République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Bejaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Master Professionnel en Informatique

Option : ***Administration et sécurité des réseaux***

Thème:

Configuration de la sécurité d'accès au niveau du routeur d'un réseau intranet

Réalisé par :

M^elle^ BEDJOU Lamia
M^elle^ BENSLIMANE Nadia

Devant le jury composé de:

President: M^r^ LARBI Ali
Encadreur : M^r^ TOUAZI Djoudi
Examinateurs: M^r^ KHENOUS Lachemi
M^elle^ SABRI Salima

Année universitaire: 2011 – 2012

Remerciements

En premier lieu, je remercie le BON DIEU Fidèle, compatissant et puissant pour la santé, la force, le courage, la persévérance que nous a donné tout au long de ce travail.

Mes remerciements vont encore à tous mes enseignants de l'université de Bejaia en particulier à Mr TOUAZI Djoudi qui a accepté de diriger ce mémoire.

Je remercie également les membres de jury d'avoir bien voulu accepter de faire partie de la commission d'examinateur.

Je remercie aussi :

Mes très chers parents qui n'ont jamais cessé un instant de m'encourager tout au long de ma vie, à mes frères, à tout mes amis.

Ainsi que tous ceux et celles qui de prés ou de loin m'ont aidée et portée dans leurs cœurs jusqu'à ce stade.

Lamia BEDJOU

Je dédie ce mémoire

À mon très cher père Abdelhak qui a toujours été un exemple de patience, de labeur pour moi, À ma très chère mère Rachida que j'aime plus que tout au monde, qui ma toujours soutenue et été là pour moi et pour mes trois frères.

J'espère que vous trouverez dans ce travail toute ma reconnaissance que Dieu vous garde pour nous.

À mes chers frères : Hani, Rayan et Anis à qui je souhaite tout le bonheur et beaucoup de réussite.

À toute ma famille mes grands-mères, tentes, oncles, cousins, cousine.

À mes amies : Hassina, Dyhia, Cherifa, Wassila, Salima, Naima, Souad.

À Bachir qui a toujours su me raisonner, et qui ma soutenu ces trois dernières années.

À mon binôme et amie Nadia avec qui j'ai partagé quatre ans de bons moments inoubliables, c'était un vrai plaisir de travailler avec toi.

À celle qui a la formule magique de nous redonner sourire quand tout aller mal et qui nous a toujours, encouragé un grand merci à tata Radia.

À tous les gens qui me connaissent.

Lamia BEDJOU

Remerciements

"L'éducation n'est, en somme, que l'art de révéler à l'être humain le sens intime qui doit gouverner ses actes, préparer l'emploi de ses énergies et lui communiquer le goût et la force de vivre pleinement."

Henry Bordeaux (1870-1963)

Ma profonde gratitude et mon éternelle reconnaissance

À mes parents,

Pour leur amour et leur abnégation qu'ils ont dévotieusement consentis pour que nous puissions un jour être dignes de leurs immenses sacrifices et de leurs espoirs.

À mes Professeurs, Spécialement à Mr Djoudi TOUAZI

Pour leur patience et leur disponibilité permanente et sans faille qui nous permit d'emprunter cette voie si noble et interminable, privilège sublime qu'est la quête du savoir. Spécialement à Mr Djoudi TOUAZI qui a accepté de nous encadrer, ainsi qu'aux membres de jury qui ont acceptés d'examiner notre travail.

À mes amis

Instigateurs malgré eux de cette émulation, seule force interne et mystérieuse qui anime en nous ce désir et cette ambition de parvenir à des sommets qui feront la fierté de nos parents, de notre université, et de notre pays.

Nadia BENSLIMANE

C'est avec un cœur ouvert et une immense joie que je dédie ce modeste travail à :

Mes très chers, respectueux et magnifiques parents que j'aime le plus au monde, mon cher père qui a toujours su me raisonner et m'orienter dans mes choix, ma maman chérie qui a toujours était là pour moi, qui a su me redonner raison quand je l'ai perdu, me redonner espoir quand j'en n'en avais plus, et qui a toujours su dessiner un sourire sur mon visage même quand tout aller vraiment mal, je leurs dédie ce travail car j'en suis sure qu'ils le méritent même un peu plus que moi.

Mon grand frère ***A.Hakim*** *qui ne rate pas une occasion de me faire pleurer, mais que j'aime beaucoup et que c'est un peu grâce à lui que j'ai suivi ce bon chemin qui est la quête du savoir, et à qui je souhaite bon courage pour sa soutenance de Doctorat. À mon petit frère* ***A.Hafid*** *et à ma petite princesse* ***Zora*** *que j'appelle à suivre le chemin de leurs ainés.*

À mes chers cousins et cousines, ci nombreux et tous spéciaux dans mon cœur que même un autre mémoire ne me suffirais pas pour tous les citer, à mes tentes et mes oncles, mon papi et ma mamie, à la mémoire de tata Khoujia, et tous ceux qui nous ont quittés un peu trop tôt.

À tous mes amis ; Souhila, Dyhia, Soad, Aicha et ses sœurs.

Spécialement à mon binôme, meilleure amie et sœur « Lamia » et sa famille, ainsi qu'à Latamen qui a toujours su être au prés de moi, m'écouter et toujours me faire rire. Je vous aime.

À tous ceux qui vont lire ce mémoire.

Nadia BENSLIMANE

Table des matières

Liste des figures

Liste des Tableaux

Liste des abréviations

ACL : **A**ccess **C**ontrol **L**ists

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

ARP : **A**ddress **R**esolution **P**rotocol

AS : **A**utonomous **S**ystem

BGP : **B**order **G**ateway **P**rotocol

CCNA : **C**isco **C**ertified **N**etwork **A**ssociate

CPU : **C**entral **P**rocessing **U**nit

DHCP : *Dynamic Host Configuration Protocol*

DMZ : **D**emilitarized **Z**one

DNS : **D**omain **N**ame **S**ervice

DOS : **D**enial **o**f **S**ervice

EGP : **E**xterior **G**ateway **P**rotocol

FTP : **F**ile **T**ransfer **P**rotocol

HDLC : **H**igh **L**evel **D**ata Link **C**ontrol

H-IDS : **H**ost-**I**ntrusion **D**etection **S**ystem

HTTP : **H**yper **T**ext **T**ransfert **P**rotocol

ICMP : **I**nternet **C**ontrol **M**essage **P**rotocol

IDS : **I**ntrusion **D**etection **S**ystems

IGP : **I**nterior **G**ateway **P**rotocol

IGRP : **I**nterior **G**ateway **R**outing **P**rotocol

IOS : **I**nternetworking **O**perating **S**ystem

IP : **I**nternet **P**rotocol

ISO : **I**nternational **S**tandard **O**rganization

LAN : **L**ocal **A**rea **N**etwork.

LSA : **L**ink-**S**tate **A**dvertisement

MAC : **M**edium **A**ccess **C**ontrol

MAN : **M**etropolitan **A**rea **N**etwork

N-IDS : **N**etwork-**I**ntrusion **D**etection **S**ystem

NM : **N**etwork **M**odule

NvRam : **N**on-**V**olatile **R**andom **a**ccess **m**emory

OSI : **O**pen **S**ystem **I**nterconnexion.

OSPF : **O**pen **S**hortest **P**ath **F**irst

RARP : **R**everse **A**ddress **R**esolution **P**rotocol

RIP : **R**outing **I**nformation **P**rotocol

RTP : **R**eal-time **T**ransport **P**rotocol

SMTP : **S**imple **M**ail **T**ransfer **P**rotocol

SNMP : **S**imple **N**etwork **M**anagement **P**rotocol

SPF : **S**hortest **P**ath **F**irst algorithm

TCP : **T**ransmission **C**ontrol **P**rotocol

Telnet : **T**erminal **N**etwork Protocol

TFTP : **T**RIVIAL **F**ile **T**ransfer **P**rtocol

UDP : **U**ser **D**atagram **P**rotocol

VLAN : **V**irtual **L**ocal **A**rea **N**etwork

VTY : **V**irtual **T**elet**Y**pe

WAN : **W**ide **A**rea **N**etwork

WIC : **W**AN **I**nterface **C**ard

Introduction Générale

Introduction Générale

Les réseaux informatiques sont devenus essentiels à la bonne marche des entreprises. En effet, les entreprises sont de plus en plus grandes, multinationales, délocalisées et éclatées. La croissance accélérée de ces réseaux qui sont de plus en plus ouverts sur Internet, est à priori bénéfique, pose néanmoins un problème important de sécurité. Il en résulte un nombre croissant d'attaques qui peuvent aboutir à de graves conséquences professionnelles et financières en menaçant l'intégrité, la confidentialité et la disponibilité de l'information. De nombreuses entreprises ont compris l'importance de ces enjeux, ce qui les a poussées à émerger dans le domaine de la sécurité informatique.

La sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration réseau. La difficulté que représente la sécurité dans son ensemble est de trouver un compromis entre deux besoins essentiels : le besoin d'ouvrir des réseaux pour profiter de nouvelles opportunités commerciales et le besoin de protéger des informations privées ou publiques et des informations commerciales stratégiques.

L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Les administrateurs doivent donc trouver un moyen d'interdire l'accès au réseau à certains utilisateurs tout en l'accordant à d'autres.

Les outils classiques tels que les mots de passe et les dispositifs de sécurité physiques se révèlent utiles mais dans la pluparts des cas, ils n'offrent pas la souplesse que procure le filtrage de trafic réseau.

Dans le cadre de notre projet de fin d'études, il nous a été proposé de faire une étude sur la gestion du trafic à l'aide des listes de contrôle d'accès au niveau d'un routeur, la compréhension approfondie des listes de contrôle d'accès et l'administration des routeurs est l'une des principales compétences requises chez un administrateur réseau. Les administrateurs utilisent des listes de contrôle d'accès pour arrêter le trafic dans son intégralité ou pour l'autoriser partiellement sur leurs réseaux. Pour mener à bien ce travail, nous avons adopté le plan suivant :

Dans le premier chapitre, nous présenterons un ensemble de concepts théoriques liés aux réseaux informatique. Le second chapitre est consacré à la sécurité des réseaux, ses

principes. Nous avons aussi parlé de quelques solutions proposées (pare-feu, les IDS, la cryptographie, les VLANs et les ACLs...). Dans le troisième chapitre, nous parlerons du routeur, ses fonctionnalités ainsi que le rôle important qu'il joue dans la sécurité des réseaux. Ensuite nous étudierons dans le quatrième chapitre la gestion de trafic par les listes de contrôle d'accès. Dans le cinquième chapitre, nous allons mettre en œuvre les listes de contrôle d'accès en donnant quelques exemples d'application. Nous terminerons enfin ce mémoire par une conclusion générale.

Chapitre 1

Généralités sur les réseaux

Chapitre 1

Généralités sur les réseaux informatiques

Introduction

Un réseau informatique est constitué d'un ensemble de systèmes informatiques interconnectés les uns avec les autres grâce à des équipements et supports de communications. L'objectif est de permettre à plusieurs machines de communiquer entre elles à fin d'assurer des échanges d'informations et un partage de ressources matérielles ou de données. Du point de vue de l'utilisateur, le réseau doit être le plus transparent possible: ses applications doivent être capables de communiquer toutes seules avec le reste du réseau, sans l'intervention humaine.

1. Les différents types de réseaux

On classe les différents réseaux selon leurs tailles, leurs vitesses de transfert ainsi que leurs étendues, donc on parlera de [9] :

Réseau personnel (PAN), Réseau local (LAN), **Réseau métropolitain (MAN), Réseau étendu (WAN).**

2. Topologie des réseaux

On peut différencier deux types de topologies, **la topologie physique** et **la topologie logique** (voir Annexe E).

3. Les modèles de références

3.1. Le Modèle OSI

L'ISO[1] (International Standardization Organization) a normalisé sa propre architecture sous le nom d'OSI (Open Systems Interconnection). L'architecture OSI permet l'interconnexion des réseaux hétérogènes. Ce modèle est composé de 7 couches (niveaux). Les services des couches supérieures peuvent intervenir sur chaque couche immédiatement inférieure (voir ANNEXE A).

3.2. Le modèle TCP/IP

On parle de TCP/IP, en dénommant ainsi les deux protocoles sur lesquels repose le réseau, TCP/IP est basé sur un modèle de référence de quatre couches, il sert à la plus grande partie des échanges de données sur Internet. La couche transport, sur laquelle s'appuient directement les applications, fournit deux types de service ; un service en mode connecté, fiable avec le protocole TCP (Transmission Control Protocol) et un service de transport allégé **UDP** (*User Datagram Protocol*) qui opère en mode de transport non connecté, au niveau des datagrammes. L'architecture TCP/IP comprend de nombreux programmes applicatifs, utilitaires et protocoles complémentaires. [9,10]

Les principaux protocoles et applications de l'environnement TCP/IP sont :

- **HTTP**, *HyperText Transport Protocol*, assure le transfert de fichiers hypertextes entre un serveur Web et un client Web ;
- **FTP**, *File Transfer Protocol*, est un système de transfert de fichiers à distance (transfert, suppression, création...) ;
- **TELNET**, *TELetypewriter NETwork protocol* (ARPA) ou *TERminaL NETwork protocol*, système de terminal virtuel, permet l'ouverture de sessions avec des applications distantes.
- **SMTP**, *Simple Mail Transfer Protocol*, offre un service de courrier électronique.
- **TFTP**, *Trivial FTP*, est une version allégée du protocole FTP.
- **DNS**, *Domain Name System*, est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse Internet (adresse IP).

[1] ISO (International Standardization Organisation) organisme dépendant composé de 140 organismes nationaux de normalisation, a développé un modèle de référence appelé modèle OSI.

- **ICMP**, *Internet Control and error Message Protocol*, permet la signalisation de la congestion, la synchronisation des horloges et l'estimation des temps de transit... Il est utilisé par l'utilitaire **Ping** qui permet de tester la présence d'une station sur le réseau.

4. Internet et intranet

4.1. Internet

Internet est un système mondial d'interconnexion de réseau informatique, utilisant un ensemble standardisé de protocoles de données. C'est donc un réseau de réseaux, composé de millions de réseaux aussi bien publics, privés, universitaires, commerciaux et gouvernementaux dont leur piles de protocoles est compatible avec la pile TCP/IP. Internet transporte un large spectre d'information et permet l'élaboration d'applications et de services variés comme le courrier électronique, la messagerie instantanée et le World Wide Web.

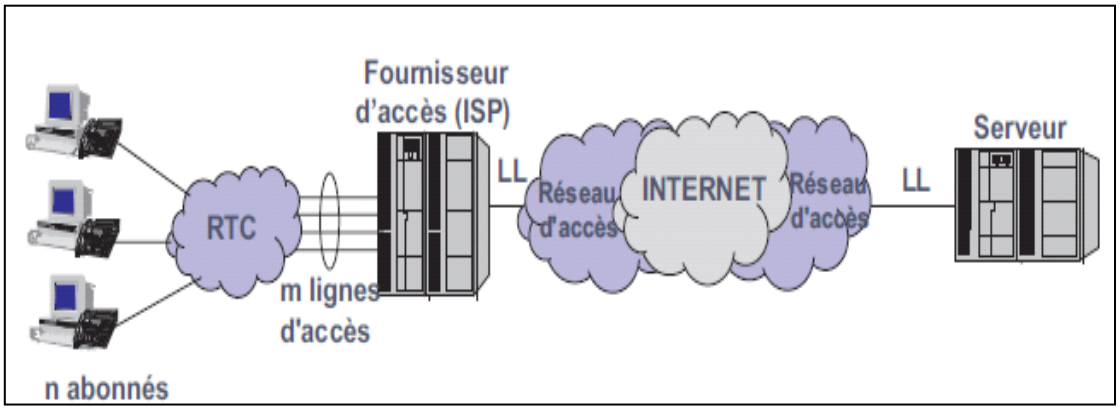


Figure 1 - L'acheminement des données jusqu'au serveur

L'accès à Internet peut être obtenu grâce à un fournisseur d'accès à Internet (FAI) via divers moyens de communication électronique : soit filaire (réseau téléphonique commuté (RTC), ADSL [2], fibre optique jusqu'au domicile) , soit sans fil (par satellite,3G[3]).

[2] **ADSL**: **A**symmetric **D**igital **S**ubscriber **L**ine. Technique de transmission qui permet, via modem adapté, d'utiliser une partie de la bande passante des lignes téléphoniques ordinaires.
[3] **3G** : c'est la **troisième génération** (3G) désigne une génération de normes de téléphonie mobile.

4.2. Intranet

Intranet est un petit réseau d'entreprise qui a accès à Internet. Il consiste à utiliser les standards client-serveur de l'internet (en utilisant les protocoles TCP/IP).

Les Intranets sont principalement utilisés en tant que système d'information générale. En effet, cette technologie permet de regrouper en un seul endroit une quantité non négligeable de données, que ce soit des informations sur les clients, sur les fournisseurs, une gestion de stock, un centre de documentation, une messagerie électronique, etc., le tout commun à l'ensemble de l'entreprise ou de l'organisation. Cela permet d'avoir un accès centralisé et cohérent à la mémoire de l'entreprise. On parle ainsi de *capitalisation de connaissances*. De cette façon, il est généralement nécessaire de définir des droits d'accès pour les utilisateurs de l'intranet aux documents, donc une authentification de ceux-ci afin de leur permettre un accès personnalisé à certains documents.

Et voici quelques unes des fonctions que peut réaliser un intranet [17] :

- Mise à disposition d'informations sur l'entreprise,
- Mise à disposition de documents techniques,
- Moteur de recherche de documentations,
- Un échange de données entre collaborateurs,
- Annuaire du personnel,
- Gestion de projet, aide à la décision, agenda, ingénierie assistée par ordinateur,
- Messagerie électronique,
- Forum de discussion, liste de diffusion, chat en direct,
- Visioconférence,
- Portail vers internet.

4.2.1. Équipements d'interconnexion d'un intranet

Un réseau local est constitué d'équipements reliés par un ensemble d'éléments matériels et logiciels. Les principaux équipements matériels d'interconnexion mis en place dans les réseaux locaux sont [7,15] :

- **Carte réseau** : Elle est employée pour faire communiquer un ordinateur avec d'autres éléments, tels que des serveurs, des imprimantes ou même des PCs.

- **Répéteur** : C'est un élément qui régénère et augmente le signal pour le transmettre d'un réseau à un autre. Il agit au niveau 1(physique) du modèle OSI.
- **Pont (Bridge)** : Est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole pour n'en former qu'un seul réseau logique. Le pont travaille au niveau logique (couche 2 du modèle OSI).
- **Routeur** : Un routeur opère au niveau de la couche réseau du modèle OSI(niveau 3). Ils permettent de relier des réseaux sur de longues distances et à examiner l'adresse réseau pour prendre des décisions de routage.
- **Commutateur (Switch)** : Équipement de niveau 2 (couche liaison de données) du modèle OSI. Les commutateurs sont généralement utilisés pour réorganiser un réseau, isoler des serveurs, segmenter des réseaux.
- **Passerelle (Gateway)** : Les passerelles permettent de relier des réseaux locaux de types différents, par exemple un réseau local et Internet. En effectuant le routage, l'ensemble du réseau local peut accéder à Internet par l'intermédiaire de la passerelle.

Conclusion

Ce chapitre nous a permis de mieux cerner les notions de bases sur les réseaux, d'avoir une idée sur les différents types de réseaux ainsi que les différentes topologies et aussi d'éclaircir la notion de couche dans le modèle OSI et le modèle TCP / IP. Nous avons finit par une présentation de l'internet et surtout de l'intranet qui est le domaine de notre travail.

Dans le prochain chapitre, nous aborderons la sécurité des réseaux informatiques qui compte actuellement parmi les sujets les plus importants au sein d'une entreprise ou dans les réseaux informatiques.

Chapitre 2

La sécurité des réseaux

Chapitre 2

La sécurité des réseaux

Introduction

Notre dépendance vis à vis des ordinateurs est de plus en plus prononcée et l'informatique est devenue pour l'entreprise un outil obligatoire de gestion, d'organisation, de production et de communication. De ce fait les données mises en œuvre par le système d'information, les échanges internes et externes, la garde d'archives et d'informations personnelles sont exposés aux actes de malveillance de différentes natures. Ce qui a poussé nombreuses industries d'émerger dans le domaine de la sécurité informatique et des réseaux afin d'analyser leurs systèmes de façon correcte et d'élaborer des solutions adaptées à leurs besoins opérationnels. Dans ce chapitre, nous parlerons alors des principes de la sécurité des réseaux ainsi que de quelques solutions proposées.

