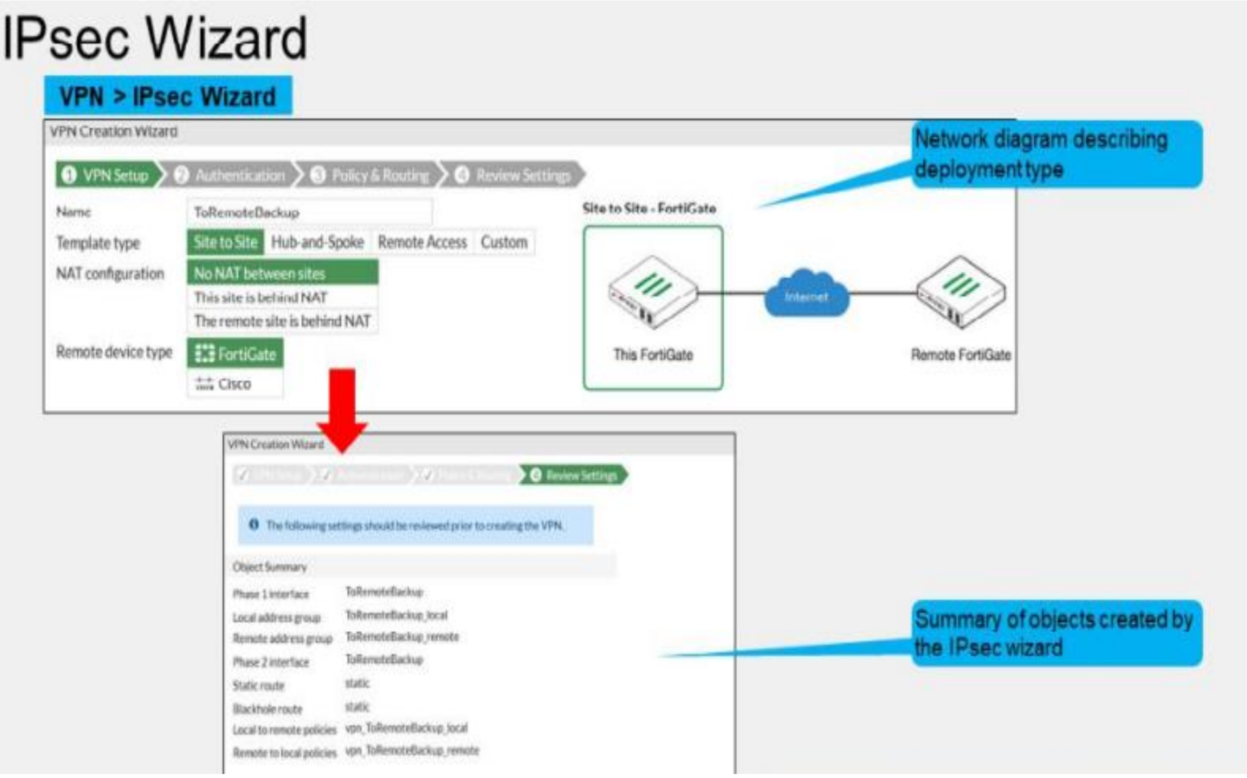
IPsec VPN Configuration

In this lab, I will configure site-to-site IPsec VPN tunnels between two FortiGate devices. First, i will configure a dial-up tunnel, and then a static tunnel. Then, i will add a second VPN tunnel that will act as a backup tunnel between the FortiGate devices.

Objectives

1. Deploy a site-to-site VPN between two FortiGate devices
2. Set up dial-up and static remote gateways
3. Configure redundant VPNs between two FortiGate devices



IPsec Wizard

VPN > IPsec Wizard

VPN Creation Wizard

Name: ToRemoteBackup

Template type: Site to Site | Hub-and-Spoke | Remote Access | Custom

NAT configuration: No NAT between sites | This site is behind NAT | The remote site is behind NAT

Remote device type: FortiGate | Cisco

Network diagram describing deployment type

VPN Creation Wizard

The following settings should be reviewed prior to creating the VPN.

Object Summary

Phase 1 interface	ToRemoteBackup
Local address group	ToRemoteBackup_local
Remote address group	ToRemoteBackup_remote
Phase 2 interface	ToRemoteBackup
Static route	static
Blackhole route	static
Local to remote policies	vpn_ToRemoteBackup_local
Remote to local policies	vpn_ToRemoteBackup_remote

Summary of objects created by the IPsec wizard

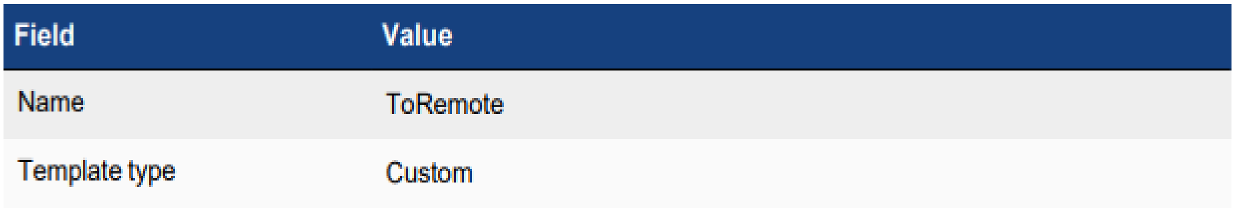
Part 1: Configuring a Dial-Up IPsec VPN Between Two FortiGate Devices

In this lab, i will configure a dial-up VPN between Local-FortiGate and Remote-FortiGate.

Local-FortiGate will act as the dial-up server and Remote-FortiGate will act as the dial-up client.

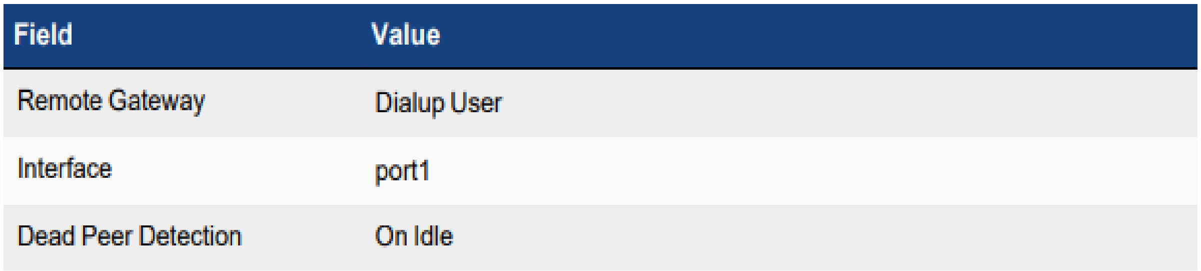
Steps of part 1 :

1. **Create Phase 1 and Phase 2 on Local-FortiGate (Dial-Up Server)**
   Here is the configured steps :



