Configuration du pare-feu

Objectif

Cette documentation à pour but d'expliquer comment configurer un pare-feu en détaillant chaque étapes.

Notre machine contient 2 cartes contrôleurs de réseau plus celle de la carte mère. Le système est un Debian 8 (jessy).

La carte eth0 est reliée au LAN (Coté 172.31.1.0/24).
La carte eth1 est reliée à la DMZ (Coté 192.168.80.0/24).
La carte eth2 est reliée à internet (Coté 0.0.0.0[172.16.2.0/24]).

Routage

Tout d'abord, on modifie le fichier *sysctl.conf*, pour faire en sorte que lors du démarrage de la machine, le routage sera toujours actif.

```
# vim /etc/sysctl.conf
#Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#reboot
```

Pour notre part, les routes par défauts n'étaient pas bonnes. Donc on a créer un fichier qu'on a ensuite mis dans le dossier “/etc/init.d/”

```
#!/bin/sh
### BEGIN INIT INFO
# Provides:          route restore
# Required-Start:
# Required-Stop:
# Should-Start:
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Set route based on the line in this file
# Description:
### END INIT INFO
# ==== ROUTING ==== #
# ADD
route add -net 192.168.222.0/24 gw 172.16.2.245 dev eth2
route add -net 192.168.0.0/16 gw 172.31.1.1 dev eth0
route del default gw 172.31.1.1
route add default gw 172.16.2.254 dev eth2
route add -net 172.25.0.0/24 gw 172.31.1.1 dev eth0
# DEL
```

```
route del -net 169.254.0.0/16
```

NAT

Dans cette partie, on va cacher toutes les adresses IP du LAN par l'IP de la carte **eth2**.

```
# iptables -A POSTROUTING -o eth2 -j MASQUERADE -m comment --comment
"Translation d\'adresse pour internet"
```

Ensuite, Nous allons rediriger les paquets entrant sur la carte eth2 sur le port 80 vers la DMZ sur le port 8080.

```
# iptables -A PREROUTING -i eth2 -p tcp -m tcp --dport 80 -j DNAT --to-
destination 192.168.80.10:8080
```

Filtrage

Table de Filtrage

N° Règle	Interface D'arrivé	IP source	Port source	IP dest	Port dest	Protocole	Action	Description
1	172.16.2.1	*	*	192.168.80.10/3	8080	tcp	Accept	Internet vers DMZ (NAT)
2	172.31.1.2	192.168.30.0/24	*	192.168.80.10/3	8080	tcp	Accept	Vlan user vers DMZ
3	172.31.1.2	192.168.10.0/24	*	192.168.80.10/3	8080	tcp	Accept	Vlan Admin vers DMZ
10	192.168.80.254	192.168.80.10/32	*	172.25.0.110/32	8081	tcp	Accept	DMZ vers VLAN serveur
20	172.31.1.2	192.168.30.0/24	*	*	*	*	Accept	Vlan user vers internet
21	172.31.1.2	192.168.10.0/2	*	*	*	*	Accept	Vlan Admin vers inernet
30	172.31.1.2	192.168.10.0/24	*	172.31.1.2/32	SSH	tcp	Accept	Autorise le SSH sur le parefeu
31	172.31.1.2	192.168.10.0/24	*	192.168.80.10/3	SSH	tcp	Accept	Autorise le SSH pour la DMZ
		*	*	*	*	*	Reject	Par défaut on refuse

Commande sous Iptables

En entrée(INPUT), sur l'une des cartes réseau du pare-feu :

```
# iptables -A INPUT -i eth0 -p tcp -m tcp --dport 22 -m comment --comment
"__Autorise le SSH depuis le LAN__" -j ACCEPT
# iptables -A INPUT -i eth2 -p tcp -m tcp --dport 80 -m comment --comment
"__Autorise le HTTP depuis l\'exterieur__" -j ACCEPT
# iptables -A INPUT -p icmp -m comment --comment "__Autorise le ping__" -j
ACCEPT
# iptables -P INPUT DROP
```

Lorsqu'il y a un paquet qui doit traverser le pare-feu, il passera pas la table FORWARD :

```
# iptables -A FORWARD -i eth0 -o eth2 -p udp -m udp --dport 53 -m comment --
comment "__Autorise la communication du LAN vers le DNS__" -j ACCEPT
```

```
# iptables -A FORWARD -i eth2 -o eth0 -p udp -m udp --sport 53 -m comment --
comment "__Autorise la communication du DNS vers le LAN__" -j ACCEPT
# iptables -A FORWARD -i eth0 -o eth2 -p tcp -m tcp --dport 3128 -m comment
--comment "__Autorise la communication du LAN vers le proxy__" -j ACCEPT
# iptables -A FORWARD -i eth2 -o eth0 -p tcp -m tcp --sport 3128 -m comment
--comment "__Autorise la communication du proxy vers le LAN__" -j ACCEPT
# iptables -A FORWARD -p icmp -m comment --comment "__Autorise le ping__" -j
ACCEPT
# iptables -A FORWARD -i eth1 -o eth0 -p tcp -m tcp --dport 8070 -m comment
--comment "__Autorise l'aller du serveur WEB vers le VLAN sur le port
8070(Serveur d\'application)__" -j ACCEPT
# iptables -A FORWARD -i eth0 -o eth1 -p tcp -m tcp --sport 8070 -m comment
--comment "__Autorise le retour du VLAN  vers la DMZ sur le port
8070(Serveur d\'application)__"-j ACCEPT
# iptables -A FORWARD -i eth2 -o eth1 -p tcp -m tcp --dport 8080 -m comment
--comment "__Autorise l'aller du pare-feu (NAT) vers la DMZ sur le port
8080(Serveur WEB)__" -j ACCEPT
# iptables -A FORWARD -i eth1 -o eth2 -p tcp -m tcp --sport 8080 -m comment
--comment "__Autorise le retour de la DMZ vers le pare-feu sur le port
8080(Serveur WEB)__" -j ACCEPT
# iptables -P FORWARD DROP
```