République Algérienne Démocratique et Populaire Ministère de
L'Enseignement Supérieur et de la Recherche Scientifique
UNIVERSITE MOULOUD MAMMERI DE TIZIOUZOU

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE

Département D'ELECTRONIQUE

Mémoire de Fin d'études

En vue de l'obtention du diplôme de master en Electronique

Spécialité : Réseaux et Télécommunication

Filière: Génie Electrique

Thème

Mise en œuvre de la sécurité d'un réseau d'entreprise en utilisant les ACLs

Présenté par :

AMRAR SALIM

Encadré par :

F.OUALOUCHE

Année Universitaire: 2015/2016

Remerciements

Je remercie le bon **Dieu** qui ma aidée à surmonter toutes les difficultés rencontrées au long de cette période pour mener à terme ce travail.

Je tien a remercier et à exprimer ma profonde gratitude à mon promoteur Mr.**Oualouche** qui ma suivi durant ce travail.

Je tien à remercier les membres de **jury** d'avoir accepté de juger mon travail.

C'est l'occasion de remercier tous le corps **enseignants** depuis les études primaires.

Enfin**, Je** tien à remercier également ma **famille** et mes **amis** pour leurs aides considérables.

Dédicaces

« Louange à **DIEU**, le seul et unique »

Je dédie ce mémoire :

À mes très chers **parents** qui m'ont prodigué avec amour et patience leur précieux réconfort dans le long périple de mon cursus de formation.

À mes chers frères, **Younes** (nounou), **Samy**

À toute ma **famille** et à tous mes **amis** qui mon aidé de prés ou de loin, en particulier : mon oncle **Fateh**, **Massinissa**, **Slimane**, **Louiza**.

À l'ensemble de mes enseignants qui m'ont nourri de leurs savoirs et de leurs expériences.

GLOSSAIRE

AIM : Adaptive Identification and Mitigation

ARP : Address Resolution Protocol

ACL : Access Control List

ACE : Access Control Entre

BGP : Border Gateway Protocol

BPDU : Pont Protocol Data Unit

DNS : Domaine Name Service

TCP : Transmission contrôle Protocole

ICMP : Internet Control Message Protocol

DHCP : Dynamique Host Configuration Protocol

FTP : File Transfert Protocol

HTTP : Hyper Texte Transfer Protocol

S-http : Secure hyper text transfert protocol

SMTP : Simple Mail transfert protocol

SSH : Secure Shell

SSL : Secure Sockets Layer

TFTP : Trivial File Transfert Protocol

MAC : Media Access Network

DNS : Domain Name System

TCP : Trensfer Control Protocol

IDS : Intrusion Detection System

IPsec : Internet Protocol Security

NPS : Network Policy Server

NAP : Network Access Protection

NAT : Network Address Translaton

PKI : Port Address Translation

GLOSSAIRE

OSI : Open System Interconnection

RADIUS : Remote Authetification Dial In User Service

Liste des figures

SOMMAIRE

CHAPITRE 3 : LISTES DE CONTROLE D'ACCES(ACL)

CHAPITRE 4 : Application et résultats de la simulation

Introduction générale

Aujourd'hui, les systèmes informatiques occupent une place prédominante dans les entreprises, dans les administrations et dans le quotidien des particuliers. Ce phénomène à été analysé, entre autre, par l'essor de l'internet qui séduit chaque jour de plus en plus d'internautes par les nombreux avantages et la diversité des services rendus accessibles. Il peuvent aussi bénéficier à moindre couts, de moyens de communication rapides, partager des ressources de traitement et de stockage de grandes capacités, faciliter les échanges commerciaux et financière, fournir et utiliser de nombreux services en ligne, participer à des communautés virtuelle et à des réseaux sociaux et plus généralement , partager et accéder à l'information.

Notre dépendance croissante aux systèmes informatiques dans divers aspects de la vie quotidienne et leur omniprésence soulèvent inévitablement des questions quant à leurs sécurités et à la sécurité des informations qui leurs sont confiées. La croissance accélérée de ces systèmes informatiques posent néanmoins un problème majeur : ils en découlent un nombre croissant d'attaque qui peuvent aboutir à de graves conséquences professionnelles et financières en menaçant l'intégrité, la confidentialité et la disponibilité de l'information. Les menaces informatiques peuvent se catégoriser de la manière suivante :

- Accès physique ;
- Interception de communication ;
- Détournement ou altération de message ;
- Intrusion.

Afin de pouvoir immuniser un système contre ces menaces, il est nécessaire de :

- Se tenir informé des mises à jours des OS (système d'exploitation) et les correctifs des failles ;
- Mettre en place des dispositifs permettant de sécuriser l'infrastructure réseau ;
- De corriger les erreurs de conception et d'implémentation par les constructeurs (comme CISCO, Microsoft…etc.) dés que la vulnérabilité est découverte.

L'objectif visé dans notre travail de mémoire est d'implémenter une politique de sécurité basée sur le principe de filtrage, de l'organisation et de l'administration du réseau informatique de l'entreprise. Et comme le matériel réseau utilisé au sein de cette entreprise est pratiquement le matériel CISCO, donc la mise en œuvre de la politique de sécurité est inspirée de différentes techniques, méthodes et stratégies qui caractérisent ce matériel.

Introduction générale

Notre mémoire est structuré en quatre chapitres, le premier chapitre intitulé<<généralités sur la sécurité des réseaux informatique>>, à pour but de donner des informations sur la sécurité et les réseaux informatiques. Le deuxième chapitre, comporte la présentation du réseau d'entreprise et les méthodes de sécurité appliquées. Le troisième chapitre, comporte une étude bien détaillé sur les listes de contrôle d'accès(ACL). Après avoir étudié les failles et anomalies du réseau existant le quatrième chapitre, propose une politique de sécurité qui portera une bonne administration du réseau et qui propose une configuration basé sur un système de filtrage des différentes entités. Et enfin nous terminerons ce modeste travail par une conclusion générale.

Généralités sur la sécurité des réseaux informatique

1. Préambule:

Dans le monde moderne, Internet est devenue un outil primordial qu'ont utilise pour exercer diverses activités comme le travail, l'étude, l'achat en ligne, la communication …etc. Cette révolution technologique à été accompagné par une augmentation phénoménale du nombre d'utilisation d'internet. Vu les différents infrastructures des divers secteurs sociaux, économiques, militaires, gouvernementales, sont connectées à internet. Une attaque informatique est devenue une arme très dangereuse et très destructive, grâce à elle on peut paralyser tout un pays, un projet stratégique. Les attaques informatiques ne cessent d'être dirigées contre les entreprises. En effet, la menace qui plane sur un système est un fait, plus l'entreprise possède des informations importantes, plus elle y sera soumise. Cependant, il existe des moyens qui permettent de garder élevé le seuil de sécurité des systèmes mettant en place des contre-mesures pour réduire les risques des attaques et la compromission des données.

Dans ce chapitre, nous allons voir les différents aspects liés à la sécurité informatique, les types d'attaques et leurs mécanismes de détection et la protection des réseaux informatiques.

2. Définition d'un réseau informatique:

Un réseau informatique est un ensemble d'équipement informatique reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques et partager les ressources matériels et logiciels.

2.1. Architecture des réseaux :

Les réseaux sont structurés du point de vue fonctionnel en deux catégories :

- ✓ réseaux poste a poste (Peer to Peer)
- ✓ réseaux à serveur dédié (client /serveur)

2.2. Différents types de réseaux :

On distingue différents types de réseaux : selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue.

- **Classification selon la taille :**

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

- **Selon leurs topologies :**

La façon dans laquelle les ordinateurs sont interconnectés physiquement est appelée **topologie physique**.

Les topologies physiques basiques sont :

✓ la topologie **en bus** :

Cette topologie est représentée par un câblage unique des unités réseaux. Il a également un faible coût de déploiement et la défaillance d'un nœud (ordinateur) ne scinde pas le réseau en deux sous-réseaux. Ces unités sont reliées de façon passive par dérivation électrique ou optique.

✓ la topologie **en étoile** :

Aussi appelé Hub and spoke c'est la topologie la plus courante actuellement. Omniprésente, elle est aussi très souple en matière de gestion et dépannage de réseau : la panne d'un nœud ne perturbe pas le fonctionnement global du réseau.

✓ la topologie **en anneau :**

Un réseau a une topologie en anneau quand toutes ses stations sont connectées en chaine les unes aux autres par une liaison bipoint de la dernière à la première. Chaque station joue le rôle de station intermédiaire.

- **Selon leurs modes de connexion :**

- mode avec connexion
- mode sans connexion

- **Selon leurs méthodes d'accès :**

- méthode d'accès par Token ring
- méthode d'accès CSMA/CD (à compétition)
- méthode d'accès par Standard FDDI

2.3. 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 Protocole) : est un protocole fiable, orienté connexion qui permet l'acheminement sans erreur de paquet issues d'une station a une autre.

- **Protocole ICMP** (internet control message Protocol) : est un protocole qui permet le contrôle des erreurs de transmission.

- **Protocole DHCP** (dynamique host configuration Protocol) : est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station.

- **ftp** (file transfert Protocol) : permet de transférer des fichiers d'une machine à une autre.

- **http** (hyper texte Transfer Protocol) : est le protocole de communication du web permettant d'échanger des documents hyper textes contenant des données (texte, images, vidéos, sons).

- **TFTP** (trivial file transfert Protocol ou protocole simplifié de transfert de fichier) :est un protocole simplifié de transfert de fichiers, au contraire du ftp qui utilise lui tcp.

3. La sécurité informatique :

3.1. Définition :

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce a quoi s'attendent les utilisateurs de systèmes informatique en regard de la sécurité.

3.2. Les critères de la sécurité :

- **Disponibilité :** demande que l'information soit disponible aux personnes autorisées seulement.
- **Confidentialité :** demande que l'information sur le système ne peut être lue que par les personnes autorisées.
- **Intégrité :** demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.
- **Non-répudiation :** permet de garantir qu'une transaction ne peut être niée.
- **authentification :** garantit l'identité des correspondants ou des partenaires qui communiquent. [1]

3.3. Politique de sécurité :

3.3.1. Définition :

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

- D'identifier les besoins en temps de sécurité, les risques informatiques et leurs éventuelles conséquences.
- D'élaborer des règles et des instructions (méthodes) à mettre en œuvre dans les différents services de l'organisation pour les risques identifiées.
- De surveiller et détecter les vulnérabilités du système d'information et se tenir informer des failles sur les logiciels et matériels utilisés.
- De définir des engagements à entreprendre et les personnes à contacter on cas d'illégale ou détection d'une menace.

3.3.2. Les types de politique de sécurité :

- La politique qui interdit tout par défaut :dans cette approche, tout ce qui n'est pas explicitement permis est interdit .elle consiste à définir les services a autoriser et les droits de chaque utilisateur.
- La politique qui autorise tout par défaut :dans cette approche, tout est permit sauf ce qui est considérer dangereux donc tous ce qui n'est pas explicitement interdit est autorisé. Elle consiste à analyser les différents risques d'application qui doivent s'exécute.

3.4. Risques de sécurité :

Les risques se mesurent en fonction de deux critères principaux : la ***vulnérabilité*** et la ***sensibilité***.

*La vulnérabilité désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau est un point facile à approcher. Un élément de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible.

*La sensibilité désigne le caractère stratégique d'un composant du réseau. Celui-ci peut être très sensible, vu son caractère stratégique mais quasi invulnérable, grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre la plupart des risques. [2]

On peut classer les risques en deux catégories :

✓ Structurels ils sont liés à l'organisation et la démarche d'une entreprise.

✓ Accidentels ils sont indépendants de l'entreprise.

Enfin, selon les niveaux de sensibilité et de vulnérabilité, on distingue souvent quatre niveaux de risques, selon qu'ils sont ***acceptables***, ***courants***, ***majeurs*** ou ***inacceptables.***

• Acceptables : Ils n'induisent aucune conséquence grave pour les entités utilisatrices du réseau. Ils sont facilement rattrapables.

• Courants : Ce sont ceux qui ne portent pas un préjudice grave.

• Majeurs : Ils sont liés à des facteurs rares. Ils causent des préjudices ou des dégâts importants, mais ils peuvent encore être corrigés.

• Inacceptables : Ils sont, en général, fatals pour l'entreprise. Ils peuvent entraîner son dépôt de bilan. [2]

3.5. Type de menaces :

On peut également classer les menaces en deux catégories selon qu'elles ne changent rien (menaces passive) ou qu'elles perturbent effectivement le réseau (menaces active).

- Les menaces passives : consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même. Il en résulte des difficultés à détecter ce type de malveillance, car elles ne modifient pas l'état du réseau.
- Les menaces actives : nuisent à l'intégrité des données. Elles se traduisent par différents types d'attaques. On distingue le brouillage, le déguisement, l'interposition.

Autres menaces :

- Les menaces dues aux *accidents* (statistiquement 26 % des causes) [2] sont le fait d'incendies, d'inondations, de pannes d'équipements ou du réseau, de catastrophes naturelles… L'utilisation ou l'exploitation maladroite, la mauvaise conception ou la réalisation hasardeuse, le défaut de qualité.
- Les menaces dues aux *erreurs* (évaluées à 17 %) [2].
- Les menaces dues à la *malveillance* (57 % dont 80 % sont d'origine interne) [2] concernent les actes tels que le vol des équipements, les copies illicites de logiciels et de documents techniques, le sabotage matériel et l'attaque logique (virus, modification…), les intrusions et l'écoute, les actes de vengeance.

3.5.1. Les attaques informatiques :

3.5.1.1. Les types d'attaque :

Les personnes malveillantes utilisent plusieurs façons d'attaque qui peuvent être regroupées en trois familles différentes :

A. Les attaques directes : c'est l'attaque la plus simple. (Voir figure1)

Figure 1: Attaque directe

B. Les attaques indirectes par rebond:

Les attaques par rebond, consistent à attaquer une machine par l'intermédiaire d'une autre machine. (Voir figure2)

En effet, le rebond à deux avantages:

- ✓ Masquer l'identité(@IP) du hacker
- ✓ Utiliser éventuellement les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour attaquer.

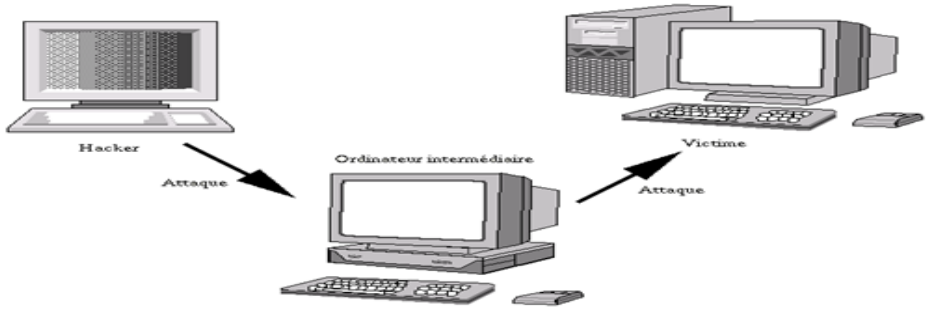


Figure 2: Attaque indirecte par rebond

C. Les attaques indirectes par réponse :

Cette attaque est une dérivée du précédente (par rebond).Elle offre les mêmes avantages, du point de vue du hacker. (Voir figure3)

Figure 3: Attaque indirecte par réponse

3.5.1.2. Les techniques d'attaques :

A. les attaque réseaux : elles profitent des vulnérabilités et des sensibilités du réseau, voici quelque exemple d'attaques réseaux :

1. Attaque par usurpation d'adresse IP (IP spooffing)

L'usurpation d'adresse IP est une technique consistant 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. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis. (Voir figure4) [4]

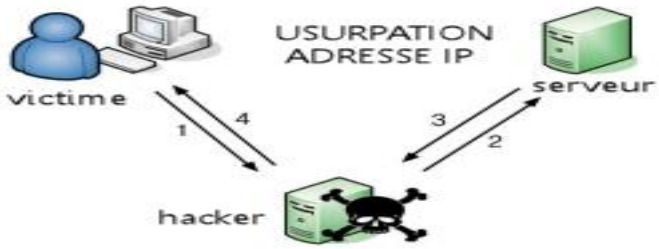


Figure 4: usurpation d'adresse IP

2. Attaque par usurpation d'adresse MAC

Les attaques Usurpation d'adresse MAC sont des attaques contre l'authentification. L'attaque d'usurpation d'adresse MAC *(MAC spoofing)* consiste donc à se faire passer pour quelqu'un qu'on n'est pas en réalité. Il suffit à l'intrus d'utiliser l'identité d'une autre station (Son adresse MAC) soit pour monter une attaque sans se faire repéré. [4]

3. Dns Spoofing :

Fournir de fausses réponses aux requêtes DNS, il existe deux techniques pour effectuer cette attaque :

- **Empoisonnement du cache DNS**

  Est une technique permettant de leurrer les serveurs DNS afin de leurs faires croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse. Une fois que le serveur DNS a été empoisonné, l'information est mise dans un cache, rendant ainsi vulnérables tous les utilisateurs de ce serveur.

- **Dns ID spoofing**

  Est un piratage informatique attaque, de sorte que les données sont introduites dans un Domain Name System (DNS) résolveur de cache, ce qui provoque le serveur de noms pour retourner une incorrecte adresse IP, détourner le trafic vers l'ordinateur de l'attaquant (ou tout autre ordinateur).

4. ARP spoofing

Cette attaque à rediriger le trafic d'une machine vers une autre. Grace à cette redirection, une personne mal intentionnée peut se faire passer pour une autre. De plus, le pirate peut rerouter (transférer) les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien.

5. Tcp session hijacking

Le détournement de session**,** parfois aussi connu sous le nom biscuit détournement est l'exploitation d'une validité de session de l'ordinateur Parfois a également appelé une clé de session à obtenir un accès non autorisé à des informations ou des services dans un système informatique. En particulier, il est utilisé pour désigner le vol d'un cookie magique utilisé pour authentifier un utilisateur vers un serveur distant. Il a un intérêt particulier pour les développeurs web, les cookies HTTP utilisés pour maintenir une session sur de nombreux sites Web peuvent être facilement volés par un attaquant à l'aide d'un ordinateur intermédiaire ou avec l'accès aux cookies enregistrés sur l'ordinateur de la victime.

6. Port scanning

Elle consiste à préciser quels ports sont ouverts afin de déterminer les vulnérabilités du système. Le firewall va dans tous les cas bloquer ces scans en annonçant le port comme fermé.

B. les attaques applicatives:

1. Les problèmes de configuration

En générale les administrateurs réseau se contente d'utilisé les configurations par défaut. Celle-ci sont souvent non sécurisées afin de facilité l'exploitation du logiciel. De plus, des erreurs peuvent apparaitre lors de la configuration d'un logiciel. [1] Une mauvaise configuration d'un serveur peut entrainer l'accès à des fichiers important ou mettre en jeu l'intégrité du système d'exploitation.

2. Les scripts

Un langage de script est un langage de programmation qui permet de manipuler les fonctionnalités d'un système informatique configuré pour fournir à l'interpréteur de ce langage un environnement et une interface qui déterminent les possibilités de celui-ci.

Le langage de script est généralement exécuté à partir de fichiers contenant le code source du programme qui sera interprété. (Voir figure5)

Figure 5 : Script

3. Les injections SQL

La faille SQLi, abréviation de "SQL Injection", soit "**injection SQL**" en français, est un groupe de méthodes d'exploitation de faille de sécurité d'une application interagissant avec une base de données. Elle permet d'injecter dans la requête SQL en cours un morceau de requête non prévu par le système et pouvant en compromettre la sécurité. [9] Comme le montre la figure si dessous. (Voir figure6)

Il existe plusieurs types d'injection SQL :

- ✓ La méthode "**bind based**"
- ✓ La méthode "**error based**
- ✓ La méthode "**union based**
- ✓ la méthode "**Stacked queries**

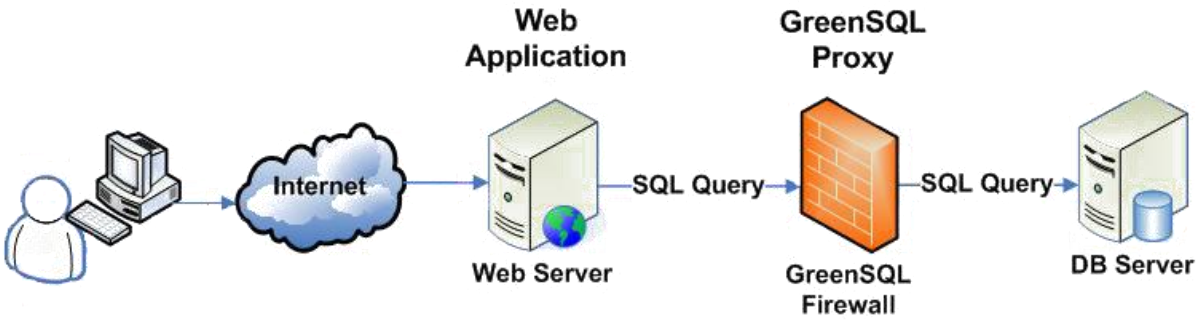


Figure 6: Les injections SQL

4. Man in the middle

L'attaque MITM est une attaque contre l'intégrité. L'attaque MITM est une redirection complète d'une connexion entre deux machines. [1] Chacun des deux interlocuteurs croit dialoguer directement avec l'autre, mais en réalité, il adresse ses données à une troisième

machine qui joue le rôle d'un routeur et renvoie les trames modifiées vers le véritable destinataire. (Voir figure7)

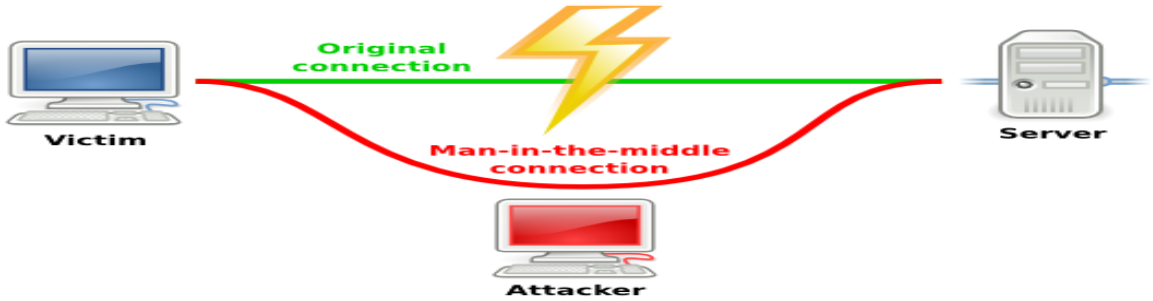


Figure 7 : homme de milieu

5. Le déni de service(DOS)

Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, 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.

6. Attaque de mot de passe

Il est facilement d'obtenir un programme fendant de mot de passe tel que la « fente ». Ce programme essaie simplement de deviner le mot de passe d'un compte.les moyens d'obtention des mots de passe des utilisateurs sont :

- **Les keyloggers**

Un enregistreur de frappe (en anglais, *keylogger*) est un logiciel espion ou un périphérique qui espionne électroniquement l'utilisateur d'un ordinateur. Le but de cet outil est varié, et peut se présenter sous des airs de légitimité, mais il ne peut être assuré qu'en espionnant l'intimité informatique de l'utilisateur.

- **L'ingénierie sociale**

. L'ingénierie sociale (ou *social engineering* en anglais) est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs.[4] Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, l'attaquant abuse de la confiance, de l'ignorance ou de la crédulité des personnes possédant ce qu'il tente d'obtenir.

- **L'espionnage**

Un logiciel espion (aussi appelé mouchard ou espiogiciel ; en anglais ***spyware***) est un logiciel qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.[1] L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

7. Les virus

Un virus informatique est un automate auto réplicatif à la base non malveillant, mais aujourd'hui souvent additionné de code malveillant, conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ».[4] Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc.

7.1. Le cheval de Troie

Un cheval de Troie désigne un type de programme informatique malveillant, invasif et parfois destructeur. Il est souvent porté :

❖ soit par un logiciel sous licence et protégé, modifié par des hackers pour en faire cadeau à la communauté numérique.

❖ soit par certains gratuiciels. [5]

7.2. Un ver

Un ver, contrairement à un virus informatique. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. L'activité d'un ver a souvent des effets secondaires comme :

- le ralentissement de la machine infectée
- le ralentissement du réseau utilisé par la machine infectée
- le plantage de services ou du système d'exploitation de la machine infectée

8. Hameçonnage

L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

Lorsque cette technique utilise les SMS pour obtenir des renseignements personnels, elle s'appelle SMiShing.

9. Les portes dérobées (backdoor)

Une porte dérobée peut être introduite soit par le développeur du logiciel, soit par un tiers. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle (par contournement de l'authentification). Enfin, selon l'étendue des droits que le système d'exploitation donne au logiciel contenant la porte dérobée, le contrôle peut s'étendre à l'ensemble des opérations de l'ordinateur.

- Parmi les motivations amenant les développeurs de logiciel à créer des portes dérobées, il y a :

- l'intérêt pratique d'un accès facile et toujours ouvert au logiciel
- la possibilité de désactiver subrepticement le logiciel en cas de désaccord avec son client

- Parmi les motivations amenant les pirates informatiques à installer une porte dérobée :

- la possibilité de surveiller ce que fait l'utilisateur légitime et de copier ou détruire des données ayant une valeur
- la possibilité de prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malfaisantes
- le contrôle d'un vaste réseau d'ordinateurs

4. Les mécanismes de prévention et détection d'attaque

➢ **Les systèmes de prévention d'intrusion**

Un système de prévention d'intrusion est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. Il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues. Comme les IDS, ils ne sont pas fiables à 100 % et risquent même en cas de faux positif de bloquer du trafic légitime. [8]

➢ **Les systèmes de détection d'intrusion**

Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Il existe trois grandes familles distinctes d'IDS :

- Les NIDS (Network Based Intrusion Detection System) ;
- Les HIDS (HostBased Intrusion Detection System) ;
- Les IDS hybrides.

5. Les mécanismes de sécurité

➢ **Cryptographie**

Le cryptage est un processus qui permet d'assurer la sécurité des informations personnelles et confidentielles. Il s'agit d'un procédé par lequel des segments de données sont mélangés mathématiquement à l'aide d'un mot de passe. [9]

✓ **le cryptage symétrique**

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages. (Voir figure8)

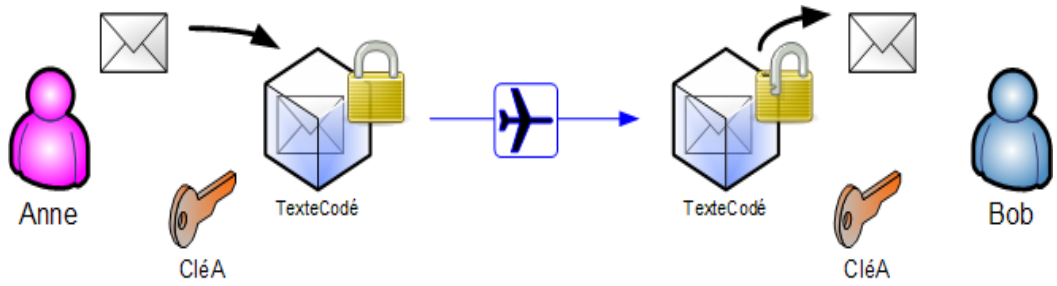


Figure 8: Cryptage symétrique

✓ **le cryptage asymétrique**

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le

message et l'autre de le décoder. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu. Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message. (voir figure 9)

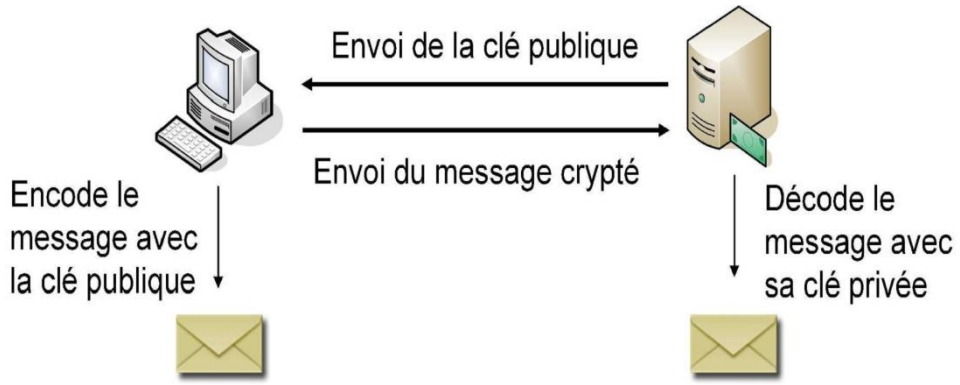


Figure 9: Cryptage asymétrique

- **la signature**

✓ **signature numérique**

La signature numérique (parfois appelée signature électronique) est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.

Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères.

Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies :

- **Authentique** : l'identité du signataire doit pouvoir être retrouvée de manière certaine.

- **Infalsifiable** : la signature ne peut pas être falsifiée.
- **Non réutilisable** : la signature n'est pas réutilisable.
- **Inaltérable** : un document signé est inaltérable.
- **Irrévocable** : la personne qui a signé ne peut le nier.

✓ **les certificats**

Un certificat électronique (aussi appelé certificat numérique ou certificat de clé publique) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges.

Il est signé par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique (virtuelle). (Voir figure 10)

Un **certificat électronique** est un ensemble de données contenant :

- Au moins une clé publique.
- Des informations d'identification, par exemple.
- Au moins une signature.

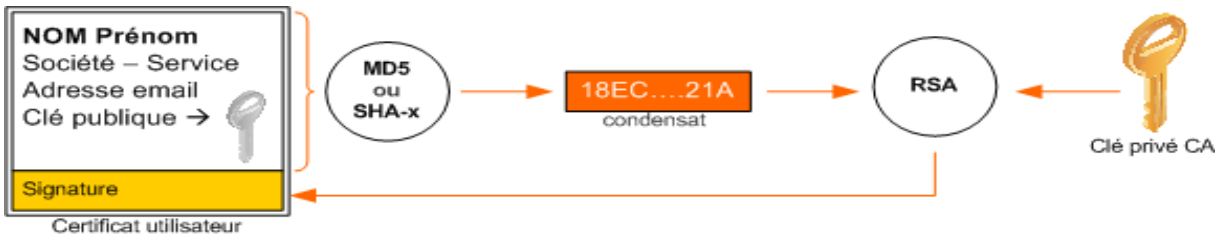


Figure 10: Certificat électronique

➢ **Pare-feu**

C'est un ensemble de différents composants matériels (physique) et logiciels (Logique) qui contrôle le trafic intérieur/extérieur selon une politique de sécurité.
Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage Indiquant les adresses IP autorisées à communiquer avec les machines aux réseaux, il

S'agit ainsi d'une passerelle filtrante. [2] le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau. (La figure 11) schématise le fonctionnement d'un pare-feu.

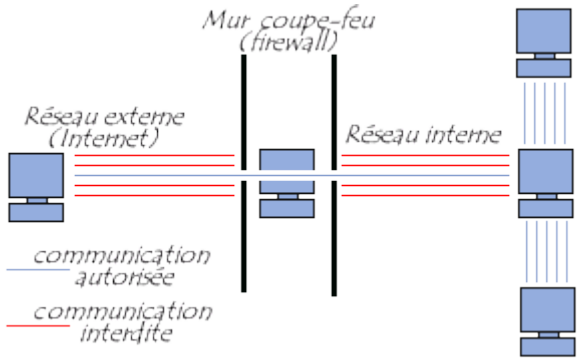


Figure 11 : pare-feu

➢ **les Anti-virus**

Les anti-virus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels Malveillants (dont les virus informatique ne sont qu'une catégorie).

Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).[7]

Différentes méthodes sont possibles :

- Les principaux antivirus du marché se concentrent sur des fichiers et comparent alors la signature virale du virus aux codes à vérifier.
- La méthode heuristique est la méthode la plus puissante, tendant à découvrir un code malveillant par son comportement. Elle essaie de le détecter en analysant le code d'un programme inconnu. Parfois de fausses alertes peuvent être provoquées.

6. Les protocoles de sécurité :

➢ **Protocole IPsec**

IPsec (*Internet Protocol Security*), défini comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques et un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. IPsec se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme.[4]

De plus, IPsec opère à la couche réseau (couche 3 du modèle OSI) contrairement aux standards antérieurs qui opéraient à la couche application (couche 7 du modèle OSI), ce qui le rend indépendant des applications.

➢ **Protocole SSL**

Transport Layer Security (**TLS**), et son prédécesseur **Secure Sockets Layer** (**SSL**), sont des protocoles de sécurisation des échanges sur Internet. Le protocole SSL a été développé à l'origine par Netscape. L'IETF a poursuivi le développement en le rebaptisant Transport Layer Security (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.

TLS (ou SSL) fonctionne suivant un mode client-serveur. Il permet de satisfaire aux objectifs de sécurité suivants :

- l'authentification du serveur
- la confidentialité des données échangées (ou session chiffrée)
- l'intégrité des données échangées ;
- de manière optionnelle, l'authentification du client (mais dans la réalité celle-ci est souvent assurée par le serveur).

➢ **Protocole HTTPs**

plus connu sous l'abréviation **HTTPS** — littéralement « protocole de transfert hypertexte sécurisé » est la combinaison du http avec une couche de chiffrement comme SSL. [10]

- HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce. Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur et reçues du serveur. Il peut permettre de valider l'identité du visiteur, si celui-ci utilise également un certificat d'authentification client.
- HTTPS est généralement utilisé pour les transactions financières en ligne. Il est aussi utilisé pour la consultation de données privées.

➢ **Protocole SSH**

Secure Shell **(SSH)** est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un *sniffer* pour voir ce que fait l'utilisateur. Le protocole SSH a été conçu avec l'objectif de remplacer les différents programmes rlogin, telnet, rcp, ftp et rsh.

Le protocole SSH existe en deux versions majeures : la version 1.0 et la version 2.0.

SSH peut également être utilisé pour transférer des ports TCP d'une machine vers une autre, créant ainsi un tunnel. Cette méthode est couramment utilisée afin de sécuriser une connexion qui ne l'est pas en la faisant transférer par le biais du tunnel chiffré SSH.

- **Protocole PKI**

Une infrastructure à clés publiques (ICP) délivre des certificats numériques. Ces certificats permettent d'effectuer des opérations cryptographiques, comme le chiffrement et la signature numérique qui offrent les garanties suivantes lors des transactions électroniques :

Les ICP permettent l'obtention de ces garanties par l'application de processus de vérification d'identité rigoureux et par la mise en œuvre de solutions cryptographiques fiables (éventuellement évaluées), conditions indispensables à la production et à la gestion des certificats électroniques.

Une infrastructure à clés publiques fournit des garanties permettant de faire a priori confiance à un certificat signé par une autorité de certification grâce à un ensemble de services.

- **Gestion du rôle serveur NPS :**

Le serveur NPS vous permet de créer et de mettre en œuvre des stratégies d'accès réseau à l'échelle d'une entreprise pour assurer l'intégrité des clients, l'authentification et l'autorisation des demandes de connexion. Vous pouvez également utiliser le serveur NPS en tant que proxy RADIUS pour transmettre les demandes de connexion au serveur NPS ou à d'autres serveurs RADIUS que vous configurez dans des groupes de serveurs RADIUS distants.

Le serveur NPS vous permet de configurer et de gérer de manière centralisée l'authentification d'accès réseau, l'autorisation et les stratégies d'intégrité des clients avec les trois fonctionnalités suivantes :

- **Serveur RADIUS**

Lorsque vous utilisez le serveur NPS en tant que serveur RADIUS, vous configurez des serveurs d'accès réseau, tels que des points d'accès sans fil et des serveurs VPN, en tant que clients RADIUS dans le serveur NPS. Vous configurez également des stratégies réseau dont le serveur NPS se sert pour autoriser les demandes de connexion, et vous pouvez configurer la gestion de compte RADIUS de telle sorte que le serveur NPS enregistre les informations de comptes dans des fichiers journaux sur le disque dur local ou dans une base de données Microsoft SQL. [12]

- **Serveur de stratégie NAP**

Lorsque vous configurez le serveur NPS en tant que serveur de stratégie NAP, le serveur NPS évalue les déclarations d'intégrité envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau (NAP) qui tentent de se connecter au réseau. Le serveur NPS agit également en tant que serveur RADIUS lorsqu'il est configuré avec la protection NAP. Vous pouvez configurer des stratégies NAP et des paramètres dans le serveur NPS, y compris les programmes de validation d'intégrité système, la stratégie de contrôle d'intégrité et les groupes de serveurs de mise à jour qui permettent aux ordinateurs clients de mettre à jour leur configuration afin de se conformer à la stratégie réseau de votre organisation.

- **Proxy RADIUS**.

Lorsque vous utilisez le serveur NPS en tant que proxy RADIUS, vous configurez des stratégies de demande de connexion qui spécifient, d'une part, les demandes de connexion transmises par le serveur NPS à d'autres serveurs RADIUS et d'autre part, les serveurs RADIUS auxquels vous souhaitez transmettre les demandes de connexion. Vous pouvez également configurer le serveur NPS de manière à ce qu'il transmette les données de comptes à un ou plusieurs ordinateurs dans un groupe de serveurs RADIUS distants à des fins de journalisation.

- **Les VPN**

Un **réseau privé virtuel**, quelques fois abrégé **RPV** au Québec et **VPN** ailleurs, de l'anglais Virtual Privat network. Est un système permettant de créer un lien direct entre des ordinateurs distants. On utilise notamment ce terme dans le travail à distance notamment, ainsi que pour l'accès à des structures de type cloud computing. [10]

Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local.

Cependant, l'infrastructure de VPN (généralement un serveur) dispose des informations permettant d'identifier l'utilisateur. Cela permet aussi de contourner les restrictions géographiques de certains services proposés sur Internet. Le VPN permet également de construire des réseaux overlay. L'utilisation de VPN n'est généralement pas légalement restreinte. (La Figure 12) montre le principe de protocole de tunnelisation.

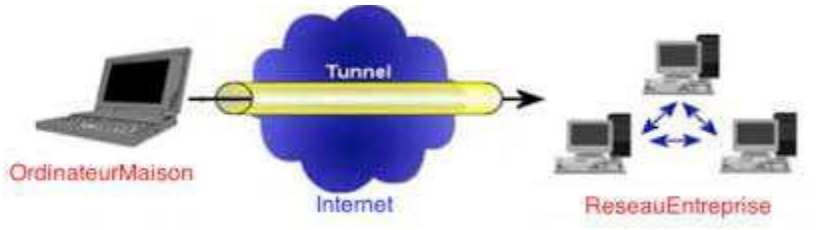


Figure 12 : principe de VPN

- **Les VLANs** :

Un **réseau local virtuel**, communément appelé **VLAN** (pour *Virtual LAN*), est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur réseau. Les VLAN présentent plusieurs intérêts. [10]

Il existe 3 types différents de VLAN :

- VLAN de niveau 1 (ou VLAN par port) : on y définit les ports du commutateur (Switch) qui appartiendront à tel ou tel VLAN.
- VLAN de niveau 2 (ou VLAN par adresse MAC) : on indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN, cette solution est plus souple que les VLAN de niveau 1.
- VLAN de niveau 3 (ou VLAN par adresse IP) : même principe que pour les VLAN de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN.

Pour déployer des VLAN, cela sous entend que le commutateur (Switch) utilisé soit gérable et qu'il gère les VLAN du niveau désiré.

➢ **Le NAT**

On dit qu'un routeur faitdu (NAT) (« traduction d'adresse réseau »lorsqu'il fait correspondre les adresses IP internes non uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4. (Voir figure 11)[11]

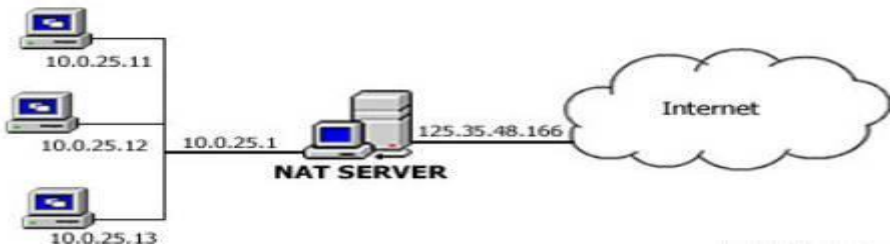


Figure 13: Network address translation

- **Types de NAT :**
- ***Nat statique :***

Où un ensemble d'adresses internes fait l'objet d'une traduction vers un ensemble de même taille d'adresses externes. Ces NAT sont dites statiques car l'association entre une adresse interne et son homologue externe est statique .La table d'association est assez simple, de type un pour un et ne contient que des adresses.

- ***Nat dynamique :***

Où un ensemble d'adresses internes est transféré dans un plus petit ensemble d'adresses externes. Ces NAT sont dites dynamiques car l'association entre une adresse interne et sa contrepartie externe est créée dynamiquement au moment de l'initiation de la connexion. Ce sont les numéros de ports qui vont permettre d'identifier la traduction en place.

7. Discussion :

La sécurité informatique est un domaine très vaste qui nécessite beaucoup de prudence et de vigilance. Il existe beaucoup de vulnérabilités auxquelles il faut faire face en utilisant les différents outils et techniques de sécurité informatique. Bien configuré et protéger le réseau, système et application est la clé de la bonne conduite d'une politique de sécurité au sein d'une organisation. Un bon administrateur réseau et système doit toujours prévoir toute sorte d'attaques en suivant les différent étapes nécessaire afin de sécuriser les données de l'organisation parce que la plupart du temps ces attaques sont irréversible.

1. Préambule :

Les attaques informatiques constituent aujourd'hui l'un des fléaux de notre civilisation moderne. Il ne se passe plus une semaine sans que l'on apprenne que telle entreprise ou telle banque a essuyé de lourdes pertes financières en raison d'une déficience de la sécurité de son réseau. Par conséquent les entreprises ne peuvent plus ignorer ces risques et se croire a l'abri de telles épreuves. C'est pour cela que nous sommes penchés sur la sécurité d'une société prise comme exemple, nous allons pour lever toute ambigüité et découvrir son architecture réseau. Tout au long de ce chapitre, nous présenterons et étudierons les principaux points critiques qui dévoilent les risques potentiels encourus en décrivant les causes qui les engendrent. Puis nous proposerons une nouvelle structure de l'architecture de l'entreprise avec les solutions à mettre en place pour avoir une meilleure sécurité.

2. Présentation de l'architecture existante :

Notre étude va portée sur l'identification des différentes failles de sécurité informatique d'une entreprise prise comme exemple dont l'architecture est représentée par (figure 14) .

- L'architecture réseau que nous avons choisi représente celle de la plupart des petites entreprises. A cet effet, le réseau étudié est composé des éléments suivants :

- 1 routeur : Il assure le routage des paquets de l'entreprise et qui est aussi considéré comme un point de défaillance.
- 1 commutateur (Switch 2960) : il assure le transfère des données (manque d'optimisation).
- Modem ADSL : Est le périphérique utiliser dans l'entreprise pour transférer des informations entre plusieurs ordinateur, ce modem ne possède pas de mot de passe.
- Des postes clients : ces postes représentent les différents ordinateurs se trouvant dans les bureaux de l'entreprise. Ces ordinateurs ne possédant pas de mots de passes ou bien les mots de passes utilisés sont faibles.
- Des serveurs : représentent les postes de données, de fichiers utilisés par le personnel de l'entreprise.
- Un firewall (ASA 5505) : il intègre des fonctionnalités de reconnaissance des utilisateurs mais ce dernier est mal configuré et aussi ya un manque de contacte ou de communication entre le fournisseur de se produit et les administrateurs réseau d'entreprise.

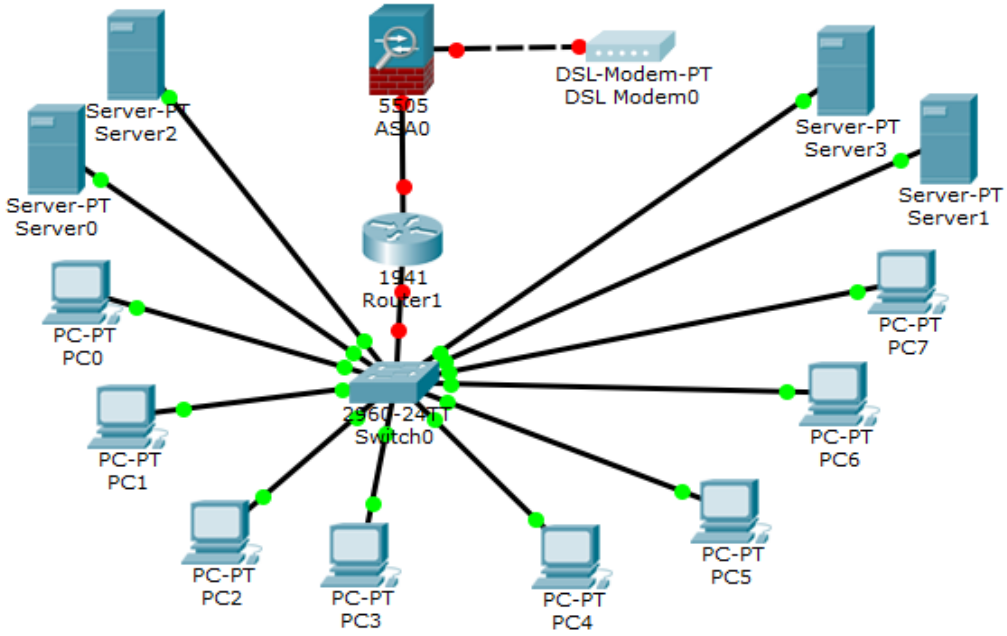


Figure 14 : Architecture existante

3. Présentation du matériel :

Les routeurs Cisco

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. [19] La fonction principale d'un routeur Cisco consiste à diriger les paquets destinés à des réseaux locaux et distant en :

✓ Déterminant le meilleur chemin pour l'envoi des paquets.
✓ Transférant les paquets vers leurs destination.

Les Switches Cisco(Catalyst Cisco) :

Les commutateurs Cisco Catalyst, nouvelle famille de périphérique autonomies à configuration fixe, apportent aux postes de travail une connectivité Faste Ethernet et Gigabit Ethernet optimisent les services de LAN sur les réseaux d'entreprise. [19]

➢ Caractéristiques :

✓ Fonctionnalités intelligentes à la périphérie du réseau.

✓ Un commutateur est également l'un des éléments fondamentaux utilisés lors de la création d'un petit réseau.

✓ Un commutateur peut être connecté sans être configuré.

4. Critiques du réseau existant :

- Le réseau est centralisé autour d'un seul switch.
- Le réseau est non administré.
- Le réseau est non sécurisé contre les intrusions d'une façon fiable.
- Accès non limité (l'accès est autorisé pour chaque machine ou unité émettrice vers n'importe quelle unité réceptrice).

4.1. Les vulnérabilités de l'architecture réseau :

➢ **Plusieurs points d'entrées du réseau (multiple entry points)**

Dans le réseau de télécommunication de l'entreprise, il existe plusieurs points d'entrée du réseau, le fait d'avoir plusieurs points d'entrée constitue une faille car il est difficile d'assurer une bonne politique de contrôle d'accès sur les entités externe utilisant le réseau d'entreprise et les services fournis.

➢ **Le Routeur**

Vu que toute l'infrastructure est connectée directement ou indirectement à ce seul routeur. La panne de se dernier causera la déconnexion de tous les autres utilisateurs. En cas de faillite du routeur, il n'y aura aucune connectivité avec le réseau externe (internet).

4.2. Les vulnérabilités de configuration et de gestion du réseau :

➢ **Mots de passe faible**

Les commutateurs et les routeurs sont protégés par des mots de passe faibles comme « Cisco » et « rtgs ». Les intrus auront ainsi des diverses option qui leur permettront de causer des dommages et d'interrompre les activités métier. Cette vulnérabilité existe à cause du manque de lignes directrices de sécurité de mot de passe, et la mauvaise appréciation des conséquences de l'utilisation de mots de passe faibles.

4.3. Vulnérabilités de configuration et de gestion des firewalls :

- **Trafic sortant non étroit (étendue)**

Les règles du firewall n'interdisent pas aux IP internes de se connecter au réseau externe. Ceci peut permettre à un intrus d'initier un « reverse tunnel » de l'intérieur de l'entreprise vers sa machine, et ainsi lui permettre de dévier les règles « externes » du firewall.

- **La dépendance de la gestion et la configuration des firewalls avec le fournisseur**

Pour la gestion et la configuration des firewalls, l'entreprise dépend toujours du fournisseur de celui-ci. En effet il y a un manque de compréhension vis-à-vis de la configuration du firewall et de ce qui est permis ou non. De même la présence du fournisseur est toujours nécessaire pour répondre aux questions techniques. Ce qui peut causer un problème de configuration si ce dernier n'est pas joignable.

- **Plusieurs comptes pour la gestion du firewall**

Les comptes d'administration des firewalls sont partagés par au moins deux employés de l'entreprise et le fournisseur. Ainsi, les responsabilités ne sont pas bien définies, il est impossible d'auditer les changements des configurations des firewalls. Et le manque de documentation des changements effectués, constitue une vulnérabilité sérieuse du mécanisme de défense de l'entreprise.

4.4. Vulnérabilité de gestion et de configuration du système :

- **Le manque d'une bonne politique de mot de passe**

L'inexistence d'une politique de mot de passe imposée au niveau du domaine est en soit une défaillance car il n'y a aucune manière de garantir un niveau minimum de complexité de mot de passe.

- **Stations de travaille non verrouillées**

Les postes de travail utilisés pour administrer le système et les postes de travail appartenant aux différents services de l'entreprise ne sont pas verrouillés quand ils ne sont plus utilisés. Ceci peut permettre aux inconnues d'introduiront ou d'avoir un accès non autorisé aux privilèges administratifs attribués à ces postes. [16]

➢ **Activités d'administrateur non surveillées**

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

5. Les solutions proposées :

5.1. L'architecture proposée :

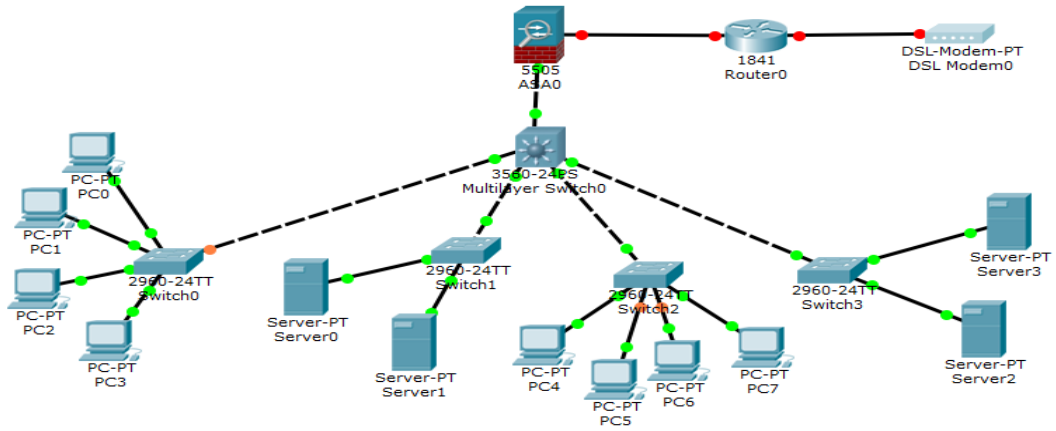


Figure 15 : Architecture proposée

5.2. Les changement de l'architecture

- **L'ajout d'un failover**

Pour remédier au point de défaillance que constitue le routeur dans l'architecture réseau, la solution que nous proposerons est l'ajout d'un fédérateur pour implémenter la technique de tolérance aux pannes (failover).il consiste à mettre en marche un seul commutateur à la fois. Le déclenchement du deuxième commutateur ne s'effectuera qu'après la panne du premier.

- **La sécurisation des points d'entrées réseau**

Nous proposons des solutions pour sécuriser les points d'entrées selon les vulnérabilités exister :

- Pour l'échange des mails au niveau interne et externe d'entreprise, nous utiliseront le serveur de messagerie Exchange2010.

- Pour les publications web, nous ajouterons un serveur web, qui renfermera le site d'entreprise.

5.3. Solution de configuration et de gestion du firewall

- **La formation des équipes de travail**

Afin de remédier aux problèmes de la dépendance du fournisseur pour la configuration et la gestion du fierewall, nous suggérons d'organiser périodiquement des formations pour améliorer les compétences des équipes de travail et les connaissances sur la technologie actuellement utilisées au niveau de l'infrastructure d'entreprise.

- **L'utilisation d'un seul compte pour la gestion du firewall et de la documentation**

Pour ne pas permettre des accès non autorisés, des changement non contrôlés et l'impossibilité de surveiller des activité de l'administrateur, la solution proposée est de désigner un seul administrateur pour gérer le compte ,et s'il a besoin de subordonnés ils doivent avoir chacun leurs comptes différents de l'administrateur pour exécuter les charges de gestion.

- **La restriction du trafic sortant et entrant**

Les règles du firewall doivent être bien réfléchies pour bien exploiter ses fonctionnalités, comme exemple, la configuration des ACL, de sorte à limiter le trafic sortant du réseau interne vers le réseau externe.

5.4. Solution de gestion et de configuration du système

- **La mise en place d'une bonne politique du mot de passe**

Le service d'annuaire Active Directory de Microsoft serveur2012,prend en charge toutes les exigences citées plus haut pour mettre en place une bonne politique de sécurité.il permet aussi de spécifier la durée de validité de mot de passe, s'il doit être changer à la première utilisation ou non.[16]

- **L'utilisation anti-virus TREND MICRO**

  La sécurité d'une entreprise s'évalue par la capacité de protection de son anti-virus, suite aux failles de sécurité, nous proposons l'utilisation de trend micro. Parmi les

fonctionnalités dont il dispose qui nous ont convaincu de son bon fonctionnement nous pouvons citer :

- ✓ Former une structure des groupes d'administration qui assure la protection antivirus de la société.
- ✓ Recevoir et diffuser de façon centralisée sur les ordinateurs les mises à jour des bases et les modules de programme des applications antivirales.
- ✓ Recevoir les notifications sur les événements critique dans le fonctionnement des applications de la protection antivirus.
- ✓ Administrer les licences de toutes les applications antivirales installées.

Ces fonctionnalités facilitent la mise en place d'un responsable de sécurité chargé d'administrer, surveiller, déployer et mettre à jour l'antivirus.

