MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

du Diplôme Master en Electronique

Option: Télécommunication et Réseau

Thème :

Implémentation d'une politique de sécurité pour une infrastructure réseau d'entreprise

Proposé et dirigé par :

Mr. LAHDIR.M

Mr. KIBOUH.M

Présentée par :

M^{elle} . YESGUER Fatima

Année universitaire 2012/2013

Remerciement

Je remercie tout d'abord par excellence sa grandeur ***« le bon Dieu »****, qui m'a donné le courage et la patience tout au long de ma vie.*

Mes premiers remerciements vont à mes chères parents, que Dieu les protège et leurs procure une longue vie.

Mes remerciements s'adressent à mon promoteur ***M^r^ LAHDIR.M*** *avec ses conseils et ses remarques constitutives. Ainsi qu'à mon Co-promoteur* ***M^r^ KIBOUH.M*** *qui a veillé sur le bon déroulement de ce travail.*

Sans oublies le personnel d'Institut International Des Nouvelles Technologies qui ont été à la hauteur de leurs nobles tâches et leurs accueil chaleureux tous au long de ce projet ainsi que leurs esprits d'ouverture et leurs disponibilités.

Tous mes infinis remerciements vont à tous les enseignants qui ont collaboré à notre formation , pour le riche savoir qu'ils nous ont transmis avec rigueur et dévouement .

Mes sincères sentiments vont à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce projet. En particulier ma chère famille et amis.

Mes respect aux membres de jury, qui me feront l'honneur d'accepter et de juger ce modeste travail, et d'apporter leurs réflexions et leurs critiques scientifiques.

Dédicace

Ce présent travail est un résultat de grands sacrifices, de recherche de planification, de fatigue et de patience, et c'est la fin de plusieurs années d'études, de travail et de navettes.

Je dédie ce fruit à ceux qui m'ont aidé et sans leurs soutient ce travail n'aurait jamais vue le jour à :

- ***Allah qui m'a donné le courage et la force et qui m'a toujours orienté vers le bon sens.***
- ***Mes très cher parents a ceux que je ne pourrais jamais rendre assez, que dieu les protèges***
- ***Mes très chers frères Larbi, Fahem, Seddik et chères sœur Lynda et Zahia***
- ***A mon fiancé qui ma soutenue et qui a crue en moi je pourrai jamais te remercier assez***
- ***Mes très chers Amis sans exception;***
- ***Tous le personnel d'Institut International Des Nouvelles Technologies ;***

A toute la promo 2012-2013

A toute la promo 2011-2012

Listes des figures

Chapitre I:Architectecture d'un réseau informatique d'une entreprise

Chapitre II: Etat de l'art sur la sécurité des réseaux informatique

Sommaire

Chapitre II: *Etat de l'art sur la sécurité des réseaux informatique*

Chapitre III : ***Implémentation des solutions***

Résumé

Pour réaliser cet objectif, nous avons organisé notre mémoire en trois chapitres. Le premier chapitre est consacré à étudier de façon simple un exemple d'une architecture réseau existante ,cerner ses maillions faibles et expliquer brièvement la manière dont les pirates exploitent ses faiblesses. Dans le second chapitre, nous avons proposé des solutions adéquates aux exigences de l'entreprise tout en définissant la sécurité des réseaux informatiques et leur utilité dans l'entreprise . Le troisième chapitre est consacré à la mise en œuvre de la politique de sécurité proposée pour mieux protéger notre réseau d'entreprise.

Pour conclure notre travail par une conclusion, ainsi que par des perspectives ouvertes pour l'amélioration de notre travail.

Introduction

Introduction

Un réseau informatique est un maillage de micro-ordinateurs interconnectés dans le but d'assurer le transfert de fichiers, le partage des ressources (imprimantes et données), l'exploitation de la messagerie ou l'exécution et la maintenance des programmes à distance. Quel que soit le type de systèmes informatiques utilisés au sein d'une entreprise, leur interconnexion pour constituer un réseau, est indispensable. Aujourd'hui les entreprises utilisent de plus en plus d'informations, ce qui nécessite une meilleure organisation de ces dernières. L'outil informatique joue donc un rôle primordial sur ce plan. Pour faciliter la transmission de ces données informatisées, les entreprises s'organisent autour d'un réseau, mais il ne se passe plus une semaine sans que l'on apprenne que telle entreprise ou tel institut a essuyé de lourdes pertes financières en raison d'une déficience de la sécurité de son système d'information. Par conséquent, les entreprises ne peuvent plus ignorer ces risques et se croire à l'abri de telles épreuves.

Ces entreprises sont ouvertes sur internet, afin qu'elles puissent publier les informations les concernant et de communiquer plus largement avec les acteurs qui interagissent avec elles. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, de destruction, vol d'informations confidentielles,… etc.

Afin d'assurer la sécurité de ces entreprises, la mise en œuvre d'une politique de sécurité rigoureuse s'impose. Celle-ci doit identifier de manière claire et non-ambiguë les objectifs de sécurité à assurer, ainsi que les règles de sécurité qui régissent la manière dont les ressources sont utilisées pour protéger le système. Afin de répondre a cette exigence de sécurité pour une entreprise, nous proposons dans ce projet d'étudier une architecture réseau d'une entreprise existante, détecter ses failles de sécurité pour proposer et implémenter une politique de sécurité optimale qui permettra d'assurer une meilleure sécurité de ces informations vers l'extérieur.

Pour réaliser cet objectif, nous organisons notre mémoire en trois chapitres. Le premier chapitre est consacré à étudier de façon simple un exemple d'une architecture réseau existante ,cerner ses maillions faibles et expliquer brièvement la manière dont les pirates exploitent ses faiblesses. Dans le second chapitre, nous proposons des solutions adéquates aux

exigences de l'entreprise tout en définissant la sécurité des réseaux informatiques et leur utilité dans l'entreprise . Le troisième chapitre est consacré à la mise en œuvre de la politique de sécurité proposée pour mieux protéger notre réseau d'entreprise.

Nous terminons notre mémoire par une conclusion ainsi que par des perspectives ouvertes pour l'amélioration de notre travail.

CHAPITRE I

Architecture d'un réseau informatique d'une entreprise

I.1 Préambule

Toute entreprise existante d'une certaine taille dispose en général d'un réseau informatique ; même celles qui n'en sont qu'à une idée de projet viable y pense très souvent à une éventuelle mise en œuvre d'un réseau informatique au sein de leur structure. Mais la plus part de ces entreprises ignore l'importance de définir une politique de sécurité avant la mise en place de leur réseau et l'étude suivant on est la prouve.

I.2 Présentation de l'entreprise

L'offre du 2int est centrée sur les systèmes et réseaux, le développement d'applications, les bases de données et les environnements "Open Source". Sans oublier les formations utilisateurs spécifiques autour des Applications bureautiques et de travail collaboratif.

Le groupe 2int a bâtit un savoir-faire et une expérience incomparables, au service de ses clients. Des centaines d'organisations s'appuient sur 2intPartners. On site l'exemple 2snetparners.

La Société 2sntPartners est constituée d'ingénieurs informatiques, forts d'une expérience depuis plus de 9 ans dans le monde du réseau, sécurité informatique, et développement web. Leur expérience les a permis de pouvoir cerner les besoins des entreprises dans le dépannage, l'assistance et la gestion des parcs. 2sntPartners déploie des services de vente, d'installation, de gestion et de maintenance de matériels informatiques et de réseaux, L'offre se complète de logiciels de sécurité et de bureautique, incluant (Antivirus, licences Microsoft, etc...)

I. 2.1 Organigramme de l'entreprise

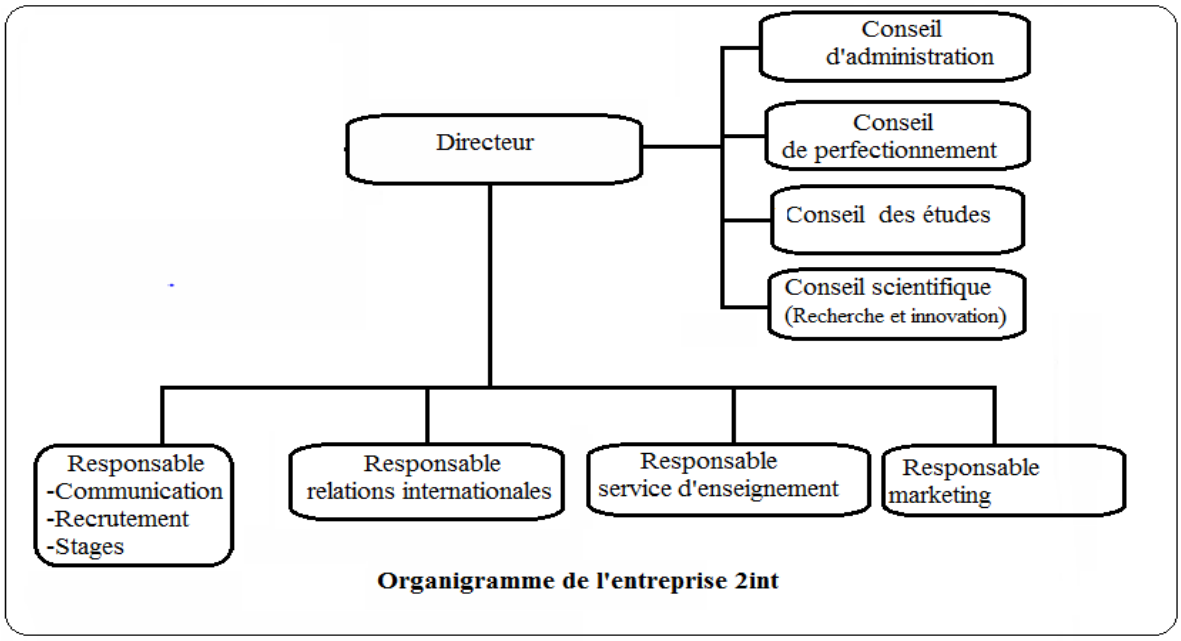


Figure I.1: Organigramme d'entreprise 2int

I.2.2 Organigramme de service d'accueil

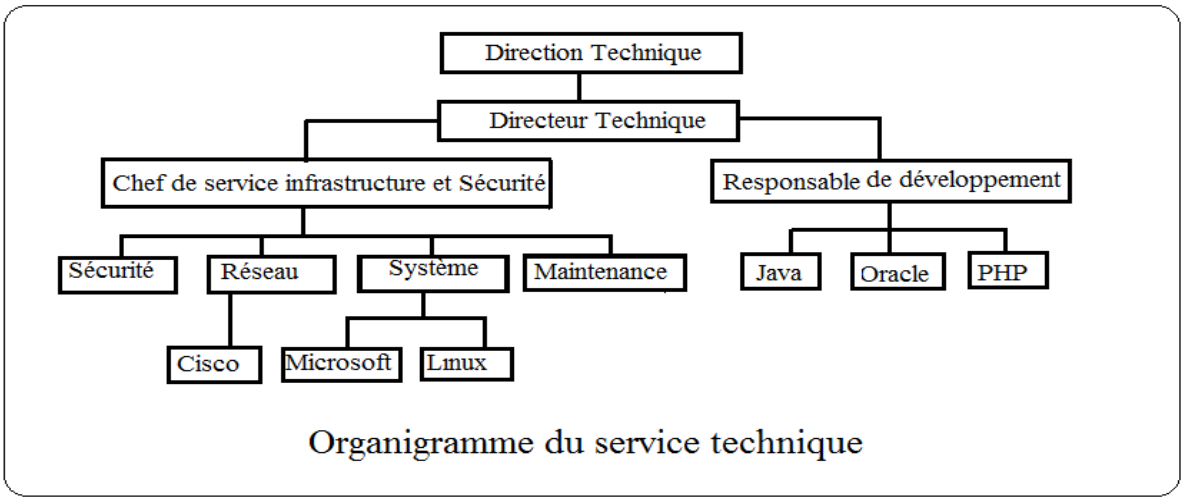


Figure I.2 - Organigramme du service technique

I.3 Architecture informatique de l'entreprise existante

Dans notre démarche, il sera donc question de présenter dans un premier temps une architecture réseau existante à laquelle on apportera des améliorations et on implémentera une sécurité adéquates.

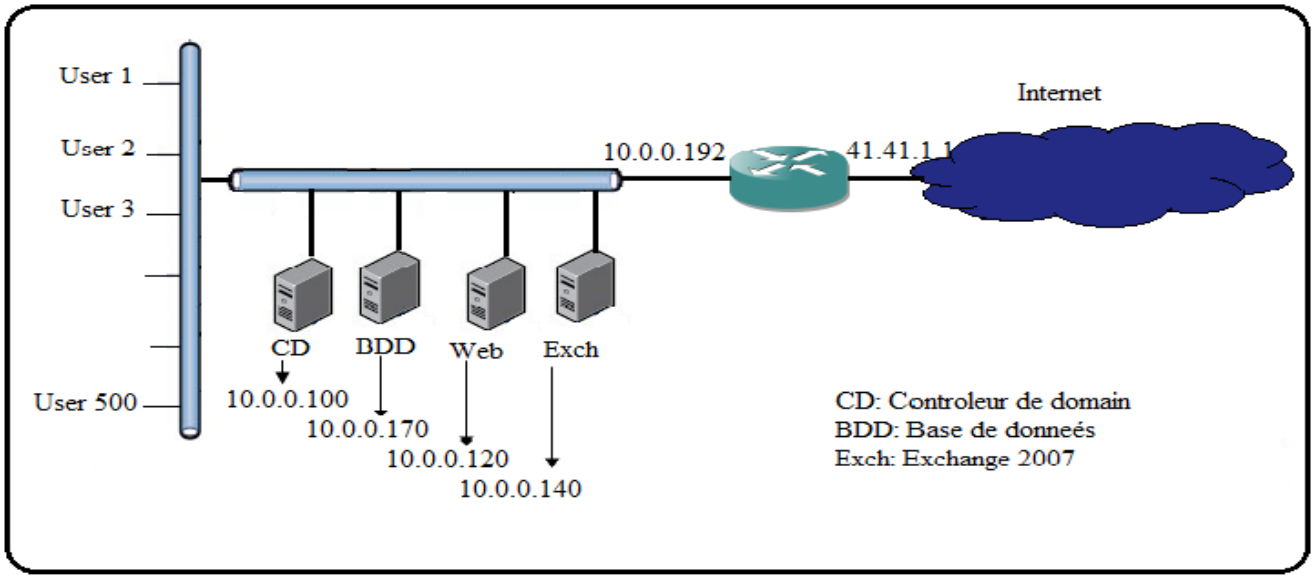


Figure I.3 : Structure existante de l'entreprise

I.3.1 Etude d'existence

Notre architecture est constituée des éléments suivant :

- 500 PC
- Deux routeurs CISCO 3600
- 25 Switch CISCO (2950 et 2960)
- Un DC serveur (Contrôleur de domaine)
- Un server Web
- Un serveur Exchange 2007
- Un serveur base de données

I.3.2 Critique de l'existant

Une analyse du réseau d'une entreprise, nous a permis de définir un nombre de contraintes pouvant réduire ces performances voir même sa dégradation, certains de ces contraintes peuvent être un obstacle à la réalisation de la mission de cette entreprise

a. Mots de Passe Faibles

Les routeurs son protégés par des mots de passe faibles comme « cisco » et « rtgs ». Les intrus auront ainsi des diverses options qui leur permettront de causer des dommages et

d’interrompre les activités métier. Cette vulnérabilité existe à cause du manque de lignes directrices de sécurité de mot de passe, et la mauvaise appréciation des conséquences de l’utilisation de mots de passe faibles.

b. Diverses vulnérabilités exploitables à distance

Des diverses vulnérabilités exploitables à distance existent à cause de la complexité de l’application, la sous-estimation de la mise en œuvre des correctifs, et le manque d’une stratégie de gestion de correctifs au niveau de l’entreprise. Ces vulnérabilités peuvent permettre aux intrus d’avoir un accès administratif non autorisé aux systèmes. Des vulnérabilités exploitables à distance ont été identifiées dans tous les systèmes Windows dans les sites cette entreprise

c. Le manque d’une bonne politique de mot de passe

Il n'y a aucune politique de mot de passe imposée au niveau du domaine est en soi une vulnérabilité car il n'y a aucune manière de garantir un niveau minimum de complexité de mot de passe.

d. Implémentation par défaut et vulnérable de la base de données

Il n’existe pas un mot de passe pour l’utilisateur « User1» d’Oracle dans les serveurs . Ceci peut permettre à un intrus d’avoir un accès à la base de données et de causer un déni de service. Les serveurs d’application Oracle contiennent également plusieurs vulnérabilités exploitables à distance, qui peuvent permettre aux intrus d’avoir un accès administratif non autorisé.

e. Anti-virus McAfee n’est pas totalement configuré

Bien que la direction de systèmes de paiements ait apparemment fortement investi pour obtenir une solution d'Anti-virus de McAfee, l'efficacité de la solution est affaiblie par le fait qu'elle n'est pas totalement configurée ou qu’elle n'est pas étroitement surveillée. McAfee ePolicyOrchestrator n'est pas encore configuré pour informer les administrateurs en cas de production d’un incident relatif à un virus ou d'un problème relatif au logiciel comme l’échec de la mise à jour. Ainsi la console d'Anti-virus n’est pas étroitement surveillée à cause de sa présence dans la salle de serveur et de l’inexistence d’un responsable de sécurité chargé de la surveiller et de la mettre à jour régulièrement.

f. Sauvegardes non chiffrées

Les sauvegardes de la base de données sont actuellement stockées en texte clair sur les bandes de sauvegarde. Ceci peut permettre à un intrus d'obtenir des informations confidentielles s'il réussit à accéder aux bandes de sauvegarde.

g. Ports ouverts et services démarrés

Beaucoup de ports ouverts sur les serveurs, qui sont probablement relatifs à des services inutiles. Le fait d'avoir des services inutiles démarrés augmente les points d'entrée au réseau qui peuvent être utilisés par les intrus. Ceci rend aussi la gestion de la sécurité de ces serveurs plus difficile puisque tous ces services doivent être régulièrement mis à jour et leur configuration doit être périodiquement revue.

h. Activités d'administrateurs non surveillées

Les administrateurs ont le privilège d'arrêter la journalisation, supprimer des événements du journal du système ou même supprimer le journal. L'installation actuelle rend pratiquement impossible de détecter la falsification des journaux système ou toutes autres activités non autorisées d'administrateur.

i. Aucune planification de sauvegarde NTDS

Aucune sauvegarde n'est planifier dans l'entreprise se qui constitue un grand danger pour cette dernier, de le cas de pannes ou d'une catastrophe Natural, toutes les données et les enregistrement de l'entreprise serons perdues

Un seul contrôleur de domaine partage le trafic réseau pour la gestion de demain active directory et les tolérances au pannes .

j. Absence de délégation des personnes qui fait le help desk (les techniciens de maintenance de Park informatique

k. Aucune sécurité de la base de données DNS

l. Aucune mise à niveau business , si en augmente le niveau de sécurité , les ressources matériel diminue, le cout des ces dernière augmente. assurer un équilibrage entre ces trois paramètres est très important

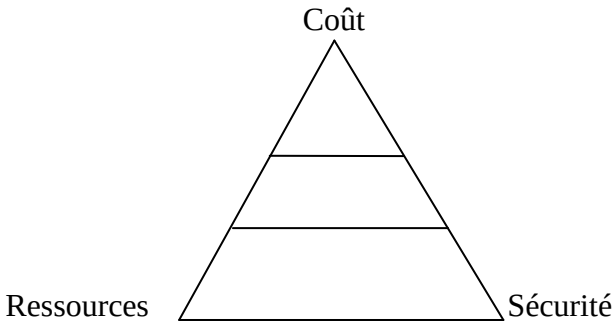


Figure I.4: La pyramide d'exigence de conception logiciels

m. Absences des formations et sensibilisations des utilisateurs

n. Stations non verrouillées

Les postes de travail utilisés pour administrer les systèmes, et même les postes de travail appartenant au service bure

au ne sont pas verrouillés quand ils ne sont pas utilisés. Ceci peut permettre aux intrus d'avoir un accès non autorisé aux privilèges administratifs attribués à ces postes de travail.

o. Redondance de serveur Web

Il existe un seul serveur web qui assure le service dans toute l'entreprise ce qui implique l'augmentation du trafic réseau et engendre la saturation de ce serveur (absence de tolérance aux pannes et manque de sécurité dans l'entreprise)

I.4 Les pirates

Le terme de pirate englobe toutes les personnes qui enfreignent les lois de l'informatique. Ces lois sont établies par chaque pays, cela pose un problème car Internet est accessible à tous les habitants de la planète et certains actes sont des infractions pour les uns mais pas obligatoirement pour les autres. On observe quatre types de hacker :

a. Black Hats (les chapeaux Noires)

Cette catégorie de hackers a en générale, un niveau de connaissance et de créativité relativement élevé. Les hackers aiment étudier et exploiter les failles de tous types de système : base de données, serveur applicatif, serveur web…

b. White Hats (les chapeaux blancs)

Techniquement, l'action menée par les white hats est très proche de celle des black hats. Cependant, elle se différencie par le but ou la finalité.

En effet, les « white hackers » ont plutôt comme ambition d'aider à la sécurisation du système, sans en tirer profit de manière illicite.

Les whites hats ont pour but de découvrir les vulnérabilités du système pas encore connues ou non publiques, en utilisant les mêmes techniques employées par les hackers au chapeau noir.

c. Suicide Hackers (Un Script kiddie)

Sont des pirates informatiques débutants n'ayant pas les capacités nécessaires à la gestion de la sécurité informatique. Un script est un programme, un ensemble de commandes permettant d'effectuer des opérations plus ou moins complexes. Kiddie vient du mot anglais "kid", qui signifie enfant. Ce mot fait référence au manque de capacité de ces pirates débutants. Ils sont relativement dangereux, car ils peuvent modifier et/ou altérer les fonctionnalités d'un système, grâce à des scripts qu'ils n'ont pas mis au point eux-mêmes et qu'ils ne maîtrisent donc pas forcément.

d. Gray Hats (les chapeaux gris)

Le hacker au chapeau gris est un peu un hybride du chapeau blanc et du chapeau noir. Son intention n'est pas forcément mauvaise mais il commet cependant occasionnellement un délit.

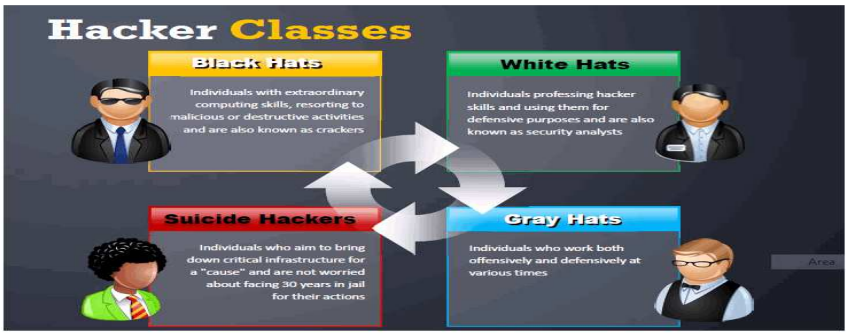


Figure I.4: Les classes de hacker

Remarque : Beaucoup de hackers qui se disent white hats s'apparentent en réalité plus à des grey hats, dans le sens où ils ne révèlent pas toujours leurs découvertes et en profitent à des fins personnelles

I.5 Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini :

- **Les vulnérabilités :** Ce sont les failles de sécurité dans un ou plusieurs systèmes.

Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

- **Les attaques (exploits):** Elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- **Les contre-mesures :** Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).
- **Les menaces :** Ce sont des adversaires capables de monter une attaque exploitant une vulnérabilité.

I.6 Les types de menaces

- **Menaces accidentelles (risques)**

Les menaces accidentelles sont celles qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles sont : défaillance de systèmes, fautes opérationnelles et bogues dans les logiciels.

- **Menaces intentionnelles (attaques)**

Une menace intensionnelle est une action exécutée par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources.
Les menaces intentionnelles peuvent être passives ou actives.

- **Menaces passives** :

  Elles ne modifient pas le comportement du système, et peuvent ainsi passer inaperçues.

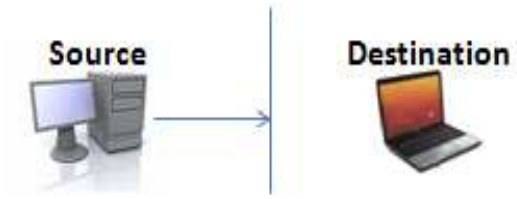
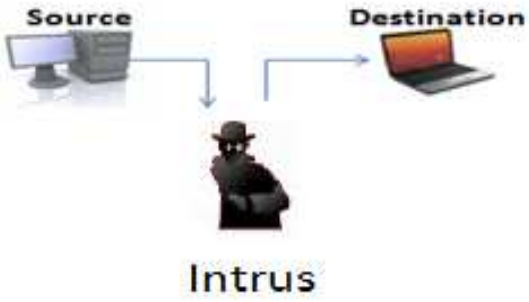
- **Menaces actives**

  Elles modifient le contenu des informations du système ou le comportement du système. Elles sont en général plus critique que les passives.

I.7 C'est quoi une attaque ?

Les menaces viennent d'individus compétents intéressés par l'exploitation des faiblesses de sécurité. Ces menaces sont mises en œuvre à l'aide d'une variété d'outils, de scripts et de programmes permettant de lancer des attaques contre des réseaux et leurs périphériques. En général, les périphériques réseau attaqués sont des points d'extrémité comme les serveurs et les ordinateurs de bureau.

Il existe cinq catégories de menaces : divulgation, interruption, modification, destruction et enlèvement. Elles sont classées en quatre types génériques

Type d'attaque	Schéma correspondant
Interruption : (Attaque sur la disponibilité)	
Interception : (Attaque sur la confidentialité).	
Modification : (Attaque sur l'intégrité)	

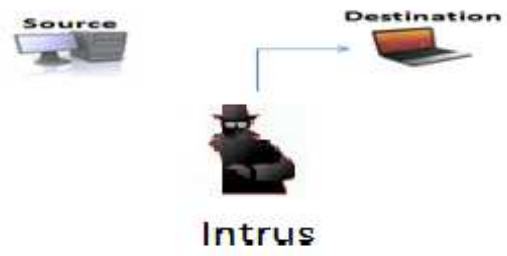
Fabrication : (Attaque sur l'authenticité)	

Tableau I.1 : **Classification des attaques selon le type générique**

Les attaques touchent généralement les trois composantes suivantes d'un système : **La couche réseau**, en charge de connecter le système au réseau, **le système d'exploitation**, en charge d'offrir un noyau de fonction au système, et **la couche applicative**, en charge d'offrir des services spécifiques.

Toutes ces composantes d'un système constituent autant de moyens de pénétration pour des attaques de toute nature. Le schéma suivant présente les *composantes d'un système susceptibles d'être attaquées*:

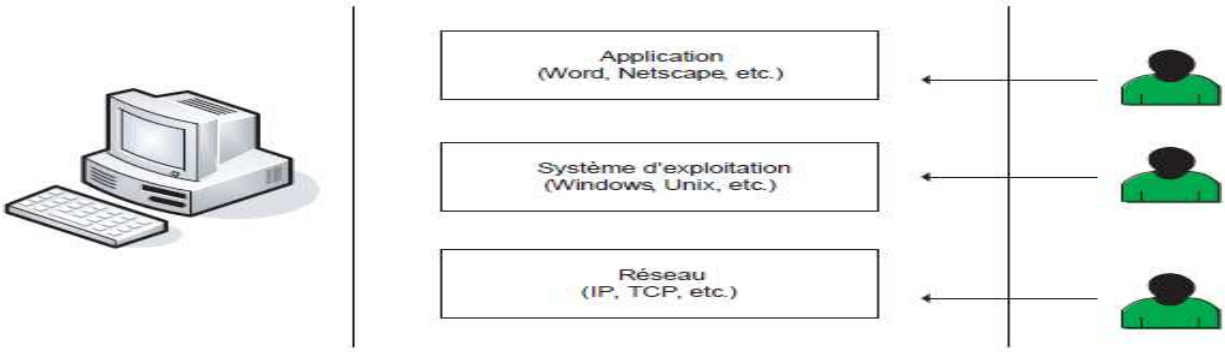


Figure I. 5 : Composantes d'un système susceptibles d'être attaquée

I.7.1 Objectifs des attaques

- Désinformer
- Empêcher l'accès à une ressource
- Prendre le contrôle d'une ressource
- Récupérer de l'information présente sur le système
- Utiliser le système compromis pour rebondir

- Constituer un réseau de « botnet » (ou réseau de machines zombies).

I.7.2 Les techniques d'attaques

Parmi les types d'attaques du réseau on distingue

I.7.2.1 Virus

Un virus informatique est un programme malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les CD/DVD, les clefs USB, etc.

I.7.2.2Ver

Un ver est un programme qui peut se reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique (disque dur, fichier…) pour se propager, donc un ver est un virus réseau. Voici la façon dont le ver se propagerait sur le réseau :

- Il s'introduisait sur une machine
- Il dressait une liste des machines qui lui étaient connectées
- Il forçait les mots de passe à partir d'une liste de mots
- Il se faisait passer pour un utilisateur auprès des autres machines
- Il créait un petit programme sur la machine pour pouvoir se reproduire

I.7.2.3 Rootkit

Un rootkit ("jeu de démarrage" en français) est un programme malveillant dont la principale fonctionnalité est de dissimuler la présence de son activité et celle des autres programmes néfastes aux yeux de l'utilisateur du système et des logiciels de sécurité (antivirus, pare-feu, IDS). Certains rootkit peuvent en plus de cette fonctionnalité principale, installer des backdoors (porte dérobée).

Les rootkits ont deux caractéristiques principales :

- Ils modifient profondément le fonctionnement du système d'exploitation
- Ils se rendent invisibles (difficile à les détecter)

I.7.2.4 Déni de service (DoS)

L'attaque n'obtient pas un accès au système informatique sur le réseau mais il parvient à mettre en panne certains composants stratégiques (le serveur de messagerie, le site web, etc..). Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources. La plus part des attaques par déni de service exploitent des failles liées à l'implémentation d'un protocole du modèle TCP/IP .

On distingue deux types de déni de service :

- ✓ **Déni de service par saturation :**

Il génère un grand volume de trafic en le faisant passer pour un trafic légitime vers une machine choisie par le pirate. Ce trafic sature le réseau et empêche le trafic normal de passer et la machine devient incapable de répondre aux requêtes réelles.

- ✓ **Déni de service par exploitation de vulnérabilité :**

Consiste à exploiter une faille d'un système distant afin de le rendre inutilisable.

Lorsque le déni de service est provoqué par plusieurs machines, on parle alors de déni de service distribuée (DDOS). Les attaques par déni de service distribué les plus connues sont Tribal Flood Network et Trinoo. Le déni de service utilise diverses techniques d'attaque qui sont

a) Ping Of Death

Cette attaque exploite les anciennes implémentations de TCP/IP de certains systèmes d'exploitation ; Le principe de Ping de la mort consiste tout simplement à créer un datagramme IP d'une taille supérieure à la normale (> 65535 O). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage.

Plus aucun système n'est vulnérable à ce type d'attaque.

Figure I.6: Ping of Death

b) Attaque smurf :

L'intrus inonde la victime par un grand nombre de Pings pour le saturer, et la technique la plus utilisée s'exécute en deux phases. Dans la première phase, l'intrus usurpe l'adresse IP de la cible pour l'utiliser comme adresse source. Et dans la deuxième phase, l'intrus envoie un maximum de Pings en diffusion directe à destination d'un réseau contenant un grand nombre d'hôtes. L'adresse source étant transformée en l'adresse de la victime.

Si le routeur d'entrée accepte de faire passer les diffusions directes, tous les hôtes du réseau vont répondre à l'adresse source qui est l'adresse de la victime ce qui implique que la machine victime se bloque et elle devient inutilisable.

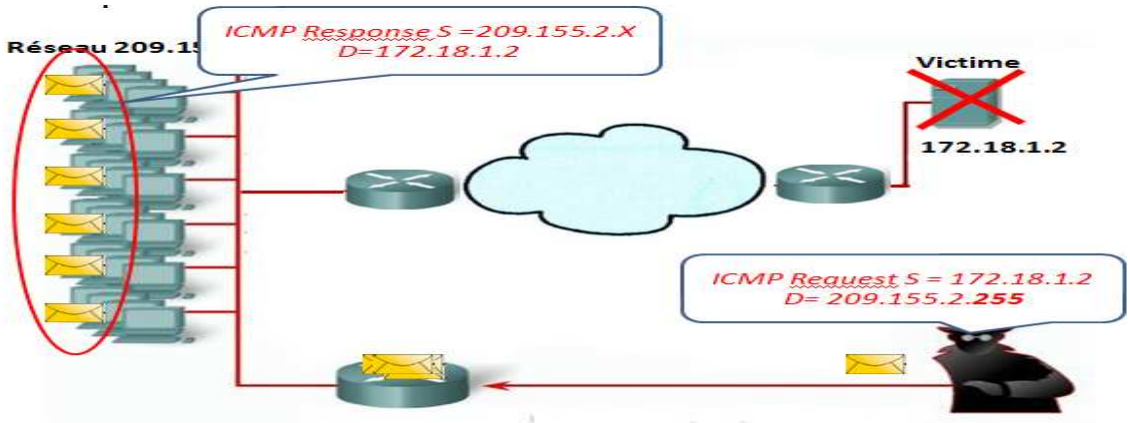


Figure I.7 : attaque smurf

c) TCP SYN Flood

L'intrus inonde la victime par un grand nombre TCP SYN pour lui faire croire qu'une demande de connexion est arrivée. L'intrus utilise une fausse adresse de retour pour ne pas recevoir les réponses de la victime. La victime répond par un paquet SYN ACK et se met en attente d'un paquet ACK de l'intrus, et chaque demande est mise dans une file d'attente en attendant que l'ACK correspondant arrive. Les réponses étant destinées à une fausses adresse, la victime ne recevra jamais de paquet ACK et la file est vite débordée, alors la victime ne pourra plus répondre à une demande légitime de connexion.

Pour bien expliquer le TCP SYN Flood nous utilisons le schéma suivant

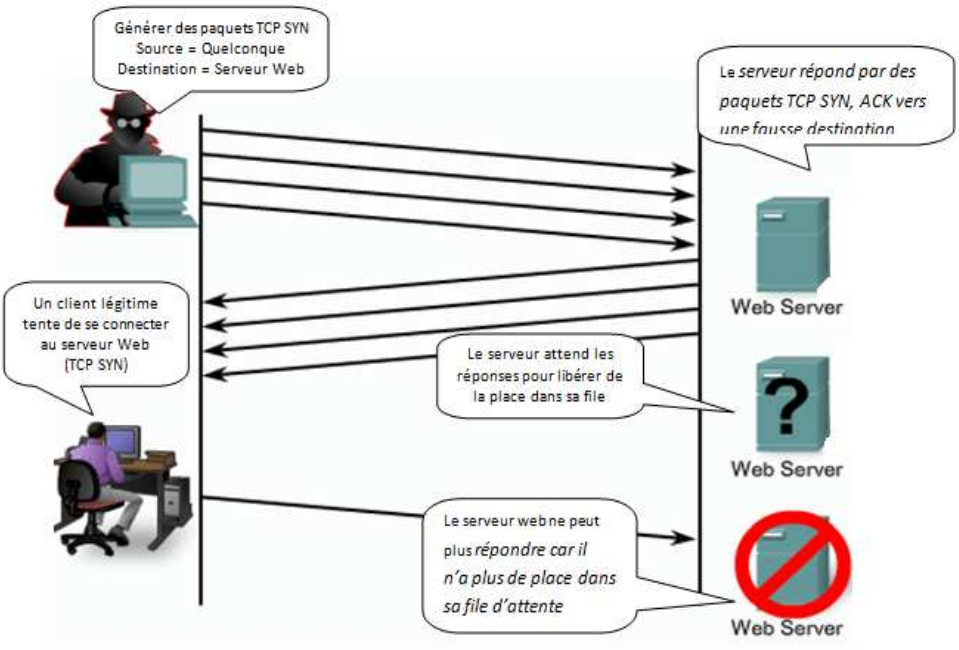


Figure I.8 : Le TCP SYN Flood

a. Ip Spooffing :

Usurpation d'adresse IP, on fait croire que la requête provient d'une machine autorisée.

- Principe : envoyer un paquet avec une fausse adresse IP source
- Il est impossible de trouver la véritable source du paquet
- L'émetteur ne peut pas recevoir ses réponses
- Utilisé dans de nombreuses attaques
  - Dénis de service
  - Pour profiter d'une relation de confiance entre deux machines

Figure I.9 : Usurpation d'adresse IP

d) ARP Spoofing

Cette attaque appelée aussi Arp Redirect, redirige le trafic réseau d'une ou plusieurs machines vers la machine du pirate. Elle s'effectue sur le réseau physique des victimes.

Cette attaque corrompt le cache de la machine victime. Le pirate envoie des paquets ARP réponse (ARP Reply) à la machine cible indiquant que la nouvelle adresse MAC correspondant à adresse IP d'une passerelle (par exemple) est la sienne. La machine de pirate recevra donc tout le trafic à destination de la passerelle, il lui suffira alors d'écouter passivement le trafic (et/ou le modifier). Il routera ensuite les paquets vers la véritable destination telle indiquée dans la figure suivante

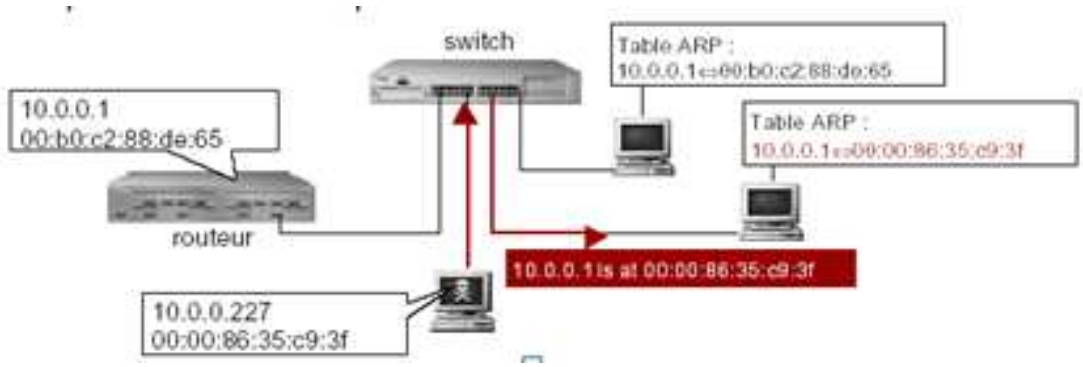


Figure I.10 : ARP Spoofing

e) DNS Spoofing

Le protocole DNS (Domain Name System) a rôle de convertir un nom de domaine (par exemple www.2int.com) en son adresse IP (par exemple 134.38.10.1) et réciproquement, à savoir : convertir une adresse IP en un nom de domaine. Cette attaque consiste à faire parvenir de fausses réponses aux requêtes DNS émises par une victime.

Figure I.11 : DNS Spoofing

I.7.2.5 Les attaques d'accès

Est u ne attaque qui exploite les vulnérabilités de système pour rentrer dans des zones sensible telle que la base de données, les serveurs …Etc. Parmi ces attaques d'accès on trouve :

✓ Attaque de mot de passe :

Cette attaque vise à trouver le mot de passe d'un utilisateur sur un ordinateur ou sur un équipement réseau. Si l'intrus arrive à trouver le mot de passe, il peut accéder à une ressource, ou ouvrir une porte dérobé pour des futurs accès.

Les techniques les plus utilisés sont

a) **Attaques par dictionnaire :** Cette technique consiste à essayer toutes les combinaisons jusqu'à trouver le mot de passe.

b) **Attaque par force brute :**

Dans ce genre d'attaque, le hacker va essayer d'obtenir un mot de passe avec un dictionnaire de mots et de noms propres, et il les essaie un à un pour vérifier si le mot de passe est valide. Ces attaques se font avec des programmes qui peuvent deviner des milliers de mots de passe à la seconde. Avec ce type d'attaques, un tel mot de passe peut être craqué en quelques minutes.

✓ Trust exploitation :

Dans cette attaque, l'intrus utilise les privilèges d'une autre entité de confiance pour pénétrer dans un système sécurisé. Voilà ce que l'attaquant fait pour accomplir son but, d'après la figure suivante :

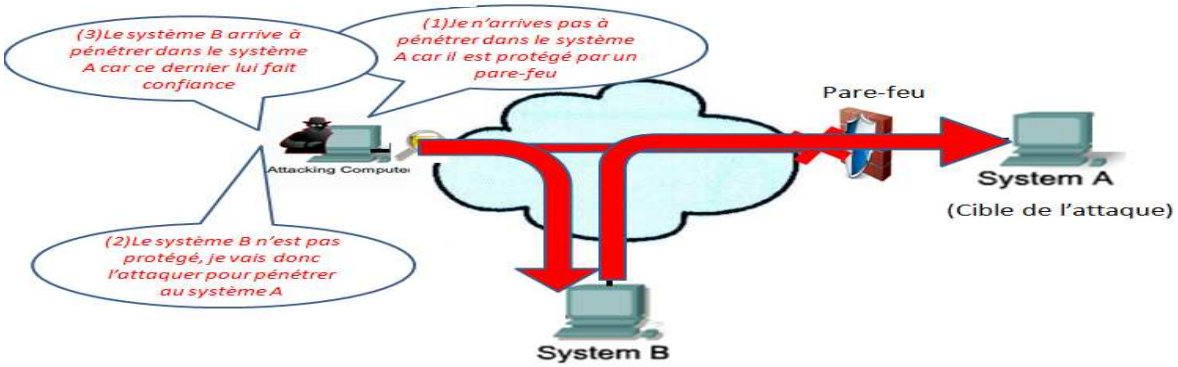


Figure I.12: Trust exploitation

✓ **Port redirection :**

La redirection de port est un type de Trust exploitation qui fait passer un flux sur un port non autorisé par le pare-feu en le faisant passer pour un flux d'un autre port autorisé. La figure ci-dessous illustre beaucoup plus cette attaque.

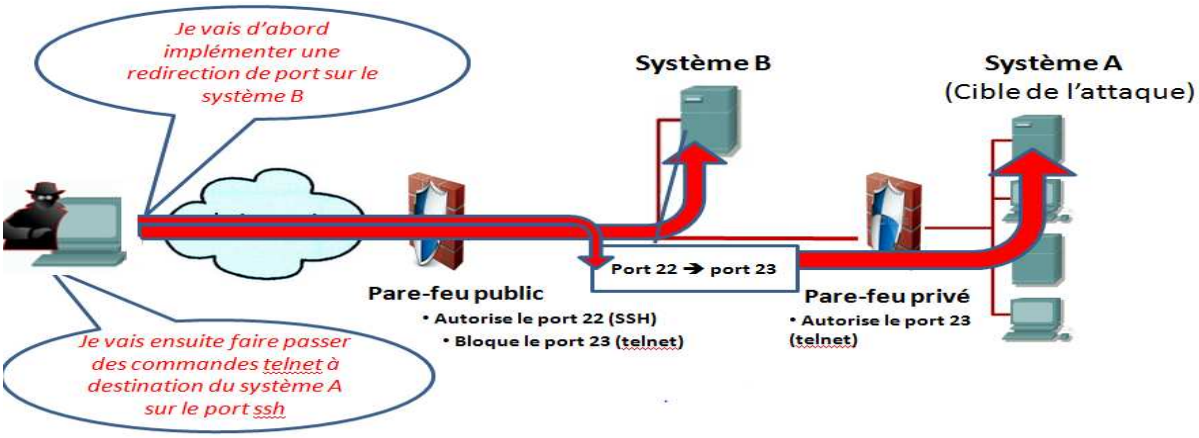


Figure I.13:Port redirection

I.7.2.6 Attaque man in the middle

Ce type d'attaque est nommé aussi par **MITM**, est un scénario d'attaque dans lequel un pirate écoute la communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties. La plupart des attaques man in the middle consiste à écouter le réseau à l'aide d'outils d'écoute de réseau tel que : les services de point d'accès wifi ou de passerelle réseau pour centraliser les communications à son niveau. Donc La victime peut se connecter et utiliser normalement le réseau sans savoir que le flux passe par une tierce personne.

I.7.2.6 Espiogiciels (spyware)

Est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur dans lequel il est installé afin de les envoyer vers la société qui le diffuse pour lui permettre de dresser le profil des internautes. Les récoltes des informations peuvent être les adresses WEB des sites visités, les mots clés saisis dans les moteurs de recherche, des informations personnelles, etc.

I.7.2.7 Les bombes logiques

Elles sont de véritables bombes à retardement. Ce sont de petits programmes restant inactifs tant qu'une condition n'est pas remplie, une fois la condition remplie (une date par exemple), une suite de commandes est exécutée (dont le but, le plus souvent, hélas, est de faire le plus de dégâts possible). 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.

- ✓ **Les attaques par messageries:**

En dehors des nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques à celle-ci :

1) **Le Pourriel (spam en anglais) :**

Le pourriel ou spam en anglais, désigne les communications électroniques massives, notamment de courriers électroniques, non sollicitées par les destinataires, à des publicitaires ou malhonnêtes.

2) **L'Hameçonnage (phishing en anglais) :**

L'hameçonnage est une technique de fraude visant à obtenir des informations confidentielles telles que des mots de passe ou des numéros de carte de crédit au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales.

3) **Le Canular informatique (hoax en anglais) :**

Un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Ils encombrent le réseau, et font perdre du temps à leurs destinataires

I.7.2.8 Enumération

Il définit le processus d'extraction de nom d'utilisateur, nom de machine, ressources réseau, le partage, les services système.

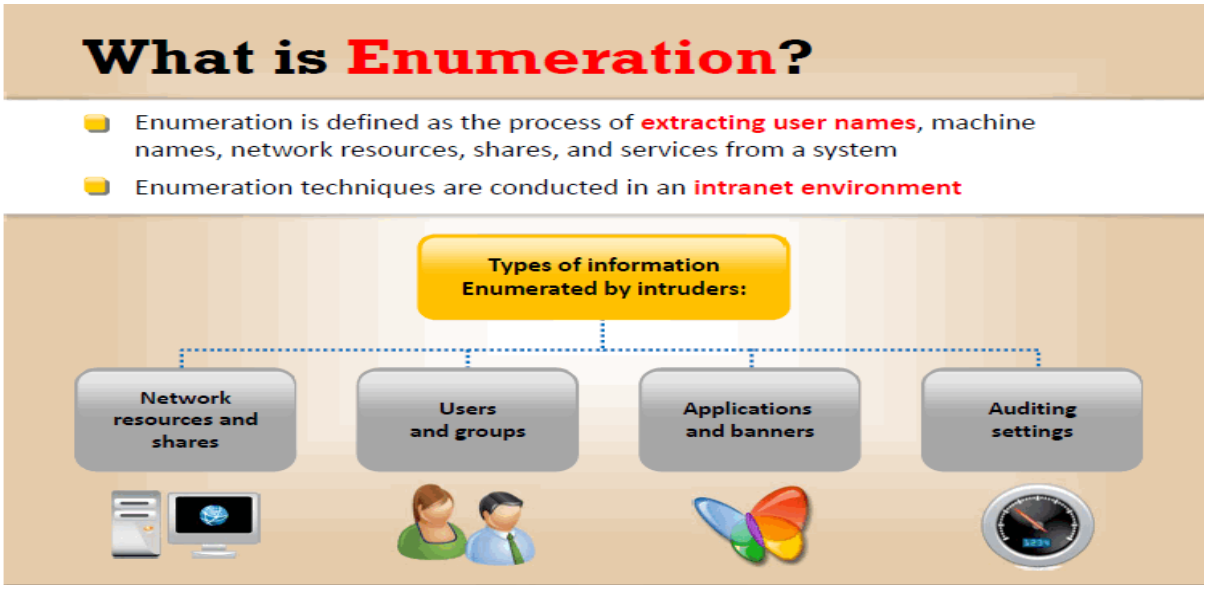


Figure I.14: Enumération

✓ **Technique d'énumération**

- Extraction (Password par défaut, email IDs, Transfert Zone DNS,…)

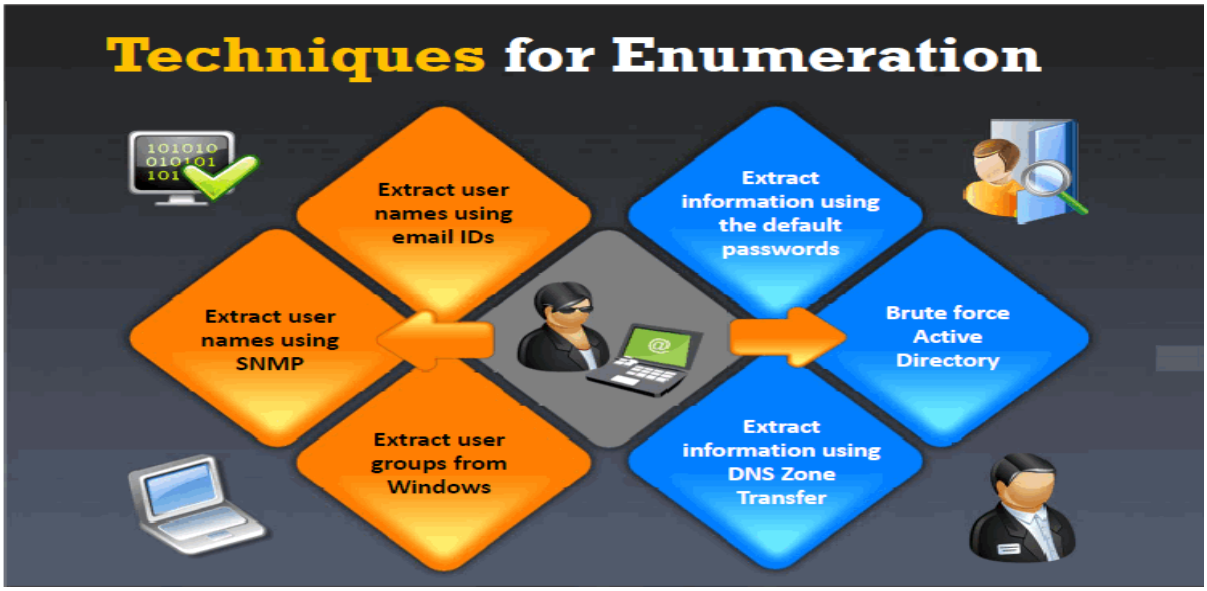


Figure I.15 : But d'énumération

Nous présentant ci-après quelque commende d'énumération sous UNIX/LINUX :

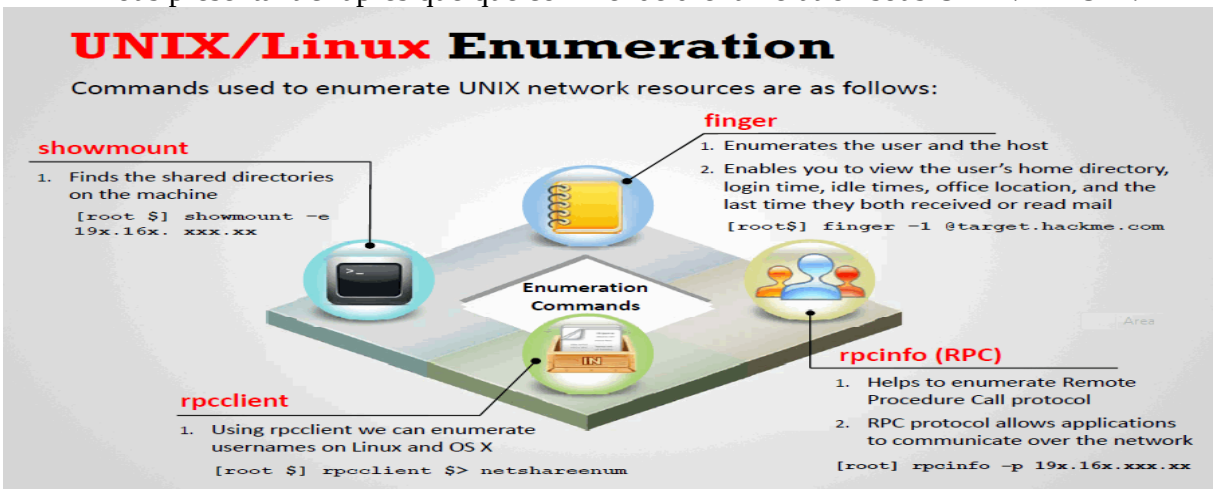


Figure I.16 : Commande d'énumération sous UNIX/Linux

I.7.2.9 Trajan and Backdoors

Un cheval de Troie est un programme qui se cache lui-même dans un autre Programme apparemment au-dessus de tout soupçon. Quand la victime lance ce programme, elle lance par-là même le cheval de Troie caché. Actuellement, les chevaux de Troie les plus utilisés sont : Back Orifice 2000, Netbios, Socket de Troie….

La méthode la plus efficace pour se protéger de ces programmes est d'utiliser un bon antivirus.

Une porte dérobée n'est pas un programme, mais une fonctionnalité d'un programme permettant de donner un accès secret au système. Ce genre de fonctionnalité est souvent ajouté à un logiciel par l'éditeur, afin de lui permettre de surveiller l'activité du logiciel, ou de prendre le contrôle en cas de sollicitation. Généralement, les pirates informatiques une fois entrés dans le système, créent une porte dérobée afin de pourvoir y avoir accès à n'importe quel moment.

Il existe plusieurs types de Trajan tel indiqué dans la figure suivante :

Figure I.17 : Types de Trojans

I.7.2.10 Sniffer (Ecoute du réseau)

Est un dispositif logiciel permettant d'écouter le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent sur ce réseau. Le sniffer peut ainsi servir à déceler les failles de sécurité, mais il peut aussi être utilisé de façon malveillante (pour intercepter les mots de passe du réseau par exemple)

I.7.2.11 Social Engineering

Consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence ;

Figure I.18 :Victimes commun de Social Engineering

I.7.2.12 Session hacking

- Détournement de session se réfère à l'exploitation de la session d'ordinateur valide où un attaquant prend le relais d'une session entre deux ordinateurs
- Le pirate d' ID de session valide sera utilisée pour entrer dans le système et récupéré les données Snoop
- En-session TCP hachage ,un preneur prend en charge une session TCP entre deux machines ;
- Comme la plupart d'authentification se produit seulement au début d'une session TCP, ce qui permet à l'attaquant d'accéder à une machine

I.7.2.13 Evading IDS, Firewalls and Honepots

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, chantage. Parmi les outils les plus utilisé on trouve BackTrack.

BackTrack : C'est une distribution Linux dédiée à l'analyse du réseau, aux tests d'intrusions et à l'audit de la sécurité des systèmes d'information. Avec plus d'une centaine d'outils de sécurité, BackTrack constitue une plateforme idéale pour les spécialistes de la sécurité.

- ✓ **Les types d'IDS**

1-**La détection d'intrusion de réseau à base (Network Based Intrusion Detection System) :**

Le NIDS analyse et contrôle le trafic réseau, cherchant d'éventuelles traces d'attaques en générant des alertes lorsque des paquets suspects sont détectés.

2-**hôte basé sur la détection d'intrusion (Host Based Intrusion Detection System):**

Les HIDS analyse et contrôle des informations contenues sur un équipement précis (ex: un serveur). Ainsi, contrairement à un NIDS, le HIDS récupère les informations qui lui sont données par le matériel ou le système d'exploitation. Il y a pour cela plusieurs approches : signatures, comportement (statistiques) ou délimitation du périmètre avec un système d'ACL.

3-**Connexion Surveillance des fichiers**

Des outils de traçabilité (logging) doivent être mis en œuvre pour garder une trace des événements, comme par exemple :

- qui est venu, quand, quelle a été la durée de la transaction ?
- qu'a-t-on consulté ou modifié ?
- quelle ont été les ressources utilisées ?

La consultation régulière des fichiers historiques constitués doit notamment permettre de vérifier les anomalies dans le trafic des transactions (par exemple les messages répétitifs en provenance d'une même adresse extérieure te rejetés par le firewall peuvent être un signe d'essai d'intrusion).

4 - **Vérification de l'intégrité du fichier** : Vérification que les fichiers sont bien ceux qu'on croit être qu'ils n'ont pas été altérées durant la communication

La figure suivante résume les différents types illustrés précédemment :

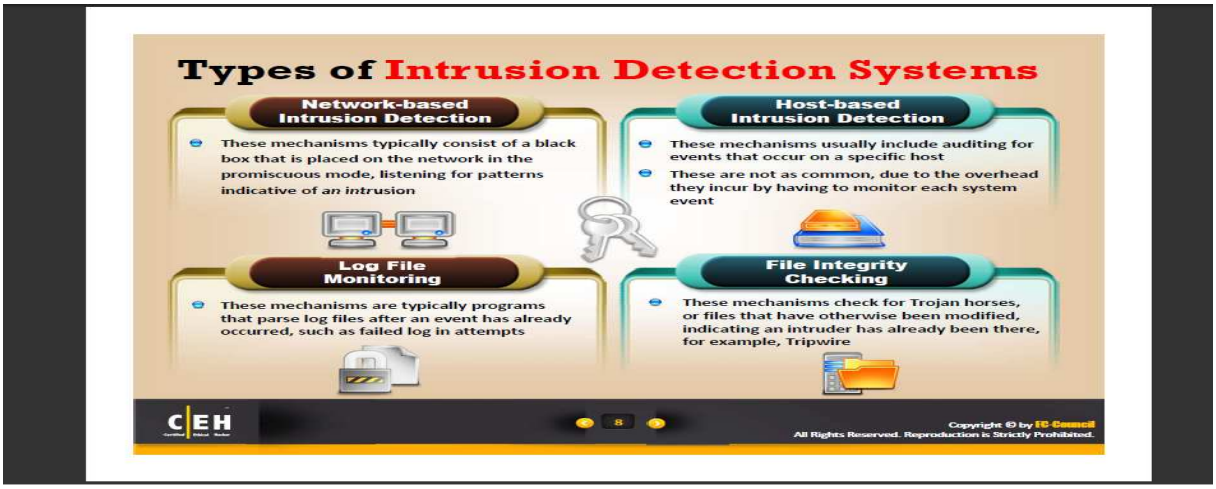


Figure I.19: Type d'IDS

I.7.2.14 Buffer Overflows (dépassement de tampon)

Une des failles les plus courantes est le dépassement de tampon. Suite à une action d'un pirate (ou un incident), un programme écrit en mémoire hors de l'espace prévu à cette effet: par exemple, s'il reçoit trop de données, il va *dépasser* la limite prévue, et écrire sur d'autre données. En créant des données spécifiques, le pirate pourra faire exécuter celle-ci (dangereux).

