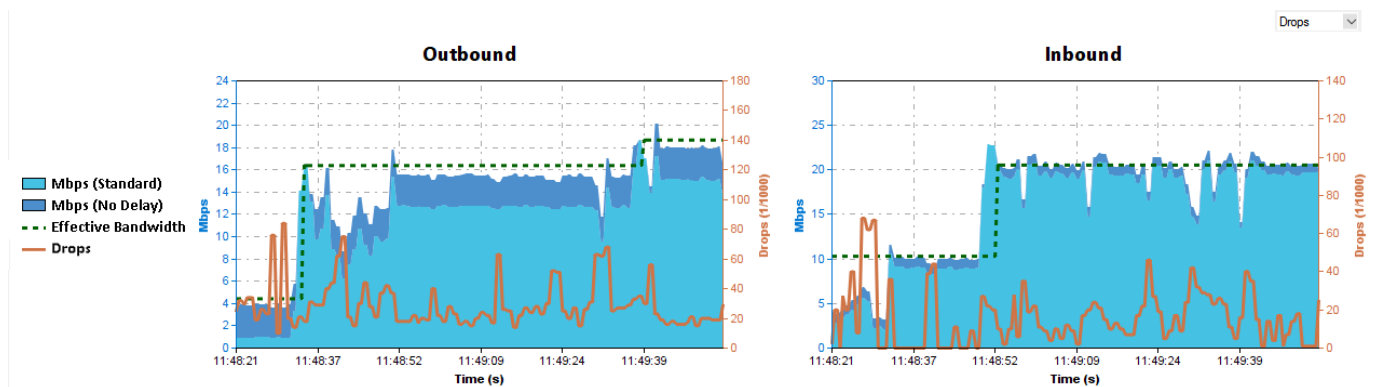


How to Configure Adaptive Bandwidth Protection for VPN Tunnels with SD-WAN

<https://campus.barracuda.com/doc/96026177/>

Adaptive Bandwidth Protection is used to effectively shape traffic on the VPN transport by using the link quality metrics collected by Dynamic Bandwidth and Latency (Round Trip Time) Detection. This allows the firewall to always shape traffic using, instead of a static number as the bandwidth, a consistently, dynamically updated value that reflects the current state of the transport. Changing link metrics are immediately applied to Adaptive Bandwidth Detection. Traffic shaping uses an internal traffic shaping tree for SD-WAN, distinguishing only between no-delay (VOIP) and standard traffic.



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](#).
- 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. Modify Default Shaping Tree

On both VPN endpoints, edit the Internet QoS band to use the STD virtual interface.

1. Go to **CONFIGURATION > Configuration Tree > Box > Traffic Shaping**.

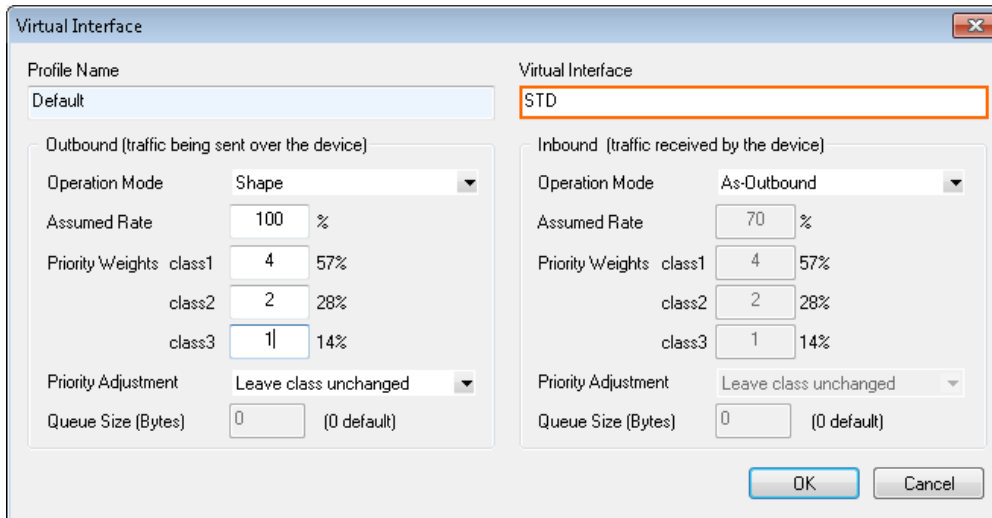
2. Click **Lock**.

