République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : **Sciences et Technologies** Filière : **Génie Electrique**

Spécialité : **TELECOMMUNICATION ET RESEAUX**

Présenté par
TALMAT AISSI GHENIMA
AKNOUCHE Celia

Thème

Etude et configuration d'un système de sécurité ASA 5510

Mémoire encadré par :
Mr LAAZRI

Promotion 2017

Remerciements

Nous remercions tout d'abord, Allah qui nous a donné la force et le courage pour terminer nos études et élaborer ce modeste travail.

Nous tenons à exprimer nos plus sincères remerciements à notre promoteur Mr LAAZRI, qui nous a aidé au long du travail.

Un grand merci à Mr khadir Wahab et à Mr Tiguercha Rafik de l'école 2int pour leurs encouragements et leurs orientations qui nous ont beaucoup aidés.

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

Nous tenons à remercier également nos amis (es) et nos familles pour leurs aides considérables.

DEDICACE

A MA RAISON DE VIVRE, D'ESPÉRER

A MA SOURCE DE COURAGE, A CEUX QUE J'AI DE PLUS CHER :

MON PAPA, MA MAMAN, POUR LEUR AMOUR, LEUR SOUTIEN ET LEUR CONFIANCE.

A MES FRÈRES QUE J'AIME BEAUCOUP

A MES ADORABLES SŒURS, MES CHÈRES BELLES SŒURS, MES PETITS BÉBÉS D'AMOUR MASSI ET ALYANE ,MES COUSINES ET COUSINS SURTOUT CELIA ET TOUTE LA FAMILLE TALMATAISSI

A MA CHÈRE AMIE, SŒUR ET BINÔME CYCY

A TOUS MES AMIS SURTOUT DJOUDJOU ET SOUS.

LILIA

DEDICACE

A MA RAISON DE VIVRE, D'ESPÉRER

A MA SOURCE DE COURAGE, A CEUX QUE J'AI DE PLUS CHER :

MON PAPA, MA MAMAN, POUR LEUR AMOUR, LEUR SOUTIEN ET LEUR CONFIANCE.

A MON FRÈRE QUE J'AIME BEAUCOUP

A MON ADORABLE SŒUR ET SON MARI AINSI QUE MON BÉBÉ D'AMOUR ALÉS, COUSINES ET COUSINS ET TOUTE LA FAMILLE AKNOUCHE.

A MA CHÈRE AMIE, SŒUR ET BINÔME LYLIA.

A TOUS MES AMIS SURTOUT DJOUDJOU ET SOUS.

CELIA

LISTE DES FIGURES

LISTE DES FIGURES

Glossaire

AIM	Adaptive Identification and Mitigation
ACL	Access Control Entry
AIP SSM	Advanced Inspection and Prevention Security Services Module
ARP	Adress Resolution Protocol
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CA	Certificate Authority
CSC SSM	Content Security and Control Security Services Module
CIFS	(Common Internet File Systèm)
DDoS	Distributed Denial-of-Service a
DMZ	Demilitarized Zone
DNS	Domain Name System
FTP	File Transfer Protocol
GNS3	Graphical Network Simulator
HTTPS	Hypertext Transfer Protocol Secure
IDA	Identity and Access
ICMP	Internet Control Message Protocol
IOS	Inter-network Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MAN	Métropolitain Area Network

NAT Network Address Translation

NFS Network Address Translation

NCP Netware Core Protocol

OSI Open Systems Interconnection

PAT Port Address Translation

QOS Quality of Service

RADIUS Remote Authentication Dial In User Service

RAID Rendundant Array of Independent Disks

RVP Réseau privé virtuel

RPF Reverse Path Forwarding

SMB Server Message Block

SSH Secure Shell

SSL Secure Socket Layer

SNMP Simple Network Management Protocol

SMTP Simple Mail Transfer Protocol

SQL Structured Query Language

TCP Transfer Control Protocol

TFTP Trivial File Transfer Protocol ou protocole simplifié de fichiers

Telnet Telecommunications Network

Glossaire

USB Universal Serial Bus

VPN Virtual Private Network

VLAN Virtual Local Area Network

WAN Wide Area Network

Sommaire

Chapitre II

Sommaire

RESUME

Les réseaux et systèmes information sont devenus des outils indispensables au fonctionnement des entreprises. Ils sont aujourd'hui déployés dans tous les secteurs professionnels : les entreprises de communication, les banques, les assurances, la médecine ou encore le domaine militaire. Initialement isoles les uns des autres, ces réseaux sont dans le présent interconnectes et le nombre de points d'accès ne cesse de croitre.

Ce développement phénoménal s'accompagne naturellement de l'augmentation du nombre d'utilisateurs. Ces utilisateurs, connu ou non, ne sont pas forcément pleins de bonnes intentions vis-à-vis de ses réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et système pour essayer d'accéder à des informations sensible dans le but de les lire, les modifier ou les détruire, pour porter atteinte au bon fonctionnement du système ou encore tout simplement par jeu.

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines vu l'expansion et l'importance grandissante des réseaux informatiques lesquels ces derniers ont engendré le problème de sécurité des systèmes information. Dans la plupart d'organisations informatisées, partager les données directement entre machine et leur souci majeur. Il s'avère indispensable de renforcer les mesures de sécurité dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Afin d'assurer le bon fonctionnement global de l'entreprise, on utilise une technique d la décomposition du réseau en zone de sécurités séparées.

Cette décomposition appelée (DMZ) nécessite la mise en place d'un firwall pour pouvoir l'administrer.

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

Les réseaux et systèmes information sont devenus des outils indispensables au fonctionnement des entreprises. Ils sont aujourd'hui déployés dans tous les secteurs professionnels : les entreprises de communication, les banques, les assurances, la médecine ou encore le domaine militaire. Initialement isoles les uns des autres, ces réseaux sont dans le présent interconnectes et le nombre de points d'accès ne cesse de croitre.

Ce développement phénoménal s'accompagne naturellement de l'augmentation du nombre d'utilisateurs. Ces utilisateurs, connu ou non, ne sont pas forcément pleins de bonnes intentions vis-à-vis de ses réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et système pour essayer d'accéder à des informations sensible dans le but de les lire, les modifier ou les détruire, pour porter atteinte au bon fonctionnement du système ou encore tout simplement par jeu.

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines vu l'expansion et l'importance grandissante des réseaux informatiques lesquels ces derniers ont engendré le problème de sécurité des systèmes information. Dans la plupart d'organisations informatisées, partager les données directement entre machine et leur souci majeur. Il s'avère indispensable de renforcer les mesures de sécurité dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Afin d'assurer le bon fonctionnement global de l'entreprise, on utilise une technique d la décomposition du réseau en zone de sécurités séparées.

Cette décomposition appelée (DMZ) nécessite la mise en place d'un firwall pour pouvoir l'administrer.

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

Dans notre projet fin d'étude on va voir comment mettre en place un firwall matériel et sa configuration de base dans un réseau il s'agit de Cisco ASA 5510, et aussi on va définir la solution de translation d'adresse IP (NAT) cette dernière permet de convertir les adresse privées a des adresses publique.

Pour réaliser cette démarche on a partagé notre projet on trois chapitre

Le premier chapitre comporte une présentation pour les réseaux informatiques, qu'elle va englober une définition pour le réseau informatique, ces différents types, ces caractéristique, et aussi comment garantie une connexion entre les composons de réseau, et la connexion entre un réseau et un autre.

Le deuxième chapitre montre les différentes menaces qui peuvent atteindre un système d'information d'une entreprise ces menaces qui peut être d'une source humain ou technique.

Et aussi explique la politique de sécurité qui contient plusieurs aspects et aussi qui définit plusieurs mesures de sécurité pour face au divers menaces réseau et pour mettre le système d'information d'une entreprise en haut sécurité.

Le troisième chapitre inclus la conception de notre projet au on va définir le firewall et ces différents fonctionnalité. On va définir l'équipement utilisé pour réaliser notre démarche on parle de Cisco ASA 5510 on va voir ces divers composant.

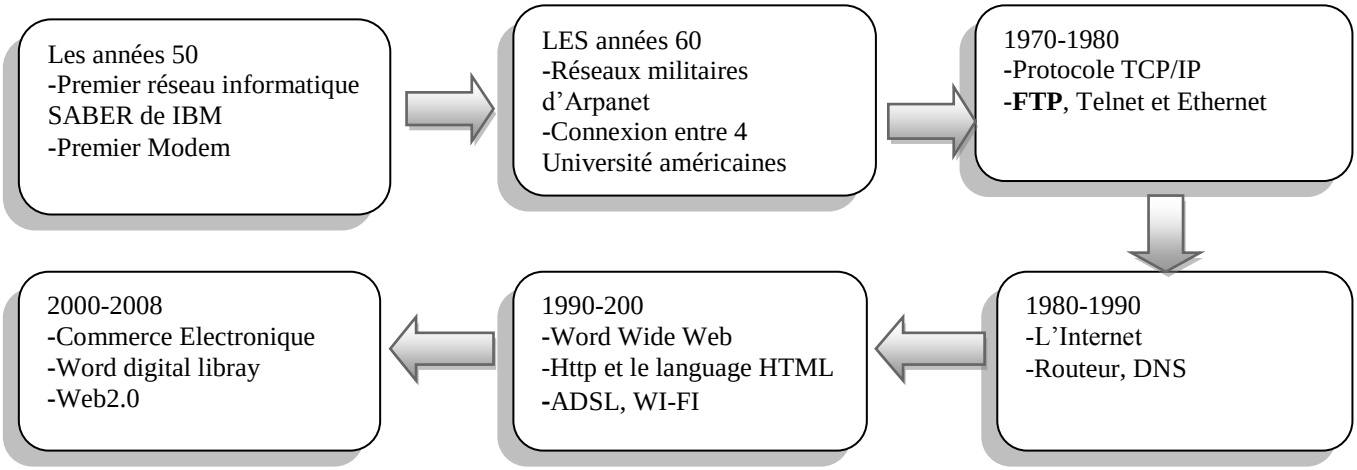
Et aussi comportes l'implémentation pour faire configurer Cisco ASA.

I.1 .Préambule

L'installation d'un réseau est d'un point de vue matériel un processus assez linéaire ; il est impératif de faire les choses dans un certain ordre, afin de s'assurer du bon fonctionnement futur de l'ensemble.

Dans ce chapitre, nous allons se familiariser avec les différents éléments qu'un réseau doit constituer pour qu'une information émise d'un ordinateur puisse être acheminée et routée vers son ordinateur réceptif voulu.

I.2-Historique



L'ordinateur est un outil très pratique; mais une fois en réseau, l'tendue de ses possibilités devient pratique infinie. Voici l'histoire des moyens de communications et des réseaux informatiques qui ont permis l'apparition d'internet.

Dans les années 50, SABER réalisé par IBM été le premier réseau informatique dans un but commercial a la fin de cette période la BELL crée le premier Modem permettant de transmettre des données binaires sur une simple ligne téléphonique.

A partir des années 60 et dans un but militaires l'ARPANET un département américain de la défense crée un réseau de communication capable de résister à une attaque nucléaire, et grâce au financement du ministère de la défense une connexion des premiers ordinateurs entre 4 universités américaines à été établie.

Les années 70, Bob KAHN et VINT CERF élaborent un protocole permettant d'acheminer des données sur un réseau il s'agit de TCP/IP et l'année 1973 a connu la création d'un protocole FTP.

A partir des années 80 Vint Cerf lance un plane d'interconnexion qui a été le plan de départ de réseau internet. La société Cisco Système fabrique le premier routeur. Les années 90 ont vu l'explosion du protocole http ainsi le langage HTML et le développement des réseaux haut débit telles que l'ADSL WI-FI….etc

Le développement de réseau et ces déférentes technologies n'été pas arrêté, et le commerce mondial devenant par l'utilisation d'internet un commerce électronique, et la bibliothèque mondiale devient une bibliothèque numérique mondiale.

I.3. Définition d'un réseau informatique

Un réseau informatique est une collection de PC et d'autres dispositifs interconnectés par câble pour pouvoir communiquer entre eux et partager les ressources et information. Il permet de faire circuler des éléments entre chacun de ces objets selon les règles bien définies.

I.4. Classification des réseaux

On distingue quatre classes de réseaux : selon la taille, l'organisation, la méthode d'accès et le type de machine.

I.4.1. Classification selon la taille

La figure I.1 nous montre les différents types des réseaux selon la taille, et on distingue :

- Les **LAN** (Local Area Network) : réseaux locaux pour de courtes distances avec des débits de quelques dizaines de Mbits /seconde jusqu'à quelques centaines.
- Les **MAN** (Metropolitan Area Network) : Destinés à courir de très grands périmètres qui sont fédérateurs de réseaux locaux.
- **WAN** (Wide Area Network) : qui signifie réseau étendu, permettent de connecter plusieurs LAN éloignées entre elles. Le débit devient de plus en plus faible en fonction de la distance. « Internet est un regroupement de WAN

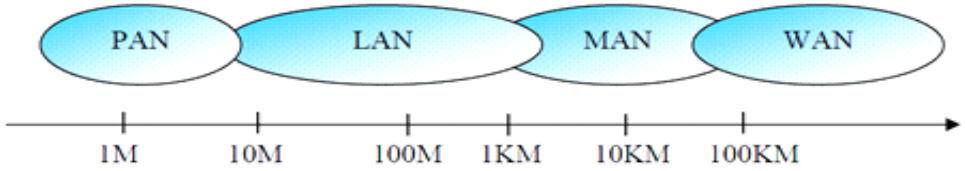


Figure I.1 classification selon la taille

I.4.2. Classification selon l'organisation

- **Architecture d égal à égal (Peer to Peer)**

Parfois appelée poste à poste dans cet ur central jouant le rôle d'un serveur dédié. Ainsi chaque ordinateur dans tel réseau est parfois serveur, parfois client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources.

- **Architecture de type client /serveur**

Un réseau d'architecture client/serveur est celui ou les ordinateurs (clients) sont reliés à un serveur dédié qu'est un ordinateur central fournit des services réseaux au client.

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur qui est une machine généralement très puissante en terme de capacité d'entrée-sortie, qui leurs fournit des services. Ces services sont des programmes fournissant les données telles que les fichiers, une connexion…

I.4.3. Classification selon la méthode d'accès

C'est le classement selon l'arrangement physique, c'est-à-dire la configuration spatiale du réseau et les machines qui le composent, on distingue généralement les topologies suivantes :

- **Topologie en bus**

Tous les équipements sont branchés en série sur le serveur (voir figureI.2). Chaque poste reçoit l'information mais seul le poste pour lequel le message est adressé traite l'information. On utilise un câble coaxial pour ce type de topologie.

Figure I.2: Topologie en bus

- **Topologie en anneau**

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

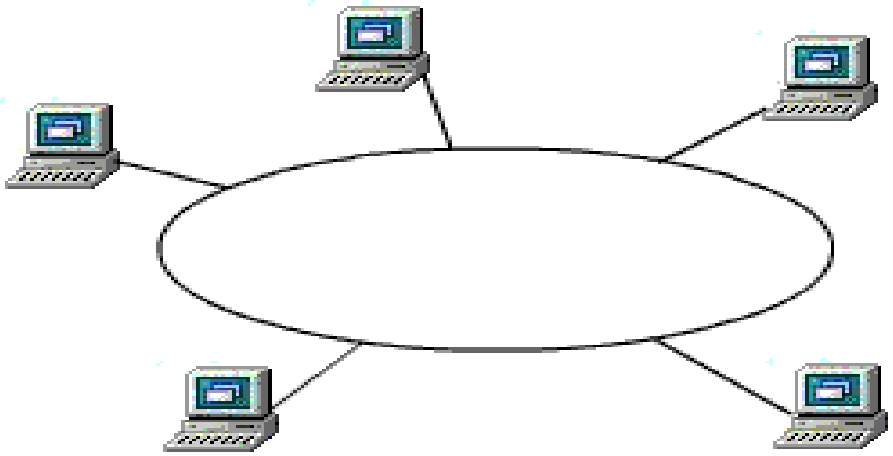


Figure I.3: Topologie en anneau

- **Topologie en étoile**

C'est la topologie réseau la plus courante, notamment avec les réseaux Ethernet, les ordinateurs du réseau sont relies a un système matériel central appelé concentrateur (ex : hub). Il comprend un certain nombre de jonction auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Donc il assure la communication entre les différentes jonctions.

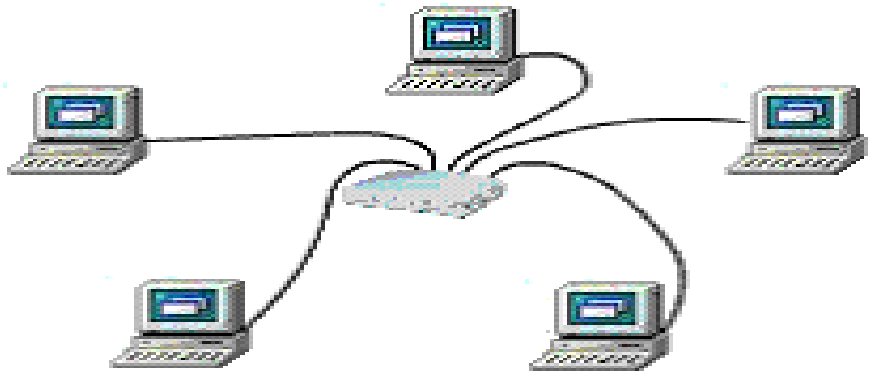


Figure I.4: Topologie en étoile

Ce type de réseaux est facile à maintenir mais la défectuosité du nœud central provoque un arrêt de tout le réseau.

I.5.Support de transmission

Les supports de transmission sont nombreux. Parmi ceux-ci, on distingue : les supports Métalliques, non métalliques et immatériels. Lors de la conception d'un réseau, le choit du support de transmission dépendra d'un certain nombre de critères parmi lesquels on distingue :

- Le cout.
- Bande passante : la bande passante d une voie est la plage de fréquence sur laquelle la voie est capable de transmettre des signaux sans que leur affaiblissement soit trop important.
- Vitesse de transmission.
- Distance du câble.
- Insensibilité au bruit.
- Type du signale véhiculé (analogique ou numérique).

I.5.1. Câble coaxial

La figure illustre la structure d'un câble coaxial.

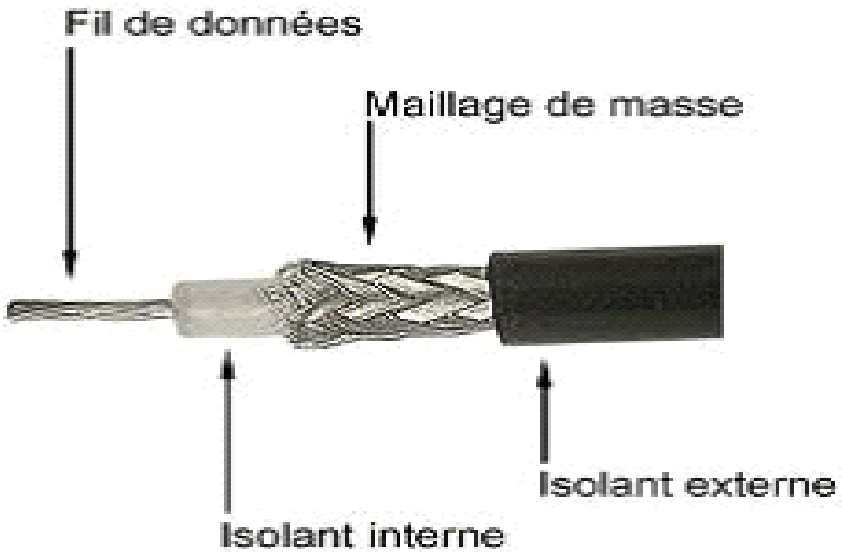


Figure I.5: câble coaxial

Le câble coaxial ou ligne coaxiale est une ligne de transmission ou liaison asymétrique, utilisée en hautes fréquences d'un câble à deux conducteurs.
La capacité de transmission de ce câble dépend de sa longueur et des caractéristiques physiques des conducteurs et de l'isolant.

- La gaine permet de protéger le câble de l environnement extérieur. Elle est habituellement en caoutchouc (parfois en chlorure de polyvinyle (PVC), éventuellement en téflon).
- Le blindage (enveloppe métallique) entourant les câbles permet de protéger les données transmises sur le support des parasites (autrement appelé bruit) pouvant causer une distorsion des données.
- L isolant entourant la partie centrale est constitué d un matériau diélectrique permettant d éviter tout contact avec le blindage, provoquant des interactions électriques (court-circuit).

On distingue habituellement deux types de câble coaxial utilisé pour des transmissions en bande de base :

- **Thicknet :** Epais et raide (diamètre environ 12mm) à cause de son blindage, il est recommandé pour l'installation de câble fédérateur. Sa gaine est jaune. Utilisée pour 10base 5.

- **Thinnet :** D'un diamètre plus réduit, il est plus pratique dans des installations comprenant des courbes. De plus, il est plus économique, mais dispose d'un blindage moins conséquent utilisée pour 10 bases 2.

Le câble coaxial offre de nombreux avantages du fait de sa capacité à s'étendre sur une plus grande distance et de son cout parmi les plus faibles. C'est une technologie utilisée depuis de nombreuses années pour les types de communications de données.

