How to Configure SD-WAN Using the VPN GTI Editor

https://campus.barracuda.com/doc/96026452/

SD-WAN is a feature of the TINA VPN protocol that can be used in site-to-site VPN tunnels to send traffic via multiple transports simultaneously. Each transport can use a different WAN link. The transport used by VPN traffic is configured in the SD-WAN settings of the connection object used in the matching access rule. For the advanced traffic shaping and adaptive routing features, Dynamic Bandwidth Detection must be enabled in the GTI group.

For more information, see SD-WAN.

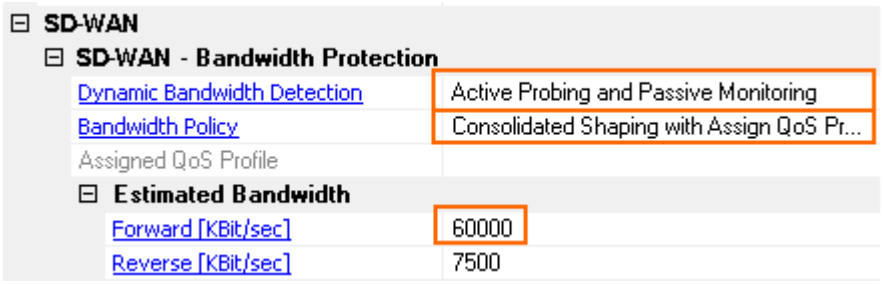
Before You Begin

- Create a VPN Group and add the VPN services to the VPN group. For more information, see How to Create a VPN Tunnel with the VPN GTI Editor.

Step 1. (optional) Enable Dynamic Bandwidth Detection

To use the advanced transport selection and traffic shaping features for SD-WAN, enable Dynamic Bandwidth Detection in the GTI group settings.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > VPN GTI Editor**.
2. Click **Lock**.
3. Double-click the VPN Group. The **Group** window opens.
4. From the **Dynamic Bandwidth Detection** list, select the probing policy:
   - **Active Probing and Passive Monitoring**
   - **Active Probing Only**
   - **No Probing - use Estimated Bandwidth**
5. From the **Bandwidth Policy** list, select **Assign QoS Profile** or **Consolidated Shaping with Assign QoS Profile**.
6. Enter the **Estimated Bandwidth**:
   - **Forward [KBit/sec]** – Enter the outbound bandwidth for this link. This value is used as the starting point for Dynamic Bandwidth Detection.



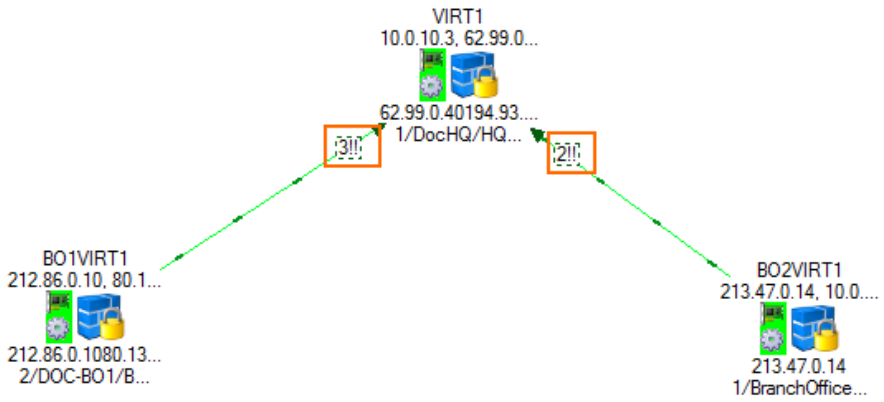
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 2. Add a VPN Transport to a VPN Tunnel

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > VPN GTI Editor**.
2. Click **Lock**.
3. Select the VPN Group in the **Group** tab. The VPN services and configured tunnels are displayed in the GTI editor map.
4. Click a VPN tunnel.
5. Click **Add Transport**. The **TINA Tunnel** window opens.
6. Configure the network settings for the transport. The peer IP addresses must be different for each transport. For more information, see How to Create a VPN Tunnel with the VPN GTI Editor.
7. In the **Tunnel Properties** column, configure:
   - **SD-WAN Classification** – Select **Bulk**, **Quality** or **Fallback**.
   - **SD-WAN-ID** – Select the SD-WAN ID. Each SD-WAN Class/ID combination can be used only once per VPN tunnel.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

The number of VPN transports for a VPN tunnel is now displayed in the GTI editor map. E.g., two transports: **2!!**

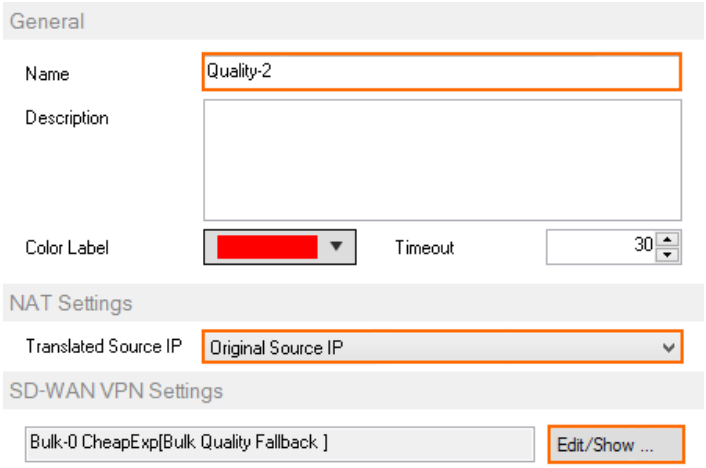
When using two transports the second transport must have the **SD-WAN-ID** set to `0`. For example: *bulk0* or *quality0*.



