



# How to Configure OSPF Routing over TINA VPN

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 Barracuda NextGen F-Series Firewalls by using the respective values below:

	Example Values for the Local Barracuda NextGen Firewall F-Series	Example Values for the Remote Barracuda NextGen Firewall F-Series
<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>Virtual Server Additional 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

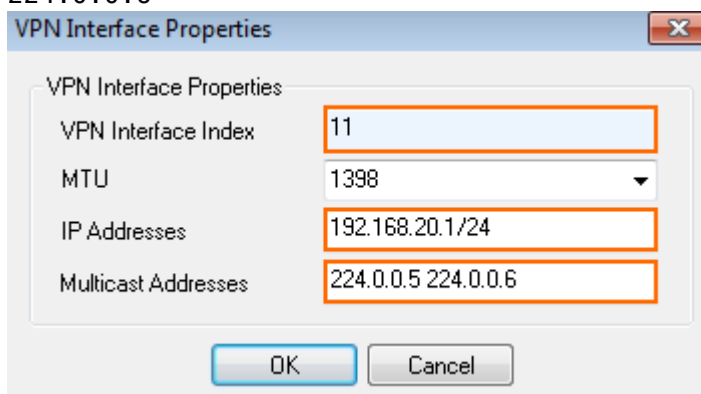
## Before You Begin

- 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 > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the **Settings** tab, click the **Click here for Server Settings** link. The **Server Settings** window opens.
4. In the **Server Settings** window, click the **Advanced** tab.
5. Next to the **VPN Next Hop Interface Configuration** table, click **Add**.
6. 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 NextGen Firewall F-Series, or 192.168.20.2/24 for the remote NextGen Firewall F-Series.
  - In the **Multicast Addresses** field, enter the OSPF Multicast Addresses: 224.0.0.5 224.0.0.6



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



VPN Next Hop Interface Configuration

VPN Interf...	MTU	IPs	Multicast
vpn11	1398	192.168.20.1/24	224.0.0.5 224.0.0.6

Add... Edit... Delete

7. In the **Server Settings** window, click **OK**.

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

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

Introduce the IP address of the VPN Next Hop interface as a virtual server IP address.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Server Properties** .
2. Click **Lock** .
3. In the **Additional IP** table, add the IP address of the VPN Next Hop interface.

Additional IP

Additional IP	Label	Reply to Ping	Descrip
172.16.0.254	IP3	1	
194.93.0.10	IP4	1	
10.20.0.3	IP5	1	
10.0.10.84	IP6	1	
192.168.20.1	IP7	1	

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

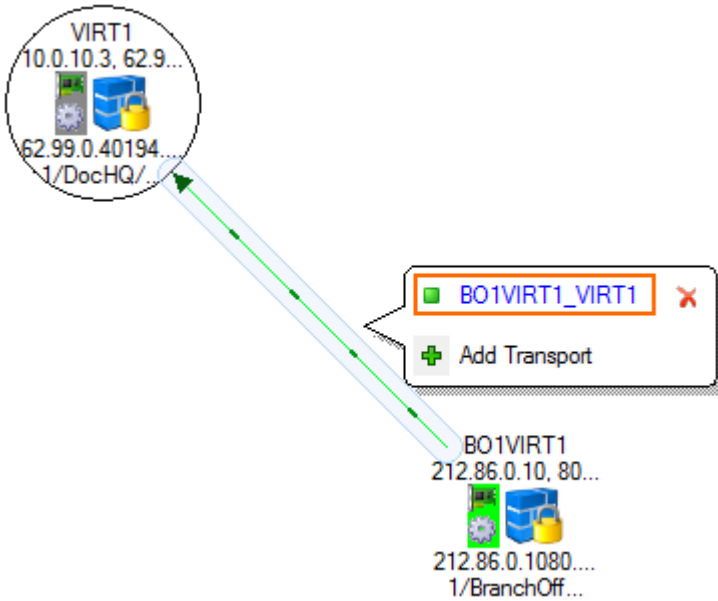
### Step 3. Configure the TINA Site-to-Site VPN Tunnels

You can configure the VPN tunnel using the GTI Editor for managed F-Series Firewalls, or using the Site-to-Site configuration dialog if you are using standalone F-Series 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](#).



