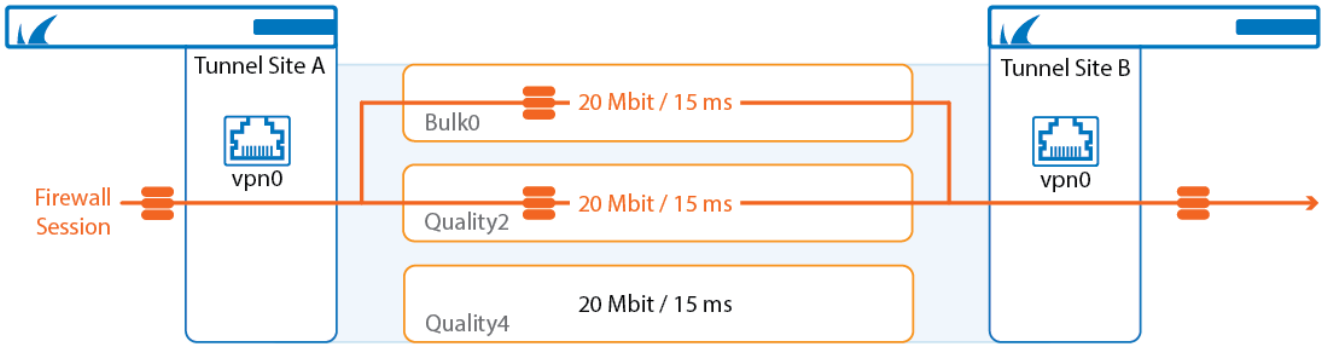
How to Configure Traffic Duplication for VPN Tunnels with SD-WAN

https://campus.barracuda.com/doc/96026180/

Traffic Duplication copies packets and sends them over the primary and secondary transport simultaneously to ensure that traffic continues uninterrupted even if one VPN transport goes down. At the other VPN endpoint, the packet stream is reassembled. Traffic Duplication should be used only for critical, real-time traffic using two transports with the same latency and bandwidth.



Limitations

- Not available for transports using IPv6 VPN envelopes.
- Latency (Round Trip Time) and bandwidth must be identical for both transports.

Before You Begin

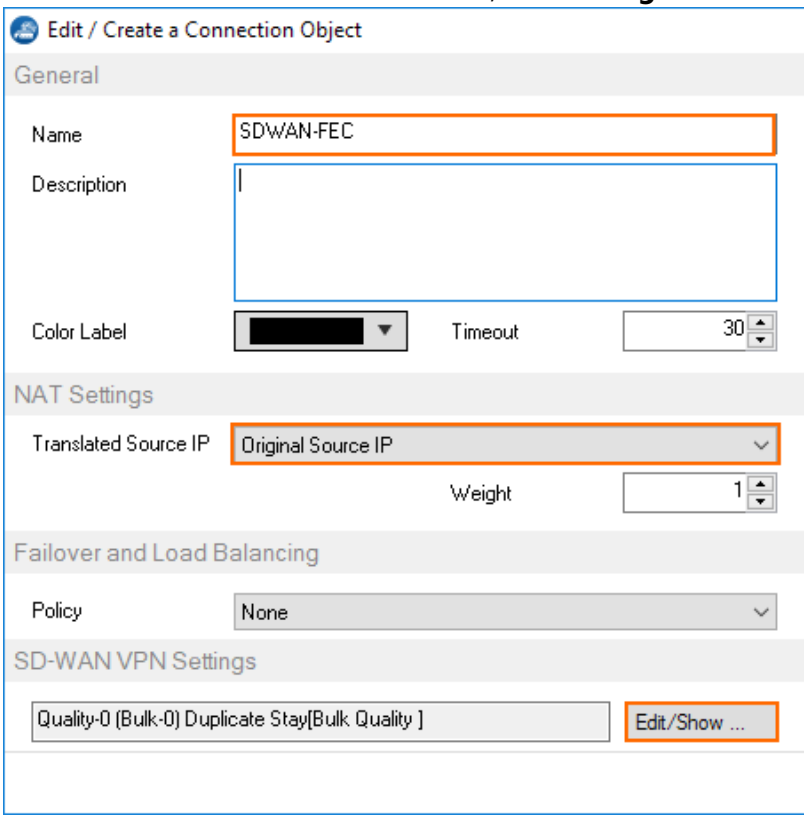
Create a multi-transport VPN tunnel between two CloudGen Firewalls:

- Create a TINA site-to-site VPN tunnel. For more information, see How to Create a TINA VPN Tunnel between CloudGen Firewalls or How to Create a VPN Tunnel with the VPN GTI Editor.
- Add one or more additional transports to the VPN tunnel. For more information, see How to Add a VPN Transport to a TINA VPN Tunnel with Explicit Transport Selection or How to Configure SD-WAN Using the VPN GTI Editor.

