Subject: Re: [RFC] network namespaces
Posted by ebiederm on Tue, 12 Sep 2006 03:28:47 GMT
View Forum Message <> Reply to Message

Dmitry Mishin <dim@openvz.org> writes:

> On Monday 11 September 2006 18:57, Herbert Poetzl wrote:
>> I completely agree here, we need a separate namespace
>> for that, so that we can combine isolation and virtualization
>> as needed, unless the bind restrictions can be completely
>> expressed with an additional mangle or filter table (as
>> was suggested)
>
> iptables are designed for packet flow decisions and filtering, it has nothing
> common with bind restrictions. So, it may be only packet flow
> scheduling/filtering, but it will not help to resolve bind-time IP conflicts.

Please read the archive, where the suggestion was made.

What was suggested was a new table, with it's own set of chains.
So we could make filtering decisions on where sockets could be bound.

That is not a far stretch from where iptables is today.

Do you have some concrete arguments against the proposal?

Eric

_____
Containers mailing list
Containers@lists.osdl.org
https://lists.osdl.org/mailman/listinfo/containers