1. Les principes de la sécurité informatique

1.1. Terminologies de la sécurité informatique

- **Vulnérabilité :** C'est une faille de sécurité dans un ou plusieurs systèmes, qui peut être exploitable ou non.
- **Attaque (exploit) :** Elle représente le moyen d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité.
- **Contre-mesure :** C'est une procédure ou technique permettant de résoudre une vulnérabilité ou d'empêcher une attaque spécifique.
- **Menace :** C'est un adversaire déterminé capable de monter une attaque exploitant une vulnérabilité.
- **Politique de sécurité :** Elle définit un certain nombre de règles, de procédures permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

1.2. Les objectifs de la sécurité

La sécurité informatique, d'une façon générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité vise généralement ses objectifs :

- **La confidentialité :** Protection de données émises sur le réseau compréhensibles seulement par des entités autorisées.
- **Authentification :** Garantie que les données reçues proviennent bien de l'entité émettrice.
- **Intégrité :** Garantie que les données reçues n'ont subi aucune modification lors du transport dans le réseau.
- **Non répudiation** : C'est la propriété qui assure la preuve de l'authenticité d'un acte.

1.3. Les différents types d'attaques réseau

Vu que l'informatique est un domaine très vaste, alors le nombre de vulnérabilités présentes sur un système peut donc être important. Ainsi, on ne doit pas s'étonner si les attaques visant ces failles soient à la fois très variées et très dangereuses. Et pour cela, dans un premier temps, nous allons analyser ce que nous appelons « *anatomie d'une attaque* », puis dans un second temps, nous présenterons les différentes techniques d'attaques et observerons leurs déroulements.

1.3.1. Anatomie d'une attaque

Aussi nommés « les 5 P », ces verbes anglophones forment le squelette de toute attaque informatique : Probe, Penetrate, Persist, Propagate, Paralyze. Et voila en détail chacune de ces étapes [18] :

- **Probe** : Consiste en la collecte d'informations, et cette collecte peut s'effectuer de plusieurs manières.
- **Penetrate** : C'est l'utilisation des informations récoltées pour pénétrer un réseau.
- **Persist** : Afin de pouvoir se ré-infiltrer ultérieurement, il est donc nécessaire de créer un compte avec des doits de super utilisateur.
- **Propagate** : ça consiste à observer ce qui est accessible et disponible sur le réseau local.
- **Paralyse** : Sur cette étape, le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur.

1.3.2. Les techniques d'attaques réseaux

Si une personne mal intentionnée veut acquérir des ressources, il existe un grand nombre d'attaques qui lui permet de les appropriées, de les bloquer ou de les modifier.

Certaines requièrent plus de compétence que d'autres. Ces attaques ont plusieurs types à savoir :

a. Les attaques passives (Écoute du réseau)

Consistent à écouter sans modifier les données ou le fonctionnement du réseau, on site par exemple :

i. Le sniffing des mots de passe et des paquets

Le sniffing qu'on appel le reniflage en français est une méthode qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations. Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles.

ii. Le scanning

Un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les Hackers utilisent les scanners pour savoir comment ils vont procéder pour attaquer une machine.

b. Les attaques actives

Ces attaques consistent à modifier des données, à se glisser dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau, exemple :

i. L'attaque par déni de service

Les attaques par déni de service en anglais (Denial of Service, Dos) sont destinées à refuser des services à des hôtes légitimes qui essayent d'établir des connexions. Les attaques par déni de service sont utilisées par les pirates pour bloquer les réponses système.

ii. Le spoofing IP

C'est une technique qui permet à un pirate de transmettre à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Donc il s'agit d'une modification des paquets envoyés afin de faire croire au destinataire qu'ils proviennent d'une autre machine.

2. Quelques solutions de sécurité

2.1. Le firewall (pare-feu)

Le **firewall** est un logiciel ou un matériel qui joue le rôle d'une barrière entre nous et le monde extérieur.

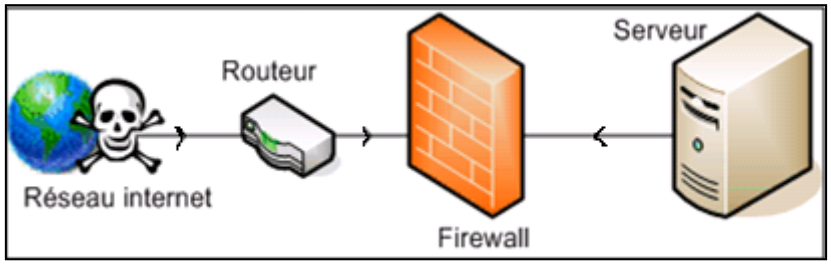


Figure 2 - Architecture d'un Firewall

Le pare-feu permet de filtrer les paquets de données échangés avec le réseau, donc il représente une *passerelle* filtrante comportant au minimum les interfaces réseau suivantes :

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

2.1.1. Contre quoi protège-t-il ?

Certains firewalls autorisent seulement le passage du courrier électronique. Ainsi, ils protègent contre toute autre attaque qu'une attaque basée sur le service de courrier. D'autres firewalls sont plus tolérants, ils bloquent uniquement les services reconnus comme étant dangereux.

En générale, les firewalls sont configurés pour empêcher tout accès non authentifiés du réseau externe. Ceci, plus qu'autre chose, protège les machines des réseaux internes contre les vandales qui essaient de s'y loger, mais laisse un accès libre aux utilisateurs s'ils veulent communiquer avec l'extérieur.

Les firewalls sont intéressants dans le sens ou ils constituent un point unique ou la sécurité peut être imposée. Tous les échanges passeront par lui. Des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux pourront être données.

2.1.2. Contre quoi ne protège t-il pas ?

Logiquement un firewall ne peut pas protéger contre des attaques qui ne passent pas par lui, ni contre les traitres et les idiots à l'intérieur de l'entreprise. Si un espion industriel décide de faire sortir des données, il y arrivera.

Les firewalls n'assurent pas parfaitement la protection contre les virus. Pour transférer des fichiers il y a différentes manière de les coder. Les utilisateurs doivent être vigilants et respecter un certains nombre de règles, la première est bien évidement de ne jamais ouvrir un fichier attaché à un mail sans être sur de sa provenance, car un firewall ne pourra pas remplacer leurs attentions et leurs consciences.

2.1.3. Les différents types de firewalls

a. Les firewalls bridge

Ce sont des firewalls très répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus. Leurs interfaces ne possèdent pas d'adresse IP, et leur rôle consiste en la transmission des paquets d'une interface à une autre en leur appliquant des règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination.

b. Les firewalls matériels

Ils sont directement intégrés dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est la simplicité d'interaction avec les autres fonctionnalités du routeur.

Leurs niveaux de sécurité est de plus très bon. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un firewall d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance son besoin et choisir le constructeur du routeur avec soin.

c. Les firewalls logiciels

Présents à la fois dans les serveurs et les routeurs, on peut les classer en :

- ***Les firewalls personnels***

Ils sont généralement commerciaux et ils sont destinés pour sécuriser un ordinateur particulier. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

- ***Les firewalls plus « sérieux »***

Ils sont généralement utilisés sous linux, car cet OS offre un niveau de sécurité élevé et un contrôle plus adéquat, en générale ils ont pour but d'avoir le même comportement que les firewalls matériels des routeurs, ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux.

2.1.4. Fonctionnement d'un système firewall

Un système firewall contient un ensemble de règles prédéfinies permettant :

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

Ces règles permettent la mise en œuvre d'une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

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

Sans nul doute la première méthode est la plus sûre, mais toutefois elle impose une définition précise et contraignante des besoins en communication. [17]

2.1.5. Les différents types de filtrages

a. Le filtrage simple de paquet « *stateless packet filtering »*

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet en

effectuant une analyse sur les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine du réseau externe, ces paquets transitent par le firewall et possèdent les en-têtes suivants :

- L'adresse IP de la machine émettrice. (identification de la machine émettrice).
- L'adresse IP de la machine réceptrice. (identification de la machine cible).
- Le type de paquet (TCP, UDP, ICMP … etc.).
- Le numéro de port [4].

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

Le tableau ci-dessous donne des exemples de règles de firewall :

Règle	Action	Ip Source	Ip destination	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	Any

Tableau 1 - Exemple de règles du firewall

Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs firewall sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables.

- **Limite**

Le premier problème vient du fait que l'administrateur réseau est rapidement contraint à autoriser un trop grand nombre d'accès, pour que le Firewall offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions TCP provenant de l'Internet avec un port supérieur à 1024. Ce qui laisse beaucoup de choix à un éventuel pirate. Enfin, ce type de filtrage ne résiste pas à certaines attaques de type IP Spoffing ou encore certaines attaques de type DOS.

[4] Un port : est un numéro associé à un service ou une application réseau.

b. Le filtrage de paquet avec état *« stateful inspection»*

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall. Le Firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques DoS.

Il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de **filtrage dynamique de paquets** est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur.

Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, ***il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications***. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

- **Limite**

Une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et réponses des clients et serveurs.

c. Le filtrage applicatif « ou pare-feu de type proxy »

Le filtrage applicatif est comme son nom l'indique est réalisé au niveau de la couche Application. Ce type de filtrage est appelé généralement « passerelle applicative» (ou *« proxy »*) car les requêtes sont traitées par le Proxy par exemple une requête de type Http sera filtrée par un processus proxy Http. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

Donc le pare-feu proxy est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif.

- **Limite**

Le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles.

2.2. Architecture DMZ

Quand certaines hôtes du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, etc.), on est souvent appeler à créer une nouvelle interface vers un réseau différent, qui est accessible de l'extérieur ainsi que du réseau interne, et cela sans risquer de nuire à la sécurité de l'entreprise. Et c'est ce qu'on appel *« zone démilitarisé »* (notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée qui contient des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

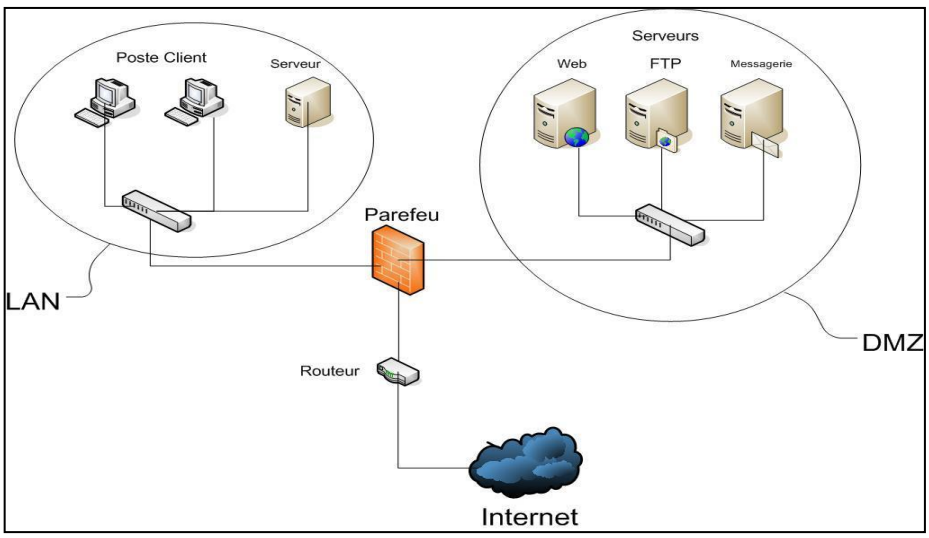


Figure 3 – Architecture DMZ

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

- Autorisation du trafic du réseau externe vers la DMZ,
- Interdire le trafic du réseau externe vers le réseau interne,
- Autorisation du trafic du réseau interne vers la DMZ,

- Autorisation du trafic du réseau interne vers le réseau externe,

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise. [17]

2.3. La cryptographie

La cryptographie permet de se protéger contre de nombreuses faiblesses de sécurité et de contrôler la sécurité des systèmes d'information. Cette science peut cependant être aussi utilisée par les auteurs de virus afin de renforcer leur caractère nocif. La cryptographie permet d'assurer l'authenticité, l'intégrité et la confidentialité des données.

2.3.1. La Cryptographie Symétrique

Elle est basée sur une clé unique partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. [2]

2.3.2. La Cryptographie Asymétriques (à clé publique)

Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés : une est privée et n'est connue que par l'utilisateur, l'autre est publique et donc accessible par tout le monde.

2.4. Les systèmes de détection d'intrusions(IDS)

Un système peut subir plusieurs attaques, il est donc nécessaire d'avoir un logiciel spécialisé capable de surveiller les données qui transitent sur ce système, et qui peut réagir si des données semblent suspectes. Les systèmes de détection d'intrusions (IDS) conviennent parfaitement pour réaliser cette tâche. [18]

2.4.1. Les différentes sortes d'IDS

Les IDS se caractérisent par leur domaine de surveillance. Celui-ci peut se situer au niveau d'un réseau d'entreprise, d'une machine hôte, d'une application…, il existe trois sortes distinctes d'IDS :

a. **La Détection d'Intrusion Réseau (N-IDS)** *(Network Based Intrusion Detection System)*

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau. Les N-IDS assurent la sécurité au niveau du réseau en utilisant principalement des capteurs qui sont souvent des hôtes dont leur seul tâche est l'analyse du trafic réseau et d'envoyer une alerte à une console sécurisée. Ils agissent de manière invisible ce qui les rend

difficile à localiser et à atteindre par un attaquant. Les capteurs peuvent être placés avant ou après le pare-feu, ou encore dans une zone sensible que l'on veut spécialement protéger.

b. La détection d'Intrusion basée sur l'hôte H-IDS (*Host Based Intrusion Detection System)*

Ils analysent seulement l'information concernant cet hôte. Ces systèmes n'ont pas à contrôler le trafic du réseau mais uniquement les activités d'un hôte donné, ce qui leur donne une grande précision sur les types d'attaques subies. [3]

c. Détection d'Intrusion basée sur une Application

Les IDS basés sur les applications sont un sous-groupe des IDS hôtes (H-IDS), mais on les mentionne séparément. Ces IDS sont mis entre l'utilisateur et son application donc contrôlent l'interaction entre un utilisateur et un programme. Puisque ils opèrent ainsi il est facile de filtrer tout comportement notable.

2.5. Les VLANs (Virtual Local Area Network)

Le commutateur (switch) a pour fonction de permettre la cohabitation de différents sous-réseaux physiques, qui ne communiquent pas nécessairement entre eux, sur le même équipement.

Pour atteindre cet objectif, le principe du VLAN (Virtual LAN) a été créé. À la base, un port du commutateur est assigné à un VLAN particulier et seuls les ports du même VLAN peuvent s'échanger de l'information. [6]

Il existe plusieurs méthodes de construction de VLAN : [7]

- **VLAN par port** : il est défini en associant chaque VLAN à un port du commutateur. Son avantage, c'est qu'il est facile d'emploi. L'inconvénient est qu'on ne définit qu'un seul VLAN par port.
- **VLAN basée sur l'adressage MAC** : il s'agit de dire quelles adresses MAC (adresses physiques) appartiennent à tel VLAN. L'avantage est que des stations sur un même port peuvent être sur des VLAN différents. L'inconvénient, c'est la difficulté de manipulation des adresses MAC.
- **VLAN par sous-réseau** (niveau 3) : il s'agit de définir, en utilisant les adresses IP *(Internet Protocol*), un VLAN par sous réseau. Cela permet une configuration plus facile. De plus, des stations sur un même port peuvent appartenir à des VLAN différents.

- **VLAN par Protocole** : est obtenu en associant un réseau virtuel par type de protocole du réseau (par exemple TCP/IP), regroupant ainsi toutes les machines utilisant le même protocole dans un même VLAN.

2.6. Les listes de contrôles d'accès (ACL)

Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole. Une ACL permet de soit autoriser du trafic (permit) ou de le bloquer (deny). Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output). Une ACL est analysée par l'IOS de manière séquentielle. Dès qu'une règle correspond au trafic, l'action définie est appliquée, le reste de l'ACL n'est pas analysé. Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté.

Conclusion

Nous avons vu en premier lieu dans ce chapitre les principes de la sécurité ; les terminologies, les objectifs fixés par la sécurité, les mécanismes d'une attaque. En deuxième lieu nous avons présenté quelques solutions qui permettent d'assurer une politique de sécurité efficace tel que le firewall, la cryptographie, les IDS, les Vlans et enfin les listes de contrôle d'accès.

Dans le chapitre qui suit, nous présenterons un élément d'interconnexion qui est le routeur et le rôle qu'il joue dans l'apport d'une bonne sécurité.

Chapitre 3

La sécurité dans les routeurs

Chapitre 3

La sécurité dans les routeurs

Introduction

Pour acheminer le trafic entre différents réseaux on peut utiliser un routeur, qui est un équipement d'interconnexion de réseaux informatiques qui permet d'assurer le routage des paquets entre deux réseaux ou plus, afin de déterminer le chemin qu'un paquet de données va emprunter.

La sécurité des routeurs est un principe crucial dans tout déploiement de sécurisation. Les routeurs sont des objectifs définis pour les attaquants d'un réseau. Si un attaquant arrive à compromettre un routeur d'accès, ce dernier peut lui être potentiellement utile. La connaissance du rôle des routeurs dans un réseau va nous aider à comprendre leurs vulnérabilités.

1. Architecture d'un routeur

À l'instar d'un ordinateur personnel, un routeur par exemple de type CISCO est équipé d'un system d'exploitation nommé **IOS** (Internet Operating System). IOS fournit des fonctionnalités qui permettent à un routeur Cisco d'envoyer et de recevoir du trafic tel que les fonctions de routage et un accès fiable et sécurisé aux ressources du réseau.

Cette plate-forme logicielle est proposée aux clients sous la forme d'images. Ces images sont chargées sur un routeur avant de commencer le processus de configuration.

Chaque routeur possède les mêmes composants de base qu'un ordinateur standard. Il est doté d'un processeur (UC), de mémoire, ainsi que de diverses interfaces d'entrée / sortie.

1.1. Composants internes

Tous les routeurs Cisco ont une architecture interne qui peut être représentée par : [19]

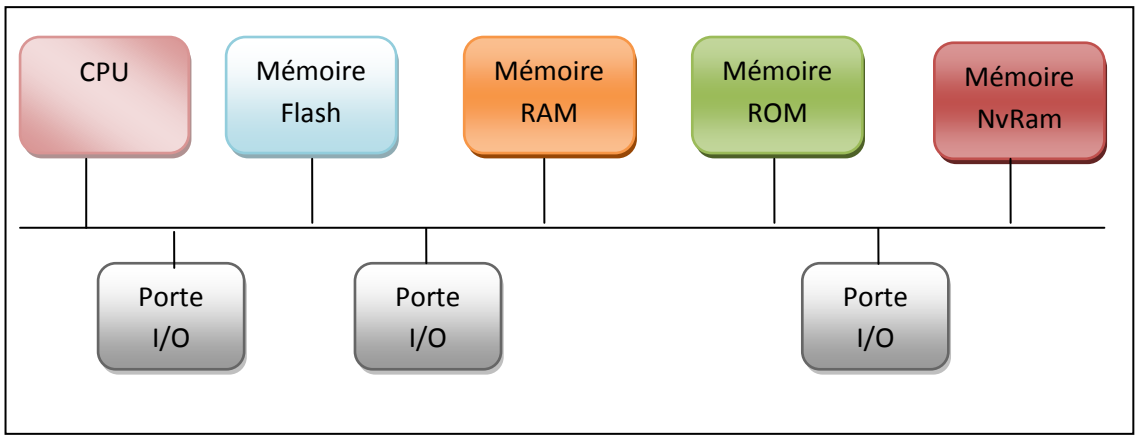


Figure 4 - Composants internes d'un routeur

- **Mémoire NvRam : (***Non-Volatile Random Access Memory*), c'est la Ram non volatile, elle est utilisée comme emplacement de stockage pour le fichier de configuration du routeur au démarrage. Elle solutionne le problème de la coupure de l'alimentation, puisqu'elle conserve les données.
- **Une mémoire ROM :** Contient le *BootStrap*, la séquence de démarrage du routeur. Cette mémoire n'est utilisée qu'au démarrage du routeur.
- **Une mémoire RAM :** Elle est utilisée par le système d'exploitation pour maintenir les informations durant le fonctionnement. Elle peut contenir les tampons, les tables de routage, la table ARP, la configuration mémoire et un nombre important d'autres choses. Et comme c'est de la RAM, lors de la coupure de l'alimentation, elle est effacée.
- **Une mémoire FLASH :** La mémoire flash représente une sorte de ROM effaçable et programmable, sur beaucoup de routeurs, la mémoire flash est utilisée pour maintenir une image IOS.
- **Unité centrale (CPU) :** L'unité centrale, ou le microprocesseur, est responsable de l'exécution du système d'exploitation (chez Cisco, c'est IOS) du routeur.
- **Les portes I/O** : l'interfaçage vers le monde extérieur est important. Chaque routeur possède des interfaces LAN qui sont en général des ports Ethernet et des interfaces WAN incluant des ports séries.

1.2. Composants externes

Les composants externe d'un routeur sont constitués d'un certains nombre de ports (console, auxiliaire), de slots (NM, WIC), d'interfaces (LAN, WAN), une alimentation et un interrupteur.

