République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Mouloud MAMMERI de TIZI-OUZOU

Faculté de Génie Electrique et d'Informatique

Département d'Informatique

Mémoire de fin d'études

En vue de l'obtention du diplôme de master II en Informatique

Option : Réseau, Mobilité et Systèmes Embarqués

Thème :

Implémentation d'une politique de sécurité par chiffrement avec les certificats dans une entreprise

Proposé et dirigé par :

Mr: A. DIB

Réalisé par :

M^{lle}: SI SALEM Zahia

M^{lle}: TALHI Dalila

Promotion: 2013/2014

Remerciements

Nous tenons à exprimer notre profonde gratitude à notre promoteur MR A.DIB pour son suivis et ses conseils tout au long de l'élaboration de notre mémoire.

Notre parfaite considération à l'ensemble des enseignants qui ont contribué à notre formation.

Nos sincères salutations aux membres du jury qui nous font l'honneur d'examiner et de juger notre travail.

Enfin, nous tenons à remercier toutes les personnes qui ont contribué de prés ou de loin à la réalisation de ce modeste travail.

Dédicaces

Mes chers parents, a toi ma mère a toi mon père que j'aime beaucoup je dédie ce travail qui est le fruit de vos soutien et vos encouragement .

A mes chers frères et sœurs que dieu vous protège, mes tantes, oncles et mes deux grandes mères pour leurs amour et gentillesse.

A tout mes amis a ma binôme Dalila.

A tout la famille du près ou du loin.
A toute la promotion RMSE 2013/2014.

Zahia

Dédicaces

Je dédie ce modeste travail à mes très chers parents, mes chers frères, ma belle sœur, à mes tantes et oncles pour leurs soutient pendant toute la durée de mes études.

A mon petit(e) qui va arriver dans 6 mois.

A mes amis Tourkia,Souhila,Fairouz et Arezki sans oublier ma binôme Zahia .

A tout la famille du près ou du loin.

A toute la promotion RMSE 2013/2014.

Dalila

Table des matières

Chapitre I

Table des matières

Table des matières

Chapitre III

Liste des figures

Liste des tableaux

Introduction général

Introduction générale

L’évolution rapide des réseaux informatiques, privés ou publics engendre un volume toujours plus important de données sauvegardées et transmises, générant ainsi de nouveaux besoins en matière de sécurité. Dans un mode où l’entreprise dépend de plus en plus de son système informatique, la sécurité est donc devenue une préoccupation primordiale.

L’apparition de l’informatique et des télécommunications a contribué à une complexité accrue des problèmes et des solutions de sécurité en amenant des notions telles que virus informatiques, accès non autorisé aux données, fausses informations, etc. Mais avec ces nouveaux moyens de communication est arrivée la nécessité de protéger le contenu de certains messages des inévitables curieux. Dans ce contexte la cryptographie est l’un des mécanismes de sécurité de la transmission d’information, elle consiste à transformer un message clair en un message indéchiffrable pour tous, sauf les destinataires du message. On utilise pour cela un algorithme cryptographique et une ou plusieurs clés, secrètes ou publiques. L’émetteur crypte son message à l'aide d'un algorithme, le transmet crypté, et le récepteur peut alors le décrypter à l'aide d'une même clé.

La cryptologie a longtemps été confinée au domaine militaire. Avec l'explosion de l'informatique, l'usage des moyens cryptographiques s'est progressivement démocratisé. Leurs contextes d'emploi se sont diversifiés : téléphonie, transactions bancaires, protection de données stockées... La confidentialité des messages n'est plus le seul objectif de la cryptographie. On souhaite notamment garantir l'intégrité d'une donnée, ou encore l'authenticité de son origine. Les mécanismes permettant d'atteindre ces objectifs sont différents. De la même manière ce n'est plus seulement la protection d'une communication qu'on cherche à assurer mais également la protection du stockage. Les problématiques peuvent être sensiblement différentes.

La démarche sécuritaire suivie consiste à mettre en place une politique de sécurité fiable. Pour y parvenir, nous étudierons en premier lieu, les différentes notions de la sécurité informatique. En second lieu, nous nous pencherons sur les notions de la cryptographie. A la fin on termine par proposer la politique de sécurité pour une entreprise quelconque.

Chapitre I : Notion générales sur la sécurité

Introduction

L'Internet est au cœur des questions de sécurité informatique, nous rappellerons brièvement ses principes de fonctionnement, placés sous un éclairage qui fera apparaître les risques qui en découlent. Pas de sûreté de fonctionnement sans un bon système d'exploitation nous passerons en revue les qualités que nous sommes en droit d'en attendre. Nous examinerons les différentes formes de malfaisance informatique, sans oublier les aspects organisationnels et sociaux de la sécurité.

Les menaces contre le système d'information entrent dans une des catégories suivantes atteinte à la disponibilité des systèmes et des données, destruction de données, corruption ou falsification de données, vol ou espionnage de données, usage illicite d'un système ou d'un réseau, usage d'un système compromis pour attaquer d'autres cibles.

La protection des systèmes d'information repose aujourd'hui sur la cryptographie, nous donnerons un exposé aussi simple que possible des principes de cette science.

I.1 Généralités sur les réseaux

I.1.1 Définition

Un réseau (Network) est un ensemble d'ordinateurs et périphériques interconnectés. Il permet de faire circuler des données informatiques et ainsi d'échanger du texte, des images, de la vidéo ou du son entre chaque équipement selon des règles et protocoles bien définis.

I.1. 2 Classification des réseaux [1]

On peut classifier les réseaux selon la distance qui sépare les ordinateurs en trois catégories :

- LAN (local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

I.1.2.1 LAN

LAN signifie *Local Area Network* (en français *Réseau Local*). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

I.1.2.2 MAN

Les MAN (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kms) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

I.1.2.3 WAN

Un WAN (*Wide Area Network ou réseau étendu*) interconnecte plusieurs LAN à travers de grandes distances géographiques. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

I.1.3 Fonctionnement d'un réseau

Pour assurer le bon fonctionnement d'un réseau, il faut réunir les supports physiques nécessaires et prévoir une bonne architecture logicielle et une normalisation de celle-ci s'impose. Deux familles d'architectures ont vu le jour : La première s'appelle ***le Modèle OSI***. La seconde est ***l'architecture TCP/IP***. Détaillons chacune d'elles :

I.2.3.1 Le Modèle OSI (Open System Interconnexion)

Ce modèle est une norme définie par *ISO* (International Standarlization Organisation). Fondé sur un principe énoncé par *JULES CESAR* « Diviser pour mieux régner».Ce modèle est composé de sept couches (elles seront détaillées ultérieurement) : ***couche physique, liaison de données, réseau, session, transport, présentation et application.***

Ce modèle permet la communication entre plusieurs réseaux hétérogènes, cette communication passe donc par un ensemble de couches empilées :

Chaque couche a un rôle précis (conversion, routage, découpage, vérification etc.)

- Chaque couche dialogue avec la couche juste au dessus et celle juste au dessous : elle fournit des services à la couche dessus et utilise les servies de la couche dessous.
- Chaque couche encapsule les données venant de la couche dessus en y ajoutant ses propres informations avant de les passer à la couche dessous (opération inverse dans l'autre sens).
- Les données traversent les couches vers le bas quand elles sont envoyées et elles remontent les couches à la réception.

Voyons donc le rôle de chacune de ces couches :

1. Couche physique : C'est le support de transmission lui-même : un fil de suivre, une fibre optique etc.

2. Couche Liaison de données : En charge d'encodes (ou moduler) les données pour qu'elles soient transportables par le couche physique et fournit également la détection d'erreur de transmission et la synchronisation.

3. Couche réseau : En charge du transport, de l'adressage et du routage des paquets.

4. Couche Transport : En charge de la liaison d'un bout à l'autre. Cette couche s'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.

5. Couche Session : En charge d'établir et maintenir des sessions (c'est-à-dire débuter le dialogue entre machines, vérifier que l'autre machine est prête à communiquer, s'identifier, etc..).

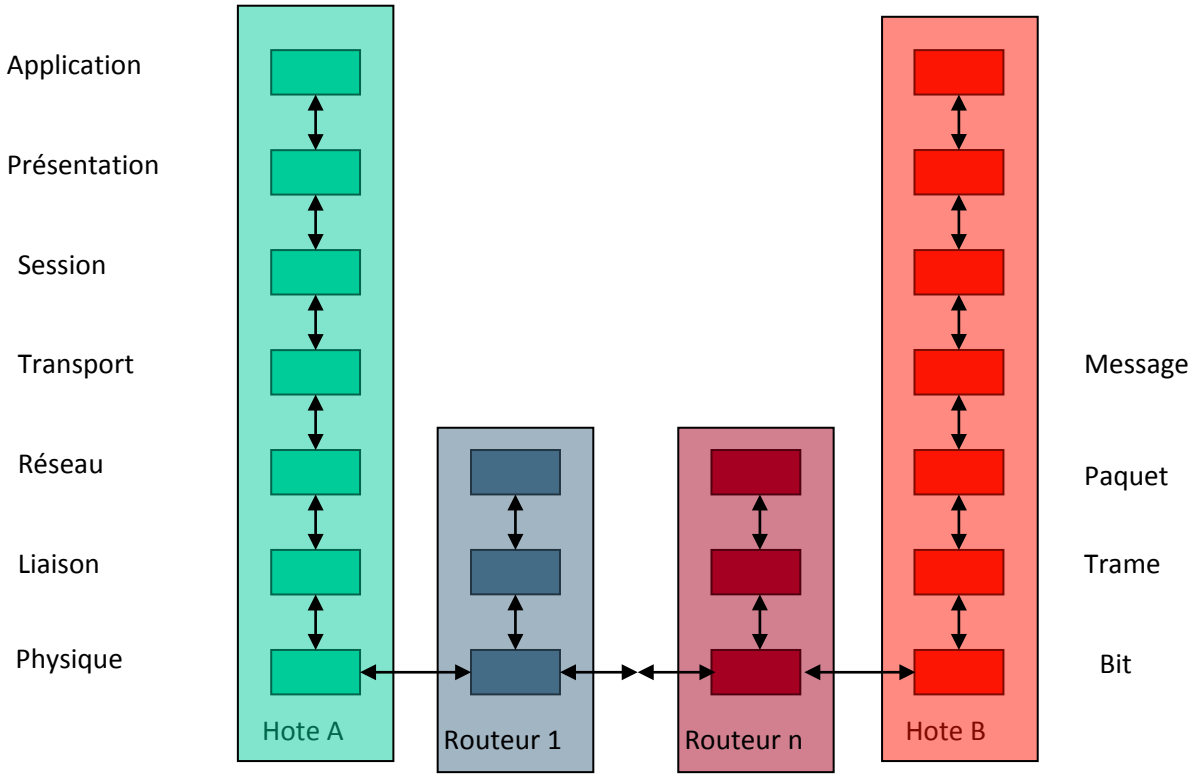


Figure I.1 : Modèle de référence OSI

6. Couche Présentation : En charge de la représentation des données (de telle sorte qu'elle soit indépendante de microprocesseur ou du système d'exploitation par exemple) et éventuellement du chiffrement.

7. Couche application : Représente la couche la plus élevée du modèle OSI, elle utilise les services de la couche présentation (indirectement des autres couches) pour exécuter une application

spécifique .l'application peut être un échange des courriers, transfert des fichiers ou toute autre application réseau.

Au niveau de chaque couche un ensemble de protocole est intégré. Un protocole réseau est un langage que vont utiliser toutes les machines d'un réseau pour communiquer entre eux. ***HTTP, FTP, TCP, IP, ICMP,*** et la totalité des autres protocoles entrent dans le modèle OSI.

I.1.3.2 Le Modèle TCP/IP [19]

Développé par l'armée américaine. Il désigne deux protocoles étroitement liés : un protocole de transport TCP (Transmission Control Protocol), et un protocole réseau IP (Internet Protocol).Le modèle TCP/IP est en fait une architecture réseau à quatre couches : ***couche hôte réseau, Internet, couche transport*** et ***application .***Détaillons chacune de ces couches :

1. Couche hôte réseau : Cette couche semble regrouper les couches : physique et liaison de données du modèle OSI. Elle permet à un hôte d'envoyer des paquets IP sur le réseau

2. Couche Internet : Cette couche est la clé de voute de l'architecture IP. Cette couche réalise l'interconnexion des réseaux (hétérogènes). Son rôle est de permettre l'injection des paquets dans n' importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination, les paquets peuvent arriver dans le désordre, le contrôle de l'ordre est la tâche des couches supérieures. L'implémentation officielle de cette couche est le protocole IP**.**

3. Couche transport : Son rôle est le même que celui de la couche transport du modèle OSI. Officiellement, cette couche n'a que deux implémentations : le protocole *TCP* et le protocole *UDP* (User Datagram Protocol)**.**

4. Couche application : Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles.

On s'est en effet aperçu avec l'usage que les logiciels réseaux n'utilisent que très rarement ces deux couches (Présentation et session), et finalement, le modèle OSI dépouillé de ces deux couches ressemble fortement au modèle TCP/IP.

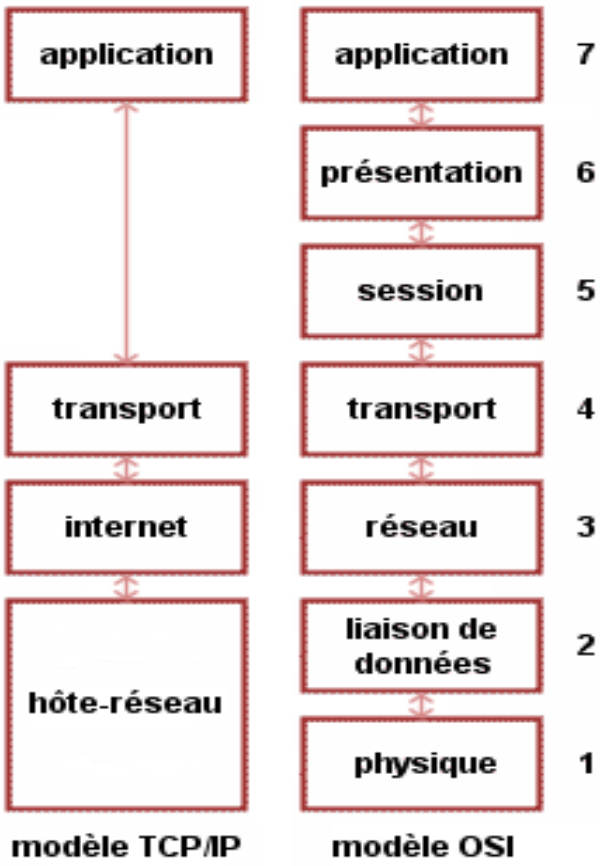


Figure I .2 : Modèle TCP et OSI

TCP/IP est le protocole utilisé dans le réseau Internet. L'implémentation de ce modèle engendre malheureusement des vulnérabilités dus au failles des langages de programmation utilisés dans l'implémentation (exp : langage C). Ces vulnérabilités peuvent être exportées par les attaquant pour réaliser leurs attaques, d'où le problème de la sécurité réseau.

I.4.La sécurité des réseaux

I.4.1.Définition [20]

En générale la sécurité informatique, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Néanmoins, les points principaux sont les suivants :

- ✓ empêcher la divulgation non-autorisée de données.
- ✓ empêcher la modification non-autorisée de données.
- ✓ empêcher l'utilisation non-autorisée de ressources réseaux ou informatiques de façon générale.

I.4.2. Terminologie de la sécurité informatique [2]

- **Intrus :** entité responsable d'une attaque de sécurité qui contourne les mécanismes de sécurité mis en place pour de différentes raisons :
  - Vérification de la sécurité d'un système.
  - Espionnage industriel ou militaire.
  - Curiosité occasionnelle par des utilisateurs (internes ou externes).
  - Divulguer l'intérieur de l'organisation ou de la société (le désir d'argent).
  - Etc.
- **Menace :** Une menace est un signe qui laisse prévoir un danger et on trouve
  - Menaces passives : consistent à écouter ou copier des informations de manière illicite.
  - Menace actives : consistent à altérer des informations ou le bon fonctionnement d'un service.
- **Vulnérabilité :** est une faille ou bug pouvant être utilisé pour obtenir un niveau d'accès illicite à une ressource ou à des privilèges supérieurs, et qui est exploité par une menace pour engendré une attaque.par exemple :
  - Utilisation des mots de passe non robustes.
  - Présence de comptes non protégés par mot de passe
  - Absence d'antivirus, pare-feu, …etc.
- **Les attaques :** 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.

I.5.Les piliers basique de la sécurité [3]

La sécurité réseau est la démarche de toute l'entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageables pour son activité, pour cela on fait appel à ces services :

- **Identification :** Information permettant d'indiquer qui vous prétendez être. Une Identification élémentaire est le nom d'utilisateur que l'on saisit dans un système informatique. Une identification plus évoluée peut être fournie par un relevé d'empreinte digitale, une analyse faciale ou rétinienne, etc.
- **Authentification :** Information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être. Une authentification élémentaire est le mot de passe que vous entrez dans le système informatique. Une authentification forte combine une chose que vous possédez et une

chose que vous connaissez (numéro de carte bancaire et code personnel, par exemple). L'authentification protège de l'usurpation d'identité.

- **Autorisation :** Information permettant de déterminer quelles sont les ressources de l'entreprise auxquelles l'utilisateur identifié et autorisé a accès, ainsi que les actions autorisées sur ces ressources. Cela couvre toutes les ressources de l'entreprise.
- **Confidentialité :** Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données. Un mot de passe ne doit jamais pouvoir être lu par un autre que son possesseur.
- **Intégrité :** Ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.
- **Disponibilité** : Ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, que ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc.
- **Non-répudiation :** Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.
- **Traçabilité :** Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure.

I.6. Le piratage [21] [4]

Pour mieux comprendre le sujet de **la sécurité en informatique**, il est nécessaire de connaitre les différents types de pirates informatiques, les types de piratage informatique ainsi que les techniques de piratage informatique, puisque les techniques de piratages vont souvent bien plus loin que les mesures de sécurité, et que cela constitue un défi.

I.6.1. Types de pirates

- **Les hackers** : ce sont « des passionnés des réseaux ». Ils veulent comprendre le fonctionnement des systèmes informatiques et tester à la fois les capacités des outils et leurs connaissances. En général, les hackers s'introduisent dans les systèmes par passion pour l'informatique et pas dans l'objectif de détruire ou de voler des données.

- **Les Crackers** : Sont des criminels informatiques dont leur but principal est de détruire ou voler des données, de mettre hors service des systèmes informatiques ou de 'kidnapper' un système informatique en vue de demander une rançon.

- **Les script-kiddies :** ce sont des pirates débutants qui agissent uniquement à l'aide des logiciels prêts à utiliser. Ils sont dans une logique de destruction ou de gain financier. Ils utilisent des outils qu'ils ne maîtrisent pas et dont ils ignorent le fonctionnement. La seule chose qu'ils font est l'exécution du logiciel et attendent le résultat.

I.6.2. Types de piratages

- **Le Hacking** : C'est l'accès non autorisé à un système ou un réseau informatique. Les pirates de **Hacking** attaquent essentiellement les réseaux informatiques (hackers, crackers et script-kiddies).
- **Le phreaking** : c'est le détournement de services de télécommunication par divers procédés, dans le but d'éviter les grosses factures de téléphone ou les oreilles indiscrètes. Un autre type de piratage téléphonique est l'utilisation détournée des téléphones cellulaires. Avec ce type de téléphones, aucune connexion physique n'est nécessaire, et il est facile d'écouter les conversations au moyen de scanners GSM et autres. Les téléphones cellulaires sont aussi facilement reprogrammables : les malfaiteurs peuvent ensuite les utiliser sans payer leurs communications, qui seront facturées aux véritables propriétaires.
- **Le « carding »** : Ces pirates s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles.
- **Les « hacktivistes »** : Se sont des hackers dont la motivation est principalement idéologique.

Finalement, plusieurs techniques de piratage informatique sont disponibles dans le marché comme suit :

- **Le « social engineering »** : c'est une technique qui consiste à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct. Elle est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de l'organisation : un technicien, par exemple un administrateur, etc.
- **Le scam** : est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur à besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.

- **Le « Spoofing IP »** ou usurpation d'adresse IP : Cette technique repose sur le fait de remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Elle permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.
- **Le « hijacking »** ou **« détournement de session »** : Le détournement de session est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

I.7. Les attaques [22]

I.7.1.Définition

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

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

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glâner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

I.7.2.Classification des attaques

- **Attaques passives :** elles ne modifient pas le comportement du système, et peuvent ainsi passer inaperçues.

- **Attaques sur la confidentialité :** leurs objectifs est d'obtention des informations sur un système, sur un utilisateur ou un projet par vol d'information via un réseau par espionnage des transmissions de données (espion de ligne, accès aux données dans des routeurs et des serveurs Internet). Méthodes possibles sont :
  - Ecoute
  - Injection de code
  - Usurpation d'identité
  - Intrusion
  - Abus de droits

- **Attaques actives :** elles modifient le contenu des informations du système ou le comportement du système. Elles sont en général plus critique que les passives.

- **Attaques sur l'intégrité :** leurs objectifs est modification ou destruction de données ou de configurations. Méthodes possibles sont :
  - Injection de code
  - Action physique
  - Intrusion
- **Attaques sur l'authentification :** leurs objectifs est l'utilisation des ressources de façon clandestine sur un système. Méthodes possibles sont:
  - Abus de droits
  - Intrusion
- **Attaques sur la disponibilité :** leurs objectifs est perturbation d'un échange par le réseau, d'un service ou d'un accès à un service. Méthodes possibles sont:
  - Abus de droits
  - Action physique
  - Intrusion

✓ **Méthodes :**

- **Intrusion :** exploitation des vulnérabilités du système pour exécuter des commandes non autorisées comme l'exploitation des erreurs de configuration (Satan, Cops), exploitation des bugs : Network Scanning, Sendmail, INN …
- **Abus de droits légitimes :** Utilisation d'une fonctionnalité du système de façon abusive, par exemple la diffusions de logiciels sur des comptes ftp anonymes, trop de requêtes pour saturer un serveur, sniffer des ports.
- **Action physique :** Destruction, altération ou changement physique d'un composant ; destruction d'un câble, débranchement d'une prise électrique…
- **Usurpation d'identité :** Utilisation d'une fausse identité pour abuser un système ou un utilisateur. changer d'adresse IP pour tromper le système : IP spoofing…
- **Injection de code :** Installation et exécution d'un module clandestin sur un système ; virus, bombes logiques (cheval de Troie), cookies, ver…
- **Ecoute :** Ecoute passive et clandestine sur le réseau dans le but de récupérer des informations ; analyseurs de réseau, sondes …

I.7.3. Les attaques par protocoles

I.7.3.1. IP spoofing :

Le spoofing consiste à usurper l'identité d'un utilisateur (se faire passer pour une personne ayant une adresse IP attribuée). Il peut se manifester sous la forme d'un courrier électronique, sur le système destinataire, provenir d'un utilisateur connu, ou plus dangereux sous la forme de paquets de données ressemblant à des paquets provenant d'une machine de confiance. Les étapes de cette attaque :

1. L'attaquant choisit sa victime (un serveur),
2. Il faut qu'il trouve ensuite une configuration pour laquelle sa victime autorise une connexion avec une machine de confiance, pour ensuite se faire passer pour la machine de confiance. Pour cela, la machine de confiance est rendue invalide, les numéros de séquence du serveur sont analysés,
3. Une connexion simulée avec des paquets falsifiés de l'attaquant est alors demandée au serveur avec des numéros de séquence devinés. Si la connexion est établie, l'attaquant modifie alors des informations pour permettre de revenir plus facilement ultérieurement.

I.7.3.2.Les Denial-of-Service (DoS) : [5]

Les attaques de type Denial-of-Service ont pour but de saturer un routeur ou un serveur afin de le ”crasher” ou en préambule d’une attaque massive. Ces types d’attaque sont très faciles `a mettre en place et très difficile à empêcher. Mais quelles sont les raisons qui peuvent pousser un attaquant à utiliser les DoS en sachant que cela peut mener à la **destruction** du routeur ou du serveur visé :

- Récupérer un accès : une attaque de type Denial-of-Service fait, la plupart du temps, partie d’une attaque visant à obtenir le contrôle d’une machine ou d’un réseau. Par exemple l’attaque de type ”SYN Flood”, très rependue, est souvent utilisée de paire avec une tentative de Spoofing,
- Masquer les traces : ce type d’attaque permet également de ”crasher” une station qui par exemple aurait pût contenir des traces du passage d’un ”Hacker”. En détruisant cette station, il s'assure ainsi une certaine pérennité,
- Se venger : très fréquemment, ces attaques sont utilisées afin d’assouvir une vengeance,
- Personnelle contre une personne, un administrateur ou bien encore une entreprise.

I.7.3.3. Attaque par épuisement de ressources (DHCP) [23]

Un serveur DHCP Dynamic Host Configuration Protocol possède un stock d'adresses IP qu'il distribue aux différents clients. Ce stock est bien sûr limité. Il y aura seulement un nombre défini de clients pouvant disposer des différentes adresses IP en même temps. Si le serveur est bien administré avec une liste «fermée» de correspondances entre adresses MAC et IP aucune attaque par épuisement n'est possible.

Si le service est mal administré ; c'est à dire que les correspondances entre adresses MAC et IP se font dynamiquement à partir d'une plage d'adresses IP vacantes, le scénario suivant est possible.

Si un pirate génère un grand nombre de requêtes DHCP semblant venir d'un grand nombre de clients différents, le serveur épuisera vite son stock d'adresses. Les «vrais» clients ne pourront donc plus obtenir d'adresse IP : le trafic réseau sera paralysé.

Si un pirate a réussi à saturer un serveur DHCP par épuisement de ressources, il peut très bien en activer un autre à la place. Ainsi il pourra ainsi contrôler tout le trafic réseau.

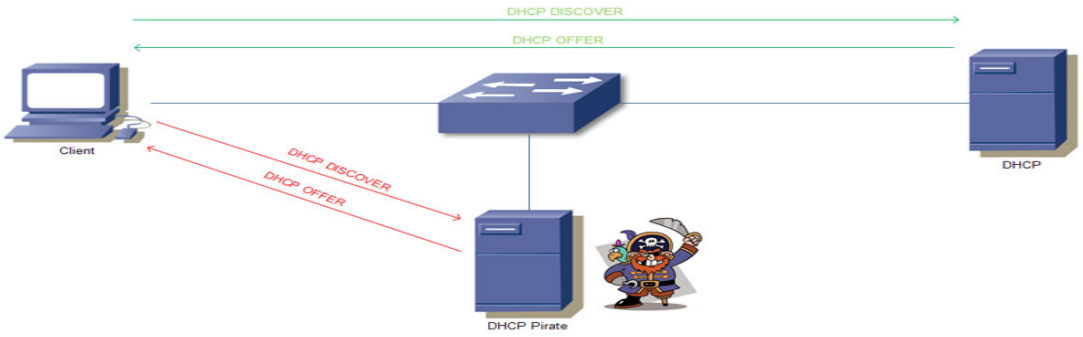


Figure I.3 : Attaque par épuisement de ressources

I.7.3.4.Attaque par redirection de port ou DNS ID spoofing

Il faut considérer trois éléments : un client, un serveur DNS et un pirate. Le client A veut communiquer avec un serveur Web, dont il connait son nom mais pas son adresse IP. Il va donc demander au serveur DNS la correspondance entre le nom et l'adresse IP. Après avoir reçu la demande et son identifiant de demande (ID) disant numéro du port sa valeur comprise entre 0 et 65535, le serveur DNS envoie la correspondance demandée. Si le pirate répond plus vite au client, à la place du serveur DNS, il pourra rediriger le trafic que le client croit envoyer au serveur Web, vers la machine qu'il veut. Par contre, il faut que le pirate connaisse l'ID de demande de correspondance. Pour cela il peut utiliser un sniffer sur le réseau, ou alors anticiper cet identifiant en envoyant des requêtes au préalable et analyser les réponses.

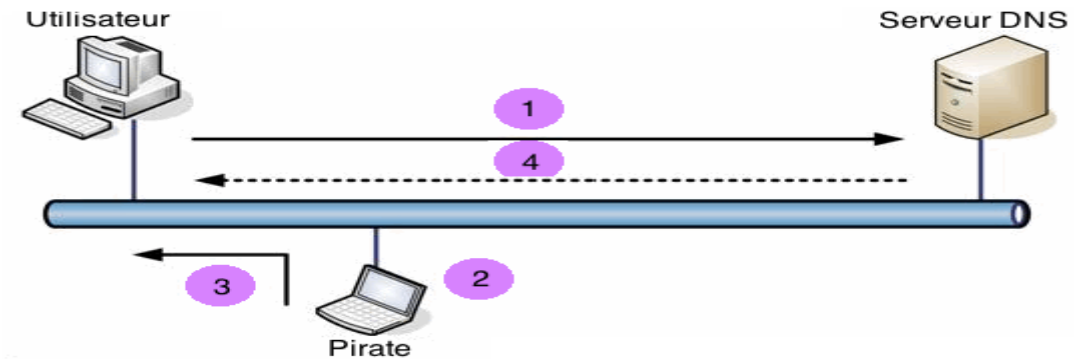


Figure I.4 : Attaque par redirection de port

I.7.3.5.Attaque par rebonds (FTP)

FTP (File Transfert Protocol, en écoute par défaut sur les ports 20 et 21) est le service utilisé pour assurer le transfert de fichiers. Il y a deux types de serveurs FTP : les serveurs FTP avec authentification par mots de passe et les serveurs anonymes. Pour les premiers, le client désirant se

connecter devra fournir un login accompagné d'un mot de passe pour authentification. Dans le cas du serveur FTP anonyme, tout le monde peut s'y connecter librement.

Le premier défaut du protocole FTP est de ne pas encrypter les mots de passe lors de leur transit sur le réseau. Les mots de passe associés aux logins circulent en clair à la merci des sniffers.

Si un pirate ne peut pas accéder à un serveur FTP non anonyme en raison d'un filtrage d'adresse IP, et si un serveur FTP en mode anonyme peut y accéder, alors le pirate peut accéder au premier par l'intermédiaire du second, et y récupérer les fichiers.

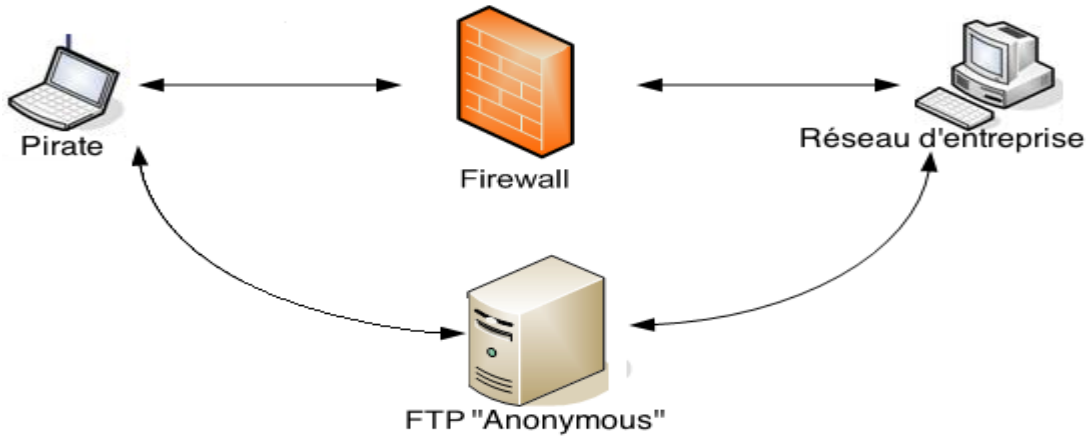


Figure I.5 : Attaque par rebonds

I.7.3.6. Le Sniffing [6]

Correspond à la surveillance des paquets IP qui transitent sur un réseau. L'un des buts finals est de récolter illégalement des mots de passe. Les logiciels, qui permettent d'analyser le trafic sont très utilisés à des fins de gestion de réseau ; ils sont disponibles généralement avec divers systèmes d'exploitation, ou en freeware sur le réseau. Ils s'exécutent sur n'importe quel PC en sniffant et en analysant les données en transit sur les lignes, pour en extraire les mots de passe transmis par l'utilisateur lors de sa demande de connexion.

Cette écoute passive de données en transit peut conduire à des intrusions illicites. Une protection peut être apportée aux mécanismes de transfert de mots de passe, le chiffrement de ceux-ci. Les mots de passe chiffrés devront alors être « cassé ». Deux possibilités :

- **l'attaque en force :** essayer toutes les permutations possibles pouvant constituer une clé pour déchiffrer le mot de passe en connaissant l'algorithme utilisé.
- **l'attaque par dictionnaire :** deviner le mot de passe chiffrés par comparaison avec des listes de mots de passe eux aussi chiffrés contenus dans des dictionnaires.

❖ **Les moyens de se protéger du sniffing :**

- tester les mots de passe des utilisateurs en utilisant les mêmes techniques que ceux qui font ce genre d'attaques.
- les sniffeurs sont difficilement détectables, c'est pourquoi il est préférable de segmenter le réseau par des ponts, routeurs ou commutateurs, pour restreindre l'action d'un sniffeur.

I.7.3.7.Attaque par le protocole RIP (Routing Information Protocol)

Ce protocole peut être utilisé pour détourner des communications : l'imposteur se fait passer pour l'émetteur autorisé, envoie de fausses informations de routage aux passerelles et aux destinataires, qui utiliseront l'adresse IP donnée par le paquet RIP de l'imposteur pour transmettre des données à destination de l'émetteur, qui est en fait le récepteur.

I.7.3.8.Attaque par requêtes ARP (Address Resolution Protocol)

Une requête ARP peut être diffusé jusqu'à ce qu'une machine se reconnaissant , et renvoie son adresse Ethernet. Mais si une requête ARP est émise avec une adresse IP inexistante, on peut générer des tempêtes de diffusion (broadcast storm),ce qui provoque la saturation de la bande passante, et rend indisponible le réseau(effondrement du réseau, déni de service) .

Pour éviter ce type d'attaque, les systèmes sont configurés de façon à limiter la diffusion (broadcast) et avec des temporisations.

I.7.3.9.Attaque ICMP (Internet Control Message Protocol) [24]

Le protocole ICMP contrôle l'acheminement des paquets de données IP, et si un problème de transmission est détecté par un routeur, celui-ci informe l'émetteur du paquet en lui envoyant un paquet ICMP.

Par exemple, des faux messages ICMP peuvent être générer pour surcharger le réseau, le rendre inutilisable, et entraîner certains dénis de service.

Autres exemples :

- paralyser le réseau en rédigeant des paquets IP vers une fausse destination
- augmenter la charge des systèmes en faisant traiter un grand nombre de messages ICMP
- empêcher un émetteur d'envoyer des données, en exploitant la facilité offerte par ICMP pour contrôler le flux d'émission des paquets. Cela provoque des conséquences sur le trafic supporté par le réseau et atteinte aux performances du réseau.

Pour éviter ce genre d'attaque, on peut :

- configurer les routeurs de sorte qu'ils ne génèrent plus qu'un certains nombre de messages ICMP pendant une période de temps donnée.

- s’appuyer sur la fonction de surveillance des systèmes de gestion de réseau pour détecter un nombre abusif de message ICMP, et déclencher l’alarme lorsque le taux de charge est anormal.

I.7.3.10.Attaque par tromperie UDP

Le protocole UDP n’effectue pas de contrôle (contrôle de flux, contrôle d’erreur et contrôle d’identification) lors de transfert de données entre 2 correspondants. N’importe qui peut donc utiliser une adresse IP d’une machine autorisée à se connecter à un système, et le pénétrer. Ces vols de sessions UDP peuvent avoir lieu sans que le serveur s’en rende compte. Afin de l'éviter il faut configurer les serveurs pour les refuser et les firewalls pour les bloquer.

I.7.3.11.Attaque par débordement de tampon (buffer overflow)

Cette attaque vise les systèmes informatiques en exploitant leurs caractéristiques internes de fonctionnement, notamment celles de leur système d’exploitation, et non celles liées aux protocoles qu’ils supportent.

Par exemple, l’attaquant fait subir des dépassements de capacités de certaines zones tampon entraînant des dysfonctionnements graves pouvant entraîner l’arrêt des systèmes.

Par exemple, le port 80 n’étant pas filtré par le pare-feu, un débordement de la mémoire tampon du serveur web via une longue requête HTTP est possible, et elle peut contenir un bout de code trafiqué qui sera exécuté par le serveur. Celui-ci écoutera le trafic et exécutera les commandes transmises par le hacker.

Solutions :

- le développeur du service réseau peut décider de se passer de C/C++ et d’employer à la place des langages qui n‘ont pas ce genre de problème de débordement de tampon comme Java ou ADA
- cas de services déjà écrits en C ou C++, il est nécessaire de recourir à des outils statistiques de vérification automatique, ou à des compilateurs qui ajoutent à la volée, du code source pour vérifier chaque accès à des tampons. Par exemple, StarGuard détecte les attaques par débordement de pile en empêchant l’adresse retour d’être modifiée.

I.8.Les virus [25]

Un virus est un programme informatique qui, a l'insu de l'utilisateur, exerce une action nuisible a son environnement ; la principale étant la modification ou la destruction des données.

Le virus est un ensemble d'instruction parasites qui s'introduisent et se cachent a l'intérieur d'autres programmes.

Un virus se développe généralement en trois phases :

- le virus s'implante dans un programme sain
- le virus se propage de façon transparente dans les autres programmes sains
- le virus déclenche son action

On distingue plusieurs catégories de virus définis selon le type d'hôte sur lequel ils s'attachent:

- les virus sur les exécutables : le virus va s'introduire dans le fichier exécutable pour accéder a la mémoire du système et s'exécuter. Ces virus sont généralement écrit en assembleur afin d'être de taille minimale.

