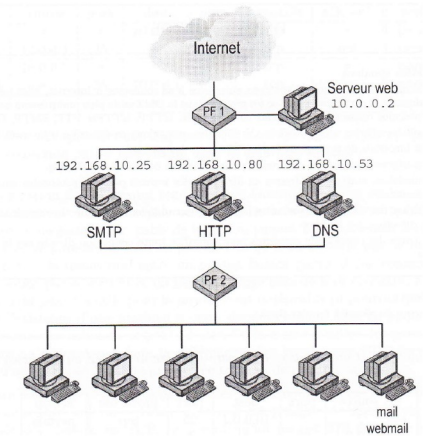
hierie des Protocoles et Logiciels Sécurisés

Pare-feux : Translation, Filtrage, Mandataires et Détection d'Intrusions

Version 1



YACINE CHALLAL

06/12/2014

Table des matières

I

Pare-feux : Translation, Filtrage, Mandataires et Détection d'Intrusions

A. Généralités sur les pare-feux

Rôle d'un pare-feu

Un pare-feu a pour rôle d'interconnecter deux réseaux ayant des niveaux de sécurité différents et d'éviter la propagation d'attaques entre les réseaux reliés

Typologie de pare-feux

On peut classifier les pare-feux selon plusieurs typologies :

- Logiciel/Matériel: un PF matériel offre un niveau de sécurité plus élevé, car le PF logiciel hérite des vulnérabilités de l'OS, des logiciels etc.
- Avec ou sans état:
  - Sans état: le PF analyse chaque paquet indépendamment des autres
  - Avec état: le PF mémorise l'état de la connexion, connaît par exemple les numéros de séquences Si un ACK tarde à venir, envoie lui-même un RST pour détruire les connexions semi-ouvertes Répond lui-même par SYN-ACK, et n'evoie SYN au destinataire que lorsqu'i reçoit ACK Modifie les numéros de séquences pour éviter les attaques qui se basent sur la déduction du prochain ISN

Fonctions de pare-feu

- Translation d'adresses: NAT/PAT
  - Dissimuler les services et architecture du réseau interne
  - Partage d'une connexion à Internet pour un grand réseau via un pool réduit (voire une seule) d'adresses publiques
- Filtrage: ACL, niveaux routage et transport
  - Prévention d'attaques,
  - Coupe propagation d'attaques
- Proxy / Reverse Proxy: filtrage niveau applicatif
  - Filtrage de contenus inappropriés,
  - Protection contre des attaques applicatives
- Détection d'Intrusions
- Autres:
  - Authentification des connexions
  - Chiffrement
  - Analyse de paquets
  - Journalisation

B. Stratégies de sécurité

Méthode

Il existe plusieurs stratégies de sécurité qui sont considérées dans la configuration des systèmes en général et des pare-feux en particulier :

- Moindre privilège: Chaque utilisateur et chaque module ne doit avoir que les droits minimaux pour effectuer ses tâches. Ainsi un serveur web sera lancé sous des droits minimaux (nobody sous unix) pour limiter les conséquences d'une vulnérabilité ou erreur de configuration
- Défense en profondeur: L'usage de plusieurs mécanismes de sécurité redondants est encouragé. Ceci permet une sécurité efficace même si l'une des protections s'avérait être vulnérable. Par exemple, même si un pare-feu bloque toutes les connexions FTP, il est nécessaire de désactiver les serveurs FTP installés par défaut
- Goulet d'étranglement Construire un pare-feu de telle sorte que tout le trafic passe à travers un seul point. C'est une configuration similaire à l'organisation des services de douanes et PAF dans un aéroport
- Maillon le plus faible : Un système de protection ne sera jamais plus efficace que son élément le plus faible. Avant d'investir de façon inconsidérée dans un élément de sécurité, on doit vérifier que tous les éléments du système possèdent une sécurité équivalente. Par exemple, il ne sert à rien d'utiliser un antivirus pour les transferts FTP si l'on ne fait pas la même chose pour HTTP, SMTP
- Déni par défaut : Interdire tout ce qui n'est pas explicitement permis. Par exemple, dans un pare-feu, décrire le trafic utile et autorisé et interdire tout le reste.
- Participation des utilisateurs : Tous les utilisateurs doivent adhérer à la stratégie de sécurité. Ceci d'oit s'appuyer sur une communication pédagogique des restrictions sécuritaires
- Simplicité : Plus un système de protection est simple, plus il a des chances d'être configuré correctement

C. Translation d'adresses

Définition : Le NAT (Network Address Translation)

Le NAT a pour rôle de connecter un réseau privé à Internet via une ou un ensemble réduit d'adresses IP publique routable.

