How to Configure a Dynamic Mesh VPN with the GTI Editor

The GTI editor greatly simplifies creating a dynamic mesh VPN network with a large number of NextGen F-Series Firewalls. You can enable dynamic mesh for all VPN services directly in the VPN group. To initiate a dynamic tunnel, traffic must match access rules that use dynamic-mesh-enabled custom connection objects on the NextGen Firewall F-Series acting as the VPN hub. Dynamic Mesh is not supported for VPN services using IPv6.

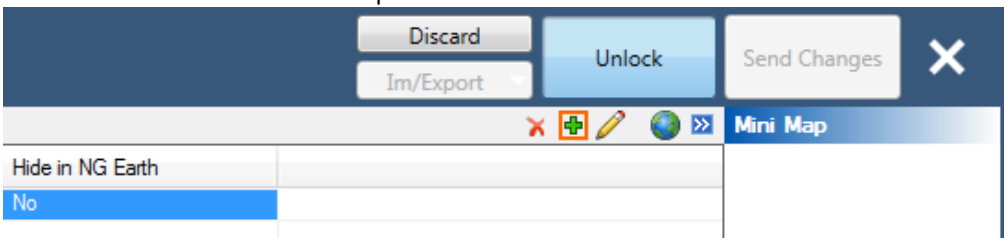
Before You Begin

- For each VPN service in the VPN Group, go to the **VPN Settings** and verify that **Allow Dyn Mesh** is set to **yes**.
- Configure the GTI Settings for each VPN service. For more information, see How to Configure VPN GTI Settings for a VPN Service.
- The VPN service that is to be used as the VPN hub must have all remote and local networks entered as **Server/GTI Networks**.
- Configure the GTI Settings for the VPN services on the managed firewalls. For more information, see How to Configure VPN GTI Settings for a VPN Service.

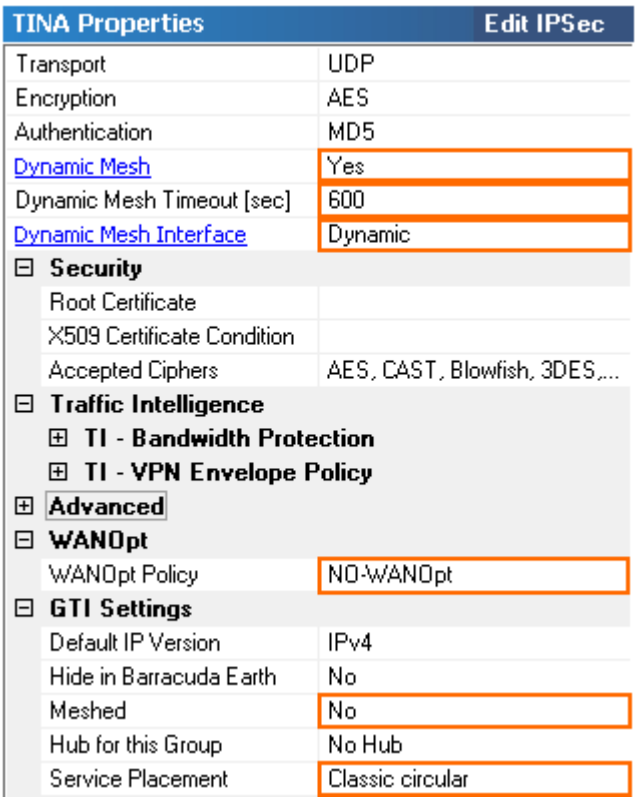
Step 1. Create a VPN Group

VPN Groups contain the default settings for all VPN tunnels in the group and the list of VPN services used to create the tunnels.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > VPN GTI Editor**.
2. Click **Lock**.
3. Click **+** to add a new VPN Group.



4. Enter the **Name**.
5. Click **OK**. The **Group** window opens.
6. Edit the default **TINA** settings:
   - **Transport** – Select **UDP**, **TCP** or **ESP**.
   - **Encryption** – Select the default encryption cipher.
   - **Authentication** – Select the default authentication hash.
   - **Dynamic Mesh** – Set to **yes**.
   - **Dynamic Mesh Interface** – Default is **Static**. Select **Dynamic** if the firewall is behind a NAT device.
   - **Dynamic Mesh Timeout** – Enter the number of seconds before a dynamic tunnel is terminated.
   - **WANOpt Policy** – Select **NO-WANOpt**. WAN Optimization cannot be used in combination with Dynamic Mesh.
   - **Meshed** – Set to **no**.
   - **Service Placement** – Select **Classic circular** to automatically arrange all VPN services in a circular pattern. If one service is selected as the VPN hub, it is placed in the center of the circle. **User** allows the user to arrange the VPN services.



