République Algérienne Démocratique et Populaire

Université Kasdi Merbah Ouargla
Faculté Des Nouvelles Technologie de l'Information et de la Communication
Département de l'Informatique et des Technologies de l'Information

Mémoire de fin d'études
pour l'obtention du diplôme de Master Professionnel
Spécialité : Réseaux, Convergence et Sécurité (RCS)
Thème

Déploiement d'une solution Anti-virus au sein du réseau de campus universitaire de Ouargla

Préparé par :

- ***BAHAZ Salma***
- ***MAMMERI Tidjani***

Présenté le 07 Juin 2015 devant le jury composé de :

- *Mr MAHDJOUB Mohamed Bachir (Président).*
- *Melle DAHRAOUI Nadia (Examinateur).*
- *Mr KAFI Mouhamed Redouane (Encadreur).*
- *Mr EUSCHI Salah (Co-Encadreur).*

Année Universitaire : 2014/2015

Remerciement

Avec un grand plaisir je remercie ***Allah*** *qui m'a aidé et m'a donné la patience, le courage et la force d'achever ce travail*

Nous avons tiens à remercier en cette occasion tout le corps professoral et administratif de département d'informatique de l'université ***Kasdi Merbah*** *de Ouargla pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.*

Nous avons à remercier sincèrement ***Mr kafi Mouhamed Radouane*** *et* ***Mr Euschi Salah,*** *qui, en tant que encadreur de mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'orientation, la confiance, l'aide et le temps qu'il a bien voulu me consacrer et sans eux ce mémoire n'aurait jamais vu le jour.*

Nous avons remercier sincèrement ***Mr BEN NADIR Sid Ali*** *qui m'a orienté et aidé.*

Nous avons remercié ***AZZAOUI Nadjet*** *qui m'a orienté* ***et*** *aidé.*

Je tiens à remercier sincèrement mes parents et mon ami ***HLITIM Sadek,*** *qui m'ont donné le courage.*

Nous avons souhaité d'adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

J'exprime également ma gratitude aux membres du jury, qui m'ont honoré en acceptant de juger ce modeste travail.

Dédicace

A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce modeste travail que je dédie:

A la mémoire de ma grande mère paternel;

A mon très cher ***père*** *et ma très chère* ***mère*** *qui n'ont pas cessé de m'encourager et de se sacrifier pour que je puisse franchir tout obstacle durant toutes mes années d'étude que Dieu me les garde en très bonne santé ; Aucune dédicace ne pourra compenser les sacrifices de mes parents;*

A mon sœur ***Souhila****, et ma petite chère sœur* ***Serine***

A mon frère ***Abd Elwahab****, et mon frère* ***Lehcen****, et mon petit frère* ***Faruok.***

A mes oncles, mes tantes, mes cousines, mes cousins spécialement, et à toute ma famille

A mes enseignants et surtout ***Mr kafi Muhamed Radouane*** *et* ***Mr Eusche SAlah,*** *mon encadreur;*

Et à tous ceux qui m'aiment et qui me cannaient de proche ou de loin.

BAHAZ Salma

Table de matière :

Chapitre III : Conception et implémentation

Liste de figures :

Liste de tableaux :

Introduction générale:

Dans la « société de l'information », la sécurité des systèmes informatiques constitue un enjeu crucial. Le contrôle de l'information traitée et partagée au sein de ces systèmes est un problème d'autant plus délicat que le nombre d'utilisateurs de ces systèmes est important. Relier ces systèmes entre eux au sein de réseaux informatiques, eux-mêmes interconnectés, complexifie donc la tâche des responsables de sécurité.

La sécurité d'un système informatique repose en premier lieu sur la mise en place d'une politique de sécurité. Celle-ci peut être définie comme un ensemble de règles permettant d'assurer trois propriétés :

- *la confidentialité des données* : seuls les utilisateurs autorisés peuvent consulter une information donnée.
- *l'intégrité des données* : seuls les utilisateurs autorisés peuvent modifier une information donnée.
- *la disponibilité du système* : le système doit être capable de rendre le service prévu en un temps borné.

Le réseau de l'université gère un parc informatique d'une centaine de machines ou plus, pour installer les applications antivirus sur ces machines obligé de se déplacer à chaque ordinateur.

Aujourd'hui, cette méthode a changé, l'installation d'une application antivirus est devenue plus facile et plus rapide en diffusant l'application sur ces machines et l'installation sera guidé à distance par le serveur d'administration.

Au long de ce rapport, nous allons résumer notre stage en 3 chapitres composé :

Le premier chapitre est un chapitre descriptif pour la sécurité des réseaux, sur lequel on va définir les menaces, les logiciels malveillants et une politique de sécurité ainsi que les principaux mécanismes de sécurité.

Le second chapitre est consacré la présentation du logiciel antivirus et son fonctionnement. Ainsi que la classification des antivirus et enfin nous avons choisi le meilleur antivirus pour notre application.

Le dernier chapitre présentera le travail effectué pendant le stage, il est consacré à la réalisation de notre application, qui consiste à implémenter un système de déploiement antivirus et sa mise à jour.

Partie I

Chapitre I :
Sécurité des systèmes informatiques

I. Introduction :

Notre université est de plus en plus dépendante de l'informatique. Quelles que soient nos activités, nous sommes confrontés directement ou indirectement à des ordinateurs : procédures administratives, virement d'argent, réservations, télécommunications ?

Avec l'expansion de l'université son système informatique est devenu plus complexe, il est aussi ouvert sur l'internet donc, il peut être exposé aux différentes menaces et attaques provoqués par des logiciels malveillants en nombre de plus important.

Il est alors nécessaire de mettre au point des méthodes et des techniques pouvant réduire considérablement ces risques, en résolvant une vulnérabilité ou en contrant une attaque spécifique. La sécurité informatique se base sur ces solutions qui permettent de mettre en place une réponse appropriée à chaque menace.

Le choix de la protection adéquate est alors possible, nécessitant de bien connaître son environnement, les objectifs de l'université et les technologies disponibles. Mettre en place une politique de sécurité efficace représente alors un long travail d'étude et de choix devant apporter la plus grande protection possible au système d'information.

II. Sécurité des systèmes informatiques:

II.1. Définition

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs des dites machines possèdent uniquement les droits qui leur ont été octroyés.

Il peut s'agir :

- d'empêcher des personnes non autorisées d'agir sur le système de façon malveillante.
- d'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système.
- de sécuriser les données pour éviter la perturbation ou des pannes.
- de garantir la non-interruption d'un service.

II.2. Évaluation de la sécurité d'un réseau:

1. ***La disponibilité*** : Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
2. ***L'intégrité :*** Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
3. ***La confidentialité :*** Seule les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché. [7]

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes l'information, tels que :

4. ***La traçabilité*** (ou **« Preuve »**) : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
5. ***L'authentification :*** L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

6. ***La non-répudiation :*** Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur. [7]

En général, la sécurité informatique consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées pour les fins auxquelles elles ont été conçues au début. De plus elle vise à inscrire l'évolution des systèmes informatique dans le cadre d'un processus d'amélioration continue.

III. La gestion des risques

III.1 Les enjeux :

Pour se protéger des pirates, il faut connaître les possibilités d'attaques. Aussi, pour se défendre d'elles, il faut commencer par accepter le danger. La mise en place d'une politique (ou plan) de sécurité consiste en :

L'identification des éléments à protéger (matériels, logiciels, données, personnes, etc.).

L'identification des attaques éventuelles des pirates dont :

- ***La dégradation*** qui consiste à perturber le réseau informatique via une panoplie de programmes parasites tels que les virus, les chevaux de Troie, les vers (WORM), les bombes, les bactéries, etc.
- ***L'altération*** des données qui s'effectue soit pendant la transmission des données sur un réseau, soit avant leur émission, soit pendant le passage sur un nœud du réseau.
- ***L'écoute*** qui consiste à surveiller et intercepter des données soit sur un poste (cheval de Troie), soit sur une ligne de communication (sniffer et probe).

Le choix d'une approche de sécurité : détermine si la sécurité du réseau nécessite de : *ne rien autoriser, n'autoriser que, autoriser tout sauf, ou tout autoriser.*

Le choix des moyens nécessaires pour pallier aux défaillances de sécurité : il s'agit d'acheter le matériel et les logiciels appropriés aux besoins et à la politique adoptée. [3]

III.2. Les vulnérabilités :

Est une faille dans un logiciel qui compromet la sécurité de l'ordinateur ou du réseau. Des configurations d'ordinateur ou de sécurité incorrectes peuvent également engendrer des 0vulnérabilités. Les menaces exploitent les failles pour endommager l'ordinateur ou les données personnelles.

- ***Les services:*** en général, ces services sont l'e-mail, le Web ou toute autre application qui communique avec une autre application. On citera par exemple les attaques contre IIS en 2001 qui ont permis la diffusion du ver CodeRed. Les vulnérabilités des services sont très dangereuses car elles ne nécessitent pas une intervention humaine
- ***Les applications*****:** les vulnérabilités des applications nécessitent souvent une intervention humaine: par exemple l'utilisateur qui active un virus par un clic de souris. Quoi de plus alléchant que des mails avec le sujet "I love You" ou avec un contenu informant que vous êtes l'heureux gagnant d'une énorme somme d'argent? Un simple clic et on se retrouve victime d'un virus, Worm ou spyware.
- ***Les actions des utilisateurs:*** les utilisateurs peuvent engendrer des vulnérabilités sur des systèmes ou des logiciels par des configurations mauvaises ou incorrectes. Un utilisateur peut reconfigurer un système ou un logiciel et ouvrir ainsi des portes à des hackers. Dans ce cas, même le système de sécurisation le plus performant, s'il est mal configuré, offre une brèche de sécurité.

III.3. Les menaces :

Est un événement, d'origine accidentelle ou délibérée, capable s'il se réalise de causer un dommage au sujet étudié. Le réseau informatique comme tout autre réseau informatique est en proie à des menaces de toutes sortes qu'il convient de recenser. [5]

- ***Les menaces passives*** : consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même. [5]
- ***Les menaces actives*** : consistent à altérer des informations ou le bon fonctionnement d'un service. [5]

III.3.1. Quels types de menaces dans le réseau de l'entreprise ?

L'expertise sécurité de SFR Business Team vous permet de renforcer la protection de vos environnements et de bénéficier d'une meilleure **maitrise des risques informatiques** tels que :

- ***Vol de données sensibles*** telles que les bilans d'entreprises, ses brevets, plan stratégique, business plan
- ***Fuite d'information*** (résultats d'étude, plan de lancement de produit, grille de prix).
- ***Piratage*** des équipements par l'utilisation malveillante d'une faille de sécurité d'un logiciel, **phishing** (réception d'un email qui invite l'utilisateur à naviguer sur un site web contrefait)
- Maladresse, **malveillance interne.**

III.4. Les attaques :

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques. [16]

IV. Les logiciels malveillants :

Est un logiciel développé par un pirate dans le but de nuire à un système informatique.

IV.1 Un Virus :

Est un logiciel malveillant, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un évènement donné. [6]

Un virus se propage de lui-même en infiltrant son code dans une application. Le nom vient de son archétype biologique. Le virus ne se limite généralement pas à sa propagation, ce qui rend inutilisable le logiciel hôte, mais lance en plus des routines malicieuses.

Les virus peuvent être classés suivant leur mode de propagation et leurs cibles:

- ***Le virus de boot*** : il est chargé en mémoire au démarrage et prend le contrôle de l'ordinateur.
- ***Le virus d'application*** : ils infectent les programmes exécutables, c'est-à-dire les programmes (.exe, .com ou .sys) en remplaçant l'amorce du fichier, de manière à ce que le virus soit exécuté avant le programme infecté. Puis ces virus rendent la main au programme initial, camouflant ainsi leur exécution aux yeux de l'utilisateur.
- ***La macro virus*** : il infecte des logiciels de la suite Microsoft Office les documents bureautiques en utilisant leur langage de programmation, qui contaminera tous les documents basés sur lui, lors de leur ouverture.

IV.2. Un ver :

Est un logiciel malveillant indépendant qui se transmet d'ordinateur à ordinateur par l'internet ou tout autre réseau et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. [1]

IV.3. Un cheval de Troie :

Un cheval de Troie est une forme de logiciel malveillant déguisé en logiciel utile. Son but : se faire exécuter par l'utilisateur, ce qui lui permet de contrôler l'ordinateur et de s'en servir pour ses propres fins, quelles qu'elles soient. Généralement d'autres logiciels malveillants seront installés sur votre ordinateur, tels que permettre la collecte frauduleuse, la falsification ou la destruction de données. [1]

IV.4. Un logiciel espion :

(Espiogiciel ou logiciel espion) est un programme ou un sous-programme, conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur, ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs. [1]

IV.5. Un logiciel publicitaire :

Est un logiciel qui affiche des annonces publicitaires sur l'écran d'un ordinateur et qui transmet à son éditeur des renseignements permettant d'adapter ces annonces au profil de l'utilisateur. [2]

IV.6. Le spam :

Est correspond à l'envoi intempestif de courriers électroniques, publicitaires ou non, vers une adresse mail. Le spam est une pollution du courrier légitime par une énorme masse de courrier indésirable non sollicité. [2]

IV.7. Un canular (Les Hoax) :

Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries avec des chaînes de mails. Certaines fausses alertes misent également sur l'ignorance des utilisateurs en matière d'informatique pour leur faire supprimer des éléments sains de leur système. [2]

IV.8. Une bombe logique :

Est la partie d'un virus, d'un cheval de Troie ou de tout autre logiciel malveillant qui contient les fonctions destinées à causer des dommages dans l'ordinateur infecté. Ainsi ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machines (on parle alors de bombe à retardement ou de bombe temporelle), par exemple le jour de la Saint Valentin, ou la date anniversaire d'un événement majeur.