3. Right click on the QoS profile and click **Add new virtual Interface**.

4. Enter STD as the **Virtual Interface**.

All other settings of this virtual interface are handled by the SD-WAN features.

5. Click **OK**.

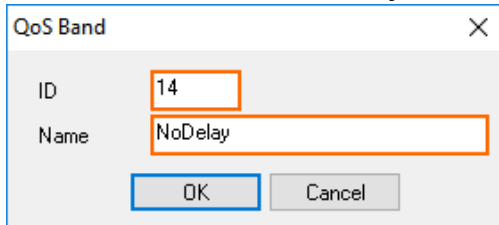


6. Click on the **QoS Band** tab.

7. Right-click and select **Add new QoS Band**. The **QoS Band** window opens.

8. Create the QoS Band for no-delay traffic :

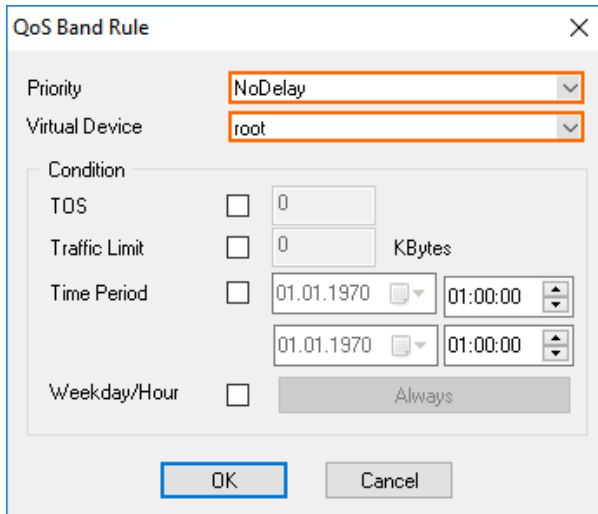
- **ID** – Enter an unused **ID**. E.g., 14
- **Name** – Enter NoDelay.



9. Click **OK**. The **QoS Band Rule** window opens.

10. Create the QoS band rule:

- **Priority** – Select **NoDelay**.
- **Virtual Device** – Select **root**.



The 'QoS Band Rule' window is shown with the following settings:

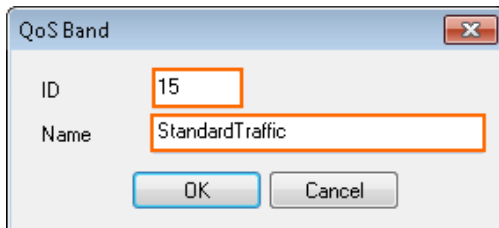
- Priority: **NoDelay** (selected in a dropdown menu)
- Virtual Device: **root** (selected in a dropdown menu)
- Condition section:
 - TOS: ☐ 0
 - Traffic Limit: ☐ 0 KBytes
 - Time Period: ☐ 01.01.1970 01:00:00 (two identical rows)
 - Weekday/Hour: ☐ Always

Buttons: OK, Cancel

11. Click **OK**.

12. Create the QoS band:

- **ID** - Enter an unused **ID**.
- **Name** - Enter **StandardTraffic**.



The 'QoS Band' window is shown with the following settings:

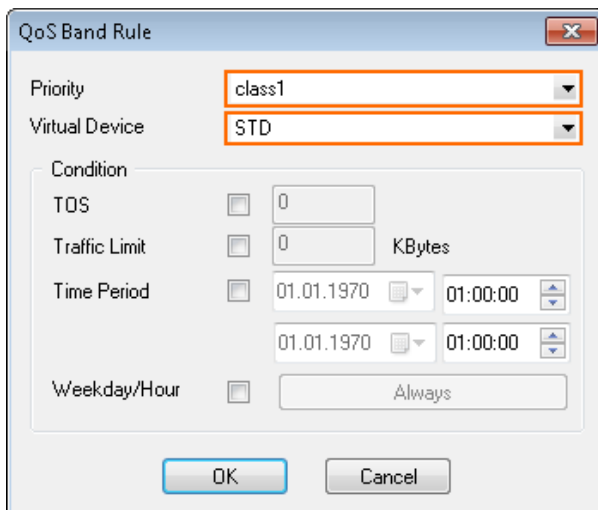
- ID: **15** (entered in a text field)
- Name: **StandardTraffic** (entered in a text field)

Buttons: OK, Cancel

13. Click **OK**. The **QoS Band Rule** window opens.

14. Create the QoS band rule:

- **Priority** - Select **class1**.
- **Virtual Device** - Select **STD**.



The 'QoS Band Rule' window is shown with the following settings:

- Priority: **class1** (selected in a dropdown menu)
- Virtual Device: **STD** (selected in a dropdown menu)
- Condition section:
 - TOS: ☐ 0
 - Traffic Limit: ☐ 0 KBytes
 - Time Period: ☐ 01.01.1970 01:00:00 (two identical rows)
 - Weekday/Hour: ☐ Always

Buttons: OK, Cancel

15. Click **OK**.

16. (optional) add additional classes to the **Standard Traffic** QoS band.

17. Click **Send Changes** and **Activate**.

The two QoS band are now listed - **VoIP** using the **root** interface and **StandardTraffic** using the **STD**

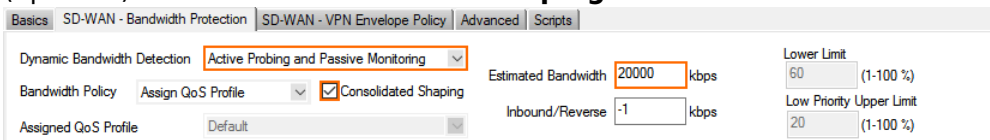
virtual interface.

QoS Profile		QoS Band				
Id - Name	Priority class	TOS	Traffic-Limit	Time-Period	Weekday-Hour	
1 - Interactive						
2 - VoIP						
3 - Business						
4 - Internet						
5 - Background						
6 - LowPrio						
7 - LowestPrio						
8 - Choke						
14 - NoDelay						
root	NoDelay					
15 - StandardTraffic						
STD	class 1					

Step 2. Enable Dynamic Bandwidth and Latency Detection and SD-WAN Bandwidth Protection

On both VPN endpoints, edit the TINA site-to-site VPN tunnel to use the **SD-WAN** QoS profile and enable Dynamic Bandwidth and Round Trip Time Detection.

- Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site VPN**.
- 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.



SD-WAN - Bandwidth Protection		SD-WAN - VPN Envelope Policy		Advanced	Scripts
Dynamic Bandwidth Detection	Active Probing and Passive Monitoring	Estimated Bandwidth	20000 kbps	Lower Limit	60 (1-100 %)
Bandwidth Policy	Assign QoS Profile	<input checked="" type="checkbox"/> Consolidated Shaping	Inbound/Reverse	-1 kbps	Low Priority Upper Limit
Assigned QoS Profile	Default				20 (1-100 %)