I.8 Les étapes de hacking

- ✓ **Phase de reconnaissance**:La première méthode c'est de collecter un ensemble d'informations comme

    - Adressage IP,
    - Noms de domaine,
    - Protocoles de réseau,
    - Services activés,
    - Architecture des serveurs,

- ✓ **Phase du scan**
    - «Scanner» de réseau (actifs ou passif, les ports, système utilisé)
    - Lecture du fichier journal (Log)
    - Écoute du réseau ou analyseur de trames ou «Sniffer» Winpcap; NeoTrace, Ettercap; Netstat;

- ✓ **Phase du gain d'accès**

Exploitation d'une faille se fait soit par un **programme malveillant** ou un script shell, souvent compilé sur la machine cible, pour extension de privilèges, erreur système, etc. Il vous faudra certaines qualités humaines pour réussir l'exploitation de failles : patience, persévérance et discrétion. C'est une étape où il faudra utiliser au mieux ses connaissances en informatique

- ✓ **Phase de maintenance d'accès**
    - Installation **d'une porte dérobée (*backdoor*)** pour pouvoir revenir
    - Installation d'un **rootkits** pour tromper l'administrateur légitime

- ✓ **Phase de couverture de traces**
    - Efface toute trace de son passage en supprimant tous les fichiers créés, et corriger les Logs.

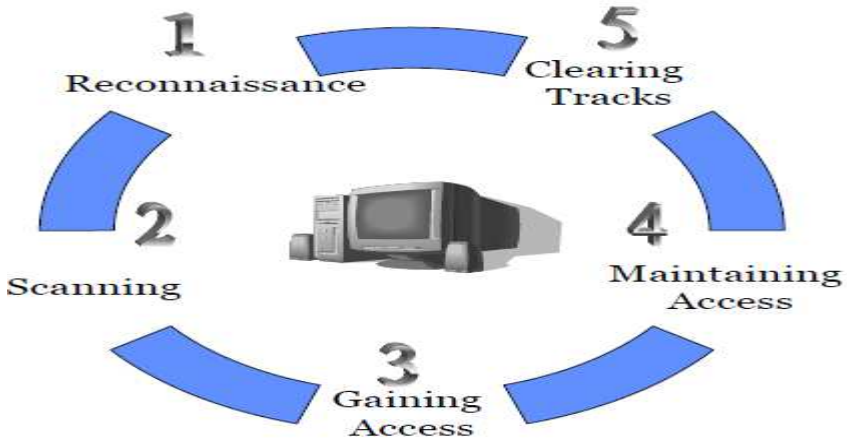


Figure I.20 : **Etape de hacking Network**

Voici quelque outil permettant de scanner un réseau

OpenVAS : est une excellente boîte à outils et services offrant une solution complète pour scanner les vulnérabilités réseaux. Cet outil open source remplace "NESSUS", un autre scanner de vulnérabilité qui n'est plus maintenu.

NMAP :"NMAP" est un outil permettant de scanner un réseau afin d'identifier les services opérationnels. Cet outil est généralement utilisé par les administrateurs sécurité pour l'audit sécurité, mais aussi par les hackers pour attaquer les systèmes. C'est un outil multi-plateforme (Unix/Linux, Windows, Mac) disposant plus d'une centaine d'options lorsqu'il est utilisé en ligne de commande.

Wireshark : C'est un outil permettant de visualiser ce qui se passe dans un réseau. A travers la bibliothèque "libpcap", il capture les paquets qui circulent dans le réseau et fournit des informations sur ceux-ci. Par exemple, à partir de Wireshark, on peut avoir des informations sur le contenu d'un paquet (IP source et destination, protocole, etc.).

Il s'agit d'un logiciel open source placé sous la licence GPL (General Public Licence), pouvant s'exécuter sur plusieurs plates-formes (UNIX/Linux, Windows, Mac)

I.9 Discussions

La connexion d’un réseau à Internet peut exposer une organisation à divers problèmes de sécurité comme nous l'avons vu précédemment dans ce chapitre. Après avoir étudier profondément l'architecture existante de l'entreprise nous avons pu cerner les failles qui pèsent sur cette dernière et comprendre les manières dont les pirates exploitent ces vulnérabilités. Notre travail ne s'arrête pas à ce niveau, il est très important de trouver des solutions aux problèmes rencontrés d'ou la nécessité du deuxième chapitre.

II. 1 Préambule

De façon générale, la sécurité du réseau informatique entre dans la sécurisation globale du système d'information d'entreprise. Plus précisément, elle consiste à respecter des procédures au niveau technique et organisationnel. L'objectif est de protéger le réseau de l'entreprise et de se prémunir contre tout type de risque pouvant dégrader ses performances. Elle consiste également à mettre en place des politiques de sécurité, comme la gestion des accès, pour garantir l'intégrité des données critiques de l'entreprise.

Assurer la sécurité d'entreprise n'a jamais été une tâche facile à faire, il faut toujours faire attention au détail petit ou grand qu'il soit. Dans ce chapitre nous allons proposer des solutions adéquates aux contraintes citer dans le premier chapitre et d'expliquer brièvement le concepts de ces dernière.

II.2 La sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles. Il convient d'identifier les exigences fondamentales en sécurité informatique.

On retrouve actuellement trop souvent des architectures de sécurité axées uniquement sur la prévention et la défense de périmètre. Il y a bien d'autres éléments qui doivent composer une architecture de sécurité. Toute architecture de sécurité (et plus globalement l'approche même de la sécurité) doit reposer sur un triptyque tel que :

- Prévention
- Détection
- Réaction

Ces trois aspects sont pour le moment très diversement couverts par le marché malgré une nécessité indéniable.

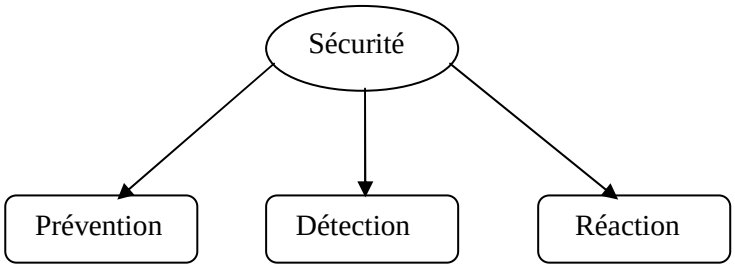


Figure II.1 : La sécurité informatique

a-**Prévention**

La prévention est fondamentale et généralement bien appréhendée par le plus grand nombre. Le principe : faire tout ce qu'il faut pour se protéger. Elle consiste le plus souvent à adopter la démarche suivante :

- Analyse des risques
- Définition d'une politique de sécurité
- Mise en œuvre d'une solution centrée sur un ou plusieurs firewalls.
- Audit de la solution
- Mises à jour

b-**Détection**

Le principe est d'être capable de détecter lorsque les mesures de prévention sont prises en défaut. La détection, même si certains outils techniques existent, est encore trop rarement intégrée aux infrastructures. De plus, à l'heure actuelle un cruel défaut de compétence est à déplorer. Il y a encore trop peu de personnes formées à ce type d'outils. La détection exige un suivi permanent de l'état des systèmes à protéger et des mécanismes de diffusion des alertes générées.

c-**Réaction**

S'il est important de savoir qu'une attaque est en cours ou qu'une attaque a réussi il est encore plus important de se donner les moyens de réagir à cet état de fait. C'est l'aspect le plus négligé actuellement même au sein des acteurs majeurs de la sécurité informatique. " Le risque zéro n'existe pas " ou encore " il n'y a pas de sécurité absolue ". Il faudrait donc toujours prévoir et se préparer au pire. Cela implique la mise en œuvre de procédures d'exploitation spécifiques à la réaction en cas d'attaque, la rédaction et le test d'un plan de continuité informatique à utiliser en cas de sinistre grave.

II.3 Politique de sécurité

La politique ou stratégie de sécurité est un plan d'actions définies par les personnes qui ont accès aux ressources technologiques et aux données vitales de l'entreprise afin de protéger son réseau contre les attaques menées soit de l'intérieur, soit de l'extérieur. Elle a pour objectif :

- 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.

II.4 Les méthodes de sécurité

II.4.1 Mise en place d'une politique de sécurité

La politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de sécurité.

II.4.2 Antivirus

Principale cause de désagrément en entreprise, les virus peuvent être combattu à plusieurs niveaux. La plus part des ordinateurs sont dotés d'un logiciel antivirus pré intégré capable de détecter les principales menaces virales s'il est régulièrement mis à jour. Avec des milliers de nouveau virus gérés chaque mois il est essentiel que la base des données des virus soit tenue à jour. La base des données des virus et l'enregistrement de logiciel antivirus qui permet d'identifier les virus connus lorsqu'ils surviennent.

II.4.3 Firewall (Pare- feu)

C'est un ensemble de différents composants matériels et logiciels qui contrôlent le trafic intérieur / extérieur selon une politique de sécurité.

Un **pare-feu** (appelé aussi *coupe-feu*, *garde-barrière* ou **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;

- une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Figure II.2 : Un pare-feu

II.4.4 Les réseaux privés virtuels (VPN)

Un VPN (Virtual Private Network) permet de simuler un réseau privé via internet en cryptant les communications entre deux points distants. Une fois le tunnel présent à travers le réseau public, entre deux machines ou deux réseaux privés, ces derniers pourront s'échanger des données de manière sécurisée, comme s'ils se trouvaient sur le même réseau local.

Le VPN permet aux entreprises de bénéficier d'une liaison sécurisée à moindre coût, a contrario des lignes spécialisées qui restent certes plus fiables et plus sûres mais moyennant un coût financier très onéreux. Les réseaux privés virtuels s'appuient, comme la plupart des technologies réseaux sur des protocoles. Plusieurs protocoles sont utilisés dans la technologie VPN. Certains d'entre eux visent uniquement à établir un tunnel, d'autres y ajoutent la composante de sécurité.

II.4.5 Cryptage et Authentification

La cryptographie est une méthode permettant de rendre secrètes (illisibles) des informations afin de garantir l'accès à un seul destinataire authentifié. Elle est essentiellement basée sur l'arithmétique : il s'agit de transformer les lettres qui composent le message en succession de chiffres (sous forme des bits dans le cas de l'informatique), puis faire des calculs sur ces chiffres pour :

- D'une part les modifier de telle façon à les rendre incompréhensible.
- Faire en sorte que le destinataire saura les décryptées.

Le fait de coder un message de façon à le rendre secret s'appelle le cryptage. La méthode inverse est t'appelée décryptage, elle nécessite une clé de décryptage.

On distingue de types de cryptages :

a- Cryptage symétrique

Le cryptage symétrique appelé également cryptage à clé secrète ou chiffrement conventionnel, utilise une même clé pour crypter et décrypter le message, très efficace et assez économe en ressource CUP. Les algorithmes de chiffrement les plus connus sont :

DES (Data Encryptions Standard) et 3DES et AES

Le principe problème de cette technique la distribution des clés dans un réseau étendu, nécessite de partager une seul clé avec chacun de nos correspondants.

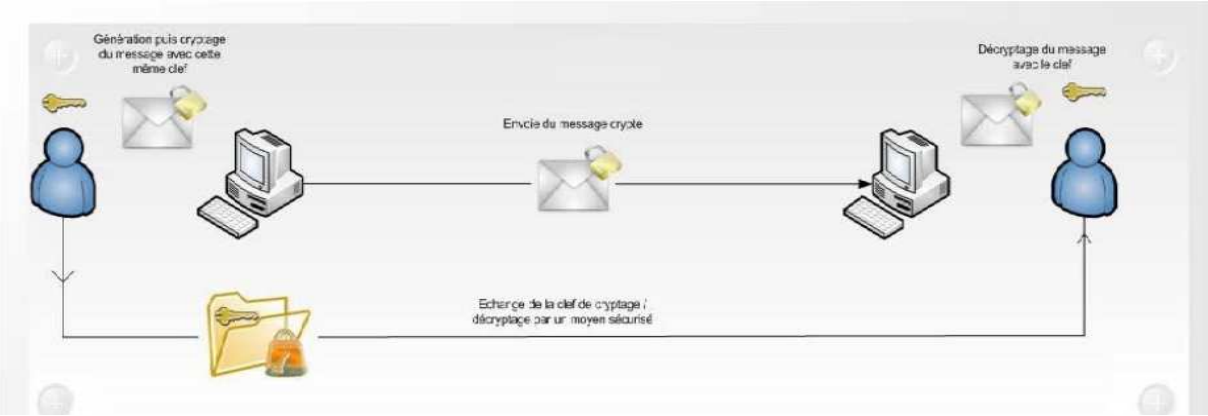


Figure II.3: Cryptage symétrique

On a un utilisateur A et un utilisateur B, lorsque l'utilisateur A veut envoyer son numéro de carte de crédit a l'utilisateur B il va le crypté avec une clé, le résultat de cryptage va transiter par Internet et lorsqu'il arrive à B il le décrypte avec la même clé et on obtient le document initial qui contient le numéro de carte de crédit.

b- Cryptage asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par son propriétaire ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante car ces deux clés générer au même temps. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- permet de signer le message donc garantir l'Authentification et la non- répudiation.
- Supporte les signatures numériques.

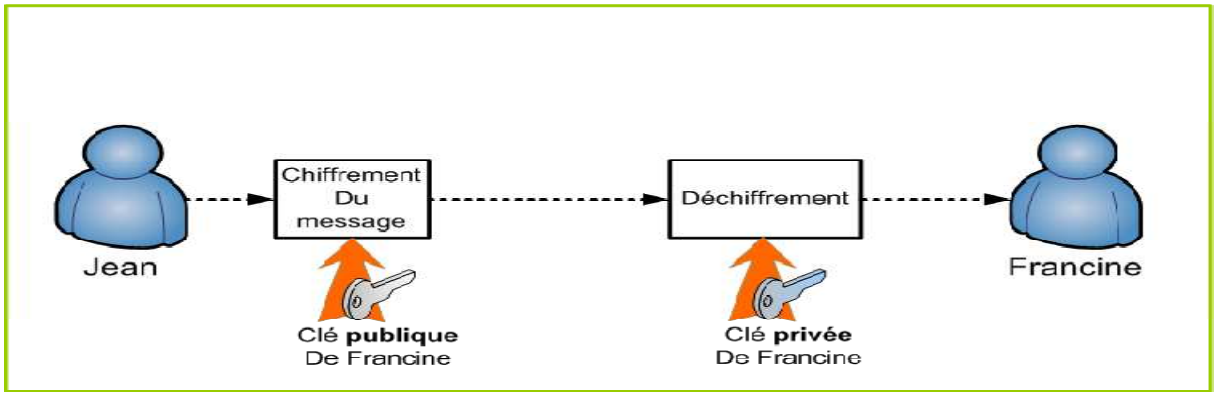


Figure II.4: Cryptage asymétrique

c- La HASH : Assuré l'intégrité du message

d- L'authentification

Permettant de vérifier les identités présumées des utilisateurs. Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle de l'authentification simple. Lorsque nécessite plusieurs facteurs on parle de l'authentification forte.

L'authentification permet de vérifier l'identité d'un utilisateur sur une des bases suivantes :

Un élément d'information que l'utilisateur connaît (mot de passe, etc)

Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat)

Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (ADN, empreinte digitale, fond de rétine.)

L'authentification intervient à différents niveaux dans les couches de protocoles du modèle internet :

Au niveau applicatif : HTTP, FTP

Au niveau transport : SSL, SSH

Au niveau réseau : IPSEC

Au niveau transmission : PAP, CHAP

II.4.6 Les différentes méthodes utilisées pour l'authentification

a) Les clés

Une clé est une valeur qui est utilisée avec un algorithme cryptographie pour produire un texte chiffré spécifique, sa taille se mesure en bits. Plus la clé est grande, plus le chiffrement est sûr.

b) Certificat numérique

b.1) Présentation

Un certificat numérique (aussi appelé certificat électronique) est un fichier permettant de certifier l'identité du propriétaire d'une clé publique, un peu à la manière d'une carte d'identité.

Un certificat est généré dans une infrastructure à clés publiques (aussi appelé **PKI** pour **Public Key Infrastructure**) par une autorité de certification (Certification Authority,CA) qui a donc la capacité de générer des certificats numériques contenant la clé publique en question. Actuellement, les certificats numériques sont reconnus à la norme **X.509 version 3**.

Ce format se compose entre autre de :

- le numéro de série.
- l'algorithme de signature.
- le nom de l'émetteur (autorité de certification).
- la date de début de fin de validité.
- l'adresse électronique du propriétaire.
- la clé publique à transmettre.
- le type de certificat.
- l'empreinte du certificat (signature électronique).

Figure II.5 :Les étapes de vérification par certificat

La signature électronique est générée par l'autorité de certification à l'aide d'informations personnelles (telles que le nom, le prénom, l'adresse e-mail, le pays du demandeur, etc) en utilisant sa propre clé privée.

Il existe de nombreux types de certificats numériques, répondant chacun à un besoin particulier. Les principaux types sont :

- Certificat de messagerie (permet de crypter et de signer ses e-mails).
- Authentification IP Sec pour un accès distant par VPN.
- Authentification Internet pour les pages Web sécurisées.
- Cryptage des données avec EFS (Encryptions File System)
- Signature de logiciel.

b.2) Le rôle d'un certificat numérique

Un certificat numérique intervient dans différents mécanismes permettant de sécuriser l'échange de données sur un réseau. On y retrouve le cryptage asymétrique ou encore la signature électronique combinée à un contrôle d'intégrité des données.

- **Les infrastructures à clés publiques (PKI) :**

Une PKI (Public Key Infrastructure), aussi appelée IGC (Infrastructure de Gestion de Clés) est une infrastructure réseau qui a pour but final de sécuriser les échanges entre les différents composants d'un réseau.

Cette infrastructure se compose de quatre éléments essentiels

- **Une autorité d'enregistrement (Registration Authorities)** : c'est cette autorité qui aura pour mission de **traiter les demandes de certificat** émanant des utilisateurs et de générer les couples de clés nécessaires (clé publique et clé privée). Son rôle peut s'apparenter à la préfecture lors d'une demande de carte d'identité.
- **Une Autorité de Certification (Certification Authorities) :** elle reçoit de l'Autorité d'Enregistrement les demandes de certificats accompagnées de la clé publique à certifier. Elle va **signer à l'aide de sa clé privée** les certificats, un peu à la manière de la signature de l'autorité sur une carte d'identité. Il s'agit du composant le plus critique de cette infrastructure en raison du degré de sécurité requis par sa clé privée.
- **Une Autorité de Dépôt (PKI Repositories) :** il s'agit de l'élément chargé de **diffuser les certificats numériques** signés par la CA sur le réseau (privé, Internet, etc).
- **Les utilisateurs de la PKI :** ce sont les **personnes effectuant des demandes** de certificat mais aussi ceux qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu.

b.3) Types d'autorités de certification

Il existe deux types principaux d'installation pour l'autorité de certification :

A-Autorité d'entreprise : à utiliser si l'autorité de certification doit délivrer des certificats dans un domaine auquel appartient le serveur (se base sur l'annuaire d'Active Directory). Cette autorité doit-être contrôleur de domaine.

B-**Autorité autonome :** permet de délivrer des certificats dans un réseau comme Internet.

Il existe deux niveaux fonctionnels pour chacun de ces deux types d'installation pour l'autorité de certificat :

a-**Autorité racine :** Cette autorité de certification est la première du réseau.

b-**Autorité secondaire :** dépend d'une autorité racine.

c) Signature numérique

Signature reposant sur un système de chiffrement à clé publique et à clé privée permettant d'authentifier l'émetteur d'un document électronique. La clé privée sert à signer et la clé publique sert à vérifier cette signature. Les principales avantages elle n'est pas répudiable, protection contre les modifications, signer directement tout ce qui est numérisation. Le seul inconvénient c'est une procédure complexe.

d) Liste de contrôle d'accès

Le mécanisme des listes de contrôle d'accès (ACL, *Access Control List*) utilise l'identité authentifiée des entités et des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau. De plus, il est susceptible d'enregistrer sous forme de trace d'audit et de répertorier les tentatives d'accès non autorisées. Tout utilisateur qui se trompe dans son mot de passe laisse une trace. Il est ainsi possible de détecter les programmes automatiques qui cherchent à pénétrer le système en essayant tous les mots de passe. Les informations utilisées sont : les listes de droits d'accès, maintenues par des centres, les mots de passe, les jetons de droits d'accès, les différents *certificats* (voir plus loin), les libellés de sensibilité des données.

Le mécanisme de contrôle d'accès peut avoir lieu aux deux extrémités de la communication (équipement d'accès et ressource du réseau).

e) RADIUS

Le protocole **RADIUS** (*Remote Authentication Dial-In User Service*), mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC.

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé **NAS**

(*Network Access Server*), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé. Il est à noter que le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.

II.5 Protocoles de sécurité

- **SSH (Secure Shell)**

Le protocole **SSH** (*Secure Shell*) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (Spoofing).

- **SSL** (Secure Socket Layer)

Protocole assurant une transmission sécurisée de données sur un site web.
Développé à l'origine par la société Netscape Communications pour son navigateur, le protocole SSL est destiné au cryptage des données. Il permet de vérifier l'authentification, la confidentialité et l'intégrité des données échangées.

Remarque : Il faut se méfier des systèmes propriétaires, contrairement à ce qu'on pourrait penser, la sécurité d'un système de chiffrement ne réside **pas** dans le secret de l'algorithme de chiffrement, mais dans le secret de la clé. Il ne faut faire confiance qu'aux systèmes qui ont été publiés et analysés.

- **Le protocole POP3**

Le protocole POP3 (Post Office Protocol version 3) occupe le port 110 ; il est nécessaire pour les personnes n'étant pas connectées en permanence à internet de pouvoir consulter les mails reçus hors connexion.

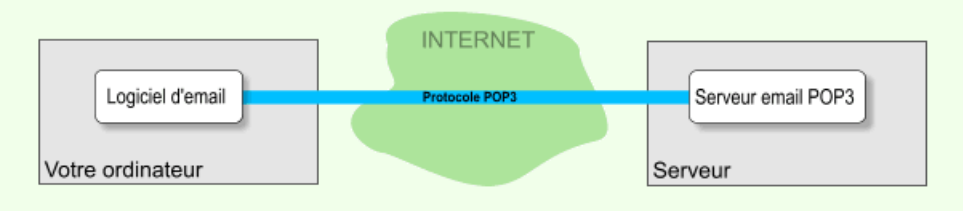


Figure II.6 :L'utilisation du protocole POP3 sans tunnel SSL

Avec le protocole POP3 que vous utilisez habituellement pour aller lire votre courrier, les mots de passe et les messages transitent **en clair** sur Internet. Il est possible de voler vos mots de passe et vos messages.

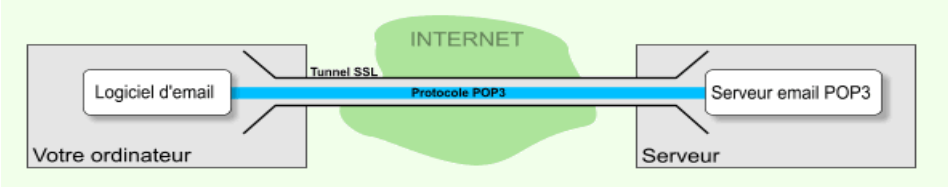


Figure II.7 :L'utilisation du protocole POP3 avec tunnel SSL

Avec le tunnel SSL, et sans rien changer aux logiciels client et serveur, vous pouvez sécuriser la récupération de vos mails: personne ne peut vous volez vos mots de passe ou emails puisque tout ce qui passe à travers le tunnel SSL est chiffré.
Mais cela nécessite d'installer STunnel sur le client **et** sur le serveur.

- **Le protocole SMTP**

Le protocole SMTP (Simple Mail Transfer Protocol) est un protocole standard permettant de transférer le courrier d'une machine à une autre. Ce protocole fonctionne en mode connecté, il est par défaut sur le port 25.

- **IPsec**

IPsec vise à sécuriser les échanges au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPSec pour IP Security Protocols.
Le protocole IPSec fournit ainsi :

- des mécanismes de confidentialité et de protection contre l'analyse du trafic.
- des mécanismes d'authentification des données (et de leur origine).
- des mécanismes garantissant l'intégrité des données (en mode non connecté).

- des mécanismes de protection contre le rejet.
- des mécanismes de contrôle d'accès. **IPsec est employé de deux manières:**

a- Mode transport :

Le mode transport prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans ce mode, l'insertion de la couche IPsec est transparente entre TCP et IP. TCP envoie ses données vers IPsec comme il les enverrait vers IPv4.

Figure II.8 :L'utilisation du protocole IPsec mode Transport

b- Mode tunnel

Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche IP incluse, puis sont envoyées vers le module IPsec. L'encapsulation IPsec en mode tunnel permet le masquage d'adresses.

Le mode tunnel est généralement utilisé entre deux passerelles de sécurité (routeur, firewall.

Alors que le mode transport se situe entre deux hôtes.

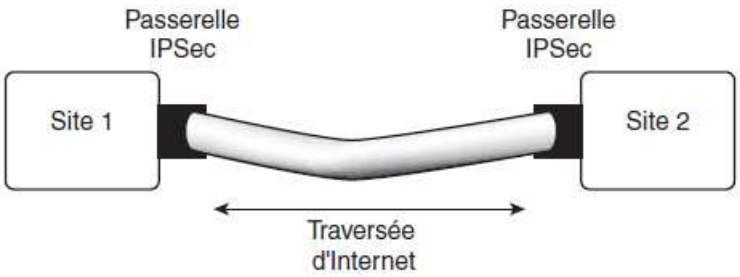


Figure II.9 :L'utilisation du protocole IPsec mode Tunnel

❖ **http/https**

S-HTTP est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP. Il permet de fournir une sécurisation des échanges lors de transactions de commerce

électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle.

II.6 Les solutions implémentées dans notre architecture

Après l'étude de l'existant, on a opté pour une infrastructure plus sécurisé afin d'atteindre un bon niveau de sécurité contre les hackers

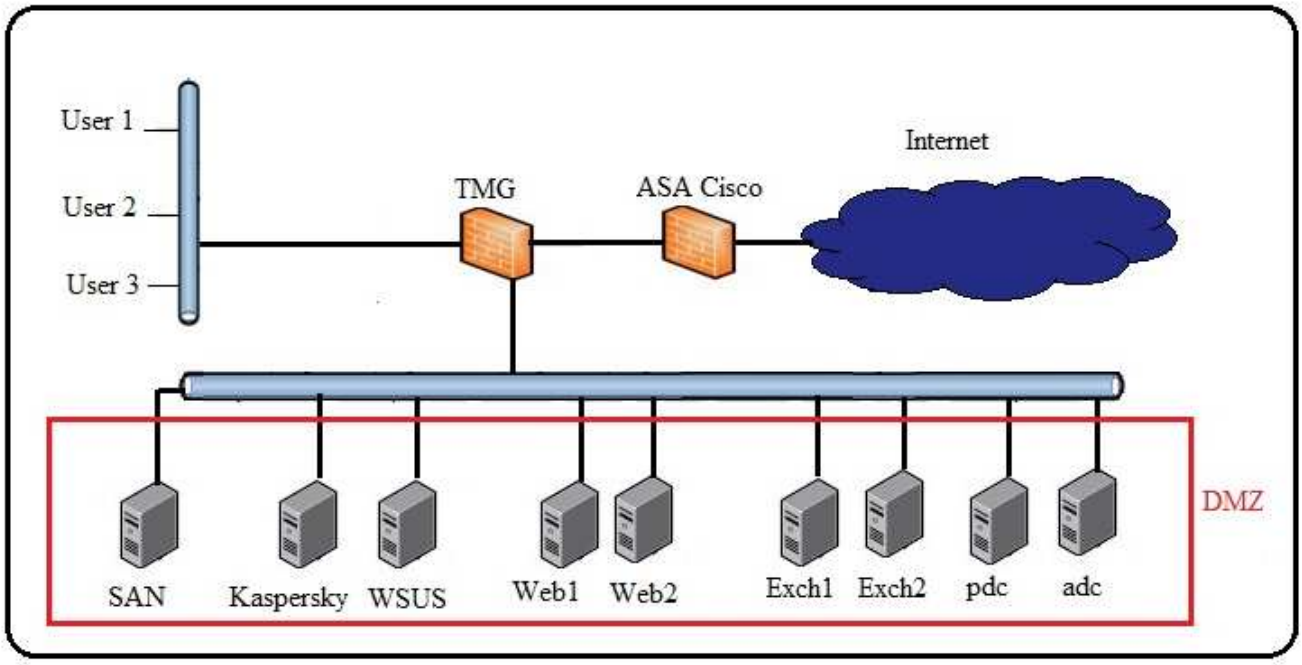


Figure II.10: Architecture final de l'entreprise

Dans le but de bien sécurisé notre infrastructure réseau on a procédé comme suit:

Mise en œuvre des solutions suivantes:

- Déployer un antivirus Kaspersky (gestion centralisée)
- Déployer un serveur de mise à jour système(WSUS) pour minimiser le trafique réseau et sécuriser les systèmes (correctifs Microsoft)
- Deux contrôleurs de domaine pdc, adc (partage de tâches, réplication et tolérance aux pannes)
- Création de zones de DNS qui permettra la résolution de nom ,
- Assuré la disponibilité de serveur DHCP avec authentification simplifier la gestion des adresses IP,
- Création et déploiement des certificats (pour la communication chiffrée entre les clients) contre le Snifing ,
- Configuration de NAP (Network Access Protection) pour la sécurité de serveur DHCP

- Configuration de serveur radius pour double authentification,
- Deux serveurs Web pour une haute disponibilité
- Gestion des stratégies de groupe (implémenté des règles de sécurité sur les client)
- Déployer un serveur de fichiers à fin de mieux gérer les droits d'accès aux informations de l'entreprise(DFS).
- Déployer deux serveur de mail Exchange pour la gestion de la messagerie,
- Déployer un firewall ASA Cisco pour protéger le réseau des menaces externes et TMG pour la gestion de connexion Internet et la protection contre les menaces Interne
- Publication sécurisé de serveur Web et serveur Exchange avec le firewall TMG Microsoft.
- Utilisation de la technologie RAID pour la sécurité de stockage des données
- Chiffrement de la communication avec IPSec et les certificats
- Utilisation de la technologie SAN comme moyen de sauvegarde
  - backup état système
  -recovery (en cas de catastrophe naturelle) ,
  -Equilibrage de charge

II.7 Les choix et solutions implémentées

II.7.1 La technologie RAID

L'utilisation de la technologie RAID qui signifie **« ensemble redondant de disques indépendants »** qui permet de constituer une unité de stockage à partir de plusieurs disques et d'y effectuer des sauvegardes régulières à partir de plusieurs disques durs. L'unité ainsi constituée (grappe) a donc une grande tolérance aux pannes ou une plus grande capacité et vitesse d'écriture. Une telle répartition de données sur plusieurs disques permet d'augmenter la sécurité et de fiabiliser les services associés donnes l'exemple RAID 1 et RAID 5.

- **RAID 1**

Egalement connu sous le nom volumes en miroir, c'est un volume à tolérance de panne qui garantit la redondance des données en utilisant deux copies, ou miroirs, du même volume. Toutes les données écrites sur le volume miroir sont écrites sur les deux volumes, qui sont situés sur des disques physiques distincts. Si un des disques physiques a un problème, les données du disque défaillant ne sont plus disponibles, mais le système continue à fonctionner en exploitant le disque non affecté.

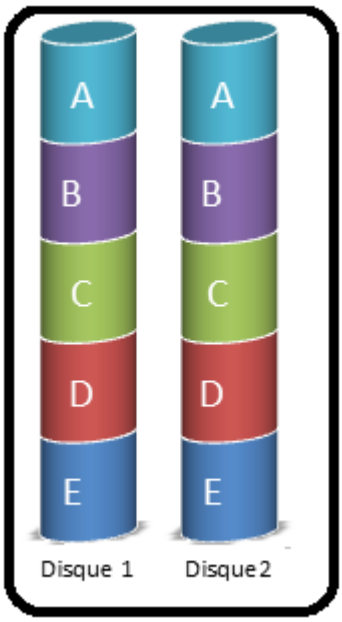


Figure II .11 : **Un volume RAID1 ou en miroir copie toutes les données sur un deuxième disque**

- **RAID 5**

Un volume RAID 5 est un volume tolérant aux pannes qui combine des zones d'espace libre d'un moins trois disques durs physiques en un seul volume logique. Les volumes RAID 5 agrègent les données par bondes avec des informations sur la parité (paire ou impaire) sur une baie de disques. Quand un disque est défaillant, Windows server 2008 se base sur ces informations parité pour recréer les données sur le disque défaillant. Les volumes RAID 5 peuvent accepter de perdre un seul disque dans la baie.

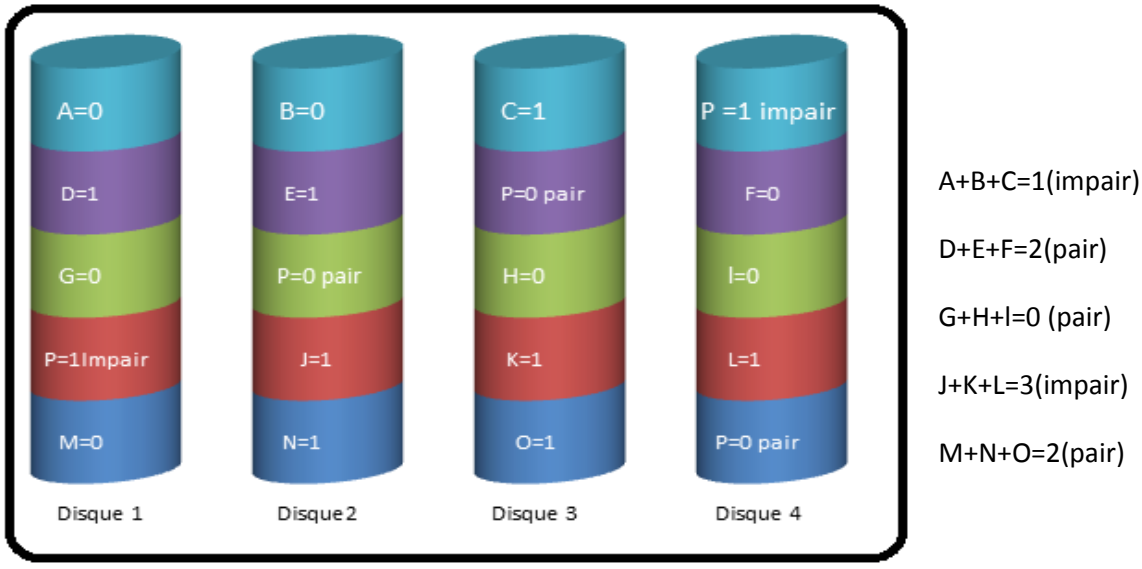


Figure II.12 :**Un volume RAID 5 calcule la parité (pair ou impair) pour la tolérance aux pannes**

Remarque : Un volume agrégé par bandes, également connu sous le nom RAID 0, est un volume dynamique qui stocke des données dans des bandes sur deux disques physiques ou plus. Ce type de volume offre les meilleures performances par rapport à tous les autres volumes disponibles dans Windows, mais ne propose pas la tolérance de panne. Si un disque dans un volume agrégé par bandes est défaillant les données de tout le volume sont perdues. Solution proposé dans le cas de stockage de données temporaire.

II.7.2 Mise en place d'un antivirus Professionnelle

La mise en place d'un antivirus Professionnelle est la partie la plus importante dans la définition d'une stratégie de sécurité de toutes entreprises, dans notre cas on opter pour l'antivirus Kaspersky admin kit , une application développée dans le but d'une exécution centralisée des principales tâches d'administration de la gestion de la sécurité du réseau informatique de l'entreprise,

II.7.2.1 Compostions de l'application

L'application Kaspersky Administration Kit se présente sous forme de trois composants principaux

- **Le *Serveur d'administration* (ci-après, Serveur)** est un entrepôt centralisé d'informations sur les applications Kaspersky installées sur le réseau local de la société et un outil efficace de gestion de ces applications.
- **L'*Agent d'administration* (ci-après, *Agent*)** coordonne les interactions entre le Serveur d'administration et les applications Kaspersky installées sur un poste spécifique du réseau (lui-même un poste de travail ou un serveur). Ce composant est unique pour toutes les applications Windows de la ligne de produits Kaspersky Open Space Security. Il existe des versions de l'Agent d'administration spécifiques aux applications Kaspersky qui fonctionnent sur Novell ou Unix.
- **La *Console d'administration* (ci-après, *Console*)** fournit l'interface utilisateur nécessaire pour les services administratifs du Serveur et de l'Agent. Le module gestionnaire est conçu comme une extension MMC (Microsoft Management Console). La Console d'administration permet de se connecter au Serveur d'administration distant par Internet.

II.7.2.2 Principales fonctions de l'application

Kaspersky Anti-Virus offre les fonctionnalités suivantes :

- Analyse en temps réel du trafic des protocoles HTTP, FTP, SMTP et POP3.
- Analyse du trafic entrant du protocole HTTPS (uniquement pour Forefront TMG).

- Large choix de paramètres de filtrage du trafic avec utilisation de groupe d'entitées réseau et de règles d'analyse.
- Maintien de l'actualité de la protection grâce à la mise à jour à intervalle régulier des bases de Kaspersky Anti-Virus.
- Identification des riskwares.
- Contrôle en temps réel du fonctionnement de Kaspersky Anti-Virus.
- Obtention d'informations sur le fonctionnement de Kaspersky Anti-Virus grâce aux rapports intégrés.
- Conservation des copies des objets bloqués dans la sauvegarde.
- Configuration détaillée des performances de l'analyse antivirus en fonction de la puissance du serveur et de la bande passante du canal Internet.
- Répartition de la charge entre les processeurs du serveur.
- Administration à distance de Kaspersky Anti-Virus à l'aide de la console d'administration qui se présente sous la forme d'un composant logiciel enfichable de console.

II.7.3 Déploiement de deux contrôleurs de domaine

Afin d'assurer le partage de tâches, réplication et tolérance aux pannes le déploiement de contrôleurs de domaine s'avère très important pour le bon fonctionnement de l'entreprise.

II.7.3.1 L'active directory

Active Directory (AD) est la mise en œuvre par **Microsoft** des services **d'annuaire LDAP** pour les **systèmes d'exploitation Windows**. L'objectif principal d'*Active Directory* est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. *Active Directory* répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.

Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

II.3.3.2 Réplication dans l'Active directory

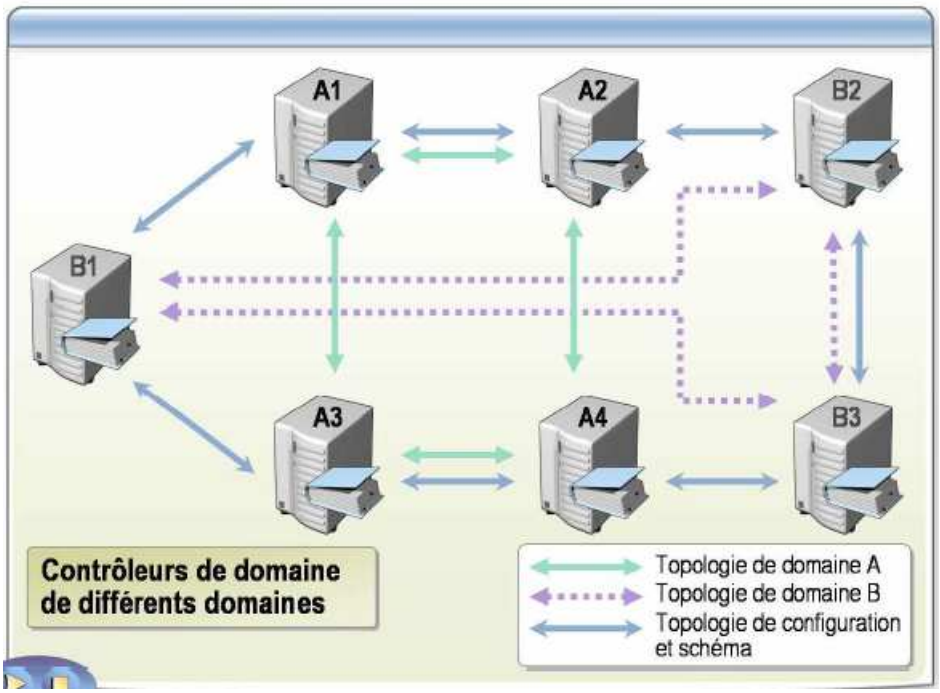


Figure II.13: Réplication dans l'Active directory

La topologie de réplication est l'itinéraire suivi par les données de la réplication à travers un réseau. La réplication se produit entre deux contrôleurs de domaine à la fois. Avec le temps, la réplication synchronise les données dans Active Directory pour toute une forêt de contrôleurs de domaine. Pour créer une topologie de réplication, Active Directory doit déterminer quels contrôleurs de domaine répliquent les données avec les autres contrôleurs de domaine.

II.7.4 Gestion centralisée

II.7.4.1 Gestion de stratégie de groupe

Les GPO (Group Policies Object) permettent de la mise en œuvre de stratégies spécifiques liées à des groupes définis dans l'Active Directory.

Les stratégies de groupe sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des éléments inscrits dans un environnement Active Directory.

Bien que les stratégies de groupe soient régulièrement utilisées dans les entreprises, elles sont également utilisées dans les écoles ou dans les petites organisations pour restreindre les actions et les risques potentiels comme par exemple le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, la gestion des imprimantes, le déploiement d'applications, etc.

Les stratégies de groupe sont analysées et appliquées au démarrage de l'ordinateur et pendant l'ouverture de session de l'utilisateur. Les ordinateurs rafraîchissent les paramètres transmis par les stratégies de groupe de façon périodique, généralement toutes les 60 ou 120 minutes, ce paramètre étant ajustable par un paramètre de stratégie de groupe.

II.7.4.2 Replication Distributed File System (DFS)

La réplication DFS correspond à un moteur de réplication multi-maître efficace qui vous permet de maintenir des dossiers synchronisés entre des serveurs par le biais de connexions réseau dont la bande passante est limitée. Elle remplace le service de réplication de fichiers (FRS) comme moteur de réplication pour les espaces de noms DFS, ainsi que pour la réplication du dossier SYSVOL des services de domaine Active Directory (AD DS) dans les domaines qui utilisent le niveau fonctionnel de domaine Windows Server 2008.

La réplication DFS utilise un algorithme de compression appelé compression différentielle à distance (RDC). L'algorithme RDC détecte les modifications des données d'un fichier et permet à la réplication DFS de répliquer uniquement les blocs de fichier modifiés à la place du fichier entier.

Pour utiliser la réplication DFS, vous devez créer des groupes de réplication et ajouter des dossiers répliqués dans ces groupes. Les groupes de réplication, les dossiers répliqués et les membres sont illustrés dans la figure ci-dessous.

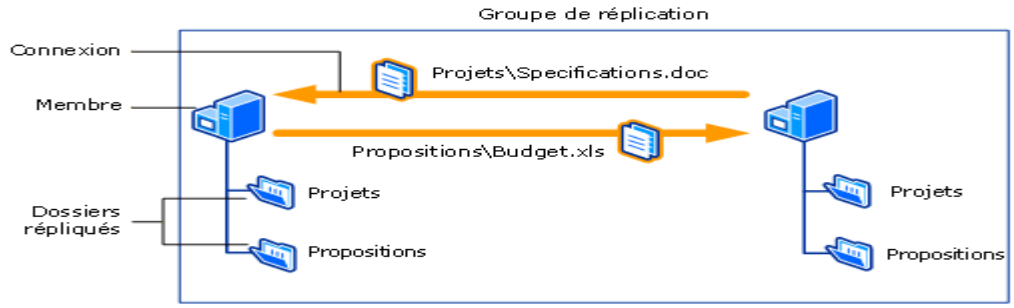


Figure II.14 : Exemple de Groupe de réplication

Cette illustration montre qu'un groupe de réplication est un ensemble de serveurs, appelés membres, qui participe à la réplication d'un ou de plusieurs dossiers répliqués. Un dossier répliqué est un dossier qui reste synchronisé sur chaque membre. Dans l'illustration, deux dossiers répliqués sont représentés : Projets et Propositions. À mesure que les données sont modifiées dans chaque dossier répliqué, les modifications sont répliquées via les connexions établies entre les membres du groupe de réplication. Les connexions entre tous les membres constituent la topologie de la réplication.

Chaque dossier répliqué possède des paramètres uniques, tels que les filtres de fichiers et de sous-dossiers qui vous permettent de filtrer différents fichiers et sous-dossiers pour chaque dossier

répliqué. Vous pouvez administrer la réplication DFS en utilisant le composant Gestion du système de fichiers distribués DFS, les commandes DfsrAdmin et Dfrdiag, ou des scripts qui appellent WMI.

Le service de réplication de fichiers (FRS) est une technologie introduite à l'origine dans Windows 2000 Server. Il répliqu e les fichiers et les dossiers qui sont stockés dans les dossiers DFS (Distributed File System) ou dans le dossier SYSVOL sur les contrôleurs de domaine.

II.7.4.3 Cluster

Accumulation de machines dans un but de travail coopérative. Systèmes informatiques indépendants, se comportant comme un seul système.

Dans Windows Server 2008, vous pouvez configurer trois types de groupes de serveur pour la répartition de charge, l'extensibilité et la haute disponibilité. Premièrement, un groupe de distribution round-robin est un ensemble d'ordinateurs qui utilisent DNS pour proposer une répartition de charge basique avec des exigences minimes de configuration. Deuxièmement, un cluster avec répartition de la charge réseau (NLB) (également appelé batterie NLB) est un groupe de serveurs utilisés pour fournir un équilibrage de la charge mais également pour augmenter l'extensibilité. Enfin, un cluster de basculement permet d'accroître la disponibilité d'une application ou d'un service dans le cas d'une défaillance du serveur.

II.7.4.4 Cluster de basculement

Un cluster de basculement est un groupe de deux ou plusieurs ordinateurs utilisés pour éviter toute indisponibilité des applications et services sélectionnés. Les serveurs mis en cluster (appelés nœuds) sont connectés via des câbles physiques les uns aux autres et au stockage disque partagé. Si l'un des nœuds est défaillant, un autre nœud prend le relais (basculement). Par conséquent, les utilisateurs connectés au serveur ne sont que peu affectés par cette défaillance.

Les serveurs d'un cluster de basculement peuvent fonctionner dans différents rôles, y compris les rôles d'un serveur de fichiers, un serveur d'impression, un serveur de messagerie ou un serveur de bases de données, et proposent la haute disponibilité pour un grand nombre d'autres services et applications.

Dans la majorité des cas, le cluster de basculement inclut une unité de stockage partagé qui est connectée physiquement à tous les serveurs du cluster, même si un seul serveur à la fois peut accéder à un volume donné dans le stockage.

II.7.4.4.1 Architecture de cluster

- **Systèmes en Clustering** : Tâches réparties sur plusieurs machines (les sites web importants).
- **Logiciels en Clustering** : une seule et une même tâches est répartie sur chaque machine (calculs).

II.7.4.4.2 Les besoins du Clusturing

- ***Augmentation de la puissance de traitement (scalability***) : On veut que la puissance de traitement suive de manière linéaire le nombre de machines du cluster.
- ***Augmentation de la disponibilité (availability):*** On veut minimiser les inconvénients liés aux pannes par la redondance des machines entre elles.
- ***Calcul Haute-Performance et Partage de charge*** : Configurations à plusieurs dizaines (centaines) de nœuds.

II.7.4.4.3 La haute disponibilité

- Assurer un redémarrage rapide en quelques minutes en cas de problème imprévu - redondance de machines.
- Pas de rupture de service perceptible aux utilisateurs.
- Ce n'est pas de la tolérance de panne

II.7.5 DHCP

Un serveur DHCP a pour but d'affecter des adresses IP à des ordinateurs. Plus concrètement, lorsqu'un ordinateur dépourvu d'adresse IPv4 est configuré pour en obtenir une automatiquement, cet ordinateur diffuse au démarrage des paquets de découverte DHCP sur le réseau. Ces messages de découverte DHCP sont alors transmet via les câbles, concentrateurs et commutateurs voisins.
La négociation entre un client et DHCP s'effectue en quatre étapes (voir la figure suivante)

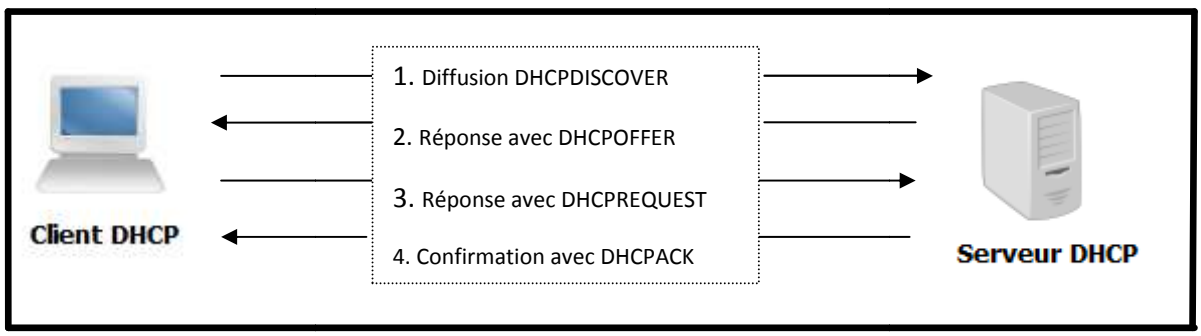


Figure II.15 :Processus d'affectation d'adresse DHCP

i. Diffusion DHCP

Lors de cette première étape, le client diffuse un message de découverte DHCP (DHCPDiscover) sur le réseau local pour identifier tous serveur DHCP disponible. Cette diffusion s'arrête au routeur le plus proche, à moins que ce dernier ne soit configuré pour la transmettre.

ii. Réponse avec DHCP Offer

Un serveur DHCP est connecté au réseau local et peut offrir au client DHCP une affectation d'adresse IP, il envoie un message mono diffusion d'offre DHCP (DHCP offer) au client DHCP

iii. Réponse avec DHCP Request

A la troisième étape de la négociation DHCP, le client répond au message DHCP Offer et demande l'adresse IP qui figure. Il peut toutefois demander l'adresse IP qui lui était précédemment affecté.

iv. Confirmation avec DHCP ACK

Si l'adresse IP demandée par le client DHCP est encore disponible, le serveur DHCP répond par un message d'accord DHCP ACK. Le client peut maintenant envoyer cette adresse IP.

II.7.6 DNS

DNS (Domain Name System) est un système d'appellation d'ordinateurs et de services réseau organisé selon une hiérarchie de domaines. L'attribution de noms DNS est utilisée sur les réseaux TCP/IP tels qu'Internet afin de localiser les ordinateurs et les services au moyen de noms conviviaux. Lorsqu'un utilisateur entre un nom DNS dans une application, les services DNS peuvent résoudre ce nom en une autre information qui lui est associée, par exemple une adresse IP Le DNS se compose des éléments suivant

- **Serveur DNS**

Un serveur DNS est un ordinateur qui exécute un programme de serveur DNS, il est sous le nom BIND avec UNIX. Les serveurs DNS contiennent des informations de bases de données DNS sur une certaine partie de structure arborescente de domaine DNS et résolvent les requêtes de résolution de noms émises par des clients DNS.

- **Zone DNS**

Une zone DNS est la partie contiguë d'un espace de noms pour laquelle un serveur fait autorité. Un serveur peut faire autorité pour une ou plusieurs zones, tandis qu'une zone peut renfermer un ou plusieurs domaines contigus. Il existe deux types de zones :

- ❖ Zone de recherche directe où les noms sont résolus en adresses IP.
- ❖ Zone de recherche Inversée, les adresses IP sont résolues en noms

- **Résolveurs DNS**

  Un résolveur DNS est un service qui a recours au protocole DNS pour requérir des informations auprès de serveurs DNS. Les résolveurs DNS communiquent soit avec des serveurs DNS distants soit avec le programme de serveur DNS qui s'exécute sur l'ordinateur local. Dans Windows server 2008, la fonctionnalité de résolveur DNS est effectuée par le service Client DNS.

- **Enregistrement de ressources**

  Les enregistrements de ressources sont des entrées de base de données DNS qui servent à répondre aux requêtes des clients DNS. Chaque serveur DNS contient les enregistrements de ressources dont il a besoin pour répondre aux requêtes qui portent sur sa portion de l'espace de noms DNS. Les enregistrements de ressources sont chacun décrits comme un type d'enregistrement spécifique, comme une adresse d'hôte IPv4,une adresse d'hôte IPv4, un pointeur …

II.7.7 Déploiement de deux serveurs Web

Les sites Web modernes fournissent des fonctionnalités comparables à celles présentes dans de nombreuses applications clientes installées localement. Ils permettent d'accéder à des bases de données dans des environnements publics et intranet et autorisent une certaine personnalisation en fonction de besoins particuliers. Les applications ou les services Web se basent sur diverses normes, protocoles et technologies de développement.

Le système d'exploitation Windows Server 2008 inclut IIS 7.0 (**Internet Information Services**), une plate-forme de services Web complète capable de prendre en charge plusieurs types de contenu et d'applications Web. IIS 7.0 propose de nettes améliorations au niveau de la gérabilité, de l'extensibilité et de la fiabilité. Elle assure également une rétrocompatibilité pour supporter les millions de sites Web déjà hébergés sur les versions précédentes d'IIS.

Dans cette partie, vous apprendrez à installer et configurer les rôles Serveur Web (IIS) et Serveur d'applications sous Windows Serveur 2008. Vous pouvez activer d'innombrables fonctionnalités et services selon les besoins de votre environnement. Ces informations vous permettront de déployer et configurer IIS et ses fonctionnalités dans des environnements de production.

II.7.8 Sécurité sur des serveurs Web

IIS 7.0 propose une large gamme de fonctionnalités et options permettant de prendre en charge différent types de services et application Web. Grâce à l'utilitaire Gestionnaire de serveur,

l'installation d'IIS et de ses fonctions et options associées est plus simple. En tant qu'administrateur système, vous êtes chargé de déployer IIS en fonction des besoins et exigences différents. Par conséquent, il est essentiel de connaitre la conception d'IIS avant d'apprendre comment installer les rôles Serveur Web et Serveur d'application.

II.7.8.1 Cas d'utilisation d'un serveur Web

Le principal avantage d'utiliser du contenu et des applications Web est l'accessibilité depuis une large gamme d'ordinateurs clients.

La plate-forme IIS a été conçue pour prendre en charge une variété de scénarios. En voici quelques exemples :

- **Site Web publics** :
  La plupart des entreprises ont des besoins relativement simples pour communiquer des informations sur Internet. Par exemple, une petite entreprise voudra sûrement proposer des informations de contact et des détails sur ses services sur un site Web simple.
- **Achats en ligne :**Internet est devenu un centre commercial qui permet aux vendeurs d'afficher et de vendre une grande variété de produits. Les sites en ligne proposent des paniers d'achat, des traitements de commandes et du support client.
- **Intranet :** Le Web propose une méthode simple pour tous les utilisateurs d'une organisation d'accéder et de présenter du contenu. Des tâches comme créer des notes de frais ou vérifier les bénéfices peuvent souvent être effectués en ligne sans avoir à contacter le personnel interne.
- **Applications d'entreprise :** Les applications sectorielles d'entreprise doivent souvent déployer et gérer des installations côté client. Pour atténuer certaines de ces problèmes, de nombreuses organisations ont créé des applications internes auxquelles les navigateurs Web peuvent accéder. Il s'agit autant de sites basiques à fonction unique que de grands systèmes distribués.
- **Applications Internet :** Les utilisateurs peuvent accéder à leur courrier électronique et créer des documents par exemple sans installer d'applications sur leurs ordinateurs. Les organisations et les équipes peuvent aussi profiter de l'accès sécurisé aux applications d'entreprise via Internet lors de leurs déplacements et s'ils travaillent à distance.
- **Extranet :** Les entreprises collaborent fréquemment avec d'autres organisations pour obtenir des services. Un scénario extranet est un cas ou les utilisateurs extérieurs à l'organisation peuvent accéder à des données. La sécurité est un souci important, mais les applications Web

représentent une méthode standard grâce à la quelles les utilisateurs peuvent accéder aux informations dont ils ont besoins

- **Hébergement Web :** De nombreuses sociétés se proposent d'héberger des sites Web pour leurs clients. Ces sociétés exécutent un très grand nombre de site Web sur un seul serveur physique, c'est pourquoi il est important de garantir la sécurité. Les performances et la fiabilité.

II.7.8.2 Les services de rôle Internet Information Service (IIS)

Les services de rôle définissent quelles fonctions et options spécifiques de la plate-forme IIS sont disponibles sur le serveur Web local. Une fois que vous avez installé IIS 7.0 sur un ordinateur équipé de Windows Server 2008, vous pouvez ajouter des composants en utilisant le Gestionnaire de serveur.