- Remove all **Local Networks** from the remote and local VPN services.
- Enter the VPN Next Hop interface ID for the remote and local VPN services. E.g., 11

TINA Tunnel BO1VIRT1_VIRT1		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
Explicit	212.86.0.10, 80.130.45.10	Authentication	MD5	Explicit	62.99.0.40, 194.93.0.10
Transport Listening IP/Hostname	<Use-Transport-Source>	TI Classification	Bulk	Transport Listening IP/Hostname	<Use-Transport-Source>
Explicit Listening	212.86.0.10, 80.130.45.10	TI-ID	0	Explicit Listening	62.99.0.40, 194.93.0.10
<b>Local Networks</b>		Compression	No	<b>Local Networks</b>	
<input checked="" type="checkbox"/> <b>Advanced</b> Routing Next-Hop OnDemand Transport Timeout OnDemand Transport Delay Device Index: 11		Dynamic Mesh	No	<input checked="" type="checkbox"/> <b>Advanced</b> Routing Next-Hop OnDemand Transport Timeout OnDemand Transport Delay Device Index: 11	
<input checked="" type="checkbox"/> <b>Proxy</b> <input checked="" type="checkbox"/> <b>Security</b> Root Certificate X509 Certificate Condition Server Key: Hash: ZNTIOP Server Certificate: Hash: ZNTIOP self-signed		Dynamic Mesh Timeout	600	<input checked="" type="checkbox"/> <b>Proxy</b> <input checked="" type="checkbox"/> <b>Security</b> Root Certificate X509 Certificate Condition Server Key: Hash: IGQFOO Server Certificate: Hash: IGQFOO self-signed	
<input checked="" type="checkbox"/> <b>Scripts</b> Start Script Stop Script		<input checked="" type="checkbox"/> <b>Traffic Intelligence</b> <input checked="" type="checkbox"/> <b>TI - Bandwidth Protection</b> <input checked="" type="checkbox"/> <b>TI - VPN Envelope Policy</b> <input checked="" type="checkbox"/> <b>Advanced</b> Key Time Limit: 10 mins Key Traffic Limit: No Limit Identification Type: Public Key Tunnel Probing: 30 secs Tunnel Timeout: 20 secs Packet Balancing: None High Performance Settings: No	<input checked="" type="checkbox"/> <b>WANOpt</b> WANOpt Policy: NO-WANOpt	<input checked="" type="checkbox"/> <b>Scripts</b>	
		<input checked="" type="checkbox"/> <b>GTI Settings</b> Hide in Barracuda NG Earth: No			

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

### Standalone F-Series 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.

- Log into the local NextGen Firewall F-Series
- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Site to Site**.
- Click **Lock**.
- Right-click in the **TINA Tunnels** tab and select **New TINA tunnel**. The **TINA tunnel** window opens.
- Enter a **Name**.
- 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 F-Series Firewalls](#).
- 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 configuration page for a VPN tunnel named 'S2SwthOSPF'. The 'Remote Networks' tab is selected, and the 'VPN Interface Index' is set to 11. Below this, there are two sections: 'Local Networks' and 'Remote Networks'. Each section has a table with a header 'Addr/Mask' and several empty rows for adding network addresses. The 'Local Networks' section also includes a 'Call Direction' dropdown set to 'Active' and a 'Local Network Scheme' dropdown set to '-explicit-'. The 'Remote Networks' section includes an 'Advertise Route' checkbox and 'Add' and 'Delete' buttons.

- 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.

The screenshot shows the 'Management IP and Network' configuration page. The 'Interface Name' is 'eth0', 'Management IP (MIP)' is '10.0.10.88', and 'Associated Netmask' is '25-Bit'. The 'Responds to Ping' and 'Use for NTPd' options are set to 'yes'. The 'Advertise Route' dropdown is highlighted with an orange box and is set to '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.



- 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="text"/> <input type="checkbox"/> Other
Gateway	10.0.10.1
Route Metric	<input type="text"/>
Source Address	<input type="text"/>
Trust Level	Unclassified
Default Gateway	<input type="text"/>
Advertise Route	yes
Route Origin	User created
Active	yes

- 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.

