How to Configure an Access Rule for a Client-to-Site VPN

https://campus.barracuda.com/doc/73719155/

To connect your routed client-to-site VPN to your network, you must add a forwarding access rule to direct traffic between the tunnel, the remote, and the home network.

Before You Begin

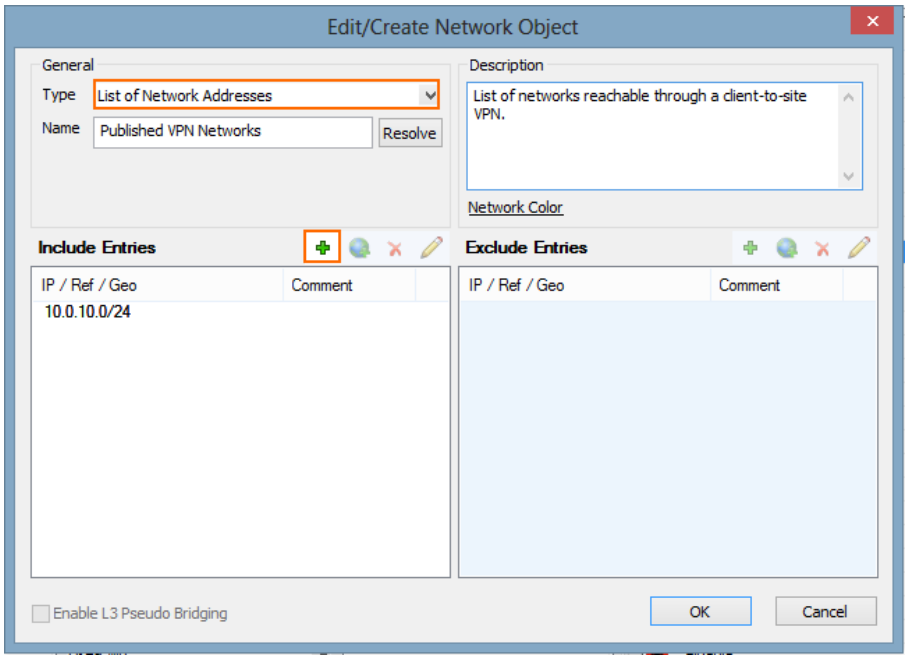
Before creating your forwarding access rules, gather the following information:

- The published VPN network(s).
- The VPN client network(s)

Step 1. Create a Network Object for the Published VPN Networks

Create a static network object for the published VPN networks. If more networks are added to published VPN networks, update the network object to reflect these changes.

- **Type** – Select **List of Network Addresses**.
- **Include Entries** – For each published VPN network, click **+** to add it to the list.

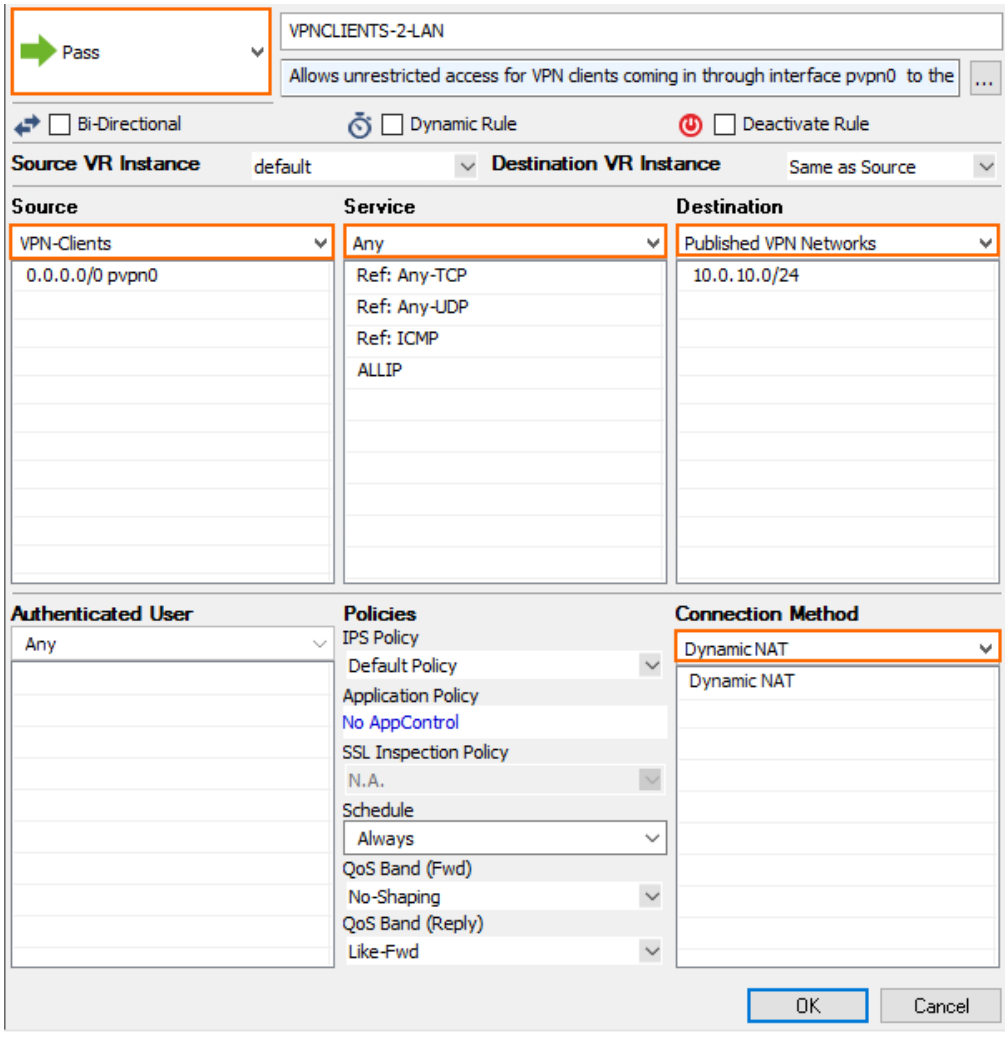


For more information, see Network Objects.

Step 2. Create a Pass Access Rule

Add a Pass access rule that allows traffic from the VPN clients to the published networks.

- **Action** – Select **Pass**.
- **Source** – Select **VPN-Clients**.
- **Service** – Select the allowed services, or **Any** to allow all services.
- **Destination** – Select the network object containing the published VPN networks created in step 1.
- **Connection Method** – Select **Dynamic NAT**.



For more information, see How to Create a Pass Access Rule.

Figures

1. c2s_access_rule_01.png
2. c2s_access_rule_02.png