Les services de rôle IIS sont organisés en plusieurs domaines :

- ✓ Fonctionnalités http communes
- ✓ Développement d'applications
- ✓ Intégrité et diagnostics
- ✓ Sécurité
- ✓ Performances
- ✓ Outils de gestion
- ✓ Service de publication FTP

II.7.9 Network Policy server(NPS)

NPS, ou Network Policy server, est un des rôles disponible sur Windows 2008 server. Il est le remplaçant d'IAS (Internet Authentication Service) disponible sur Windows 2003 Server. Au même titre qu'un serveur RADIUS, NPS gère l'authentification et les autorisations selon les différents modes de connexion (locale, VPN…)

Il permet entre autre :

- L'accès aux ressources locales via une connexion à distance (VPN…)
- Authentification via Active Directory
- Gestion des droits via GPO

II.7.9.1 Quelle relation avec NAP (Network Access Protection)

En effet, NPS propose les mêmes fonctionnalités qu'IAS et plus. NAP (Network Access Protection) est la force de NPS. Il introduit des notions de bulletins de santé (ou System Health

Validators), de serveurs de remédiation, de politique de santé… NPS agit comme serveur d'évaluation de santé pour NAP, NAP n'est pas un rôle mais une fonctionnalité du rôle NPS.

II.7.9.2 Les stratégies RADIUS

Les stratégies de requêtes de connexion : elles sont le point d'entrée des requêtes clients. C'est sur cette page qu'il nous faudra créer nos stratégies de connexion, connexion (DHCP, VPN, HRA etc).

Une stratégie de connexion NPS se décompose en deux parties :

1) **Les stratégies de requêtes de connexion**

Elles sont le point d'entrée des requêtes clients. C'est sur cette page qu'il nous faudra créer nos stratégies de connexion, généralement une par méthode de connexion (DHCP, VPN, HRA etc). Une stratégie de connexion NPS se décompose en deux parties

a. **Les conditions**

Configurez ici au minimum une condition qui permettra à cette règle d'être sélectionnée pour cette demande de connexion. Vous pouvez ajouter des critères comme l'appartenance de l'utilisateur à un groupe spécifique, l'heure de la demande ou encore son adresse IP. Pour chaque demande de connexion, NPS parcourra chaque règle de connexion (par ordre de priorité) jusqu'à ce qu'il en trouve une dans laquelle les conditions spécifiées correspondent aux paramètres de cette demande. Si aucune règle de connexion ne correspond avec la demande en cours, NPS renverra un accès refusé au client RADIUS.

Les paramètres de configuration

Lorsque le serveur NPS a trouvé une règle correspondant aux conditions précédentes, il consultera les paramètres de connexions pour savoir comment traiter cette demande. L'option importante dans cet onglet est la manière dont l'authentification sera réalisée. Il est possible de rediriger les règles sur un groupe de serveur RADIUS ,autoriser l'accès sans vérifier l'autorisation (dans ce cas, toutes les requêtes de connexion correspondantes à cette règle seront automatiquement approuvées) ou encore, ce qui est le cas par défaut, de traiter les demandes sur ce serveur NPS. Dans ce cas, la requête va être analysée dans les stratégies réseau.

b. **Les stratégies réseau**

Deuxième étape du traitement d'une requête de connexion, il s'agit de vérifier dans les stratégies réseau si la demande doit-être ou non autorisée. Pour cela, il faut créer des règles de réseau. Ces règles se décomposent en trois parties :

- **Les conditions**

Comme pour les requêtes de connexion, il s'agit de spécifier des critères permettant au serveur NPS de définir quelle règle il doit utiliser pour traiter cette demande. Dans le cas de NAP, c'est ici qu'il sera possible de vérifier si la requête provient d'un client compatible avec NAP, et si oui, si le client est conforme avec les règles de santé de l'entreprise.

- **Les contraintes de connexion**

Lorsque NPS trouve dans la liste une règle de réseau utilisable pour autoriser cette demande de connexion, il consulte la liste des contraintes. Il s'agit notamment dans notre cas des méthodes d'authentification. Il est possible de sélectionner des méthodes conventionnelles (MS-CHAP v2, EAP) mais aussi d'effectuer uniquement un test de santé, ce qui aura pour effet de ne pas authentifier l'utilisateur. Cela est par exemple utile dans le cas de l'enforcement par DHCP qui ne permet pas de fournir les informations d'authentification.

- **Les paramètres de configuration de la règle**

C'est la partie la plus importante en ce qui concerne NAP. C'est ici qu'il nous est possible de spécifier si le client peut accéder à l'intégralité du réseau (cas où la machine cliente est considérée comme « en bonne santé » vis à vis des règles de l'entreprise) ou si elle doit être restreinte à la zone de quarantaine (machine non-conforme). C'est aussi dans cet onglet qu'il est possible de spécifier si l'auto-remédiation (faculté d'indiquer au client non-conforme ce qu'il doit faire pour devenir conforme) doit être utilisé.

2) **Les stratégies de santé**

C'est ici qu'il nous faudra configurer les règles de l'entreprise en matière de « bonne santé ». Typiquement, il nous faudra créer deux stratégies de santé : la première indiquant que si le client passe avec succès tous les tests d'état il sera considéré comme « conforme » et la deuxième dans laquelle on pourrait dire que si le client échoue à un seul de ces tests il doit être considéré comme « non-conforme »

II.7.10 SAN

Un SAN (Storage Area Network) est un réseau spécialisé permettant de partager de l'espace de stockage à une librairie de sauvegarde et à des serveurs. Le réseau SAN est basé sur le protocole Fibre

Channel (FC). Le SAN est un réseau sur lequel sont connectés des serveurs et des périphériques de stockage. Chaque serveur peut accéder à chaque périphérique.

II.7.10.1 Concept du SAN

Le réseau SAN (Storage Area Network) est une technologie de **stockage en réseau**.
C'est un réseau physique en fibre optique, dont le but est de permettre la mise en relation de serveurs avec des baies de disques. Les données stockées sont routées et hiérarchisées via des commutateurs.
Le SAN connecte l'ensemble des unités de stockages et des serveurs.

Cette nouvelle solution en matière de stockage permet :

- Des regroupements de disques et de bandes.
- Des partages des ressources de stockage entre un nombre très important de systèmes de traitement et d'utilisateurs.
- Des partages de données hétérogènes.
- Un accès plus rapide aux données.
- La sauvegarde et la restauration de données hors LAN et sans serveur (soulagement du LAN des charges induites par le transfert massif de données).
- La résolution de problèmes de connectivité entre plusieurs serveurs et unités de stockage.

Ces points forts impliquent une amélioration du rendement ainsi qu'une simplification de la gestion.

II.7.10.2 Les avantages et inconvénients du SAN

II.7.10.2.1Avantage

Cette nouvelle technologie de stockage en réseau permet :

- La consolidation des informations au sein d'un réseau de stockage centralisé.
- La connexion de l'ensemble des ressources de stockage.
- Le soulagement du trafic réseau.

Ces trois points impliquent une réduction du temps de latence ainsi qu'une utilisation des ressources plus efficaces.

- L'accélération de l'extraction des données.

La technologie « Fibre Channel » utilise une boucle arbitrée offrant des vitesses de transfert de données réelles de 800 Mb/s.

- La prise en charge d'un nombre quasi illimité de matériels (si l'infrastructure est complète : serveurs, multiplexeurs, passerelles, unités de stockage).
- La simplification des sauvegardes et de la restauration.
- La prise en charge des techniques du type : déroutement, clusterisation, mise en miroir et réplication (RAID…).

Implique une protection contre la perte de données et une amélioration de la disponibilité des informations.

- Une évolutivité exceptionnelle.

Idéal pour les réseaux connaissant une croissance rapide ou qui ont besoin d'augmenter leur capacité de stockage de façon sporadique.

II.7.10.2.2 Inconvénients

Malgré tous les avantages de cette nouvelle technologie, une telle infrastructure implique quelques inconvénients... :

- Son prix !!! Plutôt élevé.

Il devient donc intéressant de passer au SAN à partir d'une cinquantaine de ports (soit trois commutateurs de 16 ports).

- Son manque de standardisation génère certains problèmes d'interopérabilité. Quelques fournisseurs recommandent d'acheter tous les composants du réseau SAN auprès d'une source unique, d'autres proposent des combinaisons de produits qui fonctionnent le mieux ensemble.

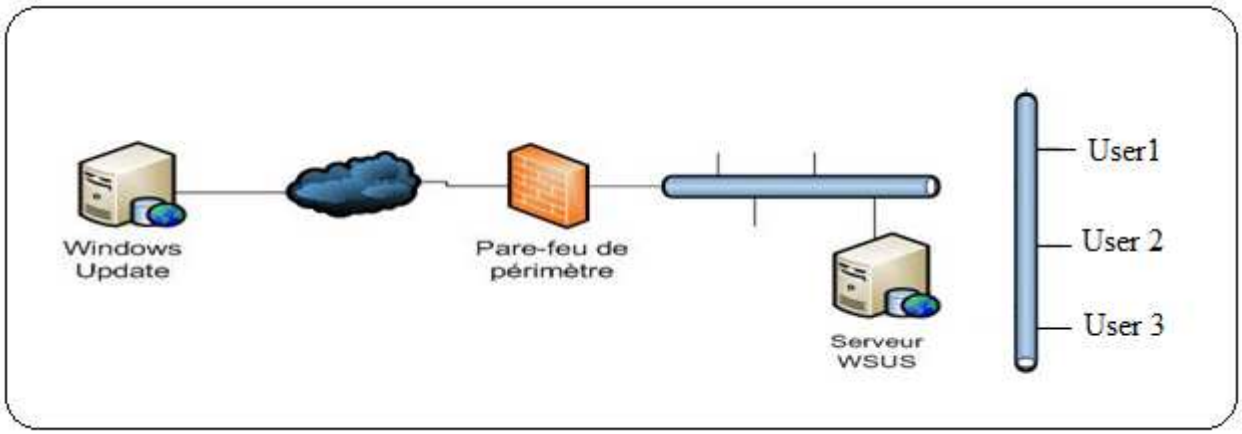
- La gestion des composants est plus difficile en fonction de l'augmentation en taille et en complexité du réseau SAN.

D'où la nécessité de choisir un logiciel de gestion robuste, permettant à partir d'une interface unique de contrôler l'ensemble du réseau de stockage.

II.7.11 Windows Server Update Service (WSUS)

Windows Server Update Services est un composant complémentaire gratuit pour Windows Server 2008 qui fonctionne comme un serveur Microsoft Update dans votre environnement. Plutôt que chaque ordinateur de votre entreprise télécharge des mégaoctets de données sur Internet, vous pouvez configurer un serveur WSUS pour qu'il soit le seul ordinateur à télécharger des mises à jour. Vous configurer ensuite tous les autres ordinateurs de l'entreprise pour qu'ils se servent du serveur WSUS comme source des fichiers de mises à jour.

- ✓ Type de déploiement utilisé dans notre étude



FigureII.16: Windows Server Update Services

- Méthode la plus simple: un serveur derrière votre pare feu qui se met à jour directement sur les serveurs de Microsoft Update
- Les mises à jour sont déployées par le biais du client de mises à jour automatique: il faut leur renseigner l'adresse du site web sur lequel il pourra récupérer les correctifs
- Création d'un site web par défaut ou alors sur un site personnalisé

Lors de l'installation, vous devez indiquer votre source de mise à jour. Mais, si pour une raison ou pour une autre vous avez besoin de changer cette source de mise à jour , il est possible à tout moment de modifier les informations que vous avez spécifiées lors de l'installation.

II.7.12 Serveur de messagerie

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique (courriel). Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie, soit un courrielleur web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages.

La plupart des serveurs de messagerie possèdent ces deux fonctions (envoi/réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs.

II.7.12.1 Microsoft Exchange Server

II.7.12.1.1 Définition

Est un logiciel collaboratif pour serveur de messagerie électronique créé par Microsoft, pour concurrencer Lotus Notes /Domino Server d'IBM, Mdaemon d'Alt' Net plus récemment des logiciels sous Linux tels que Scalix ,Zimbraou OBM. C'est un produit

de la gamme des serveurs Microsoft, conçu pour la messagerie électronique, mais aussi pour la gestion d'agenda ,de contacts et de tâches ,qui assure le stockage des informations et permet des accès à partir de clients mobiles (Outlook Mobile Access, Exchange Active Server Sync) et de clients Web (navigateurs tels que Internet Explorer ,Mozilla Firefox, Apple Safari ,Google Chrome…)

Cette solution a été choisie car elle possède l'avantage d'avoir un réseau uniforme et ainsi éviter d'éventuelles sources de conflits.

II.7.12.1.2 Pourquoi utiliser Microsoft Exchange ?

- Cette solution a été choisie car elle possède l'avantage d'avoir un réseau uniforme et ainsi éviter d'éventuelles sources de conflits.
- Enfin, Microsoft Exchange est très utilisé dans les entreprises,

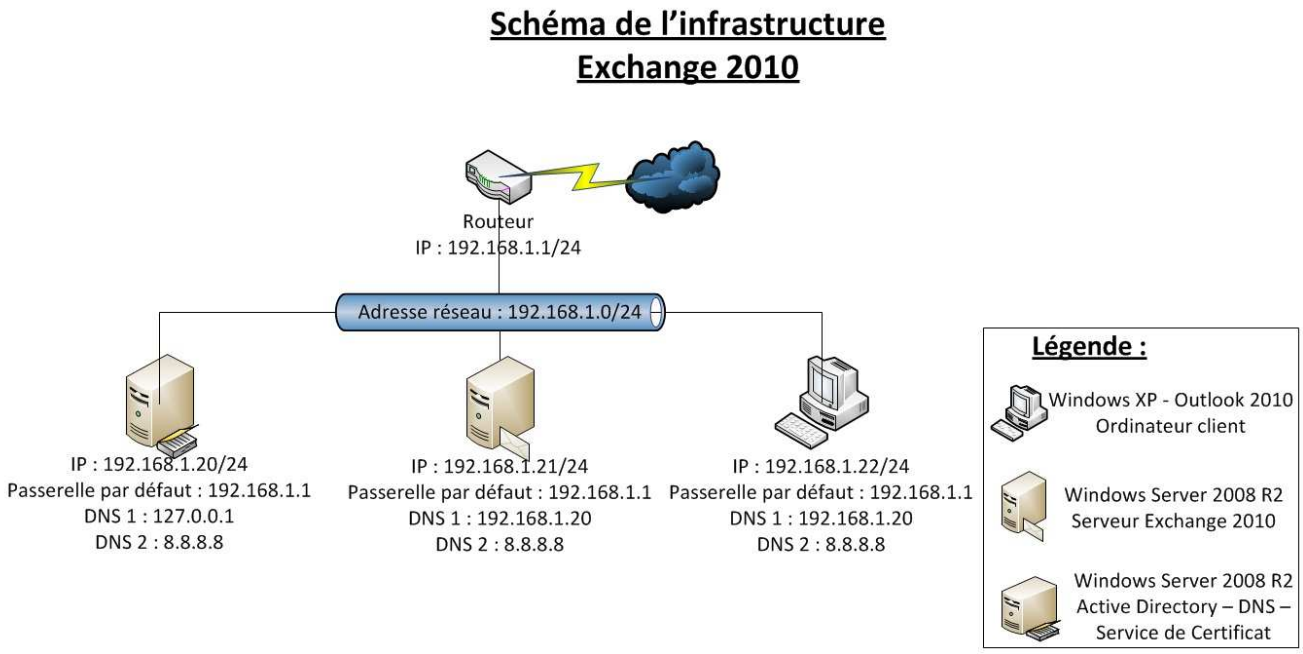


Figure II .17 : Schéma de l'infrastructure Exchange 2010

II.7.13 Firewall ASA Cisco

a. **Présentation d'un firewall ASA Cisco**

L'idée de la conception de l'Adaptative Security Appliance (ASA) est apparue par CISCO, lors de la mise en place, de la solution Self-Defending Network (Le réseau qui se défend tout seul). En effet, en associant un pare-feu très puissant à un système qui offre les services VPN, l'ASA est la solution proposée par Cisco pour garantir un réseau accessible de l'extérieur et sécurisé. Il met en place une défense face aux menaces, et bloque les attaques avant qu'elles ne se propagent dans le reste du réseau.

Grace à une interface graphique et une utilisation simplifiée des fonctionnalités, l'ASA offre aux entreprises qui souhaitent sécuriser leur réseau un outil complet et raisonnablement facile d'utilisation.

b. Présentation de l'interface graphique

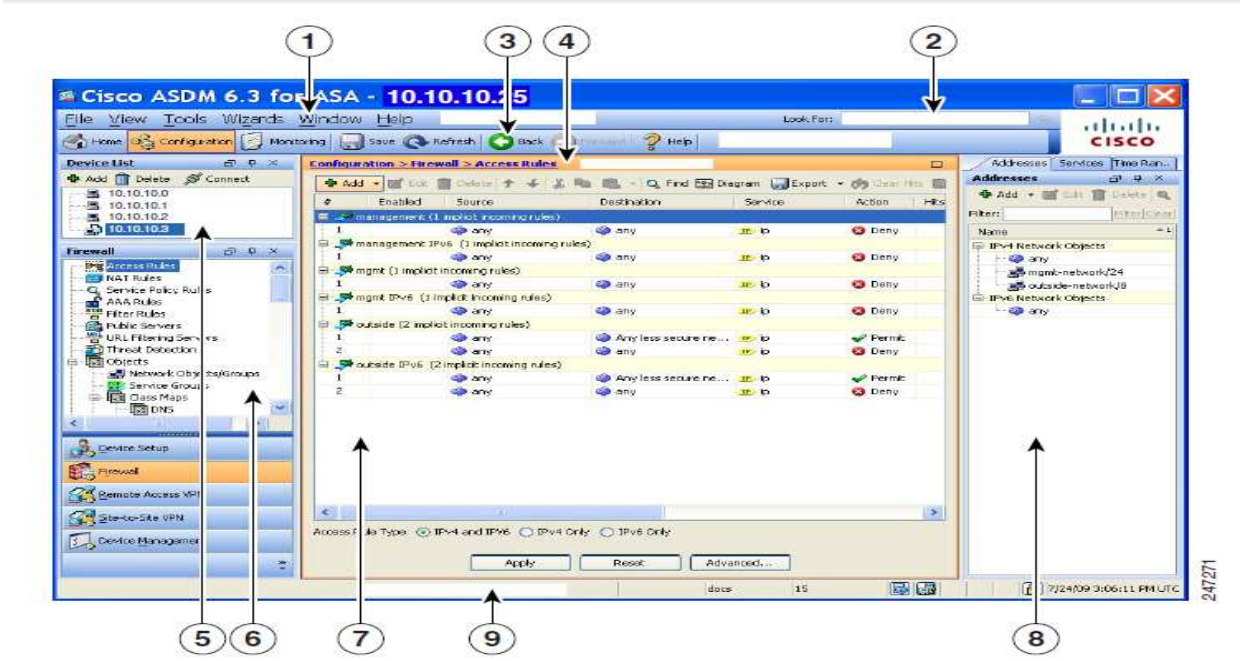


Figure II.18:Présentation graphique de l'interface du ASA Cisco

1-La barre de menu 2- Champ de recherche

3- Barre d'outils 4- Chemin de navigation

5- Le volet des listes d'appareil 6- Volet de navigation gauche

7- Volet de contenu 8- Navigation de droite

9- barre d'état

II.7.14 Threat Management Gateway (TMG)

a. Présentation de la TMG

Microsoft Forefront Threat Management Gateway (Forefront TMG),anciennement connu sous le nom Microsoft Internet Security and Acceleration Server (ISA Server),est une solution de sécurité réseau et de protection de Microsoft Windows ,décrit par Microsoft, permet aux entreprises en autorisant aux employés de façon sécuritaire et productive utilisation d'Internet

pour le travail sans se soucier des logiciels malveillants et autres menaces». La TMG est une solution logicielle de type serveur de Microsoft composée de différents éléments ayant plusieurs rôles:

- Pare-feu: Système qui permet la protection d'un ordinateur face à des intrusions provenant d'un autre réseau (Internet par exemple).

- Serveur de Proxy/Proxy-cache: Système intermédiaire entre le client et le serveur. Il va faire une requête sur le serveur à la place du client quand celui-ci ne peut pas accéder directement à la ressource. Le Proxy-cache quant à lui, va demander au serveur les informations, les transmet au client et garde une copie de celles-ci sur un espace disque (le cache) définit pour pouvoir ensuite servir plus rapidement les autres clients qui feront la même requête ultérieurement.

- Serveur VPN (Virtual Private Network):

Réseau Virtuel privé comportant des réseaux interne a une organisation.

VPN de site à site –principe

- Interconnecté des site distants (ex :une agence et la maison mère)au travers d'un réseau publique via un tunnel sécurise
- Pour les utilisateurs, les réseaux distant sont vus une extension de réseau local

VPN nomade –principe

- Permettre à utilisateurs connectés sur un réseau publique(internet)de ce connecter à leur réseau d'entreprise(ou uniquement à des ressources spécifiques)de manière sécurisé

b. Avantages et fonctionnalités TMG 2010

✓ **TMG 2010 bloque efficacement l'accès aux sites malveillants**

Utilise des données en provenance de différents fournisseurs de filtres d'URL, et des technologies contre les logiciels malveillants et l'usurpation d'identité (phishing) qui équipent déjà Internet Explorer 8. Le filtrage des sites Web permet aussi de bloquer l'accès aux sites inappropriés selon les choix d'entreprise.

✓ **Empêche l'exploitation de vulnérabilités**

Empêche les intrusions qui exploiteraient des vulnérabilités du navigateur ou de ses modules additionnels.

✓ **Détecte les logiciels malveillants du Web**

Assure une détection précise grâce à un moteur d'analyse qui combine des signatures génériques et des technologies heuristiques pour anticiper la diffusion de nouvelles variantes n'ayant pas de signatures spécifiques.

✓ **Assure les principales fonctions de protection du réseau**

Reprend les technologies de protection du réseau de Microsoft Internet Security and Acceleration Server 2006, la version précédente de Forefront TMG 2010. Cela permet de déployer un pare-feu de périmètre et une passerelle sécurisée pour des applications comme Microsoft Exchange Server et Microsoft SharePoint®.

✓ **Inspecte le trafic Web chiffré**

Examine le trafic Web chiffré SSL, ce que ne fait pas un pare-feu. Dans ces sessions chiffrées, Forefront TMG 2010 peut détecter un logiciel malveillant et contrôler l'accès à des sites interdits par l'entreprise.

✓ **Administration simplifiée**

-Centralise la gestion sur une seule console simple d'emploi

Permet aux administrateurs de créer et de gérer toutes les fonctions de sécurité Web à partir d'une seule console dans des environnements distribués.

-Fournit des rapports complets

Génère rapidement des rapports de sécurité qui peuvent être adaptés pour répondre à des besoins spécifiques de l'entreprise. S'intègre à une infrastructure Microsoft SQL Server Express ou SQL Server pour créer des rapports personnalisés.

c. La création de La DMZ avec la TMG

✓ Principe de fonctionnement

DMZ veut dire « Zone Démilitarisée », elle est appelée aussi « Réseau de périmètre ». Une DMZ utilise la même interface externe du réseau local de l'entreprise mais sur un réseau différent, il y est installé des serveurs accessibles depuis l'extérieur. L'utilisation d'une DMZ évite que des clients externes accèdent au réseau local, se qui réduit considérablement les risques d'intrusions.

Il y a deux types de DMZ : La DMZ privée et la DMZ publique.

- **Une DMZ privée** utilise dans son réseau des adresses IP privées. De ce fait, une règle de publication doit être installée sur la TMG pour accéder aux serveurs de la DMZ, ainsi depuis l'extérieur du réseau c'est l'adresse IP de l'interface externe de la TMG qui est employée pour accéder aux serveurs.

- **Une DMZ publique** utilise dans son réseau des adresses IP publiques. A ce moment là, La TMG fait office de routeur entre son interface externe (coté Internet) est l'interface coté DMZ. Pour accéder depuis Internet aux serveurs situés dans la DMZ publique on utilise l'adresse IP propre à chaque serveur.

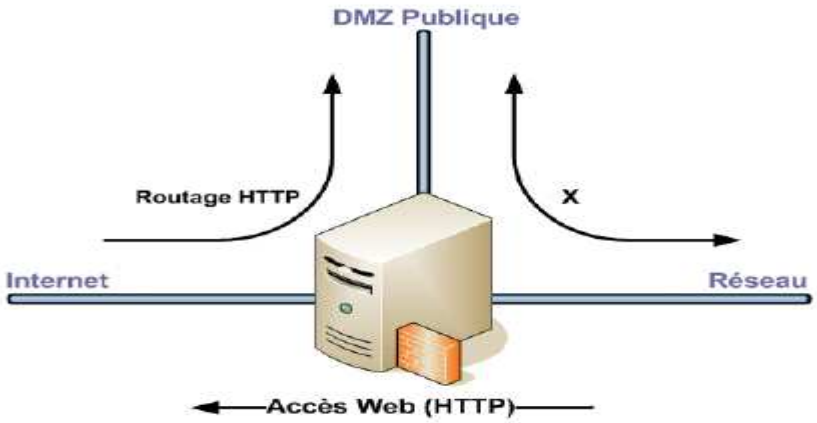


Figure II.19: **DMZ Publique**

Remarque: Une DMZ publique n'est accessible que d'un réseau externe et pas du réseau interne, sans cela des risques d'intrusions sont possible, il faudra interdire l'accès à la plage d'adresse de la DMZ dans les autorisations d'accès à Internet des clients du réseau.

II.8 Discussions

L'enjeu principal d'une architecture réseau sécurisée, est de pouvoir réglementer les accès aux ressources du réseau tant à partir du réseau local qu'à l'extérieur, tout en essayant au maximum de limiter les failles d'éventuelles attaques ou vols d'informations à fin d'accroître la sécurité du réseau local. En effet, face à des applications telle la messagerie qui permettent la mobilité donc les accès d'origine diverse, il est toujours important de définir une architecture fiable de sécurisation du réseau. L'implémentation d'une telle architecture aboutira à un gain en termes de performance et sécurité du réseau.

CHAPITRE II

Etat de l'art sur la sécurité des réseaux informatique

CHAPITRE III

Implémentation des solutions

III.1 Préambule

L'objectif de cette partie est d'implémenter une politique de sécurité pour une infrastructure réseau par les différentes nouvelles technologies tel que ASA Cisco ,certificat, IPsec, authentification radius..., ces derniers permettent aux clients de l'entreprise de partager des informations et des données en toute sécurité afin d'améliorer sa réactivité, sa compétitivité et ainsi devenir une « entreprise connectée ».

Dans ce chapitre nous allons procéder comme suit:

-Installer Admin kit pour la gestion centralisée d'un antivirus kaspersky (gestion de trafic réseau)

- installation de Windows Server Update Système pour la gestion centralisée de mise à jour système

-Installation d'active directory (la gestion simplifiée)

-Assuré la disponibilité de serveur DHCP

-Création de zones DNS qui permettra la résolution de nom

-Création de deux serveurs web (tolérances aux pannes)

-Configuration d'un ASA Cisco avec GNS3(gestion de trafic réseau)

-Installation de serveur Exchange 2010 qui assure la gestion de messagerie dans l'entreprise

-Installation de la TMG et création de règles de sécurités et de publication Web et Exchange

-Utilisation de la technologie SAN pour le stockage des données

-Utilisation du Backup pour la récupération des données dans le cas de problème (état système active directory)

-configuration ipsec avec certificat contre le Snifing

-configuration de radius server pour authentification sécurisé avec SSL (double authentification, physique et logique)

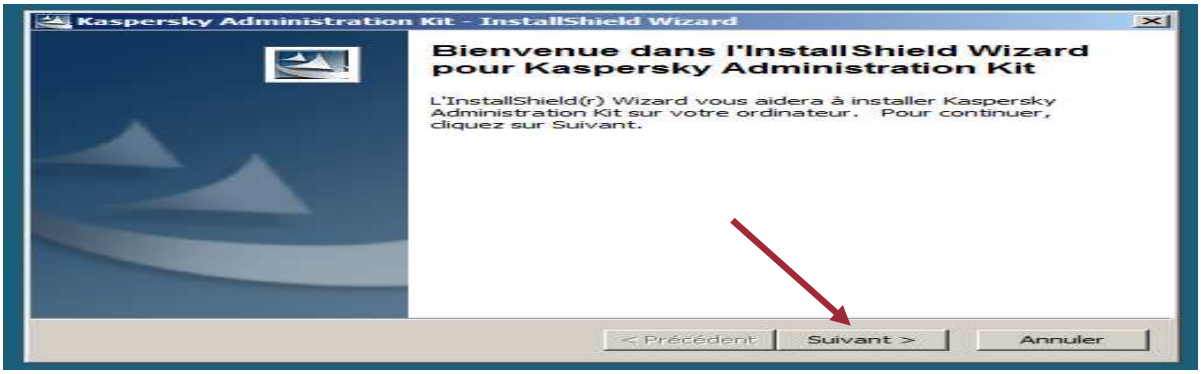
III.2 Installation de Kaspersky admin kit

On a commencé par l'installation de kaspersky parce que c'est la première sécurité de système contre les virus, Worm..., il nous a permit de paramétrer la gestion centralisée pour simplifier l'administration tel que le contrôle des mises jours à distance, déploiement de antivirus à distance et la gestion des postes clients .

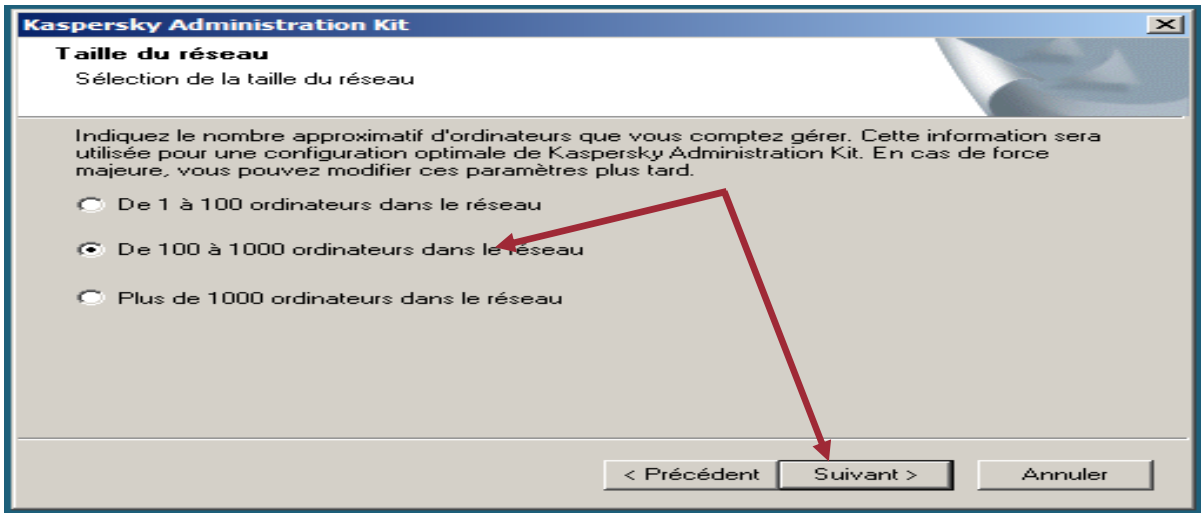
Lancer l'installation de kaspersky après avoir installer les applications suivantes:

SQLEXPR_x64_FRA, NetFx20SP1_x64

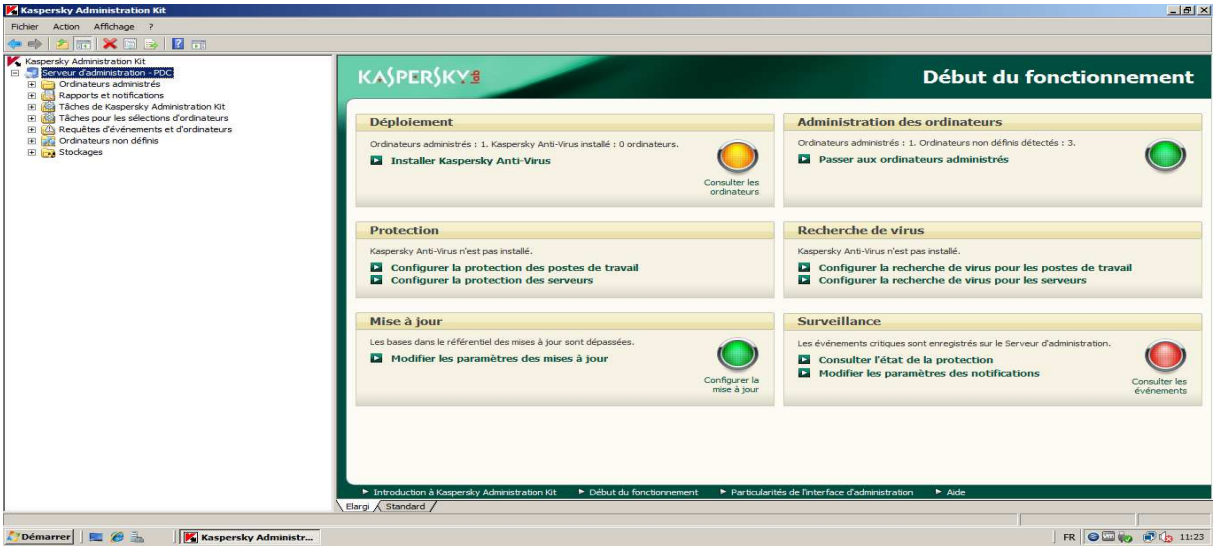
On lance l'application puis suivant



On choisi la taille du réseau selon le nombre d'ordinateurs qu'on a dans l'entreprise



L'affichage de l'interface graphique de kaspersky admin kit



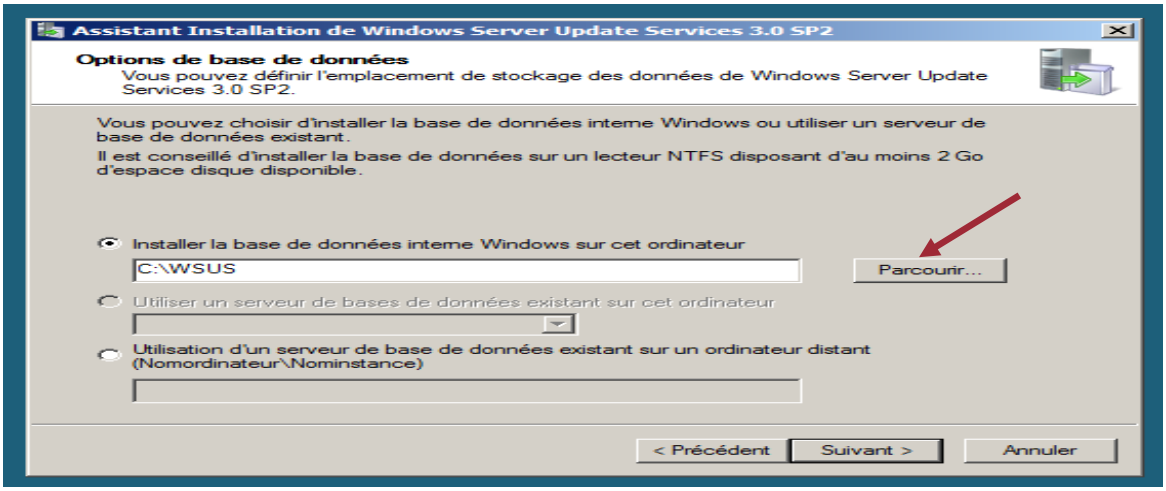
III.3 Installation Windows Server Update Service (WSUS)

Au second plan on a installé le "**Windows Server Update Service** qui permet de déployer les dernières mises à jour de produits Microsoft(correctifs systèmes)sur les ordinateurs de l'entreprise , en même temps minimisé le trafic réseau.

(Au lieu que les clients récupère les mise à jours systèmes sur internet il vont les récupérer à partir du serveur WSUS. Elles représentent 50% de la sécurité système , La plupart des hackers exploitent les failles des mises à jours pour attaquer les systèmes.
Lançant l'assistant d'installation

On choisir l'emplacement de stockage de la sauvegarde

Au début de l'installation, vous pouvez choisir le répertoire d'installation des mises à jour WSUS. Vérifiez que la case **Stocker les mises à jour localement** soit cochée si vous n'avez pas de serveur SQL. Notez aussi que le répertoire par défaut est **C:\WSUS**

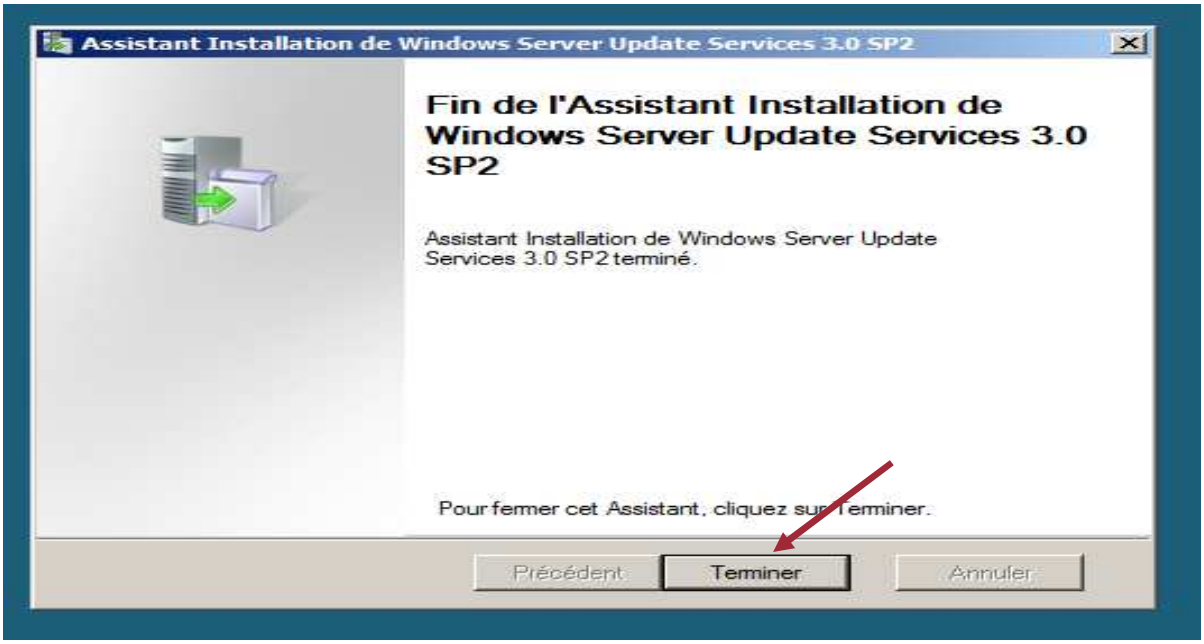


Sélection du site WEB:

Si vous avez déjà installé IIS pour un autre service Web, l'assistant d'installation vous donne le choix pour le site de WSUS:

- le site par défaut **port 80**
- ou alors la création d'un site Microsoft Windows Server Update Service accessible par le **port 8530**: ce numéro de port n'est pas paramétrable.

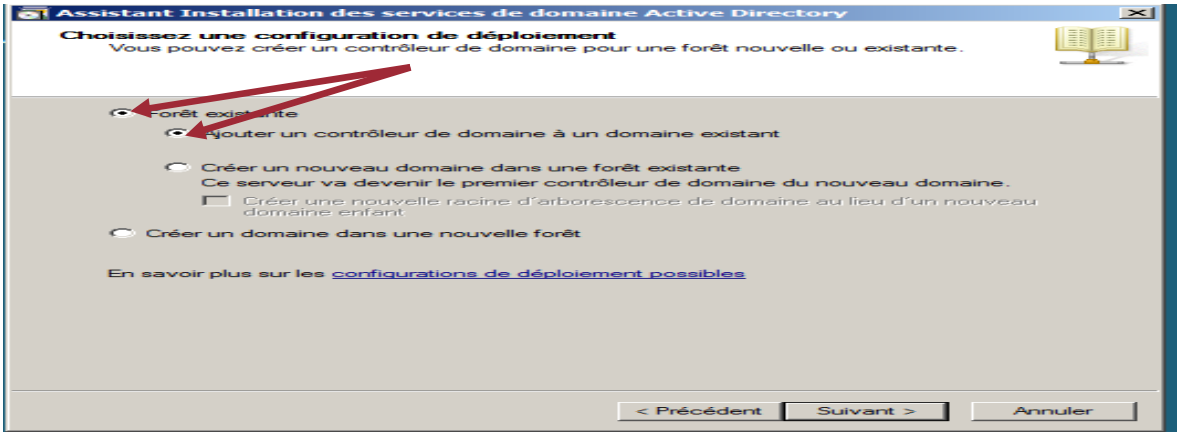
Fin de l'installation



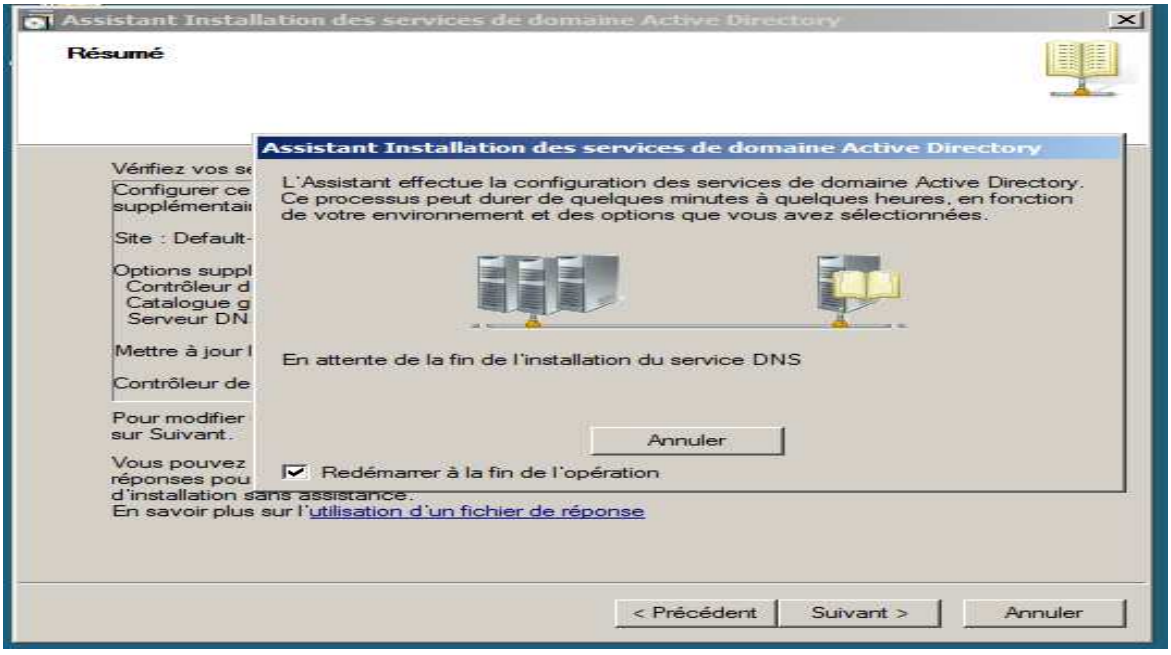
III.4 Réplication d'Active directory

On installe l'active Directory dans **adc** (auxiliaire domaine controler), on choisit **une forêt existante** vue qu'on a déjà un demain existant 2intparteners.com

Cet Active directory nous a permet de représenter et de stocker les éléments constitutifs du réseau (les ressources informatiques mais également les utilisateurs) et d'assurer une gestion centralisée dans toute l'entreprise tel que la planification des tâches.



Fin de l'installation de l'active directory

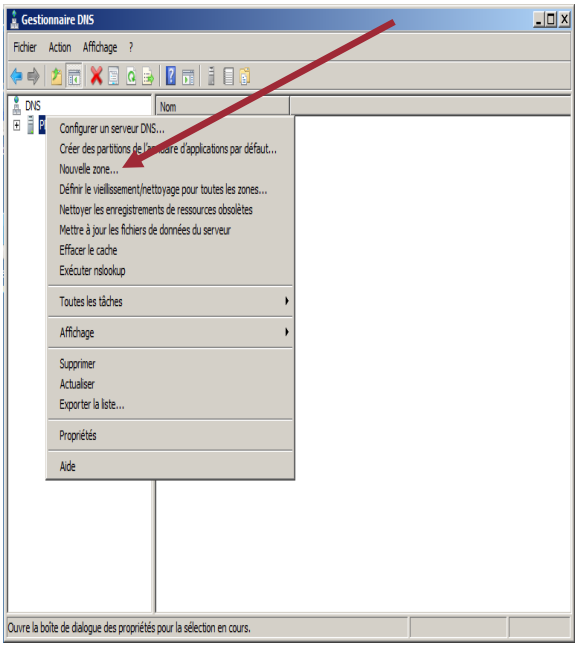


III.5 Configuration d'une zone DNS intégré a la base de données Active directory

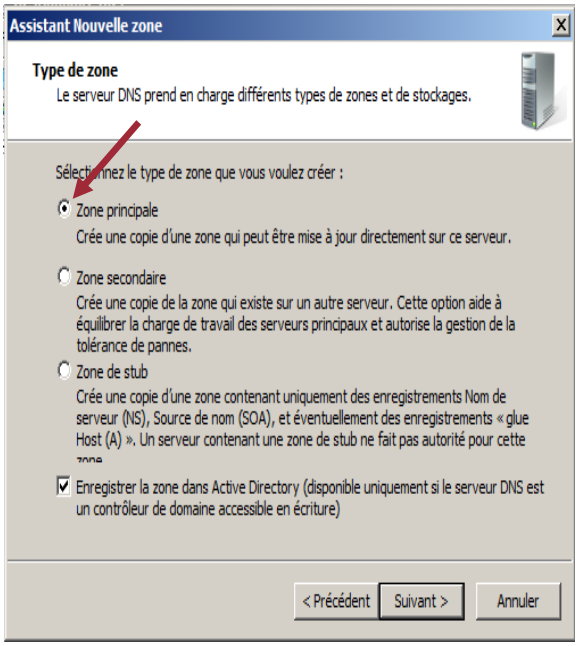
Passons à la création de zone DNS sécurisé dans la base d'Active Directory, Au lieu de choisir de stocker la base des données par défaut dans l'enregistrement WINDOWS\SYSTEM32\DNS , on la stock dans E:\ NTDS

Dans l'outil d'administrateur , **Gestionnaire DNS ,** Nouvelle zone

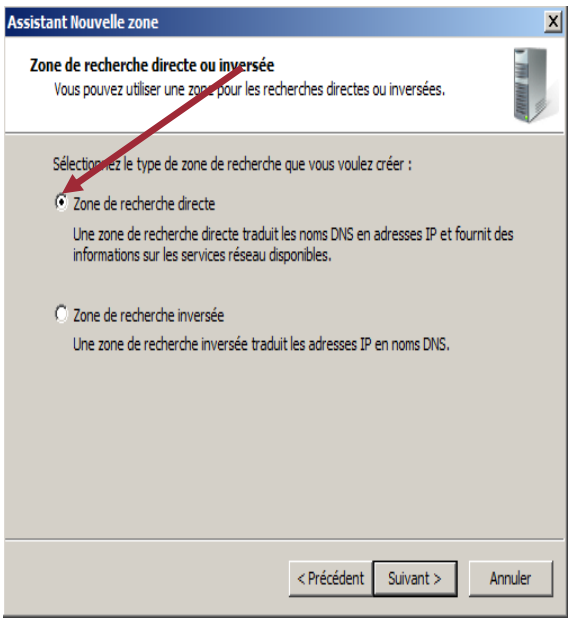
Création d'une Nouvelle zone



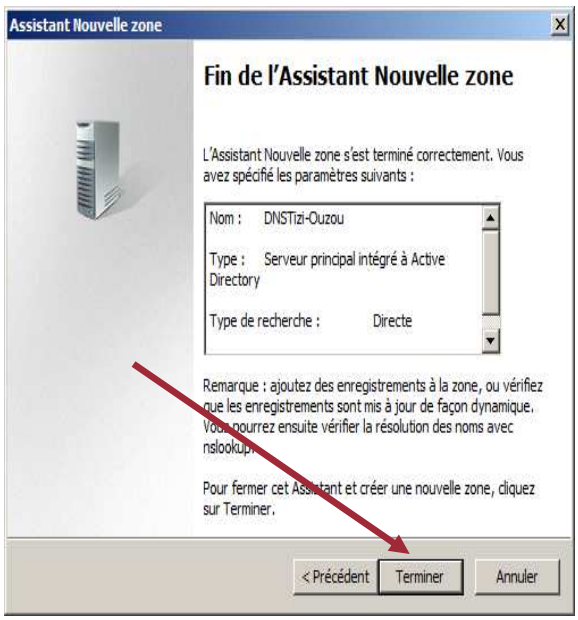
Sélectionner zone principale



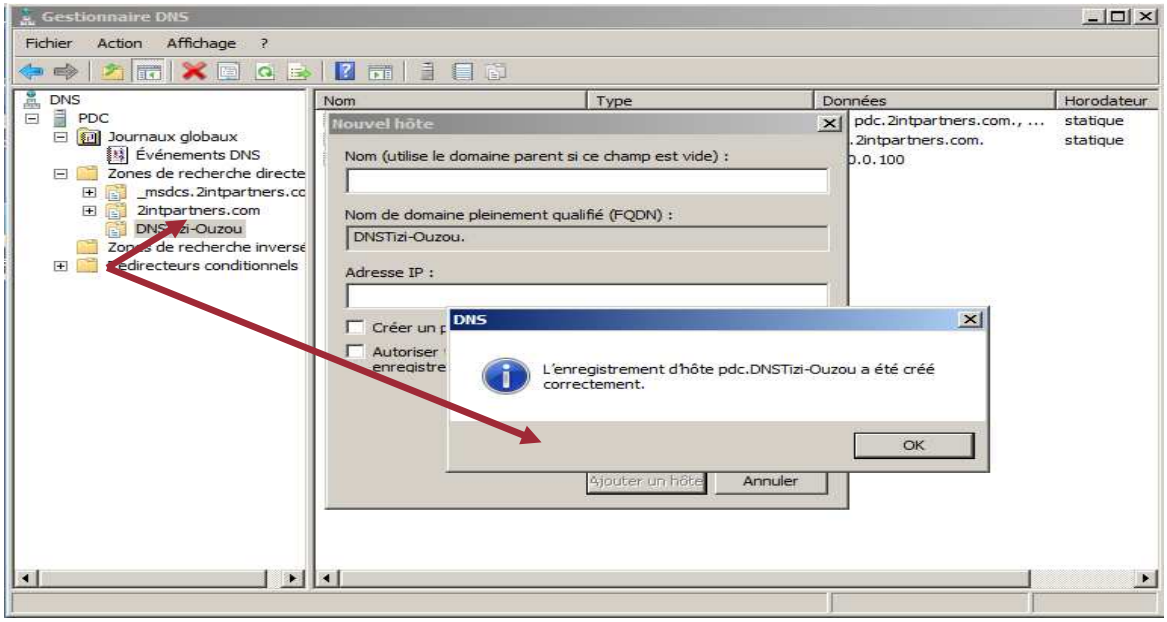
Type de recherche



Fin de création de zone



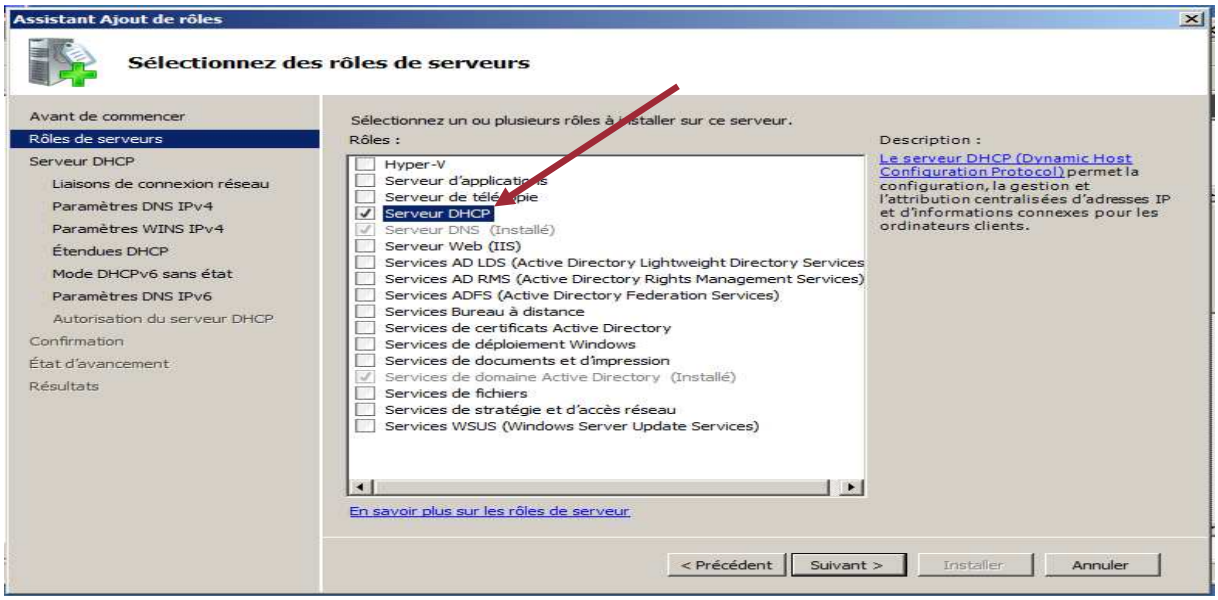
Creation d'hote dans cette zone



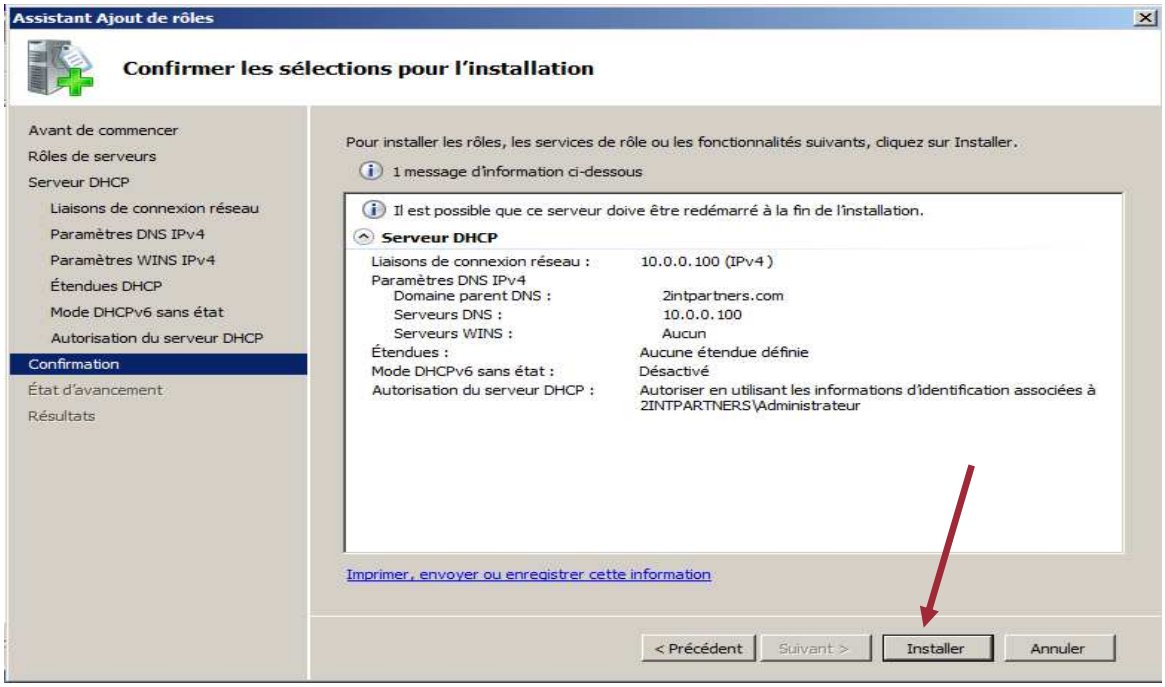
III.6 DHCP Installation et configuration du rôle

On arrive à la partie DHCP (Dynamics Host Configuration Protocol) qui consiste à gérer automatiquement les adresses IP valides aux ordinateurs clients et à d'autres périphériques réseau TCP/IP.

