Subject: *CLOSED* Good way to isolate VE networks.
Posted by sebastian on Sun, 04 Mar 2007 16:44:58 GMT
View Forum Message <> Reply to Message

Hi,

first of all: I'm new to OpenVZ and it well may be that i overlooked some obvious thing addressing my issue. But i searched the forum and the wiki but didn't found a concrete answer. So sorry if this is a typical newbie question.

I've set up some VE's in a Debian Etch HN (It's a VMWare-Machine for testing purposes). I'm using the VENET approach for networking (because of security concerns) and so far it's working fine. The VE's can access the internet and DNAT works too, but: I've found no nice way to restrict networking access between the VE's. I'm currently thinking of the following setup on the HN:

General Purpose VE's
- Database Server
- MTA
- DNS
- APT-Proxy

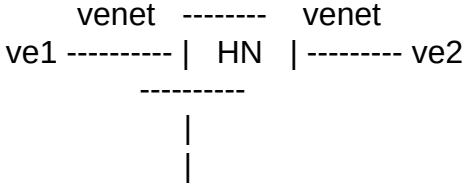
User VE's
- User VE 1
- ...
- User VE n

The User VE's should be able to access the general purpose VE's but should not be able to interconnect between them. Of course can i add matching firewall entries to all VE's but this seems like a classical case for building two networks. My problem is: I found no way to add netmasks or something similar through vzctl. What approach would you recommend in such a szenario?

Thanks very much in advance,
Sebastian

Subject: Re: Good way to isolate VE networks.
Posted by Vasily Tarasov on Mon, 05 Mar 2007 15:55:10 GMT
View Forum Message <> Reply to Message

Hmmm... venet interface is a point-to-point interface, I mean:



|
ve3

So netmask is unusefull in this situation.

VEs can be considered as completely isolated nodes, that are in a network of topology figured out above. So, what method can be used to isolate nodes in such network? Only firewall, I guess...

Vasily.

Subject: Re: Good way to isolate VE networks.
Posted by sebastian on Mon, 05 Mar 2007 19:50:42 GMT
View Forum Message <> Reply to Message

Hi,

thanks very much. I will try to implement a firewall which fullfills my needs.

Thanks again,
Sebastian

Subject: Re: *CLOSED* Good way to isolate VE networks.
Posted by syncmaster4 on Sun, 25 Mar 2007 12:51:56 GMT
View Forum Message <> Reply to Message

Sebastian,

Were you able to get this working? Can you provide a sample of your iptables? I'm struggling to get this working correctly and would love a sample to guide me; searching the net hasn't provided anything yet and I'm not an IPTABLES expert.

Thanks!
Craig

Subject: Re: *CLOSED* Good way to isolate VE networks.
Posted by sebastian on Sun, 25 Mar 2007 16:49:08 GMT
View Forum Message <> Reply to Message

Hi Craig,

first of all: I got something working but only tested the theoretical Setup on a VMWare machine because i'm waiting for Debian etch to be released. This was more like a case study. I have not verified it for production use (since i'm not an iptables/firewall expert). So please don't be disappointed if this is not what you expected.

The network is as follows:

I use the network 10.10.10.0/8 for the internal machines. I access between those machines and access from those machines to e.g. the firewall and the internet is forbidden via policies. Certain machines are then granted to perform special operations using rules. This setup may be not perfect but i will fine tune it later when i do some real testing and prepare it for production.

I used shorewall for my setup but since it is only a nice interface for iptables you don't need to use it.

I configured three zones the "net" (Internet/LAN) the "fw" (default zone for the firewall(HN)) and "int" (The network for the VEs).

/etc/shorewall/zones:

```
#ZONE   TYPE          OPTIONS        IN                  OUT
#                                    OPTIONS             OPTIONS
fw      firewall
net     ipv4
int     ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE
```

The "routeback" option is important! You can add more options to customize the setup.

/etc/shorewall/interfaces:

```
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     eth0            detect          proxyarp
int     venet0          detect          routeback
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

/etc/shorewall/policy:

```
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#                                               LEVEL
fw              int             ACCEPT
fw              net             ACCEPT
#int            net             ACCEPT
int             int             DROP            info
all             all             DROP            info
#LAST LINE -- DO NOT REMOVE
```

I forward some ports to special VEs and allow certain machines to use services on other machines (e.g. DNS and apt-proxy).

/etc/shorewall/rules (This is really dirty but as i said this is nothing used for production)

```
DNAT        net         int:10.10.10.23      tcp    80
DNAT        net         int:10.10.10.24      tcp    53
DNAT        net         int:10.10.10.24      udp    53
ACCEPT      int         int:10.10.10.22      icmp
ACCEPT      int         int:10.10.10.24      tcp    53
ACCEPT      int         int:10.10.10.24      udp    53
ACCEPT      int         net                  icmp
ACCEPT      int         int:10.10.10.24      tcp    53
ACCEPT      int         int:10.10.10.24      udp    53
ACCEPT      int         net                  icmp
ACCEPT      int         fw                   tcp    9999
ACCEPT      int         fw                   udp    9999
ACCEPT      int:10.10.10.24 net              udp    53
ACCEPT      int:10.10.10.24 net              tcp    53
```

Then i use masquerading to let special machines access the internet (e.g. the internal apt-proxy and the dns)

/etc/shorewall/masq:

```
#INTERFACE          SUBNET        ADDRESS        PROTO   PORT(S) IPSEC
eth0                10.10.10.0/8
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

If something doesn't work as expected you can of course contact me again. I had some problems implementing the setup so far and haven't had the time to polish it up. I'm looking forward to hearing from you.

best regards
Sebastian