

Re: ipfw check–state issue

Source: <http://www.derkeiler.com/Mailing–Lists/FreeBSD–Security/2005–11/0066.html>

From: Lowell Gilbert (freebsd–security–local_at_be–well.ilk.org)

Date: 11/23/05

To: Adi Tirla <tirlaadi@gmail.com>

Date: 23 Nov 2005 13:15:29 –0500

Adi Tirla <tirlaadi@gmail.com> writes:

> *heya*
>
> *i've been using freebsd's ipfw for quite a while and recently on a new*
> *server i've got this issue with ipfw that i can't understand ... something*
> *is wrong ...*
>
> *01000 8042 1947866 allow ip from any to any via fxp0*
> *01010 0 0 allow ip from any to any via lo0*
> *01014 9886 4170269 divert 8668 ip from any to any in via vr0*
> *01015 0 0 check–state*
> *01130 14679 5695969 skipto 1800 ip from any to any out via vr0 keep–state*
> *01300 0 0 deny ip from 192.168.0.0/16 <<http://192.168.0.0/16>> to any in via*
> *vr0*
> *01301 0 0 deny ip from 172.16.0.0/12 <<http://172.16.0.0/12>> to any in via*
> *vr0*
> *01302 4 140 deny ip from 10.0.0.0/8 <<http://10.0.0.0/8>> to any in via vr0*
> *01303 0 0 deny ip from 127.0.0.0/8 <<http://127.0.0.0/8>> to any in via vr0*
> *01304 0 0 deny ip from 0.0.0.0/8 <<http://0.0.0.0/8>> to any in via vr0*
> *01305 0 0 deny ip from 169.254.0.0/16 <<http://169.254.0.0/16>> to any in via*
> *vr0*
> *01306 0 0 deny ip from 192.0.2.0/24 <<http://192.0.2.0/24>> to any in via vr0*
> *01307 0 0 deny ip from 204.152.64.0/23 <<http://204.152.64.0/23>> to any in*
> *via vr0*
> *01308 0 0 deny ip from 224.0.0.0/3 <<http://224.0.0.0/3>> to any in via vr0*
> *01320 0 0 deny tcp from any to any dst–port 137 in via vr0*
> *01321 0 0 deny tcp from any to any dst–port 138 in via vr0*
> *01322 4 192 deny tcp from any to any dst–port 139 in via vr0*
> *01323 3 144 deny tcp from any to any dst–port 81 in via vr0*
> *01330 0 0 deny ip from any to any frag in via vr0*
> *01350 362 71038 deny tcp from any to any established in via vr0*
> *01400 2879 346276 deny log logamount 10 ip from any to any in via vr0*
> *01450 0 0 deny log logamount 10 ip from any to any out via vr0*
> *01800 8049 1944267 divert 8668 ip from any to any out via vr0*
> *01801 14676 5695755 allow ip from any to any*
> *01999 0 0 deny log logamount 10 ip from any to any*

FreeBSD-Security: Re: ipfw check-state issue

- > 65535 758 727615 deny ip from any to any
- >
- >
- > please enlighten me why the "almost" standard firewall from the handbook ...
- > ain't working properly !? look ... the check-state ain't matching any
- > packets ... and mostly ... packets skip the rule 1999 ... why?! i've seen
- > the "kernel: ous" too many times don't tell me i've got a third
- > network card cause it ain't so!
- >
- > another thing ... if i insert pipes for traffic shaping ... the outgoing
- > packets are inserted into the input pipes ... but not into the outgoing
- > pipes why ?
- >
- > i am missing somethin' what ?
- >
- >
- > kernel compiled with these additional options
- > options IPFIREWALL
- > options IPFIREWALL_VERBOSE
- > options IPFIREWALL_VERBOSE_LIMIT=10
- > options IPFIREWALL_FORWARD
- > options DUMMYNET
- > options HZ=1000
- > options IPDIVERT
- > enlightenment please

Any firewall where a packet may get passed to the same divert pipe multiple times isn't *close* to "almost standard." Try actually using the standard one, as your modifications don't make a lot of sense. Nor do I understand those URLs in the RFC1918 rules...

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"