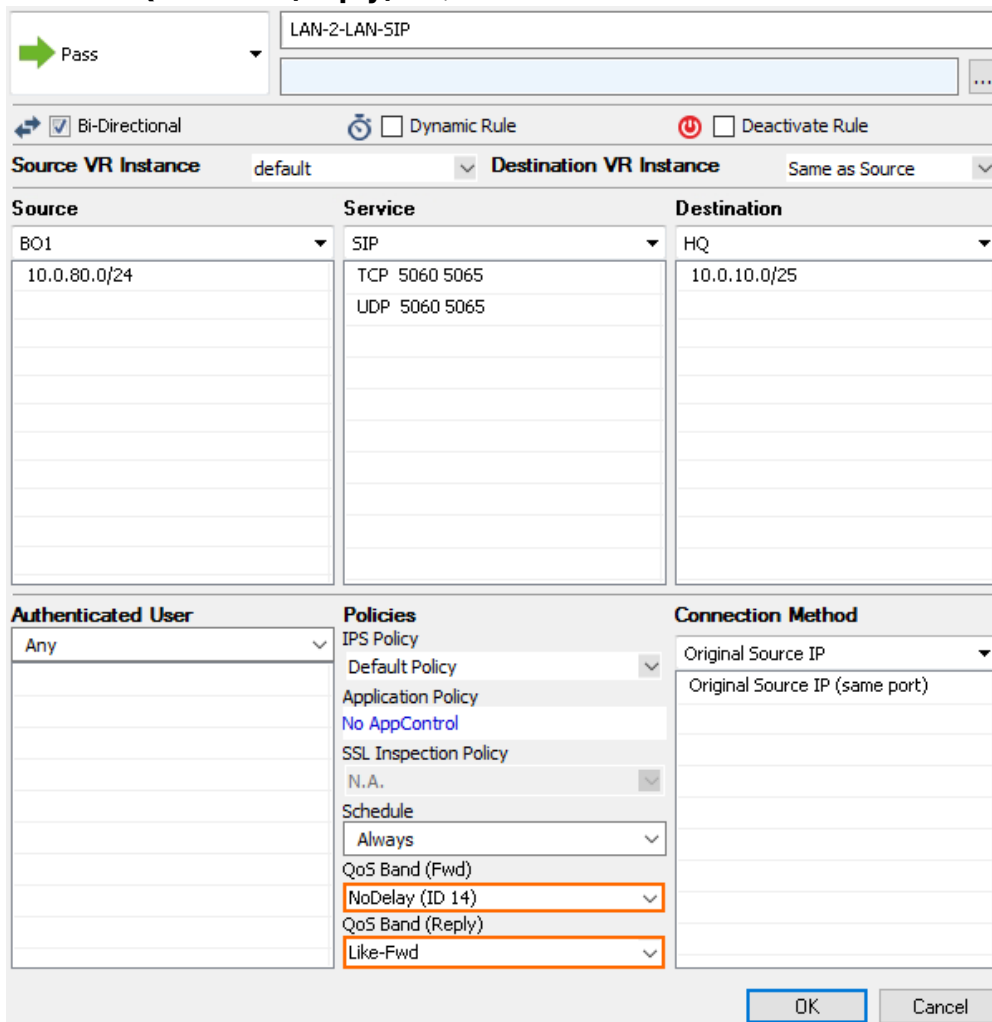
- Click **OK**.
- Click **Send Changes** and **Activate**.

After completing these changes, go to **VPN > Site-to-Site**. Right-click the transport and select **Monitor Traffic**.

Step 3. Set QoS Band for No-Delay Traffic

Set the QoS band for all access rules matching VPN traffic that should be handled as no-delay traffic. No-delay traffic should not make up more than 30% of total traffic.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall**.
2. Click **Lock**.
3. Double-click the access rule matching the no-delay traffic.
4. From the **QoS Band (Fwd)** list, select **NoDelay (ID 14)** created in Step 1.
5. From the **QoS Band (Reply)** list, select **Like-Fwd**.



Pass

LAN-2-LAN-SIP

☒ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

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

Source	Service	Destination
BO1	SIP	HQ
10.0.80.0/24	TCP 5060 5065 UDP 5060 5065	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) NoDelay (ID 14) QoS Band (Reply) Like-Fwd	Original Source IP Original Source IP (same port)