- **La surveillance d'activités d'administrateur**

Les activités de l'administrateur devraient être vérifiés afin d'assurer que les privilèges ne sont pas mal-utilisés. L'Active Directory se charge de cette tache. Il permet d'activer la journalisation, définir sa durée et de l'appliquer aux administrateurs à travers une stratégie de groupe. Ceci permet de revoir régulièrement les activités d'administrateur et d'agir immédiatement si le compte d'administrateur a été compromis. Cette configuration est typiquement administrée et surveillée par une personne autre que l'administrateur de réseau, précisément un membre de l'équipe d'audit de sécurité.

- **Le verrouillage des stations et ports physiques**

Afin de ne pas avoir un accès non autorisé aux privilèges administratifs attribués aux postes de travail. Nous implémentons des stratégies de groupe permettant le verrouillage des stations hors des horaires de travail. Pour éviter tous vol de données. Introduction de virus intentionnel ou accidentel et craquage de mot de passe, nous bloquons l'ensemble des ports physique (USB, CD/DVD, lecteur carte mémoire…etc.) grâce aux stratégies de groupe.

6. Description de la gamme ASA :

Les serveurs de sécurité adaptifs de la gamme Cisco ASA 5500 s'appuient sur une plateforme modulaire capable de fournir des services de sécurité et de VPN de prochaine génération à tous les environnement.la gamme Cisco ASA 5500 met à la disposition de l'entreprise une gamme complète de services personnalisés à travers de ses diverses édition spécifiquement conçue pour le pare-feu, la prévention des intrusions, la protection des contenues et les VPN. Ces éditions offrent une protection de haute qualité en fournissant les services adaptés à chaque site. [14]

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.

6.1. Principe de fonctionnement d'ASA :

L'ASA offre deux modes pour ses utilisateurs :

- ✓ Mode « routed » : est de niveau 3, quand il y'a de trafic, l'ASA est comme un saut sur un routeur (router hop in the network).
- ✓ Mode « transparent » : est de niveau 2, il facilite la configuration du réseau et permet de cacher le pare-feu. 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 ».

6.2. Fonctionnalités de la gamme ASA

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

- ✓ **Des fonctionnalités éprouvées de sécurité et de connectivité VPN** :

Le système de prévention des intrusions (IPS) et de firewall multifonctions, ainsi que les technologies anti-X et VPN IPSec ou SSL garantissent la robustesse de la sécurité des

applications, le contrôle d'accès par utilisateur et par application, la protection contre les vers, les virus et les logiciels malveillants, le filtrage des contenus ainsi qu'une connectivité à distance par site ou par utilisateur. [14]

✓ **La 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. [14]

✓ **L'architecture évolutive des services AIM** :

Fondement architectural de la gamme Cisco ASA 5500, AIM permet l'application de politiques de sécurité hautement personnalisables ainsi qu'une évolutivité de service sans précédent qui renforce la protection des entreprises contre l'environnement toujours plus dangereux qui les menace. [14]

7. Discussion :

L'enjeu principale d'un réseau sécurisé est de pouvoir réglementer les accès aux ressources que ça soit interne (local) ou externe(Wan), tout en essayant au maximum de limiter les failles d'éventuelles attaques ou vols d'information afin d'accroitre la sécurité du réseau local.

Dans ce chapitre nous avons présenté des solutions que nous allons implémenter, celle-ci nous permettra de définir à travers leurs fonctionnalités une meilleure planification de dépoilement.

1. Préambule :

La sécurité du réseau est un sujet de taille, dont la plus grande partie n'est pas abordée dans ce chapitre. Ceci dit, la compréhension approfondie des listes de contrôle d'accès est l'une des principales compétences requises chez un administrateur réseau. Sécuriser le réseau est la principale raison vous incitant à configurer des listes de contrôles d'accès. Ce chapitre explique comment utiliser les listes de contrôle d'accès standard et étendues dans le cadre d'une solution de sécurité. Vous y trouverez des conseils, des éléments dont il faut tenir compte, des recommandations et des lignes directrices générales sur l'utilisation des listes de contrôle d'accès.

2. Définition

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses ou aux protocoles de couche supérieure. Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau. Des listes de contrôle d'accès peuvent être configurées pour tous les protocoles réseau routés.

Une fois configurées, les listes de contrôle d'accès assurent les tâches suivantes :

- ✓ Elles limitent le trafic réseau pour accroître les performances réseau. Ainsi, la charge réseau est nettement réduite et les performances réseau sont sensiblement améliorées.
- ✓ Elles contrôlent le flux de trafic.
- ✓ Elles fournissent un niveau de sécurité de base pour l'accès réseau.
- ✓ Elles filtrent le trafic en fonction de son type.
- ✓ Elles filtrent les hôtes pour autoriser ou refuser l'accès aux services sur le réseau.

3. Fonctionnement des listes de contrôle d'accès :

Les listes de contrôle d'accès définissent des règles de contrôle pour les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie. Elles ne gèrent pas les paquets provenant du routeur lui-même. [13]

Les listes de contrôle d'accès sont configurées pour s'appliquer au trafic entrant ou sortant.

- **Listes de contrôle d'accès entrantes** : les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet.

- **Listes de contrôle d'accès sortantes** : les paquets entrants sont acheminés vers l'interface de sortie, puis traités par le biais de la liste de contrôle d'accès sortante. Les listes de contrôle d'accès sortantes sont particulièrement efficaces lorsqu'un même filtre est appliqué aux paquets provenant de plusieurs interfaces d'entrée avant de quitter la même interface de sortie.

La dernière instruction d'une liste de contrôle d'accès est toujours une instruction implicite deny. Cette instruction est automatiquement ajoutée à la fin de chaque liste de contrôle d'accès, même si elle n'est pas physiquement présente. L'instruction implicite deny bloque l'ensemble du trafic. En raison de ce refus implicite, une liste de contrôle d'accès qui n'a pas au moins une instruction d'autorisation bloquera tout le trafic. [13]

4. Type des ACLs :

Il existe deux types de listes de contrôle d'accès IPv4 : les listes standards et les listes étendues.

✓ **Listes de contrôle d'accès standard**

Les listes de contrôle d'accès standard peuvent être utilisées pour autoriser ou refuser le trafic uniquement depuis des adresses IPv4 source. [15] La destination du paquet et les ports concernés ne sont pas évalués.

✓ **Listes de contrôle d'accès étendues**

Les listes de contrôle d'accès étendues filtrent les paquets IPv4 en fonction de différents critères :

- Type de protocole
- Adresse IPv4 source
- Adresse IPv4 de destination

- Ports TCP ou UDP source
- Ports TCP ou UDP de destination
- Informations facultatives sur le type de protocole pour un contrôle plus précis

5. Comparaison des ACLs standards et étendues

5.1. Numérotation et attribution d'un nom aux ACLs

Les listes de contrôle d'accès standard et étendues et leur liste d'instructions peuvent être identifiées par un numéro ou par un nom.

Les listes de contrôle d'accès numérotées sont pratiques pour déterminer le type de liste sur des réseaux de petite taille dont la définition du trafic est plus homogène. Toutefois, le numéro n'indique pas la fonction d'une liste de contrôle d'accès. C'est pourquoi, depuis la version 11.2 de Cisco IOS, vous pouvez utiliser un nom pour identifier une liste de contrôle d'accès Cisco. [17]

Concernant les listes de contrôle d'accès numérotées, les numéros 200 à 1 299 ne sont disponibles, On porte sur les listes de contrôle d'accès IP uniquement.

5.2. Masque générique dans les ACLs :

➢ **Initiation aux masques générique :**

Les listes de contrôle d'accès IPv4 incluent l'utilisation de masques génériques. Un masque générique est une chaîne de 32 chiffres binaires utilisés pour déterminer quels bits de l'adresse examiner afin d'établir une correspondance. [17]

Les masques génériques utilisent les chiffres binaires 1 et 0 pour filtrer des adresses IP ou des groupes d'adresses IP, afin d'autoriser ou de refuser l'accès aux ressources.

Les masques génériques respectent les règles suivantes pour faire correspondre les chiffres binaires 1 et 0 :

- Bit 0 de masque générique : permet de vérifier la valeur du bit correspondant dans l'adresse.

- Bit 1 de masque générique : permet d'ignorer la valeur du bit correspondant dans l'adresse.

➢ **Utilisation d'un masque générique**

Les masques génériques sont également utilisés lors de la configuration de certains protocoles de routage IPv4 tels que le protocole OSPF, pour les activer sur des interfaces spécifiques

➢ **Calcul de masque générique :**

Le calcul des masques génériques peut être complexe. La méthode la plus rapide consiste à soustraire le masque de sous-réseau de 255.255.255.255.

- **Calcul du masque générique : exemple**

Supposons que vous souhaitiez faire correspondre uniquement les réseaux 192.168.10.0 et 192.168.11.0. Utilisons 255.255.255.255 et soustrayons le masque de sous-réseau normal, à savoir 255.255.252.0 dans cet exemple. Cette solution génère 0.0.3.255.

Vous pouvez obtenir le même résultat en utilisant des instructions telles que les suivantes :

R1(config)# **access-list 10 permit 192.168.10.0**

R1(config)# **access-list 10 permit 192.168.11.0**

Il est bien plus efficace de configurer le masque générique de la manière suivante :

R1(config)# **access-list 10 permit 192.168.10.0 0.0.3.255**

➢ **Mots-clés des bits de masque générique**

Travailler avec des représentations décimales de bits de masque générique peut être fastidieux. Les mots-clés **host** (hôte) et **any** (tous) permettent d'identifier les utilisations les plus courantes des masques génériques. Ces mots-clés facilitent également la lecture d'une liste de contrôle d'accès en offrant des indices visuels comme la source ou la destination des critères. [19]

- ✓ Le mot-clé **host** remplace le masque 0.0.0.0. Ce masque indique que tous les bits de l'adresse IPv4 doivent correspondre ou qu'un seul hôte est conforme.
- ✓ Le mot-clé **any** remplace l'adresse IP et le masque 255.255.255.255. Ce masque indique qu'il convient d'ignorer l'intégralité de l'adresse IPv4 ou d'accepter n'importe quelle adresse.

Exemple 1 : processus de masque générique avec une adresse IP unique

Dans l'exemple 1, au lieu de saisir **192.168.10.10 0.0.0.0**, vous pouvez utiliser **host 192.168.10.10**.

Exemple 2 : processus de masque générique avec une adresse IP à concordance quelconque

Dans l'exemple 2, au lieu de saisir **0.0.0.0 255.255.255.255**, vous pouvez utiliser le mot-clé **any** seul.

6. Directives concernant la création des ACLs :

6.1. Directives générales sur la création des ACLs :

L'écriture des listes de contrôle d'accès peut être une tâche complexe. Pour chaque interface, plusieurs stratégies peuvent être nécessaires pour gérer le type de trafic autorisé à entrer dans cette interface ou en sortir. Si nous avions besoin de listes de contrôle d'accès pour les deux protocoles, sur les deux interfaces et dans les deux directions, nous aurions besoin de huit listes de contrôle d'accès distinctes. Chaque interface possèderait quatre listes de contrôle d'accès : deux pour IPv4 et deux pour IPv6. Pour chaque protocole, une liste de contrôle d'accès sert au trafic entrant et une autre au trafic sortant. [15]

Vous trouverez ci-dessous quelques instructions pour utiliser les listes de contrôle d'accès :

- Utilisez des listes de contrôle d'accès sur les routeurs pare-feu entre votre réseau interne et un réseau externe, par exemple Internet.
- Utilisez des listes de contrôle d'accès sur un routeur situé entre deux sections de votre réseau pour contrôler le trafic entrant ou sortant sur une partie donnée du réseau interne.

- Configurez des listes de contrôle d'accès sur les routeurs périphériques situés à la périphérie de vos réseaux. Cela permet de fournir une protection de base contre le réseau externe ou entre une zone plus sensible et une zone moins contrôlée de votre réseau.

- Configurez des listes de contrôle d'accès pour tout protocole réseau configuré sur les interfaces de routeur périphérique.

6.2. Règle des trois P

Pour retenir la règle générale d'application des listes de contrôle d'accès, il suffit de se souvenir des trois P. Vous pouvez configurer une liste de contrôle d'accès par protocole, par direction et par interface :

- **Une liste de contrôle d'accès par protocole** : pour contrôler le flux du trafic sur une interface, définissez une liste de contrôle d'accès pour chaque protocole activé sur l'interface.

- **Une liste de contrôle d'accès par direction** : les listes de contrôle d'accès contrôlent le trafic dans une seule direction à la fois sur une interface. Vous devez créer deux listes de contrôle d'accès ; la première pour contrôler le trafic entrant et la seconde pour contrôler le trafic sortant.

- **Une liste de contrôle d'accès par interface** : les listes de contrôle d'accès contrôlent le trafic dans une seule interface, par exemple, Gigabit Ethernet 0/0.

6.3. Méthodes recommandé pour les ACLs :

L'utilisation des listes de contrôle d'accès nécessite beaucoup de précision et de soin. Les erreurs peuvent vous coûter cher et se solder par des pannes de réseau, d'importants efforts de dépannage et des services réseau médiocres. Avant de configurer une liste de contrôle d'accès, une planification de base s'impose.[17]

7. Directives concernant le placement des ACLs :

7.1. Positionnement des ACLs :

Le positionnement approprié d'une liste de contrôle d'accès peut optimiser l'efficacité du réseau. Une liste de contrôle d'accès peut être placée de sorte à réduire le trafic superflu.

Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances.

➢ **Les règles de base sont les suivantes** :

- **Listes de contrôle d'accès étendues** : placez les listes de contrôle d'accès étendues le plus près possible de la source du trafic à filtrer.
- **Listes de contrôle d'accès standard** : étant donné que les listes de contrôle d'accès standard ne précisent pas les adresses de destination, placez-les le plus près possible de la destination.

✓ La position de la liste de contrôle d'accès et le type de liste utilisé peuvent également dépendre des caractéristiques suivantes :

- **Le contrôle de l'administrateur réseau**
- **Bande passante des réseaux concernés**
- **Facilité de configuration**

7.1.1. Position des ACLs standard :

Les listes de contrôle d'accès standard permettent uniquement de filtrer le trafic en fonction d'une adresse source. Sur la figure 16, l'administrateur souhaite empêcher le trafic provenant du réseau 192.168.10.0/24 d'accéder au réseau 192.168.30.0/24.

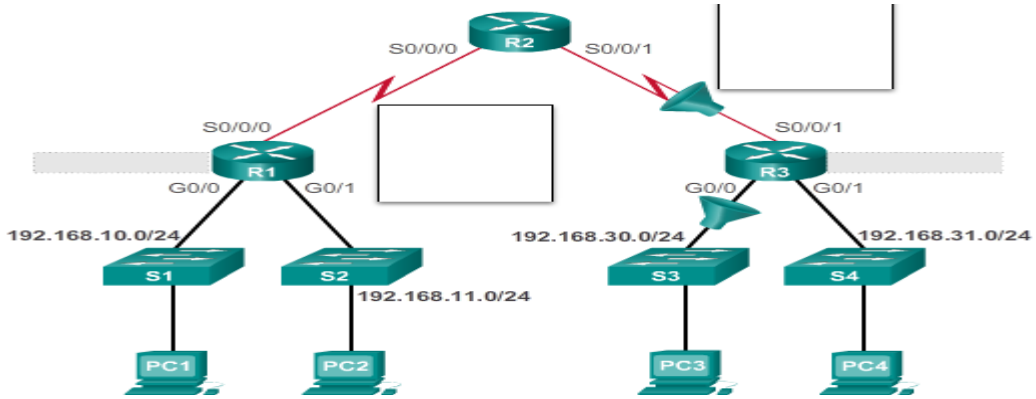


Figure 16 : Position des ACL standard

7.1.2. Emplacement des ACLs étendue :

Comme les listes de contrôle d'accès standard, les listes de contrôle d'accès étendues peuvent filtrer le trafic en fonction de l'adresse source. Cependant, une liste de contrôle d'accès étendue peut également filtrer le trafic en fonction de l'adresse de destination, du protocole et du numéro de port.

Sur la figure 17, l'administrateur de la société A, qui comprend les réseaux 192.168.10.0/24 et 192.168.11.0/24 (appelés .10 et .11 dans cet exemple), souhaite contrôler le trafic vers la société B. En particulier, l'administrateur souhaite refuser le trafic Telnet et FTP provenant du réseau .11 vers le réseau 192.168.30.0/24 (.30, dans cet exemple) de la société B. Dans un même temps, le reste du trafic provenant du réseau .11 doit être autorisé à quitter la société A sans aucune restriction.

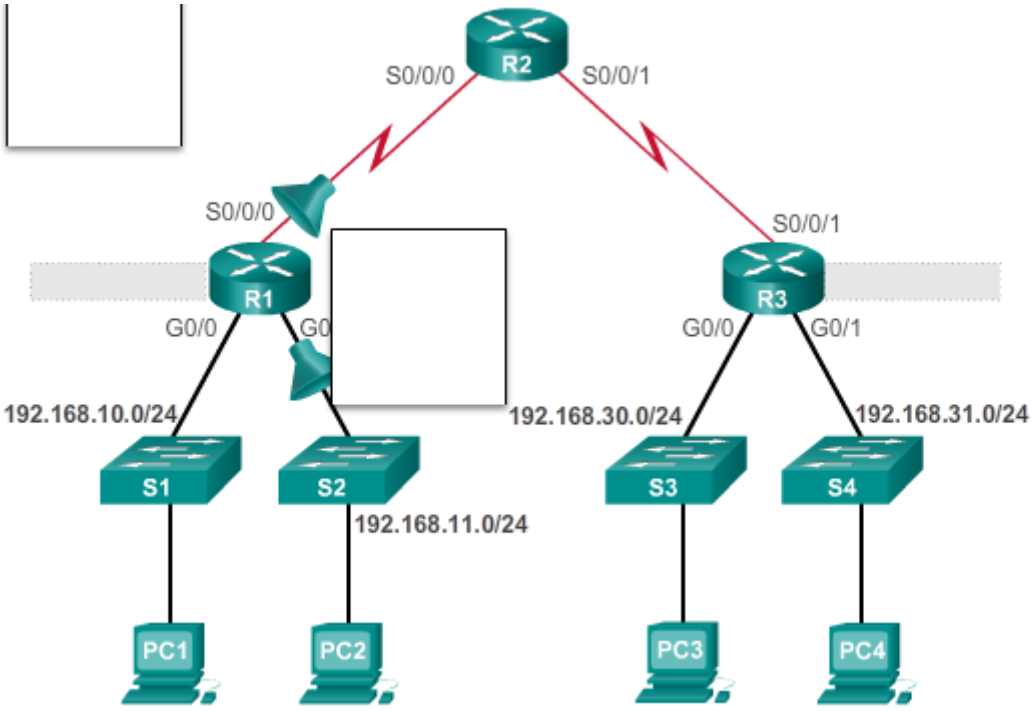


Figure 17 : Emplacement des ACL étendue

8. ACL standard IPV4

8.1. Configuration de listes de contrôle d'accès standard

Pour utiliser des listes de contrôle d'accès standard numérotées sur un routeur Cisco, vous devez d'abord créer la liste de contrôle d'accès standard, puis l'activer sur une interface.

La commande de configuration globale **access-list** définit une liste de contrôle d'accès standard associée à un numéro compris entre 1 et 99. La version 12.0.1 du logiciel Cisco IOS a élargi cette plage de numéros et permet d'attribuer les numéros 1 300 à 1 999 aux listes de contrôle d'accès standard. Cela permet d'obtenir un maximum de 798 listes de contrôle d'accès standard. [15]

La syntaxe complète de la commande des listes de contrôle d'accès standard est la suivante :

Router(config)# **access-list** *access-list-number* { **deny** | **permit** | **remark** } *source* [*source-wildcard*][**log**]

Les ACE peuvent autoriser ou refuser un hôte ou une plage d'adresses d'hôte. Pour créer une instruction d'hôte dans la liste de contrôle d'accès 10 qui autorise un hôte spécifique possédant l'adresse IP 192.168.10.0, vous devrez saisir :

R1(config)# **access-list 10 permit host 192.168.10.10**

Pour supprimer la liste de contrôle d'accès, la commande de configuration globale **no access-list** est utilisée. La commande **show access-list** permet de vérifier que la liste d'accès 10 a été supprimée.

En général, lorsqu'un administrateur crée une liste de contrôle d'accès, il connait et comprend la fonction de chaque instruction. Il est important d'ajouter des remarques. Le mot-clé **remark** est utilisé à des fins de documentation. Lorsque l'on consulte la liste de contrôle d'accès dans la configuration à l'aide de la commande **show running-config**, la remarque s'affiche également.

8.2. Création des acl standard nommées

Si vous attribuez un nom à une liste de contrôle d'accès, il vous sera plus facile d'en comprendre la fonction. Lorsque vous identifiez une liste de contrôle d'accès par un nom plutôt qu'un numéro, le mode de configuration et la syntaxe de commande sont légèrement différents.

Étape 1. À partir du mode de configuration globale, utilisez la commande **ip access-list** pour créer une liste de contrôle d'accès nommée. La commande *name* **ip access-list standard**

permet de créer une liste de contrôle d'accès standard nommée, tandis que la commande *name* **ip access-list extended** permet de créer une liste de contrôle d'accès étendue.

Étape 2. En mode de configuration des listes de contrôle d'accès nommées, utilisez les instructions **permit** ou **deny.**

Étape 3. Appliquez la liste de contrôle d'accès à une interface à l'aide de la commande **ip access-group**. Indiquez si la liste de contrôle d'accès doit être appliquée aux paquets lorsqu'ils entrent dans l'interface (**in**) ou lorsqu'ils quittent l'interface (**out**).

8.3. Modification des acl standard nommées

La figure illustre un exemple d'insertion d'une ligne dans une liste de contrôle d'accès nommée.

- Dans le premier résultat de la commande show, vous pouvez constater que la liste de contrôle d'accès nommée NO_ACCESS possède deux lignes numérotées indiquant les règles d'accès du poste de travail associé à l'adresse IPv4 192.168.11.10.
- La commande ip access-list standard permet de configurer les listes de contrôle d'accès nommées. Vous pouvez insérer ou supprimer des instructions à partir du mode de configuration des listes d'accès nommées. La commande no sequence nember permet de supprimer une instruction.
- Pour ajouter une instruction indiquant de refuser un autre poste de travail, vous devez insérer une ligne numérotée. Dans cet exemple, le poste de travail associé à l'adresse IPv4 192.168.11.11 est ajouté à l'aide du nouveau numéro d'ordre 15.
- Le résultat final de la commande show confirme que l'accès du nouveau poste de travail est maintenant refusé

```
R1# show access-lists
Standard IP access list NO_ACCESS
     10 deny    192.168.11.10
     20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
     10 deny    192.168.11.10
     15 deny    192.168.11.11
     20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Figure 18 : insertion d'une ligne dans une ACL nommée

8.4. Édition des listes de contrôle d'accès numérotées

Lorsque vous configurez une liste de contrôle d'accès standard, les instructions sont ajoutées à la configuration en cours. Cependant, il n'existe aucune fonction d'édition intégrée vous permettant de modifier une liste de contrôle d'accès. Les listes de contrôle d'accès standard numérotées peuvent être modifiées de deux façons. [18]

✓ **Méthode 1 : à l'aide d'un éditeur de texte**

Étape 1. Affichez la liste de contrôle d'accès à l'aide de la commande **show running-config**.

Étape 2. Mettez en surbrillance la liste de contrôle d'accès, copiez-la, puis collez-la dans le Bloc-notes Microsoft. Une fois que la liste de contrôle d'accès est correcte dans le Bloc-notes Microsoft, mettez-la en surbrillance et copiez-la.

Étape 3. Supprimez la liste d'accès à l'aide de la commande **no access-list 1**. Collez ensuite la nouvelle liste de contrôle d'accès dans la configuration du routeur.

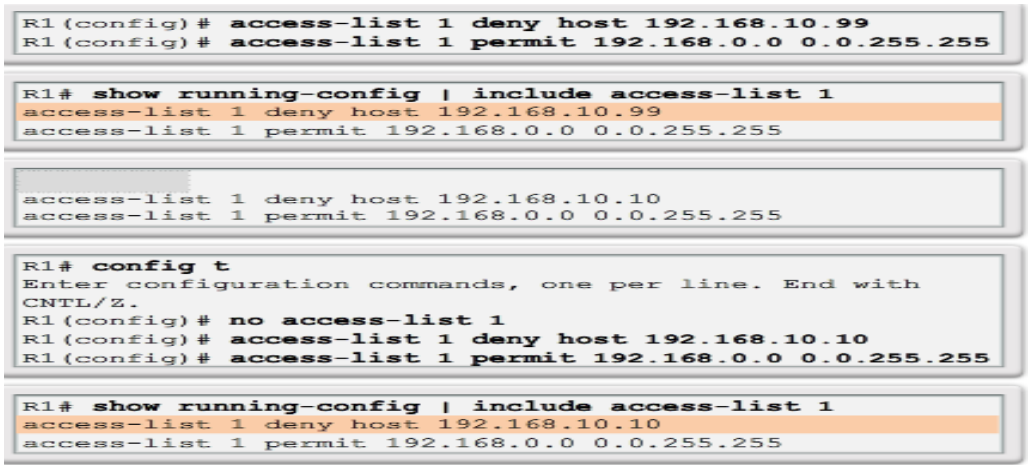


Figure 19 : modification et correction d'une ACL standard méthode 1

✓ **Méthode 2 : à l'aide du numéro d'ordre**

Étape 1. Affichez la liste de contrôle d'accès actuelle à l'aide de la commande **show access lists 1.**

Étape 2. Il faut ajouter une nouvelle instruction portant le numéro d'ordre 10, à l'aide de la Commande **10 deny host 192.168.10.10**

Étape 3. Vérifiez les modifications à l'aide de la commande **show access-lists**

```
R1(config)#access-list 1 deny host 192.168.10.99
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

```
R1#show access-lists 1
Standard IP access list 1
    10 deny   192.168.10.99
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

```
R1#conf t
R1(config)#ip access-list standard 1
R1(config-std-nacl)#no 10
R1(config-std-nacl)#10 deny host 192.168.10.10
R1(config-std-nacl)#end
R1#
```

```
R1#show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

Figure 20 : modification et correction d'une ACL standard méthode 2

9. ACL étendue IPV4

9.1. Structure d'une acl étendue

Des listes de contrôle d'accès IPv4 étendues peuvent être créées pour permettre un contrôle plus précis du filtrage du trafic. Les listes de contrôle d'accès étendues sont numérotées de 100 à 199 et de 2 000 à 2 699 ce qui offre un total de 799 numéros de listes de contrôle d'accès étendues disponibles. Vous pouvez également attribuer un nom aux listes de contrôle d'accès étendues. [15]

9.2. Configuration des ACL etendue

Les procédures de configuration des listes de contrôle d'accès étendues sont les mêmes que pour les listes de contrôle d'accès standard. La liste de contrôle d'accès étendue est d'abord configurée, puis elle est activée sur une interface. La syntaxe et les paramètres de commande sont plus complexes car ils prennent en charge des fonctions supplémentaires fournies par les listes de contrôle d'accès étendues.

9.3. Création des acl etendue nommées

La création des listes de contrôle d'accès étendues nommées est similaire à la création des listes de contrôle d'accès standard nommées.

9.4. Modification des ACL etendue :

La modification des listes de contrôle d'accès étendues est similaire à celle des listes de contrôle d'accès standard, comme évoqué précédemment.

Dans l'exemple de la figure, l'administrateur doit modifier la liste de contrôle d'accès nommée SURFING pour corriger une faute de frappe dans l'instruction concernant le réseau source.

