Contents

Introduction

Unbound is a very secure validating, recursive, and caching DNS server primarily developed by NLnet Labs, VeriSign Inc, Nominet, and Kirei. The software is distributed free of charge under the BSD license. The binaries are written with a high security focus, tight C code and a mind set that it is always under attack or remote servers are always trying to pass it bad information.

Unbound's design is a set of modular components which incorporate features including enhanced security (DNSSEC) validation, Internet Protocol Version 6 (IPv6), and a client resolver library API as an integral part of the architecture.

As for the configuration, a simple resolving caching DNS server which can be used for a single machine or multi-machine LAN is only a few lines long. Note that Unbound is not a full fledged authoritative server, but you can put in A records for forward and reverse resolution of a small private LAN.

In the future it is expected that many, if not all, other open source distributions will move to Unbound. FreeBSD 10 has already made the change as BIND is no longer included in the default install. BIND, also known as named, is getting extremely code bloated, slow and over complicated. Complication leads to security exploits and over twenty(20) of the last seventy(70) critical bugs in FreeBSD have been due to BIND itself. The other problem is BIND is used for around 70% of the worlds DNS servers leading to a monoculture environment. When an attack or exploit comes out it is advantageous as the attacker to go after the most used software. Unbound in comparison is an incredibly fast and secure DNS name server which, due to its small size, can easily be code audited for security.

Setup

The only thing you have to do is to tick Recursive DNS Resolving on index.asp page (Setup>Basic Setup tab) of your dd-wrt. Make sure you have working time/date (ntp client) otherwise Unbound will not work after reboot (DNSSEC validateing needs correct local time). It is important that you use Server IP for router NTP Client not hostname (e.g. 193.25.222.240 instead of 0.europe.pool.ntp.org).

A default configuration is stored under /tmp/unbound.conf

You can check whether your Unbound resolver validates DNSSEC signatures on this link

Whether your DNS is leaking you can check here

Custom config

Since changesets r30220 and r36376 it is possible to use custom configurations from usb. In this way you can combine multiple functions together in a single DNS server. For example you can have a caching DNS, a recursive caching DNS, a validating recursive caching DNS, an authoritative validating recursive caching DNS, DNS Over TLS, simple recursive caching DNS, TCP port 853 ENCRYPTED etc.

Simple recursive caching DNS, UDP port 53 unencrypted

- unbound.conf

```
server:
verbosity: 1
interface: 0.0.0.0
interface: ::0
outgoing-range: 60
outgoing-num-tcp: 1
incoming-num-tcp: 1
msg-buffer-size: 8192
msg-cache-size: 100k
msg-cache-slabs: 1
num-queries-per-thread: 30
rrset-cache-size: 100k
rrset-cache-slabs: 1
infra-cache-slabs: 1
infra-cache-numhosts: 200
access-control: 10.0.0.0/8 allow
access-control: 127.0.0.0/8 allow
access-control: 192.168.0.0/16 allow
username: ""
pidfile: "/var/run/unbound.pid"
root-hints: "/etc/unbound/named.cache"
target-fetch-policy: "2 1 0 0 0 0"
harden-short-bufsize: yes
harden-large-queries: yes
auto-trust-anchor-file: "/etc/unbound/root.key"
key-cache-size: 100k
key-cache-slabs: 1
neg-cache-size: 10k
minimal-responses: yes
prefetch: yes
qname-minimisation: yes
rrset-roundrobin: yes
use-caps-for-id: yes
local-data: "localhost A 127.0.0.1"
local-data: "DD-WRT A 192.168.1.1"
python:
remote-control:
forward-zone:
name: "."
forward-addr: 8.8.4.4
forward-addr: 8.8.8.8
forward-addr: 208.67.222.220
forward-addr: 208.67.222.222
```

useful commands

```
nslookup whoami.akamai.net
```

the output of this useful directive from BusyBoy will tell you what DNS you are using.