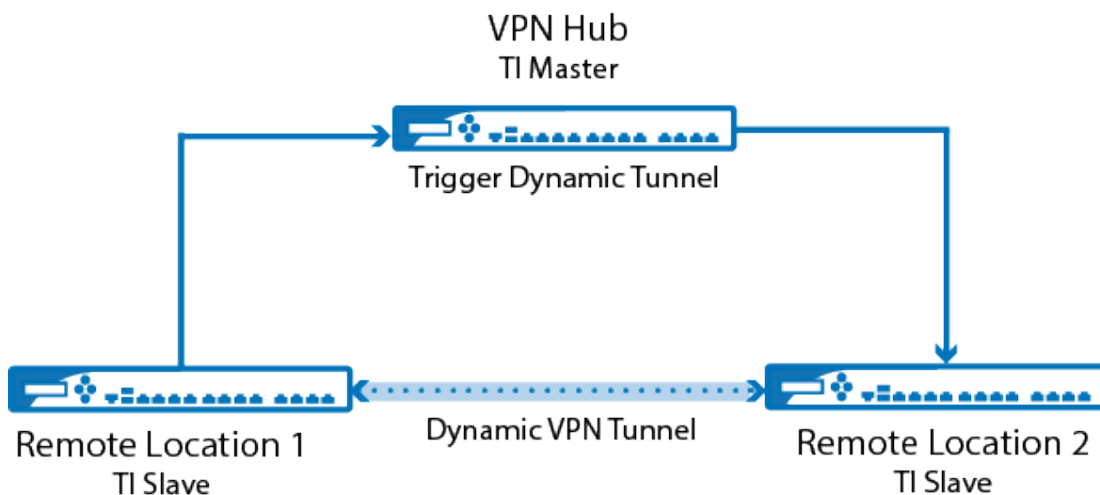


How to Configure Dynamic Mesh VPN

<https://campus.barracuda.com/doc/53248647/>

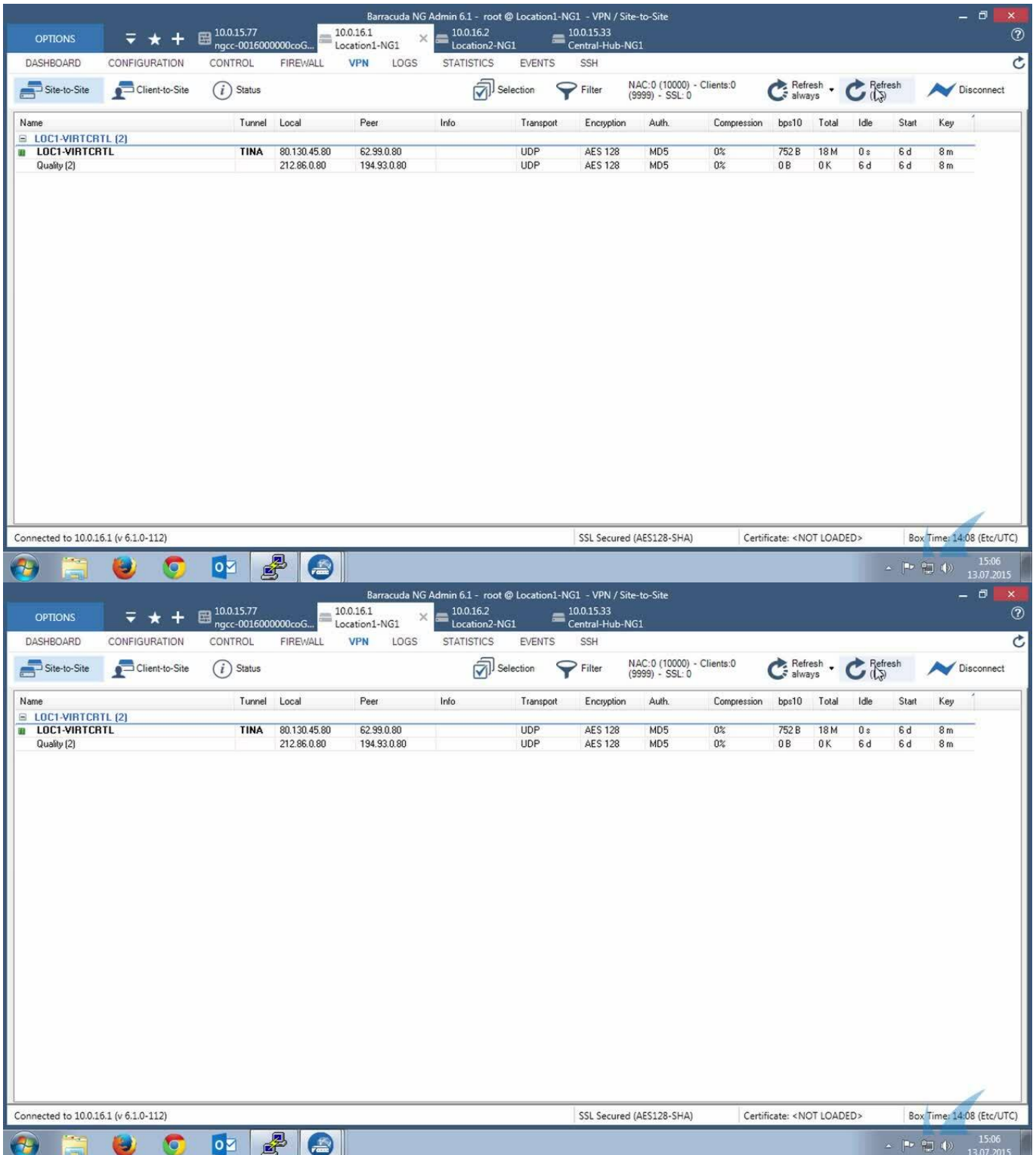
To configure a Dynamic Mesh for managed firewalls, see [How to Configure a Dynamic Mesh VPN with the GTI Editor](#).

