

How to Configure Session Balancing for VPN Tunnels with Traffic Intelligence

<https://campus.barracuda.com/doc/70582461/>

Session-based balancing for multi-transport TINA VPN tunnels is enabled per access rule in the Traffic Intelligence (TI) settings of the custom connection object. Session balancing can use a static round robin or an adaptive weighted round robin balancing policy:

- **(Static) Session Balancing** – Sessions are distributed over the configured transports by using a round-robin style balancing policy. If used without adaptive balancing, it is recommended to use transports of similar bandwidth and latency. Static balancing is available for all transport protocols. Static session balancing can be configured to balance over multiple transports in the same TI class based on the defined TI ID range.
- **Adaptive Session Balancing** – All sessions are initially balanced statically over the primary and secondary transports. Link quality metrics gathered by Dynamic Bandwidth and Latency Detection are then used to rebalance sessions with lifetimes over 5 seconds to use the optimal transport. Shorter sessions are not rebalanced. Adaptive session balancing is available only on UDP transports. It is not possible to use session balancing with all transports in a class.

Before You Begin

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

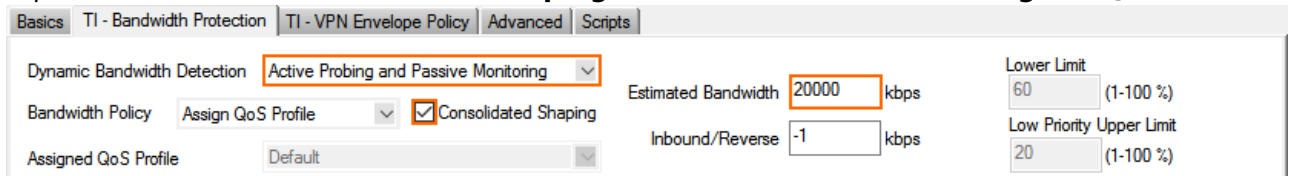
- Create a TINA site-to-site VPN tunnel. For more information, see [How to Create a TINA VPN Tunnel between F-Series Firewalls](#) or [How to Create a VPN Tunnel with the VPN GTI Editor](#).
- Add one or more additional transports to the VPN tunnel. For more information, see [How to Add a VPN Transport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

Step 1. (Adaptive Session Balancing only) Enable Dynamic Bandwidth and Latency Detection for the VPN Transports

On both VPN endpoints, edit the TINA site-to-site VPN tunnel to enable Dynamic Bandwidth and Latency Detection.

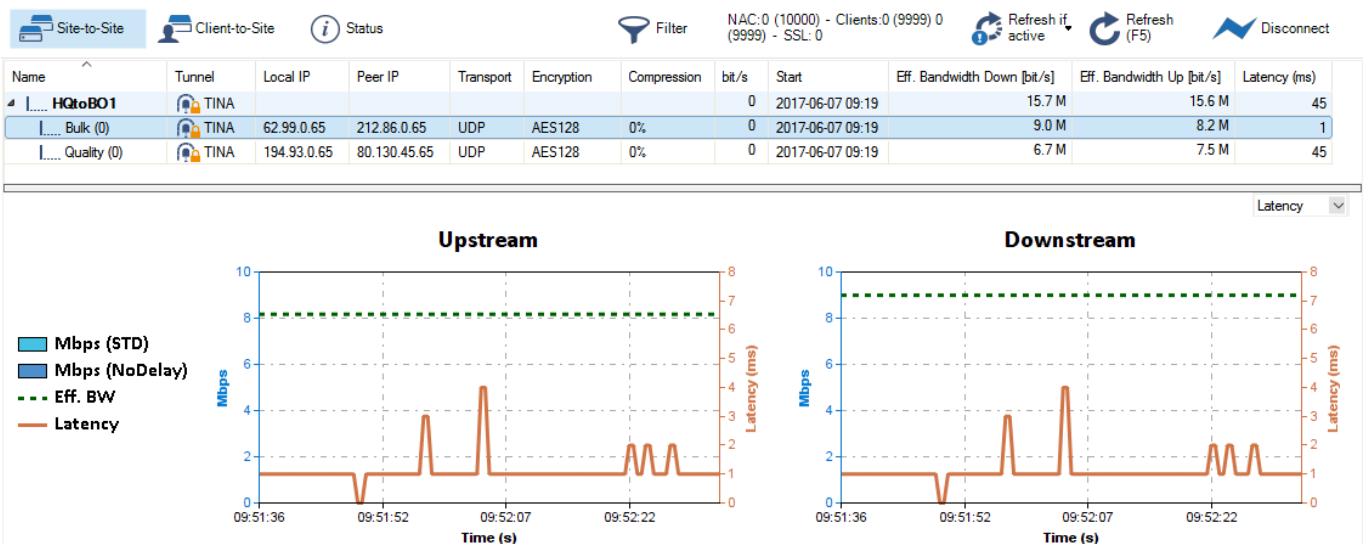
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > Assigned Services > VPN Service > Site to Site VPN**.
2. Click **Lock**.
3. Double-click the TINA VPN tunnel. The **TINA Tunnel** window opens.
4. Click the **TI - Bandwidth Protection** tab.

