
Subject: Re: strict isolation of net interfaces

Posted by [Sam Vilain](#) on Fri, 30 Jun 2006 02:48:49 GMT

[View Forum Message](#) <> [Reply to Message](#)

Serge E. Hallyn wrote:

> The last one in your diagram confuses me - why foo0:1? I would

> have thought it'd be

>

> host | guest 0 | guest 1 | guest2

> -----+-----+-----+----- -

> | | | |
> |-> lo <-----+--> lo0 ... | lo0 | lo0

> | | | |

> |-> eth0 | | |

> | | | |

> |-> veth0 <-----+--> eth0 | |

> | | | |

> |-> veth1 <-----+-----+-----+-----+--> eth0

> | | | |

> |-> veth2 <-----+-----+-----+-----+--> eth0 |

>

> [...]

>

> So conceptually using a full virtual net device per container

> certainly seems cleaner to me, and it seems like it should be

> simpler by way of statistics gathering etc, but are there actually

> any real gains? Or is the support for multiple IPs per device

> actually enough?

>

Why special case loopback?

Why not:

host | guest 0 | guest 1 | guest2

-----+-----+-----+----- -

| | | |

|-> lo | | |

| | | |

|-> vlo0 <-----+--> lo | |

| | | |

|-> vlo1 <-----+-----+-----+-----+--> lo

| | | |

|-> vlo2 <-----+-----+-----+-----+--> lo |

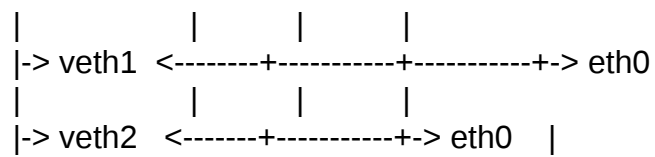
| | | |

|-> eth0 | | |

| | | |

|-> veth0 <-----+--> eth0 | |

| | | |



Sam.