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

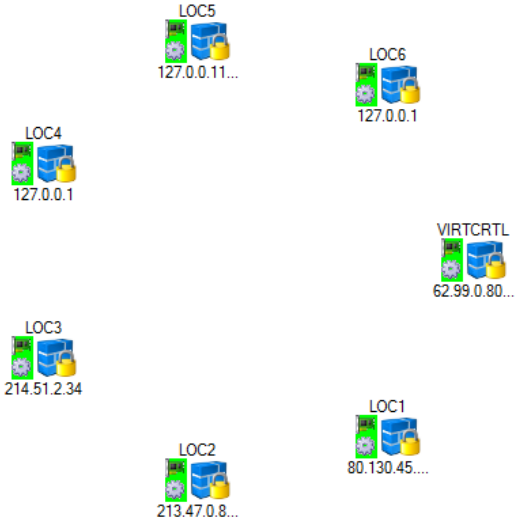
Step 2. Add VPN Services to the VPN Group

Add the VPN services to the VPN group. If you are using the GTI editor on the range or cluster level, add VPN services to the VPN group only from the range or cluster you are in.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > VPN GTI Editor**.
2. Click **Lock**.
3. In the **Group** tab, click on the VPN group. The VPN group name is displayed in the top status bar of the GTI map.

4. Click on the **Services** tab.
5. In the taskbar, select both **Group** and **Other** button.

6. Select all VPN services you want to add to the VPN group.
7. Right-click and select **Add to current Group**. The VPN services are added to the map area below.

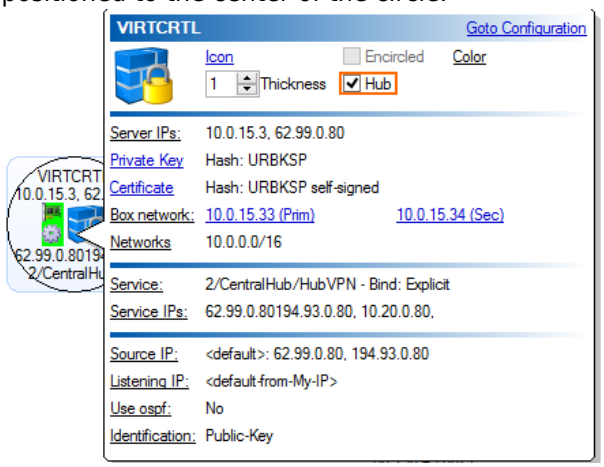


8. Click **Send Changes** and **Activate**.

Step 2. Select the VPN Hub

Select the VPN service that will act as a VPN hub.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > VPN GTI Editor**.
2. Click **Lock**.
3. Click on the VPN service you want to use as a VPN hub, and select **Hub**. The VPN Service icon is re-positioned to the center of the circle.

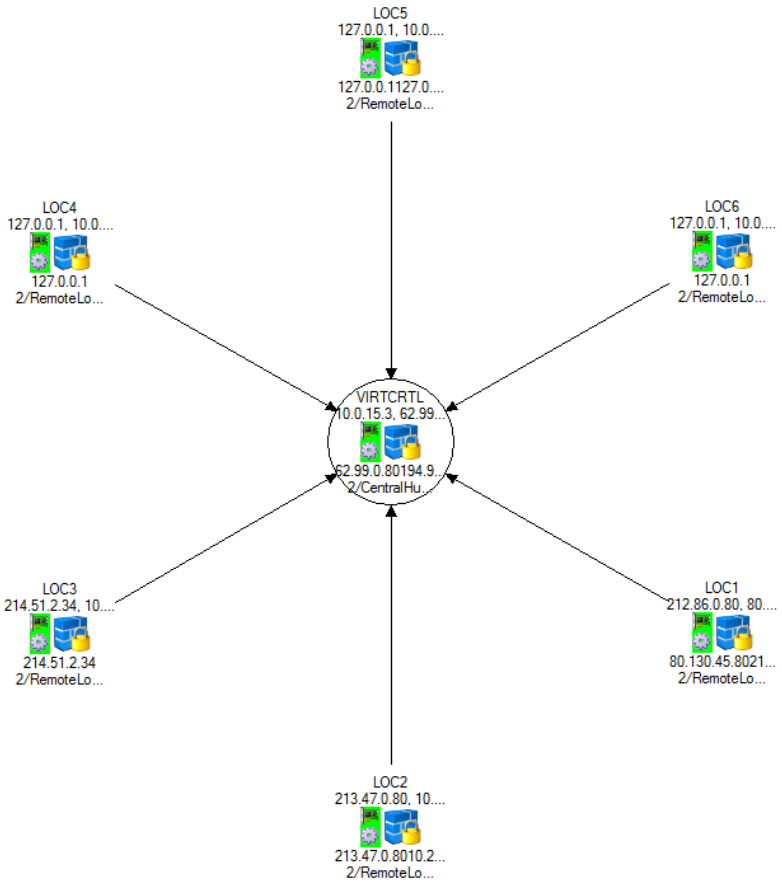


4. Click **Send Changes** and **Activate**.

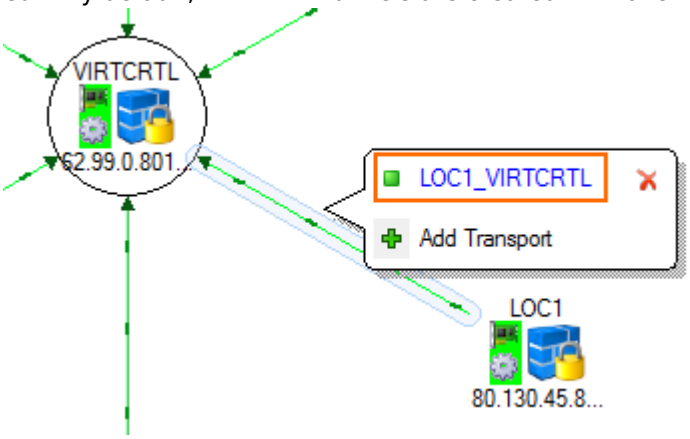
Step 3. Create VPN Tunnels to the VPN Hub

Create VPN tunnels from every NextGen Firewall F-Series to the central VPN hub.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > VPN GTI Editor**.
2. Click **Lock**.
3. For every VPN service, create a tunnel by click-and-drag from the VPN service in the circle to the VPN hub.



