How to Configure VPN Traffic Intelligence

https://campus.barracuda.com/doc/46209406/

To implement Traffic Intelligence, you must create a connection object and configure the Traffic Intelligence settings. You can then use the connection object in the access rules for the TINA VPN tunnels.

All settings configured in the following section only apply to Traffic Intelligence configuration in combination with the TINA VPN tunnel. For more information, see How to Create a TINA VPN Tunnel between F-Series Firewalls.

Step 1: Add Transport to the VPN Tunnel

In order to use Traffic Intelligence, you can add one or multiple transports to your VPN tunnel on both locations. To add additional transports to a VPN tunnel, proceed as follows:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site**.
2. Click **Lock**.
3. Click the **TINA Tunnels** tab.
4. Right click an existing TINA VPN tunnel and select **Add Transport** from the context menu.
5. Select **Bulk, Quality** or **Fallback** from the **TI Classification** drop down menu and adjust all further settings as needed. For further information on transport classification, see VPN Transport Classification
6. In the **Call Direction** section, select one of the following options.
   - **Active** – The transport actively initiates connections but also accepts connection requests. When the transport is down for a defined time, it cleans its state to accept retries from its partner.
   - **Passive –** A passive transport does not actively initiate a connection. It merely accepts requests from its partner. If the tunnel is down for a defined time, it cleans its state to accept retries from its partner.
   - **OnDemand –** The transport actively initiates a connection and terminates it during the time-outs specified by the **On Demand Transport** settings in the **TI - VPN Envelope Policy** tab.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 2: Create a Connection Object

1. Create a new connection object.
2. In the **VPN Traffic Intelligence (TI) Settings** section of the **Edit / Create a Connection Object** configuration window, click **Edit/Show**.
3. Specify the following settings:

Setting	Description
Preferred Transport Class | Preferred Transport ID	From these lists, select a transport class and transport ID for the preferred VPN transport. For more information, see VPN Transport Classification. 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	From these lists, 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 the session is balanced, depending on the amount of transport.
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 additional 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 **Send Changes** and **Activate**.

Step 3: Adjust the Firewall Ruleset

After configuring the Traffic Intelligence settings in the connection object, assign the connection object to the firewall rules. For more information, see How to Create Access Rules for Site-to-Site VPN Access.