Create a Dynamic Mesh network for three or more stand-alone Barracuda NextGen F-Series Firewalls with the central firewall acting as the VPN hub. Every firewall in the VPN Network must be configured to use Dynamic Mesh, and the VPN Hub must be the TI master and use a dynamic-mesh-enabled connection object for the access rule matching the VPN relay traffic. Dynamic Mesh can only be used in combination with TINA Site-to-Site tunnels. IPv6 envelope for the VPN tunnels is not supported.



Video

Watch the following video to see a Dynamic Mesh VPN in action:



The screenshot displays the Barracuda NG Admin 6.1 interface for Site-to-Site VPN configuration. The top navigation bar includes tabs for DASHBOARD, CONFIGURATION, CONTROL, FIREWALL, VPN, LOGS, STATISTICS, EVENTS, and SSH. The main content area shows a table of active VPN tunnels. The table has columns for Name, Tunnel, Local, Peer, Info, Transport, Encryption, Auth., Compression, bps10, Total, Idle, Start, and Key. Two tunnels are listed: LOC1-VIRTCTRL [2] and LOC1-VIRTCTRL Quality [2]. The first tunnel is in the TINA state with local IP 80.130.45.80 and peer IP 62.99.0.80. The second tunnel is also in the TINA state with local IP 212.86.0.80 and peer IP 194.93.0.80. Both tunnels use UDP transport, AES 128 encryption, MD5 authentication, and 0% compression. The interface also shows a status bar at the bottom indicating the connection is secured with AES128-SHA and the certificate is not loaded.

Name	Tunnel	Local	Peer	Info	Transport	Encryption	Auth.	Compression	bps10	Total	Idle	Start	Key
LOC1-VIRTCTRL [2]	TINA	80.130.45.80	62.99.0.80		UDP	AES 128	MD5	0%	752 B	18 M	0 s	6 d	8 m
LOC1-VIRTCTRL Quality [2]	TINA	212.86.0.80	194.93.0.80		UDP	AES 128	MD5	0%	0 B	0 K	6 d	6 d	8 m

Videolink:

<https://campus.barracuda.com/>

Before You Begin

- Create IPv4 TINA VPN tunnels between all firewalls. For more information, see [How to Create a TINA VPN Tunnel between F-Series Firewalls](#).
- Create access rules for the VPN tunnels. For more information, see [How to Create Access Rules for Site-to-Site VPN Access](#).
- Configure the NextGen Firewall F acting as a VPN hub to forward VPN traffic from one remote firewall to the others.

Step 1. Enable Dynamic Mesh

Repeat this step on every firewall in the Dynamic Mesh VPN network.

