

Internal DNS Configuration for isp1.net in a Private Network Environment

Objective

This guide describes the steps to configure Core DNS to forward all requests for **isp1.net** to **ISP DNS 1** within an isolated network. The goal is to set up an authoritative, internal-only DNS for **isp1.net**, ensuring local queries are resolved internally without reaching external DNS servers.

Requirements

- Core DNS as the main DNS resolver for internal clients
- ISP DNS 1 as authoritative for **isp1.net**
- Internal domain **isp1.net** that only resolves within the private network, avoiding external DNS lookups

Setup Steps

1. Define the Zone for isp1.net on ISP DNS 1

First, configure ISP DNS 1 to serve as the authoritative DNS for **isp1.net**.

1. Edit the ISP DNS 1 configuration file (typically located at `/etc/bind/named.conf.local`) to add the zone for **isp1.net**. Define the zone as a master and specify `allow-query` to any IP and `allow-transfer` permissions for Core DNS (10.1.0.10).

```
zone "isp1.net" {  
    type master;  
    file "/etc/bind/zones/db.isp1.net";  
    allow-query { any; };  
    allow-transfer { 10.1.0.10; };  
};
```

Create the zone file, typically at `/etc/bind/zones/db.isp1.net`. This file should include the SOA record, NS record, and A records for all devices within **isp1.net**.

```
$TTL 86400  
@ IN SOA isp-dns1.isp1.net. admin.isp1.net. (  
    2023102701 ; Serial  
    3600      ; Refresh  
    1800      ; Retry  
    1209600   ; Expire  
    86400     ; Minimum TTL  
)  
; Nameserver  
    IN NS  isp-dns1.isp1.net.  
; A records  
isp-router1  IN A  10.10.0.2  
isp-dns1     IN A  10.10.1.10  
isp-gateway  IN A  10.10.2.1  
isp-business IN A  10.10.3.1
```

Restart BIND on ISP DNS 1 to apply the changes:

```
sudo systemctl restart bind9
```

2. Configure Core DNS to Use ISP DNS 1 for isp1.net

On Core DNS, define a **stub zone** for **isp1.net** that points to **ISP DNS 1** as the authoritative DNS server for this domain.

1. Add a stub zone entry for **isp1.net** to the Core DNS configuration file, typically located at `/etc/bind/named.conf.local`. In this entry, specify the type as `stub`, set the `masters` to ISP DNS 1's IP (10.10.1.10), and add a `forwarders` directive with empty braces to prevent

forwarding to external servers.

```
zone "isp1.net" {  
    type stub;  
    masters { 10.10.1.10; };  
    forwarders {}; # Prevents external forwarding for isp1.net  
};
```

- Explanation of the `forwarders {};` Directive: By setting `forwarders {};`, we stop Core DNS from forwarding requests for **isp1.net** to any external DNS servers. This directive is crucial to ensure Core DNS exclusively queries ISP DNS 1 for this internal-only domain.
- Restart BIND on Core DNS to load the new configuration:

```
sudo systemctl restart bind9
```

3. Verifying the Configuration

Use the following steps to confirm that the configuration is working correctly.

1. Run a direct query to ISP DNS 1 from Core DNS to confirm that ISP DNS 1 is serving the **isp1.net** records correctly:

```
dig @10.10.1.10 isp-router1.isp1.net
```

Test forwarding from Core DNS by querying **isp1.net** records without specifying ISP DNS 1, confirming that Core DNS is forwarding queries correctly to ISP DNS 1:

```
dig isp-router1.isp1.net @10.1.0.10
```

Use tcpdump or a similar tool to verify that DNS requests for **isp1.net** are reaching ISP DNS 1 and returning the expected responses:

```
sudo tcpdump -i eth0 host 10.10.1.10 and port 53
```

Troubleshooting and Common Issues

1. **REFUSED Errors:** If Core DNS receives REFUSED responses, ensure that ISP DNS 1 has `allow-query` and `allow-transfer` settings configured to allow access from Core DNS (10.1.0.10).
2. **allow-query-cache Denials:** If cache queries are denied, add `allow-query-cache { 10.1.0.10; localhost; };` to ISP DNS 1 to permit Core DNS to access cached entries for faster responses.

3. **No Matching 'Forwarders' Statement:** The `forwarders {};` directive is necessary in this configuration to prevent Core DNS from forwarding **isp1.net** queries to global DNS servers. Adding this directive in the stub zone settings ensures exclusive forwarding to ISP DNS 1.
-

Revision #3

Created 27 October 2024 18:11:39 by Bryan Vest

Updated 27 October 2024 18:20:13 by Bryan Vest