ASR4 Réseau
Barrière de Sécurité

Stéphanie Moreaud

Département d'informatique
IUT Bordeaux 1

Plan

Objectif : protéger un environnement (de l'intérieur comme de l'extérieur)

- gérer les connexions sortantes à partir du réseau local
- protéger le réseau des intrusions extérieures
- surveiller/tracer le trafic entre le réseau local et internet
- autoriser certains services seulement
- ...

Mise en œuvre :

- définir une politique de sécurité
  - tout intredire, ouverture sélective ?
  - sécuriser les transferts entrants et sortants
- structurer le réseau
  - séparer les communautés, les parties ouvertes à tous et les parties accessibles sur critères

Pare-feu (*Firewall*)

Définition : Programme ou matériel chargé de protéger un réseau local du monde extérieur.

Un firewall doit contrôler tout ce qui passe, et surtout tout ce qui ne doit pas passer entre internet et le réseau local.

Fonction :

- filtrer les paquets entre un réseau interne et un réseau publique
- effectuer la translation d'adresses IP

Différents types de pare-feu

Pare-feu au niveau réseau

- basé sur le filtrage des paquets
- intervient au niveau de la couche transport

Pare-feu au niveau applicatif

- généralement basé sur des mécanismes de proxy

Pare-feu des applications

- restrictions au niveau des différentes applications

Type de matériel :

- routeur filtrant
- une station équipée de deux interfaces réseau (parfois appelée *bastion*)

Filtrage de paquets

Sous Linux, les fonctionnalités de *firewall* sont directement implémentées dans le noyau (module `netfilter`).

La commande `iptables` permet la spécification de règles pour le rejet ou l'acceptation de paquet

- filtrage des paquets IP, TCP, UDP ou ICMP
- utilisation de la table FILTER
- chaînes prédéfinies INPUT, OUTPUT et FORWARD
- possibilité de filtrer les paquets suivant l'état de la connexion
- règles traitées séquentiellement :
  - traitement stoppé dès qu'une règle peut être appliquée
  - ordre des règles important

iptables : filtrage

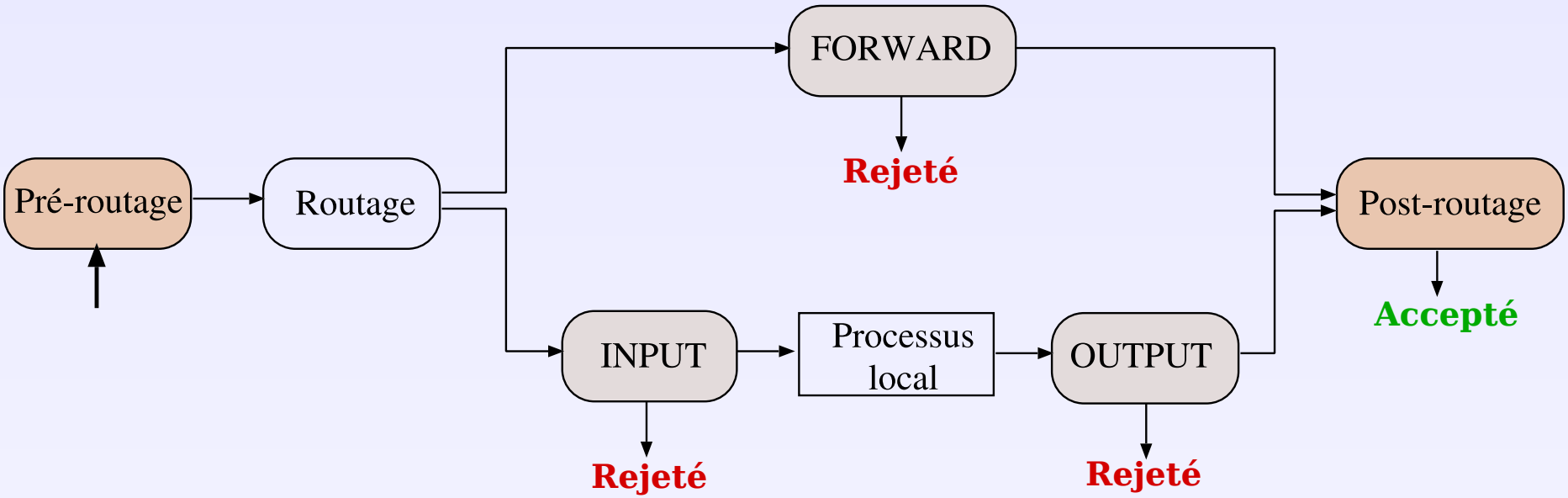


Table FILTER (filtrage des paquets)	
INPUT	paquet entrant surle routeur
OUTPUT	paquet émis par le routeur
FORWARD	paquet traversant le routeur

Cibles iptables

Cibles `iptables` (actions de filtrage)

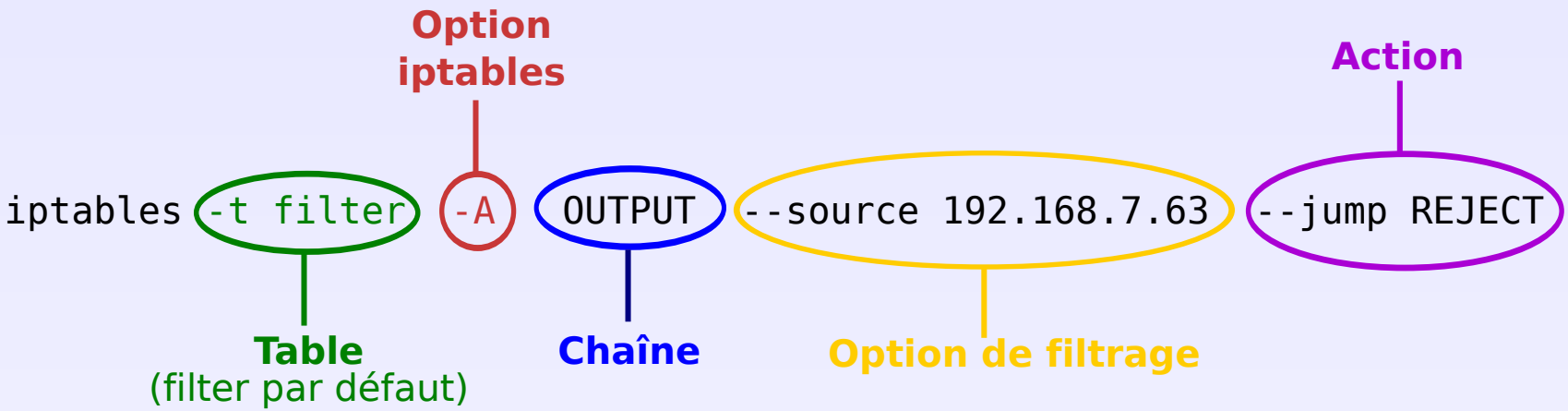
- ACCEPT : paquets/segments autorisés à poursuivre leur cheminement au travers des couches réseaux
- DROP : refus des paquets (ignorés)
- REJECT : refus du paquets et notification à l'émetteur
- LOG : génère une trace dans `/var/log/messages`