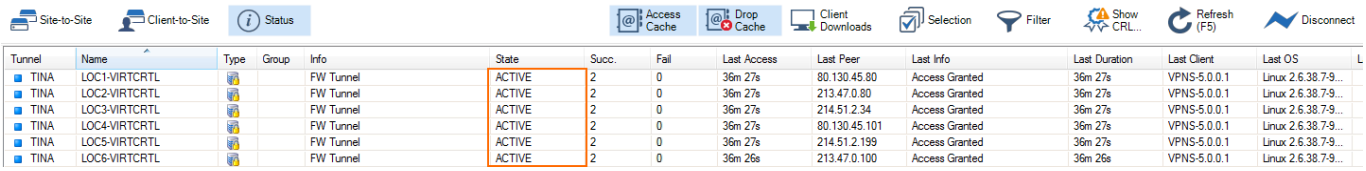
4. (optional) Click on the connection between the two VPN services and click on the transport you want to edit. By default, TINA VPN tunnels are created with one transport.



5. You can now modify the VPN tunnel as needed:
   - **Direction** – You can create VPN tunnels that use the following modes: **active-active**, **active-passive**, **on-demand**.
   - **Transport Source IP/Interface** – If needed, you can modify the transport source IP.
   - **Transport Listening IP/Interface** – Reorder the IP addresses so the first IP addresses of every VPN service can reach the Transport Listening IP addresses of all other VPN services.

     Dynamic Mesh uses the first Transport Listening IP address listed to create the dynamic tunnel.
6. Click **Send Changes** and **Activate**.

Go to the **VPN > Site to Site** and verify that all tunnels are up.



Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info	Last Duration	Last Client	Last OS
TINA	LOC1-VIRTCRTL			FW Tunnel	ACTIVE	2	0	36m 27s	80.130.45.80	Access Granted	36m 27s	VPNS-5.0.0.1	Linux 2.6.38.7-9...
TINA	LOC2-VIRTCRTL			FW Tunnel	ACTIVE	2	0	36m 27s	213.47.0.80	Access Granted	36m 27s	VPNS-5.0.0.1	Linux 2.6.38.7-9...
TINA	LOC3-VIRTCRTL			FW Tunnel	ACTIVE	2	0	36m 27s	214.51.2.34	Access Granted	36m 27s	VPNS-5.0.0.1	Linux 2.6.38.7-9...
TINA	LOC4-VIRTCRTL			FW Tunnel	ACTIVE	2	0	36m 27s	80.130.45.101	Access Granted	36m 27s	VPNS-5.0.0.1	Linux 2.6.38.7-9...
TINA	LOC5-VIRTCRTL			FW Tunnel	ACTIVE	2	0	36m 27s	214.51.2.199	Access Granted	36m 27s	VPNS-5.0.0.1	Linux 2.6.38.7-9...
TINA	LOC6-VIRTCRTL			FW Tunnel	ACTIVE	2	0	36m 26s	213.47.0.100	Access Granted	36m 26s	VPNS-5.0.0.1	Linux 2.6.38.7-9...

Step 4. (optional) Add Transports to the VPN Tunnels

If you are using multiple Internet connections, you can use Traffic Intelligence to create multiple transports for the VPN tunnels. The dynamic tunnels consolidate the static VPN tunnels into one transport per TI class (e.g., bulk0 or quality0), instead of replicating their transport configuration. This also means you have to configure all firewalls except the VPN hub to act as a TI slave. The transport is then chosen by the connection object of the NextGen Firewall F-Series initiating the connection.

For more information, see How to Configure Traffic Intelligence Using the VPN GTI Editor and Dynamic Mesh VPN Networks.

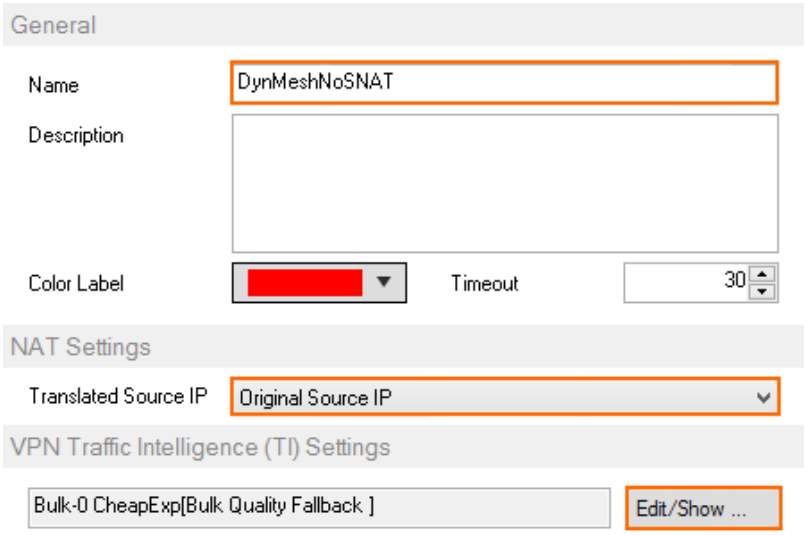
Step 5. Create Three Custom Connection Objects on the VPN Hub

You must create three custom connection objects on the VPN hub: one that triggers a dynamic tunnel and resets the tunnel timeout, one for traffic going through the dynamic tunnel while not resetting the tunnel timeout, and one for the traffic that should always be relayed through the VPN hub.

