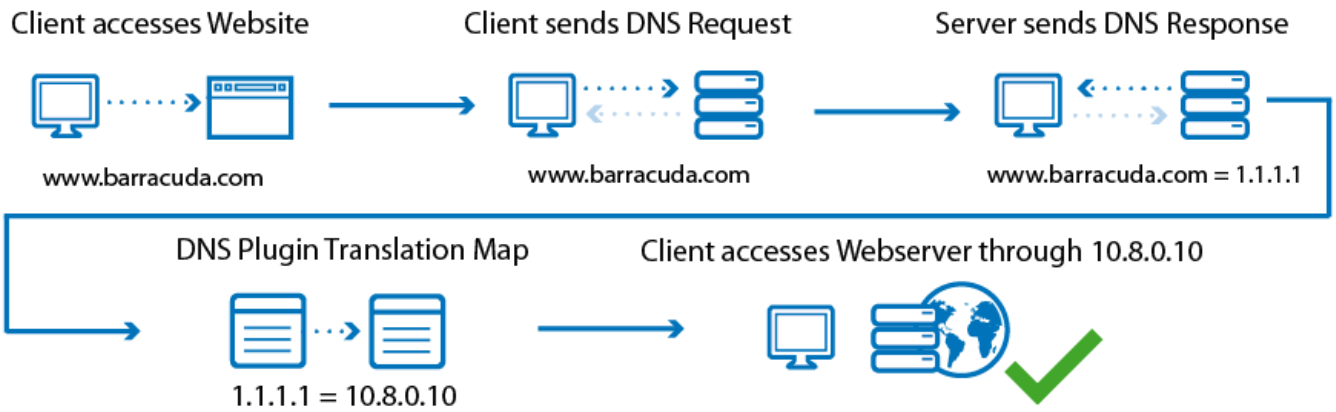
How to Configure DNS Translation Using the DNS Plugin Module

Use the DNS plugin module to replace the result of a DNS query, according to a predefined IP address translation table. A common use case is for users accessing resources that resolve to the public IP address of the firewall. Since the users are behind a NAT, they would not be able to access the resource using this address. The DNS plugin replaces the public IP address in the DNS response with the appropriate internal IP address that can be reached by the client.

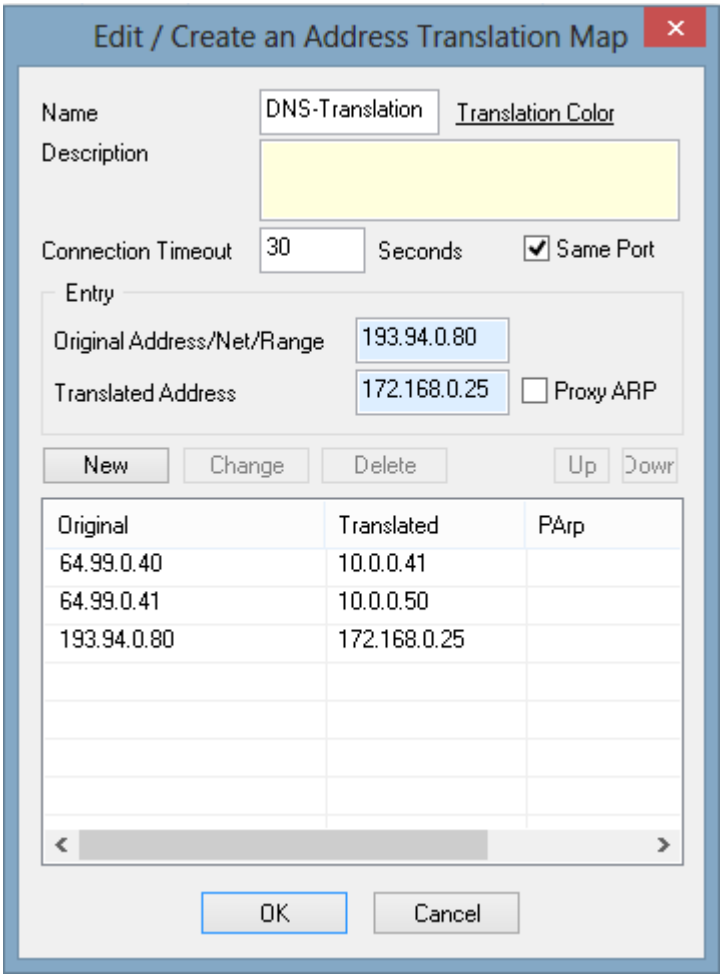


Step 1. Create a new NAT table

Create a NAT table to create a list of public IP addresses and the internal IP addresses the DNS query is translated to.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click on **Connections.**
3. Click **Lock**.

