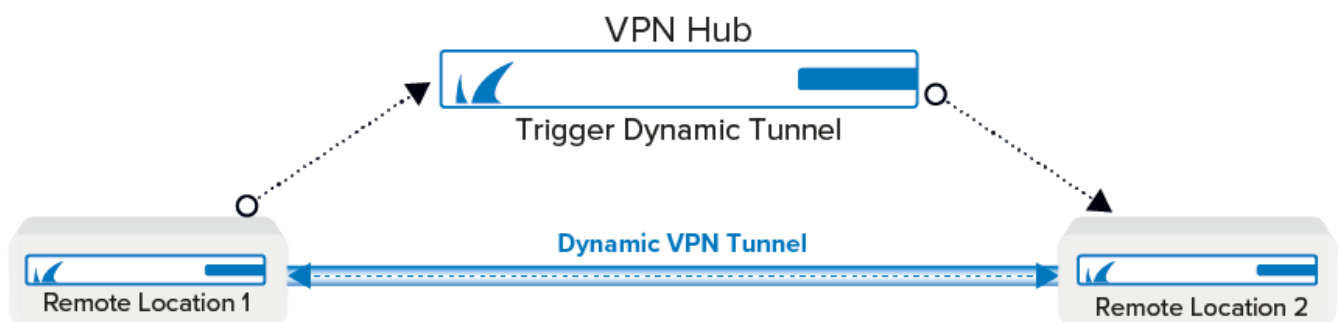


How to Configure Dynamic Mesh VPN

<https://campus.barracuda.com/doc/96026174/>

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 CloudGen 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 SD-WAN primary 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.



Before You Begin

- Create IPv4 TINA VPN tunnels between all firewalls. For more information, see [How to Create a TINA VPN Tunnel between CloudGen 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 CloudGen 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 > Configuration Tree > Box > Assigned Services > VPN-Service**).
2. Click **Lock**.
3. In the **TINA** section, verify that **Allow Dynamic Mesh** is selected.

TINA

Handshake Timeout (sec)	<input type="text" value="10"/>
Tunnel HA Sync	<input checked="" type="checkbox"/>
Allow fast requests	<input checked="" type="checkbox"/>
Pending session limit	<input checked="" type="checkbox"/>
Prebuild cookies on startup	<input type="checkbox"/>
Global TOS copy	<input type="checkbox"/>
Global replay window size [packets]	<input type="text" value="256"/>
Allow Dynamic Mesh	<input checked="" type="checkbox"/>

4. Click **OK**.
5. 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 > Assigned Services > VPN-Service**).
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.

Basics SD-WAN - Bandwidth Protection SD-WAN - VPN Envelope Policy Advanced Scripts					
Transport	<input type="text" value="UDP"/>	SD-WAN Classification	<input type="text" value="Bulk"/>	Use Dynamic Mesh	<input checked="" type="checkbox"/>
Encryption	<input type="text" value="AES"/>	SD-WAN-ID	<input type="text" value="0"/>	Dynamic Mesh Timeout [s]	<input type="text" value="600"/>
Authentication	<input type="text" value="MD5"/>	Compression	<input type="text" value="Disabled"/>	Dynamic Mesh on Dynamic Interface	<input type="checkbox"/>