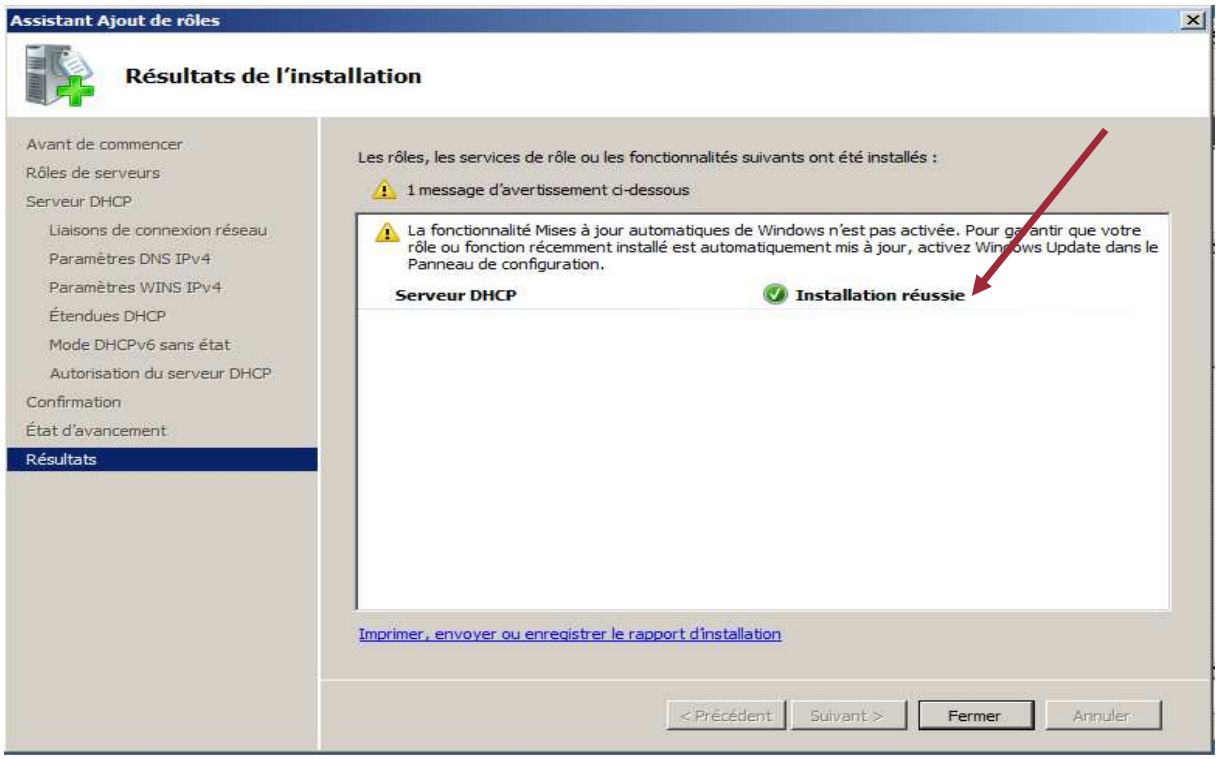
Dans l'assistant ajout de rôles on sélectionne Serveur DHCP



Confirmation et installation des paramètres DHCP

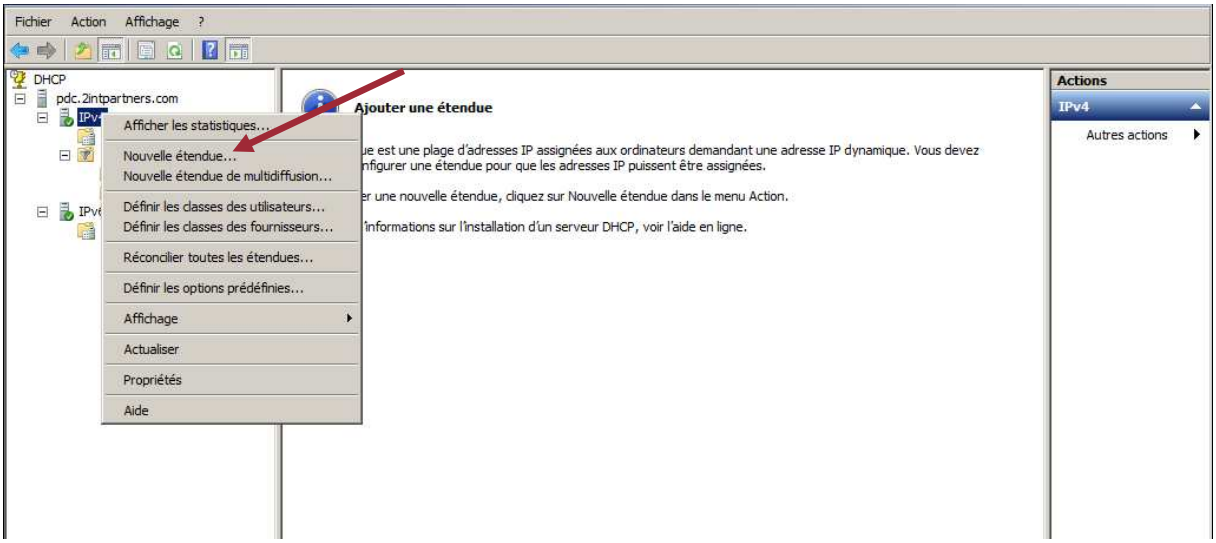


Résultats de l'installation



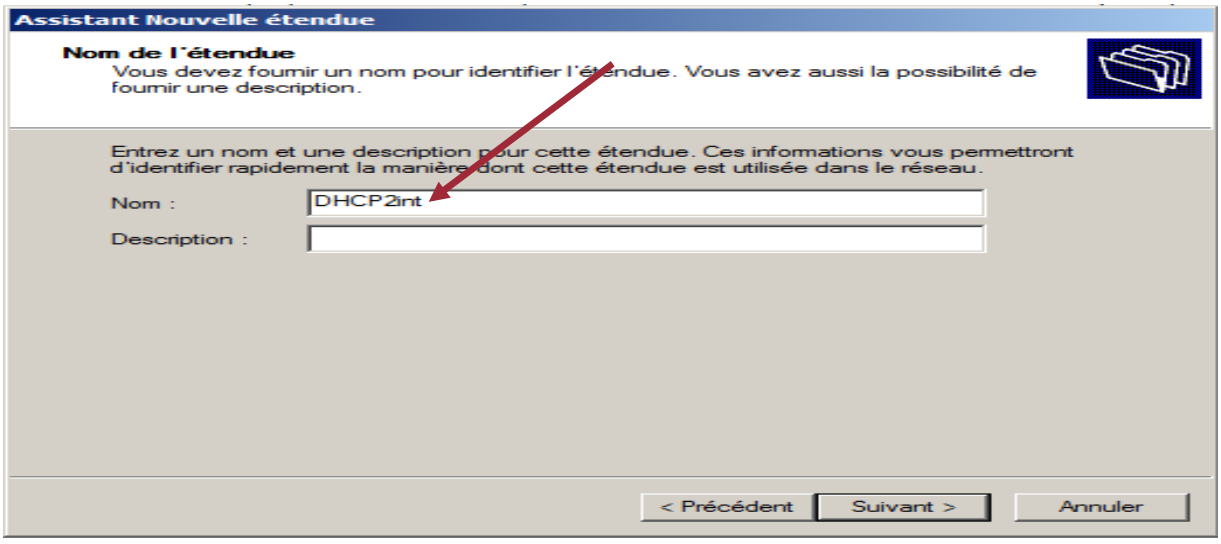
Création d'une nouvelle étendue

- Cliquez sur **Démarrer**, **Outils d'Administrations**, **DHCP**.
- La console DHCP s'ouvre.
- Cliquez avec le bouton droit sur le serveur DHCP où vous voulez créer une nouvelle étendue, puis cliquez sur **Nouvelle étendue**.



Nom de la nouvelle étendue

- Dans l'assistant de création d'une nouvelle étendue cliquez sur **Suivant**.
- Entrer un nom d'étendue dans la zone **Nom**, ce nom doit être explicite.

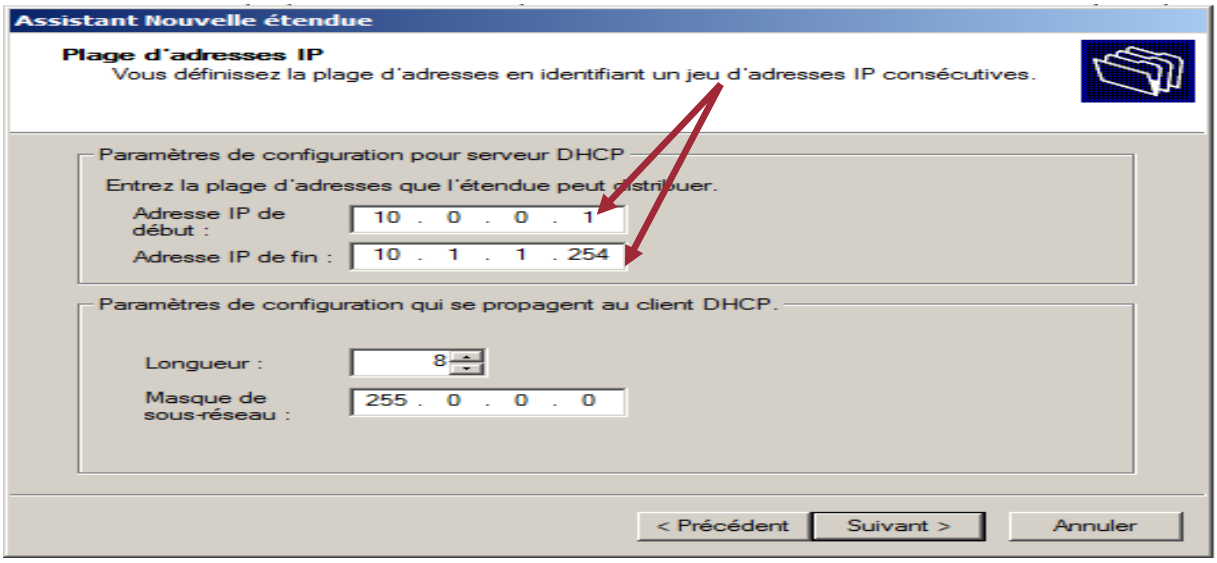


On donne une plage d'adresse de l'étendue à allouer sur le réseau

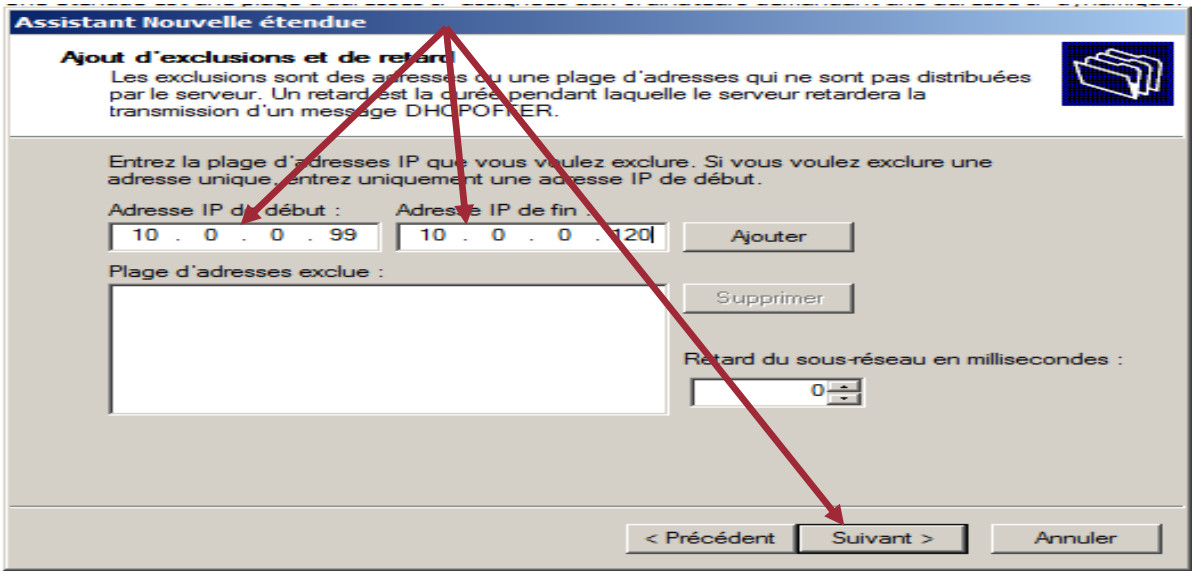
- Cliquez sur **Suivant**.
- Saisissez ensuite la plage d'adresses qui sera allouée.

  Ces adresses vont être par la suite attribuées aux clients, elles doivent être valides et ne doivent pas être déjà utilisées.
- Spécifiez ensuite le masque de sous réseau choisi.

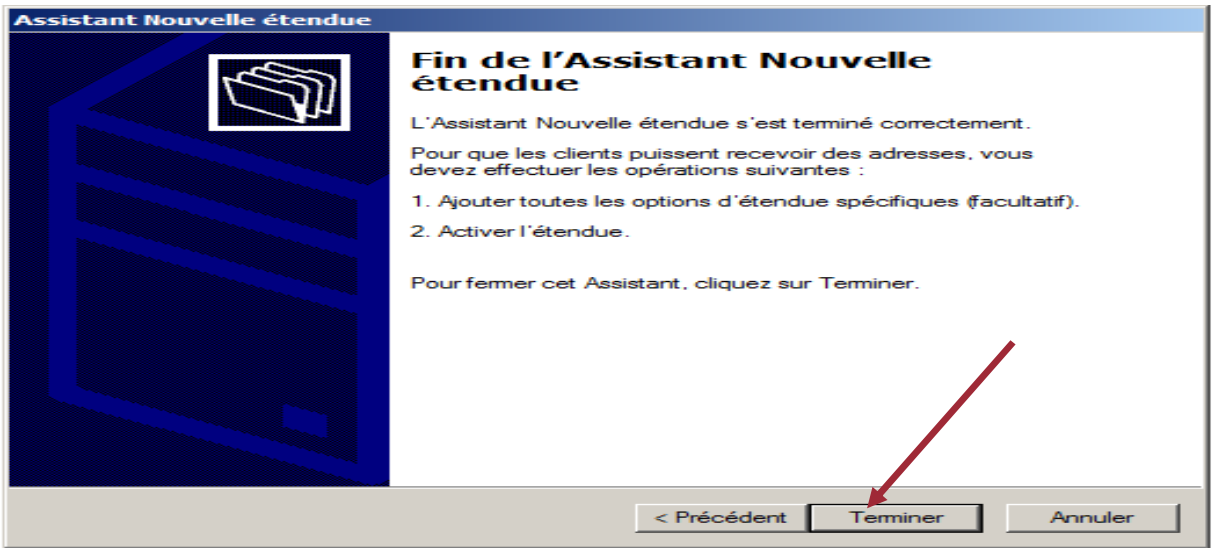
  Cliquez sur **Suivant**



Entrer la plages d'adresses exclus de l'étendue



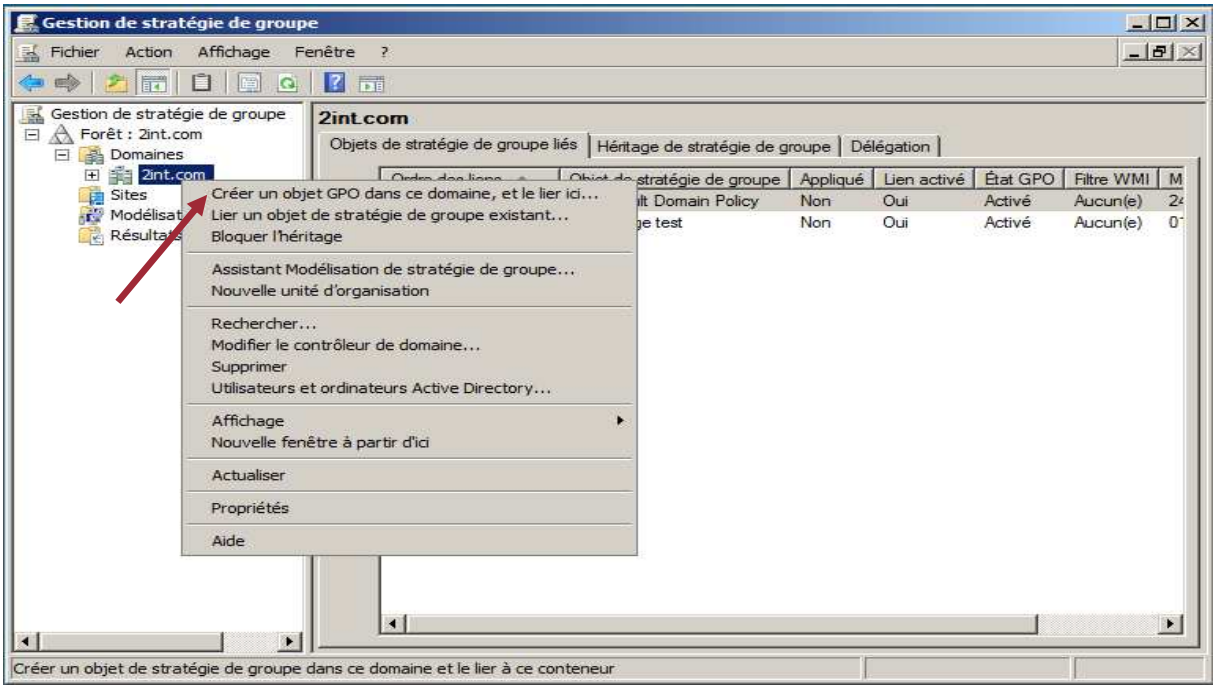
Fin de configuration de l'étendue



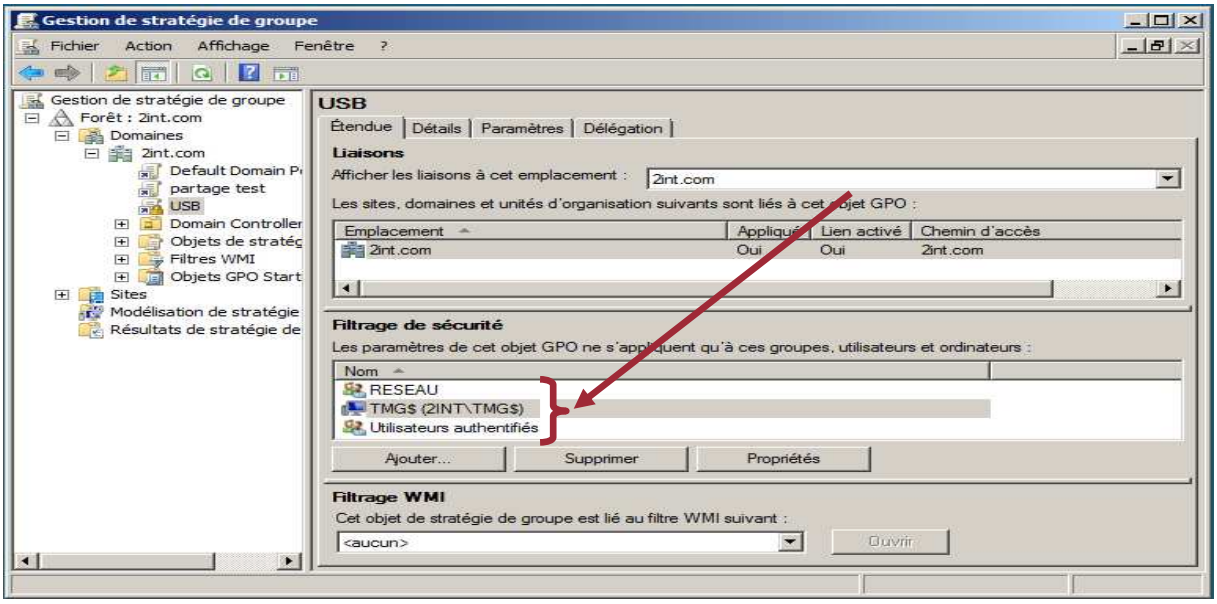
III.7 Stratégie de groupe GPO (*Group Policy Object)*

Cette étape nous a permet de créer des GPO pour la gestion centralisée simplifiée, et renforcement de l'implémentation sur utilisateur et ordinateur

-Création de GPO sous le nom USB

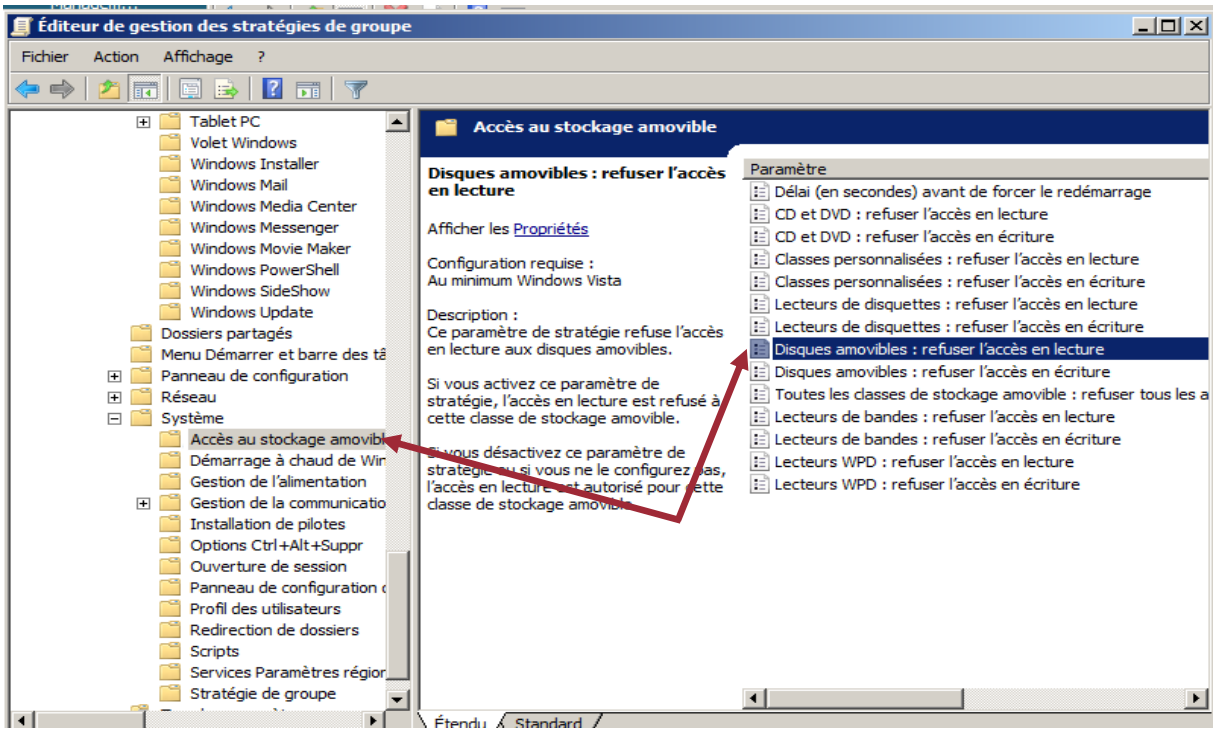


Les paramètres de cet objet GPO ne s'applique que sur les éléments suivants

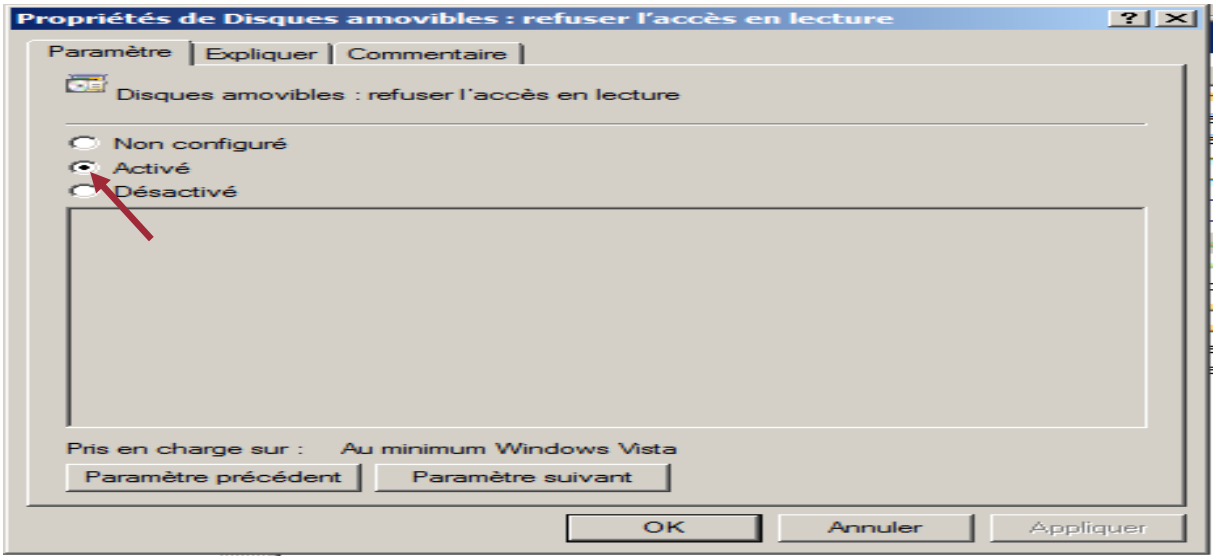


- ✓ Création de stratégie qui interdise les disques amovibles(en lecteur et écriture) pour sécuriser les données de l'entreprise

  Refuser l'accès au disque amovible en lecture

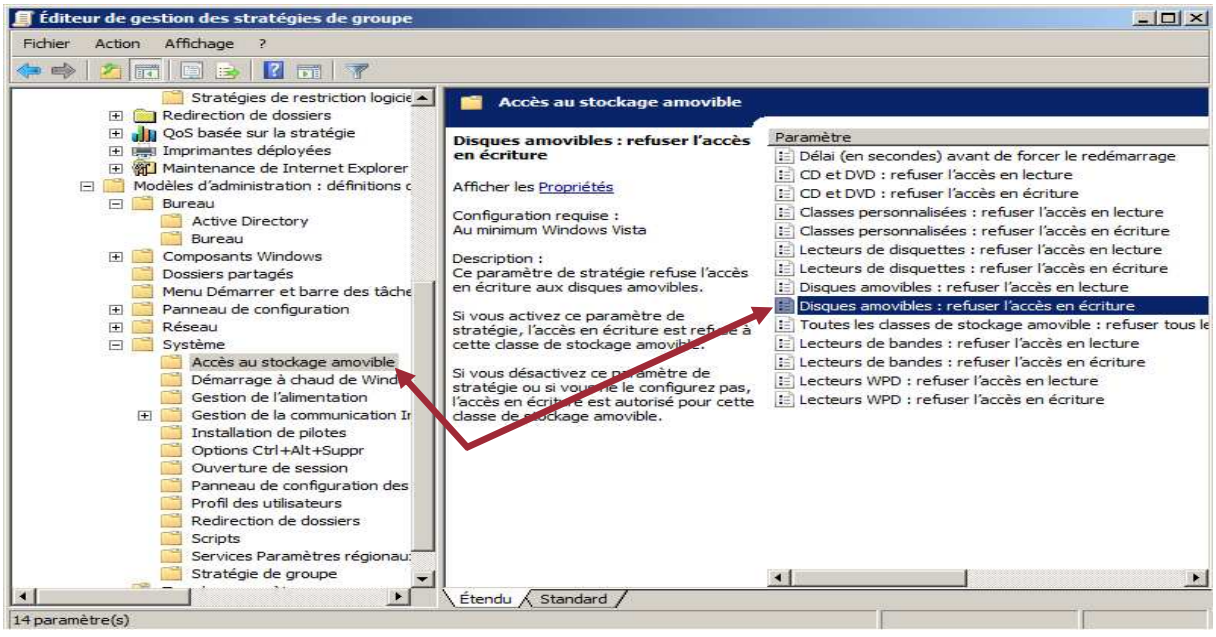


Appliquer la règle de refus de disque amovible

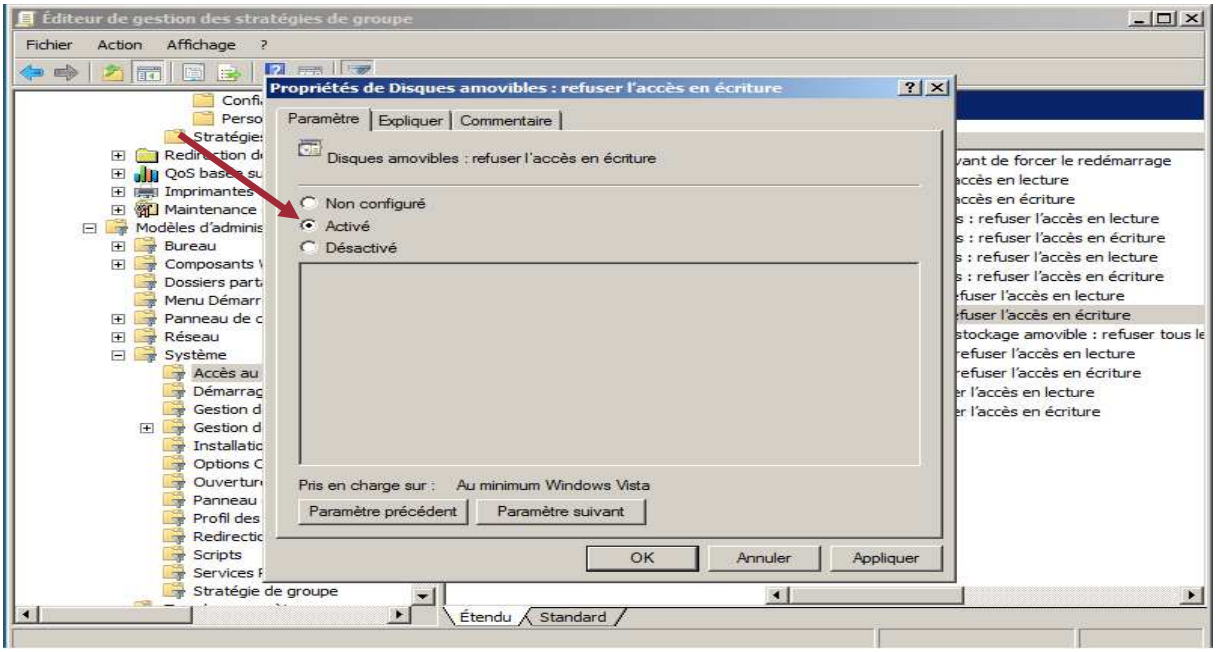


En écriture (Interdire l'installation des logiciels via la clé USB)

Dans système, Accès au stockage, Disques amovibles, refuser l'accès en écriture

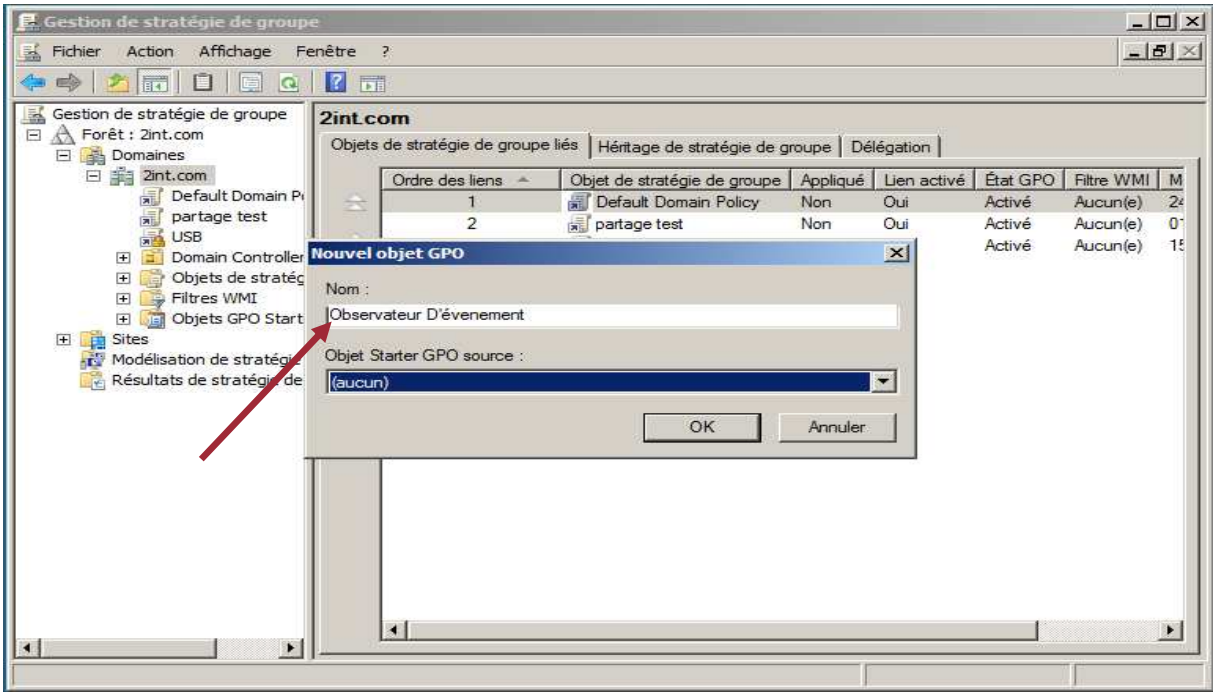


Appliquer la règle de refus en écriture pour les disques amovibles

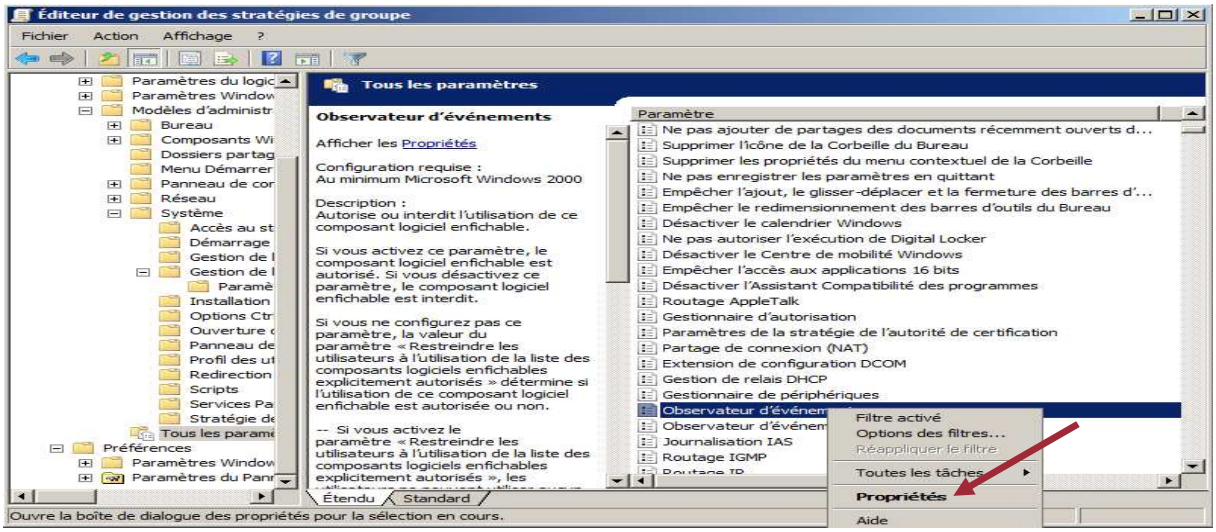


- ✓ Création de règle d'observateur d'événement pour contrôler l'accès des utilisateurs au ressources

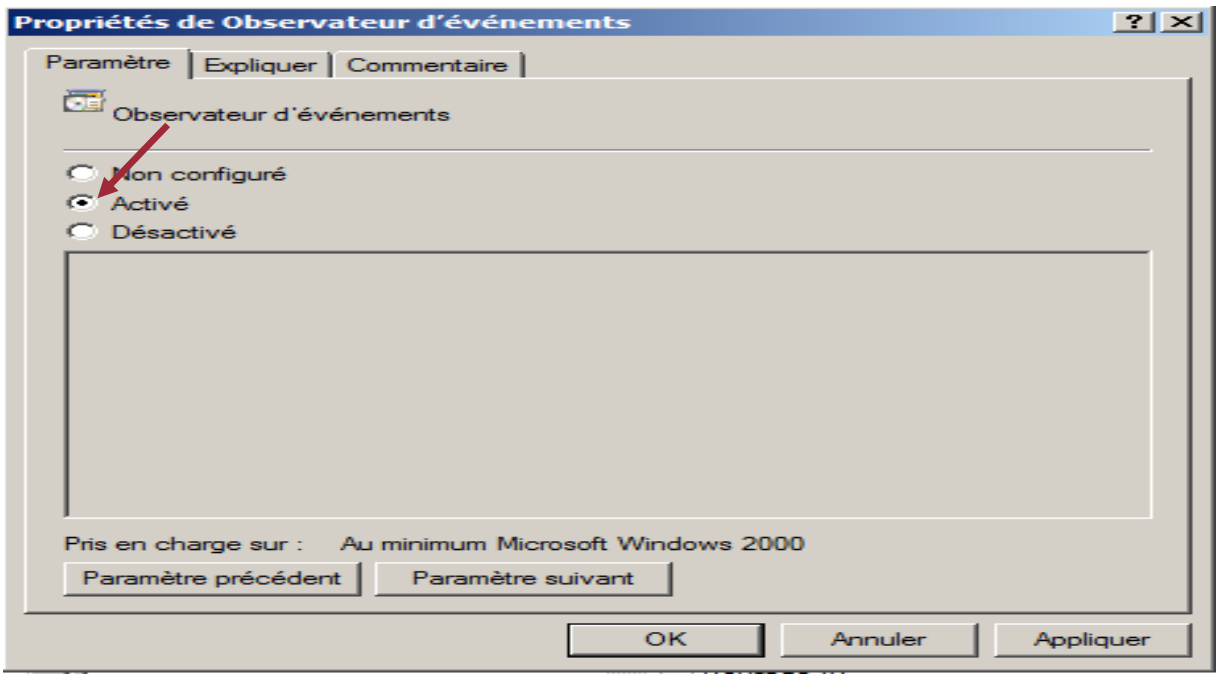
Création d'une GPO Observateur d'événement



Sélectionner Observateur d'événement ,Propriétés pour activer la règle



Activer la règle d'observateur d'évènement

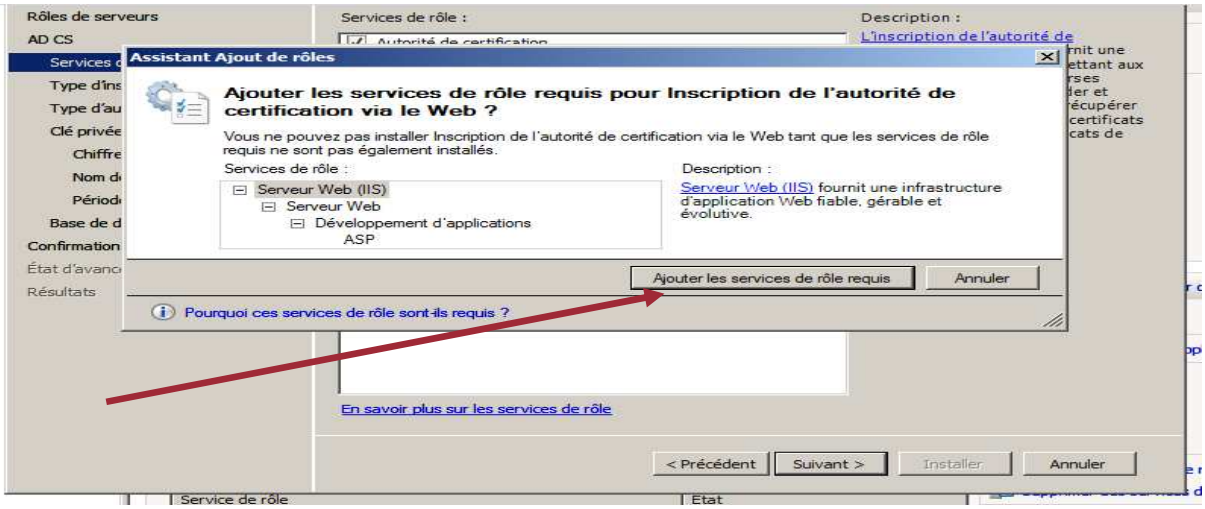


-On à ajouter une stratégie redirection de données de tous les comptes des clients vers un point de sauvegarde SAN, pour que tous les utilisateurs accèdent à leurs données de n'importe qu'elles endroit, avec n'importe qu'elle machine il trouve la même interface bureau et même données.

III.8 Installation serveur Web IIS (Information Internet Service)

Comme nous l'avons vu précédemment, le composant IIS est indispensable dans une entreprise, La réputation a été entachée à de multiples reprises dans le passé à la suite de la découverte de plusieurs failles de sécurité. Au cours des dernières années, Microsoft a pris en compte cette constatation ; le moteur de la version 7.0 a ainsi été réécrit dans le but de le rendre plus stable et sécurisé.

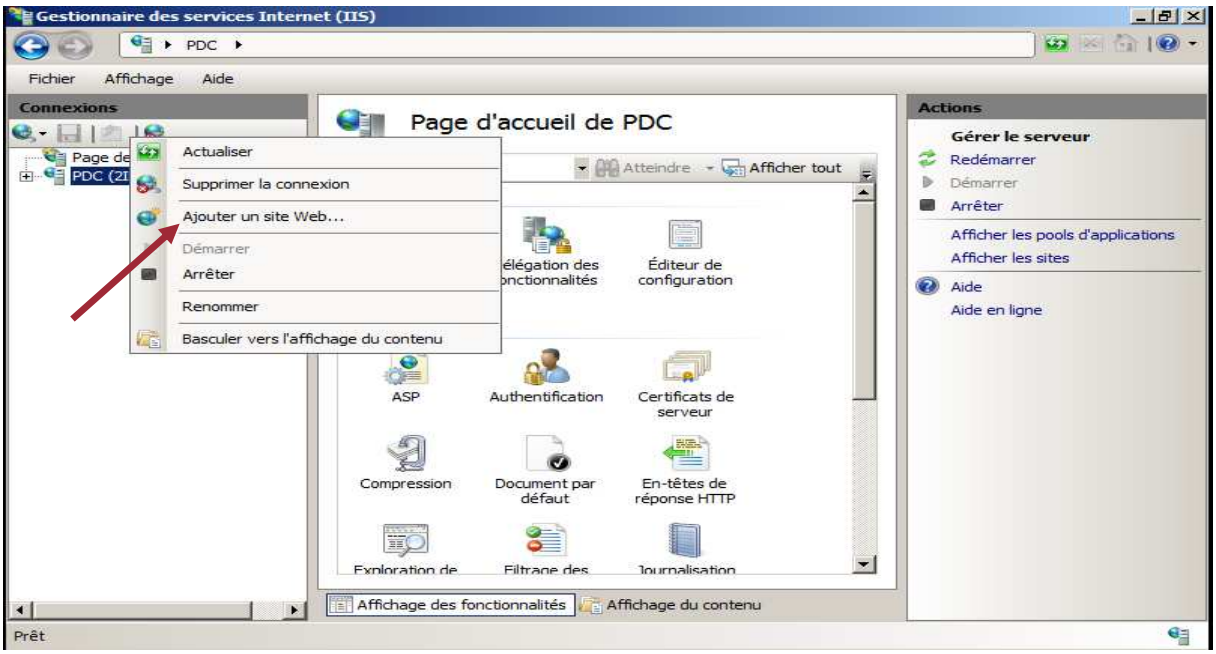
Dans l'angle ajouter des rôles on choisit le rôle IIS



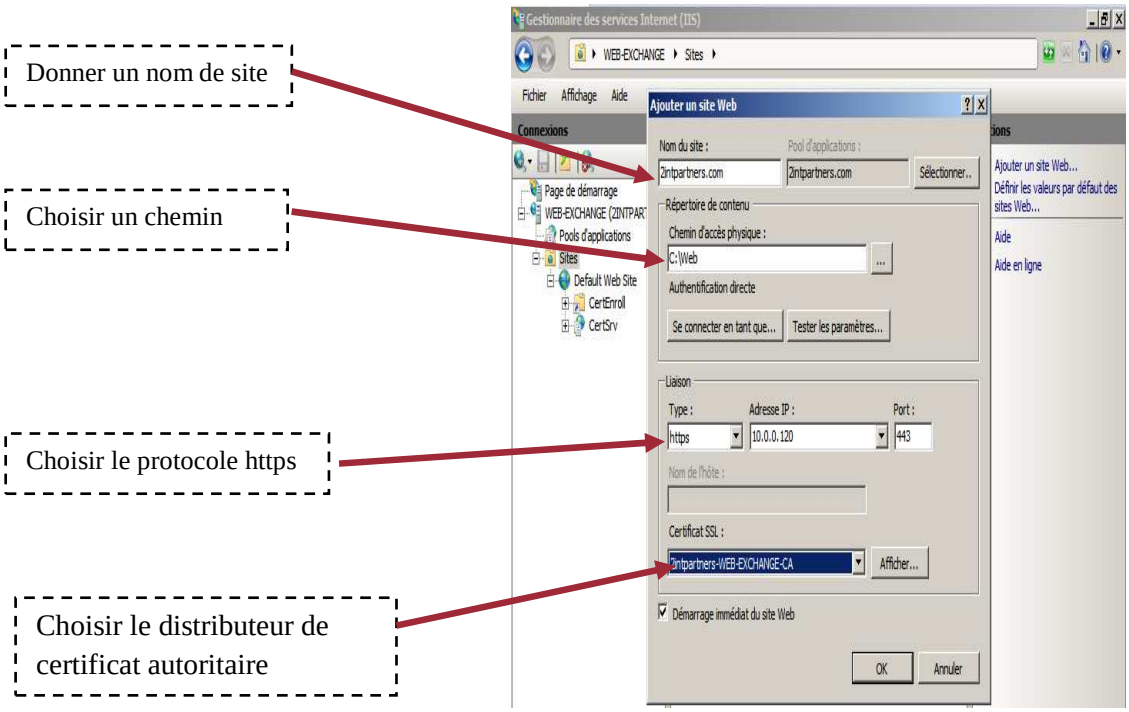
- Cliquez sur **« suivant »**
- Cliquez sur **« Terminer »** pour terminer l'installation

III.10 Ajouter un site Web

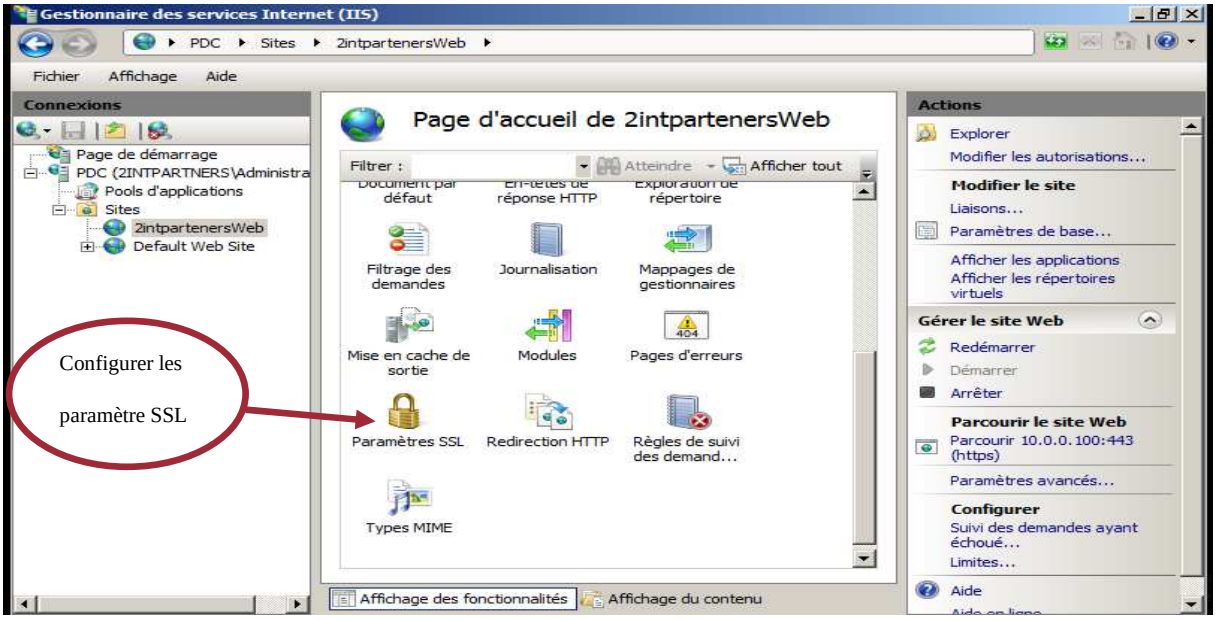
Dans le IIS ajouter un site Web



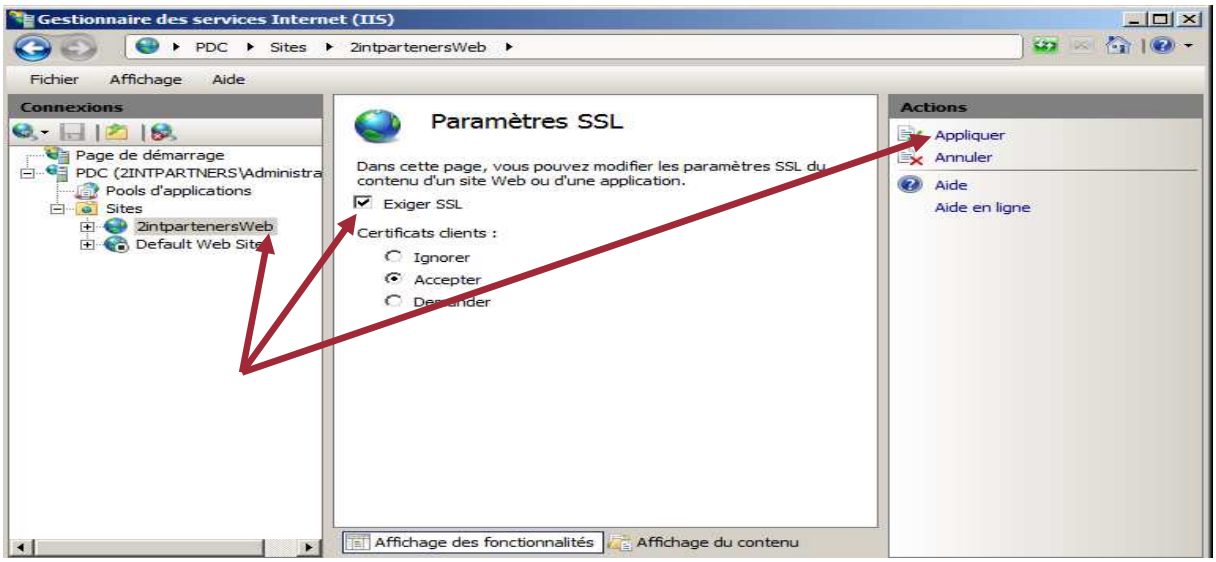
Remplir les paramètres indiquer sur l'image suivante



Choisir les paramètres SSL

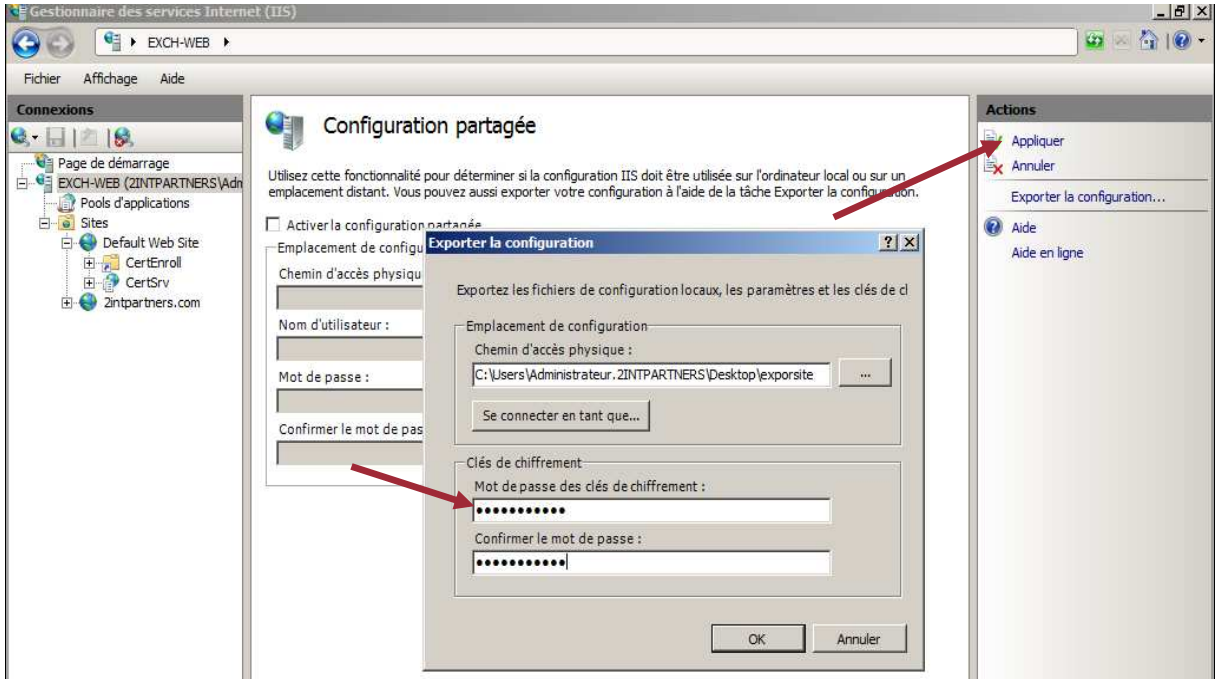


Exiger le SSL dans le site 2intpartnersWeb

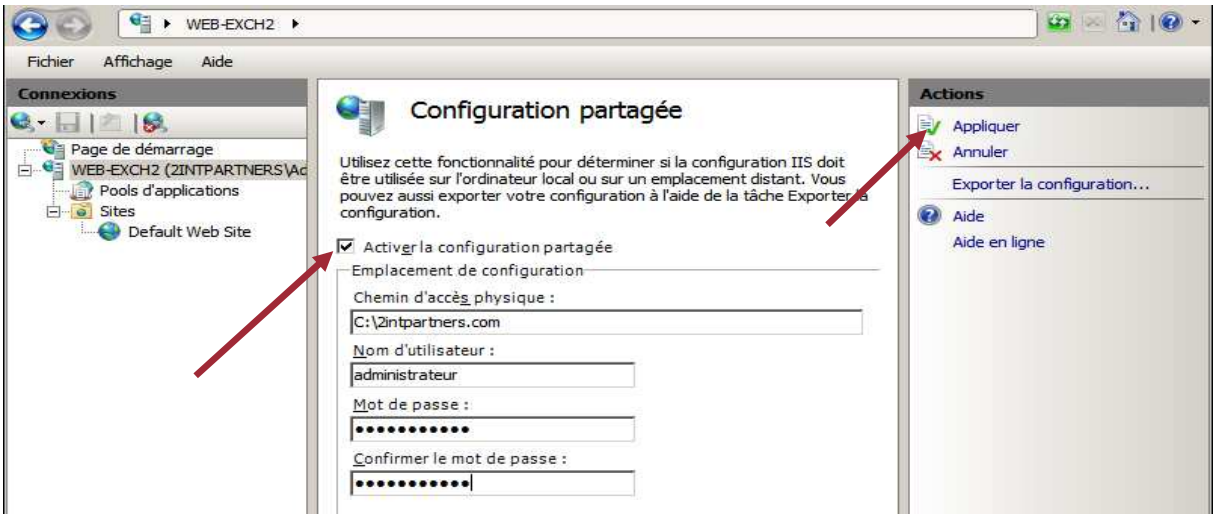


III.10.1 Exportation du site 2intpartners du serveur EXCH-WEB vers le 2eme serveur WEB- EXCH2

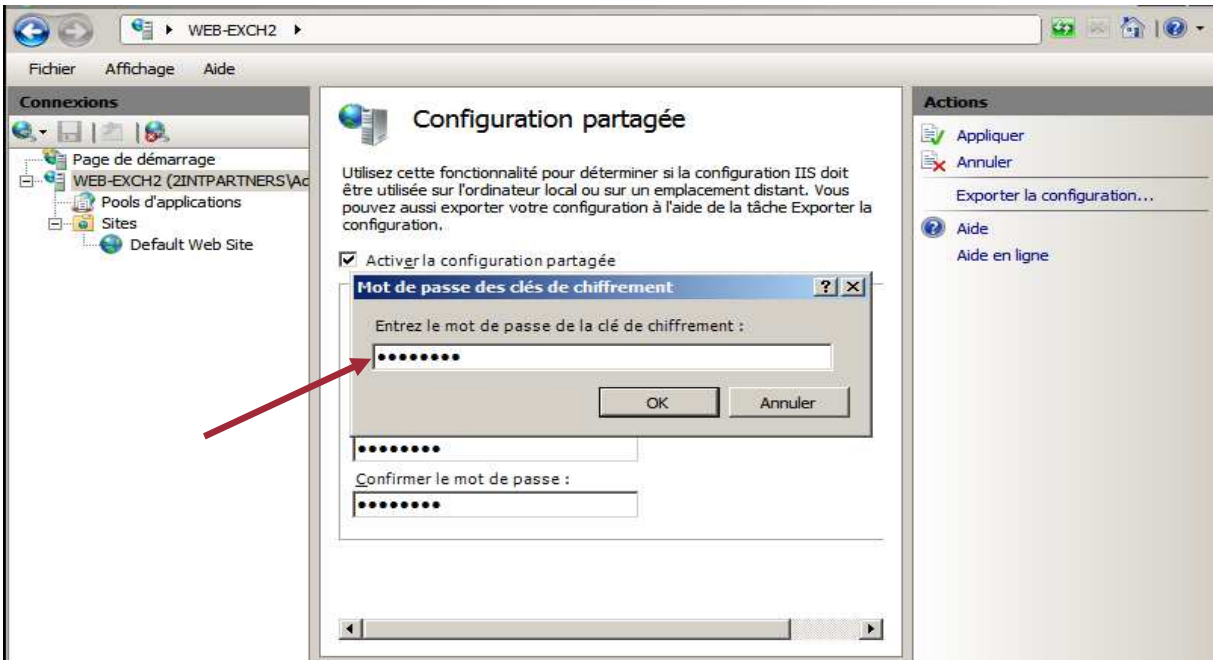
Dans le IIS, configuration partagée, Exporter la configuration on indique le chemin physique du site accompagnée d'une clé de chiffrement



