TABLE DES MATIERES

LISTE DES ABREVIATIONS

ACK:	ACKnowledged
ACL :	Access Control Lists
AIM :	Adaptative Identification Mitigation
ASA :	Adaptive Security Appliance
ADOdb:	Active Data Objects Data Base
API:	Application Programming Interface
ARP:	Address Resolution Protocol
BASE:	Basic Analysis and Security Engine
CPU:	Central Processing Unit
DNAT:	Destination Network Address Translation
DNS:	Domain Name Service
DoD:	Department of Defense
DoS:	Denial of Service
DSI :	Direction de Système d'Information
FTP:	File Transfer Protocol
GPL:	General Public License
HTML:	Hyper Text Markup Language
HTTP:	Hypertext Transfer Protocol
ICMP:	Internet Control Message Protocol
IDS:	Intrusion Detection System
INTERNET:	INTERconnected NETwork
IP:	Internet Protocol
IPS :	Intrusion Prevention Système
IR:	Infra Rouge
ISO:	International Standards Organization
LAN:	Local Area Network
MAN:	Metropolitan Area Network
MAU:	Multistation Access Unit
MFB :	Ministères des Finances et du Budget
NAT:	Network Address Translation

NIDS:	Network Intrusion Detection System
Nmap:	Network Mapper
NFS:	Network File System
OS :	Operating System
OSI:	Open Système Interconnexion
PAN:	Personal Area Network
PHP:	PHP Hypertext Preprocessor
RIP:	Routing Information Protocol
SNAT:	Source Network Address Translation
SMTP:	Simple Mail Transfer Protocol
SNMP:	Simple Network Management Protocol
SQL:	Structured Query Language
SYN:	Synchronise Sequence Numbers
SDN :	Self-Defending Network
SSM :	Security Service Module
TCP:	Transmission Control Protocol
TELNET:	TErminal NETwork
UDP:	User Datagram Protocol
UIT-T:	Union Internationale des Télécommunications
USB	Universal Serial Bus
VPN :	Virtual Protocol Network
WAN:	Wide Area Network
WWW:	World Wide Web

INTRODUCTION GENERALE

De nos jours, la sécurité informatique est devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques. La sécurité vise à protéger l'accès et la manipulation des données par des mécanismes d'authentification, d'autorisation, de contrôle, etc. Ce projet sur la sécurité informatique s'adresse à tout informaticien sensibilisé au concept de la sécurité informatique mais novice en la matière.

On a pour objectif aux techniques des attaquants pour apprendre comment se défendre. Après une définition précise des différents types de hackers et de leurs objectifs, et présente la méthodologie d'une attaque et les moyens de repérer les failles par lesquelles s'insérer dans un système. La sécurité sur le web est également présentée et les failles courantes identifiées à l'aide d'outils qui peuvent facilement être mis en place par le lecteur sur ses propres systèmes. Le but est toujours d'identifier les failles possibles pour ensuite mettre en place la stratégie de protection adaptée. Ce projet aide les internautes et les administrateurs à sécuriser leurs réseaux et les systèmes. C'est dans ce contexte que nous est venue l'idée de faire intervenir le matériel Cisco ASA pour mieux combler les lacunes dans ce domaine. D'ailleurs, c'est l'essence même de ce mémoire de fin d'études qui s'intitule : Etude et mise en place de la sécurité réseau au sein du MFB « Cisco ASA ». Ce projet est en cours d'exécution au sein du Ministère des finances et de budget Antananarivo Madagascar au Direction de système d'information.

Pour se faire, ce rapport est décomposé en quatre chapitres dont le premier se basera sur les généralités sur le réseau informatique et le second étudie les attaques informatiques et l'étude de sécurité réseaux. Tandis que le troisième chapitre exposera la conception et sécurité réseau au sein du MFB en élaborant la base de conception réseau hiérarchique et les techniques de sécurité utilisée. Et pour terminer cette étude, nous allons présenter dans le dernier chapitre notre travail proprement dit.

CHAPITRE 1
GENERALITES SUR LE RESEAU INFORMATIQUE

1.1 Introduction

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques, même si cela ne va pas sans difficulté.

1.2 Le réseau informatique

Avant l'existence des réseaux, le partage des informations entre individu se faisait uniquement soit oralement, soit par l'écriture des mémos, soit la copie d'informations sur disquette et la remise de cette disquette à l'autre personne qui devait recopier son contenu sur son ordinateur. Ces besoins ont été couverts par la suite par l'apparition et l'apogée des réseaux informatiques.

1.2.1 Définition

Le terme générique « réseau » définit un ensemble d'entités (objets, personnes, etc…) interconnectées les unes avec les autres. Un réseau est un ensemble des « choses » connectées entre elles échangeant des informations. Pour les ordinateurs, on peut parler de réseau lorsqu'il y a au moins deux ordinateurs reliés entre eux qui s'échangent des données. [1]

- Un réseau informatique est un ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (valeurs binaires, c'est-à-dire codées sous forme des signaux pouvant prendre deux valeurs : 0 et 1).
- Un nœud de réseau est un équipement (une imprimante, un ordinateur, un télécopieur,..) connecté au réseau par l'intermédiaire d'une carte réseau. Le système d'exploitation réseau est un programme qui gère l'interaction entre les nœuds d'un réseau.
- Un protocole est une spécification standard qui permet la communication entre deux équipements. Ce sont des règles et des procédures qui définissent le type de codage et la vitesse utilisée pendant la communication, ainsi que la façon d'établir et de terminer cette communication.
- Un pirate informatique est une personne malveillante qui s'attaque aux systèmes

informatique (c'est un ensemble des moyens informatiques et de télécommunication ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données) ainsi qu'aux données qu'ils contiennent.

Un virus est un programme informatique malveillant situé dans le corps d'un autre programme informatique « normal ». Lorsque nous l'exécutons ce dernier, le programme malveillant se charge en mémoire et exécute les instructions que son auteur a programmées.

- La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité du système informatique contre des menaces intentionnelles.
- Un pare-feu est un composant ou ensemble de composants qui restreint l'accès entre un réseau protégé et l'internet ou entre des différentes sections d'un même réseau.
- Les périphériques désignent les appareils qui sont reliés aux ordinateurs (par exemple : imprimantes, faxs, modems, manette de jeu,…). Tout ce qui n'est pas microprocesseur ou mémoire est périphérique.

La topologie physique est la structure physique d'un réseau. C'est-à-dire la forme, l'apparence du réseau.

La topologie logique est la structure logique d'une topologie physique. C'est donc elle qui définit comment se passe la communication dans la topologie physique. [1]

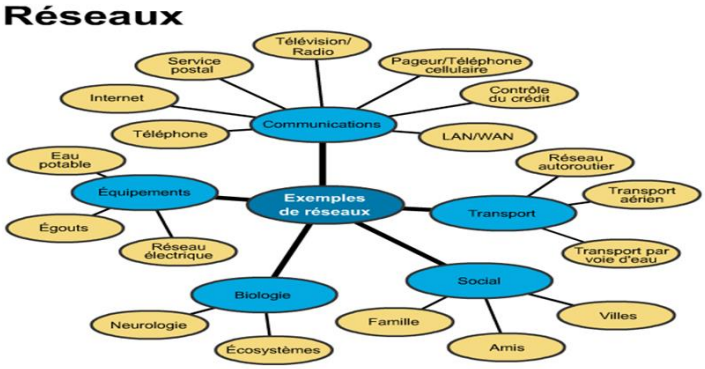


Figure 1.01 : *Exemple de réseau*

1.2.2 Les avantages du réseau informatique

Au début de l'ère informatique, les ordinateurs étaient utilisés comme des stations autonomes fonctionnant seules et indépendamment les unes des autres.

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. [1]

Un réseau informatique peut servir pour plusieurs buts distincts :

- Le partage des ressources (fichier, applications ou matériels, connexion à internet, etc.)
- La communication entre personne (courir électronique, discussion en direct, etc.)
- La communication entre processus
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)
- Le jeu vidéo multi-joueur

Les réseaux permettent aussi de standardiser les applications. Nous parlons généralement de « groupware » pour qualifier les outils permettant à plusieurs personnes de travailler en réseau. Par exemple la messagerie électronique et les agendas de groupe permettent de communiquer plus efficacement et plus rapidement.

Ce genre de système peut avoir comme avantage :

- La diminution des coûts grâce aux partages de données et des périphériques,
- La standardisation des applications,
- L'accès aux données en temps utile,
- La communication et organisation plus efficace.

Aujourd'hui, avec internet, nous assistons à une unification des réseaux. Ainsi les intérêts de la mise en place d'un réseau sont multiples, que ce soit pour une entreprise ou un particulier.

1.2.3 La topologie du réseau

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). [2]

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé topologie physique. On distingue généralement les topologies suivantes :

- Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

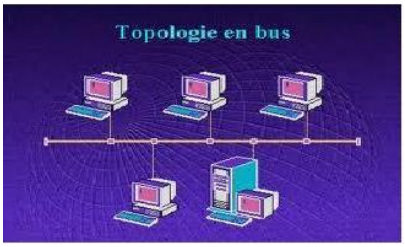


Figure 1.02 *:Topologie en bus*

Cette topologie est facile à mettre en œuvre et possède un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté. [2][3]

- Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub, littéralement moyen de roue). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Figure 1.03 : *Topologie en étoile*

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub). [2][3]

- Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour

Figure 1.04 : *Topologie en anneau*

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre eux un temps de parole. [2][3]

- Topologie en arbre

Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

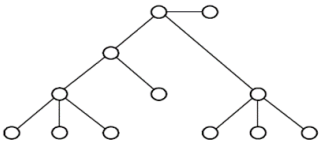


Figure 1.05 : *Topologie d'un réseau point-à-point en arbre*

- Topologie maillée

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres.

L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

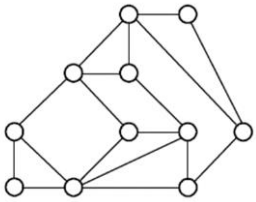


Figure 1.06 : *Topologie d'un réseau point-à-point maillé*

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet).
L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.
L'armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée. [2][3]

1.2.4 La classification des réseaux

La méthode «traditionnelle» de classification des réseaux est basée sur les distances. Elle est fondée sur le principe qui veut que les techniques de transmission changent suivant les distances à parcourir. [2]

1.2.4.1 Le PAN (Personal Area Network)

PAN, acronyme de Personal Area Network, désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Les bus utilisés les plus courants sont l'Universal Serial Bus, les technologies sans fil telles que
Bluetooth ou IR (Infra Rouge).
Le Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques.

1.2.4.2 Le LAN (Local Area Network)

Les réseaux LAN sont les réseaux locaux. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau (par exemple : un bureau, un immeuble, etc.)

1.2.4.3 Le MAN (Metropolitan Area Network)

Les MAN interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres) à des débits importants. Ainsi, un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Un MAN est formé de commutateur ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

1.2.4.4 Le WAN (Wide Area Network)

Un WAN interconnecte plusieurs LANs à travers une de grandes distances géographiques. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre le nœud du réseau.

Le plus connu des WAN est interne.

1.2.5 Les modèles réseaux

Les personnes eurent l'idée de les relier entre eux enfin qu'ils puissent échanger des données : c'est le concept du réseau. Mais pour que ces ordinateurs puissent communiquer, il a fallu mettre des liaisons physiques pour leur interconnexion. Toutefois, cette conception s'est traduite par une incompatibilité entre de nombreux réseaux informatiques: d'où l'apparition du modèle en couche pour être une référence.

1.2.5.1 Principe des modèles en couches

Lorsque les réseaux informatiques ont pris de l'importance, l'ISO (International Standards Organization) et l'UIT-T (Union Internationale des Télécommunications) ont décidé de créer un modèle de base pour définir les différentes fonctions que doit remplir un réseau. Ce modèle est baptisé modèle OSI.

1.2.5.2 Le modèle de référence OSI (Open System Interconnections)

Le modèle OSI est constitué de sept couches que nous représentons verticalement. A chaque couche est associée une fonction bien précise. Une couche ne définit pas un protocole, elle délimite un service qui peut être réalisé par plusieurs protocoles de différentes origines. Ainsi chaque couche peut contenir tous les protocoles, du moment que ceux-ci fournissent le service demandé

à ce niveau du modèle. Par contre chaque couche effectue une seule fonction et dépend des services de la couche immédiatement inférieure. De même, chaque couche fournit ses services à la couche immédiatement supérieure. [4]

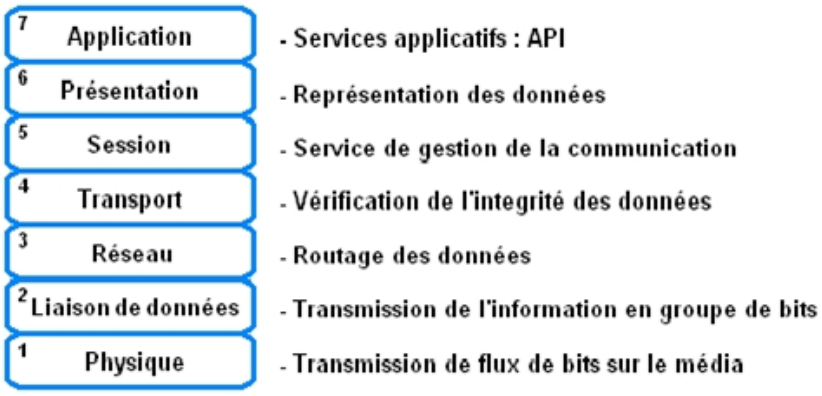


Figure 1.07 : *Modèle OSI*

De bas en haut, selon la figure ci-dessous, nous allons expliquer chaque couche réseau.

- La couche physique

Elle s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.
L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel. [4][5]

- La couche liaison des données

Son rôle est un rôle de "liant" : elle va transformer la couche physique en une liaison a priori exemple d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données. [4]

- La couche réseau

C'est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous- réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...).

La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat.

L'unité d'information de la couche réseau est le paquet

- La couche transport

Cette couche est responsable du bon acheminement des messages complets au destinataire.

Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté.

Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit.

A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session. [4][5]

L'unité d'information de la couche réseau est le message.

- La couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

- La couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

- La couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...

[4][5] [6]

1.2.5.3 Le modèle TCP/IP ou modèle DoD (Department of Defense)

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP. [4]

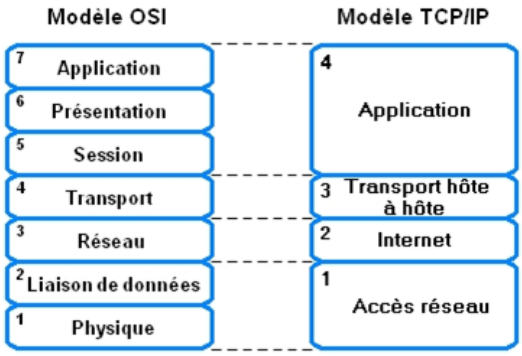


Figure 1.08 : *Modèle OSI et Modèle TCP/IP*

Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles.

Comme le modèle OSI, nous allons expliquer le rôle de chaque couche.

- La couche accès réseau ou hôte réseau

Cette couche est assez "étrange". En effet, elle semble "regrouper" les couches physiques et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte

de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau. [5]

- La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures. Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI. [5]

La couche internet possède une implémentation officielle : le protocole IP (Internet Protocol).

- La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion. [5]

- La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser.

Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP (protocole simplifié de transfert des fichiers) plus rapide que le protocole
FTP qui utilise TCP (protocole de transfert de fichiers). A l'inverse, SMTP (protocole simple de transfert de fichiers) utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs. [5]

1.2.6 La suite des protocoles TCP/IP

1.2.6.1 Internet Protocole

IP est un protocole qui se charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP. Il fournit un système de remise de données optimisé sans connexion. Le terme « optimisé » souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi. La fonctionnalité de somme de contrôle du protocole ne confirme que l'intégrité de l'en-tête IP.
Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP (et de leur ordre de réception).
Le protocole IP travaille en mode non connecté, c'est-à-dire que les paquets émis par le niveau 3 sont acheminés de manière autonome (datagrammes), sans garantie de livraison.
Le datagramme correspond au format de paquet défini par le protocole Internet. Les cinq ou six (sixième facultatif) premier mots de 32 bits représentent les informations de contrôle appelées en-tête. [4][5]

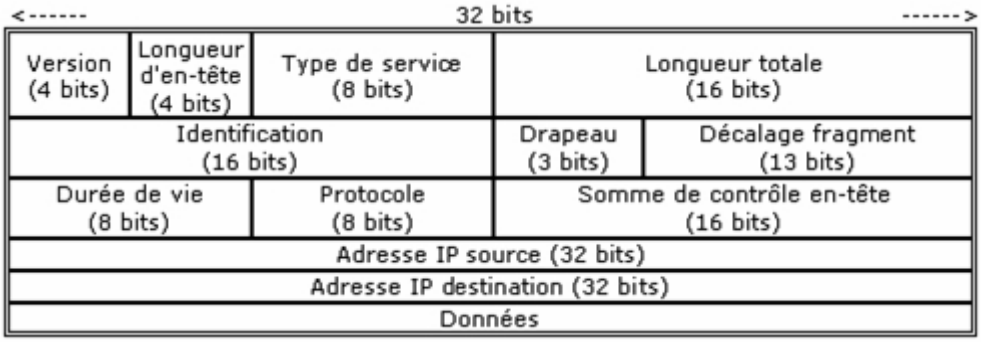


Figure 1.09 : *datagramme IP*

L'adresse IP sert à repérer un hôte unique sur l'Internet. La particularité du format d'adresse adopté avec le protocole IP est qu'il associe une partie réseau et une partie hôte en une adresse unique :

- La partie réseau est commune à l'ensemble des hôtes d'un même réseau,
- La partie hôte qui identifie chaque station du réseau

Nous avons deux versions d'adresse IP : IPV4 et IPV6 (codée sur 128 bits). IPV4 est la première version d'IP à avoir été largement déployée et qui forme la base d'internet.

Chaque interface d'un hôte IPv4 se voit attribuer une ou plusieurs adresses IP codées sur 32 bits. Au maximum 4 294 967 296 (soit 232) adresses peuvent donc être attribuées simultanément en théorie (en pratique, un certain nombre ne sont pas utilisables).

On écrit toujours ces adresses sous la forme de 4 octets notés en décimal séparés par des points. Par exemple : 192.168.10.66. [4]

À l'origine, nous avons défini plusieurs classes d'adresses IP : les classes A, B, C et D.

- Classe A

Le premier octet d'une adresse IP a une valeur strictement inférieure à 128. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

- Classe B

Le premier octet a une valeur comprise entre 128 et 192. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

- Classe C

Le premier octet a une valeur comprise entre 192 et 223. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte

- Classe D

Le premier octet a une valeur comprise entre 224 et 239. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion.

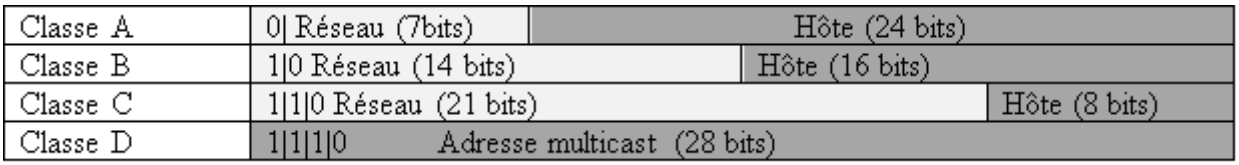


Figure 1.10 : *Etendue de chaque classe*

- Classe E

Le premier octet a une valeur supérieure à 240. Il s'agit d'une zone d'adresses réservées aux expérimentations.

