1. Introduction générale :

Le chapitre précèdent présente un certain nombre de vulnérabilité et d'attaques dans le contexte des réseaux. Ce chapitre, quant à lui 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:

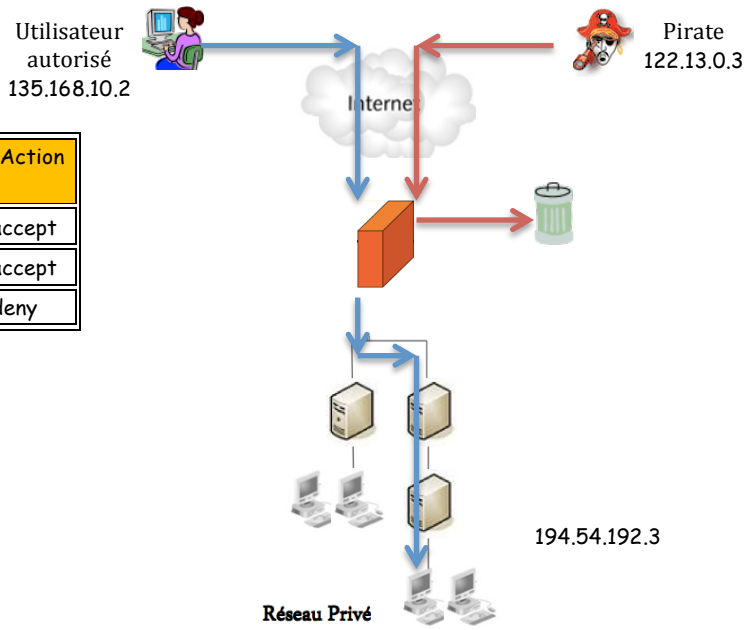
- d'autoriser uniquement les communications ayant été explicitement autorisées : **Principe d'interdiction par défaut** (recommandée).
- d'empêcher les échanges qui ont été explicitement interdits.

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

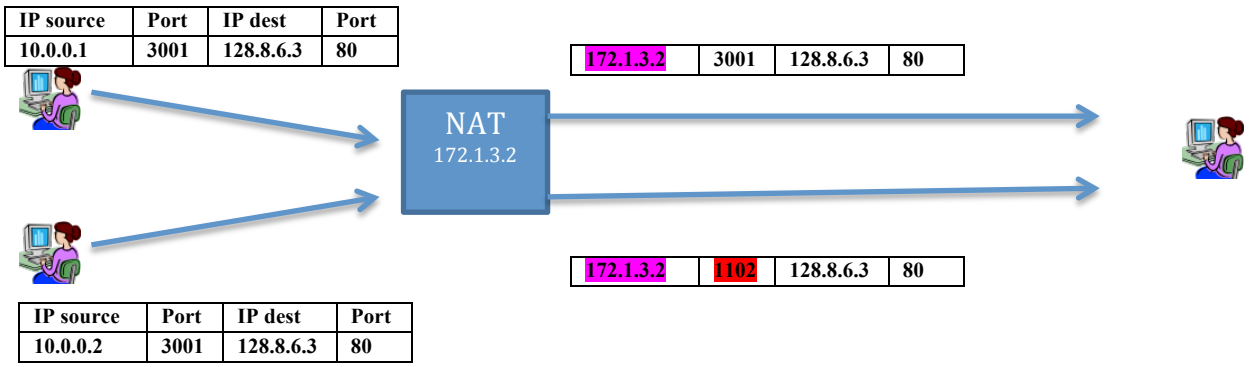


2.3.2. Génération de journal

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 :

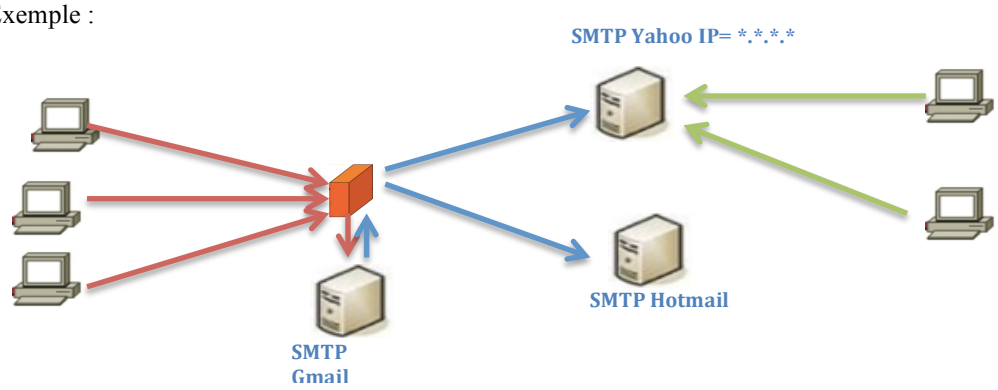


Figure : Exemple d'un pare-feu Gmail (SMTP, port 25)

