

How to Create Access Rules for Site-to-Site VPN Access

<https://campus.barracuda.com/doc/79462879/>

After configuring a VPN tunnel between two Barracuda CloudGen Firewalls, you must create a Pass access rule on both systems to allow traffic through the VPN tunnel.

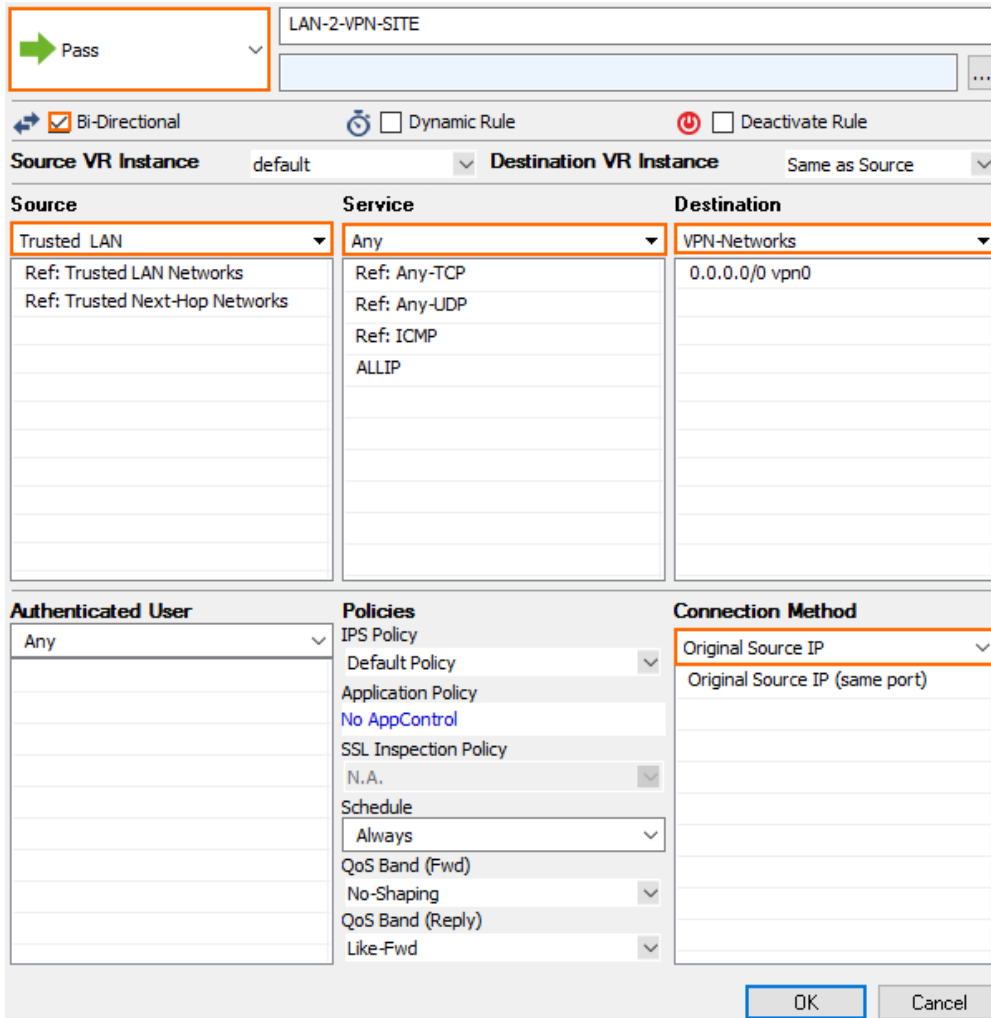
Create this access rule on both local and remote CloudGen Firewalls.

Before You Begin

- Configure a TINA or IPsec Site-to-Site VPN tunnel. For more information, see [How to Create a TINA VPN Tunnel between CloudGen Firewalls](#) or [How to Configure a Site-to-Site VPN with IPsec](#).

Create an Access Rule Allowing Traffic in and out of the VPN Tunnels

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Right click on the ruleset and select **New**. The **New Rule** window opens.
4. Enter a **Name**. E.g., LAN-2-VPN-SITE
5. Right-click the rule set and select **New > Rule** to create an access rule to match the VPN traffic:
 - **Action** - Select **Pass**.
 - **Bi-Directional** - Select the check box to apply the rule in both directions.
 - **Source** - Enter all local networks used for the VPN tunnel.
 - **Service** - Select the services allowed to access the tunnel. Default: **Any**
 - **Destination** - Enter the remote networks behind the VPN tunnel, or select **VPN_Networks**.
 - **Connection Method** - Select **Original Source IP**.



LAN-2-VPN-SITE

Pass

Bi-Directional
 Dynamic Rule
 Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source

Source	Service	Destination
Trusted LAN	Any	VPN-Networks
Ref: Trusted LAN Networks	Ref: Any-TCP	0.0.0.0/0 vpn0
Ref: Trusted Next-Hop Networks	Ref: Any-UDP	
	Ref: ICMP	
	ALLIP	

Authenticated User	Policies	Connection Method
Any	IPS Policy	Original Source IP
	Default Policy	Original Source IP (same port)
	Application Policy	
	No AppControl	
	SSL Inspection Policy	
	N.A.	
	Schedule	
	Always	
	QoS Band (Fwd)	
	No-Shaping	
	QoS Band (Reply)	
	Like-Fwd	

OK Cancel

6. Click **OK**.
7. Reorder the access rule by dragging it to the correct position in the forward firewall's ruleset. Make sure no access rule placed above it will match the traffic for the site-to-site access rule.
8. Click **Send Changes** and **Activate**.

Figures

1. VPN_Access_rule01.png

© Barracuda Networks Inc., 2019 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.