

## RE: [fw-wiz] Stateful inspect on return web traffic – eek!

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-12/0055.html>

---

*From:* Brett Charbeneau ([brett\\_at\\_wrl.org](mailto:brett_at_wrl.org))

*Date:* 12/12/03

To: [Bill@royds.net](mailto:Bill@royds.net)

Date: Fri, 12 Dec 2003 10:06:43 -0500 (EST)

On Wed, 10 Dec 2003, Bill Royds wrote:

BR> That looks like the last packets of a TCP stream that are being rejected  
BR> because your firewall is taking down the connection after your outgoing fin  
BR> packet and not waiting on the server's fin-ack packet. It may be because you  
BR> have too short of a fin-wait timeout period in your tcp stack. Default is 2  
BR> minutes (which is much too long), while 30 seconds seems to be long enough  
BR> to prevent this but not so long that you queue too many sockets.  
BR> The host names corresponding to those IP addresses seem quit legitimate  
BR> 216.75.202.105 is mail26m.collegeclub.com, 207.68.178.238 is rad.msn.com

Thanks for the response, Bill!

Huh. This makes perfect sense, and the timeout you mention would certainly seem to derail iptables.

I'll give this a shot and report back – I just need to figure out where to tune this particular setting. =8^)

Brett Charbeneau, Network Administrator Tel: 757-259-7750

Williamsburg Regional Library FAX: 757-259-7798

7770 Croaker Road [brett@wrl.org](mailto:brett@wrl.org)

Williamsburg, VA 23188-7064 <http://www.wrl.org>

BR> -----Original Message-----

BR> From: [firewall-wizards-admin@honor.icsalabs.com](mailto:firewall-wizards-admin@honor.icsalabs.com)

BR> [<mailto:firewall-wizards-admin@honor.icsalabs.com>] On Behalf Of Brett

BR> Charbeneau

BR> Sent: December 9, 2003 11:33 AM

BR> To: [firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)

BR> Subject: [fw-wiz] Stateful inspect on return web traffic – eek!

BR>

BR> Greetings,

BR>

BR> If anyone can help me figure out what's going on with my logs, I'd

BR> be EXTREMELY grateful!

BR> I have a handful of firewalls around my institution that are using

Firewall-Wizards: RE: [fw-wiz] Stateful inspect on return web traffic – eek!

BR> the 2.4.20 Linux kernel, have iptables v1.2.7a, and default drop  
BR> policies. The workstations behind the firewalls are on NAT'd networks and  
BR> have these commands for connection tracking:  
BR>  
BR> iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT  
BR> iptables -A FORWARD -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT  
BR> iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
BR>  
BR> I've recently set up a Squid proxy with the same specifics but  
BR> obviously minus the NAT'd network. Except for the explicit allow  
BR> statements for the Squid process and necessary SSH access, the rules are  
BR> very simple – default drop except for related return traffic.  
BR> In all these instances, I have an iptables rule to log any dropped  
BR> packets and I've been seeing some really strange web-related \*return\*  
BR> traffic that isn't being allowed back in.  
BR> Me no get.  
BR> I've got an example below and they look to me to be replies to web  
BR> clients that \*should\* be associated with outgoing traffic but somehow  
BR> isn't and the traffic is being dropped.  
BR> I've not heard complaints about certain web sites being  
BR> unreachable, so the clients must be getting their traffic somehow, but  
BR> clearly something is amiss.  
BR> Any guidance or hints anyone can provide would be greatly  
BR> appreciated!  
BR>  
BR>

--

---

firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

RE: [fw-wiz] Stateful inspect on return web traffic – eek!