Linux

Filtrage de paquets

Objectifs

Comprendre l'architecture de pare-feu sur GNU/Linux
Savoir créer ou peupler des tables avec des chaines et règles de filtrage
Savoir gérer ces règles (lister, numéroter, supprimer)
Filtrer les paquets en utilisant Iptables, NFTables
Filtrer les protocoles les plus courants (HTTPs, ICMP...)

SCALAR

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Filtrer des paquets sous Linux ?

LE CONCEPT DE PARE-FEU

- Un **pare-feu** permet de **filtrer le trafic entrant et/ou sortant**
  - Selon **des ports**
  - Selon **des protocoles applicatifs**
- Il existe des distributions Linux et BSD uniquement dédiées à ce rôle
  - **IPCop**
  - **NetBSD**

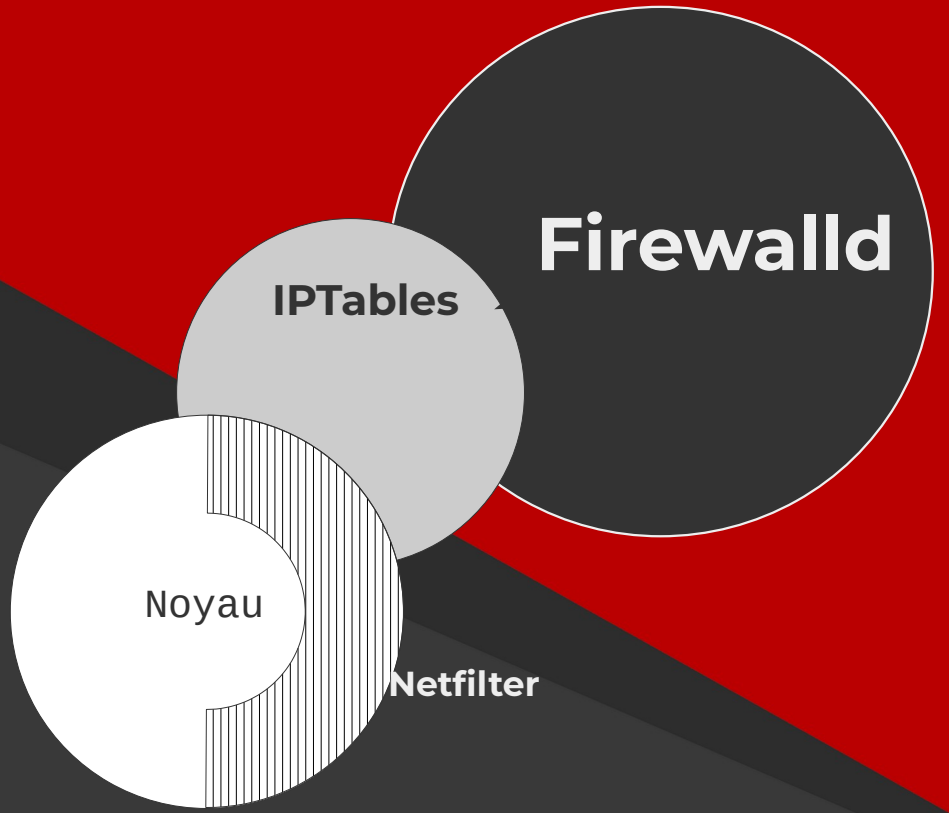
SCALAR

RAPPEL !

`Netfilter` est un composant du noyau

Il ne peut être piloté que par **`IPtables` ou `NFTables`**

`Firewalld` ou `UFW` sont des sur-couches qui viennent simplifier IPtables



plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Filtrer avec IPtables ?

IPTABLES

- Utilise un système de **tables de filtrages**
  - Elles mêmes **utilisant des chaînes**
  - **Qui vont filtrer tout ou partie des interfaces**
  - Via une **succession de règles**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

IPTABLES : LES TABLES

- **Filter**
- **NAT**
- **Mangle**
- **Raw**
- **Security**

En rouge, les tables les plus couramment utilisées

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

IPTABLES : LES CHAÎNES

Marquent une étape **de circulation des paquets** **dans une machine :**

- **INPUT** - **Entrée**, destinée à la machine locale
- **OUTPUT** - **Sortie**, émis par la machine locale
- **FORWARD** - **Traverser**, transitent par la machine

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

IPTABLES : LES PARAMÈTRES

Définissent **une action IPTables à effectuer** dans une machine :