1. Open the **VPN Settings** page (**Configuration > Full Configuration > Box > Virtual Servers > your virtual server > Assigned Services > VPN**).
2. Click **Lock**.
3. Click **Click here for Server Settings**. The **Server Settings** window opens.
4. In the **Server Configuration** section, verify that **Disable Dynamic Mesh** is set to **No**.

Server Configuration

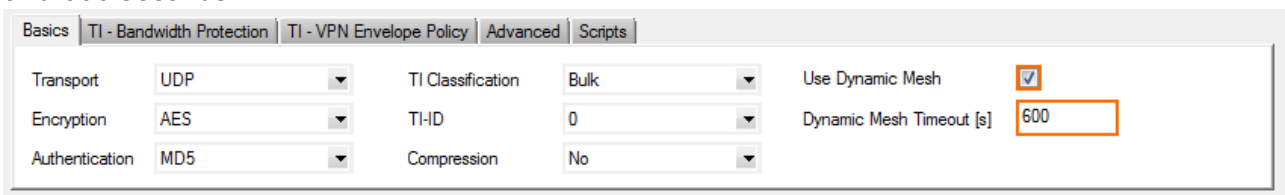
Use port 443	Yes
CRL Poll Time (min)	0
Global TOS Copy	Off
Global Replay Window Size, Packets(0...Use Default)	
Use Site to Site Tunnels for Authentication	Yes
Pending Session Limitation	Yes
Prebuild Cookies on Startup	No
Tunnel HA Sync	No
Maximum Number of Tunnels	<auto>
Allow Fast Requests	Yes
WANOpt Master	Yes
Handshake Timeout (sec)	10
Disable Dynamic Mesh	No
Add VPN Routes to Main Routing Table (Single Routing Table)	No

5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 2. Enable Dynamic Mesh for the VPN Tunnels

For each TINA tunnel, edit the TINA VPN tunnel configuration on the VPN hub and the remote firewalls to use Dynamic Mesh.

1. Open the **Site to Site** page (**Configuration > Configuration Tree > Box > Virtual Server > your virtual server > Assigned Services > VPN**).
2. Click **Lock**.
3. Double click the Site-to-Site TINA tunnel. The **TINA Tunnel** window opens.
4. Click on the **Advanced** tab.
5. Enable **Use Dynamic Mesh**.
6. (optional) Enter the **Dynamic Mesh Timeout (s)** in seconds. The timeout must be between 5 and 600 seconds.



Basic				TI - Bandwidth Protection		TI - VPN Envelope Policy		Advanced		Scripts	
Transport	UDP	TI Classification	Bulk	Use Dynamic Mesh	<input checked="" type="checkbox"/>	Dynamic Mesh Timeout [s]	600				
Encryption	AES	TI-ID	0								
Authentication	MD5	Compression	No								

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

Step 3. 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 3.1 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 > Assigned Services > 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.

General

Name

Description

Color Label Timeout

NAT Settings

Translated Source IP Weight

Failover and Load Balancing

Policy

VPN Traffic Intelligence (TI) Settings

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

TI Settings (Firewall - VPN Interaction)

Transport Policies

Transport Selection Policy

TI Learning Policy

- In the **Dynamic Mesh** section, enable **Allow Dynamic Mesh** and **Trigger Dynamic Mesh**.
- Enable **Prevent tunnel timeout**.

