

Re: Re: IPFW rules being weird?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2003-10/0214.html>

dan_at_ntlbusiness.com

Date: 10/24/03

To: "Crist J. Clark" <cjc@freebsd.org>, freebsd-net@freebsd.org
Date: Fri, 24 Oct 2003 21:34:31 +0000

Hi there.

Thank you for your reply!

This is all very confusing, hehe!

I'm not running a DNS server, the laptop which access through NAT I've set the nameservers as those of my ISP (and those listed in /etc/resolv.conf) of the FreeBSD box.

Is there anything to particular think should not be there, apart from that:

>
> *allow ip from me to any out xmit any keep-state*
>

Your help is really appreciated on this.
Many thanks!

>
> *From: "Crist J. Clark" <crstjc@comcast.net>*
> *Date: 2003/10/24 Fri PM 07:05:44 GMT*
> *To: Dan <dan@ntlbusiness.com>*
> *CC: freebsd-net@freebsd.org*
> *Subject: Re: IPFW rules being weird?*
>
> *On Fri, Oct 24, 2003 at 02:10:14AM +0100, Dan wrote:*
> *> Hello there.*
> *> Odd query for you.*
> *>*
> *> My setup is that sis0 is the ethernet which has the business cable modem*
> *> attached to it - which serves as a gateway. sis1 is the Ethernet which my*
> *> laptop connects to (wirelessly through a HE501 wireless pc card, and HE102*
> *> access point (both by Netgear)).*
> *>*
> *> The problem that is occuring, is that if I have the IPFW rules below,*
> *> everything works GREAT!*
> *>*
> *> fwcmd="/sbin/ipfw"*
> *> \$fwcmd -f flush*

freebsd-net: Re: Re: IPFW rules being weird?

> > *\$fwcmd add divert natd all from any to any via sis0*
> > *\$fwcmd add allow all from any to any*
> > *\$fwcmd add allow icmp from any to any icmptypes 0,3,8,11,12,13,14*
>
> *That last rule is kinda useless considering the rule before it, no?*
>
> > *However, the above is not "secure" as you might say.*
> > *The script below stops the laptop from being able to access th enet and i have*
> > *NO idea why!*
>
> *Many problems. The most basic being: use setup-established orr use*
> *keep-state for a given traffic flow. Mixing them will likely cause*
> *administrator confusion. You may have some reasons to use both in this*
> *ruleset, but it is very confusion as is.*
>
> *The question of which to use for your NATed adresses is answered by*
> *Big Problem Two, keep-state and natd(8) do not play well together. See*
> *the many, many, many threads on this here, on -ipfw, and on*
> *-questions. The basic issue is that the address at your end of two-way*
> *connections has the unNATed address when it hits the keep-state rules*
> *coming in from the Internet and has the NATed address when going*
> *out. Thus, you get two dynamic rules that do not match up. That spells*
> *trouble.*
>
> *As for what precisely is breaking here, from a quick read, I would*
> *expect TCP connections to work briefly, but quickly timeout. My guess*
> *is the reason it seems you are unable to access the 'Net at all is*
> *that DNS lookups are totally broken. (All non-TCP traffic is totally*
> *blocked, unlike TCP which will limp along a little.) On the way out,*
> *your rule,*
>
> *allow ip from me to any out xmit any keep-state*
>
> *Will create a dynamic rule for the UDP traffic from the NAT address to*
> *the DNS server. But the response will go through the rules with a*
> *source of the remote DNS server and destination in 192.168.0.0/24*
> *which will NOT match at the keep-state or any other rule until the*
> *default drop. Are you seeing these in the logs? Or are you running DNS*
> *server on the firewall (which would actually work)?*
>
> > *# Define the firewall command (as in /etc/rc.firewall) for easy*
> > *# reference. Helps to make it easier to read.*
> > *fwcmd="/sbin/ipfw"*
> >
> > *# Force a flushing of the current rules before we reload.*
> > *\$fwcmd -f flush*
> >
> > *# Divert all packets through the tunnel interface.*
> > *\$fwcmd add 50 divert natd all from any to any via sis0*
> >
> > *# Allow all connections that have dynamic rules built for them,*

Re: Re: IPFW rules being weird?

freebsd-net: Re: Re: IPFW rules being weird?

```
> > # but deny established connections that don't have a dynamic rule.
> > # See ipfw(8) for details.
> > $fwcmd add check-state
> > $fwcmd add pass tcp from any to any established
> >
> > # Allow all localhost connections
> > ${fwcmd} add 100 pass all from any to any via lo0
> > ${fwcmd} add 200 deny all from any to 127.0.0.0/8
> > ${fwcmd} add 300 deny ip from 127.0.0.0/8 to any
> >
> > # Allow all connections from my network card that I initiate
> > $fwcmd add allow tcp from me to any out xmit any setup keep-state
> > $fwcmd add deny tcp from me to any
> > $fwcmd add allow ip from me to any out xmit any keep-state
> > $fwcmd add allow all from 192.168.0.0/24 to any
> >
> > # Everyone on the Internet is allowed to connect to the following
> > # services on the machine. This example specifically allows connections
> > # to sshd and a webserver.
> > $fwcmd add allow tcp from any to any established
> > $fwcmd add allow tcp from any to me 80 setup
> > $fwcmd add allow tcp from any to me 21 setup
> > $fwcmd add allow tcp from any to me 22 setup
> >
> > # This sends a RESET to all ident packets.
> > $fwcmd add reset log tcp from any to me 113 in recv any
> >
> > # Enable ICMP: remove type 8 if you don't want your host to be pingable
> > $fwcmd add allow icmp from any to any icmptypes 0,3,8,11,12,13,14
> >
> > # Deny all the rest.
> > $fwcmd add deny log ip from any to any
>
> --
> Crist J. Clark | cjclark@alum.mit.edu
> | cjclark@jhu.edu
> http://people.freebsd.org/~cjc/ | cjc@freebsd.org
>
```

freebsd-net@freebsd.org mailing list

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

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