
B2 - LINUX

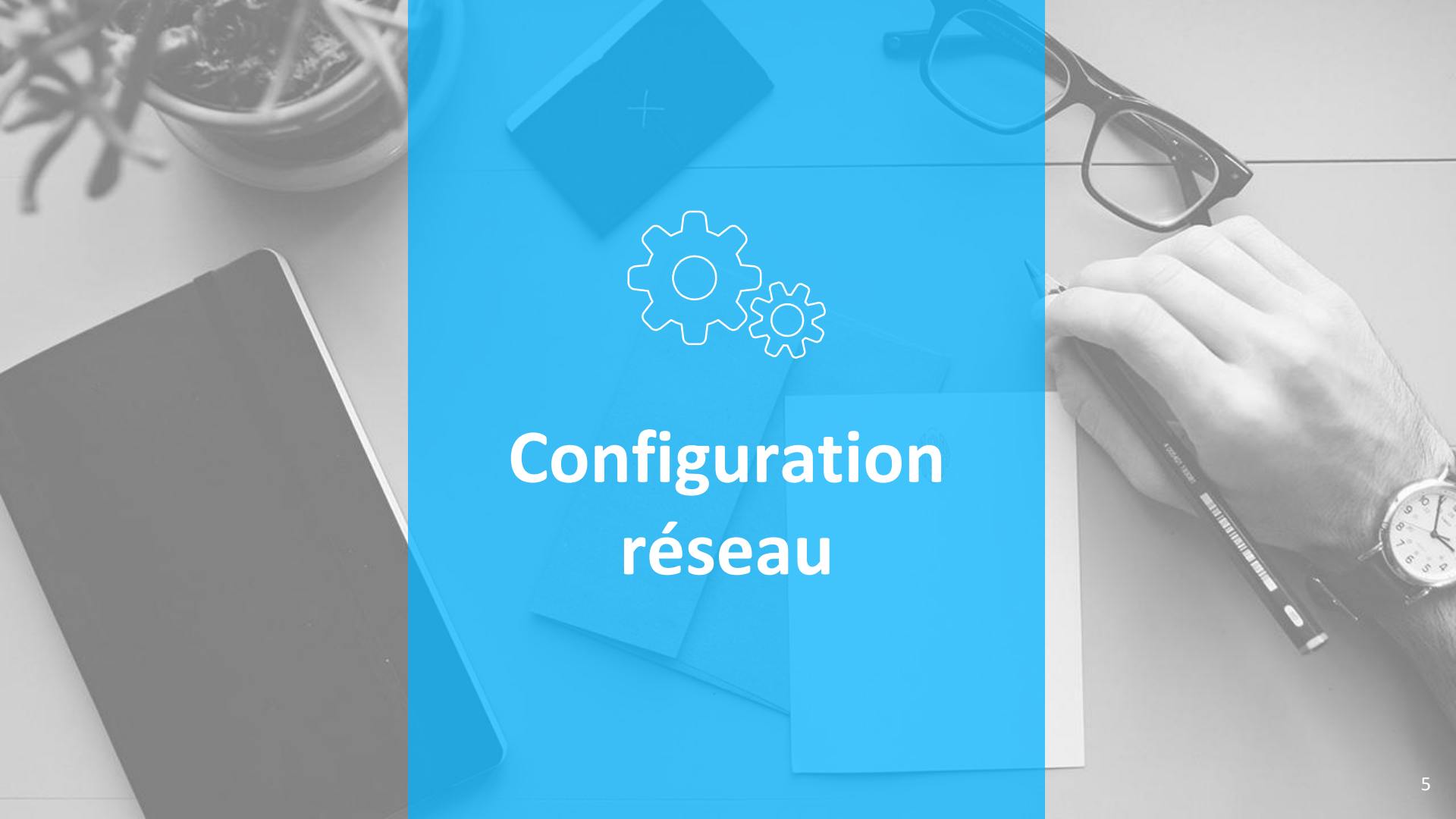
Sommaire

- → Network
- → Sécurité
- → TP

NETWORK

Commandes Utiles

- → Nslookup
- → Ip a
- → Ping
- → Traceroute
- → Tcpdump
- → Lsof
- → Curl



Configuration réseau

Configuration

→ Debian : /etc/network/interfaces/

→ Centos : /etc/sysconfig/network-scripts/ifcfg-$NETDEV

Configuration

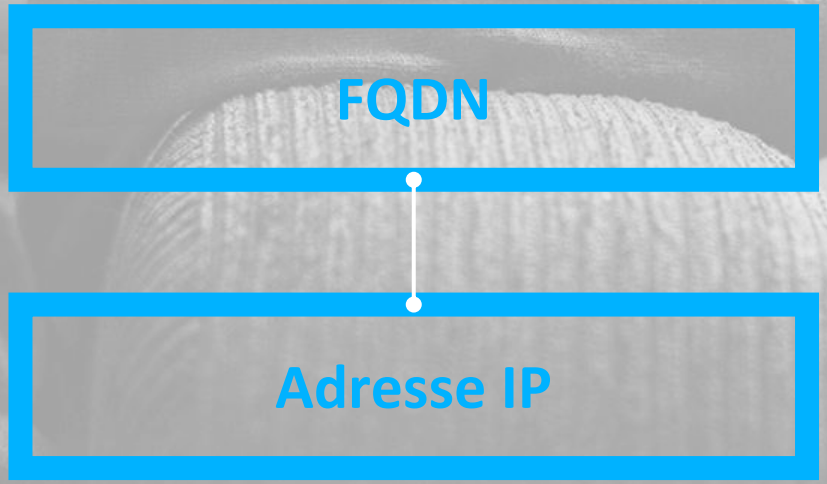
→ DHCP

```
auto eth0
allow-hotplug eth0
iface eth0 inet dhcp
```

