

## How to Create a VPN Tunnel with the VPN GTI Editor

<https://campus.barracuda.com/doc/41115851/>

VPN services on the NG Control Center are organized in VPN groups. VPN tunnels can be created and configured for all VPN services by drag and drop connections between the individual services.

### In this article:

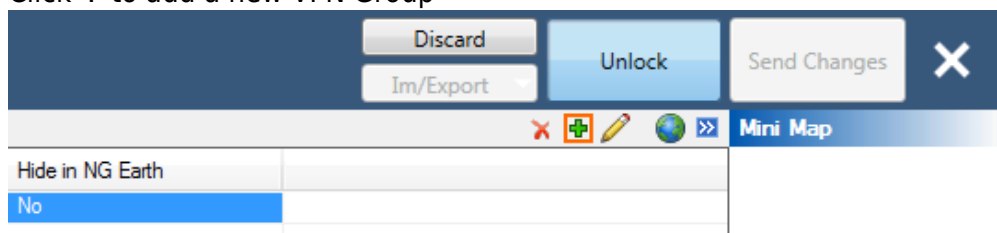
### Before you Begin

- If you want to use the GTI Editor on the range or cluster level, you must enable the **Own VPN GTI Editor** setting in the range or cluster property settings.
- Configure the GTI Settings for the VPN services on the managed Barracuda NG Firewalls. For more information, see [How to Configure VPN GTI Settings for a VPN Service](#).

### Step 1. Create a VPN Group

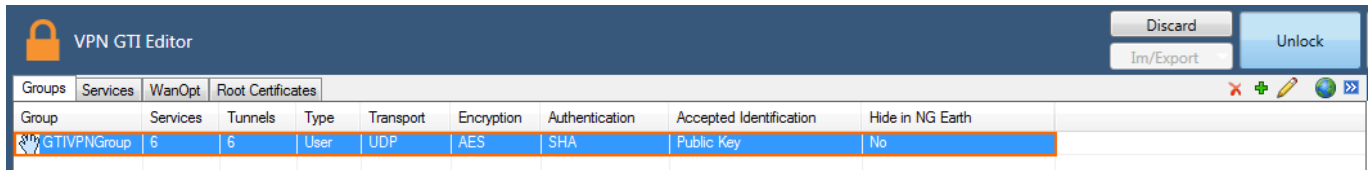
VPN Groups contain the default setting for all VPN tunnels in the group and the list of VPN services used to create the tunnels.

1. Open the **VPN GTI Editor** page (**Config > Multi-Range > Global Settings**).
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.
7. (optional) Click **Edit IPsec**.
8. Edit the default **IPsec** settings.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

The VPN group is now listed in the **Groups** tab.



Groups	Services	WanOpt	Root Certificates	Group	Services	Tunnels	Type	Transport	Encryption	Authentication	Accepted Identification	Hide in NG Earth
GTI VPN Group	6	6	User	UDP	AES	SHA	Public Key	No				

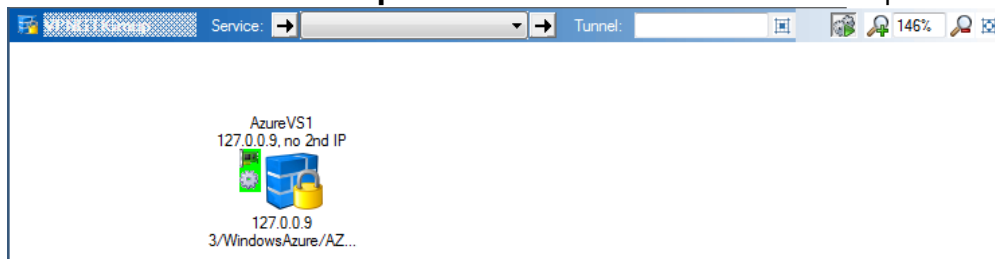
## Step 2. Add VPN Services to the VPN group

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

1. Open the **GTI Editor** page (**Config > Multi-Range > Global Settings**).
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. For each VPN service you want to add to the VPN group:
  1. Right click on the VPN service
  2. Click **Add to current Group**. The VPN service is added to the map area below.