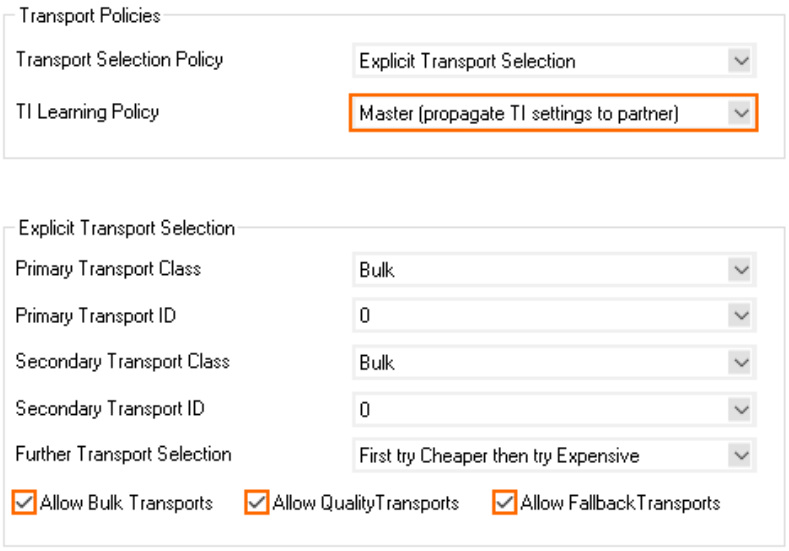
Step 5.1 Dynamic Mesh Connection Object TI Master with Idle Timeout Reset

Only connections matching an access rule with the dynamic mesh and TI master options enabled in the TI settings of the custom connection object on the VPN hub will trigger a new dynamic VPN tunnel. All other traffic will continue to go through the VPN hub. The connection objects on the remote units (TI slaves) do not need to be enabled because they are learned automatically from the VPN hub acting as the TI master. For traffic matching access rules using this connection object to keep the dynamic tunnel open, **Prevent tunnel timeout** must be enabled.

1. Go to ***your virtual server*** **> Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Right-click in the **Connections** and click **New > Connection**.
4. Enter a **Name**. E.g., DynMeshNoSNAT
5. Select **Original Source IP**.
6. In the **VPN Traffic Intelligence (TI)Settings)** section, click **Edit/Show**. The **TI Settings** window opens.



7. Set the **TI Learning Policy** to **Master (propagate TI settings to partner)**.
   In the **Dynamic Mesh** section, enable **Allow Dynamic Mesh** and **Trigger Dynamic Mesh**.
8. Enable **Prevent Tunnel Timeout**.



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

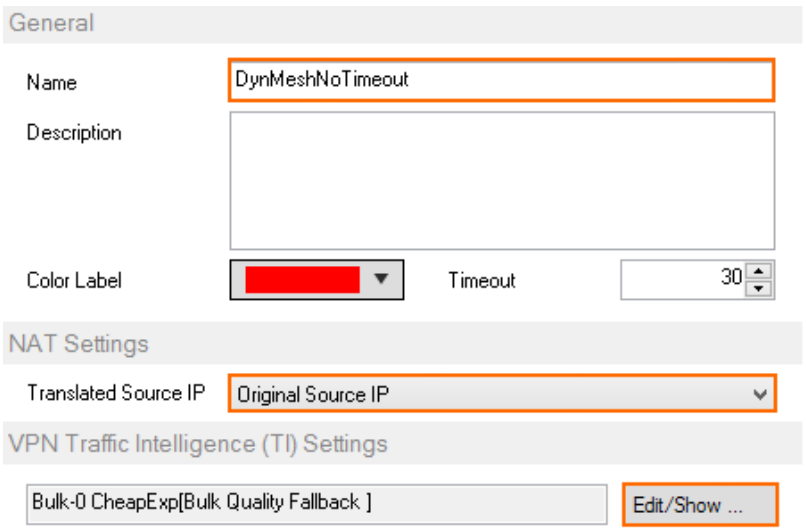
Step 5.2 Dynamic Mesh Connection Object TI Master with No Idle Timeout Reset

Only connections matching an access rule with the dynamic mesh and TI master options enabled in the TI settings of the custom connection object on the VPN hub will trigger a new dynamic VPN tunnel. All other traffic will continue to go through the VPN hub. The connection objects on the remote units (TI slaves) do not need to be enabled because they are learned automatically from the VPN hub acting as the TI master.