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

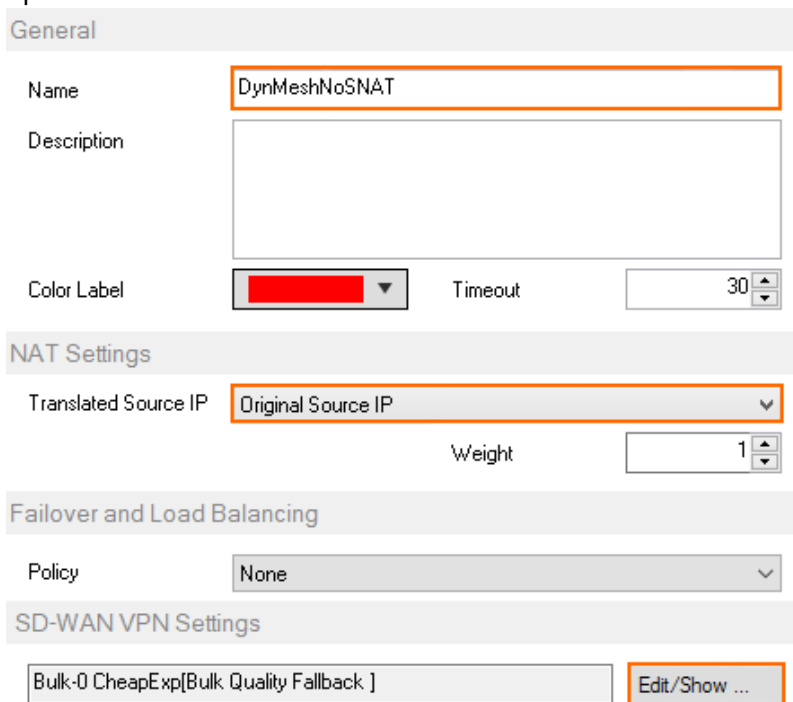
Step 3. Create Three Custom Connection Objects on the VPN Hub

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 SD-WAN Primary with Idle Timeout Reset

Only connections matching an access rule with the Dynamic Mesh and SD-WAN primary options enabled in the SD-WAN 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 (SD-WAN secondaries) do not need to be enabled because they are learned automatically from the VPN hub acting as the SD-WAN primary. For traffic matching access rules using this connection object to keep the dynamic tunnel open, **Prevent tunnel timeout** must be enabled.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 **SD-WAN VPN Settings** section, click **Edit/Show**. The **SD-WAN Settings** window opens.



General

Name: DynMeshNoSNAT

Description:

Color Label: Timeout: 30

NAT Settings

Translated Source IP: Original Source IP

Weight: 1

Failover and Load Balancing

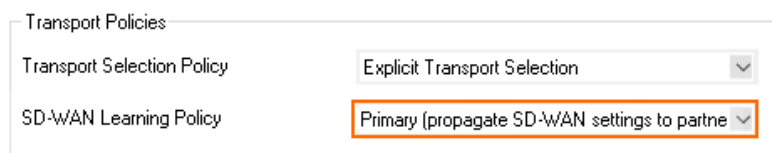
Policy: None

SD-WAN VPN Settings

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

7. Set the **SD-WAN Learning Policy** to **Primary (propagate SD-WAN settings to partner)**.

TI Settings (Firewall - VPN Interaction)



Transport Policies

Transport Selection Policy: Explicit Transport Selection

SD-WAN Learning Policy: Primary (propagate SD-WAN settings to partner)

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



Dynamic Mesh

☒ Allow Dynamic Mesh ☒ Trigger Dynamic Mesh

☒ Prevent tunnel timeout

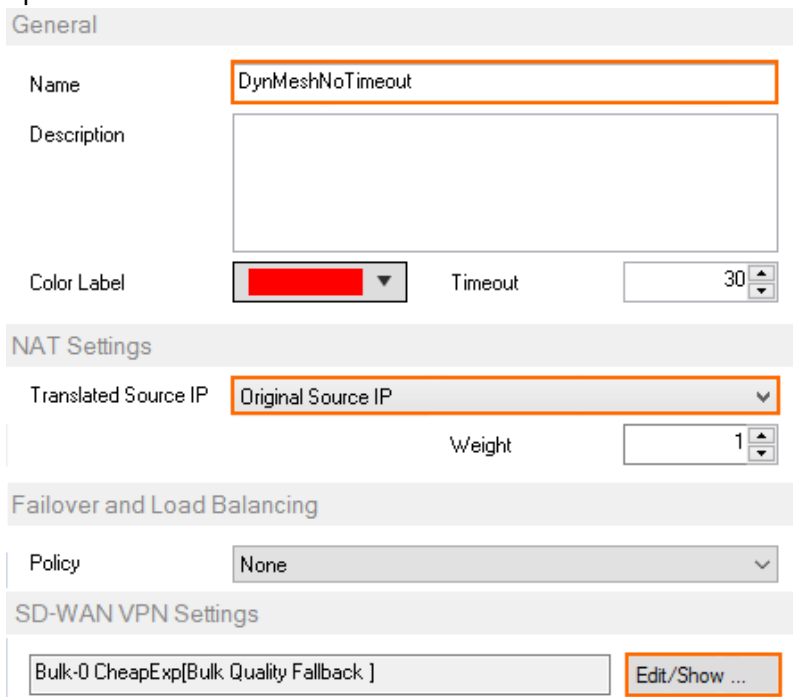
OK Cancel

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

Step 3.2 Dynamic Mesh Connection Object SD-WAN Primary with no Idle Timeout Reset