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 :

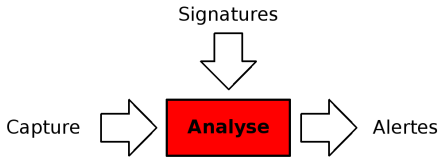
IP Source	Port Source	IP destination	Port Destination	Action
*	*	10.0.0.1	25	permis
10.0.0.1	*	*	25	Permis
*	*	*	*	interdit

3. Détection d'intrusion :

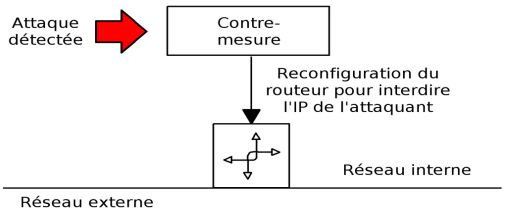
Un system de détection d'intrusion « IDS » permet de détecter immédiatement une attaque et de la bloquer automatiquement, et enfin d 'en limiter les dommages.

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

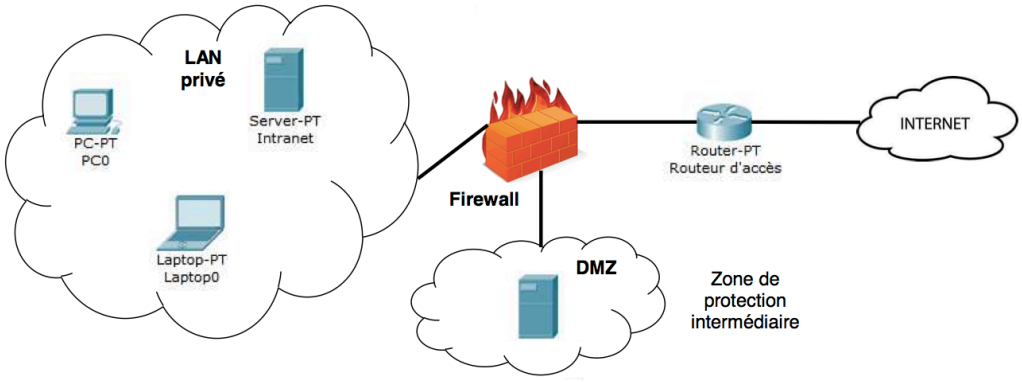
- Le proxy peut voir et enregistrer tout ce qui circule entre votre ordinateur et le web + l'administrateur du serveur proxy est mal intentionné ➔ accès a touts vos informations et l'historique de votre navigation.
- Il peut éventuellement **mettre plus longtemps à répondre**, donc il est possible que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

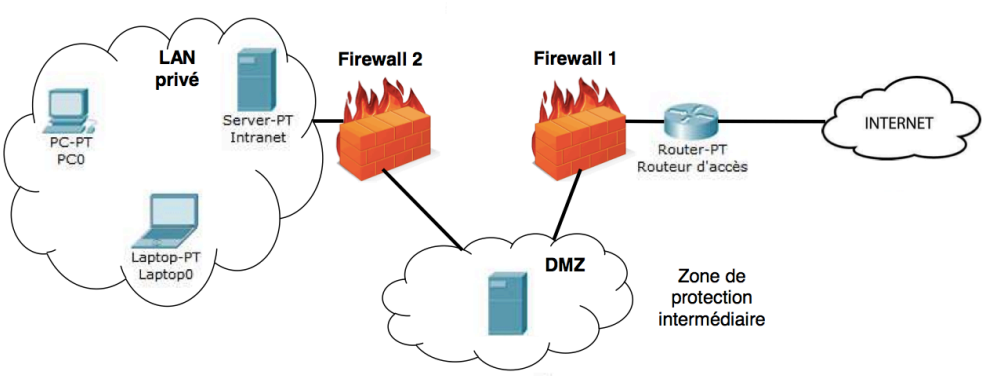


6. Architecture Réseau avec une zone démilitarisée en sandwich: « DMZ en sandwich »

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



TD4

Exo1 : Règles de filtrage d'un pare-feu sans état

On considère un pare-feu sans état qui abrite la machine 203.167.75.1
L'utilisateur de cette machine souhaite :

- Naviguer sur le **Web**.
- Recevoir des connexions **telnet** provenant de l'extérieur du réseau interne.
- Recevoir et initier de la connexion SSH de et vers internet.

Les serveurs http, telnet et SSH utilisent respectivement les ports : 80, 23 et 22.

Q : écrire la table de filtrage du pare-feu en utilisant le critère de filtrage sur les paquets SYN (c.à.d: flag SYN=1 et flag ACK = 0).