Dynamic Mesh

☒ Allow Dynamic Mesh ☒ Trigger Dynamic Mesh

☒ Prevent tunnel timeout

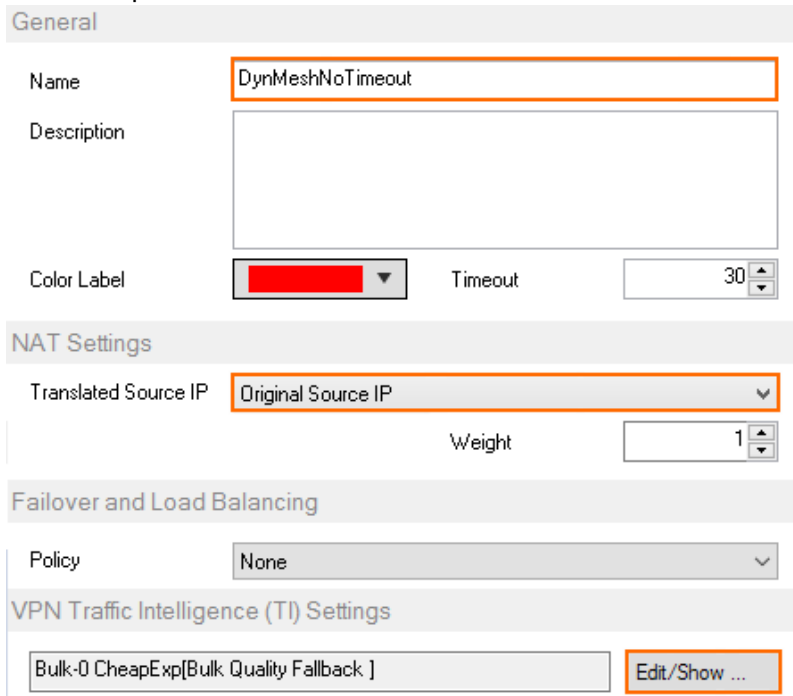
- Click **OK**.
- Click **OK**.
- Click **Send Changes** and **Activate**.

Step 3.2 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.

- Go to **your virtual server > Assigned Services > 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.



General

Name: DynMeshNoTimeout

Description:

Color Label: [Red Box] Timeout: 30

NAT Settings

Translated Source IP: Original Source IP Weight: 1

Failover and Load Balancing

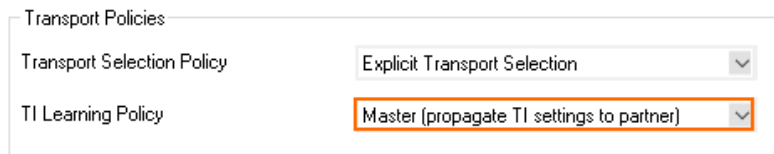
Policy: None

VPN Traffic Intelligence (TI) Settings

Bulk-0 CheapExp[Bulk Quality Fallback] Edit/Show ...

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

TI Settings (Firewall - VPN Interaction)

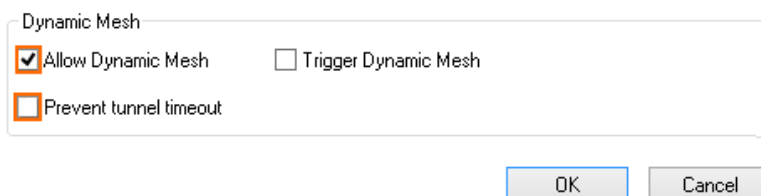


Transport Policies

Transport Selection Policy: Explicit Transport Selection

TI Learning Policy: Master (propagate TI settings to partner)

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



Dynamic Mesh

☒ Allow Dynamic Mesh ☐ Trigger Dynamic Mesh

☐ Prevent tunnel timeout

OK Cancel

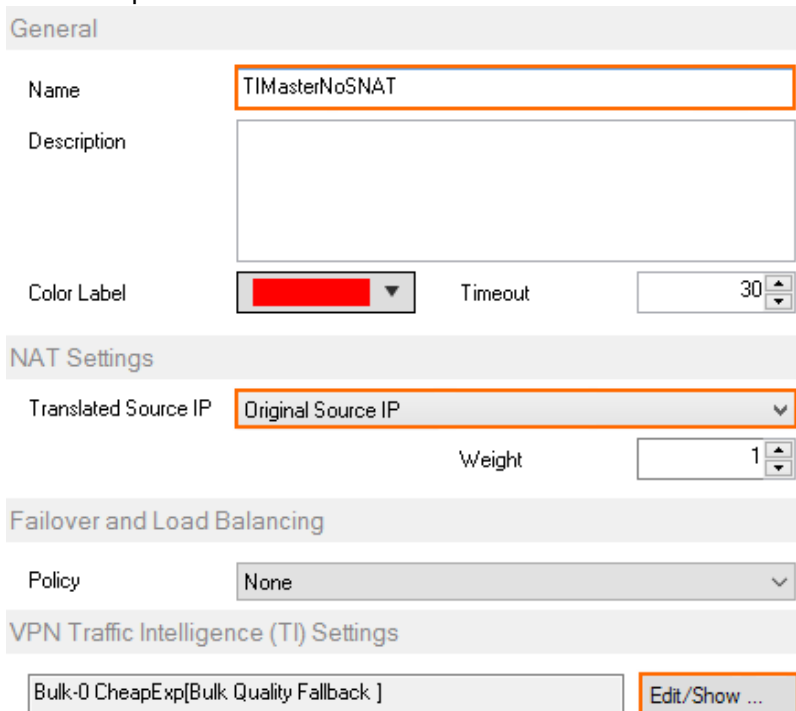
10. Click **OK**.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