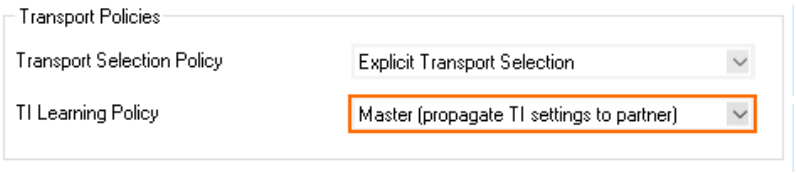
1. Go to ***your virtual server*** **> Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Right-click in the **Connections** and click **New > Connection**.
4. Enter a **Name**. E.g., `DynMeshNoTimeout`

5. Select **Original Source IP**.

6. In the **VPN Traffic Intelligence (TI)Settings)** section, click **Edit/Show**. The **TI Settings** window opens.



7. Set the **TI Learning Policy** to **Master (propagate TI settings to partner)**.



8. In the **Dynamic Mesh** section, enable **Allow Dynamic Mesh**.
9. Disable **Prevent tunnel timeout**.

10. Click **OK**.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

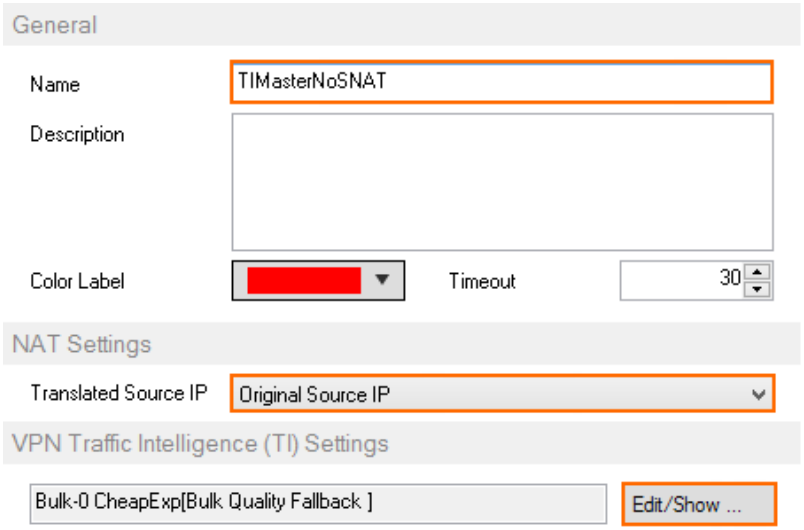
Step 5.3. Create a TI Master Connection Object for the VPN Hub for VPN Relaying

For all services that should not go through the VPN tunnel, use a custom connection object with the **TI Learning Policy** set to **Master**. Traffic matching an access rule that uses this connection object will not trigger a dynamic tunnel. Instead, it continues to go through the VPN hub.

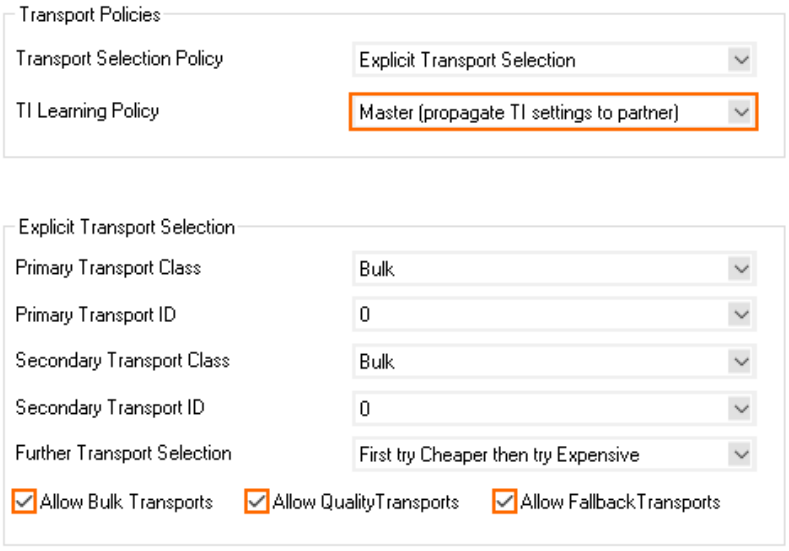
1. Go to ***your virtual server*** **> Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Right-click in the **Connections** and click **New > Connection**.
4. Enter a **Name**. E.g., `TIMasterNoSNAT`

5. Select **Original Source IP**.

6. In the **VPN Traffic Intelligence (TI)Settings)** section, click **Edit/Show.** The **TI Settings** window opens.



7. Set the **TI Learning Policy** to **Master (propagate TI settings to partner)**.
8. Verify all checkboxes in the **Dynamic Mesh** section are disabled.