I.5.2.La paire torsadée

La paire torsadée est une ligne de transmission formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but principal de limiter la sensibilité aux inférences et la diaphonie dans les câbles multi paire.

Les paires torsadées se trouvent en téléphonie, en électroacoustique, en instrumentation et en transmission de données informatiques, domaine où elles ont fait l'objet d'importants développements. Elles s'utilisent aussi dans les câbles de puissance, afin de réduire leurs émissions.

I.5.3.Fibre optique

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de lumière et sert dans la transmission de données par la lumière, et peut servir de support à un réseau « large bande » par lequel transitent aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

Entourée d'une gaine protectrice, la fibre optique peut être utilisée pour conduire de la lumière entre deux lieux distants de plusieurs centaines, voire milliers, de kilomètres. Le signal lumineux codé par une variation d'intensité est capable de transmettre une grande quantité d'information. En permettant les communications à très longue distance et à des débits jusqu'alors impossibles, les fibres optiques ont constitué l'un des éléments clés de la révolution des télécommunications. Ses propriétés sont également exploitées dans le domaine des capteurs (température, pression, etc.), dans l'imagerie et dans éclairage

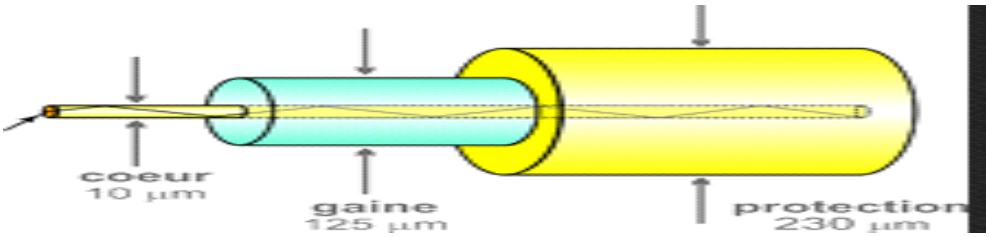


Figure I.6: La fibre optique

I.6.Equipements d'interconnexion

Les réseaux hétérogènes formant internet sont reliés entre eux grâce à des dispositifs d'interconnexion (passerelles, routeurs, ponts…) qui assurent le transfert des données

I.6.1.Carte réseau

Une carte réseau est matérialisée par un ensemble de composants électroniques soudés sur un circuit imprimé. L'ensemble constitué par le circuit imprimé et les composants soudés s'appelle une carte électronique, d'où le nom de carte réseau. La carte réseau assure l'interface entre l'équipement ou la machine dans lequel elle est montée et connectés sur le même réseau. Aujourd'hui on peut trouver des cartes réseau un peu partout, dans les ordinateurs, imprimantes, téléphones portables, consoles de jeux, télévisions… On n'utilise le terme « carte réseau » que dans le cas d'une carte électronique autonome prévue pour remplir ce rôle d'interface réseau. Ainsi, un ordinateur muni d'une interface réseau assurée par des composants soudés sur sa carte mère ne comporte pas, à proprement parler, de carte réseau. Les équipements communiquent sur le réseau au moyen de signaux qui doivent absolument respecter des normes

I.6.2. Les Hubs (concentrateurs)

Le hub est également appelé concentrateur ou répétiteur. C'est un boitier électronique assurant la liaison entre des postes et des périphériques du réseau.

On peut y connecter plusieurs stations, dont le nombre dépond de type de HUB. Un HUB sera connecté sur un autre HUB ou sur un serveur qu'avec une seule et unique ligne.

II.6.3. Les ponts

Ce sont des dispositifs permettant de relier des réseaux travaillant avec les mêmes protocoles. Aussi appelé Bridge. Ces ponts :

- offrent les services des répéteurs et permettent de segmenter le réseau en sous-réseaux indépendants, dispositif actif filtrant (collision) :
  - permettent de diminuer la charge du réseau : amélioration des performances.
  - Sécurisent des échanges entre segments
  - Sont Capable de convertir des trames de formats différents (ex : Ethernet – Token Ring). Si les stations émettrices et réceptrices se trouvent du même côté du pont, la trames ne le traversera pas pour aller polluer le deuxième segment.

I.6.4.Les Switch

Un Switch désigne un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique. Contrairement au concentrateur(ou hub), le Switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau.

Le Switch permet ainsi de libérer la bande passante en évitant ainsi le transfert de données inutiles sur le réseau.

I.6.5.Les Routeurs

Un Routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, et acheminer le différent segment des paquets en fonction de la couche trois les routeurs prennent des discision logique d'optimisation pour choisir la meilleur voie des données d'un réseau a un autre et de diriger ensuite les paquets vers le pont de sortie qui correspond au port de sortie suivant.

I.6.6.Les Passerelles

Une passerelle est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, l'information est codée et transportée différemment sur chacun des réseaux.

Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en termes de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre

I.7.Description de modèle OSI :

Le modèle OSI ou Open Systems Interconnections, créé en 1978 par l'organisation internationale de normalisation (ISO), a pour objectif de constituer un modèle de référence d'un réseau informatique et ceci dans le but de permettre la connexion entre les architectures propriétaires hétérogènes qui existaient. Ce modèle est constitué de sept couches dont chacune correspond à une fonctionnalité particulière d'un réseau, et chaque couche immédiatement adjacente Même si le modèle OSI est très peu implémenté aux couches. Il sert toujours de référence pour identifier le niveau de fonctionnement d'un composant réseau. Ainsi paradoxalement aujourd'hui, TCP/IP est mis en œuvre partout et même lorsque l'on parle de ce protocole on l'associe aux couches de modèles OSI.

Les quatre premières couches dites basses, assurent l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les trois autres couches, dites hautes, sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques.

	L'architecture de modèle OSI	
	Couches	Fonction
7	Application	C'est le programme qui a besoin du réseau pour communiquer. Exemple: navigateur internet, logiciel de messagerie ou de transfert de fichier HTTP, FTP POP…..
6	Présentation	Responsable de la représentation des données (de telle sorte qu'elle soit indépendante du type de microprocesseur ou du système d'exploitation par exemple et éventuellement de chiffrement Exemple: HTML
5	Session	En charge d'établir et maintenir des sessions (c'est-à-dire débuter le dialogue entre 2 machines.
4	Transport	Assure le contrôle de l'acheminement Exemple: TCP UDP.
3	Réseau	Gère le routage des données et la commutation Exemple : IP
2	Liaison	Assure l'acheminement point à point
1	Physique	Gère le signale en l'adaptant au support physique

		Le support physique

Figure I.7: les couches de modèle OSI

I.8.Architecture TCP/IP

Architecture de référence développée en 4 couches sur base de protocoles existants :

+ Couche application

+ Couche transport

+ Couche internet (pour "inter réseaux")

+ Couche accès réseau

TCP/IP vs OSI

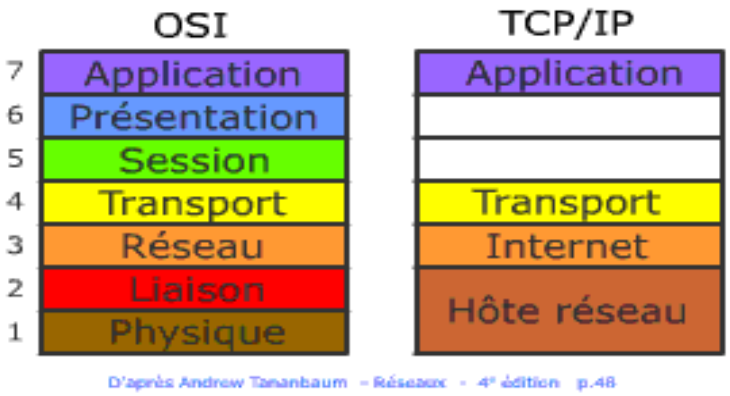


Figure I.7: Analogie de modèle OSI avec le modèle TCP/IP

TCP/IP est à la fois une architecture réseau, mais aussi l'acronyme de 2 protocoles réseau liés :

- TCP (Transmission Control Protocol) : protocole de transport
- IP (Internet protocol): protocole réseau (adressage)

L'architecture réseau TCP/IP se décompose en 4 couches dans laquelle les protocoles TCP et EP jouent un rôle important.

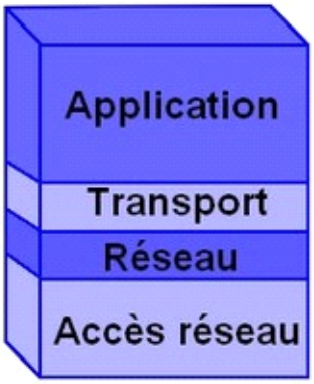


Figure I.8 : les couches de modèle TCP/IP

Couche4 : Application c'est ici que l'on trouve protocoles de communication entre les clients et les serveurs (HTTP, FTP, POP et SMTP)

Couche3 : transport on retrouve ici les protocoles de transport des données. Les plus utilisés sont : protocole TCP et protocole UDP

Couche2 : réseau dans cette couche on trouve principalement deux protocoles. Le protocole IP qui permet le routage des informations entre réseaux (Utilisation de l'adresse IP) et le protocole ICMP qui permet le contrôle d'erreur et de signalisation.

Couche 1 : accès au réseau c'est la couche de plus bas niveau sur le réseau. Cette couche contient des protocoles qui gère l'acheminement des informations entre émetteur et destinataire. On retrouve dans cette couche adresse MAC ainsi que le protocole Ethernet et le protocole WIFI (802.11).

I.9.Encapsulation des données :

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

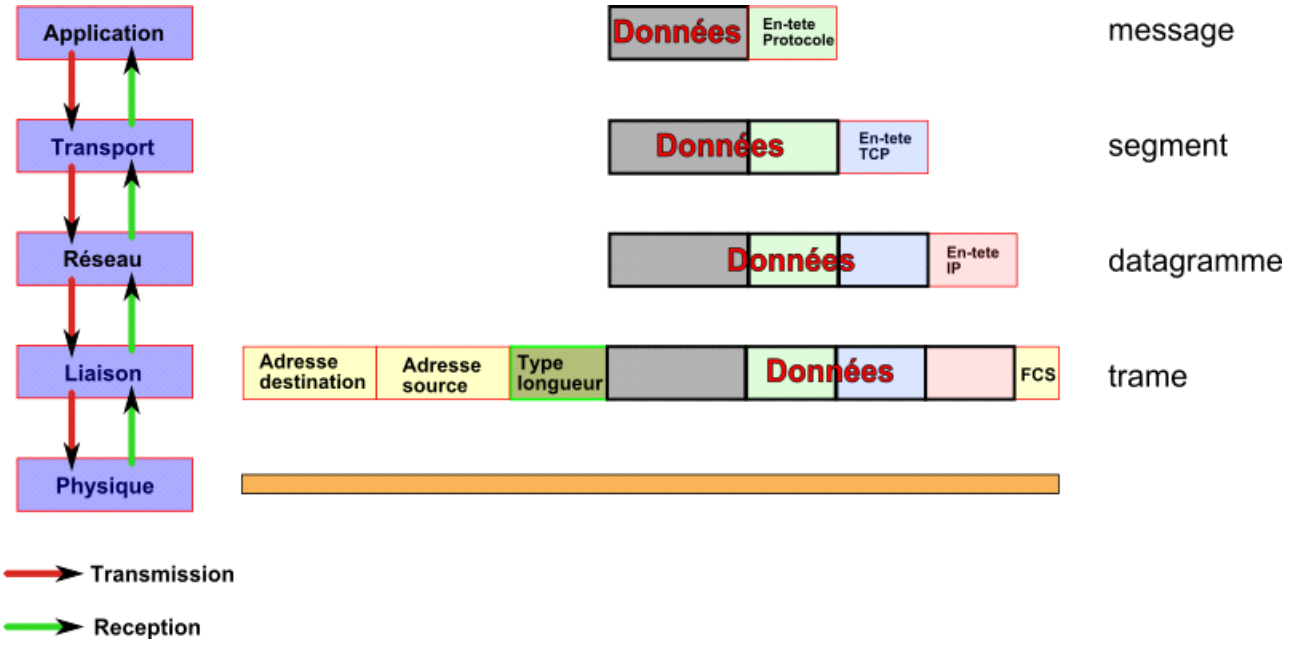


Figure I.9. : Encapsulation au niveau des couches TCP/IP

I.10.Les protocoles des données :

I.10.1.Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers(FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocoles ICMP).

Sur internet par exemple les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble relié entre eux. Cette suite de protocole s'appelle TCP/IP.

I.10.2Les différents protocoles réseaux

I.10.2.1.Protocole DNS

Le DNS (Domain Name Système) est un système essentiel au fonctionnement d'internet. C'est entre autres, le service qui permet d'établir la correspondance entre le nom de domaine et son adresse IP. L'échelle gigantesque à laquelle est déployé ce service rend le

système capital pour le monde actuel, que ce soit pour des raisons financières, économiques ou politiques.

I.10.2.2.Protocole TCP

Est un protocole fiable ce protocole sécurité d'échange de données : créé dans le but d'établir une communication de haute fiabilité entre deux exécutées sur deux ordinateurs autonomes et raccordés à un réseau (protocole orienté connexion).

I.10.2.3.Protocole IP

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différentes des paquets, mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâces à la gestion des adresses IP.

Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits), on les notes sous la forme xxx.xxx.xxx.xxx ou chaque xxx présente un entier de 0 à 255.

Par exemple 194.153.205.26 est une adresse IP, on peut distinguer deux parties dans une adresse IP :

- ✓ Les nombres de gauches désignent le réseau (on l'appelle net ID)
- ✓ Les nombres de droites désignent les ordinateurs de ce réseau (on l'appelle host ID)

I.0.2.4.Protocoles ICMP (internet contrôle protocole)

C'est un protocole qui permet le contrôle des erreurs de transmissions. En effets, comme le protocole IP ne gère que le transport des paquets et ne permet pas l'envoi de messages d'erreurs, c'est grâces à se protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau.

I.10.2.5.Protocole réseau UDP

Le protocole UDP (User Datagramme Protocol) est l'un des deux principaux protocoles utilisé sur les réseaux TCP/IP, que le réseau soit Ethernet ou sans fils. Contrairement au TCP, il ne permet pas à l'émetteur de vérifier si les données sont effectivement reçus en recevant un accusé de réception. De fait, il est sa structure est plus simple est les transferts plus rapides. Par contre, il utilise aussi 65535 ports différents pour communiquer (de 0 à 65535), chaque réseau utilise un ou plusieurs numéros pour communiquer.

I.10.2.6.Protocole ARP

ARP (adress resolution protocol) est un protocole réseau utilisé pour effectuer la correspondance adresse MAC adresse Ethernet dans les réseaux Ethernet. Il est implanté sur la couche internet de modèle TCP/IP au meme niveau que l'ICMP, IGMP….C'est également le nom de la commande réseau sous DOS qui affiche et modifie les tables de correspondance d'adresse IP/physique utilisé par le protocole.

I.10.2.7.Protocole RARP

RARP (Reverse Address Resolution Protocol) est un protocole permettant à un équipement d'obtenir son adresse IP en communiquant son adresse Ethernet à un serveur RARP [RFC 903].

RARP s'effectuera au Boot de la machine qui gardera ensuite en mémoire son adresse IP. Après avoir obtenue son adresse IP, la machine peur récupérer les fichiers de configuration.

D'autres mécanismes existent pour qu'un équipement (avec ou sans disque) obtienne son adresse IP dynamiquement. Nous verrons de tels protocoles (BOOTP, DHCP) dans un autre chapitre

I.10.2.8.Protocole RIP

RIP est un protocole de routage IP de type vecteur distance basé sur l'algorithme de routage décentralisé Bellman-Ford. Il permet à chaque routeur de communiquer aux autres routeurs la métrique, c'est-à-dire la distance qui les sépare du réseau IP (le nombre de sauts qui les sépare, ou « hops » en anglais). Ainsi, lorsqu'un routeur reçoit un de ces messages, il incrémente cette distance de 1 et communique le message aux routeurs directement accessibles.

Les routeurs peuvent donc conserver de cette façon la route optimale d'un message en stockant l'adresse du routeur suivant dans la table de routage de telle façon que le nombre de sauts pour atteindre un réseau soit minimal.

I.10.2.9.Protocole OSPF

Le protocole OSPF permet à partir d'un nœud de calculer le chemin le plus court avec les contraintes indiquées dans les contenus associés à chaque liaison

OSPF, beaucoup plus complexe que RIP, fait partie de la deuxième génération de protocoles de routage.

Il utilise une base de données distribuées qui garde en mémoire l'état des liaisons. Ces

informations forment une description de la topologie du réseau et de l'état des nœuds qui permet de définir l'algorithme de routage par un calcul des chemins les plus courts. L'utilisation de RIP est adaptée pour des réseaux relativement simples alors qu'OSPF s'applique à des réseaux d'interconnexion plus complexes.

I.10.2.10.Protocole de gestion de groupe IGMP

IGMP (internet Groupe Management Protocol), défini dans le RFC 1112, permet aux machines de déclarer leur appartenance à un ou plusieurs groupes auprès du routeur multipoint dont elles dépendent soit spontanément soit après interrogation du routeur. Celui-ci diffusera alors les datagrammes destinés à ce ou ces groupes. IGMP, comme ICMP, fait partie de IP (protocole numéro 2) et comprend essentiellement deux types de messages : un message d'interrogation (Host Membership Query), utilisé par les routeurs, pour découvrir et/ou suivre l'existence de membres d'un groupe et un message de réponse (Host Membership Report), délivre en réponse au premier, par au moins un membre du groupe concerné.

I.11.Le routage dans les réseaux

I.11.1.Fonctionnement d'un routeur

La fonction de routage traite les adresses IP en fonction de leur adresse réseau définie par le masque de sous-réseaux et les redirige selon l'algorithme de routage et sa table associée. Ces protocoles de routage sont mis en place selon l'architecture de notre réseau et les liens de communication inter sites et inter réseaux.

I.11.2.Les protocoles de routage

Les protocoles de routages permettent l'échange des informations à l'intérieur d'un système autonome. On retient les protocoles suivants **:**

- ✓ **états de lien**, ils s'appuient sur la qualité et les performances du média de communication qui les séparent. Ainsi chaque routeur est capable de dresser une carte de l'état du réseau pour utiliser la meilleure route : *OSPF*
- ✓ **vecteur de distance**, chaque routeur communique aux autres routeurs la distance qui les sépare. Ils élaborent intelligemment une cartographie de leurs voisins sur le réseau : *RIP*

- ✓ **hybride** des deux premiers, comme *EIGRP*

Les protocoles couramment utilisés sont :

- ❖ Routing Information Protocol (RIP)
- ❖ Open Shortest Path First (OSPF)
- ❖ Enhanced Interior Gateway Routing Protocol (EIGRP)

I.11.3.Type de routages

Il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un protocole de routage, il s'agit du routage statique et du routage dynamique.

I.11.3.1.Routage statique

Dans le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes (par l'intermédiaire de port de sortie ou d'IP de destination) à emprunter pour aller sur tel ou tel réseau. Concrètement, un routeur sera un pont entre deux réseaux et le routeur d'après sera un autre pont entre deux autres réseaux :

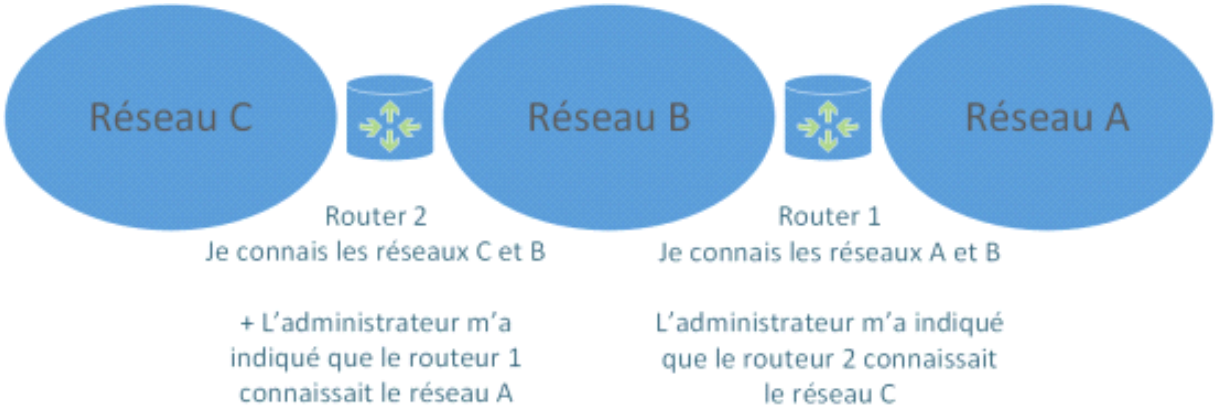


Figure I.10 : routage statique

Ici, l'administrateur a indiqué au routeur 2 que le réseau A pouvait être joint à travers le routeur 1 qu'il connait puisqu'il se situe sur le même réseau (B) que lui. Le routage statique permet donc à l'administrateur de saisir manuellement les routes sur les routeurs et ainsi de choisir lui même le chemin qui lui semble le meilleur pour aller d'un réseau A à un réseau B. Si un nouveau réseau vient à se créer sur le routeur 1 par exemple, il faudra indiquer au route B.

