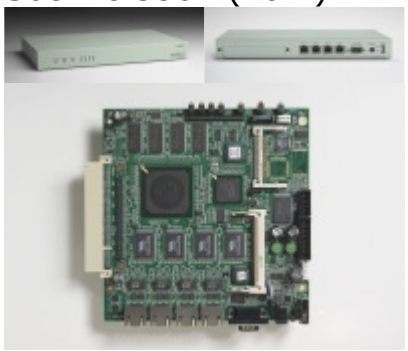
HowTo => OpenBSD => Local Caching DNS + DNSSEC (UNBOUND)

Hardware	=>	Soekris 5501 (10W)



Tools	=>	USB naar Serial Adapter voor Console Putty voor Terminal sessie middels USB Serial Adapter
Operating System	=>	OpenBSD 4.8
Software	=>	UNBOUND

Inleiding:

Door zelf lokaal een Caching DNS in te richten zal je netwerkverkeer sneller worden.
Dit komt omdat dan niet voor iedere aanvraag een verbinding naar een externe DNS dient te worden opgezet, dit effect wordt groter met meerdere gebruikers op het interne netwerk.
Alle interne servers zijn bereikbaar onder hun FQDN (Fully Qualified Domain Name).
Ook de werkplekken die hun IP via DHCP krijgen hebben nu een naam.
DNSSEC is er om risico van Cache Poisoning en man-in-the-middle attacks te voorkomen.
Aangezien BIND op OpenBSD zwaar achter loopt op de laatste ontwikkelingen, en derhalve DNSSEC niet goed ondersteund, maken we in dit document gebruik van UNBOUND.
Deze DNS is vanaf de grond opnieuw opgebouwd en ondersteund door o.a. NLnetlabs, het is zeer snel en veilig.

Pre-installatie:

Zie volgende stap.

Houdt de ingevulde variabelenlijst van de **Bijlage Variabelen** in het inleidende document **HowTo OpenBSD Firewall met Secure Anonymous Access** bij de hand tijdens instalatie/configuratie. Zodra je een variabele ziet, bv `%HOST%` vervang dit dan in zijn geheel door wat je had ingevuld, dus zeker geen %-tekens achterlaten.

Installatie:

```
root @ 10.0.10.1 - PuTTY [ksh]
# pkg_add unbound
```

Post-Installatie:

Configuratie gaat middels onderstaande bestanden.

Voor syslog socket in chroot.

```
root @ 10.0.10.1 - PuTTY [vi /etc/rc.conf.local]
syslogd_flags="${syslogd_flags} -a /var/unbound/dev/log"
```

Opstarten tijdens boot.

```
root @ 10.0.10.1 - PuTTY [vi /etc/rc.local]
if [ -x /usr/local/sbin/unbound ]; then
   echo -n ' unbound'
   /usr/local/sbin/unbound
fi
```

Wijzig de te raadplegen Nameserver.

```
root @ 10.0.10.1 - PuTTY [vi /etc/resolv.conf]
nameserver 127.0.0.1
nameserver 10.0.10.1
```

Haal de laatste versie van bestand met Root Servers.

```
root @ 10.0.10.1 - PuTTY [ksh]
# wget ftp://FTP.INTERNIC.NET/domain/named.cache -O
/var/unbound/etc/root.hints
```

Maak bestand met juiste eigenaar.

```
root @ 10.0.10.1 - PuTTY [ksh]
# cd /var/unbound/etc
# touch root.key
# chown _unbound root.key
```

Haal nu de `auto-trust-anchor-file`.
https://data.iana.org/root-anchors/
Dit XML bestand bevat de Key voor de DNSSEC Root Server validatie.
Hiermee kan een Chain-Of-Trust worden samengesteld.
De huidige Key staat hieronder, indien er een nieuwere is pas dan aan obv gegeven format.
Plaats de Key in het bestand.

```
root @ 10.0.10.1 - PuTTY [vi /var/unbound/etc/root.key]
. IN DS 19036 8 2
49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5
```

Bewaar de originele configuratie.

```
root @ 10.0.10.1 - PuTTY [ksh]
# cp -p unbound.conf unbound.conf.org
```

Verdere configuratie in dit bestand.