- les virus sur boot sector: le virus va écraser le secteur de boot d'une disquette ou d'un disque dur

- les fichiers scripts : les virus sont des macros généralement associées aux fichiers de bureautique tels que Microsoft Office. La création de tels programmes sont très faciles a mettre en œuvre (généralement un morceau de code Visual Basic) et sont indépendants du type de plate-forme sur laquelle elle s'exécute.

En tout, on a recensé plus de 1 500 virus de macros, responsables de la moitié de toutes les attaques virales.

- **Petite lexicographie sur les virus :**

Virus crypté : le virus va crypter son contenu à chaque infection pour éviter de dévoiler les chaînes de caractères qui faciliteraient le travail des anti-virus.

Virus polymorphe : c'est un virus qui essaye de changer d'apparence a chaque nouvelle infection. Cette technique est apparue pour contrer la recherche de signatures par les anti-virus.

Virus macro : c'est un virus qui exploite le langage macro de certaines plates-formes logicielles.

Virus non résident : le virus va s'exécuter a chaque fois que l'utilisateur va lancer un exécutable infecté. Quand le virus a infecte suffisamment de fichiers, il s'arrête et rend la main au programme sur lequel il est implanté.

Virus résident : le virus va s'installer dans la mémoire du système et va fonctionner pendant toute la durée de marche de la machine infectée.

I.9.Les vers (worm)

Un ver est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique. Contrairement à un virus informatique, un ver n'a pas besoin d'un programme

hôte pour se reproduire, il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. L'objectif du ver est d'espionner l'ordinateur où il se trouve, offrir une porte dérobée à des pirates informatiques, détruire les données de l'ordinateur infecté et envoyer de multiples requêtes vers un serveur internet dans le but de le saturer (déni de service). Il a pour effet le ralentissement de la machine infectée.

I.10. Trojans (Chevaux de Troie)

Un trojan est un programme malicieux qui est présenté comme un programme inoffensif tel qu'un économiseur d'écran, un petit jeu ou même un programme pour trouver et éradiquer des virus. Par analogie avec le mythe du cheval de Troie, l'utilisateur croyant manipuler un programme inoffensif va déclencher une action malveillante. Ils ne se répliquent pas a la manière des virus et ne se propage pas non plus comme les vers. On le trouve généralement attaché à des mails ou présents sur des sites de téléchargement. Les actions effectuées par les trojans sont diverses : récupération de fichiers de mots de passe, infection d'une machine avec un virus ou utilisation comme un outil pour espionner des machines distantes.

I.11.Politique de sécurité réseau [26]

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

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

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

- Identifier les besoins en terme 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 ;

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en termes de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.

De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de conseiller les décideurs sur les stratégies à mettre en œuvre, ainsi que d'être le point d'entrée concernant la communication à destination des utilisateurs sur les problèmes et recommandations en terme de sécurité.

La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :

- Un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
- Une procédure de management des mises à jour ;
- Une stratégie de **sauvegarde** correctement planifiée ;
- Un plan de reprise après incident ;
- Un système documenté à jour.

I.12.Les mécanismes (cryptage, signature électronique et certificat...)

I.12.1.La cryptographie

Permet d ‘assurer la confidentialité grâce aux systèmes de chiffrement, et l’authentification grâce à la signature numérique et au certificat.

Les **systèmes de chiffrement** sont assurés par des algorithmes de chiffrement utilisant une clé de chiffrement. Plus la clé de chiffrement est longue, plus elle nécessite de puissance et de temps de calcul pour la trouver. Il existe deux principes de chiffrement :

- **le chiffrement symétrique ou à clé privée :** la même clé permet de décrypter et de crypter les messages en l'appliquant à un algorithme. Cette clé est partagée entre les deux parties communicantes.

  Les principaux algorithmes symétriques sont DES, RC2,RC4,RC5 et IDEA(utilisé par le protocole de messagerie PGP). Ce système n'est pas adapté pour des grands réseaux comme internet.

- **le chiffrement asymétrique ou à clé publique :** il utilise deux clés différentes pour chaque utilisateur, l'une publique accessible par tout le monde et une privée qui ne doit être qu'à l'usage de son propriétaire. Le message est soit chiffré avec la clé publique du destinataire, et il sera déchiffré avec la clé privée du destinataire ou chiffré avec la clé privée de l'émetteur et déchiffré avec la clé publique de l'émetteur. On doit connaître la clé publique de ses partenaires si l'on veut leurs envoyer des données confidentielles.

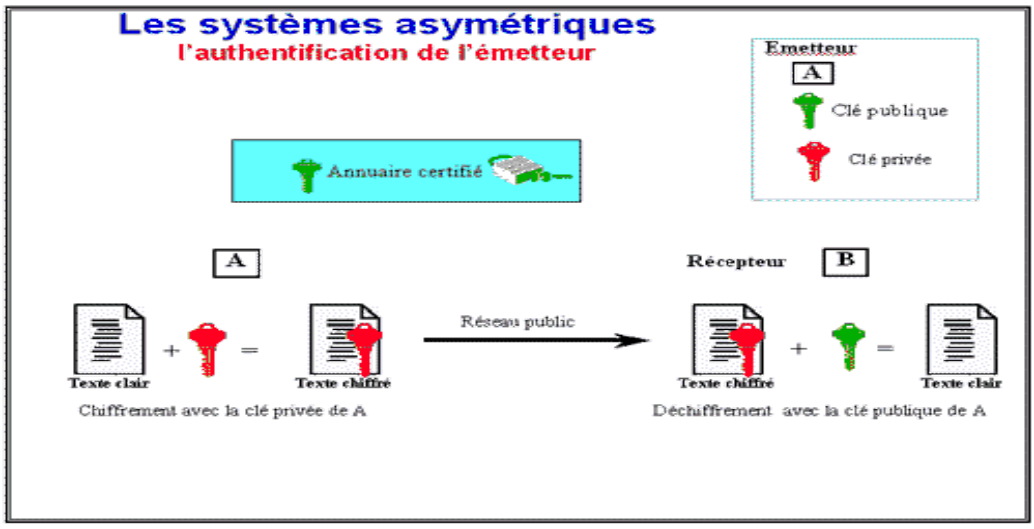


Figure I.6 : Les systèmes asymétriques (Authentification)

Explication :

- l'émetteur A à chiffré un message à l'aide de sa clé privée.
- tout le monde a accès à la clé publique de A, grâce à l'annuaire certifié. Donc tout le monde peut lire le message émis par A, après l'avoir déchiffré à l'aide de la clé publique de A

Rappel : - A est le seul capable d'émettre un message chiffré avec sa clé privée. Tous les récepteurs qui déchiffreront le message avec la clé publique de A savent que c'est A qui est l'émetteur et lui seul. L'authentification de A est donc acquise.

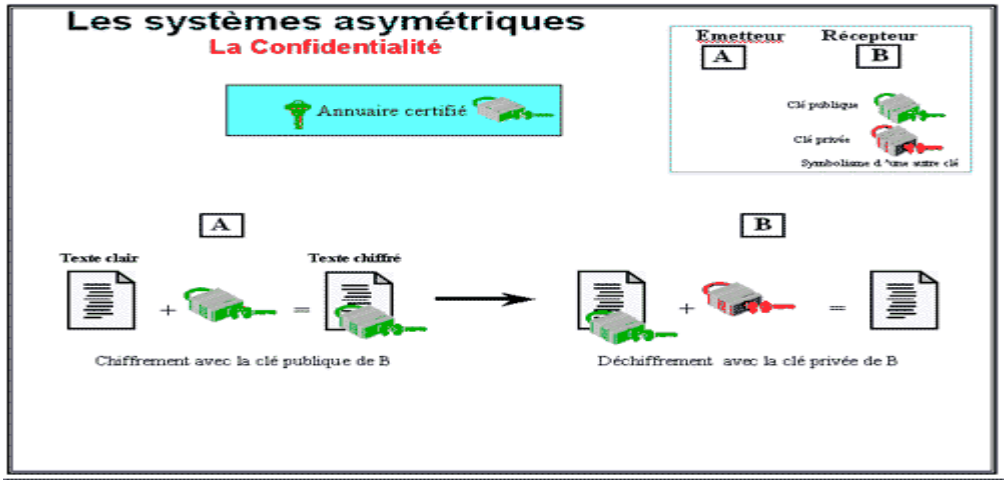


Figure I.7 : Les systèmes asymétriques (Confidentialité)

Explication :

- tout le monde a accès à la clé publique de B. Seul B peut lire le message chiffré par A, car il n'y a que lui qui possède sa clé privée qui est l'autre " moitié " de sa clé publique

Les principaux algorithmes à clé publique sont : RSA, Diffie-Hellman, EL Gamal. Le temps d'exécution de ces algorithmes produise des overheads importants. De nouveaux algorithmes, basés sur les équations les calculs de circonférences des ellipses (cryptographie à courbe elliptique), devraient les remplacer.

- En conclusion, les systèmes symétriques offrent les avantages de la vitesse de chiffrement pour assurer la confidentialité et les systèmes asymétriques eux, offrent l'assurance de la signature par l'authentification de l'émetteur et l'intégrité du texte émis.
  La combinaison de ces deux systèmes permet d'utiliser les avantages de la clé symétrique et ceux de la clé asymétrique.

I.12.2.La signature électronique [7]

Sert à signer électroniquement un document en utilisant un algorithme de chiffrement à clé publique. Le déroulement d'un échange :

- chiffrer le message avec sa clé privée pour constituer sa signature que l'on ajoute au message à envoyer,
- chiffrer le message et sa signature avec la clé publique du destinataire puis émission du message
- à la réception, le destinataire déchiffre le message avec sa clé privée et la signature avec la clé publique de l'émetteur.

Cela permet l'authentification de l'émetteur et prouve l'origine du message.

- Une **empreinte digitale** est une technique basée sur une fonction mathématique appelée fonction de hachage appliquer sur une portion du message, et le résultat de cette fonction est appelé code de hachage, il fait usage de signature numérique. Il est crypté avec la clé privé de l'émetteur et rajouté au message, puis le message est envoyé au destinataire, celui- ci décrypte le code de hachage grâce à la clé publique de l'émetteur, et le compare avec un autre code calculé grâce au message. Si les deux codes correspondent, le destinataire sait que le message n'a pas été altéré et que son intégrité n'a pas été compromise. Ce principe de signature a été amélioré par la mise en place des certificats permettant de garantir la validité de la clé fourni par l'émetteur.
- L'**enveloppe digitale (système mixte)** combine l'usage du chiffrement symétrique et du chiffrement asymétrique. Pour chiffrer des messages de grandes tailles, on utilise une clé de session, valide pour les deux interlocuteurs durant la durée de l'échange. Déroulement d'un échange entre deux interlocuteurs :

- génération aléatoire, par l'un des deux partenaires de la communication, d'une clé de session à l'aide d'un algorithme asymétrique à clé publique.
- le message est chiffré grâce à cette clé et un algorithme à clé symétrique
- la clé de session est chiffrée avec la clé publique du destinataire, c'est l'enveloppe digitale du message
- le message chiffré et l'enveloppe sont envoyés au destinataire
- celui-ci déchiffre l'enveloppe avec sa clé privé pour connaître la clé de session et ainsi décrypter le message
- le destinataire peut aussi utiliser la clé de session pour émettre des messages chiffrés vers son interlocuteur.

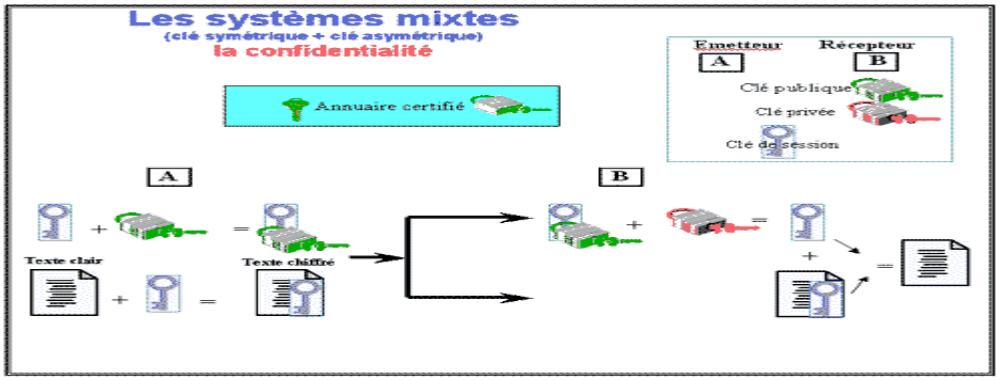


Figure I.8 : Les systèmes mixtes

I.12.3.Le certificat

C'est une structure de données qui est numériquement signée par une autorité de certification(CA). Il sert à assurer l'intégrité des clés publiques. Le CA utilise sa clé privée pour signer le certificat et assure ainsi une sécurité supplémentaire. Si le récepteur connaît la clé publique du CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et est assuré que le certificat contient donc des informations fiable et une clé publique valide.

Exemples d'applications cryptées :

- **SSL** (niveau transport) :protocole de sécurité fournissant l'authentification client/serveur ainsi que la confidentialité des données(cryptage). L'application principale de ce protocole est HTTPS : service web sécurisé.
- **S/MIME, PGP S/MIME**(Secure Multipurpose Extension) et PGP(Pretty Good Privacy, niveau applicatif) : ces deux protocoles sont utilisés pour le cryptage et la signature électronique des mails.
- **SSH** (niveau transport) : remplaçant du protocole Telnet out tout est crypté(mot de passe, session)

I.12.4. Les Antivirus

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares), également appelés virus, Chevaux de Troie ou vers selon les formes. L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques), la mémoire vive de l'ordinateur et les périphériques de stockage comme les disques durs, internes ou externes, les clés USB et les cartes à mémoire Flash. La détection d'un logiciel malveillant peut reposer sur trois méthodes :

- ✓ reconnaissance d'un code déjà connu (appelé signature) et mémorisé dans une base de données.
- ✓ analyse du comportement d'un logiciel.
- ✓ reconnaissance d'un code typique d'un virus.

I.12.5.Pare-feu [8]

Le **pare-feu** ou **firewall** protège votre ordinateur contre des intrusions par Internet. Il sert à la fois de moniteur et de filtre pour les mouvements du réseau. Son rôle est d'inspecter les échanges de données et l'identité des utilisateurs. Si certaines informations éveillent sa curiosité, il les empêche de pénétrer dans votre système. Il peut bloquer automatiquement les informations qui lui semblent suspectes. Il fonctionne comme une barrière qui empêche certains paquets d'entrer sur votre réseau. Le but est de protéger votre système contre des attaques potentielles, qui se font généralement par Internet. Un bon moyen de le faire est de fermer les ports de service qui ne sont pas indispensables.

Le pare-feu est généralement lié à deux plaques de réseau : l'une est liée à Internet, l'autre au réseau interne. Il doit être configuré pour ne pas laisser passer des paquets qui doivent transiter d'un réseau à l'autre. Le pare-feu peut être logique ou physique, logiciel ou matériel.

Enfin, il existe deux types de fonctionnement :

- ✓ Le pare-feu analyse les adresses IP et les paquets d'un réseau,
- ✓ Le pare-feu analyse les applications dans les paquets IP.

Le matériel (hardware) et les logiciels (softwares) mènent une action couplée garantissant la sécurité d'un réseau interne connecté à Internet. Le pare-feu configuré sur un serveur bloque le trafic susceptible d'être dangereux pour le réseau de l'entreprise (ou pour l'ordinateur de particuliers).

On distingue deux types de pare-feu :

- **Les filtres de paquets** inspectent uniquement l'en-tête de chaque paquet. Elle est comparée avec une liste d'autorisations. Seuls les paquets autorisés pourront passer à travers le pare-feu, comme par exemple les emails ;
- **Les applications filtres** sont plus sophistiquées. L'inspection ne se limite pas à l'en-tête, le contenu des paquets est lui aussi examiné. De ce fait, leur mise en œuvre est plus complexe, mais plus fiable.

Conclusion

Les techniques de protection contre les attaques Internet permettent de réaliser les bases de la sécurité : confidentialité, intégrité, authentification, disponibilité.

Mais malgré toutes ces techniques utilisées pour empêcher les attaques Internet, un système n'est jamais totalement sûr. La cryptographie a ses faiblesses : une clé de chiffrement pour chiffrer des données peut être cassée.

Chapitre II : Introduction à la cryptographie

Introduction

L'idée de coder un message dans le but de le rendre inintelligible à toute tierce personne ne date pas aujourd'hui .les « messages secret » ont joué un rôle important dans tous les conflits depuis que l'homme sait écrire, et sont habituellement associés aux guerres et aux agents secrets.

Le but de ce chapitre, est de présenter les fondements et le fonctionnement de la cryptographie. Il intéressera le lecteur qui connaît peu ou pas le domaine et qui souhaiterait comprendre le fonctionnement et les mécanismes mis en œuvre en cryptographie.

II.1 Cryptologie [9] [10]

La cryptologie est la science du secret, ne peut être vraiment considéré comme une science que depuis peut de temps. Cette science englobe la cryptographie, la cryptanalyse et la stéganographie, comme elle a été décrite dans cette figure en dessous.

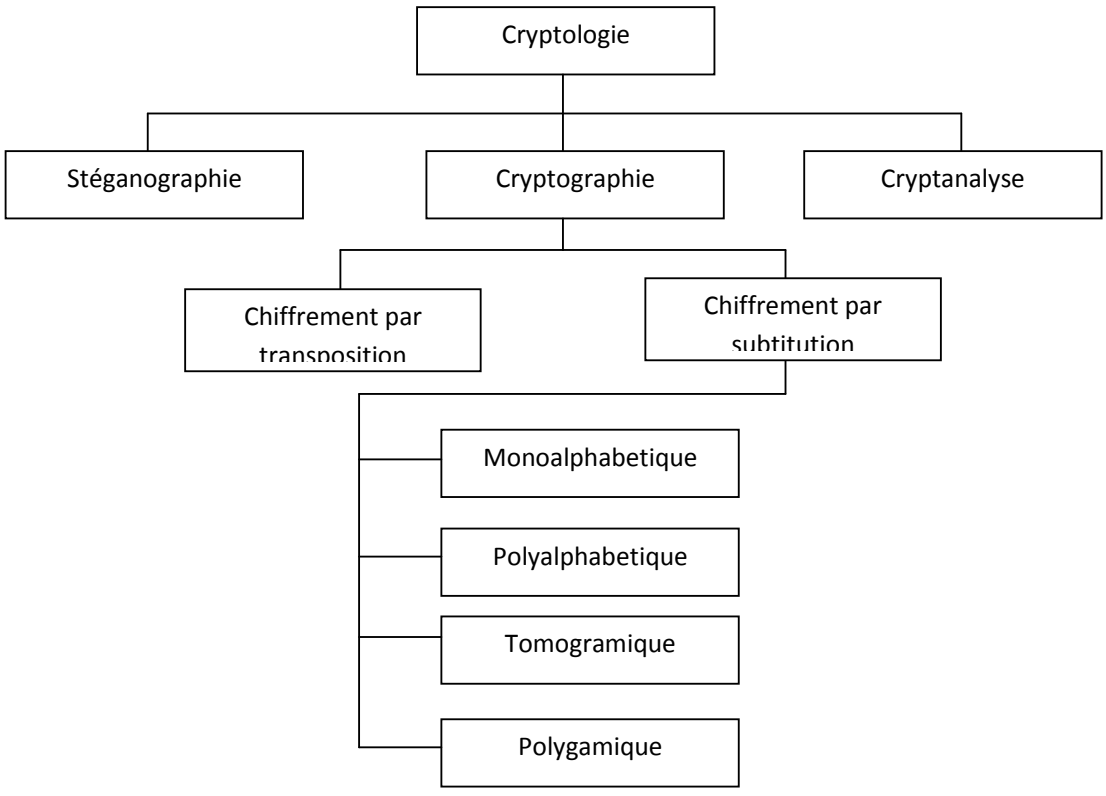


Figure II.1 les composants de la cryptologie

II.1.1 Cryptographie

La cryptographie est l'ensemble des techniques (algorithmes, matériels, logiciels) permettant de protéger une communication au moyen d'un code secret. Le mot cryptographie découle des mots grecques **« Krypto »** (je cache) et **« graphe »** (le document).

II.1.2 Cryptanalyse

La cryptanalyse est la science de reconstitution du texte en clair sans connaitre la clé. Une cryptanalyse réussie peut fournir soit le texte en clair, soit la clé de chiffrement. La cryptanalyse est surtout utilisée pour mettre en évidence les faiblesses d'un crypto-système et contribuer à améliorer la robustesse des techniques de cryptographie. Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un crypto-système, on dit alors que l'algorithme de chiffrement a été « cassé ». On distingue habituellement quatre méthodes de cryptanalyse :

- ✓ **Une attaque sur texte chiffré seulement**

  Le cryptanalyste dispose d'un ensemble de textes chiffrés par le même algorithme et cherche à déterminer le plus grand nombre de textes en clair correspondant ou encore la clé ou les clés de déchiffrement ;

- ✓ **Une attaque sur texte clair connu**

  Le cryptanalyste dispose d'un ensemble de textes en clair et leurs correspondance en textes chiffré par le même algorithme et une même clé. IL cherche à déterminer la clé de déchiffrement ou un autre algorithme permettant de déchiffrer n'importe quel autre texte chiffré par le même algorithme et la même clé ;

- ✓ **Une attaque sur texte clair choisi**

  En plus du fait que le cryptanalyste dispose de textes en clair et de leurs correspondants en textes chiffrés, il peut également choisir un texte en clair spécifique et disposer de sa correspondance en texte chiffré ;

- ✓ **Une attaque sur texte chiffré choisi**

  Consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair.

II.1.3 Stéganographie

La stéganographie sert à cacher des messages secrets dans d'autres messages, de sorte que l'existence même du secret est dissimulée. Généralement l'expéditeur écrit un message inoffensif et dissimule un message secret dans la même feuille de papier.

II.1.3.1 Le texte caché

Enfin	Voici	le	Printemps
Un	oiseau	de	Passage
Chante	Un	message	Emprunt
D'	Un	doux	Secret

Enfin	**Voici**	le	Printemps	Clé : BACD
Un	oiseau	de	Passage	Le texte caché est :
Chante	Un	**message**	Emprunt	**Voici un message secret**
D’	Un	doux	**Secret**	

II.1.3.2 La stéganographie dans les fichiers images :

De la même manière que pour le texte, il est possible de cacher de l'information dans des fichiers images. En modifiant ou altérant quelques bits du fichier, il est ainsi possible de cacher un copyright ou alors un message de son choix sans que cela se voit. En effet, cette altération sera peu ou pas visible car l'œil humain n'est pas capable de discerner des petites aberrations sur une grande image à condition que le ratio taille du message / taille de l'image ne soit pas trop grand.

En conclusion, il faut retenir que la stéganographie est une méthode de cryptographie faible : elle repose uniquement sur le fait que personne ne remarquera le canal caché. Dès lors que ce canal est connu, il n'y a plus aucune protection.

II.2 Cryptographie classique

Ce paragraphe présente plusieurs algorithmes ou méthodes de cryptographie à une époque où les mathématiques ne régnaient pas encore en maîtres sur ce domaine.

II.2.1 Cryptographie par transposition (technique grecque) [27]

Une méthode de chiffrement datée entre le Xème et VIIème siècle avant Jésus Christ repose sur l'utilisation d'un bâton appelé scytale d'un diamètre fixé. Une lanière en cuir était enroulée en hélice autour de ce bâton et le texte en clair était alors écrit sur la lanière. Ensuite, la lanière était déroulée et pouvait être envoyée (sans le bâton) au destinataire du message.

Figure II.2 Scytale grecque

Pour déchiffrer le texte chiffré, il suffisait d'utiliser un bâton possédant exactement le même diamètre que le précédent, d'y enrouler la lanière de cuir et le texte en clair pouvait alors être relu.

Le procédé utilisé par cette méthode est un chiffrement par transposition, c'est-à-dire que les lettres ne sont pas modifiées mais que seul l'ordre des lettres est changé.

II.2.2 Cryptographie par substitution [27][11]

Les systèmes de cryptographie par substitution sont considérés comme des applications bijectives des lettres de l'alphabet des messages clairs sur des lettres de l'alphabet des cryptogrammes : on remplace des caractères par d'autres. On distingue :

II.2.2.1 Chiffrement monoalphabétique [27] [12]

Chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré. Les exemples les plus célèbres sont les algorithmes de César, Rot13, et bien évidemment le code morse. Ils sont encore utilisés aujourd'hui pour cacher le sens de certains messages (par exemple la solution de certains jeux dans des journaux), mais bien sûr elles sont très peu sûrs. En effet avec ce principe, les lettres les plus fréquentes dans le texte en clair restent les plus fréquentes dans le texte chiffré, il ne cache donc pas les fréquences d'apparition des caractères. C'est une faiblesse importante puisque des techniques statistiques peuvent être utilisés pour associer aux lettres les plus fréquentes, une lettre probable et en appliquant une technique sémantique récursive, les algorithmes à base de substitutions monoalphabétiques sont facilement cassés par les spécialistes.

II.2.2.2 Chiffrement poly-alphabétique

Le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans ou plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutions mono-alphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair. On choisit une clé qui sert d'entrée dans la grille poly-alphabétique incluant autant de symboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettre particulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondant du texte en clair en utilisant la grille poly-alphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si la longueur de celle-ci est inférieure à celle du texte de départ). Bien que de nombreux systèmes existent, nous présentons ici celui qui demeure le plus connu.

a. Chiffrement de vigenère

Le chiffrement de vigenère (1523-1596) est un chiffrement à décalage par clé. Au lieu d'effectuer un décalage constant dans l'alphabet du message en clair, comme dans le code de césar, vigenère réalise un décalage lié a une clé (la clé de chiffrement).chaque lettre de la clé sert de valeur

de décalage dans l'alphabet du message en clair. Deux lettres identiques de ce message en clair ne seront donc plus obligatoirement codées de la même manière**. [12]**

Il nécessite ensuite un mot clé seulement connu par l'émetteur et le destinataire du message. C'est le premier algorithme à introduire la notion de clé**.** Le chiffrement est effectué à l'aide de la table suivante :

Clé Utilisée \ Lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

(Lettre Codée)

Figure II.3 Table de chiffrement de vigenère

Ce mot clé est répété autant de fois que nécessaire afin d'avoir autant de lettres (ou plus) que le texte en clair à chiffrer. Ensuite l'alphabet utilisé pour chiffrer une lettre est celui correspondant à la lettre du mot clé.

Le croisement de la colonne de la lettre en clair et la ligne de la lettre de la clé donne la lettre codée.

Si le texte à chiffrer est "rendons a vigenere ce qui est a vigenere", avec le mot clé "RAYMOND", le texte chiffré est "IELPCAV R VGSSAHIE AQ EHL VSR M JVJVNCDS".

II.2.2.3 Chiffrement tomogrammique

Dans les systèmes tomogrammique, chaque lettre est tout d'abord représenté par un groupe de plusieurs symboles. Ces symboles sont ensuite chiffrés séparément ou par groupe de taille fixe.

a. Chiffrement ADFGVX [12][28]

Le chiffrement ADFGVX est un système utilisé pendant la première guerre mondiale son intérêt est d'utiliser les deux styles de chiffrement : substitution et permutation.
L'algorithme se subdivise en deux étapes :

- ✓ **Chiffrement par substitution**

Utilise un tableau secret qui permet de substituer une lettre (26 possibilité) ou un chiffre (10 possibilité) par deux lettres prise parmi les six lettres A, D, F, V, G ou X.
Par exemple, si l'on utilise le tableau de chiffrement suivant :

	A	**D**	**F**	**G**	**V**	**X**
A	8	T	B	W	r	Q
D	p	4	c	g	2	9
F	3	O	5	m	x	E
G	d	A	z	j	s	Y
V	l	H	7	u	v	0
X	N	1	k	6	i	F

Tab II.1 Table 6X6 de codage

Le message « lancer assaut » deviendra : AV DG AX FD XF VA DG VG VG DG GV DA.

- ✓ **Chiffrement par transposition**

Utilise une permutation et un mot clé secret de taille n, tout d'abord on crée une grille de n colonnes sur laquelle on place ce mot secret en tête et ou l'on inscrit ensuite, ligne après ligne, le cryptogramme intermédiaire obtenu à la première étape. Ensuite, en effectue des permutations de colonnes, de sorte que les lettre du mot-clé secret soient réordonnées dans l'ordre alphabétique.
Si on reprend l'exemple précédent avec le mot clé « chat » on obtient le tableau suivant :

Clé original	C	H	A	T
Message Codé	A	V	D	G
	A	X	F	D
	X	F	V	A
	D	G	V	G
	V	G	D	G
	G	V	D	A

Tab II.2 Table de ADFGVX avec la clé « chat »

Après classement alphabétique des lettres de la clé, le tableau suivant contient le message chiffré final :

Clé classée	A	C	H	T
Message Codé Et transposé	D	A	V	G
	F	A	X	D
	V	X	F	A
	V	D	G	G
	D	V	G	G
	D	G	V	A

Tab II.3 Table de ADFGVG avec la clé classée « acht »

Le message définitif, obtenu par lecture des colonnes du tableau, est donc : DF VV DD AA XD VG VX FG GV GD AG GA. Le destinataire le déchiffrera en suivant ces mêmes étapes dans l'ordre inverse, à condition de connaître la clé originale de transposition et de disposer de la table 6×6 de codage.

II.2.2.4 Chiffrement polygamique

Dans un chiffrement polygrammique un groupe de n lettres est chiffré par un groupe de n symboles. Parmi les nombreux exemples de tels chiffrements, on citera le chiffrement de playfair.

a. Chiffrement de Playfair

Le chiffre de Playfair utilise un tableau de 5x5 lettres, contenant un mot clé ou une phrase. La mémorisation du mot clé et de 4 règles à suivre suffisent pour utiliser ce chiffrement.

Pour chiffrer un message, il faut prendre les lettres 2 par 2 et appliquer les règles suivantes en fonction de la position des lettres dans la table :

- ✓ si les 2 lettres sont identiques (ou s'il n'en reste qu'une) mettre un 'X' après la première lettre. Chiffrer la nouvelle paire ainsi constituée et continuer avec la suivante. Dans certaines variantes, on utilise 'Q' au lieu du 'X', mais n'importe quelle lettre peut faire l'affaire,
- ✓ si les lettres se trouvent sur la même ligne de la table, il faut les remplacer par celles se trouvant immédiatement à leur droite (en bouclant sur la gauche si le bord est atteint),
- ✓ si les lettres apparaissent sur la même colonne, les remplacer par celles qui sont juste en dessous (en bouclant par le haut si le bas de la table est atteint),
- ✓ sinon, remplacer les lettres par celles se trouvant sur la même ligne, mais dans le coin opposé du rectangle défini par la paire originale.

En supposant que la clé soit « exemple Playfair », le tableau doit alors être rempli comme suit :

E	X	M	P	L
A	Y	F	I	R
B	C	D	G	H
J	K	N	O	Q
S	T	U	V	Z

Tab II.4 Table 5x5 de la clé

Chiffrement du message « Cache l'or dans la souche de l'arbre » :

CA	CH	EL	OR	DA	NS	LA	SO	UC	HE	DE	LA	RB	RE

Tab. II.5 Tableau de message en clair

Le message chiffré est le suivant :

BY	DB	XE	QI	BF	JU	ER	VJ	TD	BL	BM	ER	AH	AL

Tab II.6 Tableau de message chiffré

II.2.3 Chiffrement de Vernam (masque jetable)

Le chiffrement par la méthode du masque jetable est défini comme un chiffre de Vigenère avec la caractéristique que la clef de chiffrement a la même longueur que le message clair.

Clair	M	A	S	Q	U	E	J	E	T	A	B	L	E
Clef	X	C	A	A	T	E	L	P	R	V	G	Z	C
Décalage	23	2	0	0	19	4	11	15	17	21	6	25	2
Chiffré	J	C	S	Q	N	I	U	T	K	V	H	K	G

Tab II.7 Exemple de One Time Pad

Pour utiliser ce chiffrement, il faut respecter plusieurs propriétés :

- ✓ Choisir une clef aussi longue que le texte à chiffrer,
- ✓ Protéger votre clef,
- ✓ Utiliser une clef formée d'une suite de caractères aléatoires,
- ✓ Ne jamais réutiliser une clef.

Le principe est alors de combiner clé et message par un XOR bit a bit. Cette technique est inconditionnellement sure sous réserve que la chaine commune K soit parfaitement aléatoire. L'inconvénient majeur de cette technique est qu'il faut partager des chaines aléatoires extrêmement longues.

La cryptographie classique, la sécurité des données est basée sur le secret de l'algorithme de chiffrement, mais cette technique présente de nombreux inconvénients, comme l'obligation de changer l'algorithme de chiffrement si celui-ci est divulgué par un des à l'échange.

II.3 Cryptographie moderne

Avec le temps, les cryptographes ont pris conscience qu'il n'était pas réaliste de faire reposer un système de chiffrement sur l'hypothèse qu'un attaquant n'a pas connaissance de la méthode utilisé. En conséquence, ils ont introduit un nouveau type de cryptographie dans lequel la sécurité des algorithmes de chiffrement repose uniquement sur le secret de la clé de déchiffrement, il s'agit de la cryptographie moderne.

La cryptographie moderne repose maintenant uniquement sur les mathématiques. De plus, les règles de bases sont :

- ✓ L'algorithme utilisé n'est pas secret. Il peut être diffusé librement, cela ne doit avoir aucun impact sur la facilité ou non à déchiffrer le message.
- ✓ La clé de chiffrage utilisée est secrète.

Un protocole cryptographique basé sur la non-divulgation de l'algorithme mathématique utilisé n'est pas fiable. Tôt ou tard, l'algorithme utilisé sera connu et le protocole deviendra faible. Au contraire, diffuser l'algorithme mathématique utilisé permet à la communauté de valider et de tester la robustesse de cet algorithme.

II.3.1 Historique de la cryptographie moderne [13]

Pendant de nombreuses années, la cryptographie était exclusivement réservée au domaine militaire et diplomatique. La littérature sur le sujet était donc très peu abondante. La première publication fondamentale dans le domaine a été l'article de Claude Shannon 1949/ « the communication theory of secrecy systems ».Dans lequel il jette les bases mathématiques d'un système de communication chiffrée, à partir de la définition d'un nouveau modèle : L a théorie de l'information. Une contribution importante a été ensuite celle de feistel, avec la publication au débit des année 1970 de ses travaux sur les schémas de chiffrement itératifs par blocs qui ont conduit en 1977 ans la proposition de l'algorithme DES comme standard de chiffrement à clé secrète l'accroissement de la sécurité du DES.

L'accroissement de la puissance des ordinateurs ayant remis en cause de la sécurité du DES, il a été remplacé en 2000 par un nouveau standard appelé AES. Cet algorithme est l'aboutissement de recherches récentes notamment dans le domaine de la cryptanalyse. En 1976, après la publication par Diffie et Hellman de l'article : « New Direction in Cryptography », un nouveau concept révolutionnaire de la cryptographie, qu'est la cryptographie à clé publique, a été introduit.

Plus récemment pour faire face aux nouvelles menaces par le développement des réseaux et la numérisation massive des documents, la cryptographie a dû offrir de nouvelles fonctionnalités : garantie de l'authenticité des messages (provenance et contenu), réalisé par les algorithmes de signature numérique.

Ainsi, la cryptographie moderne offre deux grandes catégories de procédés cryptographiques :

- Algorithmes de chiffrement : servent à protéger la confidentialité des données.
- Algorithmes de signatures : garantissent la provenance et l'intégrité des messages.

II.3.2 Chiffrement [14]

Un algorithme de chiffrement transforme un message, appelé texte clair, en un texte chiffré qui ne sera lisible que par son destinataire légitime. Cette transformation est effectuée par une fonction de chiffrement paramétrée par une clé de chiffrement. Un interlocuteur peut alors

déchiffrer le message en utilisant la fonction de déchiffrement s'il connait la clef de déchiffrement correspondant. Un tel système n'est sur que s'il est impossible à un intrus de déduire le texte clair du message chiffré.

II.3.2.1 Différents modes de chiffrements [15] [29]

Le mode de chiffrement correspond à la manière dont on va utiliser un algorithme de chiffrement donné. Ce mode de chiffrement consiste par exemple à rajouter de la contre-réaction entre l'entrée et la sortie de l'algorithme afin de lui rajouter des caractéristiques bien précises. Les différentes modes de chiffrement utilisés sont les suivants :

- ✓ Le mode ECB pour **Electronic Code Book**
- ✓ Le mode CBC pour **Cipher Block Chaining**
- ✓ Le mode **chiffrement en continu**
- ✓ Le mode CTAK pour **Cipher Text Auto Key**
- ✓ Le mode CFB pour **Cipher Feed Back**
- ✓ Le mode KAK pour **Key Auto Key**
- ✓ Le mode OFB pour **Output Feed Back**
- ✓ Le mode CTR pour **CounTeR**
- ✓ Le mode BC pour **Block Chaining**
- ✓ Le mode PCBC pour **Propagating Cipher Block Chaining**
- ✓ Le mode CBCC pour **Ciher Block Chaining with Checksum**
- ✓ Le mode OFBNLF pour **Output Feed Back mode with a Non Linear Function**
- ✓ Le mode PBC pour **Plaintext Block Chaining**
- ✓ Le mode PFB pour **Plaintext Feed Back**
- ✓ Le mode CBCPD pour **Cipher Block Chaining of Plaintext Difference**
- ✓ Le mode CTS pour **Cipher Text Stealing**

Dans les paragraphes suivants nous allons regarder un peu plus en détail les modes ECB, CBC, CFB et OFB. Les autres modes sont nommés à des fins d'exhaustivité mais sont rarement utilisés.

a. Mode ECB

Ce mode est le plus simple : un même bloc est toujours codé de la même manière. Il n'y a pas de rétroaction de l'entrée ou de la sortie sur la fonction de chiffrement.