Options iptables

Options iptables :

- -L affiche les règles de la table indiquée
- -F supprime toutes les règles (politique par défaut exclue)
- -P modifie la politique par défaut
- -A ajoute une règle à la fin de la table spécifiée
- -I insère la règle avant celle indiquée
- -D supprime une règle

Règles de filtrages



Exemples :

- `iptables -t filter -F`
  - ➔ supprime les règles de filtrage
- `iptables -t filter -P OUTPUT DROP`
  - ➔ définit la politique par défaut pour OUTPUT à DROP
- `iptables -t filter -L`
  - ➔ affiche les règles de filtrage et les politiques par défaut

iptables : filtrage

Options de filtrages

- Trames
  - `-i, --in-interface` : interface réseau d'entrée
  - `-o, --out-interface` : interface réseau de sortie
- Paquet IP
  - `-s, --source` : adresse IP origine du paquet
  - `-d, --destination` : adresse IP destination
  - `-p, --protocol` : tcp, udp, icmp ou all
- Segment TCP ou datagramme UDP
  - `-sport, --source-port` : port de la source
  - `-dport, --destination-port` : port de la destination

Exemples

Accepter tous les paquets venant de 192.168.30.45

```
iptables -t filter -A INPUT --s 192.168.30.45 --jump
ACCEPT
```

Laisser partir les paquets à destination de 192.168.30.45

```
iptables -t filter -A OUTPUT --destination 192.168.30.45
--jump ACCEPT
```

Accepter tous les segments tcp arrivant sur eth0 destiné à 192.168.1.1 (provenant de n'importe où)

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

Exemples

Refuser de router les paquets ICMP en transit

```
iptables -t filter -A FORWARD --protocol ICMP --jump DROP
```

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 : suivi de connexion

Quatre états possibles pour une connexion :

- NEW : nouvelle connexion établie
- ESTABLISHED : connexion déjà établie
- RELATED : connexion en relation avec une connexion déjà établie
- INVALID : n'est dans aucune des catégories précédentes

Option : -m state --state ETAT

Exemple :

