Architecture Firewall

Dieudonné Arnaud, Gouband Patrick

13 mai 2002

Table des matières

1 Introduction

Un firewall est un dispositif ayant pour but de filtrer les flux d'informations entre deux réseaux, généralement un réseau interne avec un réseau externe (Internet).
Le principal objectif d'un firerwall est de neutraliser les pénétrations en provenance de l'extérieur et de maîtriser les accès vers l'extérieur.

Rappelons qu'il existe plusieurs philosophies :
- Tout ce qui n'est pas expressément interdit est autorisé
- Tout ce qui n'est pas expressément autorisé est interdit

Il y a trois types de firewall :
- packet filter
- application gateway (proxy)
- circuit-level gateway

Un firewall peut être composé de :
- routeur (un ou plusieurs)
- bastion host
- dual-homed host
- DMZ

Il existe trois grands types d'architectures :
- Screened-host architecture
- Dual-homed host architecture
- Screened subnet architecture

L'architecture firewall correspond aux façons d'agencer les différents éléments d'un firewall. L'architecture firewall dépendra fortement de la politique de sécurité désirée.

2 Notation utilisée

Explication sur la normalisation utilisée pour les schémas :

Px : Poste de travail numéro x

Rx : Routeur numéro x

BHx : Bastion Host numéro x

DHHx : Dual-Homed Host

DMZx : DMZ numéro x

Paquet entrant : paquet arrivant d'Internet à destination du réseaux interne

Paquet sortant : paquet arrivant du réseaux interne à destination d'Internet

3 Eléments d'un firewall

3.1 Bastion host

On appelle bastion un serveur sécurisé. Il constitue le point de connexion entre le réseau interne et l'extérieur, il contient les services sensibles. C'est-à-dire que l'on met tous les services sensibles tels que DNS, MAIL, Web, FTP sur un ou des serveurs.
Le bastion host est la machine la plus susceptible d'être attaquée.

3.2 DMZ (DeMilitarised Zone)

Littéralement zone démilitarisée, zone intermédiaire (ou neutre) entre un réseau informatique interne sensible et devant être sécurisé et un réseau externe non maîtrisé (ex. : Internet). La DMZ est un sas dans lequel sont obligatoirement véhiculés les flux échangés entre les deux réseaux afin de garantir le caractère sain et inoffensif de ces flux.

Une DMZ est en général délimitée par un équipement de sécurité réseau (ex. : firewall).
Dans certains cas, on met en oeuvre des DMZs de nature différente :

- DMZ publique : recevant les flux en provenance de l'extérieur. Cette zone peut héberger le serveur de messagerie, le serveur Web et le DNS de l'entreprise.
- DMZ privée : recevant les flux en provenance du réseau interne et à destination de l'extérieur. Cette zone peut héberger un relais de messagerie sortant, un proxy-cache pour l'accès au Web.

3.3 Dual-homed host

Machine avec plusieurs interfaces connectant des réseaux.

3.4 Screning router

Routeur qui fait du packet filtering. Il peut être intéressant de mettre plusieurs routeurs ayant les mêmes règles les uns à la suite des autres, ainsi si le premier routeur est hors service il reste encore le routeur suivant.

4 Architectures firewall

Le choix du firewall dépend de la politique de sécurité, des services que l'on doit surveiller et du coût financier et humain.

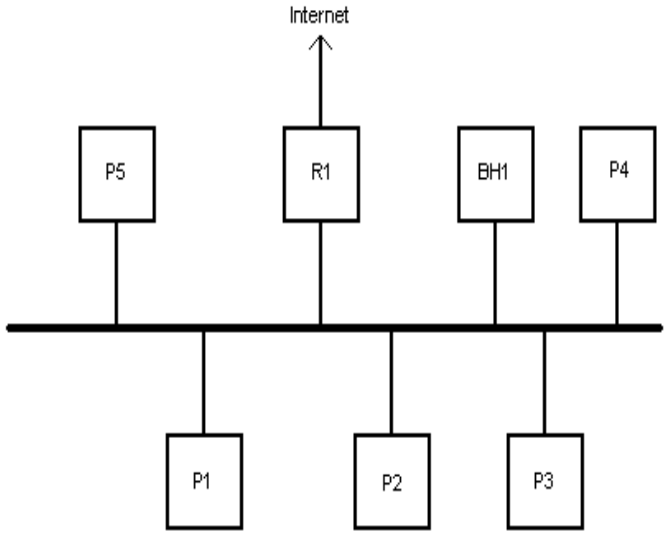
4.1 Screened host architecture

Dans cette première architecture, le firewall est constitué d'un screening router et d'un bastion host.