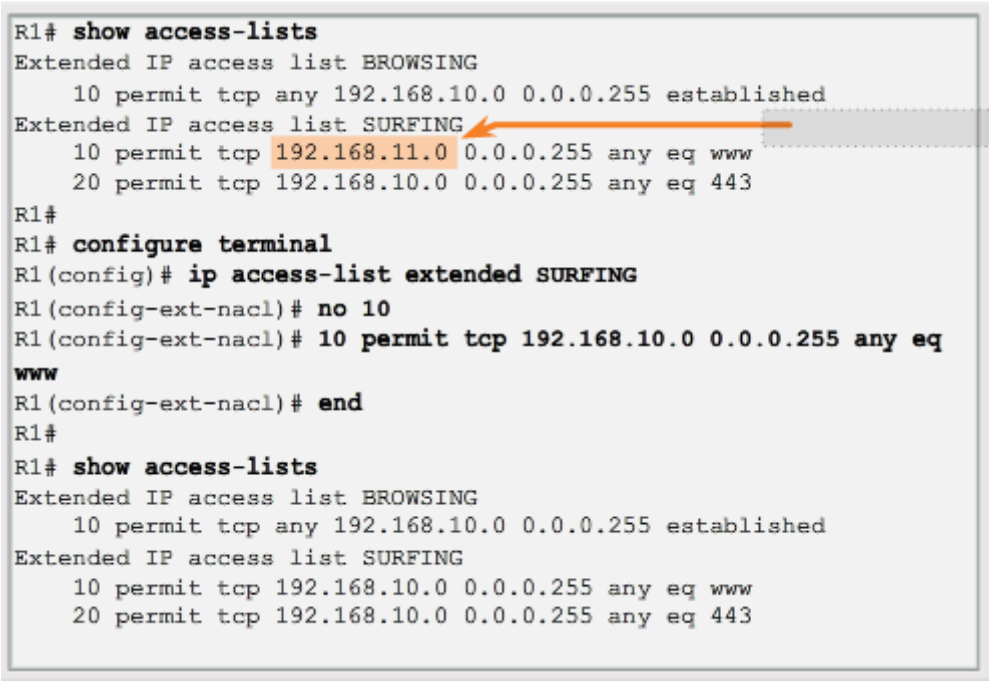


Figure 21 : modification et correction d'une ACL étendue

10. Erreurs des ACLs courantes

10.1. Dépannage des erreurs des ACL courante :

Les commandes **show** décrites précédemment permettent de repérer les erreurs de liste de contrôle d'accès les plus courantes. En général, ces erreurs concernent l'ordre de saisie des ACE et l'application de critères inappropriés aux règles des listes de contrôle d'accès.

- **1er exemple d'erreur**

Sur la figure, l'hôte 192.168.10.10 n'a établi aucune connexion avec 192.168.30.12. Dans le résultat de la commande **show access-lists**, des correspondances sont affichées pour la première instruction de refus. Cela indique que cette instruction a obtenu une correspondance du trafic.[17]

Solution : vérifiez l'ordre des ACE. L'hôte 192.168.10.10 n'a établi aucune connectivité avec 192.168.30.12 à cause de l'ordre de la règle 10 dans la liste de contrôle d'accès. Sachant que le routeur traite les listes de contrôle d'accès de haut en bas, l'instruction 10 refuse l'hôte 192.168.10.10, donc l'instruction 20 ne peut pas obtenir de correspondance. Les instructions 10 et 20 doivent être inversées. La dernière ligne autorise tout autre trafic non TCP correspondant au protocole IP (ICMP, UDP, etc.).

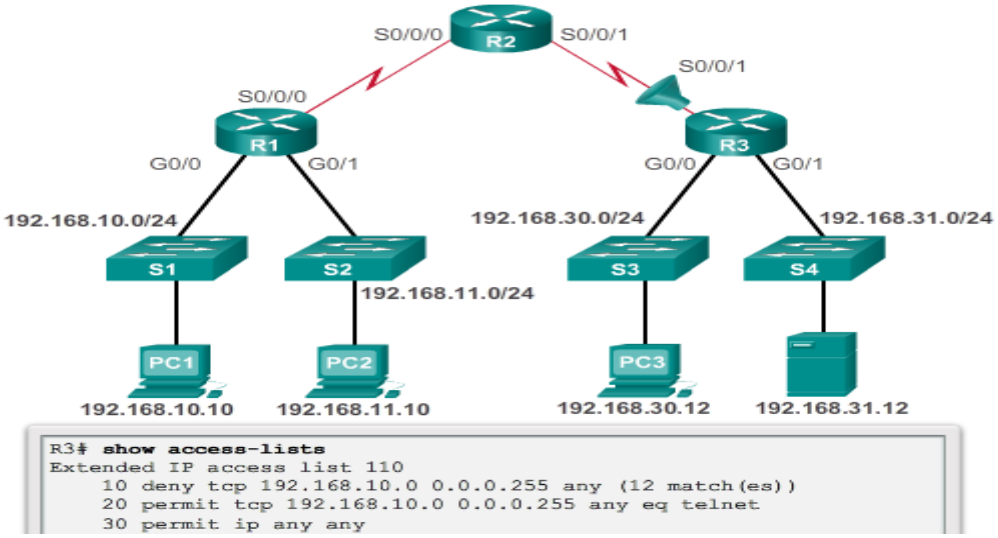


Figure 22 : la 1ére solution appliquée

- **2e exemple d'erreur**

Sur la figure, le réseau 192.168.10.0/24 ne peut pas utiliser TFTP pour se connecter au réseau 192.168.30.0/24.[17]

Solution : le réseau 192.168.10.0/24 ne peut pas utiliser TFTP pour se connecter au réseau 192.168.30.0/24, car TFTP utilise le protocole de transport UDP. L'instruction 30 dans la liste de contrôle d'accès 120 autorise tout autre trafic TCP. Cependant, étant donné que TFTP utilise le protocole UDP et non TCP, il est implicitement refusé. Souvenez-vous que

l'instruction de refus global implicite n'apparaît pas dans le résultat de la commande **show access-lists** et donc que les correspondances ne sont pas indiquées.

L'instruction 30 devrait être **ip any any**.

Cette liste de contrôle d'accès fonctionne, qu'elle soit appliquée à l'interface G0/0 (routeur R1), S0/0/1 (routeur R3) ou S0/0/0 (routeur R2) dans la direction entrante. Néanmoins, conformément à la règle voulant que les listes de contrôle d'accès étendues soient placées le plus près possible de la source, la meilleure solution est de la placer sur l'interface G0/0 (routeur R1) dans la direction entrante. Ainsi, tout trafic indésirable y est filtré sans traverser l'infrastructure réseau

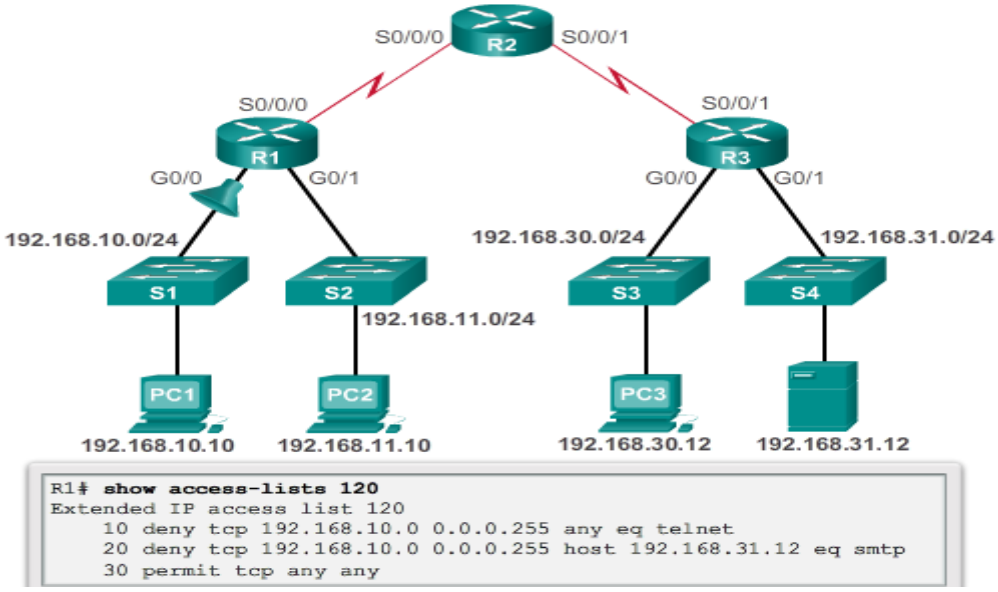


Figure 23 : la 2éme solution appliquée

11. ACL IPV6

11.1. Type des ACL ipv6

Les listes de contrôle d'accès IPv6 sont très semblables aux listes de contrôle d'accès IPv4, tant dans leur fonctionnement que dans leur configuration. Si vous connaissez déjà les listes d'accès IPv4, vous n'aurez aucun mal à comprendre et à utiliser les listes IPv6.Il existe deux types de listes de contrôle d'accès IPv4, les listes de contrôle d'accès standard et étendues. Ces deux types de liste peuvent être numérotés ou nommés. En revanche, il n'existe qu'un seul

type de liste de contrôle d'accès IPv6 et il correspond à une liste de contrôle d'accès étendue IPv4 nommée. Les listes de contrôle d'accès IPv6 numérotées n'existent pas.[13] Pour résumer, les listes de contrôle d'accès IPv6 présentent les caractéristiques suivantes :

- Elles sont nommées uniquement
- Leur fonctionnalité équivaut à celle d'une liste de contrôle d'accès IPv4 étendue

Une liste de contrôle d'accès IPv4 et une liste de contrôle d'accès IPv6 ne peuvent pas porter le même nom.

11.2. Comparaison entre ipv4 et ipv6

Bien que les adresses IPv4 et IPv6 liste sont très similaires, il existe trois différences entre eux :

- **Application d'une liste de contrôle d'accès IPv6**

La première différence concerne la commande utilisée pour appliquer une liste de contrôle d'accès IPv6 à une interface. La commande **ip access-group** permet d'appliquer une liste de contrôle d'accès IPv4 à une interface IPv4. IPv6 utilise la commande **ipv6 traffic-filter** pour effectuer la même tâche sur les interfaces IPv6.

- **Aucun masque générique**

  À la différence des listes de contrôle d'acccèsIPv4, les listes de contrôle d'accès IPv6 n'utilisent pas de masques génériques. Au lieu de cela, la longueur de préfixe est utilisée pour indiquer dans quelle mesure l'adresse IPv6 source ou de destination doit correspondre.

- **Instructions supplémentaires par défaut**

La dernière différence majeure concerne l'ajout de deux instructions d'autorisation implicites à la fin de chaque liste de contrôle d'accès IPv6. À la fin de chaque liste de contrôle d'accès IPv4 standard ou étendue, il existe une instruction implicite **deny any** ou **deny any any**. Il existe également une instruction **deny ipv6 any any** similaire à la fin de chaque liste de contrôle d'accès IPv6. En revanche, dans le cas d'IPv6, deux autres instructions implicites sont appliquées par défaut :

- **permit icmp any any nd-na**
- **permit icmp any any nd-ns**

Ces deux instructions permettent au routeur de prendre part à l'équivalent IPv6 du protocole ARP pour IPv4. Souvenez-vous qu'ARP est utilisé dans le cadre d'IPv4 pour traduire les adresses de couche 3 en adresses MAC de couche 2.

Ipv6 utilise des messages de découverte de voisin (ND pour Neighbor Discovery) ICMP pour effectuer la même opération. La découverte de voisin fait appel à des messages de sollicitation de voisin (NS pour Neighbor Solicitation) et d'annonce de voisin (NA pour Neighbor Advertisement).Les messages ND sont encapsulés en paquets IPv6 et nécessitent des services de la couche réseau IPv6 tandis que le protocole ARP pour IPv4 n'utilise pas la couche 3. Étant donné qu'IPv6 utilise le service de couche 3 pour la découverte de voisin, les listes de contrôle d'accès IPv6 doivent autoriser implicitement l'envoi et la réception des paquets ND sur une interface. Plus précisément, les messages nd-na (découverte de voisin-annonce de voisin) et nd-ns (découverte de voisin-sollicitation de voisin) sont autorisés. [13]

Rq : Tout comme les listes de contrôle d'accès nommées IPv4, les noms des listes de contrôle d'accès IPv6 sont alphanumériques, sensibles à la casse et doivent être uniques. Contrairement aux listes de contrôle d'accès IPv4, l'option standard ou étendue n'est pas nécessaire .vu que l'objectif visé est de filtrer les interfaces des équipements d'interconnexion donc pour cela j'ai utilisé les ACL ipv4 vu que elles ont la même fiabilité que L'IPv6 et aussi moins complexe a configurées.

12. Discussion :

Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau informatique. Comme nous avons vu que les listes de contrôle d'accès peuvent être configurées pour tous les protocoles réseau routés. Ce chapitre nous a donné l'occasion de développer nos connaissances sur les listes de contrôle d'accès et de voir aussi les différents types de ces dernières, avantage de chaque type, leur positionnement et leur configuration.

1. Préambule :

L'objectif de cette partie est de faire une étude des solutions à apporter au réseau de l'entreprise après une analyse de l'existant. Dans le but de mieux renforcer la sécurité du réseau de l'entreprise, nous avons procéder comme suite :

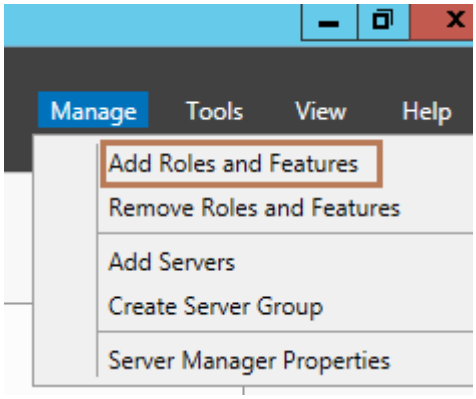
- ✓ Déploiement d'un serveur de fichier, stocker et partager des fichiers entre les utilisateurs de réseau d'une manière centralisée.
- ✓ Déploiement d'un serveur RADIUS pour gérer de façon centralisée les accès aux réseaux.
- ✓ Configuration des ACLs (listes de contrôle d'accès).
- ✓ Sécurisation des accès aux équipements réseau (fédérateur et Switch).

2. Mise en place d'un serveur de fichiers :

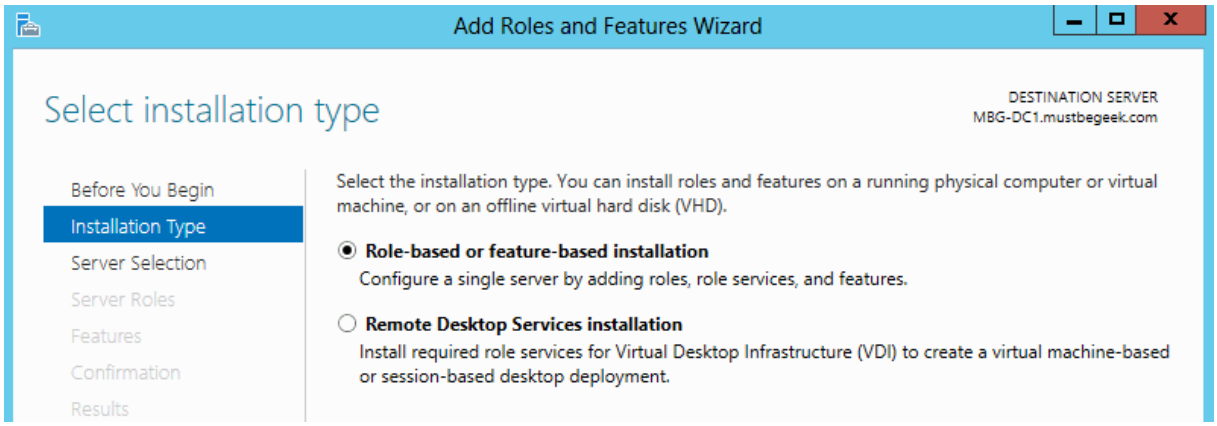
Avant d'implémenter le serveur il faut d'abord vérifiée les conditions suivantes :

- Le système de configuration est configuré correctement
- L'ordinateur est associé à un domaine Active Directory en tant que serveur membre
- Tous l'espace disque est alloué
- Le pare-feu Windows est activé
- Tous les volumes de disque existants utilisent le système de fichier NTFS

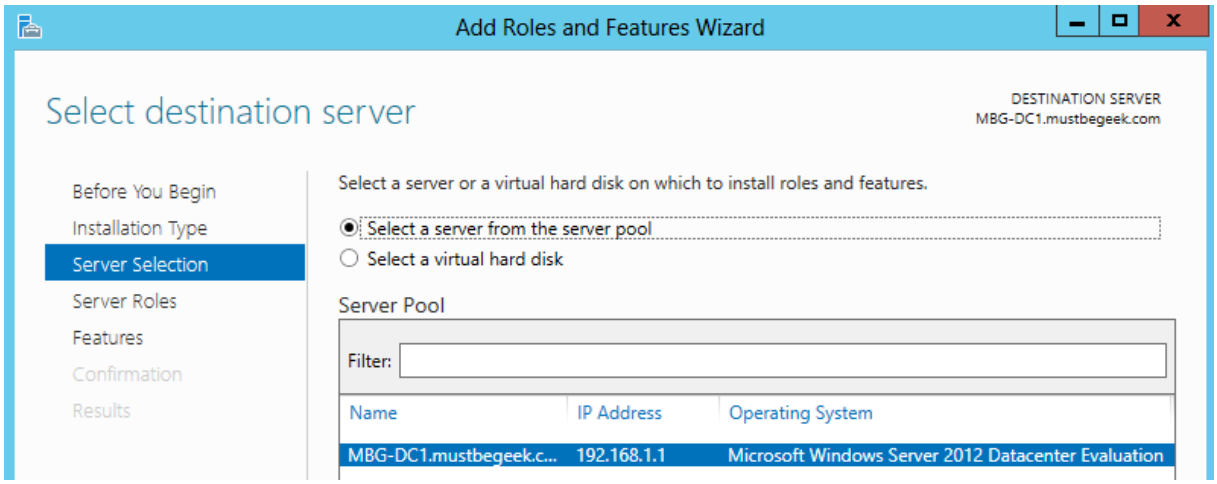
Tout d'abord, installez le rôle de serveur FTP. Dans Server2012. Alors, commençons. Ouvrez le **Gestionnaire de serveur.** Dans le menu, cliquez sur **Gérer**, puis cliquez sur **Ajouter** des **rôles et fonctionnalités**



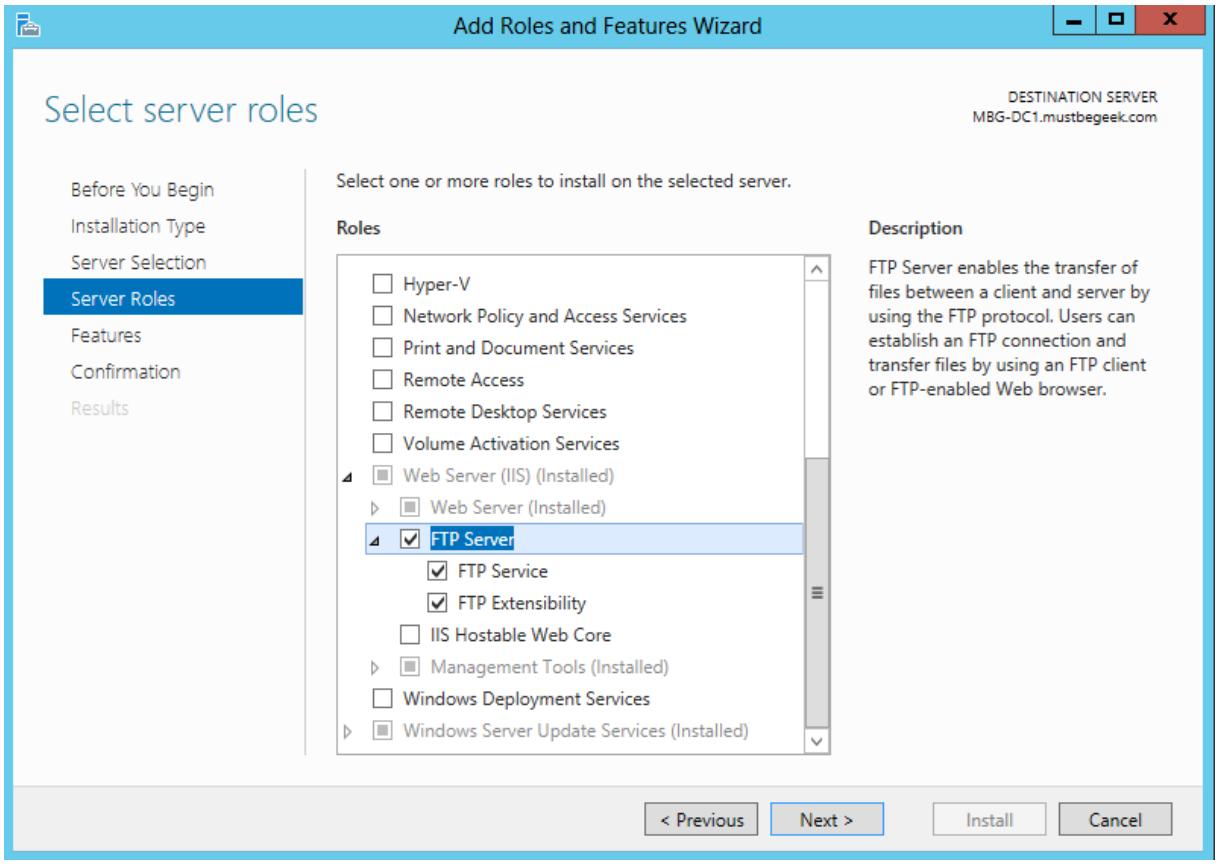
Cliquez sur **Suivant** fenêtre **Avant** de **commencer.** Cliquez sur l'installation en **fonction basée** sur les **rôles ou** la **fonctionnalité** et cliquez sur **Suivant.**



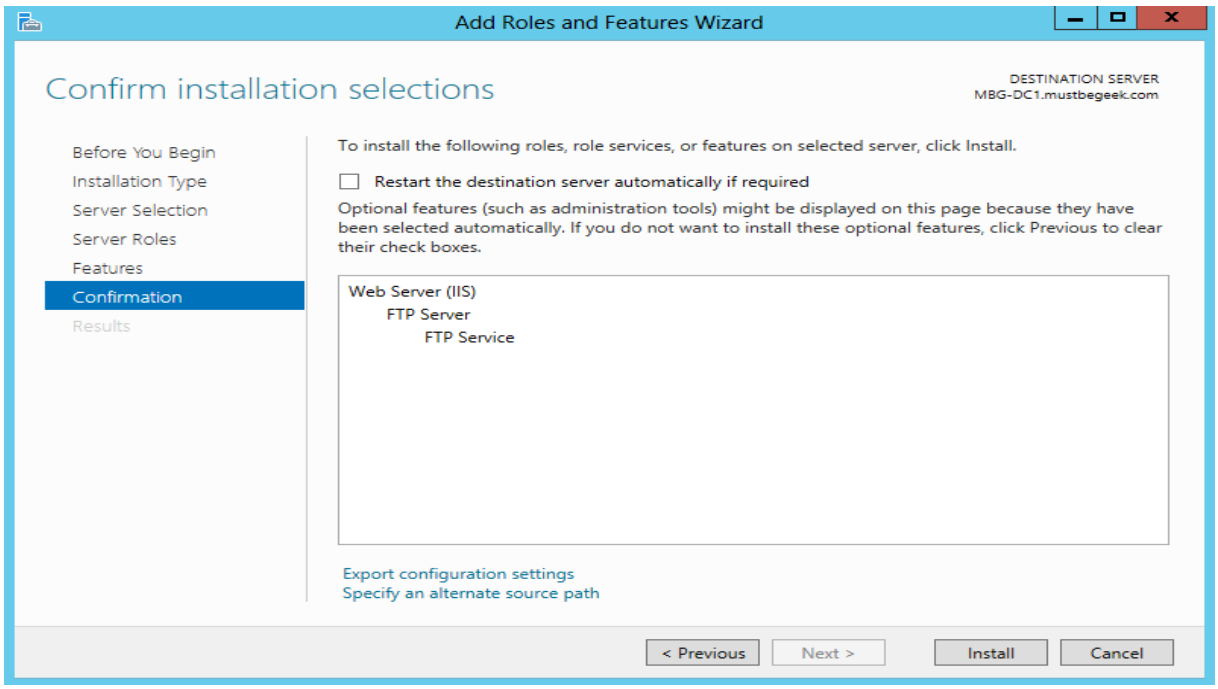
Sélectionnez le serveur et cliquez à nouveau sur Suivant.



