# Fiche technique :

# mise en place d'un pare-feu

# Table des matières

# 1. Montage réseau

## a) *Maquette réelle*

Le pare-feu se positionne au centre du réseau, de telle sorte qu'il soit connecté au WAN, à la DMZ et au LAN :

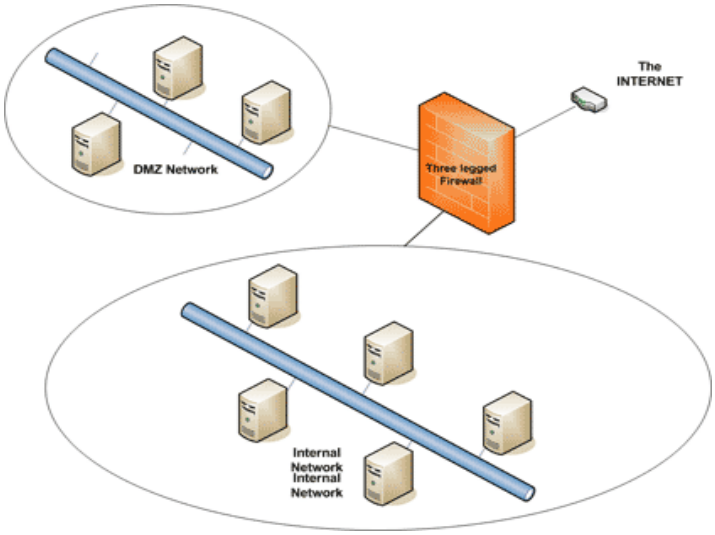


***Illustration 1: Installation d'un pare-feu***

## b) *Maquette virtuelle*

Dans VmWare, le WAN sera émulé par le switch virtuel « NAT » et les deux autres interfaces seront branchées sur des switchs internes (vmnet).

On doit avoir la configuration suivante :

| Réseau | Interface | Vmnet |
|---|---|---|
| WAN | eth0 | NAT |
| DMZ | eth1 | Vmnet3 (entre 2 et 7) |
| LAN | eth2 | Vmnet4 (entre 2 et 7) |

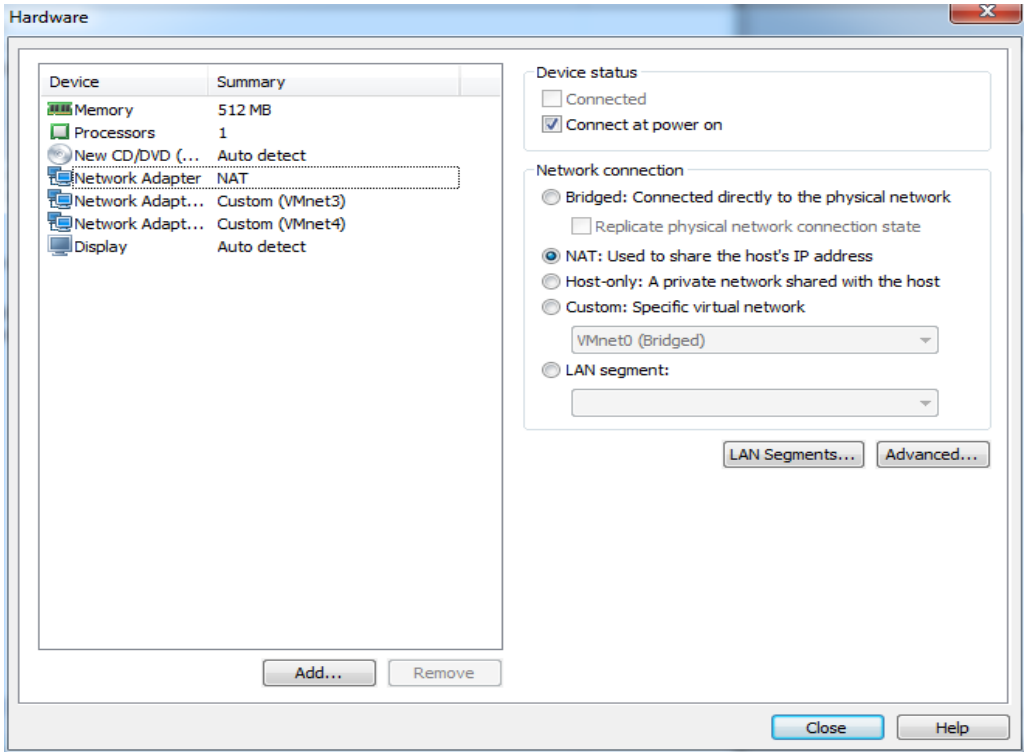


***Illustration 2: Exemple de configuration de machine virtuelle***

# 2. Configuration sous Linux

## *a) Configuration des interfaces réseaux*

Sous CentOS, la configuration réseau se trouve dans le répertoire :

/etc/sysconfig/network-scripts

Il faut donc se déplacer dans ce répertoire :

```
# cd /etc/sysconfig/network-scripts
```

### ***Connection à Internet***

Puis éditer le fichier « ifcfg-eth0 » comme suit :

```
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=dhcp
```

Il faut maintenant activer l'interface grâce à la commande suivante :

```
# ifup eth0
```

A ce stade votre machine virtuelle devrait être connectée à Internet. Vous pouvez le vérifier grâce à la commande ping (ping google.fr)

***Astuce***

Pour pouvoir « copier/coller » les lignes de commandes, vous pouvez utiliser Putty. Pour cela, vous avez besoin de l'adresse réseau de votre pare-feu côté WAN :

```
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen
1000
    link/ether 00:0c:29:2d:c9:a5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.130/24 brd 192.168.100.255 scope global eth0
    inet6 fe80::20c:29ff:fe2d:c9a5/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:0c:29:2d:c9:af brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:0c:29:2d:c9:b9 brd ff:ff:ff:ff:ff:ff
```

Ici, l'interface eth0 a l'adresse 192.168.100.130, ce qui n'est pas forcement le cas de votre machine virtuelle !