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

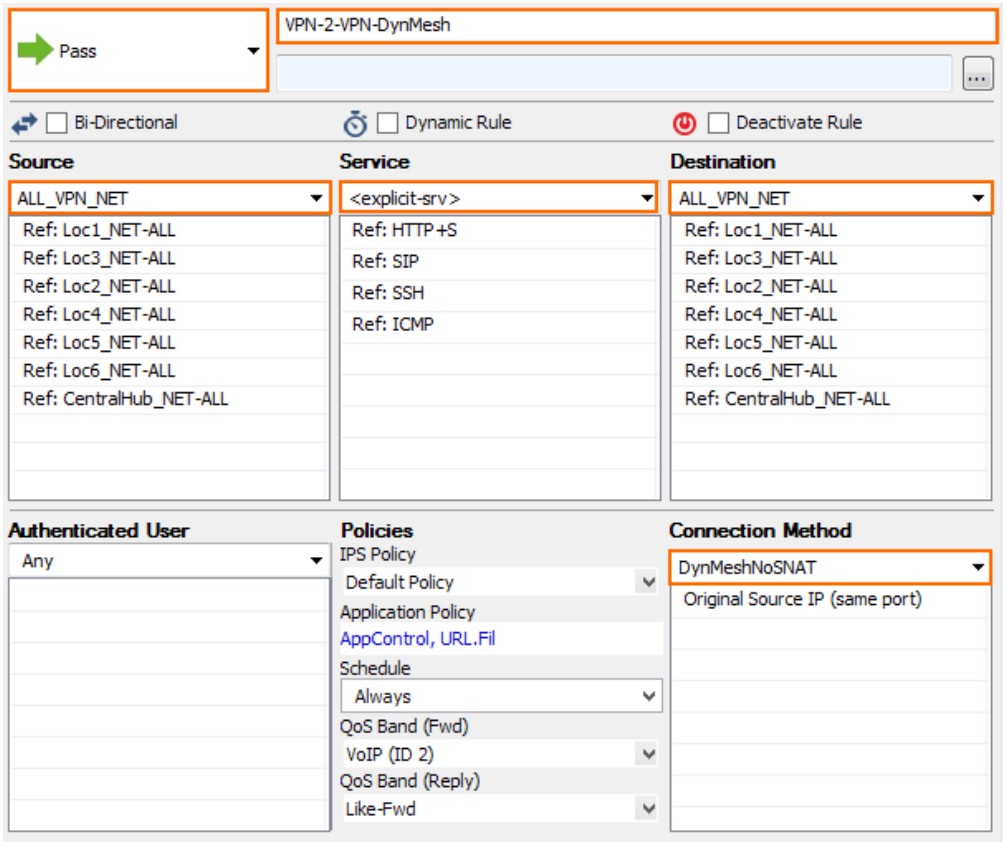
Step 6. Create three access rules on the VPN hub

Create an access rule that triggers the dynamic tunnel and another that relays the rest of the traffic.

Step 6.1. Create an Access Rule on the VPN Hub to Trigger a Dynamic Tunnel

Create an access rule on the VPN hub that will trigger a dynamic tunnel.

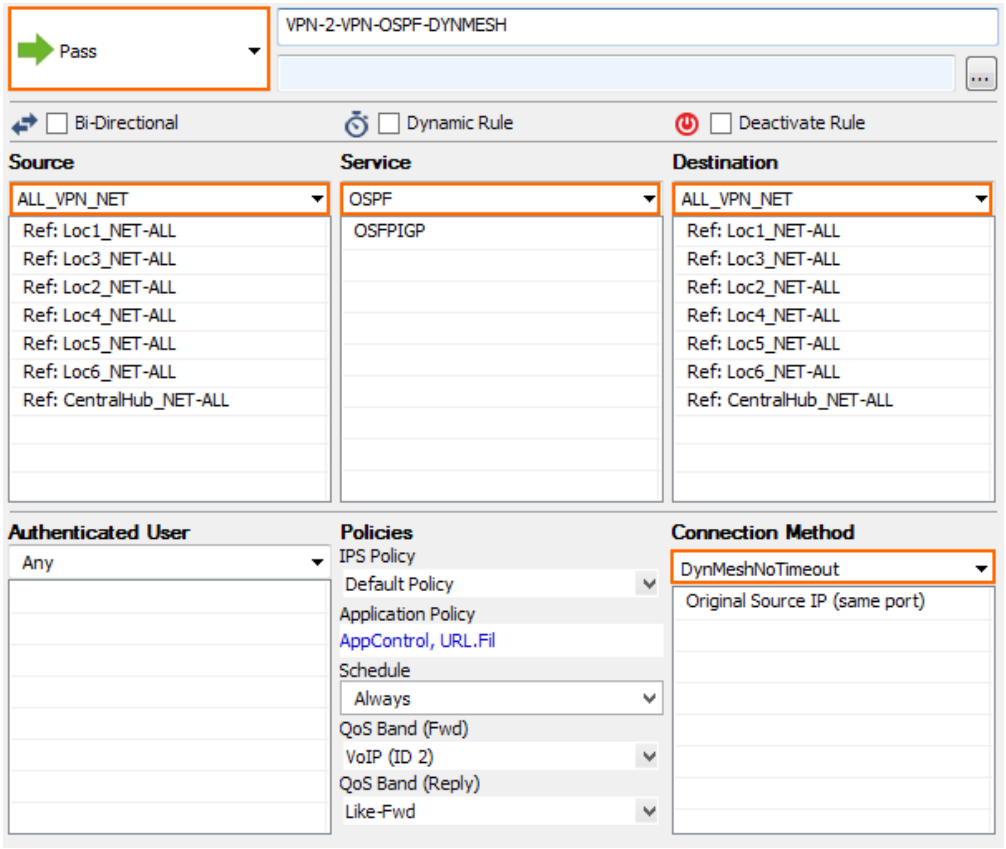
- **Action** – Select **PASS**.
- **Source** – Enter all **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Service** – Select the services that should trigger a dynamic tunnel.
- **Destination** – Enter all **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Connection Method** – Select the **DynMeshNoSNAT** custom connection object created in step 5.1.