I.11.3.2.Routage dynamique

Le routage dynamique permet quant à lui de se mettre à jour de façon automatique. La définition d'un protocole de routage va permettre au routeur de se comprendre et d'échanger

des informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Concrètement, le protocole de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleures routes à emprunter. Nous verrons un peu plus bas qu'il existe pour cela deux méthodes mais avant voici un schéma qui illustre le routage dynamique :

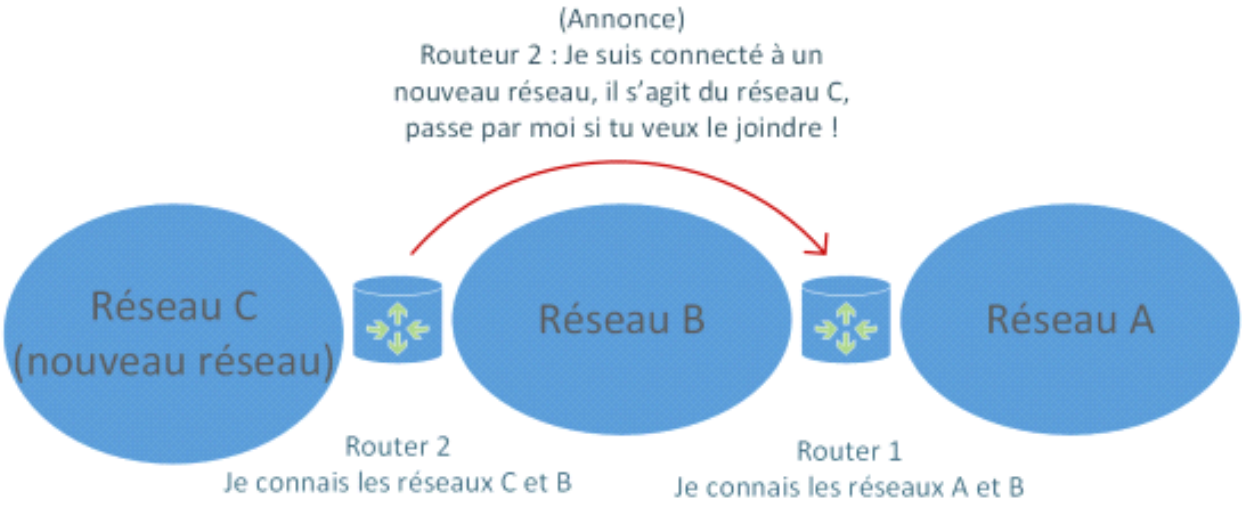


Figure I.11 : Routage dynamique

On voit ici que dans un premier temps, on ajoute le réseau C au routeur 2 (on le connecte à l'interface du routeur 2). Une annonce va ensuite suivre pour que les autres routeurs sachent que le réseau C est joignable via le Routeur 2. Par la suite, les routeurs continueront à communiquer périodiquement pour voir si chacun des routeurs est toujours joignable. Si un routeur vient a tomber et qu'une autre route existe pour accéder à un réseau, les tables de routages des routeurs vont se modifier dynamiquement via des communications faites entres les routeurs et le calcul de la meilleur route possible à emprunter. Cela facilite la transmission des informations entre les routeurs et la mise à jour des topologies réseaux. On doit bien sûr pour cela définir la façon dont ils vont communiquer et calculer les routes (le protocole de routage qu'ils doivent utiliser). Ils pourront ensuite se comprendre par l'échange de messages de mise à jour, des messages "hello" (indiquant que l'hôte est toujours joignable), des requêtes et des réponses diverses et différentes selon le protocole de routage.

I.12.Adressage

Sur Internet, les 1'ordinateurs communiquent entre eux grâce au protocole IP (*Internet Protocol*), qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Par exemple, *194.153.205.26* est une adresse IP donnée sous une forme technique.

Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

C'est l'ICANN (*Internet Corporation for Assigned Names and Numbers*, remplaçant l'IANA, *Internet Assigned Numbers Agency*, depuis 1998) qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public internet.

Déchiffrement d'une adresse IP

Une **adresse IP** est une adresse 32 bits, généralement notée sous forme de 4 nombres entiers séparés par des points. On distingue en fait deux parties dans l'adresse IP :

- ✓ une partie des nombres à gauche désigne le réseau est appelée ID de réseau (en anglais *netID*),
- ✓ Les nombres de droite désignent les ordinateurs de ce réseau est appelée ID d'hôte (en anglais *host-ID*).

I.12.1.Adresses particulières

Lorsque l'on annule la partie host-id, c'est-à-dire lorsque l'on remplace les bits réservés aux machines du réseau par des zéros (par exemple *194.28.12.0*), on obtient ce que l'on appelle l'**adresse réseau**. Cette adresse ne peut être attribuée à aucun des ordinateurs du réseau.

Lorsque la partie net id est annulée, c'est-à-dire lorsque les bits réservés au réseau sont remplacés par des zéros, on obtient l'**adresse machine**. Cette adresse représente la machine spécifiée par le host-ID qui se trouve sur le réseau courant.

Lorsque tous les bits de la partie host-id sont à 1, l'adresse obtenue est appelée l'**adresse de diffusion** (en anglais **broadcast**). Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le *net ID*.

Enfin, l'adresse 127.0.0.1 est appelée adresse de débouclage (en anglais loopback), car elle désigne la machine locale (en anglais localhost).

I.13.Discussion

Dans ce chapitre nous avons présenté quelques définitions et généralités sur les réseaux informatiques. Vu la fiabilité de communication qu'ils assurent, ils devenu aujourd'hui une nécessite dans le mode de travail. Les différentes menaces et attaques sur divers système nous ont ramené à partir de la nécessite de grandir certain besoins de sécurisation : tels que l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que les méthodes d'attaque et comment se protéger contre elles.

Dans le deuxième chapitre nous allons présenter la sécurité du réseau informatique suffisamment profond dans les déférents types de menaces, les protocoles de sécurité, les méthodes de protection et les mécanismes de protection.

II.1.Préambule

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

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

II.2.Définition de la sécurité

La sécurité informatique est une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système informatique. Quoi qu'il en soit, il n'existe aucune technique capable d'assurer l'inviolabilité d'un système.

Les principes fondamentaux de la sécurité des données dans un système d'information, car cela s'applique partout dans l'informatique, notamment dans les infrastructures qu'il convient de protéger.

Les exigences génériques de sécurité des réseaux et de l'information présentent les caractéristiques indépendantes suivantes :

II.2.1.La confidentialité

La confidentialité est la propriété d'une information de ne pouvoir être accédée que par des personnes, entités ou processus autorisés et de ne pouvoir être divulguée qu'à des personnes, entités ou processus autorisés. Cette possibilité d'accorder un accès sélectif aux informations doit être assurée tout au long de la vie de ces informations notamment au cours de leurs collectes, de leur conservation, de leurs traitements et de leurs communications. En pratique, les seules personnes autorisées à accéder aux données à caractère personnel sont les personnes dont la fonction ou les activités professionnelles justifient cet accès. Les degrés de confidentialité dépendent de la nature des informations. Des mesures de tous types peuvent être établies afin d'assurer que les données soient vues par les personnes autorisées : les mesures physiques sont communément mises en place pour accorder l'accès aux bonnes personnes comme l'installation d'un lecteur biométrique à l'entrée de locaux

informatiques. D'autres mesures logiques peuvent être configurées notamment sur des équipements, comme des règles de flux venant d'un pare-feu, ou encore une gestion des groupes et des autorisations associées.

II.2.2.L'intégrité

L'intégrité est un autre aspect de la gestion des données. Il s'agit ici de s'assurer par divers moyens que les données ne soient pas altérées au cours de leur acheminement. L'intégrité couvre deux aspects différents : l'intégrité des informations et l'intégrité des systèmes et processus. L'intégrité d'une information est la propriété de ne pas être altérée ou détruite de manière non autorisée, volontairement ou accidentellement. L'intégrité d'un système ou d'un processus est la propriété de réaliser la fonction désirée de façon complète et selon les attentes, sans être altérée par une intervention non autorisée, volontaire ou accidentelle.

II.2.3.Disponibilité des données

La disponibilité est la propriété des informations, systèmes et processus d'être accessibles et utilisables sur demande d'une entité autorisée.

La disponibilité a pour but de maintenir en condition opérationnelle tous les équipements, logiciels qui composent l'infrastructure informatique d'une société. L'attribution de la bande passante et de mesures pour éviter les éventuelles latences est également une composante de ce principe. La disponibilité repose sur des techniques de redondance (multiplication d'un équipement assurant le même service).

II.2.4.Authentification

L'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connait.

Le code secret d'un utilisateur est une information personnelle qui ne doit en aucun cas être divulgués. Il est aussi communément nommé "mot de passe".

II.3.Politique de sécurité

II.3.1.Définition

Une politique de sécurité réseau est un document générique qui définit des règles à suivre pour les accès au réseau informatique et pour les flux autorisés ou non, détermine comment les politiques sont appliquées et présente une partie de l'architecture de base de l'environnement de sécurité du réseau.
La mise en place d'une politique de sécurité adéquate est essentielle à la bonne sécurisation des réseaux et systèmes d'information.
La Politique de Sécurité exprime la stratégie de l'entreprise en matière de sécurité de l'information. Elle constitue la référence en matière de protection de ses Systèmes d'Information et traduit les exigences de sécurité en règles pragmatiques. Il n'existe pas de règles déclinables à tous, chaque entreprise présentant des particularités. Cela nécessite une étude ad hoc devant aboutir à des préconisations personnalisées.

Une politique de sécurité doit comprendre au moins les éléments suivants :

• les fondements de la sécurité de l'information propres à l'organisme intégrant les obligations légale et les missions propres à l'organisme. La politique de sécurité précisera notamment les principes régissant la protection des données à caractère personnel ;

• les exigences de sécurité à respecter en termes de confidentialité, intégrité, disponibilité, imputabilité, authenticité, fiabilité et non répudiation des informations ;

• les différents éléments de sensibilisation aux arguments et au contenu même de cette politique définie par l'organisme ;

• la description des différents rôles, responsabilités et règles organisationnelles cadrant la mise en application de la politique de sécurité ;

• la démarche de gestion des risques adoptée par l'organisme afin de détecter les risques, de les apprécier selon des critères définis et de déterminer les modalités pour les traiter en les réduisant à un niveau acceptable ;

• la description du cadre organisationnel des processus de gestion des incidents de sécurité ;

• les modalités générales de gestion de la sécurité de l'information, notamment en matière de protection et de prévision ;

• les modalités retenues par l'organisme afin d'intégrer la politique de sécurité dans les processus de développement, de maintenance et de changement ;

• les dispositions de surveillance, d'évaluation et de mises à jour de la politique de sécurité et des différents composants de sécurité mis en place.

II.3.2.Objectif d'une politique de sécurité

La définition d'une politique de sécurité n'est pas un exercice de style mais une démarche de toute l'entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageables pour son activité.

La définition d'une politique de sécurité réseau fait intégralement partie de la démarche sécuritaire de l'entreprise. Elle s'étend à de nombreux domaines, dont les suivants :

- audit des éléments physiques, techniques et logiques constituant le système d'information de l'entreprise ;
- sensibilisation des responsables de l'entreprise et du personnel aux incidents de sécurité et aux risques associés ;
- formation du personnel utilisant les moyens informatiques du système d'information ;
- structuration et protection des locaux abritant les systèmes informatiques et les équipements de télécommunications, incluant le réseau et les matériels ;
- ingénierie et maîtrise d'œuvre des projets incluant les contraintes de sécurité dès la phase de conception ;
- gestion du système d'information de l'entreprise lui permettant de suivre et d'appliquer les recommandations des procédures opérationnelles en matière de sécurité;
- définition du cadre juridique et réglementaire de l'entreprise face à la politique de sécurité et aux actes de malveillance, 80 pour 100 des actes malveillants provenant de l'intérieur de l'entreprise ;
- classification des informations de l'entreprise selon différents niveaux de confidentialité et de criticité.

Avant de définir une politique de sécurité réseau, il faut en connaître les objectifs ou finalités.

II.4.Classification des risques

II.4.1.Attaques sur les réseaux

- **Le sniffing**

Le Sniffing est une forme d'attaque sur le réseau couramment utilisée par les pirates
Le Sniffing ou reniflement de trafics constitue l'une des méthodes couramment utilisée par les pirates informatiques pour espionner le trafic sur le réseau. Dans la pratique, les hackers ont généralement recours à ce procédé pour détecter tous les messages circulant sur le réseau en récupérant des mots de passe et des données sensibles. Les pirates informatiques utilisent des sniffers réseau ou renifleurs de réseau pour pouvoir surveiller le réseau et soustraire frauduleusement les différents types de données confidentielles susceptibles de les intéresser.

- **L'IP spoofing**

« L'usurpation d'adresse IP » (également appelée mystification ou en anglais IP Spoofing) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine (figure1). Ce type d'attaque s'utilise de deux manières différentes : • La première utilité de l'IP Spoofing est la falsification de la source d'une attaque. Par RÉGIS SENET CET ARTICLE EXPLIQUE... Ce qu'est l'IPSpoofing Les risques encourus Comment s'en protéger ce qu'il faut savoir... Connaissance en système d'exploitation Linux et les bases des réseaux exemple, lors d'une attaque de type déni de service, l'adresse IP source des paquets envoyés sera falsifiée afin d'éviter de localiser la provenance de l'attaque permettant à l'attaquant d'être anonyme. • La seconde utilisation de l'IP Spoofing permet de profiter d'une relation de confiance entre deux machines pour prendre la main sur l'une des deux.

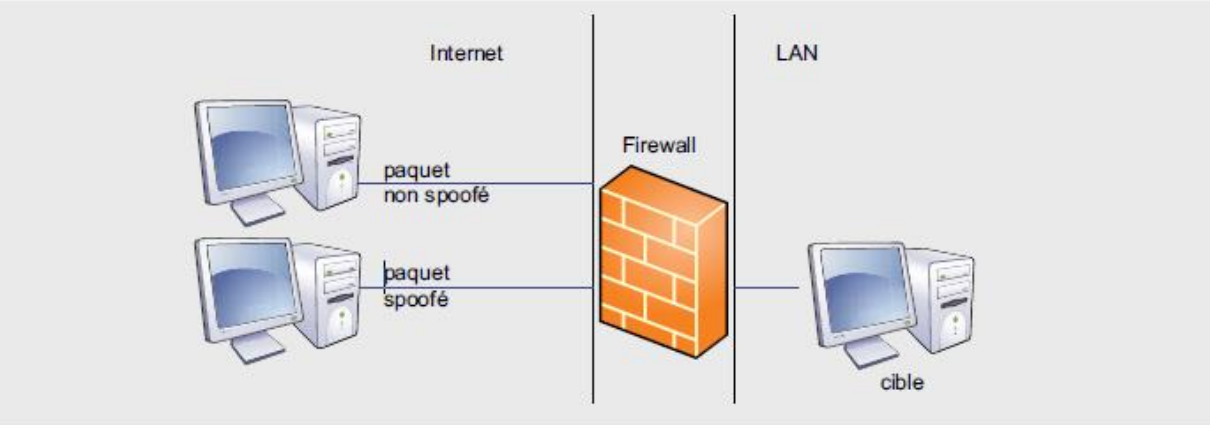


Figure I1.1 : Utilisation de paquets spoofé

II.4.2.Attaques logiciels

II.4.2.1.Ecoute

L'écoute électronique par réseau Wi-Fi est une autre méthode employée par les cybercriminels pour obtenir de l'information personnelle.

De quoi s'agit-il?

Écoute virtuelle de l'information qui est partagée sur un réseau Wi-Fi non sécurisé (non chiffré).

Quelles sont les conséquences?

- Grâce à l'écoute électronique par réseau Wi-Fi, il est possible accéder à votre ordinateur grâce à l'équipement adéquat.
- Les cybercriminels volent vos informations personnelles, y compris vos renseignements pour procéder à une ouverture de session et les mots de passe.

II.4.2.2.Un ver

Un ver est un programme capable de se propager et de s'auto-reproduire sans l'utilisation d'un programme quelconque ni d'une action par une personne. Sur chaque ordinateur où il agit, le ver crée une nouvelle liste de machines distantes cibles. En parallèle, le ver :

1. essaie de trouver les mots de passe des comptes utilisateurs,

2. essaie d'entrer dans chaque machine cible en se faisant passer pour un utilisateur de la machine ``attaquante" (après avoir cracker le mot de passe utilisateur), et en utilisant un ancien bug dans le protocole finger, qui permet de savoir quels sont les usagers connectés sur une machine distante ou sur quelle machine est connecté un utilisateur donné.

Les attaques de vers sont toutefois très rares parce que les serveurs sur internet sont de plus en plus performants (Windows NT Server ou Apache), mais c'est toujours une méthode utilisée par les hackers quand un nouveau bug est découvert dans un système d'exploitation. Les vers permettent aux agresseurs d'attaquer un maximum de sites en peu de temps. Le routeur firewall ne doit pas s'attarder à filtrer les vers : c'est la qualité du système d'exploitation qui doit permettre d'enrayer toute attaque de vers.

II.4.2.3.Un virus

Les constructeurs de firewalls tendent maintenant à fournir avec leurs produits une solution antivirus complète, qui permet de filtrer les attaques logicielles comme les chevaux de Troie, les vers, les trappes et les bombes logiques. Les éléments actifs du réseau sont désormais de véritables remparts contre une pléthore d'attaques, qu'elles soient au niveau réseau ou au niveau applicatif. Cela rend la tâche des administrateurs réseau plus simple, car toutes les fonctions de sécurité sont fédérées sur un seul et même équipement, plus robuste et entièrement administrable. Les éléments composant le réseau ne sont pas les seuls remparts aux attaques. Le système d'exploitation garantit un niveau de sécurité supplémentaire vis-à-vis des attaques de type virus.

II.4.2.4.Cheval de Troie

Un cheval de Troie est un programme qui se cache lui-même dans un autre programme apparemment au-dessus de tout soupçon. Quand la victime (l'utilisateur normal) lance ce programme, elle lance par là même le cheval de Troie caché. Actuellement, les chevaux de Troie les plus utilisés sont : Back Orifice 2000, Backdoor, Netbus, Subseven, Socket de Troie. La méthode la plus efficace pour se protéger de ces programmes néfastes est d'utiliser un bon antivirus comme Norton 2000 ou Network Associates. Des programmes spécifiques permettent également de scruter toute tentative de connexion sur les ports scrutés. Lockdown 2000 est le plus connu d'entre eux : une fois une tentative de connexion détectée, il fait un traceroute sur l'IP qui a tenté la connexion. La version 4 possède en bibliothèque 488 signatures de ``Troyans". La machine Linux devra être équipée d'un antivirus permettant de repérer non seulement les virus, mais également les chevaux de Troie.

II.4.2.5.Logiciel espion (spyware)

Fonctionnement **:** Un logiciel espion peut être téléchargé à partir de sites Web, d'e-mails, de messages instantanés et de connexions directes de partage de fichiers. Par ailleurs, un utilisateur peut, sans le savoir, recevoir un logiciel espion en acceptant un contrat de licence utilisateur final d'un programme informatique.

Que faire ?

- Utiliser un programme de sécurité Internet connu pour vous protéger de manière proactive contre les logiciels espions et les autres risques de sécurité.
- Configurer le pare-feu de ce programme de sécurité pour bloquer les demandes de communications sortantes qui n'ont pas été sollicitées.
- Ne pas accepter, ni ouvrir de messages d'erreur suspects dans votre navigateur.
- Refuser les offres de logiciels gratuits, les logiciels espions pouvant être intégrés à de telles offres.
- Toujours lire attentivement le contrat de licence utilisateur final lors de l'installation et annuler l'installation si d'autres « programmes » sont installés avec le programme souhaité.
- Tenir à jour les correctifs de sécurité et logiciels.

II.5.Autres attaques

II.5.1.Les menaces accidentelles

Les menaces accidentelles ne supposent aucune préméditation. Dans cette catégorie, sont repris les bugs logiciels, les pannes matérielles, et autres défaillances "incontrôlables". Sont le fait d'incendies, l'inondation de pannes d'équipements ou de réseau, utilisation maladroite défaut de qualité,…..

II.5.2.Les menaces intentionnelles

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque. Elles font l'objet principal des mesures de protections. Parmi elles, on compte les menaces passives et les menaces actives.

Les menaces passives sont :

Les détournements des données (l'écoute sur le réseau à l'aide des sniffeurs, les indiscrétions) : c'est le cas de l'espionnage industriel, l'espionnage commercial, les copies illicites par exemple.

Quant aux menaces actives, nous pouvons citer :

- Les modifications des informations
- la fraude financière informatique
- Le sabotage des informations
- Les modifications des logiciels

II.5.3. Attaque par déni de service

L'attaque par déni de service est causée en inondant un serveur ou un site web de requêtes dans le but de le rendre indisponible. L'attaque par déni de service peut être perpétrée par un petit nombre de ressources. Un pirate peut utiliser son seul ordinateur pour contrôler des zombies, c'est-à-dire d'autres ordinateurs infectés qui obéiront à ses commandes. Ces ordinateurs peuvent avoir précédemment été infectés par des virus ou des vers.

