How to Create a Custom Connection Object

https://campus.barracuda.com/doc/46209013/

Connection objects are used to rewrite the source IP address of a connection. Connection object is also used for outbound loadbalancing and failover support. A custom connection object allows you to combine loadbalancing / failover support with a custom source IP address.

Create a Custom Connection Object

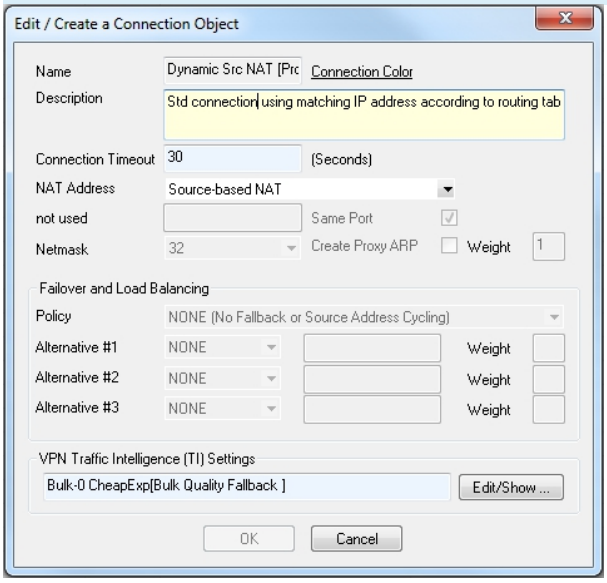
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Right-click the table and select **New Connection**. The **Edit/Create a Connection Object** window opens.
4. In the **Name** field, enter a name for the connection object. E.g., `CustomConnectionObject`
5. From the **NAT Address** list, select how the source address should be determined for your connection:
   - **Client | No Src NAT** – Uses the source IP
   - **Source-based NAT** – Dynamically chosen according to firewall routing tables. This is a general purpose option.
   - **Src NAT – 1st Srv IP (Proxyfirst)** – Uses the **First-IP[IP1]** configured in the virtual **Server Properties** the firewall service is running on.
   - **Src NAT – 2nd Srv IP (Proxysecond)** – Uses the **Second-IP[IP2]** configured in the virtual **Server Properties** the firewall service is running on.
   - **From Interface** – Explicitly specified interface. May be used to restrict the bind address to a specific interface. Selecting Interface activates further options below and in section Firewall configuration -
   - **Explicit** – Explicitly specified IP address. May be used to restrict the bind address to a specific address. Selecting **Explicit** activates further options below and in section **Firewall Configuration** – **Service Objects – General settings** – section **Failover and Load Balancing**:
     - **Same Port –** Ticking this checkbox enforces to use the same client port when establishing the connection.
     - **Explicit IP –** Here the specific IP address is to be entered.
     - **Create Proxy ARP –** If the explicitly defined IP address does not exist locally, an appropriate ProxyARP entry may be created by selecting this checkbox.
   - **Network Object** – section **Failover and Load Balancing**:
     - **Interface Name –** Here the name of the affected interface is to be entered.
   - **Translation Table –** Source NAT for a complete subnet. In order to avoid misconfiguration, the netmasks up to 16 bits can be used. Otherwise, a Proxy ARP with 10.0.0.0/8 would "blank out" the whole internal network for example.

     If you define a map, make sure that the source range using this connection is equal or smaller than the map range. If not, the firewall will wrap the larger source net

into the smaller bind net. E.g., If you use X.X.X.X/24 network as source and a Y.Y.Y.Y/25 as the map range, the IP address X.X.X.128 is mapped to Y.Y.Y.1.

6. **Map to Network –** Here the specific mapping network is to be entered.
7. **Netmask –** Here the corresponding netmask is to be entered.
8. **Proxy ARP –** This parameter is needed by a router if the addresses live in its local network. For more information, see How to Create Proxy ARP Objects.

   If the connection object applies to a multi-transport VPN tunnel, you can define the preferred and secondary transport class in the **VPN Traffic Intelligence (TI) Settings** section.



9. Click **OK**.
10. Click **Send Changes** and **Activate**.

You can now apply the connection object to your firewall rules. Double-click a rule´s number (or right click an existing firewall rule and select **Edit Rule** to open the rule configuration). From the left navigation pane, select the **Object Viewer** check box to drag connections objects from the **Object Viewer** window to the **Connection Method** table.