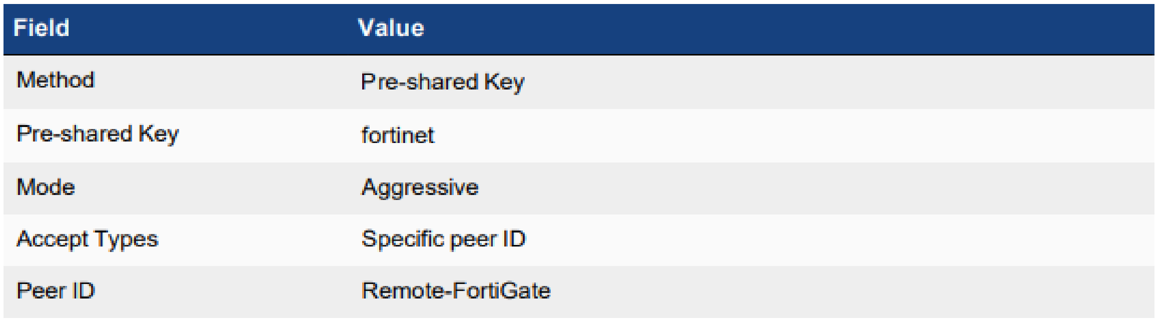
Field	Value
Name	ToRemote
Template type	Custom

Network section:



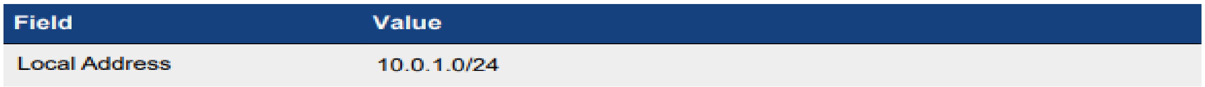
Field	Value
Remote Gateway	Dialup User
Interface	port1
Dead Peer Detection	On Idle

Authentication section:

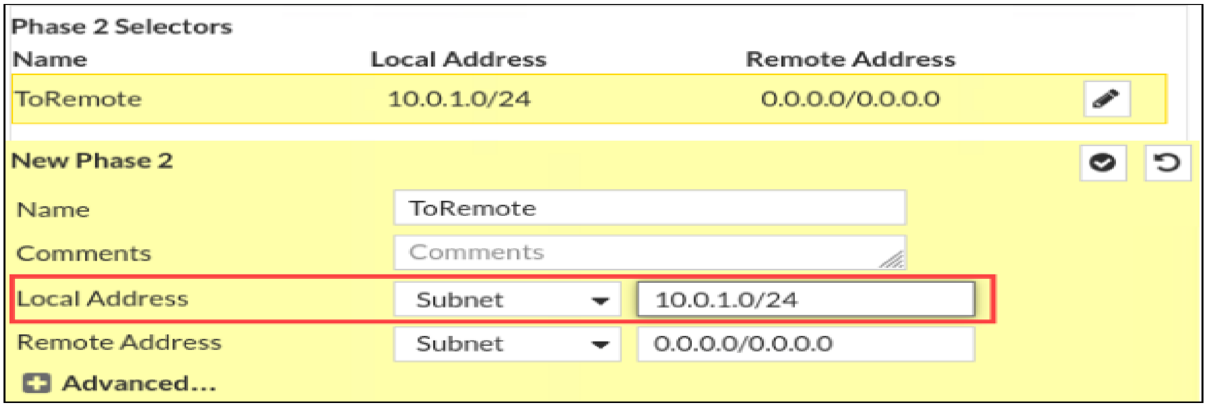


Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet
Mode	Aggressive
Accept Types	Specific peer ID
Peer ID	Remote-FortiGate

Phase 2 Selectors section



Field	Value
Local Address	10.0.1.0/24



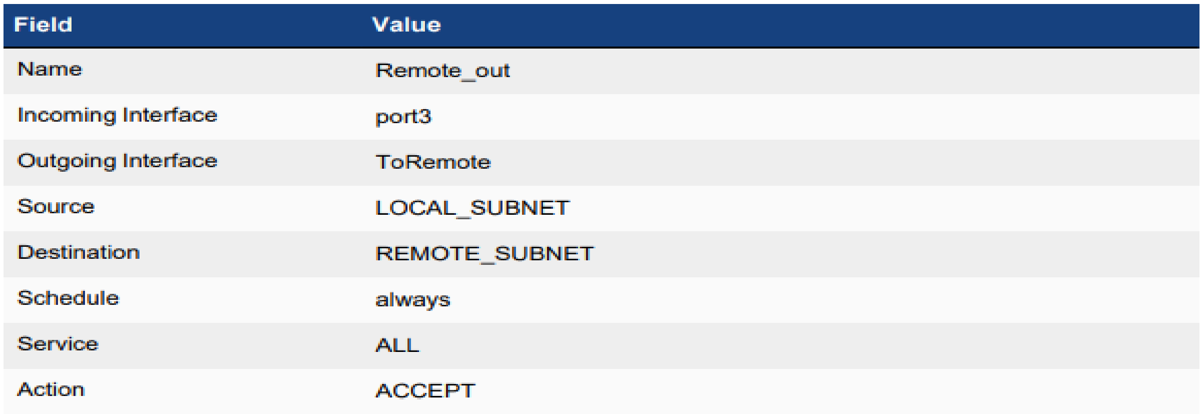
Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	10.0.1.0/24	0.0.0.0/0.0.0.0

New Phase 2

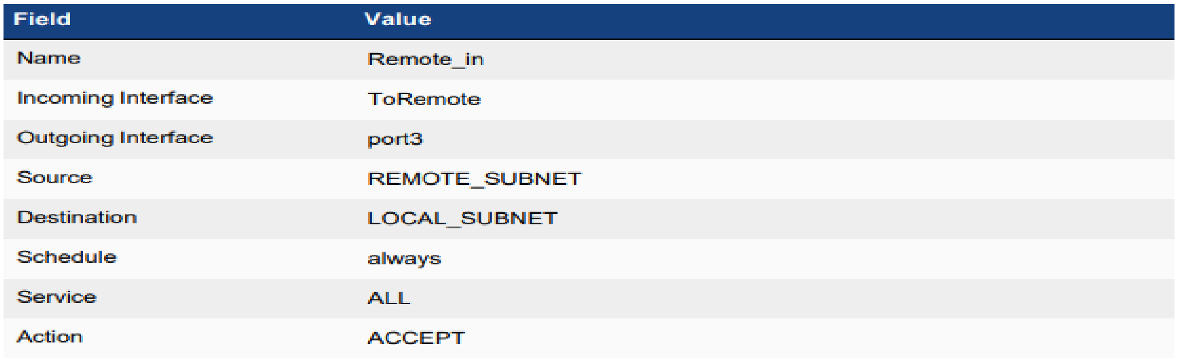
Name	ToRemote	
Comments	Comments	
Local Address	Subnet	10.0.1.0/24
Remote Address	Subnet	0.0.0.0/0.0.0.0

2. Create Firewall Policies for VPN Traffic on Local-FortiGate (Dial-Up Server)

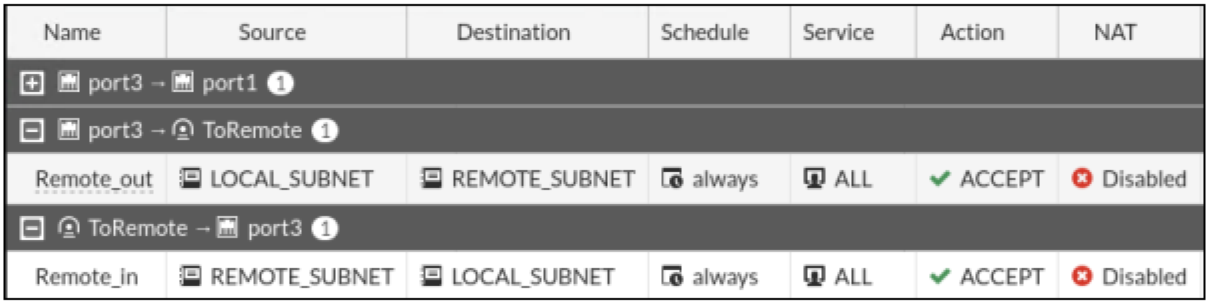


Field	Value
Name	Remote_out
Incoming Interface	port3
Outgoing Interface	ToRemote
Source	LOCAL_SUBNET
Destination	REMOTE_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

