

## Re: bind() udp behavior 2.6.8.1

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-12/3661.html>

---

**From:** Willy Tarreau ([willy\\_at\\_w.ods.org](mailto:willy_at_w.ods.org))

**Date:** 12/16/04

Date: Thu, 16 Dec 2004 07:03:46 +0100

To: Adam Denenberg <[adam@dberg.org](mailto:adam@dberg.org)>

On Tue, Dec 14, 2004 at 09:23:43PM -0500, Adam Denenberg wrote:

- > *i think you guys are all right. However there is one concern. Not*
- > *clearing out a UDP connection in a firewall coming from a high port is*
- > *indeed a security risk. Allowing a high numbered udp port to remain*
- > *open for a prolonged period of time would definitely impose a security*
- > *risk which is why the PIX is doing what it does.*

Absolutely NO ! it is not "keeping the port open", it is "keeping a SESSION open". The firewall should allow traffic from the same ip:port to the other ip:port and from no other server on the net. Your new session is totally unrelated to the old one.

- > *The linux server is*
- > *"reusing" the same UDP high numbered socket however it is doing so*
- > *exactly as the firewall is clearing its state table (60 ms) from the*
- > *first connection which is what is causing the issue.*

it is not the same session if you connect to a different remote server, and there is absolutely no reason to arbitrarily prevent an internal server from connecting to two external ones from the same IP:port. Of course, if you reconnect to the same destIP:port, it should work because in this case it is a continuation of the same session.

- > *I think a firewall ought to be aware of such behavior, but at the same*
- > *time be secure enough to not just leave high numbered udp ports wide*
- > *open for attack. I am trying to find out why the PIX chose 60 ms to*
- > *clear out the UDP state table. I think that is a random number and*
- > *probably too short of a span for this to occur however i am still*
- > *researching it.*

it is not the timing which causes trouble, it is the way it confuses new and already established sessions. Although 60 ms may seem short (you can probably never resolve anything on ADSL with a loaded link), it may be perfectly valid if the firewall agrees to open several sessions when you connect to several servers. And if you connect several times to the same server, of course it must re-open the session.

Linux-Kernel: Re: bind() udp behavior 2.6.8.1

> *Any other insight would be greatly appreciated.*

unfortunately, googling for "pix udp problem" returns 25600 responses...

Regards,  
willy

—

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@vger.kernel.org

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>