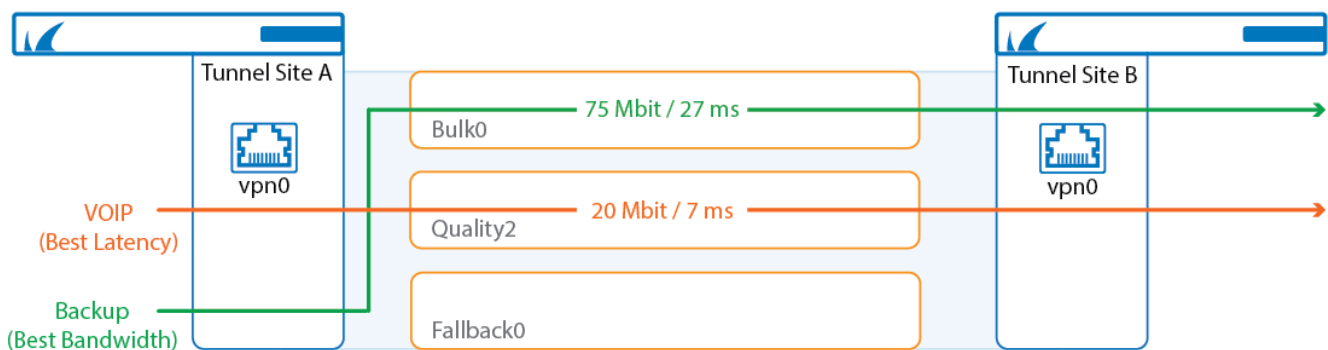


How to Configure Performance-Based Transport Selection for VPN Tunnels with SD-WAN

<https://campus.barracuda.com/doc/96026181/>

Performance-Based Transport Selection selects the VPN transport offering the best latency (Round Trip Time) or bandwidth for the traffic matching the access rule. Only UDP transports with Dynamic Bandwidth and Round Trip Time Detection are supported. Performance-Based Transport Selection can route traffic using the following policies:

- Optimize for Latency
- Optimize for Outbound Bandwidth
- Optimize for Inbound Bandwidth
- Optimize for Combined Bandwidth



Before You Begin

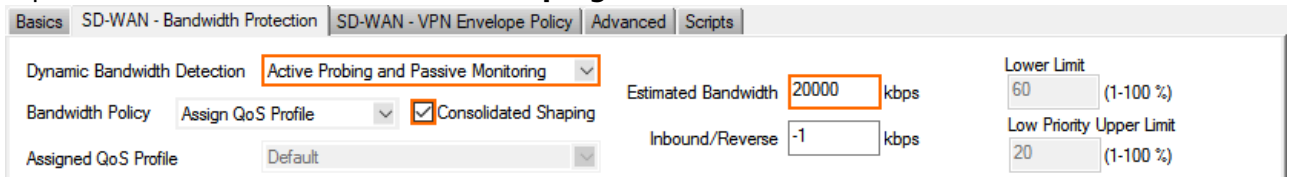
Create a multi-transport VPN tunnel between two CloudGen Firewalls:

- 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 UDP 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](#).
- Create access rules for each type of traffic going through the VPN tunnel. For more information, see [How to Create Access Rules for Site-to-Site VPN Access](#).
- (Consolidated Shaping only) Set the QoS Profile and enable shaping for the physical interfaces used by the VPN traffic.

