Using fail2ban with nftfw

Using fail2ban with nftfw

The 0.9.7 release of *nftfw* contains a new directory *fail2ban* installed in */usr/share/doc/nftfw*. The directory contains two action files for *fail2ban* allowing the system to use *nftfw* as its firewall. The action interface for *fail2ban* uses expanded editing functions in the *nftfwedit* command.

Installation

Install the action files:

```
$ cd /usr/share/doc/nftfw/fail2ban
$ sudo cp *.conf /etc/fail2ban/action.d
```

Setup the fail2ban configuration to use the new action files. It's probably wise to stop *fail2ban* while doing this.

```
$ sudo systemctl stop fail2ban
```

Set up a copy of the main configuration file:

```
$ sudo copy jail.conf jail.local
```

Then edit the `jail.local` file changing these lines to read:

```
banaction = nftfw-multiport
banaction_allports = nftfw-allports
```

You are now set. Restart *fail2ban*:

```
$ sudo systemctl start fail2ban
```

Testing

The *fail2ban* client can test the ban and unban actions.

```
$ sudo fail2ban-client set JAIL banip IP
```

You need to replace JAIL with a jail that is configured in *jail.d*, and IP by an IP address that will be banned.

The results should be:

- Look in */etc/nftfw/blacklist.d* and see that a file named `IP.auto` has been created.
- The `nftfwls` command will show you that the IP is in *nftfw*'s database. The pattern used to identify the reason of the ban will be `f2b-JAIL` where JAIL is the name of the jail used in the test.
- The nftables firewall will have been reloaded, assuming that you have actioned *nftfw.path* in *systemd* running *nftfw*'s *blacklist* command when files are changed on the *blacklist.d* directory. See 'Start the active control directories' in Install *nftfw* from Debian package.

To undo this test, use:

```
$ sudo fail2ban-client set JAIL unbanip IP
```

Caveat

I have tested the two actions included with a *fail2ban* installation, using the *fail2ban-client* commands above. However, I have not used the rules on an active installation.

Thanks

Thanks to the *nftfw* user who asked me for assistance with *fail2ban*.