How to Configure Session Balancing for VPN Tunnels with SD-WAN

https://campus.barracuda.com/doc/96026178/

Session-based balancing for multi-transport TINA VPN tunnels is enabled per access rule in the SD-WAN 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 stye balancing policy. If used without adaptive balancing, it is recommended to use transports of similar bandwidth and latency (Round Trip Time). Static balancing is available for all transport protocols. Static session balancing can be configured to balance over multiple transports in the same SD-WAN class based on the defined SD-WAN 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 CloudGen Firewalls:

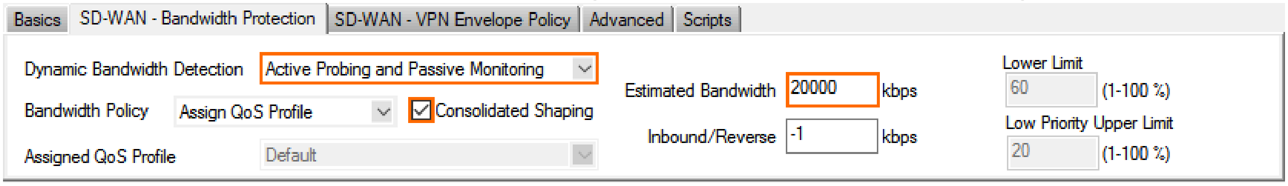
- Create a TINA site-to-site VPN tunnel. For more information, see How to Create a TINA VPN Tunnel between CloudGen Firewalls or How to Create a VPN Tunnel with the VPN GTI Editor.
- Add one or more additional transports to the VPN tunnel. For more information, see How to Add a VPN Transport to a TINA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

Step 1. (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 Round Trip Time Detection.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 **SD-WAN - Bandwidth Protection** tab.
5. From the **Dynamic Bandwidth Detection** list, select the policy:

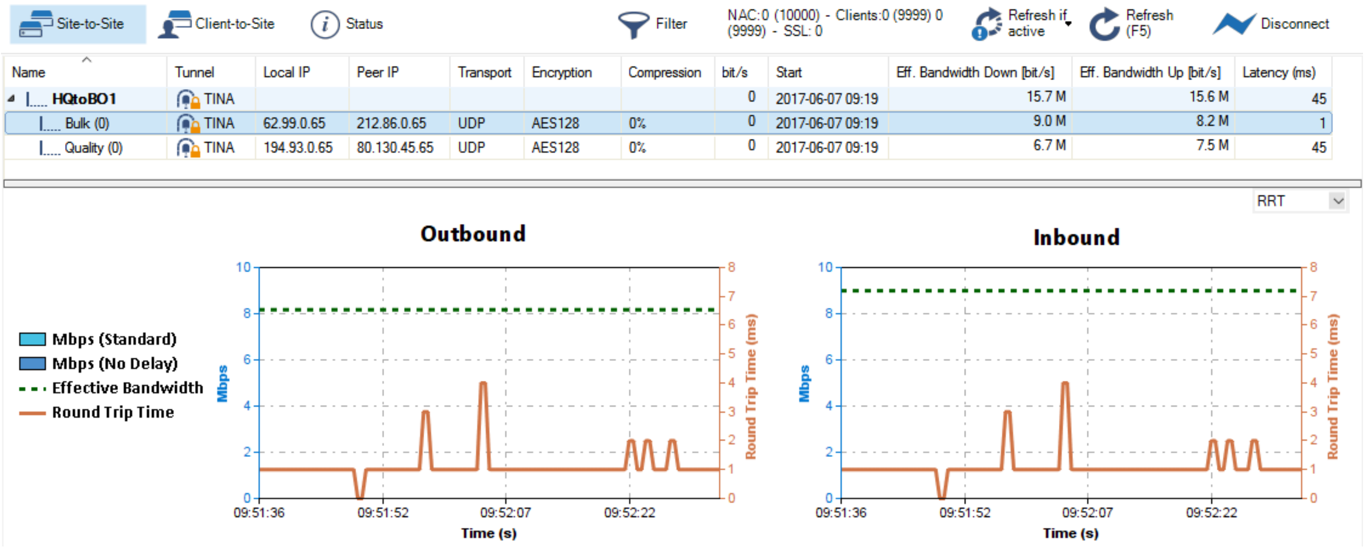
   - **Active Probing and Passive Monitoring**
   - **Active Probing Only**
   - **No Probing - use Estimated Bandwidth**
6. Enter the **Estimated Bandwidth** bandwidth.
7. (optional) Select the **Consolidated Shaping** check box and select the **Assigned QoS Profile**.



