Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG

Manuel de l'administrateur

VERSION DE L'APPLICATION : 8.5

Chers utilisateurs

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

Date d'édition du document : 27/06/2012

http://www.kaspersky.fr
http://support.kaspersky.fr

TABLE DES MATIERES

PRESENTATION DU MANUEL

Ce document représente le Manuel de l'administrateur de Kaspersky Anti-Virus 8.5 for Microsoft® ISA Server et Forefront® TMG (ci-après - "Kaspersky Anti-Virus").

Ce Manuel est destiné aux experts techniques chargés d'installer et d'administrer Kaspersky Anti-Virus et d'assister les organisations qui utilisent Kaspersky Anti-Virus.

Il s'adresse aux experts techniques qui ont l'expérience de Microsoft ISA Server/Forefront TMG.

Le manuel est conçu pour les buts suivants :

- Décrire la configuration et l'utilisation de Kaspersky Anti-Virus.
- Assurer une recherche rapide de l'information pour répondre aux problèmes liés à l'utilisation de Kaspersky Anti-Virus.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION

DANS CE DOCUMENT

Ce guide contient les sections suivantes :

Sources d'informations sur l'application (à la page 10)

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web que vous pouvez consulter pour discuter du fonctionnement de l'application.

Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG (à la page 12)

Cette section décrit les principales possibilités de l'application et contient des informations sur la configuration logicielle et matérielle requise pour installer Kaspersky Anti-Virus.

Architecture de l'application (à la page 15)

Cette section contient la description des modules de Kaspersky Anti-Virus ou de la logique de leur interaction.

Interface de l'application (à la page 19)

Cette section contient des informations sur les éléments principaux de l'interface graphique de la Console d'administration utilisée pour administrer les paramètres de Kaspersky Anti-Virus.

Licence de l'application (à la page 27)

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du Contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la licence.

Lancement et arrêt de l'application (à la page 33)

Cette section contient des informations sur la manière de lancer et d'arrêter l'application.

Etat de la protection (à la page 35)

Cette section apporte des informations sur la manière de consulter l'état de la licence de Kaspersky Anti-Virus, sur la mise à jour des bases de Kaspersky Anti-Virus ainsi que sur les statistiques relatives au fonctionnement des filtres de Kaspersky Anti-Virus.

Protection par défaut (à la page 40)

Cette section décrit le fonctionnement de Kaspersky Anti-Virus avec les paramètres par défaut.

Connexion de la Console d'administration au stockage de configuration (à la page 42)

Cette section décrit la procédure de connexion de la Console d'administration de Kaspersky Anti-Virus au stockage de configuration de Microsoft ISA Server / Forefront TMG.

A propos du partage des privilèges d'utilisation de Kaspersky Anti-Virus (à la page 45)

Cette section décrit les privilèges des administrateurs quant à l'utilisation de Kaspersky Anti-Virus.

Particularités de fonctionnement avec plusieurs administrateurs (à la page 46)

Cette section décrit les particularités de l'utilisation simultanée par plusieurs administrateurs dans les Consoles d'administration connectées à un stockage de configuration.

Mise à jour des bases (à la page 47)

Cette section contient des informations sur la mise à jour des bases de Kaspersky Anti-Virus et des instructions de configuration des paramètres de mise à jour.

Protection antivirus (à la page 54)

Cette section contient des informations sur la protection antivirus et des informations sur la configuration des stratégies de Kaspersky Anti-Virus, des paramètres d'analyse du trafic transmis via les protocoles HTTP, FTP, SMTP et POP3 et des paramètres de productivité de l'analyse.

Sauvegarde (à la page 78)

Cette section contient des informations sur la sauvegarde de Kaspersky Anti-Virus, sur la manipulation des objets placés dans la sauvegarde et sur la configuration des paramètres de celle-ci.

Diagnostic (à la page 86)

Cette section contient des informations sur les informations des journaux de Kaspersky Anti-Virus et sur la configuration des paramètres de gestion de ces journaux.

Rapports (à la page 89)

Cette section contient des informations sur les rapports de Kaspersky Anti-Virus et sur les tâches de génération de rapports ainsi que des instructions sur l'utilisation de ces derniers.

Contacter le Support Technique (à la page 97)

Cette section contient des informations sur les moyens d'obtenir de l'assistance technique et sur les conditions requises pour obtenir l'aide du Support technique.

Glossaire terminologique (à la page 99)

Cette section contient une liste des termes utilisés dans l'application et une brève définition de chacun d'eux.

Kaspersky Lab (à la page 102)

Cette section contient des informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (à la page 103)

Cette section contient des informations sur le code de programmation des éditeurs tiers utilisé dans l'application.

Notifications sur les marques de commerce (à la page 104)

Cette section répertorie les marques de commerce des titulaires de droit tiers utilisées dans ce document.

Index

Cette section permet de trouver rapidement les informations recherchées dans le document.

CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

EXEMPLE DU TEXTE	DESCRIPTION DES CONVENTIONS
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent des informations sur les actions indésirables potentielles qui peuvent amener à la perte d'informations, aux pannes de matériel ou du système d'exploitation.
Il est conseillé d'utiliser ...	Les remarques sont encadrées. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes ou des cas particuliers importants liés au fonctionnement de l'application.
Exemple : ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".

EXEMPLE DU TEXTE	DESCRIPTION DES CONVENTIONS
La *mise à jour*, c'est ... L'événement *Bases dépassées* survient.	Les éléments de sens suivants sont en italique : • nouveaux termes ; • noms des états et des événements de l'application.
Appuyez sur la touche **ENTER**. Appuyez sur la combinaison des touches **ALT**+**F4**.	Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules. Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.
Cliquez sur le bouton **Activer**.	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
➧ *Pour planifier une tâche, procédez comme suit :*	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
Dans la ligne de commande, saisissez le texte help Les informations suivantes s'affichent : Indiquez la date au format JJ:MM:AA.	Les types suivants du texte apparaissent dans un style spécial : • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir par l'utilisateur.
<Nom de l'utilisateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Web que vous pouvez consulter pour discuter du fonctionnement de l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site du support technique (base de connaissances) ;
- aide électronique ;
- documentation.

Si vous n'avez pas trouvé la solution au problème, nous vous recommandons de prendre contact avec le Support Technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page 97).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Web de Kaspersky Lab.

Page sur le site Web de Kaspersky Lab

Le site Web de Kaspersky Lab contient une page particulière pour chaque application.

Cette page (http://www.kaspersky.com/fr/anti-virus-microsoft-isa-server-forefront-tmg) fournit des informations générales sur l'application, ses possibilités et ses particularités de fonctionnement.

La page http://www.kaspersky.fr contient le lien vers la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

Page sur le site Web du Support Technique (Base de connaissances)

La Base de connaissances est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base de connaissances (http://support.kaspersky.com/fr/tmg_8_ee) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Anti-Virus, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support technique en général.

Aide électronique

L'aide électronique de l'application est offerte sous forme de l'aide contextuelle. L'aide contextuelle contient la liste et la description des paramètres pour chaque fenêtre de l'application.

Documentation

La distribution de l'application comprend les documents qui vous permettent d'installer et d'activer l'application sur les ordinateurs du réseau de l'entreprise, de configurer ses paramètres de fonctionnement et de connaître les principales astuces d'utilisation de l'application.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB SUR LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications sur notre forum (http://forum.kaspersky.fr).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, sur l'achat ou sur la prolongation de la durée d'utilisation de l'application, vous pouvez contacter nos experts du service commercial à l'aide d'un des moyens suivants :

- En appelant notre service clientèle français (http://www.kaspersky.com/fr/contacts).
- En envoyant un message avec votre question à l'adresse sales@kaspersky.com.

La réponse sera donnée en français ou en anglais suivant votre demande.

CONTACTER LE GROUPE DE LOCALISATION ET DE DOCUMENTATION

Pour contacter le Groupe de localisation et de documentation, vous pouvez envoyer un message par courrier électronique à docfeedback@kaspersky.com. Vous devez indiquer "Kaspersky Help Feedback: Kaspersky Anti-Virus 8.5 for Microsoft ISA Server et Forefront TMG" dans l'objet du message.

KASPERSKY ANTI-VIRUS 8.5 FOR MICROSOFT ISA SERVER AND FOREFRONT TMG

Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG assure une protection antivirus du trafic via les protocoles HTTP, FTP, SMTP et POP3 qui passe par le pare-feu de Microsoft ISA Server/Forefront TMG. Pour assurer la protection antivirus, les modules de Kaspersky Anti-Virus sont installés sur les serveurs physiques du réseau de l'entreprise sur lesquels est déployé le pare-feu de Microsoft ISA Server / Forefront TMG (ci-après "serveurs"). En fonction de l'option de déploiement du pare-feu de Microsoft ISA Server / Forefront TMG (cf. section "Configuration de Kaspersky Anti-Virus" à la page 16) les serveurs peuvent fonctionner de manière autonome ou être rassemblés dans un groupe ou une entreprise.

L'analyse du trafic via le protocole HTTPS est aussi prévue pour Kaspersky Anti-Virus installé sur Forefront TMG. Pour que l'analyse du trafic HTTPS soit exécutée, il faut activer l'inspection du trafic dans la console d'administration de Forefront TMG.

Kaspersky Anti-Virus offre les possibilités suivantes :

- L'analyse du trafic via les protocoles HTTP, FTP, SMTP, POP3 en temps réel à la recherche de la présence d'objets malveillants et d'objets potentiellement infectés. Selon les paramètres installés, Kaspersky Anti-Virus répare ou bloque ces objets.
- L'administration des stratégies de traitement des protocoles, de l'analyse antivirus, des exclusions de l'analyse pour différents groupes d'objets de réseau.
- La configuration des paramètres de productivité de l'application sur chaque serveur, en particulier, pour répartir la charge entre les processeurs du serveur.
- La configuration des paramètres généraux de fonctionnement de l'application pour tous les serveurs dans le groupe, tels que les paramètres de mise à jour, les paramètres de la sauvegarde et des journaux.
- La mise à jour programmée ou manuelle des bases de Kaspersky Anti-Virus. Les serveurs HTTP des mises à jour de Kaspersky Lab, les serveurs d'utilisateur HTTP, FTP ou le dossier réseau contenant l'ensemble réel des mises à jour peuvent servir de source de mise à jour.
- La configuration des paramètres de fonctionnement de l'application conformément au volume du trafic, en particulier, la configuration de la vitesse de transfert des données pour optimiser l'analyse.
- La conservation des copies des objets détectés par Kaspersky Anti-Virus dans la Sauvegarde.
- La conservation centralisée des informations sur les objets de la Sauvegarde dans la base de données.
- Administration des clés. La licence de Kaspersky Anti-Virus est octroyée pour toute l'application et non par pour des serveurs séparés.
- La surveillance en temps réel de l'application sur les serveurs.
- La consultation des statistiques générales d'utilisation de l'application sur les serveurs du groupe.
- L'administration des journaux des événements de l'application.
- La création des rapports de fonctionnement de l'application.

DANS CETTE SECTION

NOUVEAUTES

Kaspersky Anti-Virus 8.5 pour Microsoft ISA Server and Forefront TMG se différencie de la version précédente de l'application grâce aux nouveautés suivantes :

- Le nouveau moteur antivirus permet d'analyser les objets plus rapidement tout en sollicitant encore moins les ressources.
- Toutes les options de déploiement du pare-feu de Microsoft ISA Server/Forefront TMG sont prises en charge.
- La conservation des informations relatives aux objets placés dans la sauvegarde et des statistiques de fonctionnement de l'application dans la Base de données de la sauvegarde et des statistiques s'effectuent de manière centralisée.
- La nouvelle interface utilisateur permet de gérer facilement les configurations de l'ensemble des modules et des sous-systèmes de l'application.
- Le système des rôles administratifs de Microsoft ISA Server/Forefront TMG est utilisé pour partager les privilèges d'utilisation de Kaspersky Anti-Virus.
- La possibilité de restaurer la fonctionnalité de Kaspersky Anti-Virus en cas de violation de la configuration de l'application est intégrée et évite d'avoir à réinstaller l'application.

CONFIGURATIONS MATERIELLES ET LOGICIELLES

Kaspersky Anti-Virus peut fonctionner conjointement avec les produits suivants :

- Microsoft ISA Server 2006 avec SP1, Standard Edition (ci-après – Microsoft ISA Server SE).
- Microsoft ISA Server 2006, Enterprise Edition (ci-après – Microsoft ISA Server EE).
- Microsoft Forefront TMG 2010 avec SP1, Standard Edition (ci-après – Forefront TMG SE).
- Microsoft Forefront TMG 2010, Enterprise Edition (ci-après – Forefront TMG EE).

Exigences en cas d'utilisation de Kaspersky Anti-Virus sur le serveur Microsoft ISA Server SE/EE

Configuration matérielle :

- Processeur avec 1 GHz ;
- 1 Go de mémoire vive ;
- Espace disponible sur le disque dur : 2.5 Go.

Un des systèmes d'exploitation suivants est requis pour installer Kaspersky Anti-Virus :

- Microsoft Windows Server® 2003 32-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows Server 2003 R2 32-bits, Standard Edition/Enterprise Edition/Datacenter Edition.

Un des systèmes d'exploitation suivants est requis pour installer la Console d'administration de Kaspersky Anti-Virus :

- Microsoft Windows Server 2003 32-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows Server 2003 R2 32-bits, Standard Edition/Enterprise Edition/Datacenter Edition.
- Microsoft Windows® XP 32-bits avec SP3.

Exigences en cas d'installation de Kaspersky Anti-Virus sur le serveur Forefront TMG SE/EE

Configuration matérielle :

- Processeur 64-bits à 2 noyaux avec 2 GHz ;
- 2 Go de mémoire vive avec 1 GHz ;
- Espace disponible sur le disque dur : 2.5 Go.

Un des systèmes d'exploitation suivants est requis pour installer Kaspersky Anti-Virus :

- Microsoft Windows Server 2008 64-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows Server 2008 R2 64-bits, Standard Edition/Enterprise Edition/Datacenter Edition.

Un des systèmes d'exploitation suivants est requis pour installer la Console d'administration de Kaspersky Anti-Virus :

- Microsoft Windows Server 2008 R2 64-bits, Standard Edition/Enterprise Edition/Datacenter Edition.
- Microsoft Windows Server 2008 64-bits avec SP2, Standard Edition/Enterprise Edition/Datacenter Edition ;
- Microsoft Windows 7 64-bits, Professional Edition/Enterprise Edition/Ultimate Edition ;
- Microsoft Windows Vista® 64-bits avec SP2, Professional Edition/Business Edition/Enterprise Edition/Ultimate Edition.

Exigences vis-à-vis du serveur SQL sur lequel se trouve la Base de données de la sauvegarde et des statistiques

Un des systèmes d'administration des bases de données doit être installé sur le serveur :

- Microsoft SQL Server® 2008, Express Edition/Standard Edition/Enterprise Edition ;
- Microsoft SQL Server 2008 R2, Express Edition/Standard Edition/Enterprise Edition ;
- Microsoft SQL Server 2005, Standard Edition/Enterprise Edition ;
- Microsoft SQL Server 2005, Express Edition (+ Advanced Services).

ARCHITECTURE DE L'APPLICATION

Cette section contient la description des modules de Kaspersky Anti-Virus ou de la logique de leur interaction.

DANS CETTE SECTION

COMPOSITION DES MODULES ET DES SOUS-SYSTEMES DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus inclut les composants suivants :

- Le **Serveur de sécurité** est un composant assurant la fonctionnalité antivirus. Lors de l'installation, le module s'intègre au serveur Microsoft ISA Server/Forefront TMG.
- La **Console d'administration** est un module représentant l'outil Microsoft Management Console (ci-après - MMC). La console offre l'accès à l'administration de Kaspersky Anti-Virus et au contrôle de son fonctionnement.
- La **Base de données de la sauvegarde et des statistiques** est une base de données sur le serveur SQL conçue pour conserver les informations statistiques sur l'utilisation de l'application et les informations sur les objets dangereux dont les copies sont placées dans la sauvegarde par Kaspersky Anti-Virus.

Les modules Serveur de sécurité et Console d'administration s'installent sur le serveur où est déployé le pare-feu de Microsoft ISA Server/Forefront TMG. La Console d'administration peut être aussi installée sur un ordinateur séparé ayant accès au serveur où est installé le module Serveur de sécurité. En cas d'utilisation par plusieurs administrateurs, la Console d'administration peut être installée sur l'ordinateur de chaque administrateur.

La présence de la console Microsoft ISA Server/Forefront TMG, installée sur l'ordinateur, est une exigence indispensable pour installer la Console d'administration de Kaspersky Anti-Virus.

Le composant Serveur de sécurité inclut les sous-systèmes suivants :

- Les **Filtres de Kaspersky Anti-Virus** interceptent le trafic via les protocoles HTTP, FTP, SMTP et POP3, téléchargent les objets demandés par des postes clients et redirigent les objets téléchargés dans le sous-système d'analyse. Les filtres transmettent au poste client les objets demandés après l'analyse et délivrent la notification sur le blocage de l'objet.

  L'application inclut les filtres suivants :

  - Le filtre Web de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole HTTP.

    L'analyse du trafic via le protocole HTTPS est aussi prévue pour Kaspersky Anti-Virus installé sur Forefront TMG. Pour que l'analyse du trafic HTTPS soit exécutée, il faut activer l'inspection du trafic dans la console d'administration de Forefront TMG.

  - Le filtre FTP de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole FTP.

- Le filtre SMTP de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole SMTP.
- Le filtre POP3 de Kaspersky Anti-Virus est responsable de l'interception du trafic via le protocole POP3.

Les filtres de Kaspersky Anti-Virus s'intègrent au pare-feu de Microsoft ISA Server/Forefront TMG lors de l'installation de l'application.

- Le **Sous-système d'analyse** est conçu pour l'analyse antivirus des objets. Le module d'analyse reçoit les objets téléchargés en provenance des filtres de Kaspersky Anti-Virus et les analyse à la recherche de la présence éventuelle de menaces. Le module utilise l'analyseur heuristique qui permet de détecter aussi les menaces inconnues. Après l'analyse, chaque objet se voit attribué un état qui détermine les actions suivantes à exécuter sur l'objet. Les objets sains sont ignorés sans modification, les autres sont traités conformément aux paramètres de l'analyse antivirus.
- Le **Sous-système de la mise à jour** assure la mise à jour des bases de Kaspersky Anti-Virus par leur téléchargement depuis les serveurs de mise à jour de Kaspersky Lab ou à partir d'autres sources indiquées.
- Le **Sous-système de la sauvegarde** assure la sauvegarde des copies de réserve des objets détectés par Kaspersky Anti-Virus durant l'analyse antivirus, ainsi que le transfert des informations sur les objets dans la Base de données de la sauvegarde et des statistiques. Ensuite, les objets de la Sauvegarde peuvent être supprimés ou enregistrés sur le disque local ou réseau. Les copies des objets sont enregistrées dans la Sauvegarde située sur le serveur où l'objet a été détecté. Les informations sur les objets placés dans la Sauvegarde sont enregistrées dans la Base de données de la sauvegarde et des statistiques.
- Le **Sous-système de configuration** assure la sauvegarde des paramètres de Kaspersky Anti-Virus.
- Le **Sous-système de licence** assure l'administration des clés et définit le statut de la licence de Kaspersky Anti-Virus. En cas de détection d'une violation du Contrat de licence, la fonctionnalité de Kaspersky Anti-Virus est limitée.
- Le **Sous-système de surveillance** assure la collecte des informations sur l'état de Kaspersky Anti-Virus.
- Le **Sous-système des statistiques** assure la collecte des statistiques sur les objets analysés. Les informations sont enregistrées dans la Base de données de la sauvegarde et des statistiques.
- Le **Sous-système de diagnostic** assure la gestion des journaux de fonctionnement de tous les modules de l'application. Les informations peuvent être enregistrées dans les fichiers texte, sauvegardées dans le journal des événements du système d'exploitation Microsoft Windows et transmises dans le sous-système des notifications Microsoft ISA Server/Forefront TMG
- Le **Sous-système des rapports** assure la réception des rapports sur les résultats du fonctionnement de Kaspersky Anti-Virus.

CONFIGURATION DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus peut fonctionner conjointement avec le pare-feu de Microsoft ISA Server/Forefront TMG dans les options de déploiement suivantes :

- Serveur autonome Microsoft ISA Server SE/EE ou Forefront TMG SE/EE.
- Groupe autonome des serveurs Forefront TMG EE sous l'administration du gestionnaire du groupe.
- Entreprise sur la base des serveurs Microsoft ISA Server EE ; un ou plusieurs groupes des serveurs Microsoft ISA EE sous l'administration de Configuration Storage Server (ci-après – CSS).
- Entreprise sur la base des serveurs Forefront TMG EE ; un ou plusieurs groupes des serveurs Forefront TMG EE sous l'administration de Enterprise Management Server (ci-après – EMS).
- Serveur Forefront TMG SE sous l'administration de EMS.

Les données de configuration de Kaspersky Anti-Virus s'enregistrent dans le stockage de configuration Microsoft ISA Server/Forefront TMG à l'installation de l'application. La configuration de Kaspersky Anti-Virus est partagée par niveaux logiques en conformité avec le partage par niveaux logiques de la configuration de Microsoft ISA Server/Forefront TMG.

En cas de déploiement de Kaspersky Anti-Virus dans l'entreprise, les paramètres de l'application sont répartis selon trois niveaux de configuration :

- niveau du serveur : paramètres applicables uniquement pour un serveur à part ;
- niveau de l'entreprise : paramètres applicables pour tous les serveurs du groupe sur lesquels Kaspersky Anti-Virus est installé.
- niveau de l'entreprise : paramètres applicables pour tous les serveurs de l'entreprise sur lesquels Kaspersky Anti-Virus est installé.

En cas de déploiement de Kaspersky Anti-Virus sur le serveur ou sur un groupe autonome, la configuration de l'application se compose de deux niveaux logiques : niveau du serveur et niveau du groupe.

La configuration du niveau du serveur se compose des paramètres de Kaspersky Anti-Virus qui dépendent des caractéristiques logicielles et matérielles du serveur sur lequel est installé le module Serveur de sécurité. Les autres paramètres de Kaspersky Anti-Virus concernent la configuration au niveau du groupe et de l'entreprise.

L'administration des paramètres de Kaspersky Anti-Virus est effectuée à l'aide de la Console d'administration qui se connecte au stockage de configuration de Microsoft ISA Server/Forefront TMG.

Les paramètres de Kaspersky Anti-Virus au niveau du serveur peuvent être configurés uniquement pour un serveur séparé parce qu'ils dépendent des caractéristiques matérielles et logicielles de l'ordinateur sur lequel l'application est installée. L'administration au niveau du groupe et/ou de l'entreprise est prévue pour d'autres paramètres de Kaspersky Anti-Virus. Les paramètres de Kaspersky Anti-Virus au niveau du groupe sont configurés de manière centralisée pour tous les serveurs inclus dans le groupe. Les paramètres de Kaspersky Anti-Virus du niveau de l'entreprise sont configurés de manière centralisée pour tous les serveurs de l'entreprise.

En cas de déploiement de l'application sur un serveur autonome, tous les paramètres sont configurés individuellement pour le serveur.

SCENARIOS D'ANALYSE DU TRAFIC PRIS EN CHARGE

Cette section décrit les particularités de fonctionnement de Kaspersky Anti-Virus dans les scénarios types suivants de trafic :

- Le client du réseau d'entreprise interne s'adresse aux ressources externes (outbound connection).
- Le client du réseau d'entreprise interne s'adresse aux ressources d'un autre réseau via le canal protégé (VPN) ;
- Le client en dehors du réseau d'entreprise s'adresse aux ressources situées dans le réseau d'entreprise interne et publiées par les outils Microsoft ISA Server/Forefront TMG (inbound connection) ;
- Le client en dehors du réseau d'entreprise, connecté via le canal protégé (VPN), s'adresse aux ressources internes du réseau d'entreprise.

Lorsque le client du réseau d'entreprise s'adresse aux ressources externes (outbound connection), l'analyse du trafic est exécutée de la manière suivante :

- Les objets téléchargés depuis les serveurs externes (download) sont analysés via les protocoles HTTP, HTTPS et FTP ; les objets téléchargés sur les serveurs externes ne sont pas analysés.

  Le trafic via le protocole HTTPS est analysé uniquement si Kaspersky Anti-Virus est installé sur le serveur Forefront TMG et si l'inspection du trafic HTTPS entrant est activée.

- Via les protocoles SMTP et POP3 : analyse de tous les messages transmis.

Lorsque le client du réseau d'entreprise s'adresse aux ressources d'un autre réseau via le canal protégé (VPN), l'analyse du trafic est exécutée de la même manière que lorsque le client du réseau d'entreprise s'adresse aux ressources externes.

Lorsque le client en dehors du réseau d'entreprise s'adresse aux ressources d'entreprise publiées (inbound connection), l'analyse du trafic est exécutée de la manière suivante :

- Via les protocoles HTTP, HTTPS et FTP : le trafic des ressources d'entreprise au client est analysé ; le trafic du client aux ressources d'entreprise n'est pas analysé.

  Le trafic via le protocole HTTPS est analysé uniquement si Kaspersky Anti-Virus est installé sur le serveur Forefront TMG et si l'inspection du trafic HTTPS sortant est activée.

- Via les protocoles SMTP et POP3 : analyse de tous les messages transmis.

Lorsque le client en dehors du réseau d'entreprise s'adresse aux ressources d'entreprise via le canal protégé (VPN), l'analyse du trafic est exécutée de la même manière que lorsque le client en dehors du réseau d'entreprise s'adresse aux ressources d'entreprise publiées (inbound connection).

L'analyse des protocoles de chaque type est configurée dans les paramètres de Kaspersky Anti-Virus et peut être désactivée.

INTERFACE DE L'APPLICATION

Cette section contient des informations sur les éléments principaux de l'interface graphique de la Console d'administration utilisée pour administrer les paramètres de Kaspersky Anti-Virus.

La Console d'administration représente un outil spécialisé, intégré dans Microsoft Management Console (MMC).

DANS CETTE SECTION

FENETRE PRINCIPALE

La fenêtre de la Console d'administration (ci-après – fenêtre principale) est composée des éléments suivants (cf. ill. ci-après) :

- Menu et barre d'outils : ils assurent l'administration du type console MMC et offrent l'accès au système d'aide de Kaspersky Anti-Virus. Le menu et la barre d'outils se trouvent dans la partie supérieure de la fenêtre principale.
- Arborescence de la console : c'est une structure hiérarchique située dans la partie gauche de la fenêtre principale. L'arborescence de la console affiche les entrées conçues pour travailler avec les paramètres de Kaspersky Anti-Virus.
- Le panneau des résultats affiche le contenu de l'entrée sélectionnée dans l'arborescence de la console. Le panneau des résultats est situé dans la partie droite de la fenêtre principale de l'application Après avoir apporté les modifications dans les paramètres de l'application, la partie supérieure du panneau des résultats affiche le bouton **Appliquer** conçue pour appliquer les modifications que vous avez apporté dans la configuration de Kaspersky Anti-Virus.

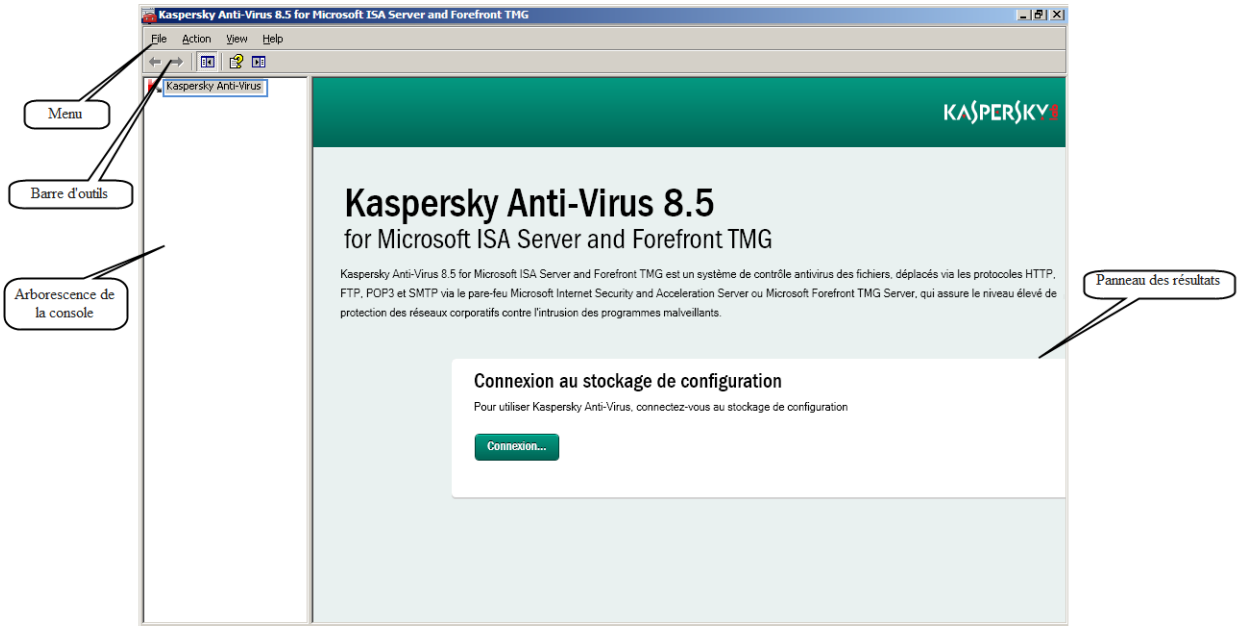

Illustration 1. Fenêtre principale

Si la connexion de la Console d'administration au stockage de configuration de Microsoft ISA Server/Forefront TMG n'est pas établie, l'arborescence de la console contient uniquement l'entrée racine **Kaspersky Anti-Virus** (cf. ill. ci-dessus). Le panneau des résultats de l'entrée affiche le bouton **Connexion** qui ouvre la fenêtre **Connexion au serveur de stockage de configuration** (cf. section "**Connexion de la Console d'administration au stockage de configuration**" à la page 42).

Entrées racine

Après la connexion au stockage de configuration de Microsoft ISA Server/Forefront TMG, l'arborescence de la console affiche les entrées racine suivantes qui correspondent au schéma de déploiement de Kaspersky Anti-Virus (cf. *Manuel d'implantation de Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*) :

- Schéma *Serveur autonome* : l'entrée du serveur. Le nom de l'entrée correspond au nom du serveur. Le panneau des résultats de l'entrée affiche les informations sur l'état de l'application sur le serveur (cf. ill. ci-après).

