

How to Create a Custom Connection Object

<https://campus.barracuda.com/doc/96026258/>

Connection objects are used to rewrite the source IP address of a connection. You can select the policy by which the translated source IP address is determined. Depending on the selected policy you can enable port address translation, and/or create proxy ARPs for the translated IP address.

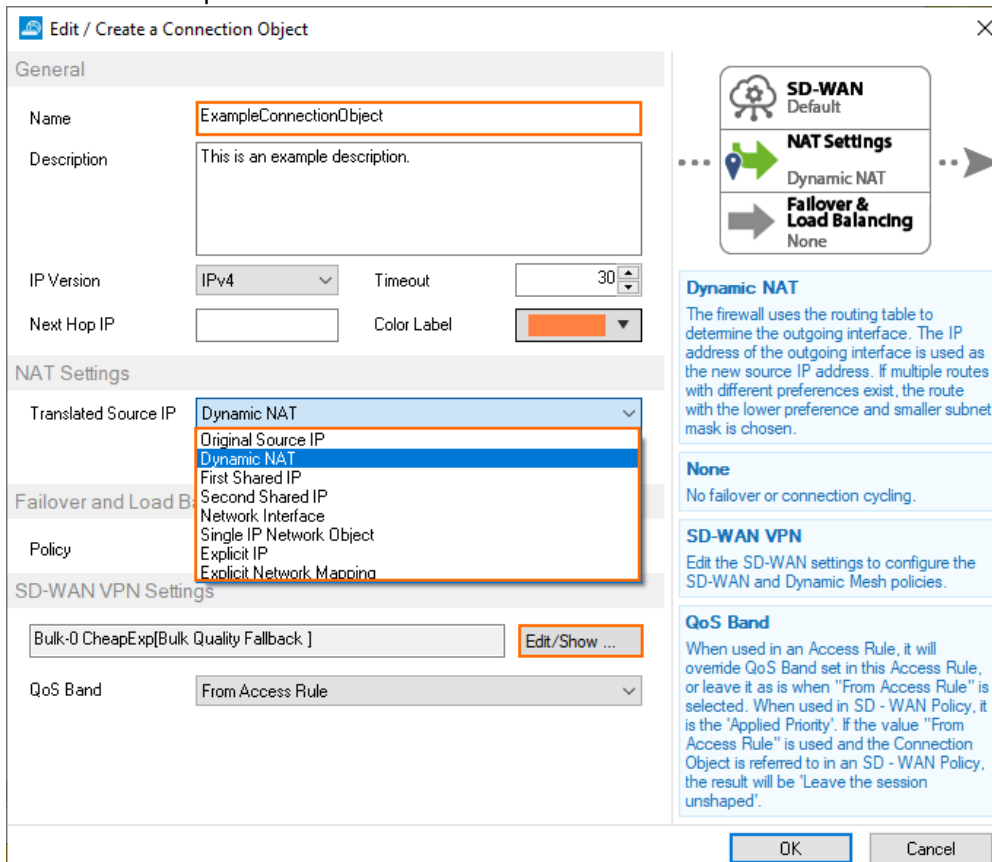
Create a Custom Connection Object without Failover or Load Balancing

The source IP address of the packet is determined by the **Translated Source IP** policy. Depending on the policy, you can also configure proxy ARPs for source IP address that are not on your local network, and disable port rewriting.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Click **Lock**.
4. Right-click the table and select **New > Connection**. The **Edit/Create a Connection Object** window opens.
5. Enter a **Name**.
6. (optional) Enter a **Description** and select a **Color Label**.
7. (optional) Enter the connection **Timeout** in seconds. Increase this value for slow connections, and decrease it for faster failover times. Default: 30 seconds
8. From the **Translated Source IP** list, select how the source address should be determined for your connection:
 - **Original Source IP**
 - **Dynamic NAT**
 - **First Shared IP**
 - **Second Shared IP**
 - **Network Interface**
 - **Interface Name** - Enter the dynamic network interface. For static interface, use **Explicit IP** instead.
 - **Use Same Port** - Select the check box to leave the port unchanged.
 - **Single IP Network Object**
 - **Network Object** - Select the network object from the **Network Object** list.
 - **Create Proxy ARP** - Select **Create Proxy ARP** for the firewall to answer ARP requests for the translated IP address.
 - **Use Same Port** - Select the check box to leave the port unchanged.
 - **Explicit IP**
 - **Explicit IP** - Enter the IP address. All source IP addresses are translated to this IP address.
 - **Create Proxy ARP** - Select **Create Proxy ARP** for the firewall to answer ARP