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise. [2]

V. Mécanismes de la sécurité :

V.1. Le Cryptage :

Le chiffrement ou cryptage est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre. Pour vérifier l'intégrité ou l'authenticité d'un document, on utilise respectivement un Message Authentification Code (MAC) ou une signature numérique. La sécurité d'un système de chiffrement doit reposer sur le secret de la clé de chiffrement et non sur celui de l'algorithme, suppose en effet que l'ennemi (ou la personne qui veut déchiffrer le message codé) connaisse l'algorithme utilisé. [8]

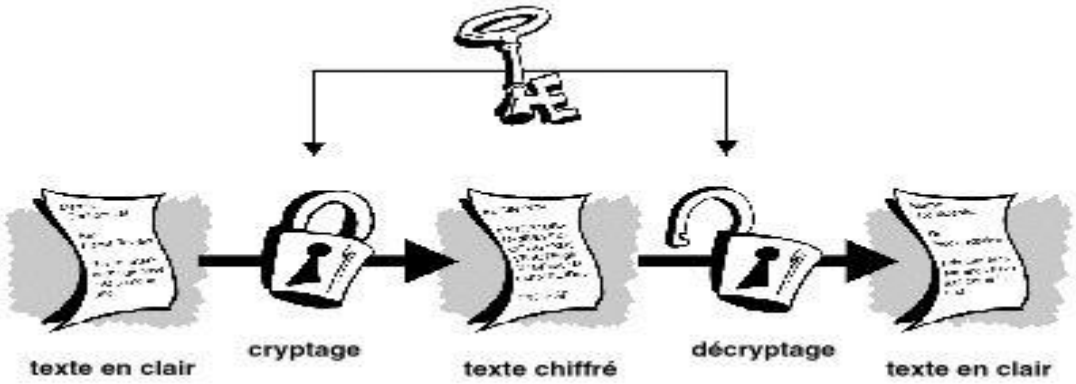


Figure I.1.Le chiffrement symétrique. [4]

V.2. Un pare-feu :

Est un logiciel ou un matériel qui vérifie les informations provenant d'Internet ou d'un réseau, puis les empêche d'accéder à l'ordinateur ou les y autorise, selon vos paramètres de pare-feu définis.

Un pare-feu vous aide à empêcher les utilisateurs ou les logiciels malveillants (tels que les vers) d'accéder à votre ordinateur via un réseau ou Internet. Un pare-feu peut également empêcher votre ordinateur d'envoyer des éléments logiciels nuisibles à d'autres ordinateurs.

Le schéma suivant illustre la façon dont un pare-feu fonctionne.

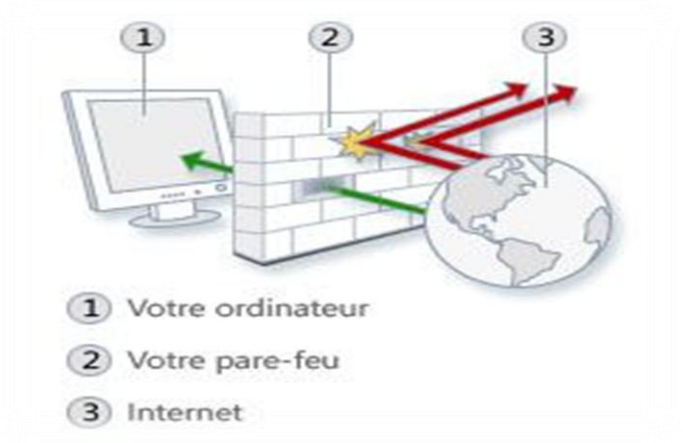


Figure I.2. Principe de pare-feu.

V.3. Un antivirus :

Est un programme capable de détecter... les virus, les vers, les troyens et parfois les spywares qui peuvent infecter un ordinateur. L'antivirus devrait être résident sur l'ordinateur, mais il existe aussi des tests d'infection virale disponibles sur le web.

Un antivirus " résident " est installé sur l'ordinateur comme n'importe quel autre programme classique. Il doit démarrer en même temps que l'ordinateur et rester actif durant tout le temps que dure la session de travail.

Le logiciel antivirus devrait obligatoirement figurer sur tout ordinateur, même non connecté à l'Internet : les clefs USB échangées d'ordinateur à ordinateur sont également des vecteurs importants de virus.

Un bon antivirus doit intervenir au moment même de l'entrée ou de la tentative d'entrée d'une peste quelconque. [4]

Lorsque le virus a été découvert, l'antivirus peut :

- nettoyer les fichiers infectés en éradiquant les virus.
- supprimer les fichiers infectés (attention aux problèmes que cela peut poser).
- écarter le virus dans une zone du disque dur où il ne peut nuire : on parle alors d'une mise en quarantaine.

V.4. Les serveurs proxy :

Un serveur proxy, permettant aux machines d'un réseau d'accéder à internet, peut combiner tout un ensemble de solutions citées précédemment.

Un serveur proxy est un ordinateur comportant deux cartes réseau, un routeur de réseau, un pare-feu et des logiciels de sécurisation:

- ***Cartes réseau:*** L'une des cartes réseau permet la connexion à internet, tandis que l'autre permet de se connecter au réseau privé.

- ***Routeur:*** Le composant logiciel routeur de réseau permet à l'ordinateur de partager une connexion entre les différents ordinateurs du réseau.

- ***Pare-feu:*** Dans la plupart des cas, il combine un pare-feu de niveau réseau et application pour offrir une sécurité maximale.

- ***Antivirus:*** Il permet d'empêcher virus, vers et chevaux de Troie d'infecter le réseau et réduit la nécessité d'installer un antivirus par poste.

- ***Filtrage:*** Le filtrage permet d'empêcher l'accès à certains sites.

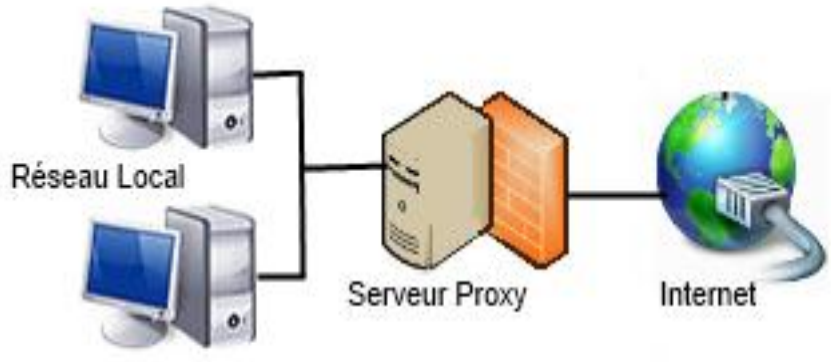


Figure I.3. Principe de serveurs proxy

VI. Mise en place d'une politique de sécurité :

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

L’objectif d’une politique de sécurité est la protection contre les attaques et les menaces. Pour se protéger contre les logiciels malveillants qui circulent essentiellement sur le réseau internet, nous devons installer et utiliser un anti-virus.

VII. Conclusion :

Le système d'information d'une entreprise peut être vital à son fonctionnement. Il est donc nécessaire d'assurer sa protection, afin de lutter contre les menaces qui pèsent sur l'intégrité, la confidentialité et la disponibilité des ressources.

Beaucoup de compétences sont nécessaires pour assurer une sécurité optimale, mais il est impossible de garantir la sécurité de l'information à 100%. Malgré tout, il existe des moyens efficaces pour faire face à ces agressions, par exemple : les antivirus.

Il est donc utile de bien savoir gérer les ressources disponibles et comprendre les risques liés à la sécurité informatique, pour pouvoir construire une politique de sécurité adaptée aux besoins de la structure à protéger. La mise en place d'un dispositif de sécurité efficace ne doit cependant jamais dispenser d'une veille régulière au bon fonctionnement du système.

Chapitre II :

Les Antivirus

I. Introduction :

Les antivirus, qu'ils soient gratuits ou payants, vous protègent contre l'exécution de codes malveillants sur votre PC. On devrait d'ailleurs les appeler des « antimalwares », car les virus informatiques ont presque intégralement disparu du paysage, remplacés par les cheval de Troie, spywares, adwares, bots, bitcoin miners, Worms (vers), ransomwares, rootkits, keyloggers, rogues, droppers, downloaders, RATs, exploits, etc. On parle donc davantage de « codes malveillants » ou de « malwares », que de « virus ».

Mais pour vous protéger efficacement contre tous ces logiciels malveillants, il faut multiplier les boucliers défensifs. Les suites intègrent plusieurs boucliers (pare-feu, protection Web, réputation Cloud, analyse comportementale, etc.) qui collaborent entre eux pour mieux vous défendre.

Par ailleurs, les suites cherchent à vous protéger non seulement contre tous ces codes dangereux, tous ces malwares, mais aussi à vous protéger contre les sites Web qui les véhiculent et contre les autres pièges auxquels vos navigations Web vous exposent (phishing, water holes, etc.).

Enfin, les suites de sécurité incorporent des protections complémentaires pour protéger vos données (coffre-fort virtuel, chiffrement, broyeur de fichiers, sauvegarde en ligne), pour protéger votre identité (gestion sécurisée des mots de passe, protection des transactions bancaires, anti-phishing évolué), et pour protéger vos enfants (contrôle parental, parfois étendu sur tous les appareils du foyer).

II. Définition d'un anti-virus :

Un antivirus est un logiciel qui a pour but de détecter et d'éradiquer les virus présents dans votre micro, et de prendre des mesures pour les empêcher de nuire.

Les antivirus sont des programmes devenus de plus en plus indispensables au fil des années. En effet, du début de l'internet : on pouvait surfer tranquillement sur la toile à l'aide d'un simple pare-feu, sans être trop inquiété, dès lors que l'on faisait attention à ce que l'on téléchargeait.

Aujourd'hui, cette époque est révolue. Le moindre site internet un peu trop malicieux peut vous infecter, la plupart du temps via des plugins (Flash, Java,…).

Son fonctionnement ne consiste pas qu'à analyser les fichiers du système, puisque si un fichier est infecté, le mal est souvent fait. Le rôle de l'antivirus consiste aussi à prévenir l'attaque virale, en analysant le comportement. [13]

Une suite de sécurité est un antivirus qui offre plusieurs services (Scan, Pare-feu, protection web, analysé de comportement, protection permanente…), il permet essentiellement de protéger les utilisateurs contre les menaces venant d'internet.

III. Fonctionnalité de l'antivirus :

III.1. Composants d'un antivirus

II1.1.a. Scanner :

Le scanner examine (scan) votre ordinateur à la demande : un fichier, un dossier ou tous les fichiers de votre disque. Un scan complet consomme beaucoup de ressources matérielles et de temps, mais il est conseillé de le faire de temps en temps. [13]

II1.1.b. Moniteur : Le moniteur analyse en temps réel les fichiers auxquels vous accédez au cours de votre utilisation normale et stoppe immédiatement une exécution virale. Il est composé de plusieurs modules dont le nom change suivant les logiciels. Par exemple Kaspersky en a quatre, chacun dédié à une tâche : email, Web, téléchargement, système. [13]

En fonction de sa configuration et de la puissance de votre ordinateur, il ralentit plus ou moins vos applications. [13]

II1.1.c. Base de signatures de virus :

Une signature est un bout de code permettant d'identifier un virus, un peu comme une empreinte digitale humaine. La base de signatures référence des dizaines de milliers de virus, troyens et variantes. Elle doit être mise à jour fréquemment pour reconnaître les nouveaux spécimens. [12]

III.2. L'antivirus résident :

Un antivirus " résident " est installé sur l'ordinateur comme n'importe quel autre programme classique. Il doit démarrer en même temps que l'ordinateur et rester actif durant tout le temps que dure la session de travail.

Le logiciel antivirus devrait obligatoirement figurer sur tout ordinateur, même non connecté à l'Internet : les clefs USB échangées d'ordinateur à ordinateur sont également des vecteurs importants de virus.

Un bon antivirus doit intervenir au moment même de l'entrée ou de la tentative d'entrée d'un malveillant quelconque.

Lorsque le virus a été découvert, l'antivirus peut :

- nettoyer les fichiers infectés en éradiquant les virus.
- supprimer les fichiers infectés (attention aux problèmes que cela peut poser).
- écarter le virus dans une zone du disque dur où il ne peut nuire : on parle alors d'une ***mise en quarantaine***. [12]

III.3. Détection de la signature :

On l'appelle aussi **scan** ou **scanning**. C'est la méthode la plus ancienne et la plus utilisée. Cette méthode consiste à analyser le disque dur à la recherche de la **signature** du virus, qui est présente dans la base de données du logiciel, si celui-ci est à jour et s'il connaît ce virus.

La signature est un **morceau de code** ou une **chaîne de caractères** du virus qui permet de l'identifier. Chaque virus a sa propre signature, qui doit être connue de l'antivirus. Cette méthode n'est pas efficace contre les nouveaux virus ou les virus dits **polymorphes**, dont la signature change à chaque réplication.

L'avantage de la technique du scan est qu'elle permet de détecter les virus avant leur exécution en mémoire, dès qu'ils sont stockés sur le disque et qu'une analyse est exécutée.

Pour rester efficace, l'antivirus doit procéder à la mise à jour régulière de sa base de données antivirale. Une fréquence de mise à jour mensuelle est un minimum acceptable. [12]

III.4. L'analyse heuristique :

C'est la méthode la plus puissante car elle permet de détecter d'éventuels virus inconnus par votre antivirus. Elle cherche à détecter la présence d'un virus en analysant le code d'un programme inconnu (en simulant son fonctionnement). Elle provoque parfois de fausses alertes. [14]

III.5. Le contrôle d'intégrité :

L'antivirus, pour contrôler l'intégrité des fichiers, va stocker un fichier central recensant l'ensemble des fichiers présents sur le disque auxquels il aura associé des informations qui peuvent changer lorsque le fichier est modifié :

- La taille.
- La date et heure de le dernière modification.
- La somme de contrôle (CRC : code de redondance cyclique) éventuelle.

Lorsqu'une analyse est effectuée (ou à l'ouverture du fichier si l'antivirus réside en mémoire), l'antivirus recalcule la somme de contrôle et vérifie que les autres paramètres n'ont pas été modifiés. Si une anomalie se présente, l'utilisateur est informé.

Pour contrer en partie cette parade, les virus ne modifient pas forcément la date de modification du fichier, ou la rétablissent. [14]

III.6. Méthodes de détection virale :

Les méthodes changent d'un logiciel à l'autre :

- Les signatures de virus (à mettre à jour souvent : il s'en crée tous les jours).

- L'analyse heuristique recherche un comportement viral dans les programmes, permettant de détecter des programmes malveillants inconnus (de sa base de signatures).

- L'examen comportemental surveille le comportement des logiciels actifs à travers les accès aux fichiers.

- Le contrôle d'intégrité permet de détecter les modifications de fichiers sur le disque.

- La détection générique multi-niveaux recherche les virus polymorphes.

Malgré une mise à jour fréquente de la base de signatures et toutes les méthodes de détection, un nouveau virus peut quand même passer inaperçu. Il a été démontré qu'aucun antivirus n'est efficace à 100 %.

IV. Evaluation des anti-virus :

Que vous soyez une petite ou une grande entreprise, vous devez installer un antivirus pour protéger au mieux votre matériel. Dans ce comparatif, nous avons sélectionné les 7 antivirus / antispyware gratuits et payants les plus en vue du moment avec leurs avantages et inconvénients.

