

1) Instalación

```
# yum install unbound
```

Nota: Tendremos usuario unbound (y su home dir)

2) Chrooted files

Lista oficial de root name servers

systemctl start unbound

systemctl enable unbound

3) Configurar

vim /etc/unbound/unbound.conf

...

interface: 192.0.2.153

...

access-control: 0.0.0.0/0 refuse

access-control: 127.0.0.0/8 allow

...

forward-zone:

name: "example.com"

forward-addr: 192.0.2.68

forward-addr: 192.0.2.73

...

domain-insecure: "example.com"

- SELinux: como dejamos todas las opciones por defecto no hay que hacer nada
- FIREWALL: puertos 53/tcp 53/udp

DNSSEC

Extensiones de seguridad al protocolo DNS

Asegura:

- La autenticidad del origen
- La integridad de los datos
- Verifica la inexistencia de un dominio

No asegura:

- Confidencialidad
- Ataques DOS(Denegación de servicio)
- Ataques de amplificación

DNSSEC se basa en la encriptación de clave pública (o asimétrica):


- La clave privada se usa para firmar el dato dns
- La clave pública se publica a través del dns para que los resolvers puedan usarlas
- La clave pública se usa para validar las firmas, y así, los datos dns

- Clients using validating resolvers get "guaranteed good" results
- Data that does not validate provides a "SERVFAIL" response from the upstream resolver

Trust Validation

DNSSEC se basa en “chains of trust”

En el punto mas alto de esta cadena están los "trust-anchors"

- (signed) root  trust-anchor
- Hasta que todos TLD no estén firmados, no será fácil
- “Trust anchors” se tienen que añadir a la configuración de los servidores dns, a través de “saltos de fe”
- “Trust anchors” son bits capaces de validar la clave usada para firmar los datos de una zona

Bibliografía

- Presentaciones pdf muy buenas sobre el dnssec en la página:

<https://kb.isc.org/article/AA-00820/0/DNSSEC-in-6-minutes.html>

- La página del proyecto:

<https://www.unbound.net/>

- Wiki, wiki, wiki...