Ouvrez Putty, puis utilisez l'adresse IP précédemment obtenue :

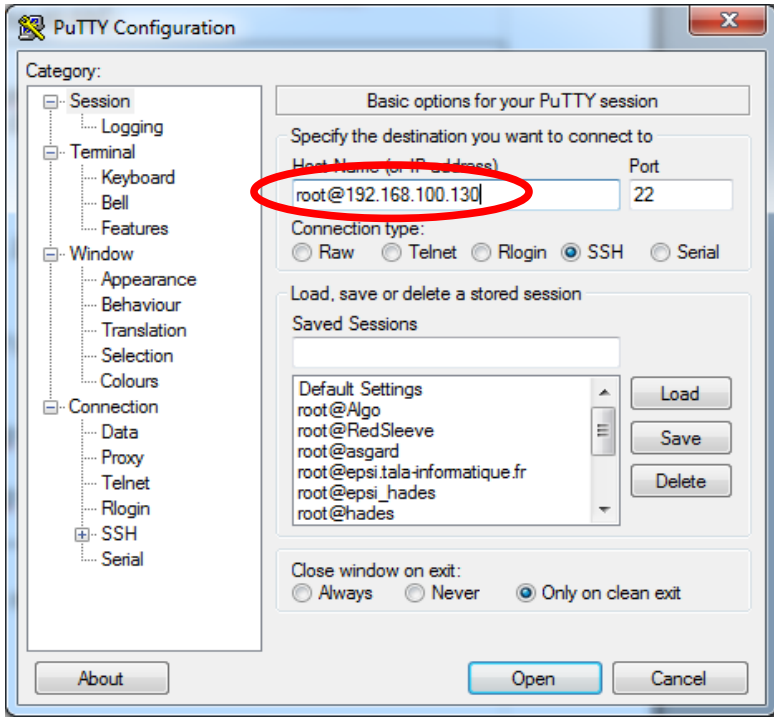


***Illustration 3: Utilisation de Putty***

### *Activation de la DMZ et du LAN*

Les deux autres interfaces doivent permettre aux machines de la DMZ et du LAN de pouvoir accéder à Internet. Pour ce faire, il nous faut attribuer des adresses IP :

- éditez le fichier « ifcfg-eth1 » comme suit :

```
DEVICE=eth1
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=192.168.1.254
NETMASK=255.255.255.0
```

- éditez le fichier « ifcfg-eth2 » comme suit :

```
DEVICE=eth2
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=192.168.2.254
NETMASK=255.255.255.0
```

Vous pouvez choisir un autre réseau que 192.168.1.0/24 et 192.168.2.0/24.

Il ne reste plus qu'à activer les deux interfaces :

```
#ifup eth1
#ifup eth2
```

## *b) Activation du routage*

Il faut maintenant activer le routage pour que les paquets envoyés par les machines de la DMZ et du LAN puissent « sortir » sur Internet. Pour cela, il faut changer ligne suivante dans le fichier /etc/sysctl.conf :

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

Il ne reste plus qu'à recharger les paramètres du noyau pour que la modification soit effective :

```
#sysctl -p
```

A ce stade, les paquets peuvent quitter le LAN et la DMZ, seulement, personne ne connaît nos réseaux 192.168.1.0/24 et 192.168.2.0/24 et il faut donc les camoufler (utiliser le NAT)

## *c) Activation du NAT*

Pour activer le NAT il faut utiliser Iptables. Tous les paquets que l'on doit « nater » sortent par l'interface eth0, c'est donc ce paramètre discriminant que nous allons utiliser :

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Maintenant que le NAT est activé, il faut regarder la chaîne **FORWARD** de la table **filter** pour s'assurer que les paquets passent :

```
# iptables -nvL FORWARD
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-
host-prohibited
```

On peut constater que la seule règle de la chaîne **FORWARD** rejette tous les paquets. Nous allons la supprimer :

```
#iptables -F FORWARD
```

Comme après chaque modification des règles du pare-feu, il faut sauvgarder :

```
#service iptables save
```

Les machines de la DMZ et du LAN peuvent maintenant accéder à Internet, seulement il faut leur paramétrer une configuration de niveau 3 (adresse IP). Nous allons utiliser le service DHCP pour le faire à notre place !

## d) Paramétrage du DHCP

### Installation

Pour installer le service DHCP, rien de plus simple :

```
#yum -y install dhcp
```

### Configuration

Pour rappel, nous devons fournir des adresses IP au LAN et à la DMZ. Cela va se traduire par deux blocs de configuration dans le fichier **/etc/dhcp/dhcpd.conf :**

```
subnet 192.168.1.0 netmask 255.255.255.0{
        authoritative;
        option routers 192.168.1.254;
        option domain-name-servers 8.8.8.8;
        range 192.168.1.10 192.168.1.50;
}
subnet 192.168.2.0 netmask 255.255.255.0{
        authoritative;
        option routers 192.168.2.254;
        option domain-name-servers 8.8.8.8;
        range 192.168.2.10 192.168.2.50;
}
```

### Démarrage et enregistrement dans le chargeur de démarrage

```
#service dhcpd start
#chkconfig dhcpd on
```

# Annexes

## 3. Index des illustrations

### Index des illustrations