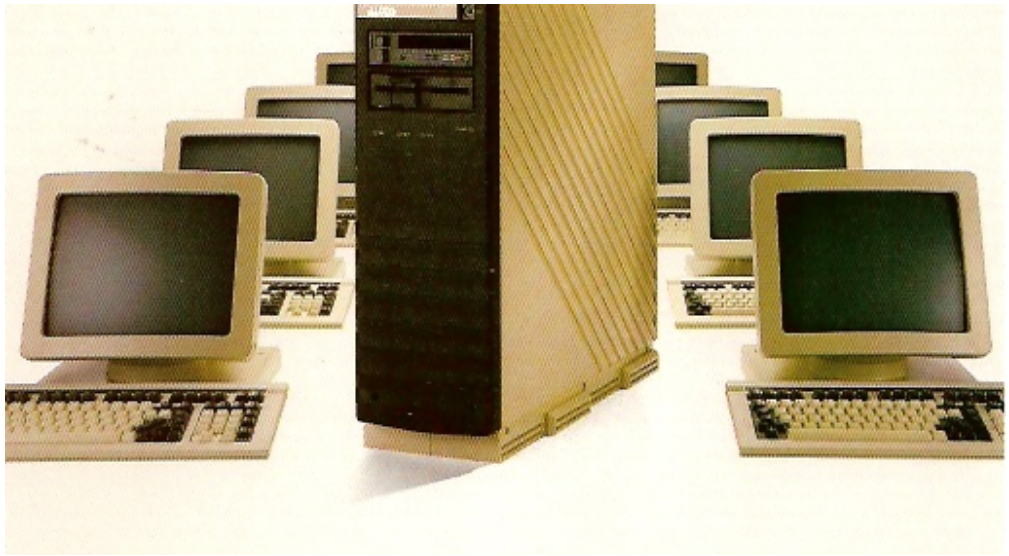
Real-time updates to signed zones using dynamic update, OpenDNSSEC and BIND views

Gavin Brown <gavin.brown@centralnic.com>
ICANN 50 London

A Brief History of CentralNic's DNS System

1994: Altos Series 1000 + Informix => UUCP => SunOS



Kickin' it old school!

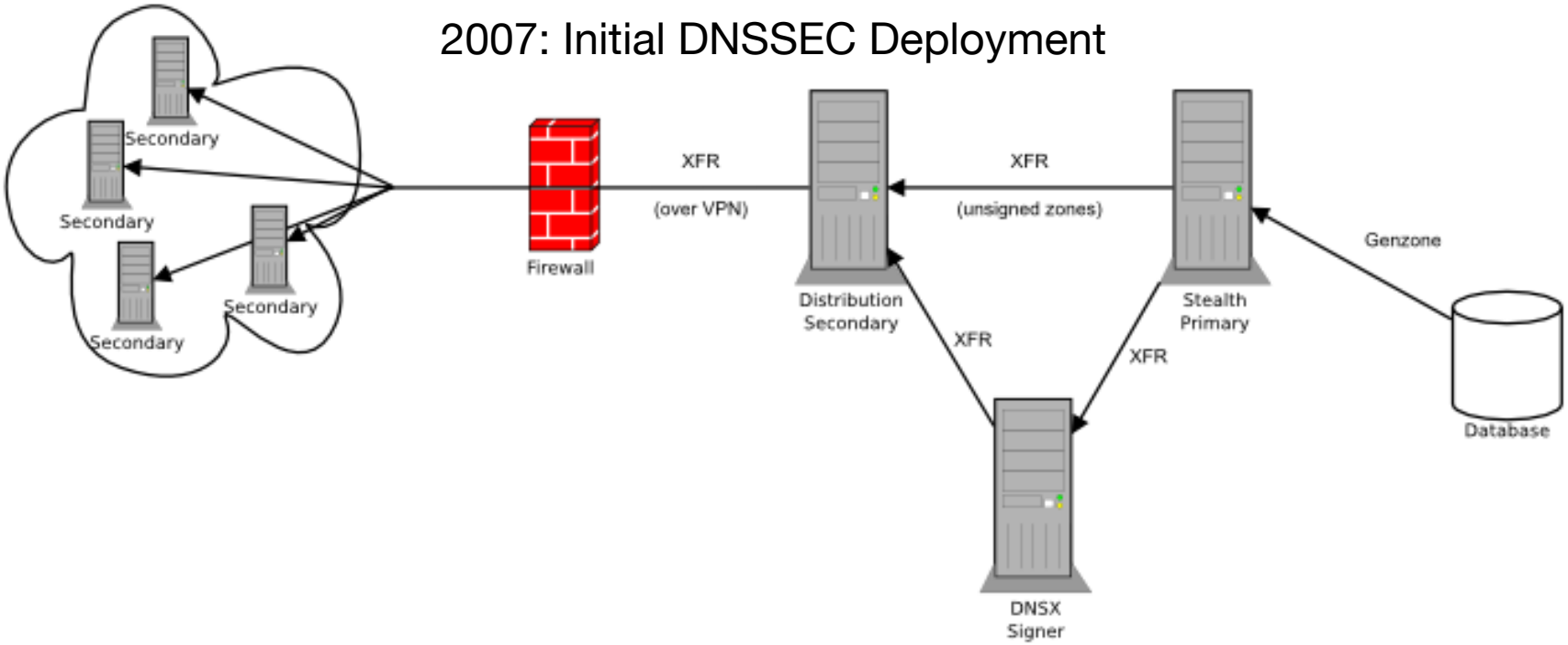
A Brief History of CentralNic's DNS System