Aujourd'hui, ces classes ont peu à peu perdu leur signification puisque l'espace d'adressage IP a été redécoupé pour être distribué plus équitablement grâce aux fonctions CIDR ou Classless Inter-Domain Routing (c'est une méthode d'allocation des adresses IP et du routage Internet Protocol paquets. L'Internet Engineering Task Force introduit CIDR en 1993 pour remplacer l'architecture précédente d'adressage de réseau basé sur des classes de conception dans l'Internet. Leur but était de ralentir la croissance des tables de routage sur les routeurs à travers l'Internet, et pour aider à ralentir l'épuisement rapide des adresses IPv4. [2]

1.2.6.2 TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) est un protocole de couche de transport orienté session et est destiné à fournir une connexion fiable entre deux systèmes pour échanger des données.
TCP garantit que tous les paquets sont reçus dans l'ordre. Cela permet de s'assurer que les deux systèmes sont prêts à échanger des données et qu'ainsi aucune information voyageant de l'un à l'autre ne sera égarée. Les services qui utilisent TCP comme mécanisme de communication attendent les requêtes des clients sur des numéros de port spécifiques. [4]

1.2.6.3 UDP (User Data Protocol)

UDP (User Data Protocol) implémente un mécanisme non fiable et non connecté pour envoyer des données. Plutôt que de fournir des techniques pour garantir la réception et séquence de données, l'UDP laisse les applications de haut niveau prendre en charge les paquets perdus ou désordonnés. Ce protocole permet l'envoi des messages appelée datagramme en évitant la surcharge due à l'envoie des ACK et l'établissement de la session. UDP est essentiellement utilisé par les communications de type diffusion. [2][3]

1.2.6.4 ICMP (Internet Control Message Protocol)

ICMP est un protocole de maintenance utilisé pour les tests et les diagnostics, qui véhicule des messages de contrôle. Il permet à deux systèmes d'un réseau IP de partager des informations d'état et d'erreur.
La commande Ping utilise les paquets ICMP de demande d'écho et de réponse à un écho afin de déterminer si un système IP donné d'un réseau fonctionne. C'est pourquoi l'utilitaire Ping est utilisé pour diagnostiquer les défaillances au niveau d'un réseau IP ou des routeurs. [2][3]

1.2.7 Fonctionnement général des protocoles applicatifs

Pour désigner les informations transmises et leur enveloppe, selon le niveau concerné, on parle de message(ou de flux) entre applications, de datagramme (ou segment) au niveau TCP, de paquet au niveau IP, et enfin, de trames au niveau de l'interface réseau (Ethernet ou Token Ring).
Les protocoles du niveau application les plus connus sont :

- HTTP (Hyper Text Transfer Protocol) permet l'accès aux documents HTML et le transfert de fichiers depuis un site WWW.
- FTP (File Transfer Protocol) pour le transfert de fichiers s'appuie sur TCP et établit une connexion sur un serveur FTP.

Telnet pour la connexion à distance en émulation terminal, à un hôte Unix/Linux.

- SMTP (Simple Mail Transfer Protocol) pour la messagerie électronique (UDP et TCP)
- SNMP (Simple Network Management Protocol) pour l'administration du réseau
- NFS (Network File System) pour le partage des fichiers Unix/Linux.

1.3 Les éléments constitutifs d'un réseau

1.3.1 Réseau local

Un réseau local est défini comme l'ensemble des ressources téléinformatiques permettant l'échange à haut débit de données entre équipements dans une zone géographique privée (entreprise, hôpital, campus, …). [2]

1.3.1.1 Le serveur

En principe lorsque nous parlons d'un réseau, il ne faut pas oublier la notion de client et serveur. Le serveur est une « grande machine » (en terme d'espace de stockage surtout), dans le cas général, capable de gérer les ressources communes à tous les utilisateurs et de fournir des services tels que le mail, le transfert de fichier, etc. De nombreuses applications fonctionnent selon l'architecture client/serveur. [1]

1.3.1.2 Le client

Les clients sont les ordinateurs qui exploitent les services du serveur. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc. Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les

machines clientes. Nous parlons ainsi de client FTP, de client de messagerie, etc. Un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur. [1]

1.3.2 Les supports physiques

Ce sont les voies de communication ou support utilisé dans le réseau. Ils peuvent être métalliques ou optiques ou onde radio.

- Le câble coaxial : c'est un ancien support de moins en moins utilisé. Il existe deux types qui sont le câble coaxial fin et le câble coaxial gros. Ses câbles ont permis de définir la norme du réseau Ethernet
- La paire torsadée : elle est formée de deux fils de cuivre spiral entourée chacune des gaines isolantes ou plastiques. Le câble de paires torsadées est formé de quatre paires.
- La fibre optique : elle est utilisée dans les transmissions à haut débit. Il existe deux types qui sont : monomode, type de câblage qui propage un faisceau et multimode qui est un câble à fibre dans laquelle la source génératrice de lumière est une diode lumineuse et elle supporte plusieurs fréquences de lumière.
- L'onde radio : nous utilisons actuellement des réseaux sans fil. Le média utilisé est alors des ondes électromagnétiques.

1.3.3 Les équipements réseaux

1.3.3.1 La carte réseau

Il s'agit d'une carte connectée sur la carte-mère de l'ordinateur et permettant de l'interfacer au support physique, c'est-à-dire à la ligne physique permettant de transmettre l'information

1.3.3.2 Le transceiver ou adapteur

C'est une interface permettant le raccordement des deux types de câbles.
Il permet d'assurer la transformation des signaux circulant sur le support physique en signaux logiques manipulables par la carte réseau, aussi bien à l'émission qu'à la réception.

1.3.3.3 Le répéteur

C’est un dispositif matériel permettant d’étendre l’utilisation d’un média (fibre optique, câble coaxial…) au-delà de ses capacités normales, en réémettant le signal et en l’amplifiant.

1.3.3.4 Le pont

C’est un équipement permettant l’interconnexion de deux réseaux de même type et travaillant avec les mêmes protocoles. Il permet de filtrer le trafic sur un réseau pour conserver le trafic local au niveau local et permettant ainsi d’établir une connectivité avec d’autres parties du réseau.
Comme chaque unité du réseau possède une adresse MAC unique, le pont effectue le suivi de ces adresses et prend des décisions suivant la valeur de ces adresses. [1]

1.3.3.5 Le concentrateur ou hub

C’est un périphérique de connexion de réseau local. Utilisé pour la connexion des segments réseaux, le concentrateur comporte plusieurs ports. Lorsque les données arrivent sur l’un des ports, elles sont copiées vers les autres et peuvent ainsi être lues et manipulées par tous les utilisateurs du réseau. Ce système ancien est lent. [1]

1.3.3.6 Le commutateur ou switch

Le commutateur est une unité de couche 2(liaison de donnée). Il prend des décisions en fonction des adresses MAC (Media Access Control address). Il vise à concentrer la connectivité tout en accroissant l'efficacité de la transmission de données. Une partie de leurs fonctions réside dans la concentration de la connectivité (ce qui permet de connecter plusieurs unités à un point du réseau). Il commute les trames des ports d'entrée (interfaces) aux ports de sortie, tout en fournissant à chaque port une pleine bande passante. Le symbole d'un commutateur est présenté dans la figure. Les flèches sur le haut représentent les chemins distincts que peuvent emprunter les données dans un commutateur. [1]

Figure 1.12 *: Commutateur de groupe de travail*

1.3.3.7 Le routeur

C’est un équipement qui dispose un certain nombre de ports. Son rôle consiste à examiner les paquets entrants puis à choisir le meilleur chemin ou route pour les transporter sur le réseau et pour les commuter vers un port de sortie.
Sur les grands réseaux (par exemple internet) le routeur sert de régulation de trafic. Il permet à n’importe quel type d’ordinateur appartenant à un réseau quelconque de communiquer avec n’importe quel autre ordinateur dans un autre réseau éparpillé dans le monde. [1]

Figure 1.13 *: Symbole d’un routeur*

1.4 Conclusion

Le développement fulgurant de la technologie a permis de créer le réseau informatique qui permet de véhiculer les données. L’utilité des débits plus élevés et la nécessité d’interconnexion entre de plus en plus de machines ont poussés les constructeurs à créer les réseaux informatiques, qui seront ensuite liés entre eux, engendrant ainsi la classification de ces réseaux en : PAN, LAN, MAN, RAN, et WAN. Des protocoles ont été adoptés pour régir les règles d’échanges, parmi eux l’OSI (Open System Interconnexion) qui classe les étapes des communications en 7 couches bien définis. Ce chapitre montre le strict minimum sur les notions de base sur les réseaux informatiques. On va voir sur le prochain chapitre les piratages informatique et l’étude de sécurité.

CHAPITRE 2

LES ATTAQUES INFORMATIQUES ET L'ETUDE DE SECURITES RESEAUX

2.1 Introduction

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.
Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant des systèmes et généralement préjudiciables. Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.
Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

2.2 Le piratage informatique

Tout accès à un système informatique, quels que soient les moyens utilisés pour y parvenir, sans en avoir eu le droit fait partie de ce que l'on appelle « piratage informatique ».
Ses aspects sont innombrables : vol et/ou destruction d'informations confidentielles, sabotage d'outils de travail informatique, détournement de ressources informatiques dont l'espace disque ainsi que l'accès internet à haut débit.

2.2.1 Typologies de pirates

2.2.1.1 Qu'est-ce qu'un hacker ?

Le terme « hacker » est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatiques aiment à penser qu'ils ont été attaqués par des pirates chevronnés ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour en exploiter les failles.
Le terme hacker a eu plus d'une signification depuis son apparition à la fin des années 50. A l'origine ce nom désignait d'une façon méliorative les programmeurs émérites, puis il servit au cours des années 70 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques. C'est au cours des années 80

que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéo, en désamorçant les protections de ces derniers, puis en en revendant des copies. Aujourd'hui ce mot est souvent utilisé à tort pour désigner les personnes s'introduisant dans les systèmes informatiques.[8][9]

2.2.1.2 Les différents types de pirates

En réalité il existe de nombreux types d'"attaquants" catégorisés selon leur expérience et selon leurs motivations :

- Les « white hat hackers », hackers au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui; Le courrier électronique est un des meilleurs exemples.
- Les « black hat hackers », plus couramment appelés pirates, c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans un but nuisible ;
- Les « script kiddies » (traduisez gamins du script, parfois également surnommés crashers, lamers ou encore packet monkeys, soit les singes des paquets réseau) sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.
- Les « phreakers » sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques (qualifiées de box, comme la blue box, la violet box, ...) connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement. On appelle ainsi « phreaking » le piratage de ligne téléphonique.
- Les « carders » s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles. Le terme carding désigne le piratage de cartes à puce.
- Les « crackers » ne sont pas des biscuits apéritifs au fromage mais des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants. Un « crack » est ainsi un programme créé exécutable chargé de modifier (patcher) le logiciel original afin d'en supprimer les protections.[8][9]

2.2.2 Les pirates informatiques

Le plus grand nombre d'entre eux est constitué par les « kiddies », c'est-à-dire des adolescents qui veulent épater leurs amis en prenant la main sur tel ou tel site plus ou moins connu. Il n'est pas indispensable d'être un génie des systèmes et des réseaux pour devenir un pirate informatique. Tout ce qu'il faut, c'est une petite dose de curiosité ajoutée à la méconnaissance des risques encourus. Du point de vue pratique, tous les outils sont disponibles sur le Web. Avec quelques mots-clés et un bon moteur de recherche, un jeune pirate se trouvera en quelques minutes en possession d'une panoplie d'outils permettant de prendre le contrôle d'une machine, quelque part dans le monde. A l'autre extrême, un petit nombre de pirates est issu de la communauté des « crackers ». Eux par contre, ils étudient les failles des systèmes et écrivent des programmes permettant d'en prendre le contrôle. Ils publient ces programmes qui sont alors mis en œuvre par des « kiddies ».[8][9]

2.2.3 Anatomie d'une attaque, Les cinq P

Toutes les attaques informatiques sont basées sur ce qu'on appelle « les 5 P » : Prospecter – Pénétrer – Persister – Propager – Paralyser

- Prospecter : C'est une phase où l'agresseur collecte des informations sur une cible potentielle. Le but de cette phase est de dresser une cartographie du réseau et d'obtenir des détails sur les systèmes. L'agresseur choisit ainsi une attaque en fonction des vulnérabilités connues pour les versions des applications utilisées ou explore la possibilité d'erreurs de configuration.
- Pénétrer : L'étape qui suit la découverte des systèmes et service potentiellement vulnérables est l'attaque. Elle peut prendre de nombreuses formes et résulter en l'exécution des programmes de l'agresseur sur l'un des systèmes. Si l'agresseur n'a gagné qu'un accès à un utilisateur sans privilèges, il tenterait d'obtenir l'accès à un compte possédant des droits d'administration. L'attaque peut simplement conduire au dysfonctionnement d'un service ou du système complet.
- Persister : Lorsqu'un agresseur parvient à trouver un système vulnérable, puis à trouver ou construire une attaque et, enfin, à s'introduire avec succès dans le système, il n'aimerait pas recommencer entièrement ce processus chaque fois qu'il souhaiterait y accéder. C'est pourquoi la première action qu'entreprend un agresseur qui réussit à « s'approprier » une

machine est d'installer un dispositif qui lui permet de revenir aisément sur le système. L'agresseur peut aussi installer un programme de contrôle à distance. Cela lui permet de travailler plus facilement à distance sur le système.

- Propager : Une fois l'agresseur bien installé sur le système, la prochaine étape consiste à évaluer ce qui devient accessible sur le réseau pirate, que ce soit au niveau des ressources ou des services à sa disposition. Le pirate va chercher à étendre son contrôle sur plusieurs systèmes.
- Paralyser : Voici l'objectif ultime d'une agression ciblée, si l'agresseur en a après votre environnement dans un but bien précis. Ce but pourrait être le vol ou la détérioration de données, la mise hors service de vos systèmes ou l'attaque d'une autre organisation depuis l'un d'eux, vous faisant ainsi passer pour responsable.[8][9]

2.2.4 Les différentes techniques d'attaque

Les attaques des systèmes informatiques sont de plus en plus automatisées par les pirates.
Elles sont basées sur trois principes : l'attaque directe, l'attaque indirecte par rebonds et l'attaque indirecte par réponse. [8]

2.2.4.1 L'attaque directe

Dans ce cas, le pirate attaque directement sa victime à partir de son ordinateur. La plupart des « kiddies » utilisent cette technique.
En effet, les programmes de cracking qu'ils utilisent ne sont que faiblement paramétrables et un grand nombre de ces logiciels envoient directement les paquets à la machine cible.

Figure 2.01 : *Principe de l'attaque directe*

2.2.4.2 L’attaque indirecte par rebonds

Son principe est le suivant : les paquets sont envoyés à un ordinateur intermédiaire qui répercute l’attaque vers la machine victime. Ce procédé permet au pirate de masquer son identité, c’est à dire son adresse IP et en même temps d’utiliser les ressources de l’ordinateur intermédiaire dont la puissance de calcul et l’espace disque pour attaquer la machine visée.

Figure 2.02 : *Principe de l’attaque indirecte par rebonds*

Une autre variante de cette attaque consiste à effectuer une multitude de rebonds. Les pirates les plus connus du monde l’ont tous utilisé pour se procurer une certaine impunité. Remonter à la source après avoir été victime d’une telle attaque n’est pas chose facile. En effet, il faudra contacter les sites correspondants qui, tour à tour, vont mettre un certain temps à trouver la cause de l’attaque puis protester auprès du site attaquant. Il reste à faire en sorte que cela ne prenne pas assez de temps avant que les traces les plus flagrantes de la machine du pirate contenues dans les routeurs ne disparaissent.[9]

2.2.4.3 L’attaque indirecte par réponse

Au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, la machine du pirate va lui envoyer une requête. Et c'est la réponse à cette requête qui va être envoyée à l'ordinateur victime.

Figure 2.03 : *Principe de l’attaque indirecte par réponse*

Plus le nombre d'ordinateurs intermédiaires compromis par le pirate sera élevé, plus le repérage de la source de l'attaque sera ardu.[9]

2.2.4.4 Le scam

Le « scam » est une pratique frauduleuse, consistant à extorquer des fonds à des internautes en leur aisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage.
L'arnaque du « scam » est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.[8]

2.2.4.5 L'IP Spoofing

La technique de l'IP Spoofing est une technique dont le principe est relativement ancien (aux alentours de 1985) mais la première attaque connue l'utilisant ne remonte qu'à 1995. Le Spoofing n'est pas une attaque en tant que telle : il s'agit d'une technique permettant de s'infiltrer dans un ordinateur en se faisant passer pour un autre en qui il a confiance (Trusted Host).
Voici le fonctionnement de cette technique: une station se fait passer pour une autre en envoyant un paquet dont l'adresse IP est autorisée à passer par le serveur visé. La source IP envoyée trompe donc la cible qui accorde l'accès en pensant avoir affaire à une machine de confiance.[9]

2.2.4.6 L'hijacking

L' hijacking ou détournement de session est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session. Beaucoup d'attaques viennent de l'intérieur des entreprises.

2.2.5 Les principales attaques

2.2.5.1 Virus

Un virus est un exécutable qui va exécuter des opérations plus ou moins destructrices sur votre machine. Les virus existent depuis que l'informatique est née et se propageaient initialement par disquettes de jeux ou logiciels divers, etc. Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

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

Les virus peuvent être très virulents. Mais ils coûtent aussi beaucoup de temps en mise en place d'antivirus et dans la réparation des dégâts causés. On peut malheureusement trouver facilement des logiciels capables de générer des virus et donc permettant à des « amateurs » n(aussi appelés « crackers ») d'étaler leur incompétence. [9]

2.2.5.2 Deni de service (DoS)

Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- L'inondation d'un réseau afin d'empêcher son fonctionnement ;
- La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- L'obstruction d'accès à un service à une personne en particulier. L'attaque par déni de service peut ainsi bloquer un serveur de fichier, rendre impossible l'accès à un serveur web, empêcher la distribution de courriel dans une entreprise ou rendre indisponible un site internet. [9][10]

2.2.5.3 Ecoute du réseau (sniffer)

Il existe des logiciels qui, à l'image des analyseurs de réseau, permettent d'intercepter certaines informations qui transitent sur un réseau local, en retranscrivant les trames dans un format plus lisible (Network packet sniffing). C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en « broadcast » sur le réseau local peuvent être interceptées. De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.[9]

2.2.5.4 L'intrusion

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique, chantage…
Ce type d'attaque consiste à exploiter une vulnérabilité d'une application en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l'application. [8][9]

2.2.5.5 Cheval de Troie

L'image retenue de la mythologie est parlante. Le pirate, après avoir accédé à votre système ou en utilisant votre crédulité, installe un logiciel qui va, à votre insu, lui transmettre par Internet les informations de vos disques durs. Un tel logiciel, aussi appelé troyen ou « trojan », peut aussi être utilisé pour générer de nouvelles attaques sur d'autres serveurs en passant par le vôtre. Certains d'entre eux sont des « key logger » c'est-à-dire qu'ils enregistrent les frappes faites au clavier.[9]

2.2.5.6 L'ingénierie sociale et l'irresponsabilité

Lorsque quelqu'un désire pénétrer dans un système informatique, sa première arme est le "bluff". Il n'y a généralement pas d'attaques réussies sans relations humaines. On appel ceci l'ingénierie sociale (social engineering), elle est basée sur quatre grands principes:

- Le contexte en ayant une bonne connaissance de l'organigramme de l'entreprise cela permet à l'agresseur d'avoir d'ores et déjà un pied dans l'entreprise. Le but en général est de connaître qu'elles sont les personnes qui sont en droit de demander telles ou telles

informations, et également à qui les demander, dans le but de se faire ultérieurement passer pour elles.

- L'audace ou le bluff : le bavardage et l'art de la parole sont deux qualités indispensables lorsque l'on veut utiliser le "social engineering". Il s'agit ici d'avoir suffisamment d'appoint et de connaissances techniques afin de faire croire à l'interlocuteur qu'il a affaire à un responsable technique de l'entreprise (ou d'un fournisseur de service). Tout ceci afin qu'il lui transmette les informations demandées sans aucun problème.
- La chance : la chance est également une part importante dans le "social engineering", cela ne marche pas à chaque fois ! Il faut de la pratique afin de bien maîtriser le séquencement du dialogue à établir.
- La patience calculée : il faut de plus savoir se montrer patient afin d'obtenir les informations désirées. Malgré tout, la méthode du "social engineering" demande une certaine rapidité (maximum : 1 heure) pour obtenir les informations voulues. Passé ce délai, il est préférable de changer d'entreprise ou d'attendre quelques jours afin de ne pas éveiller les soupçons. [8][9]

a-Le phishing

C'est une technique d'ingénierie sociale. Le phishing fait toujours autant parler de lui. Ces pages Web détournées qui ressemblent en tous points au site original, sont envoyées en même temps qu'un courrier électronique indésirable provenant d'une soi-disant banque et demandent de transmettre des données importantes / confidentielles telles que numéros de téléphone, numéros de compte bancaire et parfois de carte de crédit. Ces informations sont une aubaine pour le « phisher ». [8]

b-Les hoaxs

Tout courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues est un « hoax » ou canular. Son but est de provoquer la satisfaction de son concepteur d'avoir berné une masse énorme de personnes.
A force de recevoir des fausses nouvelles, certains internautes finissent par ne plus croire aux vraies. [8]

2.2.5.7 Man in the middle

Moins connue, mais tout aussi efficace, cette attaque permet de détourner le trafic entre deux stations. Imaginons un client C communiquant avec un serveur S. un pirate peut détourner le trafic du client en faisant passer les requêtes de C vers S par sa machine P, puis transmettre les requêtes de P vers S. Et inversement pour les réponses de S vers C.
Totalement transparente pour le client, la machine P joue le rôle de proxy. Il accédera ainsi à toutes les communications et pourra en obtenir les informations sans que l'utilisateur s'en rende compte. [9]

2.3 La sécurité informatique

2.3.1 Principe de la sécurité

Avant de pouvoir sécuriser un réseau informatique, il faut d'abord établir certains principes pour identifier les éléments à protéger.

