Université Mohammed Premier Oujda
École Nationale des Sciences Appliquées
Département : Électronique, Télécommunications et Informatique
Filière : GI/GSEIR / Niveau : GI5/GSEIR5
Module : sécurité des réseaux

TP6 Security :

Filtrage par iptables

Enseignant : Mohammed SABER

Année Universitaire : 2017/2018

Objectifs pédagogiques de TP :

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

Partie 1 : Configuration des périphériques et vérification de la connectivité de la topologie

- Configurez l'équipement pour qu'il corresponde à la topologie du réseau.
- Attribuez une adresse IP statique aux PC.
- Vérifiez la connectivité entre les périphériques par les `ping`.

Partie 2 : Filtrage avancé par iptables

- Configurez, appliquez et vérifiez des opérations des filtrages simple par `iptables` sur la table **Filter**.

Remarque : Assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre enseignant.

Ressources requises

Ressources nécessaires :

1. Trois ordinateurs Linux Debian 7 (mot de passe : **ensao (ATTENTION : NE MODIFIER PAS LE MOT DE PASSE)**) ;
2. Cinq câbles Ethernet directs (2 de couleur rouge, 2 de couleur verte, 1 de couleur blanche) ;
3. Accès à l'invite de commandes des hôtes PC1, PC2 et PC3 ;
4. Accès à la configuration TCP/IP du réseau des hôtes PC1, PC2 et PC3.
5. Deux commutateurs (Switch) ;

Consignes pour le TP

1. Suivez les instructions pour chaque étape.
2. Ne déplacez pas le matériel.
3. **N'utilisez pas les Clés USB sur les machines**.
4. A la fin de TP, SVP réorganiser votre table :
   - Éteindre toutes les machines.
   - Réorganiser les chaises à ces places avant de sortir.
   - MERCI d'avance.
5. Un rapport de TP individuel est rendu sur la plateforme Moodle à la fin de TP (en format PDF ou DOC).
6. **Chaque étudiant ne respect pas les consignes de TP sera sanctionné.**

Commandes utiles pour ces travaux pratiques

Configuration des adresses IP des interfaces par la commande ifconfig

- Chaque interface est identifiée par un nom :
  - **ethX :** première carte réseau de type Ethernet, avec **X** le numéro de l'interface ($0 \leqslant X \leqslant N$).
  - **lo :** loopback ou interface de bouclage.
- Liste des interfaces réseau configurées : `ifconfig`.
- Pour configurer une interface réseau : `ifconfig interface AdresseIP netmask MasqueRéseau up/down`

Configuration de la table de routage : la commande route

- Pour afficher la table de routage : `route -n`
- Pour ajouter une entrée de réseau à la table de routage : `route add -net AdresseRéseau(A.B.C.D) netmask MasqueRéseau(A.B.C.D) gw AdressePasserelle(A.B.C.D)`
- Pour supprimer une entrée de réseau dans la table de routage : `route del -net AdresseRéseau(A.B.C.D) netmask MasqueRéseau(A.B.C.D) gw AdressePasserelle(A.B.C.D)`
- Pour ajouter une route (un routeur) par défaut à la table de routage : `route add default gw AdressePasserelle(A.B.C.D)` Pour ajouter la route par défaut à la table de routage : `route add default`

Tester la connectivité la commande ping

La commande ping permet de vérifier l'accessibilité de l'hôte ou de la passerelle (gateway) dont le nom ou l'adresse IP est spécifié en argument.

La commande (`ping AdresseIP`) permet donc :

- Tester la connectivité du système local ;
- Identifier les couches d'où provient le problème ;
- Tests supplémentaires à réaliser pour en déterminer la cause et ainsi compléter le diagnostic.

Adresse MAC et Adresse IP

- En TCP/IP, chaque machine du réseau est identifiée par une adresse codée sur 32 bits (4 octets), son adresse IP.
- Chaque carte réseau dispose d'une adresse codée sur 48 bits (6 octets), son adresse MAC.

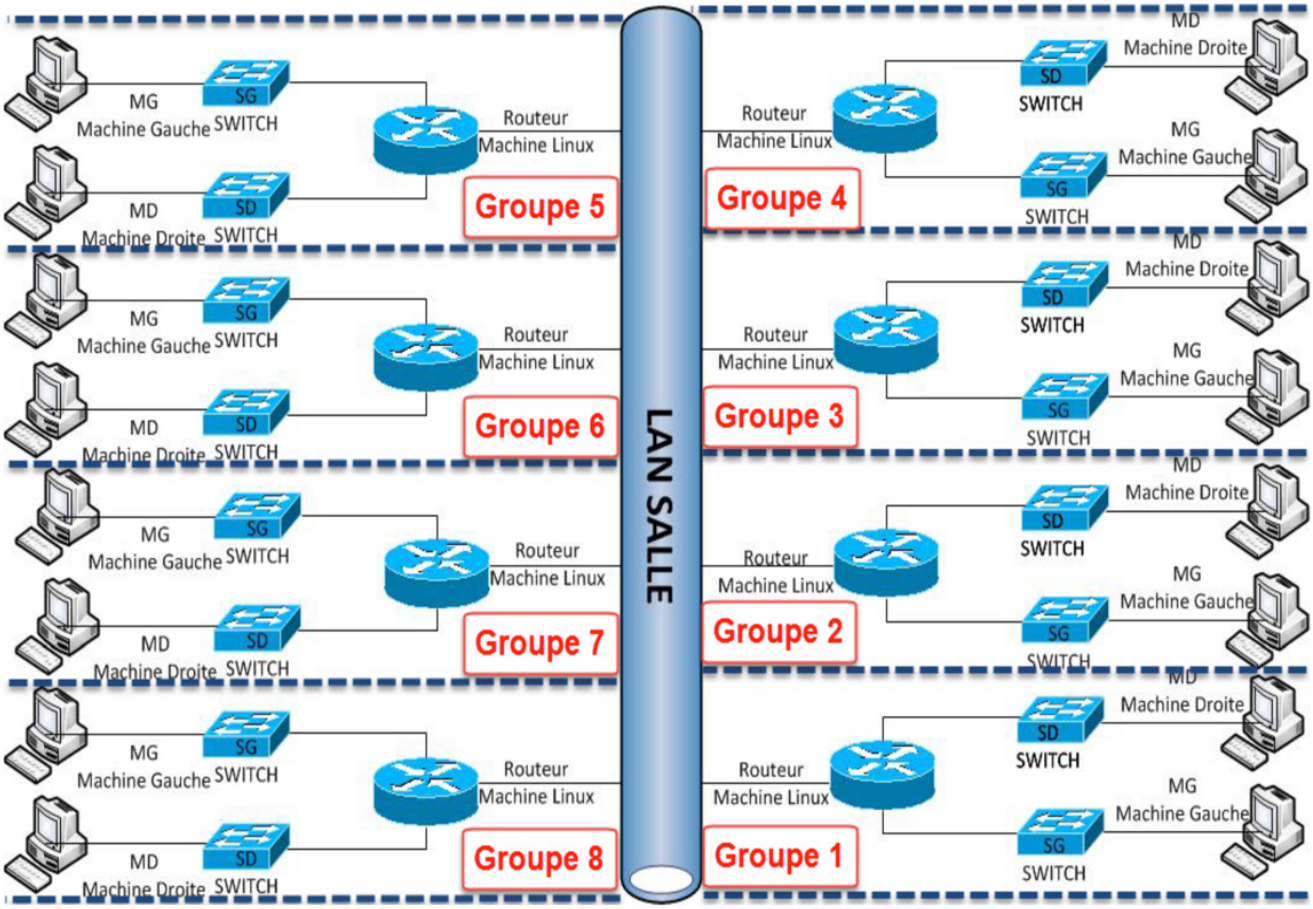
Les machines utilisent leurs adresses IP pour communiquer entre elles, mais au niveau du réseau physique sous-jacent (dans notre cas ETHERNET), c'est l'adresse MAC qui est utilisée dans les trames échangées.