Only connections matching an access rule with the Dynamic Mesh and SD-WAN primary options enabled in the SD-WAN 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 (SD-WAN secondaries) do not need to be enabled because they are learned automatically from the VPN hub acting as the SD-WAN primary.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 **SD-WAN VPN Settings** section, click **Edit/Show**. The **SD-WAN Settings** window opens.



General

Name: DynMeshNoTimeout

Description:

Color Label: Timeout: 30

NAT Settings

Translated Source IP: Original Source IP Weight: 1

Failover and Load Balancing

Policy: None

SD-WAN VPN Settings

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

7. Set the **SD-WAN Learning Policy** to **Primary** (propagate SD-WAN settings to partner).

TI Settings (Firewall - VPN Interaction)

Transport Policies	
Transport Selection Policy	Explicit Transport Selection
SD-WAN Learning Policy	Primary (propagate SD-WAN settings to partne

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

Dynamic Mesh	
<input checked="" type="checkbox"/> Allow Dynamic Mesh	<input type="checkbox"/> Trigger Dynamic Mesh
<input type="checkbox"/> Prevent tunnel timeout	
<div>OK Cancel</div>	

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

Step 3.3. Create a SD-WAN Primary Connection Object for the VPN Hub

For all services that should not go through the VPN tunnel, use a custom connection object with the **SD-WAN Learning Policy** set to **Primary**. 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 **CONFIGURATION > Configuration Tree > Box > 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., TIPrimaryNoSNAT
5. Select **Original Source IP**.
6. In the **SD-WAN VPN Settings** section, click **Edit/Show**. The **SD-WAN Settings** window opens.

General

Name:

Description:

Color Label: Timeout:

NAT Settings

Translated Source IP: Weight:

Failover and Load Balancing

Policy:

SD-WAN VPN Settings

7. Set the **SD-WAN Learning Policy** to **Primary (propagate SD-WAN settings to partner)**.

TI Settings (Firewall - VPN Interaction)

Transport Policies

Transport Selection Policy:

SD-WAN Learning Policy:

8. Verify that all check boxes in the **Dynamic Mesh** section are cleared.

Dynamic Mesh

☐ Allow Dynamic Mesh ☐ Trigger Dynamic Mesh

☐ Prevent tunnel timeout

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

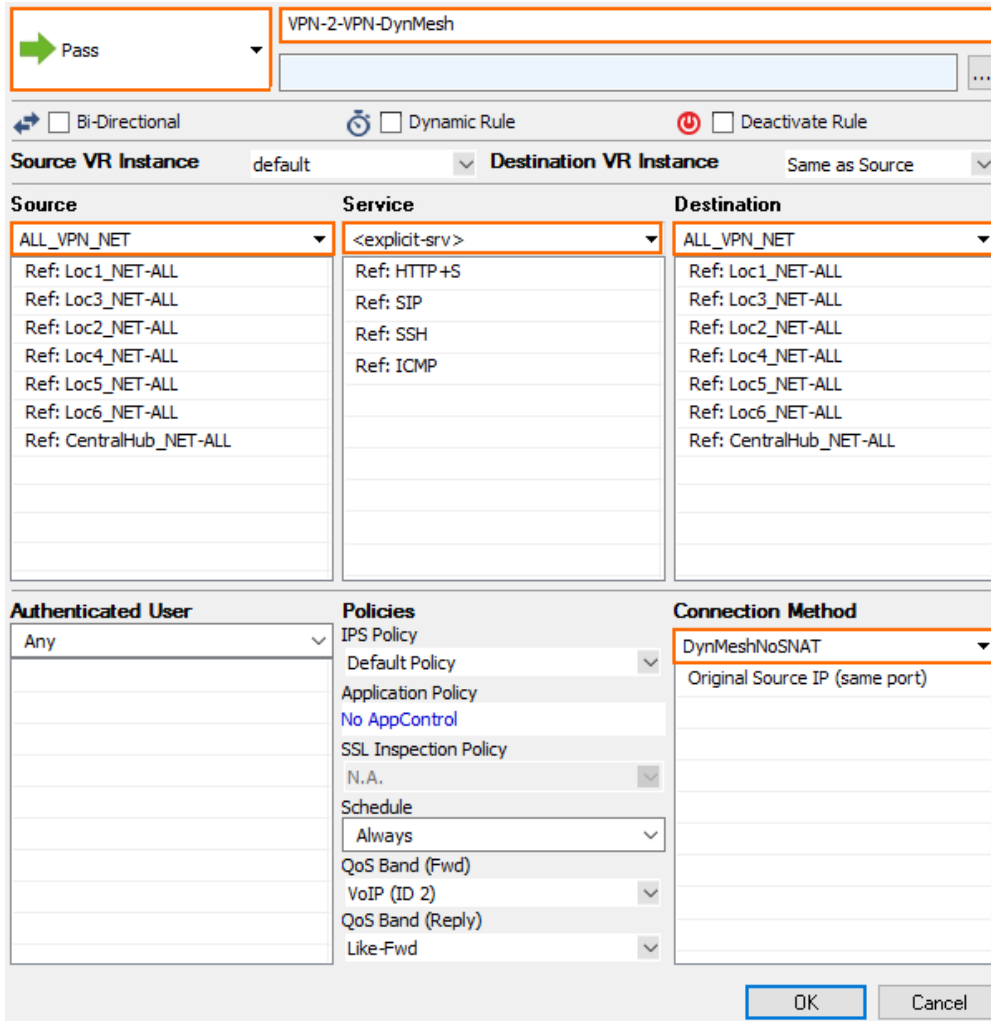
Step 4. Create Three Access Rules on the VPN Hub

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.



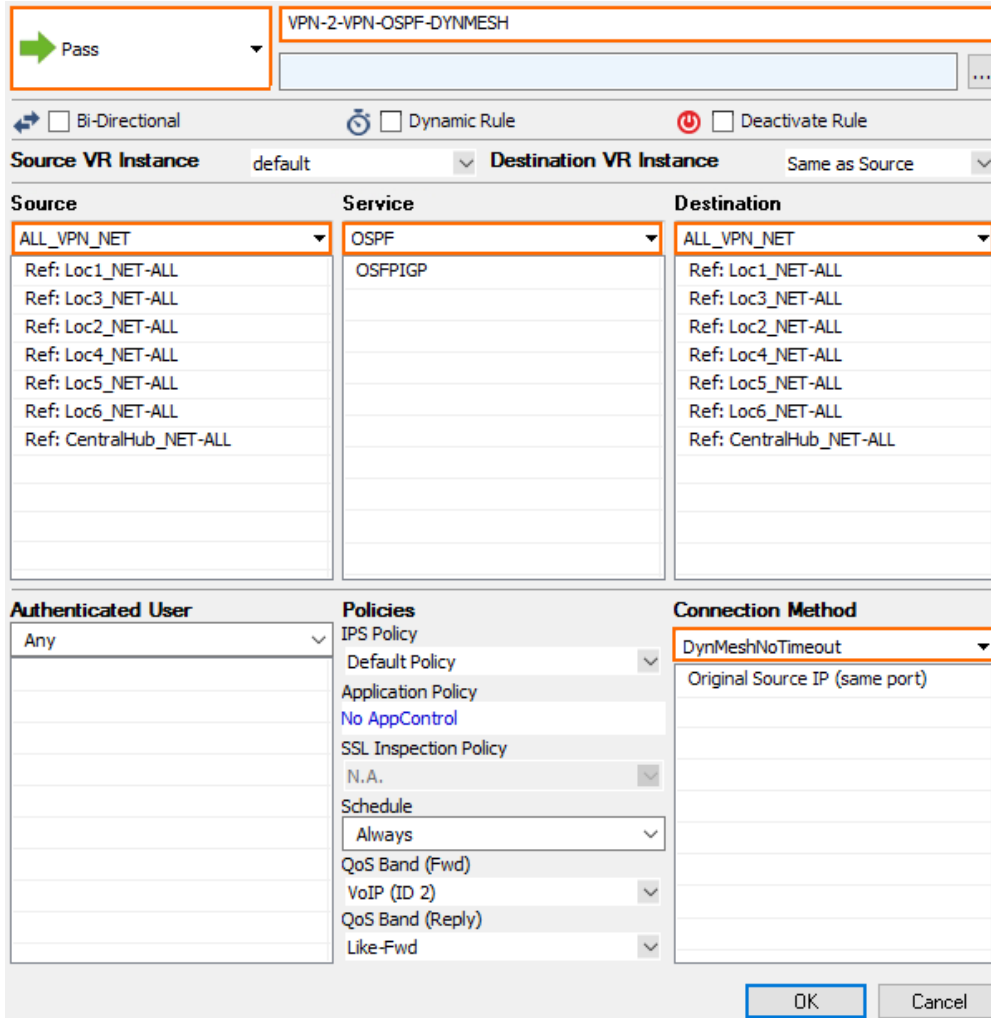
The screenshot shows the configuration window for a dynamic tunnel rule. The **Action** is set to **Pass**. The **Source VR Instance** is **default** and the **Destination VR Instance** is **Same as Source**. The **Source** list includes **ALL_VPN_NET** and several local network references. The **Service** list includes **<explicit-srv>** and several protocols. The **Destination** list includes **ALL_VPN_NET** and several local network references. The **Authenticated User** is set to **Any**. The **Policies** section includes **IPS Policy**, **Default Policy**, **Application Policy**, **No AppControl**, **SSL Inspection Policy**, **N.A.**, **Schedule**, **Always**, **QoS Band (Fwd)**, **VoIP (ID 2)**, **QoS Band (Reply)**, and **Like-Fwd**. The **Connection Method** is set to **DynMeshNoSNAT** with the option **Original Source IP (same port)**. The **OK** and **Cancel** buttons are at the bottom right.

