
How to Configure Packet-Based Balancing for VPN Tunnels with Traffic Intelligence

<https://campus.barracuda.com/doc/70582463/>

Packet-Based Balancing distributes traffic on a per-packet basis over multiple VPN transports in the same transport class. VPN transports using Packet-Based Balancing must have the same bandwidth and latency. In most cases, using Adaptive Session Balancing is preferable to Packet-Based Balancing because it allows for different link-quality requirements.

Limitations

- VPN transports must be in the same transport class.
- WAN links must have the same bandwidth and latency. For example: multiple identical WAN links from the same ISP.

Before You Begin

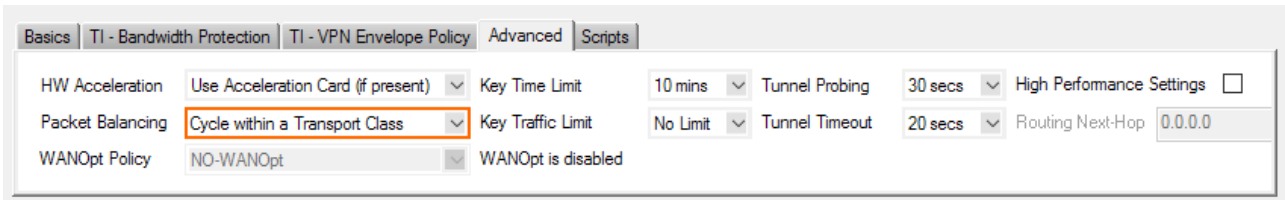
Create a multi-transport VPN tunnel between two F-Series Firewalls:

- Create a TINA site-to-site VPN tunnel. For more information, see [How to Create a TINA VPN Tunnel between F-Series Firewalls](#) or [How to Create a VPN Tunnel with the VPN GTI Editor](#).
- Add one or more additional transports in the same TI class to the VPN tunnel. For more information, see [How to Add a VPN Transport to a TINA VPN Tunnel](#) or [How to Configure Traffic Intelligence Using the VPN GTI Editor](#).

Step 1. Enable Packet-Based Balancing

Packet-Based Balancing must be enabled for all transports in the transport class.

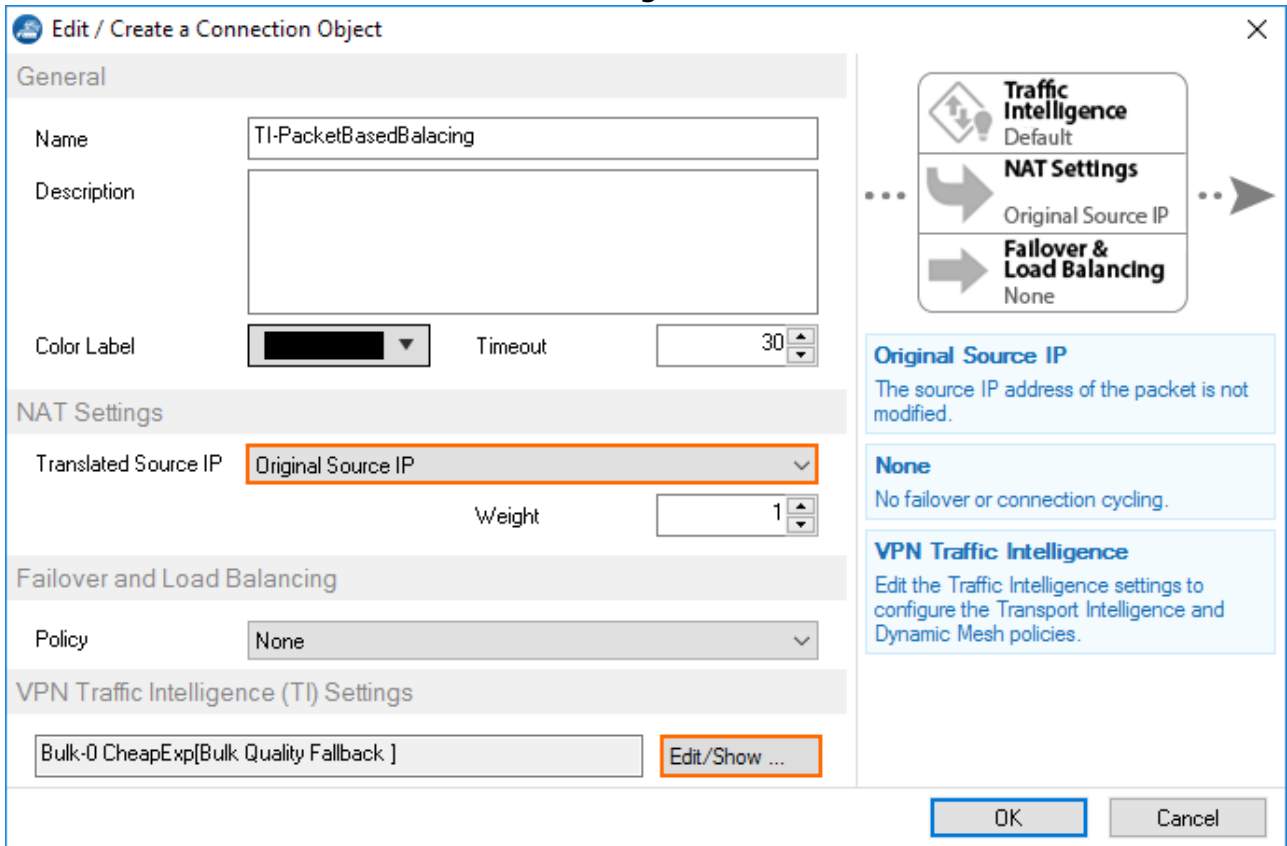
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > Assigned Services > VPN Service > Site to Site VPN**.
2. Click **Lock**.
3. Double-click the TINA VPN tunnel. The **TINA Tunnel** window opens.
4. Click the **Advanced** tab.
5. From the **Packet Balancing** list, select **Cycle within a Transport Class**.