Même si seulement 15 % des entreprises en ont été victimes, selon l'étude TELUS-Rotman, une telle cyberattaque peut causer de lourdes pertes financières si elle vise un site web transactionnel, par exemple. Des raisons politiques peuvent aussi animer les pirates informatiques, comme en témoigne l'attaque contre les sites du gouvernement du Canada en juin 2015, revendiquée par le collectif Anonymous en réponse à l'adoption du projet de loi C-51.

Face à la variété des menaces, adopter des mesures de sécurité proactives permet de prévenir ces attaques plus efficacement qu'en colmatant les brèches une à une.

II.5.4.Hameçonnage

La technique d'hameçonnage est utilisée le plus souvent par des cybercriminels, car elle est facile à exécuter et peut produire les résultats recherchés sans avoir à fournir trop d'effort.

De quoi s'agit-il?

De faux courriels, messages texte et sites Web conçus pour avoir exactement la même apparence que ceux des entreprises réelles ou qui semblent être envoyé par de vraies entreprises. Les criminels les envoient pour vous voler votre information personnelle et financière. Ceci est connu sous le nom de « mystification ».

Quelles sont les conséquences?

Les différentes techniques également

- d'hameçonnage ont comme objectifs de vous inciter à fournir aux cybercriminels vos informations. Ces derniers vous demandent de mettre à jour, de valider ou de confirmer votre compte. Les méthodes sont souvent présentées de façons officielles et intimidantes pour vous encourager à prendre les mesures nécessaires.
- L'hameçonnage permet de fournir aux cybercriminels votre nom d'utilisateur et vos mots de passe afin qu'ils puissent accéder à vos comptes (compte bancaire en ligne, les comptes commerciaux, etc.) et voler vos numéros de carte de crédit.[4]

II.6. Les protocoles de sécurité

II.6.1.protocole SSL

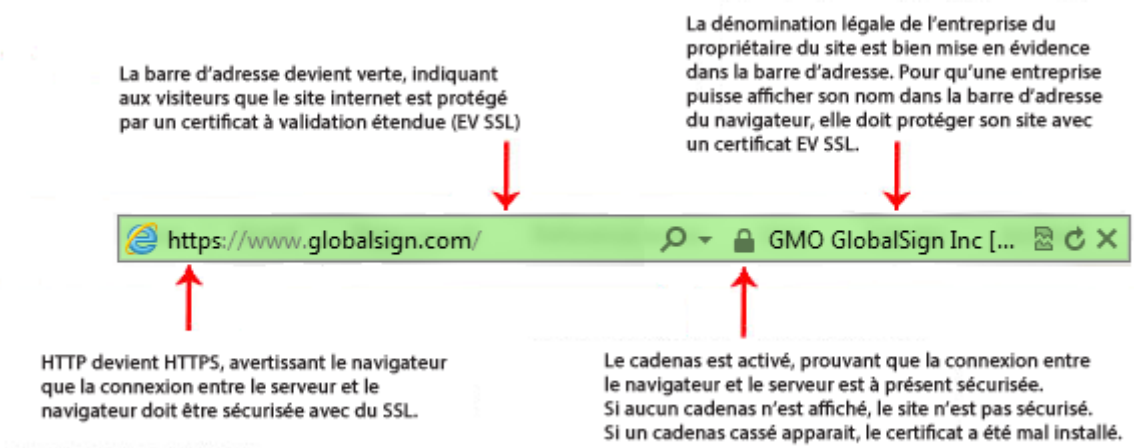
Le SSL (Secure Socket Layer) / TLS (Transport Layer Security) est le protocole de sécurité le plus répandu qui créé un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne. Dans notre société centrée sur un Internet vulnérable, le SSL est généralement utilisé lorsqu'un navigateur doit se connecter de manière sécurisée à un serveur web. (Voir figure II.2)

Figure II.2 : le SSL

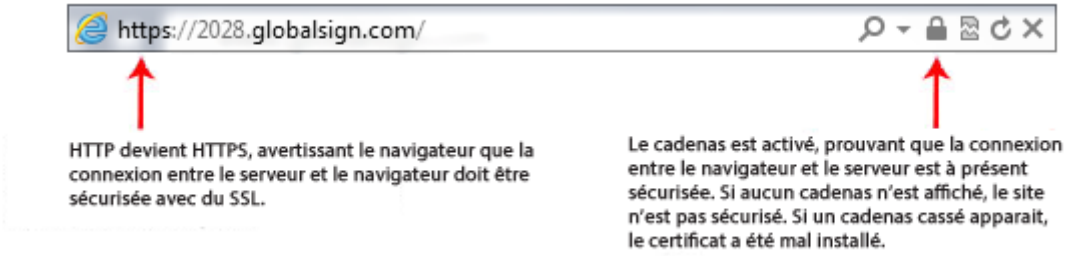
Techniquement parlant, le SSL est un protocole transparent qui nécessite peu d'interaction de la part de l'utilisateur final. Dans le cas des navigateurs, par exemple, les utilisateurs sont avertis de la présence de la sécurité SSL grâce à l'affichage d'un cadenas et du protocole « https » dans l'url (voir figure II.6.1.), et, dans le cas du SSL à validation étendue, par la barre d'adresse verte. La clé du succès du SSL est donc son incroyable simplicité pour l'utilisateur final.

Lire : bug Heartbleed - ce que vous devez savoir et notre réponse

Le certificat EV SSL (tel que GlobalSign ExtendedSSL) affiche des indicateurs visuels faciles à interpréter :



Les certificats SSL basiques (tels que les certificats GlobalSign DomainSSL et OrganizationSSL) affichent :



A l'inverse du « http » non sécurisé qui utilise le port 80 par défaut, le "https" sécurisé utilise le port 443.

« Http » est vulnérable face aux attaques d'individus ou d'organisations malveillantes qui tentent d'accéder à toute sorte d'information personnelle, telles que les informations bancaires et les informations de connexion. S'assurer que de telles informations soit envoyées au travers du protocole « http », c'est s'assurer que celles-ci seront chiffrées et protégées.

En pratique, le SSL devrait être utilisé dans les cas suivants :

- Pour sécuriser les transactions bancaires en ligne.
- Pour sécuriser les connexions et tout échange d'information confidentielle.
- Pour sécuriser les applications et les messageries web, telles que Outlook Web Access, Exchange et Office Communications Server.
- Pour sécuriser les flux de production et les applications de virtualisation tels que Citrix Delivery Platforms et les plates-formes sur le Cloud.
- Pour sécuriser les connexions entre un client de messagerie, tel que Microsoft Outlook et un serveur mail, tel que Microsoft Exchange.
- Pour sécuriser le transfert de fichiers au travers de services « https » et FTP, dans les cas de mise à jour de sites Internet par exemple.
- Pour sécuriser les connexions aux panneaux de contrôle et les activités d'hébergement, telles que Parallels, cPanel, et bien d'autres encore.
- Pour sécuriser les trafics intranet.
- Pour sécuriser les connexions aux réseaux et aux trafics de réseaux utilisant les VPNs SSL, tels que VPN Access Servers, et les applications, telles que Citrix Access Gateway.

II.6.2. Protocole SSH

Le protocole SSH (*Secure Shell*) a été mis au point en 1995 par le Finlandais Tatu Ylönen.

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

La version 1 du protocole (SSH1) proposée dès 1995 avait pour but de servir d'alternative aux sessions interactives (shells) telles que *Telnet*, *rsh*, *rlogin* et *rexec*. Ce protocole possédait toutefois une faille permettant à un pirate d'insérer des données dans le flux chiffré. C'est la raison pour laquelle en 1997 la version 2 du protocole (SSH2) a été proposée en tant que document de travail (*draft*) à l'IETF.

SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou *open source* : vous trouverez un certain nombre de clients SSH dans la section téléchargement de Comment Ca Marche.

Fonctionnement de SSH

L'établissement d'une connexion SSH se fait en plusieurs étapes :

- Dans un premier temps le serveur et le client s'identifient mutuellement

afin de mettre en place un canal sécurisé (couche de transport sécurisée).

- Dans un second temps le client s'authentifie auprès du serveur pour obtenir une session.

II.6.3.Protocole http

L'acronyme **HTTP** signifie *Hypertext Transfer Protocol* (traduction: protocole de transfert hypertexte). Ce protocole définie la communication entre un client (exemple: navigateur) et un serveur sur le World Wide Web (WWW).

Ce protocole inventé par Tim-Berner Lee au début des années 1990, fonctionne sur le principe "requête-réponse". En prenant un exemple commun, de communication entre un navigateur web (le client) et un serveur web, la communication se déroule de la manière décrite sur le schéma suivant (figure II.3).

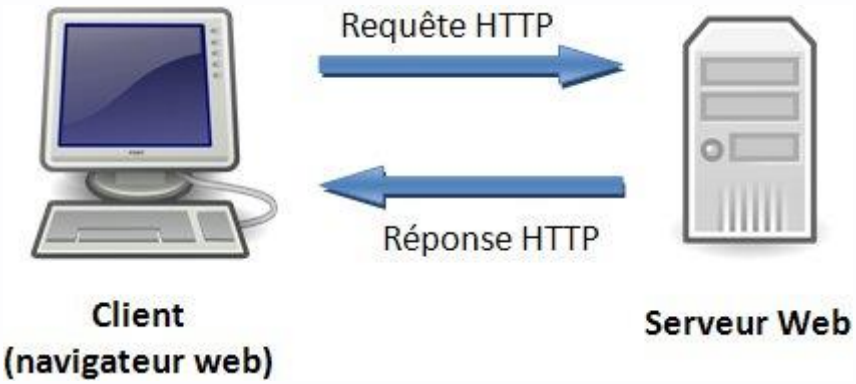


Figure II.3.Schéma d'une requête http

L'ordinateur de l'internaute utilise le navigateur pour envoyer une requête à un serveur web. Cette requête demande un document (exemple: page HTML, image, fichier CSS ...). Le serveur cherche les informations, puis il est peut-être amené à interpréter les résultats (exemple: PHP, Java ...), pour finalement envoyer la réponse. Cette réponse contient les entêtes du protocole HTTP et normalement le contenu demandé.

II.6.4.Protocole S-http

S-HTTP (*Secure HTTP*, ce qui signifie *Protocole HTTP sécurisé*) est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP mise au point en 1994 par l'EIT (*Enterprise Integration Technologies*). Il permet de fournir une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle. Une implémentation de S-HTTP a été développée par la

société *Terisa Systems* afin d'inclure une sécurisation au niveau des serveurs web et des navigateurs.

II.6.4.1.Fonctionnement de S-HTTP

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

Les messages S-HTTP sont basés sur trois composantes :

- Le message HTTP
- Les préférences cryptographiques de l'envoyeur
- Les préférences du destinataire

Ainsi, pour décrypter un message S-HTTP, le destinataire du message analyse les en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message. Puis, grâce à ses préférences cryptographiques actuelles et précédentes, et aux préférences cryptographiques précédentes de l'expéditeur, il est capable de déchiffrer le message.

II.6.5.Le protocole IPSEC

Pour sécuriser les échanges ayant lieu sur un réseau TCP/IP, il existe plusieurs approches :

- niveau applicatif (PGP) ;
- niveau transport (protocoles TLS/SSL, SSH) ;
- niveau physique (boîtiers chiffrants).

IPsec vise à sécuriser les échanges au niveau de la couche réseau. Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitant encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPSec pour IP Security Protocols.

Le protocole IPSec fournit ainsi :

- des mécanismes de confidentialité et de protection contre l'analyse du trafic ;
- des mécanismes d’authentification des données (et de leur origine) ;

- des mécanismes garantissant l'intégrité des données (en mode non connecté) ;
- des mécanismes de contrôle d'accès.

IPsec est une extension de sécurité pour le protocole IP.

II.7. Les méthodes de protection

II.7.1.Logiciels antivirus

Un logiciel antivirus est un programme ou un ensemble de programmes qui sont conçu chercher, détecter et supprimer les virus sur un système ou un réseau informatique, si il est régulièrement mis à jour et correctement entretenu La plupart du logiciel antivirus comprend une fonction d'auto mise à jour qui permet de télécharger les signatures des nouvelles menaces découvertes.

II.7.2.Le chiffrement

Le **chiffrement** ou **cryptage** est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel.

Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre. Pour vérifier l'intégrité ou l'authenticité d'un document, on utilise respectivement un *Message Authentication Code (MAC)* ou une signature numérique. On peut aussi prendre en considération l'analyse de trafic dont la communication peut faire l'objet, puisque les motifs provenant de la présence de communications peuvent faire l'objet d'une reconnaissance de motifs. Pour rendre secrète la présence de communications, on utilise la stéganographie. La sécurité d'un système de chiffrement doit reposer sur le secret de la clé de chiffrement et non sur celui de l'algorithme. Le principe de Kerckhoffs suppose en effet que l'ennemi (ou la personne qui veut déchiffrer le message codé) connaisse l'algorithme utilisé.

II.7.2.1.Le cryptage symétrique

Egalement appelé cryptage à clé privé ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux partie communicantes. Cette même clé sert à crypter et décrypter les messages.

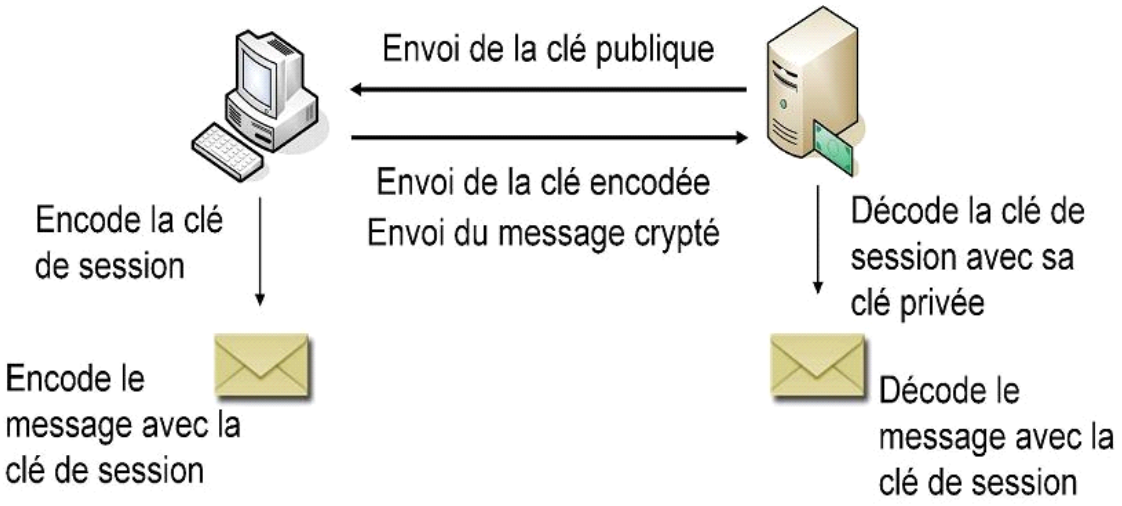


Figure II.4 Le cryptage symétrique

II.7.2.2.Le cryptage asymétrique

Quand il utilise des clés différentes : une paire composée d'une *clé publique*, servant au chiffrement, et d'une *clé privée*, servant à déchiffrer. Le point fondamental soutenant cette décomposition publique/privée est l'impossibilité calculatoire de déduire la clé privée de la clé publique.

Appelé aussi à clé publique est une méthode de chiffrement qui repose sur l'utilisateur d'une clé publique qui est diffusée et d'une clé privée, l'une permettant de coder le message et l'autre pour le coder.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

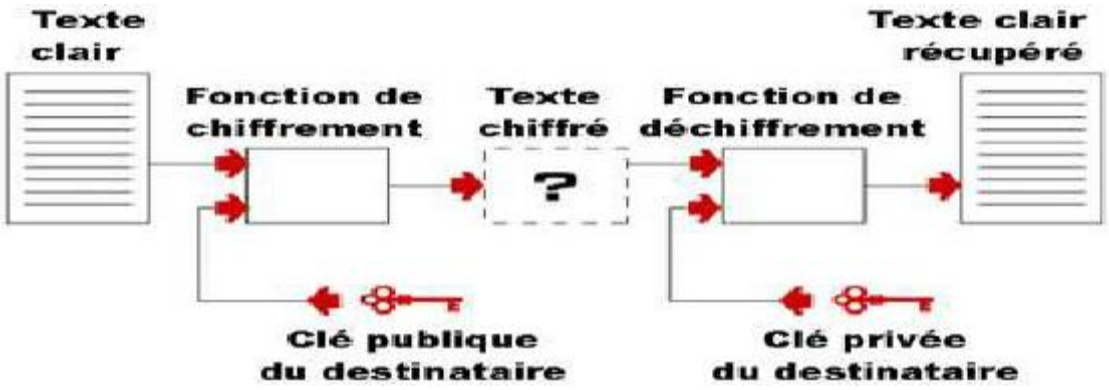


Figure II.5 le cryptage asymétrique

II.7.3.L'authentification

L'authentification pour un système informatique est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité (être humain ou un autre système...) afin d'autoriser l'accès de cette entité à des ressources du système (systèmes, réseaux, applications…)[1] conformément au paramétrage du contrôle d'accès . L'authentification permet donc, pour le système, de valider la légitimité de l'accès de l'entité, ensuite le système attribue à cette entité les données d'identité pour cette session (ces attributs sont détenus par le système ou peuvent être fournis par l'entité lors le processus d'authentification). C'est à partir des éléments issus de ces deux processus que l'accès aux ressources du système pourra être paramétré (contrôle d'accès).

Il existe quatre facteurs d'authentification classiques qui peuvent être utilisés dans le processus d'authentification d'un commettant :

- utiliser une information que seul le commettant connaît (ce que l'on connaît);
- utiliser une information unique que seul le commettant possède (ce que l'on possède);
- utiliser une information qui caractérise le commettant dans un contexte donné (ce que l'on est);
- utiliser une information que seul le commettant peut produire (ce que l'on sait faire).

II.7.4.Certificats numériques

Est un document numérique permettant de valider le lien entre une signature électronique et son signataire.

Les certificats numériques sont généralement utilisés à des fins d'identification, lors de l'établissement de tunnels sécurisés sur Internet, comme c'est le cas dans les réseaux virtuels privés(VPN) et sont émis par une autorité de certification.

II.7.5.System de détection d'intrusion

La détection d'intrusion est un processus de découverte et d'analyse de comportements hostiles dirigés contre un réseau

Le but de la détection d'intrusion est d'apporter une aide complémentaire aux pare-feux et à l'administrateur à se prémunir contre les attaques et intrusions en tout genre.

Un système de détection d'intrusions (IDS, de l'anglais Intrusion Detection System) est un périphérique ou processus actif qui analyse l'activité du système et du réseau pour détecter toute entrée non autorisée et / ou toute activité malveillante. La manière dont un IDS détecte des anomalies peut beaucoup varier ; cependant, l'objectif principal de tout IDS est de prendre sur le fait les auteurs avant qu'ils ne puissent vraiment endommager vos ressources.

Les IDS protègent un système contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du système et du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus. Selon les méthodes de détection que vous choisissez de déployer, il existe plusieurs avantages directs et secondaires au fait d'utiliser un IDS.

II.7.6.L'audit de sécurité informatique

C'est l'opération à effectuer avant de proposer et de contrôle des moyens de prévention des risques informatiques.

Un audit de sécurité est une mission d'évaluation de conformité de sécurité

II.7.7. Pare-feu

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

Contrôler le trafic sortant d'un réseau, et notamment éviter que les utilisateurs accèdent à certains nœuds du réseau.

Sécuriser le trafic entrant d'un réseau, et empêcher certains nœuds extérieurs de se connecter un réseau local.

Enfin, pour une question de **vigilance**, et éviter que certains machines mal configurées du réseau local n'envoient des données vers l'extérieur.

L e firewall ainsi défini permet de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

· Une interface pour le réseau à protéger (réseau interne).

· Une interface pour le réseau externe

II.8. Les VPN

VPN : Virtual Private Network ou RPV (réseau privé virtuel) en français est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique.

Schéma d'un accès VPN (figure II.6):

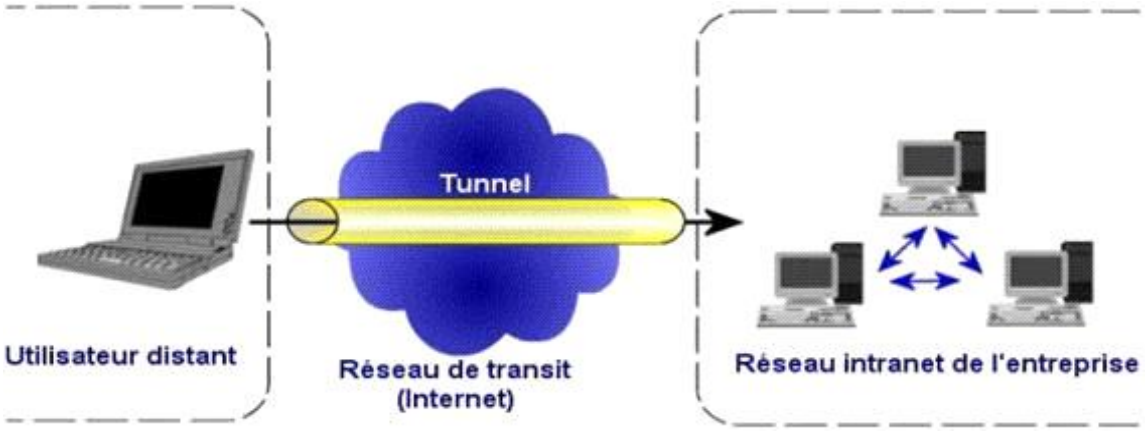


Figure II.6. : Réseau privé virtuel

II.8.1. Principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé « protocole de tunneling ».Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation.