Create New again

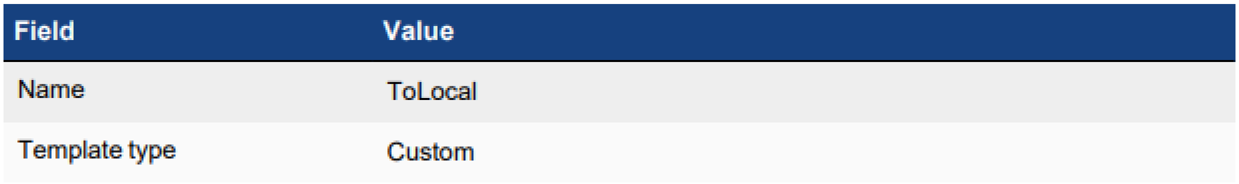


Field	Value
Name	Remote_in
Incoming Interface	ToRemote
Outgoing Interface	port3
Source	REMOTE_SUBNET
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT



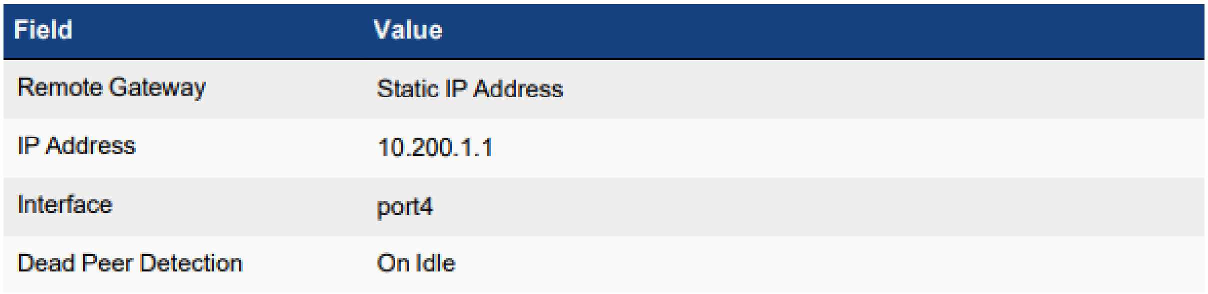
Name	Source	Destination	Schedule	Service	Action	NAT
⊞ port3 → port1 1						
⊟ port3 → ToRemote 1						
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled
⊟ ToRemote → port3 1						
Remote_in	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	✓ ACCEPT	Disabled

3. Create Phase 1 and Phase 2 on Remote-FortiGate (Dial-Up Client)



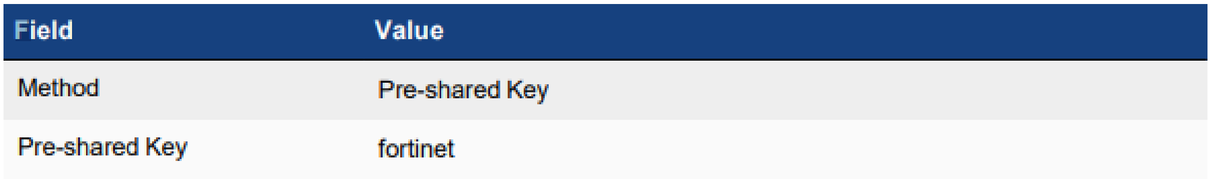
Field	Value
Name	ToLocal
Template type	Custom

Network section

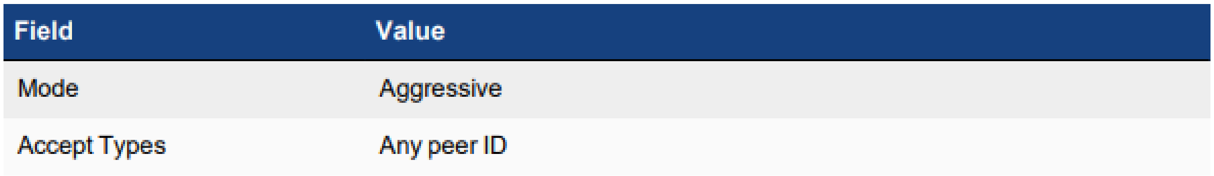


Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.1.1
Interface	port4
Dead Peer Detection	On Idle

Authentication section



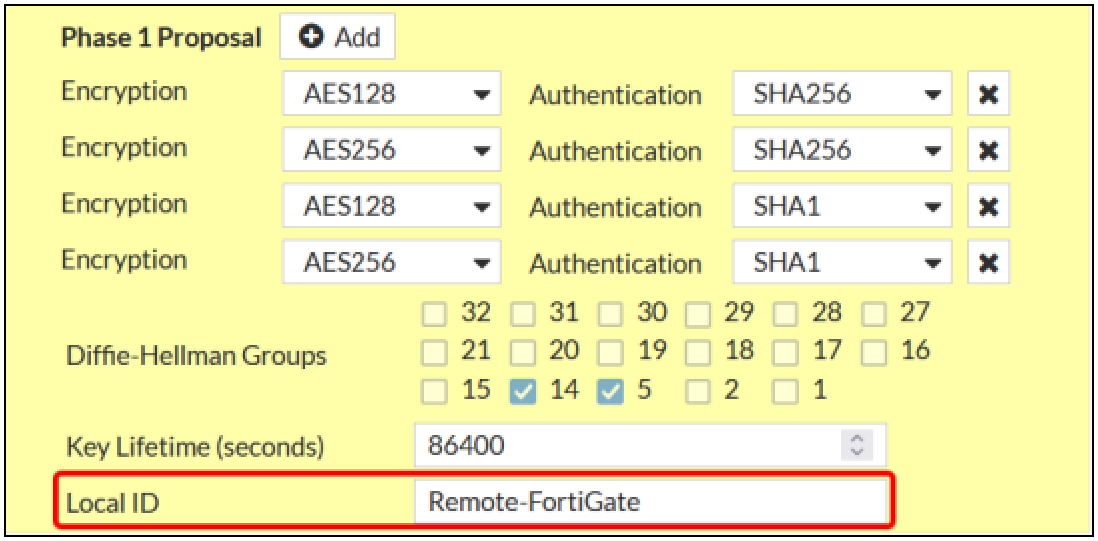
Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet



Field	Value
Mode	Aggressive
Accept Types	Any peer ID

Phase 1 Proposal section

Field	Value
Local ID	Remote-FortiGate



Phase 1 Proposal ⊕ Add

Encryption	AES128	Authentication	SHA256
Encryption	AES256	Authentication	SHA256
Encryption	AES128	Authentication	SHA1
Encryption	AES256	Authentication	SHA1