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
```

Translation d'adresses

Les réseaux privés sont cachés pour le monde extérieur

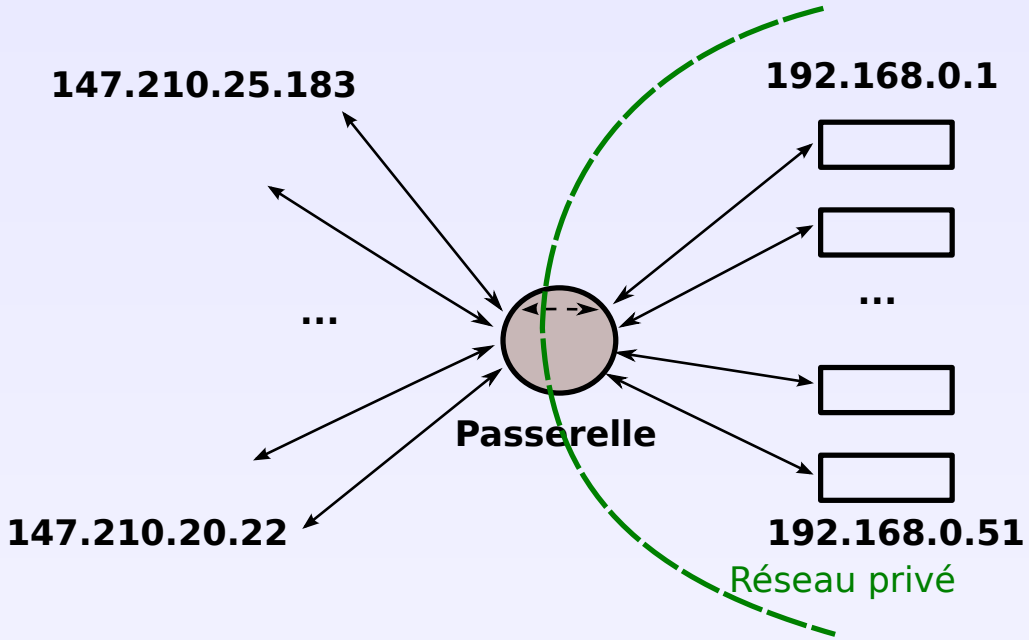
- peuvent être vu comme une seule machine
  - ➔ sécurité pour le réseau interne
  - ➔ facilite la modification de l'architecture du réseau interne et assouplit la gestion de ses adresses
  - ➔ gestion de la pénurie d'adresses
- requêtes envoyées via une passerelle
- les réponses doivent trouver le chemin retour

➔ translation d'adresses : Network Address Translation

- NAT statique : n @publiques $\leftrightarrow$ n @privées
- NAT dynamique : 1 @publique $\leftrightarrow$ n @privées

NAT statique

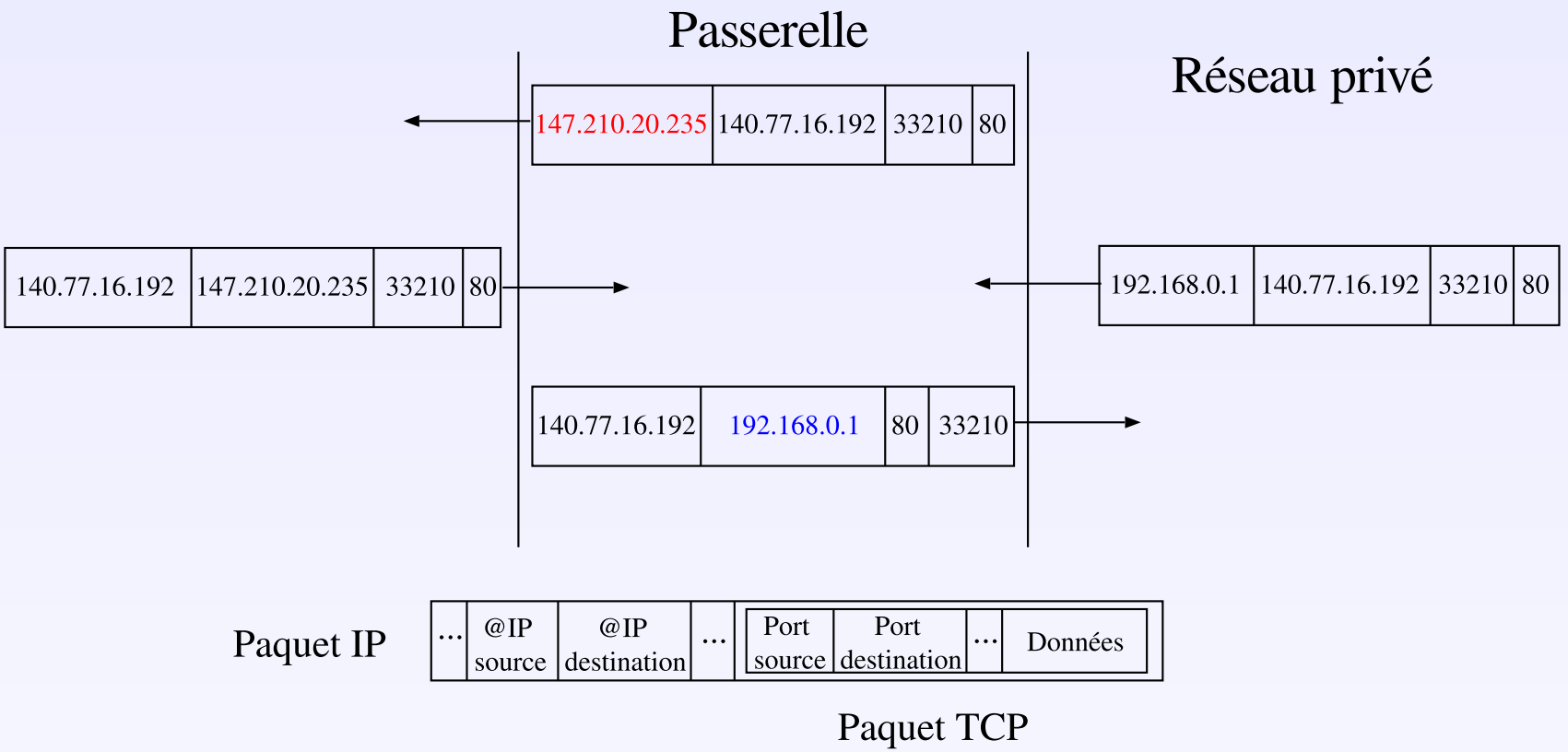
Association entre une adresse publique et une adresse privée.



- Uniformité de l'adressage dans la partie privée du réseau
  - modification correspondance @publique/@privée facile
- Sécurité : tous les flux passent par la passerelle NAT
- Pénurie d'adresses IP publiques non résolue

NAT statique

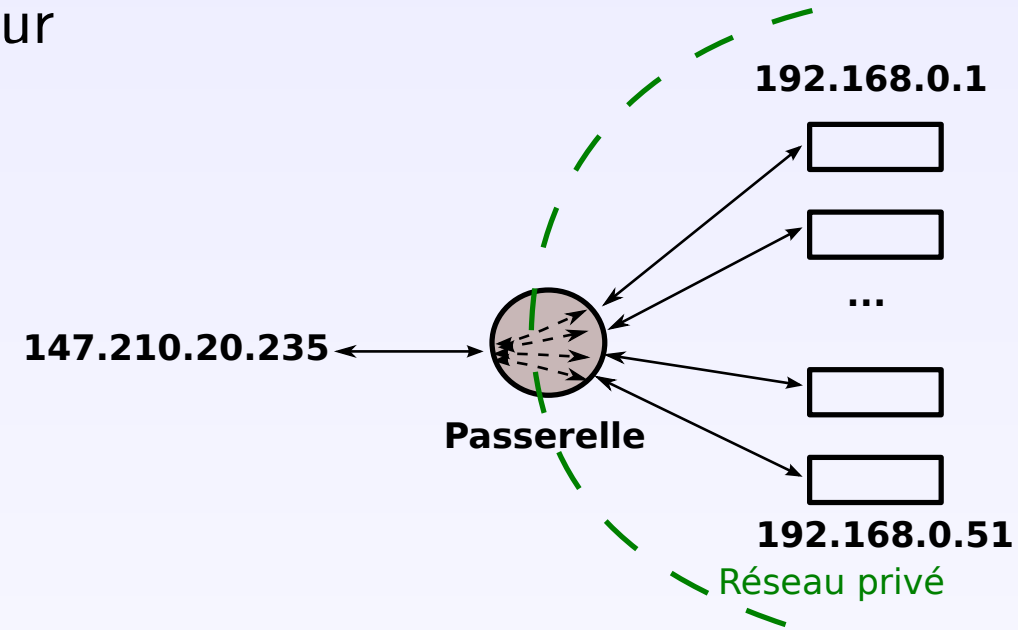
Pour chaque paquet sortant (resp. entrant), la passerelle modifie l'adresse source (resp. destination).



NAT dynamique : Masquerading

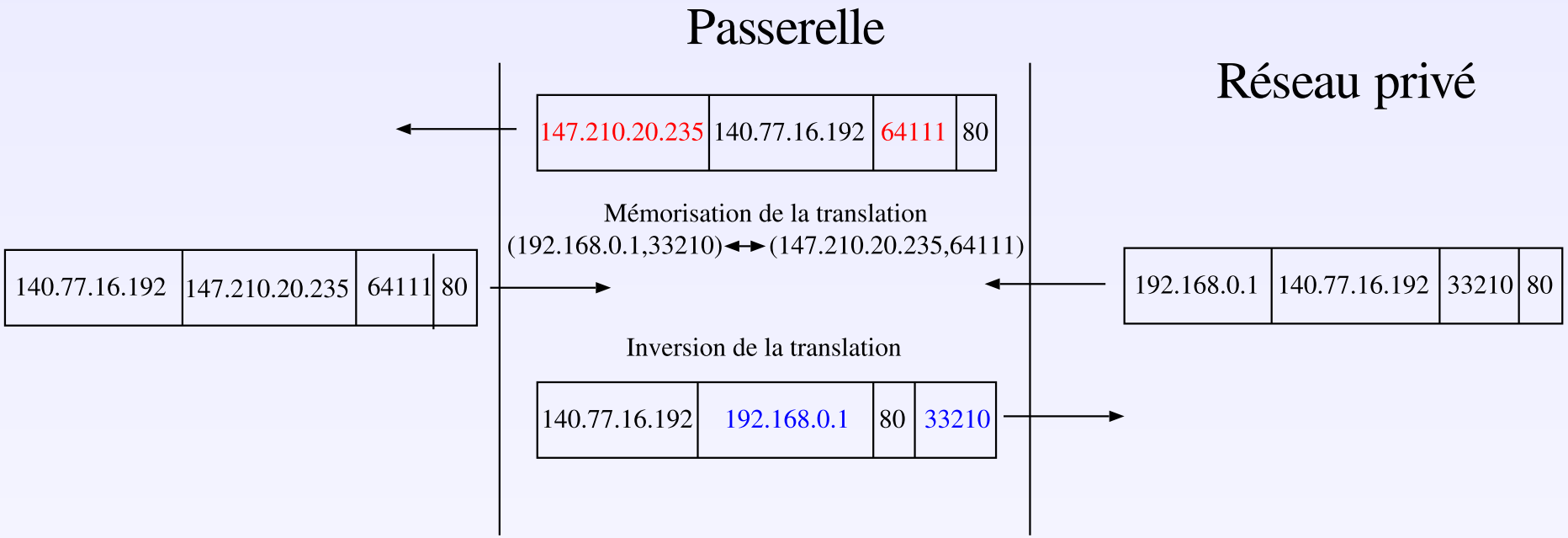
Association entre m adresses publiques et n adresses privées ($m < n$).

- plusieurs machines utilisent la même adresse IP publique à l'extérieur du réseau privé
- sécurité, tous les flux passent par la passerelle
- les machines du réseau interne ne sont pas accessibles de l'extérieur



NAT dynamique : principe

Pour chaque paquet sortant (resp. entrant), la passerelle modifie l'adresse source (resp. destination) et le numéro de port source (resp. destination).



