
Subject: all vs. default in /proc/sys/net/ipv4/conf
Posted by [John Kelly](#) on Sun, 14 May 2006 22:44:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

I was studying the openvz sysctl.conf recommendations to see if they made sense for my environment, but I did not know the difference between "all" vs. "default" in /proc/sys/net/ipv4/conf. Google had the answer, though, repeated here FYI. The search key was "/proc/sys/net/ipv4/conf/default" and the first hit was:

<http://www.securityfocus.com/infocus/1711>

I'll quote it here, in case the link becomes unavailable:

Quote:When you change variables in the /proc/sys/net/ipv4/conf/all directory, the variable for all interfaces and default will be changed as well. When you change variables in /proc/sys/net/ipv4/conf/default, all future interfaces will have the value you specify. This should only affect machines that can add interfaces at run time, such as laptops with PCMCIA cards, or machines that create new interfaces via VPNs or PPP, for example.

Subject: Re: all vs. default in /proc/sys/net/ipv4/conf
Posted by [John Kelly](#) on Sun, 14 May 2006 23:32:34 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hmmm ... or so they say.

On my 2.6.16 kernel, setting "all" with "send_redirects" and "rp_filter" does not affect the default value, or any other interface. It only affects "all."

That makes me wonder, what is the purpose of the "all" setting. Unless this behaviour is maybe a kernel bug. If anyone knows ...

Subject: Re: all vs. default in /proc/sys/net/ipv4/conf
Posted by [John Kelly](#) on Mon, 15 May 2006 00:11:12 GMT
[View Forum Message](#) <> [Reply to Message](#)

OK ...

I discovered in Documentation/networking/ip-sysctl.txt:

Quote:rp_filter - BOOLEAN

1 - do source validation by reversed path, as specified in RFC1812

Recommended option for single homed hosts and stub network routers. Could cause troubles for complicated (not loop free) networks running a slow unreliable protocol (sort of RIP), or using static routes.

0 - No source validation.

conf/all/rp_filter must also be set to TRUE to do source validation on the interface

So "all" must be set, otherwise, it will not matter if the interface setting is true. Thus the "all" setting, for this sysctl, is an AND switch.

Quote:send_redirects - BOOLEAN

Send redirects, if router.

send_redirects for the interface will be enabled if at least one of conf/{all,interface}/send_redirects is set to TRUE, it will be disabled otherwise

Default: TRUE

At least one of "all" or "interface" indicates the "all" setting, for this sysctl, is an OR switch.

So if I understand correctly, the "all" setting can be either an AND switch or an OR switch, depending on the specific sysctl.

Subject: Re: all vs. default in /proc/sys/net/ipv4/conf
Posted by [John Kelly](#) on Mon, 15 May 2006 01:33:01 GMT
[View Forum Message](#) <> [Reply to Message](#)

Now ...

The OpenVZ quick install guide recommends:

Quote:# we do not want all our interfaces to send redirects
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0

Presumably, there is no need for venet interfaces to send redirects.

If that is true, then the recommended settings will not achieve the desired result. For the send_redirects sysctl, "all" is an OR switch, so "all" FALSE will not prevent redirects on any interface which has value TRUE.

When the venet interfaces come up, they will (presumably, not tested) inherit the default value of TRUE, which is undesirable. To fix that, the default value should be FALSE. However, you may still want other interfaces, such as eth0, to send redirects, so they should be set to TRUE.

I'm not sure why you would want to send redirects on lo.

Maybe I will change my mind later, but here are the settings that seem right, atm.

Quote:# Controls redirects, no need for venet interfaces to send them

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.eth0.send_redirects = 1
net.ipv4.conf.lo.send_redirects = 0
```

Subject: Re: all vs. default in /proc/sys/net/ipv4/conf
Posted by [John Kelly](#) on Mon, 15 May 2006 05:18:16 GMT

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

John Kelly wrote on Sun, 14 May 2006 21:33: When the venet interfaces come up, they will (presumably, not tested) inherit the default value of TRUE, which is undesirable.

That's true, I tested it.

However, now I see in /etc/sysconfig/network-scripts/ifup-venet where they use:

Quote:sysctl -w net.ipv4.conf.\$vznet.send_redirects=0

to explicitly disable redirects on venet0, no matter what the prior sysctl settings were.

Now that I see how all the pieces fit together, I suppose the quick install guide recommendation is a reasonable default, because after running the /etc/sysconfig/network-scripts/ifup-venet script, the end result is that you have redirects on all interfaces except venet0.

OTOH, if you want to use `_only_` /etc/sysctl.conf to disable redirects on both venet0 and lo, and explicitly enable redirects on each hardware interface (eth0, eth1, ...), now we know how. And what's more, we know the difference between "all" vs. "default" in the sysctl settings. The securityfocus article was wrong, heh.