2.3.1.1 Définition de la politique de sécurité

La politique de sécurité est le document de référence définissant les objectifs pour suivis en matière de sécurité et les moyens mis en œuvre pour les assurer.
La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.
Dans le cas d'une entreprise, un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner à la politique de sécurité le maximum d'impact. [10]

2.3.1.2 Exigences fondamentales

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

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

La sécurité recouvre ainsi plusieurs aspects :

- intégrité des informations (pas de modification ni destruction)
- confidentialité (pas de divulgation à des tiers non autorisés)
- authentification des interlocuteurs (signature)
- respect de la vie privée (informatique et liberté)

Du point de vue de la sécurité informatique, une menace est une violation potentielle de la sécurité. Cette menace peut-être accidentelle, intentionnelle (attaque), active ou passive. [10][11]

2.3.1.3 Etude des risques

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi.
Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé. Il faut cependant prendre conscience que les principaux risques restent : les câbles arrachés, la coupure secteur, le crash disque, le mauvais profil utilisateur, etc.
Cependant, voici quelques éléments pouvant servir de base à une étude de risque:

- la valeur des équipements, des logiciels et surtout des informations ;
- le coût et le délai de remplacement de ces derniers;
- l’analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, des logs etc.) ;
- l’impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société.[8]

2.3.2 Les stratégies de sécurité

Pour se protéger contre les menaces des pirates informatiques, le déploiement de la sécurité informatique est devenu inévitable. Pour ce faire, différentes stratégies ont été adoptées.

2.3.2.1 Le principe de moindre privilège

Le principe de sécurité le plus fondamental est celui du moindre privilège. À la base, il signifie que toute entité (utilisateur, programme, système, …) ne doit disposer que des privilèges (ou droit) dont il a besoin pour effectuer ses tâches assignées. Cela limite l'exposition aux attaques ainsi que les dommages occasionnés.

2.3.2.2 La sécurité par l'hôte

La stratégie la plus courante de sécurité informatique consiste à renforcer la sécurité sur les serveurs. Chaque machine hôte fera ensuite l'objet d'une sécurisation indépendante.
Le principal frein à une sécurisation effective des serveurs tient à la complexité et à la diversité de ces derniers. De plus, ce principe ne fonctionne pas sur des machines individuelles et ne correspond pas non plus à l'échelle d'un vaste réseau sous peine d'un travail humain excessif. [10]

2.3.2.3 La sécurité par réseau

Au fur et à mesure que les environnements croissent en taille et en diversité, et que leur sécurisation machine par machine devient difficile, de plus en plus de sites se tournent vers un modèle de sécurité par réseau. Dans ce cas de figure, on met l'accent sur le contrôle de l'accès réseau aux divers serveurs et aux services qu'ils offrent au lieu de les sécuriser un par un. Ce modèle inclut donc la réalisation de systèmes de filtrage puissants que sont les pare-feu pour restreindre les communications entre le réseau interne à protéger et le réseau extérieur. [11]

2.3.3 Etat de la sécurité informatique

En dépit de la perpétuelle évolution de la technologie informatique, un fait demeure : à une nouvelle technologie est associé un lot de vulnérabilités. Ce sont, soit des erreurs de conception, soit des erreurs de programmation ou « bugs ». Si ce n'était pas le cas, il ne serait pas nécessaire de s'inquiéter de la sécurité d'un système d'information. C'est pour cela que la sécurité ne peut être sûre à 100 %. De plus, les systèmes de sécurité sont faits, gérés et configurés par des hommes.

La sécurité d'un système est souvent chère et difficile. Certaines organisations n'ont pas de budget pour ça. D'autres acceptent de courir le risque, pour eux la sécurité n'est pas une priorité. [10][11]

2.3.4 La meilleure façon de procéder

Recourir à des outils logiciels et matériels n'est pas le plus important pour mieux protéger un réseau des éventuelles attaques. Il s'agit plutôt d'une question de méthode.

2.3.4.1 Identification des informations à protéger

Un serveur contient des informations sensibles. Si personne ne consulte régulièrement ces informations, il n'y a aucune raison de les laisser sur le serveur connecté au réseau.
Quant aux données utilisées par certains utilisateurs, la mise en place d'un contrôle d'accès sérieux sur le serveur concerné est indispensable pour assurer l'authentification.
De même, chaque ordinateur ne sera accessible que par un login et un mot de passe.
Cependant, rien ne sert de sécuriser le réseau pour empêcher l'espionnage si quelqu'un peut s'emparer du disque dur. Un serveur contenant des informations sensibles doit être physiquement protégé. [11]

2.3.4.2 Recherche des failles de sécurité avant les pirates

Les « crackers » utilisent des logiciels connus pour détecter les erreurs de configuration, les erreurs de programmation des systèmes utilisés dans le réseau cible. L'idéal pour un administrateur réseau serait de trouver ces « bugs» avant le pirate et de les corriger à temps avant qu'ils soient exploités par des personnes malveillantes. La méthode pour la détection des failles est la même que celle utilisée par l'attaquant.

2.3.4.3 Suivi et gestion quotidien du système d'information

Le système informatique parfaitement inviolable n'existe pas. Au cours du temps, l'administrateur système et réseau améliore la sécurité du système dont il a la gestion, tandis que le pirate, lui, trouve de nouvelles failles plus ingénieuses. La sécurité informatique est un domaine où la surenchère est permanente. Découvrir rapidement une compromission ou une tentative de compromission permet d'éviter ou de limiter l'étendue des dommages. D'où la nécessité d'une surveillance régulière pour une détection efficace des attaques. Un système bien protégé est avant tout un système mis à jour. [10]

2.4 Les outils indispensables pour la sécurisation du réseau

Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant. Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble , de se protéger des intrusions réseaux en installant un dispositif de protection.

En fait, quel que soit le rôle que nous jouons, attaquant ou défenseur, nous utilisons des outils similaires. Car toute personne qui voudra protéger son réseau aura à cœur de le tester lui- même, et tout intrus voudra d'abord se protéger lui-même, soit des gens comme lui, soit du défenseur. [10]

2.4.1 L'antivirus

Les virus sont les principales causes de désagrément en entreprise mais ils peuvent être combattus à plusieurs niveaux.

La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signatures doit donc être très régulièrement mise à jour sur le site de l'éditeur (des procédures automatiques sont généralement possibles).

Deux modes de protection :

- Une généralisation de l'antivirus sur toutes les machines : il faut absolument prévoir une mise à jour automatique de tous les postes via le réseau.
- Une mise en place d'un antivirus sur les points d'entrée/sortie de données du réseau après avoir parfaitement identifiés tous ces points.

2.4.2 Le pare-feu ou firewall

Le firewall, appelé encore pare-feu ou garde-barrière est une barrière contre l'intrusion à partir de l'internet c'est-à-dire que c'est un programme et/ou un matériel chargé de protéger le réseau local du monde extérieur et de certains programmes malveillants placés sur l'ordinateur.

Il est conçu pour isoler le réseau local privé des flammes de l'internet ou encore de protéger la pureté des membres de ce même réseau.

De nos jours, toutes les entreprises possédant un réseau local possèdent aussi un accès à Internet afin d'accéder à la manne d'information disponible sur le réseau des réseaux et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, parfois gratuites, de destruction, de vol d'informations confidentielles. Les mobiles sont nombreux et dangereux.

Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un firewall. [13]

2.4.2.1 Principes

Pour assurer efficacement ses tâches, un pare-feu ou firewall doit être physiquement intercalé entre le réseau qu'il protège et l'extérieur. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès du réseau interne vers le réseau externe. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas, le meilleur exemple étant le jeu en ligne. En plaçant un firewall limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu d'utiliser et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. [12]

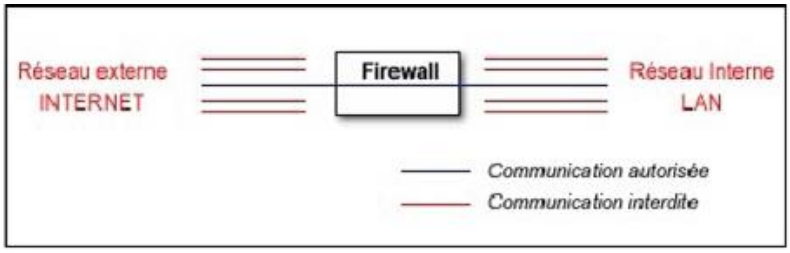


Figure 2.04 : *Architecture d'un pare-feu ou firewall*

2.4.2.2 Les différents types de pare-feu ou firewall

a. Le firewall bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker lambda. 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. [12]

b.Les firewalls matériels

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement 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 que leur interaction avec les autres fonctionnalités du routeur est simplifiée par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en terme de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la boite noire qu'est le routeur.

c. Les firewalls logiciels

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories :

- Les firewalls personnels :

  Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. 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 » :

Tournant généralement sous linux, car cet OS (Operating System) offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les firewalls matériels des routeurs, à ceci près qu'ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme. [12]

2.4.3 Les systèmes de détections d'intrusion

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. [12][13]

2.4.3.1 Snort

Snort est aussi un NIDS. Il n'est pas structuré comme Prelude. Il ne comporte pas de module comme Prelude, ce qui peut rendre son implémentation dans un réseau un peu moins souple que Prelude. Snort fonctionne en trois modes : Sniffer, PacketLogger et NIDS. Les deux premiers modes ne sont pas intéressants pour la détection d'intrusion. Le troisième mode permet, quand à, lui d'analyser le trafic réseau pour y détecter d'éventuelles attaques. [12]

2.4.3.2 Nessus

Nessus est un outil de sécurité permettant de scanner une ou plusieurs machines. Il permet aussi de tester différentes attaques pour savoir si une ou plusieurs machines sont vulnérables. Il est très utile lors de tests de pénétration (pen test) et fait gagner un temps incroyable.
Nessus se compose d'une partie serveur (qui contient une base de données regroupant différents types de vulnérabilités) et une partie client. L'utilisateur se connecte sur le serveur grâce au client et après authentification, il ordonne au serveur de procéder aux tests d'une ou plusieurs machines. Le client reçoit ensuite les résultats du test. [12]

2.4.3.3 Nmap

Nmap est un scanner de ports open source créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD.
Pour scanner les ports d'un ordinateur distant, Nmap utilise diverses techniques d'analyse
Basées sur des protocoles tels que TCP, IP, UDP ou ICMP.
De même, il se base sur les réponses particulières qu'il obtient à des requêtes particulières pour obtenir une empreinte de la pile IP, souvent spécifique du système qui l'utilise. C'est par cette méthode que l'outil permet de reconnaitre la version d'un système d'exploitation et aussi la version des services en écoute. [12][13]

2.5 Conclusion

Dans ce chapitre, on a illustré quelques différents types et caractéristiques techniques d'attaques sur le réseau informatique. Ce qui nous a permis de constater qu'il existe de nombreuses failles que les pirates peuvent exploiter. Du fait du nombre et de la variété des attaques existantes dans le monde, le renforcement des moyens de défense s'avère indispensable. On fait appel à différente sorte d'outil comme l'antivirus, les firewalls, l'IPS et le filtrage web pour assurer la protection avec du matériel Cisco ASA 5525-x. Dans le chapitre suivant, on va voir : la conception réseau hiérarchique, la généralité sur le Cisco ASA, son principe de fonctionnement, son rôle et la manipulation, le système de prévention d'intrusions et la liste de contrôle d'accès.

CHAPITRE 3

CONCEPTION ET SECURITE RESEAU AU SEIN DU MFB

3.1 Introduction

La conception de réseau hiérarchique implique la division du réseau en couches distinctes. Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global. En séparant les différentes fonctions existantes sur un réseau, la conception de réseau devient modulaire, ce qui facilite l'évolutivité et les performances. Le modèle de conception hiérarchique classique se divise en trois couches : la couche d'accès, la couche de distribution et la couche cœur de réseau. Dans ce chapitre, nous allons concevoir un réseau hiérarchique au MFB et nous abordons principalement les différents aspects liés à la sécurité dans les réseaux et nous traitons le point particulier que représentent les utilisateurs.

3.2 Architecture réseau actuel au MFB

Avant d'intégrer de nouvelles fonctionnalités et de nouvelles technologies, la nouvelle conception doit d'abord palier toutes les faiblesses identifiées du réseau actuel.

- Conception de réseau linéaire :

Ce type de conception ne permet pas d'extensibilité : le réseau ne peut donc pas s'étendre sans que cela ait un impact sur les performances.

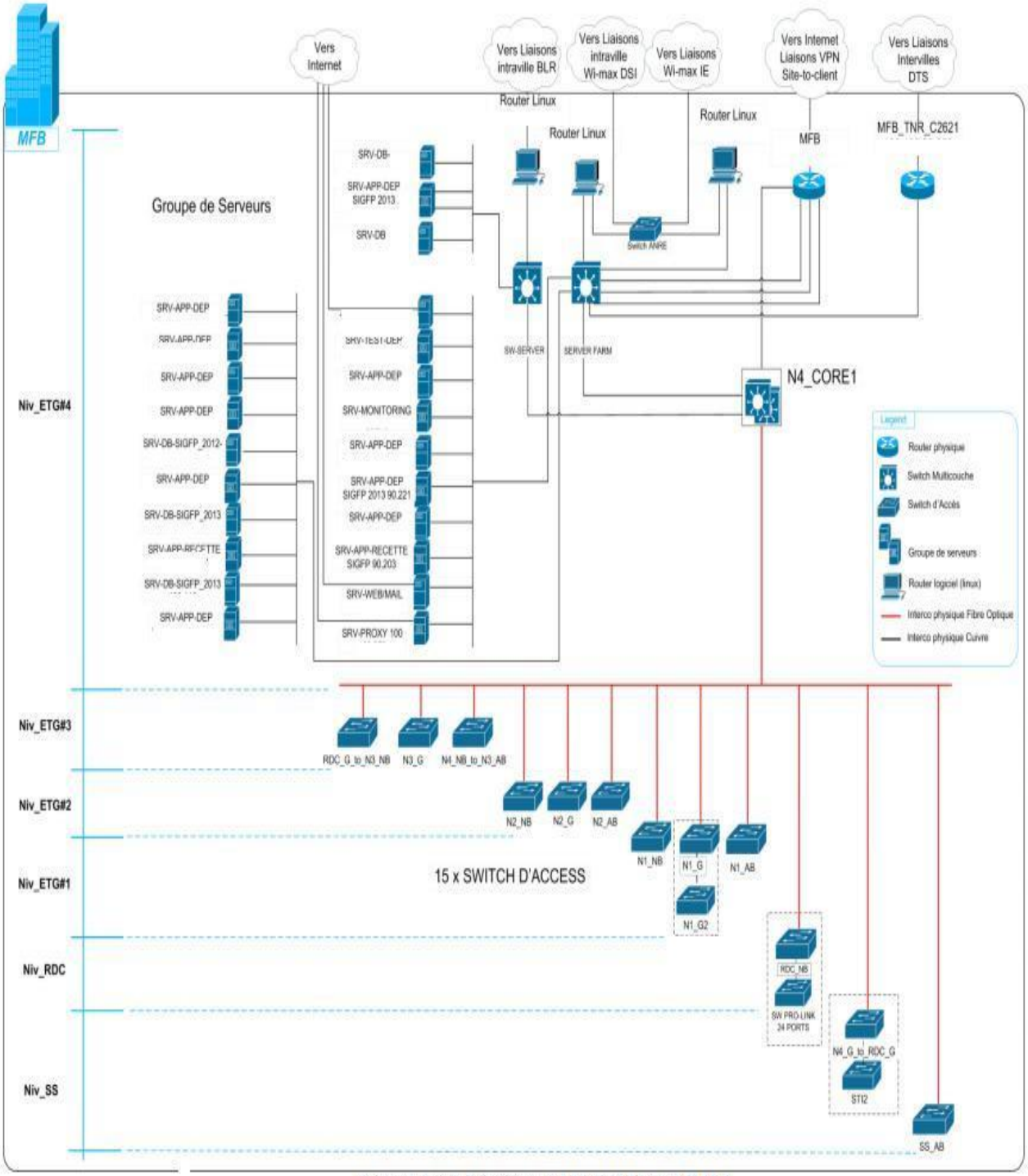
Il n'y a pas aussi de segmentation du réseau, donc impossible d'isoler ou filtrer le trafic.

- Pas de redondance :

Une panne sur un matériel du réseau peut entrainer la non-disponibilité d'une partie du réseau. De plus, on a des domaines défaillants étendus c'est-à-dire que les défaillances de liaisons et de périphériques affectent de vastes zones du réseau.

- Faiblesse de la sécurité :

La sécurité déployé est trop faible, il n'y a pas de pare-feu dynamique donc il ne fait que le filtrage et n'empêche pas tout le trafic non autorisé ou indésirable. Il n'y a pas aussi de système IDS ou IPS implémenté sur le réseau.



. *Architecture globale du réseau LAN actuel du bâtiment du MFB*

MFB/DSI/ Admin . Réseau et System

Figure 3.01 : *Architecture réseau actuel au MFB*

3.2.1 Architecture hiérarchique

La conception de réseau hiérarchique fournit des modèles de transfert de trafic efficaces, rapides et logiques pour les topologies de réseau de l'entreprise tout en minimisant le coût de la connexion de plusieurs périphériques en des extrémités du réseau. Première présenté comme une meilleure pratique par Cisco en 2002, les topologies de réseau hiérarchiques adaptent bien à l'expansion des entreprises, la mise en forme du trafic et des modèles de sécurité de réseau en séparant un réseau LAN en parties logiques qui correspondent aux besoins de l'organisation.[14]

3.2.1.1 Conception de réseau hiérarchique

En matière de réseau, une conception hiérarchique permet de regrouper des périphériques en un certain nombre de réseaux distincts qui sont alors organisés en couches. Le modèle de conception hiérarchique possède trois couches de base :

- Couche cœur de réseau : relie les périphériques de la couche de distribution.
- Couche de distribution : assure l'interconnexion entre les petits réseaux locaux.
- Couche d'accès : fournit la connectivité pour les hôtes et les périphériques du réseau.

3.2.1.2 Avantages par rapport aux réseaux non hiérarchiques

- Les réseaux hiérarchiques sont plus avantageux que les réseaux linéaires. De par la division des réseaux linéaires non hiérarchiques en sections plus petites et plus faciles à gérer, le trafic local reste véritablement local. Seul le trafic destiné aux autres réseaux est acheminé vers une couche supérieure.
- Sur un réseau non hiérarchique, les périphériques de couche 2 offrent peu d'opportunités de contrôle de diffusion et de filtrage du trafic indésirable. À mesure que de nouveaux périphériques et applications sont ajoutés à ce type de réseau, les temps de réponse se dégradent jusqu'à ce que le réseau devienne complètement inutilisable.

3.2.2 Caractéristiques et normes dans chaque couche

3.2.2.1 Couche cœur du réseau

La couche cœur de réseau est parfois appelée réseau fédérateur. Les routeurs et les commutateurs de cette couche offrent une connectivité haute vitesse. Dans un réseau local d'entreprise, la couche cœur de réseau peut assurer la connexion de plusieurs bâtiments ou sites et fournir une connectivité

pour la batterie de serveurs. Cette couche contient une ou plusieurs liaisons vers les périphériques de la périphérie du réseau, pour la prise en charge de l'accès à Internet, aux réseaux privés virtuels (VPN), à l'extranet et au réseau étendu (WAN). [14]

La mise en œuvre d'une couche cœur de réseau réduit la complexité du réseau, facilitant ainsi sa gestion et son dépannage.