Les principaux avantages d'un VPN :

- Sécurité : assure des communications sécurisées et chiffrées.
- Simplicité : utilise les circuits de télécommunication classiques.
- Economie : utilise Internet en tant que média principal de transport, ce qui évite les couts liés à une ligne dédiée.

II.8.2. Les contraintes d'un VPN :

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- Authentification d utilisateur : seule les utilisateurs autorisés doivent avoir accès au canal VPN.
- Cryptage des données : lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.
- Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

II.8.3. Les différents types de VPN

Suivant les besoin, on distingue trois types de VPN :

- **Le VPN d accès :** il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.
- **L intranet VPN :** il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants)
- **L extranet VPN :** une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces demies. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une rigoureuse des espaces d'échange.

II.9. Les VLAN

Un VLAN (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau Local Virtuel*) est un réseau local virtuel est un regroupement virtuel d'au moins deux périphériques.

Ce regroupement virtuel peut s'étendre au-delà de plusieurs commutateurs. Les périphériques sont regroupés sur la base d'un certain nombre de facteurs suivant la configuration du réseau.

Le VLAN permet de crées des domaines de diffusion (domaines de broadcast) gérés par les indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement.

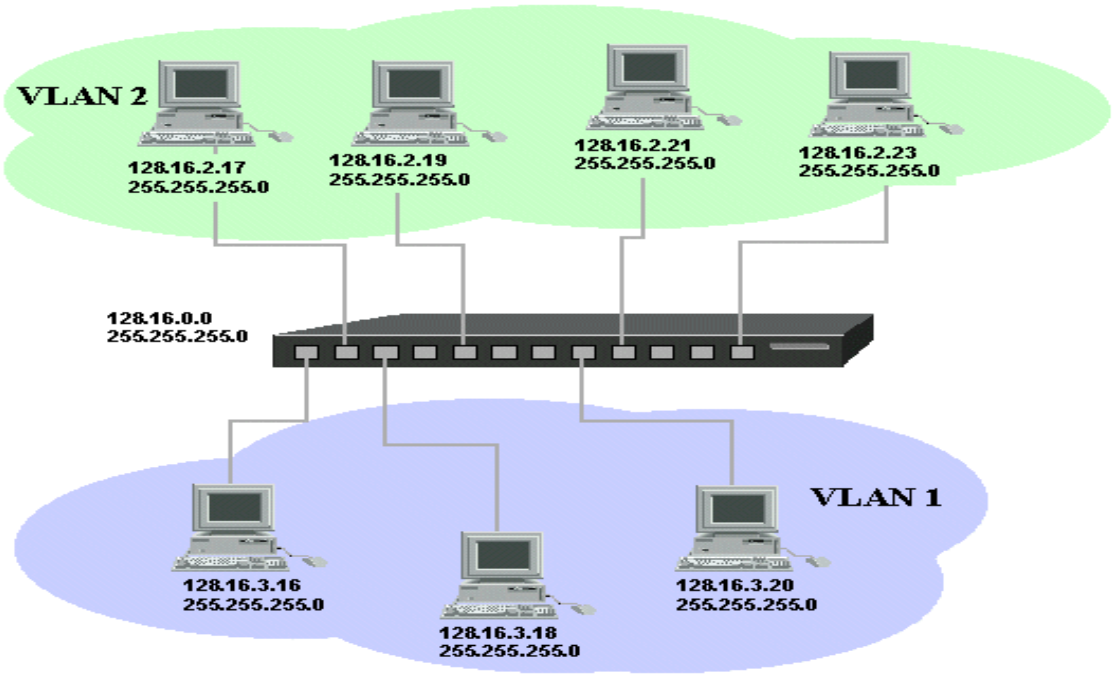


Figure II.7. : VLAN

II.9.1.Types de VLAN

II.9.1.1. VLAN niveau 1

Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais *Port-Based VLAN*) définit un réseau virtuel en fonction des ports de raccordement sur le Switch ou commutateur.

Dans le cadre des réseaux VLAN basés sur les ports, l'appartenance de chaque port du commutateur à tel ou tel réseau VLAN est configurée manuellement.

II.9.1.2. VLAN niveau 2 à L2

Un VLAN de niveau 2 (également appelé VLAN MAC, *VLAN par adresse IEEE* ou en anglais *MAC Address-Based VLAN*) consiste à définir un réseau virtuel en fonction des

adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

Chaque adresse MAC est affectée à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En effet il s'agit, à partir de l'association MAC/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapter à l'utilisation de machines portables). Si on veut changer de vlan il faut modifier l'association Mac /Vlan

II.9.1.3. VLAN niveau 3 à L3 réseaux VLAN basés sur les protocoles

Un VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 :

Le VLAN par sous-réseau (en anglais *Network Address-Based VLAN*) associe des sous réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

Le VLAN par protocole (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN. Cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles, mais n'est pas très pratique sur un réseau à prédominance IP.

II.10.Les services réseau

II.10.1. Le serveur web (http)

Le serveur http est un logiciel prenant en charge les requêtes client-serveur des protocoles http qu'il reçoit et fournit une réponse dans ce même protocole. Apache est le

serveur http le plus répondu sur internet. Ce dernier, permet en effet d'ajouter des modules supplémentaires qui enrichissent le serveur en termes de fonctionnalité.

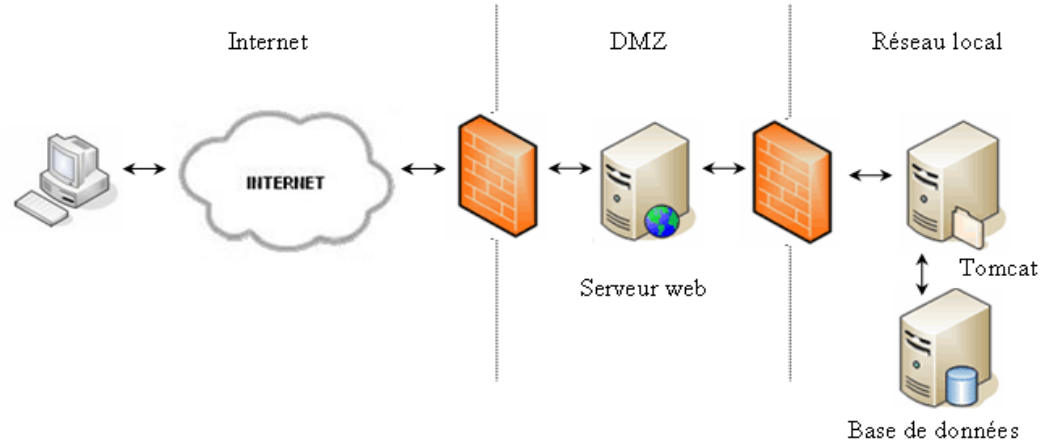


Figure II.8. Le serveur Web

II.10.2. le serveur DNC

Le serveur DNC signifiant Domain Name Service est né de la volonté de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatique tels que l'internet

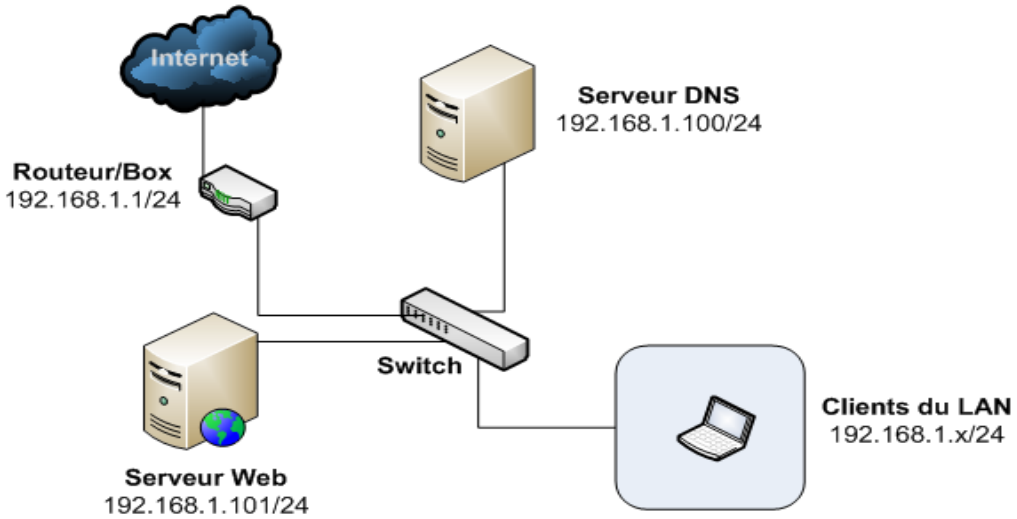


Figure II.9. Serveur DNS

II.10.3. Serveur DHCP

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

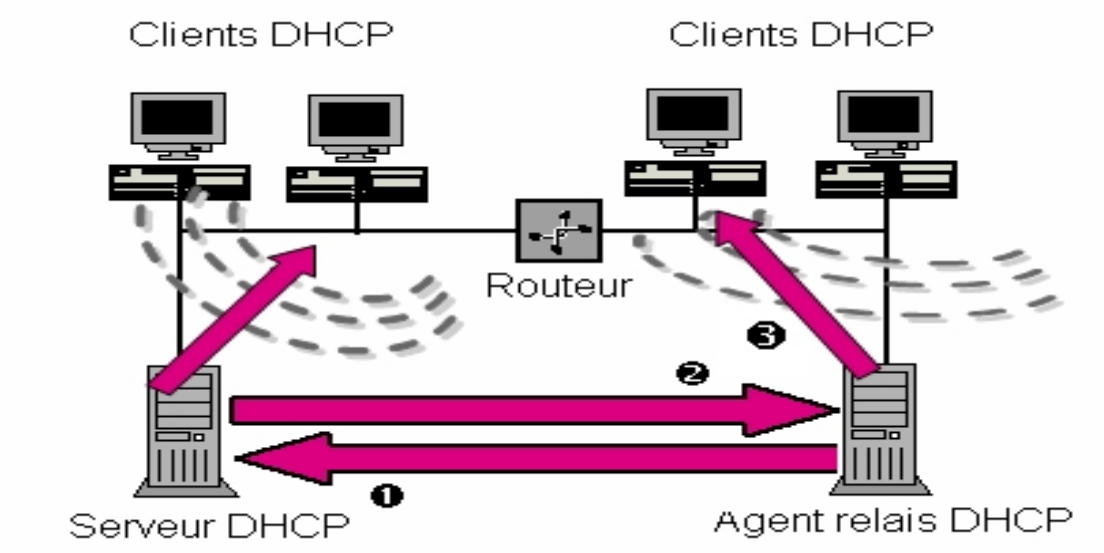


Figure II.10. Serveur DHCP

II.10.4.Le serveur Proxy

Un serveur proxy est un paquetage logiciel et/ou matériel qui permet de mettre en cache des pages Web. Il s'agit en général d'un ordinateur du réseau local à deux interfaces réseau : l'une servant à l'accès Internet, l'autre menant au réseau local. Le serveur proxy traite les requêtes Web des ordinateurs du réseau local : lorsqu'un ordinateur du réseau local émet une requête HTTP, la requête est récupérée par le serveur proxy, le serveur cherche si la page est déjà présente dans le cache (ce qui élimine le temps du chargement) et sinon est retransmise avec l'adresse publique.

Figure II.11.serveur Proxy

III.12. Présentation des logicielles

III.12.1.Windows server 2012

Microsoft Windows Server 2012 est conçu pour fournir aux entreprises la plate-forme la plus productive pour virtualiser les charges les charges de travail en utilisant la virtualisation Microsoft intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web.

Figure II.13: Server Windows

III.12.2.Active directory

Est un *annuaire* au sens informatique et technique chargé de répertorier tout ce qui touche au réseau comme le nom des utilisateurs, des imprimantes, des serveurs, des dossiers partagés, etc. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées.
Il est possible d'interroger l'annuaire pour obtenir une liste des objets possédant des attributs.

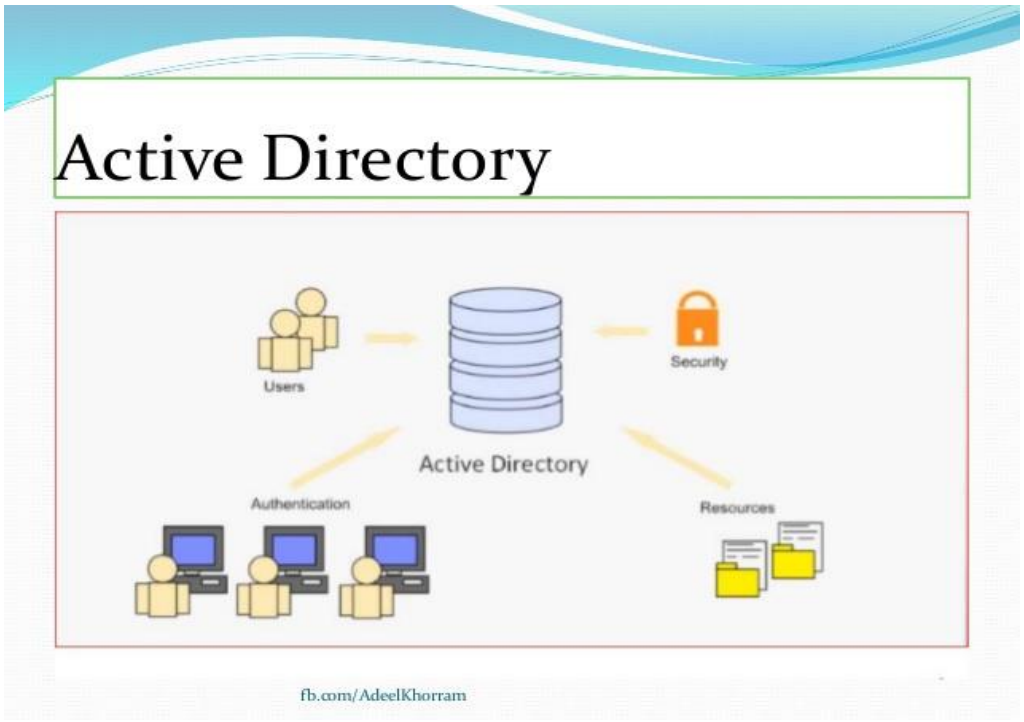


Figure II.14 : Active directory

III.13.RADIUS

Le protocole **RADIUS** (*Remote Authentication Dial-In User Service*), mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC.

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il s'agit du protocole de prédilection des fournisseurs d'accès à internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé **NAS** (*Network Access Server*), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé.

Il est à noter que le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.

III.13.1.Fonctionnement de RADIUS

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion distance ;
- Le NAS achemine la demande au serveur RADIUS ;
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
    - **ACCEPT** : l'identification a réussi ;
    - **REJECT** : l'identification a échoué ;
    - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « *challenge* ») ;

Il existe une réponse appelée **CHANGE PASSWORD** où le serveur RADIUS demande à l'utilisateur un nouveau mot de passe. Change-Password est un attribut VSA (Vendor-Specific Attributes), c'est-à-dire qu'il est spécifique à un fournisseur, et dans ce cas, c'est un attribut de Microsoft et pour être plus précis, celui de MS-Chap v2. Il n'appartient pas aux attributs radius standard définis dans la RFC 2865.

Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

Le schéma suivant récapitule les éléments entrant en jeu dans un système utilisant un serveur RADIUS :

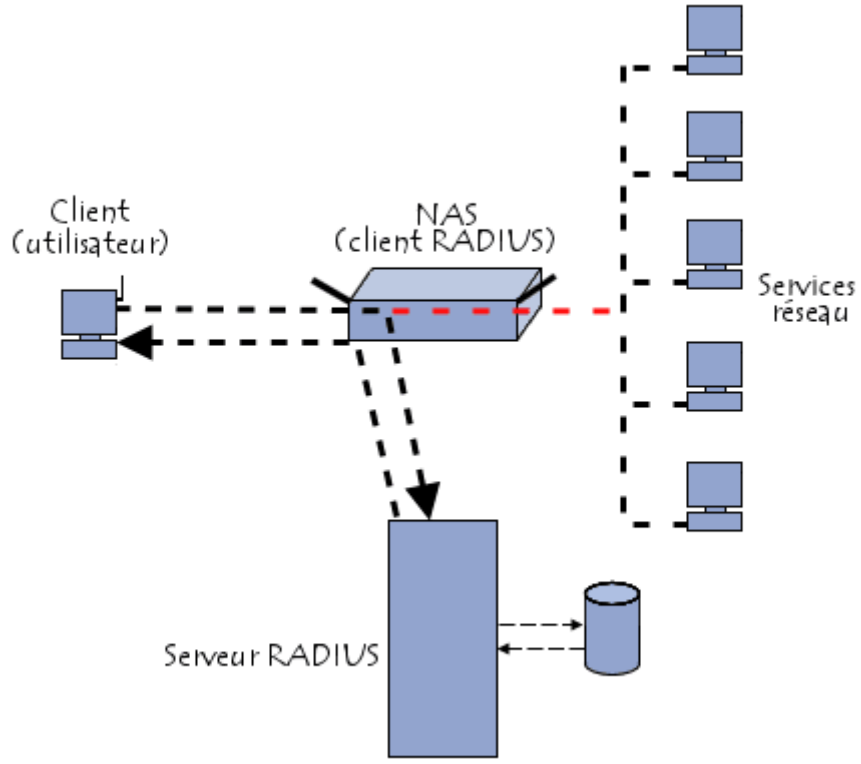


Figure II.15 : RADIUSE

III.14.La zone Démilitarisée (DMZ)

III.14.1.Définition de la DMZ

DMZ zone démilitarisée est une utilisation particulière d'un ou deux firewalls hardwares (pare feu) ceci permet de connecter un serveur sur deux réseaux à la fois mais de bloquer l'accès entre les deux réseaux. L'ordinateur est typiquement un serveur internet partagé entre un réseau local et internet .le DMZ empêchant l'accès des visiteurs internet vers le réseau interne.

III.14.2.Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « **zone démilitarisé** » (notée **DMZ**) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

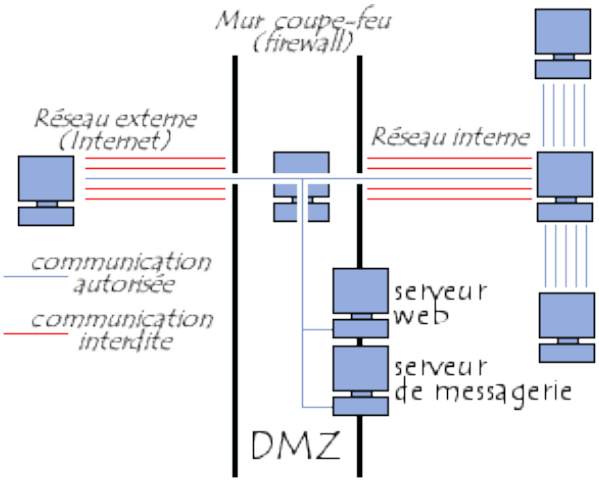


Figure II.16 : DMZ

Les serveurs situés dans la DMZ sont appelés « **bastions** » en raison de leur position d'avant poste dans le réseau de l'entreprise.

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

- Traffic du réseau externe vers la DMZ **autorisé** ;
- Traffic du réseau externe vers le réseau interne **interdit** ;
- Traffic du réseau interne vers la DMZ **autorisé** ;
- Traffic du réseau interne vers le réseau externe **autorisé** ;
- Traffic de la DMZ vers le réseau interne **interdit** ;
- Traffic de la DMZ vers le réseau externe **refusé**.

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

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

III.14.3.Fonctionnement d'un firewall avec zone démilitarisée :

Le firewall a pour fonction de surveiller les trames passant sur le réseau et de les bloquer ou de les laisser passer. Le firewall se place entre la couche physique (norme ODI) et la couche protocole. Il décide de laisser passer ou non une trame en fonction de sa source, de sa destination, et des règles d'approbation définies dans sa table de règles.

