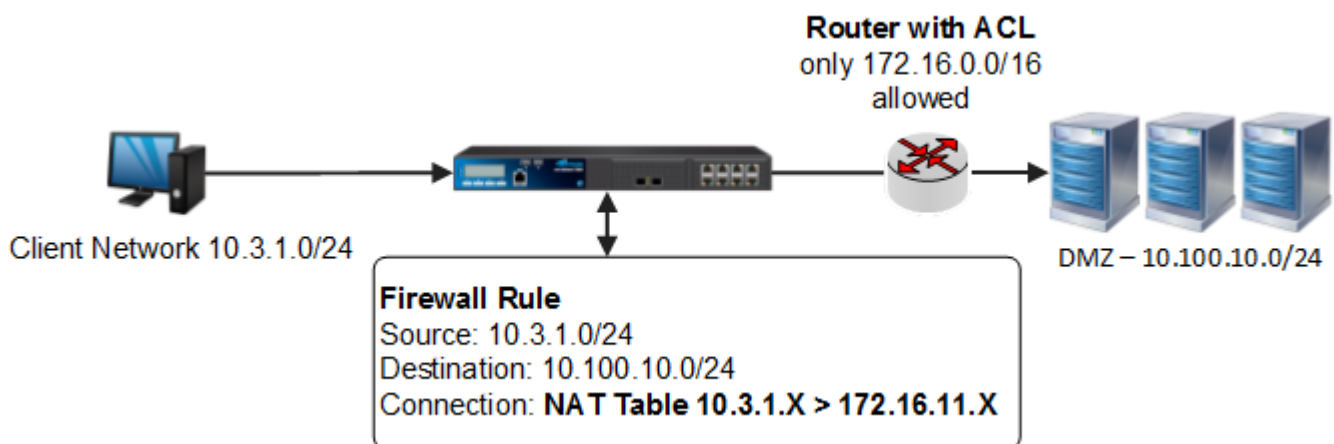


## How to Create NAT Tables (Translation Maps)

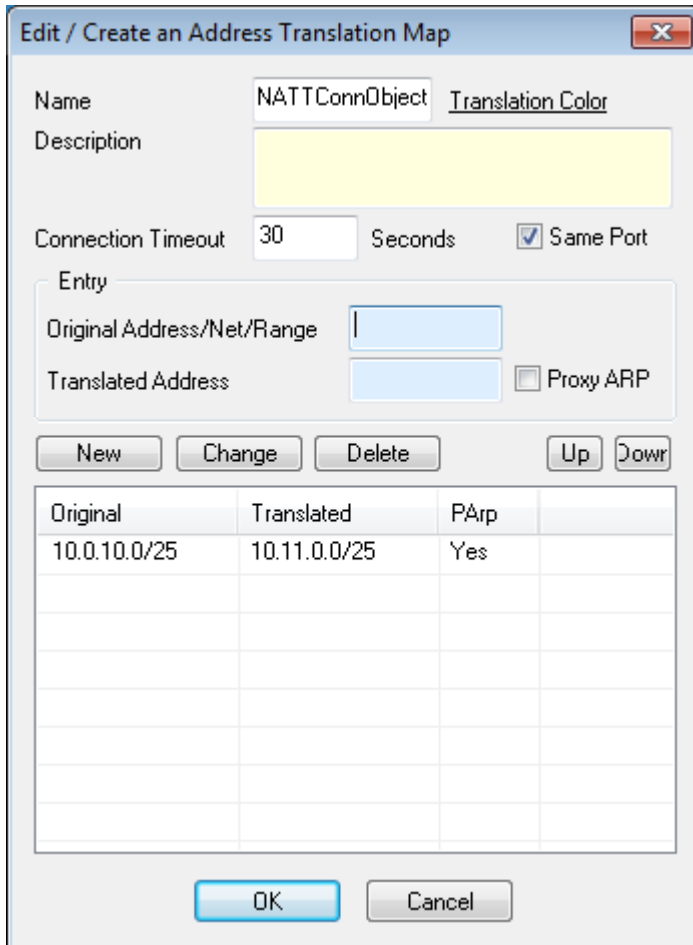
<https://campus.barracuda.com/doc/41115768/>

NAT Tables are an expanded type of source NAT for a network or IP address range. The NAT Tables connection object rewrites the source IP address to a source NAT IP address range. To rewrite both the destination and the source address of the connection, you can choose to use a NAT Table connection object with a MAP firewall rule. You can enter multiple rewriting maps that are processed from the top to the bottom. The first matching rewrite map is used.



### Create a NAT Table Connection Object

1. Open the **Forwarding Rules** page (**Config > Full Config > Virtual Servers > your virtual server > Firewall > Forwarding Rules**).
2. From the left menu, click **Connections**.
3. Click **Lock**.
4. Right-click the table and select **New > NAT Table**.
5. Enter a **Name** for the NAT Table.  
If you want to use this NAT Table in a firewall rule, select this name from the **Connection** list in the firewall rule settings.
6. In the **Original Address/Net/Range** field, enter the source IP range or network.
7. In the **Translated Address** field, enter the network that you want the source IP address or network to be rewritten to.
8. Unless the destination network is connected by a Layer 2 bridge to the source network, select the **Proxy ARP** check box.



**Edit / Create an Address Translation Map**

Name: NATTConnObject [Translation Color](#)

Description: [Empty]

Connection Timeout: 30 Seconds  Same Port

Entry

Original Address/Net/Range: [Empty]

Translated Address: [Empty]  Proxy ARP

[New] [Change] [Delete] [Up] [Down]

Original	Translated	PArp	
10.0.10.0/25	10.11.0.0/25	Yes	

[OK] [Cancel]

9. Click **New** to add the addresses to the list.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

## Apply the NAT Table to a Firewall Rule

To apply a NAT Table object to a firewall rule, select the object from the **Connection** list in the firewall rule settings.

Authenticated User	Policy	Connection Method
Any	IPS Policy	
	Default	<explicit-conn>
	Application Policy	Dynamic SNAT
	AppControl + URL Filter	<b>NATConnObject</b>
	Time Objects	No SNAT
	Always	SNAT with 3G IP
	QoS Band (Fwd)	SNAT with DHCP IP
	VoIP (ID 2)	SNAT with DSL IP
	QoS Band (Reply)	
	Like-Fwd	

OK Cancel

## Figures

1. FW\_NAT-table.png
2. FW\_CO\_NATTables01.png
3. FW\_CO\_NATTables02.png

© Barracuda Networks Inc., 2019 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.