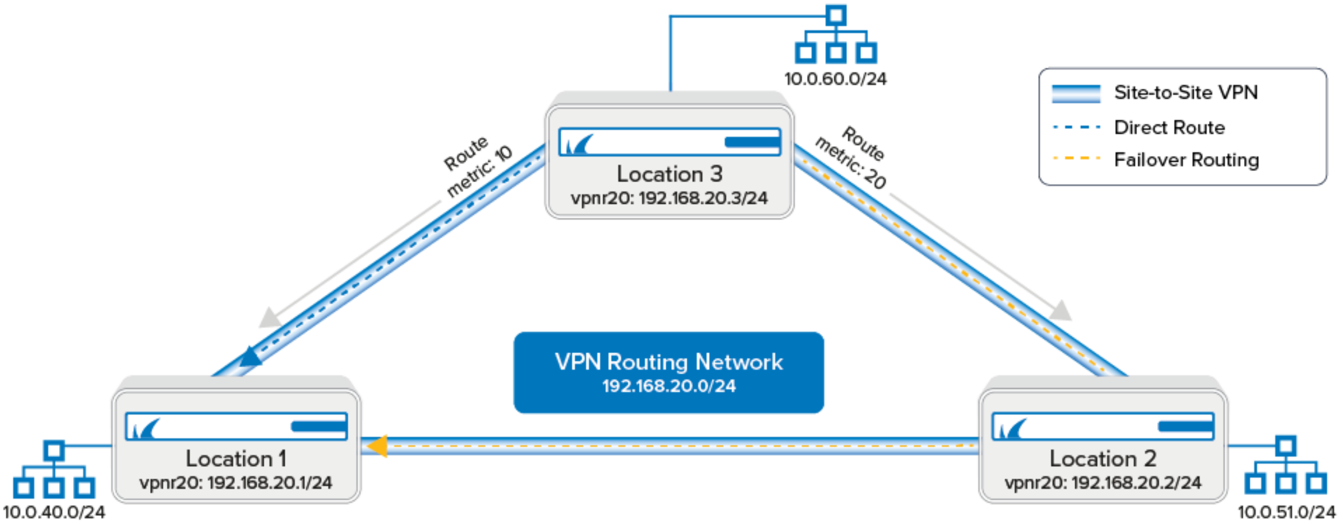
How to Configure a Routed VPN Network

https://campus.barracuda.com/doc/98210165/

In cases where SD-WAN cannot handle failover scenarios in your VPN network, use a routed VPN network. A routed VPN network uses the IP addresses assigned to the VPNR interface of the VPN tunnels as gateways. This means that the routing table and the assigned route metrics of the routes determine which tunnel is chosen. When a VPN tunnel goes down, the gateway IP address on the other side of the VPN is no longer reachable, and the route metric for the failing route is automatically increased to 65556. The backup route with the lower metric now matches and redirects the traffic over the failover route to its destination. As soon as the VPN tunnel is back up, the original route becomes available again, and traffic is sent through the direct VPN tunnel again.



Before You Begin

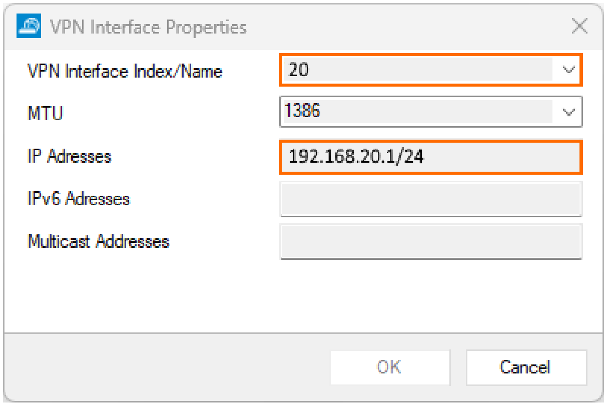
- A free subnet (e.g., `192.168.20.0/24`) for the intermediary network is needed.

Step 1. Add a VPN Next Hop Interface to Each Firewall

Add a VPN next hop interface using a /24 subnet (e.g., `192.168.20.0/24`). Use the same VPNR index for each firewall.