→ Static

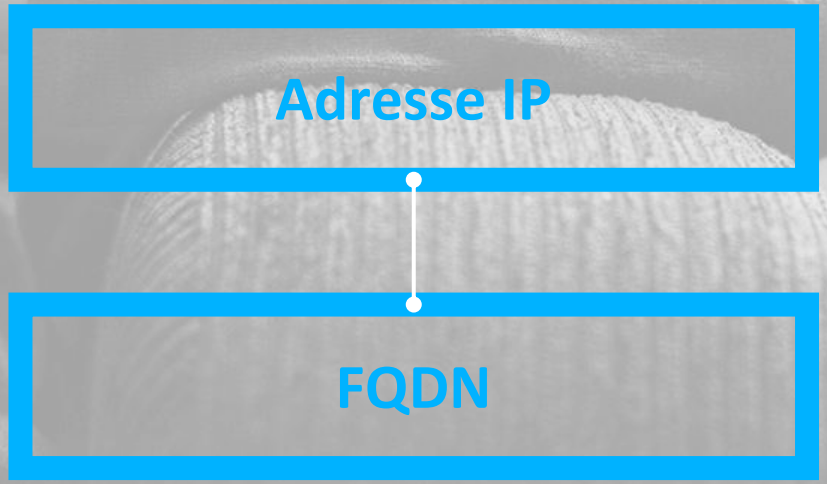
```
auto eth0
iface eth0 inet static
    address 192.0.2.7/24
    gateway 192.0.2.254
```

/etc/resolv.conf




```
nameserver 208.164.186.1
nameserver 208.164.186.2
```

/etc/hosts




```
192.168.105.2 sasa
```

Sécurité

Configuration

La sécurité physique

- ➜ par la limitation de l'accès au matériel (zones réservées, restrictions…)
- ➜ par la sécurisation physique du matériel (antivols, armoires fortes…)
- ➜ par la sécurisation virtuelle du matériel, des données et informations (lecteurs biométriques, disques chiffrés…)
- ➜ par la sécurisation des réseaux et des communications (formats de transfert chiffré : SSH…)
- ➜ par la formation du personnel aux risques.

La sécurité logicielle

- → Limiter les droits d'accès aux fichiers
- → Chiffrer des communications (GnuPG)
- → Chiffrer des dossiers
- → Limiter les tentatives de connexions
- → Mise à jour régulière

Permissions

- Les droits des fichiers d'un répertoire peuvent être affichés par la commande « ls –l »
- Les droits d'accès apparaissent alors comme une liste de 10 symboles. :

```
drwxr-xr-x
```

- Le premier symbole peut être « - », « d », soit « l » :
  - **« - »** : fichier classique
  - **« d »** : répertoire
  - **« l »** : lien symbolique

Permissions

```
drwxr-xr-x
```

- **d** : c'est un répertoire.
- **rwx** pour le 1er groupe de 3 symboles : son propriétaire peut lire, écrire et exécuter.
- **r-x** pour le 2e groupe de 3 symboles : le groupe peut uniquement lire et exécuter le fichier, sans pouvoir le modifier.
- **r-x** pour le 3ème groupe de 3 symboles : le reste du monde peut uniquement lire et exécuter le fichier, sans pouvoir le modifier.

Permissions

- 0 : `- - -` (aucun droit)
- 1 : `- - x` (exécution)
- 2 : `- w -` (écriture)
- 3 : `- w x` (écriture et exécution)
- 4 : `r - -` (lecture seule)
- 5 : `r - x` (lecture et exécution)
- 6 : `r w -` (lecture et écriture)
- 7 : `r w x` (lecture, écriture et exécution)

Permissions

- → À qui s'applique le changement
  - u (user, utilisateur) représente la catégorie "propriétaire"
  - g (group, groupe) représente la catégorie "groupe propriétaire"
  - o (others, autres) représente la catégorie "reste du monde"
  - a (all, tous) représente l'ensemble des trois catégories.

Permissions

- La modification que l'on veut faire
  - + : ajouter
  - - : supprimer
  - = : affectation
- Le droit que l'on veut modifier
  - r : read ⇒ lecture
  - w : write ⇒ écriture
  - x : execute ⇒ exécution
  - X : eXecute ⇒ exécution, concerne uniquement les répertoires

TP

- Configurer IP static
- Contacter un PC distant avec un FQDN
- Chiffrer fichier
- Limiter droits d’accès à des utilisateurs
- Installer et configurer Fail2Ban

Merci!

Des questions ?