

## How to Configure OSPF Routing over TINA VPN

<https://campus.barracuda.com/doc/96026043/>

To dynamically learn OSPF-propagated routes from a remote location connected via TINA VPN tunnel, VPN next hop interfaces are used to create an intermediary network.

You must complete this configuration on both the local and the remote CloudGen Firewalls by using the respective values below:

	Example values for the local firewall	Example values for the remote firewall
<b>VPN Next Hop Interface Index</b>	1	1
<b>VPN Next Hop Interface IP Address</b>	192.168.20.1/24	192.168.20.2/24
<b>Box Shared IP</b>	192.168.20.1	192.168.20.2
<b>VPN Local Networks</b>	empty	empty
<b>VPN Remote Networks</b>	empty	empty
<b>Router ID</b>	192.168.20.1	192.168.20.2

### Before You Begin

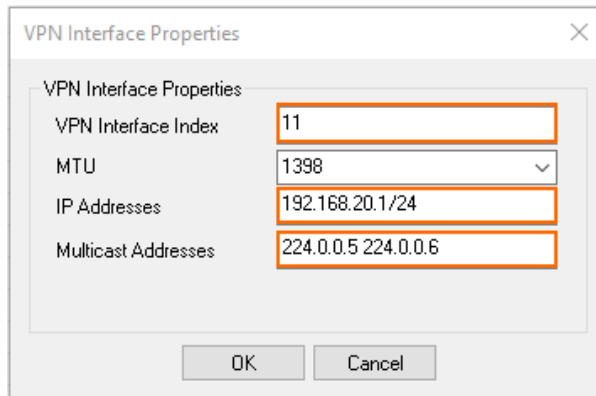
- A free /24 subnet (e.g., 192.168.20.0/24) for the intermediary network is required.

### Step 1. Add a VPN Next Hop Interface

Add a VPN next hop interface using a /24 subnet (e.g., 192.168.20.0/24).

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left menu, select **Routed VPN**.
4. Next to the **Next Hop Interface Configuration** table, click **Add**.
5. In the **VPN Interface Properties** window, configure the following settings and then click **OK**.
  - In the **VPN Interface Index** field, enter a number between 0 and 999. E.g., 11
  - In the **IP Addresses** field, enter the VPN interface IP address including the subnet. E.g., 192.168.20.1/24 for the local CloudGen Firewall, or 192.168.20.2/24 for the remote firewall.
  - In the **Multicast Addresses** field, enter the OSPF multicast addresses: 224.0.0.5

224.0.0.6



VPN Interface Properties

VPN Interface Index: 11

MTU: 1398

IP Addresses: 192.168.20.1/24

Multicast Addresses: 224.0.0.5 224.0.0.6

OK Cancel

- Click **OK**. The interface is now listed in the **Next Hop Interface Configuration** table.

#### Next Hop Interface Configuration

VPN I...	MTU	IPs	Multicast	
vpn11	1398	192.168.20.1...	224.0.0.5 224....	

Add  
 Edit  
 Delete

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

## Step 2. Add the VPN Next Hop Interface IP Address to the Firewall Listening IP Addresses

Introduce the IP address of the VPN next hop interface on the firewall.

CloudGen Firewalls installed using version 8.0.2 (or higher) do not require the interface IP address to be added to the Shared Networks table as this is handled by the host firewall ruleset.

- Go to **CONFIGURATION > Configuration Tree > Box > Network**.
- In the left menu, select **IP Configuration**.
- Click **Lock**.
- In the **Shared Networks and IPs** section, click **+**. The **Shared Network and IPs** window opens.
  - Select the virtual **Interface**.
  - In the **Network Address** field, enter the network the virtual interface resides in.
  - In the **Shared IPs in this Network** table, click **+** and add the IP address of the VPN next hop interface.
  - Click **OK**.
- Click **Send Changes** and **Activate**.

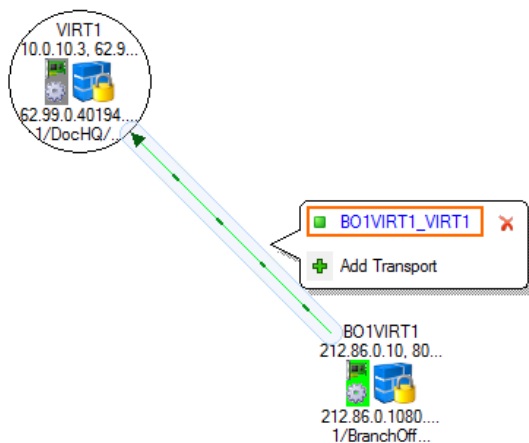
### Step 3. Configure the TINA Site-to-Site VPN Tunnels

You can configure the VPN tunnel using the GTI Editor for managed CloudGen Firewalls, or using the Site-to-Site configuration dialog if you are using standalone CloudGen Firewalls.