- Objectifs de la couche cœur de réseau

La conception de la couche cœur de réseau permet des transferts de données efficaces et très rapides entre une section du réseau et une autre. Les principaux objectifs de conception de la couche cœur de réseau sont les suivants :

  - fournir un temps utile de 100 %
  - optimiser le débit ;
  - faciliter la croissance du réseau
- Technologies de la couche cœur de réseau : Les technologies utilisées au niveau de la couche cœur de réseau incluent :
  - routeurs ou commutateurs multicouche combinant routage et commutation dans un même périphérique ;
  - redondance et équilibrage de la charge ;
  - liaisons haute vitesse et agrégées.
- Liaisons redondantes

La mise en œuvre de liaisons redondantes au niveau de la couche cœur de réseau permet aux périphériques du réseau de trouver un chemin d'accès alternatif pour l'envoi des données, en cas de panne. Lorsque les périphériques de couche 3 sont placés dans la couche cœur de réseau, ces liaisons redondantes peuvent être utilisées pour l'équilibrage de charge ainsi que pour la sauvegarde. Dans une conception de réseau linéaire de couche 2, le protocole STP (SpanningTree Protocol) désactive les liaisons redondantes, sauf en cas d'échec de la liaison principale. Ce comportement empêche l'équilibrage de charge sur les liaisons redondantes. [14]

- Topologie maillée

La plupart des couches cœur de réseau sont câblées selon une topologie à maillage global ou à maillage partiel. Dans une topologie à maillage global, chaque périphérique dispose d'une connexion avec tous les autres périphériques. Ce type de topologie offre l'avantage d'un réseau

entièrement redondant, mais sa gestion et son câblage peuvent s'avérer difficiles et onéreux. Pour les installations de grande taille, on utilise plus couramment une topologie à maillage partiel modifié. Dans ce type de topologie, chaque périphérique est connecté à au moins deux autres, créant une redondance suffisante sans la complexité d'un maillage global. [14]

Figure 3.02 : *Cœur du réseau*

3.2.2.2 Couche distribution

- La couche d'accès est généralement créée à l'aide de la technologie de commutation de couche 2. La couche de distribution, quant à elle, est créée à partir des périphériques de couche 3. Les routeurs ou les commutateurs multicouches, situés dans la couche de distribution, fournissent diverses fonctionnalités essentielles à la réalisation des objectifs de conception du réseau. Ces objectifs incluent :
  - le filtrage et la gestion des flux de trafic ;
  - la mise en application des stratégies de contrôle d'accès ;
  - le résumé des routes avant notification à la couche cœur de réseau ;
  - l'isolation de la couche cœur de réseau par rapport aux pannes ou interruptions de service de la couche d'accès ;
  - le routage entre les réseaux locaux virtuels de la couche d'accès.

Les périphériques de la couche de distribution servent également à gérer les files d'attente et la hiérarchisation du trafic, avant la transmission via le cœur du campus. [14]

- Agrégations

Des liaisons agrégées sont souvent configurées entre les périphériques de mise en réseau des couches d'accès et de distribution. Elles servent à acheminer le trafic appartenant à plusieurs réseaux locaux virtuels entre différents périphériques, sur la même liaison. Lors de la conception des liaisons agrégées, le concepteur du réseau prend en compte la stratégie de réseau local virtuel globale et les modèles de trafic réseau.

- Liaisons redondantes

Les périphériques de la couche de distribution entre lesquels il existe des liaisons redondantes peuvent être configurés de manière à équilibrer la charge du trafic entre les différentes liaisons. L'équilibrage de charge augmente la bande passante disponible pour les applications.

- Topologie de la couche de distribution

Les réseaux dotés d'une couche de distribution sont généralement câblés selon une topologie à maillage partiel. Cette topologie offre un nombre suffisant de chemins d'accès redondants pour garantir le fonctionnement du réseau en cas de panne de périphérique ou de liaison. Les périphériques de la couche de distribution situés dans le même local technique ou centre de calcul, sont interconnectés à l'aide de liaisons Gigabit. S'ils sont séparés par de longues distances, un câble en fibre optique est utilisé. Les commutateurs capables de prendre en charge plusieurs connexions en fibre haute vitesse sont assez onéreuses ; une planification minutieuse est donc nécessaire pour garantir qu'un nombre suffisant de ports à fibre optique est disponible pour la bande passante et la redondance souhaitées. [5][14]

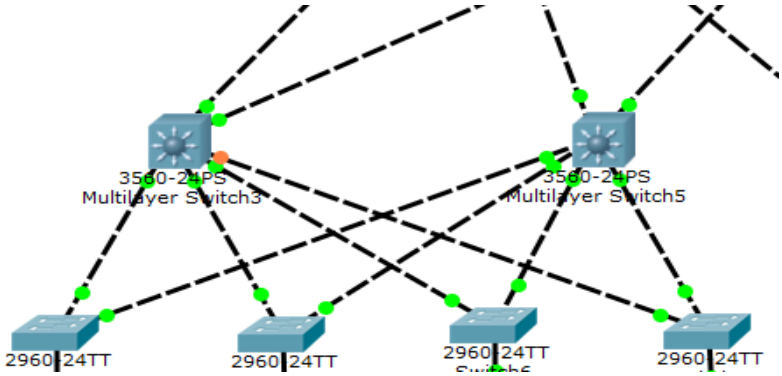


Figure 3.03 : *Couche distribution*

3.2.2.3 Couche accès

La couche d'accès correspond à la périphérie du réseau, l'endroit où les périphériques finaux se connectent. Les services et les périphériques de la couche d'accès sont situés dans chaque bâtiment du campus, chaque site distant et batterie de serveurs, et à la périphérie du réseau d'entreprise.

- Considérations physiques sur la couche d'accès

La couche d'accès de l'infrastructure de campus utilise la technologie de commutation de couche 2 pour fournir l'accès au réseau. L'accès peut se faire par l'intermédiaire d'une infrastructure

câblée permanente ou de points d'accès sans fil. La technologie Ethernet utilisée sur un câblage en cuivre impose des contraintes en termes de distance. Par conséquent, l'emplacement physique des équipements constitue l'une des principales préoccupations lors de la conception d'une couche d'accès pour une infrastructure de campus. [14][5]

- Exigences en matière de disponibilité

Dans les premiers réseaux, les seuls endroits à haute disponibilité étaient le cœur du réseau, la périphérie et les réseaux de centre de calcul. Avec la téléphonie IP, chaque téléphone doit être disponible en permanence.

Des composants redondants et des stratégies de basculement peuvent être mis en œuvre au niveau de la couche d'accès, afin d'améliorer la fiabilité et la disponibilité pour les périphériques finaux.

- Conception et facilité de gestion

Outre la connectivité de base à la couche d'accès, le concepteur doit prévoir les éléments suivants:

- Structures de création de noms
- Architecture de réseau local virtuel
- Modèles de trafic
- Stratégies de hiérarchisation

La configuration et l'utilisation sont des opérations cruciales pour les systèmes de gestion des réseaux convergents de grande taille. Il est également important de normaliser les configurations et les équipements, lorsque cela est possible. [5][14]

Le respect de principes de conception éprouvés permet d'améliorer la gestion et la prise en charge continue du réseau :

- en garantissant que le réseau ne devienne pas trop complexe ;
- en permettant un dépannage facile en cas de problème ;
- en facilitant l'ajout futur de nouveaux services et fonctions.

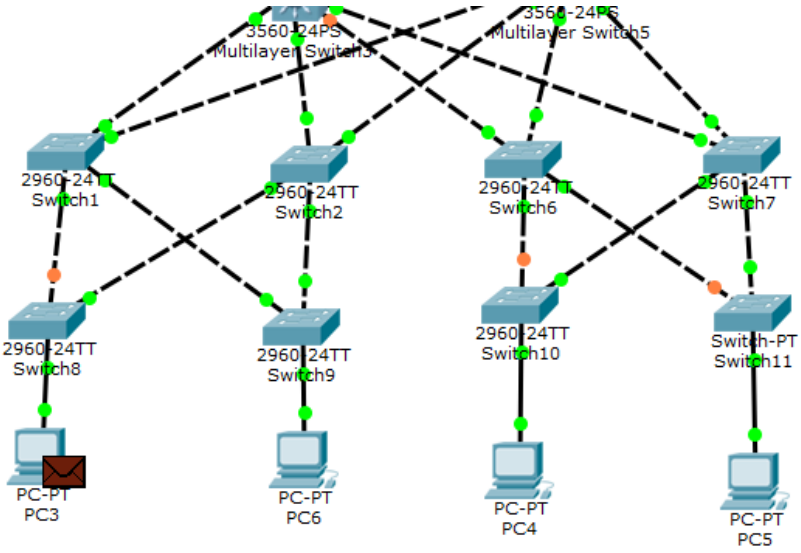


Figure 3.04 : *Couche d'accès*

3.2.3 Sécurité actuelle au MFB

3.2.3.1 Le logiciel pfsense

PfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD, il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient pour la sécurisation d'un réseau domestique ou de réseau d'entreprise.

Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web et gère nativement les VLAN. Comme sur les distributions Linux, pfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy, serveur VoIP,…

3.2.3.2 Avantages et inconvénients de pfsense

Comme toute solution de routeur/pare-feu, Pfsense possède son lot d'avantages et d'inconvénients. Mais sa polyvalence et le nombre conséquent de fonctionnalités font de cet outil une solution fiable pour les entreprises, et ce, quelles que soient la taille et l'activité de ces dernières. Le coût est un élément à prendre en compte, les systèmes d'informations ne sont pas le coeur de métier n'ont pas des budgets importants pour ce genre de solutions. Comme nous le verrons par la suite, il existe

plusieurs façons de mettre en place Pfsense, en passant par une plateforme virtuelle ou en faisant l'acquisition d'un routeur sur lequel la distribution est déjà installée. Enfin, il est important de souligner que Pfsense est très peu gourmand en termes de ressources. En effet, la configuration minimale requiert un processeur équivalent ou supérieur à 500Mhz quand la mémoire exigée est de 256Mo. Vous n'aurez donc aucune difficulté à mettre en place cette solution.

En revanche, et malgré les nombreux avantages de cette solution, il y a encore de quelques inconvénients :

- Le débit limité(faible)
- Les services offerts : upport des VLAN taggés, Routage IPv4 IPv6, NAT, Filtrage du trafic entrant et sortant pour tout type de trafic (ICMP, UDP, TCP…), Contrôle d'accès par adresses MAC ou authentification RADIUS,
- La filtrage de paquet : il a juste détecter les intrusions mais pas arrêter comme SNORT
- Le filtrage web : On ne peut pas filtrer les Url, on peut accéder à tous les sites
- Les failles du logiciel : contre les crackers

La sécurité déployé est trop faible, il n'y a pas de pare-feu dynamique donc il ne fait que le filtrage et n'empêche pas tout le trafic non autorisé ou indésirable. Il n'y a pas aussi de système IDS ou IPS implémenté sur le réseau.

3.3 Le Cisco ASA

3.3.1 définition

L'idée de la conception de l'Adaptative Security Appliance (ASA) est apparue lors de la mise en place par Cisco de la solution Self-Defending Network (le réseau qui se défend tout seul). En effet, en associant un pare-feu très puissant à un système qui offre les services Préventions d'intrusions (IPS), le filtrage web (web filtering) , l'ACL et les services VPN, l'ASA est la solution proposée par Cisco pour garantir un réseau accessible de l'extérieur et sécurisé. Il met en place une défense face aux menaces, et bloque les attaques avant qu'elles ne se propagent dans le reste du réseau. Grâce à une interface graphique et une utilisation simplifiée des fonctionnalités, l'ASA offre aux entreprises qui souhaitent sécuriser leur réseau un outil complet et raisonnablement facile d'utilisation. [15][18]

3.3.2 Description des Serveurs de Sécurité Adaptatifs de la gamme Cisco ASA 5500

C'est le premier produit de matériel de sécurité de la société Cisco. Les Serveurs de Sécurité Adaptatifs Cisco ASA 5500 combinent les meilleurs services de sécurité pour constituer une solution de sécurité spécifique. Conçue comme l'élément principal de la solution Self-Defending Network de Cisco, la gamme Cisco ASA 5500 permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activité du réseau et le trafic applicatif et d'offrir une connectivité VPN flexible. Le résultat est une gamme de puissants serveurs de sécurité réseau multifonctions capables d'assurer en profondeur la protection élargie des réseaux et des grandes entreprises tout en réduisant l'ensemble des frais de déploiement et d'exploitation et en simplifiant les tâches généralement associées à un tel niveau de sécurité. [15][18]

Figure 3.05 : *Les serveurs de sécurité adaptatifs de la gamme Cisco ASA 5500*

3.3.2.1 Principales fonctionnalités

L'ASA offre deux modes pour ses utilisateurs :

- Le mode « routed » est de niveau 3 : quand il y a du trafic, l'ASA est comme un saut sur un routeur (« router hop in the network »)
- Le mode « transparent » est de niveau 2 : Il facilite la configuration du réseau. Le mode transparent permet de cacher le pare-feu (aux intrus éventuels). On utilise aussi le mode transparent pour du trafic qui ne serait pas autorisé par un routeur. Par exemple, il permet d'autoriser du multicast en utilisant une ACL EtherType.

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

L'ASA offre de nombreuses fonctionnalités, majoritairement de sécurité. Nous vous présenterons dans la suite de cette partie celles qui nous paraissent les plus intéressantes, en soulignant que l'ASA offre beaucoup de fonctionnalités qui ne seront pas abordées. [15]

3.3.2.2 NAT (Network address translation)

L'ASA est en partie un routeur. Il est donc logique qu'il offre du NAT : Il permet de transformer les adresses privées en adresses publiques afin de pouvoir avoir accès à des réseaux externes (exemple : réseau internet).

3.3.2.3 ACL (Access Control Lists)

A chaque interface connectée à l'ASA, un numéro de sécurité (entre 0 et 100) est attribué. Le réseau intérieur se voit attribué par défaut le numéro 100 et le réseau extérieur le numéro 0. Sans aucune spécification de la part de l'utilisateur, l'ASA interdit le trafic d'une interface vers une autre interface dont le numéro de sécurité est supérieur. Il autorise d'un autre coté le trafic vers un niveau de sécurité inférieur. Les Access Lists (ACL) ont été mises en place pour pouvoir interdire ou autoriser certains trafics d'une interface vers une autre. Elles sont composées d'ACE (Access Entries). Chaque ACE autorise ou refuse un trafic, en spécifiant l'adresse source et destination ainsi que le protocole. [15]

3.3.2.4 Threat detection

L'ASA fournit une fonctionnalité très importante sous deux formes : la détection de menaces et la détection basique de menaces.
La détection basique de menaces est celle qui est installée par défaut sur l'ASA. C'est celle-ci que l'on abordera rapidement (l'autre détection de menaces est à configurer par l'utilisateur).
La détection basique de menaces détecte les activités qui pourraient être liées à une attaque, comme une attaque DoS (Deny of Service). Elle surveille le taux de paquets abandonnés et les évènements liés à sécurité, à la recherche des éléments suivants : [18]

- Refus par une ACL
- Mauvais format de paquet
- Limite de connexions atteinte
- Attaque Dos détectée
- Paquets ICMP suspects
- Surcharge sur une interface
- Paquets ayant échoué l'inspection d'applications
- Attaque « scanning » détectée

- Détection de session incomplète

Lorsque l'ASA détecte une menace, il envoie un log au système. La détection basique de menaces n'a un impact, sur les performances de l'ASA, que lorsqu'il y a des abandons de paquets ou qu'une menace est détectée. Mais même dans ce cas, l'impact est quasi-insignifiant. .[17]

3.3.2.5 Protection contre l'IP Spoofing

Pour se protéger contre cette menace, l'ASA inclut l'Unicast Reverse Path Forwarding (Unicast RPF), que l'on peut activer sur une interface. L'Unicast RPF donne l'instruction à l'ASA de regarder également l'adresse source (et non pas uniquement l'adresse de destination). En effet, pour chaque trafic que l'on autorise l'ASA à laisser passer, il crée une table de routage qui contient également la route vers l'adresse source. Il lui suffit donc d'observer l'adresse source et la table de routage afin de détecter les menaces. [18]

3.3.2.6 Les filtres HTTP, HTTPS, FTP

Etant donnée la grande taille et la nature dynamique du net, l'utilisation des ACL n'est pas suffisante pour filtrer les sites web ou les serveurs ftp. Il est donc conseiller d'utiliser l'ASA en parallèle avec un serveur utilisant un produit de filtrage internet (ex : Websense Entreprise, Secure Computing SmartFilter).
Les performances du réseau peuvent être réduites considérablement par le serveur externe. Plus il est éloigné du réseau, plus son impact est important.

3.3.3 Le principe des niveaux de sécurité

Les ASA sont des périphériques orientés Sécurité. Cela engendre de nombreuses différences dans la philosophie des commandes les plus basiques telles que la configuration des interfaces. Ainsi, à chaque interface est associé un nom et un niveau de sécurité, qui déterminent les politiques de sécurité associées.
Les niveaux de sécurité vont de 0 à 100. 100 correspond à une confiance totale et un besoin accru de protéger ce réseau ex : réseau interne tandis que 0 correspond à un réseau dont on se méfie et dont la protection ne nous concerne pas ex : Internet. Le nom inside à une interface lui attribue automatiquement un niveau de sécurité de 100. Tout autre nom d'interface, notamment outside, implique un niveau de sécurité de 0. Toutefois, il est possible de modifier le niveau de sécurité manuellement.

Les niveaux de sécurité des interfaces influent sur les points suivants :
Accès réseau : par défaut seules les communications depuis les interfaces de plus haut niveau vers celle de plus bas niveau peuvent avoir lieu. On dit que ces communications sont sortantes. Si les interfaces ont le même niveau, le trafic peut être autorisé entre elles avec la commande same-security-traffic permit inter-interface

- Moteurs d'inspection : les comportements de certains moteurs d'inspection s'adaptent en fonction du niveau :
- Filtrage : les filtrages HTTP et FTP s'appliquent uniquement aux connexions sortantes
- Contrôle NAT : doit être configuré pour les connexions sortantes
- Commande established : cette commande autorise les communications des interfaces de plus bas niveau vers celles de plus haut niveau si la connexion a été établie auparavant par l'interface de plus haut niveau. [15][18]

3.4 Le Cisco ASA 5525-X

C'est un Dispositif de sécurité. Il s'inscrit dans la phase Adaptive Threat Defense de la stratégie Self-Defending Network (SDN) de Cisco, et comprend les modèles ASA 5510, 5520 et 5540. Conçus pour couvrir les besoins des entreprises de toute taille, ces innovations offrent une administration unifiée et des capacités d'évolution pour le fonctionnement de services simultanés. Il est ainsi possible d'utiliser simultanément plusieurs opérations de services de sécurité haute performance sans augmenter la complexité de l'ensemble. Les ASA 5525-x apportent des services de défense adaptative contre les menaces et comprennent des défenses, la sécurité d'application et le confinement ainsi que le contrôle réseau. Elles assurent ainsi une protection unifiée et approfondie des ressources critiques. Les défenses réseau IPS protègent contre les vers, les virus, les pirates, … Elles assurent une micro-inspection du trafic réseau de même que la prévention des intrusions et des attaques par déni de service, la mise en corrélation des événements de sécurité se faisant au niveau de l'appliance. La gamme Cisco ASA 5525-x offre de nombreux avantages en termes de coûts et d'efficacité de déploiement de sécurité. Cela inclut des services d'extensibilité fournis par des modules logiciels et matériels, une plate-forme de standardisation depuis plusieurs emplacements, un fonctionnement simplifié grâce à un service de gestion et de surveillance commun à de nombreux services de sécurité et une plus grande simplicité de localisation des pannes. [15][18]

Type de peripheries	Dispositif de sécurité
Hauteur (Unité de rack)	1U
Poids	6,8 kg
Téchnologie de conectivité	Filaire
Protocole de liaison de données	Gigabit Ethernet
Performances	➢ Débit VPN (3DES-AES) : 300 Mbps ➢ Taux de connexion : 20 000 connexions par seconde ➢ Débit du pare-feu + prévention contre les intrusions : 600 Mbps
Interfaces	✓ 14 x 1000Base-T - RJ-45 ✓ 1 x 1000Base-T (gestion) - RJ-45 ✓ 1 x management - RJ-45 ✓ 2 x USB 2.0 - Type A
RAM	8 Go
Tension requise	CA 120-230 V (50-60 Hz)
Puissance fournie	400 Watt
Nombre de ports	14 ports

Tableau 3.01: *Description ASA 5525-x*

3.5 Modélisation de l'architecture réseau sécurisé

D'après nos études, On a conçu l'architecture réseau au Direction de Système d'Information (DSI) au sein du Ministère des finances et du budget avec la mise en place des quatre (4) Cisco ASA 5525-x pour avoir une meilleure sécurité.

