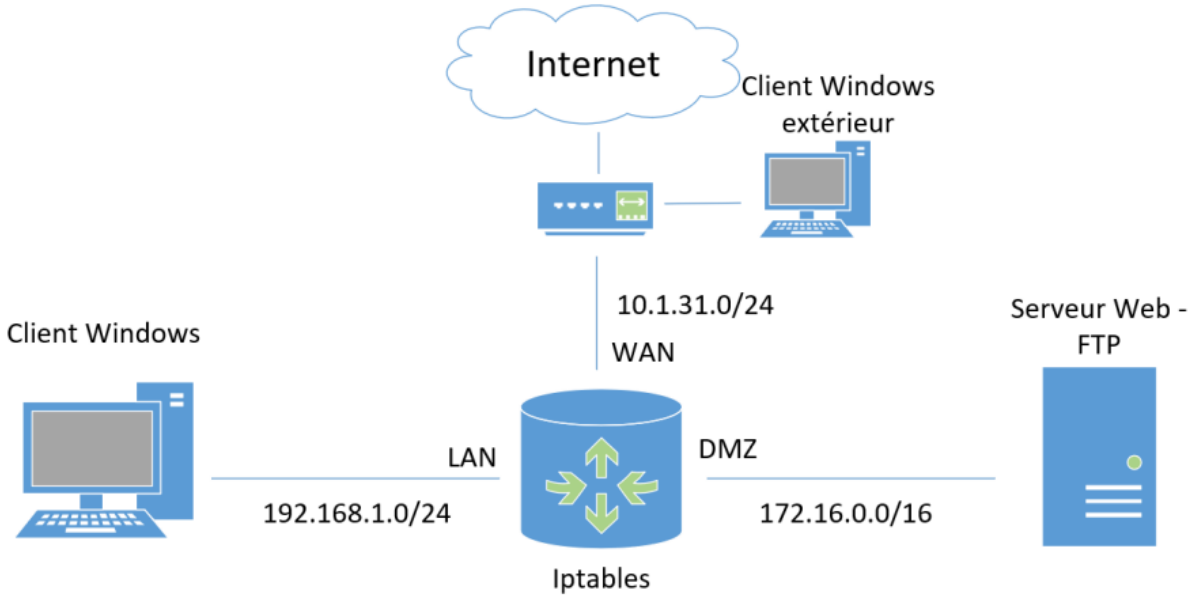
Sécurité des réseaux : Netfilter & Palo Alto

Grégoire Roumache

Avril 2021

1 Netfilter



- Configurations réseaux (dns = 208.67.222.123 - opendns):
  1. Windows (réseau interne - lan):