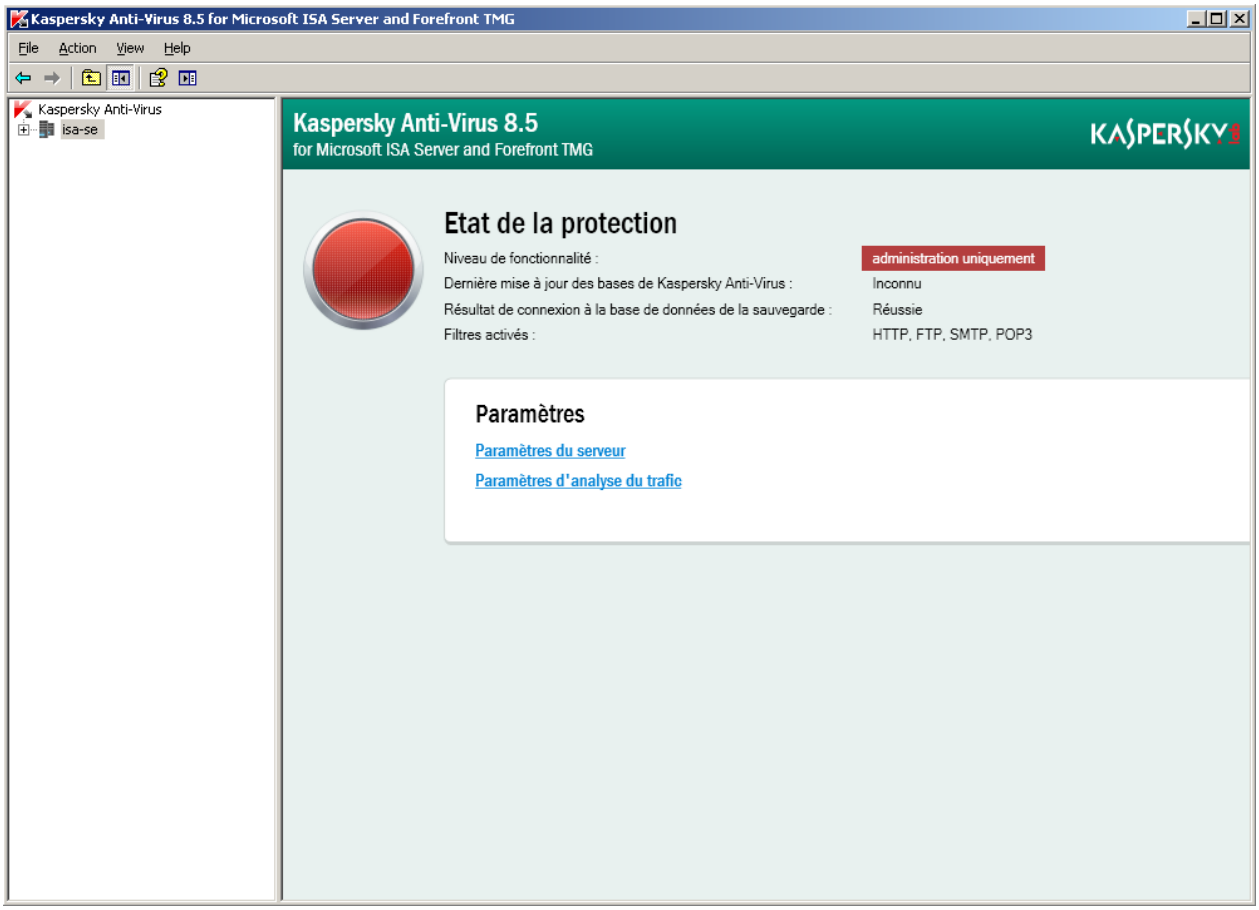

Illustration 2. Entrée du serveur (schéma de déploiement Serveur autonome)

- Schéma *Groupe Autonome* – l'entrée du groupe. Le nom de l'entrée correspond au nom du groupe. Le panneau des résultats de l'entrée affiche le tableau qui contient les informations sur les serveurs du groupe (cf. ill. ci-après).

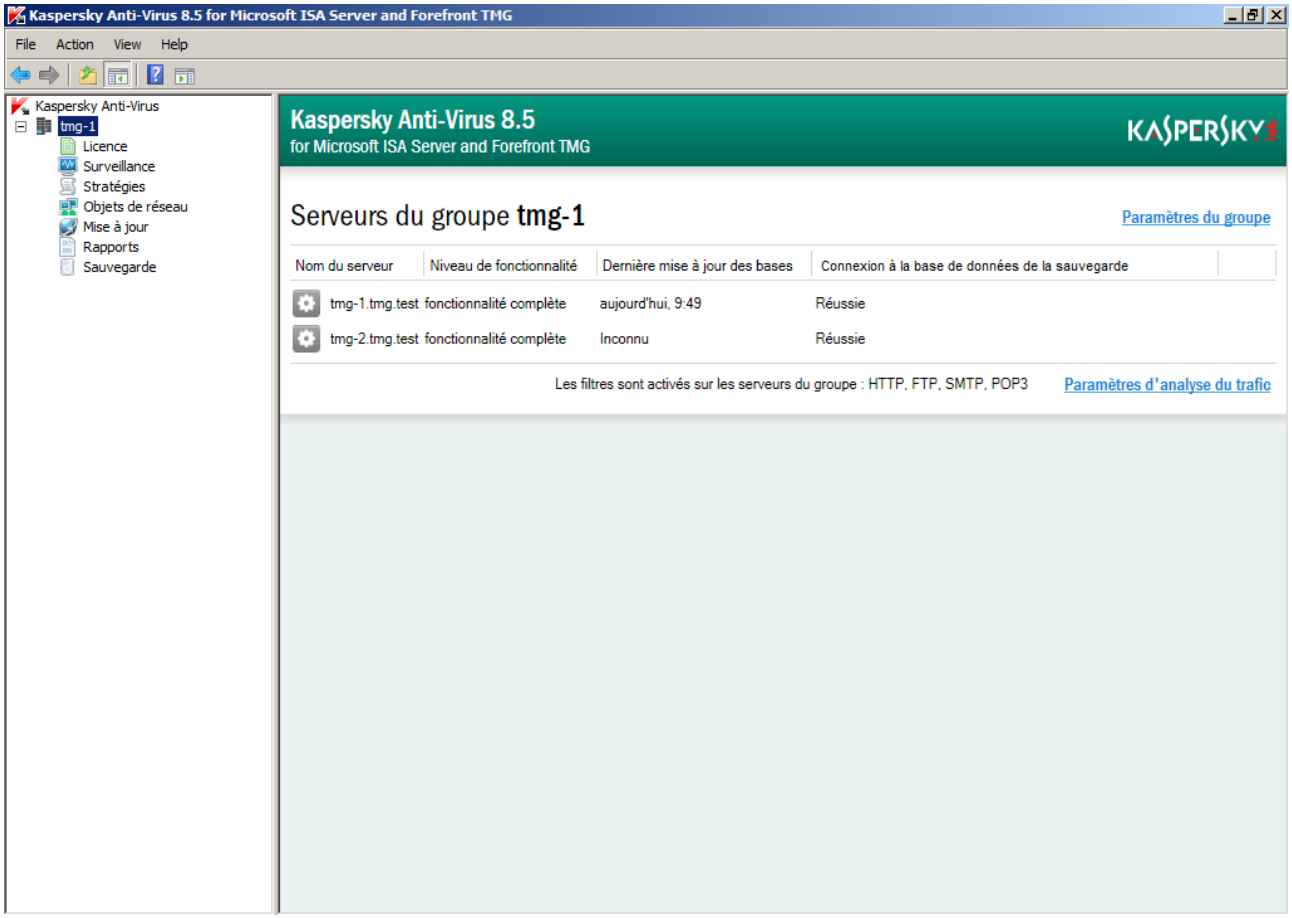

Illustration 3. Entrée du groupe (schéma de déploiement Groupe Autonome)

- Schéma *Entreprise* : l'entrée **Entreprise** et l'entrée **Groupes**. L'entrée **Groupes** inclut les entrées des groupes séparés qui font partie de l'entreprise. Le nom de l'entrée de chaque groupe correspond au nom du groupe.

La présence d'entrées de groupes séparés dans l'arborescence de la console dépend du rôle de l'utilisateur sous le compte duquel la connexion de la Console d'administration au stockage de configuration a été effectuée (cf. section "A propos du partage des privilèges d'utilisation de Kaspersky Anti-Virus" à la page 45). Pour l'utilisateur avec le rôle *Administrateur du groupe Microsoft ISA Server/Forefront TMG* ou *Auditeur du groupe Microsoft ISA Server/Forefront TMG*, l'arborescence de la console affiche uniquement les entrées des groupes dont il est l'administrateur/l'auditeur.

Le panneau des résultats des entrées racine **Entreprise** et **Groupes** affiche les panneaux déroulants suivants (cf. ill. ci-après) :

- Le panneau **Sauvegarde** contient des informations sur les Bases de données de la sauvegarde et des statistiques utilisées par Kaspersky Anti-Virus. Pour chaque Base de données de la sauvegarde et des statistiques, le panneau des résultats affiche le nom du serveur sur lequel la base de données, le nom de la base de données et l'état de connexion sont déployés, ainsi que le nombre et le volume total des objets dont les informations sont conservées dans cette base de données.

- Panneaux déroulants des informations sur les groupes. Chaque panneau déroulant d'informations sur le groupe correspond au groupe qui fait partie de l'entreprise et contient des informations sur les serveurs du groupe.

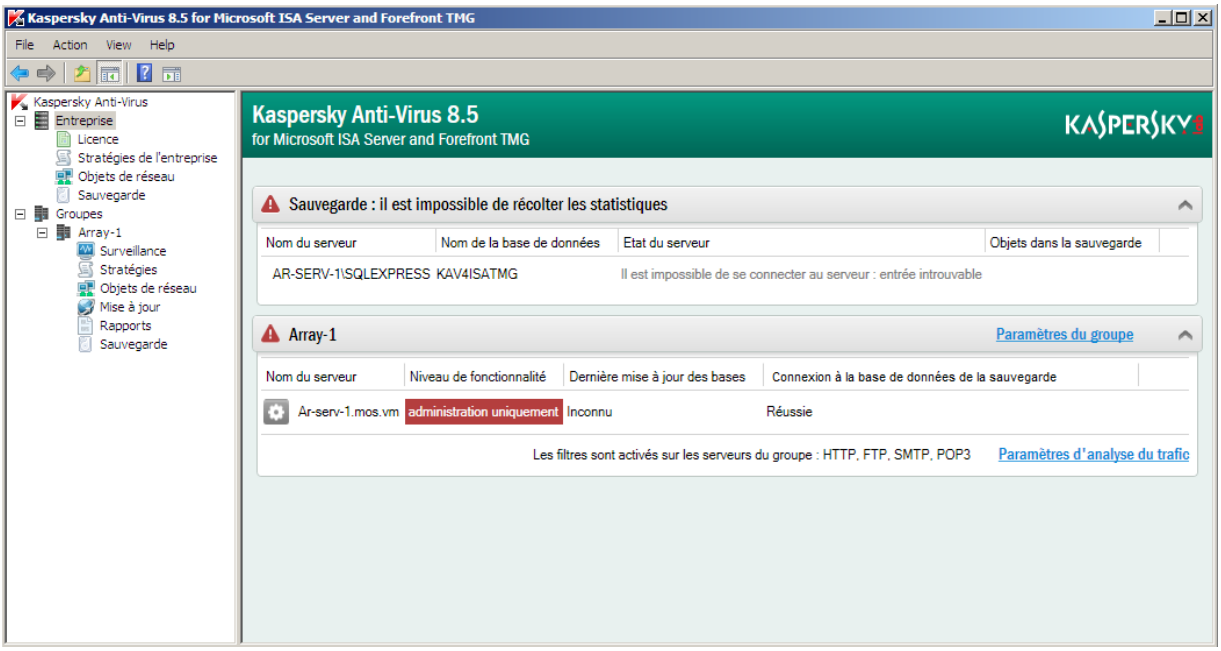

Illustration 4. Entrée Entreprise (schéma de déploiement Entreprise)

Les informations suivantes sont présentées dans le panneau des résultats de l'entrée **Serveur autonome**, dans le tableau avec les informations sur l'état de Kaspersky Anti-Virus sur les serveurs du groupe autonome, ainsi que dans les panneaux déroulants des informations sur les groupes de l'entreprise :

- Le nom du serveur (pour les schémas de déploiement *Groupe Autonome* et *Entreprise*).
- Niveau de fonctionnalité : le niveau de fonctionnalité de Kaspersky Anti-Virus qui indique la présence ou l'absence des restrictions dans le fonctionnement de l'application sur le serveur. Le niveau de fonctionnalité dépend de l'état de la licence et des bases de Kaspersky Anti-Virus.
- Dernière mise à jour des bases : la date et l'heure de la dernière mise à jour des bases de Kaspersky Anti-Virus. Si les bases de Kaspersky Anti-Virus sont dépassées ou une erreur s'est produite pendant leur mise à jour, un avertissement s'affiche.
- Connexion à la base de données de la sauvegarde : le résultat de la connexion de Kaspersky Anti-Virus à la Base de données de la sauvegarde et des statistiques.
- Liste des filtres activés de Kaspersky Anti-Virus.

> En cas d'absence de connexion de la Console d'administration au serveur, la description de l'erreur de connexion s'affiche à la place du niveau de fonctionnalité et des informations sur la mise à jour des bases et sur le résultat de la connexion à la Base de données de la sauvegarde et des statistiques.

Entrées jointes

Les entrées racine contiennent les entrées jointes suivantes conçues pour administrer les différents paramètres de Kaspersky Anti-Virus :

- **Licence** : l'entrée est conçue pour gérer les clés et consulter les informations sur la licence active (cf. section "Licence de l'application" à la page 27).
- **Surveillance** : le panneau des résultats de cette entrée affiche les statistiques de fonctionnement de l'application, les informations sur le niveau de fonctionnalité de l'application et sur l'état des bases de Kaspersky Anti-Virus (cf. section "Etat de la protection" à la page 35).

- **Stratégies** : l'entrée permet de fixer les règles de traitement des protocoles, les règles d'exclusion de l'analyse et les règles d'analyse antivirus, qui déterminent les réactions aux menaces lors de l'analyse des différents objets de réseau et protocoles (cf. section "Opération sur les règles des stratégies" à la page 63).

  Si le schéma de déploiement **Entreprise** est utilisé, l'arborescence de la console contient deux entrées conçues pour la configuration des règles des stratégies de Kaspersky Anti-Virus :

  - l'entrée **Stratégies** qui fait partie de l'entrée du groupe : pour la configuration des règles des stratégies au niveau du groupe ;
  - l'entrée **Stratégies de l'entreprise** qui fait partie de l'entrée **Entreprise** : pour la configuration des règles des stratégies au niveau de l'entreprise.

  En cas d'utilisation du schéma de déploiement *Entreprise*, le panneau des résultats de l'entrée **Stratégies**, qui fait partie de l'entrée du groupe, affiche les règles des stratégies de deux niveaux : groupe et entreprise. Dans ce cas, seules les règles des stratégies au niveau du groupe peuvent être modifiées. La manipulation des règles des stratégies du niveau de l'entreprise est effectuée dans l'entrée **Stratégies de l'entreprise** qui fait partie de l'entrée **Entreprise**.

- **Objets de réseau** : l'entrée permet de configurer les objets de réseau utilisés lors de la formation des stratégies de Kaspersky Anti-Virus (cf. section "Opération sur les objets de réseau" à la page 59).

  Si le schéma de déploiement *Entreprise* est utilisé, l'arborescence de la console contient deux entrées conçues pour la configuration des objets de réseau :

  - l'entrée **Objets de réseau** qui fait partie de l'entrée du groupe : pour configurer les objets de réseau utilisés lors de la formation des stratégies de Kaspersky Anti-Virus au niveau du groupe ;
  - l'entrée **Objets de réseau** qui fait partie de l'entrée **Entreprise** : pour configurer les objets de réseau qui peuvent être utilisés lors de la formation des stratégies de Kaspersky Anti-Virus comme niveau de l'entreprise et comme niveau du groupe.

  En cas d'utilisation du schéma de déploiement *Entreprise*, le panneau des résultats de l'entrée **Objets de réseau**, qui fait partie de l'entrée du groupe, affiche les objets de réseau de deux niveaux : groupe et entreprise. Dans ce cas, seuls les objets de réseau au niveau du groupe peuvent être modifiés. La manipulation des objets de réseau du niveau de l'entreprise est effectuée dans l'entrée **Objets de réseau** qui fait partie de l'entrée **Entreprise**.

- **Mise à jour** : l'entrée est conçue pour consulter les informations sur l'état des bases de Kaspersky Anti-Virus et de lancement de la procédure de mise à jour des bases (cf. section "Mise à jour des bases" à la page 47). Le panneau des résultats de l'entrée **Mise à jour** affiche le lien **Paramètres de mise à jour des bases de Kaspersky Anti-Virus**. La consultation et la configuration des paramètres de mise à jour des bases de Kaspersky Anti-Virus s'effectuent dans la fenêtre de configuration de l'application (cf. section "Fenêtres de configuration de l'application" à la page 24).

- **Rapports** : l'entrée est conçue pour configurer les tâches de formation des rapports et d'obtention des rapports sur le fonctionnement de Kaspersky Anti-Virus (cf. section "Rapports" à la page 89).

- **Sauvegarde** : l'entrée permet de consulter les informations sur les objets placés dans la sauvegarde sur le serveur et d'exécuter les opérations sur les objets de la sauvegarde (cf. section "Sauvegarde" à la page 78).

  Si le schéma de déploiement utilisé est *Entreprise*, l'arborescence de la console contient deux entrées conçues pour travailler avec les objets de la sauvegarde :

  - l'entrée **Sauvegarde** qui fait partie de l'entrée du groupe : pour travailler avec les objets placés dans la sauvegarde sur tous les serveurs du groupe ;
  - l'entrée **Sauvegarde** qui fait partie de l'entrée **Entreprise** : pour travailler avec les objets placés dans la sauvegarde sur tous les serveurs de l'entreprise.

  Le panneau des résultats de l'entrée **Sauvegarde**, qui fait partie de l'entrée du serveur et de l'entrée du groupe, affiche le lien **Paramètres**. La configuration des paramètres de la sauvegarde s'effectue dans la fenêtre de configuration de l'application (cf. section "Fenêtres de configuration de l'application" à la page 24).

FENETRE DE CONFIGURATION DE L'APPLICATION

Pour configurer les paramètres de Kaspersky Anti-Virus et les paramètres d'administration de l'application, les fenêtres suivantes sont prévues :

- La fenêtre **Paramètres du serveur** (cf. section "**Fenêtre Paramètres du serveur. Navigation**" à la page 24).
- La fenêtre **Paramètres du groupe** (cf. section "**Fenêtre Paramètres du groupe. Navigation**" à la page 25).
- La fenêtre **Paramètres d'analyse** (cf. section "**Fenêtre Paramètres d'analyse. Navigation**" à la page 26).

DANS CETTE SECTION

FENETRE PARAMETRES DU SERVEUR. NAVIGATION

L'ensemble des onglets de la fenêtre **Paramètres du serveur** dépend du schéma de déploiement de Kaspersky Anti-Virus :

- Si les schémas de déploiement *Groupe Autonome* et *Entreprise* sont utilisés, la fenêtre **Paramètres du serveur** est conçue pour configurer les paramètres de fonctionnement de Kaspersky Anti-Virus sur chaque serveur séparé.

  Dans ce cas, les paramètres suivants sont configurés dans la fenêtre **Paramètres du serveur** :

  - L'onglet **Général** sert à configurer la taille de la sauvegarde sur le serveur (cf. section "Configuration de la taille de la sauvegarde sur le serveur" à la page 84).
  - L'onglet **Productivité** sert à configurer les paramètres de productivité de l'analyse antivirus (cf. section "Configuration des paramètres. Productivité de l'analyse" à la page 76).

- Si le schéma de déploiement *Serveur autonome* est utilisé, les paramètres suivants sont aussi configurés dans la fenêtre **Paramètres du serveur** :

  - L'onglet **Mise à jour** sert à configurer les paramètres de mises à jour des bases de Kaspersky Anti-Virus sur le serveur (cf. section "Mise à jour des bases" à la page 47).
  - L'onglet **Sauvegarde** sert à configurer les paramètres de connexion à la Base de données de la sauvegarde et des statistiques (cf. section "Configuration des paramètres de connexion à la Base de données de la sauvegarde et des statistiques" à la page 85).
  - L'onglet **Journaux** sert à configurer les paramètres de gestion des journaux de fonctionnement de l'application (cf. section "Diagnostic" à la page 86).

Le mode d'accès à la fenêtre **Paramètres du serveur** dépend du schéma de déploiement de Kaspersky Anti-Virus.

Schéma de déploiement Serveur autonome

➧ *Pour passer à la fenêtre **Paramètres du serveur**, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).
2. Sélectionnez l'entrée du serveur dans l'arborescence de la console.
3. Ouvrez la fenêtre **Paramètres du serveur** à l'aide du lien **Paramètres du serveur** situé dans le panneau des résultats.

Schémas de déploiement Groupe Autonome et Entreprise

*Pour passer à la fenêtre **Paramètres du serveur**, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).
2. Sélectionnez une des entrées suivantes dans l'arborescence de la console :
   - Si le schéma utilisé est *Groupe Autonome :* l'entrée du groupe ;
   - Si le schéma utilisé est *Entreprise :* l'entrée **Entreprise**, l'entrée **Groupes** ou l'entrée du groupe séparé.
3. Dans le panneau déroulant des informations sur le groupe ou dans le tableau comportant la liste des serveurs du groupe, cliquez sur le bouton **Configuration**  situé à gauche du nom du serveur dont vous souhaitez consulter et configurer les paramètres.

FENETRE PARAMETRES DU GROUPE. NAVIGATION

La fenêtre **Paramètres du groupe** est utilisée dans le cas des schémas de déploiement *Groupe Autonome* et *Entreprise*.

La fenêtre **Paramètres du groupe** est conçue pour configurer les paramètres de fonctionnement de Kaspersky Anti-Virus appliqués pour tous les serveurs d'un groupe.

Les paramètres suivants sont configurés dans la fenêtre **Paramètres du groupe** :

- L'onglet **Mise à jour** sert à configurer les paramètres de mises à jour des bases de Kaspersky Anti-Virus sur les serveurs du groupe (cf. section "Mise à jour des bases" à la page 47).
- L'onglet **Sauvegarde** sert à configurer les paramètres de connexion à la Base de données de la sauvegarde et des statistiques (cf. section "Configuration des paramètres de connexion à la Base de données de la sauvegarde et des statistiques" à la page 85).
- L'onglet **Journaux** sert à configurer les paramètres de gestion des journaux de fonctionnement de l'application (cf. section "Diagnostic" à la page 86).

*Pour passer à la fenêtre **Paramètres du groupe**, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).
2. Sélectionnez une des entrées suivantes dans l'arborescence de la console :
   - si le schéma de déploiement utilisé est *Groupe Autonome* : l'entrée du groupe ;
   - si le schéma de déploiement utilisé est *Entreprise* : l'entrée **Entreprise**, l'entrée **Groupes** ou l'entrée du groupe séparé.
3. Ouvrez la fenêtre **Paramètres du groupe** à l'aide du lien **Paramètres du groupe** situé dans l'en-tête du panneau déroulant des informations sur le groupe ou au-dessus du tableau avec la liste des serveurs du groupe.

FENETRE PARAMETRES D'ANALYSE. NAVIGATION

La fenêtre **Paramètres d'analyse** est conçue pour configurer les paramètres d'analyse du trafic transmis via les protocoles HTTP, FTP, POP3 et SMTP (cf. section "Configuration des paramètres. Analyse du trafic transmis via les protocoles" à la page 74).

La configuration des paramètres d'analyse du trafic pour chaque protocole est effectuée sur l'onglet séparé de la fenêtre **Paramètres d'analyse**.

Le mode d'accès à la fenêtre **Paramètres d'analyse** dépend du schéma de déploiement de Kaspersky Anti-Virus utilisé.

Schéma de déploiement Serveur autonome

*Pour passer à la fenêtre **Paramètres d'analyse**, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).
2. Sélectionnez l'entrée du serveur dans l'arborescence de la console.
3. Ouvrez la fenêtre **Paramètres d'analyse** à l'aide du lien **Paramètres d'analyse du trafic** situé dans le panneau des résultats.

Schémas de déploiement Groupe Autonome et Entreprise

*Pour passer à la fenêtre **Paramètres d'analyse**, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).
2. Sélectionnez une des entrées suivantes dans l'arborescence de la console :
   - Si le schéma utilisé est *Groupe Autonome :* l'entrée du groupe ;
   - Si le schéma utilisé est *Entreprise :* l'entrée **Entreprise**, l'entrée **Groupes** ou l'entrée du groupe séparé.
3. Ouvrez la fenêtre **Paramètres d'analyse** à l'aide du lien **Paramètres d'analyse du trafic** situé dans l'en-tête du panneau déroulant des informations sur le groupe ou du tableau avec la liste des serveurs du groupe.

LICENCE DE L'APPLICATION

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du Contrat de licence, les types de licence, les modes d'activation de l'application et le renouvellement de la licence.

DANS CETTE SECTION

A PROPOS DU CONTRAT DE LICENCE

Le Contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Lisez attentivement le Contrat de licence avant de commencer à utiliser l'application.

Il est considéré que vous acceptez les conditions du Contrat de licence lorsque vous confirmez votre accord avec le texte du Contrat de licence au moment de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application ou ne pas utiliser l'application.

A PROPOS DE LA LICENCE

La *licence* est un droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence.

Dans le cas de la présence du contrat de licence ou du document semblable, les conditions d'utilisation de l'application citées dans ce contrat dominent sur les conditions du Contrat de licence avec l'utilisateur final.

La licence inclut les privilèges suivants :

- Le privilège d'utilisation de l'application pour analyser le trafic d'un ou de plusieurs utilisateurs.

  Le nombre d'utilisateurs dont le trafic est analysé par Kaspersky Anti-Virus est défini par les conditions du Contrat de licence.

- Le privilège de contacter le Support Technique de Kaspersky Lab.

Le volume de services offerts et la durée d'utilisation de l'application dépendent du type de licence utilisée pour activer l'application.

Il existe les types suivants de licences :

- *Evaluation* : une licence gratuite conçue pour découvrir l'application.

  La licence d'évaluation possède une courte durée de validité. Une fois la licence arrivée à expiration, Kaspersky Anti-Virus arrête de remplir toutes ces fonctions. Pour pouvoir continuer à utiliser l'application, il faut acheter une licence commerciale.

- *Commerciale* : une licence payante fournie lors de l'achat de l'application.

  Une fois que la licence commerciale arrive à expiration, l'application continue à fonctionner mais ses fonctionnalités sont réduites. Vous pouvez toujours utiliser tous les composants de l'application et exécuter l'analyse pour rechercher la présence de virus et d'autres programmes qui présentent une menace mais uniquement à l'aide des bases installées avant l'expiration de la licence. Pour poursuivre l'utilisation de toutes les fonctionnalités de Kaspersky Anti-Virus, il faut renouveler la licence commerciale.

  Il est conseillé de renouveler la licence avant son expiration afin de garantir la protection maximale contre toutes les menaces pour la sécurité d'ordinateur.

A PROPOS DU FICHIER CLE

Fichier clé est un fichier de type xxxxxxx.key. Le fichier clé est fourni à l'achat de l'application. Le fichier clé est indispensable à l'utilisation de l'application.

Si le fichier clé a été supprimé par inadvertance, pour le restaurer vous pouvez envoyer une demande au Support Technique (cf. section "Contacter le Support Technique" à la page 97).

Le fichier clé contient des informations suivantes :

- La clé est une suite unique composée de chiffres et de lettres. La clé sert, par exemple, à recevoir l'assistance technique de Kaspersky Lab.

- La restriction sur le nombre d'utilisateurs est le nombre maximal d'utilisateurs dont les requêtes aux ressources externes depuis le réseau corporatif ou aux ressources internes en dehors du réseau corporatif sont analysées par Kaspersky Anti-Virus après l'activation sur le serveur Microsoft ISA Server/Forefront TMG à l'aide de ce fichier clé.

- Date de création du fichier clé.

- La durée de validité de la licence est la durée d'utilisation de l'application prévue dans le Contrat de licence et décomptée à partir de la date de première activation de l'application à l'aide de ce fichier clé. Par exemple, 1 an.

  La durée de validité de la licence expire avant le délai périssable du fichier clé à l'aide duquel la clé active a été ajoutée.

- Le délai périssable du fichier clé est un délai défini à compter de la date de création du fichier clé. Le délai périssable du fichier clé peut être de plusieurs années. Il est possible d'activer l'application à l'aide de ce fichier clé uniquement avant l'expiration de ce délai.

  Le délai périssable du fichier clé expire si la durée de validité de la licence sur l'utilisation de l'application, activée à l'aide de ce fichier clé, a expiré.

AJOUT DE LA CLE

Pour activer l'application ou renouveler la licence, il faut ajouter une clé. Pour ce faire, le fichier clé (cf. section "A propos du fichier clé" à la page 28) est utilisé.

Si l'application n'est pas activée, seule l'administration de Kaspersky Anti-Virus est disponible. La vérification du trafic et la mise à jour des bases de Kaspersky Anti-Virus ne sont pas exécutées.

A l'expiration de la licence d'évaluation, l'administration de Kaspersky Anti-Virus est disponible uniquement. La vérification du trafic et la mise à jour des bases de Kaspersky Anti-Virus ne sont pas exécutées.

A l'expiration de la licence commerciale, l'analyse du trafic est effectuée à l'aide des bases de Kaspersky Anti-Virus présentes au moment de l'expiration de la licence. La mise à jour des bases n'est pas effectuée.

Kaspersky Anti-Virus permet d'ajouter deux clés. La clé ajoutée en premier devient une clé *active*. La présence de la clé active assure la fonctionnalité complète de l'application. La deuxième clé devient une clé supplémentaire. La *clé supplémentaire* devient une clé active soit à l'expiration de la clé active, soit lors de la suppression de la clé active. La présence de la clé supplémentaire permet d'éviter les restrictions de fonctionnalité de l'application au moment de l'expiration de la licence.

Si la clé active se retrouve dans la liste noire, la mise à jour des bases antivirus est effectuée tandis que l'analyse du trafic ne l'est pas. Cette clé peut être supprimée (cf. section "Suppression de la clé" à la page 31) ou remplacée par une autre clé (cf. section "Changement de la clé" à la page 31).

Pour ajouter une clé active ou supplémentaire, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - si le schéma de déploiement utilisé est *Entreprise*, déployez l'entrée **Entreprise** et sélectionnez l'entrée jointe **Licence** (cf. section "**Fenêtre principale**" à la page 19).

   - si le schéma de déploiement utilisé est *Serveur autonome* ou *Groupe autonome*, déployez l'entrée du groupe/du serveur et sélectionnez l'entrée jointe **Licence** (cf. section "**Fenêtre principale**" à la page 19).

3. Dans le panneau des résultats, cliquez sur le bouton **Ajouter**.

4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier clé (fichier avec l'extension key).

   Les informations sur la clé ajoutée s'afficheront dans le panneau des résultats de l'entrée **Licence** (cf. section "**Obtention des informations sur les clés**" à la page 30).

   La clé supplémentaire doit satisfaire les conditions suivantes : ne pas être ajoutée en tant que clé active et ne doit pas expirer avant la clé active. Si la clé ne satisfait pas les conditions indiquées, un message d'erreur s'affiche. Il n'est pas recommandé d'utiliser la clé de la version d'essai comme clé supplémentaire.

5. Pour que les modifications entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

OBTENTION DES INFORMATIONS SUR LES CLES

L'emplacement des informations sur les clés dépend du schéma de déploiement de Kaspersky Anti-Virus.

Schéma de déploiement *Serveur autonome*

➧ *Pour consulter les informations sur les clés, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée du serveur et sélectionnez l'entrée jointe **Licence** (cf. section "**Fenêtre principale**" à la page 19).

   Les informations sur les clés ajoutées apparaîtront dans le panneau des résultats.

Schéma de déploiement *Groupe Autonome*

➧ *Pour consulter les informations sur les clés, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée du groupe et sélectionnez l'entrée jointe **Licence** (cf. section "**Fenêtre principale**" à la page 19).

   Les informations sur les clés ajoutées apparaîtront dans le panneau des résultats.

Schéma de déploiement *Entreprise*

➧ *Pour consulter les informations sur les clés, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée **Entreprise** et sélectionnez l'entrée jointe **Licence** (cf. section "**Fenêtre principale**" à la page 19).

   Les informations sur les clés ajoutées apparaîtront dans le panneau des résultats.