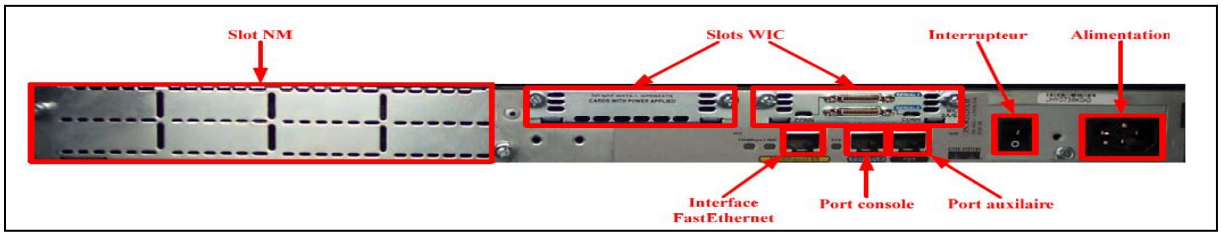


Figure 5 - Vue arrière d'un routeur Cisco

2. Fonction de routage dans les routeurs

Les routeurs assurent la fonction du routage, qui représente une façon de déterminer le trajet optimal des données entre l'expéditeur et le destinataire. Le routage est basé sur un algorithme lié au protocole de routage. L'algorithme prend en considération la durée moyenne de transmission, la charge du réseau, la longueur totale du message. Il permet au trafic provenant d'un réseau local d'atteindre sa destination après avoir traversé plusieurs réseaux intermédiaires. [1]

2.1. Table de Routage

Les routeurs disposent de tables de routage IP. Cette table contient des informations sur les destinations et la manière de les atteindre. Une entrée de table de routage contient la destination et le routeur de prochain pas (next hop) pour transmettre le datagramme.

2.2. Type de Routage

2.2.1. Routage statique

Le routage statique consiste à construire dans chaque nœud, une table indiquant pour chaque destination, l'adresse du nœud suivant. Cette table est construite par l'administrateur du réseau lors de configuration du réseau et à chaque changement de topologie. [9]

2.2.2. Routage dynamique

Le routage dynamique utilise un protocole de routage dont le principe est la diffusion périodique sur le réseau des informations de routage. Les équipements de routage échangent leurs informations de routage et mettent à jour leurs tables de routage. Pour faciliter le travail de ces protocoles de routage, il a été nécessaire de hiérarchiser la topologie d'Internet. Ce réseau est composé de systèmes autonomes(AS[5]) ayant chacun sa propre politique de routage interne, et communiquant entre eux via un protocole de routage externe. [1,15]

2.3. Protocole de Routage

Le protocole de routage définit la manière dont les routeurs s'échangent des informations afin de déterminer la meilleure route vers une destination. Il existe deux familles de protocoles de routage; les protocoles de routage Internes (IGP), et les protocoles de routage externes (EGP). [16]

2.4. Choix d'un protocole de routage

Il existe beaucoup de protocoles, en choisir un est relativement facile. Pour des réseaux locaux, RIP est le plus courant. OSPF n'est pas encore largement disponible.

Pour un protocole extérieur, on a rarement le choix du protocole. Deux systèmes autonomes qui échangent des informations doivent utiliser le même protocole. Ce choix est souvent EGP même si BGP se diffuse de plus en plus. [4]

3. Vulnérabilité des routeurs

Comme les routeurs sont des passerelles vers d'autres réseaux, ils constituent des cibles évidentes et sont soumis à une variété d'attaques. Voici quelques exemples des différents problèmes de sécurité rencontrés :

- **La configuration**

Un routeur est semblable à un ordinateur dans lequel il y a plusieurs services permis par défaut. Beaucoup de ces services sont inutiles et peuvent être utilisés par un attaquant pour la collecte d'informations ou pour l'exploitation.

[5] AS (Autonomous System) est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune.

- **Gestion du Routeur**

Le contrôle de l'accès à un routeur par des administrateurs est une tâche importante.
Il y a deux types d'accès :

- **L'accès local**

L'accès local implique une connexion directe à un port de console sur le routeur avec un terminal ou un ordinateur portable,

- **L'accès à distance**

Il représente généralement la permission Telnet, pendant l'accès à distance, les mots de passes Telnet sont envoyés en clair sur le réseau, donc une écoute sur le réseau suffit pour les connaître.
Ces failles peuvent être à l'origine des différentes attaques qui visent à prendre contrôle sur le routeur, ce qui veut dire prendre le contrôle sur l'acheminement des données dans le réseau.

4. Les routeurs et leurs rôles dans la sécurité des réseaux

Les routeurs peuvent jouer un rôle dans la garantie de la sécurité des réseaux. Ils exécutent beaucoup de travaux différents dans les réseaux modernes.
Les routeurs remplissent les rôles suivants :

- Filtre les utilisateurs ;
- Fournir un accès aux segments de réseau et aux sous-réseaux.

4.1. Filtrage des paquets

Le filtrage des paquets contrôle l'accès à un réseau en étudiant les paquets entrants et sortants, et en les transmettant ou en les stoppant en fonction de tests prédéfinis.

Un routeur filtre les paquets lors de leur transmission ou de leur annulation conformément aux règles de filtrage. Lorsqu'un paquet accède à un routeur de filtrage, certaines informations de son en-tête sont extraites. Conformément aux règles de filtrage, le routeur décide alors si le paquet peut être transmis ou rejeté. Le filtrage des paquets fonctionne sur la couche réseau du modèle OSI (Open Systems Interconnection) ou sur la couche Internet de TCP/IP.

Un routeur de filtrage des paquets, en tant que périphérique de couche 3, se réfère aux règles pour déterminer s'il doit autoriser ou refuser le trafic en fonction des adresses IP source

et de destination, du port source, du port de destination et du protocole des paquets. Ces règles sont définies en fonction des listes de contrôle d'accès.

Conclusion :

Dans ce chapitre nous avons définit qu'est ce qu'un routeur, ses composants, la fonction de routage. L'étude du routeur nous a permis de mettre en évidence les différentes failles qui peuvent infecter les routeurs, et a se poser des questions sur la façon dont on peut assurer un bon cheminement de nos donnés, ceci ne serra réalisé qu'on accordant une bonne sécurité à nos routeurs, nous allons donc présenter dans le chapitre suivant une étude détaillée sur la gestion du trafic avec des listes de contrôle d'accès, qui représente un des points important assurant une bonne sécurité.

Chapitre 4

Gestion de trafic par les listes d'accès

Chapitre 4

Gestion de trafic par les listes d'accès (ACLs)

Introduction

ACL est l'acronyme de « Access Control List » qu'on traduit par liste de contrôle d'accès. On utilisera cet acronyme ou la forme réduite **liste d'accès** car les répétions seront nombreuses.

Le but d'une liste d'accès est de définir le trafic qui devrait être autorisé ou pas à franchir le routeur, d'où le choix du terme « accès », alors qu'elle pouvait être nommés liste de contrôle de trafic, puisqu'il faut bien constater que tous les paquets ne sont pas légitimes sur le réseau, les paquets considérés comme illégales ou illégitimes doivent être interdit par le routeur. Afin de mettre en place ce filtrage, les listes d'accès représentent le moyen favorisé par les administrateurs réseaux.

Elles opèrent en fonction de l'adresse IP source, l'adresse IP de destination, du port source, port de destination, et du protocole (IP, UDP, TCP, ICMP …). Elles fonctionnent selon un ordre séquentiel et logique, en évaluant les paquets à partir du début de la liste d'instruction. [8]

Sécuriser le réseau est la principale raison qui nous incite à configurer des listes de contrôles d'accès. Ce chapitre explique comment utiliser les listes de contrôle d'accès standards et étendues. Il explique également comment les configurer sur un routeur Cisco. Avec quelques conseils, des éléments dont il faut tenir compte, des recommandations et des lignes directrices générales sur l'utilisation des listes de contrôle d'accès.

1. Rôles des listes d'accès

Les listes d'accès sont utilisées à des fins multiples, et voici les principales raisons pour lesquelles il est nécessaire de les créer : [23]

- Limiter le trafic réseau pour augmenter les performances,
- Déterminer quel type de trafic sera acheminé ou bloqué au niveau des interfaces du routeur,
- Capacité à contrôler les zones d'un accès client,

2. Principes du fonctionnement des listes d'accès

Une liste de contrôle d'accès est un groupe d'instructions, chacune d'elle comporte deux parties organisées ainsi :

> **Si** *condition_à_vérifier* **ALORS** *action*

Ces instructions définissent si les paquets sont acceptés (**permit**) donc ils pourront transiter par le routeur comme ils auraient fait en absence de liste, ou refusés (**deny**) donc les paquets seront rejetés.

Le routeur compare jusqu'à ce qu'il ait une correspondance. La condition de correspondance est examinée en premier. L'acceptation ou le refus est examiné uniquement si la condition est vraie.

Si la condition à vérifier n'est pas avérée, alors le routeur passe à l'instruction suivante quand elle existe. Si aucune correspondance n'est trouvée lorsqu'il atteint la fin de la liste, le trafic est refusé. Tout ce passe comme si la liste comportait une dernière instruction par défaut « **deny any** » qui n'apparait pas dans la liste de configuration, cette instruction interdit l'accès de tout paquet qui ne correspond pas aux instructions de la liste de contrôle d'accès.

Le trafic qui entre dans le routeur est comparé aux entrées d'ACL, donc l'ordre choisi pour les instructions qui composent la liste est très essentiel. En effet, les instructions sont lues en séquence.

Une liste est mise en œuvre sur un flux de paquet entrant sur une interface ou sur un flux de paquet sortant par une interface, si le paquet est accepté dans l'interface, il est ensuite comparé aux enregistrements de la table de routage afin de déterminer l'interface de

destination, et transmit à cette interface. Ensuite, le routeur vérifie si l'interface de destination possède une liste de contrôle d'accès.

L'organigramme suivant tente de synthétiser le cheminement d'un paquet dans une liste placé sur l'interface d'entrée.

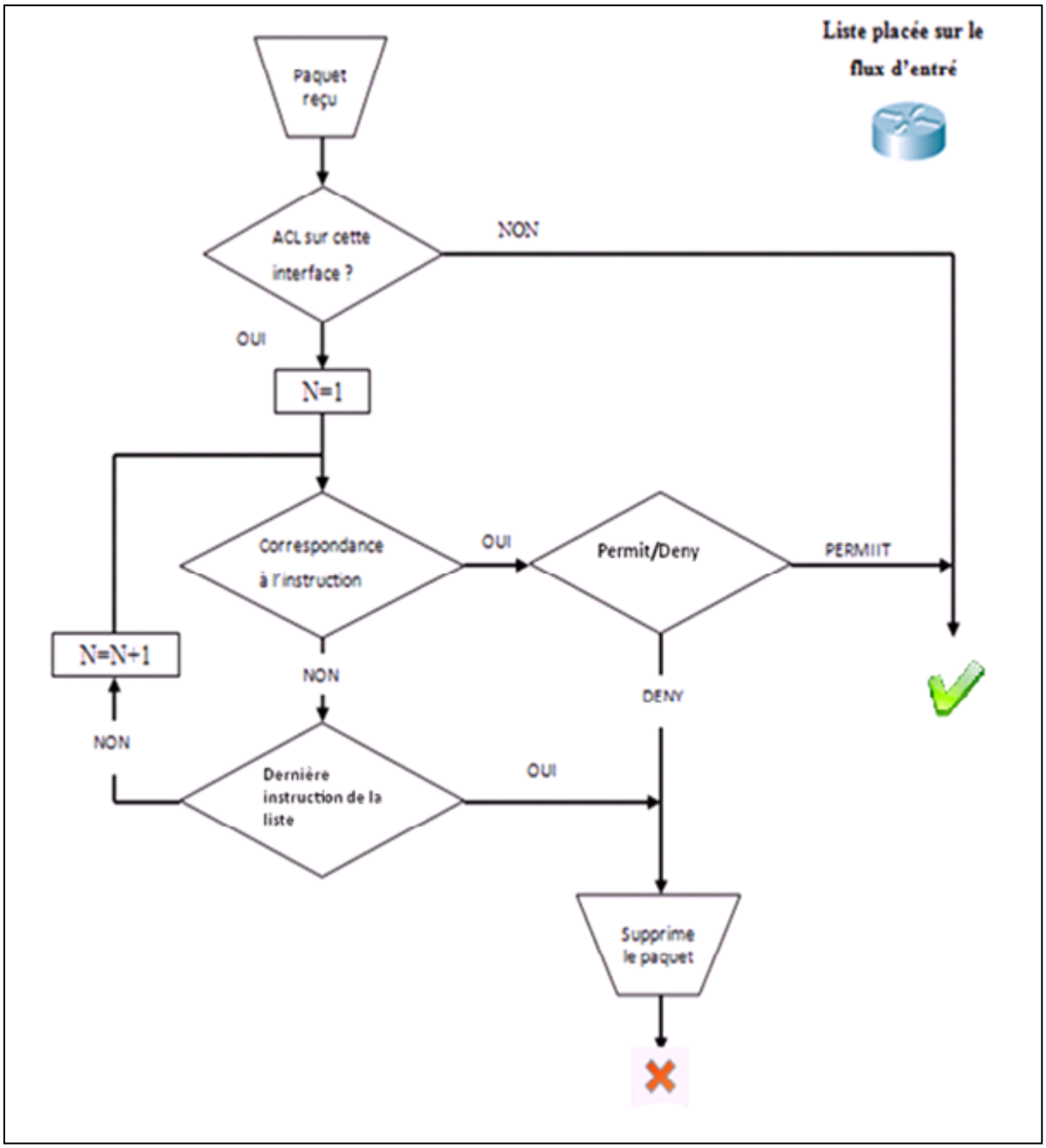


Figure 6 - Fonctionnement des listes d'accès

Ce même processus est répété quand le paquet atteint l'interface de sortie.

3. Masque générique (Wildcard Mask)

Le masque réseau a pour but d'extraire l'adresse réseau d'une adresse IP, on l'obtient on réalisant un ET logique bits à bits, entre l'adresse IP et un mot binaire ayant des « 1 » en face des bits de l'adresse réseau à retenir et des « 0 » en face de l'adresse machine à ignorer. Ce mot binaire est donc appelé masque réseau ou masque sous-réseau.

Un masque générique est l'inverse binaire d'un masque de sous-réseaux, ou, on peut dire que c'est le complément à 255 du masque de sous-réseau correspondant, quand un masque désigne les bits qu'il faut retenir, le masque générique dit quels sont les bits qu'il faut ignorer. Et quand le masque sous réseau désigne les bits qu'il faut ignorer, le masque générique dit l'inverse c'est-à-dire que ces bits représentent les bits à retenir. [8]

Un masque générique est une valeur de 32 bits divisé en quatre octets noté sous la forme décimale (comme les adresses IP et les masques de sous-réseaux), sachant que :

- "0" binaire : il y aura vérification de ce bit sur l'adresse IP de référence.
- "1" binaire : il peut varier, donc il n'y aura pas de vérification. [20]

Exemple :

Masque de sous-réseaux	**1111 1111.1111 1111.1110 0000.0000 0000**
Masque générique	0000 0000.0000 0000.0001 1111.1111 1111

Tableau 2 - Exemple de l'utilisation du masque générique

255 . 255 . 224 . 0 (Masque de sous-réseaux)

+ 0 . 0 . 31 . 255 (Masque générique)

= 255 . 255 . 255 . 255

On peut donc dire qu'un masque générique ne peut prendre que ces valeurs (pour chaque octet).

0	**1**	**3**	**7**	**15**	**31**	**63**	**127**	**255**

Exemple :

Condition de teste 128.10.0.0 (Adresse IP), 0.0.0.255 (Masque générique associé).

Nous ignorons donc l'octet de poids faible, et nous vérifions les trois octets de poids forts.

4. Les mots clés Host et Any

L'instruction {@ IP_source [masque générique] | any} permet de désigner un, plusieurs ou touts les hôtes.

Une notation améliorée est donc possible pour désigner l'ensemble des hôtes en remplaçant l'adresse IP source et masque générique par le mot-clé **any**. **0.0.0.0 255.255.255.255 ➔ any.**

La dernière instruction autorise les paquets quelle que soit leur source. De fait le rejet implicite en fin de la liste n'est plus prit en compte.

Il est aussi possible de remplacer W.X.Y.Z 0.0.0.0 qui signifie « *l'équipement W.X.Y.Z* » par l'utilisation du terme **host W.X.Y.Z**

Au lieu d'écrire à chaque fois 0.0.0.0 pour désigner le périphérique lui-même qui porte l'adresse IP indiqué. On met juste un **host** avant l'adresse IP.

5. Identification des listes d'accès

Lors de la création d'une ACL, l'administrateur peut identifier une liste en lui attribuant un nom ou un numéro unique. Quand il décide de le faire à l'aide d'un numéro, ce numéro identifie le type de la liste d'accès à mettre en place, et doit être compris dans la plage de numéros valide pour ce type.

Ce tableau représente les types de liste de contrôle d'accès ainsi que la plage de numéro correspondant :

Plage	**Description**
1 - 99, 1300 - 1999	IP standard
100 -199, 2000-2699	IP étendu
200 - 299	Ethernet type code
600 - 699	Apple Talk

700 - 799	Ethernet adress
800 - 899	Liste d'accès IPX standard
900 - 999	Liste d'accès IPX étendue

Tableau 3 - Protocoles avec ACL indiquées par numéros

Remarque :

Il n'existe aucune contrainte dans le choix du numéro de liste. Par exemple si on veut créer une première liste standard, on peut indifféremment lui attribué le numéro 1, 2,15 ou 20. De la même façon, le numéro attribué à une seconde liste n'a pas besoin de suivre le numéro attribué à la première liste.

6. Les types des listes de contrôle d'accès

Il existe plusieurs types d'ACLs comme cité dans le tableau précédent, mais le cursus de certification professionnel CCNA[6] n'envisage que les listes d'accès standard, et étendue.

6.1. Les listes numérotées standards

6.1.1. Définition

Elles sont numérotées de 1-99 ou 1300-1999, et elles représentent la forme la plus simple, elles représentent un ensemble séquentiel d'instructions d'autorisation et de refus qui s'appliquent aux adresses IP. La destination du paquet et les ports concernés ne sont pas inclus. [5]

6.1.2. Configuration d'une liste d'accès standard

Pour créer une liste standard on passe en mode de configuration globale

Figure 7 – Mode de configuration globale

[6] CCNA: Cisco Certified Network Associate. *CCNA* est une certification populaire dans les réseaux informatiques mis au point par Cisco Systems.

Après avoir accéder au mode de configuration globale on applique la règle qui nous permet de créer l'ACL standard [24]

> **Access-list** Number {**permit | deny**} @IP source [masque générique]

- ***Number*** : numéro de l'ACL. (1 – 99 ou 1300 - 1999).
- ***Permit | deny*** : Choix de l'action, autoriser ou interdire le trafic.
- ***Adresse source*** : Identifie l'adresse IP source.
- ***Masque générique*** : Toute adresse IP vérifiée par une instruction ACL se voit appliquer le masque générique correspondant à l'instruction.

Le numéro d'ACL « **Number** » est attribué à chacune des instructions qui composent la liste. Chaque nouvelle instruction créée vient s'ajouter après les instructions déjà créés (c'est à dire en bas de la liste).

Exemple :

Autoriser le trafic provenant du réseau 192.168.1.0/24, mais l'interdire pour l'hôte 192.168.1.25 de se même réseau.

> Routeur (config) # **Access-list** 2 **deny** 192.168.1.25 0.0.0.0
> Routeur (config) # **Access-list** 2 **permit** 192.168.1.0 0.0.0.255

Si les paquets sont autorisés, ils sont acheminés via le routeur vers une interface de sortie. Dans le cas contraire, ils sont abandonnés sur l'interface d'entrée.