Exo2 : pool d'adresses

Une entreprise pratique la translation dynamique d 'adresses avec un pool de 3 adresses IP (193.49.96.60, 193.49.96.61 et 193.49.96.62).

Quatre stations (A, B, C et D) souhaitent accéder au site Web dont l'adresse IP est 128.178.50.93.

Les adresses internes des stations A, B, C et D sont respectivement : 192.168.10.1, 192.168.10.2, 192.168.10.2 et 192.168.10.4.
Les quatre stations utilisent le port source 3001.

Q1 : quelle est la différence entre le NAT statique et le NAT dynamique ?

Q2 : compléter la table de translation du pare-feu pendant la connexion (plusieurs solutions correctes sont possible).

Q3 : quels sont les avantages et les inconvénients du NAT ?

Table de translation du pare-feu pendant la connexion							
Interne				Externe			
Source	Port	Destination	Port	Source	Port	Destination	Port
192.168.10.1							
192.168.10.2							
192.168.10.3							
192.168.10.4							

Exo3 : règles de filtrage d'un pare-feu à état :

On considère l'architecture décrite sur la figure 1. On suppose que l'adresse du serveur web est 10.0.0.2 et que les proxys SMTP, http et DNS possèdent respectivement les adresse : 10.0.0.25 , 10.0.0.80 et 10.0.53.

Les trois proxys sont utilisés en mode direct (donc **vers internet**) et inverse (donc **depuis internet**).

Le serveur web doit aussi être accessible depuis le réseau interne.

On désigne par DMZ_proxy toutes les adresses de la zone des proxys et par DMZ_web toutes les adresse de la zone serveur WEB.

Ecrire les règles de filtrage pour le pare-feu externe à état (pf1)

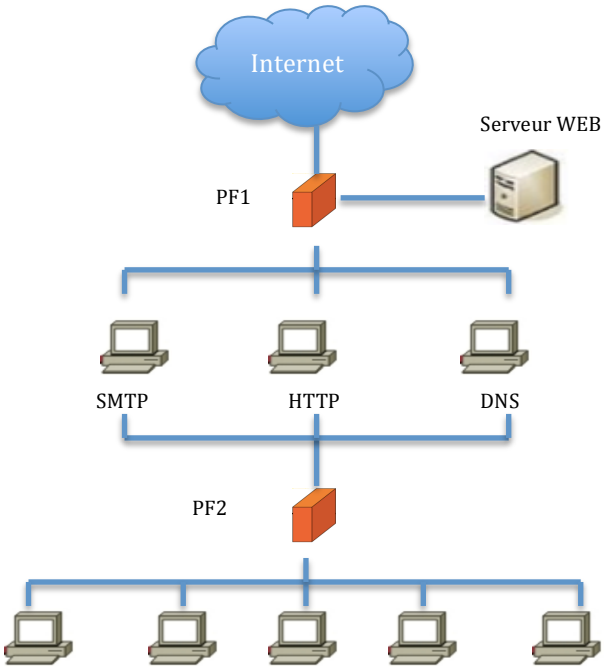


Figure1

Exo4 : résumé : réseau DMZ en sandwich

RQ : le masque du sous réseau utilisé dans cet exercice est 255.255.255.0

L'entreprise Tayssir spécialisé dans le domaine du logiciel financier, a demandé un **audit** externe sur la sécurité de son réseau informatique.

A la suite des conclusions catastrophiques de cet audit, elle a amélioré significativement ses infrastructures au niveau de la sécurité.

Voici une description sommaire de la topologie actuelle de son réseau :

1. ***Réseau interne privé***:
   - Un serveur de fichiers (ayant l'adresse IP **192.168.0**.5 sous linux), utilisé principalement par des développeurs.
   - Un serveur messagerie (**192.168.0**.4)
   - Le serveur de secrétaire (**192.168.0**.2 sous Windows)
   - Les postes de travail de tous les employés (**192.168.0**.10 à **192.168.0.**60)
   - L'ordinateur portable du directeur (**192.168.0**.9)

2. Le réseau interne est connecté a internet par le biais de ***deux pare-feux*** à état :
   - Pare-feu 1 avec 3 interfaces : (**128.178**.73.45 / **10.0.1**.1 / **10.0.2**.1)
   - Pare-feu 2 avec 2 interfaces : (**10.0.3**.1 / **192.168.0**.1)

3. Les 2 pare-feux délimitent une zone démilitarisée (DMZ en sandwich) dans laquelle se trouvent ***des proxy*** :
   - Proxy HTTP avec 2 interfaces (**10.0.2.**10 / **10.0.3**.10), port 80.
   - Proxy HTTPS avec 2 interfaces (**10.0.2**.11 / **10.0.3**.11) port 443.
   - Proxy SMTP avec 2 interfaces (**10.0.2**.12 / **10.0.3**.12) port 25.

