

How to Configure OSPF Routing over TINA VPN

<https://campus.barracuda.com/doc/79462783/>

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 |
|--|---------------------------------------|--|
| VPN Next Hop Interface Index | 1 | 1 |
| VPN Next Hop Interface IP Address | 192.168.20.1/24 | 192.168.20.2/24 |
| Box 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.

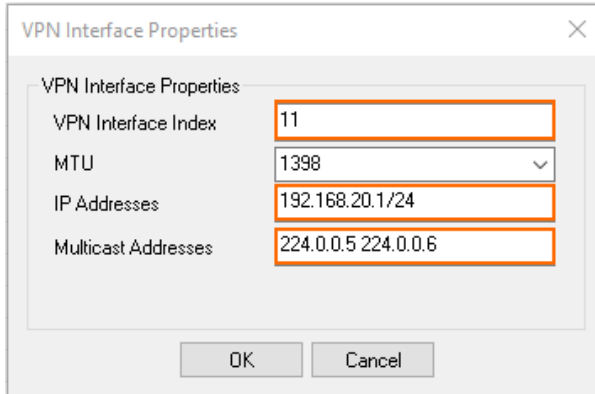
Step 1. Add a VPN Next Hop Interface

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

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 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 Properties

VPN Interface Index: 11

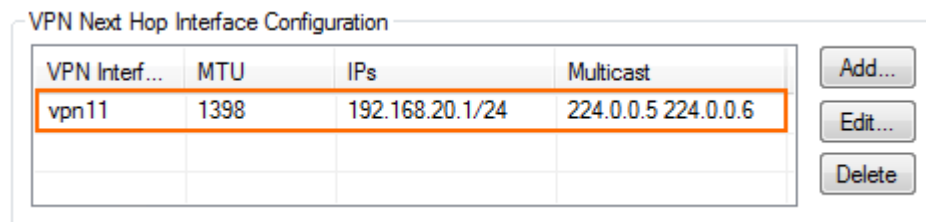
MTU: 1398

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 **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 |

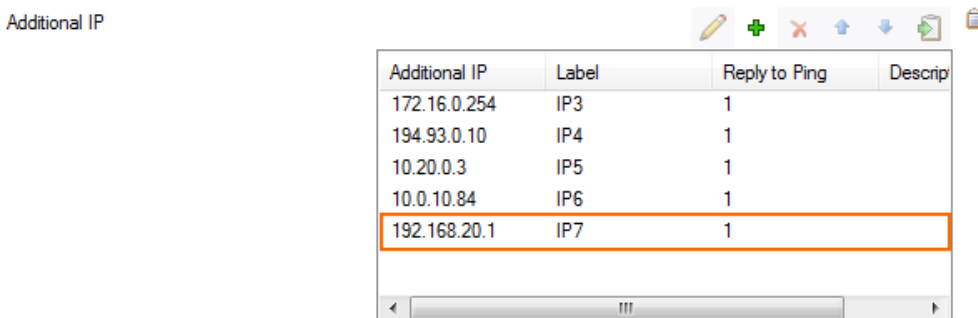
Add... Edit... Delete

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 Firewall Listening IP Addresses

Introduce the IP address of the VPN next hop interface as a box IP address.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
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**.

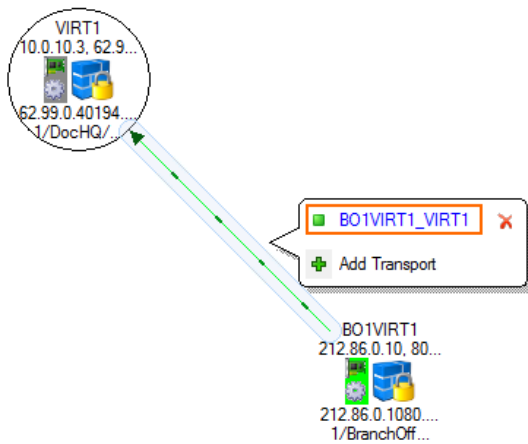
Step 3. Configure the TINA Site-to-Site VPN Tunnels