5. From the **Dynamic Bandwidth Detection** list, select the policy:
 - o **Active Probing and Passive Monitoring**
 - o **Active Probing Only**
 - o **No Probing - use Estimated Bandwidth**
6. Enter the **Estimated Bandwidth** bandwidth.
7. (optional) Select the **Consolidated Shaping** check box and select the **Assigned QoS Profile**.



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

To verify that Dynamic Bandwidth and Latency Detection is running, go to **VPN > Site-to-Site**. Right-click the transport and select **Monitor Traffic**.

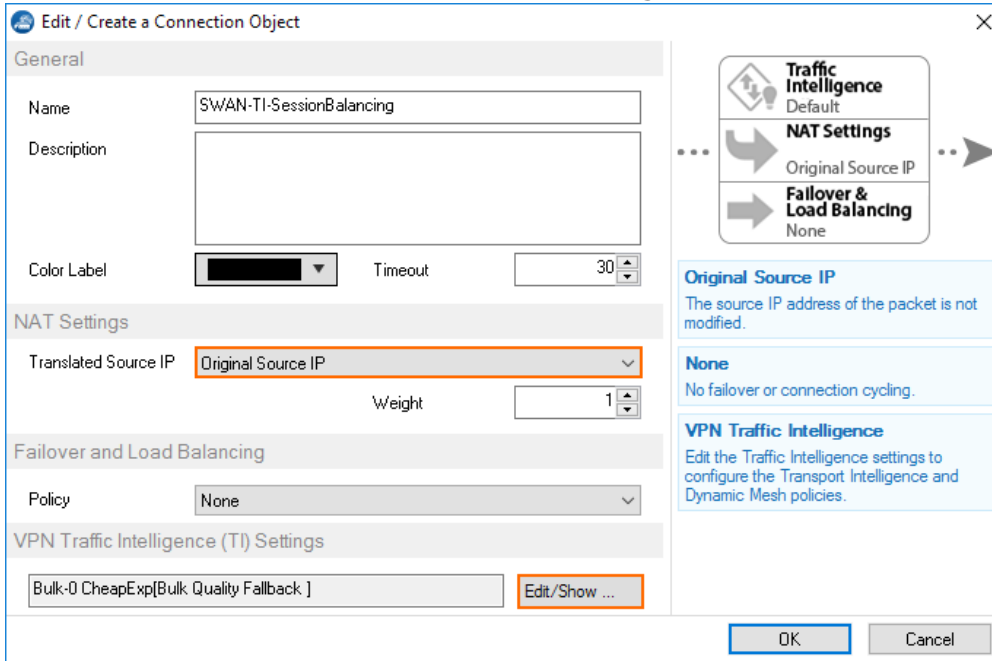


Step 2. Create a Custom Connection Object for the TI Master

Configure session balancing with explicit transport selection. You can balance between the primary and secondary transport, or over multiple IDs of the primary transport class.