requests for the translated IP address.

- **Use Same Port** – Select the check box to leave the port unchanged.
- **Explicit Network Mapping**
 - **Map to Network** – Enter the network the source IP address will be mapped to. The source and translated networks must be the same size. Otherwise, the larger source network will be wrapped into the smaller translated network.
 - **Netmask** – Select the netmask from the list.
 - **Create Proxy ARP** – Select **Create Proxy ARP** for the firewall to answer ARP requests for the translated IP address.



Edit / Create a Connection Object

General

Name: ExampleConnectionObject

Description: This is an example description.

IP Version: IPv4 Timeout: 30

Next Hop IP: Color Label: [Orange]

NAT Settings

Translated Source IP: Dynamic NAT

Failover and Load Balancing

Policy: Dynamic NAT

SD-WAN VPN Settings

Bulk-Q CheapExp[Bulk Quality Fallback] Edit/Show ...

QoS Band: From Access Rule

Dynamic NAT

The firewall uses the routing table to determine the outgoing interface. The IP address of the outgoing interface is used as the new source IP address. If multiple routes with different preferences exist, the route with the lower preference and smaller subnet mask is chosen.

None

No failover or connection cycling.

SD-WAN VPN


Edit the SD-WAN settings to configure the SD-WAN and Dynamic Mesh policies.

QoS Band

When used in an Access Rule, it will override QoS Band set in this Access Rule, or leave it as is when "From Access Rule" is selected. When used in SD - WAN Policy, it is the 'Applied Priority'. If the value "From Access Rule" is used and the Connection Object is referred to in an SD - WAN Policy, the result will be 'Leave the session unshaped'.

OK Cancel

9. Click **OK**.
10. (optional) To edit the **VPN SD-WAN** and **Dynamic Mesh** settings, click **Edit/Show**. For more information, see [SD-WAN](#) and [Dynamic Mesh VPN Networks](#).

 Edit / Create a Connection Object ✕

General

Name

Description

IP Version Timeout

Next Hop IP Color Label

NAT Settings

Translated Source IP Weight

Failover and Load Balancing

Policy

SD-WAN VPN Settings

QoS Band

SD-WAN
Default

NAT Settings
Dynamic NAT

Fallover & Load Balancing
None

Dynamic NAT
The firewall uses the routing table to determine the outgoing interface. The IP address of the outgoing interface is used as the new source IP address. If multiple routes with different preferences exist, the route with the lower preference and smaller subnet mask is chosen.

None
No failover or connection cycling.

SD-WAN VPN
Edit the SD-WAN settings to configure the SD-WAN and Dynamic Mesh policies.

QoS Band
When used in an Access Rule, it will override QoS Band set in this Access Rule, or leave it as is when "From Access Rule" is selected. When used in SD - WAN Policy, it is the 'Applied Priority'. If the value "From Access Rule" is used and the Connection Object is referred to in an SD - WAN Policy, the result will be 'Leave the session unshaped'.

11. Click **OK**.
12. Click **Send Changes** and **Activate**.

Next Steps

Use this custom connection object as the **Connection Method** in your **Pass**, **Dst NAT** or **Broad Multicast** access rules. For more information, see [Access Rules](#).

Figures

1. conn_obj_01.png
2. conn_obj_02.png

© Barracuda Networks Inc., 2024 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.