IV.1 Antivirus pour protéger son PC et ses appareils mobiles :

Les mobiles (smartphones, tablettes) utilisent des systèmes d'exploitation différents du PC. Les éditeurs doivent donc créer des protections spécifiquement pour ces appareils. La plupart des Suites de Sécurité estampillées « 2015 » sont néanmoins déclinées en versions « multi-devices ». Leur licence comprend donc l'installation sur PC, sur Mac, sur smartphones et sur tablettes, avec des versions adaptées à chaque appareil.

Toutefois, la vraie difficulté aujourd'hui consiste à livrer des protections que l'on peut piloter de façon centralisée : depuis votre PC ou une interface Web, vous devez être capable de vérifier et configurer les protections de tous les appareils du foyer et notamment des tablettes et smartphones des enfants. En la matière, Kaspersky est l'éditeur le plus avancé dans cette unification. [15]

Efficacité Défensive

(L'histogramme, meilleures sont les défenses)

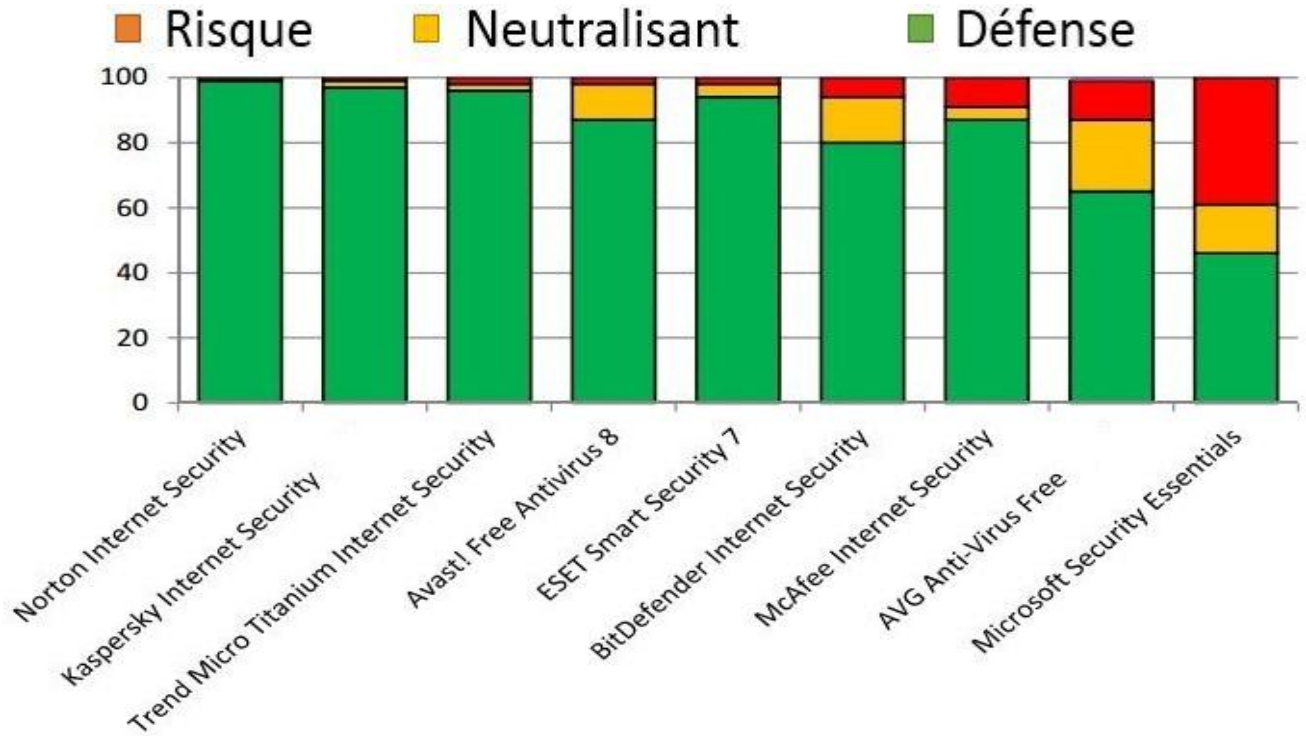


Figure II.1. Comparaison des anti-virus. [15]

IV.2. Tableau comparatif :

Le Bureau de sécurité de l'information a choisi ces 5 critères pour comparer les différentes solutions antivirus dans ce tableau.

Suite de Sécurité	**Kaspersky Antivirus 2015**	**BitdefendeAntivirus 2015**	**Norton security 2015**	**Panda Antivirus 2015**	**McAfee Antivirus 2015**
Détection de Logiciels malveillants.					
Signature électronique pour la détection de programmes malveillants	**100%**	**100%**	**99.8%**	**99.8%**	**99.9%**
Bloquer complètement les attaques	**100%**	**100%**	**100%**	**99.6%**	**99.4%**

Bloquer partiellement les attaques	**0%**	**0%**	**0%**	**0%**	**0%**
Infection nettoyage					
Parer avec succès les composants malveillants actifs	**100%**	**100%**	**100%**	**100%**	**100%**
Parer avec succès les composants malveillants actifs et inactifs	**90%**	**80%** **70%**	**60%**	**70%**	**70%** **70%**
Vitesse de scan					
Note de design	**Excellent**	**Excellent**	**Supérieur**	**très bien**	**très bien**

Tableau II-1 : Tableau Comparaison des anti-virus.

Meilleure note globale : **Kaspersky Antivirus 2015** La version 2015 de Kaspersky a protégé efficacement notre système-test des malwares et a également éliminé rapidement les différentes infections de notre PC. C'est un logiciel rapide et parfaitement conçu.

IV.3. Palmarès :

Des classements sont aussi proposés par type de tests.
Les meilleurs **en situation réelle** :

1. Kaspersky
2. Emsisoft
3. Avast et Eset

Les meilleurs pour la **détection des virus**

1. F-Secure
2. Bitdefender, Qihoo
3. Bullguard, Kaspersky

Les meilleurs pour **l'absence de faux positifs** (erreurs de détection)

1. Fortinet
2. Eset
3. Kaspersky

Les meilleurs pour l'absence **d'impact sur les performances** sur le système

1. Sophos
2. Avast, F-Secure, Kaspersky
3. Bitdefender

Les meilleurs pour la **détection heuristique** (virus non reconnus par la base virale)

1. Bitdefender
2. Kaspersky
3. Bullguard

Les meilleurs pour la **suppression de malwares**

1. Kaspersky
2. Bitdefender
3. Avira

Les meilleurs pour la protection **contre le phishing**

1. Eset, Kaspersky
2. Bitdefender, McAfee, Trend Micro
3. Fortinet

Antivirus se dégagent assez nettement, Kaspersky Antivirus 2015 nous a impressionnés par sa protection exceptionnelle, et par l'ensemble d'outils utiles.

Kaspersky Antivirus 2015 fournit une excellente valeur comme une « standard » suite antivirus. Le logiciel fournit une protection haute gamme contre les malwares; il comprend une foule de caractéristiques véritablement utiles telle qu'un scanner de vulnérabilité et des outils pour une navigation sûre; et une interface intuitive. [17]

VI. Conclusion :

Tout au long de ce chapitre, nous avons parcouru une des problématiques majeures de la sécurité informatique : les virus. Nous avons constaté qu'il existait plusieurs types de virus, dont la naissance remonte à des époques différentes, et coïncide avec les grandes phases de l'informatique. avec l'avènement de l'Internet grand public, il y a eu une multiplication des vers.

Un antivirus est une classe de logiciel qui détecte et nettoie les fichiers infectés par un virus tandis qu'une suite de sécurité internet est un bouquet de logiciels qui vise à protéger les utilisateurs contre les menaces venant d'Internet.

Mise en œuvre

Chapitre III :

Conception et implémentation

Partie I : conception

I- Introduction

Ce chapitre présente la description d'une solution proposée pour le déploiement de l'application antivirus dans les ordinateurs de l'université. Dont le but de sécuriser les ordinateurs, et préserver l'intégrité de leurs données. Cette partie comprend deux étapes. La première étape consiste à décrire la mise en œuvre de la solution proposée dans l'environnement réseau de l'université, i.e. Kaspersky Security Center, avec description de la version utilisée. La deuxième étape décrit le processus de déploiement aux postes clients, de l'application par l'agent d'administration à partir du serveur d'administration.

Et nous avons présentons l'architecteur globale du réseau de l'université, on dispose des informations précises sur l'infrastructure réseau physique qui comprend les équipements d'interconnexion de déférents réseaux locaux qui constitue le réseau d'université, avec une présentation des schémas détaillé descriptif de l'architecture des armoires réseaux.

I.1 Présentation l'architecteur globale du réseau d'université :

Le réseau de l'université kasdi Merbah Ouargla, est un réseau LAN basée sur la topologie étoile, il est composé de 5 site principal interconnecté: Rectorat, l'institut de sport , khefdji-1,khefdji-2 et Médecine. Le Deux Cœurs se trouve au niveau du site Rectortat et Khafdji-1 ces derniers sont de marque Cisco, type catalist 6500, pour les niveaux distribution et access il est utilisé switchs Cisco 2960 et cisco 4500. Les différents sites sont interconnectés par fibre optique. Il existe deux source d'accès à l'internet, l'ADSL fournit par un Modem Djawab de band passante 8 méga, et CERIST fournit par un routeur cisco3800 de band passante 100 Méga. Les serveurs ce trouves dans une zone DMZ, assuré par un firewall Cisco ASA 5045.

On conclut que Le réseau de l'université Kasdi Merbah Ouargla, est un réseau LAN basée sur la topologie étoile, il est composé de 5 site principal interconnecté relier par fibre, les équipements d'interconnexion de déférent site sont de marque Cisco. Il existe deux source d'accès à l'internet, l'ADSL fournit par un Modem Djawab de band passante 8 méga, CERIST fournit par un routeur cisco3800 de band passante 100 Méga.

La figure suivant présent l'architecteur globale :

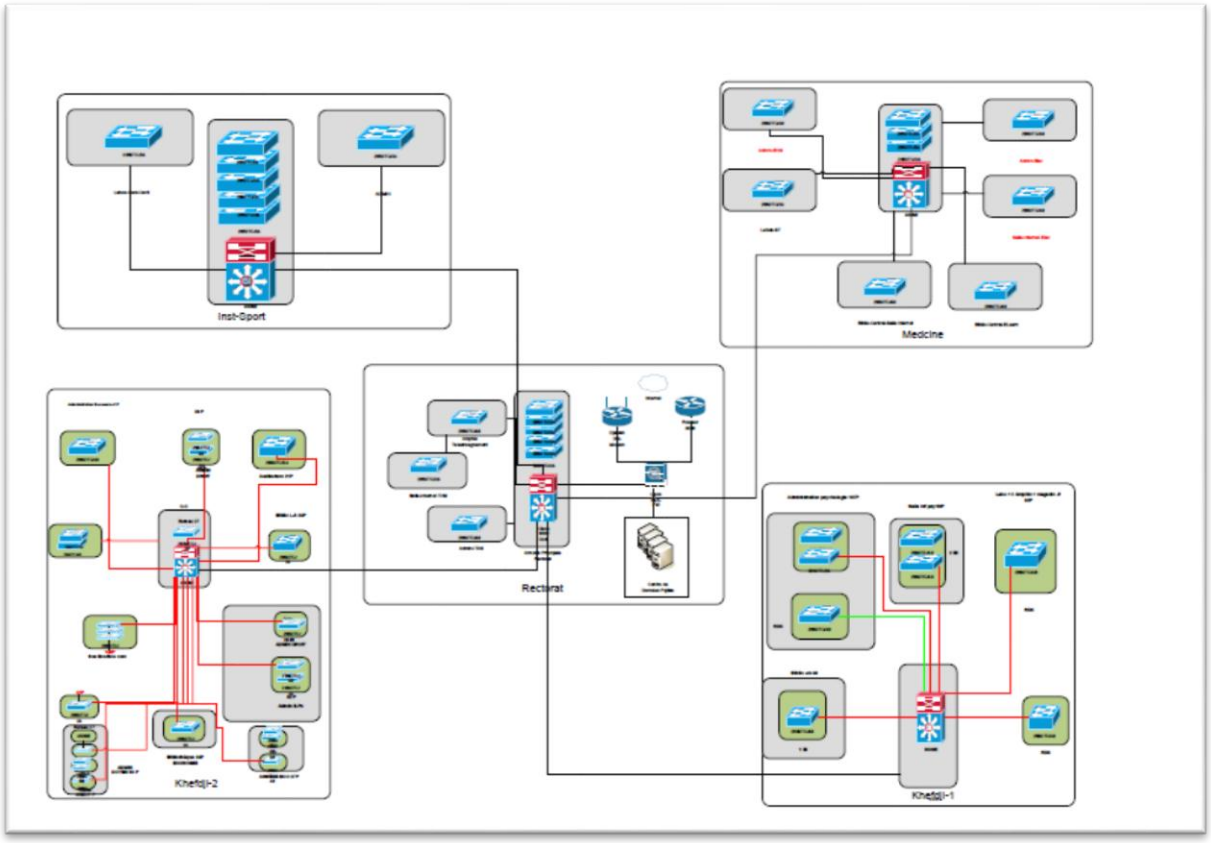


Figure *III.1* :l'architecteur globale de réseau de l'université.

I.1.a La description de réseau de Rectorat :

Les réseaux de rectorat sont constitué de quatre réseaux locaux (4 LAN) divisé entre différents emplacement :

1. Rectorat.
2. ITAS (Administration).
3. ITAS (Salle Internet).
4. Amphi téléenseignement.

❖ L'armoire principale des réseaux de faculté est placée Rectorat, deux câble fibre de source d'accès à l'internet Modem Djawab et routeur SIRICT vers l'armoire principale est présenté pour alimenter l'armoire principale par l'internet, et celle-ci diffuse set câbles fibre entre l'emplacement suivant :

- ✓ ITAS (Administration).
- ✓ ITAS (Salle Internet).
- ✓ Amphi téléenseignement.

L'armoire principale se connecte aussi par une zone DMZ contient les serveurs et le firewall ASA.