PARTIE 1 : Configuration des périphériques et vérification de la connectivité de la topologie

Atelier du réseau pour ces travaux pratiques

Atelier de TP

L'architecture de l'atelier est la suivante :



Plan d'adressage de l'atelier de TP

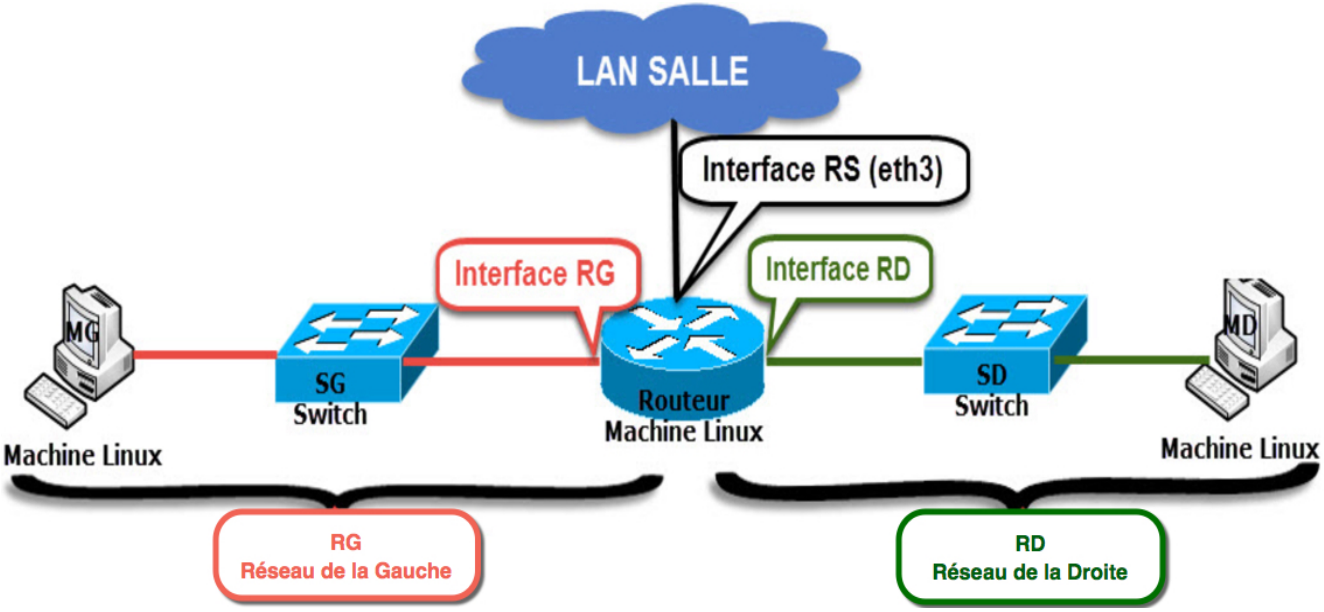
Le plan d'adressage des groupes pour ces travaux pratiques sont présentées sur le tableau suivant :

Groupe	Réseau Gauche	Réseau Droite	Réseau Salle
GR1	192.168.1.0/24	172.21.0.0/16	10.3.20.0/23
GR2	192.168.2.0/24	172.22.0.0/16	10.3.20.0/23
GR3	192.168.3.0/24	172.23.0.0/16	10.3.20.0/23
GR4	192.168.4.0/24	172.24.0.0/16	10.3.20.0/23
GR5	192.168.5.0/24	172.25.0.0/16	10.3.20.0/23
GR6	192.168.6.0/24	172.26.0.0/16	10.3.20.0/23
GR7	192.168.7.0/24	172.27.0.0/16	10.3.20.0/23
GR8	192.168.8.0/24	172.28.0.0/16	10.3.20.0/23

Étape 1 : Câblage des équipements réseau de l'atelier groupe

Tâche 1 : Connexion des périphériques réseau de l'atelier groupe

L'architecture de l'atelier réseau de chaque groupe est la suivante :



Suivez les instructions suivantes pour connecter les périphériques :

- **Câblage du réseau gauche** :
  1. À l'aide d'un câble droit Ethernet (**câble verte**), connectez la machine gauche **MG** au port de switch **SWG**.
  2. À l'aide d'un câble droit Ethernet (**câble verte**), connectez l'interface de type Ethernet **RG** du routeur au port de switch **SWG**.
- **Câblage du réseau droite** :
  1. À l'aide d'un câble droit Ethernet (**câble rouge**), connectez la machine droite **MD** au port de switch **SWD**.
  2. À l'aide d'un câble droit Ethernet (**câble rouge**), connectez l'interface de type Ethernet **RD** du routeur au port de switch **SWD**.

