Subject: Re: strict isolation of net interfaces
Posted by serue on Fri, 30 Jun 2006 16:14:42 GMT
View Forum Message <> Reply to Message

Quoting Eric W. Biederman (ebiederm@xmission.com):
> This whole debate on network devices show up in multiple network namespaces
> is just silly. The only reason for wanting that appears to be better management.

A damned good reason. Clearly we want the parent namespace to be able
to control what the child can do. So whatever interface a child gets,
the parent should be able to somehow address. Simple iptables rules
controlling traffic between it's own netdevice and the one it hands it's
children seem a good option.

> We have deeper issues like can we do a reasonable implementation without a
> network device showing up in multiple namespaces.

Isn't that the same issue?

> If we can get layer 2 level isolation working without measurable overhead
> with one namespace per device it may be worth revisiting things. Until
> then it is a side issue at best.

Ok, and in the meantime we can all use the network part of the bsdjail
lsm? :)

-serge