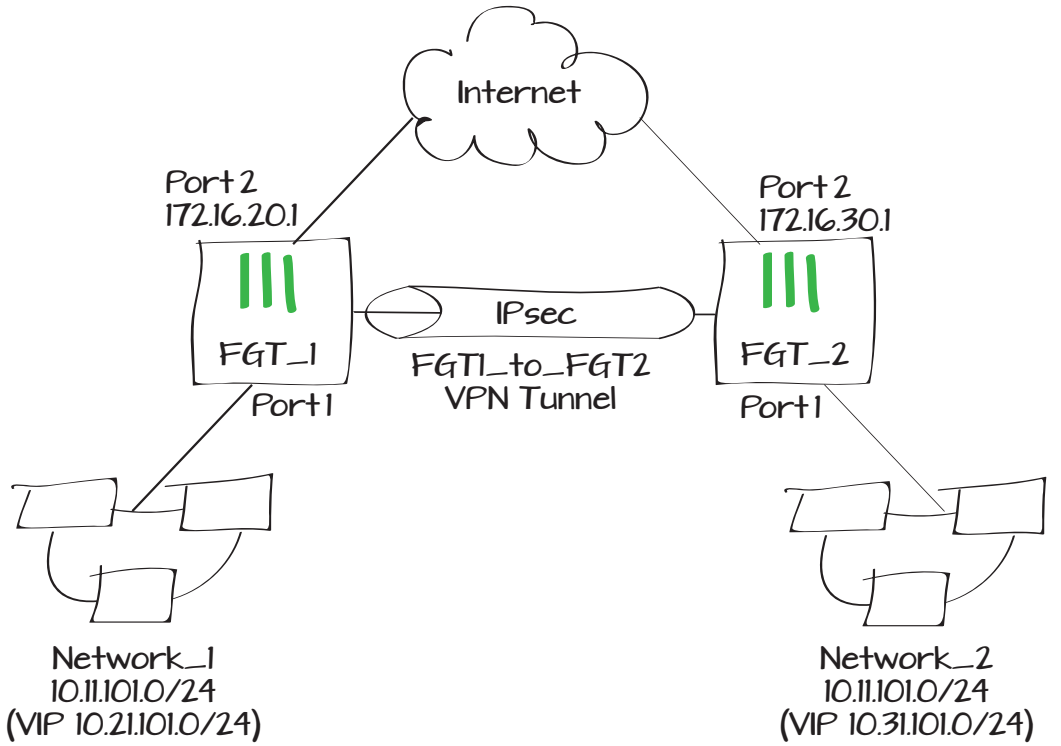
Creating a VPN with overlapping subnets

This recipe describes how to construct a VPN connection between two networks with overlapping IP addresses in such a way that traffic will be directed to the correct address on the correct network, using Virtual IP addresses and static routes.

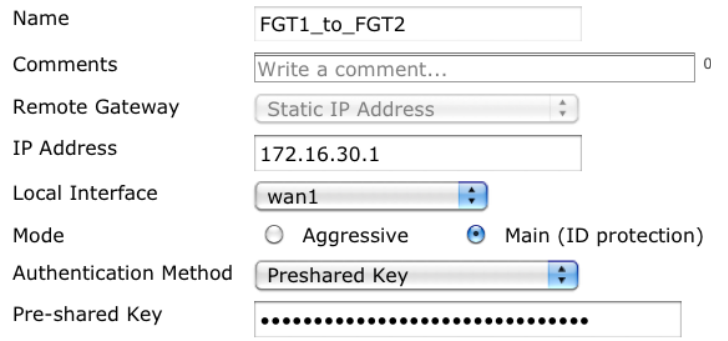
1. Creating VPN tunnels between the two FortiGate units
2. Adding the virtual IP range and address
3. Creating inbound and outbound security policies
4. Configuring static routes
5. Repeat the steps on FGT2
6. Results



Creating VPN tunnels between the two FortiGates

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**, and set the **IP Address** to the address used by the internet-facing interface of FGT_2. Set the **Local Interface** to your internet-facing interface, and enter a **Pre-shared Key**.