La figure suivant montré la diffusion des réseaux de site (Topologie en étoile) et présent un schéma détaillé descriptif de l'architecture des armoires réseaux de site :

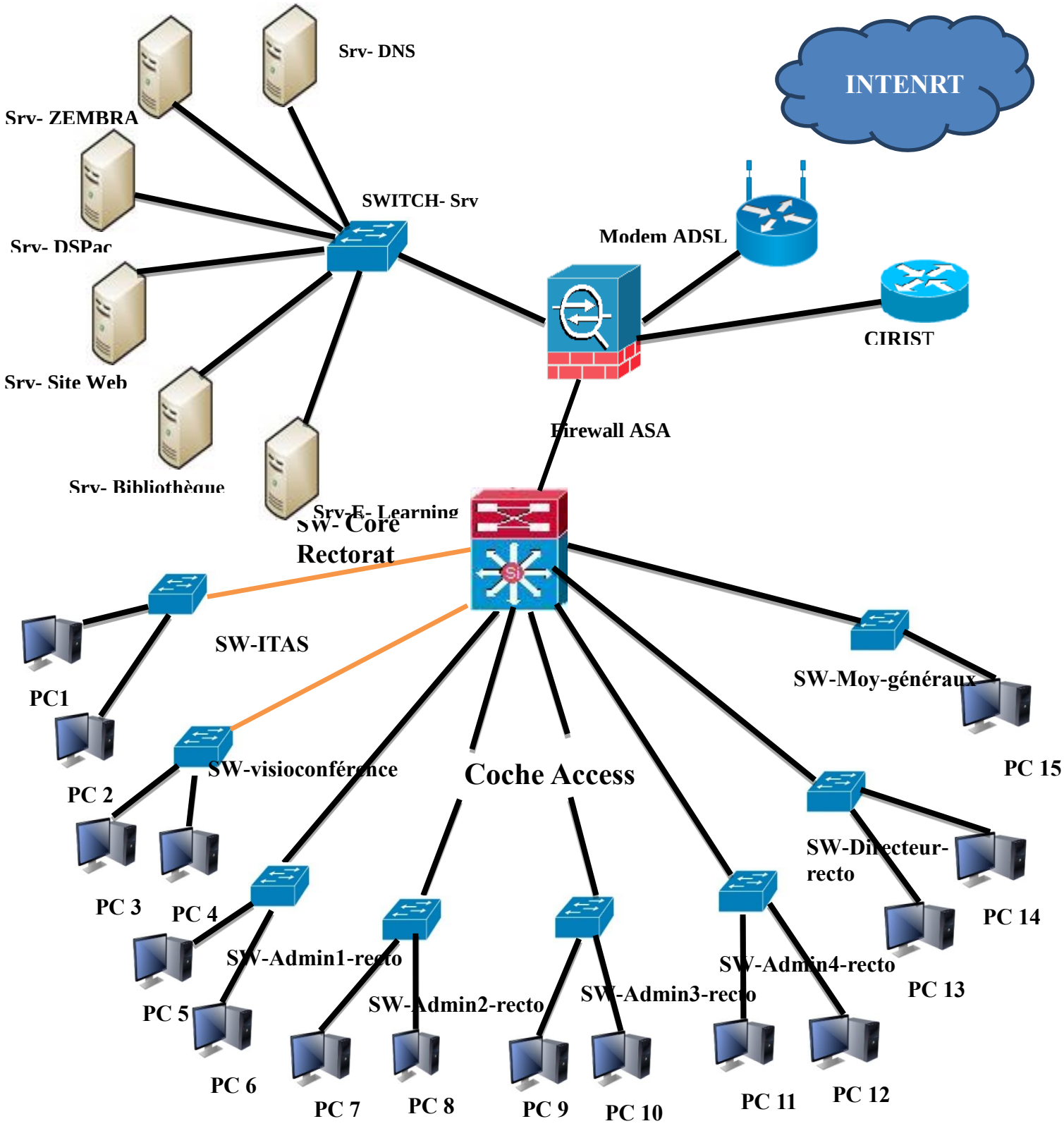


***Figure III.2** : description le réseau de rectorat*

I.2 description Kaspersky Security Center:

Cette section décrit les composants de l'application Kaspersky Security Center.

I.2.a. Kaspersky Security Center :

L'application Kaspersky Security Center a été développée pour centraliser les principales tâches d'administration et assurer le système de protection du réseau de l'entreprise. L'application offre à l'utilisateur l'accès aux informations détaillées sur le niveau de sécurité du réseau de l'entreprise et permet de configurer tous les modules de la protection construite sur la base des applications de Kaspersky Lab.

Figure III.3. *Interface Kaspersky Security Center 10*

L'application Kaspersky Security Center est un outil destiné aux administrateurs de réseaux d'entreprise et aux responsables de la sécurité.

I.2.b Architecture de l'application Kaspersky Security Center 10 :

L'application **Kaspersky Security Center 10** inclut les modules principaux suivants :

- **Serveur d'administration** Exerce la fonction de sauvegarde centralisée des informations relatives aux applications installées sur le réseau de l'organisation et d'administration de celles-ci.

- **Agent d'administration** Coordonne les interactions entre le *Serveur d'administration* et les applications « *Kaspersky Lab* » installées sur le poste de travail ou le serveur. Ce module est unique pour toutes les applications développées pour les systèmes Microsoft Windows. Pour les applications «**Kaspersky Lab** » développées pour les systèmes Novell et Unix, des versions séparées de l'*Agent d'administration* existent.
- **Console d'administration** Fournit l'interface utilisateur nécessaire pour la gestion de l'état du *Serveur d'administration* et de l'*Agent d'administration*. La *Console d'administration* est exécutée sous la forme d'une extension de Microsoft Management Console (MMC) *La Console d'administration* permet de se connecter à distance *au Serveur d'administration* par Internet.
- **Kaspersky Security Center Web-Console** Conçue pour contrôler l'état du système de protection de l'entreprise du réseau de l'organisation cliente se trouvant sous l'administration de *Kaspersky Security Center 10*.

I.2.c. Qu'est-ce que l'Agent de mise à jour ?

Kaspersky Security Center 10 permet de livrer les mises à jour sur les postes clients des groupes d'administration non pas via le *Serveur d'administration*, mais via les **agents de mise à jour** de ces groupes.

Agent de mise à jour : il s'agit de l'ordinateur entrant dans la composition du réseau du *Serveur d'administration*, destiné à la sauvegarde et au déploiement des mises à jour des bases, des paquets d'installation, des tâches groupées et des stratégies (centre relais de sauvegarde des bases, des paquets, des tâches et des stratégies). L'**Agent de mise à jour** est désigné pour tous les groupes d'administration.

Tâche principale de l'**Agent de mise à jour**: déploiement (mise à jour) des bases et des paquets d'installation sur tous les postes clients pour lesquels il a été désigné, ainsi que la réduction de la charge du *Serveur d'administration*.

Il est utile d'avoir recours à l'**Agent de mise à jour**, si sur le réseau, la majorité des sites distants ne comptent que peu d'ordinateurs. Cela permettra d'économiser le trafic VPN et un autre ordinateur ne sera pas nécessaire pour l'installation d'un Serveur d'administration secondaire.

Les agents de mise à jour reçoivent :

- **les *bases des menaces connues* :** au fil de leur apparition sur le Serveur d'administration (automatique). Ou via le lancement d'une tâche spécifique de téléchargement des bases à partir des serveurs de Kaspersky Lab.
- **les *paquets d'installation* :** après le lancement de la tâche du téléchargement à distance forcé de ce paquet. L'agent de mise à jour reçoit le paquet uniquement si la tâche est désignée pour au moins un ordinateur de son groupe.
- ***tâches*** – lancement des tâches groupées désignées à l'aide du Serveur d'administration
- ***stratégies*** - application des stratégies avec le Serveur d'administration.

I.2.d. Structure de la protection Kaspersky Security Center 10 sur le réseau :

Sur le réseau de l'organisation, il est possible d'utiliser l'une des structures types suivantes de déploiement de la protection :

- ***Un Serveur d'administration***. Tous les postes clients sont connectés à un seul *Serveur d'administration*. Le *Serveur d'administration* joue le rôle de l'**agent de mises à jour**.
- ***Un Serveur d'administration avec les agents de mise à jour***. Tous les postes clients sont connectés à un seul *Serveur d'administration*. Les postes clients qui jouent le rôle des **agents de mises à jour** sont indiqués dans le réseau. En qualité d'agents de mises à jour, il est recommandé d'utiliser l'ordinateur le plus « puissant » allumé en permanence.
- ***Hiérarchie des Serveurs d'administration***. Pour chaque segment du réseau, un *Serveur d'administration* séparé inclus dans la hiérarchie partagée des *Serveurs d'administration* est indiqué. Le *Serveur* d'administration principal joue rôle de l'*agent de mises à jour*.

I.2.e. Hiérarchie des Serveurs d'administration :

Hiérarchie des Serveurs d'administration avec les agents de mise à jour pour chaque segment du réseau, un *Serveur d'administration* séparé inclus dans la hiérarchie partagée des *Serveurs d'administration* est indiquée. Les postes clients qui jouent le rôle des **agents de mises à jour** sont indiqués dans le réseau.

Kaspersky Security Center 10 donne à l'administrateur la possibilité de hiérarchiser l'organisation des *Serveurs d'administration* installés sur le réseau de l'entreprise.

Des *Serveurs d'administration* réels ou virtuels peuvent être définis en tant que serveurs secondaires.

Les *Serveurs d'administration* peuvent fonctionner avec une hiérarchie du type « serveur principal – serveur secondaire ».

Chaque *Serveur d'administration* peut disposer de plusieurs *Serveurs d'administration* secondaires à différents niveaux de hiérarchie. Le niveau d'intégration des Serveurs secondaires n'est pas limité. De plus, les postes clients de tous les Serveurs secondaires feront partie des groupes d'administration du Serveur principal. De cette façon, les membres indépendants du réseau informatique peuvent être gérés par différents *Serveurs d'administration* qui, à leur tour, sont gérés par le Serveur principal.

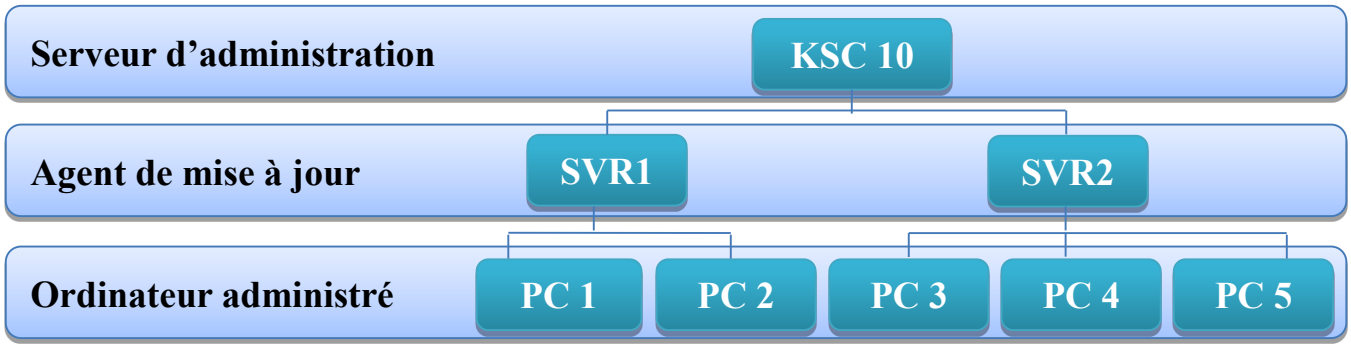


Figure III.3. *Hiérarchie des Serveurs d'administration*

Partie II : réalisation et mise en œuvre

I. Etape de déploiement

I.1. Fichiers d'installation

Plusieurs fichiers de distribution sont disponibles :

- **Outils utilisé dans partie Software**

On a utilisé Windows server 2008 R2

On a utilisé Kaspersky Security Center version 10.1.249

On a utilisé Kaspersky Security Center -Web Console version 10.0.38

On a utilisé NET Framework 4.5

Environnement Virtuel, VMware, Vsphere.

- **Outils utilisé dans partie Hardware**

On a utilisé Serveur DATA- Center de l'université.

On a utilisé 120 ordinateurs, avec comme Systèmes d'exploitation Microsoft Windows :

- Windows 7, ou Windows XP professionnelle SP2

I.1.a. Les étapes de l'installation suivis :

Dans le DATA-Center de l'université, on crée un serveur virtuel VM (Virtuel Machine). Dans Cette dernière, en a installé Windows server 2008 R2, avec 6Go de mémoire. Apres on a installé Kaspersky Security Center, Kaspersky Security Center -Web Console et .NET Framework.

- On a utilisé comme Adresse de connexion du serveur d'administration, le: nom DNS de l'ordinateur.

- Les Ports utilisé pour la connexion des clients avec le Serveur d'administration

- 13000 : pour les connexions SSL des Agents d'administration et des Consoles d'administration.
- 14000 : pour les connexions non SSL des Agents d'administration et des Consoles d'administration.

I.2. Assistant installation à distance

- Plug-ins d'administration

- Serveur d'administration de Kaspersky Security Center 10
- Agent d'administration de Kaspersky Security Center 10
- Kaspersky Endpoint Security 10 for Windows

-Paquets d'installation

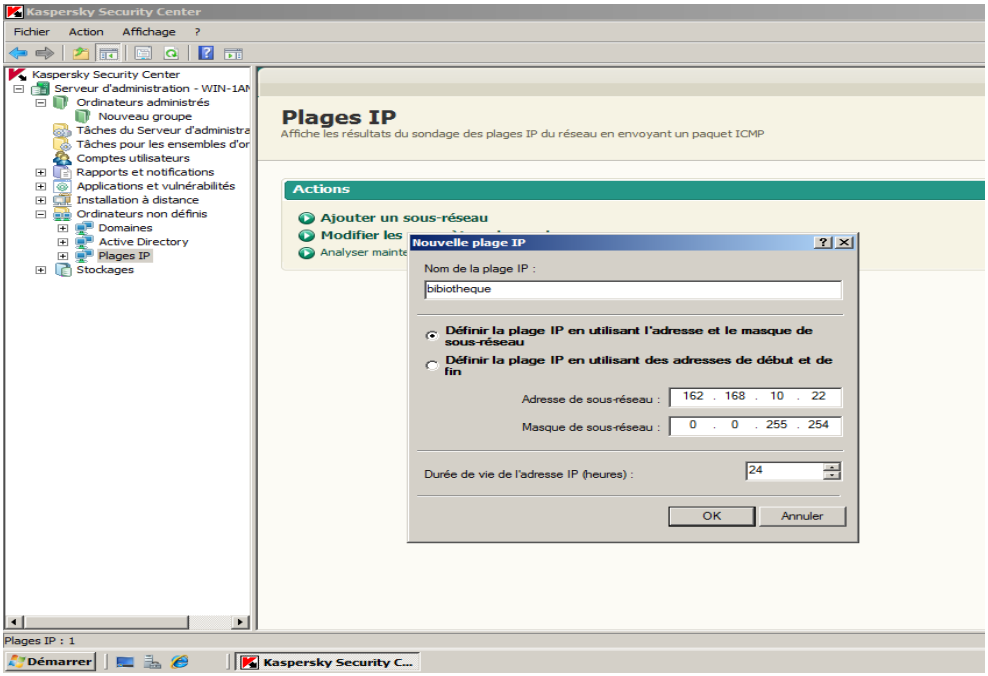
- Kaspersky Endpoint Security 10 for Windows
- Agent d'administration de Kaspersky Security Center 10
- Mise à jour Endpoint Security

I.2.1. Sélection les ordinateurs :

Vous pouvez sélectionner des groupes ou des ordinateurs individuels en vue de l'installation. Les groupes sont constitués d'ordinateurs administrés. Pour installer les produits sur les ordinateurs non définis ou même inconnus, cliquez sur le bouton plage IP, puis ajouter un sous-réseau pour Insérer les plages IP et nom de plage IP de réseau de rectorat.