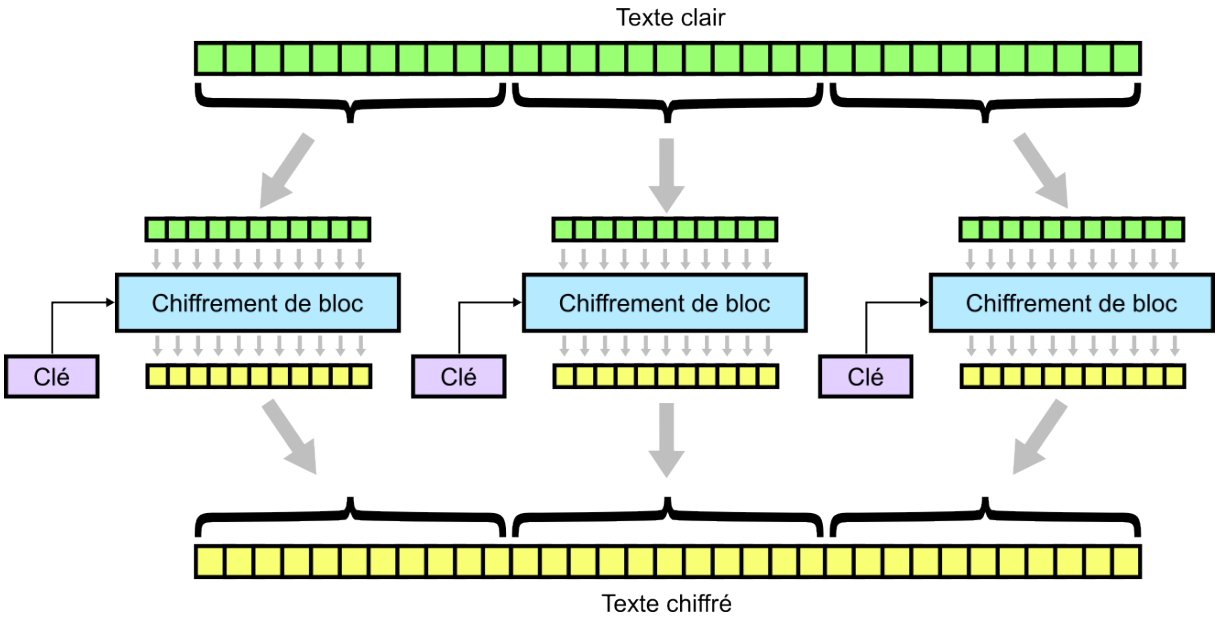


Figure II.4 Mode ECB

Les avantages de ce mode sont les suivants :

- ✓ Le travail de chiffrement ou de déchiffrement peut être parallélisé. Plusieurs machines ou CPU peuvent travailler simultanément sur des parties différentes du message.
- ✓ Une erreur de transmission d'un bit affecte uniquement le décodage du bloc courant.

Par contre, ce mode a les désavantages suivants :

- ✓ Les répétitions du texte en clair ne sont pas masquées et se retrouvent sous la forme de répétitions de textes chiffrés.
- ✓ Des portions complètes du message peuvent être modifiées, répétées ou remplacées sans difficulté.

b. Mode CBC

Dans ce mode de chiffrement, chaque bloc de texte en clair est d'abord combiné par un ou exclusif avec le dernier bloc du texte chiffré. La sortie de ce ou exclusif est ensuite appliquée à la fonction de chiffrement.

Ce mode de chiffrement dispose en plus d'un vecteur d'initialisation appelée IV (pour Initialisation Vector) qui permet d'initialiser le processus quand aucun bloc n'a encore été chiffré.

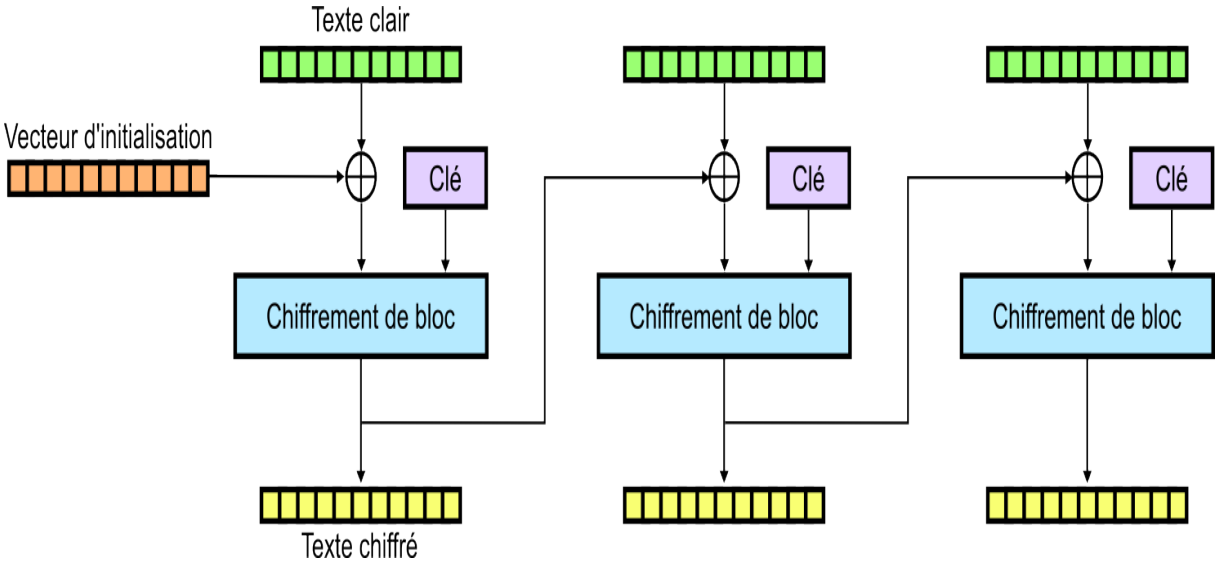


Figure II.5 Mode CBC

Les avantages de ce mode sont les suivants :

- ✓ Les répétitions de texte en clair sont masquées dans le texte chiffré.
- ✓ La valeur du vecteur d'initialisation IV n'a pas besoin d'être secrète.

Par contre, ce mode a les désavantages suivants :

- ✓ Deux textes en clair commençant pareil auront le même début de texte chiffré.
- ✓ Une erreur de transmission d'un bit affecte uniquement le décodage du bloc courant ainsi que le décodage du même bit dans le bloc suivant.

c. Mode CFB

Les modes ECB et CBC travaillent sur des blocs de texte en clair (64 bits par exemple). Ces modes ne sont pas utilisables que lorsqu'un bloc est complet. Sur des applications réseau, cela peut poser des problèmes car les valeurs à chiffrer arrivent sous forme d'octets et doivent être transmises immédiatement.

Ce mode dispose d'un vecteur d'initialisation qui a la même fonctionnalité que celui du CBC. L'octet du texte chiffré est combiné par un ou exclusif avec l'octet de texte en clair. Le résultat de cette opération est alors transmis en même temps qu'il est injecté dans la fonction de chiffrement.

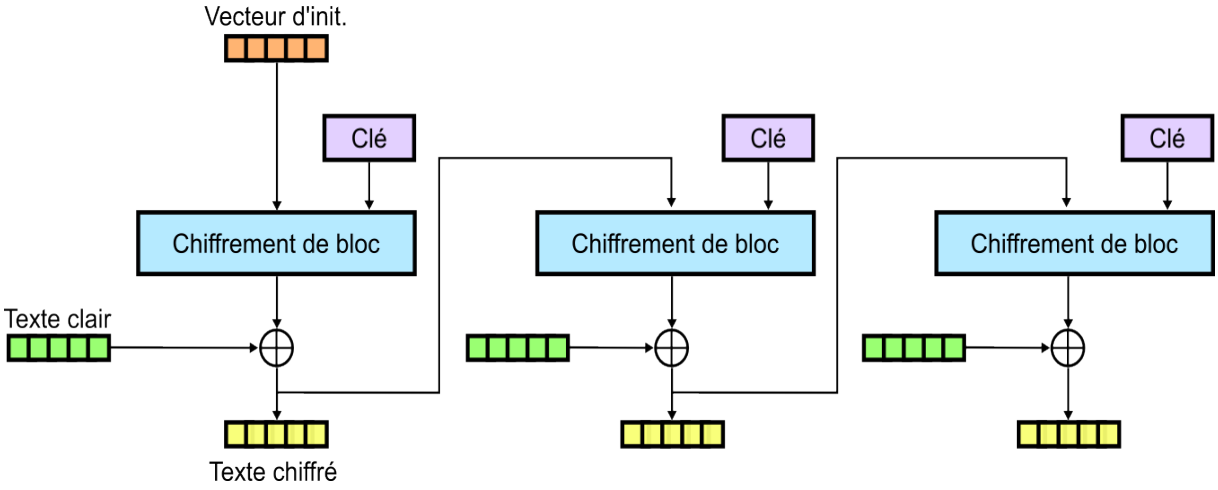


Figure II.6 Mode CFB

Les avantages de ce mode sont les suivants :

- ✓ Il est possible de chiffrer un flot de valeurs plus petites que la taille standard du bloc géré par l'algorithme.
- ✓ Les répétitions de texte en clair sont masquées dans le texte chiffré.
- ✓ La valeur du vecteur d'initialisation IV n'a pas besoin d'être secrète.

Par contre, ce mode a le désavantage suivant :

- ✓ Une erreur de transmission d'un bit affecte uniquement le décodage du bloc courant ainsi que le décodage du même bit dans le bloc suivant.

d. Mode OFB

Le mode OFB ressemble au mode CFB. La seule différence est que l'octet injecté dans la fonction de chiffrement vient du chiffrement successif du vecteur d'initialisation.

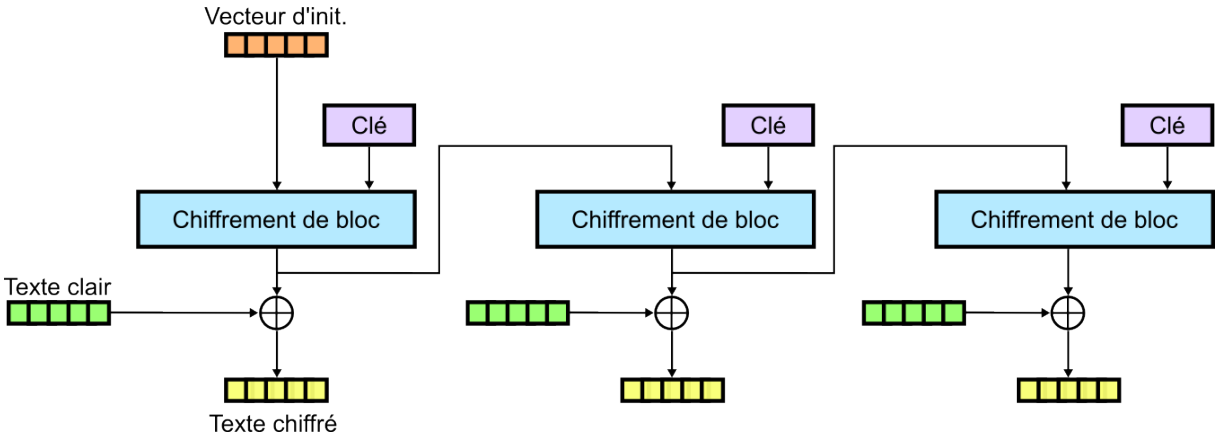


Figure II.7 Mode OFB

Les avantages de ce mode sont les suivants :

- ✓ Les répétitions de texte en clair sont masquées dans le texte chiffré.
- ✓ La valeur du vecteur d'initialisation IV n'a pas besoin d'être secrète.
- ✓ Ce mode n'amplifie pas les erreurs. Une erreur de transmission d'un bit affecte uniquement ce bit lors du décodage.

Par contre, ce mode a le désavantage suivant :

- ✓ Ce mode est très fragile vis-à-vis d'une attaque au clair. (l'attaquant possède des textes clairs ainsi que leurs versions chiffrées et est libre de les utiliser pour révéler d'autres informations secrètes comme la clé de chiffrement).

II.3.2.2 Cryptographie symétrique et asymétrique [16][17]

a. Cryptographie Symétrique

La cryptographie symétrique aussi nommée à clé secrète utilise la même clef pour chiffrer et déchiffrer un message. L'émetteur et le récepteur doivent se mettre d'accord sur une clé à utiliser et gardée secrète.

Les algorithmes à clé secrète étaient utilisés dans le domaine militaire. Ils servaient à protéger la confidentialité des messages entre leurs émetteurs et leurs destinataires. Dans un premier temps, la transformation d'un message clair en un message crypté passait par des procédures secrètes comme le montre la figure Fig. II.8. Un des premiers exemples de cette cryptographie symétrique est le chiffrement de César.

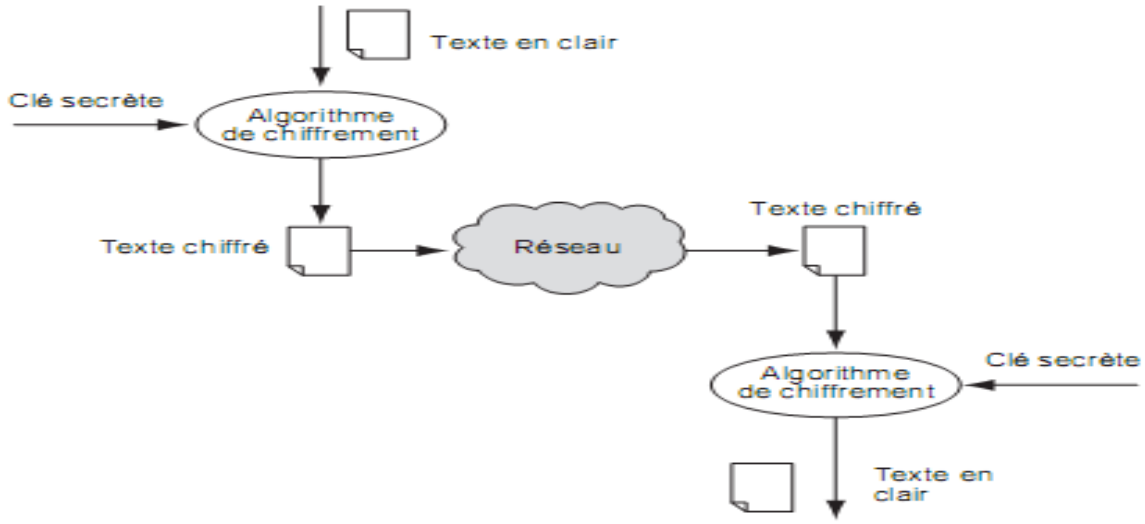


Figure II.8 Algorithme de chiffrement symétrique

Ces algorithmes fonctionnent habituellement suivant deux procédés différents, le chiffrement par blocs et le chiffrement par flot (en continu).

- ✓ **Chiffrement par flot :** le chiffrement est effectué bit-à-bit sans attendre la réception complète des données à chiffrer. Une technique de chiffrement, du nom de "One-Time Pad"(chiffrement de vernam) est utilisée pour chiffrer les flux (chiffrement de vernam).
- ✓ **Chiffrement par blocs** : opèrent sur le message en clair par groupes de bits (blocs). Il existe plusieurs algorithmes qui fonctionnent sur ce principe par exemple le DES (Data Encryption Standard) qui est l'algorithme à clé symétrique historiquement le plus connu.

b. Cryptographie asymétrique

Le principe des algorithmes de chiffrement à clés asymétriques a été introduit en 1976 par Diffie et Hellman. Ils ont été conçus pour utiliser des clés qui possèdent 2 propriétés essentielles :

- Les clés sont crées par couple souvent appelé bi-clé. Ce bi-clé est tel que tout texte chiffré par l'une quelconque des deux clés n'est déchiffrable que par l'autre clé. C'est cette caractéristique qui a donné leur nom aux algorithmes de chiffrement asymétrique
- La connaissance d'une des deux clés ne permet pas de déduire l'autre. En pratique, chaque protagoniste dispose d'un bi-clé (au moins un). On décide arbitrairement, pour chaque bi-clé, que l'une des clés est publique et l'autre privée

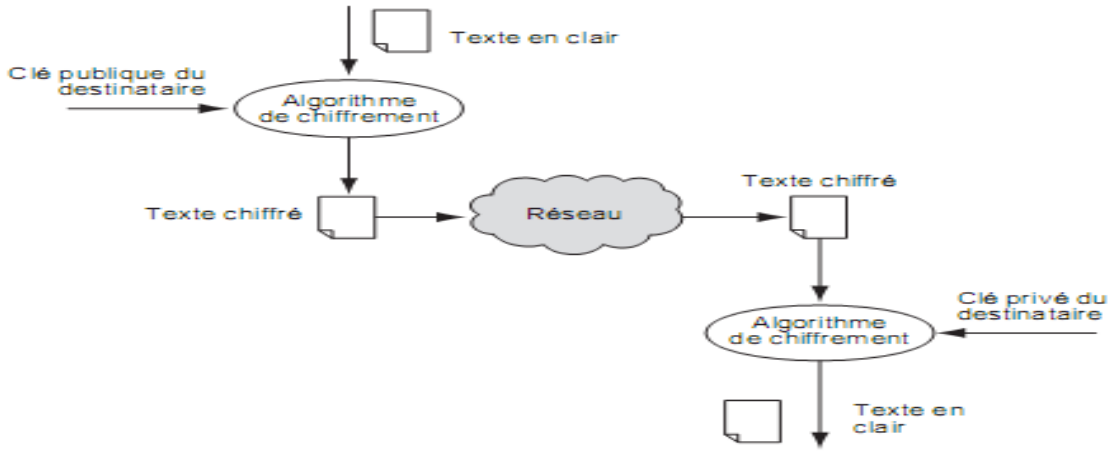


Figure II.9 Algorithme de chiffrement asymétrique

Algorithme RSA

RSA, du nom de ces inventeurs, est un algorithme de chiffrement appartenant à la grande famille "Cryptographie asymétrique".

RSA peut être utilisé pour assurer :

- ✓ la confidentialité : seul le propriétaire de la clé privée pourra lire le message chiffré avec la clé publique correspondante.
- ✓ la non-altération et la non-répudiation : seul le propriétaire de la clé privée peut signer un message (avec la clé privée). Une signature déchiffrée avec la clé publique prouvera donc l'authenticité du message.

Sa robustesse réside dans la difficulté à factoriser un grand nombre.

Principe de fonctionnement de RSA :

Si Bob souhaite recevoir des messages en utilisant le RSA, il procède de la façon suivante :

- ✓ **Création des clés :** Bob crée 4 nombres p,q, e et d :
  - p et q sont deux grands nombres premiers distincts. Leur génération se fait au hasard, en utilisant un algorithme de test de primalité probabiliste.
  - e est un entier premier avec le produit (p-1)(q-1).
  - d est tel que ed=1 modulo (p-1)(q-1). Autrement dit, ed-1 est un multiple de (p-1)(q-1). On peut fabriquer d à partir de e, p et q, en utilisant l'algorithme d'Euclide.
- ✓ **Distribution des clés :** Le couple (n,e) constitue la clé publique de Bob. Il la rend disponible par exemple en la mettant dans un annuaire. Le couple (n,d) constitue sa clé privée. Il la garde secrète.
- ✓ **Envoi du message codé :** Alice veut envoyer un message codé à Bob. Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. Alice possède la clé publique (n,e) de Bob. Elle calcule $C=M^e \bmod n$. C'est ce dernier nombre qu'elle envoie à Bob.
- ✓ **Réception du message codé** : Bob reçoit C, et il calcule grâce à sa clé privée $D=C^d \pmod n$. D'après un théorème du mathématicien Euler, $D=M^{de}=M \pmod n$. Il a donc reconstitué le message initial.

II.4 Signature numérique (signature électronique)

Le chiffrement permet de rendre les services de confidentialité. La signature électronique va permettre de garantir l'authentification de l'origine d'un document ou d'un message électronique et son intégrité. Ceci implique un certain nombre de propriétés :

- ✓ une signature ne peut être falsifiée,
- ✓ une signature donnée n'est pas réutilisable par un autre document
- ✓ la modification d'un document signé altère la signature de ce document
- ✓ une signature ne peut être reniée

Pour générer une signature électronique il faut dans un premier temps utiliser une fonction de hachage.

II.5 Fonction de hachage [30] [18]

La fonction de hachage est une fonction permettant d'obtenir un condensé (condensat ou haché) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense. Ces fonctions peuvent fournir une assurance de l'intégrité de données. Elle est utilisée pour construire une courte « empreinte numérique» de ces données ; si elles sont modifiées, l'empreinte numérique ne sera plus valide.

Une fonction de hachage H de taille de sortie n est un algorithme faisant correspondre à un message M de taille arbitraire un élément H(M) de taille n bits appelé haché. En pratique, n est de l'ordre de plusieurs centaines de bits, typiquement 128, 160, 256 ou 512 bits.

II.5.1 Propriétés de fonction de hachage

Les fonctions de hachage doivent posséder plusieurs propriétés utiles en cryptographie. Les principales sont la résistance aux attaques recherchant des collisions, des préimages ou des secondes préimages.

- ✓ **collision** : trouver deux messages distincts M1 et M2, tels que H(M1) = H(M2).
- ✓ **seconde préimage** : étant donné un message M1 choisi aléatoirement, trouver un message distinct M2 tel que H(M1) = H(M2).
- ✓ **préimage** : étant donné un haché H1 choisi aléatoirement, trouver un message M1 tel que H(M1) = H1.

Il doit être impossible pour un attaquant de trouver une collision, une pré-image ou une seconde pré-image.

II.5.2 Présentation des fonctions de la famille MD-SHA [18]

II.5.2.1 MD4 (Message Digest 4)

MD4, pour *Message Digest 4*, est un algorithme de hachage conçu par le professeur Ronald Rivest du Massachusetts Institute of Technology en 1990. La taille de la signature est de 128 bits. L'algorithme a été abandonné au profit du MD5 après la découverte de faiblesses dans sa conception (Den Boer et Bosselaers). D'autres attaques encore plus efficaces ont suivi, notamment par Hans Dobbertin du service du chiffre allemand et l'équipe chinoise à l'origine de l'attaque sur MD5 (Wang *et al.*). À ce titre, le MD4 ne peut en aucun cas être considéré comme cryptographiquement sûr puisque des collisions peuvent être générées avec un nombre d'opérations de l'ordre de 2^8 opérations . Cette magnitude est très faible en comparaison des 2^{64} nécessaires pour un paradoxe des anniversaires.

II.5.2.2 MD5 (Message Digest 5)

MD5 est une fonction de hachage cryptographique qui permet d'obtenir pour chaque message une empreinte numérique (en l'occurrence une séquence de 128 bits) avec une probabilité très forte que, pour deux messages différents, leurs empreintes soient différentes. En 1996, une faille grave (possibilité de créer des collisions à la demande) est découverte et indique que MD5 devrait être mis de côté au profit de fonctions plus robustes.

En 2004, une équipe chinoise découvre des collisions complètes. MD5 n'est donc plus considéré comme sûr au sens cryptographique. Leur attaque a permis de découvrir une collision complète sans passer par une méthode de type brute-force. La sécurité du MD5 n'étant plus garantie selon sa définition cryptographique, les spécialistes recommandent d'utiliser des fonctions de hachage plus récentes comme le SHA-256.

MD5 reste encore très utilisé comme outil de vérification lors des téléchargements. Les sites affichent encore souvent la signature en MD5 (128 bits) de leurs fichiers, bien que SHA-1 (160 bits) le remplace de plus en plus.

II.5.2.3 SHA-1 (Secure Hash Algorithm 1)

SHA-1 (*Secure Hash Algorithm*) est une fonction de hachage cryptographique conçue par la *National Security Agency* des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information (*Federal Information Processing Standard* du *National Institute of Standards and Technology* (NIST)). Elle produit un résultat (appelé « *hash* » ou *condensat*) de 160 bits.

II.5.2.4 SHA-2 (Secure Hash Algorithm 2)

SHA-2 est une famille de fonctions de hachage cryptographiques qui regroupe SHA-224, SHA-256, SHA-384 et SHA-512 publiée en 2001. Celles-ci produisent des hachés de taille différente (celle-ci est désignée par le suffixe, en bits). Le standard FIPS-180-4 (mars 2012) est augmenté de deux versions tronquées de SHA-512, SHA-512/256 (haché de 256 bits) et SHA-512/224 (haché de 224 bits). Elles utilisent des algorithmes très similaires, eux-mêmes largement inspirés de celui de SHA-1. L'un est à base de mots de 32 bits (et d'un découpage en blocs de 512 bits) pour SHA-256 et sa version tronquée SHA-224. L'autre est à base de mots de 64 bits (et d'un découpage en blocs de 1024 bits) pour SHA-512 et ses versions tronquées SHA-384, SHA-512/256 et SHA-512/224. Les attaques connues sur SHA-1 n'ont pu être transposées à SHA-2, même si la construction est proche.

II.6. Etude de l'existant

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation d'une solution informatique. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement. Cette étude consiste à mettre à découvert, de façon aussi claire que possible, l'analyse qualitative et quantitative du fonctionnement actuel du réseau informatique.

Par la suite on peut passer à une analyse, classer et donner une vue synthétique de l'ensemble des informations collectés sur le parc informatique (matériels et logiciels), la dimension du réseau (LAN : étages, bâtiments, salles, sites géographiques, diamètre du réseau, interconnexion, WAN, MAN). Enfin, on peut esquisser une modélisation à grande échelle des données ainsi obtenues.

L'état des lieux étant effectué, elle peut aboutir à une critique de l'existant qui analyse les ponts positifs et négatifs de l'environnement informatique déjà en place et dégager les améliorations à apporter : les tâches rendues et les tâches non rendues, les services rendus et les services non rendus, etc. cette critique sera ainsi un tremplin pour l'analyse des besoins. Cette analyse est en fait la nécessité ou le désir éprouvé(e) par un utilisateur. Ce besoin peut être explicite ou implicite, potentiel, avoué ou inavoué. Par conséquent, l'étude des besoins consiste à dégager les critères de migration vers la nouvelle solution ou de l'implémentation de celle-ci, à évaluer les divers avantages attendus (retour sur investissement). Elle est à réaliser sous forme de questionnaire. Cette étude donne une vue globale des besoins fonctionnels (les besoins qui expriment des actions qui doivent

être menées sur l'infrastructure à définir en réponse à des demandes) et techniques mais aussi des besoins des utilisateurs.

Ces études sont d'un atout important dans le choix des matériels qui constitueront la future infrastructure.

II.6.1. Architecture physique

Rappelons qu'un réseau informatique est un maillage de micro-ordinateurs interconnectés dans le but du partage des informations et du matériel redondant. Quelque soient le type de systèmes informatiques utilisés au sein d'une entreprise, leur interconnexion pour constituer un réseau est aujourd'hui obligatoire. La constitution de celui-ci passe par une conception qui consiste à définir :

- L'architecture physique si le réseau est inexistant, ou faire évoluer l'architecture le cas contraire. Il est abordé par la cartographie des sites, des bâtiments, des salles devant être connectés ; de même que les supports physiques et les équipements actifs.
- L'architecture logique autrement dit la topologie logique, elle fait référence à toutes les couches du réseau, les protocoles, le plan d'adressage, le routage.
- Utiliser les services des opérateurs ou des sous-traitants.
- La politique d'administration et de surveillance des équipements.
- Les services réseaux.
- Les outils de sécurité.
- La connexion avec l'extérieur : Internet.

II.6.2. Architecture logique

Afin de maintenir dans des limites raisonnables la localisation de tout problème dans un réseau dont l'ambition est initialement de connecter quelques ordinateurs, vous pouvez opter pour une architecture de réseaux routés. Ceci dans l'optique de limiter des collisions, des diffusions ou tout autre type de problèmes des réseaux partagés et surpeuplés. L'architecture logique nous permettra de trouver une solution après une analyse en termes de sous-réseaux, d'adressage IP en fonction de ces sous-réseaux, de plan d'adressage, du routage à implémenter dans le réseau.

II.6.2.1. Adressage IP

Une adresse IP est un numéro d'identification qui est attribué à chaque branchement d'appareil à un réseau informatique utilisant l'Internet Protocol. L'adresse IP est attribuée à chaque interface

avec le réseau de tout matériel informatique (routeur, ordinateur, modem ADSL, imprimante réseau, etc...) lorsqu'il fait partie du réseau informatique utilisant l'Internet Protocol comme protocole de communication entre ses nœuds. Cette adresse est assignée individuellement par l'administrateur du réseau local dans le sous-réseau correspondant, ou automatiquement via le protocole DHCP. Ainsi l'adressage peut être statique ou dynamique.

II.6.2.2. Plan d'adressage

Lorsque vous devez créer un réseau d'entreprise, ce réseau restreint à un site ou interconnectant différents sites de l'organisation, il est primordial de réfléchir à un plan d'adressage. Cette opération a pour but de définir pour chaque réseau physique (LAN et WAN) une adresse IP. Chaque ordinateur, chaque composant actif doit avoir un moyen d'être identifié sur le réseau. Pour cela, une adresse IP lui est attribuée. Il y a deux types d'adressage IP ; « privée » qui permet la communication inter-entreprise et « publique » utilisée pour la communication vers, ou depuis Internet. Un organisme spécialisé fournit les adresses IP

II.6.2.3. Routage

Les réseaux informatiques ont ceci d'intéressant: Ils couvrent des besoins aussi simples que la connexion entre deux hôtes sur un réseau local que l'interconnexion de systèmes à l'échelle planétaire (Internet). Internet et les réseaux IP sont composés d'un ensemble de réseaux reliés via des machines particulières que l'on appelle routeurs. Pour la communication au sein de ces réseaux, le protocole IP est capable de choisir un chemin (également appelé une route) suivant lequel les paquets de données seront relayés de proche en proche jusqu'au destinataire. C'est ainsi que le routage IP fonctionne de façon totalement décentralisée au niveau des machines qui constituent le réseau. Aucune n'a une vision globale de la route que prendront les paquets de données.

Le routage en lui-même est un processus par lequel des données transmises par un ordinateur d'un réseau sont acheminées vers leur destinataire qui est une machine d'un autre réseau.

II.7. Critique de l'existant

Une analyse du réseau d'une entreprise nous permis en général de définir un nombre de contraintes pouvant réduire ses performances voir sa dégradation ; et de plus certains de ces contraintes peuvent être un obstacle à la réalisation de la mission de l'entreprise :

- Trafic web important,
- Volume accru du trafic généré par chaque utilisateur,
- Accès non restreint aux données de l'administration,
- Libre accès au routeur (paramètres de configuration),
- Démotivation de certains professeurs,
- Conflit d'adressage IP.

II.8. Les services réseaux (DNS, DHCP, Messagerie, WEB,…)

Un service réseau est une fonctionnalité assurée par un ordinateur consistant en l'aptitude à la fourniture d'informations à d'autres ordinateurs via une connexion réseau normalisée. Les services réseaux se basent sur des protocoles pour fournir des fonctionnalités qui sont accessibles par l'utilisateur au niveau de la couche 7 du modèle OSI (couche application). Comme services réseaux, on peut implémenter le service de résolution de noms (machines : DNS), l'attribution d'adresse (DHCP), la messagerie, l'annuaire, le web, ...

II.9. Les critères de choix d'un firewall

Il n'existe pas de bon produit en soi. Il existe des produits qui ont un bon rapport qualité/prix, des produits qui répondent plus ou moins bien aux besoins spécifiques d'une entreprise et des produits qui s'intègrent plus ou moins bien dans l'existant. Avant de faire un choix de produit, il est nécessaire d'avoir connaissance des critères suivant pour effectuer le choix d'un firewall.

- ✓ La nature, le nombre des applications appréhendées (FTP, messagerie, HTTP, SNMP, Real Audio, vidéoconférence …).
- ✓ Le type de filtres, le niveau de filtrage (niveau applicatif, niveau TCP, niveau IP, possibilité de combiner ces niveaux).
- ✓ Les facilités d'enregistrement des actions à des fins d'audit, login, complet des paramètres de connexion, l'existence d'outils d'analyse, d'audit actif et détection d'activités suspectes.
- ✓ Les outils et facilités d'administration (interface graphique ou lignes de commandes, administration distante après authentification du gestionnaire …).
- ✓ La simplicité de système, proxy facile à comprendre et à vérifier (facilité de configuration).
- ✓ La capacité à supporter un tunnel chiffré permettant de réaliser, si nécessaire, un réseau privé virtuel (VPN).
- ✓ La disponibilité d'outils de surveillance, d'alarmes, d'audit actif.
- ✓ La possibilité d'effectuer de l'équilibrage de charge.

- ✓ L’existence dans l’organisation de compétences en matière d’administration du système d’exploitation du firewall.

II.10. Vulnérabilité et les attaques

Avec la libre circulation des informations et la haute disponibilité de nombreuses ressources, les responsables doivent connaître toutes les menaces successibles de compromettre la sécurité du fait de la vulnérabilité de leur réseau. Toute faiblesse dans un SI qui permet à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient est appelée une vulnérabilité. Au fil des années, la sécurité des SI devient un besoin absolue, alors même que la complexité de ces systèmes s'accroît, ils deviennent donc plus vulnérables aux menaces.

Les attaques (n'importe quelles actions qui compromettent la sécurité des informations) informatiques constituent aujourd'hui l'un des fléaux de notre civilisation moderne. Il est régulier de suivre que telle entreprise ou tel institut a essuyé de lourdes pertes financières en raison d'une défaillance de la sécurité de son système d'information. Par conséquent les entreprises ne peuvent pas ignorer ces risques et se croire à l'abri de telles épreuves sachant que les attaques ont des buts précis qui visent des mécanismes de sécurité précis très souvent implémentés dans les réseaux :

- ✓ Interruption d'un service : vise la disponibilité des informations,
- ✓ Interception des données : vise la confidentialité des informations,
- ✓ Modification des données : vise l'intégrité des informations,
- ✓ Fabrication des données : vise l'authenticité des informations.

II.11. Solution à la sécurité

La sécurité des SI fait très souvent l'objet de métaphores. L'on la compare régulièrement à une chaine en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue. Cela signifie qu'une solution de sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

- La sensibilisation des utilisateurs aux problèmes de sécurité ;
- La sécurité logique, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation ;

- La sécurité des télécommunications : technologies réseaux, serveurs de l'entreprise, réseaux d'accès, etc ;
- La sécurité physique, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, stations de travail des personnels, etc.

Etant donné les enjeux financiers qu'abritent les attaques, les SI se doivent de nos jours d'être protégés contre les anomalies de fonctionnement pouvant provenir soit d'une attitude intentionnellement malveillante d'un utilisateur, soit d'une faille rendant le système vulnérable.

Du fait du nombre croissant de personnes ayant accès ces systèmes par le billet d'Internet, la politique de sécurité se concentre généralement sur le point d'entrée du réseau interne. La mise en place d'un pare-feu est devenue indispensable à fin d'interdire l'accès aux paquets indésirables. On peut, de cette façon, proposer une vision restreinte du réseau interne vu de l'extérieur et filtrer les paquets en fonction de certaines caractéristiques telles qu'une adresse ou un port de communication. Bien que ce système soit une bastille, il demeure insuffisant s'il n'est pas accompagné d'autres protections, entre autres :

- La protection physique des informations par des accès contrôlés aux locaux,
- La protection contre les failles de configuration par des outils d'analyse automatique des vulnérabilités du système,
- La protection par des systèmes d'authentification fiables pour que les droits accordés à chacun soient clairement définis et respectés, ceci afin de garantir la confidentialité et l'intégrité des données.

Implémenter la sécurité sur les SI, consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible. Toujours est il que même en mettant en place tous ces mécanismes, il reste beaucoup de moyens pour contourner ces protections. A fin de les compléter, une surveillance permanente ou régulière des systèmes peut être mise en place à savoir:

- Les systèmes de détections d'intrusions ayant pour but d'analyser tout ou partit des actions effectuées sur le système afin de détecter d'éventuelles anomalies de fonctionnement.
- Utiliser le protocole HTTPs pour sécuriser des transactions HTTP adopté pour permettre une navigation sécurisée sur le web.
- L'utilisation des antivirus professionnels accompagnées de leurs mises à jour régulière.

- L'utilisation d'un serveur proxy dont le but est d'isoler une ou plusieurs machines pour les protéger. De plus le proxy possède un avantage supplémentaire en termes de performance.
- 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.

Conclusion

Dans ce chapitre, nous avons étudié les fondements de la cryptographie et son développement de temps classique au temps moderne, et aussi ses différents algorithmes nécessaires pour la protection des informations personnelles ou privés.

Nous détaillerons dans le chapitre qui va suivre le déroulement de l'application.

Chapitre III : Réalisation de la politique de sécurité

Introduction

Il reste difficile, voire impossible, d'assurer la sécurité des informations à 100%. Dont, cette dernier s'adresse pas seulement aux administrateurs systèmes et réseaux mais en général, toute personne appelée à participer en collaboration à la gestion de l'outil informatique dans ce contexte (chef d'entreprise, formateur...) les sensibilisé au secret professionnel.

Dans ce chapitre nous essaierons de trouver des solutions de sécurité de base afin que n'importe quelle PME peux l'adopté, pour garantir l'intégrité, la confidentialité, la disponibilité des données et des applications.

III.1. Présentation des outils utilisés

III .1.1. La VMware Workstation 10.0.1

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 10.0.1 Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web.

