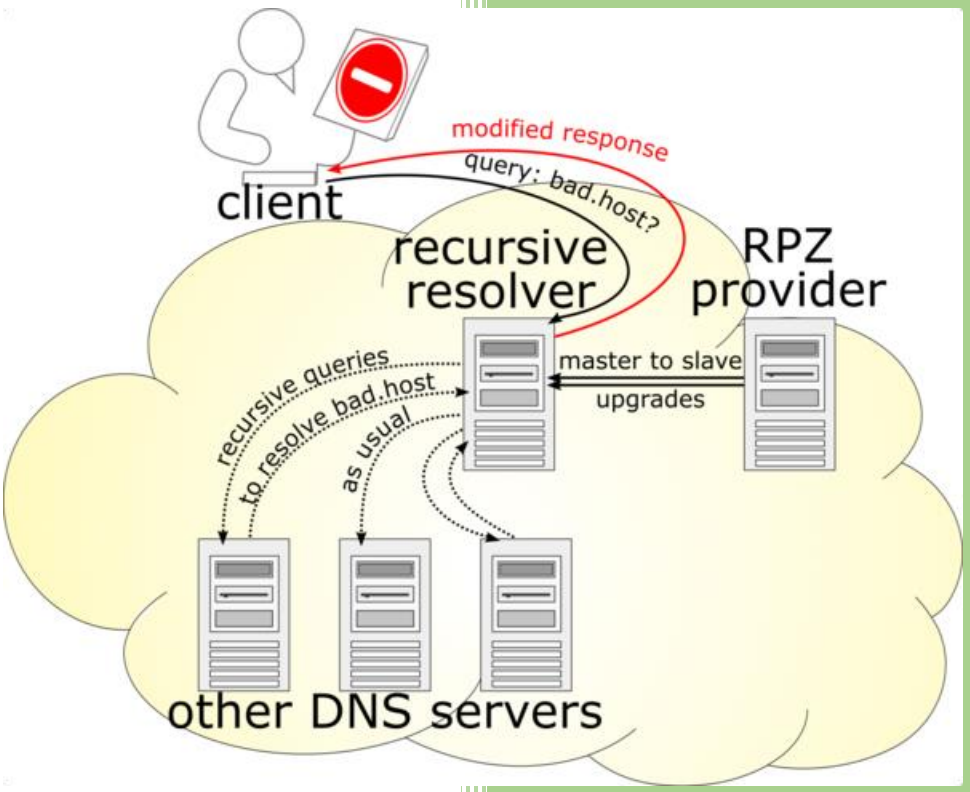
2022

Using Unbound response policy zones



https://discourse.pi-hole.net/u/jpgpi250

24-1-2022

1. About this manual. 2
2. Unbound. 2
3. Response Policy Zones (RPZ). 2
4. Pro-Con using response policy zones. 3
5. Configuration. 3
6. Test the RPZ configuration. 4
7. Pi-hole integration. 4
8. Using TMPFS to store the zone files. 5
9. DoH response policy zone. 5
10. Change Log 6

1. About this manual.

Using this guide will configure unbound to reply NXDOMAIN for specific (malware) domains, even if pi-hole has been temporary disabled.

If you are reading this document, using Adobe Reader, you may click on a hyperlink to content in this document. Use the combination <Alt> <left arrow> to return to the previous location.

"Back" and "Forward" buttons can also be added to the toolbar. If you right-click on the tool bar, under "Page Navigation", they are referred to as "Previous View" and "Next View".

This document is hosted on GitHub, you can open the document (pdf), using this link.

Copying and pasting from this manual into Putty doesn't seem to work all the time. If you get an error, try typing the command…

2. Unbound.

This guide assumes you have already installed and configured unbound. Basic unbound installation instructions, as recommended by the pi-hole developers, can be found here. Unbound has a lot of configuration options, most of them explained here. Optimizing the performance of unbound can be achieved, using these guidelines.

3. Response Policy Zones (RPZ).

Adding response policy zones to unbound makes unbound act as a DNS firewall, basically the same thing pi-hole is already doing for you, however:

- Pi-hole can be temporary disabled (menu / disable)
- Pi-hole can be configured to allow unrestricted access, using a whitelist regex entry (*) for one or more clients, using group management.
- Pi-hole only updates lists once a week (default – user can change this).

By using unbound response policy zones, the clients will never be able to obtain an IP address for the entries in the RPC zone(s), you have configured. You can read more about response policy zones here. The unbound response policy zone documentation can be found here.

4. **Pro-Con using response policy zones.**

Pro: After a response policy zone configuration has been added, unbound will download the file automatically.

Pro: Unbound will respect the settings in the SOA record and refresh the zone without user intervention.

Con: All entries in the rpz file(s) are blocked, the response to the client depends on the chosen *rpz-action-override* option.

Con: There are no options to whitelist specific entries.

Con: When using the DoH rpz, Apple uses a proprietary implementation of oDoH (oblivious DNS over HTTPS), the domains, used to make *icloud private relay* work, are blocked. This implies, for pi-hole users, the pi-hole config option BLOCK_ICLOUD_PR=false, will not have the desired effect (unbound DoH rpz always blocks the required entries – for more information, read section 6.2 in this document).