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

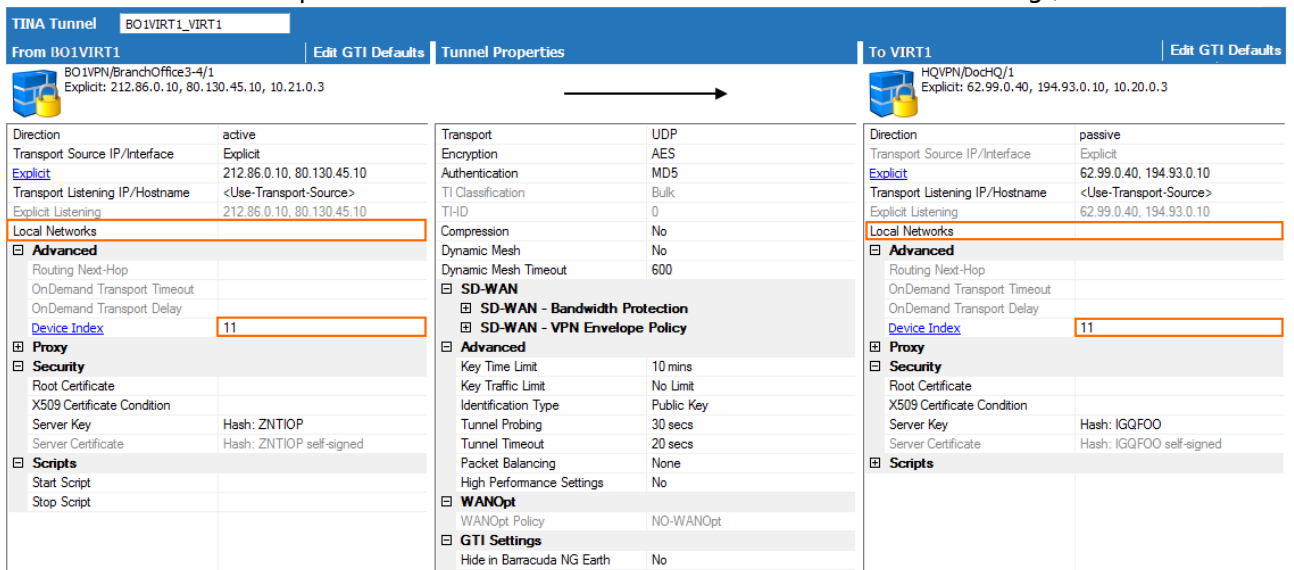
In the GTI Editor

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



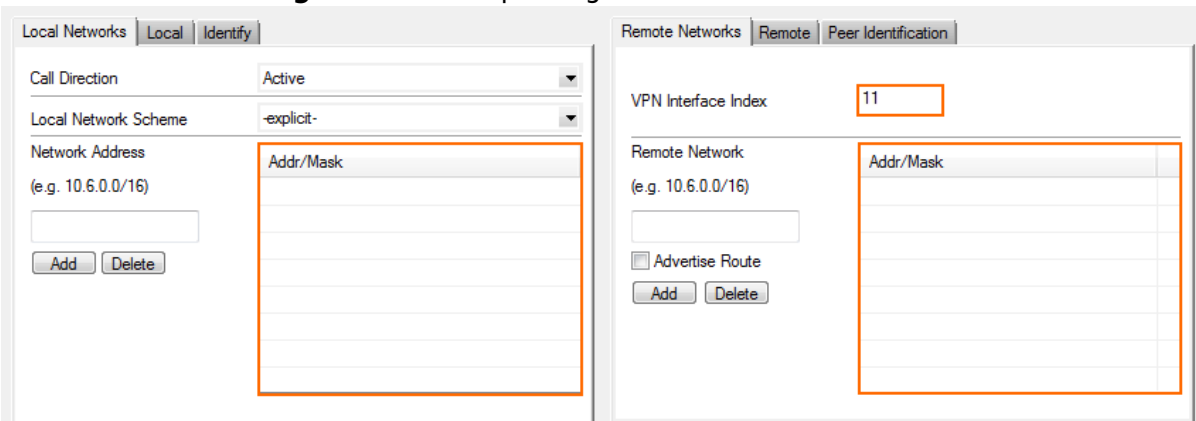
| From BO1VIRT1 | Tunnel Properties | To VIRT1 |
|--|---|--|
| Direction: active Transport Source IP/Interface: Explicit Explicit: 212.86.0.10, 80.130.45.10, 10.21.0.3 Transport Listening IP/Hostname: <Use-Transport-Source> Explicit Listening: 212.86.0.10, 80.130.45.10 Local Networks: [Highlighted] Advanced: Routing Next-Hop, OnDemand Transport Timeout, OnDemand Transport Delay, Device Index: 11 Proxy: [Expanded] Security: Root Certificate, X509 Certificate Condition, Server Key (Hash: ZNTIOP), Server Certificate (Hash: ZNTIOP self-signed) Scripts: Start Script, Stop Script | Transport: UDP Encryption: AES Authentication: MD5 TI Classification: Bulk THD: 0 Compression: No Dynamic Mesh: No Dynamic Mesh Timeout: 600 SD-WAN: SD-WAN - Bandwidth Protection, SD-WAN - VPN Envelope Policy Advanced: 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) WANOpt: WANOpt Policy (NO-WANOpt) GTI Settings: Hide in Barracuda NG Earth (No) | Direction: passive Transport Source IP/Interface: Explicit Explicit: 62.99.0.40, 194.93.0.10, 10.20.0.3 Transport Listening IP/Hostname: <Use-Transport-Source> Explicit Listening: 62.99.0.40, 194.93.0.10 Local Networks: [Highlighted] Advanced: Routing Next-Hop, OnDemand Transport Timeout, OnDemand Transport Delay, Device Index: 11 Proxy: [Expanded] Security: Root Certificate, X509 Certificate Condition, Server Key (Hash: IGQFOO), Server Certificate (Hash: IGQFOO self-signed) Scripts: [Expanded] |

