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

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master en Electronique

Option : Réseaux et télécommunication

Thème :

Sécurisation d'une infrastructure DMZ avec ASA 5510

Proposé et dirigé par :

Mr. LAHDIR Mourad

Mr. MAMOU Amar

Présenté par :

M^{lle} .ABTOUT Nadjia

M^{lle}. DOUANI Dalila

Année universitaire 2012/2013

REMERCIEMENTS

En premier lieu nous remercions notre **DIEU** le tous puissant de nous avoir donné la foi, la santé et nous à permit de bien mener ce travail.

Avant d'entreprendre la rédaction de notre mémoire, nous souhaitons vivement remercier et exprimer notre gratitude à

:

Notre promoteur **Mr LAHDIR Mourad,** à qui nous sommes très reconnaissants pour ses remarques et ses conseilles.

Notre profonde gratitude et sincères remerciements à notre encadreur

Mr MAMOU Amar pour son suivi, sa disponibilité et ses orientations.

Nous tenons à exprimer nos reconnaissances et notre sincère gratitude à tous les enseignants de bonne foi qui nous ont accompagnés durant notre formation.

Sans oublier de remercier Toute la promotion ELN 2012/2013

qui nous ont aidé, et contribuer, de pré et de loin à la réalisation de ce modeste travail.

NADJIA, DALILA

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents qui m'ont soutenu tout au long de mes études et qui ont contribué à ma réussite, que dieu les garde et leur donne une longue vie.

Mes chers frères Sofiane et Nacer qui m'ont aidé tout au long de ce travail.

Mon petit frère Jugurtha et ma sœur Nacera que j'aime beaucoup et à qui je souhaite une bonne réussite dans leurs études et dans leurs vies.

Toute ma famille ABTOUT et mes amis.

Tous ceux qui m'aime et que j'aime que je n'ai pas cité, mais que je n'ai pas oublié.

Mes cher binôme DALILA et sa famille, à qui je souhaite une bonne réussite.

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents qui m'ont soutenu tout au long de mes études et qui ont contribué à ma réussite, que dieu les garde et leur donne une longue vie.

Mes chers frères qui m'ont beaucoup conseillé et aidé tout au long de ce travail.

Mes sœurs Baya et Rachida qui m'ont soutenu tout au long de mon parcours.

Mes neveux et mes nièces

Toute ma famille et mes amis surtout Lynda.

Toute la promotion ELN 2012/2013.

Ma chère binôme NADJIA et toute sa familles, à qui je souhaite une bonne réussite.

Chapitre III: La pratique

Bien que les réseaux aient tous un trait commun, qui est le partage des données et des ressources entre leurs utilisateurs, chaque réseau est unique en raison des protocoles utilisés, des services offerts, de son emplacement physique, du milieu dans lequel il est utilisé et de sa configuration. Pour cette raison, il ne peut pas y avoir de solutions universelles qui répondent aux exigences de tous les réseaux en matière de sécurité. Ces solutions doivent plutôt répondre aux besoins particuliers de chaque réseau. Si on met en œuvre des mesures de sécurité pour un réseau, sans avoir comprendre les besoins précis pour de telles contre mesures et les avantages que le réseau en retirera. On dépensera de l'argent pour rien.

La décomposition du réseau en zones de sécurité séparées est l'une des solutions les plus fiables qu'une entreprise peut adapter pour la protection de ses ressources matérielles et logicielles. Elle est un moyen de luter contre la violation potentielle du système de sécurité et les attaques contre la confidentialité. La bonne gestion de cette zone permet de minimiser les attaques venant du réseau externe, en autorisant les services dont l'entreprise a besoin. Cette décomposition appeler DMZ (zone démilitarisé) nécessite la mise en place d'un firewall pour pouvoir administrer cette zone.

L'ASA 5500 séries est l'une des solutions proposée par Cisco. Il met à la disposition de l'entreprise une gamme complète de services personnalisés, à travers ses diverses éditions conçues spécifiquement pour le pare-feu. Ces différentes éditions offrent une protection de qualité supérieure, en apportant à chaque installation les services dont elle a besoin à savoir la prévention des intrusions, la protection des contenus et les VPN,…etc.

L'objectif de ce mémoire est de sécurisé une infrastructure DMZ à l'aide de l'ASA Cisco 5510 en créant une stratégie de filtrage pour gérer le trafic entre les réseaux de l'entreprise et le réseau externe (Internet). Il se divise en trois chapitres;

Le premier chapitre présente des généralités sur la sécurité des réseaux informatiques; types de menaces, méthodes de protection,…etc.

Dans le deuxième chapitre, nous exposerons un réseau dépourvu d'une DMZ ; les critiques du réseau existant, solution proposé,…etc.

Le troisième chapitre sera consacré à l'application sur la création de la zone démilitarisé (DMZ) et la configuration de l'ASA Cisco 5510, Nous terminerons par une conclusion générale.

I.1. Préambule

Les réseaux dominent le monde informatique, les grandes entreprises ne peuvent plus survivre sans que leurs machines soient connectées à un réseau étendu (WAN ou Internet).

La sécurité d'un réseau est un niveau de garantie pour que l'ensemble des machines ce dernier fonctionnent d'une façon optimale. En conséquence, la mise en œuvre de la sécurité est indispensable au sein d'un réseau afin de le protéger de toute sorte d'intrusion malveillante.

Dans ce chapitre nous allons présenter des notions générales sur la sécurité des réseaux informatiques.

I.2. Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements informatique et d'autre dispositifs interconnecter entre eux afin d'échanger des informations et partager les ressources matériels et logiciels.

I.3. Architecture des réseaux

Les réseaux sont structurés du point de vue fonctionnel en deux catégories: réseaux poste à poste et réseaux à serveur dédié (client / serveur).

I.4. Classification des réseaux informatiques

On peut classer les réseaux selon plusieurs critères, par exemple la distance entre entités communicantes, la topologie et le type d'accès

- **Classification selon la taille**
  - Les réseaux locaux LAN (Local Area Network)
  - Les réseaux MAN (Métropolitain Area Network)
  - Les réseaux étendus WAN (Wide Area Network)
- **Classification selon la Topologie**
  - Topologie en bus
  - Topologie en anneau
  - Topologie en étoile

- **Classification selon la méthode d'accès**
  - ü Méthode d'accès CSMA/CD
  - ü Méthode d'accès par Token ring
  - ü Méthode d'accès par Standard FDDI
- **Classification selon le mode de connexion**
  - ü Mode avec connexion
  - ü Mode sans connexion

I.5. Les protocoles réseaux

- **Protocole DNS (Domaine Name Service)**: Est Une base de données utilisée sur les réseaux IP pour transposer les noms d'ordinateurs en adresse IP.
- **Protocole TCP (Transmission contrôle Protocol):** Est un protocole fiable, orienté connexion qui permet l'acheminement sans erreur de paquets issues d'une station à une autre.
- **Protocole ICMP(Internet Control Message Protocol):** Est un protocole qui permet le contrôle des erreurs de transmission. En effet, comme le protocole IP ne gère que le transport des paquets et ne permet pas l'envoi de messages d'erreur, c'est grâce à ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau.
- **Protocole DHCP (Dynamic Host Configuration Protocol):** Est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut.
- **Protocole POP3:** Est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique. Cette opération nécessite une connexion à un réseau TCP/IP. Le port utilisé est le **110**
- **FTP (File Transfert Protocol):** Permet de transférer des fichiers d'une machine à une autre. L'utilisation de FTP depuis un poste client pour aller chercher ou déposer un fichier sur un serveur nécessite de la part de l'utilisateur de se connecter avec un nom et un mot de passe .donc si l'utilisateur n'est pas reconnu la connexion ne sera pas établie.

- **SMTP (Simple Mail Transfer Protocol)**: Est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique. Il est assez facile de tester un serveur SMTP en utilisant le port **25.**
- **HTTP (Hyper Text Transfer Protocol**): Est le protocole de communication du web permettant d'échanger des documents hyper textes contenants des données sous la forme de texte, d'image fixes ou animées et de sons. Tout client web communique avec le port **80** d'un serveur http.
- **Protocole Telnet**: Le protocole Telnet est un protocole standard d'internet permet de relier les interfaces de terminaux et d'applications à travers internet. Il s'appuie sur une connexion TCP sur le port **23** pour envoyer des données.
- **SNMP** (**Simple Network Management Protocol**): est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
- **TFTP** (**Trivial File Transfer Protocol** ou **Protocole simplifié de transfert de fichiers**) : est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP. TFTP reste très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feu, etc.) ou pour démarrer un PC à partir d'une carte réseau.

Pour assurer le bon fonctionnement du réseau et faire face aux menaces éventuelles qui peuvent le mettre hors service il est nécessaire de le sécurisé. Pour cela nous allons présenter des notions sur la sécurité des réseaux informatiques dans le but de se familiariser avec les différentes menaces.

I.6. Définition de sécurité

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles, ce qui implique la réalisation les fonctions essentielles suivantes:

- Ø Disponibilité: demande que l'information soit **disponible** aux personnes autorisées.
- Ø Confidentialité: demande que l'information sur le système ne puisse être **lue** que par les personnes autorisées.
- Ø Intégrité: demande que l'information sur le système ne puisse être **modifiée** que par les personnes autorisées.

- Ø Non répudiation: permet de garantir qu'une transaction ne peut être **niée**.
- Ø Authentification: garantit l'identité des correspondants ou des partenaires qui communiquent.

I.7.Politique de sécurité

La politique de sécurité définit un certain nombre de règles ,de procédures et une bonne pratique permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation. Elle a pour objectif:

- ü D'identifier les besoins en temps de sécurité, les risques informatiques et leurs éventuelles conséquences.
- ü D'élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiées.
- ü De surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériel utilisés.
- ü De définir les actions à entreprendre et les personnes à contacter on cas de détection d'une menace.

I.8. Type de menaces

Les menaces sont considérées comme une violation potentielle du système de sécurité, elles viennent d'individus compétents à cause des vulnérabilités de système de sécurité.

I.8.1. Les menaces accidentelles: Les menaces accidentelles peuvent se manifester ou résulter de l'exposition ou de la modification d'un objet, elles peuvent êtres des erreurs des utilisateurs ou d'administrateur, matériel ou accidents de nature industrielle.

I.8.2.Les menaces intentionnelles: Une menace intentionnelle est une action exécutée par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources.

Les attaques intentionnelles peuvent êtres:

- **Menaces passives:** Basée sur l'écoute de l'exécution, son rôle est de collecter les informations. En générale il est très difficile de détecter une attaque passive car elle n'interagit pas dans le fonctionnement du système.

- **Menaces actives (attaque) :** Les menaces actives ou attaques envers un système provoque l'altération d'information contenues dans ce système, ou des modifications de l'état de fonctionnement du système, ce type de menaces est facile à détecter.

I.9. L'augmentation des menaces

Au fil des années, les outils et les méthodes permettant d'attaquer les réseaux ont constamment évolués.

Comme la figure suivante le montre en 1985, un pirate devait posséder un ordinateur de pointe, des connaissances en programmation et en réseaux pour réaliser des attaques élémentaires avec des outils rudimentaires.

Au fil du temps, les méthodes et les outils d'attaque se sont améliorés et les pirates n'ont plus eu besoin de posséder le même niveau de connaissances. Les exigences pour devenir pirate débutant ont effectivement diminué. Des personnes qui auparavant n'auraient pas commis de délits informatiques sont à présent à même de le faire.

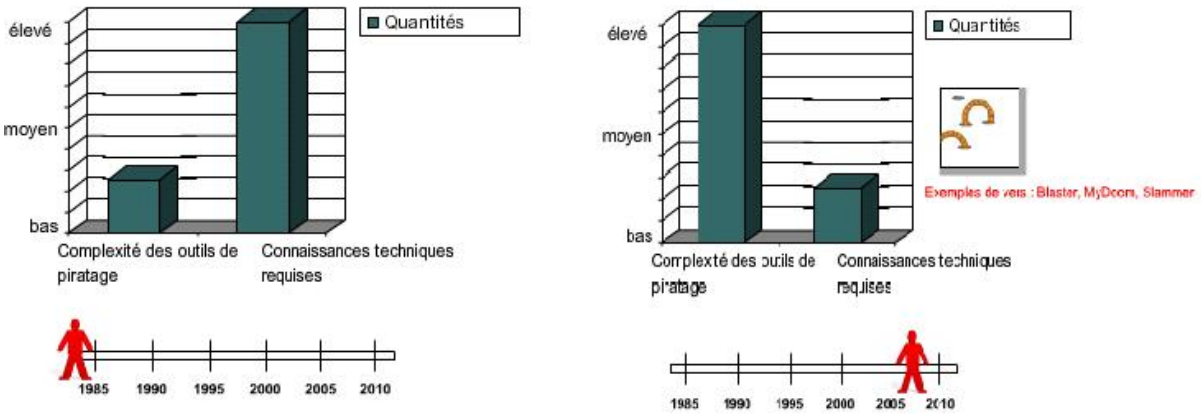


Figure II.1. : L'augmentation des menaces

I.10. Les menaces contre la sécurité

- **Pirate (cracker):** Autre terme désignant les personnes qui utilisent leurs connaissances des systèmes informatiques pour accéder de manière non autorisée à ces systèmes ou réseaux, habituellement dans un but personnel ou lucratif.

- **Bidouilleur (hacker):** Terme général utilisé dans le passé pour désigner un expert en programmation. Actuellement, ce terme est souvent utilisé de manière péjorative pour désigner un individu qui tente d'accéder de manière non autorisée aux ressources des réseaux avec une intention malveillante.
- **Braqueurs:** Sont plus dangereux que les hackers et mettent en panne des systèmes informatiques entiers, volent ou endommagent des données confidentielles, détériorent des pages web et vont même jusqu'à interrompre l'activité.
- **Fouineur:** Individu qui recherche des vulnérabilités dans des systèmes ou réseaux et qui signale ces vulnérabilités à leurs propriétaires de manière à ce qu'ils puissent les éliminer. ils ont une éthique qui les oppose à tout usage abusif des systèmes informatiques.

Les fouineurs tendent généralement à sécuriser les systèmes informatiques, à l'opposé, les pirates veulent y pénétrer par intrusion.

- **Spammeur:** Individu qui envoie une grande quantité de courriers non sollicités. Les spammeurs utilisent souvent des virus pour prendre possession d'ordinateurs familiaux et utiliser ces derniers pour leurs envois massifs.
- **Hameçonner:** Individu qui utilise le courrier ou d'autres moyens pour amener par la ruse d'autres utilisateurs à leur fournir des données sensibles, comme des numéros de cartes de crédit ou de passeports. L'hameçonner se fait passer pour une institution de confiance qui aurait un besoin légitime de ces données sensibles.

I.11. Les faiblesses de sécurité

- **Faiblesses technologiques**

Les technologies informatiques et de réseau ont des faiblesses de sécurité intrinsèques. Celles-ci comprennent:

Ø Les faiblesses du protocole TCP/IP: par exemple les protocoles HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol) et ICMP (Internet Control Message Protocol) sont intrinsèquement non sécurisés.

Ø Les faiblesses du système d'exploitation: Tous les systèmes d'exploitation (UNIX, Linux, Windows NT, XP et Vista) présentent des problèmes de sécurité qui doivent être résolus.

Ø Les faiblesses de l'équipement réseau: tels que les routeurs, et les commutateurs, ont des faiblesses de sécurité qui doivent faire l'objet d'une détection et

d'une protection. Ces faiblesses concernent la protection des mots de passe, le manque d'authentification, les protocoles de routage et les ouvertures dans les pare-feu.

- **Faiblesses de configuration**

Les administrateurs réseau et les ingénieurs système doivent apprendre ce que sont les faiblesses de configuration et les compensées en configurant convenablement leurs équipements informatiques et réseau. Les exemples fréquents qu'on peut citer sont les suivants:

- ü Paramètres par défaut non sécurisés dans les produits logiciels
- ü Équipement réseau mal configuré: par exemple, des listes d'accès, des protocoles de routage ou des chaînes de communauté SNMP mal configurées peuvent ouvrir de larges failles dans la sécurité.

- **Faiblesses dans la stratégie de sécurité**

Il existe des risques de sécurité pour le réseau si les utilisateurs ne respectent pas la stratégie de sécurité.

I.12. Les techniques d'attaques

Ø Attaque contre la communication

Est un type d'attaque contre la confidentialité, qui consiste à accéder sans modification aux informations transmises ou stockées, l'information n'est pas altérée par celui qui en prélève une copie. Ces attaques sont donc indétectables par le système et peuvent seulement êtres parées par des mesures préventives.

Ø Interposition

Il s'agit d'un «déguisement» en émission ou en réception, il consiste à tromper les mécanismes d'authentification pour se faire passer pour un utilisateur (personne ou service disposant des droits dont on a besoin) pour compromettre la confidentialité, l'intégrité ou la disponibilité.

Exemple: Le vol d'adresse (IP spoofing)

Ce type d'attaque n'implique rien de plus que l'usurpation d'une adresse source. Cela consiste à utiliser une machine en se faisant passer pour une autre.

Ø **Coupure**

Est un accès avec modification à des informations transmises sur des voies de communication, il s'agit donc d'une attaque contre l'intégrité.

Ø **Attaque logicielles**

- **Les virus**

Un "virus" est un bout de programme glissé volontairement dans une application dans le but de nuire. Il est possible d'attraper un virus avec n'importe quelle application que l'on a installée et que l'on exécute, ce n'est pas un problème typique d'une connexion permanente.

Un virus ne peut être introduit dans sa machine que si l'on exécute une application infectée, application récupérée sur l'Internet ou sur n'importe quel autre support informatique: Disquette, CD ROM etc.

Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement de logiciel puis exécution de celui-ci sans précautions.
- Ouverture sans précautions de documents contenant des macros.
- Pièce jointe de courrier électronique (exécutable, script type VBs…).
- Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité du logiciel de courrier (normalement JavaScript est sans danger).

- **Le Cheval de Troie**

Un cheval de Troie ou troyen (Trojan Horse ou Trojan) n'est ni un virus ni un ver, parce qu'il ne se reproduit pas. Un cheval de Troie introduit sur une machine a pour but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet. Les opérations suivantes peuvent être effectuées par l'intermédiaire d'un cheval de Troie :

- Récupération des mots de passe grâce à un keylogger.
- Administration illégale à distance d'un ordinateur.
- Relais utilisé par les pirates pour effectuer des attaques.
- Serveur de spam (envoi en masse des e-mails).

- **Les vers**

Un ver est un programme indépendant, qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter.

Il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise.

Comme un virus, un ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles.

- **L'écoute du réseau(Le sniffing)**

Grâce à un logiciel appelé "sniffer", il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées.

Si quelqu'un se connecte par Telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception.

Ø **Autres attaques**

- **Attaque par déni de service (DoS)**

Une attaque par déni de service (DoS, Dinial of Service) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services aux ressources d'une organisation. Il s'agit la plus part de temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

Le principe de ces attaques consiste à envoyer des paquets IP ou des données de taille afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.

- **Intrusion**

L'intrusion dans un système informatique à pour but la réalisation d'une menace et donc une attaque. Les conséquences peuvent êtres catastrophiques: vol, fraude, incident diplomatique…etc.

Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valide sur les machines qu'il a recensées, pour ce faire, plusieurs méthodes sont utilisées par le pirate.

Ø L'ingénierie sociale, c'est-à-dire en contactant directement certains utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leur mot de passe.

Ø la consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateurs valides.

Ø l'exploitation des vulnérabilités des logiciels.

Ø les attaques par force brute, consistant à essayer de façon automatique différents mots de passe sur une liste de compte.

- **Attaque de l'homme de milieu**

L'attaque de l'homme de milieu ou man-in-the middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous contrôle d'un pirate.

Ce dernier peut transformer à sa façon les données à la volée, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur.

Pour mettre en œuvre l'échange réseau approprier, il faut soit que la machine du pirate se trouve physiquement sur le chemin réseau emprunté par les flux de données, soit que le pirate réussisse à modifier le chemin réseau afin que sa machine deviennent un des points de passage.

- **Usurpation d'adresse IP (IP spoofing)**

L'usurpation d'adresse IP est une technique consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement.

La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage des paquets (pare-feu). Ainsi, un paquet écoué avec l'adresse IP d'une machine interne semblera provenir d'un réseau interne et sera relayé à la machine cible.

- **Le craquage de mot de passe**

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toute les combinaisons sont essayées jusqu'à trouver la bonne), cette technique longue, et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machine

I.13. Les protocoles de sécurité

- **Protocole SSL**

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (HTTP, FTP, etc.….). Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

- Le navigateur du client fait une demande de transaction sécurisée au serveur.
- Suite à la requête du client, le serveur envoie son certificat au client.
- Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- Le client choisit l'algorithme.
- Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
- Le navigateur vérifie que le certificat délivré est valide.
- Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

- **Le protocole SSH**

Le protocole SSH (*Secure Shell*) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

- **Le protocole IPsec**

IPSec est un protocole permettant de sécuriser les échanges au niveau de la couche réseau.

Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Le protocole IPSec est basé sur trois modules

- IP authentification Header(AH) concernant l'intégrité, l'authentification et la protection contre le rejet des paquets à encapsuler.
- Encapsulating security payload (ESP) définissant le chiffrement de paquet, ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejeu
- Security association (SA) définissant l'échange des clés et des paramètres de sécurité. Les SA rassembles ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP.

- **Le protocole Secure HTTP**

S-http(Secure HTTP, ce qui signifie Protocole HTTP sécurisé) permet de fournir une sécurisation des échanges lors de transaction de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle.

Contrairement à SSL qui travail au niveau de la couche de transport, S-HTTP assure une sécurité basée sur des messages au-dessus du protocole HTTP, en marquant individuellement les documents HTML à l'aide de certificats. Alors que SSL est indépendant de l'application utilisée et chiffre l'intégralité de la communication,

S-HTTP est fortement lié au protocole HTTP et chiffre individuellement chaque message.

I.14. Les méthodes de protections

I.14.1. Antivirus

Logiciel permettant de détecter et de supprimer les virus informatiques sur n'importe quel type de stockage (disque dur, disquette, CD-ROM, etc.). Pour être efficace ce type de logiciel demande des mises à jour très fréquentes au cours desquelles il mémorise les nouvelles formes de virus en circulation.

I.14.2. Réseau privé virtuel (VPN)

Il est dit virtuel car il relie deux réseaux locaux par l'intermédiaire d'internet et privé car seuls les ordinateurs faisant partie du réseau VPN peuvent accéder aux données.

Lorsqu'on ne peut se permettre de relier deux réseaux locaux par une ligne spécialisée (en raison de cherté), une solution existe. Celle de relier par support de transmission qui est internet.

Sur internet les données sont facilement captées et écoutées, ce qui nuit à la sécurité et la confidentialité de l'entreprise.

D'où l'utilité de placer un Proxy (faisant souvent office d'un firewall) sur chacun des réseaux locaux à relier. Ainsi lorsqu'un ordinateur envoie un message d'une partie d'un VPN vers une autre partie, il passe d'abord par un proxy qui va crypter le message (par des algorithmes de cryptage). Il l'envoie ensuite au proxy correspondant à d'autre partie. Celui-ci décrypte le message et le remet à son destinataire.

I.14.3. La cryptographie

La cryptographie est un ensemble de techniques permettant de transformer les données dans le but de cacher leur contenu, empêcher leur modification ou leur utilisation illégale. Ceci permet d'obtenir un texte chiffré dont seul celui qui possède les clés de déchiffrement pourra accéder à ce texte, en effectuent des transformations inverses (ou encore des algorithmes de déchiffrements). Désormais, elle sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

La taille des clés de chiffrement dépond de la sensibilité des données à protéger. Plus ces clés sont longues plus le nombre de possibilités de clés est important, par conséquent il sera difficile de deviner la clé qui à été utilisée (cette difficulté réside dans la puissance et le temps nécessaire pour deviner la clé).

Les algorithmes de chiffrement se divisent en deux catégories :

- **Chiffrement symétrique**

Dans ce cas de chiffrement, l'émetteur et le récepteur utilisent la même clé secrète qu'ils appliquent à un algorithme donné pour chiffrer ou déchiffrer un texte.