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.



The screenshot shows the configuration window for a rule named "VPN-2-VPN-OSPF-DYNMESH". The rule is set to "Pass" action. It is configured with the following settings:

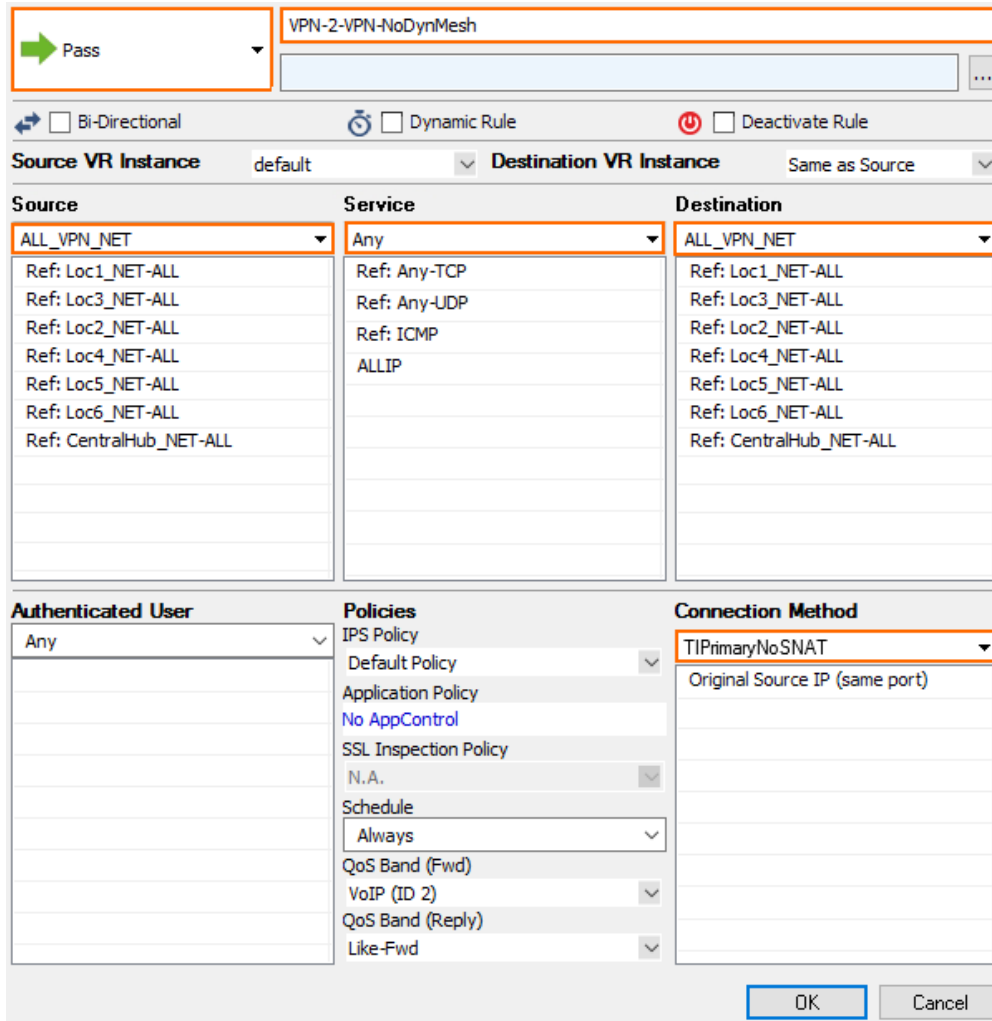
- Source VR Instance:** default
- Destination VR Instance:** Same as Source
- Source:** ALL_VPN_NET (with references: Loc1_NET-ALL, Loc3_NET-ALL, Loc2_NET-ALL, Loc4_NET-ALL, Loc5_NET-ALL, Loc6_NET-ALL, CentralHub_NET-ALL)
- Service:** OSPF (with reference: OSPFIGP)
- Destination:** ALL_VPN_NET (with references: Loc1_NET-ALL, Loc3_NET-ALL, Loc2_NET-ALL, Loc4_NET-ALL, Loc5_NET-ALL, Loc6_NET-ALL, CentralHub_NET-ALL)
- Authenticated User:** Any
- Policies:**
 - IPS Policy: Default Policy
 - Application Policy: No AppControl
 - SSL Inspection Policy: N.A.
 - Schedule: Always
 - QoS Band (Fwd): VoIP (ID 2)
 - QoS Band (Reply): Like-Fwd
- Connection Method:** DynMeshNoTimeout (Original Source IP (same port))

Buttons at the bottom: OK, Cancel.

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 **TIPPrimaryNoSNAT** custom connection object created in Step 3.3.



☒ Pass

VPN-2-VPN-NoDynMesh

☐ Bi-Directional
 ☐ Dynamic Rule
 ☐ Deactivate Rule

Source VR Instance: default
 Destination VR Instance: Same as Source

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	Policies	Connection Method
Any	IPS Policy Default Policy Application Policy No AppControl SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd) VoIP (ID 2) QoS Band (Reply) Like-Fwd	TIPrimaryNoSNAT Original Source IP (same port)

OK Cancel

Step 5. Create Custom Connection Objects on the Remote Firewalls

On every remote firewall in the Dynamic Mesh VPN network, create a SD-WAN secondary connection object to allow dynamic mesh.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 **SD-WAN VPN Settings** section, click **Edit/Show**. The **SD-WAN Settings** window opens.

General

Name

Description

Color Label Timeout

NAT Settings

Translated Source IP

Weight

Failover and Load Balancing

Policy

SD-WAN VPN Settings

7. Set the **SD-WAN Learning Policy** to **Secondary (learn SD-WAN settings from partner)**.

TI Settings (Firewall - VPN Interaction)

Transport Policies

Transport Selection Policy

SD-WAN 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_dyn_mesh.png
2. vpn_dynmesh.png
3. vpn_dynmesh02.png
4. vpn_dynmesh03.png
5. vpn_dynmesh06a.png
6. vpn_dynmesh04b.png
7. vpn_dynmesh05.png
8. vpn_dynmesh06a.png
9. vpn_dynmesh06b.png
10. vpn_dynmesh07.png
11. vpn_dynmesh06a.png
12. vpn_dynmesh08b.png
13. vpn_dynmesh09.png
14. vpn_dynmesh10.png
15. vpn_dynmesh11.png
16. vpn_dynmesh09a.png
17. vpn_dynmesh09b.png
18. 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.