
Subject: Re: Bridging inside the CT, snort in-line?!
Posted by [ivani](#) on Wed, 06 Apr 2011 13:56:37 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi vitorallo,

I'm looking for a solution for my problem with the snort IDS.
The parent host run openvz, and I've installed the CentOS 5.5, this is output of uname:

```
uname -a
Linux snortlab 2.6.18-194.8.1.el5.028stab070.5 #1 SMP Fri Sep 17 19:10:36 MSD 2010 i686 i686
i386 GNU/Linux
```

I'm not sure what kind of interface is venet0:0, I thought it was xen.

I tried this:

```
snort -vv -i lo
Running in packet dump mode
```

```
==== Initializing Snort ====
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "lo".
Decoding Ethernet
```

```
==== Initialization Complete ====
```

```
.,_  -*> Snort! <*-
o" )~  Version 2.9.0.4 IPv6 GRE (Build 110)
""  By Martin Roesch & The Snort Team:
    Copyright (C) 1998-2011 Sourcefire, Inc., et al.
    Using libpcap version 1.1.1
    Using PCRE version: 6.6 06-Feb-2006
    Using ZLIB version: 1.2.3
```

```
Commencing packet processing (pid=21572
```

Well, this works fine. But, if I try:

```
snort -vv -i venet0:0
Running in packet dump mode
```

```
==== Initializing Snort ====
Initializing Output Plugins!
pcap DAQ configured to passive.
```

Acquiring network traffic from "venet0:0".
Decoding Linux SLL

--== Initialization Complete ==--

```
.,_  -*> Snort! <*-  
o" )~ Version 2.9.0.4 IPv6 GRE (Build 110)  
"" By Martin Roesch & The Snort Team:  
    Copyright (C) 1998-2011 Sourcefire, Inc., et al.  
    Using libpcap version 1.1.1  
    Using PCRE version: 6.6 06-Feb-2006  
    Using ZLIB version: 1.2.3
```

Commencing packet processing (pid=5776)
Can't acquire (-1) - cooked-mode frame doesn't have room for sll header!

And the snort can't start.

I've googled many pages, forums, mail lists, but I'm still lost about this weird problem.

Any ideas?

Thank you so much.

Regards,

Ivani Nascimento
