



Neohapsis is currently accepting applications for employment. For more information, please visit our website www.neohapsis.com or email hr@neohapsis.com

Neohapsis > Archives > Snort IDS> 2002-10

snort's putting the -i bond0 into promisc didn't propagate back through to the underlying eth interfaces.

In Red Hat 7.3, with the default 2.4.18-3 kernel, it's really easy to bond multiple channels to snort them all. The technique is documented in /usr/src/linux/Documentation/networking/bonding.txt. In brief:

```
grep bond0 /etc/modules.conf || echo alias bond0 bonding >/etc/modules.conf
ifconfig bond0 promisc up
for if in eth1 eth2 ...;do
    ifconfig $if promisc up
    ifenslave bond0 $if
done
snort ... -i bond0 ...
```

Works great. The ifenslave invocations whinge a bit about all the things they can't do with the unnumbered interfaces, but it all works.

I used 3 Compaq DL-320s for a test setup. Each of these comes with two eeepro100 interfaces; in one I've added a third such interface in the PCI slot. On each box the eth0 is the mgmt interface (NB when you add a PCI card eeepro100 it becomes eth0 and the two builtin NICs renumber to eth1 and eth2).

Besides running the eth0 interfaces to a hub, I tied the two eth1s from the dual-interface traffic generators to the eth1 and eth2 builtins on the 3-interface box, with crossover cables, running 100BaseT. I used the above invocations to get snort cooking with its default sigs, listening to bond0 with eth1 and eth2 enslaved to it. Snort sat idle. I fired up a ping -f on one of the generators and snort jumped up to 25% CPU; then launched ping -f on the other generator and it jumped to 55%. Each generator was emitting c. 20,000 packets/second, default ping packet size (64 bytes).

When I next tried tcpreplay[1], all was not as happy, until I stumbled across the above-mentioned need to promisc the interfaces manually as you're ifconfigging them. Once I got that, things got lots more better. Do remember when benchmarking with tcpreplay to make sure to tcpdump -s 0, so you aren't using captures with truncated packets.

-Bennett

[1] <URL:<http://tcpreplay.sf.net/>>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQE9ndnWHZWg9mCTffwRAtCFAJ9IzubCJoETWQ7OUWNjLmGPdXN6uACcDOyk
1A7vzBnfnXlu4poD+LapsEs=

=c5vE

-----END PGP SIGNATURE-----

This sf.net email is sponsored by:ThinkGeek

Welcome to geek heaven.

<http://thinkgeek.com/sf>

Snort-users mailing list

Snort-users@lists.sourceforge.net

Go to this URL to change user options or unsubscribe:

<https://lists.sourceforge.net/lists/listinfo/snort-users>

Snort-users list archive:

<http://www.geocrawler.com/redir-sf.php3?list=snort-users>

• **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

Portions of this site ©1998-2007, Neohapsis, Inc. Questions, comments or feedback welcomed. webmaster@neohapsis.com