Dans WEB-EXCH2 on active la configuration partagée en cliquant sur appliquer



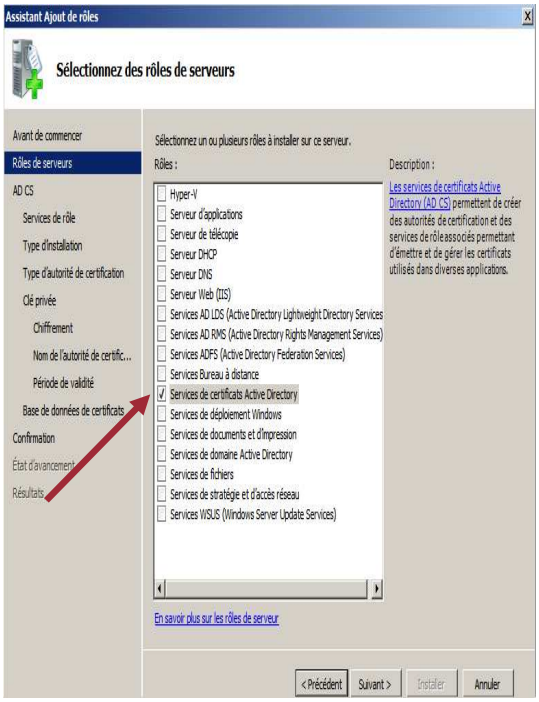
Après l'activation de la configuration partagée on tape le mot de passe des clés chiffrées utilisées dans WEB-EXCH



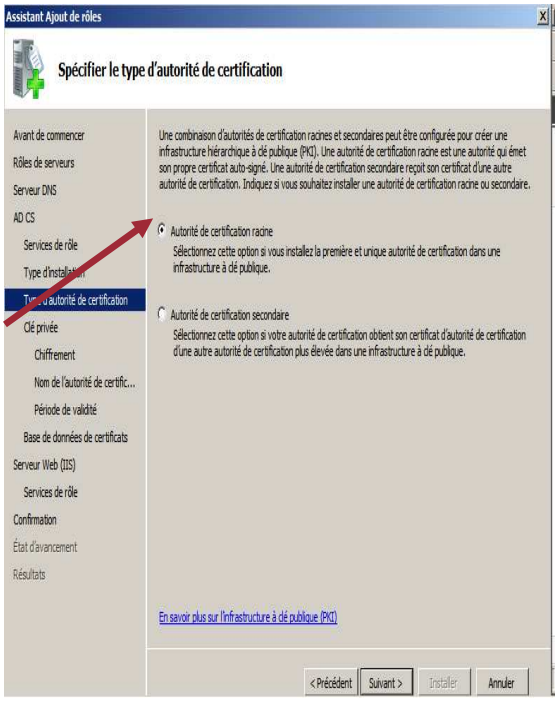
III.11 Installation de service de certificat Active Directory

Dans le web1.exchange on installe le service de certificat pour chiffrer la communication

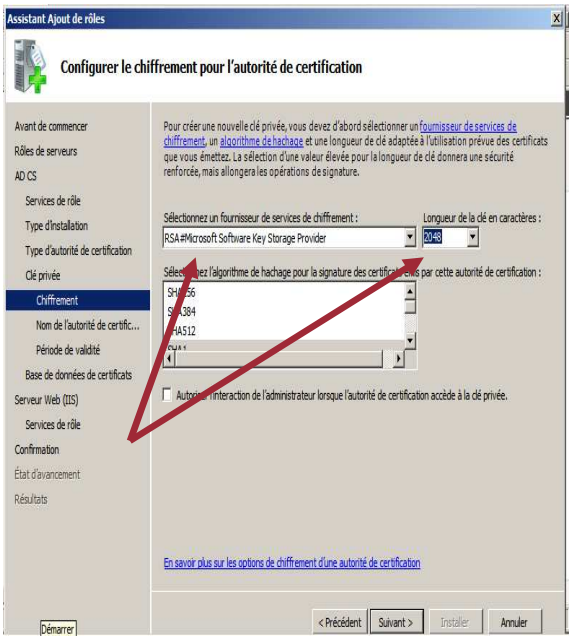
Installation du rôle



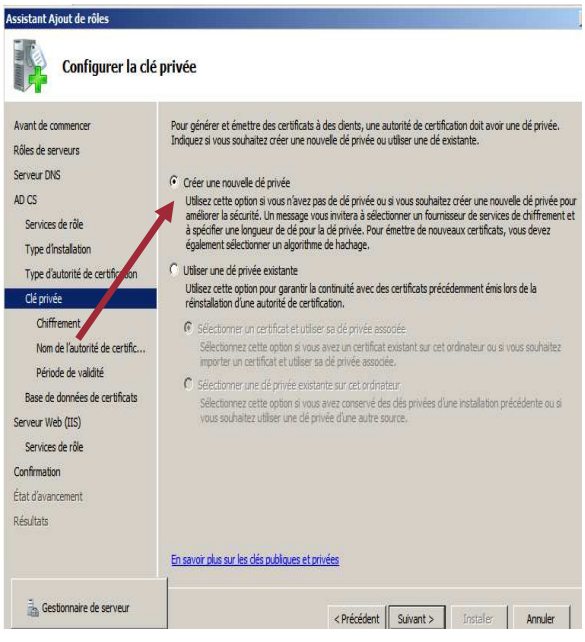
Choisir l'instalation autorité racine



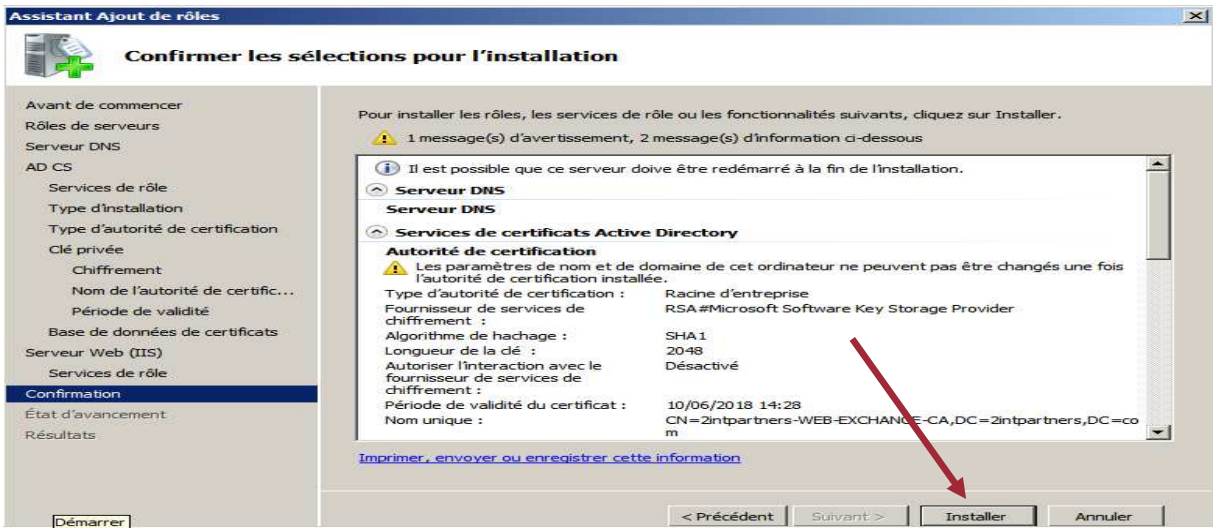
Le type de chiffrement



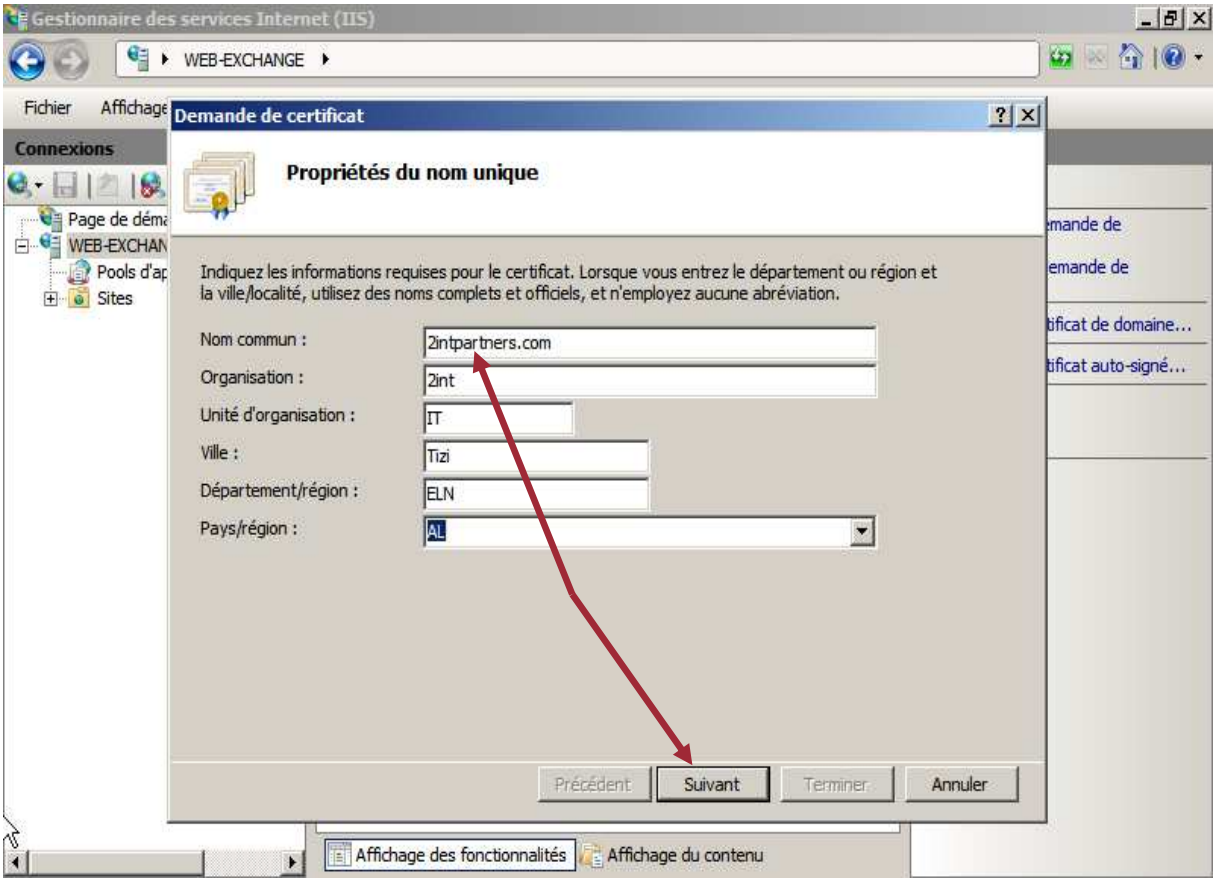
Demander une nouvelle clé privée



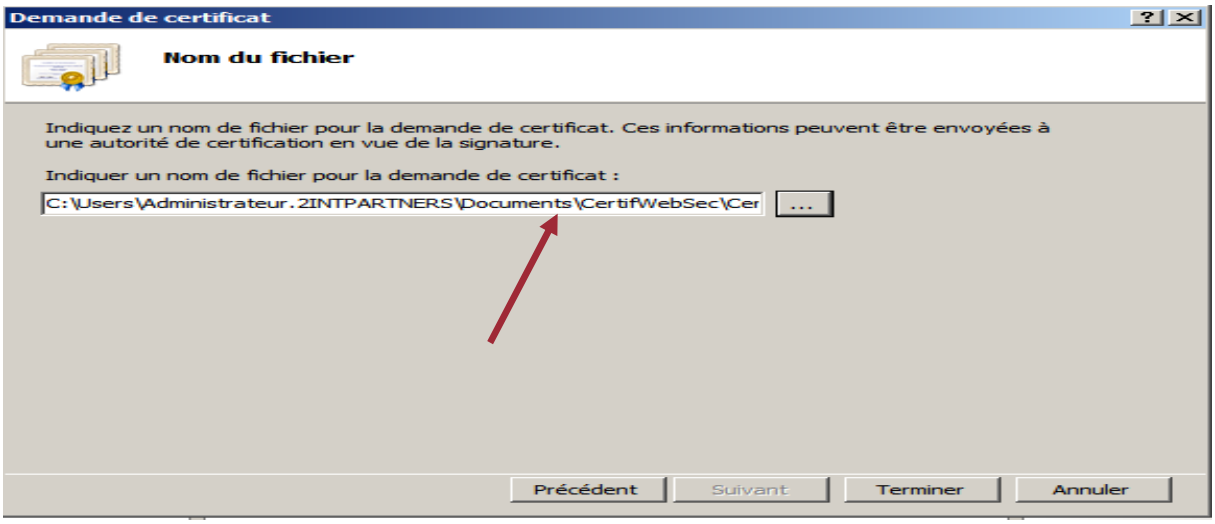
Confirmer les sélection précédentes



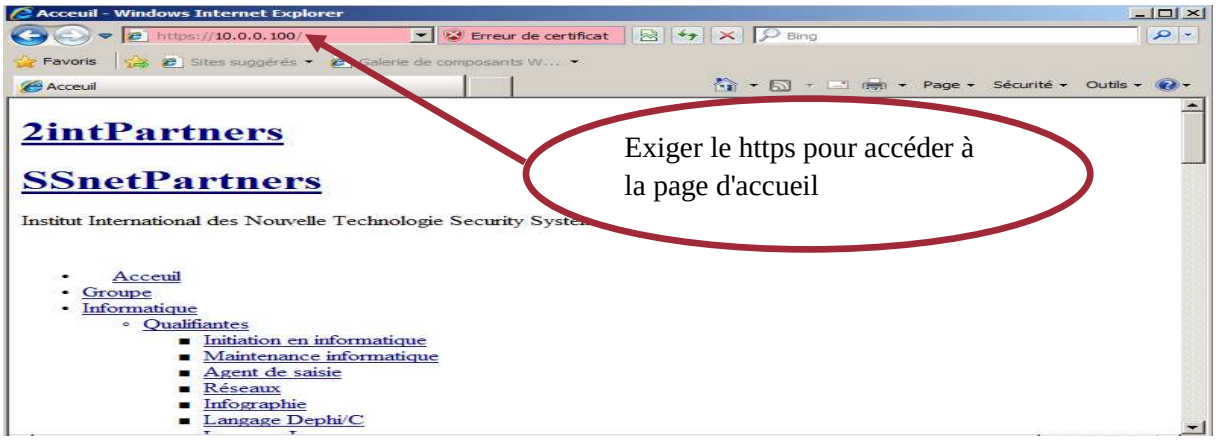
Demande de certificat dans IIS



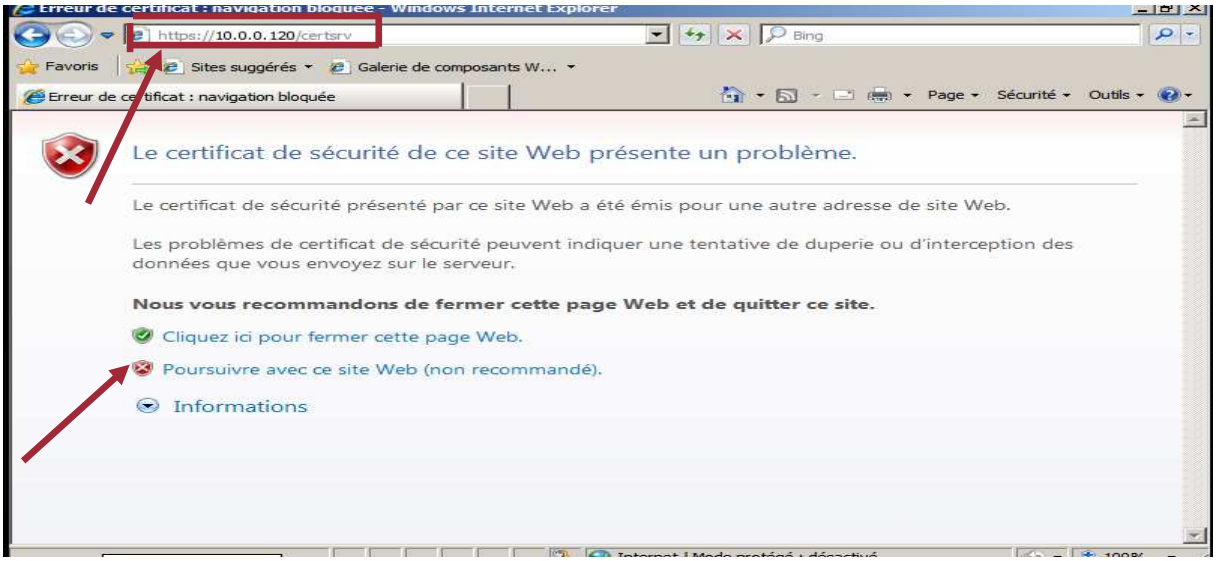
Choisir un emplacement pour l'enregestrement de la demande puis terminer



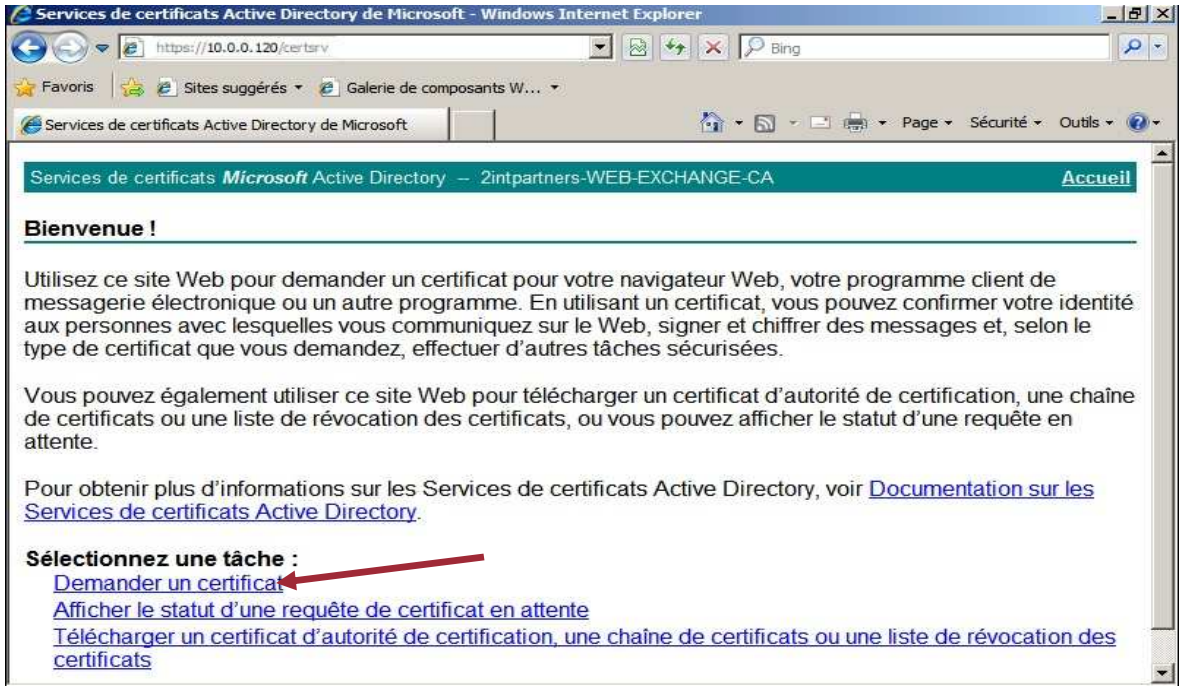
Affichage de la page d'accueil



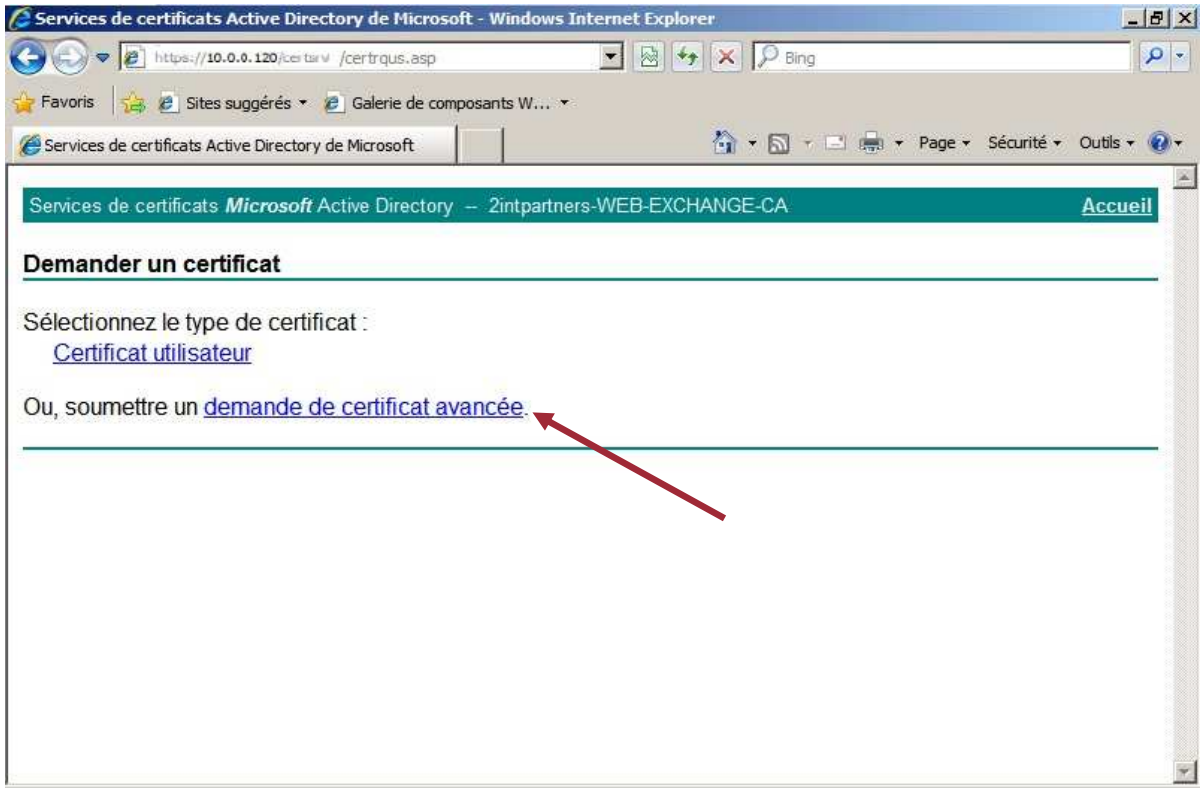
Demande de certificat via le Web



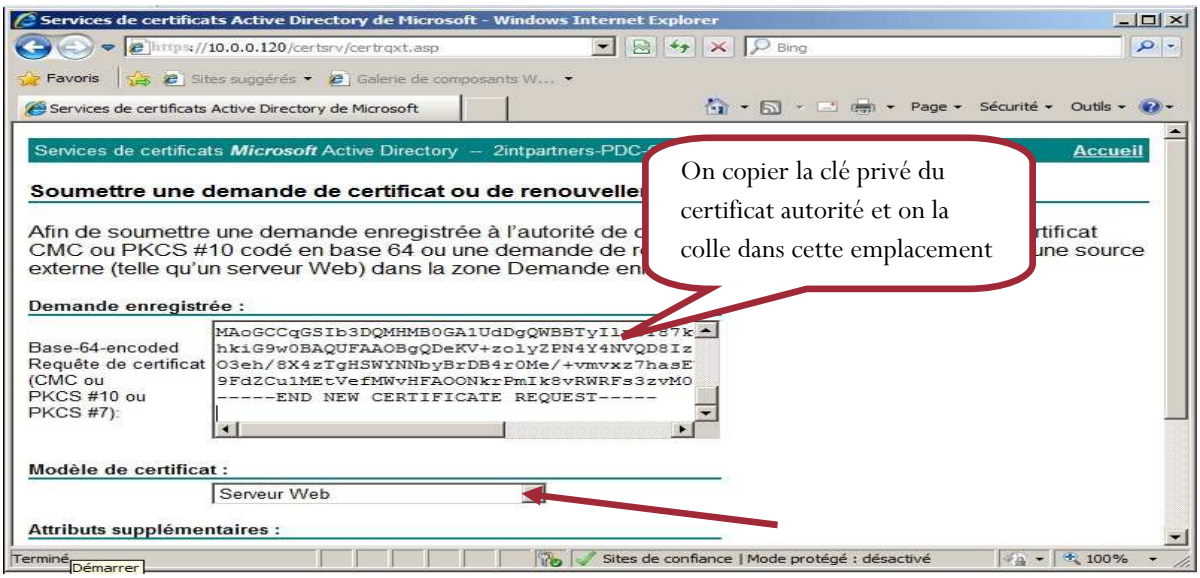
Demander un certificat



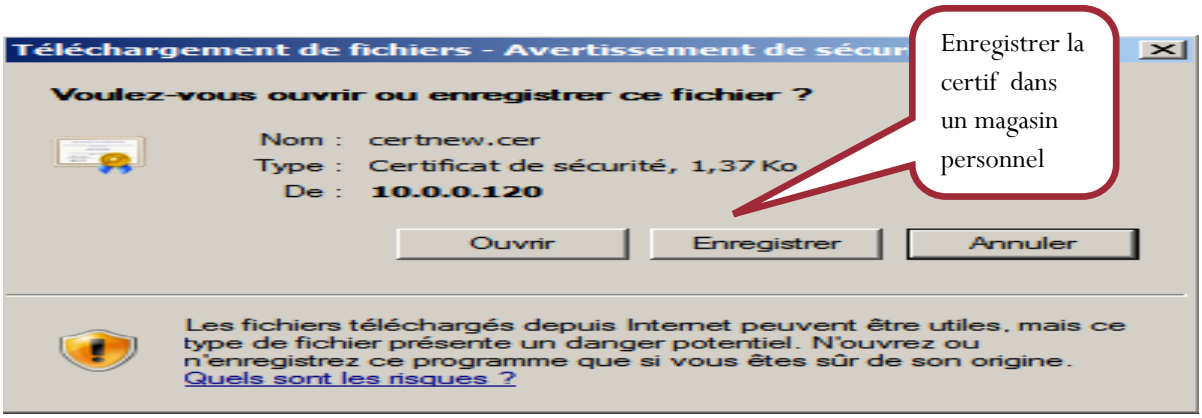
Soumettre une demande de certificat pour la communication Web



Copier le contenue du fichier enregistrer précédâmes dans la demande via IIS

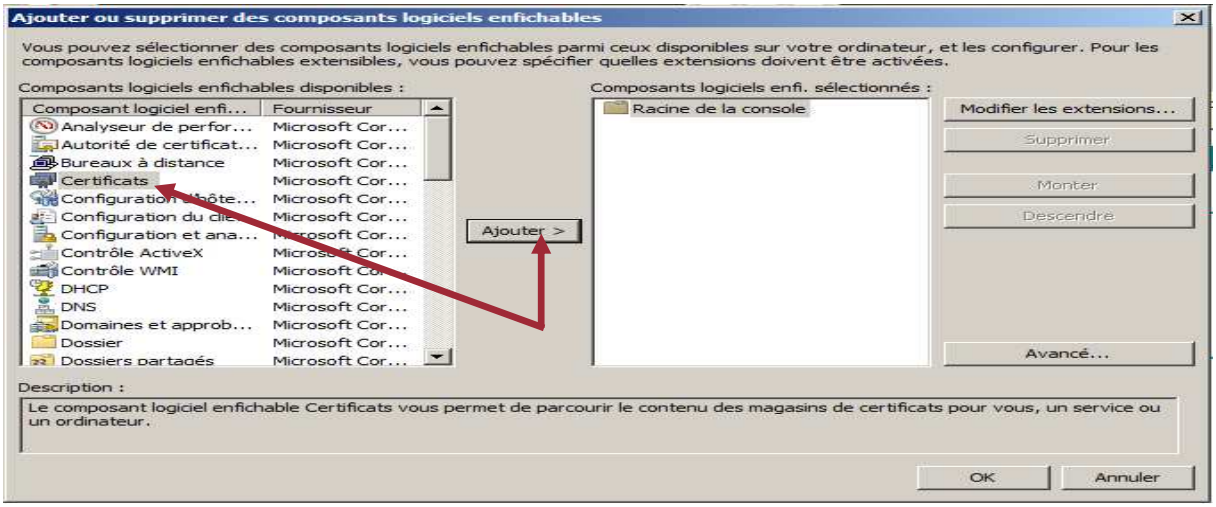


Enregistrer le certificat dans un magasin



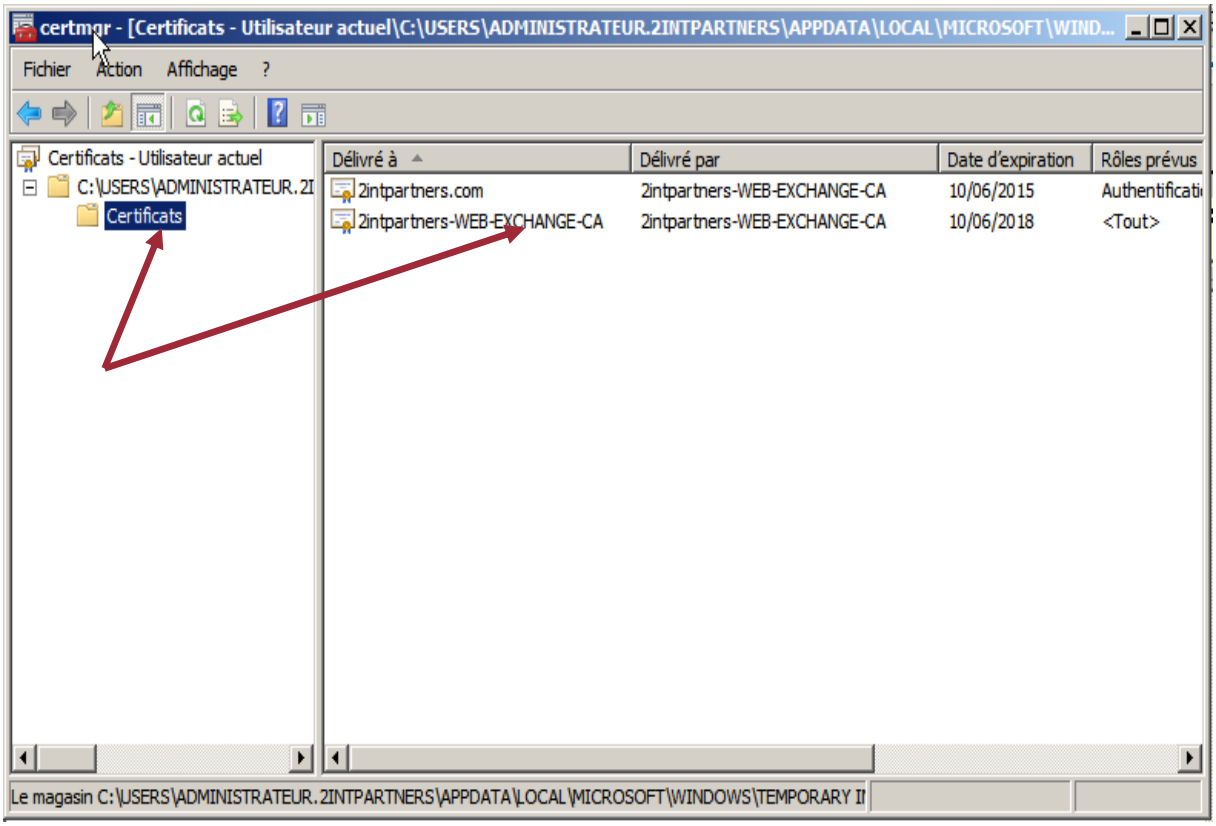
Terminer la demande de certificat dans le IIS

On exécute la console mmc.exe, dans le menu fichier on sélectionne Ajouter ou Supprimer un fichier enfichable, on clique sur Certificats puis Ajouter ,on valide par ok



On enregistre la console mmc sur le Bureau pour les deux certificats

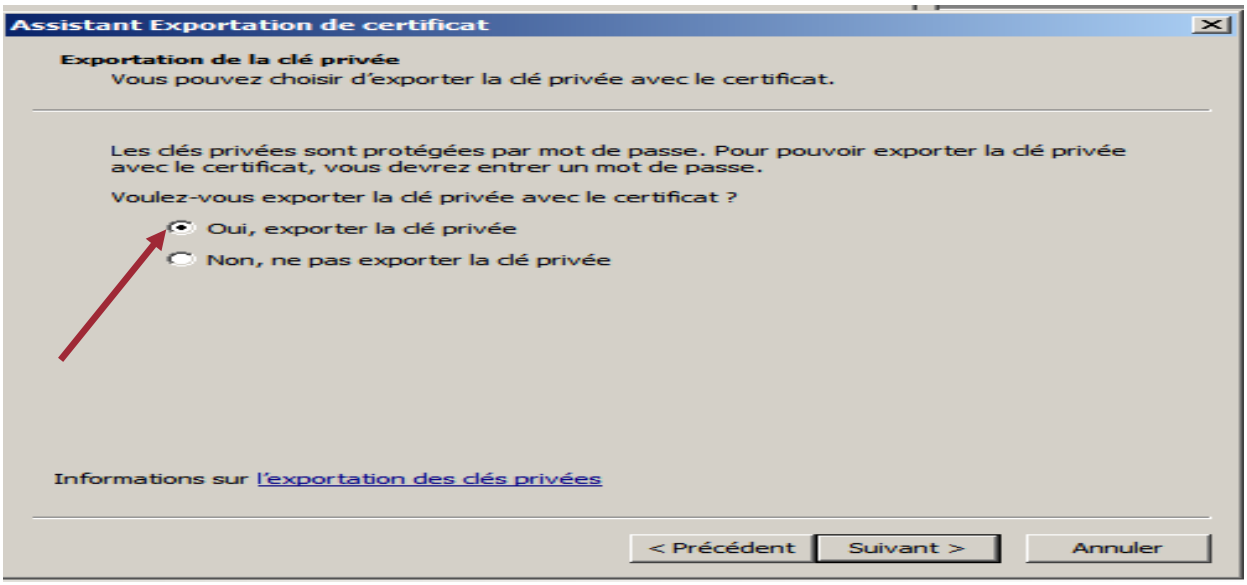
Vérification dans la console mmc l'existence des certificats créer précédemment



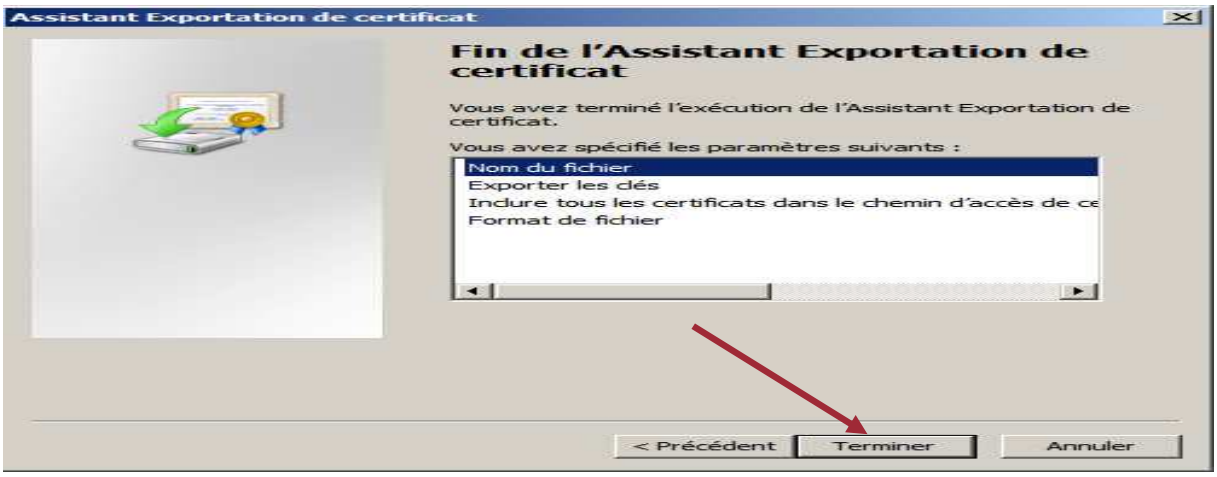
III.11.1 Exportation des certificats dans un magasin

Clic droite sur certificat, choisir exporter,

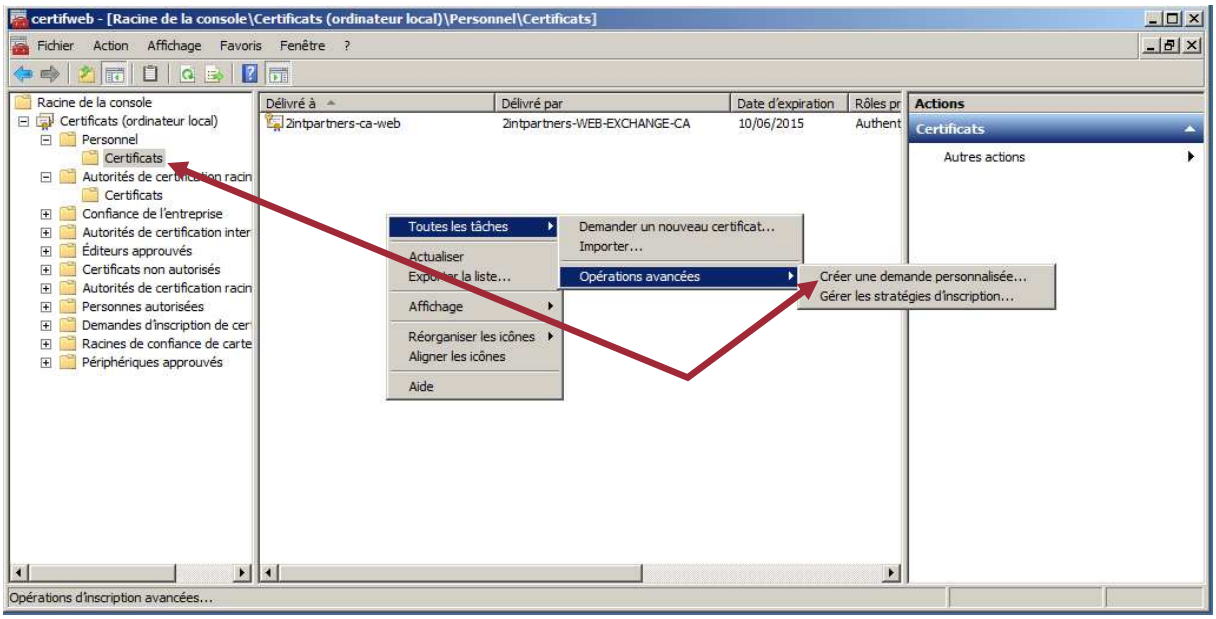
Dans la fenêtre qui apparait on coche la case oui, exporté la clé privé



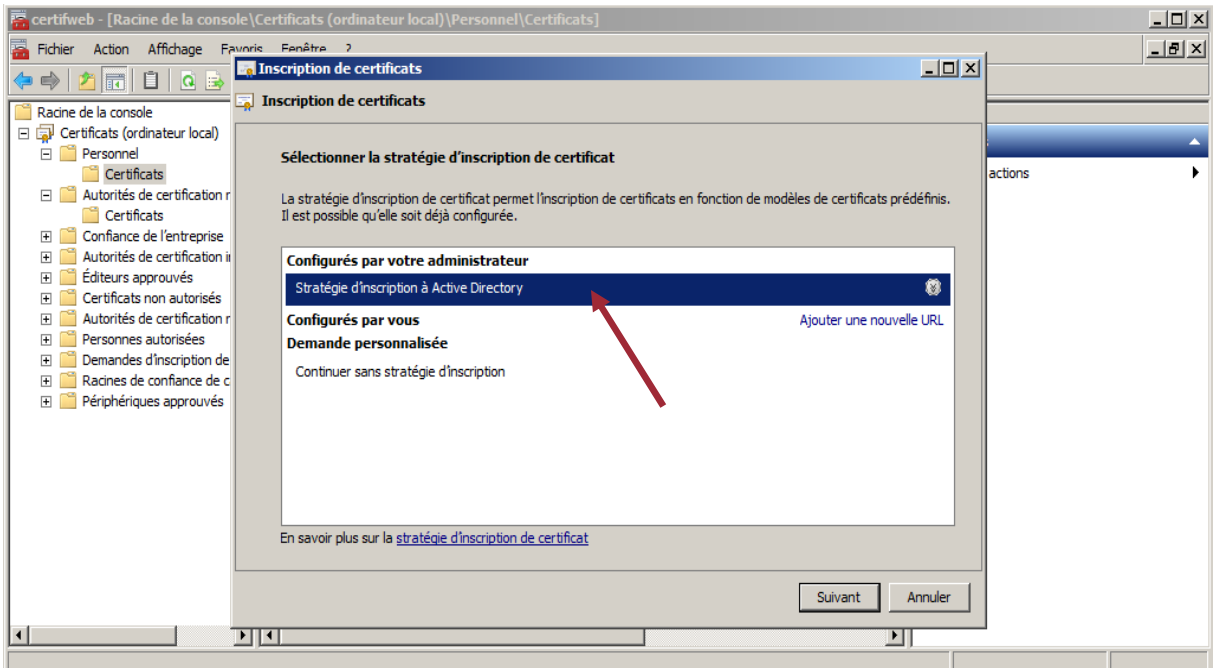
Cliqué sur Ok pour terminer l'assistant d'Exportation de certificat.



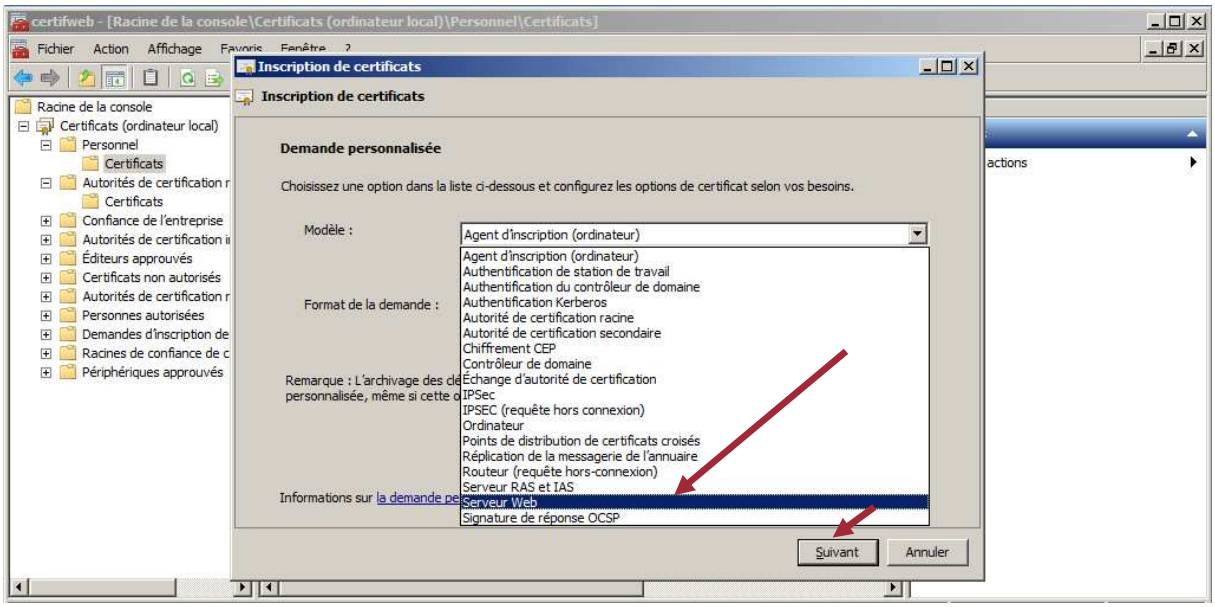
Dans **mmc**, magasin Personnel, choisir **gérer les stratégies d'inscription**



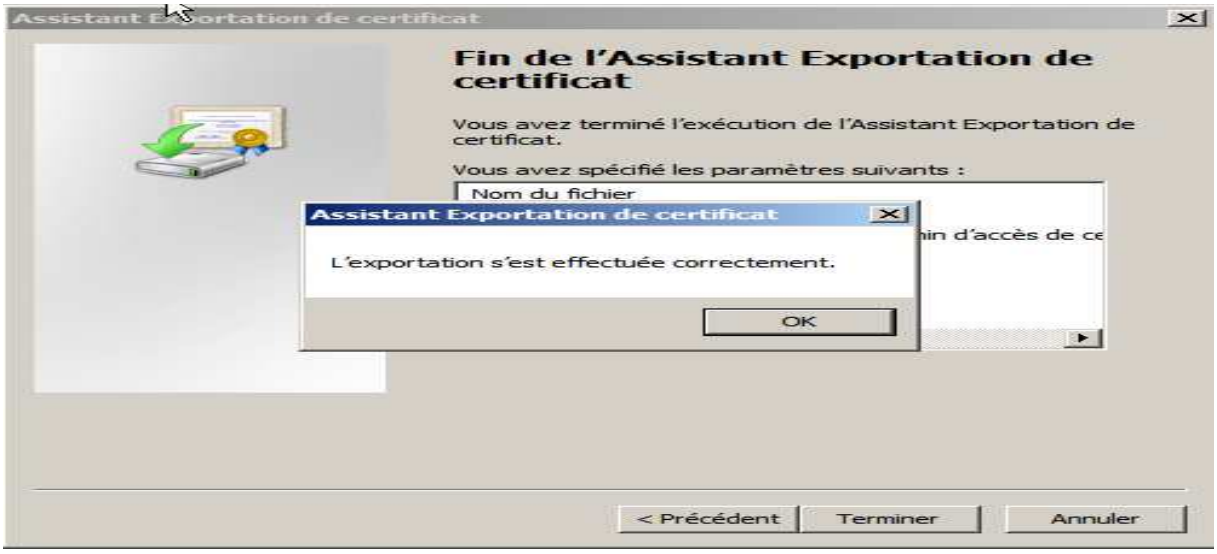
Choisir la stratégie d'inscription de certificats à l'Active Directory



Choisir l'inscription via le web puis suivant



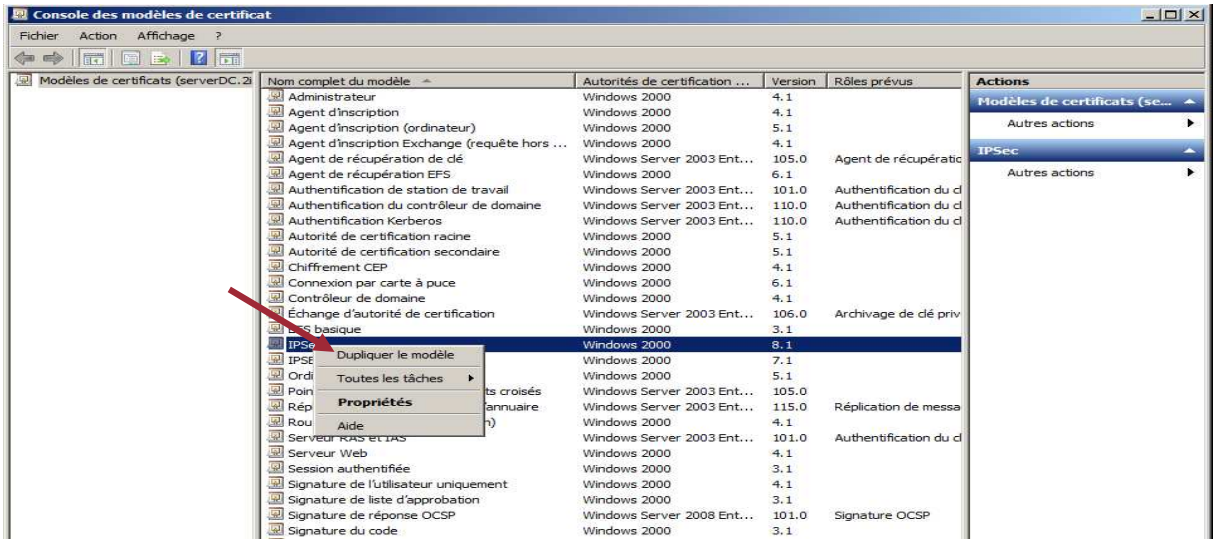
Cliquer sur Ok pour mettre fin à l'assistance d 'exportation de certificat



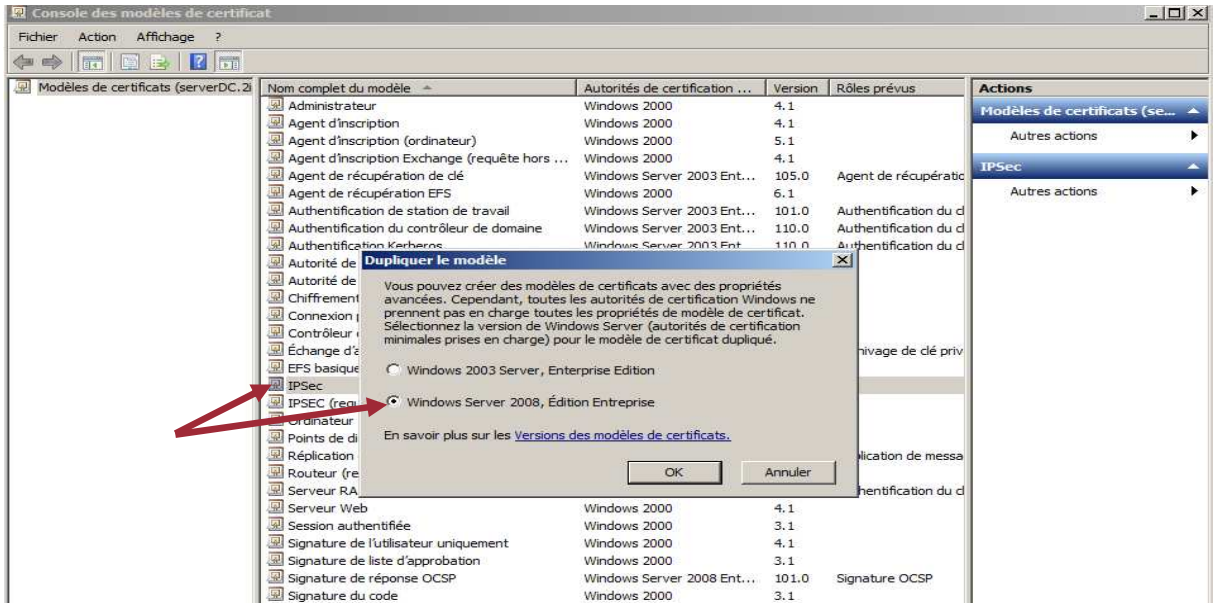
III.11.2Création d'un certificat IPsec

Le certificat IPSec est un moyen de chiffrement de communication entre les postes, c'est une solution choisie contre le Snifing

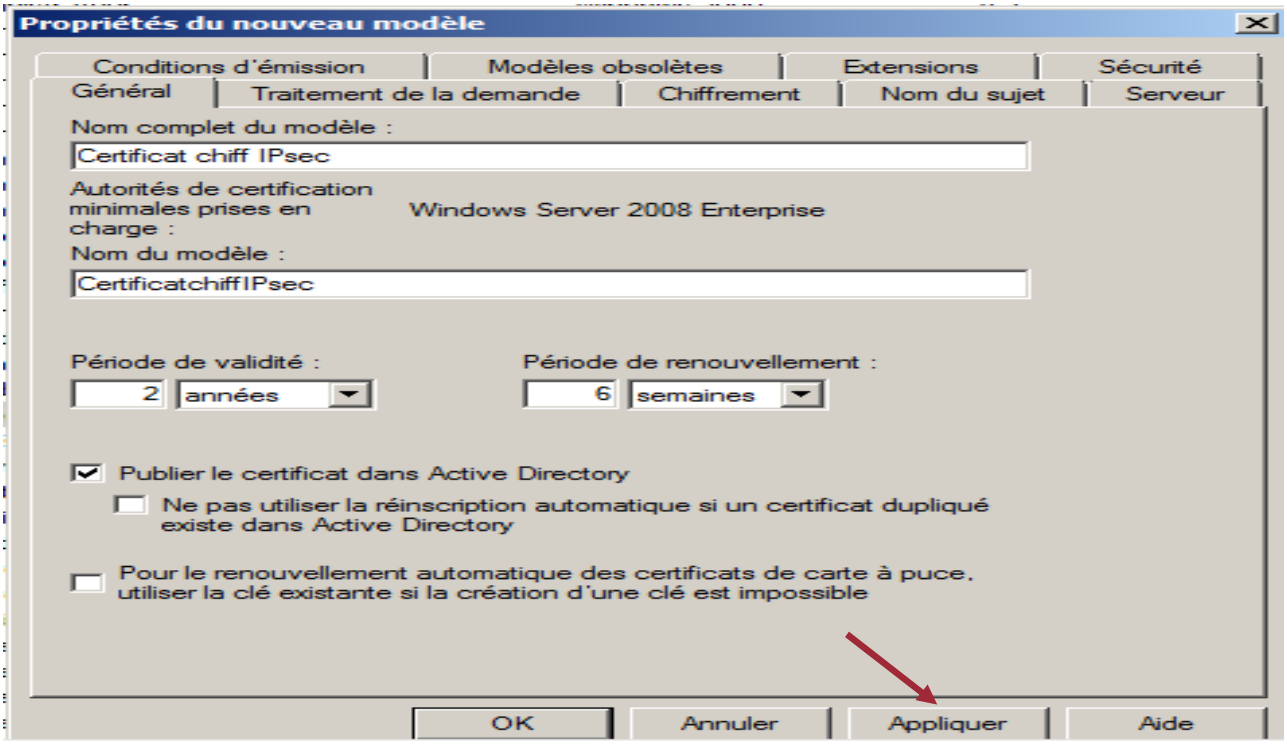
Dans outils d'administration, Autorité de certificat, clique droit sur modèle de certificats, gérer et on choisi dans la liste IPSec



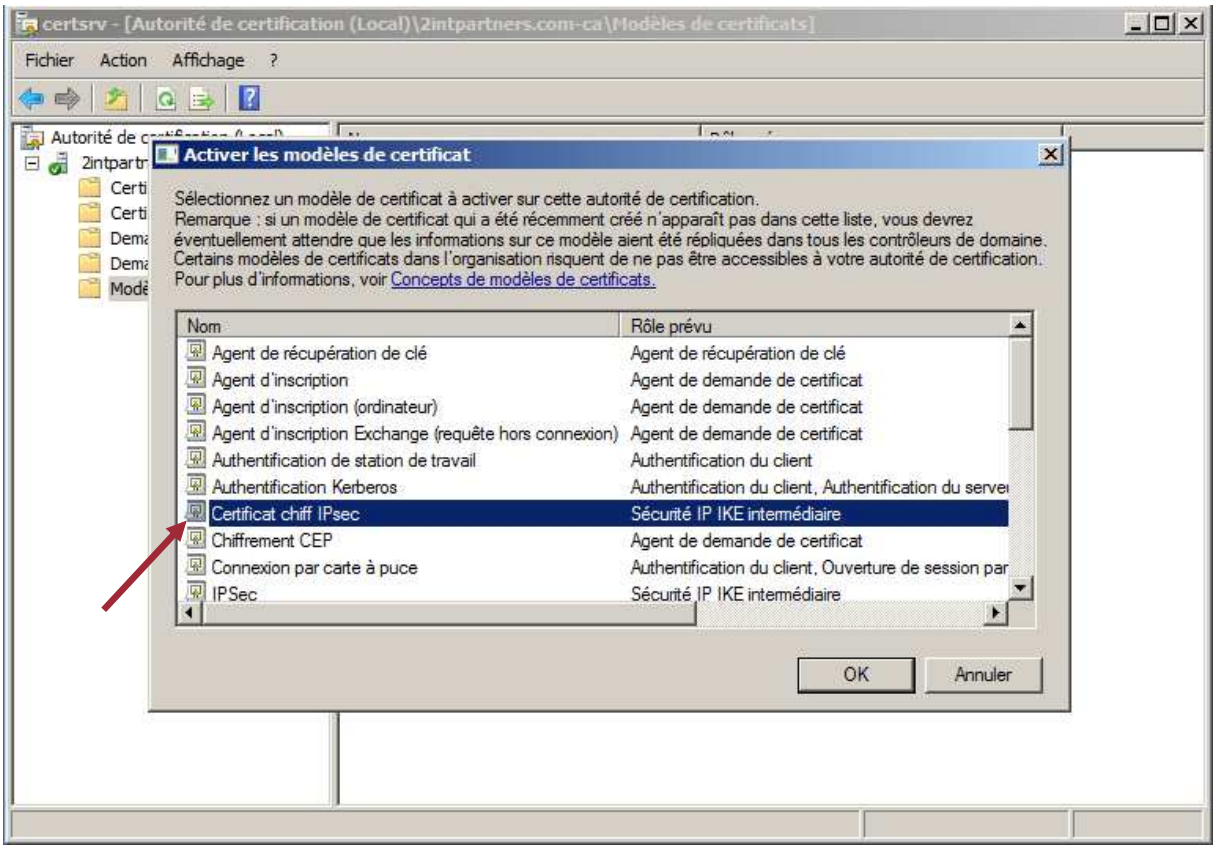
Choisir sur quel serveur dupliquer le modèle