5. **Configuration.**
You need to prepare for the example configuration (see below) by creating a folder for the zonefile(s), and apply the necessary permissions:

```
sudo mkdir -p /etc/unbound/zonefiles
sudo chown unbound:unbound /etc/unbound/zonefiles
sudo chmod 755 /etc/unbound/zonefiles
```

The permissions above assume you are running unbound with user unbound (username: unbound in the main unbound configuration file), change the permissions, if required.

To add a response policy zone (example urlhaus), simply add a configuration file in /etc/unbound/unbound.conf.d/, name rpz.conf, content:

```
server:
module-config: "respip validator iterator"

rpz:
    name: urlhaus
    zonefile: zonefiles/urlhaus.zone
```

```
    url: https://urlhaus.abuse.ch/downloads/rpz
    rpz-action-override: nxdomain
    rpz-log: yes
    rpz-log-name: urlhaus
```

The path in the above example is for a setup, using chroot, which means:

- zonefile: zonefiles/urlhaus.zone is actually /etc/unbound/zonefiles/urlhaus.zone
- rpz-log-name: the name will appear in the unbound log message: … [urlhaus] …

If you don't use chroot, you need to use the full path of the referred files.

Additional considerations:

- You can only have one **modules-config** entry in all of your unbound configuration files, the last entry read will be used.
- Some modules are incompatible, use **unbound-checkconf** to check for possible problems.
- Checkout the unbound response policy zone documentation.
- Pi-hole integration requires an additional setting, see here.

Restart unbound to activate the changes, Unbound will automatically download the zone during startup.

6. **Test the RPZ configuration.**
   The zone file will be downloaded when unbound starts. Verify the file exists and has content (/etc/unbound/zonefiles/urlhaus.zone), check the unbound log for errors and warnings, if the file is not automatically created.

   The RPZ file, we configured in the example, contains a test entry, which we can use to verify functionality. Run **dig testentry.rpz.urlhaus.abuse.ch** from any workstation, an NXDOMAIN reply should be returned. Check the unbound log, you should find a log entry:

```
info: rpz: applied [urlhaus] testentry.rpz.urlhaus.abuse.ch. rpz-nxdomain …
```

7. **Pi-hole integration.**

   WARNING: This only works with unbound v1.14.1 or higher!

   When using pi-hole + unbound, unbound is used as the upstream resolver. Pi-hole has a special status type (8 – Blocked by upstream server, NXDOMAIN with RA bit unset). By adding an additional setting to the unbound response policy zone configuration, the pi-hole query log will tag rpz blocked entries with this status.

This additional setting can only be used with in combination with **rpz-action-override: nxdomain** and needs to be included for each zone:

```
rpz-signal-nxdomain-ra: yes
```

Result (pi-hole):

Time	Type	Domain	Client	Status	Reply
2022-01-06 09:26:15	A	testentry.rpz.urlhaus.abuse.ch	y50eth0.localdomain	Blocked (external, NXRA)	NXDOMAIN (2.1ms)

8. **Using TMPFS to store the zone files.**
   Due to the limited time to live configuration in the downloaded file, the zone file will be updated every 5 minutes, which you may not like, when using an SD card. To prevent the additional wear on the SD card, you can ensure the system uses memory (tmpfs) to store this file (no SD card writes).

   To achieve this, add a line to /etc/fstab

```
tmpfs /etc/unbound/zonefiles tmpfs nodev,nosuid,gid=unbound,uid=unbound,mode=0755,size=1M 0 0
```

   Again, change the permissions, if required. **If you are going to add multiple RPZ sources, and thus store additional zone files, increase the size**.

   - Stop unbound (sudo service unbound stop)
   - Mount the zonefiles folder (sudo mount /etc/unbound/zonefiles)
   - Start unbound (sudo service unbound start)

   Or simply reboot the pi, the folder will be auto mounted, unbound started and the zone file downloaded.

9. **DoH response policy zone.**
   You might have read the document, explaining how to block DoH (DNS over HTTPS) IP addresses on a pfsense firewall, however, you cannot use this method on all firewalls.

   To provide some protection against DoH, you can add a response policy zone, containing the domain names of known DoH servers.

   To add the DoH response policy zone, add the following to your unbound config file:

```
rpz:
    name: doh
    zonefile: zonefiles/doh.zone
    url: https://raw.githubusercontent.com/jpgpi250/piholemanual/master/DOH.rpz
    rpz-action-override: nxdomain
```

```
rpz-log: yes
rpz-log-name: doh
```

- Remember, you need the *server / module-config* configuration section (see above), these entries should only appear once in your config files.
- Pi-hole integration requires an additional setting, see here.

The rpz file on GitHub is updated daily.

10. Change Log

26-11-2021

- Version 1 (draft). Report issues here.

29-12-2021

- Added some config warnings
- Format of rpz log entry has changed in 1.14.0

02-01-2022

- Added DoH (DNS over HTTPS) response policy zone.

24-01-2022

- Added pi-hole integration (requires unbound 1.14.1 or higher).