NAT : Accéder à un service LXC du réseau fermé depuis l'extérieur (réseau de l'école)

Problématique

Nous illustrerons notre problématique à travers un exemple. Comme vous le savez, les services du GInfo sont confinés dans des Linux Containers, la plupart étant sur BOR. Ces LXC ne sont pas accessibles depuis le réseau du GINFO (16.0) mais uniquement depuis BOR où ils sont confinés dans un réseau (10.61.15.0) (sauf exception). Le but de étant de pouvoir accéder aux services de ces LXC en passant par un intermédiaire qui lui est accessible depuis l'extérieur (l'extérieur désigne ici le réseau du GInfo ou réseau interne de l'école)

Par exemple, si l'on veut accéder au serveur WEB hébergé sur BOR en 10.61.15.26, on doit pouvoir, depuis l'extérieur (réseau de l'école et du GInfo), taper dans notre navigateur 10.61.16.10 et avoir accès au serveur WEB.

Dans notre cas, c'est BOR qui effectuera le routage. On a choisi de ne pas mettre ces règles sur Odin pour séparer le serveur DNS/DHCP de BOR. Comme ça si Odin tombe (c'est une vieille machine), les services seront toujours en ligne.

Dans la pratique : ouvrir un port pour un service

Bor étant déjà configuré, pour rediriger un port tcp vers un service un ajoutera simplement une règle NAT comme ceci : (**manipulation à effectuer bien entendu sur BOR et NON sur le LXC**)

```
$> iptables -t nat -A PREROUTING -p tcp -i br0 --dport 80 -j DNAT --to-destination 10.61.15.26:80
```

Cette règle redirige tout le flux entrant en tcp sur le port 80 de BOR vers le LXC du réseau fermé 10.61.15.26:80, qui héberge apache. On fera la même règle pour le port 443.

A chaque fois qu'on rajoute une règle, on pense à rendre cette règle persistante au démarrage en sauvant les règles dans le fichier des iptables persistantes :

```
$> sudo iptables-save > /etc/iptables/rules.v4
```

Pour que cela marche, il faut que le paquet suivant soit installé :

```
$> sudo apt-get install iptables-persistent
```

Explications de la configuration de BOR

Cette configuration revient à considérer que BOR est un routeur. Seul lui est accessible depuis

l'extérieur et si l'on veut accéder à un service présent sur une LXC, on doit ouvrir des ports.

Voici la configuration réseau de BOR :

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# INTERFACE ACCESSIBLE EXTERIEUR
auto br0
iface br0 inet dhcp
    bridge-ifaces eno1
    bridge-ports eno1
    up ifconfig eno1 up
    address 10.61.16.10
    network 10.61.16.0
    netmask 255.255.255.0
    gateway 10.61.16.254

iface eno1 inet manual

# INTERFACE FERMEE EXTERIEUR DMZ
auto br1
iface br1 inet static
    address 10.61.15.1
    netmask 255.255.255.0
    network 10.61.15.0
    broadcast 10.61.15.255
    bridge_ports none
```

Bor dispose de deux interfaces (des bridges) :

→ **br0** : celle utilisée pour communiquer avec internet (10.61.16.10)

→ **br1** : celle utilisée par les LXC du réseau (10.61.15.0/24)

Pour “faire le lien” entre ces deux interfaces, et rediriger des ports, on active le IP FORWARDING pour tout ce qui entre et sort de br1. (c'est capital, on doit refuser le forwarding sauf pour cette interface). A la fin, on obtient une suite de commandes pour que cette configuration fonctionne (ces commandes sont temporaires et écrasées au démarrage)

/etc/adefinir

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -s 10.61.15.0/24 -j MASQUERADE
iptables -P FORWARD DROP
iptables -A FORWARD -i br1 -o br0 -j ACCEPT
iptables -A FORWARD -i br0 -o br1 -j ACCEPT
```

```
#Redirections des ports pour accéder aux services de l'extérieur
#Ports WEB
iptables -t nat -A PREROUTING -p tcp -i br0 --dport 2505 -j DNAT --to-destination 10.61.15.26:22
#Ports SAMBA
iptables -t nat -A PREROUTING -p tcp -i br0 --dport 137 -j DNAT --to-destination 10.61.15.24:137
iptables -t nat -A PREROUTING -p tcp -i br0 --dport 138 -j DNAT --to-destination 10.61.15.24:138
iptables -t nat -A PREROUTING -p udp -i br0 --dport 137 -j DNAT --to-destination 10.61.15.24:137
iptables -t nat -A PREROUTING -p udp -i br0 --dport 138 -j DNAT --to-destination 10.61.15.24:138
iptables -t nat -A PREROUTING -p tcp -i br0 --dport 139 -j DNAT --to-destination 10.61.15.24:139
iptables -t nat -A PREROUTING -p tcp -i br0 --dport 445 -j DNAT --to-destination 10.61.15.24:445
```

Pour rendre les règles iptables permanentes, voir plus haut de ce tutoriel (iptables-persitent). Pour ce qui est de l'ip forwarding, il faut l'activer dans `/etc/sysctl.conf` en dé-commentant la ligne :

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

From:
https://wiki.centrale-med.fr/ginfo/ - **Wiki GInfo**

Permanent link:
https://wiki.centrale-med.fr/ginfo/musee:tutoriels:ouvrir_un_service_lxc_depuis_de_l_exterieur

Last update: **15/10/2018 20:43**