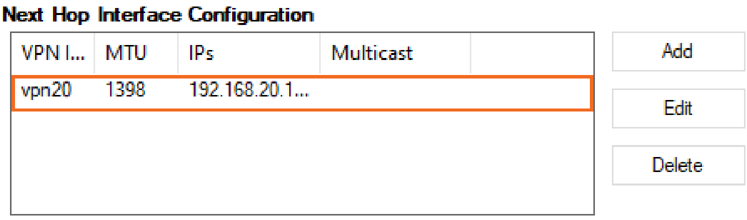
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left menu, select **Routed VPN**.

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**.
    1. In the **VPN Interface Index** field, enter a number between `0` and `999`. E.g., `20`
    2. In the **IP Addresses** field, enter a free IP address for the VPN interface IP address, including the subnet. E.g., `192.168.20.1/24`



VPN Interface Index/Name: 20
MTU: 1386
IP Adresses: 192.168.20.1/24
IPv6 Adresses:
Multicast Addresses:

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



Next Hop Interface Configuration

VPN I...	MTU	IPs	Multicast
vpn20	1398	192.168.20.1...	

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

Repeat for each firewall in the VPN network. If possible, use the same VPNR interface index on each firewall.

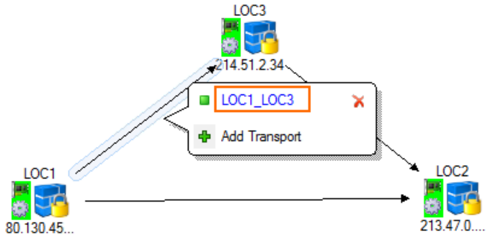
Step 2. Configure the Site-to-Site VPN Tunnel between the Firewalls

You can configure VPN tunnels connecting the firewalls using the GTI Editor for managed CloudGen Firewalls, or using the site-to-site configuration dialog if you are using stand-alone CloudGen Firewalls. This procedure works for TINA, IPsec IKEv1, and IPsec IKEv2.

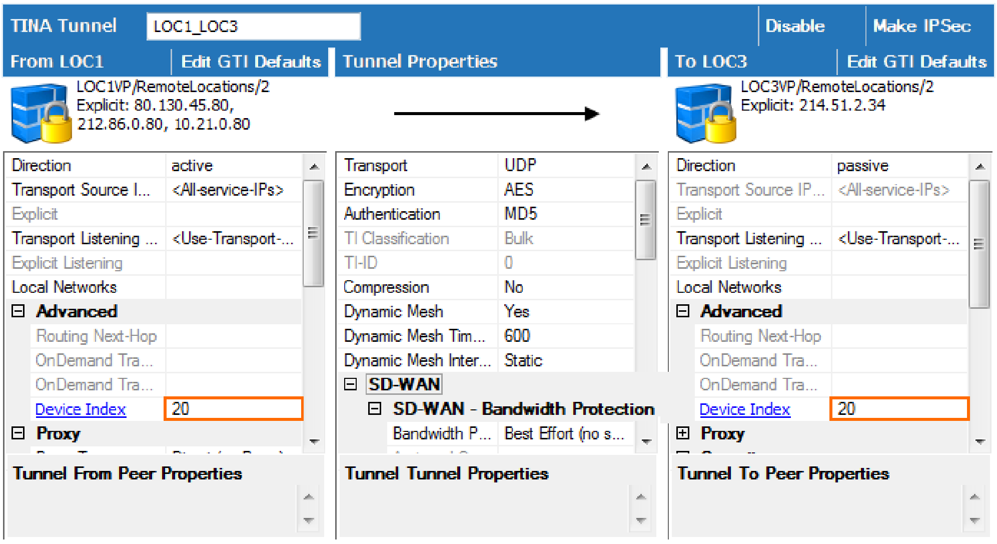
In the GTI Editor

Remove the local and remote networks and add the VPN next hop interface ID to the VPN tunnels.