Remarque : Adresses privées

Des plages d'adresses IP non routables sont réservées aux réseaux privés

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

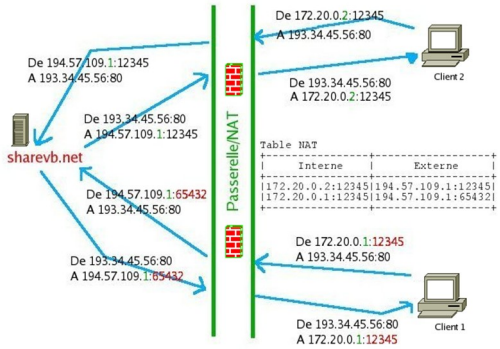
Méthode : Comment se fait le NAT

Remplacer l'adresse source de tous les paquets quittant le réseau interne pour Internet par une seule adresse publique

- Il est suffisant d'avoir une seule adresse publique pour connecter toutes les stations du réseau privé à Internet
- Les PF ou routeurs qui gèrent le NAT doivent gérer une table de translation
- Ceci permet de cacher les services et architecture interne du réseau

Exemple

La figure suivante illustre un exemple d'un pare-feu effectuant la fonction de NAT :



Exemple de NAT

Quand une machine interne se connecte vers l'extérieur, le NAT remplace son adresse source privée par une adresse IP publique routable. Afin de différencier deux flux appartenant à deux machines différentes, le NAT associe à chaque machine un numéro de port différent (généralement généré aléatoirement) et maintient la correspondance dans la table NAT.

Complément : NAT dynamique / statique

Dans le NAT dynamique, l'adresse attribuée à une machine interne (IP publique + numéro de port) est générée dynamiquement et change d'une connexion à une autre.

Il est parfois utile voire nécessaire d'attribuer toujours la même adresse à une machine interne spécifique (serveur web par exemple) pour qu'elle puisse être accessible de l'extérieur sur la même adresse.

Dans ce cas, il est possible de configurer le NAT pour fixer l'adresse publique (IP + numéro de port) attribuée à une machine interne.

On parle alors de NAT statique.

D. Filtrage

Dans ce qui suit on définira le concept de filtrage en général puis on étudiera les règles de filtrage

1. Filtrage : Généralités

Définition : Fonction de filtrage

Il s'agit de filtrer le trafic qui circule entre les zones auxquelles est connecté le PF.

Les règles de filtrage sont définies par l'administrateur du PF.

Exemple : Politique de filtrage

- Connexions d'une origine interne vers Internet sont permises
- Connexions d'Internet vers une machine interne: seules certaines destinations et services précis seront autorisés (HTTP, SMTP, etc.)

Critères de filtrage

- Adresse IP source ou destination
- Protocole (TCP, UDP, ICMP, ...) et port
- Drapeaux et options: TCP SYN, ACK, ICMP, ...

Exemple : Règles de filtrage

- Refuser un paquet externe portant une adresse IP interne (spoofing)
- Autoriser le ping (echo-request) dans une direction et uniquement les réponses (echo-reply) de ces requêtes dans l'autre direction

2. Règles de filtrage

Règle de filtrage

La configuration d'un PF repose sur des règles de filtrage. Dans chaque règle on spécifie les caractéristiques du paquet

- adresses source,
- adresses destination,
- ports,
- drapeux, etc.

On spécifie l'action à prendre

- Permission,
- interdiction

Attention : Ordre des règles

Pour chaque paquet reçu, le PF parcourt la liste des règles jusqu'à ce qu'il en trouve une qui s'applique. L'ordre est donc très important. On doit toujours terminer par une règle générale qui s'applique à tous les paquets et qui les détruit.