Maintenant, développez le **rôle serveur Web (IIS).** Sélectionnez le serveur **FTP** et cliquez sur **Suivant.**

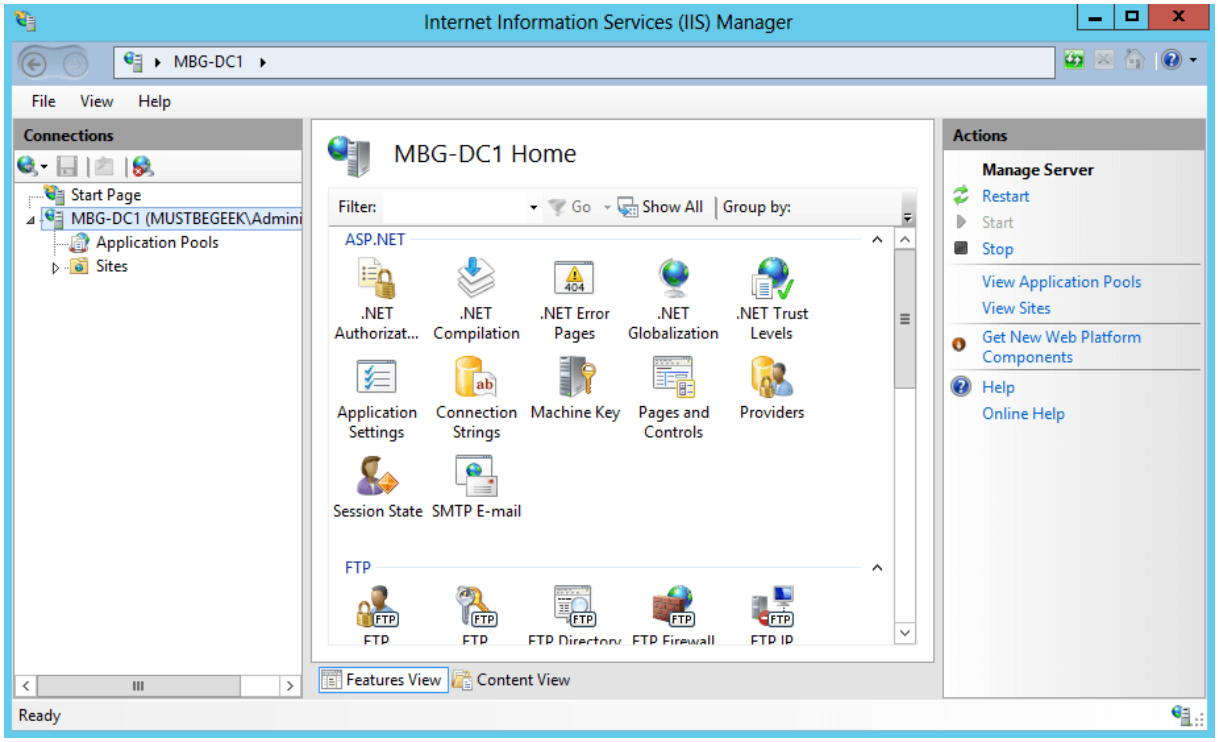


On n'a pas besoin d'ajouter des fonctionnalités, de sorte à nouveau sur **Suivant.** Cliquez sur Terminer dans la fenêtre de confirmation

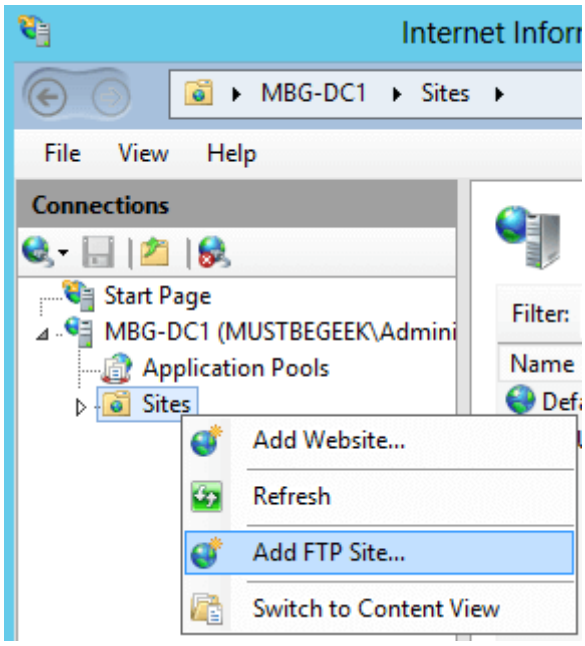


Application et résultats de la simulation

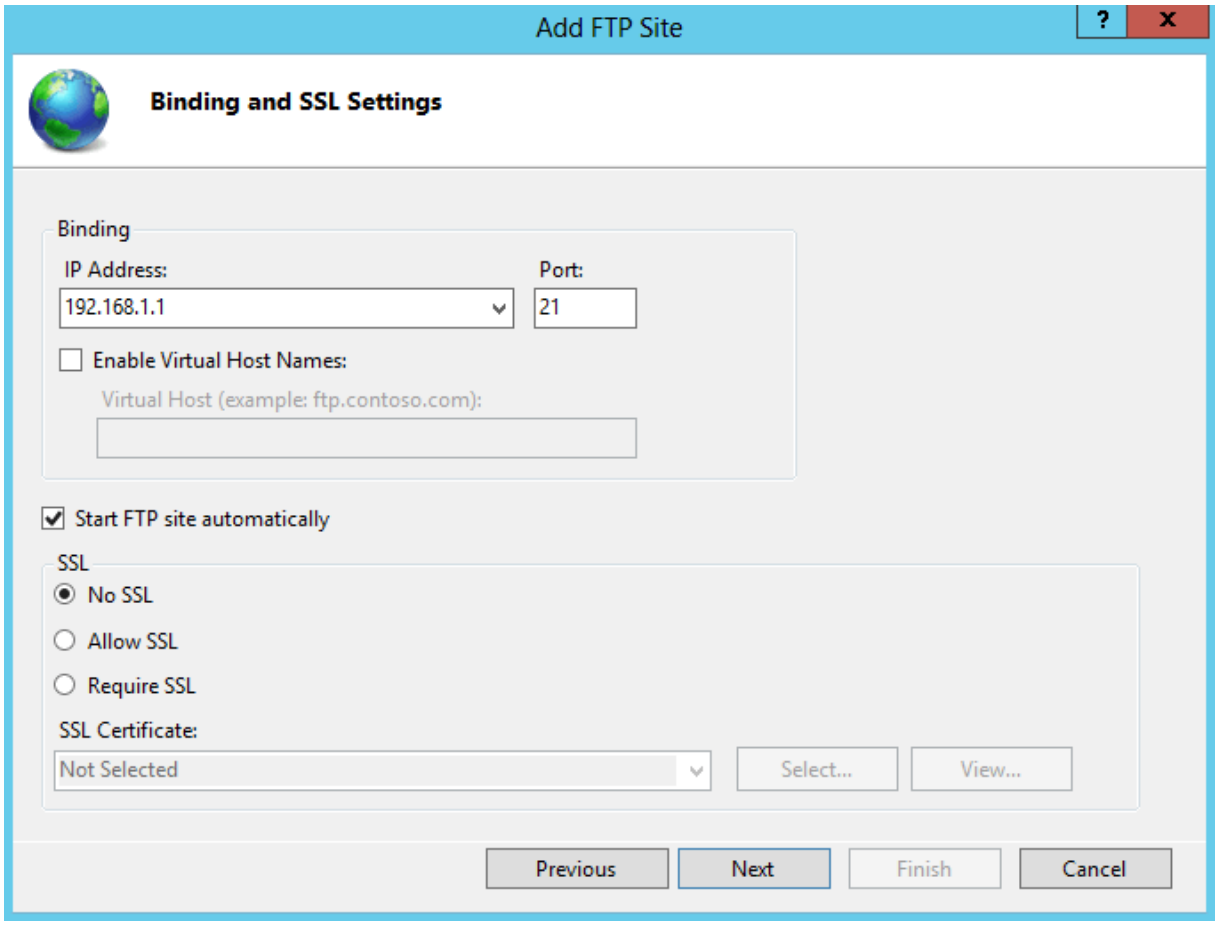
Après avoir installé **FTP** rôle **de serveur,** ouvrez la console **Internet Information Services (IIS).** Se connecter au serveur local. Développez le serveur local.



Faites un clic droit sites et cliquez sur **Ajouter** un **site FTP.**

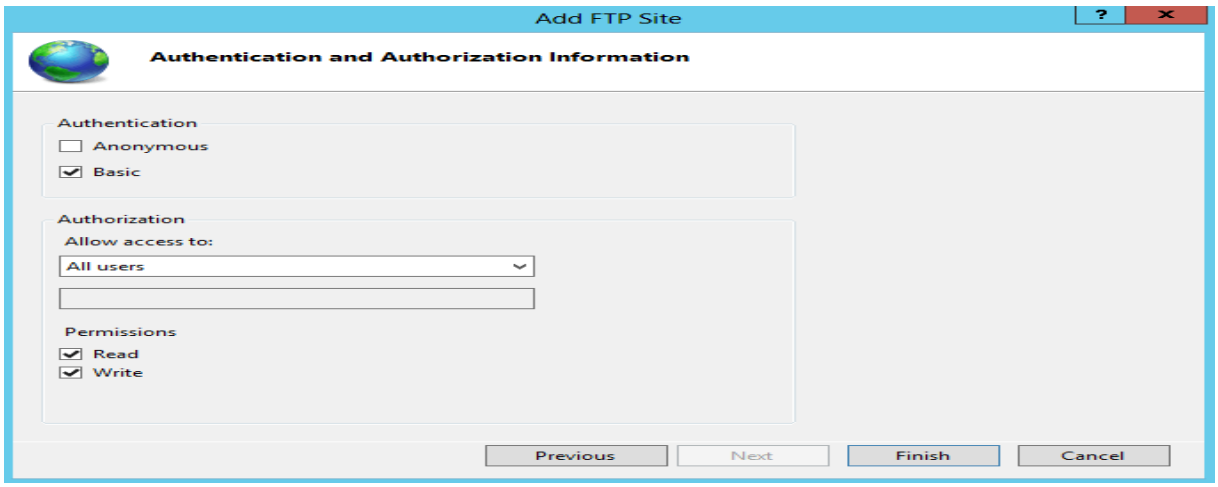


Consultez le **site FTP de démarrage automatique.** Choisissez **Non SSL** et cliquez sur **Suivant.**

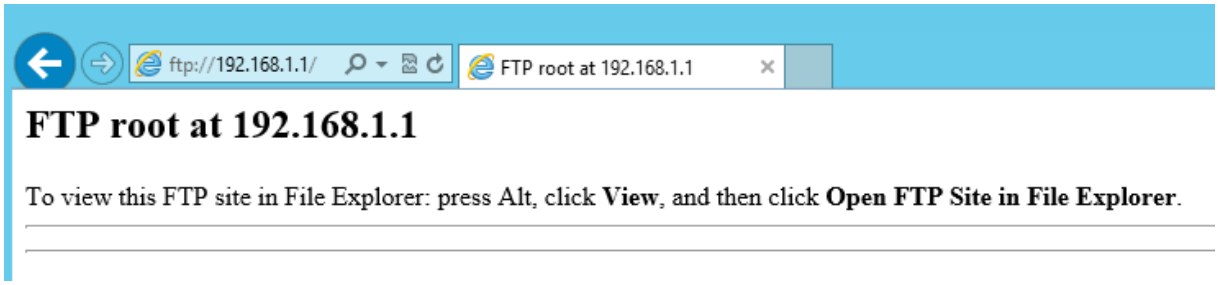


Choisissez **Basic**.

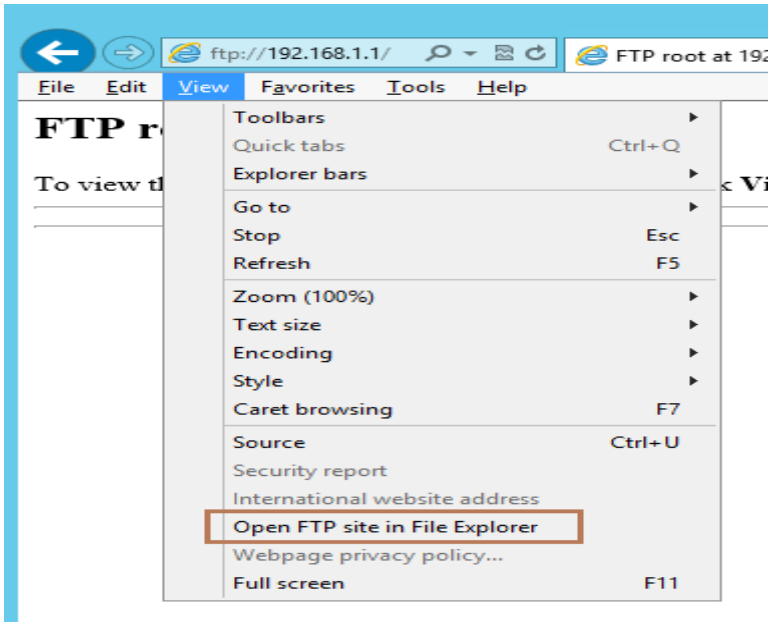
Sous **autorisation,** sélectionnez **tous** les **utilisateurs** pour permettre l'accès FTP à tous les utilisateurs du domaine. Vérifiez à la fois **lire** et **écrire** dans les **autorisations.**



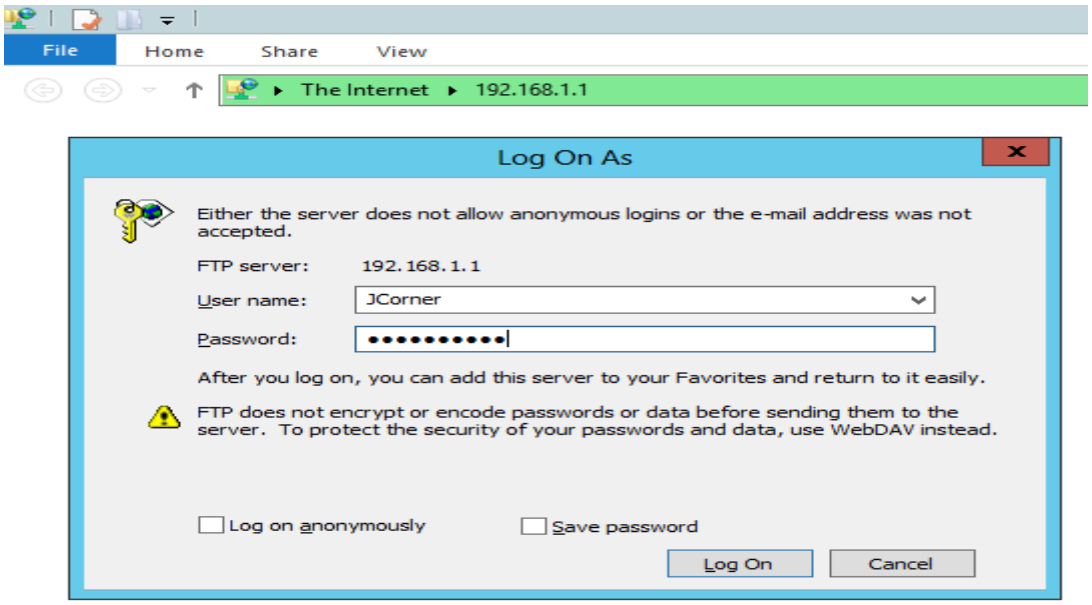
Maintenant parcourir le serveur FTP de la machine cliente. Tapez l'adresse IP sur le navigateur comme ***ftp://192.168.1.1/.*** Il montrera la page suivante



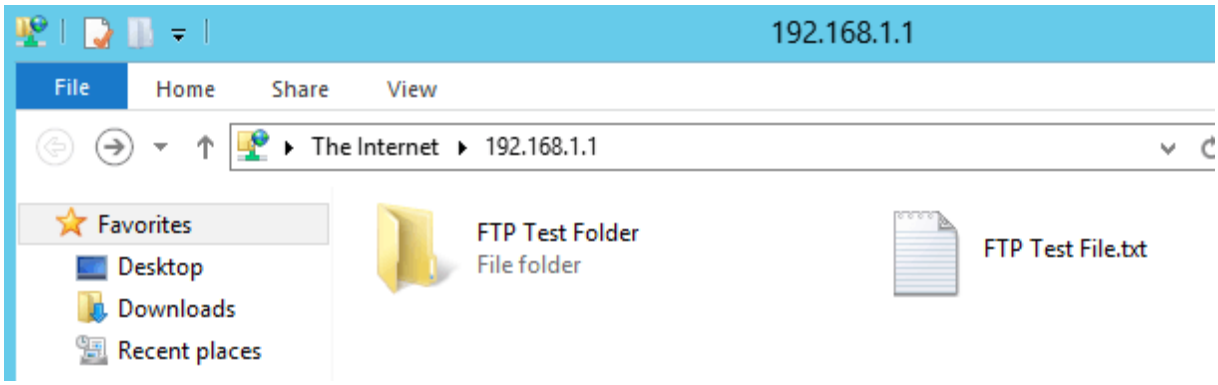
Maintenant, appuyez sur la touche **ALT** de votre clavier qui montrera la barre de menu. Ensuite, cliquez sur **Affichage** et cliquez sur **site FTP Ouvrir dans** l'Explorateur **de fichiers.**



Entrez le nom d'utilisateur et mot de passe qui a été créé dans Utilisateurs et ordinateurs AD. Puis cliquez **sur Connexion.**



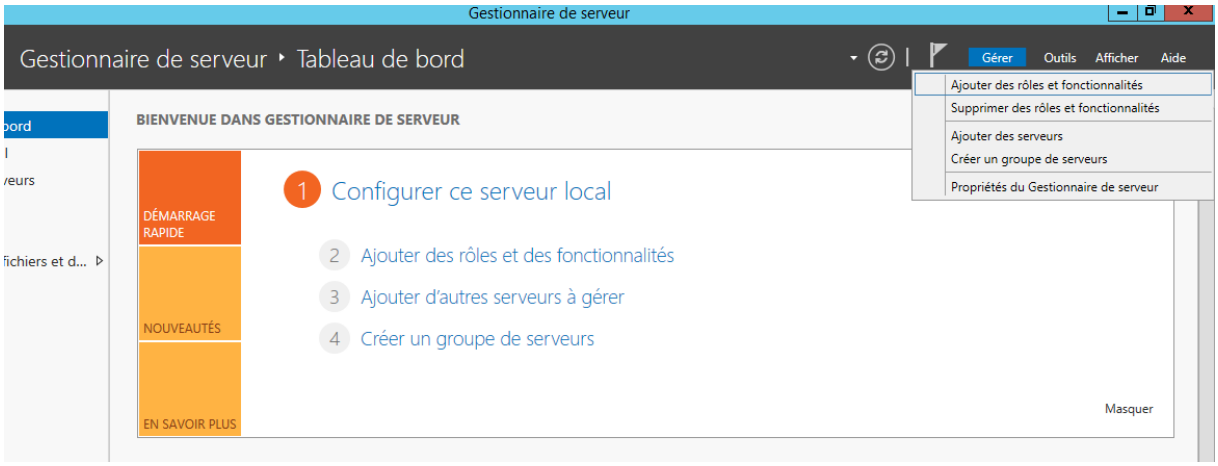
Après avoir cliqué sur le bouton de connexion, vous pouvez voir les fichiers sur le serveur FTP.



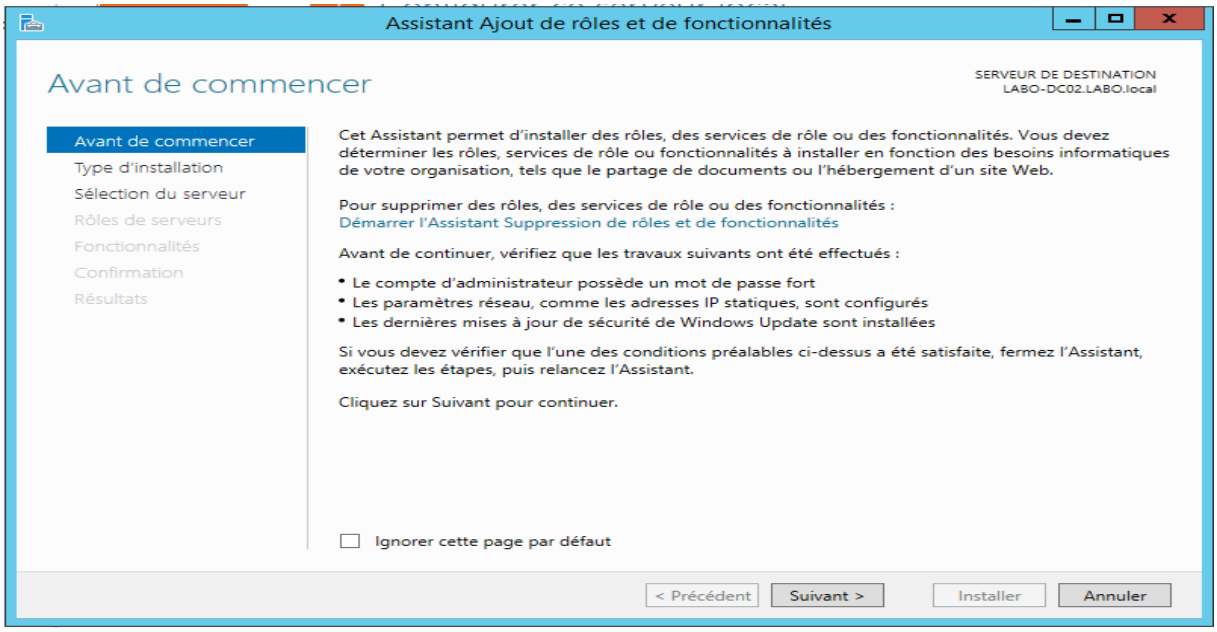
3. Configuration du serveur Radius :

- **Installation du rôle NPS**

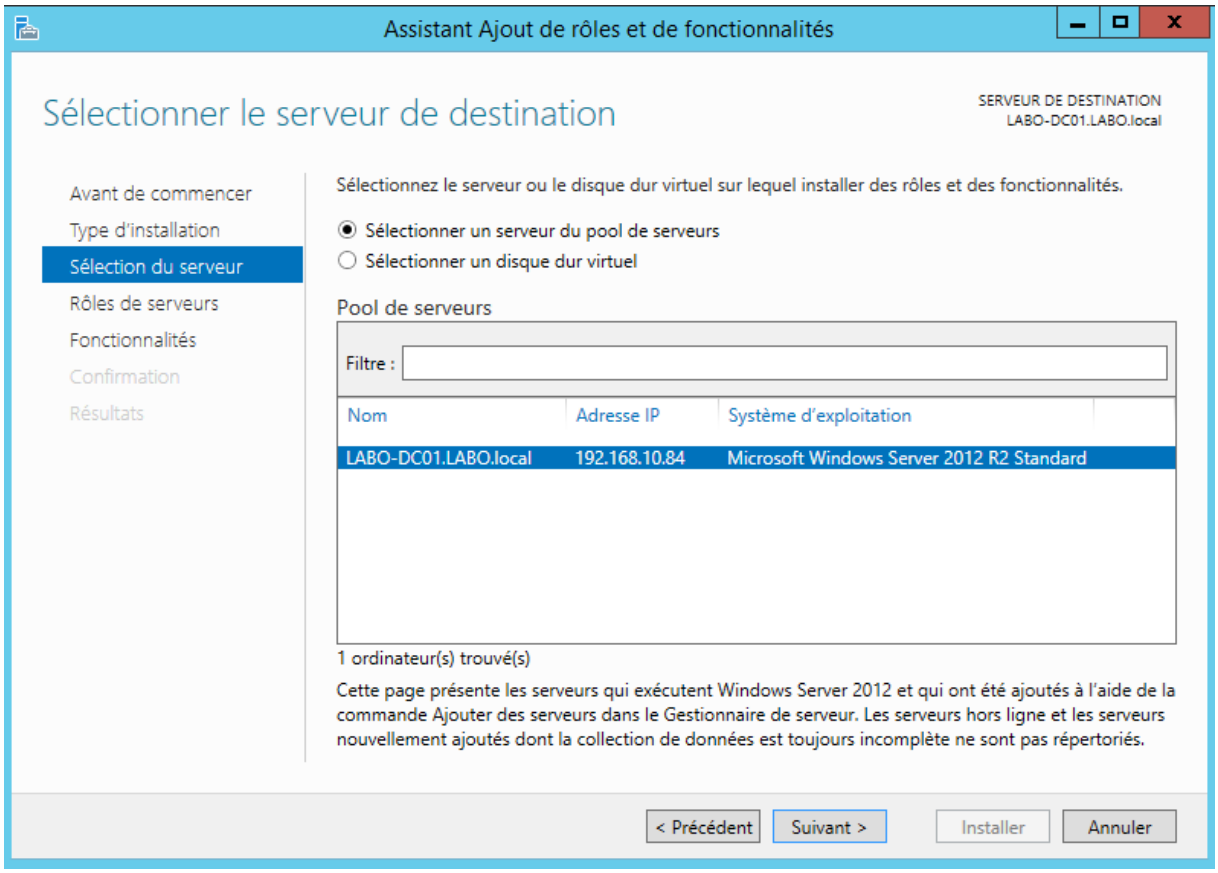
Ouvrir le gestionnaire de serveur-gérer-ajouter des rôles et fonctionnalités



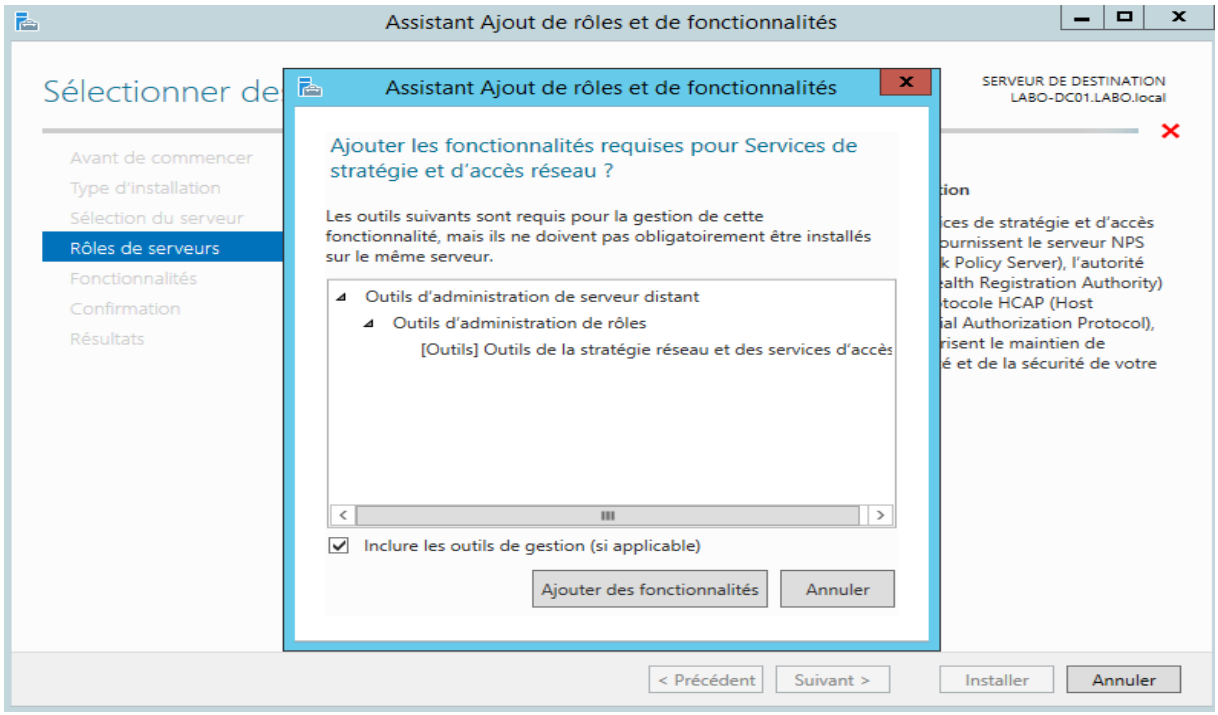
Cliquer sur suivant, Cocher Installation basée sur un rôle ou une fonctionnalité
Cliquer sur Suivant.