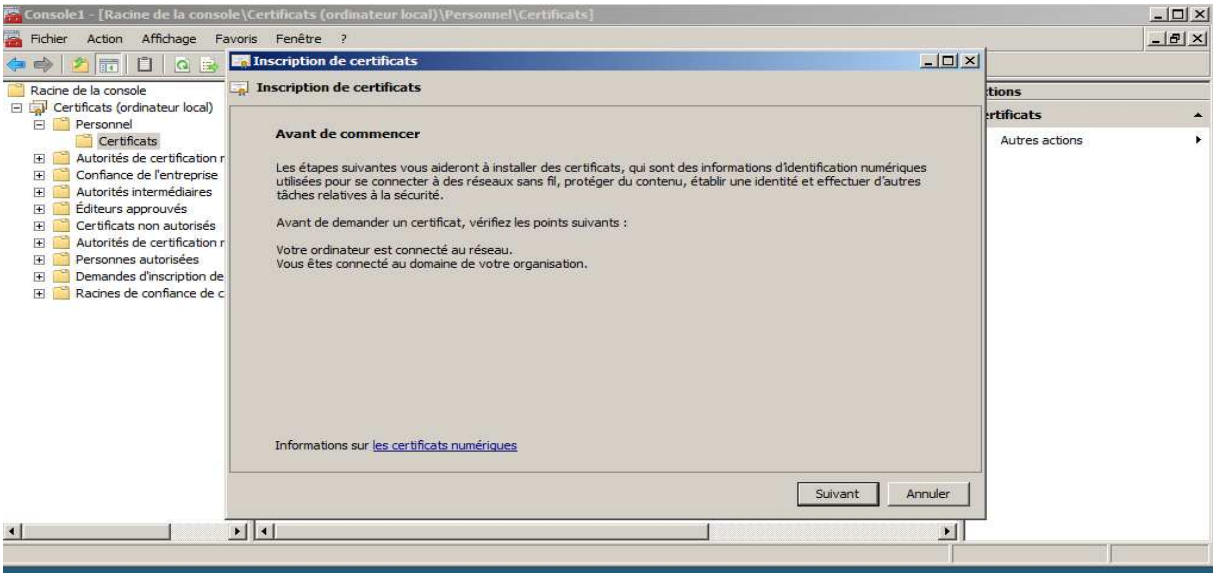
Donner un nom au modèle de certificat à dupliquer et cliquer sur appliquer



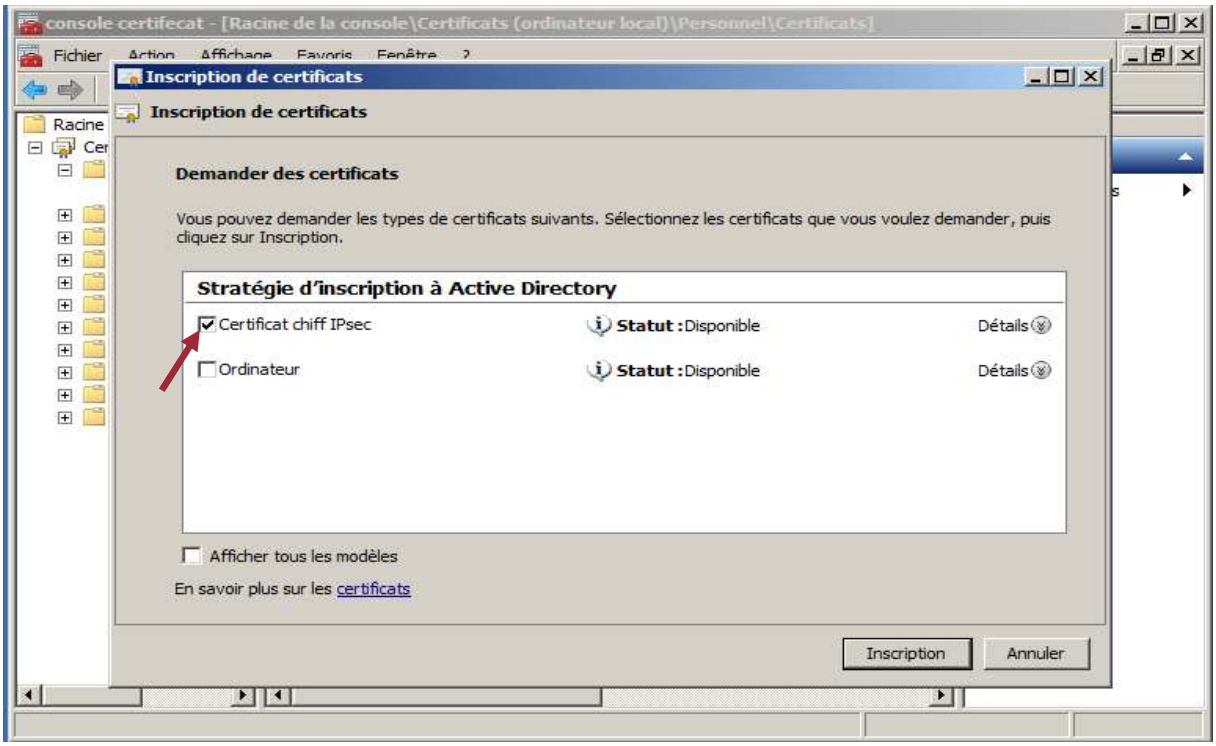
Dans le modèles de certificat, Nouveau, on clique sur modèle de certificat à délivrer et on choisi certificat chiff IPsec



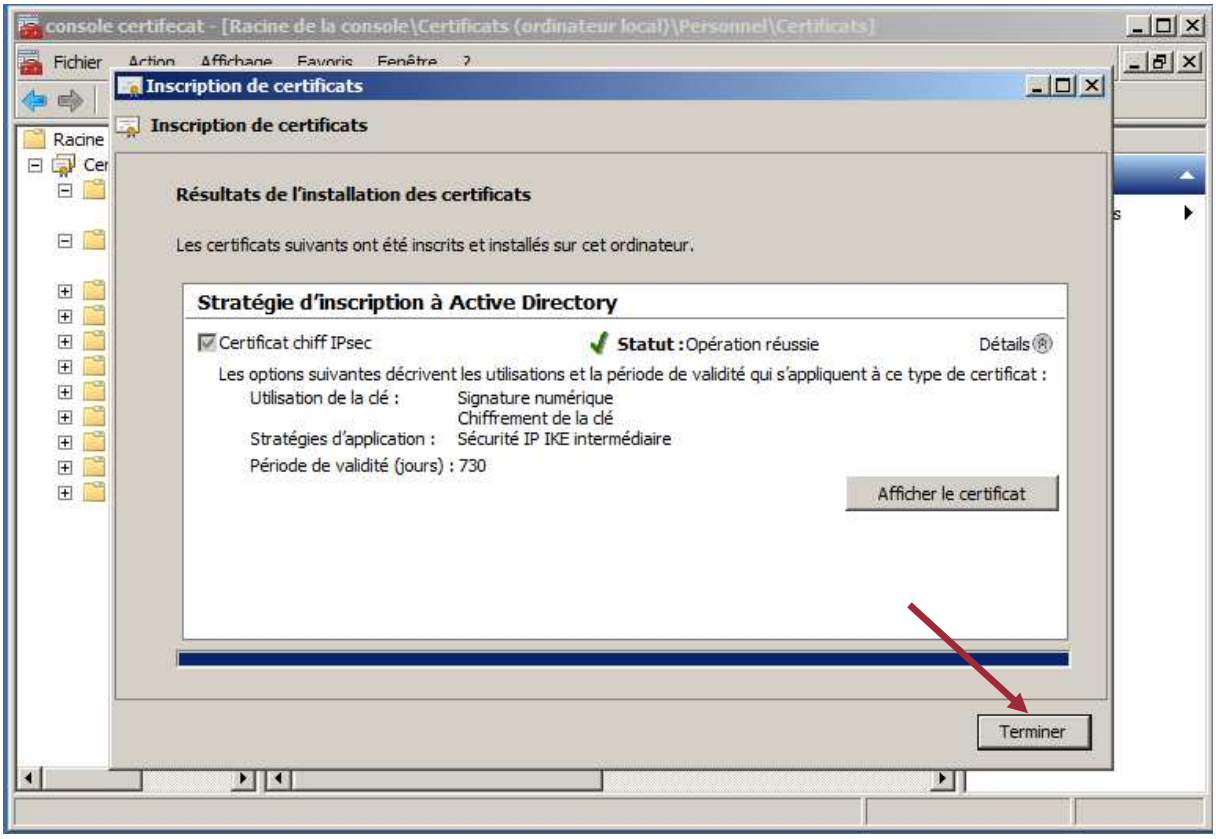
Clique droit sur certificat dans le magasin personnel, toutes les tâches, demander un nouveau certificat



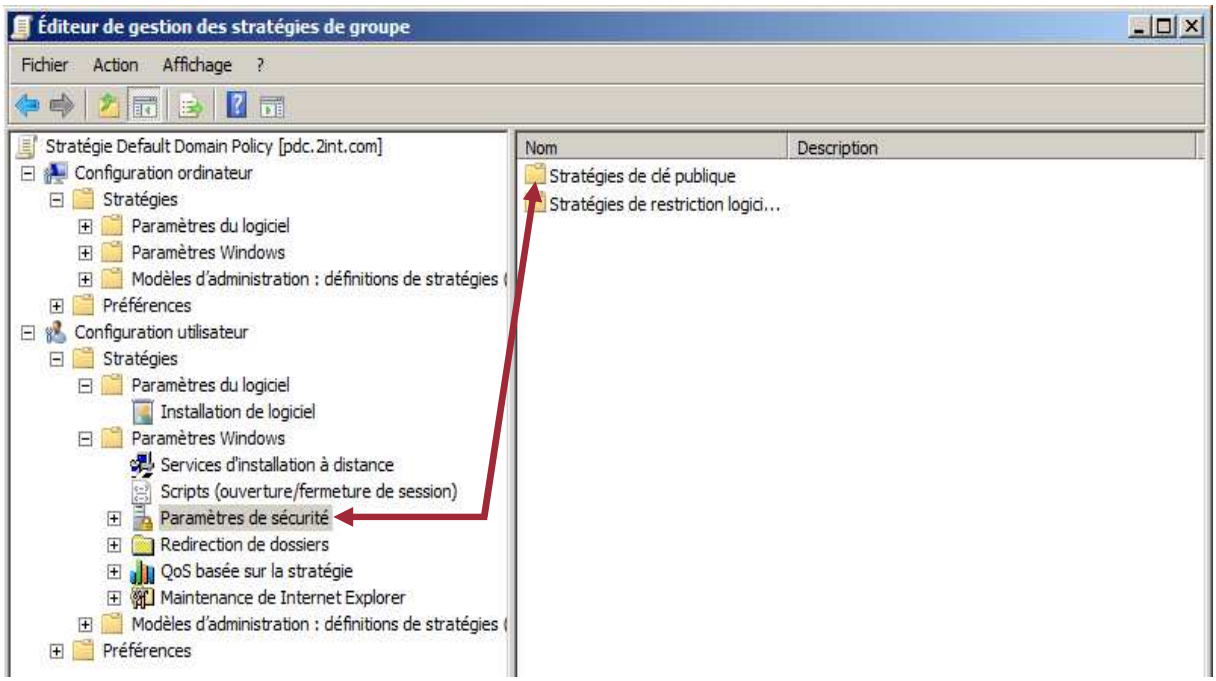
Choisir le modèle certificat chiff IPsec créer précédemment puis clique sur inscription



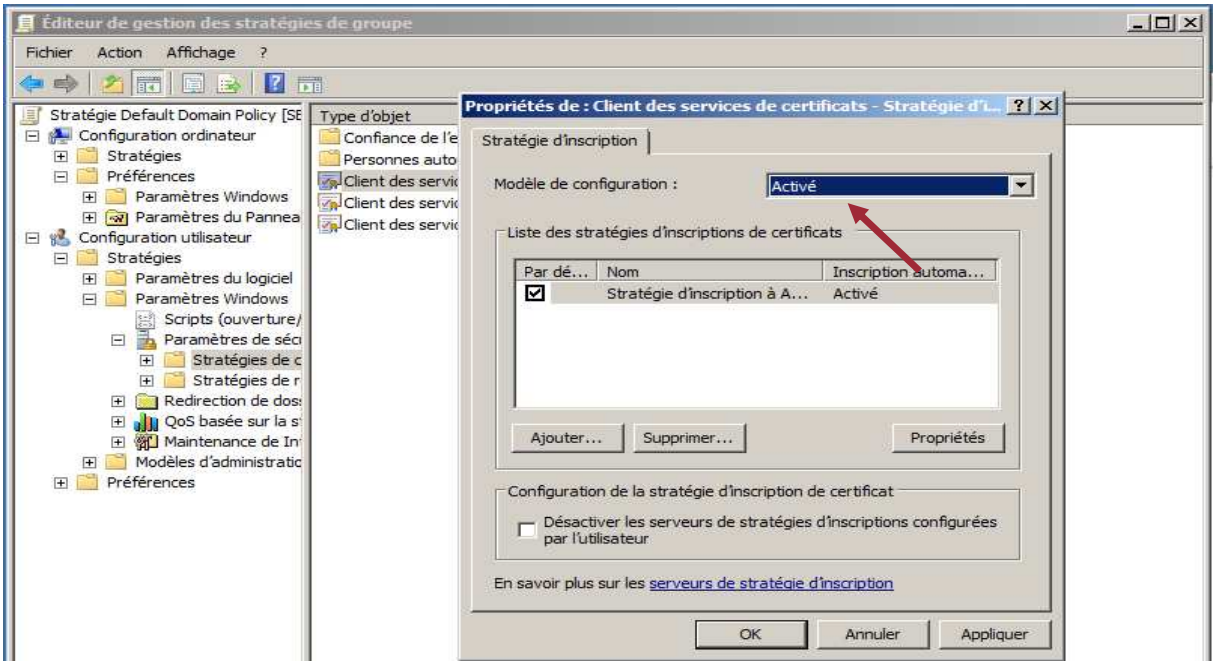
Fin d'inscription du certificat chiff IPsec avec succès



Dans l'éditeur de stratégie de groupe on choisi Paramètre de sécurité puis stratégies de clé publique

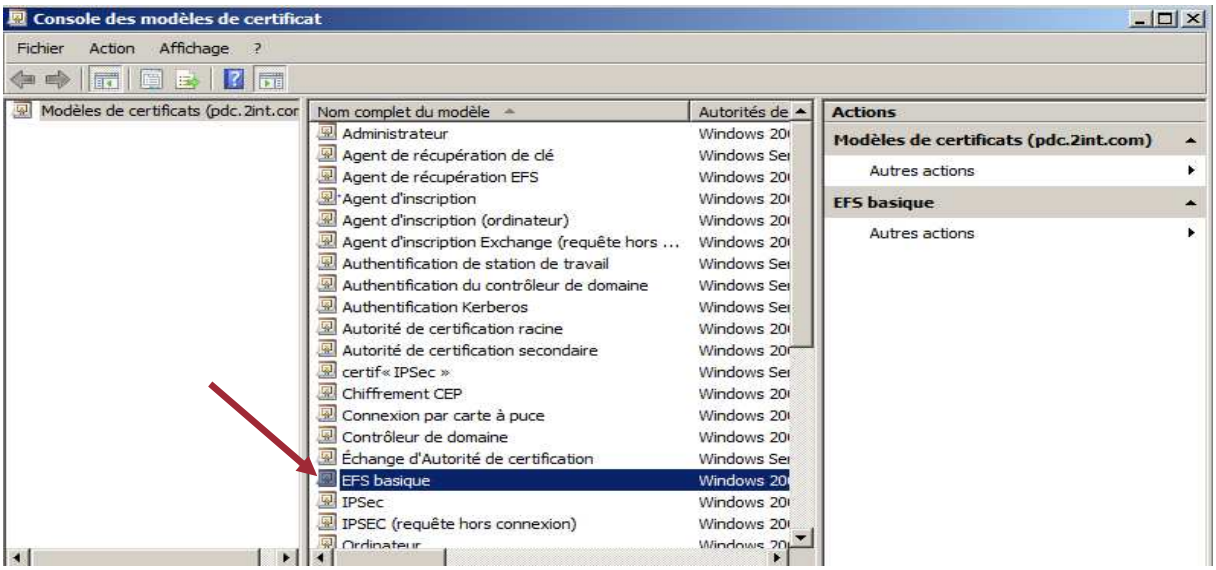


On active l'inscription automatique des clients au service de certificat IPsec et on active cette stratégie

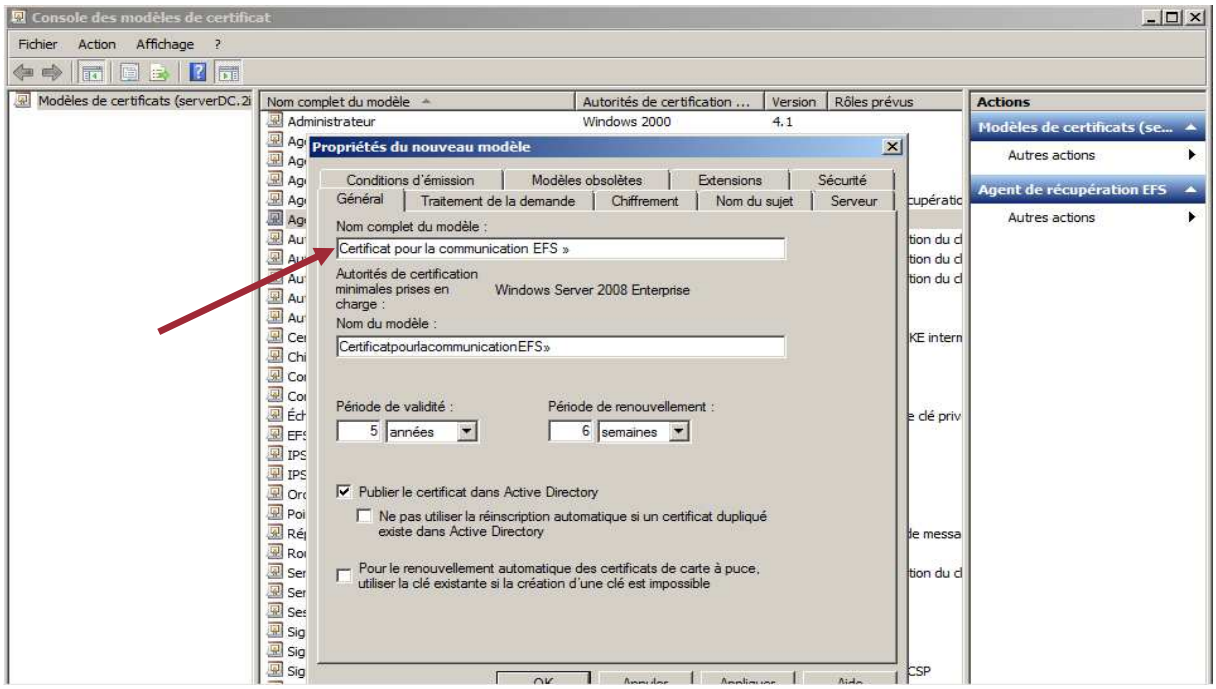


III.11.3 Création d'un certificat pour la communication EFS

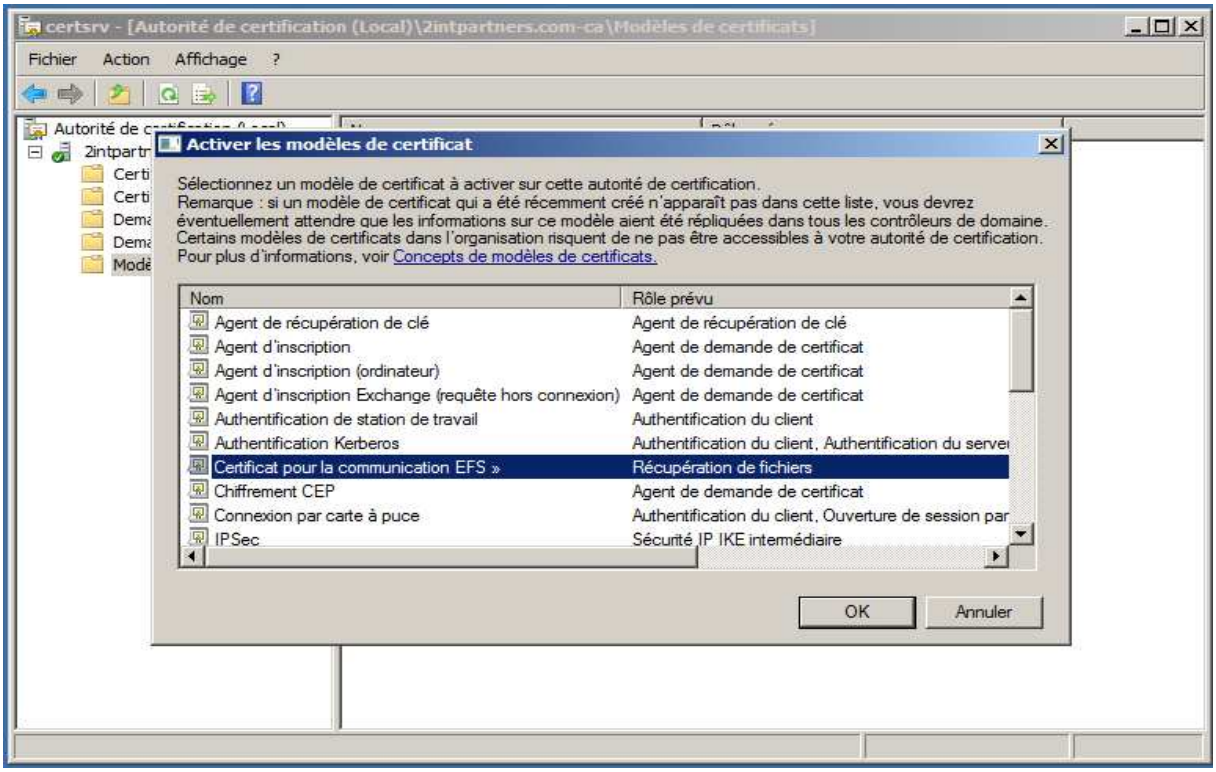
De la même façon que avec le IPsec on sélectionne EFS basique un modèle qui s'applique sur Windows 2000 dans la listes existante par défaut



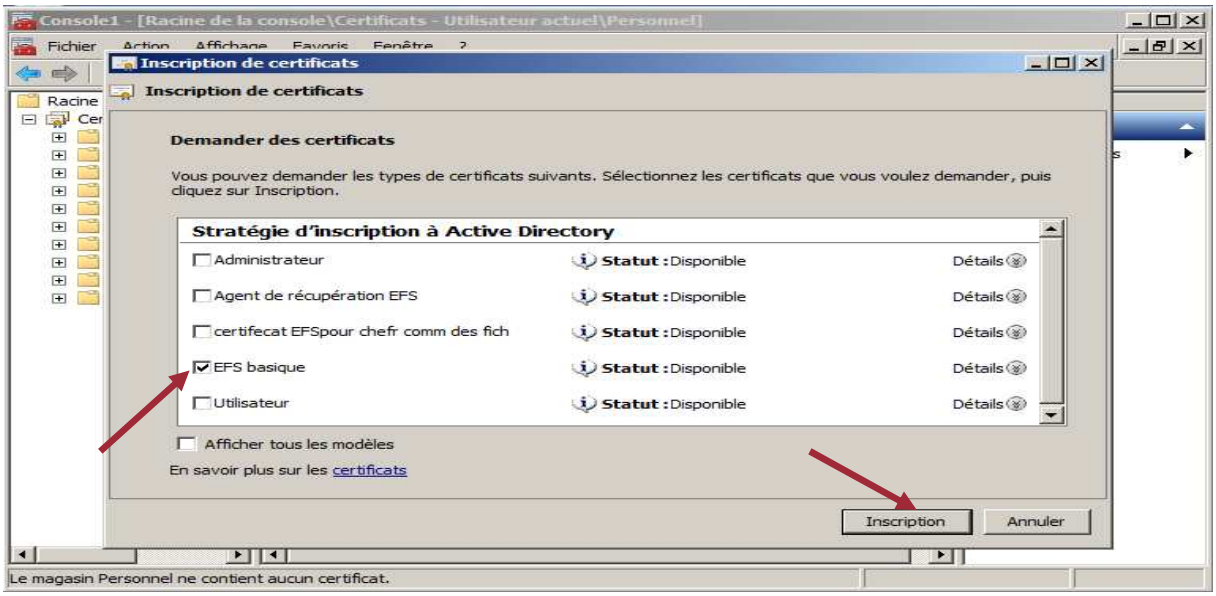
On donne un nom pour le modèle EFS



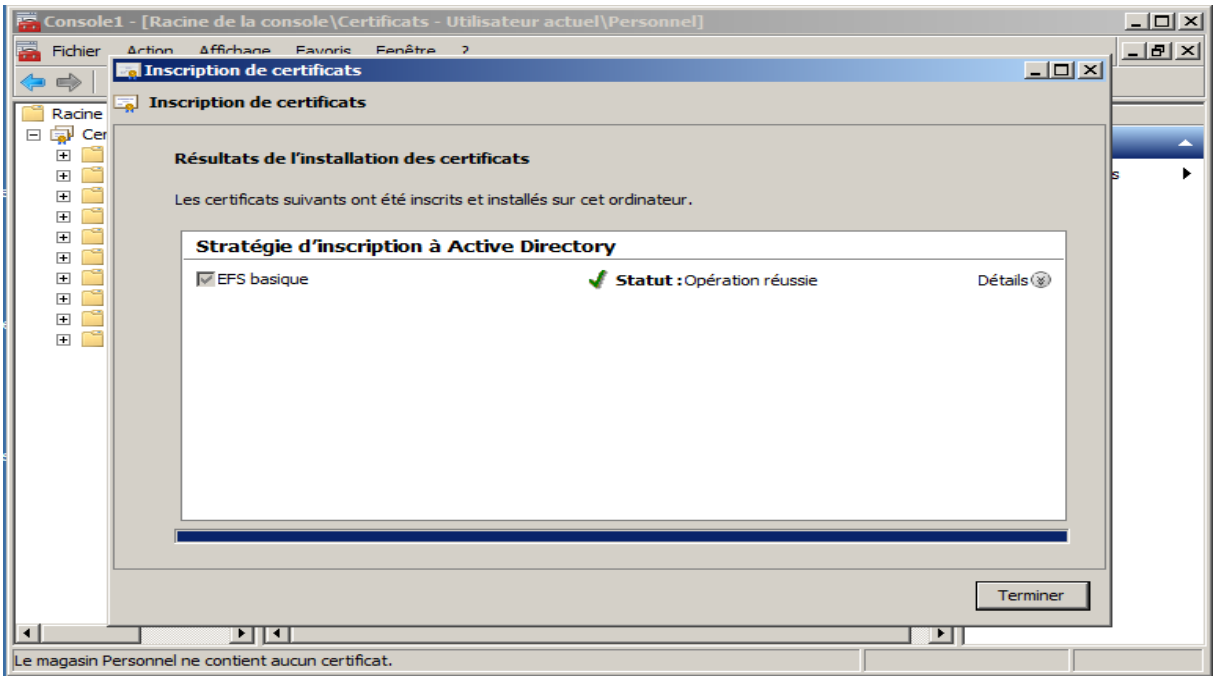
On active le modèle dupliquer sur Windows 2008



Dans la console mmc on fait une demande d'inscription de certificat, on choisi EFS basique



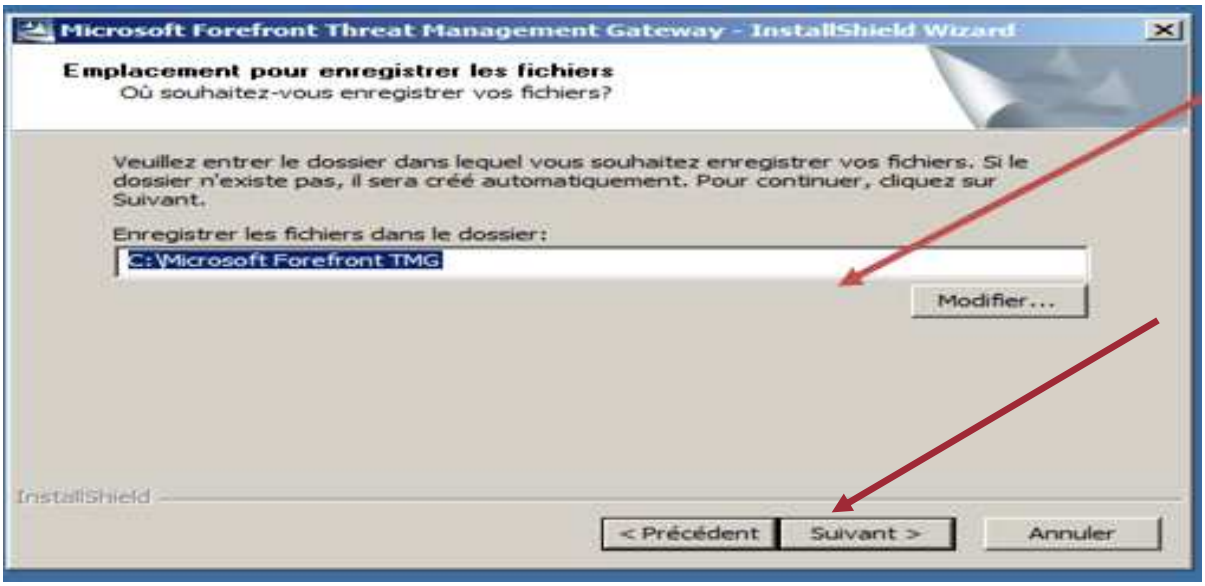
Fin de l'inscription du certificat EFS basique



III.12 **Installation de Threat Management Gateway 2010 (TMG)**

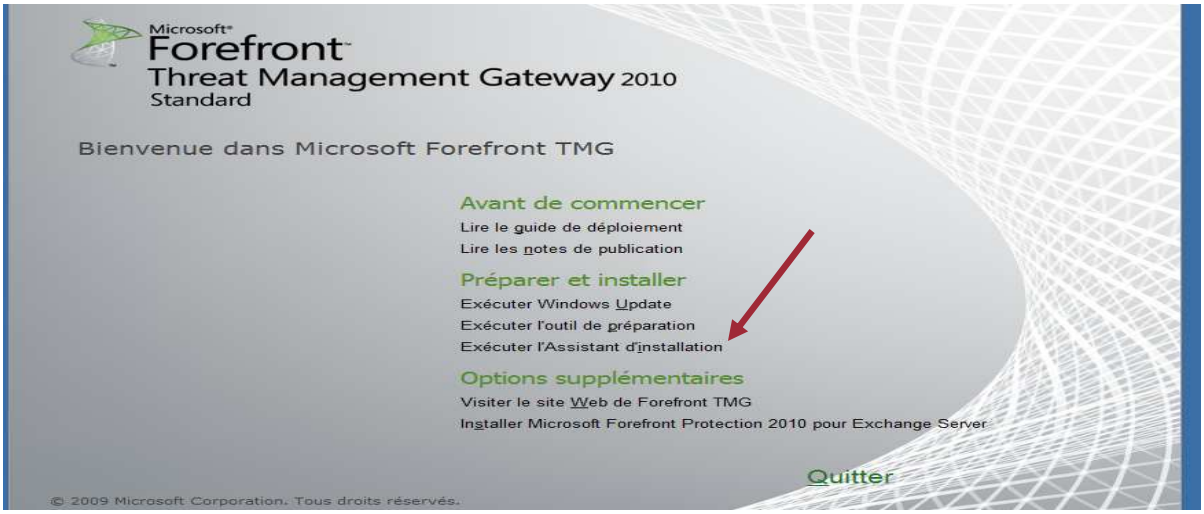
Cette solution nous a permet d'administrer de créer et de gérer toutes les fonctions de sécurité Web à partir d'une seule console dans des environnements distribués ainsi de nous fournir des rapports complets qui nous permettra de rependre aux exigences de l'entreprise. Sans oublier sa résistance aux divers attaques.

On lance l'application

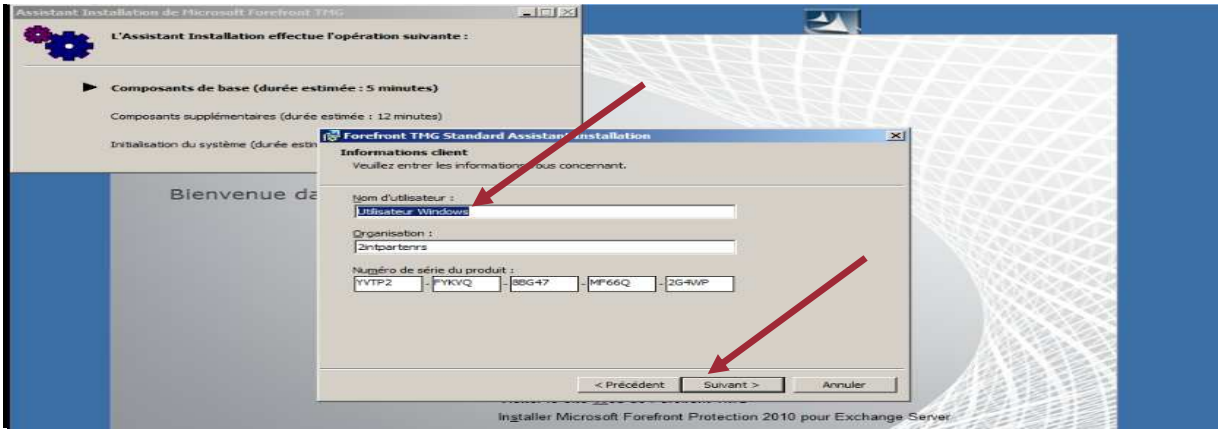


Après avoir fait une mise à jour pour le système et installer les outils de préparation pour l'installation on lance l'application TMG

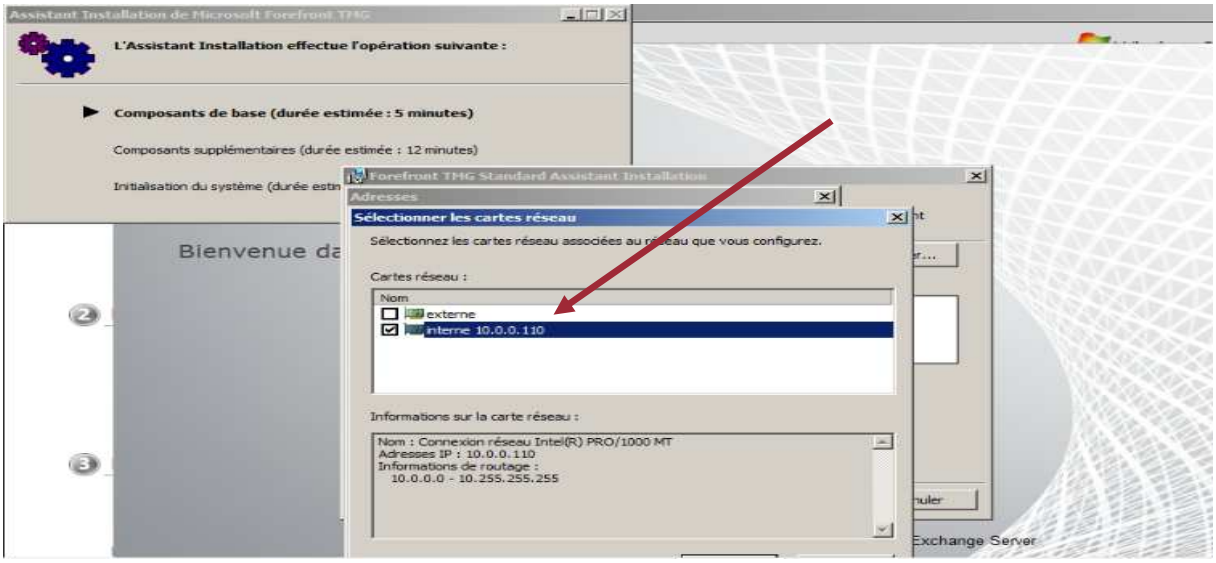
Exécuter l'assistant d'installation



On tape un nom d'utilisateur, Organisation et on clique sur suivant



On choisit la carte interne



Choisir de configurer les paramètres réseau ou de les faire ultérieurement

III.12.1 Créations de règles d'accès

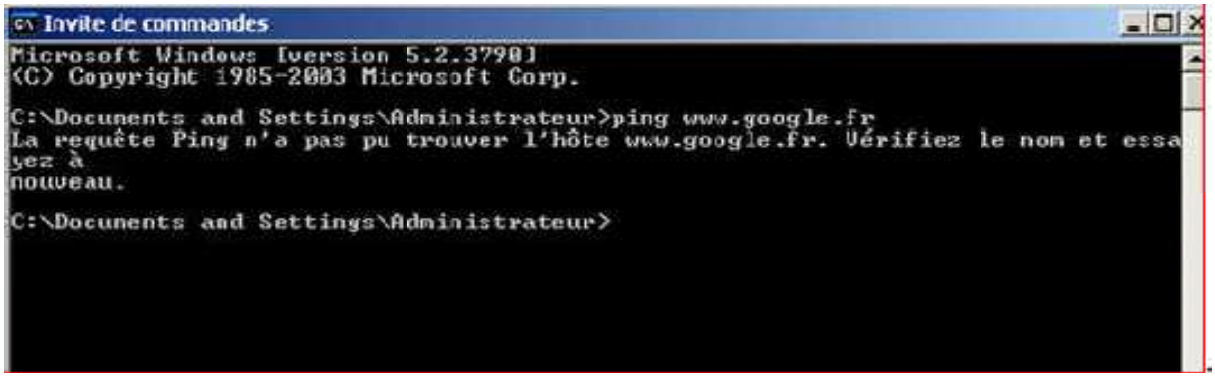
a. La règle par défaut

La première et seule règle qui existe par défaut au niveau de la TMG est celle qui dit que tout le trafic est refusé depuis tous les réseaux à destination de tous les réseaux, donc il faut autoriser les trafics supplémentaires

b. Création de la règle d'accès (http, https, FTP)

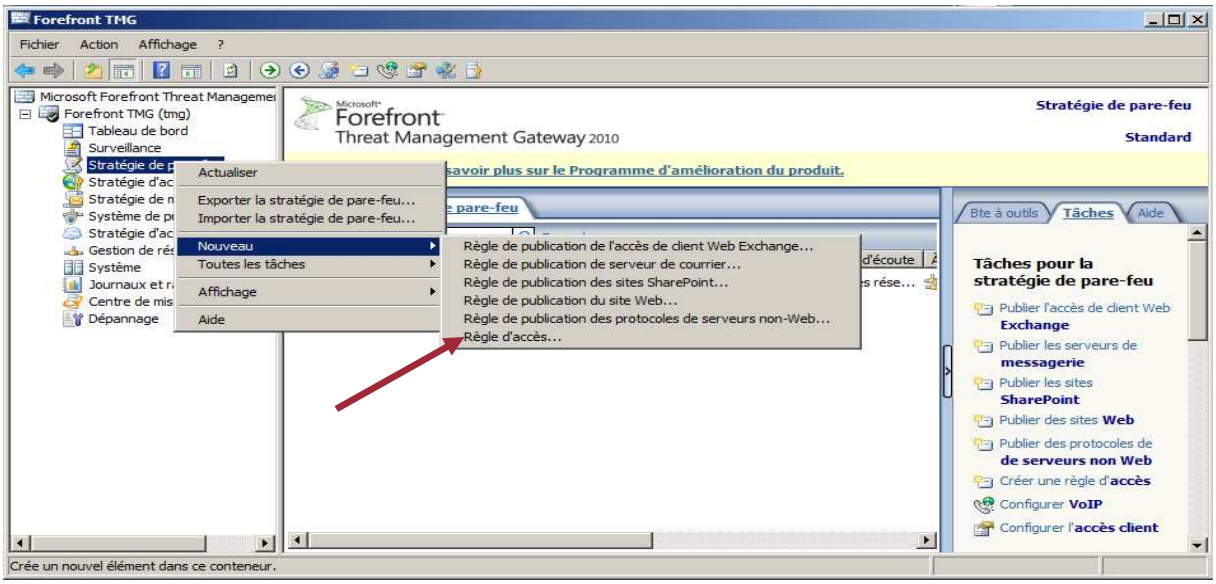
Cette règle d'accès permet aux ordinateurs du réseau interne de se connecter à internet au travers du protocole comme http, https et encore FTP depuis le réseau local.

Test avant la création de la règle : (https, http, FTP)

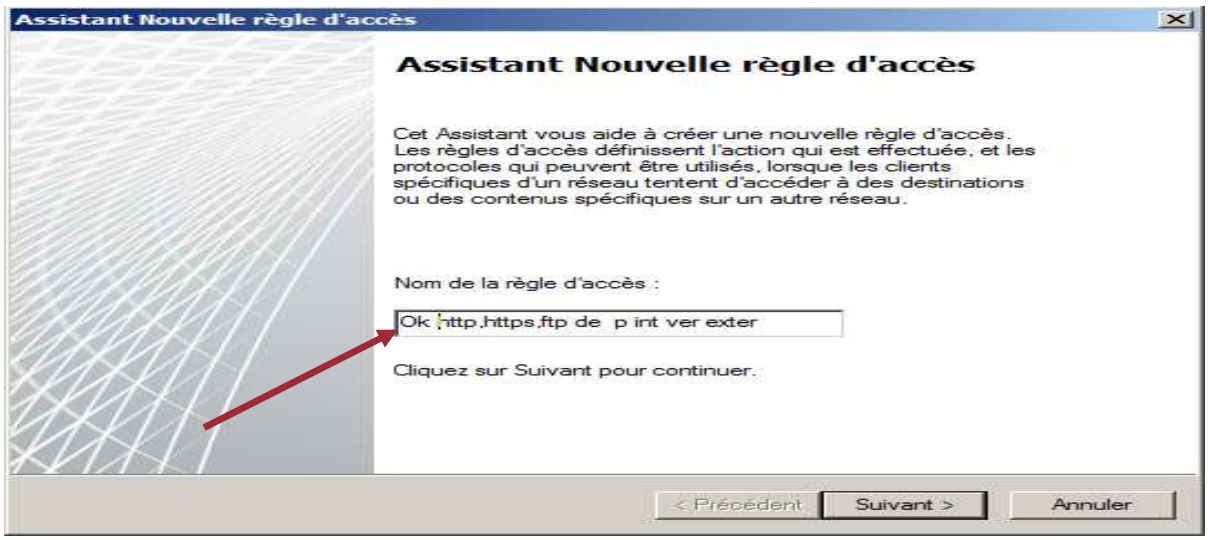


Le ping est échoué car la TMG bloque tout le trafic par défaut.

Pour créer la règle d'accès qui autorise ce trafic on suit les étapes suivantes :

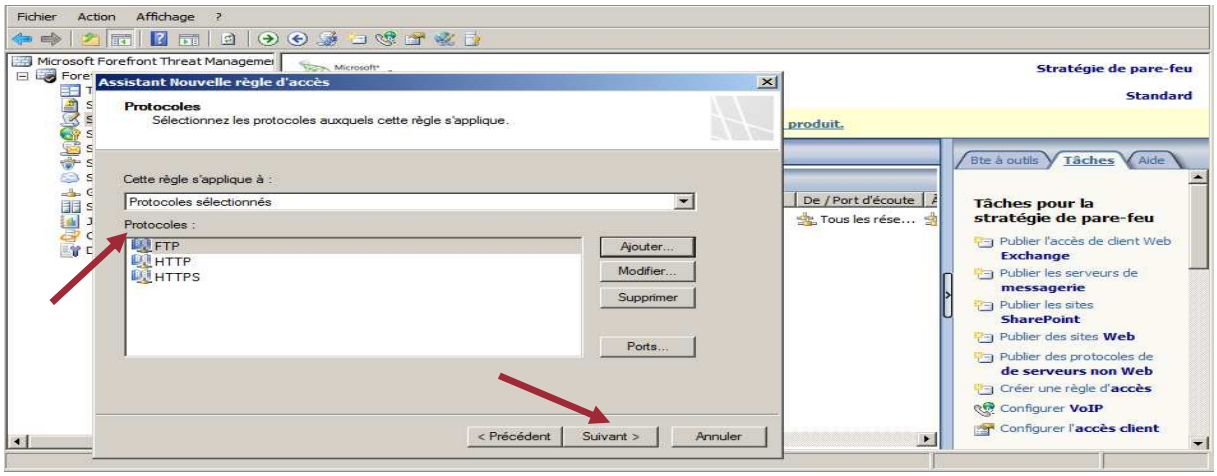


L'assistant de nouvelle règle d'accès s'ouvre, on lui effectue le nom « ok, http,https,ftp de p int ver ext», puis on clique sur suivant.



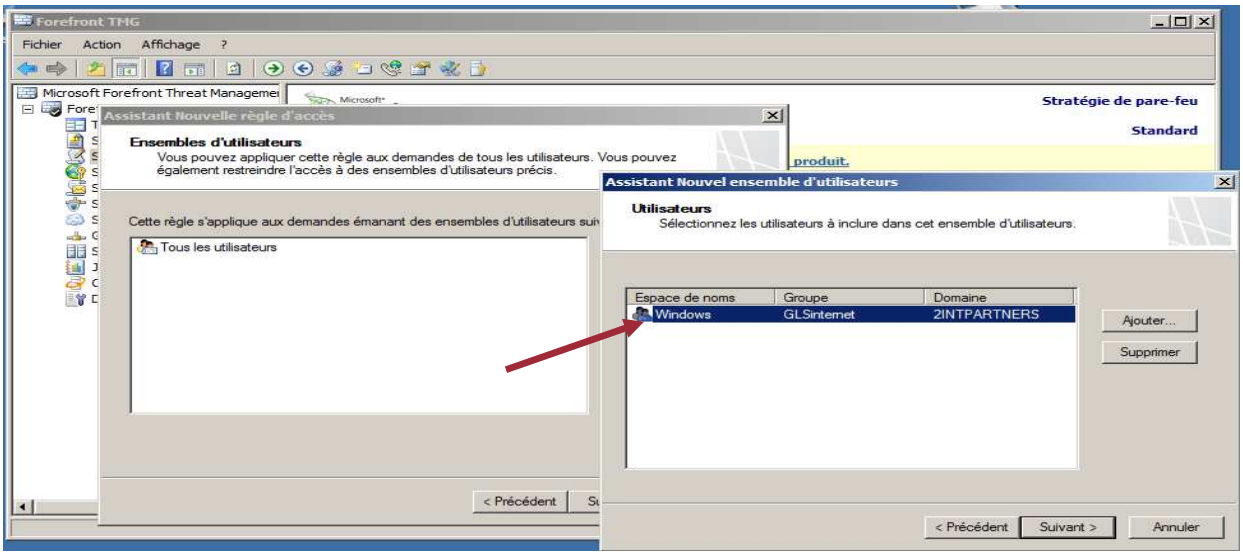
Sélection de protocole

Cette règle n'autorise pas tous le trafic mais des protocoles sélectionnés; http, https et le protocole de transfert des fichiers ftp

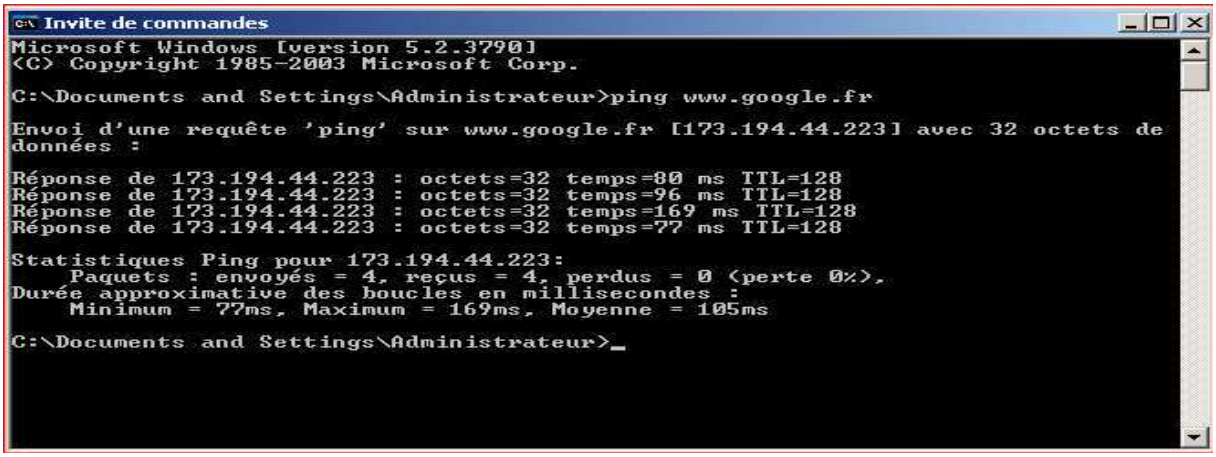


On clique sur suivant, une nouvelle fenêtre s'ouvre dont on indique la source du trafic qui est le réseau interne émanant à destination du réseau externe, on clique sur suivant

La règle par défaut s'applique sur tous les utilisateurs, on ajoute le groupe GLSinternet qui à les privilèges de se connecter et supprimer "tous les utilisateurs" et on clique sur suivant puis appliquer la règle pour finir



Test après la création de la règle :

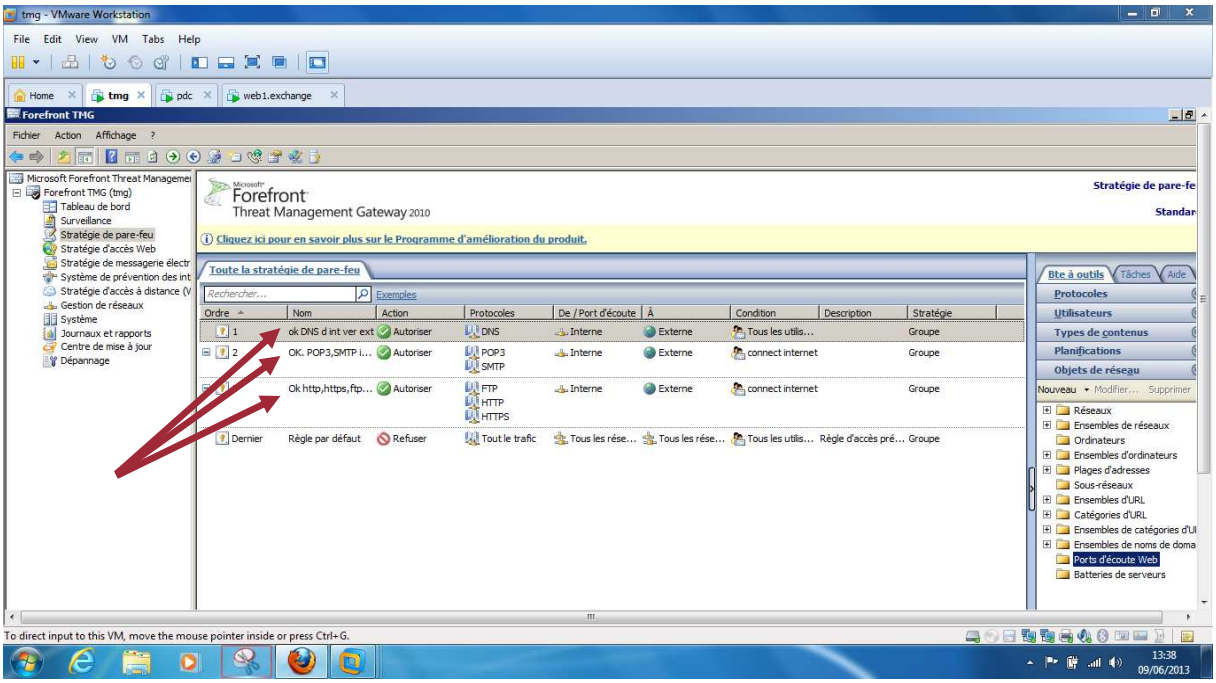


c. Autorisation de DNS et refusé tous le reste par défaut

De la même façon qu'on créer la règle précédente ,on autorise l'utilisation du DNS qui permettra la résolution des noms.

d. Autorisation de SMTP et POP3, et refusé tous le reste par défaut

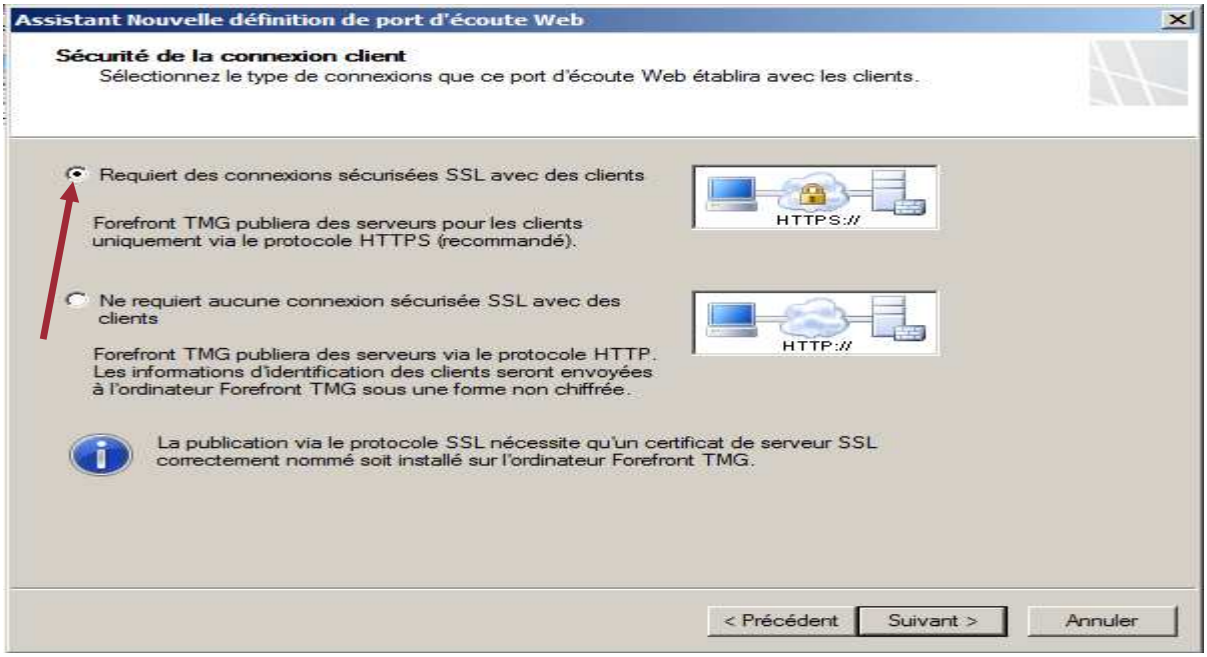
Cette règle servira à la sécurité de messagerie. Mais cette fois ici l'autorisation se fait de l'intérieur vers l'extérieur et de l'extérieur vers l'intérieur afin d'envoyer et de recevoir des messages de n'importe qu'elle endroit .