	Source	Port	Dest	Port	Protocole	action
1	*	*	10.0.0.1	25	Tcp	Permis
2	10.0.0.1	*	*	25	Tcp	Permis
3	*	*	*	*	*	Interdit

Deny All Rule

Exemple : PF sans mémoire

On considère la politique de filtrage qui consiste à n'autoriser que le mail (SMTP sur le port 25). La table des règles de filtrage serait comme suit :

	Source	Port	Dest	Port	Protocole	action
1	*	*	10.0.0.1	25	Tcp	Permis
2	10.0.0.1	25	*	*	Tcp	Permis
3	10.0.0.1	*	*	25	Tcp	Permis
4	*	25	10.0.0.1	*	Tcp	Permis
5	*	*	*	*	*	Interdit

Autoriser SMTP uniquement (sans mémoire)

Cette configuration souffre d'une permissivité non souhaitée, par exemple :

- Selon la règle 2, il suffit qu'une station porte l'adresse du serveur et port 25 pour se connecter à n'importe quelle destination
- Selon 4, il suffit qu'un paquet ait port 25 pour se connecter à n'importe quel port du serveur mail.

Une solution à ce problème serait de préciser les flags TCP pour empêcher le flux dans une certaine direction

Exemple : PF sans mémoire avec flags TCP

Avec un PF sans mémoire et test sur des flags TCP, la table de filtrage qui n'autorise que le protocole SMTP sur port 25 serait la suivante :

	Source	Port	Dest	Port	Protocole	ACK?	action
1	*	*	10.0.0.1	25	Tcp	*	Permis
2	10.0.0.1	25	*	*	Tcp	Oui	Permis
3	10.0.0.1	*	*	25	Tcp	*	Permis
4	*	25	10.0.0.1	*	Tcp	Oui	Permis
5	*	*	*	*	*	*	Interdit

Autoriser SMTP uniquement avec PF sans mémoire et test sur flags TCP

Exemple : PF avec mémoire

La même politique de filtrage avec un PF avec mémoire donnera lieu à la table suivante :

	Source	Port	Dest	Port	Protocole	action
1	*	*	10.0.0.1	25	Tcp	Permis
2	10.0.0.1	*	*	25	Tcp	Permis
3	*	*	*	*	*	Interdit

Autoriser SMTP uniquement en utilisant un PF avec mémoire

Il faudra donc préciser uniquement la direction de la connexion. Le PF autorise implicitement le flux de retour .

Complément : Les ACL

ACL (Access Control List) sont implémentées dans les routeurs. Il s'agit d'une suite de ACE (Access Control Entry) décrivant les règles de filtrage

Syntaxe

access-list {numéro} {deny|permit} {source} {masque inverse}

access-list {numéro} {deny|permit} {protocole} {source} {masque inverse} [port] {destination} {masque inverse} [port] {log | log-input} [fragments] [established]

Exemple : Autoriser le trafic icmp

```
access-list 100 permit icmp any any /* détruit tout le reste du trafic */
access-list 100 deny ip any any log-input
```

