Subject: no firewall?
Posted by goeldi on Wed, 14 Jun 2006 09:29:31 GMT
View Forum Message <> Reply to Message

I checked the manual and searched this forum about this. And it seems to me - after doing a step-by-step install - that I can only run a working vz when I shut down iptables on the host system. i.e. I can run vz and start the vps with vzctl start n, but I cannot access it via SSH or ping.

The manual tells me to disable iptables on the host system. When I do this, everything works. But how about security?

BTW: I already loaded these modules:
iptable_filter iptable_mangle ipt_limit ipt_multiport ipt_tos ipt_TOS ipt_REJECT ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_LOG ipt_length ip_conntrack ip_conntrack_ftp ip_conntrack_irc ipt_conntrack ipt_state ipt_helper iptable_nat ip_nat_ftp ip_nat_irc ipt_REDIRECT

The host is CentOS 4.3 with Kernel 2.6.8-022stab077.1 and the vps is CentOS too.

Subject: Re: no firewall?
Posted by Vasily Tarasov on Wed, 14 Jun 2006 10:03:08 GMT
View Forum Message <> Reply to Message

You can use iptables on Hardware node without any problems,
so, the reason why you can't get into VPS is wrong rules for iptables, I guess.

You can post your iptables rules here and I'll try to find out what's wrong.

Good luck.

Subject: Re: no firewall?
Posted by goeldi on Wed, 14 Jun 2006 10:06:00 GMT
View Forum Message <> Reply to Message

thank you very much. here they are:

Table: nat
Chain PREROUTING (policy ACCEPT)
target prot opt source destination

Chain POSTROUTING (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

```
Table: mangle
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

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

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Table: filter
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0           0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:10000
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:110
ACCEPT     tcp  --  192.168.2.3          0.0.0.0/0           tcp dpt:5901 state NEW
ACCEPT     tcp  --  192.168.2.3          0.0.0.0/0           tcp dpts:5900:5902 state NEW
ACCEPT     tcp  --  192.168.2.3          0.0.0.0/0           tcp dpt:22 state NEW
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:25
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp multiport ports 220 state NEW
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp multiport ports 993 state NEW
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp multiport ports 143 state NEW
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp multiport ports 995 state NEW
```

```
ACCEPT     tcp  --  0.0.0.0/0          0.0.0.0/0          tcp multiport ports 80 state NEW
ACCEPT     tcp  --  192.168.2.8        0.0.0.0/0            tcp state NEW
ACCEPT     tcp  --  192.168.2.3        0.0.0.0/0            tcp dpt:19150 state NEW
           tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpts:6881:6999 state NEW
           udp  --  0.0.0.0/0          0.0.0.0/0          udp dpts:6881:6999 state NEW
ACCEPT     tcp  --  192.168.2.3        0.0.0.0/0            tcp multiport ports 7634
ACCEPT     tcp  --  195.141.143.40     0.0.0.0/0            tcp multiport ports 22 state NEW
ACCEPT     tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:22
ACCEPT     tcp  --  192.168.2.3        0.0.0.0/0            tcp dpt:8080 state NEW
ACCEPT     tcp  --  192.168.2.4        0.0.0.0/0            tcp multiport ports 5901 state NEW
REJECT     all  --  0.0.0.0/0          0.0.0.0/0          reject-with icmp-host-prohibited
```

Subject: Re: no firewall?
Posted by Vasily Tarasov on Wed, 14 Jun 2006 10:16:53 GMT
View Forum Message <> Reply to Message

Can you, please give
iptables -nv -L
output, 'cause I can't see interface names in your previous post.

Also, please, clarify a little your configuration:
Hardware node IP and IP of VPS.

Thanks.

Subject: Re: no firewall?
Posted by goeldi on Wed, 14 Jun 2006 11:15:27 GMT
View Forum Message <> Reply to Message

Hardware node is 192.168.2.210 and VPS is 192.168.2.211

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   16  1012 RH-Firewall-1-INPUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RH-Firewall-1-INPUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 21 packets, 3044 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain RH-Firewall-1-INPUT (2 references)
 pkts bytes target     prot opt in     out     source               destination
```

```
    0     0 ACCEPT     all  --  lo     *      0.0.0.0/0           0.0.0.0/0
    0     0 ACCEPT     icmp --  *      *      0.0.0.0/0           0.0.0.0/0           icmp type 255
    0     0 ACCEPT     esp  --  *      *      0.0.0.0/0           0.0.0.0/0
    0     0 ACCEPT     ah   --  *      *      0.0.0.0/0           0.0.0.0/0
    0     0 ACCEPT     udp  --  *      *      0.0.0.0/0           224.0.0.251         udp dpt:5353
    0     0 ACCEPT     udp  --  *      *      0.0.0.0/0           0.0.0.0/0           udp dpt:631
    0     0 ACCEPT     all  --  *      *      0.0.0.0/0           0.0.0.0/0           state
RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:10000
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:110
    0     0 ACCEPT     tcp  --  *      *      192.168.2.3         0.0.0.0/0           tcp dpt:5901 state NEW
    0     0 ACCEPT     tcp  --  *      *      192.168.2.3         0.0.0.0/0           tcp dpts:5900:5902 state
NEW
    0     0 ACCEPT     tcp  --  *      *      192.168.2.3         0.0.0.0/0           tcp dpt:22 state NEW
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           state NEW tcp dpt:25
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp multiport ports 220 state
NEW
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp multiport ports 993 state
NEW
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp multiport ports 143 state
NEW
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp multiport ports 995 state
NEW
    0     0 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp multiport ports 80 state
NEW
    0     0 ACCEPT     tcp  --  *      *      192.168.2.8         0.0.0.0/0           tcp state NEW
    0     0 ACCEPT     tcp  --  *      *      192.168.2.3         0.0.0.0/0           tcp dpt:19150 state NEW
    0     0            tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp dpts:6881:6999 state NEW
    0     0            udp  --  *      *      0.0.0.0/0           0.0.0.0/0           udp dpts:6881:6999 state NEW
    0     0 ACCEPT     tcp  --  *      *      192.168.2.3         0.0.0.0/0           tcp multiport ports 7634
    0     0 ACCEPT     tcp  --  *      *      195.141.143.40      0.0.0.0/0           tcp multiport ports 22
state NEW
   12   768 ACCEPT     tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *      192.168.2.3         0.0.0.0/0           tcp dpt:8080 state NEW
    0     0 ACCEPT     tcp  --  *      *      192.168.2.4         0.0.0.0/0           tcp multiport ports 5901
state NEW
    4   244 REJECT     all  --  *      *      0.0.0.0/0           0.0.0.0/0           reject-with
icmp-host-prohibited
```