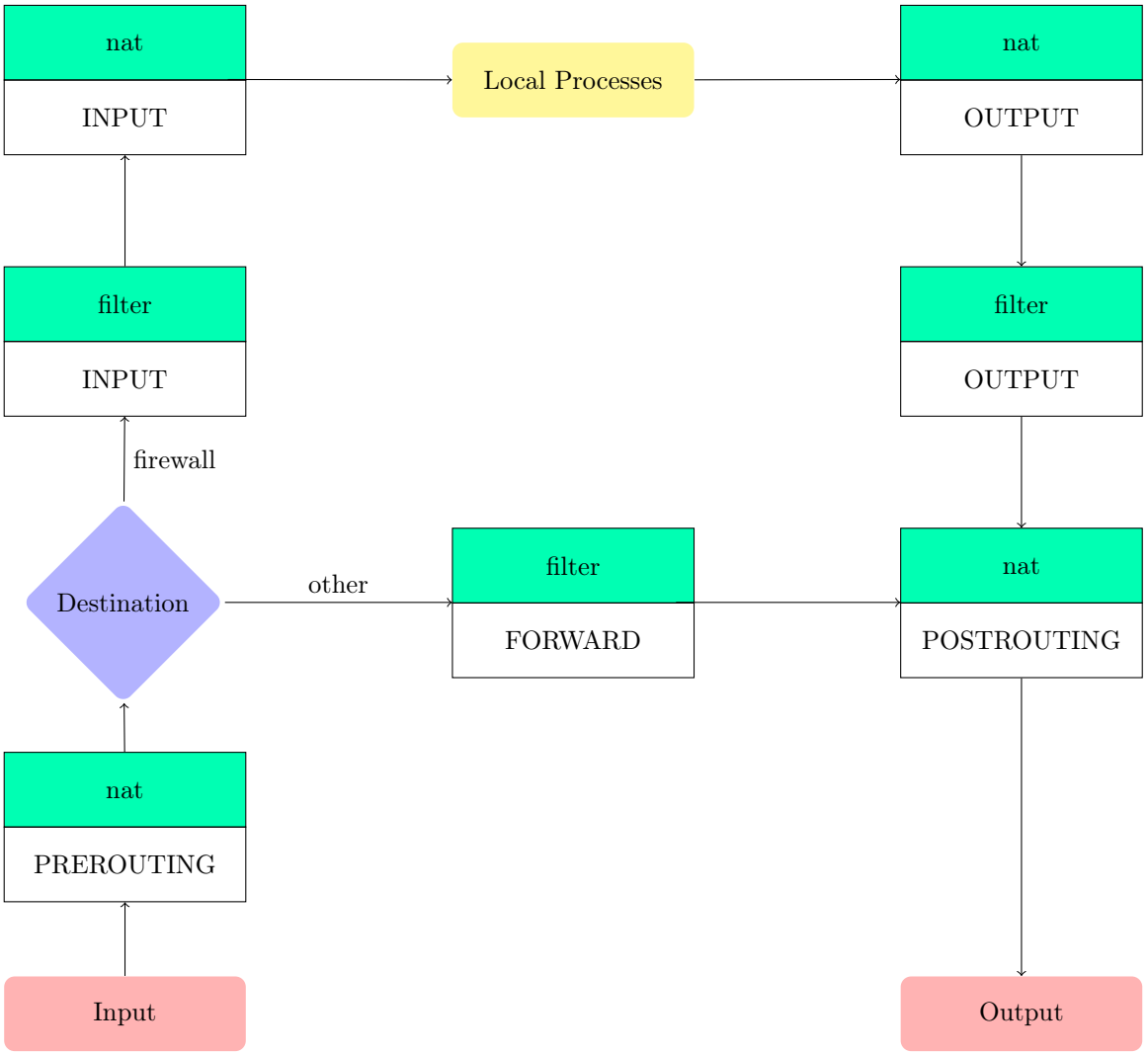
ip	192.168.1.2
netmask	255.255.255.0
gateway	192.168.1.1

  2. Serveur (réseau interne - dmz):

ip	172.16.0.2
netmask	255.255.0.0
gateway	172.16.0.1

  3. Firewall:

enp0s3	/	dhcp	(accès par pont)
enp0s8	ip	192.168.1.1	
enp0s8	netmask	255.255.255.0	(réseau interne - lan)
enp0s8	gateway	/	
enp0s9	ip	172.16.0.1	
enp0s9	netmask	255.255.0.0	(réseau interne - dmz)
enp0s9	gateway	/	



- Tables et chaines:
  1. Filter
     - input/ouput = paquets en provenance/destination du parefeu
     - forward = paquets traversant le parefeu
  2. Nat
     - input/ouput = paquets en provenance/destination du parefeu
     - prerouting/postrouting = modification des ip dans les paquets pour le nat
- Tableau de règles (table nat):

chain	**type**	**input interface**	**output interface**	**input ip**	**output ip**	**protocole**	**port**
postrouting	snat	`<lan>`	`<wan>`	`<wan>`	/	/	/
postrouting	snat	`<dmz>`	`<wan>`	`<wan>`	/	/	/
prerouting	dnat	`<wan>`	`<dmz>`	/	`<dmz>`	tcp	20,21,80
prerouting	dnat	`<wan>`	`<dmz>`	/	`<dmz>`	tcp	61337:22

– Tableau de règles (table filter):

chain	priority	source ip	source port	dest. ip	dest. port	protocol	ouput interface	permission
input	999	*	*	*	*	*	*	reject
output	999	*	*	*	*	*	*	reject
forward	999	*	*	*	*	*	*	reject
input	1	*	*	*	*	*	lo	accept
output	1	*	*	*	*	*	lo	accept
forward	1	<lan>	*	*	443	tcp	<wan>	accept
forward	1	<lan>	*	<dns>	53	udp	<wan>	accept
forward	1	<lan>	*	*	*	icmp	<dmz>	accept
forward	1	<lan>	*	*	20,21,80	tcp	<dmz>	accept
forward	1	<wan>	*	*	20,21,80	tcp	<dmz>	accept
forward	1	<wan>	*	*	22	tcp	<dmz>	accept
input	1	<wan>	*	<firewall>	*	icmp	/	accept
input	1	<lan>	*	<firewall>	*	icmp	/	accept
input	1	<dmz>	*	<firewall>	*	icmp	/	accept
input	1	<wan>	*	<firewall>	22	tcp	/	accept

Remarque: on n'autorise pas le protocole https directement mais le protocole tcp et le port 443 car le contenu est chiffré.