Dynamic Bandwidth Detection: Active Probing and Passive Monitoring
Bandwidth Policy: Assign QoS Profile ☑ Consolidated Shaping
Assigned QoS Profile: Default
Estimated Bandwidth: 20000 kbps
Inbound/Reverse: -1 kbps
Lower Limit: 60 (1-100 %)
Low Priority Upper Limit: 20 (1-100 %)

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

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



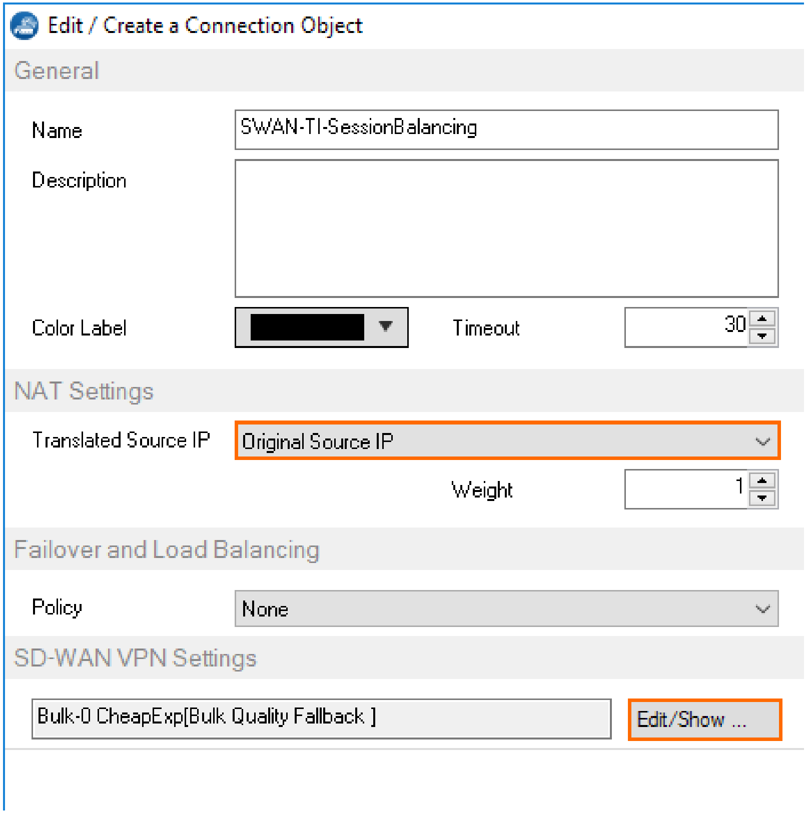
Name	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start	Eff. Bandwidth Down [bit/s]	Eff. Bandwidth Up [bit/s]	Latency (ms)
HQtoBO1	TINA						0	2017-06-07 09:19	15.7 M	15.6 M	45
Bulk (0)	TINA	62.99.0.65	212.86.0.65	UDP	AES128	0%	0	2017-06-07 09:19	9.0 M	8.2 M	1
Quality (0)	TINA	194.93.0.65	80.130.45.65	UDP	AES128	0%	0	2017-06-07 09:19	6.7 M	7.5 M	45

Step 2. Create a Custom Connection Object for the Firewall Acting as SD-WAN Primary

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 > 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**.



Edit / Create a Connection Object

General

Name: SWAN-TI-SessionBalancing

Description:

Color Label: ■ Timeout: 30

NAT Settings

Translated Source IP: Original Source IP

Weight: 1

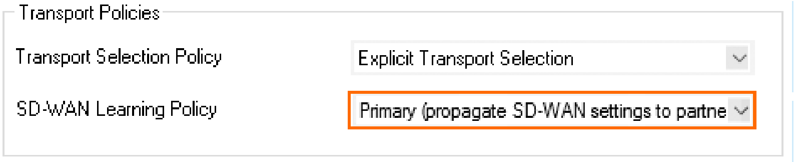
Failover and Load Balancing

Policy: None

SD-WAN VPN Settings

Bulk-0 CheapExp[Bulk Quality Fallback]

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

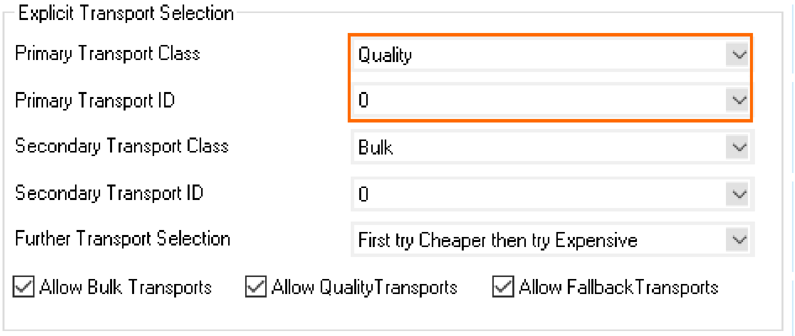


Transport Policies

Transport Selection Policy: Explicit Transport Selection

SD-WAN Learning Policy: Primary (propagate SD-WAN settings to partne

8. Configure the primary transport class and ID:
   - **Primary Transport Class** – Select the SD-WAN class of the primary transport.
   - **Primary Transport ID** – Select the ID for the primary transport.



