Connection Objects

https://campus.barracuda.com/doc/13304881/

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.

You can use the predefined connection objects or you can create new connection objects.

Create a Connection Object

To create a new connection object:

1. Go to the **FIREWALL > Connection Objects** page.
2. In the **Connection Objects** section, click **Add Connection Object**.
3. Enter a **Name** for the connection object.
4. From the **Nat Type** 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 Source 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.
   - **No Source NAT** – The original source IP address of the packet is not changed.
   - **From Interface** – Source NAT is using the first IP address on a specific interface.
     - Select the interface from the **Interface** list.
   - **Explicit** – 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 Barracuda NextGen Firewall X-Series.
5. When using **From Interface** or **Explicit** as **Nat Type**, configure the following settings if required:
   - Select the **PAT** check box to use Port Address Translation (PAT, also known as NAT overloading). PAT extends NAT so that port numbers are also translated. Use PAT to pool several private IP addresses to one public IP address.
6. 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 the **FIREWALL > Connection Objects** page.
2. In the **Connection Objects** section, click **Add Connection Object**.
3. Enter a **Name** for the connection object.
4. From the **NAT Type** list, select either **Explicit** (to use the IP address that you specify) or **From 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 addresses 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.
        - **Random** – Randomly uses one of the available IP addresses and interfaces specified in this object.
    - Specify the following for each of the alternate links:
        - **NAT Type** – Select one of these options:
            - **Interface** – Source NAT using the first IP address on the interface selected from the **Interface** list.
            - **Explicit** – 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**.

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

Edit a Connection Object

You can edit new connection objects and copies of the predefined connection objects.

To edit a connection object:

1. Go to the **FIREWALL > Connection Objects** page.
2. In the **Connection Objects** table, under **Actions**, 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**.

To edit a predefined connection object:

1. Click the copy symbol next to the object in the **Predefined Connection Objects** table. A copy of the connection object appears in the **Connection Objects** section.
2. Edit the settings for the object.
3. Click **Save**.

Delete a Connection Object

To 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 (SNAT)** connection object. It automatically uses the WAN IP address of the ISP uplink with the lowest metric according to the firewall's routing table.

© 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.