Ce cryptage à un inconvénient, puisqu'il faut que les deux parties possèdent la clé secrète, il faut donc la transmettre d'un bout à l'autre, ce qui est risqué sur un réseau non fiable comme internet car la clé peut ainsi être interceptée.

- **Chiffrement asymétrique**

Ces systèmes se caractérisent par la présence d'une entité pour chaque interlocuteur désirant communiquer des données. Chaque interlocuteur possède une bi-clé ou couple de clés calculées l'une en fonction de l'autre.

- ü Une premier clé, visible, appelée clé publique est utilisée pour chiffrer un texte en clair.
- ü Une deuxième clé, secrète, appelée clé privée est connue seulement par le destinataire, qui est utilisé pour déchiffrer un texte.

I.14.4. Pare-feu

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet).

Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- ü Une interface pour le réseau à protéger (réseau interne) ;
- ü Une interface pour le réseau externe.

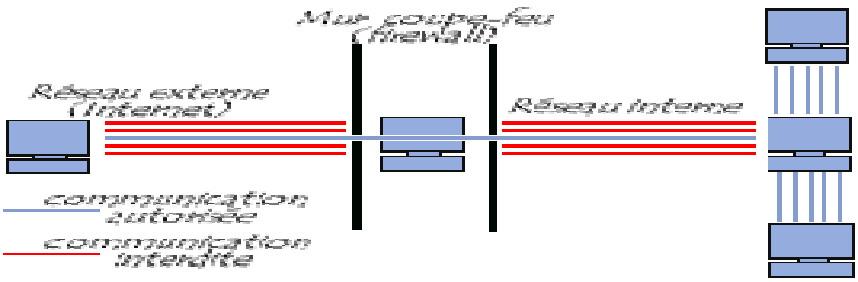


Figure II.2: Le principe de fonctionnement d'un pare feu

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

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

Dans le cas où le système pare-feu est fourni dans une boîte noire « clé en main », on utilise le terme d'« appliance ».

Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées.
- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

I.14.4.a. Les différents types de filtrages

Ø Le filtrage simple de paquet (Stateless)

Méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau a un autre, en se basant sur:

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Et bien sur le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le Firewall ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

Ø Le filtrage dynamique

Le filtrage de paquet dynamique ou "avec état", permet de pallier les limites du filtrage de paquet statique. Le filtrage de paquet dynamique fait le suivi des paquets sortants dont il a autorisé la transmission et n'autorise que le retour des paquets de réponse correspondants. Lorsque le premier paquet est transmis au réseau public (Internet), un filtre inverse est créé

de façon dynamique de façon à permettre le retour du paquet de réponse. Pour qu'il puisse être considéré comme une réponse, le paquet entrant doit provenir de l'hôte et du port auquel le paquet sortant a été envoyé.

Ø Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Ce filtrage opère donc au niveau 7 du modèle OSI (couche application), Le filtrage applicatif suppose une connaissance des protocoles utilisés par chaque application. Il permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

I.14.4.b.Les limites des firewalls

Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portable peut porter fortement préjudice à la politique de sécurité globale.

Afin de garantir un niveau de protection maximale il est nécessaire d'administrer le pare-feu et notamment de surveiller son activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies

I.15. Les services réseaux

- **Serveur Web (HTTP)**

Est un logiciel capable d'interpréter les requêtes HTTP qu'il reçoit et fournit une réponse dans ce même protocole. Apache est le serveur HTTP le plus répandu sur internet .ce dernier, permet en effet d'ajouter des modules supplémentaires qui enrichissent le serveur en terme de fonctionnalités.

- **Serveur DNS**

Le service DNS signifiant Domain Name Services est né de la volonté de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques tels que l'Internet.

Les machines ne sachant communiquer qu'à travers l'échange d'adresses IP difficiles à mémoriser pour l'homme, le DNS agit comme un annuaire téléphonique en fournissant la correspondance entre le nom de la machine et son adresse IP. Ainsi, lorsque l'on veut se connecter à un ordinateur dont on connaît le nom d'hôte, on interroge un serveur DNS qui nous renvoie l'adresse IP correspondant à ce nom.

- **Serveur FTP**

Un serveur FTP est utilisé dans le cas où l'on souhaite rendre disponible des fichiers (dans un réseau local ou sur internet) et ce que ce soit de manière anonyme ou grâce à des comptes utilisateurs.

L'échange des fichiers peut se faire dans les 2 sens, soit en téléchargement à partir du serveur ftp (download) vers l'utilisateur (client) ou soit dans le sens contraire, en téléchargement à partir de l'utilisateur vers le serveur ftp (upload).

- **Le serveur DHCP**

Le serveur DHCP signifie Dynamic Host Configuration Protocol et désigne un protocole réseau dans le rôle est d'assurer la configuration automatique des paramètres IP d'une machine. Cela inclure son adresse IP, son masque de sous réseau, son adresse de broadcast, l'adresse de réseau, ou encore l'adresse des routeurs et de la passerelle par défaut.

- **Le Proxy**

Un serveur est à l'origine une machine qui fait fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. Les serveurs proxy isolent les réseaux locaux et protègent les hôtes des menaces extérieures. L'efficacité des serveurs proxy repose sur leur capacité à mettre en cache les pages Web**.** La possibilité d'utiliser un service proxy pour HTTP constitue un réel avantage. De nombreux clients peuvent accéder au contenu HTTP avec un meilleur délai de réponse.

I.16.Discussion

Dans ce chapitre nous avons présenté des généralités sur les réseaux informatiques. Vu la fiabilité de communication qu'ils assurent, ils sont devenus aujourd'hui une nécessité dans le mondes du travail. Les différentes menaces et attaques sur divers systèmes nous ont ramené à parler de la nécessité de garantir certain besoins de sécurisation: tels que l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que les méthodes d'attaques utilisées et comment se protéger contre elles.

Dans le chapitre suivant nous allons présenter le cas d'existence d'une entreprise et la solution que nous lui proposerons pour améliorer la sécurité de son réseau.

II.1.Préambule

Le but de ce chapitre est de présenter un plan de sécurité pour l'appliquer au niveau du réseau de l'entreprise. Nous allons présenter le réseau existant et ses critiques ainsi que Les services de sécurités adaptatifs Cisco ASA qui permet aux administrateurs de mieux segmenter le trafic réseau et de créer des zones de sécurité séparées.

II.2. Présentation de l'entreprise

L'école 2int (Institut International des nouvelles Technologies) est centrée sur les systèmes et réseaux, le développement d'applications, les bases de données et les environnements "Open Source". Sans oublier les formations utilisateurs spécifiques autour des Applications bureautiques et de travail collaboratif.

II.3. Architecture d'organisme d'accueil

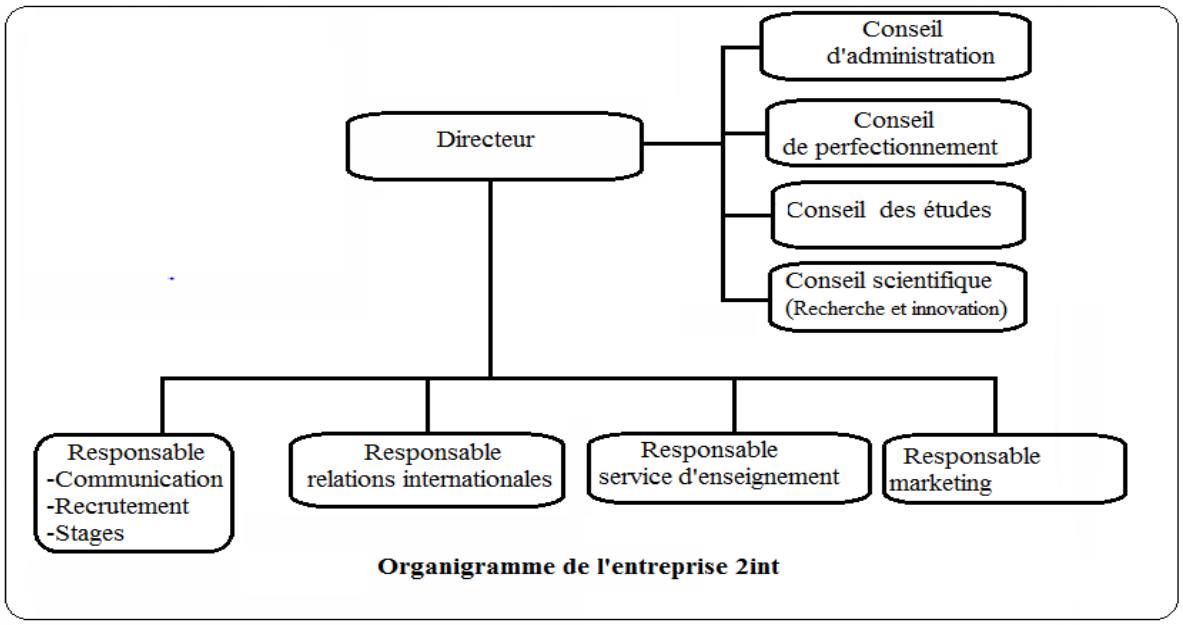


Figure II.1.Organigramme de l'entreprise 2int

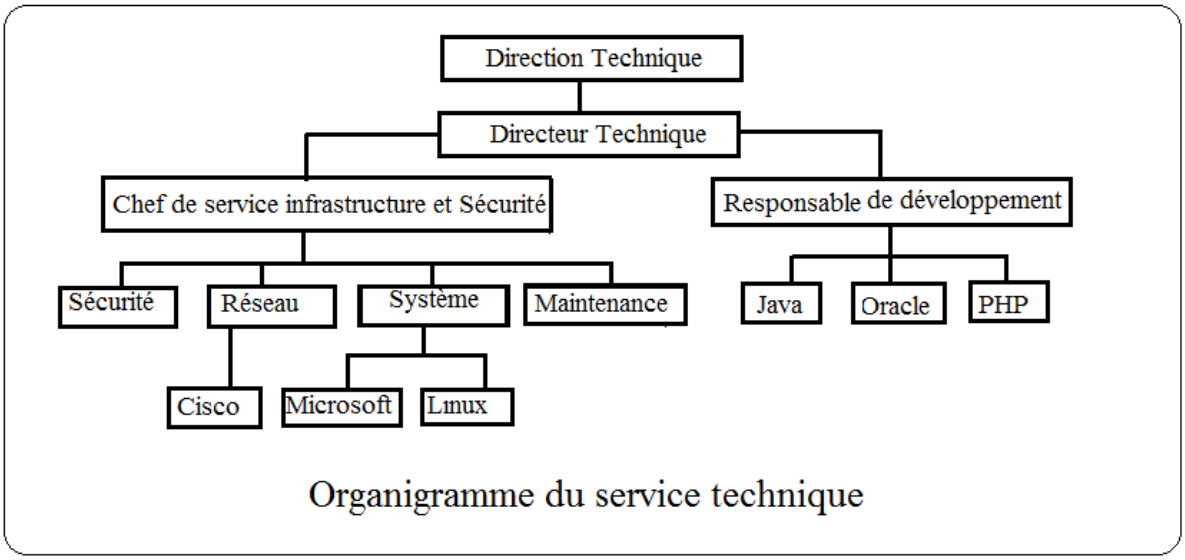


Figure II.2. Organigramme du service technique

II.4. Architecture du réseau d'entreprise existant

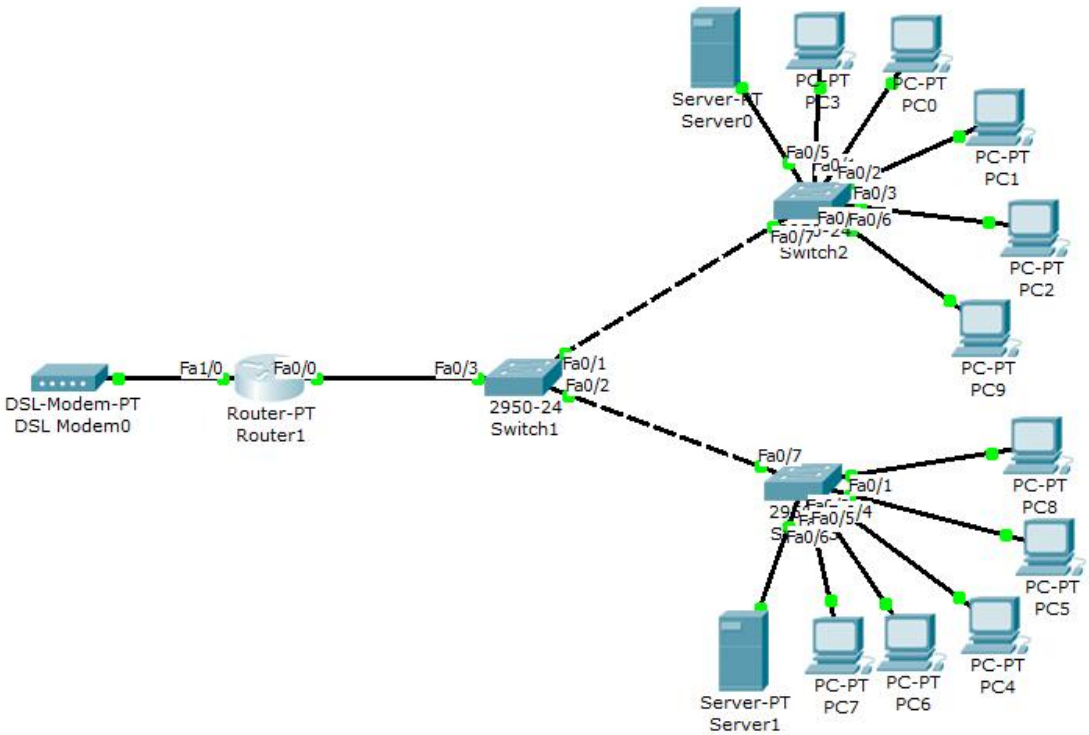


Figure II.3. Architecture du réseau existant

Materiels existants:

- Tois switch Cisco (CATALYST Cisco)
- Des poste client
- Un routeur
- Modem ADSL

II.5. Critiques du réseau existant

Critique 1 : Le réseau est installé anarchiquement et non administré

Critique 2 : Le réseau installé est non sécurisé contre les intrusions d'une façon fiable.

Critique 3 : l'accès est permis de chaque unité émettrice vers n'importe quelle unité destinataire (accès non limité).

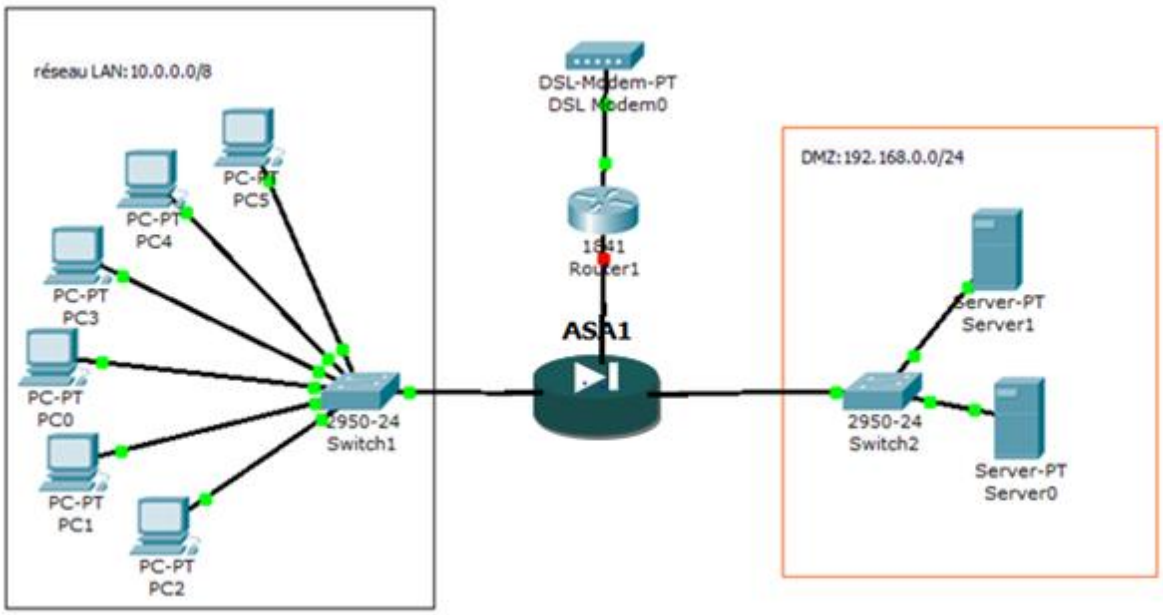
II.6. Solutions proposées

A l'issu d'une étude préalable de réseau existant nous avons opté pour l'implémentation du plans de sécurité suivants :

- Ø Administration et ordonnancement du réseau local.
- Ø Configuration d'un firewall (ASA 5510)

L'architecture du réseau avec les solutions proposées dans ce plan de sécurité est présentée

par la figure II.4



FigureII.4. Architecture du réseau proposer

Matériels à utiliser

- Deux serveurs (serveur Active directory et serveur des fichiers)
- Des postes clients
- Routeur Cisco 3600
- Switch Cisco (CATALYST Cisco)

Logiciels à utiliser

- Dans les postes serveurs (Windows server 2008)
- Dans les postes clients (Windows XP)

II.7. Présentation du matériel

II.7.1.Les Routeurs Cisco

La fonction principale d'un routeur Cisco consiste à diriger les paquets destinés à des réseaux locaux et distants en:

- Ø Déterminant le meilleur chemin pour l'envoi des paquets,
- Ø Transférant les paquets vers leur destination.

II.7.2. Les Switch Cisco (CATALYST Cisco)

Les commutateurs intelligents Cisco Catalyst, nouvelle famille de périphériques autonomes à configuration fixe, apportent aux postes de travail une connectivité Fast Ethernet et Gigabit Ethernet optimisent les services de LAN sur les réseaux d'entreprise.

- ces caractéristiques sont:

Ø Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de Contrôle d'accès (ACL) élaborées et une sécurité optimisée.

Ø Sécurité du réseau assurée par une série de méthodes d'authentification, des technologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.

II.8. Présentation des logiciels

II.8. 1. Windows XP

Windows XP est un système d'exploitation de Microsoft qui a vu le jour en 2001. Il a l'objectif de s'adapter pour le monde professionnel ainsi que pour l'utilisation personnelles avec par exemple la prise en charge de jeux récents, de lecture vidéo et audio, ...etc. Il s'agit également de la nouvelle version de Windows 2000.Il peut servir de mise à jour pour Windows 2000, Windows Millenium ou Windows 98.C'est un système dont le noyau est basé sur 32 Bits. L'innovation remarquable de ce système d'exploitation est la nouvelle interface graphique utilisateur (GUI) incluant de nouvelles icônes et couleurs. Ce système est également plus stable que ses prédécesseurs.

La version de Windows XP professionnel plus complète, propose, outre les innovations apportées par l'édition familiale (stabilité et fiabilité accrues, interface plus intuitive, aide en ligne, paramétrage d'un pare-feu, outils multimédia vidéo et audio, photo du système, etc.), des options inédites que les utilisateurs seront ravis de disposer pour leur usage professionnel.

Windows XP Professionnel offre un certain nombre de fonctions non incluses dans la version "familiale" telles que :

- La possibilité d'être membre d'un domaine et la possibilité que l'ordinateur soit géré depuis un serveur.

- Un contrôle d'accès spécifique à certains dossiers pour pouvoir éviter l'accès de certains utilisateurs (mais il peut être contourné par un autre système d'exploration).
- La fonction bureau à distance permet de contrôler l'ordinateur par un autre système sous XP dans un réseau local ou par Internet.
- Une fonction qui permet de faire une copie automatique des fichiers d'un autre ordinateur.
- L'Encrypting File System, qui chiffre automatiquement les données du disque dur ce qui permet de le rendre illisible sans entrer le mot de passe.
- Les fonctions de maintenance de l'ordinateur comme les patchs qui servent de mises à jour.

II.8. 2. Windows Server 2008

Après la sortie du nouveau système d'exploitation de Microsoft « Windows Vista », la suite logique était donc la sortie du nouveau système d'exploitation serveur de Microsoft

« Windows Server 2008 ». Il va donc remplacer à terme l'ancien système d'exploitation Windows Server 2003 aujourd'hui, utilisé dans la majorité des entreprises.

Windows Server 2008 et Windows Vista embarquent donc le même kernel c'est-à-dire le NT 6.0. On constate donc des similitudes aux niveaux des nouveautés comme par exemple l'introduction de l' « UAC » (User Account Control) qui permet d'appliquer le principe du moindre privilège en accordant des privilèges restreints et des similitudes au niveau de l'interface avec l'apparition de « Windows Aero » offrant une interface plus conviviale.

Microsoft à adapté Windows pour que la version 2008 répond aux besoins et aux attentes des entreprises et des informaticiens qu'ils soient programmeurs ou administrateurs.

II.8. 2.a. Nouveautés de Windows Server 2008

Un certain nombre de nouveautés ont été apportées dans Windows Server 2008 comme par exemple :

- **Server Core**

Dans Windows Server 2008, on a maintenant la possibilité d'installer une version minimale de Windows. Cette version est dépourvue d'interface graphique. De cette façon la sécurité est améliorée puisqu'on va installer que le strict minimum utile.

Une installation « Server Core » permet d'utiliser les mêmes composants que dans la version « normale » comme le serveur DHCP, DNS ou Active Directory par exemple.
On administre donc le serveur par des lignes de commande que l'on tape dans une fenêtre de commande

- **Active Directory Domain Services: Read-Only Domain Controller**

Une nouveauté dans Windows Server 2008 est la possibilité d'installer un contrôleur de domaine en lecture seule.

En effet, lorsque la sécurité physique du serveur ne peut pas être garantie comme dans le cas de succursales par exemple, on a la possibilité d'installer un RODC, Read-Only Domain Controller, sur lequel on ne va donc rien pouvoir écrire et qui ne vas stocker aucun mot de passe. Ce RODC est donc une copie du contrôler de domaine « principal ».

- **Auditing Active Directory Domain Services Access**

Dans Windows Server 2003, il n'y avait qu'une seule catégorie pour l'audit des activités dans Active Directory, qui était donc soit « enabled » soit « disabled ». Dans Windows Server 2008, la catégorie a été subdivisée en 4 sous-catégories :

- Directory Service Access
- Directory Service Change
- Directory Service Replication
- Detailed Directory Service Replication

- **Fine-Grained Password Policies**

Microsoft Windows Server 2008 offre la possibilité de définir plusieurs politiques de mots de passe pour différents utilisateurs.
Dans les anciennes versions du système d'exploitation serveur de Microsoft, une seule politique de mot de passe était créée pour tous les utilisateurs du domaine, ce qui n'était donc pas très optimisé sachant que certains comptes étaient plus importants que d'autres.
On peut donc faire en sorte que les comptes sensibles comme les comptes administrateurs requièrent un mot de passe plus complexe qu'un compte normal.

Le Gestionnaire de serveur

Le Gestionnaire de serveur est l'outil principal de l'administrateur sous Windows Server 2008. Il permet de configurer et de gérer avec un seul outil l'ensemble des tâches qui lui sont dévolues.

II.9. Active Directory

Active Directory est le nom du service d'annuaire (au sens informatique) du Microsoft. AD permet de regrouper toutes les informations concernant le réseau que ce soient les utilisateurs, les machines ou les applications. L'utilisateur peut ainsi trouver facilement des ressources partagées et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de sécurisation des accès aux ressources répertoriées. AD a pour objectif de permettre la gestion des comptes, des ordinateurs, des ressources et de la sécurité d'une façon centralisée, dans le cadre d'un domaine.

II.9.1. Le service de domaine Active Directory (AD DS)

Les services de domaine Active Directory fournissent les fonctionnalités d'une solution de gestion des identités et des accès (IDA:Identity and Access) pour les réseaux d'entreprise sous Windows.

IDA est nécessaire pour maintenir la sécurité des ressources d'une entreprise tels que: fichiers, messages électroniques, applications et bases de données.