Les informations suivantes sur la clé active s'affichent dans le panneau des résultats :

- **Clé**.

  Séquence unique de lettres et de chiffres au format XXXX-XXXXXX-XXXXXXXX.

- **Type de licence**.

  Type de licence.

  Les types de licence suivants sont prévus pour Kaspersky Anti-Virus :

  - **Commerciale**. La licence payante avec la durée de validité définie lors de l'achat de Kaspersky Anti-Virus.
  - **Evaluation**. Licence gratuite avec durée de validité limitée conçue pour découvrir Kaspersky Anti-Virus.

- **Restriction**.

  Le nombre maximal d'utilisateurs dont les requêtes aux ressources externes depuis le réseau corporatif ou aux ressources internes en dehors du réseau corporatif sont analysées par Kaspersky Anti-Virus conformément à la restriction de licence.

- **Date d'expiration**.

  Date d'expiration de la licence.

- **Etat de la licence**.

  Etat de la licence de Kaspersky Anti-Virus. Valeurs du champ possibles :

  - **Licence actuelle**. La licence n'a pas expiré, elle est active.
  - **La durée de validité de la licence a expiré**. La licence a expiré, les fonctionnalités de Kaspersky Anti-Virus sont limitées.

- **Utilisateur**.

  Le nom de l'utilisateur ayant conclu le contrat de licence. La valeur de ce champ peut être différente du nom de l'utilisateur de la Console d'administration.

Pour la clé supplémentaire, le panneau des résultats affiche les informations relatives au contrat de licence et à la date d'expiration (calculée en prenant compte de la date d'expiration de la clé active).

CHANGEMENT DE LA CLE

Vous pouvez changer la clé active. Ceci permet d'éviter la restriction temporaire des fonctionnalités de l'application, par exemple, en cas de suppression successive de la clé et d'ajout d'une nouvelle clé.

Pendant le processus de remplacement de la clé, toutes les fonctionnalités de l'application sont disponibles.

Tous les changements apportés entreront en vigueur uniquement après l'application des modifications de la configuration.

SUPPRESSION DE LA CLE

Vous pouvez supprimer la clé active ou supplémentaire. Lors de la suppression de la clé active, la clé supplémentaire devient automatiquement active.

Si vous avez supprimé la clé active mais que la clé supplémentaire n'a pas été ajoutée, la fonctionnalité de l'application est limitée. Seule l'administration de l'application est accessible.

Tous les changements apportés entreront en vigueur uniquement après l'application des modifications de la configuration.

CONFIGURATION D'UNE NOTIFICATION SUR L'EXPIRATION DE LA DUREE DE VALIDITE DE LA LICENCE

L'application vérifie la durée de validité de la licence après chaque mise à jour des bases et à minuit chaque jour selon l'heure locale du serveur sur lequel Kaspersky Anti-Virus est installé.

Lorsque la date d'expiration de la licence approche, l'enregistrement correspondant est porté au Journal de fonctionnement de l'application kavisaYYYYMMDD.log, et si les paramètres de notifications d'ISA Server ou de Forefront TMG sont configurés, un message électronique est envoyé à l'adresse indiquée lors de la configuration. Par défaut, la notification est envoyée 30 jours avant l'expiration de la licence. Vous pouvez modifier le délai de la notification.

Pour configurer les paramètres de notification sur l'expiration de la licence, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - si le schéma de déploiement *Entreprise* est utilisé, déployez l'entrée **Entreprise** et sélectionnez l'entrée jointe **Licence** (cf. section "**Fenêtre principale**" à la page 19).

   - si le schéma de déploiement *Serveur autonome* ou *Groupe autonome* est utilisé, déployez l'entrée du groupe/du serveur et sélectionnez l'entrée jointe **Licence** (cf. section "**Fenêtre principale**" à la page 19).

3. A l'aide du lien **Configurer** situé dans la partie inférieure du panneau des résultats, ouvrez la fenêtre **Paramètres de notifications**.

4. Si vous voulez que les notifications soient consignées dans le fichier du Journal de fonctionnement de l'application kavisaYYYYMMDD.log, cochez la case **Signaler l'expiration de la licence** et définissez le nombre de jours dans le champ de saisie **Jours**.

5. Cliquez sur le bouton **OK**. La fenêtre **Paramètres de notifications** se ferme. Les enregistrements sur l'expiration de la licence seront portés au journal de fonctionnement de l'application chaque jour, à compter du jour de début du délai défini de la notification.

6. Pour que les modifications entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

Pour obtenir des notifications par courrier électronique, il faut configurer les paramètres de notifications d'ISA Server ou de Forefront TMG.

LANCEMENT ET ARRET DE L'APPLICATION

Après l'installation de l'application, le service *Kaspersky Anti-Virus 8.5 for ISA Server et Forefront TMG* (kavisasrv.exe) se lance automatiquement, en assurant le fonctionnement de Kaspersky Anti-Virus.

Pour arrêter Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la console d'administration Microsoft ISA Server / Forefront TMG.
2. Sélectionnez une des entrées suivantes dans l'arborescence de la console :
   - si le schéma utilisé est *Serveur autonome :* l'entrée du serveur ;
   - si le schéma utilisé est *Groupe Autonome* ou *Entreprise :* l'entrée du groupe.
3. Exécutez une des actions suivantes :
   - si Kaspersky Anti-Virus fonctionne avec le serveur de Forefront TMG, sélectionnez l'entrée **Système** ;
   - si Kaspersky Anti-Virus fonctionne avec le serveur de Microsoft ISA Server, sélectionnez l'entrée **Configuration**, puis l'entrée jointe **Paramètres**.
4. Dans le panneau des résultats, sélectionnez l'onglet **Filtres Web** et activez le filtre Web de Kaspersky Anti-Virus à l'aide de la commande du menu contextuel **Désactiver**.
5. Sélectionnez l'onglet **Filtres des applications** et activez le filtre FTP de Kaspersky Anti-Virus, le filtre POP3 de Kaspersky Anti-Virus et le filtre SMTP de Kaspersky Anti-Virus à l'aide de la commande du menu contextuel **Désactiver**.
6. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées. Dans la boîte de dialogue qui s'ouvre, sélectionnez l'option d'enregistrement des modifications accompagnée du redémarrage des services Microsoft ISA Server/Forefront TMG et cliquez sur le bouton **OK**.
7. Arrêtez le service *Kaspersky Anti-Virus 8.5 for ISA Server et Forefront TMG* dans le gestionnaire des services Microsoft Windows. Kaspersky Anti-Virus sera arrêté.

   Si vous arrêtez le service de Kaspersky Anti-Virus sans désactiver les filtres dans Microsoft ISA Server/Forefront TMG, alors le service démarrera automatiquement dans un certain temps après l'arrêt.

Suite à l'arrêt de Kaspersky Anti-Virus, le trafic passant par les protocoles HTTP, FTP, SMTP et POP3, est transmis sans analyse.

Pour lancer Kaspersky Anti-Virus après l'arrêt, procédez comme suit :

1. Ouvrez la console d'administration Microsoft ISA Server / Forefront TMG.
2. Sélectionnez une des entrées suivantes dans l'arborescence de la console :
   - si le schéma utilisé est *Serveur autonome :* l'entrée du serveur ;
   - si le schéma utilisé est *Groupe Autonome* ou *Entreprise :* l'entrée du groupe.

3. Exécutez une des actions suivantes :

   - si Kaspersky Anti-Virus fonctionne avec le serveur Forefront TMG, sélectionnez l'entrée **Système** ;

   - si Kaspersky Anti-Virus fonctionne avec le serveur de Microsoft ISA Server, sélectionnez l'entrée **Configuration**, puis l'entrée jointe **Paramètres**.

4. Dans le panneau des résultats, sélectionnez l'onglet **Filtres des applications** et activez le filtre FTP de Kaspersky Anti-Virus, le filtre POP3 de Kaspersky Anti-Virus et le filtre SMTP de Kaspersky Anti-Virus à l'aide de la commande du menu contextuel **Activer**.

5. Sélectionnez l'onglet **Filtres Web** et activez le filtre Web de Kaspersky Anti-Virus à l'aide de la commande du menu contextuel **Activer**.

6. Cliquez sur le bouton **Appliquer** pour enregistrer les modifications apportées. Dans la boîte de dialogue qui s'ouvre, sélectionnez l'option d'enregistrement des modifications accompagnée du redémarrage des services Microsoft ISA Server/Forefront TMG et cliquez sur le bouton **OK**.

Après l'activation des filtres, le service *Kaspersky Anti-Virus 8.5 for ISA Server et Forefront TMG* se lance automatiquement. Quand le service est lancé, Kaspersky Anti-Virus exécute l'analyse du trafic transmis via les protocoles HTTP, FTP, SMTP et POP3.

ETAT DE PROTECTION

Dans le panneau des résultats de l'entrée **Surveillance**, vous pouvez consulter les informations relatives à l'état de la licence, à la mise à jour des bases de Kaspersky Anti-Virus ainsi qu'aux statistiques de fonctionnement des filtres de Kaspersky Anti-Virus.

Pour consulter les statistiques de fonctionnement de l'application ainsi que les informations relatives à la licence et à l'état des bases de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - Si le schéma de déploiement utilisé est *Serveur autonome*, déployez l'entrée du serveur et sélectionnez l'entrée jointe **Surveillance** (cf. section "**Fenêtre principale**" à la page 19).

   - Si le schéma de déploiement utilisé est *Groupe autonome* ou *Entreprise*, déployez l'entrée du groupe et sélectionnez l'entrée jointe **Surveillance** (cf. section "**Fenêtre principale**" à la page 19).

Le panneau des résultats affiche les blocs d'information suivants : le bloc **Licence** (à la page 35), le bloc **Mise à jour des bases de Kaspersky Anti-Virus** (à la page 37), le bloc **Statistiques de fonctionnement des filtres en une semaine** (à la page 38).

DANS CETTE SECTION

BLOC LICENCE

Le contenu du bloc **Licence** dépend du schéma de déploiement de Kaspersky Anti-Virus utilisé.

Schéma de déploiement *Serveur autonome*

- **Fonctionnalité**.

  Niveau de fonctionnalité de l'application.

  Les options suivantes sont proposées :

  - **Fonctionnement complet**. Aucune restriction n'est imposée sur le fonctionnement de l'application.
  - **Mise à jour uniquement**. La clé fait partie de la liste noire. Seule la mise à jour des bases est disponible, le trafic n'est pas analysé.
  - **Administration uniquement**. La clé active de Kaspersky Anti-Virus n'est pas ajoutée ou la licence d'évaluation a expiré. Seule l'administration de Kaspersky Anti-Virus est disponible, le trafic n'est pas analysé et la mise à jour des bases n'est pas disponible.
  - **Mise à jour non disponible**. La licence commerciale a expiré. La mise à jour des bases n'est pas disponible, le trafic est analysé à l'aide des bases téléchargées lors de la dernière mise à jour.

- **Etat de la licence**.

  Etat de la licence de Kaspersky Anti-Virus. Valeurs du champ possibles :

  - **Licence actuelle**. La licence n'a pas expiré, elle est active.
  - **La durée de validité de la licence a expiré**. La licence a expiré, les fonctionnalités de Kaspersky Anti-Virus sont limitées.
  - **Absente**. L'application n'est pas activée.

- **Date d'expiration de la durée de validité de la licence**

  Date d'expiration de la licence. S'affiche si la clé active est ajoutée dans l'application.

  Si la clé n'est pas ajoutée, le champ affiche le message **Absente**.

- **Clé supplémentaire**.

  Informations sur la clé supplémentaire Valeurs du champ possibles :

  - **Ajoutée**. La clé supplémentaire est ajoutée tandis que le délai de validité de la clé active n'a pas expiré.
  - **Absente**. S'affiche dans deux cas :
    - la clé supplémentaire n'a pas été ajoutée ;
    - la clé supplémentaire a été ajoutée mais est arrivée à expiration.

Au cours de la connexion, le bloc affiche la ligne **Connexion**. Si la connexion au serveur n'a pas réussi, le bloc affiche le message **Impossible de se connecter au serveur**. Ces informations sont mises à jour automatiquement toutes les 60 secondes.

La partie inférieure du bloc **Licence** affiche le lien de passage à l'entrée **Licence** (cf. section "**Fenêtre principale**" à la page 19).

Schémas de déploiement *Groupe autonome* et *Entreprise*

- Informations relatives au niveau de fonctionnalité de Kaspersky Anti-Virus sur les serveurs du groupe. Valeurs possibles :
  - **Fonctionnement complet**.

    Kaspersky Anti-Virus possède toutes les fonctionnalités sur l'ensemble des serveurs faisant partie du groupe et n'a aucune restriction.

  - **Serveurs avec fonctionnalité limitée**.

    Nombre de serveurs faisant partie du groupe pour lesquels la fonctionnalité de Kaspersky Anti-Virus se distingue de la fonctionnalité complète.

    Kaspersky Anti-Virus peut se voir attribuer les restrictions suivantes :

    - **Mise à jour uniquement**. La clé fait partie de la liste noire. Seule la mise à jour des bases est disponible, le trafic n'est pas analysé.
    - **Administration uniquement**. La clé active de Kaspersky Anti-Virus n'est pas ajoutée ou la licence d'évaluation a expiré. Seule l'administration de Kaspersky Anti-Virus est disponible, le trafic n'est pas analysé et la mise à jour des bases n'est pas disponible.
    - **Mise à jour non disponible**. La licence commerciale a expiré. La mise à jour des bases de Kaspersky Anti-Virus n'est pas disponible, le trafic est analysé à l'aide des bases téléchargées lors de la dernière mise à jour.

- **Etat de la licence**.

  Etat de la licence de Kaspersky Anti-Virus. Valeurs du champ possibles :

  - **Licence actuelle**. La licence n'a pas expiré, elle est active.
  - **La durée de validité de la licence a expiré**. La licence a expiré, les fonctionnalités de Kaspersky Anti-Virus sont limitées.
  - **Absente**. L'application n'est pas activée.

- **Date d'expiration de la durée de validité de la licence**

  Date d'expiration de la licence. S'affiche si la clé active est ajoutée dans l'application.

  Si la clé n'est pas ajoutée, le champ affiche le message **Absente**.

- **Clé supplémentaire**.

  Informations sur la clé supplémentaire Valeurs du champ possibles :

  - **Ajoutée**. La clé supplémentaire est ajoutée tandis que le délai de validité de la clé active n'a pas expiré.
  - **Absente**. S'affiche dans deux cas :
    - la clé supplémentaire n'a pas été ajoutée ;
    - la clé supplémentaire a été ajoutée mais est arrivée à expiration.

Au cours de la connexion, le bloc affiche la ligne **Connexion**. Si la connexion à un ou plusieurs serveurs du groupe n'est pas établie, le bloc affiche le message **Impossible de se connecter à N serveurs sur M** (où M correspond au nombre de serveurs dans le groupe et N est le nombre de serveurs auxquels la connexion n'est pas établie). Ces informations sont mises à jour automatiquement toutes les 60 secondes.

La partie supérieure du bloc **Licence** affiche le lien de passage à l'entrée **Licence** (cf. section "**Fenêtre principale**" à la page 19).

BLOC MISE A JOUR DES BASES DE KASPERSKY ANTI-VIRUS

Le contenu du bloc **Mise à jour des bases de Kaspersky Anti-Virus** dépend du schéma de déploiement de Kaspersky Anti-Virus utilisé.

Schéma de déploiement *Serveur autonome*

- **Dernière mise à jour**.

  Date et heure de la dernière mise à jour des bases de Kaspersky Anti-Virus sur le serveur. Si les bases sont dépassées, le champ contient le message **Les bases sont dépassées**.

- **Résultat de la dernière mise à jour**.

  Résultat de la dernière mise à jour des bases de Kaspersky Anti-Virus sur le serveur.

  Contient une des valeurs suivantes obtenues lors de la dernière mise à jour des bases de Kaspersky Anti-Virus :

  - **La mise à jour a réussi**. La dernière mise à jour des bases a réussi.
  - **Erreur**. La mise à jour des bases de Kaspersky Anti-Virus n'a pas été effectuée sur le serveur, des erreurs de mise à jour des bases se sont produites, les bases sont dépassées ou corrompues.
  - **Mise à jour non disponible**. La licence commerciale a expiré. La mise à jour des bases de Kaspersky Anti-Virus n'est pas disponible, le trafic est analysé à l'aide des bases téléchargées lors de la dernière mise à jour.

- **Date et heure d'édition des bases**.

  Date et heure d'édition des bases de Kaspersky Anti-Virus installées sur le serveur.

- **Nombre d'enregistrements**.

  Nombre d'enregistrements dans les bases de Kaspersky Anti-Virus.

Au cours de la connexion, le bloc affiche la ligne **Connexion**. Si la connexion au serveur n'a pas réussi, le bloc affiche le message **Impossible de se connecter au serveur**. Ces informations sont mises à jour automatiquement toutes les 60 secondes.

La partie supérieure du bloc **Mise à jour des bases antivirus** affiche le lien de passage à l'entrée **Mise à jour** (cf. section "**Fenêtre principale**" à la page 19).

Schémas de déploiement *Groupe autonome* et *Entreprise*

- Informations relatives à l'état des bases de Kaspersky Anti-Virus sur les serveurs du groupe :
  - **Les bases sont à jour**.

    Sur tous les serveurs faisant partie du groupe, la dernière mise à jour des bases de Kaspersky Anti-Virus a réussi. Toutes les bases des serveurs sont à jour.
  - **Serveurs avec des problèmes de mise à jour des bases**.

    Nombre de serveurs faisant partie du groupe sur lesquels la dernière mise à jour des bases de Kaspersky Anti-Virus n'a pas réussi, erreurs de mise à jour des bases, bases dépassées ou corrompues.
- **Date et heure d'édition des bases**.

  Date d'édition des bases la plus ancienne sur l'ensemble des dates d'édition des bases sur tous les serveurs du groupe.
- **Nombre d'enregistrements dans les bases**.

  Nombre d'enregistrements dans les bases de Kaspersky Anti-Virus sur le serveur avec la date d'édition des bases la plus ancienne.

Au cours de la connexion, le bloc affiche la ligne **Connexion**. Si la connexion à un ou plusieurs serveurs du groupe n'est pas établie, le bloc affiche le message **Impossible de se connecter à N serveurs sur M** (où M correspond au nombre de serveurs dans le groupe et N est le nombre de serveurs auxquels la connexion n'est pas établie). Ces informations sont mises à jour automatiquement toutes les 60 secondes.

La partie supérieure du bloc **Mise à jour des bases de Kaspersky Anti-Virus** affiche le lien de passage à l'entrée **Mise à jour** (cf. section "**Fenêtre principale**" à la page 19).

BLOC STATISTIQUES DE FONCTIONNEMENT DES FILTRES EN UNE SEMAINE

Le bloc **Statistiques de fonctionnement des filtres en une semaine** affiche les informations relatives au fonctionnement des filtres joints de Kaspersky Anti-Virus. Si un filtre est désactivé, les statistiques sur ce filtre ne s'affichent pas. Les informations correspondent aux 7 derniers jours, date actuelle comprise.

Chaque filtre utilisé est accompagné de diagrammes en barres et de paramètres numériques affichant les résultats du traitement des objets analysés :

- **Objets entrés en vue d'être analysés**.

  Nombre total d'objets analysés et transmis selon le protocole sélectionné.
- **Menaces**.

  Nombre d'objets infectés et pouvant contenir une menace détectées lors de l'analyse du trafic transmis via le protocole sélectionné. Kaspersky Anti-Virus affiche les statistiques qui correspondent aux paramètres de détection définis par l'utilisateur lors de la création des règles de la stratégie d'analyse.

- **Erreurs d'analyse**.

  Nombre d'erreurs lors de l'analyse des objets transmis via le protocole sélectionné.

  L'erreur lors de l'analyse de l'objet se produit, par exemple, si une erreur s'est produite dans le fonctionnement des sous-systèmes de l'application (par exemple l'instance du moteur antivirus ou le Gestionnaire d'analyse).

- **Délais d'analyse dépassés**.

  Nombre de cas de dépassement de la période maximale pendant laquelle Kaspersky Anti-Virus analyse l'objet.

  Dans la limite de cette période, Kaspersky Anti-Virus exécute le téléchargement et l'analyse des données. Si à l'expiration de la période établie, l'objet n'a pas été entièrement téléchargé ou Kaspersky Anti-Virus n'a pas terminé son analyse, le transfert de l'objet au client est réalisé sans l'analyser.

Si Kaspersky Anti-Virus ne parvient pas à se connecter à la Base des données de la sauvegarde et des statistiques, à la place des statistiques de fonctionnement des filtres, le bloc affiche un message d'erreur de connexion. Ces informations sont mises à jour automatiquement toutes les 60 secondes.

PROTECTION PAR DEFAUT

Après l'installation, Kaspersky Anti-Virus commence l'analyse du trafic avec les paramètres définis par défaut. Tous les serveurs sur lesquels l'application est installée utilisent les paramètres d'analyse du trafic transmis via les protocoles, ainsi que les paramètres de productivité et les règles des stratégies de Kaspersky Anti-Virus (cf. section "Règles préinstallées des stratégies et règles des stratégies par défaut" à la page 57).

Paramètres d'analyse des connexions par défaut

Kaspersky Anti-Virus intercepte et analyse le trafic transmis via les protocoles HTTP, FTP, POP3 et SMTP. L'application analyse tous les types d'objets, y compris les objets joints. Lors de l'analyse des données transmises via les protocoles SMTP et POP3, Kaspersky Anti-Virus analyse l'en-tête, l'objet du message et les fichiers joints. Kaspersky Anti-Virus détecte les menaces de tous les types connus et les objets qui peuvent contenir une menace.

Pendant le téléchargement et l'analyse des objets transmis via les protocoles HTTP et FTP, Kaspersky Anti-Virus retient le transfert des données au client. Le temps maximal de retard du transfert des données via le protocole HTTP est de 30 secondes ; via le protocole FTP, il est de 15 secondes. Une fois ce délai expiré, Kaspersky Anti-Virus commence la transmission des données au client. Avant la fin de l'analyse de l'objet, 30% des données transmises via le protocole HTTP sont retenues, et 10% des données transmises via le protocole FTP.

La fonction de récupération du chargement des objets en cas d'interruption de la connexion via les protocoles HTTP et FTP est désactivée. La compatibilité avec le standard du protocole HTTP version 0.9 et le fonctionnement avec les commandes FTP ne faisant pas partie de l'ensemble standard des commandes du protocole FTP ne sont pas pris en charge.

Par défaut, le temps d'analyse maximal d'un objet pour tous les protocoles est de 1800 secondes. Si Kaspersky Anti-Virus n'a pas le temps d'analyser un objet au cours de ce délai, l'objet est transmis au client sans analyse.

Exclusions de l'analyse par défaut

Les objets suivants sont exclus de l'analyse :

- Les objets protégés par mot de passe.
- Pour les connexions via les protocoles HTTP et FTP, tous les objets qui passent entre le poste client et les serveurs de confiance.

  Les serveurs de confiance sont : *.kaspersky.com, *.adobe.com, *.microsoft.com, *.windows.com, *.windowsupdate.com, *.windowsupdates.com.
- Les objets de type Flash vidéo, WMSP qui passent par le protocole HTTP.

Actions à exécuter sur les menaces détectées par défaut

Lorsqu'un objet infecté ou un objet pouvant contenir des menaces est détecté, Kaspersky Anti-Virus exécute les actions suivantes :

- Pour les connexions via les protocoles HTTP et FTP, il bloque l'objet en le remplaçant par le message de modèle sur la menace détectée. Les objets composés, incluant la partie infectée, sont aussi bloqués.
- Pour les connexions via les protocoles SMTP et POP, il répare l'objet, si la réparation est impossible, il le bloque. Les parties infectées des objets composés sont supprimées.

Par défaut, Kaspersky Anti-Virus ne conserve pas dans la sauvegarde les copies des objets bloqués et réparés.

Productivité de l'analyse par défaut

Lors du traitement des flux de données importants, plusieurs exemplaires du moteur antivirus fonctionnent simultanément. Leur quantité est calculée selon la formule 2n+1, où n est le nombre de processus logiques du serveur physique sur lequel le pare-feu de Microsoft ISA Server/Forefront TMG est installé. Un moteur antivirus est sélectionné pour analyser les objets "rapides".

Kaspersky Anti-Virus analyse jusqu'à 128 objets dans la mémoire vive du serveur sans enregistrement sur le disque dur. La taille maximale des objets qui sont analysés sans enregistrement sur le disque dur est de 128 Ko.

Kaspersky Anti-Virus place jusqu'à 1024 objets dans la file d'attente de traitement. Si le nombre indiqué des objets se trouve en attente de traitement, un nouvel objet est transmis sans être analysé. Kaspersky Anti-Virus ajoute dans le Journal de l'analyse du trafic les informations sur les objets transmis sans être analysés.

CONNEXION DE LA CONSOLE D'ADMINISTRATION AU STOCKAGE DE CONFIGURATION

La Console d'administration de Kaspersky Anti-Virus assure l'administration par Kaspersky Anti-Virus. Pour commencer à utiliser l'application, vous devez vous connecter à la Console d'administration du stockage de configuration de Microsoft ISA Server / Forefront TMG.

DANS CETTE SECTION

ACTIONS PREALABLES AVANT LA CONNEXION DE LA CONSOLE D'ADMINISTRATION

Pour connecter la Console d'administration de Kaspersky Anti-Virus au stockage de configuration de Microsoft ISA Server/Forefront TMG, vous pouvez utiliser le compte Microsoft Windows sous lequel la Console d'administration a été lancée (c'est-à-dire le compte actuel) ou un autre compte indiqué lors de la connexion.

Le compte sous lequel la connexion au stockage de configuration Microsoft ISA Server/Forefront TMG a lieu, doit posséder les privilèges de consultation ou de lecture/enregistrement de la configuration de Kaspersky Anti-Virus (cf. section "A propos du partage des privilèges d'utilisation de Kaspersky Anti-Virus" à la page 45).

Pour obtenir l'accès au service *Kaspersky Anti-Virus 8.5 for ISA Server and Forefront TMG* (kavisasrv.exe), assurant le fonctionnement de Kaspersky Anti-Virus, le compte de l'utilisateur doit faire partie d'un des groupes suivants des utilisateurs du système d'exploitation Windows : Utilisateurs DCOM (Distributed COM Users), Administrateurs du domaine ou groupe des administrateurs locaux.

Le compte, sous lequel la connexion au stockage de configuration a lieu, est aussi utilisé lors de la connexion de la Console d'administration à la Base de données de la sauvegarde et des statistiques. Pour pouvoir utiliser les objets de la Sauvegarde, assurez-vous que le compte, sous lequel la connexion a lieu, possède les privilèges de lecture et d'enregistrement des informations dans la Base de données de la sauvegarde et des statistiques.

En cas de déploiement de Kaspersky Anti-Virus dans le groupe de travail, il faut assurer également la possibilité de connexion à la Base de données de la sauvegarde et des statistiques. Pour ce faire, procédez comme suit :

1. Sur le serveur physique sur lequel le système d'administration de la base de données Microsoft SQL Server est installé avec la Base de données de la sauvegarde et des statistiques, créer un compte, via les outils du système d'exploitation Microsoft Windows, identique au compte sous lequel la Console d'administration de Kaspersky Anti-Virus se lance.

2. Configurer pour le compte créé les privilèges nécessaires d'accès à la Base de données de la sauvegarde et des statistiques via les outils du système d'administration de la base de données Microsoft SQL Server.

CONNEXION AU STOCKAGE DE CONFIGURATION

Pour connecter la Console d'administration de Kaspersky Anti-Virus au stockage de configuration Microsoft ISA Server/Forefront TMG, procédez comme suit :

1. Lancez la Console d'administration de Kaspersky Anti-Virus.

   La fenêtre **Connexion au serveur du stockage de configuration** (cf. ill. ci-après) s'ouvre.

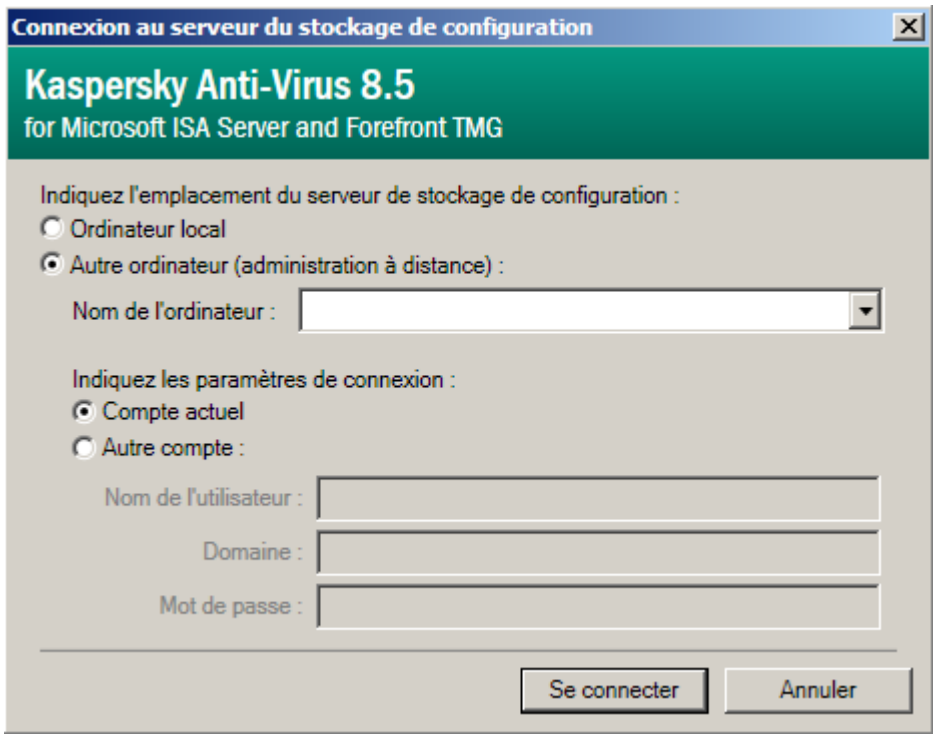

*Illustration 5. Fenêtre **Connexion au serveur du stockage de configuration***

Si auparavant la Console d'administration s'est connectée avec succès au stockage de configuration, la fenêtre affiche tous les paramètres de la dernière connexion réussie, sauf le mot de passe de l'utilisateur.

2. Sélectionnez l'option d'emplacement du stockage de configuration :

   - **Ordinateur local**

     La Console d'administration de Kaspersky Anti-Virus se connecte au stockage de configuration situé sur le même ordinateur sur lequel la Console d'administration a été lancée.

     Cette valeur est sélectionnée par défaut si auparavant la Console d'administration ne se connectait pas au stockage de configuration. Si la connexion est réitérée, la fenêtre affiche les paramètres de la dernière connexion réussie.

   - **Autre ordinateur (administration à distance)**

     La Console d'administration de Kaspersky Anti-Virus se connecte au stockage de configuration situé sur un autre ordinateur.

     Utilisez cette option de connexion s'il faut effectuer l'administration à distance de Kaspersky Anti-Virus. Dans ce cas, il faut définir les paramètres de connexion et le nom/l'adresse IP de l'ordinateur sur lequel le stockage de configuration se trouve.

3. Si le stockage de configuration est situé sur un ordinateur distant, indiquez les paramètres de connexion suivants :

   - **Nom de l'ordinateur**

     Nom et adresse IP de l'ordinateur sur lequel la connexion a lieu.

     Si la connexion de la Console d'administration au stockage de configuration est exécutée pour la première fois, il faut indiquer l'adresse IP dans ce champ, ainsi que le nom de l'ordinateur (si l'ordinateur fait partie du domaine, il faut indiquer le nom complet du domaine) ou le nom NetBIOS de l'ordinateur sur lequel le stockage de configuration se trouve.

