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

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master II en Electronique

Option : Réseaux et télécommunication

Thème :

Mise en place d'un pare-feu en utilisant le Smoothwall.

Proposé et dirigé par :

Mr. M.LAHDIR

Présenté par :

Mr. DOUICHER Yacer

Mr. SISSOKO Seydou

Année universitaire 2011/2012

Remerciements

Nous remercions en premier lieu Dieu tout puissant de nous avoir accordé la puissance et la volonté pour terminer ce travail.

A travers ce modeste travail, nous tenons à remercier vivement notre encadreur « Mr. LAHDIR Mourad» maître de conférences, Pour ses conseils précieux qu'il nous a apportées durant notre étude et réalisation de ce projet.

Nos remerciements les plus vifs s'adressent aussi à messieurs le président et les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les enseignants qui ont collaboré à notre formation depuis notre premier cycle d'étude jusqu'à la fin de Notre cycle universitaire.

Enfin il est de notre devoir d'exprimer tous nos remerciements aux personnes qui ont contribué à la réalisation de ce travail.

Mr. DOUICHER Yacer

Mr. SISSOKO Seydou

Au nom de dieu le clément et le miséricordieux

Je dédie ce modeste travail à :

- ✓ Mes très chers parents, pour leur soutien et tous les efforts qu'on m'a donnée le long de mon parcours et je leur souhaite bonne santé et longue vie ;
- ✓ Mes très chères frères : Lounes et Abderezak ;
- ✓ Mon grand père Mouloud ;
- ✓ Mes amis et à tous mes camarades de la promotion ;
- ✓ Tous ceux qui me sont chers.

y. Douicher

Dédicaces

Je dédie ce modeste travail à mes très chers parents, pour leur soutien et tous les efforts qu'on ma donnée le long de mon parcours et je leurs souhaite bonne santé et longue vie.

Je dédie ce modeste travail aussi à tous mes amis.

A tous mes enseignants qui ont fait leurs possibles pour nous donner le maximum d'informations concernant notre étude.

Et finalement pour la promotion **Master Electronique 2012.**

S. Seydou

Sommaire

CHAPTRE II

Chapitre III

Table des figures

Table des figures

Liste des tableaux

Introduction

De nos jours, la plus part des entreprises possèdent de nombreux postes informatiques qui sont en général reliés entre eux par un réseau local. Ce réseau permet d'échanger des données entre les divers collaborateurs internes à l'entreprise et ainsi de travailler en équipe sur des projets communs.

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi**.** L'objectif de ce travail est de sécuriser le réseau interne d'entreprise contre les menaces extérieures avec un coût minimal, en utilisant une architecture de réseau sécurisée qui comporte un élément essentiel qui est le firewall. Cet outil a pour but de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut également permettre de délimiter l'accès interne vers l'extérieur.

Notre travail est reparti en trois chapitres :

Premièrement, en commençant par des généralités sur les réseaux informatiques. Dans lequel, nous allons expliquer en détail les différents éléments d'un réseau, tels que : définition d'un réseau, l'intérêt d'un réseau, les architectures possibles pour un réseau, classification des réseaux, les équipements d'interconnexion du réseau, les supports de transmission, les protocoles utilisés dans le réseau, puis nous terminerons cette première partie par une discussion.

Le deuxième chapitre sera basé sur la sécurité des réseaux informatique. Dans ce chapitre, nous allons définir la sécurité informatique, les causes de l'insécurité, puis proposer les solutions possibles et nous terminerons ce chapitre par une discussion.

Le troisième chapitre sera exclusivement consacré sur le **smoothwall**. Dans ce chapitre, nous allons définir **smoothwall**, Comment fonctionne-il, Comment installer et configurer **smoothwall,** Puis nous terminons cette partie avec une discussion.

Et enfin, nous terminons notre mémoire par une conclusion et des perspectives ouverts par ce travail.

I.1. Préambule :

Le mot réseau est très souvent employé dans un sens qui le lie aux communications. Ainsi tout un chacun connaît le réseau téléphonique, le réseau routier, le réseau de neurone, de même le réseau d'amis.

En informatique deux ordinateurs reliés entre eux par un câble forment déjà un réseau. On peut ainsi connecter deux « PC » avec un câble croisé et faire des transferts de fichiers d'un disque dur vers l'autre. On utilisera pour cela un logiciel adapté au protocole d'émission et de réception des données par le port parallèle.

Deux réseaux reliés entre eux par un quelconque moyen permettant aux informations de circuler (ligne téléphonique, satellite...) forment un nouveau réseau. Il faut pour cela, ce qui n'est pas si simple, qu'un protocole commun d'échange puisse être utilisé.

Internet est un réseau fait de réseaux qui peuvent utiliser un protocole commun d'échange de données.

Dans ce chapitre, nous allons expliquer en détail les différents éléments d'un réseau et leurs caractéristiques.

I.2. Définition d'un réseau :

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations.

Le terme réseau en fonction de son contexte peut designer plusieurs choses :

- décrire la façon dont les machines d'un site sont interconnectées ;
- spécifier les protocoles qui sont utilisés pour que les machines communiquent on peut parler de réseau TCP/IP.

I.3. Intérêt d'un réseau :

- partage de fichiers, d'applications, de périphériques informatiques ;
- communication entre personnes (grâce au courrier électronique, le dialogue en direct, ...) ;
- communication entre processus (entre des machines industrielles) ;
- garantie de l'unicité de l'information (bases de données).

I.4. Architecture d'un réseau :

On distingue deux catégories de réseaux :

I.4.1. Les réseaux poste à poste (Peer to Peer / égal à égal) :

Dans cette architecture Les données ne sont pas centralisés et tous les ordinateurs connectés ont le même statut et se partagent toute l'information et tous les services sans l'aide d'un serveur.

I.4.2. Réseaux organisés autour d'un serveur (Client/serveur) :

Tous les ordinateurs (clients) sont reliés à un serveur dédié qui Centralise les données relatives au bon fonctionnement du réseau.

I.5. Classification des réseaux :

Les réseaux informatiques peuvent être classés en se basant sur plusieurs critères, par exemple la distance entre entités communicantes, la topologie et le type d'accès ….

I.5.1. Classification selon leur taille :

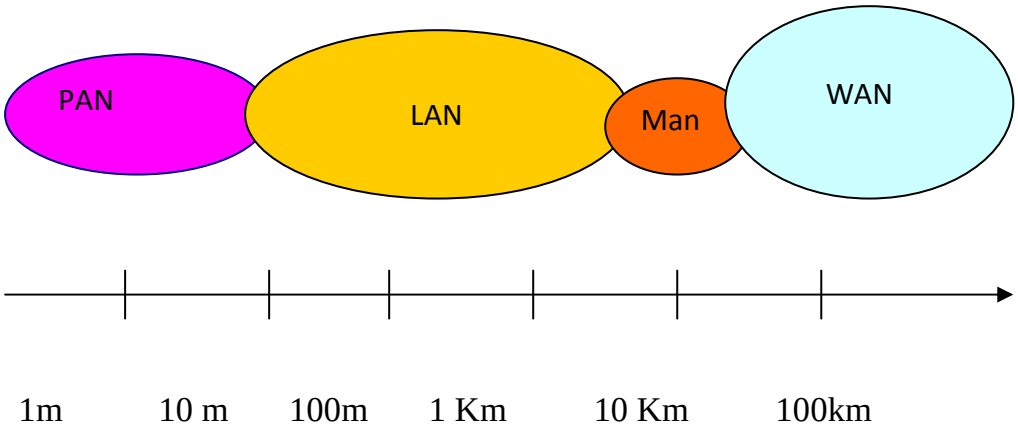


Figure -I.1- : Classification des réseaux informatiques selon leur taille.

I.5.1.a. Réseaux personnels (PAN) :

Les PAN (Personal Area Network), la plus petite taille de réseau. Ces réseaux personnels interconnectent sur quelques mètres entre les équipements personnels tels que GSM, portable, organiseur etc.… d'un même utilisateur.

I.5.1.b. Les réseaux locaux (LAN) :

LAN signifies Local Area Network. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

I.5.1.c. Les réseaux métropolitains (MAN) :

Les MAN (Métropolitain Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

I.5.1.d. Les réseaux étendus (WAN) :

Un WAN (Wide Area Network ou réseau étendu) permet de communiquer à l'échelle d'un pays, ou de la planète entière, les infrastructures physiques pouvant être terrestres (infrastructures au niveau sol), ou spatiales à l'aide de satellites de télécommunications c'est le cas de l'Internet.

I.5.2. Classification selon la topologie :

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce au matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique.

I.5.2.a. Topologie en bus :

Dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

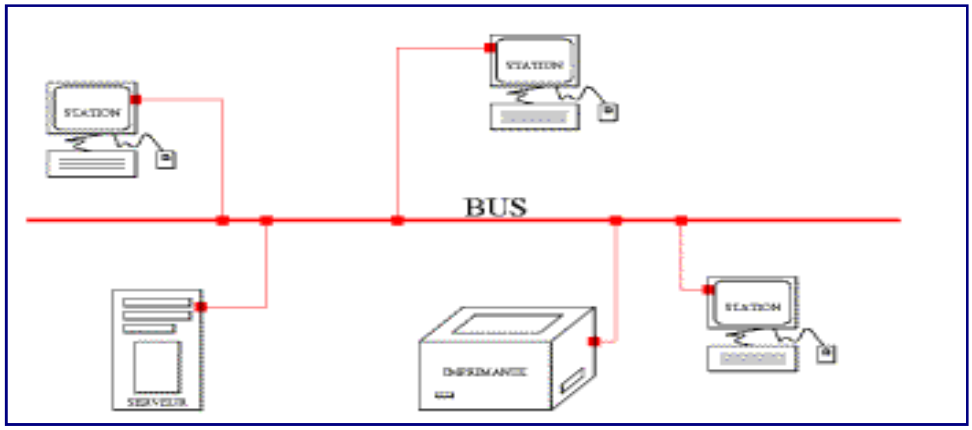


Figure -I.2- : Topologie en bus.

I.5.2.b. <u>Topologie en anneau</u> :

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole" successivement.

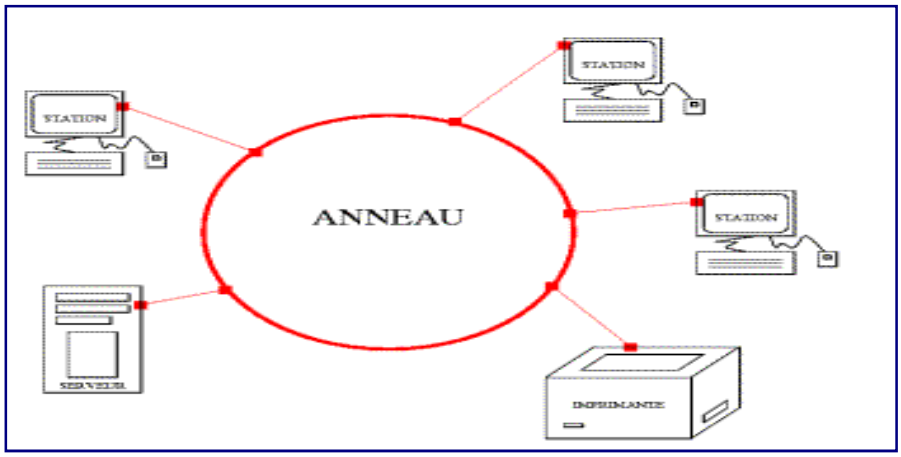


Figure -I.3- : Topologie en anneau.

I.5.2.c. Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé Hub ou concentrateur.

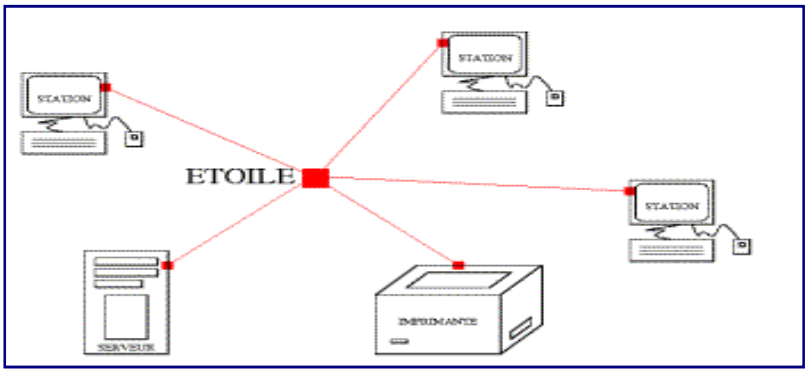


Figure -1.4-: Topologie en étoile.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile est beaucoup moins vulnérable car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau.

I.5.3. Classification selon le mode de connexion :

I.5.3.a Les modes avec connexion :

Le mode avec connexion consiste à faire appel à 3 phases distinctes:

- L'établissement de la connexion, le transfert de données et la libération de la connexion ;
- Dans le mode avec connexion, la transmission des données est sécurisée puisque l'émetteur et le récepteur se mettent d'accord, et par la suite le contrôle est effectué, au moins, au niveau des deux extrémités ;

- l'émetteur et le récepteur négocient, sur quelques paramètres définissant les limites admissibles pour le transfert des données, c'est la négociation de la qualité de service.

I.5.3.b Les modes sans connexion :

Le mode sans connexion n'a pas besoin de présence, à la fois et en même temps, des entités communicantes distantes. Il n'y a pas de négociation entre l'émetteur et le récepteur. Pour mettre en place cette connexion, il faut penser à une logistique afin de s'assurer du transfert des données : c'est la structure en couches, telle que chaque couche rend service à celle qui est inférieure.

Dans une communication en mode non connecté, les données (ou unités de données) sont connues à l'avance, et joignes par des informations de contrôle ainsi que l'adresse complète des deux entités c'est-à-dire émetteur et récepteur.

I.5.4. Classification selon la Méthodes d'Accès

Dans un réseau local, chaque nœud est susceptible d'émettre sur le même câble de liaison. L'ensemble des règles d'accès, de durée d'utilisation et de surveillance constitue le protocole d'accès aux câbles ou aux média de communication. Les méthodes d'accès proprement dites sont aux nombres de deux : CSMA/CD, Token Ring (jeton).

I.5.4.a. La méthode d'accès CSMA/CD :

CSMA (Carrier Sens Method Access) utilisé dans la norme 802.3 et Ethernet. Son principe est celui de la politesse : on ne parle que quand personne ne parle.

Lorsque la station veut émettre, elle écoute. Si personne d'autre n'émet, elle émet. Si une autre station émet, elle attend. Ensuite soit elle réessaye plus tard (CSMA

non persistant, la méthode n'est plus utilisée), soit elle écoute et lorsque c'est libre elle émet (CSMA persistant).

Cette méthode a un inconvénient : lorsque deux stations attendent, elles vont émettre en même temps. Les deux signaux vont se superposer et être incompréhensibles. On appelle cela une collision. Pour résoudre ce problème on va effectuer une détection des collisions (CD : Collision Détection). D'où le nom de CSMA/CD.

I.5.4.b. La méthode d'accès par jeton :

Dans le cas des réseaux à topologie en anneau ou en bus, une trame vide circule en permanence sur le câble qui relie l'ensemble des machines. Cette trame s'appelle le jeton. Le jeton circule et passe de nœud en nœud d'une manière séquentielle. Seul le détenteur du jeton peut transmettre un message.

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. Les Routeurs :

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre.). Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en terme de taille de paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation.

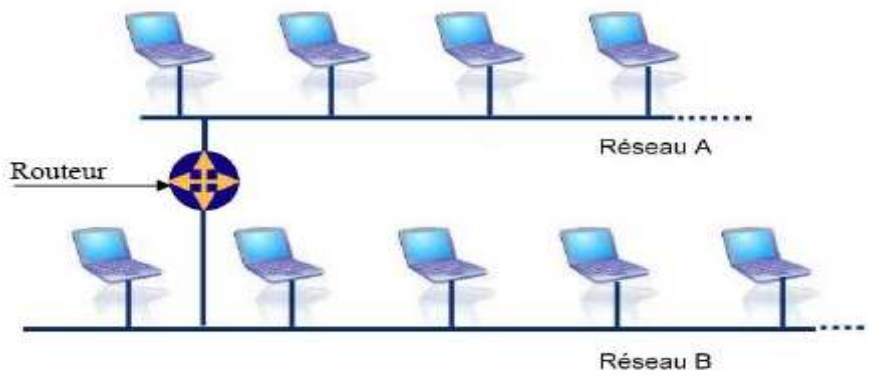


Figure -I.5- : Routeur connecté à deux réseaux locaux.

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leurs permettant d'acheminer les paquets quelque soit l'architecture.

I.6.2. Les Hubs (concentrateurs) :

Le Hub est également appelé concentrateur ou répétiteur. C'est un boîtier électronique assurant la liaison des postes et des périphériques du réseau. Le répétiteur se contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau (dont le destinataire).

I.6.3. Switch :

Egalement appelé Commutateur, Boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au 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.6.4. Les Passerelles :

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles 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.

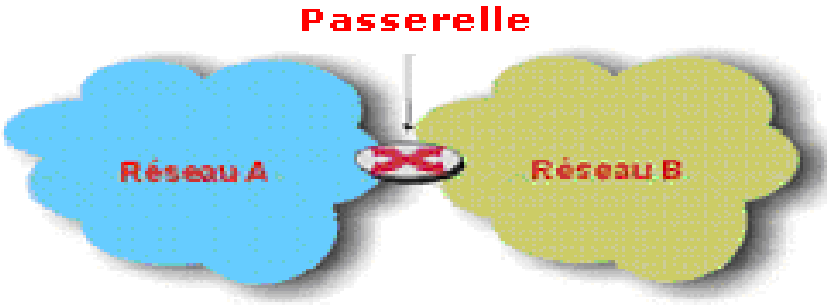


Figure -I.6- : deux réseaux reliés avec passerelle.

I.6.5. Les ponts :

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont.

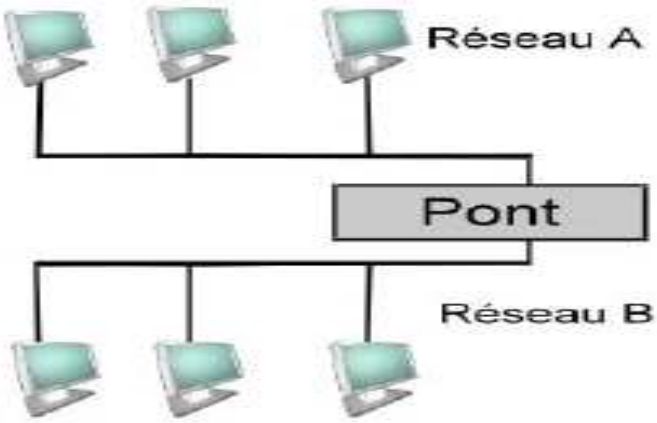


Figure -I.7- : Deux réseaux relient avec un pont.

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (MAC) du destinataire et de l'émetteur. Si jamais le pont ne connaît pas l'émetteur, il stocke son adresse dans une table afin de se "souvenir" de quel côté du réseau se trouve l'émetteur.

I.7. Support de transmission :

Un support de transmission est 'un moyen d'interconnexion et de Transfert de données entre les périphériques finaux et intermédiaires du réseau.

I.7.1. Caractéristiques de supports de transmissions :

Les supports de transmissions de donnée sont choisis en fonction de nombreuses caractéristiques, les principales étant les suivantes :

- Installation et maintenance ;
- 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.7.2. Types de supports de transmissions :

Il existe trois formes élémentaires de support réseau sur lesquelles les données sont transportées :

I.7.2.a. Supports en cuivre :

Le support le plus souvent utilisé pour les communications de données est un câblage qui utilise des fils de cuivre pour la transmission de bits de données et de contrôle entre les périphériques réseau.

- **Câble à paires torsadées :**

- **Câble à paires torsadées non blindées (UTP) :** (Unshielded twisted-pair)

Le câblage à paires torsadées non blindées (UTP), tel qu'il est utilisé dans les réseaux locaux Ethernet, se compose de quatre paires de fils à code de couleur qui ont été torsadées puis logées dans une gaine en plastique souple.

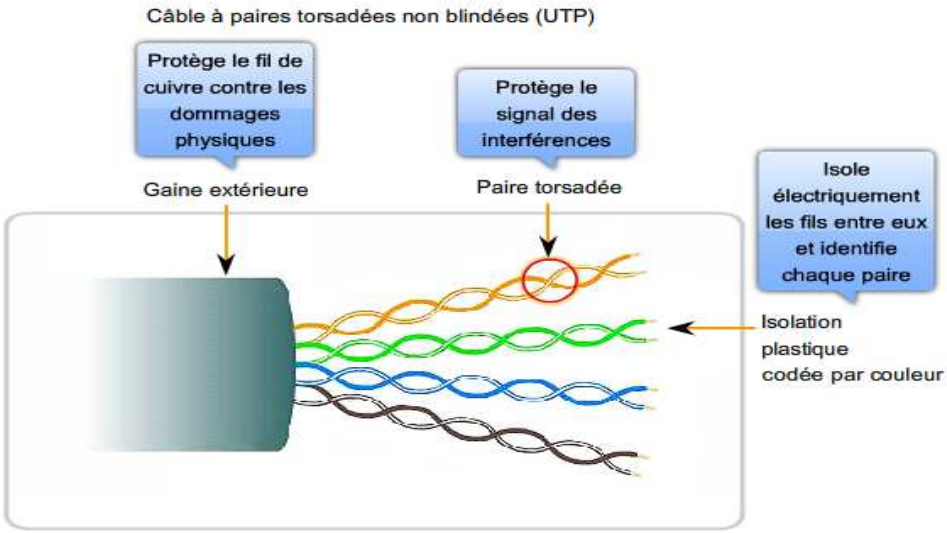


Figure -I.8- : câble UTP.