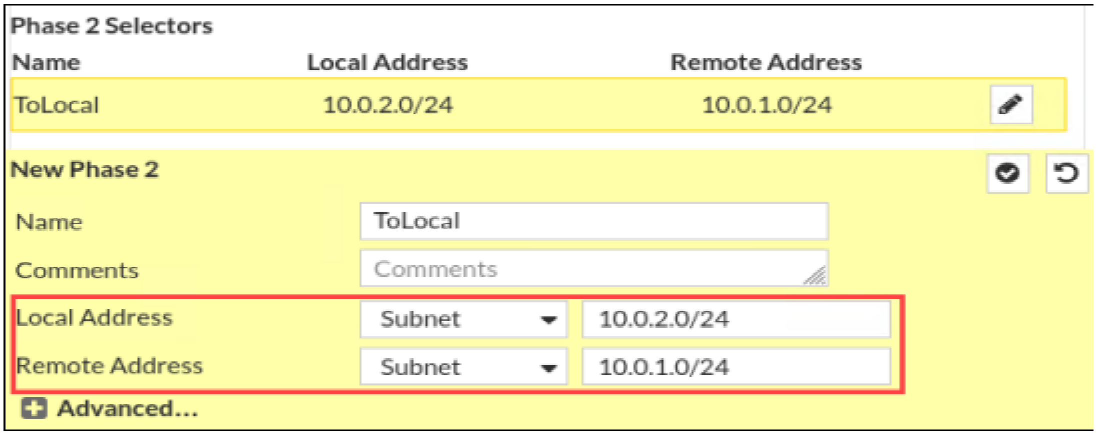
Diffie-Hellman Groups
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 ☑ 14 ☑ 5 □ 2 □ 1

Key Lifetime (seconds) 86400

Local ID Remote-FortiGate

Phase 2 Selectors section

Field	Value
Local Address	10.0.2.0/24
Remote Address	10.0.1.0/24



Phase 2 Selectors

Name	Local Address	Remote Address
ToLocal	10.0.2.0/24	10.0.1.0/24

New Phase 2

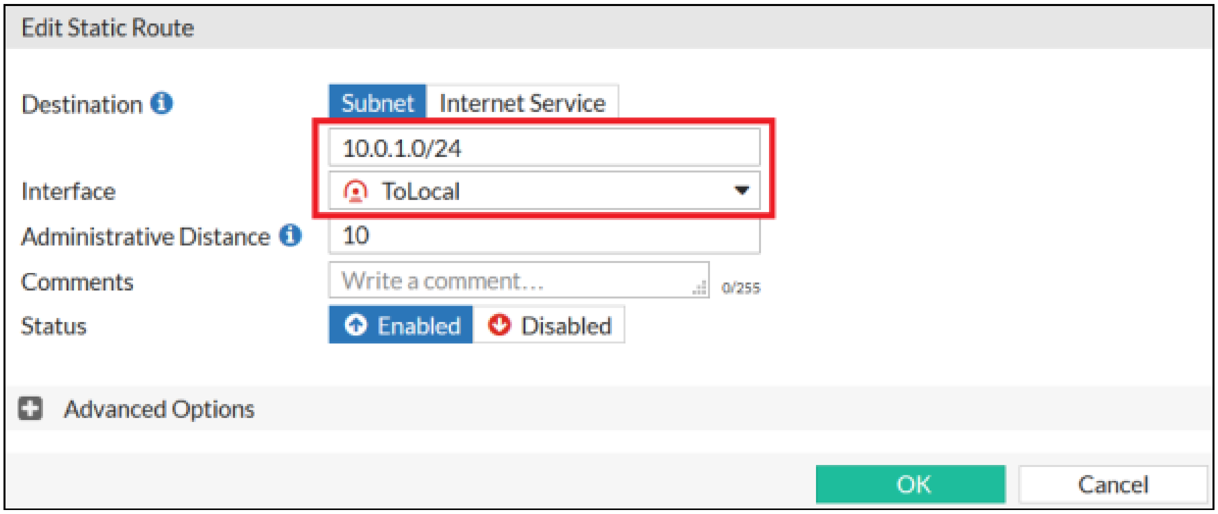
Name ToLocal

Comments Comments

Local Address Subnet 10.0.2.0/24

Remote Address Subnet 10.0.1.0/24

4. Create a Static Route for VPN Traffic on Remote-FortiGate (Dial-Up Client)



Edit Static Route

Destination: Subnet | Internet Service

10.0.1.0/24

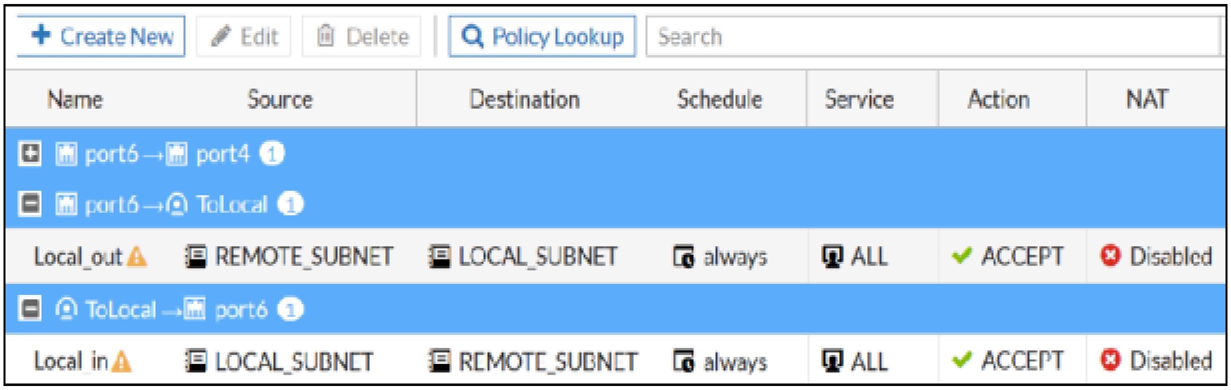
Interface: ToLocal

Administrative Distance: 10

Comments: Write a comment... 0/255

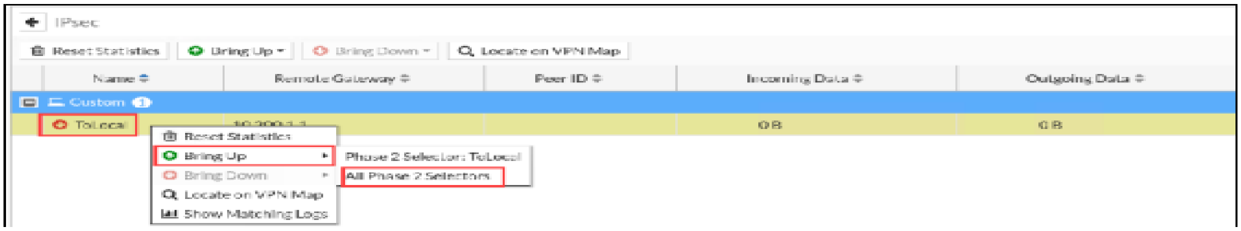
Status: Enabled | Disabled

5. Create the Firewall Policies for VPN Traffic on Remote-FortiGate (Dial-Up Client)



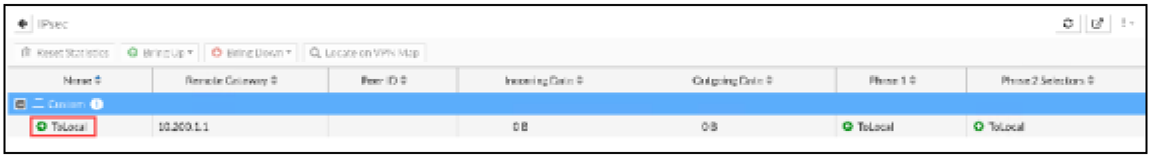
Name	Source	Destination	Schedule	Service	Action	NAT
port6 → port4 1						
port6 → ToLocal 1						
Local_out	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	✓ ACCEPT	Disabled
ToLocal → port6 1						
Local_in	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled

6. Test and Monitor the VPN



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
Custom 1				
ToLocal	10.200.1.1		0 B	0 B

The Name column of the VPN now contains a green up arrow, which indicates that the tunnel is up. If required, click the refresh button in the upper-right corner to refresh the widget .