6.1.3. Positionnement d'une liste d'accès standard

Les ACL ne prennent en compte que les adresses IP sources, elles sont souvent utilisées pour filtrer les datagrammes proche de la destination finale pour ne pas détruire un paquet important, l'exemple qui suit illustre ce concept :

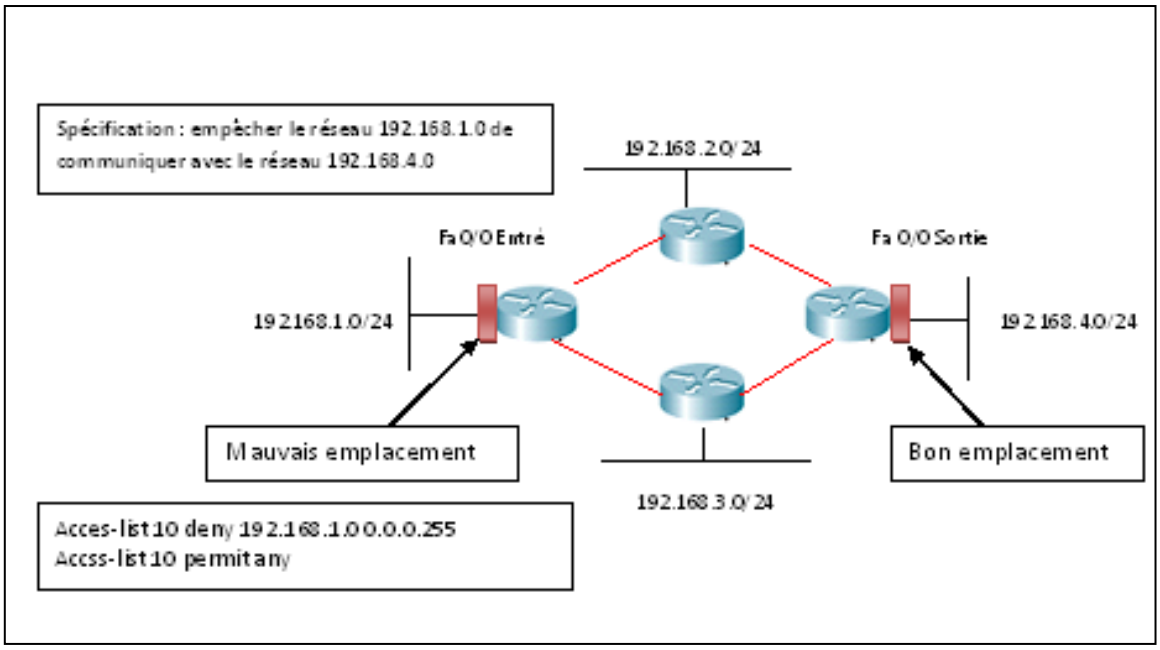


Figure 8 - Positionnement d'une ACL standard

Mauvais emplacement : Puisque si on met l'ACL 10 sur fa0/0 (entré), on empêche aussi au réseau 192.168.1.0 de communiquer avec les réseaux 192.168.2.0 et 192.168.3.0

On peut conclure que pour respecter le cahier de charge c'est-à-dire la circulation du trafic dans le réseau selon les règles définies, les listes d'accès standard doivent être placées prés de la destination, car si on place ce type de liste prés de la source, elle filtre tout, donc au fur et à mesure que l'administrateur la place loin de la source, la liste se fait de plus en plus sélective.

6.2. Les listes numérotées étendues

6.2.1. Définition

On utilise plus souvent les listes d'accès étendues que les listes d'accès standards car elles fournissent une plus grande gamme de contrôle. Elles sont numérotées de 100 -199 et 2000 – 2699, elles vérifient les adresses d'origine et de destination du paquet, mais elles peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifient les ACLs.

Pour une même liste de contrôle d'accès, plusieurs instructions peuvent être configurées, et doivent avoir le même numéro de la liste d'accès pour que toutes ces instructions soient associées à la même liste.

Le filtrage en fonction du protocole et du numéro de port nous permet de créer des listes de contrôle d'accès étendues très spécifiques.

6.2.2. Configuration d'une liste d'accès étendue

La syntaxe de la commande permettent de créer l'ACL étendue est la suivante :

> ***Routeur (config) # Access-list*** number {***permit*** | ***deny***} Protocol @IP source [masque source générique] @IP destination [masque destination générique] ***Opérateur*** Opérande

- ***Number :*** numéro de l'ACL. (100 -199 ou 2000-2699)
- ***Permit / deny :*** autoriser ou interdire le trafic.
- ***Protocole :*** Type du protocole (IP, TCP, UDP, ICMP…).
- ***Adresse source / destination :*** Identifie l'adresse IP source, et destination.
- ***Opérateur :*** Opérateur à choisir parmi les opérateurs suivant :

lt	**L**ess **t**han	Plus petit que
gt	Greater **t**han	Plus grand que
eq	**eq**ual	Egale à
neq	**N**ot **eq**ual	Différent de
range	**range**	Plage inclusive

Tableau 4 - Tableau d'Opérateur

Un opérateur placé après l'adresse source teste le port source, un opérateur placé après l'adresse destination teste le port destination.

L'opérateur **range** attend deux arguments, par exemple : range 1000 2500 donne donc un résultat vrai pour tout port compris en 1000 inclus et 2500 inclus. Les autres opérateurs n'attendent qu'un seul argument.

- ***Opérande :*** Numéro de port, optionnel, qu'il s'agisse du protocole UDP ou du protocole TCP, les champs port source et destination sont exprimés en 16 bits. Le numéro de port s'étend donc de 0 à 65535.

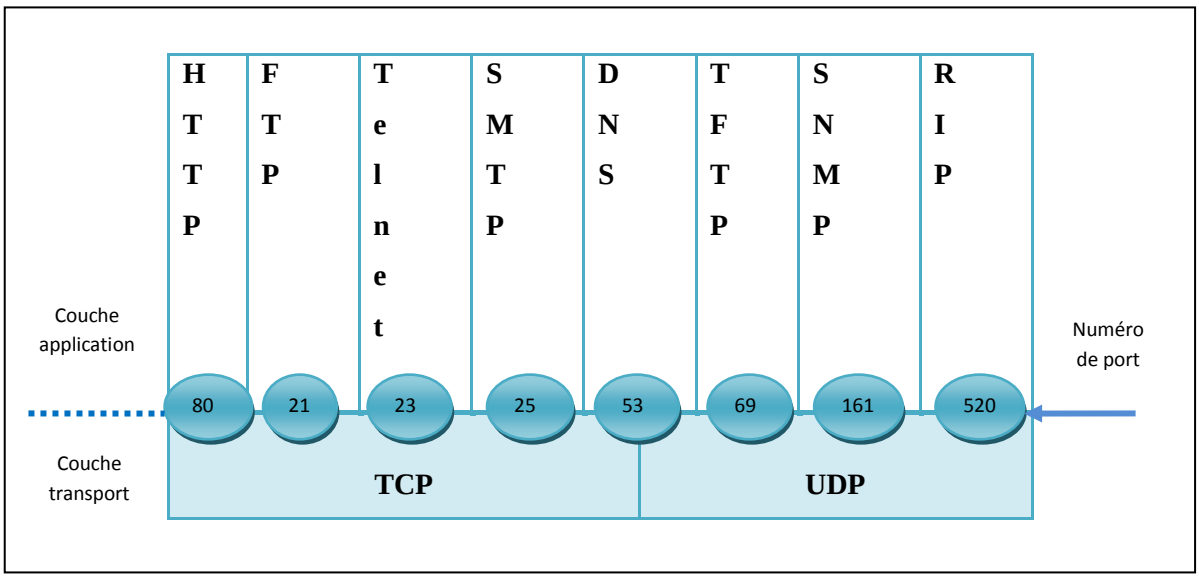


Figure 9 - Ports de couche application-transport

La commande dans la liste étendu **tcp**, ou **udp** accepte un numéro de port, ou pour quelques-uns des ports connus, un mot clé qui peut venir se substituer au numéro et augmenter la lisibilité de la configuration, tels que Telnet, FTP et SMTP.

Exemple :

- **Interdire le trafic du réseau de source 10.0.0.0/8 sur le port 80 (www) du host 192.168.1.1**

> Routeur (config) # **Access-List** 101 **deny tcp** 10.0.0.0 0.225.255.255 **host** 192.168.1.1 **eq** 80 **established**

Le mot clé **established** ne peut s'appliquer qu'aux listes étendues **tcp**. Seul TCP fonctionne en mode connecté et nécessite l'établissement du circuit virtuel (échange en trois temps). Quand le mot clé **established** est utilisé, la condition fournit un résultat vrai. Le tout premier segment de ce qui n'est à ce moment qu'une tentative d'établissement porte un drapeau **ACK** à l'état **0** (non positionné). Tout les segments qui suivent sur ce circuit ont le drapeau **ACK** positionné (égal à **un**).

- Filtrer toutes les demandes de PING (echo) entrant sur l'interface Serial 0/0 de Router avec la liste étendue 100.

> Router (config) # access-list 100 deny icmp any any echo

Router (config) #interface serial0/0

Router (config-if) # ip access-group 100 in

- **Autoriser le trafic issu du réseau interne 10.0.0.0/8 et destiné aux serveurs DNS du réseau externe.**

> Router (config) # access-list 120 permit udp 10.0.0.0 0.0.0.255 any eq 53

Le trafic DNS est transporté à l'aide du protocole de transport UDP, le port destination est le port UDP 53 affecté à l'application DNS.

6.2.3. Positionnement d'une liste d'accès étendue

Contrairement aux listes standards, les ACL étendues prennent aussi en compte les adresses de destination, la contrainte qui consistait à devoir placer la liste standard au plus près de la destination disparait, donc on doit les placées le plus proches des équipements sources concernés, afin de détruire les paquets le plus vite possible, l'exemple qui suit illustre ce concept.

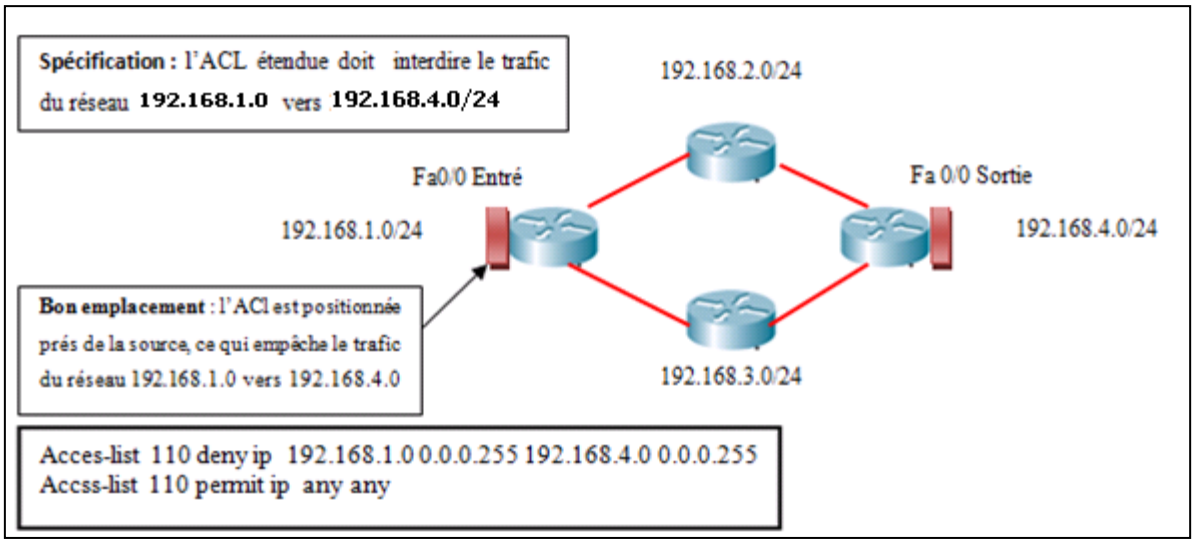


Figure 10 - Positionnement d'une ACL étendue

Une liste d'accès étendue devrait se placer sur le flux entrant de l'interface la plus proche de la source du trafic à contrôler.

6.3. Les listes d'accès nommées

Les listes d'accès nommées IP ont été introduites afin d'attribuer des noms aux ACLs standards et étendues à la place des numéros.

Elles permettent donc une identification aisée de la liste en lui attribuant un nom évocateur. [8]

6.3.1. Configuration d'une liste d'accès nommée

Il est ainsi possible de modifier le numéro qui permettait de définir le type de liste d'accès, standard ou étendue, en attribuant des noms à ces listes d'accès. La syntaxe est un peu modifiée, car on doit spécifier le type de l'ACL, la syntaxe est donc la suivante :

IP Access-list {extended | **standard}** *nom_Acl*

Exemples :

Routeur (config) **# IP Access-list standard** liste1

Routeur (config) # **IP Access-List Extended** Étudiant

6.3.2. Intérêt des listes nommées

Dans l'histoire de l'IOS, les listes d'accès nommées ont précédés les listes d'accès séquencées, car sans les listes d'accès séquencées, supprimer une instruction de la liste numérotée standard ou étendue entraînait la suppression de la liste en son entier. La seule solution était de créer des listes d'accès nommées.

6.4. Les listes d'accès séquencées

Bouleverser l'ordre des instructions incluait de supprimer complètement la liste pour la changer par une nouvelle liste. Mais dans une liste dite « séquencée », à chaque instruction est associé un numéro qui rappel l'emplacement de l'instruction dans la liste et grâce a ces numéros, il devient possible d'insérer une nouvelle instruction à un endroit prescrit dans une liste existante ou encore de supprimer une instruction sans devoir supprimer toute la liste. [8]

Exemple d'application :

On crée une liste d'accès séquencée appelée **Séquence**

```
Router (config) # IP Access-list standard Séquence
Router (config-std-nacl)# permit 192.168.0.0 0.0.0.255
Router (config-std-nacl)# permit 192.168.1.0 0.0.0.255
Router (config-std-nacl)# deny 192.168.0.0 0.0.3.255
```

Pour visualiser le contenu de la liste Séquence, on insère la commande suivante :

```
Router # show access-list Séquence
        Standard IP access list Séquence
                10 permit 192.168.0.0 0.0.0.255
                20 permit 192.168.1.0 0.0.0.255
                30 deny 192.168.0.0 0.0.3.255
```

Pour supprimer l'instruction qui porte le numéro de Séquence 30.

```
Router (config) # ip access-list standard Séquence
Router (config-std-nacl)# no 30
```

Autre nouveauté permise par cette version de l'IOS, la commande **do** qui évite d'avoir à ressortir du mode de configuration en cours pour observer les commandes déjà entrées.

```
Router (config-std-nacl) # do show ip access-list Séquence
        Standard IP access list Séquence
                10 permit 192.168.0.0 0.0.0.255
                20  permit 192.168.1.0 0.0.0.255
```

6.5. Listes d'accès datées

Une liste d'accès datée permet de restreindre le trafic en se basant sur des critères de temps ou de date, ça peut être l'heure de la journée, le jour de la semaine.

Une instruction fondée sur le temps utilise en argument une plage de temps qui doit être définie au préalable, les commandes qui permettent de définir cette plage de temps sont :

- **time-range** : Crée une plage de temps et lui attribue un nom. L'exécution de cette commande fait entrer dans un sous-mode qui contient deux autres commande **absolute** et **periodic** :

  - **Absolute** : Définit un intervalle de temps borné par une date de début et une date de fin la syntaxe générale de cette commande est :

    > **Absolute** [**start** temps date] [**end** temps date]

  - **Periodic :** Cette commande est utile quand il faut définir une plage de temps se reproduisant de façon récurrente. En voici la syntaxe :

    > **Periodic** les jours de la semaine hh : mm **to** les jours de la semaine hh : mm

Exemple:

> Routeur (config) # **access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range AccésTelnet**
> Routeur (config-time-range) # **absolute start** 10:00 12 septembre 2012
> Routeur (config-time-range) # **periodic** Monday Tuesday 10:00 **to** 18:00

Dans cet exemple, nous autorisons l'accès Telnet aux utilisateurs du réseau **10.1.1.0** sur le réseau **172.16.1.0** à partir du **12 Septembre 2012** à **10h**, deux jours par semaines, du **Lundi** au **Mardi** et de **10h** à **18h**.

Les listes de contrôle d'accès basées sur le temps offrent les avantages suivants [14] :

- Elles renforcent le contrôle des administrateurs réseau en autorisant ou en refusant l'accès aux ressources.
- Elles permettent aux administrateurs réseau de contrôler les messages de journalisation. Les entrées des listes de contrôle d'accès peuvent enregistrer le trafic à certains moments de la journée, mais pas tout le temps.

7. Application d'une liste d'accès à une interface

Une liste d'accès comportant une suite d'instructions de filtrage va être appliquée sur une interface du routeur, pour le trafic entrant ou pour le trafic sortant. [21]

Une ACL n'a aucun effet sur le trafic tant qu'elle n'a pas été activée.

L'administrateur active la liste on l'appliquant à une interface, à une ligne console ou aux lignes vty à l'aide des commandes suivantes :

- **Mettre une ACL sur une interface**

> Router (Config) # **interface** [type + port]
>
> Router (Config-if) # *protocol-name* **access-group** [number | name **[in** | **out]**]

- **Mettre une ACL sur une ligne console ou vty**

> Router (Config) # line [console | vty] num
>
> Router (Config-line) # *protocol-name* ***access-class*** [number | name [in | **out]**]

On associe donc à chaque interface du routeur une ACL, on peut aussi préciser le sens du trafic, c'est à dire ***in*** ou ***out***, selon qu'on souhaite que l'ACL s'applique aux paquets entrant dans le routeur ou bien aux paquets qui quittent le routeur par une interface donnée. [22]

Une ACL de type **in** est associée à une interface qui contrôle le trafic entrant dans le routeur.

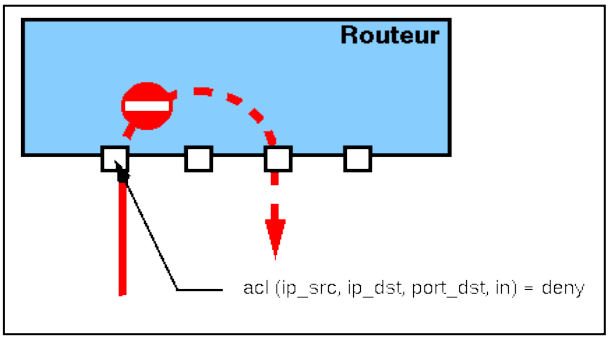


Figure 11 - ACL de type « in »

Une ACL de type **out** est associée à une interface qui contrôle le trafic qui quitte le routeur.

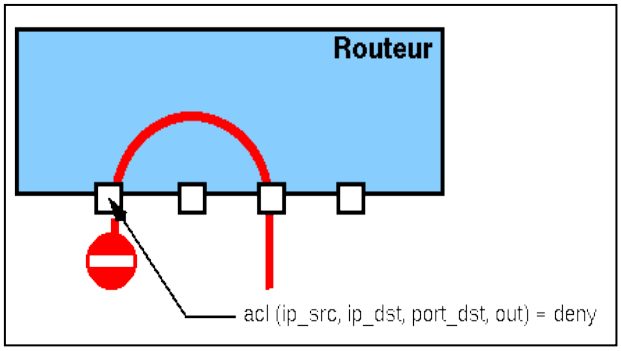


Figure 12 - ACL de type « out »

Exemple:

- Par exemple pour appliquer la liste numéro 10 sur le flux du protocole IP entrant de l'interface fa 0/0, l'administrateur utilise la commande suivante :

  Router (Config) # interface FA 0/0

  Router (Config-if) # **ip access-groupe** 10 **in**

- On veut restreindre les connexions à une ligne virtuelle vty, le protocole choisi est Telnet. La commande correspondante s'applique en configuration de ligne :

  Router (Config) # line vty 0 5
  Router (Config-if) # ip **access-class**10 **out**

En premier lieu il peut sembler un peu bizarre de filtrer l'accès Telnet selon qu'il entre ou qu'il sort. En réalité ce n'est pas le flux de parquets qui est contrôlés ici mais l'établissement de session. Quand il s'agit de restreindre l'établissement d'une session Telnet sur cet équipement, c'est l'argument "in" qui convient. Quand il s'agit d'interdire l'établissement d'une autre session Telnet sur un second équipement depuis la session hôte ouverte sur le premier équipement, c'est l'argument "out" qui s'applique.

7.1. Régle des 3 P

L'IOS accepte de nombreuses listes dans le fichier de configuration mais limite leur application sur les interfaces. Impossible par exemple d'appliquer deux listes IP sur le flux entrant d'une même interface.

Il faut faire très attention cependant au comportement de l'interface ILC qui ne génère aucun message d'erreur quand on applique une ACL sur un flux d'interface qui contient déjà une liste ajouté avant, l'interface se contente de remplacer l'ancienne liste par la nouvelle.

En revanche, toujours pour une même interface, il est possible d'appliquer une liste d'accès sur le flux entrant, une autre sur le flux sortant.

La règle est donc la suivante : [8]

On peut appliquer donc une liste d'accès **par** interface, **par** protocoles et **par** sens de flux. Cisco nomme cette règle la règle des 3 P ;

- **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 pour une interface, telle que Fast Ethernet 0/0.

Soyons un peu plus concret sur ce point en imaginant un routeur dote de deux interfaces, mettant en œuvre les trois protocoles IP, TCP, et UDP. Ce routeur se voit donc appliquer jusqu'à 12 listes d'accès.

8. Edition des listes d'accès

Dans les anciennes versions de l'IOS la modification d'une liste d'accès nécessitait une attention particulière. Puisque la suppression d'une instruction entrainait la suppression de l'ACL entière. Il était aussi impossible d'ajouter une instruction entre deux instructions existantes. Une nouvelle instruction était ajoutée automatiquement en bas de liste en cour d'édition. [8]

Donc pour pouvoir ajouter des instructions de condition supplémentaires dans une liste d'accès, l'administrateur devait supprimer toute la liste et recréer une autre avec de nouvelles instructions.

Ce problème a été résolue avec les listes d'accès séquencées, cependant, ce ne sont pas toutes les versions de l'IOS qui offrent cette option.

La création, la mise à jour, le debuggage nécessitent beaucoup de temps et de rigueur dans la syntaxe. Il est donc conseillé de créer les listes d'accès à l'aide d'un éditeur de texte (bloc note) et de faire un copier/coller dans la configuration du routeur.

9. Désactivation d'une liste d'accès

Pour désactiver une ACL, (comme toujours selon la logique Cisco), les manipulations sont les mêmes que pour l'activer, en utilisant le mot clé « **no** » devant la commande. [25]

Exemple :

> Routeur (config) # **no acces-list {numéro}**

Utilisez la commande **show access-lists** pour s'assurer que la liste a été supprimée.