La plage d'adresse du réseau rectorat est défini par:

- 10.21.0.0 /24
- 10.22.0.0 /24
- 10.29.0.0 /24



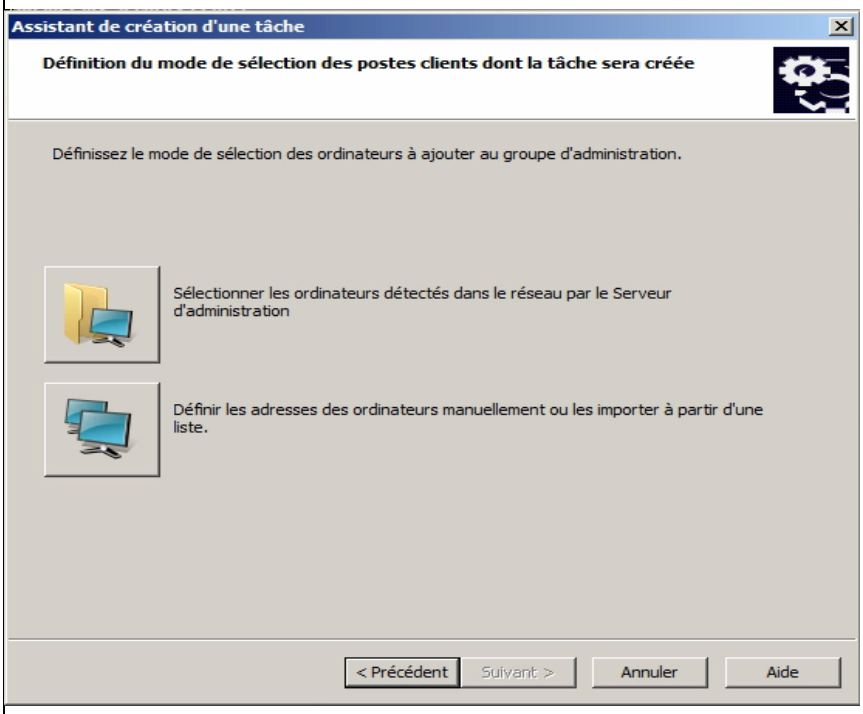
Cliquez sur sélectionner les ordinateur à installer. Ensuite, vous pouvez sélectionner les ordinateurs détectés par le Serveur d'administration, soit spécifies les adresses des

ordinateur manuellement. Le Serveur d'administration tentera d'effectuer l'installation sur tous les ordinateurs spécifiés.

I.2.2. Méthode d'installation

L'assistant essais toujours d'installer les produit en utilisant l'Agent d'administration que n'est pas encore installé sur l'ordinateur, il tente d'effectuer l'installation au moyen des outils Windows. La présente section décrit chaque méthode d'installation.

Si Kaspersky Endpoint Security et l'Agent d'administration doivent être installés sur l'ordinateur, L'assistant installe l'Agent d'administration en moyen des outils Windows, puis installe KES 10 en utilisant l'Agent d'administration.

Sélectionné les ordinateurs	
	- Le bouton supérieur permet la sélection des ordinateurs ajoutés à un groupe. - Une tâche de groupe sera créée en conséquence. - Le bouton du bas permet de sélectionner les ordinateurs non définis ou des ordinateurs distincts issus différents groupes. - Une tâche pour sélections d'ordinateur sera créée en conséquence.

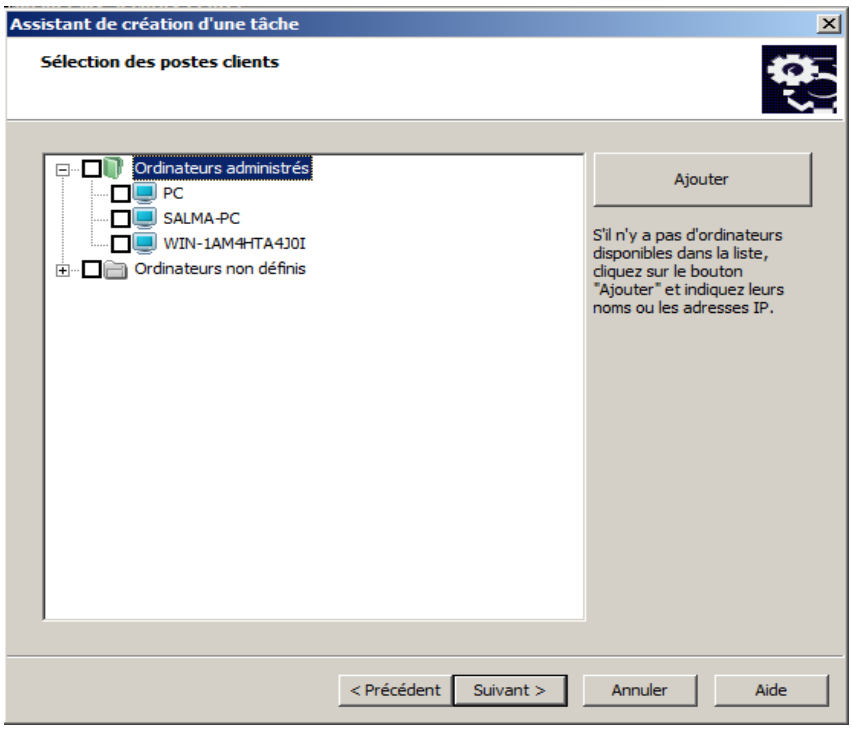


Figure III.4. *Sélection les ordinateurs*

-les ordinateur sont détectes automatiquement au démarrage du serveur.

-Les ordinateurs non définis sont structurés par domaine et par groupes de travail

-Vous pouvez ajouter des ordinateur non détectés par nom ou par adresse IP

Méthode d'installation

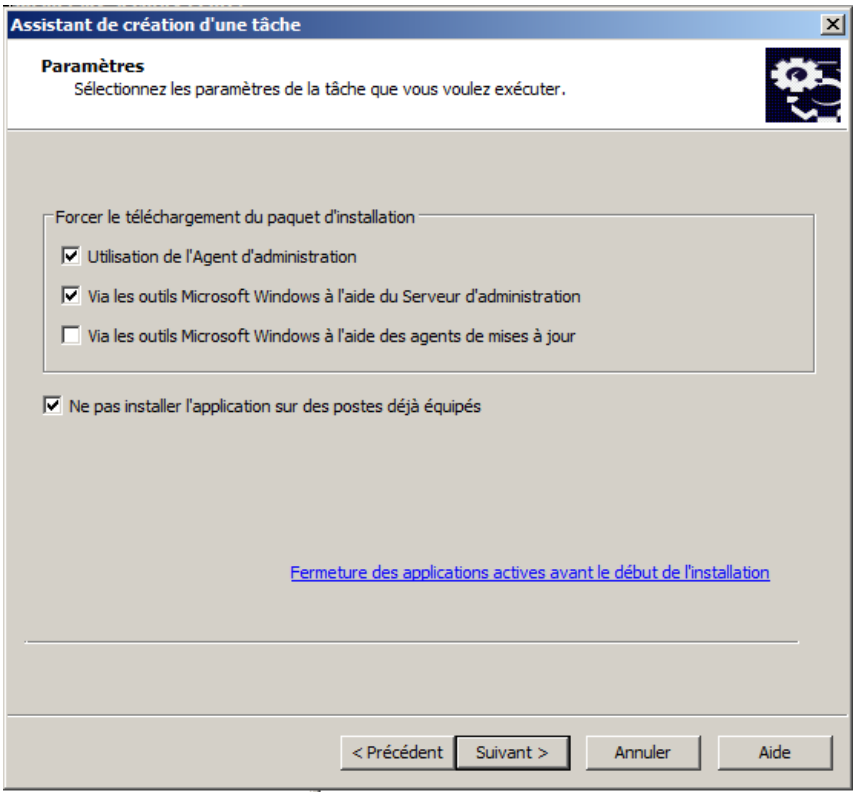


Figure III.5. *Méthode d'installation*

-méthode d'installation par défaut : au moyen de l'Agent d'administration.

-l'Agent d'administration n'est pas encore installé, au moyen des outils Windows.

I.2.3. Supervision du processus d'installation

- L'assistant d'installation utilise les paramètres spécifies par l'administration pour créer et démarrer immédiatement la tâche d'installation du produit sur les ordinateurs sélectionnés. Ensuite, il ouvre automatiquement la page de tâche de la Console d'administration.

- La page de tâches affiche la progression, de la tâche sur l'ordinateur sélectionné. Une installation peut être prête à l'exécution, en cours d'exécution, en attente de redémarrage, achevée avec succès ou renvoyer une erreur. Le nombre d'ordinateur est affiché pour chaque état sur le graphique sectoriel et dans le tableau.

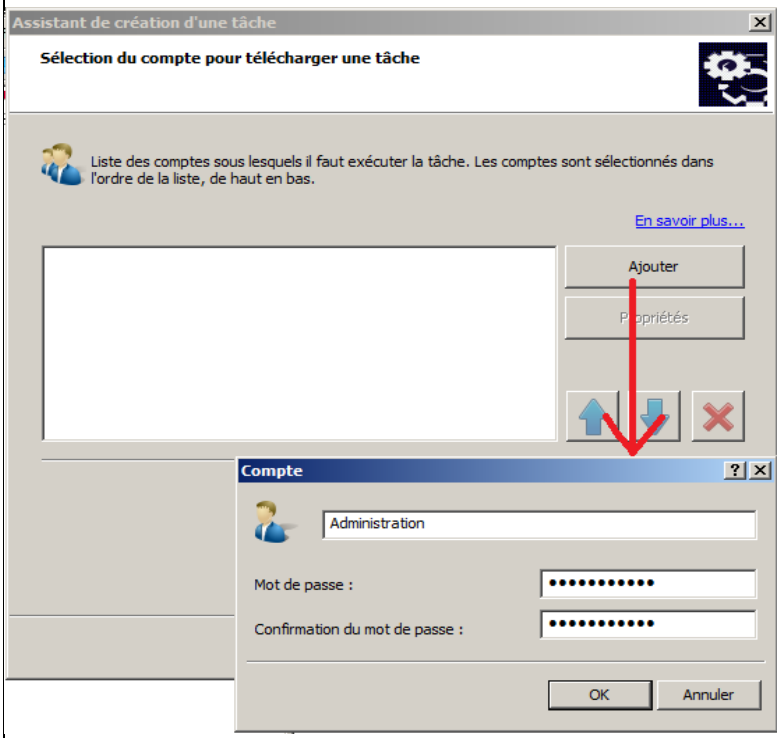
Sélectionne un compte	
	- ajoutez un compte disposant des droits d'administration sur les ordinateurs sélectionnes. - Plusieurs comptes peuvent être ajoutes - Par défaut, la liste est vide. Le compte du service du serveur d'administration est utilisé. - Le compte système locale et les comptes ne sont d'aucune utilité: ils ne disposent d'aucun droit à distance.

Figure III.6. *Sélectionne un compte*

A travers a ajouter nom et mot de passe utilisateur et démarrer la tâche d'installation de produit

Tâche d'installation

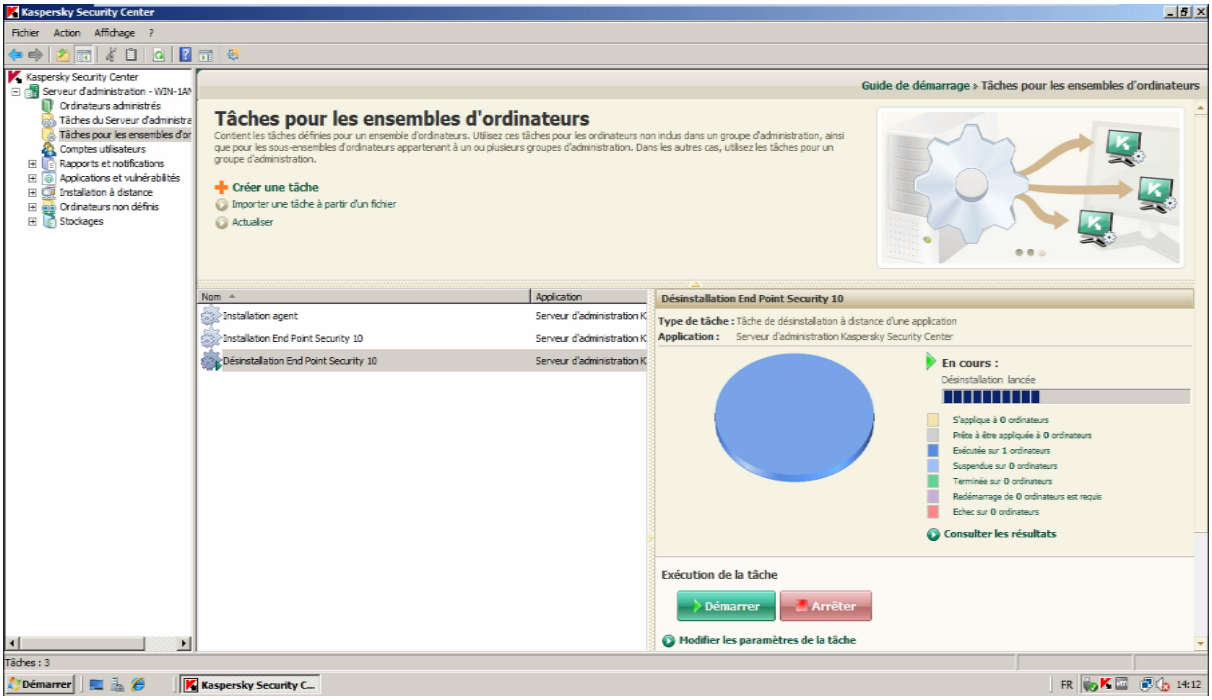


Figure III.7. *Tâche d'installation*

- L'assistant crée et démarre immédiatement la Tâche d'installation à distance.
- Le lien **consulter les résultats** permet de visualise l'état d'avancement de la tâche et les erreurs d'installation.