Toutes les machines sont branchées sur le même brin réseau, mais elles n'accèdent pas directement pour tous les services à Internet. C'est à dire, que pour les services sensibles, comme SMTP, DNS, FTP, etc... les données passent obligatoirement par une machine spécialisée appelée bastion host. Cette machine possède des proxy donnant accès à ces services.

L'idée principale de cette méthode est de sécuriser très fortement quelques machines (les bastion host), où l'administrateur réseau concentre son attention. Tous les paquets passent obligatoirement par le screening router, et en fonction de la configuration de celui-ci, passent par le bastion host ou pas.

FIG. 1 – Screened host architecture



Explication du schéma :

Paquet entrant :
- Il arrive sur le routeur R1
- Est-ce un service sensible ?

Si oui :
- Il va sur le bastion host BH1
- Il accède enfin à la machine Px

Si non :
- Il accède directement à la machine Px

Paquet sortant :
- Est-ce un service sensible ?

Si oui :
- Il va sur le bastion host BH1
- Il va ensuite au routeur R1
- Il accède enfin à Internet

Si non :
- Il va ensuite au routeur R1

- Il accède enfin à Internet

Avec cette architecture et les règles que l'on a données au screening router, on peut accéder directement au routeur, mais avec d'autres règles, le routeur n'acceptera que des paquets provenant du bastion host et enverra lui même tout ses paquets au bastion host.

Le screening router est assez simple à configurer contrairement au bastion host dont la configuration reste difficile.

Un des problèmes de cette architecture est que l'on a un brin unique donc les paquets Internet circulent sur le réseau interne.

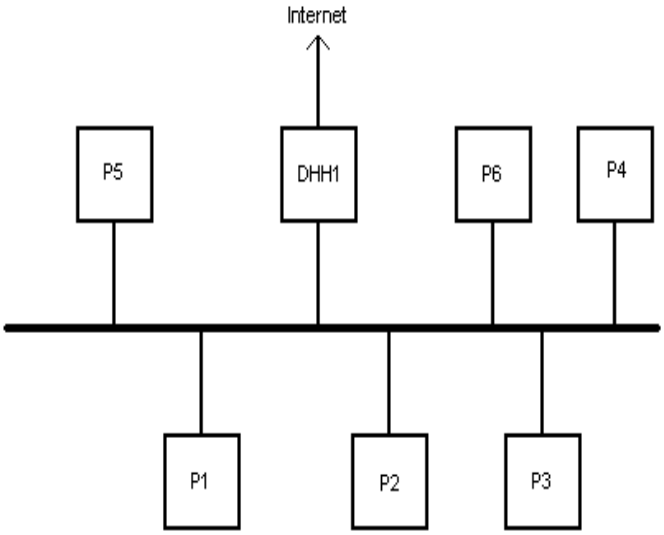
Si l'attaquant franchi le bastion host, il n'y a plus aucune protection. Si la configuration du screening n'est pas infaillible, l'attaquant peut éviter le bastion host, et donc avoir accès a tout le réseau.

4.2 Dual-homed host architecture

Dans cette architecture, le firewall est uniquement constituée d'une machine possédant 2 interfaces, une vers Internet, l'autre vers le réseau local. Cette machine s'appelle dual-homed host.

Cette machine possède comme dans le cas des bastions host des services sur ces 2 interfaces qui peuvent fonctionner via des proxy. C'est le seul élément qui protège le réseau. Le dual-homed host ne doit pas faire de routing afin d'éviter que les paquets ne le traversent.