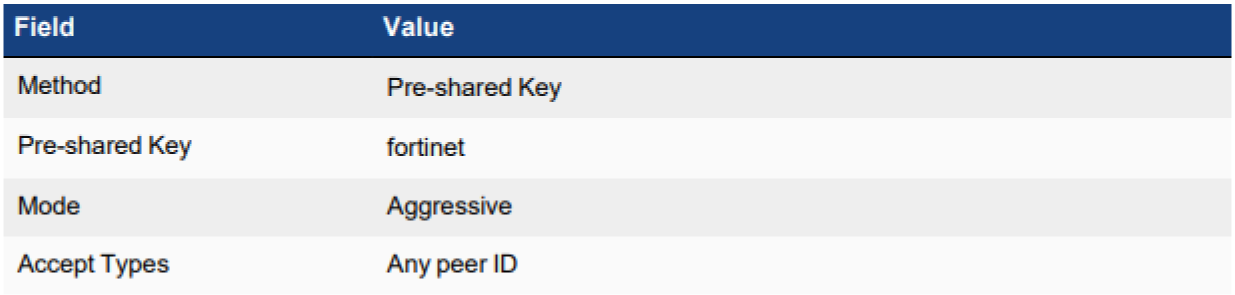
Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
ToLocal	10.200.1.1		0 B	0 B	ToLocal	ToLocal

Part 2: Configuring a Static IPsec VPN Between Two FortiGate Devices

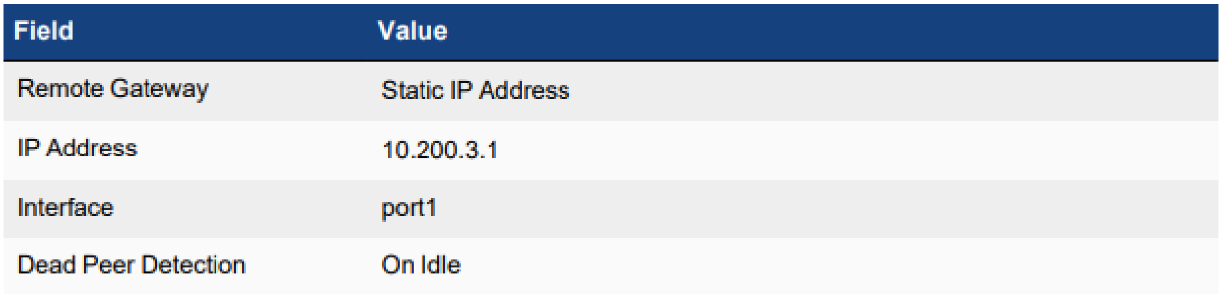
In this part, i will configure a static VPN between Local-FortiGate and Remote-FortiGate. I will also configure a static route on Local-FortiGate for VPN traffic

Steps of part 2 :

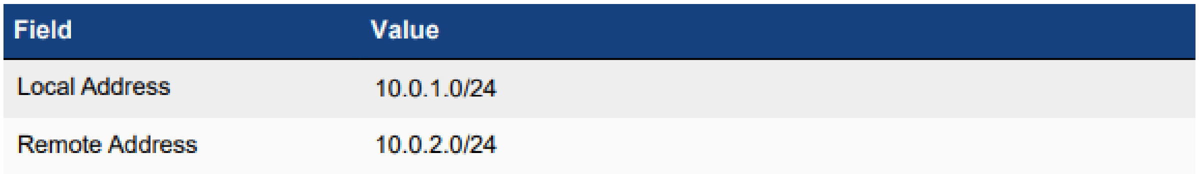
1. Create Phase 1 and Phase 2 on Local-FortiGate



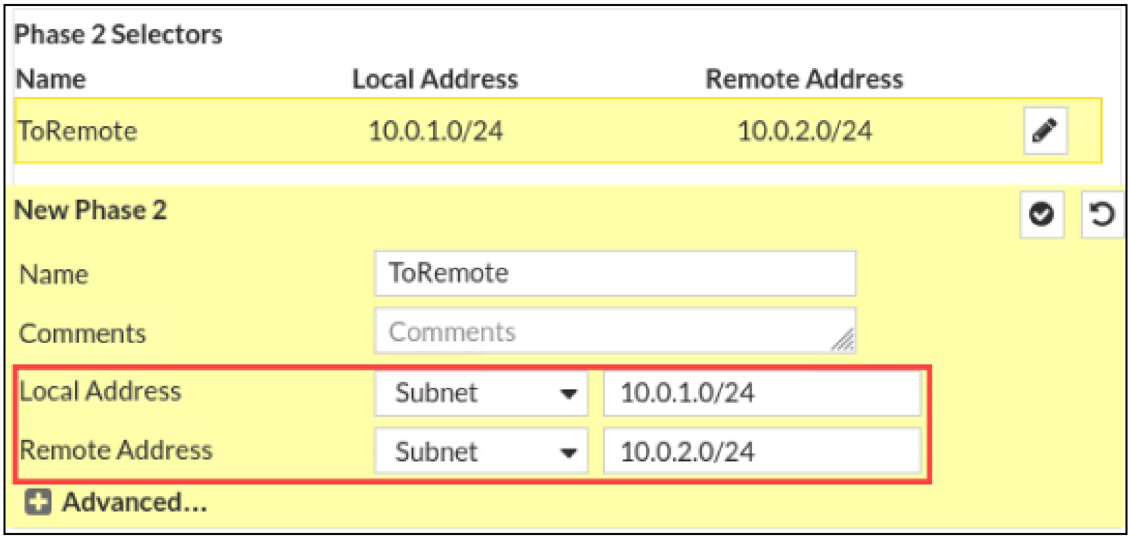
Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet
Mode	Aggressive
Accept Types	Any peer ID



Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.3.1
Interface	port1
Dead Peer Detection	On Idle