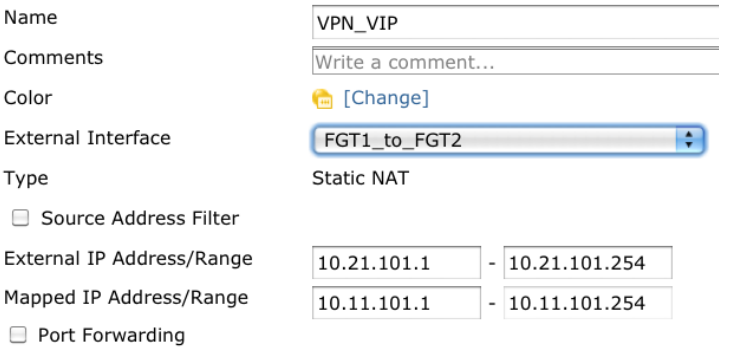
Then create the Phase 2, selecting your Phase 1 from the list.

Adding the virtual IP range and address

Go to **Firewall Objects > Virtual IPs > Virtual IPs**.

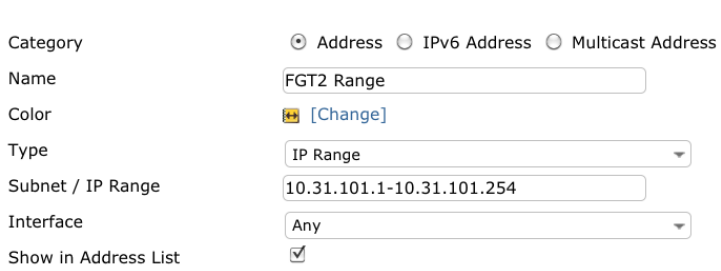
You will need to create a Virtual IP range that will used to redirect the traffic to the correct subnet. Give the VIP an appropriate name, and set the IPsec tunnel interface as the **External Interface**.

Set the **External IP Address** to a range in the subnet you'll be redirecting from (10.21.101.1-10.21.101.254) and the **Mapped IP address** to the internal network range (10.11.101.1-10.11.101.254).



Now go to **Firewall Objects** > **Address** > **Addresses**.

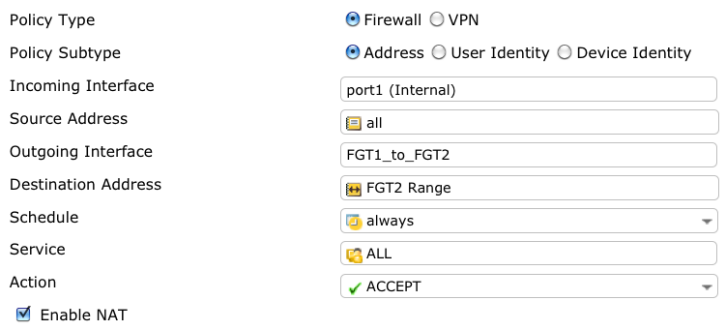
Create a new address, setting the **Type** to **IP Range**, and entering the VIP range of FGT2 (10.31.101.1-10.31.101.254).



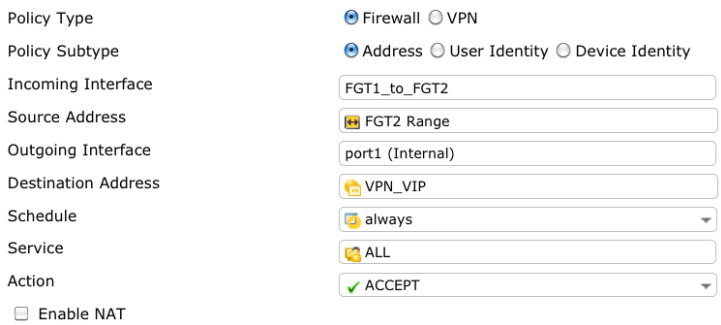
Creating inbound and outbound security policies

Go to **Policy > Policy > Policy**.