La torsion a pour effet d'annuler les signaux indésirables. Lorsque deux fils d'un circuit électrique sont rapprochés, les champs électromagnétiques externes créent la même interférence dans chaque fil. Le récepteur la traite de manière égale bien

qu'opposée. En conséquence, les signaux causés par des interférences électromagnétiques provenant de sources externes sont annulés dans les faits.

- **Câble à paires torsadées blindées (STP) :** (Shielded Twisted-Pair)

Un autre type de câblage utilisé dans les réseaux est le câble à paires torsadées blindées (STP). Comme l'illustre la figure suivante, la norme STP utilise deux paires de fils enveloppées dans un revêtement tressé ou un film métallique.

Le câble STP protège le faisceau entier de fils à l'intérieur du câble ainsi que les paires de fils individuelles. Le câblage STP offre une meilleure protection parasitaire que le câblage UTP, mais à un prix relativement plus élevé.

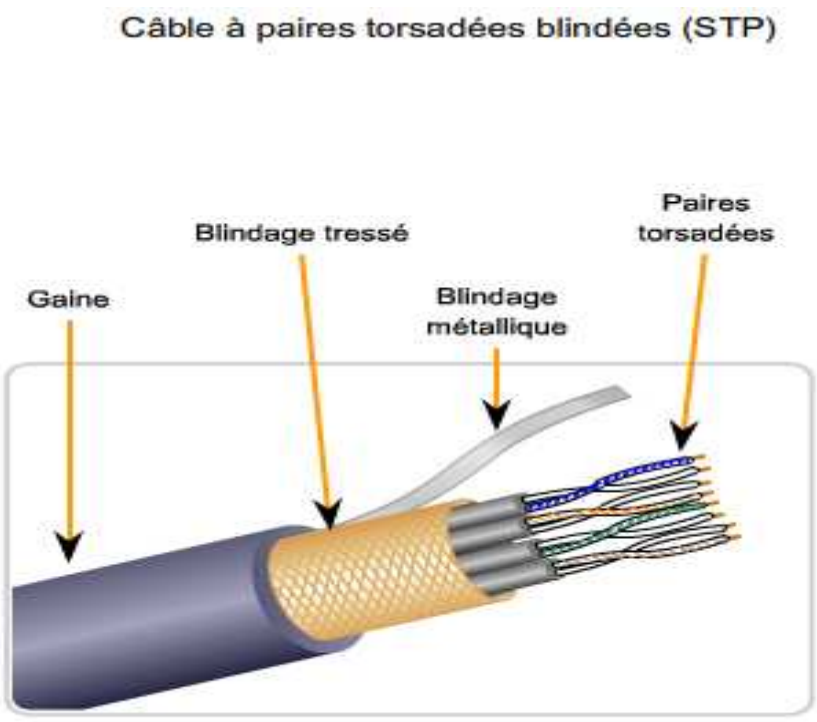


Figure -I.9- : câble STP**.**

- **Les connecteurs utilisés pour le câble à paires torsadées :**

Prise murale.

RJ45 : câble réseau 8 fils.

Figure -I.10- : prise et connecteurs RJ45.

- **<u>Câble coaxial</u> :**

Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible, comme l'illustre la figure ci-dessous.

Sur ce matériau isolant, une torsade de cuivre ou un film métallique constitue le second fil du circuit qui agit comme protecteur du conducteur intérieur. Cette seconde couche, ou blindage, réduit également les interférences électromagnétiques externes. La gaine du câble enveloppe le blindage.

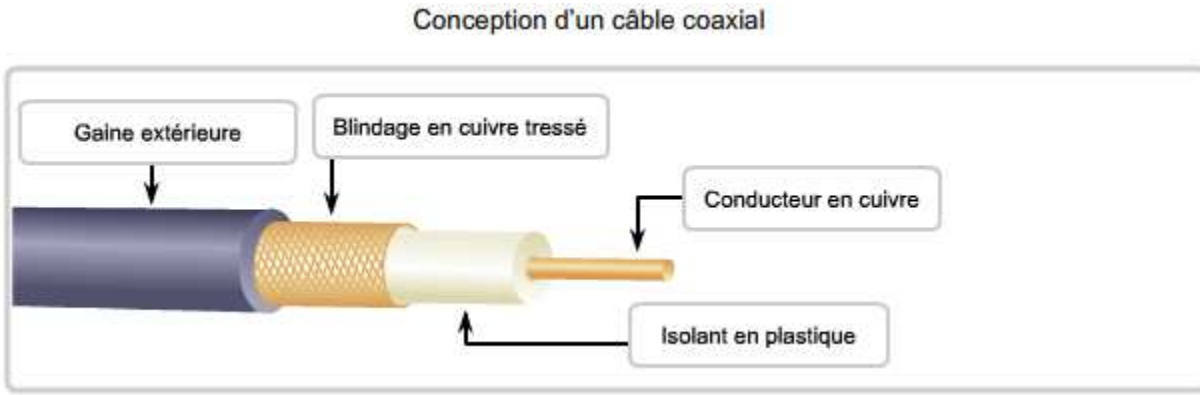


Figure -I.11- : câble coaxial.

Le câble coaxial est également le support le plus largement employé pour le transport par fil de signaux de radiofréquence élevée, en particulier les signaux de télévision par câble. La télévision par câble classique, qui émet exclusivement dans une direction, était composée entièrement de câbles coaxiaux.

Il existe différents types de câble coaxial :

- **Câble coaxial RG 58** :(câble coaxial mince), est utilisé pour les transmissions de données Ethernet dans la limite de longueur maximale de 200m sans régénérer le signal.

  Ce support tend à disparaitre, car il est incompatible avec les réseaux Ethernet haut débit.

- **Câble coaxial RG 11** :(câble coaxial épais), présente un meilleur niveau de blindage, il permet de faire transiter des données jusqu'à 500m par tronçon.

- **Câble coaxial large bande :** CATV (community antenna television), est le câble utilisé pour la transmission de chaines de télévision par câble, sa largeur de bande beaucoup plus élevée (jusqu'à 500 MHZ) autorisant la transmission d'image.

➢ **Les connecteurs utilisés pour le câble coaxial :**

Figure -I.12- connecteurs câble coaxial.

I.7.2.b. Supports en fibre optique :

Le câblage en fibre optique utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Les bits sont codés sur la fibre comme impulsions lumineuses. Le câblage en fibre optique prend en charge des débits de bande passante de données brutes très élevés. La plupart des normes de transmission actuelles n'approchent cependant pas encore la bande passante potentielle de ce support.

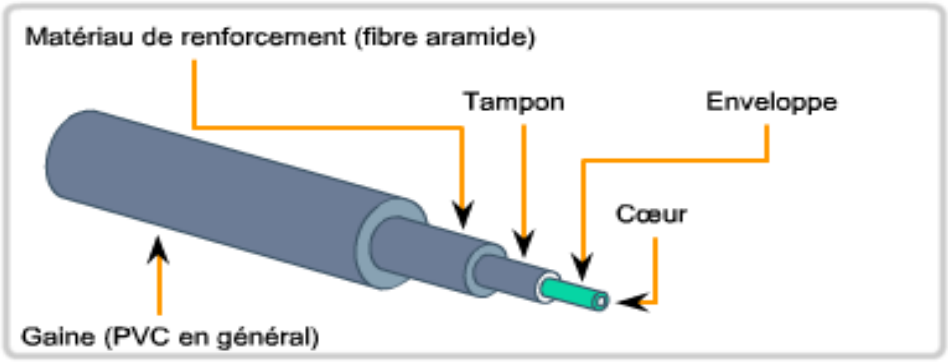


Figure -I.13- : fibre optique.

Des lasers ou des diodes électroluminescentes (DEL) génèrent les impulsions lumineuses utilisées pour représenter les données transmises sous forme de bits sur le support. Des dispositifs à semi-conducteur électronique appelés photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.

Les câbles à fibre optique peuvent être classés en deux grands types : monomode et multimode.

- **Fibre optique monomode :**

  La fibre optique monomode transporte un seul rayon lumineux, généralement émis par un laser. La lumière laser étant unidirectionnelle et voyageant au centre de la fibre, ce type de fibre peut transmettre des impulsions optiques sur de très longues distances.

- **Fibre optique multimode :**

La fibre multimode utilise en principe des émetteurs à DEL qui ne créent pas une seule onde lumineuse cohérente. La lumière d'une DEL entre au contraire dans la fibre multimode selon différents angles. La traversée de la fibre prenant ainsi plus ou moins de temps, des longueurs de fibre importantes peuvent générer des impulsions troubles à l'arrivée à l'extrémité réceptrice. Cet effet, appelé distorsion modale, limite la longueur des segments de fibre multimode.

- **Les connecteurs**

Figure -I.14- : connecteurs fibre optique.

I.7.2.c. <u>Supports sans fil</u> :

Certaine milieux autorisent la transmission des ondes électromagnétiques (l'air, le vide, …), et peuvent être utilisés par les réseaux sans fil comme support de transmission. On nome alors ces milieux conducteurs l'espace hertzien.

Une onde électromagnétique est caractérise par :

- Sa fréquence en Hertz, c'est-a-dire le nombre d'oscillations observées en une seconde ;

- Sa longueur d'onde, en mètre, correspondant à la distance entre deux maxima (ou deux minima) consécutifs.

En fonction de leurs fréquences, les ondes électromagnétiques ont étés classées en plusieurs familles. Notant que la capacité d'une onde à traverser la matière physique varie à l'inverse de sa fréquence (les ondes de bases et moyennes fréquences « radio » n'ont aucune difficulté à passer les obstacles, ce qui est impossible aux ondes de trais haute fréquences « infrarouge ».

I.8. Modèle de référence OSI :

OSI signifie (Open Systems Interconnection). Ce modèle a été mis en place par l'ISO (International Standard Organization) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

Le modèle OSI définit 7 niveaux différents pour le transfert de données, ces niveaux sont également appelés couches.

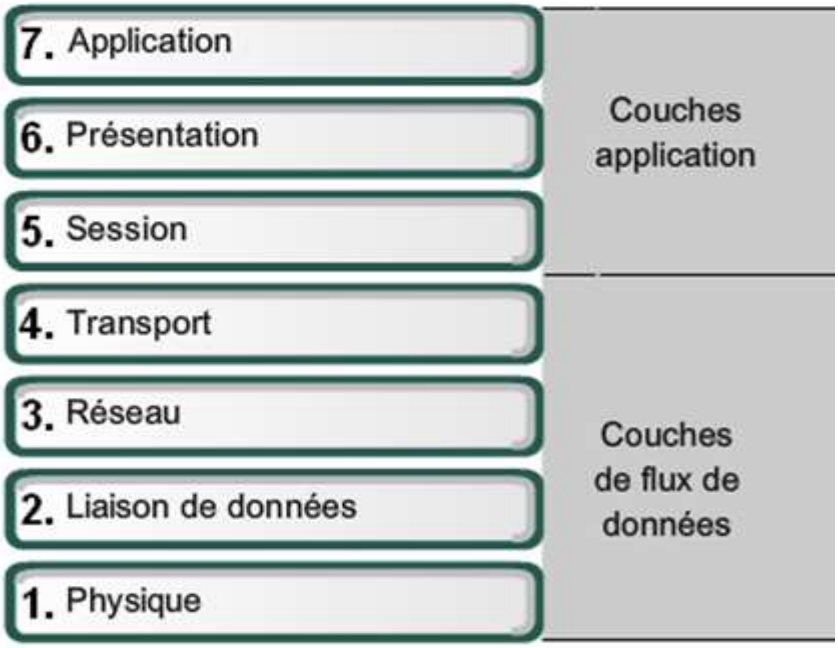


Figure -I.15- : les 7 couches du modèle OSI.

Couche Application (7)

- Sert d'interface entre les applications à chaque extrémité du réseau ;
- Permet d'échanger des données entre les programmes s'exécutant sur les hôtes source et de destination.

Couche Présentation (6)

- Codage et conversion des données de la couche application afin que les données issues du périphérique source puissent être bien interprétées sur le périphérique de destination ;
- Compression des données de sorte que celles-ci puissent être décompressées par le périphérique de destination ;
- Chiffrement des données en vue de leur transmission et déchiffrement des données reçues par le périphérique de destination.

Couche Session (5)

- Permet d'initier un dialogue entre les applications source et de destination ;
- Initier et maintenir un dialogue ;
- Redémarrer les sessions interrompues ou inactives pendant une longue période.

Couche Transport (4)

- Permet l'acheminement de bout en bout sans se soucier des relais intermédiaires ;
- Fragmentation du message en unités plus petites dites segments ;
- Multiplexage.

Couche réseau (3)

- Permet l'acheminement de bout en bout en tenant compte des nœuds intermédiaires ;
- Routage et ordonnancement des paquets.

Couche liaison de données (2)

- Structuration des données en trames ;
- Masquer les caractéristiques physiques ;
- Contrôle d'erreur à l'émission et à la réception.

Couche physique (1)

- Assurer la transmission de bits entre les entités physiques ;
- Spécifie la nature du support de communication ;
- Le mode de connexion et le brochage le cas échéant ;
- La technique de codage des bits en signaux électriques ;
- Les tensions et les fréquences utilisées.

I.9. Modèle TCP/IP (modèle Internet) :

Le modèle TCP/IP est structuré en quatre couches de protocoles qui doivent s'exécuter pour que les communications réussissent. TCP (Transfert Contrôle Protocole) se charge du transport de bout en bout pour toute application, IP (Internet Protocole) est responsable du routage à travers le réseau.

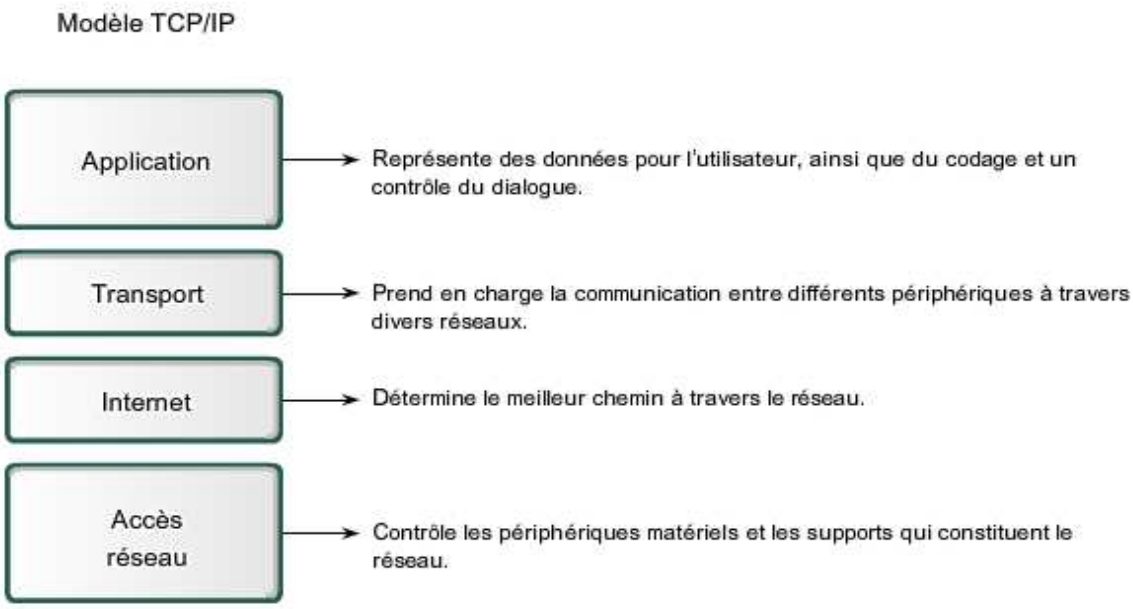


Figure -I.16- : les 4 couches du modèle TCP/IP.

I.10. Protocols multiples (encapsulation) :

Le message reçu par l'hôte comporte habituellement de nombreux protocoles en plus de la donnée courante.

- **Encapsulation :** veut dire Ajout d'entêtes à la donnée ou à une série d'entêtes précédents.

- **Décapsulation :** veut dire Suppression d'entêtes.

La figure suivante montre les étapes de l'encapsulation des données à travers les couches du TCP/IP :

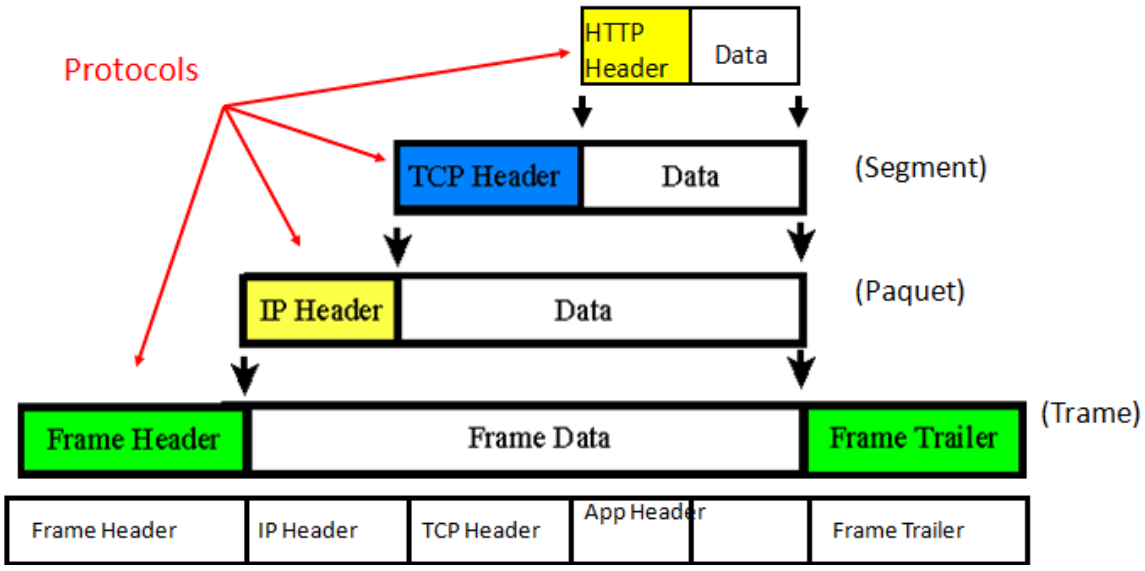


Figure -I.17- : encapsulation de données.

I.11. Adressage du réseau :

L'adressage est l'une des premières fonctions des protocoles de la couche réseau. Il permet de mettre en œuvre la transmission de données entre des hôtes situés sur un même réseau ou sur des réseaux différents.

Tous les périphériques appartenant à un réseau doivent être identifiés de manière unique. Au niveau de la couche réseau, les paquets de communication doivent être identifiés par les adresses source et de destination des systèmes des deux côtés. Avec l'adressage IPv4, cela implique que chaque paquet comporte, dans l'en-tête de la couche 3, une adresse source 32 bits et une adresse de destination 32 bits.

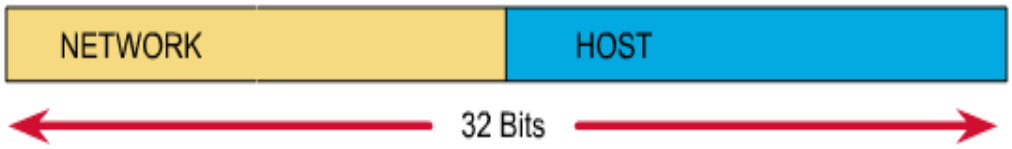
Une adresse IP a deux portions:

- **Adresse réseau** (Network) :

L'adresse qui fait référence au réseau. Tous les bits de la partie hôte sont mis à 0

➢ **Adresses d'hôte (**Host) :

Des adresses attribuées aux périphériques finaux sur le réseau. Les bits de la partie hôte sont formés par des 0 et des 1 (ne sont pas tous à 0, ne sont pas tous à 1).



Plages d'adresses :

Classe	adresses
A	0. 0. 0. 0 à 127. 255. 255. 255
B	128. 0. 0. 0 à 191. 255. 255. 255
C	192. 0. 0. 0 à 223. 255. 255. 255
D	224. 0. 0. 0 à 239. 255. 255. 255
E	240. 0. 0 .0 à 247. 255. 255. 255

Tableau -I.1- : plages d'adresses.

I.12. Les principaux protocoles de modèle TCP/IP :

I.12.1. Protocoles de couche application

➢ **Protocole DNS :** (Domain Name Service), est utilisé pour traduire les adresses Internet en adresses IP.

- **Protocole http :** (Hypertext Transfer Protocol), est utilisé pour transférer les fichiers qui constituent les pages du Web.

- **Protocole SMTP :** (Simple Mail Transfer Protocol), est utilisé pour transférer les courriels et les pièces jointes.

- **Protocole Telnet :** protocole d'émulation de terminal, est utilisé pour permettre un accès distant aux serveurs et aux périphériques réseau.

- **Protocole FTP :** (File Transfer Protocol), est utilisé pour le transfert interactif de fichiers entre les systèmes.

I.12.2. Protocoles de couche transport

- **Protocole TCP : (**Transmission Control Protocol), il gère les conversations individuelles entre des serveurs Web et des clients Web.

  Divise les messages HTTP en parties de plus petite taille, appelées segments, pour les envoyer au client de destination.

  Il est responsable du contrôle de la taille et du débit d'échange de messages entre le serveur et le client, de la fiabilité (numéros de séquence en cas de pertes).

- **Protocole UDP :** (user datagram protocol) est un protocole simple, sans connexion, Il présente l'avantage d'imposer peu de surcharge pour l'acheminement des données. Les blocs de communications utilisés dans le protocole UDP sont appelés des datagrammes.

I.12.3. Protocole de couche internet :

- **Protocole IP : (**internet Protocol), il gère la fragmentation des données, ainsi qu'il achemine les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP.

- **Protocole ARP :** (address resolution Protocol), détermine l'adresse de couche liaison de données pour les adresses IP connues.