Correspondance sauvegardée dans la table NAT

- (@s_privée, p_source) ↔ (@publique, p_source')

Problèmes liés à NAT dynamique

Translation d'adresse sur des protocoles qui ne sont pas basés sur TCP ou UDP ?

- implémentation d'une méthode spécifique au protocole
- cas des protocoles dont les paquets contiennent des données relatives aux adresses IP (ex : FTP mode actif)
  - utilisation de proxy

Comment rendre joignables des machines du réseau local ?

- redirection de port (port forwarding/mapping).

➔ connexions entrantes sur un port donné redirigées vers une machine du réseau privé (sur un port qui peut être le même ou non).

iptables : NAT

Fonctionnalités d'iptables :

- filtrage de paquets
- NAT
- marquage de paquets

➔ Trois tables de chaînes : FILTER , NAT et MANGLE.

FILTER (filtrage des paquets)		NAT (translation d'adresses)	
INPUT	paquet entrant sur le routeur	PREROUTING	NAT de destination
OUTPUT	paquet émis par le routeur	POSTROUTING	NAT de source
FORWARD	paquet traversant le routeur	OUTPUT	NAT sur les paquets émis localement

iptables : NAT

Les chaînes prédéfinies déterminent les paquets qui seront traités :

- PREROUTING : paquets entrants (destinés à l' hôte ou en transit)
- POSTROUTING : paquets sortants (transmis ou crées par l'hôte)

Cibles `iptables` pour le NAT

- SNAT : remplacement de l'adresse IP source par la valeur spécifiée (POSTROUTING)
- DNAT : remplacement de l'adresse IP destination par la valeur spécifiée (PREROUTING et OUTPUT)
- MASQUERADE : change l'adresse de l'émetteur par l'adresse de l'interface spécifiée (POSTROUTING)

Exemples