Exemple : Autoriser un flux émanant d'un réseau précis

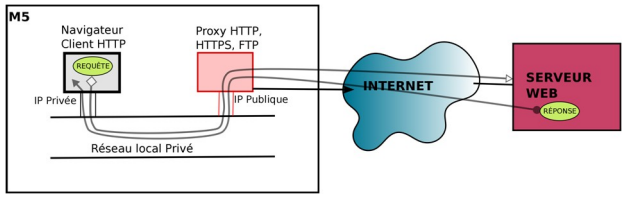
```
!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected.
access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

E. Proxy

Méthode : Rôle d'un proxy

Un proxy traite le filtrage au niveau applicatif. Dans cette configuration, un client communique avec un serveur sans connexion directe, il passe par le proxy. de ce fait,aucun paquet n'est directement échangé entre le client et Internet.

La figure suivante illustre une telle configuration :



Proxy

Complément : Filtrage applicatif

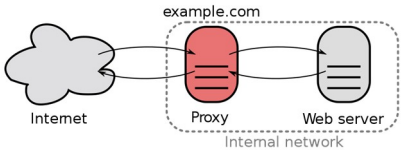
Un proxy peut examiner le contenu d'un paquet et le filtrer si ce contenu n'est pas approprié

Exemple : Fonctionnement du Proxy dans ISA Server

Lorsque le service Web proxy (w3proxy.exe) reçoit une requête, il vérifie si le serveur ISA possède des règles de protocoles ou des règles de sites et contenus. En fonction de la définition des règles, un refus, une authentification ou une acceptation est accordée. Si l'accès est autorisé, alors le service Web proxy fait appel au driver NAT. Ce dernier modifie l'adresse source du client (interne) par celle du serveur ISA (externe). Il modifie aussi le port source par un port aléatoire dynamique, et garde une correspondance entre l'ancien et le nouveau port. Quand le serveur Web Internet répond, il envoie sa réponse à l'adresse du serveur ISA sur le numéro de port choisi par le driver NAT. Quand le serveur ISA reçoit cette réponse, il consulte la table de correspondance et la renvoie au client du réseau privé.

Reverse Proxy

Un proxy inverse (reverse proxy) est habituellement placé en frontal de serveurs web. Le proxy inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes . La figure suivante illustre une telle configuration :



Reverse Proxy

Cette technique permet d'assurer les fonctions suivantes:

- Mémoire cache : le proxy inverse peut décharger les serveurs Web de la charge de pages/objets statiques par la gestion d'un cache web local. On parle alors d'« accélérateur web » ou d'« accélérateur HTTP ».
- Intermédiaire de sécurité : le proxy inverse protège un serveur Web des attaques provenant de l'extérieur.
- Chiffrement SSL : le proxy inverse peut être utilisé en tant que « terminateur SSL », par exemple par le biais de matériel dédié,
- Répartition de charge : le proxy inverse peut distribuer la charge d'un site unique sur plusieurs serveurs Web applicatifs. Selon sa configuration, un travail de ré-écriture d'URL sera donc nécessaire,
- Compression : le proxy inverse peut optimiser la compression du contenu des sites.

F. Architectures de Pare-Feux

Dans ce chapitre nous allons explorer les différentes architectures possibles de déploiement de pare-feux. Nous étudierons pour chacune d'elles les avantages et inconvénients.

1. Pare-feu personnel

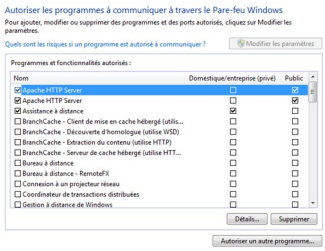
Définition

Il s'agit d'un pare-feu installé sur un poste de travail et configuré par l'utilisateur du poste. Il permet d'autoriser certaines applications à générer du flux vers l'extérieurs et de filtrer les flux acceptables en entrée.

Pare-feu personnel

Exemple : Pare-feu Windows

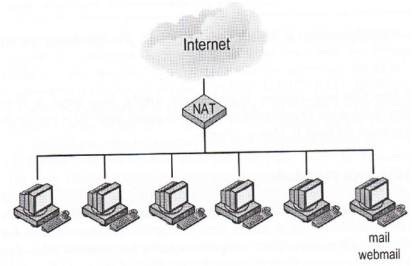
Sous windows on peut configurer le pare-feu pour bloquer toutes les connexions entrantes et sortantes. Lorsqu'un programme souhaite envoyer un paquet sur Internet, le logiciel va demander à l'utilisateur de confirmer cette action. La figure suivante illustre la boîte de dialogue permettant de configurer les accès par application.



Configuration d'un pare-feu windows

2. NAT et filtrage

Il s'agit de connexion d'un réseau local à Internet en utilisant du filtrage et NAT comme illustré sur la figure suivante :