Step 6.2. Create an Access Rule on the VPN Hub to Trigger a Dynamic Tunnel without Resetting the Idle Timeout of the Dynamic Tunnel

Create an access rule on the VPN hub that will trigger a dynamic tunnel.

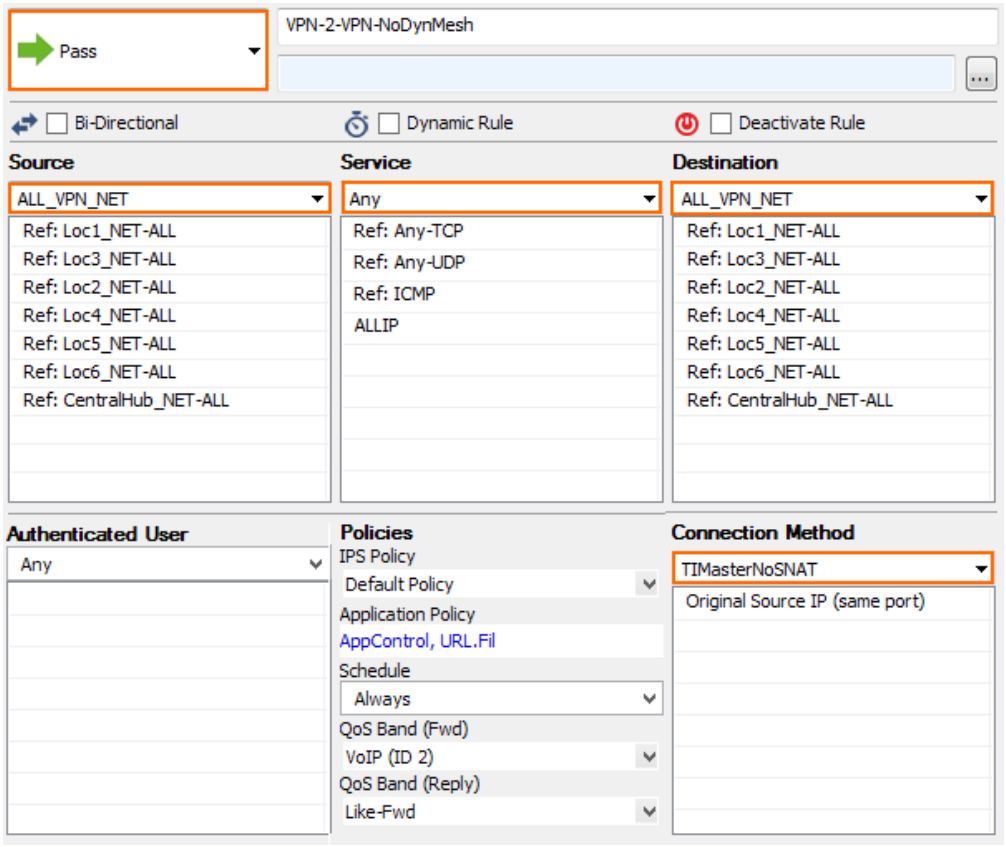
- **Action** – Select **PASS**.
- **Source** – Enter all **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Service** – Select the services that should go through the dynamic tunnel if it is up, otherwise go through the VPN hub.
- **Destination** – Enter all **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Connection Method** – Select the **DynMeshNoTimeout** custom connection object created in step 5.2.



Step 6.3. VPN Relaying Without Triggering a Dynamic Tunnel

Create an access rule on the VPN hub that allows the remote firewalls to send traffic to other remote firewalls through the VPN hub. Place this access rule below the rule triggering the dynamic tunnels.

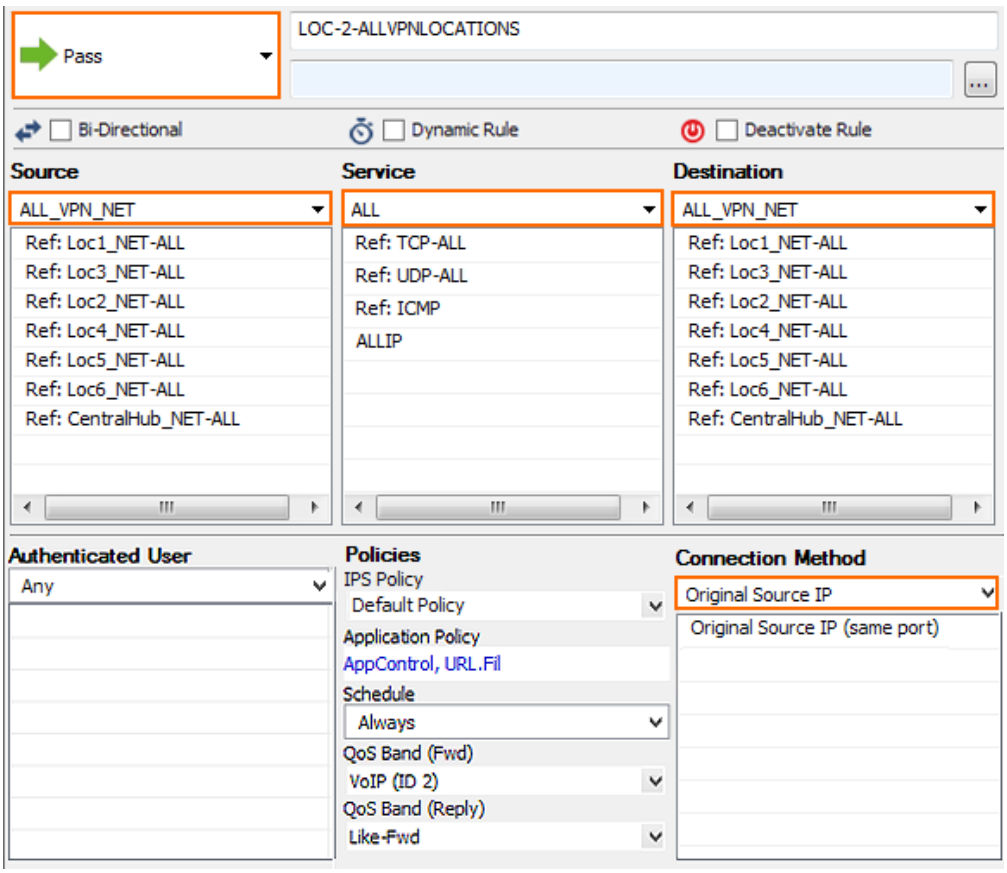
- **Action** – Select **PASS**.
- **Source** – Enter all **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Service** – Select **Any**.
- **Destination** – Enter all **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Connection Method** – Select the **TIMasterNoSNAT** custom connection object created in Step 5.2.



