How to Create a Custom Connection Object

https://campus.barracuda.com/doc/72516180/

A connection object defines the outgoing interface and source (NAT) IP address for traffic matching the access rule. If an explicit source IP address is specified, the appropriate link will be selected based on the routing table. If the source interface is specified, the corresponding source IP address from a routing table lookup is used.

Create a Connection Object

1. Go to **FIREWALL > Connection Objects**.
2. In the **Connection Objects** section, click **Add Connection Object**.
3. Enter a **Name** for the connection object.
4. Enter a **Description** for your connection object.
5. For **Connection Timeout**, enter the time in seconds to wait for a connection to be established. A lower value means faster failover. Use high values for congested connections to avoid unnecessary failovers. The default value is 30 seconds.
6. From the **Translated Source IP** drop-down list, select the type of NAT to use.
   This setting lets you specify which source IP address and interface are to be used in case of fallback. This is especially important if you are using multiple ISPs. Connecting via the backup provider using the wrong source IP address causes the return traffic routing to fail.
   - **Dynamic NAT** – The firewall uses the routing table to find a suitable interface for routing the packet and uses the IP address of the relevant interface as the new source IP address.
   - **Original Source IP**– The original source IP address of the packet is not changed.
   - **Network Interface** – Source NAT uses the first IP address on a specific interface.
     - Select the interface from the **Interface** list.
   - **Explicit IP** – Uses the IP address that is specified in the **Explicit IP Address** field.
     - Enter the IP address in the **Explicit IP Address** field.
     - If the IP address does not exist locally, select the **Proxy ARP** check box to create an appropriate Proxy ARP entry. Proxy ARP makes it possible for ARP requests to be answered for IP addresses that are not implemented in the firewall.
7. When using **Network Interface** or **Explicit** as **Translated Source IP**, configure the following settings if required:
   - Leave **Use Same Port** unchecked to use Port Address Translation (PAT, also known as NAT overloading). Port Address Translation extends NAT so that port numbers are also translated. Use Port Address Translation to pool several private IP addresses to one public IP address.
8. Click **Save** .

The connection object appears in the **Connection Objects** section.

Failover and Link Load Balancing

You can specify multiple source IP addresses and interfaces in the same connection object. This allows failover or session-based balancing between up to four links. Balancing can be achieved using either a round robin or weighted random algorithm.

1. Go to **FIREWALL > Connection Objects**.
2. In the **Connection Objects** section, click **Add Connection Object**.
3. Enter a **Name** for the connection object.
4. From the **Translated Source IP** list, select either **Explicit IP** (to use the IP address that you specify) or **Network Interface** (to use the IP address of the link).
5. In the **Failover and Load Balancing** section, configure the following settings:
   - **Multilink Policy** – Defines what happens if multiple links are configured. Available policies are:
     - **None** – No fallback or source address cycling. This is not what you want for this object.
     - **Failover** – Falls back to the first alternate address and interface, called Alternate 1. If Alternate 1 fails, fail over to Alternate 2 and so on. When the original link (the one configured in the top section) becomes available, the firewall automatically resumes directing traffic to that interface.
     - **Weighted Round Robin** – Uses the IP addresses and interfaces configured as Alternate 1, 2, and 3, along with this interface, in weighted round robin fashion.
     - **Weighted Random** – Randomly uses one of the available IP addresses and interfaces specified in this object.
   - Specify the following for each of the **Alternate** links:
     - **Translated Source IP** – Select one of these options:
       - **Interface Name** – Source NAT using the first IP address on the interface selected from the **Interface** list.
       - **Explicit IP** – Uses the IP address in the IP address field.
     - **Weight** – Only used for the weighted round robin policy. The weight numbers represent the traffic balancing ratio of the available links. The higher the relative number, the more the link is used. For example, if four links are configured in this object, weight values of 6, 2, 1, and 1 mean that traffic is balanced over the configured interfaces in a ratio of 6:2:1:1. As a result, 60% percent of the traffic passes over Link #1, 20% of the traffic passes over Alternate 1, 10% of the traffic is directed to Alternate 2, and 10% to Alternate 3.
6. Click **Add**.

VPN Traffic Intelligence (TI) Settings

Traffic Intelligence (TI) provides multiple VPN transports with each transport capable of using a

different WAN connection, thereby expanding on the concept of a traditional VPN tunnel with only one VPN transport to one logical VPN tunnel.