En résumé, voici une architecture normalisée qu'on a prise en compte dans le cadre de ce mémoire dans la figure 3.06

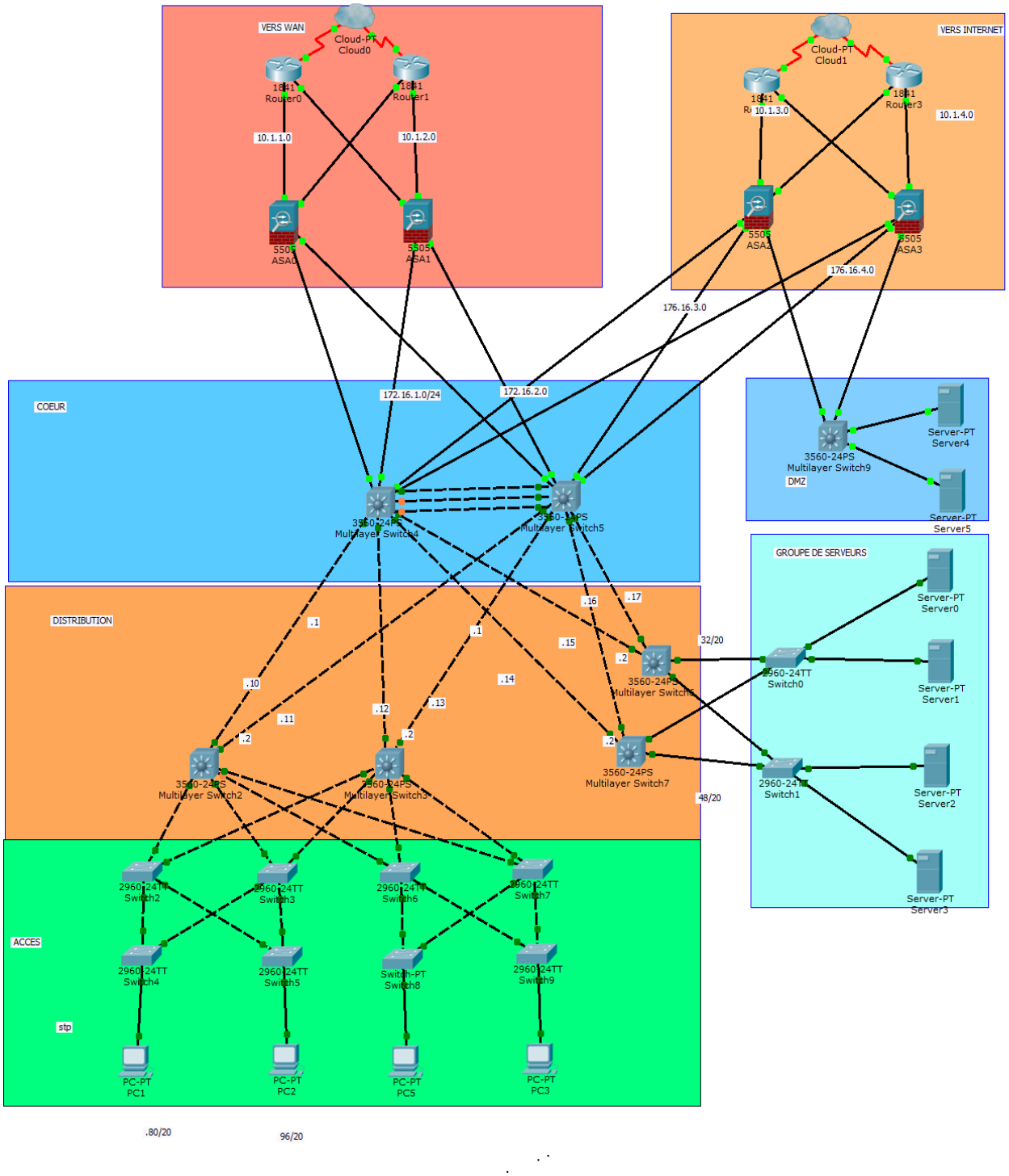


Figure 3.06 : *Architecture globale réseau DSI*

On met deux par deux le Cisco ASA pour éviter la coupure de communication ou panne réseau.

Donc on met deux Cisco ASA à la liaison entrante c'est-à-dire à la liaison vers la connexion internet (EDGE Internet) et deux ASA de la liaison du MFB vers l'annexe, autre entreprise et/ou vers le MFB à la province ; Pour bien sécuriser contre les attaques, le partage des données et de filtrer l'utilisateur accéder à l'internet.

3.6 Mise en place du module de sécurité

On met dans les 2 Cisco ASA vers le réseau WAN ou vers l'EDGE WAN le module IPS et on met le module de filtrage Web et le module IPS dans le Cisco ASA vers l'accès internet.

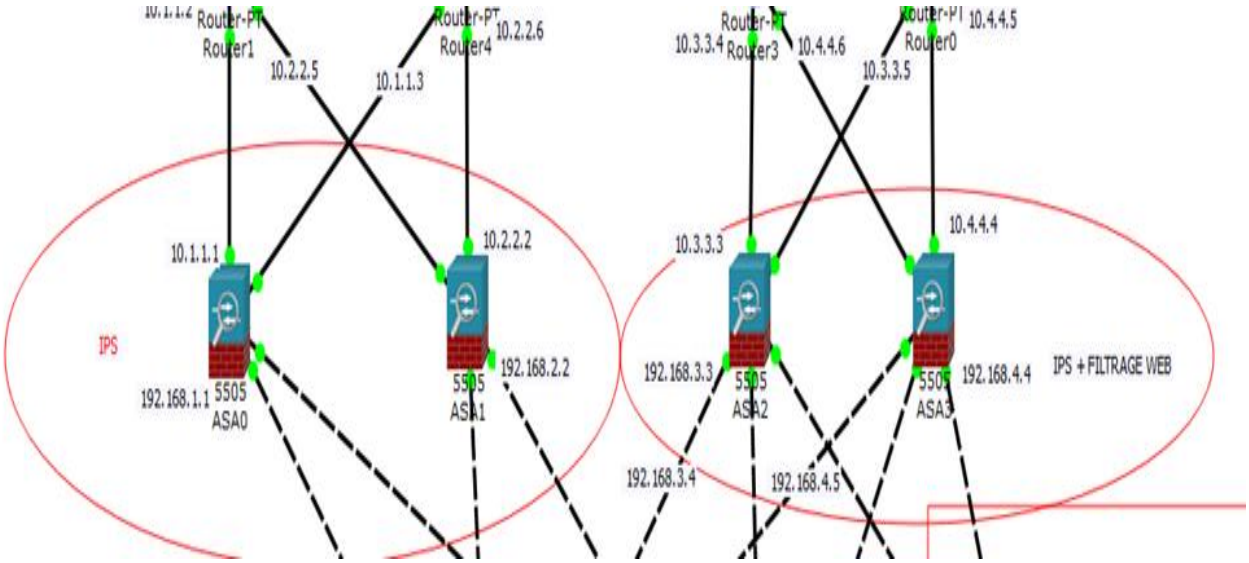


Figure 3.07 : *Mise en place du module de sécurité*

3.6.1 Le filtrage web

Le filtrage Web par URL désigne une solution ou une technologie d'analyse et de filtrage, dont l'objectif est de contrôler les accès aux sites et applications Web, pour l'ensemble des utilisateurs du réseau.

Généralement, l'administrateur paramètre la solution de filtrage, pour bloquer les accès aux sites estimés comme inappropriés dans le cadre professionnel ou jugés dangereux pour la sécurité informatique de l'entreprise. Ce dispositif permet également de protéger la responsabilité juridique des employeurs, en bloquant l'accès aux sites de téléchargements illégaux de documents , de

musique, films ou logiciels, de vidéos en streaming, ou aux espaces d'expressions en ligne comme réseaux sociaux, forums ou blogs, pour limiter les propos controversés. Enfin la mise en place d'une solution de filtrage permet d'optimiser les ressources de bande passante. Chaque type de structure a des besoins Internet spécifiques, liés à son activité, à son organisation et à sa politique interne. L'utilisation d'Internet doit répondre aux problématiques de sécurité, de préservation de la bande passante et de productivité, tout en restant adaptée à l'utilisation de chaque service voire de chaque employé.

Ce système de filtrage doit configurer en pratique à l'aide des logiciels comme le Websense.

3.6.2 La prévention d'intrusion

La prévention d'intrusion est un ensemble de technologies de sécurité ayant pour but d'anticiper et de stopper les attaques. La prévention d'intrusion est appliquée par quelques IDS récents et diffère des techniques de détection d'intrusion décrites précédemment : au lieu d'analyser les logs du trafic, c'est-à-dire découvrir les attaques après qu'elles se soient déroulées, la prévention d'intrusion essaie de prévenir ces attaques.
Là où les systèmes de détection d'intrusion se contentent de donner l'alerte, les systèmes de prévention d'intrusion bloquent le trafic jugé dangereux.

3.6.2.1 Les systèmes de prévention d'intrusion (IPS)

Le principe de fonctionnement d'un IPS est symétrique à celui d'un IDS (IPS hôte et IPS réseau), ajoutant à cela l'analyse des contextes de connexion, l'automatisation d'analyse des logs et la coupure des connexions suspectes. Contrairement aux IDS classiques, aucune signature n'est utilisée pour détecter les attaques. Avant toute action, une décision en temps réel est exécutée (i.e., l'activité est comparée à un ensemble de règles). Si l'action est conforme à l'ensemble de règles, la permission de l'exécuter sera accordée et l'action sera exécutée. Si l'action est illégale (c'est-à-dire si le programme demande des données ou veut les changer alors que cette action ne lui est pas permise), une alarme est donnée. Dans la plupart des cas, les autres détecteurs du réseau (ou une console centrale) en seront aussi informés dans le but d'empêcher les autres ordinateurs d'ouvrir ou d'exécuter des fichiers spécifiques. Le diagramme ci-après illustre le fonctionnement d'un IPS. [15][17]

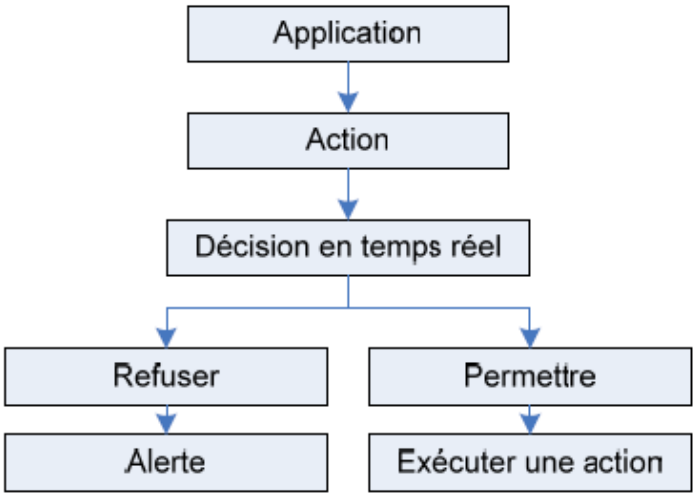


Figure 3.08 : *Fonctionnement d'un IPS*

Les IPS fournissent les fonctionnalités suivantes:

- La surveillance du comportement d'application se rapproche des IDS basés sur une application, c'est-à-dire que le comportement de l'application est analysé et noté (quelles données sont normalement demandées, avec quels programmes elle interagit, quelles ressources sont requises, etc.).
- La création de règles pour l'application : dérivé de la surveillance du comportement d'application, cet ensemble de règles donne des informations sur ce que peut faire ou non une application.
- La fonctionnalité d'alerte suite aux violations permet d'envoyer une alerte en cas de déviation (c'est-à-dire lorsqu'une attaque est détectée). L'alerte peut aller d'une simple entrée dans un journal à un blocage de ressources, par exemple.
- La corrélation avec d'autres événements implique un partage d'informations entre des senseurs coopératifs, afin de garantir une meilleure protection contre les attaques.
- L'interception d'appels au système : avant qu'un appel au système (rootkit) soit accepté, il doit être complètement vérifié (par exemple, quel programme a demandé l'appel au système, sous quelles autorisations d'utilisateur tourne le processus root..., à quoi l'appel système essaie-t-il d'accéder, etc.). Cette fonctionnalité permet la surveillance des essais de modification d'importants fichiers du système ou de la configuration.

- D’autres fonctionnalités sont possibles, comme la compréhension des réseaux IP (architecture, protocoles, etc.), la maîtrise des sondes réseau/analyse des logs, la défense des fonctions vitales du réseau.

La prévention d'intrusion est une technique relativement nouvelle par comparaison aux autres techniques. Cette approche fait interagir des technologies hétérogènes : pare-feu, VPN, IDS, anti-virus, etc. [15][17]

3.6.2.2 L’IPS ASA

Les ASA peuvent utiliser l’AIP SSM. C’est un module de prévention d’intrusion qui surveille et effectue des analyses en temps réel du trafic sur le réseau en cherchant les anomalies et les mauvais usages basés sur une bibliothèque de signatures étendue.

Lorsque le système repère une activité non-autorisée, il peut mettre fin à la connexion en cours, bloquer l’hôte attaquant, enregistrer l’incident, et envoyer une alerte au gérant du réseau. Les autres connexions légitimes continuent à fonctionner indépendamment, sans interruption.

- AIP SSM

L’AIP SSM utilise un logiciel d’IPS (Intrusion Prevention Services) avancé qui fournit un service de protection pour stopper le trafic malicieux, notamment les vers et les virus réseau, avant qu’ils n’affectent le reste du réseau.

- CSC SSM

Il fournit une protection contre les virus, les spywares, les spams et tout autre trafic non-désiré en scannant les paquets FTP, HTTP et SMTP que l’utilisateur lui demande de scanner.

- Le module ASA IPS

Le module ASA IPS exécute une application séparée de l'ASA. Le module ASA IPS pourrait inclure une interface de gestion externe de sorte que vous pouvez connecter au module ASA IPS directement; si elle ne dispose pas d'une interface de gestion, vous pouvez vous connecter au module ASA IPS via l'interface ASA. L'ASA IPS SSP sur ASA 5525-X comprend des interfaces de données; ces interfaces fournissent densité de ports supplémentaires pour l'ASA. Cependant, l'ensemble par-mis de l'ASA ne soit pas augmentée.

Le trafic passe par les pare-feu vérifie avant d'être transmis au module ASA IPS. Lorsque vous identifiez le trafic pour IPS inspection sur l'ASA, les flux de trafic à travers l'ASA et le module ASA IPS comme suit. Note: ". Mode en ligne" Cet exemple est pour Voir la section «Modes de

fonctionnement» pour des informations sur "mode promiscuité", où l'ASA n'envoie une copie du trafic vers le module ASA IPS. [15][17]
Ce système doit configurer par un logiciel ASDM en pratique, mais on ne peut simuler en Packet tracer.

3.7 La liste de contrôle d'accès

3.7.1 Définition

Les ACLs offrent la possibilité de positionner des droits d'accès supplémentaires. Le propriétaire d'un fichier peut grâce aux ACLs accorder des privilèges à un ou plusieurs utilisateurs et/ou groupes qui se substitueront aux droits d'accès de base. Avec les ACLs c'est possible de donner des droits à un utilisateur qui ne fait pas partie du groupe en ne modifiant pas les droits pour les autres. De même on peut autoriser des droits d'accès pour un groupe d'utilisateurs qui n'est pas le groupe du fichier. Il n'y a pas des limites concernant le nombre d'utilisateurs ou groupes à ajouter avec les ACLs. [15][17]

3.7.2 Description d'ACL

Une ACL sur un pare-feu ou un routeur filtrant, est une liste d'adresses ou de ports autorisés ou interdits par le dispositif de filtrage.

Les Access Control List sont divisés en trois grandes catégories, l'ACL standard, l'ACL étendue et la nommée-étendue. [15][17]

- L'ACL standard ne peut contrôler que deux ensembles : l'adresse IP source et une partie de l'adresse IP source, au moyen de masque générique.
- L'ACL étendue peut contrôler l'adresse IP de destination, la partie de l'adresse de destination (masque générique), le type de protocole (TCP, UDP, ICMP, IGRP, IGMP, etc.), le port source et de destination, les flux TCP, IP TOS (*Type of service*) ainsi que les priorités IP.
- L'ACL nommée-étendue est une ACL étendue à laquelle on a affecté un nom.

3.7.3 Fonctionnement d'ACL

Il est possible de résumer le fonctionnement des ACL de la façon suivante :

- Le pâquet est vérifié par rapport au 1er critère défini

- S'il vérifie le critère, l'action définie est appliquée
- Sinon le paquet est comparé successivement par rapport aux ACL suivants
- S'il ne satisfait aucun critère, l'action *deny* est appliquée

Les critères sont définit sur les informations contenues dans les en-têtes IP, TCP ou UDP

Des masques ont été défini pour pouvoir identifier une ou plusieurs adresses IP en une seule définition

- Ce masque défini la portion de l'adresse IP qui doit être examinée
- 0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés
- deny 10.1.3.0 avec 0.0.0.255 : refus de toutes les IP commencant par 10.1.3

3.7.4 Les extended ACL

Les extended ACL permettent filtrer des paquets en fonction de l'adresse de destination IP

- Du type de protocole (TCP, UDP, ICMP, IGRP, IGMP, ...)
- Port source
- Port destination
- …

3.8 Le DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessible de l'extérieur (comme c'est le cas par exemple pour un serveur web, un serveur de messagerie, un serveur FTP public, ...) il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité interne. On parle ainsi de zone démilitarisé (souvent notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public.

Ceci se crée en isolant les équipements du réseau (en restant connecté) et y assigné des commandes ACL pour régler ses communications avec le reste du réseau. [21]

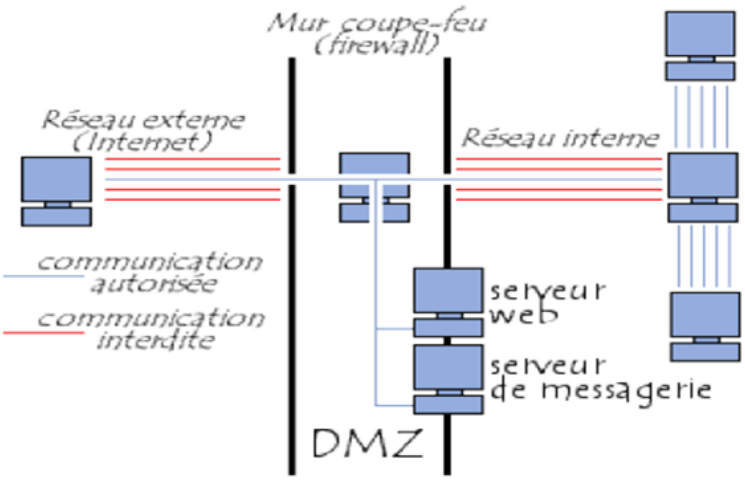


Figure 3.09 : *Zone démilitarisée*

Dans le cas de notre réseau campus, la zone démilitarisée sera situé sur un parc de serveurs qui sera protégée grâce à des pare-feu et des règles de filtrages tout prêt des serveurs internes.