4. Create a NAT table mapping the external IP addresses to the internal IP addresses. For more information, see How to Create NAT Tables (Translation Maps)

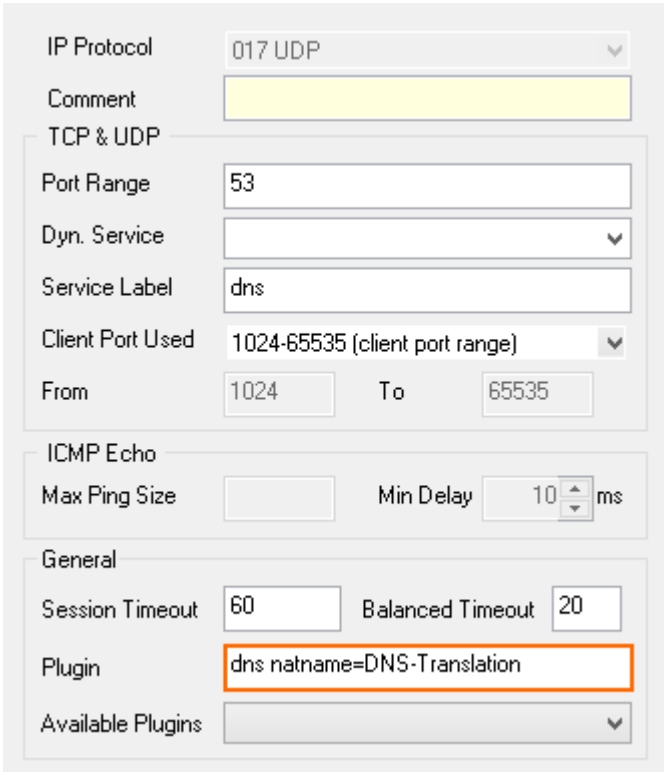


5. Click **Send Changes** and **Activate**.

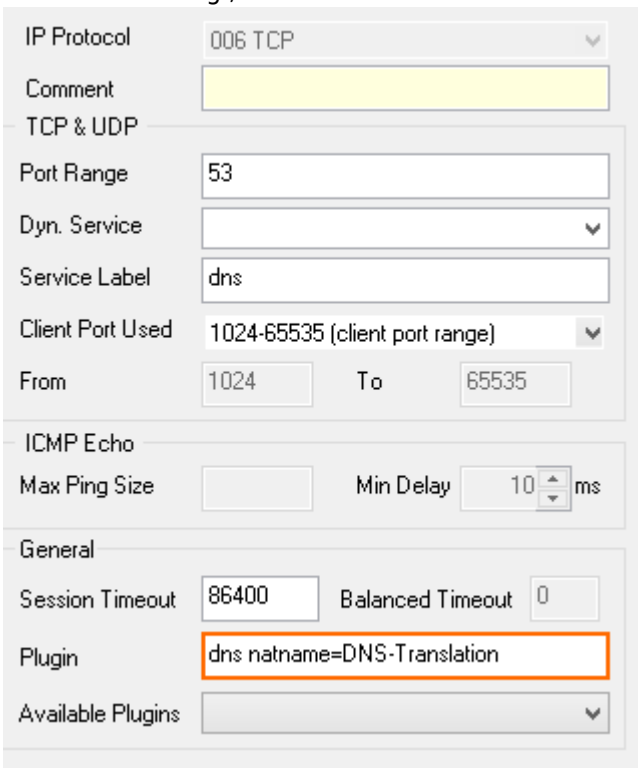
Step 2. Create or edit a service object

Create or edit a service object matching the DNS query of the client, and modify it to use the NAT table