- **Câblage du réseau vers le réseau de la salle** :
  1. À l'aide d'un câble droit Ethernet (**câble blanc**), connectez l'interface de type Ethernet **Rs** du routeur au **port (prise) de la goulotte**.

Tâche 2 : Démarrage des machines réseau de l'atelier groupe

Démarrer les trois machines, avec les informations suivantes :
- **Compte administrateur** : login (**root**), mot de passe (**ensao**).
- **Compte utilisateur** : login (**ensao**), mot de passe (**ensao**).
- **ATTENTION ! ! ! ! : NE CHANGER PAS LES MOTS DE PASSE**.

Étape 2 : Configuration des équipements réseau de l'atelier groupe

Soit le plan d'adressage détaillé suivant :

Groupe	Périphérique	Adresse IP	Masque sous-réseau	Passerelle	Interface
GR1	**Host MD**	172.21.0.2	255.255.0.0	172.21.0.1	eth0
	Interface RD	172.21.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.1.2	255.255.255.0	192.168.1.1	eth0
	Interface RG	192.168.1.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR2	**Host MD**	172.22.0.2	255.255.0.0	172.22.0.1	eth0
	Interface RD	172.22.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.2.2	255.255.255.0	192.168.2.1	eth0
	Interface RG	192.168.2.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR3	**Host MD**	172.23.0.2	255.255.0.0	172.23.0.1	eth0
	Interface RD	172.23.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.3.2	255.255.255.0	192.168.3.1	eth0
	Interface RG	192.168.3.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR4	**Host MD**	172.24.0.2	255.255.0.0	172.24.0.1	eth0
	Interface RD	172.24.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.4.2	255.255.255.0	192.168.4.1	eth0
	Interface RG	192.168.4.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3

GR5	**Host MD**	172.25.0.2	255.255.0.0	172.25.0.1	eth0
	Interface RD	172.25.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.5.2	255.255.255.0	192.168.5.1	eth0
	Interface RG	192.168.5.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR6	**Host MD**	172.26.0.2	255.255.0.0	172.26.0.1	eth0
	Interface RD	172.26.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.6.2	255.255.255.0	192.168.6.1	eth0
	Interface RG	192.168.6.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR7	**Host MD**	172.27.0.2	255.255.0.0	172.27.0.1	eth0
	Interface RD	172.27.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.7.2	255.255.255.0	192.168.7.1	eth0
	Interface RG	192.168.7.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR8	**Host MD**	172.28.0.2	255.255.0.0	172.28.0.1	eth0
	Interface RD	172.28.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.8.2	255.255.255.0	192.168.8.1	eth0
	Interface RG	192.168.8.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3

Tâche 1 : Configuration des équipements réseau gauche de l'atelier groupe

1. Configurez l'interface Ethernet **eth0** de la machine **MG** avec l'adresse IP statique à l'aide des paramètres de votre groupe du tableau précédent. (**utilisation de la commande** `ifconfig`).
2. Pour éviter le problème de désactivation de l'interface. Créez un script pour la configuration de l'interface Ethernet **eth0** de la machine **MG**. Pour cela :
   (a) Créez un script "**Confmg**" suivant :

```
--------------------------------------------------------------------------
#!/bin/bash
while true
do
# Commande de configuration de votre interface eth0 de la machine gauche:
# Sachant que x est le numéro de votre groupe
ifconfig eth0 192.168.x.2 netmask 255.255.255.0 up
sleep 1
done
--------------------------------------------------------------------------
```

(b) Modifier le droit d'exécution de "**Confmg**" par la commande suivante : `chmod 777 confmg`.

(c) Lancer le "**Confmg**" par la commande suivante : `./confmg &`.

3. Affichez la table de routage de la machine. `route -n`).
4. Ajoutez la route par défaut pour la machine **MG** avec l'adresse IP passerelle indiqué dans le tableau précédent. (**utilisation de la commande** `route add default gw 192.168.x.1`).
5. Affichez la table de routage de la machine. `route -n`).
6. Configurez l'interface Ethernet gauche du routeur **RG** avec l'adresse IP statique à l'aide des paramètres du tableau précédent. (**utilisation de la commande** `ifconfig`).

(a) Créez un script "**Confmr**" suivant :

```
-------------------------------------------------------------------------
#!/bin/bash
while true
do
# Commande de configuration de votre interface eth0/eth1 de la machine gauche:
# Sachant que x est le numéro de votre groupe
ifconfig eth0/1 192.168.x.1 netmask 255.255.255.0 up
sleep 1
done
-------------------------------------------------------------------------
```

(b) Modifier le droit d'exécution de "**Confmr**" par la commande suivante : `chmod 777 confmr`.

(c) Lancer le "**Confmg**" par la commande suivante : `./confmr &`.

Tâche 2 : Test de connectivité/configuration des équipements réseau gauche de l'atelier groupe

1. Ouvrir un terminal sur la machine **MG**.
2. Lancer la commande ***ping*** pour tester la connectivité de l'interface Ethernet de la machine **MG** avec l'interface Ethernet gauche du routeur **RG**. À partir de l'hôte **MG**, envoyez une requête ***ping*** à l'interface de type Ethernet du routeur **RG**.
3. La requête `ping` a-t-elle abouti ?
4. À partir du routeur, envoyez une requête ***ping*** à l'interface Ethernet de la machine `MG`.
5. La requête `ping` a-t-elle abouti ?
6. Si la réponse à l'une des deux questions est non, vérifiez les configurations de routeur pour identifier l'erreur. Ensuite, relancez des requêtes ***ping***jusqu'à ce que la réponse aux deux questions soit oui.
7. Ouvrez un navigateur Web sur la machine **MG** et accédez à Internet. Les requêtes `WEB` ont-elles abouti ? Doivent échouer. Pourquoi ?