Explicit Transport Selection

Primary Transport Class: Quality

Primary Transport ID: 0

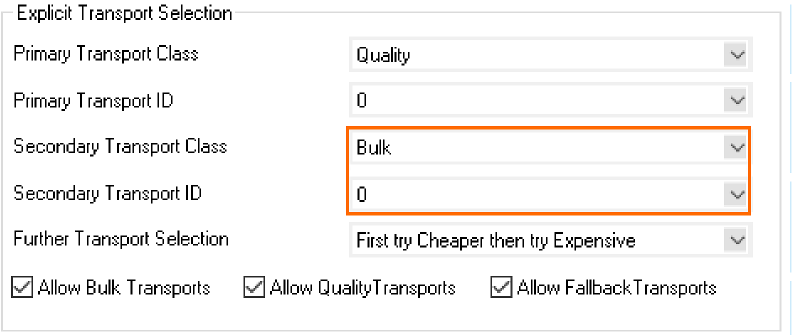
Secondary Transport Class: Bulk

Secondary Transport ID: 0

Further Transport Selection: First try Cheaper then try Expensive

☑ Allow Bulk Transports ☑ Allow QualityTransports ☑ Allow FallbackTransports

9. (Balancing between primary and secondary transports only) Configure the secondary transport class and ID:
   - **Secondary Transport Class** – Select the SD-WAN class secondary transport.
   - **Secondary Transport ID** – Select the ID for the secondary transport.



Explicit Transport Selection

Primary Transport Class: Quality

Primary Transport ID: 0

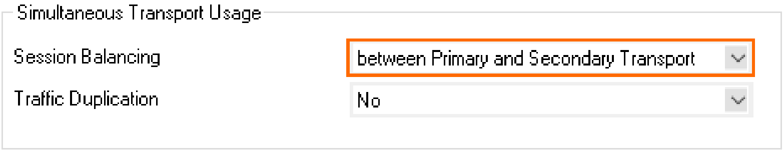
Secondary Transport Class: Bulk

Secondary Transport ID: 0

Further Transport Selection: First try Cheaper then try Expensive

☑ Allow Bulk Transports ☑ Allow QualityTransports ☑ Allow FallbackTransports

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



Simultaneous Transport Usage

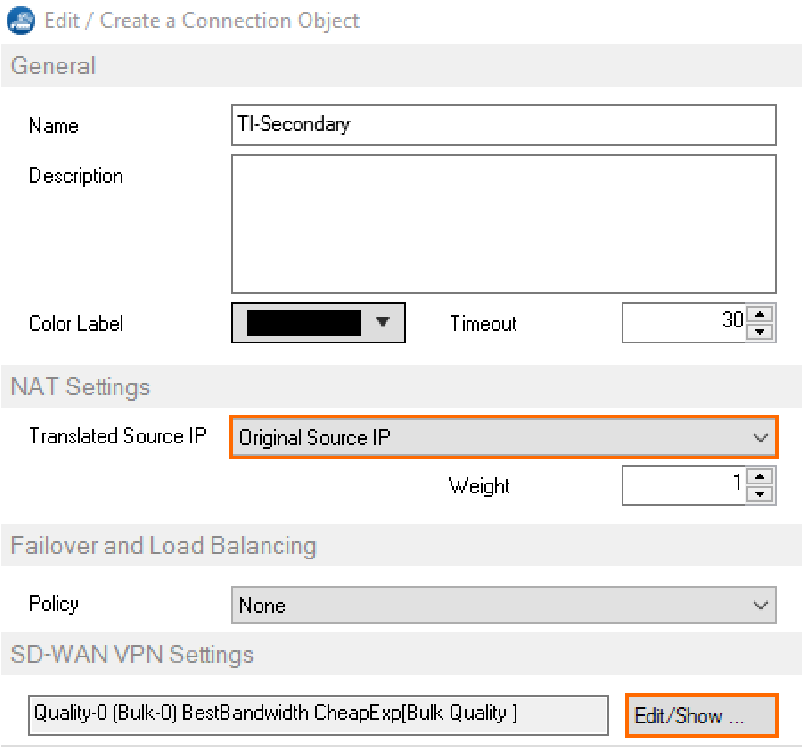
Session Balancing: between Primary and Secondary Transport

Traffic Duplication: No

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

Step 3. Create a Custom Connection Object for the Firewall Acting as 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 a **Name**.
5. From the **Translated Source IP** list, select **Original Source IP**.