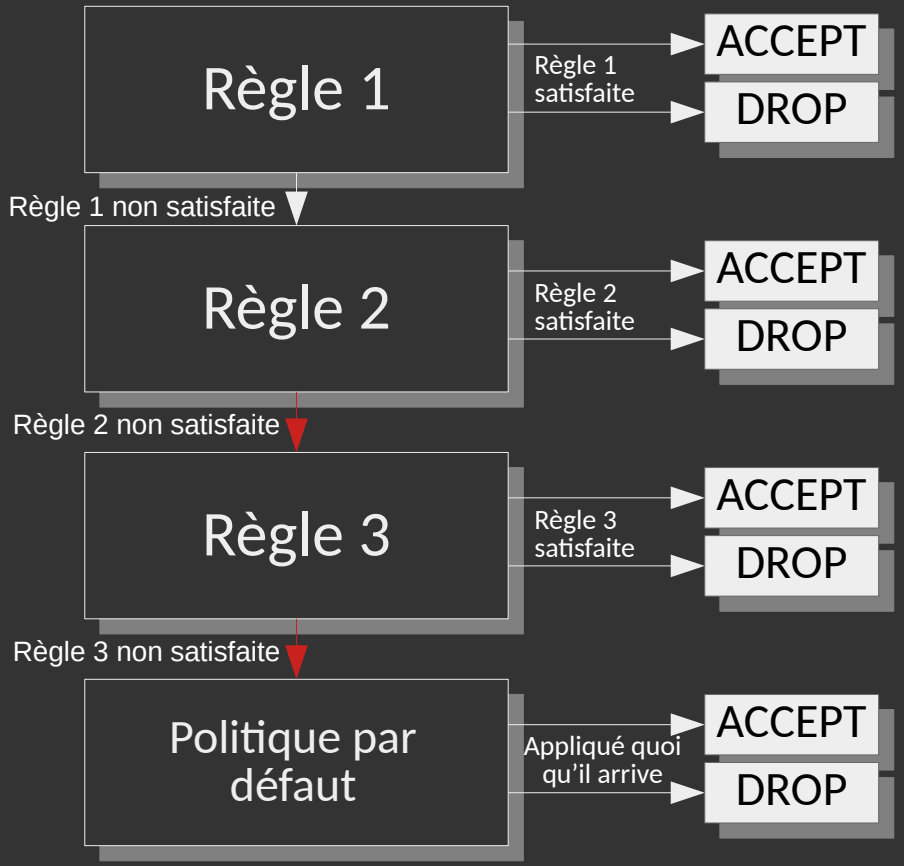
- **-A** *Append* : **modifie une chaîne, ajouté à la fin de celle-ci**
- **-I** *Insert* : **insère une règle en début de chaîne**
- **-D** *Delete* : permet de **supprimer une règle**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

IPTABLES : LES ACTIONS

- Une fois notre paquet testé**, l'action** à entreprendre **sera appelée par «** `-j` **» et sera :**
  - **ACCEPT**
  - **DROP**

Traitement des règles de filtrage



Consulter les règles IPtables

- Pour **consulter les règles actives d'une table :**

```
# iptables -L -t NOM_TABLE
```

- Pour **retrouver les commandes ayant écrites ces règles :**

```
# iptables -S -t NOM_TABLE
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Politique de filtrage sur IPtables ?

Politique de filtrage

- **2 modes** principaux :
  - **Tout ce qui n'est pas interdit est autorisé**
  - **Tout ce qui n'est pas explicitement autorisé est interdit !**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

POLITIQUE DE FILTRAGE

Cette politique définit le comportement par défaut lorsque le paquet à été testé et ne concorde à aucune règle de filtrage

```
# iptables -P chaîne action
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Règles IPTables

- **Syntaxe** d'une règle :

```
# iptables -A chaîne -s ip_source -d ip_dest
-p protocole --dport port -j action
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Pensez aux
FLUX RETOURS !

Une communication est à double sens, or, certains retours se font souvent sur un port aléatoire quand on est à l'origine de la communication

Alors comment faire pour filtrer des paquets arrivant sur un port aléatoire ?

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Les Flux Retours

Les pare-feu modernes détectent ces flux retours

Du moment qu'ils correspondent à une sortie autorisée

```
# iptables -A chaîne -m state --state
ESTABLISHED,RELATED -j action
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

ATTENTION !

Un mauvais ordre ou une mauvaise règle peut avoir des conséquences dramatiques !

La commande «nmap -F » depuis une machine distante, suivie de l'IP de notre machine, nous permettra de savoir rapidement si nos ports sont bloqués ou non

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Comment GÉRER les RÈGLES ?