Tâche 3 : Configuration des équipements réseau droite de l'atelier groupe

1. Configurez l'interface Ethernet **eth0** de la machine **MD** avec l'adresse IP statique à l'aide des paramètres de votre groupe du tableau précédent. (**utilisation de la commande** `ifconfig`).
2. Pour éviter le problème de désactivation de l'interface. Créez un script pour la configuration de l'interface Ethernet **eth0** de la machine **MD**. Pour cela :

(a) Créez un script "**Confmd**" suivant :

```
-------------------------------------------------------------------------
#!/bin/bash
while true
do
# Commande de configuration de votre interface eth0 de la machine gauche:
# Sachant que x est le numéro de votre groupe
ifconfig eth0 172.x.0.2 netmask 255.255.0.0 up
sleep 1
done
-------------------------------------------------------------------------
```

(b) Modifier le droit d'exécution de "**Confmd**" par la commande suivante : `chmod 777 confmd`.

(c) Lancer le "**Confmd**" par la commande suivante : `./confmd &`.

3. Affichez la table de routage de la machine. `route -n`).
4. Ajoutez la route par défaut pour la machine **MD** avec l'adresse IP passerelle indiqué dans le tableau précédent. (**utilisation de la commande** (**utilisation de la commande** `route add default gw 172.x.0.1`).
5. Affichez la table de routage de la machine. `route -n`).
6. Configurez l'interface Ethernet droite du routeur **RD** avec l'adresse IP statique à l'aide des paramètres du tableau précédent. (**utilisation de la commande** `ifconfig`).

(a) Modifier le script "**Confmr**" suivant :

```
-------------------------------------------------------------------------
#!/bin/bash
while true
do
# Commande de configuration de votre interface eth1/eth0 de la machine gauche:
# Sachant que x est le numéro de votre groupe
ifconfig eth0/1 192.168.x.1 netmask 255.255.255.0 up
ifconfig eth1/0 172.x.0.1 netmask 255.255.0.0 up
sleep 1
done
-------------------------------------------------------------------------
```

(b) Relancer le "**Confmr**" par la commande suivante : `./confmr &`.

Tâche 4 : Test de connectivité/configuration des équipements réseau droite de l'atelier groupe

1. Ouvrir un terminal sur la machine **MD**.
2. Lancer la commande ***ping*** pour tester la connectivité de l'interface Ethernet de la machine **MD** avec l'interface Ethernet gauche du routeur **RD**. À partir de l'hôte **MD**, envoyez une requête ***ping*** à l'interface de type Ethernet du routeur **RD**.
3. La requête ping a-t-elle abouti ?
4. À partir du routeur, envoyez une requête ***ping*** à l'interface Ethernet de la machine **MD**.
5. La requête `ping` a-t-elle abouti ?
6. Si la réponse à l'une des deux questions est non, vérifiez les configurations de routeur pour identifier l'erreur. Ensuite, relancez des requêtes ***ping*** jusqu'à ce que la réponse aux deux questions soit oui.

7. Ouvrez un navigateur Web sur la machine **MD** et accédez à Internet. Les requêtes `WEB` ont-elles abouti ? Doivent échouer. Pourquoi ?

Tâche 5 : Configuration des équipements réseau salle de l'atelier groupe

1. L'interface Ethernet salle **eth3** du routeur **RS** est déjà configurée par une adresse IP automatique à l'aide DHCP.
2. A l'aide la commande `ifconfig eth3`, récupérer l'adresse IP de **RS**, elle est sous forme **10.3.x.y/8**.
3. Affichez la table de routage du routeur. `route -n`).

Tâche 6 : Test de connectivité/configuration des équipements réseau Gauche-droite de l'atelier groupe

1. À partir de l'hôte **MD**, envoyez une requête ***ping*** au hôte **MG**.
2. La requête ***ping*** a-t-elle abouti ?
3. À partir de l'hôte **MG**, envoyez une requête ***ping*** au hôte **MD**.
4. La requête ***ping*** a-t-elle abouti ?
5. Tous ces ***ping*** doivent échouer. Pourquoi ?

Tâche 7 : Activation de routage sur le routeur de l'atelier groupe

Les machines Linux ne sont pas des routeurs par défaut, il faut activer le routage au niveau des machines jouent le rôle d'une routeur.

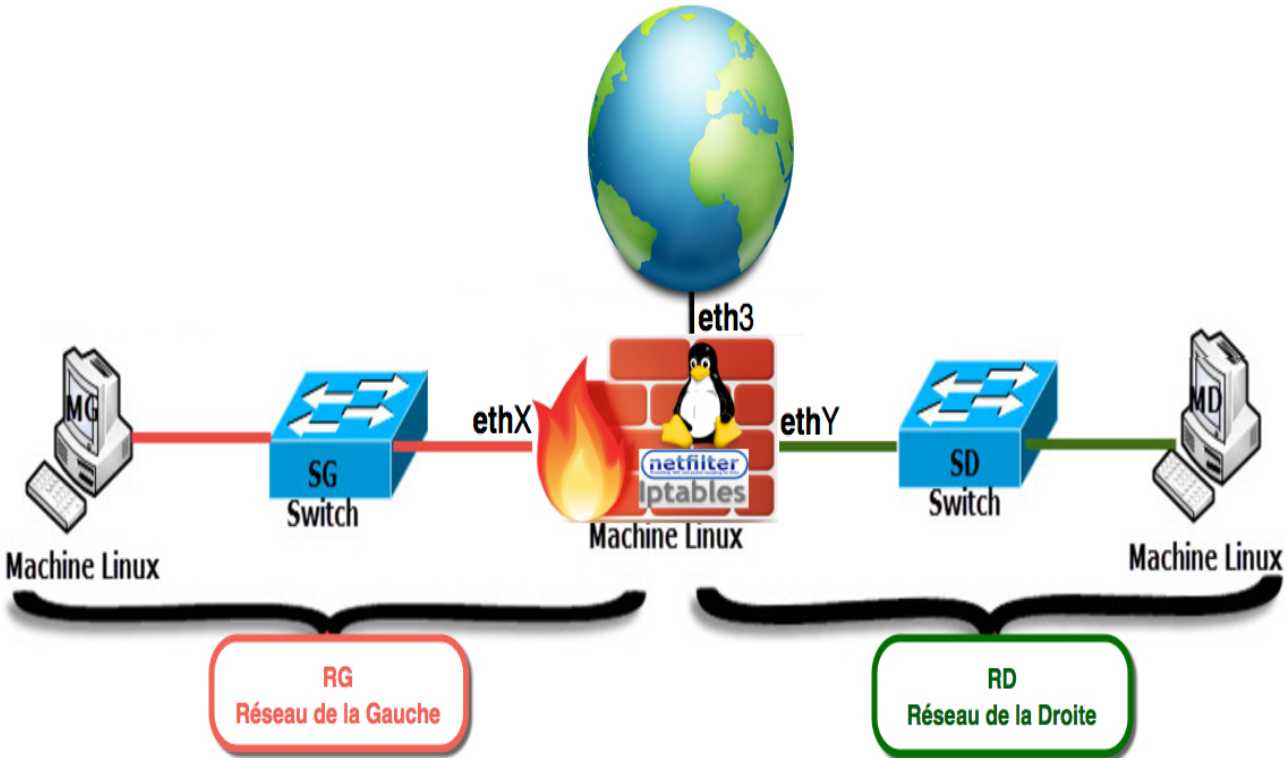
1. Ouvrir un terminal sur le routeur.
2. Activez le routage sur le routeur par la commande suivante : `echo 1 > /proc/sys/net/ipv4/ip_forward`.