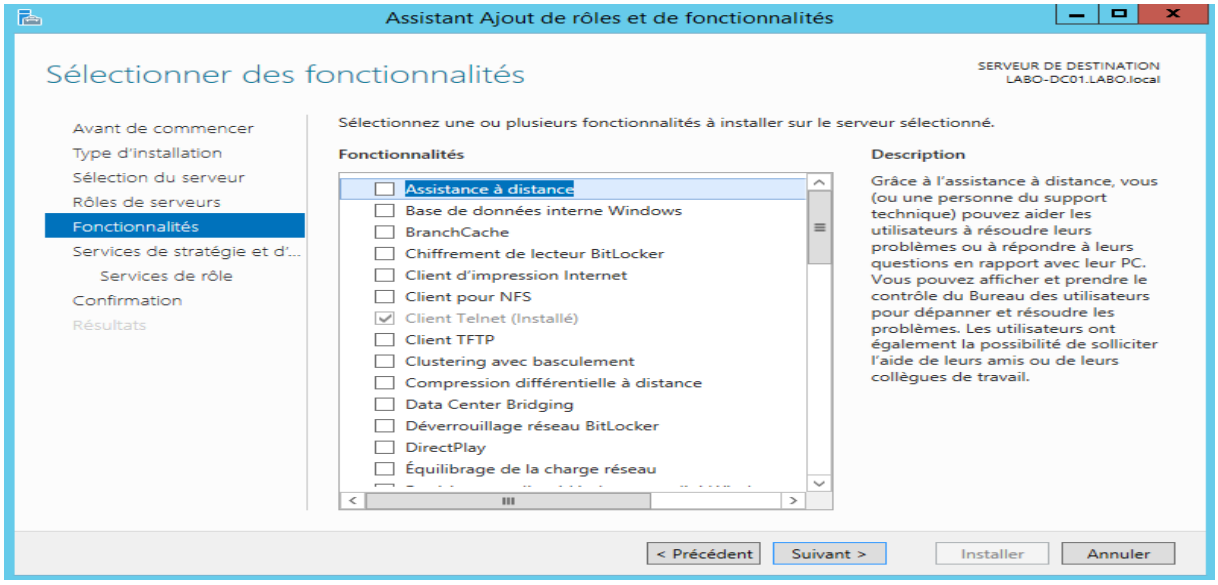
Cocher : Sélectionner un serveur du pool de serveurs
Sélectionner le serveur sur lequel vous voulez installer le rôle NPS
Cliquer sur Suivant



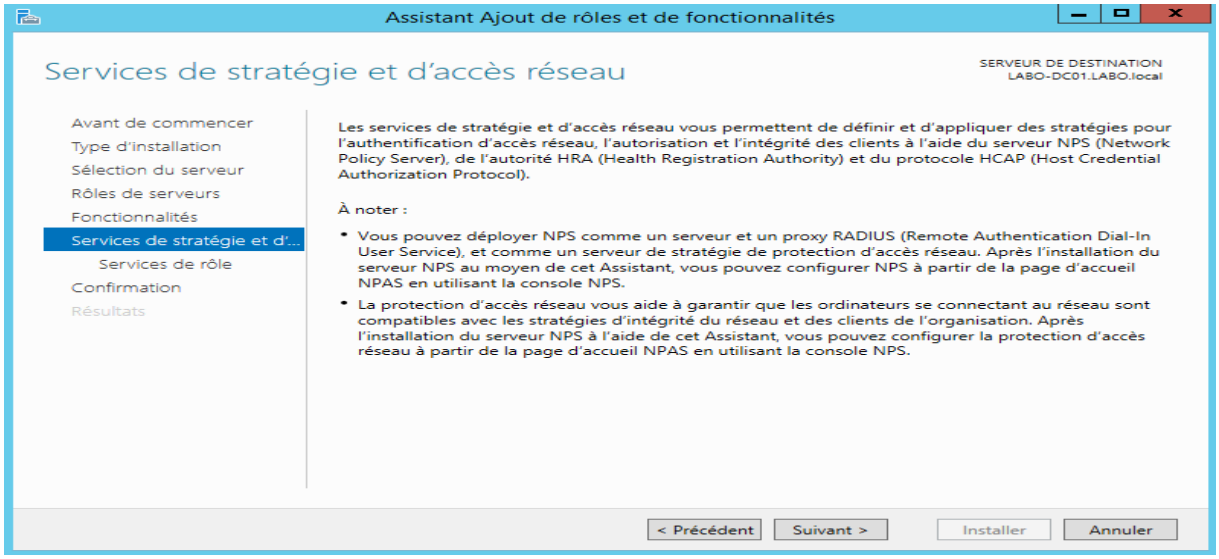
Cocher : Service de stratégie et d'accès réseau
Cliquer sur Ajouter des fonctionnalités
Cliquer sur Suivant



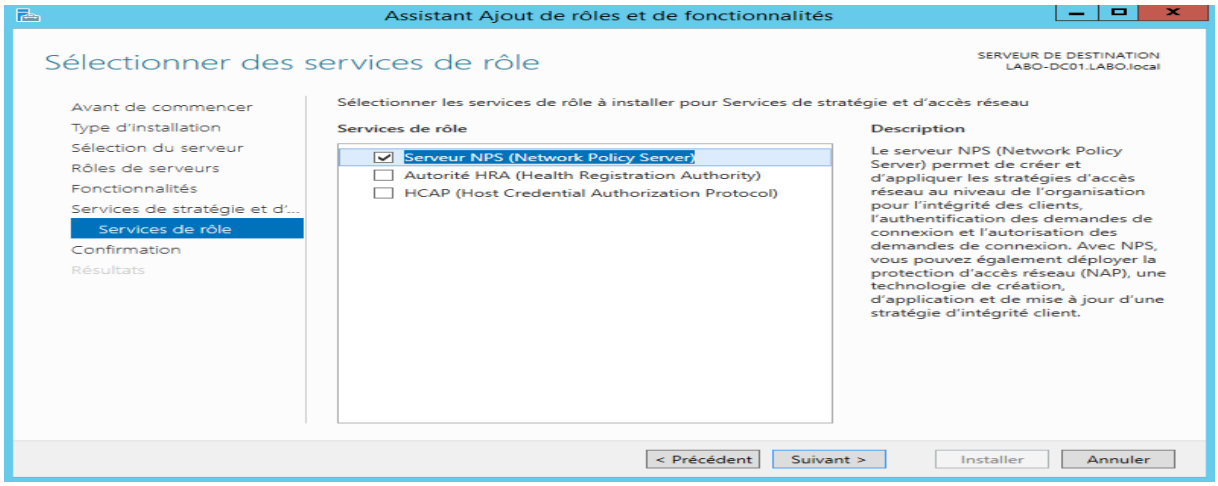
Cliquer sur Suivant



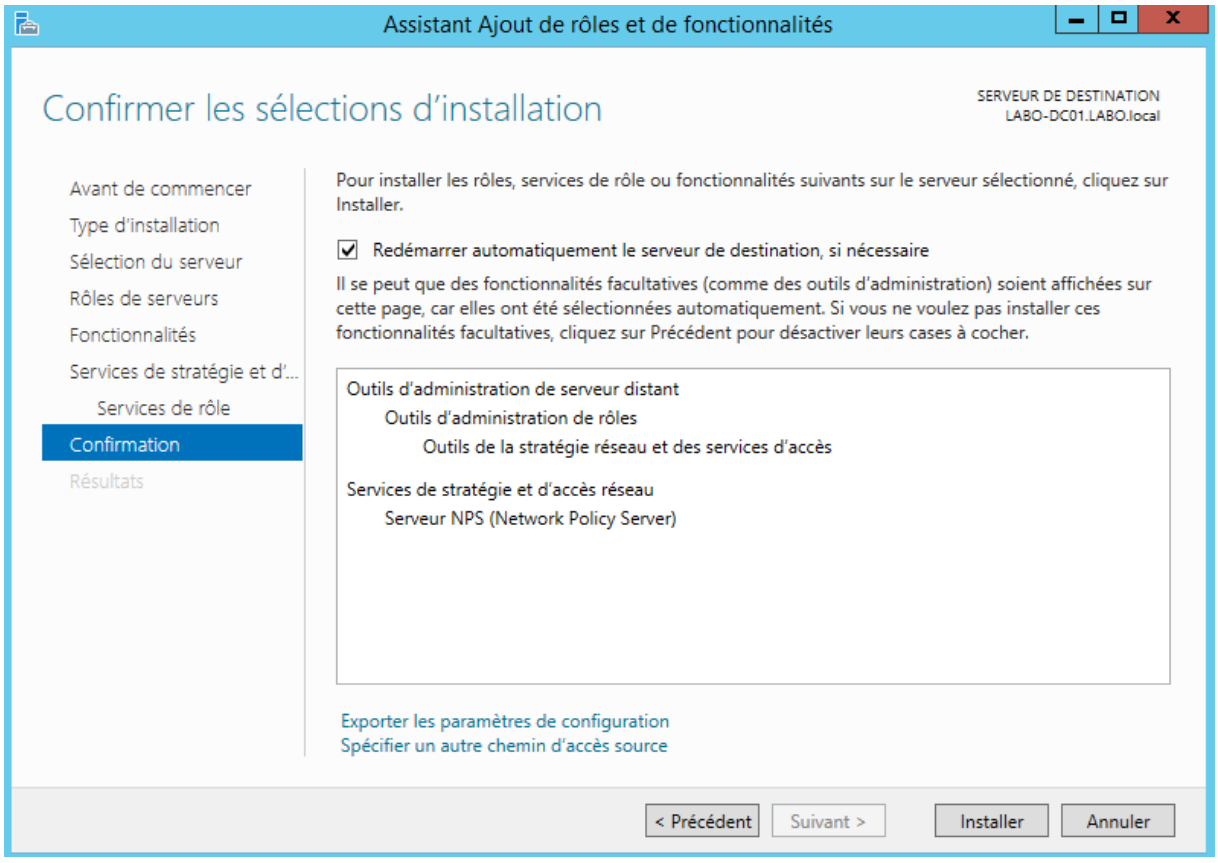
Cliquer sur Suivant



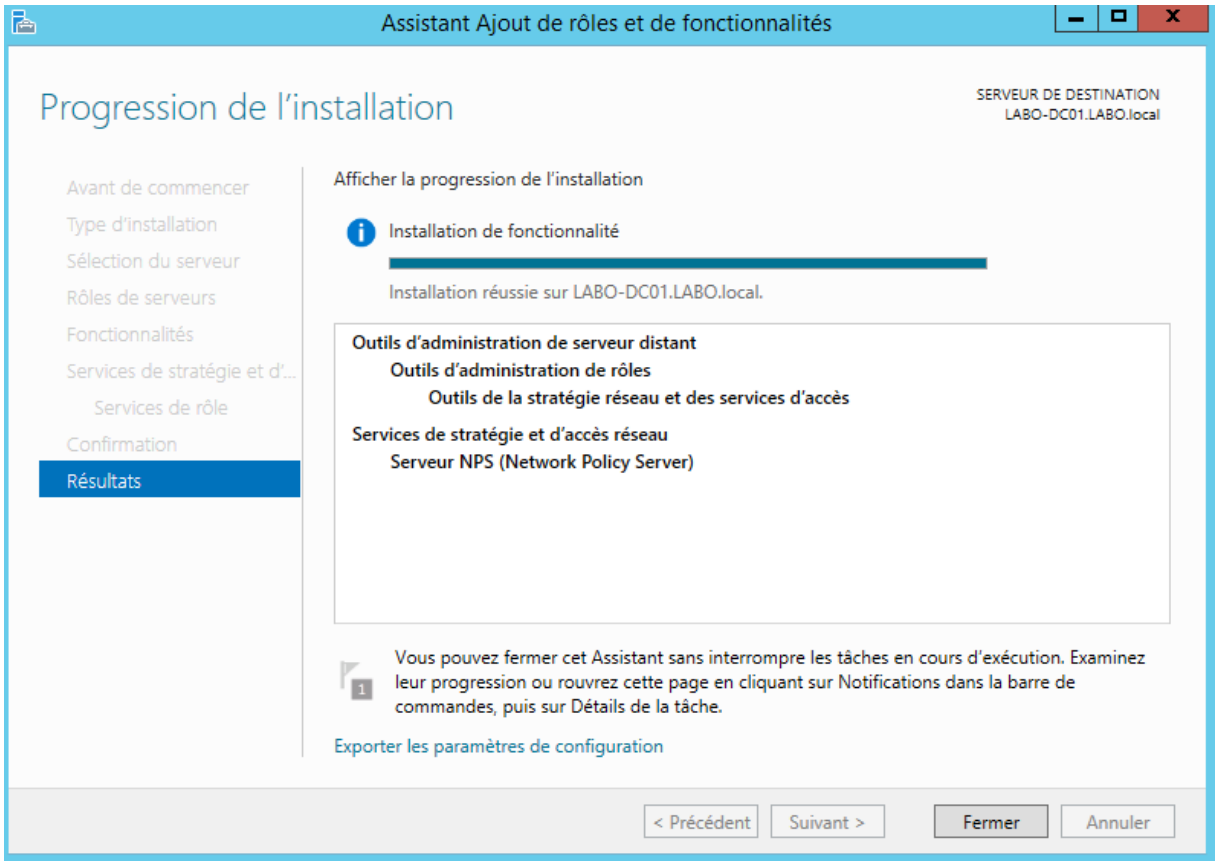
Cocher : Serveur NPS (Network Policy Server)
Cliquer sur Suivant



Cocher : Redémarrer automatiquement le serveur de destination, si nécessaire (suivant vos impératifs)
Cliquer sur Installer

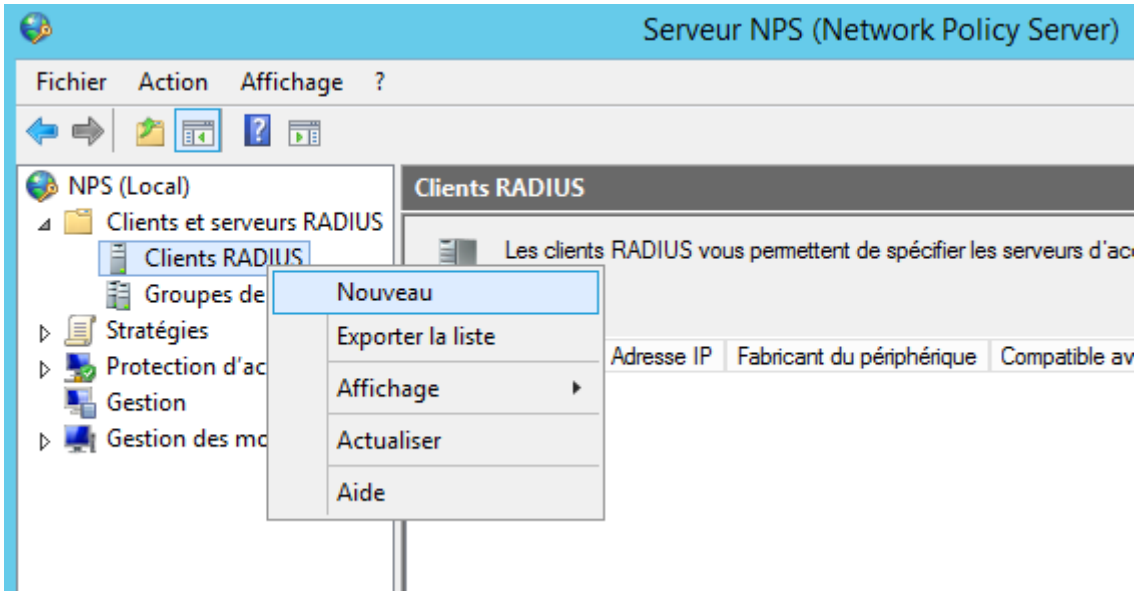


Cliquer sur Fermer

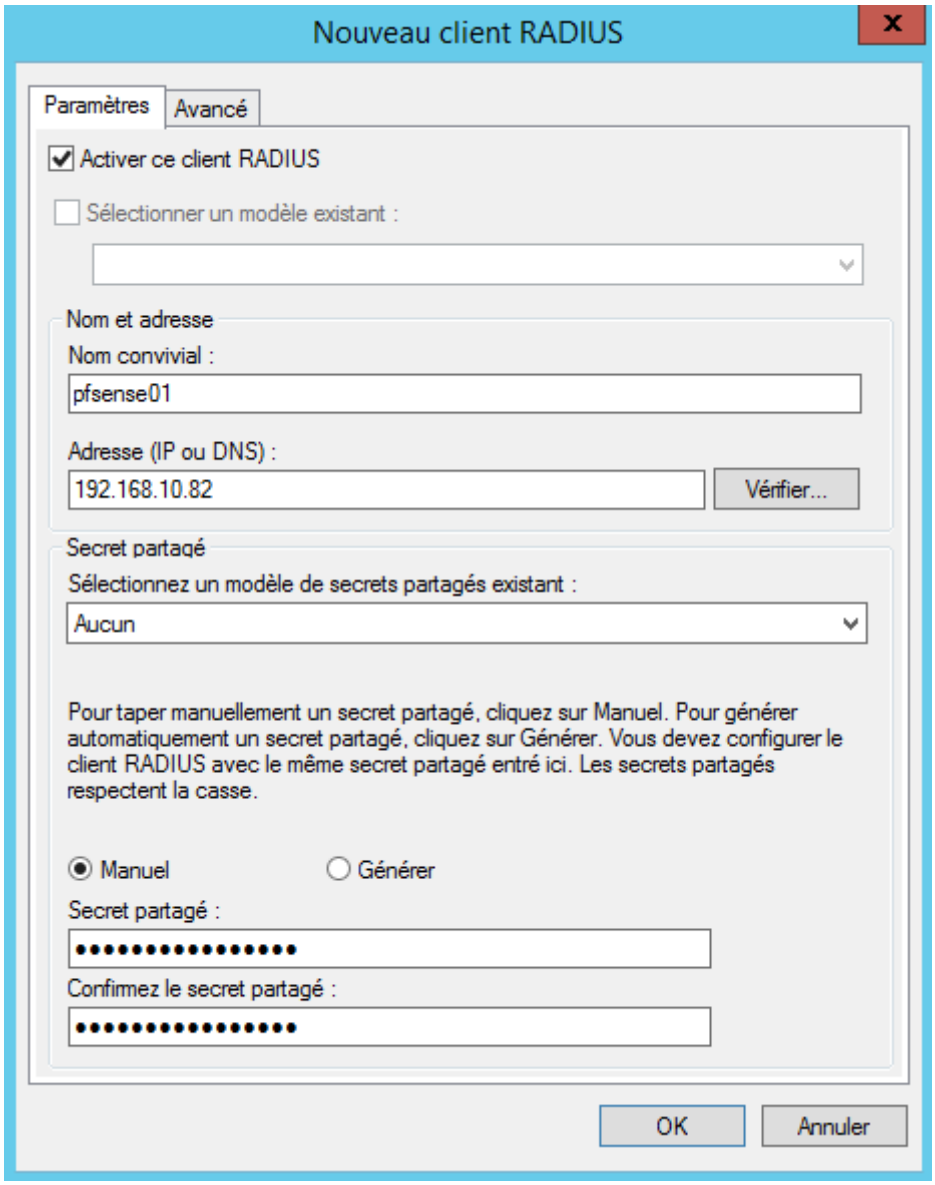


➢ **Ajout d'un nouveau client Radius :**

Panneau de configuration - Outils d'administration - Serveur NPS (Network Policy Server)



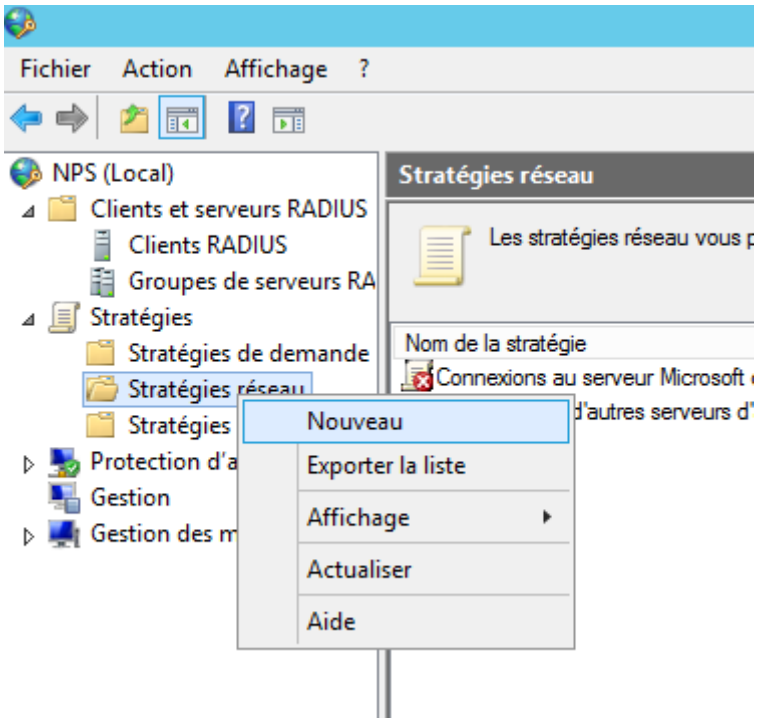
Clients et serveurs RADIUS - Clients RADIUS – Nouveau



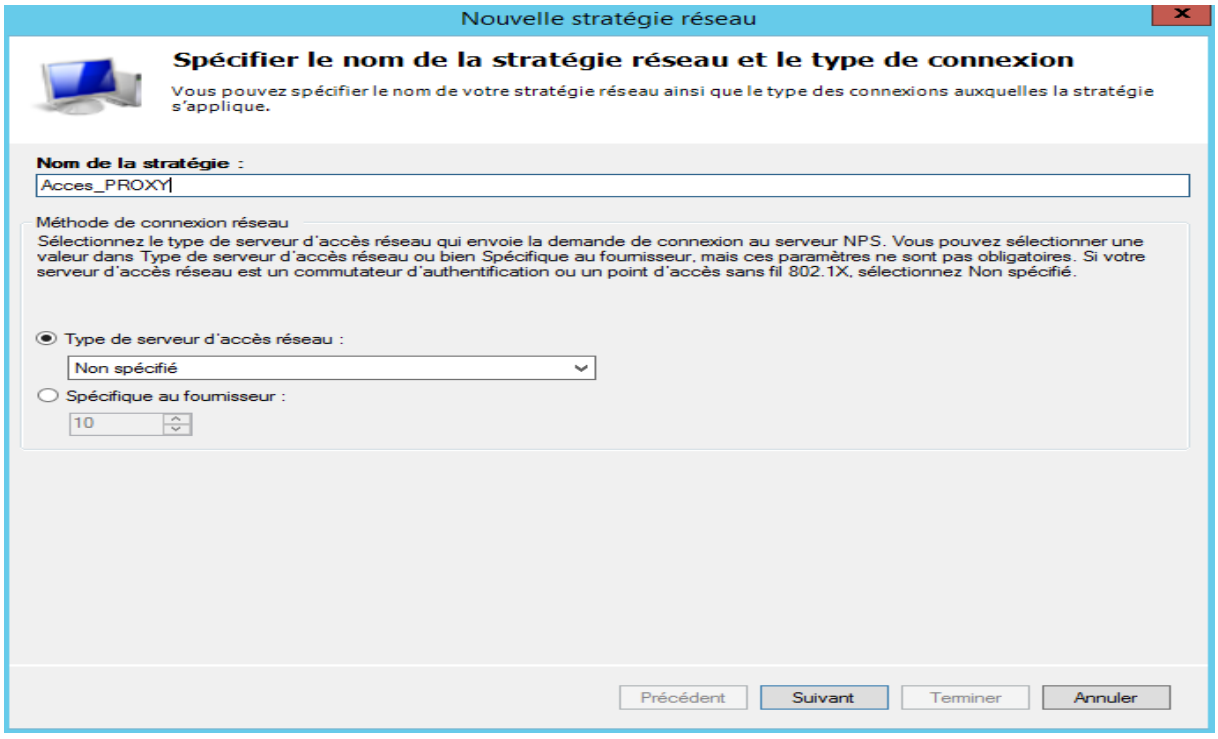
Cocher : Activer ce client RADIUS
Nom convivial : Nom pour identifier le client
Adresse (IP ou DNS) : Saisir l'IP du client ou son nom DNS (le serveur NPS doit pouvoir le résoudre)
Secret partagé : Indiquer un code qui sera partagé par le client et le serveur RADIUS
Cliquer sur OK.

- **Création d'une nouvelle stratégie :**

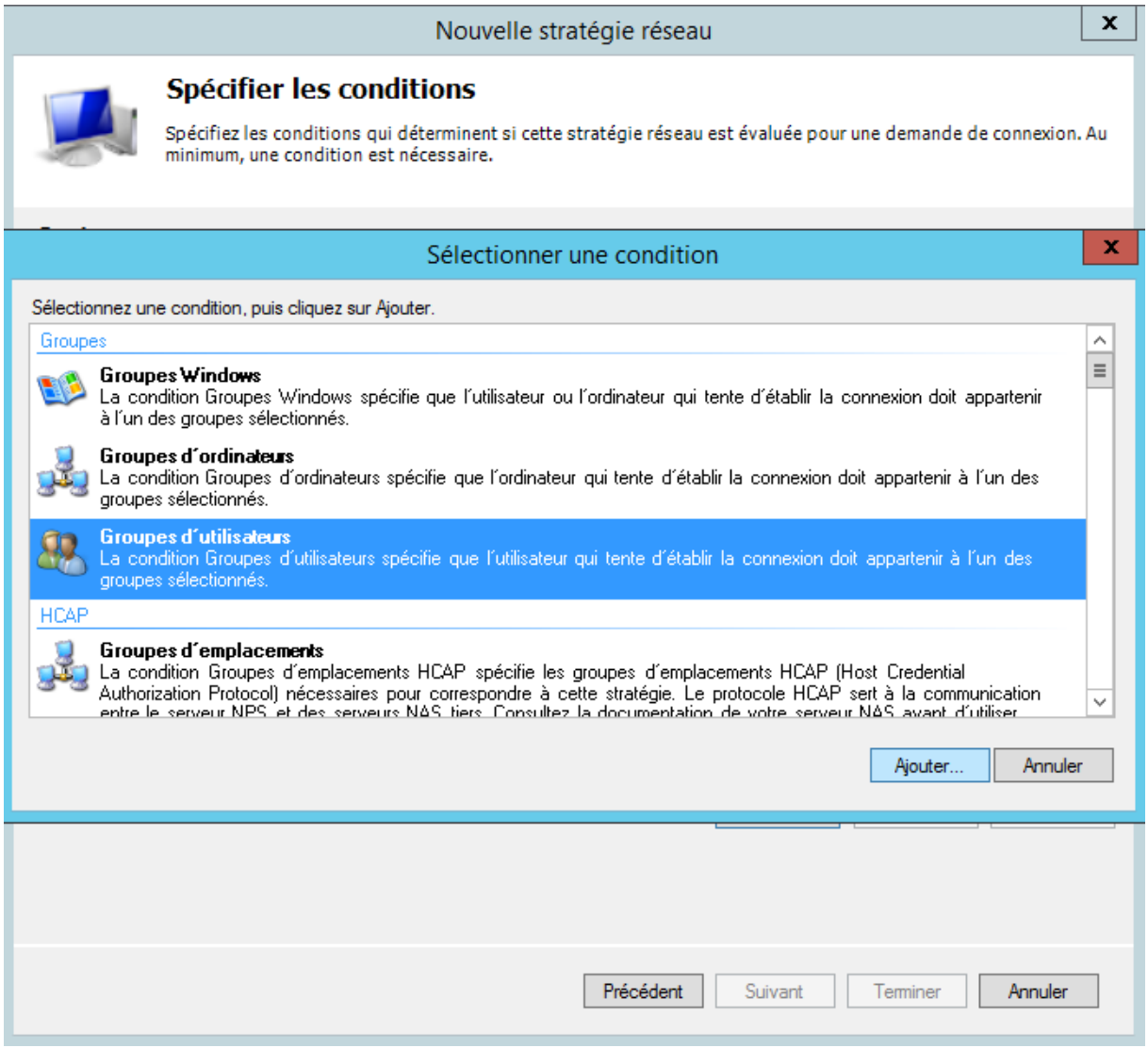
Dans mon exemple, je vais autoriser un groupe de sécurité à s'authentifié sur le serveur Radius NPS (local) - Stratégies - Stratégies réseau - Cliquer droit Nouveau