Step 1. Enable Dynamic Bandwidth and Latency Detection for Each Transport

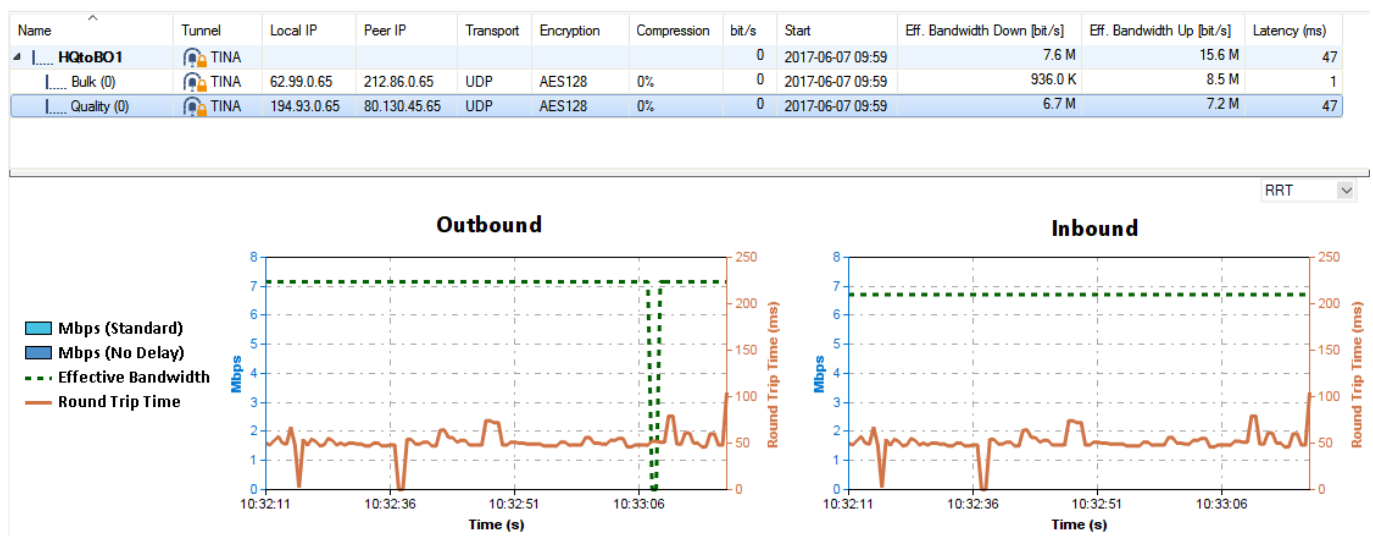
On both VPN endpoints, edit all transports to enable Dynamic Bandwidth and Round Trip Time Detection.

- Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN Service > Site-to-Site**.
- Click **Lock**.
- Double-click the TINA VPN tunnel. The **TINA Tunnel** window opens.
- Click the **SD-WAN - Bandwidth Protection** tab.
- From the **Dynamic Bandwidth Detection** list, select the policy:
 - Active Probing and Passive Monitoring
 - Active Probing Only
 - No Probing - use Estimated Bandwidth
- Enter the **Estimated Bandwidth** bandwidth.
- (optional) Select the **Consolidated Shaping** check box




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

After completing these changes, go to **VPN > Site-to-Site**. Right-click the transport and select **Monitor Traffic**. The Round Trip Time, drop rate, and traffic on the transport is now displayed in real time.



Step 2. 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. 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

Description

Color Label Timeout

NAT Settings

Translated Source IP Weight

Failover and Load Balancing

Policy

SD-WAN VPN Settings

6. To edit the **VPN SD-WAN** settings, click **Edit/Show**. The **SD-WAN Settings** window opens.
7. Configure the **Transport Policies**:
 - **Transport Selection Policy** – Select the criteria to optimize for:
 - **Optimize for Inbound Bandwidth**
 - **Optimize for Outbound Bandwidth**
 - **Optimize for Combined Bandwidth**
 - **Optimize for Latency**
 - **SD-WAN Learning Policy** – Select **Primary**.

