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