Après l'installation Kaspersky Endpoint Security et Agent d'administration voici la résulta de l'installation

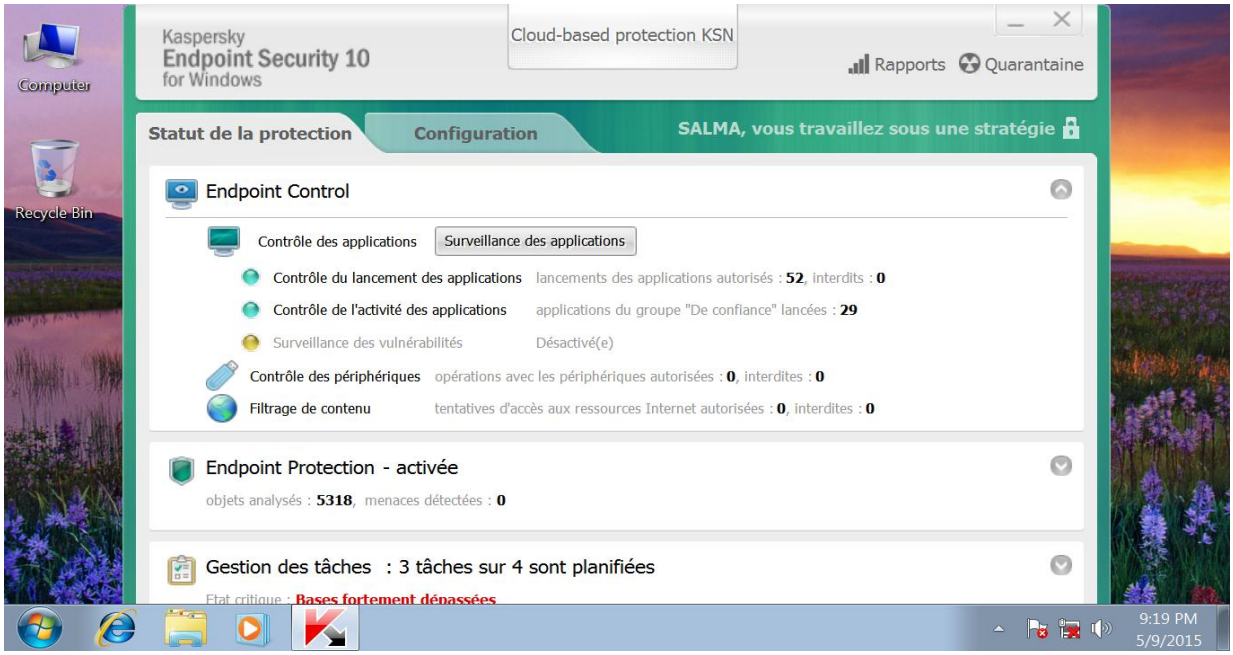


Figure III.8. *Interface Kaspersky Endpoint Security 10*

I.2.4. Télécharger la mise à jour

Les mises à jour centralisées dans KSC10 et KES10 reposent sur deux tâches. L'une d'entre elles télécharge les mises à jour dans référentiel, et l'autre les distribue aux terminaux :

- Téléchargement des mises à jour dans le stockage : est une tâche du Serveur d'administration de Kaspersky Security Center. Une seule tâche de ce type peut être configurée sur le Serveur.
- Téléchargement des mises à jour : est une tâche de Kaspersky Endpoint Security. Il peut exister un nombre quelconque de tâche de ce type, mais généralement, une ou deux seulement sont configurées pour chaque groupe.

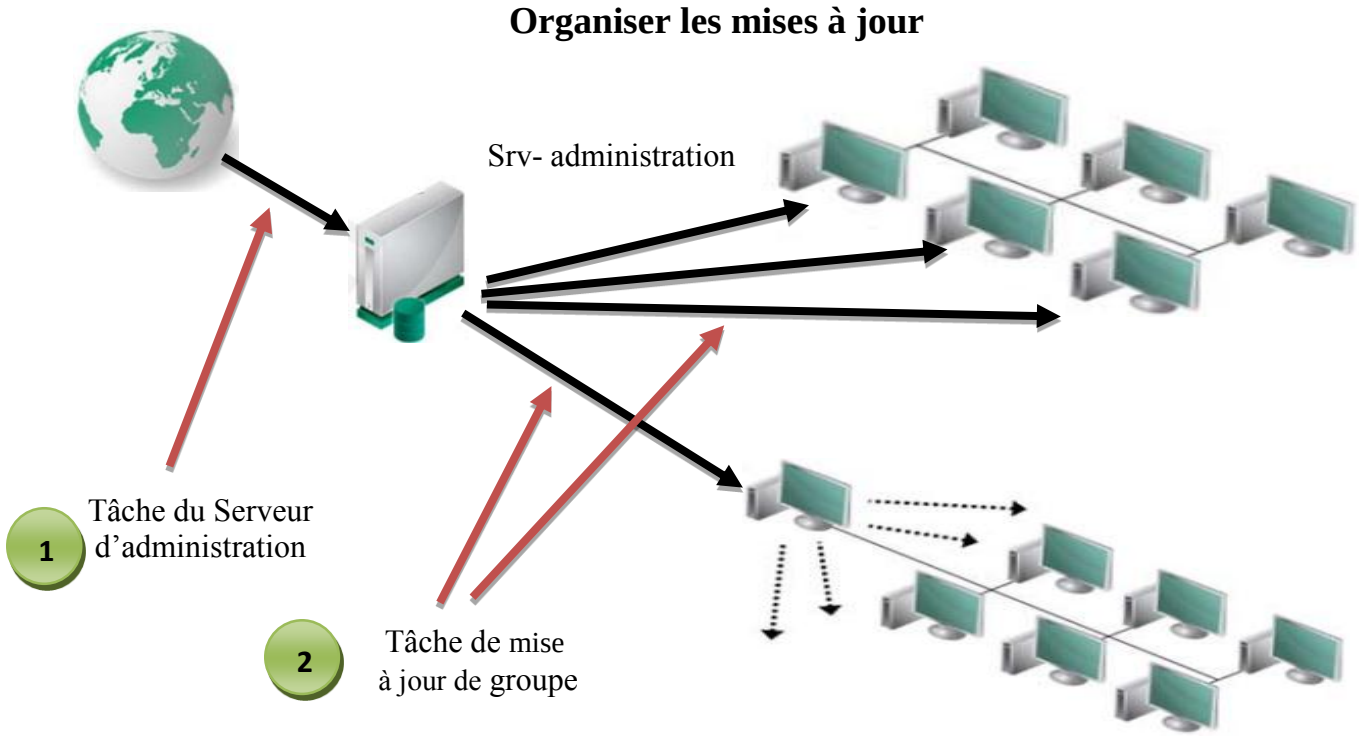


Figure III.9. *Organiser les mises à jour*

I.2.4.a. la mise à jour du Serveur

La tâche la mise à jour du serveur d'administration est nommée d'après avoir choisi le Téléchargement des mises à jour dans le stockage. Elle est créée par l'Assistant de démarrage rapide et se trouve dans la console d'administration.

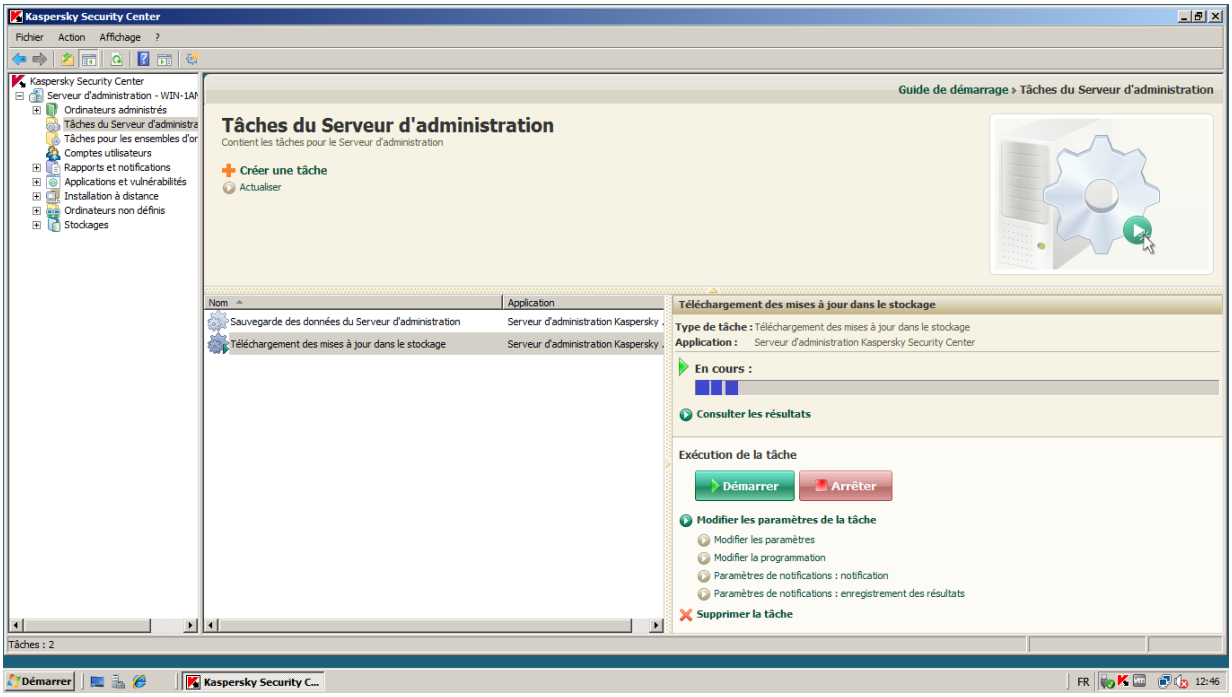


Figure III.10. *Interface mise à jour du Serveur*

I.2.4.b. la mise à jour des groupes (postes client)

Pour assurer le traitement de tous les ordinateurs administrés, une tâche de mise à jour doit être une tâche de groupe on a créée dans le Serveur d'administration. L'Assistant de démarrage rapide crée ce type de tâche : **mise à jour.**

Trois groupes sont organisés chacun selon sa plage et que la procédure de mise à jour optimale est différente d'un groupe à l'autre, on a créé une tâche de mise à jour personnalisée pour chaque groupe.

Tâche de mise à jour du groupe

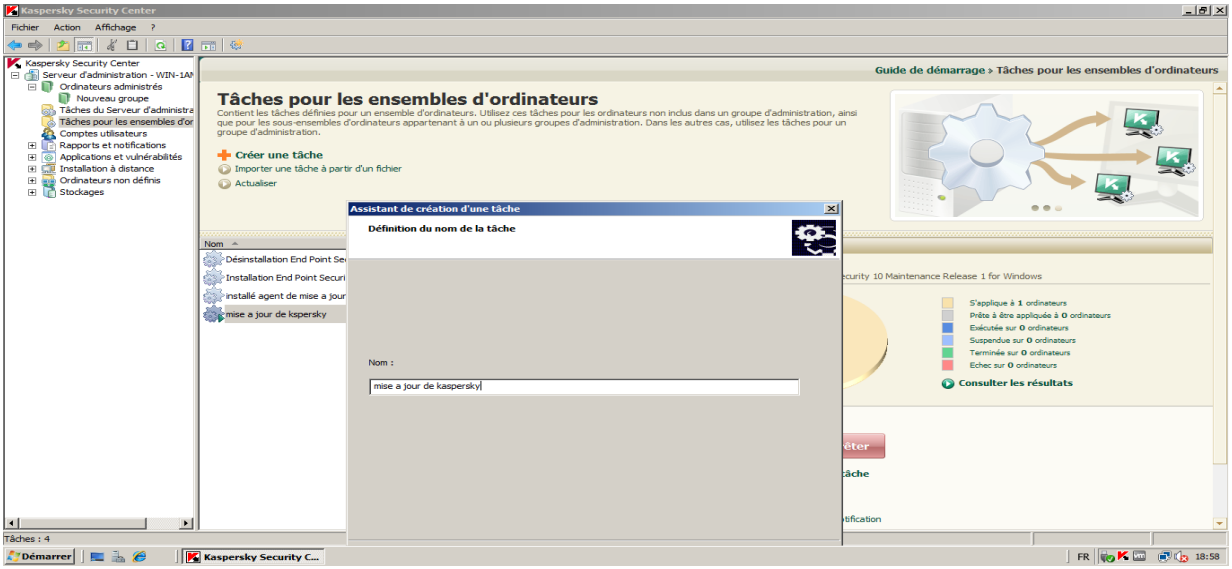


Figure III.11.*création tâche de mise à jour du groupe*

Sélectionner de type de tâche

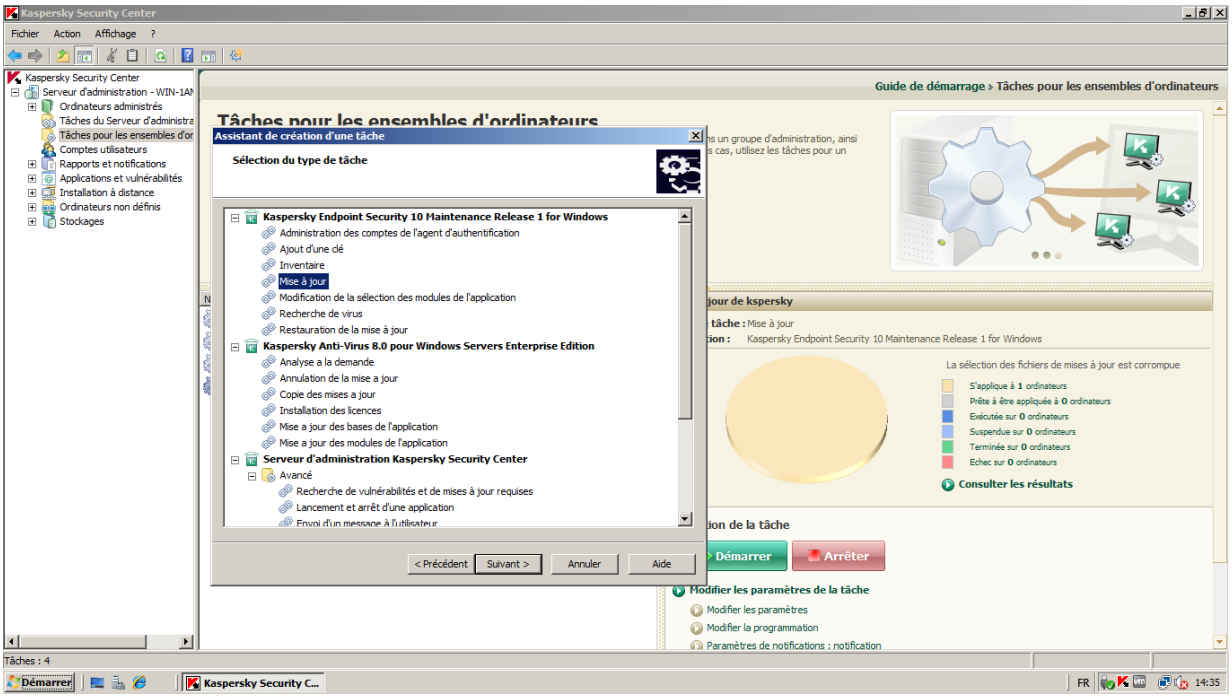


Figure III.12. *Sélectionner la tâche de mise à jour*

Dans cette étape il faut choisir la Source des mises à jour pour télécharger ce paquet.

