

Services, journalisation et pare-feu

420-2S5-EM Serveurs 1:
Services intranet

H25 – Rencontre 6

Contenu du cours

- C'est quoi un **service** ?
- Gestion des services sous Linux (Démarrage, Arrêt, etc...)
- Débogage et **journalisation**
- Le **pare-feu**, qu'est-ce que c'est exactement ?
- Présentation du **pare-feu d'Ubuntu** serveur

C'est quoi un service ?

Un **service** est un programme qui roule **en arrière-plan**. Ce type de programme n'a généralement **pas été écrit pour favoriser l'interaction humaine**.

Parmi les différents services, on retrouve certains éléments clés du système.

On les appelle parfois **daemons** (origine grecque: daimon « divinité »). Par convention, leur nom se termine souvent par un **d**.

Exemples: sshd, httpd, etc.

Gestion des **services** sous Ubuntu

> Démarrer un service présentement arrêté

```
 sudo systemctl start [nom du service]
```


> Arrêter un service en cours d'exécution

```
 sudo systemctl stop [nom du service]
```

> Consulter l'état d'un service

```
 sudo systemctl status [nom du service]
```

> Activer l'exécution automatique d'un service au démarrage

```
 sudo systemctl enable [nom du service]
```

> Désactiver l'exécution automatique d'un service au démarrage

```
 sudo systemctl disable [nom du service]
```

La **journalisation** sous Ubuntu

Jusqu'à récemment, il n'y avait pas de système de centralisation des journaux et des logs sous Ubuntu. Aujourd'hui, nous avons **journald**, un service de traitement et de centralisation des journaux.

> Afficher tous les journaux, page par page

```
 sudo journalctl
```

> Afficher tous les journaux d'un service en particulier

```
 sudo journalctl -u [nom du service]
```

> Afficher tous les journaux d'un service en particulier, d'aujourd'hui.

```
 sudo journalctl -u [nom du service] --since today
```

> Afficher tous les journaux d'un service en particulier, entre deux dates.

```
 sudo journalctl -u [nom du service] --since 2023-12-31 --until 2024-01-01
```

La **journalisation** sous Ubuntu

Plusieurs systèmes utilisent encore la vieille méthode. C'est-à-dire **qu'ils stockent encore les journaux dans des fichiers de texte brute**.

L'inconvénient, c'est qu'il est **plus difficile de les filtrer** et de les lier les uns aux autres.

Les fichiers « logs » sont généralement stockés dans « **/var/log** ».

Les commandes « **head** », « **tail** », « **less** » et « **grep** » vous seront utiles pour filtrer les fichiers.

Quand aller voir les journaux ?

- Lorsqu'un service ou un programme est en difficulté.
- Lorsque je désire surveiller les performances d'un service ou d'un programme.
- Lorsque je veux faire des audits de sécurité.
- Lorsque je fais du débogage.

Pare-feu sous Ubuntu 🔥 🧱

Pour bien comprendre ce qu'est qu'un **pare-feu**, il faut d'abord saisir la notion de **port**.



Pare-feu sous Ubuntu 🔥 🧱

Jouons avec la sémantique un peu. Au lieu de parler de **ports**, appelons cela des **portes**.

Chacune d'entre elle mène à votre ordinateur.



