République Algérienne Démocratique et Populaire
Université Abou Bekr Belkaid- Tlemcen
Faculté des Sciences
Département d'informatique
Laboratoire de Recherche
« Système, Technologies de l'information et de la communication »

Mémoire de fin d'études

Pour l'obtention du diplôme d'ingénieur d'état en informatique

Option : Système d'information avancé

Thème

Installation et configuration d'un firewall

Réalisé par :

-Bendahmane Ahmed

Présenté le 28/09/2011 devant le jury composé de MM.

- Mme Iles Nawel (Président)
- Mme DIDI Fedoua (Encadreur)
- Mr Benmammar Badr Eddine (Examinateur)
- Mr Benamar Abdelkrim (Examinateur)

Année universitaire : 2010/2011

Dédicace

Je didié ce modeste travail à :

Mes chers parents Pour tous les sacrifices qu'ils ont consentis pour que je réussisse.

Je le dédié également à :

Mes sœurs.

Mes oncles et tantes.

Mes amis.

Ma copine

En un mot à touts les gens qui contribué ma réussite de prés ou de loin.

Je remercie également tous mes professeurs de la 1ére année primaire jusqu'à la cinquième année universitaire.

Table des matières

Introduction

Le réseau local est le cœur de la majeure partie de l'activité informatique.
Cette considération justifie à elle seule d'accorder une attention particulière à la sécurisation des réseaux locaux, des intranets.
Par ailleurs, il est généralement estimé que la majorité des malveillances informatiques ont une origine ou complicité interne aux organismes (la malveillance constituant déjà la catégorie la plus significative des pertes par rapport aux deux autres : accidents et erreurs).
Devant cette spécificité il est donc essentiel d'examiner dans une optique sécuritaire l'infrastructure du réseau local dés sa conception.
Il est aisé d'échafauder sur le papier des configurations de systèmes d'information, comprenant leurs réseaux et multiples branches, sécurisés avec les techniques les plus sophistiquées en matière de « firewalls » et de contrôles d'accès, mais il est fréquent qu'un audit sérieux révèle encore de nombreuses insuffisances, notamment sur le plan physique (accès aux équipements, continuité de fonctionnement).
Ce sont précisément des situations de ce type qu'il est nécessaire de prendre en compte dans une conception de réseau local sécurisé.
Cette conception s'inscrit dans le cadre de la mise en œuvre d'une politique de sécurité globale.
Dans ce PFE, on a essayé de maitriser tous les aspects ayant trait à l'installation et surtout la configuration d'un firewall dans n'importe quel topologie de réseau à sécuriser.

CHAPITRE I Généralités sur les réseaux et la sécurité

I. Les réseaux informatiques

Le terme générique « réseau » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

Réseau informatique: ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques.

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

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc).
- La communication entre personnes (courrier électronique, discussion en direct, etc).
- La communication entre processus (entre des ordinateurs industriels par exemple).
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau).

II. Similitudes entre types de réseaux :

Les différents types de réseaux ont généralement les points suivants en commun :

a) *Serveurs :* ordinateurs qui fournissent des ressources partagées aux utilisateurs par un serveur de réseau.
b) *Clients :* ordinateurs qui accèdent aux ressources partagées fournies par un serveur de réseau.
c) *Support de connexion :* conditionne la façon dont les ordinateurs sont reliés entre eux.
d) *Données partagées :* fichiers accessibles sur les serveurs du réseau
Imprimantes et autres périphériques partagés : fichiers, imprimantes ou autres éléments utilisés par les usagers du réseau.
e) *Ressources diverses :* autres ressources fournies par le serveur.

III. Les différents types de réseaux :

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

On fait généralement trois catégories de réseaux :

LAN signifie local area network (en français Réseau Local). 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).

MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN

permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.

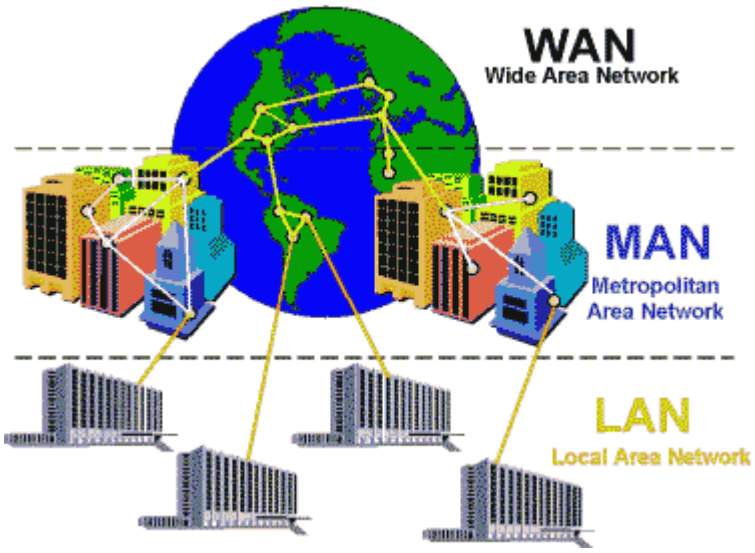


Figure I.1 : Exemple des trois types de réseaux

IV. Le modèle OSI :

OSI (Open System Interconnexion) défini en 1977 régit la communication entre 2 systèmes informatiques. A chaque niveau, les deux systèmes doivent communiquer "compatibles". En matériel réseau, nous n'utilisons que les niveaux inférieurs, jusqu'au niveau 3. Ces niveaux sont également appelés « couches ».
L'OSI est un modèle de base normalisé par l'International Standard Organisation (ISO).
Il est composé de 7 couches :
Couche 7 « application »: gère le format des données entre logiciels.
Couche 6 « présentation »: met les données en forme, éventuellement de l'encryptage et de la compression, par exemple mise en forme des textes, images et vidéo.
Couche 5 « session »: gère l'établissement, la gestion et coordination des communications.
Couche 4 « transport »: s'occupe de la gestion des erreurs, notamment avec les protocoles UDP et TCP/IP.
Couche 3 « réseau »: sélectionne les routes de transport (routage) et s'occupe du traitement et du transfert des messages: gère par exemple les protocoles IP (adresse et le masque de sous-réseau) et ICMP. Utilisé par les routeurs et les Switchs manageables.
Couche 2 « liaison de données »: utilise les **adresses MAC**. Le message Ethernet à ce stade est la trame, il est constitué d'un en-tête et des informations. L'en-tête reprend l'adresse MAC de départ, celle d'arrivée + une indication du protocole supérieur.
Couche 1 « physique »: gère les connexions matérielles et la transmission, définit la façon dont les données sont converties en signaux numériques: ça peut-être un câble coaxial, paires sur RJ45, onde radio, fibre optique, ...

A chacun de ces niveaux du modèle OSI, on encapsule un en-tête et une fin de trame (message) qui comporte les informations nécessaires en suivant les règles définies par le protocole réseau employé. Le protocole est le langage de communication (la mise en forme) utilisé pour le transfert des données (actuellement TCP/IP mais d'autres ont été utilisés comme NetBeui (antérieur à Windows 98), Novell IPX, ...).

Application	Couche Application	7	Couche Application	
	Couche Présentation	6	Couche Présentation	
	Couche Session	5	Couche Session	
Transport des données	Couche Transport	4	Couche Transport	
	Couche Réseau (Network)	3	Couche Réseau (Network)	Paquet
	Couche liaison de données (Data Link)	2	Couche liaison de données (Data Link)	Trames
	Physique (Physical)	1	Couche Physique (Physical)	BIT

Tableau I.1 Support de communication

V. Le modèle TCP/IP :

Le modèle TCP/IP s'inspire du modèle OSI auquel il reprend l'approche modulaire mais réduit le nombre à quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. Ce n'est pas le cas du modèle TCP/IP. C'est actuellement le modèle théorique le plus utilisé.

Protocoles utilisés	Modèle TCP/IP	correspondance en OSI
SMTP, POP, TELNET, FTP	Couche application	Application
		Présentation
		Session
TCP / UDP, gestion des erreurs	Couche Transport	Transport
IP / ARP et RARP /ICMP / IGMP	Couche Internet	Réseau
	Couche Accès réseau	Liaison de donnée
		Physique

Tableau I.2 Correspondance de modèle TCP /IP et OSI

De nouveau, on ajoute à chaque niveau un en-tête, les dénominations des paquets de données changent chaque fois:
Le paquet de données est appelé message au niveau de la couche application

Le message est ensuite encapsulé sous forme de segment dans la couche transport. Le message est donc découpé en morceau avant envoi pour respecter une taille maximum suivant le MTU.
Le segment une fois encapsulé dans la couche Internet prend le nom de datagramme
Enfin, on parle de trame envoyée sur le réseau au niveau de la couche accès réseau
Les couches du modèle TCP/IP sont plus générales que celles du modèle OSI.

a. Couche application :

La Couche Application reprend les applications standards en réseau informatique et Internet:
SMTP: "Simple Mail Transport Protocol" gère le transfert de mails entre serveurs (pour renseignements supplémentaires, voire Exchange et IIS dans le cours YBET sur les systèmes d'exploitation)
POP: gère le transfert des mails entre un serveur de messagerie et un ordinateur client
TELNET: connexion sur une machine distante (serveur) en tant qu'utilisateur
FTP (File Transfert Protocol), transfert des fichiers via Internet et beaucoup d'autres.

b. Couche transport :

La Couche transport : permet le transfert des données et les contrôles qui permettent de vérifier l'état de la transmission.
Les protocoles des couches suivantes permettent d'envoyer des données issues de la couche application. On ne définit pas réellement les logiciels qui communiquent, mais des numéros de ports associés au type d'application (numéro variant de 0 à 65535, 2^{16}). Par exemple, la navigation Internet utilise le port TCP 80, l'https, le 443, le FTP utilise le 21, ...
La couche transport gère 2 protocoles de transport des informations, indépendamment du type de réseau utilisé:
TCP est orienté connexion (il vérifie la bonne transmission de données par des signaux d'accusés de réception -acknowledge - du destinataire), il assure ainsi le contrôle des données
UDP, archaïque et non orienté connexion, n'assure aucun contrôle de transmission des données, par exemple utilisé en streaming.
Ces 2 types (orienté connexion ou pas) sont une notion utilisée pour les firewalls. Si vous fermez un port en TCP, l'envoi d'un message ne renvoie pas de signal de retour (acknowledge), faisant croire que l'adresse IP est libre, non utilisée. En UDP au contraire, un port fermé ne renvoit pas d'informations, faisant croire à une adresse IP utilisée. Le protocole UDP renvoie uniquement un message si le port est en erreur (ne répond pas)

c. Couche INTERNET :

La couche INTERNET est chargée de fournir le paquet des données. Elle définit les datagrammes et gère la décomposition / recomposition des segments.
La couche Internet utilise 5 protocoles, seuls les 3 premiers sont importants):
Le protocole IP: gère les destinations des messages, adresse du destinataire
Le protocole ARP (Adresse Resolution Protocol): gère les adresses des cartes réseaux et la correspondance avec l'adresse IP. Chaque carte a sa propre adresse MAC d'identification codée sur 48 bits.
Le protocole ICMP (Internet Control Message Protocol) : gère les informations relatives aux erreurs de transmission. ICMP ne les corrige pas, il signale uniquement que le message contient des erreurs, utilisé par exemple par la commande ping.

Le protocole RARP (Reverse Address Resolution Protocol) : gère l'adresse IP pour les équipements réseaux qui ne peuvent en récupérer une automatiquement par lecture d'information dans un fichier de configuration ou via un serveur DHCP. Lorsqu'un équipement réseau démarre, le gestionnaire réseau lit l'adresse IP à utiliser, ce qui est impossible pour certains équipements qui ne possèdent pas de disques durs (principalement les terminaux)

Le protocole IGMP (Internet Group Management Protocol) : permet d'envoyer le même message à des ordinateurs qui font partie d'un groupe. Il permet aussi à ces machines de s'abonner et se désabonner d'un groupe. La principale application HARDWARE de l'IGMP se retrouve dans les SWITCH_manageables. Ce protocole permet de regrouper des stations.

d. Couche Accès réseau :

La couche Accès réseau spécifie la forme sous laquelle les données doivent être transmises. Elle prend en charge les notions suivantes:

- Type de réseaux (Ethernet, Token Ring, ...), y compris les cartes réseaux.
- Transfert des données.
- Synchronisation de la transmission de données.
- Mise en forme (format) des données.
- Conversion analogique/numérique pour les modems téléphoniques.
- Contrôle des erreurs.

VI. Sécurité et attaques

1. Qu'est-ce que la sécurité d'un réseau ?

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs desdites machines possèdent uniquement les droits qui leur ont été octroyés.

Il peut s'agir :

- D'empêcher des personnes non autorisées d'agir sur le système de façon malveillante
- D'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système
- De sécuriser les données en prévoyant les pannes
- De garantir la non-interruption d'un service, etc.

2. Les causes de l'insécurité :

On distingue généralement deux types d'insécurité :

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 la non-désactivation de services réseaux non nécessaires à l'utilisateur)

L'état passif d'insécurité c'est-à-dire lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose

3. Type d'attaque :

Nombreuses ont été et sont encore les attaques informatiques. Nous en donnons un bref aperçu, triées par cible d'attaque :

a) *Hardware* : le hardware est un point d'attaque facile car il est visible. La liste des attaques humaines est sans fin, que ces dernières soient involontaires ("*oops, mon coca sur le clavier*") ou volontaires (vengeance).

b) *Software* : le software peut être détruit, modifié, effacé, déplacé. Le résultat est identique dans chaque cas, on perd l'accès au programme voulu. La modification est sans doute la pire des attaques car elle peut causer de dangereux troubles ultérieurs. Les bombes logiques, les chevaux des Troie, les virus sont différentes techniques de modification ayant chacune leurs propres spécificités.

c) *Données* : la confidentialité des données peut être mise en défaut par "*mise sur écoute*", par simple requête, en déroutant les appareils de sortie de données ... La modification des données est en général plus compliquée à mettre en œuvre car elle nécessite un plus grande connaissance technologique.

d) *Réseau* : les réseaux ajoutent à l'ensemble de la sécurité le problème de la communication. L'utilisation de moyens de transports partagés et les accès longue distance sont deux points cruciaux dont il faut tenir compte.

e) *Accès* : l'utilisation abusive d'un accès peut découler sur des pertes de performances, des pertes commerciales, mais aussi des pertes de données.

f) *Personnel* : n'oublions pas que l'humain reste un des points faibles en sécurité. D'un simple mainteneur qui tombe malade à l'employé qui touche une somme pour fournir un mot de passe, les causes d'infractions liées au personnel sont nombreuses.

VII. Techniques de Hacking

1. L'ingénierie sociale & l'irresponsabilité :

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

a) *Le contexte :* en ayant une bonne connaissance de l'organigramme de l'entreprise cela permet à l'agresseur d'avoir d'ores et déjà un pied dans l'entreprise. Le but en général est de connaître quelles sont les personnes qui sont en droit de demander telles ou telles informations, et également à qui les demander, dans le but de se faire ultérieurement passer pour elles. . .

b) *L'audace ou le bluff* : L'art de la parole et l'audace sont deux qualités indispensables lorsque l'on veut utiliser le "social engineering". II s'agit ici d'avoir suffisamment d'appoint et de connaissances techniques afin de faire croire à l'interlocuteur qu'il a affaire à un responsable technique de l'entreprise (ou d'un fournisseur de service). Tout ceci afin qu'il lui transmette les informations demandées sans aucun problème.

c) *La chance :* la chance est également une part importante dans le "social engineering", cela ne marche pas à chaque fois ! Il faut de la pratique afin de bien maîtriser le séquencement du dialogue à établir.

d) *La patience calculée :* il faut de plus savoir se montrer patient afin d'obtenir les informations désirées. Malgré tout, la méthode du "social engineering" demande une certaine rapidité pour obtenir les informations voulues, passé ce délai, il est préférable de changer d'entreprise ou d'attendre quelques jours afin de ne pas éveiller les soupçons. En général, les personnes ne sont pas formées à la notion de sécurité informatique ce qui entraîne des situations qui auraient pu être évitées.

2. Le Denial-of-Service (DoS):

Les attaques de type Denial-of-Service ont pour but de saturer un routeur ou un serveur afin de le "crasher" ou en préambule d'une attaque massive. Ces types d'attaque sont très faciles à mettre en place et très difficile à empêcher. Mais quelles sont les raisons qui peuvent pousser un attaquant à utiliser les DoS en sachant que cela peut mener à la "destruction" du routeur ou du serveur visé :

a) *Récupérer un accès :* une attaque de type Denial-of-Service fait, la plupart du temps, partie d'une attaque visant `à obtenir le contrôle d'une machine ou d'un réseau. Par exemple l'attaque de type "SYN Flood", tr`es répandue, est souvent utilisée de paire avec une tentative de "Spoofing".

b) *Masquer les traces :* ce type d'attaque permet également de "crasher" une station qui par exemple aurait peut contenir des traces du passage d'un "Hacker". En détruisant cette station, il s'assure ainsi une certaine pérennité.

c) *Se venger :* tr`es fréquemment, ces attaques sont utilisées afin d'assouvir une vengeance personnelle contre une personne, un administrateur ou bien encore une entreprise. . . . . .

Voici quelques exemples de programmes disponibles sur Internet permettant de réaliser ce genre d'attaque:

- Ping 'O Death.
- Land – Blat.
- Jolt.
- Tear Drop – SynDrop.

3. L'IP Spoofing:

Le Spoofing est une technique permettant de s'infiltrer dans un ordinateur en se faisant passer pour un hôte de confiance (Trusted Host).

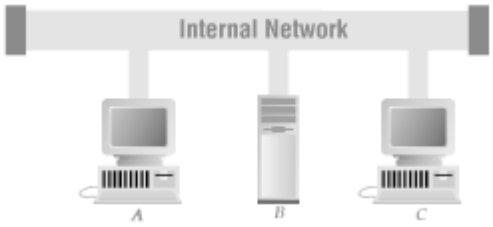
Avant de rentrer dans des détails plus techniques, voici un bref résumé du fonctionnement de cette technique: une station se fait passer pour une autre en envoyant un paquet dont l'adresse IP est "autorisée" par le serveur visé. La source IP envoyée trompe donc la cible qui accorde l'accès en pensant avoir affaire à une machine de confiance. Il existe différents types de Spoofing, nous n'aborderons ici que les notions d'IP Spoofing, celles ayant traits aux DNS Spoofing, Web Spoofing, . . . ne sont pas exposées.

Non Blind Spoofing (NBS) :

Dans ce contexte, l'utilisation de la technique du Spoofing a pour but d'interférer avec une connexion dont les paquets traversent un sous-réseau dont le "Hacker" a accès. Il peut donc aisément capturer et analyser les paquets qui sont échangés. En général, cette technique est utilisée lorsqu'il s'agit d'interagir entre deux machines du même sous-réseau ou alors il faut avoir un accès sur un routeur important (transatlantique par exemple) - la place rêvée pour un

Hacker. Comme les paquets doivent impérativement traverser le sous-réseau, il est très facile de récupérer les paquets et d'obtenir les numéros de séquence (SEQ) et d'acknowledgment (ACK).
Ce type de Spoofing est principalement utilisé pour les trois attaques suivantes:

- SYN Flooding.
- Connexion Killing.
- Connexion Hijacking.



I.2 Configuration nécessaire pour le Non Blind Spoofing

L'ordinateur 'A' va demander une connexion sur l'ordinateur 'C' alors que l'ordinateur 'B' espionne le trafic sur le réseau local. Il est donc possible pour l'ordinateur 'B' d'interrompre la relation entre 'A' et 'C' puis de se faire passer pour l'ordinateur 'A' car il a accès aux numéros de séquence (SEQ) et d'acknowledgment (ACK).

a. Blind Spoofing (BS) :

La technique du Blind Spoofing (aveugle) nécessite une tout autre configuration que pour le Non Blind Spoofing. L'avantage est qu'elle ne requière pas que l'attaquant (Hacker Server) soit capable de capturer les paquets émis par la station cible (Target Host).
C'est pourquoi cette technique est appelée "aveugle". L'attaquant doit donc pouvoir prédire les paquets qui seront envoyés par la station qu'il désire attaquer. Afin d'utiliser le Blind Spoofing, il est nécessaire de connaître les adresses IP de quatre stations:
La cible visée (Target Host).
Une machine de "confiance" pour la cible visée (Trusted Host).
Une adresse de station non accessible sur le réseau (unreachable).
Un attaquant. . . (Hacker Server).
L'utilisation de cette technique est basée sur le principe de la relation de confiance qu'il est possible d'instaurer entre deux machines à l'aide par exemple des systèmes utilisant les fichiers /etc/hosts.equiv ou les fichiers ~/.rhosts. En utilisant ces mécanismes, l'authentification se fera uniquement par vérification de l'adresse IP de la station qui demande la connexion (pas de vérification d'identité à l'aide d'un mot de passe par exemple). Dans ce contexte, le Spoofing peut s'avérer intéressant . . . . L'attaque à proprement parler va se dérouler en cinq étapes bien distinctes:
Choix de la station cible (Target Host) selon des critères personnels: défis technique, vengeance,. . .
Recherche et découverte d'une station de "confiance" (Trusted Host) (showmount, rpcinfo).
Elimination de la station de "confiance" et "sampling" des numéros de séquence TCP.