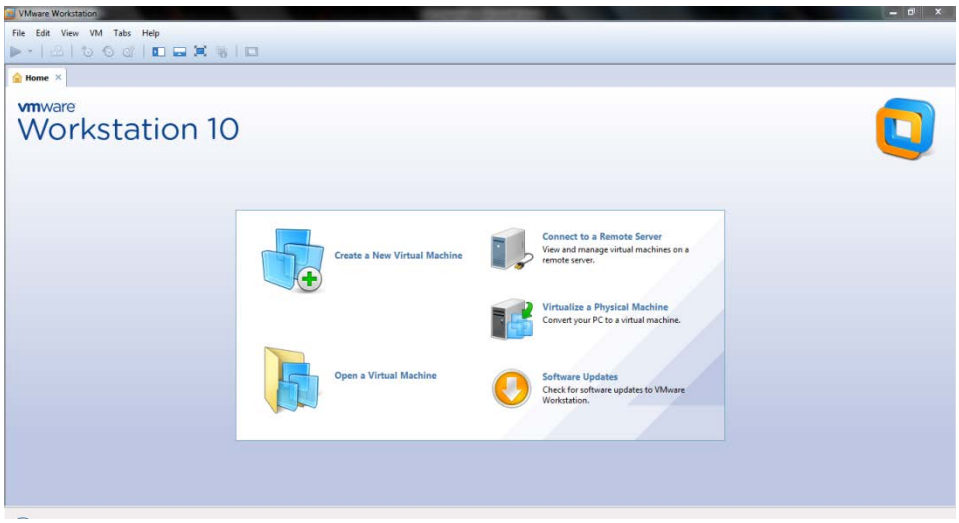


Figure III.1: VMware Workstation10.0.1

III. 1.2. Microsoft Windows Server 2008

Microsoft Windows Server 2008 est conçu pour fournir aux entreprises la plate-forme la plus productive pour virtualiser les charges de travail en utilisant la virtualisation Microsoft intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web.

Figure III.2: Windows server 2008

III.1.3. Microsoft Windows Server 2012 R2

Windows Server 2012 R2 offre une grande variété de fonctionnalités nouvelles et améliorées couvrant la virtualisation de serveurs, le stockage, le réseau défini par les logiciels, la gestion et l'automatisation des serveurs, les plateformes d'application et Web, la protection de l'accès et des informations, l'infrastructure VDI (Virtual Desktop Infrastructure) et bien plus encore.

Figure III.3: Windows Server 2012 R2

III.1.4. Active directory

Pour réaliser la gestion des objets sans liens avec la disposition réelle des protocoles réseaux employés, nous avons utilisé Active Directory qui est un annuaire des objets du réseau. Il permet aux utilisateurs de localiser, gérer et utiliser facilement les ressources, en organisant l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets. Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants de façon complètement centralisée.

Figure III.4: Active Directory.

III.1.5. Les caractéristiques du PC utilisé

Vu que notre application exige des ressources matérielles, l'utilisation d'un PC afin regrouper les solutions proposées, réseaux et systèmes. Les caractéristiques du PC portable professionnel utilisé sont :

- ✓ Processeur I3 x64 bits
- ✓ RAM 6Go
- ✓ Disque dur 300 G
- ✓ Système Windows 7 Edition Integrale x64 bits
- ✓ Prise en charge de la virtualisation.

III.2. Les étapes suivies pour la mise en place de notre application

Vu qu'il est impossible d'implémenter toute l'infrastructure réseau pour l'entreprise de base (entreprise virtuelle) avec les solutions réseaux et systèmes proposées. Nous l'avons

simplifié de sorte à permettre la mise en place de notre politique de sécurité basique pour n'importe qu'elle PME.

Etape I : La préparation des machines

Nous avons préparé les machines suivantes :

- ✓ Une autorité de certification. (WS 2012)
- ✓ Un contrôleur de domaine. (WS 2012)
- ✓ Un serveur membre pour l'installation de la TMG. (WS 2008)
- ✓ Un serveur membre pour l'installation de Microsoft Exchange Server 2013. (WS 2012)
- ✓ Un serveur membre pour l'installation de serveur Web. (WS 2008)

Etape II: Installation et configuration de l'autorité de certification racine

1. Installation de l'autorité de certification (CA)

Dans notre cas et comme la plupart des organisations, une autorité de certification racine est le premier service de rôle des services de certificats Active Directory (AD CS) installé.

On va installer une seule autorité de certification déployée, c'est l'autorité de certification racine qui établit les fondati+ons et règles de base qui régissent l'émission de certificat et l'utilisation de toute infrastructure à clé publique. Notre autorité de certification racine est une autorité de certification autonome.

Une fois l'autorité de certification racine traite la demande de certificat par le domaine contrôleur principal l'exposition de l'autorité de certification va être minimisé en la conservant hors connexion.

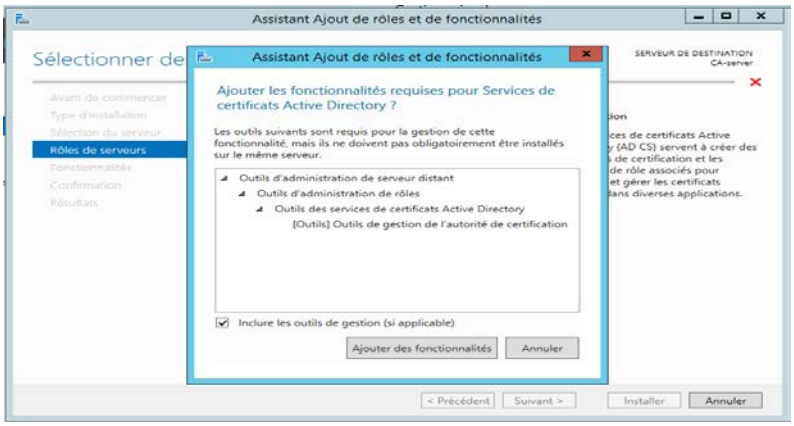


Figure III.5: Installation d'AD CS

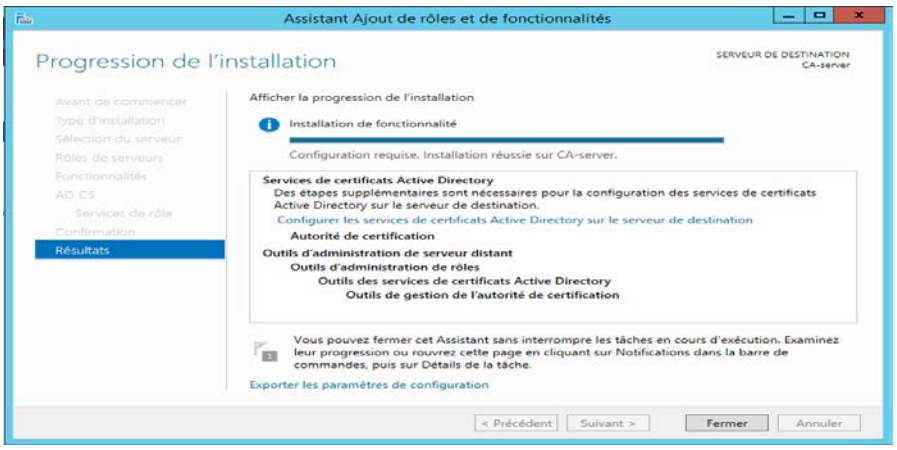


Figure III.6: Fin d'installation d'AD CS pour CA

2. Configuration de l'autorité de certification (CA)

Ci-dessous, la premier figure on configure l'autorité de certification comme étant CA autonome, la deuxième figure on choisi le type de l'autorité de certification dans notre cas est racine.

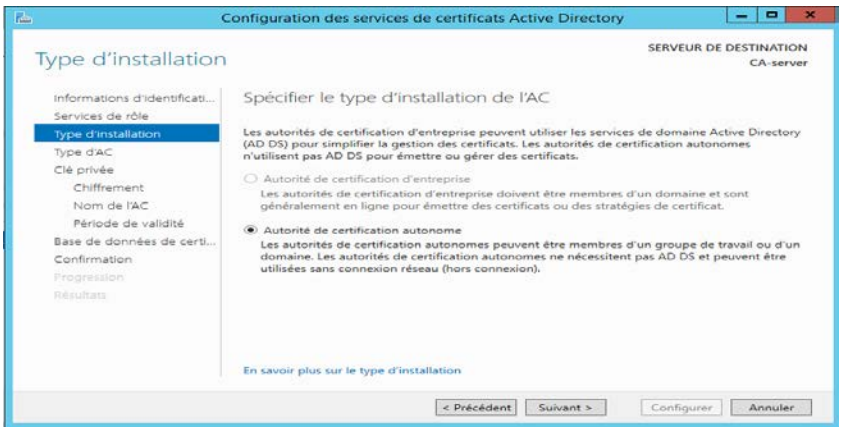


Figure III.7: CA autonome

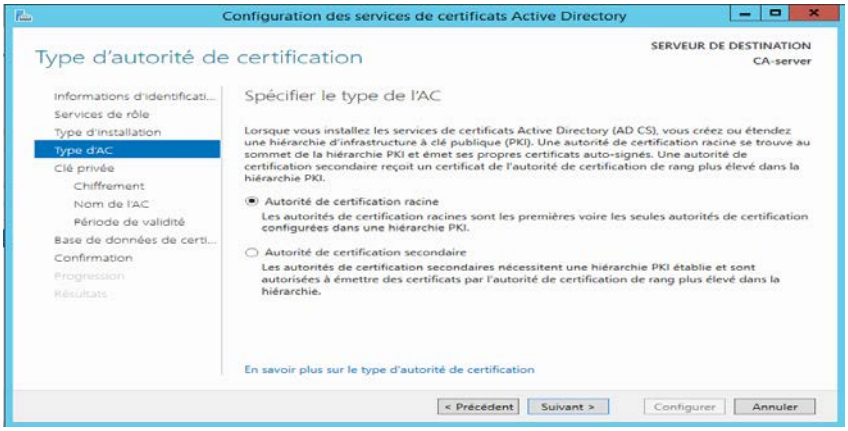


Figure III.8: CA racine

Dans l'annexe A, vous trouvez l'installation de différents rôles et fonctionnalités de l'autorité de certification racine.

Etape III: Installation et configuration du domaine contrôleur principale

1. Installation du domaine contrôleur principale (PDC)

Après l'installation du service Active Directory pour le serveur domaine contrôleur principal montrer dans la première figure, la deuxième montre sa création. L'installation du service AD DS et DNS est en même temps. Dans l'annexe B vous trouvez les différentes étapes mener à l'installation et la configuration de l'Active Directory.

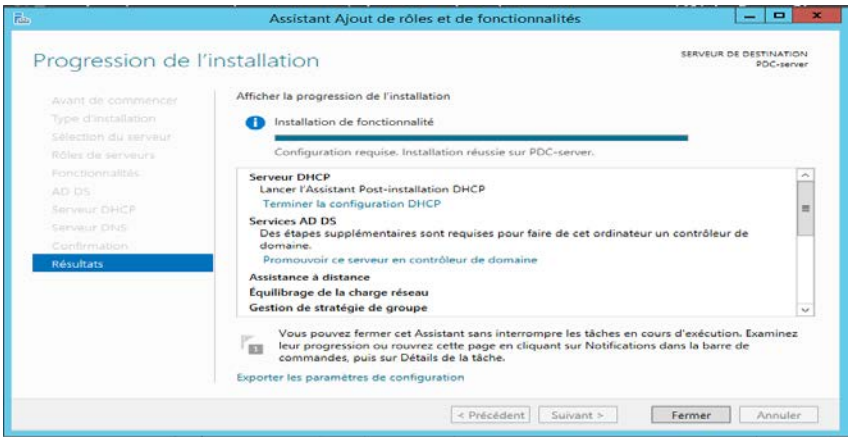


Figure III.9: Fin d'installation d'AD DS pour PDC

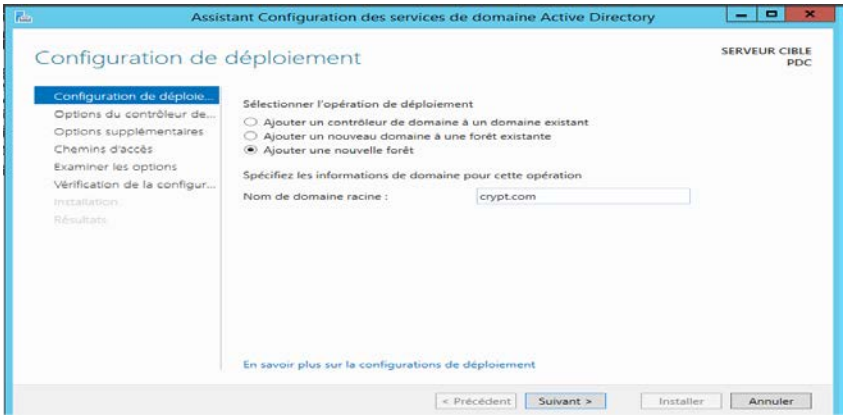


Figure III.10: Création du domaine contrôleur principal

Après le redémarrage du serveur PDC, la figure suivante nous montre comment accéder au domaine créé.

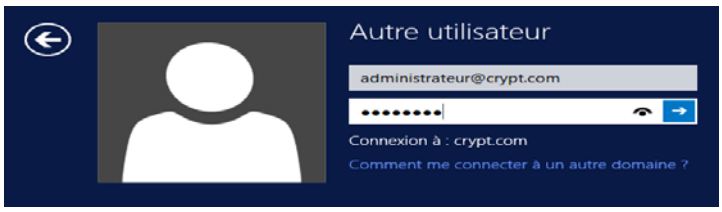


Figure III.11: Accès au domaine

2. L'ajout d'un serveur ou machine membre

Un serveur ou une machine membre ne sont pas des contrôleurs de domaine mais seulement des membres du domaine. Pour ajouter un membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur comme le montre la figure suivante :

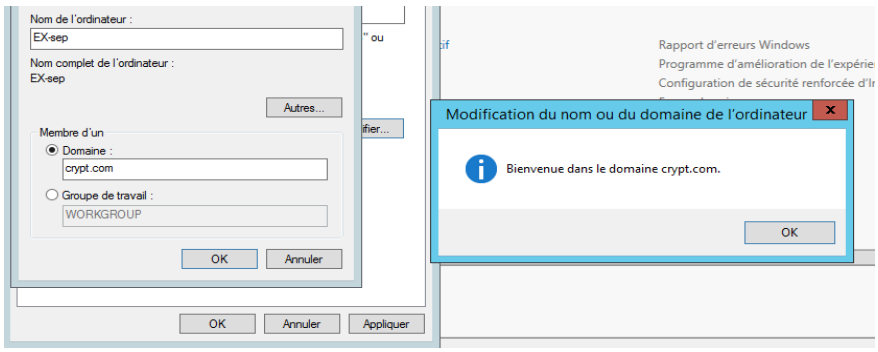


Figure III.12: ajout d'une machine au domaine

3. Installation des rôles et fonctionnalités pour le domaine contrôleur principal

3.1. Installation du serveur DHCP

Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les paramètres tels que (serveur de noms, passerelle par défaut, nom du réseau), le serveur DHCP alloue à un client, un bail d'accès au réseau, pour une durée déterminée (durée du bail). Le serveur passe en paramètres au client toutes les informations dont il a besoin.

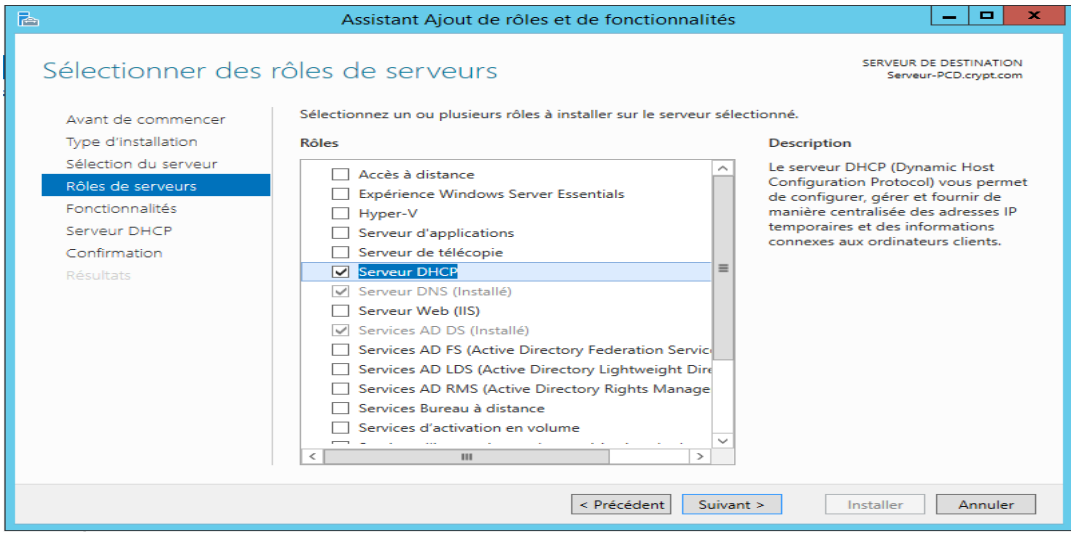


Figure III.13: Installation du serveur DHCP

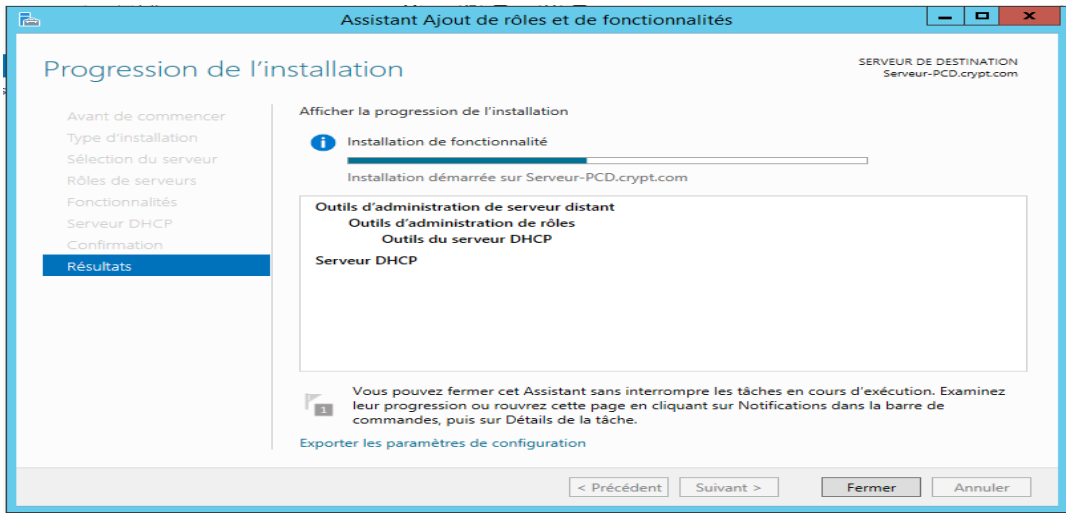


Figure III.14: Lancement de l'installation du serveur DHCP

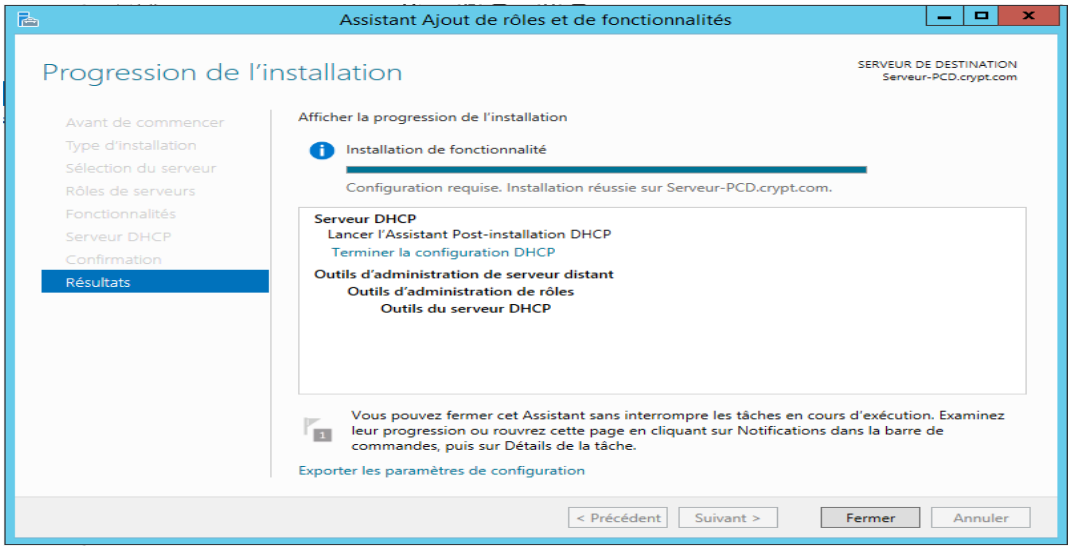


Figure III.15: Fin d'installation du serveur DHCP

3.2. Configuration d'une étendue DHCP

Une étendue est un groupement administratif des adresses IP des ordinateurs d'un sous-réseau qui utilisent le service DHCP. L'administrateur crée d'abord une étendue pour chaque sous-réseau physique, puis utilise l'étendue pour définir les paramètres utilisés par les clients. Une étendue possède les propriétés suivantes :

- une plage d'adresses IP où inclure ou exclure les adresses utilisées pour les offres de bail de service DHCP.
- un masque de sous-réseau, qui détermine le sous-réseau correspondant à une adresse IP spécifique.
- un nom d'étendue.
- des valeurs de durée de bail, qui sont affectées aux clients DHCP recevant des adresses IP allouées de manière dynamique.
- des options d'étendue DHCP configurées pour être affectées aux clients DHCP, telles qu'un serveur DNS, l'adresse IP d'un routeur et l'adresse d'un serveur WINS.
- des réservations, utilisées de manière optionnelle pour s'assurer qu'un client DHCP reçoit toujours la même adresse IP.

Les figures qui suivent montrent les étapes conçus pour configurer une étendue DHCP ou bien pool d'adressage.

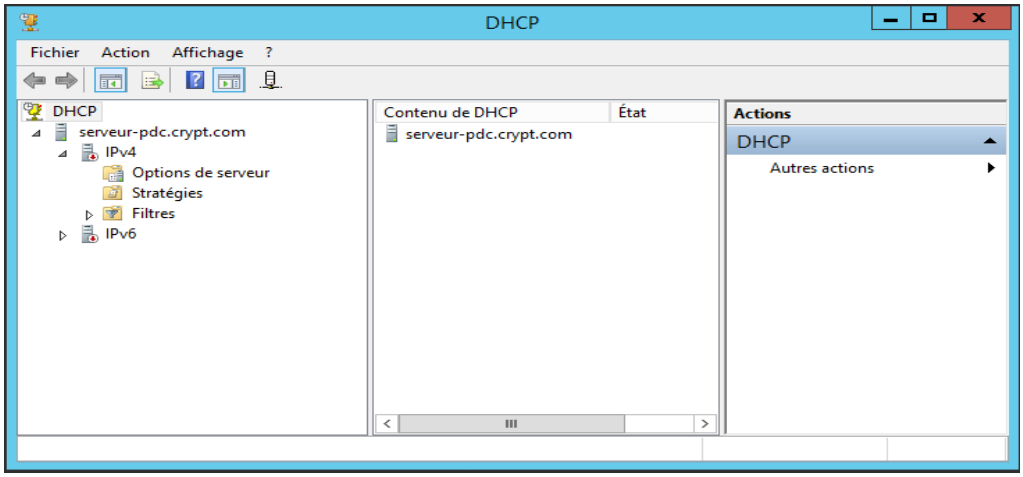


Figure III.16: Interface du serveur DHCP

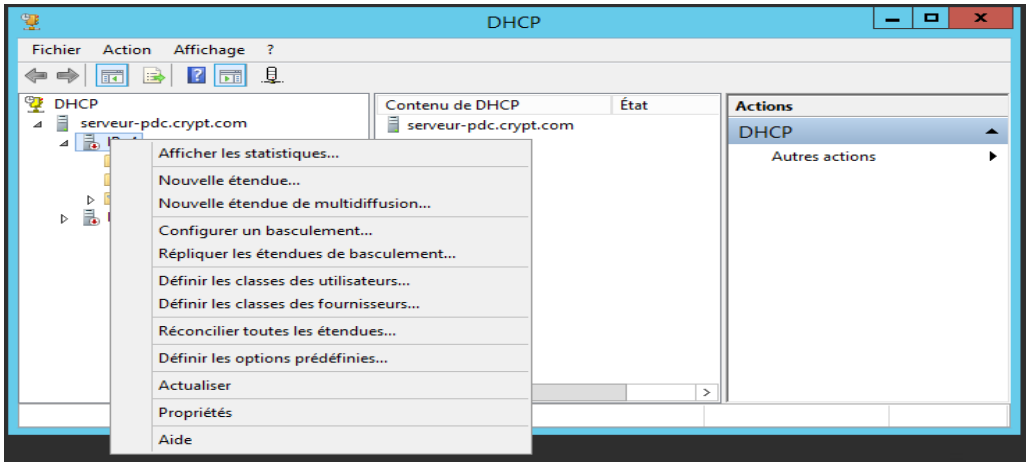


Figure III.17: Une nouvelle étendue

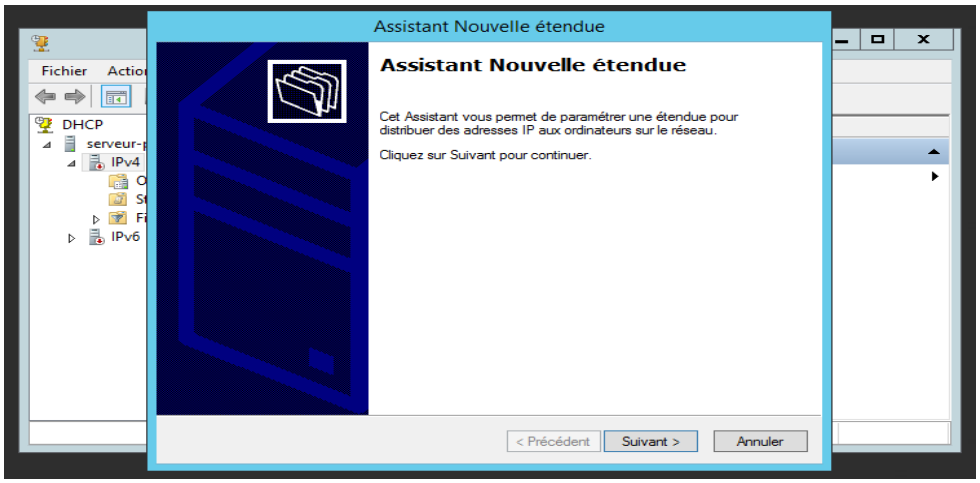


Figure III.18: Assistant nouvelle étendue

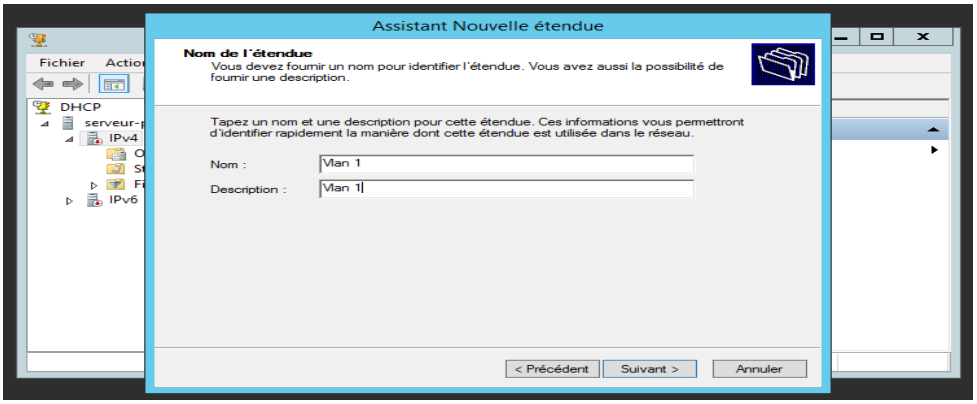


Figure III.19: Nom de l'étendue

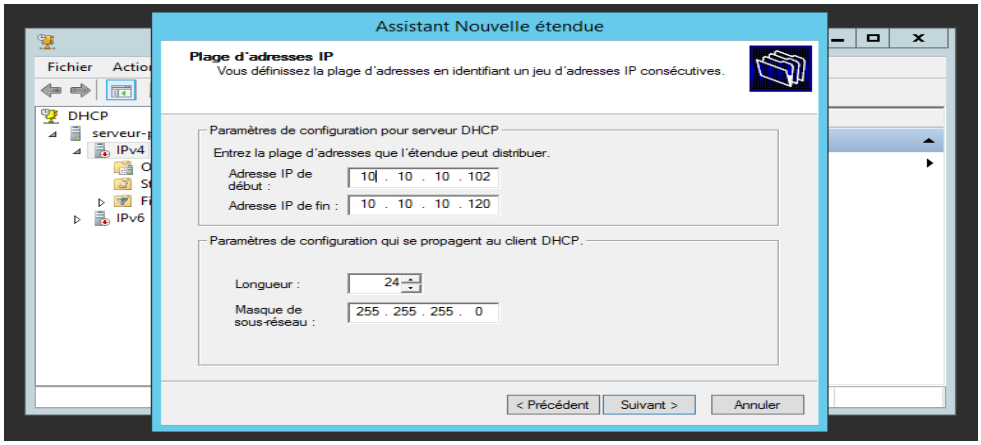


Figure III.20: Plage d'adresse IP

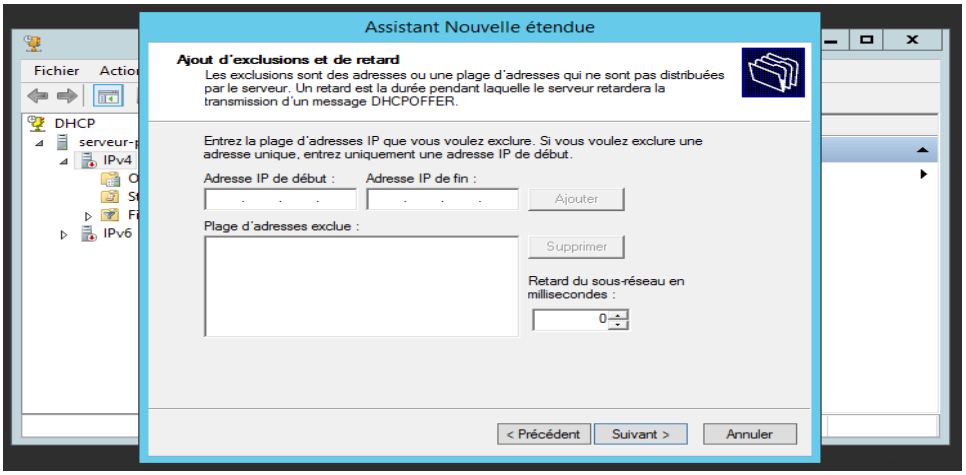


Figure III.21: Ajout des exclusions

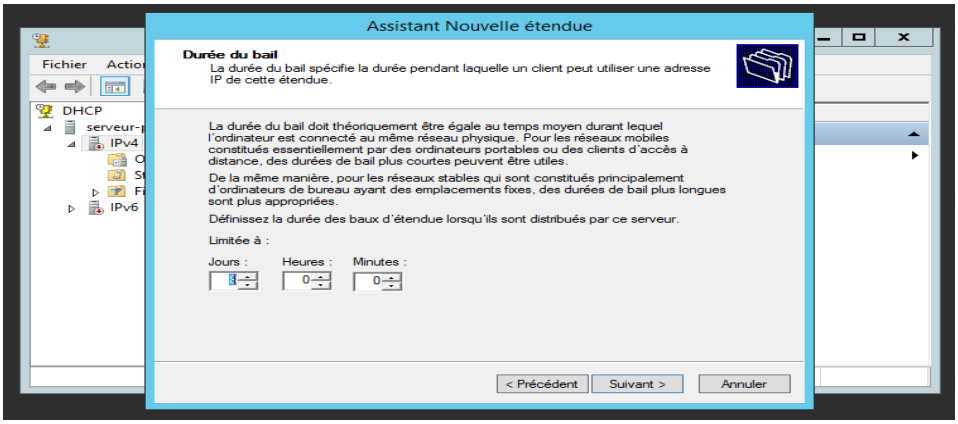


Figure III.22: Durée du bail

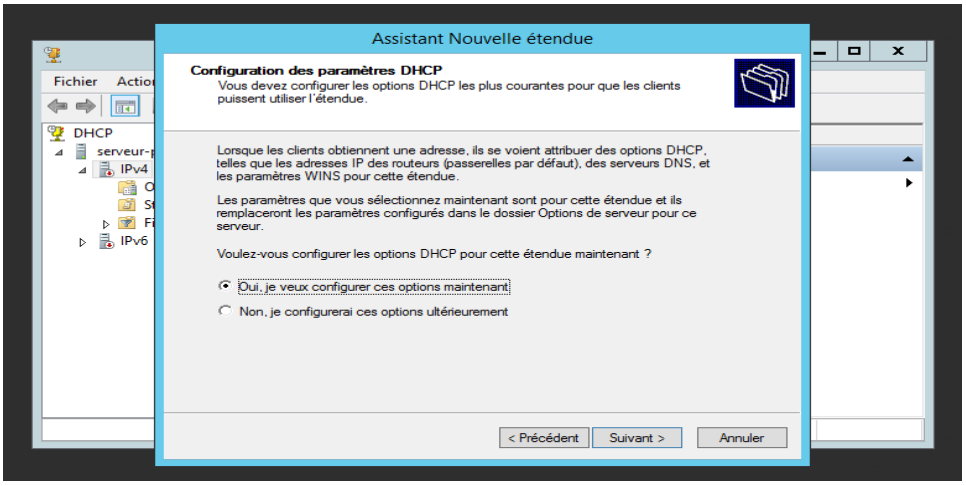


Figure III.23: Configuration des paramètres DHCP

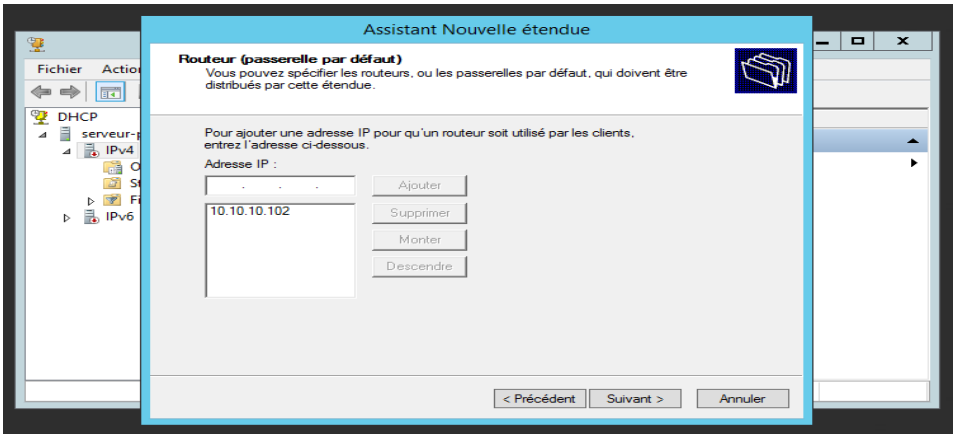


Figure III.24: Passerelle par défaut

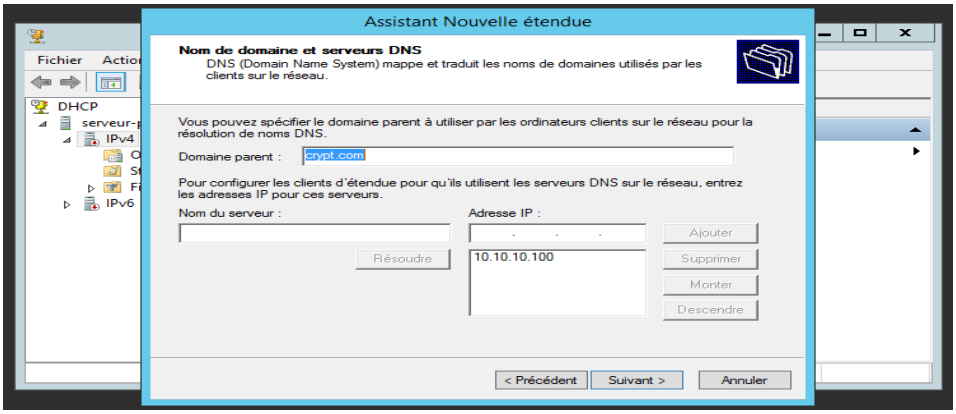


Figure III.25: Nom de domaine

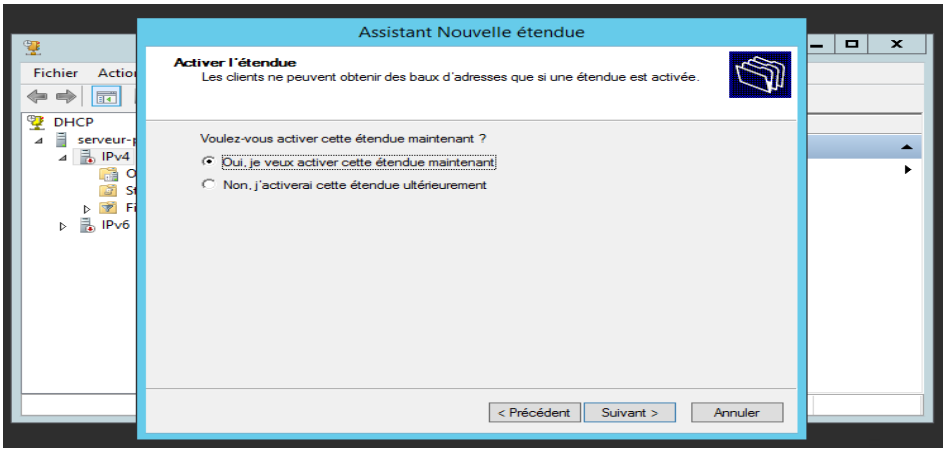


Figure III.26: Activer l'étendue

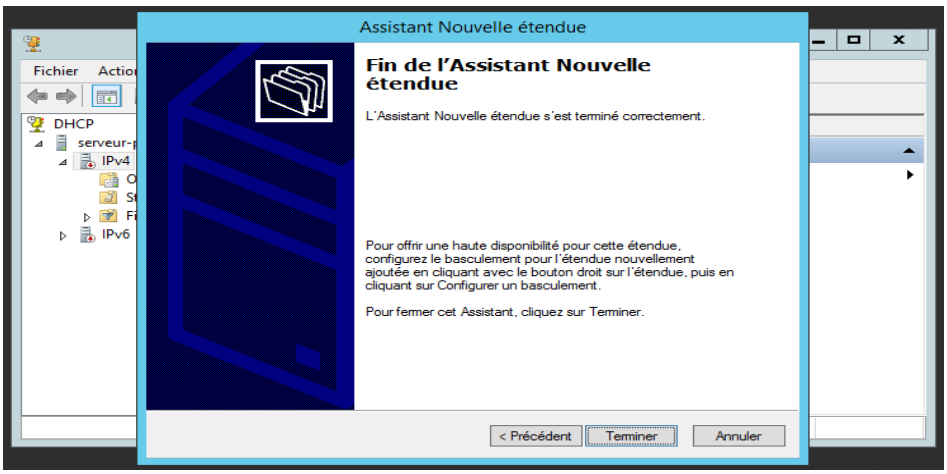


Figure III.27: Fin de l'assistant nouvelle étendue

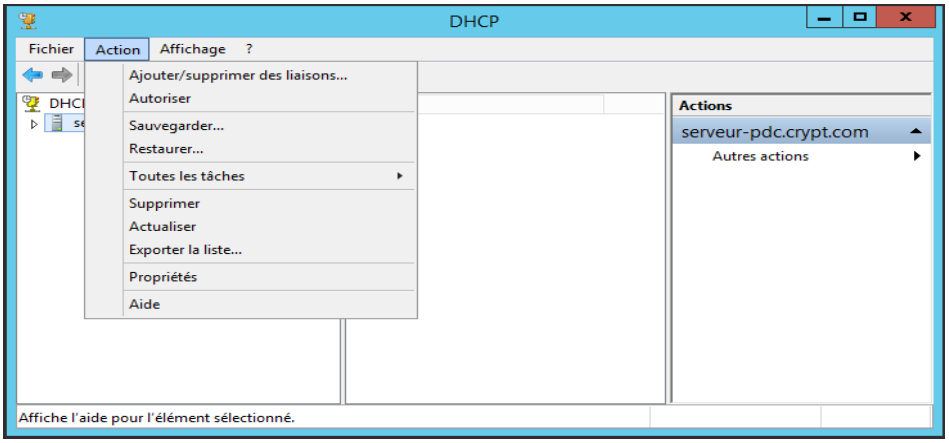


Figure III.28: Actualiser et autorisé l'étendue

La figure suivante illustre l'étendue du serveur DHCP est bien activer.