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. Verify that the **Local Networks** for the remote and local VPN services are empty.
5. Enter the VPN next hop interface ID for the remote and local VPN services. E.g., `20`
   The following example shows the configuration for a TINA tunnel:


TINA Tunnel LOC1_LOC3 — Disable — Make IPSec

From LOC1 — Edit GTI Defaults | Tunnel Properties | To LOC3 — Edit GTI Defaults

LOC1VP/RemoteLocations/2
Explicit: 80.130.45.80, 212.86.0.80, 10.21.0.80

LOC3VP/RemoteLocations/2
Explicit: 214.51.2.34

Direction	active
Transport Source I...	<All-service-IPs>
Explicit	
Transport Listening ...	<Use-Transport-...
Explicit Listening	
Local Networks	
⊟ **Advanced**	
Routing Next-Hop	
OnDemand Tra...	
OnDemand Tra...	
Device Index	20
⊟ **Proxy**	

Transport	UDP
Encryption	AES
Authentication	MD5
TI Classification	Bulk
TI-ID	0
Compression	No
Dynamic Mesh	Yes
Dynamic Mesh Tim...	600
Dynamic Mesh Inter...	Static
⊟ **SD-WAN**	
⊟ **SD-WAN - Bandwidth Protection**	
Bandwidth P...	Best Effort (no s...

Direction	passive
Transport Source IP...	<All-service-IPs>
Explicit	
Transport Listening ...	<Use-Transport-...
Explicit Listening	
Local Networks	
⊟ **Advanced**	
Routing Next-Hop	
OnDemand Tra...	
OnDemand Tra...	
Device Index	20
⊞ **Proxy**	

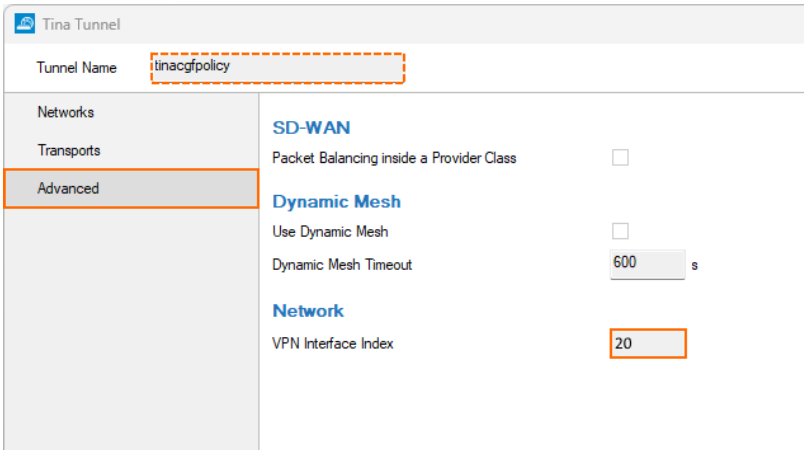
Tunnel From Peer Properties | **Tunnel Tunnel Properties** | **Tunnel To Peer Properties**

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

Stand-Alone CloudGen Firewalls

Configure a VPN tunnel using the VPN next hop interface between all firewalls.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site**.
2. Create a new TINA or IPsec VPN tunnel.
3. 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, How to Configure a Site-to-Site IPsec IKEv1 VPN Tunnel, or How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel.
4. Leave the **Local** and **Remote Network** empty.
5. In the **Remote Networks** tab, enter the **VPN Interface Index** number that you created in the **VPN Interface Configuration** in Step 1. E.g., `20`
   The following example shows the configuration for a TINA tunnel:



Tina Tunnel

Tunnel Name: tinacgfpolicy

Networks

Transports

Advanced

SD-WAN

Packet Balancing inside a Provider Class □

Dynamic Mesh

Use Dynamic Mesh □

Dynamic Mesh Timeout: 600 s

Network

VPN Interface Index: 20

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

Repeat this step until all three firewalls are connected via a Site-to-Site VPN tunnel with each other.

