

Re: diagnosis – was Re: some reality about iptables, please

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2003-08/5657.html>

From: David (dbree_at_duo-county.com)

Date: 08/29/03

Date: Fri, 29 Aug 2003 16:30:49 -0500

To: Debian-User List <debian-user@lists.debian.org>

On Thu, Aug 28, 2003 at 06:36:00PM -0400, Bret Comstock Waldow wrote:

> *No from Debian Mozilla. Here's an example of the messages:*

> *Aug 28 17:35:55 ganessa kernel: DROPT:IN= OUT=eth0 SRC=192.168.2.30*

> *DST=205.156.51.200 LEN=44 TOS=0x00 PREC=0x00 TTL=64 ID=21328 DF*

> *PROTO=TCP SPT=34131 DPT=80 WINDOW=5840 RES=0x00 SYN URGP=0*

>

> *I'm curious that IN is blank.*

I'm going to pick up here.. I'll address some of your issues from other messages without quoting.

I think it's because it's an outgoing packet.. From appearances, it looks like your first (SYN) packet from Mozilla is being blocked.

I have to agree with the others that your best bet is to start from scratch and use one of the iptables setup tools. I used firestarter myself.. but there seems to be quite a bit of agreement that shorewall is good.. I'm sure either (or possibly others) would do the job well. I think the main thing is to first sit down and work out exactly what your setup is, then go from there using the setup tool of your choice.

I didn't study your rules, but from just scanning over them, there appears to be some redundancy in them..

RE: your complaint about the way the maintainer didn't write the rules for us.. I think that it would be impossible to write a general-purpose ruleset that would be appropriate for everyone.. and if he had attempted to do so, would probably have caused more problems and bug reports than he could handle.

RE: where to put the rules..

Many like to put them in the ip-up.d directory, and this is the way firestarter did mine.. (I have a dial-up using ppp0 interface).. with the references to the outside made via the ip address.

Debian-User: Re: diagnosis – was Re: some reality about iptables, please

However, it seemed that doing all this setup might be taking too long to get me online, so I just changed these ip address references to the references to ppp0 and put them in the rc?.d directories, so now, this is all done at bootup rather than each time I dial up. AFAICT, this seems to be working well. With this setup, I'm not online for any brief instant where I'm open before policy is set to DROP.

Also, for additional documentation, in your /usr/share/doc/iptables/html/ directory, you have the packet-filtering-HOWTO and the NAT-HOWTO. You may have this in your ruleset already, but with your setup, you will probably have to deal with NAT.

Again, I really believe that you'd be best served to use a tool. Once these rules are in place, you can then go in and correct any problems you might have, and fine-tune anything you don't feel comfortable with.

--

To UNSUBSCRIBE, email to debian-user-request@lists.debian.org with a subject of "unsubscribe". Trouble? Contact listmaster@lists.debian.org