– Afficher les règles iptables:

  – `iptables -t filter -L [<chaine>] --line-numbers -n`
  – `iptables -t nat -L [<chaine>] --line-numbers -n`

Remarque: dès qu'un paquet correspond à une règle, cette règle s'applique et les autres sont ignorées.

– Pour transformer la machine debian en routeur, il faut décommenter la ligne suivante dans `/etc/sysctl.conf`:

```
net.ipv4.ip_forward=1
```

Remarque: il faut ajouter des default gateways sur toutes les machines (sauf si dhcp).

– Utiliser conntrack pour permettre le trafic provenant de connexions déjà établies:

  – Installer conntrack: `apt install conntrack`
  – Lister les connexions: `conntrack -L`
  – Autoriser les connexions établies/liées:

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

– Script pour flush les iptables et autoriser les connexions déjà établies:

```
#!/bin/bash
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -t nat -F INPUT
iptables -t nat -F OUTPUT
```

```
iptables -t nat -F PREROUTING
iptables -t nat -F POSTROUTING
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

- Mettre en place le nat:
  - Source nat:
    ```
    iptables -t nat -A POSTROUTING -j SNAT \
        -o <output_interface> --to-source <ip_publique>
    ```
  - Source nat avec masquerade:
    ```
    iptables -t nat -A POSTROUTING -j MASQUERADE \
        --out-interface <output_interface>
    ```
  - Destination nat (pour tous les ports & tous les protocoles):
    ```
    iptables -t nat -A PREROUTING -j DNAT \
        -i <input_interface> --to-destination <ip_privée>
    ```
  - Destination nat (pour un port & un protocole):
    ```
    iptables -t nat -A PREROUTING -j DNAT \
        -i <input_interface> --to-destination <ip_privée> \
        -p tcp --dport 80
    ```

- Script pour mettre en place le nat:

```
#!/bin/bash
iptables -t nat -A POSTROUTING -j MASQUERADE \  # SNAT
    --out-interface enp0s3                      # SNAT

iptables -t nat -A PREROUTING -j DNAT \         # ftp,web
    -i enp0s3 --to-destination 172.16.0.2 \     # ftp,web
    -p tcp --dport 20,21,80                     # ftp,web

iptables -t nat -A PREROUTING -j DNAT \         # ssh
    -i enp0s3 --to-destination 172.16.0.2:22 \  # ssh
    -p tcp --dport 61337                        # ssh
```

- Créer une règle iptables:

```
iptables -A <chain>        # <chain>    = INPUT  | OUTPUT | FORWARD
-j <target>                # <target>   = ACCEPT | REJECT | DROP
-p <protocol>              # <protocol> = tcp    | udp    | icmp
-i <input_interface>   -o <output_interface>
-s <source_ip_address> -d <destination_ip_address>
--sport <source_port>  --dport <destination_port>
```

- Script pour les tables filter:

```
#!/bin/bash

#### Tout autoriser sur l'interface loopback
iptables -A INPUT  -i lo -j ACCEPT
iptables -A OUTPUT -i lo -j ACCEPT

#### LAN -> WAN
iptables -A FORWARD -i enp0s8 -o enp0s3 -p tcp --dport 443 -j ACCEPT
```

```
iptables -A FORWARD -i enp0s8 -o enp0s3 -p udp --dport 53  -j ACCEPT -d 208.67.222.123

#### LAN -> DMZ
iptables -A FORWARD -i enp0s8 -o enp0s9 -p icmp -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p tcp  -j ACCEPT --dport 20,21,80

#### WAN -> DMZ
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 20,21,80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 22       -j ACCEPT

#### ANY -> Firewall
iptables -A INPUT -i enp0s3 -d <firewall>  -p icmp -j ACCEPT
iptables -A INPUT -i enp0s8 -d 192.168.1.1 -p icmp -j ACCEPT
iptables -A INPUT -i enp0s9 -d 172.16.0.1  -p icmp -j ACCEPT