Tâche 8 : Test de connectivité/configuration des équipements réseau Gauche-droite de l'atelier groupe

1. À partir de l'hôte **MD**, envoyez une requête ***ping*** au hôte **MG**.
2. La requête ***ping*** a-t-elle abouti ?
3. À partir de l'hôte **MG**, envoyez une requête ***ping*** au hôte **MD**.
4. La requête ***ping*** a-t-elle abouti ?
5. Si la réponse à l'une des deux questions est non, vérifiez les configurations de votre atelier pour identifier l'erreur. Ensuite, relancez des requêtes ***ping*** jusqu'à ce que la réponse aux deux questions soit oui.

PARTIE 2 : Configuration et Mise en place de règles de filtrage simples

Atelier de TP



Étape 3 : Bloquer tous le monde

Tâche 1 : Affichage des informations sur les trois tables de Netfilter

1. Ouvrir un terminal sur le routeur/Firewall.
2. Voir le manuel de la commande `iptables`. (**Utilisation** : `man iptables`).
3. Lister les règles de filtrage par défaut lorsque le pare-feu est activé pour les trois tables. (**Utilisation** : `iptables` avec les options adéquates).

Tâche 2 : Suppression des règles existantes sur les différentes chaines de différentes tables

1. Ouvrir un terminal sur le routeur/Firewall.
2. Supprimer les règles des chaînes de la **table filter** (**INPUT**, **FORWARD** et **OUTPUT**). (**Utilisation** : `iptables` avec les options adéquates).
3. Supprimer les chaînes personnelles de la **table filter**. (**Utilisation** : `iptables` avec les options adéquates).
4. Supprimer les chaînes de la **table nat** (**PREROUTING**, **OUTPUT** et **POSTROUTING**). (**Utilisation** : `iptables` avec les options adéquates).

5. Supprimer les chaînes personnelles de la **table nat**. (**Utilisation** : `iptables` avec les options adéquates).
6. Vérifiez que vous pouvez atteindre les réseaux par `ping` ?
   (a) A partir de **MD**, envoyez une requête `ping` vers **MG** et **Routeur/Firewall**. Les requêtes `ping` ont-elles abouti ?
   (b) A partir de **MG**, envoyez une requête `ping` vers **MD** et **Routeur/Firewall**. Les requêtes `ping` ont-elles abouti ?
   (c) A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **MG** et **MD**. Les requêtes `ping` ont-elles abouti ?

Tâche 3 : Application d'une politique par défaut pour la table filter

1. Ouvrir un terminal sur le routeur/Firewall.
2. Pour les trois tables, quelle est la stratégie par défaut ? (**Utilisation** : `iptables` avec les options adéquates).
3. Ajouter un politique de sécurité forte qui bloque tout sauf ce qui est explicitement autorisé pour la table Filter (sur les différentes chaines de la table). (**Utilisation** : `iptables` avec les paramètres adéquats).
4. Vérifier maintenant la stratégie par défaut ? (**Utilisation** : `iptables` avec les options adéquates).

Tâche 4 : Test de la politique par défaut pour la table filter

1. A partir de **MD**, envoyez une requête `ping` vers **MG** et **Routeur/Firewall**.
2. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
3. A partir de **MG**, envoyez une requête `ping` vers **MD** et **Routeur/Firewall**.
4. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
5. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **MG** et **MD**.
6. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
7. A partir de **Routeur/Firewall**, envoyez une requête `ping` **127.0.0.1**.
8. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Étape 4 : Autorisation des réseaux de confiance

Dans votre groupe, le firewall a trois cartes réseaux ("**eth**X", "**eth**Y" et "**eth3**"), ainsi que l'interface de loopback ("**lo**").

Tâche 1 : Autorisation du réseau loopback (127.0.0.0/8)

Nous pouvons avoir toute confiance en réseau **loopback**, car il est interne à la mémoire de votre machine/routeur/firewall.

1. Ouvrir un terminal sur le routeur/Firewall.
2. Autoriser toutes les connexions sortantes des processus locaux par cette interface "**lo**" ayant une adresse source de loopback et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).

3. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
4. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **127.0.0.1**.
5. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
6. Autoriser toutes les connexions rentrantes dans les processus locaux par cette interface "**lo**" ayant une adresse source de loopback et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).
7. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
8. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **127.0.0.1**.
9. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Tâche 2 : Autorisation du réseau droit

Nous pouvons avoir toute confiance en réseau **droit**, car il est votre LAN interne.