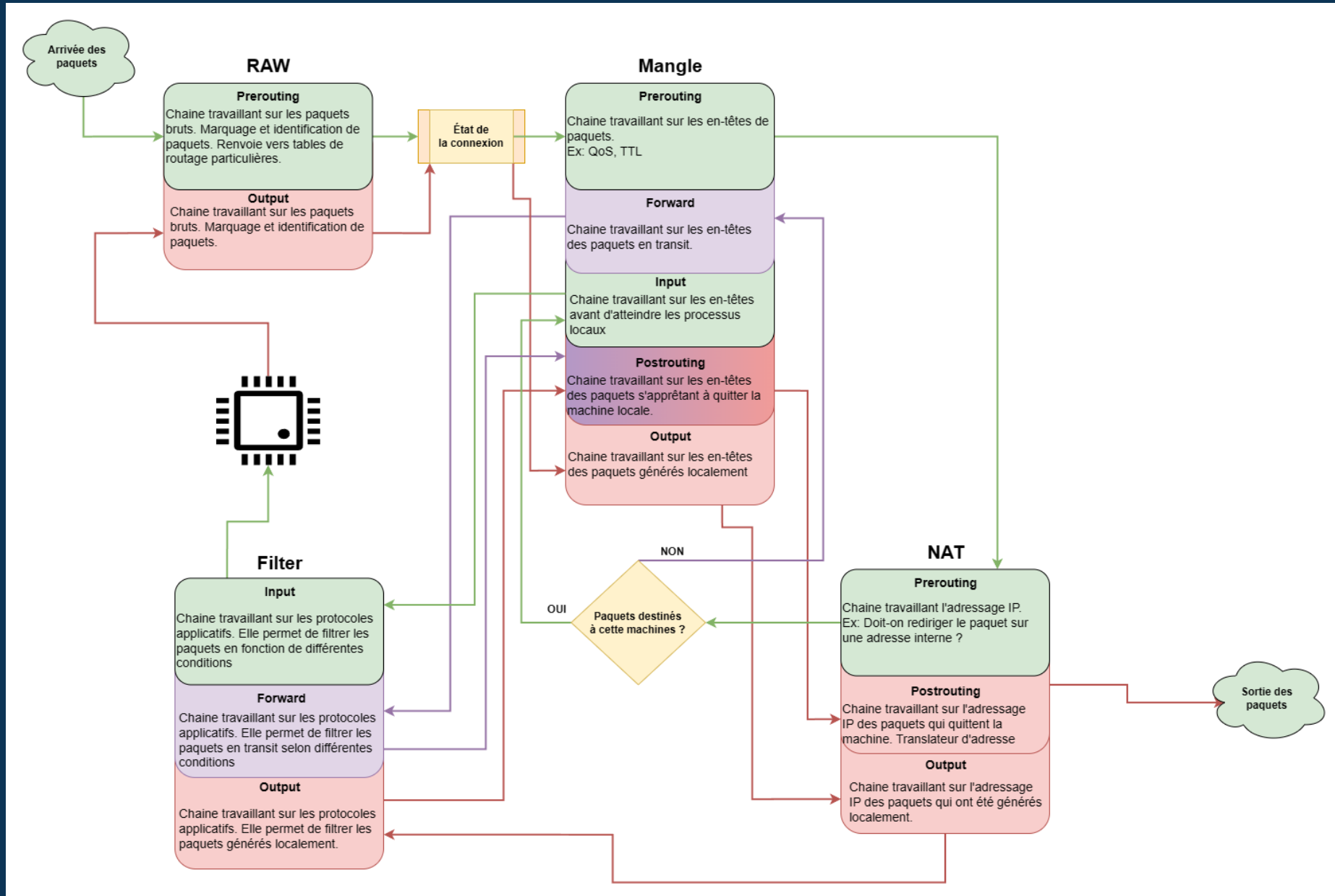
Pare-feu sous Ubuntu

- Il existe 65 535 portes (ports) distinctes menant à votre ordinateur.
- Le travail du pare-feu est comparable à celui d'un portier. Il surveille chaque porte. Selon ce qu'on lui indiquera, il peut:
 - Vous laissez passer (dans une direction, dans l'autre ou même les deux).
 - Vous refuser le passage.

Pare-feu sous Ubuntu

| | UFW (Uncomplicated Firewall) | Iptables |
|-------------------|--|---|
| Complexité | Conçu pour être convivial et facile d'utilisation. | Iptables est plus puissant mais plus complexe également. |
| Syntaxe | Syntaxe simple et intuitive | Syntaxe plus détaillée nécessitant parfois plusieurs lignes pour un service. |
| Persistance | Gérer automatiquement | Sauvegarde doit être fait manuellement. |
| Abstraction | Crée une abstraction des tables pour l'utilisateur. | Contrôle détaillé de chaque table, permettant des configurations plus avancées. |
| Préconfigurations | La version « desktop » vient avec des règles préconfigurées. | Aucune préconfiguration, laissant toute la responsabilité à l'utilisateur. |

Schéma d'Iptables



Quelques exemples UFW

> Activer le pare-feu UFW (Désactivé par défaut)

```
 sudo ufw enable
```

> Désactiver le pare-feu UFW

```
 sudo ufw disable
```

> Lister les règles du pare-feu

```
 sudo ufw status
```

> Autoriser le trafic entrant sur le port 22 (ssh)

```
 sudo ufw allow 22
```

> Autoriser le trafic entrant sur le port 8080 depuis n'importe quelle adresse dans le sous-réseau 192.168.1.0/24

```
 sudo ufw allow from 192.168.1.0/24 to any port 8080
```