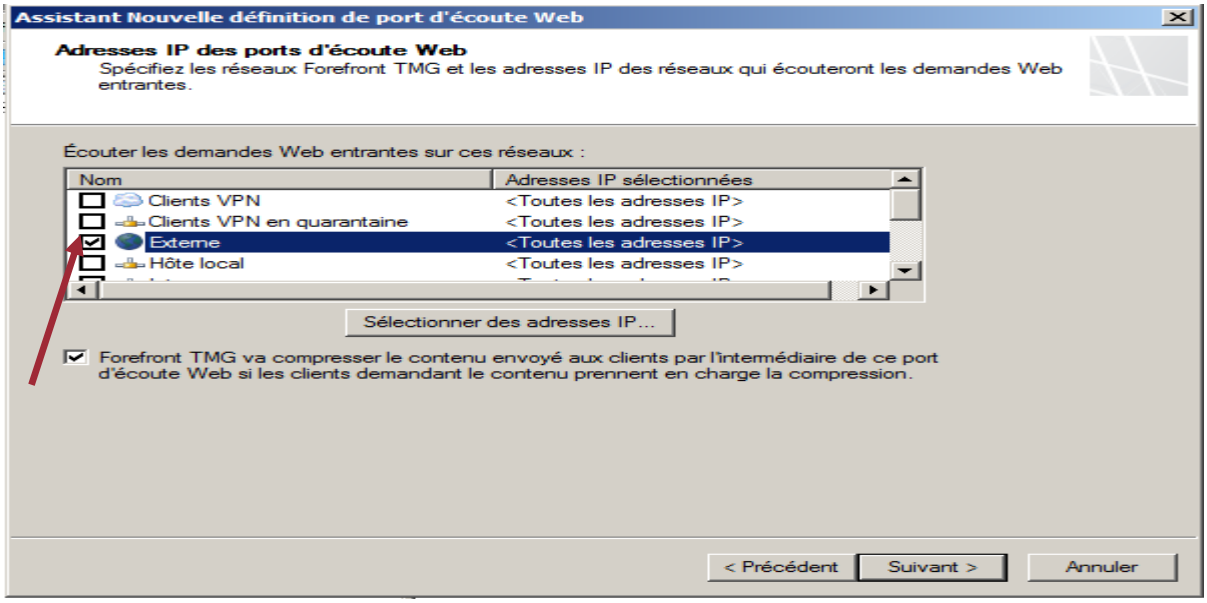
e. La configuration d'un port d'écoute

La configuration du port d'écoute pour écouter les requêtes HTTPS sur l'interface externe de carte réseau externe de TMG, On commence par un nom pour le port d'écoute

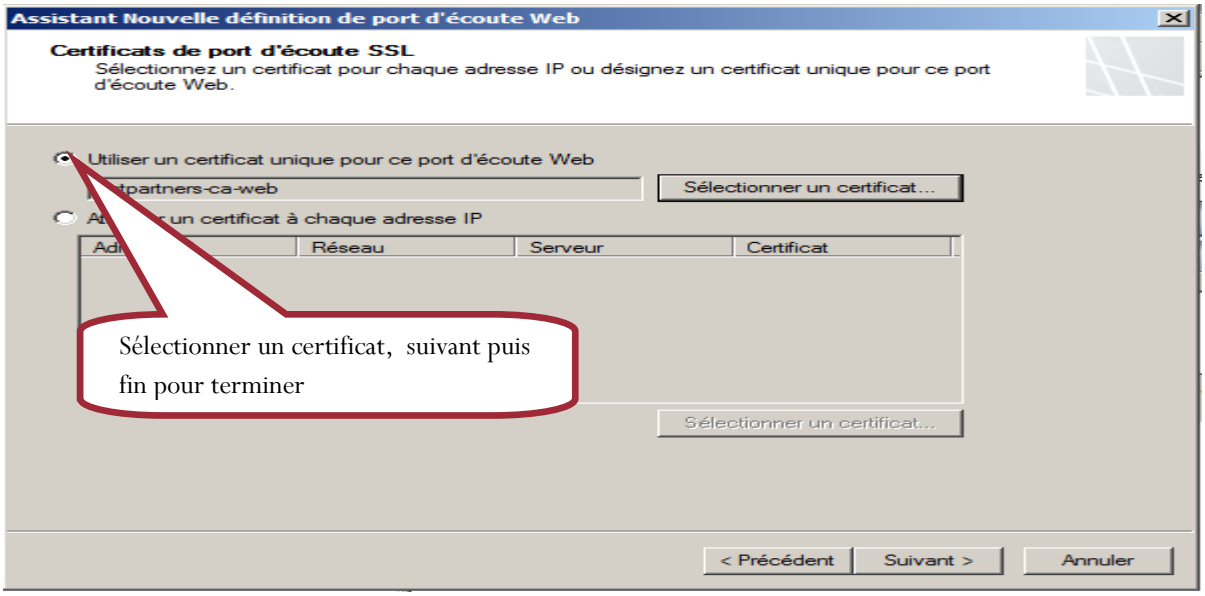
On choisi une connexion sécurisées SSL



On choisi les réseaux et les adresses IP à écouter sur web



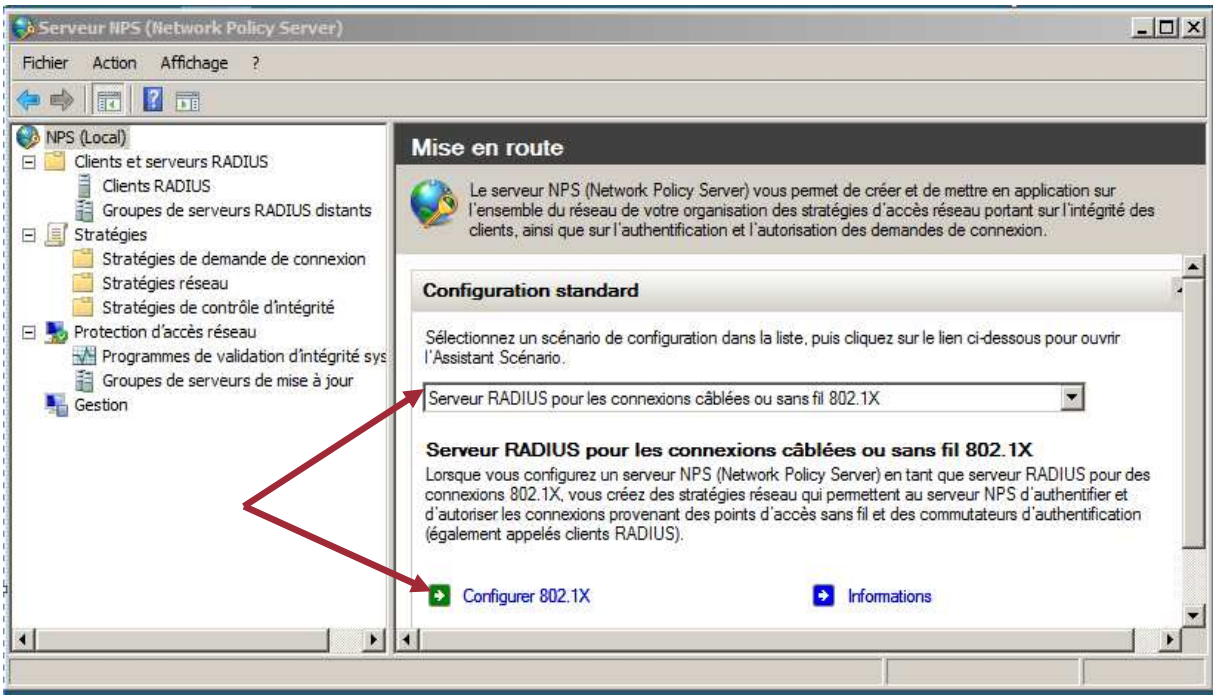
On Sélectionne un certificat pour le port d'écoute , un clique sur suivant puis terminer



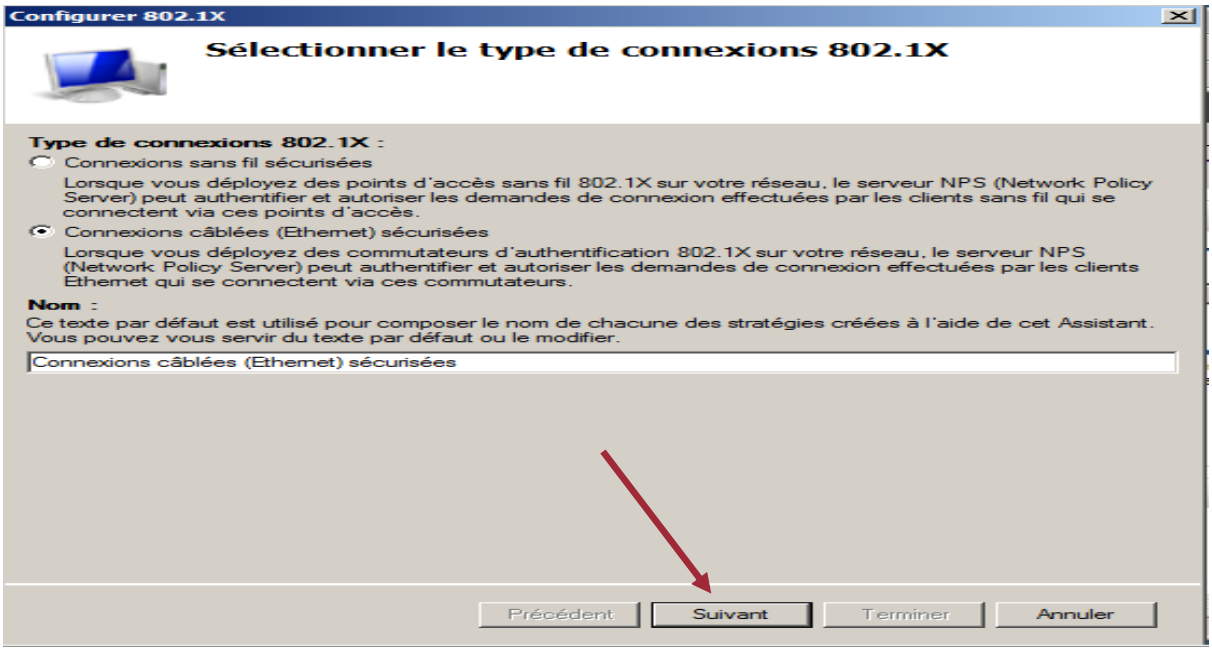
III.13 Le serveur d'authentification Radius (NPS)

a) Stratégie d'authentification réseau

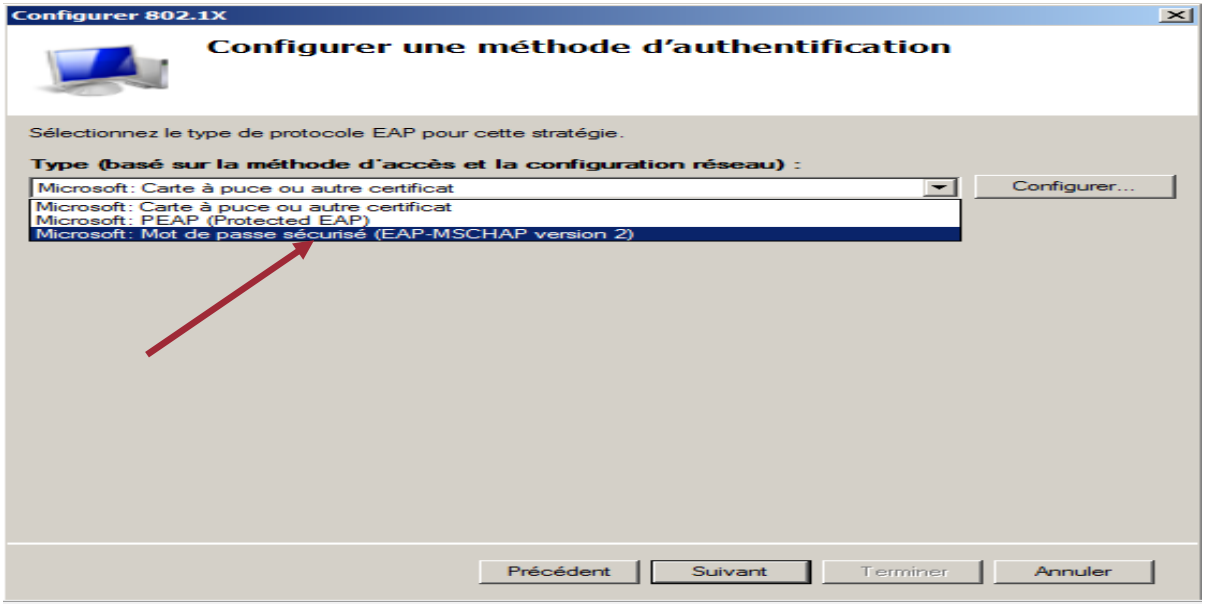
✓ Authentification RADIUS (Choisir serveur RADIUS pour les connexions câblées ou sans fil 802.1X puis on clique sur configurer 802.1X)



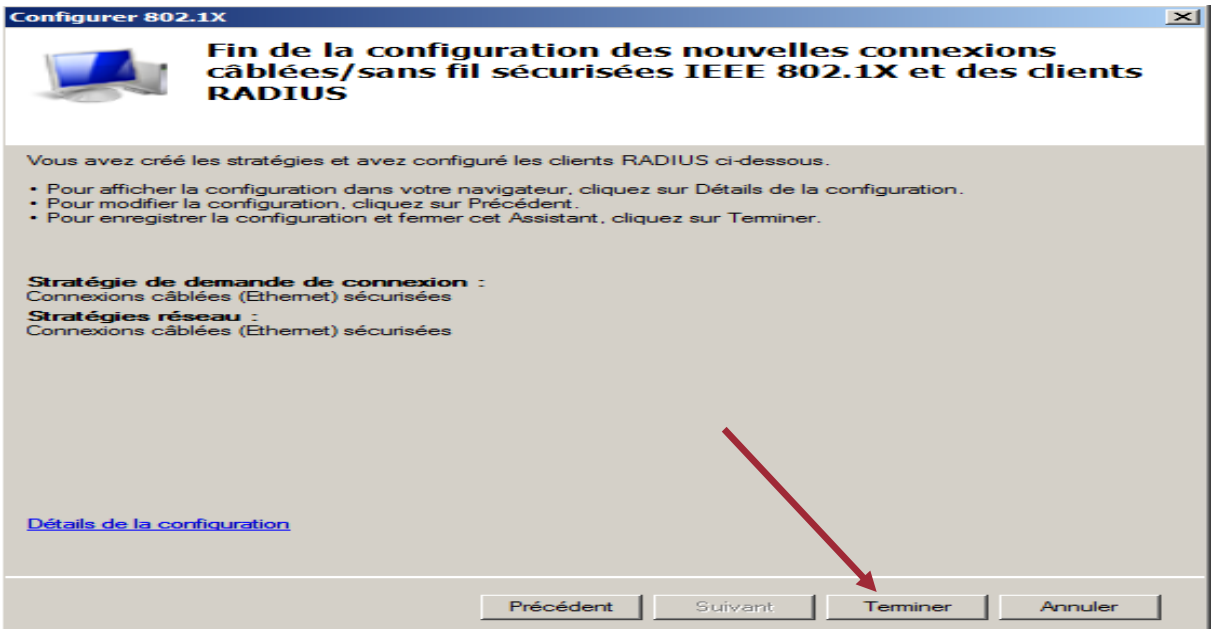
On choisir les connexions câblées (Ethernet) sécurisées puis suivant



On choisi la méthode d'authentification à configurer et on clique sur suivant



Pour finir cette configuration des nouvelles connexions câblées sécurisées IEEE 802.1X et des clients RADIUS on clique sur terminer

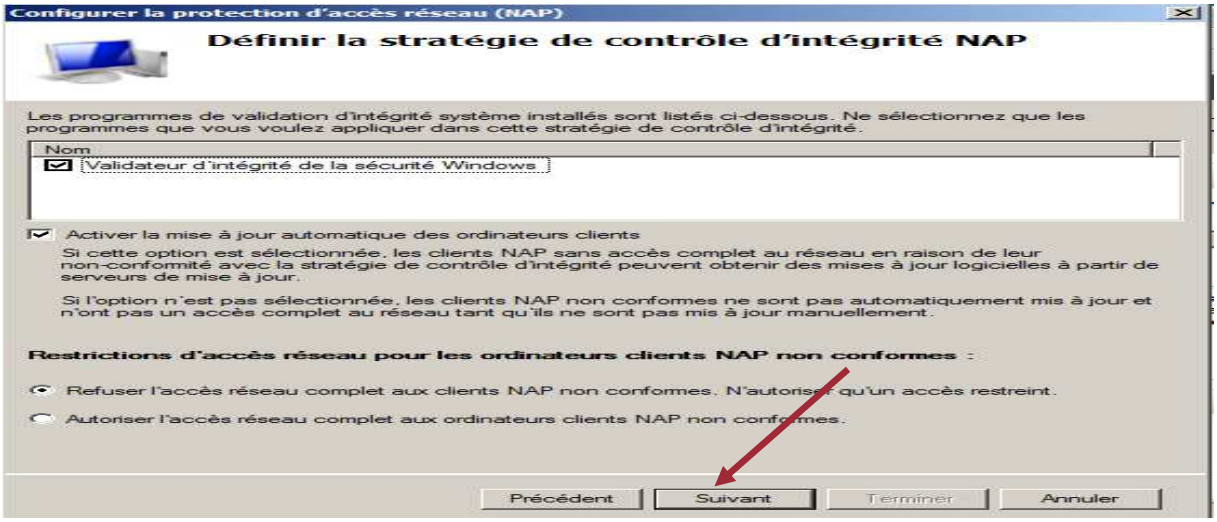


✓ Authentification par le NAP

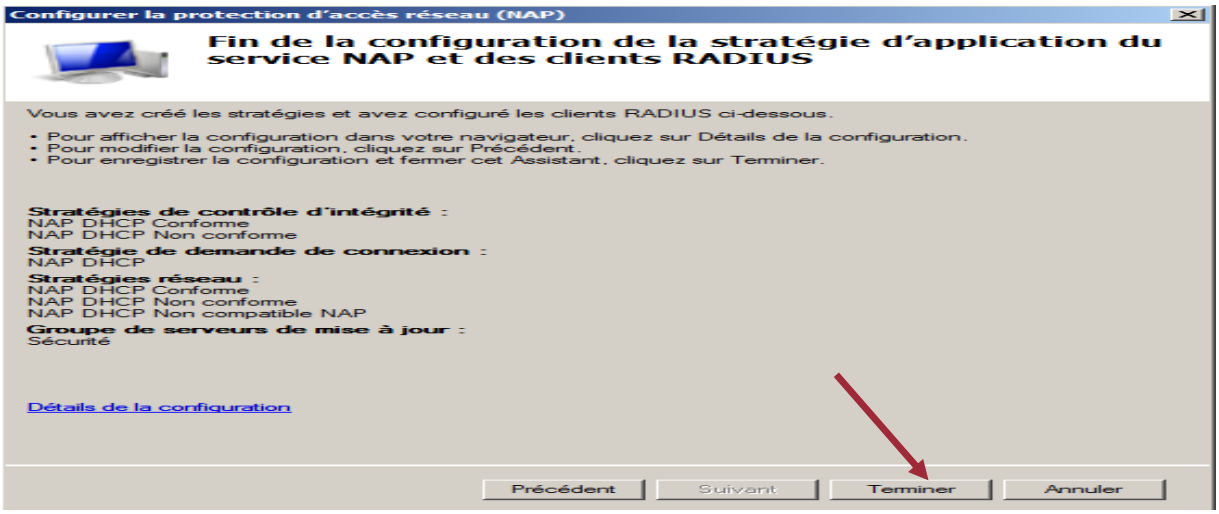
On commence par choisir la protection d'accès réseau (NAP) puis un clique sur "Configurer la protection d'accès réseau (NAP)

On choisi le protocole DHCP comme méthode de connexion réseau à utiliser avec la protection d'accès réseau NAP

Refus de l'accès réseau aux clients non conforme

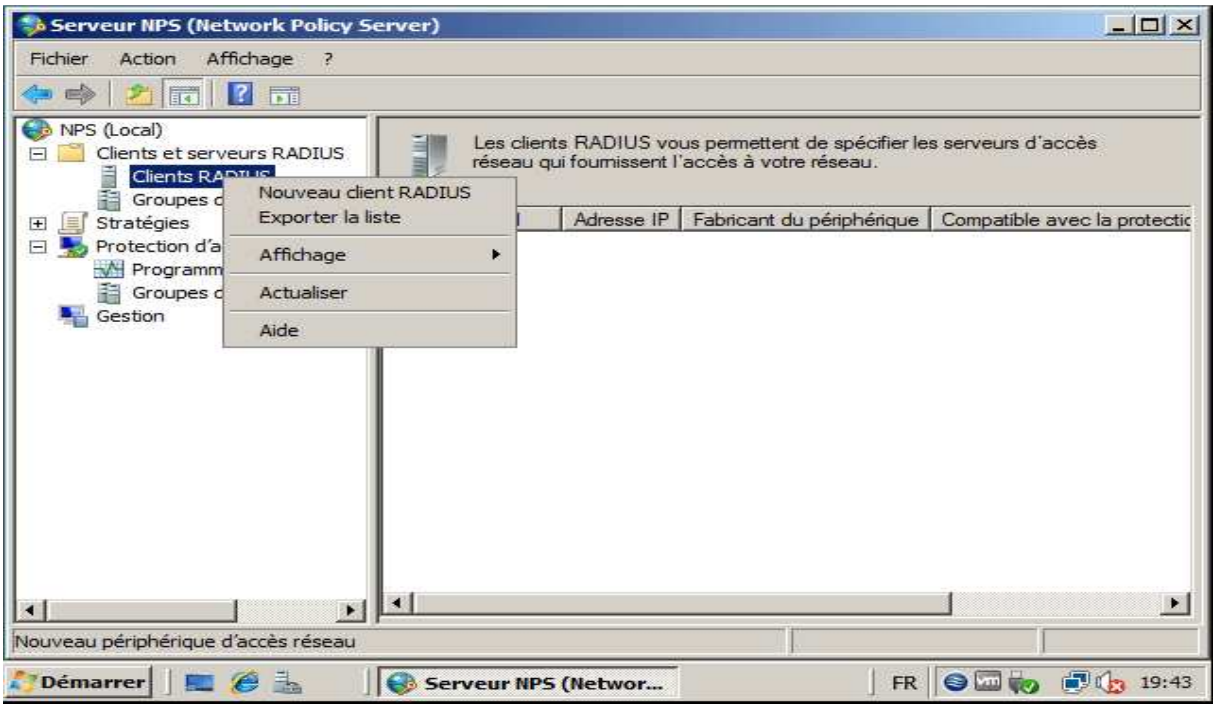


Cette page résume tous les paramètres qu'on a configurer pour le NAP, On clique sur terminer pour finir la configuration

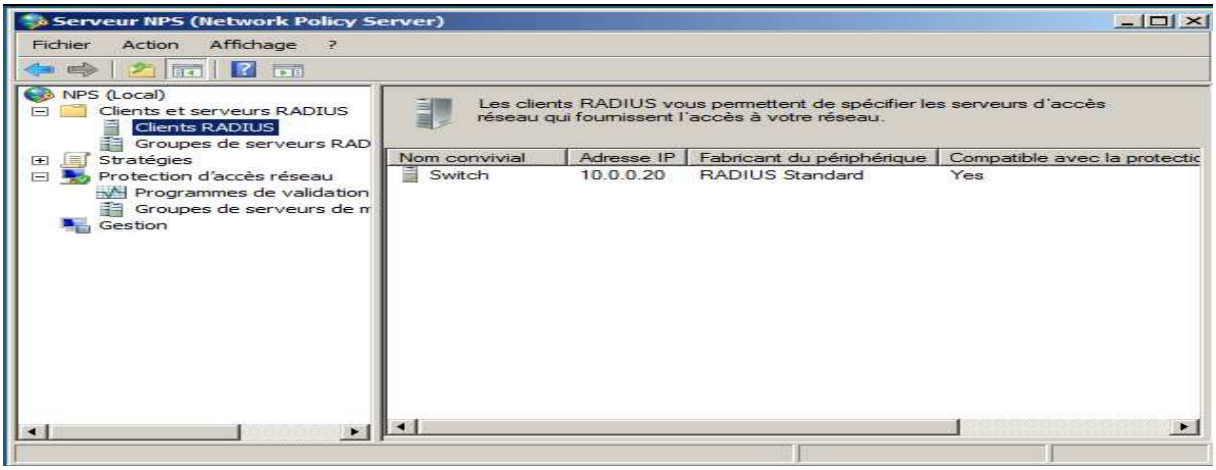


III.13.1 Ajout des Clients RADIUS

Le conteneur Clients RADIUS l'ensemble des serveurs d'accès distants qui sont des clients vis-à-vis du serveur NPS. Pour qu'un serveur d'accès distant fasse partie de cette liste, il suffit de l'y ajouter en utilisant l'assistant Ajouter un client RADIUS



Les équipements réseaux (Switch, Serveur…) doivent être ajoutés en tant que client RADIUS. Pour qu'ils soient reconnus au niveau de serveur RADIUS. Donc pour ajouter un client RADIUS, il suffit d'entrer son nom de domaine DNS ou bien son adresse IP ainsi qu'une chaîne de caractère permettant de le reconnaître facilement. Il faut ensuite choisir le type de technologie RADIUS à utiliser (ici RADIUS standard), une clé partagée (optionnelle) pour crypter et décrypter les échanges entre le client RADIUS et le serveur NPS. On peut aussi côcher la case « **Les requêtes doivent contenir l'attribut de l'authentificateur de message** » qui aura pour effet de forcer le client RADIUS à s'authentifier à chaque connexion auprès du serveur NPS en envoyant une signature numérique. On termine par ok

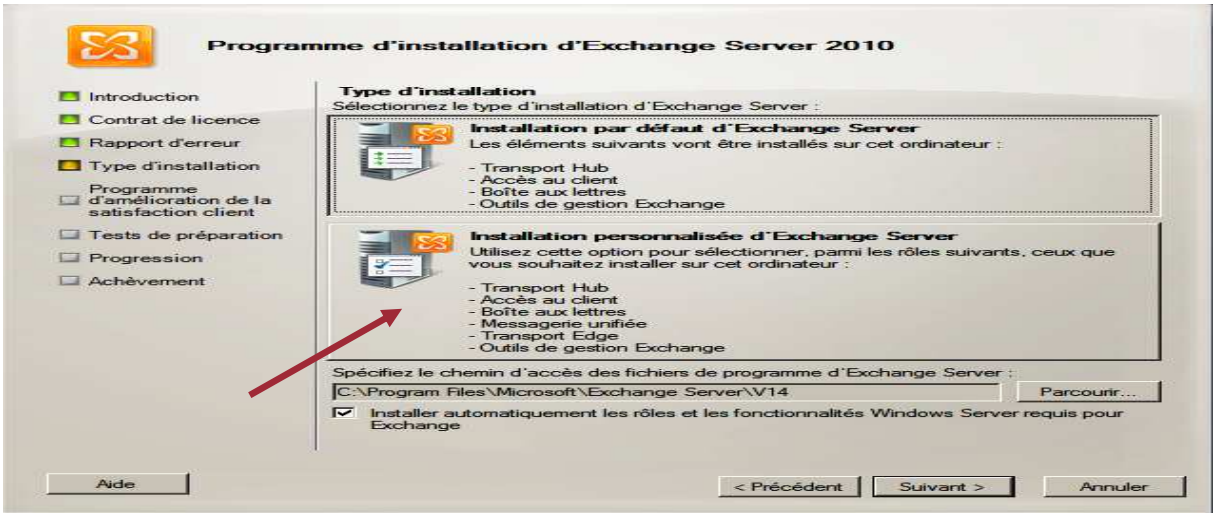


III.14 Installation d'exchange

Lancement du programme d'installation

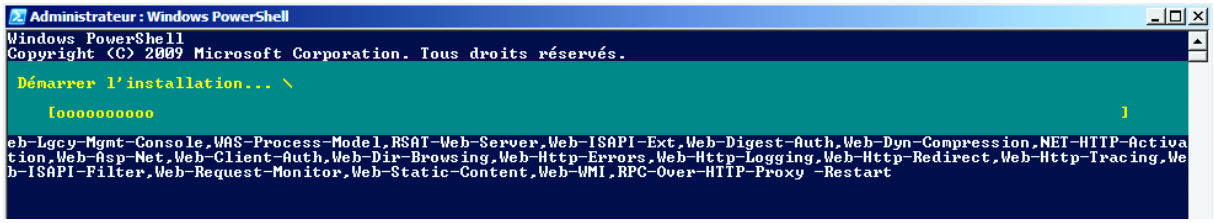
Appuis sur installer Microsoft Exchange pour continuer l'installation

Choisir le mode d'installation puis suivant

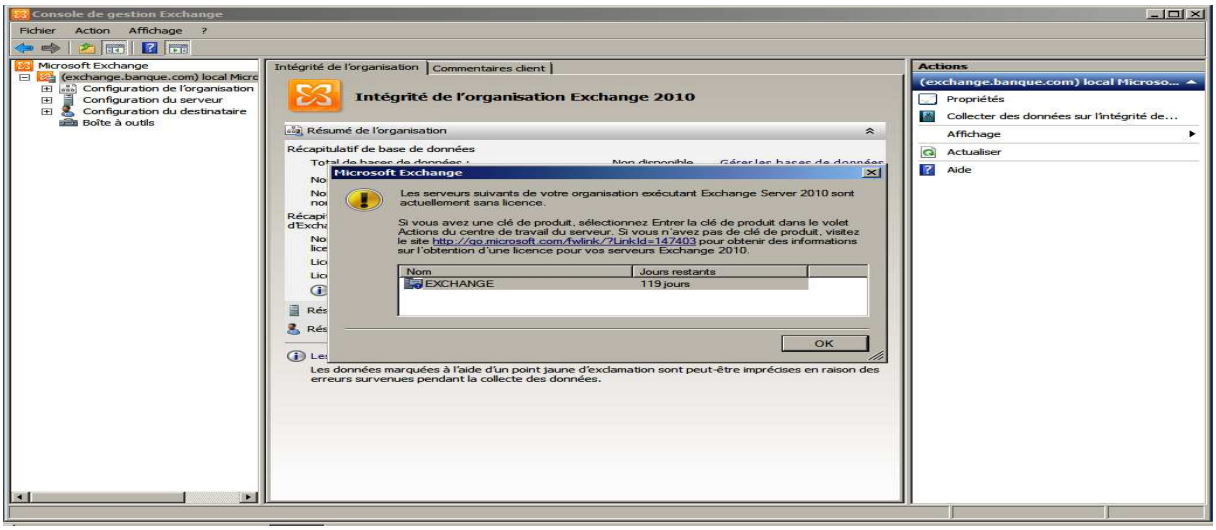


Confirmer s'il y'a des clients exécutant Outlook 2003

Démarrage de l'installation dans le PowerShell

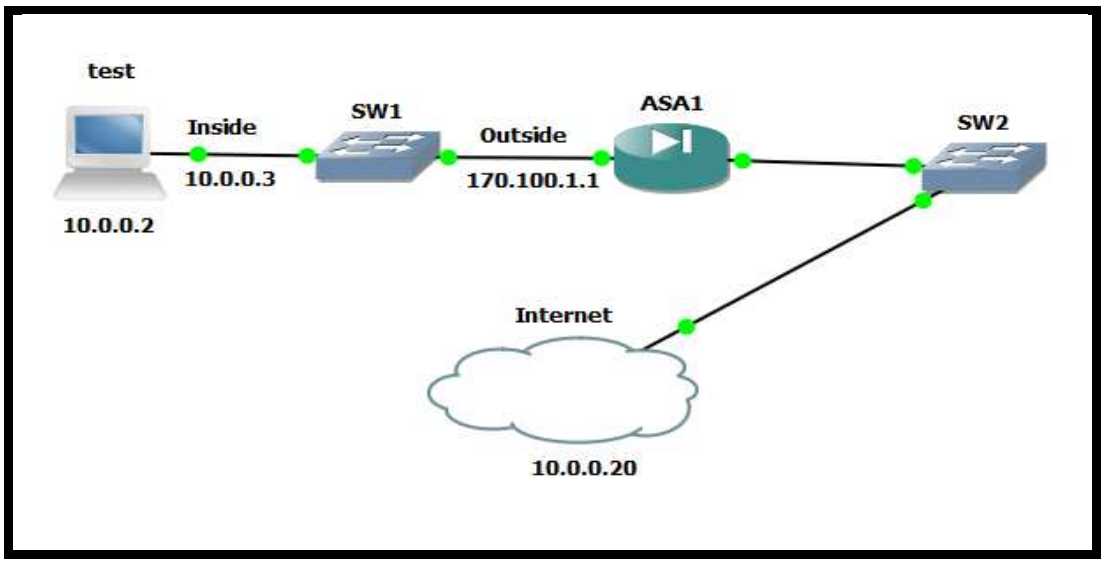


Interface graphique de L'Exchange 2010



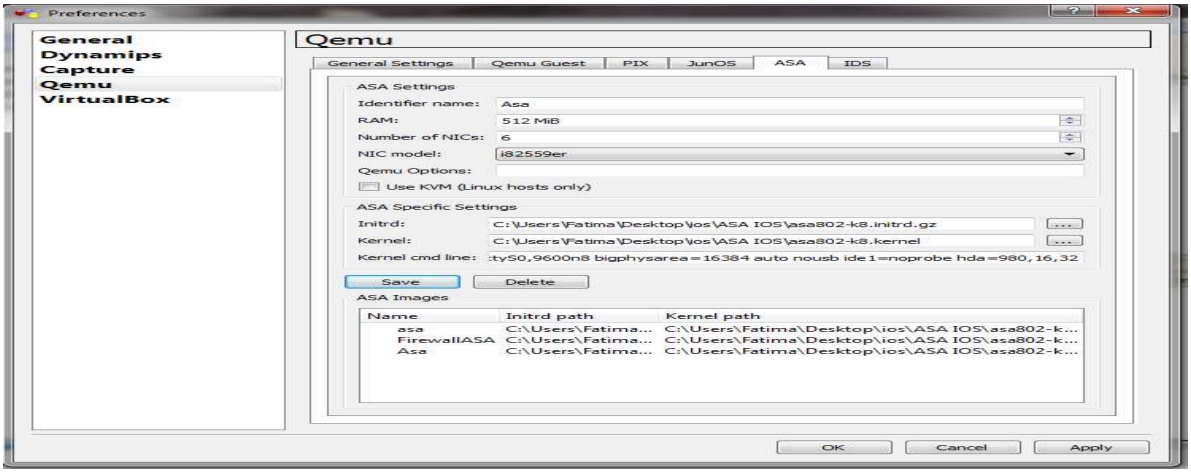
III.15 Mise en place de firewall

Dans GNS3 on a pu réaliser l'architecture suivant qui nous permettra de configurer le ASA et d'installer la console asdm

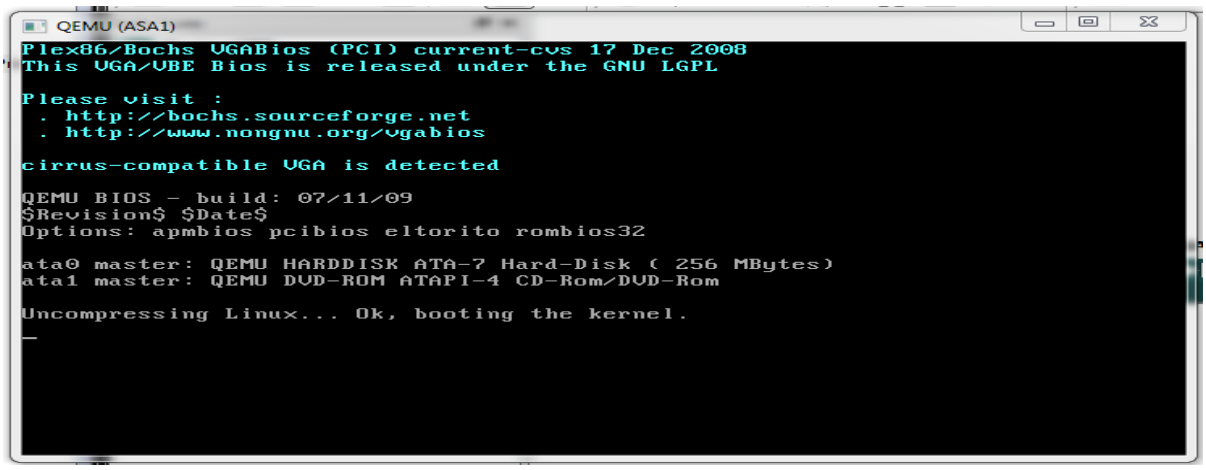


a) Configuration d'ASA

Chargement de l'image système asa 5010 et de lui donner un nom puis un clique sur save



Démarrage du système



Configuration de la console du pare-feu ASA

Copier le fichier asdm-647.bin à la mémoire flash

```
ASA1(config)# copy tftp: flash:
Address or name of remote host []? 10.0.0.2
Source filename []? asdm-647.bin
Destination filename [asdm-647.bin]?
Accessing tftp://10.0.0.2/asdm-647.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Vérification du contenu de la mémoire flash

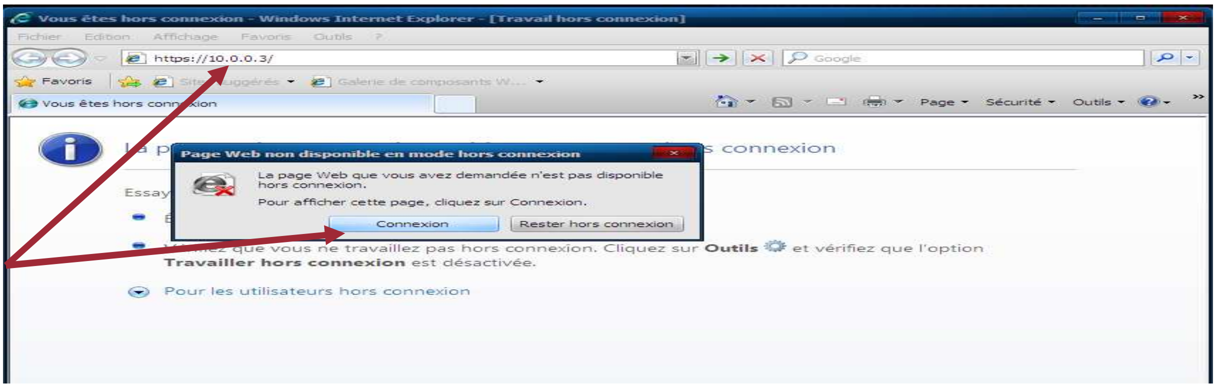
```
ASA1(config)# show flash
--#--  --length--  -----date/time------  path
    6  4096        Apr 25 2013 20:06:13  .private
    7  0           Apr 25 2013 19:51:18  .private/mode.dat
    8  0           Apr 25 2013 20:34:52  .private/DATAFILE
    9  1587        Apr 25 2013 20:34:52  .private/startup-config
   10  4096        Apr 25 2013 20:09:59  boot
   11  0           Apr 25 2013 20:34:52  boot/grub.conf
   13  17902288    Apr 25 2013 20:37:39  asdm-647.bin

255320064 bytes total (194011136 bytes free)
ASA1(config)#
```

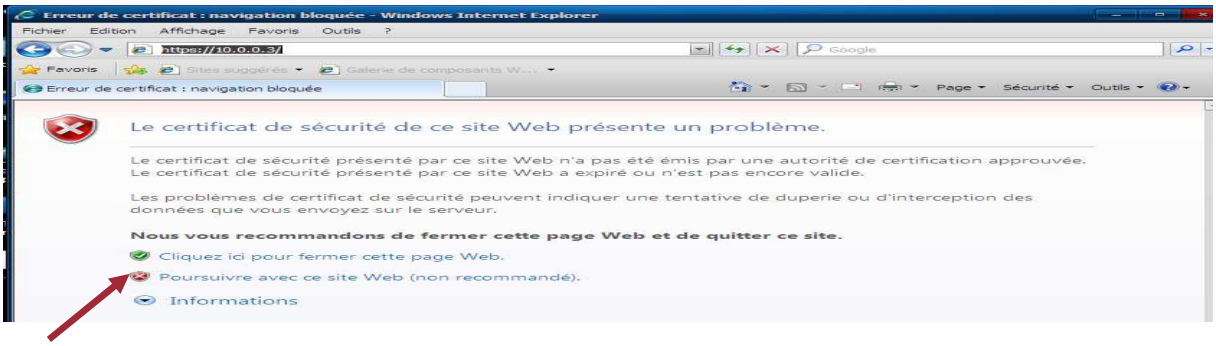
Configuration du serveur http