10. Les commentaires sur les listes de contrôle d'accès

On peut utiliser la commande **remark** pour inclure des commentaires (remarques) sur les entrées de toute ACL standard ou étendue. Les remarques rendent l'ACL plus facile à comprendre et à analyser. Chaque remarque est limitée à 100 caractères.

La remarque peut être placée avant ou après un **permit** ou un **deny**. On doit juste faire attention ou on doit mettre la remarque de sorte qu'il soit clair que cette remarque décrit le trafic à autoriser ou le trafic à refuser.

Pour commenter des listes de d'accès, on utilise donc la commande de configuration globale ***access-list*** **numéro-liste-accès** ***remark*** **remarque**. Pour supprimer une remarque, utilisez la forme **no** de cette commande. [8]

Pour une entrée dans une liste de contrôle d'accès nommée, on utilise la commande de configuration **remark access-list**. Pour supprimer la remarque, utilisez la forme **no** de cette commande.

Exemple :

- **Liste d'accès numérotée**

> Routeur (config) **# IP Access-list** 1 **remark** permettre tout le réseau
>
> Routeur (config) **# IP Access-list** 1 permit 192.168.10.0 0.0.0.255

- **Liste d'accès nommée**

> Routeur (config) **# IP Access-list** extended NoTelnet
>
> Routeur (config-ext-nacl) **# remark** ne pas permettre l'accès telnet à l'uilisateur
>
> Routeur (config-ext-nacl) **# deny tcp host** 192.168.10.5 any **eq telnet**

11. Visualisation et vérification d'une liste d'accès

On utilise la commande **show access-lists** pour afficher le contenu de toutes les listes de contrôle d'accès, et la commande **show access-lists** suivie du nom ou du numéro d'une liste de contrôle d'accès pour afficher le contenu de cette liste d'accès. [20]

Conclusion

Ce chapitre nous a permit de comprendre la notion de listes de contrôle d'accès. Et en résumé on peut dire que les liste d'accès permettent de vérifier les adresses c'est-à-dire d'autoriser ou de refuser des hôtes, des plages d'adresses ou des protocoles vers d'autres réseaux données. Ces ACLs sont utilisées pour réduire le trafic et permettre de diminuer la surcharge du réseau. Ces règles jouent aussi un rôle dans la sécurité en protégeant des parties du réseau, et ainsi établir une base solide pour la sécurisation de niveau supérieur(niveau applicatif).

Dans le chapitre qui suit, nous allons donner quelques exemples d'application des listes d'accès.

Chapitre 5

La mise en œuvre des listes d'accès

Chapitre 5

La mise en œuvre des listes d'accès

Introduction

L'un des points essentiel du travail d'un administrateur ou technicien réseau est de configurer des services sécurisés. Les fonctionnalités abordées dans les chapitres précédents sont très importantes dans les réseaux et ne peuvent s'arrêter à cause d'une faille de sécurité. Les points abordés dans ce chapitre concernent la configuration de la sécurité d'accès au niveau d'un routeur, la mise en place des listes d'accès représente une option basique qui permet d'assurer une sécurité accru.

1. Présentation de l'architecture

Nous créerons nos scénarios sur l'architecture ci-dessous qui représente un ensemble de réseaux locaux répartis en trois zones (Zone 1, 2, 3) connectés à un réseau externe par l'intermédiaire d'un Fournisseur d'Accès Internet (FAI), les adresses IP qu'on a attribué à l'ensemble des périphériques des réseaux locaux sont des adresses IP privées, celles du réseau externe sont des adresses publiques. Et pour la configuration de ces périphériques on a fait recours au logiciel de simulation **Packet Tracer** (voir l'ANNEXE C).

Nous nous référons donc dans nos exemples sur cette architecture, la création d'une topologie est assez complexe mais hors sujet. Nous avons donc créé cette architecture dans le seul but de bien comprendre le bon fonctionnement des listes d'accès. Elle est simplifiée et est mieux adaptée pour nos scénarios :

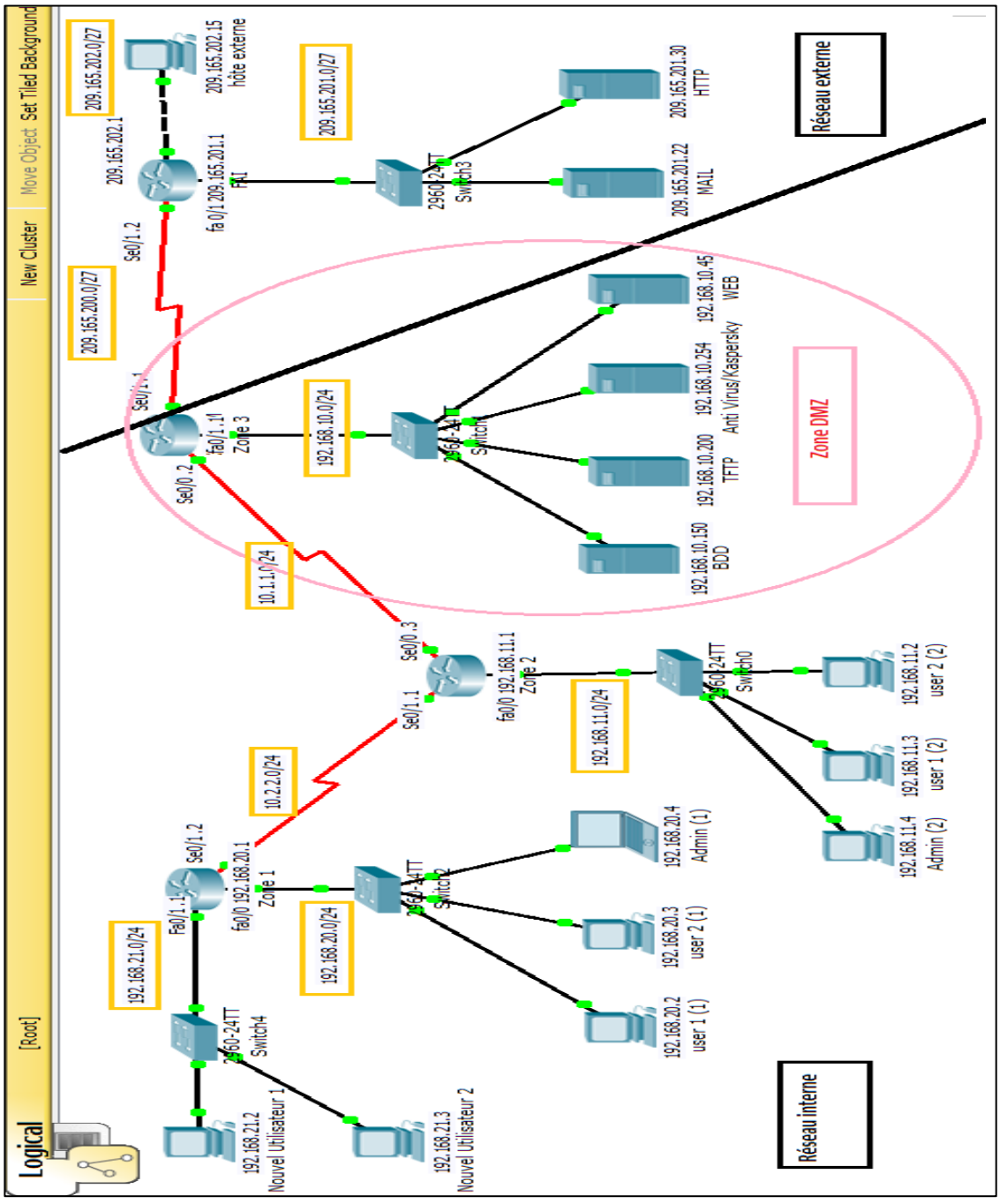


Figure 23 - Présentation de l'architecture

Le tableau suivant donne l'ensemble des périphériques, interfaces et leurs adresses :

Périphérique	Interface	Adresse IP	Masque de sous réseaux
Zone 1	FA 0/0	192.168.20.1	255.255.255.0
	FA 0/1	192.168.21.1	255.255.255.0
	SE 0/1	10.2.2.2	255.255.255.0
Zone 2	SE 0/1	10.2.2.1	255.255.255.0
	SE 0/0	10.1.1.3	255.255.255.0
	FA 0/0	192.168.11.1	255.255.255.0
Zone 3	SE 0/0	10.1.1.2	255.255.255.0
	FA 0/1	209.165.200.1	255.255.255.0
	FA 0/1	192.168.10.1	255.255.255.0
Nouvel Utilisateur 1	Carte réseau	192.168.21.2	255.255.255.0
Nouvel Utilisateur 2	Carte réseau	192.168.21.3	255.255.255.0
User1 (zone1)	Carte réseau	192.168.20.2	255.255.255.0
User2 (zone1)	Carte réseau	192.168.20.3	255.255.255.0
Admin (zone1)	Carte réseau	192.168.20.4	255.255.255.0
Admin (zone2)	Carte réseau	192.168.11.4	255.255.255.0
User (zone2)	Carte réseau	192.168.11.3	255.255.255.0
User (zone2)	Carte réseau	192.168.11.2	255.255.255.0
Web	Carte réseau	192.168.10.45	255.255.255.0
BDD	Carte réseau	192.168.10.150	255.255.255.0
TFTP	Carte réseau	192.168.10.200	255.255.255.0
Anti Virus/Kaspersky	Carte réseau	192.168.10.254	255.255.255.0
Admin (zone3)	Carte réseau	192.168.10.2	255.255.255.0
FAI	SE 0/1	209.165.200.2	255.255.255.224
	FA 0/0	209.165.202.1	255.255.255.224
	FA 0/1	209.165.201.1	255.255.255.224
MAIL	Carte réseau	209.165.201.22	255.255.255.224
http	Carte réseau	209.165.201.30	255.255.255.224
hôte externe	Carte réseau	209.165.202.15	255.255.255.224

Tableau 5 - Table d'adressage

2. Configuration de base d'un routeur

Avant de procéder à la mise en œuvre des listes d'accès sur l'architecture on doit d'abord configurer chaque routeur (Zone1, Zone 2, Zone3).

a. Configuration du nom de routeur

```
Router > enable
Router # Configuration terminal
Router (config) # hostname nom_du_routeur
```

nom_du_routeur représente dans notre exemple : Zone 1, Zone 2, Zone 3, FAI.

b. Configuration d'une interface du routeur

- **Passage en mode de configuration d'interface**

Chaque interface possède un type (Serial, Ethernet, FastEthernet), et doit avoir une adresse IP et un masque de sous réseau :

```
Router (config) # interface type port
Router (config-if) # ip address <@IP de l'interface > <masque sous réseau>
```

- **La détermination du taux de transmission ou top d'horloge : *clock rate***

Dans le cas des liaisons **série** (entre les routeurs), l'horloge doit être activée en spécifiant sa fréquence à l'aide de la commande :

```
Router (config-if) # clock rate <fréquence>
```

c. Activation de l'interface

La commande qui suit permet d'activer

```
Routeur (config-if) # no shutdown
```

d. Configuration de la fonction du routage

Nous allons appliquer sur chaque routeur d'une des trois zones ainsi que le FAI la fonction de routage, avec le protocole de routage **RIP** (Routage dynamique). Ce qui donne aux périphériques l'accès vers tous les autres emplacements.

La commande permettant de configurer le routage RIP sur un routeur est la suivante :

Routeur (config) # **router rip**

Routeur : Zone1, 2, 3, FAI.

Routeur (config) # **network [**network address**]**

Network_address : les réseaux physiquement connectés au routeur.

e. Commande d'enregistrement de la configuration courante

Après avoir configuré les noms des routeurs, interfaces et fonction de routage, on doit sauvegarder la configuration actuelle pour la réappliquer automatiquement en cas de redémarrage du routeur. La commande qui nous permet la sauvegarde s'exécute en mode Privilégié :

Routeur # **copy running-config startup-config**

f. Commande de visualisation de la configuration

La commande qui permet d'afficher la configuration est :

Routeur # **show** running-config

La configuration de chaque routeur doit être similaire à celle-ci :

```
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.1.1.2 255.255.255.0
!
interface Serial0/1
 ip address 209.165.200.1 255.255.255.224
 clock rate 9600
!
router rip
 network 10.0.0.0
 network 192.168.10.0
 network 209.165.200.0
```

Figure 14 - Configuration d'un routeur

g. Vérification de la connectivité

Avant d'appliquer les listes de contrôle d'accès, il est important de vérifier qu'on dispose d'une connectivité complète. Bien que la table de routage soit utile pour évaluer l'état du réseau (**show ip route**), on peut cependant tester la connectivité à l'aide de la commande **PING**.

h. Mesures de base de la sécurité du routeur

Les routeurs présentent plusieurs types et niveaux d'accès (Telnet, ligne virtuelle (vty), ligne auxiliaire, mode enable, etc.). Chacun de ces accès est protégé par un mot de passe.
Une politique de mot de passe doit être définie et appliquée pour éviter leur compromission. Voila donc quelque niveau d'accès et la façon dont on doit les configurer.

- **Mot de passe de console** : Ce mot de passe limite l'accès au périphérique par une connexion console.

```
Router (config) # line console 0
Router (config-line) # password cisco
Router (config-line) # login
```

Mot de passe console

- **Application d'un mot de passe à l'accès Privilégié :** On doit, se connecter en mode privilégié, puis en mode de configuration globale pour effectuer cette manipulation :

```
Router (config) # enable password cisco
Router (config) # enable secret cisco
Router (config-line) # login
```

Attribution normale

Attribution cryptée

- **Configuration de l'accès Telnet au routeur**

Il est possible d'autoriser les administrateurs à se connecter au routeur via une session Telnet à partir de n'importe quel poste.

```
Router (config) # line vty 0 4
Router (config-line) # password cisco
Router (config-line) # login
```

5 sessions Telnet

Remarque :

Il est recommandé d'utiliser des mots de passe différents pour chacun de ces niveaux d'accès. En effet, bien que l'utilisation de plusieurs mots de passe différents ne facilite pas l'ouverture d'une session, cette précaution est nécessaire pour protéger convenablement l'infrastructure réseau contre l'accès non autorisé.

Les mots de passe doivent aussi être changés suivant une périodicité. Ils doivent être fort c'est-à-dire composé de chiffres, caractères spéciaux (@§!&#), majuscules et minuscules. Ceci permet d'éviter les attaques par dictionnaire ou par force brute.

Dans notre exemple on a pris **cisco** comme mot de passe pour tous les niveaux de sécurité, juste a fin de faciliter la tâche.

3. Les listes d'accès standards numérotées et nommées

Les listes standards définissent l'action d'autoriser ou de refuser des paquets en fonction de l'adresse IP source sur un routeur. Les exemples qu'on va proposer portent principalement sur la configuration de listes de contrôle d'accès standard numérotées et nommées, l'application de ces listes aux interfaces des routeurs, ainsi que sur la vérification et le test de leurs mise en œuvre.

3.1. Configuration des listes d'accès standards numérotées

Avant de passer à la configuration des listes d'accès standards rappelons que :

- La syntaxe de la commande qui permet de créer une liste standard est :
  Access-List Number {**permit | deny**} @IP source [masque générique]
- Les listes d'accès standards sont configurées en mode de configuration globale.
- Pour les listes d'accès standards, utilisez un nombre entre 1 et 99.

Exemple d'application :

Scénario :

Les nouveaux utilisateurs (1, 2) placés sur le réseau **192.168.21.0/24** ont le droit d'accéder à l'ensemble des ressources du réseau à l'exception du réseau **192.168.10.0/24**.

Procédure :

Pour résoudre se problème on utilise la liste d'accès suivante :

> Routeur (config) # **Access-List** 1 **deny** 192.168.21.0 0.0.0.255
>
> Routeur (config) # **Access-List** 1 **permit** any

La première instruction refuse l'accès du réseau **192.168.21.0** vers le réseau **192.168.10.0**, tandis que la deuxième instruction autorise l'accès vers tout autre emplacement.

Maintenant on doit choisir le routeur qui va recevoir cette liste, comme le montre bien le schéma ci-dessous, six interfaces sont placées entre le réseau 192.168.21.0 et le réseau 192.168.10.0/24.

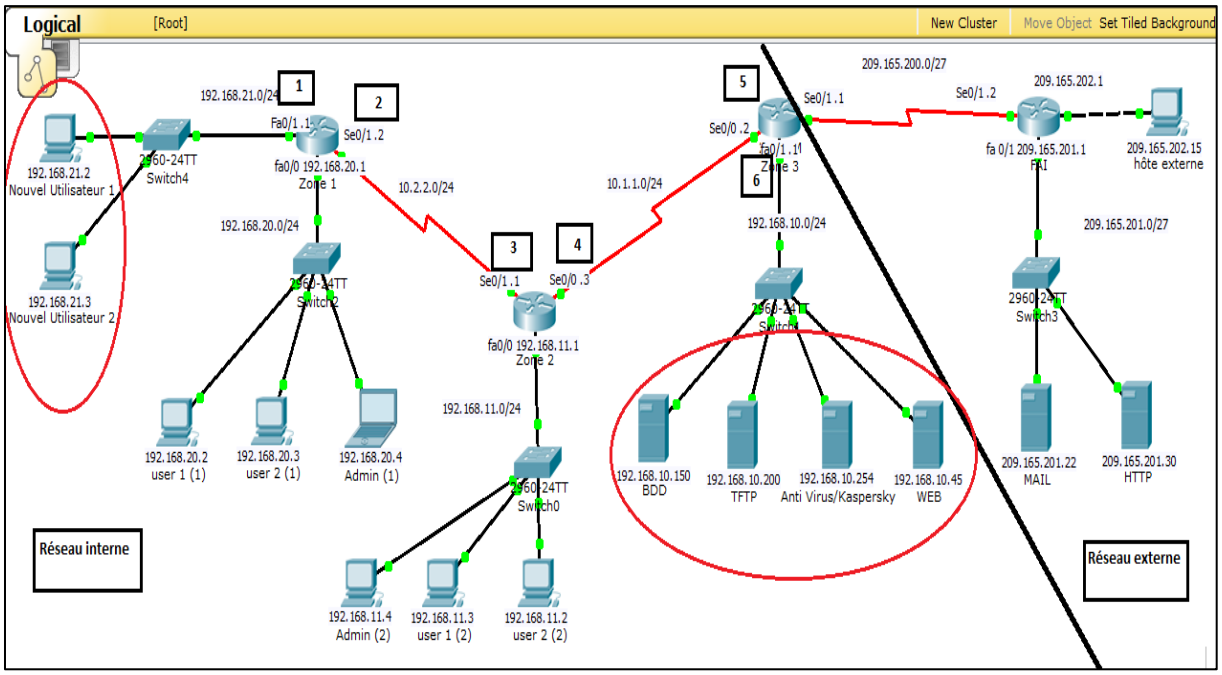


Figure 15 - Exemple de l'exigence 1

Essayons de placer la liste d'accès « **1** » sur chacune des interfaces successivement et observons les résultats et les conséquences dans le tableau qui suit :

Repère	Routeur	Interface	In / Out	Accès au réseau			
				192.168.20.0	192.168.11.0	192.168.10.0	209.165.200.224
1	Zone 1	Fa 0/1	In	NON	NON	NON	NON
2	Zone 1	Se 0/1	Out	OUI	NON	NON	NON
3	Zone 2	Se 0/1	In	OUI	NON	NON	NON
4	Zone 2	Se 0/0	Out	OUI	OUI	NON	NON
5	Zone 3	Se 0/0	In	OUI	OUI	NON	NON
6	Zone 3	Fa 0/1	Out	**OUI**	**OUI**	**NON**	**OUI**

Tableau 6 - Essai de la liste d'accès « 1 » sur les différentes interfaces

Comme le résultat qu'on veut obtenir est d'interdire l'accès au réseau **192.168.10.0** et l'autoriser vers les autres réseaux, l'ACL **1** doit être placée sur le routeur Zone3 qui est le plus proche de la destination, sur le flux sortant (**out**).

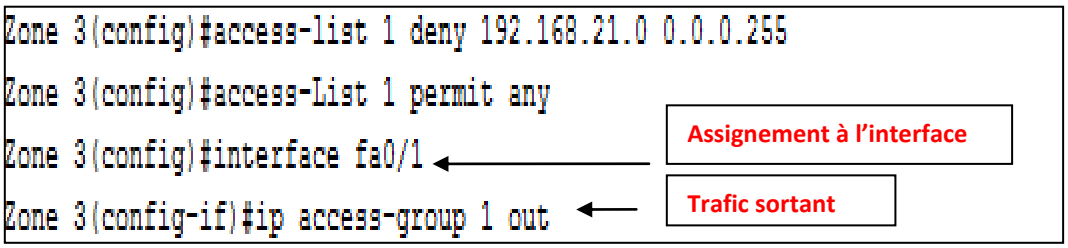


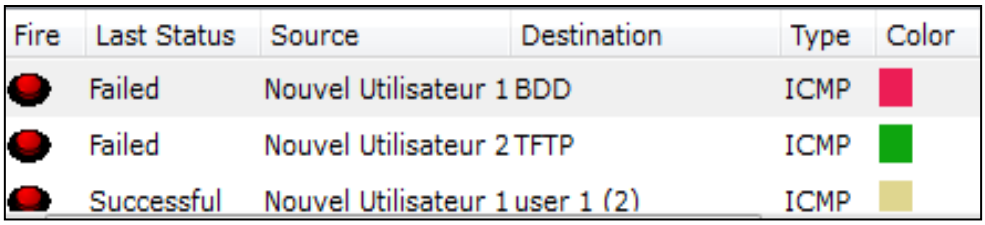
Figure 16 - Configuration de l'ACL 1

La commande **IP Access-group 1 out** permet appliquer la liste d'accès standard « **1** » en sortie de l'interface **fa0/1**.