Step 3. Create Connection Objects to Use VPN Transports

To choose a specific SD-WAN class and ID, you must create connection objects. Connection objects can also contain information on fallback and failover transports. One of the VPN services is the primary for the VPN connection. You must configure one primary and one secondary for the VPN connection. For more information, see SD-WAN.

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**.
6. Click **Edit/Show** in the **SD-WAN VPN Settings** section. The **SD-WAN Settings** window opens.



7. Configure the **SD-WAN Transport Selection**:
   - **Transport Selection Policy** – Select the transport according to the link quality metrics gathered by Dynamic Bandwidth Detection. For more information, see SD-WAN and How to Configure Performance-Based Transport Selection for VPN Tunnels with SD-WAN.

- **SD-WAN Learning Policy** – One VPN service is the primary, the other the secondary. The SD-WAN settings in the connection object of the primary will override the SD-WAN settings of the secondary.
- **Primary Transport Class** – Select the SD-WAN class of the primary transport.
- **Primary Transport ID** – Select the ID for the primary transport.
- **Secondary Transport Class** – Select the SD-WAN class of the secondary transport.
- **Secondary Transport ID** – Select the ID for the secondary transport.
- **Further Tries Transport Selection** – Select the policy by which failover transports are chosen if both the primary and secondary fail. Depending on the additional available VPN transports, you can define more than one backup path. Select from the following predefined policies:
  - **First try Cheaper then try Expensive**
  - **Only try Cheaper**
  - **First try Expensive then try Cheaper**
  - **Only try Expensive**
  - **Stay on Transport (no further tries)**
- **Session Balancing** – Select to balance sessions using static or adaptive balancing. For more information, see SD-WAN and How to Configure Session Balancing for VPN Tunnels with SD-WAN.
- **Traffic Duplication (FEC)** – Select to duplicate and simultaneously send VPN traffic over two transports. For more information, see SD-WAN and How to Configure Traffic Duplication for VPN Tunnels with SD-WAN.

8. Click **OK**.
9. Click **OK**.

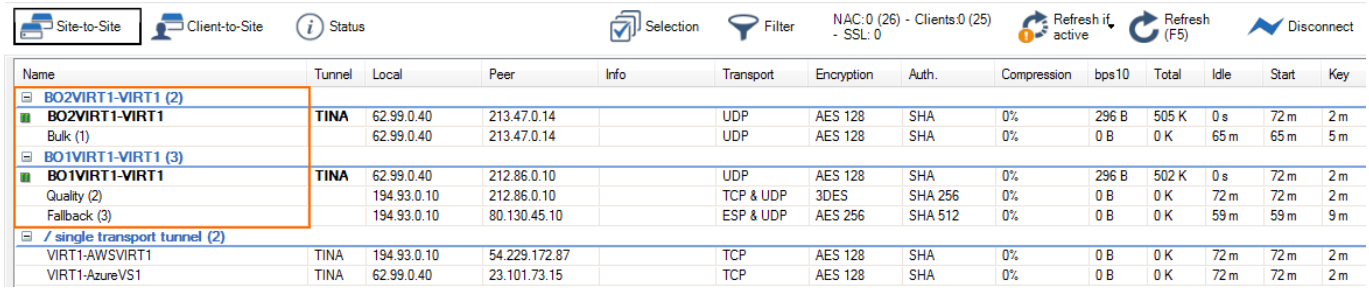
Make sure you are using the connection objects on both CloudGen Firewalls.

Step 4. Assign Access Rules to use the SD-WAN Connection Objects

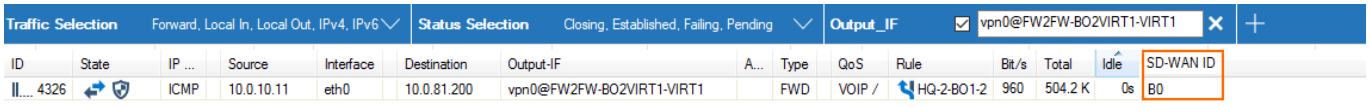
Modify access rules matching VPN traffic to use the custom connection objects created in Step 3.

Monitoring

Each VPN transport is listed on the **VPN > Site-to-Site** and **VPN > Status** pages when logged directly into the CloudGen Firewall.



Verify the intended traffic is using the intended transport by checking the **SD-WAN ID** column in **Firewall > Live** and **Firewall > History** .



Figures

1. VPN_group_settings.png
2. gti_ti_01.png
3. gti_ti_02.png
4. gti_ti_04.png
5. gti_ti_03.png