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
VPNR Next Hop Interface Index	1	1
VPN Next Hop Interface IP Address	192.168.20.1/24	192.168.20.2/24
Virtual Server Additional IP	192.168.20.1	192.168.20.2
VPN Local Networks	empty	empty
VPN Remote Networks	empty	empty
Router ID	192.168.20.1	192.168.20.2

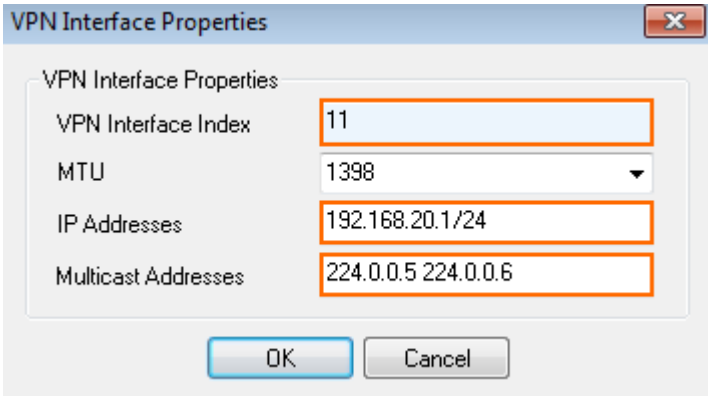
Before You Begin

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

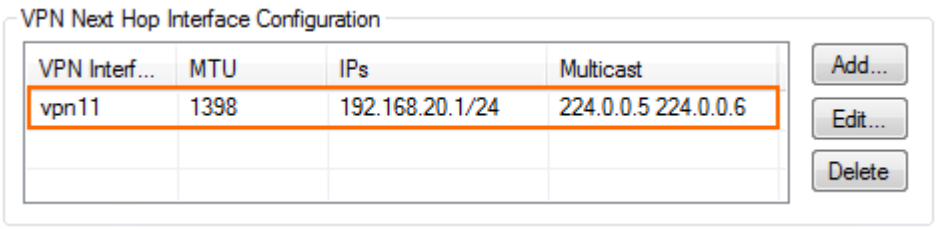
Step 1. Add a VPN Next Hop Interface

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.

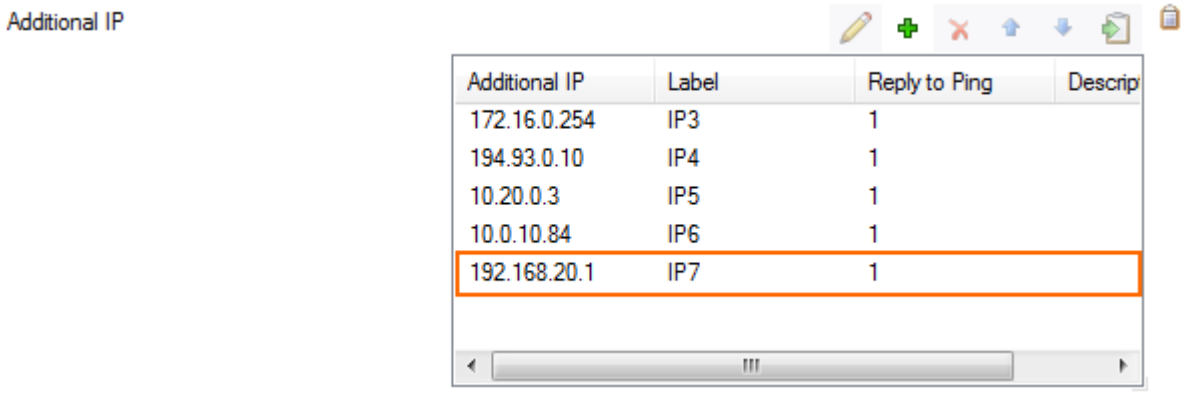


7. In the **Server Settings** window, click **OK**.
8. Click **Send Changes** and **Activate**.

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.