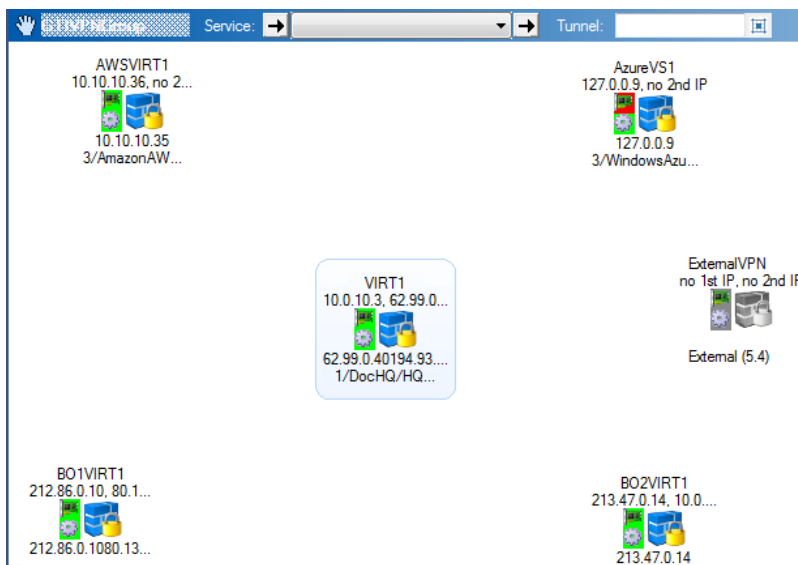


6. Click **Send Changes** and **Activate**.

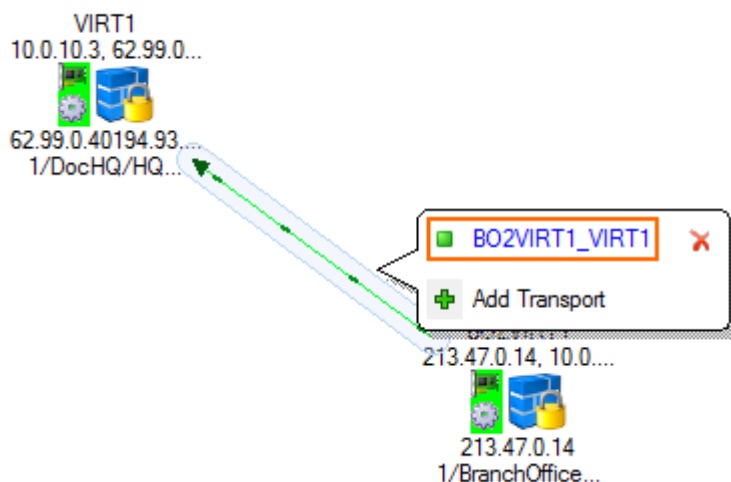
## Step 3. Create a VPN Tunnel

Create VPN tunnels by drag and dropping connections from one VPN service to the other. Per default the VPN service you start with is the active unit, the destination the passive unit. This can be changed in the tunnel configuration settings.

1. Open the **GTI Editor** page (**Config > Multi-Range > Global Settings**).
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 **Server** tab. In the GTI map area the VPN services icons in the VPN are displayed.



5. Create a VPN tunnel by drag and drop from the active VPN service to the passive VPN service. A line is displayed between the VPN services.
6. Click on the connection between the two VPN services and click on the transport you want to edit. Per default TINA VPN tunnels are created with one transport.



7. You can now modify the VPN tunnel as needed:
  - **Direction** - You can create VPN tunnels using the following modes: **active-active, active-passive, on-demand**.
  - **Transport Source IP/Interface** - If needed you can modify the transport source IP. Per default the IP address.
  - **Transport Listening IP/Interface** - If needed you can modify the transport listening IP.
  - **Local Network** - If needed modify the networks that are available through this VPN tunnel.
8. Click **Send Changes** and **Activate**.

You can view the collective state of all GTI VPN tunnel of a NG Firewall on the Status page of the NG Control Center.

