

## Re: Firewall rules that discriminate by connection duration

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-11/0012.html>

---

**From:** D. (xlr8me\_at\_gmail.com)

**Date:** 11/11/04

Date: Thu, 11 Nov 2004 09:43:25 -0500

To: John Webster <jwebster@es.net>

I already suggested ipfw & dummynet to him, I attached his response.

I couldn't see any other way to do it which wouldn't mess up all other persistent connections (http1.1, etc).

On Wed, 10 Nov 2004 14:45:43 -0700, Brett Glass <brett@lariat.org> wrote:

>  
> *Yes. It's persistent connections that you want to throttle. You cannot*  
> *throttle P2P on the basis of port number, because many P2P systems use*  
> *well known ports such as 80.*  
>  
> --Brett Glass  
>

On Wed, 10 Nov 2004 11:16:45 -0800, John Webster <jwebster@es.net> wrote:

>  
>  
>  
>  
> --On Thursday, November 11, 2004 05:36:06 +1100 Peter Jeremy <PeterJeremy@optushome.com.au>  
wrote:  
>  
> > On Wed, 2004–Nov–10 13:23:21 +0200, Vlad GALU wrote:  
> > > On Tue, 9 Nov 2004 20:10:30 -0700 (MST), Brett Glass <brett@lariat.org> wrote:  
> > > > I'm interested in crafting firewall rules that throttle connections  
> > > > that have lasted more than a certain amount of time. (Most such  
> > > > connections are P2P traffic, which should be given a lower priority  
> > > > than other connections and may constitute network abuse.) Alas, it  
> > > > doesn't appear that FreeBSD's IPFW can keep tabs on how long a  
> > > > connection has been established. Is there another firewall for  
> > > > FreeBSD that can?  
> > >  
> > > All firewalls in FreeBSD can, actually. It's part of the stateful  
> > > inspection feature. The only thing they lack is a match parameter  
> > > based on the timer.

FreeBSD-Security: Re: Firewall rules that discriminate by connection duration

> >  
> > *That's a bit of a stretch. Stateful inspection associates a single  
> > timeout with each connection. The timeout is reset when a valid  
> > packet is seen on that connection and the connection blocked if the  
> > timeout expires.*  
> >  
> > *Brett needs a timeout that is initialised when the connection is setup  
> > and not reset. When it expires, you need to perform some different  
> > action rather than just block the connection. You might be able to  
> > reuse some of the existing stateful inspection code but I don't  
> > believe it's a trivial change.*  
>  
>  
> *How about ipfw and dummysnet? Maybe set up pipes for p2p traffic?*  
>  
>  
>

--

Want Gmail?  
Just ask, and I'll hook you up.

---

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