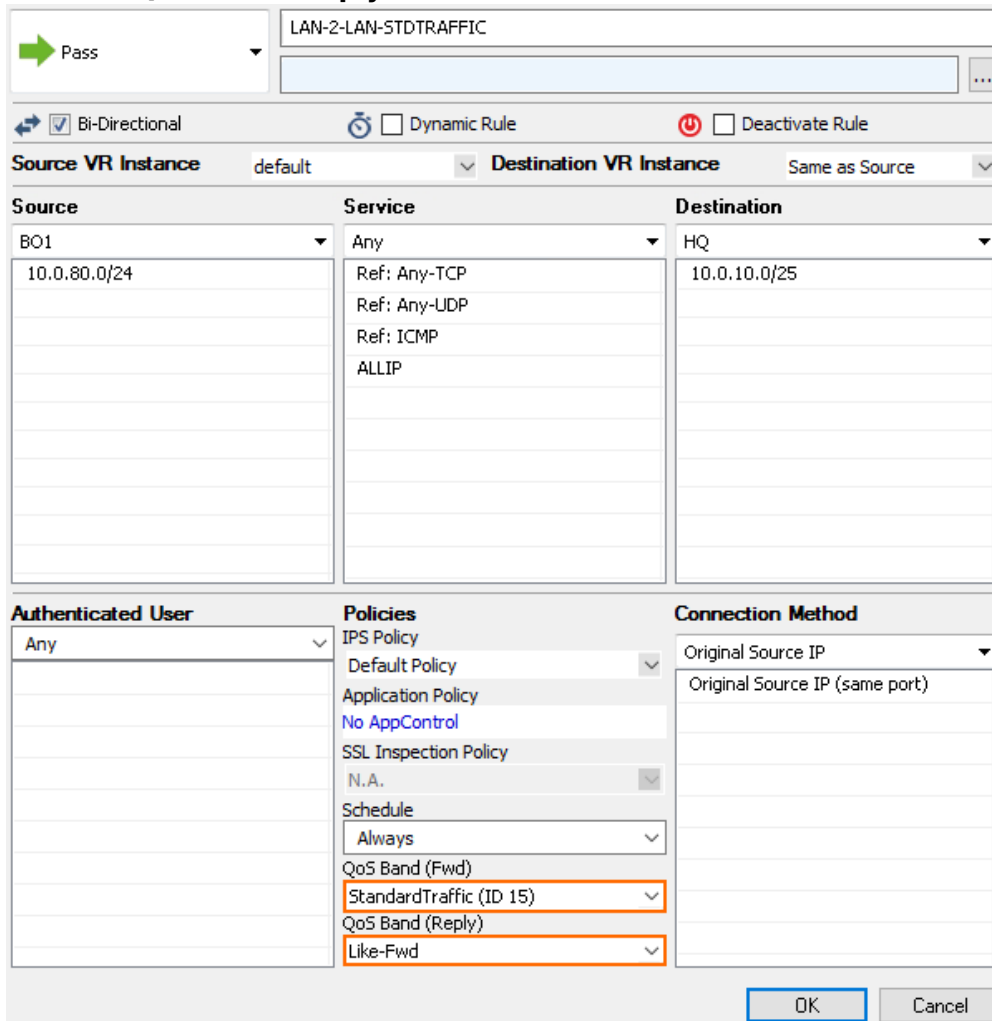
OK Cancel

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

Step 4. Set QoS Band for Standard Traffic

All other VPN traffic is classified as standard traffic. Standard traffic can take up to 70% of the bandwidth.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall**.
2. Click **Lock**.
3. Double-click the access rule matching the standard traffic.
4. From the **QoS Band (Fwd)** list, select **StandardTraffic (ID 15)** created in Step 1.
5. From the **QoS Band (Reply)** list, select **Like-Fwd**.



Pass

LAN-2-LAN-STDTRAFFIC

☒ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

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

Source	Service	Destination
BO1	Any	HQ
10.0.80.0/24	Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	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) StandardTraffic (ID 15) QoS Band (Reply) Like-Fwd	Original Source IP Original Source IP (same port)

OK Cancel

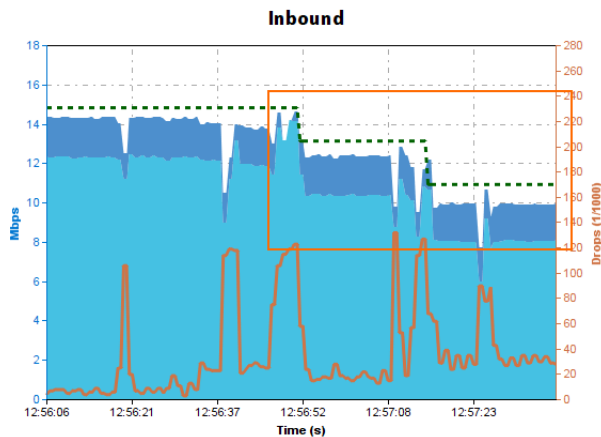
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

The firewall now protects the no-delay traffic and automatically adjusts shaping to the currently available bandwidth. Shaping down happens continuously as needed; shaping up is detected every couple of minutes. Go to the **FIREWALL > Shaping** page to see the built-in shaping tree used for the adaptive SD-WAN features.