Tentative de forcage de paquets IP en tant que station de ”confiance” et connexion sur la machine cible.
Mise en place d'une Backdoor.
Le principe de fonctionnement est relativement simple, la station attaquante (Hacker Server) va tenter de se faire passer pour une station de ”confiance” (Trusted Host) aux yeux de la station cible (Target Host). Il s'agit, une fois que la station de ”confiance” a été trouvé, de rendre inaccessible (unreachable) cette dernière (à l'aide d'un DoS par exemple) afin qu'elle ne puisse par interférer avec la tentative d'attaque. Ensuite, il est nécessaire d'établir une ”première” connexion avec la station cible afin de se faire une idée précise de l'état actuel des numéros de séquence (SEQ) et d'acquittement. Pour cela, une simple connexion sur un port TCP quelconque (SMTP par exemple), juste avant de lancer une attaque, permettra d'obtenir le numéro de séquence initial fournit par la station cible (il sera judicieux d'effectuer cela plusieurs fois afin également d'obtenir un RTT (Round Trip Time) moyen). A partir de la, il est possible de tenter de forcer un paquet IP (le plus rapidement possible) à destination de la station cible en se faisant passer pour la station de ”confiance”. Le problème étant que l'attaquant ne voit pas les paquets qui vont être émis par la station cible, il faudra donc qu'il arrive à les prédire afin de réagir en conséquence.

4. Les Backdoors :

Depuis que les intrusions informatiques existent, leurs adeptes ont mis au point un certain nombre de techniques leur facilitant l'accès aux systèmes pénétrés. La technique la plus connue, et sans doute la plus utilisée, est celle des Backdoors (portes dérobées ou portes de service). Elles permettent, à celui qui en connait l'existence et le fonctionnement, de revenir sur un système de façon détournée, c'est-à-dire sans passer par les méthodes d'authentification habituelles.
En règle générale, les Backdoors permettent différents types d'actions sur le système ou elles sont installées:

- se reconnecter sur la machine même après un changement de mots de passe ou d'ajouts de systèmes de sécurité.
- rendre invisible les connexions et les actions réalisées.
- faciliter l'accès à la station sans avoir à utiliser des trous de sécurité existants (security holes).
- déranger le travail des utilisateurs par l'envoie de messages, la modification de fichiers, l'affichage d'images, la lecture de fichiers son. . .
- exécuter certaines commandes bien ciblées permettant d'avoir une vision de l'état de la station (processus, connexions réseau, utilisateurs. . .) ou de modifier le contenu de certains fichiers de configuration (mots de passe, réseau,. . .).

Il existe différents types de Backdoors, certaines n'ont une utilité qu'une fois l'accès à la station accordé, d'autres permettent par exemple de contourner les différents types de Firewalls.
Voici quelques exemples de Backdoors fréquemment trouvées sur les systèmes UNIX: Password Cracking, Rhosts + +, Login.

5. Remote Buffer Overflow Exploits

La fonction principale d'un processeur est de traiter et de déplacer des données. Lors de ces traitements, le processeur a besoin d'un emplacement afin de sauvegarder rapidement les données traitées. La taille des registres ne permet pas à ceux-ci de jouer ce rôle. Ces informations sont donc sauvées, à l'aide de commandes spécifiques et plus rapides, dans une zone mémoire appelée *pile*. Elle est stockée en mémoire à une adresse spécifique (qui peut-être changée) et de taille variable.

a. Structure de la pile :

Voilà, brièvement, comment fonctionne le processeur à ce niveau: si le registre N est utilisé et qu'une sous-procédure est exécutée et qu'elle requière l'utilisation de ce même registre (N), le processeur doit sauver le contenu de ce registre dans la pile afin de pouvoir le restaurer après la terminaison de la sous-procédure. Pour cela, le processeur doit connaître l'adresse de retour lorsque la sous-procédure se termine. Cette adresse est donc également sauvée dans la pile avant son exécution. Lorsque la sous-procédure se terminera le processeur "sautera" (jump) à l'adresse de retour précédemment stockée dans la pile. La pile a une seconde utilité, celle de stocker en mémoire les nouvelles données créées ou reçues par le programme.
NB: La gestion des entrées/sorties dans la pile utilise la méthode du LIFO (Last In - First Out)

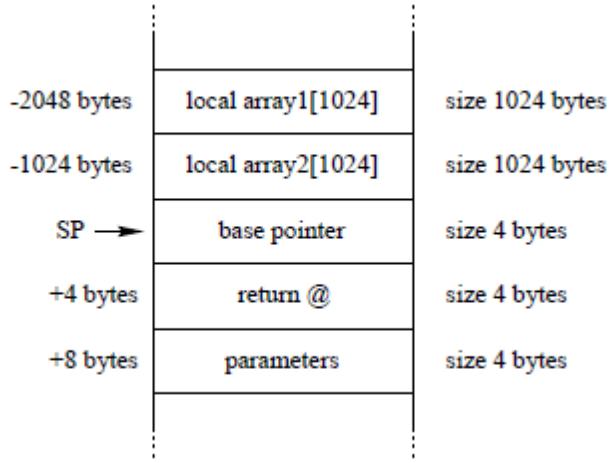


Figure I.3 Exemple de pile contenant deux tableaux, le pointeur de pile (SP) et l'adresse de retour.

b. Abuser l'adresse de retour :

Lors de l'exécution de la procédure le processeur sauve l'adresse de retour dans la pile, lorsque la procédure se terminera le processeur retournera à l'adresse spécifiée et continuera son travail...
Si (par hasard !) une procédure écrivait plus d'octets (bytes) dans une variable locale afin que la taille nécessaire à son stockage dans la pile dépasse celle de l'adresse de retour, on appellerait ceci un *Buffer Overflow*. En reprenant la structure de pile précédente et en inscrivant 1032 fois le caractère "X" dans le tableau local "array2", la procédure va alors dépasser sa propre adresse de retour.

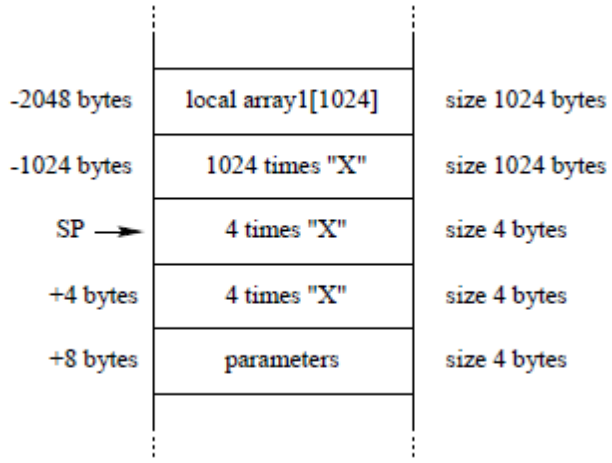


Figure I.4 Exemple de Buffer Overflow en saturant le tableau ”array2” ainsi que le Stack Pointer et l’adresse de retour de sous-procédure.

VIII. Méthodes de défense

Le but de la sécurité informatique est de préserver la confidentialité, l'intégrité et la disponibilité des données du réseau. Certaines méthodes de défense permettent de prévenir les attaques, d'autres, moins efficaces, ne font qu'une détection ultérieure.

a. *Le cryptage* : en transformant les données afin qu'elles deviennent incompréhensibles pour un observateur extérieur, on peut se protéger des interceptions et modifications. En plus de la confidentialité, le cryptage permet donc d'atteindre un certain seuil d'intégrité en tenant compte du fait que des données qui n'ont pas de signification à la lecture peuvent difficilement être modifiées de manière sensée. Le cryptage est un des outils les plus importants de la sécurité informatique mais il ne résout pas non plus tous les problèmes de sécurité. De plus, il est important de noter qu'un cryptage mal utilisé peut donner un sentiment de sécurité alors qu'il n'en n'est rien.

b. *Contrôle software* : les programmes se doivent d'être sécurisés afin d'exclure les tentatives d'attaques extérieures. Que ce soit réfléchi durant la phase de développement, implémenté par le système d'exploitation ou partie restrictive du programme, le contrôle software touche l'utilisateur assez directement ce qui en fait un des premiers sujets venant à l'esprit.

c. *Contrôle hardware* : il existe de nombreux appareils assistant la sécurité. Citons des cartes d'implémentation de cryptage, des vérificateurs d'identité, des contrôleurs d'accès disque, ...

d. *Politique* : les lois en matière de crime informatique sont aujourd'hui encore assez floues, lentes à se développer. La communauté informatique n'a pas encore vraiment adopté de standards en matière de comportement éthique. Malgré que certaines organisations poussent de tels développements, ils ne sont encore qu'à leurs balbutiements.

e. *Contrôle physique* : sans doute le contrôle le plus évident. Il comprend le verrouillage de porte, gardes, backups, planning prévu en cas de catastrophes naturelles. N'oublions pas que les techniques les plus simples sont souvent les meilleures.
f. *Bonne pratique* : les réseaux informatiques fournissent aux utilisateurs une énorme liberté. Aussi, le public se doit bien souvent encore de comprendre lui-même quels sont les comportements inappropriés en matière de réseau.

1. Cryptographie :

a. Chiffrement et déchiffrement :

Les données qui peuvent être lues et comprises sans mesures spéciales sont appelées texte clair (ou libellé). Le procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance est appelée chiffrement [dans le langage courant on parle plutôt de cryptage et de ses dérivés: crypter, décrypter]. Chiffrer du texte clair produit un charabia illisible appelé texte chiffré (ou cryptogramme). Nous utilisons le chiffrement pour garantir que l'information est cachée à qui elle n'est pas destinée, même ceux qui peuvent lire les données chiffrées. Le processus de retour du texte chiffré à son texte clair originel est appelé déchiffrement.

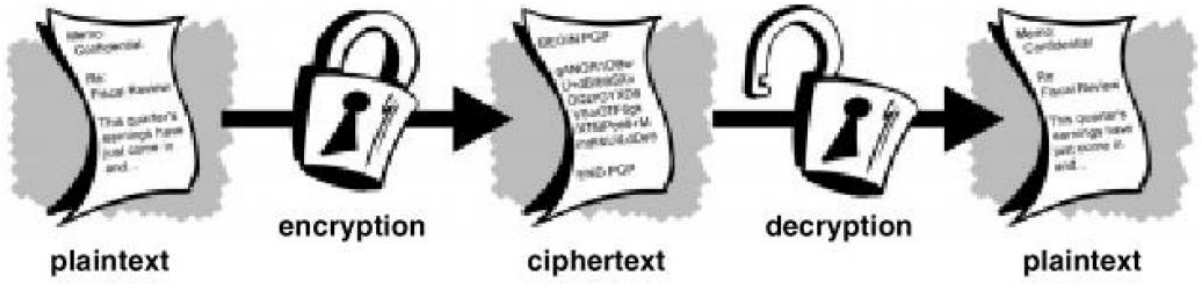


Figure I.5 Chiffrement et déchiffrement

b. Définition de la cryptographie?

La cryptographie est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie vous permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu.
Alors que la cryptographie est la science de la sécurisation des données, la cryptanalyse est la science de l'analyse et du cassage des communications sécurisées. La cryptanalyse classique mêle une intéressante combinaison de raisonnement analytique, d'application d'outils mathématiques, de découverte de redondances, de patience, de détermination, et de chance. Les cryptanalyses sont aussi appelés attaquants.
La cryptologie embrasse à la fois la cryptographie et la cryptanalyse.

c. La fonctionnalité de la cryptographie :

Un algorithme cryptographique, ou chiffre, est une fonction mathématique utilisée dans le processus de chiffrement et de déchiffrement. Un algorithme cryptographique fonctionne en combinaison avec une clé – un mot, un nombre, ou une phrase – pour chiffrer le texte clair. Le même texte clair se chiffre en un texte chiffré différent si l'on utilise des clés différentes. La sécurité des données chiffrées est entièrement dépendante de deux choses: la force de l'algorithme cryptographique et le secret de la clé.

Un algorithme cryptographique, plus toutes les clés possibles et tous les protocoles qui le font fonctionner constitue un crypto système. PGP est un crypto système.

d. Cryptographie conventionnelle (clé privée) :

Dans la cryptographie conventionnelle, aussi appelée chiffrement à clé secrète ou à clé symétrique, une [seule et même] clé est utilisée à la fois pour le chiffrement et le déchiffrement. Le Data Encryption Standard (DES) est un exemple de crypto système conventionnel qui est largement employé par le Gouvernement fédéral américain.

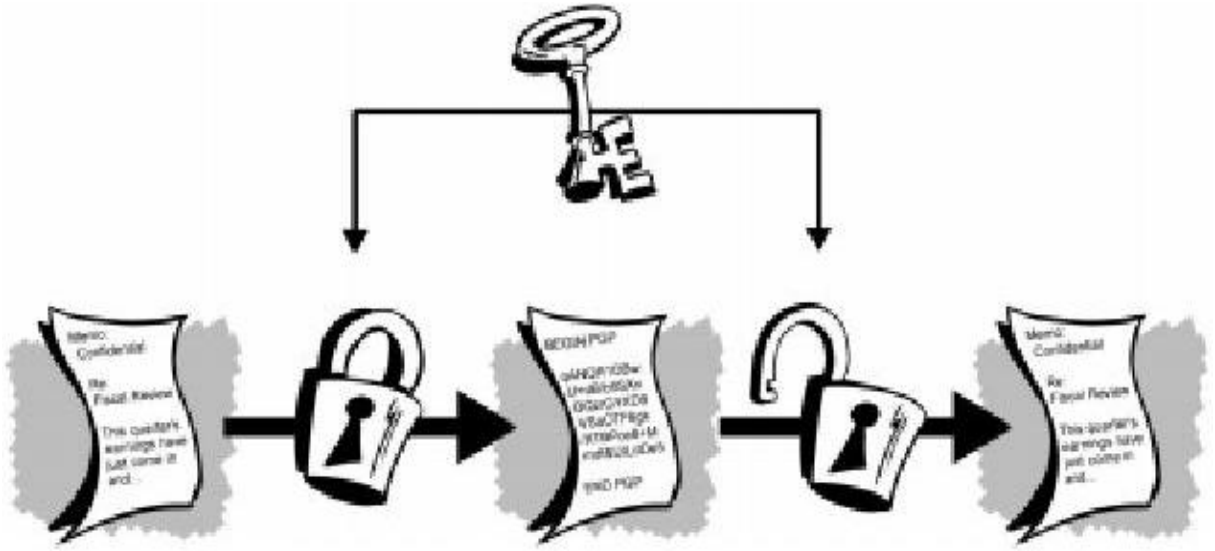


Figure I.6 Chiffrement conventionnel

e. Gestion de clé et chiffrement conventionnel :

Le chiffrement conventionnel a des avantages. Il est très rapide. Cependant, le chiffrement conventionnel seul en tant que moyen de transmission de données sécurisées peut être assez onéreux simplement en raison de la difficulté de la distribution sécurisée de la clé.

Pour qu'un expéditeur et un destinataire communiquent de façon sûre en utilisant un chiffrement conventionnel, ils doivent se mettre d'accord sur une clé et la garder secrète entre eux. S'ils sont dans des lieux géographiques différents, ils doivent faire confiance à un messager, au Bat Phone, ou à un autre moyen de communication sûr pour empêcher la divulgation de la clé secrète pendant la transmission. Quiconque a entendu par hasard ou intercepté la clé en transit peut plus tard lire, modifier, et contrefaire toutes les informations

chiffrées ou authentifiées avec cette clé. Le problème continuel avec le chiffrement conventionnel est la *distribution de la clé*: comment donnerez-vous la clé au destinataire sans que personne ne puisse l'intercepter?

f. La cryptographie à clé publique :

La cryptographie à clé publique repose sur un schéma asymétrique qui utilise une paire de clés pour le chiffrement: une clé publique, qui chiffre les données, et une clé privée correspondante, aussi appelée clé secrète, qui sera utilisée pour le déchiffrement. Nous publions largement la clé publique, tout en gardant la clé privée secrète. Toute personne en possession d'une copie de notre clé publique peut ensuite chiffrer des informations que nous seul pourrons lire.

Il est mathématiquement impossible de déduire la clé privée de la clé publique.

Quiconque a une clé publique peut chiffrer des informations mais ne peut pas les déchiffrer. Seule la personne qui a la clé privée correspondante peut déchiffrer les informations.

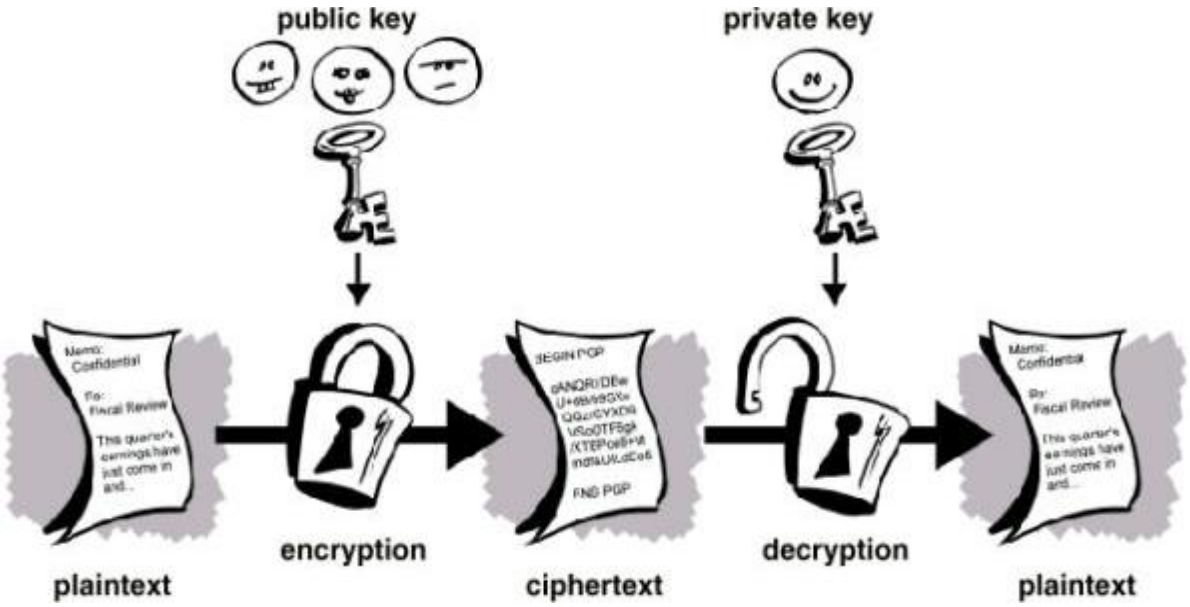


Figure I.7 Chiffrement à clé publique

Le principal avantage de la cryptographie à clé publique est qu'elle permet à des gens qui n'ont pas d'accord de sécurité préalable d'échanger des messages de manière sûre.

g. Comment fonctionne PGP (crypto système hybride.) :

PGP combine à la fois les meilleures fonctionnalités de la cryptographie conventionnelle et de la cryptographie à clé publique. PGP est un *crypto système hybride*.

Quand un utilisateur chiffre du texte clair avec PGP, PGP compresse d'abord le texte clair. La compression de données économise du temps de transmission par modem et de l'espace disque et, ce qui est plus important, renforce la sécurité cryptographique. La plupart des techniques de cryptanalyse exploitent les redondances trouvées dans le texte clair pour craquer le texte chiffré. La compression réduit ces redondances dans le texte clair, ce qui augmente grandement la résistance à la cryptanalyse. (Les fichiers qui sont trop petits pour être compressés ou qui ne se compressent pas bien ne sont pas compressés.)

PGP crée ensuite une *clé de session*, qui est une clé secrète qui ne sert qu'une fois.
Cette clé est un nombre aléatoire généré à partir des mouvements aléatoires de votre souris et des touches du clavier sur lesquelles vous tapez. Cette clé de session fonctionne avec un algorithme de chiffrement conventionnel très sûr et rapide qui chiffre le texte clair; le résultat est le texte chiffré. Une fois que les données sont chiffrées, la clé de session est elle-même chiffrée avec la clé publique du destinataire. Cette clé de session chiffrée par la clé publique est transmise avec le texte chiffré au destinataire.

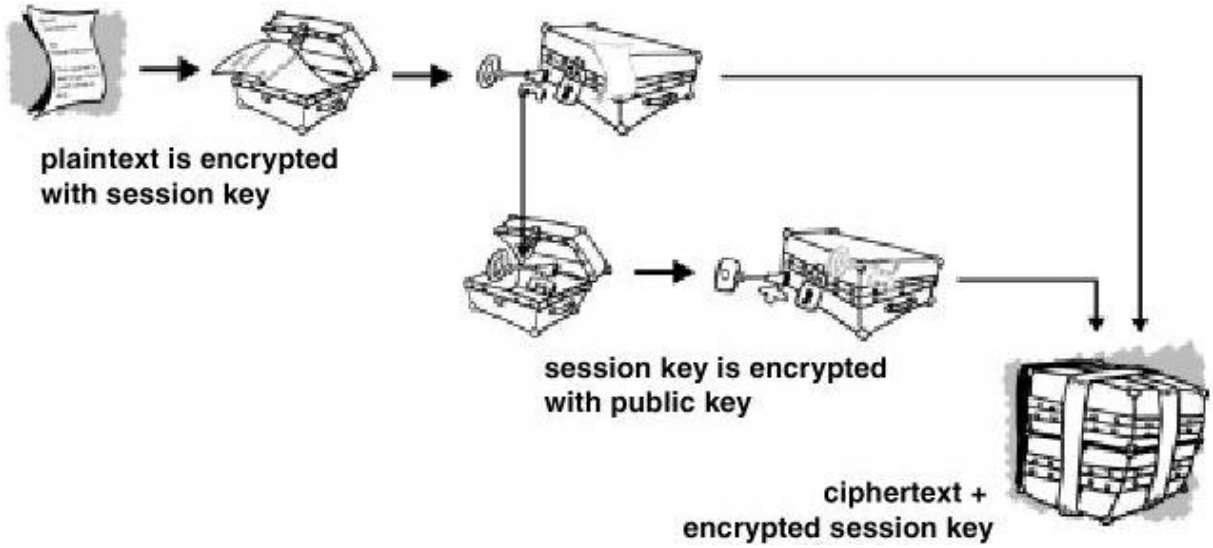


Figure I.8 Comment fonctionne le chiffrement de PGP

Le déchiffrement fonctionne de la manière inverse. La copie de PGP du destinataire utilise la clé privée de celui-ci pour retrouver la clé de session temporaire, que PGP utilise ensuite pour déchiffrer le texte chiffré de manière conventionnelle.

