Subject: Iptables problem - when enabled, can't access VPSes
Posted by tomfra on Thu, 13 Sep 2007 16:52:09 GMT
View Forum Message <> Reply to Message

I know some people reported different problem related to iptables but none of the forum posts (and not just on this forum) helped me solve my particular problem...

The problem: When firewall is enabled, I can't ping or in any other way access the VPS, when it's disabled, it works just fine.

Here are the facts:

* Hardware node works OK, has iptables / CSF firewall installed.

* Kernel is 2.6.18 custom compiled, behaviour of the related problem is the same with standard OpenVZ kernel though.

* IP forwarding is enabled - cat /proc/sys/net/ipv4/ip_forward returns 1.

* OS: CentOS 5 x86_64, all standard packages updated via yum daily.

* VPS IP address is added to csf.allow list and is properly added as an allowed IP to iptables rules.

I have attached my iptables rules as set by CSF. There are currently 2 IPs on the csf.deny list (hackers) and 2 IPs on the csf.allow list. Those IPs are the MAIN_NODE_IP and TEST_VPS_IP. There are real IPs on the original list of course.

Any ideas what could be causing this problem are *very* welcome.

Thanks for your time!

Tomas

File Attachments
1) csf_iptables_rules.txt, downloaded 441 times

Subject: Re: Iptables problem - when enabled, can't access VPSes
Posted by tomfra on Thu, 13 Sep 2007 23:38:14 GMT
View Forum Message <> Reply to Message

OK, I may have found the solution myself... Instead of writing it here since it's a bit longer, you can read it at http://forum.lxlabs.com/index.php?t=msg&goto=13353&# msg_13353 .

I will welcome any comments on the solution - mainly I would like to know where it would open some security holes etc. I am not an iptables expert so it's quite possible...

Tomas

Subject: Re: Iptables problem - when enabled, can't access VPSes
Posted by ugob on Fri, 14 Sep 2007 02:40:17 GMT
View Forum Message <> Reply to Message

Yes, OpenVZ needs to use the FORWARD table for iptables so that traffic from/to the VEs are routed through the HN.

I think the person in the Lxlabs forum did a great job to minimize any potential security risk associated with the use of the FORWARD table. However, you must use iptables to firewall your VE's afterward, either using FORWARD rules on the HN, or using iptables inside the VEs.

Ugo

Subject: Re: Iptables problem - when enabled, can't access VPSes
Posted by tomfra on Fri, 14 Sep 2007 10:43:14 GMT
View Forum Message <> Reply to Message

ugob wrote on Fri, 14 September 2007 04:40However, you must use iptables to firewall your VE's afterward, either using FORWARD rules on the HN, or using iptables inside the VEs.

I realized that if I enable the venet0 forwarding, any VPS traffic will not be affected by the HN firewall. This is not that bad since I plan to install firewall on each of the VPSes (they will all be owned by myself, for different projects), but it would still be nice if the VPS traffic was, to a degree, affected by the HN firewall - so that for example a hacker's IP would get blocked for all of the VPSes on the HN, even if the attack was committed towards only one of them.

Then I would have a firewall on the VPS itself, filtering the traffic further. I don't know how to accomplish that though. As I mentioned on the LXLabs forum, I am no iptables expert. But I can see some disadvantages of such a system and it would probably be just a complication anyway.

Tomas

Subject: Re: Iptables problem - when enabled, can't access VPSes
Posted by ugob on Fri, 14 Sep 2007 10:47:31 GMT
View Forum Message <> Reply to Message

ugob wrote on Fri, 14 September 2007 04:40However, you must use iptables to firewall your VE's afterward, either using FORWARD rules on the HN, or using iptables inside the VEs.

tomfra wrote on Fri, 14 September 2007 06:43I realized that if I enable the venet0 forwarding, any VPS traffic will not be affected by the HN firewall. This is not that bad since I plan to install firewall on each of the VPSes (they will all be owned by myself, for different projects), but it would still be nice if the VPS traffic was, to a degree, affected by the HN firewall - so that for example a hacker's IP would get blocked for all of the VPSes on the HN, even if the attack was committed towards only one of them.

Using FORWARD rules on the HN, you could achieve this.
