Using fail2ban with nftfw

Using fail2ban with nftfw

The 0.9.7 and later releases 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 ban action interface for *fail2ban* uses expanded editing functions in the *nftfwedit* command to add an IP address into *nftfw*. It will create a file in `/etc/nftfw/blacklist.d` and add the IP to *nftfw*'s database. The unban action will remove the file but will leave the IP address information in the database.

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
```

We need to make a change to `fail2ban`'s main configuration file, as distributed it's in `/etc/fail2ban/jail.conf`. The file should not be edited, instead it's conventional to make a copy called `jail.local` and edit that.

If you don't have `/etc/jail.local`:

```
$ cd /etc/fail2ban
$ sudo cp jail.conf jail.local
```

If you do:

```
$ cd /etc/fail2ban
$ sudo cp jail.local jail.local.bak
```

Then edit (use *sudo* before your edit command) 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
```

Is it working?

fail2ban logs the ban action and the IP that it used but says nothing about the action that is executed. The action will create a file named`ipaddress.auto` in `/etc/nftfw/blacklist.d` and the IP address will be entered into *nftfw*'s database. Database entries are accompanied by a 'pattern' which indicates the source of the ban. The *fail2ban* actions for *nftfw* set the pattern to be `f2b-` followed by the name of the Jail.

Use the *nftfwls* command to see the current state of *nftfw*. It uses the contents of `/etc/nftfw/blacklist.d` to select only active blacklisted IPs. To show all the entries in the database use `nftfwls -a`. You should see some `f2b` entries in the database.

Alternatively you can use the *nftfwedit* command to look at one of the IP's that *fail2ban* has logged.

```
$ nftfwedit IPADDRESS
```

Will tell you if the IP is in the database, and if so, whether it's active (i.e. in `/etc/nftfw/blacklist.d`).

What to do for *fail2ban* unban

As distributed, the two *fail2ban* action files will act on *fail2ban* unban actions by removing the IP from the `/etc/nftfw/blacklist.d` directory but not from the *nftfw* database. It's not clear whether this is the right thing to do, it may be better to just ignore the unban instruction and let *nftfw* time out the IP address. If you would like to try this, cd to `/etc/fail2ban/action.d` and use sudo with your editor to modify each of `nftfw-allports.conf` and `nftfw-multiport.conf`. Change

```
actionunban = /usr/bin/nftfwedit -r <ip>
```

to

```
# actionunban = /usr/bin/nftfwedit -r <ip>
actionunban =
```

The # is a comment so you can put it back later if needed. Now restart *fail2ban*.

Caveat

I have tested the two actions included with a *fail2ban* installation, using the *fail2ban-client* commands above. Initial results from the user that asked for this capability show that this is working as expected.

Thanks

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