NAT et filtrage

Méthode : Configuration standards

- Translation dynamique d'adresses pour toutes les adresses internes
- Translation statique d'adresses pour les serveurs devant être accessibles depuis Internet (par exemple, SMTP et HTTP pour le serveur de courrier électronique)
- Filtrage des connexions sortantes pour n'autoriser que les protocoles nécessaires (par exemple, HTTP, HTTPS, FTP, SMTP, DNS)
- Filtrage des connexions entrantes pour interdire les connexions directes sur le pare-feu

Attention : Limitations

- Il n'existe pas d'nalyse de contenu (comme les virus) du trafic venant d'Internet
- Depuis Internet, des connexions directes sont effectuées sur des serveurs internes

Remarque : Applications

- Niveau de sécurité requis : peu élevé
- Peu adapté pour les serveurs qui nécessitent d'être accessible à un large public (tels que les serveurs web)

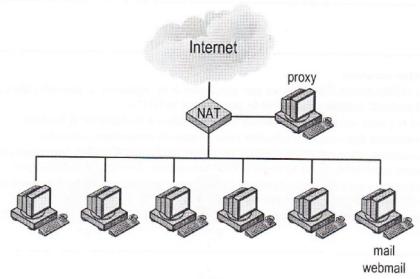
3. Pare-feu avec zone démilitarisée (DMZ)

Définition : Demiliterized Zone (DMZ)

Une DMZ est une zone qui n'est connectée directement ni à Internet ni au réseau interne. Dans cette zone on installe les serveurs sensibles (web, relais, etc.)

Exemple

Dans l'architecture suivante, le serveur proxy est mis dans une DMZ



DMZ

Méthode : Configuration standard

- Les machines internes ne sont pas autorisées à se connecter à Internet. Elles peuvent uniquement communiquer avec le serveur proxy dans la DMZ.
- Seul le proxy est autorisé à établir des connexions à direction d'Internet.
- Translation dynamique d'adresses pour toutes les adresses internes
- Translation statique d'adresses pour les serveurs devant être accessibles depuis Internet (par exemple, SMTP et HTTP pour le serveur de courrier électronique)
- Filtrage des connexions sortantes pour n'autoriser que les protocoles nécessaires (par exemple, HTTP, HTTPS, FTP, SMTP, DNS)
- Filtrage des connexions entrantes pour interdire les connexions directes sur le pare-feu

Attention : Limitations

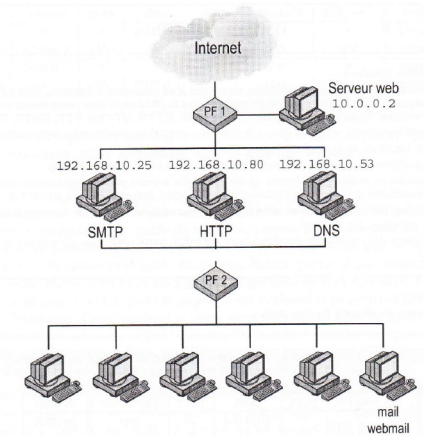
- Le pare-feu est un point critique. Toute vulnérabilité du pare-feu peut être exploitée pour accéder à l'ensemble des serveurs internes.
- Tous les services passent au travers du proxy. Si l'un des services est vulnérable, c'est tout le trafic qui peut être compromis (espioné, bloqué, redirigé, modifié, etc.)

Remarque : Applications

- Niveau de sécurité requis : moyen

4. Pare-feu avec zone démilitarisée en sandwitch

La figure suivante illustre une telle architecture :



DMZ en sandwitch

On utilise deux pare-feux, un de chaque côté de la DMZ. On évite de connecter directement les deux pare-feux en forçant le trafic à traverser les proxy qui sont connectés à chaque pare-feu. On utilise un proxy différent pour chaque service pour éviter la contamination en cas d'attaque. Le réseau local qui relie les proxy doit être commuté (switch) plutôt que partagé (hub) pour éviter l'écoute du trafic.

Méthode : Configuration standard

- Les machines internes ne sont pas autorisées à se connecter à Internet. Elles peuvent uniquement communiquer avec les proxy dans la DMZ, et de plus uniquement avec les protocoles respectifs des proxy.
- Seuls les proxy sont autorisés à établir des connexions à direction d'Internet.
- Les fonctions de routage sont désactivées sur les proxy
- Translation dynamique d'adresses pour toutes les adresses internes
- Translation statique d'adresses en direction des proxies pour les protocoles autorisés à entrer
- Filtrage des connexions sortantes pour n'autoriser que les protocoles nécessaires en direction des proxies
- Filtrage des connexions entrantes pour interdire les connexions directes sur le pare-feu

Remarque : Applications

Niveau de sécurité requis : élevé

