Subject: Veth und Snort
Posted by jms1000 on Wed, 26 Jan 2011 12:32:05 GMT
View Forum Message <> Reply to Message

Hi,

ich tappe im dunkeln, vielleicht kann mir jemand passende Tipps geben ?

Ich habe auf dem Host mehrere Interfaces die ich mit Veth auf den Container durch reiche. So lange ich das IP-Routing für die Interface aktiv habe (als IP-Adressen eingerichtet), klappt alles wunderbar. Auch kann ich auf den diversen Interfacen auf dem Host und dem Container einen Tcpdump starten, der wunderbar loggt.

Nun will ich aber eines der Interface ohne IP-Adressen laufen lassen und das Interface mit dem Monitorport eines Switches verbinden. Im Container soll das dann durch Snort geloggt werden.

Wenn ich besagten Monitorport an einem Interface anschließe, kann ich Daten mit Tcpdump auf dem eth-Interface (reales Interface) des Host sehen, nicht aber auf dem Veth-Interfaces des Hosts oder des Containers.

Meiner Vermutung nach klemmt hier vielleicht irgend so ein sysctl Eintrag.

Kann hier jemand helfen ???

Mfg.jms

Subject: Re: veth und snort
Posted by curx on Thu, 27 Jan 2011 11:33:05 GMT
View Forum Message <> Reply to Message

Hi,

wie sollte es auch funktionieren.

das "spezielle" veth Device kann keine Pakete vom Monitoring Port abbekommen, daher sehe ich 2 Möglichkeiten:

1) (software) bridge (im HUB Modus) mit dem realen Interface (am MonitoringPort des Switches) und veth

2) exclusiver Zugriff des containers auf das reale Interface

Gruß,
 Thorsten

Subject: Re: veth und snort
Posted by jms1000 on Thu, 27 Jan 2011 11:50:49 GMT
View Forum Message <> Reply to Message

curx wrote on Thu, 27 January 2011 06:33Hi,

1) (software) bridge (im HUB Modus) mit dem realen Interface (am MonitoringPort des Switches) und veth

2) exclusiver Zugriff des containers auf das reale Interface

das habe ich nicht ganz verstanden, warum das nicht gehen sollte.
wenn ich "normales" ip-routing auf den VETH interfacen habe, tut alles. klemme ich aber den switch-monitor-port dran, tut es nicht mehr.

und wie bekomme ich 2) umgesetzt ? das sollte doch mit dem veth eigentlich klappen. oder gibt es etwas besonders für das "exclusiv" ?

mfg.

Subject: Re: veth und snort
Posted by curx on Sun, 30 Jan 2011 22:42:43 GMT
View Forum Message <> Reply to Message

Hi,

nun ja, Du schreibst ja selbst:

> . So lange ich das IP-Routing für die Interface aktiv habe (...) Nun will ich aber eines der Interface ohne IP-Adressen laufen lassen und das Interface mit dem Monitorport eines Switches verbinden (...) kann ich Daten mit Tcpdump auf dem eth-Interface (reales Interface) des Host sehen, nicht aber auf dem Veth-Interfaces (...) des Containers

^_ und wie sollte hier die IPv(4|6) Pakete von ethX (lokalem ethernet Interface am Monitorport) nach vethX (virtuell ethernet Interface) gelagen, wenn kein IP Routing aktiv ist.

Ausgangslage:

monitor_port_des_switch <--> reale_netzwerk_karte <--> veth
 ^_____^

1)
monitor_port_des_switch <--> reale_netzwerk_karte <--> veth

(---- bride im hub modus ----)

2)
monitor_port_des_switch <--> reale_netzwerk_karte als exl.Zugriff in den container

siehe -> http://wiki.openvz.org/Using_real_network_device

Gruß,
Thorsten
