
Subject: Re: OpenVZ and Bastille/iptables?

Posted by [marsvin](#) on Sat, 23 Dec 2006 22:39:00 GMT

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

You know I think I jumped the gun a bit there

Enabling ipforwarding manually made the VPS work again but when the firewall is running it still blocks all access to the VPS. At least it seems to block the routing to the VPS, since no dropped packets turn up in the log I just get this:

```
ssh 10.0.0.102
```

```
ssh: connect to host 10.0.0.102 port 22: No route to host
```

I will list the things you asked for (with the firewall enabled):

```
route -nv
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.0.0.102	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
10.0.0.103	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
10.0.0.101	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
10.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	10.0.0.2	0.0.0.0	UG	0	0	0	eth0

```
ifconfig -a
```

```
eth0    Link encap:Ethernet  HWaddr 00:30:48:5C:28:60
        inet addr:10.0.0.12  Bcast:255.255.255.255  Mask:255.255.255.0
        inet6 addr: fe80::230:48ff:fe5c:2860/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:14344 errors:0 dropped:0 overruns:0 frame:0
        TX packets:10559 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1415554 (1.3 MiB)  TX bytes:1706761 (1.6 MiB)
        Interrupt:177
```

```
eth1    Link encap:Ethernet  HWaddr 00:30:48:5C:28:61
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
        Interrupt:193
```

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
```

inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:8 errors:0 dropped:0 overruns:0 frame:0
TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:560 (560.0 b) TX bytes:560 (560.0 b)

sit0 Link encap:IPv6-in-IPv4
NOARP MTU:1480 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

venet0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1
RX packets:5618 errors:0 dropped:0 overruns:0 frame:0
TX packets:5561 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:535413 (522.8 KiB) TX bytes:523141 (510.8 KiB)

cat /proc/sys/net/ipv4/ip_forwarding
1

iptables -nv -L
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination LOG flags 0 level 4 prefix
0 0 LOG tcp -- !lo * 0.0.0.0/0 127.0.0.0/8 LOG flags 0 level 4 prefix
`INPUT DROP 0`
0 0 DROP tcp -- !lo * 0.0.0.0/0 127.0.0.0/8
47 3052 ACCEPT 0 -- * * 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
0 0 LOG 0 -f * * 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 4 prefix
`INPUT DROP 1`
0 0 DROP 0 -f * * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
0 0 LOG 0 -- * * 224.0.0.0/4 0.0.0.0/0 LOG flags 0 level 4 prefix
`INPUT DROP 2`
0 0 DROP 0 -- * * 224.0.0.0/4 0.0.0.0/0
0 0 PUB_IN 0 -- eth+ * 0.0.0.0/0 0.0.0.0/0
0 0 PUB_IN 0 -- ppp+ * 0.0.0.0/0 0.0.0.0/0
0 0 PUB_IN 0 -- slip+ * 0.0.0.0/0 0.0.0.0/0
0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpts:137:139
0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpts:137:139
0 0 DROP 0 -- * * 0.0.0.0/0 224.0.0.0/8
0 0 LOG 0 -- * * 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 4 prefix
`INPUT DROP 4`

```
0 0 DROP 0 -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain FORWARD (policy DROP 0 packets, 0 bytes)

```
pkts bytes target prot opt in out source destination
0 0 ACCEPT 0 -- * * 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
```

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

```
pkts bytes target prot opt in out source destination
37 13716 PUB_OUT 0 -- * * eth+ 0.0.0.0/0 0.0.0.0/0
0 0 PUB_OUT 0 -- * * ppp+ 0.0.0.0/0 0.0.0.0/0
0 0 PUB_OUT 0 -- * * slip+ 0.0.0.0/0 0.0.0.0/0
```

Chain INT_IN (0 references)

```
pkts bytes target prot opt in out source destination
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0
0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpts:137:139
0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpts:137:139
0 0 DROP 0 -- * * 0.0.0.0/0 224.0.0.0/8
0 0 LOG 0 -- * * 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 4 prefix
`INT_IN DROP 6`
0 0 DROP 0 -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain INT_OUT (0 references)

```
pkts bytes target prot opt in out source destination
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 0 -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain PAROLE (9 references)

```
pkts bytes target prot opt in out source destination
0 0 ACCEPT 0 -- * * 0.0.0.0/0 0.0.0.0/0
```

Chain PUB_IN (3 references)

```
pkts bytes target prot opt in out source destination
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 3
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 0
0 0 ACCEPT icmp -- * * 0.0.0.0/0 0.0.0.0/0 icmp type 11
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:25
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:110
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:143
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:465
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:993
0 0 PAROLE tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:995
0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpts:137:139
0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpts:137:139
```

0	0	DROP	0	--	*	*	0.0.0.0/0	224.0.0.0/8	
0	0	LOG	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 4 prefix
`PUB_IN DROP 3'									
0	0	DROP	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	LOG	0	--	*	*	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 4 prefix
`PUB_IN DROP 5'									
0	0	DROP	0	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain PUB_OUT (3 references)

pkts	bytes	target	prot	opt	in	out	source	destination
35	12668	ACCEPT	0	--	*	*	0.0.0.0/0	0.0.0.0/0