5. produit du marché

La figure suivante compare quelques produits du marché :

	Filtre hors contexte	Filtre contextuel	Proxy circuit	Proxy applicatif
Produit type	ACL Cisco	Pare-feu-1 (CheckPoint)	PIX (Cisco)	Gauntlet
Modèle d'implémentation	Automate sans mémoire secondaire	Automate à mémoire	Automate à mémoire	Automate à mémoire
NAT/PAT	Non	Oui	Oui	Oui
Performant	Oui	Oui	Oui	Non
Universalité	Elémentaire	Moyenne	Moyenne	Forte
Puissance d'expression	Couches 3, 4	Couches 3, 4	Couches 3, 4	Couche 7
Nombre de règles de filtrage	Faible	Important	Important	Faible

Produits du marché

G. Systèmes de Détection d'Intrusions (IDS)

Méthode

Un IDS analyse le trafic aux alentours du pare-feu en permanence et essaye de découvrir des attaques. Quand une attaque est découverte, l'IDS soit informe l'administrateur pour intervention manuelle sur le pare-feu, soit reconfigurer, automatiquement, le pare-feu pour mettre en place des filtres nécessaires pour bloquer l'attaque

Techniques de détection d'intrusions

Il existe deux grandes catégories d'IDS (ou techniques de détection d'intrusions) :

- Par signature d'attaque, par exemple:
  - Recevoir sur interface externe un paquet dont l'adresse IP est interne (IP Spoofing)
  - Tentatives de connexions sur plusieurs adresses (scan du réseau)

  Cette technique souffrent de plusieurs inconvénients :

  (-) Une base de données des signatures doit être mise à jour régulièrement

  (-) Détecter uniquement les attaques connues

  (-) Un attaquant peut contourner ces signatures
- Caractérisation du trafic en se basant sur des statistiques du trafic observé, si une valeur dépasse ses limites habituelles alors une attaque est suspectée. Des exemples de statistiques seraient la distribution du trafic en fonction des protocoles, adresses sources, adresses destinations, durée de connexions, bande passante, etc.

  cette technique souffre du grand nombre de faux positifs: à cause de la difficulté de caractériser un trafic normal

Définition : Network IDS

L'IDS est installé sur une station du réseau et écoute le trafic pour détecter les intrusions. Deux cartes réseau sont utilisées: une connectée à Internet pour espionner le trafic. Les alarmes sont envoyées sur un port du pare-feu au moyen de la seconde carte réseau, ce qui entraine, éventuellement une reconfiguration du pare-feu

Définition : Host IDS

Il s'agit d'un agent installé sur toutes les stations du réseau qui surveille constamment les fichiers de configuration, base de registres, paramètres du système pour détecter une anomalie. Il peut par exemple: détecter :

- qu'un utilisateur obtienne d'une façon soudaine des droits d'administrateur
- l'installation d'un logiciel ne correspondant pas aux logiciels habituellement installés sur le réseau

Snort

Snort est un IDS célèbre, dont les règles sont décrites dans un langage simple :

- l'en-tête de règle contient :
  - l'action de la règle (la réaction de snort);
  - le protocole qui est utilisé pour la transmission des données (snort en considère trois: TCP, UDP et ICMP);
  - les adresses IP source et destination et leur masque;
  - les ports source et destination sur lesquels il faudra vérifier les paquets.
- les options de la règle (entre parenthèse) qui contiennent

- le message d'alerte;
- les conditions qui déterminent l'envoi de l'alerte en fonction du paquet inspecté.

Exemple

L'exemple de règle suivant permet de détecter les tentatives de login sous l'utilisateur root, pour le protocole ftp (port 21) :

alert tcp any any -> 192.168.1.0/24 21 (content: "USER root"; nocase; msg: "Tentative d'accès au FTP pour l'utilisateur root";)

Série d'exercices sur les pare-feux, NAT, filtrage, proxy et IDS

II

A. Règles de filtrage d'un pare-feu sans mémoire

