RRI - DNS Servers Proposed Architecture

1. Requirement

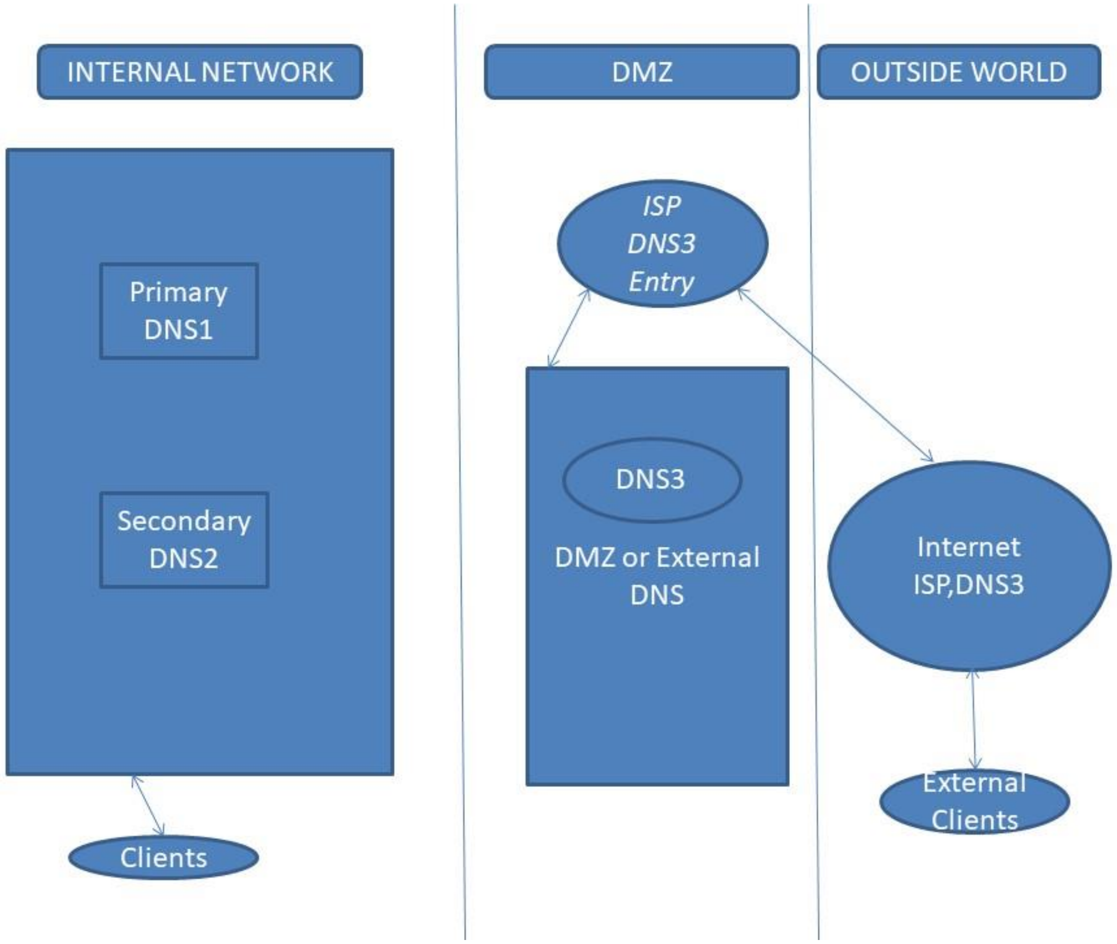
The requirement is as follows:

- Install and configure the latest version of BIND in Debian Linux in the Primary and Secondary DNS servers
- BIND should run in chrooted jail
- Configure our domain and populate the zone files
- There should be two VIEWS - internal and external. Queries from the LAN should give out private IP address and queries from WAN/internet should give out our public IP address.
- The DNS/BIND server should be configured for security and also prevent DNS attacks. The two VMs running the latest version of Debian Linux OS will be provided.

2. Proposed Solution & Architecture

As per best practices & security concepts. It’s recommended that the Local zone is segregated from the external zone. i.e. 2 DNS Servers (Primary & Secondary) will be configured for the Local zone & one external DNS Server (Which can be maintained in a separate network (DMZ) will have the Server’s public IP records).

- 2 DNS Servers (Primary & Secondary) will be hosted in chroot environment to provide name resolution for Local resources belonging to the Domain.
- 1 DNS Server (External DNS Server) will be hosted in a different DMZ network that will host all the required public IP records of the RRI Servers.
- The External DNS Server doesn’t need Secondary server as the configuration back up can be restored with less time. However, you can have a standby VM (Replica Instance in PowerOff Mode).
- The externa DNS Server’s IP will be NATTED to the respective ISP IP’s.



3. Pre-Requisites & Initial Impact

- The ISPs must provide the feature to host RRI domain’s Internal DNS IP Addresses.
- There will be an initial DNS propagation period from the ISP.
- All Server related records must be provided pre-hand from RRI (MX, WWW etc..)
- DMZ parameters to be defined from RRI.