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

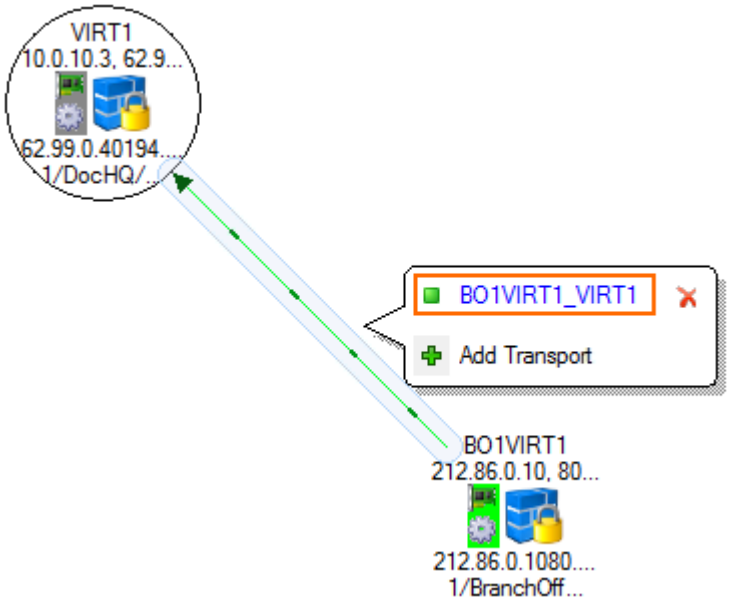
Step 3. Configure the TINA Site-to-Site VPN Tunnels

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.

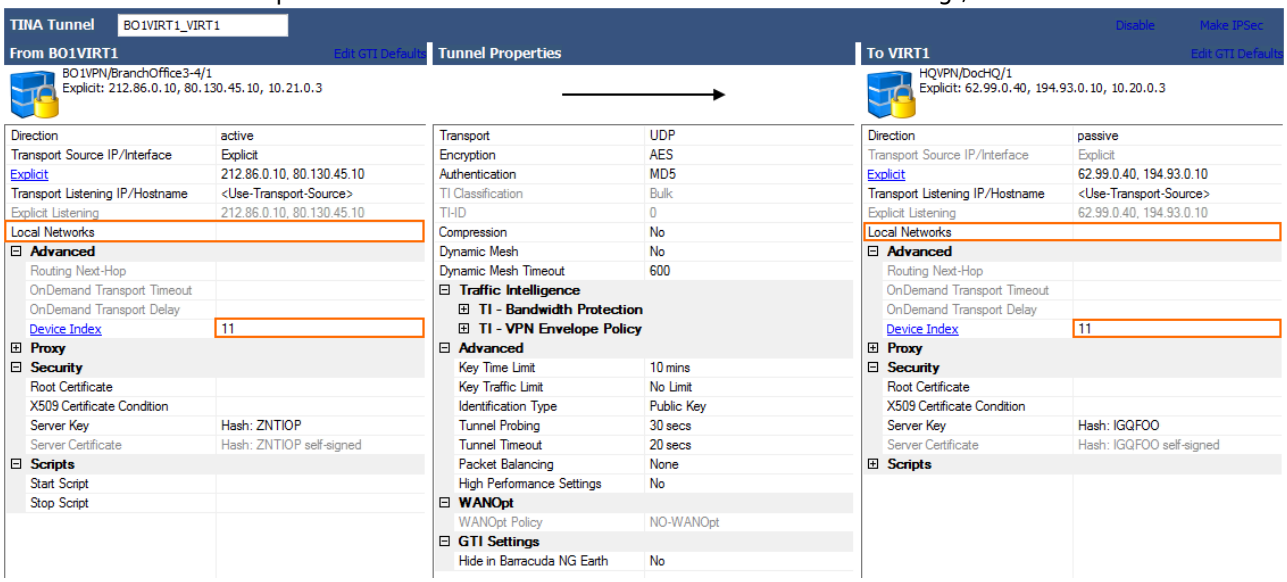
In the GTI Editor

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.