```
asa1(config)# exit
asa1# conf t
asa1(config)# http server enab
asa1(config)# http 10.0.0.2 255.255.255.255 inside
asa1(config)#
```

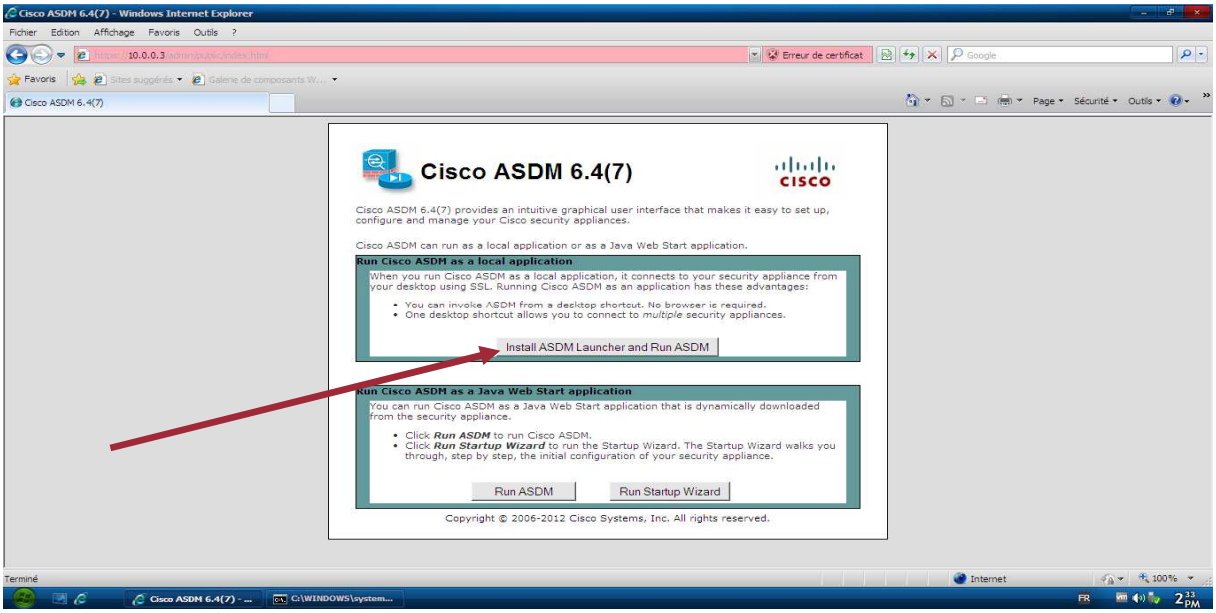
Dans URL d'internet explorer en tapes l'adresse de l'interface Inside, il est obligatoire d'utilisé https sinon sa marche pas



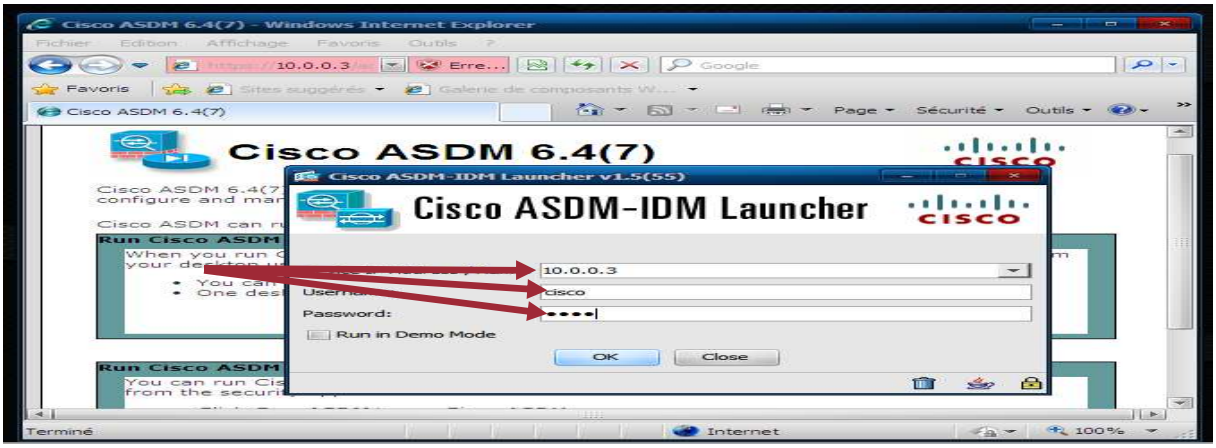
Poursuivre avec ce site web



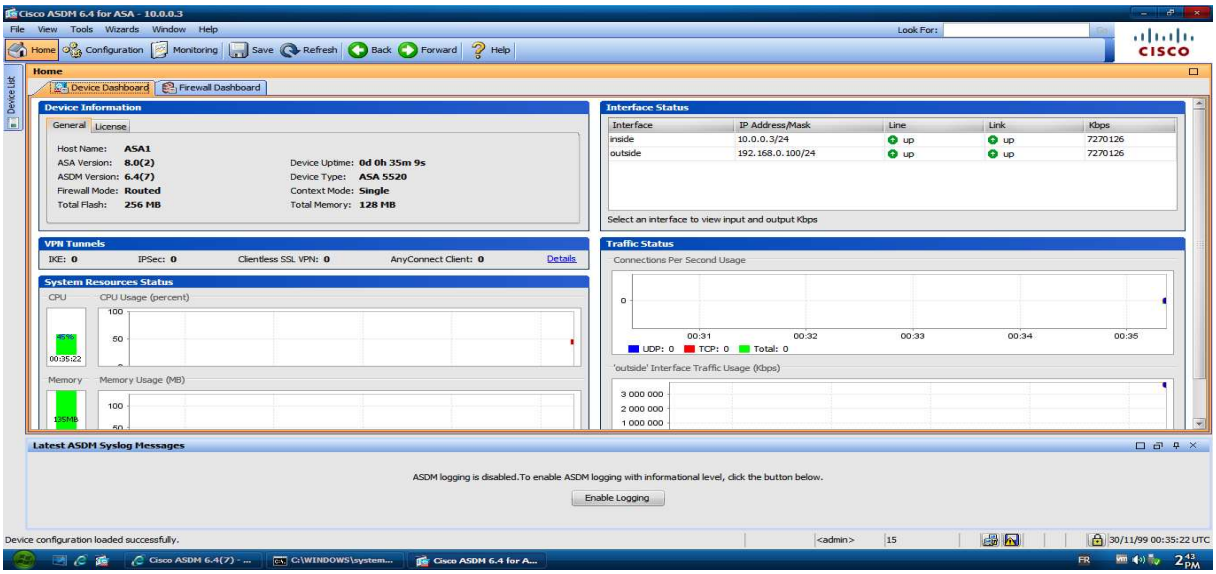
Installation d'ASDM



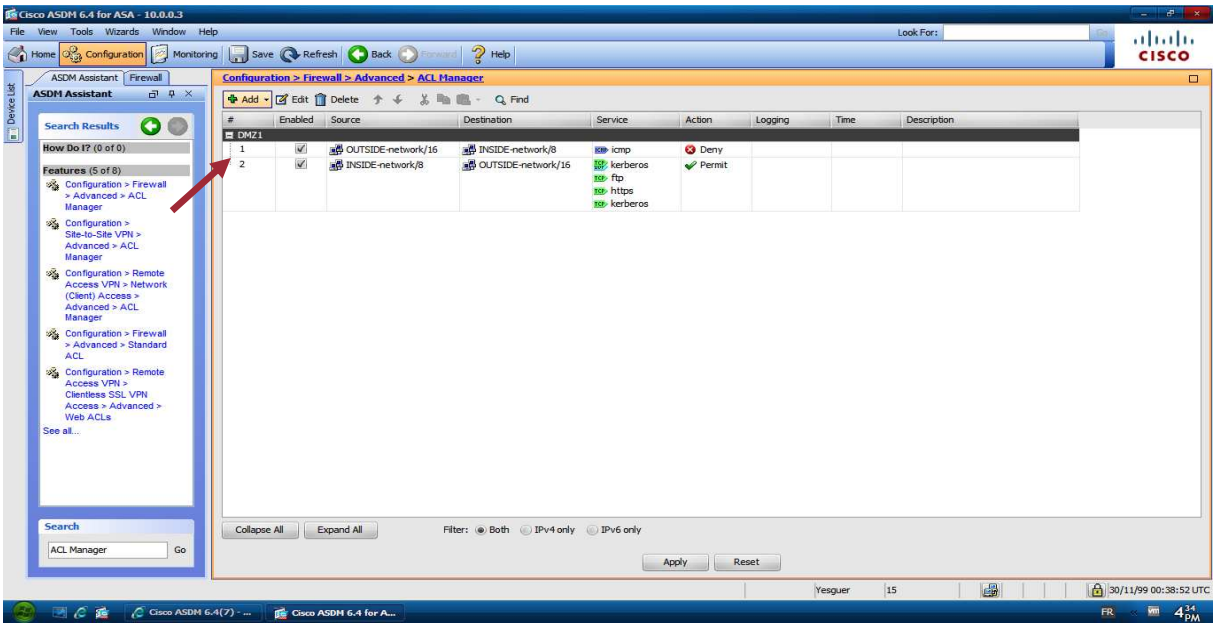
Accès à l'interface graphique



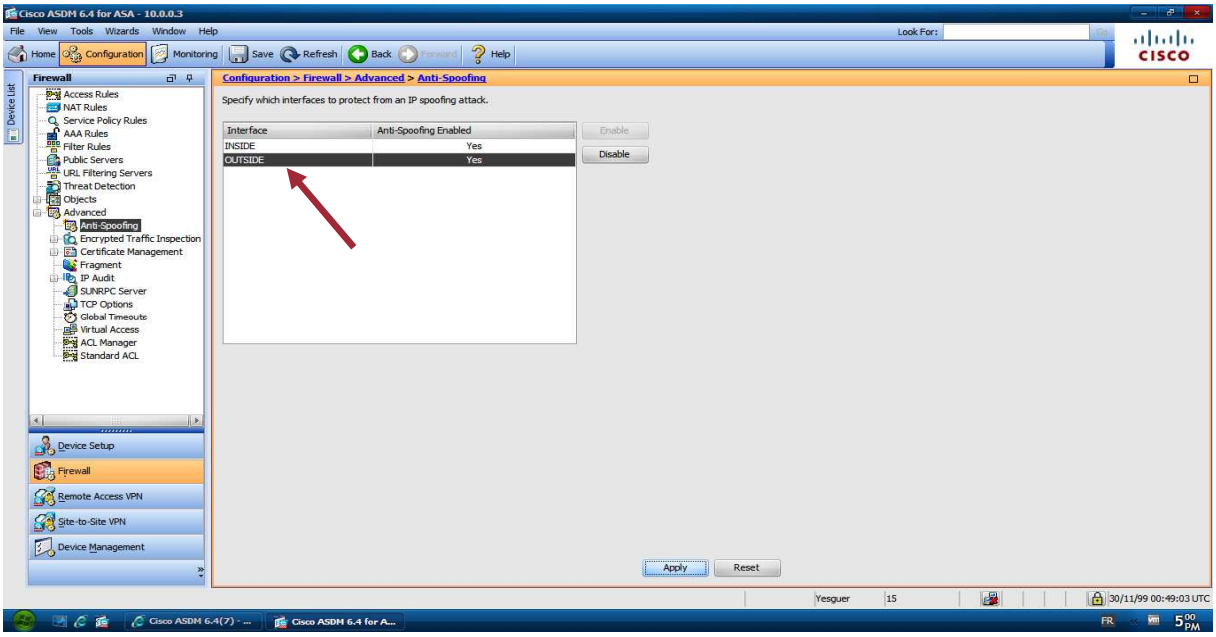
L'interface graphique de l'asdm



Nous avons créer deux règles dans la DMZ du ASA dont la premier est d'interdise le ping de l'extérieur de l'entreprise vers l'intérieurs, la deuxième c'est d'autoriser les protocoles http,https pour utiliser la connexion internet et le protocole ftp ajouter au protocole kerberos qui est un protocole d'authentification de l'active directory



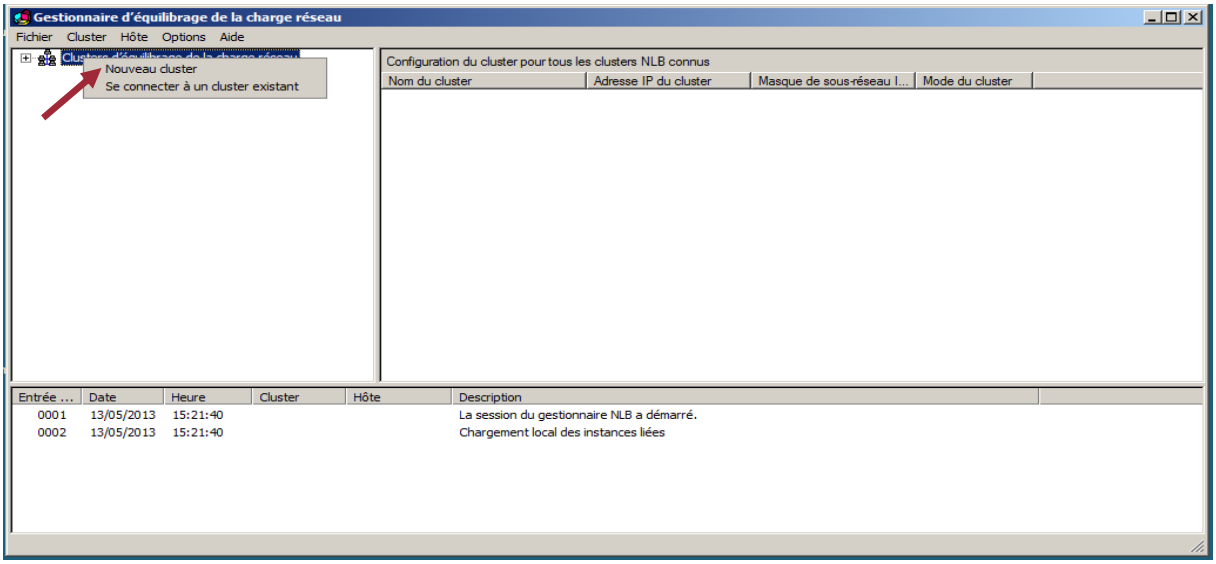
Activation de l'anti-Spoofing



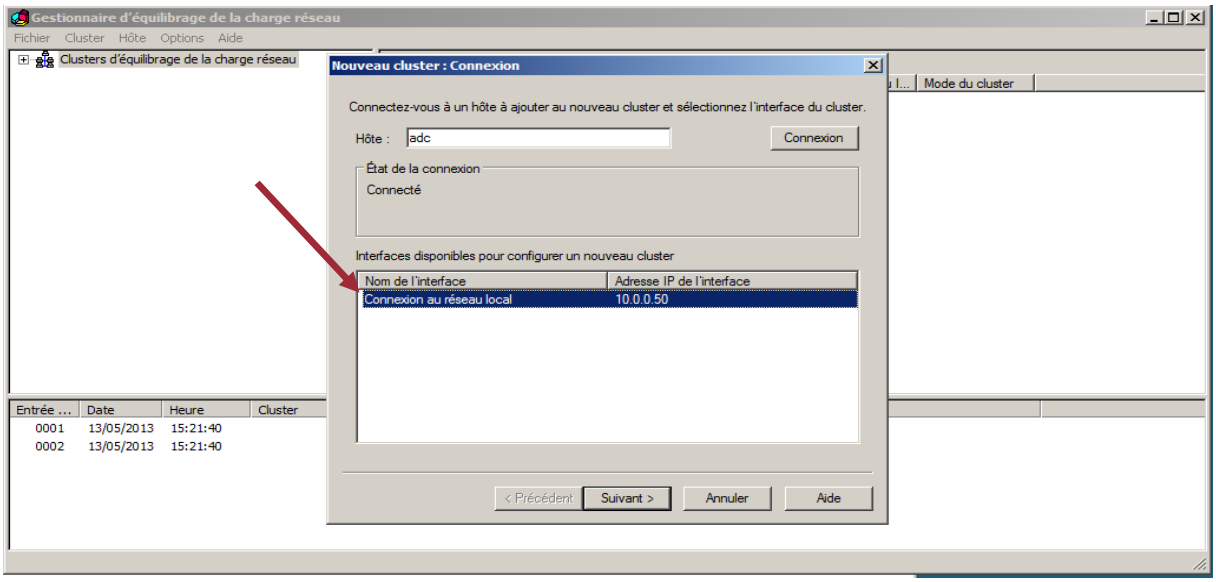
III.16 Gestionnaire d'équilibrage de charge réseau

Dans les fonctionnalités on ajoute le gestionnaire d'équilibrage de charge puis on crée un nouveau cluster et on le configure tel indiqué dans les étapes suivantes :

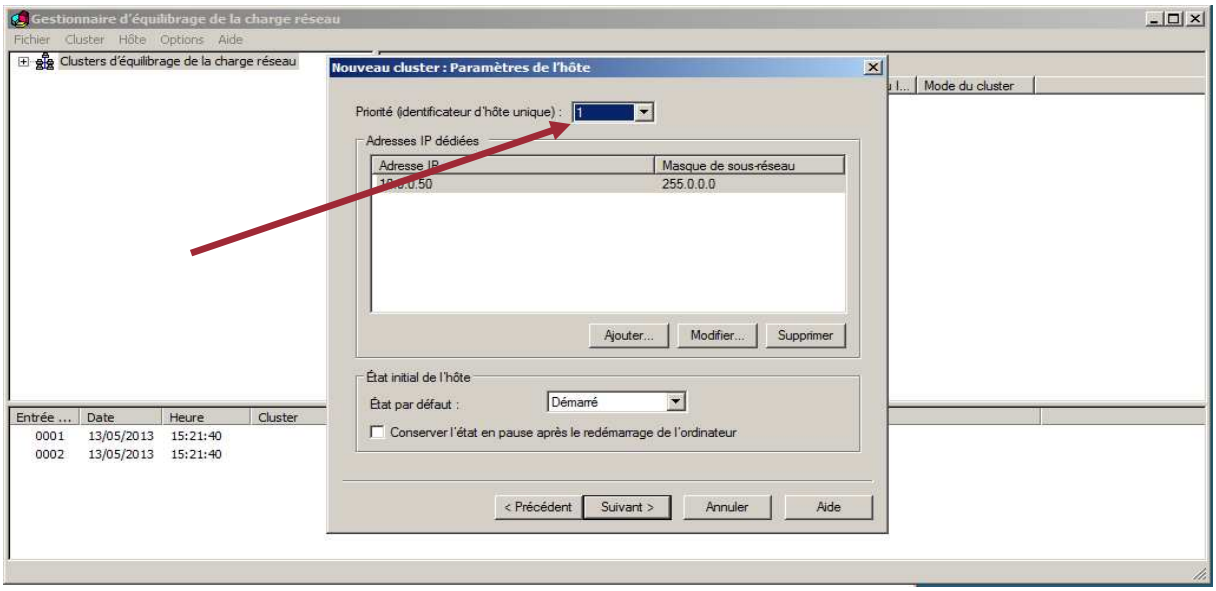
Création de nouveau cluster



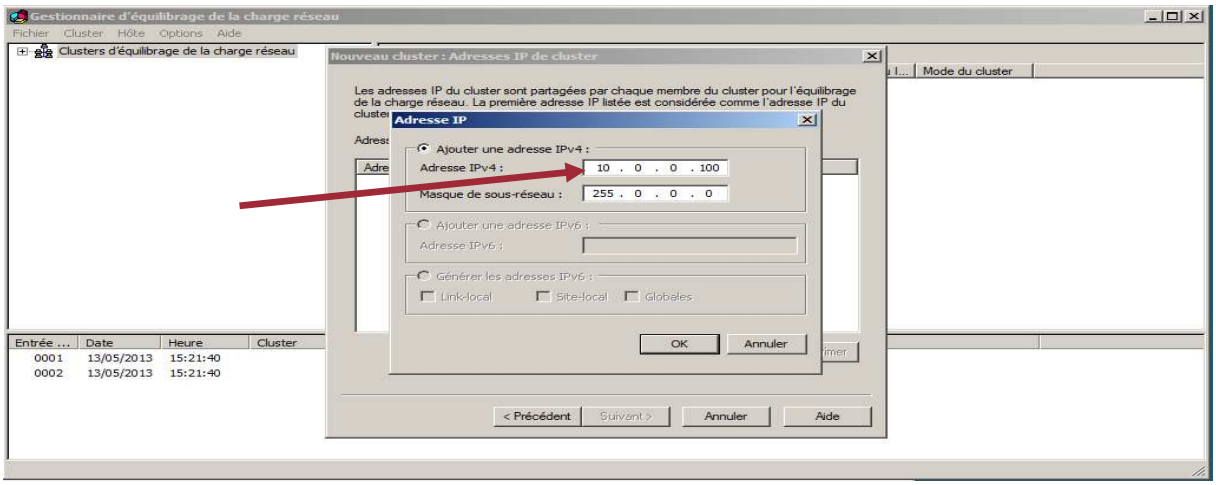
On se connecte à l'hôte adc



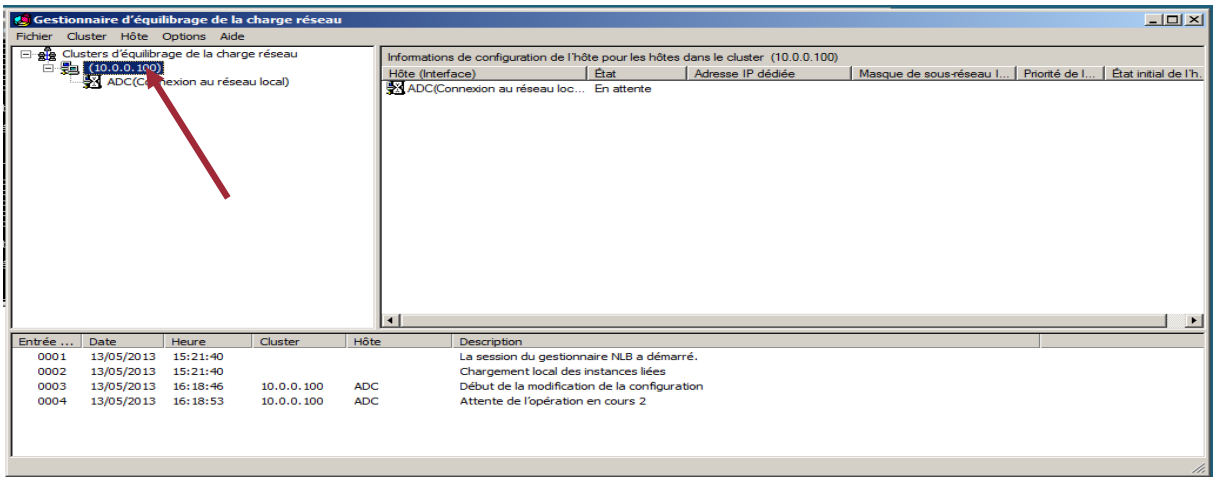
On sélectionne la priorité on donne 1 dans notre cas



On attribut l'adresse 10.0.0.100 pour notre cluster

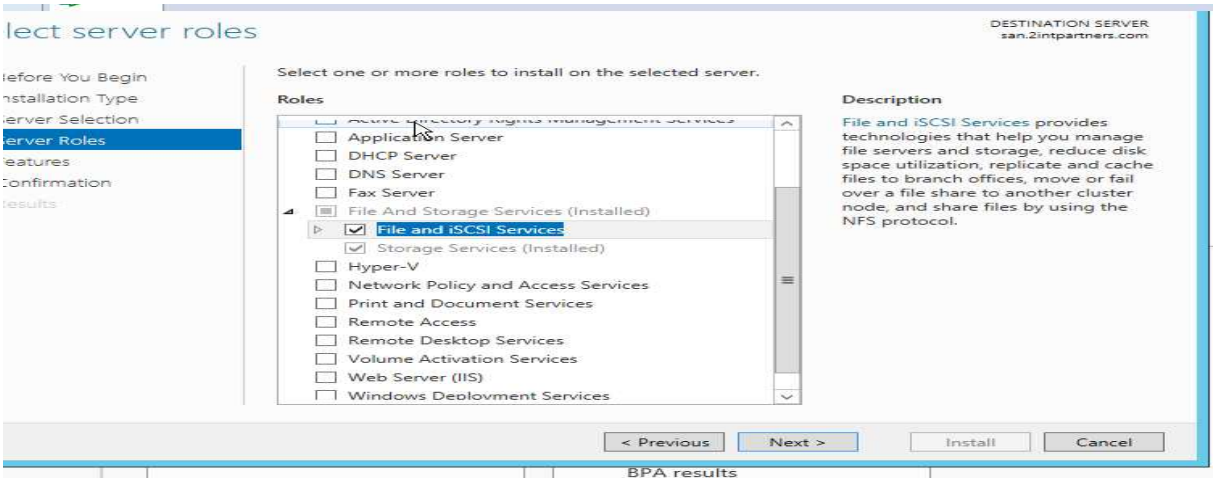


On finit par avoir la configuration suivante :

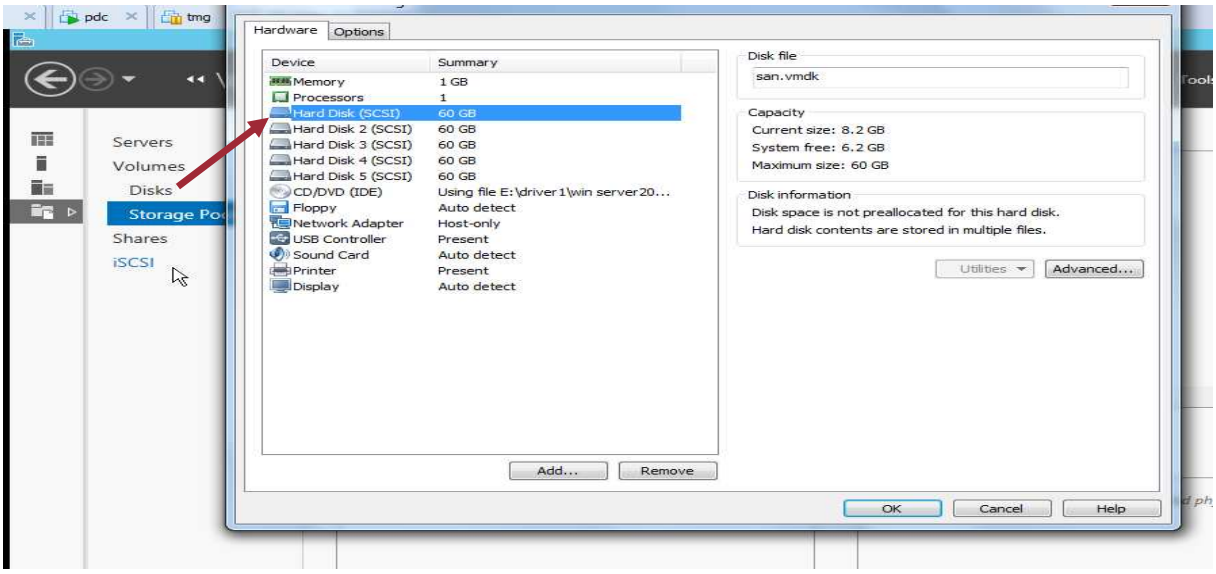


III.17 La technologie SAN

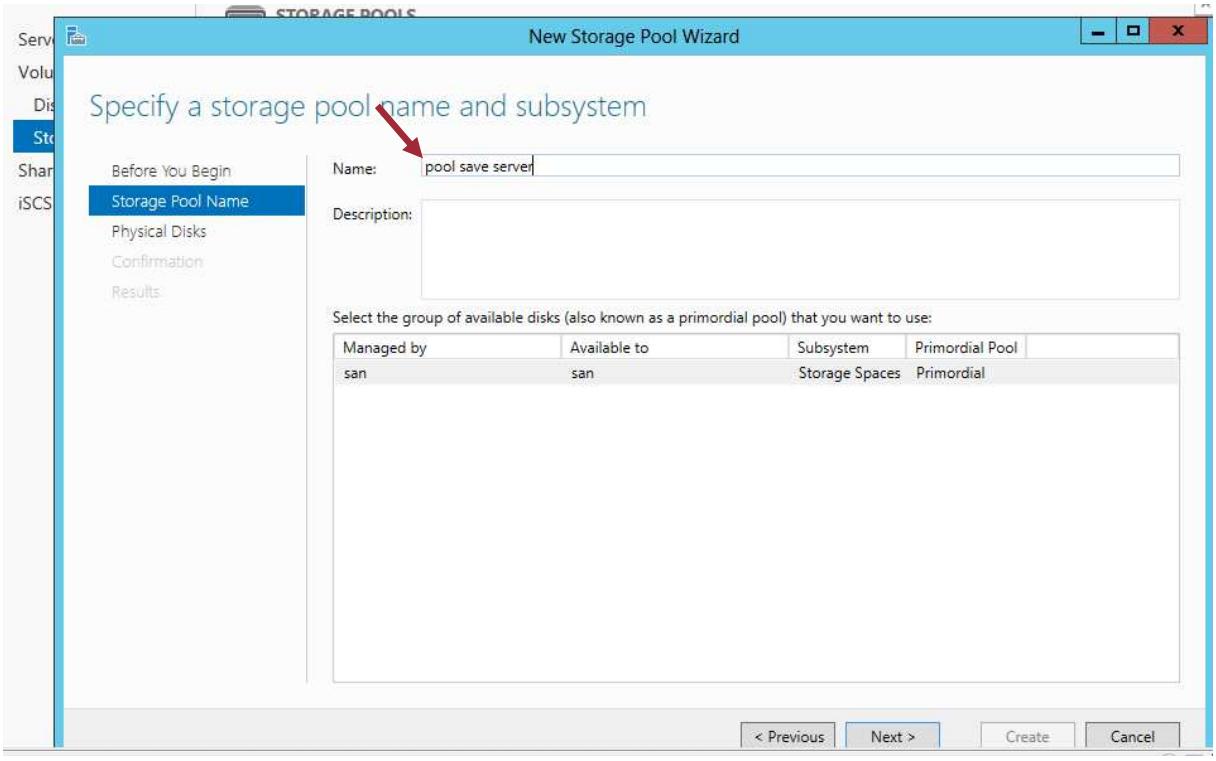
Installation de rôle Windows Server 2012



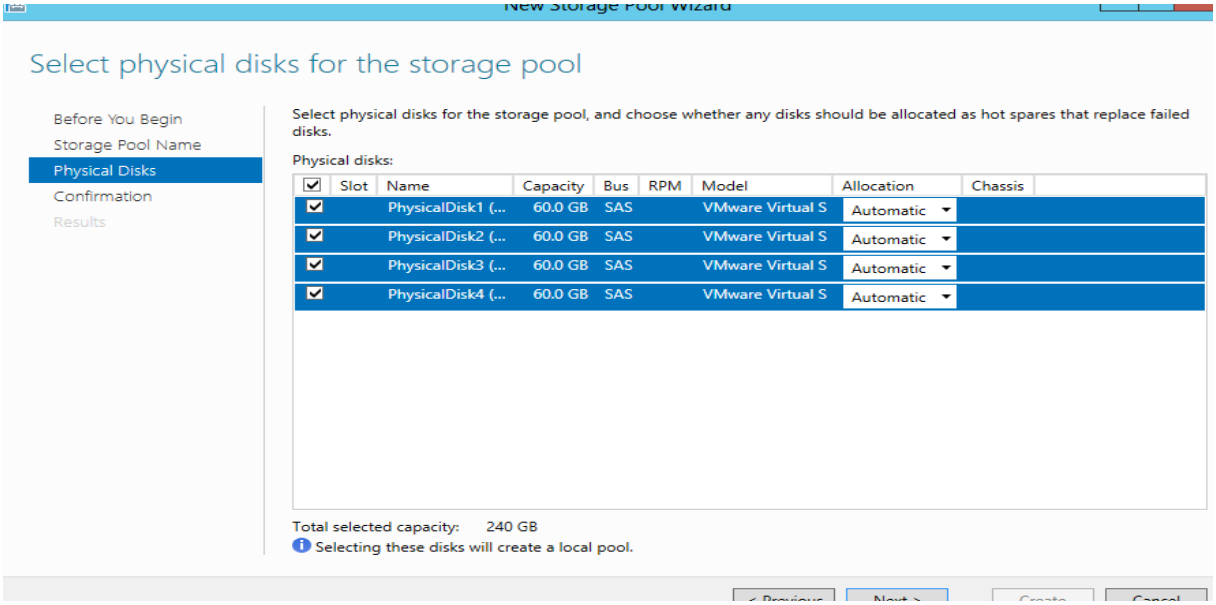
Ajouter des disques physiques dans la configuration de la vmware



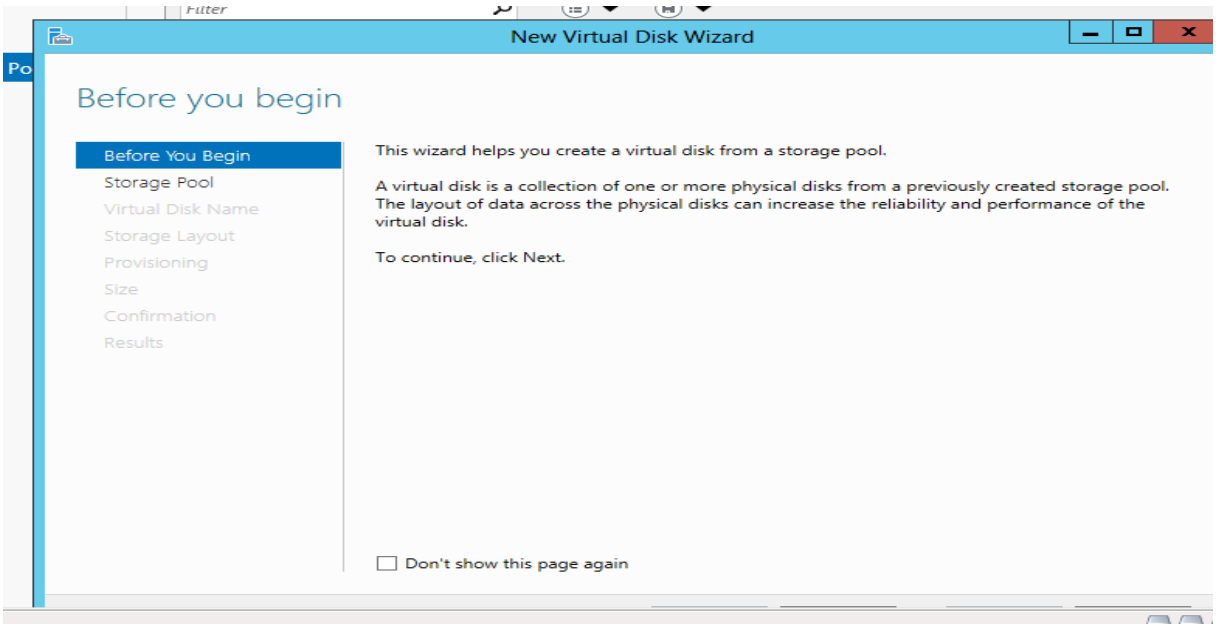
Création de pole de stockage



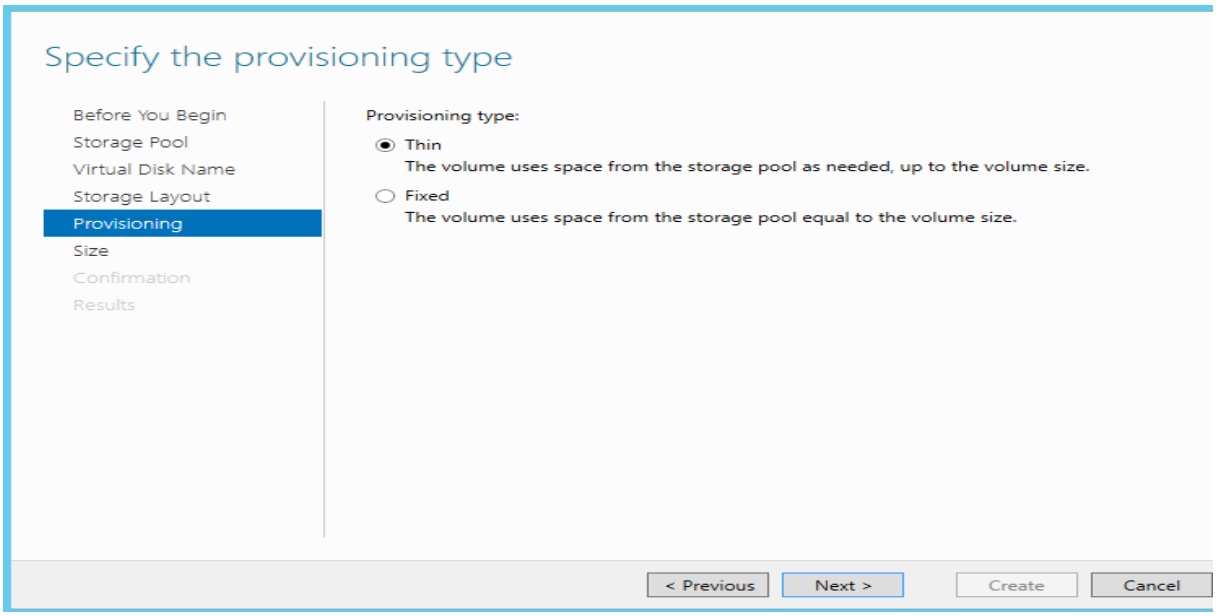
Sélectionner le nombre de disque pour le pool parmi les disques physique qu'on a ajouter dans la vmware précédemment



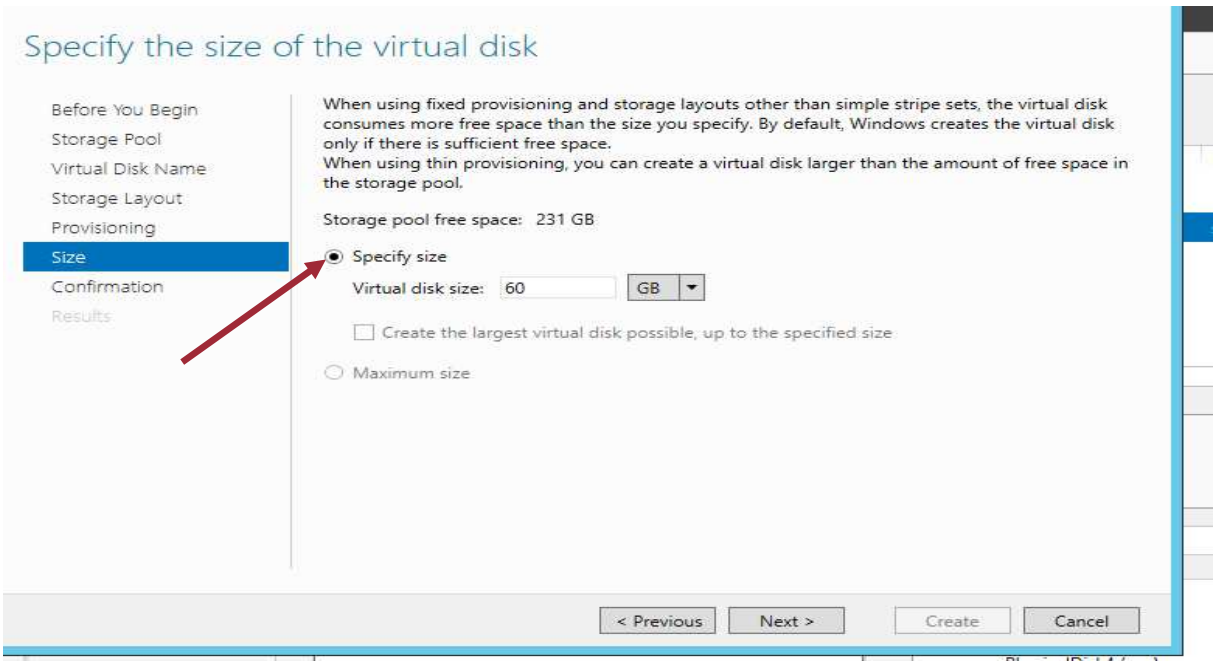
Création de nouveau disque virtuel dans le pool créer "pool save server"



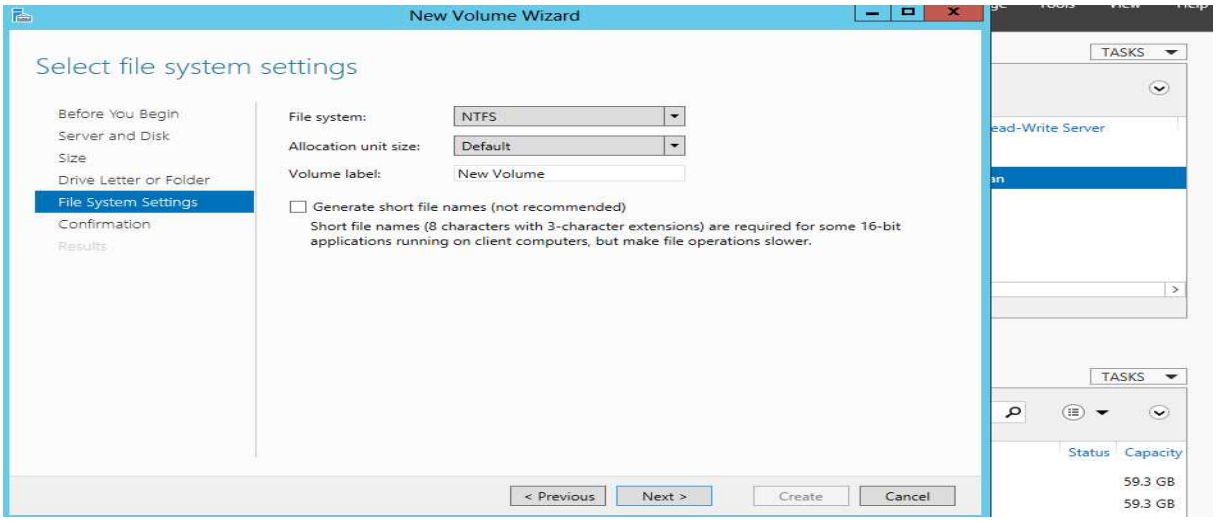
Choisir le type de disque (Dynamique ou statique)



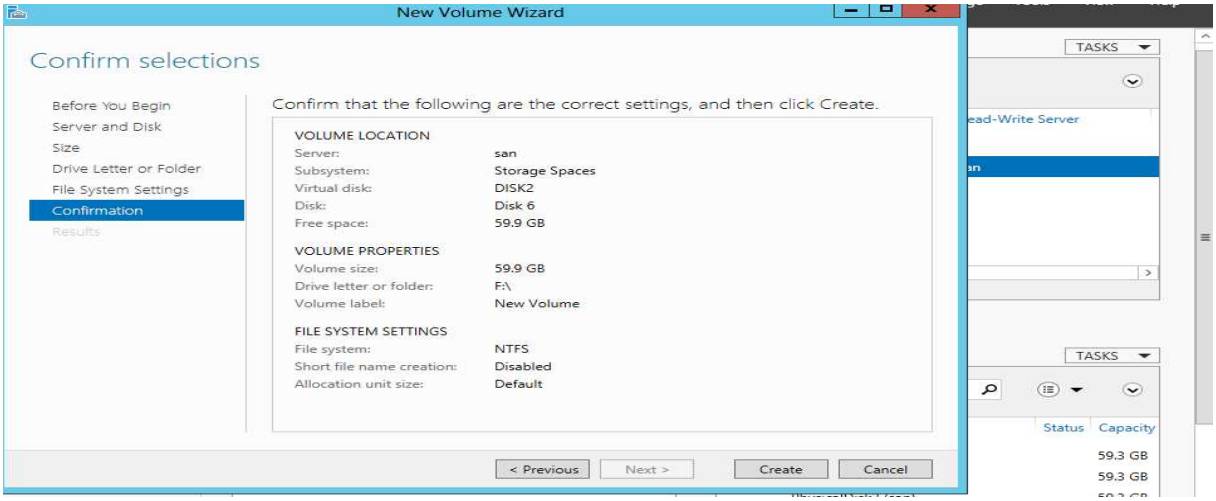
Choisir la taille de disque virtuel (60GB dans notre cas)



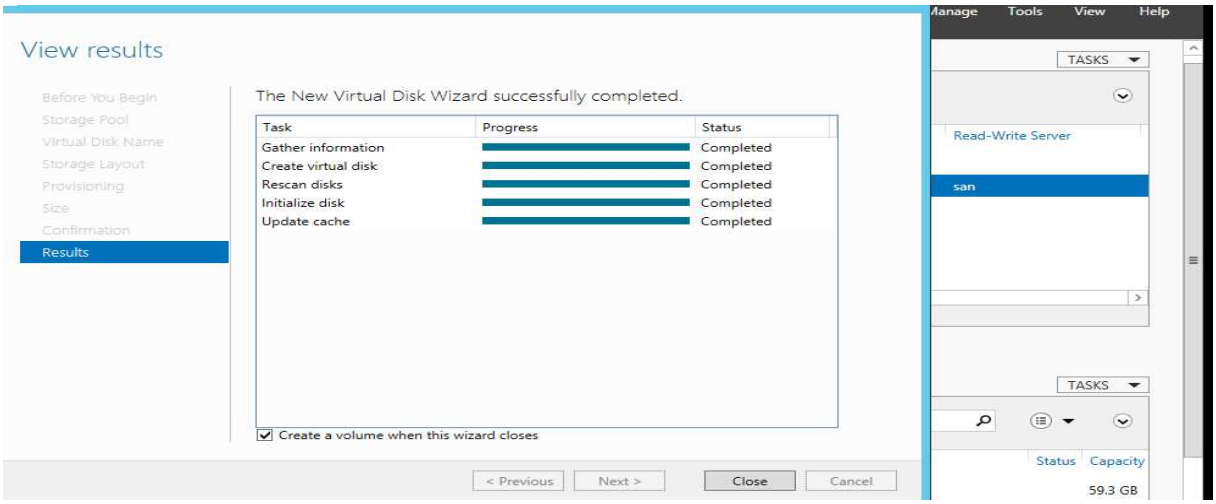
Type de fichier système



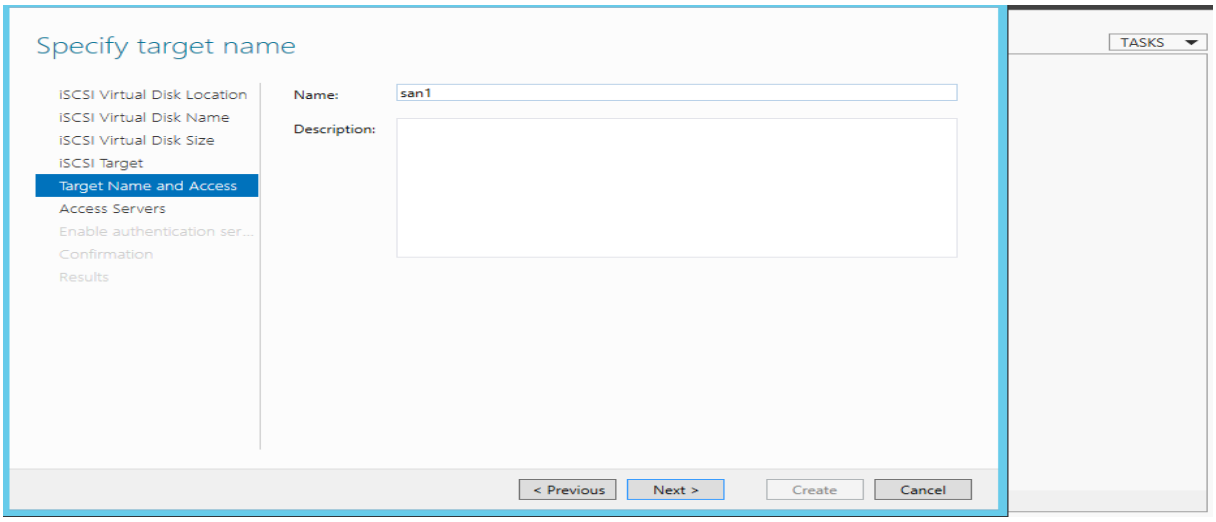
Attribuer la lettre F pour le disque virtuel et on clique sur create pour confirmer



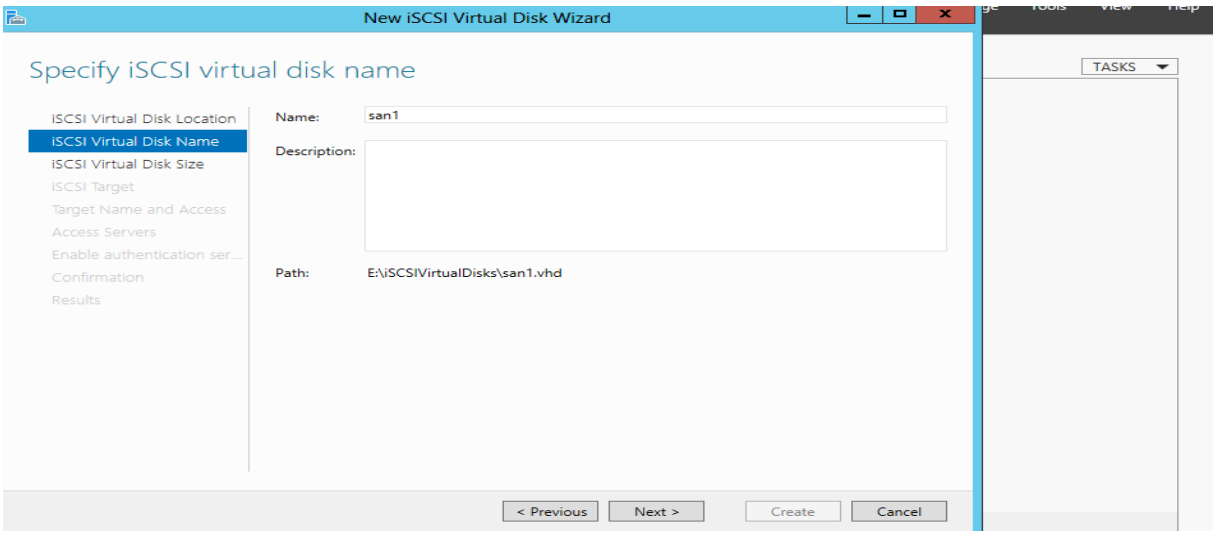
Fin de création de disque virtuel



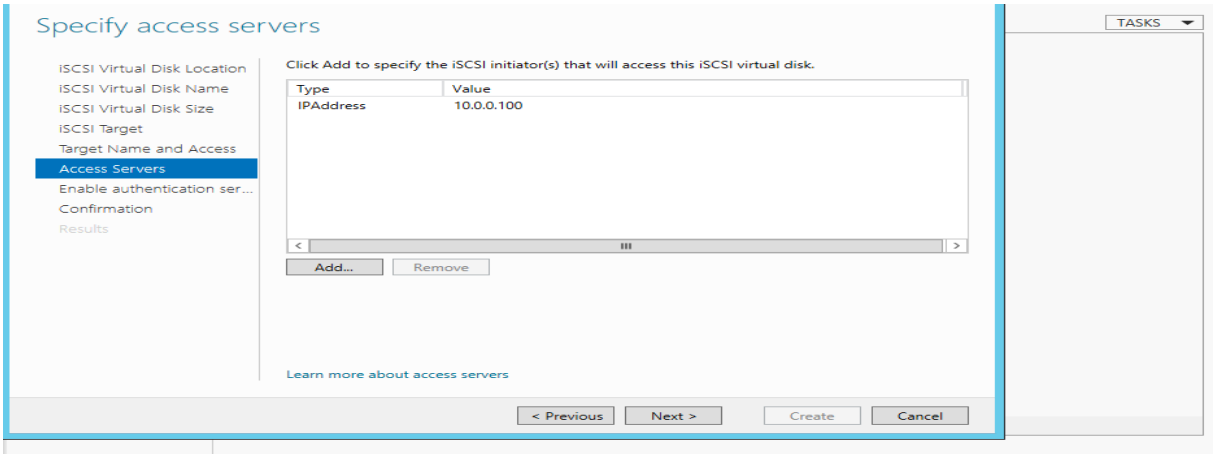
Donner un nom d'accès san1 pour la machine a qui attribué le disque virtuel



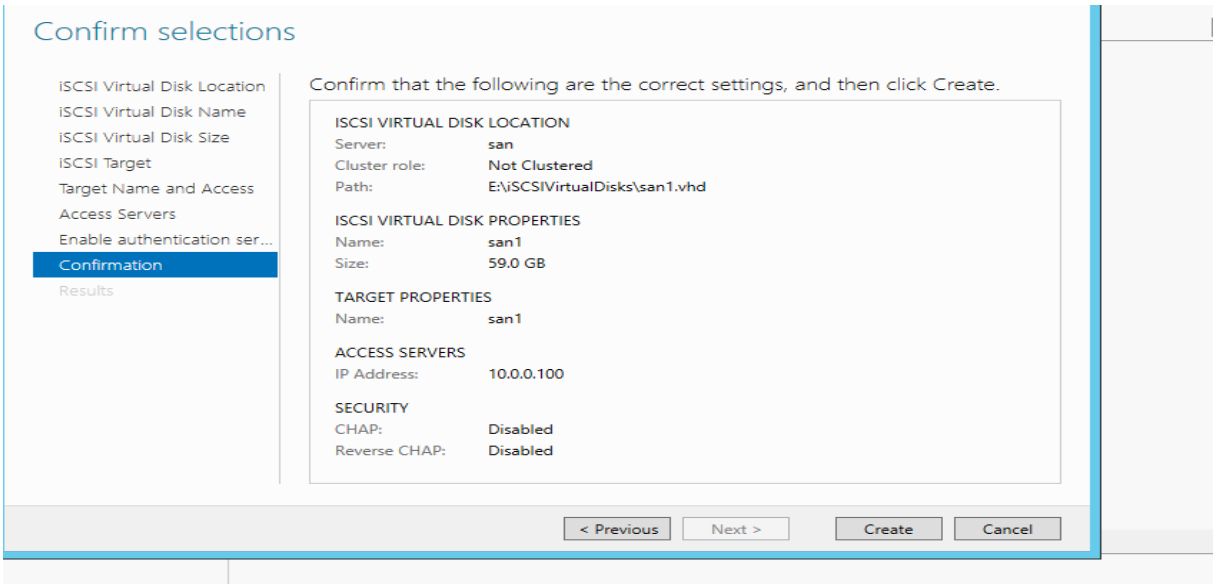
Création de nouveau disque iSCSI



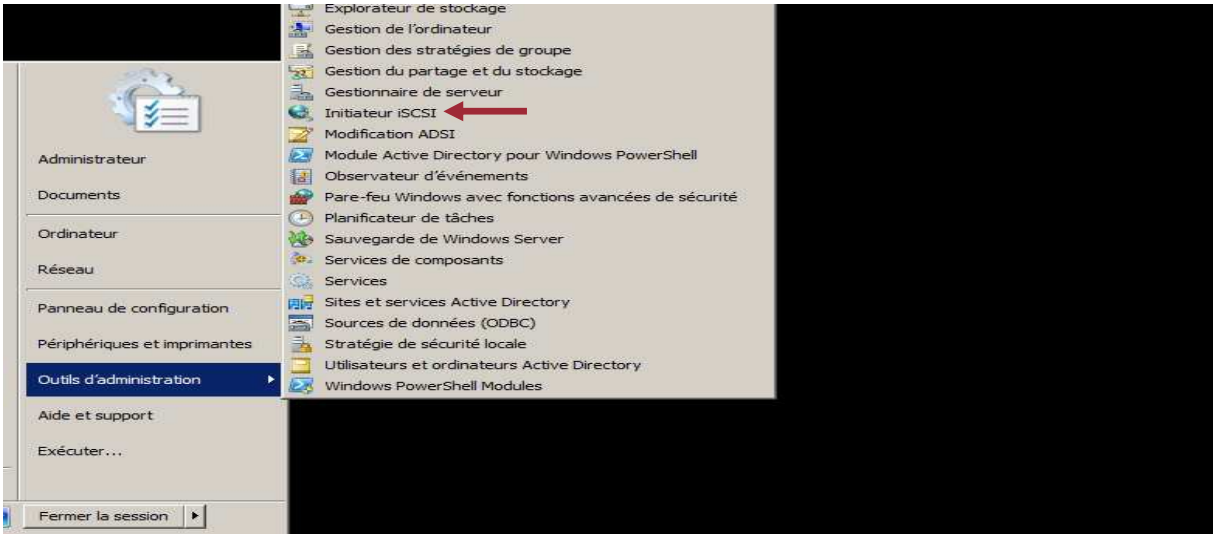
Associer l'adresse du pdc **(Principal Domain Controller)**



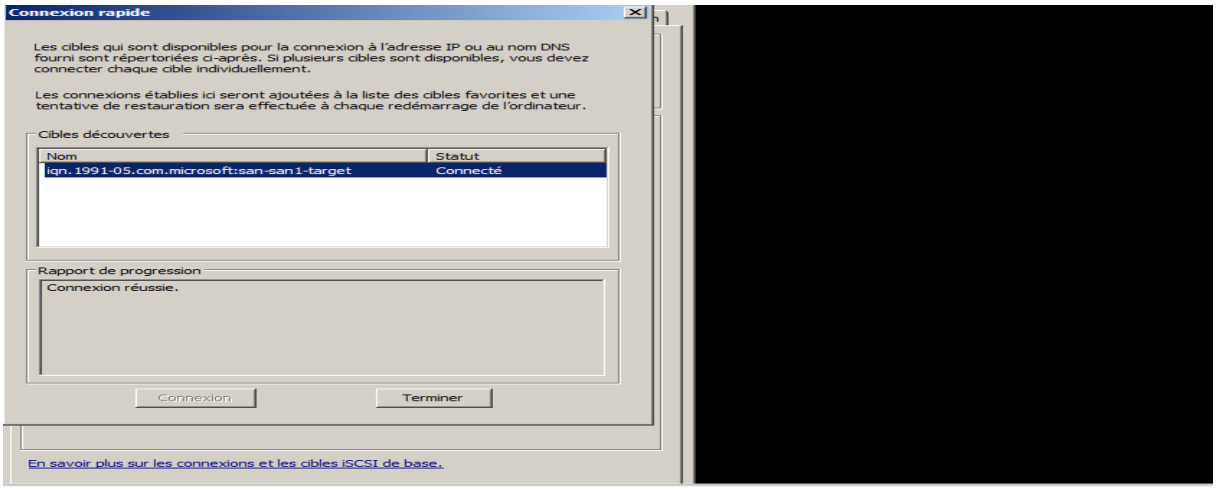
Confirmer la sélection pour la création du iSCSI



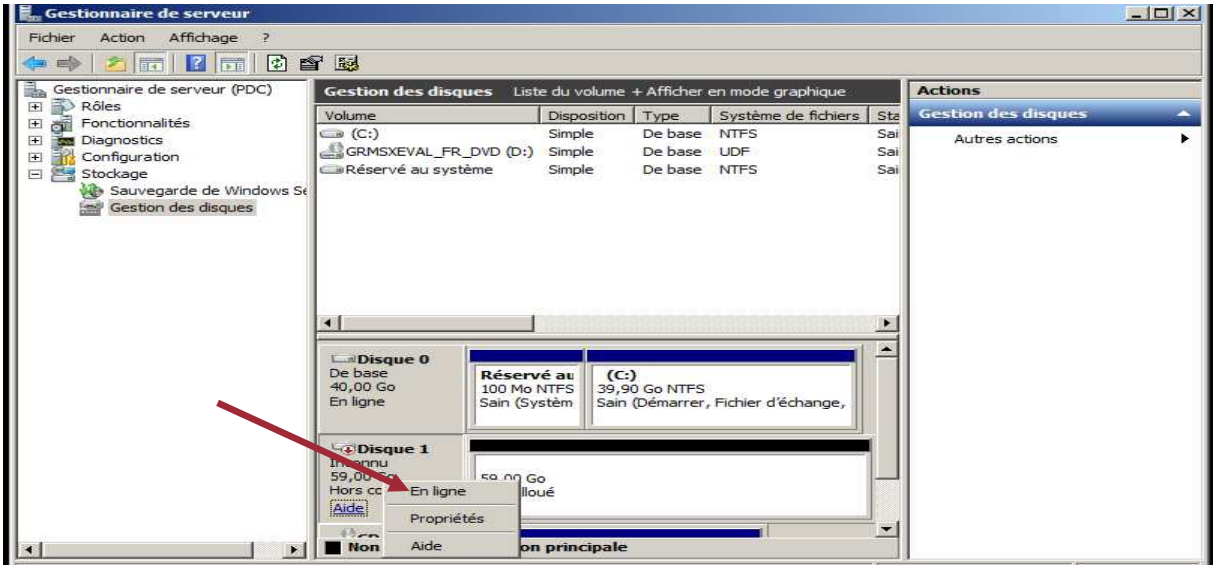
Dans le pdc , sélectionner initiateur iSCSI



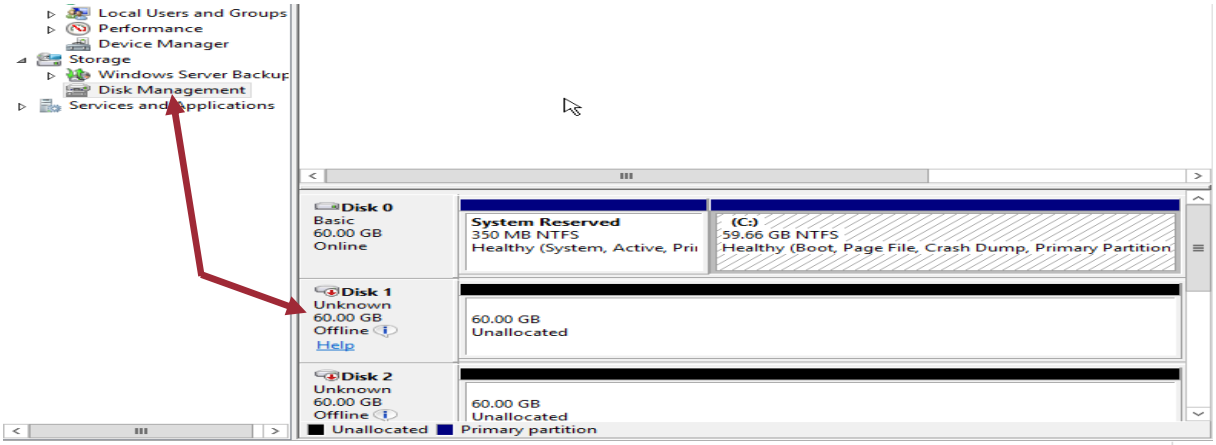
Connexion avec le disque physique du SAN



Dans le **Gestionnaire de serveur, Gestion des disques,** on met en ligne le **disque1**

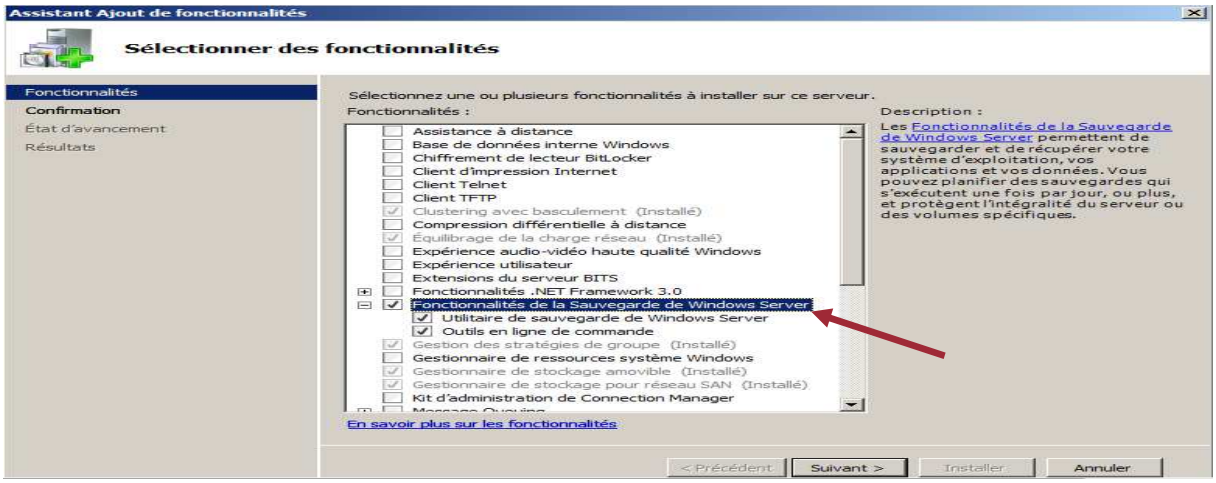


On fait la même chose avec le autres disques

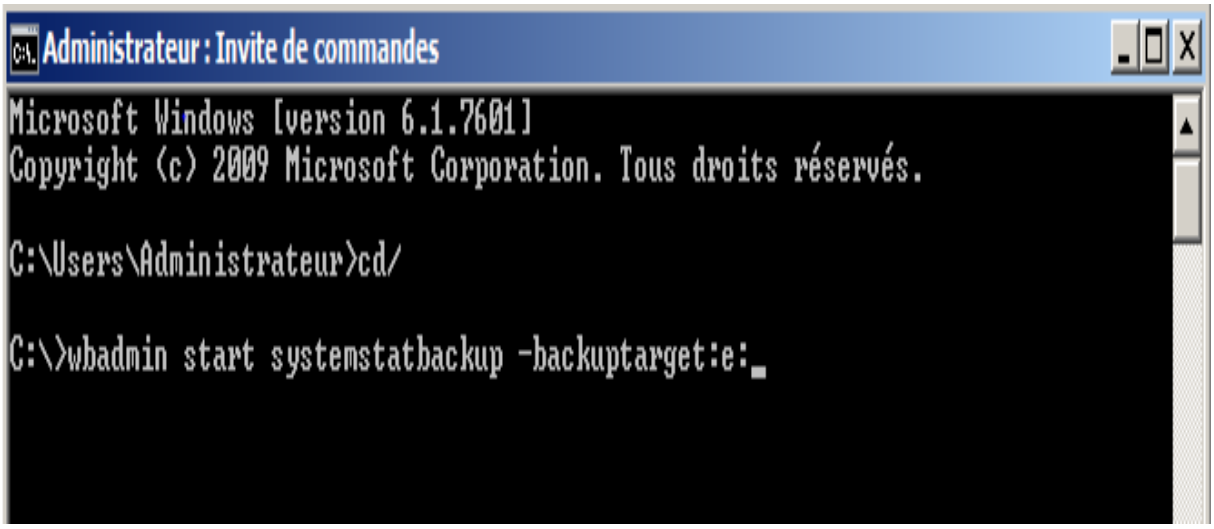


III.18 Backup

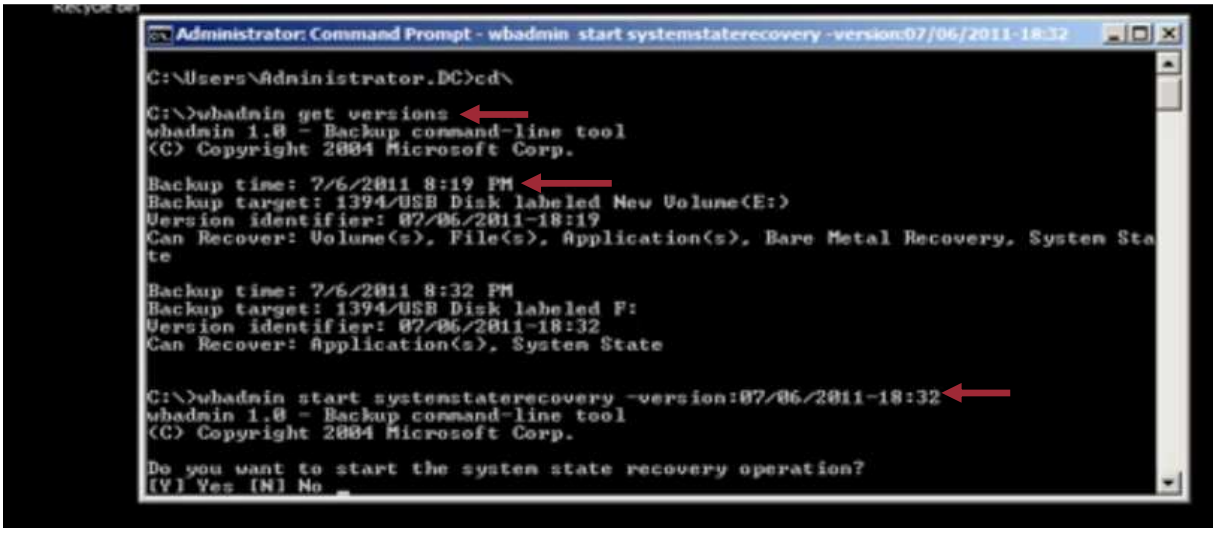
Installation de la fonctionnalité de sauvegarde de Windows Server



Dans l'invite de commande on tape la commande suivante pour lancer le backup



Cas de récupération de la sauvegarde



III.19 Discussions

Dans les grandes entreprises se limiter à un seul produit de sécurité n'est jamais suffisant. C'est pour cela qu'on a mis plusieurs pare-feu, ajouter au déploiement d'un antivirus et aux sauvegardes quotidienne ainsi qu'assuré les mise à jours de tous systèmes de l'entreprise s'avère très importantes.

La sécurité doit évoluer dans le temps, en s'adaptant aux changements technologiques, aux nouvelles exigences du métier de l'entreprise, ainsi qu'aux changements quotidiens, financiers, humains ainsi que techniques.

Conclusion

Conclusion

Au terme de travail, nous souhaitons rappeler, brièvement, les conclusions auxquelles nous avons abouti, et mentionner un certain nombre de questions ouvertes et de pistes de réflexion.

La question qui s'est trouvée à l'origine de nos investigations était celle de l'implémentation d'une politique de sécurité pour une infrastructure réseau d'entreprise,
Pour ce faire ,nous avons cherché, dans le premier chapitre, à montrer la plupart des vulnérabilités qui pèsent sur l'entreprise et quelques définitions sur la façon dont les pirates peuvent exploiter ces dernières(failles).

Après avoir bien étudié les problèmes détectés, nous avons pu définir un ensemble de solutions répondant aux critiques précédentes et les mettre en œuvre afin d'assurer pour l'entreprise une meilleure sécurité à l'avenir.

Ce projet m'a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il ma initié au monde de la recherche sur les réseaux surtout en ce qui concerne la sécurité. Il m'a également permis de découvrir les nouvelles technologies de Microsoft et Cisco ainsi que le Hacking.

Dans les grandes entreprises, se limiter à un seul produit de sécurité n'est jamais suffisant. C'est pour cela qu'on a établi plusieurs solutions telles que: les pare-feux, les certificats, ajoutés au déploiement d'un antivirus et aux sauvegardes quotidiennes et qu'on a assuré les mise à jours des systèmes ce qui s'avère très importantes.

Néanmoins, la sécurité absolu n'existe pas essentiellement parce que nous sommes à la merci de la conjoncture. Le temps qui passe apporte le changement et en matière de sécurité , le changement se traduit souvent par l'apparition ou la découverte de nouvelles sources de risques, ce qui nous amène à rester toujours dans le domaine de la recherche dans le but de comprendre et de maîtriser les nouvelles technologies afin de prendre de l'avance sur les hackers et prédire les risque possibles.

Conclusion

D'autre améliorations peuvent être implémenter comme la réplication DFS (Distributed File System) et le failover pour la tolérance aux pannes et assurer la disponibilité des services dans l'entreprise.

En conclusion, je suis très satisfaite de ce stage qui a ajouté une dimension professionnelle ainsi qu'un apport personnel crucial pour ma poursuite d'étude et mon avenir professionnel.

ANNEXE

RAID

En informatique, le terme de RAID (Redundant Array of Independent/Inexpensive Disks, c'est-à-dire un groupe de disques redondants et indépendants/bon marché) désigne une architecture matérielle (et parfois logicielle) permettant d'accélérer, de sécuriser et/ou de fiabiliser les accès aux données stockées sur disques durs. Cette architecture est basée sur la multiplication des disques durs, par opposition à la méthode sled (Single Large Expensive Disk) où toutes les données sont rassemblées sur un seul disque de prix élevé.

La première description de cette architecture apparut dans une publication de 1987 intitulée A Case of Redundant Arrays of Inexpensive Disks (RAID) (Patterson, Gibson & Katz - Universitéde Californie - Berkeley). Cet article comparait le RAID au sled et proposait cinq niveaux différents de RAID, chacun d'eux ayant ses avantages et ses inconvénients.

SCSI

SCSI, Small computer System Interface en anglais, est un standard définissant un bus informatique permettant de relier un ordinateur à des périphériques ou bien même à un autre ordinateur. Le standard décrit les spécifications mécaniques, électriques et fonctionnelles du bus.

Backup

(Sauvegarde) Enregistrement de fichiers sur un support autre que le disque dur (disquette, CD...). Le backup permet de récupérer vos données sauvegardées en cas d'erreur sur votre disque dur.

Appliance

Se dit de toutes sortes de machines dont la principale caractéristique est de pouvoir être (théoriquement) simplement branchées pour fonctionner immédiatement de manière parfaitement opérationnelle. C'est souvent un dispositif (pare-feu ou IDS par exemple) contenu dans une boîte (souvent noire).

DDoS

Distributed Denial of service ou déni de service distribué.

DoS

Denial of Service. Déni de service. C’est une attaque destinée à paralyser ou ralentir un service (FTP, STMP etc) empêchant les utilisateurs autorisés à l’exploiter normalement. Il peut conduire à l’arrêt complet du serveur.

Service web

A l'ère du village planétaire, la technologie des services web est aujourd'hui de plus en plus incontournable et se présente comme le nouveau paradigme des architectures logicielles. C'est une technologie qui permet à des applications de communiquer à travers le réseau Internet, indépendamment des plates-formes d'exécution et des langages de programmation utilisés. Dans les entreprises, l'accès aux serveurs web externes (Internet) fait très souvent l'objet d'une décision de la direction et non de l'administrateur réseau à fin d'attribuer des autorisations aux utilisateurs. Dans ce cas on peut implémente un proxy pour réglementer l'accès à Internet et la sécurité. Pour un déploiement d'un serveur web en interne (Intranet) au sein d'une organisation, le serveur doit héberger les informations internes, être placé dans un sous réseau et non accessible depuis l'extérieur. Contrairement à un serveur web externe (Extranet), les informations sont hébergées dans un sous-réseau public et accessible par tout internaute.

BIBLIOGRAPHIE

Bibliographie

[1] MCTS 70-642 Configuration d'une infrastructure réseau avec Windows Server 2008, Tony NORTHRUP, J.C Mackin; 2008

[2] MCTS 70-643 Configuration d'une infrastructure d'applications avec Windows Server 2008; J.C Mackin, Anil Desai ; août 2008

[3] MCTS 70-646 Administrateur d'entreprise sur Windows Server 2008;Orin THOMAS, John POLICELLI, lan McLean, J.C.MACKIN, Paul MANCUSO, DAVID R.MILLER et GranMaster, 2008

[4] MESSAVUSSU Adotevi Enyonam et MOUMOUNI MOUSSA Harouna "Les stratégies de sécurité et système de protection contre les intrusions," ***Paris Graduate School of Management***
ECOLE SUPERIEURE DE GENIE INFORMATIQUE, Décembre 2008

[5] Mise en Oeuvre d'une infrastructure réseau sécurisée par ISA Server, M^{elle} YADDADENE Farida et TOUMI Nedjma,UMMTO,2012

[6] Cisco ASA 5500 Series Configuration Guide using ASDM, Software Version 6.3

[7] Microsoft Threat Management Gateway (TMG),Jim Harrison,Yuri Diogenenes et Mohit Saxena, Dr. Tom Shinder

[8] CompTIA Security + Deluxe, Emmett Dulaney,2009

[9] http://technet.microsoft.com/fr-fr/library/cc732863%28v=ws.10%29.aspx

[10] http://www.labo-microsoft.org/articles/NPS_Configuration/

[11] http://www.memoireonline.com/12/09/3035/m_Audit-et-definition-de-la-politique-de-securite-du-reseau-informatique-de-la-fi20.html

[12] http://www.cisco.com/en/US/docs/security/asa/asa83/asdm63/configuration_guide/start.html#wp1152007

[13] http://www.cisco.com/en/US/docs/security/asa/asa83/asdm63/configuration_guide/vpn_gen.html#wp1106725

[14] http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00808c9a87.shtml

[15] http://www.inetdoc.net/guides/tutoriel-secu/tutoriel.securite.dissimulation.trojan.html

[16] http://www.funinformatique.com/les-outils-du-hacker/

GLOSSAIRE

Glossaire

A

AES **Authentification Encryption System**

ACL Access Control List

ARP Address Resolution Protocol

ASA Adaptative Security Appliance

E

EFS Encrypting File System

D

DES Data Encryption Standard

DFS Replication Distributed File System

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

DNS Domain Name System

DOS Deny Of Service

DDOS Distributed Deny Of Service

F

FTP File Transport Protocol

H

HTTP Hyper Text Transfert Protocol

HTTP-S Hyper Text Transfert Protocol Secure

HIDS Host Based Intrusion Detection System

I

ICMP Internet Control Message Protocol

IGC Infrastructure de Gestion de Clés

IP Internet Protocol

IPsec Internet Protocol Secure

iSCSI Internet Small Computer System Interface

G

GPL General Public Licence

GPO Group Policies Object

L

LAN Local Area Network

Glossaire

LDAP Light weight Distributed Data Interface

M

MAC Media Access Control

MITM Man in the middle

N

NAP Network Access Protection

NTFS New Technology File System

NIDS Network Based Intrusion Detection System

NPS Network Policy server

P

PKI Public Key Infrastructure

POP Post Office Protocol

POP3 Post Office Protocol version 3

R

RADIUS Remote Authentification Dial In User Service

RARP Reverse Address Resolution Protocol

S

SAN Storage Area Network

SHA Secure hash algorithm

SMTP Simple Mail Transfer Protocol

SSH Secure Shell

SSL Secure Socket Layer

SYN Synchronous Idle

T

TCP Transfer Control Protocol

TMG Threat Management Gateway

V

VPN Les réseaux privés virtuels

W

WSUS Windows Server Update Service