How to Add a VPN Transport to a TINA VPN Tunnel with Explicit Transport Selection

https://campus.barracuda.com/doc/73719192/

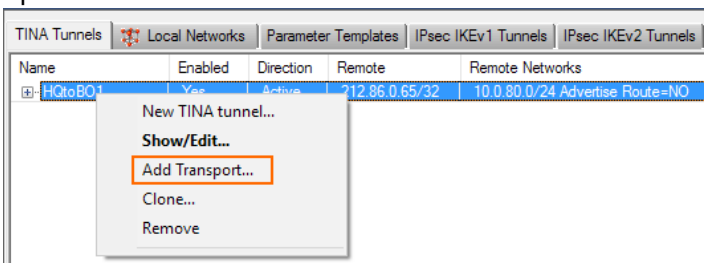
Add multiple VPN transports to your TINA site-to-site VPN tunnel to use Traffic Intelligence (TI). The TI settings in the access rules matching the traffic determine which transport is used.

Before You Begin

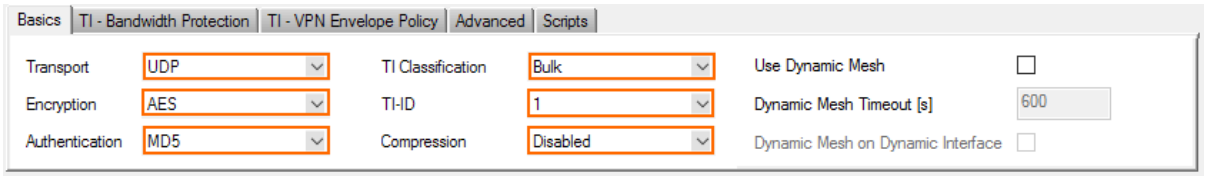
Create a TINA site-to-site VPN tunnel between two CloudGen Firewalls. For more information, see How to Create a TINA VPN Tunnel between CloudGen Firewalls.

Step 1. Add a Transport to the VPN Tunnel

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN Service > Site to Site**.
2. Click **Lock**.
3. Right-click an existing TINA VPN tunnel and select **Add Transport**. The **TINA Tunnel** window opens.