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



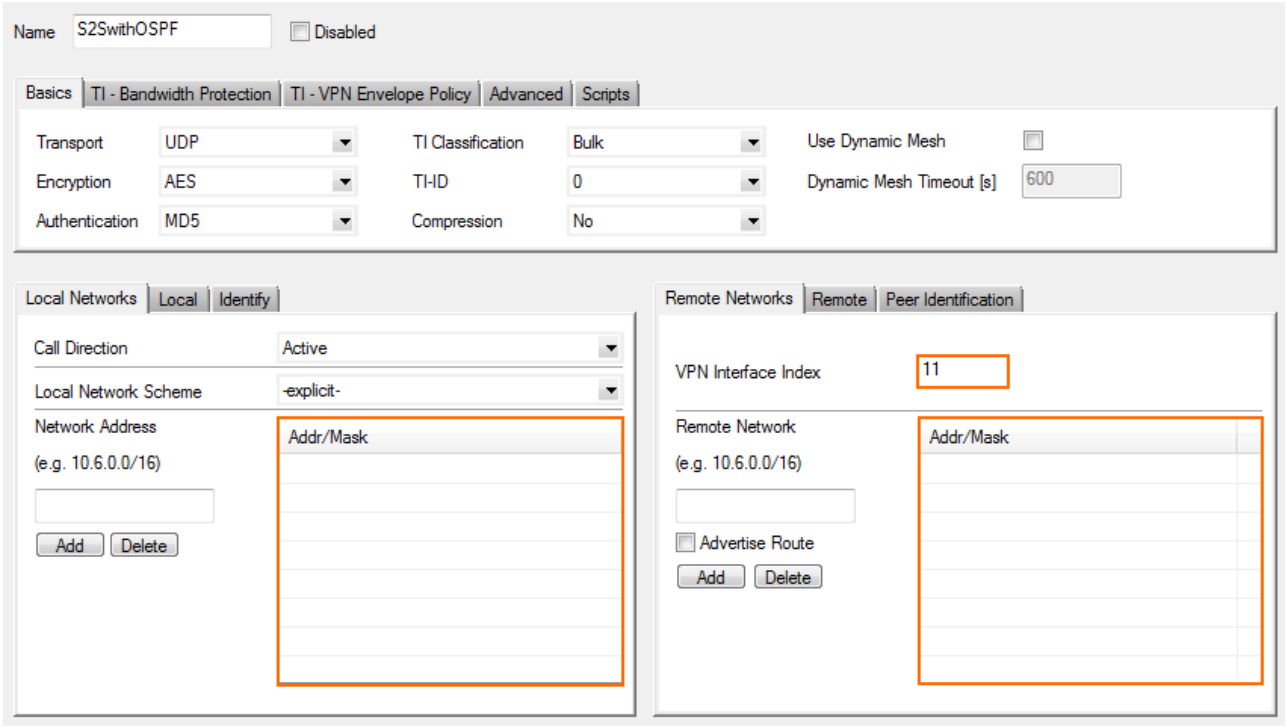
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

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.

1. Log into the local NextGen Firewall F-Series
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > 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 F-Series 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