La configuration la plus rependue pour un réseau connecté à Internet est une configuration avec firewall et zone démilitarisée (DMZ). Un firewall est placé entre Internet, le réseau local LAN, et une zone spéciale appelée DMZ, qui contient serveurs Web, Extranets, FTP, etc…, qui doit pouvoir être accédée d'Internet et du LAN local. La DMZ est une sorte de zone tampon entre l'extérieur et le réseau interne:

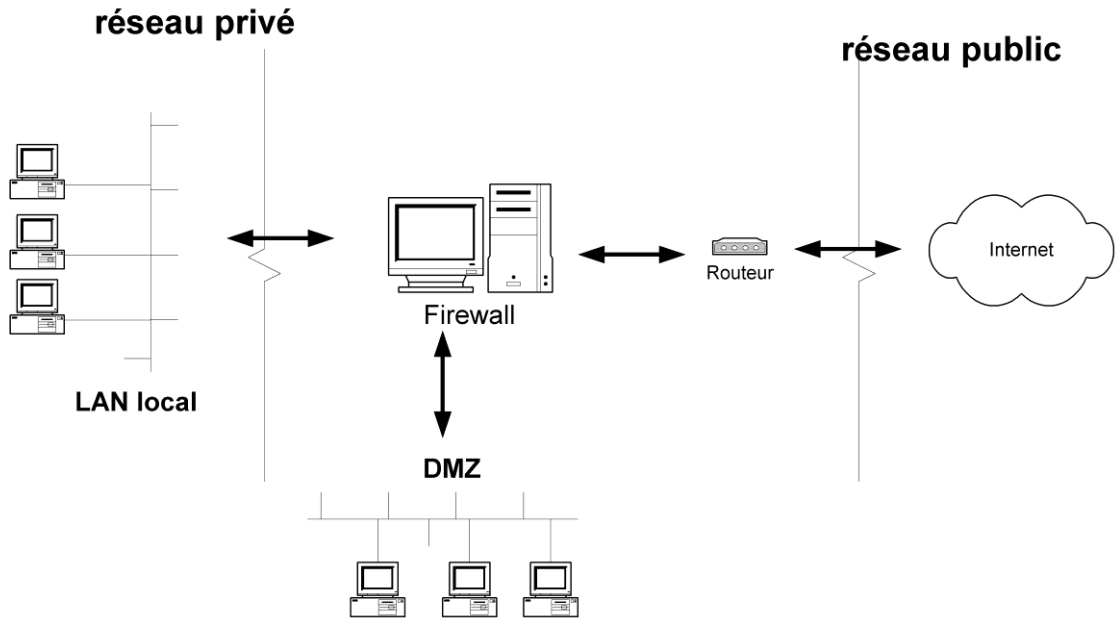


Figure II.17 : DMZ

Le firewall permet alors de filtrer les trames et de les diriger vers telle ou telle zone en fonction des règles internes définies par les administrateurs.

III.15. Le chargement de l'ASDM

Avant toute chose, il faut charger et configurer la version de l'ASDM. Pour cela, démarrer votre serveur TFTP sur votre ordinateur. Configurez le répertoire de travaille de votre serveur pour faire en sorte que l'ASDM soit disponible.

Retournez ensuite dans la console de l'ASA et saisissez la commande suivante :

 # copy tftp flash:/nom_de_votre_image_ASDM

Ensuite, il faut préciser que vous utiliserez cette version en saisissant la commande suivante :

 # asdm image nom_de_votre_image_ASDM

Puis configurer le serveur HTTP qui exécutera l'ASDM via les commandes suivantes :

 # http server enable

 # http 172.16.99.0 255.255.255.0 WAN

La dernière commande permet d'autoriser l'accès à l'ASDM depuis le WAN.

Pour pouvoir vous connecter à l'ASDM, vous devez configurer un compte, comme suit :

 # user nom-de-l'utilisateur password mot_de_passe

Pour tester cet accès en ouvre un navigateur sur l'ordinateur et en saisissant l'adresse d' ASA, dans cet exemple il s'agit de https://172.16.99.254. Et en obtiens la page suivante :

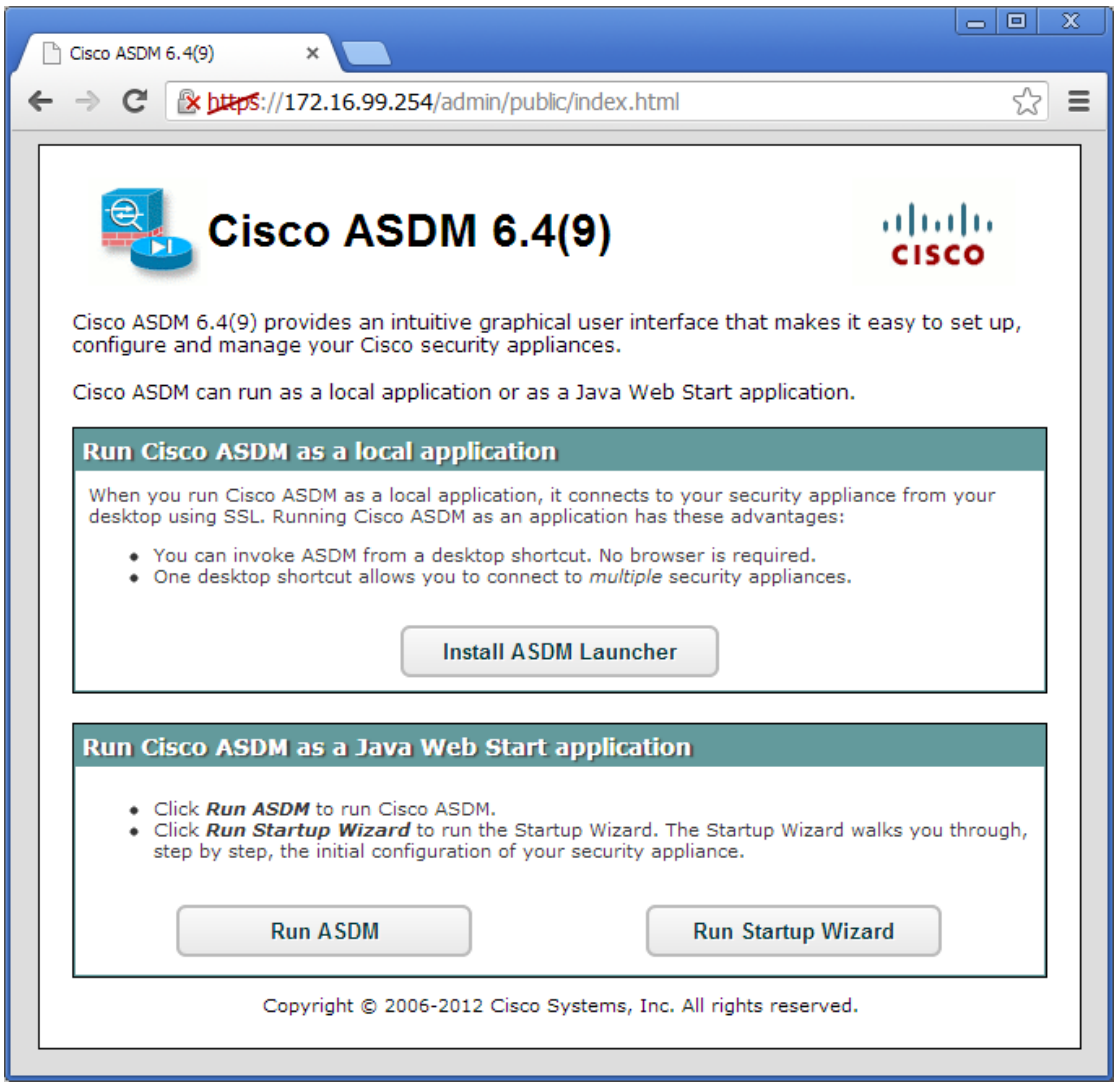


Figure II.18. Installation de l'ASDM

Cliquez sur **Run ASDM**

Le navigateur va procéder au téléchargement d'un plug-in java. Une fois téléchargé, on cliquer dessuspour le "lancer".

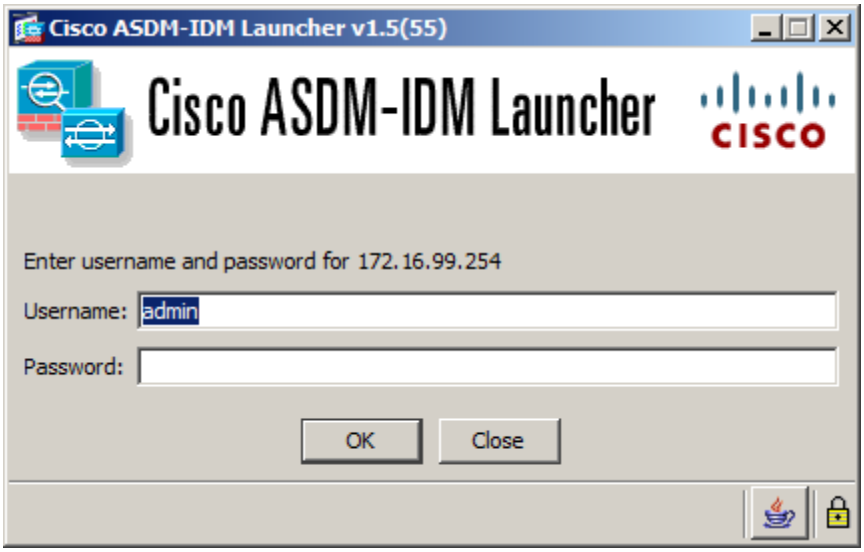


Figure II.19 : L'authentification de l'utilisateur.

Saisir **les identifiants** créés précédemment. Et voilà le client ASDM est démarré :

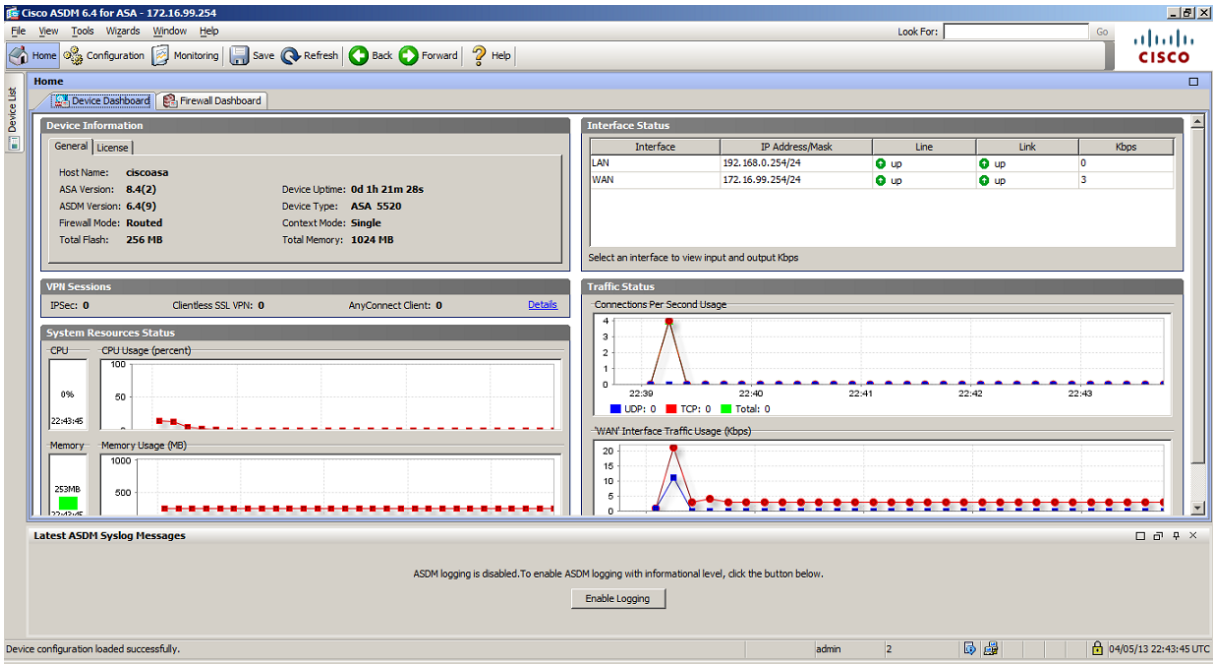


Figure II.20. Le menu Home de l'interface ASDM

II.16.Discussion

Dans ce chapitre nous avons présenté quelques définitions sur la sécurité des systèmes d'information. Elle représente aujourd'hui une tâche de fond à prendre en compte par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent et assurent la gouvernance de son système d'information. Ainsi plusieurs méthodes d'analyse des systèmes informatiques proposent des démarches de certification afin de garantir une image pérenne aux entreprises intégrant les processus de sécurité dans la liste de leur préoccupation managériale.

III.1.Préambule

De nos jours, toutes les entreprises possédant un réseau local qui ont 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. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise.

Et pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un firewall et de mieux un firewall matériel qui propose 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 et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données.

Le but de ce chapitre est de présenter un plan de sécurité pour l'appliquer au niveau du réseau de l'entreprise. Nous allons présenter le réseau existant et ses critiques ainsi qu'on va présenter une solution pour mieux sécuriser se réseau qui sont les services de sécurités adaptatifs Cisco ASA qui permet aux administrateurs de mieux segmenter le trafic réseau et de créer des zone de sécurité séparées.

Partie 1 Etude de réseau existant

III.2.Etude de l'architecture de réseau de départ. (Existant)

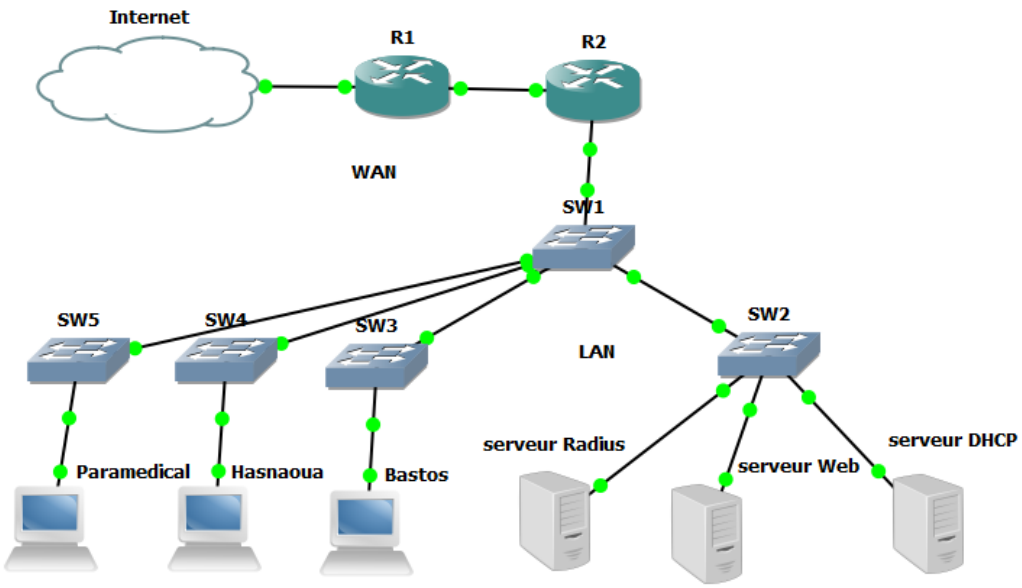


Figure III.1. Architecture de réseau existant

III.3.Les critiques du réseau existant

Critique 1 : le réseau est installé anarchiquement et non administré.

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

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

Critique 4 : l'absence de VLANs (augmentation du trafic réseau).

Critique 5 : le serveur DHCP n'est pas sécurisé (les attaques de DHCP spoofing).

Critique 6 : Manques firewall pour sécuriser l'accès (DMZ, ACL, zone base firewall).

Critique 7 : Le manque de sécurité au niveau de port de Switch (les attaques par « mac flooding » et les attaque « man in the middle ».

III.4.Solution proposé

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

Ø Administration et ordonnancement du réseau local.

Ø Configuration d'un firewall (ASA 5510).

Et pour améliorer le parc informatique on a mit en place des VLANs séparons les réseaux (bastos, Hasnaoua, paramédical) et Sécuriser les ports des Switch.

III.4.1.Nouvelle architecture en utilisant le pare-feu ASA

L'architecture du réseau avec les solutions proposées dans ce plan de sécurité est présentée par la figure III.2 :

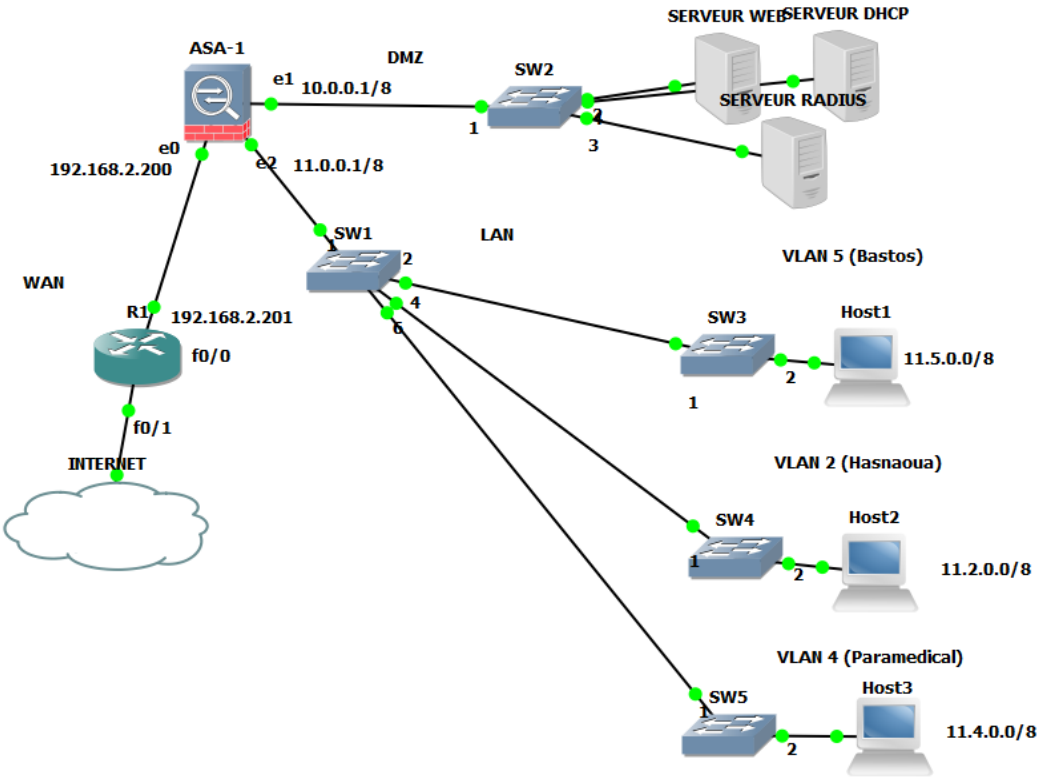


Figure III.2 : Nouvelle architecture en utilisant le pare-feu ASA Cisco

III.5.Présentation du matériel

III.5.1.Les Routeurs Cisco

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

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

III.5.2.Les Switch Cisco (CATALYST Cisco)

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

Ces caractéristiques sont :

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

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

III.6. Présentation de la gamme Cisco ASA 5500

La gamme Cisco ASA 5500 inclut les boitiers de sécurité adaptatifs Cisco ASA 5505, 5510, 5520 et 5540.

Il s'agit de quatre serveurs de sécurité ultra-performante issue de l'expertise de Cisco Système en matière de développement de solutions de sécurité et VPN reconnues et leaders sur leur marché. Cette gamme utilise les dernières technologies des serveurs de sécurité Cisco PIX 500, des capteurs Cisco IPS 4200 et des concentrateurs Cisco VPN 3000.

Conçue comme l'élément principal de la solution Self-Defending Network de Cisco (réseau qui se défend tout seul), 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.

III.7.Description des Serveurs de Sécurité Adaptatifs de la gamme Cisco ASA 5500

Les Serveurs de Sécurité Adaptatifs Cisco® ASA 5500 combinent les meilleurs services de

VPN et de sécurité, et l'architecture évolutive AIM (Adaptive Identification and Mitigation), pour constituer une solution de sécurité spécifique. Conçue comme l'élément principal de la solution Self-Defending Network de Cisco (le réseau qui se défend tout seul), 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 des PME/PMI 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.

Réunissant sur une même plate-forme une combinaison puissante de nombreuses technologies éprouvées, la gamme Cisco ASA 5500 vous donne les moyens opérationnels et économiques de déployer des services de sécurité complets vers un plus grand nombre de sites. La gamme complète des services disponibles avec la famille Cisco ASA 5500 permet de répondre aux besoins spécifiques de chaque site grâce à des éditions produits conçues pour les

PME comme pour les grandes entreprises. Ces différentes éditions offrent une protection de qualité supérieure en apportant à chaque installation les services dont elle a besoin. Chaque édition de la gamme Cisco ASA 5500 regroupe un ensemble spécialisé de services – firewall, VPN SSL et IPSec, protection contre les intrusions, services Anti-X ,,, etc. qui répondent exactement aux besoins des différents environnements du réseau d'entreprise.
Et lorsque les besoins de sécurité de chaque site sont correctement assurés, c'est l'ensemble de la sécurité du réseau qui en bénéficie.

III.8.Principes avantages technologiques et nouveautés de la gamme ASA 5500

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

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

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

- **Services évolué de prévention des intrusions**

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

- **Services anti-x à la pointe de l'industrie**

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

- **Services multifonctions de gestion et de surveillance**

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

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

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

III.9.Principe de fonctionnement d'ASA

L'ASA offre deux modes pour ses utilisateurs :

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

Le mode transparent est de niveau 2 : il facilite la configuration du réseau et permet de cacher le pare-feu (aux intrus éventuels).