Create a firewall policy to handle outbound VPN traffic, with the network-facing interface as the **Incoming Interface**, and the IPsec interface as **Outgoing**. Set the **Destination Address** to the VIP Address Range. Enable NAT.



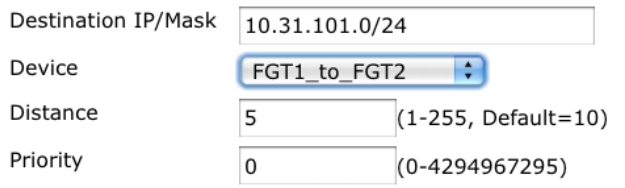
Create a second security policy to handle inbound VPN traffic, with the IPsec interface as the **Incoming Interface**, network-facing interface as **Outgoing**, and your VIP range as the **Destination Address**. Disable NAT.



Configuring static routes

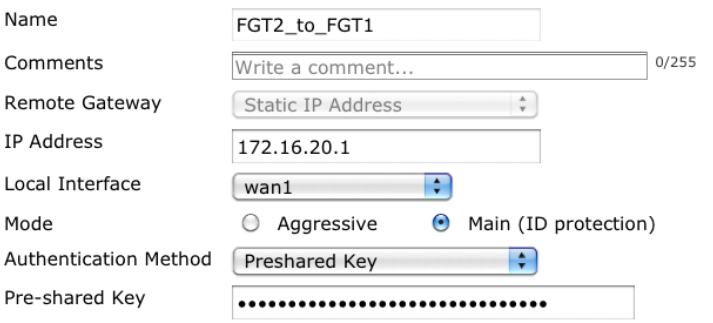
Go to **Router > Static > Static Routes**.

Create a new Static Route, with the **Destination IP** as 10.31.101.0/24. For your **Device**, select your FGT1_to_FGT2 VPN interface. Set the Distance to lower than the default of 10, to prioritize this route.

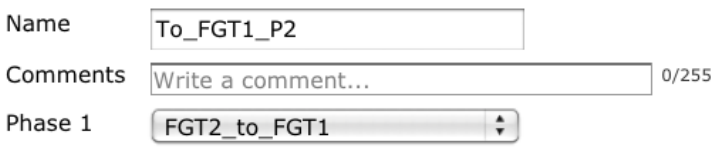


Repeat these steps on FGT2

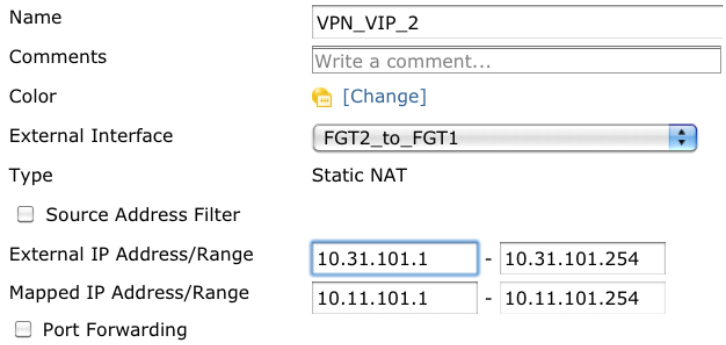
First, create the Phase 1 on FGT_2, using FGT_1's internet-facing interface IP for the Phase 1 IP Address, and the FGT_2's internet-facing interface as **Local Interface**.



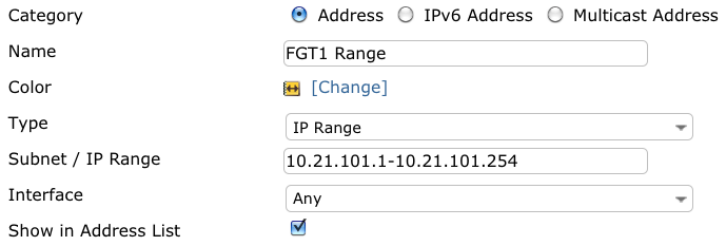
Create the Phase 2 for FGT_2.



Create the VIP Range, setting the IPsec tunnel interface as the **External Interface**, the **External IP Address** to the intended local VIP range (10.31.101.1-10.31.101.254) and the **Mapped IP Address** to the internal network range (10.11.101.1-10.11.101.254).