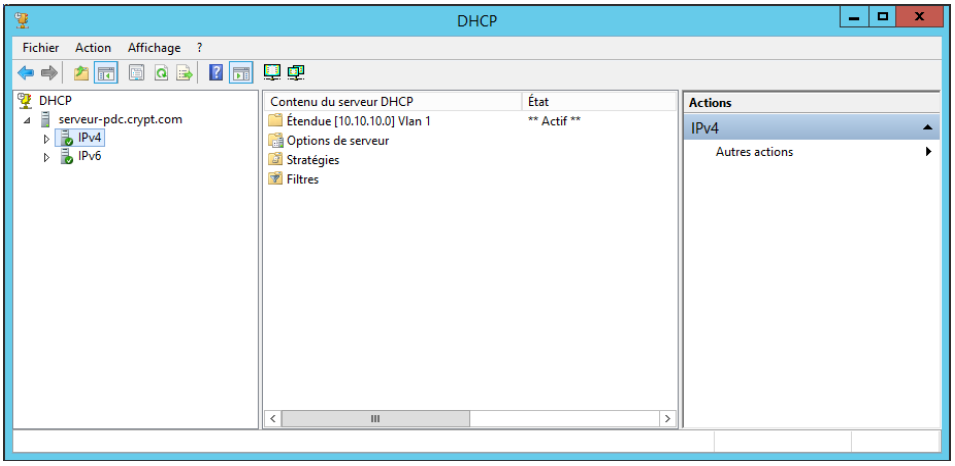


Figure III.29: Etendue activée

3.3. Création d'une zone de recherche inversée

La zone de recherche inversée permettre de retrouver un nom d'hôte à partir de son adresse IP. Cela peut-être utile dans certains cas. Cette zone peut être utilisée par les services d'anti-spam afin de contrôler si l'expéditeur des e-mails est bien le serveur nommé dans les en-têtes e-mail.

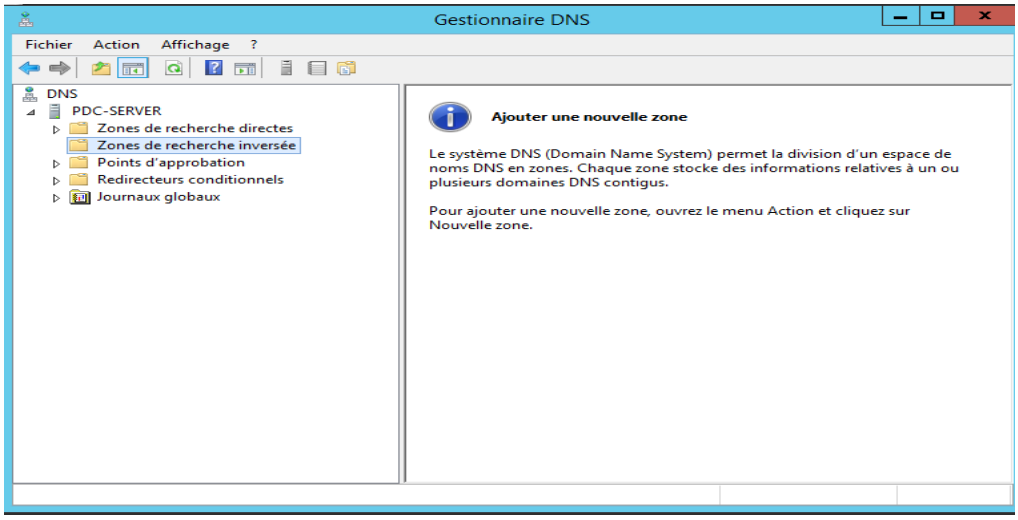


Figure III.30: Avant l'ajout de la zone

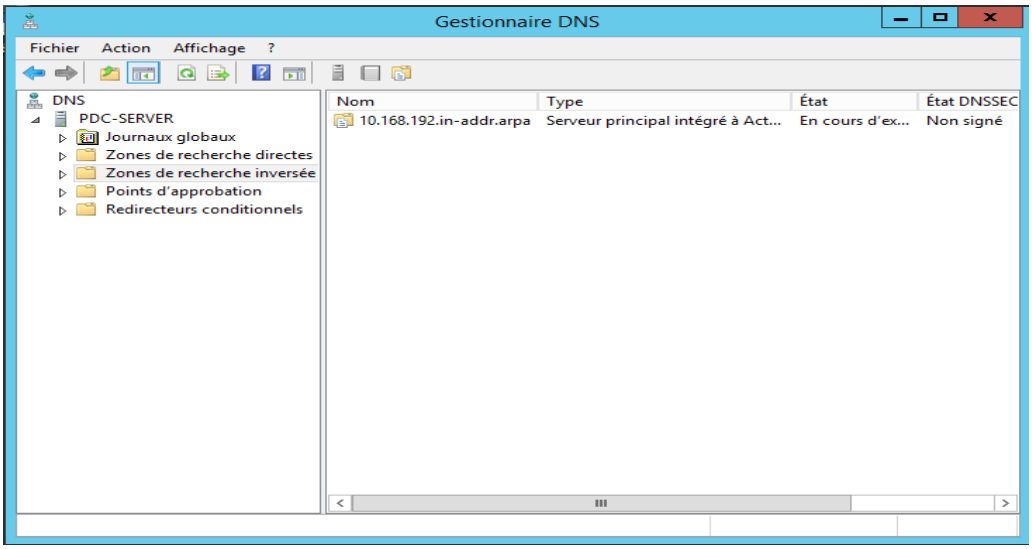


Figure III.31: Après l'ajout de la zone

Dans l'annexe B, vous trouvez les étapes pour configurer une zone de recherche inversé sous le gestionnaire DNS.

Etape IV: Générer une demande de certificat à l'autorité de certification racine

Avant que le contrôleur de domaine effectue une demande de certificat un service de certificat Active Directory doit être installer.

1. Installation de l'AD CS sous le contrôleur de domaine principale

On considère le contrôleur de domaine principal comme CA secondaire.

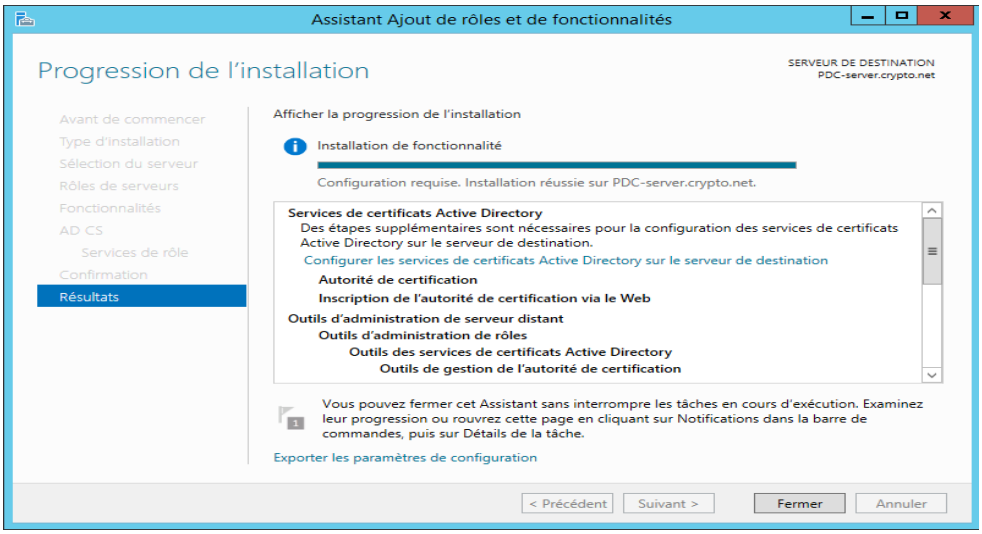


Figure III.32: Fin d'installation d'AD CS sous PDC

2. Configuration de l'autorité de certification secondaire

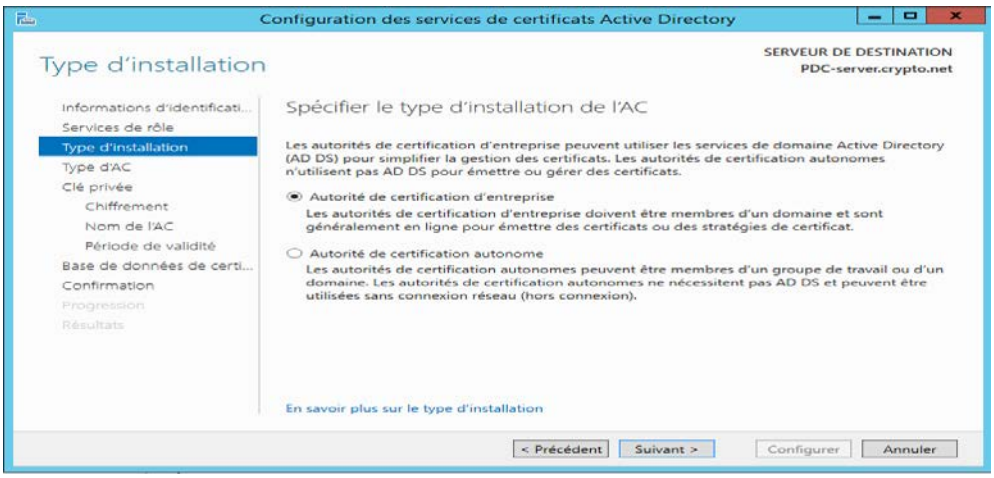


Figure III.33: Type d'installation de l'AC

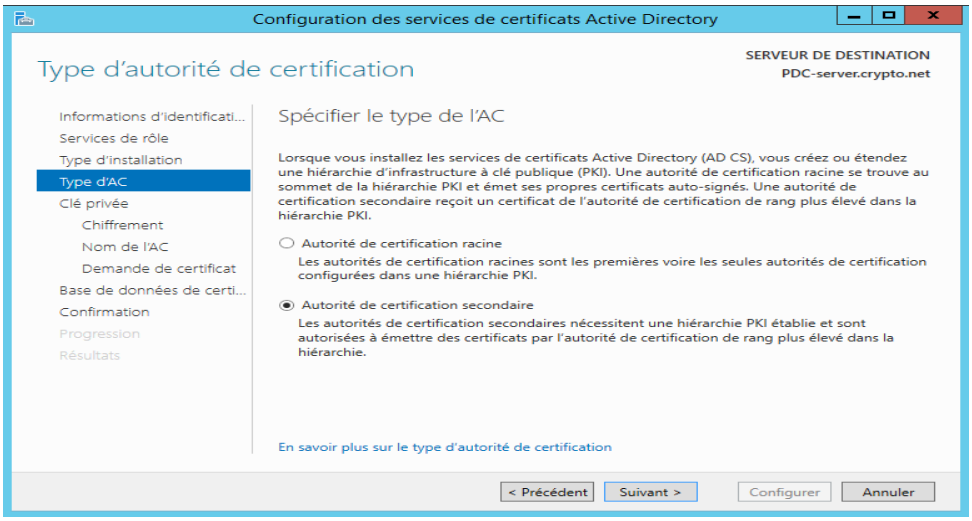


Figure III.34: Autorité de certification secondaire

Dans l'annexe A, vous trouvez l'installation complète de AD CS sous le contrôleur de domaine principal.

3. AC Secondaire génère une demande de certificat a AC Racine

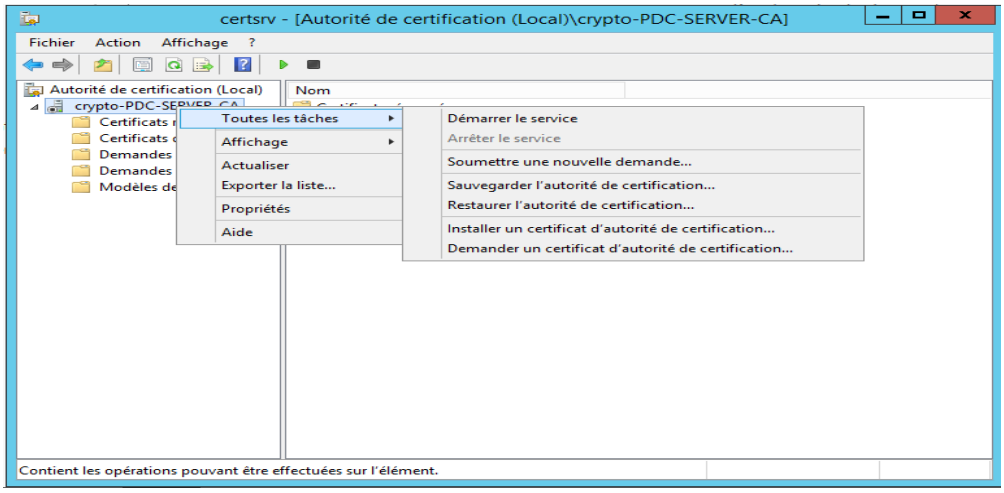


Figure III.35: Demande d'un certificat d'autorité de certification

Là on saisi l'adresse de CA-Server et entrée.

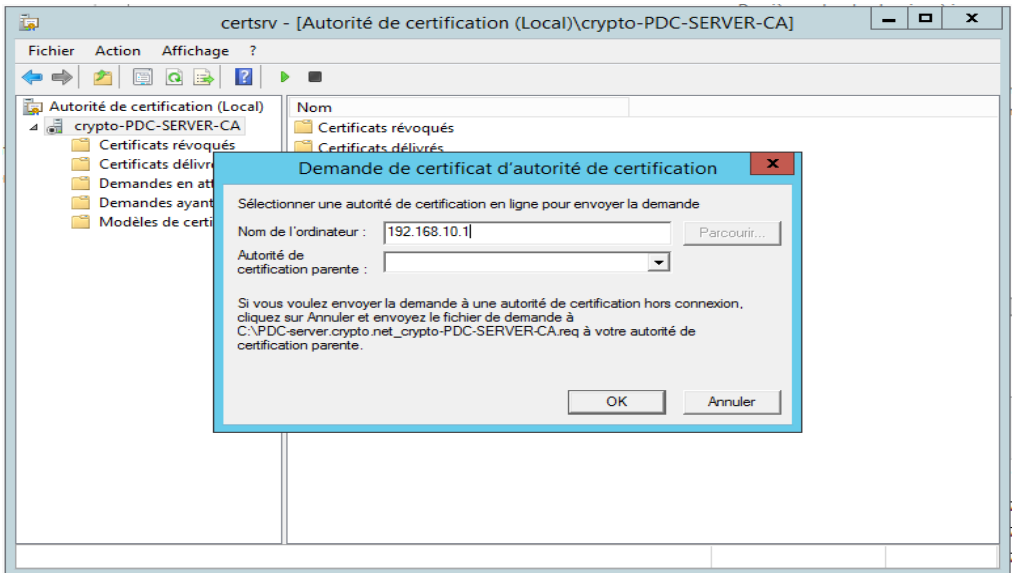


Figure III.36: Sélection de l'autorité de certification racine

Et nous affiche le nom de l'autorité de certification racine.

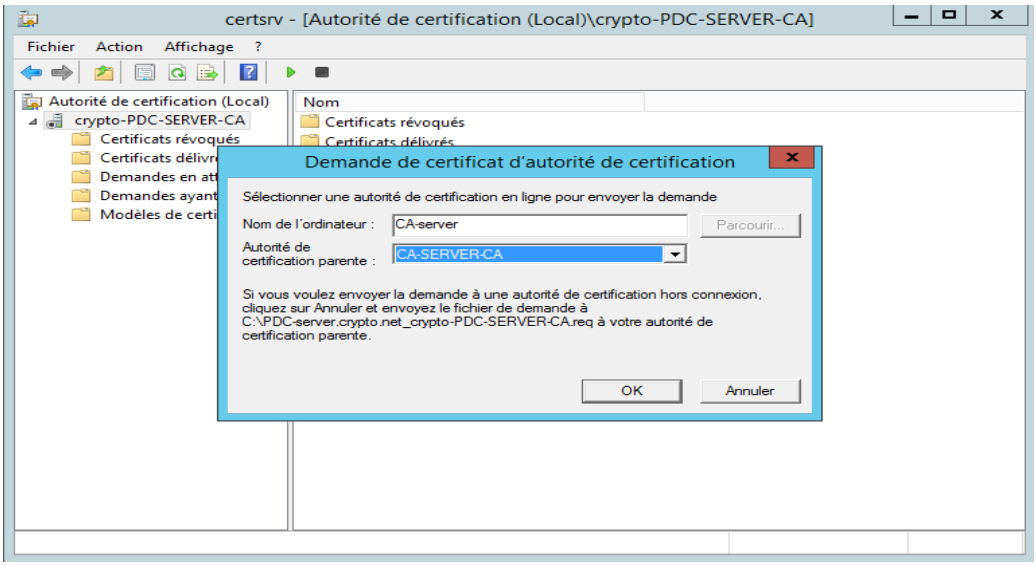


Figure III.37: Nom de l'autorité de certification racine qui s'affiche

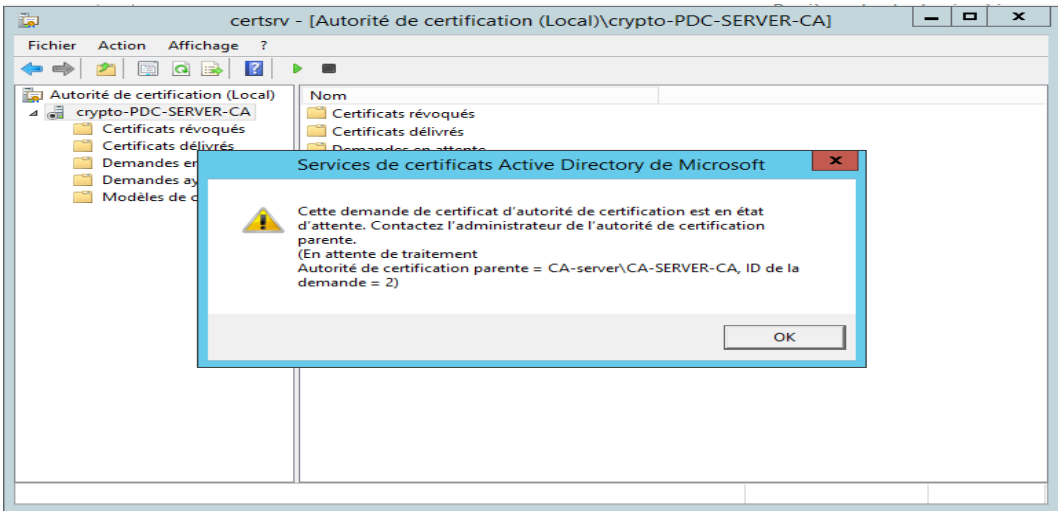


Figure III.38: Demande de certificat envoyer

Cette demande doit être validé et signé par l'administrateur de l'autorité de certificats racine (CA-Server) dans le cas ou le mode de travail est Workgroupe dans le cas contraire si un client est membre de domaine (Entreprise) toutes demandes de certificats est délivré par défaut .

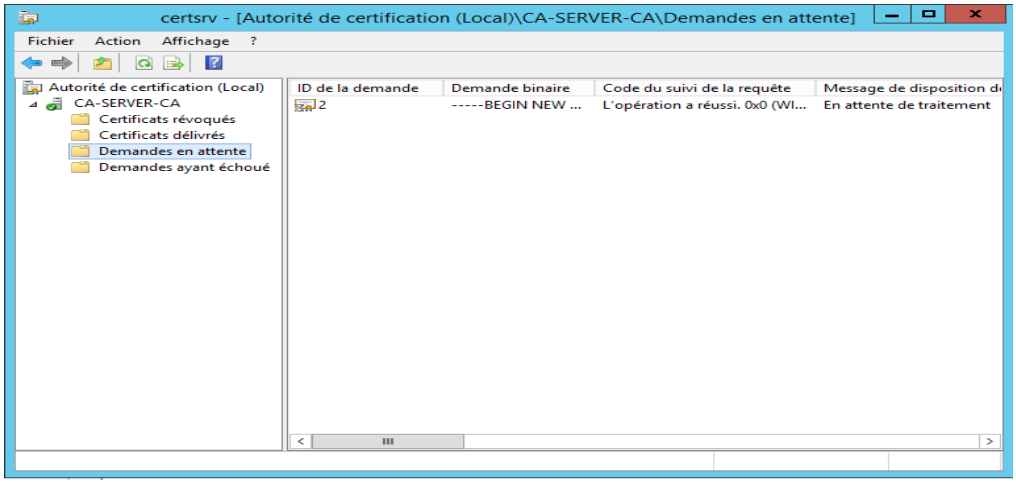


Figure III.39: Demande de certificat en attente

Dans la figure suivante l'administrateur de l'autorité de certification racine va délivrer la demande de certificat effectuer par l'autorité de certification secondaire dans le cas contraire c'est un refus.

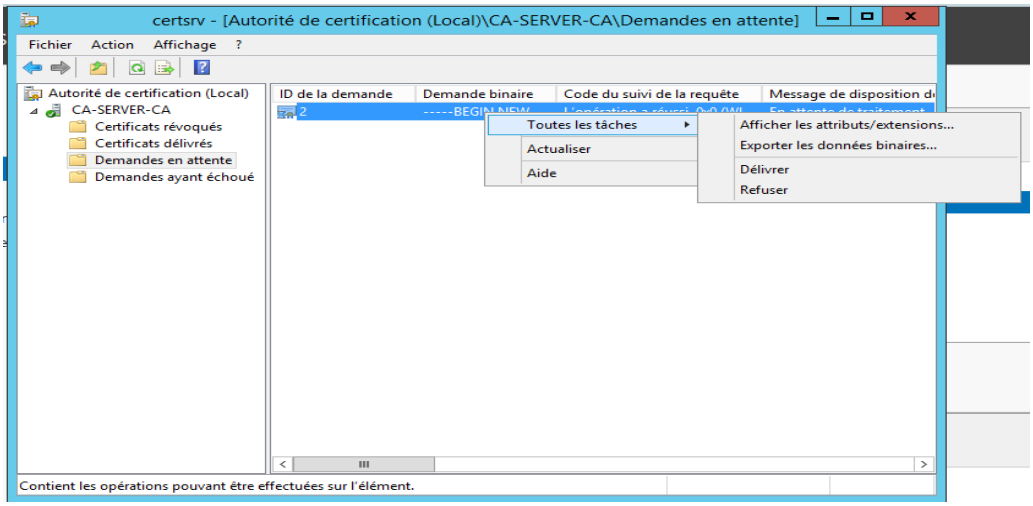


Figure III.40: Demande de certificat délivrer par AC racine

Une fois cette demande est délivrer on la trouve dans Certificats délivrés.

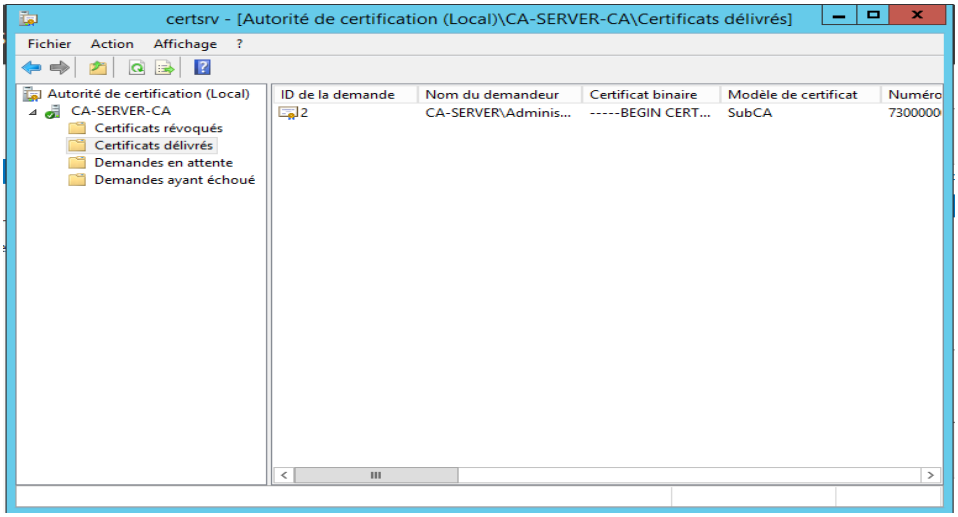


Figure III.41: Certificat délivrer

Dans (PDC-Server) l'autorité de certification secondaire on installe le certificat délivré, avant cela on doit déconnecter (CA-Server) l'autorité de certification racine la mettre Hors-ligne avec cette commande :

certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE

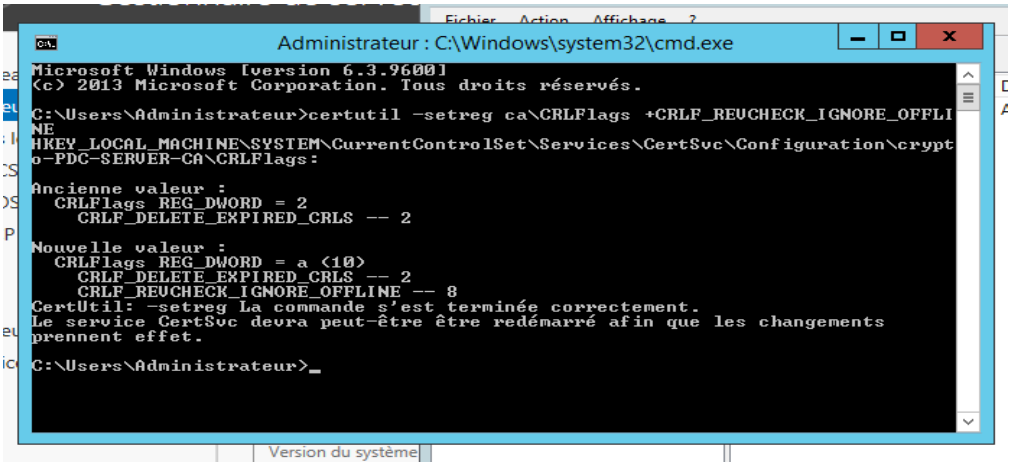


Figure III.42: Commande pour déconnecter AC racine

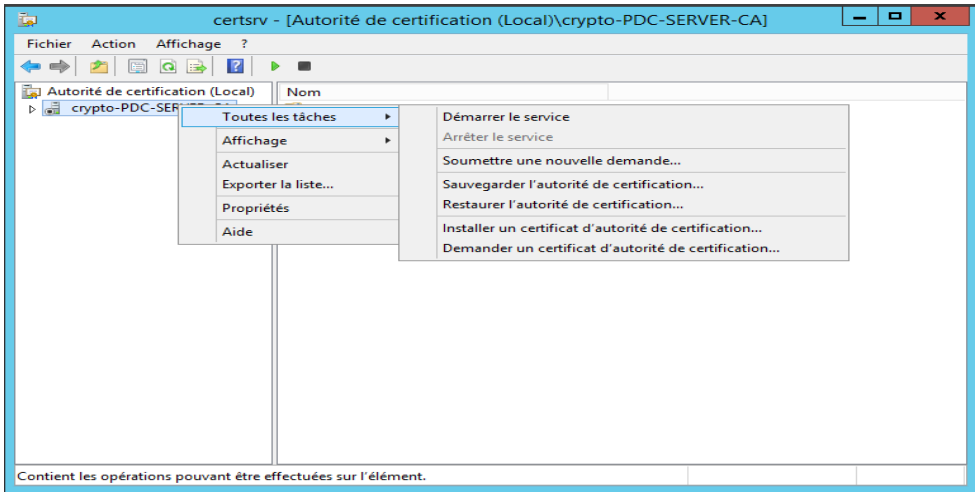


Figure III.43: Installation du certificat par AC secondaire

Après l'installation du certificat, l'autorité de certification secondaire est active et prête pour délivrer des certificats. La figure suivante montre les modèles de certificats.

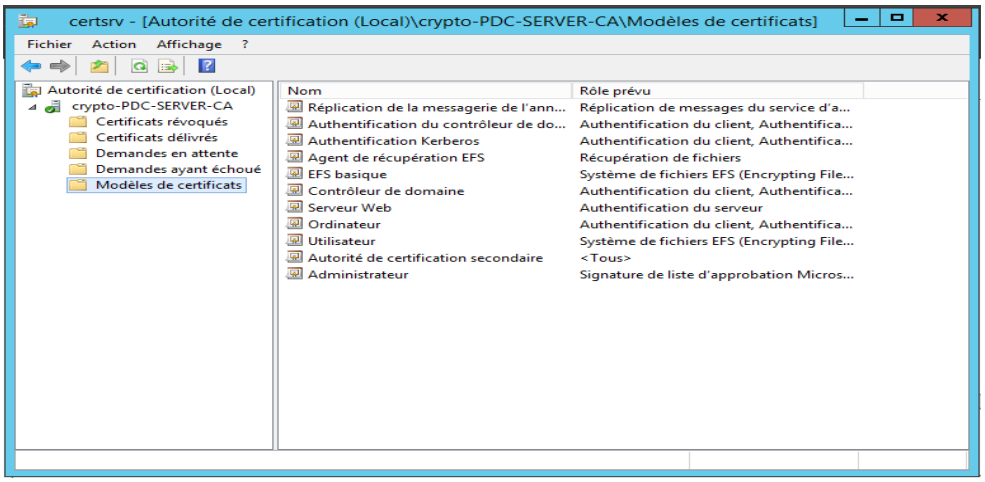


Figure III.44: Modèles de certificats

Etape V: Installation et configuration de machine membre

1. Installation et configuration de la TMG

Avant d'installer la TMG l'ajout et la configuration de deux cartes réseau (interne et externe) est exigé pour éviter toutes problèmes durant l'installation.

la figure suivante montre l'installation des pré-condition pour le serveur TMG sous Windows Server 2008.

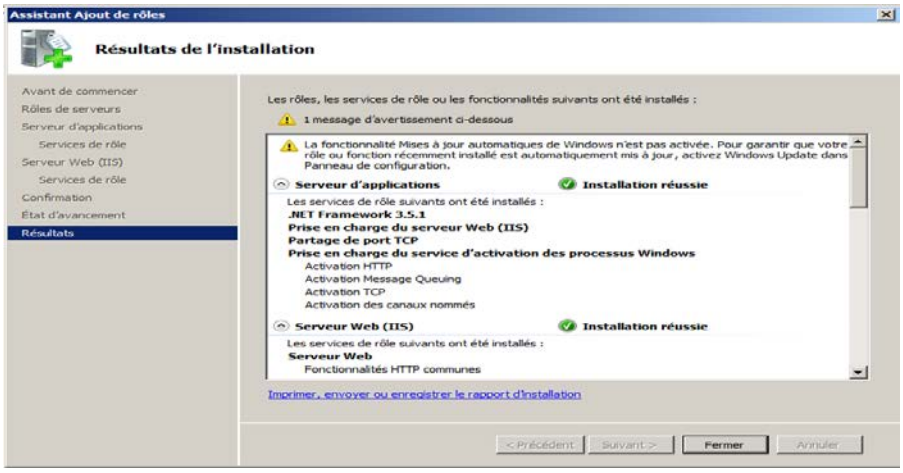


Figure III.45: Les pré-conditions de la TMG

1.2. Lancement de l'installation de la TMG

Les différentes étapes d'installation de la TMG sont définies dans l'annexe C**.**

Figure III.46: La console de gestion de la TMG.

1.3. La création des règles de la TMG

Il est indispensable de configurer les règles qu'il faut autoriser avant d'entreprendre n'importe quelle configuration au niveau interne, car la TMG interdit par défaut tout le trafic entrant et sortant sur tous les réseaux (internes, externes et locaux). Nous avons autorisé les règles, DNS, PING, HTTP /HTTPS en spécifiant, pour chacun d'eux le réseau entrant, sortant et les utilisateurs sur les quels elles seront appliquées. Comme exemple de création d'une règle TMG, nous prenons celle du DNS qui permet de spécifier un ordinateur sur le quel elle s'applique. Et afin de restreindre le trafic HTTP /HTTPS autorisé nous créons une règle pour empêcher l'accès à certains sites.

- **Exemple de la règle DNS**

Pour la création de la règle d'accès DNS, stratégie de pare-feu -> entrons le nom DNS.

Figure III.47: création de la règle d'accès DNS.

Notre objectif étant d'autoriser la règle DNS, sélectionnons autoriser.

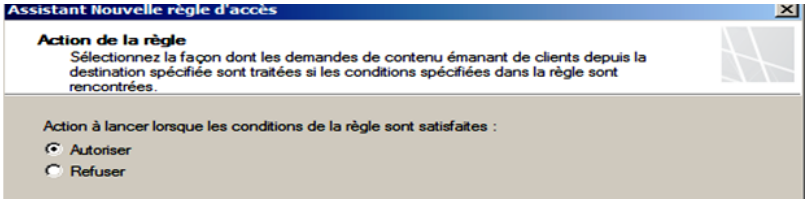


Figure III.48: Choix de l'action de la règle.

Dans ajout de protocoles nous spécifions sur quels protocoles s'applique cette règle (DNS).

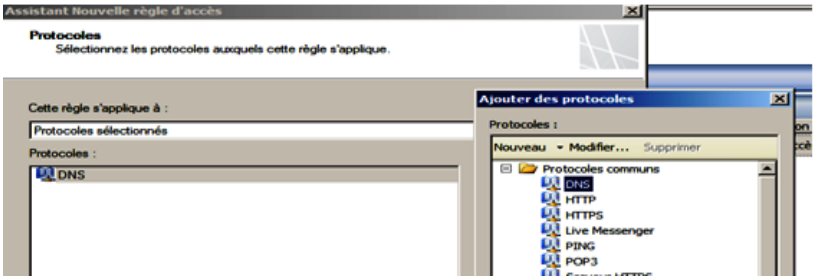


Figure III.49: Sélection des protocoles.

- **Exemple de la règle pour empêcher l'accès à certain sites**

Définissons les utilisateurs sur lesquels s'applique cette règle.

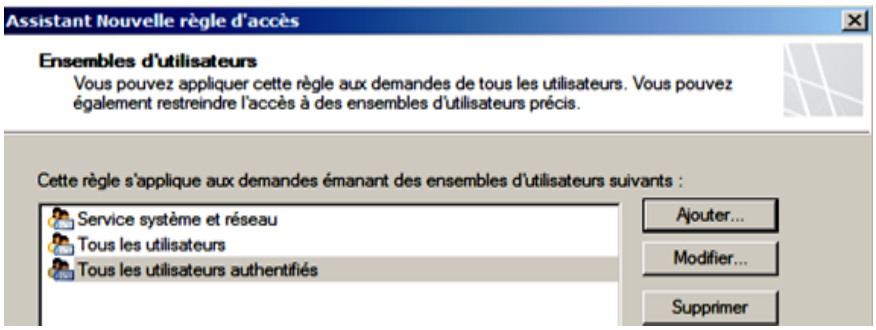


Figure III.50: L'ensemble des utilisateurs concernés par la règle de refus.

Choisissons les sites à exclure, comme les réseaux sociaux, les sites d'achat e-commerce et autres.