On utilise aussi le mode transparent pour autoriser le trafic qui est bloqué par un routeur en utilisant les ACLs. Par défaut, l'ASA est en mode routed.

III.10.Les fonctionnalités d'ASA

III.10.1.ACL (Access Control Lists)

Cette publication vise à comprendre comment ACL fonctionne sur Cisco ASA Firewalls.

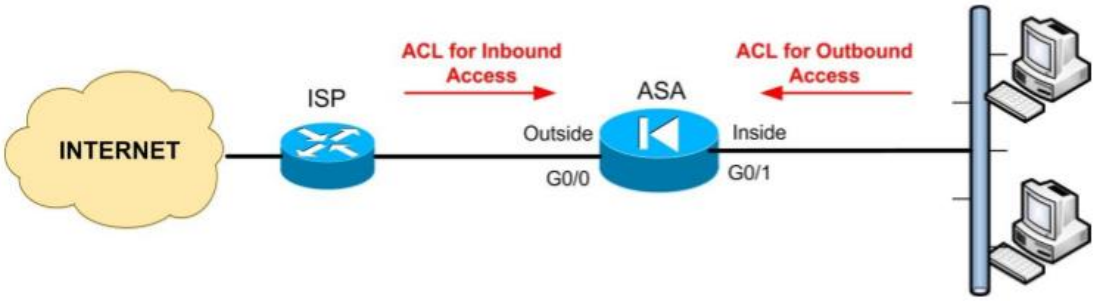


Figure III.3. : ACL

Les ACL permettent de filtrer les accès entre les différents réseaux ou de filtrer les accès au routeur lui même.

Les paramètres contrôlés sont:

- Adresse source
- Adresse destination
- Protocole utilisé
- Numéro de port

Les acls peuvent être appliquées sur le traffic entrant ou sortant. Il y a deux actions: soit le trafic est interdit, soit le traffic est autorisé.
Les ACLs sont prises en compte de façon séquentielle. Il faut donc placer les instructions les plus précises en premier et l'instruction la plus générique en dernier.
Par défaut, tout le trafic est interdit.

- ✓ **Différence entre les acls standards et étendues**

➢ **L'ACL standard** filtre uniquement sur les adresses IP sources. Elle est de la forme: **access-list numéro-de-la-liste {permit|deny} {host|source source-wildcard|any}**
Le numéro de l'acl standard est compris entre 1 et 99 ou entre 1300 et 1999.

➢ **L'ACL étendue** filtre sur les adresses source et destination, sur le protocole et le numéro de port.

Elle est de la forme: access-list numéro de la liste {deny|permit} protocole source masque-source [operateur [port]] destination masque-destination [operateur [port]][established][log]
Quelques opérateurs:

- eq : égal
- neq : différent
- gt : plus grand que
- lt : moins grand que

III.11.NAT Translation d'adresses

Principe du NAT

Le mécanisme de translation d'adresses (en anglais *Network Address Translation* noté NAT) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6répondra à terme à ce problème).
En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.

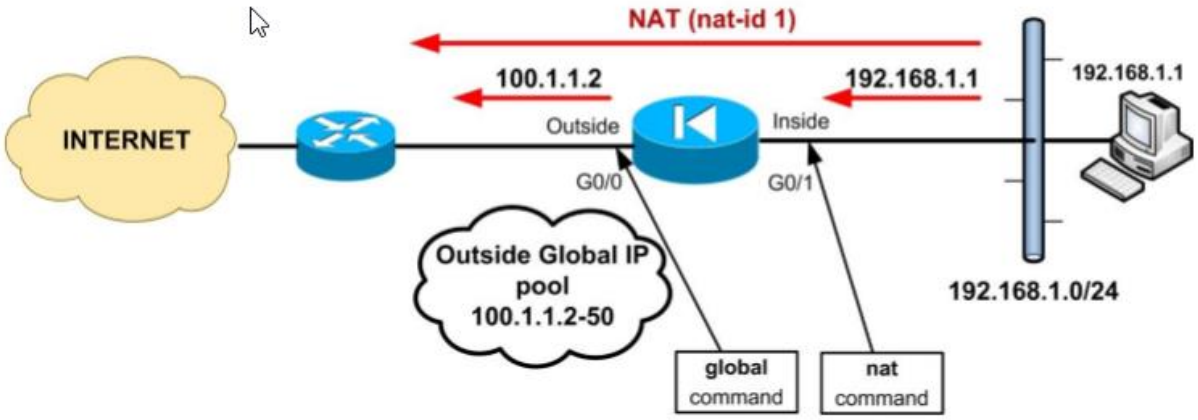


Figure III.4 : NAT

Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.

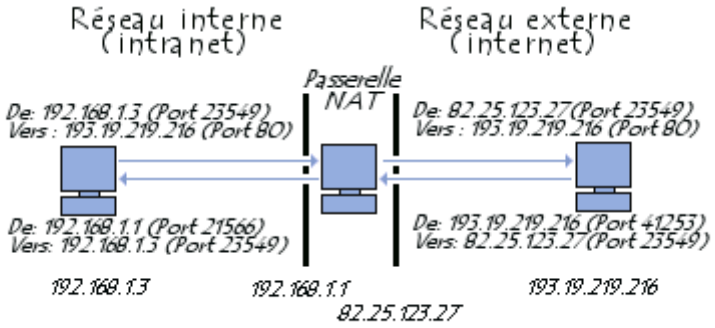


Figure III.5 : La passerelle NAT

D'autre part, le mécanisme de translation d'adresses permet de **sécuriser** le réseau interne étant donné qu'il camoufle complètement l'adressage interne. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de la même adresse IP.

Espaces d'adressage

L'organisme gérant l'espace d'adressage public (adresses IP routables) est l'*Internet Assigned Number Authority* (**IANA**). La RFC 1918 définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque

d'entrer en conflit avec une adresse IP publique allouée par l'IANA. Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :

- Classe A : plage de 10.0.0.0 à 10.255.255.255 ;
- Classe B : plage de 172.16.0.0 à 172.31.255.255 ;
- Classe C : plage de 192.168.0.0 à 192.168.255.55 ;

Toutes les machines d'un réseau interne, connectées à internet par l'intermédiaire d'un routeur et ne possédant pas d'adresse IP publique doivent utiliser une adresse contenue dans l'une de ces plages. Pour les petits réseaux domestiques, la plage d'adresses de 192.168.0.1 à 192.168.0.255 est généralement utilisée.

➢ **Translation statique**

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple *192.168.0.1*) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où *n* adresses IP routable sont nécessaires pour connecter *n* machines du réseau interne.

➢ **Translation dynamique**

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP. C'est la raison pour laquelle le terme de « **mascarade IP** » (en anglais *IP masquerading*) est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.

III.12.PAT (Port Address Translation) ou Overoading

Le Port Address Translation vient complémenter le NAT. En effet, supposant que nous ne disposants pas d'adresse IP publique suffisante pour toutes nos machines locales, il va donc falloir partager réutiliser nos adresses.

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

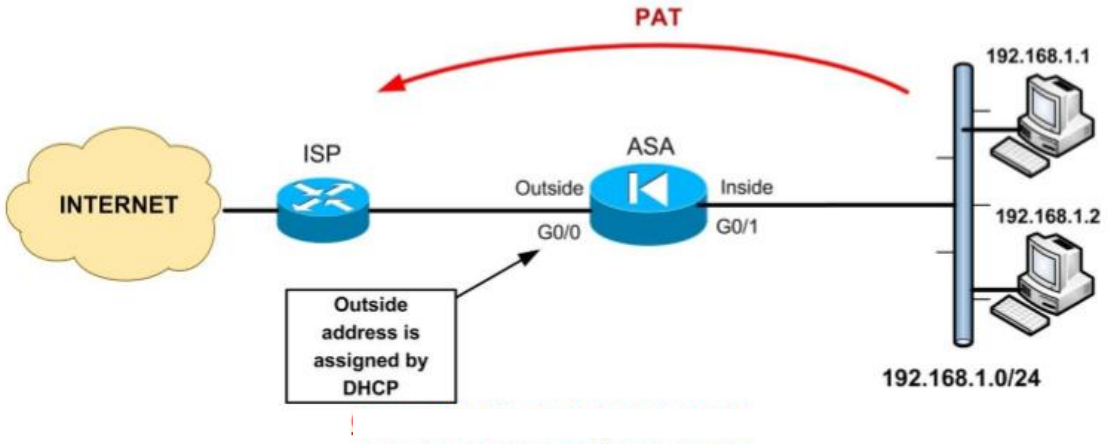


Figure III.6 : PAT

III.13.Serveur de sécurité adaptatif CISCO ASA 5510

Le Serveur de Sécurité Adaptatif Cisco ASA 5510 propose des services évolués de réseau et de sécurité aux PME et aux filiales et agences des grandes entreprises, sous la forme d'une solution économique et facile à déployer. L'application Web Adaptive Security Device Manager de Cisco, intégrée à la solution, permet de gérer et de surveiller facilement ces services. Les coûts de déploiement et d'exploitation liés à un tel niveau de sécurité sont ainsi réduits. Le serveur de sécurité adaptatif Cisco ASA 5510 fournit des services ultraperformants de firewall et VPN, trois interfaces 10/100 Fast Ethernet intégrées, des services optionnels de lutte contre les vers et de prévention des intrusions via le module AIP-SSM ou des services complets de protection contre les programmes nuisibles via le module CSCSSM.

La combinaison exceptionnelle de ces services sur une plate-forme unique fait de Cisco ASA 5510 un choix idéal pour les entreprises cherchant une solution de sécurité économique et extensible avec DMZ. Pour répondre à la multiplication des besoins des entreprises, le serveur Cisco ASA 5510 peut évoluer vers une densité d'interfaces supérieure et s'intégrer dans des environnements de réseau commuté via la prise en charge VLAN, grâce à l'installation d'une licence de mise à niveau Security Plus. Cette licence de mise à niveau optimise également la continuité des activités grâce aux services de haute disponibilité de type actif/veille.

III.14. La connexion des machines sous GNS3

III.14.1.Le chargement de l'IOS de l'ASA

Pour ce qui concerne la configuration d'un firewall (ASA), Il faut tout simplement aller dans **[Edit]**, sélectionner **[préférences ...]**.

Puis on suit les étapes suivantes :

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

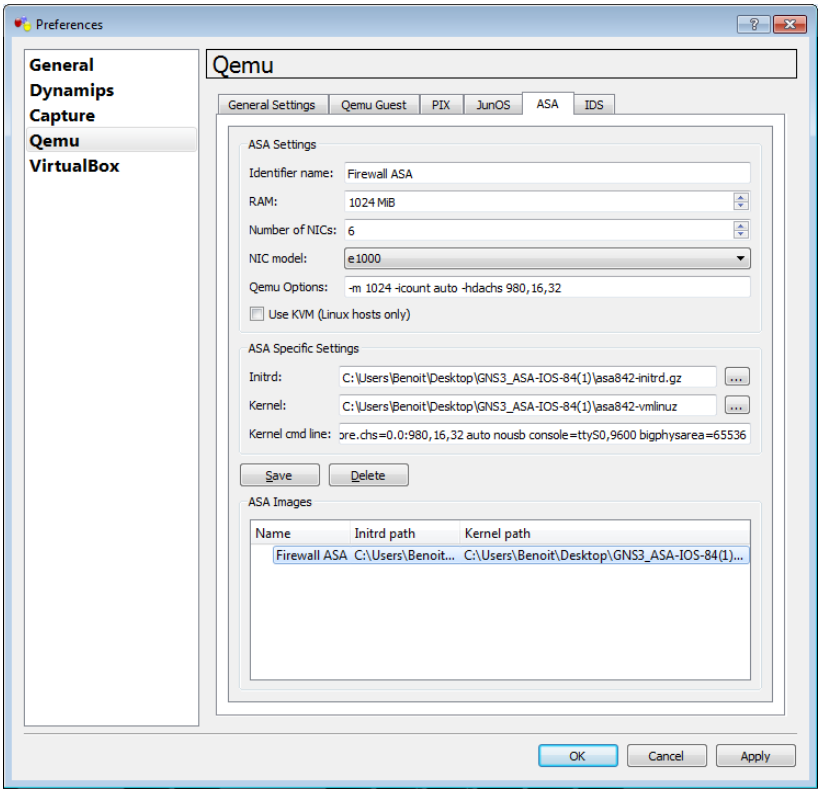


Figure III.7. Localisation de binaire de Qemu.

III.14.2.La configuration du routeur

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 192.168.2.201 255.255.255.0
R1(config-if)#no sh
R1(config-if)#ex
R1(config)#int f0/1
R1(config-if)#ip add 192.168.2.200 255.255.255.0
% 192.168.2.0 overlaps with FastEthernet0/0
R1(config-if)#ip add 10.0.0.1 255.0.0.0
R1(config-if)#no sh
R1(config-if)#
*Mar  1 00:37:35.283: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to
 up
*Mar  1 00:37:36.283: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEtherne
t0/1, changed state to up
```

III.14.3.La configuration des interfaces du l'ASA

L'attribution des adresses se fait comme tout autre équipement Cisco, néanmoins on doit préciser la nature de l'interface inside ou outside et le niveau de sécurité de chaque interface.

Rappelons-nous le principe de fonctionnement de l'ASA, chaque interface d'ASA possède un niveau de sécurité compris entre 0 et 100.

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

ASA-1

```
ciscoasa(config)# int gi
ciscoasa(config)# int gigabitEthernet 0
ciscoasa(config-if)# ip add 192.168.2.200 255.255.255.0
ciscoasa(config-if)# nameif Outside
INFO: Security level for "Outside" set to 0 by default.
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
ciscoasa(config)# int gi
ciscoasa(config)# int gigabitEthernet 1
ciscoasa(config-if)# ip add 10.0.0.1 255.0.0.0
ciscoasa(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)# securi
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
ciscoasa(config)# int gi
ciscoasa(config)# int gigabitEthernet 2
ciscoasa(config-if)# ip add 11.0.0.1 255.0.0.0
ciscoasa(config-if)# nameif Inside
INFO: Security level for "Inside" set to 100 by default.
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
ciscoasa(config)#
```

III.14.4.Configuration de protocole de routage

Le routage permet au réseau pour connecter

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.201
```

+III.14.5.Configuration du NAT

Le réseau LAN dispose d'une plage d'adresse privée alors que la DMZ dispose d'une plage d'adresse publique. Pour que les postes du réseau LAN puissent se connecter à internet il leur faut une adresse IP routable. Pour résoudre se problème nous avons configuré le NAT :

- ✓ Depuis l'intérieur vers l'extérieur NAT Dynamique.
- ✓ Depuis la DMZ vers l'extérieur NAT Dynamique.

```
ciscoasa(config)# object network inside-network
ciscoasa(config-network-object)# subnet 11.0.0.0 255.0.0.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

```
ciscoasa(config)# object network DMZ-network
ciscoasa(config-network-object)# subnet 10.0.0.0 255.0.0.0
ciscoasa(config-network-object)# nat (DMZ,outside) dynamic interface
```

III.14.6.La configuration de l'ACL

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

```
ciscoasa(config)# access-list to-server permit tcp any host 10.0.0.10
ciscoasa(config)# class-map traffic-to-server
ciscoasa(config-cmap)# match access-list to-server
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class traffic-to-server
ciscoasa(config-pmap-c)# set connection embryonic-conn-max 5
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# exit
ciscoasa# wr
Building configuration...
Cryptochecksum: 290272ae 3b18e28f 425479a8 30bf86a3

2209 bytes copied in 2.420 secs (1104 bytes/sec)
[OK]
```

III.14.7.Configuration des VLANs et la configuration des interfaces

Les VLANs (Virtual LANs) permettent entre autre de diviser un même Switch en plusieurs domaines de diffusions. A savoir trois domaines de diffusions distincts. Dans

chacun de ses Vlan on place une partie des interfaces du Switch, ensuite on connecte chaque interface du routeur à une interface placée dans le VLAN souhaité

a. Vlan BASTOS

```
SwitchUMMTO>enable
SwitchUMMTO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchUMMTO(config)#vlan 5
SwitchUMMTO(config-vlan)#name Bastos
```

b. VLAN HASNAOUA

```
SwitchUMMTO(config)#vlan 2
SwitchUMMTO(config-vlan)#name Hasnaoua
```

c. VLAN Paramédical

```
SwitchUMMTO(config-vlan)#nam
SwitchUMMTO(config-vlan)#name Paramedical
```

Affectation des interface aux VLAN

d. Interfaces BASTOS

```
SwitchUMMTO(config)#interface range fastEthernet 0/2-3
SwitchUMMTO(config-if-range)#switchport mode access
SwitchUMMTO(config-if-range)#switchport access vlan 5
```

e. Interfaces Hasnaoua

```
SwitchUMMTO(config)#interface range fastEthernet 0/4-5
SwitchUMMTO(config-if-range)#switchport mode access
SwitchUMMTO(config-if-range)#switchport access vlan 2
```

f. Interfaces Paramédical

```
SwitchUMMTO(config)#interface range fastEthernet 0/6-7
SwitchUMMTO(config-if-range)#switchport mode access
SwitchUMMTO(config-if-range)#switchport access vlan 4
```

III.14.8.Configuration des ports

```
SwitchDMZ(config)#interface fastEthernet 0/2
SwitchDMZ(config-if)#switchport mode access
SwitchDMZ(config-if)#switchport port-security
SwitchDMZ(config-if)#switchport port-security mac-address 0001.6359.5E44
SwitchDMZ(config-if)#swi
SwitchDMZ(config-if)#switchport po
SwitchDMZ(config-if)#switchport port-security vi
SwitchDMZ(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
SwitchDMZ(config-if)#switchport port-security violation shu
SwitchDMZ(config-if)#switchport port-security violation shutdown
```

III.15.Test

Le test a été effectué avec l'outil hping3 sur debian8

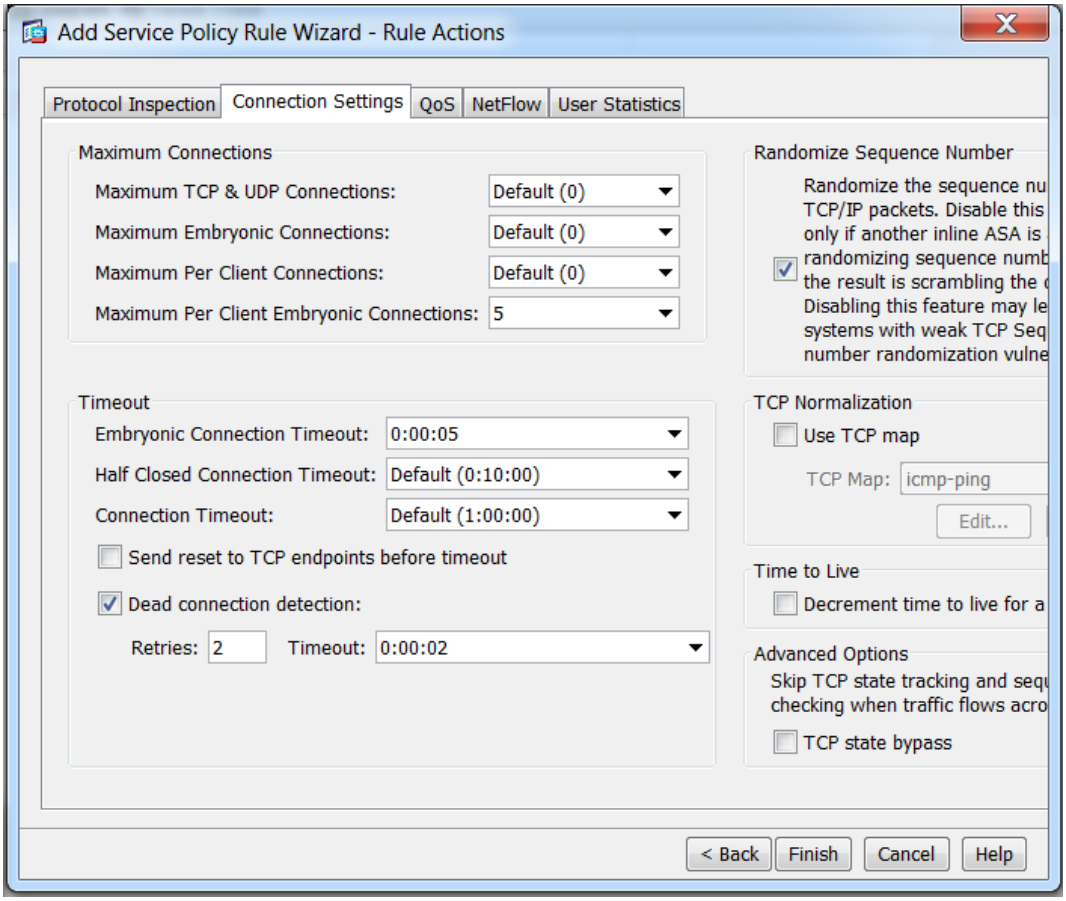
Debian8 est un système d'exploitation linux

La commande pour faire le tcp synflood

Hping3-i u1 –S 80 10.0.0.100