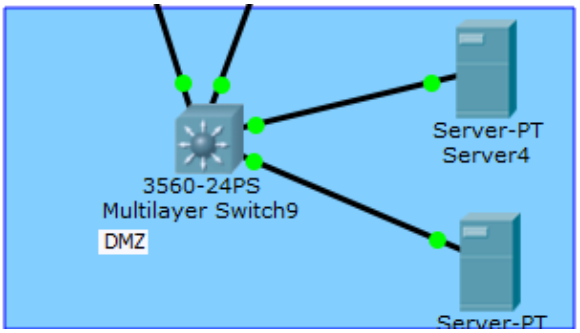


Figure 3.10 : *Piles de serveurs*

3.9 Serveurs internes

Ce sont ceux qui ne doivent pas être accessible qu'à l'intérieur du réseau. Ils sont la partie qui doit être le mieux protégé du réseau car ils contiennent les bases données de l'entreprise par exemple.

Ils devraient être sécurisés à tous les niveaux du modèle OSI, dans notre cas, on s'en occupe des règles de filtrage, attribuer l'adresse IP et le DHCP.

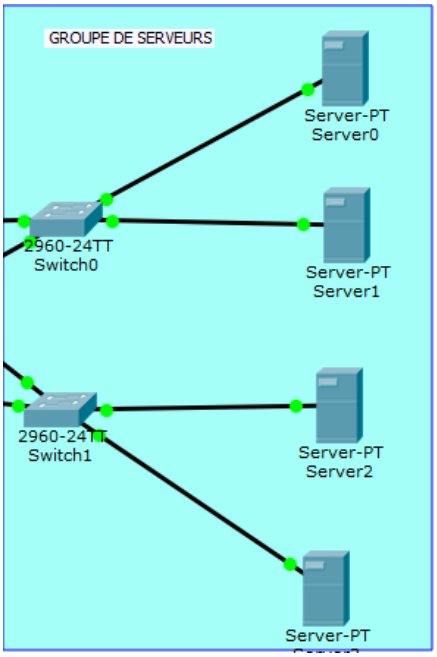


Figure 3.11 : *Groupe des serveurs*

3.10 Conclusion

On a pu voir donc dans ce chapitre que les serveurs de Sécurité Adaptatif Cisco ont la meilleure combinaison de services de Sécurité. Ils permettent de bénéficier de fonctionnalités de contrôle de listes d'accès , la détection de menaces et la détection basique de menaces, Protection contre l'IP Spoofing ou de regarder également l'adresse source (et non pas uniquement l'adresse de destination), de transformer les adresses privées en adresses publiques , de blocage et de filtrage web, le système de préventions d'intrusions et la liste de contrôle d'accès.

Dans le chapitre suivant, on va simuler sur le logiciel packet tracer : L'etherchannel, la haute disponibilité du reseau et la liste de contrôle d'accès avec le matériel Cisco ASA 5505.

CHAPITRE 4
SIMULATION DE LA LISTE DE CONTROLE D'ACCES AVEC CISCO ASA 5505, L'ETHERCHANNEL ET LE STP

4.1 Introduction

Dans ce chapitre, nous allons simuler ce que l'on a énoncé dans les chapitres précédents, afin de voir comment fonctionne le Cisco ASA.

4.2 Présentation de Packet Tracer

Packet Tracer est un environnement basé sur la simulation pour la description et la configuration de réseaux correspondant au CCNA Cisco. Il offre les possibilités suivantes [12] :

Item	Description
Espace de travail logique (Logical Workspace)	• Création de topologies réseaux • Equipements: générique, réel, modulaire (Routers, switches, hosts, hubs, bridges, wireless access points, et clouds (nuages)) • Connexion des équipements à travers différents medias réseau
Espace de travail physique (Physical Workspace)	• Hiérarchie des périphériques, répartiteur, immeuble, ville et inter-villes, • chargement des graphismes des utilisateurs
Mode temps-réel (Realtime Mode)	• Realtime protocol updates • Medium-fidelity Cisco IOS CLI configuration of switches and routers
Simulation Mode	• Animation de Packets • Capture de packets (packet sniffer) • Modèle ISO, PDU détaillé, and visualisation des tables (MAC, NAT, ARP) • Scenarios multi-paquets par l'utilisateur

Tableau 4.01: *Résumé des fonctions principales du logiciel*

4.2.1 Présentation de l'écran principal

Il dispose d'une barre de menu classique D'une barre d'outils principale comportant les fonctionnalités de base de gestion de fichier, d'impression …

D'une barre d'outils à droite comportant les outils minimaux nécessaires

Ainsi que trois boites à outils :

- choix du type de matériel (ordinateur, routeurs, etc...)
- choix du matériel en fonction du type
- résultats de l'échange de données. [13]

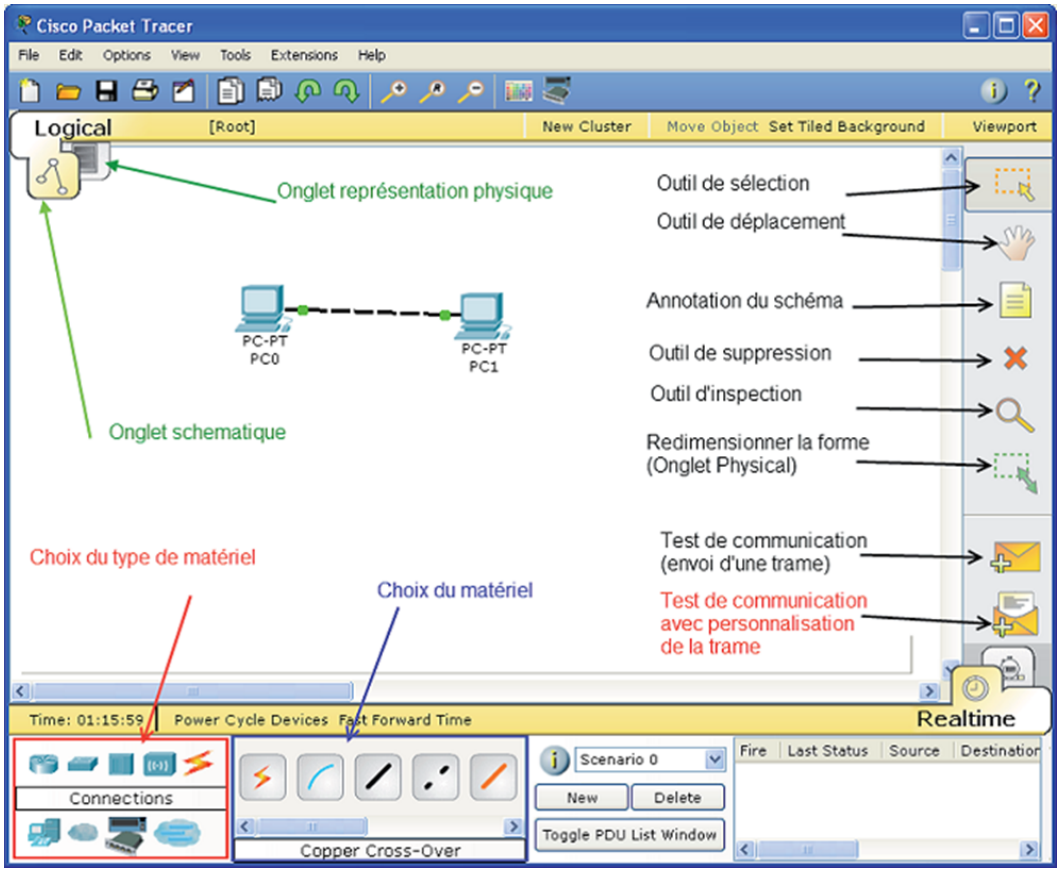


Figure 4.01 : *Ecran principal de Packet Tracer*

Il dispose d'une barre de menu classique ;

D'une barre d'outils principale comportant les fonctionnalités de base de gestion de fichier, d'impression, etc....

D'une barre d'outils à droite comportant les outils minimaux nécessaires.

Ainsi que trois boites à outils : choix du type de matériel, choix du matériel en fonction du type, résultats de l'échange de données.

4.2.2 Les principaux protocoles

Ce tableau présente les différents protocoles disponibles dans Packet Tracer selon les couches du modèle OSI.

Couches	Protocoles
Physique	Pas d'objet
Liaison	Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP STP, VTP, DTP, CDP, 802.1q, LACP , … L2 QoS, SLARP, Auto Secure Wifi: simple WEP, WPA
Réseau	IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, GRE, Routage: RIPv1/v2/ng, Multi-Area OSPF, EIGRP, Static Routing Sécurité: Context Based Access Lists, Zone-based policy firewall et intrusion Protection System (sur certain routeur) Multilayer Switching, L3 QoS, NAT
Transport	TCP and UDP, TCP Nagle Algorithm & IP Fragmentation
Session	Pas d'objet
Présentation	Pas d'objet
Application	HTTP, HTTPS, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, Radius, Syslog, …

Tableau 4.02: *Récapitulatifs des principaux protocoles*

4.2.3 Spécification des équipements disponibles

Packet Tracer propose les principaux équipements réseaux composant nos réseaux actuels. Chaque équipement possède une vue physique comprenant des modules à ajouter, une vue configuration pour configurer les principales options via une interface graphique et une vue permettant la configuration via CLI (Command Line Interface).

- Routeur,
- Commutateur Terminaux (ordinateur, portable, serveur, imprimante et téléphone IP),

- Point d'accès Modem,
- Concentrateur.

Sachant que chaque équipement se voit attribuer un certain nombre de modules, permettant d'ajouter soit des ports supplémentaires, soit des nouveaux types de port. Les équipements propriétaires Cisco ont la possibilité de se voir attribuer les nouveaux IOS disponibles sur le site Cisco.

4.2.3.1 Configuration

L'onglet Config permet de configurer l'équipement sélectionné.
Les boutons situés à gauche de la fenêtre déterminent le groupe de paramètres à configurer.
Par exemple: si une carte réseau FastEthernet équipe l'appareil, il sera possible de définir les paramètres de la carte en sélectionnant celle-ci avec le bouton FastEthernet et en renseignant les champs et cases à cocher de la partie droite de la fenêtre.

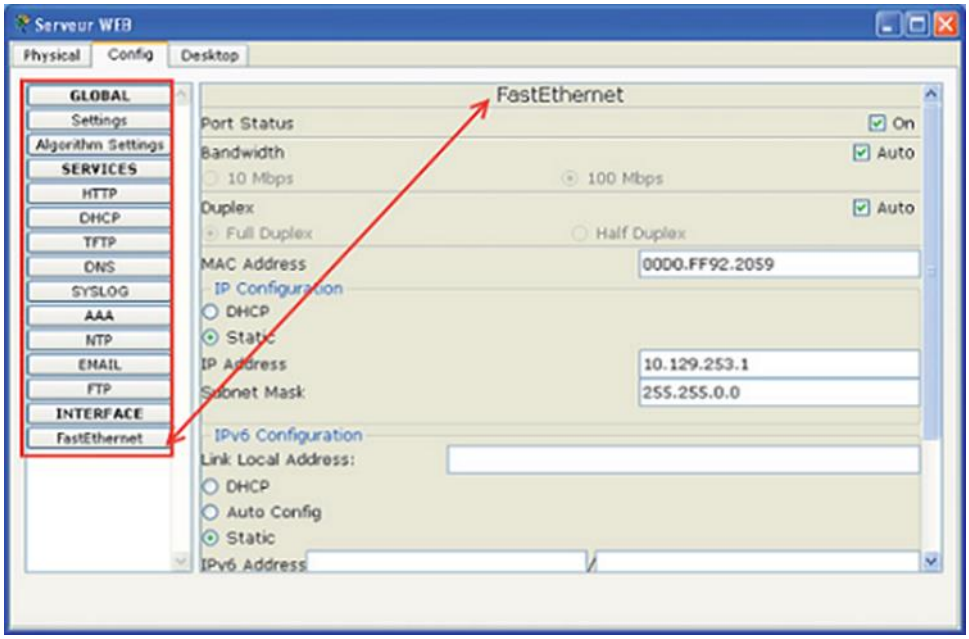


Figure 4.02 : *Paramétrage dans l'onglet configuration*

4.2.3.2 Configurations du PC

Les équipements terminaux sont les stations (PC), l'imprimante et le serveur. Pour les configurer, on double clique et on choisit l'onglet Desktop pour les stations et Config pour les autres.

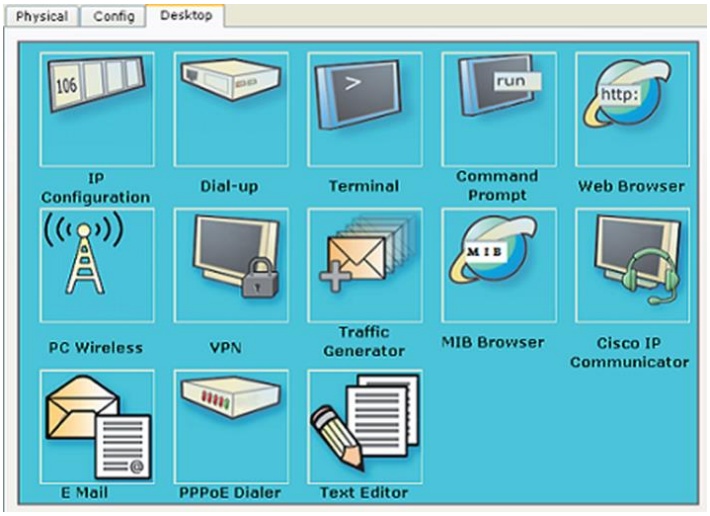


Figure 4.03 : *Onglet desktop*

- IP configuration : permet de configurer les paramètres réseau de la machine.
- Dial-Up : permet de configurer un modem s'il est présent dans l'équipement.
- Terminal : permet d'accéder à une fenêtre de programmation (HyperTerminal).
- Command prompt : est la fenêtre DOS classique permettant de lancer des commandes en ligne de commande (PING, IPCONFIG, ARP, etc...).
- WEB Browser : il s'agit d'un navigateur Internet.
- PC Wireless : permet de configurer une carte WIFI si elle est présente dans l'équipement.
- VPN : permet de configurer un canal VPN sécurisé au sein du réseau.
- Traffic generator : permet pour la simulation et l'équipement considéré de paramétrer des trames de communications particulières (exemple : requête FTP vers une machine spécifiée).
- MIB Browser : permet par l'analyse des fichiers MIB d'analyser les performances du réseau.
- CISCO IP Communicator : Permet de simuler l'application logicielle de téléphonie développée par CISCO.
- E-Mail : client de messagerie.
- PPPoE Dialer : pour une liaison Point à Point (Point to Point Protocol). [18] [20]

4.3 Simulation

Packet Tracer permet de simuler le fonctionnement d'un réseau par l'échange de trames Ethernet et la visualisation de celles-ci.

Il existe deux modes de simulation :

- la simulation en temps réel (REALTIME): elle visionne immédiatement toutes les séquences qui se produisent en temps réel,
- la simulation permettant de visualiser les séquences au ralenti entre deux ou plusieurs équipements comme la figure 4.06 nous montre.

4.3.1 Simulation en temps réel

- Réalisation d'un PING

Un ping fait appel au protocole ICMP avec le message numéro 8. Packet Tracer permet de faire un ping rapidement avec l'outil « Add Single PDU » représenté sous forme de petite enveloppe.

- Sélectionner l'outil,
- Cliquer sur l'ordinateur émetteur du PING,
- Cliquer ensuite sur l'ordinateur Destinataire du PING.

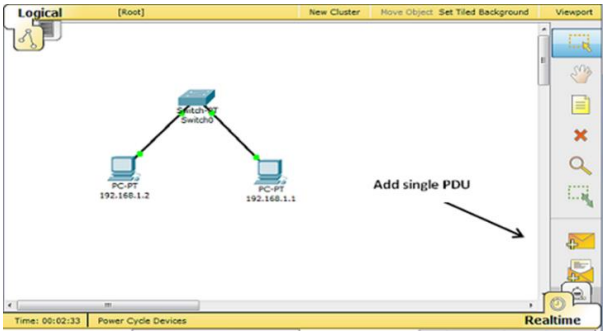


Figure 4.04 : *L'outil de réalisation d'un ping rapide*

- La fenêtre d'état informera de la réussite (Successfull) ou de l'échec (Failed) de transaction

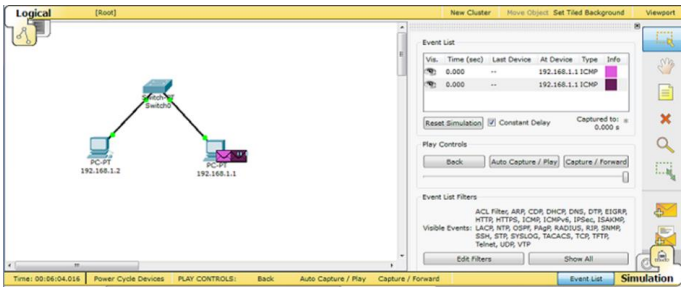


Figure 4.05 : *La fenêtre d'état de la transaction*

- Simulation en ligne de commande

Comme sur un vrai ordinateur, il est possible par ligne de commande de saisir des commande réseau (IPCONFIG, PING, ARP...).

- Ouvrir la fenêtre de configuration de l'ordinateur en cliquant sur sa représentation,
- Choisir l'onglet Desktop,
- Sélectionner l'outil Command Prompt,
- Saisir la commande souhaitée,
- Valider par la touche ENTREE.

La figure 4.06 suivante montre un test de connectivité avec la commande « ping ».

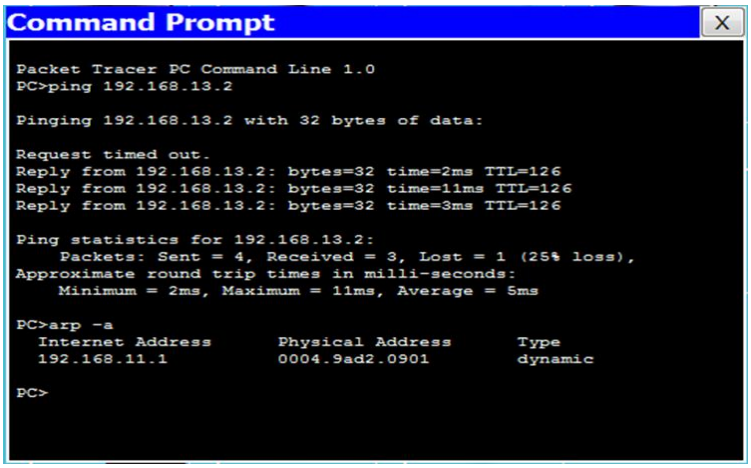


Figure 4.06 : *Test de connectivité en ligne de commande*

Les commandes disponibles dans la fenêtre Command prompt :

- arp : affiche la table arp.
- delete : permet de supprimer les fichiers se trouvant dans c : directory.
- dir : affiche les listes des fichiers dans c : directory.
- ipconfig : affiche la configuration logique et physique du matériel.
- netstat : affiche les protocoles statiques et celles du réseau TCP/IP.
- nslookup : vérification du DNS.
- ping : envoi de requêtes.
- snmpget : permet de visualiser la configuration snmp.
- telnet : permet de voir les clients telnet.
- tracert : permet de tracer la route de destination.
- help : affiche les listes des commandes disponibles,

- etc…

4.3.2 Simulation d'un accès WEB

Si le réseau intègre un serveur HTTP, il est possible de simuler un accès WEB.
Accéder à la configuration du poste en cliquant sur son image ;

- Aller dans l'onglet Desktop,
- Choisir Web Browser,
- Saisir l'adresse ou le nom du serveur WEB.

4.3.3 Simulation d'une messagerie

Le principe est le même que celui décrit ci-dessus. Il suffit de disposer d'un serveur POP et SMTP.

4.4 Simulation d'architecture réseau DSI au MFB

4.4.1 Configurations du Cisco ASA

Il est fortement recommandé de sauvegarder fréquemment la configuration ASA pour assurer qu'aucun travail ne soit perdu en cas de panne de courant ou un redémarrage accident.

Enregistrement de la configuration peut être facilement fait en utilisant la commande d'écriture en mémoire:
ASA (config) **# write memory**
Effacement configuration existante :

Cette première étape est facultative car elle efface la configuration. Si le pare-feu a été préalablement configuré ou utilisé, il est une bonne idée de commencer avec les réglages d'usine. Si nous ne sommes pas certains, nous préférons l'essuyer et recommencer à zéro. Une fois que la configuration est supprimée, nous devons forcer un redémarrage, ll faut commencer ce processus nouveau:

ciscoasa (config) # **write erase**
Effacer la configuration dans la mémoire flash? [confirmer]
[D'ACCORD]
ciscoasa (config) # **reload**
config du système a été modifié. Sauvegarder? [Y] es / [N] o: N

Proceed with reload? [confirmer]

ciscoasa (config) #

Ensuite, nous avons besoin de configurer le mot de passe Activer, requis pour l'accès en mode d'exécution privilégié.

