

Configuring Unbound

1. Log in using SSH/Putty/... to your RESOLVER machine:

(i.e. for group 1, you would use resolv.grp1.dns.nsrc.org)

```
$ ssh sysadm@resolv.grpXX.dns.nsrc.org
```

```
*** PLEASE MAKE SURE YOU ARE LOGGED IN TO YOUR 'RESOLV' MACHINE, AND ***  
*** NOT IN YOUR 'AUTH1' or 'AUTH2' ***
```

2. On your RESOLVER machine (which you just logged into

```
$ cd /usr/local/etc/unbound/  
$ sudo cp unbound.conf.sample unbound.conf
```

Now edit the file unbound.conf:

NOTE: Here, remember to use your favorite editor: ee, jed, joe, vi, ...

```
$ sudo ee unbound.conf
```

or

```
$ sudo vi unbound.conf
```

... and make the following changes:

- a) enable listening - find the lines with:

```
# interface: ...  
# interface: ...
```

and just under, add this line:

```
interface: 0.0.0.0
```

- b) access control - find the lines with:

```
# access-control: ...  
# access-control: ...
```

and just under, add this line:

```
access-control: 10.20.0.0/16 allow
```

- c) chroot security - find the line

```
# chroot: "/usr/local/etc/unbound"
```

and just under, add this line:

```
chroot: ""
```

NOTE: We would normally not turn off chroot, which is a security mechanism, but we need to do this here in the lab, because of restrictions from the virtualization environment. In a production environment, we wouldn't do this.

- d) set the root-hints file - find the line with:

```
# root-hints: ""
```

and just under, add this line:

```
root-hints: "/usr/local/etc/unbound/named.root"
```

e) re-enable the 10.in-addr.arpa zone - find the line with:

```
# local-data-ptr: "192.0.2.3 www.example.com"
```

and just under, add this line:

```
local-zone: "10.in-addr.arpa." nodefault
```

f) enable remote control - find the line with:

```
# control-enable: no
```

and CHANGE it (by removing # in front) to:

```
control-enable: yes
```

- find the line with:

```
# control-interface: 127.0.0.1
```

and CHANGE it to:

```
control-interface: 0.0.0.0
```

- find the line with:

```
# control-port: 8953
```

and CHANGE it to:

```
control-port: 8953
```

- finally, uncomment the following 4 lines:

```
# server-key-file: "/usr/local/etc/unbound/unbound_server.key"
```

becomes

```
server-key-file: "/usr/local/etc/unbound/unbound_server.key"
```

```
# server-cert-file: "/usr/local/etc/unbound/unbound_server.pem"
```

becomes

```
server-cert-file: "/usr/local/etc/unbound/unbound_server.pem"
```

```
# control-key-file: "/usr/local/etc/unbound/unbound_control.key"
```

becomes

```
control-key-file: "/usr/local/etc/unbound/unbound_control.key"
```

```
# control-cert-file: "/usr/local/etc/unbound/unbound_control.pem"
```

becomes

```
control-cert-file: "/usr/local/etc/unbound/unbound_control.pem"
```

Save the file, exit.

You still need to copy named.root root hints file where unbound can find it.

```
$ cd /usr/local/etc/unbound
$ sudo cp /etc/namedb/named.root .
```

3. Create the control keys:

```
$ sudo unbound-control-setup
```

4. Test the configuration:

```
$ sudo unbound-checkconf
```

5. edit /etc/rc.conf and add:

```
unbound_enable="YES"
```

6. start unbound!

```
$ sudo service unbound start
```

7. Change your /etc/resolv.conf to use your newly configured Unbound, on this machine (RESOLV), but on AUTH1 and AUTH2 as well:

```
# vi /etc/resolv.conf
```

Change the nameserver line to:

```
nameserver 10.20.XX.3
```

... where XX is the number of your group

8. Test

```
$ dig
$ dig noc.dns.nsrc.org
```

Make sure you see SERVER: ...(10.20.XX.3) at the bottom of dig's output.

```
$ dig version.bind txt chaos
```

What does the output say ?

9. In a previous lab, you may have configured BIND on the AUTH1 host to function as a recursive.

If so, now is the time to turn it off.

NOTE: You do NOT need to do this unless you have enabled recursion in your BIND config.

So we need to go on our AUTH1 host, and change the resolv.conf.

Log on to your master (auth1.grpX.dns.nsrc.org), and change the /etc/resolv.conf so that it now uses your newly configured unbound:

```
$ sudo ee /etc/resolv.conf
```

And make it look like this:

```
search dns.nsrc.org  
nameserver 10.20.X.3
```

... where X is the number of your group

Then test that you can resolv *.dns.nsrc.org names:

```
$ dig noc.dns.nsrc.org
```

Check the SERVER: statement at the bottom of the dig output to make sure you are running with the correct server

Finally, turn off recursion on the AUTH1 host.

Edit /etc/namedb/named.conf (sudo ee ...) and make the following changes:

From this:

```
allow-recursion { 127.0.0.1; 10.20.0.0/16; };
```

To this:

```
// allow-recursion { 127.0.0.1; 10.20.0.0/16; };  
recursion no;
```

If these statements aren't there, don't worry, just skip this step!

Save the file, and restart named:

```
$ sudo service named restart
```