- **protocole RARP :** détermine les adresses réseau lorsque les adresses de couche liaison de données sont connues.

- **protocole ICMP :**(internet control message Protocol), fournit des fonctions de contrôle. Il est utilisé par les routeurs pour signaler une erreur.

- **Protocole IGMP :** Ce protocole permet au groupe de machines d'utiliser les ressources de réseau de façon efficace et optimale.

I.13. Discussion

Ce chapitre est consacré à l'étude générale sur les réseaux informatiques. Les réseaux peuvent être classifie selon leur taille, topologie, mode de connexion et leurs méthodes d'Accès, ainsi que les supports de transmission utilisés.

L'utilisation de réseaux d'ordinateurs partageant des serveurs apporte une grande souplesse. Pour les individus les réseaux permettent l'accès à de très nombreuses ressources.

II.1. Préambule :

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet.

La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques. Ce chapitre a pour but de présenter globalement la manière dont les "pirates et Hackers" opèrent afin de pénétrer les Systems informatiques en espérant qu'il aide à pallier `a ce type de problème de plus en plus fréquent.

Nous définissons dans ce chapitre le terme de sécurité des réseaux ainsi que les méthodes des attaques utilisées et comment se protéger contre elles tel que :
les pare-feux (en anglais « firewall »).

II.2. Définition :

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

La sécurité informatique inclue les bonnes pratiques pour protéger les ordinateurs et les données qui y sont stockées.

Dès lors qu'un ordinateur n'est pas isolé mais relié à une ou plusieurs machines via un réseau local ou internet, il devient vulnérable aux attaques.

Ces attaques peuvent survenir par le biais de problèmes de :

- Mise en œuvre (environnement de sécurité déficient) ;
- Authentification de l'utilisateur (contournement ou connexion forcée) ;
- Logiciel (erreurs, failles programmes, vers, virus, chevaux de Troie) ;
- Réseau (écoute, mascarade, attaques de routeurs) ;
- Matériel (failles ou défaillance des matériels).

II.3. Les causes de l'insécurité :

On distingue généralement deux types d'insécurités :

- l'état actif d'insécurité, c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur) ;

- l'état passif d'insécurité, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

II.4. Pourquoi les systèmes sont vulnérables

- La sécurité est chère et difficile. Les organisations n'ont pas de budget pour ça ;
- La sécurité ne peut être sûre à 100%, elle est même souvent inefficace ;
- La politique de sécurité est complexe et basée sur des jugements humains ;
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité ;
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence ;
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes (erreur humaine).

II.5. Pourquoi un système ne peut être sûr à 100%

Il est impossible de garantir la sécurité totale d'un système pour les raisons suivantes :

- Les bugs dans les programmes courants et les systèmes d'exploitation sont nombreux ;
- La cryptographie a ses faiblesses : les mots de passe peuvent être cassés ;
- Même un système fiable peut être attaqué par des personnes abusant de leurs droits.
- Plus les mécanismes de sécurité sont stricts, moins ils sont efficaces ;
- On peut s'attaquer aux systèmes de sécurité eux-mêmes…

II.6 Objectifs de la sécurité informatique :

La sécurité informatique vise généralement cinq principaux objectifs :

- L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information ;
- La non répudiation, permettant de garantir qu'une transaction ne peut être niée ;
- L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

II.7 Les champs d'application de la sécurité informatique :

Ces objectifs s'appliquent dans différents domaines ou champs d'applications, chacun faisant appel à des techniques différentes pour atteindre le ou les mêmes objectifs; ces champs sont:

- la sécurité physique ;
- la sécurité personnelle ;
- la sécurité procédurale (audit de sécurité. procédures informatiques...) ;
- la sécurité des émissions physiques (écrans, câbles d'alimentation, courbes de consommation de courant...) ;
- la sécurité des systèmes d'exploitation ;
- la sécurité des communications.

II.8. Terminologie de la sécurité informatique :

La sécurité informatique utilise un vocabulaire bien défini que nous utilisons dans ce chapitre. De manière à bien comprendre ce chapitre, il est nécessaire de définir certains termes :

II.8.1. Le risque :

Le risque en termes de sécurité est généralement caractérisé par l'équation suivante :

$$Risque = \frac{Menace * Vulnérabilité}{Contre\ menace}$$

II.8.2. Les menaces :

L'ensemble des actions de l'environnement d'un système pouvant entraîner des pertes financières.

II.8.2.a. Types de menaces :

- **Les menaces non intentionnelles :**

- Pannes ou dysfonctionnements du Matériel ;
- Pannes ou dysfonctionnements du logiciel de base ;
- Erreurs d'exploitation (oubli de sauvegarde, écrasement de fichiers) ;
- Erreurs de manipulation des informations (erreur de saisie, erreur de transmission, erreur d'utilisation) ;
- Erreurs de conception des applications ;
- Erreurs d'implantation.

- **Les menaces intentionnelles :**

L'ensemble des actions malveillantes (qui constituent la plus grosse partie du risque). Qui devraient être l'objet principal des mesures de protection.

- **Menaces passives :** détournement des données (l'écoute, les indiscrétions).

Exemples :

- Espionnage industriel ;
- Espionnage commercial ;
- violations déontologiques ;
- Détournement des logiciels (Exemple: copies illicites).

- **Menaces actives :**

  - Modifications des informations (la fraude financière informatique, le sabotage des informations logique) ;
  - Modification des logiciels **(**Bombes logiques, virus, ver….).

II.8.2.b. Méthodes utilisées pour les attaques :

- La négligence interne des utilisateurs vis à vis des droits et autorisations d'accès ;
- Se faire passer pour un ingénieur pour obtenir des infos comme le mot de passe ;
- Beaucoup de mot de passe sont vulnérables à une attaque systématique ;
- Les clefs de cryptographie trop courtes peuvent être cassées ;
- L'attaquant se met à l'écoute sur le réseau et obtient des informations ;
- IP spoofing : changer son adresse IP et passer pour quelqu'un de confiance ;
- Injecter du code dans la cible comme des virus ou un cheval de Troie ;
- Exploitation des faiblesses des systèmes d'exploitation, des protocoles ou des applications.

II.8.2.c. Outils des attaquants :

- Programmes et scripts de tests de vulnérabilité et d'erreurs de configuration ;
- Injection de code pour obtenir l'accès à la machine de la victime (cheval de Troie) ;
- Echange de techniques d'attaques par forums et publications ;
- Utilisation massive de ressources pour détruire des clefs par exemple ;
- Les attaquants utilisent des outils pour se rendre anonyme et invisible sur le réseau.

II.8.3. Les vulnérabilités :

Ces sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

II.8.4. Les contre-mesures :

Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).

II.9. Pourcentages des différentes causes de pertes :

- Actions malveillantes **61%** (en croissance)
- Risques accidentels **24%**
- Pannes et erreurs **12%**
- Autres **3%**

II.10. Étapes de la sécurité informatique :

II.10.1 Analyse de risques :

- Identification des menaces potentielles et des risques encourus ;
- Estimation de leur probabilité ;
- Etude de leur impact.

II.10.2. Politique de sécurité :

La politique de sécurité définit les objectifs de sécurité et le plan d'actions pour maintenir un certain niveau de sécurité des systèmes informatiques d'une organisation.

- Elaboration des règles et des procédures techniques ou organisationnelles à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Détermination des moyens de protection :
  - Identification, authentification ;
  - Politiques d'autorisations et privilèges ;
  - Gestion des droits et des privilèges ;
  - Contrôles d'accès logiques et physiques ;
  - Profils de protection, classes de fonctionnalités ;
  - Évaluation, certification, accréditation, agrément, …
  - Journalisation ("audit") des événements liés à la sécurité.
- Planification d'une stratégie de sauvegarde ;
- Elaboration d'un plan de crise (au cas où ...) ;
- Elaboration d'un plan de reprise après incident ;
- Evaluation régulière du dispositif de sécurité mis en place ;
- Surveillance et détection des vulnérabilités du système d'information ;
- Veille concernant les failles logicielles et matérielles afin d'être en mesure de les parer ;
- Sensibilisation des utilisateurs à la sécurité informatique.

II.11. Techniques de sécurisation :

II.11.1. Sécurité physique :

Sécurité des infrastructures matérielles : salles sécurisées, lieux ouverts au public, postes de travail des personnels, etc.

II.11.2 Sécurité logicielle : (Sécurité des données)

Sécurisation des serveurs, des stations de travail. Chiffrement des données, authentification, contrôle d'accès.

II.11.3 Sécurité des réseaux :

Protection et configuration de l'infrastructure réseau (routeurs et Switchs). Pare-feu, IDS (Systèmes de détection d'intrusion).

II.12. Pare-feu :

II.12.1. Pourquoi un firewall ? :

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

Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une tel architecture est basé sur un firewall. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas, le meilleur exemple étant le jeu en ligne. En plaçant un firewall limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

II.12.2. Définition :

Il s'agit d'un dispositif de protection entre un réseau local et un autre réseau qui peut être un autre réseau local ou internet.
Un pare-feu vise principalement 2 objectifs :

- ✓ contrôler et protéger les hôtes du réseau local contre la divulgation non autorisé d'informations, les virus, les chevaux de Troie… ;

- ✓ protéger les serveurs internet contre des commandes jugées dangereuses pour les serveurs tels que "Telnet" ou contre les modifications ou l'altération de données sur le serveur ;

Un pare-feu est également un assemblage d'une partie matérielle (ordinateur) et d'un ou plusieurs logiciels installés sur cette machine.

II.12.3. Le possible et l'impossible de pare-feu :

II.12.3.a. Ce que peut faire un pare-feu :

- ✓ Etre un guichet de sécurité: un point central de contrôle de sécurité plutôt que de multiples contrôles dans différents logiciels clients ou serveurs ;
- ✓ Appliquer une politique de contrôle d'accès ;
- ✓ Enregistrer le trafic: construire des journaux de sécurité ;
- ✓ Appliquer une défense en profondeur (multiples pare-feux).

II.12.3.b. Ce que ne peut pas faire un pare-feu :

- o Protéger contre les utilisateurs internes (selon leurs droits) ;
- o Protéger un réseau d'un trafic qui ne passe pas par le pare-feu (exemple de modems additionnels) ;

- Protéger contre les virus ;
- Protéger contre des menaces imprévues (hors politique) ;
- Etre gratuit et se configurer tout seul.

II.12.4. Architecture usuelle :

Il existe deux principales architectures : simple et complexe (ou sensible)

II.12.4.a. Architecture simple :

L'architecture simple est représentée ci-dessous. Le réseau local est protégé par un filtre de paquets placé en coupure.

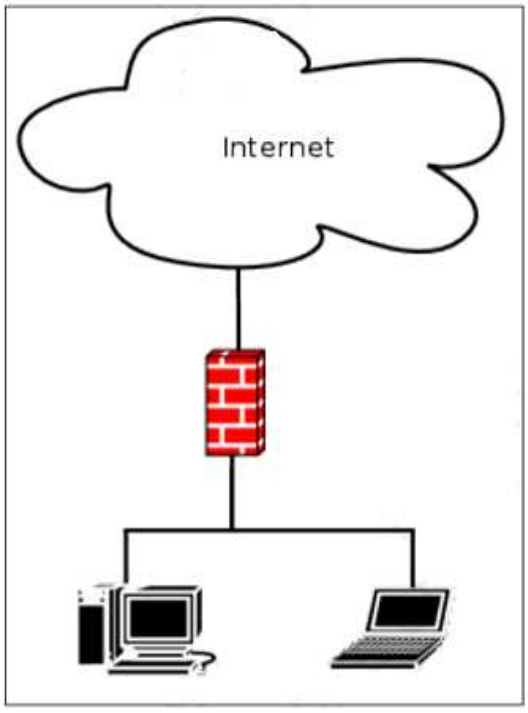


Figure -II.1- : architecture simple.

II.12.4.b. Architecture sensible :

L'architecture sensible est représentée ci-dessous :

Cette architecture est plus compliqué par apport à celle de l'architecture simple, mais a des avantages tel que :

- Filtrage des connexions ;
- Analyse des flux à la recherche de codes malicieux ;
- Mise en cache des documents les plus demandés.

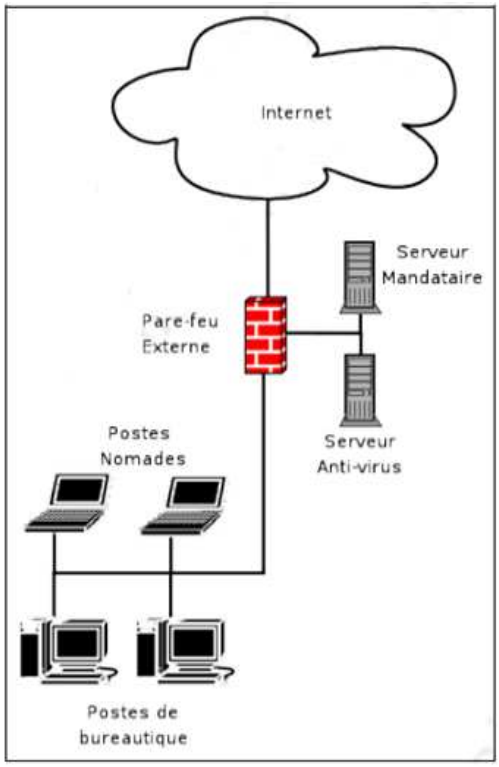


Figure -II.2- : architecture sensible.

II.12.5. Principes de fonctionnement :

Un firewall agit sur un ensemble des règles définies correctement par un utilisateur se basant généralement sur le principe suivant : **Tout ce qui n'est pas explicitement autorisé est interdit.** Cela signifie que les règles constituant une partie de la configuration du firewall doivent explicitement autoriser une action ou un flux de données pour que la connexion puisse établir.

II.12.5.a. Filtrage de paquets :

Internet et les réseaux fonctionnent par envoi/réception de blocs de données appelées « paquets ». Un firewall analyse chacun de ces paquets sur base d'un certain nombre de caractéristiques définies dans les règles. Un firewall fonctionnant sur le principe du filtrage de paquets analyse les en-têtes des paquets échangés entre deux ordinateurs en considérant les éléments suivants :

- L'adresse IP de la machine émettrice ;
- L'adresse IP de la machine réceptrice ;
- Le type de paquet TCP, UDP, ICMP ou IP ;
- Le service ou port demandé.

Le tableau ci-dessous montre un exemple de configuration d des règles d'un firewall :

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

Tableau -II.1- : configuration d'un pare-feu.

II.12.5.b. Filtrage de contenu :

Certains firewalls permettent en plus du filtrage de paquets d'analyser et de filtrer les données contenues dans les paquets. Cela permet dans certains cas de :

- ✓ empêcher la consultation de sites web Internet interdits ;
- ✓ empêcher le téléchargement de fichiers ou logiciels malicieux ;
- ✓ empêcher l'envoi et la réception par e-mail de fichiers potentiellement dangereux.

En plus des fonctionnalités énoncées ci-dessus, certains firewalls vérifient même que le contenu applicatif du trafic traversant le firewall (protocole applicatif utilisé, instructions, codification, …) correspond effectivement au protocole applicatif attendu. Ceci permet d'éviter par exemple qu'un cracker accède à un cheval de Troie en utilisant un autre protocole applicatif à travers le port 80 (http).

La figure suivante montre le principe fonctionnement du pare-feu :

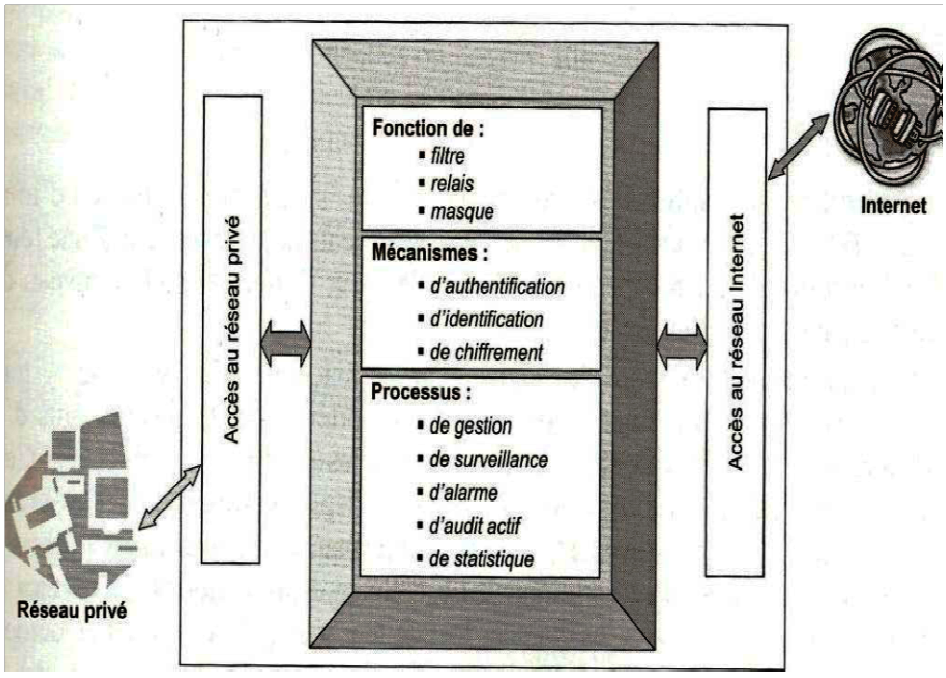


Figure -II.3- : principe de fonctionnement de pare-feu.

II.12.6. Les différents types de firewall :

On distingue deux différents types de firewall :

- les firewalls logiciels ;
- les firewalls matériels.

II.12.6.a. Les pare-feux logiciels :

Présents à la fois dans les serveurs et les machines, on peut les classer en plusieurs catégories :

- **Les firewalls personnels**

Ils sont pour la plupart commerciaux et ont pour but de sécuriser un ordinateur particulier. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, pour rester accessible à l'utilisateur final, ils s'orientent plus vers la simplicité d'utilisation, et donc mettent de côté l'aspect technique.

Ces pare-feux ont plusieurs avantages : ils apportent une sécurité en bout de chaîne (au niveau de la machine cliente), et sont pour la plupart assez facilement personnalisable.

Comme tous produits, ils ont aussi des inconvénients : ils sont assez facilement contournable par des pirates, et compte tenue de leur grand nombre, un classement est impossible.

- **Les firewalls plus « sûre »**

Ils se trouvent généralement sous Linux, car ce Système d'Exploitation offre une sécurité réseau plus élevée et aussi un contrôle plus précis. Ils ont généralement le même comportement que les firewalls matériels des routeurs, à la seule différence qu'ils sont configurables à la main.

Le firewall le plus courant est « iptables », qui utilise directement le noyau Linux. Toutes les fonctionnalités des firewalls de routeurs sont réalisables sur cette plateforme.

Il existe des distributions Linux permettant de transformer un ordinateur en pare-feu dédié et complet, que l'on considèrera par la suite comme pare-feu matériel.

On peut citer par exemple : Smoothwall, IPCop et Endian Firewall, qui sont dérivés du package « Netfilter ».

II.12.6.b. Les pare-feux matériels :

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel.

Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en terme de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur.

II.12.7. Les différents types de filtrage :

II.12.7.a. Filtrage de paquets :

- **Le filtrage simple de paquets :**

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « stateless packet filtering »). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

- **Le filtrage dynamique :**

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglo-saxon est « stateful inspection » ou « stateful packet filtering », traduisez « filtrage de paquets avec état ».

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

II.12.7.b. <u>Le filtrage applicatif</u> :

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage

applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).

Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou « proxy »), car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission.

II.13. Discussion :

La sécurité d’un réseau est extrêmement importante au sein d’une entreprise. C’est pourquoi, la mise en place de solutions de protection, de surveillance tels que pare-feux, antivirus, …, permet de répondre à ce besoin de sécurisation.

La sécurité ne révèle sa valeur qu'en cas de problème. Fort de ce constat, il vaut mieux appliquer de la sécurité avant d'être attaqué afin de, au minimum limiter les dégâts. Après, il sera trop tard.

III.1. Préambule:

Smoothwall est un projet qui a été initié au Royaume-Uni à l'été 2000 par Lawrence Manning (principal développeur de code) et Richard Morrell (Manager du projet). Leur idée de base était de créer une distribution Linux qui pouvait convertir un ordinateur personnel en un équipement pare-feu. Avec l'aide d'autres contributeurs comme John Faulty et Tom Ellils.

Cette distribution a été développée à partir de RedHat linux (devenu plus tard Fedora Project) en vue d'un usage facile qui ne nécessite aucune connaissance en Linux.

En effet, Smoothwall Express est totalement administrable via une interface WEB. Il permet de sécuriser les échanges entre Internet et le réseau interne de l'entreprise quel que soit son architecture (nous verrons plus loin dans ce chapitre les architectures possibles à configurer via Smoothwall Express).

III.2. Définition :

Smoothwall est un système de distribution de pare-feu d'exploitation basé sur Linux établi pour courir comme firewall/router consacré. Employer le smoothwall est une grande manière de gagner des possibilités supplémentaires. Smoothwall est fortement stable, fonctionne sur une variété de matériel. Il emploie IPTABLES pour commander et conduire le trafic.