Edit / Create a Connection Object

General

Name: TI-Secondary

Description:

Color Label: ▼ Timeout: 30

NAT Settings

Translated Source IP: Original Source IP

Weight: 1

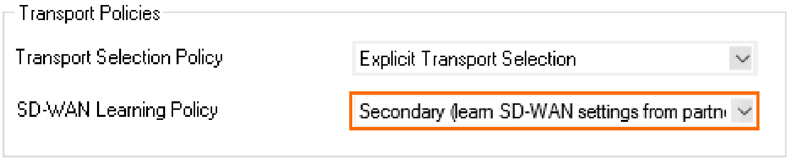
Failover and Load Balancing

Policy: None

SD-WAN VPN Settings

Quality-0 (Bulk-0) BestBandwidth CheapExp[Bulk Quality]

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



Transport Policies

Transport Selection Policy: Explicit Transport Selection

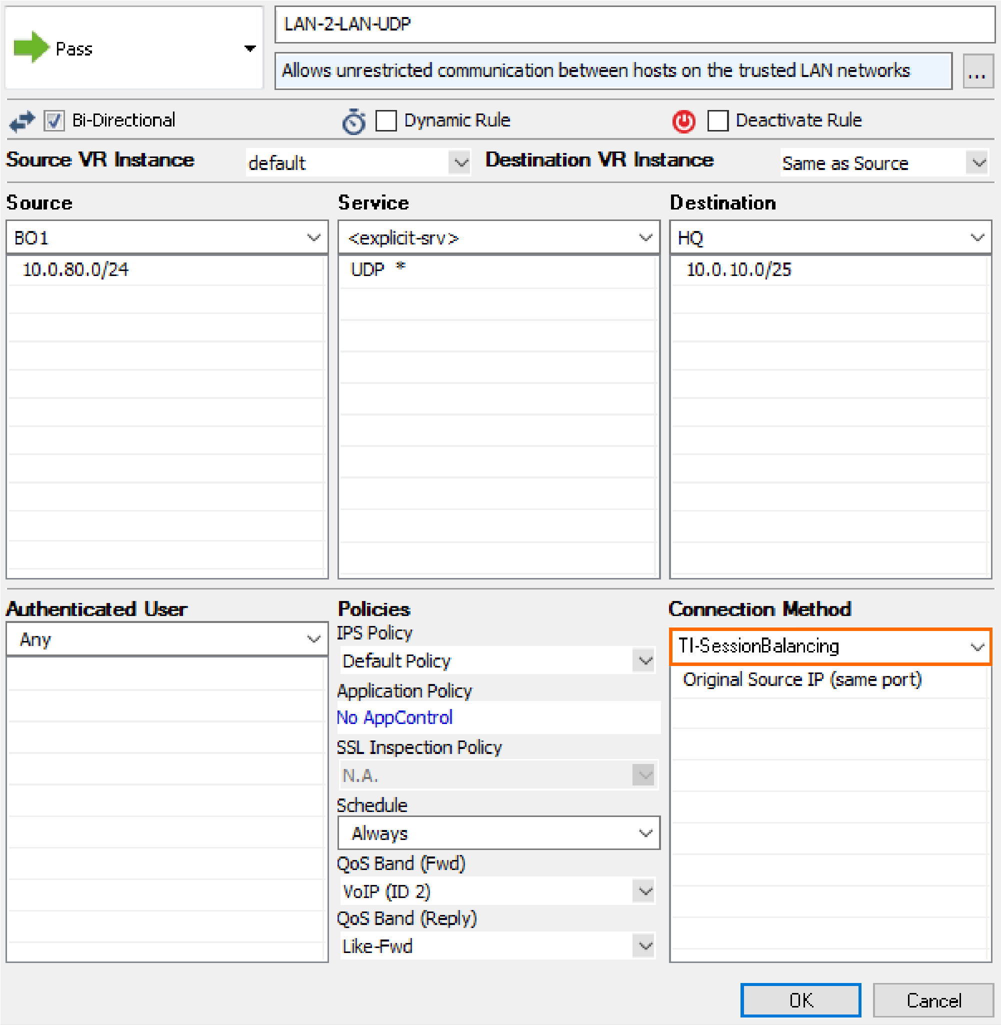
SD-WAN Learning Policy: Secondary (learn SD-WAN settings from partn

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

Step 4. Modify the 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.