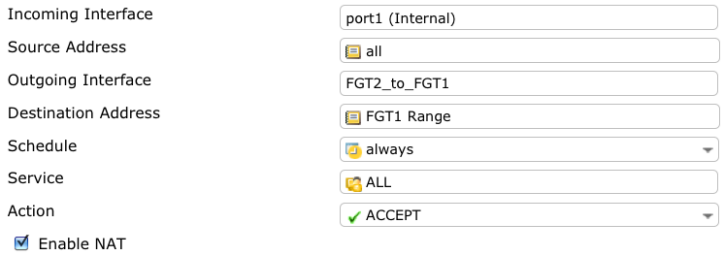


Create the address range, setting the **Type** to **IP Range**, and entering the VIP range of FGT1 (10.21.101.1-10.21.101.254).

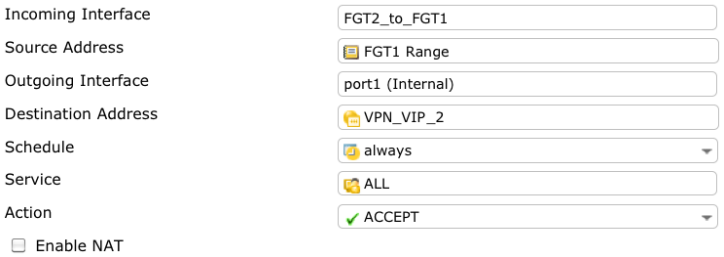


Create the two firewall policies to handle outbound and inbound VPN traffic.

For the outbound policy, select your internal-network-facing port as the **Incoming Interface**, and the IPsec interface as **Outgoing**. Set the **Destination Address** to the VIP Address Range. Enable NAT.

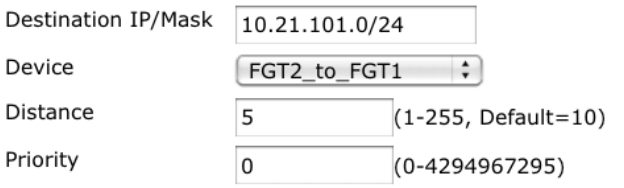


For the inbound, set the IPsec interface as the **Incoming Interface**, internal port as **Outgoing**, and your VIP range as the **Destination Address**. Disable NAT.



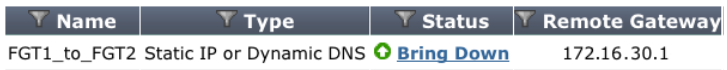
Then create the Static Route, with the **Destination IP** as 10.21.101.0/24. For your **Device**, select your VPN interface.

Set the Distance lower than 10.



Results

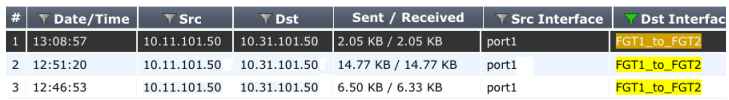
On a FortiGate unit, you can go to **VPN > Monitor > IPsec Monitor** to see the status of the VPN tunnel.



Connect to the VPN, using a network device in Network_1. Access the address 10.31.101.50, and your session will be redirected to Network_2's 10.11.101.50.

Then, from a VPN-connected device in Network_2, visit 10.21.101.50, and you will access Network_1's 10.11.101.50.

Go to **Log & Report > Traffic Log > Forward Traffic** and filter the **Src Interface** column with the VPN Interface name to see incoming VPN traffic and the **Dst Interface** column to see outgoing.



#	Date/Time	Src	Dst	Sent / Received	Src Interface	Dst Interfac
1	13:08:57	10.11.101.50	10.31.101.50	2.05 KB / 2.05 KB	port1	FGT1_to_FGT2
2	12:51:20	10.11.101.50	10.31.101.50	14.77 KB / 14.77 KB	port1	FGT1_to_FGT2
3	12:46:53	10.11.101.50	10.31.101.50	6.50 KB / 6.33 KB	port1	FGT1_to_FGT2