III.3. Exigences matérielles pour installer SmoothWall :

La configuration nécessaire à l'installation de Smoothwall dépend du nombre de machines connectées en même temps et des services utilisés. Il nécessite un environnement comportant les caractéristiques minimales suivantes pour être déployé:

Système/ matériel	Spécifications/ recommandations	
Processeur	Intel Pentium 200 ou processeur compatible.	
Mémoire	128 Méga Octets de RAM pour les fonctionnalités minimales	
Disque dur	2 Giga Octets – IDE et SCSI supportés.	
Clavier	Si le système de boot permet de démarrer sans clavier alors celui-ci n'est requis que pour le premier démarrage (Installation et configuration)	
Carte Vidéo	Requise seulement lors de l'installation	
Moniteur	Requis seulement lors de l'installation	
CD-ROM	Requise seulement lors de l'installation	
Lecteur Disquette	Recommandé pour une éventuelle mise à jour pour les vieilles versions	
Types de connections Internet	**Internet**	carte réseau (NIC) fonctionnelle
	ADSL	Support PCI ou modem USB requis
	RNIS	Une carte RNIS ou un port RS232 ou connecteur USB externe est requis
	Modem	Un modem, support RS232, ISA ou modem PCI
Cartes d'accès réseau	Au minimum un support d'une carte réseau. Selon le type de connexion vers Internet le nombre de carte réseaux requis sera augmenté	

Tableau -III.1- : Configuration minimale requise pour l'installation smoothwall.

Voici à titre indicatif quelques exemples :

- **Config minimum (jusqu'à 10 utilisateurs) :**
  - Processeur I386 min 90Mhz ;
  - Au moins 32Mb de RAM (64Mb recommandé) ;
  - Disque dur ide/scsi 1 Gb ;
  - Carte graphique compatible VGA ;
  - Carte réseau Ethernet ;
  - Connexion Internet (Modem, Câble, ISDN, ADSL,...).

- **Entre 10 et 40 utilisateurs :**
  - Processeur i386 min 400Mhz ;
  - Au moins 128Mb de RAM ;
  - Disque dur ide/scsi 20/40 Go.

- **Jusqu'à 500 utilisateurs :**
  - Processeur i386 min 700Mhz ;
  - Au moins 256Mb de RAM (512 recommandé) ;
  - 2 disques durs SCSI de grande capacité montés en RAID1.

III.4. Architectures possibles avec SmoothWall :

Avant d'aller plus loin, il est nécessaire de définir les termes interface Green, interface Red, interface Purple et interface Orange :

- **Interface Green (verte) :**

Désigne l'interface réseau (carte réseau) de Smoothwall qui sera directement reliée au réseau interne câblé de l'entreprise.

- **Interface Red (rouge) :**

Désigne l'interface de Smoothwall qui sera reliée à Internet.

- Interface **Purple (violet)** :

  Désigne l'interface réseau sans fil de Smoothwall.

- Interface **Orange (orange)** :

Désigne l'interface de Smoothwall qui sera reliée à la zone démilitarisée (partie du réseau de l'entreprise où l'on isole les serveurs). Cette zone est sauf exception câblée…

La figure suivante pourrait éclaircir encore plus sur la signification de ces différents termes :

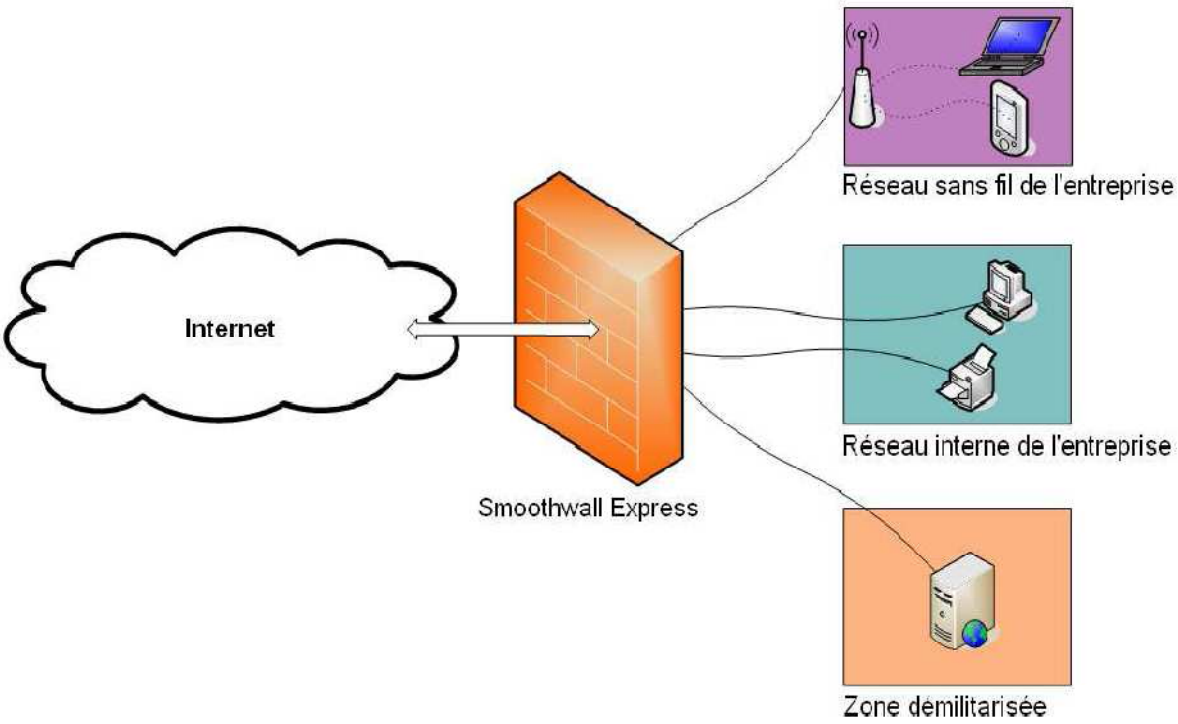


Figure -III.1- : Définition des interfaces Green, Red, Orange et Purple.

Voyons maintenant les architectures réseau qu'offre Smoothwall :

- **Architecture Green :**

Cette architecture est utilisée si Smoothwall devait utiliser une seule carte réseau qui sera reliée au réseau interne de l'entreprise.
L'interface rouge est dans cette configuration reliée directement à un modem (ou RNIS).

- **Architecture Green + Orange :**

Architecture basée sur deux cartes réseau. La première est utilisée pour relier le réseau interne de l'entreprise. La deuxième relie la zone démilitarisée. L'interface rouge est dans cette configuration aussi reliée directement à un modem/RNIS.

- **Architecture Green +Red :**

Smoothwall utilisera dans ce cas de figure une carte réseau pour se connecter au réseau interne et une autre pour relier Internet.

- **Architecture Green + Orange + Red :**

Cette architecture est choisie dans le cas où l'on utilise trois cartes réseau pour relier Smoothwall à la zone démilitarisée, le réseau interne et Internet.

- **Architecture Green + Purple (Red is modem/ISDN):**

Ici l'interface rouge est directement reliée à un modem/RNIS. Smoothwall sera en outre relié au réseau interne de l'entreprise via une carte réseau (généralement une carte Ethernet) et au réseau sans fil de l'entreprise via une carte réseau sans fil.

❖ **Architecture Green + Purple + Orange :**

Smoothwall propose cette architecture afin de se connecter via trois cartes réseaux séparées aux : zones démilitarisée, réseau sans fil et réseau interne de l'entreprise. L'interface rouge est directement reliée à un modem/RNIS.

❖ **Architecture Green + Purple + Red :**

Ici on utilise deux cartes réseaux pour câbles (afin de relier le réseau interne de l'entreprise et Internet à Smoothwall) et une carte réseau sans fil pour connecter le réseau sans fil de l'entreprise au pare-feu.

❖ **Architecture Green + Purple + Orange + Red :**

Cette configuration réseau utilise trois cartes réseaux pour câbles (afin de relier le réseau interne de l'entreprise, la zone démilitarisée et Internet à Smoothwall) et une carte réseau sans fil pour connecter le réseau sans fil de l'entreprise au pare-feu.

Smoothwall offre donc 8 configurations réseau possibles. L'une de ces configurations devra être choisie et traitée lors de l'installation.

III.5. Services par défaut offerts par SmoothWall :

Les fonctionnalités assurées par défaut par Smoothwall sont les suivantes :

- ✓ Possibilité d'administration via une interface web ;
- ✓ Consultation de l'état de la machine sur laquelle est installé le pare-feu (état de la mémoire et les disques durs) ;
- ✓ supervision du trafic réseau en temps réel sur les différentes cartes ;
- ✓ services de proxy web, SIP, POP3, IM ;
- ✓ Service DHCP ;
- ✓ service DNS (statique et dynamique) ;
- ✓ service de temps NTP ;

- ✓ accès distant via SSH ;
- ✓ système de détection d'intrusions ;
- ✓ VPN IPSec ;
- ✓ filtrage (par état) ;
- ✓ NAT ;
- ✓ priorité de trafic et QoS ;
- ✓ consultation de différents types de logs ;
- ✓ possibilités de maintenance (mise à jour du système ou de pilotes, backup, add on…).

Plusieurs autres fonctionnalités peuvent être ajoutées via des adds-on.

III.6. Politique de pare-feu par défaut pour SmoothWall :

Quand on démarre la machine Smoothwall pour la première fois (mode console) et qu'on tape la commande shell : iptables –L, nous aurons la liste des règles par défaut du pare-feu. La politique par défaut est la suivante:

Chain INPUT (policy DROP) :

Tout le trafic entrant vers la machine Smoothwall est rejeté.

Chain OUTPUT (policy ACCEPT) :

Le trafic sortant de la machine Smoothwall est autorisé.

Chain FORWARD (policy DROP) :

Le trafic transitant par la machine Smoothwall est rejeté.

Nous présentons dans ce qui suit le résultat complet de la commande iptables –L :

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ipblock    0    --  anywhere             anywhere
ipblock    0    --  anywhere             anywhere
ipblock    0    --  anywhere             anywhere
advnet     0    --  anywhere             anywhere
advnet     0    --  anywhere             anywhere
advnet     0    --  anywhere             anywhere
spoof      0    --  anywhere             anywhere
spoof      0    --  anywhere             anywhere
spoof      0    --  anywhere             anywhere
timedaccess  0    --  anywhere             anywhere
ACCEPT     0    --  anywhere             anywhere
ACCEPT     0    --  anywhere             anywhere
secin      0    --  anywhere             anywhere
block      0    --  anywhere             anywhere
LOG        0    --  anywhere             anywhere            LOG level warning
REJECT     0    --  anywhere             anywhere            reject-with icmp-po
rt-unreachable

Chain FORWARD (policy DROP)
target     prot opt source               destination
ipblock    0    --  anywhere             anywhere
ipblock    0    --  anywhere             anywhere
--More--(20%)
ipblock    0    --  anywhere             anywhere
secout     0    --  anywhere             anywhere
ACCEPT     0    --  anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     0    --  anywhere             anywhere            state RELATED,ESTAB
LISHED
outbound   0    --  anywhere             anywhere            state NEW
ACCEPT     0    --  anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     0    --  anywhere             anywhere            state RELATED,ESTAB
LISHED
outbound   0    --  anywhere             anywhere            state NEW
ACCEPT     0    --  anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     0    --  anywhere             anywhere            state RELATED,ESTAB
LISHED
outbound   0    --  anywhere             anywhere            state NEW
portfwf    0    --  anywhere             anywhere
ACCEPT     0    --  anywhere             anywhere
ACCEPT     0    --  anywhere             anywhere
MINIUPNPD  0    --  anywhere             anywhere
MINIUPNPD  0    --  anywhere             anywhere
MINIUPNPD  0    --  anywhere             anywhere
LOG        0    --  anywhere             anywhere            LOG level warning
--More--(48%)
REJECT     0    --  anywhere             anywhere            reject-with icmp-po
rt-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain MINIUPNPD (3 references)
target     prot opt source               destination

Chain advnet (3 references)
target     prot opt source               destination

Chain allows (1 references)
target     prot opt source               destination

Chain badtraffic (1 references)
target     prot opt source               destination