On a choisi Kaspersky Security Center comme source de téléchargement des mises à jour par ce que ce travail est déjà appliqué dans réseau local.

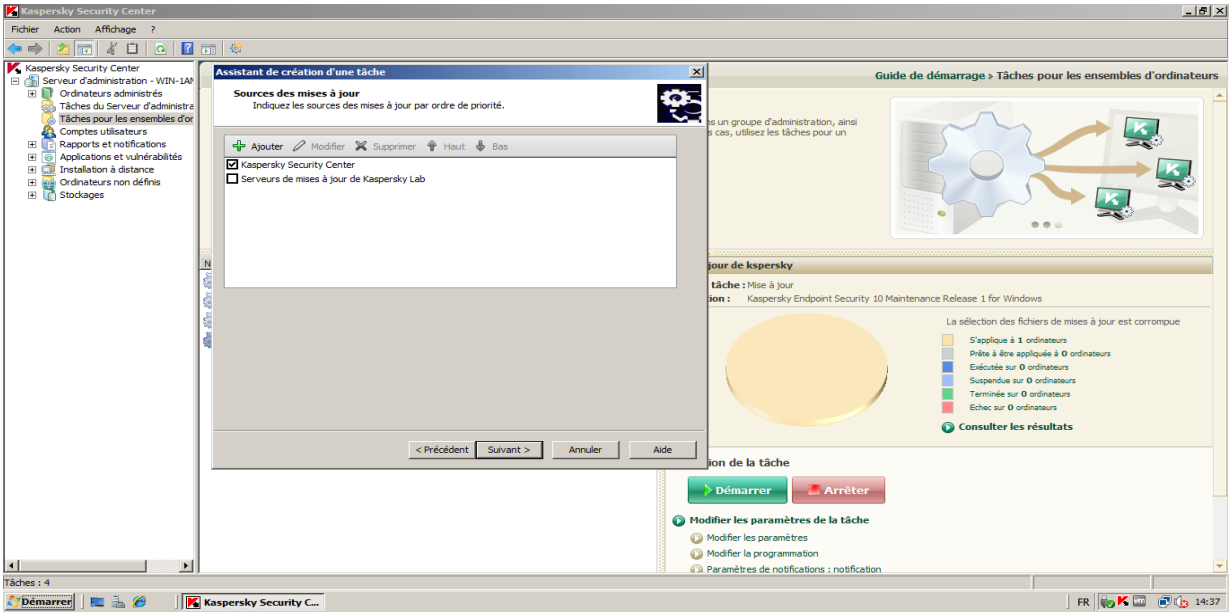


Figure III.13. *Choisir source des mises à jour*

I.2.4.c. Planification de mise à jour

- On a programmé pour l'actualisation des mises à jour pour ce fonctionner chaque jour à 09:00 h
- Par défaut, le Serveur d'administration sélectionne automatiquement l'intervalle de démarrage aléatoire en fonction du nombre d'ordinateur présent dans le groupe.

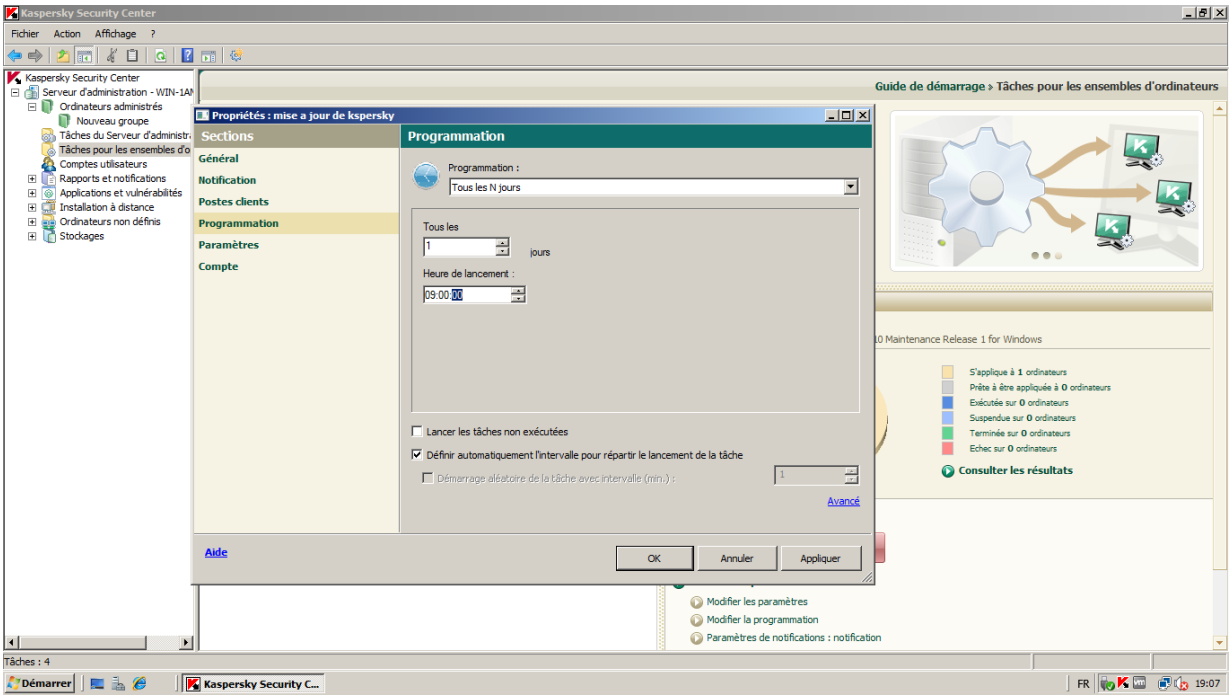
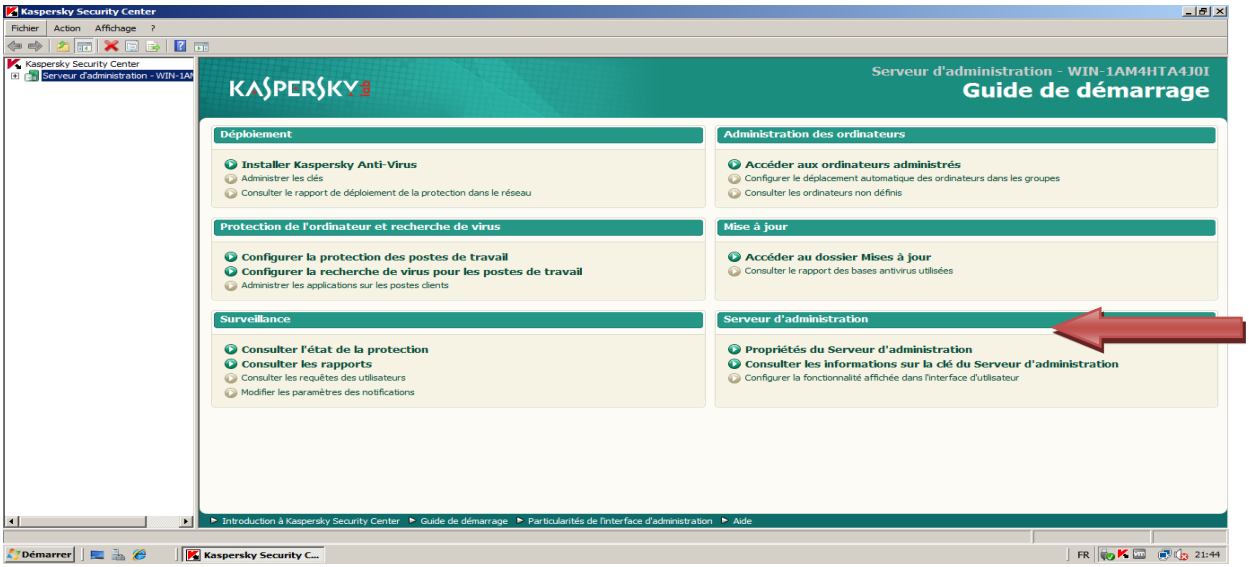


Figure III.14. *Planification de mise à jour*

I.2.4.d.Etat général des mises à jour

L'état général dépend des états des ordinateurs et de la date à laquelle les mises à jour ont été téléchargées pour la dernière fois dans le référentiel.



I.2.5. Méthode de désinstallation

I.2.5.a. Tâche de désinstallation des applications

- Type de Tâche
- désinstaller les applications incompatibles
- sélection des applications à désinstaller
- paramètres de redémarrage
- ordinateurs cibles
- compte
- planification
- création et démarrage