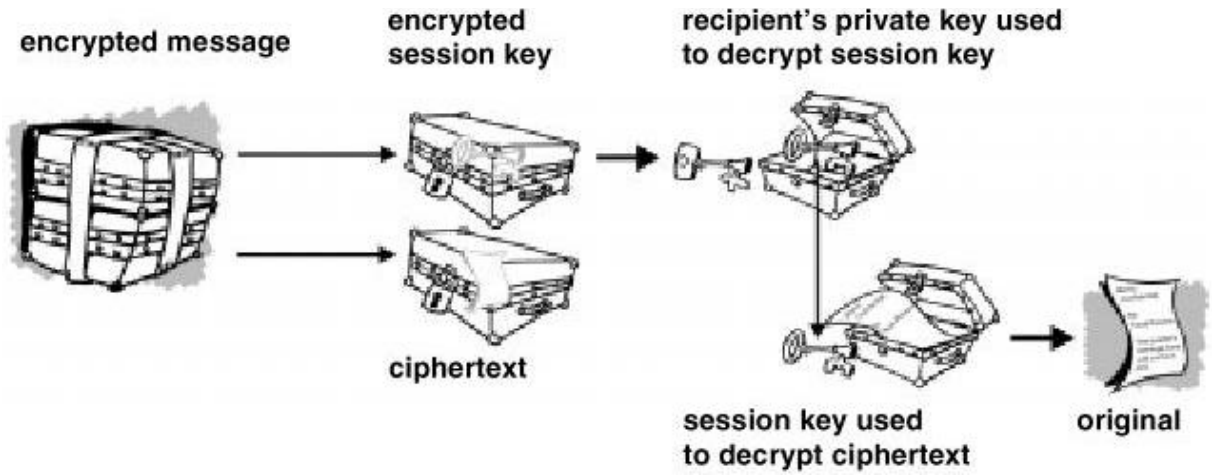


Figure I.9 Comment fonctionne le déchiffrement de PGP

La combinaison des deux méthodes de chiffrement associe la commodité du chiffrement à clé publique avec la vitesse du chiffrement conventionnel. Le chiffrement conventionnel est environ 1000 fois plus rapide que le chiffrement à clé publique. Le chiffrement à clé publique fournit quant à lui une solution aux problèmes de distribution de la clé et de transmission des

données. Utilisées toutes les deux, la performance et la distribution de la clé sont améliorées sans aucun sacrifice sur la sécurité.

2. Le réseau privé virtuel (VPN)

a. Qu'est-ce qu'un VPN ?

Le VPN (Virtual Private Network), réseau privé virtuel, est une technologie permettant de communiquer à distance de manière privée, comme on le ferait au sein d'un réseau privé de type intranet d'entreprise.
Ces réseaux offrent deux avantages majeurs :
De hautes performances en termes de bande passante, autrement dit des communications à très haut débit et de très grande qualité.
La sécurité et la confidentialité des données.
En d'autres termes, il est aujourd'hui possible, grâce à ces technologies, d'étendre son réseau privé d'entreprise à toute la planète.
Ainsi, un commercial en déplacement pourra se connecter au réseau de son entreprise indépendamment du lieu où il se trouve. A tout moment il peut envoyer ou recevoir des données confidentielles de manière sécurisée et rapide.
De manière similaire, deux sites d'une même entreprise pourront être virtuellement réunis en un seul site, l'interconnexion entre ces deux sites offrant les mêmes prestations qu'un réseau local.
Il existe deux types différents de VPN :

- Le VPN IPSec sur le réseau IP Public.
- Le VPN MPLS sur un réseau IP Privé.

Le VPN IP Public est un réseau s'appuyant sur Internet, tandis que le VPN IP Privé est un réseau entièrement hébergé par l'opérateur.

b. VPN IPSec (IP Public) :

Dans un réseau VPN IP Public, les données sont cryptées chez l'expéditeur avant d'emprunter un tunnel VPN à travers Internet qui le relie au récepteur. Elles sont ensuite décryptées chez le récepteur.

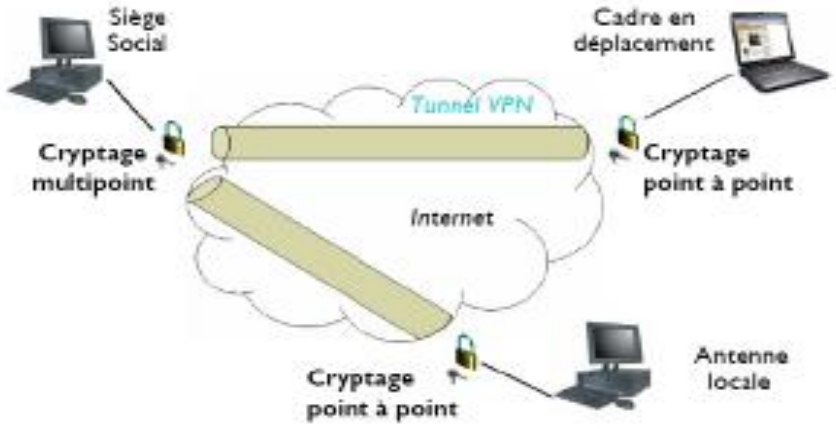


Figure I.10 VPN IPSec

On parle de cryptage « point à point » lorsqu'il n'y a qu'un expéditeur et un récepteur (par exemple, le siège social et une antenne locale), et on parle de cryptage « multipoint » lorsqu'il y en a plusieurs (par exemple, le siège social et les différents cadres en déplacement). Le tunnel VPN relie directement l'expéditeur et le récepteur par le biais du réseau classique Internet, empêchant un utilisateur tiers d'intercepter les données, qui demanderaient en outre à être décryptées avant de pouvoir être lues.

c. VPN IP MPLS (IP Privé) :

Dans un VPN IP Privé, il n'y a pas de cryptage point à point. Les données ne transitent pas via Internet, mais via un réseau spécial hébergé par l'opérateur, qui traite les données de manière spécifique. Autrement dit, contrairement au VPN IP Public, les données ne subissent aucun traitement au niveau des ordinateurs de l'expéditeur et du récepteur, elles subissent ce traitement au niveau du réseau MPLS hébergé par l'opérateur.

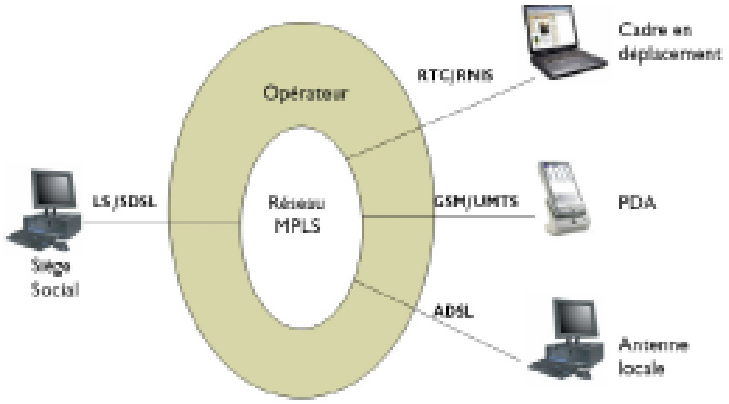


Figure I.11 VPN IP MPLS

A l'entrée du réseau MPLS, les données arrivent par paquets à un routeur étiqueteur d'extrémité (LER, Label Edge Routeur) qui leur assigne une étiquette (label) en fonction de leur nature, leur provenance, leur mode de transport… puis il leur assigne un trajet spécifiquement adapté à cette étiquette. Les paquets de données ainsi étiquetés suivent leur trajet spécifique, balisé par des routeurs étiqueteurs intermédiaires (LSR, Label Switching Routeur) qui les « aiguillent » sur le bon chemin tout au long de leur trajet. Ce système d'étiquetage des données permet au responsable du réseau au sein de l'entreprise de définir des ordres de priorité. Il peut par exemple configurer son réseau de manière à ce que les données provenant du siège social soient prioritaires sur toutes les autres. Il peut également rendre prioritaires les données multimédia, afin de permettre par exemple l'usage de la vidéoconférence.

d. Comparaison IP Public /IP Privé :

	IP public	IP privé
Connexion	Connexion sécurisée via Internet	Connexion directe sur le réseau de l'opérateur
Rapidité	Ralentissements dus au cryptage et au décryptage.	Optimisée (choix de la route la plus rapide)
Sécurité	Cryptage + tunnels. Mais chaque site est vulnérable aux attaques de par le fait qu'il est connecté à Internet.	Réseau entièrement privé géré par l'opérateur.
Administration, gestion, mise en œuvre	Supervision, gestion et mise en œuvre des équipements réalisés par le client ou par une société de service.	Supervision gestion et mise en œuvre des équipements réalisées par l'opérateur. Mise à disposition d'une solution de supervision centralisée
Evolutivité	Configuration complète du nouveau site à faire, redéfinition de l'attribution des tunnels.	Nouvelle connexion au réseau de l'opérateur – pas de modification de configuration pour le client.

Tableau I.3 Comparaison IP Public /IP Privé

Pour un choix de moindre coût il faut mieux choisi IP public (internet) mais si en veut faire plus de sécurité il faut mieux choisir IP privé.

3. Firewall (pare feu) :

Dès lors qu'un réseau privé est connecté à un réseau public, son intégrité peut être affectée par des intrusions. Pour contrer ces intrusions, l'idée est de placer des équipements appelés pare-feu (ou « firewall ») à la frontière de ce réseau, leur but étant de filtrer tout le trafic échangé avec le réseau extérieur et de ne laisser passer que le trafic autorisé.

Si l'objectif premier des pare-feu est de se protéger des intrusions sur les réseaux privés, il existe d'autres objectifs bien souvent mis en avant dans les brochures commerciales. Il s'agit principalement d'améliorer la productivité des entreprises en contrôlant l'accès qui est fait à Internet par les employés. En effet, l'accès étant filtré, les employés ne peuvent bien souvent plus consulter Internet à des fins personnelles. Les ressources du réseau de l'entreprise sont donc mieux exploitées et les employés se concentrent davantage sur leur travail.

Les techniques de filtrage se sont beaucoup enrichies depuis le milieu des années 1990. Plusieurs familles de pare-feu existent, suivant que le filtrage, plus ou moins fin, est réalisé au

niveau IP (Internet Protocol), TCP (Transport Control Protocol) ou applicatif, sur un équipement de réseau ou un ordinateur personnel. Des techniques de filtrage ont récemment été développées pour améliorer les performances de filtrage, comme les mécanismes d'inspection de paquet dynamique (« stateful inspection ») et les systèmes de prévention d'intrusion (IPS : Intrusion Prevention System). Enfin, plusieurs architectures de pare-feu aboutissent à des niveaux de sécurité plus ou moins élevés.

4. DMZ (zone démilitarisée) :

Notion de cloisonnement :

Les systèmes pare-feu permettent de définir des règles d'accès entre deux réseaux.
Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « cloisonnement des réseaux » (le terme isolation est parfois également utilisé).

Architecture DMZ :

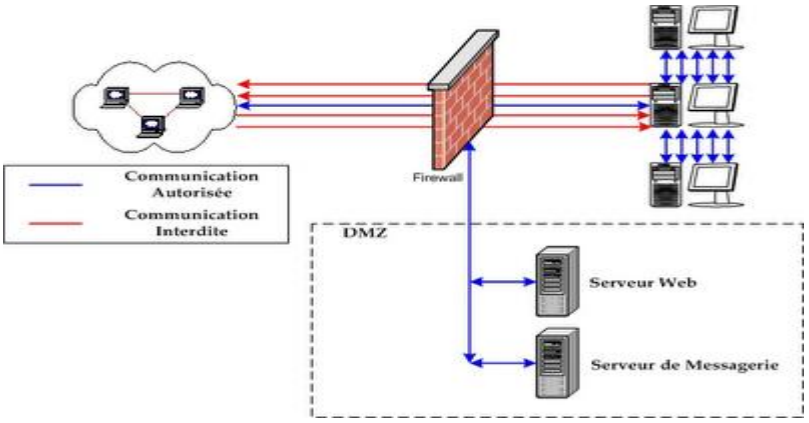


Figure I.12 Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé » (notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. La figure ci-dessous montre la position d'une DMZ au sein d'un réseau.
Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant poste dans le réseau de l'entreprise.
La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.

- Trafic du réseau interne vers la DMZ autorisé.
- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe interdit.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.
Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

5. NAT « Network Address Translation » :

Principe du NAT :

Le mécanisme de translation d'adresses « NAT » a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).
En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.
Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle. Cette passerelle peut être un routeur tel que montré dans la figure suivante.

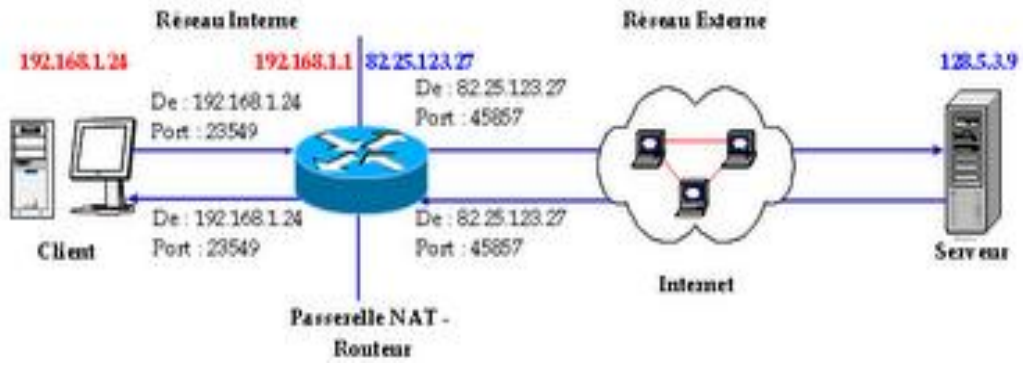


Figure I.13 Le mécanisme de translation d'adresses

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

Espaces d'adressages :

L'organisme gérant l'espace d'adressage public (adresses IP routables) est l'IANA. La RFC 1918 définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse IP publique allouée par l'IANA.

Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :

Classe A : plage de 10.0.0.0 à 10.255.255.255 ;

Classe B : plage de 172.16.0.0 à 172.31.255.255 ;

Classe C : plage de 192.168.0.0 à 192.168.255.55 ;

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

Translation statique :

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

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

Avantages et inconvénients du NAT statique :

En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible sur Internet. Par contre, on remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP... D'autre part, tant qu'à donner une adresse publique par machine, pourquoi ne pas leur donner cette adresse directement plutôt que de passer par un intermédiaire ? A cette question, on peut apporter plusieurs éléments de réponse. D'une part, il est souvent préférable de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées. Ainsi, si on doit faire des modifications, changements, interventions sur le réseau local, on peut facilement changer la correspondance entre les adresses privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche. D'autre part, on gâche un certain nombre d'adresses lorsqu'on découpe un réseau en sous-réseaux (adresse de réseau, adresse de broadcast...), comme lorsqu'on veut créer une DMZ pour rendre ses serveurs publiques disponibles. Avec le NAT statique, on évite de perdre ces adresses.

Malgré ces quelques avantages, le problème de pénurie d'adresses n'a toujours pas été réglé. Pour cela, on va se pencher sur la NAT dynamique.

Translation dynamique :

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

Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables, le NAT dynamique utilise le mécanisme de translation de port (PAT - Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

Avantages et inconvénients du NAT dynamique :

Comme nous l'avons vu, le NAT dynamique permet à des machines ayant des adresses privées d'accéder à Internet. Cependant, contrairement au NAT statique, il ne permet pas d'être joint par une machine de l'Internet. Effectivement, si le NAT dynamique marche, c'est parce que le routeur qui fait le NAT reçoit les informations de la machine en interne (Adresse IP, port TCP/UDP). Par contre, il n'aura aucune de ces informations si la connexion est initialisée de l'extérieur... Le paquet arrivera avec comme adresse de destination le routeur, et le routeur ne saura pas vers qui rediriger la requête en interne.

La NAT dynamique ne permet donc que de sortir sur Internet, et non pas d'être joignable. Il est donc utile pour partager un accès Internet, mais pas pour rendre un serveur accessible. De plus, étant donné que l'on peut "cacher" un grand nombre de machines derrière une seule adresse publique, cela permet de répondre à notre problème de pénurie d'adresses.

Par contre, les machines n'étant pas accessibles de l'extérieur, cela donne un petit plus au niveau de la sécurité.

IX. But de la sécurité

La sécurité informatique tente de maintenir six caractéristiques principales :

a. *La confidentialité :* représente le fait que les données informatiques ne sont accessibles que par les personnes autorisées. Le type d'accès s'étalant de la simple connaissance de l'existence de l'objet à la surimpression de celui-ci. La confidentialité reste la notion de sécurité informatique la plus proche du monde réel et semble dès lors la plus claire.

b. *L'authentification:* dans le cas d'un simple message, le service d'authentification assure que le message provient de l'endroit d'où il prétend venir. Dans le cas d'un échange bidirectionnel, deux aspects sont présents. Il faut assurer que les deux entités sont bien ce qu'elles affirment être. De plus, le service d'authentification doit montrer que la connexion ne peut être brouillée par une troisième entité essayant de se faire passer pour un des deux correspondants.

c. *L'intégrité :* signifie que l'information ne peut être modifiée que par les personnes autorisées ou seulement par les moyens autorisés. L'intégrité reste un domaine très large couvrant à la fois les modifications, les moyens de modification mais également l'après-modification et donc la consistance.

d. *La disponibilité :* se reflète dans l'information et dans les services. Ce domaine est aujourd'hui en pleine expansion. Il regroupe des sujets aussi variés que les temps de réponse, la tolérance aux fautes, le contrôle de concurrence, le partage équitable de ressources, ...
e. *La non-répudiation :* permet au récepteur ou à l'émetteur de ne pas refuser un message transmis. Donc, quand un message est envoyé, le récepteur peut prouver que le message a bien été envoyé par l'émetteur. De même, lorsqu'un message est reçu, l'émetteur peut prouver que le message a bien été reçu par le bon récepteur.

f. *Le contrôle d'accès :* représente la capacité de limiter et de contrôler les accès aux systèmes et applications via les liens de communication. Pour cela, chaque entité demandant un accès se voit identifiée ou authentifiée afin de lui adapter ses droits d'accès.

Ce sont ces six buts qui forment ensemble la sécurité informatique. Parfois, ils se chevauchent mais ils peuvent éventuellement être mutuellement exclusifs (ex. une confidentialité trop forte entraînant une perte de disponibilité).

X. Conclusion

Dans ce chapitre, on a présenté quelques notions générales sur réseau et la sécurité, dans le prochain chapitre on va détailler l'une des solutions de protection de réseaux la plus efficace et qui est très fortement conseillée de déployer même sur le PC personnel: le firewall.

CHAPITE II : Généralités sur les firewalls

I. Définition

La traduction officielle du terme anglais firewall est, mur anti feu ou pare-feu . La définition qui est associée est la suivante :
« Dispositif informatique qui filtre les flux d'informations entre un réseau interne à un organisme et un réseau externe en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur. »
Cette description souffre de quelques erreurs parmi lesquelles le recours aux notions d'intérieur et d'extérieur qui sont des notions étrangères à l'équipement et qui relèvent en fait de choix d'architecture, et un présupposé restrictif sur la politique de sécurité applicable.
On pourra retenir de façon assez large qu'il s'agit d'un dispositif informatique de filtrage de protocoles réseaux (routables) et, par extension, d'un système ou d'un groupe de systèmes permettant d'imposer une politique de sécurité entre plusieurs périmètres réseaux.

Figure II.14 Le pare-feu

II. Le fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :
-soit d'autoriser uniquement les communications ayant été explicitement autorisées
-soit d'empêcher les échanges qui ont été explicitement interdits.
Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité adoptée par l'entreprise désirant mettre en œuvre un filtrage des communications. La première méthode de pare-feu est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

III. Principes du filtrage :

Selon l'équipement, des informations sont extraites des flux réseaux depuis une ou plusieurs des couches 2 à 7 du modèle OSI, éventuellement corrélées entre elles, et comparées à un ensemble de règles de filtrage. Un état peut être mémorisé pour chaque flux identifié, ce qui permet en outre de gérer la dimension temporelle avec un filtrage en fonction de l'historique du flux.

