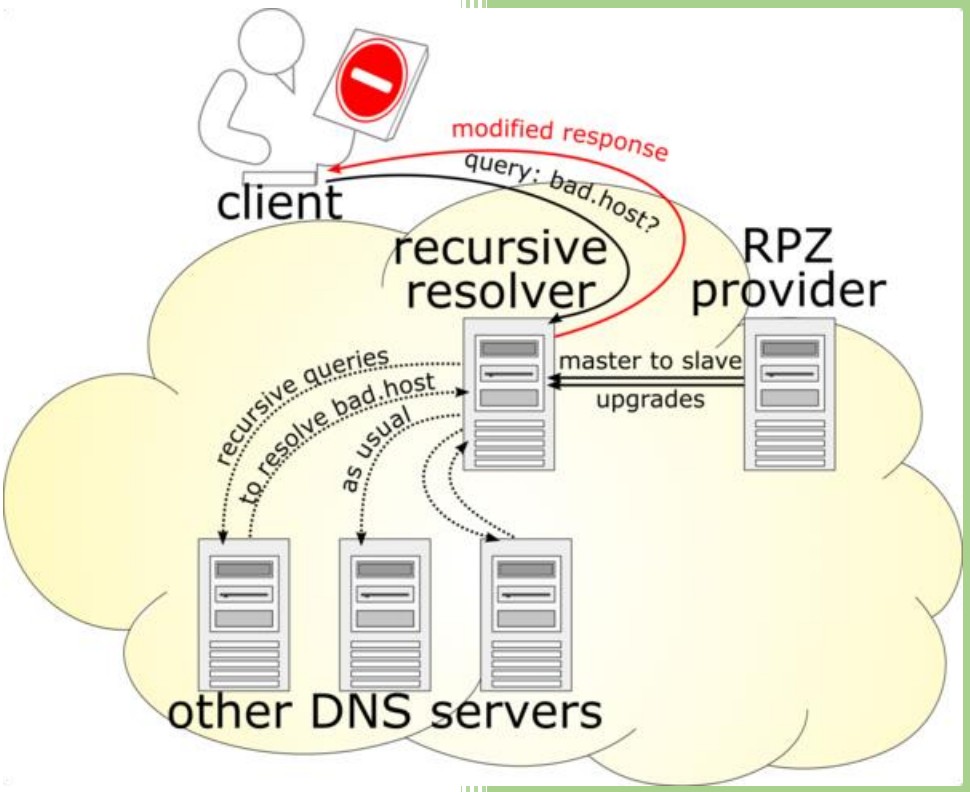
2021

Using Unbound response policy zones



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

26-11-2021

1. About this manual. 2
2. Unbound. 2
3. Response Policy Zones (RPZ). 2
4. Configuration. 2
5. Test the RPC configuration. 3
6. Using TMPFS to store the zone files. 4
7. Change Log 4

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.

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.

4. 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-log: yes
    rpz-log-name: log/urlhaus.log
```

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: log/urlhaus.log is actually /etc/unbound/log/urlhaus.log

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

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

5. **Test the RPC 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 [log/urlhaus.log] testentry.rpz.urlhaus.abuse.ch. nxdomain
```

6. **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.

7. **Change Log**
   26-11-2021

   Version 1 (draft). Report issues here.