4. Enfin, le serveur Web public (10.0.1.2) de l'entreprise est situé dans une zone DMZ simple différente de celle des proxys.

Par la suite aucun des problèmes de sécurité n'est dû à un dysfonctionnement au niveau des DMZ, des proxys ou des pare-feux.

Q1 : Dessiner **le schéma du réseau** de l'entreprise et écrire les **tables de filtrage** des deux pare-feux.

Pour des raisons de simplicité d'utilisation, l'administrateur du système a choisi la même marque d'anti virus sur le proxy SMTP et sur le serveur de messagerie.

Q2 : Commenter ce fait.

Un beau jour, l'un des développeurs se vante d'avoir eu accès à la liste des fichiers de tous les employés de Tayssir.

Q3 : expliquer en quoi l'architecture actuelle du réseau de cette entreprise **favorise** (laisse) ce genre d'évènement.

Deux jours plus tard, des documents confidentiels « décrivant les spécifications du dernier prototype de logiciel révolutionnaire développé par Tayssir » se trouvent sur internet (alors que ces document ne sont distribués que sur le réseau Interne de l'entreprise) !!!

Q4 : donner 2 explications vraisemblables (semble vrai, logique).

Un matin, l'administrateur système constate que tous les postes de travail sont infectés par un VER connu depuis plusieurs mois qui se propage via le réseau.

Q5 : donner la source d'infection la plus probable

Le directeur remarque que la productivité de l'un des développeurs, programmeur de talent n'est pas rentable. Il réalise que son employé joue des heurs avec un jeu en ligne (counter strike).
Le directeur, surpris que la configuration du réseau de l'entreprise laisse fonctionner ce jeu (ce jeu utilise un Protocol bloqué par le pare-feu) ➔ il demande des explications à l'administrateur système. Ce dernier lui répond que la configuration réseau de l'entreprise n'est pas la mis en cause.

Q6 : comment est-il possible de faire fonctionner un tel jeu ? Quel est le principe fondamental qui a été violé dans ce cas ?

TD4 (correction)

Exo1 :

IP Source	Port Source	IP destination	Port Destination	Flag SYN (syn=1, ack=0)	Action
203.167.75.1	*	*	80	*	permis
*	80	203.167.75.1	*	non	permis
*	*	203.167.75.1	23	*	permis
203.167.75.1	23	*	*	non	permis
203.167.75.1	*	*	22	*	permis
*	22	203.167.75.1	*	non	permis
*	*	203.167.75.1	22	*	permis
203.167.75.1	22	*	*	non	permis
*	*	*	*	*	Interdit, log

Exo2 :

1) Différence entre le NAT statique et dynamique :

Avec le **NAT statique** (port forwarding) , les adresses qui entrent en jeu sont **fixées à l'avance**. Ceci permet de rediriger des paquets précis vers une machine interne, ***même si celle-ci n'a pas envoyé de paquets vers l'extérieur***.

Le NAT dynamique choisit les adresses (insérer une entrée) à la volée, ***en fonction des paquets envoyés par les machines internes.***

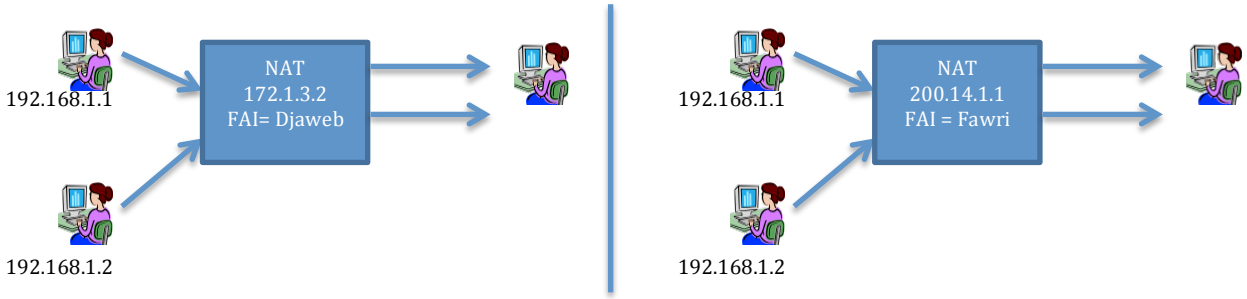
2) Avantages et inconvénients :

a. Avantage :