Step 3.3. Create a TI Master Connection Object for the VPN Hub

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 > Assigned Services > 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.



General

Name: TIMasterNoSNAT

Description:

Color Label: Timeout: 30

NAT Settings

Translated Source IP: Original Source IP Weight: 1

Failover and Load Balancing

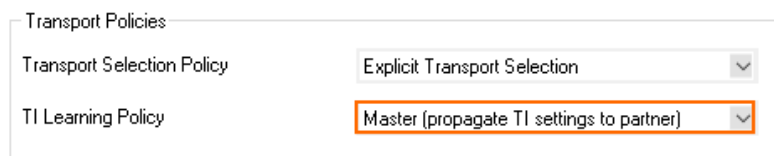
Policy: None

VPN Traffic Intelligence (TI) Settings

Bulk-0 CheapExp[Bulk Quality Fallback] **Edit/Show ...**

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

TI Settings (Firewall - VPN Interaction)

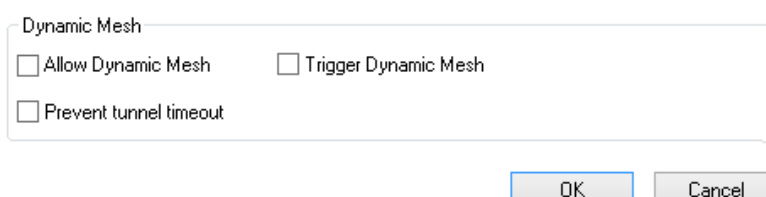


Transport Policies

Transport Selection Policy: Explicit Transport Selection

TI Learning Policy: Master (propagate TI settings to partner)

8. Verify all checkboxes in the **Dynamic Mesh** section are disabled.



Dynamic Mesh

☐ Allow Dynamic Mesh ☐ Trigger Dynamic Mesh

☐ Prevent tunnel timeout

OK Cancel

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

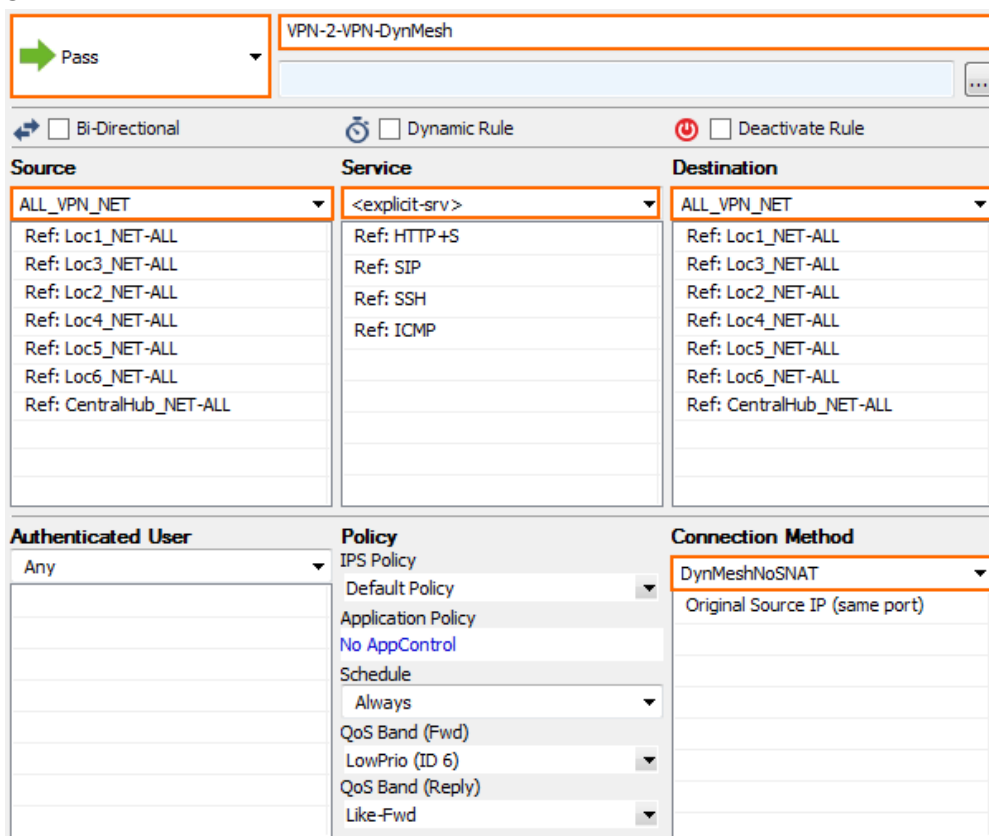
Step 4. Create Three Access Rules on the VPN Hub