Gérer les règles

- Elles sont **numérotées dans l'ordre de leur création**
- **Ce numéro est nécessaire pour demander leur suppression,** pour l'obtenir :

```
# iptables -L chaine --line-numbers -n
```

Pour supprimer :

```
# iptables -D chaine numéro
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

GÉRER LES RÈGLES

Pour effacer la configuration d'IPtables, ou « **flusher** » :

```
# iptables -F
```

Sauvegarder les règles Iptables **sur RHEL/CentOS :**

```
# iptables-save > /etc/sysconfig/iptables.rules
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Gérer les règles

Demander à IPTables de **prendre en compte les nouvelles règles :**

```
# iptables-restore
```

Au démarrage, le système effectue cette commande pour être sûr de bien appliquer vos règles de filtrage définies avant l'extinction

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Filtrer grâce à...

NFTABLES?

NFTABLES :

- Iptables était l'interface de gestion traditionnelle du pare-feu
- Elle est **remplacée par `NFtables`**
  - **Beaucoup plus performant**
  - Code plus propre
  - **Gère plusieurs réseaux dans une seule règle**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

NFTABLES :

- **Les règles sont appliquées de manière atomiques, plutôt que d'aller cherche un jeu de règles complet**
- **Fournis une API `Netlink` pour les applications tierces**
- Remplace certaine parties de l'infrastructure noyau « Nelfilter »
- **Plus de débit**

SCALAR

NFTABLES :

- **Réunis en un composant unique les protocoles IPv4 et IPv6**
- **Nftables remplace les utilitaires suivants**
  - `Iptables/Iptables6`
  - `arptables`
  - `ebtables`

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Super, on s'en sert comment ?

Un peu de VOCABULAIRE tout d'abord

Utilisation NFTables

SCALAR

Chaine va **CONTENIR** les règles de filtrage

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Utilisation NFTables

Vérifiez la liste des tables :

```
sudo nft list tables
```

I.Créer une table :

```
sudo nft add table ip NOM
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Utilisation NFTables

Supprimer une table :

```
sudo nft delete table ip NOM
```

***Ne fonctionnera PAS si la table n'est pas vide…**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Utilisation NFTables

Il faut donc **flusher la table**, puis supprimer !

```
sudo nft flush table ip NOM
sudo nft delete table ip NOM
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Utilisation NFTables

2.Créer une chaîne :

```
nft ‘add chain ip NOM_TABLE NOM_CHAINE
{ type filter hook input priority 0;}’
```

*** : Il est important ici de choisir le bon « hook » !**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Utilisation NFTables

3. Ajouter une règle de filtrage :

sudo **nft 'add rule TABLE CHAINE PROTOCOLE DPORT|SPORT accept|drop'**

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Euhh.. un..

EXEMPLE?

ACCEPTER LE TRAFIC HTTP

```
nft add rule ma_table_IPv4 ma_chaine_entrée tcp dport 80 accept
nft add rule ma_table_IPv4 ma_chaine_sortie tcp sport 80 accept
nft add rule ma_table_IPv4 ma_chaine_entrée drop
nft add rule ma_table_IPv4 ma_chaine_sortie drop
```

N'oubliez pas que l'ordre des règles à une importance, il faut donc mettre les règles les plus restrictives en dernier !

plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Insérer une RÈGLE

```
#après une règle précise (handle) exemple : après la 4
nft add rule ma_table ma_chaine position 4 tcp dport 80 accept
#avant une règle précise :
nft insert rule ma_table ma_chaine position 4 tcp dport 80 accept
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

SUPPRIMER UNE RÈGLE

```
#on doit d'abord trouver son identifiant (handle)
nft -a list table ip ma_table
#Supprimer la règle une fois son handle obtenu :
nft delete rule ma_table ma_chaine handle 4
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Pensez aux FLUX RETOURS !

LES FLUX RETOURS, MAIS AVEC NFT

On parle ici de « `connexion tracking` »

Du moment qu'ils correspondent à une sortie autorisée

```
# nft add rule NOM_TABLE NOM_CHAINE
ct state established, related, ACTION
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Et BANNIR une IP?

Bannissement d'IP

```
nft add rule ma_table ma_chaine ip saddr @IP accept|drop
nft add rule ma_table ma_chaine ip daddr @IP accept|drop
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Et BLOQUER le PING ?

Bloquer le Ping

```
nft add rule ma_table ma_chaine_sortie icmp type echo-request accept
nft add rule ma_table ma_chaine_sortie drop
nft add rule ma_table ma_chaine_entrée icmp type echo-reply accept
nft add rule ma_table ma_chaine_entrée drop
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25

Et sauvegarder mes règles NFT ?

GÉRER LES RÈGLES

Pour **sauvegarder les règles** NFTables :

```
# nft -s list ruleset >> /home/user/save
```


plus d'info sur www.linkedin.com/in/surquincedric
csurquin.pro@pm.me 07.82.69.95.25