Chain block (1 references)
target     prot opt source               destination
ACCEPT     0    --  anywhere             anywhere            state RELATED,ESTAB
LISHED
ACCEPT     0    --  anywhere             anywhere
xtaccess   0    --  anywhere             anywhere
--More--(52%)
```

Afin de changer les règles de pare-feu, il faut utiliser la commande iptables avec les options adéquates. Une aide sur iptables est disponible sur linux en tapant directement man iptables.

III.7. Application :

III.7.1. Présentation :

Basé principalement sur la mise en place et sécurité des réseaux locaux (LANs), ce travail nous a permis de développer nos connaissances en matière de réseaux informatiques. Ayant jusqu'à présent principalement basé nos études sur le smoothwall, il nous a semblé important de nous mettre en contact de manière plus directe avec d'autres aspects de l'informatique, afin de découvrir une nouvelle approche de la matière et mieux cerner les besoins des utilisateurs.

III.7.2. Objectif :

L'élément central de ce travail reste, bien entendu, sécurité réseau LAN. Toutes les tâches que nous allons réaliser sont fortement liées au réseau informatique, à son déploiement, son organisation et son administration. L'idée générale est de permettre au client, à l'entreprise (réseau LAN), de pouvoir partager ses informations, ses données et ses moyens informatiques en toute sécurité afin d'améliorer sa réactivité, sa compétitivité et ainsi devenir une « entreprise connectée ».

III.7.3. Cahier de charge :

Pour la réalisation de notre travail, on dispose les paramètres suivants :

III.6.3.a. Paramètres physique :

- 07 Ordinateurs Windows (clients) ;
- 01Commutateur (Switch) ;
- Unité centrale sur laquelle on installe le smoothwall ;
- Deux cartes réseau Ethernet.

III.7.3.b. Paramètres logiciels :

- Système d'exploitation Windows XP sur les postes clients ;
- Antivirus ;
- Smoothwall.

III.7.4. Mise en place d'un réseau local :

Il y a plusieurs façons de mettre en place un réseau d'entreprises (LAN), selon leurs architecture (client/serveur, client/client) et leurs topologie (bus, étoile, anneau,….).

Dans notre projet, nous avons opté pour une architecture (client/serveur) et topologie en étoile.

Voici l'état de l'informatique avant la réalisation de notre projet :

- Le labo possédait 7 ordinateurs fonctionnant sous Windows XP ;
- Les ordinateurs étaient branchés en réseau par un connecteur RJ45 ;
- les ordinateurs (clients) étaient reliés par un Switch ;
- Un accès Internet était disponible ;
- Aucune sécurité Internet n'était disponible.

La figure suivante montre l'architecture du réseau de labo avant notre l'intervention :

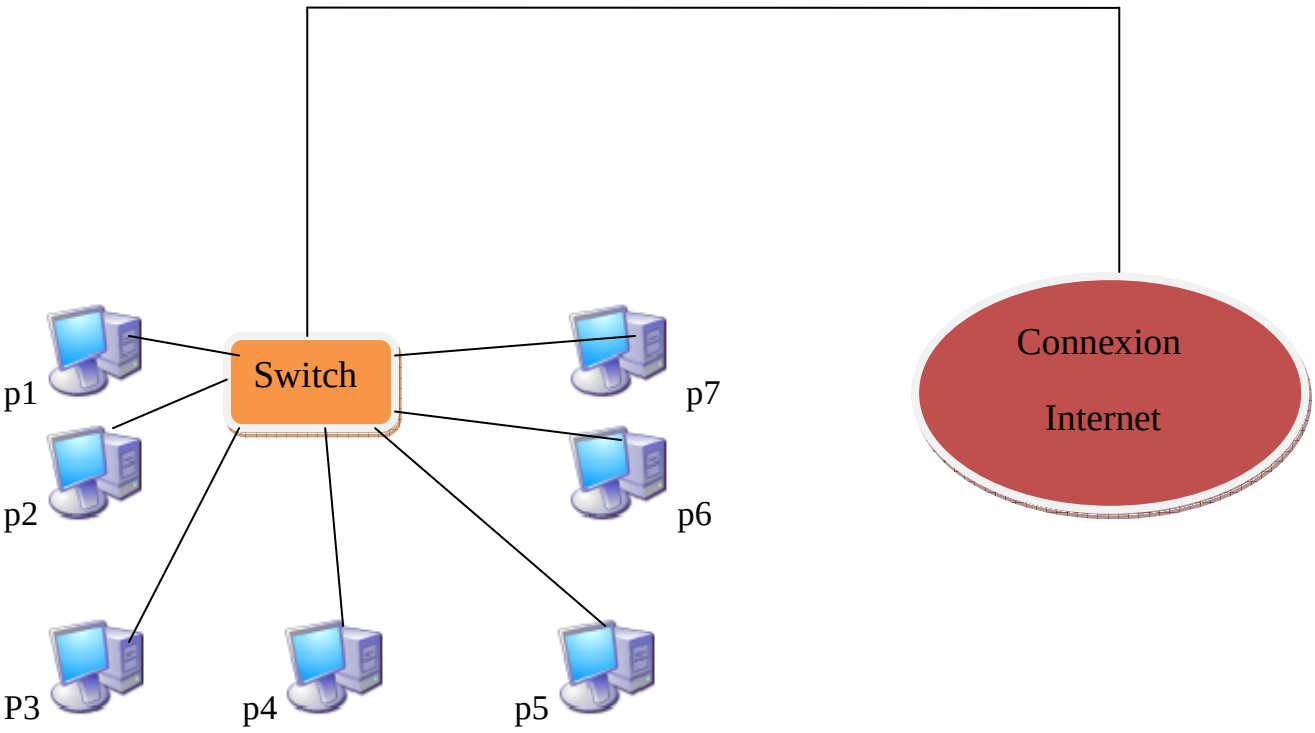


Figure -III.2- : Etat du réseau avant l'intervention.

Ce réseau n'est pas du tout sécurisé. L'un des nos objectifs est de lui sécuriser avec un coût minimal.

Adresses attribué pour les postes client :

Poste 1 : **192.168.0.2**

Poste 2 : **192.168.0.3**

Poste 3 : **192.168.0.4**

Poste 4 : **192.168.0.5**

Poste 5 : **192.168.0.6**

Poste 6 : **192.168.0.7**

Poste 7 : **192.168.0.8**

III.7.5. Solution proposée :

Notre contribution est de réaliser les opérations suivantes :

- ✓ Accès à Internet de manière sécurisée pour tous les ordinateurs du labo ;
- ✓ Organisation d'une architecture d'échange de données sur le réseau.

III.7.6. Mise en place de la solution :

La mise en place de la solution concernant l'accès à Internet de manière sécurisée par tous les ordinateurs du labo est de mettre une unité centrale possédant deux cartes réseaux sur laquelle on installe un smoothwall entre le réseau interne et le réseau externe (internet,…). Puisque le smoothwall représente un pare-feu logiciel qui protège le réseau local (LAN) contre les menaces et les intrusions provenant de l'extérieur.

Pour celui de l'organisation d'une architecture d'échange de données sur le réseau, on garde même architecture de celle précédente. En ajoutant un nouveau matériel (pare-feu) entre le réseau local et l'extérieur.

Voici la réorganisation du réseau après l'intervention sur la figure ci-dessous :

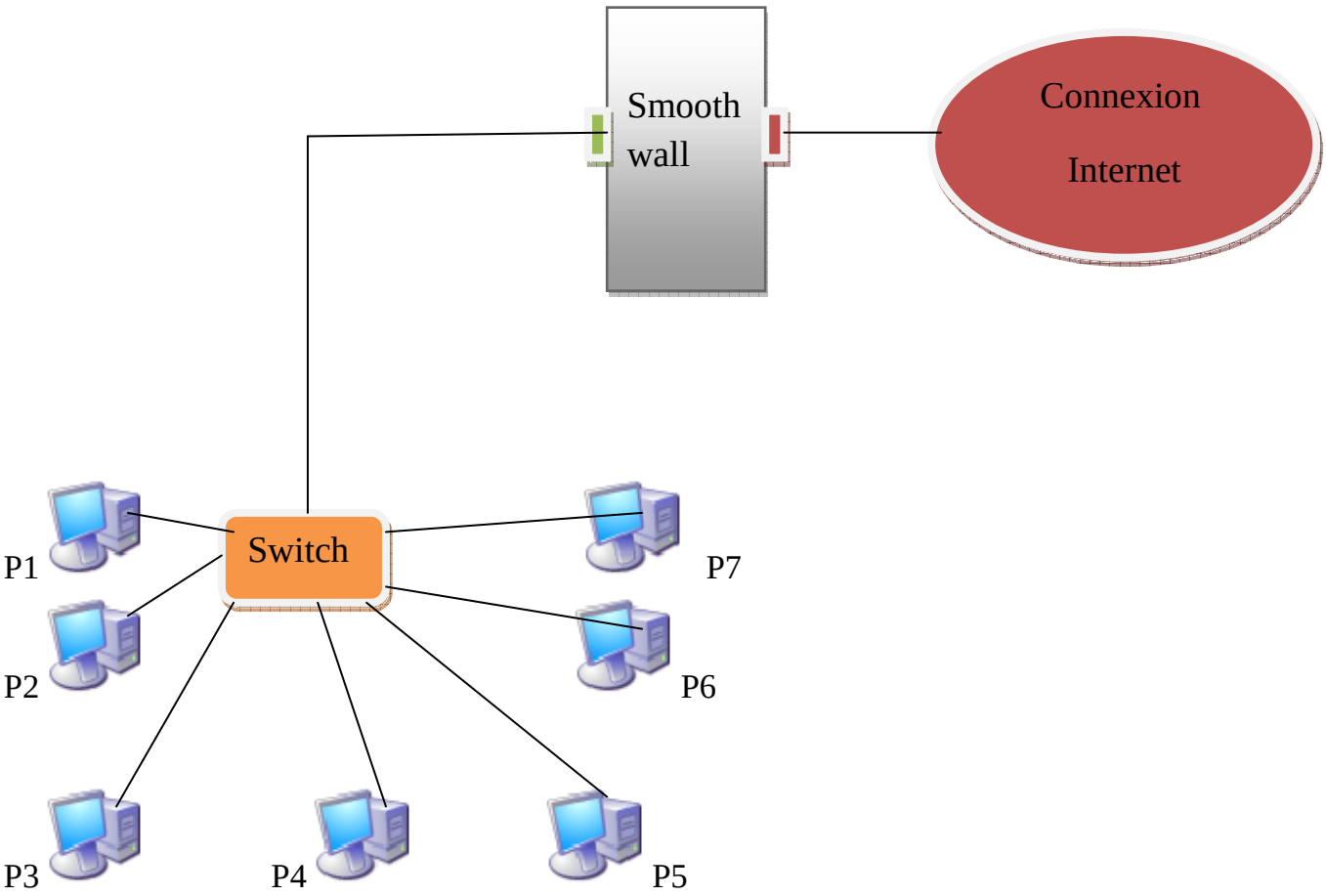


Figure -III.3- : Etat du réseau après l'intervention.

- **Adresses IP attribué pour les postes client :**

Poste 1 : **192.168.0.2**

Poste 2 : **192.168.0.3**

Poste 3 : **192.168.0.4**

Poste 4 : **192.168.0.5**

Poste 5 : **192.168.0.6**

Poste 6 : **192.168.0.7**

Poste 7 : **192.168.0.8**

- **Adresses IP attribué pour les cartes réseaux de SmoothWall :**

Carte verte : **192.168.72.142**

Carte rouge : à régler sur DHCP si l'adresse IP et l'adresse DNS sont fournies par fournisseur d'accès. Dans notre cas nous l'avons configuré automatiquement.

Jusque là on n'a pas encore abouti à notre objectif. Il nous reste la partie la plus importante qui est l'installation et la configuration de smoothwall.

Comme smoothwall c'est des versions, dans notre cas on a utilisé la version « smoothwall express 3 ».

Pour avoir ce dernier, Il faut d'abord télécharger l'image Iso (21 Mo environ) sur le site www.smoothwall.org , puis graver cette image sur un cdrom.

III.7.7. Installation et configuration :

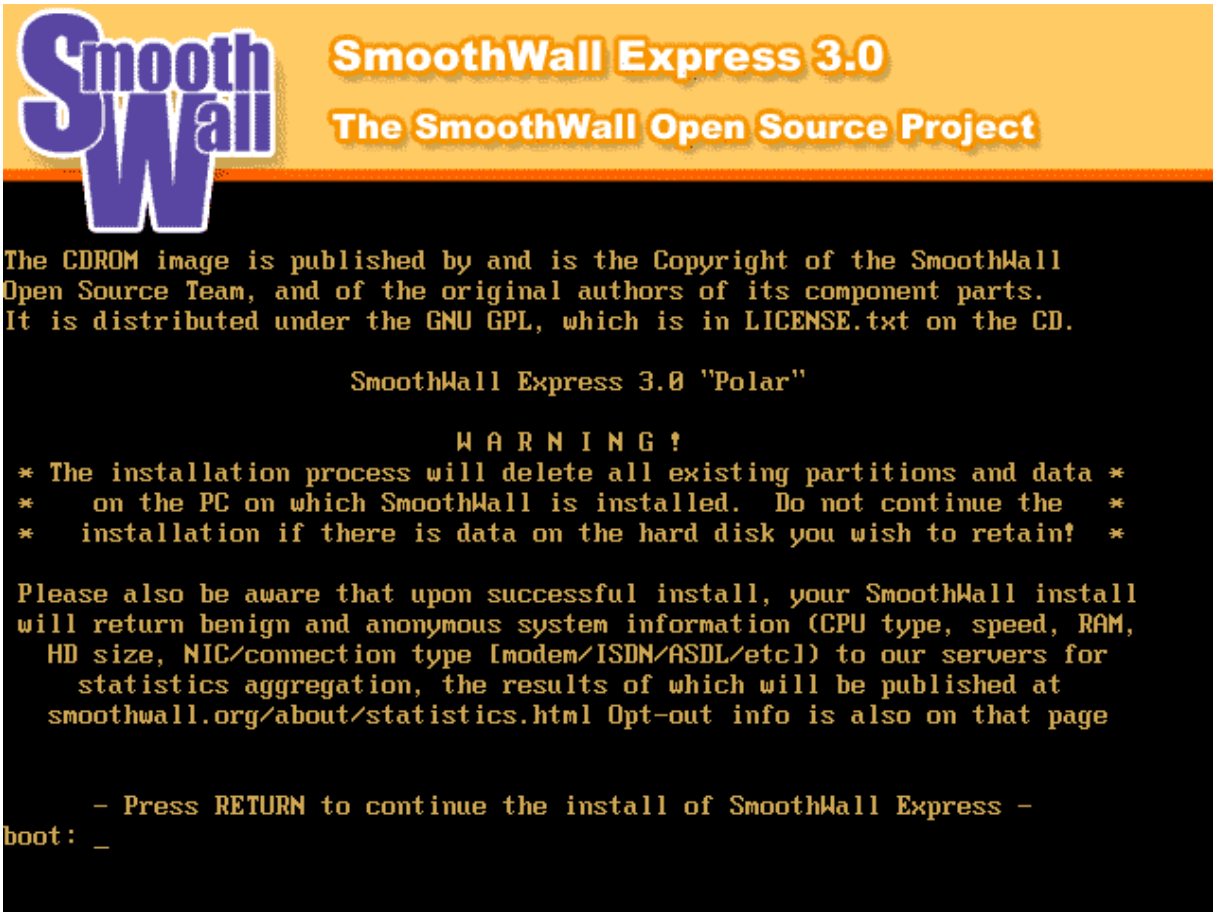
Pour installer Smoothwall, Il faut insérer le cdrom dans lecteur puis redémarrer la machine. Les étapes sont :

- Fenêtre de bienvenue ;
- Choix du mode d'installation (cdrom) ;

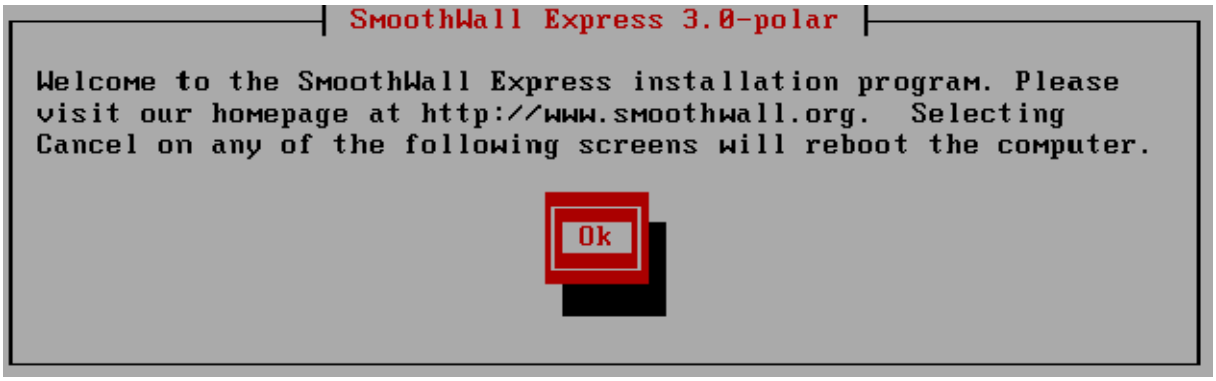
- Préparation du disque dur (partition et formatage : toutes les données présentes sur le disque sont effacées !) ;
- Configuration réseau (carte verte : IP statique 192.168.72.142) ;
- Installation de SmoothWall ;
- Configuration clavier (français) et zone horaire ;
- Hostname (exemple: master) ;
- Configuration ISDN (Choisir disable si vous n'utilisez pas ce mode de connexion à Internet) ;
- Configuration USB ADSL (idem) ;
- Configuration Ethernet.

Voici les étapes d'installation de smoothwall express 3 avec images :

Nous avons booté la machine avec le CD ROM que nous avons gravé, on a eu l'image suivante :

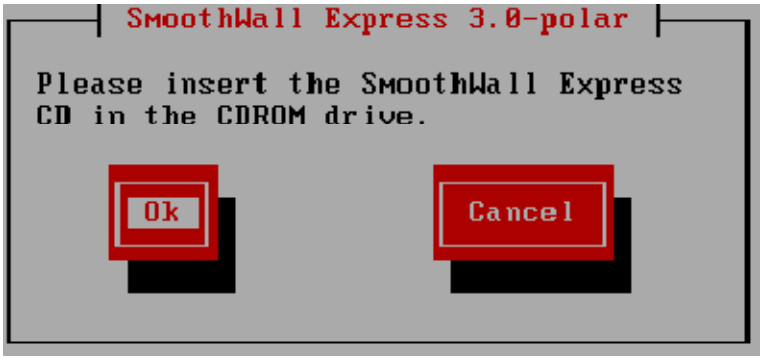


Après avoir lire les informations affichés, cliquer sur **ENTER.** La zone de dialogue suivante s'ouvre :

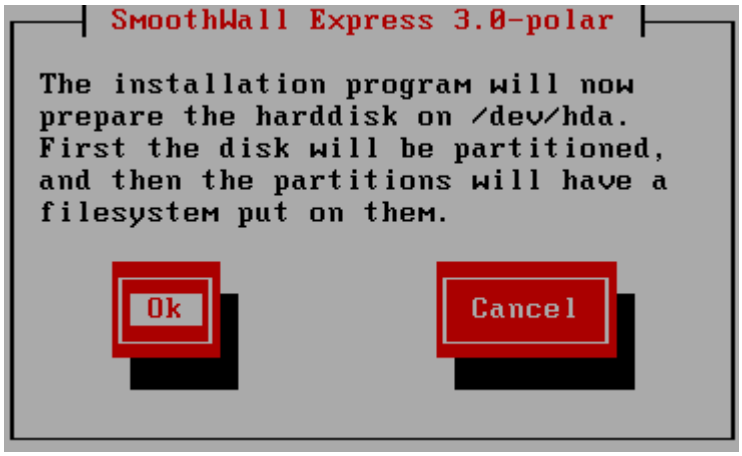


Cliquer sur OK pour continuer.

La zone de dialogue suivante s'ouvre :



Cliquer sur OK pour continuer. La zone de dialogue suivante s'ouvre :



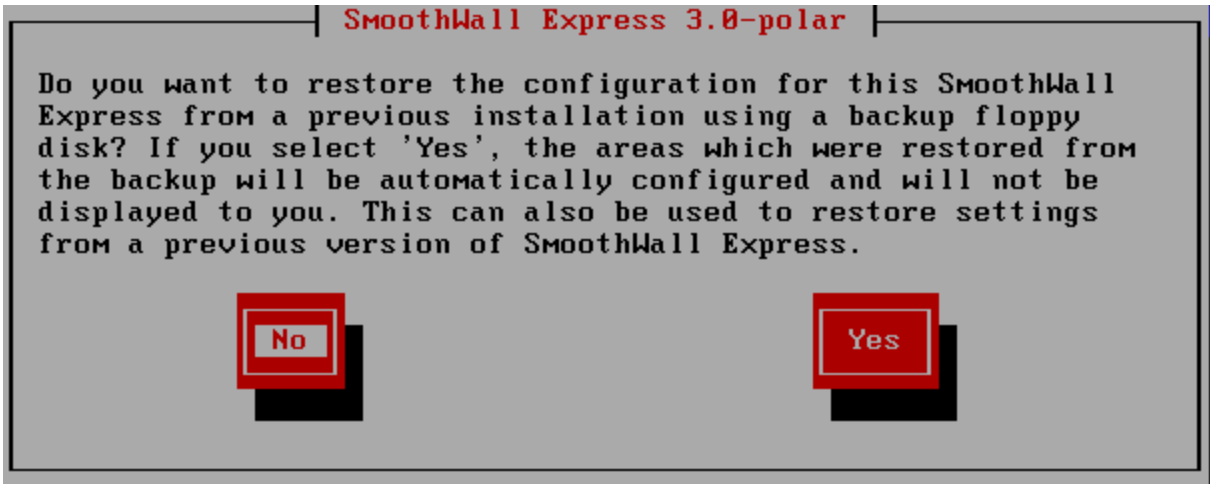
Cliquer sur OK pour continuer. La zone de dialogue suivante s'ouvre :

Remarque :

Le procédé d'installation **EFFACE TOUTES LES DONNÉES** à partir du disque dur du poste de travail. Cliquer sur OK pour confirmer. Des dossiers Express de SmoothWall sont installés. Si complet, félicitations !La zone de dialogue s'ouvre :

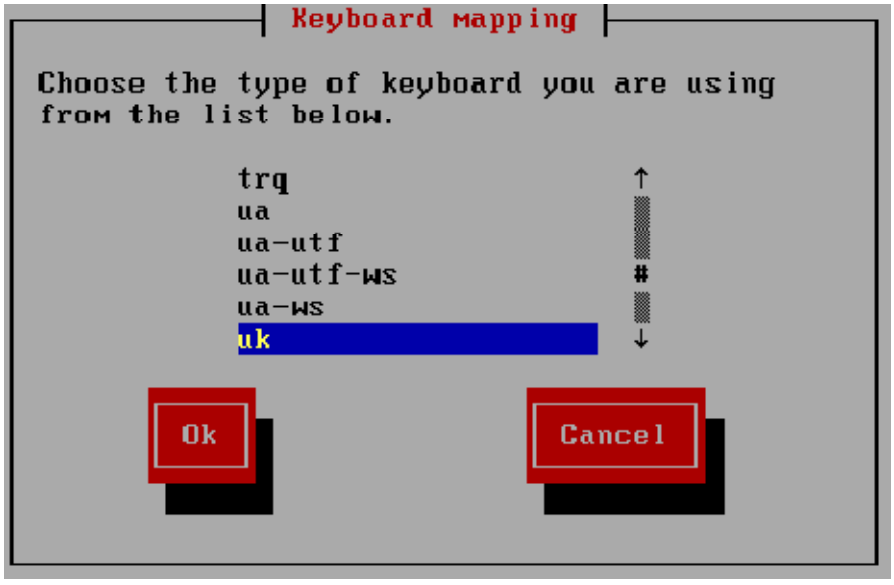
Cliquer sur OK.

La zone de dialogue suivante s'ouvre :

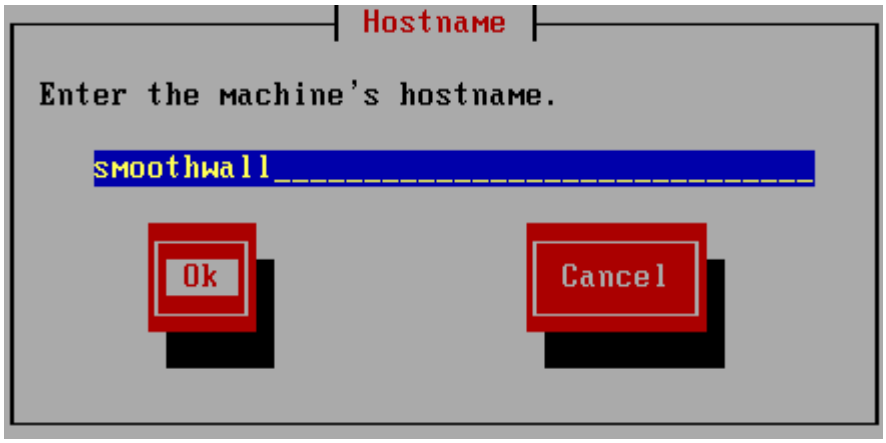


Si vous choisissez **YES**, vous accédez à la mise à niveau et les options de restauration pour SmoothWall. Dans notre cas on clique sur **NO** pour l'installer.

La zone de dialogue suivante s'ouvre :

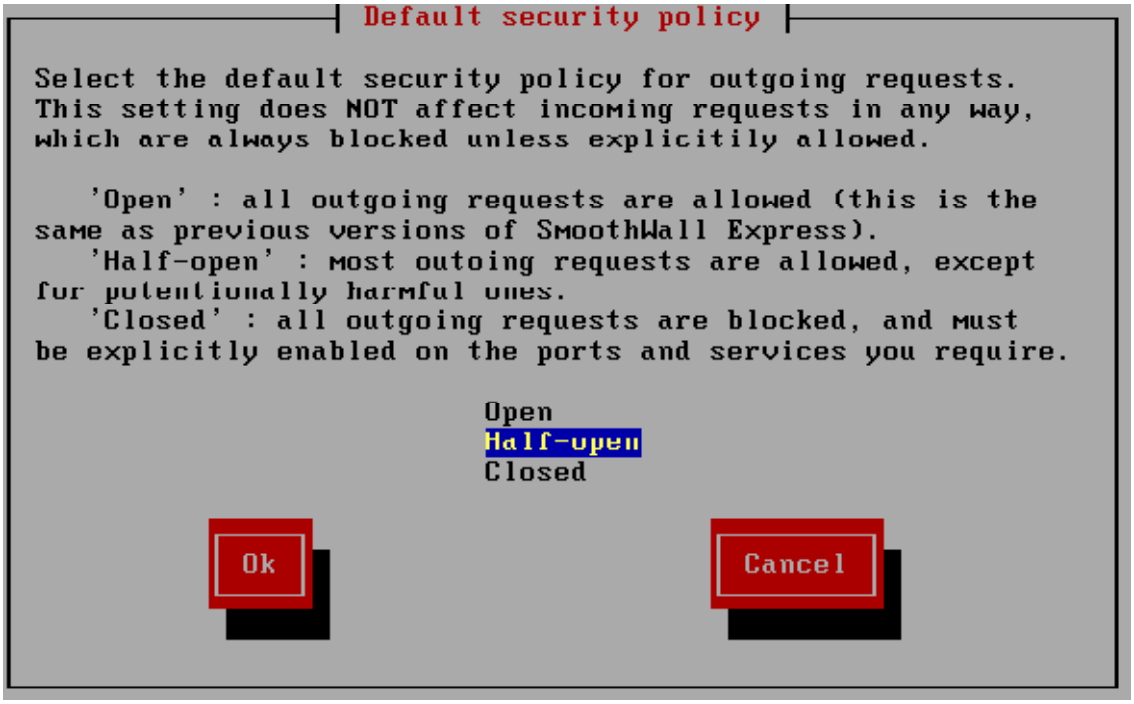


Choisir type de clavier, puis cliquer sur OK. La zone de dialogue de hostname s'ouvre :

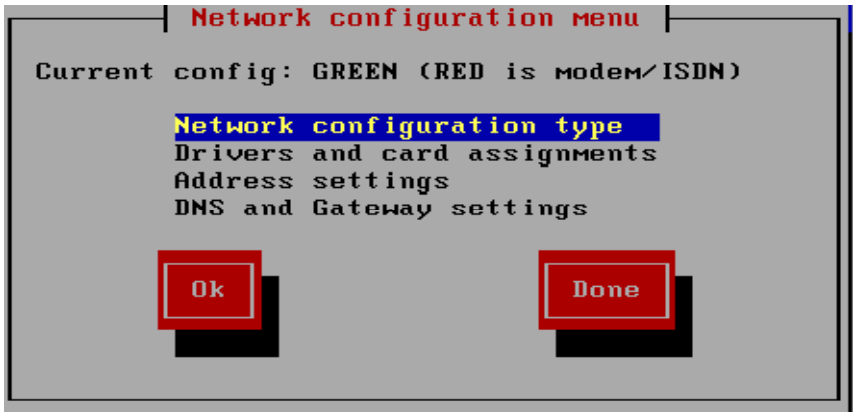


Donner un nom pour le smoothwall, puis cliquer sur OK

La zone de dialogue de politique de sécurité par défaut s'ouvre :

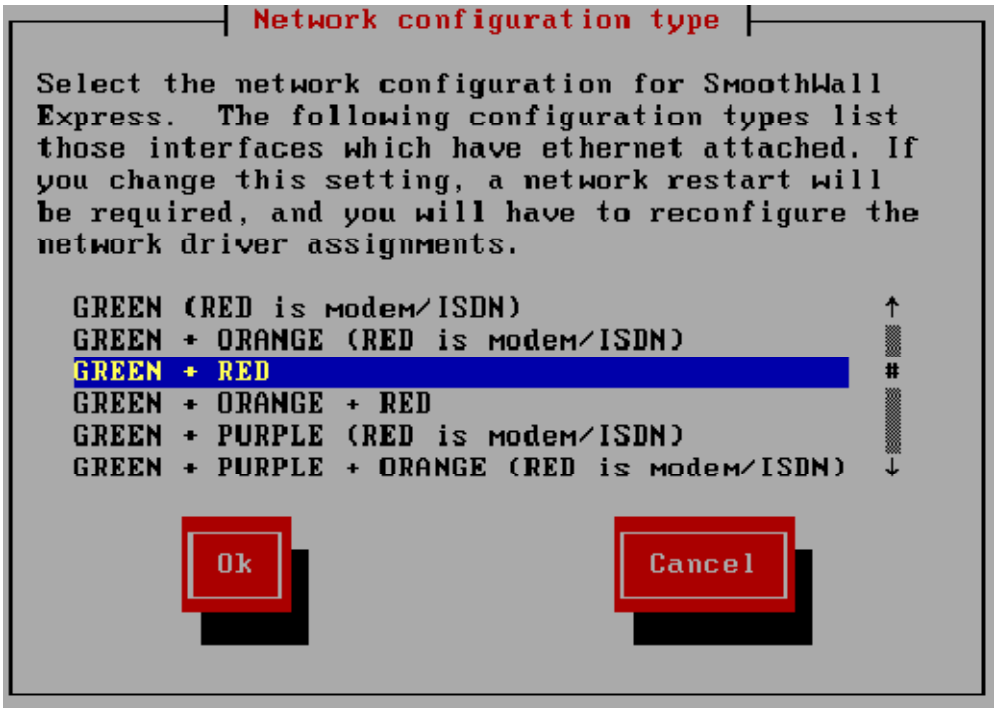


Dans notre travail nous avons choisi le half-open (laisse/bloque partiellement les requêtes Sortantes).En cliquant sur OK, le menu de configuration de réseau s'ouvre :



Choisir **Network configuration type** (type de configuration réseau), puis cliquer sur OK.

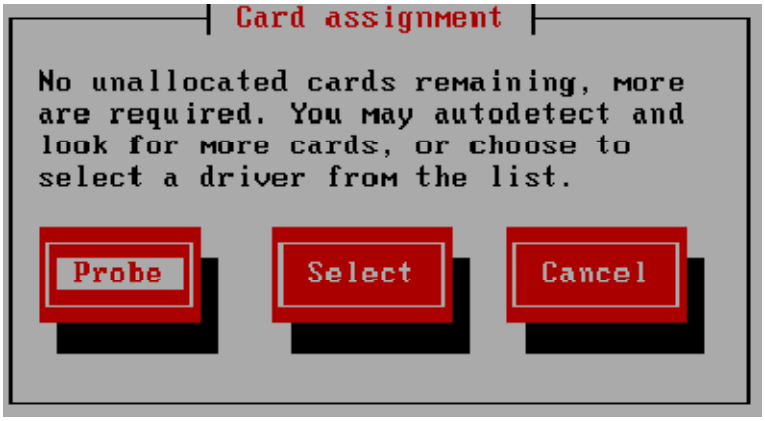
La fenêtre de type de configuration réseau s'ouvre :



Choisir **GREEN + RED** et cliquer sur OK. Taper sur la touche ENTRER. Pour qu'on revient au menu de configuration de réseau.

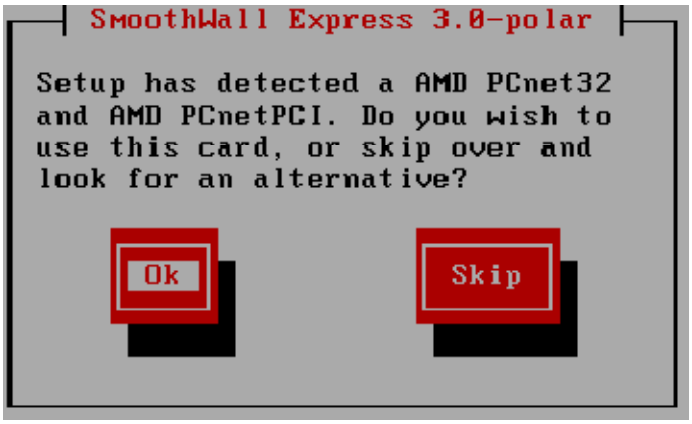