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

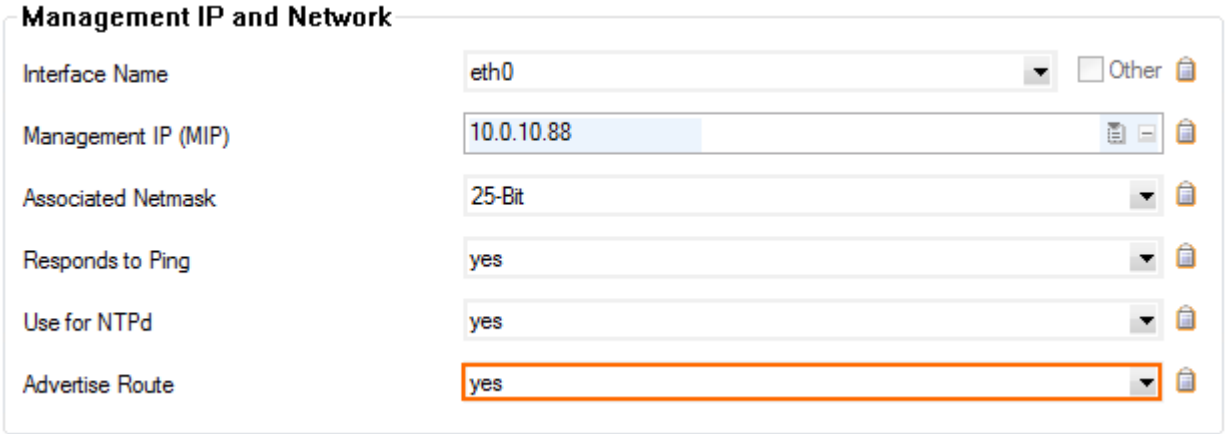
Step 4. Configure the OSPF Service

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

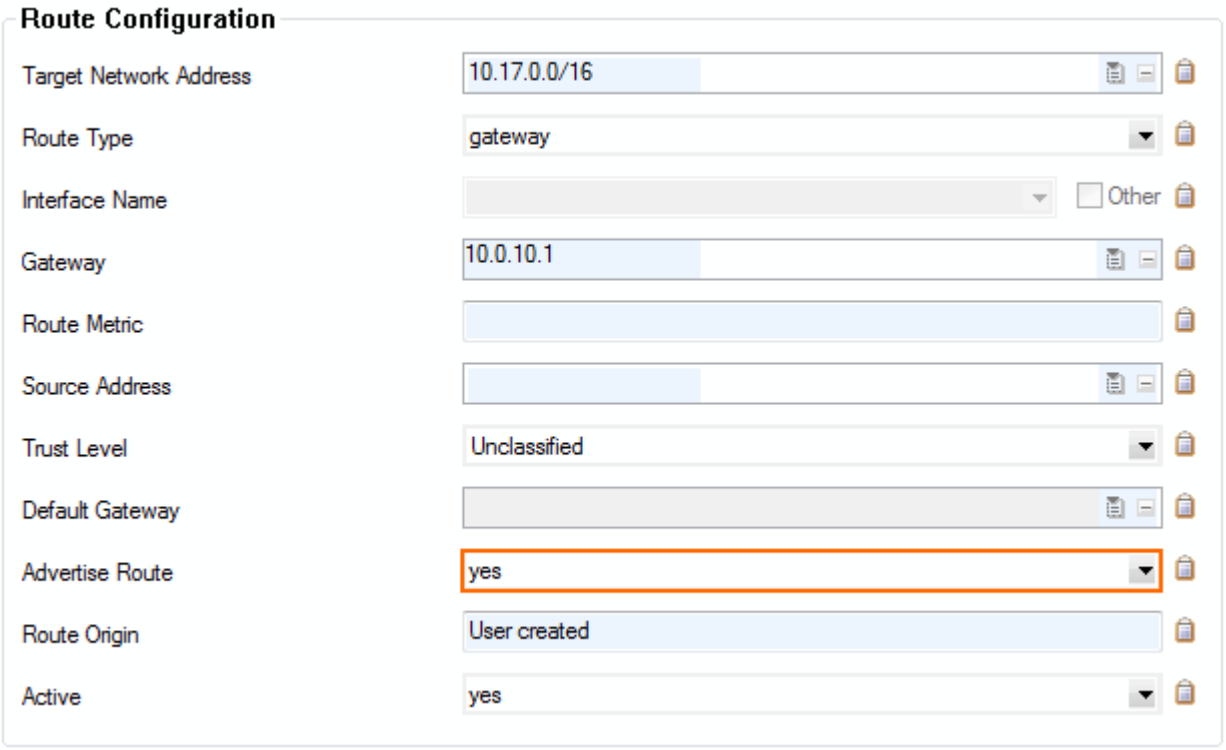
Select the routes you want to propagate.

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.



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**.



