Subject: CSF xt_connlimit on vm failed
Posted by Bapu Desi on Fri, 24 Jun 2011 09:10:08 GMT
View Forum Message <> Reply to Message

Hello everybody,

i'm trying to find solution but i found nothing about my problem can you please help me it will be grateful of you.

i have installed CSF on my vm based on proxmox but i have only 2 error i have fixed all others but can't find solution for 2 only.

on Vm

Quote:server24535:~# /etc/csf/csftest.pl

Testing ip_tables/iptable_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing xt_connlimit...FAILED [Error: iptables: Unknown error 18446744073709551615] - Required for CONNLIMIT feature
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/ipt_REDIRECT...OK

I would like to fix xt_connlimit.
Network is set as bridge and not venet.

on main server i have set for my /etc/vz/vz.conf
Quote:
IPv4 iptables kernel modules
IPTABLES="ipt_REJECT ipt_recent ipt_owner ipt_REDIRECT ipt_tos ipt_TOS ipt_LOG ip_conntrack ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_le ipt_length ipt_state iptable_nat ip_nat_ftp"

also do i need to edit
these files?
Quote:/var/lib/vz/private/101/etc/sysconfig/iptables-config
/var/lib/vz/private/102/etc/sysconfig/iptables-config
/var/lib/vz/root/101/etc/sysconfig/iptables-config
/var/lib/vz/root/102/etc/sysconfig/iptables-config

when i have added xt_connlimit to /etc/vz/vz.conf

Quote:## IPv4 iptables kernel modules
IPTABLES="ipt_REJECT ipt_recent ipt_owner ipt_REDIRECT ipt_tos ipt_TOS ipt_LOG ip_conntrack ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_le ipt_length ipt_state iptable_nat ip_nat_ftp xt_connlimit"

now getting this these warning when entering in the VM

Quote:server24535:~# vzctl enter 101
Warning: Unknown iptable module: ipt_le, skipped
Warning: Unknown iptable module: xt_connlimit, skipped

thank you in advance for your help

Subject: Re: CSF xt_connlimit on vm failed
Posted by siterack_net on Sat, 10 Sep 2011 18:40:40 GMT
View Forum Message <> Reply to Message

I too would like to know a workaround to this, as I would definitely find connection limiting a plus.

I often have clients that buy into those pay for traffic scams, where the seller just uses a bot to hit the site over and over, spiking system loads.
While I use csf to kill off excessive processes, connection limiting would probably be more effective.

Since OpenVZ uses a "monolithic" kernal, I'm not sure how to get this working, as CSF states monolithic kernals tyoically lack this function.

Subject: Re: CSF xt_connlimit on vm failed
Posted by hostingDNS on Mon, 23 Jan 2012 11:01:32 GMT
View Forum Message <> Reply to Message

I find solution :

add xt_connlimit to vz.conf

uninstall vzctl :

yum remove vzctl vzctl-lib

install vzctl again :

yum install vzctl vzctl-lib

restart vz :

service vz restart

Subject: Re: CSF xt_connlimit on vm failed
Posted by cheitac on Wed, 08 Feb 2012 08:28:35 GMT
View Forum Message <> Reply to Message

Hi All!

I have same problem too.
Warning: Unknown iptable module: ipt_le, skipped
Warning: Unknown iptable module: xt_connlimit, skipped

kernel 2.6.18-274.7.1.el5.028stab095.1 host OS CENTOS 5.7 latest.

Subject: Re: CSF xt_connlimit on vm failed
Posted by lelik67 on Fri, 10 Feb 2012 15:06:36 GMT
View Forum Message <> Reply to Message

The issue is that, due to the way RH builds iptables, there have been longstanding disparities between the iptables userspace tool and the kernel. For example, in Fedora 6/RHEL 5/CentOS 5, although there is an iptables module in /lib/iptables/libipt_connlimit.so which supports the connlimit match in iptables, there is no corresponding netfilter module in /lib/modules/(version)/kernel/net/ipv4/netfilter/
to handle it in the kernel.

Since there is no stock kernel support for connlimit, the iptables module included in these distros is rather useless.

To have connlimit working there are three options:

1. Upgrade your node kernel to a newer version (Co-operation of your VPS provider is required).

The connlimit module finally went into mainline at kernel v2.6.23.
xxx://xxx.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.23

Latest stable kernel for RHEL5 2.6.18 does not have it.
xxx://wiki.openvz.org/Download/kernel/rhel5/028stab095.1

But latest stable kernel for RHEL6 2.6.32 does:
xxx://wiki.openvz.org/Download/kernel/rhel6/042stab044.17

2. Patch it and maintain your own build (Super co-operation of your VPS provider is required as they have to compile a custom kernel for you).

See xxx://xxx.netfilter.org/projects/patch-o-matic/pom-external.html#pom-external-connlimit

3. Find a pre-built module maintained elsewhere.

Hope this helpful.

Subject: Re: CSF xt_connlimit on vm failed
Posted by Dexus on Wed, 21 Mar 2012 08:56:25 GMT
View Forum Message <> Reply to Message

^
That is not the case here.

connlimit is working on the node and in the containers, only VZ tools are reporting this warning about unknown module...

This is from the host node with connlimit module loaded on CentOS 6...

```
# lsmod | grep connlimit
xt_connlimit           3446  1
nf_conntrack          80693  7
vzrst,xt_connlimit,nf_conntrack_ftp,iptable_nat,nf_nat,nf_conntrack_ipv4,xt_state

# iptables -A INPUT -p tcp --syn --dport 23 -m connlimit --connlimit-above 2 -j REJECT

# iptables --list -n | grep conn
REJECT     tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:23 flags:0x17/0x02 #conn/32 > 2
reject-with icmp-port-unreachable
```

As you can see it's working.

But there is still a warning on every vz tool execution...

```
# vzlist
Warning: Unknown iptable module: xt_connlimit, skipped
      CTID      NPROC STATUS    IP_ADDR         HOSTNAME
```

Here is vzlist trace, where you can see that vzlist is reporting warning after it load the modules list from vz.conf...

```
open("/etc/vz/vz.conf", O_RDONLY)       = 3
stat("/etc/vz/vz.conf", {st_mode=S_IFREG|0644, st_size=1392, ...}) = 0
```

```
fstat(3, {st_mode=S_IFREG|0644, st_size=1392, ...}) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7fdafb187000
read(3, "## Global parameters\nVIRTUOZZO=y"..., 4096) = 1392
write(2, "Warning: Unknown iptable module:"..., 54Warning: Unknown iptable module:
xt_connlimit, skipped) = 54
write(2, "\n", 1
)                       = 1
read(3, "", 4096)                       = 0
close(3)                                = 0
```