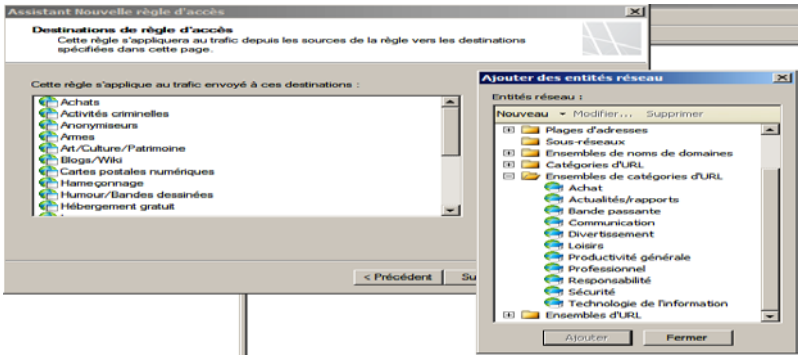


Figure III.51: La sélection des catégories d'URL non autorisées.

Afin de valider et enregistrer toute modification apportée à la TMG, nous cliquons sur Appliquer.

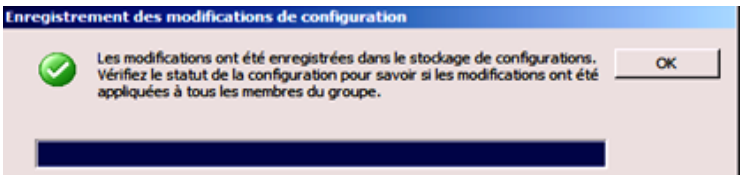


Figure III.52: Enregistrement des modifications

2. Installation et configuration du Server Exchange 2013

L'installation du serveur de messagerie Exchange exige des pré-requis.

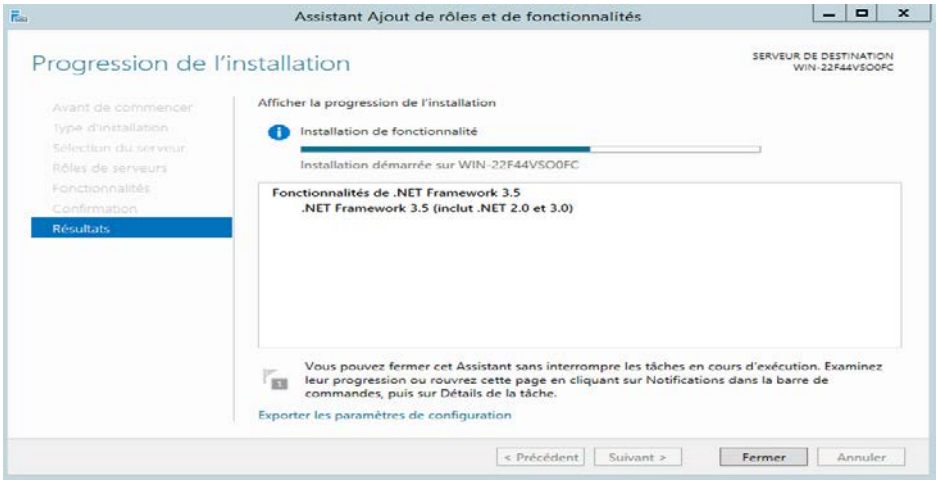


Figure III.53: Ajout de fonctionnalité Framework

Pour vérifier et installer les pré-requis nous avons le choix de les ajouter au serveur via le gestionnaire de serveur ou bien via l'interpréteur de commande PowerShell.

- **Dans Windows PowerShell**

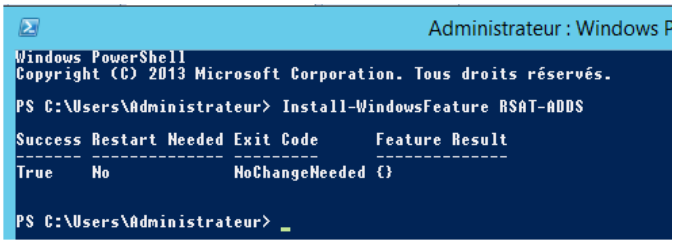


Figure III.54: Installation pack d'administration des outils à distance

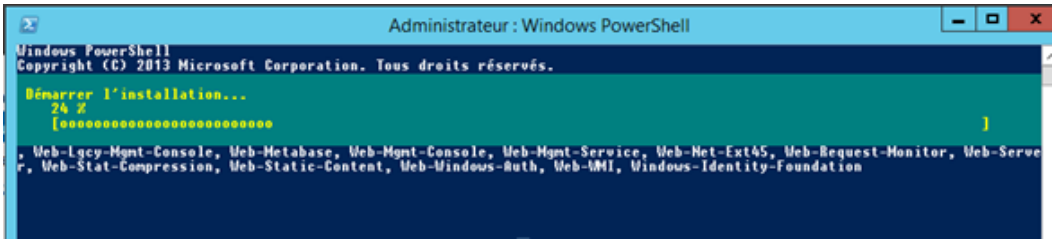


Figure III.55: Installation des pré-requis

Après un redémarrage de l'ordinateur à la fin de l'installation des fonctionnalités, il faut changer le mode de démarrage du service de partage de ports net.TCP, afin de le passer en mode automatique.

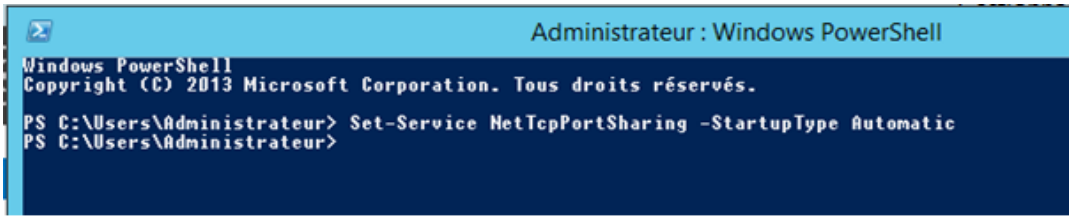


Figure III.56: Le passage au mode automatique

Nous allons maintenant commencer à préparer l'Active Directory pour installer Exchange Server 2013. Pour ce faire nous allons ouvrir l'invite de commande et se positionner à l'emplacement du programme d'installation de Microsoft Exchange Server 2013. Voir l'annexe C.

3. Installation du serveur Web IIS

Le rôle du serveur Web l'IIS 7.0 de Windows Server 2008 est de partager des informations avec des utilisateurs sur internet, intranet ou extranet. IIS nous permet d'avoir une plateforme web unifiée, améliorée et permet de personnaliser les sites web. Voir annexe C.

Conclusion

La mise en place de cette politique de sécurité, nous a permis de mettre en pratique d'avoir de nouveaux acquis et l'améliorations de nos connaissances portant sur la sécurité réseau.

Lors de la réalisation de cette application nous avons tout fait pour collecter le maximum d'informations et renseignements qui touchent la sécurité informatique.

Conclusion général

Depuis long temps la sécurité réseau est un facteur le plus sérieux que connaissent les entreprises dotées d'un réseau informatique .Il est impossible de sécuriser totalement un système d'information, car il y'aura toujours des hackers pour découvrir des nouvelles failles dans le système, mais on peut toujours rendre une solution plus difficile en appliquant des nouvelles approches, cela nous permettra d'avoir un haut niveau de sécurité des données.

La réalisation de ce mémoire nous a permis d'accroitre nos connaissances dans le vaste domaine de la sécurité. Cela en usant des différents outils, concepts et mécanismes de la sécurité. En découvrant le monde de la cyber-attaque, les motivations des pirates, nous nous sommes rendu compte des limites de la sécurité.

Nous tenons à souligner que la cryptographie est large domaine de recherche et un domaine sensible car il concerne la sécurité des données.

En conclusion, nous souhaitons que cette politique de sécurité que nous avons mise en place, malgré toutes les contraintes temporelles et matérielles, soit enrichie et approfondie dans l'avenir.

ANNEXES

A.1. Autorité de certification

Certificat, également connu sous le certificat de clé publique ou un certificat numérique, est un document électronique qui utilise une signature numérique de lier une clé publique à une identité. L'identité peut être n'importe quoi. Par exemple, il pourrait être représenté un utilisateur, un dispositif, un service ou même quelques lignes de code.

Le certificat peut être utilisé pour signer l'identité et pourrait être vérifiée par d'autres. Par exemple, un message étant signé par un certificat a pu être vérifiée par le récepteur, de sorte qu'il sera en mesure de savoir si le message est celui d'origine ou a été modifié par quelqu'un d'autre. Le certificat peut également être utilisé pour chiffrer et déchiffrer. C'est la raison pour laquelle nous pouvons lier un certificat sur un site Web afin que les données entre le navigateur et le serveur soient garantis, car ils sont été chiffrés et signés par le certificat.

L'autorité de certification (CA) prend la responsabilité de délivrer les certificats. Dans Windows utilisant le service de certificat Active Directory.

Dans une entreprise, il pourrait y avoir plus d'un CA, ils seront organisés hiérarchiquement. Le niveau supérieur serait l'autorité de certification racine, qui a un certificat signé par lui-même. Le certificat de toutes les autorités subordonnées doit être sollicitée et signé par l'autorité de certification racine.

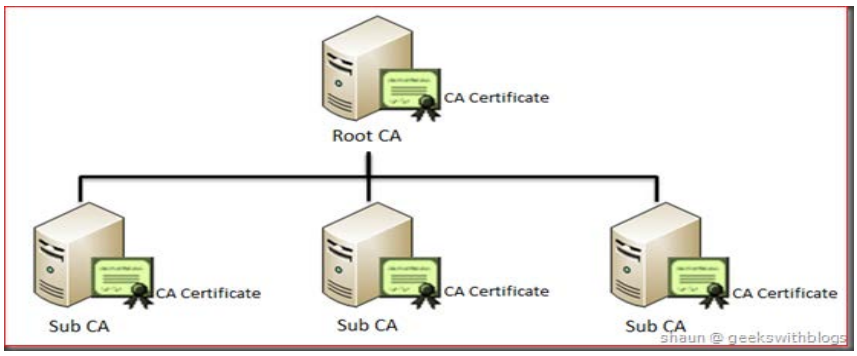


Figure A.1: Structure de CA racine et secondaire

A.2. Installation et configuration d'AD CS de CA racine

- Les illustrations suivantes montrent l'installation du service AD CS.

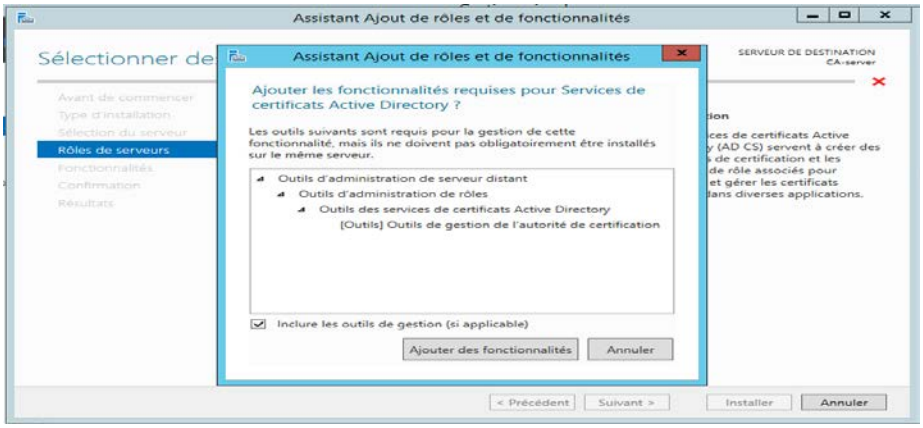


Figure A.2: Illustration 1

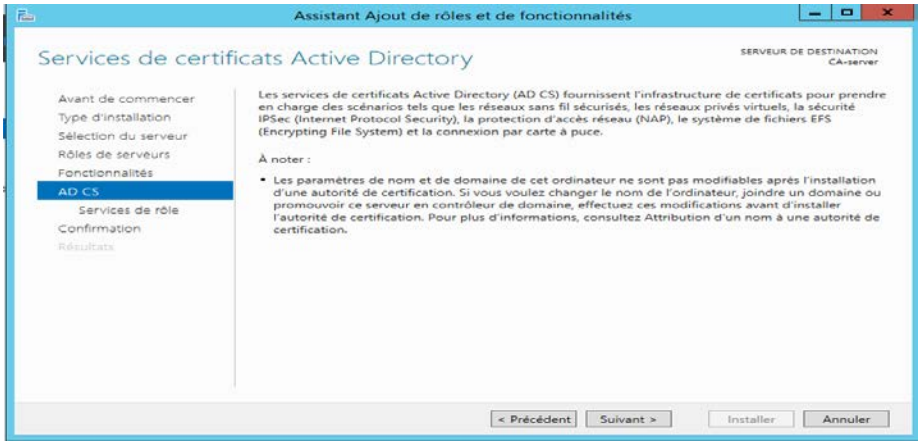


Figure A.3: Illustration 2

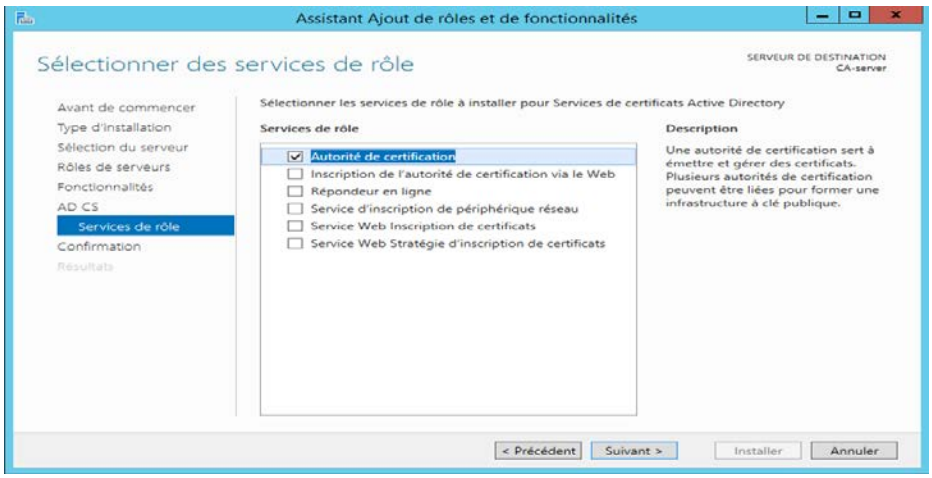


Figure A.4: Illustration 3

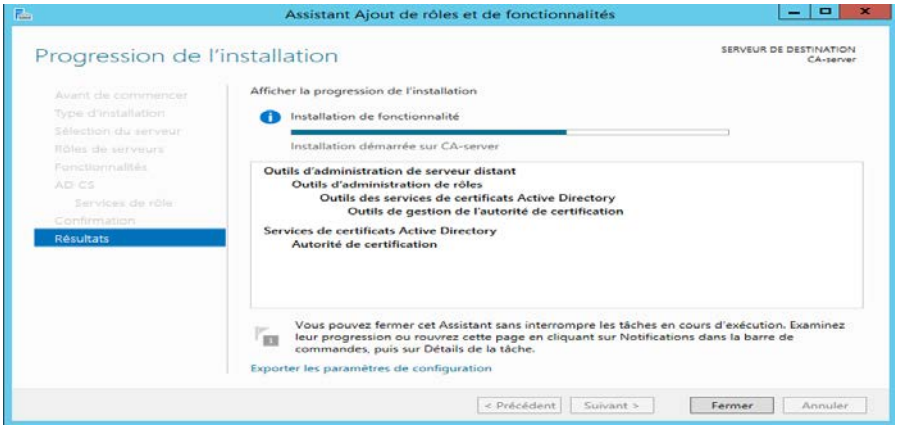


Figure A.5: Illustration 4

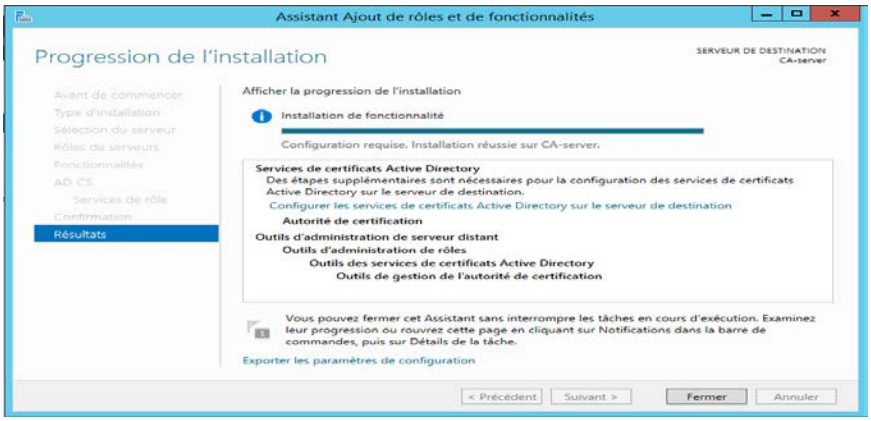


Figure A.6: Fin d'installation d'AD CS

- Dans ce qui suit-on complète la configuration de AD CS pour l'autorité de certification racine.

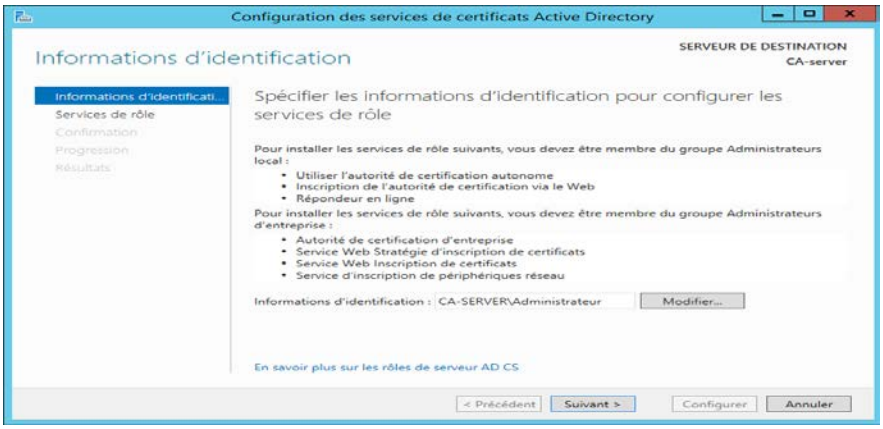


Figure A.7: Informations avant de compléter la configuration de CA

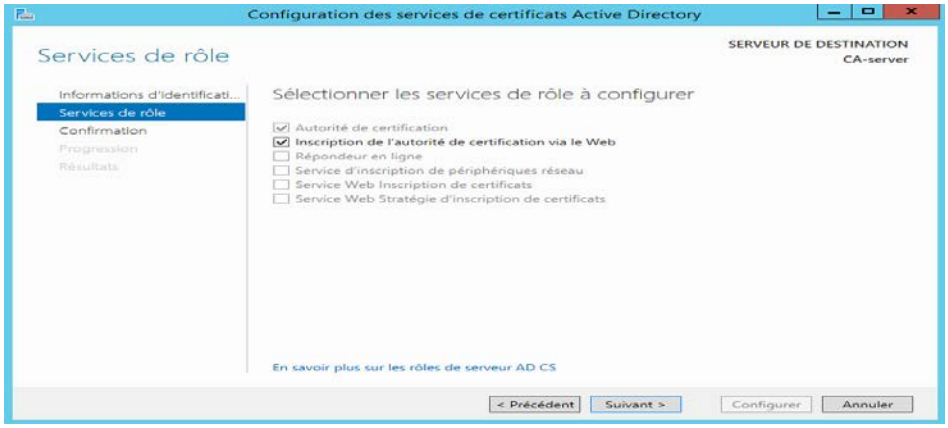


Figure A.8: Spécification des rôles à configurer

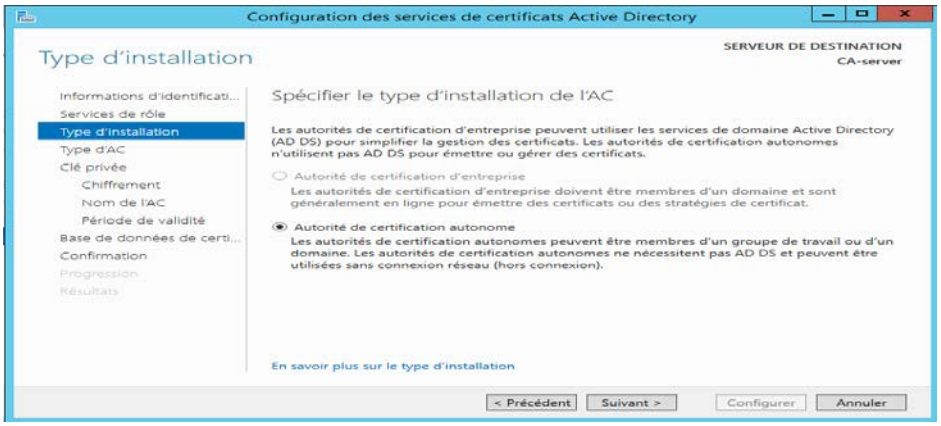


Figure A.9: Choisir le type d'installation de CA

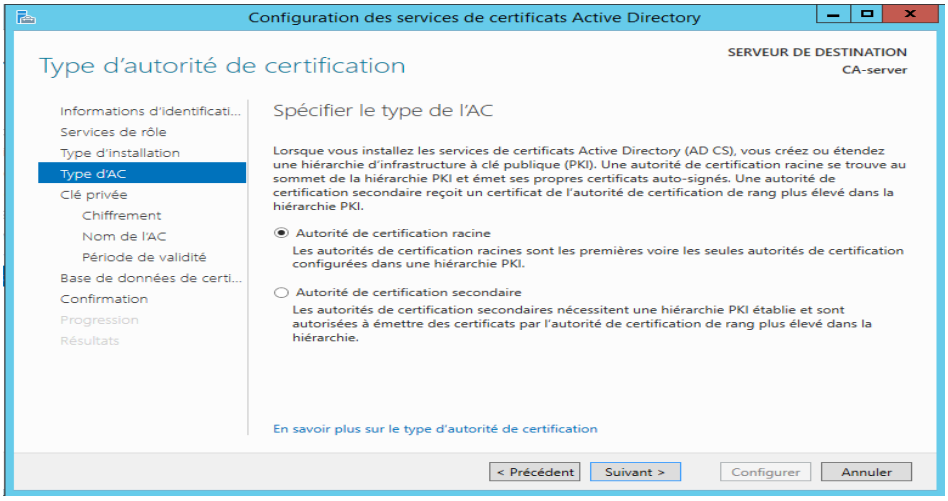


Figure A.10: Choisir le type de CA

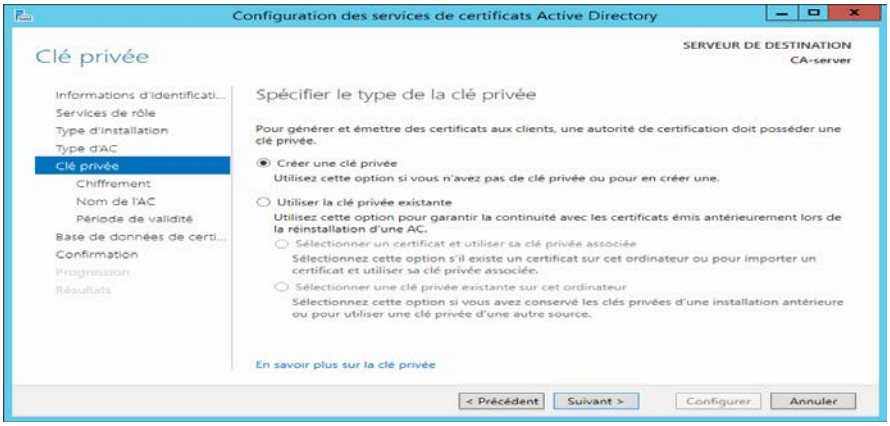


Figure A.11: Auto création de la clé publique pour CA

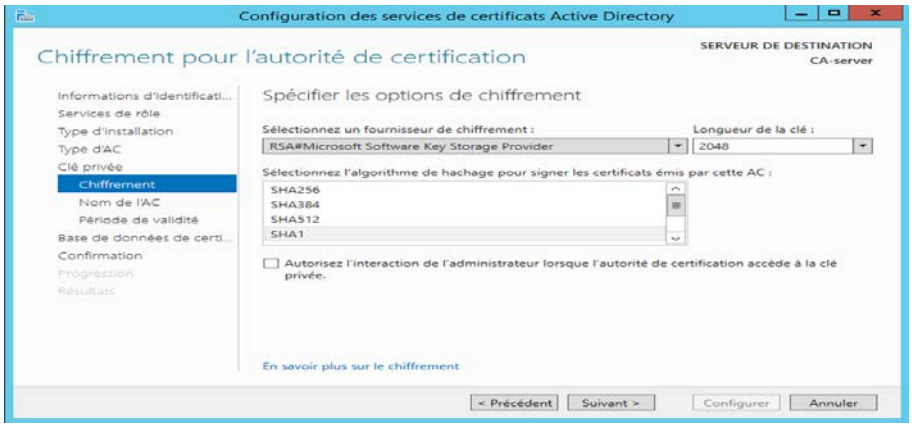


Figure A.12: Type de chiffrement de la clé

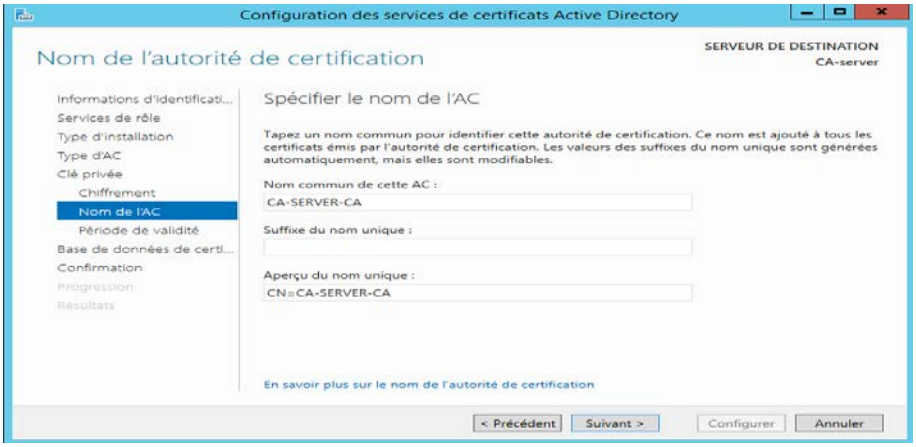


Figure A.13: Un nom pour l'autorité de certification racine

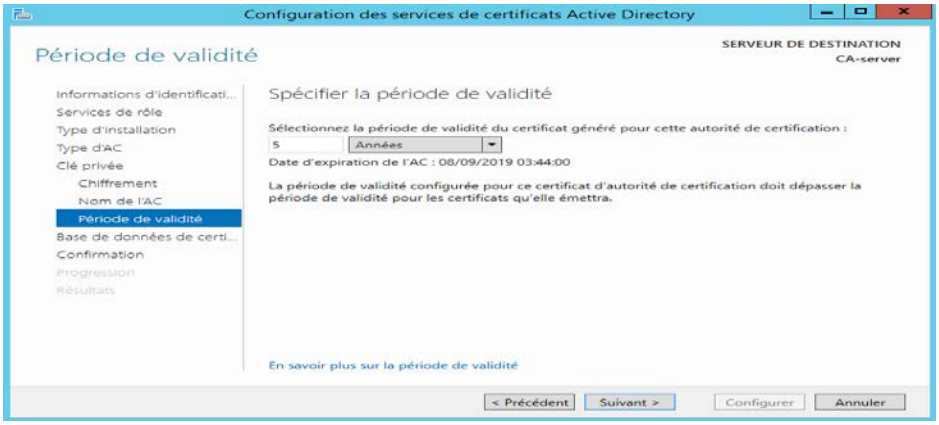


Figure A.14: Durée de vie du certificat générer par CA

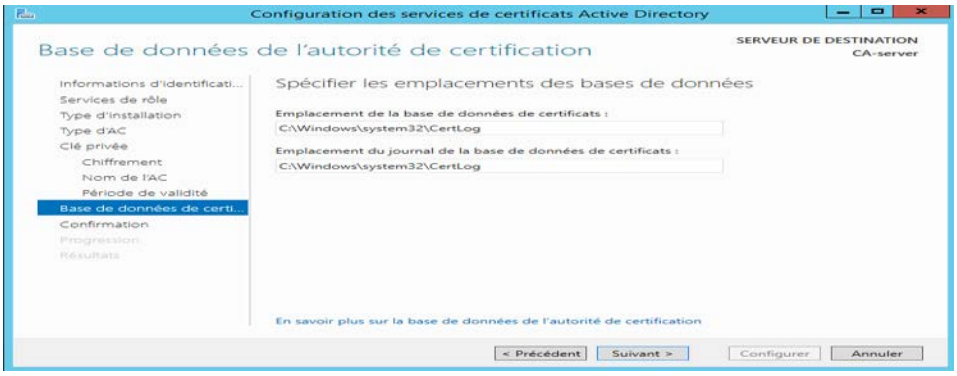


Figure A.15: Emplacement de la base de données des certificats

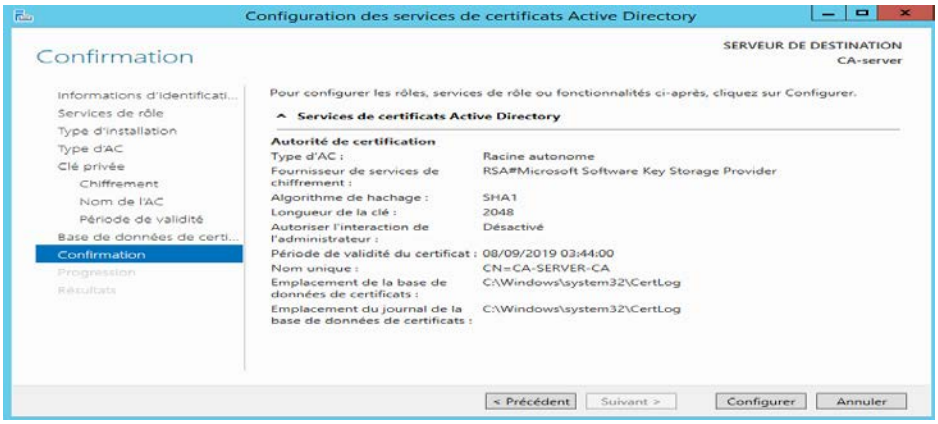


Figure A.16: Récapitulatif de la configuration de CA

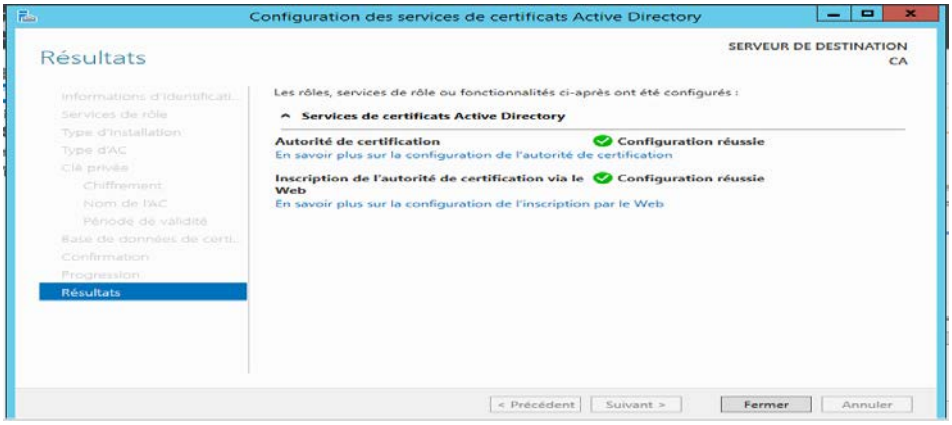


Figure A.17: Fin de la configuration de CA

A.2. Ajout de quelques rôles et fonctionnalité pour CA racine

L'illustration suivante montre l'ajout des rôles et fonctionnalités pour l'autorité de certification racine.

