Subject: Re: iptables modules in VE

Posted by maratrus on Thu, 28 Aug 2008 08:20:17 GMT

View Forum Message <> Reply to Message

Hi,

try the following way:

- make sure that ipset utility is installed inside VE
- make sure that iptables utility knows about "set" module for example:

```
#iptables -m set --help
```

- if the previous points are done try to do the following:

```
#ipset -N test iphash
#ipset -X iphash
```

if the first command fails, you have to give your VE net_admin capability:

```
#vzctl stop VE_ID
#vzctl set VE_ID --capability net_admin:on --save
#vzctl start VE_ID
```

where VE_ID - is an ID of your VE.
after that the previous ipset commands inside VE shoud work.
- make sure that you are able to use ipset module inside VE:

```
# ipset -N mytest iphash
# iptables -A FORWARD -m set --set mytest src -j ACCEPT
# iptables -D FORWARD -m set --set mytest src -j ACCEPT
# ipset -X mytest
```

if this test is success (it issues without errors) the command

```
# shorewall show capabilities
```

should show Ipset Match: Available inside VE.

P.S. But keep in mind that the group of ip_set modules are not virtualized, so all of yours VEs and HN use the same resources and this is the violation of encapsulation.
Also be careful with permitting various capabilities to your VE.

P.P.S. I'm afraid that these modules won't be virtualized right now, because ipset modules are not included in mainstream kernel and goes like the extensions.