Pass

LAN-2-LAN-UDP

Allows unrestricted communication between hosts on the trusted LAN networks

☑ Bi-Directional □ Dynamic Rule □ Deactivate Rule

Source VR Instance: default

Destination VR Instance: Same as Source

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

SSL Inspection Policy: N.A.

Schedule: Always

QoS Band (Fwd): VoIP (ID 2)

QoS Band (Reply): Like-Fwd

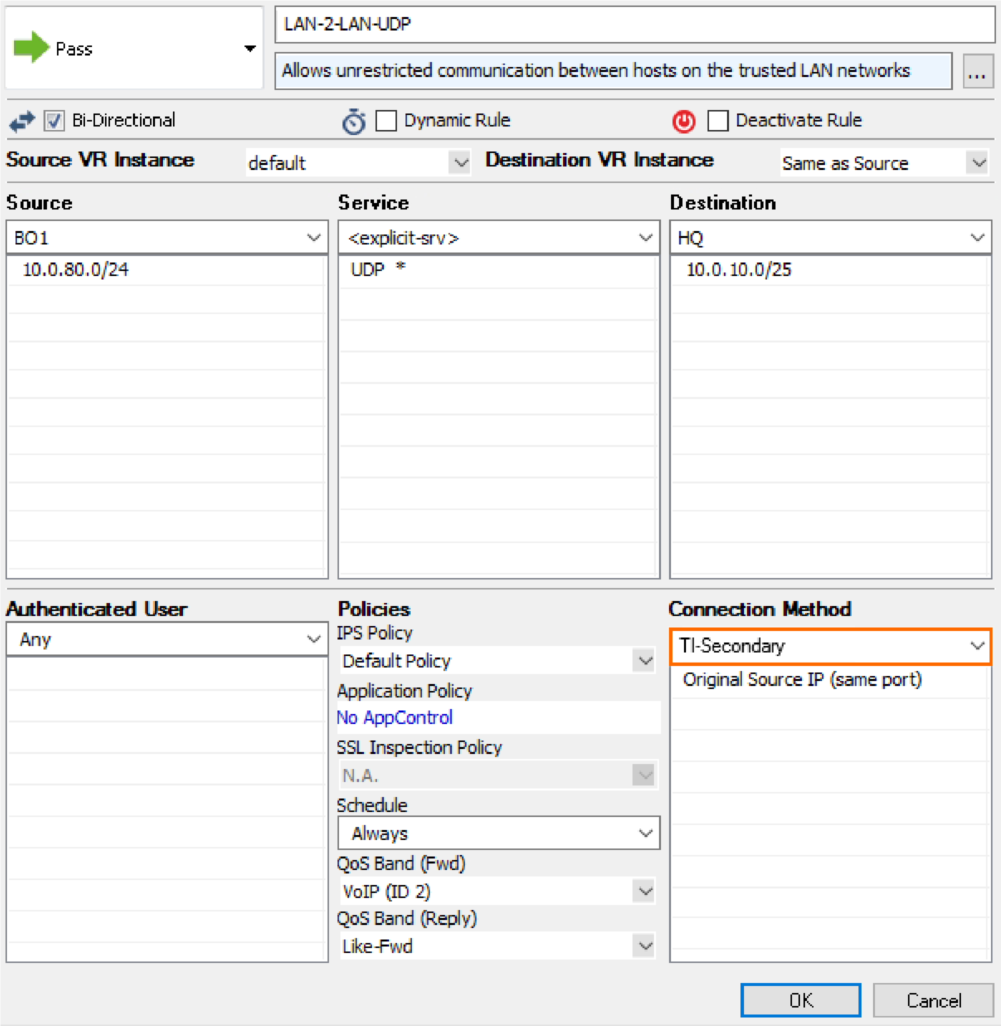
Connection Method: TI-SessionBalancing – Original Source IP (same port)

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

Step 5. Modify the 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.



Pass

LAN-2-LAN-UDP

Allows unrestricted communication between hosts on the trusted LAN networks

☑ Bi-Directional   □ Dynamic Rule   □ Deactivate Rule

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

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

SSL Inspection Policy: N.A.

Schedule: Always

QoS Band (Fwd): VoIP (ID 2)

QoS Band (Reply): Like-Fwd

Connection Method: TI-Secondary – Original Source IP (same port)

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

Figures