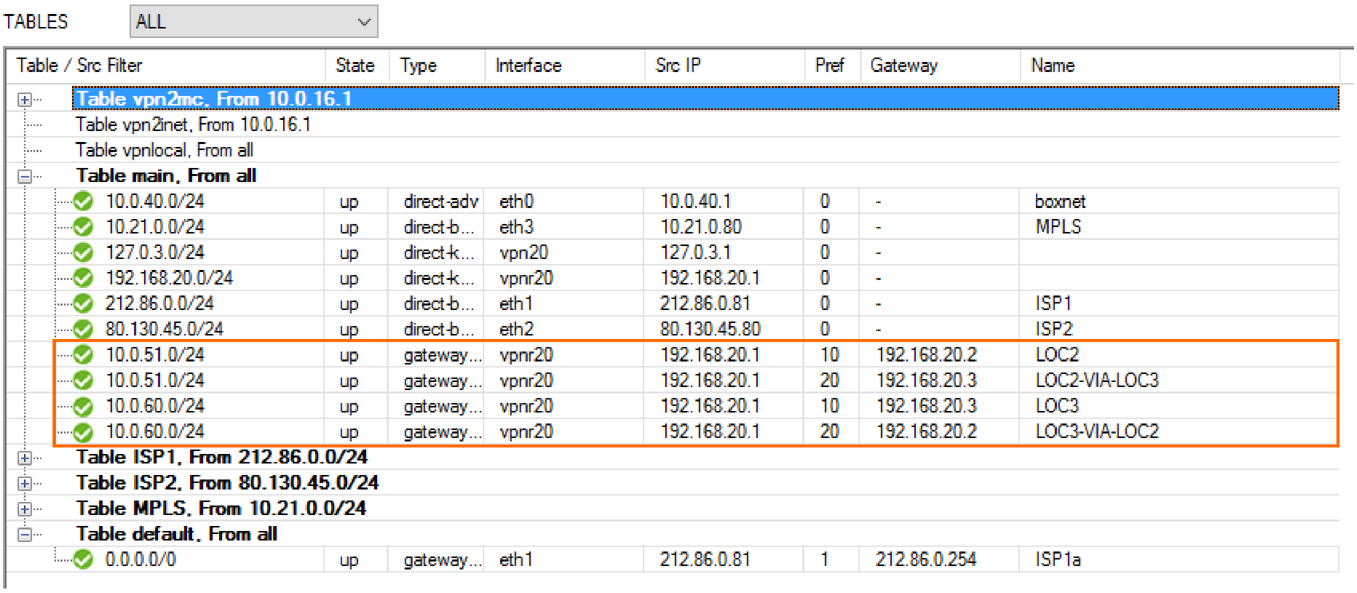
Step 3. Configure Gateway Routes for the Location 1 Firewall

Create the following primary and backup gateway routes on the Location 1 firewall. For more information, see How to Configure Gateway Routes.

1. Log into the Location 1 firewall.
2. Create a gateway route to Location 3:
   - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.60.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.3`
   - **Metric** – Enter `10`.
3. Create a gateway route to Location 2:
   - **Target Network Address** – Enter the Location 2 network in CIDR format: `10.0.51.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 2 firewall: `192.168.20.2`
   - **Metric** – Enter `10`.
4. Create a backup gateway route to Location 3 via Location 2:
   - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.60.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.2`
   - **Metric** – Enter `20`.

5. Create a backup gateway route to Location2 via Location 3:
    - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.51.0/24`
    - **Route Type** – Select **gateway**.
    - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.3`
    - **Metric** – Enter 20.
6. Activate the network configuration on the Location 3 firewall. For more information, see How to Activate Network Changes.

The Location 1 routing table now includes all gateway routes to reach the remote networks with failover routes in case the VPN tunnel goes down.



TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vpn2mc, From 10.0.16.1							
Table vpn2inet, From 10.0.16.1							
Table vpnlocal, From all							
Table main, From all							
✓ 10.0.40.0/24	up	direct-adv	eth0	10.0.40.1	0	-	boxnet
✓ 10.21.0.0/24	up	direct-b...	eth3	10.21.0.80	0	-	MPLS
✓ 127.0.3.0/24	up	direct-k...	vpn20	127.0.3.1	0	-	
✓ 192.168.20.0/24	up	direct-k...	vpnr20	192.168.20.1	0	-	
✓ 212.86.0.0/24	up	direct-b...	eth1	212.86.0.81	0	-	ISP1
✓ 80.130.45.0/24	up	direct-b...	eth2	80.130.45.80	0	-	ISP2
✓ 10.0.51.0/24	up	gateway...	vpnr20	192.168.20.1	10	192.168.20.2	LOC2
✓ 10.0.51.0/24	up	gateway...	vpnr20	192.168.20.1	20	192.168.20.3	LOC2-VIA-LOC3
✓ 10.0.60.0/24	up	gateway...	vpnr20	192.168.20.1	10	192.168.20.3	LOC3
✓ 10.0.60.0/24	up	gateway...	vpnr20	192.168.20.1	20	192.168.20.2	LOC3-VIA-LOC2
Table ISP1, From 212.86.0.0/24							
Table ISP2, From 80.130.45.0/24							
Table MPLS, From 10.21.0.0/24							
Table default, From all							
✓ 0.0.0.0/0	up	gateway...	eth1	212.86.0.81	1	212.86.0.254	ISP1a