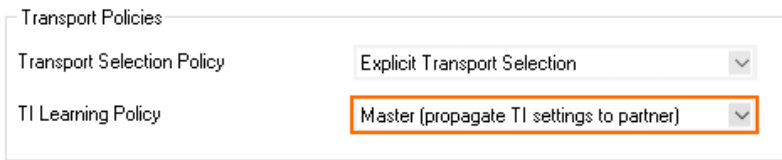
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Right-click the table and select **New Connection**. The **Edit/Create a Connection Object** window opens.
4. In the **Name** field, enter a name for the connection object.

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



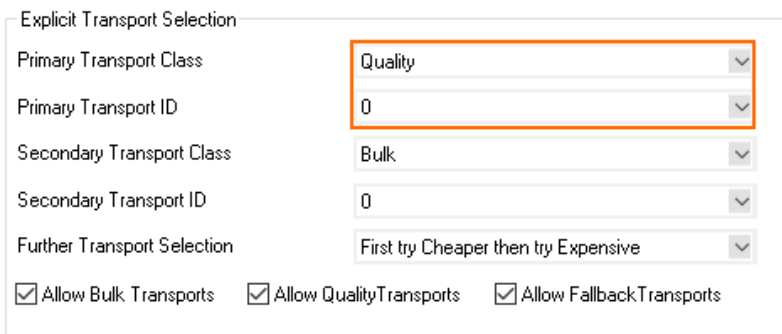
6. To edit the **VPN Traffic Intelligence** settings, click **Edit/Show**. The **TI Transport Selection** window opens.

7. From the **TI Learning Policy** drop-down list, select **Master**.



8. Configure the primary transport class and ID:

- o **Primary Transport Class** - Select the TI class of the primary transport.
- o **Primary Transport ID** - Select the ID for the primary transport.



9. (Balancing between primary and secondary transports only) Configure the secondary transport class and ID:

- o **Secondary Transport Class** - Select the TI class secondary transport.
- o **Secondary Transport ID** - 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

10. In the **Simultaneous Transport Usage** section, select the **Session Balancing** policy:
- o **None** – Disable session balancing.
 - o **between Primary and Secondary Transport** – Sessions are balanced between the primary and secondary transport. Select this option for adaptive balancing.
 - o **(static session balancing only) from ID=0 to ID=X** – Sessions are balanced between all available transports in the TI class of the primary transport with a TI ID in this range.

