

Re: tricking myself w/ multihoming

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2004-03/0371.html>

From: Brian Reichert (reichert_at_numachi.com)

Date: 03/23/04

Date: Tue, 23 Mar 2004 17:32:25 -0500

To: Barney Wolff <barney@databus.com>

On Tue, Mar 23, 2004 at 04:47:23PM -0500, Barney Wolff wrote:

> *First question, probably irrelevant – how did you get 255.255.255.255 as
> the broadcast addr on rl1?*

Good question. Said interface is set via dhclient, and values are provided by my cable company.

> *If 198.175.254.1 is really your external gateway, why is the default
> route heading inside? Are there so many inside nets that you can't
> list them as explicit routes?*

It's not 'inside', it's out my second pipe (the cable modem). This box has been my secondary MX, NS, and my squid cache (outgoing).

My public IP is routed over my DSL line.

This box, though, is my 'back door'; I vector higher-bandwidth traffic out over it (via NAT and otherwise), and maintain some incoming TCP tunnels, so I can crawl into my net when my primary ISP is having issues.

> *Try adding 00045 fwd 198.175.254.1 tcp from 198.175.254.8 25 to any .*

Ok, I'll give that a shot. Hmm, nope, no effect.

> *But really, the problem is better solved by setting your default
> route to 198.175.254.1 rather than playing ipfw games.*

True enough, but then how to I route squid queries, etc. out that interface?

What I want, magically, is 'replies to packets from not-my-net in via rl0 to go out via 198.175.254.1'. I'm having trouble phrasing that in an ipfw-flavored way.

> *How is DNS
> working?*

freebsd-net: Re: tricking myself w/ multihoming

Well. :) I have two internal caches (one available on each pipe), and two servers (again, one on each pipe). I also run a pair of keyed NTP servers. Bear in mind, I've got scads of machines on my net. This is the only dual-homed box, and hence some of my confusion.

> *Oh, and please do put some more secure rules in if you're really*
> *Internet connected.*

Oh, 198.175.254.1 is a far more fully developed firewall, no worries there.

> *Tcpdump on this box shows me the incoming packets coming to*
> *198.175.254.8, but I'm not seeing these replies to these packets*
> *going out at all, much less to 198.175.254.1.*
>
> *Probably going out rll.*

Then tcpdump should show that, shouldn't it?

```
# tcpdump -nl host 198.175.254.8
```

I see packets coming in:

```
17:19:06.120189 205.206.231.27.45785 > 198.175.254.8.25: S  
1457712783:1457712783(0) win 5840 <mss 1460,sackOK,timestamp 346982066  
0,nop,wscale 0> (DF)
```

But no packets going out from 198.175.254.8, on either interface...
Is natd rewriting them before tcpdump gets to see them? How do I prevent these packets from being diverted?

Thanks for the feedback, BTW...

> --
> *Barney Wolff* <http://www.databus.com/bwresume.pdf>
> *I'm available by contract or FT, in the NYC metro area or via the 'Net.*

```
--  
Brian Reichert <reichert@numachi.com>  
37 Crystal Ave. #303 Daytime number: (603) 434-6842  
Derry NH 03038-1713 USA BSD admin/developer at large
```

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