# Cours 3 : Firewall et DMZ

Rabii El Ghorfi

# Pourquoi un firewall?

## Definition

Programme, ou un matériel, chargé de vous protéger du monde extérieur en contrôlant tout ce qui passe, et surtout tout ce qui ne doit pas passer entre internet et le réseau local.

pourquoi un firewall?

**Contrôle.** Gérer les connexions sortantes a partir du réseau local.

**Sécurité.** Protéger le réseau interne des intrusions venant de l'extérieur.

**Vigilance.** Surveiller/tracer le trafic entre le réseau local et internet.

# Firewall


Plusieurs types de firewalls :

- Pare-feu au niveau réseau
- Pare-feu au niveau applicatif
- Pare-feu des applications

# Différents types de firewalls

Pare-feu niveau réseau. (iptables, paquet filter, . . . )

- ⋆ Firewall fonctionnant à un niveau bas de la pile TCP/IP
- ⋆ Basé sur le filtrage des paquets
- ⋆ Possibilité (si mécanisme disponible) de filtrer les paquets suivant l'état de la connexion

Intérêt : Transparence pour les utilisateurs du réseau

Pare-feu au niveau applicatif. (inetd, xinetd, . . . )

- ⋆ Firewall fonctionnant au niveau le plus haut de la pile TCP/IP
- ⋆ Généralement basé sur des mécanisme de proxy

Intérêt : Possibilité d'interpréter le contenu du trafic

Pare-feu des applications. (/etc/ftpaccess pour ftp, . . . )

- ⋆ Restrictions au niveau des différentes applications

# DMZ

## Definition (DMZ)

Une zone démilitarisée (DMZ) est un sous-réseau se trouvant entre le réseau local et le réseau extérieur.

Propriétés :

- Les connexions à la DMZ sont autorisées de n'importe où.
- Les connexions à partir de la DMZ ne sont autorisées que vers l'extérieur.

Intérêt :

- Rendre des machines accessible à partir de l'extérieur (possibilité de mettre en place des serveurs (DNS, SMTP, ...).

# Iptables et filtrage(1/2)

- Filtrage des paquets IP, TCP, UDP ou ICMP
- Spécification de règle pour le rejet ou l'acceptation de paquet
- Utilisation de la table FILTER et des chaînes INPUT, OUTPUT et FORWARD
- Règles traitées de manière séquentielle : Le paquet sort dès qu'il rencontre une règle qui peut lui être appliquée

Exemples :

- Accepter tous les paquets en provenance de n'importe où et destinés à l'adresse du routeur 192.168.1.1.

```
iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP
-j ACCEPT
```

- Accepter de router les paquets entrant sur eth0 tels que :

| @source | @dest | P-source | P-dest |
|---|---|---|---|
| 0/0 | 192.168.1.58 | 1024-65535 | 80 |

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o
eth1 -p TCP --sport 1024:65535 --dport 80 -j ACCEPT
```

# Iptables et filtrage(2/2)

- Accepter un paquet ICMP “echo-request” (ping) par seconde

```
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -i eth0 -j ACCEPT
```

- Accepter 5 segments TCP ayant le bit SYN positionné par seconde (permet d’éviter de se faire inonder)

```
iptables -A INPUT -p tcp --syn -m limit --limit 5/s -i eth0 -j ACCEPT
```

- Accepter de router les paquets entrants sur eth0 tels que :

| @source | @dest | P-source | P-dest |
|---|---|---|---|
| 0/0 | 192.168.1.58 | 1024-65535 | 80 ou 443 |

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP --sport 1024:65535 -m multiport --dport 80,443 -j ACCEPT
```

# Iptables et suivi des connexions

- Suivi des connexions disponible (*conntrack*)
- Quatre états possibles pour une connexion :

| | |
|---|---|
| NEW . | Nouvelle connexion établie |
| ESTABLISHED . | La connexion analysée est déjà établie |
| RELATED . | La connexion est en relation avec une connexion déjà établie (ftp-data par exemple) |
| INVALID . | Le paquet reçu n'appartient à aucune des trois catégories précédentes. |

Exemples :

- Autoriser tous les paquets émis par le routeur concernant des connexions déjà établies.

```
iptables -A OUTPUT -o eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

# Iptables et suivi des connexions

- Suivi des connexions disponible (*conntrack*)
- Quatre états possibles pour une connexion :

| | |
|---|---|
| NEW . | Nouvelle connexion établie |
| ESTABLISHED . | La connexion analysée est déjà établie |
| RELATED . | La connexion est en relation avec une connexion déjà établie (ftp-data par exemple) |
| INVALID . | Le paquet reçu n'appartient à aucune des trois catégories précédentes. |

Exemples :

- Autoriser le routeur à relayer tous les paquets reçus concernant de nouvelles connexions sur le port 22.

```
iptables -A FORWARD -p tcp -i eth0 --dport 22 --sport
1024:65535 -m state --state NEW -j ACCEPT
```

# Outils de diagnostic

**Traces iptables.** Possibilité de tracer certaines actions iptables.

exemple :

1. Tracer toutes les actions iptables :

```
iptables -A OUTPUT -j LOG
iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG
```

2. Rajouter une règle pour tracer les paquets rejetés

```
iptables -N LOG_DROP
iptables -A LOG_DROP -j LOG --log-prefix
'[IPTABLES DROP] : '
iptables -A LOG_DROP -j DROP
```

**nmap, nessus,....** Logiciels permettant de diagnostiquer l'état d'un firewall (trouver les ports ouverts, détecter les services utilisant les ports, ...)