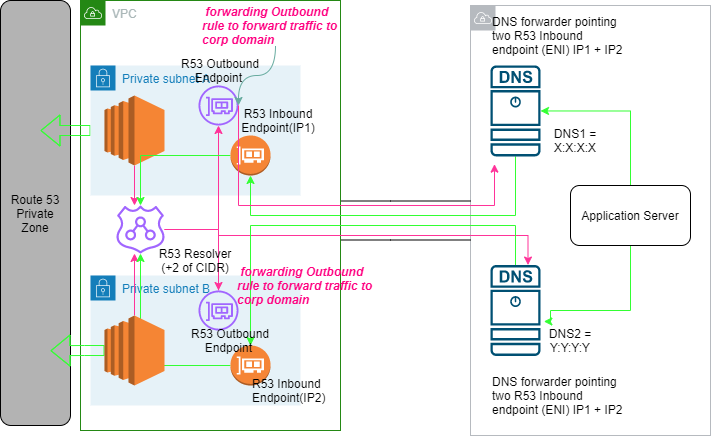
***Hybrid DNS with Route 53 end points***



1. Created AWS end infrastructure with two private subnets , two EC2 instances, R53 private hosted zone with a DNS record mapped with 2 private EC2 instances using Cloud formation template
2. Created simulated on premise environment with 2 Linux DNS(BIND) servers
3. Connection is established between AWS and Onpremise (AWS simulated on premise) through VPC peering. We could have site to site VPN connection or Direct connect between these two environments. VPC peering is created and the route table of AWS system is modified to direct traffic from VPC to on premise with target as VPC peering and destination as CIDR of on-premise. Route table of on-premise network is updated to direct traffic from on premise to VPC with target as VPC peering and destination as CIDR of AWS CIDR.
4. **Created R53 Inbound endpoints i**n two private subnets in AWS VPC and integrate LINUX based DNS forwarder with Inbound endpoints (IP addresses are specified) in **named conf file.** Inbound endpoints are presented as ENI in both subnets.
5. Ifcfg-eth0 file of Application server in sysconfig is updated to point DNSs with their private IP address.
6. Created R53 Outbound endpoints **i**n two private subnets in AWS VPC. It will in turn provision ENI. **Outbound forwarder rule is created to forward traffic to on premise domain** names.

DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules (example.com and www.example.com), outbound DNS queries are routed using the rule that contains the most specific domain name (www.example.com).

Thus , AWS side servers would be able to communicate with on premise domain and on premise domain with AWS side private hosted zone using R53 endpoints.