How to Configure Traffic Intelligence Using the VPN GTI Editor

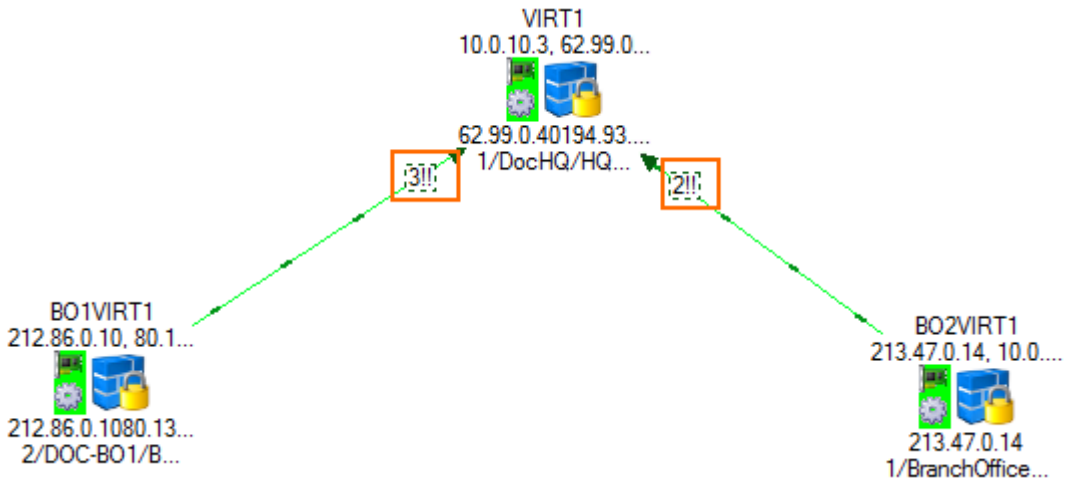
https://campus.barracuda.com/doc/48203312/

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. Depending on the type of traffic, you can decide which transport route should be used and what kind of fallback should be provided if one of the transport routes goes down. You can use the GTI editor to add additional IPv4 and IPv6 transports to TINA VPN tunnels.

Step 1. 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 on a VPN tunnel.
5. Click on **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 only be used once per VPN tunnel.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

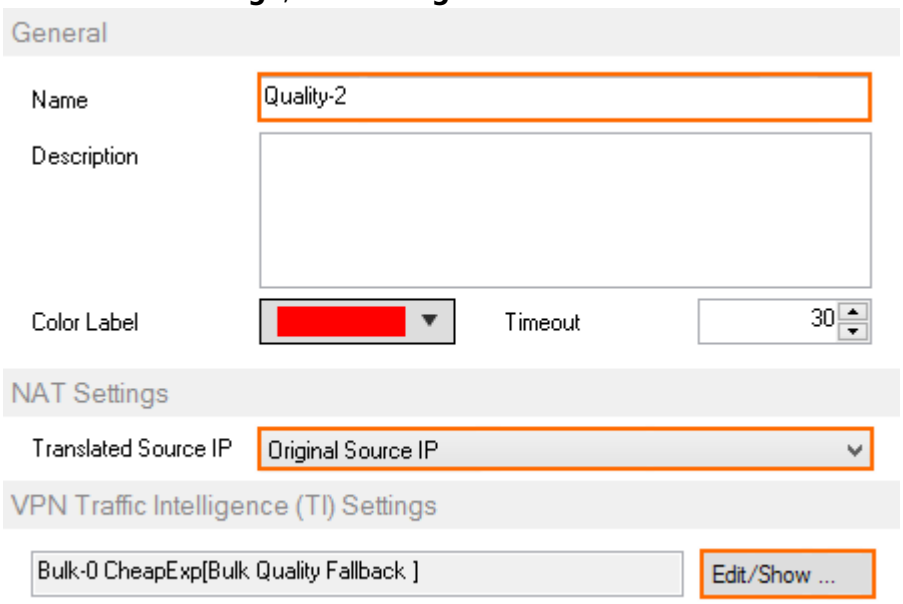
The number of VPN transports for a VPN tunnel is now displayed in the GTI editor map. E.g., two transports: **2!!**



Step 2. 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 in for the VPN connection. You must configure one master and one slave for the VPN connection. For more information, see Traffic Intelligence.

1. Create a new custom Connection Object object in the Forwarding Firewall service for each location. For more information, see How to Create a Custom Connection Object.
   In the **NAT Settings**, select **Original Source IP**.