Field	Value
Local Address	10.0.1.0/24
Remote Address	10.0.2.0/24



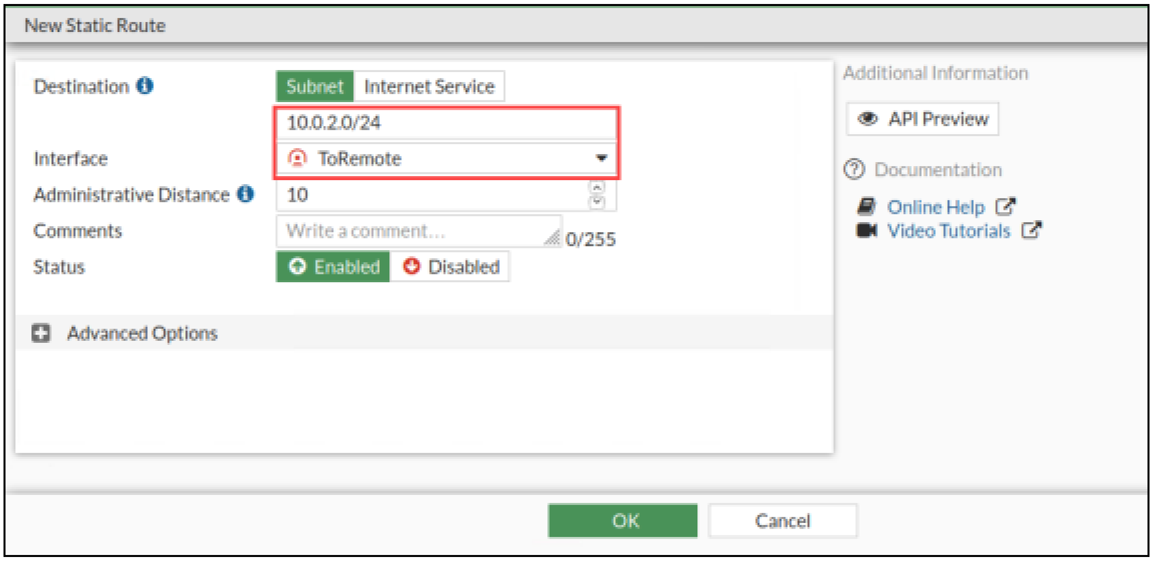
Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	10.0.1.0/24	10.0.2.0/24

New Phase 2

Name	ToRemote	
Comments	Comments	
Local Address	Subnet	10.0.1.0/24
Remote Address	Subnet	10.0.2.0/24

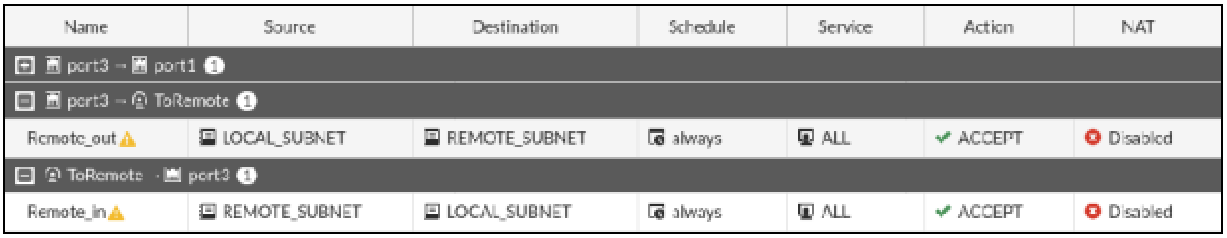
2. Create a Static Route for VPN Traffic on Local-FortiGate



New Static Route

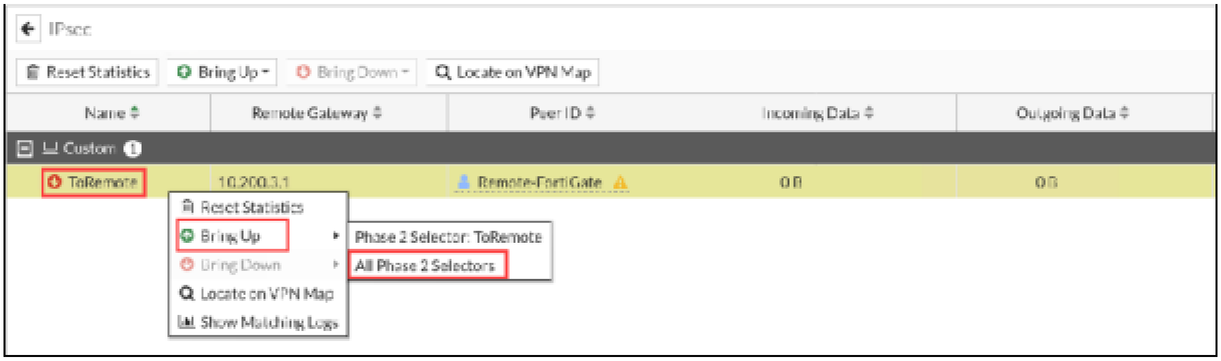
Destination	Subnet / Internet Service 10.0.2.0/24
Interface	ToRemote
Administrative Distance	10
Comments	Write a comment... 0/255
Status	Enabled / Disabled

3. Create Firewall Policies for VPN Traffic on Local-FortiGate

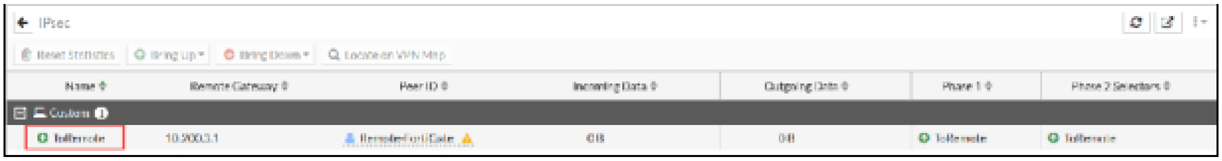


Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1						
port3 → ToRemote 1						
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled
ToRemote → port3 1						
Remote_in	REMOTE_SUBNET	LOCAL_SUBNET	always	ALL	✓ ACCEPT	Disabled

4. Test and Monitor the VPN



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
Custom 1				
ToRemote	10.200.3.1	Remote-FortiGate	0 B	0 B



Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
ToRemote	10.200.3.1	Remote-FortiGate	0 B	0 B	ToRemote	ToRemote

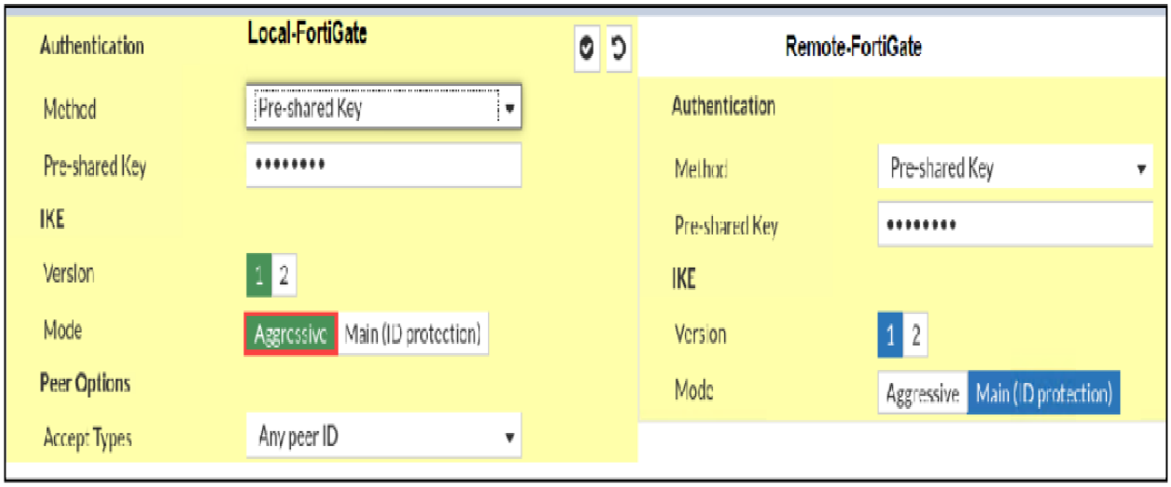
Part 3: Configuring Redundant Static IPsec VPN Tunnels Between Two FortiGate Devices

In this part, i will configure one more VPN tunnel between Local-FortiGate and Remote-FortiGate for redundancy purposes.