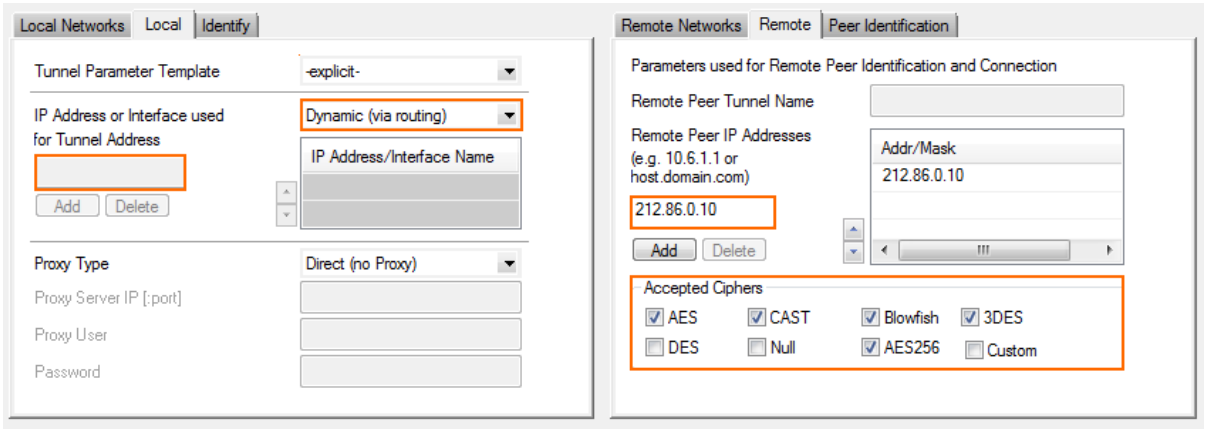


4. (IPv6 only) Select the **IPv6** check box. IPv6 is supported only for the VPN envelope.
5. Configure the **Basic** TINA tunnel settings. For more information, see TINA Tunnel Settings.
   - **Transport** – Select the transport encapsulation: **UDP** (recommended), **TCP**, **TCP&UDP**, **ESP**, or **Routing**.
   - **Encryption** – Select the encryption algorithm: **AES**, **AES256**, **3DES**, **CAST**, **Blowfish**, **DES**, or **Null**.
   - **Authentication** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, **SHA512**, **NOHASH**, **RIPEMD160**, or **GCM**.
   - **TI Classification** – Select the TI classification.
   - **TI-ID** – Select the TI ID. Each TI class/ID combination can be used only once.
   - **Compression** – Select **Packet** or **Stream** compression. Do not use in combination with WAN Optimization.



6. In the **Direction** tab, select the **Call Direction** from the drop-down list. At least one of the firewalls must be active.

   Configure the CloudGen Firewall with a dynamic IP address to be the active peer. If both firewalls use dynamic IP addresses, a DynDNS service must be used. For more information, see How to Configure VPN Access via a Dynamic WAN IP Address.
7. Click the **Local** tab, and configure the **IP address or Interface used for Tunnel Address**:
   - **(IPv4 only) First Server IP** – First IP address of the virtual server the VPN service is running on.
   - **(IPv4 only)Second Server IP** – Second IP address of the virtual server the VPN service is running on.
   - **Dynamic (via routing)** – The firewall uses a routing table lookup to determine the IP address.
   - **Explicit List (ordered)** – Enter one or more explicit IP addresses. Multiple IP addresses are tried in the listed order.
   - In the **Remote** tab, enter either one or more IPv4 or IPv6 addresses or an FQDN as the **Remote Peer IP Addresses,** and click **Add**.



8. In the **Remote** tab, select the **Accepted Ciphers**. The list of accepted ciphers must contain the cipher selected in the previously configured **Encryption** settings.
9. (optional) Click the **Identity** tab and configure the **Identification Type** and **Server Protocol Key** for this transport. By default, the **Identity** settings of the TINA tunnel is used.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

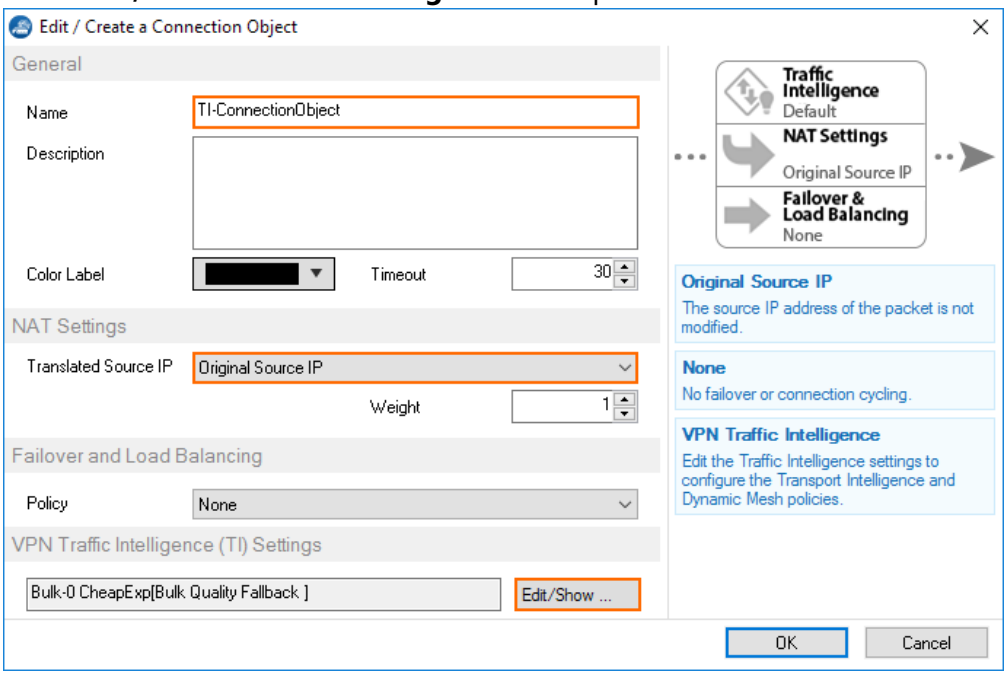
Step 2. Add the VPN Transport on the Remote Firewall