Les types de filtrage les plus courants sont :

- Liaison (adresse MAC Ethernet,...),
- Réseau (entêtes IP, IPX,... et type/code ICMP),
- Transport (ports TCP/UDP),
- Filtrage adaptatif (« stateful inspection ») ou dynamique,
- Session (« circuit level gateway », « proxys » génériques),
- Application : serveur(s) mandataire(s)/relais applicatifs (« proxys »).

Dans la pratique une combinaison des types précédents est utilisée : un pare-feu protégeant un serveur http fera passer les requêtes clientes à travers un relais applicatif tandis que la réponse serveur ne sera analysée qu'au niveau transport pour mettre à jour l'état des sessions dynamiques.

1. **Le filtrage de paquets IP :**

Il s'agit d'un filtrage réalisé au niveau des couches 2 à 4 dans un routeur - une passerelle -, un pont ou un hôte.

Les critères se basent sur les champs des entêtes des différentes couches ainsi que sur l'interface d'entrée ou de sortie du paquet :

- Couche 2 : adresse MAC,
- protocole IP (généralement limité au choix accepté/refusé à l'exception des types 1 ICMP, 6 TCP et 17 UDP qui bénéficient d'une meilleure granularité),
- durée de vie (TTL : typiquement les paquets arrivant à expiration peuvent être éliminés),
- adresses IPs source et destination,
- « Flags » et options IP.
- Couche 4 (et ICMP) :
- ports source et destination (TCP/UDP),
- « Flags » TCP,
- type/code (ICMP).

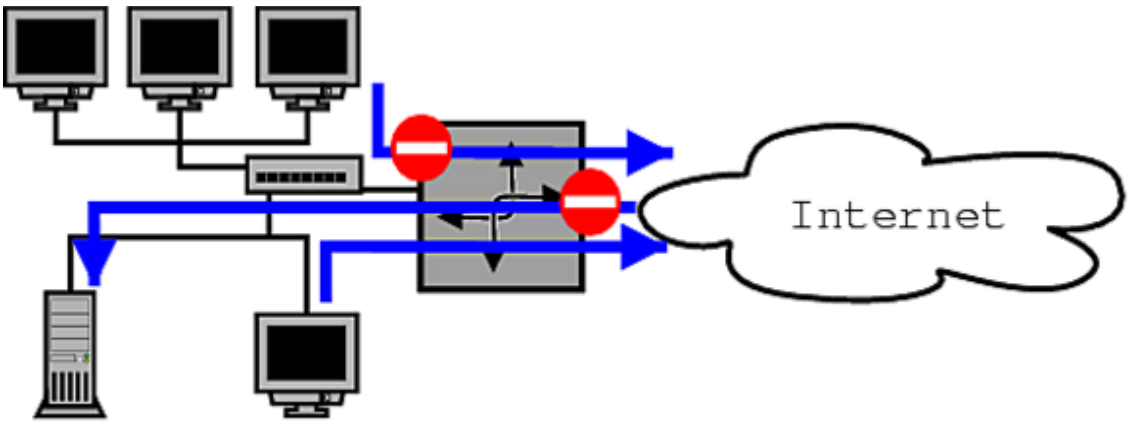


Figure II.15 Le filtrage de paquets IP

Les avantages :

- l'espace noyau est performant mais plus risqué (une faille induit un risque de compromission administrateur/root),
- il est facilement adaptable au routage (un routeur est par essence un filtre),
- il est transparent pour l'utilisateur,
- il permet une corrélation adresse source/interface en particulier :
- « anti-spoof » (les paquets avec une adresse source correspondant à l'adressage interne ne peuvent venir de l'extérieur),
- « egress filtering » (vérifier que les adresses sources sortant du domaine interne sont cohérentes avec le plan d'adressage).
- cependant il suppose que les applications respectent les ports par défauts assignés par l'IANA (si on laisse ouvert l'accès au port 25/tcp (smtp), un serveur http écoutant sur ce port au lieu de 80/tcp sera alors accessible),
- en l'absence d'historique, beaucoup de ports doivent rester ouverts pour permettre le passage des paquets en retour. Exemple de règles pour l'accès web (http) :
  192.168.10.0/24:1024-65535 => *:80
  192.168.10.0/24:1024-65535 <= *:80

Les inconvénients :

- il ne gère pas l'abstraction de la résolution de nom (mal adapté au filtrage des bannières insérées depuis domaine. envahissant.tld,...),
- la fragmentation IP pose problème (les informations de la couche transport peuvent être : absentes du 1er paquet, réparties sur plusieurs paquets, n'apparaissent pas dans les paquets suivants,...),
- l'adresse et le port source ne sont pas des données fiables,
- le filtrage des services RPC (« Remote Procédure Call ») est complexe : les ports ne sont pas standardisés et sont assignés dynamiquement (on ne peut se limiter à filtrer le service de mappage, une recherche par balayage des ports restant possible),
- il ne peut prendre en compte les services avec ports dynamiques : FTP,...
- il est difficile de filtrer spécifiquement un ou des hôtes si DHCP est employé sans précaution,
- il n'y a généralement pas de filtrage des utilisateurs.

2. <u>Le filtrage en couches 5 à 7 : les serveurs mandataires :</u>

On peut distinguer deux types de serveur mandataire (« proxy », qui agit en lieu et place de son mandant, un serveur ou un client) :

a. <u>*Les génériques, appelés « Circuit Level Gateway »*</u> qui valident la session avant d'ouvrir une connexion (vérifications adresses/ports source et destination, identifiant utilisateur, éventuelle requête ident,...) ; il s'agit généralement de SOCKS (la V4 supporte TCP uniquement, et la V5 rajoute l'UDP et le support de protocoles d'authentifications fortes),

b. <u>*Les relais applicatifs,*</u> qui ne supportent qu'un protocole de haut niveau particulier (http, smtp,...), dont les principales caractéristiques sont :

- relais soumis à la politique de sécurité,

- ne supporte qu'un sous-ensemble minimal de la RFC de manière à avoir un code réduit et donc moins susceptible d'inclure une faille majeure,
- peut inclure une fonction cache.

La notion de « reverse-proxy » est parfois employée : elle désigne les relais qui sont mandataires pour un serveur ; le cas le plus courant, donc appelé « proxy », étant de faire écran pour des clients.

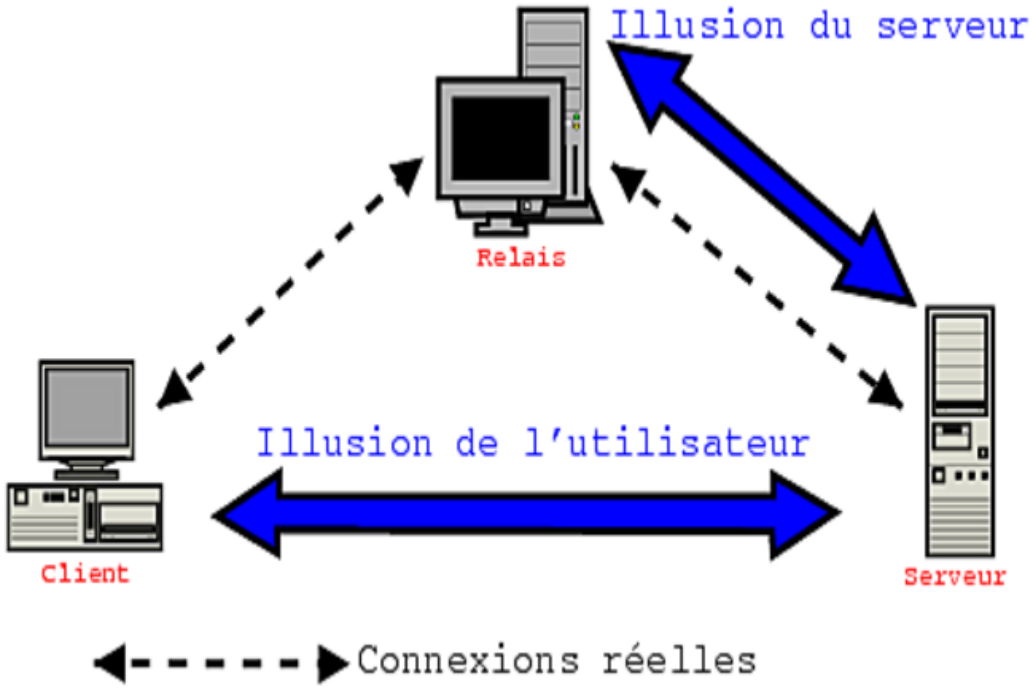


Figure II.16 Le serveur mandataire

Les avantages :

- Possibilité de filtrage de contenu (scripts, applets java, ActiveX,...) et sémantique, mais qui n'est pas toujours utilisable dans la pratique, beaucoup de sites recourant massivement à ces technologies sans offrir de présentation alternative,
- interface possible avec un antivirus (protocole d'échange le plus courant : CVP développé par Check Point Software),
- authentification possible des utilisateurs,
- masque les adresses des machines clientes.

Les inconvénients :

- ne nécessite pas de fonction de routage,
- processus en espace utilisateur [une vulnérabilité peut être moins critique si les privilèges sont bien gérés, mais vulnérabilités additionnelles du système d'exploitation sous-jacent - pile IP, journalisation,...-] qui peut être plus lent (changements de contexte noyau/espace utilisateur),
- anonymisation des clients ou des serveurs avec les mêmes limitations que le filtrage de contenu,
- nécessite un serveur relais différent par application ou de se limiter à un filtrage générique,

- il faut un processus par connexion (20 utilisateurs dont le butineur réalise 5 connexions simultanées induit 100 processus ou fils),
- ne peut être employé pour des protocoles aux spécifications fermées,
- sont difficilement transparents :
- configuration spécifique des clients (par exemple des butineurs),
- bibliothèque client spécifique (SOCKS),
- « redirection » par filtre de paquets basée sur le port destination.

3. Le filtrage dynamique et adaptatif

Ce mécanisme se veut le meilleur des deux mondes précédents en apportant une capacité de filtrage applicative tout en restant au niveau de la couche transport/session.

Le filtrage dynamique ajoute la prise en compte de l'historique au simple filtrage de paquet : l'idée de base étant qu'avec un échange client/serveur si un paquet est passé dans un sens il en passera un dans l'autre (commutation de la source et destination du couple IP/port pour les paquets TCP/UDP). Diverses temporisations sont introduites : poignés de main TCP, fermeture de connexion ou de session,.... Ce mode permet de générer à la volée des règles temporaires de filtrage des paquets. Ces dernières disparaissent lorsqu'aucun paquet ne passe pendant un délai configuré ou avec la fermeture de la session en TCP (RST, FIN).

En reprenant l'exemple précédent de l'accès au service http : Règle dynamique : 192.168.10.0/24:1024-65535 => *:80

Initiation d'une connexion : 192.168.10.12:1036 => 10.0.0.1:80

Règle générée temporairement : 192.168.10.12:1036 <= 10.0.0.1:80

Le filtrage adaptatif recherche, en outre, des signatures dans le segment de données des paquets afin de déterminer le type et l'état du protocole applicatif transporté et de procéder ainsi à des vérifications de cohérences. C'est dans cette catégorie que l'on peut ranger le terme de « stateful inspection » utilisée par divers éditeurs.

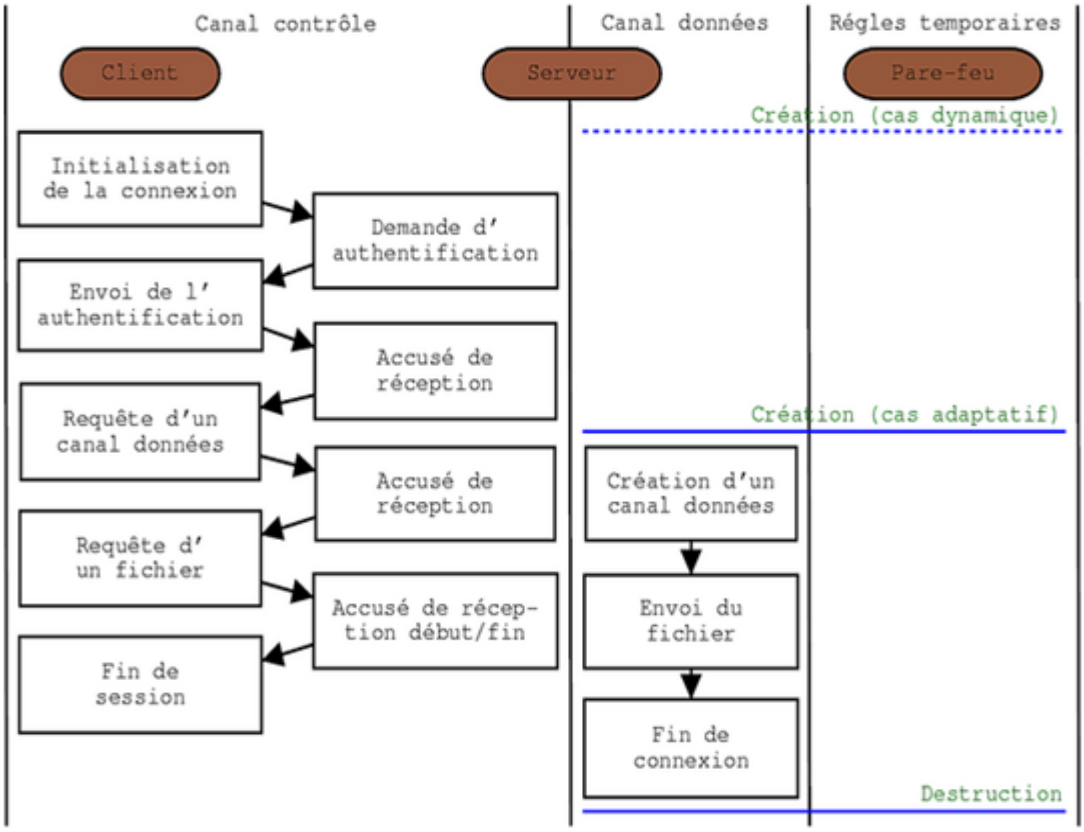


Figure II.17 Règles dynamiques et adaptatives pour une session FTP active

Les avantages :

- Moins de ports ouverts qu'avec le filtrage de paquet simple,
- Analyse du contenu applicatif avec les performances et les risques du mode noyau.

Les inconvénients :

- Limitation de l'adaptatif aux protocoles applicatifs connus et documentés,
- A l'inverse du serveur mandataire applicatif, le filtre adaptatif peut être induit en erreur quant à l'état du protocole et donc être source de comportements vulnérables (création de règles dynamiques sous contrôle d'un client distant par exemple).

IV. Les autres fonctionnalités

L'évolution des pare-feu a conduit à l'ajout de fonctionnalités dont le domaine peut sembler connexe. Parmi celles-ci ont peut distinguer :

a. *Les réseaux privés virtuels « VPN » :* les possibilités proposées vont de la création d'un « extranet » (réseau interne multi-site utilisant des tunnels chiffrant entre sites) à la sécurisation de l'accès aux ressources internes des itinérants ;

b. *L'authentification :* peut être intégrée dans les relais, qui peuvent alors généralement s'interfacer avec les serveurs d'authentification les plus répandus (Radius, SecurID,...)

c. *Élection du routeur :* les hôtes étant supposés avoir une adresse IP de passerelle par défaut statique, la redondance est assurée par plusieurs routeurs qui partagent cette adresse et se coordonnent grâce une diffusion « multicast » utilisant le protocole 112/ip. Dans le domaine on trouve VRRP (RFC 3768) évolution du protocole HSRP de Cisco et CARP issu du monde OpenBSD et étendu aux autres BSDs mais qui n'est pas officialisé par l'IANA,

d. *Synchronisation des tables de filtrage :* OpenBSD a développé pfsync pour le système de filtrage pf ; utilisant toujours du « multicast » mais sur 240/ip également sans officialisation de l'IANA.

La traduction d'adresse qui consiste à réécrire les champs adresse IP source et/ou destination pour permettre le routage d'adresses privées, répondre à la pénurie d'adresses IPv4, tenter de dissimuler le plan d'adressage interne,...

enfin certains équipements se proposent d'inclure des filtres du niveau applicatif, comme un antivirus, la recherche de contenus licencieux, une sonde de détection d'intrusion,...Cela se fait généralement au prix d'une consommation de ressources (recherches de signatures) qui peut grever les performances globales, et cela contrevient au principe de minimisation de la taille du code pour minimiser les risques de faille résiduelle.

V. Les différents types de firewall

1. Les firewalls bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse Ip, et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker lambda. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc « Faire » avec ses règles, et essayer de les contourner.

Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence.

Ces firewalls se trouvent typiquement sur les Switchs.

Les Avantages

- Impossible de l'éviter (les paquets passeront par ses interfaces)
- Peu coûteux

Inconvénients :

- Possibilité de le contourner (il suffit de passer outre ses règles)
- Configuration souvent contraignante
- Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

2. Les firewalls matériel

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. De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile, et le constructeur a eu toute latitude pour produire des systèmes de codes « signés » afin d'authentifier le logiciel (système RSA ou assimilés). Ce système n'est implanté que dans les firewalls haut de gamme, car cela évite un remplacement du logiciel par un autre non produit par le fabricant, ou toute modification de ce dernier, rendant ainsi le firewall très sûr. Son administration est souvent plus aisée que les firewalls bridges, les grandes marques de routeurs utilisant cet argument comme argument de vente. Leur niveau de sécurité est de plus très bon, sauf découverte de faille éventuelle comme tout firewall. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un firewall d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance ses besoins et choisir le constructeur du routeur avec soin.

Avantages :

- Intégré au matériel réseau.
- Administration relativement simple.
- Bon niveau de sécurité.

Inconvénients :

- Dépendant du constructeur pour les mises à jour.
- Souvent peu flexibles.

3. Les firewalls logiciels

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

Les firewalls personnels

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

Avantage :

- Sécurité en bout de chaîne (le poste client).
- Personnalisable assez facilement.

Inconvénients :

- Facilement contournable.
- Difficiles à départager de par leur nombre énorme.

4. Les firewalls plus « sérieux »

Tournant généralement sous linux, car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les

firewalls matériels des routeurs, à ceci prêt qu'ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme.

Avantage :

- Personnalisables
- Niveau de sécurité très bon

Inconvénients :

- Nécessite une administration système supplémentaire

Ces firewalls logiciels ont néanmoins une grande faille : ils n'utilisent pas la couche bas réseau. Il suffit donc de passer outre le noyau en ce qui concerne la récupération de ces paquets, en utilisant une librairie spéciale, pour récupérer les paquets qui auraient été normalement « droppés » par le firewall. Néanmoins, cette faille induit de s'introduire sur l'ordinateur en question pour y faire des modifications... chose qui induit déjà une intrusion dans le réseau, ou une prise de contrôle physique de l'ordinateur, ce qui est déjà Synonyme d'inefficacité de la part du firewall.

VI. Les réactions des firewalls aux attaques classiques

IP spoofing

L'IP spoofing consiste à modifier les paquets IP afin de faire croire au firewall qu'ils proviennent d'une adresse IP considérée comme « de confiance ». Par exemple, une IP présente dans le réseau local de l'entreprise. Cela laissera donc toute latitude au hacker de passer outre les règles du firewall afin d'envoyer ses propres paquets dans le réseau de l'entreprise. Les derniers firewalls peuvent offrir une protection contre ce type d'attaque, notamment en utilisant un protocole VPN, par exemple IPSec. Cela va crypter les entêtes des paquets, et ainsi rendre impossible leur modification par un intrus, et surtout, l'intrus ne pourra générer de paquets comme provenant de ce réseau local, ce dernier n'ayant pas la clé nécessaire au cryptage. Les algorithmes utilisés dans de tels protocoles sont de type RSA.

DOS et DDOS

Le DOS, ou Denial Of Service attack, consiste à envoyer le plus de paquets possibles vers un serveur, générant beaucoup de trafic inutile, et bloquant ainsi l'accès aux utilisateurs normaux. Le DDOS, pour Distributed DOS, implique venir de différentes machines simultanées, cette action étant le plus souvent déclenchée par un virus : ce dernier va d'abord infecter nombre de machines, puis à une date donnée, va envoyer depuis chaque ordinateur infecté des paquets inutiles vers une cible donnée. On appelle aussi ce type d'attaque « flood ». Les firewalls ici n'ont que peu d'utilité. En effet, une attaque DOS ou DDOS utilise le plus souvent des adresses sources différentes (le but n'est pas de récupérer une réponse ici) et souvent, impossible de distinguer ces paquets des autres... Certains firewalls offrent une protection basique contre ce genre d'attaque, par exemple en droppant les paquets si une source devient trop gourmande, mais généralement, ces protections sont inutiles. Cette attaque brute reste un des gros problèmes actuels, car elle est très difficilement évitable.

Port scanning

Ceci constitue en fait une « pré-attaque » (Etape de découverte). Elle consiste à déterminer quels ports sont ouverts afin de déterminer quelles sont les vulnérabilités du système. Le firewall va, dans quasiment tous les cas, pouvoir bloquer ces scans en annoncent le port comme « fermé ». Elles sont aussi aisément détectables car elles proviennent de la même source faisant les requêtes sur tous les ports de la machine. Il suffit donc au firewall de bloquer temporairement cette adresse afin de ne renvoyer aucun résultat au scanner.