Teste des résultats :

Une fois qu'on a configuré et appliqué l'ACL, les nouveaux utilisateurs (1,2) ne peuvent pas être en mesure d'envoyer des requêtes **PING** au réseau **192.168.10.0/24**, mais ils sont libres de communiquer avec les autres périphériques. Pour tester cette bonne fonctionnalité, on va tenter de faire un **PING** vers le **Serveur BDD** à partir de l'un des **« Nouvel utilisateur »** du réseau 192.168.21.0

Le résultat du teste est illustré dans la figure suivante :



Fire	Last Status	Source	Destination	Type	Color
	Failed	Nouvel Utilisateur 1	BDD	ICMP	
	Failed	Nouvel Utilisateur 2	TFTP	ICMP	
	Successful	Nouvel Utilisateur 1	user 1 (2)	ICMP	

Figure 17 - Résultat du teste après application de l'ACL 1

On voit bien que la requête **PING** envoyée du **nouvel Utilisateur 1** vers le **serveur BDD** a échoué (**Failed**), ainsi que la requête du **nouvel Utilisateur 2** vers le **serveur TFTP**, mais le PING du **nouvel Utilisateur 1** vers **utilisateur 1** du réseau 192.168.20.0 est bien reçu d'où le résultat (**Successful**). On déduit donc que L'ACL **1** a été bien appliquée.

3.2. Configuration des listes d'accès standards nommées

La syntaxe de la commande qui permet de créer une liste standard est :

> **IP Access-List {extended | standard}** *nom_Acl*

Exemple d'application :

Scénario :

Pour éviter la distraction des utilisateurs placés dans le réseau **192.168.20.0/24**, Nous leur interdisons d'accéder au réseau externe. Seul l'administrateur pourra y accéder.

Procédure :

Pour cette procédure, nous avons utilisé une liste d'accès standard nommée « **interdire** » qui vas rejeter toute tentative d'accès des utilisateurs 1 et 2 vers le réseau externe mais on laissant un libre accès à l'administrateur.

La commande suivante nous permet de créer une ACL standard nommée assignée en sortie, à l'interface Se 0/1 du routeur le plus proche du réseau externe (**Zone3**).

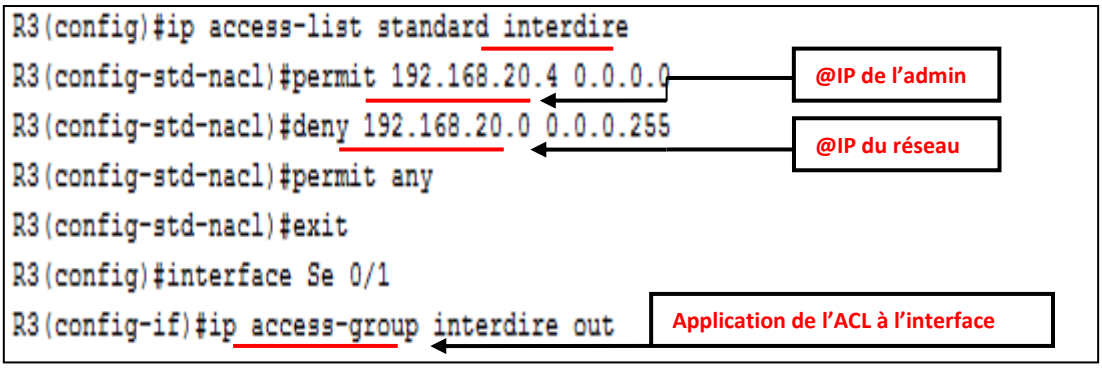


Figure 18 - La liste d'accès standard nommé « interdire »

Teste des résultats :

Après avoir appliqué l'ACL « **interdire** » sur le réseau **192.168.20.0**, les utilisateurs 1 et 2 n'ont plus le droit de se connecter au réseau externe, mais l'administrateur reste libre, et voici le résultat du **PING**.

Fire	Last Status	Source	Destination	Type	Color
	Failed	user 1 (1)	MAIL	ICMP	
	Failed	user 2 (1)	HTTP	ICMP	
	Successful	Admin (1)	MAIL	ICMP	

Figure 19 - Résultat des PING après application de l'ACL « interdire »

4. Les listes d'accès étendues numérotées et nommées

Les listes d'accès étendues sont des scénarios de configuration du routeur qui décrivent si celui-ci accepte ou refuse des paquets selon l'adresse source ou destination, ainsi qu'en fonction du protocole ou du port. Les listes d'accès étendues présentent une meilleure souplesse et une plus grande précision que les listes d'accès standards. Ces exemples portent principalement sur la définition de critères de filtrage, la configuration de listes d'accès étendues, l'application de ces listes aux interfaces des routeurs, ainsi que sur la vérification et le test de leur mise en œuvre.

4.1. Configuration des listes d'accès étendues numérotées

Rappelons d'abord que :

- la syntaxe des listes d'accès étendues numérotées est :

Access-List number {***permit*** **|** ***deny***} Protocol @IP source [masque source générique] @IP destination [masque destination générique] ***Opérateur*** Opérande

- Placer les listes d'accès étendues au plus près que possible de la source du paquet pour le détruire plus vite.
- Pour les listes d'accès étendues, on utilise un nombre entre 100 et 199.

Exemple d'application :

Scénarios :

1) Pour le réseau **192.168.11.0/24**, bloquez l'accès Telnet aux utilisateurs vers tous les emplacements, et l'autoriser à l'administrateur.
2) Prévenir les attaques de type « spoofing ».
3) Protéger le réseau interne.

Procédure 1: Pour le réseau 192.168.11.0/24, bloquez l'accès Telnet aux utilisateurs vers tous les emplacements, et l'autoriser pour l'administrateur.

La liste qui prend en charge cette restriction est configurée sur le routeur « Zone2 » et appliquée en entrée de l'interface Fast Ethernet 0/0.
En mode de configuration globale, on configure la liste de contrôle d'accès avec le numéro **110**. On souhaite tout d'abord autoriser le trafic Telnet vers tout emplacement pour l'administrateur du réseau 192.168.11.0/24 et le bloquer à toutes les autres adresses IP de ce même réseau :

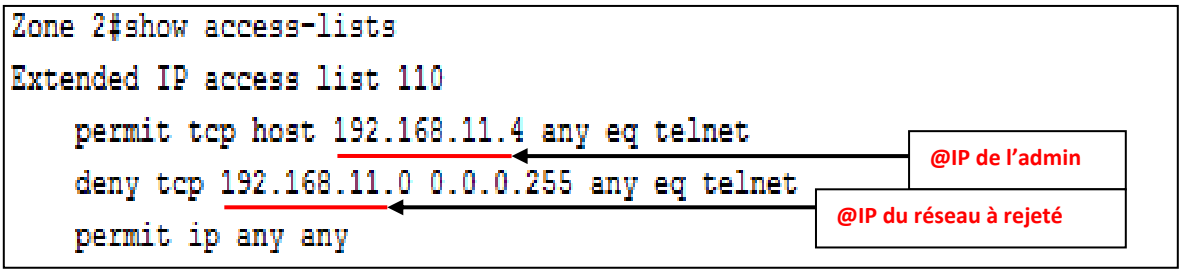


Figure 20 - Restriction de l'accès Telnet

Ensuite nous appliquons cette ACL (110) en entrée (in) sur l'interface Fa0/0.

Remarque :

Telnet sécurisé est fourni lorsque les utilisateurs sont invités par le routeur de s'authentifier par l'intermédiaire de mots de passe. Chaque port Telnet sur un routeur est connu sous le nom d'un terminal virtuel. Il ya un maximum de cinq Virtual Terminal ports sur le routeur, permettant à cinq sessions simultanées Telnet. Sur le routeur, les ports de terminaux virtuels sont numérotés de 0 à 4. On va définir un mot de passe pour l'accès Telnet via les ports de terminaux virtuels avec les commandes de configuration suivantes :

```
Zone 2(config)#line vty 0 4
Zone 2(config-line)#password cisco
Zone 2(config-line)#login
```

Figure 21 - Application d'un mot de passe aux lignes VTY

Dans cet exemple, les ports de terminal virtuel de 0 à 4 utilisent le mot de passe "**Cisco**":

Teste des résultats :

Après avoir assigné l'ACL **110** à l'interface Fa 0/0 du routeur « **Zone 2 »**, l'administrateur du réseau **192.168.11.0/24** aura un accès **Telnet**, mais pas les autres utilisateurs de ce réseau, comme le montre ci bien les résultats suivants :

- L'administrateur tente de se connecter à une adresse IP du routeur, le routeur fournit une invite semblable à ce qui suit :

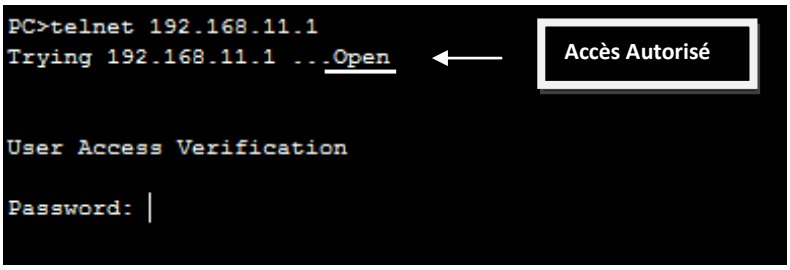


Figure 22 - Ouverture d'une session Telnet

Si l'administrateur entre le mot de passe correct non privilégié, l'invite suivante apparaît :

Figure 23 - Accès en mode non privilégié

L'administrateur aura maintenant un accès non privilégié sur le routeur et peut accéder au mode privilégié en entrant la commande **enable**, puis le mot de passe associé.

Figure 24 - Résultat positif du teste d'accès Telnet

- Et si l'un des utilisateurs du réseau **192.168.11.0/24** dont on a interdit de se connecter tente de le faire, il ne pourra pas, et aura le résultat suivant :

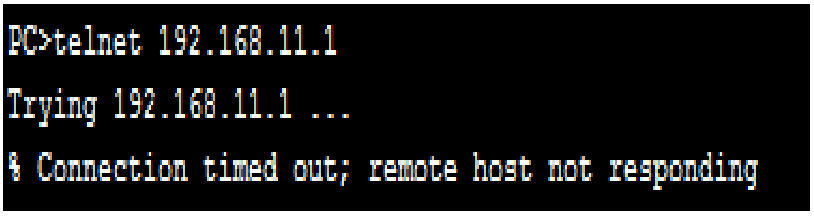


Figure 25 - Résultat négatif du teste

Procédure 2: Prévenir les attaques de type « spoofing »

Pour éviter ce type d'attaque, qui consiste à tenter d'usurper une adresse IP source interne valide, on interdit tout accès de l'extérieur aux adresses réservées aux essais en mode bouclé (c'est-à-dire 127.x.x.x), les adresses de multicast (c'est-à-dire 224.x.x.x – 239.x.x.x) ainsi que les adresses IP du réseau.

Nous devons configurer une liste d'accès de manière à ce que des hôtes Internet ne puissent pas facilement usurper une adresse réseau interne.

On crée donc une liste d'accès **113** comme suite :

```
Zone 2(config)#access-list 113 deny ip 192.168.11.0 0.0.0.255 any
Zone 2(config)#access-list 113 deny ip 192.168.20.0 0.0.0.255 any
Zone 2(config)#access-list 113 deny ip 192.168.21.0 0.0.0.255 any
Zone 2(config)#access-list 113 deny ip 127.0.0.0 0.255.255.255 any
Zone 2(config)#access-list 113 deny ip 224.0.0.0 31.255.255.255 any
Zone 2(config)#access-list 113 permit ip any any
Zone 2(config)#interface Se 0/0
Zone 2(config-if)#ip access-group 113 in
```

Figure 26 - Configuration de la liste 113

Les trois premières instructions empêchent les utilisateurs externes d'usurper une adresse IP source des réseaux internes 192.168.11.0, 192.168.20.0, 192.168.21.0

La quatrième instruction leurs empêche d'utiliser la plage d'adresses réservées aux essais en mode bouclé.

La cinquième instruction empêche les pirates d'utiliser la plage d'adresses de multicast (c'est-à-dire 224.0.0.0 – 239.255.255.255) pour générer du trafic interne indésirable.

Ensuite nous appliquons cette ACL à l'interface la plus proche de la source c'est-à-dire à l'interface Se0/0 du routeur Zone 2, en flux entrant.

Procédure 3: Protéger le réseau interne

- Afin d'éviter la distraction des nouveaux utilisateurs du réseau **192.168.21.0/24**, nous leur bloquons l'accès au serveur WEB du réseau externe 209.165.201.30, mais nous leur autorisons l'accès aux autres ressources du réseau interne.

Pour appliquer cette restriction, nous utilisons l'ACL étendue **120** :

```
Zone1(config)#access-list 120 deny tcp 192.168.21.0 0.0.0.255 209.165.201.30 0.0
.0.0 eq www
Zone1(config)#access-list 120 permit ip any any
Zone1(config)#interface fa0/1
Zone1(config-if)#ip access-group 120 in
```

Figure 27 - Configuration de la restriction au serveur web externe

Teste des résultats :

Pour tester le bon fonctionnement de la liste **120**, il suffit d'écrire l'adresse IP du serveur Web externe (**209.165.201.30**) sur le **web browser** de l'un des nouveaux utilisateurs le test échoue, la page web ne s'affiche pas. Comme le montre la figure suivante :

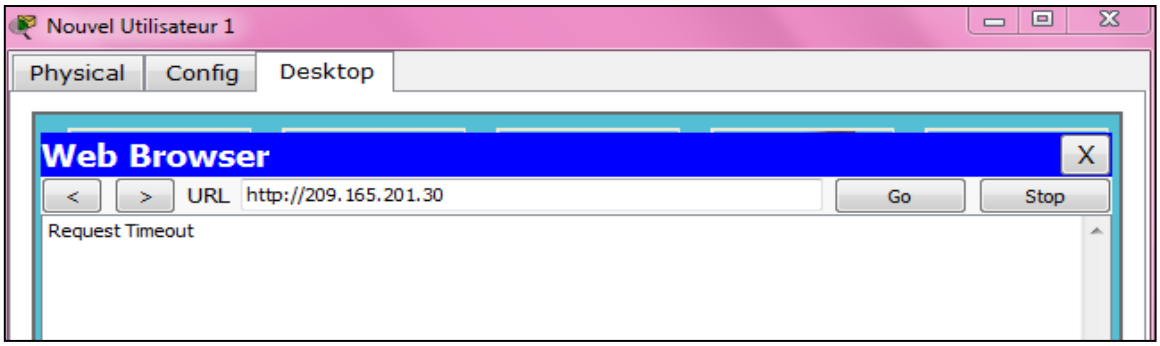


Figure 28 - Teste de connexion au serveur web externe

Mais si on essaye d'effectuer un PING depuis l'un des nouveaux utilisateurs le teste réussi (successful).

Fire	Last Status	Source	Destination	Type	Color
	Successful	Nouvel Utilisateur 1	user 2 (2)	ICMP	
	Successful	Nouvel Utilisateur 1	HTTP	ICMP	
	Successful	Nouvel Utilisateur 2	HTTP	ICMP	

Figure 29 - résultat positif de la requête Ping

4.2. Configuration des listes d'accès étendues nommées

Rappelons d'abord que :

- la syntaxe des listes d'accès étendues nommées est :

  Routeur (config) # **IP Access-List extended** nom_de_liste

Scénario

Protéger le réseau DMZ

Procédure : on autorise l'accès au web pour les utilisateurs internes et externes, empêcher le Ping pour les utilisateurs externes le permettre pour les utilisateurs du réseau interne.

On doit d'abord définir une liste de contrôle d'accès étendue nommée pour le trafic externe afin de déterminer le type de trafic autorisé à entrer sur le réseau DMZ. Le trafic entrant sur le réseau DMZ proviendra d'Internet ou du réseau d'entreprise demandant des services Web. La stratégie sur le routeur « zone 3 » doit être conçue pour filtrer le trafic Internet. Le routeur « zone 3 » ayant une connexion au fournisseur de services (FAI), il constitue le meilleur emplacement pour la liste de contrôle d'accès.

- Nous créons donc une liste d'accès étendue **nommée Firewall** pour le trafic externe qui autorise l'entrée de demandes Web sur le réseau, Cette ligne autorise l'entrée sur le réseau DMZ des services Web destinés au serveur Web :

> Zone 3 (config) # **ip access-list extended Firewall**
> Zones 3 (config-ext-nacl) # permit tcp **any** 192.168.10.45 0.0.0.0 eq **www**

Cette instruction permet donc, au réseau interne comme au réseau externe d'envoyer des demandes de service sur le port 80 (www).

- Après avoir défini la liste, il faut s'assurer que seul le trafic en provenance du réseau interne et externe peut être autorisé à y revenir.

> Zones 3(config-ext-nacl) # permit **tcp any any established**

Dans cette ligne, le mot clé **established** (Facultatif) pour le protocole TCP indique qu'une connexion est établie.

- Il est nécessaire de permettre aux utilisateurs du réseau interne d'envoyer des requêtes **PING** au serveur Web. Toutefois, les utilisateurs du réseau externe ne doivent pas bénéficier du même privilège pour des raisons de sécurité.

Nous ajoutons donc des instructions à la liste d'accès « Firewall » qui donnent le droit aux utilisateurs du réseau interne d'envoyer des requêtes PING au serveur WEB.

> Zone 3(config) # permit icmp 192.168.21.0 0.0.0.255 host 192.168.10.45
>
> Zone 3(config) # permit icmp 192.168.20.0 0.0.0.255 host 192.168.10.45
>
> Zone 3(config) # permit icmp 192.168.11.0 0.0.0.255 host 192.168.10.45

- Tout autre trafic est refusé :

> Zone 3(config) # deny ip any any

Cette commande n'est pas vraiment nécessaire, puisque même si, on ne la met pas, ce refus serra tout de même fait. On l'ajoute donc juste pour qu'elle soit explicite.

- Puisque c'est une liste d'accès étendue, on l'assigne à l'interface Fa 0/1 qui est l'interface la plus proche de la source, sur le flux sortant.

> Zone 3(config) # interface Fa 0/1

Zone 3(config-if) # ip access-group **Firewall** out

On utilise la commande **show-access-lists** pour vérifier la syntaxe de la liste nommée « Firewall », le résultat généré est le suivant :

```
Zone 3#show access-list
Extended IP access list Firewall
    permit tcp any host 192.168.10.45 eq www
    permit icmp 192.168.20.0 0.0.0.255 host 192.168.10.45
    permit icmp 192.168.21.0 0.0.0.255 host 192.168.10.45
    permit icmp 192.168.11.0 0.0.0.255 host 192.168.10.45
    deny ip any any (3 match(es))
```

Figure 30 - Visualisation de l'ACL Firewall

Remarque :

Les **Match(es)** correspondent aux paquets entrants que la liste n'a pas rejetés.

Teste des résultats :

Avant de tester le bon fonctionnement de la liste **Firewall,** nous devons d'abord configurer le serveur Web, pour ce faire, on choisit d'abord le service (http), puis on clique sur le bouton http et on insère le nom du site après <hr> (www.google.com dans notre cas).

