Subject: Re: unlock iptables in netns
Posted by Patrick McHardy on Mon, 16 Jun 2008 11:16:00 GMT
View Forum Message <> Reply to Message

Alexey Dobriyan wrote:
> On Mon, Jun 16, 2008 at 12:26:03PM +0200, Patrick McHardy wrote:
>>
>> By the way, is there already work done for conntrack/NAT namespace
>> support? I have this patch that uses marks for something very similar
>> that should be easy to adjust.
>
> Yes, right now I'm fighting something which looks like double free
> of conntrack during clone(CLONE_NEWNET)/exit test despite none created
> in netns. And unknown to me dimensions of input and output packet codepaths.
> :^)
>
> Preliminaty details:
> struct nf_conn::ct_net which pins netns

 From the VLAN code, I thought namespaces could also be identified
numerically. That would reduce the size increase of struct nf_conn.

> netns of expectation is netns of master conntrack by definition
> per-netns conntrack hash
> per-netns expect hash
> per-netns unconfirmed list

That all makes sense.