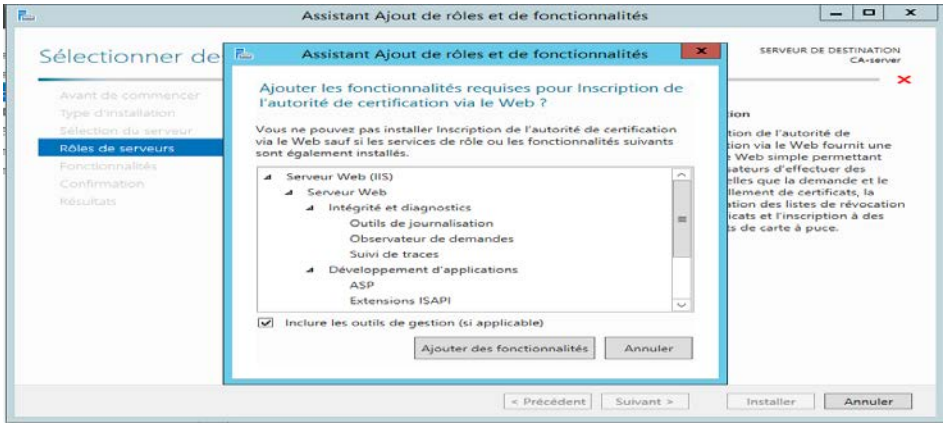


Figure A.18: Illustration

A.3. Installation d'AD CS sous le contrôleur de domaine principal

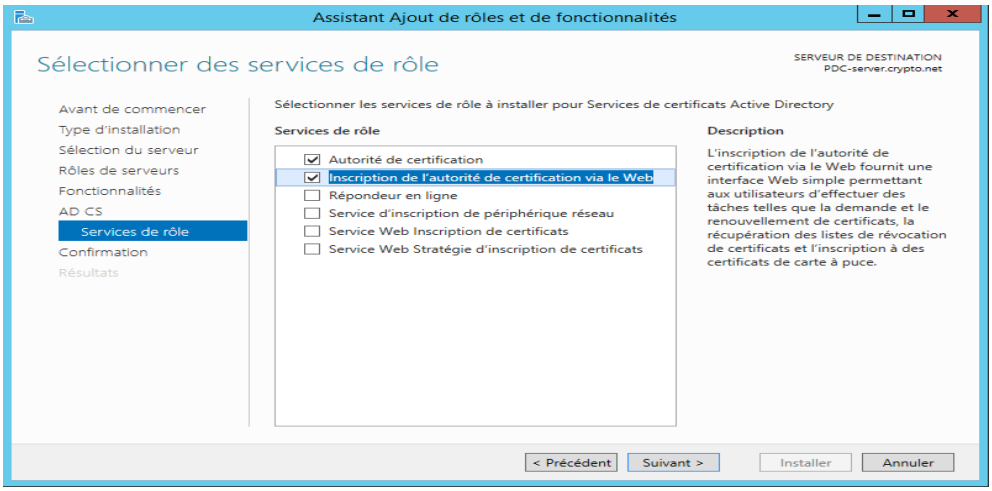


Figure A.19: Sélection des rôles d'AD CS

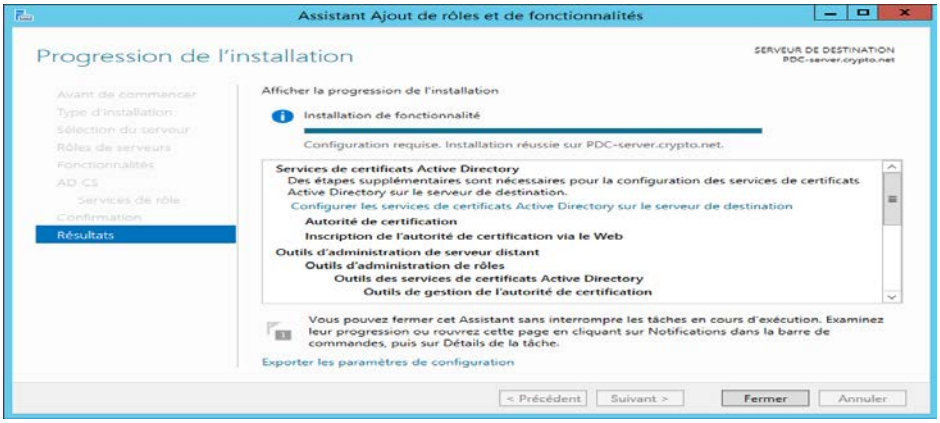


Figure A.20: Fin d'installation des services d'AD CS

A.4. Configuration d'AD CS en autorité de certification secondaire

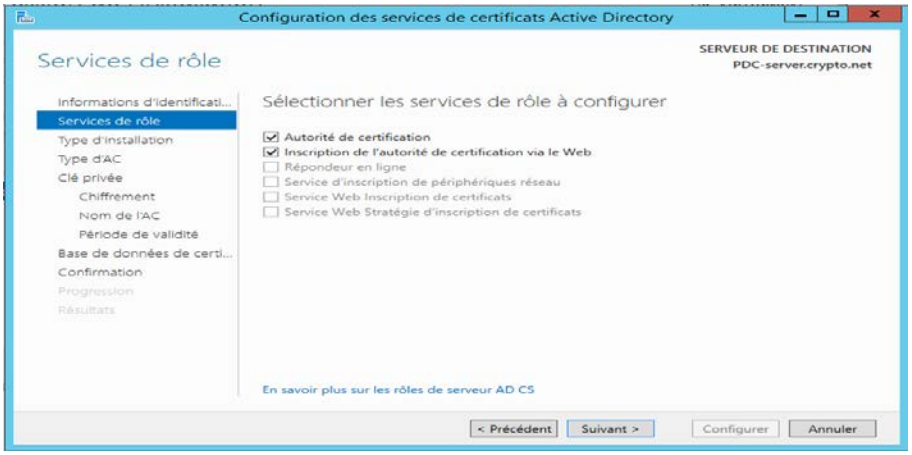


Figure A.21: Les rôles à configurer

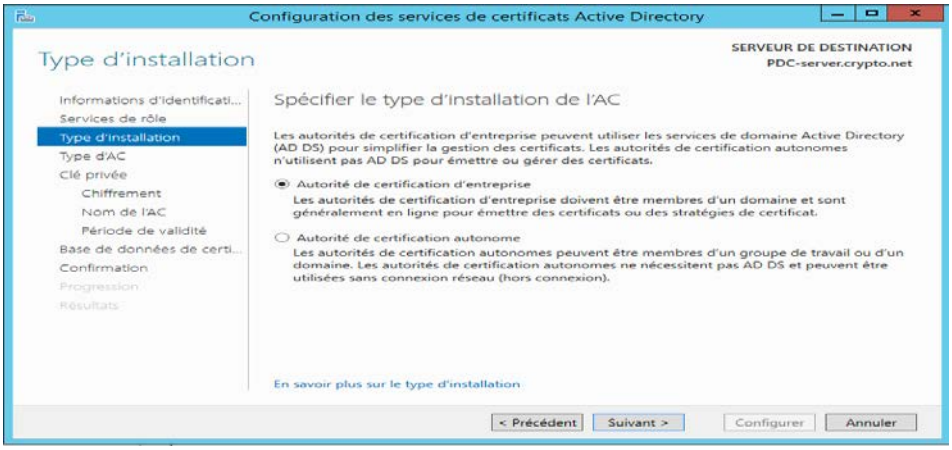


Figure A.22: Type d'installation d'AC

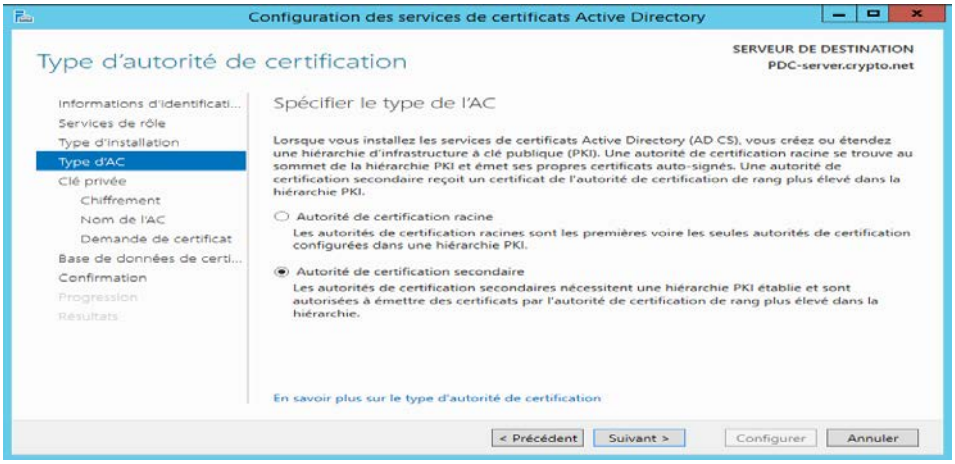


Figure A.23: Type d'AC

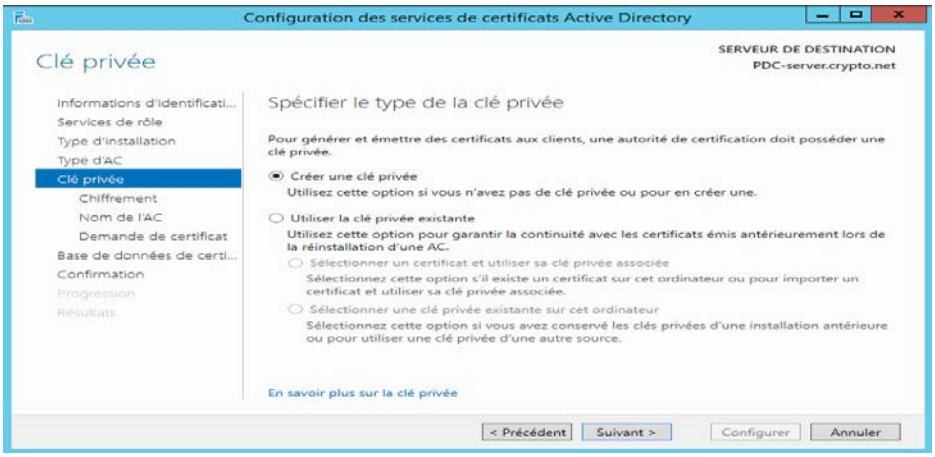


Figure A.24: Type de la clé privé

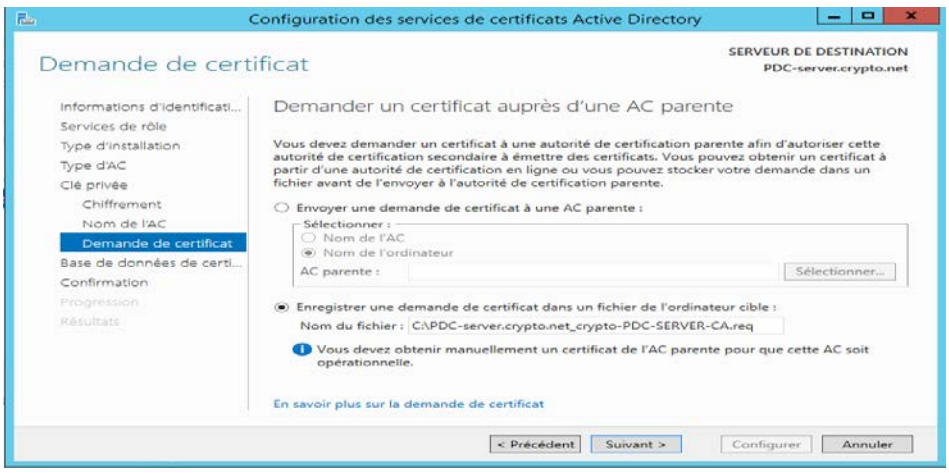


Figure A.25: Enregistrement d'une demande de certificat

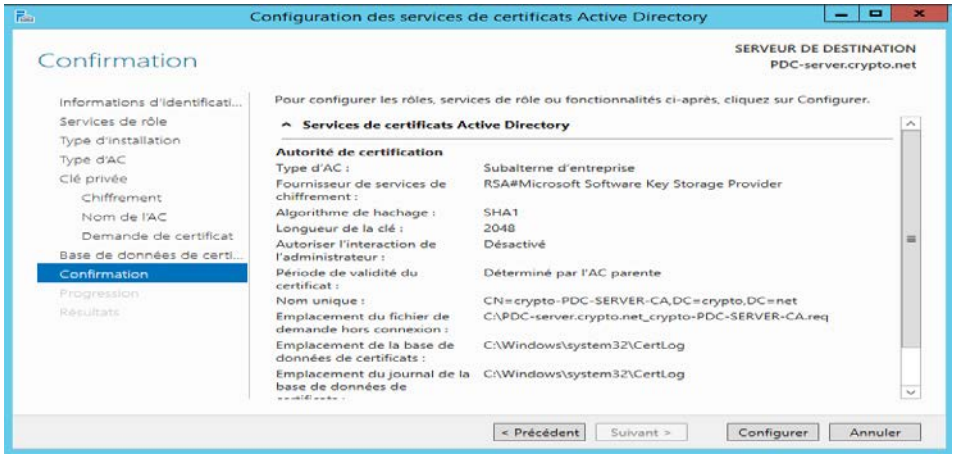


Figure A.25: Un récapitulatif de la configuration

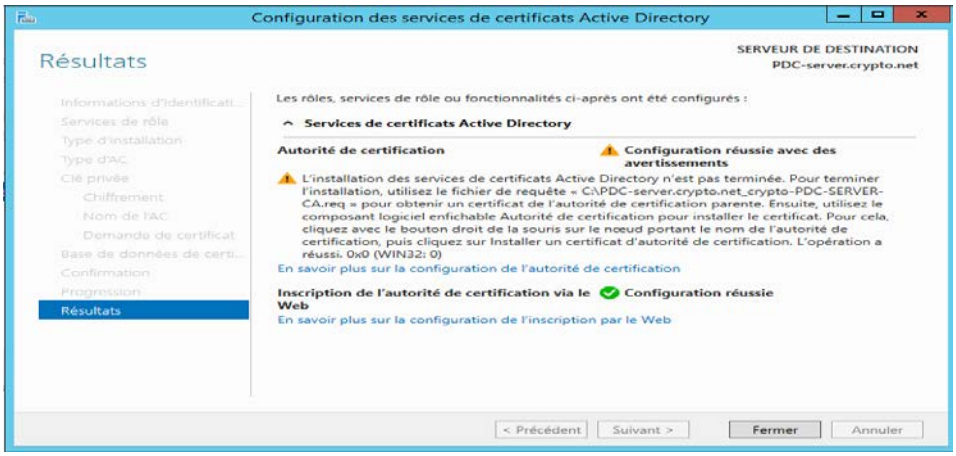


Figure A.26: Configuration réussite d'AD CS

Dans la figure suivante on voit bien que le service de l'autorité de certification n'est pas activé.

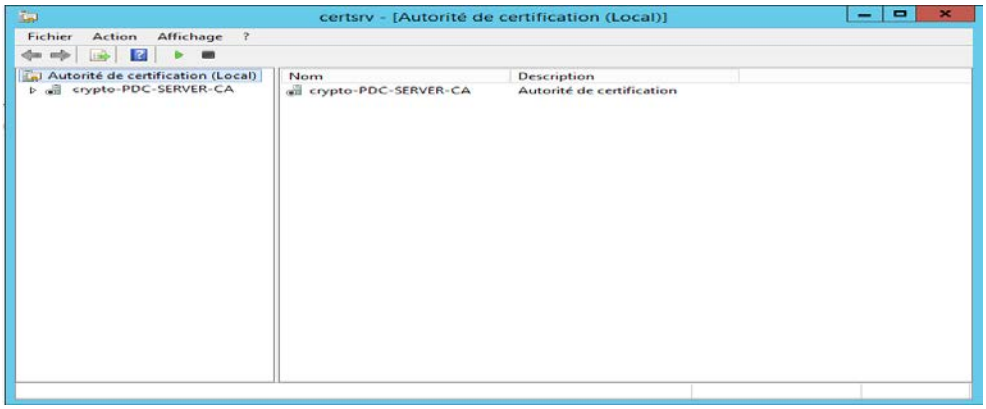


Figure A.27: Autorité de certification de CA secondaire**.**

B.1. PDC un contrôleur de domaine principal

C'est le contrôleur de domaine principal dans un réseau Microsoft. C'est l'Ordinateur qui valide les connexions au domaine et gère la base de données d'annuaires pour le Domaine. Il mémorise les modifications apportées aux comptes de tous les utilisateurs.

B.2. Présentation d'Active Directory

Active Directory est le nom du service d'annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire Active Directory est basé sur les standards TCP/IP, DNS, LDAP, Kerberos,...

Il doit être entendu au sens large, c'est-à-dire qu'Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone,...) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, …Il permet de recenser toutes les informations concernant le réseau, que ce soient les utilisateurs, les machines ou les applications. Ainsi il constitue le noyau central de toute l'architecture réseau et a vocation à permettre à un utilisateur de retrouver et d'accéder à n'importe quelle ressource identifiée par ce service.

Active Directory est donc un outil destiné aux utilisateurs mais dans la mesure où il permet une représentation globale de l'ensemble des ressources et des droits associés, il constitue également un outil d'administration et de gestion du réseau. Il fournit à ce titre des outils permettant de gérer la répartition de l'annuaire sur le réseau, sa duplication, la sécurisation et le partitionnement de l'annuaire de l'entreprise.

Figure B.1: Active Directory

B.2.1. Installation et configuration de l'Active Directory

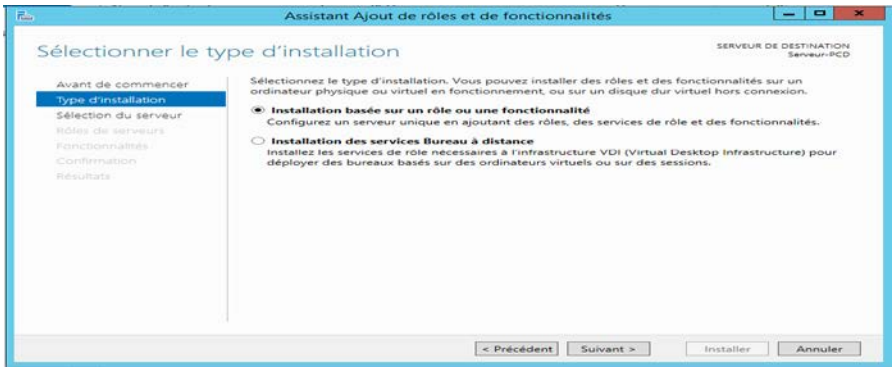


Figure B.2: Lancement d'ajout des rôles et fonctionnalités

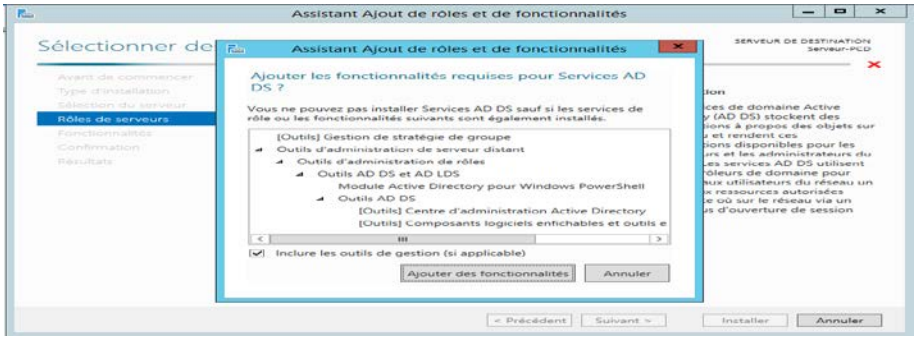


Figure B.3: Sélectionner AD DS pour l'installer

Les étapes qui précèdent l'installation d'AD DS sont montrées dans les trois illustrations suivantes.

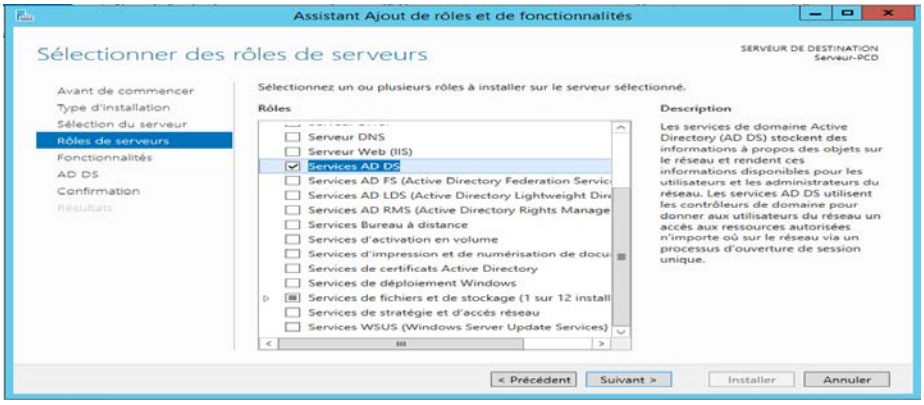


Figure B.4: Illustration 1

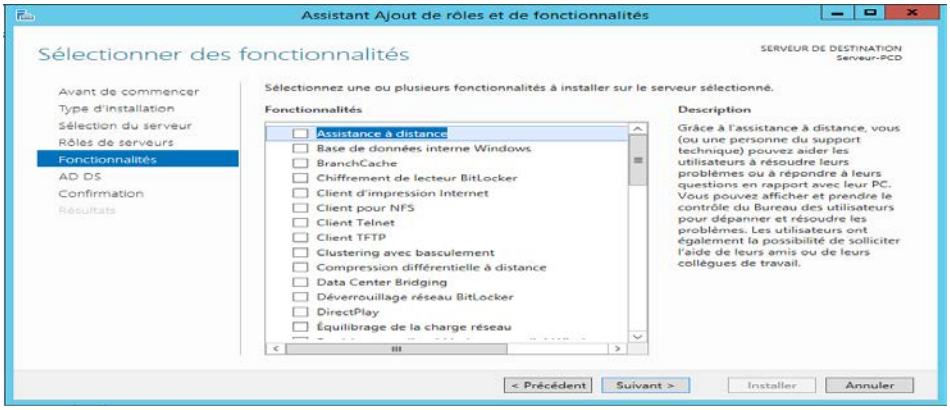


Figure B.5: Illustration 2

Figure B.6: Illustration 3

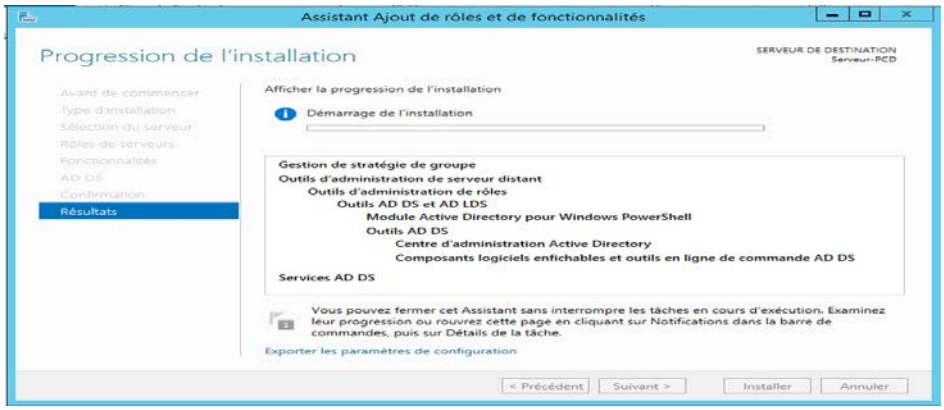


Figure B.7: Début de l'installation de l'Active Directory

Figure B.8: Fin d'installation d'AD DS

Les figures suivantes montrent la création du domaine contrôleur principal.

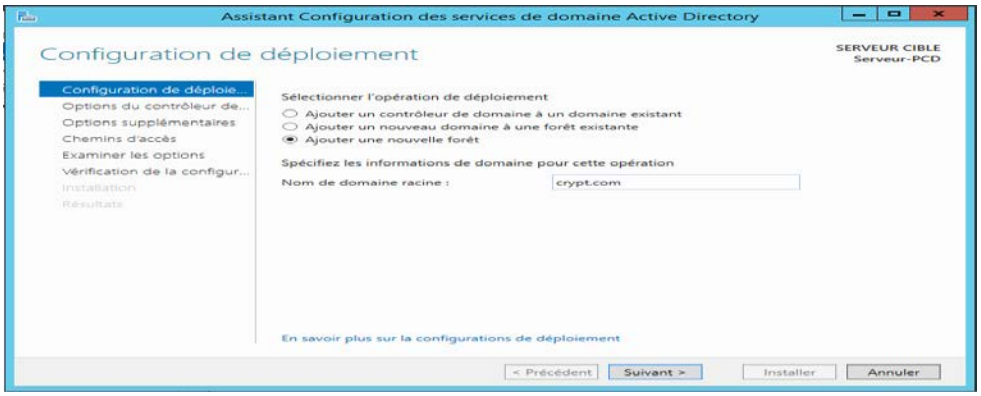


Figure B.9: Un nom pour le domaine

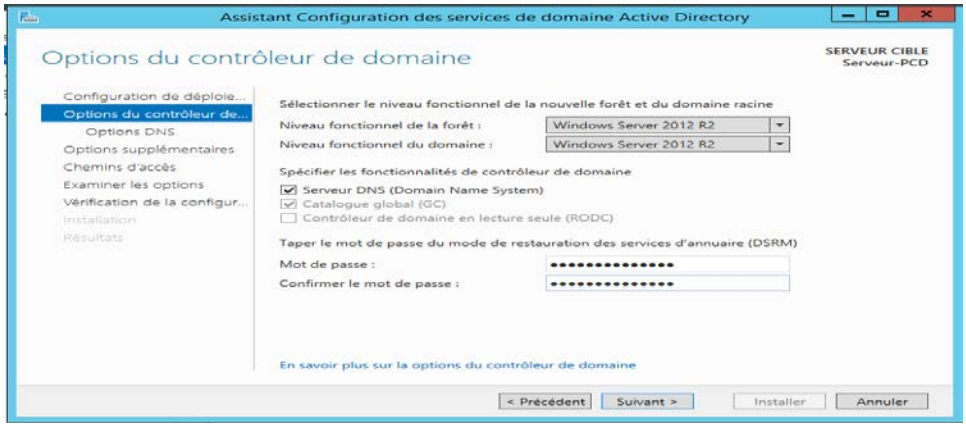


Figure B.10: Mot de passe

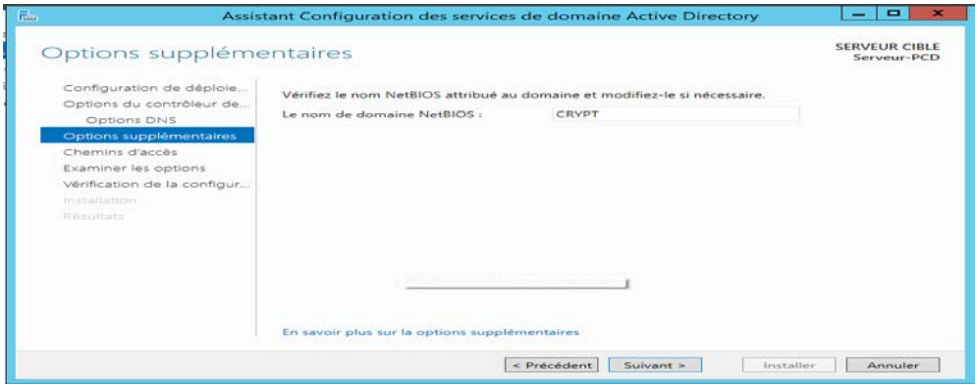


Figure B.11: Nom de domaine NetBIOS

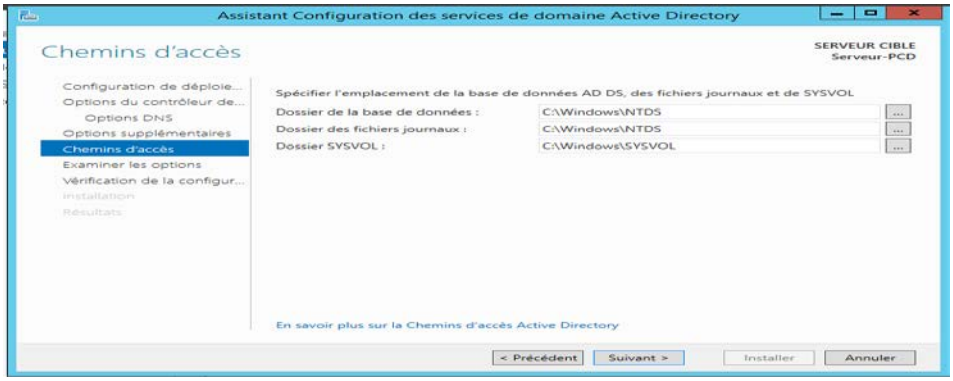


Figure B.12: Emplacement de la base de données d'AD DS

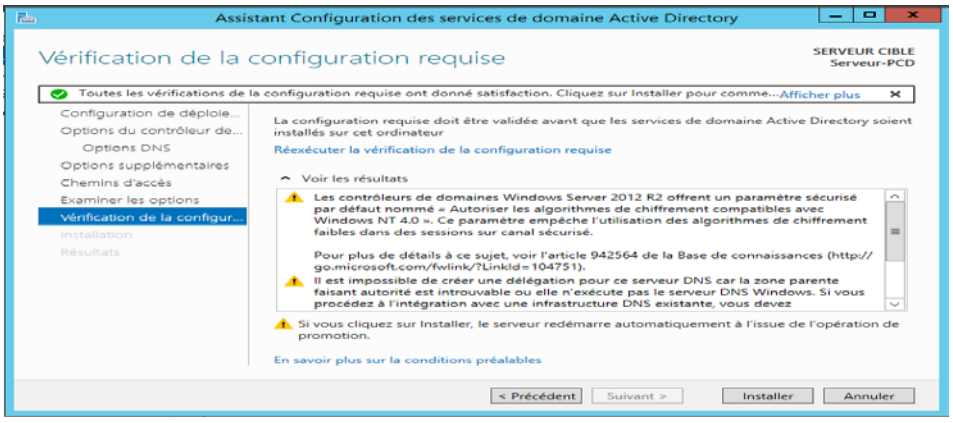


Figure B.13: Un récapitulatif de la configuration d'AD DS

Après la vérification de la configuration est valide on clique sur Installer pour finir l'installation des services de domaine d'Active Directory.

La figure suivante montre qu'AD DS et DNS sont installés.

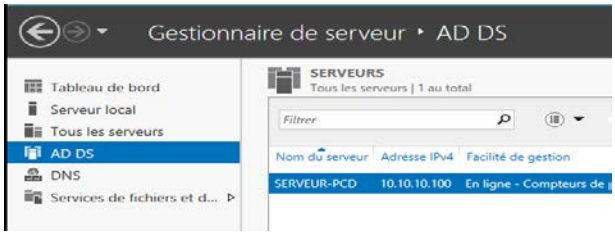


Figure B.14: AD DS et DNS installer

B.3.Configuration d'une zone de recherche inversé pour DNS

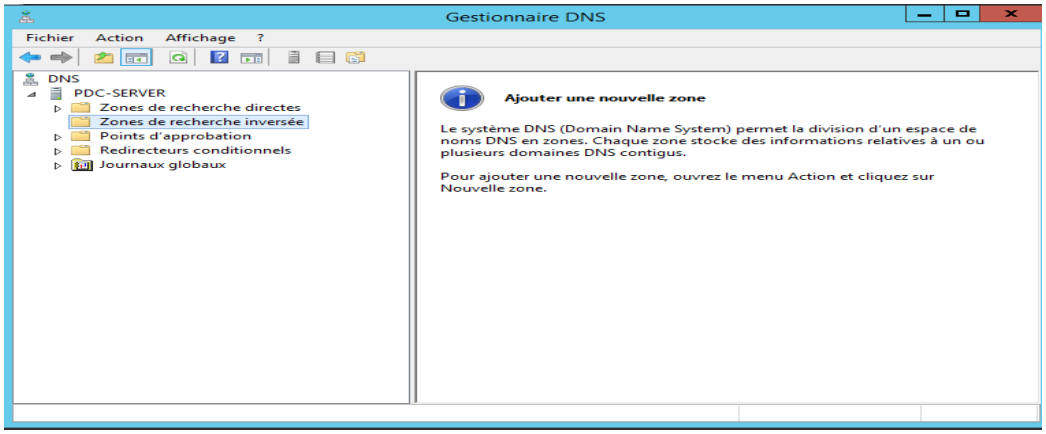


Figure B.15: Interface du gestionnaire DNS

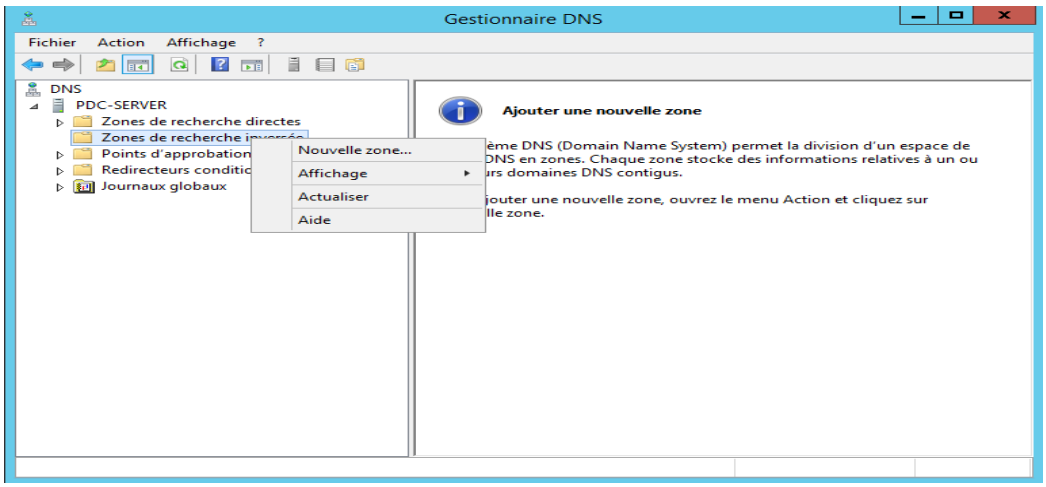


Figure B.16: Création d'une nouvelle zone inversée

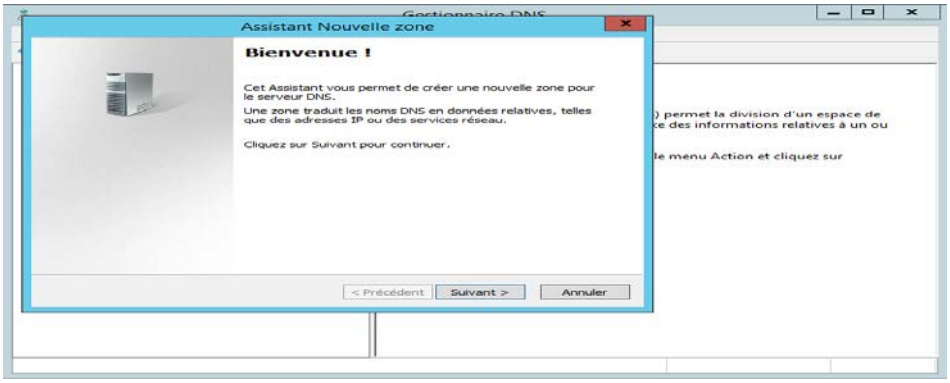


Figure B.17: Assistant nouvelle zone

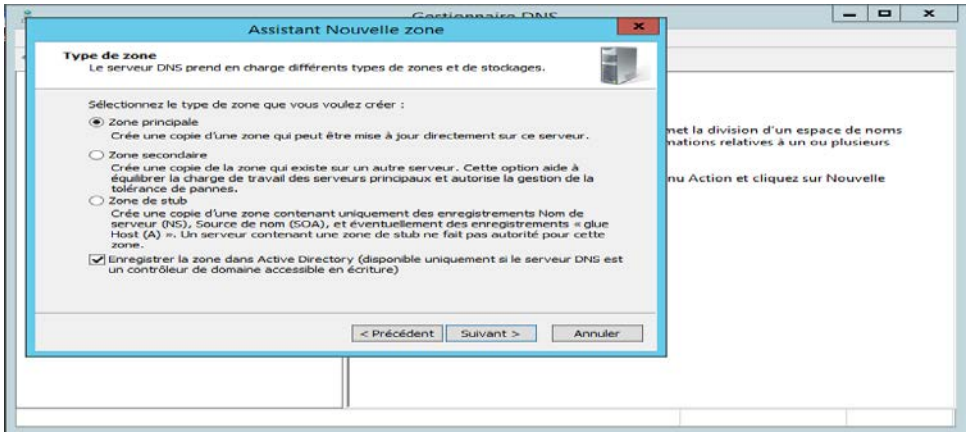


Figure B.18: Type de la zone

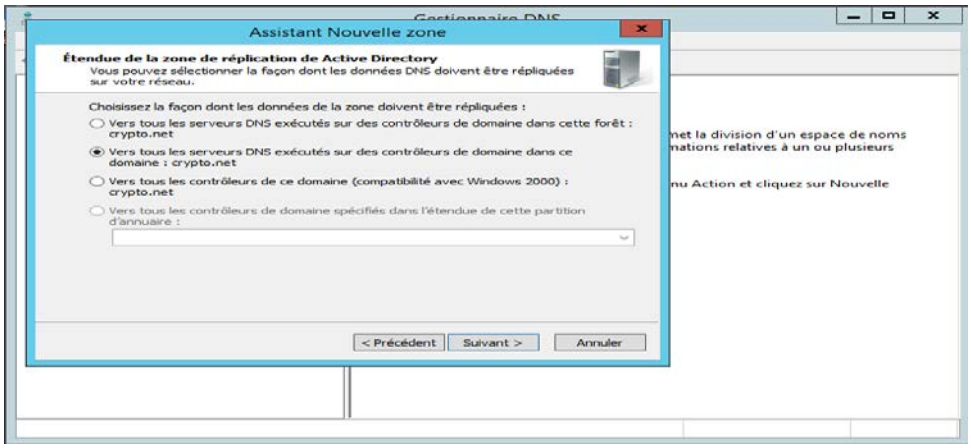


Figure B.19: Etendue de la zone

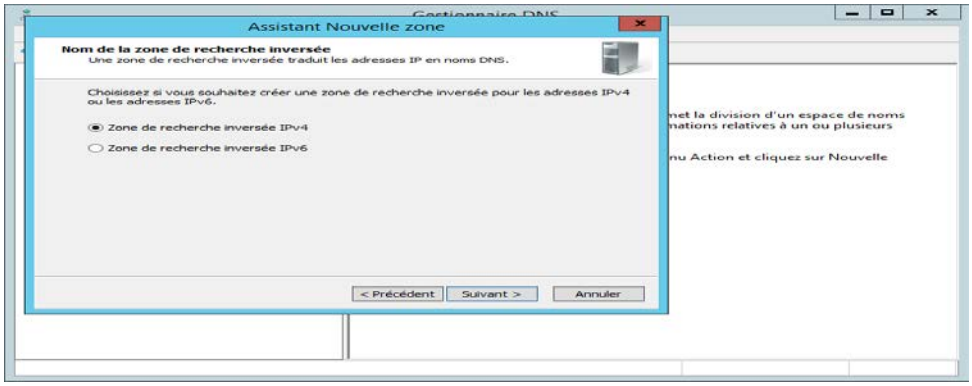


Figure B.20: Type de l'IP

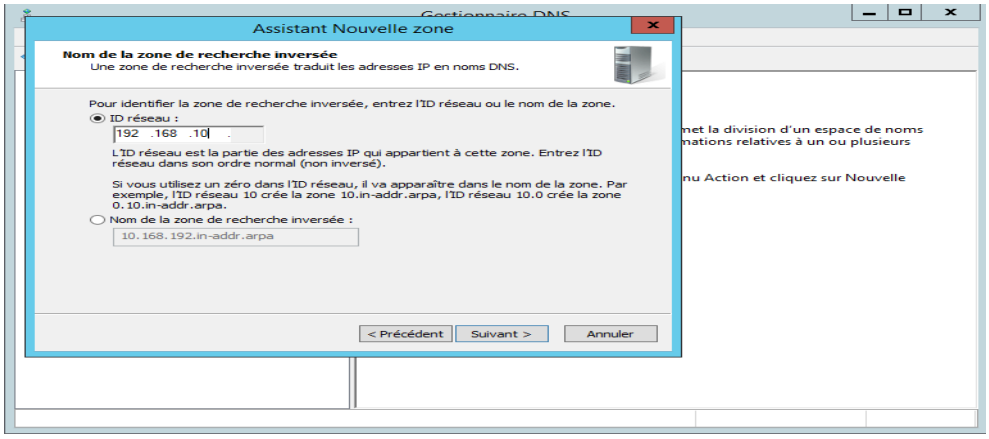


Figure B.21: Saisi de l'ID de réseau

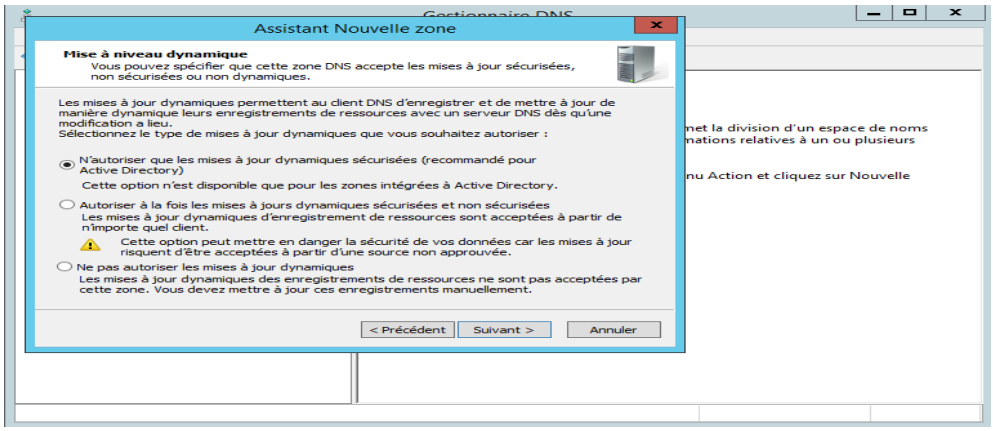


Figure B.22: Mises à jour dynamiques automatiques

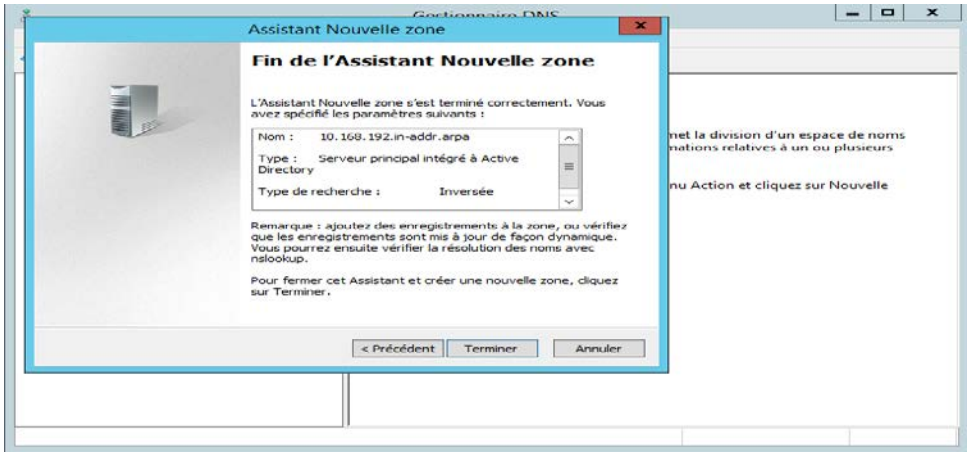


Figure B.23: Fin de l'assistant nouvelle zone

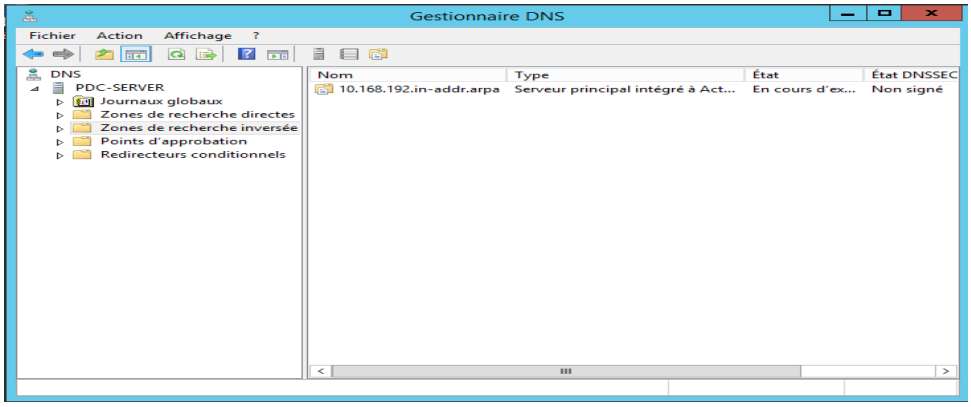


Figure B.24: Nouvelle zone de recherche est crée

C.1. Installation de la TMG

Au lancement du programme d'installation en obtient la fenêtre suivante :

Figure C.1: Lancement de l'installation de la TMG

Le processus d'installation est subdivisé en trois étapes :

- ✓ **Etape 1:** Exécuter Windows Update cela permettra d'installer les dernières mises à jour.
- ✓ **Etape 2:** Exécuter l'outil de préparation pour installer l'ensemble des Pré-requis nécessaires pour le déploiement de la plate-forme TMG comme suit :

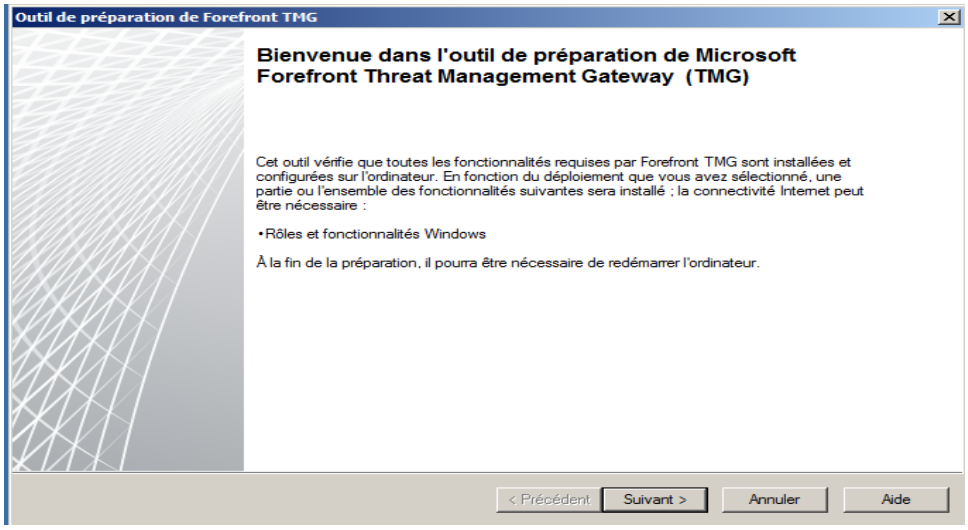


Figure C.2: Lancement de l'exécution des outils de préparation.