Transport Policies

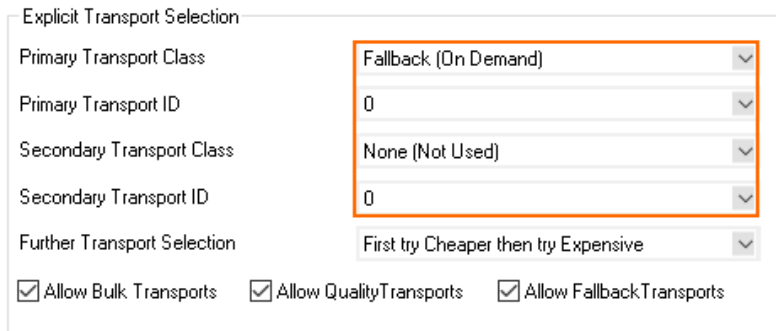
Transport Selection Policy

SD-WAN Learning Policy

8. Configure the **Explicit Transport Selection** as the fallback if no more transports with Dynamic

Bandwidth and Round Trip Time Detection are available.


- **Primary Transport Class** – Select the primary transport class.
- **Primary Transport ID** – Select the ID for the primary transport.
- **Secondary Transport Class** – Select the secondary transport class.
- **Secondary Transport ID** – Select the ID for the secondary transport.



9. Click **OK**.
10. 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 a **Name**.
5. From the **Translated Source IP** list, select **Original Source IP**.

 Edit / Create a Connection Object

General

Name

Description

Color Label Timeout

NAT Settings

Translated Source IP Weight

Failover and Load Balancing

Policy

SD-WAN VPN Settings

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

Transport Policies

Transport Selection Policy

SD-WAN Learning Policy

Explicit Transport Selection

Primary Transport Class

Primary Transport ID

Secondary Transport Class

Secondary Transport ID

Further Transport Selection

☒ Allow Bulk Transports ☒ Allow QualityTransports ☒ Allow FallbackTransports

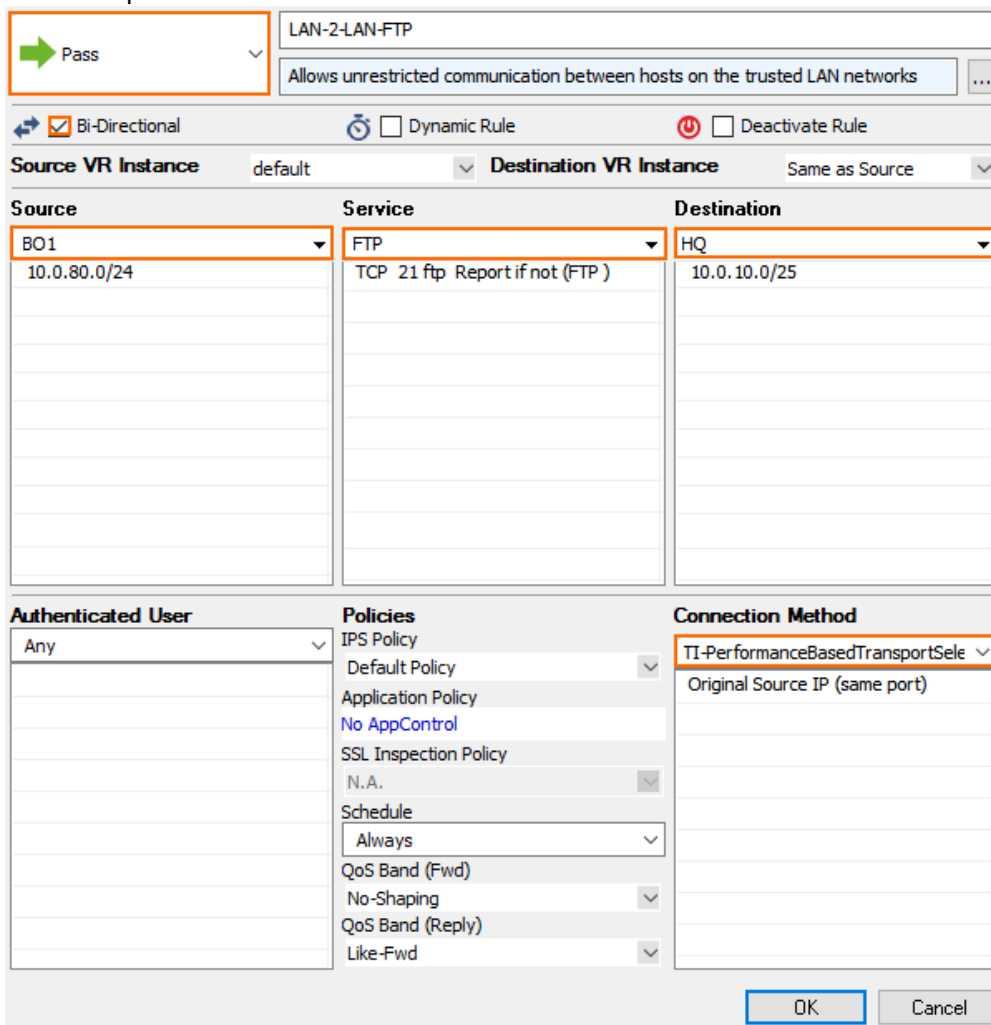
- Click **OK**.
- Click **Send Changes** and **Activate**.