Une infrastructure doit assurer les fonctionnalités suivantes:

- Mémoriser les informations sur les utilisateurs, les groupes et les autres identités.
- Authentifier une identité.
- Contrôle d'accès.
- Fournir une trace d'audit.

II.10. Serveur de fichier

Un serveur de fichiers fournit un emplacement central sur votre réseau où vous pouvez stocker des ressources (fichiers) et les partager avec des utilisateurs de votre réseau.

Lorsque les utilisateurs ont besoin d'un fichier important qui doit être accessible pour un grand nombre de personnes, ils peuvent accéder à distance au fichier situé sur le serveur de fichiers au lieu de transférer le fichier entre les ordinateurs individuels.

On utilise généralement l'un des quatre protocoles suivants:

- FTP (File Transfer Protocol)
- CIFS (Common Internet File System) anciennement nommé SMB (Server Message Block)

- NFS (Network File System)
- NCP (Netware Core Protocol)

Le choix du protocole dépend principalement de la méthode d'accès des utilisateurs. CIFS est utilisé par les systèmes d'exploitation Microsoft Windows, NFS est répandu dans le milieu UNIX. Toute fois des implémentations de ces protocoles sont disponibles pour tout type de système. Ces deux protocoles permettent d'établir des liaisons permanentes entre le client et le serveur.

II.10.1. Installation du serveur de fichier

Windows server 2008 simplifie les taches de création, de partage et d'administration en regroupant toutes les fonctionnalités du serveur de fichiers autour d'un seul et même rôle. Il existe trois types de partage de fichier sur Windows: SMB, NFS et DFS.

- SMB est un partage qui fonctionne avec tous les autres systèmes d'exploitation MAC OS X et Linux.
- NFS quand à lui, est exclusivement utilisé pour partager des fichiers entre machines Windows et UNIX.
- DFS permet de faire le partage de fichiers via un unique espace de noms. Les utilisateurs n'ont plus à se soucier du nom de serveur mais juste d'un espace de nom. DFS permet aussi de faire de la redondance en faisant de la réplication.

II.11. Serveur web

Les sites web permettent d'accéder à des bases de données dans des environnements publics et intranet et autorisent une certaine personnalisation en fonction de besoins particuliers. Les applications ou les services Web se basent sur diverses normes, protocoles et technologies de développement.

Le système d'exploitation Windows server 2008 inclut IIS7.0 (Internet Information Services), une plate-forme de services web complète capable de prendre en charge plusieurs types de contenus et d'applications web. IIS7.0 propose de nettes améliorations au niveau de la gestion de l'extensibilité et de la fiabilité. Elle assure également une rétrocompatibilité pour supporter les millions de sites Web déjà hébergés sur les versions précédentes d'IIS.

Cas d'utilisation des serveurs Web

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

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

- Sites web publics: la plupart des entreprises ont des besoins relativement simples pour communiquer des informations sur internet.
- Achats en ligne: internet est devenu un centre commercial qui permet aux vendeurs d'afficher et de vendre une grande variété de produits.
- Intranet: le Web propose une méthode simple pour tous les utilisateurs d'une organisation d'accéder et de présenter du contenu.
- Applications d'entreprise: les applications sectorielles d'entreprise doivent souvent déployer et gérer des installations côté client.
- Applications internet: les utilisateurs peuvent accéder à leur courrier électronique et créer des documents par exemple sans installer d'applications sur leurs ordinateurs. Les organisations et les équipes peuvent aussi profiter de l'accès sécurisé aux applications d'entreprise via internet lors de leur déplacement et s'ils travaillent à distance.
- Extranet: est un cas ou les utilisateurs extérieurs à l'organisation peuvent accéder à des données. La sécurité est un souci important, mais les applications Web représentent un bon choix parce qu'elles proposent une méthode standard grâce à laquelle les utilisateurs peuvent accéder aux informations dont ils ont besoin.

Les services de rôle IIS

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

II.12. La Zone Démilitarisée (DMZ)

II.12.1. Définition :

Dans la sécurité informatique, une zone démilitarisée (DMZ) est un sous-réseau isolé par un pare-feu. Ce sous-réseau contient des machines se situant entre un réseau interne (LAN) et un réseau externe (Internet). Sur ce réseau nous disposons d'un espace confiné, d'une taille limitée. Le nombre de serveurs présents sur ce réseau est limité, de sorte à ne pas permettre une trop grande interaction entre les serveurs. Dans ce réseau « haute sécurité », il n'y a aucun poste utilisateur, chaque flux à destination de l'un de ces serveurs (qu'il provienne d'internet ou d'un réseau interne) est clairement défini sur le firewall. De cette manière, nous maitrisons précisément les connexions à destination et en provenance de ces machines

Quelques règles spécifiques sont applicables aux DMZ

Il convient de sécuriser spécifiquement ces machines, en limitant les services rendus Par ces serveurs. De plus, il faut désinstaller/désactiver ce qui ne serait pas nécessaire. Dans le cas d'un serveur Windows, il convient par exemple de désactiver les partages Windows.

Il ne faut surtout pas laisser trainer des exécutables de test du réseau (type nmap,… etc.) Sur ce serveur (même si ces derniers ne sont que des programmes d'installation). Si un hacker parvenait par un moyen non prévu à lancer ces exécutables, il pourrait compromettre la sécurité de cette DMZ.

Les flux entre serveurs au sein de la DMZ sont à limiter. Si ces derniers sont nombreux et sensibles, il faut dans ce cas envisager de mettre en place une seconde DMZ, déplacer certains de ces serveurs sur la nouvelle DMZ et autoriser les flux spécifique sur le Firewall. Il est courant pour le architectures « avancées » de disposer d'un certain nombre de DMZ. Au final, il ne s'agit là que de segmenter les réseaux et de filtrer les interactions entre ces réseaux.

II.12. 2. Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise.

Pour pouvoir appliquer la politique de sécurité de l'entreprise .Nous proposons de séparer le réseau LAN de l'entreprise en mettant le serveur des fichiers et le serveur active directory dans la zone démilitarisée et les postes client dans une autre zone puis les interconnecter à l'aide des Switch et routeurs , pour gérer le trafic entre les zone nous allons implémenter ASA Cisco 5510

La politique de sécurité mise en œuvre sur la DMZ est la suivante:

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe autorisé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise. Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

II.13. Description de la gamme Cisco ASA 5500

Les serveurs de sécurité adaptatifs de la gamme Cisco ASA 5500 s'appuient sur une plate-forme modulaire capable de fournir des services de sécurité et de VPN de prochaine génération à tous les environnements. La gamme Cisco ASA 5500 met à la disposition de l'entreprise une gamme complète de services personnalisés à travers de ses diverses éditions spécifiquement conçues pour le pare-feu, la prévention des intrusions, la protection des *contenus et les VPN. Ces éditions offrent une protection de haute qualité en fournissant les services adaptés à chaque site.

La gamme Cisco ASA 5500 permet la normalisation sur une unique plate-forme afin de réduire les frais opérationnels associés à la sécurité. L'environnement commun de configuration simplifie la gestion et réduit les couts de formation du personnel tandis que la plate-forme matérielle commune de la gamme permet de réaliser des économies sur les pièces de rechange.

II.14. Principaux avantages technologiques et nouveautés de la gamme ASA 5500

La gamme Cisco ASA 5500 aide les entreprises à protéger plus efficacement leurs réseaux tout en garantissant une exceptionnelle protection de leurs investissements grâce aux éléments clés suivants :

- **technologie reconnue de firewall et VPN protège contre les menaces**

Développée autour de la même technologie éprouvée qui a fait le succès du serveur de sécurité Cisco PIX et de la gamme des concentrateurs Cisco VPN 3000. La gamme Cisco ASA 5500 est la première solution à proposer des services VPN-SSL (Secure Sockets Layer) et IP sec (IP Security) protégés par la première technologie de firewall du marché. Avec le VPN SSL, l'ASA 5500 est une passerelle SSL performante qui permet l'accès à distance sécurisé au réseau à travers d'un navigateur web banalisé pour les utilisateurs nomades.

- **service évolué de prévention des intrusions**

Les services proactifs de prévention des intrusions offrent toutes les fonctionnalités qui permettent de bloquer un large éventuel de menaces-vers, attaques sur la couche applicative ou au niveau du système d'exploitation, logiciels espions, messagerie instantanée.

- **services anti-X à la pointe de l'industrie**

La gamme Cisco ASA 5500 offre des services complèts anti-X à la pointe de la technologie-protection contre les virus, les logiciels espions, le courrier indésirable et le phishing ainsi que le blocage de fichiers, le blocage et le filtrage des URL et le filtrage de contenu en associant le savoir faire de Trend micro en matière de protection informatique à une solution Cisco de sécurité réseau éprouvée.

- **services multifonctions de gestion et de surveillance**

Sur une même plate-forme, la gamme Cisco ASA 5500 forme des services de gestion et de surveillance utilisables de manière intuitive grâce au gestionnaire Cisco ASDM(Adaptative Security Device Manager) ainsi que des services de gestion de catégorie entreprise avec Cisco Security management suite.

- **réduction des frais de déploiement et d'exploitation**

La solution multifonctions Cisco ASA 5500 permet la normalisation de la plate-forme, de la configuration et de la gestion, contribuant à réduire les frais de déploiement et d'exploitation récurrents

II.15. Principe de fonctionnement d'ASA

L'ASA offre deux modes pour ses utilisateurs :

Le mode «routed» est de niveau 3: quand il ya de trafic, l'ASA est comme un saut sur un routeur (router hop in the network)

Le mode «transparent» est de niveau 2: il facilite la configuration du réseau et permet de cacher le pare-feu (aux intrus éventuels). On utilise aussi le mode transparent pour autoriser le trafic qui est bloqué par un routeur en utilisant les ACLs.

Par défaut, l'ASA est en mode «routed»

II.16. Les fonctionnalités d'ASA

II.16.1. ACL (Access Control Lists)

A chaque interface connectée à l'ASA, un niveau de sécurité (entre 0 et 100) est attribué, le niveau de sécurité 100 se voit attribué par défaut au réseau dont on a la maitrise (LAN) et le niveau 0 se voit attribué au réseau extérieur. L'ASA interdit le trafic d'une interface vers une autre interface dont le niveau de sécurité est élevé. Il autorise le trafic d'une interface de niveau de sécurité inférieur.

Les ACL (Access Lists) ont été mises en place pour pouvoir gérer le trafic entre les interfaces selon le besoin de l'entreprise.

- **Utilité d'une liste d'accès**

Une liste d'accès va servir à :

- supprimer des paquets pour des raisons de sécurités.
- filtrer des mises à jour de routage.
- filtrer des paquets en fonction de leur priorité (QOS :Quality of Servise).
- définir le trafic intéressant pour des configurations spécifiques (NAT, ISDM ,…etc.)

Ø **Principe de fonctionnement**

Une liste d'accès, comportant une suite d'instruction de filtrage, va être appliquée sur une interface du routeur, pour le trafic sortant. Il va falloir appliquer une logique sur les interfaces en sortie ou en entrée.

- Les paquets peuvent être filtrés en entrée (quand ils entrent sur une interface) avant la décision de routage.
- Les paquets peuvent être filtrés en sortie (avant de quitter une interface) après la décision de routage.
- Le mot clef IOS est «deny» pour signifier que les paquets doivent être filtrés, précisément les paquets seront permis selon les critères définis.
- La logique de filtrage est configurée dans les listes d'accès.
- Une instruction implicite rejette tout le trafic à la fin de chaque liste d'accès.

Ø **Types d'ACL**

Il existe deux types d'ACL :

ACL Standard: Permet l'analyse du trafic en fonction de l'adresse IP source, elles sont appliquées le plus proche possible de la destination en raison de leur faible précision.

ACL Etendues: permet l'analyser du trafic en fonction d'adresse IP source, adresse IP destination, port source, port destination et protocole (IP, TCP, UDP, ICMP…), elles sont appliquées le plus proche possible de la source.

II.16.2. Translation d'adresse (NAT)

Vu le nombre limité d'adresses Ipv4 routables, des techniques comme le NAT et le PAT sont utilisées pour gérer au mieux cette ressource rare du monde du réseau. L'ASA est en partie un routeur donc il est logique qu'il offre du NAT.

Le NAT (Network Address Translation) consiste à établir des relations entre l'adresse privée dans un réseau et l'adresse publique pour se connecter à internet. On distingue deux types du NAT:

- **NAT statique**: elle consiste à associer à une adresse IP interne une adresse IP externe. La correspondance est fixe

- **NAT dynamique**: une plage d'adresses publiques est mise au niveau du routeur et lorsqu'une machine du réseau local veut accéder à internet, on lui attribue temporairement et dynamiquement une adresse publique prise dans cette plage.
- **PAT (Port Address Translation) ou Overloading**

Principe

Le Port Addres Translation vient complémenter le NAT. En effet, supposant que nous ne disposons pas d'adresses IP publiques suffisantes pour toutes nos machines locales, il va donc falloir partager et réutiliser nos adresses.

PAT permet à plusieurs hôtes internes de partager une adresse unique sur une interface externe en ajoutant des numéros de port différents à chaque connexion c'est-à-dire que pour distinguer les requêtes des différentes machines, on va utiliser le numéro du port.

II.17. Serveur de sécurité adaptatif Cisco ASA 5510

Le serveur de sécurité adaptatif Cisco ASA 5510 propose des services évolués de réseau et de sécurité aux petites et moyennes entreprises et aux filiales et agences des grandes entreprises, sous la forme d'une solution économique et facile à déployer.

Les avantages d'ASA Cisco 5510

La gamme Cisco ASA 5510 fournit des services de pare-feu et de VPN ultraperformants, des services de prévention des intrusions et de réduction des vers extrêmement sophistiqués grâce au module AIP SSM ou des services complets de protection contre les programmes malveillants grâce au module CSC SSM.

Les entreprises peuvent déployer jusqu'à cinq pare-feu virtuels dans une même appliance afin de compartimenter le contrôle des politiques de sécurité au niveau des services.

Cette virtualisation renforce la sécurité et réduit les coûts globaux de gestion et d'assistance tout en permettant le regroupement de plusieurs périphériques de sécurité dans une même appliance.

Le Tableau suivant représente la Fonctionnalité et capacité de la plate-forme Cisco ASA 5510

Fonctionnalité	**description**
Débit de pare-feu	Jusqu'à 300 Mbit/s
Débit maximal de pare-feu et du système de prévention des intrusions	Jusqu'à 150 Mbit/s avec l'AIP SSM-10 Jusqu'à 300 Mbit/s avec l'AIP SSM-20
Débit de VPN	Jusqu'à 170 Mbit/s
Sessions simultanées	50 000 ; 130 000
Sessions VPN Ipsec site à site	250
Options des licenses Anyconnect VPN Premium	2, 10, 25, 50, 100 ou 250
Contextes de sécurité	Jusqu'à 5
Interfaces	5 ports Fast Ethernet ; 2 ports Gigabit Ethernet + 3 ports Fast Ethernet
VLAN supportés	50 ; 100*
Évolutivité	Clustering VPN et équilibrage de charge
Haute disponibilité	Non supporté ; mode actif/actif, mode actif/passif*

Tableaux II.1. Fonctionnalité d'ASA Cisco 5510

II.18. Discussion

Dans ce chapitre nous avons présenté le réseau d'une entreprise existant ainsi que ses critiques. La solution proposée était de réorganiser l'architecture du réseau et de centraliser leur base de données. Nous avons présenté également la configuration d'un pare-feu pour mieux géré le trafic

Dans le chapitre suivant nous allons présentés les différentes étapes qui nous permettront la bonne réalisation de notre application.

III.1.préambule

Le but de ce chapitre est de concevoir une zone démilitarisée permettant à une entreprise d'isoler les postes clients (LAN) de la zone de fourniture de services (DMZ) et de les protéger contre les attaques provenant des réseaux extérieurs. Nous commencerons par présenter les différents services et rôles introduits dans les serveurs Active Directory ensuite nous exposerons le simulateur GNS3 qui sera utilisé pour la configuration des éléments réseaux tel que le routeur et le firewall ASA Cisco en utilisant la configuration des listes de contrôle d'accès (ACL).

III.2. La topologie

Voici la topologie que nous avons choisi à mettre en place pour la création de notre réseau

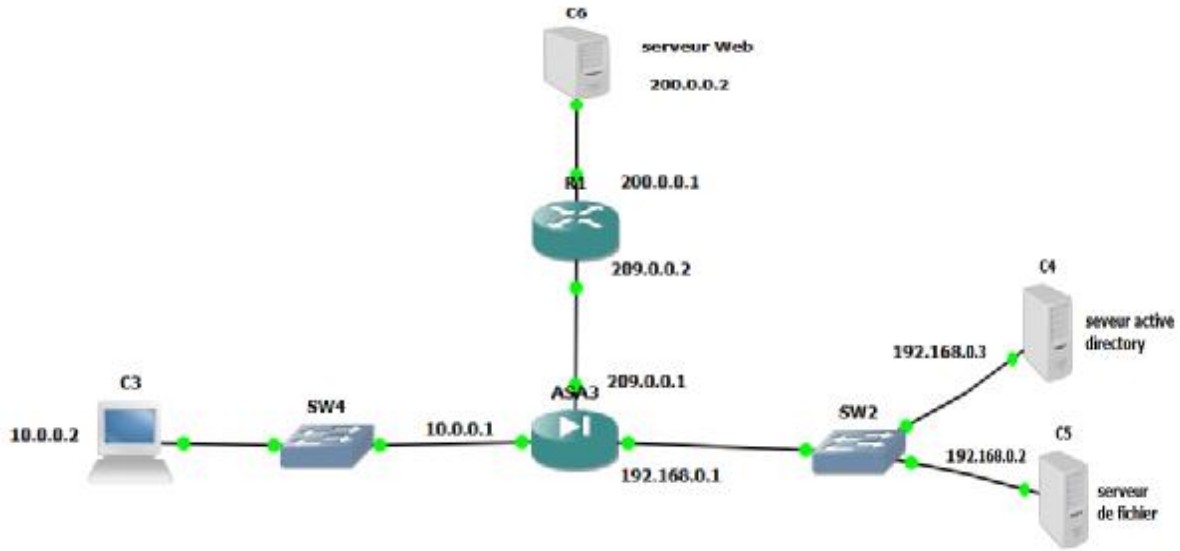


Figure III.1. Topologie du réseau choisi

Matériels utilises

- Trois postes serveurs
- Un poste client
- Un pare-feu (ASA)
- Un routeur
- Deux Switch

Logiciels utilises

- Dans les postes serveurs (Windows server 2008)

- Dans le poste client (Windows XP)
- VMware Workstation (pour la configuration des serveurs et client)
- GNS3 (pour la simulation graphique d'équipement réseau)

La première étape de notre travail consiste à configurer les serveurs:

III.3.Installation de serveur Active Directory:

Nous allons configurer le serveur de domaine Active Directory et nous installerons le service DNS et le service DHCP.

dcpromo: permet d'installer le serveur de domaine Active Directory**.**

Dans démarrer, Gestionnaire de serveur, rôles puis ajouté des rôles on coche l'icône «service de domaine Active Directory» pour l'installer le menu

Lors de l'installation serveur de domaine Active Directory on va nommer le domaine comme suite:

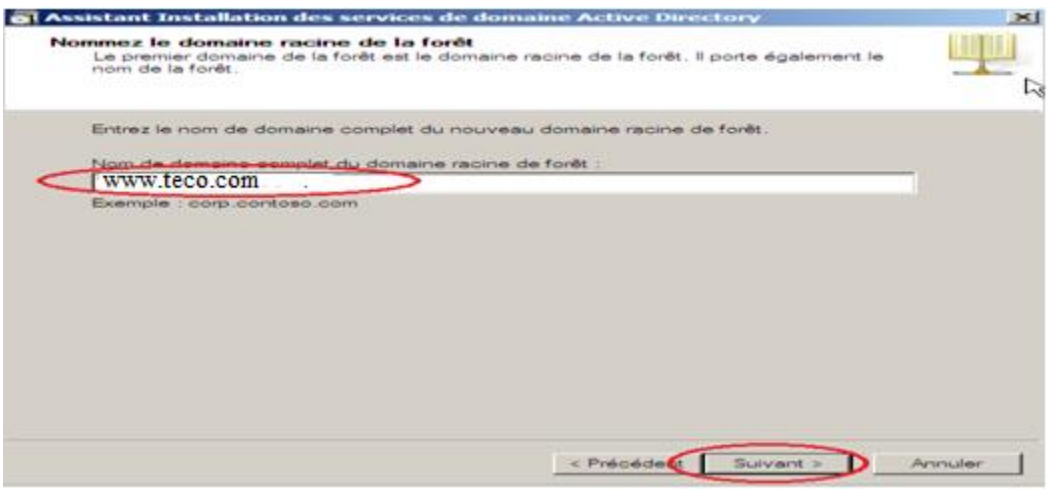


Figure III.2. Nom du domaine Active directory

On aura la figure suivante et on coche sur l'icône DNS pour continuer

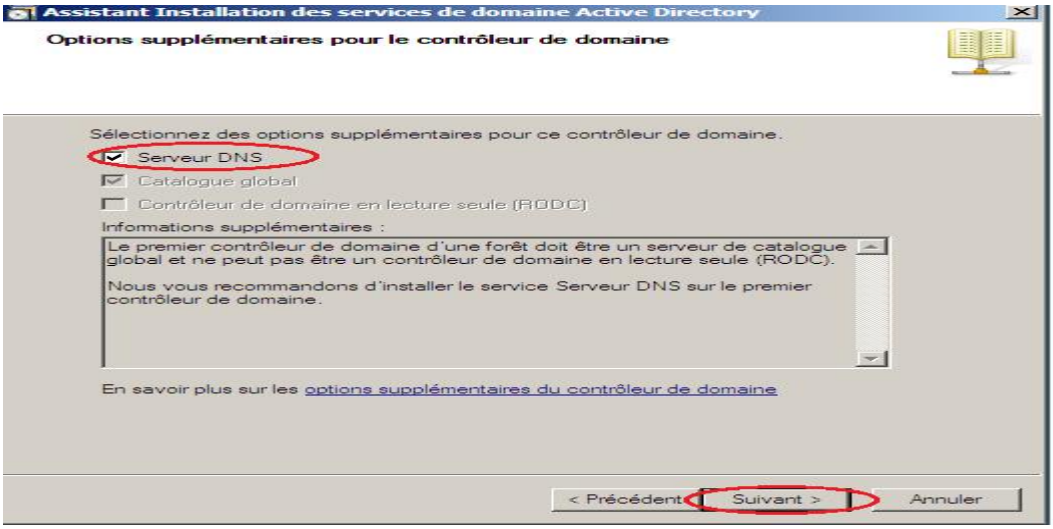


Figure III.3. Configuration du DNS

Dans le menu démarrer, Gestionnaire de serveur, rôles, ajouté des rôles on coche l'icône serveur DHCP pour l'installer