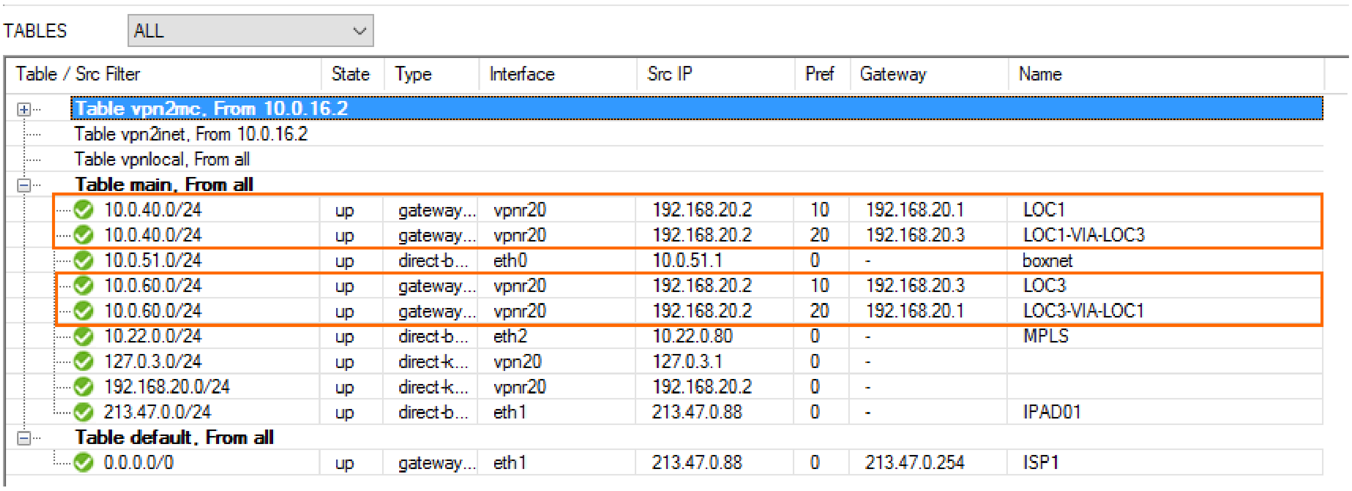
Step 4. Configure Gateway Routes for the Location 2 Firewall

Create the following primary and backup gateway routes on the Location 1 firewall. For more information, see How to Configure Gateway Routes.

1. Log into the Location 2 firewall.
2. Create a gateway route to Location 3:
    - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.60.0/24`
    - **Route Type** – Select **gateway**.
    - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.3`
    - **Metric** – Enter 10.

3. Create a gateway route to Location 1:
   - **Target Network Address** – Enter the Location 2 network in CIDR format: `10.0.15.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 2 firewall: `192.168.20.1`
   - **Metric** – Enter `10`.
4. Create a backup gateway route to Location 3 via Location 1:
   - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.51.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.1`
   - **Metric** – Enter `20`.
5. Create a backup gateway route to Location1 via Location 3:
   - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.15.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.3`
   - **Metric** – Enter `20`.
6. Activate the network configuration on the Location 3 firewall. For more information, see [How to Activate Network Changes](#).

The Location 2 routing table now includes all gateway routes to reach the remote networks with failover routes in case the VPN tunnel goes down.



