

Monitoring and Verification:

To monitor the devices, navigate to **Device Manager>Device & Groups Managed FortiGate**. First one by one right click on each device click **Edit**.

The screenshot shows the FortiGate Device Manager interface. The 'Device Manager' tab is selected. Under 'Device & Groups', 'Managed FortiGate (3)' is highlighted. A table lists three devices: BR-FW, DC-FW, and HQ-FW. A right-click context menu is open over the DC-FW device, with the 'Edit' option at the bottom highlighted by a red arrow.

Device Name	Config Status	Host Name	IP Address	Platform
BR-FW	Synchronized	BR-FW	192.168.5.1	FortiGate-VM64-KVM
DC-FW			192.168.3.1	FortiGate-VM64-KVM
HQ-FW			10.0.1.254	FortiGate-VM64-KVM

Type the Location in the Map and Click **OK**.

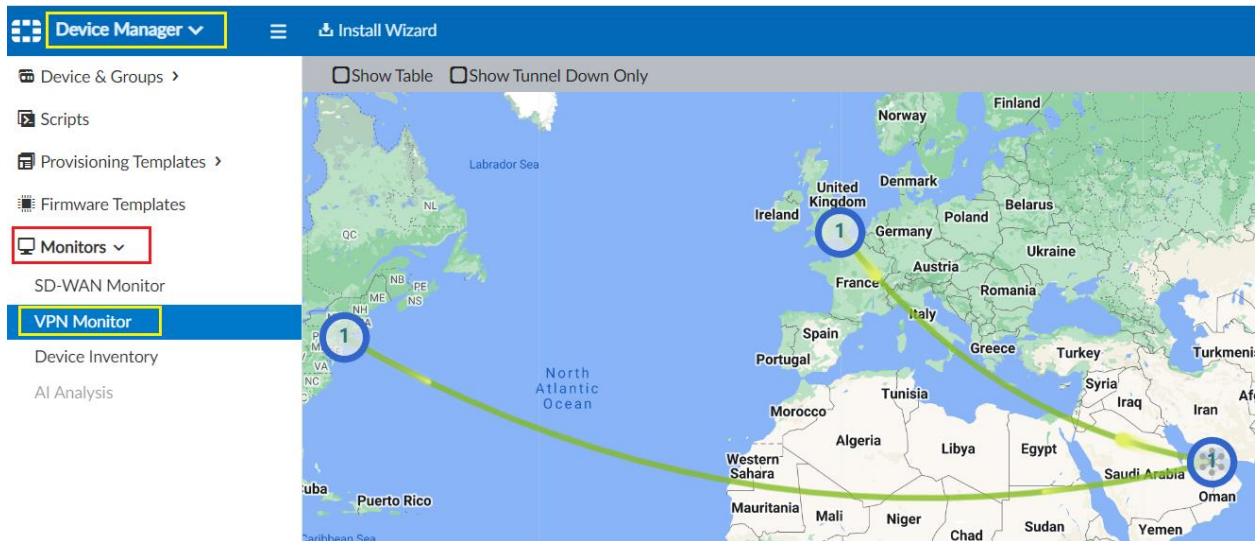
The screenshot shows the 'Edit Device' form for DC-FW. The form contains fields for Name, Description, IP Address, Serial Number, Firmware Version, Admin User, Password, Connected Interface, HA Mode, and Meta Fields. A map of New York City is shown on the right, with a red pin and a text box containing 'New York, NY, USA'. The 'OK' button is highlighted with a red arrow.