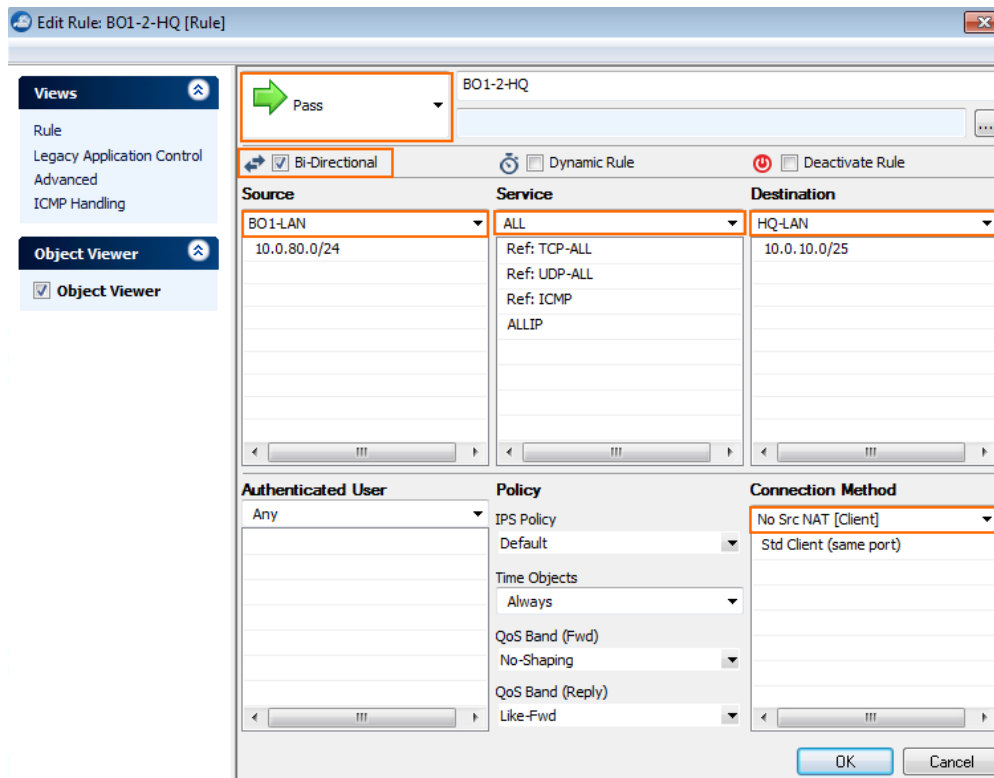
1/DocHQ	6.0	     						
HQ-NG1	Headquarters Box 1	10.0.10.88	6.0.0		Austria	VF25	VIRT1	     
2/DOC-BO1	5.4	     						
BO-NG1	Branch Office Box 1	10.0.11.92	5.4.4		Italy	VF25	BO1VIRT1	     
3/AmazonAWS	6.0	     						
AWSNG1		10.0.10.91	6.0.0		Ireland	VF25	AWSVIRT1	     

## Step 4. Create Access Rules to Allow VPN Traffic

You must create access rules on both NG Firewalls involved in the VPN tunnel to allow traffic in and out of the VPN tunnel.

Example Access Rule for a VPN tunnel from Branch Office 1 (BO1) to the Headquarters (HQ). The access rules need to be added to the BO1 and HQ forwarding firewall:

- **Action** - Select **PASS**.
- **Bi-Directional** - Enable bidirectional.
- **Source** - Select the network object for the **BO1LAN**.
- **Service** - Select **ALL**.
- **Destination** - Select the network object for the **HQ LAN**.
- **Connection Method** - Select **No Src NAT [Client]**.



## Next Steps

- You can use the GTI editor to configure additional transports using Traffic Intelligence. For more information, see [How to Configure Traffic Intelligence Using the VPN GTI Editor](#).
- You can use the GTI editor to configure Traffic Shaping for the VPN tunnels. For more information, see [Traffic Shaping](#).

## Figures

1. gti\_groups01.png
2. gti\_groups02.png
3. gti\_add\_VPN01.png
4. gti\_add\_VPN02.png
5. gti\_map\_01.png
6. gti\_map\_02.png
7. gti\_map\_03.png
8. gti\_fw\_rule01.png

© Barracuda Networks Inc., 2019 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.