Après l'installation des services on aura la fenêtre suivante

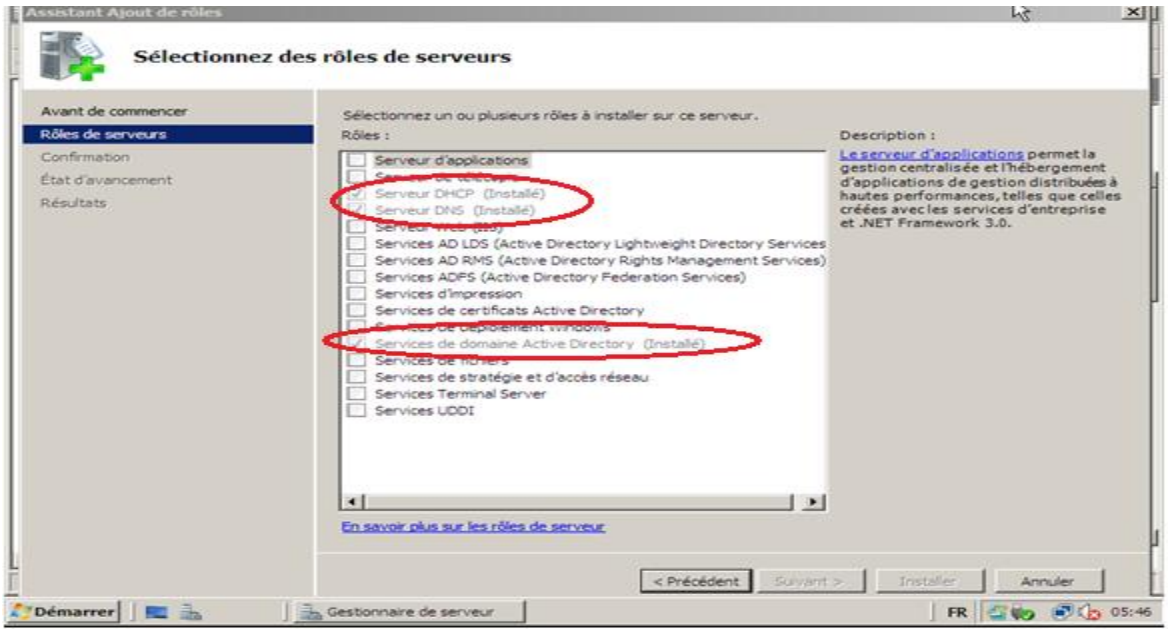


Figure III.4. Résultat de la configuration de domaine Active directory

Dans le domaine nommé «www.teco.com» on a créé une unité d'organisation nommé «départementELN » dont on a créé deux groupes et chaque groupe contient des utilisateurs c'est-à-dire qu'on a créé des comptes aux quels l'utilisateur (travailleur) peut accéder à distance

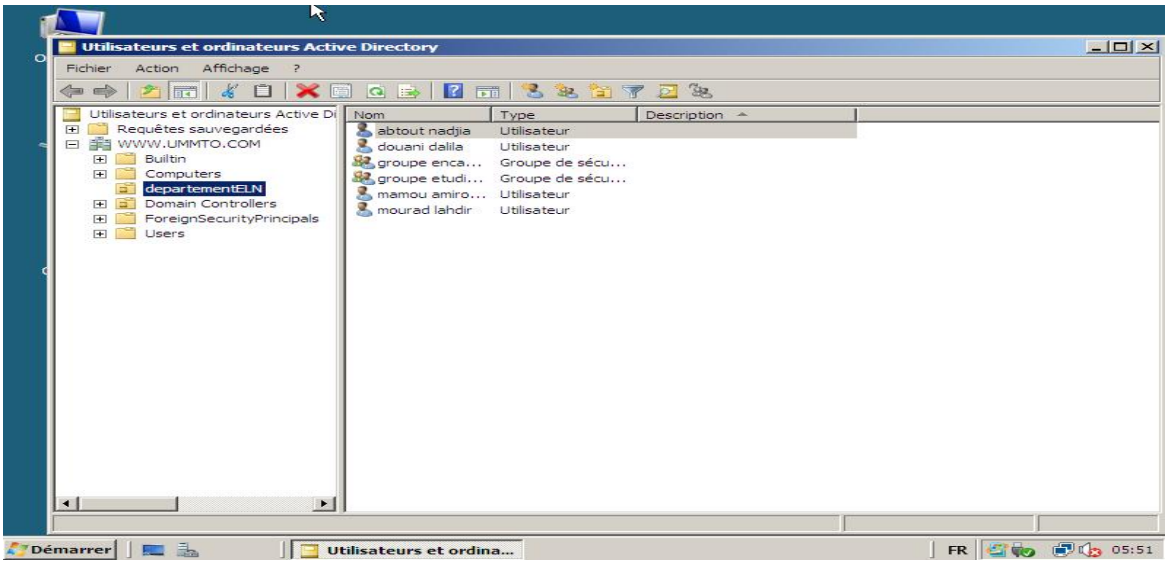


Figure III.5. Utilisateurs et ordinateurs Active directory

III.4.Installation de serveur de fichier

On va créé le serveur de fichier pour pouvoir centraliser le partage des fichiers.

Dans le menu démarrer, Gestionnaire de serveur, rôles, ajouté des rôles on coche l'icône service de fichier

La seconde tache est effectuée à l'aide de la commande « **dcpromo** » en sélectionnant l'icône « Ajouter un contrôleur de domaine à un domaine existant »

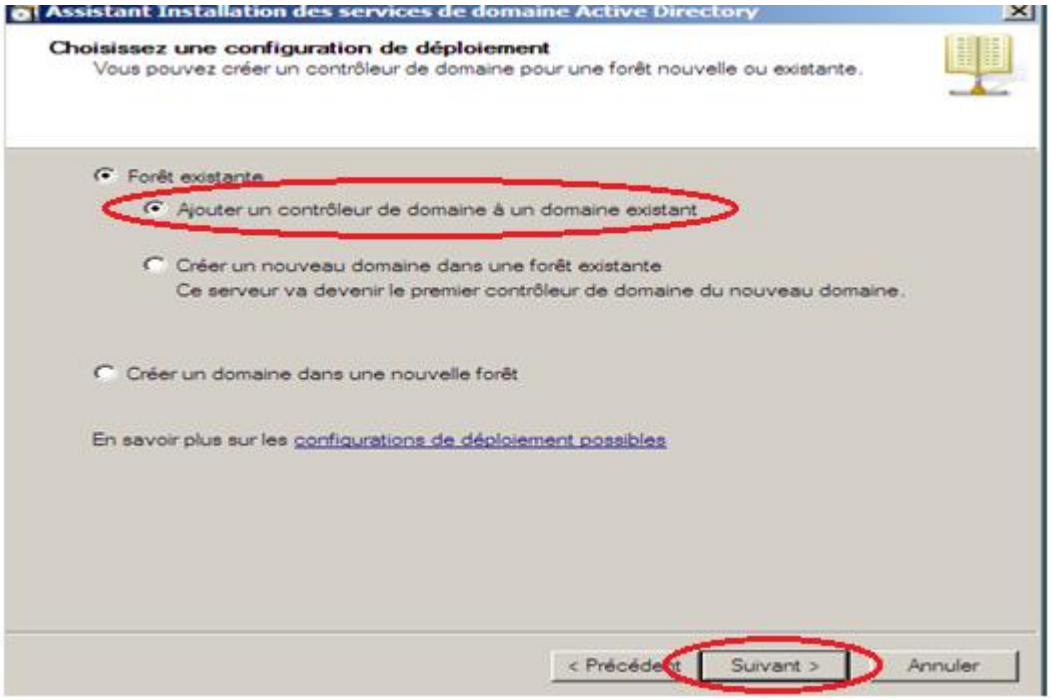


Figure III.6. Choix d'une configuration de déploiement

On aura la fenêtre de dialogue suivante dans laquelle on va spécifier le compte à utiliser pour effectue l'installation et le mot de passe correspondant.

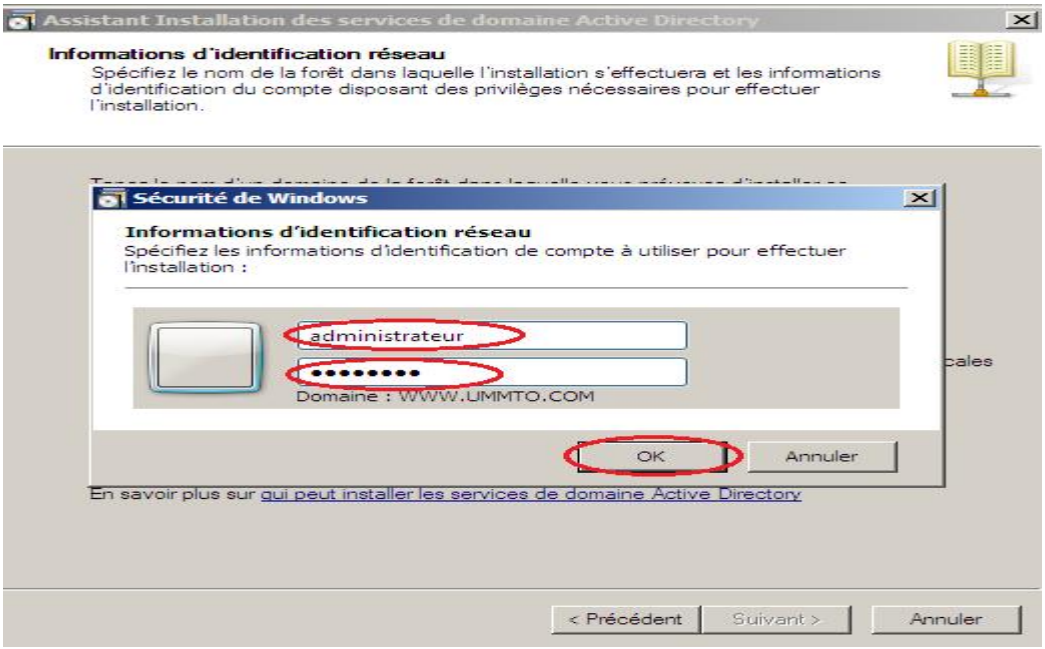


Figure III.7. Informations d'identification réseau

Nous allons gérer le partage des fichiers en autorisant à un groupe (groupe étudiant) l'accès en lecture seul et d'interdire l'accès pour l'autre groupe (groupe encadreurs), pour effectuer cette tache: démarrer, outil d'administration, Gestion de partage et du stockage, on aura la figure suivante

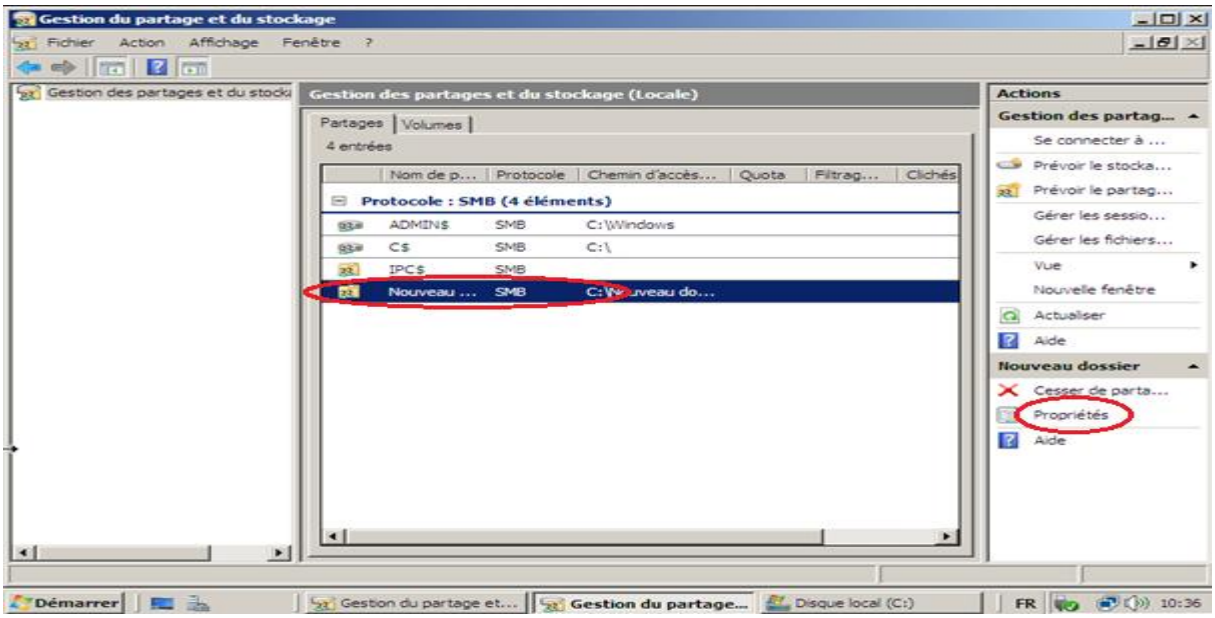


Figure III.8. Partage de dossier

On clique sur « propriétés», Autorisation, Autorisation de partage, on coche l'icône « Lecture »

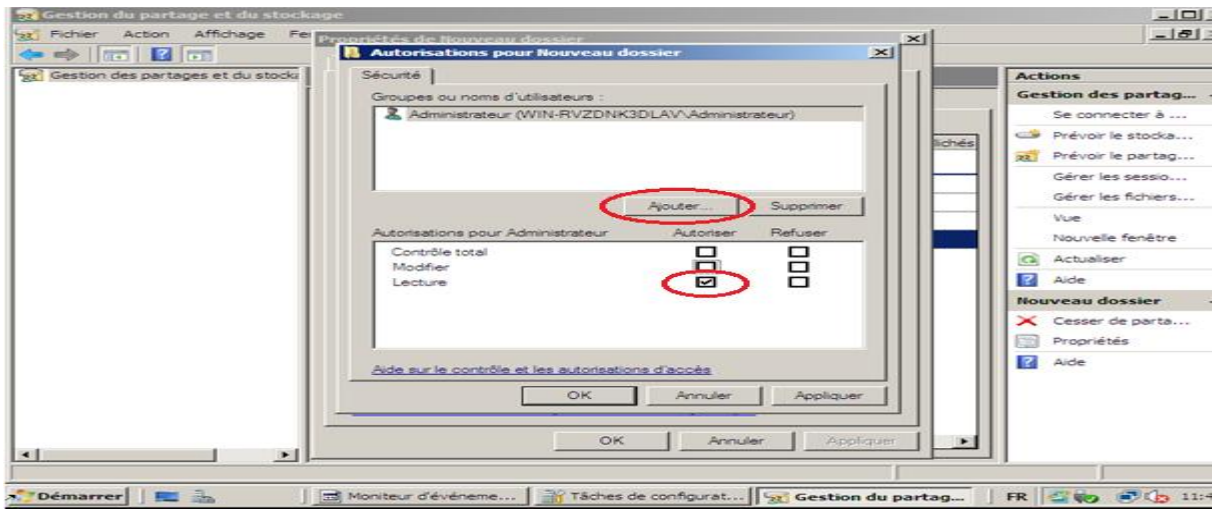


Figure III.9. Spécification du mode de partage

On clique sur l'icône Ajouter, on ajoute au groupes d'utilisateurs le groupe (groupe étudiant) qu'on a autorisé.

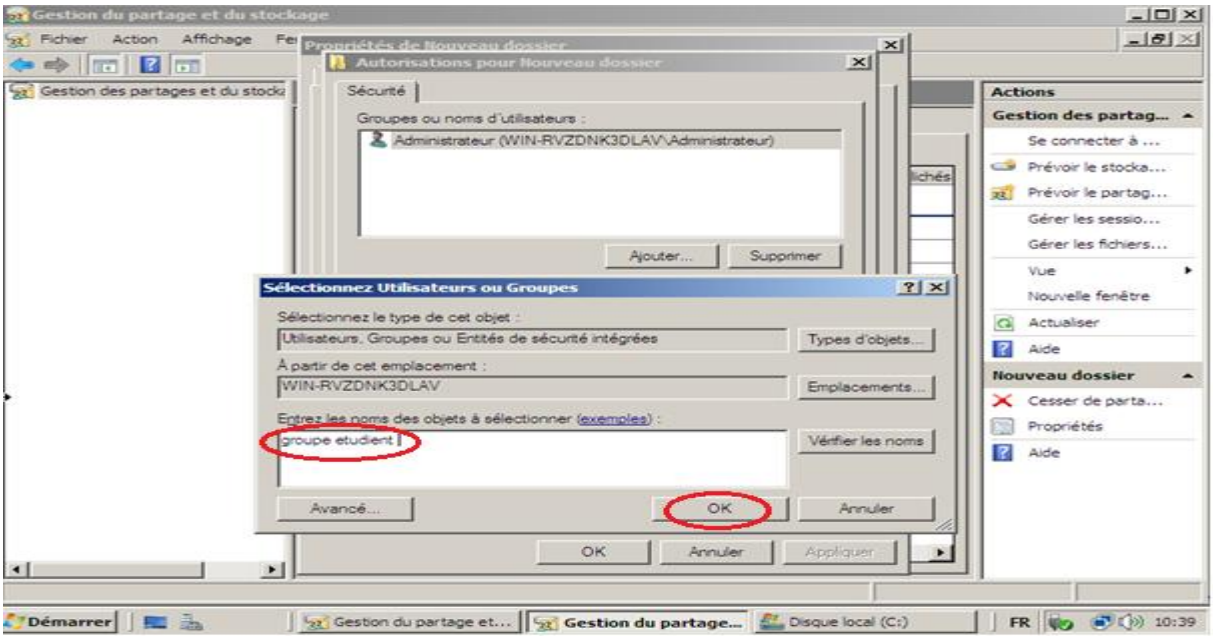


Figure III.10. La sélection d'utilisateurs et groupe

III.5.Installation de serveur Web

L'installation du serveur Web consiste à installer le rôle « serveur Web (IIS)»comme le montre la fenêtre suivante:

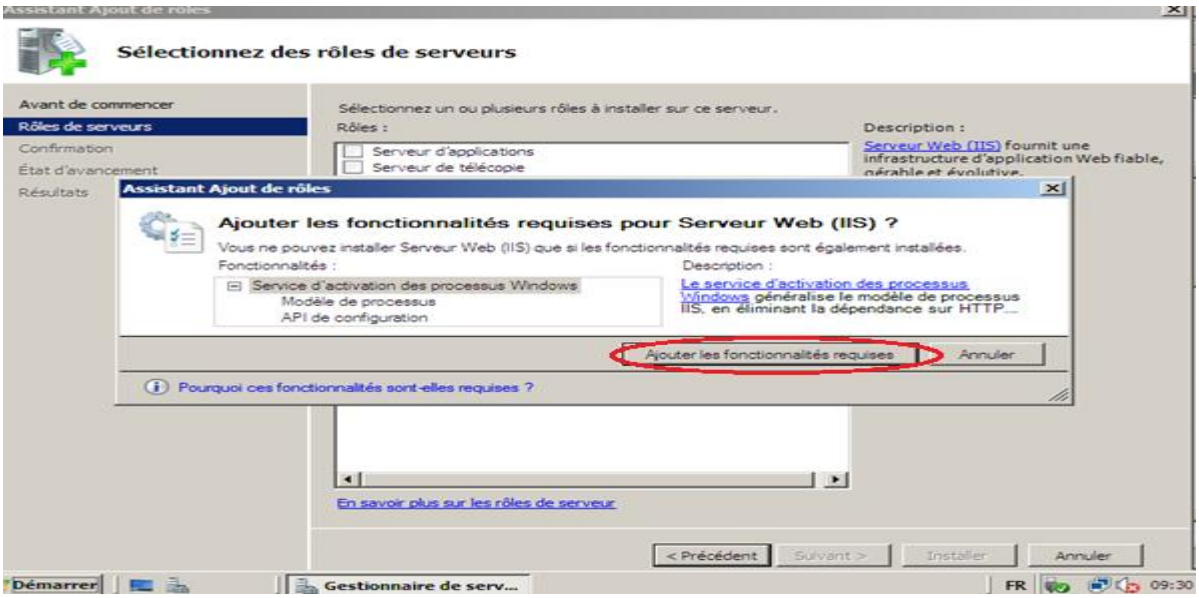


Figure III.11. Installation de serveur Web

Après l'installation de service IIS on va créer un site Web: Dans le menu démarrer, outils d'administration, Gestionnaire des services Internet (IIS), la fenêtre de dialogue suivante s'ouvre, on clique sur « Ajouter un site Web».

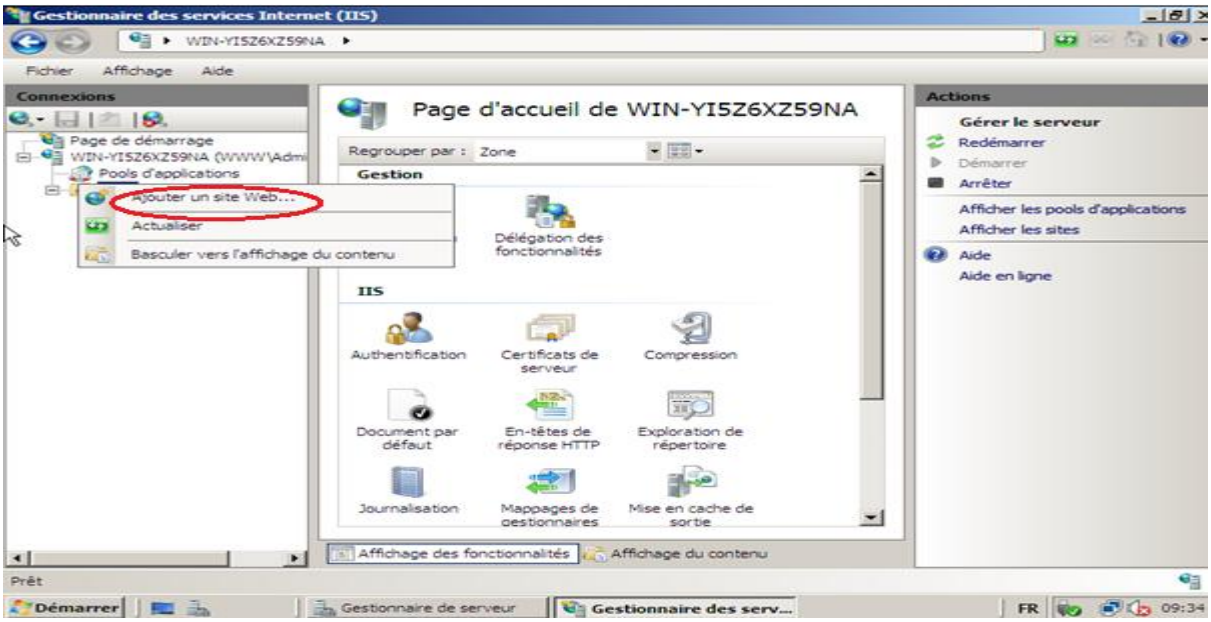


Figure III.12. Création d'un site Web

III.6.Le logiciel «GNS3»

GNS3 est un simulateur graphique d'équipement réseaux qui nous permet de créer des topologies de réseaux complexes et d' établir des simulations. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco. L'IOS c'est le système d'exploitation des routeurs et Switch et firewall Cisco et pour entrer dans l'interface graphique de chaque éléments il faut télécharger son IOS, GNS3 est compatible avec : Windows, Linux,…etc.