1. Go to **FIREWALL > Connection Objects**.
2. In the **Connection Objects** section, click **Add Connection Object**.
3. Enter a **Name** for the connection object.
4. From the **Translated Source IP** list, select either **Explicit IP** (to use the IP address that you specify) or **Network Interface** (to use the IP address of the link).
5. In the **VPN Traffic Intelligence (TI) Settings** section, configure the following settings:
   - **Transport Selection Policy** – Performance-Based Transport Selection selects the optimal transport based on the policy selected in the TI settings of the custom connection object. Only UDP transports with Dynamic Bandwidth and Latency Detection enabled are included in the Performance-Based Transport Selection policy. The transport selections are made from the point of view of the TI master. The following policies are available:
     - **None** – Set this value if you do not want to use TI.
     - **Explicit Transport Selection** – Set this value if you want to configure the further settings individually.
     - **Optimize for Inbound Bandwidth** – Traffic is sent through the VPN transport with the highest available downstream bandwidth for the QoS class from the TI master's point of view. No-delay traffic uses the total bandwidth as the criteria. Standard traffic uses the total bandwidth minus the no-delay traffic to make the decision of which transport to use.
     - **Optimize for Outbound Bandwidth** – Traffic is sent through the VPN transport with the highest available upstream bandwidth for the QoS class from the TI master's point of view. No-delay traffic uses the total bandwidth as the criteria. Standard traffic uses the total bandwidth minus the no-delay traffic to make the decision of which transport to use.
     - **Optimize for Combined Bandwidth** – Traffic is sent through the VPN transport with the highest bandwidth calculated by adding the upstream and downstream bandwidths from the TI master's point of view.
     - **Optimize for Latency** – Traffic is sent through the VPN transport with the lowest latency. If the latency changes, the selected transport is also updated.
   - **TI Learning Policy** – Depending on its role, the firewall (Master) either propagates the TI settings to or (Slave) receives the TI settings from the partner, or (Slave) receives the TI settings from the partner.
   - **Primary Transport Class** – The three VPN transport classes are classified according to their "cost":
     - **Bulk** – For cheap and potentially unreliable connections. Bulk transports are recommended for xDSL or cable WAN connections.
     - **Quality** – For a more reliable line, such as a business-quality Internet line or MPLS links.
     - **Fallback** – For the most expensive lines. Fallback transports are recommended for dial-in lines or WWAN connections.
   - **Secondary Transport ID** – Each VPN transport class is made up of eight class IDs (0 - 7), which define the VPN transport cost in more detail. The class IDs provide you with more

configuration options for creating VPN transports in a single VPN tunnel. A higher metrics indicates a more expensive transport.
- **Further Transports** – Select the transports that are used if the primary and secondary VPN transports fail. Depending on the additional available VPN transports, you can define more than one backup path. Select from the following predefined policies:
  - **First try Cheaper then try Expensive**
  - **Only try Cheaper**
  - **First try Expensive then try Cheaper**
  - **Only try Expensive**
  - **Stay on Transport (no further tries)**
  - **Allow Bulk Transports** – Select the box to allow bulk transports.
  - **Allow Quality Transports** – Select the box to allow quality transports.
  - **Allow Fallback Transports** – Select the box to allow fallback transports.
- **Session Balancing** – Static session balancing can be configured to balance over just the primary and secondary transports or multiple transports in the same TI class based on the TI ID range defined in the connection object.
- **Traffic Duplication** – Select **Yes** to enable copying packets and simultaneously sending them through the selected primary and secondary transport.

After you have successfully created this connection object, you can go to the **FIREWALL > Access Rules** page and apply it to a rule that directs outgoing traffic.

Edit a Connection Object

1. Go to **FIREWALL > Connection Objects**.
2. In the **Actions** column of the **Connection Objects** table, click the edit symbol (✎) for the object that you want to edit.
3. In the **Edit Connection Object** window, edit the settings for the object.
4. Click **Save**.

Delete a Connection Object

1. Go to the **FIREWALL > Connection Objects** page.
2. In the **Connection Objects** table, under **Actions**, click the trash can icon for the object that you want to delete.
3. Click **OK** to delete the connection object.

Example – HTTP and HTTPS Traffic to the Internet

To allow HTTP and HTTPS connections from the local 192.168.200.0/24 network to the Internet, the firewall must perform source-based NAT. Instead of using the source IP address from the client residing in the LAN, the connection is established between the WAN IP address of the firewall and the destination IP address. Reply packets belonging to this session are replaced with the client's IP address within the LAN.

For this example, use the predefined **Default (Source NAT)** connection object. It automatically uses the WAN IP address of the ISP uplink with the lowest metric according to the firewall's routing table.

Figures

1. edit.png