

## How to Configure a Forwarding Firewall Rule for a Client-to-Site VPN

<https://campus.barracuda.com/doc/41116181/>

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

### In this article:

### Before You Begin

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

- The network address for the VPN service (e.g., *10.0.0.2*)
- The VPN client network (e.g., *192.168.6.0/24*)

### Step 1. Create a Static Network Object

Create a static network object for the VPN client network

Type	Name	Include Entries
Generic Network Object (IP, Network, Ranges)	VPNClientNetwork	VPN Client Network (e.g., 192.168.6.0/24)

For more information on how to create Network Objects, see [How to Create Network Objects](#).

### Step 2. Add a Pass Firewall Rule

To give the VPN network range access to the local network, add a [Pass Firewall Rule](#). In the rule, configure the following settings:

- **Source** - The VPN network subnet (e.g., **VPNClientNetwork**).
- **Bi-directional** - Select this check box.
- **Destination** - The local network (e.g., **10.0.0.0/24**).

- **Connection Method** - From this list, select **No Src NAT [Client]**.

© 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.