1. Ouvrir un terminal sur le routeur/Firewall.
2. Autoriser toutes les connexions sortantes vers le réseau droit par l'interface "**eth**Y" ayant une adresse source de réseau droit et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).
3. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
4. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **MD**.
5. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
6. A partir de **MD**, envoyez une requête `ping` vers **Routeur/Firewall**.
7. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
8. Autoriser toutes les connexions rentrantes depuis le réseau droit par l'interface "**eth**Y" ayant une adresse source de réseau droit et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).
9. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
10. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **MD**.
11. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
12. A partir de **MD**, envoyez une requête `ping` vers **Routeur/Firewall**.
13. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Tâche 3 : Autorisation du réseau gauche

Nous pouvons avoir toute confiance en réseau **gauche**, car il est votre LAN interne.

1. Ouvrir un terminal sur le routeur/Firewall.
2. Autoriser toutes les connexions sortantes vers le réseau gauche par l'interface "**eth**X" ayant une adresse source de réseau gauche et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).
3. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).

4. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **MG**.
5. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
6. A partir de **MG**, envoyez une requête `ping` vers **Routeur/Firewall**.
7. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
8. Autoriser toutes les connexions rentrantes depuis le réseau gauche par l'interface "**eth**X" ayant une adresse source de réseau gauche et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).
9. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
10. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **MG**.
11. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
12. A partir de **MG**, envoyez une requête `ping` vers **Routeur/Firewall**.
13. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Tâche 4 : Autorisation du réseau de la salle

Nous pouvons avoir toute confiance en réseau **de la salle**, car il est votre LAN interne.

1. Ouvrir un terminal sur le routeur/Firewall.
2. Autoriser toutes les connexions sortantes vers le réseau de la salle par l'interface "**eth**3" ayant une adresse source de réseau de la salle et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).
3. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
4. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **Passeralle** du firewall (**10.3.x.y**, utiliser la commande `route -n` pour le visualiser).
5. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
6. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **Routeur/Firewall** de votre groupe voisin.
7. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
8. Autoriser toutes les connexions rentrantes depuis le réseau de la salle par l'interface "**eth**3" ayant une adresse source de réseau de la salle et à destination des machines de ce réseau. (**Utilisation** : `iptables` avec les paramètres adéquats).
9. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
10. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **Passeralle** du firewall (**10.3.x.y**, utiliser la commande `route -n` pour le visualiser).
11. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
12. A partir de **Routeur/Firewall**, envoyez une requête `ping` vers **Routeur/Firewall** de votre groupe voisin.
13. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Étape 5 : Autorisation des communications entre les réseaux de groupe

Dans votre groupe, vous avez trois réseaux (Salle (via eth3), droit (via ethY) et gauche (via ethX)), dans cette étape, nous voulons autorisé les communications entre eux (forwarding) via le firewall.

Tâche 1 : Autorisation des connexions entre le réseau droit et le réseau gauche

Nous pouvons avoir toute confiance pour les communications entre le réseau **droit** vers le réseau **gauche** et inversement.

1. Ouvrir un terminal sur le routeur/Firewall.
2. Autoriser toutes les connexions ayant une adresse source de **réseau droit** et une adresse de destination de **réseau gauche**. (**Utilisation** : `iptables` avec les paramètres adéquats).
3. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
4. A partir de **MG**, envoyez une requête `ping` vers **MD**.
5. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
6. A partir de **MD**, envoyez une requête `ping` vers **MG**.
7. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
8. Autoriser toutes les connexions ayant une adresse source de **réseau gauche** et une adresse de destination de **réseau droit**. (**Utilisation** : `iptables` avec les paramètres adéquats).
9. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
10. A partir de **MG**, envoyez une requête `ping` vers **MD**.
11. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
12. A partir de **MD**, envoyez une requête `ping` vers **MG**.
13. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Tâche 2 : Autorisation des connexions entre le réseau droit et le réseau salle

Nous pouvons avoir toute confiance pour les communications entre le réseau **droit** vers le réseau **salle** et inversement.

1. Ouvrir un terminal sur le routeur/Firewall.
2. Autoriser toutes les connexions ayant une adresse source de **réseau droit** et une adresse de destination de **réseau salle**. (**Utilisation** : `iptables` avec les paramètres adéquats).
3. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
4. A partir de **MD**, envoyez une requête `ping` vers un **firewall** d'un autre groupe ou vers la passerelle du firewall (trouver dans la tache de l'étape 4).
5. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

6. Autoriser toutes les connexions ayant une adresse source de **réseau salle** et une adresse de destination de **réseau droit**. (**Utilisation** : `iptables` avec les paramètres adéquats).
7. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
8. A partir de **MD**, envoyez une requête `ping` vers un **firewall** d'un autre groupe ou vers la passerelle du firewall (trouver dans la tache de l'étape 4).
9. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Tâche 3 : Autorisation des connexions entre le réseau droit et le réseau salle

Nous pouvons avoir toute confiance pour les communications entre le réseau **gauche** vers le réseau **salle** et inversement.

1. Ouvrir un terminal sur le routeur/Firewall.
2. Autoriser toutes les connexions ayant une adresse source de **réseau gauche** et une adresse de destination de **réseau salle**. (**Utilisation** : `iptables` avec les paramètres adéquats).
3. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
4. A partir de **MG**, envoyez une requête `ping` vers un **firewall** d'un autre groupe ou vers la passerelle du firewall (trouver dans la tache de l'étape 4).
5. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
6. Autoriser toutes les connexions ayant une adresse source de **réseau salle** et une adresse de destination de **réseau gauche**. (**Utilisation** : `iptables` avec les paramètres adéquats).
7. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
8. A partir de **MG**, envoyez une requête `ping` vers un **firewall** d'un autre groupe ou vers la passerelle du firewall (trouver dans la tache de l'étape 4).
9. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

