

---

Subject: RHEL6 and stateful firewall inside container  
Posted by [masse](#) on Wed, 01 Feb 2012 11:17:06 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hello users@openvz.org

I'm trying to upgrade our rhel5 based openvz servers to rhel6 but I got problem with iptables. If I try to use firewall inside container, I can load rules, but firewall rejects all incoming packets. Host is redhat-6 and container is centos-6. I tested with kernels

vzkernel-2.6.32-042stab044.17.x86\_64  
vzkernel-2.6.32-042stab048.1.x86\_64  
vzkernel-2.6.32-042stab049.2.x86\_64

My firewall config

```
# Generated by iptables-save v1.4.7 on Wed Feb  1 13:05:26 2012
*mangle
:PREROUTING ACCEPT [2:381]
:INPUT ACCEPT [2:381]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [4:559]
:POSTROUTING ACCEPT [4:559]
COMMIT
# Completed on Wed Feb  1 13:05:26 2012
# Generated by iptables-save v1.4.7 on Wed Feb  1 13:05:26 2012
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [4:559]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Wed Feb  1 13:05:26 2012
```

Is it know problem or is it my misconfiguration? Firewall on redhat-5 is functioning fine.

--

Mikko Hirvonen <[Mikko.V.Hirvonen@helsinki.fi](mailto:Mikko.V.Hirvonen@helsinki.fi)>  
Helsingin yliopisto / Tietotekniikkakeskus / Verkkopalvelut

---

Subject: Re: RHEL6 and stateful firewall inside container  
Posted by [Vasily Averin](#) on Wed, 01 Feb 2012 12:39:26 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hi Mikko,

1) You need to enable conntrack support for container, it is disabled by default.  
IIRC following command should be enough to enable conntrack support for specified container only:

```
# vzctl set <CTID> --iptables iptable_filter --iptables ip_conntrack --save
```

2) Also you need to load all modules on the host before loading of rules inside container.  
Container cannot load modules, even indirectly. that's why loading of iptables rules failed inside container.

we recommend to add all required modules into iptables service configuration on the host.  
on CentOS6 nodes you need to add all used modules into IPTABLES\_MODULES variable in /etc/sysconfig/iptables-config file.

thank you,  
Vasily Averin

On 02/01/2012 03:17 PM, Mikko Vasili Hirvonen wrote:

> Hello users@openvz.org

>

> I'm trying to upgrade our rhel5 based openvz servers to rhel6 but I got

> problem with iptables. If I try to use firewall inside container, I can

> load rules, but firewall rejects all incoming packets. Host is redhet-6

> and container is centos-6. I tested with kernels

>

> vzkernel-2.6.32-042stab044.17.x86\_64

> vzkernel-2.6.32-042stab048.1.x86\_64

> vzkernel-2.6.32-042stab049.2.x86\_64

>

> My firewall config

> # Generated by iptables-save v1.4.7 on Wed Feb 1 13:05:26 2012

> \*mangle

> :PREROUTING ACCEPT [2:381]

> :INPUT ACCEPT [2:381]

> :FORWARD ACCEPT [0:0]

> :OUTPUT ACCEPT [4:559]

> :POSTROUTING ACCEPT [4:559]

> COMMIT

> # Completed on Wed Feb 1 13:05:26 2012

> # Generated by iptables-save v1.4.7 on Wed Feb 1 13:05:26 2012

> \*filter

> :INPUT ACCEPT [0:0]

> :FORWARD ACCEPT [0:0]

> :OUTPUT ACCEPT [4:559]

> -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

```
> -A INPUT -p icmp -j ACCEPT
> -A INPUT -i lo -j ACCEPT
> -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
> -A INPUT -j REJECT --reject-with icmp-host-prohibited
> -A FORWARD -j REJECT --reject-with icmp-host-prohibited
> COMMIT
> # Completed on Wed Feb  1 13:05:26 2012
>
> Is it know problem or is it my misconfiguration? Firewall on redhat-5 is
> functioning fine.
>
>
```

---

---

Subject: Re: RHEL6 and stateful firewall inside container  
Posted by [Vasily Averin](#) on Wed, 01 Feb 2012 12:41:01 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

On 02/01/2012 04:39 PM, Vasily Averin wrote:

```
> Hi Mikko,
>
> 1) You need to enable conntrack support for container, it is disabled by default.
> IIRC following command should be enough to enable conntrack support for specified container
> only:
> # vzctl set <CTID> --iptables iptable_filter --iptables ip_conntrack --save
```