TABLES ALL

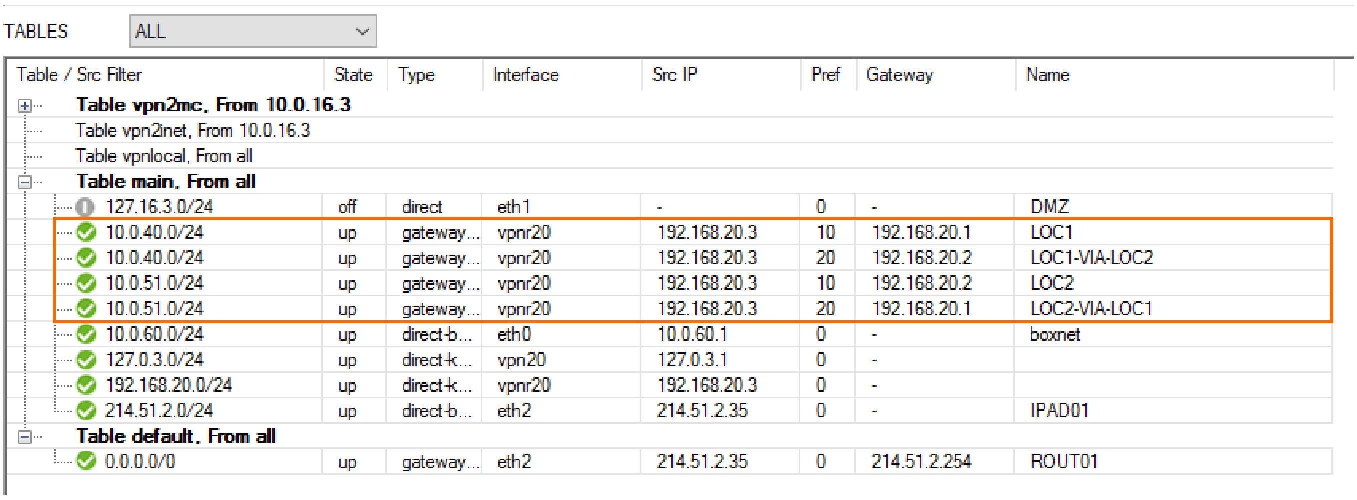
Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vpn2mc, From 10.0.16.2							
Table vpn2inet, From 10.0.16.2							
Table vpnlocal, From all							
Table main, From all							
✓ 10.0.40.0/24	up	gateway...	vpnr20	192.168.20.2	10	192.168.20.1	LOC1
✓ 10.0.40.0/24	up	gateway...	vpnr20	192.168.20.2	20	192.168.20.3	LOC1-VIA-LOC3
✓ 10.0.51.0/24	up	direct-b...	eth0	10.0.51.1	0	-	boxnet
✓ 10.0.60.0/24	up	gateway...	vpnr20	192.168.20.2	10	192.168.20.3	LOC3
✓ 10.0.60.0/24	up	gateway...	vpnr20	192.168.20.2	20	192.168.20.1	LOC3-VIA-LOC1
✓ 10.22.0.0/24	up	direct-b...	eth2	10.22.0.80	0	-	MPLS
✓ 127.0.3.0/24	up	direct-k...	vpn20	127.0.3.1	0	-	
✓ 192.168.20.0/24	up	direct-k...	vpnr20	192.168.20.2	0	-	
✓ 213.47.0.0/24	up	direct-b...	eth1	213.47.0.88	0	-	IPAD01
Table default, From all							
✓ 0.0.0.0/0	up	gateway...	eth1	213.47.0.88	0	213.47.0.254	ISP1

Step 5. Configure Gateway Routes for the Location 3 Firewall

Create the following primary and backup gateway routes on the Location 3 firewall. For more information, see How to Configure Gateway Routes.

1. Log into the Location 3 firewall.
2. Create a gateway route to Location 1:
   - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.15.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.1`
   - **Metric** – Enter `10`.
3. Create a gateway route to Location 2:
   - **Target Network Address** – Enter the Location 2 network in CIDR format: `10.0.51.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 2 firewall: `192.168.20.2`
   - **Metric** – Enter `10`.
4. Create a backup gateway route to Location 1 via Location 2:
   - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.15.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.2`
   - **Metric** – Enter `20`.
5. Create a backup gateway route to location 2 via location 1:
   - **Target Network Address** – Enter the Location 3 network in CIDR format: `10.0.51.0/24`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the IP address assigned to the VPNR interface of the Location 3 firewall: `192.168.20.`**`1`**
   - **Metric** – Enter `20`.
6. Activate the network configuration on the Location 3 firewall. For more information, see How to Activate Network Changes.

The Location 3 routing table now includes all gateway routes to reach the remote networks with failover routes in case the VPN tunnel goes down.

