Subject: Internet access from VE (again)
Posted by Thomasd on Wed, 13 Feb 2008 20:51:55 GMT
View Forum Message <> Reply to Message

I get access to the outside, but only using IPs

```
# ping yahoo.com
ping: unknown host yahoo.com
# ping 66.94.234.13
PING 66.94.234.13 (66.94.234.13) 56(84) bytes of data.
64 bytes from 66.94.234.13: icmp_seq=1 ttl=52 time=42.7 ms
```

Also, this is the same as on the HW node

```
# cat /etc/resolv.conf
nameserver 208.109.188.1
nameserver 208.109.188.2
```

how can I get the VE to work with domain names?

Subject: Re: Internet access from VE (again)
Posted by Thomasd on Wed, 13 Feb 2008 21:06:51 GMT
View Forum Message <> Reply to Message

I should add this:
(from the host)

```
# iptables -t filter -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere            tcp dpt:search to:10.0.20.10:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:domain to:10.0.20.10:53
DNAT       udp  --  anywhere             anywhere             udp dpt:domain to:10.0.20.10:53
DNAT       tcp  --  anywhere             anywhere            tcp dpt:xinupageserver to:10.0.20.20:22
```

```
DNAT       tcp  --  anywhere             anywhere            tcp dpt:samsung-unidex to:10.0.40.10:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:trap to:10.0.40.20:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:imap to:10.0.40.20:143
DNAT       tcp  --  anywhere             anywhere            tcp dpt:smtp to:10.0.40.20:25
DNAT       tcp  --  anywhere             anywhere            tcp dpt:yo-main to:10.0.40.40:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:4080 to:10.0.40.80:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:x11-ssh-offset to:10.0.60.10:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:6020 to:10.0.60.20:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:6040 to:10.0.60.40:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:6080 to:10.0.60.80:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:8010 to:10.0.80.10:22

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  10.0.0.0/16          anywhere            to:<my main ip>

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

then, when trying to do a ping yahoo.com from the VE, I did this on the host:

