

# How to Configure DNS Translation Using the DNS Plugin Module

#### https://campus.barracuda.com/doc/17470/

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 > 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 <u>How to Create NAT Tables (Translation Maps)</u>.

## Barracuda CloudGen Firewall



Nan	ne 🛛	DNS-Tra	anslation		
Des	cription				
	L	_			
Colo	or Label		Ti Ti	meout	30
Use	Same Port [				
N/	AT Table				🖶 🗙 🛧 🖣
	Orginal Netv	vork	Translated Base	e IP	Proxy Arp
Ø	64.99.0.40		10.0.0.41		
Ø	64.99.0.41		10.0.0.50		
Ø	193.94.0.80		172.168.0.25		

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 > 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

## Barracuda CloudGen Firewall



IP Protocol	017 UDP		~	
Comment				
Port Range	53			
Dyn. Service			~	
Service Label	dns			
Client Port Used	1024-65535 (client port range)			
From	1024	То	65535	
ICMP Echo				
Max Ping Size		Min Delay	10 🌲 ms	
General				
Session Timeout	60	Balanced Ti	meout 20	
Plugin	dns natname=DNS-Translation			
Available Plugins			~	

- 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

IP Protocol	006 TCP		$\vee$	
Comment TCP & UDP				
Port Range	53			
Dyn. Service			~	
Service Label	dns			
Client Port Used	1024-65535 (client port range) 🗸 🗸			
From	1024	То	65535	
ICMP Echo				
Max Ping Size		Min Delay	10 📥 ms	
General				
Session Timeout	86400	Balanced T	imeout 0	
Plugin	dns natname=DNS-Translation			
Available Plugins			¥	

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 > 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 NAT.

Deer	LAN-2-DNSServers					
Pass	Ť 📃					
🛹 📃 Bi-Directional		Š □ Dynamic Rule		🕘 🗌 Deactivate Rule		
Source VR Instance	default			stance Same as Source		~
Source		Service		Destinat	ion	
Trusted LAN	Ý	DNS	¥	DNS Serv	/ers	~
Ref: Trusted LAN Networks		UDP 53 dns Report if n	ot (STD-D			
Ref: Trusted Next-Hop Net	works	TCP 53 dns Report if n	ot <mark>(</mark> STD-D			
Authenticated User		Policies		Connect	ion Method	
Any	~	IPS Policy		Dynamic	NAT	~
		Default Policy	$\sim$	Dynamic	NAT	
		Application Policy		- Contracting		
		No AppControl				
		SSL Inspection Policy				
		N.A.	$\sim$			
		Schedule				
		Always	~			
		QoS Band (Fwd)				
		No-Shaping	$\sim$			
		QoS Band (Reply)				
		Like-Fwd	$\sim$			
L		LINCHTWU	v	[	OK Car	ncel

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.

## Barracuda CloudGen Firewall



#### Figures

- 1. dns\_translation.png
- 2. DNS\_Doctoring\_01.png
- 3. DNS\_Doctoring\_02.png
- 4. DNS Doctoring 03.png
- 5. DNS\_Doctoring\_04.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.