Sorry, I did not noticed that you're using mangle table too, so you need to add also "--iptables iptable\_mangle" into command above.

```
> 2) Also you need to load all modules on the host before loading of rules inside container.
> Container cannot load modules, even indirectly. that's why loading of iptables rules failed inside
> container.
> we recommend to add all required modules into iptables service configuration on the host.
> on CentOS6 nodes you need to add all used modules into IPTABLES_MODULES variable in
> /etc/sysconfig/iptables-config file.
>
> thank you,
> Vasily Averin
>
> On 02/01/2012 03:17 PM, Mikko Vasili Hirvonen wrote:
>> Hello users@openvz.org
>>
>> I'm trying to upgrade our rhel5 based openvz servers to rhel6 but I got
>> problem with iptables. If I try to use firewall inside container, I can
>> load rules, but firewall rejects all incoming packets. Host is redhet-6
>> and container is centos-6. I tested with kernels
>>
>> vzkernel-2.6.32-042stab044.17.x86_64
```

```
>> vzkernel-2.6.32-042stab048.1.x86_64
>> vzkernel-2.6.32-042stab049.2.x86_64
>>
>> My firewall config
>> # Generated by iptables-save v1.4.7 on Wed Feb  1 13:05:26 2012
>> *mangle
>> :PREROUTING ACCEPT [2:381]
>> :INPUT ACCEPT [2:381]
>> :FORWARD ACCEPT [0:0]
>> :OUTPUT ACCEPT [4:559]
>> :POSTROUTING ACCEPT [4:559]
>> COMMIT
>> # Completed on Wed Feb  1 13:05:26 2012
>> # Generated by iptables-save v1.4.7 on Wed Feb  1 13:05:26 2012
>> *filter
>> :INPUT ACCEPT [0:0]
>> :FORWARD ACCEPT [0:0]
>> :OUTPUT ACCEPT [4:559]
>> -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
>> -A INPUT -p icmp -j ACCEPT
>> -A INPUT -i lo -j ACCEPT
>> -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
>> -A INPUT -j REJECT --reject-with icmp-host-prohibited
>> -A FORWARD -j REJECT --reject-with icmp-host-prohibited
>> COMMIT
>> # Completed on Wed Feb  1 13:05:26 2012
>>
>> Is it know problem or is it my misconfiguration? Firewall on redhat-5 is
>> functioning fine.
>>
>>
>
```

---

Subject: Re: RHEL6 and stateful firewall inside container

Posted by [masse](#) on Thu, 02 Feb 2012 08:51:10 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Thank you Vasily. It is functioning now. I saw it is documented in vzctl man page too.

On 02/01/2012 02:41 PM, Vasily Averin wrote:

> On 02/01/2012 04:39 PM, Vasily Averin wrote:

>> Hi Mikko,

>>

>> 1) You need to enable conntrack support for container, it is disabled by default.

>> IIRC following command should be enough to enable conntrack support for specified container only:

```

>> # vzctl set <CTID> --iptables iptable_filter --iptables ip_conntrack --save
>
> Sorry, I did not noticed that you're using mangle table too, so you need to add also "--iptables
iptables_mangle" into command above.
>
>> 2) Also you need to load all modules on the host before loading of rules inside container.
Container cannot load modules, even indirectly. that's why loading of iptables rules failed inside
container.
>> we recommend to add all required modules into iptables service configuration on the host.
>> on CentOS6 nodes you need to add all used modules into IPTABLES_MODULES variable in
/etc/sysconfig/iptables-config file.
>>
>> thank you,
>> Vasily Averin
>>
>> On 02/01/2012 03:17 PM, Mikko Vasili Hirvonen wrote:
>>> Hello users@openvz.org
>>>
>>> I'm trying to upgrade our rhel5 based openvz servers to rhel6 but I got
>>> problem with iptables. If I try to use firewall inside container, I can
>>> load rules, but firewall rejects all incoming packets. Host is redhet-6
>>> and container is centos-6. I tested with kernels
>>>
>>> vzkernel-2.6.32-042stab044.17.x86_64
>>> vzkernel-2.6.32-042stab048.1.x86_64
>>> vzkernel-2.6.32-042stab049.2.x86_64
>>>
>>> My firewall config
>>> # Generated by iptables-save v1.4.7 on Wed Feb  1 13:05:26 2012
>>> *mangle
>>> :PREROUTING ACCEPT [2:381]
>>> :INPUT ACCEPT [2:381]
>>> :FORWARD ACCEPT [0:0]
>>> :OUTPUT ACCEPT [4:559]
>>> :POSTROUTING ACCEPT [4:559]
>>> COMMIT
>>> # Completed on Wed Feb  1 13:05:26 2012
>>> # Generated by iptables-save v1.4.7 on Wed Feb  1 13:05:26 2012
>>> *filter
>>> :INPUT ACCEPT [0:0]
>>> :FORWARD ACCEPT [0:0]
>>> :OUTPUT ACCEPT [4:559]
>>> -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
>>> -A INPUT -p icmp -j ACCEPT
>>> -A INPUT -i lo -j ACCEPT
>>> -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
>>> -A INPUT -j REJECT --reject-with icmp-host-prohibited
>>> -A FORWARD -j REJECT --reject-with icmp-host-prohibited

```

```
>>> COMMIT
>>> # Completed on Wed Feb  1 13:05:26 2012
>>>
>>> Is it know problem or is it my misconfiguration? Firewall on redhat-5 is
>>> functioning fine.
>>>
>>>
>>
>
```

--

Mikko Hirvonen <Mikko.V.Hirvonen@helsinki.fi>  
Helsingin yliopisto / Tietotekniikkakeskus / Verkkopalvelut

---