6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 2. Create a Custom Connection Object for the TI Master

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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 a **Name**
5. From the **Translated Source IP** list, select **Original Source IP**.



6. To edit the **VPN Traffic Intelligence** settings, click **Edit/Show**. The **TI Transport Selection** window opens.
7. From the **TI Learning Policy** list, select **Master**.

Transport Policies

Transport Selection Policy	Explicit Transport Selection
TI Learning Policy	Master (propagate TI settings to partner)

- From the **Primary Transport Class** list, select the primary transport class.
- From the **Primary Transport ID** list, select the ID for the primary transport.

Explicit Transport Selection

Primary Transport Class	Quality
Primary Transport ID	0
Secondary Transport Class	Bulk
Secondary Transport ID	0
Further Transport Selection	First try Cheaper then try Expensive

Allow Bulk Transports
 Allow Quality Transports
 Allow Fallback Transports

- From the **Secondary Transport Class** list, select the same transport class used for the primary transport.
- From the **Secondary Transport ID** list, select the ID for the secondary transport.

Explicit Transport Selection

Primary Transport Class	Quality
Primary Transport ID	0
Secondary Transport Class	Bulk
Secondary Transport ID	0
Further Transport Selection	First try Cheaper then try Expensive

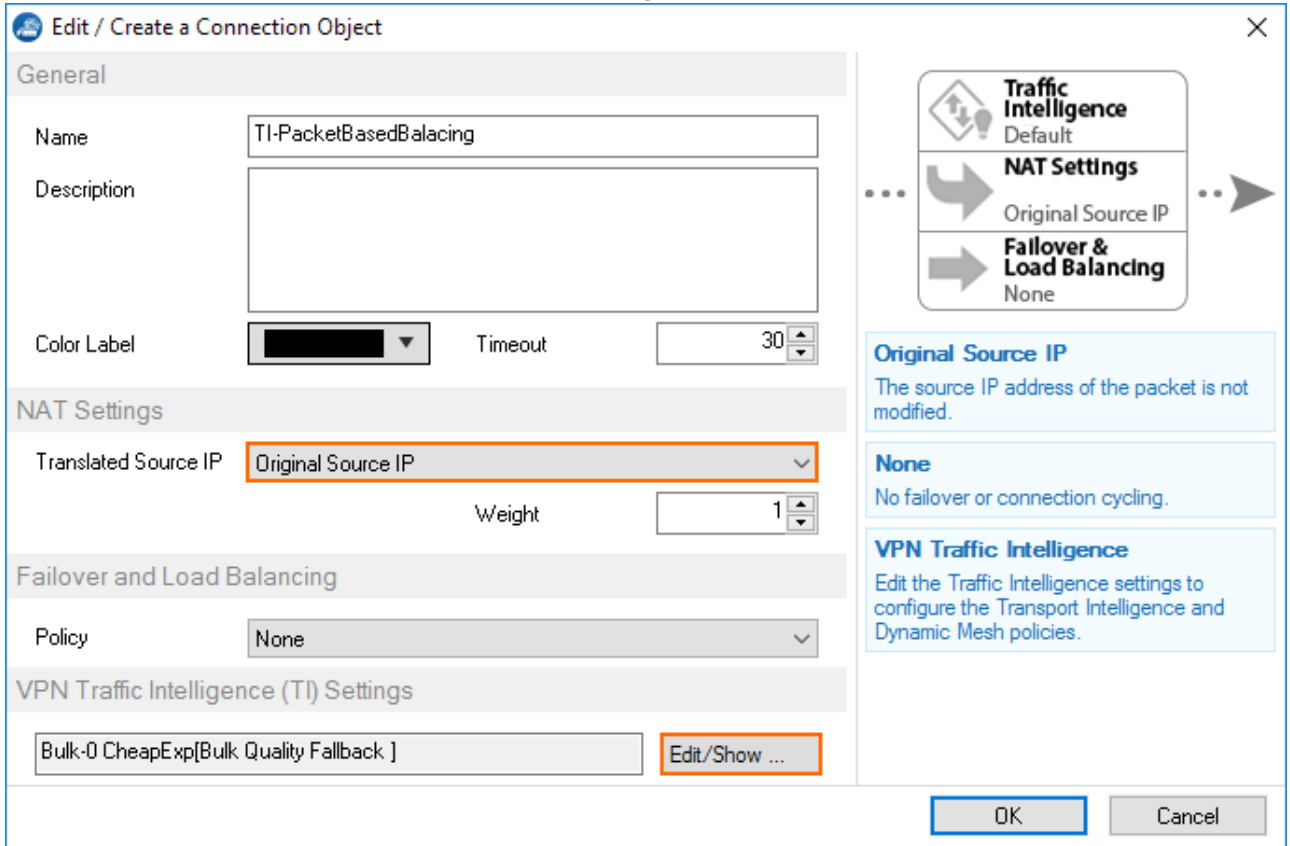
Allow Bulk Transports
 Allow Quality Transports
 Allow Fallback Transports

- Click **OK**.
- Click **Send Changes** and **Activate**.

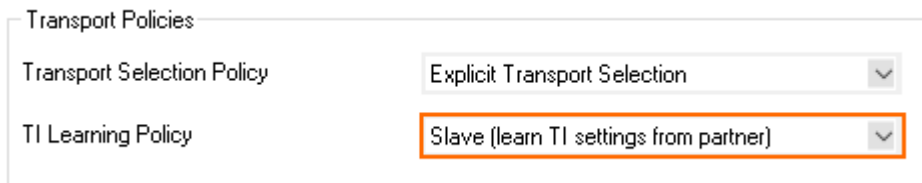
Step 3. Create a Custom Connection Object for the TI Slave

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
- In the left menu, click **Connections**.
- Right-click the table and select **New Connection**. The **Edit/Create a Connection Object** window opens.
- Enter a **Name**.

5. From the **Translated Source IP** list, select **Original Source IP**.



6. To edit the **VPN Traffic Intelligence** settings, click **Edit/Show**. The **TI Transport Selection** window opens.
7. From the **TI Learning Policy** drop-down list, select **Slave**.