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

- 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.



LAN-2-LAN-FTP
 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	Service	Destination
BO1 10.0.80.0/24	FTP TCP 21 ftp Report if not (FTP)	HQ 10.0.10.0/25

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Policy Application Policy No AppControl SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd) No-Shaping QoS Band (Reply) Like-Fwd	TI-PerformanceBasedTransportSele Original Source IP (same port)

OK Cancel

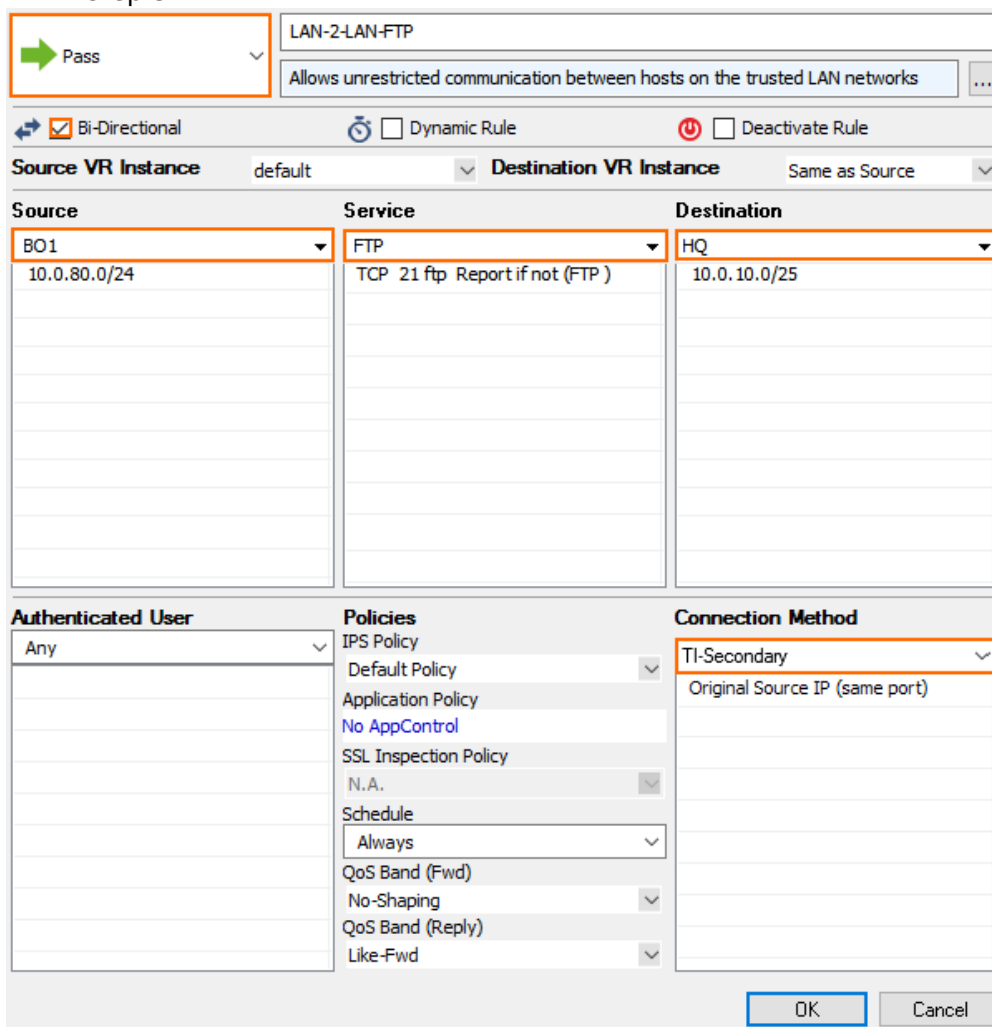
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

