Subject: Problème insoluble
Posted by anotherservice on Wed, 20 Jul 2011 08:08:45 GMT
View Forum Message <> Reply to Message

Bonjour à tous,

Mon premier message sur ce forum, après une semaine de cheveux arrachés, je me tourne vers vous pour un problème qui m'échappe complètement.

Voici ma configuration actuelle (simplifiée pour le case) :

- Un noeud Proxmox, à jour avec :

vmbr0 (bridge interne indépendant)
vmbr1 (bridge externe avec eth0 dedans) et la configuration IPV4 fixe du serveur dédié suivante :

```
auto vmbr1
iface vmbr1 inet static
        address 46.105.111.210
        netmask 255.255.255.0
        network 46.105.111.0
        broadcast 46.105.111.255
        gateway 46.105.111.254
        bridge_ports eth0
        bridge_stp off
        bridge_fd 0
```

Jusqu'ici tout fonctionne parfaitement.

- Une machine virtuelle OpenVZ (container) avec des interface en veth (pas de venet).
Une première interface eth0, bridgée avec vmbr0 sur l'interne, config IP en DHCP (sans gateway par défaut) provenant d'une autre VM, aucun souci, fonctionnement optimal.
Une seconde interface eth1, bridgée avec vmbr1 sur l'externe, config IP fixée avec une IP failover et la config suivante :

```
auto eth1
iface eth1 inet static
        address 91.121.49.65
        netmask 255.255.255.255
        broadcast 91.121.49.65
        post-up route add 46.105.111.254 dev eth1
        post-up route add default gw 46.105.111.254
        post-down route del 46.105.111.254 dev eth1
        post-down route del default gw 46.105.111.254
```

Pour que cela fonctionne, j'ai une adresse MAC virtuelle créée dans l'interface OVH :

02:00:00:2a:21:95 proxy96041 91.121.49.65 ovh

Pour configurer cette MAC virtuelle, le fichier de configuration du container contient :

NETIF="ifname=eth0,bridge=vmbr0,mac=00:10:20:25:6E:00,host_ifname=veth96041.0,host_mac=00:18:51:44:91:73;ifname=eth1,bridge=vmbr1,mac=02:00:00:2a:21:95,host_ifname=veth96041.1,host_mac=00:18:51:E5:0E:58

Jusque là tout va bien. Nous voilà au problème.

1) Sans rien faire de plus que ça, j'arrive à pinger la machine virtuelle sur son IP, mais sans vraiment y arriver.

J'effectue un ping depuis mon PC personnel à la maison :

C:\ping -t 91.121.49.65

Envoi d'une requête 'Ping' 91.121.49.65 avec 32 octets de données*:
Réponse de 91.121.49.65*: octets=32 temps=49 ms TTL=57
Réponse de 91.121.49.65*: octets=32 temps=45 ms TTL=57
Réponse de 91.121.49.65*: octets=32 temps=46 ms TTL=57
Réponse de 91.121.49.65*: octets=32 temps=45 ms TTL=57
Réponse de 91.121.49.65*: octets=32 temps=45 ms TTL=57

Sur le noeud physique :

root@on-005:/etc/vz/conf# tcpdump -i vmbr1 host 91.121.49.65
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmbr1, link-type EN10MB (Ethernet), capture size 96 bytes
02:37:49.332028 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2201, length 40
02:37:49.332083 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2201, length 40
02:37:50.332827 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2202, length 40
02:37:50.332861 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2202, length 40
02:37:51.335764 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2203, length 40
02:37:51.335798 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2203, length 40
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel

Mais sur la VM rien, le calme plat :

root@proxy-96041:/# tcpdump -i eth1 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes

Et même, le tcpdump freeze !