Dans le menu de configuration de réseaux, on sélectionne **Drivers and card assignments** puis ENTRER, La fenêtre suivante s'ouvre :

Cliquer sur OK puis ENTRER, une fenêtre de **Card assignment** s'ouvre :

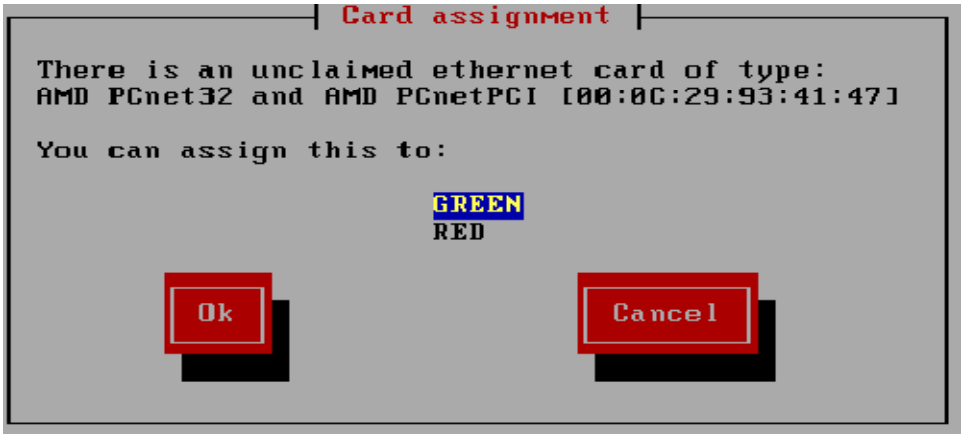


Choisir **Probe** et cliquer sur **entrer** pour détecter automatiquement les NICs (Network Interface Card).

L'information sur les cartes détectées est montrée :

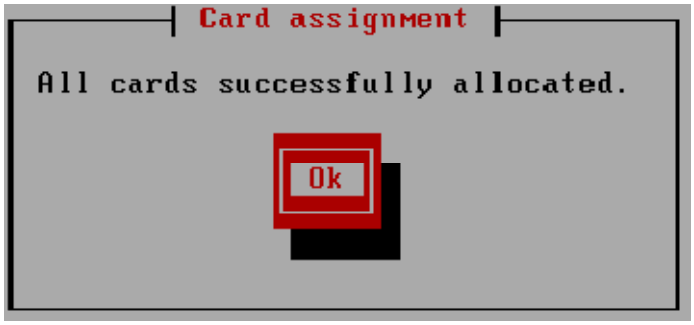


Sélectionner OK puis ENTRER pour continuer. La fenêtre de **Card assignment** s'ouvre :



Choisir **GREEN** et cliquer sur OK. Répéter les étapes ci-dessus pour la **RED**

La zone de dialogue suivante s'ouvre :



Cliquer sur OK pour revenir au menu de configuration de réseau. Sélectionner

Address settings et cliquer sur OK. La zone de dialogue d'affectation d'adresse s'ouvre :

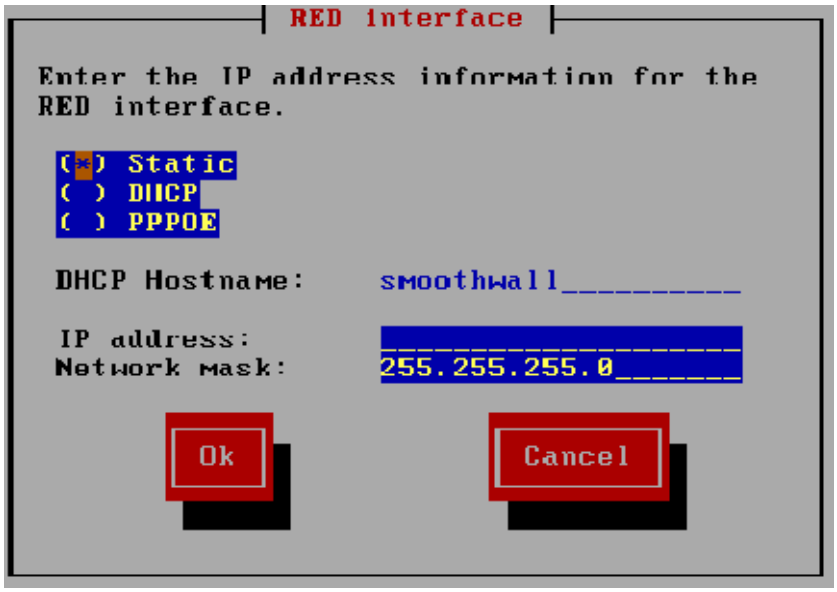
Sélectionner GREEN puis sur OK. La zone de dialogue suivante s'ouvre :

Cliquer sur OK pour continuer. La zone de dialogue d'interface s'ouvre :

Donner l'adresse IP et le masque sous- réseau de carte verte

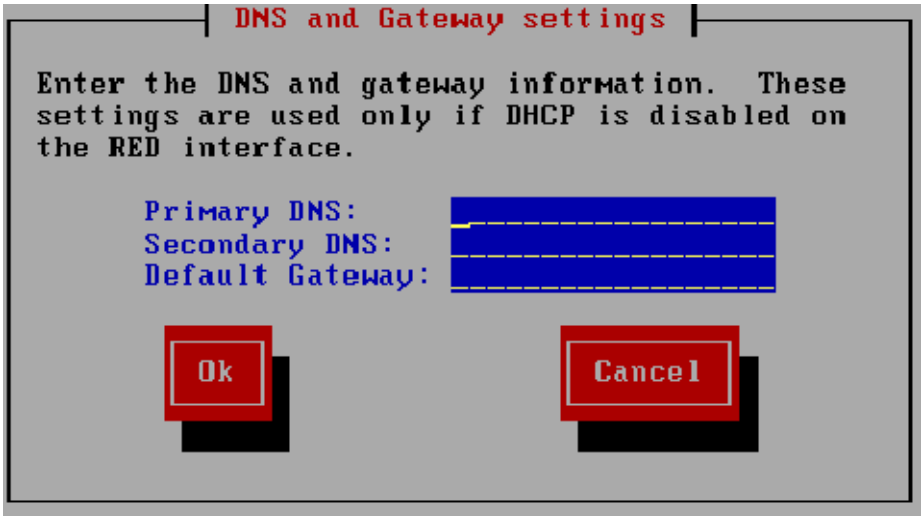
Cliquer sur OK et taper sur ENTRER pour revenir à la zone de dialogue d'affectation d'adresse :

Cliquer sur **DONE** pour configurer la carte rouge (RED). La zone de dialogue d'interface s'ouvre :



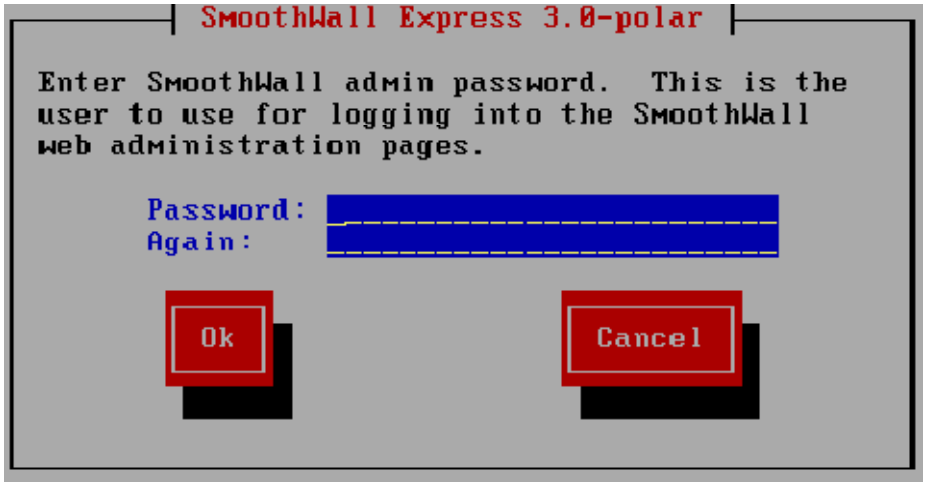
Attribuer une adresse IP statique en cliquant **STATIC** ou Dynamique en cliquant sur **DHCP** puis OK, en suite taper sur ENTRER. Dans la zone de dialogue d'affectation d'adresse, cliquer sur DONE puis ENTRER pour revenir au menu de configuration de réseau.

Sélectionner **DNS and Gateway settings** et taper sur ENTRER. La zone de DNS et la passerelle par défaut s'ouvre :



Donner une adresse IP pour DNS primaire et la passerelle par défaut qui doivent être égale à l'adresse de la carte REED. Cliquer sur OK puis sur ENTRER.

Dans le menu de configuration de réseau, sélectionner DONE puis taper ENTRER afin de revenir à la fenêtre de menu dont en cliquant sur **Finished** en suite ENTRER pour continuer le processus d'installation. La zone de dialogue suivante s'ouvre :



Entrer un mot de passe **ADMIN** (administrateur) et cliquer sur OK puis sur ENTRER.

La zone de dialogue suivante s'ouvre :

Entrer un mot de passe utilisateur **ROOT** puis cliquer sur OK en suite sur ENTRER pour redémarrer la machine.

Remarque :

- L'utilisateur "**ROOT**" a le control total du firewall.
- L'utilisateur "**ADMIN**" peut changer les paramètres du firewall.

III.7.8. Administration de SmoothWall :

Le pare-feu smoothwall est alors autonome et peut être administré à distance par une interface web, à partir d'un poste relié au réseau vert, en connectant comme utilisateur "admin". Pour ceci il faudrait taper l'adresse URL (uniforme Resource local) de smoothwall (adresse IP de la carte verte (green)) dans la barre d'adressage de navigateur web, en spécifiant le numéro de port **:**

https://192.168.72.142:441 (accès sécurisé)

http://192.168.72.142:81 (non sécurisé)

Une authentification par login et mot de passe est alors demandée :

La page d'accueil de Smoothwall Express s'ouvre :

La page d'accueil affiche un message de bienvenue, un graphe représentant des statistiques sur le trafic entrant et sortant et surtout est composé de 9 menus qui sont : Control, About, Services, Networking, VPN, Logs, Tools, Maintenance, shutdown et help.

- **Menu About**

Quand on clique sur **About**, une page à plusieurs onglets apparait avec l'onglet status sélectionné :

On aperçoit sur cette page les services disponibles et leur status. S'ils sont en marche, alors la case en face du nom du service est colorée en vert. Sinon, la case est colorée en gris.

- L'onglet **About >advanced** donne des détails sur le matériel de la machine (mémoire disponibles, disque dur, secteur de boot…).

- L'onglet **About >traffic graphs** permet de visualiser les graphes décrivant le trafic réseau sur chacune des interfaces de Smoothwall Express. On y retrouve aussi des statistiques sur le débit courant, le débit par heure, par jour et d'autres informations de ce genre.

- L'onglet **About >bandwidth bars** montre l'état de la bande passante consommée sur les interfaces réseau de Smoothwall Express en temps réel.

- L'onglet **About >traffic monitor** quant à lui permet de visualiser en temps réel l'évolution de la bande passante (graphe de bande passante).

- L'onglet **About >my smoothwall** enfin montre des informations sur le système d'exploitation Smoothwall Express installé sur la machine.

- **Menu services**

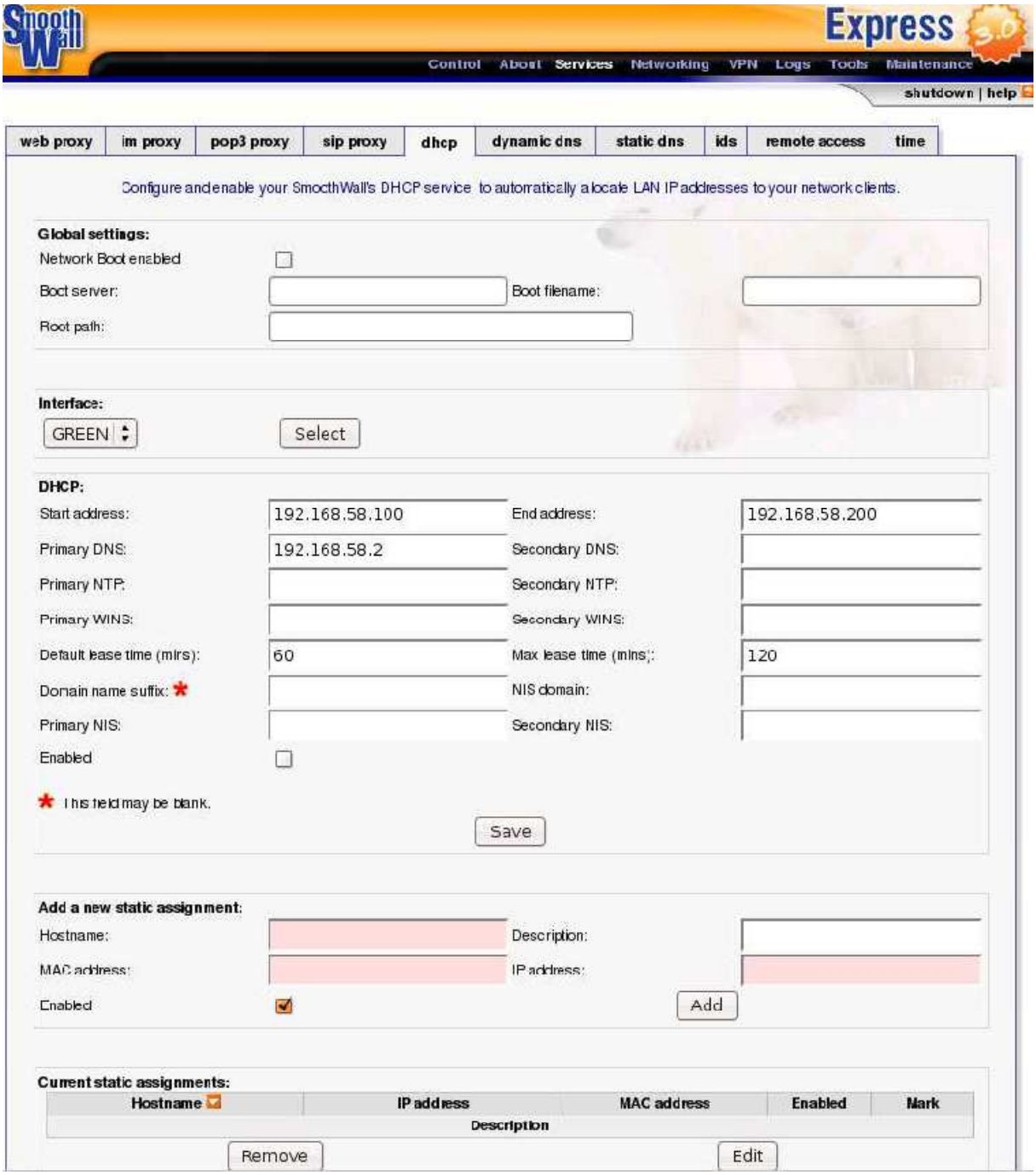
Quand on clique sur le menu Services, une page à plusieurs onglets apparait avec l'onglet web proxy :

Cet onglet présente les différentes options qu'offre le proxy web de Smoothwall Express. On peut y apercevoir l'adresse du proxy distant (remote proxy), la taille du cache, les paramètres d'authentification du proxy et ainsi de suite…

- L'onglet **Services >Im proxy** présente les options de proxy de messagerie instantanées (instant messaging proxy).

- L'onglet **Services >pop3 proxy** permet d'activer si désiré le proxy transparent de l'antivirus P3Scan qui aura pour tâche de protéger contre les virus provenant d'emails utilisant le Protocole pop3.
- L'onglet **Services >SIP proxy** permet de paramétrer le proxy SIP (Session Initiation Protocol) qui sert pour la gestion de sessions.

- L'onglet **Services >DHCP** permet de paramétrer le serveur DHCP de Smoothwall Express et de l'activer.



- L'onglet **Services >dynamic DNS** sert à attribuer des noms de domaines à certains services offerts par l'entreprise et accessible via Internet. Ceci est surtout nécessaire lorsque le fournisseur d'accès internet affecte des adresses IP dynamiques à l'abonnement de l'entreprise.

- L'option **Services >static DNS** sert quant à elle à affecter une fois pour toute un nom de domaine à une adresse IP.

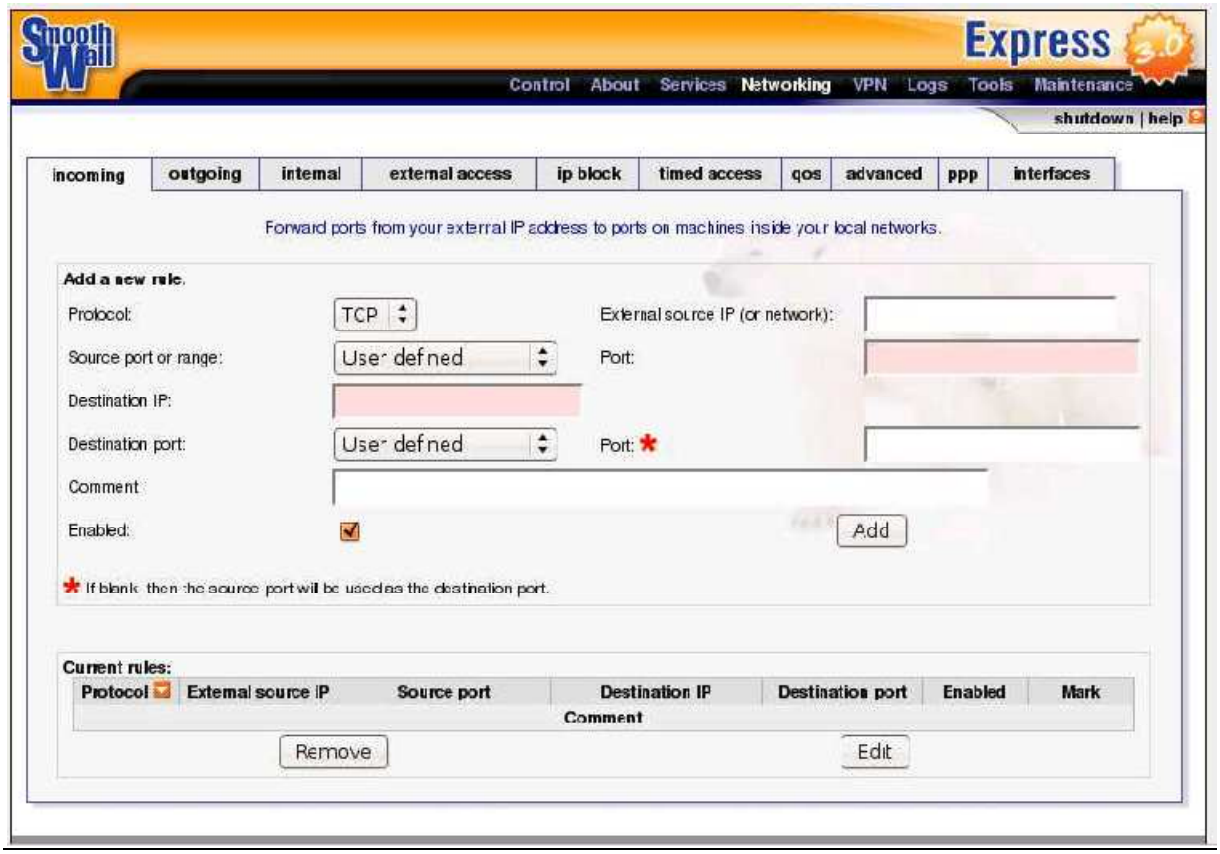
- L'onglet **Services >IDS** (Intrusion Detection System) permet d'activer l'ids de Smoothwall Express et de le mettre à jour.

- L'onglet **Services >remote access** permet de sécuriser l'accès distant à Smoothwall Express. Ainsi on peut activer ou désactiver le service SSH. On peut aussi limiter l'accès web aux administrateurs à des URL biens connues.

- L'onglet **Services >time** permet de configurer les paramètres de l'heure et de la date de la machine où Smoothwall Express est installé.

➢ Menu Networking

Quand on clique sur le menu Networking, une page à plusieurs onglets apparait :



- L'onglet **Networking >incoming** sert à définir les règles de pare-feu pour le trafic entrant (depuis les adresses IP externes) aux ports des machines du réseau local.

- L'onglet **Networking >outgoing** sert à controller le trafic sortant, c'est à dire l'accès des machines locales à des services externes.

- L'onglet **Networking >internal** sert à activer l'accès pour un hôte appartenant à la partie Orange ou Purple du réseau de l'entreprise à un port d'une machine appartenant à la partie verte de l'entreprise (réseau local).

- L'onglet **Networking >external acces** permet de configurer la façon dont on accède aux services qu'offre la machine Smoothwall à partir de machines externes.

- L'onglet **Networking >ipblock** sert à ajouter des règles restrictives de pare-feu pour des adresses IP ou des adresses de réseaux.

- L'onglet **Networking >timed access** sert à configurer des temps d'accès pour des machines du réseau interne. Ceci sert à limiter par exemple le temps de connexion Internet au temps de travail.

- L'onglet **Networking >Qos** sert à éditer les paramètres de qualité de service du réseau tels que vitesses de téléchargement optimale, priorité du trafic en fonction des protocoles.

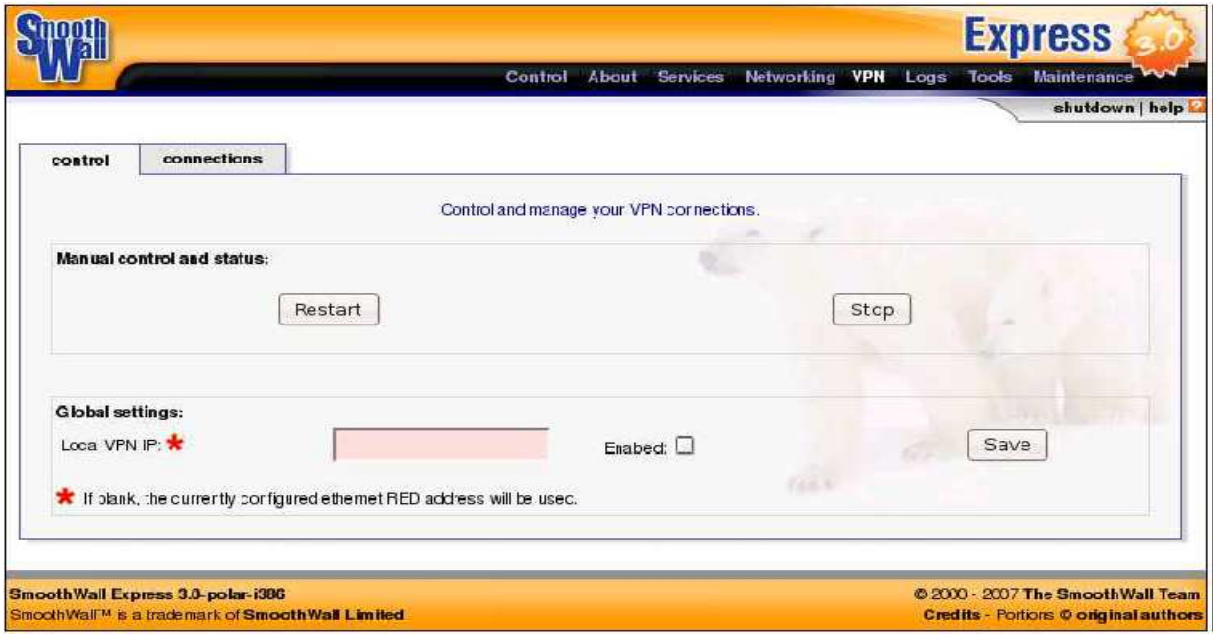
- L'onglet **Networking >advanced** sert à configurer les options des paquets ICMP provenant à la machine Smoothwall.

- L'onglet **Networking >ppp** sert à configurer les options des communications basées sur le protocole point-to-point.