Tâche pour requête d'ordinateurs

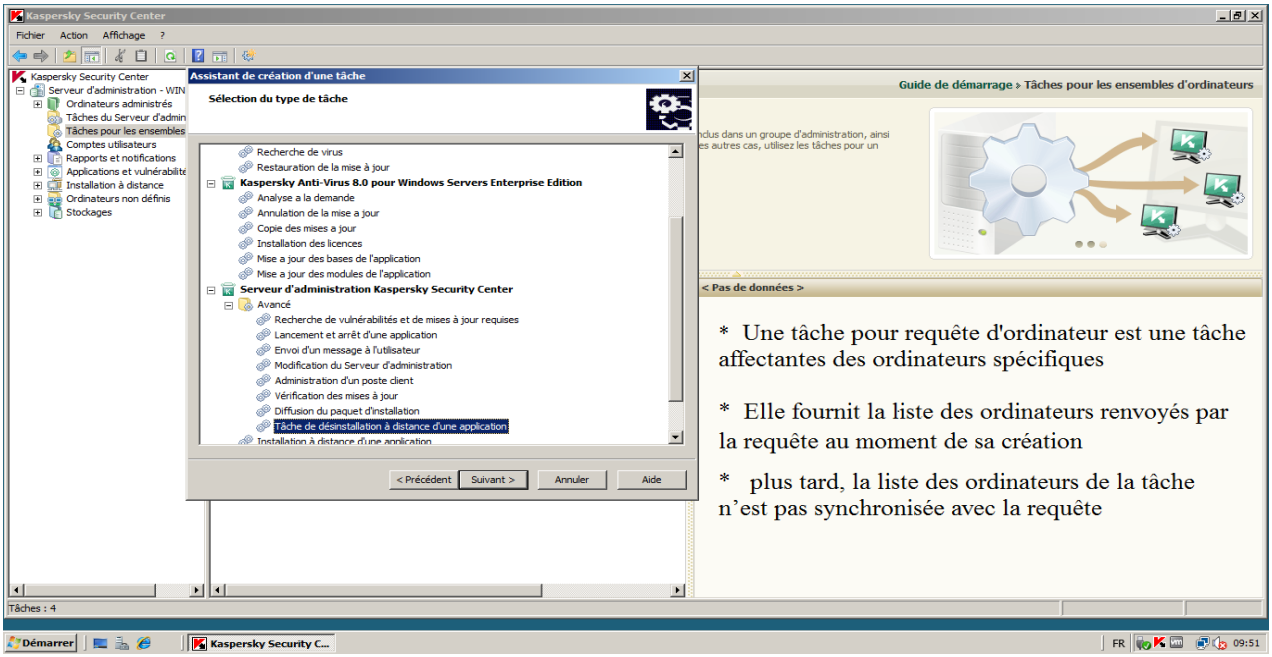


Figure III.15. *Tâche pour requête d'ordinateurs*

Désinstallation d'une application distante

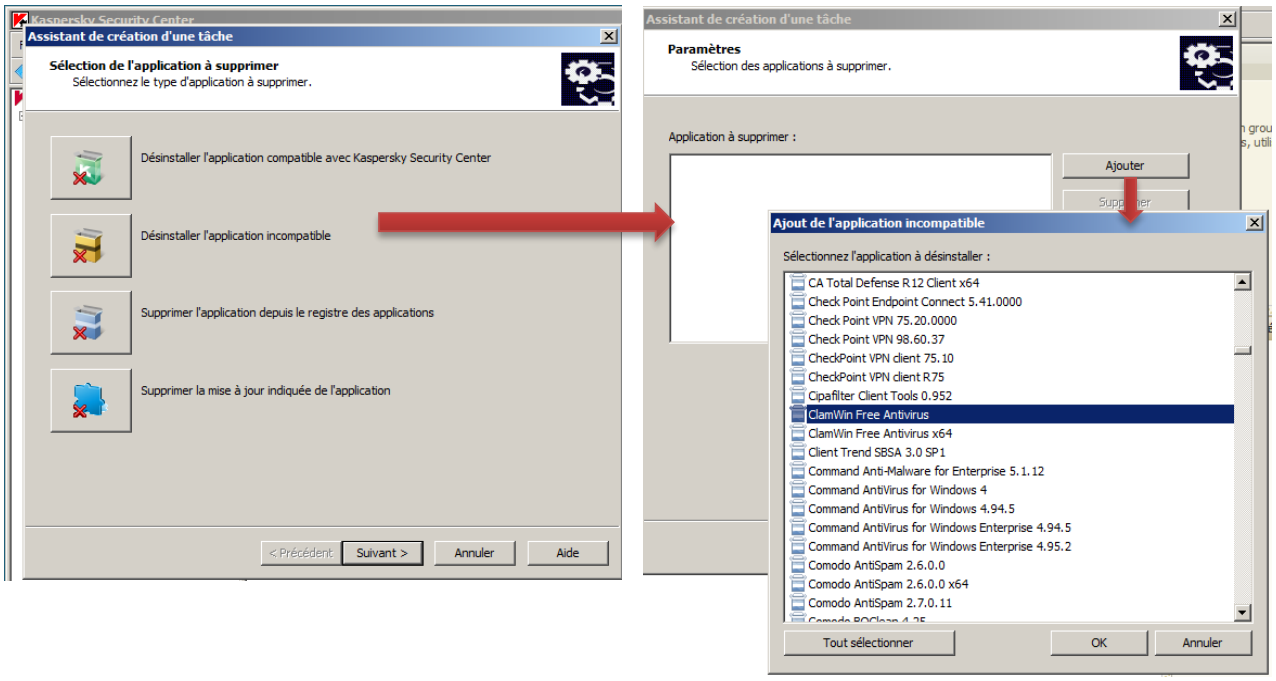


Figure III.16. *Désinstallation d'une application distante*

Tâche de Redémarrage

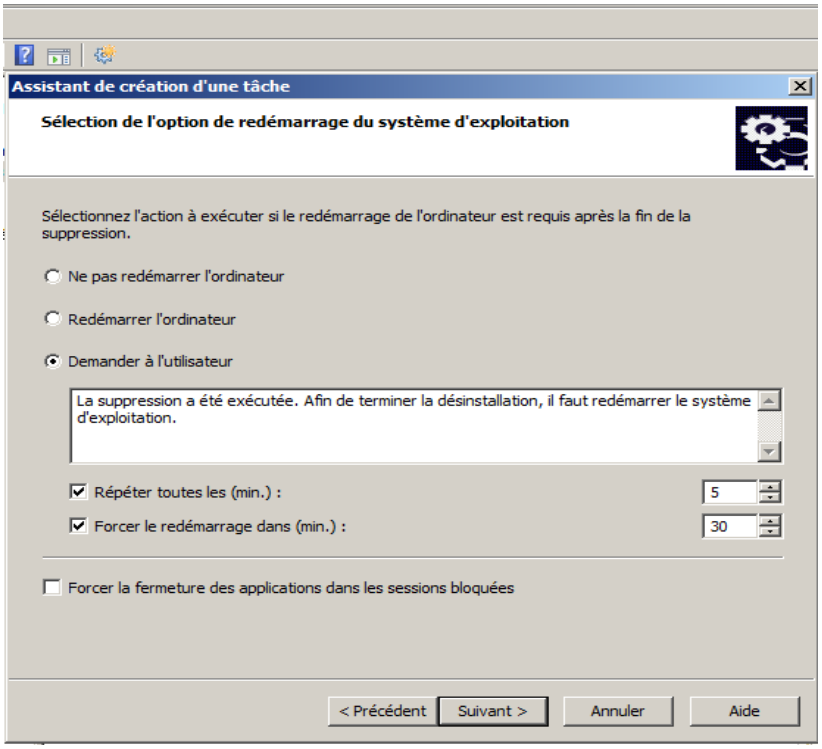


Figure III.17. *Redémarrage*

-A la différence de l'installation, la désinstallation nécessite généralement le redémarrage de l'ordinateur.

-Sue les postes de travail, l'approche optimale consiste à afficher une invite destinée à l'utilisateur.

Sélectionner un Compte

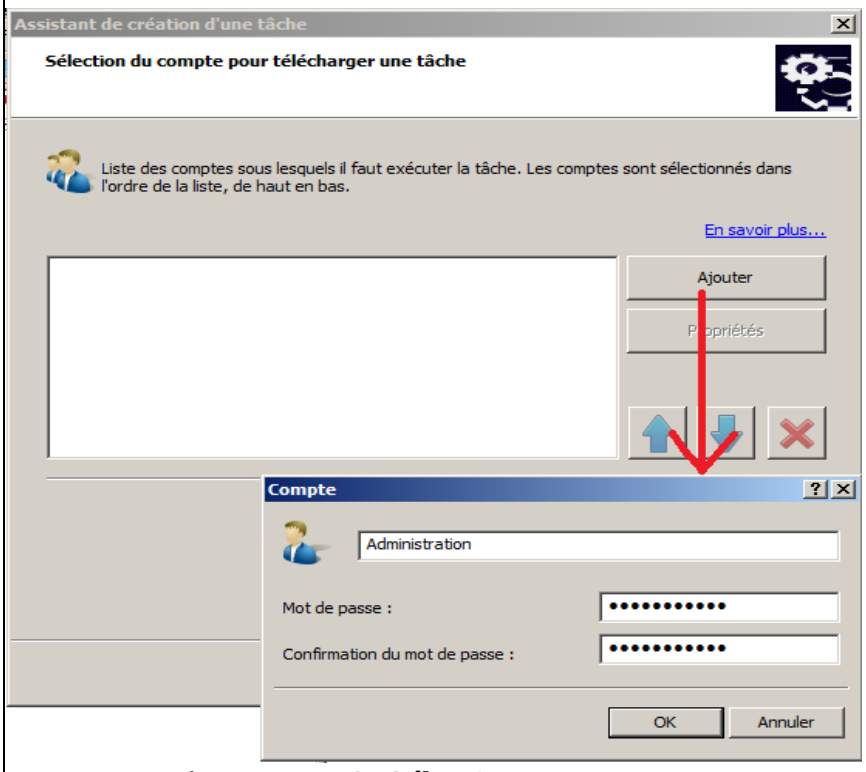


Figure III.18. *Sélectionner un compte*

-La tâche a besoin d'un compte pour la copie des fichiers et la désinstallation, de manière similaire à une distance.

-Si l'Agent d'administration est installé sur les ordinateurs, il n'est pas nécessaire de spécifier le compte.

-L'Agent d'administration généralement installé dans ce cas. Sinon, les informations relatives aux applications incompatibles ne seraient pas disponibles sur le Serveur d'administration.

Tâche désinstallation

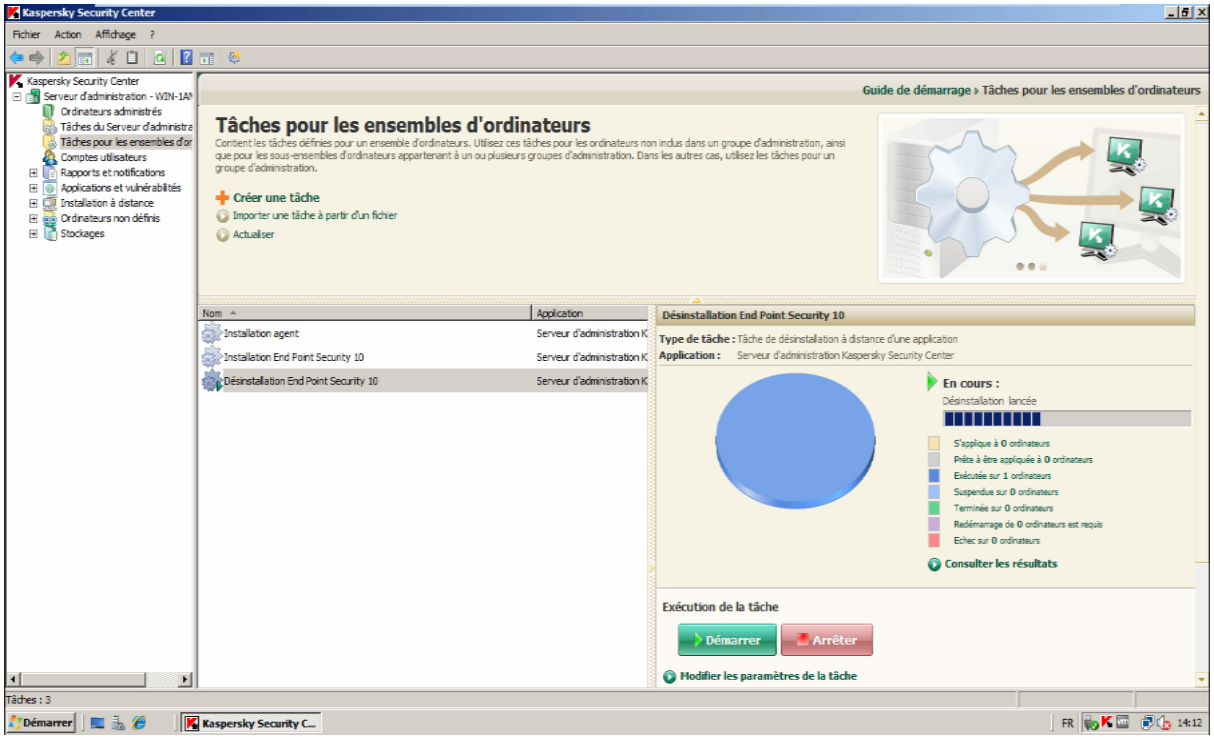


Figure III.19 : *Tâche de désinstallation*

III- conclusion :

Au cours de ce dernier chapitre, nous avons réalisé une application de déploiement d'une solution antivirus a tous les étapes de cette solution ont été réalisées, après avoir réglé le problème des ports utilisés pour connecter les poste clients au serveur.

Nous avons implémenté un système de mise à jour dont le but de sécuriser les PC des utilisateurs.

Les avantages de cette démarche sont :

- essentiellement un gain de temps, la mise à jour est téléchargée une fois sur le serveur et ensuite déployé sur les autres postes.
- Une économie dans la bande de passante, le téléchargement est centralisé au niveau du serveur.

Conclusion générale

Conclusion générale

La défense en profondeur des réseaux passe par une bonne stratégie préventive pour penser ses réseaux et leurs interconnexions de façon sécurisée. Cette approche doit être complétée une fois le réseau en opération pour permettre de détecter des anomalies qui peuvent être révélatrices.

Ce travail nous a permis d'avoir une idée plus claire sur les applications du domaine de la sécurité informatique. Nous avons également découvert Kaspersky Security Center 10 C'est un programme utile pour déploiement de l'application. Cette application qu'on a élaborée est un programme pour mise à jour l'antivirus distant et pour simplifier le processus de sécurité les informations concernant l'université.

L'élaboration de ce travail nous a permis, d'une part, d'approfondir les connaissances et le savoir-faire acquis durant les années de notre formation à l'université Ouargla, et d'autre part, de préparer notre intégration à la vie professionnelle

Le travail que nous avons réalisé pourrait être complété et poursuivi sous différents aspects, notamment :

- Mise en place d'une solution pour La sécurité des ordinateurs par antivirus qui permettent de mettre en place une réponse appropriée à chaque menace.
- Amélioration des mécanismes de sécurité dans le réseau de l'université.

Liste des abréviations

ASA: ***A****daptive* ***S****ecurity* ***A****ppliance*

ADSL : ***A****symmetric* ***D****igital* ***S****ubscriber* ***L****ine*

BDD: ***B****ase* ***D****e* ***D****onnées*

CRC : ***C****ode de* ***R****edondance* ***C****yclique*

DSP : ***D****igital* ***S****ignal* ***P****rocessor*

DNS : ***S****ystème de* ***N****oms de* ***D****omaine*

MMC : ***M****icrosoft* ***M****anagement* ***C****onsole*

KSC : ***K****aspersky* ***S****écurité* ***C****enter*

KEP : ***K****aspersky* ***E****nd-****P****oint*

USB : ***U****niversel* ***S****erial* ***B****us*

Bibliographie

[1] Dominique Mouchené, Sécurité informatique, juin 2005.

[2] DUCROS Magalie, la Sécurité informatique, Soutenu le 25 avril 2002.

[3] Elie MABO, La sécurité des systèmes informatiques (Théorie), support de cours, 2010.

[4] Guillaume CHARPENTIER, Olivier MONTIGNY, Mathieu ROUSSEAU, Virus et Antivirus, Janvier 2004.

[5] La sécurité des réseaux, support de cours, Mercredi, 8. novembre 2006.

[6] Laurent Poinsot «Introduction à la sécurité informatique», support de cours, Université Paris 13.

[7] Rabehi Sidi Mohamed El Amine, « Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11 », Projet de fin d'étude, Université Abou Bakr Belkaid, Tlemcen-Algérie, 2011.

[8] Simon Edwards, Dennis Technology Labs, 7th October 2013.

Net graphie

[9] Web sécurité : http: //www.commentcamarche.net/.19/03/2015 22:32

[10] Web sécurité : http://lemeilleurantivirus.fr/le-meilleur-antivirus-pour-windows-8/. 28/03/2015

[11] Web sécurité : http://www.info-virus.com/Antivirus.htm 22/03/2015 00:09h

[12] Web sécurité : http://www.vulgarisation-informatique.com/ 23/04/2015 02:49h

[13] Web sécurité : http://www.vulgarisation-informatique.com/fonctionnement-antivirus.php 23/02/2015 13.45h

[14] Web sécurité : http://www.tomsguide.fr/article/comparatif-meilleures-suites-securite-antivirus,2-1554.html .htm 01/02/2015 22:39

[15] Web sécurité : http://www.logitheque.com/articles/comparatif_antivirus_et_les_meilleurs_antivirus_sont_474.htm 01/02/2015 22:26

[16] Web sécurité : https://www.cases.lu/logiciels-malveillants.html 10/02/2015 11:45

Résumé :

Ce travail a pour objectif principal de présenter est la mise en place d'une solution antivirus Kaspersky centralisée, dans le réseau intranet de l'université Kasdi Merbah ouargla. Le déploiement de cette solution permet l'administration, installation, lancement des mises ajour depuis le nœud central. La solution proposée tourne dans un serveur virtuel, avec la technologie de vertualisations Vmware vsphere.

Mots-Clés: vertualisations Vmware, vsphere, Antivirus, Kaspersky.

Abstract:

This work has as main objective to present is the establishment of a centralized antivirus Kaspersky solution in the intranet of the University kasdi merbah ouargla. The deployment of this solution enables the administration, installation, launch set aperture from the central node. The proposed solution runs in a virtual server, with the technology of VMware vSphere vertualisations.

Keywords: Vmware, vsphere, antivirus, Kaspersky.

الملخص:

هذا العمل هدفه الاساسي انشاء حلول مكافحة الفيروسات المركزية في الشبكة لجامعة قاصدي مرباح بورقلة. نشر هذا الحل يساعد عمال الادارة على تركيب وتوزيع تحديثات مكافحة الفيروسات كاسبرسكي المركزية لحل مقترح يكمن في الخادم الاداري.

الكلمات المفتاحية: الخادم الإداري، تحديث، مكافحة الفيروسات، كاسبرسكي.