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

Step 4.1. 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 3.1.



The screenshot shows the configuration of an access rule in the Barracuda CloudGen Firewall. The rule is named "VPN-2-VPN-DynMesh". The Action is set to "Pass". The Source is "ALL_VPN_NET", Service is "<explicit-srv>", and Destination is "ALL_VPN_NET". The Connection Method is "DynMeshNoSNAT".

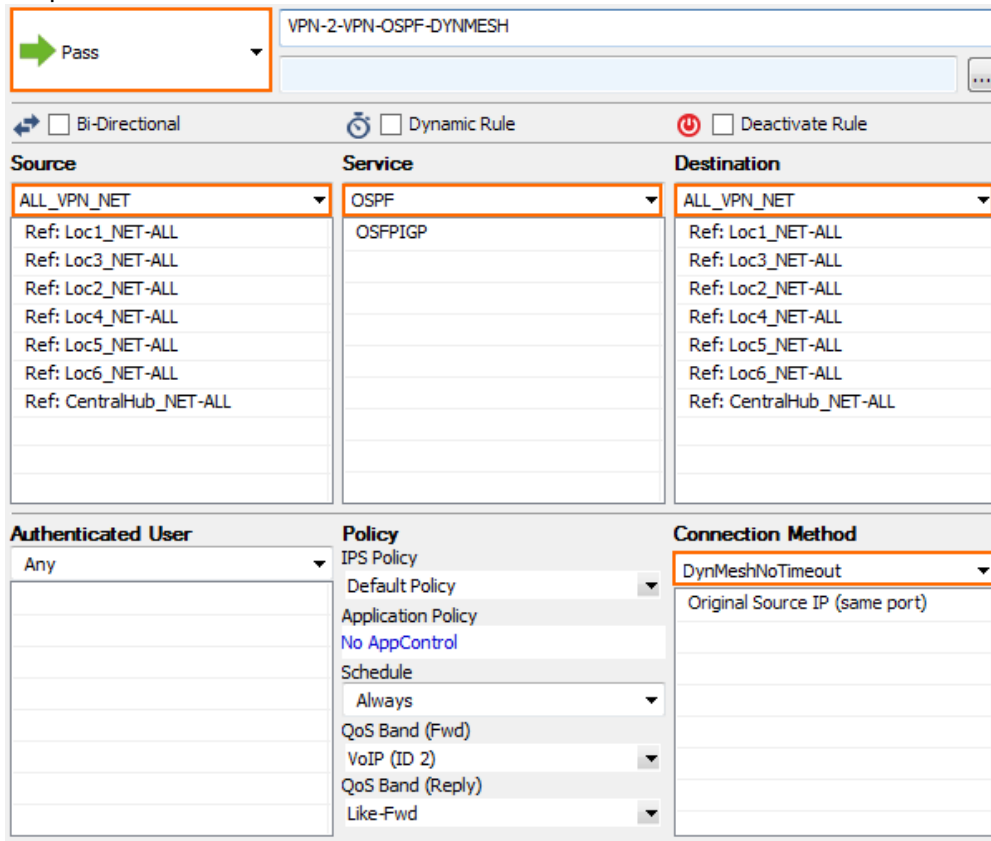
Source	Service	Destination
ALL_VPN_NET	<explicit-srv>	ALL_VPN_NET
Ref: Loc1_NET-ALL	Ref: HTTP+S	Ref: Loc1_NET-ALL
Ref: Loc3_NET-ALL	Ref: SIP	Ref: Loc3_NET-ALL
Ref: Loc2_NET-ALL	Ref: SSH	Ref: Loc2_NET-ALL
Ref: Loc4_NET-ALL	Ref: ICMP	Ref: Loc4_NET-ALL
Ref: Loc5_NET-ALL		Ref: Loc5_NET-ALL
Ref: Loc6_NET-ALL		Ref: Loc6_NET-ALL
Ref: CentralHub_NET-ALL		Ref: CentralHub_NET-ALL