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

Step 4.2 Configure the OSPF Router

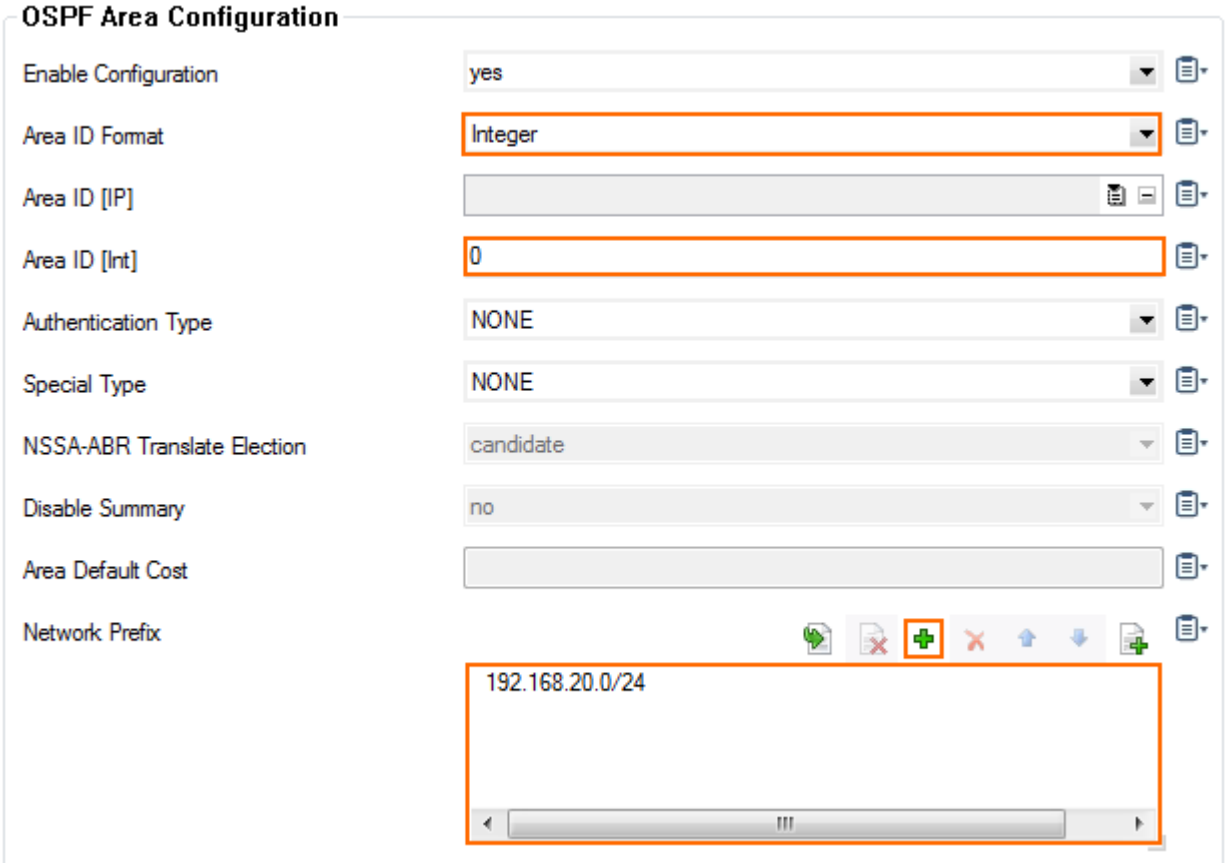
Enable OSPF and use the VPN Next Hop interface IP address as the Router ID.

1. Go to **CONFIGURATION** > **Configuration Tree > Box > Virtual Servers > *your virtual server* > 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 NextGen Firewall F-Series, or `192.168.20.2` for the remote NextGen Firewall F-Series.

6. In the left menu, click **OSPF Router Setup**.
7. Select **Cisco Type** from the **ABR Type** dropdown.
8. Enter the **Terminal Password**. Use this password if you must directly connect to the dynamic routing daemon via command line for debugging purposes.
9. 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`