#### In the GTI Editor

Edit the VPN tunnel to remove the local and remote networks and add the VPN next hop interface ID.

1. Go to the global/range/cluster **GTI Editor**.
2. Click **Lock**.
3. Click on the VPN tunnel, and click on the first Transport to edit the VPN tunnel configuration. For more information, see [How to Create a VPN Tunnel with the VPN GTI Editor](#).



4. Remove all **Local Networks** from the remote and local VPN services.
5. Enter the VPN next hop interface ID for the remote and local VPN services. E.g., 11

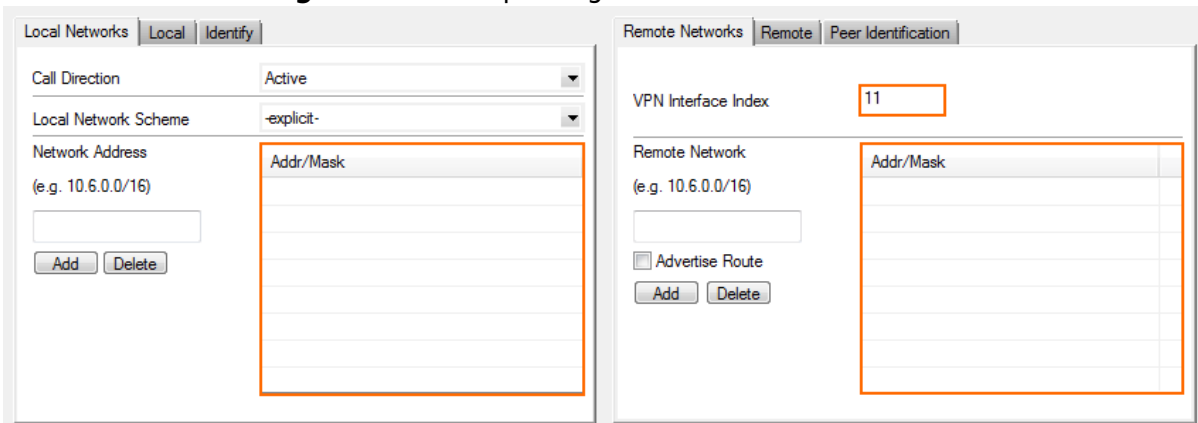
TINA Tunnel		Tunnel Properties		To VIRT1	
From BO1VIRT1				To VIRT1	
BO1VPN/BranchOffice3-4/1 Explicit: 212.86.0.10, 80.130.45.10, 10.21.0.3				HQVPN/DocHQ/1 Explicit: 62.99.0.40, 194.93.0.10, 10.20.0.3	
Direction	active	Transport	UDP	Direction	passive
Transport Source IP/Interface	Explicit	Encryption	AES	Transport Source IP/Interface	Explicit
Transport Listening IP/Hostname	<Use-Transport-Source>	Authentication	MD5	Transport Listening IP/Hostname	<Use-Transport-Source>
Explicit Listening	212.86.0.10, 80.130.45.10	TI Classification	Bulk	Explicit Listening	62.99.0.40, 194.93.0.10
Local Networks		THD	0	Local Networks	
Advanced		Compression	No	Advanced	
Routing Next-Hop		Dynamic Mesh	No	Routing Next-Hop	
OnDemand Transport Timeout		Dynamic Mesh Timeout	600	OnDemand Transport Timeout	
OnDemand Transport Delay		SD-WAN		OnDemand Transport Delay	
Device Index	11	SD-WAN - Bandwidth Protection		Device Index	11
Proxy		SD-WAN - VPN Envelope Policy		Proxy	
Security		Advanced		Security	
Root Certificate		Key Time Limit	10 mins	Root Certificate	
X509 Certificate Condition		Key Traffic Limit	No Limit	X509 Certificate Condition	
Server Key	Hash: ZNTIOP	Identification Type	Public Key	Server Key	Hash: IGQFOO
Server Certificate	Hash: ZNTIOP self-signed	Tunnel Probing	30 secs	Server Certificate	Hash: IGQFOO self-signed
Scripts		Tunnel Timeout	20 secs	Scripts	
Start Script		Packet Balancing	None		
Stop Script		High Performance Settings	No		
		WANOpt			
		WANOpt Policy	NO-WANOpt		
		GTI Settings			
		Hide in Barracuda NG Earth	No		

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

## Standalone CloudGen Firewalls

On both the remote and local firewalls, configure a TINA VPN tunnel with the VPN Interface Index. Leave the local and remote networks empty.