- L'onglet **Networking >interfaces** sert à définir les adresses IP des différentes interfaces réseaux, le serveur DNS, la passerelle par défaut...

➢ Menu VPN

Quand on clique sur le menu VPN, la page suivante apparaît :

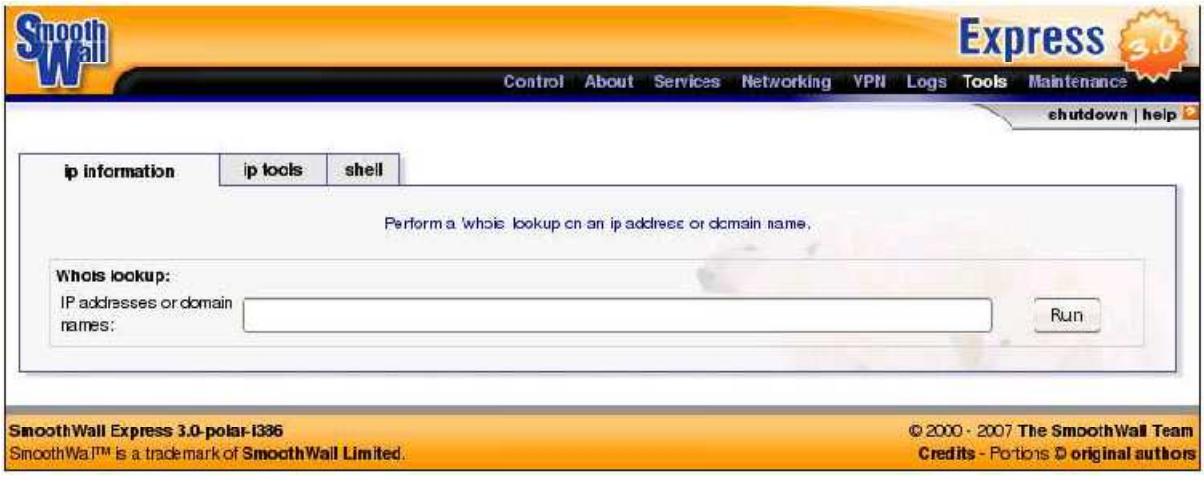


- L'onglet **VPN >control** sert à activer/stopper les connections par réseaux Virtuels Privés à travers Internet (interface Red).
- L'onglet **VPN >connections** sert à définir de nouvelles connections VPN.

➢ Menu logs

- L'onglet **Logs >system** sert à visualiser les logs de système.
- L'onglet **Logs >web proxy** sert à visualiser les logs du proxy web.
- L'onglet **Logs >firewall** sert à visualiser les logs du pare-feu.
- L'onglet **Logs >IDS** sert à visualiser les logs de l'IDS.
- L'onglet **Logs >instant messages** sert à visualiser les logs de la messagerie instantanée
- L'onglet **Logs >email** sert à visualiser les logs du service POP3 Anti-virus.

➢ Menu Tools

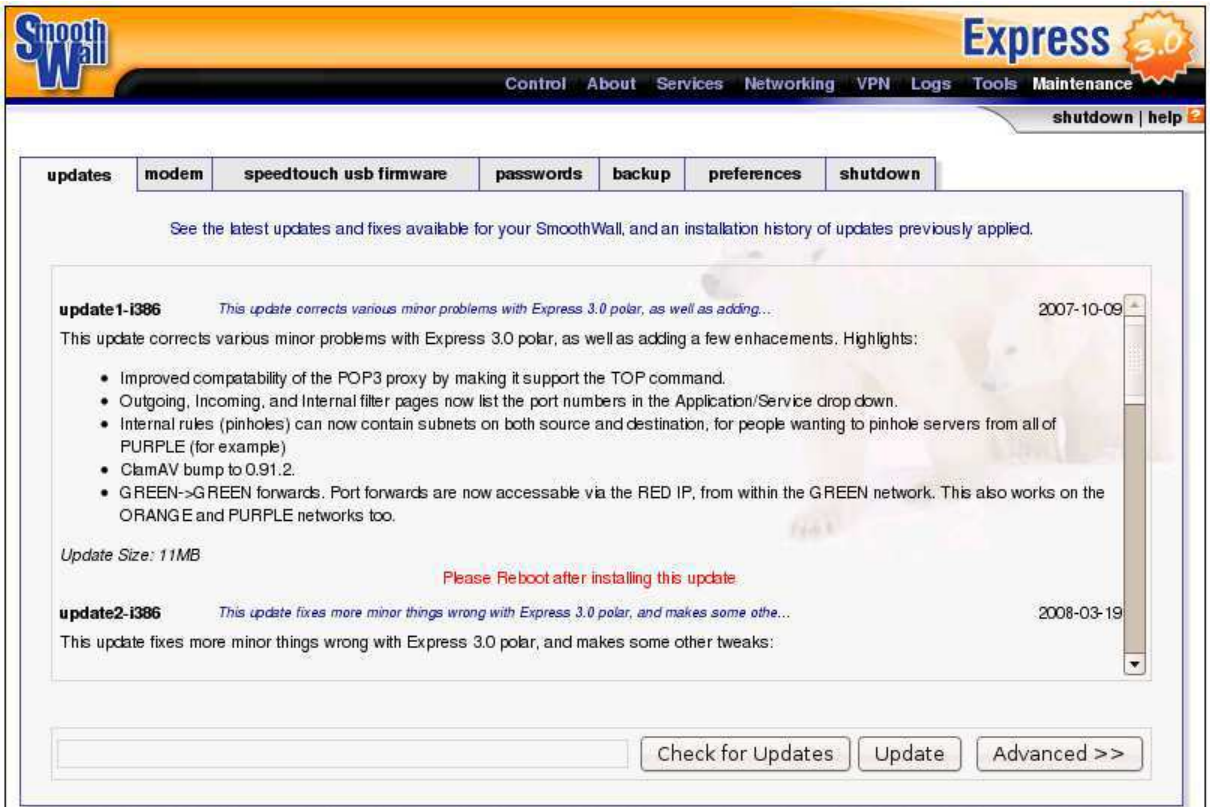


- L'onglet **Tools >IP informations** permet d'obtenir des informations concernant une adresse IP ou un nom de domaine.

- L'onglet **Tools >IP tools** permet d'utiliser deux outils classiques de test de connectivité à savoir ping et traceroute.

- L'onglet **Tool >shell** permet de se connecter en mode console sécurisée à la machine.

- **Menu maintenance**



- L'onglet **Maintenance >updates** sert à chercher des mises à jour pour Smoothwall Express.

- L'onglet **Maintenance >Modem** sert à configurer les paramètres du modem.

- L'onglet **Maintenance >speedtouch usb firmware** permet de télécharger des fichiers pour l'installation des modems speedtouch directement sur la machine Smoothwall Express.

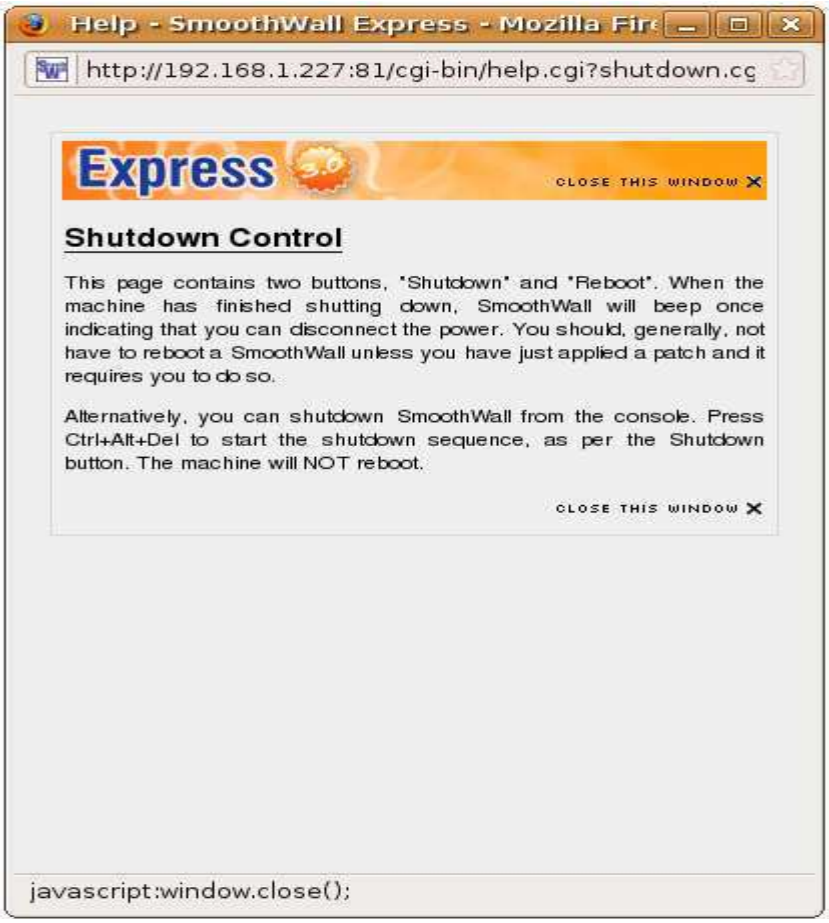
- L'onglet **Maintenance >passwords** permet de définir des mots de passe pour les utilisateurs admin et dial.

- L'onglet **Maintenance >backup** permet de créer une disquette de restauration (ou une image de restauration).

- L'onglet **Maintenance >préférences** permet de configurer des paramètres de l'interface web de Smoothwall.

- L'onglet **Maintenance >shtdown** permet d'éteindre ou de redémarrer le système.

➢ Menu help



- L'onglet help permet d'obtenir de l'aide détaillée sur la page sélectionnée.

III.7.9. Contrôle du trafic réseau :

Dans cette partie nous allons voir :

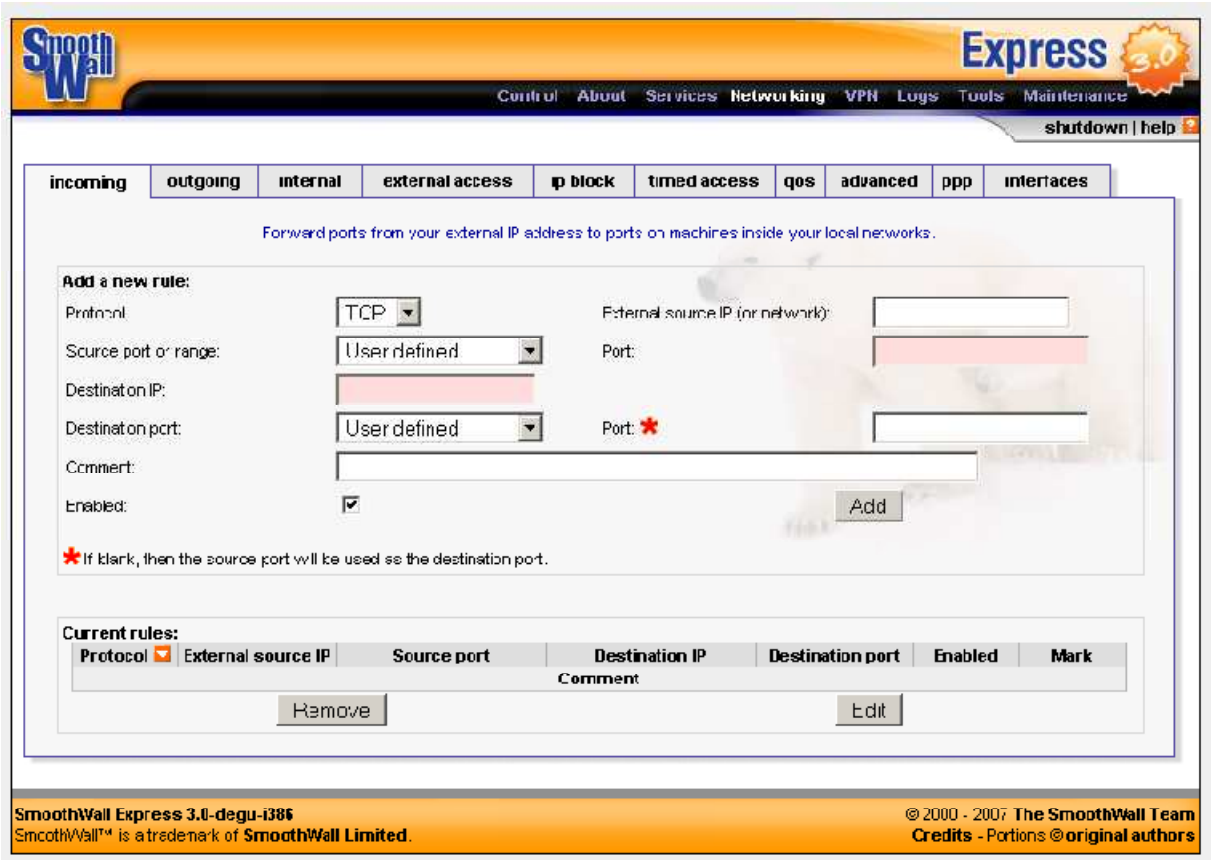
- Gestion du trafic entrant et sortant ;
- Contrôle du trafic interne et l'accès aux services ;
- Blocage IP spécifique ;
- Configuration de l'accès à l'Internet chronométré ;
- Configuration des options de réseau avancées.

III.7.9.a. Contrôle du trafic entrant :

SmoothWall Express, par défaut, bloque tout le trafic qui provient de l'interface rouge.

Pour cela il faudrait d'abord autoriser les ports qu'on voudrait utiliser.

Pour créer un port de transmission: Accéder à **Networking > incoming** page:



Configurer les paramètres suivants:

- **Protocol :** Sélectionner une des options suivantes:
  TCP - Le protocole par défaut
  UDP - le protocole sans connexion.

- **External source IP (or network):**

Spécifier les IP externe où réseau peut envoyer du trafic vers les IP de destination ou laisser ce champ vide si tout le trafic vers l'IP de destination doit être autorisé. Par exemple un serveur web accessible au public.

- **Source port or range :**

Spécifier le port sur l'adresse IP source du trafic entrant. Par exemple, le port 80 (le numéro de port HTTP standard, serait normalement spécifié pour le trafic à transmettre à un serveur Web).

- **Port :**

Chaque règle doit contenir un seul numéro de port, ou une plage de ports spécifiée comme deux numéros de port séparés par deux points (:) caractère. Par exemple, 123:456.

- **Destination port :**

Dans le menu déroulant, sélectionner **user defined**, Puis spécifier le numéro de port de destination.

- **Comment :**

Entrer un commentaire décrivant cette règle.

- **Enabled :**

Sélectionner cette option pour activer la règle.

Cliquer sur **add** (Ajouter) pour que l'information soit transférée à la section actuelle des règles ci-dessous. La règle prend effet immédiatement.

Dans la zone actuelle des règles, sélectionner la règle et cliquer sur **Edit** pour modifier ou **Remove** pour supprimer.

III.7.9.b. Contrôle du trafic sortant :

On peut autoriser, désactiver ou limiter l'accès à l'Internet en fonction de chaque interface interne.

Pour créer une règle **outgoing** :

Accéder à **Networking > outgoing** page:

Configurer les paramètres suivants:

Dans la zone **interface défaults**, on peut choisir l'interface qu'on souhaite configurer en sélectionnant parmi les options suivantes:

- ✓ **Blocked with exceptions :**

Bloquer tout le trafic provenant de l'interface sauf pour les exceptions énumérées dans la zone **current exceptions.**

- ✓ **Allowed with exceptions** :

Autoriser tout le trafic provenant de l'interface sauf pour les exceptions énumérées dans la zone **current exceptions**.

Cliquer sur **Save** pour enregistrer la sélection.

- ➢ **Interface :**

Pour ajouter une exception à l'interface verte, on sélectionne sur GREEN.

- ➢ **Application or service(s)**

Dans cette zone on sélectionne **User defined** pour entrer le numéro du port désigné.

- ➢ **Add always allowed machine**

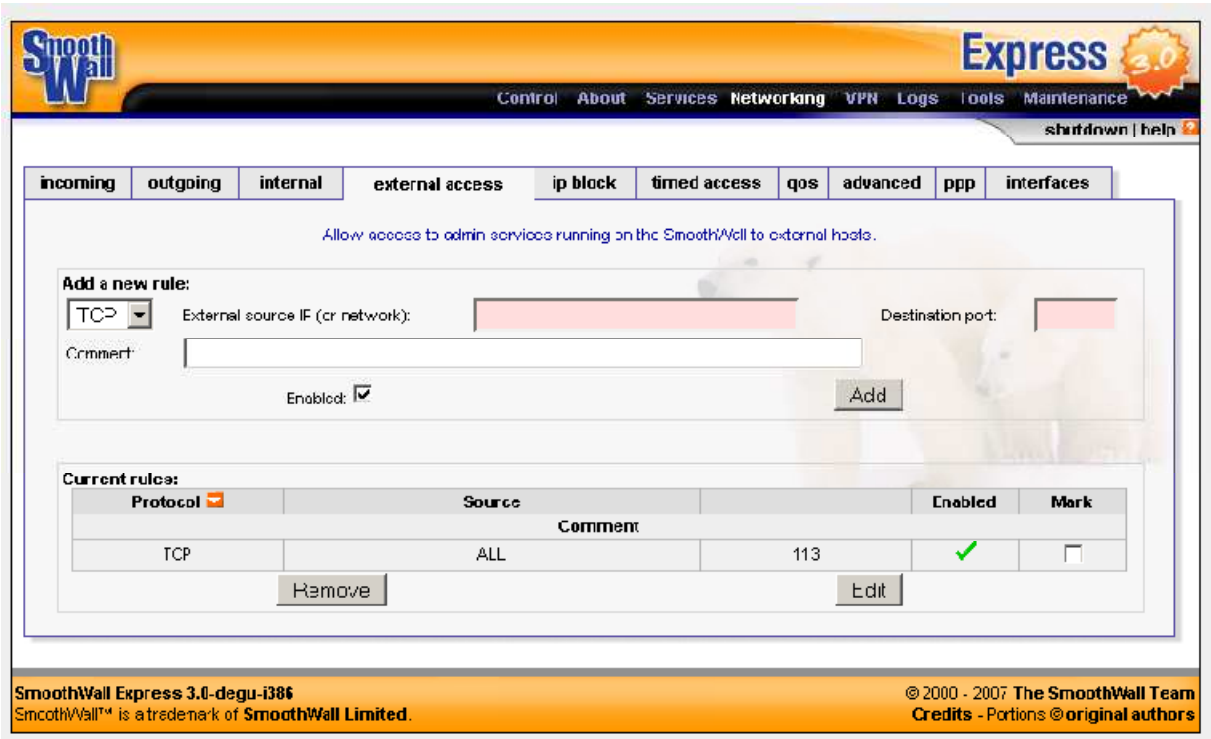
Nous pouvons toujours autoriser l'accès à l'Internet pour certains clients en spécifiant les adresses Ip de leurs machines dans la case **ip address**.

III.7.9.c. Gestion de l'accès aux services

Nous pouvons mettre en place une liste de connexions autorisées à partir d'ordinateurs externes à notre réseau via une adresse IP / ports sur l'Internet (interface rouge). Ceci est typiquement utilisé pour accorder des protocoles HTTP, HTTPS ou SSH pour l'administration distante de SmoothWall Express.

Pour gérer l'accès aux services:

Accéder à **Networking > external access** page:



Configurer les paramètres suivants:

- **Protocol**

Sélectionner parmi les options suivantes: TCP, UDP.

- **External source IP(or network)**

Entrer l'adresse IP de la source externe à permis d'accéder aux services d'administration fonctionnant sur SmoothWall Express.

- **Destination port**

Entrez le numéro de port sur le SmoothWall qui acceptera les données de la adresse source spécifiée. Tous les autres ports seront bloqués.

Par exemple : port HTTPS =441.

Port SSH =222.

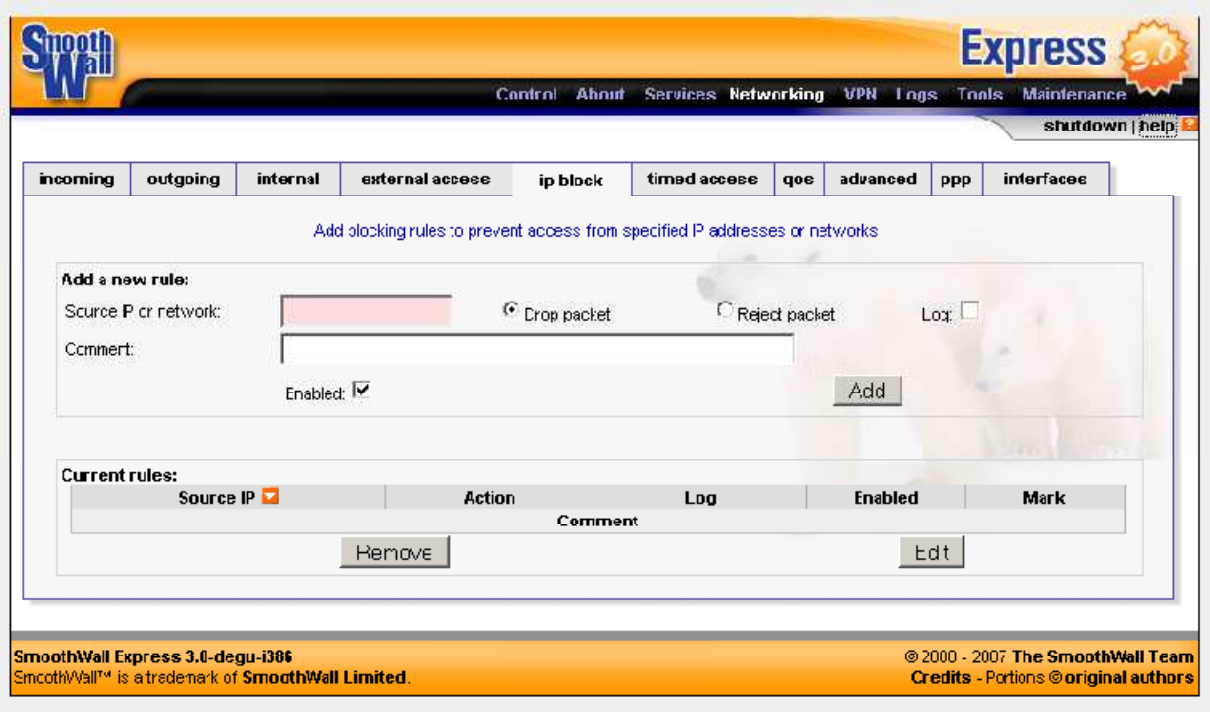
Remarque: L'accès externe via le protocole HTTP n'est pas recommandé car ce protocole ne crypte pas les données.

III.7.9.d. Bloquer sélectivement les adresses IPs

Nous pouvons bloquer sélectivement les adresses IP externes d'accéder à SmoothWall Express et toutes les machines derrière elle.

Pour bloquer les adresses IP externes:

Accéder à **Networking > ip block** page:



Configurer les paramètres suivants:

- **Source IP or network**

  Entrer l'adresse IP source de la machine que nous souhaitons bloquer.

- **Drop packet**

  On peut sélectionner cette option pour ignorer complètement toute demande de l'adresse IP d'une machine spécifiée.

- **Reject packet**

  Sélectionner cette option pour rejeter le paquet.

- **Log**

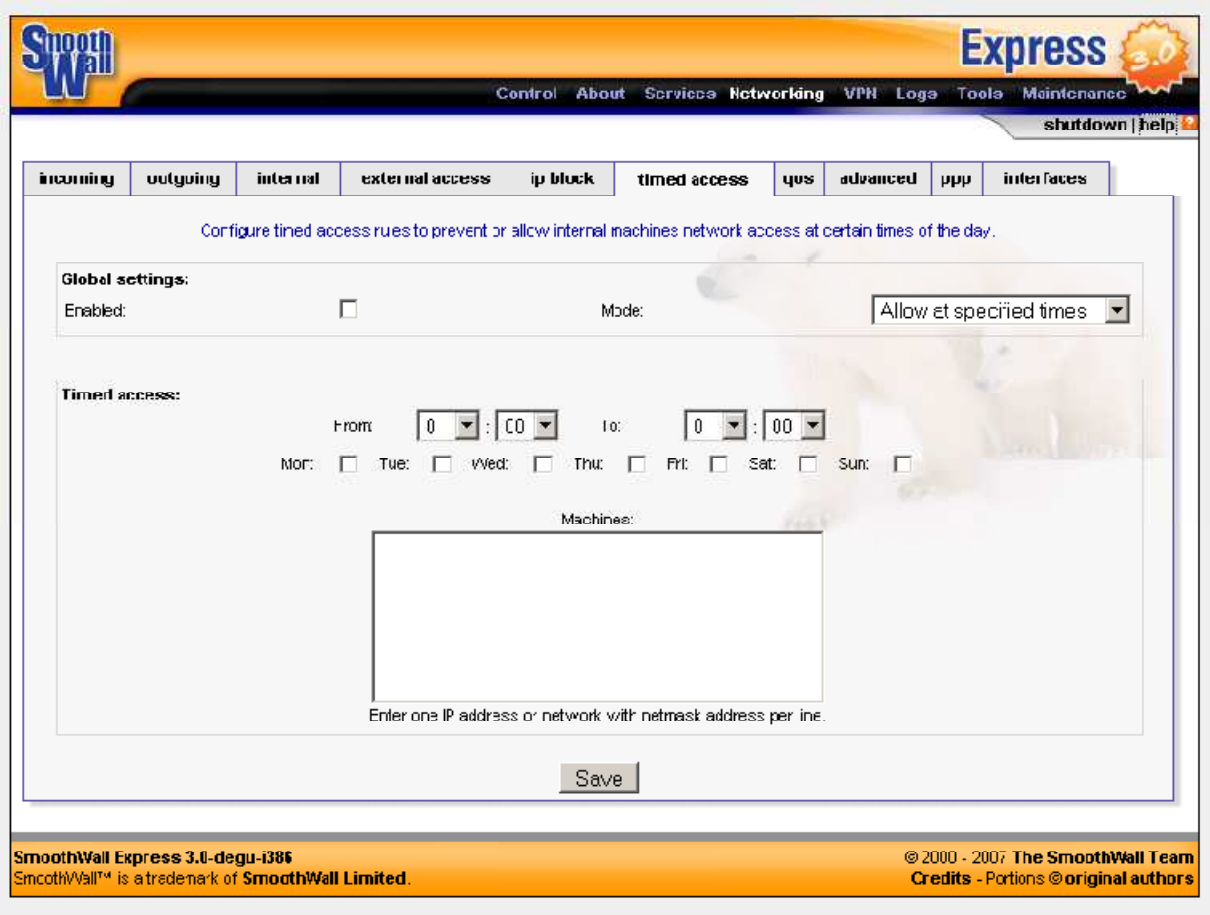
  Sélectionner cette option pour enregistrer l'activité.

III.7.9.e. Configuration les moments d'accès à l'Internet

SmoothWall Express peut autoriser ou interdire l'accès à Internet à certains moments de la journée pour un groupe spécifique de clients.

Pour configurer l'accès à l'Internet chronométré:

Accéder à **Networking > timed access** page:



Configurer les paramètres suivants:

- **Enabled**

  Sélectionner cette option pour activer les paramètres.

- **Mode**

Dans la liste déroulante, sélectionner une des options suivantes:

- ✓ **Allow at specified times**, l'accès à Internet est autorisé à des moments précis.
- ✓ **Reject at specified times**, l'accès à Internet est bloqué à des moments précis.

➢ **From –To**