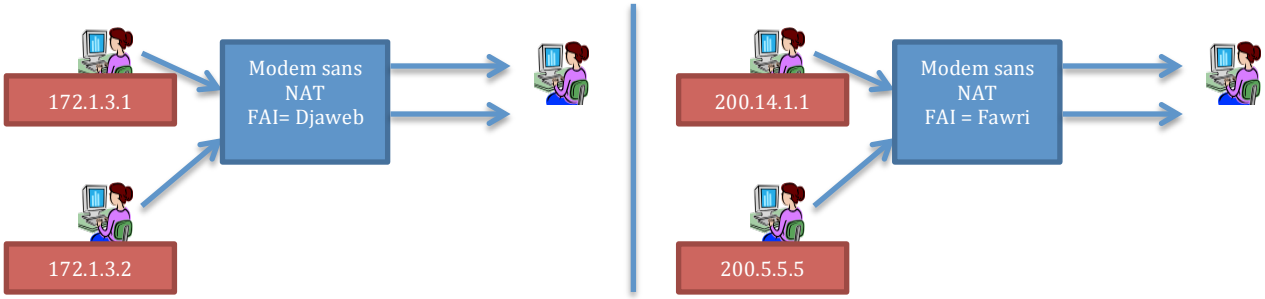
- Le NAT permet de connecter un nombre important (plusieurs) de machine à Internet en n'utilisant que peu d'adresse IP publiques (une seule adresse) ➔ **réduit le cout car l'achat d'adresse IP est coûteux.**

- Dans le NAT dynamique : Puisqu'aucune connexion ne peut être initiée vers **une machine cachée** (qui se trouve dans le réseau interne) derrière un pare-feu (ex : routeur) ➔ **le NAT apporte une protection supplémentaire.**

- **Le NAT facilite la maintenance du réseau.** Par exemple : le changement de fournisseur d'accès (FAI Djaweb 172.x.x.x à Fawri 200.x.x.x) ➔ changement de l'adresse IP public c'est tout➔ ne nécessite pas une reconfiguration de toutes les machines (pas de changement d'adresse privé).



Si on n'a pas le NAT, chaque machine doit acheter une adresse publique pour chaque machine.



b. Inconvénients :

- **Une attaque** venant **de l'intérieur** du réseau interne vers Internet sera **plus difficile à tracer** (car touts les postes utilisent la même adresse publique). Car les **Logs ne sont pas conservés**
- Certains protocoles ne permettent pas la modification des paquets ➔ on ne peut pas l'utiliser : par exemple IPsec .

3) Il existe plusieurs réponses à cette question selon la règle d'attribution du *pool.*

On considère ici (la solution proposé dans cet exercice) que le pare-feu effectuant le NAT :

- **distribue dans un premier temps** (au début) **les adresses IP disponibles** dans le *pool.*
- Puis, **lorsque le pool est vide** (on a utilisé toutes les adresses) ➔ **il distribue une adresse déjà utilisée** mais change le port source.

Table de translation du pare-feu pendant la connexion							
Interne				Externe			
Source	Port	Destination	Port	Source	Port	Destination	Port
192.168.10.1	3001	128.178.50.93	80	193.49.96.60	3001	128.178.50.93	80
192.168.10.2	3001	128.178.50.93	80	193.49.96.61	3001	128.178.50.93	80
192.168.10.3	3001	128.178.50.93	80	193.49.96.62	3001	128.178.50.93	80
192.168.10.4	3001	128.178.50.93	80	193.49.96.62	3002	128.178.50.93	80

Autre solution : On pourrait également imaginer que le pare-feu ne distribue qu'une seule adresse IP (par exemple, les autres sont réservées des utilisateurs privilégié) et translate tous les ports source qui provoquent des collision.

Exo3 : voir Q1 de l'exo 4, avec la différence que les proxys ici (même le proxy http) accepte des connexion depuis l'extérieur.

M. Bada

Exo4 :

1. le schéma du réseau Tayssir est donné sur la figure ci-dessous.