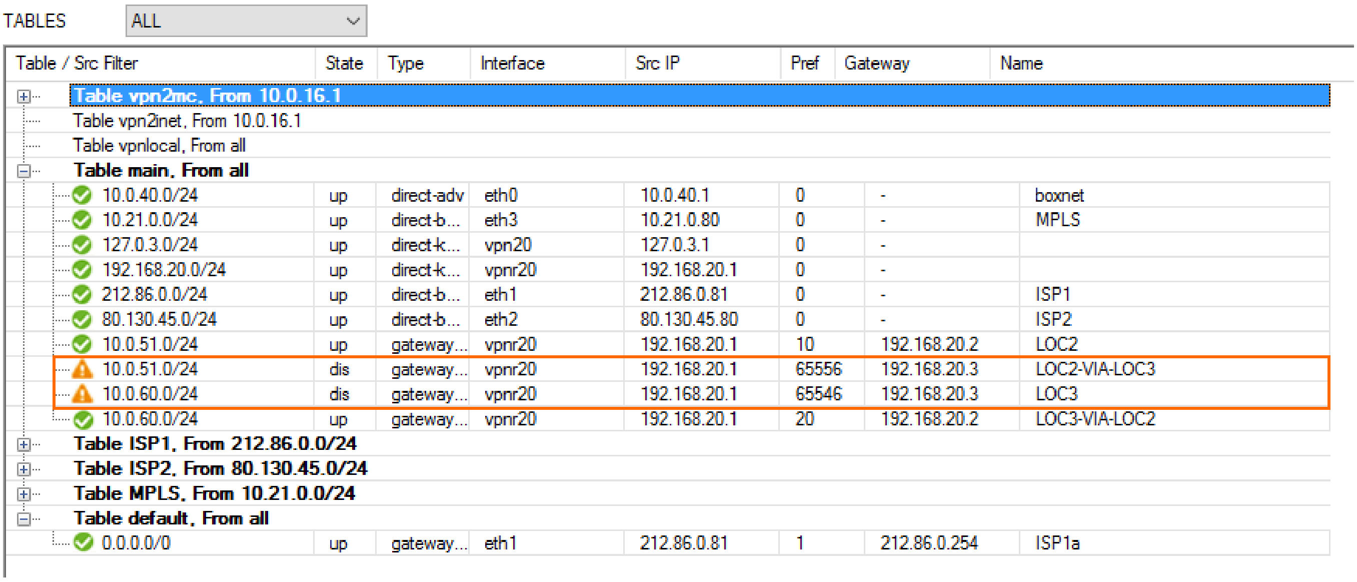


TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
⊞ **Table vpn2mc, From 10.0.16.3**							
Table vpn2inet, From 10.0.16.3							
Table vpnlocal, From all							
⊟ **Table main, From all**							
! 127.16.3.0/24	off	direct	eth1	-	0	-	DMZ
✓ 10.0.40.0/24	up	gateway...	vpnr20	192.168.20.3	10	192.168.20.1	LOC1
✓ 10.0.40.0/24	up	gateway...	vpnr20	192.168.20.3	20	192.168.20.2	LOC1-VIA-LOC2
✓ 10.0.51.0/24	up	gateway...	vpnr20	192.168.20.3	10	192.168.20.2	LOC2
✓ 10.0.51.0/24	up	gateway...	vpnr20	192.168.20.3	20	192.168.20.1	LOC2-VIA-LOC1
✓ 10.0.60.0/24	up	direct-b...	eth0	10.0.60.1	0	-	boxnet
✓ 127.0.3.0/24	up	direct-k...	vpn20	127.0.3.1	0	-	
✓ 192.168.20.0/24	up	direct-k...	vpnr20	192.168.20.3	0	-	
✓ 214.51.2.0/24	up	direct-b...	eth2	214.51.2.35	0	-	IPAD01
⊟ **Table default, From all**							
✓ 0.0.0.0/0	up	gateway...	eth2	214.51.2.35	0	214.51.2.254	ROUT01