FIG. 2 – Dual-homed host architecture



Explication du schéma :

Paquet entrant :
- Il arrive sur le dual-homed host DHH1
- En fonction des règles le paquets passe ou pas

Si oui :
- Il arrive à la machine destinatrice

Si non :
- Le paquet est bloqué

Paquet sortant :
- Il arrive sur le dual-homed host DHH1
- En fonction des règles le paquets passe ou pas

Si oui :
- Il accède à Internet

Si non :
- Le paquet est bloqué

Un des gros avantages de cette solution, est que tous les paquets circulant sur le réseau ont une adresse interne (adresse source et destination). Comme

il n'y a pas de fonction de routing, l'attaquant ne peut pas fabriquer de paquets ayant une adresse interne.

La configuration du dual-homed host est délicate car c'est le seul point de sécurité, cette machine ne doit pas laisser passer les paquets directement. (c'est la fonction de routing)

Il existe une unique protection contre les blackhat, si celle-ci est franchie, le réseau est vulnérable.

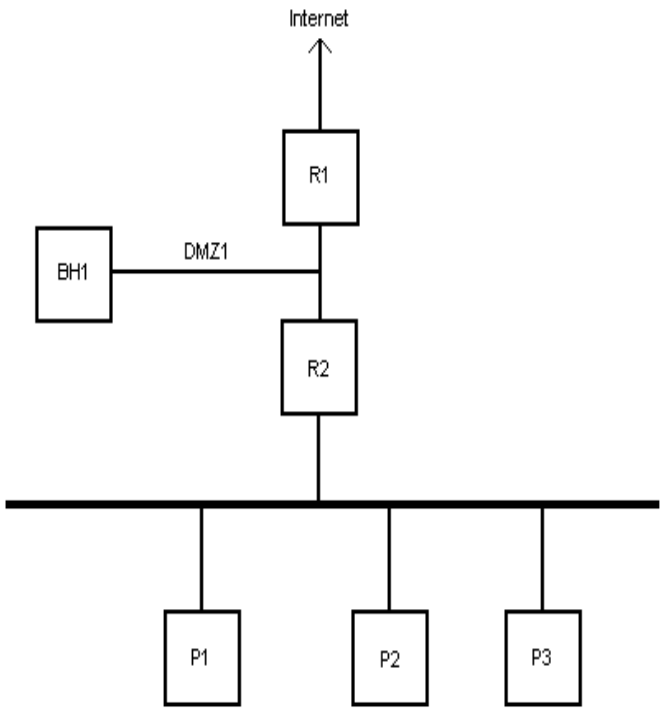
4.3 Screened subnet architecture

Le firewall est constitué de deux screening routers et d'un bastion host. (nous verrons que cette architecture possède plusieurs variantes)

Le principal défaut de l'architecture screened host architecture est la vulnérabilité du bastion host, c'est pour cela que l'on cherche à l'isoler en ajoutant un deuxième routeur.

On crée ainsi une DMZ dans laquelle sera situé le bastion host. On isole le bastion host autant de l'Internet que du réseau interne. Le bastion host contient tous les services sensibles.

FIG. 3 – Screened subnet architecture



Explication du schéma :

Paquet entrant :
- Il arrive sur le routeur R1
- Il va sur le bastion host BH1
- Il va sur le routeur R2
- Il arrive à la machine destinatrice

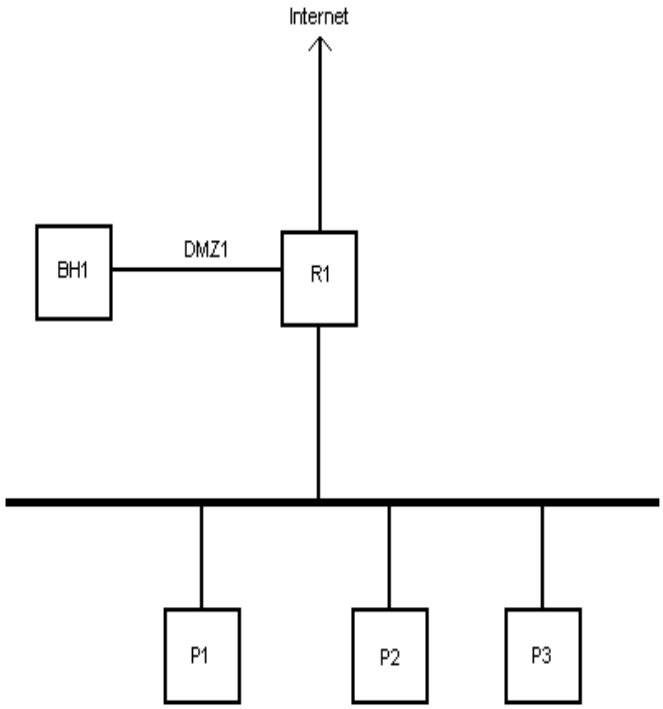
Paquet sortant :
- Il va ensuite au routeur R2
- Il va sur le bastion host BH1
- Il va ensuite au routeur R1
- Il accède enfin à Internet