Apres avoir cliqué sur suivant nous choisissons d'installer les services et fonctionnalités de TMG et la console de gestion.

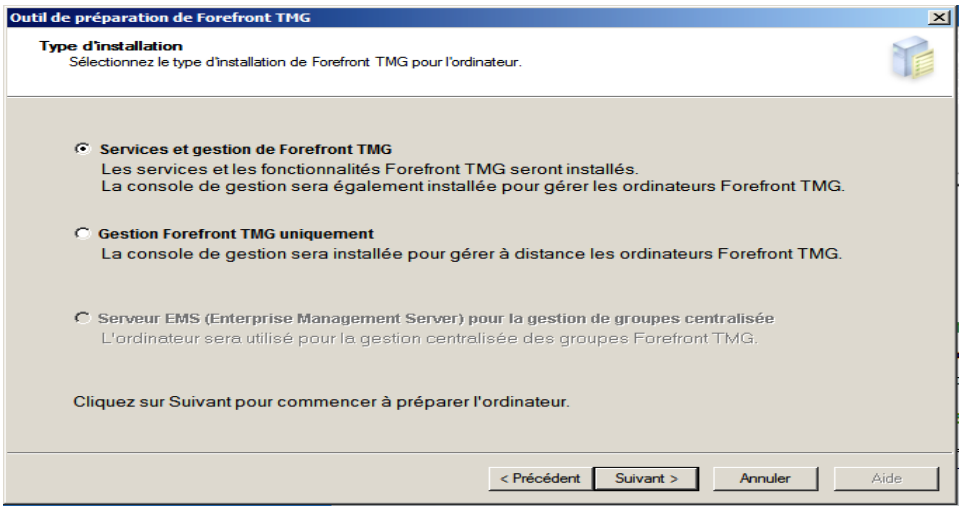


Figure C.3: Le choix des fonctionnalités de la TMG.

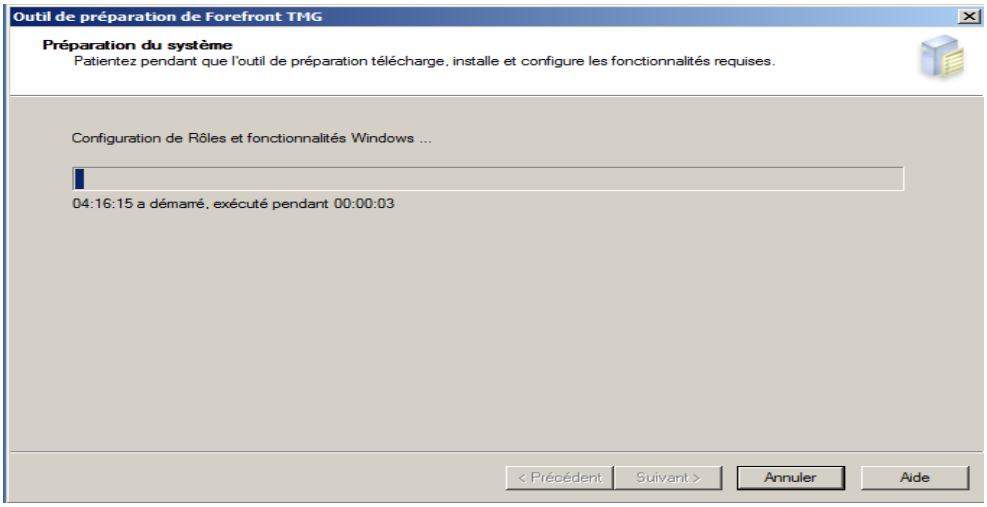


Figure C.4: Préparation des outils.

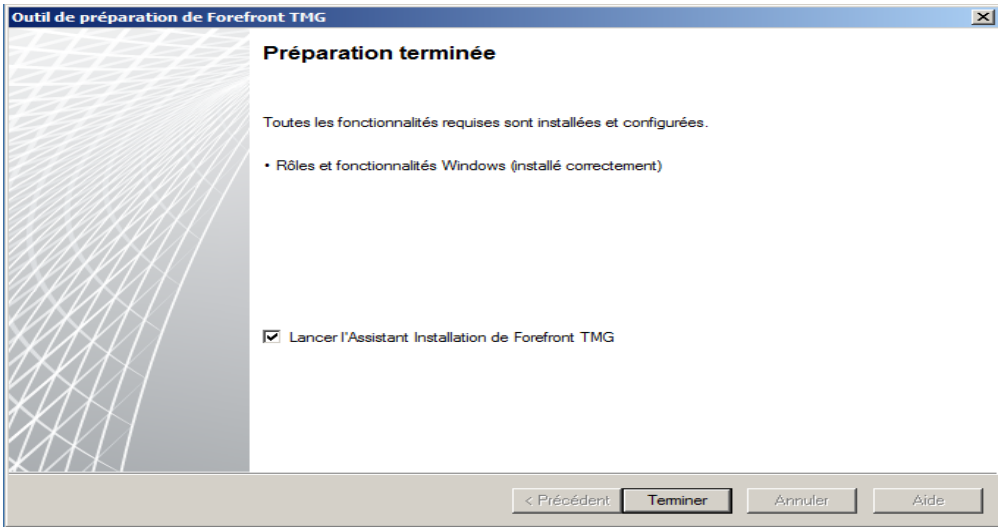


Figure C.5: Fin de préparation des outils et lancement d'assistant d'installation de la TMG

Voici la liste des rôles et fonctionnalités TMG qui seront activés après l'exécution de la deuxième étape :

- Network Policy Server.
- Routing and Remote Access Services.
- Active Directory Lightweight Directory Service Tools.
- Network Load Balancing Tools.
- Windows PowerShell.
- Microsoft .NET Framework 3.5 SP1.
- Windows Web Services API.
- Microsoft Windows Installer 4.5.
- Microsoft Chart Controls for Microsoft .NET Framework 3.5 and 3.5 SP1.

✓ **Etape 3 :** Exécuter l'assistant d'installation.

Après le lancement de l'assistant d'installation nous obtenons la figure suivante :

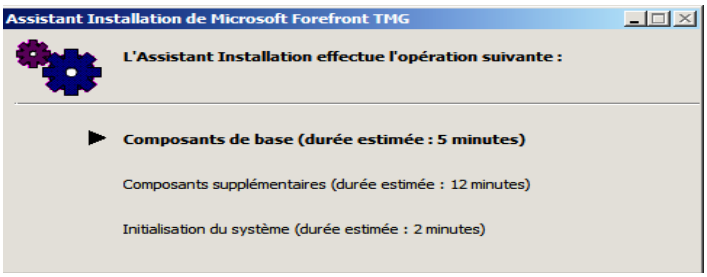


Figure C.6: Assistant d'installation de la TMG.

Pour valider la licence du produit il nous ait demandé d'introduire le nom de l'utilisateur et la compagnie.

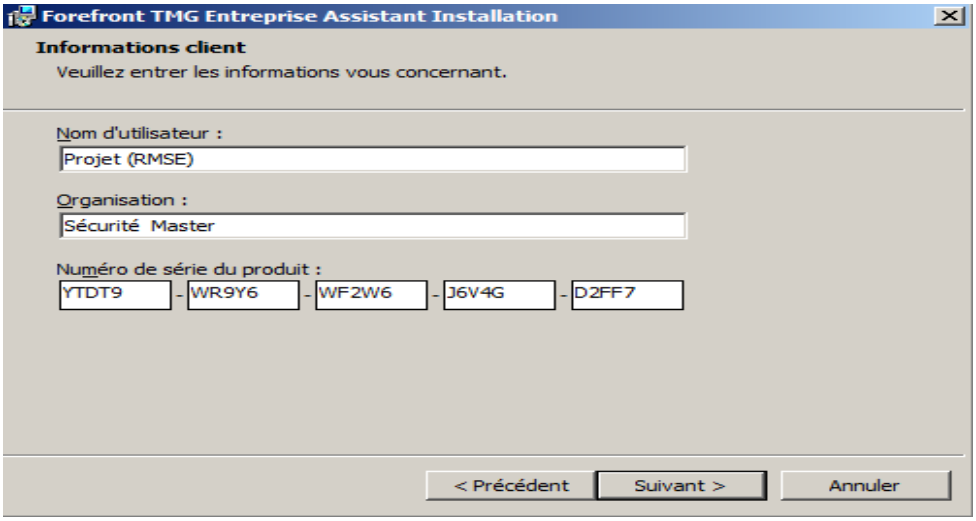


Figure C.7: Validation de la licence.

Le produit étant validé, il nous ait demandé d'ajouter les cartes réseau. Après la sélection de la carte interne les plages d'adresse de celle-ci seront calculées et listées il ne reste plus qu'à valider.

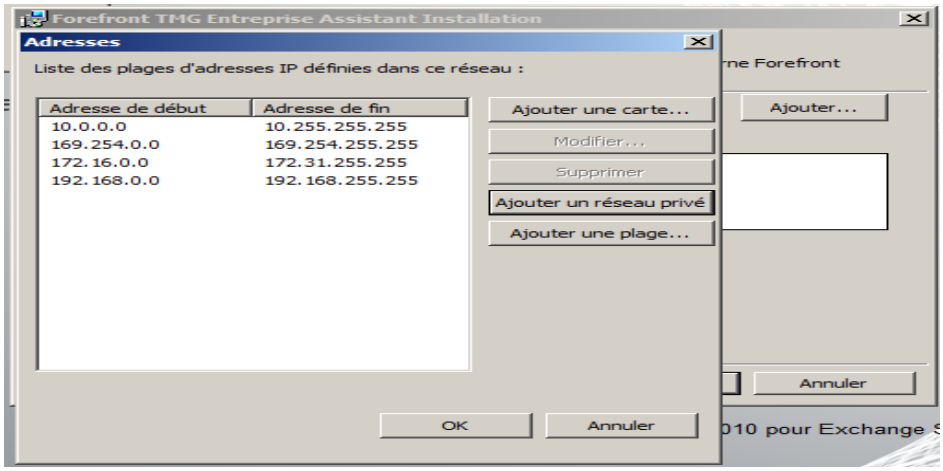


Figure C.8: Liste de la plage des valeurs.

A la fin de l'installation de Forefront TMG, nous pouvons lancer la gestion de la TMG.

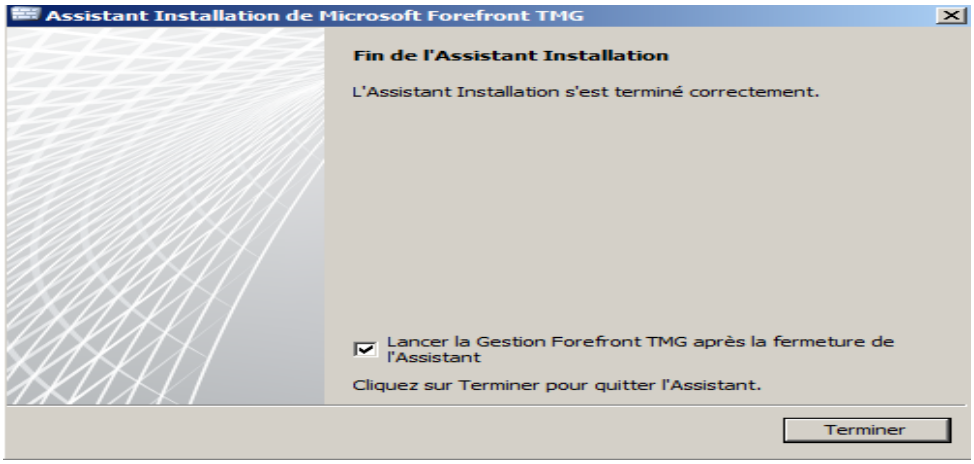


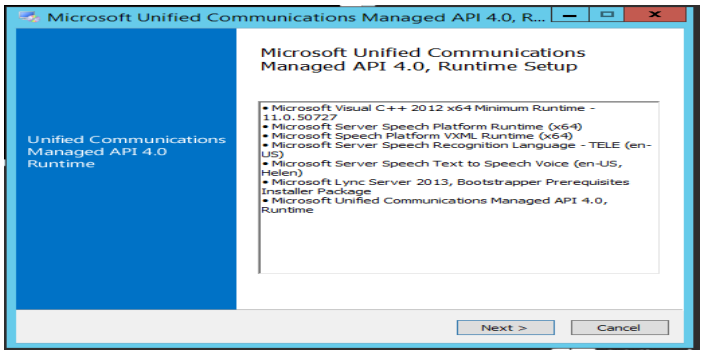
Figure C.9: Fin d'assistant d'installation

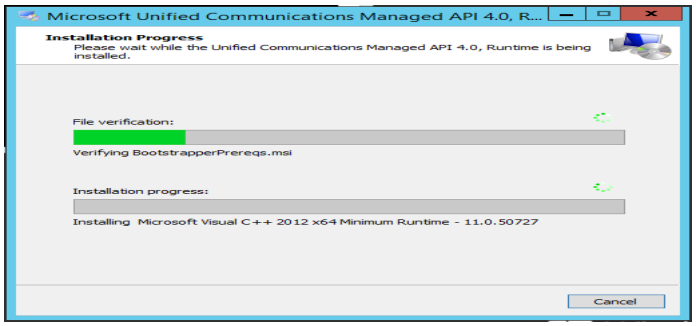
C.2. Installation et configuration du Server Exchange 2013

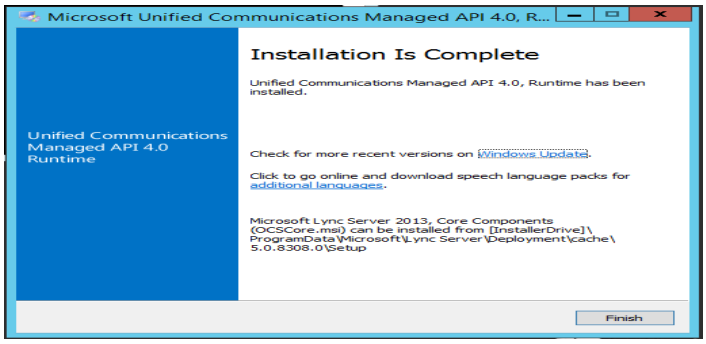
Figure C.10: Préparation de schéma Active Directory

Avant de passer a l'installation de l'Exchange on dois installer on dois installer ces trois pack dans l'ordre suivant:

Pack 1

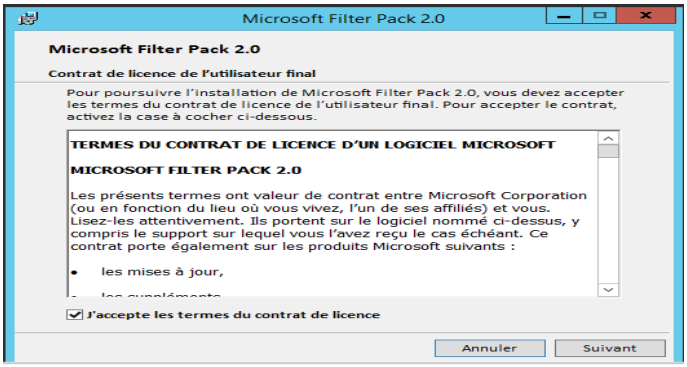


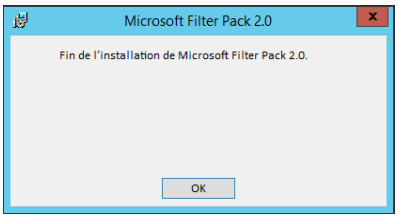




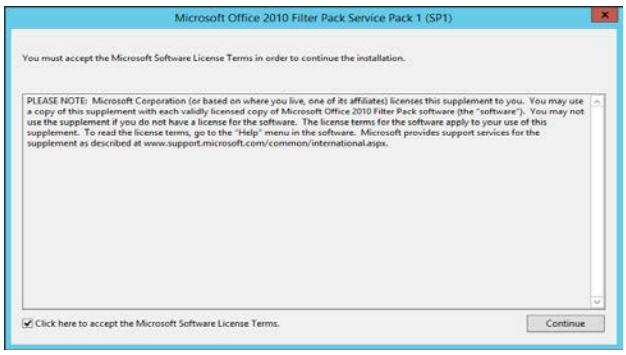
Pack 2

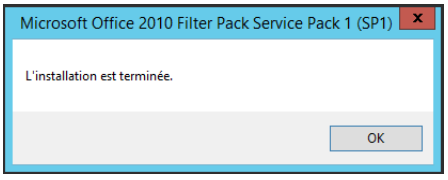

Microsoft Filter Pack 2.0
Bienvenue dans l'Assistant Installation de Microsoft Filter Pack 2.0
Le programme d'installation vous guide tout au long des étapes requises pour installer Microsoft Filter Pack 2.0 sur l'ordinateur.
Ce logiciel est protégé par la loi relative au droit d'auteur et par les conventions internationales. Toute reproduction ou distribution partielle ou totale du logiciel, par quelque moyen que ce soit, est strictement interdite. Toute personne ne respectant pas ces dispositions se rendra coupable du délit de contrefaçon et sera passible des sanctions pénales prévues par la loi.
Annuler
Suivant


Microsoft Filter Pack 2.0
Microsoft Filter Pack 2.0
Contrat de licence de l'utilisateur final
Pour poursuivre l'installation de Microsoft Filter Pack 2.0, vous devez accepter les termes du contrat de licence de l'utilisateur final. Pour accepter le contrat, activez la case à cocher ci-dessous.
TERMES DU CONTRAT DE LICENCE D'UN LOGICIEL MICROSOFT
MICROSOFT FILTER PACK 2.0
Les présents termes ont valeur de contrat entre Microsoft Corporation (ou en fonction du lieu où vous vivez, l'un de ses affiliés) et vous. Lisez-les attentivement. Ils portent sur le logiciel nommé ci-dessus, y compris le support sur lequel vous l'avez reçu le cas échéant. Ce contrat porte également sur les produits Microsoft suivants :
les mises à jour,
J'accepte les termes du contrat de licence
Annuler
Suivant


Microsoft Filter Pack 2.0
Fin de l'installation de Microsoft Filter Pack 2.0.
OK

Pack 3


Microsoft Office 2010 Filter Pack Service Pack 1 (SP1)
You must accept the Microsoft Software License Terms in order to continue the installation.
PLEASE NOTE: Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. You may use a copy of this supplement with each validly licensed copy of Microsoft Office 2010 Filter Pack software (the "software"). You may not use the supplement if you do not have a license for the software. The license terms for the software apply to your use of this supplement. To read the license terms, go to the "Help" menu in the software. Microsoft provides support services for the supplement as described at www.support.microsoft.com/common/international.aspx.
Click here to accept the Microsoft Software License Terms.
Continue


Microsoft Office 2010 Filter Pack Service Pack 1 (SP1)
L'installation est terminée.
OK

Nous sommes maintenant prêt pour installer Exchange Server 2013. Rendez-vous dans les sources et ouvrez le **setup.exe**. Dans un premier temps nous allons vérifier les mises à jour logiciel de Exchange.

Figure C.11: Vérifier les mises à jour

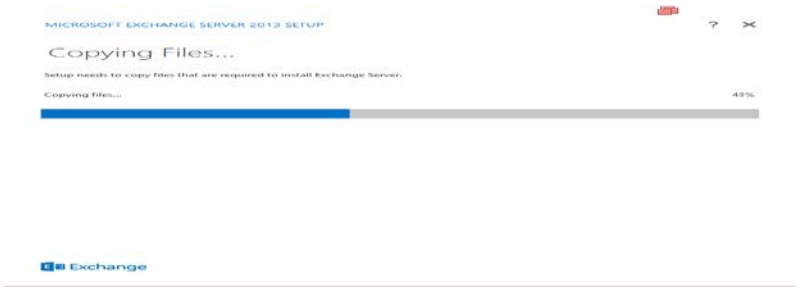


Figure C.12: La copie des fichiers

Après la copie des fichiers est terminée, on cliquez sur Next. On arrive sur une page d'introduction :

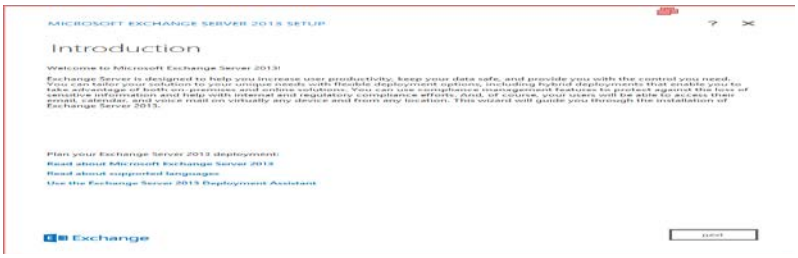


Figure C.13: Introduction

Figure C.14: On accepte ensuite la licence

On arrive maintenant sur la page de sélection d'installation des rôles. Dans notre cas on a choisi d'installer les 2 rôles sur ce serveur. A noter que sur Exchange Server 2013, nous avons que 2 rôles disponibles.

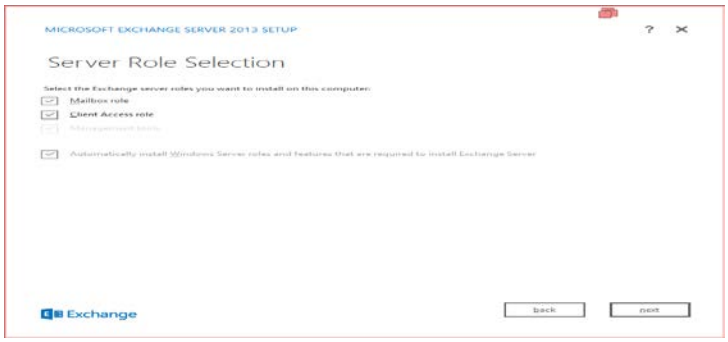


Figure C.15: Sélection des rôles

Les illustrations qui suivent montrent l'avancement de l'installation du Serveur Exchange 2013.

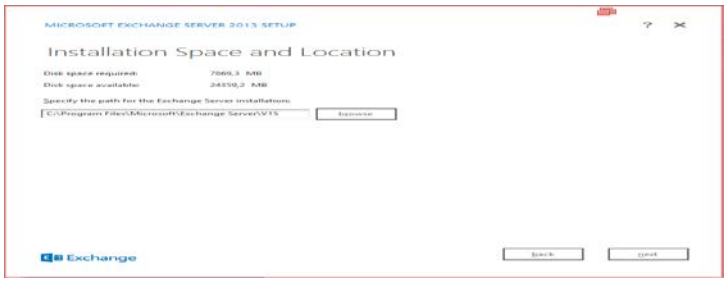


Figure C.16 : Illustration 1

Figure C.17 : Illustration 2

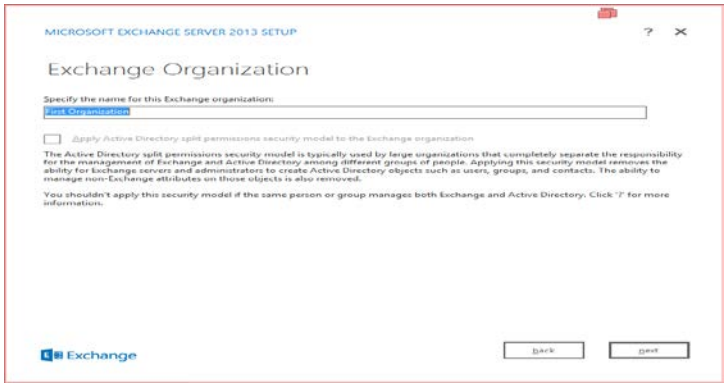


Figure C.18 : Illustration 3

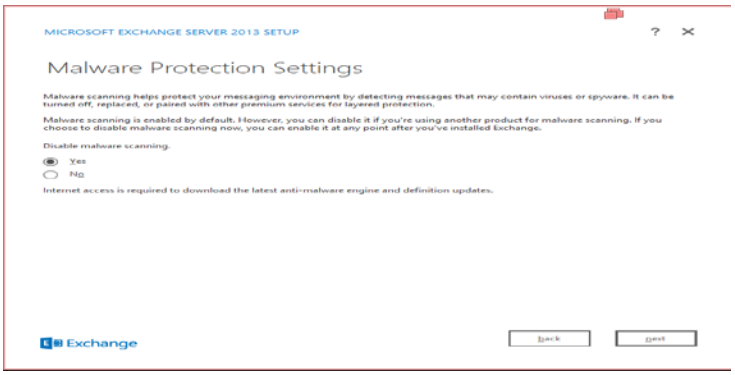


Figure C.19 : Illustration 4

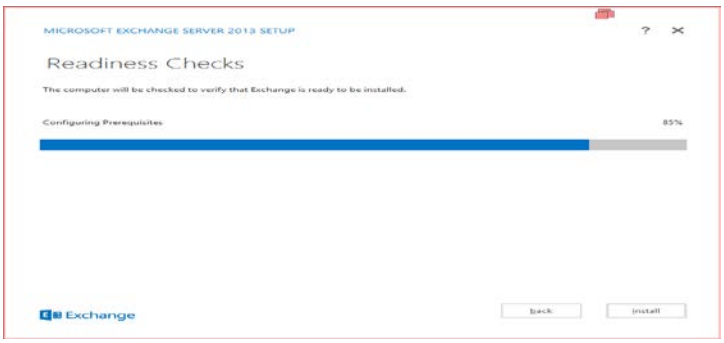


Figure C.20 : Illustration 5

Figure C.21 : Illustration 6

C.3. Installation de serveur Web IIS

Le serveur Web IIS fournit une infrastructure d'application web fiable et gérable et évolutive, pour l'ajouter comme fonctionnalité sous le contrôleur de domaine principal, aller au menu démarrer -> outil d'administration -> gestionnaire de serveur, et l'ajouter comme rôle, les figures suivantes illustrent la procédure.

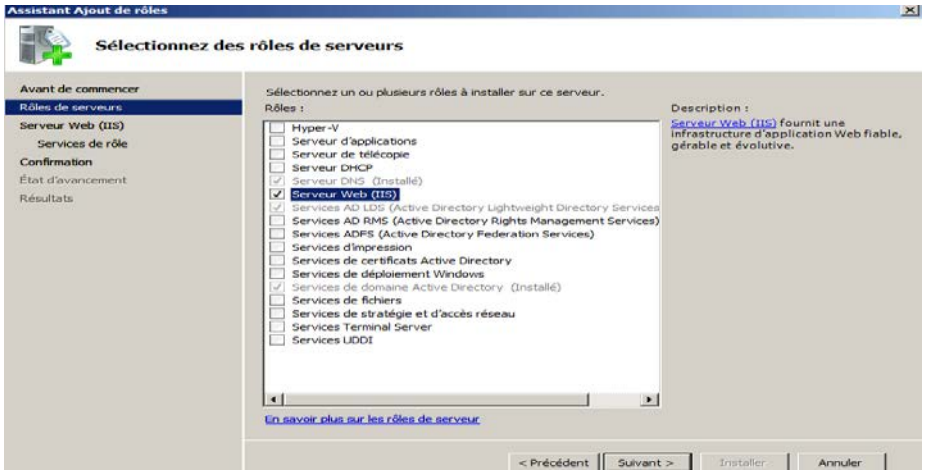


Figure C.10: Illustration 1

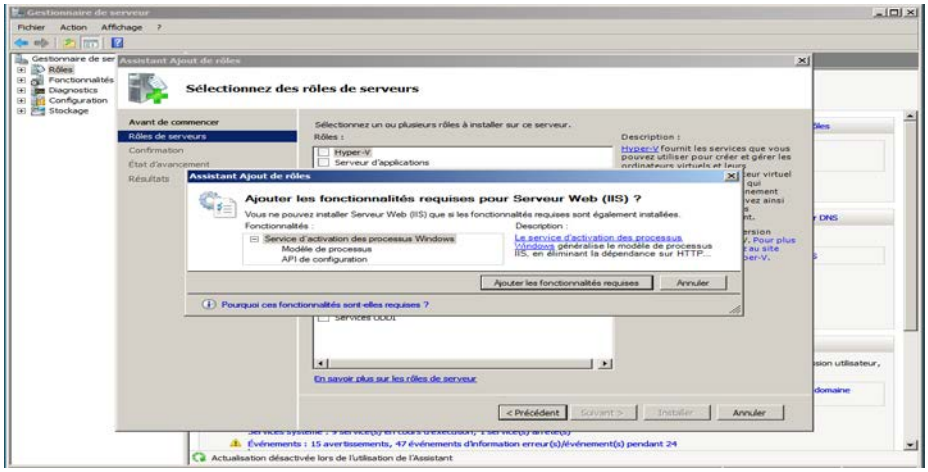


Figure C.11: Illustration 2

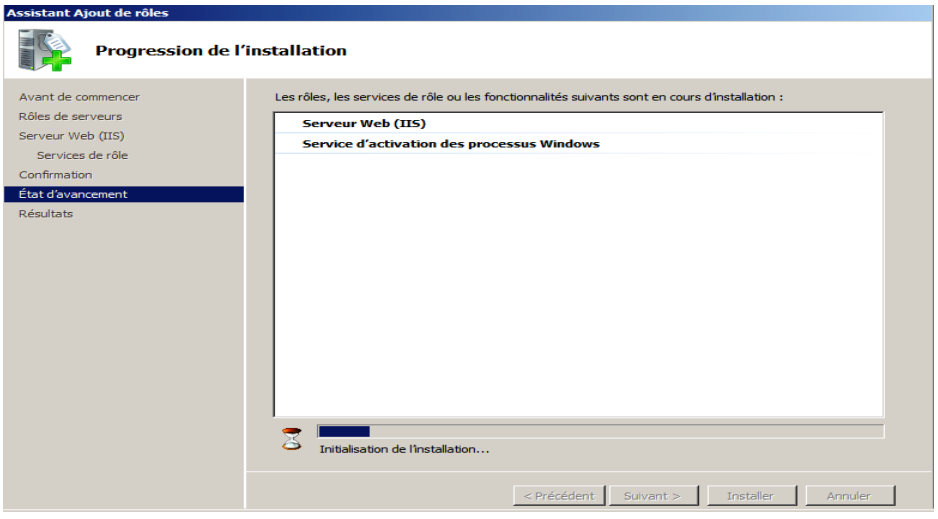


Figure C.12: Illustration 3

Bibliographie

Documents écrits

[1]: C.Llorens, L.Levier,D.Valois , Tableaux de bord de la sécurité réseau2eme edition,PARIS2006.

[2] : Cours sécurité réseaux M1 (Cours MR Daoui)

[3] : Tableaux de bord de la sécurité réseaux 2ème édition EYROLLES

[4] *:* Abdoul Karim Ganamé - Doctorant en sécurité informatique

[5] : Sécurité Informatique / Attaques Informatique : Jean-Olivier Gerphagnon & Marcelo Portes de Albuquerque

[6] : les attaques internet (DESS IIR) Cyrille Duret & Nathalie Gaillard

[7] : les attaques internet (DESS IIR) Cyrille Duret & Nathalie Gaillard

[8] : Hacking Interdit Auteurs Alexandre GOMEZ-URBINA, Micro Application 1ère Édition

[9] : Bruce Schneider, Cryptographie Appliquée. 2eme édition, 2001.Vulbert.

[10] : Philippe PERRET ,Cryptographie .Feverier, 2007.

[11] : Michel Riguidel, Sécurité informatique et reseaux, PARIS 2006.

[12] : T.ebrahimi , F.Leprévost, B.Warusfel , Cryptographie et securité des systesmes et reseaux ,January 2006.PARIS

[13] : Bruno Martin, Codage, Cryptograhie et Applications.1^{ere} édition, 2004.Presses polytechniques et Universitaires Romandes.

[14] : Françoise levy, Cryptographie moderne,Ecole Nationale Superieure des thecniques avancées.

[15] : A. Oulamara & G.Ouarezki ,Conception et réalisation d'une application de cryptage basé sur les reseaux de feistel. These de Master, Tizi Ouzou,2012.

[16] : C.Chebli, Signature et chiffrement, These de doctorat ,LIBAN 2003.

[17] : Pascal Lafourcade, Vérification de protocoles cryptographiques en présence de théories équationnelles, Thèse de Doctorat ÉCOLE NORMALE SUPÉRIEURE DE CACHAN,Septembre 2006.

[18] : T.Peyrin, Analyse de fonctions de hachage cryptographiques, Thèse de Doctorat ENS, Versailles, novembre 2008.

Webgraphie

[19]: http://www.frameip.com/tcpip/

[20] : http://www.securiteinfo.com/conseils/introsecu.shtml

[21] : http://securiteinformartique.wordpress.com/2011/11/12/les-types-de-piratage/

http://www.lefaso.net/spip.php?article12772

[22] : http://www.commentcamarche.net/contents/attaques/

[23] : http://www.inetdoc.net/guides/tutoriel-secu/tutoriel.securite.attaquesprotocoles.dhcp.html

[24]:http://www.isikef.rnu.tn/francais/pages/cours/mehrez%20boularess/td2%20ids%20corrige.pdf

[25] : http://www.2stop.me/Ezines/secuinfo/numero%205/numero05.html

[26] : http://www.commentcamarche.net/contents/1033-introduction-a-la-securite-informatique

[27] : http://ram-0000.developpez.com/tutoriels/cryptographie/

[28] : http://fr.wikipedia.org/wiki/Chiffre_ADFGVX

[29] : http://fr.wikipedia.org/wiki/Mode_d%27op%C3%A9ration_%28cryptographie%29

[30] : http://www.commentcamarche.net/contents/212-signature-electronique

Résumé

Notre étude consiste à faire les testes de pénétration d'un réseau avec implémentation de sécurité pour quelques failles étudier en essayant de préserver le réseau des différentes attaques.
Pour mieux comprendre le sujet, nous allons d'abord parler dans le 1er chapitre réseaux informatiques et les différentes attaques, on détaillera dans le 2éme chapitre les bases de teste de pénétration, et dans le 3éme chapitre on propose les solutions de sécurité, Enfin, dans le dernier chapitre, on illustrera les différentes fonctionnalités de notre application avec des captures d'écran.