1. Log into the local CloudGen Firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site**.
3. Click **Lock**.
4. Right-click in the **TINA Tunnels** tab and select **New TINA tunnel**. The **TINA tunnel** window opens.
5. Enter a **Name**.
6. Configure the **Transport**, **Encryption** and **Authentication** settings as well as the **Local** and **Remote** public IP addresses. For more information, see [How to Create a TINA VPN Tunnel between CloudGen Firewalls](#).
7. Exchange the **Peer Identification** keys.
8. In the **Remote Networks** tab, enter the **VPN Interface Index** number that you created in the **VPN Interface Configuration** in step 1. E.g. 11



The screenshot shows the 'TINA Tunnel' configuration window with two tabs: 'Local Networks' and 'Remote Networks'. The 'Local Networks' tab is active, showing fields for 'Call Direction' (set to 'Active'), 'Local Network Scheme' (set to '-explicit-'), and 'Network Address' (with a placeholder '(e.g. 10.6.0.0/16)'). Below these is an 'Add' button and a 'Delete' button. The 'Remote Networks' tab is also visible, showing a 'VPN Interface Index' field with the value '11', a 'Remote Network' field (with a placeholder '(e.g. 10.6.0.0/16)'), an 'Advertise Route' checkbox, and 'Add' and 'Delete' buttons. Both tabs have a table with a header 'Addr/Mask' and several empty rows.

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

## Step 4. Configure the OSPF Service

The OSPF setup must be completed on both the local and remote firewalls. The configuration steps and values are the same except for the Router ID and propagated networks.

### Step 4.1 Configure which Routes to Propagate into OSPF

Select the routes you want to propagate.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.

3. To propagate the management network, set **Advertise Route** to **yes** in the **Management IP and Network** section.

**Management IP and Network**

Interface Name	eth0	<input type="checkbox"/> Other
Management IP (MIP)	10.0.10.88	
Associated Netmask	25-Bit	
Responds to Ping	yes	
Use for NTPd	yes	
Advertise Route	yes	

4. In the left menu, click on **Routing**.
5. Double-click on the direct attached and gateway routes you want to propagate. The **Routes** window opens.
6. Set **Advertise Route** to **yes** and click **OK**.

**Route Configuration**

Target Network Address	10.17.0.0/16	
Route Type	gateway	
Interface Name		<input type="checkbox"/> Other
Gateway	10.0.10.1	
Route Metric		
Source Address		
Trust Level	Unclassified	
Default Gateway		
Advertise Route	yes	
Route Origin	User created	
Active	yes	

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

#### Step 4.2 Configure the OSPF Router

Enable OSPF and use the VPN Next Hop interface IP address as the Router ID.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
2. Click **Lock**.
3. Set **Run OSPF Router** to **Yes**.
4. Set **Operation Mode** to **advertise-learn**.
5. Enter the **Router ID**. Typically the VPN next hop interface IP address is used. E.g., 192.168.20.1 for the local CloudGen Firewall, or 192.168.20.2 for the remote firewall.

**Operational Setup**

Run OSPF Router	yes	
Run RIP Router	no	
Run BGP Router	no	
Hostname	HQVIRT1	
Operation Mode	advertise-learn	
Router ID	192.168.20.1	 

6. In the left menu, click **OSPF Router Setup**.
7. Select **Cisco Type** from the **ABR Type** drop-down.
8. Enter the **Terminal Password**. Use this password if you must directly connect to the dynamic routing daemon via command line for debugging purposes.  

The password can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).
9. Click **Send Changes** and **Activate**.