Authenticated User	Policy	Connection Method
Any	IPS Policy	DynMeshNoSNAT
	Default Policy	Original Source IP (same port)
	Application Policy	
	No AppControl	
	Schedule	
	Always	
	QoS Band (Fwd)	
	LowPrio (ID 6)	
	QoS Band (Reply)	
	Like-Fwd	

Step 4.2. 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 3.2.



VPN-2-VPN-OSPF-DYNMESH

Pass

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

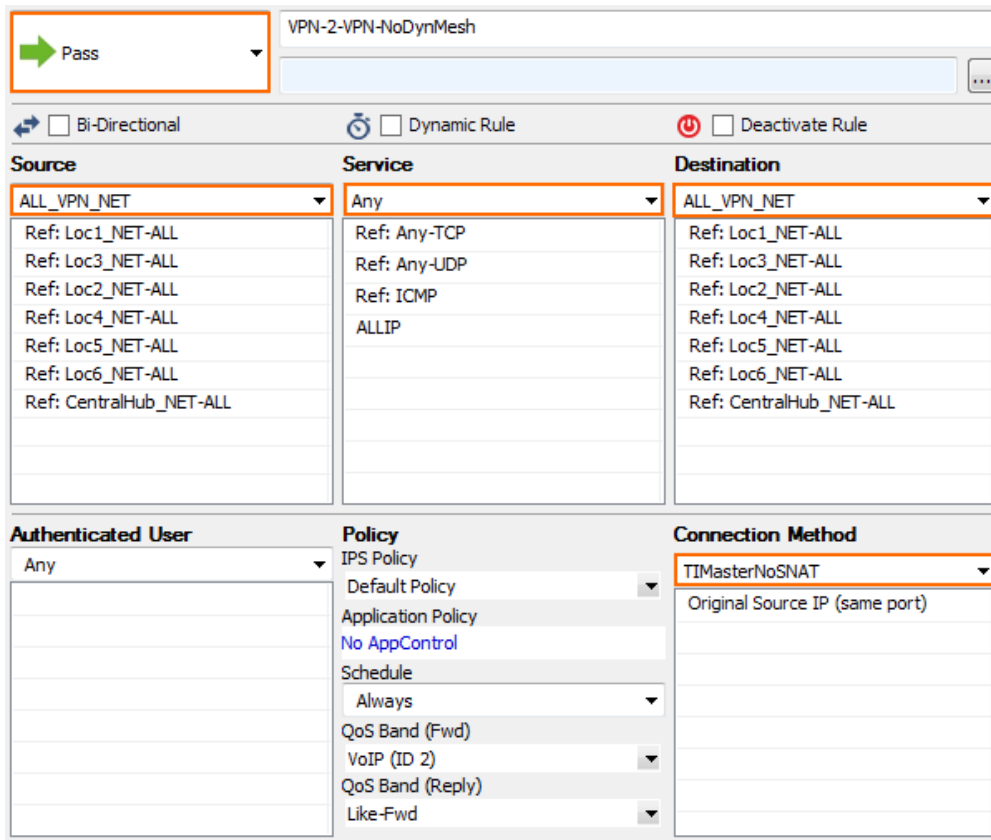
Source	Service	Destination
ALL_VPN_NET	OSPF	ALL_VPN_NET
Ref: Loc1_NET-ALL	OSPF	Ref: Loc1_NET-ALL
Ref: Loc3_NET-ALL	OSPF	Ref: Loc3_NET-ALL
Ref: Loc2_NET-ALL	OSPF	Ref: Loc2_NET-ALL
Ref: Loc4_NET-ALL	OSPF	Ref: Loc4_NET-ALL
Ref: Loc5_NET-ALL	OSPF	Ref: Loc5_NET-ALL
Ref: Loc6_NET-ALL	OSPF	Ref: Loc6_NET-ALL
Ref: CentralHub_NET-ALL	OSPF	Ref: CentralHub_NET-ALL