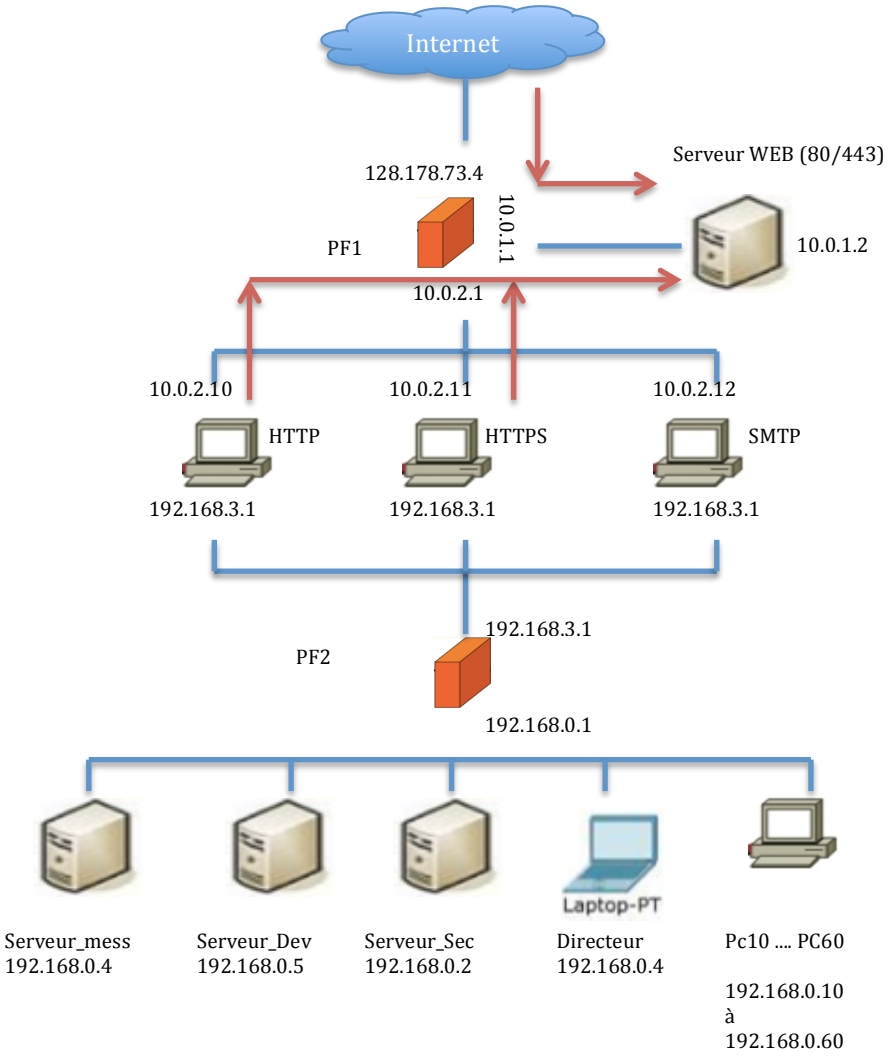


Figure : Direction de connexion pour le serveur Web (PF1)

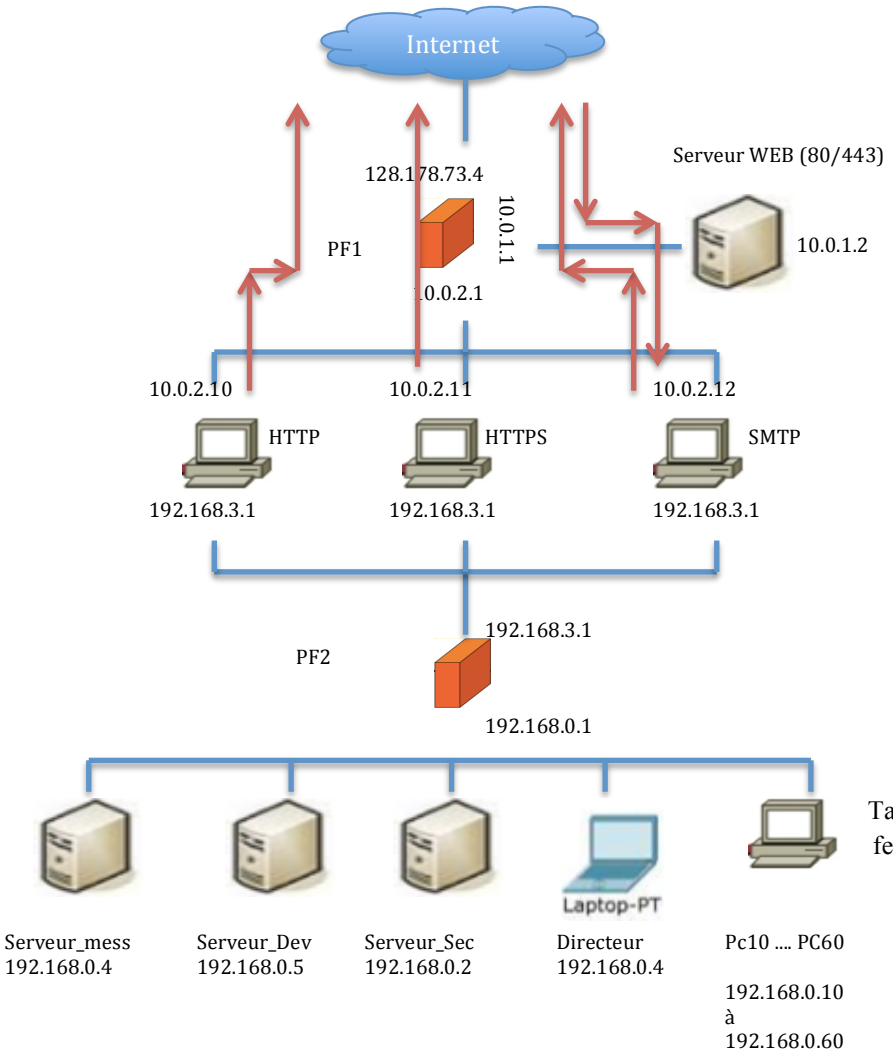


Table du pare-feu PF1 :