Exploit

Les exploits se font en exploitant les vulnérabilités des logiciels installés, par exemple un serveur Http, Ftp, etc. Le problème est que ce type d'attaque est très souvent considéré comme des requêtes tout a fait « valides » et que chaque attaque est différente d'une autre, vu que le bug passe souvent par reproduction de requêtes valides non prévues par le programmeur du logiciel. Autrement dit, il est quasiment impossible au firewall d'intercepter ces attaques, qui sont considérées comme des requêtes normales au système, mais exploitant un bug du serveur le plus souvent. La seule solution est la mise à jour périodique des logiciels utilisés afin de barrer cette voie d'accès au fur et à mesure qu'elles sont découvertes.

VII. Intérêts et limites du pare-feu

Avantage :

- Avec une architecture réseau cohérente, on bénéficie d'une centralisation dans la gestion des flux réseaux.
- De plus, avec un plan d'adressage correct, la configuration du pare-feu est peu ou pas sensible au facteur d'échelle (règles identiques pour 10 comme 10000 équipements protégés).
- L'utilisation de la journalisation offre une capacité d'audit du trafic réseau et peut donc fournir des traces robustes en cas d'incident, si le pare-feu n'est pas lui-même une des cibles.
- Enfin le pare-feu permet de relâcher les contraintes de mise à jour rapide de l'ensemble d'un parc en cas de vulnérabilité sur un service réseau : il est possible de maintenir une certaine protection des équipements non vitaux au prix de la dégradation du service avec la mise en place d'un filtrage.

Inconvénients :

- La capacité de filtrage d'un équipement dépend de son intégration dans le réseau mais le transforme en goulet d'étranglement (capacité réseau et ressources du pare-feu).
- De par sa fonction, le pare-feu est un point névralgique de l'architecture de sécurité avec de fortes contraintes de disponibilité. Il existe des solutions permettant la synchronisation de l'état des pare-feu, comme l'élection du routeur avec VRRP, ou le système de haute disponibilité CARP/pfsync développé pour OpenBSD, mais beaucoup de configurations reposent encore sur un équipement unique.

Enfin une bonne gestion d'un pare-feu nécessite la compréhension des protocoles filtrés surtout lorsque les interactions deviennent complexes comme dans les cas FTP, H323,...avec le transport de paramètres de connexion dans le segment de données. De plus il apparaît bien souvent des effets de bord liés aux diverses fonctions (couches réseaux filtrées, traduction d'adresses) et influencées par l'ordre d'application des règles.

Conclusion

Nous avons vu dans ce chapitre les différents types de firewalls, les différentes attaques et parades. Il ne faut pas perdre de vue qu'aucun firewall n'est infaillible et que tout firewall n'est efficace que si bien configuré. De plus, un firewall n'apporte pas une sécurité maximale et n'est pas une fin en soi. Il n'est qu'un outil pour sécuriser et ne peut en aucun cas être le seul instrument de sécurisation d'un réseau. Un système comportant énormément de failles ne deviendra jamais ultra-sécurisé juste par l'installation d'un firewall.
Toutes ces technologies sont et seront en pleine évolution, car la base même de tout cela est de jouer au chat et à la souris entre les hackers et les programmeurs de firewall ainsi que les administrateurs. Une grande bataille d'imagination qui n'aura certainement jamais de fin.

CHAPITRE III : Installation et configuration d'un firewall

I. Introduction

Dans ce chapitre, on va présenter en détail l'acheminement de notre travail, qui consiste en l'installation d'une passerelle avec règles de filtrage et de sécurité pour sécuriser un LAN.
Et la présentation d'un réseau à sécuriser.

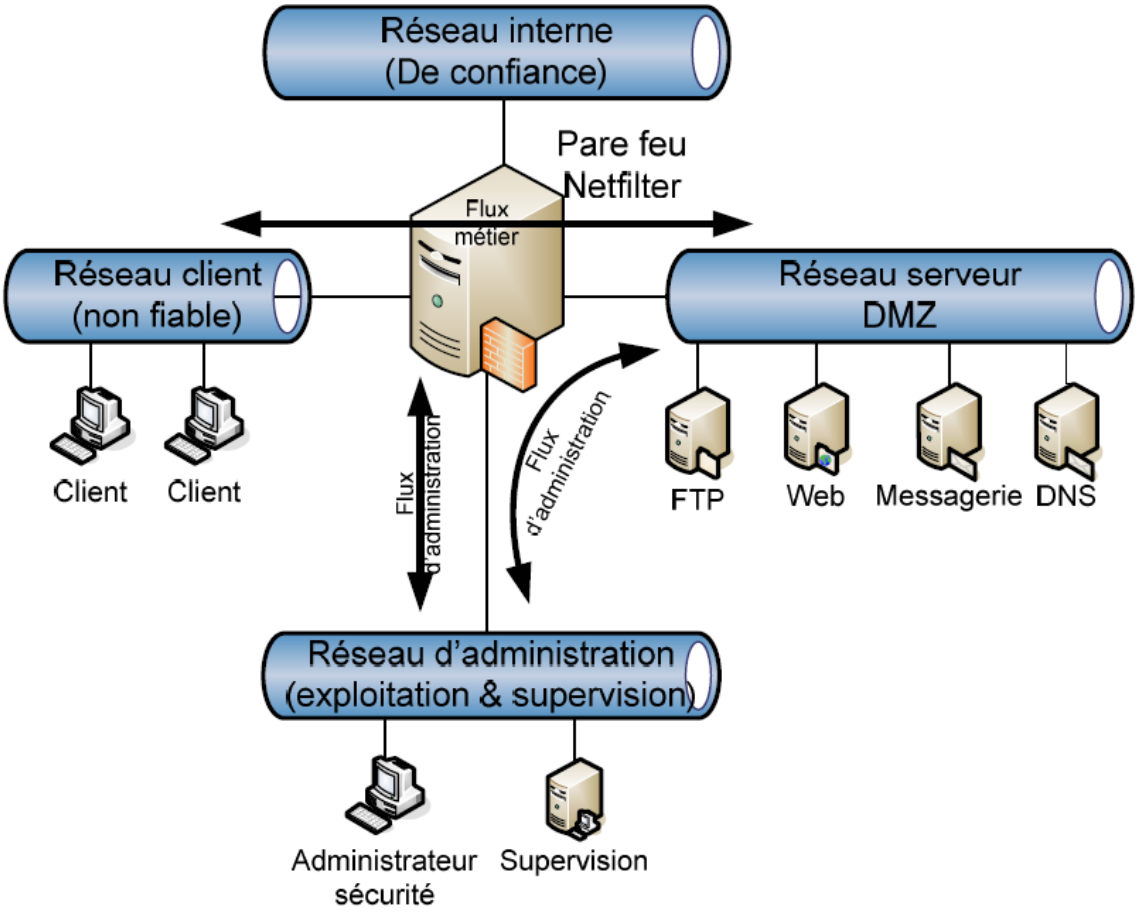


Figure II.17 : Réseau test

II. Etude comparative

Pour mener à bien notre travail, trois solutions s'offraient à nous

- Routeur ADSL Cisco 2600
- Pare-feu matériel
- Machine dédiée avec une distribution Linux Orientée passerelle Internet

Plusieurs distributions s'offraient à nous pour la mise en place d'une machine dédiée faisant office de passerelle Internet dont quelques une ci-dessous :

- Debian Sarge
- Ipcop
- Smooth Wall

III. Comparatif des différents solutions

Solution	Cisco 2600	Ordinateur Dédié	Pare-feu Matériel
			
Processeur	Cisco 2612(MPC860) Processor (révision 0x101)	Athlon XP 1800+	
Ram	64 Mo Dram	2x 512Mo DDR-SDRAM PC3200 (Chips Samsung)	64 Mo Dram
Disque Dur	8Mo Flash	Maxtor 40 Go 7200 RPM - Garantie 3 ans	
Carte Réseaux	2x Ethernet/IEEE 802.3	4x Intel Pro/100 série S:	4x Ethernet, Fast Ethernet
Nombre d'interface Réseaux possible	2	4	4
Coût Main d'œuvre en heure estimée (Install +configuration)	3h	4h	3h

Administration	HyperTerminal, Telnet, snmp	Interface Web (ssl), ssh	Interface web
Evolution Possible	Oui (très couteuse)	Oui	Non
Fonction	-DHCP	-DHCP	-Règle de filtrage
Disponible	-Règle de filtrage	-Règle de filtrage (PareFeu) -Serveur DNS (cache) -Proxy Web (graphes du proxy)	(Pare-feu)

Tableau II.4 Comparatif des solutions matérielle

IV. Solution choisie

Pour plusieurs raisons voir tableau ci-dessus, la solution de la machine dédiée a été privilégiée. La solution de la machine dédiée nous permettait d'établir des règles de filtrage plus poussés. De plus la machine dédiée nous apportait plus d'informations sur la connexion, les machines connectées aux réseaux, l'état du réseau etc.
Et parmi les inconvénients de cette solution est l'environnement.
La machine dédiée apporte d'avantage d'options que le routeur Cisco 2600 : consultation des journaux, des détails plus importants, une facilité de visualisation et de configuration.
Nous avons choisis Smoothwall pour un choix personnel puisque il n'était pas déjà traité.

V. Présentation de SmoothWall

SmoothWall est le nom de la communauté qui utilise le pare-feu Smoothwall Express.
SmoothWall Express est en fait une distribution Linux, Open Source et distribuée sous licence GPL. Smoothwall Express est dédiée à être utilisée comme pare-feu dans un réseau d'entreprise. 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. Smoothwall

Express permet de sécuriser les échanges entre Internet et le réseau interne de l'entreprise quel que soit son architecture.

VI. Architectures possibles avec Smoothwall Express

Avant d'aller plus loin, il est nécessaire de définir les termes interface *Vert*, interface *Rouge*, interface Violet et interface *Orange* :

a) Interface **Vert** : Désigne l'interface réseau (carte réseau) de *Smoothwall Express* qui sera directement reliée au réseau interne câblé de l'entreprise.
b) Interface **Rouge** : Désigne l'interface de *Smoothwall Express* qui sera reliée à Internet.
c) Interface **Violet** : Désigne l'interface réseau sans fil de *Smoothwall Express*.
d) Interface **Orange** : Désigne l'interface de *Smoothwall Express* 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…

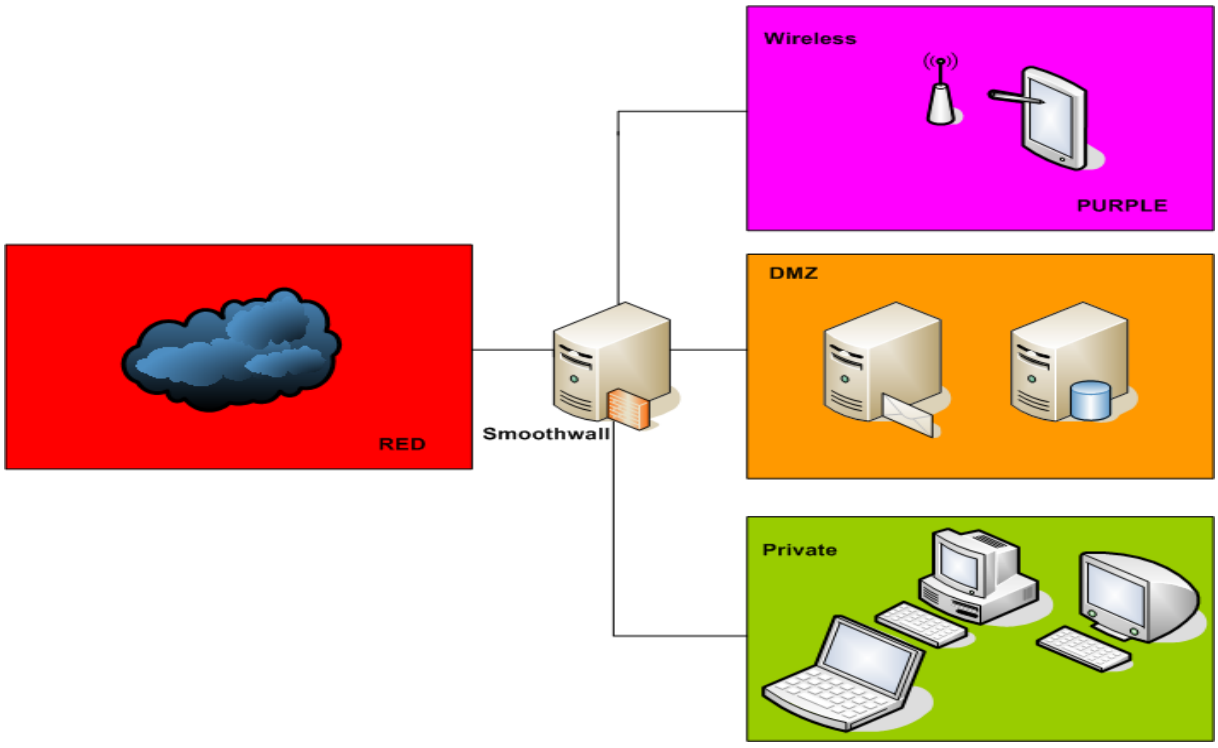


Figure II.18 Définition des interfaces Vert, Rouge, Orange et Violet

Il faut noter aussi que ces appellations ne sont pas propres à la communauté Smoothwall. On utilise généralement ces mêmes termes quelque soit le pare-feu.
Voyons maintenant les architectures réseau qu'offre Smoothwall Express :

e) Architecture vert : Cette architecture est utilisée si *Smoothwall Express* 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).
f) Architecture vert + 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.

g) Architecture vert+Rouge : *Smoothwall Express* utilisera dans ce cas de figure une carte réseau pour se connecter au réseau interne et une autre pour relier Internet.

h) Architecture vert + Orange + Rouge : L'architecture Green + Orange + Red est choisie dans le cas où l'on utilise trois cartes réseau pour relier *Smoothwall Expres* à la zone démilitarisée, le réseau interne et Internet.

i) Architecture vert + violet (Rouge is modem/ISDN): Ici l'interface rouge est directement reliée à un modem/RNIS. Smoothwall Express 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…

j) Architecture vert + violet + Orange : *Smoothwall Express* 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.

k) Architecture vert+ violet + Red : Ici on utilise deux cartes réseaux pour câbles (afin de relier le réseau interne de l'entreprise et Internet à *Smoothwall Express*) et une carte réseau sans fil pour connecter le réseau sans fil de l'entreprise au pare-feu.

l) Architecture vert + violet + 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 Express*) et une carte réseau sans fil pour connecter le réseau sans fil de l'entreprise au pare-feu.

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

Remarque :

L'installation de Smoothwall Express sur un disque dur provoquera la perte totale des données qu'il contient. Smoothwall Express n'est en outre pas développé pour fonctionner avec un autre système d'exploitation. Un double boot n'est pas possible sur une machine où est installée Smoothwall Express.

-Les spécifications suivantes sont les spécifications matérielles minimales et des recommandations pour SmoothWall Express:

Système / Matériel	Exigence / recommandations	
Processeur	Intel Pentium 200 ou processeurs compatibles.	
Mémoire	128 Mo de RAM. Plus de RAM est requis pour des services supplémentaires.	
Stockage	2 giga-octets de disque dur - périphériques IDE et SCSI pris en charge.	
Cartes d'interface réseau	A minimum of one supported network interface card (NIC). Si la connexion à Internet se fait via un dispositif à large bande comme un modem câble, ADSL ethernet présentées, ou d'une autre ethernet présenté connexion, vous aurez besoin d'une seconde carte.	
Clavier	Si le BIOS système supporte démarrage sans clavier, ce n'est que requis pour l'installation initiale.	
Carte vidéo	Seulement requis lors de l'installation SmoothWall Express.	
Moniteur	Seulement requis lors de l'installation SmoothWall Express.	
CD-ROM	Seulement requis lors de l'installation SmoothWall Express.	
Lecteur de disquette	Recommandé pour la mise à niveau des versions précédentes.	
Type de connexion internet	Internet	une carte réseau approprié est requis.
	ADSL	une carte PCI ou un modem USB soutenue est nécessaire.
	RNIS	une carte RNIS soutenus ou externe RS232 ou USB adaptateur connecté est nécessaire.
	Modem	un modem, un modem pris en charge RS232, ISA ou PCI est nécessaires

Tableau II.5 les spécifications matérielles minimales et des recommandations pour SmoothWall Express

VII. Les messages et les conventions

L'installation SmoothWall Express et les programmes de la configuration initiale utilisent une interface à base de texte qui est compatible avec tous les types de carte graphique.

Les commandes clavier suivantes sont utilisées pour interagir avec les programmes:

Clés	Explication
Flèches	Déplacer le curseur / focus / mettre en évidence entre les options.
Tab	Les progrès de la mise au point à l'objet écran suivant.
Espace	sur un bouton si elle a le focus.
Entrée ou Retour	Clique sur un bouton si elle a le focus. Clique OK si l'accent n'est pas actuellement sur un bouton.
Annuler	Quitte la section courante de l'installation ou le processus de configuration sans enregistrer ou de activant tous les changements.

	Si le programme d'installation est exécuté dans le cadre du processus d'installation pour la première fois, la Bouton pour quitter le programme d'installation et exiger que le processus d'installation pour être redémarré.
Fait	Indique que la configuration de la fonction actuelle est terminée. Les modifications seront sauvegardées et activé et le contrôle sera de retour au menu ou à la procédure d'installation.
Finis	Quitte fois tous les changements de configuration ont été réalisés dans le programme d'installation.
Ok	la sélection de l'option en surbrillance, reconnaît un message ou précède à l'écran suivant.

VIII. Installation et configuration de Smoothwall express:

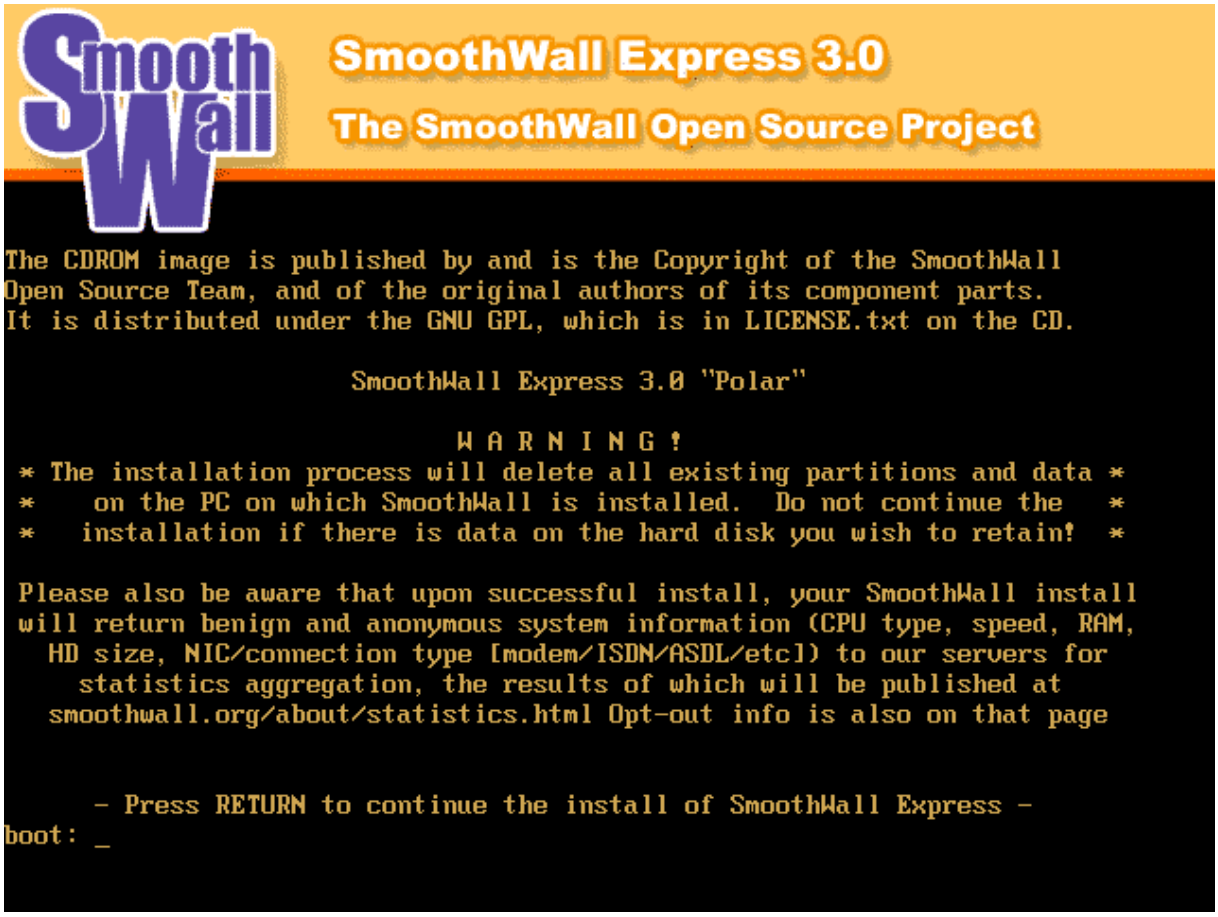
Installez SmoothWall Express est conçu pour fonctionner sur un poste de travail avec un CD-ROM.

Il vérifie automatiquement le poste de travail et des composants matériels et installe SmoothWall Express en conséquence.

Pour installer SmoothWall Express : on a procédé aux étapes suivantes :

1.Sur le site http://www.smoothwall.org/ http://www.smoothwall.org/ on a téléchargé et gravé un CD de SmoothWall Express.