Ciscoasa> **enable**

Mot de passe: cisco

ciscoasa # **configure terminal**

ciscoasa (config) #

Nous devons utiliser des interfaces VLAN, qui sont configurés avec leurs adresses IP appropriées et ensuite (étape suivante) caractérisé interfaces que l'intérieur (privé) ou à l'extérieur (publics):

ASA (config) # **Interface vlan 1**

ASA (config) # **Description Private-Interface**

ASA (config-if) # **ip add 172.16.1.1 255.255.255.0**

ASA (config-if) # **no shutdown**

ASA (config) # **Interface vlan 2**

ASA (config) # **Description Public-Interface**

ASA (config-if) # **ip add 10.1.1.1 255.255.255.0**

ASA (config-if) # **no shutdown**

ASA (config) # **interface Ethernet 0/0**

ASA (config-if) # **switchport access vlan 2**

ASA (config-if) # **no shutdown**

Sinon, l'interface publique (VLAN2) peut être configuré pour obtenir automatiquement son adresse IP via DHCP avec la commande suivante:

ASA (config) # **Interface vlan 2**

ASA (config) # **Description Public-Interface**

ASA (config-if) **# ip add dhcp setroute**

ASA (config-if) # **no shutdown**

Après avoir configuré VLAN1 et VLAN2 avec les adresses IP appropriées, nous avons configuré Ethernet 0/0 comme un lien d'accès pour VLAN2 afin que nous puissions l'utiliser comme une interface publique physique. Sur Ethernet totale 16 interfaces du ASA, au moins un doit être réglé avec l'accès vlan switchport 2 pour notre routeur pour se connecter à ports Ethernet 0/1 à 0/16 doivent également être configurés avec la commande **no shutdown** pour les rendre opérationnels. Tous ces ports sont, par défaut, les liens d'accès pour VLAN1. L'invention concerne les commandes de configuration pour les deux premières interfaces Ethernet que la configuration est de ASA (config) **# interface Ethernet 0/1**

ASA (config-if) # **no shutdown**

ASA (config-if) # **interface Ethernet 0/2**

ASA (config-if) # **no shutdown**

Nous devons désigner l'intérieur interfaces (privé) et à l'extérieur (public). Cette étape est essentielle et aidera l'ASA comprendre quelle interface est connecté au réseau de confiance (privé) et public:

ASA (config) # **Interface vlan 1**

ASA (config-if) # **nameif inside**

Niveau de sécurité pour «l'intérieur» fixé à 100 par défaut.

ASA (config) **# Interface vlan 2**

ASA (config-if) # **nameif outside**

Niveau de sécurité pour "l'extérieur" mis à 0 par défaut

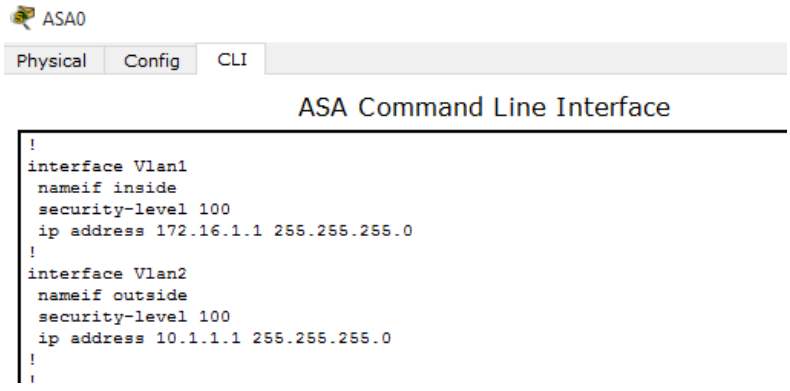


Figure 4.07 : *Configuration interface vlan*

Les interfaces DMZ sont généralement configurés avec un niveau de 50 sécurité.

La commande de configuration de route par défaut est nécessaire pour l'ASA pour acheminer les paquets en dehors du réseau via le saut suivant, généralement un routeur. Dans le cas où l'interface publique (VLAN2) est configuré en utilisant la commande **ip adress dhcp setroute**, la configuration de la passerelle par défaut n'est pas nécessaire.

ASA (config) # **route inside 0.0.0.0 0.0.0.0 172.16.1.3**

Route par défaut du Cisco ASA

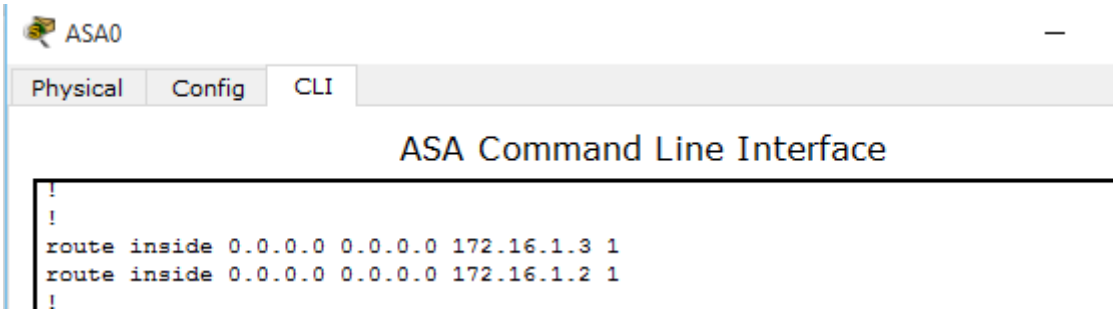


Figure 4.08 : *Configuration route*

Nous voyons le guide de configuration d'introduction pour les appareils ASA. Nous avons couvert certaines commandes nécessaires pour obtenir tous les utilisateurs réseau de service, tout en expliquant en détail toutes les commandes utilisées lors du processus de configuration.

4.4.2 ASA Configuration ACL

Parce que la majorité des configurations ASA ACL vont être en utilisant un type d'ACL étendue, cette section se concentre sur la configuration de ce type et montre un exemple de la façon dont ils peuvent être utilisés pour contrôler une partie du trafic de base. On présente les commandes requises pour configurer une ACL étendue :

Entrez en mode d'exécution privilégié.

asa> **enable**

Entrez en mode de configuration globale.

asa # **configure terminal**

Créer et configurer une entrée étendue ACL (ACE) - Répéter au besoin.

asa(config)#**access-list** acl-name **extended {deny | permit}** {protocol-name | protocol-number} {**any | host** source-ip-address | source-ip-address source-netmask} {**any | host** destination-ip-address | destination-ip-address destination-netmask} [operator port [port]]

Appliquer l'ACL à l'interface appropriée.Le nom de l'interface est adaptée à la valeur de nameif configuré.

asa(config)#**access-group** acl-name {**in | out} interface** interface-name

4.4.2.1 ASA ACL Exemple de configuration

Pour clarifier la configuration d'une ACL étendue, cette section va sur un exemple de la façon dont ils peuvent être utilisés pour contrôler le trafic, ainsi que leur interaction avec les règles ACL implicites.

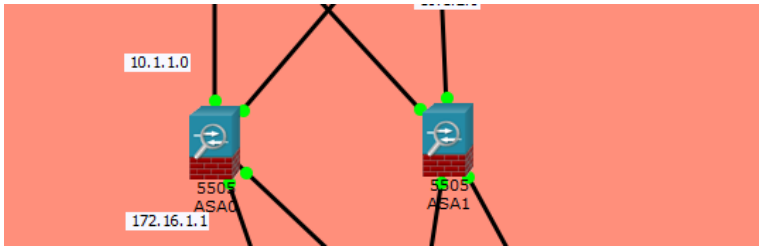


Figure 4.09 : *ASA ACL Topologie*

Une chose importante à garder à l'esprit est la configuration actuelle des niveaux de sécurité. Le trafic passant d'un niveau à un niveau inférieur de sécurité plus élevé de sécurité est autorisé par défaut. Les étapes indiquées suivants comprennent toutes les étapes qui sont nécessaires pour mettre cette ASA dans cette configuration.

4.4.2.2 Exemple d'extrait de commande

Entrez en mode d'exécution privilégié.

asa> **enable**

Entrez en mode de configuration globale.

asa # **configure terminal**

- listes d'accès autorisés

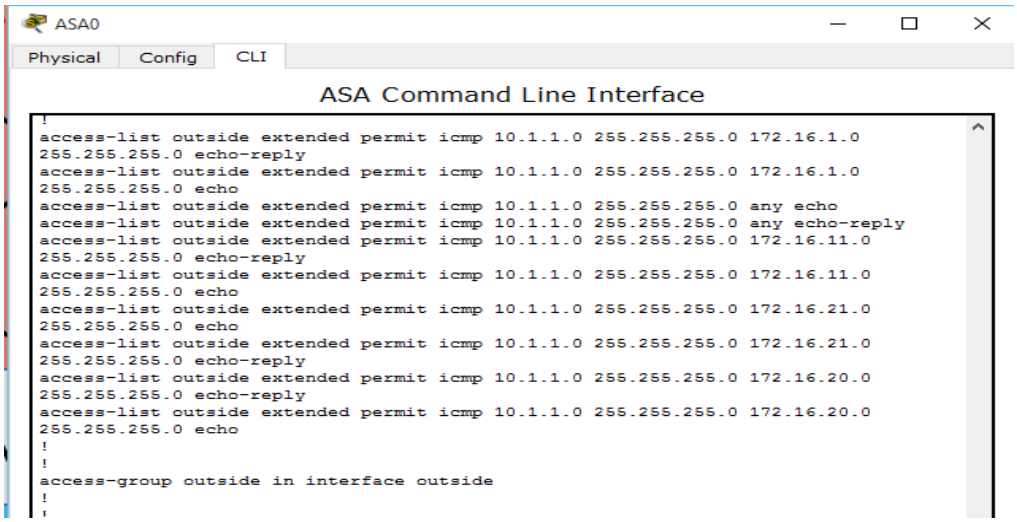


Figure 4.10 : *Configuration d'ACL permit*

- Configurations du Liste d'accès refusés

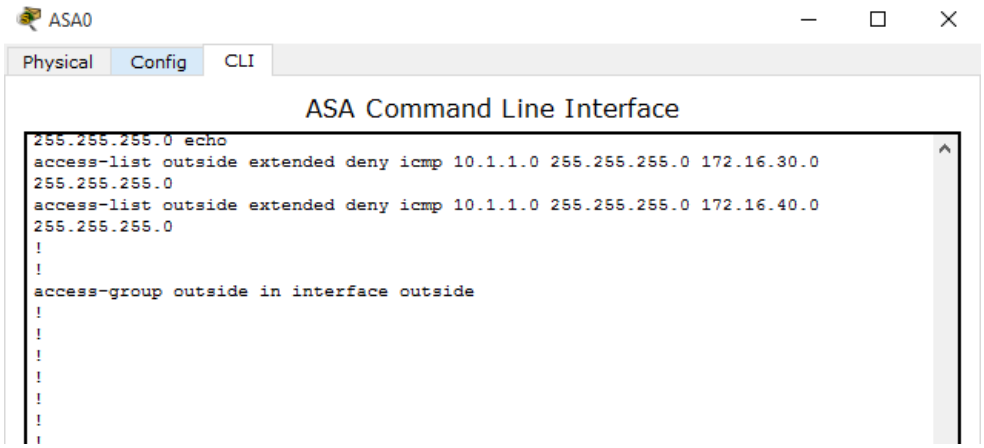


Figure 4.11 : *ACL refusé*

Ici on a refusé le réseau 172.16.30.0 d'accéder au réseau 10.1.1.0 ou à l'extérieur du Cisco ASA. L'interface VLAN 1 ou l'extérieur du Cisco ASA tend vers le réseau WAN du MFB.

Donc le reseau 172.16.10.0 seulement peut accéder à ces réseaux 10.1.1.0 ou 10.2.2.0

Notez qu'une entrée d'ACL était nécessaire pour le trafic allant de haut en bas ou (gauche à droite). En effet, l'interface de haut a été configuré avec un niveau de sécurité qui est inférieur à celui de

l'interface bas. Le trafic doit être configuré (ce comportement peut être modifié) par rapport aux niveaux de sécurité plus élevée à des niveaux de sécurité inférieurs.

4.4.3 Tests de connectivités et analyses des paquets envoyés dans ce réseau

4.4.3.1 Test de fonctionnement

Une fois la configuration terminée, on pourra vérifier à l'aide de diverses commandes si on a pu interconnecter en voyant le paquet transmis et le paquet bloqués.

4.4.3.2 Vérification du fonctionnement du réseau

Pour la vérification du fonctionnement du réseau, on peut demander à un périphérique d'envoyer un ping (il s'agit d'une requête ICMP de type echo-request appelé communément « ping ») à un autre périphérique, il suffit d'utiliser l'icône en forme d'enveloppe (Add Simple PDU (P)) présenté à la figure suivante. La zone en bas à droite de l'écran vous renseigne sur la réussite (successful) ou l'échec (failed) de la requête.

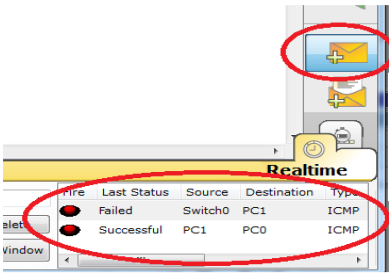


Figure 4.12 : *Icône « Add Simple PDU » et résultat de la requête ICMP.*

- Le ping peut échouer alors que la communication fonctionne. Cela peut être le cas lorsque le réseau et le destinataire fonctionnent correctement mais que la configuration de celui-ci lui interdit de répondre aux requêtes de type ping.
- Le ping peut réussir, indiquant qu'une machine (un serveur Web par exemple) est joignable, mais le service sur cette machine peut être indisponible rendant l'accès impossible aux pages Web du serveur etc…

4.4.3.3 Interprétation des résultats avec la commande ping

Un test avec ping permet principalement de connaître deux choses :

- Les périphériques concernés peuvent-ils communiquer ensemble
- Le temps de parcours des paquets, ce qui donne une idée sur la qualité de la vitesse de transmission des informations sur le réseau.

L'échec ou la réussite d'un ping n'est pas toujours significatif :

- Le ping peut échouer alors que la communication fonctionne. Cela peut être le cas lorsque le réseau et le destinataire fonctionnent correctement mais que la configuration de celui-ci lui interdit de répondre aux requêtes de type ping.
- Le ping peut réussir, indiquant qu'une machine (un serveur Web par exemple) est joignable, mais le service sur cette machine peut être indisponible rendant l'accès impossible aux pages Web du serveur.

4.4.3.4 Test de fonctionnement d'ACL

Dans ce cas, on veut faire le test d'un PC refusé par l'ACL et un PC accédé aux réseaux 10.1.1.0 ou 10.2.2.0

- Ping du PC avec adresse IP 172.16.10.1

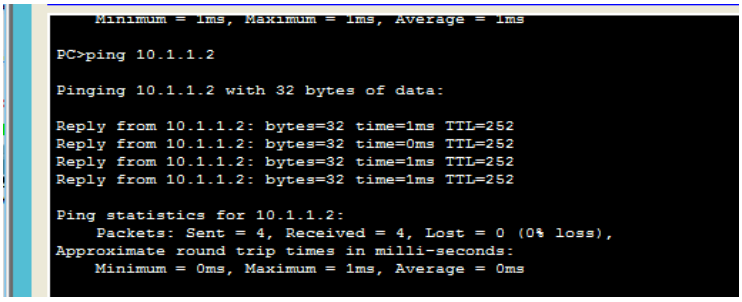


Figure 4.13 : *Résultats ping PC*

- Reply from 10.1.1.2
  - Indique l'adresse IP est 10.1.1.2 a bien répondu. Cela nous renseigne que les deux périphériques sont capables de communiquer ensemble.
  - Il y a 4 lignes car par défaut 4 paquets sont envoyés par la commande ping (variable selon le système d'exploitation), tous ont réussis.
- Bytes=32

La taille des données incluses dans le paquet envoyé (ce n'est pas la taille totale du paquet envoyé).

Time=1ms

Dans un environnement réel tel qu'un réseau local, le temps de parcours des paquets est généralement inférieur à 30ms.

- TTL=252

  Durée de vie d'un paquet (l'explication sera fournie ultérieurement)

- Ping statistics for 10.1.1.2

  Chacun des 4 paquets envoyés a reçu une réponse, la perte de paquets correspond donc à 0%.

- Round trip time

  En moyenne, il a fallu 0 ms (0 millisecondes) pour l'acheminement des paquets sur le réseau.

- Ping du PC avec adresse IP 172.16.30.1

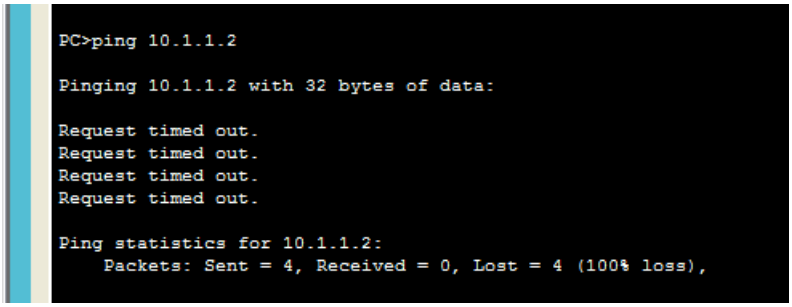


Figure 4.14 : *Résultat Ping*

Cela nous renseigne que les deux périphériques ne sont pas capables de communiquer ensemble.