Steps of part 3 :

4. **Review the VPN Configuration on Both FortiGate Devices**

   Compare the **authentication** section of each fortigate



Local-FortiGate

Authentication

Method: Pre-shared Key

Pre-shared Key: ••••••••

IKE

Version: 1 2

Mode: Aggressive Main (ID protection)

Peer Options

Accept Types: Any peer ID

Remote-FortiGate

Authentication

Method: Pre-shared Key

Pre-shared Key: ••••••••

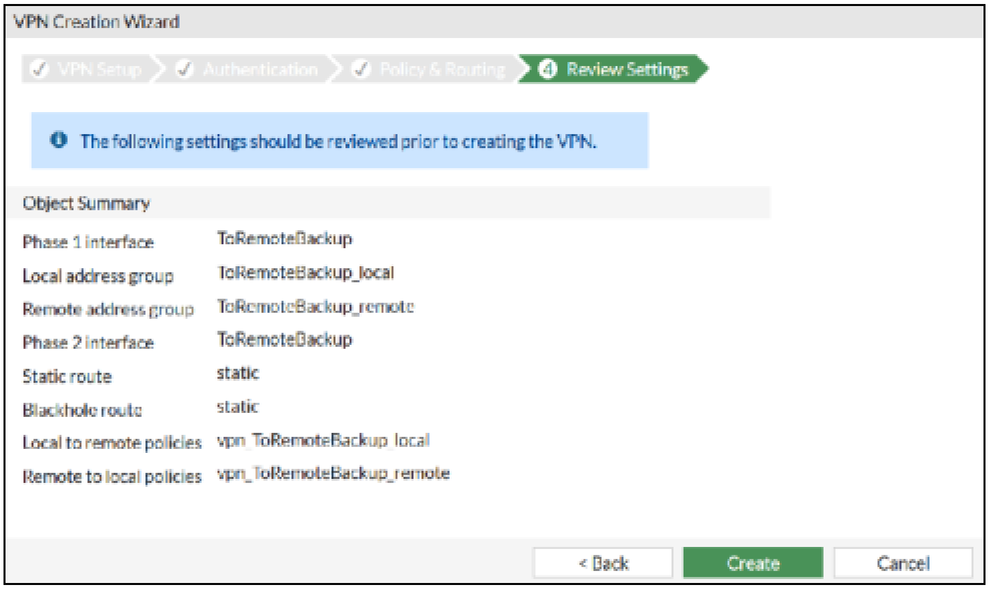
IKE

Version: 1 2

Mode: Aggressive Main (ID protection)

5. **Create a Backup VPN Tunnel Using the IPsec Wizard**

   i configured a backup VPN tunnel on Local-FortiGate, named ToRemoteBackup, here is the result :



VPN Creation Wizard

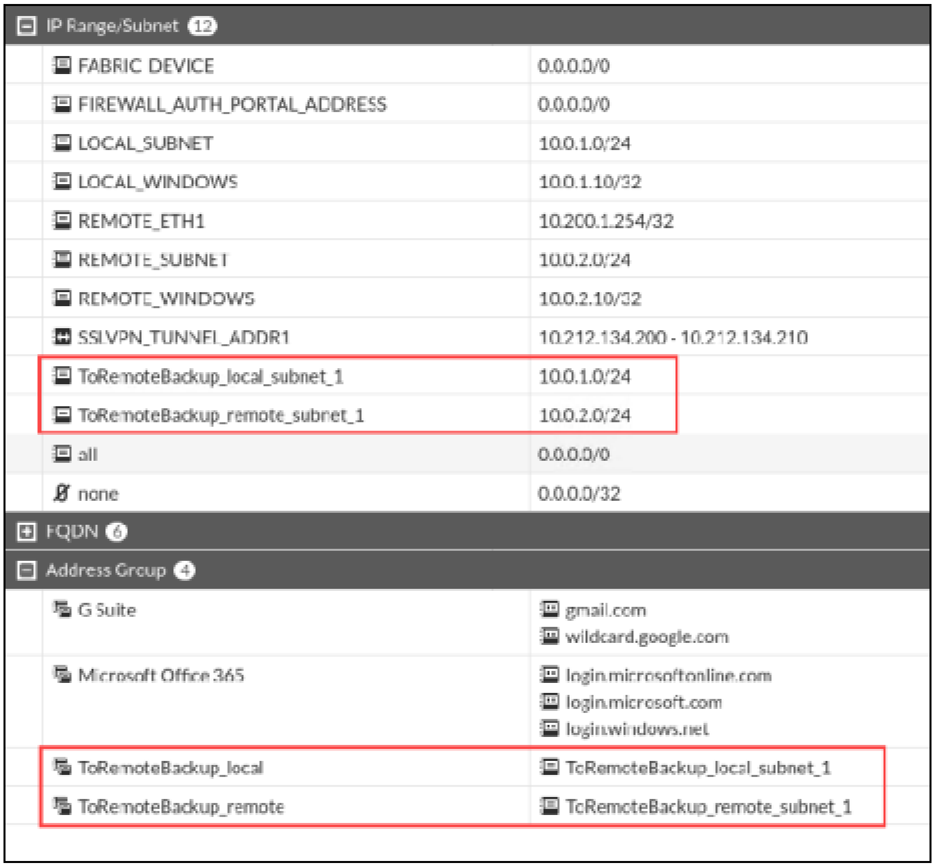
The following settings should be reviewed prior to creating the VPN.

Object Summary

Phase 1 interface	ToRemoteBackup
Local address group	ToRemoteBackup_local
Remote address group	ToRemoteBackup_remote
Phase 2 interface	ToRemoteBackup
Static route	static
Blackhole route	static
Local to remote policies	vpn_ToRemoteBackup_local
Remote to local policies	vpn_ToRemoteBackup_remote

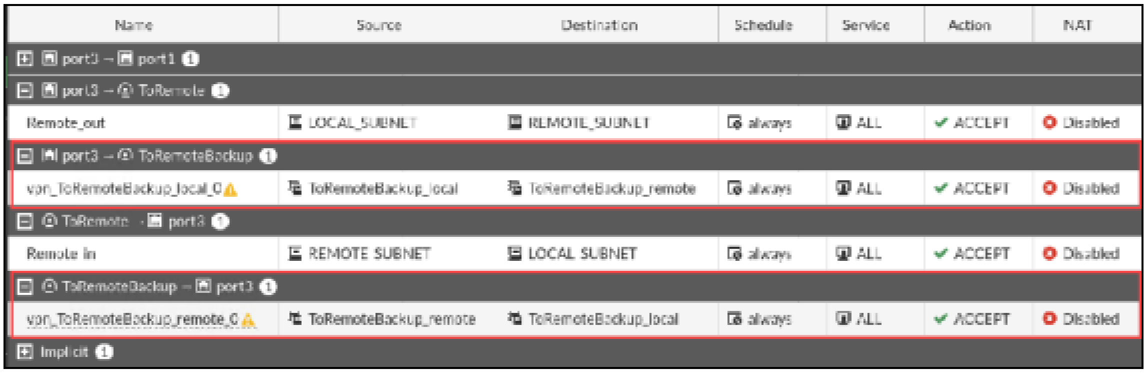
6. Review the Objects the IPsec Wizard Created