     Kaspersky Anti-Virus enregistre les paramètres de la précédente connexion réussie de la Console d'administration au stockage de configuration. Si une nouvelle connexion de la Console d'administration au stockage de configuration est exécutée, la liste déroulante permet de sélectionner le nom de l'ordinateur auquel la connexion avait réussi.

   - Compte pour la connexion :

     - **Compte actuel**

       La Console d'administration utilise le compte actuel (c'est-à-dire le compte Microsoft Windows sous lequel la Console d'administration est lancée) pour se connecter au stockage de configuration.

       Ce paramètre est sélectionné par défaut si auparavant la Console d'administration ne se connectait pas au stockage de configuration. Si la connexion est réitérée, la fenêtre affiche les paramètres de la dernière connexion réussie.

     - **Autre compte**

       La Console d'administration utilise un compte Microsoft Windows différent du compte actuel pour se connecter au stockage de configuration.

       En cas de sélection de cette option, il faut indiquer le nom d'utilisateur, le mot de passe du compte et le nom de domaine dans lequel le compte est enregistré (si l'ordinateur sur lequel le stockage de configuration se trouve fait partie du domaine).

4. Si vous exécutez la connexion à un ordinateur distant avec un compte différent du compte actuel, indiquez la valeur des paramètres **Nom de l'utilisateur** et **Mot de passe**. Si l'ordinateur sur lequel se trouve le stockage de configuration fait partie du domaine, saisissez aussi la valeur du champ **Domaine**.

   Si le compte, sous lequel la connexion a lieu, ne possède pas assez de privilèges pour se connecter au stockage de configuration, Kaspersky Anti-Virus affiche sur l'écran un message relatif à cet événement.

5. Cliquez sur le bouton **Connexion**.

Suite à la connexion de la Console d'administration au stockage de configuration, l'arborescence de la console affiche les entrées prévues pour travailler avec les paramètres de Kaspersky Anti-Virus. La composition des entrées dans l'arborescence de la console dépend du schéma de déploiement de Kaspersky Anti-Virus utilisé (cf. *Manuel d'implantation de Kaspersky Anti-Virus*) et du rôle de l'utilisateur sous le compte duquel la connexion de la Console d'administration au stockage de configuration a eu lieu (cf. section "A propos du partage des privilèges d'utilisation de Kaspersky Anti-Virus" à la page 45).

Si la connexion de la Console d'administration au stockage de configuration n'est pas établie (par exemple, une erreur s'est produite lors de la connexion), l'arborescence de la console contient uniquement l'entrée racine **Kaspersky Anti-Virus**. Vous pouvez établir la connexion à l'aide du bouton **Connexion** situé dans le panneau des résultats de l'entrée **Kaspersky Anti-Virus**.

A PROPOS DU PARTAGE DES PRIVILEGES D'UTILISATION DE KASPERSKY ANTI-VIRUS

Le système des rôles administratifs de Microsoft ISA Server/Forefront TMG est utilisé pour partager les privilèges des utilisateurs sur le fonctionnement de Kaspersky Anti-Virus. Le rôle administratif de Microsoft ISA Server/Forefront TMG définit l'ensemble de privilèges des utilisateurs quant à l'exécution de certaines actions avec Kaspersky Anti-Virus.

Les privilèges des utilisateurs conformément à leur rôle administratif sont définis de la manière suivante (cf. tableau ci-après).

Tableau 2. Les rôles administratifs de Microsoft ISA Server/Forefront TMG et les privilèges lors de l'utilisation de Kaspersky Anti-Virus

ROLE	PRIVILEGES
Administrateur de l'entreprise Microsoft ISA Server/Forefront TMG	Installation de l'application sur tous les serveurs de l'entreprise. Le lancement de la Console d'administration. Lecture/Enregistrement de la configuration de Kaspersky Anti-Virus au niveau de l'entreprise et au niveau du groupe (pour tous les groupes qui font partie de l'entreprise).
Auditeur de l'entreprise Microsoft ISA Server/Forefront TMG	Le lancement de la Console d'administration. Consultation de la configuration de Kaspersky Anti-Virus au niveau de l'entreprise et au niveau du groupe (pour tous les groupes qui font partie de l'entreprise). Si l'utilisateur tente d'appliquer des modifications à la configuration au niveau de l'entreprise ou au niveau du groupe, Kaspersky Anti-Virus affiche un message indiquant l'insuffisance de privilèges pour modifier la configuration.
Administrateur du groupe Microsoft ISA Server/Forefront TMG	Installation de l'application sur les serveurs du groupe dont l'utilisateur est l'administrateur. Le lancement de la Console d'administration. La lecture/l'enregistrement de la configuration de Kaspersky Anti-Virus au niveau du groupe (pour le groupe dont l'utilisateur est l'administrateur). Les entrées des autres groupes ne peuvent pas être consultées par l'utilisateur. Consultation de la configuration du niveau de l'entreprise. Si l'utilisateur tente d'appliquer des modifications à la configuration du niveau de l'entreprise, Kaspersky Anti-Virus affiche un message relatif à l'insuffisance des privilèges pour modifier la configuration.
Auditeur du groupe Microsoft ISA Server/Forefront TMG	Le lancement de la Console d'administration. La consultation de la configuration de Kaspersky Anti-Virus au niveau du groupe (pour le groupe dont l'utilisateur est l'auditeur). Les entrées des autres groupes ne peuvent pas être consultées par l'utilisateur. Consultation de la configuration du niveau de l'entreprise. Si l'utilisateur tente d'appliquer des modifications à la configuration au niveau de l'entreprise ou au niveau du groupe, Kaspersky Anti-Virus affiche un message indiquant l'insuffisance de privilèges pour modifier la configuration.

L'utilisateur avec le rôle *Auditeur de contrôle du groupe Microsoft ISA Server/Forefront TMG* ne possède pas les privilèges de lancement de la Console d'administration et de la consultation/modification de la configuration de Kaspersky Anti-Virus. Lors de la tentative de connexion au stockage de configuration de Microsoft ISA Server/Forefront TMG sous le compte de cet utilisateur, Kaspersky Anti-Virus affiche un message relatif à l'insuffisance des privilèges de connexion.

PARTICULARITES D'UTILISATION PAR PLUSIEURS ADMINISTRATEURS

En cas d'utilisation par plusieurs administrateurs, la Console d'administration peut être installée sur l'ordinateur de chaque administrateur. Cette section décrit les particularités de l'utilisation simultanée par plusieurs administrateurs dans les Consoles d'administration connectées à un stockage de configuration.

En cas d'utilisation simultanée par plusieurs administrateurs, la configuration de l'application enregistrée dans le stockage de configuration de Microsoft ISA Server/Forefront TMG peut être différente de la configuration affichée dans la Console d'administration. Ceci peut avoir lieu, par exemple, suite à la modification des paramètres de Kaspersky Anti-Virus via une autre Console d'administration.

Les modifications apportées à la configuration de Kaspersky Anti-Virus s'affichent dans la Console d'administration immédiatement, mais elles sont utilisées par l'application uniquement après l'application des modifications de la configuration à l'aide du bouton **Appliquer** situé dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19).

Les privilèges de modification de la configuration de Kaspersky Anti-Virus sont accordés aux utilisateurs conformément à leur rôle administratif sur Microsoft ISA Server/Forefront TMG (cf. section "A propos du partage des privilèges d'utilisation de Kaspersky Anti-Virus" à la page 45). L'utilisateur doté du rôle *Administrateur de l'entreprise Microsoft ISA Server/Forefront TMG* possède les privilèges de modification de la configuration au niveau de l'entreprise et au niveau du groupe (pour tous les groupes qui font partie de l'entreprise). L'utilisateur doté du rôle *Administrateur du groupe Microsoft ISA Server/Forefront TMG* possède les privilèges de modification de la configuration au niveau du groupe (pour le groupe dont il est l'administrateur). Si l'utilisateur n'a pas assez de privilèges de modification de la configuration de Kaspersky Anti-Virus, en cliquant sur le bouton **Appliquer** Kaspersky Anti-Virus affiche sur l'écran le message relatif à cet événement et la configuration, affichée dans la Console d'administration, est réenregistrée automatiquement par la configuration depuis le stockage de configuration de Microsoft ISA Server/Forefront TMG.

Avant d'appliquer les modifications de la configuration, Kaspersky Anti-Virus compare la configuration au moment de la dernière application des paramètres dans cette Console d'administration (à l'aide du bouton **Appliquer**) avec la configuration de l'application dans le stockage de configuration de Microsoft ISA Server/Forefront TMG. Si les paramètres d'un niveau de configuration sont différents, une requête s'affiche à l'écran. Vous pouvez exécuter une des actions suivantes :

- Réenregistrer les paramètres dans le stockage de configuration de Microsoft ISA Server/Forefront TMG. Finalement, la configuration affichée dans la Console d'administration sera appliquée, et les modifications apportées auparavant par d'autres administrateurs dans le stockage de configuration, seront annulées.

- Actualiser les paramètres affichés dans la Console depuis le stockage de configuration. Suite à une mise à jour, les paramètres modifiés dans la Console d'administration depuis la dernière application des paramètres seront réenregistrés par les paramètres depuis le stockage de configuration de Microsoft ISA Server/Forefront TMG.

MISE A JOUR DES BASES

Cette section contient des informations sur la mise à jour des bases et des instructions de configuration des paramètres de mise à jour.

DANS CETTE SECTION

A PROPOS DE LA MISE A JOUR DES BASES

Chaque jour, de nouveaux virus et de nouveaux programmes malveillants apparaissent dans le monde. Les analystes antivirus de Kaspersky Lab recueillent des informations sur les virus et les programmes malveillants et les moyens de les neutraliser qu'ils consignent dans les *bases de Kaspersky Lab* (ci-après les "bases"), et Kaspersky Lab utilise ces bases pour protéger les ordinateurs-clients se trouvant dans le réseau de l'entreprise.

Les fichiers des bases contiennent la description de tous les programmes malveillants et des moyens de réparer les objets qui en sont victimes dont Kaspersky Lab a connaissance, la description des programmes qui peuvent être utilisés par les individus malintentionnés pour nuire à l'ordinateur ou aux données de l'utilisateur ainsi que les catégories de filtrage de contenu créées par Kaspersky Lab et utiliser pour analyser le contenu des fichiers.

Pour assurer un haut niveau de protection, les bases doivent être mises à jour régulièrement.

Au cours de la mise à jour, Kaspersky Anti-Virus compare les bases utilisées par l'application avec les bases qui se trouvent dans la source de mise à jour. Si les bases diffèrent, Kaspersky Anti-Virus télécharge uniquement la partie manquante des fichiers des bases. L'application ne copie pas les bases dans leur ensemble : cela permet d'accélérer la mise à jour et de réduire le volume de trafic transmis.

La distribution de Kaspersky Anti-Virus comprend les bases qui permettent à l'application d'effectuer la protection antivirus. Le temps que l'application s'installe, les bases peuvent être dépassées ; il est donc recommandé de mettre à jour les bases juste après l'installation de l'application.

Les bases installées dans l'application sont considérées dépassées si elles ont été éditées il y a au moins deux jours.

Kaspersky Anti-Virus met à jour les bases à partir des sources suivantes :

- Serveurs de mise à jour Kaspersky Lab

  L'application télécharge la mise à jour des bases à partir des serveurs HTTP de Kaspersky Lab. Les experts de Kaspersky Lab mettent à jour les bases sur les serveurs de mise à jour toutes les heures.

- Serveur HTTP ou serveur FTP.

  L'application télécharge la mise à jour des bases à partir du serveur HTTP local ou à partir du serveur FTP.

- Dossier réseau

  L'application télécharge la mise à jour des bases à partir du dossier réseau.

  Lors de la mise à jour des bases de Kaspersky Anti-Virus à partir du serveur HTTP, du serveur FTP ou du dossier réseau, le téléchargement des bases s'effectue à l'aide de l'utilitaire installé Kaspersky Update Utility.

  Pour de plus amples informations sur le fonctionnement de Kaspersky Update Utility cf. la Base de connaissances de Kaspersky Lab" *(*http://support.kaspersky.com/fr/faq/?qid=208284544*).*

Une fois les fichiers de mise à jour copiés à partir de la source de mise à jour sélectionnée (cf. section "Sélection de la source de mise à jour" à la page 49), l'application active automatiquement les bases obtenues et s'en sert pour analyser le trafic.

La mise à jour est effectuée de manière programmée ou manuelle (cf. section "Mise à jour manuelle des bases" à la page 51). Les experts de Kaspersky Lab recommandent de configurer la mise à jour programmée selon une fréquence d'une fois par heure (cf. section "Configuration de la mise à jour programmée des bases" à la page 52).

Dans le cas du schéma de déploiement *Serveur autonome*, la source et la programmation de la mise à jour sont indiquées dans les paramètres du serveur. Dans le cas des schémas de déploiement *Groupe autonome* et *Entreprise*, la source et la programmation de la mise à jour sont indiquées dans les paramètres du groupe. Le téléchargement des bases à partir de la source de mise à jour s'effectue de manière distincte par chaque serveur en fonction du schéma de déploiement utilisé. Pour de plus amples informations sur les schémas de déploiement, cf. *Manuel d'installation de "Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG*".

Si la licence commerciale a expiré ou si la clé n'est pas ajoutée, la mise à jour des bases de Kaspersky Anti-Virus n'est pas disponible.

Vous pouvez à tout moment consulter l'état des bases (cf. section "Consultation des informations relatives à l'état des bases" à la page 48).

CONSULTATION DES INFORMATIONS RELATIVES A L'ETAT DES BASES

Kaspersky Anti-Virus affiche les informations relatives à l'état des bases installées sur chaque serveur.

Les informations relatives à l'état des bases installées sur le serveur sont mises à jour toutes les 30 secondes.

➧ *Pour consulter les informations relatives à l'état des bases, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - Si le schéma de déploiement *Serveur autonome* est utilisé, déployez l'entrée du serveur et sélectionnez l'entrée jointe **Mise à jour**.

     Le panneau des résultats affiche les informations relatives à l'état des bases installées sur le serveur.

   - Si le schéma de déploiement *Groupe autonome* ou *Entreprise* est utilisé, déployez l'entrée du groupe et sélectionnez l'entrée jointe **Mise à jour**.

     Le panneau des résultats affiche les informations relatives à l'état des bases installées sur le serveur du groupe.

3. Pour chaque serveur, le panneau des résultats affiche les paramètres suivants :

- **Nom du serveur**.

  Nom du serveur pour lequel les informations relatives à l'état des bases de Kaspersky Anti-Virus s'affichent.

- **Date d'édition des bases**.

  Date et heure d'édition de la dernière version des bases de Kaspersky Anti-Virus installées sur le serveur.

  Si Kaspersky Anti-Virus n'a pas pu se connecter au serveur pour obtenir des informations sur les bases, ce champ affiche un message d'information sur l'état de connexion. Les valeurs possibles des messages d'information sont les suivantes :

  - **Connexion**. Kaspersky Anti-Virus tente d'obtenir l'accès au serveur.
  - **Erreur de connexion : <description de l'erreur>**. Kaspersky Anti-Virus n'a pas pu obtenir l'accès au serveur à cause de l'erreur indiquée.
  - **Les bases sont absentes ou corrompues**. Kaspersky Anti-Virus a téléchargé les bases endommagées depuis la source des mises à jour ou les bases ont été supprimées manuellement depuis le serveur. La case du tableau s'affiche en rouge.

- **Enregistrements dans les bases**.

  Nombre d'enregistrements dans les bases de Kaspersky Anti-Virus.

  Si les bases de Kaspersky Anti-Virus sont absentes sur serveur ou corrompues, le champ affiche le message **Aucune donnée**.

- **Dernière mise à jour des bases**.

  Date et heure de la dernière mise à jour des bases de Kaspersky Anti-Virus. Correspond aux valeurs de la date et de l'heure établies sur le serveur sélectionné.

  Si la connexion au serveur a réussi, ce champ affiche la date de la dernière mise à jour des bases.

  Si les bases sont dépassées (qu'elles ont été éditées il y a au moins deux jours), ce champ affiche le message **Les bases sont dépassées** et la case du tableau s'affiche en rouge.

- **Résultat de la dernière mise à jour des bases**.

  Etat de la dernière mise à jour des bases de Kaspersky Anti-Virus.

  Si la connexion au serveur a réussi, le champ contient une des valeurs suivantes obtenues lors de la dernière mise à jour des bases :

  - **Bases mises à jour** si la mise à jour des bases a réussi.
  - **Mise à jour en cours** si Kaspersky Anti-Virus met à jour les bases.
  - **Mise à jour inaccessible** si la licence a expiré ou si aucune clé n'est ajoutée.
  - **Erreur : <description de l'erreur>** s'il n'est pas possible de mettre à jour les bases de Kaspersky Anti-Virus pour le moment. La case rouge du tableau décrit la raison de l'erreur apparue lors de la tentative de mise à jour des bases.

SELECTION DE LA SOURCE DE MISE A JOUR

Si vous souhaitez télécharger directement les mises à jour des bases sur les serveurs à partir des serveurs HTTP de mise à jour de Kaspersky Lab, vous pouvez sélectionner la source de mise à jour **Serveurs de mise à jour de Kaspersky Lab**. Dans ce cas, les fichiers de mise à jour des bases sont téléchargés sur Internet par chaque serveur.

Si vous souhaitez télécharger les mises à jour des bases à partir d'une source dans le réseau de l'entreprise, vous pouvez sélectionner la source de mise à jour **Serveur HTTP / FTP ou dossier réseau** et vous servir de l'utilitaire Kaspersky Update Utility pour télécharger les mises à jour des bases à partir des serveurs de mise à jour de Kaspersky Lab dans le dossier ou sur le serveur. Dans ce cas, les fichiers de mise à jour sont téléchargés une fois depuis Internet dans le dossier réseau ou sur le serveur HTTP/FTP, et ensuite sont diffusés, à l'intérieur du réseau, sur les serveurs de Kaspersky Lab pour lesquels les paramètres de mise à jour indiquent la source sélectionnée.

Dans le cas du schéma de déploiement *Serveur autonome*, la source de mise à jour des bases est indiquée dans les paramètres du serveur. Dans le cas des schémas de déploiement *Groupe autonome* et *Entreprise*, la source de mise à jour des bases est indiquée dans les paramètres du groupe. Ainsi, en cas d'utilisation du schéma de déploiement *Entreprise*, vous pouvez indiquer les mêmes sources de mise à jour à utiliser dans tous les groupes de l'entreprise ou indiquer une source de mise à jour distincte pour chaque groupe. Dans ce cas, tous les serveurs faisant partie du groupe utiliseront une source de mise à jour.

Pour sélectionner une source de mise à jour des bases de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Ouvrez une des fenêtres suivantes de configuration des paramètres de l'application :

   - si le schéma de déploiement utilisé est *Serveur autonome :* la fenêtre **Paramètres du serveur** (cf. section "**Fenêtre Paramètres du serveur. Navigation**" à la page 24) ;

   - si le schéma de déploiement utilisé est *Groupe Autonome* ou *Entreprise :* la fenêtre **Paramètres du groupe** (cf. section "**Fenêtre Paramètres du groupe. Navigation**" à la page 25).

3. Sélectionnez l'onglet **Mise à jour**.

4. Sélectionnez la source de mise à jour :

   - Si vous souhaitez que la mise à jour soit effectuée à partir des serveurs de mise à jour de Kaspersky Lab, sélectionnez l'option **Serveurs de mise à jour de Kaspersky Lab**.

   - Si vous souhaitez que la mise à jour soit effectuée à partir d'un serveur HTTP, FTP ou d'un dossier réseau, sélectionnez l'option **Serveur HTTP/FTP ou dossier réseau** et indiquez l'adresse du serveur ou le nom complet du dossier dans le champ de saisie.

     Pour le serveur HTTP ou FTP, indiquez dans le champ de saisie l'adresse URL, pour le dossier réseau, indiquer le nom complet au format standard UNC.

5. Si la connexion au serveur de mise à jour des bases de Kaspersky Anti-Virus utilise un serveur proxy, indiquez les paramètres du serveur proxy. Pour ce faire, procédez comme suit :

   a. Cliquez sur le bouton **Serveur proxy**.

      La fenêtre **Serveur proxy** s'ouvre.

   b. Cochez la case **Utiliser le serveur proxy**.

   c. Exécutez une des actions suivantes :

      - Si le serveur de Microsoft ISA Server / Forefront TMG est utilisé pour accéder à la source de mise à jour, sélectionnez l'option **Serveur proxy local**.

        Kaspersky Anti-Virus utilise le serveur de Microsoft ISA Server / Forefront TMG pour se connecter à la source de mise à jour.

      - Si un autre serveur proxy est utilisé pour accéder à la source de mise à jour, sélectionnez l'option **Serveur proxy distant**. Dans les champs **Adresse** et **Port**, indiquez l'adresse IP et le numéro de port réseau du serveur proxy.

        Kaspersky Anti-Virus utilise le serveur proxy distant pour se connecter à la source de mise à jour.

   d. Si le serveur proxy servant à se connecter à la source de mise à jour utilise la vérification de l'authenticité, cochez la case **Vérification de l'authenticité nécessaire** et indiquez le **Nom de l'utilisateur** et le **Mot de passe**.

   e. Cliquez sur le bouton **OK** dans la fenêtre **Serveur proxy**.

6. Cliquez sur le bouton **OK** sous l'onglet **Mise à jour**.

   La fenêtre de configuration des paramètres de l'application se ferme.

7. Pour que la modification de la stratégie de Kaspersky Anti-Virus entre en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

Kaspersky Anti-Virus utilise la source de mise à jour indiquée lors de la mise à jour programmée ou manuelle des bases.

Si l'application a commencé la mise à jour programmée des bases avant l'application des nouveaux paramètres, la mise à jour se termine avec les paramètres précédents et la mise à jour suivante s'effectue avec les nouveaux paramètres.

MISE A JOUR MANUELLE DES BASES

Pour mettre à jour les bases de Kaspersky Anti-Virus manuellement, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - Si le schéma de déploiement utilisé est *Serveur autonome*, déployez l'entrée du serveur et sélectionnez l'entrée jointe **Mise à jour** (cf. section "**Fenêtre principale**" à la page 19).

   - Si le schéma de déploiement utilisé est *Groupe autonome* ou *Entreprise*, déployez l'entrée du groupe et sélectionnez l'entrée jointe **Mise à jour** (cf. section "**Fenêtre principale**" à la page 19).

3. En fonction du schéma de déploiement, effectuez une des actions suivantes :

   - Si le schéma de déploiement utilisé est *Serveur autonome*, cliquez sur le bouton **Mettre à jour les bases de Kaspersky Anti-Virus**.

     Kaspersky Anti-Virus mettra à jour les bases sur le serveur à partir de la source de mise à jour indiquée.

   - Si le schéma de déploiement *Groupe autonome* ou *Entreprise* est utilisé, sélectionnez les serveurs sur lesquels les bases doivent être mises à jour :

     - Si vous souhaitez mettre à jour les bases sur tous les serveurs du groupe, cliquez sur le bouton déroulant **Mettre à jour les bases de Kaspersky Anti-Virus** et sélectionnez la valeur **Sur tous les serveurs**.

       Kaspersky Anti-Virus mettra à jour les bases sur tous les serveurs affichés dans le tableau à partir de la source de mise à jour sélectionnée pour le groupe.

     - Si vous souhaitez mettre à jour les bases sur des serveurs séparés, sélectionnez un ou plusieurs serveurs dans le tableau, cliquez sur le bouton déroulant **Mettre à jour les bases de Kaspersky Anti-Virus** et sélectionnez la valeur **Sur le serveur sélectionné**.

       Kaspersky Anti-Virus mettra à jour les bases sur les serveurs sélectionnés à partir de la source de mise à jour sélectionnée pour le groupe.

Si la licence commerciale a expiré ou si la clé n'est pas ajoutée, la mise à jour des bases de Kaspersky Anti-Virus n'est pas disponible.

CONFIGURATION DE LA MISE A JOUR PROGRAMMEE DES BASES

Dans le cas du schéma de déploiement *Serveur autonome*, la programmation de la mise à jour est indiquée dans les paramètres du serveur. Dans le cas des schémas de déploiement *Groupe autonome* et *Entreprise*, la programmation de la mise à jour est indiquée dans les paramètres du groupe. Ainsi, dans le cas du schéma de déploiement *Entreprise*, vous pouvez indiquer les mêmes programmations de mise à jour à utiliser dans tous les groupes de l'entreprise ou indiquer une programmation distincte pour chaque groupe. Dans ce cas, tous les serveurs faisant partie du groupe utiliseront une programmation de mise à jour.

Pour configurer la mise à jour programmée des bases de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Ouvrez une des fenêtres suivantes de configuration des paramètres de l'application :

   - si le schéma de déploiement utilisé est *Serveur autonome :* la fenêtre **Paramètres du serveur** (cf. section "**Fenêtre Paramètres du serveur. Navigation**" à la page 24) ;

   - si le schéma de déploiement utilisé est *Groupe Autonome* ou *Entreprise :* la fenêtre **Paramètres du groupe** (cf. section "**Fenêtre Paramètres du groupe. Navigation**" à la page 25).

3. Sélectionnez l'onglet **Mise à jour**.

4. Cochez la case **Actualiser les bases selon la programmation**.

5. Indiquez la valeur du paramètre **Fréquence**.

   Le bloc **Fréquence** permet d'indiquer la fréquence de mise à jour des bases de Kaspersky Anti-Virus.

   Le paramètre est accessible si la case **Actualiser les bases selon la programmation** est cochée.

   Les valeurs de fréquence de mise à jour suivantes sont possibles :

   - **Toutes les 30 minutes**.
   - **Chaque heure**.
   - **Toutes les 2 heures**.
   - **Toutes les 4 heures**.
   - **Toutes les 6 heures**.
   - **Toutes les 12 heures**.
   - **Chaque jour**. Permet d'effectuer la mise à jour une ou deux fois par jour à l'heure indiquée. Pour cette valeur, les paramètres complémentaires suivants sont disponibles :
     - **A**. Définit l'heure principale de lancement de la tâche de mise à jour. La valeur par défaut est 12:00.
     - **Actualiser complémentairement dans**. Définit l'heure supplémentaire de lancement de la tâche de mise à jour La valeur par défaut est 00:00.

       Si la case est cochée, Kaspersky Anti-Virus récupère automatiquement les mises à jour à l'heure supplémentaire indiquée.

       Si la case est décochée, Kaspersky Anti-Virus récupère les mises à jour uniquement à l'heure indiquée dans le champ **A**.

       La case est cochée par défaut.

   Si la case **Actualiser les bases de Kaspersky Anti-Virus selon la programmation** a été cochée dans l'Assistant de configuration initiale, la valeur **Chaque heure** est sélectionnée dans la liste. En cas de restauration des valeurs par défaut, la valeur **Chaque jour** est sélectionnée dans la liste.

6. Cliquez sur le bouton **OK** sous l'onglet **Mise à jour**.

   La fenêtre de configuration des paramètres de l'application se ferme.

7. Pour que la modification des paramètres de Kaspersky Anti-Virus entre en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale. La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

Kaspersky Anti-Virus effectue la mise à jour programmée des bases à la fréquence indiquée.

Si la licence commerciale a expiré ou si la clé n'est pas ajoutée, la mise à jour des bases de Kaspersky Anti-Virus n'est pas disponible.

PROTECTION ANTIVIRUS

Cette section contient des informations sur la protection antivirus et des informations sur la configuration des stratégies de Kaspersky Anti-Virus, des paramètres d'analyse du trafic transmis via les protocoles HTTP, FTP, SMTP et POP3 et des paramètres de productivité de l'analyse.

DANS CETTE SECTION

A PROPOS DE LA PROTECTION ANTIVIRUS

La fonction principale de Kaspersky Anti-Virus est la protection des postes clients contre des objets malveillants qui passent via le pare-feu Microsoft ISA Server/Forefront TMG. Kaspersky Anti-Virus analyse en temps réel le trafic transmis via les protocoles HTTP, FTP, POP3 et SMTP à la recherche de la présence d'objets malveillants ainsi que d'objets pouvant contenir une menace.

L'analyse du trafic via le protocole HTTPS est aussi prévue pour Kaspersky Anti-Virus installé sur Forefront TMG. Pour que l'analyse du trafic HTTPS soit exécutée, il faut activer l'inspection du trafic dans la console d'administration de Forefront TMG.

Lors de l'analyse du trafic transmis via les protocoles HTTP et FTP, Kaspersky Anti-Virus intercepte les données et retarde leur envoi au client pour une période de temps définie, durant laquelle l'analyse et la vérification des données a lieu. Une fois ce délai écoulé, Kaspersky Anti-Virus commence la transmission des données au client qui les a demandées. Pour accélérer l'obtention de l'objet par le poste client, le transfert des données commence avant la fin de l'analyse de l'objet mais seul l'objet analysé est entièrement transmis (s'il ne contient aucune menace). Si, suite à l'analyse, Kaspersky Anti-Virus a décelé que l'objet était infecté ou pouvait contenir une menace, la transmission de l'objet est interrompue et l'objet bloqué.

Si Kaspersky Anti-Virus n'a pas le temps d'analyser l'objet dans le temps maximal imparti pour l'analyse, l'objet est transmis au client sans être analysé. Kaspersky Anti-Virus ajoute les informations sur l'objet transmis sans analyse, dans le Journal de l'analyse du trafic.

Lors de l'analyse des messages transmis via les protocoles SMTP et POP3, Kaspersky Anti-Virus analyse l'en-tête, l'objet du message et les fichiers joints.

L'analyse est exécutée en fonction des enregistrements des bases antivirus.

Les objets reconnus infectés ou pouvant contenir une menace, sont traités par Kaspersky Anti-Virus conformément aux paramètres établis de la protection antivirus. La copie de l'objet à traiter peut être enregistrée par l'application dans la sauvegarde. Puis, vous pouvez enregistrer la copie de l'objet sur le disque local ou réseau ou la supprimer depuis la sauvegarde.

Les paramètres de fonctionnement de Kaspersky Anti-Virus, tels que le temps de retard des données avant l'envoi au client, le volume des données retenues, le modèle de changement de l'objet des messages bloqués, sont définis par les *paramètres d'analyse du trafic* (cf. section "*Configuration des paramètres. Analyse du trafic transmis via les protocoles*" à la page 74). Les paramètres d'analyse du trafic sont appliqués pour toutes les connexions.

Les paramètres de protection antivirus appliqués uniquement pour les connexions et les protocoles sélectionnés peuvent être configurés à l'aide des *stratégies de Kaspersky Anti-Virus* (cf. section "*Stratégies et objets de réseau de Kaspersky Anti-Virus*" à la page 55).

Les stratégies de Kaspersky Anti-Virus définissent les paramètres suivants de la protection antivirus :

- les paramètres de traitement du trafic transmis via les protocoles HTTP et FTP, tels que la prise en charge de récupération du chargement des données lors de l'interruption de la connexion, la prise en charge des commandes inconnues du client FTP ;
- les types de menaces détectés par Kaspersky Anti-Virus ;
- les actions exécutées par Kaspersky Anti-Virus en cas de détection d'objets infectés protégés par mot de passe et d'objets pouvant contenir une menace ;
- les paramètres d'exclusion des objets de l'analyse antivirus.

Les *paramètres de productivité de l'analyse* permettent d'optimiser le fonctionnement de Kaspersky Anti-Virus au niveau d'un serveur à part (cf. section "*Configuration des paramètres. Productivité de l'analyse*" à la page 76). Kaspersky Anti-Virus peut traiter simultanément plusieurs objets. Le nombre d'objets traités parallèlement dépend du nombre d'instances du moteur antivirus lancées et fonctionnant simultanément. Le mode d'analyse des objets dans la mémoire permet d'analyser les objets sans les conserver dans le catalogue de travail sur le disque dur. L'utilisation des objets pour l'analyse permet d'augmenter ou de réduire le débit de Kaspersky Anti-Virus et, par cela même, contrôler la charge sur le serveur selon le volume du trafic qui transite via le pare-feu.