Step 1. Create a Custom Connection Object for the SD-WAN Primary

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.

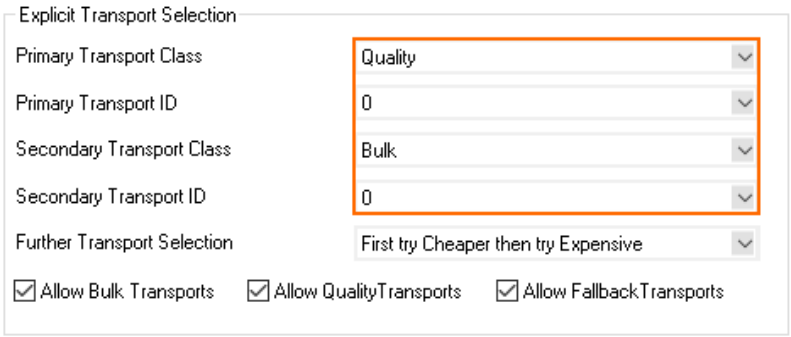
2. In the left menu, click **Connections**.
3. Right-click the table and select **New Connection**. The **Edit/Create a Connection Object** window opens.
4. Enter the **Name**.
5. From the **Translated Source IP** list, select **Original Source IP**.



6. To edit the **SD-WAN VPN** settings, click **Edit/Show** . The **SD-WAN Settings** window opens.
7. Configure the **Transport Policies**:
   - **Transport Selection Policy** – Select **Explicit Transport Selection**.
   - **SD-WAN Learning Policy** – Select **Primary**.



8. Configure the **Explicit Transport Selection**:
   - **Primary Transport Class** – Select the primary transport.
   - **Primary Transport ID** – Select the ID for the primary transport.
   - **Secondary Transport Class** – Select the secondary transport.
   - **Secondary Transport ID** – S elect the ID for the secondary transport.
9. From the **Traffic Duplication (FEC)** list, select **Yes**.

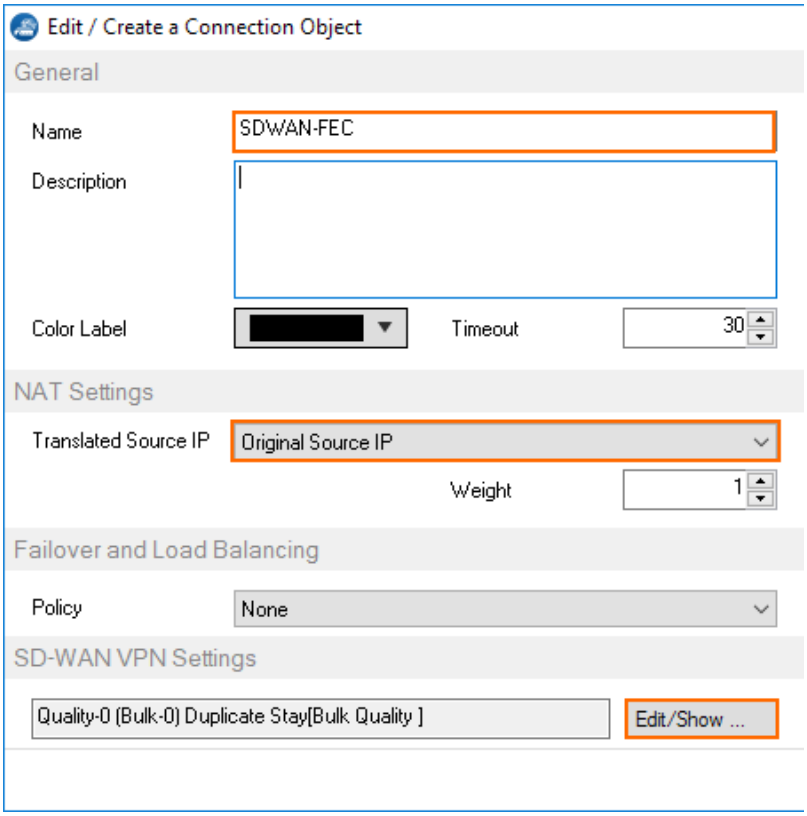




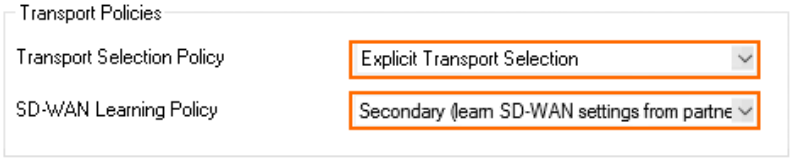
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