Duplicate the VPN transport configuration on the remote firewall. At least one firewall must be configured to use an active call direction.

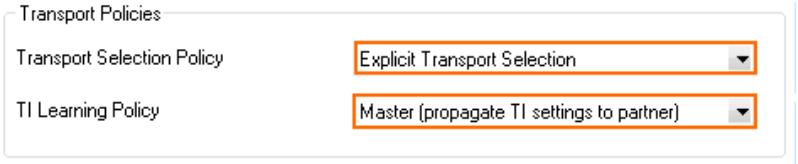
Step 3. Create a Custom Connection Object for the TI Master

Create a custom connection object to route traffic into the new VPN transport and configure the firewall as a TI master.

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**. The **TI Settings** window opens.

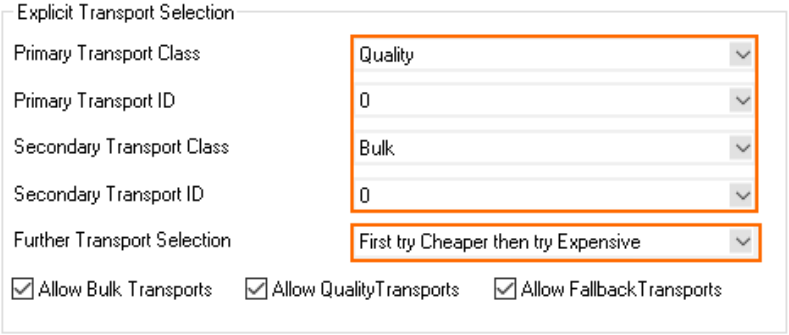


7. From the **Transport Selection Policy** drop-down list, select **Explicit Transport Selection**.
8. From the **TI Learning Policy** drop-down list, select **Master (Propagated TI settings to partner)**.



9. Configure the **Explicit TI Transport Selection** policy:
   - **Primary Transport Class** – Select the default transport class for the traffic matching this rule.
   - **Primary Transport ID** – Select the default transport ID for the traffic matching this rule.
   - **Secondary Transport Class** – Select the backup transport class.
   - **Secondary Transport ID** – Select the backup transport ID.

- **Further Transport Selection** – Select the transports that are used if the primary and secondary VPN transports 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)**
- **Allow Bulk Transports | Allow Quality Transports | Allow Fallback Transports** – Enable all transport classes that can be used as a backup path in combination with the **Further Transport Selection** setting.