Authenticated User	Policy	Connection Method
Any	IPS Policy	DynMeshNoTimeout
	Default Policy	Original Source IP (same port)
	Application Policy	
	No AppControl	
	Schedule	
	Always	
	QoS Band (Fwd)	
	VoIP (ID 2)	
	QoS Band (Reply)	
	Like-Fwd	

Step 4.3. 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 3.3.



VPN-2-VPN-NoDynMesh

Pass

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
ALL_VPN_NET	Any	ALL_VPN_NET
Ref: Loc1_NET-ALL	Ref: Any-TCP	Ref: Loc1_NET-ALL
Ref: Loc3_NET-ALL	Ref: Any-UDP	Ref: Loc3_NET-ALL
Ref: Loc2_NET-ALL	Ref: ICMP	Ref: Loc2_NET-ALL
Ref: Loc4_NET-ALL	ALLIP	Ref: Loc4_NET-ALL
Ref: Loc5_NET-ALL		Ref: Loc5_NET-ALL
Ref: Loc6_NET-ALL		Ref: Loc6_NET-ALL
Ref: CentralHub_NET-ALL		Ref: CentralHub_NET-ALL

Authenticated User	Policy	Connection Method
Any	IPS Policy	TlMasterNoSNAT
	Default Policy	Original Source IP (same port)
	Application Policy	
	No AppControl	
	Schedule	
	Always	
	QoS Band (Fwd)	
	VoIP (ID 2)	
	QoS Band (Reply)	
	Like-Fwd	

Step 5. Create Custom Connection Objects on the Remote Firewalls

On every remote firewall in the Dynamic Mesh VPN network, create a TI Slave connection object to allow dynamic mesh.

1. Go to **your virtual server > Assigned Services > 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., DynMeshAllow
5. Select **Original Source IP**.
6. In the **VPN Traffic Intelligence (TI)Settings** section, click **Edit/Show**. The **TI Settings** window opens.

General

Name:

Description:

Color Label: Timeout:

NAT Settings

Translated Source IP: Weight:

Failover and Load Balancing

Policy:

VPN Traffic Intelligence (TI) Settings

7. Set the **TI Learning Policy** to **Slave (learn TI settings from partner)**.

TI Settings (Firewall - VPN Interaction)

Transport Policies

Transport Selection Policy:

TI Learning Policy:

8. In the **Dynamic Mesh** section, enable **Allow Dynamic Mesh**.

Dynamic Mesh

☒ Allow Dynamic Mesh ☐ Trigger Dynamic Mesh

☐ Prevent tunnel timeout

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

Step 6. Modify the VPN Access Rule on the Remote Firewalls

On every remote firewall, create or modify the access rule that allows traffic through the dynamic tunnel. Apply the connection object to allow dynamic mesh.

- **Action** - Select **PASS**.
- **Bi-Directional** - Select the check box to apply the rule in both directions.
- **Source** - Enter all local networks used for the VPN tunnel.

- **Service** – Select the services that should go through the dynamic tunnel if it is up, otherwise go through the VPN hub.
- **Destination** – Enter the **Local Networks** for all remote firewalls and the **Local Networks** for the VPN hub.
- **Connection Method** – Select the **DynMeshAllow** custom connection object created in Step 5.

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 **Site-to-Site** configuration for each tunnel.

Figures

1. vpn_dynmesh00.png
4. vpn_dynmesh01.png
5. vpn_dynmesh02.png
6. vpn_dynmesh03.png
7. vpn_dynmesh06a.png
8. vpn_dynmesh04b.png
9. vpn_dynmesh05.png
10. vpn_dynmesh06a.png
11. vpn_dynmesh06b.png
12. vpn_dynmesh07.png
13. vpn_dynmesh06a.png
14. vpn_dynmesh08b.png
15. vpn_dynmesh09.png
16. vpn_dynmesh10.png
17. vpn_dynmesh11.png
18. vpn_dynmesh09a.png
19. vpn_dynmesh09b.png
20. vpn_dynmesh06b.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.