Sécurité Informatique

Chapitre 4 : Pare-feu / IDS / IPS

1. Introduction générale :

Ce chapitre a pour objectif de fournir les informations nécessaires à la mise en place d'une architecture réseau sécurisé. Selon les besoins, différents composants peuvent être utilisés pour sécuriser un réseau, par ex : un ou plusieurs **pare-feu**, un **système de détection d'intrusion**, ou encore **des proxys.**

2. Pare-feu :

2.1. Qu'est-ce qu'un pare-feu?

Un pare-feu (firewall en anglais), est **un système** « ensemble de composants » permettant de protéger un ordinateur ou un réseau d'ordinateurs contre des intrusions provenant d'un autre réseau (notamment internet).

2.2. Domaine à protéger ?

Les pare-feu sont utilisés chaque fois que l'on désir **interconnecter** deux réseaux possédant **des niveaux de sécurité différents.**

Ex : la connexion d'un réseau d'entreprise à Internet.

2.3. Fonctionnement d'un système pare-feu (Comment ?)

2.3.1. Le filtrage (fonction principale):

Un système pare-feu applique une politique de contrôle d'accès « ensembles de règles prédéfinies » entre les deux réseaux permettant de:

- autoriser le paquet (***allow***) ;
- bloquer le paquet (***deny***) ;
- De rejeter la demande de connexion sans avertir l'émetteur (***drop***).

RQ : Une raison pour l'utilisation de DROP plutôt que DENY est d'éviter de donner des informations sur les ports qui sont ouverts. Bloquer des paquets donne les raisons exactes pour lesquelles le paquet a été bloqué

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant soit:

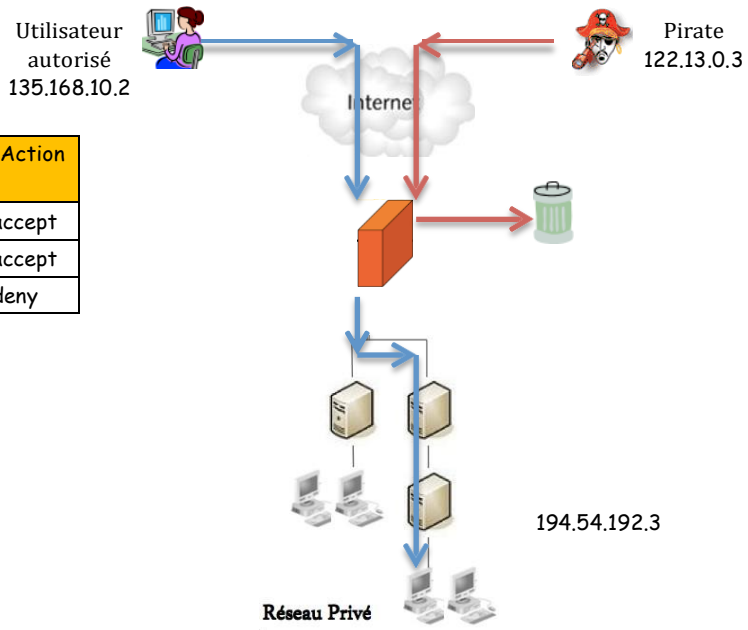
- d'autoriser uniquement les communications ayant été explicitement autorisées : **Principe d'interdiction par défaut** (recommandée).
- d'empêcher les échanges qui ont été explicitement interdits.

2.3.1.1. Critères de filtrage :

Le filtrage est effectué en fonction de :

- L'adresse IP source et destination.
- Protocole (TCP, UDP, ICMP, ...)
- Port (http 80, SMTP 25, FTP, ...)
- Drapeaux (SYN, ACK, ...)

Règle	IP source	IP dest	Protocol	Port source	Port dest	SYN	Action
1	135.168.10.2	194.54.192.3	tcp	*	25	*	accept
2	194.54.192.3	135.168.10.2	tcp	25	*	*	accept
3	*	*	*	*	*	*	deny