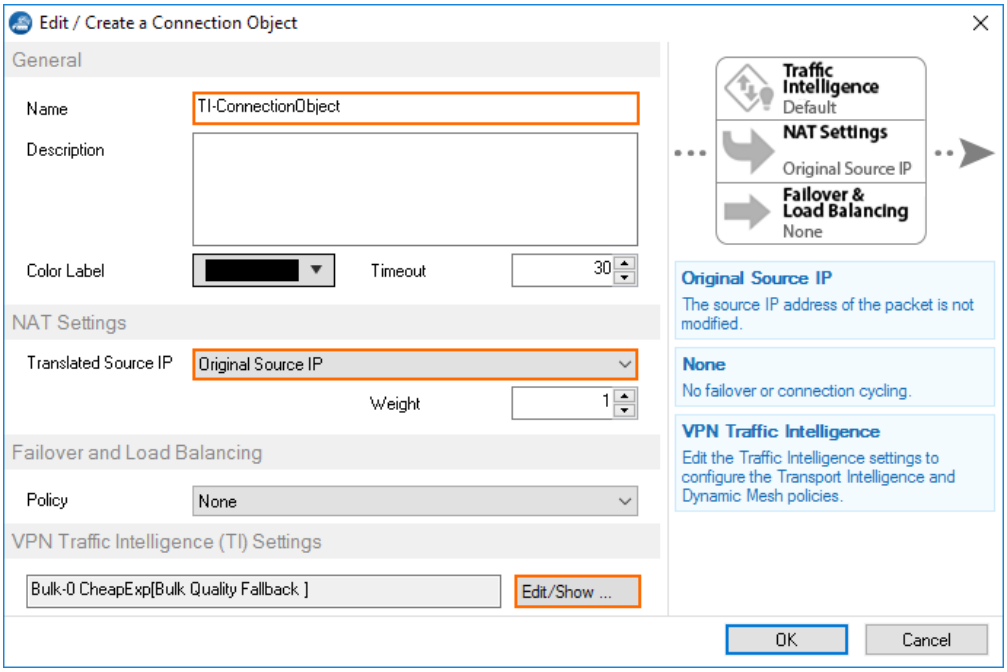


10. (TCP transports only) Configure **TCP Transport Traffic Prioritization** settings:
    - **When using BULK Transports** – The priority level for the bulk transport class.
    - **When using QUALITY Transports** – The priority level for the quality transport class.
11. (Dynamic Mesh only) Configure the **Dynamic Mesh** settings. For more information, see Dynamic Mesh VPN Networks.
12. Click **OK**.
13. Click **OK**.
14. Click **Send Changes** and **Activate**.

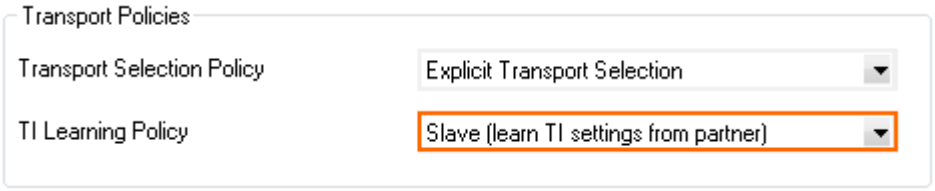
Step 4. Create a Custom Connection Object for the TI Slave

Create a custom connection object to route traffic into the new VPN transport and configure the firewall as a TI slave.

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**. The **TI Settings** window opens.



7. From the **TI Learning Policy** drop-down list, select **Slave**. All other TI settings are learned from the TI master.



8. Click **OK**.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 3. Edit Access Rules Matching the VPN Traffic

Edit the access rules matching the VPN traffic on both firewalls to use the custom connection objects. If multiple firewalls are connected in a hub and spoke VPN network, the firewall acting as the VPN hub must be the TI master. Create multiple access rules and connection objects to statically route VPN traffic through different VPN transports.

For more information, see How to Create Access Rules for Site-to-Site VPN Access.

Next Steps

Configure advanced Traffic Intelligence features such as:

- How to Configure Adaptive Bandwidth Protection for VPN Tunnels with Traffic Intelligence
- How to Configure Session Balancing for VPN Tunnels with Traffic Intelligence
- How to Configure Traffic Duplication for VPN Tunnels with Traffic Intelligence
- How to Configure Performance-Based Transport Selection for VPN Tunnels with Traffic Intelligence

Figures

1. ti_add_transport_01.png
2. ti_add_transport_02.png
3. ti_add_transport_03.png
4. ti_add_transport_04.png
5. ti_add_transport_04a.png
6. ti_add_transport_04b.png
7. ti_add_transport_04.png
8. ti_add_transport_05a.png