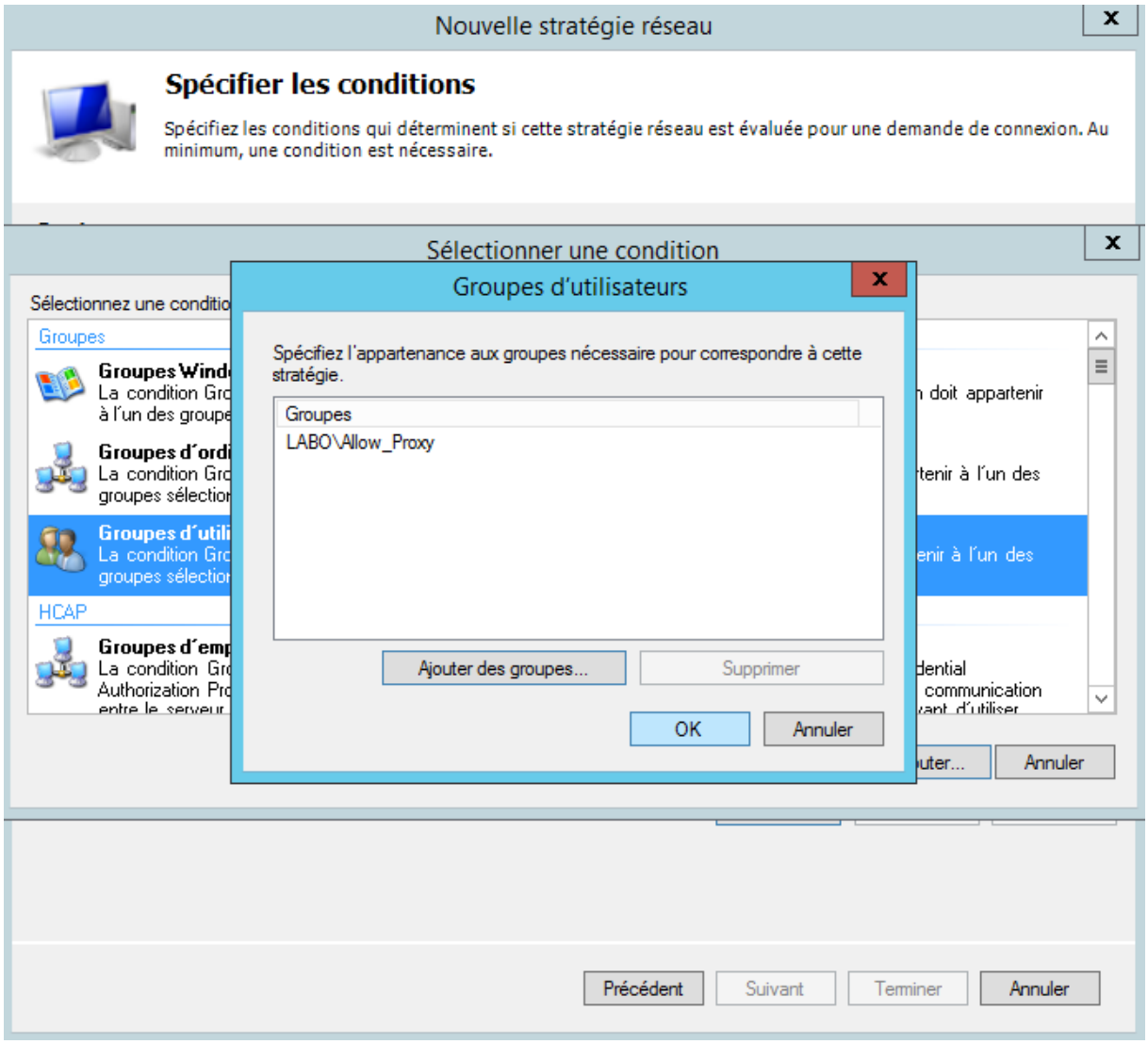
Nom de la stratégie : Indiquer le nom de votre stratégie
Cliquer sur Suivant



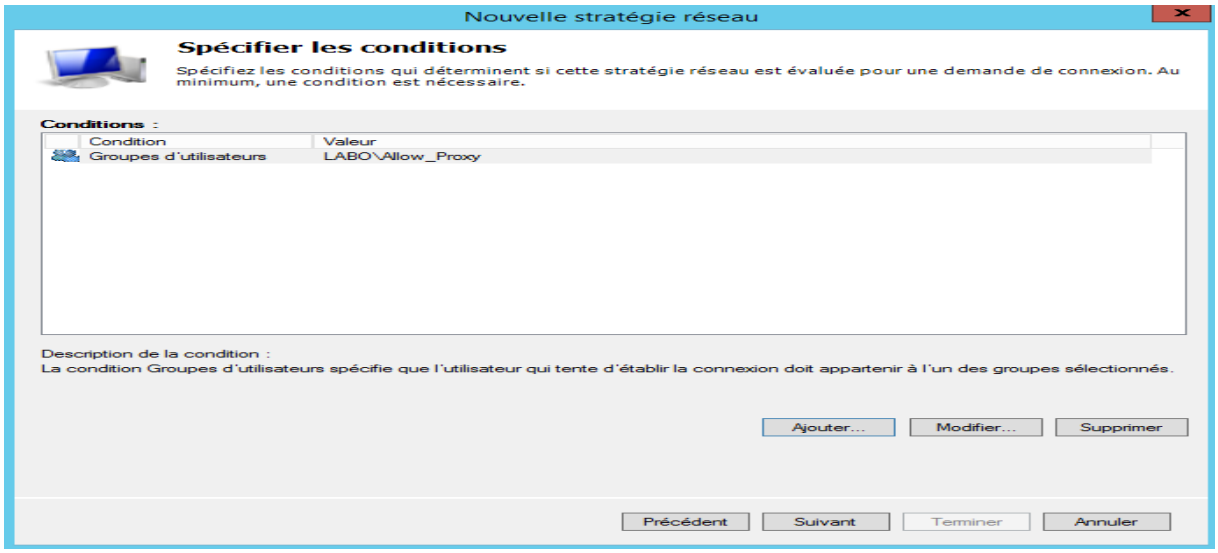
Sélectionner Groupes d'utilisateurs
Cliquer sur Ajouter



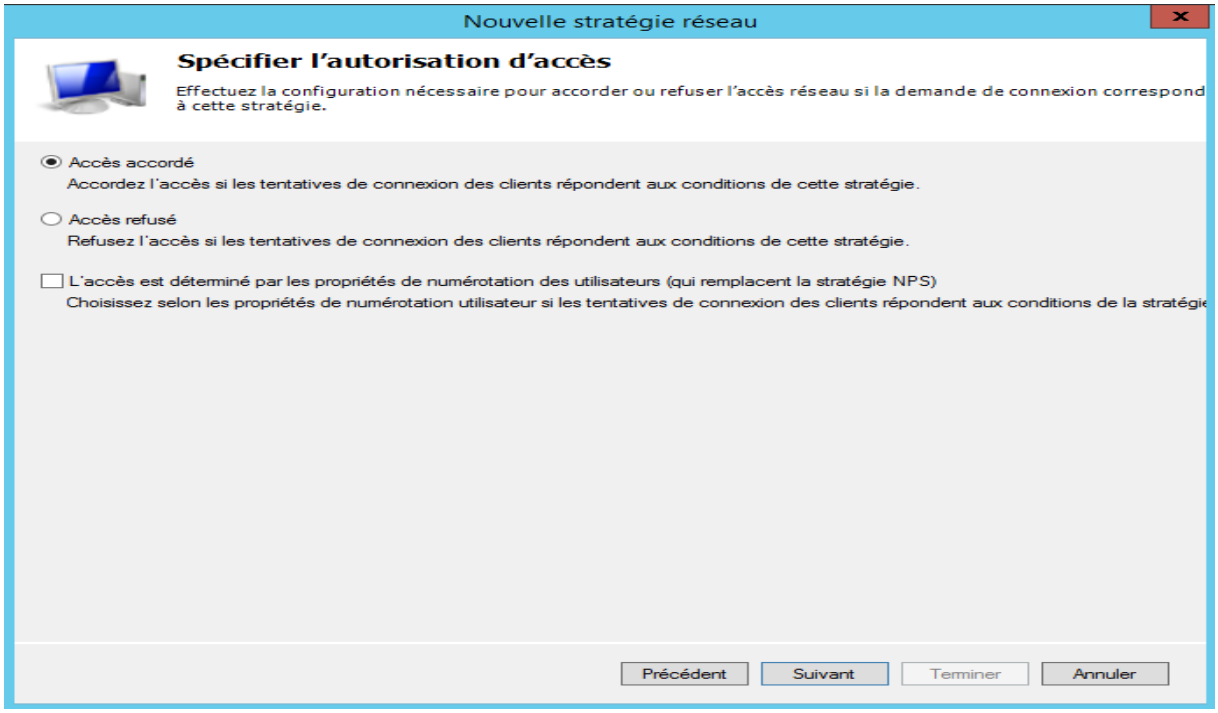
Cliquer sur ajouter des Groupes
Sélectionner vos groupes
Valider en cliquant sur OK



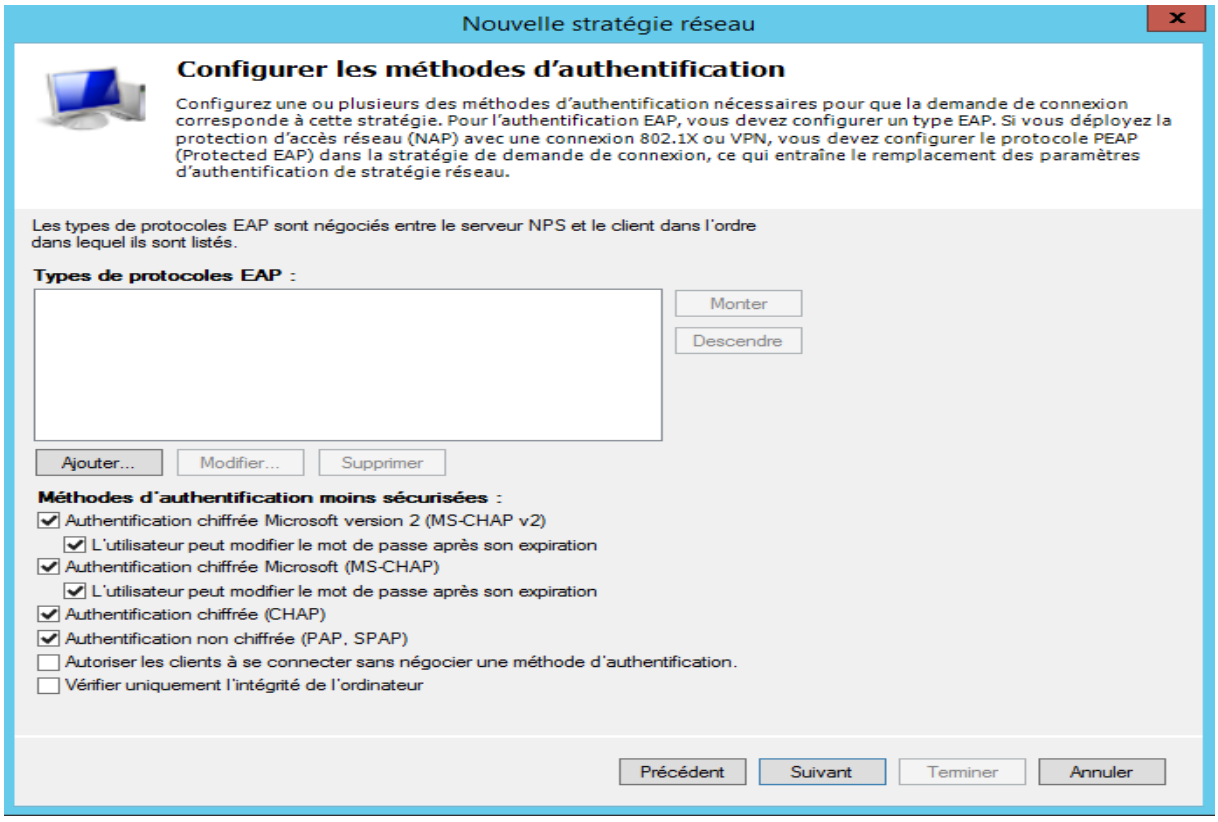
Cliquer sur Ajouter si vous désirez ajouter des conditions, pour mon exemple je n'en rajouterai pas
Cliquer sur Suivant



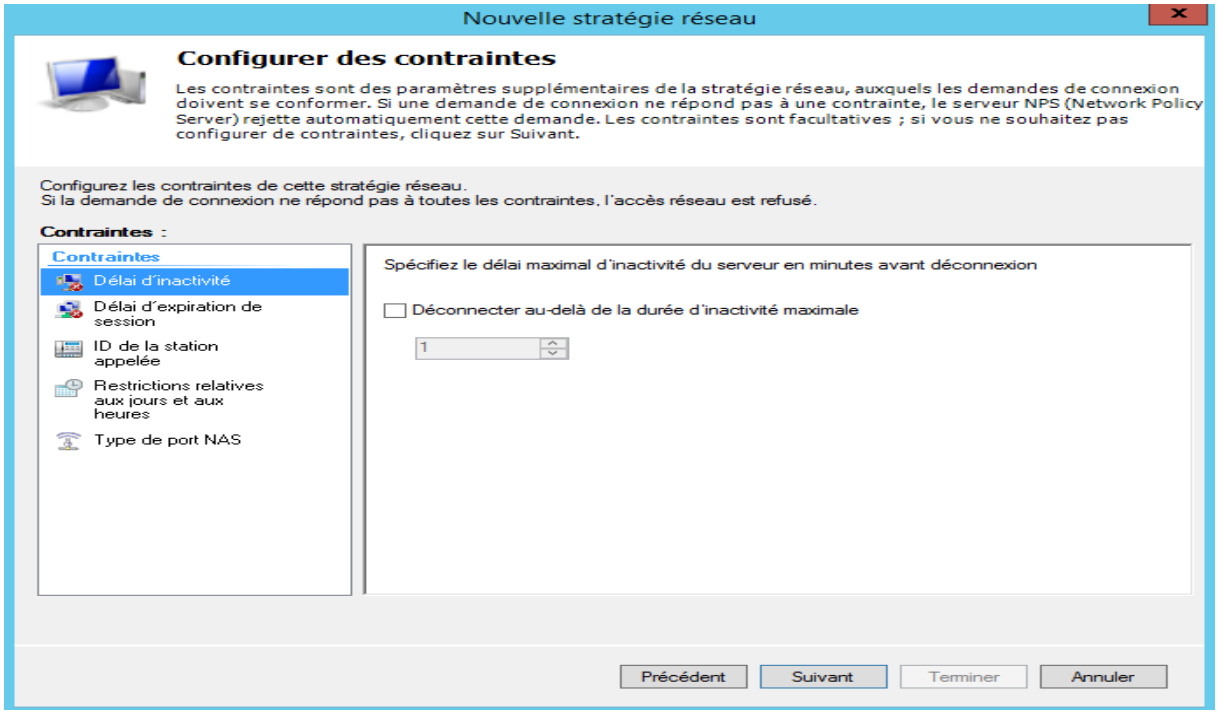
Cocher : Accès accordé
Cliquer sur Suivant



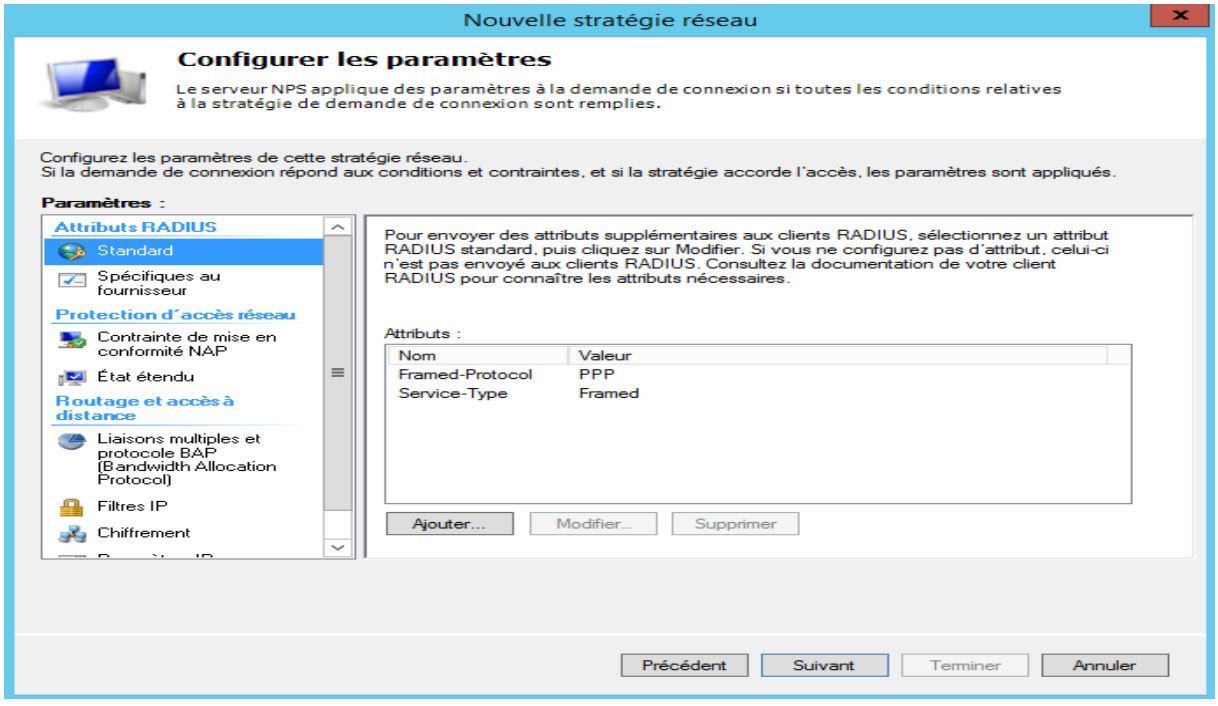
Cocher comme ma Capture d'écran
Cliquer sur Suivant



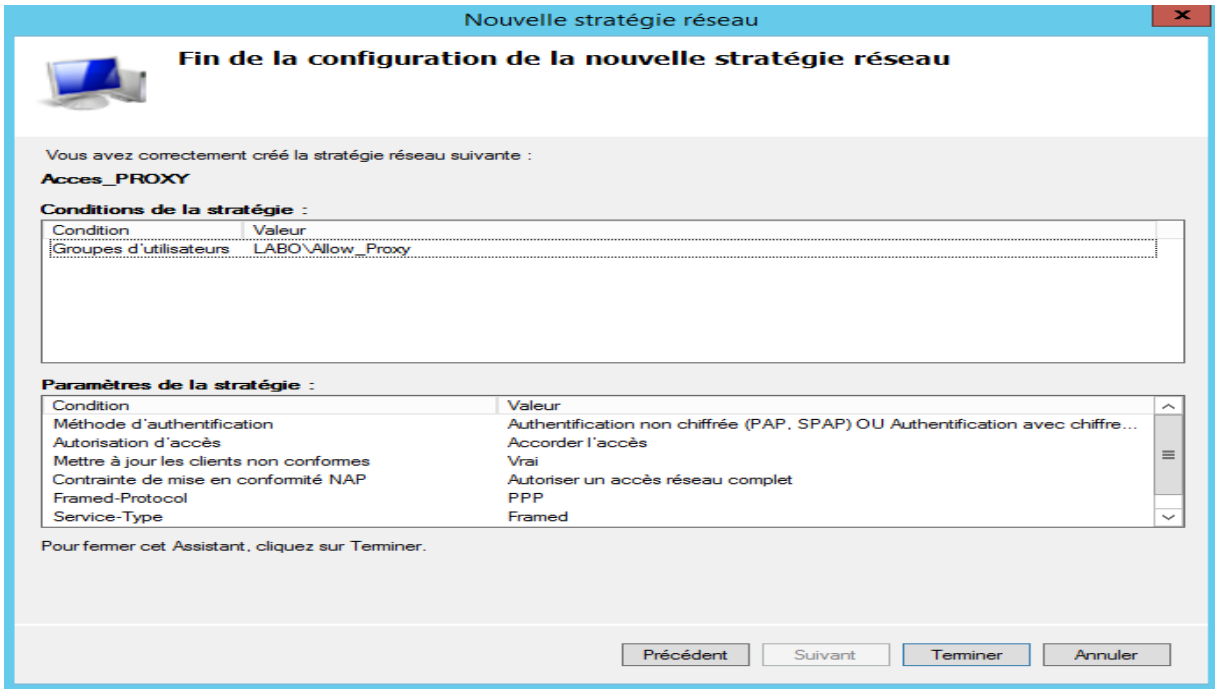
Cliquer sur Suivant



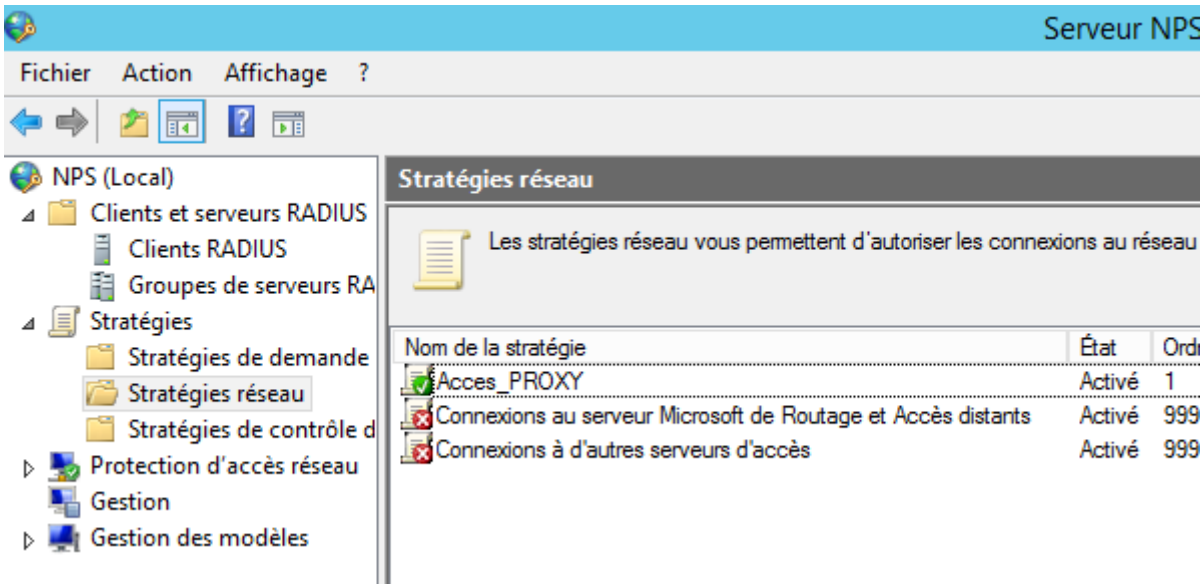
Cliquer sur Suivant



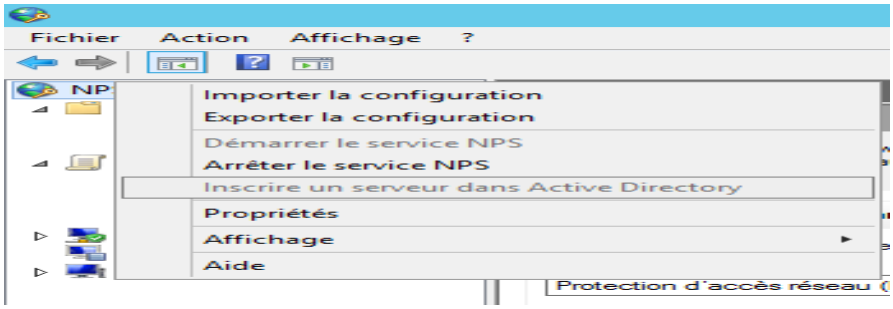
Cliquer sur Terminer



La nouvelle stratégie est bien créée



Pour finir la configuration, on inscrit le serveur NPS dans le domaine Active Directory



4. PARTIE SIMULATION :

Pour la protection contre les attaques, nous avons opté pour utiliser le logiciel de simulation pakcet–tracer.

4.1. Le logiciel « PACKET TRACER »

➢ **Définition** :

Packet tracer est un logiciel fournit par Cisco, il nous permet de concevoir, configurer et simuler des réseaux.

Il nécessite pour son fonctionnement le matériel suivant :

- ✓ Intel pentium 200 MHZ
- ✓ 64 MB de RAM
- ✓ 30 MB de disque dur

➢ **Technologie et protocole supportés :**

Il supporte toute sorte de câbles (câble série, faste Ethernet, gigabit Ethernet, fibre optique) ainsi que les technologies suivante : VLAN, DHCP, ACL, comme il introduit les couches du modèle OSI lors de l'acheminement du paquet. Il supporte les équipements suivants :PC , routeur , Switch , point d'accès ,hub ,nuage ,pont ,serveur ,imprimante , répétiteur.

Quand on lance Packet Tracer,

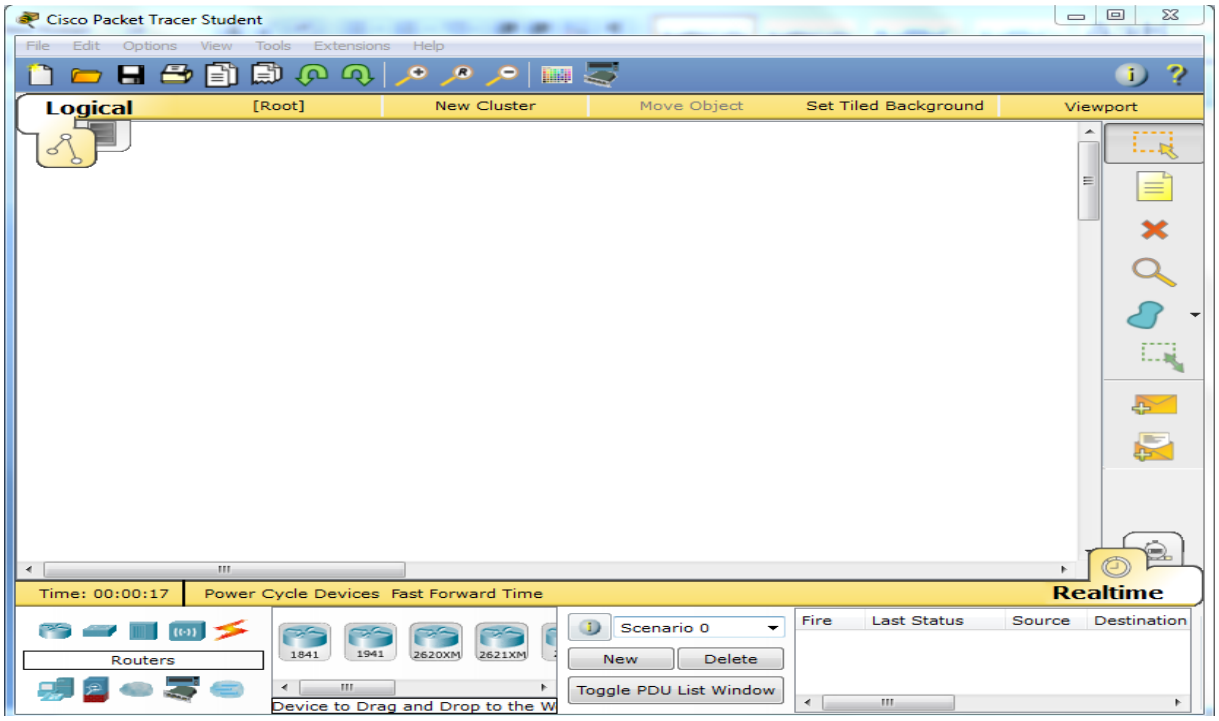


Figure 24 : la page principale du logiciel

Les éléments de sa barre d'outils sont :

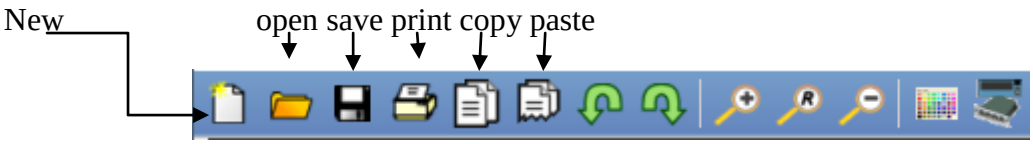


Figure 25 : Barre d'outils

Les icones des différents éléments à utiliser pour créer le réseau se trouvent dans l'emplacement que la figure montre et il suffit juste de cliquer sur l'un de ces éléments et lui faire glisser sur l'espace réservé pour créer le réseau.