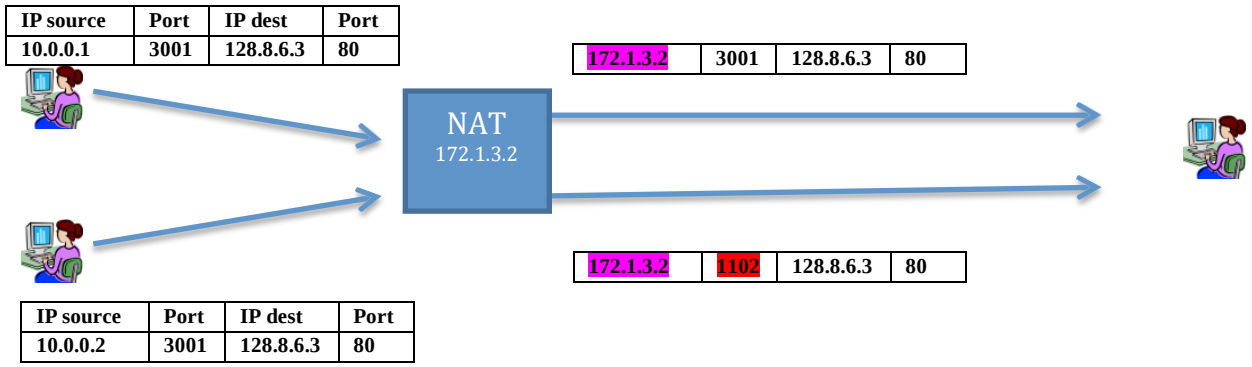


2.3.2. Génération de journal

Un pare-feu peut générer des journaux pour le trafic qu'il accepte ou qu'il rejette. Ces journaux rendent possible la détection de tentative d'intrusion, ou dans le cas d'une attaque réussie, l'identification de la source de l'attaque. Ils peuvent également permettre de détecter des erreurs de manipulation et de configuration.

2.3.3. Translation d'adresse réseau :

La translation d'adresses réseau (NAT) est un mécanisme qui devient nécessaire lorsqu'on connecte un réseau privé à Internet. Pour communiquer avec Internet, on a besoin d'utiliser une adresse IP publique et donc routable.



Le mécanisme du NAT

Interne				Externe			
Source	**Port**	**Dest**	**Port**	**Source**	**Port**	**Dest**	**Port**
~~10.0.0.1~~	3001	128.8.6.3	80	172.1.3.2	3001	128.8.6.3	80
~~10.0.0.1~~	~~3001~~	128.8.6.3	80	172.1.3.2	1102	128.8.6.3	80

Table de translation

- Le principe du NAT consiste à remplacer l'adresse source de tous les paquets quittant le réseau interne par une seule adresse en créant l'impression que tous les paquets viennent de la même machine.
- A la réception d'une réponse, le pare-feu vérifier la table de translation pour trouver la bonne machine (émettrice)

Si deux machines internes souhaitent accéder au même port de la même adresse de destination, et si elles utilisent le même port source, une collision se produit. ➔ Pour éviter ce problème, le pare-feu doit changer le port source de l'un des deux paquets (voir l'exemple).

2.4. Type de pare-feu :

A. Selon le filtrage :

i. ***Pare-feu sans état :*** analyse chaque paquet indépendantes autres paquets, sans prendre en considération les paquets du passé.

ii. ***Pare-feu à état :*** il mémorise l'état de chaque connexion en cours. Ils n'analysent pas seulement si le paquet lui même est valide, mais aussi s'il est compatible avec l'état actuel de la connexion « ***le numéro de séquence***, ***les drapeaux*** qui peuvent être portés par les prochains paquets. Ex : le paquet d'ACK ne peut pas être reçu avant SYN et SYN-ACK »

B. Selon les composants :

i. ***Un pare-feu logiciel*** peut être implémenté en utilisant une simple station de travail sur laquelle un logiciel spécifique est installé.

ii. ***Un pare-feu matériel :*** consiste a utiliser un matériel spécialisé.

2.5. Règles de filtrage

Demande de connexion vers un serveur (SYN) :

- Le client qui initier la connexion
- Pour le port source, on utilise n'importe quelle Numéro (libre). Ex : port source = 2567
- Comme port de destination, il faut utiliser le numéro du port du serveur (un numéro prédéfinit : http = 80, SMTP = 25, ...).
- Le flag SYN est autorisé.

Réponse du serveur

- Le serveur doit utiliser son propre port (prédéfinit) comme port source.
- **Ne peut pas initier** une connexion **avec un client simple** ➔ Ne doit pas contenir le flag SYN uniquement.

