How to Configure Traffic Intelligence Using the VPN GTI Editor

https://campus.barracuda.com/doc/73719491/

Traffic Intelligence (TI) 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 TI 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 Traffic Intelligence.

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 Traffic Intelligence, 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.

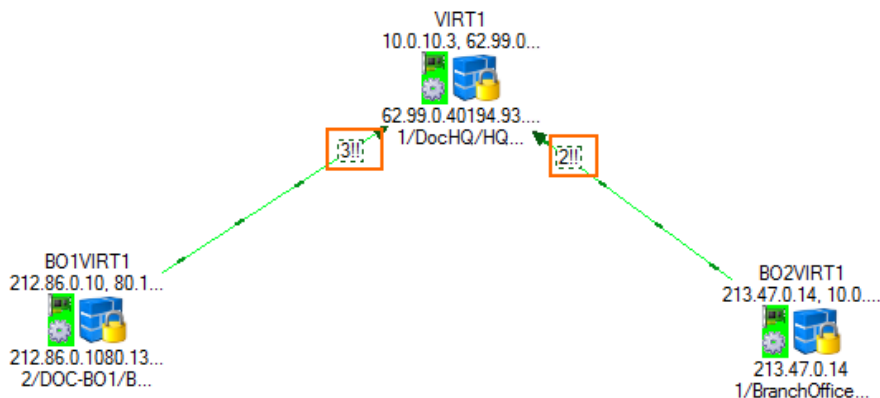| Traffic Intelligence	
TI - Bandwidth Protection	
Dynamic Bandwidth Detection	Active Probing and Passive Monitoring
Bandwidth Policy	Consolidated Shaping with Assign QoS Pr...
Assigned QoS Profile	
Estimated Bandwidth	
Forward [KBit/sec]	60000
Reverse [KBit/sec]	7500

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:
   - **TI Classification** – Select **Bulk**, **Quality** or **Fallback**.
   - **TI-ID** – Select the Traffic Intelligence ID**.** Each TI 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 **TI-ID** set to 0. For example: *bulk0* or *quality0*.

Step 3. Create Connection Objects to Use VPN Transports

To choose a specific TI 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 master for the VPN connection. You must configure one master and one slave for the VPN connection. For more information, see Traffic Intelligence.

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. Click **Edit/Show** in the **VPN Traffic Intelligence (TI) Settings** section. The **TI Settings** window opens.

7. Configure the **TI Transport Selection:**
   - **Transport Selection Policy** – Select the transport according to the link quality metrics gathered by Dynamic Bandwidth Detection. For more information, see Traffic Intelligence

and [How to Configure Performance-Based Transport Selection for VPN Tunnels with Traffic Intelligence](#).

- **TI Learning Policy** – One VPN service is the master, the other the slave. The TI settings in the connection object of the master will override the TI settings of the slave.
- **Primary Transport Class** – Select the TI class of the primary transport.
- **Primary Transport ID** – Select the ID for the primary transport.
- **Secondary Transport Class** – Select the TI class of the secondary transport.
- **Secondary Transport ID** – Select the ID for the secondary transport.
- **Further Tries Transport Selection Policy** – 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 [Traffic Intelligence](#) and [How to Configure Session Balancing for VPN Tunnels with Traffic Intelligence](#).
- **Traffic Duplication (FEC)** – Select to duplicate and simultaneously send VPN traffic over two transports. For more information, see [Traffic Intelligence](#) and [How to Configure Traffic Duplication for VPN Tunnels with Traffic Intelligence](#).

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 Traffic Intelligence 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.

Name	Tunnel	Local	Peer	Info	Transport	Encryption	Auth.	Compression	bps10	Total	Idle	Start	Key
⊟ **BO2VIRT1-VIRT1 (2)**													
BO2VIRT1-VIRT1	**TINA**	62.99.0.40	213.47.0.14		UDP	AES 128	SHA	0%	296 B	505 K	0 s	72 m	2 m
Bulk (1)		62.99.0.40	213.47.0.14		UDP	AES 128	SHA	0%	0 B	0 K	65 m	65 m	5 m
⊟ **BO1VIRT1-VIRT1 (3)**													
BO1VIRT1-VIRT1	**TINA**	62.99.0.40	212.86.0.10		UDP	AES 128	SHA	0%	296 B	502 K	0 s	72 m	2 m
Quality (2)		194.93.0.10	212.86.0.10		TCP & UDP	3DES	SHA 256	0%	0 B	0 K	72 m	72 m	2 m
Fallback (3)		194.93.0.10	80.130.45.10		ESP & UDP	AES 256	SHA 512	0%	0 B	0 K	59 m	59 m	9 m
⊟ **/ single transport tunnel (2)**													
VIRT1-AWSVIRT1	TINA	194.93.0.10	54.229.172.87		TCP	AES 128	SHA	0%	0 B	0 K	72 m	72 m	2 m
VIRT1-AzureVS1	TINA	62.99.0.40	23.101.73.15		TCP	AES 128	SHA	0%	0 B	0 K	72 m	72 m	2 m

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

ID	State	IP ...	Source	Interface	Destination	Output-IF	A...	Type	QoS	Rule	Bit/s	Total	Idle	TI ID
‖... 4326	⇄ 🛡	ICMP	10.0.10.11	eth0	10.0.81.200	vpn0@FW2FW-BO2VIRT1-VIRT1		FWD	VOIP /	🔧 HQ-2-BO1-2	960	504.2 K	0s	B0

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