```
iptables -t nat -F
```

➔ supprime les règles NAT

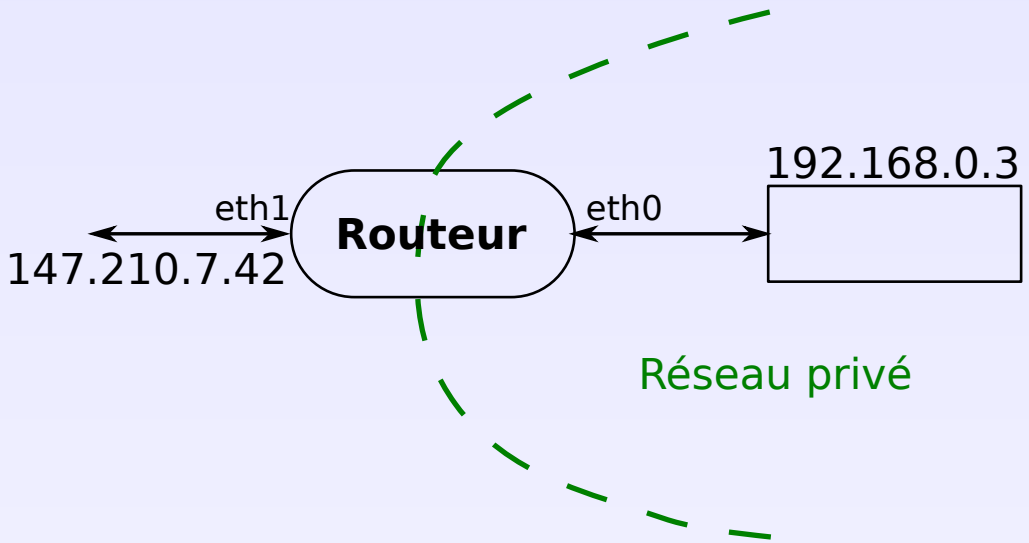
```
iptables -t nat -A POSTROUTING --out-interface eth0 --jump
MASQUERADE
```

➔ translation d'adresse dynamique