2000: Slackware + BIND8

Praise "Bob"

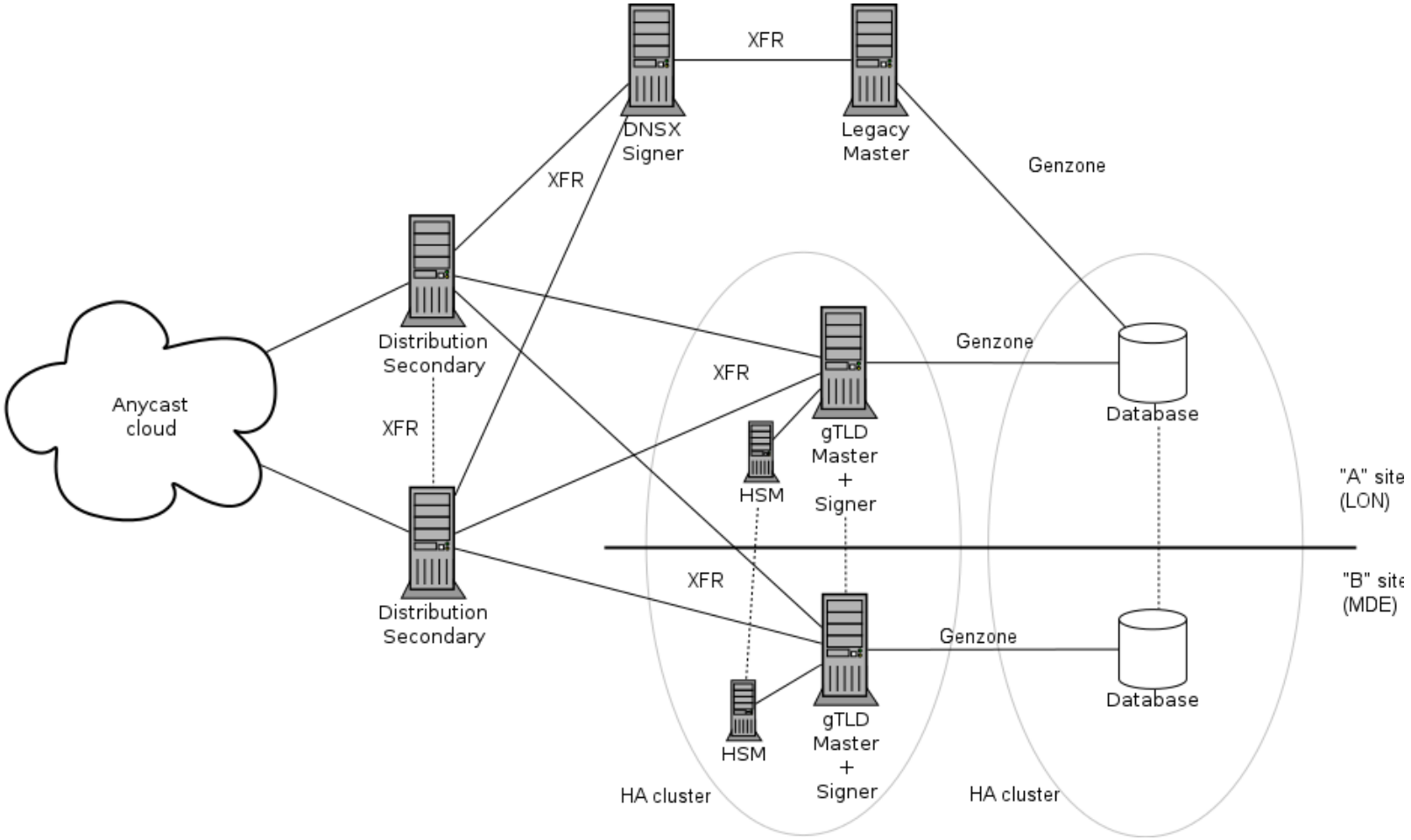
Later: BIND9, migration to CentOS, addition of NSD, Anycast