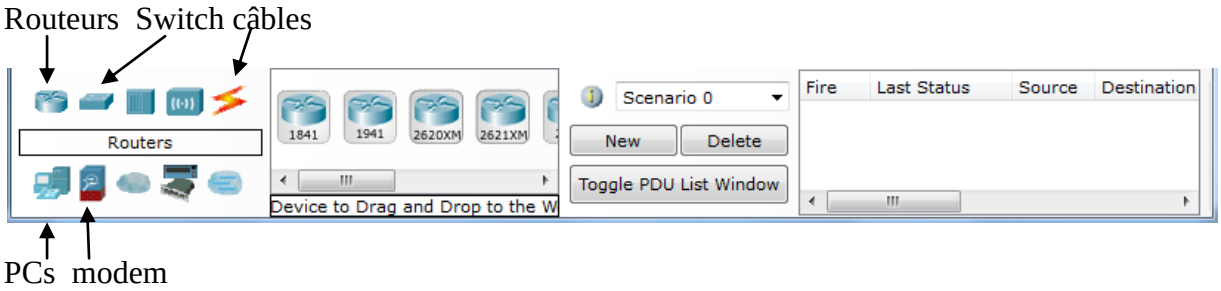


Figure 26 : barre des équipements réseau

- **Mode de packet tracer** :

Mode topologie :

Pour créer un réseau. Ce mode introduit les types de connexions suivantes :

✓ Cooper straight-through: C'est un standard Ethernet pour connecter différents équipements

Exemple :

Hub-----→routeur

Switch---→pc

Routeur--→hub

La connexion peut être réaliser par les ports suivants : 10 MBS Copper(Ethernet) ,100 MBS Copper (faste Ethernet) et 1000 MBS Copeer(GB Ethernet).

✓ Copper cross-over : C'est un standard Ethernet pour connecter deux équipements de même couche OSI.

✓ Fibre : Elle est utilisée pour mettre des connexions entre ports fibre (100 MBS et 1000 MBS).

✓ Wireless : N'est établie qu'entre les PC et les points d'accès, plusieurs PC peuvent être connecté à un seul point d'accès.

✓ Phone : C'est une connexion établie entre PC et routeur, PC et Switch, elle est utiliser pour la configuration a distance.

➢ **Simulation mode** :

Pour tester les différentes situations configurées en mode topologie. On peut créer des nouveaux scénarios en cliquant sur le bouton « «NEW » ».pour ajouter un autre paquet en clique sur  , dans ce mode on peut voir le parcours d'un paquet dans les différents couches de modèle OSI ainsi que sa durée de vie.

✓ Différentes situation d'un paquet :

- L'arrivée d'un paquet avec succès
- L'arrivée d'un paquet avec échec
- Un paquet qui entre dans la fille d'attente

Avant de l'appliquer nous avons mis au point le réseau suivant :

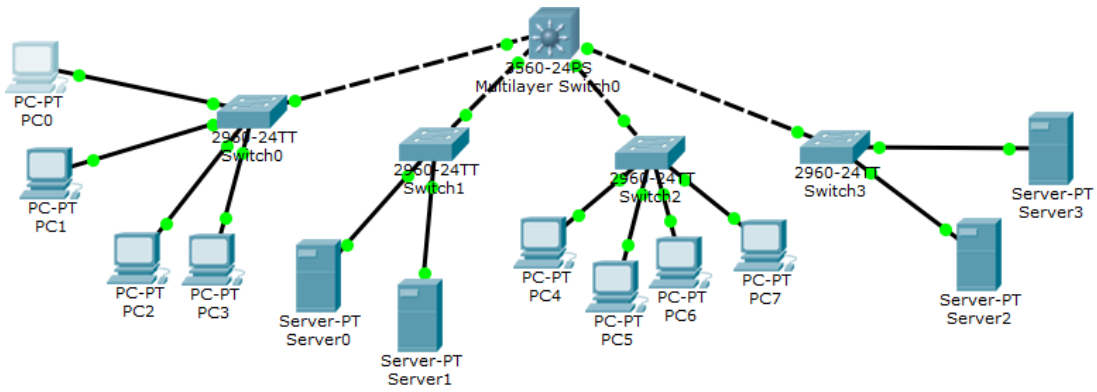


Figure 27 : Réseau local avec la solution proposée

4.2. Explication et configuration des étapes de la mise on œuvre

Nous pouvons dire en résumé que le réseau local se compose de 4 Vlan :

✓ VLAN 10 : @ dynamique allant de 172.128 .0.2 à 172.128.0.7 avec comme masque 255.255.0.0, la passerelle étant ,172.128.0.2

✓ VLAN 20 : @ dynamique allant de 172.128 .0.10 à 172.128.0.13 avec comme masque 255.255.0.0, la passerelle étant ,172.128.0.10

- ✓ VLAN 30 : @ dynamique allant de 172.128 .0.18 à 172.128.0.23 avec comme masque 255.255.0.0, la passerelle étant ,172.128.0.18

- ✓ VLAN 40 : @ dynamique allant de 172.128 .0.14 à 172.128.0.17 avec comme masque 255.255.0.0, la passerelle étant ,172.128.0.14

4.2.1 Explication des étapes de la mise en œuvre de la solution

Les étapes de la procédure suivit pour appliquer la solution proposée sont les suivant :

Etape n°1 : créer les vlan suivant :

Vlan 10 : est le sous-réseau pour switch0.

vlan20 : est le sous-réseau pour switch1.

vlan30 : est le sous-réseau pour switch2.

vlan40 : est le sous-réseau pour switch3.

Etape n°2 : affecter les Vlans crées aux différentes interfaces des Switch aux quelles sont connectées les ordinateurs.

Etape n°3 : créer 03 listes de contrôle d'accès(ACL) pour spécifier les ordinateurs ou bien les sous-réseaux qui doivent communiquer entre eux et les autres qui ne le doivent pas. Les exemples qu'on a pris pour l'application de ces ACL sont :

- ✓ ACL1 : bloquer l'accès au « pc0 » du switch0 d'accéder vers le « pc4 » du switch2.
- ✓ ACL2 : permettre l'accès vers tous les sous-réseaux pour le « pc1» du switch0 et cette application est envisageable pour la maintenance des ordinateurs à distance sans se déplacer.
- ✓ ACL3 : bloquer l'accès au « pc5 » du switch2 vers le serveur « serveur0 » du switch1 et permettre l'accès vers tous les sous-réseaux.

4.2.2. Configuration des étapes

- **Configuration de Switch fédérateur** :

federateur>enable //*pour passer en mode priviligié*//
federateur#config t //*pour le passage en mode de configuration globale*//
Enter configuration commands, one per line. End with CNTL/Z.
federateur(config)#hostname federateur //*pour définer le nom du switch fédérateur*//
federateur(config)#interface vlan 1
federateur(config-if)#ip address 172.128.0.1 255.255.0.0
federateur(config-if)#no shutdown //*activer l'interface*//
federateur(config-if)#exit //*quitter le mode actuel*//
federateur(config)#vtp mode server
Device mode already VTP SERVER.
federateur(config)#vtp domain DEPARTELECTRONIQUE.COM
ChangingVTP domain name from ELECTRONIQUE.fr to DEPARTELECTRONIQUE.COM
federateur(config)#vtp version 2
VTP mode already in V2.
federateur(config)#vlan 10
federateur(config-vlan)#name laboinfo1 //*donner un nom au VLAN crée*//
federateur(config-vlan)#exit
federateur(config)#interface vlan 10 //* mode configuration de l'interface VLAN10*//
federateur(config-if)#ip address 172.128.0.2 255.255.0.
federateur(config-if)#no shutdown //*active l'interface*//
federateur(config-if)#exit //*quitter le mode actuel*//
//*Remarque: il faut suivre juste ces memes instructions dans les 7 dernières lignes de configuration pour les autres VLANs*//
federateur(config)#access list 101deny icmp host 172.128.0.3 host 172.128.0.19 //*crée ACL1*//
federateur(config)#access list 101 permit host 172.128.0.3 any //*crée ACL2*//
federateur(config)#interface vlan 10//*associer l'ACL1 à l'interface *//
federateur(config-if)#ip access-group 101 out
federateur(config-if)#exit
federateur(config)#access list 102 permit icmp host 172.128.0.4 any //*crée ACL2*//
federateur(config)#interface vlan 10
federateur(config-if)# ip access-group 102 out
federateur(config-if)#exit
federateur(config)#access list 103deny icmp host 172.128.0.20 host 172.128.0.11 //*crée ACL3*//
federateur(config)#access list 103deny icmp host 172.128.0.20 any
federateur(config)#interface vlan 30
federateur(config-if)#ip access-group 103 out
federateur(config-if)#exit

- **Configuration de switch0**

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname laboinfo 1
Switch(config)#hostname laboinfo1
laboinfo1(config)#vtp mode client
Setting device to VTP CLIENT mode.
laboinfo1(config)#interface vlan 1
laboinfo1(config-if)#ip address 172.128.0.2 255.255.0.0
laboinfo1(config-if)#no shutdown
laboinfo1(config-if)#exit
laboinfo1(config)#interface fa0/1
laboinfo1(config-if)#switchport mode trunk
laboinfo1(config-if)#no shutdown
laboinfo1(config-if)#exit
laboinfo1(config)#interface fa0/2
laboinfo1(config-if)#switchport mode access //*mettre l'interface en mode accès*//
laboinfo1(config-if)#switchport access vlan 10 //*affecter le VLAN10 à l'interface*//
laboinfo1(config-if)#no shutdown
laboinfo1(config-if)#exit
laboinfo1(config)#interface fa0/3
laboinfo1(config-if)#switchport mode access
laboinfo1(config-if)#switchport access vlan 20
laboinfo1(config-if)#no shutdown
laboinfo1(config-if)#exit
```

- **configuration de switch2**

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname laboinfo2
laboinfo2(config)#vtp mode client
Setting device to VTP CLIENT mode.
laboinfo2(config)#interface vlan 1
laboinfo2(config-if)#ip address 172.128.0.18 255.255.0.0
laboinfo2(config-if)#no shutdown
laboinfo2(config-if)#exit
```

```
laboinfo2(config)#interface fa0/1
laboinfo2(config-if)#switchport mode trunk
laboinfo2(config-if)#no shutdown
laboinfo2(config-if)#exit
laboinfo2(config)#interface fa0/2
laboinfo2(config-if)#switchport mode access
laboinfo2(config-if)#switchport access vlan 30
laboinfo2(config-if)#no shutdown
laboinfo2(config-if)#exit
laboinfo2(config)#interface fa0/3
laboinfo2(config-if)#switchport mode access
laboinfo2(config-if)#switchport access vlan 40
laboinfo2(config-if)#no shutdown
laboinfo2(config-if)#exit
```

- **configuration de switch1**

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname serveur
serveur(config)#vtp mode client
Setting device to VTP CLIENT mode.
serveur(config)#interface vlan 1
serveur(config-if)#ip address 172.128.0.10 255.255.0.0
serveur(config-if)#no shutdown
serveur(config-if)#exit
serveur(config)#interface fa0/1
serveur(config-if)#switchport mode trunk
serveurI(config-if)#no shutdown
serveurI(config-if)#exit
serveurI(config)#interface fa0/2
serveurI(config-if)#switchport mode access
serveurI(config-if)#switchport access vlan 20
serveurI(config-if)#no shutdown
serveurI(config-if)#exit
serveurI(config)#interface fa0/3
serveurI(config-if)#switchport mode access
serveurI(config-if)#switchport access vlan 10
serveurI(config-if)#no shutdown
serveurI(config-if)#exit
```

- **configuration de switch3**

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname serveur
ServeurII(config)#vtp mode client
Setting device to VTP CLIENT mode.
ServeurII(config)#interface vlan 1
ServeurII(config-if)#ip address 172.128.0.14 255.255.0.0
ServeurII(config-if)#no shutdown
ServeurII(config-if)#exit
ServeurII(config)#interface fa0/1
ServeurII(config-if)#switchport mode trunk
ServeurII(config-if)#no shutdown
ServeurII(config-if)#exit
ServeurII(config)#interface fa0/2
ServeurII(config-if)#switchport mode access
ServeurII(config-if)#switchport access vlan 40
ServeurII(config-if)#no shutdown
ServeurII(config-if)#exit
ServeurII(config)#interface fa0/3
ServeurII(config-if)#switchport mode access
ServeurII(config-if)#switchport access vlan 10
ServeurII(config-if)#no shutdown
ServeurII(config-if)#exit

- **sécurisation de l'accès aux Switch:**

  Pour une meilleure sécurité des accès aux Switch, nous avons chiffré le mot de passe et imposé des mots de passe d'au moins dix caractères et enfin on a limité le nombre de tentative de connexion à trois tentatives.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname federateur
federateur(config)#service password-encryption
federateur(config)#security password min-length 10
federateur(config)#enable secret SALIM12345
federateur(config)#username admin privilage 15 secret SALIM12345
federateur(config)#line console0
federateur(config)#password SALIM
federateur(config)#loging
federateur(config)#line vty 0
federateur(config-line)#transport input ssh
federateur(config-line)#loging local
federateur(config-line)#exit
federateur(config)#line aux 0
federateur(config-line)#no exec
federateur(config-line)#exit
```

4.2.3. Vérification ACL crée :

La figure ci-dessous représente le résultat obtenue lors d'un Ping de la première liste de contrôle d'accès

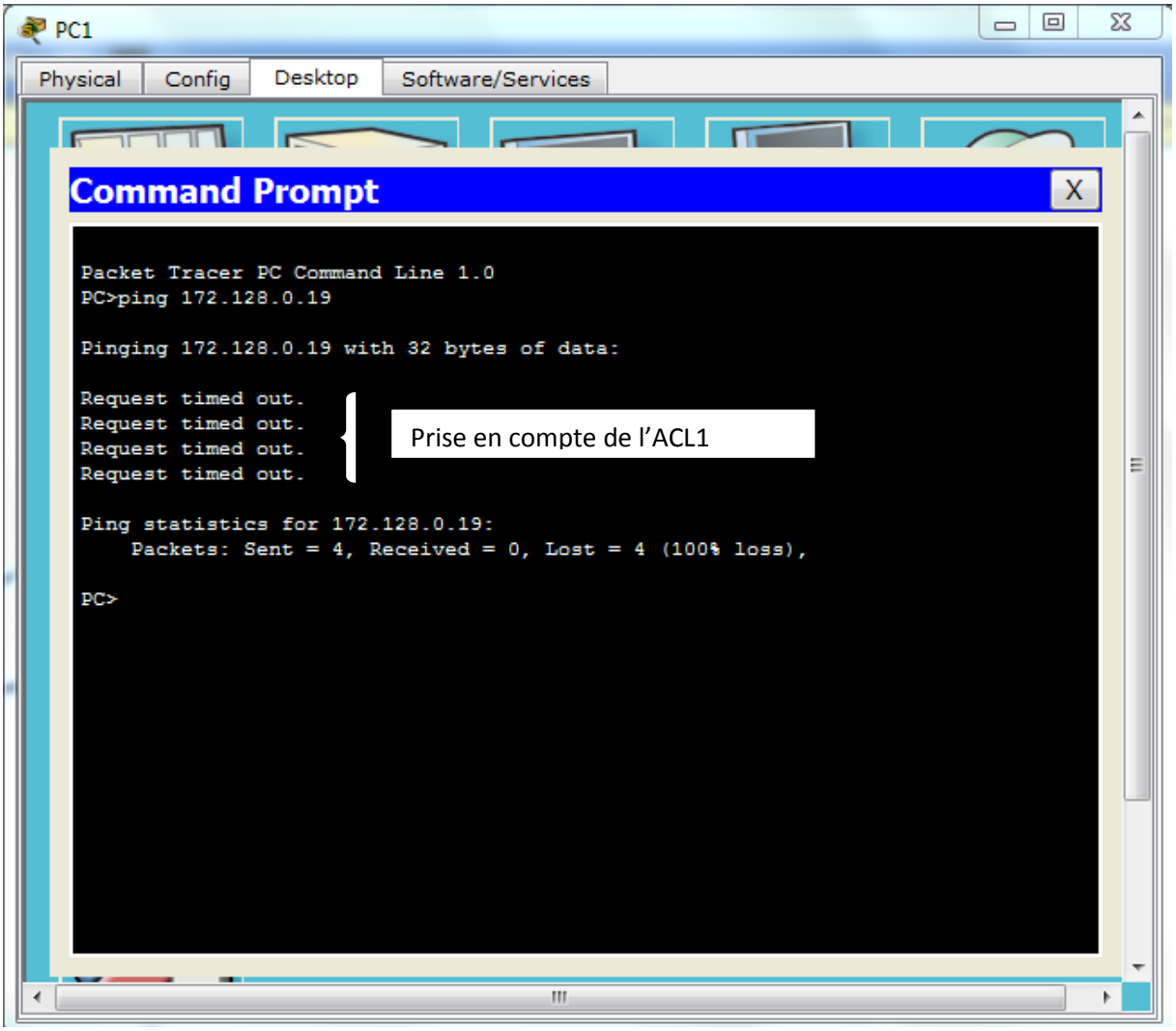


Figure 28 : Teste après la création de l'ACL1

La figure ci-dessous représente le résultat obtenue lors d'un Ping de la deuxième liste de contrôle d'accès

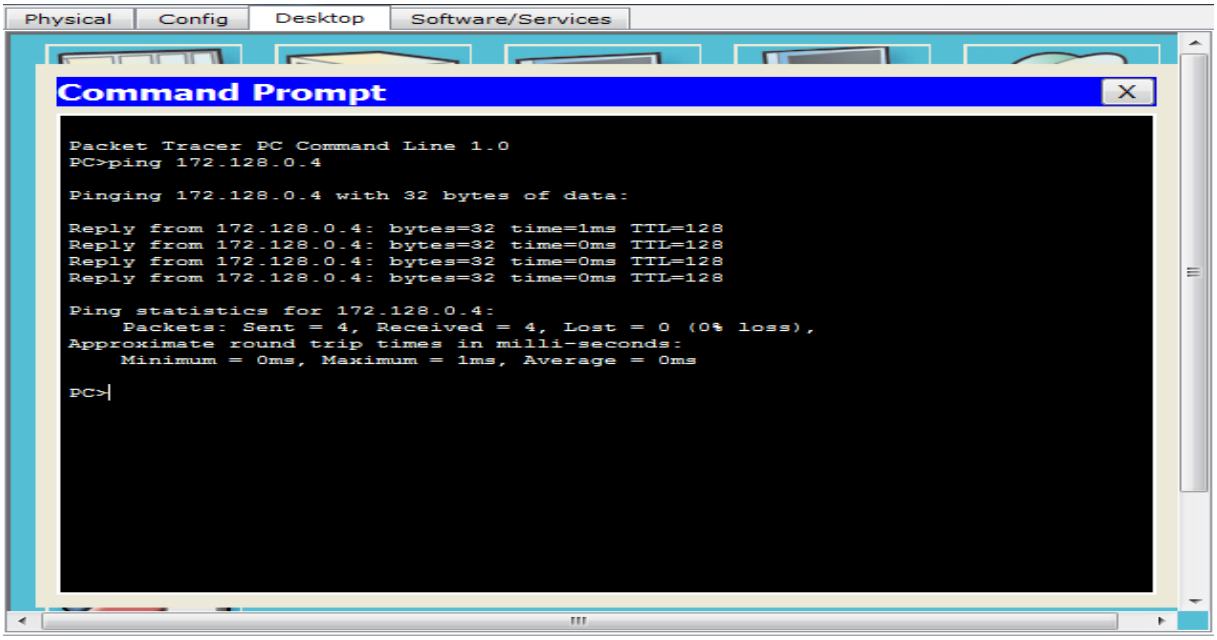


Figure 29 : Teste après la création de l'ACL2

La figure ci-dessous représente le résultat obtenue lors d'un Ping de la troisième liste de contrôle d'accès

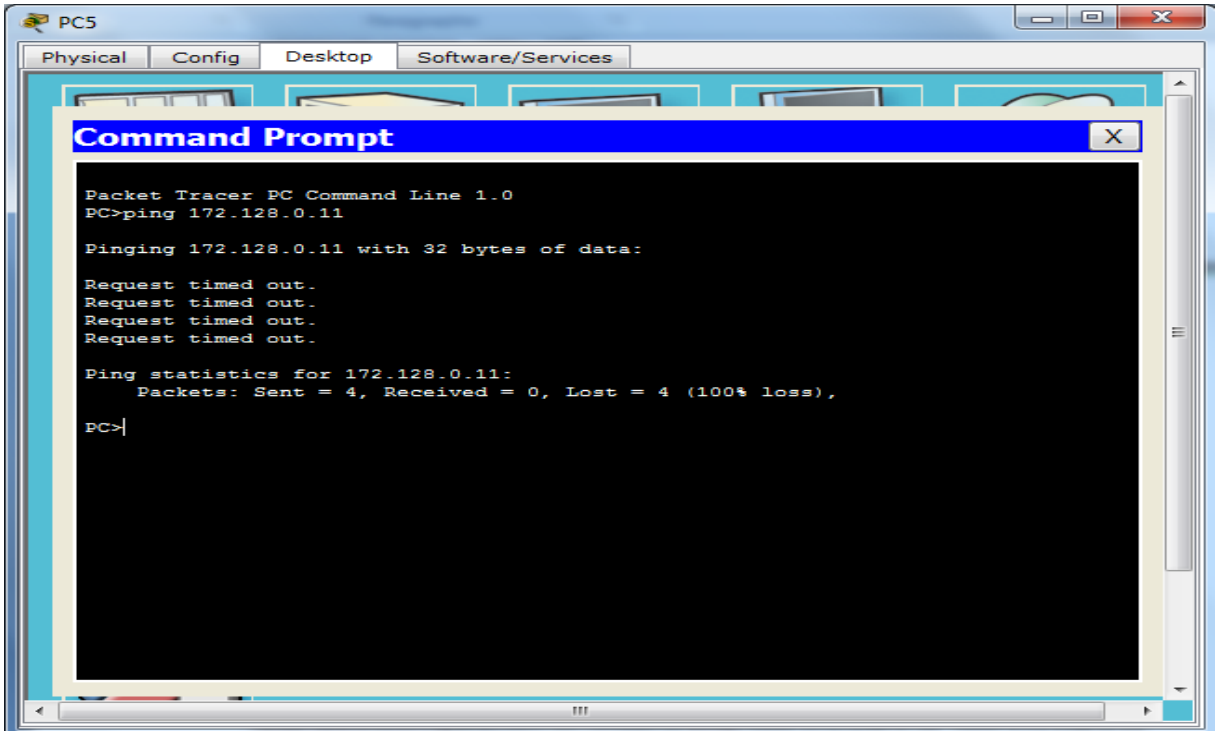


Figure 30 : Teste après la création de l'ACL3

5. Discussion :

Ce chapitre est consacré à l'implémentation de solutions proposées, des tests de fonctionnement sur les solutions déployées on été faits.

D'après les résultats de la simulation obtenue, on constate que les listes de contrôle d'accès qu'on a appliqué sur le fédérateur 3550 nous a permit de sécuriser le réseau local de l'entreprise.il est pratiquement impossible d'assurer une sécurité totale et sure à cent pour cent, c'est pour cela les grandes entreprises ne se limite pas à un seul produit.

Conclusion générale

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

Dans notre mémoire, nous nous somme intéressés à une technique(méthode), qui nous aide à mettre en place et en marche une politique de sécurité dans le but de faire face à ces différentes menaces et attaques, cette politique de sécurité est basée sur l'installation et la configuration d'un serveur de fichiers et d'un serveur RADIUS ainsi la configuration des autres élément d'interconnexion du réseau afin d'avoir plus de sécurité en utilisant des listes de contrôle d'accès(ACL).

Ce projet nous à permis d'acquérir des connaissances dans de nombreux domaines. En effet il nous à initié au monde de la recherche sur les réseaux informatique surtout en ce qui concerne la sécurité, ainsi les différents modes de communication, leur application ainsi que les protocoles qui les gèrent.

Grace à notre modeste travail, nous avons eu l'occasion de voir beaucoup de choses de plus prés et d'enrichir nos connaissances, nous avons aussi eu la chance de mettre nos capacités en valeur et de faire face aux situations critiques et obstacles et apprendre comment procéder pour s'en sortir.

En effet, la sécurité est comme une chaine et elle est proportionnel aux différentes menaces, c'est ce qui à fait de la sécurité un sujet très vaste et très important en même temps, dont nous envisageons quelque perspectives pour la continuation de ce travail :

- ✓ S'intéresser à d'autre aspect de sécurité par exemple : la configuration d'un VPN ;
- ✓ Conception d'un réseau sans fil pour ajouter l'unité commerciale au réseau de l'entreprise.

BIBLIOGRAPHIE/WEBOGRAPHIE

[1] ELIE MABO, “la sécurité des systèmes informatique (théorie), support de cours, 2010.

[2] La sécurité des réseaux, support de cours, mercredi 8 novembre 2006

[3] DOMINIQUE SERET, AHMED MEHAOUA et NELIZE DORIA, « réseaux et télécommunication », support de cours université René Descartes-Paris-2006.

[4] LAURENCE MONACO, « quelques définition »,2010 .

[5] LAURENT BLOCH et CHRISTOPHE WOLFHNGEL, « sécurité informatique-principes et méthodes », livre vol.276, 2007.

[6] LAURENT POINSOT « Introduction à la sécurité informatique », support de cours, université Paris13.

[7] RABHI SIDI MOHAMED EL AMINE « mise en place d’un serveur RADIUS sous linux ».

[8] AUROBINDO SUNDRAM, met à jour le, février 2005, « An intrusion intrusion detection », ACMcrossroad student magazine, http://www.acm.org/crossroads/xrds2-4/intrus.html.

[9] TRAN VAY TAY, « le système de détection des intrusions et le système d’empêchement des intrusions », rapport de stage de fin d’étude, 2005.

[10] Jacob Zimmermann et al. , « Vers une détection d’intrusion à fiabilité et pertinence prouvable», Thèse de doctorat, Université de Technology, Australie, 2006.

[11] JEAN-LUC ARCHIMBAUD, « la sécurité et les réseaux (Unix –IP), http://www.urec.fr/jla.html , octobre1995.

[12] BERNARD COUSIN, « sécurité des réseaux informatiques » , support de cours, université de rennes1.

[13] Configuration des listes d’accès IP, http://www.cisco.com/cisco/web/support/CA/fr/109/1094/1094955_ACLsamples.html.

[14] Serveur de sécurité Adaptif Cisco ASA5500, http://www.cisco.com/go/asa

[15] JM.DEBROISE, « Cisco les ACL », BTS IG SIO.

BIBLIOGRAPHIE/WEBOGRAPHIE

[16] Implémentation d'une politique de sécurité au réseau informatique de l'entreprise ENIEM de Tizi-Ouzou, Mr HADDAD ABBAS et Mlle ALICHE SONIA, UMMTO, 2010.

[17] http://ressource,intenseschool.com/ccna-lab-practice-ciscopacket/.html.

[18] http://ieonline.microsoft.com/#ies/io/sécurité-routeur-switch.mht

[19] VINCENT REMASEIILLES, « la sécurité des réseaux avec Cisco », 2008, ENI Edition.