Avoine 2010

On considère un pare-feu sans mémoire dont le critère de filtrage repose sur les requêtes SYN (paquets dont le flag SYN est 1 et le flag ACK est 0). On souhaite que le serveur de messagerie (128.178.1.1) sur le réseau interne puisse recevoir et envoyer des messages de et vers Internet.

Question

Ecrire les règles de filtrage du pare-feu dans le tableau suivant :

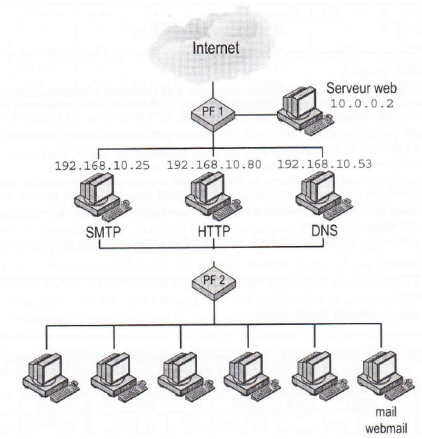
Source	Port	Destination	Port	Protocole	SYN	Action

Table règles Exo1

B. Règles de filtrage d'un pare-feu avec mémoire

Avoine 2010

On considère l'architecture décrite dans la figure suivante.



Architecture DMZ en Sandwitch

On suppose que l'adresse du serveur web est 10.0.0.2 et que les proxies SMTP, HTTP et DNS possèdent respectivement les adresses 192.168.10.25, 192.168.10.80, et 192.168.10.53.

Les trois proxies 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 proxies et par dmz.web toutes les adresses de la zone du serveur web

Question

Ecrire les règles de filtrage pour le pare-feu externe avec mémoire (PF1)

C. Peer-to-Peer

Avoine 2010

Pourquoi les systèmes d'échange de fichiers peer-to-peer (Napster, Gnutella, Kazaa) ne permettent pas d'échanger des fichiers entre deux utilisateurs pratiquant la translation dynamique d'adresses ?

D. Pool d'adresses

Avoine 2010

Une entreprise pratique la translation dynamique d'adresses avec un pool de trois 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, 192.168.10.3 et 192.168.10.4. Les quatre machine utilisent le port source 3001.

Question

Compléter la table de translation du pare-feu pendant la connexion (plusieurs solutions correctes sont possibles).

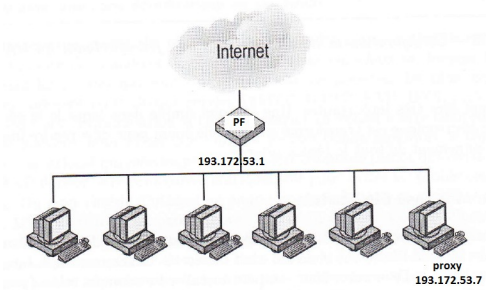
table de translation du pare-feu pendant la connexion							
interne				externe			
source	port	destination	port	source	port	destination	port

Table de translation

E. Contournement d'un proxy

Avoine 2010

On considère le réseau local 193.172.53.0 représenté sur la figure suivante :



Proxy mal placé

Les utilisateurs possèdent un compte (non privilégié) sur chacune des machines du réseau excepté sur la passerelle 193.172.53.1. L'administrateur installe un proxy HTTP sur l'une de ces machines (193.172.53.7) afin d'optimiser et de contrôler les accès aux sites web externes. Les navigateurs des utilisateurs sont paramétrés par défaut pour utiliser ce proxy.

Question 1

Comment les utilisateurs peuvent-ils simplement contourner le proxy ?

Afin de renforcer sa politique de sécurité, l'administrateur décide d'installer un pare-feu à mémoire au niveau de la passerelle. Il le configure de telle sorte à ce que seule la machine 193.172.53.7 puisse accéder à Internet, pour n'effectuer que des requêtes HTTP ou DNS.

Question 2

Ecrire la table de filtrage du pare-feu.

Question 3

Proposer une méthode qui permette aux utilisateurs de naviguer sur le Web sans utiliser le proxy.

F. IDS et proxy

Avoine 2010

Les logs d'un serveur web contiennent une série d'entrées du type suivant [adresse source, date, requête, résultat, octets transférés] :

```
128.178.146.216 - - [24/Sep/2003 :16 :50 :42+0200]"GET
/default.ida ?XXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XX%u9090%u6858%ucbd3%u7801%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u819
0%u00c3%u0003%u8b00%531b%53ff
%u0078%u0000%u00=a %HTTP/1.0" 404 209
```

Question 1

De quoi peut-il bien s'agir ?

Question 2

Comment faudrait-il configurer un système de détection d'intrusion (IDS) pour détecter et réagir à ces attaques ?

Question 3

En supposant que le serveur se trouve derrière un proxy inverse, comment le proxy pourrait-il aider à éviter ces attaques ?

Question 4

Laquelle de ces deux solutions, IDS ou proxy inverse, est-elle préférable ?