Étape 6 : Refuser la connexion d'une machine

Tâche 1 : Refuser la connexion de la machine MD

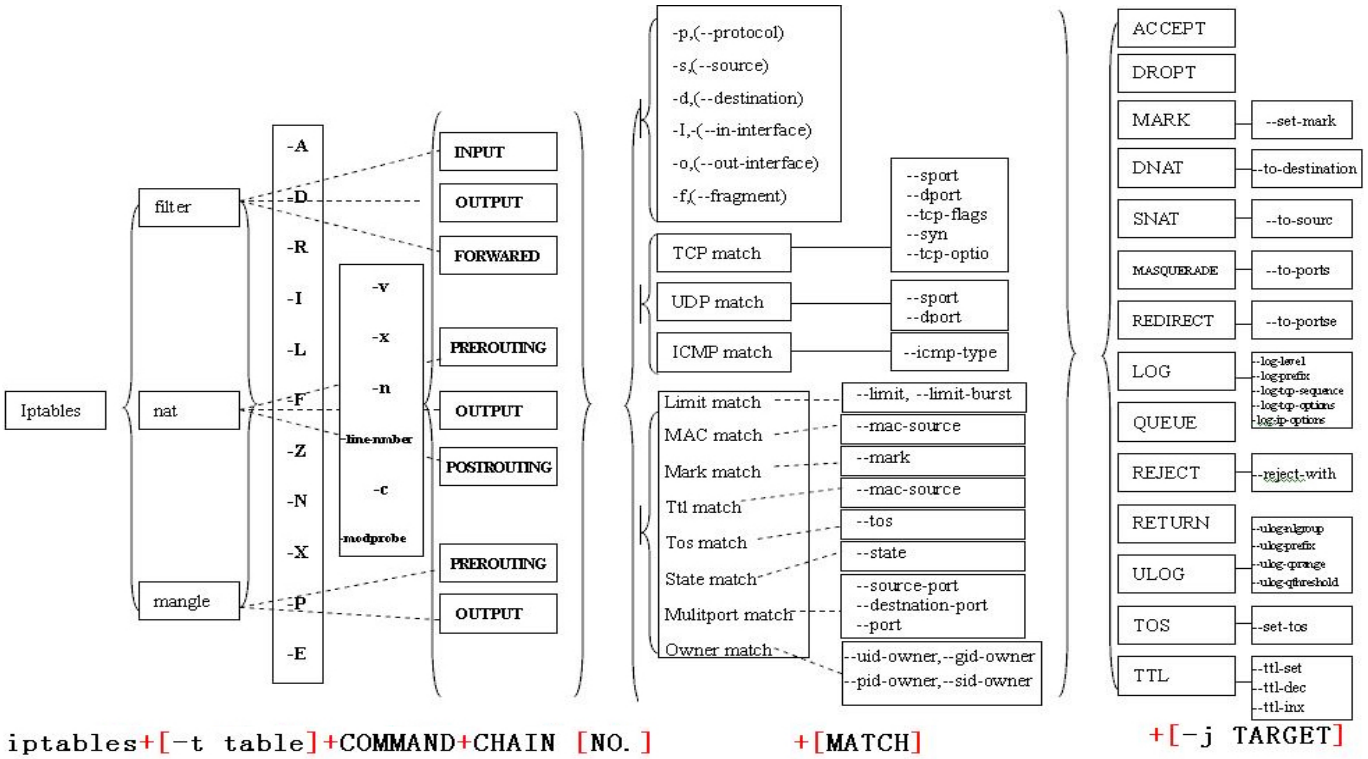
1. Ouvrir un terminal sur le routeur/Firewall.
2. Refuser la connexion d'une machine ayant comme adresse source de la machine **MD**. (**Utilisation** : `iptables` avec les paramètres adéquats).
3. Modifier la liste des règles des différentes chaines des étapes précédentes pour prendre en considération cette action. (**Utilisation** : `iptables` avec les paramètres adéquats).
4. Afficher les chaines et les règles de filtrage pour la table filter. Que-remarquez vous ? (**Utilisation** : `iptables` avec les options adéquates).
5. A partir de **MD**, envoyez une requête `ping` vers **MG**.
6. Les requêtes `ping` ont-elles abouti ? Pourquoi ?
7. A partir de **MD**, envoyez une requête `ping` vers **Firrewall**.
8. Les requêtes `ping` ont-elles abouti ? Pourquoi ?

ANNEXE : Manuel de la commande `iptables`

La syntaxe de la commande **iptables** est :

`#iptables -t table -(option-chaine) CHAINE -(option-match) critère-correspondance --jump/-j action/cible`

- `-t table` : permet de spécifier une table parmi les trois tables (**FILTER**, **NAT** et **MANGLE**), la table **FILTER** est utilisé par défaut.
- `-option-chaine chaine` : permet de spécifier une opération sur une chaine parmi les cinq chaines (**INPUT**, **OUTPUT**, **PREROUTING**, **POSTROUTING** et **FORWARD**) (**Attentio** les noms des chaines doit être en majuscule).
- `-option-match critère-correspondance` : est présenté par un ensemble des paramètres et des critères de correspondance.
- `-j/--jump action/cible` : permet de spécifier une action (cible).



Les valeurs de `-option-chaine chaine` sont :

- `-L` : Affiche toutes les règles actives des chaines.
- `-F CHAINE` : Supprime toutes les règles de la chaîne. Si aucune chaîne n'est spécifiée, toutes celles de la table sont vidées.
- `-N CHAINE` : Crée une nouvelle chaîne utilisateur avec le nom passé en paramètre.
- `-X CHAINE` : Supprime la chaîne utilisateur. Si aucun nom n'est spécifié, toutes les chaînes utilisateur seront supprimées
- `-P CHAINE cible` : Modifie la politique par défaut de la chaîne. Il faut indiquer en paramètre la cible à utiliser.
- `-A CHAINE règle` : Ajoute une règle à la fin de la chaîne spécifiée.
- `-I CHAINE [numéro]/[règle]` : Insère une règle avant celle qui suit l'option `-I`.
- `-D CHAINE [numéro]/[règle]` : Supprime une règle de la chaîne.
- ...