STRATEGIES ET OBJETS DE RESEAU DE KASPERSKY ANTI-VIRUS

Cette section contient des informations sur les stratégies, les règles des stratégies et les objets de réseau de Kaspersky Anti-Virus.

DANS CETTE SECTION

A PROPOS DES STRATEGIES DE KASPERSKY ANTI-VIRUS

Les paramètres d'analyse, spécifiques aux conditions entre les clients à part et les serveurs via le protocole sélectionné, sont configurés à l'aide des stratégies.

Dans le cas du schéma de déploiement *Entreprise*, les stratégies du groupe et les stratégies de l'entreprise sont utilisées. Les stratégies de l'entreprise sont appliquées pour les serveurs de tous les groupes inclus dans l'entreprise. Les stratégies du groupe sont appliquées uniquement pour les serveurs de ce groupe.

Dans le cas du schéma de déploiement *Serveur autonome* ou *Groupe Autonome*, seules les stratégies du groupe sont utilisées.

L'application prévoit trois types de stratégies :

- *Stratégie de traitement des protocoles* qui définit les paramètres de traitement du trafic au niveau des protocoles FTP et HTTP.
- *Stratégie d'exclusion de l'analyse* qui définit les paramètres d'exclusion des objets de l'analyse antivirus.
- *Stratégie d'analyse antivirus* qui définit les paramètres de détection des menaces et des actions à exécuter sur les objets détectés.

L'ensemble des stratégies de tout niveau de la configuration inclut une stratégie de chaque type.

Les stratégies sont appliquées dans l'ordre suivant :

1. Stratégie de traitement des protocoles.
2. Stratégie d'exclusion de l'analyse.
3. Stratégie d'analyse antivirus.

A PROPOS DES REGLES DES STRATEGIES DE KASPERSKY ANTI-VIRUS

Une stratégie est composée d'une ou de plusieurs règles. Chaque règle détermine comment Kaspersky Anti-Virus traite les objets du trafic qui passe par les protocoles, indiqués dans la règle, entre les objets de réseau indiqués.

Kaspersky Anti-Virus analyse les données source du trafic (le protocole, l'objet-source de réseau, et l'objet cible de réseau) selon la liste des règles de la stratégie (cf. section "Consultation de la liste des règles des stratégies" à la page 63). Dans le cas de coïncidence de toutes les trois données sources du trafic avec les conditions d'application d'une règle quelconque, les actions prescrites par cette règle sont exécutées.

Dans la liste des règles des trois types de stratégies, les règles sont situées conformément à l'ordre de leur application.

Vous pouvez établir l'ordre d'application des règles dans la liste (cf. section "Modification de l'ordre d'application des règles de la stratégie" à la page 70).

Si dans la stratégie d'un type plusieurs règles avec les mêmes conditions d'application sont définies, la règle, située en premier dans la liste des règles de la stratégie, est appliquée. L'analyse suivante selon la liste des règles de la stratégie de ce type n'est pas effectuée et Kaspersky Anti-Virus passe à la liste des règles de la stratégie de type suivant.

En cas d'utilisation des schémas de déploiement *Serveur autonome* et *Groupe Autonome*, la liste générale des règles des stratégies du groupe se forme de la manière suivante :

1. Règle de la stratégie de traitement des protocoles.
2. Règle de la stratégie d'exclusion de l'analyse.
3. Règle de la stratégie d'analyse antivirus.

Les règles des stratégies de l'entreprise se composent de règles appliquées avant les règles des stratégies du groupe et des règles appliquées après les règles des stratégies du groupe. En cas d'utilisation du schéma de déploiement *Entreprise*, la liste générale des règles des stratégies se forme de la manière suivante :

1. Stratégie de traitement des protocoles :
    a. règles de la stratégie de l'entreprise applicables avant les règles de la stratégie du groupe ;
    b. règles de la stratégie du groupe ;
    c. règles de la stratégie de l'entreprise applicables après les règles de la stratégie du groupe.

2. Stratégie d'exclusion de l'analyse :
    a. règles de la stratégie de l'entreprise applicables avant les règles de la stratégie du groupe ;
    b. règles de la stratégie du groupe ;
    c. règles de la stratégie de l'entreprise applicables après les règles de la stratégie du groupe.
3. Stratégie d'analyse antivirus :
    a. règles de la stratégie de l'entreprise applicables avant les règles de la stratégie du groupe ;
    b. règles de la stratégie du groupe ;
    c. règles de la stratégie de l'entreprise applicables après les règles de la stratégie du groupe.

Pour chaque stratégie, des règles par défaut sont prévues. Elles s'affichent dans la liste des règles à côté des stratégies que vous avez créées et sont toujours applicables au dernier moment. Pour la stratégie d'exclusion de l'analyse et pour la stratégie d'analyse antivirus, les règles préinstallées sont aussi prévues (cf. section "Règles préinstallées des stratégies et règles des stratégies par défaut" à la page 57).

REGLES PREINSTALLEES DES STRATEGIES ET REGLES DES STRATEGIES PAR DEFAUT

Les règles par défaut et les règles préinstallées sont prévues pour chaque type de stratégie parmi les trois types présentés. Elles s'affichent dans la liste des règles à côté des règles que vous avez créées.

Vous pouvez modifier et supprimer les règles préinstallées.

Contrairement aux règles créées ou préinstallées, les règles par défaut ne sont pas à modifier ou supprimer. La règle par défaut est toujours située en dernière place dans la liste des règles de la stratégie, c'est-à dire, au dernier moment à être utilisée si aucune autre règle n'a été appliquée.

Les règles par défaut et les règles préinstallées prévues pour les stratégies de Kaspersky Anti-Virus sont décrites ci-après.

Stratégie de traitement des protocoles

Une règle par défaut est indiquée pour la stratégie de traitement des protocoles. Cette règle fonctionne pour toutes les connexions et possède les paramètres suivants :

- La compatibilité avec l'ancien standard du protocole HTTP de version 0.9 est désactivée.
- La fonction de récupération du chargement des objets dans le cas d'interruption de la connexion lors du transfert via les protocoles HTTP et FTP est désactivée.
- L'utilisation des commandes FTP, non incluses dans l'ensemble standard des commandes du protocole FTP, est désactivée.

Dans le cas du schéma de déploiement *Entreprise*, la règle par défaut se rapporte à la stratégie du niveau de l'entreprise et s'applique après la stratégie au niveau du groupe.

Stratégie d'exclusion de l'analyse

Pour la stratégie d'exclusion de l'analyse, les règles suivantes sont indiquées :

- La règle par défaut. Fonctionne pour toutes les connexions et possède les paramètres suivants :
    - L'analyse de tous les types d'objets est activée.
    - L'analyse des objets joints est activée.

- La règle préinstallée "Sites de confiance". Fonctionne pour les connexions via les protocoles HTTP et FTP et pour l'objet de réseau préinstallé "Sites de confiance". Conformément à cette règle, lors de la requête aux serveurs qui sont définis par l'objet de réseau "Sites de confiance", tous les objets sont exclus de l'analyse.

- La règle préinstallée "Flux vidéo". Fonctionne pour les connexions via le protocole HTTP et pour tous les objets de réseau. Conformément à cette règle, les objets de type Flash vidéo, WMSP sont exclus de l'analyse.

Dans le cas du schéma de déploiement *Entreprise*, la règle par défaut se rapporte à la stratégie du niveau de l'entreprise et s'applique après la stratégie au niveau du groupe. Les règles préinstallées se rapportent à la stratégie au niveau du groupe.

Stratégie d'analyse antivirus

Pour la stratégie de l'analyse antivirus, les règles suivantes sont indiquées :

- La règle par défaut. Fonctionne pour toutes les connexions et possède les paramètres suivants :
  - La détection des menaces de tout type et des objets qui correspondent probablement aux paramètres de détection est activée.
  - La réparation des objets malveillants est désactivée.
  - La suppression des parties infectées des objets composés est désactivée. L'objet composé, incluant la partie infectée, est bloqué.
  - Le blocage de tous les objets malveillants détectés est activé.
  - Le blocage des objets, pouvant contenir une menace, est activé.
  - Le blocage de tous les objets détectés, protégés par mot de passe, est désactivé.
  - L'enregistrement des copies d'objets dans la sauvegarde est désactivé.
- La règle préinstallée "Réparation du courrier électronique". Fonctionne pour les connexions via les protocoles SMTP et POP3 et pour tous les objets de réseau et possède les paramètres suivants :
  - La détection des menaces de tout type et des objets qui correspondent probablement aux paramètres de détection est activée.
  - La réparation des objets malveillants est activée.
  - La suppression des parties infectées des objets composés est activée.
  - Le blocage des objets, pouvant contenir une menace, est activé.
  - Le blocage de tous les objets détectés, protégés par mot de passe, est désactivé.
  - L'enregistrement des copies d'objets dans la sauvegarde est désactivé.

Dans le cas du schéma de déploiement *Entreprise*, la règle par défaut se rapporte à la stratégie du niveau de l'entreprise et s'applique après la stratégie au niveau du groupe. La règle préinstallée se rapporte à la stratégie au niveau du groupe.

A PROPOS DES OBJETS DE RESEAU

Les objets de réseau sont utilisés dans les règles pour indiquer les clients dont les requêtes verront cette règle appliquée, et pour indiquer les serveurs dont les requêtes verront cette règle appliquée, ainsi que pour indiquer les clients et les serveurs pour lesquels la règle ne fonctionnera pas.

Dans le cas du schéma de déploiement *Entreprise*, les objets de réseau au niveau du groupe et les objets de réseau au niveau de l'entreprise sont utilisés. Les objets de réseau au niveau de l'entreprise sont utilisés dans les règles au niveau du groupe et dans les règles au niveau de l'entreprise. Les objets de réseau au niveau du groupe sont utilisés uniquement dans les règles au niveau du groupe.

Quatre types d'objets de réseau sont prévus :

- *Ordinateur* : un ordinateur séparé avec l'adresse IP indiquée.
- *Sous-réseau* : une multitude d'ordinateurs dont les adresses font partie du sous-réseau indiqué.
- *Plage des adresses IP* : une multitude d'ordinateurs dont les adresses IP font partie de la plage indiquée.
- *Ensemble des noms de domaines* : un ou plusieurs ordinateurs dont les noms de domaines correspondent aux noms indiqués.

Les objets de réseau de type *Ordinateur*, *Sous-réseau* et *Plage des adresses IP* sont utilisés pour indiquer les clients dont les requêtes verront la règle appliquée. Les objets de réseau de type *Ordinateur*, *Sous-réseau*, *Plage des adresses IP* et *Ensemble des noms de domaine* sont utilisés pour indiquer les serveurs dont les requêtes verront la règle appliquée.

CONFIGURATION DES PARAMETRES. STRATEGIES ET OBJETS DE RESEAU DE KASPERSKY ANTI-VIRUS

Cette section contient des informations sur la configuration des stratégies de Kaspersky Lab.

A l'aide des stratégies de Kaspersky Anti-Virus, vous pouvez indiquer les paramètres de traitement des protocoles, les paramètres d'exclusion des objets de l'analyse et les paramètres de protection antivirus pour différents objets de réseau et protocoles.

DANS CETTE SECTION

OPERATION SUR LES OBJETS DE RESEAU

Vous pouvez exécuter les actions suivantes avec les objets de réseau :

- créer les objets de réseau du type sélectionné (cf. section "Création de l'objet de réseau" à la page 60) ;
- consulter et modifier les paramètres des objets de réseau (cf. section "Modification de l'objet de réseau" à la page 62) ;
- supprimer les objets de réseau (cf. section "Suppression de l'objet de réseau" à la page 62).

DANS CETTE SECTION

CONSULTATION DE LA LISTE DES OBJETS DE RESEAU

L'affichage de la liste des objets de réseau dépend du schéma de déploiement utilisé par Kaspersky Anti-Virus.

Schémas de déploiement Serveur autonome et Groupe Autonome

Pour consulter la liste des objets de réseau, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée du serveur (schéma de déploiement *Serveur autonome*) ou l'entrée du groupe (schéma de déploiement *Groupe Autonome*) et sélectionnez l'entrée jointe **Objets de réseau** (cf. section "**Fenêtre principale**" à la page 19).

   Le panneau des résultats affichera quatre panneaux déroulants dont chacun d'entre eux contient la liste des objets de réseau d'un type.

Schéma de déploiement Entreprise

Pour consulter la liste des objets de réseau, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - Déployez l'entrée du groupe et sélectionnez l'entrée jointe **Objets de réseau** (cf. section "**Fenêtre principale**" à la page 19).

     Le panneau des résultats affichera quatre panneaux déroulants qui contiennent chacun la liste des objets réseau d'un type au niveau du groupe ou au niveau de l'entreprise. La liste indique le niveau de configuration auquel l'objet correspond.

   - Déployez l'entrée **Entreprise** et sélectionnez l'entrée jointe **Objets de réseau** (cf. section "**Fenêtre principale**" à la page 19).

     Le panneau des résultats affichera quatre panneaux déroulants dont chacun d'entre eux contient la liste des objets de réseau d'un type du niveau de l'entreprise.

CREATION D'UN OBJET DE RESEAU

Pour créer un objet de réseau, procédez comme suit :

1. Ouvrez la liste des objets de réseau (cf. section "Consultation de la liste des objets de réseau" à la page 60).

   En cas d'utilisation du schéma de déploiement *Entreprise*, sélectionnez une des entrées suivantes :

   - si vous voulez créer un objet de réseau au niveau de l'entreprise : l'entrée **Objets réseau**, jointe à l'entrée **Entreprise** ;

   - si vous voulez créer un objet de réseau au niveau du groupe : l'entrée **Objet réseau**, jointe à l'entrée du groupe.

2. Cliquez sur le bouton **Ajouter** situé dans la barre à outils et sélectionnez le type de l'objet réseau.

   La fenêtre de l'Assistant de création de l'objet réseau s'ouvrira.

   Le type de fenêtre de l'Assistant de création d'un objet de réseau dépend du type d'objet de réseau sélectionné.

3. Dans la fenêtre de l'Assistant, saisissez le nom de l'objet de réseau créé et indiquez les paramètres de l'objet de réseau selon son type.

Dans le cadre d'un type d'objets de réseau, le nom de l'objet de réseau doit être unique.

- Pour l'objet *Ordinateur*, indiquez l'**adresse IP**.

  L'adresse IP de l'ordinateur à l'aide duquel l'objet de réseau est défini.

  L'adresse IP de l'objet de réseau est indiquée au format IPv4.

  La règle de la stratégie où cet objet de réseau est utilisé, s'applique uniquement pour l'adresse IP indiquée.

- Pour l'objet *Sous-réseau*, indiquez les paramètres suivants :

  - **Adresse du réseau**.

    L'adresse IP du sous-réseau à l'aide duquel l'objet de réseau est défini.

    L'adresse IP du sous-réseau est indiquée au format IPv4.

  - **Masque du réseau**.

    Le masque du sous-réseau qui définit le nombre d'adresses IP sélectionnées depuis l'adresse définie du réseau.

    Par exemple, le masque de sous-réseau de type 255.255.0.0 sélectionne 65534 adresses des périphériques de réseau depuis l'adresse définie du sous-réseau.

- Pour l'objet *Plage des adresses IP*, indiquez les adresses IP qui définissent le début et la fin de la plage des adresses, à l'aide de laquelle l'objet de réseau est défini (les paramètres **Début de la plage**, **Fin de la plage**).

  Il faut définir l'adresse IP de début et de fin de la plage des adresses au format IPv4.

  La règle de la stratégie, où cet objet de réseau est utilisé, s'applique uniquement pour les adresses IP qui font partie de la plage.

- Pour l'objet *Ensemble des noms de domaines*, formez la liste **Noms de domaines**.

  La liste des noms de domaine des ordinateurs à l'aide desquels l'objet de réseau est défini. La règle de la stratégie où cet objet de réseau est utilisé, s'applique uniquement pour les noms de domaine indiqués dans cette liste.

  La liste des noms de domaine doit comprendre au moins un nom de domaine.

  Exécutez une des actions suivantes :

  - Si vous voulez ajouter un nom de domaine dans la liste, cliquez sur le bouton **Ajouter** et saisissez le nom dans le champ de saisie dans la fenêtre **Nouveau nom de domaine** qui s'ouvre.

    Le nom de domaine peut contenir le symbole de service *, qui signifie n'importe quel nombre de domaine du niveau inférieur. Par exemple, le nom de domaine *.microsoft.com comprend les noms de domaine microsoft.com, www.microsoft.com ou files.download.microsoft.com. Le symbole * peut être utilisé qu'une fois et qu'au début du nom de domaine.

  - Si vous voulez supprimer le nom de domaine de la liste, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.

4. Cliquez sur le bouton **OK**. La fenêtre de l'Assistant de création d'un objet de réseau se ferme.

5. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

L'objet de réseau créé sera utilisé par l'application uniquement après l'application des modifications de configuration.

MODIFICATION DE L'OBJET DE RESEAU

Pour modifier les paramètres de l'objet de réseau, procédez comme suit :

1. Ouvrez la liste des objets de réseau (cf. section "Consultation de la liste des objets de réseau" à la page 60).

   Dans le cas du schéma de déploiement *Entreprise*, vous pouvez modifier les objets de réseau du niveau de l'entreprise uniquement dans l'entrée **Objets de réseau**, faisant partie de l'entrée **Entreprise**. Dans l'entrée **Objets de réseau**, faisant partie de l'entrée du groupe, les objets de réseau du niveau de l'entreprise peuvent uniquement être consultés.

2. Sélectionnez dans la liste l'objet de réseau dont vous souhaitez modifier les paramètres et ouvrez la fenêtre de la configuration des paramètres de l'objet de réseau à l'aide d'un des moyens suivants :

   - à l'aide du bouton **Modifier** situé dans la barre d'outils ;
   - en double-cliquant sur l'objet de réseau sélectionné ;
   - à l'aide de l'option du menu contextuel.

   Le type de fenêtre de configuration des paramètres de l'objet de réseau dépend du type d'objet de réseau sélectionné.

3. Dans la fenêtre de configuration, modifier les paramètres indiqués lors de la création de l'objet de réseau (cf. section "Création de l'objet de réseau" à la page 60).

4. Cliquez sur le bouton **OK**. La fenêtre de configuration des paramètres de l'objet de réseau se ferme.

5. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

SUPPRESSION DE L'OBJET DE RESEAU

Vous pouvez supprimer un objet de réseau sélectionné dans la liste.

Les objets de réseau utilisés dans les règles de la stratégie ne peuvent pas être supprimés. Si vous voulez supprimer un objet de réseau utilisé dans la règle de la stratégie, supprimez d'abord cet objet de la liste des objets de réseau utilisés dans la fenêtre des propriétés de la règle de la stratégie (cf. section "Modification de la règle de la stratégie" à la page 69).

Dans le cas du schéma de déploiement *Entreprise*, les objets de réseau du niveau de l'entreprise peuvent être supprimés uniquement dans la liste des objets de réseau du niveau de l'entreprise (cf. section "Consultation de la liste des objets de réseau" à la page 60). Dans la liste générale des objets de réseau du groupe ou de l'entreprise, les objets de réseau du niveau de l'entreprise sont uniquement à consulter.

Les modifications dans la liste des objets de Kaspersky Anti-Virus entreront en vigueur uniquement après l'application des modifications de la configuration.

OPERATION SUR LES REGLES DES STRATEGIES

Vous pouvez exécuter les actions suivantes avec les règles des stratégies :

- créer les règles du type sélectionné (cf. section "Création de la règle de la stratégie" à la page 67) ;
- consulter et modifier les paramètres des règles (cf. section "Modification de la règle de la stratégie" à la page 69) ;
- désactiver et activer les règles (cf. section "Modification de la règle de la stratégie" à la page 69) ;
- modifier l'ordre d'application des règles dans la composition de la stratégie (cf. section "Modification de l'ordre d'application des règles de la stratégie" à la page 70) ;
- supprimer les règles (cf. section "Suppression de la règle de la stratégie" à la page 70).

DANS CETTE SECTION

CONSULTATION DE LA LISTE DES REGLES DES STRATEGIES

L'affichage de la liste des règles des stratégies dépend du schéma de déploiement utilisé par Kaspersky Anti-Virus.

Schéma de déploiement *Serveur autonome*

Pour consulter la liste des règles des stratégies de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).
2. Déployez l'entrée du serveur et sélectionnez l'entrée jointe **Stratégies** (cf. section "**Fenêtre principale**" à la page 19).

Le panneau des résultats affichera trois panneaux déroulants qui contiennent chacun la liste des règles de la stratégie d'un type.

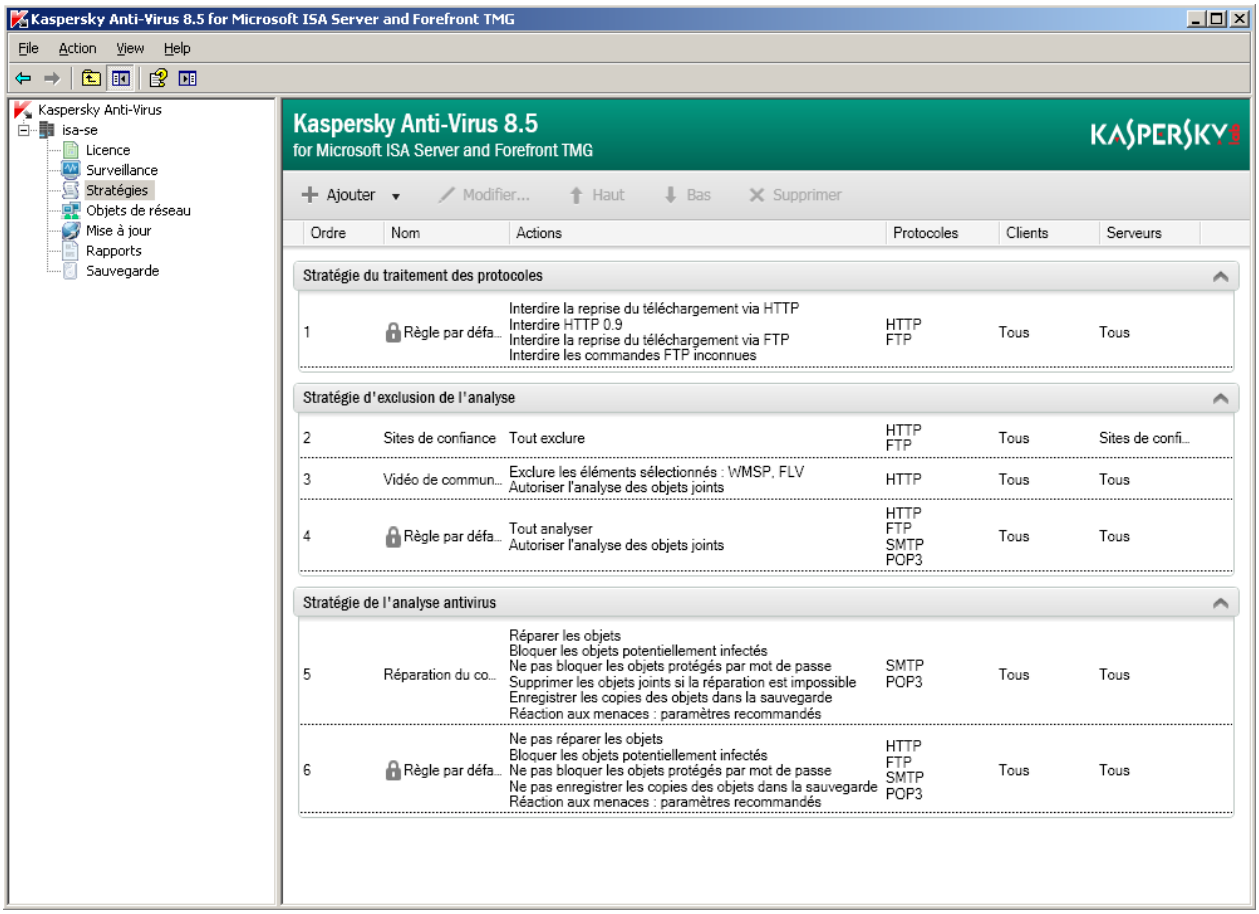

Illustration 6. Liste des règles des stratégies Schéma de déploiement Serveur autonome

Le numéro définissant l'ordre d'application de cette règle s'affiche dans la liste à gauche du nom de la règle. Les règles désactivées s'affichent en gris dans la liste des règles des stratégies (cf. section "Modification de la règle de la stratégie" à la page 69). L'icône s'affiche à côté des règles ne pouvant pas être modifiées.

Schéma de déploiement *Groupe Autonome*

➧ *Pour consulter la liste des règles des stratégies de Kaspersky Anti-Virus, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée du groupe et sélectionnez l'entrée jointe **Stratégies** (cf. section "**Fenêtre principale**" à la page 19).

Le panneau des résultats affichera trois panneaux déroulants qui contiennent chacun la liste des règles de la stratégie d'un type.

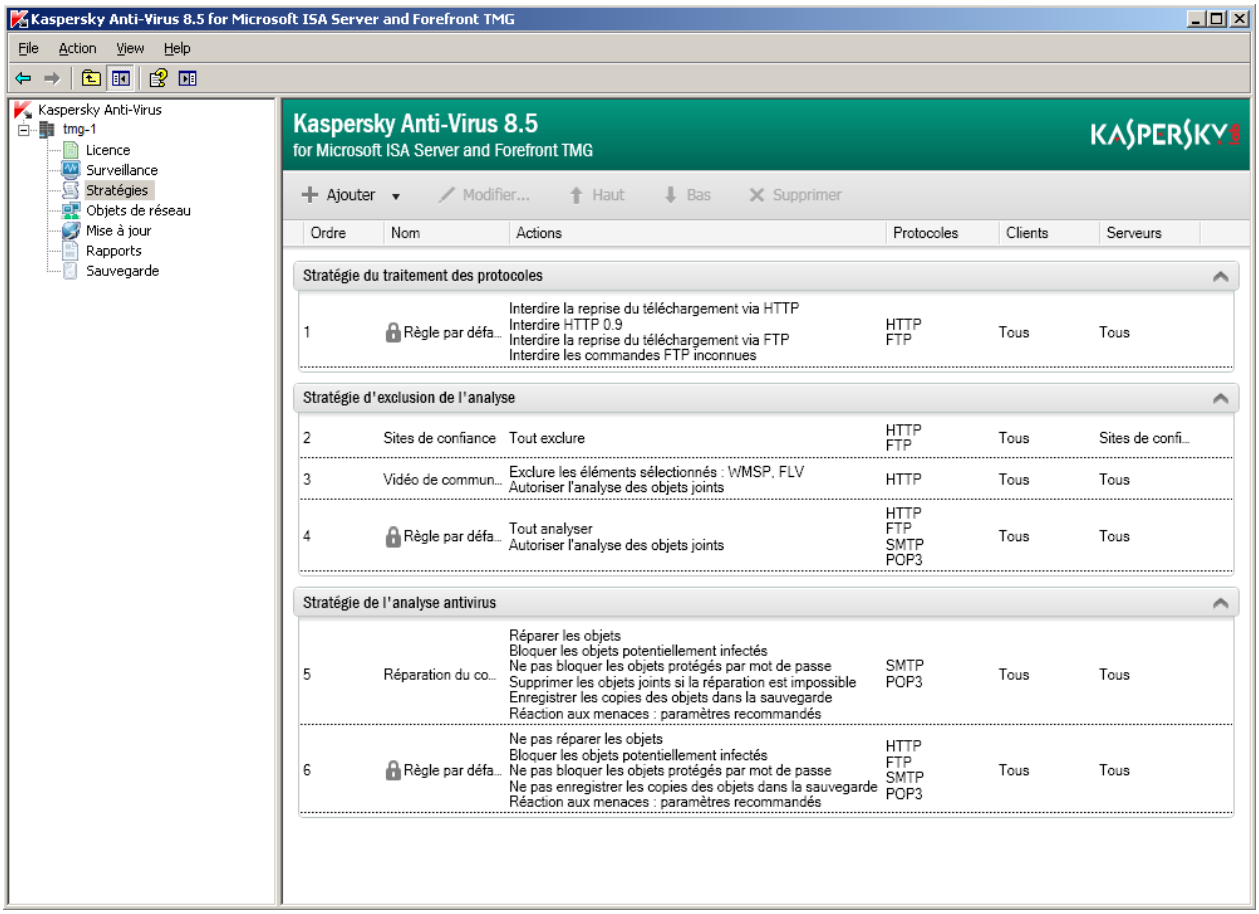

Illustration 7. Liste des règles des stratégies Schéma de déploiement Groupe Autonome

Le numéro définissant l'ordre d'application de cette règle s'affiche dans la liste à gauche du nom de la règle.

Les règles désactivées sont affichées en gris dans la liste des règles des stratégies. L'icône s'affiche à côté des règles ne pouvant pas être modifiées.

Schéma de déploiement *Entreprise*

➧ *Pour consulter la liste des règles des stratégies de Kaspersky Anti-Virus, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - Déployez l'entrée du groupe et sélectionnez l'entrée jointe **Stratégies** (cf. section "**Fenêtre principale**" à la page 19).

     Le panneau des résultats affichera trois panneaux déroulants qui contiennent chacun les règles de la stratégie au niveau du groupe et les règles de la stratégie au niveau de l'entreprise. Chaque panneau contient trois blocs de règles :

     - règles de stratégie de l'entreprise applicables avant la stratégie du groupe ;

     - règles de la stratégie du groupe ;

- règles de stratégie de l'entreprise applicables après la stratégie du groupe.