```
# tcpdump -n -i venet0
tcpdump: WARNING: arptype 65535 not supported by libpcap - falling back to cooked socket
tcpdump: WARNING: venet0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on venet0, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
13:07:43.534691 IP 10.0.40.10.32921 > 208.109.188.1.domain:  42549+ A? yahoo.com. (27)
13:07:43.534723 IP 10.0.40.10.32921 > 10.0.20.10.domain:  42549+ A? yahoo.com. (27)
13:07:43.535025 IP 10.0.20.10.domain > 10.0.40.10.32921:  42549- 0/13/0 (238)
13:07:43.535049 IP 208.109.188.1.domain > 10.0.40.10.32921:  42549- 0/13/0 (238)
13:07:43.536025 IP 10.0.40.10.32921 > 208.109.188.2.domain:  42549+ A? yahoo.com. (27)
13:07:43.536053 IP 10.0.40.10.res > 10.0.20.10.domain:  42549+ A? yahoo.com. (27)
13:07:43.536312 IP 10.0.20.10.domain > 10.0.40.10.res:  42549- 0/13/0 (238)
13:07:43.536335 IP 208.109.188.2.domain > 10.0.40.10.32921:  42549- 0/13/0 (238)
13:07:43.536688 IP 10.0.40.10.32921 > 208.109.188.1.domain:  42549+ A? yahoo.com. (27)
13:07:43.536714 IP 10.0.40.10.32921 > 10.0.20.10.domain:  42549+ A? yahoo.com. (27)
13:07:43.537109 IP 10.0.20.10.domain > 10.0.40.10.32921:  42549- 0/13/0 (238)
13:07:43.537138 IP 208.109.188.1.domain > 10.0.40.10.32921:  42549- 0/13/0 (238)
13:07:43.537303 IP 10.0.40.10.32921 > 208.109.188.2.domain:  42549+ A? yahoo.com. (27)
13:07:43.537324 IP 10.0.40.10.res > 10.0.20.10.domain:  42549+ A? yahoo.com. (27)
13:07:43.537759 IP 10.0.20.10.domain > 10.0.40.10.res:  42549- 0/13/0 (238)
13:07:43.537789 IP 208.109.188.2.domain > 10.0.40.10.32921:  42549- 0/13/0 (238)
13:07:43.537992 IP 10.0.40.10.32921 > 208.109.188.1.domain:  25734+ A? yahoo.com. (27)
13:07:43.538012 IP 10.0.40.10.32921 > 10.0.20.10.domain:  25734+ A? yahoo.com. (27)
13:07:43.538459 IP 10.0.20.10.domain > 10.0.40.10.32921:  25734- 0/13/0 (238)
13:07:43.538488 IP 208.109.188.1.domain > 10.0.40.10.32921:  25734- 0/13/0 (238)
13:07:43.538641 IP 10.0.40.10.32921 > 208.109.188.2.domain:  25734+ A? yahoo.com. (27)
```

13:07:43.538661 IP 10.0.40.10.res > 10.0.20.10.domain: 25734+ A? yahoo.com. (27)
13:07:43.539097 IP 10.0.20.10.domain > 10.0.40.10.res: 25734- 0/13/0 (238)
13:07:43.539126 IP 208.109.188.2.domain > 10.0.40.10.32921: 25734- 0/13/0 (238)
13:07:43.539288 IP 10.0.40.10.32921 > 208.109.188.1.domain: 25734+ A? yahoo.com. (27)
13:07:43.539306 IP 10.0.40.10.32921 > 10.0.20.10.domain: 25734+ A? yahoo.com. (27)
13:07:43.539732 IP 10.0.20.10.domain > 10.0.40.10.32921: 25734- 0/13/0 (238)
13:07:43.539767 IP 208.109.188.1.domain > 10.0.40.10.32921: 25734- 0/13/0 (238)
13:07:43.539926 IP 10.0.40.10.32921 > 208.109.188.2.domain: 25734+ A? yahoo.com. (27)
13:07:43.539945 IP 10.0.40.10.res > 10.0.20.10.domain: 25734+ A? yahoo.com. (27)
13:07:43.540381 IP 10.0.20.10.domain > 10.0.40.10.res: 25734- 0/13/0 (238)
13:07:43.540410 IP 208.109.188.2.domain > 10.0.40.10.32921: 25734- 0/13/0 (238)

(208.109.188.1 and 208.109.188.2 are my nameservers)

Subject: Re: Internet access from VE (again)
Posted by maratrus on Thu, 14 Feb 2008 12:09:22 GMT
View Forum Message <> Reply to Message

Hi,

1. I suppose that the problem is in your PREROUTING rules
Quote:Chain PREROUTING (policy ACCEPT)
target prot opt source destination
DNAT tcp -- anywhere anywhere tcp dpt:search to:10.0.20.10:22
DNAT tcp -- anywhere anywhere tcp dpt:domain to:10.0.20.10:53
DNAT udp -- anywhere anywhere udp dpt:domain to:10.0.20.10:53
DNAT tcp -- anywhere anywhere tcp dpt:xinupageserver to:10.0.20.20:22
DNAT tcp -- anywhere anywhere tcp dpt:samsung-unidex to:10.0.40.10:22
DNAT tcp -- anywhere anywhere tcp dpt:trap to:10.0.40.20:22
DNAT tcp -- anywhere anywhere tcp dpt:imap to:10.0.40.20:143
DNAT tcp -- anywhere anywhere tcp dpt:smtp to:10.0.40.20:25
DNAT tcp -- anywhere anywhere tcp dpt:yo-main to:10.0.40.40:22
DNAT tcp -- anywhere anywhere tcp dpt:4080 to:10.0.40.80:22
DNAT tcp -- anywhere anywhere tcp dpt:x11-ssh-offset to:10.0.60.10:22
DNAT tcp -- anywhere anywhere tcp dpt:6020 to:10.0.60.20:22
DNAT tcp -- anywhere anywhere tcp dpt:6040 to:10.0.60.40:22
DNAT tcp -- anywhere anywhere tcp dpt:6080 to:10.0.60.80:22
DNAT tcp -- anywhere anywhere tcp dpt:8010 to:10.0.80.10:22

Can you please explain what do these rules mean? Especially
Quote:DNAT tcp -- anywhere anywhere tcp dpt:domain to:10.0.20.10:53
DNAT udp -- anywhere anywhere udp dpt:domain to:10.0.20.10:53
Try to remove all these rules.

2. If it doesn't help can you please answer some questions?
Is it possible to ping yahoo.com from HN?

Can you please provide us with the tcpdump output when you ping yahoo.com from HN?
Can you please use for example 4.2.2.4 as a nameserver on HN and inside VPS?

Thank You!

Subject: Re: Internet access from VE (again)
Posted by Thomasd on Tue, 04 Mar 2008 00:35:08 GMT
View Forum Message <> Reply to Message

sorry for the long delay. I spend a while in a hospital and wasn't really dealing with this

to bring a conclusion to this post:
It now works using another DNS server.

For some reason, my provider's DNS works with the HN but not from the VE (I'd be very curious if anyone has any theory about why).

I switched to OpenDNS and it all works fine!

Subject: Re: Internet access from VE (again)
Posted by maratrus on Tue, 04 Mar 2008 09:58:39 GMT
View Forum Message <> Reply to Message

Hi,

1. Could you please explain what does this rule mean?

DNAT udp -- anywhere anywhere udp dpt:domain to:10.0.20.10:53

You haven't changed any iptables rule on HN just set another nameserver inside VPS, have you?

In my opinion when DNS request comes from VE to HN the above rule changes it destination address from 208.109.188.1 to 10.0.20.10:53. Is it expected behavior?

Subject: Re: Internet access from VE (again)
Posted by Thomasd on Wed, 05 Mar 2008 07:01:00 GMT
View Forum Message <> Reply to Message

yes, this is what happened. It finally got totally troubleshooted today

I have a DNS server in a VE; and a rule on the HN that forwards connections on port 53 to the DNS server.

The problem ended up being what you described: various VE would try to make a DNS request and it ended up to the DNS VE.

the answer was to add: -i eth0 in the rule, so only connections coming from eth0 would land to the DNS server, but not the ones originating from inside.

Yesterday, I thought it was fixed because I disabled the rules while I was trying to fix it...