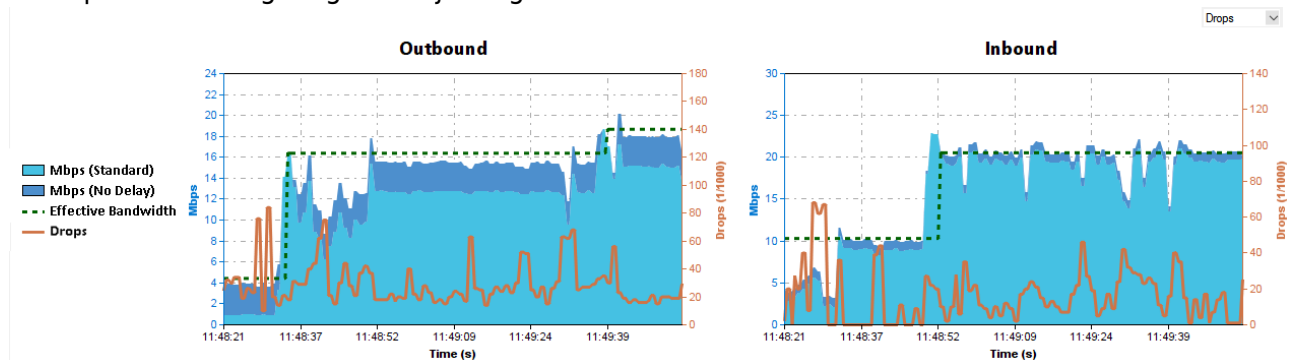
Interface	Dir	Rate-Max	Rate-Sum (Sessions)	Queue Fills	CI1 (Total Bytes / Packets / Drops)	CI2 (Total Bytes / Packets / Drops)	CI3 (Total Bytes / Packets / Drops)	ND (Total Bytes / Packets / Drops)
[VPN]-HQtoB01								
root	OUT	3.0 M	2.6 M (1 / 7)	0	1.3 M (1.3 G / 980.683 / 16)			1.2 M (1.4 G / 1.113.232 / 0)
NoDelay	OUT	2.7 M	0 B	0				0 B (1.3 G / 1.067.051 / 0)
STD	OUT	1.4 M	1.3 M (6 / 6)	0	1.3 M (1.3 G / 980.699 / 2.204)			
Quality (0)								
root	OUT	7.3 M	0 B	0	0 B (500.8 M / 375.687 / 498)			0 B (315.4 M / 249.045 / 0)
NoDelay	OUT	6.6 M	0 B	0				0 B (181.7 M / 143.466 / 0)
STD	OUT	5.2 M	0 B	0	0 B (501.5 M / 376.185 / 2.352)			

Go to **VPN > Site-to-Site** and enable monitoring on the transport to see the effective bandwidth, drops, Round Trip Time, and a stacked graph for no-delay and standard traffic. Note how the dark blue no-delay traffic is protected even through bandwidth changes.

- Example monitoring diagram for deteriorating bandwidth:



- Example monitoring diagram adjusting for more available bandwidth:



Figures

1. Bandwidth_protection.png
2. sdwan_shaping_01.png
3. sdwan_shaping_04.png
4. sdwan_shaping_05.png
5. sdwan_shaping_02.png
6. sdwan_shaping_03.png
7. sdwan_shaping_06.png
8. adapt_bandw_protection_01.png
9. adapt_bandw_protection_03.png
10. adapt_bandw_protection_04.png
11. Bandwidth_protection_Shaping_view.png
12. probing_monitoring.png
13. Bandwidth_protection.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.