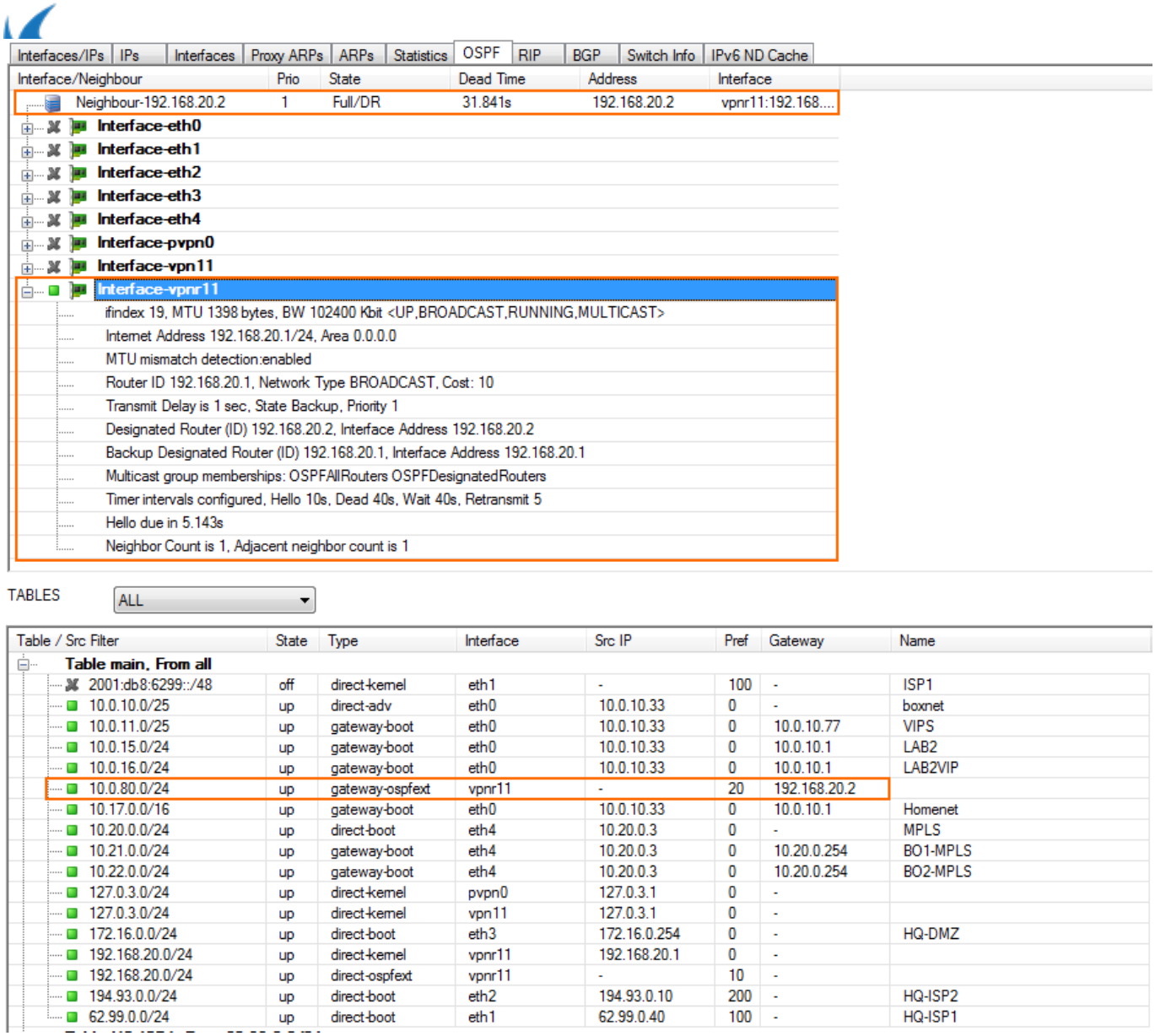


11. Click **OK**.
12. Click **Send Changes** and **Activate**.

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:



Interfaces/IPs | IPs | Interfaces | Proxy ARPs | ARPs | Statistics | OSPF | RIP | BGP | Switch Info | IPv6 ND Cache