La figure III.13 est la première qui s'œuvre lorsque on click sur le logiciel «GNS3», cette figure nous présente l'emplacement des différentes icones qu'on utilise pour créer un réseau:

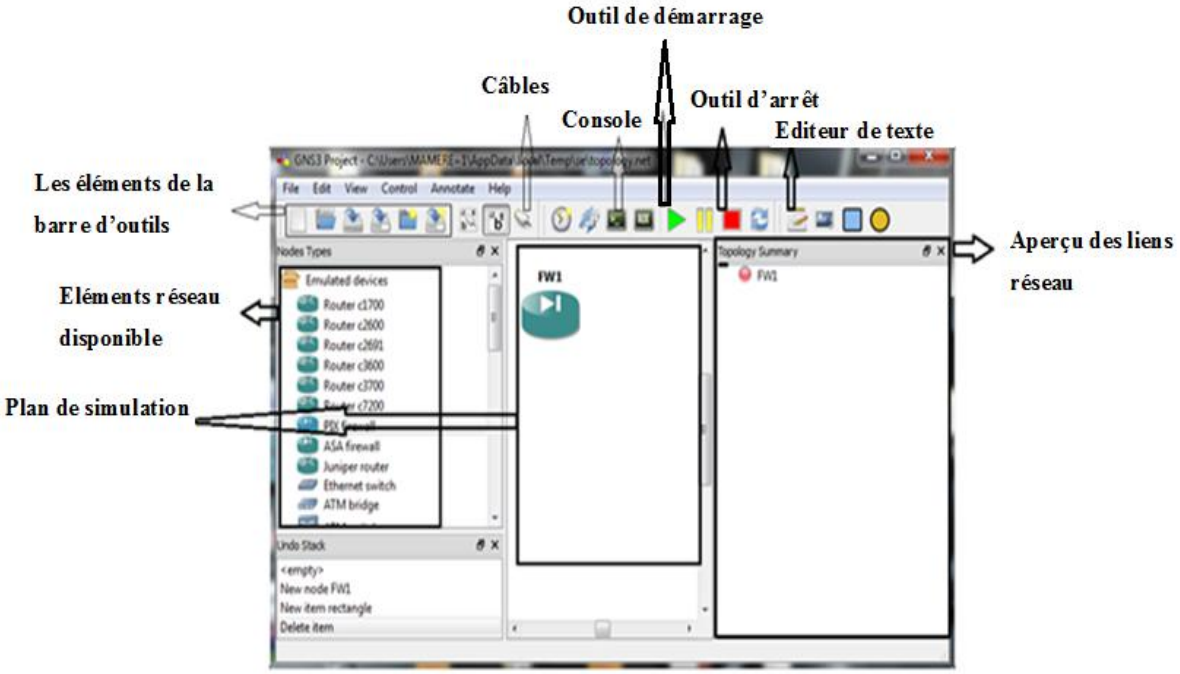


Figure III.13. Détail de la fenêtre du simulateur

Pour ce qui concerne la configuration d'un firewall (ASA), On click sur EDIT puis Préférences la figure III.14 s'œuvre. Puis on suit les étapes suivantes:

- Sélectionner l'onglet **Qemu.**
- Dans le champ binary image on click sur parcourir (…) pour indiquer l'emplacement de l'IOS du ASA, on charge l'image «Initrd» et l'image «Kernel»
- On click sur « Save» puis « APPLY» et «OK»

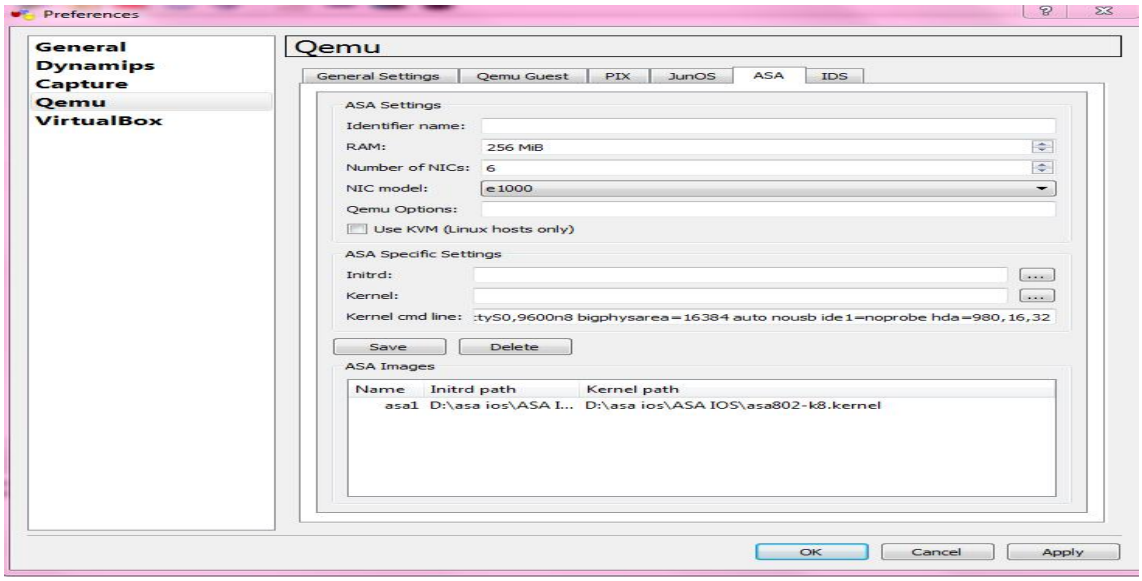


Figure III.14. Localisation du binaire de Qemu

La deuxième partie de notre travail consiste à configurer le routeur et l'ASA

III.7.Configuration du routeur:

On introduit les adresses IP pour les interfaces et on les active pour pouvoir les interconnecter aux autres réseaux, les commandes sont les suivantes:

```
Router(config)#int f0/0
Router(config-if)#ip add 209.0.0.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#ex
*Mar  1 00:01:30.167: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:01:31.167: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config)#int f0/1
Router(config-if)#ip add 200.0.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
*Mar  1 00:02:00.891: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:02:01.891: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

III.8.Configuration de protocole de routage:

Un routeur relie plusieurs réseaux. Pour ce faire, il dispose de plusieurs interfaces chacune appartenant à un réseau IP différent. Lorsqu'un routeur reçoit un paquet IP sur une interface, il détermine laquelle (interface) utiliser pour transférer le paquet vers sa destination et pour cet objectif, on utilise le protocole de routage RIP et on cite les réseaux qui sont connectés directement aux deux interfaces de routeur.

```
Router(config-if)#router rip
Router(config-router)#version 2
Router(config-router)#network 200.0.0.0
Router(config-router)#network 209.0.0.0
Router(config-router)#exit
```

III.9.Configuration des interfaces du l'ASA

Rappelons-nous le principe de fonctionnement de l'ASA. Chaque interface d'ASA possède un niveau de sécurité compris entre 0 et 100. Si nous accordons une grande confiance au réseau se trouvant derrière une interface (le réseau dont nous avons la maîtrise par exemple), nous allons lui attribuer un niveau de sécurité élevé (100). A l'inverse, si nous n'avons pas confiance en un réseau (par exemple Internet), nous lui attribuerons un niveau de sécurité 0.

La zone DMZ nous lui attribuerons un niveau de sécurité 50 pour que l'accès à cette zone soit similaire au réseau interne et au réseau externe.

```
ciscoasa> en
Password:
ciscoasa# config t
ciscoasa(config)# int e0/0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# ip add 10.0.0.1 255.0.0.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# int e0/1
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# ip add 209.0.0.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# int e0/2
ciscoasa(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)# security
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip add 192.168.0.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

On configure le protocole RIP pour l'ASA et on cite les trois réseaux directement connectés.

```
ciscoasa(config)# router rip
ciscoasa(config-router)# version 2
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 209.0.0.0
ciscoasa(config-router)# network 192.168.0.0
ciscoasa(config-router)# exit
```

Dans cette étape nous allons tester le fonctionnement de l'ASA et nous essayerons d'accéder aux différents réseaux en utilisant le navigateur web (la page web de chaque réseau déjà créée) de chaque poste. Pour lancer le test on donne l'adresse IP de destinataire illustrée dans la figure suivante:

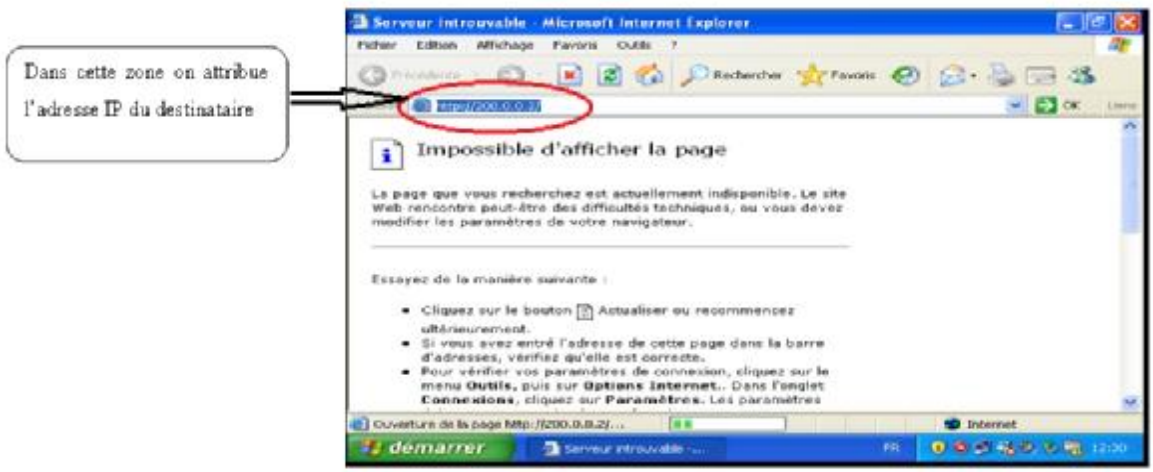


Figure III.15. Test avec le navigateur Web

D'après le principe de fonctionnement de l'ASA, les clients du réseau LAN peuvent accéder à la DMZ et au réseau externe (serveur Web), les postes de la DMZ peuvent accéder au réseau externe (serveur Web) mais ne peuvent pas accéder au réseau LAN, alors que le serveur Web ne peut pas accéder ni à la DMZ ni au réseau LAN.

Premièrement, nous testons l'accès du réseau LAN vers le réseau externe (serveur Web 200.0.0.2) et vers la DMZ (poste 192.168.0.2)

Le premier test est réussi: le client à accéder au serveur Web.

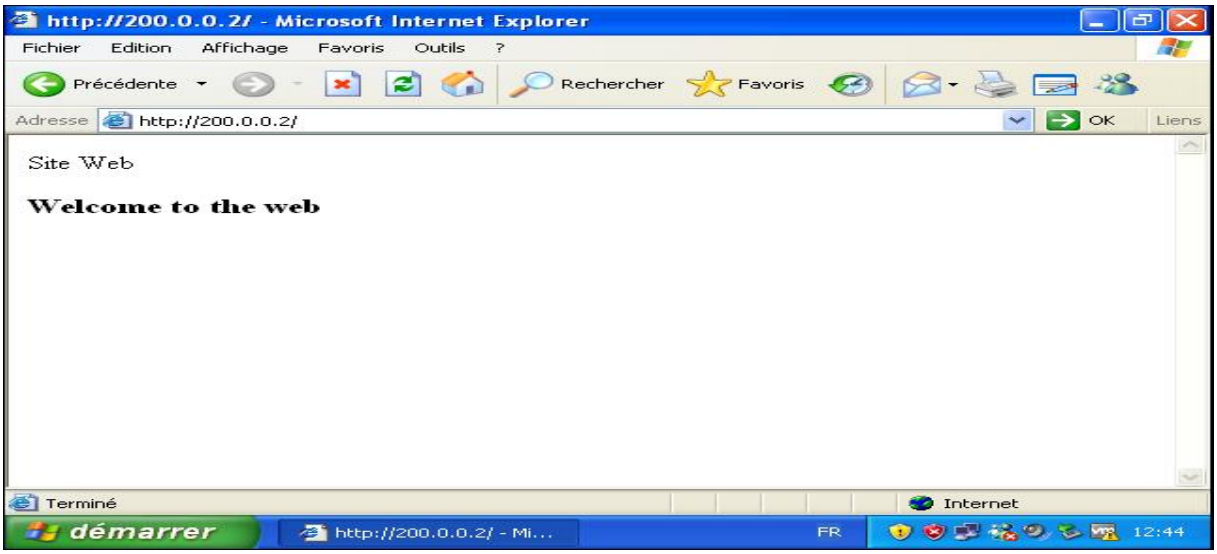


Figure III.16. Résultat de test d'accès du client au serveur Web

Le client a accédé à la DMZ

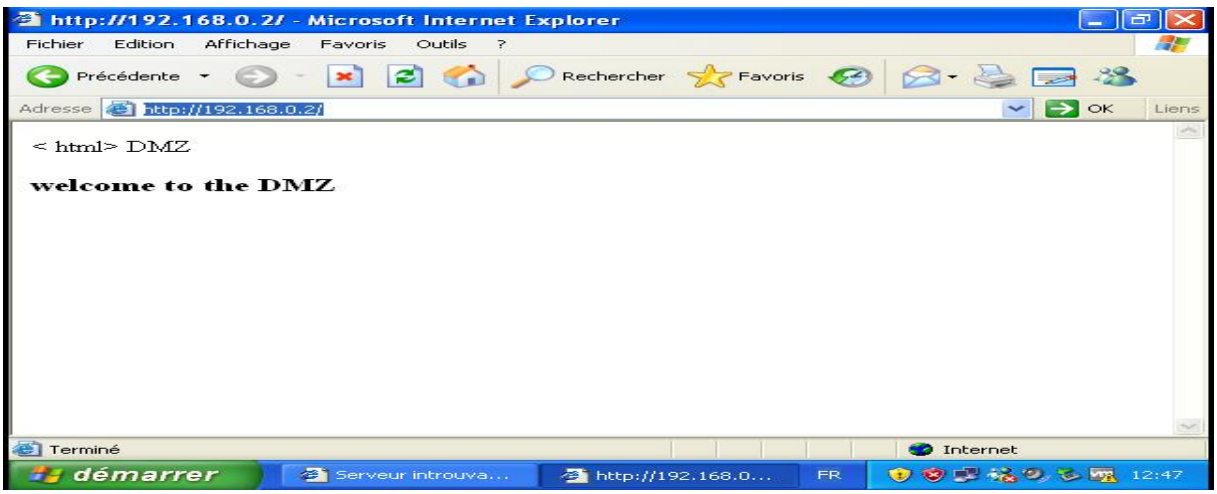


Figure III.17. Résultat de test d'accès du client à la DMZ

Deuxièmement, nous testons l'accès de la DMZ vers le réseau LAN (poste 10.0.0.2) et le réseau externe (serveur Web 200.0.0.2):

a- La DMZ accède au réseau externe (serveur Web)

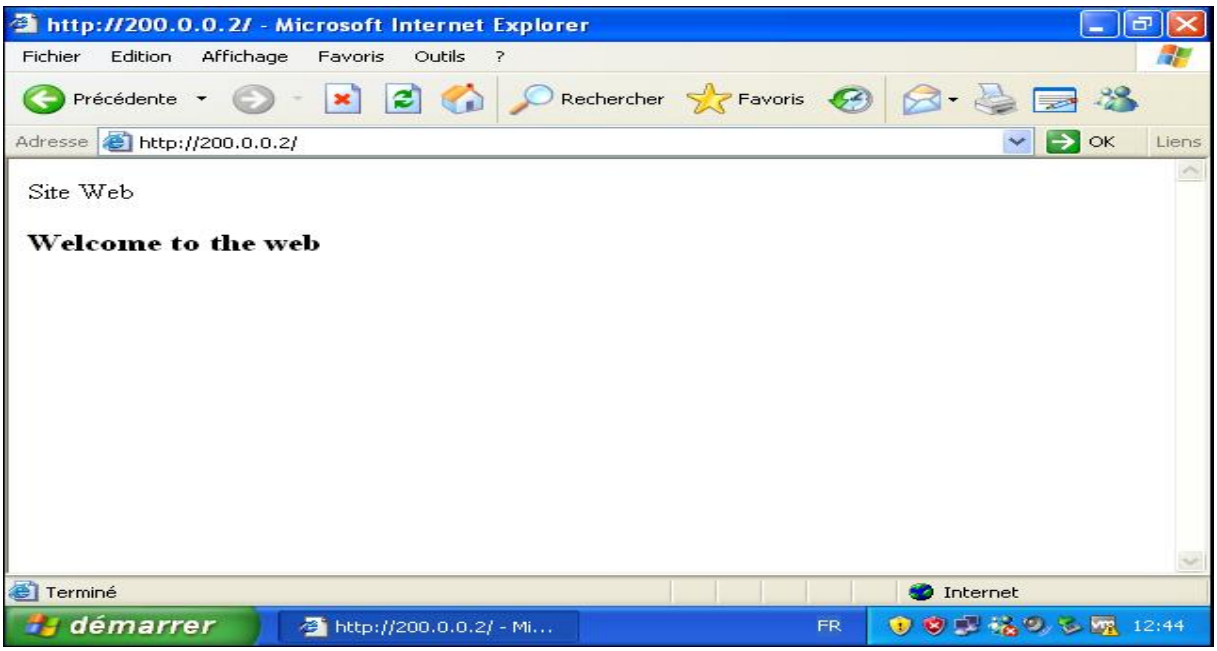


Figure III.18. Résultat de test d'accès de la DMZ au serveur Web

b- La DMZ n'a pas pu accéder au réseau LAN

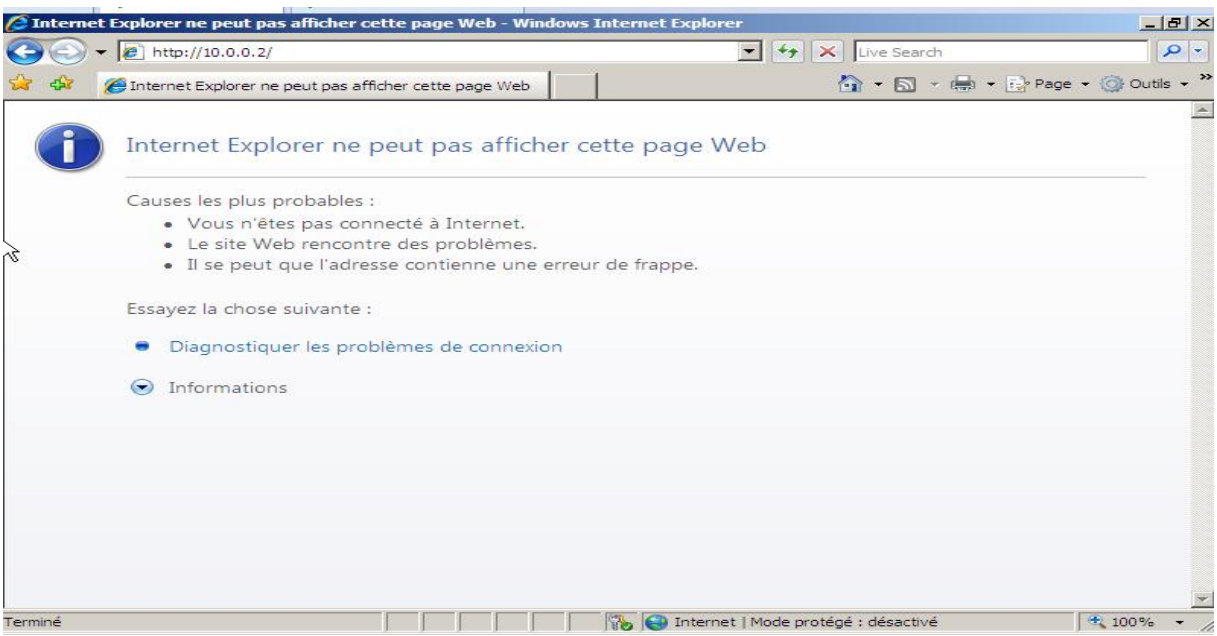


Figure III.19. Résultat de test d'accès de la DMZ au réseau LAN

Enfin nous allons tester l'accès de réseau externe (serveur Web) vers le réseau LAN (10.0.0.2) et la DMZ (192.168.0.2):

a- Le serveur Web ne peut pas accéder au réseau LAN

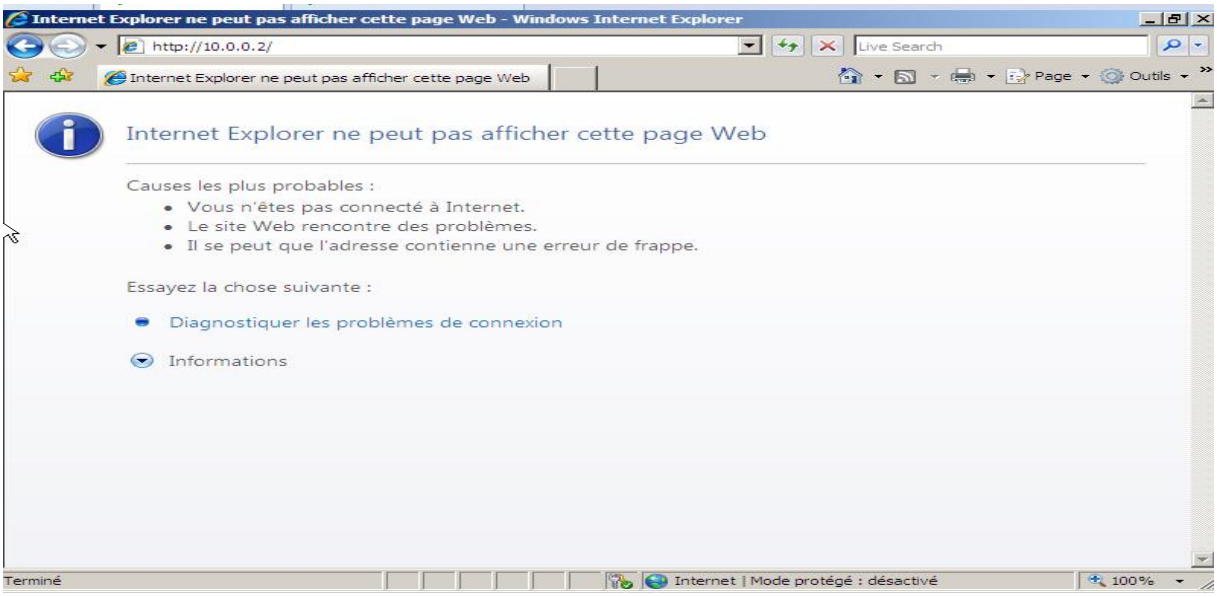


Figure III.20. Résultat de test d'accès du serveur Web au réseau LAN

b- Le serveur Web ne peut pas accéder à la DMZ

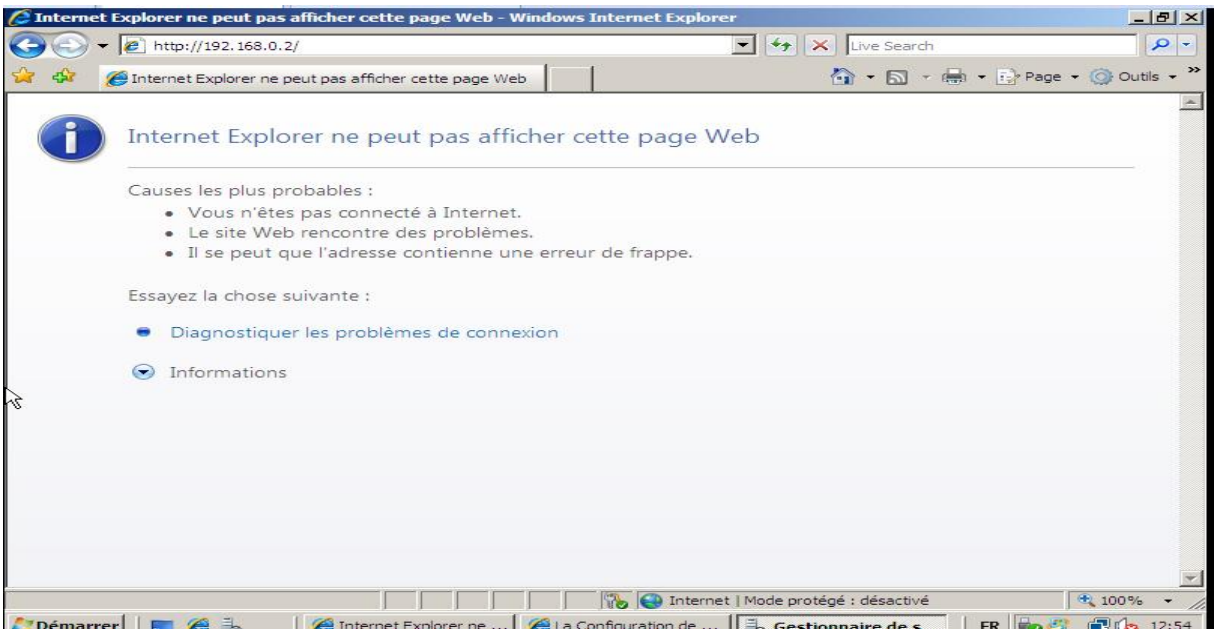


Figure III.21. Résultat de test d'accès du serveur Web à la DMZ

Les résultats des tests effectués pour l'ASA sont bons, l'ASA fonctionne convenablement.

III.10.Configuration des ACL

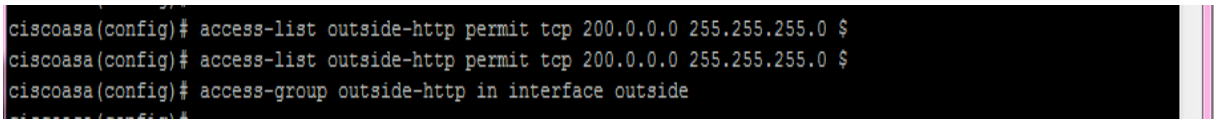
Pour pouvoir autoriser le trafic entre un réseau de niveau de sécurité inferieur à un autre réseau de niveau de sécurité supérieur, on fait appel aux ACL

Les ACL permettent de maître en place la stratégie de filtrage à effectuer, On configure une ACL avec la commande suivante:

Access-list outside-http permit tcp 200.0.0.0 255.255.255.0 192.168.0.0 255.255.255.0 eq X

X: désigne le numéro du port.