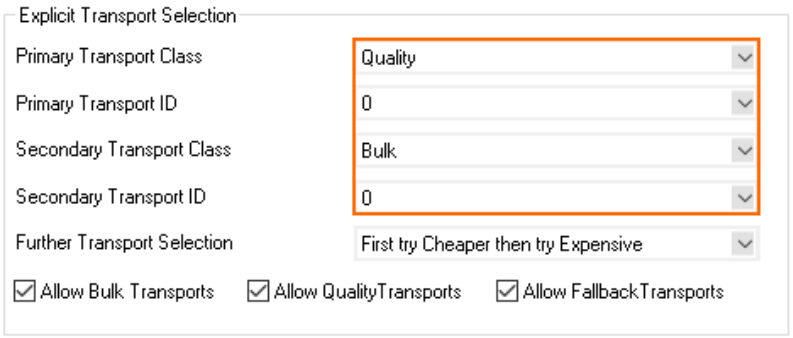
Step 3. Create a Custom Connection Object for the SD-WAN Secondary

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Right-click the table and select **New Connection**. The **Edit/Create a Connection Object** window opens.
4. Enter the **Name**.
5. From the **Translated Source IP** list, select **Original Source IP**.



6. To edit the **SD-WAN VPN** settings, click **Edit/Show**. The **SD-WAN Settings** window opens.
7. From the **SD-WAN Learning Policy** drop-down list, select **Secondary**.



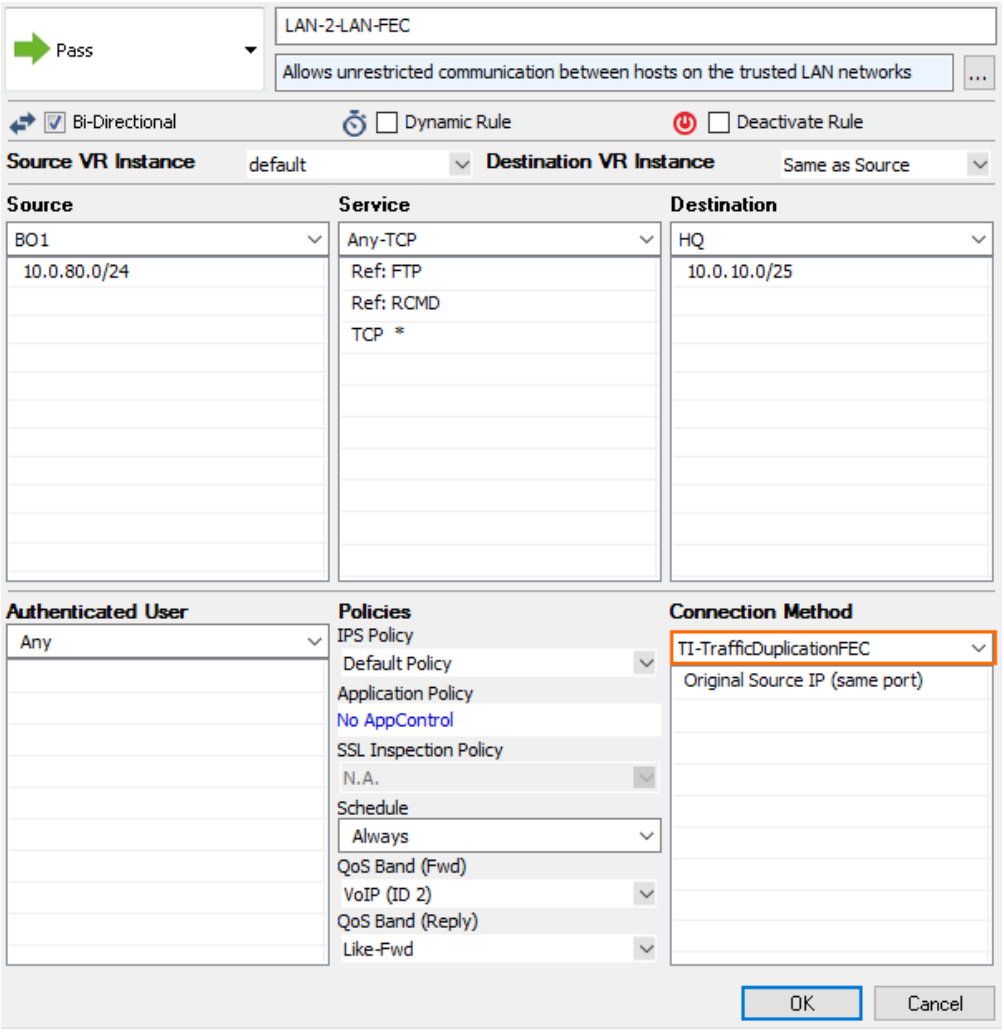




8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 4. Modify Access Rule on the Firewall Acting as SD-WAN Primary