Comme indiqué sur la documentation OpenVZ, je rajoute alors la route de l'IP fail-over sur le bridge vmbr1 (et ceci à chaque start/stop de la VM) :

#!/bin/bash
ip route add 91.121.49.65 dev vmbr1

Et là miracle, tout apparaît nickel, mais avec un énorme hic (et c'est ici que j'espère votre éclairage) :

Sur le noeud physique :

root@on-005:/etc/vz/conf# tcpdump -i vmbr1 host 91.121.49.65
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmbr1, link-type EN10MB (Ethernet), capture size 96 bytes
02:54:16.247584 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2924, length 40
02:54:16.247621 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2924, length 40
02:54:17.265167 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2925, length 40
02:54:17.265196 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2925, length 40
02:54:18.250581 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2926, length 40
02:54:18.250638 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2926, length 40
02:54:19.250505 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2927, length 40
02:54:19.250545 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2927, length 40
02:54:20.252028 IP 164.218.11.109.rev.sfr.net > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2928, length 40
02:54:20.252066 IP 91-121-49-65.ovh.net > 164.218.11.109.rev.sfr.net: ICMP echo reply, id 256, seq 2928, length 40

Mais sur la VM, il croit parler au noeud physique ! :

root@proxy-96041:/# tcpdump -i eth1 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
02:54:18.250606 IP on-005.olympe-network.com > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2926, length 40
02:54:18.250630 IP 91-121-49-65.ovh.net > on-005.olympe-network.com: ICMP echo reply, id 256, seq 2926, length 40
02:54:19.250526 IP on-005.olympe-network.com > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2927, length 40
02:54:19.250542 IP 91-121-49-65.ovh.net > on-005.olympe-network.com: ICMP echo reply, id 256, seq 2927, length 40
02:54:20.252045 IP on-005.olympe-network.com > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2928, length 40
02:54:20.252060 IP 91-121-49-65.ovh.net > on-005.olympe-network.com: ICMP echo reply, id 256, seq 2928, length 40
02:54:21.254168 IP on-005.olympe-network.com > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2929, length 40
02:54:21.254187 IP 91-121-49-65.ovh.net > on-005.olympe-network.com: ICMP echo reply, id 256, seq 2929, length 40
02:54:22.255895 IP on-005.olympe-network.com > 91-121-49-65.ovh.net: ICMP echo request, id 256, seq 2930, length 40
02:54:22.255916 IP 91-121-49-65.ovh.net > on-005.olympe-network.com: ICMP echo reply, id 256, seq 2930, length 40

Il voit les paquets arriver depuis le noeud physique et lui répond directement, le noeud physique retranscrit ensuite bien les paquets, comme s'il faisait de la NAT...

Et cela est très embêtant, car par exemple les logs d'un serveur web ou d'un serveur FTP à l'intérieur de la VM donnent tous comme IP source celle du noeud physique. Et il n'y a pas de header contenant l'IP source, elle est translatée...

Le traceroute est correct et ne voit pas le noeud physique :

C:\tracert 91.121.49.65

Détermination de l'itinéraire vers 91-121-49-65.ovh.net [91.121.49.65]
avec un maximum de 30 sauts*:

1	<1 ms	<1 ms	<1 ms	neufbox [192.168.1.1]
2	40 ms	41 ms	42 ms	1.218.11.109.rev.sfr.net [109.11.218.1]
3	40 ms	40 ms	39 ms	157.117.0.109.rev.sfr.net [109.0.117.157]
4	41 ms	*	41 ms	010G.th2-1-6k.routers.ovh.net [86.66.127.118]
5	45 ms	56 ms	*	gsw-2-6k.fr.eu [213.186.32.162]
6	45 ms	45 ms	45 ms	rbx-g1-a9.fr.eu [213.251.128.105]
7	81 ms	45 ms	*	vss-5a-6k.fr.eu [178.33.100.26]
8	44 ms	44 ms	44 ms	91-121-49-65.ovh.net [91.121.49.65]

Itinéraire déterminé.

Je n'ai activé aucun NAT iptables, voici la commande :

```
root@on-005:/etc/vz/conf# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Est-ce les "MASQUERADE" (activés par défaut ?!) qui sont responsables de ce problème ?
Si oui comment les enlever ? Sinon avez-vous une solution ?

Merci de votre patience, j'espère avoir été clair et pouvoir trouver de l'aide ici !

Merci d'avance

Cordialement,
Samuel