On autorise le service http (port 80) ainsi que HTTPS (port443) pour permettre à la DMZ de se connecter à internet et récupérer des données comme nous le montre la figure suivante:



La figure suivante montre Le résultat de test d'accès de serveur Web vers la DMZ après la configuration des ACL.

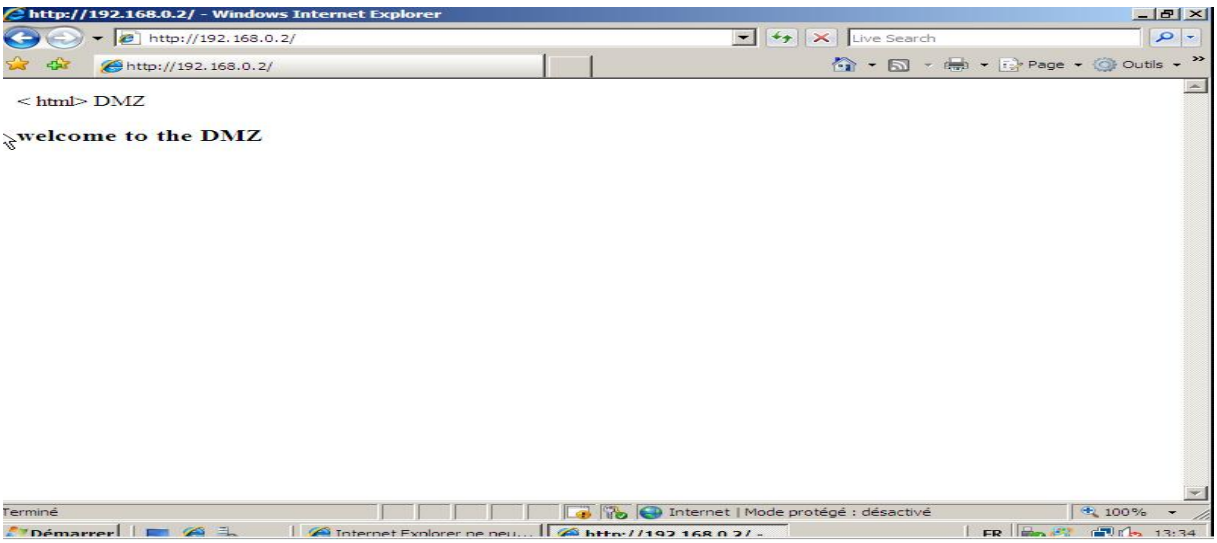


Figure III.22. Résultat de test d'accès du serveur Web au réseau LAN

III.11.Le service Telnet

Le service Telnet permet aux travailleurs nomades d'accéder à distance à leurs comptes dans le serveur d'entreprise et effectuer leurs travaux, il doit être installé sur le serveur puis configuré au niveau de l'ASA. Pou installer le service Telnet au niveau du serveur:

On clique sur le menu démarrer, Gestionnaire de serveur, fonctionnalité, ajouter les fonctions, on coche l'icône serveur Telnet et l'icône client Telnet comme nous le montrent les figures suivantes respectivement.

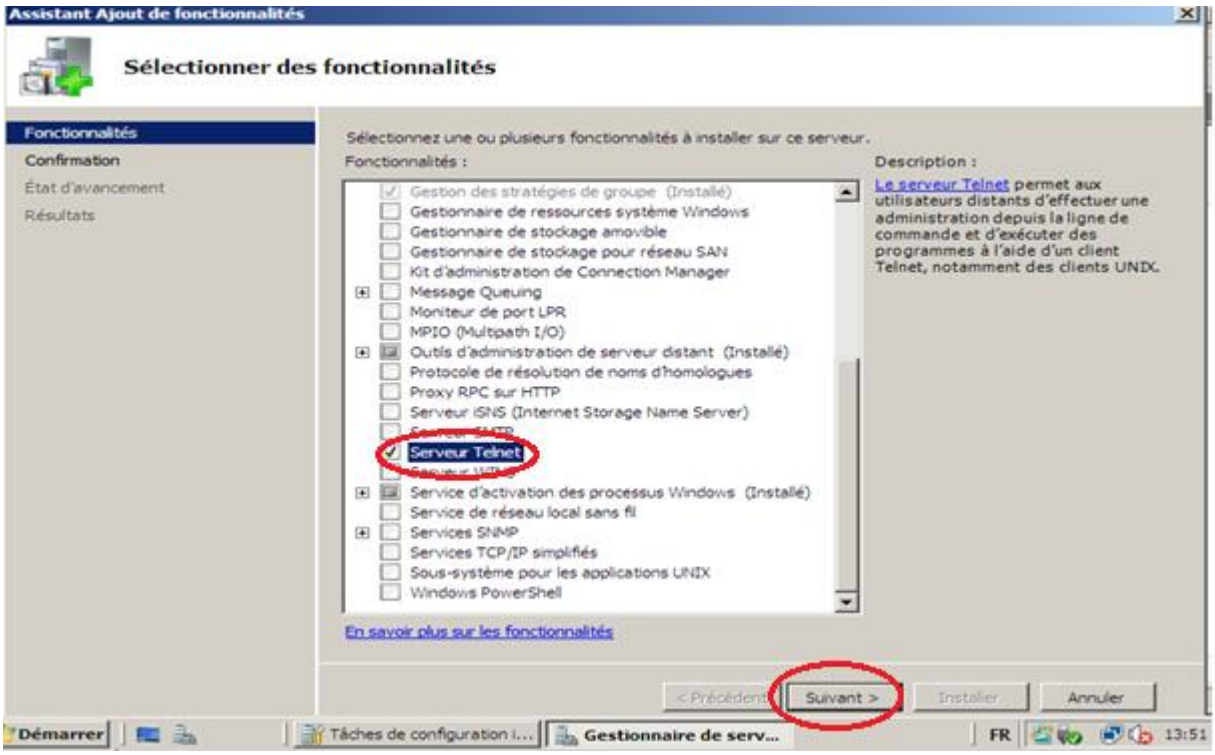


Figure III.23. Installation du Serveur Telnet

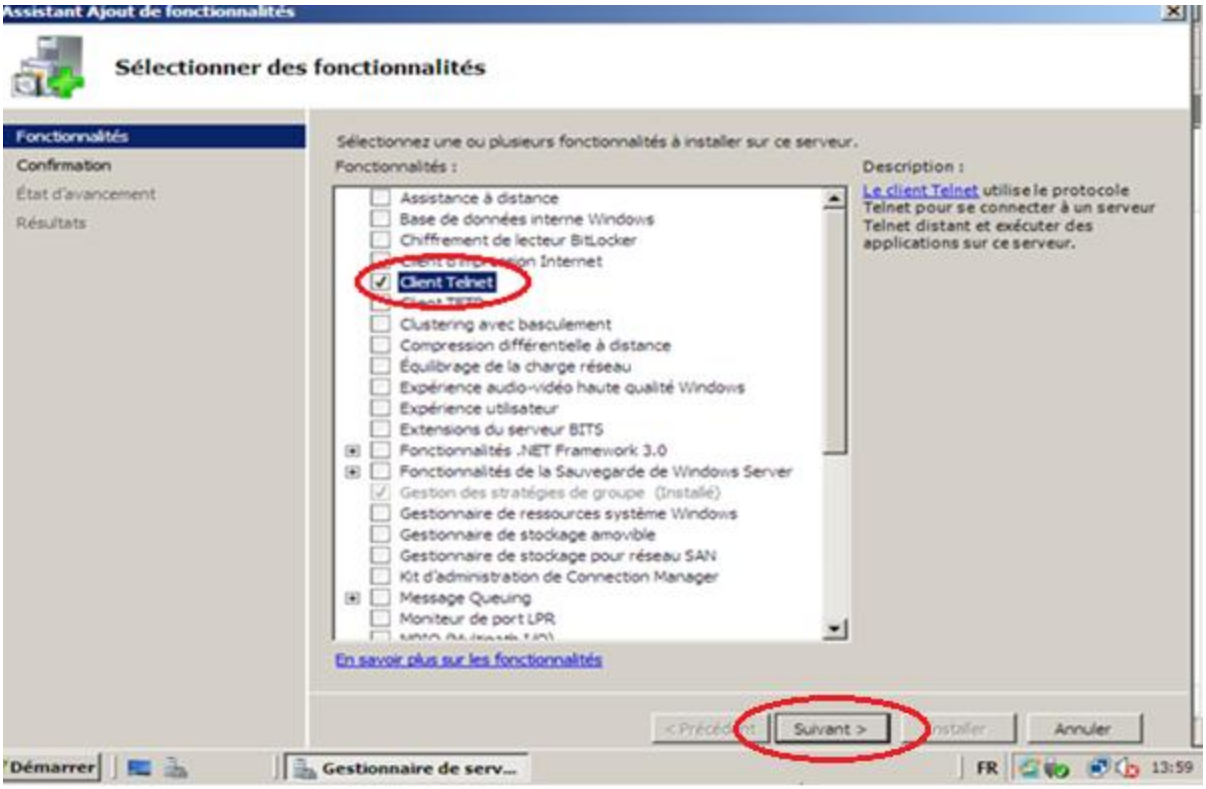


Figure III.24. Installation du client Telnet

Ainsi les résultats de l'installation:

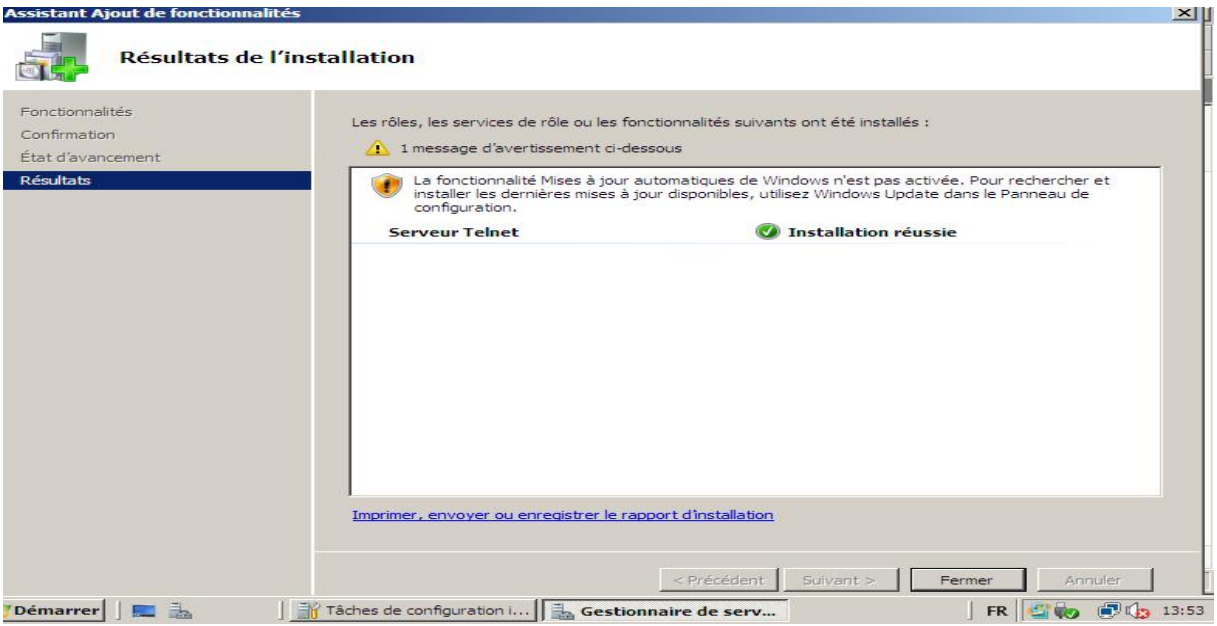


Figure III.25. Résultat d'installation du Serveur Telnet

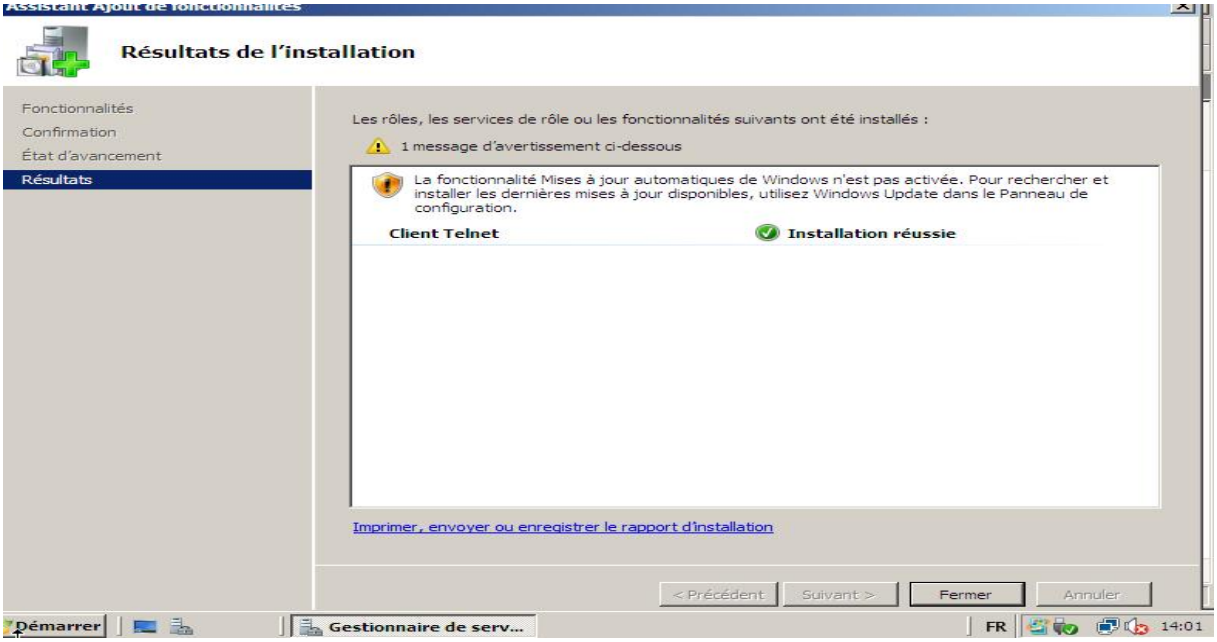


Figure III.26.Résultat d'Installation du client Telnet

+

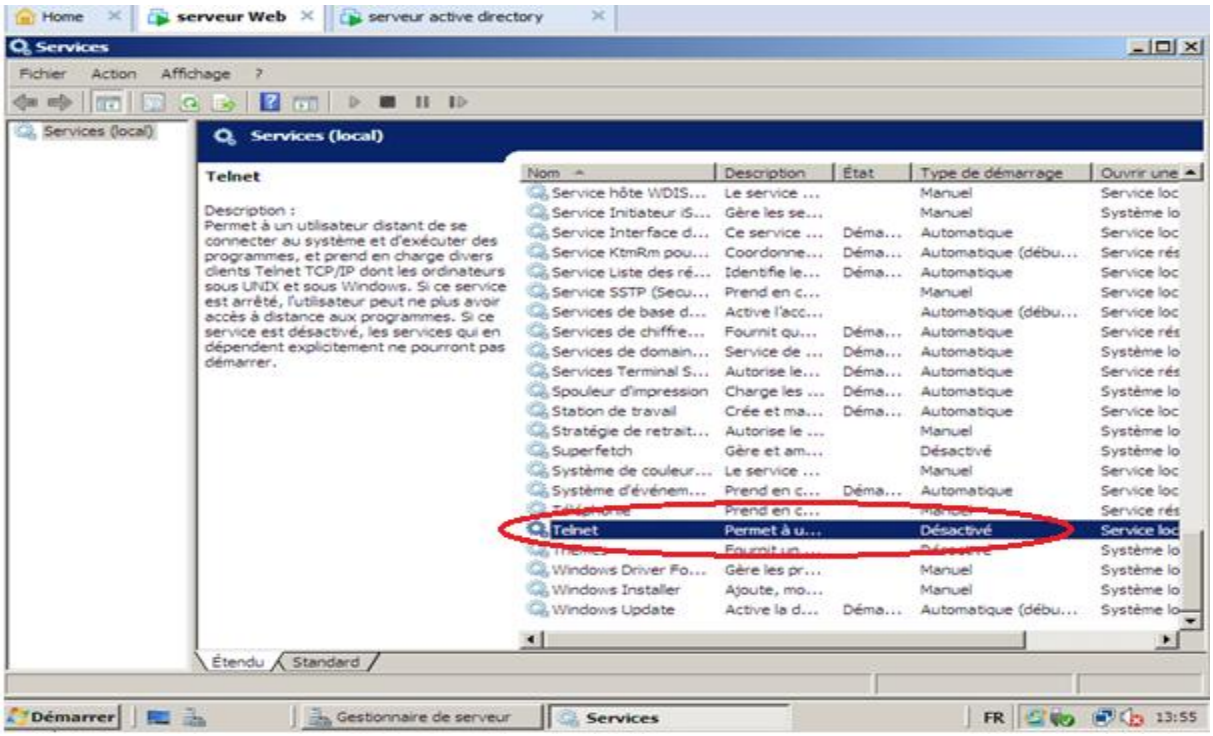


Figure III.27. Installation du Service Telnet

Une page de dialogue s'affiche, on change le type de démarrage au mode «Automatique».

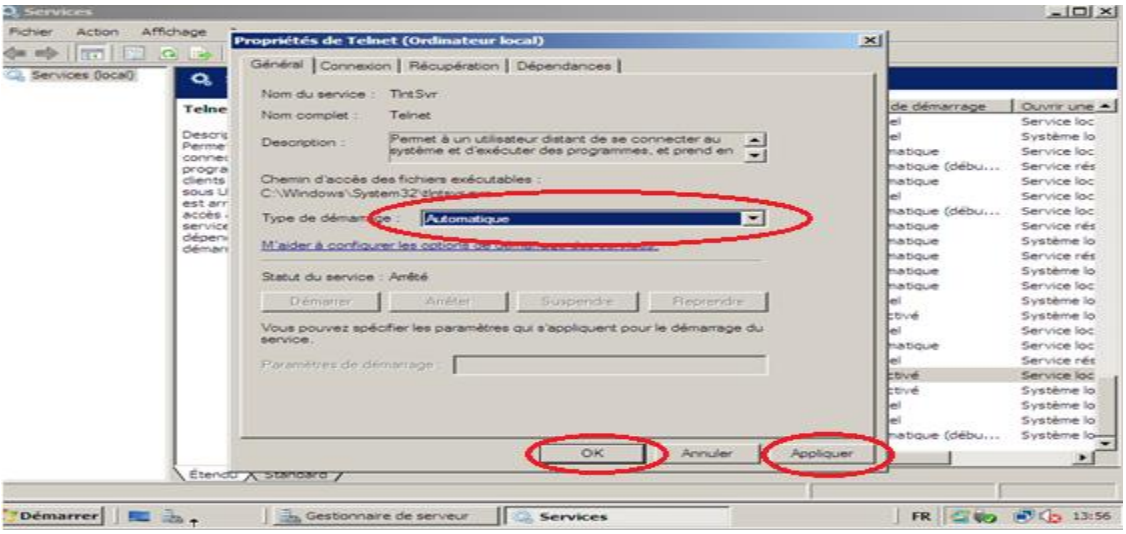


Figure III.28. Choix du mode de démarrage Telnet

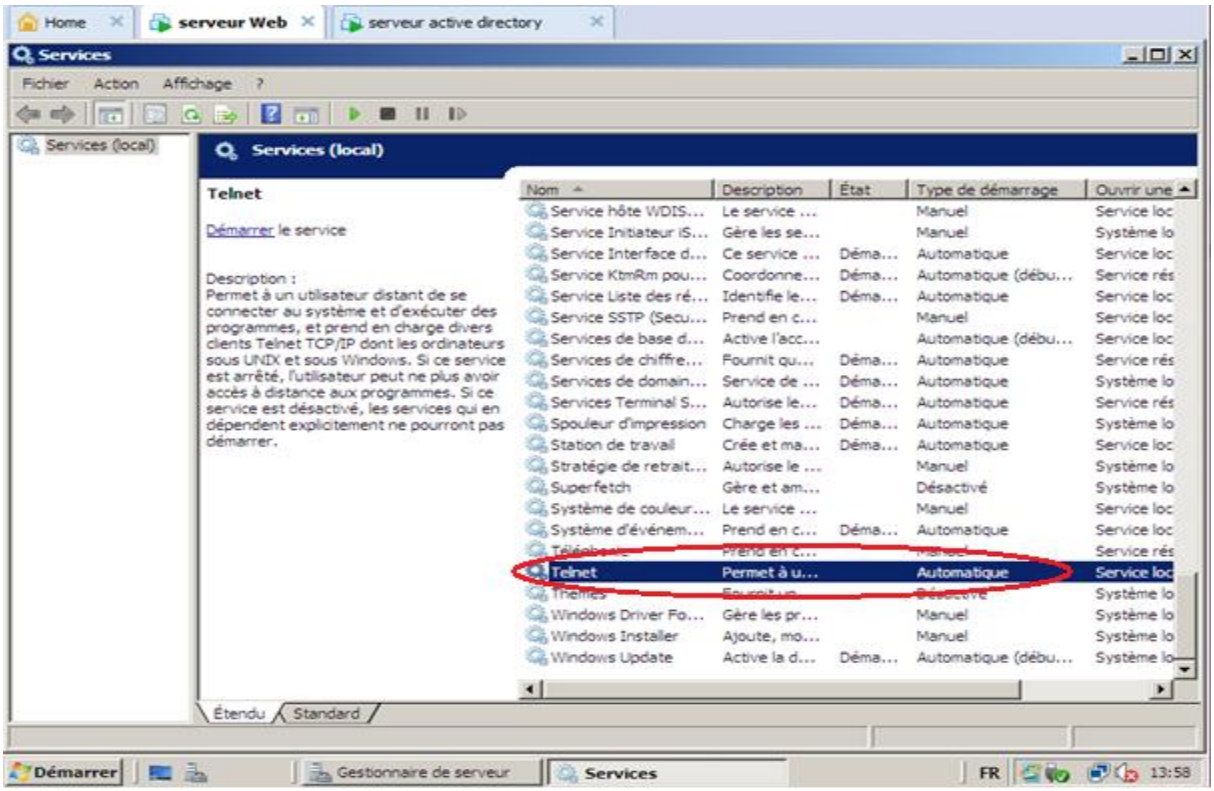


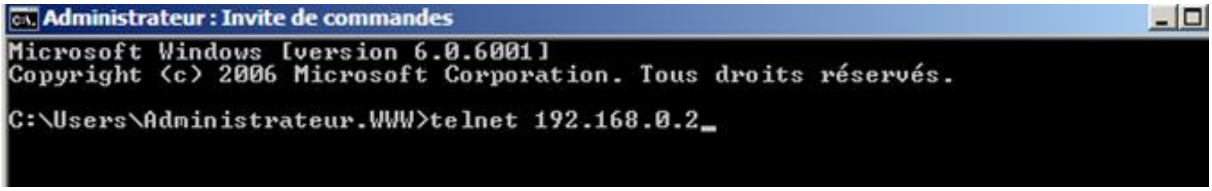
Figure III.29. Résultat d'installation de service Telnet

On autorise le service Telnet (port 69) au niveau de l'ASA comme suit:

```
ciscoasa(config)#
ciscoasa(config)# access-list outside-http permit tcp 200.0.0.0 255.255.255.0 $
ciscoasa(config)#
```