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. In the left menu, click on **Services**.
4. Edit or create a new service object for DNS queries.
5. Double-click on the UDP port 53 entry. The **Service Entry Parameters** window opens.
6. From the **Available Plugins** list, select **dns natname=Translation Map**.
7. Add the name of the NAT table to the **Plugin** string in the following format: **dns natname=YOUR NAT TABLE NAME** E.g., `dns natname=DNS-Translation`



8. Click **OK**.
9. Double-click on the TCP port 53 entry. The **Service Entry Parameters** window opens.
10. From the **Available Plugins** list, select **dns natname=Translation Map**.
11. Add the name of the NAT table to the **Plugin** string in the following format: **dns natname=YOUR NAT TABLE NAME** E.g., `dns natname=DNS-Translation`

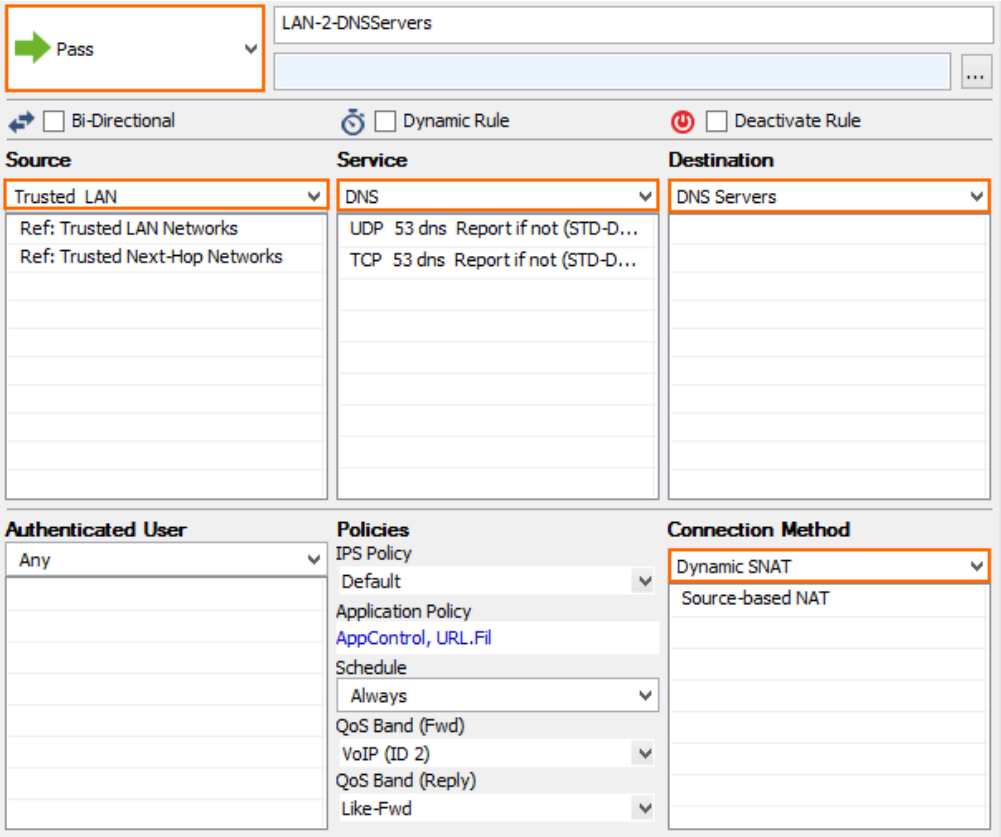


12. Click **OK**
13. Click **OK**.
14. Click **Send Changes** and **Activate**.

Step 3. Create an access rule to intercept client DNS queries

Create an access rule that matches DNS queries of the client using the modified service object.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create an access rule:
   - **Action** – Select **PASS**.
   - **Source** – Select **Trusted LAN**
   - **Service** – Select the modified DNS service object created in step 2.
   - **Destination** – Select **Internet** or enter the IP addresses of your DNS Servers.
   - **Connection Method** – Select **Dynamic SNAT**.



4. Click **OK**
5. Drag and drop the access rule so that no access rule above it matches DNS client traffic.
6. Click **Send Changes** and **Activate**

DNS queries returning the **Original** IP address listed in the NAT table are now replaced by the corresponding **Translated** IP address.

Figures