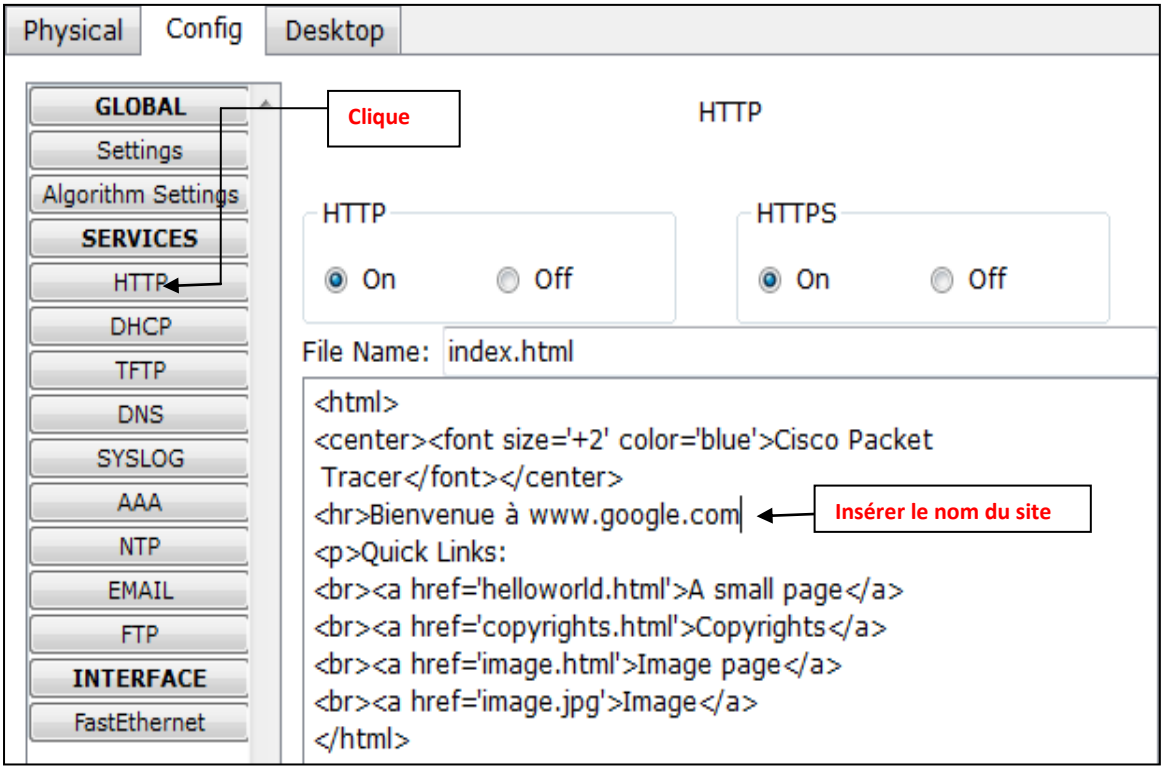


Figure 31 - Configuration du serveur HTTP

- On vérifie maintenant l'accessibilité du serveur WEB de la zone DMZ depuis le réseau interne en envoyant une requête PING.

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Per
	Failed	hôte externe	WEB	ICMP		0.000	N
	Successful	user 2 (2)	WEB	ICMP		0.000	N
	Successful	Admin (1)	WEB	ICMP		0.000	N

Figure 32 - Teste du résultat de l'ACL Firewall avec une requête Ping

On remarque l'échoue de la requête PING envoyée depuis l'hôte externe, et le succès de cette dernière depuis des utilisateurs du réseau interne.

- On vérifie maintenant que l'hôte externe bénéficie toujours de l'accès au WEB.

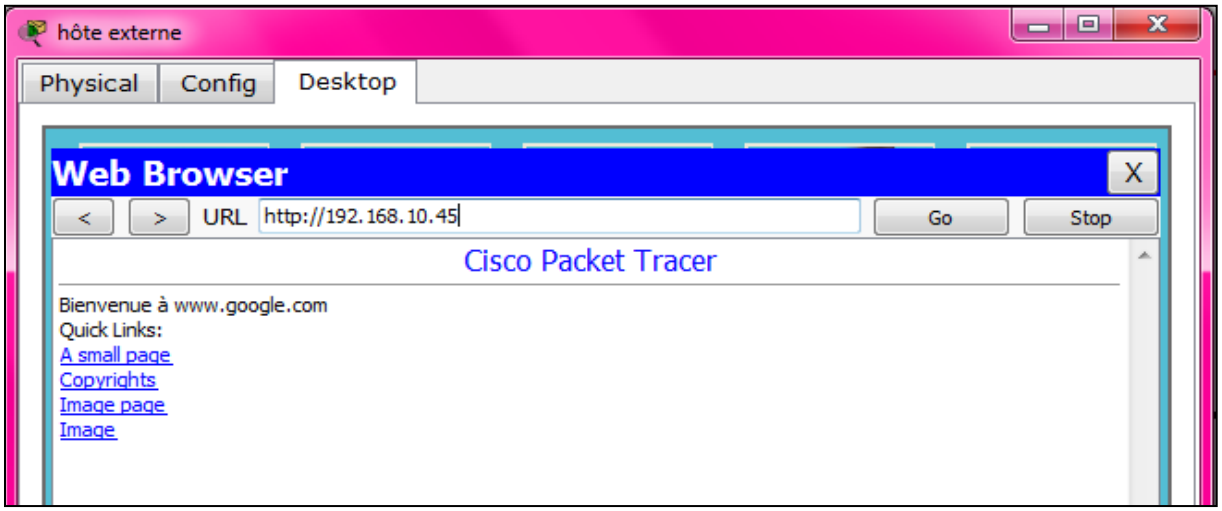


Figure 33 - Teste du résultat de l'ACL Firewall avec une connexion au serveur Web

On remarque donc que l'hôte externe peut toujours accéder au serveur WEB, malgré qu'elle ne puisse pas envoyer une requête PING.

Conclusion

À l'issu de ce chapitre, nous avons conçu et mis en œuvre une politique de sécurité pour un réseau intranet connecté à l'extérieur avec des listes de contrôle d'accès. Nous avons donc effectué des restrictions sur des adresses IP, ainsi que des restrictions sur des services et des applications sur certaines machines.

Ces restrictions ont été méthodiquement mises en œuvre respectivement dans le cadre des listes d'accès standards et étendues, numérotées et nommées. Et on a aussi sécurisé les accès d'administration du routeur pour éviter toute altération de sa configuration.

Conclusion Générale

Conclusion Générale

L'importance de l'informatique, pour nos entreprises, nos industries, notre société entière, et pour chacun de nous en tant qu'individu, poursuit une progression fulgurante depuis une décennie. Pourtant, tous les services informatiques dont nous dépendons sont des subsistances fragiles constituées de composants matériels, logiciels et humains, devant fonctionner en parfaite état jour après jour. L'administrateur qui a pour rôle de préserver la qualité de son système informatique, ne doit pas oublier l'existence de menaces, aussi nombreuses que variées, la sécurité est donc indispensable.

Le présent projet, était une opportunité pour nous d'aborder de près ce domaine, qui est en expansion à l'heure actuelle. L'objectif de notre travail est donc de veiller à la sécurité d'accès au niveau d'un routeur dans un réseau Intranet ; contre les attaques malveillantes qui viennent soient du réseau interne, soient du réseau externe, La méthodologie adoptée dans ce travail est comme suit :

Dans un premier temps nous avons présenté les différents concepts sur les réseaux, nous avons défini l'internet et l'intranet, les équipements d'interconnexion, les principales topologies physiques et logiques existantes avec un accent sur le modèle OSI et TCP/IP.
Ensuite nous avons présenté les principes de base de la sécurité ; les terminologies, les objectifs ainsi que les types d'attaques et quelques solutions pour renforcer la sécurité tels que les pare-feux (Firewall), La cryptographie, le système de détection d'intrusion (IDS), les réseaux virtuels (VLANs) et les listes de contrôle d'accès. Nous avons ensuite étudié le routeur, son architecture, pour apprendre à mettre en place une configuration de base pour ensuite appliquer les listes de contrôle d'accès(ACL).

Ensuite nous avons fait une étude détaillée sur les listes de contrôle d'accès, leurs types, leurs mode de fonctionnement, ces listes s'avèrent un outil incontournable pour assurer la sécurité, elles sont très utilisées car elles permettent de filtrer des machines émettant des paquets IP dans leurs versions standards, le filtrage des protocoles et le contrôle d'applications grâce aux numéros de ports dans leurs versions étendues.

Le travail qui nous a été demandé est de concevoir et de mettre en ouvre une politique de sécurité empêchant tout accès indésirable au sein du réseau, on a choisi que ce réseau soit ouvert vers l'extérieur pour mieux expliquer la notion de sécurité d'accès. Nous avons donc prévu à travers des exemples d'application des restrictions concernant les protocoles et

services comme refuser ou permettre l'accès au serveur web de la DMZ de l'intérieur ou de l'extérieur, permettre ou refuser le PING, ainsi que la sécurisation des accès d'administration en refusant l'accès à distance au routeurs (Telnet) pour tout les utilisateurs sauf pour les administrateurs pour éviter toutes altération de la configuration au niveau des routeurs.
Ces restrictions ont été méthodiquement mises en ouvre dans le cadre des listes d'accès standards et étendues.

La variété des tâches que nous avons accomplies nous a permis d'appréhender de nombreux domaines tels que la manipulation du matériel et la configuration des listes d'accès.

Bibliographie & Nétographie

Bibliographie

[1] Djoudi TOUAZI, Le routage Internet : Les réseaux tolérants aux délais, Mémoire de Magistère en Informatique, Réseaux et Systèmes Distribués, Université de Bejaia, 2005.

[2] Hugo ETIEVANT, Remy FABREGES, Mise en place d'un réseau sécurisé, Maîtrise IUP Génie Informatique Réseau, seau Université Claude Bernard - Lyon 1, Novembre 2002.

[3] Hassen TURKI, Gestion de la sécurité dans les réseaux TCP/IP : « SATAN », Mémoire Ingénieurs en Télécommunications, École supérieure des communications de Tunis, 2004/2005.

[4] Olivier CHATEL, ADMINISTRATION RESEAU, Projet de Fin d'Études**,** ENSIMAG, 1992-1993.

[5] Vincent REMAZEILLES, La sécurité des réseaux avec Cisco, Edition ENI, Février 2009.

[6] Denis VALOIS, Tableaux de bord de la sécurité réseau, Edition Eyrolles, 2006.

[7] Moussa DAVOU, Mise en place d'un Intranet au Ministère de l'Économie et des Finances, Mémoire d'ingénieur de conception en informatique, Université Polytechnique Bobo-Dioulasso, Janvier 2001.

[8] Andrés VAUCAMPS, CISCO, Sécurité des routeurs et contrôle du trafic réseau, Edition Eni, Décembre 2010.

[9] Claude SERVIN, RÉSEAUX ET TÉLÉCOMS Cours et exercices corrigés, Edition Dunod, 2003.

[10] Jean MEHAT, Réseaux et transmissions de données, Université de Paris 8, Département d'informatique, 19 février 2010.

[11] Guy PUJOLLE, RÉSEAUX ET TÉLÉCOMS Avec exercices corrigés, Edition Eyrolles, Septembre 2006.

[12] Jean-Luc MONTAGNIER, Réseaux d'entreprise par la pratique, Edition Eyrolles.

[13] Eric ROBIN, Configuration des routeurs et routage Basique, 25 Octobre 2005.

[14] Cisco Networking Academy, CCNA 4.0 Notion de base sur les réseaux, 2007/2008

Nétographie

[15] TCP/IP Internet/Intranet/Extranet, http://www.resoo.org

[16] Mohsen SOUISSI, Routage IP,

(http://pillop.dunkklar.org/divers/Cours%20Daniel/linux/routage.slides.pdf)

[17] Encyclopédie Informatique, Comment ça Marche, (http://www.commentcamarche.net)

[18] David BURGERMEISTER, Jonathan KRIER, Les Systèmes de Détection d'Intrusions, (http://dbprog.developpez.com/securite/ids/IDS.pdf)

[19] http://fr.wikibooks.org

[20] http://www.scribd.com/

[21] http://www.lolokai.com/2012/03/26/securite/les-acl-sur-les-equipements-cisco/

[22] http://www.cnrs.fr/

[23] http://technet.microsoft.com

[24]http://www.cisco.com/

[25]ACL Cisco,

(http://cosy.univ-reims.fr/~fnolot/Download/Cours/reseaux/m2pro/ACL-Cisco.pdf)

ANNEXES

Annexe A

Les couches du modèle OSI et TCP/IP

A.1. Les couches du modèle OSI

Niveau	Couches	Description	Exemple
7	**Application**	La couche application est responsable de la communication entre le réseau et les applications. Elle offre le service réseau à l'application qui le demande.	navigateurs Web Chat Firewall Applicatif
6	**Présentation**	Cette couche s'occupe surtout de traduire les données pour que les 2 systèmes puissent communiquer entre eux et se comprendre.	Cryptage des données Compression des données
5	**Session**	Cette couche permet à deux applications de créer une connexion qui est permanente. Donc la couche session ouvre, gère et ferme les sessions entre deux systèmes hôte en communication.	Ouverture de session Windows Authentification
4	**Transport**	La couche transport divise les données envoyées par les systèmes de l'hôte émetteur et les rassemble en flux de données sur le système de l'hôte récepteur. Assure une transmission de bout en bout des données. La couche transport assure la fiabilité et la régulation du transfert de données.	UDP TCP Firewall
3	**Réseaux**	La couche réseau détermine le chemin d'accès physique des données à transmettre, en fonction des conditions de fonctionnement du réseau, de la priorité du service ou autre.	Routeur
2	**Liaison de donnée**	Elle assure un transit fiable des données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique, de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et du contrôle de flux.	HDLC Switch Pont
1	**Physique**	C'est le niveau le plus bas, il définit les spécifications électriques, mécaniques, procédurales et fonctionnelles permettant d'activer, de maintenir et de désactiver la liaison physique entre les systèmes d'extrémité.	Hub Câble réseau, fibre optique Carte réseau

Tableau A.5 - Différentes couches du modèle OSI

A.2. Les couches du modèle TCP/IP

Le tableau suivant décrit les types de services proposés et les protocoles utilisés sur chaque couche du modèle TCP/IP :

Couche	Description	Protocoles
Application	C'est la couche de haut niveau, elle englobe les couches OSI d'application, de présentation et de session. Elle s'assure que les données soient correctement "empaquetées" pour qu'elles soient lisibles par la couche suivante.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP.
Transport	Propose la gestion des sessions de communication entre les ordinateurs hôtes. Définit le niveau de service et l'état de la connexion utilisés lors du transport des données.	TCP, UDP, RTP
Internet	Cette couche doit s'assurer que les données envoyées arrivent correctement à destination.	IP, ICMP, ARP, RARP
Accès réseau	elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.	Ethernet,Token Ring, X.25, Frame Relay

Tableau A.6 - Différentes couches du modèle TCP/IP

Annexe B

Les adresses internet

B.1 Présentation générale de l'adresse IP

IPv4, et **IPv6** représentent les deux versions d'adresses IP qui existent aujourd'hui. Presque tous les réseaux utilisent la première, tandis qu'un nombre croissant d'entreprise ont adopté la seconde, qui est l'avenir des adresses IP.

- **IPv4 :** Identifiant unique de chaque machine, la version 4 de l'Internet Protocol existe depuis septembre 1981 et est décrite par la norme RFC 791, elle est codé sur 4 octets, soit 32 bits.
- **IPV6** : La sixième version de l'Internet Protocol a été développée dans les années 90 et sa norme (la RFC 2460) a été fixée en décembre 1998. Les adresses IPv6 sont stockées sur 16 octets (128 bits).

Chaque adresse IP d'une machine est appelée *adresse logique.* Elle est codé sur 32 bits soit 4 octets. Elle est composée de deux parties qui sont les suivantes:

- Le **Net ID** qui correspond à l'adresse réseau, qui identifie les systèmes qui sont situés sur le même réseau physique.
- Le **Host ID** qui correspond à l'adresse de la machine sur le réseau, elle identifie un poste de travail, le serveur, le routeur etc.

Dans un "*champ*", les chiffres vont de 0 à 255. (0.0.0.0 à 255.255.255.255), cela représente un total de 4 294 967 296, IP différentes.

A. 2 Les classes d'adresses IP

On utilise des **classes d'adresses IP** pour les ranger de façon logique et ordonnées. Il y a 5 classes différentes, les trois premières classes étant utilisées dans les réseaux standards.

Le tableau suivant montre les différentes classes, les plages d'adresses et leurs spécifications :

Classes	Plage d'adresse	Spécification
A	**1.0.0.1** à **126.255.255.254**	Cette classe est faite pour les très grands réseaux, elle comporte donc 127 réseaux différents et plus de 16 millions de machines par réseau.
B	**128.0.0.1** à **191.255.255.254**	Cette classe comporte donc 16575 réseaux différents et plus de 6500 machines par réseau.
C	**192.0.0.1** à **223.255.255.254**	Cette classe est faite pour les petits réseaux puisqu'elle ne peut accueillir que 254 hôtes. Elle comporte 2 millions de réseaux et 245 machines par réseaux.
D	**224.0.0.0** à **239.255.255.255**.	C'est une classe utilisée pour le multicasting.
E	Le premier octet de cette classe est compris entre 240 et 255.	Cette classe a été définie comme étant une classe pour les ordinateurs de recherches.

Tableau B.7 - Les classes d'adresses IP

B.3 Les Adresses particulières

- **L'Adresse de Loopback** : Toutes les adresses IP dont le premier octet possède la valeur 127 sont réservées aux tests du logiciel réseau. Si un paquet de données est adressé par exemple à l'adresse 127.2.5.10, il sera renvoyé à l'intérieur du réseau vers son expéditeur. Il est ainsi possible de vérifier que le logiciel local TCP/IP est installé et configuré correctement. Dans ce type de boucle de test (**Loop**), le paquet de données parcourt les couches OSI 7 à 3. Les couches matérielles 1 et 2 ne sont pas prises en compte.
- **L'adresse 0.0.0.0** : Cette adresse est l'adresse par défaut (aller n'importe où quand on ne trouve pas d'entrée correspondant à une adresse réseau de destination), on emprunte l'adresse (ou le port ou l'interface) de sortie indiquée dans la table de routage.
- **L'adresse de diffusion (Broadcast)** : Tout les bits du champ de l'adresse machine (HOST-ID) sont mis à un, cette adresse sert à adresser un message à toutes les machines du réseau.

- **Les adresses IP Privées** : Ces adresses sont destinées uniquement aux réseaux internes privés (réseaux locaux). Les adresses privées ne sont pas acheminés sur Internet, ce sont celle définies par le RFC1918:

Classe	Plages d'adresses internes RFC 1918
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Tableau B.8 - Les Adresses IP privées

B.4 Le masque de sous-réseau

Le masque de sous-réseau indique quelle partie de l'adresse IP est utilisée pour indiquer la partie réseau, et la partie réservée à l'adressage d'un hôte particulier. Il existe un masque de sous-réseau par défaut pour chaque type de classe d'adresses, qui indique comment l'adresse doit être interprétée dans le cas normal.
Le tableau suivant représente les classes d'adresses et leurs masques correspondant :

Classe d'adresses	Adresse exemple	Adresse réseau	Adresse de diffusion	Masque de sous réseau
A	22.96.5.200	22.0.0.0	22.255.255.255	255.0.0.0
B	141.65.23.1	141.65.0.0	141.65.255.255	255.255.0.0
C	193.2.5.65	193.2.5.0	193.2.5.255	255.255.255.0

Tableau B.9 - Exemple d'adresses IP et leurs masques correspondants

Une fois ce masque créé, il suffit de faire un ET entre la valeur à masquer et le masque afin de garder intacte la partie souhaitée et annuler le reste. Ainsi, un masque réseau (en anglais netmask) se présente sous la forme de 4 octets séparés par des points (comme une adresse IP), il comprend des zéros au niveau des bits de l'adresse IP à annuler, et des 1 au niveau de ceux à conserver.

Annexe C

C.1 Présentation de Packet Tracer

Packet Tracer est un logiciel qui offre la possibilité de concevoir un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur créé son réseau grâce à des équipements tels que les routeurs, les commutateurs, les serveurs ou des ordinateurs. Ces équipements nécessitent ensuite d'être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements connectés, il est possible pour chacun d'entre eux, de configurer les adresses IP, le routage, etc.

C.2 Exploration de l'interface de Packet Tracer

Lorsque Packet Tracer démarre, il présente une vue logique du réseau en mode temps réel. La figure qui suivra montre un aperçu général de l'interface de Packet Tracer :

(1) C'est la zone principale de l'interface de Packet Tracer, elle représente le lieu de travail logique. Il s'agit de la zone vierge étendue dans laquelle des périphériques peuvent être placés et connectés.

(2) : Représente la zone ou les équipements sont regroupés en catégories accessibles pour les utilisateurs, elle contient donc des symboles qui représentent des groupes de périphériques.

(3) : Une fois la catégorie sélectionnée dans la zone (2), le type d'équipement peut être transmit à la zone (3), le nom du groupe de périphérique d'affiche, il reste qu'a choisir ce dont on a besoin.

(4) : Permet de passer du mode temps réel au mode simulation.

(5) : Permet d'ajouter des indications dans le réseau

(6) : Cette zone contient un ensemble d'outils:

- ***Select:*** pour déplacer ou éditer des équipements;
- ***Move Layout:*** permet de déplacer le plan de travail;
- ***Place Note:*** place des notes sur le réseau;
- ***Delete:*** supprime un équipement ou une note;
- ***Inspect:*** permet d'ouvrir une fenêtre d'inspection sur un équipement.