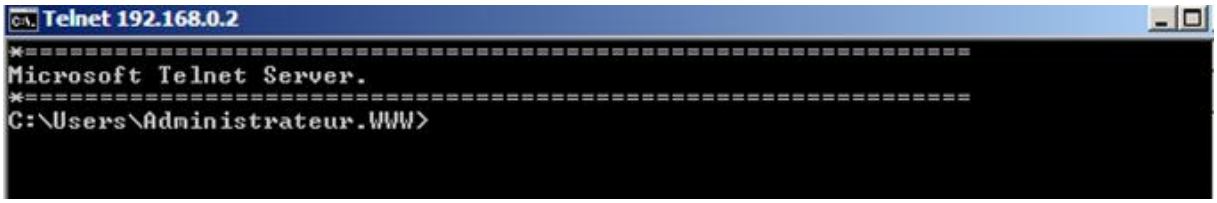
Le test de Telnet:

A partir du serveur web, dans l'invite de commande, on tape Telnet 192.168.0.2:

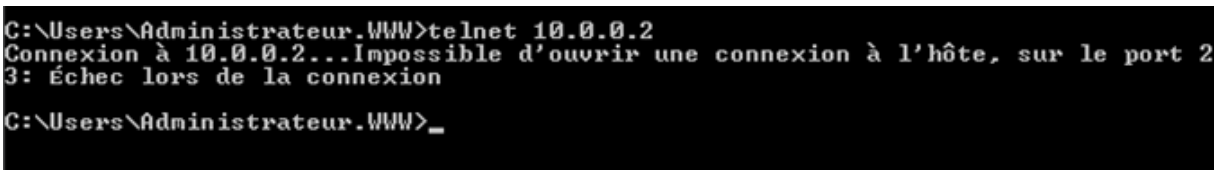


Il nous demande de s'authentifier pour pouvoir accéder au serveur des fichiers

On a accédé à l'intérieur de l'invite de commande de serveur des fichiers



On ne peut pas accéder au réseau LAN avec le service Telnet car l'ASA interdit le trafic du réseau externe vers le réseau LAN comme le montre la teste suivant



Le test de ping :

On a essayé ,au prealable,notre test de ping et les résultats sont presentés ci-dssous:

```
C:\Documents and Settings\Administrateur>ping 200.0.0.2

Envoi d'une requête 'ping' sur 200.0.0.2 avec 32 octets de données :

Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 200.0.0.2:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Documents and Settings\Administrateur>ping 192.168.0.2

Envoi d'une requête 'ping' sur 192.168.0.2 avec 32 octets de données :

Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.0.2:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

En conséquence, les postes ne peuvent pas faire le Ping, cela devrait marcher car le ping est initié du côté le plus sécurisé, mais par défaut, l'ASA ne fait pas de suivi d'état ICMP et pour remédier à ce problème nous allons activer l'inspection ICMP.

a- Créer l'inspection

```
ciscoasa(config)# class-map inspection-default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
```

b- Activer l'inspection ICMP

```
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# class inspection-default
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# inspect icmp error
ciscoasa(config-pmap-c)# exit
```

L'étape précédente n'est pas une solution complète pour le problème, nous devons créer des access-list adaptées au type de trafic que l'on veut faire passer

c- Configurer l'ACL pour autoriser le ping

```
ciscoasa(config)#  access-list outside-ping permit icmp 200.0.0.0 255.255.255.$
ciscoasa(config)# access-group outside-ping in interface outside
```

III.12. Autoriser le TFTP et FTP

Le service FTP est activé par défaut dans les serveurs alors que le service TFTP n'est pas activé donc il faut l'activer au niveau de serveur, pour cela on clique sur le menu démarrer, Gestionnaire de serveur, fonctionnalité, ajouter les fonctions et on coche l'icône client TFTP

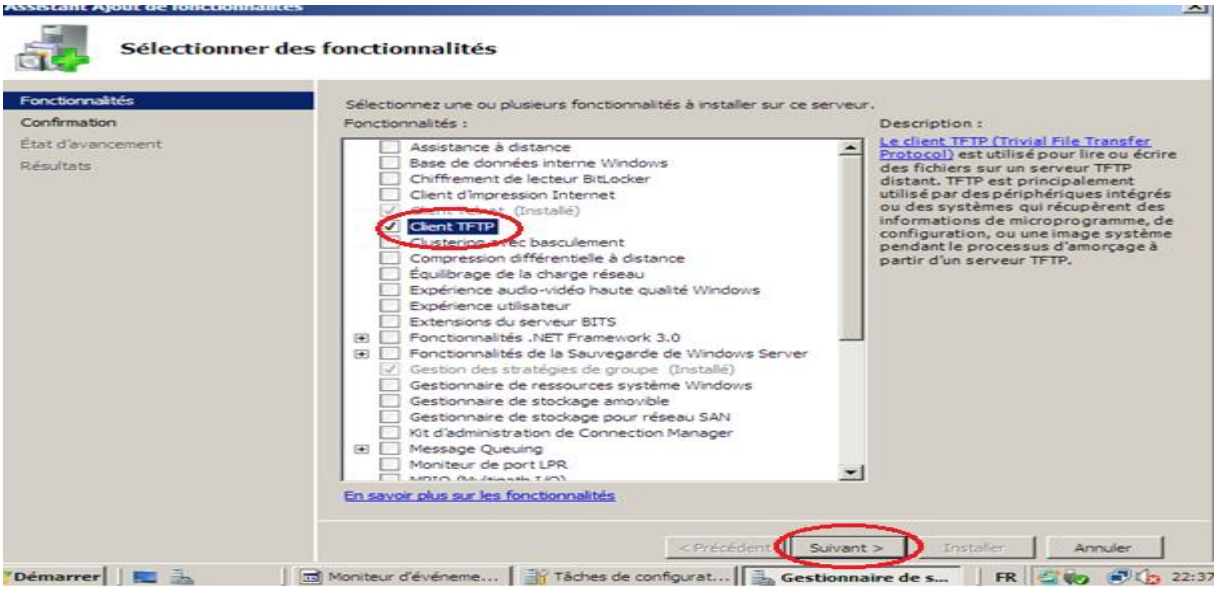


Figure III.30. Installation du Client TFTP

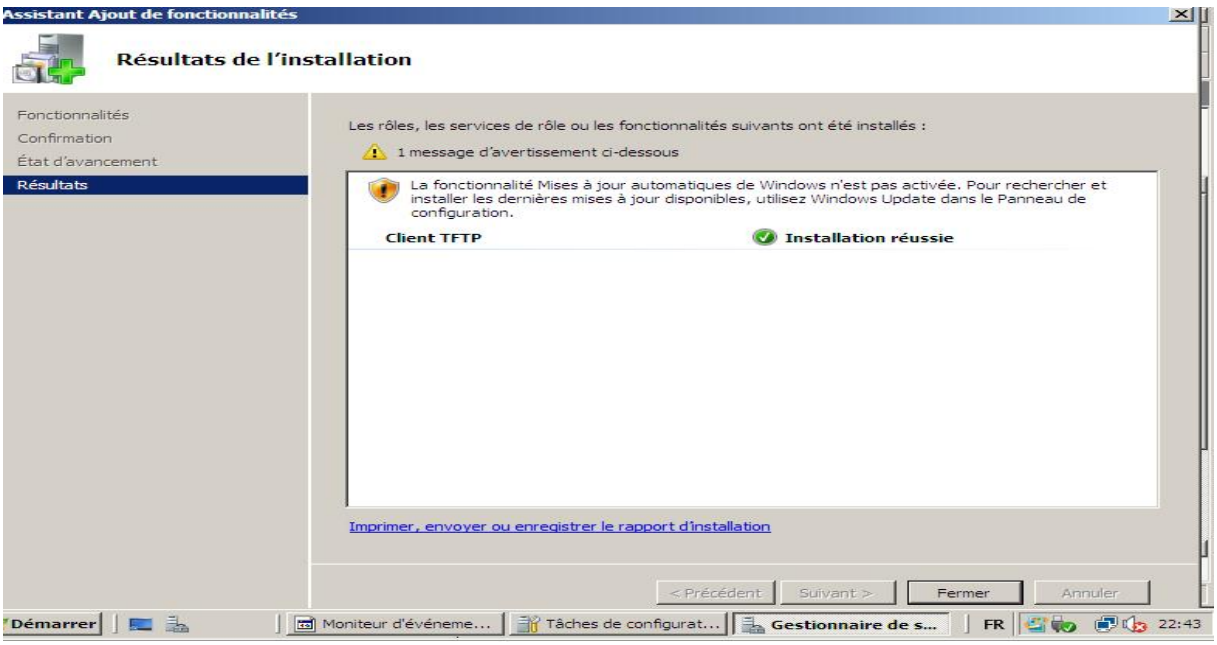


Figure III.31. Résultat d'installation du Client TFTP

a- Configurer l'inspection TFTP et FTP

```
ciscoasa(config)# access-list outside-http permit tcp 200.0.0.0 255.255.255.0 $
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)#  class inspection-default
ciscoasa(config-pmap-c)# inspect ftp
ciscoasa(config-pmap-c)# inspect tftp
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)#
```

a- Configurer l'ACL pour autoriser le service TFTP (port 69)

```
ciscoasa(config-pmap-c)# access-list outside-tftp permit tcp 200.0.0.0 255.255$
ciscoasa(config)# access-group outside-tftp in interface outside
```

La commande suivante permet de copier le fichier de configuration du routeur vers le serveur TFTP: **copy runnig-config tftp**

III.13.Service SNMP: permet de gérer les équipements réseaux

Activer le service SNMP au niveau du serveur: menu démarrer, Gestionnaire de serveur, fonctionnalité, ajouter les fonctions et on coche l'icône service SNMP

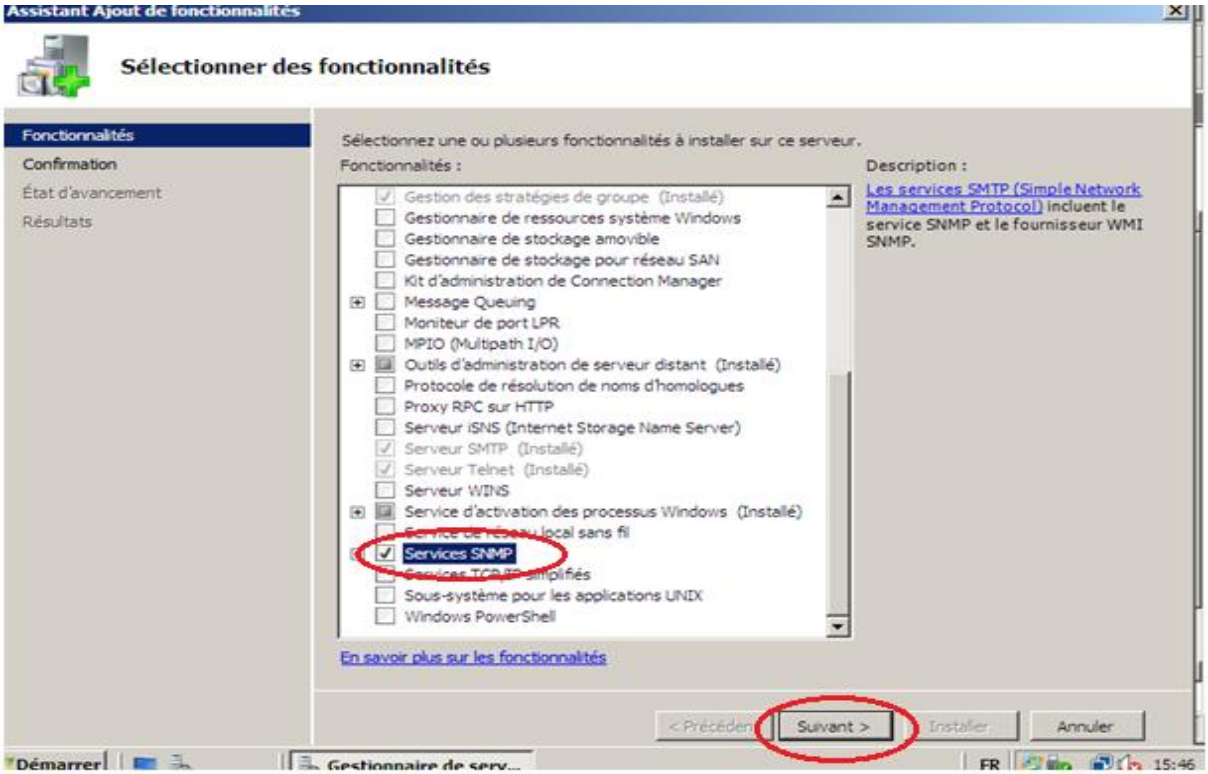


Figure III.32. Installation du Serveur SNMP

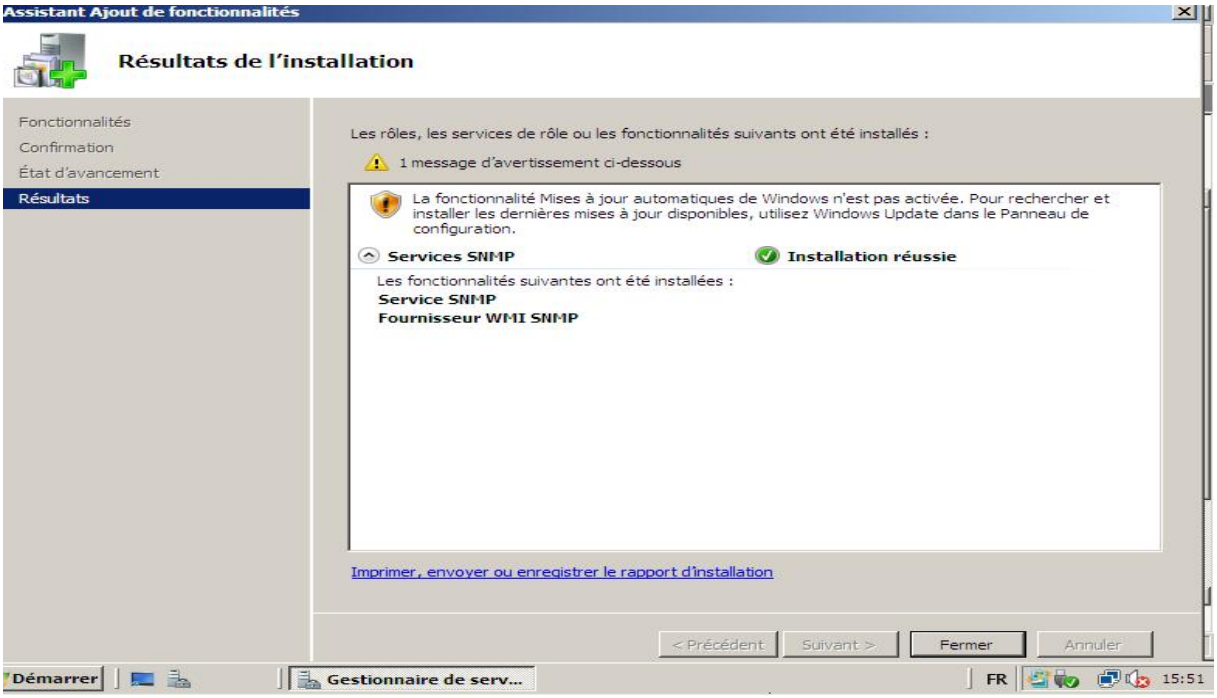


Figure III.33.Résultat d'installation du Service SNMP

Configurer l'ACL pour autoriser le service SNMP:

```
ciscoasa(config)# access-list outside-snmp per
ciscoasa(config)# access-list outside-snmp permit tcp 200.0.0.0 255.255.255.0 $
ciscoasa(config)# access-group outside-snmp in interface outside
```

III.14.Le service DNS: il sert à transposer les noms d'ordinateurs en adresse IP.

Configurer l'ACL pour autoriser le service DNS

```
ciscoasa(config)# access-list outside-dns permit tcp 200.0.0.0 255.255.255.0 1$
ciscoasa(config)# acc
ciscoasa(config)# access-group outside-dns in interface outside
ciscoasa(config)#
```

On doit ajouter l'inspection DNS

Test: dans le poste du réseau externe (serveur Web), démarrer, exécuter, WWW.UMMTO.COM et OK

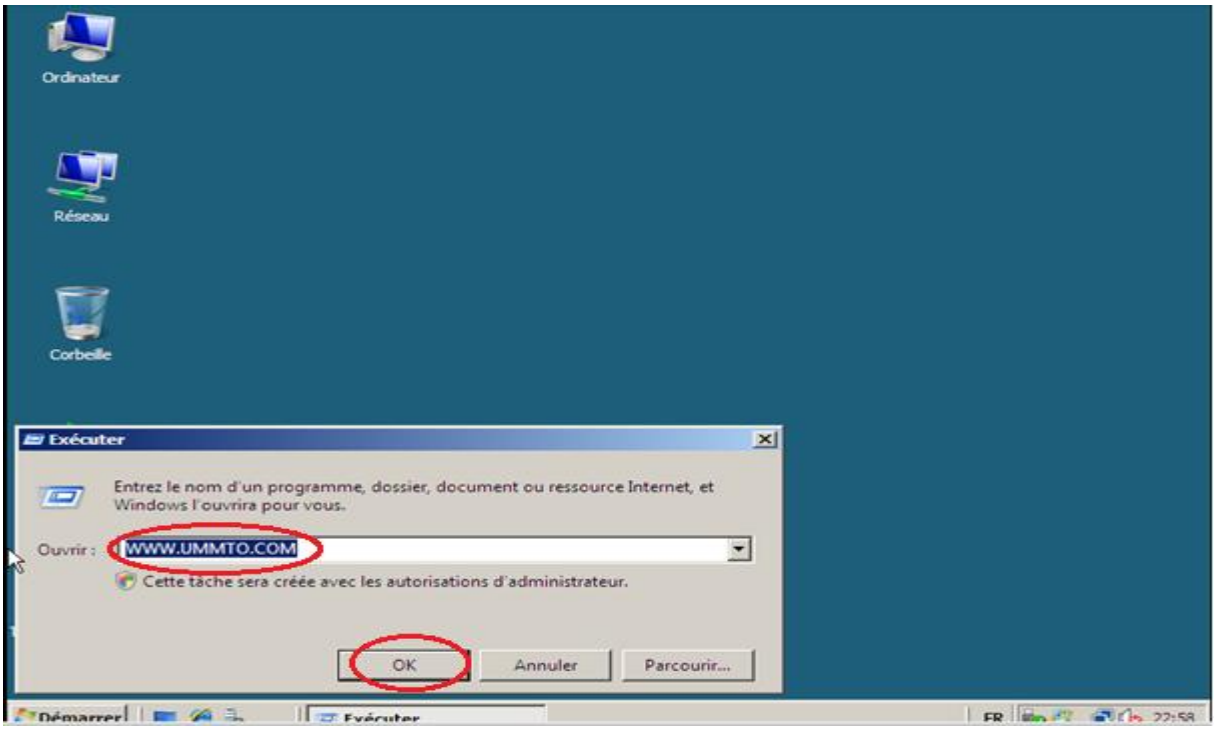


Figure III.34. Test de service DNS

Teste de DNS est réussi : on a accédé à la DMZ

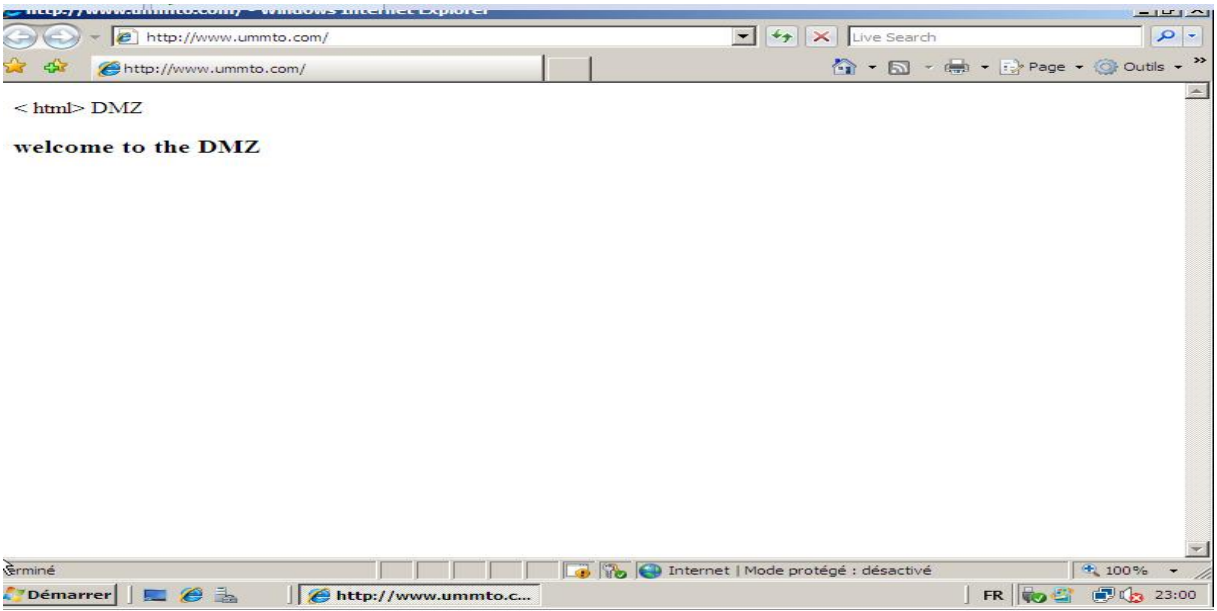


Figure III.35. Résultat du test de service DNS

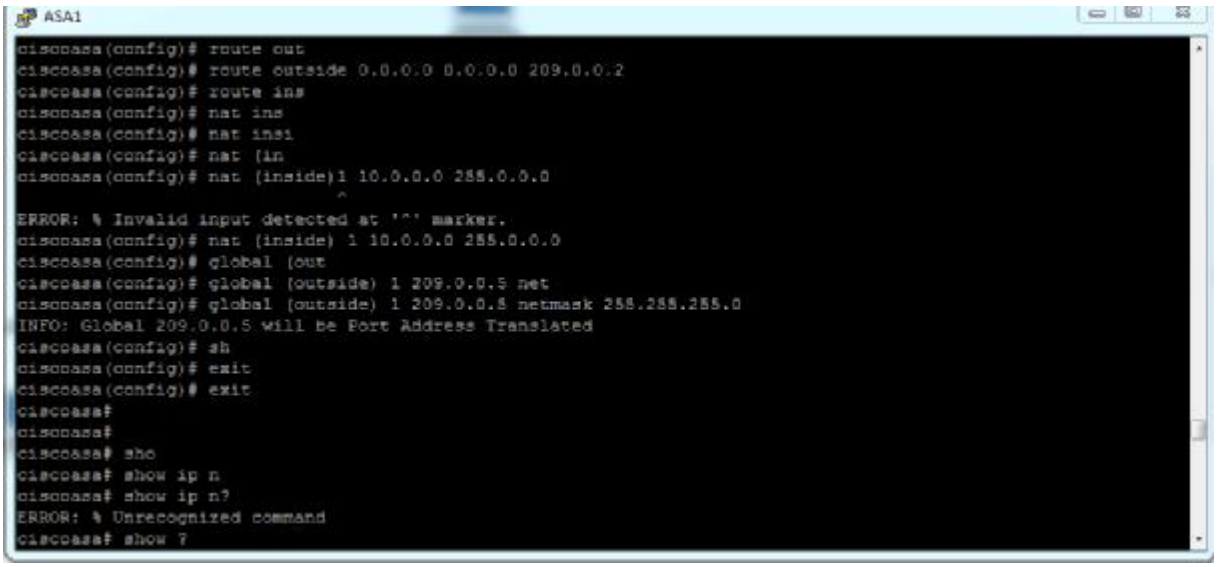
III.15.Le service SMTP (port 25)

Permet le transfert du courrier électronique vers les serveurs de messagerie électronique