A Brief History of CentralNic's DNS System



A Brief History of CentralNic's DNS System

2012: new deployment to support new gTLDs



Signer Configuration

- Genzone writes zone files to disk
- Tells ODS to sign
- ODS tells BIND to reload
- BIND sends NOTIFY to slave(s)

2013: dynamic DNS update

- Real-time update of zone data
- Application code assembles update packet (RFC 2136) and sends to master server for unsigned zone
- Updated zone data is then signed and distributed
- Problem: unsigned zone data must now be exposed over port 53 so dynamic updates can be accepted

Dynamic Update: Requirements

- No new infrastructure (physical or virtual)
- Both unsigned and signed zones served over port 53 from the same system
- Solution: BIND views

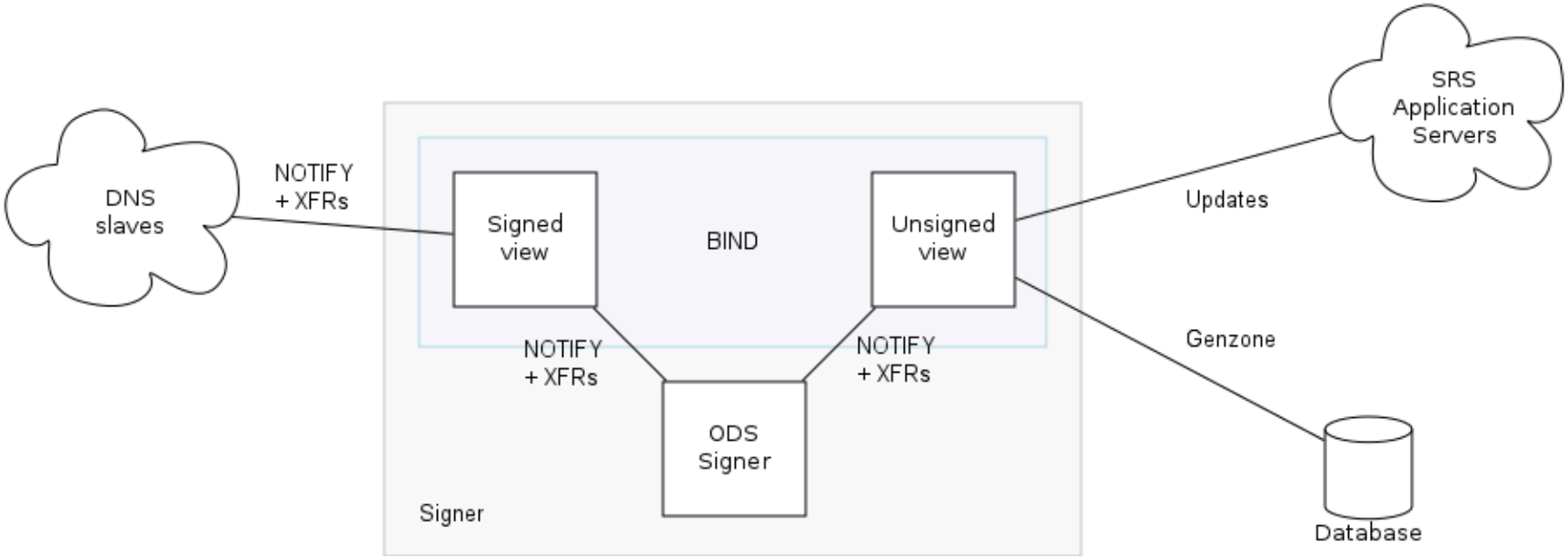
BIND Views

- Essentially virtual DNS servers inside the same BIND process
- Similar to HTTP virtual hosts
- Routing determined by source or destination address of query packet
- Views can contain the same zones but use different zone files

Implementation

- Add additional IP addresses as alias on server's network adapter
  - one extra for BIND
  - one for OpenDNSSEC
- Configure ODS to listen on IP and accept NOTIFY packets/do XFRs
- Configure BIND with two views based on destination address:
  - "unsigned":
    - uses zone files produced by genzone
    - accepts dynamic updates from SRS
    - sends NOTIFY packets to ODS
  - "signed"
    - uses zone files produced by ODS
    - sends NOTIFY packets to slave(s)

Implementation



Configuration - BIND

```
options {
          listen-on { 192.168.1.199; 192.168.1.219; };
          notify explicit;
          # more goes here
};

view "unsigned" {
          match-destinations { 192.168.1.199; };
          notify-source 192.168.1.199;
          also-notify { 192.168.1.198; };
          allow-update { key ”srs-update-key.tsig"; };
