Subject: Cant block DDoS to a VPS? How to do it?
Posted by postcd on Sat, 16 Nov 2013 21:05:51 GMT
View Forum Message <> Reply to Message

Hi,

there is a DDoS on one of the OpenVZ VPSs on the server, what helps is the command:

vzctl set 520 --ipdel theipaddressofthevps --save

i think this command nullroute the traffic to VPS. Then VPS is not usable by that IP.

Im using DDoS deflate on the Host node server and when did this command to show server connections sorted by number:

CONNECTIONS

netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n

```
     55 212.185.55.15
     57 212.185.55.80
     79 212.185.55.89
     92 212.185.55.58
     97 212.185.55.225
    113 212.185.55.10
    113 212.185.55.113
    183
```

(it can be seen there are around 100 connections from some IPs, these are almost certainly the attackers, it is repeating)

LISTING IPTABLES BANS

```
[root@server ~]# iptables -L | grep 212.185
DROP       all  --  212-185-55-0.dumb.cat.com/20  anywhere
DROP       all  --  212-185-55-58.dumb.cat.com  anywhere
DROP       all  --  212-185-55-113.dumb.cat.com  anywhere
DROP       all  --  212-185-55-15.dumb.cat.com  anywhere
DROP       all  --  212-185-55-10.dumb.cat.com  anywhere
DROP       all  --  212-185-55-89.dumb.cat.com  anywhere
DROP       all  --  212-185-55-225.dumb.cat.com  anywhere
DROP       all  --  212-185-55-0.dumb.cat.com/24  anywhere
[root@ns308203 ~]#
```

How is it possible these IPs overloadig server (hostserver + VPS) even they are banend in IPtables?

Any ideas on how to block them for good from my server? (PS IP number was changed to keep

anonymity)

logs from a VPS:
/var/log/apache2/access.log
::1 - - [16/Nov/2013:21:32:53 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
::1 - - [16/Nov/2013:21:32:54 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
::1 - - [16/Nov/2013:21:32:55 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
::1 - - [16/Nov/2013:21:32:56 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
::1 - - [16/Nov/2013:21:32:57 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
::1 - - [16/Nov/2013:21:32:58 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
::1 - - [16/Nov/2013:21:32:59 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
FULLL of this

/var/log/apache2/other_vhosts_access.log
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:33 +0000] "GET / HTTP/1.0" 200 668 "8574at.info" "Mozilla/5.0 (compatible; heritrix/1.7.0 +http://www.0sz9o7t8r25.com/)"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:39 +0000] "GET / HTTP/1.0" 200 666 "wgcki.net" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:x.xxx) Gecko/20041027 Mnenhy/0.6.0.104"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:30 +0000] "GET / HTTP/1.0" 200 669 "61lqveh.info" "Mozilla/5.0 (compatible; http://www.3d3128.com/bot/)"
ns1.customersite.com:80 212.185.56.29 - - [16/Nov/2013:21:32:30 +0000] "GET / HTTP/1.0" 200 665 "zygla.ru" "Mozilla/4.0 compatible ZyBorg/1.0 Dead Link Checker (wn.zyborg@looksmart.net; http://www.g293if.com)"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:30 +0000] "GET / HTTP/1.0" 200 668 "0xt964ix.ru" "Mozilla/4.0 compatible ZyBorg/1.0 Dead Link Checker (wn.zyborg@looksmart.net; http://www.19619.com)"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:30 +0000] "GET / HTTP/1.0" 200 675 "ph8v734w2347en.biz" "Mozilla/3.01 (compatible; Netbox/3.5 R92; Linux 2.2)"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:48 +0000] "-" 408 0 "-" "-"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:48 +0000] "-" 408 0 "-" "-"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:48 +0000] "-" 408 0 "-" "-"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:49 +0000] "-" 408 0 "-" "-"
ns1.customersite.com:80 212.185.56.58 - - [16/Nov/2013:21:32:49 +0000] "-" 408 0 "-" "-"

It appears like some Website based attack / bot right?
Im curious why iptables dont block it, why should htaccess block rule work?

Subject: Re: Cant block DDoS to a VPS? How to do it?

Posted by grep on Sun, 17 Nov 2013 02:16:32 GMT
View Forum Message <> Reply to Message

When you block IPs on HN Node it will not affect openvz containers.
You need to block bad IPs on container. Maybe you can block on HN when drop IPs to forward chain and not to input.

If
212.185.56.58 - - [16/Nov/2013:21:32:49 +0000] "-" 408 0 "-" "-"Is an attacking IP it seems to be very simple HTTP flood which you can block it easy. Just write a script which parse the http log and check the num of connections which call /. If greater than x then drop. Or use mod security, but this will use more cpu.
Or just block all traffic which has no referrer.

And it seems that bad IPs just come from one subnet - block it & write abuse with tcpdump file as proof.

If you delete the IP from your Hostsystem the traffic should be nullrouted. If not then ask your dc, maybe they 'hard-route' the IP to your server.

If you want to try migrating the DDoS check out litespeed and nginx. But your HN must have enough network speed and if ddos goes to hard then you may get in trouble with your dc.

Quote:
::1 - - [16/Nov/2013:21:32:59 +0000] "OPTIONS * HTTP/1.0" 200 152 "-" "Apache/2.2.14 (Ubuntu) (internal dummy connection)"
FULLL of thisnormal.

Subject: Re: Cant block DDoS to a VPS? How to do it?
Posted by postcd on Mon, 18 Nov 2013 14:23:27 GMT
View Forum Message <> Reply to Message

grep, thank you for valuable info. I blocked the IP on VPS and also added deny from rules into .htaccess on that VPS.
It appears VPS was not yet overloaded.

Also here is the script/SW/Fail2ban which may help automatically banning abusers who load some webpage/element repeatedly:

Subject: Re: Cant block DDoS to a VPS? How to do it?
Posted by grep on Mon, 18 Nov 2013 19:08:21 GMT
View Forum Message <> Reply to Message

Hi,

yes, i meant such a script. It is better to block IPs before they hit to webserver, if bad ip hit

webserver and webserver just block this ip it will have more load than just blocking it with iptables.

And i recommend you to check out nginx and litespeed. If using this you wouldnt need to block smaller attacks because this webservers can just handle it.
If the attacker make his attacke less simple then your regex will fail and you gonna overloaded again.