Monitoring

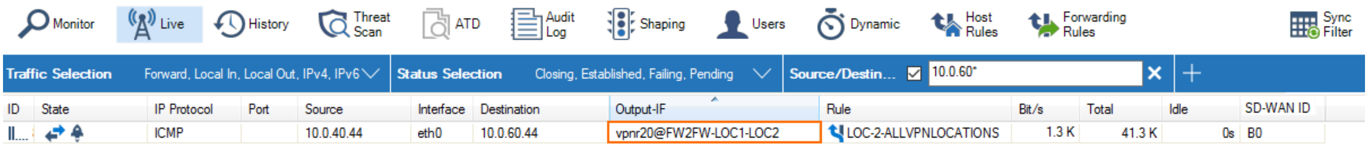
The VPN tunnels are now monitored like all other gateway routes. When a tunnel goes down, the VPNR interface IP address of the remote firewall is no longer reachable, and the gateway route metric is automatically increased to 65556. Traffic will then use the backup route with the lower metric to reach the destination through the other VPN tunnel. Go to **CONTROL > Network** to see the routing table.



TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
⊞ **Table vpn2mc, From 10.0.16.1**							
Table vpn2inet, From 10.0.16.1							
Table vpnlocal, From all							
⊟ **Table main, From all**							
✓ 10.0.40.0/24	up	direct-adv	eth0	10.0.40.1	0	-	boxnet
✓ 10.21.0.0/24	up	direct-b...	eth3	10.21.0.80	0	-	MPLS
✓ 127.0.3.0/24	up	direct-k...	vpn20	127.0.3.1	0	-	
✓ 192.168.20.0/24	up	direct-k...	vpnr20	192.168.20.1	0	-	
✓ 212.86.0.0/24	up	direct-b...	eth1	212.86.0.81	0	-	ISP1
✓ 80.130.45.0/24	up	direct-b...	eth2	80.130.45.80	0	-	ISP2
✓ 10.0.51.0/24	up	gateway...	vpnr20	192.168.20.1	10	192.168.20.2	LOC2
⚠ 10.0.51.0/24	dis	gateway...	vpnr20	192.168.20.1	65556	192.168.20.3	LOC2-VIA-LOC3
⚠ 10.0.60.0/24	dis	gateway...	vpnr20	192.168.20.1	65546	192.168.20.3	LOC3
✓ 10.0.60.0/24	up	gateway...	vpnr20	192.168.20.1	20	192.168.20.2	LOC3-VIA-LOC2
⊞ **Table ISP1, From 212.86.0.0/24**							
⊞ **Table ISP2, From 80.130.45.0/24**							
⊞ **Table MPLS, From 10.21.0.0/24**							
⊟ **Table default, From all**							
✓ 0.0.0.0/0	up	gateway...	eth1	212.86.0.81	1	212.86.0.254	ISP1a

Go to **FIREWALL > Live** to see which VPN tunnel is used.



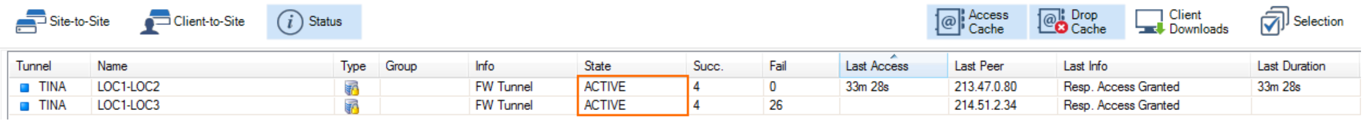
Traffic Selection Forward, Local In, Local Out, IPv4, IPv6

Status Selection Closing, Established, Failing, Pending

Source/Destin... ☑ 10.0.60*

ID	State	IP Protocol	Port	Source	Interface	Destination	Output-IF	Rule	Bit/s	Total	Idle	SD-WAN ID
II....		ICMP		10.0.40.44	eth0	10.0.60.44	vpnr20@FW2FW-LOC1-LOC2	LOC-2-ALLVPNLOCATIONS	1.3 K	41.3 K	0s	B0

Go to **VPN > Status** to see if the VPN tunnels are up.



Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info	Last Duration
TINA	LOC1-LOC2			FW Tunnel	ACTIVE	4	0	33m 28s	213.47.0.80	Resp. Access Granted	33m 28s
TINA	LOC1-LOC3			FW Tunnel	ACTIVE	4	26		214.51.2.34	Resp. Access Granted	

Figures