          include “gtlds-unsigned.conf";
};

view "signed" {
          match-destinations { 192.168.1.219; };
          notify-source 192.168.1.219;
          also-notify { 192.168.1.150; };
          allow-update { none; };
          include “gtlds-signed.conf";
};
```

Configuration - OpenDNSSEC

conf.xml:

```
<Configuration>
  <!-- more goes here -->
  <Signer>
    <Listener>
      <Interface>
        <Address>192.168.1.198</Address>
        <Port>53</Port>
      </Interface>
    </Listener>
    <NotifyCommand>/usr/sbin/rndc reload %zone in signed</NotifyCommand>
  </Signer>
</Configuration>
```

Configuration - OpenDNSSEC

addns.xml:

```
<?xml version="1.0" encoding="utf-8"?>
<Adapter>
  <DNS>
    <Inbound>
      <RequestTransfer>
        <Remote>
          <Address>192.168.1.199</Address>
        </Remote>
      </RequestTransfer>
      <AllowNotify>
        <Peer>
          <Prefix>192.168.1.199</Prefix>
        </Peer>
      </AllowNotify>
    </Inbound>
  </DNS>
</Adapter>
```

Configuration - OpenDNSSEC

zonelist.xml:

```
<Zone name=”tld">
  <Policy>default</Policy>
  <SignerConfiguration>/var/opendnssec/signconf/tld.xml</SignerConfiguration>
  <Adapters>
    <Input>
      <Adapter type="DNS">/etc/opendnssec/addns.xml</Adapter>
    </Input>
    <Output>
      <Adapter type="File">/var/opendnssec/signed/tld</Adapter>
    </Output>
  </Adapters>
</Zone>
```

Comments

- Use externally visible IPs to allow for debugging + monitoring
- Genzone still used to process updates for batch processes
- Genzone has to “freeze” and “thaw” the zone in the unsigned view before generating a new file
  - i.e. rndc [freelthaw] $zone in unsigned
- OpenDNSSEC DNS adapter has some issues
  - Getting great support from Sara and Matthijs!

Questions

Contact Details:

CentralNic Global Headquarters
CentralNic Ltd. 35-39 Moorgate, London, EC2R 6AR, UK

Tel: +44 (0)20 33 88 0600
Fax: +44 (0)20 33 88 0601