Geographic Coordinate: 40.7127753 (Latitude) -74.0059728 (Longitude)

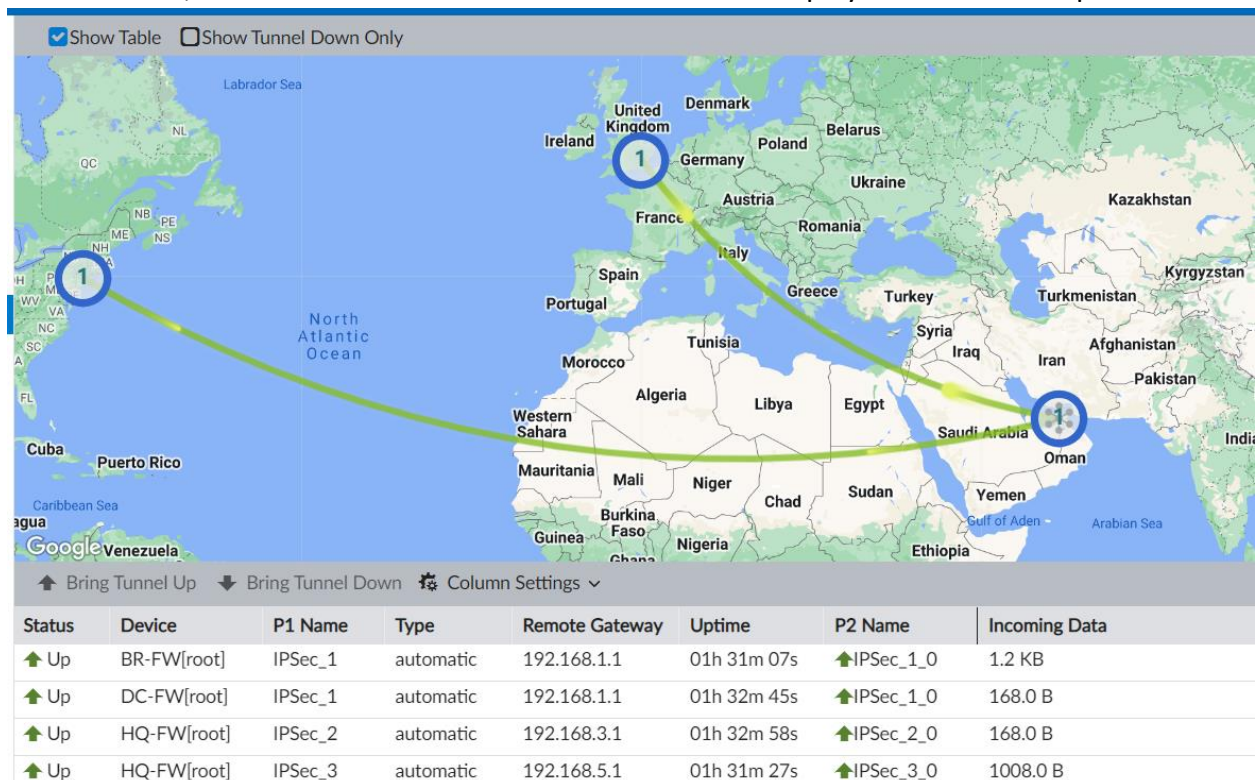
Repeat the same tasks for other two firewalls HQ-FW and BR-FW.

VPN Monitor:

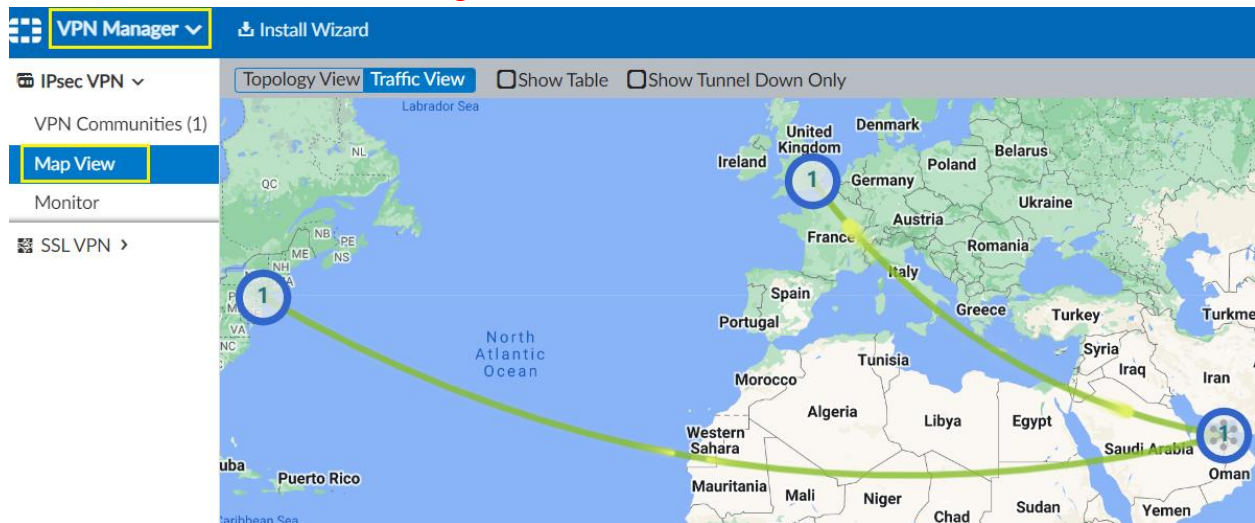
Go to **Device Manager > Monitors > VPN Monitor**. The map view of traffic for all communities is displayed.



In the toolbar, select **Show Table**. A table of information is displayed under the map.



Also, can monitor from **VPN Manager >IPsec VPN >VPN Communities >MAP View**



Let's login read-only to all three firewall one by one to verify the configuration has been pushed. In this case HQ-FW navigate to **Policy & Objects >Firewall Policy**

The screenshot shows the 'Policy & Objects' section with 'Firewall Policy' selected. The table below lists the configured policies.

ID	Name	From	To	Source	Hit Count	Destination
1	Allow-FMG	LAN (port3)	WAN-1 (port1)	all	234	all
2	LAN to DC VPN	LAN (port3)	IPSec_2	all	0	all
4	LAN to BR VPN	LAN (port3)	IPSec_3	all	0	all
3	DC VPN to LAN	IPSec_2	LAN (port3)	all	1	all
5	BR VPN to LAN	IPSec_3	LAN (port3)	all	2	all
0	Implicit Deny	any	any	all	0	all

Navigate to **VPN >IPsec Tunnels** to verify the tunnel configuration has been applied.

The screenshot shows the 'VPN' section with 'IPsec Tunnels' selected. The table below lists the configured tunnels.

Tunnel	Interface Binding	Status	Ref.
IPSec_2	WAN-1 (port1)	Up	4
IPSec_3	WAN-1 (port1)	Up	4

Navigate to **Network > Static Routes** the routes have been created and have been pushed from FortiManager.

HQ-FW	≡	Q
Dashboard	View	Search
Network	Destination	Gateway IP
Interfaces	Interface	Status
DNS	Distance	Priority
Packet Capture	0.0.0.0/0	192.168.1.254
SD-WAN	10.0.2.0/24	192.168.3.1
Static Routes	10.0.3.0/24	192.168.5.1

Also, can verify VPN Logs to navigate to **Log & Report > Events > VPN**

HQ-FW	≡	Q
Network	Refresh	Download
Policy & Objects	Add Filter	
Security Profiles	Date/Time	Level
VPN	Action	Status
User & Authentication	Message	VPN Tunnel
System	5 seconds ago	delete_ipsec_sa
Security Fabric	38 seconds ago	negotiate
Log & Report	38 seconds ago	negotiate
Forward Traffic	38 seconds ago	negotiate
Local Traffic	38 seconds ago	negotiate
Sniffer Traffic	38 seconds ago	install_sa
Events	5 minutes ago	tunnel-stats
	5 minutes ago	tunnel-stats
	19 minutes ago	tunnel-stats
	19 minutes ago	tunnel-stats