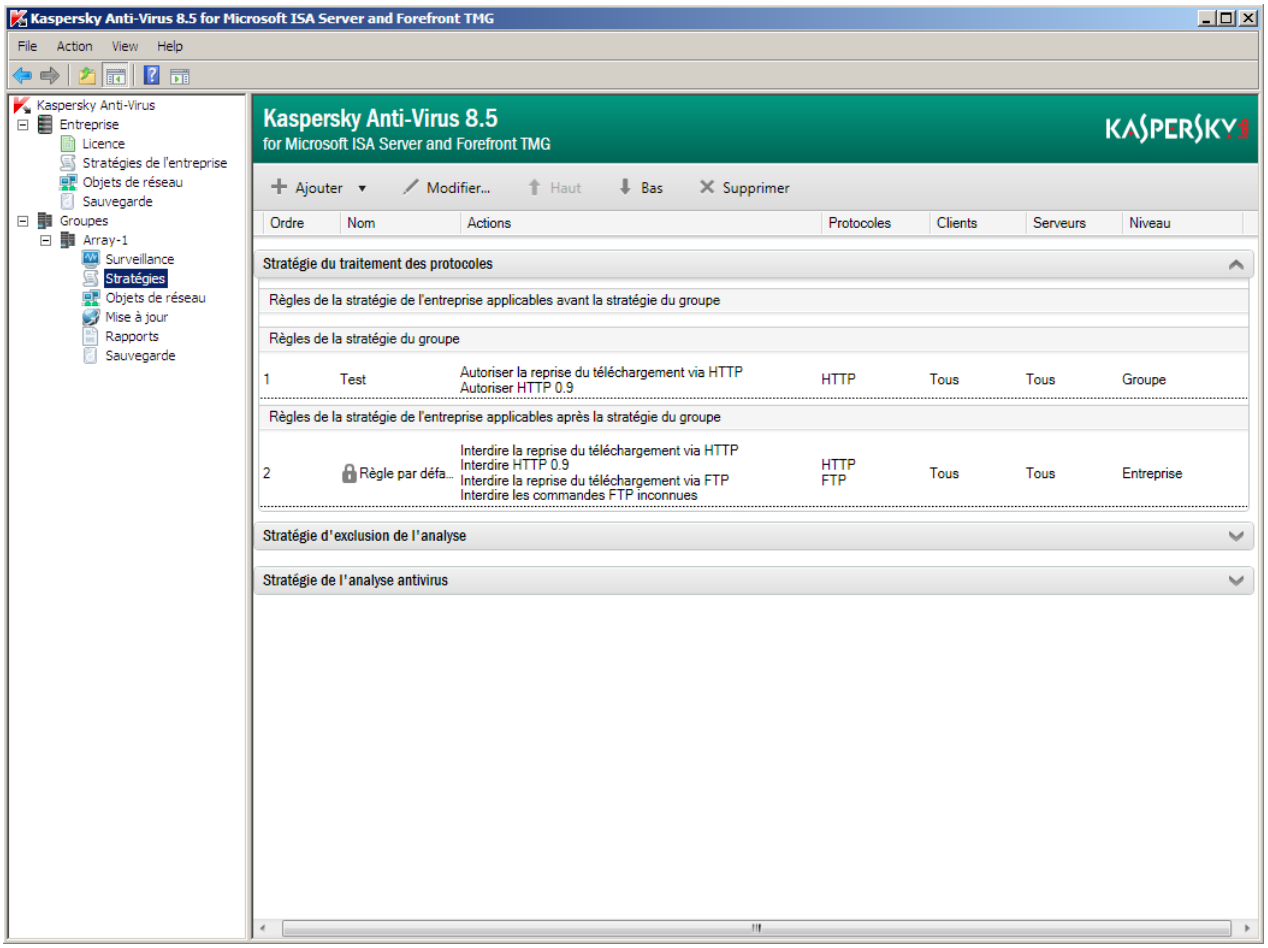

Illustration 8. Liste des règles du niveau du groupe et du niveau de l'entreprise.

Le niveau de configuration de l'application, auquel la règle correspond, est indiqué dans la liste des règles dans la colonne **Niveau**. Le numéro définissant l'ordre d'application de cette règle s'affiche dans la liste à gauche du nom de la règle.

- Déployez l'entrée **Entreprise** et sélectionnez l'entrée jointe **Stratégies de l'entreprise** (cf. section "**Fenêtre principale**" à la page 19).

  Le panneau des résultats affichera trois panneaux déroulants qui contiennent chacun les règles de la stratégie du niveau de l'entreprise. Chaque panneau contient deux blocs de règles :

  - règles de stratégie de l'entreprise applicables avant la stratégie du groupe ;

- règles de stratégie de l'entreprise applicables après la stratégie du groupe.

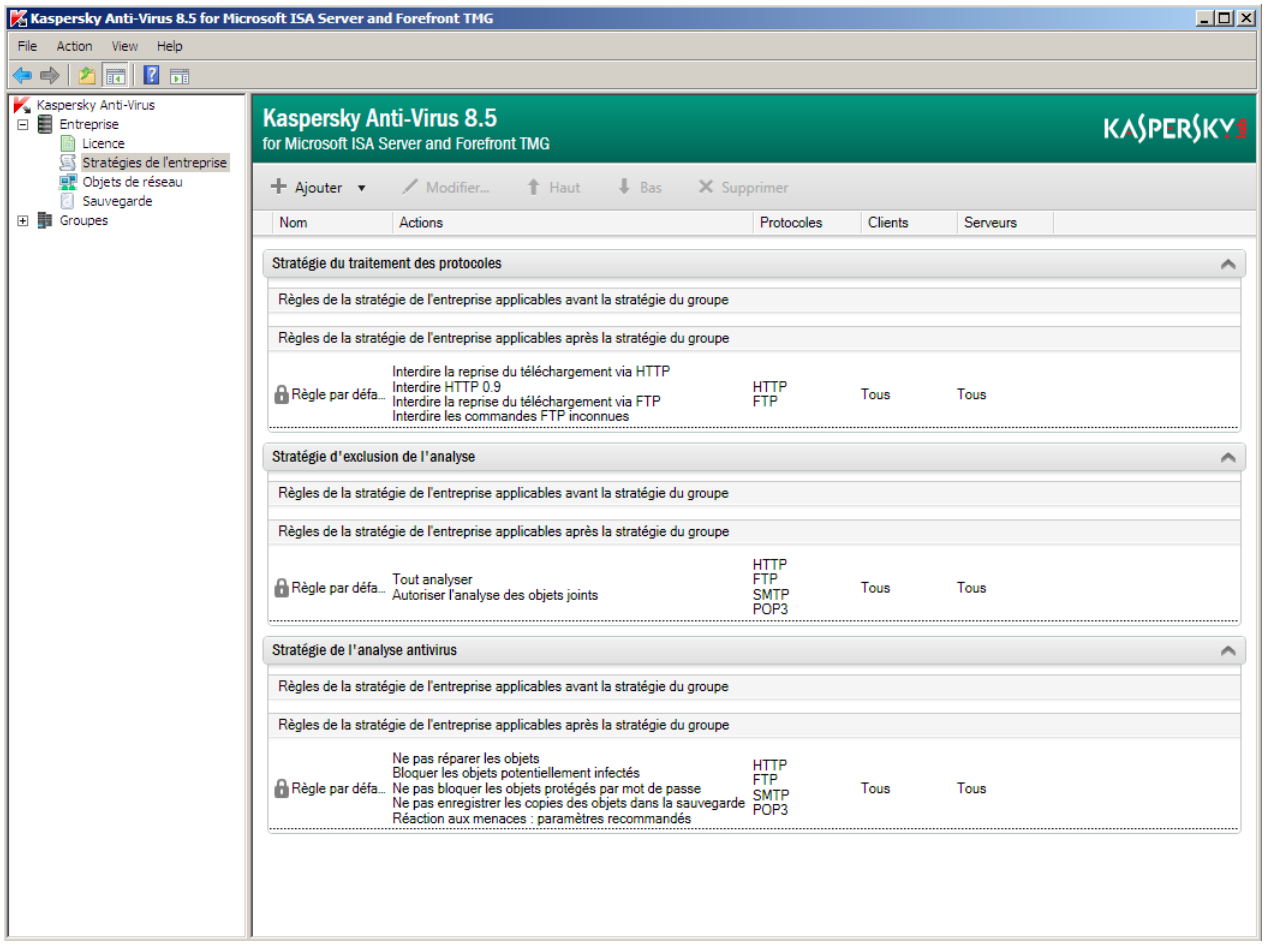

Illustration 9. Liste des règles des stratégies du niveau de l'entreprise. Schéma de déploiement Entreprise

L'ordre d'application des règles de la stratégie de l'entreprise est défini par l'emplacement des règles dans la liste : la règle située plus haut s'applique avant la règle située plus bas.

Les règles désactivées s'affichent en gris dans la liste des règles au niveau du groupe et au niveau de l'entreprise (cf. section "Modification de la règle de la stratégie" à la page 69). L'icône s'affiche à côté des règles ne pouvant pas être modifiées.

CREATION D'UNE REGLE DE STRATEGIE

La création des règles s'effectue à l'aide de l'Assistant de création de la règle.

➡ *Pour créer une règle de la stratégie, procédez comme suit :*

1. Ouvrez la liste des règles des stratégies (cf. section "Consultation de la liste des règles des stratégies" à la page 63).

   En cas d'utilisation du schéma de déploiement *Entreprise*, sélectionnez une des entrées suivantes :

   - si vous voulez créer une règle de la stratégie du niveau de l'entreprise : l'entrée **Stratégie de l'entreprise**, jointe à l'entrée **Entreprise** ;
   - si vous voulez créer une règle de la stratégie au niveau du groupe : l'entrée **Stratégies** jointe à l'entrée du groupe.

2. Cliquez sur le bouton **Ajouter** situé dans la barre à outils et sélectionnez le type de la règle créée.

   L'Assistant de création de la règle s'ouvrira.

3. Dans la fenêtre de l'Assistant de création de la règle, indiquez successivement les paramètres suivants :

   - Le nom de la règle créée (dans la fenêtre **Nom de la règle**).

     Le nom de la règle doit être unique au type de stratégie sélectionné sur un niveau de configuration. Si le schéma de déploiement de Kaspersky Anti-Virus suppose plusieurs niveaux de configuration, le nom de la règle de la stratégie au niveau du groupe peut coïncider avec le nom de la règle de la stratégie au niveau de l'entreprise.

   - Les protocoles auxquels cette règle sera appliquée et les paramètres spécifiques de la règle de ce type (cf. section "Paramètres des règles des stratégies" à la page 70).

4. Dans la fenêtre de l'Assistant, indiquez les objets réseau suivants :

   - Les objets de réseau dont les requêtes verront cette règle appliquée (clients), et, le cas échéant, les exclusions, soit les clients pour lesquels cette règle ne fonctionnera pas pour les requêtes (dans la fenêtre **Sélection des clients**).

   - Les objets de réseau dont les requêtes verront cette règle appliquée (clients), et, le cas échéant, les exclusions, soit les clients pour lesquels cette règle ne fonctionnera pas pour les requêtes (dans la fenêtre **Sélection des serveurs**).

     Les listes des clients et des serveurs doivent contenir au moins un objet de réseau. Par défaut, la règle s'applique pour toutes les connexions : l'objet de réseau spécial **Tous** est automatiquement indiqué pour les clients et les serveurs.

     Pour modifier la liste des objets de réseau pour lesquels la règle est appliquée, exécutez une des actions suivantes :

     - Si vous voulez ajouter des objets de réseau, ouvrez la fenêtre **Objets réseau** à l'aide du bouton **Ajouter** situé dans la fenêtre de l'Assistant. Dans la fenêtre **Objets réseau**, sélectionnez l'objet réseau dans l'arborescence des objets et cliquez sur le bouton **Ajouter**. L'objet réseau sélectionné s'affichera dans la liste des objets dans la fenêtre **Sélection des clients** ou **Sélection des serveurs**.

     - Si vous voulez supprimer l'objet réseau de la liste, cliquez sur le bouton **Supprimer** situé dans la fenêtre **Sélection des clients** ou **Sélection des serveurs**.

5. Dans la fenêtre **Sélection des serveurs**, cliquez sur le bouton **Terminer**. La fenêtre de l'Assistant de création des règles se ferme. La règle créée sera ajoutée dans la liste des règles de la stratégie du type sélectionné.

   Par la suite, vous pouvez modifier l'ordre d'application de la règle créée ou la déplacer d'un bloc de règles de la stratégie vers un autre (cf. section "Modification de l'ordre d'application des règles de la stratégie" à la page 70).

6. Pour que la modification de la stratégie de Kaspersky Anti-Virus entre en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

MODIFICATION DE LA REGLE DE LA STRATEGIE

Vous pouvez consulter et modifier les paramètres de la règle de tout type dans la fenêtre des propriétés de la règle.

Vous ne pouvez pas modifier les paramètres des règles par défaut. Les règles préinstallées ainsi que les règles que vous avez créées sont accessibles à la modification.

Pour modifier la règle de la stratégie, procédez comme suit :

1. Ouvrez la liste des règles des stratégies (cf. section "Consultation de la liste des règles des stratégies" à la page 63).

   Dans le cas du schéma de déploiement *Entreprise*, vous pouvez modifier les règles des stratégies du niveau de l'entreprise uniquement dans la liste des règles de la stratégie du niveau de l'entreprise (dans l'entrée **Stratégies de l'entreprise**, faisant partie de l'entrée **Entreprise**). Dans la liste des règles des stratégies du groupe et de l'entreprise (dans l'entrée **Stratégies** qui fait partie de l'entrée du groupe), les règles des stratégies du niveau de l'entreprise peuvent uniquement être consultées.

2. Sélectionnez dans la liste une règle, les paramètres de laquelle vous voulez modifier, et ouvrez la fenêtre des propriétés de la règle par un des moyens suivants :

   - à l'aide du bouton **Modifier** situé dans la barre d'outils ;
   - en double-cliquant sur la règle sélectionnée ;
   - à l'aide de l'option du menu contextuel.

   L'ensemble des paramètres dans la fenêtre des propriétés de la règle dépend du type de règle sélectionnée.

3. Sous les onglets de la fenêtre des propriétés, configurez les paramètres de la règle (cf. section "Paramètres des règles des stratégies" à la page 70).

   Par défaut, toutes les règles créées sont activées, c'est-à-dire, elles sont utilisées dans le fonctionnement de Kaspersky Anti-Virus. Si vous voulez désactiver ou activer une règle, exécutez une des actions suivantes :

   - Pour désactiver une règle, décochez la case **Activer la règle** sous l'onglet **Général**. Dans le bloc déroulant comprenant la liste des règles de la stratégie, la règle désactivée s'affiche en gris. Cette règle ne sera pas utilisée par Kaspersky Anti-Virus.
   - Pour activer la règle désactivée, cochez la case **Activer la règle** sous l'onglet **Général**.

   Vous pouvez aussi désactiver ou activer la règle à l'aide des options du menu contextuel **Désactiver** et **Activer** dans la liste des règles.

4. Cliquez sur le bouton **Appliquer**, puis sur le bouton **OK**. La fenêtre des propriétés de la règle se ferme.

5. Pour que la modification de la stratégie de Kaspersky Anti-Virus entre en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

MODIFICATION DE L'ORDRE D'APPLICATION DES REGLES DE LA STRATEGIE

Vous pouvez modifier l'ordre d'application des règles qui font partie de la stratégie en déplaçant la règle sélectionnée en haut ou en bas dans la liste des règles de la stratégie. Le déplacement de la règle est possible uniquement au sein de la stratégie à laquelle cette règle appartient.

Pour les règles par défaut, il est impossible de modifier l'ordre d'application. La règle par défaut est toujours appliquée en dernier si aucune autre règle n'a été appliquée.

Dans le cas du schéma de déploiement *Entreprise*, vous pouvez déplacer les règles de la stratégie du niveau de l'entreprise uniquement dans la liste des règles de la stratégie du niveau de l'entreprise. Dans la liste générale des règles des stratégies du groupe et de l'entreprise, les règles de la stratégie de l'entreprise peuvent uniquement être consultées.

Vous pouvez déplacer les règles de la stratégie entre les blocs des règles qui sont appliquées avant les stratégies du groupe et après les stratégies du groupe.

Le nouvel ordre d'application des règles des stratégies de Kaspersky Anti-Virus sera utilisé par l'application uniquement après l'application des modifications de la configuration.

SUPPRESSION DE LA REGLE DE LA STRATEGIE

Vous pouvez supprimer la règle sélectionnée dans le bloc de la stratégie.

Les règles par défaut ne peuvent pas être supprimées.

Dans le cas du schéma de déploiement *Entreprise*, vous pouvez supprimer les règles de la stratégie du niveau de l'entreprise uniquement dans la liste des règles de la stratégie du niveau de l'entreprise. Dans la liste générale des règles des stratégies du groupe et de l'entreprise, les règles de la stratégie de l'entreprise peuvent uniquement être consultées.

Les modifications, faisant partie des règles de la stratégie de Kaspersky Anti-Virus, entreront en vigueur uniquement après l'application des modifications de la configuration.

PARAMETRES DES REGLES DE LA STRATEGIE

La règle de la stratégie est définie par les paramètres suivants :

- **Nom de la règle**.

  Nom de la règle de la stratégie, unique dans le cadre du type de stratégie sélectionné sur un niveau de configuration.

  Si le schéma de déploiement de Kaspersky Anti-Virus suppose plusieurs niveaux de configuration de l'application, le nom de la règle de la stratégie au niveau du groupe peut coïncider avec le nom de la règle de la stratégie au niveau de l'entreprise.

- Liste des protocoles auxquels cette règle sera appliquée :

  - pour les règles de la stratégie d'exclusion de l'analyse et de la stratégie d'analyse antivirus : les protocoles HTTP, FTP, POP3 et SMTP ;

  - pour la règle de la stratégie de traitement des protocoles : les protocoles HTTP et FTP.

- Paramètres spécifiques qui correspondent au type de règle :
  - pour les règles de la stratégie de traitement des protocoles : les actions exécutées lors du traitement des connexions par les protocoles différents (cf. section "Paramètres de traitement des protocoles" à la page 71) ;
  - pour la règle de la stratégie d'exclusion de l'analyse : les paramètres d'exclusion des objets de l'analyse (cf. section "Paramètres d'exclusion de l'analyse" à la page 72) ;
  - pour la règle de la stratégie d'analyse antivirus : les paramètres de détection lors de l'analyse et les actions exécutées sur les objets infectés protégés par mot de passe et les objets pouvant contenir une menace (cf. section "Paramètres d'analyse antivirus" à la page 72).
- La liste des clients : des objets de réseau aux requêtes à partir desquels cette règle sera appliquée, et la liste des exclusions : des clients pour les requêtes à partir desquels cette règle ne fonctionnera pas.
- La liste des serveurs : des objets de réseau pour lesquels cette règle sera appliquée pour les requêtes et la liste des exclusions : des serveurs pour lesquels cette règle ne fonctionnera pas pour les requêtes.

DANS CETTE SECTION

PARAMETRES DE TRAITEMENT DES PROTOCOLES

La règle de la stratégie de traitement des protocoles est définie par l'ensemble de paramètres suivant :

- **Autoriser la reprise du téléchargement** (via le protocole HTTP).

  Prise en charge de la récupération du chargement des fichiers transmis via le protocole HTTP.

  Si la case est cochée, le programme de chargement des objets (par exemple, le gestionnaire de chargement des fichiers) peut relancer le transfert de l'objet en cas de rupture de connexion. L'activation de cette fonction augmente la sécurité de transfert des fichiers sur des connexions lentes.

  La prise en charge de la récupération du chargement via le protocole HTTP augmente le risque de pénétration d'une menace.

  Si la case est décochée, la prise en charge de la récupération du chargement sera désactivée.

  La case est décochée par défaut.

  La case est disponible si la case **Appliquer la règle au protocole HTTP** est cochée.

- **Autoriser HTTP 0.9**.

  Prise en charge de la compatibilité avec l'ancien standard du protocole HTTP version 0.9.

  Si la case est décochée, la prise en charge de la compatibilité avec le protocole HTTP 0.9 est désactivée.

  La case est décochée par défaut.

  La case est disponible si la case **Appliquer la règle au protocole HTTP** est cochée.

- **Autoriser la reprise du téléchargement** (via le protocole FTP).

  Prise en charge de la récupération du chargement des fichiers via le protocole FTP.

  Si la case est cochée, le programme de chargement des objets peut relancer le transfert de l'objet en cas de rupture de connexion. L'activation de cette fonction augmente la sécurité de transfert des fichiers sur des connexions lentes.

La prise en charge de la récupération du chargement via le protocole FTP augmente le risque de pénétration d'une menace.

Si la case est décochée, la prise en charge de la récupération du chargement sera désactivée.

La case est décochée par défaut.

La case est disponible si la case **Appliquer la règle au protocole FTP** est cochée.

- **Autoriser les commandes FTP inconnues**.

  Prise en charge des commandes inconnues à partir du client FTP.

  Si la case est cochée, Kaspersky Anti-Virus transmet les commandes inconnues sur le serveur FTP.

  Si la case est décochée, Kaspersky Anti-Virus bloque les commandes inconnues.

  La case est décochée par défaut.

  La case est disponible si la case **Appliquer la règle au protocole FTP** est cochée.

Les commandes suivantes de FTP sont prises en charge : USER, PASS, ACCT, CWD, CDUP,SMNT, QUIT, REIN, PORT, PASV, TYPE, STRU, MODE, RETR, STOR, STOU, APPE, ALLO, REST, RNFR, RNTO, ABOR, DELE, RMD, MKD, PWD, LIST, NLST, SITE, SYST, STAT, HELP, NOOP, FEAT, OPTS, SIZE, MDTM, MLST, MLSD, EPRT, EPSV, XMKD, XRMD, XPWD, XCUP, XCWD.

PARAMETRES D'EXCLUSION DE L'ANALYSE

La règle de la stratégie d'exclusion de l'analyse est définie par l'ensemble de paramètres suivant :

- **Exclure tous les objets**.

  Kaspersky Anti-Virus exclut de l'analyse tous les objets transmis via le protocole sélectionné.

- **Exclure les types sélectionnés des objets**.

  Lors du traitement du trafic transmis via les protocoles HTTP et FTP, Kaspersky Anti-Virus exclut de l'analyse uniquement les objets sélectionnés dans la liste des types des objets. Pour tous les autres objets, l'analyse est exécutée.

- **Exclure les objets joints pour les protocoles HTTP, FTP, SMTP, POP3**.

  L'exclusion de l'analyse des objets qui sont inclus dans les objets-conteneurs. L'objet-conteneur contient des objets joints. Par exemple, les archives sont des objets-conteneurs, ainsi que les messages avec les pièces jointes, les images de disques.

  Si la case est cochée, Kaspersky Anti-Virus exclut de l'analyse tous les objets joints transmis par les protocoles HTTP et FTP et les objets joints du niveau 2 ou plus transmis par les protocoles SMTP et POP3.

  Si la case n'est pas cochée, Kaspersky Anti-Virus analyse tous les objets joints.

  La case est accessible si l'option **Exclure les types sélectionnés des objets** a été sélectionnée.

  Par défaut, la case **Exclure les objets joints pour les protocoles HTTP, FTP, SMTP, POP3** n'est pas cochée.

PARAMETRES DE L'ANALYSE ANTIVIRUS

La règle de la stratégie d'analyse antivirus est définie par l'ensemble de paramètres suivant :

- Les paramètres de détection applicables par Kaspersky Anti-Virus. Par défaut, l'application détecte les choses suivantes :
  - virus et vers ;
  - chevaux de Troie ;
  - utilitaires malveillants ;

- programmes publicitaires ;
- programmes pornographiques ;
- autres programmes ;
- menaces non identifiées.

L'application peut aussi détecter les objets qui correspondent probablement aux paramètres de détection.

- Les actions exécutées par Kaspersky Anti-Virus sur les objets qui correspondent aux paramètres de détection :
  - **Bloquer**.

    Kaspersky Anti-Virus bloque les objets qui correspondent aux paramètres de détection définis dans la fenêtre **Configuration des paramètres de détection**.

    En cas de blocage de l'objet, Kaspersky Anti-Virus ne transmet pas l'objet bloqué au client. Le client reçoit un message lui indiquant que l'objet a été bloqué.

    Kaspersky Anti-Virus ne transmet pas le message sur le blocage de l'objet si la partie de l'objet a été transmis au client avant la fin de l'analyse ou si le transfert des objets est effectué via le protocole FTP.

    Cette valeur est sélectionnée par défaut.

  - **Réparer**.

    Kaspersky Anti-Virus tente de réparer les objets qui correspondent aux paramètres de détection définis dans la fenêtre **Configuration des paramètres de détection**. Si la réparation de l'objet est impossible, Kaspersky Anti-Virus bloque l'objet.

  - **Supprimer les objets joints irréparables**.

    Suppression des parties infectées des objets composés. S'il est impossible de supprimer la partie infectée, Kaspersky Anti-Virus bloque tout l'objet-conteneur.

    La case est accessible si l'option **Réparer** a été sélectionnée en tant qu'action à exécuter sur l'objet.

    La case est décochée par défaut.

  - **Enregistrer les copies des objets dans la sauvegarde**.

    Enregistrement dans la Sauvegarde des copies des objets bloqués ou réparés par Kaspersky Anti-Virus. Les objets dont les copies sont enregistrées dans la sauvegarde peuvent être supprimés ou enregistrés sur le disque local ou réseau.

    La case est décochée par défaut.

- Actions que Kaspersky Anti-Virus exécute sur les objets protégés par mot de passe :
  - **Bloquer les objets protégés par mot de passe**.

    Prévention automatique du téléchargement des objets protégés par mot de passe.

    Si la case est décochée, Kaspersky Anti-Virus télécharge les objets protégés par mot de passe sans les analyser.

    Le transfert libre des objets, protégés par mot de passe, augmente le risque de pénétration des menaces.

    La case est décochée par défaut.

  - **Enregistrer les copies des objets dans la sauvegarde**.

    Enregistrement dans la Sauvegarde des copies des objets protégés par mot de passe, bloqués par Kaspersky Anti-Virus. Les objets dont les copies sont enregistrées dans la sauvegarde peuvent être supprimés ou enregistrés sur le disque local ou réseau.

    La case est accessible si la case **Bloquer les objets protégés par mot de passe** est cochée.

    Par défaut, la case **Enregistrer les copies des objets dans la Sauvegarde** est décochée.

CONFIGURATION DES PARAMETRES. ANALYSE DU TRAFIC TRANSMIS VIA LES PROTOCOLES

Cette section contient des informations sur les paramètres d'analyse du trafic transmis via les protocoles HTTP, FTP, SMTP et POP3, et décrit la procédure de configuration des paramètres d'analyse du trafic.

Les paramètres d'analyse du trafic sont appliqués pour toutes les connexions et définissent les règles de traitement du flux des données transmises via les protocoles HTTP et FTP, ainsi que les modèles de changement de l'objet des messages électroniques bloqués.

DANS CETTE SECTION

CONFIGURATION DES PARAMETRES D'ANALYSE DU TRAFIC

Pour configurer les paramètres d'analyse du trafic, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres d'analyse** (cf. section "**Fenêtre Paramètres d'analyse. Navigation**" à la page 26).
2. Configurez les paramètres d'analyse du trafic sous un des onglets suivants de la fenêtre :
   - **HTTP** (cf. section "**Paramètres d'analyse du trafic HTTP**" à la page 74) ;
   - **FTP** (cf. section "**Paramètres d'analyse du trafic FTP**" à la page 75) ;
   - **SMTP** (cf. section "**Paramètres d'analyse du trafic SMTP et POP3**" à la page 76) ;
   - **POP3** (cf. section "**Paramètres d'analyse du trafic SMTP et POP3**" à la page 76).
3. Si vous voulez revenir aux valeurs des paramètres d'analyse, installées par défaut, cliquez sur le bouton **Restaurer les valeurs par défaut**.
4. Cliquez sur le bouton **OK**. La fenêtre **Paramètres d'analyse** se ferme.
5. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

PARAMETRES D'ANALYSE DU TRAFIC HTTP

Pour configurer l'analyse du trafic HTTP, les paramètres suivants sont prévus :

- **Temps maximal avant l'envoi des données au client (sec)**.

  Temps maximal durant lequel Kaspersky Anti-Virus retarde l'envoi des données analysées. Dans la limite de cette période de temps, Kaspersky Anti-Virus exécute le téléchargement et l'analyse des données. Si à l'expiration du délai imparti, l'objet n'a pas été entièrement téléchargé ou Kaspersky Anti-Virus n'a pas terminé son analyse, le transfert des données au client est effectué. Une partie des données n'est pas transmise au client jusqu'à la fin de l'analyse.

La plage des valeurs est de 0 à 3600 secondes.

La valeur par défaut est 30 secondes.

- **Volume de données retenu avant la fin de l'analyse (%)**.

  Partie des données (en pourcentage) que Kaspersky Anti-Virus ne transmet pas au client avant la fin de l'analyse et avant la fin de l'analyse de l'objet.

  Kaspersky Anti-Virus analyse uniquement l'objet entièrement téléchargé. Pour accélérer l'obtention de l'objet par le poste client, le transfert des données commence avant la fin de l'analyse de l'objet, mais seul l'objet analysé sera entièrement transmis (à condition qu'il ne contienne aucune menace). Si Kaspersky Anti-Virus n'a pas eu le temps d'analyser l'objet pendant le délai imparti pour l'analyse d'un objet, l'objet est transmis sans être analysé.

  Prend la valeur dans la plage de 10 à 90%.

  La valeur par défaut est 30%.

- **Vitesse de transfert des données au client avant la fin de l'analyse de l'objet**.

  Vitesse relative avec laquelle Kaspersky Anti-Virus transmet l'objet non analysé au client ayant demandé cet objet.

  Le transfert d'une partie des données au client avant la fin de l'analyse s'effectue dans le but de maintenir la connexion avec le client. Il n'est pas recommandé de transmettre sans les analyser d'importants fragments d'objet parce que ceci augmente le risque de pénétration d'une menace.

  Plus le curseur est à droite, plus la vitesse de transfert des données au client est élevée.

  Par défaut, le curseur est placé sur le second segment de la règle à gauche. La valeur optimale du paramètre peut être obtenue uniquement avec l'expérience parce que la valeur dépend de la vitesse de l'analyse antivirus et de la vitesse de transfert des données selon le canal de réseau utilisé.

PARAMETRES D'ANALYSE DU TRAFIC FTP

Pour configurer l'analyse du trafic FTP, les paramètres suivants sont prévus :

- **Temps maximal avant l'envoi des données au client (sec)**.

  Temps maximal durant lequel Kaspersky Anti-Virus retarde l'envoi des données analysées. Dans la limite de cette période de temps, Kaspersky Anti-Virus exécute le téléchargement et l'analyse des données. Si à l'expiration du délai imparti, l'objet n'a pas été entièrement téléchargé ou Kaspersky Anti-Virus n'a pas terminé son analyse, le transfert des données au client est effectué. Une partie des données n'est pas transmise au client jusqu'à la fin de l'analyse.

  La plage des valeurs est de 0 à 3600 secondes.

  La valeur par défaut est 15 secondes.

- **Volume de données retenu avant la fin de l'analyse (%)**.

  Partie des données (en pourcentage) que Kaspersky Anti-Virus ne transmet pas au client avant la fin de l'analyse et de l'analyse de l'objet.

  Kaspersky Anti-Virus analyse uniquement l'objet entièrement téléchargé. Pour accélérer l'obtention de l'objet par le poste client, le transfert des données commence avant la fin de l'analyse de l'objet, mais seul l'objet analysé sera entièrement transmis (à condition qu'il ne contienne aucune menace). Si Kaspersky Anti-Virus n'a pas eu le temps d'analyser l'objet pendant le délai imparti pour l'analyse d'un objet, l'objet est transmis sans être analysé.

  Prend la valeur dans la plage de 10 à 90%.

  La valeur par défaut est 10%.

PARAMETRES D'ANALYSE DU TRAFIC SMTP ET POP3

Pour configurer l'analyse du trafic SMTP et POP3, les paramètres suivants sont prévus :

- **Remplacer le texte du champ "Sujet" des messages infectés**.

  Le changement du contenu du champ **Sujet** des messages infectés par le texte composé selon un modèle défini. La modification du champ **Sujet** permet au destinataire d'identifier visuellement le message, qui contient des objets infectés, sans ouvrir ce message.

  Si la case est cochée, le champ de saisie requiert l'indication du texte qui sera affiché à la place de l'objet des messages infectés. Une variable à partir de la liste déroulante **Ajouter une macro** peut être ajoutée dans le texte, qui remplace l'objet des messages infectés.

  Si la case est décochée, après le traitement par Kaspersky Anti-Virus le message infecté avec l'en-tête d'origine est transmis à l'utilisateur.

  La case est cochée par défaut.

- **Ajouter une macro**.

  Bouton déroulant qui permet d'ajouter une variable dans le texte qui modifie l'objet des messages infectés.

  Contient la macro **%SUBJECT%**, qui permet d'ajouter dans le texte l'objet d'origine du message.

  Ce bouton est disponible si la case **Changer le texte du champ "Objet" des messages infectés** est cochée.

CONFIGURATION DES PARAMETRES. PRODUCTIVITE DE L'ANALYSE

Les paramètres de productivité de l'analyse permettent d'optimiser le fonctionnement de Kaspersky Anti-Virus au niveau du serveur séparé.