Règle inverse :

- Pour chaque requête (règle), on doit y avoir une réponse (pare-feu sans état)
- Dans le cas des pare-feu à état : les règles concernent uniquement la direction dans laquelle la connexion doit être ouverte. Les paquets de réponse qui arrive dans la direction opposée sont implicitement autorisés

Exemple :

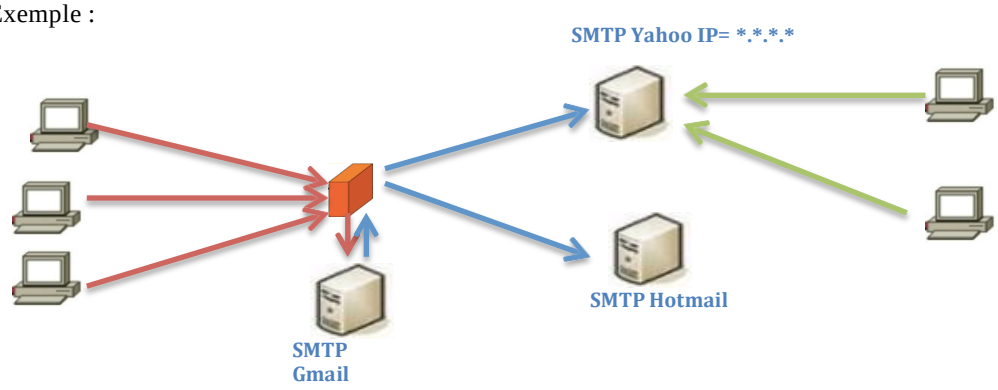


Figure : Exemple d'un pare-feu Gmail (SMTP, port 25)

2.5.1. pare-feu sans état :

- **cas1 : sans l'utilisation des Flags :**

IP Source	Port Source	IP destination	Port Destination	Action
*	*	10.0.0.1	25	permis
10.0.0.1	25	*	*	permis
10.0.0.1	*	*	25	Permis
*	25	10.0.0.1	*	Permis
*	*	*	*	interdit

Problème :

- Cet exemple contient des erreurs (il est plus permissif) !!!
- *Les connexions pouvant être établis en sens inverse* ➔ la règle 4 permet à n'importe quelle machine (l'attaquant utilise le port source 25) de scanner les port de notre serveur (Gmail)

- **cas2 : avec l'utilisation des Flags (solution du 1er pbm) :**

IP Source	Port Source	IP destination	Port Destination	Flag SYN (syn=1, ack=0)	Action
*	*	10.0.0.1	25	*	permis
10.0.0.1	25	*	*	Non	permis
10.0.0.1	*	*	25	*	Permis
*	25	10.0.0.1	*	Non	Permis
*	*	*	*		interdit

Dans le cas d'un Flag = **SYN (syn=1, ack=0),** les choix possibles sont :

- * ➔ tout est permis.
- **Non** ➔ syn=0, ack=0 | syn=0, ack=1 | syn=1, ack=1
- **Oui** ➔ Syn=1, ack=0

RQ :

Lorsque le **Flag = SYN set ?**

- * ➔ tout est permis.
- **Non** ➔ syn=0, ack=0 | syn=0, ack=1
- **Oui** ➔ Syn=1, ack=0| syn=1, ack=1

2.5.2. pare-feu à état :

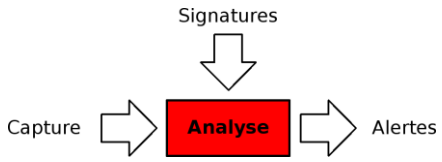
IP Source	Port Source	IP destination	Port Destination	Action
*	*	10.0.0.1	25	permis
10.0.0.1	*	*	25	Permis
*	*	*	*	interdit

3. Détection d'intrusion :

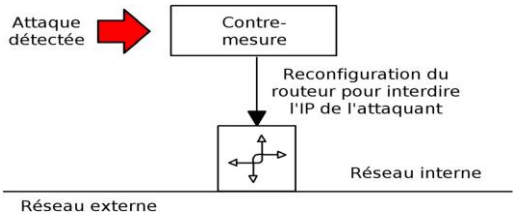
Un system de détection d'intrusion « IDS » permet de détecter immédiatement une attaque et de la bloquer automatiquement, et enfin d 'en limiter les dommages.

Principe de fonctionnement : Un IDS analyse le trafic en permanence et essaie de découvrir les attaques. En fonction de son degré de sophistication, il peut :

- *simplement informer l'administrateur* dans le but d'une intervention manuelle.



- Ou *automatiquement reconfigurer le pare-feu* pour mettre en place (ajouter) des filtres nécessaires pour bloquer l'attaque.