Le routeur R1 a pour mission de protéger le bastion host contre les attaques venant d'Internet. Le bastion host reste quand même exposé aux attaques. Le routeur R2 élimine la possibilité de sniffer à partir du bastion host. Les deux routeurs n'ont pas forcément les mêmes règles. Même si l'attaquant parvient jusqu'au bastion host, il lui reste le routeur R2 à passer pour accéder au réseau interne.

Dans cette architecture le bastion host doit être bien configuré même si il reste le routeur R2 pour protéger le réseau interne.

Il existe une variante de la screened subnet architecture avec un routeur au lieu de deux, mais il possède trois interfaces pour permettre au bastion host de se situer sur une DMZ.

FIG. 4 – Une variante de screened subnet architecture

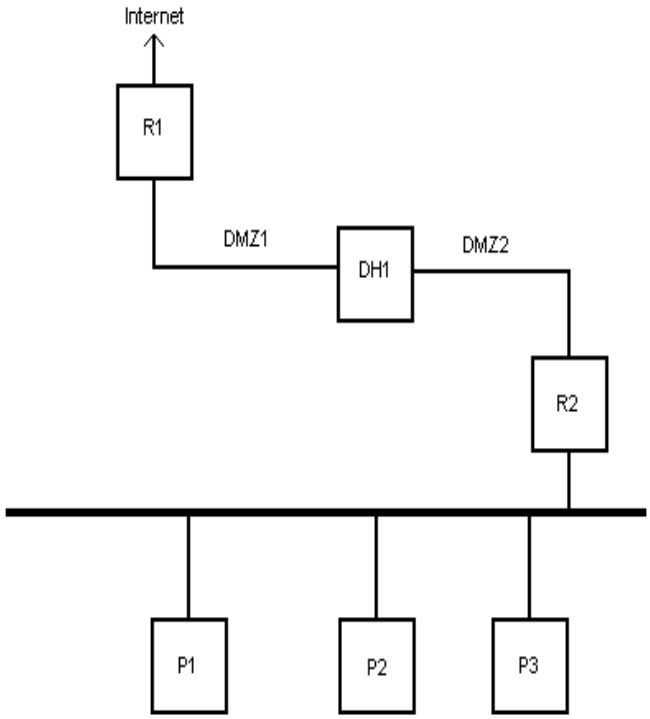


Nous avons vus les trois principales architectures de firewall que nous pourrions appeler architectures classiques, dans la suite nous allons vous présenter différentes architectures découlant de celles-ci.

