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

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

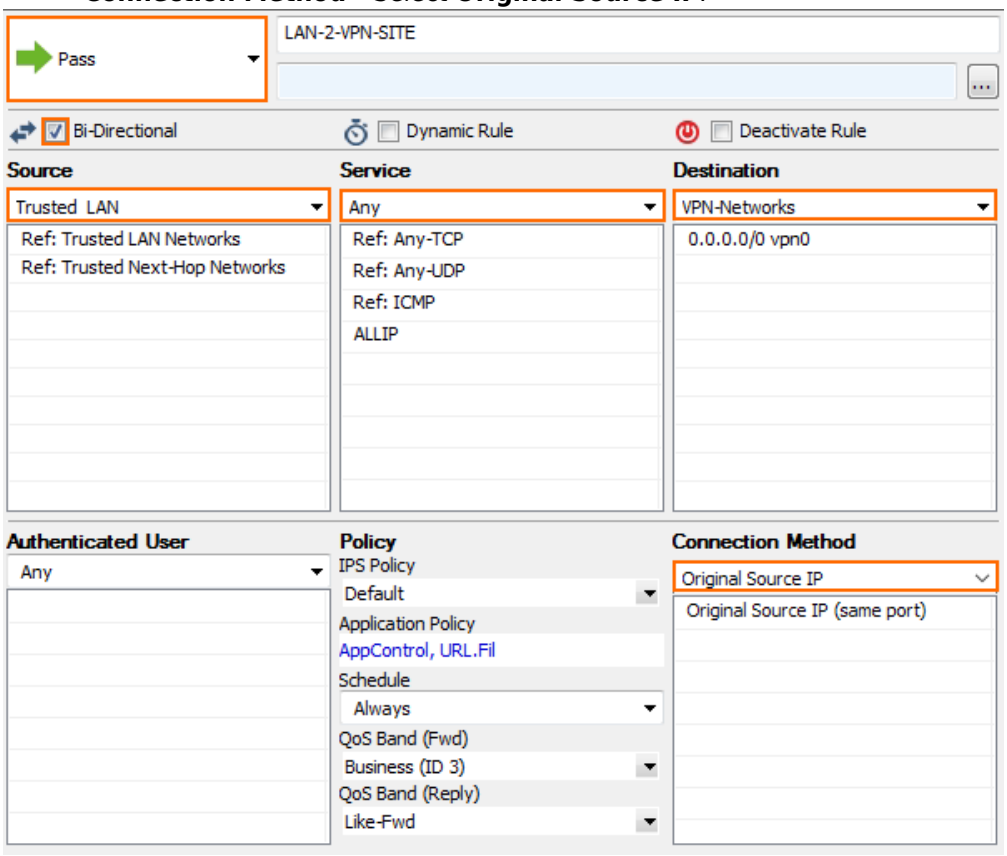
Create this access rule on both local and remote F-Series Firewalls.

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 F-Series 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. From the **Edit Rule** menu in the left menu, click **New**. The **New Rule** window opens.
4. Enter a **Name** E.g., `LAN-2-VPN-SITE`
5. In the **New Rule** window, configure the settings to allow traffic between both systems:
   - **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**.



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