Subject: Re: [PATCH 2.6.21-rc6] [netfilter] early_drop imrovement
Posted by Eric Dumazet on Fri, 06 Apr 2007 08:24:33 GMT
View Forum Message <> Reply to Message

On Fri, 06 Apr 2007 12:00:29 +0400
Vasily Averin <vvs@sw.ru> wrote:

> When the number of conntracks is reached ip_conntrack_max limit, early_drop() is
> called and tries to free one of already used conntracks in one of the hash
> buckets. If it does not find any conntracks that may be freed, it
> leads to transmission errors.
> However it is not fair because of current hash bucket may be empty but the
> neighbour ones can have the number of conntracks that can be freed. With the
> following patch early_drop() will search conntracks in all hash buckets.

Have you tested your patch in a DOS situation ?
Some machines have a huge ip_conntrack_max.
A single scan of the whole table might take 1000 ms or even more.