```
root@WEB-SERVER:/home/admin-user# hping3 -i u1 -S -p 80 10.0.0.100
```

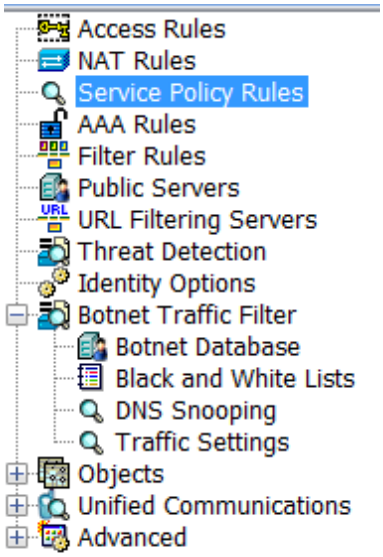
Donc pour commencé on test sans limiteur de connexions



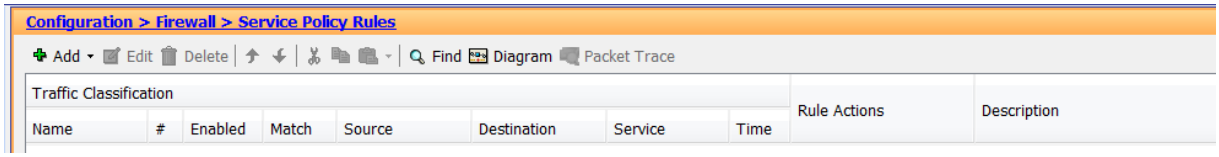
Pour commencer à limité les connexions

On ouvre ASDM et on choisi la section configuration

Ensuite on choisi « Service Policy Rules »

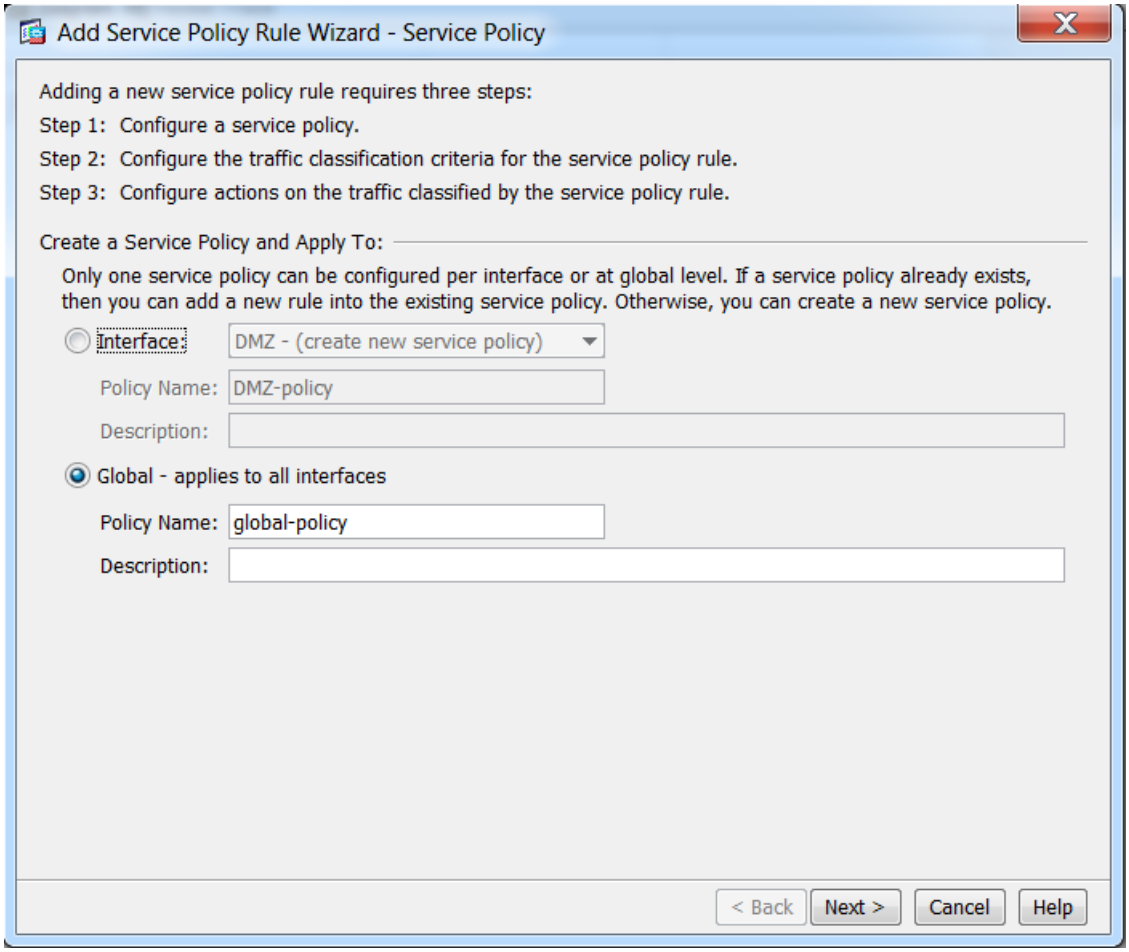


Après ça on doit ajouter une politique (Policy) pour la limitation pour ce faire on va juste cliquer sur ADD dans service policyrules

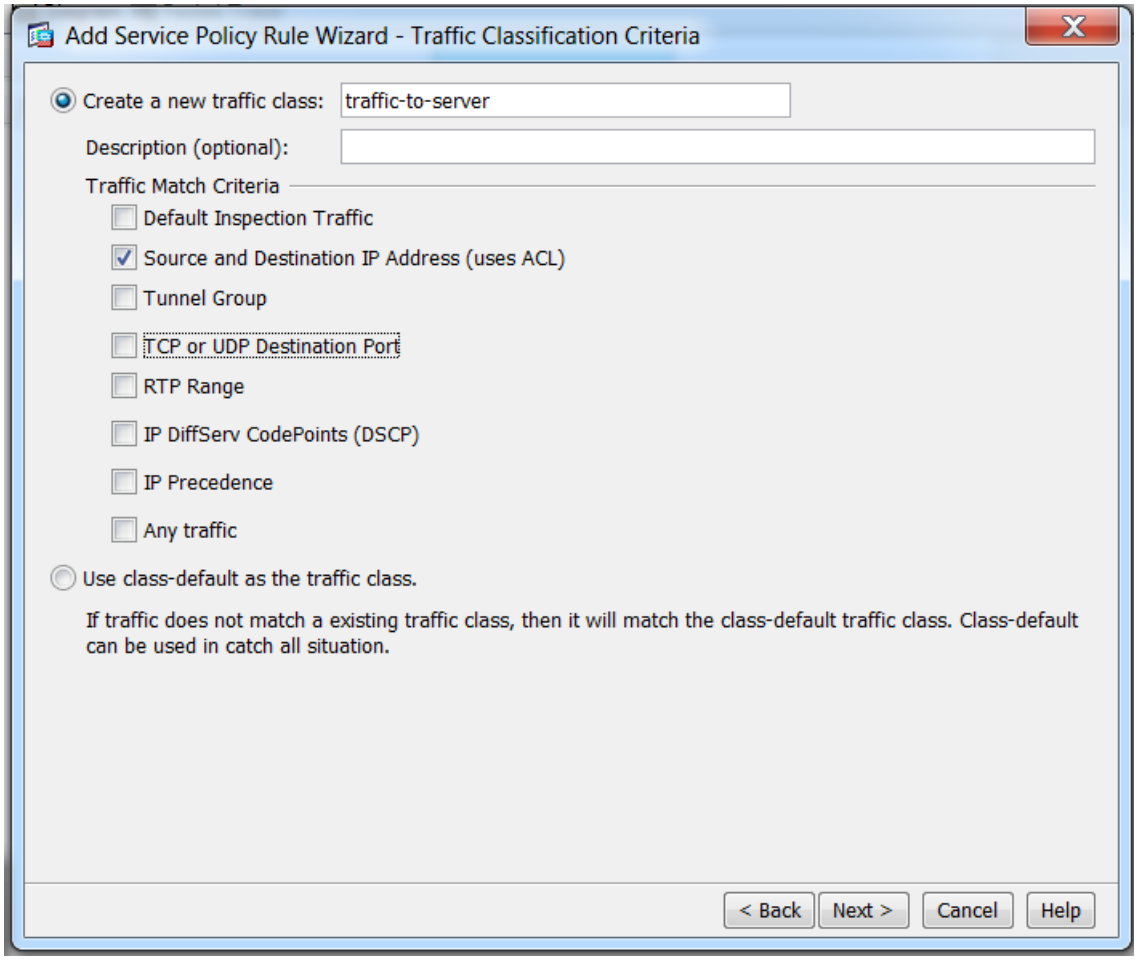


Ensuite y a 4 étapes qu'on va suivre

On peut choisir une interface « DMZ, Inside, Outside » ou bien une politique définie (Policy)



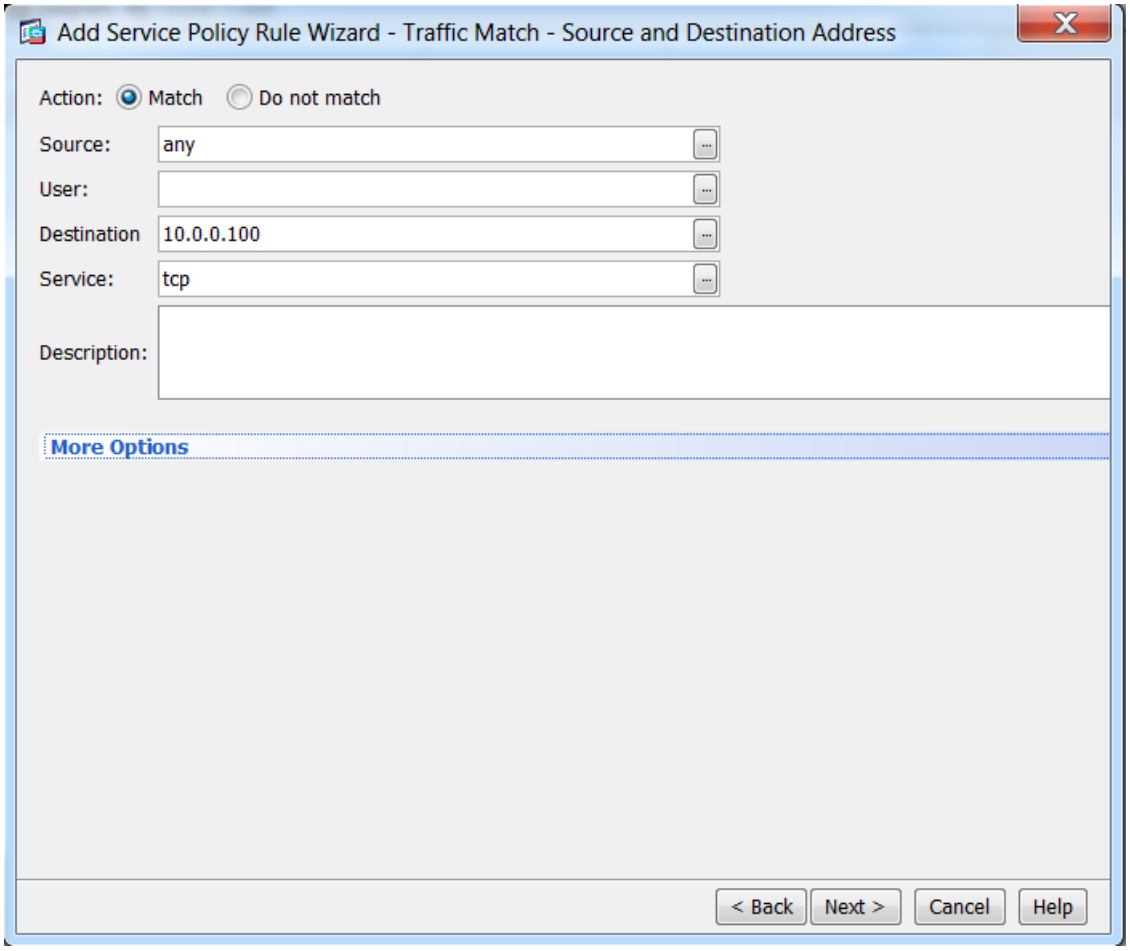
Après ça on crée un nom d'une et le critère qui lui convient, dans notre cas on a choisi ACL « access Lists »



Ensuite, on doit ajouter une IP source et destination pour notre règle

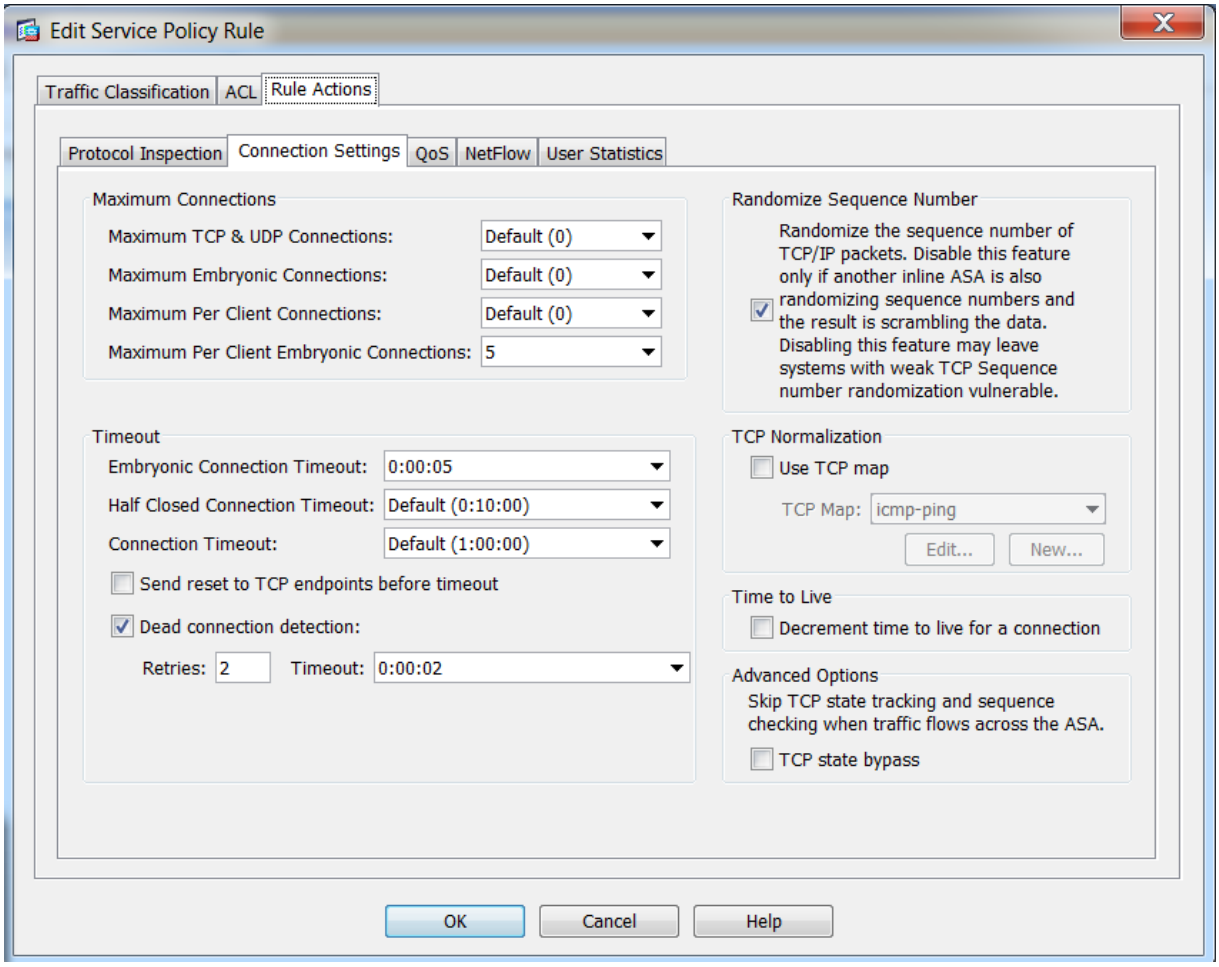
La source=le client

La destination=le serveur

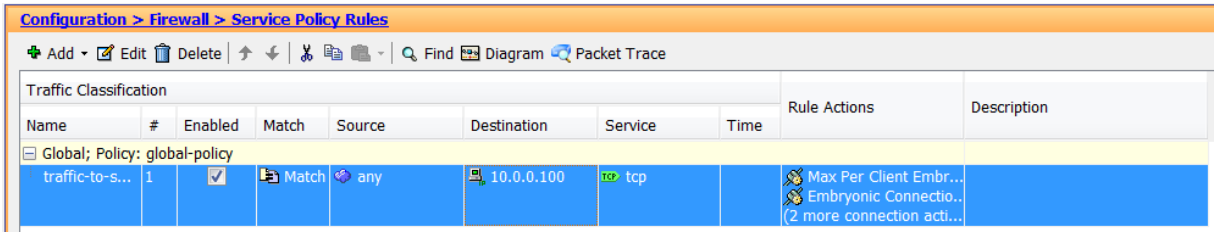


On a écrit « any » pour accepter toutes les connexions entrantes, puisue on ne connait pas les adresses sur internet qui se connectent sur notre serveur

Et en fin l'étape 4, qui est la plus importante, nous permet de limité les connexions, donc on a configuré le nombre de connexions maximales par client à 5, et un timeout (veut dire que le serveur attendra un certain temps avant d'abandonner le paquet) à 5 secondes et on a activé la détection des connexions dead (qui ne sont plus valables) ou 2 tentatives seront émises avec un timeout de 2 secondes



Le résultat de cet ajout est comme suit sur l'image suivante



On a refait le test avec la même commande pour tester notre règle configurée et on a eu le résultat suivant

```
ASA-UMMTO# show conn
5 in use, 8811 most used
TCP outside 192.168.3.3:1678 DMZ 10.0.0.100:80, idle 0:00:00
TCP outside 192.168.3.3:1677 DMZ 10.0.0.100:80, idle 0:00:00
TCP outside 192.168.3.3:1532 DMZ 10.0.0.100:80, idle 0:00:00
TCP outside 192.168.3.3:1531 DMZ 10.0.0.100:80, idle 0:00:00
TCP outside 192.168.3.3:1530 DMZ 10.0.0.100:80, idle 0:00:00
```

5 connections maximales par client

Connexions*

Maximales*

Discussion

D’après les tests et les résultats obtenus, on constate que la configuration de pare –feu ASA serait une solution adéquate dans la plupart des entreprises surtout ceux dotées de nouvelle technologies. Ce dernier bloque tous les attaques qui viennent de l’extérieur.

Conclusion générale

Dans cette mémoire on a étudié un mécanisme de sécurité pour élaborer une politique de sécurité au sein d'un réseau, il s'agit de Firewall qui offre plusieurs solutions pour faire face au menace qui peut atteindre un réseau d'entreprise depuis l'extérieur, ou on a parlé sur les principaux fonctionnement comme le filtrage des paquet et aussi sur la translation des adresses IP(NAT). Cette dernière elle peut cacher le réseau d'entreprise derrière un réseau publique cela il accompagnera de protéger son réseau de plusieurs attaque qui ont d'une source externe.

Cependant ces menaces qui peut atteindre un réseau et aussi de source interne, un employer ou un utilisateur de réseau depuis l'intérieur de l'entreprise peut exploiter les faille de la politique de sécurité, par une simple connaissance de réseau il peut accéder à n'importe quelle source d'information dans des domaine et des tache qu'elle ne concerne pas, il peut voler, détruire, et aussi modifier ces informations.

Et pour ces raisons la mise en place des mesures de sécurité qui peuvent réduire les risques internes est très nécessaire, une solution telle que les VLAN (Virtuel Local Area Network) est très rependu pour faire séparer les différent tache d'une entreprise.

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

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

Nous estimons que la configuration d'ASA que nous avons réalisée va répondre aux exigences et besoins des utilisateurs de fait qu'elle permet d'offrir une meilleure sécurité

Bibliographie

J.F.Pillou «Tout la sécurité informatique », Ed.Dunod.2005

Wimmial Puech « classification des réseaux » centre Universitaire de formation et de recherche, 2006.

Eric Filiol, les virus informatiques CERAM, « Fondamentaux des sciences de l'information ».

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

« Sécurité des réseaux informatiques » Université de Rennes1 ; 2008

Guy Pujolle, les réseaux locaux, Eyrolles, 2003.

« Sécurisation d'une infrastructure DMZ avec ASA 5510 », université UMMTO département d'Electronique. Thèse Master, l'année 2012-2013.

Pierre Jaquet, Lavoisier, Les réseaux et l'informatique de l'entreprise, 2003.

http:// WWW.idum.eu/spip.php configuration de gns3 pour la mise en place d'un pare-feu Cisco ASA

http:// WWW.google.fr/ la sécurité des réseaux dans les entreprises

http:// WWW.google.fr/ le réseau informatique

http:// WWW.google.fr/présentation Microsoft 2012 server

http:// WWW.GOOGLE.FR/cISCO ASA server édition standard

https://www.pensezcybersecurite.gc.ca/index-fr.aspx

http://lesdefinitions.fr/securite-informatique#ixzz4etFOneKT