

iptables Docker Engine

```
docker- - DNAT . INPUT docker- , .  
docker', FORWARD, DOCKER-USER.
```



```
# DO NOT FORGET TO RESTART DOCKER ENGINE AFTER APPLYING IPTABLES RULES  
  
*mangle  
:PREROUTING ACCEPT [0:0]  
:INPUT ACCEPT [0:0]  
:FORWARD ACCEPT [0:0]  
:OUTPUT ACCEPT [0:0]  
:POSTROUTING ACCEPT [0:0]  
COMMIT  
  
*nat  
:PREROUTING ACCEPT [0:0]  
:INPUT ACCEPT [0:0]  
:OUTPUT ACCEPT [0:0]  
:POSTROUTING ACCEPT [0:0]  
COMMIT  
  
*filter  
:INPUT ACCEPT [0:0]  
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  
-A INPUT -i lo -j ACCEPT  
-A INPUT -p icmp -j ACCEPT  
# Docker traffic  
-A INPUT -i docker0 -j ACCEPT  
-A INPUT -i br-+ -j ACCEPT  
# Latera Gws  
-A INPUT -s 188.120.244.146 -j ACCEPT  
-A INPUT -s 5.63.158.193 -j ACCEPT  
-A INPUT -j DROP  
:FORWARD ACCEPT [0:0]  
:OUTPUT ACCEPT [0:0]  
:DOCKER-USER - [0:0]  
-A DOCKER-USER -m state --state RELATED,ESTABLISHED -j RETURN  
# Docker traffic  
-A DOCKER-USER -i docker0 -j RETURN  
-A DOCKER-USER -i br-+ -j RETURN  
# Latera Gws  
-A DOCKER-USER -s 188.120.244.146 -j RETURN  
-A DOCKER-USER -s 5.63.158.193 -j RETURN  
# HTTP(S)  
-A DOCKER-USER -p tcp -m conntrack --ctdir ORIGINAL --ctorigdstport 80 -j RETURN  
-A DOCKER-USER -p tcp -m conntrack --ctdir ORIGINAL --ctorigdstport 443 -j RETURN  
-A DOCKER-USER -j DROP  
COMMIT
```

:

1. docker- DOCKER-USER, -- INPUT.
2. DOCKER-USER RETURN, Docker Engine.
3. DOCKER-USER conntrack, DNAT .

iptables (, /etc/network/iptables.up.rules Debian /etc/sysconfig/iptables Oracle Linux) Docker Engine.

:

1. iptables;
2. Docker Engine (: **sudo systemctl stop docker**, **docker-**,);
3. iptables;
4. Docker Engine (: sudo systemctl start docker)
5. docker- ().



Docker Engine iptables . , Docker Engine (. <https://github.com/moby/moby/issues/12294>).

iptables Debian Linux [iptables-apply](#) (,). iptables, .

1. iptables « ». iptables, .
2. iptables . («») docker' , , .