#### Client externe -> Firewall
iptables -A INPUT -i enp0s3 -d <firewall> -p tcp --dport 22 -j ACCEPT

#### Tout interdire
iptables -A INPUT   -j REJECT
iptables -A OUTPUT  -j REJECT
iptables -A FORWARD -j REJECT
```

– Rendre les iptables persistentes

  – `apt install iptables-persistent`
  – `iptables-save`
  – `systemctl restart networking`

2 Palo Alto – de la connexion au vpn jusqu'à la connexion au ftp

Attention !

- pour quitter la machine vmware, utiliser `ctrl+alt gauche`
- il faut *commit* tous les changements avant qu'ils soient effectifs

1. Se connecter au VPN:
   (a) faire un clic droit sur l'icône *openvpngui* dans la barre d'outils windows
   (b) importer le fichier de configuration et après, cliquer sur *connecter*
   (c) se connecter avec:
      - login = Student@irti.iesn.be
      - password = voir moodle
2. Lancer les machines:
   (a) se rendre sur `https://10.1.31.191/`, et se connecter avec:
      - login = Student@irti.iesn.be
      - password = Tigrou007=
   (b) dans le menu de gauche, cliquer sur la deuxième icône, puis cliquer sur le nom de la vm à lancer
   (c) cliquer sur *actions*, à droite du nom de la vm, et lancer la machine
   (d) cliquer sur *lancer remote console*, pour ouvrir la machine dans vmware
   (e) aller sur `https://<ip_mgmt>/` dans le navigateur de la machine hôte

   Remarque: il faut absolument utiliser *https*.
3. Configuration de base de palo alto:
   (a) se connecter à la machine palo alto avec:
      - login = admin
      - password = Tigrou007
   (b) changer la langue vers l'anglais (en bas à droite)
   (c) exporter la configuration vierge en allant sur *device/setup/operations/export*
4. Configuration réseau de palo alto:
   (a) créer une *zone*: aller dans *network/zones*
      - name = outside
      - type = layer3
   (b) créer des *interface management profile*: aller dans *network/network profiles/interface mgmt*
      - name = ping-and-response-pages
      - network services = ping, response pages
      - name = ping-only
      - network services = ping
   (c) ajouter des sous-interfaces ethernet: aller dans *network/interfaces/ethernet*
      - ethernet1/2
      - interface type = layer3
      - config/security zone = new zone
         - name = inside
         - type = layer3

- ipv4/ip = <ip_guide_de_connexion>
- advanced/management profile = ping-and-response-pages

- ethernet1/3
- interface type = layer3
- config/security zone = new zone
  - name = outside
  - type = layer3
- ipv4/ip = <ip_guide_de_connexion>
- advanced/management profile = ping-only

(d) faire du troubleshooting: aller dans *device/troubleshooting*

- select test = ping
- host = 1.1.1.1
- cliquer sur *execute*
- cliquer sur *ping 1.1.1.1*, dans la colonne *test result*

5. Configurer le snat sur palo alto:

(a) créer des tags: aller dans *objects/tags*

- name = danger
- color = purple

- name = egress (egress = traffic vers l'extérieur)
- color = blue

- name = dmz
- color = orange

- name = internal
- color = yellow

(b) créer une politique SNAT (= source nat): aller dans *policies/nat*

- general/name = source-egress-outside
- general/tags = egress
- general/group rules by tag = egress
- original packet/source zone = inside
- original packet/destination zone = outside
- original packet/destination interface = ethernet1/1
- translated packet/translation type = dynamic ip and port
- translated packet/address type = interface address
- translated packet/interface = ethernet1/1

(c) créer des règles de politique de sécurité: aller dans *policies/nat*

- general/name = egress-outside
- general/tags = egress
- general/group rules by tag = egress
- source/source zone = inside
- destination/destination zone = outside

(d) vérifier la connexion à internet sur la machine windows (elle doit être configurée en statique)

6. Configurer le service ftp sur palo alto (dnat):

(a) créer le service ftp: aller dans *objects/services*

- name = service-ftp
- destination port = 20-21
- tags = dmz

(b) créer une politique dnat (= destination nat): aller dans *policies/nat*

- general/name = destination-dmz-ftp
- general/tags = internal
- general/group rules by tag = internal
- original packet/source zone = inside
- original packet/destination zone = inside
- original packet/destination interface = ethernet1/2
- original packet/service = service-ftp
- original packet/destination address = **adresse ethernet1/2**
- translated packet/static ip = static ip
- translated packet/translated address = **adresse serveur ftp**

Remarque: original packet/destination address $\Longrightarrow$ translated packet/translated address

(c) créer des règles de politique de sécurité: aller dans *policies/nat*

- general/name = internal-dmz-ftp
- general/tags = internal
- general/group rules by tag = internal
- source/source zone = inside
- destination/destination zone = dmz
- destination/destination address = **adresse ethernet1/2**
- services url category/service = service-ftp

(d) vérifier la connexion au serveur ftp sur la machine windows: `ftp://<ip_firewall>/` (ethernet1/2)