4.4 Split-screened subnet architecture

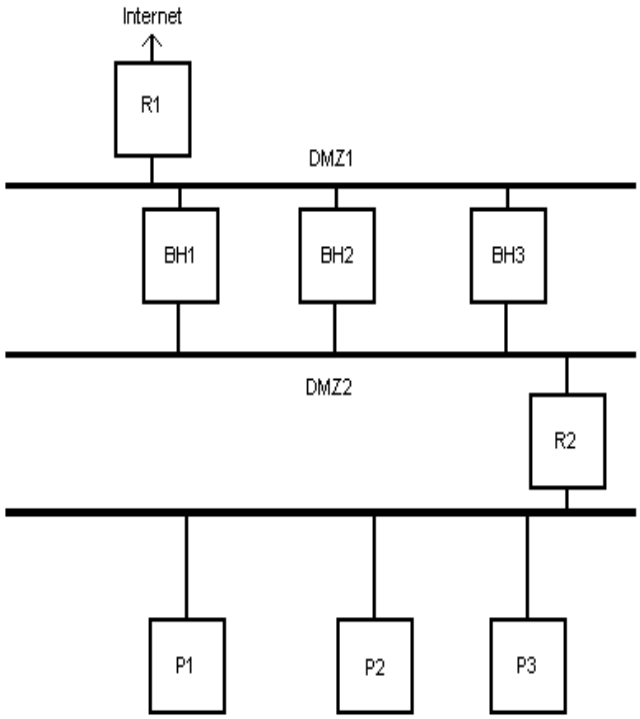
La principale caractéristique de cette architecture est de posséder plusieurs DMZ entre les routeurs extérieur et intérieur.

FIG. 5 – Split-screened subnet architecture avec dual-homed host



Cette architecture est basée sur la screened subnet architecture mais avec un dual-homed host à la place du bastion host, donc il y a deux DMZ.

FIG. 6 – Split-screened subnet architecture avec plusieurs bastion host



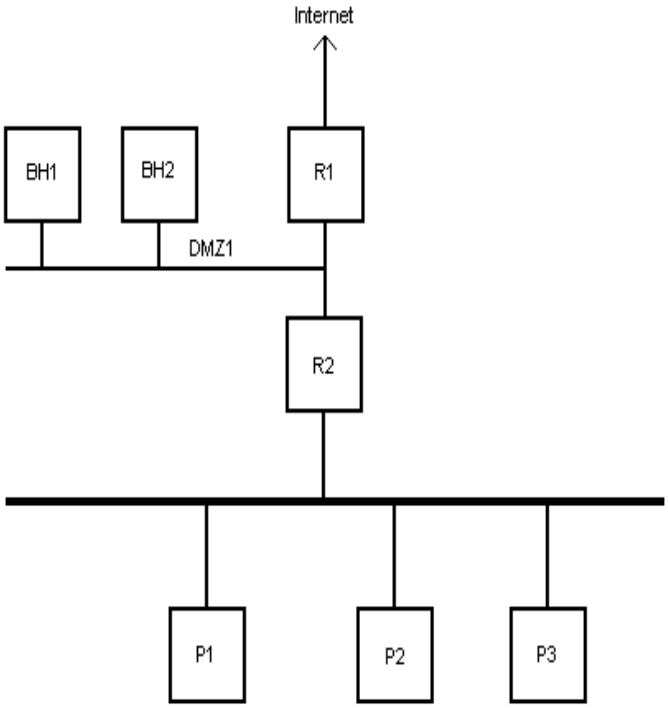
Dans cette architecture on sépare les services sensibles sur différents bastion host placés entre les deux DMZ.

Cette architecture permet d'accélérer le débit du réseau car chaque machine traite un service particulier. Si un bastion host est corrompu les autres ne le sont pas.

Les split-screened subnet architecture sont particulièrement appropriées pour les réseaux nécessitant une sécurité de haut niveau et pour les entreprises proposant des services en ligne.

