

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

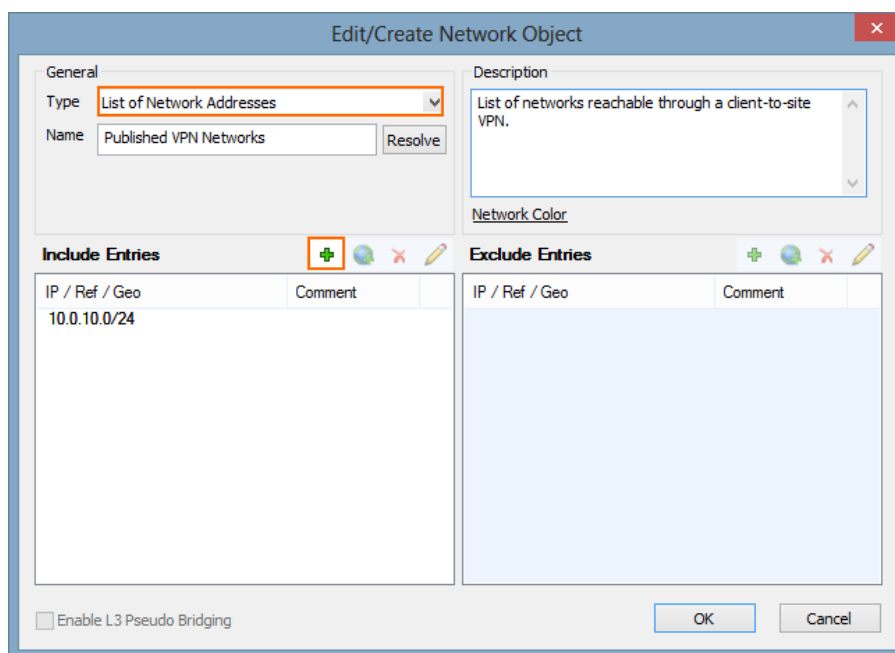
Before creating your forwarding access rules, gather the following information:

- 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.



Edit/Create Network Object

General

Type: **List of Network Addresses**

Name:

Description

Network Color

Include Entries

IP / Ref / Geo	Comment
10.0.10.0/24	

Exclude Entries

IP / Ref / Geo	Comment
----------------	---------

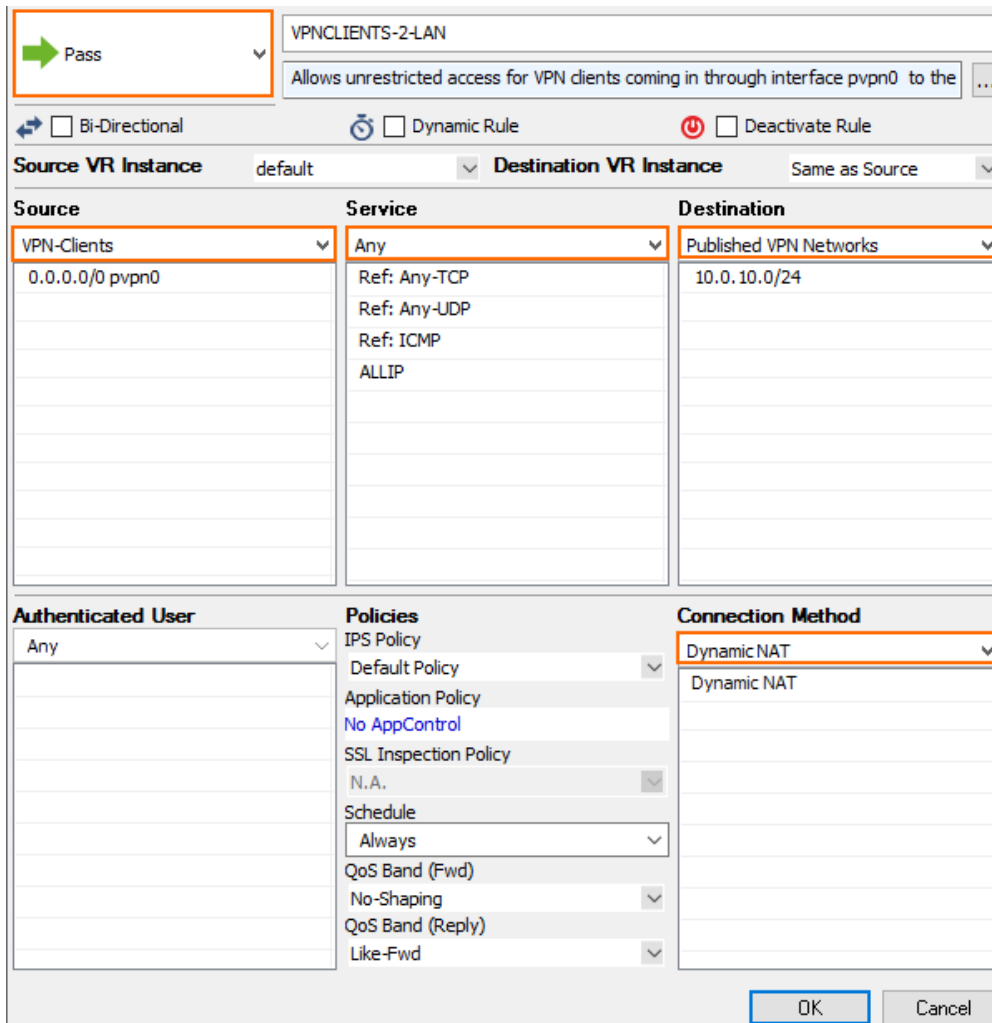
Enable L3 Pseudo Bridging

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**.



The screenshot shows the configuration window for a new access rule. The rule name is "VPNCLIENTS-2-LAN" and the description is "Allows unrestricted access for VPN clients coming in through interface pvpn0 to the ...". The rule is configured with the following settings:

Source	Service	Destination
VPN-Clients 0.0.0.0/0 pvpn0	Any Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Published VPN Networks 10.0.10.0/24

Additional settings include:

- Action:** Pass
- Bi-Directional:**
- Dynamic Rule:**
- Deactivate Rule:**
- Source VR Instance:** default
- Destination VR Instance:** Same as Source
- Authenticated User:** Any
- Policies:**
 - IPS Policy: Default Policy
 - Application Policy: No AppControl
 - SSL Inspection Policy: N.A.
 - Schedule: Always
 - QoS Band (Fwd): No-Shaping
 - QoS Band (Reply): Like-Fwd
- Connection Method:** Dynamic NAT

Buttons for "OK" and "Cancel" are visible at the bottom right.

For more information, see [How to Create a Pass Access Rule](#).

Figures

1. c2s_access_rule_01.png
2. c2s_access_rule_02.png

© Barracuda Networks Inc., 2020 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.