#### Step 4.3. Create an OSPF Area Setup

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
2. Click **Lock**.
3. In the left menu click **OSPF Area Setup**.
4. In the **OSPF Area Configuration**, click + to add **Areas**.
5. Enter the OSPF area **Name**.
6. Click **OK**. The **Areas** window opens.
7. From the **Area ID Format** dropdown, select **Integer**.
8. Enter the **Area ID[Int]**. E.g., 0
9. If authentication is selected in the **Parameter Template** select the **Authentication Type**.
10. Click + add the VPN next hop interface network to the **Network Prefix** table: E.g., 192.168.20.0/24

**OSPF Area Configuration**

Enable Configuration	yes	
Area ID Format	Integer	
Area ID [IP]		
Area ID [Int]	0	
Authentication Type	NONE	
Special Type	NONE	
NSSA-ABR Translate Election	candidate	
Disable Summary	no	
Area Default Cost		
Network Prefix	<div>192.168.20.0/24</div>	

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

## Step 6. Verify the OSPF Service Configuration

On the **CONTROL > Network** page, verify that OSPF is active on the VPN next hop interface and that the remote CloudGen Firewall is listed as an OSPF neighbor. The routes learned via OSPF are listed with a type of **gateway-ospf** in the routing table. The **Interface** is the VPN next hop interface and the **Gateway** the IP address of the remote VPN next hop interface IP address.

Local Firewall **CONTROL > Network > OSPF** page:

Interfaces/IPs	IPs	Interfaces	Proxy ARPs	ARPs	Statistics	OSPF	RIP	BGP	Switch Info	IPv6 ND Cache					
Interface/Neighbour	Prio	State	Dead Time	Address	Interface										
Neighbour-192.168.20.2	1	Full/DR	31.841s	192.168.20.2	vpn11:192.168....										
Interface-eth0															
Interface-eth1															
Interface-eth2															
Interface-eth3															
Interface-eth4															
Interface-pvpn0															
Interface-vpn11															
Interface-vpn11	ifindex 19, MTU 1398 bytes, BW 102400 Kbit <UP,BROADCAST,RUNNING,MULTICAST> Internet Address 192.168.20.1/24, Area 0.0.0.0 MTU mismatch detection:enabled Router ID 192.168.20.1, Network Type BROADCAST, Cost: 10 Transmit Delay is 1 sec, State Backup, Priority 1 Designated Router (ID) 192.168.20.2, Interface Address 192.168.20.2 Backup Designated Router (ID) 192.168.20.1, Interface Address 192.168.20.1 Multicast group memberships: OSPFAI/Routers OSPFDesignatedRouters Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5 Hello due in 5.143s Neighbor Count is 1, Adjacent neighbor count is 1														

TABLES

ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
<b>Table main, From all</b>							
2001:db8:6299::/48	off	direct-kernel	eth1	-	100	-	ISP1
10.0.10.0/25	up	direct-adv	eth0	10.0.10.33	0	-	boxnet
10.0.11.0/25	up	gateway-boot	eth0	10.0.10.33	0	10.0.10.77	VIPS
10.0.15.0/24	up	gateway-boot	eth0	10.0.10.33	0	10.0.10.1	LAB2
10.0.16.0/24	up	gateway-boot	eth0	10.0.10.33	0	10.0.10.1	LAB2VIP
10.0.80.0/24	up	gateway-ospfext	vpn11	-	20	192.168.20.2	
10.17.0.0/16	up	gateway-boot	eth0	10.0.10.33	0	10.0.10.1	Homenet
10.20.0.0/24	up	direct-boot	eth4	10.20.0.3	0	-	MPLS
10.21.0.0/24	up	gateway-boot	eth4	10.20.0.3	0	10.20.0.254	BO1-MPLS
10.22.0.0/24	up	gateway-boot	eth4	10.20.0.3	0	10.20.0.254	BO2-MPLS
127.0.3.0/24	up	direct-kernel	pvpn0	127.0.3.1	0	-	
127.0.3.0/24	up	direct-kernel	vpn11	127.0.3.1	0	-	
172.16.0.0/24	up	direct-boot	eth3	172.16.0.254	0	-	HQ-DMZ
192.168.20.0/24	up	direct-kernel	vpn11	192.168.20.1	0	-	
192.168.20.0/24	up	direct-ospfext	vpn11	-	10	-	
194.93.0.0/24	up	direct-boot	eth2	194.93.0.10	200	-	HQ-ISP2
62.99.0.0/24	up	direct-boot	eth1	62.99.0.40	100	-	HQ-ISP1

Remote Firewall **CONTROL > Network > OSPF** page:





## Figures

1. OSPF\_VPN\_01.png
2. OSPF\_VPN\_02.png
3. OSPF\_VPN\_GTI\_01.png
4. OSPF\_VPN\_GTI\_02.png
5. S2S\_routed\_VPN.png
6. tina\_bgp06d.png
7. tina\_bgp06c.png
8. OSPF\_VPN\_05.png
9. OSPF\_VPN\_06.png
10. OSPF\_VPN\_08.png
11. OSPF\_VPN\_09.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.