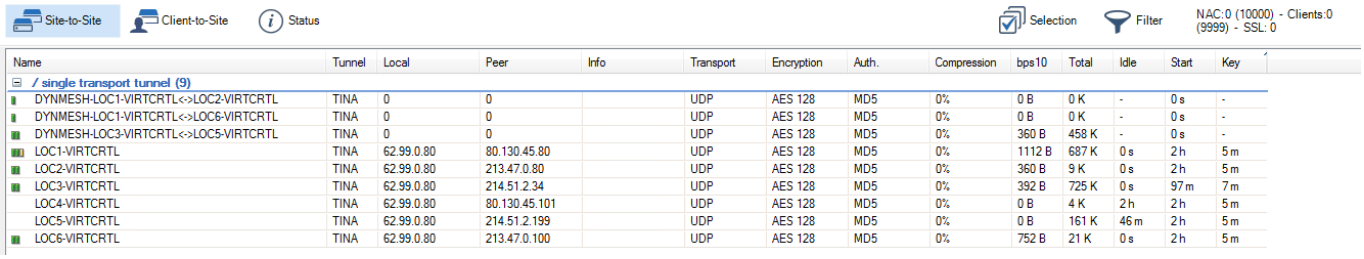
Step 7. Create Access Rules on the Remote Firewalls

Create an access rule to allow traffic into the VPN tunnel on every remote NextGen Firewall F-Series.

- **Action** – Select **PASS**.
- **Source** – Enter all **Local Networks**.
- **Service** – Select **Any** or the service that should go over the dynamic mesh.
- **Destination** – Enter all **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Connection Method** – Select **Original Source IP**. Verify that the **TI Learning Policy** is set to **Slave**.



You now have a dynamic mesh VPN network that automatically creates dynamic VPN tunnels when traffic matches an access rule using a dynamic-mesh-enabled connection object. Go to **VPN > Site-to-Site** to see all dynamic tunnels on the remote firewalls or on the VPN hub. Dynamic tunnels are terminated automatically after no traffic has passed through them for the **Dynamic Mesh Timeout** defined in the GTI VPN Group.



Name	Tunnel	Local	Peer	Info	Transport	Encryption	Auth.	Compression	bps10	Total	Idle	Start	Key
/ single transport tunnel (9)													
DYNMESH-LOC1-VIRTCRTL<->LOC2-VIRTCRTL	TINA	0	0		UDP	AES 128	MD5	0%	0 B	0 K	-	0 s	-
DYNMESH-LOC1-VIRTCRTL<->LOC6-VIRTCRTL	TINA	0	0		UDP	AES 128	MD5	0%	0 B	0 K	-	0 s	-
DYNMESH-LOC3-VIRTCRTL<->LOC5-VIRTCRTL	TINA	0	0		UDP	AES 128	MD5	0%	360 B	458 K	-	0 s	-
LOC1-VIRTCRTL	TINA	62.99.0.80	80.130.45.80		UDP	AES 128	MD5	0%	1112 B	687 K	0 s	2 h	5 m
LOC2-VIRTCRTL	TINA	62.99.0.80	213.47.0.80		UDP	AES 128	MD5	0%	360 B	9 K	0 s	2 h	5 m
LOC3-VIRTCRTL	TINA	62.99.0.80	214.51.2.34		UDP	AES 128	MD5	0%	392 B	725 K	0 s	97 m	7 m
LOC4-VIRTCRTL	TINA	62.99.0.80	80.130.45.101		UDP	AES 128	MD5	0%	0 B	4 K	2 h	2 h	5 m
LOC5-VIRTCRTL	TINA	62.99.0.80	214.51.2.199		UDP	AES 128	MD5	0%	0 B	161 K	46 m	2 h	5 m
LOC6-VIRTCRTL	TINA	62.99.0.80	213.47.0.100		UDP	AES 128	MD5	0%	752 B	21 K	0 s	2 h	5 m

Figures