

Re: IPFW compiled in kernel: Where is it reading the config?

Re: IPFW compiled in kernel: Where is it reading the config?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-12/msg00029.html>

- *From:* "W. D." <WD@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 13 Dec 2007 12:39:44 -0600
-

At 05:00 12/13/2007, Gary Palmer wrote:

The config file locaton that I specify in rc.conf doesn't appear to be being used:

```
firewall_script="/usr/local/etc/ipfw.rules"
```

You require

```
firewall_enable="YES"
```

in /etc/rc.conf for the rules to be looked at

Also, firewall_script may be the wrong configuration parameter to use. firewall_script is expected to be a shell script to configure the firewall. If you just want a file of rules, set firewall_type instead. e.g.

```
firewall_type="/etc/rc.firewall.rules"  
firewall_enable="YES"
```

and then put your rules one line at a time into the specified file. i.e.

```
add allow ip from any to any via lo0  
(etc)
```

ipfw is a kernel module. It will not show up in "ps aux". If "ipfw list" does not come back with an error message, then it is likely running. You can check for the ipfw module using

```
kldstat
```

(assuming you did not compile ipfw into a custom kernel)

To check the syntax of a list of rules (note: not a shell script) then

Re: IPFW compiled in kernel: Where is it reading the config?

you can use

```
ipfw -n /path/to/rules/file
```

From the man page

-n Only check syntax of the command strings, without actually passing them to the kernel.

Regards,

Gary

Thanks, Gary! This is much of what I was looking for.

Start Here to Find It Fast!? -> [http://www.US-Webmasters.com/best-start-page/\\$8.77 Domain Names](http://www.US-Webmasters.com/best-start-page/$8.77%20Domain%20Names) -> <http://domains.us-webmasters.com/>

freebsd-security@xxxxxxxxxxx mailing list

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

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