2. Click **Edit/Show** in the **VPN Traffic Intelligence (TI) Settings** section. The **TI Settings** window opens.
3. Configure the **TI Transport Selection:**
   - **Preferred Transport Class** – Select the transport class you configured for the VPN transport.
   - **Preferred Transport ID** – Select the transport ID you configured for the VPN transport.
   - **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.
   - **Advanced TI Settings** – Configure failover, backup transports, session balancing and priority levels of transports.

Setting	Description

Preferred Transport Class | Preferred Transport ID	Select a transport class and transport ID for the preferred VPN transport. If the preferred VPN transport goes down, the session is switched seamlessly to the backup VPN transport specified by the **Second Try Transport Class** and **Second Try Transport ID** settings.
Second Try Transport Class | Second Try Transport ID	Select a transport class and transport ID for the backup VPN transport. The backup VPN transport is used when the preferred VPN transport goes down.
Balance Sessions	Specifies how many transports and/or which transports are used to balance the session.
Further Tries Transport Selection Policy	Specifies which transports should be used if the backup VPN transport fails. You can select of the following predefined policies: ■ First try Cheaper then try Expensive ■ Only Cheaper ■ Only Expensive ■ Stay on transport (no further tries) Depending on the available VPN transports, you can define more than one backup path.
TI Learning Policy	The **TI Learning Policy** setting is required because the traffic selection of VPN transport assignment is done by a matching firewall rule of the Firewall service. Because a firewall is required for each end of the site-to-site tunnel, different settings can be configured for the preferred VPN transport at each site. To prevent this, define one site as the master site that synchronizes its **TI Transport Selection** settings with those of its partner site.
Allow Bulk Transports | Allow Quality Transports | Allow Fallback Transports	To limit the classes that can be used for a backup path when you enable the **Further Tries Transport Selection Policy** setting, select or clear these check boxes.
When using BULK Transports	The priority level for the Bulk transport class. This setting only applies to bandwidth protected VPNs.
When using QUALITY Transports	The priority level for the Quality transport class. This setting only applies to bandwidth protected VPNs.

4. Click **OK**.
5. Click **OK**.

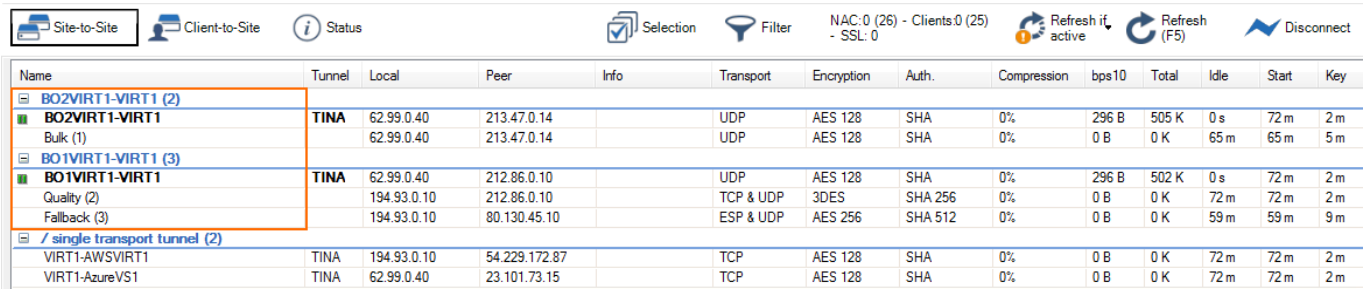
Make sure you are using the connection objects on both NextGen F-Series Firewalls.

Step 3. Assign access rules to use the Traffic Intelligence connection objects

You must modify access rules which allow traffic to enter and exit the VPN tunnel to use the custom connection objects created in Step 2.

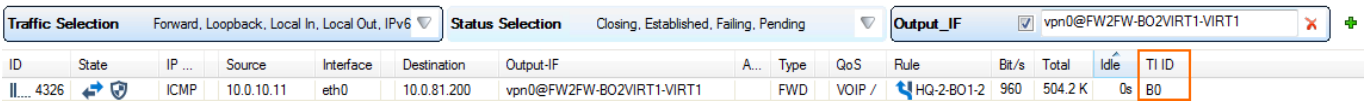
Monitoring

Each VPN transport is listed on the **VPN > Site-to-Site** and **VPN > Status** pages when logged directly in to the NextGen Firewall F-Series.



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. gti_ti_01.png
2. gti_ti_02.png
3. gti_ti_04.png
4. gti_ti_03.png