Figure : Direction de connexion pour les proxys (PF1)

IP Source	Port Source	IP destination	Port Destination	Action
*	*	10.0.1.2 (serveur_web)	80/443	permis
*	*	Z_SiteWeb	*	interdit
Z_SiteWeb	*	*	*	interdit
10.0.2.10	*	*	80	permis
10.0.2.11	*	*	443	permis
10.0.2.12	*	*	25	Permis
Z_Proxys	*	*	*	interdit
*	*	10.0.2.12	25	permis
*	*	Z_Proxys	*	interdit
*	*	*	*	Interdit, log

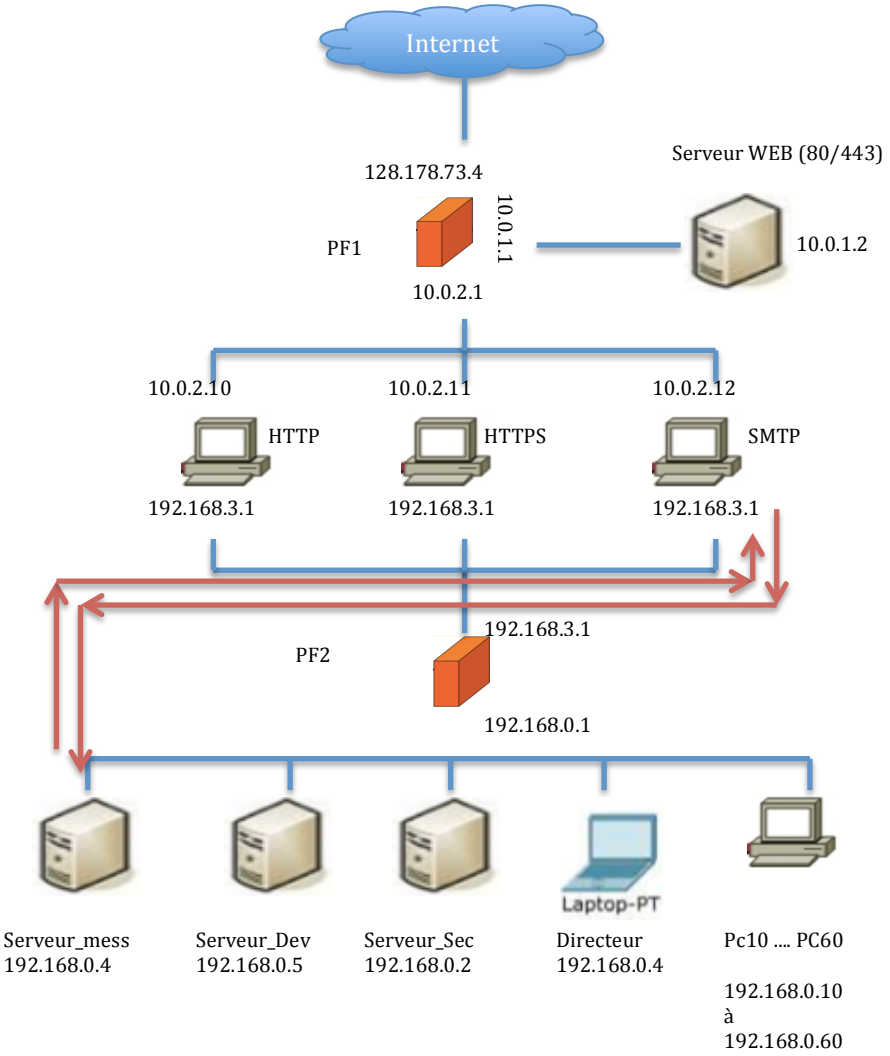


Figure : Direction de la connexion seulement entre le serveur messagerie et le proxy SMTP (dans les 2 sens : accéder a la boite et déposer un mail par un autre serveur messagerie)

