Subject: *SOLVED* iptables support inside vps
Posted by pshempel on Mon, 30 Oct 2006 18:02:36 GMT
View Forum Message <> Reply to Message

I am attempting to configure a vps as a nat gateway for a openvpn server running in the vps.

How much of the iptables support is there within a VPS?
Should I expect a full support or limited?
If limited can there be something placed on the wiki that states just how much support there is?

I have read through many documents that seem to give the impression there is complete firewall support inside a vps

I am using 2.6.16 testing kernel.
I have compiled every module that relates to iptables networking into the kernel.

I am presently using shorewall to configure my iptables rules but seem to have a complete failure to setup a basic natted vpn service using shorewall.

Here is the output of shorewall show capabilities.

Shorewall has detected the following iptables/netfilter capabilities:
NAT: Not available
Packet Mangling: Available
Multi-port Match: Available
Extended Multi-port Match: Not available
Connection Tracking Match: Not available
Packet Type Match: Not available
Policy Match: Not available
Physdev Match: Not available
Packet length Match: Available
IP range Match: Not available
Recent Match: Not available
Owner Match: Not available
Ipset Match: Not available
CONNMARK Target: Not available
Connmark Match: Not available
Raw Table: Not available
IPP2P Match: Not available
CLASSIFY Target: Not available
Extended REJECT: Available
Repeat match: Not available
MARK Target: Not available
Mangle FORWARD Chain: Available

I have been using shorewall for about six years now and have a good grasp of how to setup shorewall, so I am confident that my configurations are correct.

TIA for the responses.

Philip

NanoHub.org Systems Admin

Subject: Re: iptables support inside vps
Posted by Vasily Tarasov on Tue, 31 Oct 2006 06:23:18 GMT
View Forum Message <> Reply to Message

Hello,

You wrote:
Quote:
How much of the iptables support is there within a VPS?
Should I expect a full support or limited?
If limited can there be something placed on the wiki that states just how much support there is?

Support of iptables is slightly limited. You can see which modules are available in VE using vzctl manpage: read there about --iptables command.
Note, that by default not all iptables modules are permited in VE (look in /etc/vz/vz.conf).

HTH,
vass.

Subject: Re: iptables support inside vps
Posted by pshempel on Tue, 31 Oct 2006 14:36:42 GMT
View Forum Message <> Reply to Message

Well should this rule work then?

/sbin/iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
But returns with uknown chain, but when doing a iptables -L it returnes with FORWARD chain as a rule. Is this implemented (forwarding packets)?

Shorewall now reports this

NAT: Available
Packet Mangling: Available
Multi-port Match: Available
Extended Multi-port Match: Not available
Connection Tracking Match: Not available

Packet Type Match: Not available
Policy Match: Not available
Physdev Match: Not available
Packet length Match: Available
IP range Match: Not available
Recent Match: Not available
Owner Match: Not available
Ipset Match: Not available
CONNMARK Target: Not available
Connmark Match: Not available
Raw Table: Not available
IPP2P Match: Not available
CLASSIFY Target: Not available
Extended REJECT: Available
Repeat match: Not available
MARK Target: Not available
Mangle FORWARD Chain: Available

Thanks

Philp

NanoHub.org Systems Admin

Subject: Re: iptables support inside vps
Posted by Vasily Tarasov on Thu, 02 Nov 2006 06:20:12 GMT
View Forum Message <> Reply to Message

Hello,

There is one more trick. As you now different iptables features are located in different kernel modules. Usually when iptables command see the feature, which kernel module isn't loaded, it loads appropriate module. But in VE it's prohibited to load kernel modules! Conclusion: before using specific rule you shuld make sure that appropriate module is loaded on _HN_.
The easiest way to do it, I suppose, first run the iptables comand that you want in VE, on HN and then flush it. After that all kernel modules that are needed for this command are loaded and you can fealessly executed this command in VE.

For example in you case:

[HN]# vzctl start 112

Starting VPS ...
VPS is mounted
Adding IP address(es): <ip address>
Setting CPU units: 1000
Setting devices
VPS start in progress...
[HN]# iptables -A FORWARD -j ACCEPT
[HN]# lsmod | wc
    44   146   1721
[HN]# iptables -F
[HN]# lsmod | wc
    44   146   1721
[HN]# vzctl enter 112
entered into VPS 112
[VE]#
[VE]# iptables -A FORWARD -j ACCEPT
[VE]# iptables -L
Chain FORWARD (policy ACCEPT)
target   prot opt source   destination
ACCEPT   all -- anywhere   anywhere

Chain INPUT (policy ACCEPT)
target   prot opt source   destination

Chain OUTPUT (policy ACCEPT)
target   prot opt source   destination

HTH,
vass.