Parameters

General Settings

Parameter	Description
Name	Name of the connection object.
Description	Significant connection object description.
Connection Color	Choose a color, in which you want the connection object to be displayed in the **Firewall** - **Connections** window.

Connection Timeout	This general option for all connection types is the timeout for trying to establish a connection. The default value is 30 seconds. Increasing this value can be useful for very protracted connection partners. Decreasing this value can be useful for faster failover mechanisms.
NAT Address	This parameter specifies the Bind IP. The following options are available: • **Proxyfirst | Src NAT - 1st Server IP –** First IP address of server under which firewall service is operating. May be used to restrict the bind address or when policy routing is activated. • **Proxysecond | Src NAT - 2nd Server IP –** Second IP address of server under which firewall service is operating. May be used to restrict the bind address or when policy routing is activated. • **Proxy Dyn | Dynamic Source NAT (default) –** Dynamically chosen according to firewall routing tables. This is a general purpose option. • **Client | No Src NAT –** IP Address of the Client. Source IP = Bind IP. • **Explicit –** Explicitly specified IP address. May be used to restrict the bind address to a specific address. Selecting **Explicit** activates further options below and in section **Firewall Configuration – Service Objects** - **General settings** – section **Failover and Load Balancing**: ◦ **Same Port –** Ticking this checkbox enforces to use the same client port when establishing the connection. This setting has no effect if the **Failover and Loadbalancing policy** is not set to **NONE**. ◦ **Explicit IP –** Here the specific IP address is to be entered. ◦ **Create Proxy ARP –** If the explicitly defined IP address does not exist locally, an appropriate ProxyARP entry may be created by selecting this checkbox. • **From Interface –** Explicitly specified interface. May be used to restrict the bind address to a specific interface. Selecting Interface activates further options below and in section **Firewall configuration – Service Objects** - **General Settings** – section **Failover and Load Balancing**: ◦ **Interface Name –** Here the name of the affected interface is to be entered. • **Translation Table –** Source NAT for a complete subnet. In order to avoid dramatic misconfiguration, the netmask is limited to up to 16 bits. Otherwise, a Proxy ARP with 10.0.0.0/8 would "blank out" the whole internal network for example. If you define a map, you've got to make sure that the source range using this connection is equal or smaller than the map range. If not, the firewall will wrap the larger source net into the smaller bind net. • **Map to Network –** Here the specific mapping network is to be entered. • **Netmask –** Here the corresponding netmask is to be entered. • **Proxy ARP –** This parameter is needed by a router if the addresses live in its local network. For more information, see How to Create Proxy ARP Objects.

The section **Failover and Load Balancing** is only available with parameter **Address Selection** set to **Explicit** or **Interface**.

Failover and Load Balancing

Parameter	Description
Policy	This parameter allows you to specify what should happen if the connection cannot be established. Especially when having multiple providers and policy routing this parameter comes handy because it allows you to specify which IP address/interface has to be used for backup reasons. Otherwise, connecting via the backup provider using the wrong IP address in conjunction with the backup provider would make routing back quite impossible. Available policies are: • **NONE –** (No Fallback or Source Address Cycling) [default setting] Selecting this option deactivates the fallback feature. • **Fallback –** (Fallback to alternative Source Addresses) Causes use of the alternative IP addresses/interfaces specified below. • **SEQ –** (Sequentially Cycle Source Addresses) Causes cycling of the IP addresses/interfaces specified below. • **RAND –** (Randomize Source Addresses) Causes randomized usage of the IP addresses/interfaces specified below.
Alternative/Type	Here up to three Alternative IP addresses or interfaces can be configured for use with the selected policy. Usage of alternative interfaces is recommended when no permanently assigned IP address exists on an interface.
Weight	Assigns a weight number to the IP address or interface. Higher numbers mean higher priority. When performing load balancing, the weight numbers represent the traffic balancing ratio of the available links. A weigh ratio of 40:20:10 means that traffic is balanced over the configured interfaces in a ratio of 4:2:1. Thus the first link will process twice as much traffic as link two and four times as much as link three.

VPN Traffic Intelligence (TI) Settings

Settings configured in this section only apply to Traffic Intelligence configuration in combination with TINA tunnel VPN technology. See Traffic Intelligence for details.

Figures

1. conn_obj.png