Les valeurs de `-(option-match) critère-correspondance` sont :

- `--source/-s` : Cette option est suivie par l'adresse de la machine qui a émis le paquet. L'adresse de la machine est spécifiée par son IP (**N.N.N.N**) ou par le nom de machine. Si l'adresse est précédée de l'opérateur unaire de négation (**!N.N.N.N**) (point d'exclamation), la condition sera remplie si l'adresse de l'émetteur est différente de celle indiquée. On peut aussi à la suite de l'adresse indiquer un masque de sous-réseau en séparant ces 2 éléments par un / (barre oblique) (**N.N.N.N/M.M.M.M**).
- `--destination/-d` : Indique l'adresse de destination du paquet, avec les mêmes possibilités que pour –**source**.
- `--in-interface/-i` **Chaînes INPUT, FORWARD ou PREROUTING** : Interface d'entrée. Suivie par le nom de l'interface par laquelle doivent arriver les paquets. Par exemple, ce sera **ppp0** pour un modem, ou **eth0** pour la première carte Ethernet. Le nom de l'interface peut être précédé d'un ! (point d'exclamation) pour inverser le test.
- `--out-interface/-o` **Chaînes FORWARD, OUTPUT ou POSTROUTING** : Interface de sortie. Suivi du même paramètre que pour l'option `--in-interface`. Dans ce cas-là est testée l'interface par laquelle vont être envoyés les paquets.
- `--protocol/-p` **Protocole** : Permet de vérifier le protocole du paquet. Les valeurs littérales pouvant être utilisées à la suite de cette option sont `tcp`, `udp`, `icmp` ou all qui les regroupe toutes.
- `--source-port --protocol tcp` ou `--protocol udp` **Port source** : Cette option permet de vérifier le port source (celui utilisé par l'émetteur). Il est spécifié sous forme numérique ou par nom de service (comme `http` ou `smtp`). On peut aussi indiquer une plage de port en séparant les deux bornes par **:** (deux points). Par exemple **25 :110** pour tous les ports compris entre **25** et **110**. Pour exclure le ou les ports spécifiés, il faut utiliser un **!** (point d'exclamation) après `--source-port`.
- `--destination-port --protocol tcp` ou `--protocol udp` **Port destination** : Compare le port utilisé pour se connecter sur la machine avec la valeur ou plage de valeur indiquée. Ces dernières sont indiquées comme pour –**source-port**.
- `--state/-m state` **État du paquet** : Une liste de plusieurs valeurs peut être indiquée en les séparant par des virgules. L'état de ce paquet est comparé alors à ces valeurs. **NEW** correspond à un paquet initiant une nouvelle connexion. **ESTABLISHED** est un paquet participant à une conversation déjà établie. **RELATED** est pour un paquet qui ouvre une nouvelle connexion, mais ceci en rapport avec une précédente déjà établie. **INVALID** indique un paquet qui n'est rattaché à aucune connexion.
- **Minimize-Delay** : Améliore la réactivité des connexions en réduisant le délai (ssh, telnet, ftp contrôle, tftp, flux DNS).
- **Maximize-Throughput** : Améliore le débit au prix d'une possible détérioration de l'interactivité de la session. Les temps de latence ne sont pas importants (ftp-data,www, transfert de zone DNS).
- **Maximum-Reliability** : Certitude que les données arrivent sans perte - Améliore la fiabilité (snmp, smtp).
- **Minimize monetary cost** : minimise le délai, meilleure rentabilité (nntp, icmp).
- Le module limit permet les options suivantes :
  - `--limit` : limite le nombre de concordances dans un espace-temps donné, grâce à un modificateur de nombre et de temps paramétré sous la forme suivante : <**nombre**>/<**temps**>. Par exemple, en écrivant `--limit` **5/hour**, une règle effectue son contrôle de concordance seulement cinq fois par heure.
  - `--limit-burst` : limite le nombre de paquets pouvant être comparés à une règle, à un moment donné.
- ...

Les valeurs de `--jump/-j action/cible` sont :

- Une fois les règles spécifiés, il faut indiquer vers quelle **cible/action** envoyer le paquet en cas de test probant (**ACCEPT**, **DROP**, **REJECT**, **LOG**, **SNAT**, **DNAT**, **MASQUERADE**). Cela se fait avec l'option `--jump` ou en abrégé `-j` suivie par le nom de la cible.
  - **ACCEPT** : Permet d'accepter un paquet grâce à la règle vérifiée.
  - **DROP** : Rejet d'un paquet sans message d'erreur si la règle est vérifiée.
  - **REJECT** : Rejet avec un retour de paquet d'erreur à l'expéditeur si la règle est vérifiée.
  - **LOG** : Permet d'écrire un ligne de log avec les infos du paquet (adresses, port, portocol...).
  - **SNAT** : Permet de modifier l'adresse source du paquet.
  - **DNAT** : Permet de modifier l'adresse destination du paquet.
  - **MASQUERADE** : Une passerelle (gateway) transforme les paquets sortants passant par elle pour donner l'illusion qu'ils sortent de la passerelle (gateway) elle-même par un port alloué dynamiquement, lorsque la passerelle (gateway) reçoit une réponse sur ce port, elle utilise une table de correspondance entre le port et les machines du réseau privé qu'elle gère pour lui faire suivre le paquet.
- Certaines de ces cibles nécessitent des options pour les paramétrer. Elles sont indiquées sous la même forme que les options de tests. Voici quelques cibles courantes.
  - `--to-source` : la cible **SNAT** qui modifie l'adresse source dans le paquet pour remplacer celle existante. On peut indiquer une seule IP, ou une plage d'adresses IP en séparant les bornes par un – (tiret). On peut aussi modifier le port en spécifiant un port (ou une plage de ports) en le séparant de l'adresse par : (deux points).
  - `--to-destination` : la cible DNAT qui modifie l'adresse IP de destination. Le format du paramètre suivant –to-destination est le même que pour `--to-source`.
  - `--log-prefix` : il s'agit de la cible **LOG**. Cette option est suivie d'une chaîne de moins de 30 caractères qui préfixe les lignes insérées dans les fichiers journaux. Ca permet de repérer ces lignes plus facilement par la suite.
  - `--reject-with` : c'est la cible **REJECT** qui indique quel type de message **ICMP** doit être envoyé vers la machine dont le paquet est rejeté. A la suite de l'option, on peut trouver par exemple **icmp-net-unreachable** (réseau inaccessible), **icmp-host-unreachable** (machine inaccessible), **icmp-port-unreachable** (port inaccessible), **icmp-proto-unreachable** (protocole inaccessible), **icmp-net-prohibited** (réseau interdit) ou **icmp-host-prohibited** (machine interdite). Si le type de protocol est **tcp**, on peut aussi trouver **tcp-reset** qui indique qu'il faudra envoyer un paquet avec le flag **RST** dans l'en-tête **TCP** permettant de fermer une connexion.