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 the access rule is now balanced according to the performance criteria selected in the SD-WAN settings of the connection object in the matching access rule. To find out which transport has the best bandwidth or Round Trip Time, go to the **VPN > Site-to-Site** page and compare the values in the **Eff Bandwidth Down**, **Eff Bandwidth Up**, or **Latency** columns for all transports configured in the connection object. Go to the **FIREWALL > Live** page and, in the **SD-WAN** column of the traffic

matching the access rule with the Performance-Based Transport Selection connection object, verify that the best transport is used. In this case, the Q0 transport is the primary transport, but the B0 transport offers the better bandwidth. Therefore, according to the **Best Combined Bandwidth** policy, traffic is sent through the B0 transport.

Site-to-Site

Client-to-Site

Status

Filter

NAC: 0 (10000) - Clients: 0 (9999) 0

Refresh if active

Re (F)

Name	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Latency (ms)	Dyn. Bandwidth Detection	Eff. Bandwidth Down (bit/s)	Eff. Bandwidth Up (bit/s)	Start
HQtoBO1	TINA	62.99.0.65	212.86.0.65	UDP	AES128	0%	23.8 M	48	No	27.3 M	30.2 M	2017-05-31 14:45
Bulk (0)	TINA	194.93.0.65	80.130.45.65	UDP	AES128	0%	0	5	Yes	21.9 M	22.6 M	2017-05-31 14:45
Quality (0)	TINA	194.93.0.65	80.130.45.65	UDP	AES128	0%	0	48	Yes	5.4 M	7.6 M	2017-05-31 14:53

Monitor

Live

History

Threat Scan

Audit Log

Shaping

Users

Dynamic

Host Rules

Forwarding Rules

Traffic Selection

Forward, Local In, Local Out, IPv4, IPv6

Status Selection

Closing, Established, Failing, Pending

Port

5001

+

ID	State	IP Protocol	Port	Source	Interface	Destination	Output-IF	QoS	Rule	bit/s	Total	Idle	SD-WAN ID
		TCP	5001	10.0.10.40	eth0	10.0.80.40	vpn0@F...	Internet /	LAN-2-LAN-TCP	21.6 M	59.8 M	0s	B0 (Q0)
		TCP	5001	10.0.10.40	eth0	10.0.80.40	vpn0@F...	Internet /	LAN-2-LAN-TCP	0	924.0	21s	B0 (Q0)

Next Steps

Combine Performance-Based Transport Selection with Adaptive Bandwidth Protection.

For more information, see [How to Configure Adaptive Bandwidth Protection for VPN Tunnels with SD-WAN](#).

Figures

1. ti_performance_based_transport_selection1.png
2. adapt_bandw_protection_01.png
3. TI_dyn_bandwidth_detect_no_traffic.png
4. performance_based_transport_selection_01.png
5. performance_based_transport_selection_011a (1).png
6. performance_based_transport_selection_01b.png
7. performance_based_transport_selection_01a.png
8. performance_based_transport_selection_03.png
9. performance_based_transport_selection_05.png
10. performance_based_transport_selection_04.png
11. transport_selection_vpn_s2s.png
12. transport_selection_fw_live.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.