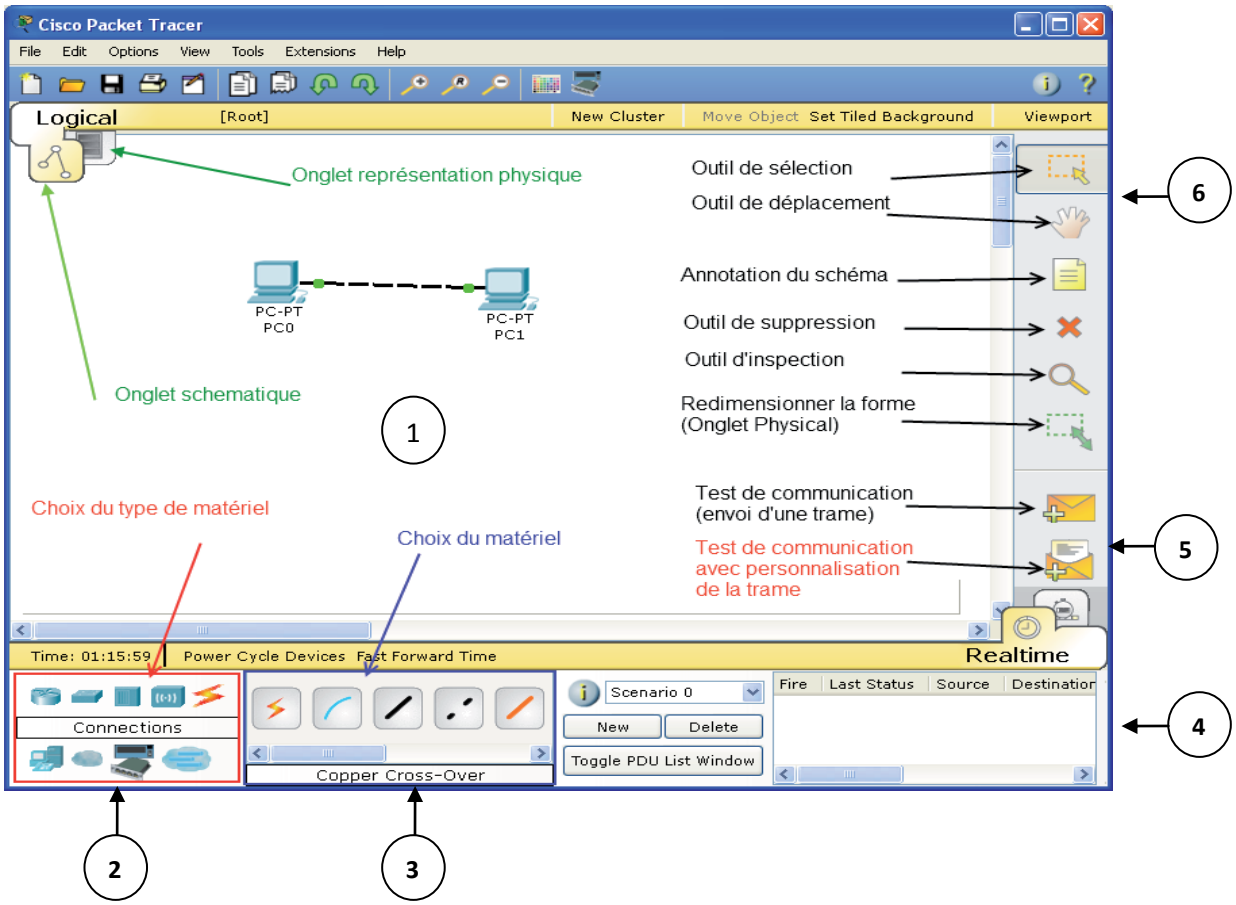


Figure C.3 - L'interface du simulateur Packet Tracer

Construire un réseau

Pour construire un réseau, l'utilisateur doit faire un choix parmi les 8 catégories proposées par Packet Tracer : les routeurs, les switchs, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), des équipements personnalisés et enfin, une connexion multiutilisateurs.

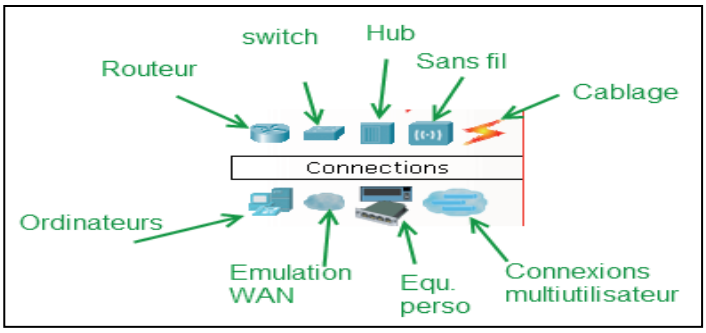


Figure C.4 - Types d'équipements

Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit ou on veut le mettre.

Ensuite on devrait relier deux équipements, il faut donc choisir la catégorie "Connections" puis cliquer sur la connexion désirée.

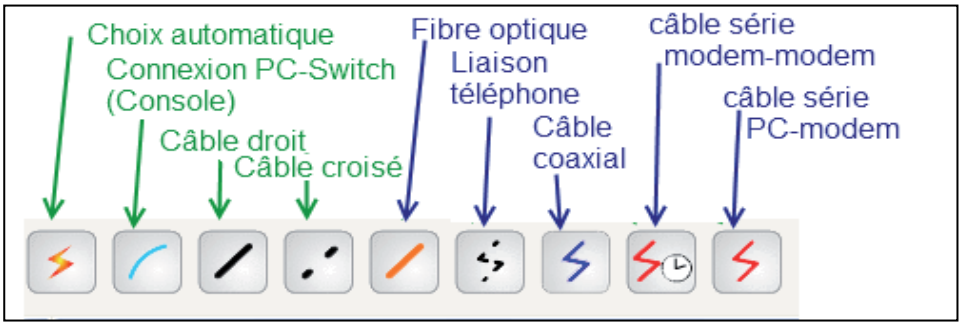


Figure C.5 - Les différentes connexions proposées

Pour les liaisons, voila les types de câble réseau qu'il faut utiliser :

Câbles droits :

• PC à Hub • PC à Switch • Switch à Routeur

Câbles croisés :

• Switch à Switch • Hub à Hub • Routeur à Routeur

• PC à PC • Hub à Switch • PC à Routeur

Pour les liaisons séries entres routeurs, il faudra rajouter le module WIC 2T au routeur. Ce module permet de rajouter une interface série afin de relier deux réseaux. Une des deux extrémités doit fournir une horloge. Pour ajouter ce type d'interface, il faut utiliser la souris en « glisser/déposer » dans un slot libre. Il faut aussi penser à éteindre le module (en cliquer sur l'interrupteur du module).

C.3 Configuration d'un équipement

Lorsqu'on veut ajouter un ordinateur (appelé PC-PT dans Packet Tracer), on a la possibilité de le configurer en cliquant dessus, une fois ajouté dans le réseau. On a donc une fenêtre qui s'ouvre et qui contient 3 onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur Web).

Dans l'onglet Config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton FastEthernet en-dessous du bouton INTERFACE)

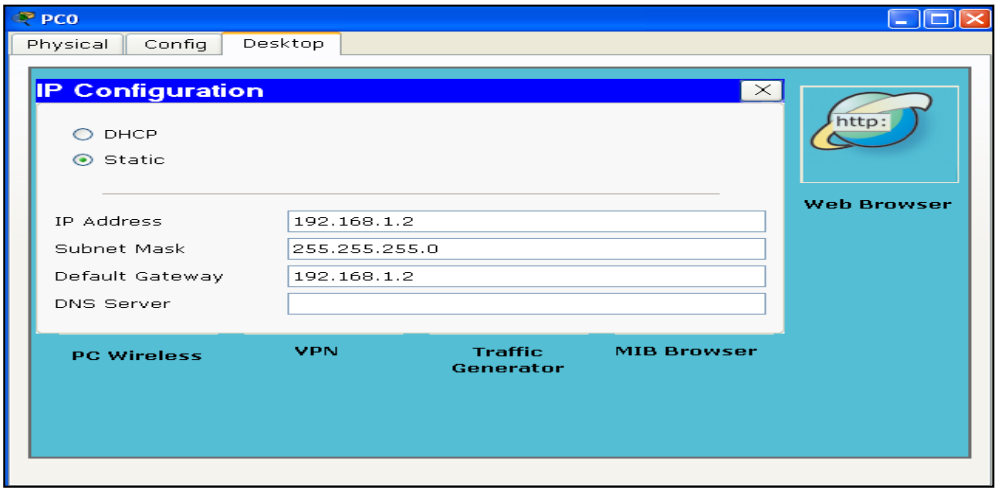


Figure C.6 - Configuration des machines

C.4 Mode simulation

Une fois qu'on a créé le réseau il est maintenant prêt à fonctionner, il est possible de passer du mode Realtime en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau.

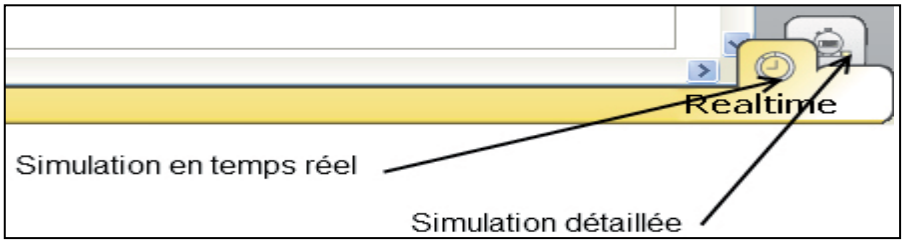


Figure C.7 - Passage entre le mode simulation et mode Realtime

En mode simulation, la fenêtre principale est fractionnée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles.

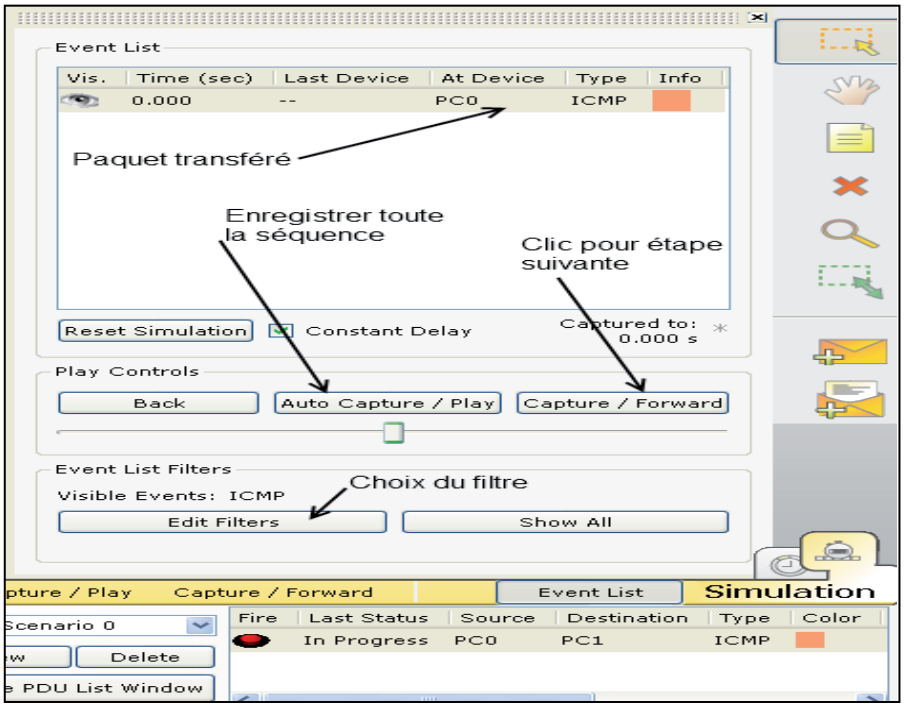


Figure C.8 - la partie simulation

C.5 Les différents modes d'exécutions d'un routeur

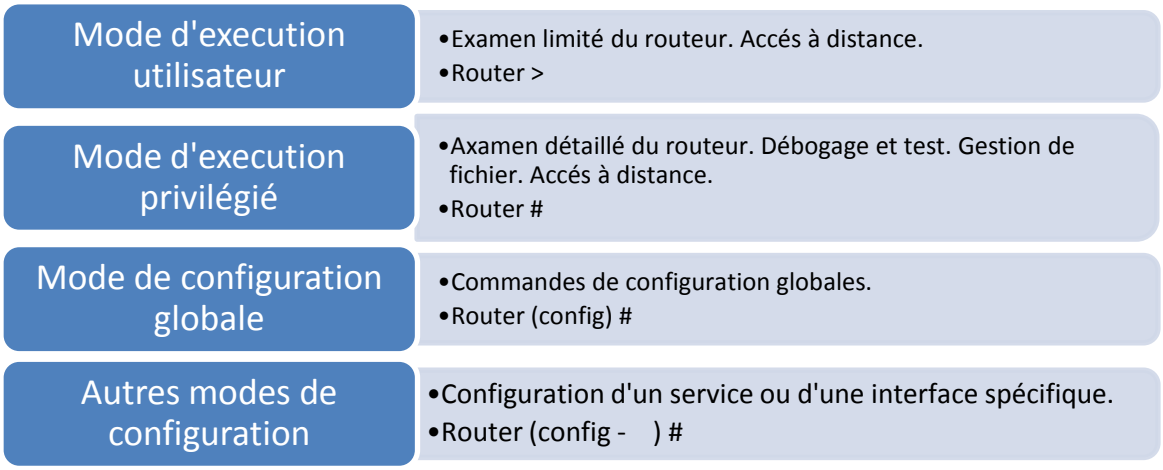


Figure C.9 - Les différents modes d'exécutions

a. **Mode utilisateur:** Ce mode nous permet de consulter toutes les informations liées au routeur sans pouvoir les modifier. Le Shell[7] est le suivant:

```
Router >
```

b. **Utilisateur privilégié:** Il permet de visualiser l'état du routeur et d'importer/exporter des images IOS.

```
Router #
```

c. **Mode de configuration globale**: Permet d'utiliser les commandes de configuration générales du routeur :

```
Router (config) #
```

d. **Mode de configuration d'interfaces**: Ce mode permet d'utiliser des commandes de configuration des interfaces :

```
Router (config-if) #
```

e. **Mode de configuration de ligne:** Permet de configurer une ligne

```
Router (config-line) #
```

f. **Mode spécial:** RXBoot Mode de maintenance qui peut servir, notamment, à réinitialiser les mots de passe du routeur :

```
rommon >
```

[7] **Shell** : C'est une interface texte qui permet à l'utilisateur de communiquer avec l'ordinateur.

C.6 Passage entre les différents modes d'exécution

- **Utilisateur normal:** Aucune commande à effectuer, c'est dans ce mode que commence une session.
- **Utilisateur privilégié (à effectuer à partir du mode normal):**

  Router > enable

  Router #

➢ **Mode de configuration globale (à effectuer à partir du mode Privilégié):**

Router # configure terminal

Router (config) #

➢ **Mode de configuration d'interface (à effectuer à partir du mode de configuration globale):**

Router (config) # interface nom_interface

Router (config-if)#

➢ **Mode de configuration de ligne (à effectuer à partir du mode de configuration globale):**

Router (config) # line nom_de_la_ligne

Router (config-line) #

Annexe D

Les Numéros de port

Un numéro de port est un champ de 16 bits qui doit être associé à la conversation entre les hôtes pour garantir que le paquet atteint le service approprié sur le serveur. Les hôtes exécutant TCP/IP associent des ports au niveau de la couche transport à certaines applications. Les numéros de port servent à distinguer les différentes conversations qui circulent simultanément sur le réseau. Les numéros de port sont nécessaires lorsqu'un hôte communique avec un serveur exécutant plusieurs services. Les numéros de port sont représentés par 2 octets dans l'en-tête d'un segment TCP ou UDP. Cette valeur sur 16 bits peut représenter des numéros de port compris entre 0 et 65535. ON distingue trois catégories de port qui sont défini définis dans le document RFC1700 (Request For Comments) : les ports bien connus, les ports enregistrés, et les ports dynamiques ou privés.

1. **les ports bien connus** (Well Known Ports) : Ces ports bien connus sont contrôlés et assignés par l'IANA. Comme leur nom l'indique, ces ports sont utilisés pour des services de réseaux bien connus, tels que FTP, Telnet ou DNS. Les numéros de port bien connus sont compris entre 0 et 1023.
2. **les ports enregistrés** (Registered Ports) : Ils sont compris entre 1024 à 49151, ils sont utilisés pour les programmes exécutés par les utilisateurs. Parmi ces services on a MSN messenger port 1863.
3. **les ports dynamiques** *:* Ils sont compris entre 49152 à 65535, Également appelés ports éphémères, ces ports sont généralement affecter de façon temporaire à des applications clientes lorsqu'une connexion est initiée.

Remarque :

- Les ports d'un serveur sont généralement compris entre 0 et 1023, un serveur (ordinateur que l'on contacte pour des services tels que FTP, Telnet, ...) possède des numéros de port fixes auxquels l'administrateur réseau a associé des services.
- Côté du client, le port est choisi aléatoirement parmi ceux disponibles par le système d'exploitation. Les ports du client ne seront jamais compris entre 0 et 1023 (supérieur à 1023).

Le tableau ci-dessous, est un condensé des numéros de protocole et des numéros de port les plus utilisés.

N° couche	Protocole	N° de port
3(Réseau)	IP	4
3	ICMP	1
3	IGMP	2
3	**RSVP**	46
3	EGP	8
3	IGRP	88
3	OSPF	89
3	BGP	179
3	Bootp	68
4 (Transport)	UDP	17
4	TCP	6
5(session)	DNS	53
7(Application)	SNMP	161/162
7	TFTP	79
7	SSH	22
7	Telnet	23
7	FTP	21
7	SMTP	25
7	http	80
7	POP3	110

Tableau E.1 - Couche, protocole et numéro de port associé

Annexe E

Les topologies des réseaux

E.1. Topologie physique *(Topologie de câblage)*

Définit l'emplacement exacte des équipements du réseau, ainsi que la manière dont laquelle ils sont interconnectés. On distingue les topologies suivantes :

a. Topologie en Bus

Elle permet de relier tous les ordinateurs à une même ligne de transmission par l'intermédiaire de câble.

b. Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé *hub* ou *concentrateur*. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. Son rôle est d'assurer la communication entre les différentes jonctions.

c. Topologie en anneau

Les ordinateurs dans cette topologie communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole" successivement.

d. Topologie hybride

La topologie hybride utilise un mélange de différents genres de topologies réseaux, comme les topologies en bus, en anneau et en étoile.

E.2. Topologie Logique *(Topologie d'accès)*

Définit une méthode d'accès standard entre les équipements, le mode de fonctionnement du réseau, ainsi que la répartition des nœuds et le type de relation entre eux. Les méthodes d'accès les plus courantes sont :

a. Ethernet

C'est un standard de transmission de données dont le principe repose sur un bus partagé : chaque station émet quand elle le souhaite mais, au moment ou deux stations émettent en même temps, il y a collision (plusieurs trames de données se trouvent sur le bus

simultanément). Dans ce cas les émissions sont stoppées, les deux machines interrompent leur communication et attendent un délai aléatoire, puis la première ayant passé ce délai peut alors réémettre. [12]

b. L'anneau à jeton (*token ring*)

C’est une technologie d'accès au réseau basé sur le principe de la communication au tour à tour, chaque ordinateur du réseau à la possibilité de parler à son tour. Ce jeton est un paquet de données circulant en boucle d’un ordinateur à un autre du réseau, il détermine quel ordinateur a le droit d'émettre des informations.

Lorsqu'un ordinateur est en possession du jeton, il peut émettre pendant un temps donné, après il remet le jeton à l'ordinateur suivant.

Résumé

La multiplication des moyens d'accès et l'ouverture des réseaux vers l'extérieur de l'entreprise fragilisent le système d'information. Il devient alors la cible d'attaques qui visent à modifier l'information mais aussi à paralyser le système.
Les moyens mis en œuvre pour le protéger se regroupent sous le vocabulaire de « sécurité des Réseaux informatique ».

L'objectif de ce mémoire est de veiller à assurer une bonne sécurité d'accès au réseau Intranet. Pour cela, nous avons présenté les notions de base sur les réseaux locaux, après nous avons entamé la sécurité informatique en couvrant quelques stratégies. Ensuite nous avons introduit le routeur, son architecture, et le rôle qu'il joue dans le contrôle d'accès, ensuite nous avons présenté les listes de contrôle d'accès (ACLs), leurs types, leurs modes de fonctionnement et leurs configurations.

Sur le plan applicatif, nous avons configuré des restrictions pour le trafic entrant et sortant à l'aide des listes de contrôle d'accès standards et étendues.

Mots-clés : Réseaux locaux, routeur, sécurité informatique, ACL.

Abstract

The multiplication of means of access and open networks to the outside of the company weakens the information system. It becomes the target of attacks designed to amend the information but also to paralyze the system. "Security of Computer Networks" is the name which contains the means used to protect the network.

The objective of this thesis is to ensure good access security to intranet. For this, we presented the basics of local area networks, after we started covering some security strategies. Then we introduced the router, its architecture and its role in access control, and then we presented the access control lists (ACLs), their types, their operating modes and configurations.

On the application, we set restrictions for incoming and outgoing traffic using access control lists standard and extended.

Keywords: Local area networks, router, computer security, ACL.