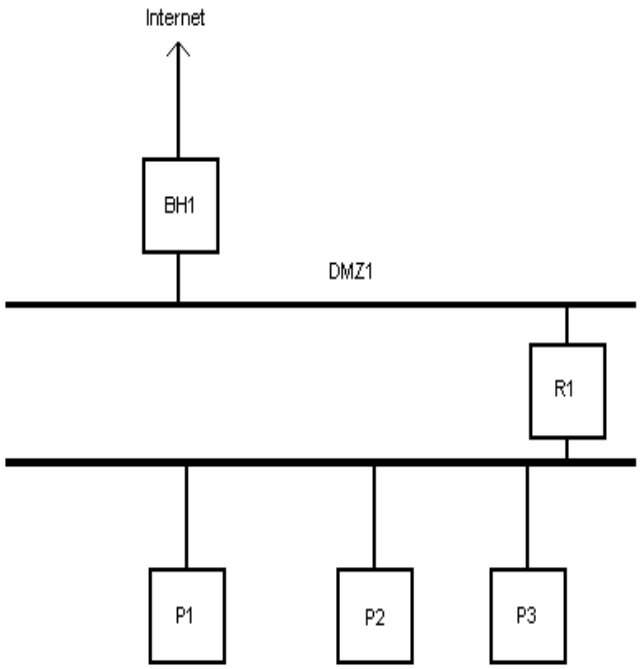
4.5 Autres architectures firewall

FIG. 7 – Screened subnet architecture avec deux bastion host



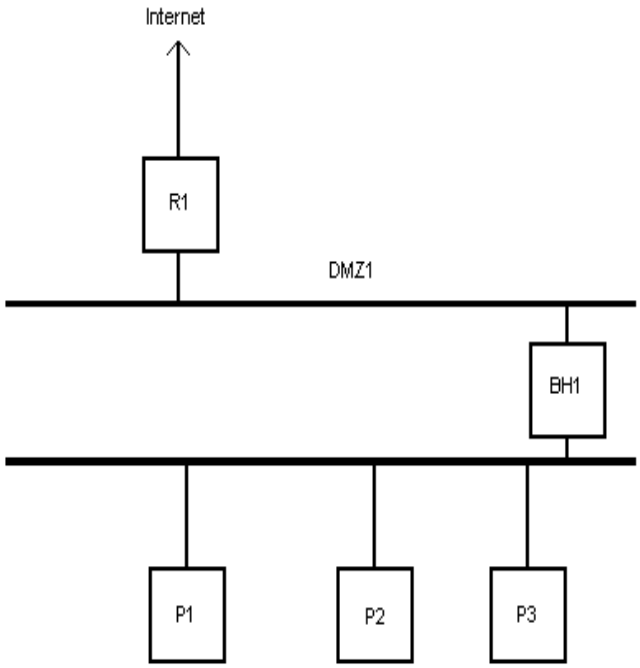
C'est une variante du screened subnet architecture mais avec deux bastion host pour séparer les services sensibles. Si un bastion host est corrompu les autres ne le sont pas.

FIG. 8 – Un bastion host sert de routeur extérieur



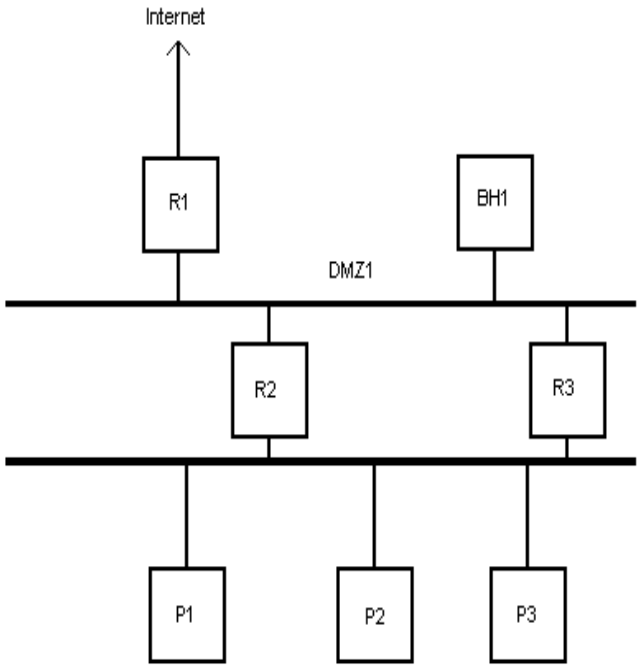
Le bastion host fait office de routeur extérieur en plus de ses fonctions habituelles. Si un attaquant arrive à prendre le contrôle du bastion host, il reste encore le routeur intérieur à franchir donc le réseau interne est encore intègre contrairement à l'exemple suivant.

FIG. 9 – Un bastion host sert de routeur intérieur, mauvaise solution



Le bastion host fait office de routeur intérieur en plus de ses fonctions habituelles. Le bastion host est visible de l'extérieur or si un attaquant arrive à prendre le contrôle du bastion host, il a accès à tout le réseau interne.