4.4.3.5 Test de fonctionnement de STP

Voici la topologie de la partie STP :

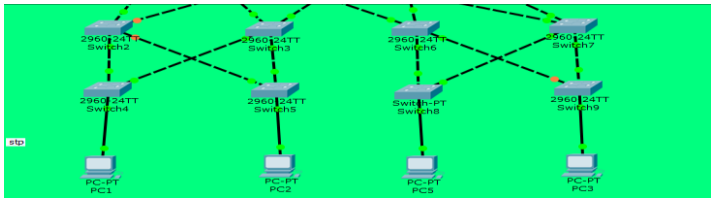


Figure 4.15 : *Topologie STP*

On va simuler une connexion entre PC 5 et PC 3. Tout d'abord on va faire un test de connectivité :

```
Pinging 192.168.17.2 with 32 bytes of data:

Reply from 192.168.17.2: bytes=32 time=1ms TTL=127
Reply from 192.168.17.2: bytes=32 time=0ms TTL=127
Reply from 192.168.17.2: bytes=32 time=0ms TTL=127
Reply from 192.168.17.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.17.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Figure 4.16 : *Premier ping PC3 vers PC5*

On va maintenant sectionner un lien actif

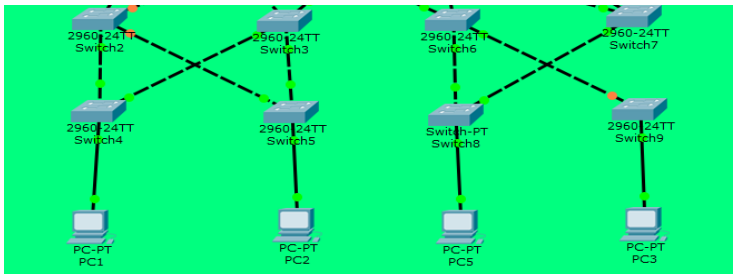


Figure 4.17 : *Topologie après coupure*

On refait le test de connectivité, et on a :

```
PC>ping 192.168.17.2

Pinging 192.168.17.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.17.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Figure 4.18 : *Ping après coupure*

Ceci est dû au temps de convergence de STP avant que l'autre lien ne redémarre. Puis le lien coupé redémarre à nouveau après quelques secondes :

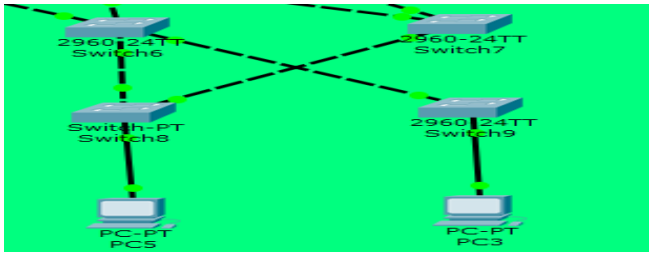


Figure 4.19 : *Redémarrage du lien*

Après on refait le test de connectivité :

```
PC>ping 192.168.17.2

Pinging 192.168.17.2 with 32 bytes of data:

Reply from 192.168.17.2: bytes=32 time=0ms TTL=127
Reply from 192.168.17.2: bytes=32 time=0ms TTL=127
Reply from 192.168.17.2: bytes=32 time=0ms TTL=127
Reply from 192.168.17.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.17.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4.20 : *Succès de l'envoi*

On remarque que la connexion a été rétablie entre PC3 et PC5

4.4.3.6 Simulation Etherchannel

Figure 4.21 : *Commutateurs reliés par des liens agrégés*

Les switch multicouches au niveau cœur sont configurés identiquement : protocole d'échange LACP et groupe 1. S'ils ne sont pas dans le même groupe ils ne peuvent pas communiquer. Les liens agrégés doivent pouvoir transmettre les données comme un seul lien entre ces les 2 switch multicouches. En cas de coupure, d'un ou de deux liaisons, les échanges doivent encore rester intacts.

Figure 4.22 : *Echange de PDU à travers les 2 switch multicouches*

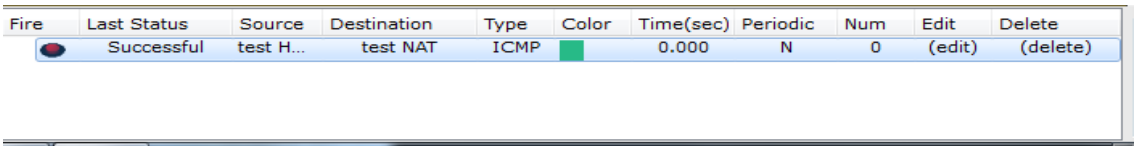


Figure 4.23 : *Résultat de l'envoi*

On voit que l'enveloppe transite à travers les trois liens comme sur un seul et arrive bien à destination.

Après coupure d'un lien voyons le résultat en mode simulation :

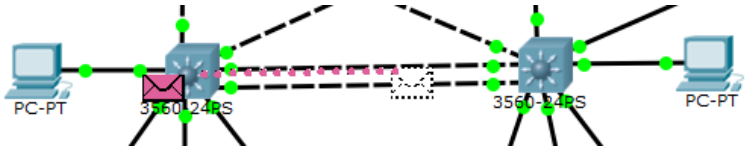


Figure 4.24 : *Echange de PDU à travers les 2 switch multicouches*

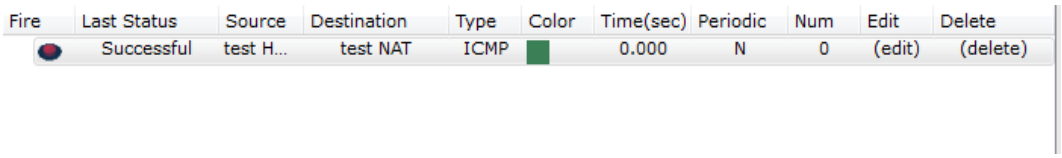


Figure 4.25 : *Résultat de l'envoi*

On a encore un succès. C'est-à-dire qu'Etherchannel assure vraiment la disponibilité de la communication entre ces commutateurs en maintenant les échanges intacts malgré les coupures. On sait aussi que grâce à Etherchannel, on augmente le débit au niveau de lignes agrégées. Malheureusement, il n'y a pas d'outil permettant d'évaluer cela sous Packet Tracer.

4.5 Conclusion

Pour conclure, on a vu que le serveur de sécurité adaptatifs ou ASA est l'une des meilleurs matériel de sécurité jusqu'à maintenant avec les techniques de système de prévention d'intrusion,le filtrage web et la contrôle de liste d'accès.

Et d'autre part Spanning Tree Protocol et EtherChannel assurent la disponibilité au sein du réseau.

CONCLUSION GENERALE

Les réseaux sont devenus indispensables au fonctionnement des systèmes d'information modernes, et il n'est plus possible aujourd'hui d'imaginer un système qui pourrait s'en passer. En termes de sécurité, ils demeurent souvent un véritable casse-tête, nécessitant de jongler entre les besoins de communication, les fonctionnalités offertes par les technologies et un niveau de sécurité acceptable. La mise en œuvre d'une politique de sécurité efficace est d'autant plus délicate que le domaine évolue très rapidement et qu'elle impose de nombreuses compétences à tous les niveaux. L'utilisation d'un réseau informatique peut donc s'avérer dangereuse, mais il existe des moyens plus ou moins efficaces de se protéger avec notamment : Des solutions de raccordement adaptées, une organisation sans faille.

La sécurité par définition, est une réponse à un état d'insécurité, permettant d'installer la confiance. Si de nombreuses entreprises et organisations ont consentis des efforts énormes dans la course vers les technologies pour assurer la sécurité, force est de constater que les réponses proposées restent bien souvent inopérantes ou insatisfaisantes. En effet, les technologies de l'information et de la communication sont très évolutives et la criminalité informatique suit cette dynamique.

Par ailleurs, l'arrivé du matériel Cisco ASA a répondu cette problème de sécurité avec sa technique de sécurité comme le système de prévention d'intrusion , la liste de contrôle d'accès, le filtrage web, la protection contre l'IP spoofing, elle est venue l'idée de faire intervenir ce matériel pour mieux combler les lacunes dans ce domaine.

A la fin de ce travail, je peux dire que j'ai bien pu avoir une visibilité concrète sur un domaine bien spécifique qui est la sécurité informatique. Ce travail m'a été profitable en terme d'acquérir une bonne expérience professionnelle, à travers laquelle j'ai eu l'occasion d'appliquer mes connaissances scientifiques et de confronter la notion théorique à la pratique.

ANNEXE 1

ETHERCHANNEL

A1.1 Définition

Mettre en place un etherchannel entre deux switch revient à combiner deux (ou plus) connexions afin d'augmenter la bande passante entre les deux dispositifs. Un peu comme si les deux connexions ne formaient qu'une.

A1.2 LACP

Le protocole LACP permet la mise en place d'agrégat de liens qui permet de regrouper plusieurs liens physiques en un seul lien logique et ainsi améliorer les performances en termes de bande-passante, de haute disponibilité et de répartition de charge.

LACP signifie Link Aggregation Control Protocol est un protocole de niveau 2 qui a pour référence IEEE 802.3ad.Il existe une alternative au protocole LACP par l'intermédiaire du protocole PAgP qui est un protocole propriétaire Cisco. [17]

A1.3 Conditions requises

Pour la mise en place de l'EtherChannel sous Cisco, les conditions suivantes doivent être respectées :

- Support de l'EtherChannel sur les interfaces de l'équipement
- Même mode duplex (full duplex / half duplex)
- Même vitesse
- La plage de VLANs autorisés doit être la même des deux côtés sinon l'EtherChannel passera en mode Desirable.

A1.4 Architecture etherchannel

On partira du principe où sur chaque switch, ce sont les ports fastEthernet 0/1 et 0/2 qui sont utilisés pour l'agrégation.

Switch1 FastEthernet 0/1 connecté sur le Switch2 FastEthernet 0/1

Switch1 FastEthernet 0/2 connecté sur le Switch2 FastEthernet 0/2 [17]

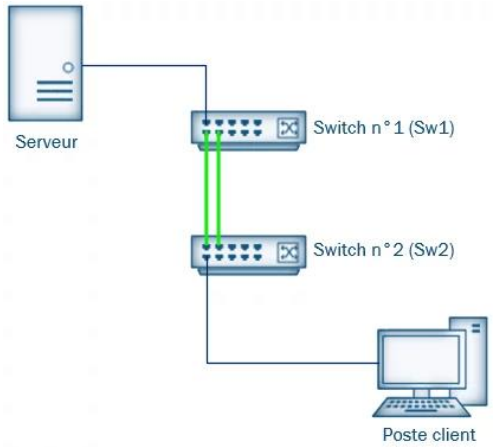


Figure A1.01 : *Architecture EtherChannel*

Pour la réalisation de cet exemple, on doit utiliser le logiciel Cisco Packet Tracer.

A1.5 Configuration des switch

Switch1

switch1> en

switch1# configure terminal

switch1(config)# interface range fastethernet 0/1 - 2

switch1(config-range-if)# switchport mode trunk

switch1(config-range-if)# channel-protocol lacp

switch1(config-range-if)# channel-group 1 mode active

switch1(config-range-if)# no shut

switch1(config-range-if)# exit

switch1(config)#exit

switch1#

On a donc ici mis les deux ports FastEthernet dans un groupe, on les a mis en mode trunk, on a précisé qu'on voulait utiliser le Protocol LACP (il existe aussi PAGP, la différence de configuration se situe uniquement dans le mode à choisir), on a défini le mode passif (l'etherchannel ne fonctionnera que si lacp est active sur l'autre switch aussi). [17]

Switch2

switch2> en

switch2# configure terminal

switch2(config)# interface range fastethernet 0/1 - 2

switch2(config-range-if)# switchport mode trunk

switch2(config-range-if)# channel-protocol lacp

switch2(config-range-if)# channel-group 1 mode passive

switch2(config-range-if)# no shut

switch2(config-range-if)# exit

switch2(config)#exit

switch2#

A1.6 Vérification de l'étherchannel

switch1#show etherchannel summary

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

u - unsuitable for bundling

U - in use f - failed to allocate aggregator

d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group Port-channel Protocol Ports

------+-------------+-----------+---

1 Po1(SU) LACP Fa0/1(I) Fa0/2(I)

ANNEXE 2

HSRP (Hot Standby Router Protocol)

A2.1 HSRP

A2.1.1 Présentation

HSRP (Hot Standby Router Protocol) est un protocole de redondance, propriétaire Cisco, permettant de mettre en place une tolérance de panne pour les passerelles par défaut (RFC2281) et est basé sur le fonctionnement d'ARP (Adress Resolution Protocol). Ses particularités.[16]

- Version 1 (IPv4):
- Adresse multicast : 224.0.0.2
- Port : UDP 1985
- MAC Virtuelle: 0000.0c07.acXX
- Version 2 (IPv4):
- Adresse multicast : 224.0.0.102
- Port : UDP 1985
- MAC Virtuelle : 0000.0c9f.fXXX
- Version 2 (IPv6):
- Adresse multicast : FF02::66
- Port : UDP 2029
- MAC Virutelle : 0005.73A0.0XXX
- (XX est le numéro du groupe exprimé en hexadécimal)
- 2.4.1.2 Entête HSRP

Après configuration, les routeurs d'un même groupe s'échangent des paquets contenant les informations sur eux-mêmes et les règles à suivre dans HSRP.

- OpCode : 0 = Hello (le routeur est actif), 1 = Coup (le routeur veut devenir la passerelle active), 2 = Resign (le routeur cède sa place de passerelle active).
- Etat : Défini l'état du routeur qui envoi le message (0 = initial, 1=learn, 2=listen, 4=Speak, 8=Standby, 16=active)
- HelloTime: Intervalle en secondes entre deux messages de type «hello»

- HoldTime: Délai en secondes au-delà duquel un routeur est considéré comme hors service si aucun message «hello» n'est reçu de sa part.
- Priorité: Influence le choix de la passerelle active. La préférence va à la plus grande priorité. (Défaut = 100)
- Groupe: identifiant du groupe HSRP.
- Authentification: 8 caractères (8x8bits) définissant un mot de passe en clair
- Adresse IP Virtuelle: Adresse IP virtuelle pour le groupe HSRP en question.

Version (8)	OpCode (8)	Etat (8)	HelloTime (8)
HoldTime (8)	Priorité (8)	Groupe (8)	Réserve (8)
Authentification			
Authentification			
Adresse IP Virtuelle			

Figure A2.01 : *Informations dans l'entête*

A2.1.2 Etats du routeur HSRP

- Initial : Etat initial lorsque HSRP se met route ou qu'un changement de configuration a lieu.
- Learn : Le routeur n'a pas encore appris son adresse IP virtuelle, ni reçu de messages «hello». Le routeur est en attente d'un message du routeur actif.
- Listen : Le routeur connait son adresse IP virtuelle mais n'est ni le routeur actif, ni standby et attend un message de ceux-ci.
- Initial : Etat initial lorsque HSRP se met route ou qu'un changement de configuration a lieu.
- Speak : Le routeur participe à l'élection du routeur actif et émet les messages «hello» périodiques.
- Standby : Le routeur est candidat pour devenir le prochain routeur actif et envoi des messages «hello» périodiques.
- Active : Le routeur est la passerelle active et route le trafic destiné à l'adresse MAC virtuelle du groupe.
- Timers :
- Hello: 3s

- Hold timer: 10s
- Modifiables via la commande standby [#] timers hello hold

A2.1.3 Fonctionnement

Un groupe de routeurs fonctionne comme un routeur virtuel en partageant une adresse IP virtuelle et une adresse MAC virtuelle. Un routeur actif exécute l'acheminement des paquets pour les hôtes locaux. Les autres routeurs fournissent un « secours automatique » en cas de panne du routeur actif. Les routeurs en attente demeurent au repos en ce qui a trait à l'acheminement des paquets du côté client. [16]

Cet état de repos est appelé aussi standby.

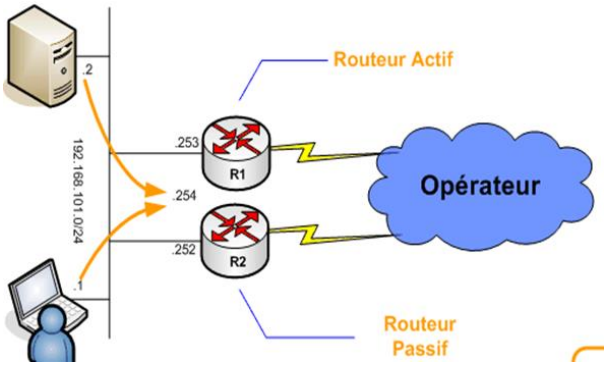


Figure A2.02 : *Etat initial des routeurs*

En partageant une seule même adresse IP et MAC, plusieurs routeurs peuvent être considérés comme un seul routeur "Virtuel". Les membres du groupe de ce routeur virtuel sont capables de s'échanger des messages d'état et des informations.

Un routeur physique peut donc être "responsable" du routage et un autre en redondance.

Si le routeur, que nous appellerons primaire, a un problème, le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent les mêmes adresses IP et MAC. [16]

A2.1.4 Configurations

Voici un exemple de code :

R1(config)#interface Fastethernet 0/0

R1(config-if)# ip address 192.168.0.2 255.255.255.0

R1(config-if)#standby 1 ip 192.168.0.1

R1(config-if)#standby 1 priority 105

R1(config-if)#standby 1 preempt

R1(config-if)#standby 1 track fa0/0

R1(config-if)#standby authentication string x

- La commande « standby x » permet de définir le groupe HSRP où le routeur est placé
- "standby priority xxx" définit une priorité au routeur. Celui qui possédera la plus grande valeur sera élus actif. Si la configuration du routeur ne stipule pas la priorité, alors la valeur par défaut de 100 sera appliquée.
- "standby preempt" permet d'accélérer le processus d'élection.
- "standby ip xxx.xxx.xxx.xxx" indique l'adresse IP virtuelle partagée entre les deux routeurs.
- "standby track xxxxxx" permet de superviser une interface et de baisser de 10 la valeur de la priorité HSRP si elle devenait Down.
- standby authentication string x configuration de la clé partagée

.

BIBLIOGRAPHIES

[1] N. Pascal, « *Réseau Informatique de réseaux Master 1 informatique*» http://www.info.univ-angers.fr/pub/pn/,UFR Sciences de l'Université d'Angers, 2006 ;

[2] A. André, « *Réseau Informatique* », http://www.httr.ups-tlse.fr/pedagogie/cours/, Université Paul Sabatier – Toulouse III, 2005 ;

[3] A. Ratsimbazafy, « *Réseaux Informatiques* », Cours L2-TCO, Dép. TCO-E.S.P.A., A.U. : 2010-2011.

[4] L. E. Randriarijaona « *cours TCP/IP* », Cours 3ème année, Dép. Tél. – E.S.P.A., A.U : 2012-2013

[5] L. E. Randriarijaona « *cours conception du réseau d'entreprise* », Cours M1, Dép. Tél. – E.S.P.A., A.U : 2013-2014

[6] A. Stéphane« *cours Réseaux* », TS IRIS – LEGT Louis Modeste-Leroy – Évreux, 2004 ;

[7] http://www.frameip.com;2007

[8] P. Bruno, «*Support de cours Réseaux* », EISTI, EISTI – Cergy, 2001 ;

[9] L. Bloch, C. Wolfhugel. « *Sécurité Informatiques* »: principes et méthodes. 2005

[10] L. Yves « *Sécurité* », 2002, http://lescop.free.fr/cours/securite.pdf

[11] http://packetstormsecurity.org , 2003

[12] E. Maiwald, « *Sécurité des réseaux* », Campus press, 2001.

[13] M. Suter, lic. phil. I, collaborateur scientifique, Center for Security Studies (CSS), ETH

Zurich « *Sécurité informatique* ».2003

[14] CCNA Discovery version 4.exe, « *Conception et prise en charge des réseaux informatiques* »2003

[15] www.Cisco.com //ASA5500(5505,5510,5520,etc)Séries Firewall Security A.mht, 2009

[16]C.D. Stefano et S. Wong, *« Les protocoles de redondance HSRP, VRRP et CARP* », 2007

[17] CISCOMADESIMPLE.BE «*Configuration de base d'un Etherchannel entre deux Switch*»,2007

[18] Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6 - Starting Interface ,2010

[19]« *TP mise en œuvre du Spanning Tree* », BTS SIO-SISR 5, Lyvée du Grand NouméaConfiguration (ASA 5505) [Cisco ASA 5500-X Series Next-Generation Firewalls] - Cisco.htmtm,2010

[20]T. Delage, « *Network Address Translation, Port Address Translation* », GRETA VIVA5/IUT Valence, 2012

[21]http://www.certa.fr, « *Filtrage et parefeux* », 2006

[22]C. Milard, « *Cours pare-feu* », comment ça marche, licence GNU FDL, ed 2003

PAGE DE RENSEIGNEMENTS

Nom : MIHARISOA RAMBOARISON

Prénom : Fenitriniaina

Adresse de l'auteur : Lot 1126 G 40 Tsivatrinikamo Antsirabe 110

Téléphone : +261 33 18 235 70

E-mail : fenitraramboarison@gmail.com

Titre du mémoire :

ETUDE ET MISE EN PLACE DE LA SECURITE RESEAU AU SEIN DU MFB « CISCO ASA »

Nombre de pages : 99

Nombre de tableaux : 3

Nombre de figures : 57

Directeur de mémoire : Monsieur RANDRIARIJAONA Lucien Elino

Téléphone : +261 32 04 747 95

Email : elrandria@yahoo.com

RESUME

Nous avons tout au long de notre travail mis en place un système sécurisé avec le matériel Cisco. La sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau filaire ou non filaire ; aucune entreprise ne peut prétendre vouloir mettre en place une infrastructure réseau, quelque soit sa taille, sans envisager une politique de sécurité. On a vu dans ce projet la généralité sur le réseau qui explique quelques concepts utilisés dans le réseau informatiques, vue globale sur la sécurité réseau qui a parlé sur la sécurité réseau en générale, les attaques informatiques et quelques protocoles de sécurité. L'implémentation de la solution retenue face aux menaces : le système de prévention d'intrusion et la liste de contrôle d'accès avec le Cisco ASA 5525-x.

Mots clés : Hiérarchique, Sécurité, Redondance, ASA, IPS

ABSTRACT

We have throughout our work set up a secure system with Cisco hardware. Computer security is almost indispensable for the proper functioning of a wired or wireless network, no company can claim to want to set up a network infrastructure, whatever its size, without considering a security policy : generality in this project we saw on the network that explains some concepts used in the computer network provides a summary, overall view of network security, who spoke on general network security, computer attacks and some security protocols; The implementation of the solution to face threats: intrusion prevention system and the access control list with the Cisco ASA 5525-X.

Keys words : Hierarchical, Security, Redondancy, ASA, IPS