```
iptables -t nat -A POSTROUTING --out-interface eth0 --jump
SNAT --to-source 147.210.7.42
```

➔ Remplace l'adresse source des paquets a envoyer sur eth0 par 147.210.7.42

iptables : NAT



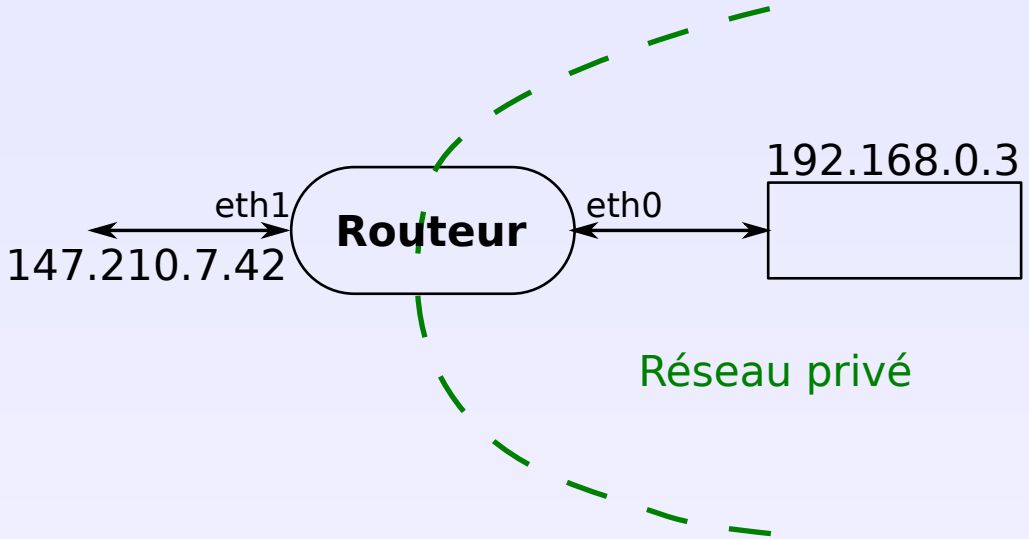
Modifier la destination du paquet avant le routage (reçu de l'extérieur).

```
iptables -t nat -A PREROUTING -d 147.210.7.42 -i eth1 -j
DNAT --to-destination 192.168.0.3
```

Modifier la source du paquet après le routage (paquet émis à partir du réseau privé).

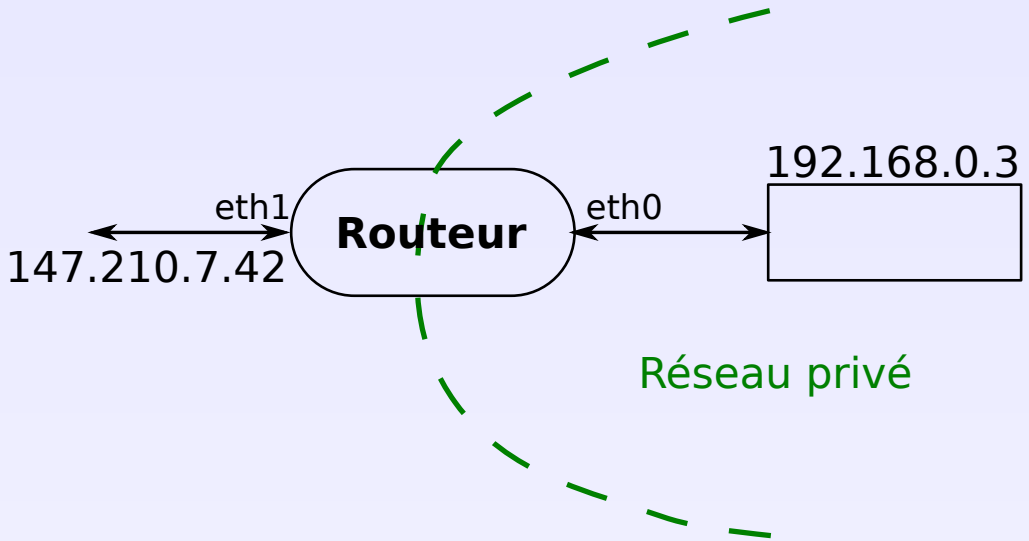
```
iptables -t nat -A POSTROUTING -s 192.168.0.3 -o eth1 -j
SNAT --to-source 147.210.7.42
```

iptables : NAT



Exercice : Comment faire pour que le routeur puisse envoyer un paquet à la machine du réseau privé à l'adresse 147.210.7.42 ?

iptables : NAT

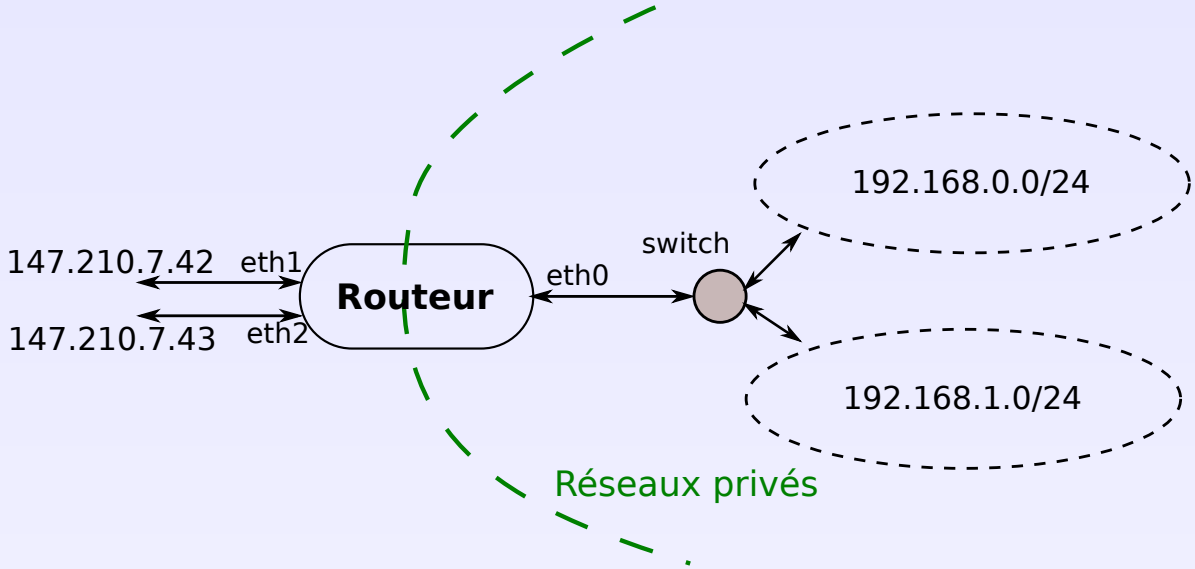


Exercice : Comment faire pour que le routeur puisse envoyer un paquet à la machine du réseau privé à l'adresse 147.210.7.42 ?

Réponse : Il faut modifier la destination du paquet émis localement avant le routage.

