

TCP Header Rewrite

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2005-05/0386.html>

From: John Oxley (john.oxley_at_gmail.com)

Date: 05/05/05

Date: Thu, 5 May 2005 13:39:00 +0200

To: exim-users@exim.org, questions@freebsd.org

Hi,

I am cross posting this to [exim-users@exim](mailto:exim-users@exim.org) and [questions@freebsd](mailto:questions@freebsd.org) because my problem lies with both.

Okay, the scenario:

I am an ISP dealing with a lot of clients who like sending lots and lots of mail. Currently they are all sending out through a smart host, which checks mail for spam and viruses. All local bandwidth is given at the maximum of the carrier (radio, leased line etc) and international bandwidth is limited to what the client pays for. This is the way mail flows.

```
      local
      ^
      I
      I
client --> smarthost --> router --> shaper --> international
```

The smarthost is a FreeBSD-5.3-STABLE system running exim 4.50 built from the exim-mysql port. The router is transparent.

This setup works well as is, but the problem is that the shaper thinks that the traffic has come from the smarthost itself, and not the client, and thus the client isn't being bandwidth limited for international mail.

My solution to this would be to rewrite the TCP header on the smarthost of all mail packets going out to make them look like they came from the client rather than the smart host. That way the shaper will pick up the packets as though they were from the customer and appropriately shape them.

The Exim Side of things:

=====

I was thinking of rewriting the remote_smtp transport to send mail to a program which then sends the message off with modified headers. I would do it something like this

remote_smtp:

freebsd-questions: TCP Header Rewrite

```
driver = pipe
command = HEADER_MOD_COMMAND
```

Is there a better way of doing this? Correct me if I am wrong, but this will send the entire mail to STDIN of HEADER_MOD_COMMAND?

The FreeBSD side of things (**hairy**):

=====

Once I have the mail sent to the command i was thinking of sending it off through a pipe of some description. I am wondering however to do this. PF with AltQ, which I have never done before, or should I use a ipfw pipe with a divert? And how would I do it on this side?

Has anyone done something similar to this? I would have to take the mail and look at the contents to see where it came from in order to mangle the headers, then reintroduce through the pipe. What sort of processor overhead will I be looking at? I am not too worried because CPU time is much cheaper than bandwidth.

The smarhost is currently a 2.8Ghz server but can be upgraded if the load gets too high.

TIA

-John

freebsd-questions@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@freebsd.org"