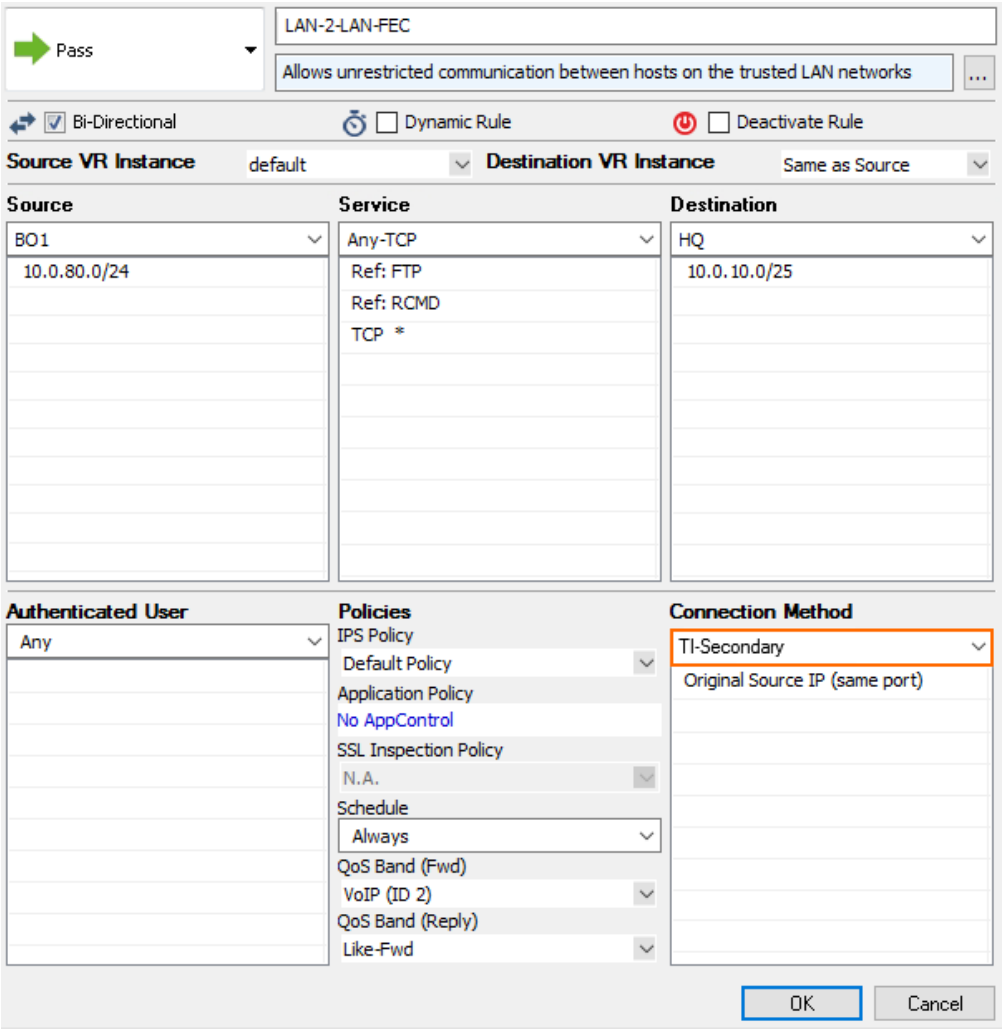
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Right-click the ruleset and select **New > Rule** to create an access rule to match the VPN traffic you want to balance:
   - **Action** – Select **Pass**.
   - **Bi-Directional** – Select the check box to apply the rule in both directions.
   - **Source** – Select a network object for all local networks.
   - **Service** – Select a service object from the list.
   - **Destination** – Select the network object containing the remote networks.
   - **Connection Method** – Select the connection object for the SD-WAN primary created in Step 2.



4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Step 5. Modify Access Rule on the Firewall Acting as SD-WAN Secondary

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Right-click the ruleset and select **New > Rule** to create an access rule to match the VPN traffic you want to balance:
   - **Action** – Select **Pass**.
   - **Bi-Directional** – Select the check box to apply the rule in both directions.
   - **Source** – Select a network object for all local networks.
   - **Service** – Select a service object from the list.
   - **Destination** – Select the network object containing the remote networks.
   - **Connection Method** – Select the connection object for the SD-WAN secondary created in Step 3.



4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Traffic matching these access rules is now duplicated on the primary and secondary transport. Failure of one of the transports is completely transparent and no packet is dropped. In the **VPN** tab, Traffic Duplication is not visualized. Traffic Duplication can be tested very easily by disabling one transport. If traffic fails over instantly with no packets dropped and with no delay, Traffic Duplication is working correctly.

Figures

1. ti_traffic_replication.png
2. sdwan_FEC_01.png
3. sdwan_FEC_01a.png
4. sdwan_FEC_01b.png
5. sdwan_FEC_01.png
6. sdwan_FEC_03.png
7. sdwan_FEC_04a.png
8. sdwan_FEC_04.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.