Subject: Re: Bridging inside the CT, snort in-line?!
Posted by vitorallo on Mon, 02 Feb 2009 14:47:17 GMT
View Forum Message <> Reply to Message

Of course it is not a silly question.
Deploying snort in line means create an IPS and not an IDS. IPSes - intrusion detection and
prevention - work by analyzing the traffic and reacting "in line" by applying a response like: block,
rewrite and so on. To do that they need to stay in the middle of the traffic flow.

Any good IPS (I work for Internet Security Systems) has two interface. IPS are deployed literally in
the middle of the traffic trunk.

internet ----- firewall ---- (portA)IPS(portB)---- inner network

usually IPSes are transparent! there is a bridge/special nic driver that brings the traffic over the
two interfaces and blocks it when needed

Snort can work as an IPS, it is actually an IDS. To do that, it needs to stay upon a network bridge.
it can grab traffic from libpcap or the iptables QUEUE. For the IPS/Bridge we need the second
feature.

Using little bit of fancy ASCII art...

```
..iptables QUEUE.. <----------- snort
!--------------------!
!---linux bridge---!
+......................+
A---- TRAFFIC --- B
```

My aim is to scale security architecture, creating an easy re-distributable template with snort in
line to secure the
Virtual Infrastructure!!! THAT WILL BE COOL... of course I
want to share it open.

Unfortunately, to do it I need to bridge inside the CT, I need
linux bridge.ko (bridge utils) active inside and iptables running.

No problem for iptables, snort and all the rest.. but I cannot bridge eth0 and eth1 (virtual
interfaces) inside the CT...

Imagine how cool it would be....to have something like

----Host networking----VirtualWorld---IPS transparent---multiple OpenVZ machines