2. Puis on a procédé à l'installation avec l'écran suivant qui s'est affiché :



Cette boîte de dialogue nous permet de choisir le type de configuration réseau qui convient à notre installation.

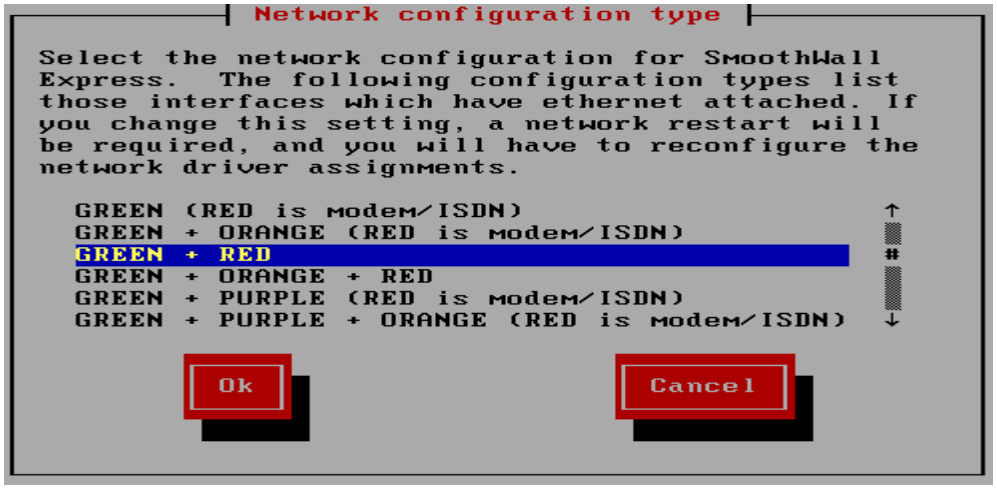


Figure III.19 type de configuration réseau.

Ici nous utilisons la configuration « green + red », un réseau sécurisé (la zone verte) et le réseau Internet (zone Rouge).

Enfin nous devrons indiquer la manière par laquelle l'interface rouge obtient son adresse IP. Ceci dépend du FAI et du type de connexion.

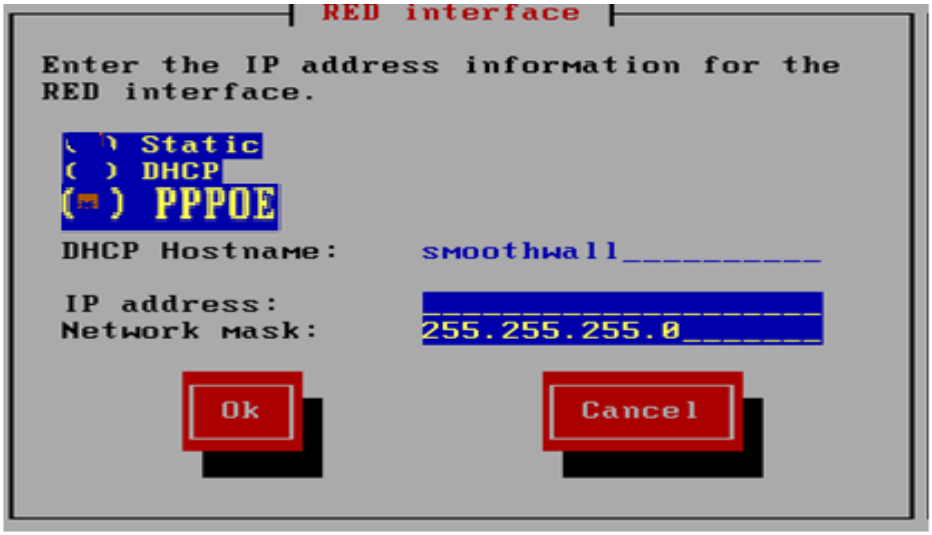


Figure III.20 : Configuration de l'interface rouge

Après l'installation, la configuration se fait directement sur la machine, ou à distance avec un terminal en mode sécurisé SSH ; ssh (192.168.0.1 sur le port 222) en mode console.

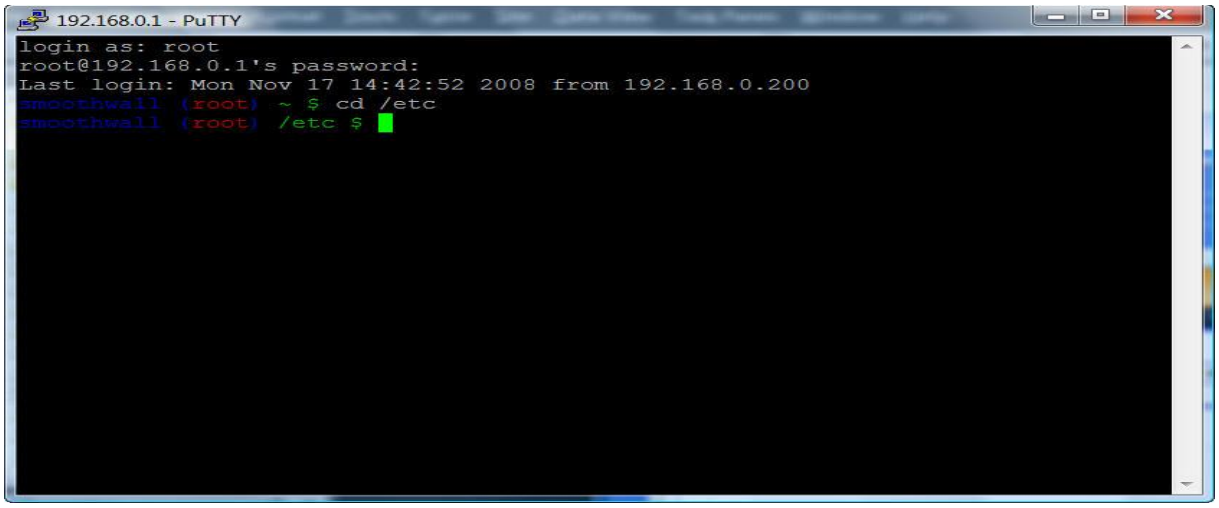


Figure III.21 : Mode console.

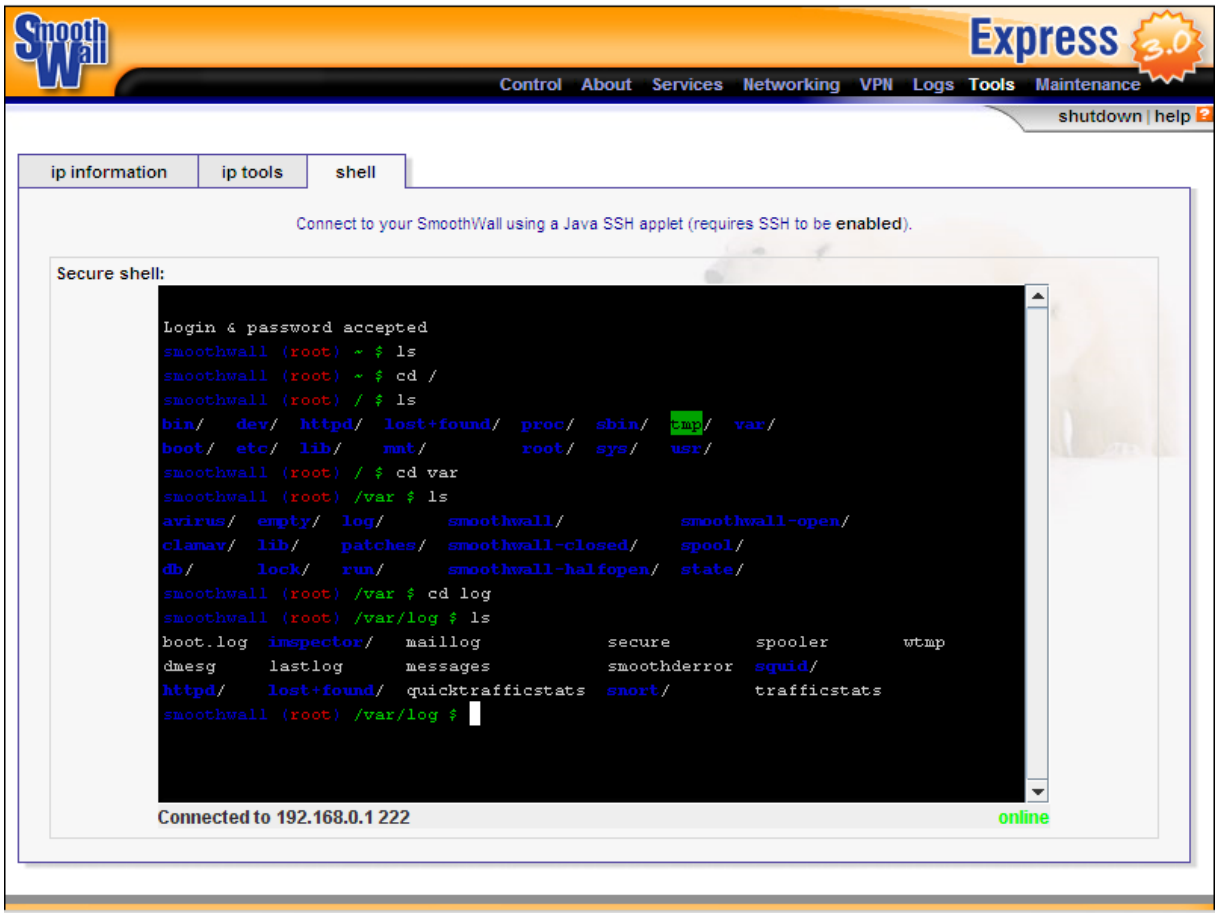


Figure III.22 : Mode console via le port 222

En trouve au niveau de Smoothwall différents outils sont disponibles, parmi eux l'outil Netfilter-iptables qui est conçu pour le filtrage.

IX. Filtrage réseau et pare-feu avec Netfilter et iptables

1. Généralités

Depuis la version 2.4, Linux contient un module destiné au filtrage réseau, **Netfilter**. Il se configure au moyen d'un outil appelé **iptables**.

Le filtrage réseau consiste en l'examen des paquets réseaux et à prendre des décisions sur le traitement à leur appliquer. C'est ce que fait un **pare-feu** ou, en anglais, **firewall**. Avec un système GNU/Linux, pour configurer des règles de pare-feu, il faudra donc simplement utiliser Netfilter à l'aide d'iptables.

Cet article s'interesse uniquement au filtrage réseau IPV4 (qui est probablement celui que vous utilisez si cela ne vous évoque rien). Cela est possible pour d'autres protocoles et les principes exposés ici resteront pour la plupart valides.

Netfilter travaille sur des paquets réseaux. Il s'agit de parties des informations transmises. Pour, par exemple, télécharger un fichier, celui-ci est découpé en plusieurs paquets avant de

transiter sur le réseau. Chacun de ces paquets comporte en plus des données, des informations ajoutées par les couches réseaux. Ce sont sur ces informations que s'effectueront les tests de filtrage.
La couche réseau Linux présente plusieurs **points d'accès** (en anglais **hook**). Netfilter dispose de **fonctions de rappel** (**callback**). Celles-ci sont des suites d'instructions qui précisent ce qui doit être fait lorsque survient un événement.
Concrètement, lorsqu'un paquet réseau atteint un de ces points d'accès, il est passé à Netfilter par l'intermédiaire de sa fonction de rappel. Il est alors examiné pour prendre une décision concernant son traitement futur.
Netfilter se comporte comme un automate qui compare le paquet successivement à plusieurs règles.

File d'attente	Fonction de la file d'attente	Transformation de paquet dans la chaîne	Fonction de la chaîne
Filter	Filtrage de paquet	F ORWARD	Filtre les paquets destinés à des serveurs accessibles par une autre carte réseau sur le pare-feu.
		INPUT	Filtre les paquets destinés au pare-feu.
		OUTPUT	Filtre les paquets émis par le pare-feu.
Nat	Traduction d'adresse réseau	PREROUTING	Habituellement utilisé pour traduire

			les adresses avant le routage. La principale utilisation est le « destination NAT » (DNAT).
		POSTROUTING	Habituellement utilisé pour traduire les adresses après le routage. La principale utilisation est le « source NAT » (SNAT).
		OUTPUT	Traduction d'adresse réseau pour les paquets générés par le pare-feu.
Mangle	Modification des paquets	PREROUTING POSTROUTING OUTPUT INPUT FORWARD	Modification du paquet IP.

Tableau III.7 : Les différentes files d'attente et chaînes

Traitement des paquets par iptables

Il est nécessaire de spécifier la table et la chaîne pour chaque règle définie. Il y a cependant une exception : la plupart des règles sont relatives au filtrage ; ainsi, toute chaîne qui est définie sans table associée fera partie de la table filter. La table filter est donc la table par défaut.

Pour mieux comprendre, il suffit de se référer à la figure ci-dessous. Dans cette figure, un paquet TCP venant d'Internet arrive sur l'interface réseau du pare-feu via le réseau A pour créer une connexion.

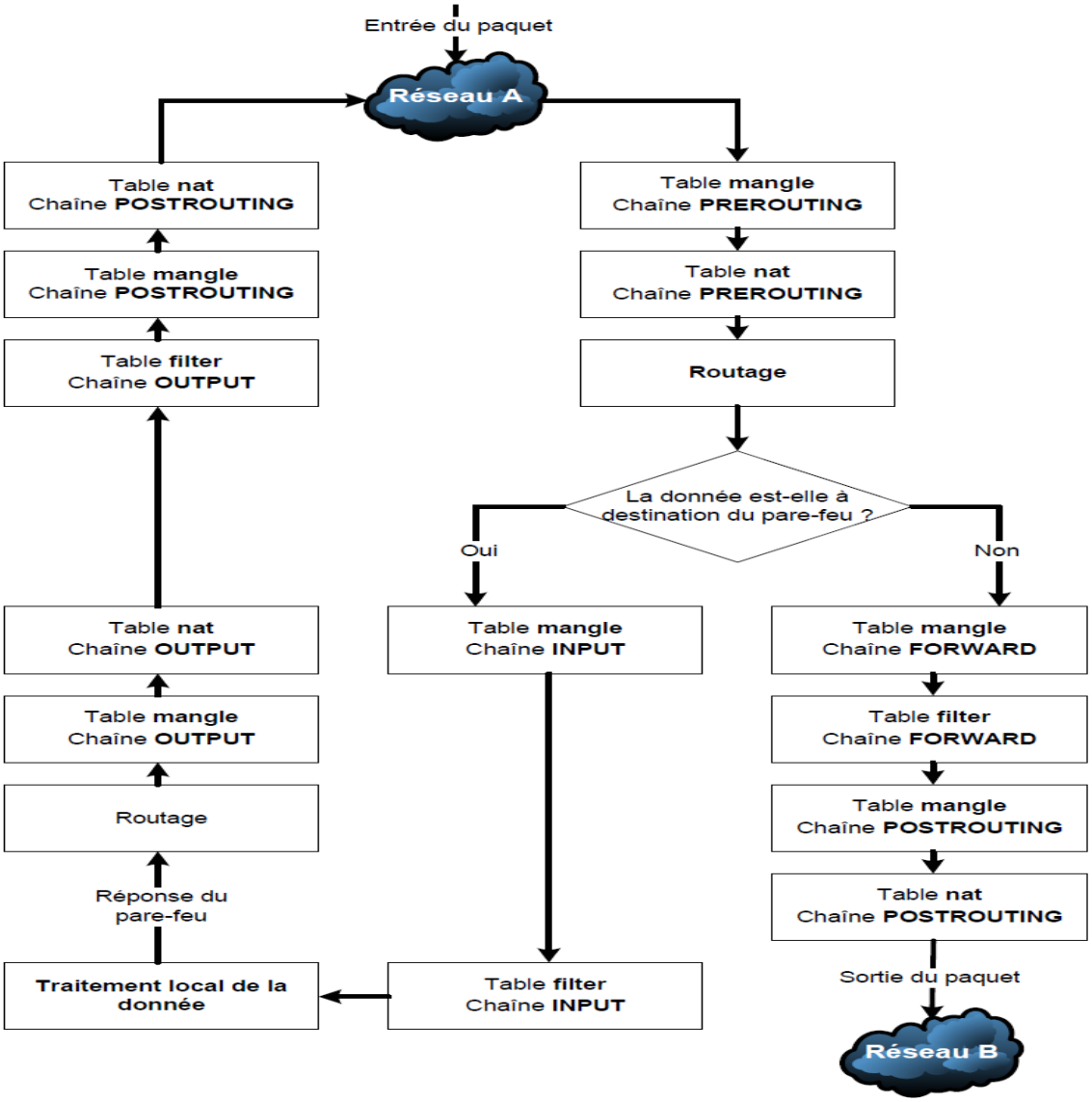


Figure III.19 Diagramme de traitement des paquets dans iptables

Cibles et sauts :

Chaque règle du pare-feu inspecte chaque paquet IP et puis tente de l'identifier afin de déterminer quelle opération est à effectuer dessus. Une fois la cible identifiée, le paquet est mis en attente pour un traitement ultérieur. Le tableau ci-dessous liste les utilisations des cibles prédéfinies.

Cible	Description	Options les plus utilisées
ACCEPT	○ Iptables stoppe le traitement ○ Le paquet est autorisé à passer	N/A
DROP	○ Iptables stoppe le traitement ○ Le paquet est bloqué	N/A
LOG	○ L'information sur le paquet est envoyée au démon syslog pour journalisation. ○ Iptables continue le	--log—prefix ''string' Indique à iptables de préfixer tous les messages de journalisation avec un chaîne de caractére définie par l'utilisateur.

	traitement avec la règle suivante dans la table. o Comme il n'est pas possible de journaliser et de bloquer en même temps. Il est d'usage d'avoir deux règles similaires à la suite. La première enregistre le paquet. La seconde le bloque.	Fréquemment utilisé pour indiquer pourquoi le paquet a été bloqué. --log-level « niveau » Indique à iptables et syslog le niveau de journalisation à utiliser.Le niveaux est debug.info.notice.warning.err.crit.alert.emerg
REJECT	o Fonctionne comme la cible DROP, mais retourne en plus un message à l'émetteur du paquet indiquant que le paquet a été bloqué.	--reject-with raison La raison indique quel type de message est retourné. Les raisons peuvent être les suivantes : icmp-port-unreachable (default) icmp-net-unreachable icmp-host-unreachable icmp-proto-unreachable icmp-net-prohibited icmp-host-prohibited tcp-reset echo-reply
DNAT	o Utilisé pour faire une traduction de l'adresse réseau de destination, c'est à- dire une réécriture de l'adresse IP de destination du paquet.	--to-destination <adresse> [-<adresse>][:<port>[-<port>]] Indique à iptables ce que l'(les)adresse(s) IP et le(s) port(s) de destination doivent être.
SNAT	o Utilisé pour faire une traduction de l'adresse réseau source, c'est-à-dire une réécriture de l'adresse IP source du paquet. o L'adresse IP source est définie par l'utilisateur.	--to-source <addresse>[-<addresse>][:<port>-<port>] Spécifie l'adresse IP source et les ports à utiliser par SNAT.
MASQUERADE	o Utilisé pour faire une traduction d'adresse réseau source. o Par défaut, l'adresse IP source est la même que celle utilisée par l'interface du pare-feu. o Cette option doit être utilisée lorsque l'IP de l'interface est susceptible de changer, par exemple dans le cas d'une connexion PPP.	[--to-ports <port>[-<port>]] Spécifie la plage de ports source à laquelle le port source peut être mappé.

Tableau III.8 Description des cibles les plus utilisées

Les cibles SNAT et MASQUERADE sont quasiment similaires, mais il existe des différences subtiles : la cible MASQUERADE est une forme spécialisée de SNAT. Utilisée de façon basique comme la cible SNAT, elle ne nécessite aucune option --to-source, car a été spécialement créée pour fonctionner avec des adresses IP dynamiques.
Si un système utilise uniquement des adresses IP statiques, il est préférable d'utiliser la cible SNAT. Il est toujours possible d'utiliser la cible MASQUERADE au lieu de SNAT, mais au détriment de l'efficacité, car MASQUERADE doit vérifier à chaque fois l'adresse IP source.

Opérations importantes

Chaque ligne d'un script iptables a non seulement un saut, mais elle a aussi un certain nombre d'options en ligne de commande qui sont utilisées pour ajouter des règles aux chaînes qui correspondent aux caractéristiques du paquet, comme l'adresse IP source ou le port TCP. Il y a aussi des options qui peuvent être utilisées pour purger une chaîne. Le tableau ci-dessous liste la plupart des options couramment utilisées.

Commande	Description
-t <-table->	Si la table n'est pas spécifiée, alors la table choisie par défaut est filter. Les tables prédéfinies sont : filter, nat, mangle.
-j <cible>	Saute à la cible spécifiée lorsque le paquet correspond la règle.
-A Ajoute	la règle à la fin de la chaîne.
-F Flush.	Supprime toutes les règles de la table sélectionnée.
-p < type-protocole>	Protocole à surveiller. Le type inclut icmp, tcp, udp, etc.
-s < addresse-ip>	Adresse IP source à surveiller.
-d < addresse-ip >	Adresse IP destination à surveiller.
-i <nom-interface>	Interface d'entrée à surveiller (le paquet entre par cette interface).
-o < nom-interface >	Interface de sortie à surveiller (le paquet sort par cette interface).