```
ciscoasa(config)# access-list outside-smtp permit tcp 200.0.0.0 255.255.255.0 $
ciscoasa(config)# access-group outside-smtp in interface outside
```

III.16.Configuration du PAT

Le réseau LAN dispose d'une plage d'adresse privé alors que la DMZ dispose d'une plage d'adresse publique. Pour que les postes du réseau LAN puissent se connecter à internet il leurs faut une adresse IP routable. Pour résoudre se problème il faut appliquer le PAT(Port Address Translation)



III.17.Discussions

D'après les résultats de la simulation, on constate que la liste de contrôle d'accès, la configuration de protocole RIP et le routage dynamique qu'on a appliqué sur le ASA 5510 d'une façon a autoriser les utilisateurs externes d'avoir un accès vers la DMZ de l'entreprise et de bloquer leur accès vers le réseau local sont bien vérifiés.

Dans notre projet, nous nous sommes intéressé à mettre en place une stratégie de sécurité pour pouvoir sécuriser au maximum le réseau d'une entreprise contre les menaces et attaques éventuelles qui risque de l'atteindre. Cette politique est basée sur la décomposition du réseau en zones de sécurités séparées appelées DMZ et la configuration d'un pare-feu, qui nécessite l'utilisation des ACL (listes contrôle d'accès) et la translation d'adresse NAT.

La première tache qu'on a effectué dans notre projet était l'installation et la configuration de Windows serveur 2008(serveur Active Directory, serveur des fichiers et serveur web).

La deuxième tache consistait à la configuration de l'ASA 5510 en appliquant une stratégie de filtrage bien définie.

La solution qu'on a proposé a permet à l'entreprise d'assurer un niveau de sécurité considérable, à savoir la sécurité du réseau interne, la maitrise et la gestion d'accès à la base de données.

Grace aux testes effectués et les résultats obtenus, nous avons déduit que l'ASA serait une solution adéquate dans la plus part des entreprises surtout ceux dotées de nouvelle technologies.

Nous estimons que la mise en place d'une infrastructure DMZ avec l'ASA que nous avons réalisée va répondre aux exigences et besoins des utilisateurs de fait qu'elle permet d'offrir une meilleure sécurité.

Préambule

OSI signifie (Open Systems Interconnection) a été mis en place par l'ISO International Standard Organisation afin de normaliser les communications entre les ordinateurs d'un réseau. En effet, à l'origine des réseaux chaque constructeurs avait son système propriétaire et de nombreux réseaux incompatibles. Se modèle a permet de standardiser la communication entre les machines de différent constructeurs.

Description du Modèle OSI

Le modèle OSI décrit les échanges de données en 7 sous-ensembles fonctionnels successives appelées couches ou niveaux.

- Ø Pour chaque couche du modèle, la norme OSI précise les services qu'elle rend à la couche inférieure, les fonctions qu'elle réalise, et la manière dont elle utilise les services des couches supérieures.
- Ø Les fonctionnalités de chaque couche peuvent être réalisées par des dispositifs logiciels (niveaux supérieurs) ou matériels (niveaux inférieurs)

I.6.1.Les couches du modèle OSI :

Modèle OSI		
Niveau	**couche**	**Rôle de la couche**
Niveau 7	Couche application	-Interface entre les services réseau et les applications (SMTP, Telnet, FTP, HTTP)
Niveau 6	Couche présentation	-la représentation de l'information échangée entre processus d'application. -Traitement spécial tel que le cryptage
Niveau 5	Couche session	-s'occupe de l'établissement, de la coordination des communications. -définit l'ouverture et la destruction des machines des sessions de communication entre les machines de réseau.
Niveau 4	Couche transport	-Gère la remise correcte des informations (gestion des erreurs), Et assure le contrôle de l'acheminement.

Niveau 3	Couche réseau	-gère l'adressage et le routage des données c'est-à-dire leur acheminement via le réseau.
Niveau 2	Couche liaison de données	-définit l'interface avec la carte réseau. Définit le partage du média de transmission.
Niveau 1	Couche physique	-gère les connexions matérielles. -définit la façon dons les données sont converties en signaux numériques sur les média de communication.

Tableau I.1.le modèle OSI

Description du modèle TCP/IP

TCP/IP est une suite de protocoles. Le signale TCP/IP signifie « transmission control Protocol/ Internet Protocol » .TCP/IP représente l'ensemble des règles de communication sur Internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP pour pouvoir acheminer des paquets de données.TCP/IP est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Ø Le fonctionnement des messages en paquets.
- Ø L'utilisation d'un système d'adresses.
- Ø L'acheminement des données sur le réseau (routage).
- Ø Le contrôle des erreurs de transmission de données.

Niveau	**Modèle TCP/IP**	**Modèle OSI**	**Protocole TCP/IP**
Niveau 4	Couche application	Couche application	Telnet,HTTP,DNS,SMTP, DNS ,FTP,HTTP.
		Couche présentation	
		Couche session	
Niveau 3	Couche transport	Couche transport	TCP et UDP
Niveau 2	Couche Internet	Couche réseau	IP,ARP,RARP,ICMP,IGMP

Niveau 1	Couche accès réseau	Couche liaison de données	FTS, FDDI, PPP, Ethernet, anneau à jeton (Token Ring)
		Couche physique	

Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice.

A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

- le paquet de données est appelé message au niveau de la couche application.
- le message est ensuite encapsulé sous forme de segment dans la couche transport. Le message est donc découpé en morceaux avant envoi.
- Le segment une fois encapsulé dans la couche Internet prend le nom de datagramme.
- Enfin, on parle de trame au niveau de la couche accès réseau.

Préambule

L'objectif de cette partie est d'apprendre les différentes fonctionnalités des équipements matériels ainsi que leurs configurations de base. L'équipement qu'on va décrire est le routeur

Le routeur :

Qu'est ce qu'un routeur ?

Les ordinateurs sont constitués de quatre composants de base : un processeur, de la mémoire, des interfaces et un bus. Un routeur est aussi doté de ces éléments, nous pourrions donc en conclure qu'il s'agit d'un ordinateur réservé à un usage particulier. Le routeur étant entièrement dédié au routage, aucun de ses composants n'est consacré aux unités de sortie vidéo et audio, aux dispositifs d'entrée, tels que le clavier et la souris, ainsi qu'aux logiciels conviviaux typiques d'un ordinateur multimédia moderne.

L'architecture interne du routeur Cisco prend en charge les composants qui jouent un rôle important dans le processus de démarrage. Les composants de configuration internes d'un routeur sont les suivants :

- **Mémoire RAM/DRAM** : mémoire qui stocke les tables de routage et les files d'attente de paquets. La mémoire RAM sert également de mémoire temporaire et/ou d'exécution au fichier de configuration du routeur lorsque ce dernier est sous tension. Le contenu de la mémoire RAM est perdu lors d'une mise hors tension ou d'un redémarrage.
- **Mémoire NVRAM :** mémoire non volatile (NV) qui stocke le fichier de configuration de sauvegarde/démarrage du routeur. Son contenu est conservé lors d'une mise hors tension ou d'un redémarrage.
- **Mémoire flash :** mémoire « morte » électriquement effaçable qui contient l'image du système d'exploitation. Elle permet d'effectuer des mises à niveau logicielles sans retirer ni remplacer les puces du processeur. Son contenu est conservé lors d'une mise hors tension et d'un redémarrage. Elle peut stocker plusieurs versions de la plate-forme logicielle Cisco IOS.
- **Mémoire ROM** : mémoire « morte » en lecture seule. Elle contient les diagnostics de mise sous tension, un programme d'amorçage et logiciel d'exploitation.
- **Interfaces** : connexions réseau situées sur la carte-mère ou sur des modules d'interface distincts, par lesquelles les paquets entrent et sortent du routeur. Elles sont identifiées par une adresse réseau.

A l'image des ordinateurs qui ont besoin de système d'exploitation pour exécuter les applications, les routeurs doivent être équipés d'une plate-forme logicielle : l'IOS (Internetworking Operating Software) pour gérer le routage et exécuter les fichiers de configuration. Ces fichiers contrôlent les flux de données entrants dans le routeur. Plus précisément, en utilisant des protocoles de routage qui permettent de choisir le meilleur chemin pour les paquets.

Les commandes CISCO

« enable » ou « ena » ou « en » pour passer en mode administrateur sur l'équipement réseau.
Toutes les commandes indiquées ci-dessous sont à effectuer en mode administrateur.
Pour obtenir de l'aide sur une commande faite nom de la commande suivie d'un point d'interrogation :
ex : show ?

Le tableau suivant représente les différentes commandes utilisé pour la configuration d'un Switch et d'u routeur Cisco.

Commandes	*Descriptions*
configure terminal ou conf t ou confterm	Entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
exit	Sort et remonte d'un cran dans la hiérarchie des menus
`hostname ou host <hostname>`	Permet de modifier le nom de l'équipement réseau
enable secret <password>	Assigne un mot de passe encrypté à enable
interface ethernet | fastethernet | Serial | loopback <interface>ouint e | fa | s | lo	Entre dans le mode de configuration del'interface
ip address <address><mask>ouip add	Configure l'interface avec l'ip et le masque de réseau
bandwidth ou band	Indique une bande passante
encapsulation <encap> [<type]> ou encap	Fournit l'encapsulation de l'interface
no shutdown ou no shut	Active ou Désactive l'interface
Les commandes de sauvegarde :	

copy running-config startup-configou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM
copy running-configtftpou copy run tftp	Sauvegarde la configuration courante vers un serveur TFTP
copy startup-configtftpou	Sauvegarde la configuration situé en
copy star tftp	NVRAM vers un serveur TFTP
copy tftp startup-configou copy tftp star	Charge un fichier de configuration d'un serveur TFTP en NVRAM
copy tftp running-configou copy tftp run	Charge un fichier de configuration d'un serveur TFTP dans la configuration courante
Commandes	***Descriptions***
erase startup-config ou erase star	Efface la configuration de la NVRAM
Configuration d'une connexion en telnet:	
router# conf t	
router(config)# line console 0	
router(config)# login	
router(config)# passwordxyz	
Les commandes de configurations du routage :	
router <xxx> [<process-id>,<autonomous system>] rip,ospf,bgp,igrp,eigrp,is-is,...	Configure le protocole de routage d'un routeur
exemple de configuration du routage RIP:	
router# conf t	
router(config)# router rip	
router(config-router)# version 1-2	la version 2 apporte le routage CIDR et l'utilisation de VLSM, un nombre de sauts à 128
router(config-router)#network *networknumber*	
exemple de configuration du routage OSPF:	
router# conf t	

router(config)# router ospf 10	
router(config-router)# network network number	
exemple de configuration du routage IGRP:	
router# conf t	
router(config)# router igrpautonomous system	
router(config-router)# network *networknumber*	
exemple de configuration du routage EIGRP:	
router# conf t	
router(config)# router eigrpautonomous system	
router(config-router)# network *networknumber*	
exemple de configuration du routage BGP:	
router# conf t	
router(config)# router bgp*autonomous system*	
router(config-router)# network *networknumber* [mask *network-mask*] [route-map *route-map-name*]	
D'autres commandes de routage	
ip multicast-routing	Permet de faire du routage multicast
ip rsvp bandwidth [*interface-kbps*] [*singleflow-kbps*]	Active la réservation RSVP sur une interface
Les commandes sur un Switch :	
vlan database vlan 1 name <vlan name>	Accès à la database et écriture dans le fichier

	vlan.dat
Exemple de configuration d'un vlan :	
switch# vlan database switch(vlan)# vlan<number><name> switch(vlan)# exit switch(config)#interface fa<iface-number> switch(config)#interface range fa... switch(config-if)#switchport mode access	affectation sur un port affectation sur un ensemble de ports on passe le mode de configuration de l'interface
Commandes	***Descriptions***
switch(config-if)# switchport access vlan <number-name>	on active le vlan sur le ou les interfaces
Activation du trunking sur l'interface	Le truncking sert dans l'extention d'un domaine VLAN sur d'autre switch, pour se faire CISCO utilise le protocole VTP VLAN Trunking Protocol
switchporttrunkencap dot1q	Il y a 2 protocoles utilisés dans l'étiquetage: le protocole ISL (CISCO) et le protocole 802.1q (IEEE)
switchport mode trunk	On active le mode trunk sur le port du commutateur serveur et client qui font le trunk le reste des ports sont en mode access
vlan database vtpdomain<domain-name> vtp server	Création d'un serveur VTP
vlan database vtpdomain<domain-name> vtp client	Création d'un client VTP
ip default-gateway <ip-gateway>	On peut définir une passerelle par défaut pour communiquer entre VLAN, pour se faire on utilise un routeur
encapsulation ISL | dot1q <vlan-number>	en mode interface on peut spécifier le type d'encapsulation sur le routeur
D'autres commandes communes :	
reload	Redémarre l'équipement réseau
setup	Passe en mode de configuration assisté
ping [<address>]	ping seul, permet de faire un ping étendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface

	directement connecté.
Les commandes show :	
show interfaces oushint	Donne une description détaillé sur les interfaces
show running-configoush run	affiche la configuration courante
Commandes	***Descriptions***
show startup-configoush star	affiche la configuration en NVRAM
show ip route ouship route	affiche la table de routage
show ip<routing-protocol> [<options>]	affiche les informations sur le protocole de routage défini
show ipprotocols	affiche des informations sur les protocoles utilisés
show ?	donne toutes les commandes show disponibles

les commandes basiques pour la configuration d'un firewall

A

Administrateur Réseau : Personne responsable de l'organisation, de la configuration et la gestion du réseau.

Administration à distance : Administration d'un ordinateur par un administrateur, situé sur un autre système relié au premier par le réseau

ADSL: Asymmetric **D**igital **S**ubscriber **L**ine

Adresse IP : c'est une adresse logique définit sur 32 bits, utilisée par le protocole TCP/IP, pour identifier de façon unique chaque ordinateur sur le réseau.

Adresse MAC : Media **A**ccess **C**ontrol : Adresse physique, définit sur 48 bits. Unique, elle permet d'identifier le matériel réseau. Les 24 premiers bits identifient le fabriquant et les 24 restantes, fournissent un identifiant au matériel (appelé familièrement numéro de série).

ARP : Adress **R**esolution **P**rotocol, protocole de résolution d'adresses utilisé pour la correspondance entre les adresse IP et les adresses Ethernet.

AP (**A**ccess **P**oint) : point d'accès

ARP : Adresse Resolution Protocol.

ACL : Access Control List

B

BIT : BInary digi**T** : chiffre dans un système de numérotation à la base 2. On le notre par zéro (0) ou un (1). Un bit est représenté physiquement par un élément capable de prendre deux valeurs.

Broadcast : le broadcast consiste à envoyer une information à tout les ordinateur du réseau.

C

CISCO : est une entreprise informatique américaine qui vendait, à l'origine, uniquement du matériel réseau (routeur et Switch Ethernet).

Control d'accès : Méthode de vérification de l'identité d'un utilisateur pour s'assurer de son bon droit à utiliser un service. Généralement, le control d'accès se fonde sur la connaissance d'un nom d'utilisateur et d'un mot de passe.

Client : Programme ou ordinateur utilisant une ressource partagée fournie par un autre ordinateur appelé serveur.

Collision : événement qui se produit dans un réseau local lorsque deux stations d'un réseau Ethernet émettent simultanément sur le support unique.

CSMA/CA (Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance**) :** méthode d'accès utilisée dans les réseaux sans fil.

Commande : Ordre que l'ordinateur doit exécuter. L'ordinateur est dit en mode direct si la commande est exécutée immédiatement après qu'elle ait été tapée et envoyée à l'unité centrale.

CSMA/CD (Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etected**)** : méthode d'accès utilisée dans les réseaux Ethernet.

D

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) : Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP.

DA : Adresse Destination

DL : Data Length

DNS (Domain **N**ame **S**ystem) : Il s'agit d'une base de données distribuée, utilisée sur l'Internet pour la correspondance entre les noms des machines et leurs adresses IP.

DSSS (**D**irect **S**equency **S**pread **S**pecteum) : technique d'étalement de spectre à séquence directe dans la transmission radio.

DVD (Digital **V**ersatile **D**isc**).**

E

Ethernet : type de réseau local parmi les plus utilisé initialement développé par Xerox. Il utilise la technique CSMA/CD et correspond à la norme IEEE 802.3.

ETCD : Equipement **T**erminal de **C**ircuit de **D**onnées, tout dispositif servant de port d'entrées vers un système de transmission.

ETTD : Equipement **T**erminal de **T**raitement de données .Tout dispositif, dans un réseau, générant, stockant ou traitant l'information.

EPROM: Electrically Programmable Read **O**nly Memory.

Mémoire morte programmable électriquement. Type de ROM qui peut être efface à l'aide de rayons Ultra-violets afin de pouvoir être programmé. Cette opération de programmation nécessite toute fois un dispositif spécial

F

FDDI : Fibre Distributed Data Interface.

FAT: File Allocation Table - Système de fichiers de DOS et Windows

FTP : File Transfert Protocol.

FCS : Frame Ckeck Séquence

Fichier : Unité d'information se composant d'un ou plusieurs articles.

H

HDLC : Dynamic Host Configuratio Protocol.

HDCP : Dynamic Hoste Configuration Protocol.

HTTP : Hypertext Transfert Protocol

I

IEEE (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers): Une organisation de standardisation qui développe des spécifications pour les réseaux Ethernet, Token Ring et Token Bus.

Interface : une voie d'échange d'information qui permet à un ordinateur ou plusieurs ordinateurs ou des équipements extérieurs (imprimantes, moniteurs, modems) de communiquer.

IPV6 : version future du protocole IP. Commence à être implémentée par les grands constructeurs de systèmes informatiques. L'apport majeur de cette nouvelle version est un espace d'adressage beaucoup plus important que dans la version actuelle : 128 bits au lieu de 32.

ISO : International **S**tandard **O**rganisation

ICMP : Internet Control and Error Message Protocol.

IGMP : Internet Group Management Protocol.

IP : Internet Protocol.

L

LAN (**L**ocal **A**rea **N**etwork) : réseau local d'entreprise. Est un ensemble d'ordinateur appartenant à une même organisation et relié entre eux par un réseau.

Login : nom de connexion, code d'accès unique qui identifie un utilisateur lorsqu'il accède à un ordinateur. C'est aussi l'opération qui permet l'accès à un ordinateur

M

MAC (Media **A**ccess **A**ontrol**) :** la sous couche de la couche liaison du modele IEEE 802.11.

Masque de sous réseau : Un **masque de sous-réseau** permet d'identifier un sous-réseau

MAN (Mitropolitan **A**rea **N**etwork) : C'est l'interconnexion de plusieurs LAN géographiquement proches.

MS-DOS (Microsoft-**D**isk **O**perating **S**ystem**) :** ancien système de Microsoft

Modem : est un appareil qui permet à l'ordinateur d'utiliser la ligne téléphonique pour communiquer avec un autre ordinateur

N

NT : New Technologie. Système d'exploitation de Microsoft qui a pour caractéristiques principales de garder Windows comme base, mais en supprimant le DOS comme couche inférieure.

NTFS: New Technology File System.

Système de fichiers avancé qui offre des performances, une sécurité, une fiabilité et des fonctionnalités et qui fonctionne le mieux avec un disque volumineux. Seul le système de fichiers NTFS permet d'utiliser des fonctionnalités comme AD et la sécurité basée sur les domaines

NTFS : New Technology File System.

NOS : Network Operating System

O

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing): algorithme de cordage
OS (**O**perating **S**ystème) : système d'exploitation.
OSI (Open **S**ystem **I**nterconnexion) : Un standard ISO concernant le réseau (partie logicielle).

P

PC : Signifie « Personnel Computer », en français ordinateur individuel.

Dénomination officielle adoptée par IBM pour désigner son premier micro-ordinateur.

Paquet: Désigne, lors de la communication entre deux dispositifs informatiques, un ensemble de données groupées selon un format donné

PING (Packet INternet Groper) : Commande de base de tout système d'exploitation permettant de tester les connexions entre deux hôtes du réseau utilisant TCP/IP.

R

RAM (Random **A**ccess **M**emory**):** mémoire à lecture-écriture.

RJ45 : Type de connecteur similaire à une prise téléphonique, mais de plus grande taille. Utilisé pour un câblage à paire torsadée

RIP : Routring Information Protocol

ROM: Read Only Memory. Mémoire morte dont le contenu est défini à l'usine.

S

Segment: Câble ou ensemble de câbles reliés sans équipements d'interconnexion.

Série : Désigne un type d'entrées/ sorties où la transmission de données se fait bit par bit.

Spam: Le Spam est un mot d'origine anglaise, désigne les communications électroniques massives.

Le Spam est un email indésirable envoyé à des milliers de personnes qui peut être des emails publicitaires qu'on peut recevoir dans notre boite aux emails. Les Spam encombrent aussi les boites aux lettres.

Synchrone : Dans la transmission synchrone, les bits sont envoyés de façon successive sans séparation entre chaque caractère.

SSL: Secure Sockets Layer - (1994) Protocole de communication sécurisée créé par Netscape. Protocole utilisé pour communiqué avec un serveur.

T

TCP : Transmission Control Protocol.

TCP/IP (Transmission **C**ontrol **P**rotocol/**I**nternent **P**rotocol**)**

Trame : l'unité de transmission de la couche liaison. Une trame peut comporter un en-tête et / ou une queue, et bien sur des octets de donnés.

U

UTP: (Unshielded Twisted Pair) Paire torsadée non blindée

UDP : User Datagramme Protocol

V

VPN : Virtual Private Network - "Réseau privé virtuel". Il s'agit d'un lien virtuel, créant l'illusion d'une liaison directe privée entre des machines reliées en fait par un autre réseau

W

WAN (Wide **A**rea **N**etwork) : ou réseau étendu interconnecte plusieurs LAN à travers de grandes distances géographiques

X

X25 : un protocole de communication normalisé par commutation de paquets

Xwindows system : ou **X11** ou plus simplement **X**, est un protocole définissant les notations de clients, gestionnaire d'interfaces et de surface d'affichage virtuelle. Le serveur affiche les différentes fenêtres sur un écran physique. Le gestionnaire d'interfaces (Window-manager) autorise l'utilisateur à déplacer des fenêtres. Il gère l'essentiel de la présentation de l'écran et des interactions avec l'utilisateur.

-F.YADDADENE : « Mise en œuvre d'une politique de sécurité au réseau informatique de l'entreprise ENIEM de Tizi-ouzou », université Mouloud Mammeri Tizi-ouzou, département d'électronique, thèse Master, l'année 2011-2012.

-A.HADDAD : « Implémentation d'une politique de sécurité au réseau informatique de l'entreprise ENIEM de Tizi-ouzou », université Mouloud Mammeri Tizi-ouzou, département d'électronique, thèse Master, l'année 2010-2011.

-Y.DOUICHER : « Mise en place d'un pare-feu en utilisant la Smoothwall », université Mouloud Mammeri Tizi-ouzou, département d'électronique, thèse Master, l'année 2011-2012

-N.AIT DAHMANE : « Mise en place d'un tunnel VPN implémenté sur ASA Cisco », université Mouloud Mammeri Tizi-ouzou, département d'électronique, thèse Master, l'année 2011-2012

-J.F. PILLOU **:** « Tout sur la sécurité informatique », 2^{éme} édition, Pris : dunod, 2009 : collation 232 p.

-V.ANDRE : « Cisco. Protocoles, concepts de routage et sécurité : 19 ateliers et travaux pratiques 159 questions-réponses », Paris : Ellipses 2011 : collation 327.p. ill ; 24 cm : (Kite de formation).

-O.THOMAS : « Microsoft MCITP 70-646 administrateur Windows server 2008 »: Paris: dunod,2008: collation[VI-744] p.ill; 24 cm: (Kite de formation).

-J.C.MACKIN: « Microsoft MCITP 70-647 administrateur d'entreprise sur Windows server 2008»,Paris : dunod, 2008: collation [VI-619]p.ill; 24cm: (Kite de formation).

-D.HOLME : « configuration d'une infrastructure active directory avec Windows server 2008» : Paris : Dunod, 2008 : collation [VI-948]p.ill :24cm : (Kite de formation).

-J.c.MACKIN : « Microsoft MCTS 70-643 configuration d'une infrastructure d'applications avec Windows server 2008» : Paris : Dunod, 2008 : [XVII-664]p.ill ;24cm : (Kite de formation).

Site internet

-www.cisco.com/AdaptativeSecurityAppliance.

-www.commentçamarche.com.

-www.mémoireonlingne.com

-www.networksorcry.com