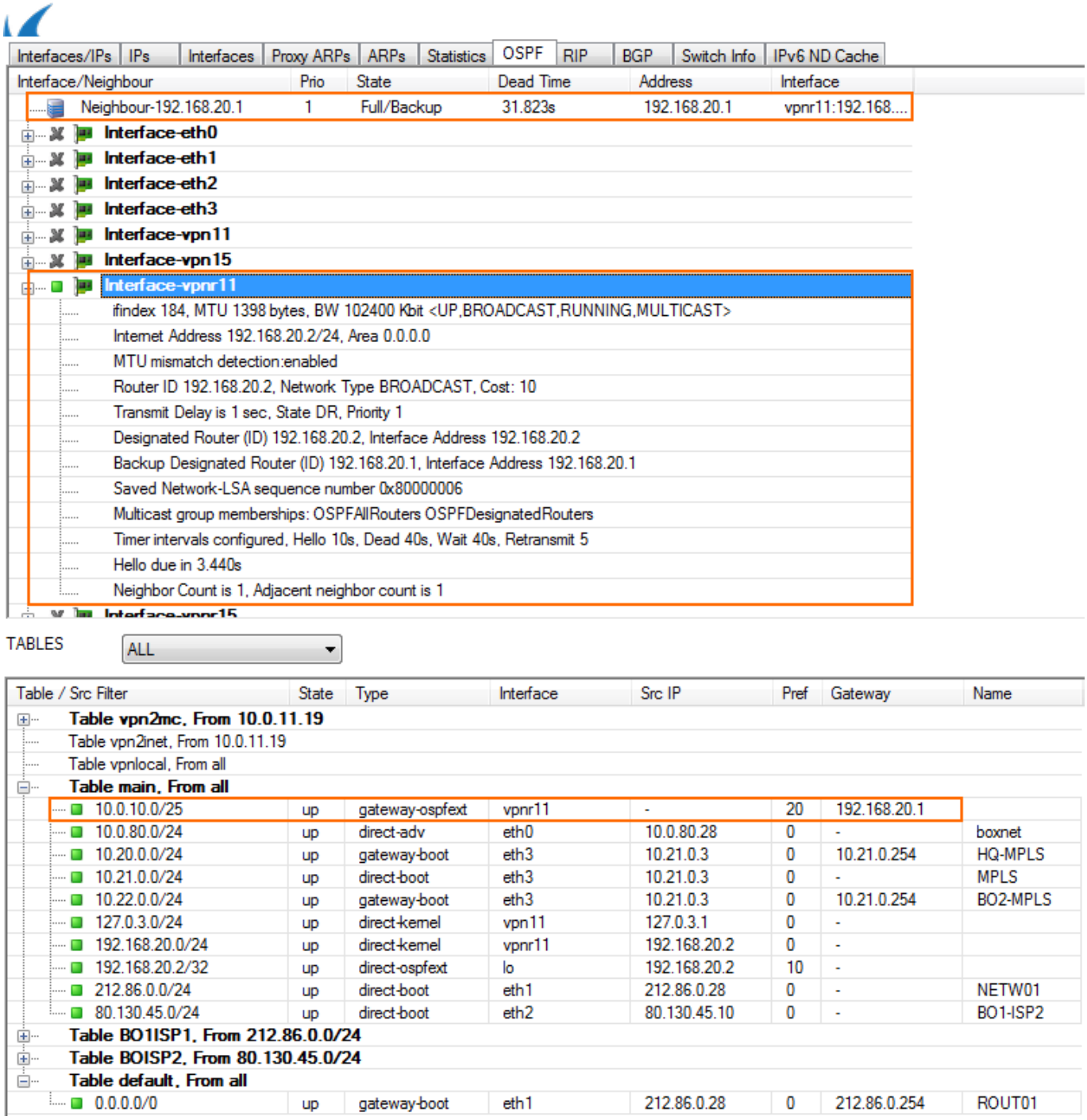
Interface/Neighbour	Prio	State	Dead Time	Address	Interface
Neighbour-192.168.20.2	1	Full/DR	31.841s	192.168.20.2	vpnr11:192.168....
Interface-eth0					
Interface-eth1					
Interface-eth2					
Interface-eth3					
Interface-eth4					
Interface-pvpn0					
Interface-vpn11					
Interface-vpnr11					

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: OSPFAllRouters 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
Table main, From all							
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	vpnr11	-	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	vpnr11	192.168.20.1	0	-	
192.168.20.0/24	up	direct-ospfext	vpnr11	-	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:



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.

Figures