Subject: Hosting Company setup .....
Posted by schjeall on Wed, 25 Feb 2009 20:25:11 GMT
View Forum Message <> Reply to Message

I was thinking about how hosting companies setup OpenVZ when it comes to providing access to a VE with a public ip-address. How do they configure networking (using veth or venet), security (if using veth, how do they avoid sniffing of traffic) etc.

Can anyone come with an explanation?

My idea is to use venet. Each VE is assigned an ip-address in the range 192.168.2.1/24. ip-masquerade is setup on the HN.

```
 Internet  (Public ip's are mapped to e.g. 192.168.1.1/24)
   |
 +--+---+  xxx.yyy.xxx.yy1 -> 192.168.1.1
 |ROUTER|  xxx.yyy.xxx.yy2 -> 192.168.1.2
 +-+----+  xxx.yyy.xxx.yyn -> 192.168.1.n
  D|
  M|
  Z|
+--+------------+
| Hardware node | Listenens for 192.168.1.x/24:[1..n] and
|               | dnat any port + ip to 192.168.2.x:[1..n]
+---------------+
| IP tables     | 192.168.1.x:any port dnat 192.168.2.x:any port
|               |
+---------------+
| N1 | N2 | N3  | venet 192.168.2.1/24
+---------------+
```

My idea is probably not correct and I need some guidance on how to make this work. I want all ports on any VE to be available, when doing something on the corresponding public IP. Therefore I map all public ip's to 192.168.1.x:[1..n] and dnat this to each VE assigned ip address 192.168.2.x:[1..n].

How can dnat be used even smarter or can this be solved more elegantly?