

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

<https://campus.barracuda.com/doc/96026133/>

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

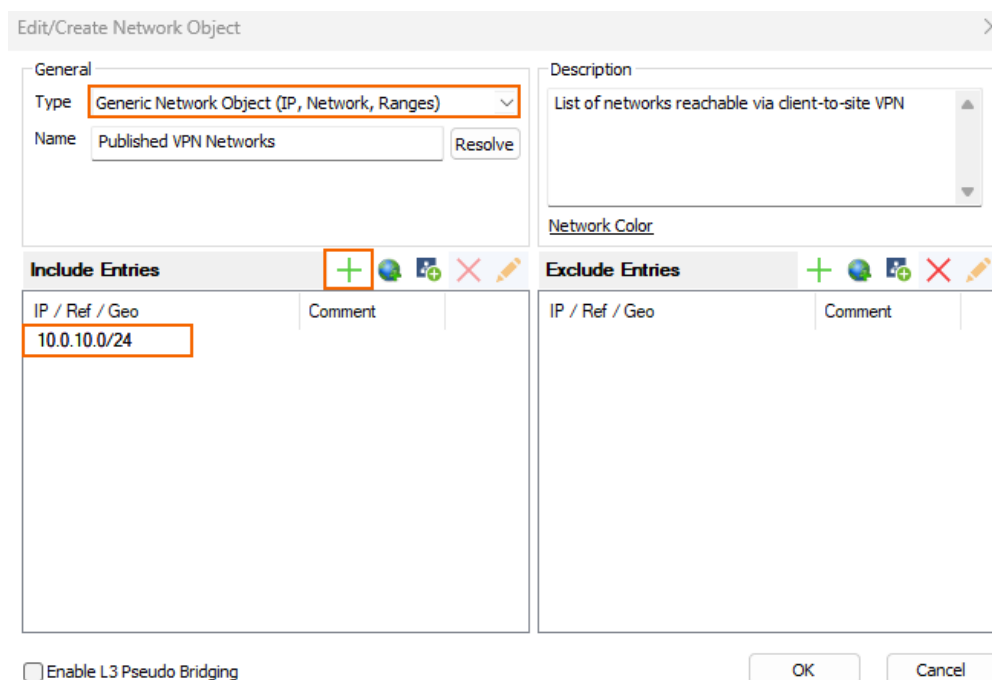
Before creating your forwarding access rules, gather the following information:

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

### Step 1. Create Network Objects

Create static network objects for the published VPN network(s) and the VPN client network(s).

- **Type** – Select **Generic Network Object**.
- **Include Entries** – For each network, click + to add it to the list.



Edit/Create Network Object

General

Type: **Generic Network Object (IP, Network, Ranges)**

Name: Published VPN Networks

Description: List of networks reachable via client-to-site VPN

Network Color

Include Entries

IP / Ref / Geo	Comment
10.0.10.0/24	

Exclude Entries

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

☐ Enable L3 Pseudo Bridging

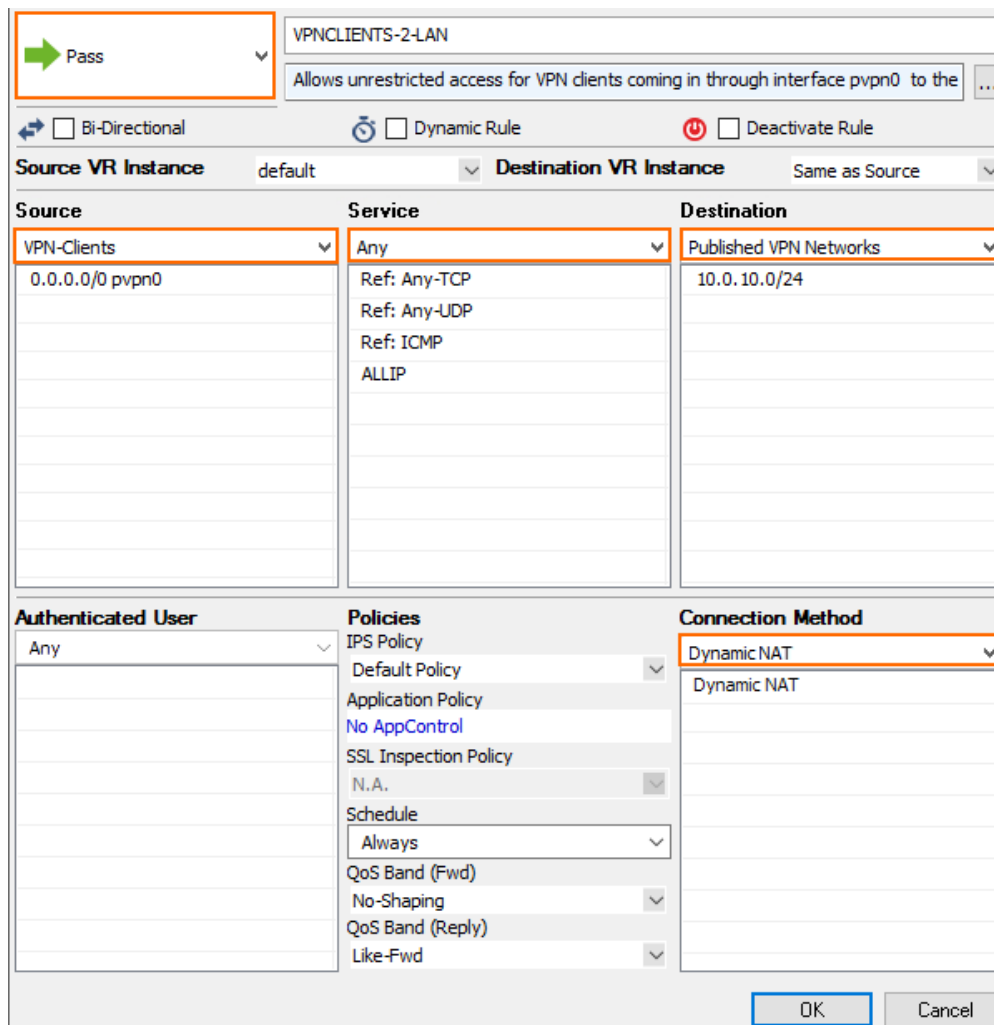
OK Cancel

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 the network object containing the VPN client network(s) created in Step 1.
- **Service** – Select the allowed services, or **Any** to allow all services.
- **Destination** – Select the network object containing the published VPN network(s) 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 as follows:

Source VR Instance	Source	Service	Destination VR Instance	Destination	Authenticated User	Policies	Connection Method
default	VPN-Clients 0.0.0.0/0 pvpn0	Any Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Same as Source	Published VPN Networks 10.0.10.0/24	Any	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	Dynamic NAT Dynamic NAT

Buttons: OK, Cancel

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

## Figures

1. net\_object.png
2. c2s\_access\_rule\_02.png

© 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.