

## Re: Snort sensor placement

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2001-09/0157.html>

---

*From:* [JSeddon@semtech.com](mailto:JSeddon@semtech.com)

*Date:* 09/28/01

Subject: Re: Snort sensor placement  
To: Florin Andrei <[florin@sgi.com](mailto:florin@sgi.com)>  
Message-ID: <OFE519AAA3.06C53C5B-ON88256AD4.007CDA5A@semtech.com>  
From: [JSeddon@semtech.com](mailto:JSeddon@semtech.com)  
Date: Thu, 27 Sep 2001 15:51:07 -0700

There's a subtle but sometimes important difference between having a receive-only cable, and running snort on an interface with no IP address.

That difference is that the receive-only cable exists in the real world and an ip-less interface exists in the virtual world. In most cases you are right. You can safely assume that an interface with no IP will not be subject to ip connections, innocent or not. However, if you REALLY REALLY REALLY want to make sure, you make an receive only cable. A receive only cable will guard you against misconfiguration, a mistake in the stack code, an unknown bug in the software driver for the nic that passes traffic with no ip address...anything you can think of. It is foolproof.

Lots of mistakes are made in configuring computers. Lots of bugs/vulns exist that haven't been publicly released. None of that will matter with a receive only cable.

Another example, in most cases you can do Start-Shutdown-Shutdown to turn of windows boxes, that's a function of the virtual world. However, if you REALLY REALLY REALLY want to make sure the motherboard isn't getting power, you pull the plug.

James

Florin Andrei  
<[florin@sgi.com](mailto:florin@sgi.com)> To: [focus-ids@securityfocus.com](mailto:focus-ids@securityfocus.com)  
om> cc:  
Subject: Re: Snort sensor placement  
09/27/01  
03:24 PM

## SecurityFocus IDS: Re: Snort sensor placement

On Thu, 2001-09-27 at 09:39, Rui Lapa wrote:

> *Ever heard of receive only cables?*

>

> [http://personal.ie.cuhk.edu.hk/~msg0/sniffing\\_cable/](http://personal.ie.cuhk.edu.hk/~msg0/sniffing_cable/)

But, isn't this functionally identical to running the sensor on an interface without an IP address?

If you activate the interface, but don't assign an IP address, Snort is still able to run, but no IP connection could be made. It's the same thing as with RO-cables, but simpler.

--

Florin Andrei

"This is a Klingon." "Where did it came from?" "Oklahoma." (from Star Trek Enterprise series premiere)

---

- **Previous message:** [Dave Vehrs: "RE: Snort sensor placement"](#)
- **Maybe in reply to:** [Brian Carvalho: "Snort sensor placement"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)