

OpenVZ a Firewall

Defaultní konfigurace OpenVZ je poněkud restriktivní k provozování stavového firewallu v kontejnerech, proto je potřeba provést následující úpravu nastavení:

V souboru **/etc/vz/conf/CTID.conf** vyhledáme položku **NETFILTER** a upravíme ji takto

```
NETFILTER="full"
```

Pokud tam volba ještě není, tak ji přidáme. Ve výchozím stavu bývá zakázán stavový firewall.

Ve starších verzích OpenVZ bylo nutné ještě nastavit, jaké moduly firewallu může kontejner využívat: Do souboru **/etc/vz/vz.conf** přidáme následující řádky

[/etc/vz/vz.conf](#)

```
## IPv4 iptables kernel modules to be enabled in CTs by default
IPTABLES="ipt_REJECT ipt_tos ipt_TOS ipt_LOG ipt_limit ipt_multiport
iptables_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length
ipt_state ip_conntrack_ftp ip_conntrack ipt_comment"
## IPv4 iptables kernel modules to be loaded by init.d/vz script
IPTABLES_MODULES="$IPTABLES"

## Enable IPv6
IPV6="yes"

## IPv6 ip6tables kernel modules
IP6TABLES="ip6_tables ip6table_filter ip6table_mangle ip6t_REJECT
ip6t_LOG nf_conntrack_ipv6"
```

Uvedené nastavení je globální pro všechny VPS. Pokud z nějakého důvodu chceme firewall povolit jen pro některé kontejnery, přidáme do příslušného **conf** souboru virtuálu řádky [IPTABLES](#) a [IP6TABLES](#)



Aby to fungovalo, je potřeba uvedené moduly načíst ještě před startem kontejnerů !

V Centosu se provádí natažení všech potřebných modulů přidáním popř. editací řádku v těchto konfiguračních souborech:

[/etc/sysconfig/iptables-config](#)

```
IPTABLES_MODULES="ip_tables ipt_REJECT ipt_tos ipt_limit ipt_multiport
iptables_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length
ipt_LOG ipt_state ipt_TOS ip_conntrack_ftp ip_conntrack ipt_comment"
```

[/etc/sysconfig/ip6tables-config](#)

```
IP6TABLES_MODULES="ip6_tables ip6table_filter ip6table_mangle  
ip6t_REJECT ip6t_LOG nf_conntrack_ipv6"
```

V Debianu bude potřeba provést obdobný krok pomocí **/etc/modules**

[/etc/modules](#)

```
xt_comment  
xt_DSCP  
ipt_LOG  
nf_nat  
ip6t_REJECT  
ip6table_mangle  
ip6table_filter  
ip6_tables  
xt_length  
xt_hl  
xt_tcpmss  
xt_TCPMSS  
iptable_mangle  
iptable_filter  
xt_multiport  
xt_limit  
xt_dscp  
ipt_REJECT  
ip_tables  
nf_conntrack_ipv6  
nf_defrag_ipv6  
xt_state  
nf_conntrack_ipv4  
nf_conntrack  
nf_defrag_ipv4
```

Na závěr povolte ipcontrack v openvz, jinak nebude správně fungovat firewall:

[/etc/modprobe.d/openvz.conf](#)

```
options nf_conntrack ip_conntrack_disable_ve0=0
```

Poznámka: pokud vám po nějakém upgradu kernelu přestane fungovat správně firewall na hostitelském stroji (klasicky se projevuje tak, že dropuje všechny příchozí pakety), nastavte tuto volbu také i když firewall v kontejnerech nepotřebujete.

Nyní proveďte restart stroje a firewall je připraven k používání

From:

<https://wiki.spoje.net/> - **SPOJE.NET**

Permanent link:

https://wiki.spoje.net/doku.php/howto/vps/openvz/openvz_iptables

Last update: **2016/01/18 14:24**

