
Subject: Pushing traffic to a public IP on a container.
Posted by [pnunn](#) on Mon, 10 Jan 2011 03:25:18 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi folks,

I'm guessing this must be a faq somewhere, but I've been trying for days to sort this out with no success at all.

I have a setup with a Node with one Nic, which has a 192.168.333.x address on it.

I have containers running on this with 192.168.333.a-k on them, and all is fine as long as I'm on this network.

I have one container with 111.123.344.456 a public address, which I can ping from outside the 192 network, but try as I might I cannot get ssh or anything else to route to it, unless I'm within my 192 network.

I've tried the suggestions here on iptables rules (most of which seem to be related to restricting traffic, no such problem here, adding routes etc.. but still no joy at all.

Currently there is no firewall on the Node nor the container.

I'm sure this must be easy and that I'm missing something fundamental here.

```
iptables dump on the node is
iptables --line-numbers -t nat -L && iptables -t filter -L && iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
num target    prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
num target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
num target    prot opt source          destination
Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain FORWARD (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination

Chain INPUT (policy ACCEPT)
target    prot opt source          destination
```

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain POSTROUTING (policy ACCEPT)

target prot opt source destination

route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.333.46	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
192.168.333.45	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
192.168.333.42	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
111.123.344.456	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
192.168.333.35	0.0.0.0	255.255.255.255	UH	0	0	0	venet0
192.168.333.0	0.0.0.0	255.255.255.128	U	0	0	0	eth0
0.0.0.0	192.168.333.1	0.0.0.0	UG	100	0	0	eth0

(addresses changed to protect the guilty)..

Can anyone shed any light on what I'm doing wrong.

I tried vzfirewall, but no joy there either (although it did correctly block some traffic).

Running out of ideas..

Thanks heaps.

Peter.