RPZ - Response Policy Zones

Response Policy Zones (RPZ) is a mechanism that makes it possible to define your local policies in a standardised way and load policies from external sources. [1]. The base functionality of blocking DNS is similar to piHole but without the pretty graphics. (there are no plans to add the pretty grphics).

Note: Domains blocked by RPZ are not DROPped or REJECTed like when using a Firewall Rule. RPZ only blocks the domain name lookup. If your user decides to enter an IP address to get to their favorite site, RPZ will not stop it from happening. If this is needed you may be better off of using IP Address Blocklists.

Installation

Note: The test version of the RPZ add-on is installed manually until approved by the IPFire Developers. It is installed similar to this method:

https://www.ipfire.org/docs/devel/ipfire-2-x/addon-howto#testing-the-install-uninstall-update-routines-and-add-on-itself

~~rpz can be installed with the Pakfire web interface or via the console~~:

```
~~pakfire install rpz~~
```

Usage

There is no web interface for this add-on. To run this add-on open the serial console, or the local terminal and access the IPFire box via SSH. There are four simple scripts available for set-up:

rpzAllowBlock - Loads custom allow lists and blocks lists into unbound RPZ

rpzConfig - Create, remove or replace an external RPZ config file

rpzMetrics - Locates RPZ names from the message logs and sort by hits. Selecting all logs (1 year) may take ~60 seconds to complete.

rpzSleep - Disable the RPZ for a NUMBER of seconds (default 5 minutes).

PS - I am looking for someone to assist with a WebGUI.

Custom allow list or block list

The `rpzAllowBlock` application loads custom allow lists and blocks lists into unbound RPZ. Update the lists first and then run the `rpzAllowBlock` command.

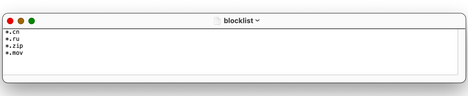
Allow list

Sometimes outside RPZ lists will block a website that requires access. Allowed items can be added to this list.

Edit the `/var/ipfire/rpz/allowlist` and add the needed websites:

Block list

The block list operates in the same way and is located at `/var/ipfire/rpz/blocklist` :



After saving the lists, launch this from the command line to load these files into unbound:

```
rpzAllowBlock
```

Create a config file for RPZ

`rpzConfig` assists in creating, removing or replacing an RPZ config file

```
Usage:  rpzConfig  <options> <name> <url>

Options:
  add <name> <url>     adds new RPZ config file by RPZ name

  remove <name> <url>  removes unneeded RPZ files by RPZ name

  replace <name>       replaces an existing RPZ files with a new config file

    <name>             unique alpha-numeric name for the RPZ file.  This name appears in the message log and
                       is the basename for the config file. e.g., threatfox, urlhaus, PopUpAdsHZ

    <url>              URL for RPZ.  Must be in a format similar to https://example.com/path/filename.
                       Other protocols such as file://, ftp://, etc. will not work.
```

Example command:

```
rpzConfig add MxUltimateHZ https://raw.githubusercontent.com/hagezi/dns-blocklists/main/rpz/ultimate.txt
```

Example response:

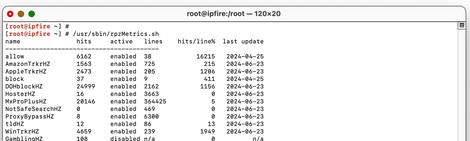
Note: whenever a RPZ config file is added, removed, or replaced, the upbound reload (i.e., `unbound-control reload`) is run. This loads all of the new settings. Keep in mind this may pause DNS up to ~60 seconds depending on the size of the RPZ files. Large RPZ files will slow down the unbound reload time and slow down a DNS lookup. Over 1,000,000 lines of RPZ files (total for all RPZ files) is NOT recommended.

Metrics of RPZ usage

Locates RPZ names from the message logs and sort by hits. Selecting all message logs (1 year or 53 log files) may take ~60 seconds to complete.

```
Usage:  rpzMetrics <number of message logs>
    default <number of message logs> is 2
```

Example response:

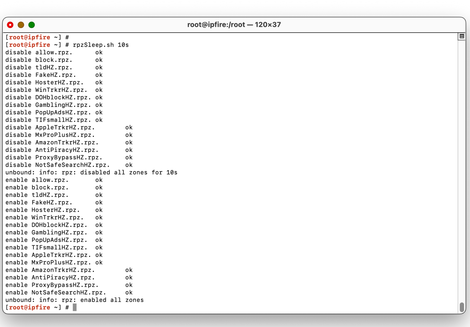


Disable RPZ for N time

Pause for NUMBER seconds. SUFFIX may be 's' for seconds, 'm' for minutes, 'h' for hours or 'd' for days.

```
Usage:  rpzSleep <sleep time>
        default <sleep time> is 5 minutes
```

Example response:



Links

- https://en.wikipedia.org/wiki/Response_policy_zone
- https://unbound.docs.nlnetlabs.nl/en/latest/topics/filtering/rpz.html
- https://github.com/jppgi250/piholemanual/blob/master/doc/Unbound%20response%20policy%20zones.pdf

1. https://unbound.docs.nlnetlabs.nl/en/latest/topics/filtering/rpz.html ↩