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 'Call Direction' set to 'Active', 'Local Network Scheme' set to '-explicit-', and an empty table for 'Network Address' with columns for 'Addr/Mask'. The 'Remote Networks' tab is also active, showing 'VPN Interface Index' set to '11', an empty table for 'Remote Network' with columns for 'Addr/Mask', and an 'Advertise Route' checkbox. Both tables have 'Add' and 'Delete' buttons below them.

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**.

- 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 | |

- In the left menu, click on **Routing**.
- 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 | |
| Gateway | 10.0.10.1 |
| Route Metric | |
| Source Address | |
| Trust Level | Unclassified |
| Default Gateway | |
| 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 > 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 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 alphanumeric 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 | 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 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:

| 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

index 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 |
|-----------------------------|-------|-----------------|-----------|--------------|------|--------------|----------|
| 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 | 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:

| Interface/Neighbour | Prio | State | Dead Time | Address | Interface |
|--|------|-------------|-----------|--------------|--------------------|
| Neighbour-192.168.20.1 | 1 | Full/Backup | 31.823s | 192.168.20.1 | vpn11:192.168.20.1 |
| Interface-eth0 | | | | | |
| Interface-eth1 | | | | | |
| Interface-eth2 | | | | | |
| Interface-eth3 | | | | | |
| Interface-vpn11 | | | | | |
| Interface-vpn15 | | | | | |
| Interface-vpnr11 | | | | | |
| 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: OSPFAllRouters 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 |
|--|-------|-----------------|-----------|--------------|------|--------------|----------|
| Table vpn2mc, From 10.0.11.19 | | | | | | | |
| Table vpn2inet, From 10.0.11.19 | | | | | | | |
| Table vpnlocal, From all | | | | | | | |
| Table main, From all | | | | | | | |
| 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-kernel | vpn11 | 127.0.3.1 | 0 | - | |
| 192.168.20.0/24 | up | direct-kernel | 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 |
| Table BO1ISP1, From 212.86.0.0/24 | | | | | | | |
| Table BOISP2, From 80.130.45.0/24 | | | | | | | |
| Table default, From all | | | | | | | |
| 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](#).

Figures

1. OSPF_VPN_01.png
2. OSPF_VPN_02.png
3. OSPF_VPN_03.png
4. OSPF_VPN_GTI_01.png
5. OSPF_VPN_GTI_02.png
6. S2S_routed_VPN.png
7. tina_bgp06d.png
8. tina_bgp06c.png
9. OSPF_VPN_05.png
10. OSPF_VPN_06.png
11. OSPF_VPN_08.png
12. OSPF_VPN_09.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.