```
iptables -t nat -A OUTPUT -d 147.210.7.42 -j DNAT
--to-destination 192.168.0.3
```

iptables : NAT



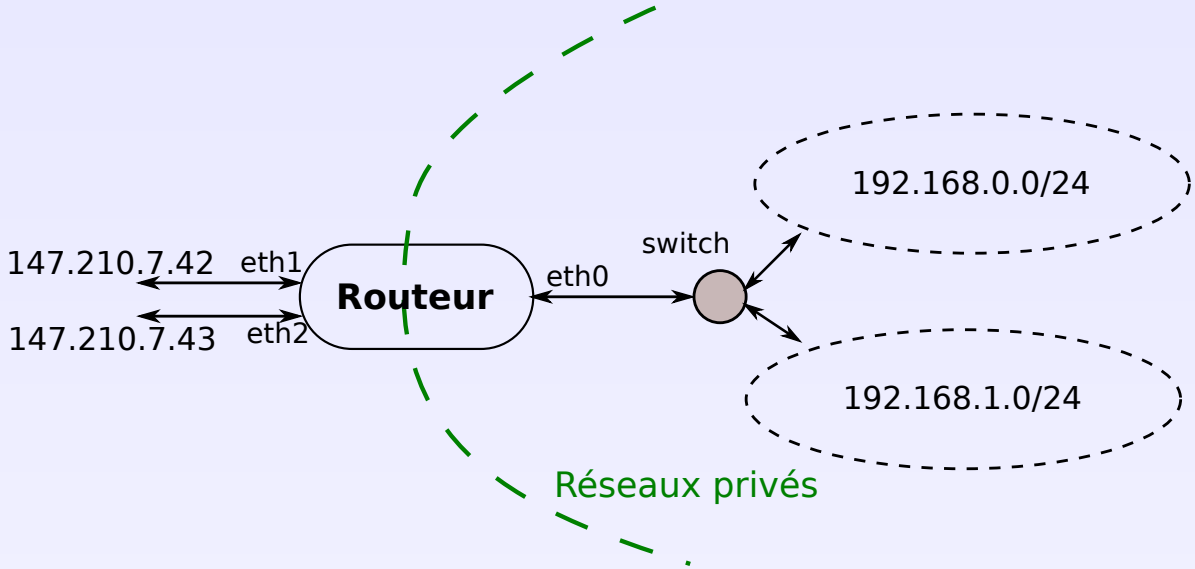
Association entre toutes les adresses privées du sous-réseau 192.168.0.0/24 et l'interface eth1.

```
iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24
-j MASQUERADE
```

Association entre les adresses privées du sous-réseau 192.168.1.0/24 et l'interface eth2.

```
iptables -t nat -A POSTROUTING -o eth2 -s 192.168.1.0/24
-j MASQUERADE
```

Transfert de port



Transférer les connexions sur le port 80 de l'adresse 147.210.7.42 sur la machine ayant l'adresse privée 192.168.0.200 sur le port 8080 :

```
iptables -t nat -A PREROUTING -p tcp -d 147.210.7.42
--dport 80 --sport 1024:65535 -j DNAT --to
192.168.0.200:8080
```

Sauvegarde et configuration perenne

Enregistremente des règles iptables

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

Restauration des tables sauvegardées

```
iptables-restore < /etc/iptables.rules
```

Chargement depuis /etc/network/interfaces

