Subject: IRC
Posted by zwtint on Fri, 17 Aug 2007 21:13:25 GMT
View Forum Message <> Reply to Message

Hello,

How can I disable IRC access for VPSes globally?
(or for ips)

openvz based on centos 5

Regards,

A.

Subject: Re: IRC
Posted by alticon-brian on Fri, 17 Aug 2007 21:59:18 GMT
View Forum Message <> Reply to Message

You can always set up an iptables rule on the HN blocking 6660-6669. Unfortunately, this is only going to block a few ports and anyone with a bit of knowledge can easily re-configure their server software to use non-standard ports.

That being said, you can always drop the iptables rule in place and then run nmap periodically to see whats running on non-standard ports and give it a look-see.

Subject: Re: IRC
Posted by zwtint on Sat, 18 Aug 2007 06:33:16 GMT
View Forum Message <> Reply to Message

Hey,

Can you please let me know that ipables rules?

My provider also did something on the main IP of the node:

root@atdn:~#nmap 66.246.220.34

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2007-08-18 08:30 CEST
Interesting ports on 66.246.220.34:
Not shown: 1672 closed ports
PORT STATE SERVICE
22/tcp open ssh
6666/tcp filtered irc-serv

6667/tcp filtered irc
6668/tcp filtered irc
6699/tcp filtered napster
6881/tcp filtered bittorent-tracker
6969/tcp filtered acmsoda
7000/tcp filtered afs3-fileserver

Nmap finished: 1 IP address (1 host up) scanned in 17.485 seconds
root@atdn:~#

Can I do also something like that?

Regards,

Subject: Re: IRC
Posted by dowdle on Sat, 18 Aug 2007 18:44:45 GMT
View Forum Message <> Reply to Message

I'd recommend the solution recommended in the OpenVZ Wiki:

Setting up an iptables firewall
http://wiki.openvz.org/Setting_up_an_iptables_firewall

Just edit the script to add the ports you want on your host node. For VPSes, just create a file for each VPS that specifies just what ports you want open and plop that into the /etc/firewall.d directory. Works rather well in my somewhat limited experience.

The only problem with this solution is that the firewall rules do not follow the VPS when it is migrated from one physical host to another... although I imagine anyone who wanted to could add that functionality to the vzmigrate script and check to see if a firewall file for the VPS exists (after coming up with a standard name for the VPS files... like VEID for example) and to migrate that as well... and then restart the firewall service on the destination machine after the migration is complete.

I doubt this functionality will ever become a stock part of vzmigrate or vzctl... because so many people have their own, usually custom, firewall setups.

Subject: Re: IRC
Posted by zwtint on Sat, 18 Aug 2007 18:59:54 GMT
View Forum Message <> Reply to Message

Hey,

Thanks for your post.

The only problem if I create a custom firewall rule on the VPS, the root (costumer) can easily modify it so he earn access to IRC.

I would need a very strict rules about IRC cos my server provider do an instant termination of server if they found any IRC activities!

Any other idea?

Subject: Re: IRC
Posted by dowdle on Sat, 18 Aug 2007 19:07:00 GMT
View Forum Message <> Reply to Message

Well, the firewall script in the wiki was designed to be used from the host node. All firewall rules for the host node and all of the VPSes are controlled from the host node... and they can not (as I understand it) be modified from within the VPS.

The VPS root user might try and create firewall rules from within the VPS but it will not affect the rules set on the host node... so even if within the VPS it is setup to accept IRC traffic... if the host node created VPS firewall doesn't allow it, it isn't going to get in.

Subject: Re: IRC
Posted by zwtint on Sat, 18 Aug 2007 19:20:21 GMT
View Forum Message <> Reply to Message

Okey, I try it.

I already made a rule to block 6667 port out and incoming but its not works.

Other, Can I limit the bandwidth of VPS per gigabyte?

Not by speed!

Regards,

Subject: Re: IRC
Posted by dowdle on Sat, 18 Aug 2007 20:39:50 GMT
View Forum Message <> Reply to Message

Can you have a monthly bwlimit of a VPS? I believe so. In the OpenVZ wiki there is an article on such... and I believe it uses iptables. Now I don't know if you can easily integrate both the hn based firewall and the bwlimit functions into a single iptables script or not... so that might be a challenge. Also, I can't really say how well the bwlimit article works because I haven't read it or used it myself.