Pour configurer les paramètres de productivité de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres du serveur** (cf. section "**Fenêtre Paramètres du serveur. Navigation**" à la page 24).
2. Sélectionnez l'onglet **Productivité**.
3. Configurez les paramètres de productivité de l'analyse conformément à vos exigences :

   - **Nombre d'instances du moteur antivirus**.

     Nombre d'instances du moteur antivirus de l'application, qui fonctionneront simultanément pour augmenter la capacité de trafic de Kaspersky Anti-Virus lors du traitement des flux de données importants.

     La valeur de ce paramètre est calculée par défaut selon la formule 2n+1, où n est le nombre de processus logiques du serveur physique sur lequel est installé le pare-feu de Microsoft ISA Server/Forefront TMG.

     Prend la valeur dans la plage de 1 à 256.

   - **Pour analyser uniquement les objets "rapides"**.

     Nombre d'instances du moteur (de 1 à 255) réservés par l'application pour analyser les objets "rapides".

     Le moteur antivirus peut fonctionner simultanément uniquement avec un objet. Pour éviter une situation où tous les moteurs sont occupés par l'analyse des objets de grande taille et où les objets plus petits s'accumulent dans la file d'attente, il est recommandé de sélectionner au moins un moteur pour analyser les objets "rapides".

     Un moteur antivirus est sélectionné par défaut pour analyser les objets "rapides".

     Uniquement les objets du trafic HTTP, correspondants aux critères suivants, se rapportent aux objets "rapides" :

     - les fichiers texte de taille inférieure à 2 Mo ;
     - les fichiers graphiques de taille inférieure à 2 Mo ;
     - tous les autres objets (excepté les objets exécutables) de taille inférieure à 256 Ko.

- **Nombre maximal d'objets analysés dans la mémoire**.

  Nombre maximal des objets que Kaspersky Anti-Virus analyse dans la mémoire vive du serveur sans les sauvegarder sur le disque dur.

  Si l'objet est de taille supérieure au paramètre défini **Taille maximale des objets analysés dans la mémoire** ou un nombre d'objets, égal au paramètre **Nombre maximal d'objets analysés dans la mémoire** est analysé dans la mémoire, l'objet est d'abord sauvegardé sur le disque dur.

  La plage des valeurs possibles est comprise entre 1 à 1024 objets, inclus.

  Par défaut, 128 objets sont analysés dans la mémoire.

- **Taille maximal de l'objet analysé dans la mémoire (Ko)**.

  Taille maximale des objets que Kaspersky Anti-Virus analyse dans la mémoire vive sans les sauvegarder sur le disque dur.

  Si l'objet est de taille supérieure au paramètre défini **Taille maximale des objets analysés dans la mémoire** ou un nombre d'objets, égal au paramètre **Nombre maximal d'objets analysés dans la mémoire** est analysé dans la mémoire, l'objet est d'abord sauvegardé sur le disque dur.

  La plage des valeurs possibles de la taille des objets analysés dans la mémoire est de 16 à 1024 Ko.

  Par défaut, la taille maximale est limitée par 128 Ko.

- **Nombre maximal des objets en attente d'analyse**.

  Nombre maximal des objets que Kaspersky Anti-Virus place en attente de traitement. Si le nombre indiqué des objets se trouve en attente de traitement, un nouvel objet est transmis sans être analysé. Kaspersky Anti-Virus ajoute les informations sur l'objet transmis sans analyse, dans le Journal de l'analyse du trafic.

  La longueur maximale de la file d'attente est de 16383 objets. La file d'attente ne peut pas être inférieure à un objet.

  Par défaut, 1024 objets sont compris dans la file d'attente.

- **Temps maximal d'analyse, sec**.

  Temps maximal en secondes durant lequel Kaspersky Anti-Virus analyse l'objet téléchargé. Si le temps d'analyse dépasse la valeur indiquée, l'objet est transmis au client sans être analysé. Kaspersky Anti-Virus ajoute les informations sur l'objet transmis sans analyse, dans le Journal de l'analyse du trafic.

  La plage des valeurs est comprise entre 1 et 86400 secondes, inclus.

  La valeur par défaut est 1800 secondes.

4. Si vous voulez revenir aux valeurs par défaut des paramètres d'analyse, cliquez sur le bouton **Restaurer les valeurs par défaut**.

5. Cliquez sur le bouton **OK**. La fenêtre **Paramètres du serveur** se ferme.

6. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

SAUVEGARDE

Cette section contient des informations sur la sauvegarde de Kaspersky Anti-Virus, sur la manipulation des objets placés dans la sauvegarde et sur la configuration des paramètres de celle-ci.

DANS CETTE SECTION

A PROPOS DE LA SAUVEGARDE

Conformément aux paramètres d'analyse antivirus, Kaspersky Anti-Virus peut conserver la copie de l'objet dans la sauvegarde avant de bloquer ou de réparer cet objet. Dans ce cas, les informations sur l'objet sont enregistrées dans la Base de données de la sauvegarde et des statistiques.

Kaspersky Anti-Virus peut conserver les données suivantes : l'adresse IP du client, l'adresse IP du serveur, les noms des objets classés par l'application comme infectés ou potentiellement infectés, les objets des messages classés par l'application comme infectés ou potentiellement infectés.

La sauvegarde se place sur le serveur dans le dossier de sauvegarde des données de l'application. En cas d'utilisation des schémas de déploiement *Groupe Autonome* et *Entreprise*, la sauvegarde s'installe sur chaque serveur sur lequel le composant Serveur de sécurité est installé (cf. section "Composition des modules et des sous-systèmes de Kaspersky Anti-Virus" à la page 15). Les copies des objets sont conservées dans la sauvegarde du serveur sur lequel ces objets ont été détectés.

La Base de données de la sauvegarde et des statistiques est placée sur le serveur SQL indiqué lors de l'installation de l'application. Pendant l'utilisation de l'application, vous pouvez indiquer un autre emplacement de la Base de données de la sauvegarde et des statistiques (cf. section "Configuration des paramètres de connexion à la Base de données de la sauvegarde et des statistiques" à la page 85).

L'option de déploiement de la Base de données de la sauvegarde et des statistiques dépend du schéma de déploiement de Kaspersky Anti-Virus utilisé :

- En cas d'utilisation du schéma de déploiement *Serveur autonome*, les informations sur tous les objets placés dans la sauvegarde, sont enregistrées dans une base de données sur le serveur SQL (cf. ill. ci-après).

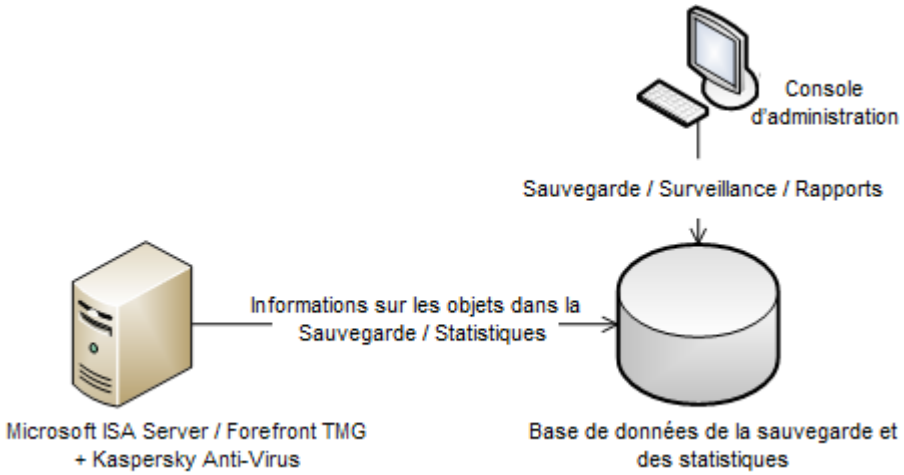

Illustration 10. Schéma de déploiement Serveur autonome

- En cas d'utilisation du schéma de déploiement *Groupe Autonome*, tous les serveurs du groupe utilisent la base unique des données pour sauvegarder les informations sur les objets placés dans la sauvegarde. Ainsi, les informations sur les objets placés dans la sauvegarde de tous les serveurs d'un groupe, sont enregistrées de manière centralisée (cf. ill. ci-après).

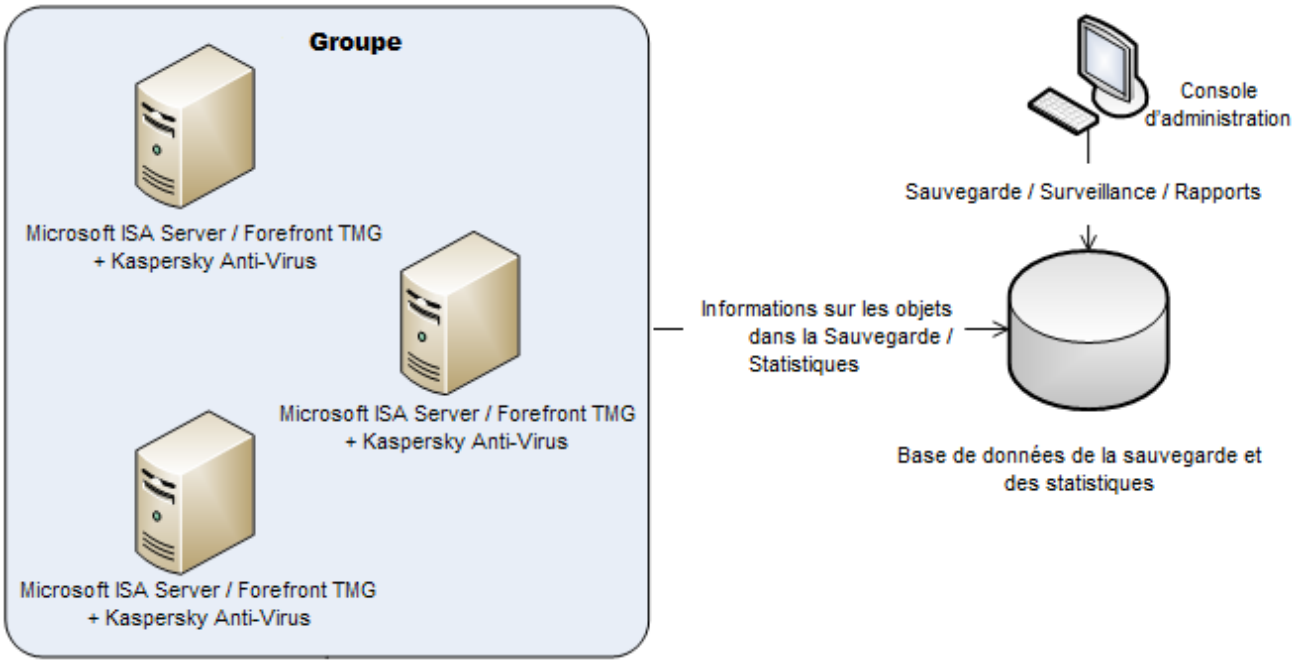

Illustration 11. Schéma de déploiement Groupe Autonome

- En cas d'utilisation du schéma de déploiement *Entreprise*, il est possible d'utiliser la Base unique de données de la sauvegarde et des statistiques pour tous les groupes de l'entreprise ou les Bases séparées de données de la sauvegarde et des statistiques pour chaque groupe ou le bloc des groupes. L'administration centralisée des objets placés dans la sauvegarde, est prise en charge uniquement si tous les groupes de l'entreprise utilisent la Base unique de données de la sauvegarde et des statistiques (cf. ill. ci-après).

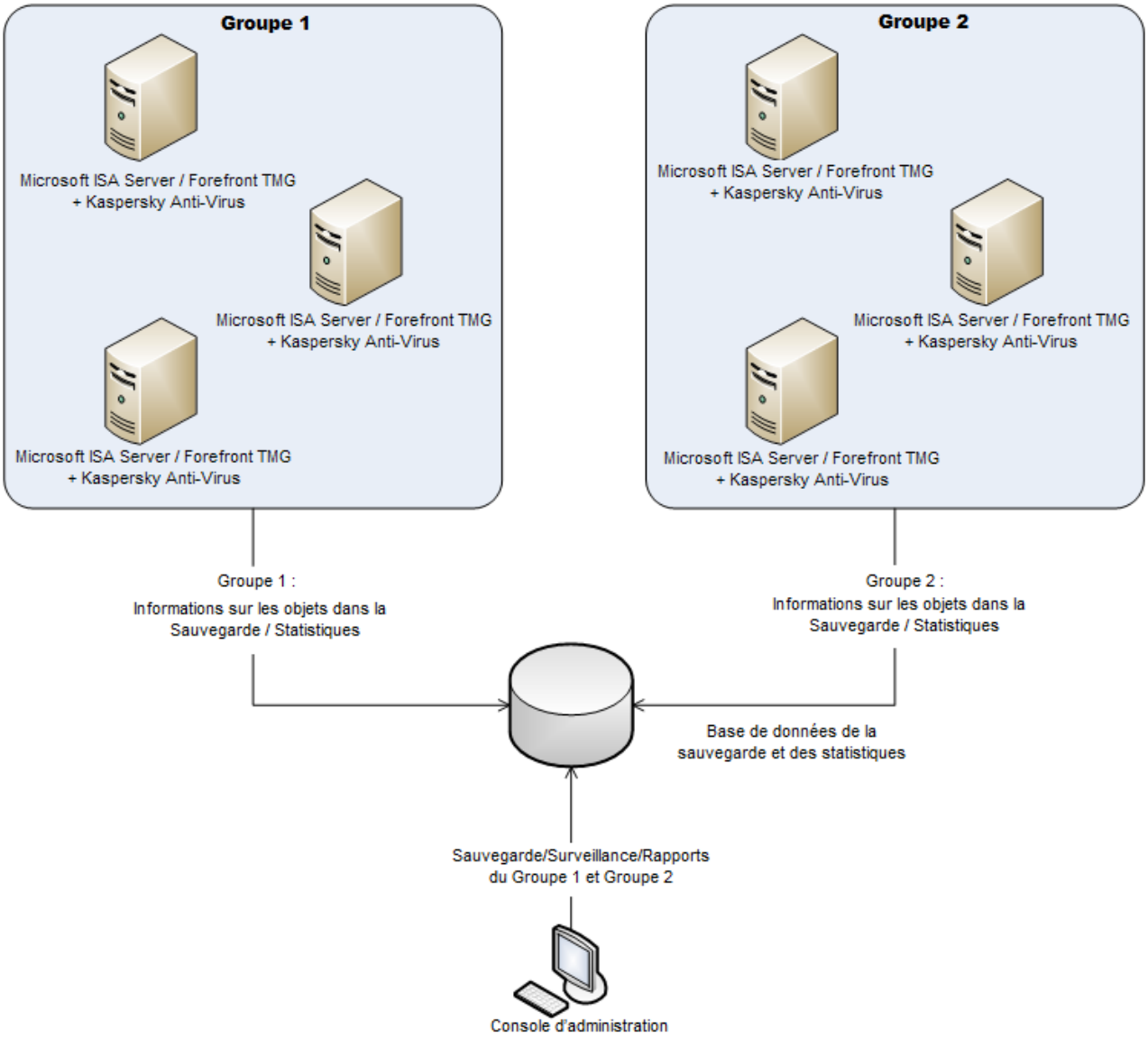

Illustration 12. Schéma de déploiement Entreprise : Base de données de la sauvegarde et des statistiques unique

L'option de déploiement de la Base de données de la sauvegarde et des statistiques est définie à l'étape de déploiement de l'application (cf. le *Manuel d'installation de "Kaspersky Anti-Virus 8.5 for Microsoft ISA Server and Forefront TMG"*).

La manipulation des objets placés dans la sauvegarde est effectuée via la Console d'administration de Kaspersky Anti-Virus (cf. section "Fenêtre principale" à la page 19).

La connexion de la Console d'administration à la Base de données de la sauvegarde et des statistiques s'effectue sous le compte utilisateur au nom duquel la Console d'administration a été lancée. Avant de commencer le travail avec les objets de la sauvegarde, assurez-vous que votre compte possède les privilèges de lecture et d'enregistrement des informations dans la Base de données de la sauvegarde et des statistiques.

En cas de déploiement de Kaspersky Anti-Virus dans le groupe de travail, il faut assurer également la possibilité de connexion à la Base de données de la sauvegarde et des statistiques. Pour ce faire, procédez comme suit :

1. Sur le serveur physique sur lequel le système d'administration de la base de données Microsoft SQL Server est installé avec la Base de données de la sauvegarde et des statistiques, créer un compte, via les outils du système d'exploitation Microsoft Windows, identique au compte sous lequel la Console d'administration de Kaspersky Anti-Virus se lance.

2. Configurer, pour le compte créé, les privilèges d'accès nécessaires à la Base de données de la sauvegarde et des statistiques via les outils du système d'administration des bases de données Microsoft SQL Server.

CONSULTATION DE LA LISTE DES OBJETS DE LA SAUVEGARDE

L'affichage de la liste des objets, placés dans la sauvegarde, dépend du schéma de déploiement de Kaspersky Anti-Virus.

Schéma de déploiement *Serveur autonome*

- *Pour consulter la liste des objets de la sauvegarde, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée du serveur et sélectionnez l'entrée jointe **Sauvegarde** (cf. section "**Fenêtre principale**" à la page 19).

   Le panneau des résultats affichera les informations sur les objets placés dans la sauvegarde du serveur.

Schéma de déploiement *Groupe Autonome*

- *Pour consulter la liste des objets de la sauvegarde, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée du groupe et sélectionnez l'entrée jointe **Sauvegarde** (cf. section "**Fenêtre principale**" à la page 19).

   Le panneau des résultats affichera les informations sur les objets placés dans les sauvegardes de tous les serveurs du groupe.

Schéma de déploiement *Entreprise*

- *Pour consulter la liste des objets de la sauvegarde, procédez comme suit :*

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Exécutez une des actions suivantes :

   - Déployez l'entrée du groupe et sélectionnez l'entrée jointe **Sauvegarde** (cf. section "**Fenêtre principale**" à la page 19).

     Le panneau des résultats affichera les informations sur les objets placés dans les Sauvegardes de tous les serveurs du groupe sélectionné.

- Déployez l'entrée **Entreprise**, sélectionnez l'entrée jointe **Sauvegarde** et cliquez sur le bouton **Sélectionner** situé dans la partie supérieure du panneau des résultats. Dans la fenêtre **Base de données** qui s'ouvre, sélectionnez la base de données de la sauvegarde et des statistiques dont vous souhaitez consulter les informations et cliquez sur le bouton **OK**.

  Le panneau des résultats affiche les informations sur les objets, obtenues à partir de la Base de données de la sauvegarde et des statistiques sélectionnée.

La partie inférieure du panneau des résultats de l'entrée **Sauvegarde** affiche les informations sur le nombre et le volume total des objets dont les informations sont enregistrées dans la Base de données de la sauvegarde et des statistiques. Outre cela, si dans la liste des objets un ou plusieurs objets ont été choisis, la partie inférieure du panneau des résultats affiche les informations sur le nombre et le volume total des objets sélectionnés.

Les informations sur les objets de la sauvegarde s'affichent page par page.

Pour se déplacer entre les pages, vous pouvez utiliser les boutons de navigation, situés dans la partie supérieure du panneau des résultats.

La liste des objets de la sauvegarde prévoit une fonction de tri. Vous pouvez exécuter le tri de la liste selon une des colonnes du tableau qui contient des informations sur les objets.

Outre cela, lors de l'utilisation de la liste des objets de la sauvegarde, vous pouvez configurer la composition et l'ordre des attributs des objets affichés dans le tableau.

La composition configurée et l'ordre des attributs des objets s'enregistrent lors des lancements suivants de la Console d'administration.

FILTRAGE DE LA LISTE DES OBJETS DE LA SAUVEGARDE

Pour faciliter la consultation et la recherche d'informations sur les objets, le filtrage des données est prévu.

Le filtre permet de sélectionner les objets selon les valeurs texte dans toutes les colonnes du tableau qui sont affichées au moment de recherche, sauf les colonnes **Résultat du traitement** et **Taille (octets)**.

Le champ de saisie de la requête de recherche est situé au-dessus de la barre d'outils.

OPERATIONS SUR LES OBJETS DE LA SAUVEGARDE

Vous pouvez exécuter les actions suivantes sur les objets placés dans la sauvegarde :

- consulter les propriétés des objets de la sauvegarde (cf. section "Consultation des propriétés de l'objet" à la page 83) ;
- supprimer les objets de la sauvegarde (cf. section "Suppression de l'objet de la sauvegarde" à la page 83) ;
- conserver les objets de la sauvegarde à l'endroit indiqué sur le disque local ou réseau (cf. section "Enregistrement de l'objet de la sauvegarde" à la page 84).

Le placement des objets dans la sauvegarde est exécuté automatiquement, si la conservation des copies des objets détectés dans la sauvegarde est activée (cf. section "Paramètres d'analyse antivirus" à la page 72). La possibilité de placer manuellement les objets dans la sauvegarde n'est pas prévue.

DANS CETTE SECTION

CONSULTATION DES PROPRIETES DE L'OBJET

Pour consulter les propriétés de l'objet placé dans la sauvegarde, procédez comme suit :

1. Ouvrez la liste des objets de la sauvegarde (cf. section "Consultation de la liste des objets de la sauvegarde" à la page 81) et sélectionnez l'objet dont vous souhaitez consulter les propriétés.

   Pour rechercher l'objet requis, vous pouvez utiliser le tri de la liste ou le filtrage (cf. section "Filtrage de la liste des objets de la sauvegarde" à la page 82).

2. Ouvrez la fenêtre **Propriétés de l'objet** à l'aide d'un des moyens suivants :

   - à l'aide du bouton **Propriétés** situé dans barre d'outils ;
   - en cliquant sur la touche **ENTER** ;
   - à l'aide de l'option du menu contextuel ;
   - à l'aide du double click de la souris sur l'objet sélectionné.

   La fenêtre **Propriétés de l'objet** affichera tous les attributs de l'objet sélectionné.

SUPPRESSION DE L'OBJET DE LA SAUVEGARDE

La suppression des objets de la sauvegarde peut être exécutée manuellement ou automatiquement.

Vous pouvez supprimer tous les objets de la sauvegarde ou uniquement les objets sélectionnés.

Pour supprimer les objets de la sauvegarde, procédez comme suit :

1. Ouvrez la liste des objets de la sauvegarde (cf. section "Consultation de la liste des objets de la sauvegarde" à la page 81).

2. Supprimez l'objet ou les objets par un des moyens suivants :

   - à l'aide du bouton **Supprimer** situé dans barre d'outils ;
   - en cliquant sur la touche **DELETE** ;
   - à l'aide de l'option du menu contextuel.

En même temps que la suppression de l'objet de la sauvegarde, les informations sur l'objet sont supprimées de la Base de données de la sauvegarde et des statistiques.

La suppression automatique des objets de la sauvegarde est effectuée en fonction de la restriction établie pour la taille de la sauvegarde sur le serveur (cf. section "Configuration de la taille de la sauvegarde sur le serveur" à la page 84).

ENREGISTREMENT DE L'OBJET DE LA SAUVEGARDE

Vous pouvez enregistrer les objets de la sauvegarde à l'emplacement indiqué sur le disque local ou de réseau.

N'oubliez pas que l'enregistrement des objets de la sauvegarde sur le disque dur peut infecter l'ordinateur.

La possibilité de conservation d'un ou de plusieurs objets choisis dans le tableau est prévue.

Les objets sont enregistrés au format d'origine.

PARAMETRES DE LA SAUVEGARDE

Vous pouvez configurer les paramètres suivants de la sauvegarde :

- la taille maximale de la sauvegarde sur le serveur (cf. section "Configuration de la taille de la sauvegarde sur le serveur" à la page 84) ;
- les paramètres de connexion à la Base de données de la sauvegarde et des statistiques (cf. section "Configuration des paramètres de connexion à la Base de données de la sauvegarde et des statistiques" à la page 85).

DANS CETTE SECTION

CONFIGURATION DE LA TAILLE DE LA SAUVEGARDE SUR LE SERVEUR

Pour configurer la taille de la sauvegarde sur le serveur, procédez comme suit :

1. Ouvrez la fenêtre **Paramètres du serveur** (cf. section "**Fenêtre Paramètres du serveur. Navigation**" à la page 24).
2. Sélectionnez l'onglet **Général**.
3. Configurez la valeur du paramètre **Taille maximale de la sauvegarde (Mo)**.

   Taille maximale totale des objets que Kaspersky Anti-Virus conserve dans la Sauvegarde. Si la taille de l'objet qui entre dans la Sauvegarde, au total avec les objets déjà présents, dépasse la valeur indiquée, l'objet qui est entré le premier sera supprimé.

   La plage des valeurs possibles est de 1 à 1048576 Mo.

   Par défaut, la taille maximale de la Sauvegarde est de 5120 Mo.
4. Cliquez sur le bouton **OK**. La fenêtre **Paramètres du serveur** se ferme.
5. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

CONFIGURATION DES PARAMETRES DE CONNEXION A LA BASE DE DONNEES DE LA SAUVEGARDE ET DES STATISTIQUES

Pour configurer les paramètres de connexion à la Base de données de la sauvegarde et des statistiques, procédez comme suit :

1. Ouvrez une des fenêtres suivantes de configuration des paramètres de l'application :

   - si le schéma de déploiement utilisé est *Serveur autonome :* la fenêtre **Paramètres du serveur** (cf. section "**Fenêtre Paramètres du serveur. Navigation**" à la page 24) ;

   - si le schéma de déploiement utilisé est *Groupe Autonome* ou *Entreprise :* la fenêtre **Paramètres du groupe** (cf. section "**Fenêtre Paramètres du groupe. Navigation**" à la page 25).

2. Sélectionnez l'onglet **Sauvegarde** et cliquez sur le bouton **Modifier**.

3. Dans la fenêtre **Paramètres de connexion** qui s'ouvre, configurez les paramètres de connexion à la Base de données de la sauvegarde et des statistiques conformément à vos exigences :

   - Le compte, indiqué lors de l'installation, est utilisé pour se connecter à la Base de données de la sauvegarde et des statistiques. Le cas échéant, indiquez un autre compte pour se connecter à la Base de données de la sauvegarde et des statistiques utilisée.

     Le compte indiqué doit posséder les privilèges de lecture et d'enregistrement des informations dans la Base de données de la sauvegarde et des statistiques.

   - Le cas échéant, configurez l'emplacement des informations sur les objets de la sauvegarde dans une autre base de données. Saisissez le nom du serveur SQL et le nom de la base de données créée auparavant sur le serveur SQL.

     La possibilité de déplacer les informations d'une base de données à une autre via les outils Kaspersky Anti-Virus n'est pas prévue. Vous pouvez exécuter le déplacement des données via les outils du système d'administration des bases de données Microsoft SQL Server.

4. Cliquez sur le bouton **OK**. La fenêtre de configuration des paramètres de l'application se ferme.

5. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

DIAGNOSTIC

Les informations sur le fonctionnement de l'application peuvent être enregistrées dans les journaux de Kaspersky Anti-Virus, consignées dans le journal des événements du système d'exploitation Microsoft Windows et transmises dans le sous-système des notifications Microsoft ISA Server/Forefront TMG

La fonction d'obtention des notifications de Microsoft ISA Server/Forefront TMG par courrier électronique est configurée via Microsoft ISA Server/Forefront TMG.

Cette section contient des informations sur les journaux de Kaspersky Anti-Virus, sur la configuration des paramètres de gestion de ces journaux, ainsi que des informations sur les journaux des événements Microsoft Windows.

DANS CETTE SECTION

A PROPOS DES JOURNAUX DES EVENEMENTS

Kaspersky Anti-Virus enregistre les informations sur son fonctionnement dans les journaux des événements suivants :

- Le journal des événements du système d'exploitation Microsoft Windows. La source isav est indiquée pour les journaux liés au fonctionnement de Kaspersky Anti-Virus.
- Journal de Kaspersky Anti-Virus :
  - Journal de l'analyse du trafic. Contient les informations sur les objets qui correspondent aux paramètres de détection et les informations sur les actions exécutées par Kaspersky Anti-Virus par rapport à ces objets. Le nom du fichier journal de l'analyse du trafic inclut la date de création du journal et possède le format viruslogYYYYMMDD.log, où DD correspond au jour, MM au mois et YYYY à l'année.
  - Journal de fonctionnement de l'application. Contient les informations sur les événements apparus pendant le fonctionnement de Kaspersky Anti-Virus. Le nom du fichier journal de fonctionnement de l'application inclut la date de création du journal et possède le format kavisaYYYYMMDD.log, où DD correspond au jour, MM au mois et YYYY à l'année.
  - Journal de fonctionnement des filtres. Contient les informations sur les événements apparus pendant le fonctionnement des filtres de Kaspersky Anti-Virus. Le nom du fichier journal de fonctionnement des filtres inclut la date de création du journal et possède le format kavfltYYYYMMDD.log, où DD est le jour, MM le mois et YYYY l'année.

Les fichiers journaux de Kaspersky Anti-Virus sont conservés dans le dossier logs situé dans le dossier de conservation des données de l'application sur le serveur.

Vous pouvez configurer les paramètres de gestion des journaux de Kaspersky Anti-Virus (cf. section "Configuration des paramètres de gestion des journaux de Kaspersky Anti-Virus" à la page 87).

CONFIGURATION DES PARAMETRES DE GESTION DES JOURNAUX DE KASPERSKY ANTI-VIRUS

Pour configurer les paramètres de gestion des journaux de Kaspersky Anti-Virus, procédez comme suit :

1. Ouvrez une des fenêtres suivantes de configuration des paramètres de l'application :

   - si le schéma de déploiement utilisé est *Serveur autonome* : la fenêtre **Paramètres du serveur** (cf. section "**Fenêtre Paramètres du serveur. Navigation**" à la page 24) ;

   - si le schéma de déploiement utilisé est *Groupe Autonome* ou *Entreprise* : la fenêtre **Paramètres du groupe** (cf. section "**Fenêtre Paramètres du groupe. Navigation**" à la page 25).

2. Sélectionnez l'onglet **Journaux**.

3. Configurez le niveau de diagnostic en indiquant les valeurs des paramètres suivants :

   - **Journal de l'analyse du trafic**.

     Niveau de détails des informations enregistrées dans le Journal de l'analyse du trafic. Ce journal contient les informations sur les objets analysés qui correspondent aux paramètres de détection et les informations sur les actions exécutées par Kaspersky Anti-Virus par rapport à ces objets.

     Les niveaux de diagnostic suivants sont accessibles :

     - **Minimal**. Kaspersky Anti-Virus enregistre dans le journal uniquement les événements principaux, par exemple, les événements liés à la détection ou au blocage des objets qui contiennent ou peuvent contenir une menace. Les erreurs d'analyse, de réparation ou de balayage de ces objets se rapportent également à ce niveau de diagnostic.

     - **Mise au point**. Kaspersky Anti-Virus enregistre dans le journal tous les événements se rapportant au niveau minimal de diagnostic ainsi que les informations actualisées sur le fonctionnement de l'application. Si à ce niveau de diagnostic Kaspersky Anti-Virus enregistre dans le journal un grand nombre de messages, cela peut entraîner une baisse de la productivité et remplir rapidement l'espace de disque. Il est recommandé d'activer ce mode uniquement pour détecter les erreurs dans le fonctionnement de l'application.

     La valeur **Minimal** est établie par défaut.

   - **Journaux de fonctionnement de l'application**.

     Niveau de détails des informations enregistrées dans le Journal de fonctionnement de l'application et dans le Journal de fonctionnement des filtres.

     Les niveaux de diagnostic suivants sont accessibles :

     - **Minimal**. Kaspersky Anti-Virus enregistre dans le journal uniquement les événements principaux, par exemple, les événements pour lesquels l'analyse des objets reçus n'a pas lieu. Les erreurs de filtrage lors de l'obtention des objets depuis le serveur, les erreurs de transfert ou d'analyse des objets reçus se rapportent également à ce niveau de diagnostic.

