

## Re: weird iptables behaviour

---

*Source:* <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-11/msg00512.html>

---

- *From:* Fabio <[nsafve\\_DELETE\\_ME\\_@xxxxxx](mailto:nsafve_DELETE_ME_@xxxxxx)>
  - *Date:* 24 Nov 2006 12:13:56 GMT
- 

On Fri, 24 Nov 2006 13:13:16 +1100, Grant wrote:

On 24 Nov 2006 00:48:55 GMT, Fabio <[nsafve\\_DELETE\\_ME\\_@xxxxxx](mailto:nsafve_DELETE_ME_@xxxxxx)> wrote:

I've got a strange problem with IP Masquerade:  
PC1 is connected to internet and PC2 uses PC1  
as the gateway.

From PC2 i can ping and even traceroute any URL

(for example ping and traceroute [www.wikipedia.org](http://www.wikipedia.org)  
works great) but i can open very few web pages.  
I only can see there 3 sites:  
[www.mozilla.org](http://www.mozilla.org) [www.beppegrillo.it](http://www.beppegrillo.it) [www.google.com](http://www.google.com)  
but I can't open for example [www.yahoo.com](http://www.yahoo.com) and much more.  
More than that is I can use skype from PC2, so I absolutely  
don't have a clue about what to do.

Would it be you're not clamping MTU? I have ('egress' is called from  
FORWARD chain, MAX\_MSS="1380" here):

```
# clamp MTU for new TCP connections to world
if [ -n "$MAX_MSS" ]
then
iptables -A egress -p tcp --tcp-flags SYN,RST SYN \
-j TCPMSS --set-mss $MAX_MSS
else
iptables -A egress -p tcp --tcp-flags SYN,RST SYN \
-j TCPMSS --clamp-mss-to-pmtu
fi
```

Grant.

Thank you for your help Grant,  
I've created a new chain called "egress" with iptables -N egress, then  
I've added the clamp part to my script and added

## Re: weird iptables behaviour

the option `-v` to iptables, and now i get:

```
root@darkstar:~# sh condis
MASQUERADE all opt -- in * out ppp0 0.0.0.0/0 -> 0.0.0.0/0
ACCEPT all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 state RELATED,ESTABLISHED
ACCEPT all opt -- in * out * 192.168.1.0/24 -> 0.0.0.0/0
DROP all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0
TCPMSS tcp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 tcp flags:0x06/0x02 TCPMSS set 1380
root@darkstar:~#
```

Anyway i get the same problem:

ping all, watch fews

I've tryied the bing the MTU values of the eth devices to 1380

and the valute of ppp0 (in `/etc/ppp/options`) to 1412

(1412 is suggested by `pppoe-setup`), but i didn't resolve

the problem, i really don't know what to do

thank you for your help

Fabio

.