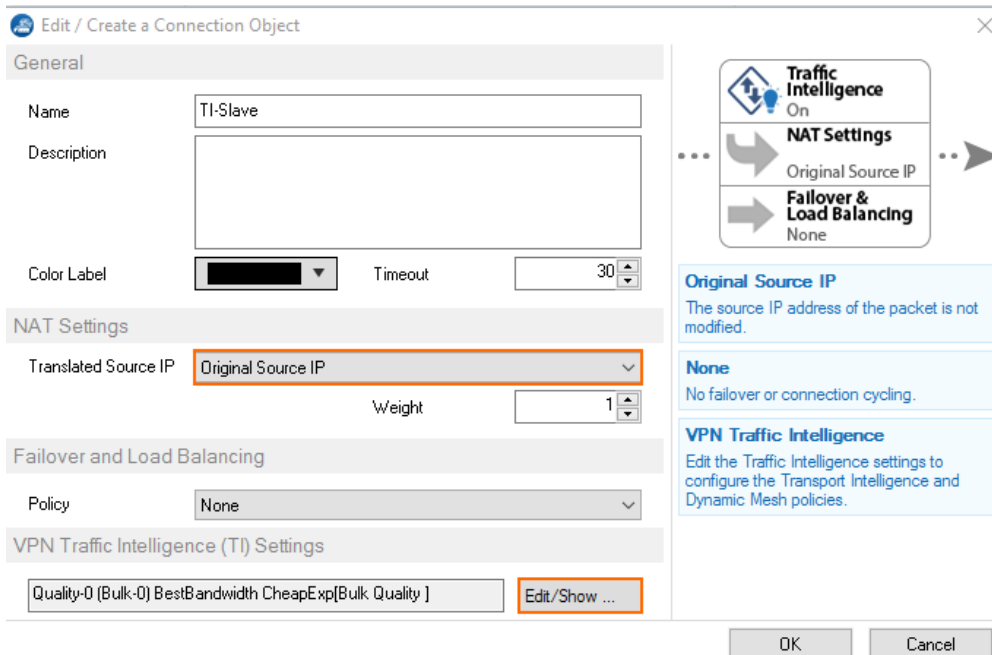
Simultaneous Transport Usage

Session Balancing	between Primary and Secondary Transport
Traffic Duplication	No

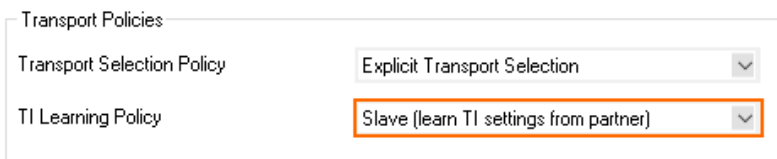
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

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

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** 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

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:
 - o **Action** – Select **Pass**.
 - o **Bi-Directional** – Select the check box to apply the rule in both directions.
 - o **Source** – Select a network object for all local networks.
 - o **Service**– Select a service object from the list.
 - o **Destination** – Select the network object containing the remote networks
 - o **Connection Method** – Select the connection object for the TI Master created in step 2.

<div style="display: flex; justify-content: space-between;"> Pass LAN-2-LAN-UDP </div> <div style="border: 1px solid gray; padding: 2px;">Allows unrestricted communication between hosts on the trusted LAN networks</div>		
<div style="display: flex; justify-content: space-between;"> <input checked="" type="checkbox"/> Bi-Directional <input type="checkbox"/> Dynamic Rule <input type="checkbox"/> Deactivate Rule </div>		
Source BO1 10.0.80.0/24	Service <explicit-srv> UDP *	Destination HQ 10.0.10.0/25
Authenticated User Any	Policies IPS Policy Default Policy Application Policy No AppControl Schedule Always QoS Band (Fwd) VoIP (ID 2) QoS Band (Reply) Like-Fwd	Connection Method TI-SessionBalancing Original Source IP (same port)
<div style="display: flex; justify-content: flex-end; gap: 10px;"> OK Cancel </div>		

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:
 - o **Action** – Select **Pass**.
 - o **Bi-Directional** – Select the check box to apply the rule in both directions.
 - o **Source** – Select a network object for all local networks.
 - o **Service** – Select a service object from the list.
 - o **Destination** – Select the network object containing the remote networks
 - o **Connection Method** – Select the connection object for the TI Slave created in step 3.

<div style="display: flex; justify-content: space-between;"> Pass LAN-2-LAN-UDP </div> <div style="border: 1px solid gray; padding: 2px; font-size: small;">Allows unrestricted communication between hosts on the trusted LAN networks</div>		
<div style="display: flex; justify-content: space-between;"> <input checked="" type="checkbox"/> Bi-Directional <input type="checkbox"/> Dynamic Rule <input type="checkbox"/> Deactivate Rule </div>		
Source	Service	Destination
<div style="border: 1px solid gray; padding: 2px;"> BO1 10.0.80.0/24 </div>	<div style="border: 1px solid gray; padding: 2px;"> <explicit-srv> UDP * </div>	<div style="border: 1px solid gray; padding: 2px;"> HQ 10.0.10.0/25 </div>
Authenticated User	Policies	Connection Method
<div style="border: 1px solid gray; padding: 2px;"> Any </div>	<div style="border: 1px solid gray; padding: 2px;"> IPS Policy Default Policy Application Policy No AppControl Schedule Always QoS Band (Fwd) VoIP (ID 2) QoS Band (Reply) Like-Fwd </div>	<div style="border: 1px solid gray; padding: 2px;"> <div style="border: 2px solid orange; padding: 2px;">TI-Slave</div> Original Source IP (same port) </div>
<div style="display: flex; justify-content: flex-end; gap: 10px;"> OK Cancel </div>		

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

Figures

1. adapt_bandw_protection_01.png
2. TI_session_balancing_00a.png
3. TI_session_balancing_01.png
4. TI_session_balancing_01a.png
5. TI_session_balancing_01b.png
6. TI_session_balancing_01c.png
7. TI_session_balancing_01d.png
8. performance_based_transport_selection_01.png
9. TI_session_balancing_01e.png
10. TI_session_balancing_04.png
11. TI_session_balancing_04a.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.