Tableau III.9 Critères généraux de sélection

Commande	Description
-p tcp --sport <port>	Port TCP source. Peut être une valeur unique ou une plage dans ce format : numéro-portde-départ:numéro-port-fin.
-p tcp --dport <port>	Port TCP destination. Peut être une valeur unique ou une plage dans ce format : numéroport-de-départ:numéro-port-fin.
-p tcp --syn	Utilisé pour identifier une nouvelle demande de connexion TCP. « ! –syn » indique « tout sauf une nouvelle requête de connexion ».
-p udp --sport <port>	Port UDP source. Peut être une valeur unique ou une plage dans ce format : numéro-portde-départ:numéro-port-fin.
-p udp --dport <port>	Port UDP destination. Peut être une valeur unique ou une plage dans ce format : numéroport-de-départ:numéro-port-fin.

Tableau III.10 Critères de sélection tcp et udp

Correspondance	Description
--icmp-type <type>	Les types les plus couramment utilisés sont echo-reply et echo-request

Tableau III.10 Critère de sélection ICMP (ping)

Il est possible d'utiliser la fonction limit pour réduire la vulnérabilité du système à certains types d'attaques par déni de service. Ici, la défense contre des attaques par SYN flood a été mise en place en limitant le nombre de segments TCP avec le bit SYN fixé à un nombre maximal de cinq par seconde.

Commande	Description
-m multiport --sport <port, port>	Une variété de ports source TCP/UDP, séparés par des virgules.
-m multiport --dport <port, port>	Une variété de ports destination TCP/UDP, séparés par des virgules.
-m multiport --port <port, port>	Une variété de ports TCP/UDP, séparés par des virgules. Les ports source et destination sont supposés être les mêmes.
-m --state <état>	Les états les plus utilisés sont les suivants : **ESTABLISHED**: Le paquet est une partie d'une connexion où il y a eu un échange bilatéral. **NEW**: Le paquet est le début d'une nouvelle connexion. **RELATED**: Le paquet est le début d'une nouvelle connexion secondaire. C'est une caractéristique commune des protocoles comme le transfert des données FTP ou une erreur ICMP. **INVALID**: Le paquet ne peut pas être identifié. Peut être en raison de l'insuffisance des ressources du système, ou des erreurs ICMP qui ne correspondent pas à un flux de donnée existant. L'annexe 1 fournit des informations complémentaires sur les états des connexions.

Tableau III.11 Critères étendus de sélection

1. **Quelque exemple de règle :**

Effacer de toutes les règles :

Iptables –F

Listage des règles :

Iptables –L –t FILTER, iptables -L –t MANGLE, iptables –L –t nat

Blocage basé sur l'interface :

Iptables –A INPUT –i eth0 –s 10.10.10.0/24 –j DROP

Blocage base sur le protocol:

Iptables –A INPUT –p udp –dport 514 –j ACCEPT

Effacer toutes les régles d'une chaîne :

Iptables –Z –t NAT (Z : zero)

Création d'une nouvelle chaîne :

Iptables –N nom (ex : iptables –N INTRANET)

Renommer une chaîne : **iptables –E ancien nouveau**

Redirection vers la nouvelle chaîne : **iptables –A INPUT –s 10.10.10.0/24 –j INTRANET**

Plusieurs ports : **iptables –A INPUT –p tcp –m multiport –dport 23,80 –j DROP**

@MAC : **iptables –A INPUT –p tcp –m mac –mac-source 00 :bb :aa :cc :ed :08 –j DROP**
@MAC : **iptables –A INPUT –p tcp –m mac –mac-destination 00 :bb :aa :cc :ed :08 –j DROP**

2. Expérimentation et Application au réseau test :

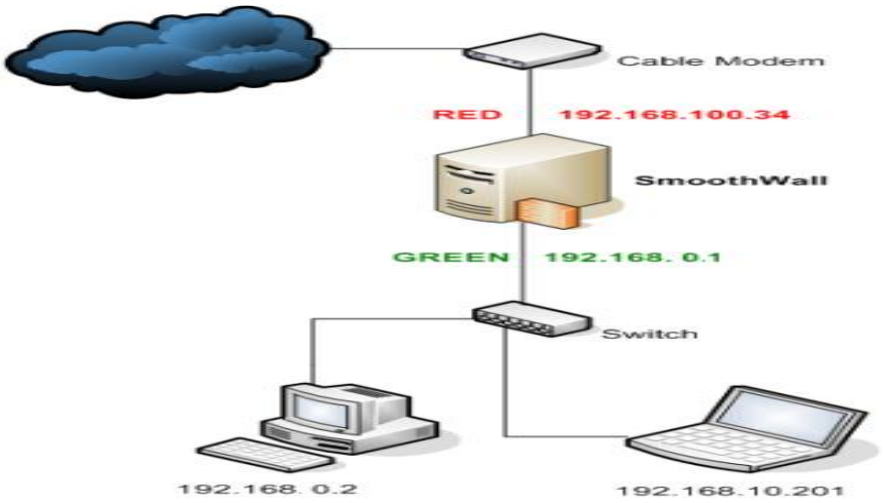


Figure III.22 réseau test

1. Génération des régles :

Initialisation de la table filter :
Iptables –F
Iptables -X

On ignore tout ce qui entre ou transite par la passerelle :
Iptables –P INPUT DROP
Iptables –P FORWARD DROP

On accepte, ce qui sort
Iptables –P OUTPUT ACCEPT

Autorise l'accès à la loopback,
Iptables –A INPUT –i lo –j ACCEPT
Iptables –A OUTPUT –o lo –j ACCEPT

On autorise les clients à accède à internet en créant une nouvelle chaîne, appelons-la « local-internet »

Iptables –N local-internet

« local-internet » concerne toutes les connections sauf celles venant d'internet

Iptables –A local-internet –m state –state NEW –i ! ppp0 -j ACCEPT

Evidemment, une fois acceptés comme "local-internet", les connections peuvent continuer

Iptables –A local-internet –m state –state ESTABLISHED, RELATED –j ACCEPT
Iptables –A INPUT –j local-internet
Iptables –A FORWARD –j local-internet

Initialisation des tables nat et mangle

Iptables -t nat -F
Iptables -t nat -X
Iptables -t nat –P PREROUTING ACCEPT
Iptables -t nat –P POSTROUTING ACCEPT
Iptables -t nat –P OUTPUT ACCEPT

Iptables -t mangle -F
Iptables -t mangle –X
Iptables -t mangle -P PREROUTING ACCEPT
Iptables -t mangle -P POSTROUTING ACCEPT

Partage de connexion :
Iptables -t nat –A POSTROUTING –s 192.1680.0/24 –o ppp0 –j MASQUERADE

Activation de la passerelle :
Echo "[activation de la passerelle]"
Echo 1> /proc/sys/net/ipv4/ip_forward

Fonctionnalités serveurs:
A ce stade, tous nos clients du réseau local et de la passerelle ont accès à internet. Mieux, On suppose qu'on possède un serveur http ou messagerie … nos clients du réseau local, ont accès à notre serveurs Mais personne depuis internet ne peux accéder ce serveur que vous hébergés. Il est bien-sûr possible de déverrouiller ponctuellement l'accès à un serveur depuis internet, voila quelque exemple :
Autorisation du serveur ssh(22)
Iptables –A INPUT –p tcp –dport ssh –j ACCEPT
Autorisation du serveur smtp(25)
Iptables –A INPUT –p tcp –dport smtp –j ACCEPT

Autorisation du serveur http(80)
Iptables –A INPUT –p tcp –dport www –j ACCEPT

2. Enregistrement : les logs

Il peut être intéressant d'enregistrer les tentatives de connexion à votre machine, les scans de ports. Mais attention, si tous les ports scannés sont enregistrés, le serveur risque de saturer aussi bien en performance CPU aussi bien qu'en espace disque.

Pour enregistrer les scans de ports TCP furtifs avec un maximum de trois par secondes, il suffit d'ajouter la ligne suivante avant la règle rejetant le paquet.

Iptables –A INPUT –m limit –limit 3/s LOG –log-prefix "BAD INPUT"

Chaque ligne sera préfixée par BAD INPUT, le préfixe pouvant faire jusqu'à 29 caractères.
Le fichier messages dans le répertoire /var/log contient tout l'historique on peut l'afficher a l'aide de commende cat.

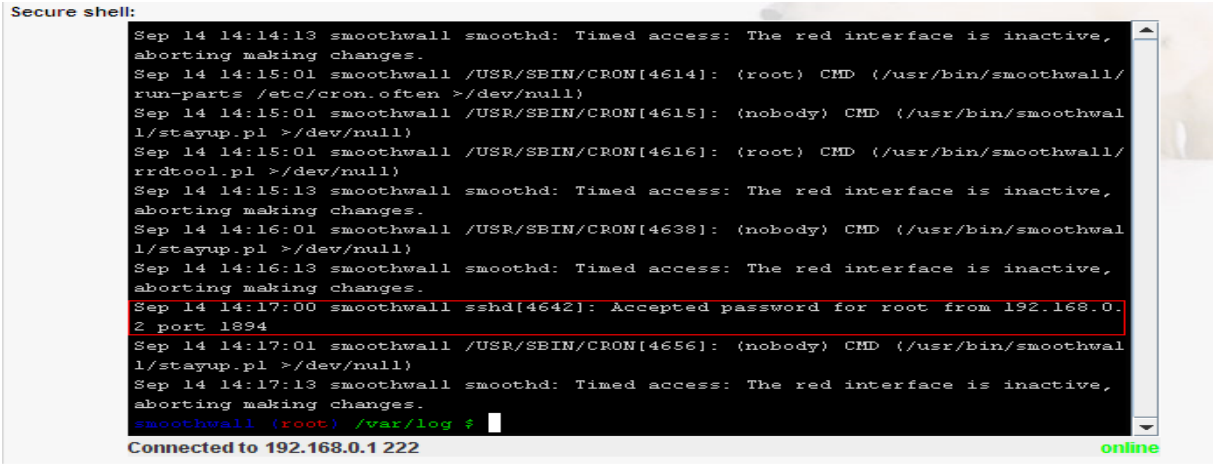


Figure III.23 Exemple de log

3. Génération de script firewall

La configuration du pare-feu iptables Smoothwall est stockée dans / etc / rc.d / rc.firewall.up, afin d'apporter des modifications au pare-feu, vous aurez besoin pour éditer ce script. Notez que vous pouvez utiliser divers pseudonymes dans le script de pare-feu pour faire référence à des interfaces réseau vert et rouge (c'est à dire, RED_DEV $, GREEN_DEV $), les adresses IP (c'est à dire, GREEN_ADDRESS $), les adresses réseau (c'est à dire, GREEN_NETADDRESS $), et des sous-réseaux (ie, $ GREEN_NETMASK). Ces alias sont définis dans / var / Smoothwall / Ethernet / réglages et que ce fichier ne doit pas être modifié, car il est généré par le programme de configuration de Smoothwall.
Notez que si votre interface ROUGE est un modem, RNIS ou via PPPoE ou PPPoA, vous ne pouvez pas utiliser l'alias $ RED_DEV, mais besoin de spécifier le nom de l'interface réelle, par exemple, ppp0.

4. Appliquer les modifications

Toute modification apportée au script de pare-feu ne prendra pas effet immédiatement.

Après avoir modifié le script du pare-feu, on doit soit redémarrer le Smoothwall, ou exécuter la commande suivante à partir d'une ligne de commande:

```
/etc/rc.d/rc.netaddress.down; /etc/rc.d/rc.netaddress.up
```

Ce sera une nouvelle demande de pare-feu, et les modifications dans le script de pare-feu devraient prendre effet.
Notons que on a du exécuté cette commande sur une seule ligne, sinon la connexion SSH sera résilié. Notons également que si on veut utiliser le proxy Web Smoothwall en mode transparent, et utiliser les scripts rc.netaddress.down pour redémarrer le pare-feu sans avoir à

redémarrer le PC, les règles appropriées iptables pour rediriger le trafic Web via le proxy ne seront pas chargées.

Pour appliquer le script au démarrage, il a fallu rajouter dans le fichier /etc/rc.d la ligne :
/etc/init.d/firewall
Notre script contenant un certain nombre d'argument, Start pour démarrer, stop pour l'arrêter, restart pour le redémarrer et status pour voir les régles en cours, dont voici le contenu.

############################REGLES PAR DEFAUT############################
firewall_start () {
echo "[Initialisation de la table filter]"
Iptables –F
Iptables –X

echo "[Politique par défaut de la table filter]"

#On ignore tout ce qui entre ou transite par la passerelle
Iptables –P INPUT DROP
Iptables –P FORWARD DROP

#On accepte, ce qui sort
Iptables –P OUTPUT ACCEPT

#Autorise l'accès à la loopback,
Iptables –A INPUT –i lo –j ACCEPT
Iptables –A OUTPUT –o lo –j ACCEPT

########################LOCAL-INTERNET################################

echo "[On autorise les clients à accède à internet]"
#en créant une nouvelle chaîne, appelons-la « local-internet »
Iptables –N local-internet

#On définit le profil de ceux qui appartiendront à "local-internet"
Iptables –A local-internet –m state –state NEW –i ppp0 -j DROP

#Evidemment, une fois acceptés comme "local-internet", les connections peuvent continuer
Iptables –A local-internet –m state –state ESTABLISHED, RELATED –j ACCEPT
Iptables –A INPUT –j local-internet
Iptables –A FORWARD –j local-internet

```
#######################LES TABLES NAT ET MANGLE#########################
echo "[Initialisation des tables nat et mangle]"

      Iptables  -t nat -F
      Iptables   -t nat -X
      Iptables   -t nat –P PREROUTING ACCEPT
      Iptables   -t nat –P POSTROUTING ACCEPT
      Iptables   -t nat –P OUTPUT ACCEPT

      Iptables  -t mangle  -F
      Iptables   -t mangle  –X
      Iptables   -t mangle  -P PREROUTING ACCEPT
      Iptables   -t mangle  -P OUTPUT ACCEPT

############################LE MASQUERADING################################
#Commentez ces 2 lignes, si vous ne faîtes pas du masquerading (nat)
echo "[Mise en place du masquerading]"
      Iptables   -t nat –A POSTROUTING –s 192.1680.0/24 –o ppp0 –j MASQUERADE

############################ACTIVATION DE LA PASSERELLE#################
      Echo  "[activation de la passerelle]"
      Echo 1> /proc/sys/net/ipv4/ip_forward

################################PAS DE SYNFLOOD############################

echo "[pas de synfood]"
      if [ -e /proc/sys/net/ipv4/tcp_syncookies ] ; then
          echo 1 > /proc/sys/net/ipv4/tcp_syncookies
      fi

################################PAS DE PING#################################
#Commentez ces 6 lignes, si vous autorisez les  pings sur votre passerelle
echo "[Pas de Ping]"
      echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
      echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
      if  [ -e /proc/sys/net/ipv4/icmp_ignore_bogus_error_respinses ] ; then
          echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
      fi

###################On prépare iptables pour utilisation de logs#################
      iptables –A INPUT –j LOG --log-prefix "BAD INPUT"
      iptables  -P INPUT DROP

      iptables –A INPUT –j LOG –log-prefix “Bad FORWARD”
```

```
        iptables –P FORWARD DROP

##########################Fonctionnalités serveurs ############################

echo  "[étude Fonctionnalités serveurs, visibles depuis internet]"

#A ce stade, tous nos clients du réseau local et de la passerelle ont accès à internet.
#Mieux, On suppose qu'on possède un serveur http ou messagerie … nos clients du réseau

#en décommettant les 2 ou 3 lignes correspondantes

#Autorisation du serveur ssh(22)
        #Iptables –A INPUT –p tcp –dport ssh –j ACCEPT

#Autorisation du serveur smtp(25)
        #Iptables –A INPUT –p tcp –dport smtp –j ACCEPT
#Autorisation du serveur  http(80)
        #Iptables –A INPUT –p tcp –dport www –j ACCEPT

echo "[firewall activé!]"
}

firewall_stop () {

        iptables –F
        iptables -X
        iptables –P INPUT ACCEPT
        iptables – P FORWARD ACCEPT
        iptables – P OUTPUT ACCEPT

        iptables  -t nat - F
        iptables  - t nat -X
        iptables  - t nat –P PREROUTING ACCEPT
        iptables  - t nat –P POSTROUTING ACCEPT
        iptables  - t nat –P OUTPUT ACCEPT

        iptables  - t mangle -F
        iptables  - t mangle -X
        iptables  - t mangle –P PREROUTING ACCEPT
        iptables  - t mangle –P OUTPUT ACCEPT

echo "[firewall désactivé!]"
}
```

```
        firewall_restart () {
        firewall_stop
        sleep2
        firewall_start
}



case "$1" in
‘start’)
firewall_start
;;
‘stop’)
firewall_stop
;;
‘restart’)
firewall_restart
;;
‘status’)
iptables –L
iptables –t nat –L
iptables –t mangle –L
;;
*)
echo "Usage: firewall {start|stop|restart|status}"
esac
```

5. Les Tests du firewall

Apres la mise en marche de firewall on doit tester sa fonctionnalité. Dans notre test l'interface rouge (internet) est représenter par un PC (IP : 192.168.0.1).On effectué trois test listés ci-dessous :

a) Les pings

Avant d'activer le firewall :

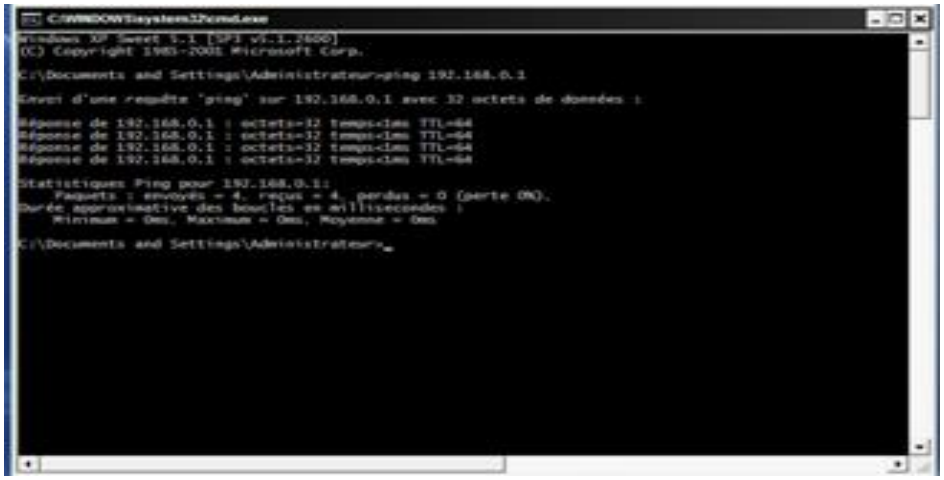


Figure III.23: Ping avant d'activer le firewall

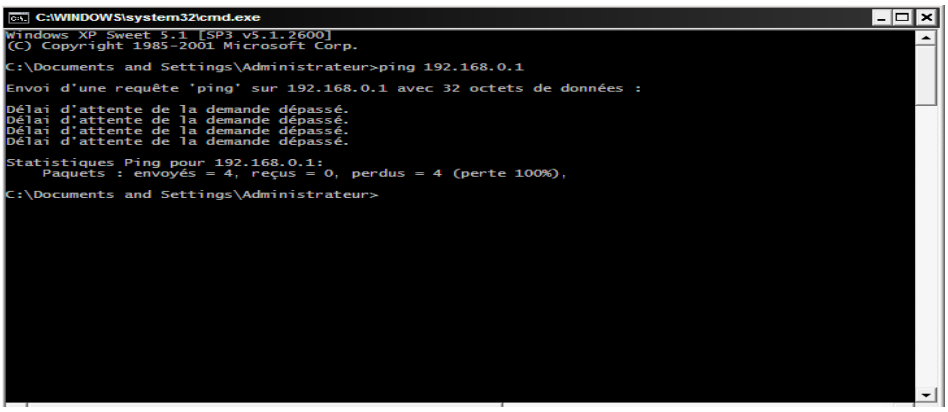


Figure III.24: Ping après l'activation de firewall

b) Scanner les ports

Pour scanner les ports on utilise : zenmap

Avant d'activer le firewall :

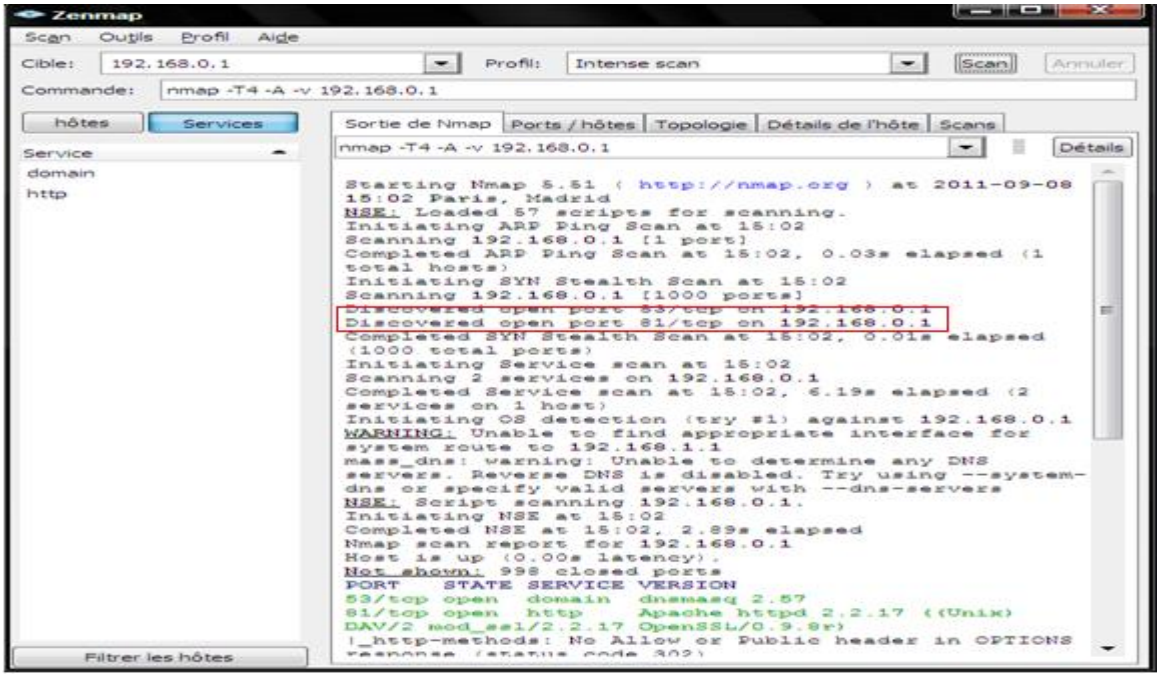


Figure III.25: Résultat du scan avant l'activation du par feu (scanner de port)

Comme on peut le voir, il y a 2 ports ouverts.