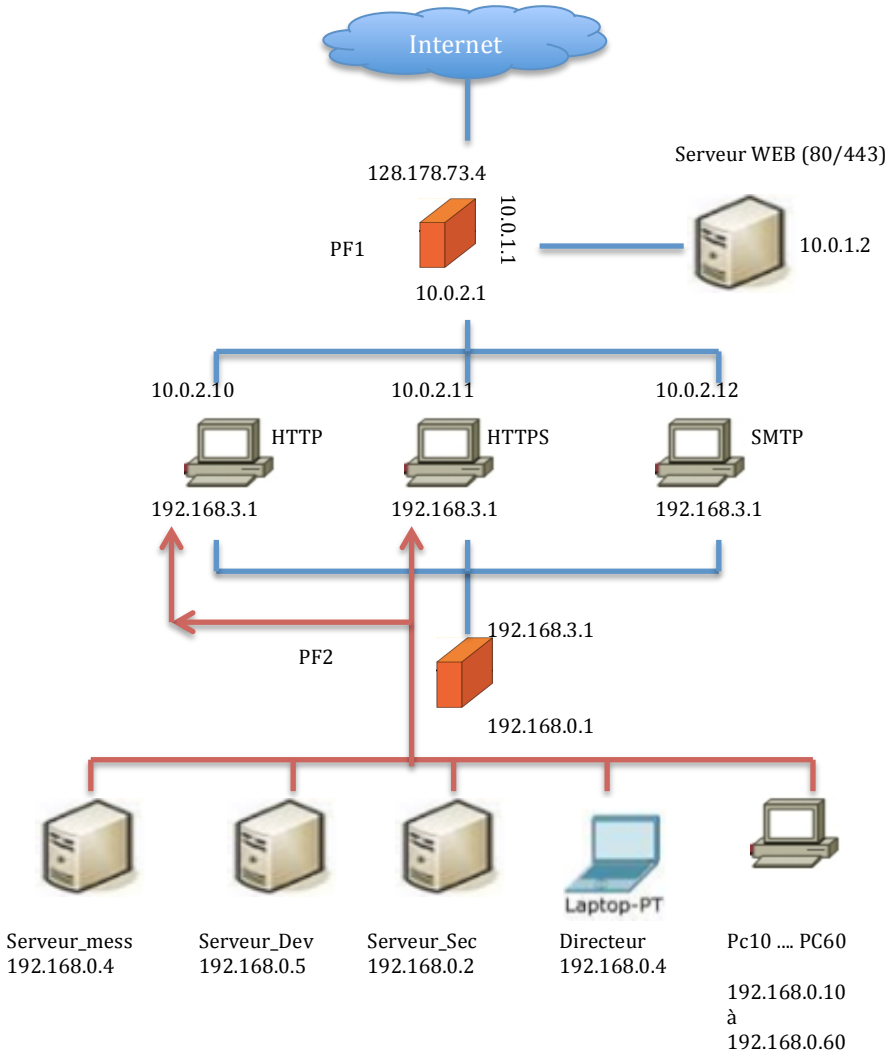


Figure : touts les membres de la zone interne peuvent accéder aux Proxys WEB, mais les proxy_WEB ne peuvent pas initier une connexion avec la zone interne

Table du pare-feu PF2 :

IP Source	Port Source	IP destination	Port Destination	Action
10.0.3.12	*	192.168.0.4	25	permis
*	*	Z_Interne	*	interdit
192.168.0.4 (Serv_mess)	*	10.0.3.12 (proxy SMTP)	25	permis
Z_Interne	*	10.0.3.10 (proxy HTTP)	80	permis
Z_Interne	*	10.0.3.11 (proxy HTTPS)	443	permis
Z_Interne	*	*	*	interdit
*	*	*	*	Interdit. log

2. le fait d'utiliser 2 antivirus c'est bien (défense en profondeur) MAIS **utiliser le même Antivirus ➔ perte de temps + compliquer l'architecture (violer le principe de simplicité).**

Solution : l'utilisation de ***deux produits différents*** ➔ élargir le spectre des attaques détectées.

3. le pare-feu protège le réseau contre les attaques externes ➔ le **niveau de la sécurité**, pour ce qui concerne les attaque **interne** est **MINIMAL.**

4. plusieurs scénarios sont possibles :

- Le document se trouve sur l'ordinateur du directeur ➔ directeur connecté sans protection à la maison ou un hôtel.
- Un employé de l'entreprise a pu divulguer (vendre) les documents confidentiels (difficile d'éviter ce genre de menace).
-

5. infection du réseau interne par un VER :

- Toujours, la source d'infection est très probablement le portable du directeur ➔ le VER se propage dans tout le réseau Interne.
- L'un des employés a utilisé **un point d'accès sauvage (non sécurisé par un PF. Exp : point d'accès Android avec la 3G)**

6.

a. l'employé a réussi de lancer le jeu en utilisant un point d'accès sauvage (une connexion sans fil pour établir une connexion non sécurisé).

b. les principes de sécurité violée :

- **Le maillon (élément) faible :** la sécurité de l'ensemble de réseau ne sera pas plus élevée que celle du maillon faible. Cad :

  le niveau de sécurité < ou = le niveau de l'élément le plus faible.

- **Le principe de goulet d'étranglement** n'est plus respecté si on utilise un point d'accès sauvage (**une porte sans gardien**) ➔