Subject: Re: IRC
Posted by locutius on Sat, 18 Aug 2007 21:42:14 GMT
View Forum Message <> Reply to Message

iptables is a bitch because all the time you must keep a clear record of your rulez and for any configuration worthy of a modern webserver the rulez get long and complex to read

as a basic requirement for any server facing the cloud i recommend advanced policy firewall http://rfxnetworks.com/apf.php it is a simple to use intuitive script for loading rules into iptables

in addition to dynamic rules there are static global rules which can be used to loaded blocklists into iptables. i have servers blocking 2.6 million IPs or 64% of the net in the kernel at very very very small cost (5% cpu)

you can easily obtain lists of IRC networks and other nasty stuff. ipfiltering those bad guys will make your server most unattractive to anyone who needs a server to run evil IRC

btw your hosts attempts are ridiculous, slap him

EDIT:

to be clear, there is nothing wrong with local irc as a service. it is everything and the evil that comes with irc you dont want. my best guess is what you want is to remove the possibility the VPS are used to join evil undernet etc and if eggdrops are installed then they are limited. the above iptables solution will do that for you and more. NOTE: enable egress filtering

Subject: Re: IRC
Posted by zwtint on Sun, 19 Aug 2007 07:20:47 GMT
View Forum Message <> Reply to Message

hey,

Are you sure that IRC thing will work?

Because the ips added by loopbacks such as

```
lo:256    Link encap:Local Loopback
          inet addr:xx.xx.xxx.xxx  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

So I have to remove them before it can be useful for VPSes.

A.

Subject: Re: IRC

Posted by dowdle on Sun, 19 Aug 2007 12:30:29 GMT
View Forum Message <> Reply to Message

I didn't understand what you were talking about.

If you look at the design as stated in the firewall script it says:

Quote:This setup emulates (to the VEs anyway) an external hardware firewall. It protects the HN from any access and then defines what services and ports are allowed/banned for individual VEs. This leaves the firewall controlled by the site administrator, not be individual VEs and the hackers who've gotten into them.

So, it sounds to me that they have a design philosophy that matches your goals, right?

When in doubt, give it a try it and test it out.

Subject: Re: IRC
Posted by zwtint on Sun, 19 Aug 2007 16:42:08 GMT
View Forum Message <> Reply to Message

Okey, then I dont understand:S

```
# the IP block allocated to this server
SEGMENT="192.168.0.0/24"
# the IP used by the hosting server itself
THISHOST="192.168.0.1"
# services that should be allowed to the HN; services for VEs are configured in /etc/firewall.d/*
OKPORTS="53"
# hosts allowed full access through the firewall, to all VEs and to this server
DMZS="12.34.56.78 90.123.45.67"
```

Its ok, what is OKPORTS? it should be allowed everything except IRC access, so what should I write there?

next:

```
# This file is processed by /etc/init.d/firewall
VEID="1"                    # the VE's ID#
VENAME="Customer1"          # A human-friendly label for the VE
VEIP="192.168.1.34"         # the IP address for this VE
OPENPORTS="80 443"          # ports that should be universally opened to the entire Internet
DMZS="1.2.3.0/24 5.6.7.8/32"  # IPs and blocks that should have full access to the VE's services
BANNED=""                   # IPs and blocks that should be entirely blocked from the VE's services
```

Okey, so what is VEID? should I add like 01,02,03 etc.. or should I create such file for every VPS? or can I do it globally?

OPENPORTS: as I said, everything is open except IRC access, what should I write there?

DMZS: I dont understand again, every ip is allowed

BANNED: what? every ip is allowed

Then I dont know where should I put IRC ports and what ports should I put there.

Sorry if Im too lame:(

A.

Subject: Re: IRC
Posted by dowdle on Sun, 19 Aug 2007 17:05:48 GMT
View Forum Message <> Reply to Message

zwtint wrote on Sun, 19 August 2007 10:42what is OKPORTS? it should be allowed everything except IRC access, so what should I write there?

No, rather than allowing everything but some ports... this firewall denies everything but the ports you specify.

Quote:what is VEID?

A VEID is your Virtual Environment Identifier... or the number of your VPS.

Quote:should I create such file for every VPS? or can I do it globally?

You create a separate file for each VPS... that way you can have different firewall rules (allowing the needed services) for each VPS.

Quote:OPENPORTS: as I said, everything is open except IRC access, what should I write there?

Again, it is a deny everything except for what is allowed type of firewall.

Quote:DMZS: I dont understand again, every ip is allowed

That is so you can specify IPs or ranges of IPs where your firewall doesn't block them.

Quote:BANNED: what? every ip is allowed

This is if you want to ban an IP or range of IPs from all services even those you have allowed.

Quote:Sorry if Im too lame:(

Just try it... and play with it... and hopefully it'll make more sense to you. I'm not sure why I have to explain all of this to you... because I thought most of it was explained on the wiki page.

Subject: Re: IRC
Posted by zwtint on Sun, 19 Aug 2007 17:20:35 GMT
View Forum Message <> Reply to Message

Okey,

Finally, which I enable in OPENPORTS that will be enabled on VPS.

So if I enable port 88 and 89 there, the user can only run anything or access the vps on 88, 89 ports and he cant run any softrware on other ports.

m I right?

A.

Subject: Re: IRC
Posted by dowdle on Sun, 19 Aug 2007 18:31:58 GMT
View Forum Message <> Reply to Message

There are two basic ports settings:

1) Ports you define for the host node in the firewall script
2) Ports you define for the VPSes in the /etc/firewall.d/ files you create.

So, you are creating a firewall for the host node... and it can have what ports you want it to have open... AND you are creating separate firewalls for each VPS... and they can have just the ports you want them to have open.

So, if you enable port 22 on the hn, that only affects the host node. If you enable port 80 in a VPS, it only affects that VPS.

Getting back to your question, yes... the ports you allow through are the only ones that traffic will be allowed through on... so while a VPS user might bind a program/service to a particular port, unless it is allowed in the VPS' /etc/firewall.d/ file, it'll get dropped before the VPS ever sees it.

Subject: Re: IRC
Posted by zwtint on Sun, 19 Aug 2007 18:34:08 GMT
View Forum Message <> Reply to Message

Then its a very bad solution cause vps means costumer has root access and can do whatever he wants.

So he must always email me or anything to open ports for him

Any other idea?

Subject: Re: IRC
Posted by zwtint on Sun, 19 Aug 2007 19:28:26 GMT
View Forum Message <> Reply to Message

This topic can be closed as solved!

The correct iptables rule:

/sbin/iptables -D FORWARD -p tcp --dport 6660:6669 -j DROP

which close the most popular ports!

A.

Subject: Re: IRC
Posted by dowdle on Sun, 19 Aug 2007 19:44:00 GMT
View Forum Message <> Reply to Message

Listen, you can't have it both ways.

At the very start... the design for that firewall said... so that the admin of the host node can administer the firewall for the host node AND the VPSes.

Someone should NOT be running arbitrary services on their VPS. You should be aware of what services they are running.

I guess you could emulate the behavior you want by opening up all service ports (look at /etc/services) and leaving out only IRC related ones.

Subject: Re: IRC
Posted by zwtint on Sun, 19 Aug 2007 19:49:52 GMT
View Forum Message <> Reply to Message

Okey, thank you

Now, I would need a script which checks for irc processes thourhg VPSes.(and maybe kill them automatically)

Maybe is there any around?

Regards,

Subject: Re: IRC
Posted by locutius on Mon, 20 Aug 2007 20:10:01 GMT

zwtint wrote on Sun, 19 August 2007 15:28This topic can be closed as solved!

The correct iptables rule:

/sbin/iptables -D FORWARD -p tcp --dport 6660:6669 -j DROP

which close the most popular ports!

you have closed 10 ports all of which can be reconfigured within an irc server and you think your irc security problem is solved?

irc services can be renamed to anything, they can mascarade as legit services

your profile of a script kiddy is woefully inadequate if you think closing 10 ports and a police script will stop him

if you want the whole hog but cant handle a properly configured firewall then install a traffic sniffer and set alarms for irc, p2p, whateva. Com**** et al use them, there are plenty about

---

Subject: Re: IRC
Posted by zwtint on Tue, 21 Aug 2007 06:01:52 GMT

Hello,

You are right. Ihave just closed the main ports for irc and ircd server.

A.
