

## Re: ipfw and nmap

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2005-02/3660.html>

---

**From:** Matthew Seaman (*m.seaman\_at\_infracaninophile.co.uk*)

**Date:** 02/24/05

Date: Thu, 24 Feb 2005 11:37:33 +0000

To: snltch <dot.snltch@gmail.com>

On Wed, Feb 23, 2005 at 11:49:39AM -0500, snltch wrote:

> *I am fairly new to IPFW, I have question regarding the stateful part*  
> *of it. Now I may just be misunderstanding this so set me straight if I*  
> *am. From what I understand when you add a check-state rule and then*  
> *following that a rule to keep-state, if a packet destined for that*  
> *port is new and "setup" was not added to the keep-state rule then*  
> *wouldn't it get denied at the check-state rule since keep-state did*  
> *not add a dynamic rule? My problem is this, and again this may not*  
> *even be correct but I have a BSD box that is simply providing me SSH*  
> *capabilities..here are the rules for it:*  
>  
> *add check-state*  
> *add allow all from any to any 22 in via fxp0 keep-state*  
> *then the default to deny rule.*

One way of coding up firewall rules to allow incoming SSH connections and disallow generic port probes would be something like this:

```
add check-state
deny tcp from any to any established
add allow tcp from any to me 22 setup in via fxp0 keep-state
[ ... other rules for tcp services you want open ... ]
```

ie. You're testing for the first incoming packet, with the SYN flag set -- which results in a dynamic rule being created that effectively slots into the rule set at the 'add check-state' line. Then deny any TCP packets flowing in any direction that *\*don't\** have the SYN flag set. So TCP connections that are generated in the correct sequence will be allowed, but bouncing random TCP packets with weird flag combinations off your server will be filtered. You will need additional rules to support starting up outgoing connections.

Note that this only works for TCP --- UDP, ICMP and other protocols have no corresponding concept of 'open' or 'closed' connection state.

Note too that there is nothing to prevent port scanners simply setting

freebsd-questions: Re: ipfw and nmap

the 'SYN' flag in the probe packets they send to your server.

- > *Now is there a way to allow setup connections but disallow port*
- > *scanners like nmap from seeing it as being open?*

If you want people to be able to SSH into your systems from outside, then you have to have port 22 (or some port with sshd listening on it) open. In that case, you can not prevent people using tools like nmap to discover that the port is open.

In recent months there has been a lot of automated scanning for SSH servers and attempts to break in via some account/password pairs which were created by default on some Linux distros. The answer to securing your server against such probes is not to attempt to hide the fact that you're running a SSH server, but to enforce security policies on how ssh is used:

- root login via SSH is not permitted (The 'PermitRootLogin no' setting in /etc/ssh/sshd\_config).
- Make sure that all accounts that do not correspond to real users have locked passwords and /sbin/nologin as their shell.
- Force all users either to use key-based auth for remote access, or use one-time passwords (opie), or use Kerberos, or failing that (and only as a last resort) permit password auth, but enforce a strict "good password" policy. That means regularly running a password cracker against your password file and locking out accounts where the password can be broken.

Cheers,

Matthew

--

Dr Matthew J Seaman MA, D.Phil.

PGP: <http://www.infracaninophile.co.uk/pgpkey>

Tel: +44 1304 617253

8 Dane Court Manor

School Rd

Tilmanstone

Kent, CT14 0JL UK

- 
- application/pgp-signature attachment: [stored](#)