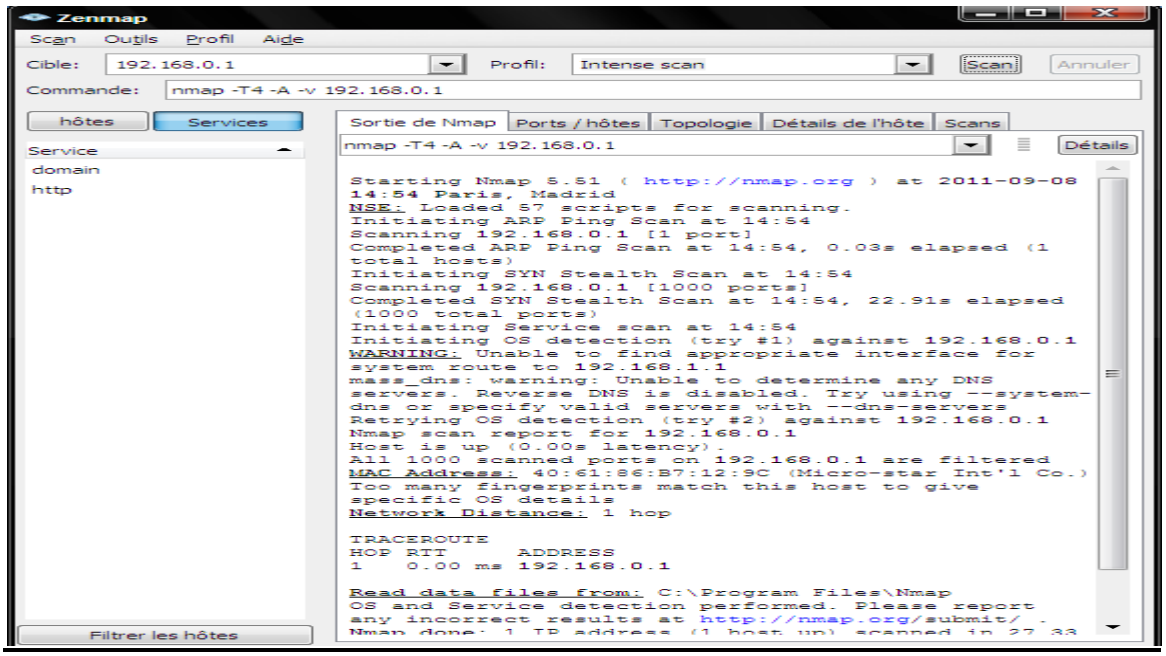


Figure III.26: Résultat du scan Apres (scanner de port)

Le scan ne donne rien comme résultat car le firewall a empêché le scan.

c) Bloquer un port

A titre d'exemple en prend le port 53, pour la vérification on utilise toujours Zenmap. Pour bloquer un port on utilise la commande iptables suivante :

iptables –A INPUT –p tcp –dport 53 --j DROP

Avant d'introduire la règle dans le script :

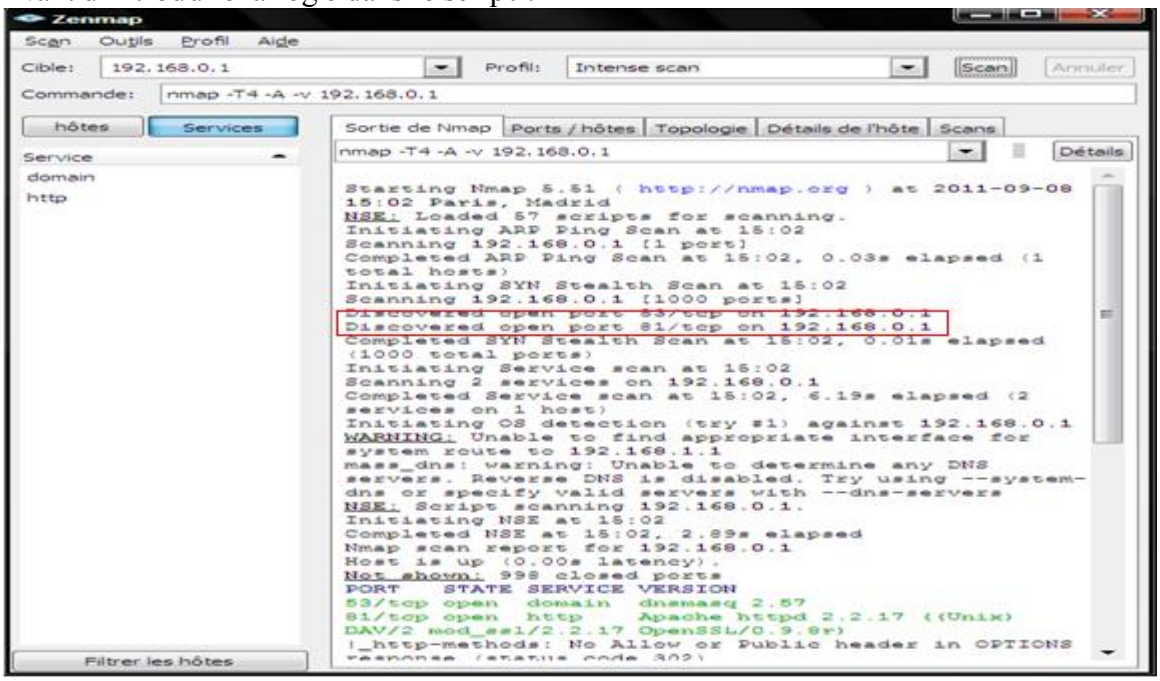


Figure III.27: Résultat de scan avant (Bloquer un port)

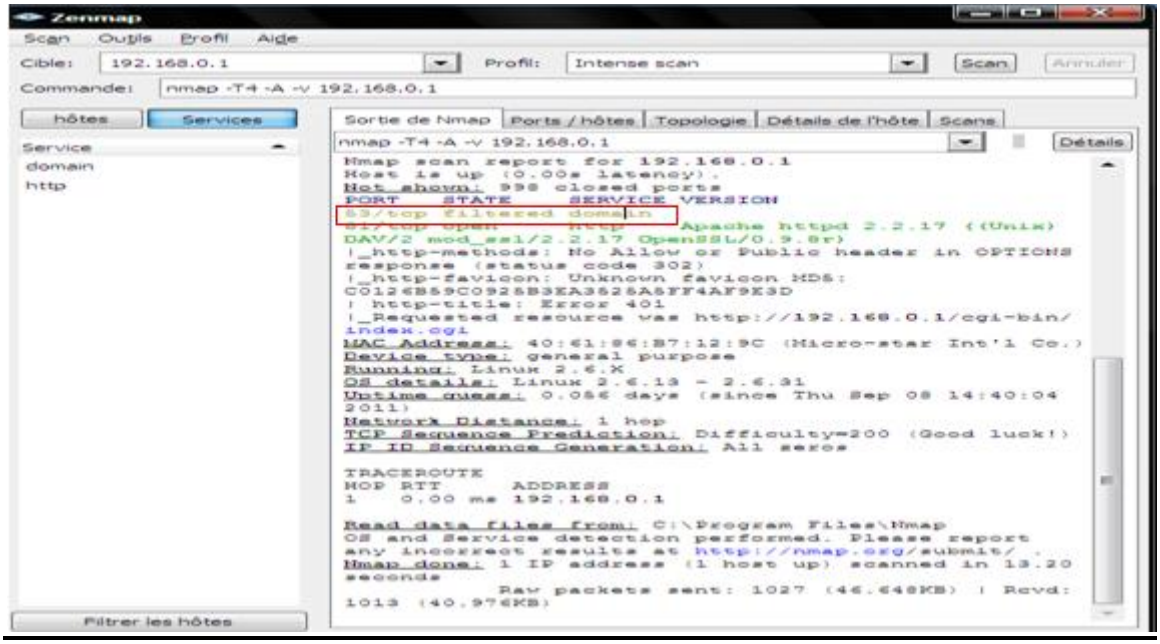


Figure III.28: Résultat du scan Après (Bloquer un port)

Conclusion

Maitriser les outils de sécurisation des réseaux locaux n'est pas chose aisée, surtout que le nombre de failles ne cesse d'augmenter et les intrusions nombreuses.
Protéger sa vie privée, ses données ou l'accès à son réseau est une nécessité à notre époque.
Dans ce chapitre, on a monté un réseau test qui nous a permis d'expérimenter le degré de sécurité qu'apporte un firewall à un réseau local ou même à un PC personnel.
En résume, les résultats observés nous permettent de dire que nous avons réussi à sécuriser notre réseau contre certaines attaques connues, car les méfaits des virus et autres programmes espions ne sont nullement arrêtés par le firewall. Ce point faible du firewall n'a pas trouvé de solutions, car il n'est pas envisageable à ce jour de faire rechercher les virus par le firewall, sinon on ralentirait dramatiquement le réseau, chose qui est exclue à moins d'avoir des avancées concernant la rapidité de traitements dans un proche avenir. On a procédé à plusieurs essais pour connecter des utilisateurs non autorisés, sans succès. Le firewall fonctionne correctement sans être parfait à 100 pourcent.

Conclusion Générale

Dans ce PFE, on s'est proposé de nous intéresser à la sécurité des réseaux informatiques et en particulier à la mise en place d'un firewall, qui filtrera tout ce qui rentre et sort du réseau privé vers INTERNET. Pour cela, on s'est d'abord intéressé aux attaques existantes et aux techniques de sécurité utilisées jusqu'à ce jour. Entre autre, l'authentification, le contrôle d'accès, la confidentialité et l'intégrité des données, le non répudiation etc.

Il existe un moyen pour effectuer plusieurs actions sécuritaires en même temps et à un endroit névralgique, qui pourrait être l'entrée du réseau privé, par l'intermédiaire d'un firewall, d'où notre intérêt pour ce moyen efficace de sécuriser un réseau LAN. C'est ce qui a motivé ce travail, et donc on a installé et configuré un firewall, en établissant des règles de filtrage précises, selon nos besoins et on a ensuite effectué des tests de bon fonctionnement, en utilisant un réseau test constitué du firewall au milieu de réseau LAN privé et le net.

Les résultats obtenus nous confortent dans l'idée que pour sécuriser les données névralgiques ou tout bêtement sa vie privée, un firewall s'impose comme une solution très efficace et peu coûteuse.

Références Bibliographiques

[1] www.smoothwall.org/ dernier visite le : 26/09/2011

[2] Cisco CCNA1 –Module 9 –Piles des protocoles TCP/IP et adressage IP – V3.1.

[3] Mme Nadia Nouali -Les firewalls comme solution aux problèmes de sécurité -2008

[5] www.c-sait.net/cours/iptables dernier visite le : 25/09/2001

[6] patrick Ducrot-Sécurité Informatique-2009
www.ducrot.org/securite.pdf

[7] Sécurité des réseaux informatiques - Bernard Cousin -Université de Rennes 1

[8] Guide de configuration Netfilter-iptables.

Liste de figure

Liste des tableaux

Liste des abréviations

A

ACK : l'acquittement d'une donnée ou d'une information consiste à informer son émetteur de sa bonne réception. On utilise souvent le terme ack pour un acquittement, ce terme correspond à l'équivalent anglais du terme : acknowledgement.

ADSL:L'Asymmetric Digital Subscriber Line (ADSL) est une technique de communication qui permet d'utiliser une ligne téléphonique ou une ligne RNIS pour transmettre et recevoir des données numériques de manière indépendante du service téléphonique proprement dit (contrairement aux modems dits analogiques). Cette technologie est massivement mise en œuvre par les fournisseurs d'accès à Internet pour le support des accès dits « haut-débit ».

ARP : L'Address resolution protocol (ARP, protocole de résolution d'adresse) est un protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse ethernet), ou même de tout matériel de couche de liaison. Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

B

BIOS :Le Basic Input Output System (BIOS, en français : « système élémentaire d'entrée/sortie ») est, au sens strict, un ensemble de fonctions, contenu dans la mémoire morte (ROM) de la carte mère d'un ordinateur, lui permettant d'effectuer des opérations élémentaires lors de sa mise sous tension, par exemple la lecture d'un secteur sur un disque. Par extension, le terme est souvent utilisé pour décrire l'ensemble du micrologiciel de la carte mère.

BSD : Berkeley Software Distribution, abrégé en BSD, désigne en informatique une famille de systèmes d'exploitation Unix, développés à l'Université de Californie (Berkeley) entre 1977 et 1995 par un groupe de programmeurs qui comprend notamment Bill Joy, Marshall Kirk McKusick et Kenneth Thompson.

D

DES : Le Data Encryption Standard (DES) est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable. Quand il est encore utilisé c'est généralement en Triple DES, ce qui ne fait rien pour améliorer ses performances. DES a notamment été utilisé dans le système de mots de passe UNIX.

DHCP:Dynamic Host Configuration Protocol (DHCP) est un terme anglais désignant un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms NBNS (connus sous le nom de serveurs WINS sur les réseaux de la société Microsoft).

DMZ : En informatique, une zone démilitarisée (ou DMZ, de l'anglais demilitarized zone) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.
Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

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

F

FTP : Le File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

H

HSRP : Hot Standby Router Protocol (HSRP) est un protocole propriétaire de Cisco implémenté sur les routeurs et les commutateurs de niveau 3 permettant une continuité de service. HSRP est principalement utilisé pour assurer la disponibilité de la passerelle par défaut dans un sous-réseau en dépit d'une panne d'un routeur.

I

IANA :L'Internet Assigned Numbers Authority (IANA) est une organisation dont le rôle est la gestion de l'espace d'adressage IP d'Internet, et des autres ressources partagées de numérotation requises soit par les protocoles de communication sur Internet, soit pour l'interconnexion de réseaux à Internet.

ICMP :Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.

IDE : Un environnement de développement intégré (EDI ou IDE en anglais pour Integrated Development Environment) est un programme regroupant un ensemble d'outils pour le développement de logiciels.

IGMP : Internet Group Management Protocol (IGMP) est un protocole qui permet à des routeurs IP de déterminer de façon dynamique les groupes multicast qui disposent de clients dans un sous-réseau.

IP : Internet Protocol (abrégé en IP) est une famille de protocoles de communication de réseau informatique conçus pour et utilisés par Internet. Les protocoles IP sont au niveau 3 dans le modèle OSI. Les protocoles IP s'intègrent dans la suite des protocoles Internet et permettent un service d'adressage unique pour l'ensemble des terminaux connectés.

IPS : Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque.

L

LAN : Un réseau local, souvent désigné par l'acronyme anglais LAN de Local Area Network, est un réseau informatique tel que les terminaux qui y participent (ordinateurs, etc.) s'envoient des trames au niveau de la couche de liaison sans utiliser de routeur intermédiaire.

LIFO : Last In, First Out, souvent abrégé par l'acronyme LIFO, signifie « dernier arrivé, premier sorti ». Cette expression est utilisée en informatique pour décrire une manière de traiter des données. La dernière donnée ajoutée à la structure est ainsi la première à être retirée. La structure de pile repose sur ce principe.

M

MAC : Le Contrôle d'accès au support (Media Access Control en anglais ou MAC) est une sous-couche, selon les standards de réseaux informatiques IEEE 802.x, de la partie inférieure de la couche de liaison de données dans le modèle OSI.

MAN : Un réseau métropolitain (en anglais Metropolitan Area Network, MAN) désigne un réseau composé d'ordinateurs habituellement utilisé dans les campus ou dans les villes. Le réseau utilise généralement des fibres optiques.

N

NAT :En réseau informatique, on dit qu'un routeur fait du Network Address Translation (NAT) (« traduction d'adresse réseau »[1]) lorsqu'il fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables.

NIC : Une carte réseau est matérialisée par un ensemble de composants électroniques soudés sur un circuit imprimé. L'ensemble constitué par le circuit imprimé et les composants soudés s'appelle une carte électronique, d'où le nom de carte réseau.

O

OSI : Le modèle OSI (de l'anglais Open Systems Interconnection, « Interconnexion de systèmes ouverts ») d'interconnexion en réseau des systèmes ouverts est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation).

P

PGP : La cryptographie hybride est un système de cryptographie faisant appel aux deux grandes familles de systèmes cryptographiques : la cryptographie asymétrique et la cryptographie symétrique. Les logiciels comme PGP et GnuPG reposent sur ce concept qui permet de combiner les avantages des deux systèmes.

POP : POP (Post Office Protocol littéralement le protocole du bureau de poste), est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.

R

RAM : La mémoire vive, mémoire système ou mémoire volatile, aussi appelée RAM de l'anglais Random Access Memory (que l'on traduit en français par mémoire à accès direct.

RARP : RARP (pour Reverse ARP) permet à partir d'une adresse matérielle (adresse MAC) de déterminer l'adresse IP d'une machine. En résumé, RARP fait l'inverse de ARP.

RFC : Les requests for comments (RFC), littéralement « demande de commentaires », sont une série numérotée de documents officiels décrivant les aspects techniques d'Internet, ou de différent matériel informatique (routeurs, serveur DHCP).

RJ45 : Un connecteur RJ45 est une interface physique souvent utilisée pour terminer les câbles de type paire torsadée.

RNIS : Un réseau numérique à intégration de services (RNIS, en anglais ISDN pour Integrated Services Digital Network) est une liaison autorisant une meilleure qualité et des vitesses pouvant atteindre 2 Mbit/s (accès S2) contre 56 kbit/s pour un modem classique.

RSA : Rivest Shamir Adleman (presque toujours abrégé en RSA) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

S

SCSI :SCSI, Small Computer System Interface en anglais, est un standard définissant un bus informatique permettant de relier un ordinateur à des périphériques ou bien même à un autre ordinateur.

SMTP : Le Simple Mail Transfer Protocol (littéralement « Protocole simple de transfert de courrier »), généralement abrégé SMTP, est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

SSH : Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

T

TCP : Transmission Control Protocol (littéralement, « protocole de contrôle de transmissions ») abrégé TCP, est un protocole de transport fiable, en mode connecté, documenté dans la RFC 793 de l' IETF.

TELNET : Telnet (TErminal NETwork ou TELecommunication NETwork, ou encore TELetype NETwork) est un protocole réseau utilisé sur tout réseau supportant le protocole

TCP/IP. Il appartient à la couche session du modèle OSI et à la couche application du modèle ARPA.

TTL : Transistor-Transistor Logic ou TTL est une famille de circuits logiques utilisée en électronique inventée dans les années 1960. Cette famille est réalisée avec la technologie du transistor bipolaire et tend à disparaître du fait de sa consommation énergétique élevée (comparativement aux circuits CMOS).

U

UDP : L'User Datagram Protocol (UDP, en français protocole de datagramme utilisateur) est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport de la pile de protocole TCP/IP : dans l'adaptation approximative de cette dernière au modèle OSI, il appartiendrait à la couche 4, comme TCP.

V

VPN : Dans les réseaux informatiques et les télécommunications, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel ».

VRRP : Virtual Router Redundancy Protocol (protocole de redondance de routeur virtuel, VRRP) est un protocole non propriétaire redondant décrit dans la RFC 3768 dont le but est d'augmenter la disponibilité de la passerelle par défaut servant les hôtes d'un même sous-réseau.

W

WAN : Un réseau étendu (terme recommandé au Québec par l'OQLF[1]), souvent désigné par l'anglais Wide Area Network (WAN), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Le plus grand WAN est le réseau Internet.

Dans ce PFE, on s'est proposé de nous intéresser à la sécurité des réseaux informatiques et en particulier à la mise en place d'un firewall, qui filtrera tout ce qui rentre et sort du réseau privé vers INTERNET. Pour cela, on s'est d'abord intéressé aux attaques existantes et aux techniques de sécurité utilisées jusqu'à ce jour. Entre autre, l'authentification, le contrôle d'accès, la confidentialité et l'intégrité des données, le non répudiation etc.

Le premier chapitre consiste a étudier le réseau local et les méthodes de hackings ainsi les méthodes de défenses associe puis en a étudier le firewall et enfin un étude pratique sur le système de protection Smoothwall et outil de filtrage netfilter a l'aide d'iptables ...