     - **Mise au point**. Kaspersky Anti-Virus enregistre dans le journal tous les événements se rapportant au niveau minimal de diagnostic ainsi que les informations actualisées sur le fonctionnement de l'application. Par exemple, les événements liés à la purge de la Sauvegarde, aux erreurs de fonctionnement du Gestionnaire de l'analyse des objets ou du moteur antivirus se rapportent à ce niveau de diagnostic. Si à ce niveau de diagnostic Kaspersky Anti-Virus enregistre dans le journal un grand nombre de messages, cela peut entraîner une baisse de la productivité et remplir rapidement l'espace de disque. Il est recommandé d'activer ce mode uniquement pour détecter les erreurs dans le fonctionnement de l'application.

     La valeur **Minimal** est établie par défaut.

4. Définissez la fréquence de création des journaux et des paramètres de leur conservation :

   - **Créer un nouveau fichier du journal une fois tous les**.

     Fréquence de création des journaux de Kaspersky Anti-Virus. Cette valeur est applicable à tous les journaux de Kaspersky Anti-Virus : Journal de fonctionnement de l'application, Journal de fonctionnement des filtres et Journal de l'analyse du trafic.

     Les valeurs suivantes de fréquence sont accessibles :

     - **1 jour**. Kaspersky Anti-Virus crée le journal chaque jour à 00h00 à l'heure du serveur sur lequel le composant Serveur de sécurité est installé et y enregistre tous les événements fixés au cours des dernières vingt-quatre heures.
     - **7 jours**. Kaspersky Anti-Virus crée le journal une fois tous les 7 jours et y enregistre tous les événements de la semaine à compter de la date de création du journal.
     - **30 jours**. Kaspersky Anti-Virus crée le journal une fois tous les 30 jours et y enregistre tous les événements de la semaine à compter de la date de création du journal.

     Par défaut, Kaspersky Anti-Virus crée les journaux une fois tous les 30 jours.

     Lors de la création d'un nouveau fichier journal, Kaspersky Anti-Virus transforme le fichier actuel du journal en journal d'archive.

   - **Conserver pas plus du nombre indiqué de fichiers de chaque journal**.

     Le nombre maximal de fichiers des journaux de chaque type conservés par Kaspersky Anti-Virus. Cette valeur est applicable à chaque type des journaux de Kaspersky Anti-Virus : Journal de fonctionnement de l'application, Journal de fonctionnement des filtres et Journal de l'analyse du trafic. Lorsque cette valeur est obtenue, Kaspersky Anti-Virus supprime le fichier journal qui a été créé avant tous les autres fichiers.

     La plage des valeurs possibles et de 1 à 365.

     Par défaut, Kaspersky Anti-Virus conserve cinq journaux (quatre journaux d'archives et un journal utilisé pour enregistrer les événements au moment actuel).

     Les journaux d'archives ne sont pas actualisés.

5. Cliquez sur le bouton **OK**. La fenêtre de configuration des paramètres de l'application se ferme.

6. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale. La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

RAPPORTS

Cette section contient des informations sur les rapports de Kaspersky Anti-Virus et sur les tâches de génération de rapports ainsi que des instructions sur l'utilisation de ces derniers.

DANS CETTE SECTION

A PROPOS DES RAPPORTS DE KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus permet de recevoir les rapports de la protection antivirus pour la période que vous avez indiquée. Le rapport de chaque filtre activé de Kaspersky Anti-Virus affiche les informations relatives aux résultats de traitement des objets analysés.

Les rapports sont générés en fonction des informations conservées dans la Base de données de la sauvegarde et des statistiques.

Le rapport indique le nombre total d'objets analysés ainsi que, pour chaque filtre de Kaspersky Anti-Virus, les informations suivantes :

- le nombre d'objets considérés sains suite à l'analyse ;
- le nombre d'objets réparés ;
- le nombre d'objets pouvant contenir une menace ;
- le nombre d'objets considérés infectés suite à l'analyse ;
- le nombre d'objets protégés par mot de passe ;
- le nombre d'objets ignorés conformément aux stratégies de Kaspersky Anti-Virus ;
- le nombre d'objets ignorés en raison de l'absence d'une licence active ;
- le nombre d'objets ignorés pour des erreurs d'analyse ;
- le nombre d'objets ignorés à cause du dépassement du délai maximal d'analyse.

Le rapport est un fichier au format HTML. Le modèle qui sert à générer les rapports ne peut être modifié.

Kaspersky Anti-Virus permet de générer un rapport programmé ou à la demande sur l'état de la protection antivirus (rapport "rapide").

Les paramètres du rapport programmé sont définis par la *tâche de génération de rapport*. Kaspersky Anti-Virus lance de temps en temps la tâche de génération de rapport sur le serveur où est installé le module Serveur de sécurité. En cas d'utilisation des schémas de déploiement *Groupe autonome* et *Entreprise*, les rapports sur l'état de la protection antivirus sur tous les serveurs faisant partie du groupe sont créés sur l'un des serveurs du groupe. Vous pouvez sélectionner le serveur sur lequel seront générés les rapports (cf. section "Sélection du serveur de génération des rapports" à la page 91).

L'application prévoir une tâche préinstallée de génération du rapport sur l'état de la protection antivirus. La tâche préinstallée permet de générer un rapport tous les lundis à 00:01 à l'heure du serveur utilisé pour créer les rapports. Le rapport intègre les données des 7 derniers jours. La tâche préinstallée est désactivée par défaut. Vous pouvez activer, modifier ou supprimer la tâche préinstallée.

La liste des tâches de génération de rapport et la liste des rapports prêts s'affichent dans l'entrée **Rapports** de la Console d'administration de Kaspersky Anti-Virus (cf. section "Consultation de la liste des rapports et des tâches de génération de rapports" à la page 90). Vous pouvez ouvrir le rapport généré pour l'afficher dans le navigateur (cf. section "Consultation du rapport" à la page 95).

Le rapport généré par programmation peut être généré manuellement sans attendre le lancement suivant de la tâche de génération de rapport (cf. section "Lancement manuel de la tâche de génération de rapport" à la page 94).

Si vous avez besoin d'un rapport uniquement de protection antivirus pour une période donnée, vous pouvez générer un rapport "rapide" (cf. section "Génération d'un rapport "rapide"" à la page 94). Le rapport généré manuellement et le rapport "rapide" après la génération s'affichent dans la liste des rapports prêts et s'ouvrent dans une nouvelle fenêtre du navigateur installé par défaut (ou dans un nouvel onglet si le navigateur était ouvert).

Les rapports générés sont enregistrés dans la Base de données de la sauvegarde et des statistiques.

CONSULTATION DE LA LISTE DES RAPPORTS ET DES TACHES DE GENERATION DE RAPPORTS

Pour consulter la liste des tâches de génération de rapports et la liste des rapports générés, procédez comme suit :

1. Ouvrez la Console d'administration et connectez-vous au stockage de configuration de Microsoft ISA Server/Forefront TMG (cf. section "Connexion de la Console d'administration au stockage de configuration" à la page 42).

2. Déployez l'entrée du serveur (schéma de déploiement *Serveur autonome*) ou l'entrée du groupe (schémas de déploiement *Groupe autonome* et *Entreprise*) et sélectionnez l'entrée jointe **Rapports** (cf. section "**Fenêtre principale**" à la page 19).

   Le tableau **Tâches de génération de rapports** se trouve dans la partie supérieure du panneau des résultats.

   Le tableau **Rapports générés** se trouve dans la partie inférieure du panneau des résultats. Le tableau affiche les rapports "rapides" et les rapports générés à l'aide de la tâche sélectionnée dans la liste des tâches.

Le tableau **Tâches de génération de rapports** contient les colonnes suivantes :

- **Nom de la tâche**.

  Le nom de la tâche de génération de rapport.

- **Etat de la tâche**.

  L'état de la tâche de génération de rapport. Contient une des valeurs suivantes :

  - **Activée**. La tâche est activée, Kaspersky Anti-Virus forme les rapports selon l'horaire indiqué dans la tâche.

  - **Désactivée**. La tâche est désactivée, Kaspersky Anti-Virus ne crée pas de rapports selon cette tâche.

- **Heure du dernier lancement**.

  La date et l'heure du dernier lancement de la tâche de génération de rapport.

  Valeurs du champ possibles :

  - **N'a jamais été lancée**. Kaspersky Anti-Virus n'a pas formé les rapports pour cette tâche.
  - **Date et heure de lancement**. L'heure du dernier lancement de la tâche.
  - **Date et heure, erreur**. Le serveur SQL n'a pas été accessible à l'heure planifiée pendant la génération du rapport. Le champ indique la date et l'heure du dernier lancement ignoré de la tâche.
  - **Le serveur n'est pas accessible**. Il est impossible de se connecter au serveur que Kaspersky Anti-Virus utilise pour créer les rapports.

- **Planification**.

  La fréquence de lancement de la tâche selon la génération du rapport.

Le tableau **Rapports générés** affiche, pour chaque rapport, les paramètres suivants :

- **Nom du rapport**.

  Le nom du rapport.

  Si le rapport a été généré à l'aide de la tâche, son nom coïncide avec le nom de la tâche. Si le rapport a été créé à la demande, le champ affiche le nom "rapport rapide".

- **Date de création**.

  La date et l'heure de création du rapport.

- **Période**.

  La période pour laquelle le rapport contient les informations sur l'état de la protection antivirus.

Par défaut, la liste des rapports est triée dans l'ordre inverse selon le temps de création du rapport.

SELECTION DU SERVEUR DE GENERATION DES RAPPORTS

En cas d'utilisation des schémas de déploiement *Groupe autonome* et *Entreprise*, les rapports sur l'état de la protection antivirus sur tous les serveurs faisant partie du groupe sont créés sur l'un des serveurs du groupe.

Les rapports sont générés par défaut sur le premier serveur du groupe sur lequel Kaspersky Anti-Virus est installé. Si vous supprimez l'application sur ce serveur, le serveur par défaut utilisé sera un serveur aléatoire faisant partie du groupe sur lequel Kaspersky Anti-Virus est installé.

Pour sélectionner le serveur utilisé pour générer les rapports, procédez comme suit :

1. Ouvrez la liste des tâches de génération de rapports (cf. section "Consultation de la liste des rapports et des tâches de génération de rapports" à la page 90).
2. Cliquez sur le bouton **Serveur sur lequel seront générés les rapports** situé sous la liste des tâches de génération de rapport et sélectionnez le nom du serveur dans la liste des serveurs faisant partie du groupe.
3. Pour que les modifications entrent en vigueur, cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

   Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

Kaspersky Anti-Virus créera des rapports sur le serveur sélectionné.

OPERATIONS SUR LES TACHES DE GENERATION PROGRAMMEE DES RAPPORTS

Vous pouvez exécuter les actions suivantes avec les tâches de génération de rapport :

- créer des tâches (cf. section "Création d'une tâche de génération de rapport" à la page 92) ;
- consulter et modifier les tâches (cf. section "Consultation et modification des tâches de génération de rapport" à la page 93);
- supprimer les tâches (cf. section "Suppression de la tâche de génération de rapport" à la page 93) ;
- lancer l'exécution des tâches manuellement (cf. section "Lancement manuel des tâches de génération de rapports" à la page 94).

DANS CETTE SECTION

CREATION D'UNE TACHE DE GENERATION DE RAPPORT

Pour créer une tâche de génération de rapport, procédez comme suit :

1. Ouvrez la liste des tâches de génération de rapports (cf. section "Consultation de la liste des rapports et des tâches de génération de rapports" à la page 90).
2. Cliquez sur le bouton **Ajouter** situé dans la barre d'outils au-dessus de la liste des tâches. La fenêtre **Tâche de génération de rapport** s'ouvre.
3. Indiquez les paramètres suivants :

   - **Nom de la tâche**.

     Nom de la tâche de génération de rapport qui s'affiche dans la liste des tâches de génération programmée des rapports. Kaspersky Anti-Virus attribue ce nom à tous les rapports créés au lancement de la tâche.

     Le nom de la tâche doit être unique.

   - **Fréquence**.

     Définit le mode de lancement de la tâche de génération de rapport sur l'état de la protection antivirus.

     Valeurs possibles :

     - **Tous les N jours** : Kaspersky Anti-Virus forme le rapport selon l'intervalle correspond au nombre de jours indiqué dans le champ de saisie. Cette option est sélectionnée par défaut avec la valeur 1 jour.
     - **Une fois par semaine**. Kaspersky Anti-Virus génère le rapport une fois par semaine le jour indiqué dans le champ **Jour de la semaine**.

       Pour cette valeur, le paramètre suivant est disponible :

       - **Jour de la semaine** : jour de la semaine où Kaspersky Anti-Virus lance la tâche de génération du rapport. Le jour sélectionné par défaut est le lundi.
     - **Chaque mois, le jour indiqué**. Kaspersky Anti-Virus génère le rapport une fois par mois le jour indiqué dans le champ de saisie. Le jour sélectionné par défaut est le premier du mois.

     Quelles que soient les valeurs des paramètres de fréquence, la tâche de génération de rapport est lancée à 00:01 selon l'heure du serveur physique utilisé pour la génération des rapports.

4. Si vous souhaitez désactiver la génération programmée de rapports à l'aide de la tâche créée, décochez la case **Activer la tâche**. La case est cochée par défaut.

5. Cliquez sur le bouton **OK**. La fenêtre **Tâche de génération de rapport** se ferme.

6. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

La tâche de génération créée sera utilisée par l'application uniquement après l'application des modifications de configuration.

CONSULTATION ET MODIFICATION DES TACHES DE GENERATION DE RAPPORT

Pour modifier la tâche de génération de rapport, procédez comme suit :

1. Ouvrez la liste des tâches de génération de rapports (cf. section "Consultation de la liste des rapports et des tâches de génération de rapports" à la page 90).

2. Sélectionnez dans la liste les paramètres que vous souhaitez modifier, et ouvrez la fenêtre **Tâche de génération de rapport** selon l'une des méthodes suivantes :

   - à l'aide du bouton **Modifier** situé dans la barre d'outils au-dessus de la liste des tâches ;
   - en cliquant sur la touche **ENTER** ;
   - en double-cliquant sur la tâche sélectionnée ;
   - à l'aide de l'option du menu contextuel.

3. Dans la fenêtre **Tâche de génération de rapport**, modifiez les paramètres de la tâche (cf. section "Création d'une tâche de génération de rapport" à la page 92).

4. Cliquez sur le bouton **OK**. La fenêtre **Tâche de génération de rapport** se ferme.

5. Cliquez sur le bouton **Appliquer** dans la partie supérieure du panneau des résultats de la fenêtre principale (cf. section "Fenêtre principale" à la page 19). La configuration de Kaspersky Anti-Virus conservera toutes les modifications apportées depuis la dernière application des paramètres.

Les nouvelles valeurs des paramètres de Kaspersky Anti-Virus seront utilisées par l'application uniquement une fois les modifications de la configuration appliquées.

Kaspersky Anti-Virus génèrera la tâche de génération de rapport avec de nouveaux paramètres.

SUPPRESSION DE LA TACHE DE GENERATION DE RAPPORT

Vous pouvez supprimer la tâche de génération de rapport sélectionnée dans la liste.

Kaspersky Anti-Virus ne supprime pas les rapports formés auparavant selon cette tâche. Si au moment de la suppression de la tâche Kaspersky Anti-Virus exécute la création du rapport selon cette tâche, l'application termine la génération du rapport, puis supprime la tâche.

Les modifications dans la liste des tâches de génération de rapport entreront en vigueur uniquement après l'application des modifications de la configuration.

LANCEMENT MANUEL DE LA TACHE DE GENERATION DE RAPPORT

Pour lancer manuellement une tâche de génération de rapport, procédez comme suit :

1. Ouvrez la liste des tâches de génération de rapports (cf. section "Consultation de la liste des rapports et des tâches de génération de rapports" à la page 90).

2. Dans la liste, sélectionnez la tâche pour laquelle vous souhaitez générer un rapport.

   Vous pouvez sélectionner aussi bien une tâche avec le statut "activé" qu'avec le statut "désactivé".

3. Cliquez sur le bouton **Lancer** situé dans le panneau d'administration au-dessus de la liste des tâches.

Kaspersky Anti-Virus génère un rapport pour la période indiquée dans les paramètres de la tâche (cf. section "Création d'une tâche de génération de rapport" à la page 92). L'application ajoute le rapport au tableau **Rapports générés** et ouvre le rapport dans une nouvelle fenêtre du navigateur sélectionné par défaut (ou dans un nouvel onglet si le navigateur est déjà ouvert).

Le lancement manuel de la tâche de génération de rapport influence la prochaine génération programmée de ce rapport indiqué dans la tâche.

Si le service *Kaspersky Anti-Virus 8.5 for ISA Server and Forefront TMG* est désactivé (kavisasrv.exe) ou si le serveur SQL sur lequel est installé la Base de données de la sauvegarde et des statistiques est inaccessible, le rapport ne sera pas généré. Kaspersky Anti-Virus affiche à l'écran un message indiquant que le serveur/la base de données est inaccessible.

GENERATION D'UN RAPPORT "RAPIDE"

Pour générer un rapport "rapide", procédez comme suit :

1. Ouvrez la liste des rapports (cf. section "Consultation de la liste des rapports et des tâches de génération de rapports" à la page 90).

2. Cliquez sur le bouton **Créer le rapport rapide** situé au-dessus de la liste des rapports. La fenêtre **Création d'un rapport rapide** s'ouvre.

3. Indiquez la période pour laquelle Kaspersky Anti-Virus génère le rapport :

   - **de** : date de début de la période ;

   - **à** : date de fin de la période.

     Par défaut, les champs indiquent la date actuelle. Les dates sont indiquées en fonction de l'heure du serveur physique utilisé pour la création des rapports. Les calendriers présents dans les champs de sélection des dates peuvent également être utilisés pour indiquer la période du rapport généré.

4. Cliquez sur le bouton **Créer**.

La fenêtre **Création d'un rapport rapide** se ferme. Kaspersky Anti-Virus génère un rapport sur l'état de la protection antivirus qui contient les données pour la période allant de 00:00 pour la date de début à 23:59 pour la date de fin.

Kaspersky Anti-Virus ajoute le rapport au tableau **Rapports générés** et ouvre le rapport dans une nouvelle fenêtre du navigateur par défaut (ou dans un nouvel onglet si le navigateur est ouvert).

OPERATIONS SUR LES RAPPORTS PRETS DE KASPERSKY ANTI-VIRUS

Vous pouvez exécuter les actions suivantes avec les rapports prêts :

- consulter les rapports (cf. section "Consultation du rapport" à la page 95);
- enregistrer les rapports sur le disque (cf. section "Enregistrement du rapport" à la page 95);
- supprimer les rapports (cf. section "Suppression du rapport" à la page 96).

DANS CETTE SECTION

CONSULTATION DU RAPPORT

Pour consulter le rapport généré, procédez comme suit :

1. Ouvrez la liste des rapports générés (cf. section "Consultation de la liste des rapports et des tâches de génération de rapports" à la page 90).
2. Sélectionnez le rapport dans le tableau **Rapports générés** et ouvrez le fichier HTML du rapport de l'une des manières suivantes :
   - en cliquant sur le bouton **Consulter** situé sur le panneau d'administration au-dessus de la liste des rapports ;
   - en cliquant sur la touche **ENTER** ;
   - à l'aide de l'option du menu contextuel ;
   - en double cliquant sur la ligne du rapport sélectionné.

   Le rapport sélectionné s'ouvre dans une nouvelle fenêtre du navigateur sélectionné par défaut (ou dans un nouvel onglet si le navigateur est ouvert).

ENREGISTREMENT DU RAPPORT

Vous pouvez enregistrer le rapport sélectionné dans la liste ou plusieurs rapports au format HTML sur le disque local.

Le nom du fichier enregistré dépend du mode de génération du rapport et du schéma de déploiement de Kaspersky Anti-Virus utilisé :

- Le rapport généré à l'aide de la tâche est enregistré par Kaspersky Anti-Virus dans un fichier portant le nom suivant :
  - dans le cas du schéma de déploiement *Serveur autonome* – "<nom de la tâche de génération de rapport_date et heure de création du rapport>.html" ;

- dans le cas des schémas de déploiement *Groupe autonome* et *Entreprise* – "<nom de la tâche de génération de rapport_date et heure de création du rapport_nom du groupe>.html".

- Le rapport "rapide" est enregistré par Kaspersky Anti-Virus dans un fichier portant le nom suivant :

  - dans le cas du schéma de déploiement *Serveur autonome* – "rapport rapide_<date et heure de création du rapport>.html" ;

  - dans le cas des schémas de déploiement *Groupe autonome* et *Entreprise* – "rapport rapide_<date et heure de création du rapport_nom du groupe>.html".

Si le nom du rapport contient un des caractères suivants : \ / : * ? " < > |, Kaspersky Anti-Virus remplace chacun de ces caractères par le caractère _ (tiret bas) lors de l'enregistrement du rapport.

En cas d'erreur lors de l'enregistrement du fichier de rapport sur le disque, Kaspersky Anti-Virus affiche à l'écran un message d'erreur indiquant que l'enregistrement du fichier est interrompu.

SUPPRESSION DU RAPPORT

Vous pouvez supprimer un rapport sélectionné dans la liste ou plusieurs rapports.

La suppression du rapport n'influence pas la tâche ayant généré ce rapport.

CONTACTER LE SUPPORT TECHNIQUE

Cette section contient des informations sur les moyens d'obtenir de l'assistance technique et sur les conditions requises pour obtenir l'aide du Support technique.

DANS CETTE SECTION

MODES D'OBTENTION DE L'ASSISTANCE TECHNIQUE

Si vous n'avez pas trouvé la solution à votre problème dans la documentation de l'application ou dans l'une des sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page 10), nous vous recommandons de contacter le Support Technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

Avant de contacter le Support Technique, il est recommandé de prendre connaissance des Conditions d'accès au Support Technique (http://support.kaspersky.com/support/rules).

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- Par téléphone. Cette méthode permet de contacter les experts du Support Technique en français.
- En envoyant une demande depuis Mon Espace Personnel sur le site Web du Support Technique. Cette méthode permet de contacter les experts du Support Technique via un formulaire.

L'assistance technique est fournie uniquement aux utilisateurs qui ont acheté une licence commerciale d'utilisation de l'application. Les utilisateurs ayant obtenu une licence d'essai n'ont pas droit à l'assistance technique.

SUPPORT TECHNIQUE PAR TELEPHONE

En cas de problème urgent, vous pouvez téléphoner aux experts du Support Technique francophone (http://www.kaspersky.com/fr/support-contact).

Avant de vous adresser au Support Technique, veuillez prendre connaissance des règles applicables (http://support.kaspersky.com/support/details). Nos experts pourront ainsi vous venir en aide plus rapidement.

OBTENTION DE L'ASSISTANCE TECHNIQUE VIA MON ESPACE PERSONNEL

Mon Espace personnel est la section qui vous est réservée (https://support.kaspersky.com/fr/PersonalCabinet) sur le site du Support Technique.

Pour pouvoir accéder à Mon Espace Personnel, vous devez vous inscrire sur la page d'enregistrement (https://my.kaspersky.com/fr/registration) et obtenir ainsi un numéro de client et un mot de passe pour accéder à votre Espace Personnel. Pour ce faire, vous aurez besoin du fichier clé (cf. section "A propos du fichier clé" à la page 28).

Mon Espace Personnel permet de réaliser les opérations suivantes :

- Envoyer des demandes au Support Technique et au Laboratoire d'étude des virus ;
- Communiquer avec le Support Technique sans devoir envoyer des messages électroniques ;
- Suivre le statut de vos demandes en temps réel ;
- Consulter l'historique complet de votre interaction avec le Support Technique ;
- Obtenir une copie du fichier de licence en cas de perte ou de suppression de celui-ci.

Formulaire de demande au Support Technique

Vous pouvez envoyer une demande par voie électronique au Support Technique en anglais et en français.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- Type de demande ;
- Nom et numéro de version de l'application ;
- Contenu de la demande ;
- Numéro de client et mot de passe ;
- Adresse électronique.

L'expert du Support Technique répond via Mon Espace Personnel et en envoyant un message électronique à l'adresse indiquée dans la demande.

Demande électronique adressée au Laboratoire d'étude des virus

Certaines demandes ne sont pas envoyées au Support Technique mais au Laboratoire d'étude des virus.

Vous pouvez envoyer au Laboratoire d'étude des virus les types de demandes suivantes :

- *Programme malveillant inconnu* : vous soupçonnez le fichier de contenir un virus mais Kaspersky Anti-Virus ne détecte aucune infection.

  Les experts du Laboratoire d'étude des virus analysent le code malveillant envoyé et en cas de détection d'un virus inconnu jusque-là, ils ajoutent sa définition à la base des données accessible lors de la mise à jour des logiciels antivirus.

- *Faux positif de l'application* Kaspersky Anti-Virus considère un fichier comme un virus mais vous êtes convaincu que ce n'est pas le cas.

- *Demande de description d'un programme malveillant* : vous souhaitez obtenir la description d'un virus détecté par Kaspersky Anti-Virus sur la base du nom de ce virus.

Vous pouvez également envoyer une demande au Laboratoire d'étude des virus depuis le formulaire de demande (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr), sans vous enregistrer dans Mon Espace Personnel.

GLOSSAIRE

A

Activation de l'application

L'application devient entièrement fonctionnelle. L'utilisateur peut activer l'application pendant ou après son installation. Pour activer l'application, l'utilisateur doit avoir le code d'activation ou le fichier de licence.

Analyse du trafic

Analyse des objets transmis via les protocoles (par exemple, HTTP, FTP, SMTP, POP3), en temps réel à l'aide des informations de la version actuelle (dernière version) des bases de Kaspersky Anti-Virus.

Analyseur heuristique

Technologie d'identification des menaces dont les informations ne sont pas reprises dans les bases de Kaspersky Lab. L'analyseur heuristique permet d'identifier les objets dont le comportement dans le système est semblable à celui des menaces. Les objets identifiés à l'aide de l'analyseur heuristique sont considérés comme potentiellement infectés. Par exemple, un objet contenant les séquences de commandes propres aux objets malveillants (ouverture d'un fichier, l'écriture dans un fichier) peut être considéré comme potentiellement infecté.

B

Base de donnees de la sauvegarde et des statistiques

La Base de données sur le serveur SQL conçue pour conserver les informations statistiques sur l'utilisation de l'application et les informations sur les objets dangereux dont les copies sont placées dans la sauvegarde par Kaspersky Anti-Virus.

Bases de Kaspersky Anti-Virus

Bases de données qui contiennent la description des menaces pour la sécurité de l'ordinateur et connues par Kaspersky Lab au moment de l'édition des bases. Les enregistrements dans les bases permettent de détecter le code malveillant dans les objets analysés. Les bases sont formées par les experts de Kaspersky Lab et sont mises à jour toutes les heures.

Blocage d'un objet

Interdiction d'accès à un objet de la part d'applications tiers. L'objet bloqué ne peut être lu, exécuté, modifié ni supprimé.

C

Cle active

Clé utilisée actuellement pour faire fonctionner l'application.

Cle supplementaire

Clé attestant du droit d'utilisation de l'application mais non utilisée pour le moment.

Copie de sauvegarde

Création d'une copie de sauvegarde d'un fichier avant qu'il ne soit réparé ou supprimé et placé dans la Sauvegarde avec la possibilité de le restaurer ultérieurement, par exemple en vue de l'analyser à l'aide des bases mises à jour.

D

Duree de validite de la licence

La durée de validité de la licence est la période pendant laquelle vous pouvez utiliser les fonctions de l'application et les services supplémentaires. Le volume des fonctions accessibles et des services complémentaires dépend du type de licence.

F

FICHIER CLE

Fichier du type xxxxxxx.key. Le fichier clé est fourni à l'achat de l'application. Le fichier clé est indispensable à l'utilisation de l'application.

L

LICENCE

La licence est un droit d'utilisation de l'application, limité dans le temps, qui est octroyé dans le cadre du Contrat de licence.

LISTE NOIRE DES CLES

Base de données contenant des informations sur les clés bloquées par Kaspersky Lab. Le contenu du fichier et la liste noire sont mis à jour avec les bases.

M

MISE A JOUR

Fonctionnalité de Kaspersky Lab qui permet de maintenir à jour la protection de l'ordinateur. Pendant la mise à jour, l'application copie les mises à jour des bases depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur, les installe et les met en application.

O

OBJET

Corps du message ou simple pièce jointe, par exemple sous forme de fichier exécutable. Cf. également objet-conteneur.

OBJET-CONTENEUR

Objet composé de plusieurs objets, d'archives, message contenant une pièce jointe. Cf. également Objet.

OBJET INFECTE

Objet dont un extrait de code est identique à un extrait de code d'une menace connue. Les experts de Kaspersky Lab déconseillent d'utiliser ces objets.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient un code modifié d'une menace connue ou un code dont le comportement ressemble à celui d'une menace.

R

REPARATION D'OBJETS

Méthode utilisée pour le traitement des objets infectés qui permet de restaurer les données totalement ou partiellement. Certains objets infectés ne peuvent pas être réparés.

S

SAUVEGARDE

Dossier spécial prévu pour conserver les copies de sauvegarde des objets créés avant leur réparation ou leur suppression.

SERVEURS DE MISE A JOUR DE KASPERSKY LAB

Serveurs HTTP et FTP de Kaspersky Lab à partir desquels l'application de Kaspersky Lab obtient la mise à jour des bases et des modules de l'application.

STRATEGIE

Une ou plusieurs règles qui définissent les paramètres de la protection antivirus appliquées uniquement pour les connexions et les protocoles sélectionnés.

L'application prévoit trois types de stratégie : Stratégie de traitement des protocoles, Stratégie d'exclusion de l'analyse et Stratégie d'analyse antivirus.

STRATEGIE D'ANALYSE ANTIVIRUS

Définit les paramètres de détection des menaces et des actions à exécuter sur les objets détectés.

STRATEGIE D'EXCLUSION DE L'ANALYSE

Définit les paramètres d'exclusion des objets de l'analyse antivirus.

STRATEGIE DE TRAITEMENT DES PROTOCOLES

Définit les paramètres de traitement du trafic au niveau des protocoles FTP et HTTP.

SUPPRESSION DE L'OBJET

Méthode de traitement de l'objet qui supprime physiquement l'objet de l'endroit où il a été détecté par l'application (disque dur, dossier, ressource réseau). Il est recommandé d'appliquer cette méthode de traitement aux objets dangereux qui ne peuvent pas être réparés pour telle ou telle raison.

KASPERSKY LAB ZAO

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement "IDC Worldwide Endpoint Security Revenue by Vendor"). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

Produits. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases antivirus de Kaspersky Lab sont actualisées toutes les heures*, tandis que *les bases antispam* sont actualisées *toutes les 5 minutes*.

Technologies. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

Réalisations. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site officiel de Kaspersky Lab :	http://www.kaspersky.fr
Encyclopédie de virus :	http://www.securelist.com/fr/
Laboratoire Anti-Virus :	newvirus@kaspersky.com(uniquement pour l'envoi d'objets suspects sous forme d'archive)
	http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr
	(pour les demandes auprès des experts en virus)
Forum de Kaspersky Lab :	http://forum.kaspersky.fr

INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal_notices.txt situé dans le dossier d'installation de l'application.

NOTIFICATIONS SUR LES MARQUES DE COMMERCE

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Forefront, Microsoft, SQL Server, Windows, Windows Server et Windows Vista sont des marques de Microsoft Corporation déposées aux Etats-Unis et dans d'autres pays.

INDEX

O

P

R

S

T