

bpf packet capture and SOCK_STREAM socket redirects...

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2008-03/msg00322.html>

- *From:* "Alireza Torabi" <alireza.torabi@xxxxxxxxxx>
 - *Date:* Sat, 22 Mar 2008 01:25:03 +0000
-

On Fri, Mar 21, 2008 at 6:16 PM, Julian Elischer <julian@xxxxxxxxxxxxxx> wrote:

Alireza Torabi wrote:

```
> On Fri, Mar 21, 2008 at 6:35 AM, Peter Jeremy
> <peterjeremy@xxxxxxxxxxxxxxxxxxxx> wrote:
>> On Thu, Mar 20, 2008 at 11:27:53AM +0000, Alireza Torabi wrote:
>> >Imagine this:
>> >
>> > | (1)
>> > packets
>> > | | (4)
>> > [nic1] [nic2]
>> > bpf SOCK_STREAM
>> > | (2) |
>> > -----
>> > [FreeBSD] (3)
>> >
>> >1) all user traffic are being monitored
>> >2) bpf on [nic] is capturing these packets
>> >3) after processing we know a connection is about to be
```

established from A to B

```
>> >
>> >NOW:
>> >4) I want to deliver this packet to the socket on [nic2]
>> >and as this is a tcp socket it'll take care of it from there
>> >(my code here for this sockets sends and arbitrary data to A making it
>> >think it came from B)
>> >
>> >Have a look at divert(4). I suspect it comes closest to what you want.
>> >
>> >--
>> >Peter Jeremy
>> >Please excuse any delays as the result of my ISP's inability
```

to implement

bpf packet capture and SOCK_STREAM socket redirects...

>> an MTA that is either RFC2821-compliant or matches their

claimed behaviour.

>>

>

> Yes. It sounds promising. I was reading natd and planning to read ipfw

> source interestingly!

also I think you may want the 'fwd' call in ipfw...

I won't be using ipfw(8) at all as this is monitoring a copy of all the packets flowing through a core switch on a span/rmon 'ed switch port.

I don't quite understand your question..

(despite the picture)

where is A and where is B?

As I say I can only see a copy of these hosts' traffic over an rmon/span 'ed (Cisco terms) switch port.

and why 2 nics?

[nic1] is connected to above switch port and is bpf ing all the the packets (promisc) and [nic2] has it's own ip address and connected to a normal switch port, hence can send and receive data. ie talk to A or B

User traffic where?

on a switch?

coming in and out of this machine?

bpf is reading all the incoming packets coming to [nic1] off.

you need to define a little more of the picture..

Julian

btw, are you the Julian netgraph(8)?

- > Thanks
- >
- > Alireza

-
- > freebsd-net@xxxxxxxxxxx mailing list
 - > <http://lists.freebsd.org/mailman/listinfo/freebsd-net>
 - > To unsubscribe, send any mail to "freebsd-net-unsubscribe@xxxxxxxxxxx"

freebsd-net@xxxxxxxxxxx mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-net>
To unsubscribe, send any mail to "freebsd-net-unsubscribe@xxxxxxxxxxx"