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
- Click **Lock**.
- Set **Run OSPF Router** to **Yes**.
- Set **Operation Mode** to **advertise-learn**.
- Enter the **Router ID**. Typically the VPN Next Hop interface IP address is used. E.g., 192.168.20.1 for the local NextGen Firewall F-Series, or 192.168.20.2 for the remote NextGen Firewall F-Series.

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

- In the left menu, click **OSPF Router Setup**.
- Select **Cisco Type** from the **ABR Type** dropdown.
- Enter the **Terminal Password**. Use this password if you must directly connect to the dynamic routing daemon via command line for debugging purposes.
- Click **Send Changes** and **Activate**.



### Step 4.3. Create an OSPF Area Setup

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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 style="border: 1px solid orange; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>192.168.20.0/24</span> </div> </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 NextGen Firewall F-Series 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:

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...
<b>Interface-eth0</b>					
<b>Interface-eth1</b>					
<b>Interface-eth2</b>					
<b>Interface-eth3</b>					
<b>Interface-eth4</b>					
<b>Interface-pvpn0</b>					
<b>Interface-vpn11</b>					
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: OSPFAIRouters 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

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
<b>Table main, From all</b>							
2001:db8:6299::/48	off	direct-kemel	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-kemel	pvpn0	127.0.3.1	0	-	
127.0.3.0/24	up	direct-kemel	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-kemel	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:

Interface/Neighbour	Prio	State	Dead Time	Address	Interface
Neighbour-192.168.20.1	1	Full/Backup	31.823s	192.168.20.1	vpn11:192.168...

<b>Interface-vpnr11</b>	
ifindex 184, MTU 1398 bytes, BW 102400 Kbit <UP,BROADCAST,RUNNING,MULTICAST>	
Internet Address 192.168.20.2/24, Area 0.0.0.0	
MTU mismatch detection:enabled	
Router ID 192.168.20.2, Network Type BROADCAST, Cost: 10	
Transmit Delay is 1 sec, State DR, 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	
Saved Network-LSA sequence number 0x80000006	
Multicast group memberships: OSPFAIRouters OSPFDesignatedRouters	
Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5	
Hello due in 3.440s	
Neighbor Count is 1, Adjacent neighbor count is 1	

TABLES

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
<b>Table vpn2mc, From 10.0.11.19</b>							
Table vpn2inet, From 10.0.11.19							
Table vpnlocal, From all							
<b>Table main, From all</b>							
10.0.10.0/25	up	gateway-ospfext	vpn11	-	20	192.168.20.1	
10.0.80.0/24	up	direct-adv	eth0	10.0.80.28	0	-	boxnet
10.20.0.0/24	up	gateway-boot	eth3	10.21.0.3	0	10.21.0.254	HQ-MPLS
10.21.0.0/24	up	direct-boot	eth3	10.21.0.3	0	-	MPLS
10.22.0.0/24	up	gateway-boot	eth3	10.21.0.3	0	10.21.0.254	BO2-MPLS
127.0.3.0/24	up	direct-kemel	vpn11	127.0.3.1	0	-	
192.168.20.0/24	up	direct-kemel	vpn11	192.168.20.2	0	-	
192.168.20.2/32	up	direct-ospfext	lo	192.168.20.2	10	-	
212.86.0.0/24	up	direct-boot	eth1	212.86.0.28	0	-	NETW01
80.130.45.0/24	up	direct-boot	eth2	80.130.45.10	0	-	BO1-ISP2
<b>Table BO1ISP1, From 212.86.0.0/24</b>							
<b>Table BOISP2, From 80.130.45.0/24</b>							
<b>Table default, From all</b>							
0.0.0.0/0	up	gateway-boot	eth1	212.86.0.28	0	212.86.0.254	ROUT01

### Step 6. Create Access Rules for VPN Traffic

Create access rules on both local and remote firewalls to allow traffic from the learned networks through the VPN tunnel. For more information, see [How to Create Access Rules for Site-to-Site VPN Access](#).



