les messages entrants concernant la biologie ou des champs d'étude apparentés recevront généralement un indice de probabilité moindre. Si un message comprend des mots qui le classeraient comme non sollicité mais est envoyé par un membre de la liste de contacts, il est marqué comme légitime dans la mesure où les expéditeurs d'une liste de contacts réduisent la probabilité générale qu'il s'agisse de courrier indésirable.

6.3.4.3 Liste blanche

En général, une liste blanche est une liste d'éléments ou de personnes qui ont été acceptées ou ont obtenu une autorisation d'accès. Le terme « liste blanche de messagerie » définit une liste de contacts dont l'utilisateur désire recevoir les messages. Ces listes blanches sont basées sur des mots-clés recherchés pour une adresse électronique, des noms de domaines ou des adresses IP.

Si une liste blanche fonctionne en « mode exclusif », les messages de toutes les autres adresses, domaines ou adresses IP seront écartés. Si elle fonctionne en mode non exclusif, ces messages ne seront pas supprimés, mais filtrés d'une autre façon.

Une liste blanche fonctionne sur le principe opposé d'une liste noire. Les listes blanches sont relativement faciles à maintenir, plus que les listes noires. Pour un meilleur filtrage des courriers indésirables, nous vous recommandons d'utiliser des listes blanches et des listes noires.

6.3.4.4 Liste noire

Généralement, une liste noire est une liste d'éléments ou de personnes non acceptées ou interdites. Dans le monde virtuel, c'est une technique qui permet d'accepter des messages de tous les utilisateurs qui ne figurent pas sur cette liste.

Il existe deux types de listes noires. D'une part, les utilisateurs peuvent créer leur propre liste noire dans leur programme de blocage du courrier indésirable. D'autre part, on peut trouver sur Internet de nombreuses listes noires professionnelles régulièrement mises à jour, créées par des institutions spécialisées.

Une liste noire repose sur le principe opposé à celui d'une liste blanche. Il est essentiel d'utiliser des listes noires pour bloquer efficacement le courrier indésirable, mais ces listes très difficiles à tenir à jour car de nouveaux éléments à bloquer apparaissent jour après jour. Nous recommandons d'utiliser à la fois la liste blanche et la liste noire pour mieux filtrer le courrier indésirable.

6.3.4.5 Contrôle côté serveur

Le contrôle côté serveur est une technique permettant d'identifier le courrier indésirable de masse d'après le nombre de messages reçus et les réactions des utilisateurs. Chaque message laisse sur le serveur une empreinte numérique unique en fonction de son contenu. En fait, c'est un numéro d'identification unique qui ne dit rien sur le contenu du message. Deux messages identiques auront une empreinte identique, alors que des messages différents auront une empreinte différente.

Si un message est marqué comme courrier indésirable, son empreinte est envoyée au serveur. Si le serveur reçoit plusieurs empreintes identiques (correspondant à un certain message de courrier indésirable), cette empreinte est stockée dans la base d'empreintes de courrier indésirable. Lorsqu'il analyse des messages entrants, le programme envoie les empreintes de ces messages au serveur. Le serveur renvoie des informations indiquant quelles empreintes correspondent à des messages déjà identifiés comme courrier indésirable par d'autres utilisateurs.