```
auto eth0
iface eth0 inet dhcp
    [...]
    pre-up iptables-restore < /etc/iptables.rules
```

Serveur de proximité (proxy ou mandataire)

Un proxy est un intermédiaire dans une connexion entre le client et le serveur

- le client s'adresse toujours au proxy
- le proxy est spécifique à une application (HTTP, FTP,...)

➔ modification des informations échangées entre client et serveur possible.

Fonctions :

- cache : conserve en mémoire les requêtes et informations pour une réutilisabilité
- enregistrement : garde une trace détaillée des échanges
- filtre : filtre au niveau des requêtes
- Autres : anonymat, traduction d'adresse

Proxy : logiciels et protocoles

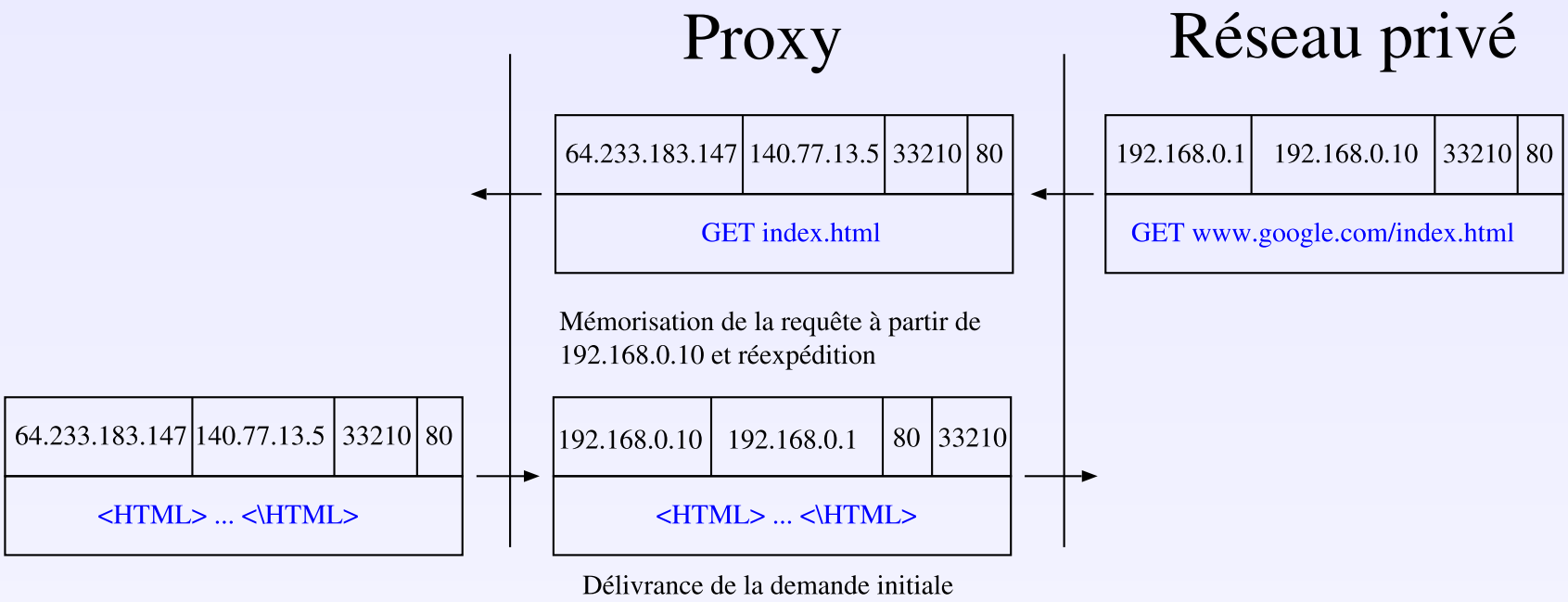
Logiciels

- modules proxy pour certains serveurs Web
  - exp : Apache
- Squid : proxy open source pour Unix
  - protocoles FTP, HTTP, Gopher, et HTTPS.

Protocoles

- SOCKS : protocoles proxy générique [RFC 1928]

Proxy : exemple



Structurer le réseau : DMZ

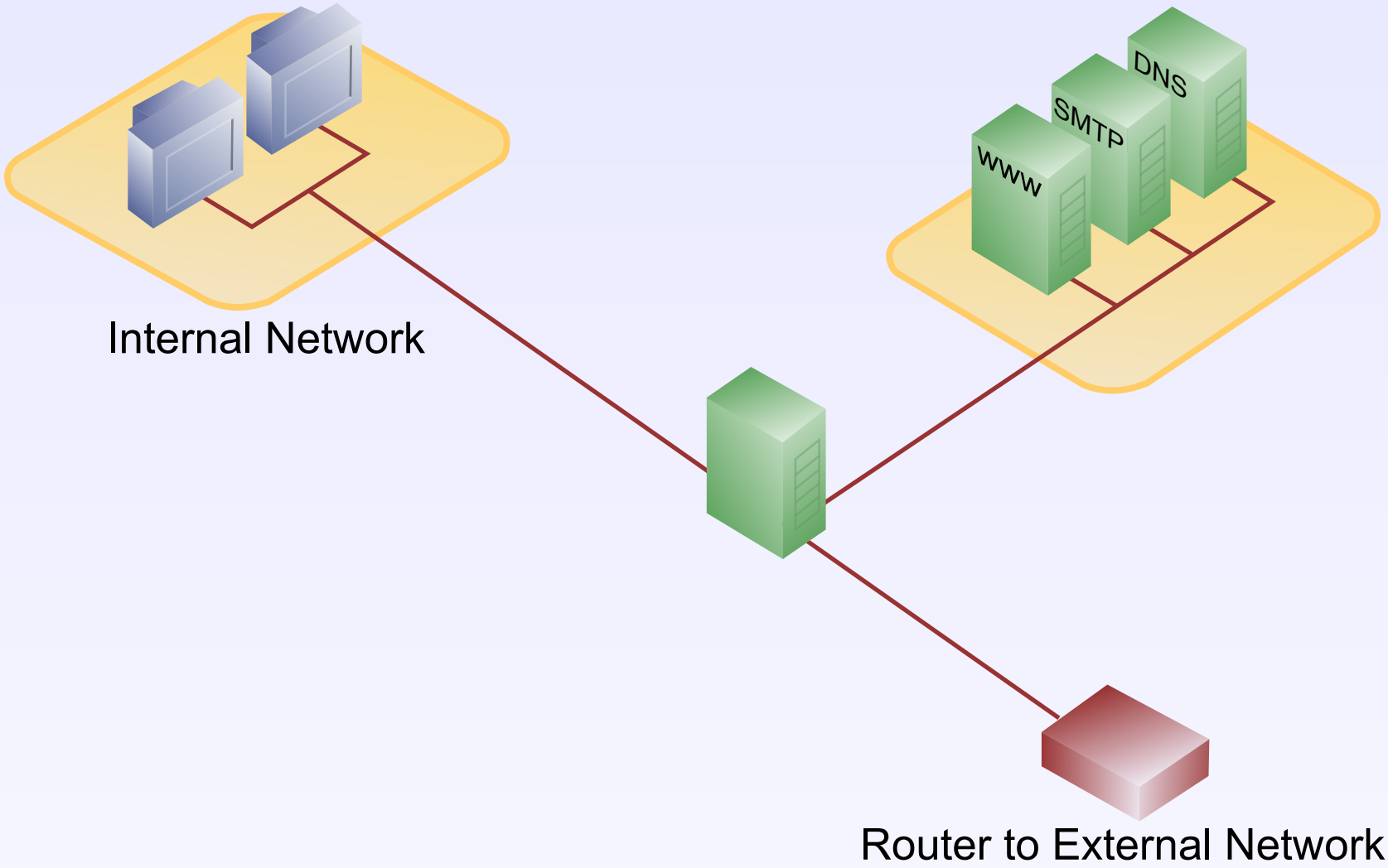
Definition : Une zone démilitarisée (DMZ) est un sous-réseau séparé du réseau local et isolé par un pare-feu.

Objectif : rendre des machines accessibles à partir de l'extérieur (serveurs DNS, SMTP,...) sans compromettre la sécurité du réseau local.

➔ la DMZ possède un niveau de sécurité intermédiaire.

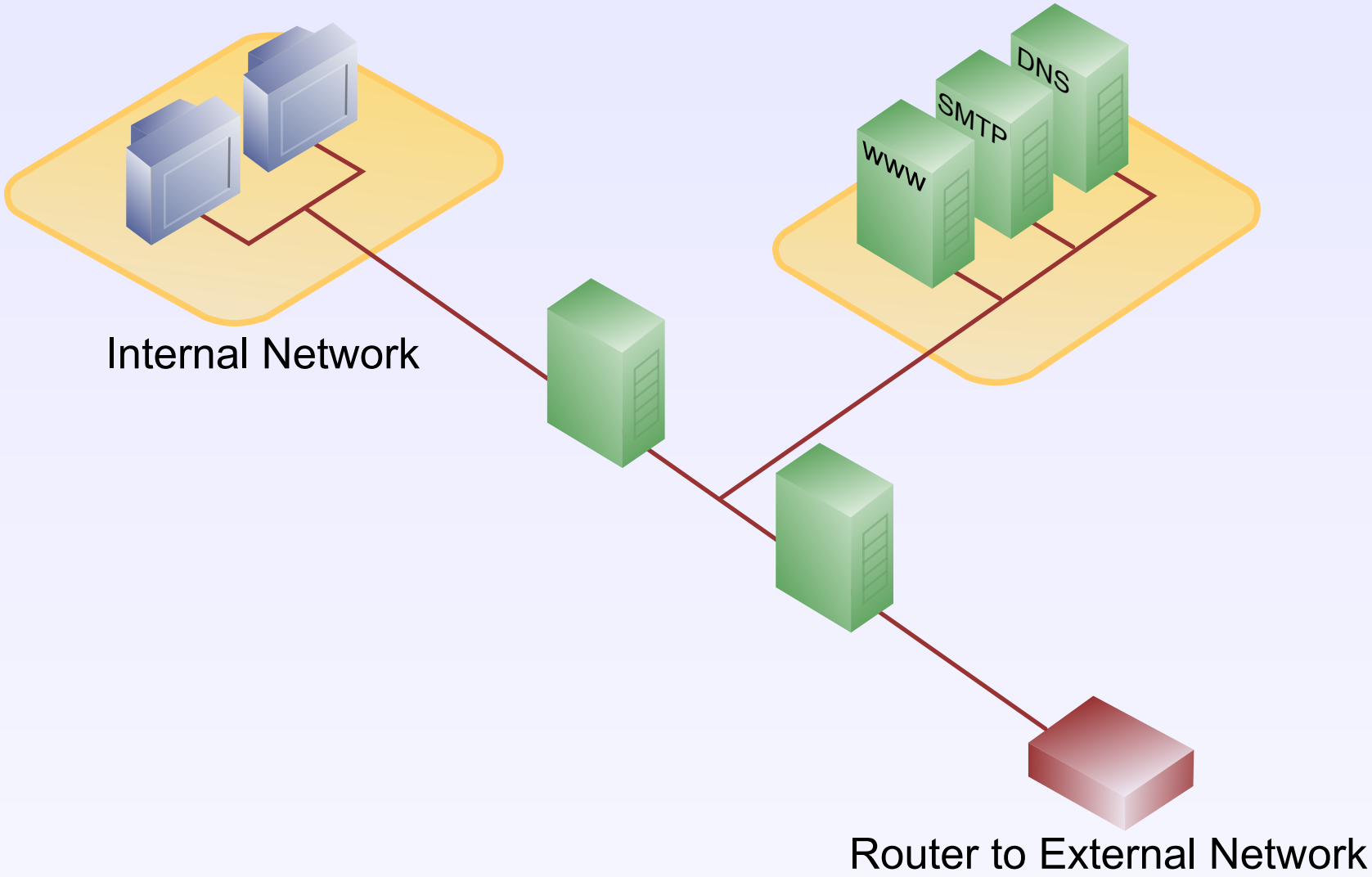
- Les connexions à la DMZ sont autorisées de n'importe où.
- Les connexions à partir de la DMZ peuvent être autorisées vers l'extérieur.
- Les connexions vers le réseau privé sont interdites.

DMZ avec 1 firewall



source : Wikipedia

DMZ avec 2 firewalls



source : Wikipedia