Sélectionner à partir de quand à quand et les jours de la semaine pour autoriser ou bloquer l'accès à Internet.

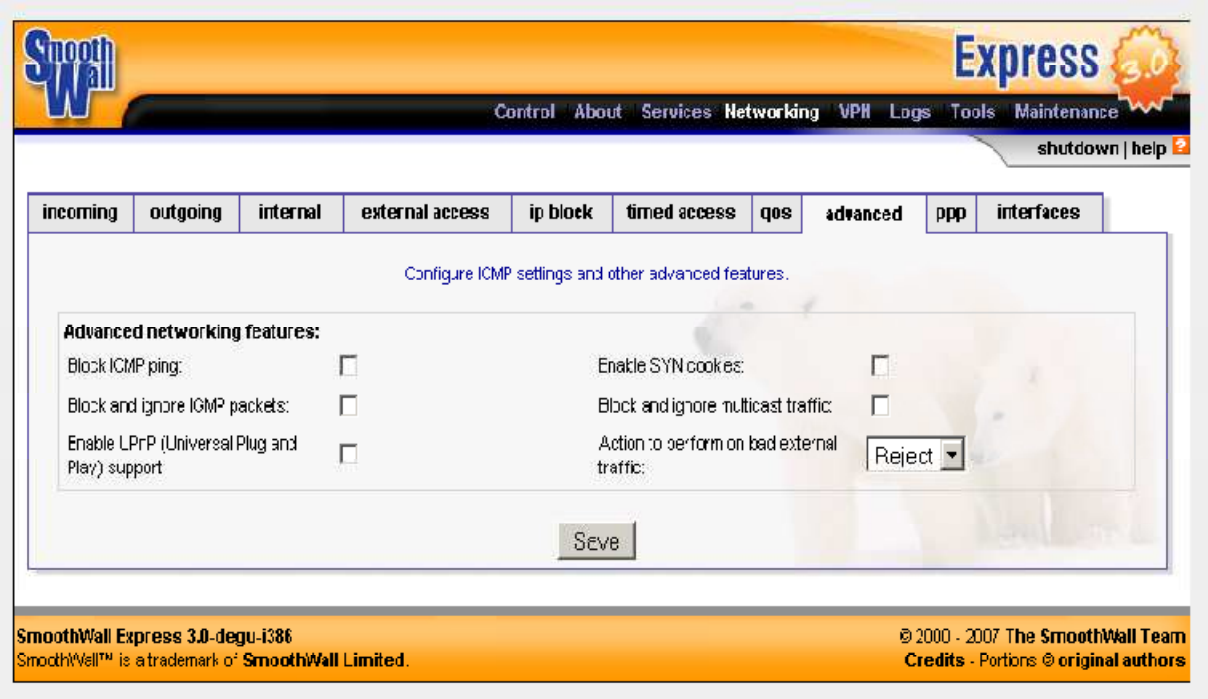
➢ **Machines**

Entrer une adresse IP ou un réseau avec un masque sous réseaux par ligne.

III.7.9.f. Configuration des options de réseau avancées

SmoothWall Express peut être configuré pour gérer ICMP (Internet Control Message Protocol) et d'autres options de réseau avancées.

Accéder à **Networking > advanced** page:



Configurer les paramètres suivants:

- **Block ICMP ping**

Sélectionner cette option pour arrêter SmoothWall Express répondre à des messages de PING soit l'Internet ou depuis le réseau local.

- **Enable SYN cookies**

Sélectionner cette option pour activer les cookies SYN comme un mécanisme de défense contre les attaques SYN Flood, et d'éviter un déni de service (DOS).

- **Block and ignore IGMP packets**

Sélectionner cette option pour bloquer et ne pas tenir compte IGMP (Internet Group Management Protocol). Cela réduit les messages parasites dans les fichiers journaux.

- **Block and ignore multicast traffic**.

Sélectionner cette option pour bloquer les multi-diffusions des messages et à les empêcher d'être connecté.

- **Enable UPnP (Universal Plug and Play) support**

Sélectionner cette option pour activer le support pour Universal Plug and Play (UPnP) clients.

- **Action to perform on bad external traffic**

Dans la liste déroulante, sélectionner la façon de gérer le trafic qui n'est pas transmis. Les options disponibles sont les suivants:

Reject - Répondre à un message ICMP port inaccessible.
Remarque: Il sera ainsi plus facile pour un attaquant de déterminer quels ports SmoothWall Express a ouvert.

Drop – Ne pas répondre. L'attaquant aura plus de difficulté à trouver des ports

ouverts sur SmoothWall Express.

Tip: Pour la capacité maximum de discrétion, de combiner Drop avec Block ICMP ping.

Cliquer sur **save** pour enregistrer les paramètres.

En fin, à cette étape notre objectif est atteint.

III.8. Discussion :

Routage et pare-feu sont souvent les plus difficiles problèmes aux administrateurs. SmoothWall Express intègre les diverses fonctionnalités nécessaires pour un pare-feu (Filtrage web, connexion à un ids, logs de pare-feu...), il offre une interface graphique conviviale et légère. La supervision du trafic en temps réel est non négligeable par rapport à d'autres pare-feu existants (graphes et barres de bande passante...).

Avec un investissement minimal de temps et de matériel, un administrateur est en mesure d'avoir un routeur et pare-feu combiné fonctionnant simultanément. SmoothWall offre une bonne sécurité et permet le partage de connexion Internet sur le réseau local.

Pour une solution de sécurité simple mais puissant, ou pour un excellent outil pour en apprendre davantage sur le protocole TCP / IP et le routage de sécurité, SmoothWall doit être votre premier choix.

Conclusion

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

Le travail que nous avons mené nous a permis de découvrir beaucoup d'informations que l'on ignorait sur la sécurité du réseau d'entreprise tel que les risques et les menaces provenant d'Internet : virus, « chevaux de Troie », pourriels, logiciels espions (spyware)…,

Ce dernier nous a également permis de découvrir les logiciels de simulation "**VMware Worktation**" et "**Oracle VM VirtualBox**".

Le pare-feu smoothwall que nous avons disposé entre le réseau local et l'internet, surveille les connexions. Il filtre les connexions entrantes et sortantes du réseau informatique selon des règles établies par l'administrateur réseau. Il empêche ainsi l'intrusion de pirates. Le pare-feu tient à jour un journal de connexions qui offre un inventaire des connexions effectuées au réseau de l'entreprise.

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

Il est également nécessaire de préciser que le Smoothwall est seulement un composant de sécurité, il ne protégera donc pas à lui seul un réseau. Il est nécessaire de l'inclure dans une démarche qui prendra en compte d'autres paramètres tel que l'Anti-virus et la mise à jour des applications.

Et voilà ainsi se termine notre modeste travail. Nous espérons avoir été assez précis dans nos explications ainsi que nos exemples et que ce travail vous a apporté quelque chose...

ADSL: ASYMMETRIC DIGITAL SUBSCRIBER LINE.

ARP: ADDRESS RESOLUTION PROTOCOL

CATV: COMMUNITY ANTENNA TELEVISION

CD: COLLISION DÉTECTION

CSMA: CARRIER SENS METHOD ACCESS

DHCP: DYNAMIC HOST CONFIGURATION PROTOCO

DNS: DOMAIN NAME SERVICE

DOS: DISK OPERATING SYSTEM

FTP: FILE TRANSPORT PROTOCOL

GPL: GENERAL PUBLIC LICENCE

HTTP: HYPERTEXT TRANSFER PROTOCOL

HTTPS: HYPERTEXT TRANSFER PROTOCOL SECURE

ICMP: INTERNET CONTROL MESSAGE PROTOCOL

IDE: INTEGRATED DEVELOPMENT ENVIRONMENT.

IDS: INTRUSION DETECTION SYSTEM)

IGMP: INTERNET GROUP MANAGEMENT PROTOCOL

IP: INTERNET PROTOCOLE

ISA: INTERNET SECURITY AND ACCELERATION

LAN: LOCAL AREA NETWORK

MAC: MEDIA ACCESS CONTROL

MAN: MÉTROPOLITAIN AREA NETWORK

NAT: NETWORK ADDRESS TRANSLATION

NIC: NETWORK INTERFACE CARD

NTP: NETWORK TIME PROTOCOL

OSI: OPEN SYSTEMS INTERCONNECTION

PAN: PERSONAL AREA NETWORK

PCI: PROTOCOL-CONTROL INFORMATION

POP3: POST OFFICE PROTOCOL VERSION 3

PPP: PROTOCOL POINT-TO-POINT

QOS: QUALITY OF SERVICE

RAM: RANDOM ACCESS MEMORY

RARP: REVERSE ADDRESS RESOLUTION PROTOCOL

RJ45: REGISTERED JACK 45

RNIS: RESEAU NUMERIQUE A INTEGRATION DE SERVICES

SCSI: SMALL COMPUTER SYSTEM INTERFACE

SIP: SESSION INITIATION PROTOCOL

SMTP: SIMPLE MAIL TRANSFER PROTOCOL

SSH: SECURE SHELL

STP: SHIELDED TWISTED-PAIR

TCP: TRANSFERT CONTRÔLE PROTOCOLE

UDP: USER DATAGRAM PROTOCOL

URL: UNIFORME RESOURCE LOCAL

USB: UNIVERSAL SERIAL BUS

UTP: UNSHIELDED TWISTED-PAIR

VGA: VIDEO GRAPHICS ARRAY

VPN: VIRTUELS PRIVES A TRAVERS INTERNET

WAN: WIDE AREA NETWORK OU RÉSEAU ÉTENDU

[1] Guy pujolle**, <les réseaux>,** Eyrolles, 2008

[2] Danièle dromard et Dominique Seret**, < Architecture des réseaux>,** Pearson Education France, 2009

[3] G florin, S natkin **<La sécurité>,** CNAM- Cédric

[4] David j.stang & Sylvia Moon**, <sécurité réseaux>,** Dunod Paris, 1996

[5] Jean baptiste Favre**, < firewall: architecture et déploiement>,** Créative Commons, 2006

[6] D. Brent Chapman, Elisabeth D. Wwicky**,** <**La sécurité sur Internet Firewalls>,** O'Reilly, 1996.

[7] Bernard boutherin et Benoit delaunay**,** < **linux- sécuriser un réseau**> 3ème edition Eyrolles, 2006

[8] Société alpha-engineering**,** < **White book smoothwall express 3.0>,** Aout 2009

[9] Hassina chaouche, Djamila kadouche**,** <**sécurité réseaux**>**,** UMMTO**,** Département électronique, promotion 2003

[10] Bouklouch abderrehmane, Oulde Bellah Mohammed**, <etude des protocols pour réseaux informatiques>,** Institut des télécommunications Abdelhafid BOUSSOUF .Oran, Télécommunication, Juin 2005.

[11] http://www.smoothwall.org

[12] http://www.skullbox.net/smoothwall.php

[13] http://www.smoothwall.net

[14] http://www.minuxland.com/spip.php?article25

[15] http://www.linuxnetmag.org/2002-05-25-linux-firewall-smoothwall-ipcop

[16] http://www.linux-tip.net/cms/content/view/316/26/

[17] http://wiki.monitoring-fr.org/securite/

[18] http://www.frameip.com

[19] http://www.techrepublic.com/blog/doityourself-it-guy/diy-smoothwall-express-a-free-firewall-distribution/907?tag=content;siu-container

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

Résume

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

D'habitue, nous savons que pour protéger le réseau interne il faudrait installer le pare-feu entre le réseau local et externe. Cette solution ne convient pas pour quelqu'un qui n'a pas les moyens de se procurer de cet outil.

L'objectif de notre travail est de sécuriser le réseau interne d'entreprise contre les menaces extérieures avec un coût minimal, en utilisant une architecture de réseau sécurisée qui comporte un élément essentiel qui est le pare-feu Smoothwall.

Mots clés :

Réseaux Informatiques, sécurité réseau d'entreprise, pare-feu, SmoothWall.