Subject: HN iptables blocking http access
Posted by lurnux on Tue, 29 May 2007 07:08:43 GMT
View Forum Message <> Reply to Message

Hi,

I've just started using openvz and I'm stuck with HN iptables.

I've installed Centos4 HN according instructions found in wiki.
Now everything works great except http access from every VN, when I try to go to google.com with links or use any kind of http access to anywhere i'll get only "No route to host". After some digging around i found that the requests are stuck in HN iptables rule.

Tcpdump shows:
09:59:05.748720 IP HN > VN: icmp 68: host eh-in-f99.google.com unreachable - admin prohibited
09:59:08.748990 IP VN > eh-in-f99.google.com.http: S 2235774822:2235774822(0) win 5840 <mss 1460,sackOK,timestamp 392992619 0,nop,wscale 2>

In iptables those requests are stuck with the last rule:
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited
and I don't know what I should allow to get this one working.

Subject: Re: HN iptables blocking http acces
Posted by rickb on Tue, 29 May 2007 07:15:30 GMT
View Forum Message <> Reply to Message

of course your iptables rule is blocking the traffic. what do you want your iptables rule to do?

Subject: Re: HN iptables blocking http acces
Posted by lurnux on Tue, 29 May 2007 08:22:08 GMT
View Forum Message <> Reply to Message

I would like it to allow surfing from all of VN's.

Subject: Re: HN iptables blocking http acces
Posted by rickb on Tue, 29 May 2007 08:28:44 GMT
View Forum Message <> Reply to Message

But your rule is REJECT. Have you tried to remove the rule?

Subject: Re: HN iptables blocking http acces
Posted by lurnux on Tue, 29 May 2007 08:43:03 GMT
View Forum Message <> Reply to Message

Yes and after that it works, however I need something before that
REJECT rule which would allow that www connection.

Subject: Re: HN iptables blocking http acces
Posted by kingneutron on Tue, 29 May 2007 11:53:13 GMT
View Forum Message <> Reply to Message

Rick, this is much like the "fallthru" ACLs in Squid.

He wants to allow $something-safe, and anything *after* that should by REJECTed by default.

What he needs is how to define $something-safe in iptables, just before the no-no trips to protect his system.

Subject: Re: HN iptables blocking http acces
Posted by Vasily Tarasov on Fri, 01 Jun 2007 07:24:57 GMT
View Forum Message <> Reply to Message

Hello,

this is the a very commoin iptables rule to allow http traffic in FORWARD chain. Please, read some iptables guide, e.g. http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables

HTH,
Vasily.

Subject: Re: HN iptables blocking http acces
Posted by rickb on Fri, 01 Jun 2007 07:31:23 GMT
View Forum Message <> Reply to Message

yes, agreed. This is how almost every firewall config works. allow a,b,c and disallow d-z. However, if the admin doesn't know what a,b,c are, its not going to work.

so, your question is more of a business logic one, and that is, what services do you want to offer with your vps? Once you know that, create a list of the ports and protocls they use (smtp- 25tcp, dns 53tcp/udp, etc) and create allow rules to pass them through. then, add your reject rule at the end.

bottom line, when you add your reject rule without and allow rules, its like unplugging the network cable. this isn't specific to openvz, its just basic firewall theory.