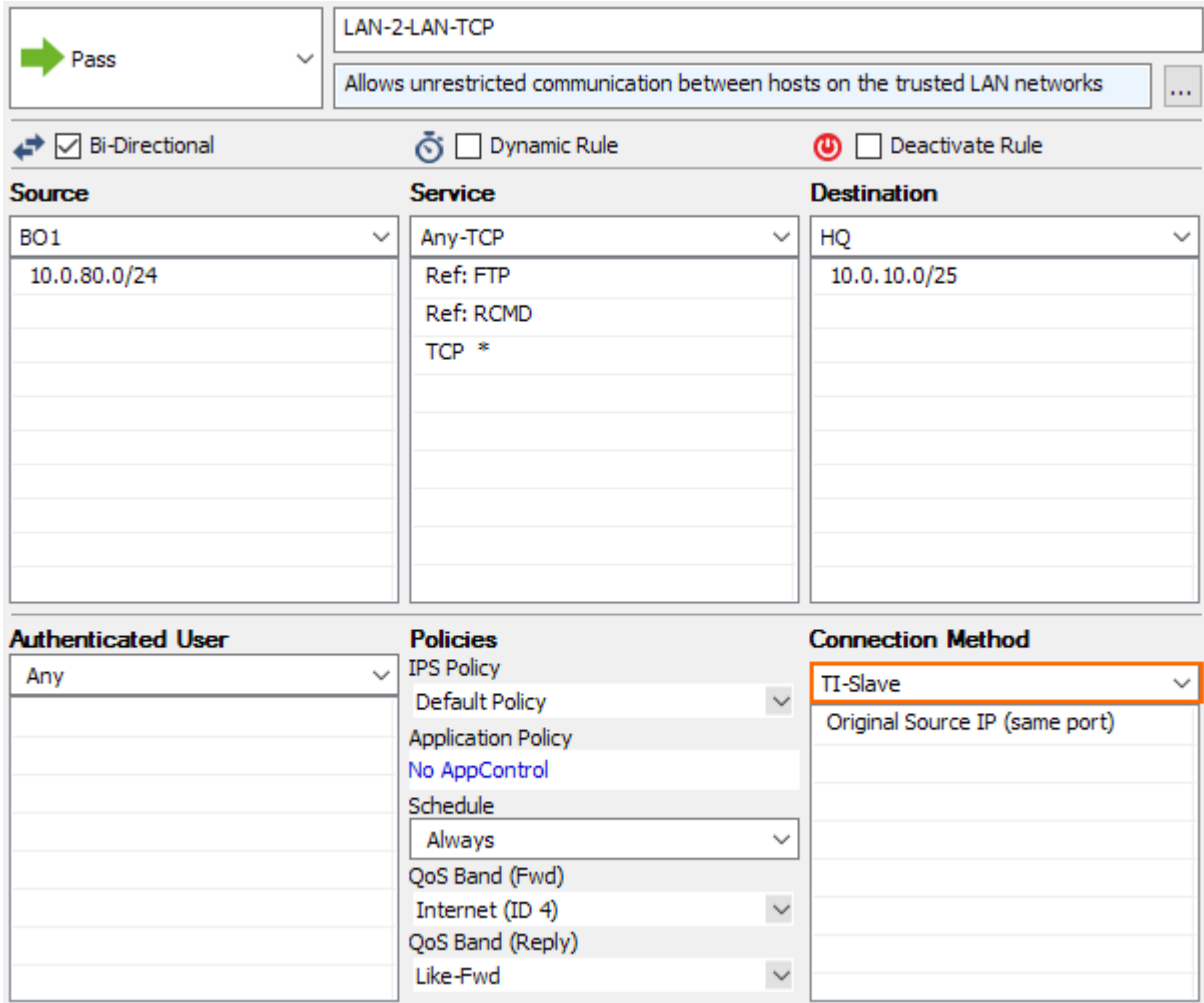


8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 4. Modify Access Rule on the Firewall Acting as TI Master

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
- Click **Lock**.
- 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 TI master created in step 2.



Pass

LAN-2-LAN-TCP

Allows unrestricted communication between hosts on the trusted LAN networks

Bi-Directional
 Dynamic Rule
 Deactivate Rule

Source	Service	Destination
BO1 10.0.80.0/24	Any-TCP Ref: FTP Ref: RCMD TCP *	HQ 10.0.10.0/25

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Policy Application Policy No AppControl Schedule Always QoS Band (Fwd) Internet (ID 4) QoS Band (Reply) Like-Fwd	TI-Slave Original Source IP (same port)

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

Step 5. Modify Access Rule on the Firewall Acting as TI Slave

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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 TI slave created in step 3.

<input type="checkbox"/> Pass		LAN-2-LAN-TCP Allows unrestricted communication between hosts on the trusted LAN networks	
<input checked="" type="checkbox"/> Bi-Directional		<input type="checkbox"/> Dynamic Rule	
		<input type="checkbox"/> Deactivate Rule	
Source	Service	Destination	
BO1 10.0.80.0/24	Any-TCP Ref: FTP Ref: RCMD TCP *	HQ 10.0.10.0/25	
Authenticated User	Policies	Connection Method	
Any	IPS Policy Default Policy Application Policy No AppControl Schedule Always QoS Band (Fwd) Internet (ID 4) QoS Band (Reply) Like-Fwd	TI-Slave Original Source IP (same port)	

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

Traffic matching these access rules and using the VPN transports are now balanced per packet within the transport class.

Figures

1. TI_packet_balacing_01.png
2. TI_packet_balacing_02.png
3. TI_session_balacing_01a.png
4. TI_session_balacing_01b.png
5. TI_session_balacing_01c.png
6. TI_packet_balacing_02.png
7. TI_session_balacing_01e.png
8. TI_packet_balacing_05.png
9. TI_packet_balacing_05.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.