3.1. Méthodes de détection d'intrusions :

Comme pour les codes malveillants, les attaques bien connues en réseau possèdent **une signature** précise. Les IDS se basent sur une base de données des signatures d'attaques connues qui est comparée avec le trafic observé.
D'autres IDS se basent sur la **Caractérisation du trafic (comportement)**

4. Proxy :

Les proxys (ou serveur relais) sont capables de traiter la sécurité au niveau de ***la couche Application.***

Ils travaillent sous la forme d'**intermédiaire** ou un serveur que l'on mandaterait pour faire quelque chose.

Au travers un proxy, un client peut communiquer avec un serveur (http, SMTP, FTP, DNS, ...) sans avoir besoin d'établir une connexion directe avec ce dernier.

4.1. Proxy http :

Si on place un serveur proxy entre votre ordinateur et Internet :

- Votre ordinateur est connecté au serveur proxy.
- C'est le proxy qui est connecté à Internet.
- Vous demandez des pages à ce serveur
- **Il analyse votre requête *(Filtrage)*** pour voir si elle est autorisée ou non
- Il va chercher les pages demandées sur Internet
- **Il analyse la page *(module de protection contre les codes malveillants)*** et vous renvoie les pages demandées.

Les avantages

- Le surf anonyme : Ce n'est pas votre adresse qui est vue sur les sites, mais l'adresse du proxy
- La protection de votre ordinateur : Ce n'est pas vous qui êtes en première ligne sur Internet, vous êtes donc mieux protégé.
- Le filtrage : comme toutes les requêtes et les réponses passent par le proxy, il est possible de filtrer ce que l'on autorise à sortir ou à entrer

Les inconvénients

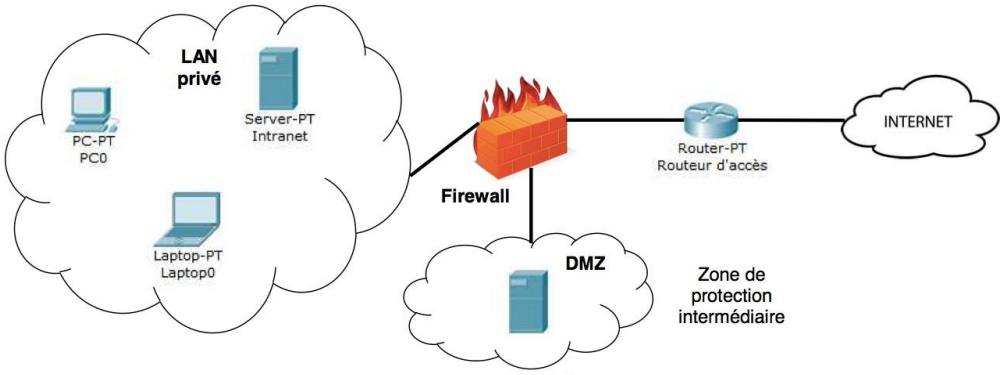
- Le proxy peut voir et enregistrer tout ce qui circule entre votre ordinateur et le web + l'administrateur du serveur proxy est mal intentionné ➔ accès a touts vos informations et l'historique de votre navigation.
- Il peut éventuellement **mettre plus longtemps à répondre**, donc il est possible que le surf à travers un proxy soit un peu plus lent que le surf direct sur Internet.

5. Architecture Réseau avec une zone démilitarisée simple : « Simple DMZ »

Les zones démilitarisées « DMZ » sont utilisées lorsqu'un **niveau de sécurité intermédiaire** est requis.

Une DMZ est une zone qui ***n'est connectée directement à Internet, ni au réseau interne*** (cad il faut mettre un pare-feu pour chaque DMZ).

Dans cette zone, on peut installer des serveurs proxy (http, FTP, DNS, SMTP,...), des serveurs WEB, etc... ➔ Selon ce qu'on va mettre dans cette zone, on rajoute les règles de filtrage appropriées.



6. Architecture Réseau avec une zone démilitarisée en sandwich: « DMZ en sandwich »

Pour une **sécurité Maximal**, on utilise deux pare-feu (sandwich), un de chaque coté de la DMZ. En forçant le trafic à traverser les proxys.

On utilise un proxy diffèrent pour chaque service « SMTP, http, FTP, DNS,... » dans ***le but*** d'éviter une contamination si l'un des proxy venait à être compromis (piraté).

Pour éviter que l'un des proxy puisse espionner le trafic d'un autre ➔ le réseau local qui relie les proxys doit être commuté (Switcher) + les tables ARP doivent être configurées statiquement pour eviter les problèmes d'ARP Spoofing