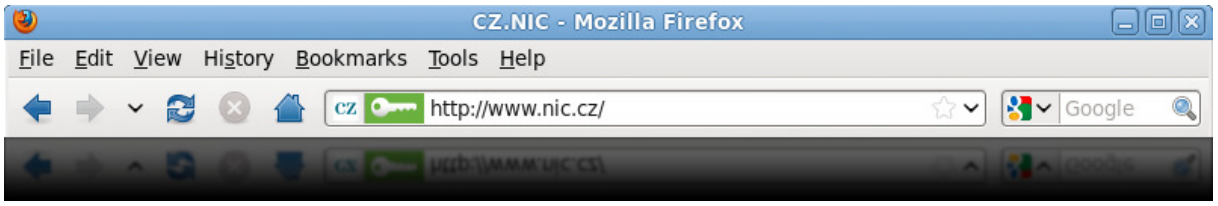
root @ 10.0.10.1 - PuTTY [vi /var/unbound/etc/unbound.conf]

```
###############################################################################
#######
###                              unbound.conf
###
###############################################################################
#######

###          Authoritative, Validating, Recursive Caching DNS
###

server:
    verbosity: 1

    interface: 127.0.0.1
    interface: 10.0.10.1

    port: 53

    do-ip4: yes
    do-ip6: no

    do-udp: yes
    do-tcp: no

    access-control: 127.0.0.0/8 allow
    access-control: 10.0.0.0/16 allow

    private-address: 10.0.0.0/16
    private-domain: "%DOMEIN%"

    root-hints: "/var/unbound/etc/root.hints"

    auto-trust-anchor-file: "/var/unbound/etc/root.key"
```

```
    hide-identity: yes
    hide-version: yes

    harden-glue: yes
    harden-dnssec-stripped: yes

    use-caps-for-id: yes

    cache-min-ttl: 3600
    cache-max-ttl: 86400

    prefetch: yes

    unwanted-reply-threshold: 10000

    do-not-query-localhost: no

    val-clean-additional: yes

### Lokale Zones voor machines op het LAN
#
    local-zone: "%DOMEIN%." static

    local-data: "%HOST%.%DOMEIN%. IN A 10.0.10.1"
    local-data: "dhcp1.%DOMEIN%.  IN A 10.0.10.10"
    local-data: "dhcp2.%DOMEIN%.  IN A 10.0.10.11"
    local-data: "dhcp3.%DOMEIN%.  IN A 10.0.10.12"
    local-data: "dhcp4.%DOMEIN%.  IN A 10.0.10.13"
    local-data: "dhcp5.%DOMEIN%.  IN A 10.0.10.14"

    local-data-ptr: "10.0.10.1    %HOST%.%DOMEIN%"
    local-data-ptr: "10.0.10.10   dhcp1.%DOMEIN%"
    local-data-ptr: "10.0.10.11   dhcp2.%DOMEIN%"
    local-data-ptr: "10.0.10.12   dhcp3.%DOMEIN%"
    local-data-ptr: "10.0.10.13   dhcp4.%DOMEIN%"
    local-data-ptr: "10.0.10.14   dhcp5.%DOMEIN%"
```

Dit onderdeel is niet strikt noodzakelijk, het is ook niet op de Soekris.
Toch installeren, want het geeft direct het resultaat weer van DNSSEC.
Het is een plugin voor Firefox.
http://www.dnssec-validator.cz/

Dit is waar we het allemaal voor doen.



De kleur van de sleutel geeft aan wat de status is, klik op de sleutel voor een popup met meer info.
Helaas blijken er nog heel weinig domeinen met DNSSEC, wij zijn early adopters!

Test:

Tijdelijk, voor de duur van de test, verhogen loglevel.

```
root @ 10.0.10.1 - PuTTY [vi /var/unbound/etc/unbound.conf]
verbosity: 3
```

Bekijk PID van unbound.

```
root @ 10.0.10.1 - PuTTY [ksh]
# ps -aux
```

Opnieuw inlezen configuratie.

```
root @ 10.0.10.1 - PuTTY [ksh]
# kill -1 <PID>
```

Kijk nu naar de gedetailleerde output.

```
root @ 10.0.10.1 - PuTTY [ksh]
# tail -f /var/log/daemon
```

Links:

http://www.openbsd.org/
http://www.chiark.greenend.org.uk/~sgtatham/putty/
http://unbound.net/documentation/index.html

Boeken:

Alternative DNS Servers: Choice and Deployment, and Optional SQL/LDAP Back-Ends