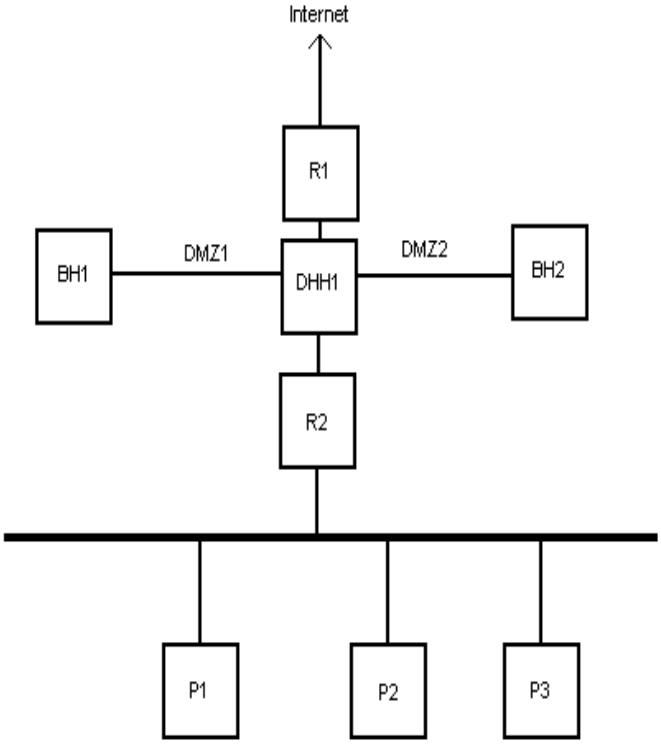
FIG. 10 – Plusieurs routeurs intérieurs, mauvaise solution



Dans cette architecture on utilise plusieurs routeurs intérieurs. Un des problèmes rencontrés est que les routeurs intérieurs décident de faire passer le trafic interne sur la DMZ.

4.6 Une architecture firewall un peu plus complexe

FIG. 11 – Une architecture firewall un peu plus complexe



Dans notre firewall il y a une DMZ publique la DMZ1 où pourrait être installé un web mail (mail accessible depuis une page HMTL). Dans la DMZ2 qui serait privée on installerai le serveur POP et SMTP.

Ce firewall serait assez cher mais il présente l'avantage que chaque machines a un rôle particulier.

Même si l'attaquant arrive à accéder à la DMZ1 il lui reste encore la DMZ2 et le routeur intérieur à passer pour arriver au réseau interne.

5 Conclusion

Nous avons vu les différents éléments composants un firewall, puis les trois grands types d'architecture firewall.

L'architectue d'un firewall dépend de la politique de sécurité, du niveau de sécurité que l'on veut obtenir en fonction du prix (homme et matériel) que l'on veut y mettre.

Aucun firewall n'est parfait, nous avons étudié différentes architectures firewall ayant des degrés de complexité divers. Même le firewall le plus complexe peut être contourné si les règles des différents éléments composants celui-ci ne sont pas adéquates.

De plus pour compléter un firewall on peut aussi installer des IDS.

6 Glossaire

DNS : Domain Name Service

FTP : File Transfert Protocol

IDS : détecteur d'intrusion

packet filtering : le packet filtering contrôle les paquets en fonction de l'adresse de destination, de l'adresse source et des protocoles utilisés.

proxy : Un utilisateur, réel ou virtuel, exécutant une tâche sous l'identité et pour le compte d'un autre, généralement pour exploiter une proximité technique entre l'utilisateur et la ressource accédée.

SMTP : Simple Mail Transfert Protocol

7 Références

site web

http ://www.mnis.fr/home/
http ://www.chez.com/firewalls/chapitre2.html#24
http ://www.tele.ucl.ac.be/ELEC2920/1997/firewall/Firewalls.html
http ://www.freenix.fr/unix/linux/HOWTO/Firewall-HOWTO-3.html
http ://www.devhell.org/ rix/me/texts/firewall.txt

bibliographie

Building Internet firewalls O'REILLY
Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman

TCP/IP administration réseau O'REILLY
Craig Hunt

TCP/IP illustré VUIBERT
W. Richard Stevens