Ipsec wizard created all other objects ,firewallpolicy,static route ,addresses:



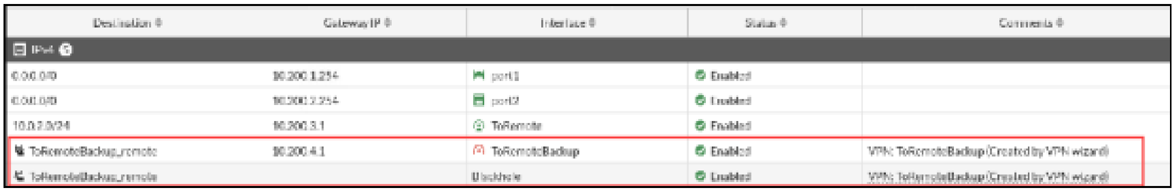
⊟ IP Range/Subnet 12	
FABRIC DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
LOCAL_SUBNET	10.0.1.0/24
LOCAL_WINDOWS	10.0.1.10/32
REMOTE_ETH1	10.200.1.254/32
REMOTE_SUBNET	10.0.2.0/24
REMOTE_WINDOWS	10.0.2.10/32
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
ToRemoteBackup_local_subnet_1	10.0.1.0/24
ToRemoteBackup_remote_subnet_1	10.0.2.0/24
all	0.0.0.0/0
none	0.0.0.0/32
⊞ FQDN 6	
⊟ Address Group 4	
G Suite	gmail.com wildcard.google.com
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net
ToRemoteBackup_local	ToRemoteBackup_local_subnet_1
ToRemoteBackup_remote	ToRemoteBackup_remote_subnet_1

Firewall policies:



Name	Source	Destination	Schedule	Service	Action	NAT
⊞ port3 → port1 1						
⊟ port3 → ToRemote 1						
Remote_out	LOCAL_SUBNET	REMOTE_SUBNET	always	ALL	✓ ACCEPT	Disabled
⊟ port3 → ToRemoteBackup 1						
vpn_ToRemoteBackup_local_0 ⚠	ToRemoteBackup_local	ToRemoteBackup_remote	always	ALL	✓ ACCEPT	Disabled
⊟ ToRemote → port3 1						
Remote in	REMOTE SUBNET	LOCAL SUBNET	always	ALL	✓ ACCEPT	Disabled
⊟ ToRemoteBackup → port3 1						
vpn_ToRemoteBackup_remote_0 ⚠	ToRemoteBackup_remote	ToRemoteBackup_local	always	ALL	✓ ACCEPT	Disabled
⊞ Implicit 1						

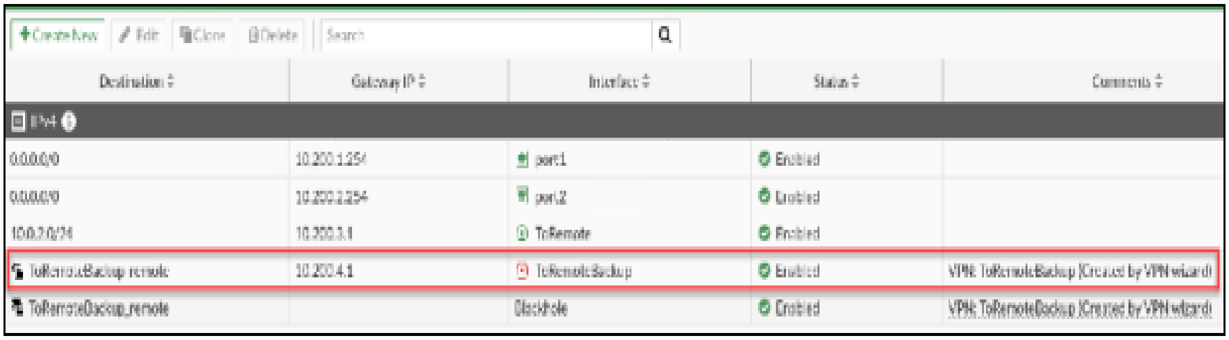
Static routes :



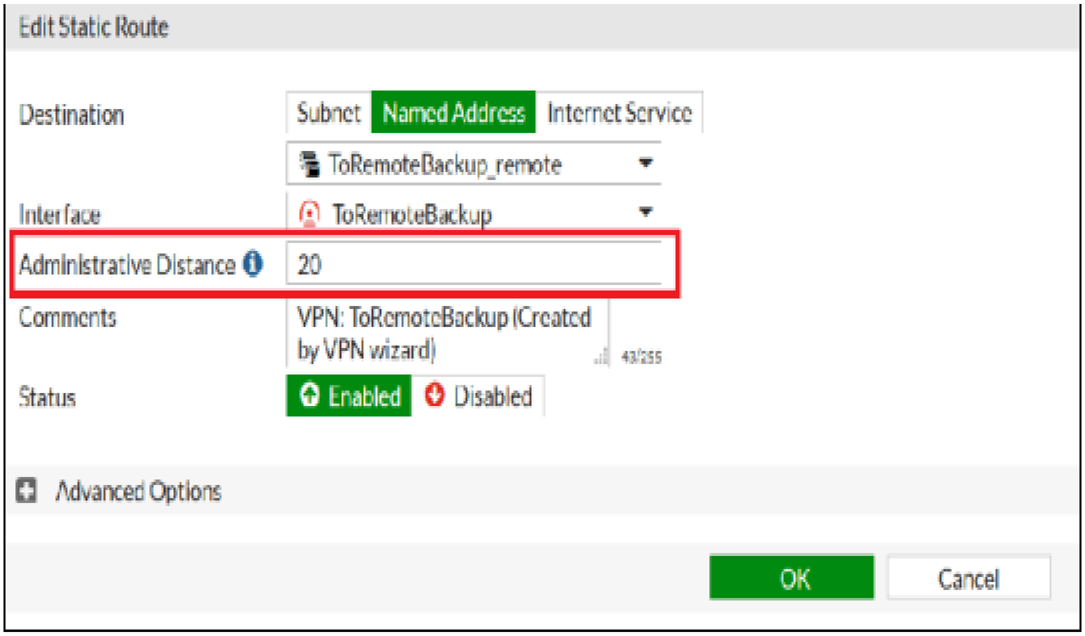
Destination	Gateway IP	Interface	Status	Comments
⊟ IPv4 5				
0.0.0.0/0	10.200.1.254	port1	Enabled	
0.0.0.0/0	10.200.2.254	port2	Enabled	
10.0.2.0/24	10.200.3.1	ToRemote	Enabled	
ToRemoteBackup_remote	10.200.4.1	ToRemoteBackup	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)
ToRemoteBackup_remote		Blackhole	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)

7. Adjust Routing for the Backup VPN Tunnel on Local-FortiGate

I increased the administrative distance of the static route the IPsec wizard created for the ToRemoteBackup VPN, so the tunnel is only used when the ToRemote VPN is down



Destination	Gateway IP	Interface	Status	Comments
IPv4				
0.0.0.0/0	10.200.1.254	port1	Enabled	
0.0.0.0/0	10.200.2.254	port2	Enabled	
10.0.2.0/24	10.200.3.1	ToRemote	Enabled	
ToRemoteBackup_remote	10.200.4.1	ToRemoteBackup	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)
ToRemoteBackup_remote		Blackhole	Enabled	VPN: ToRemoteBackup (Created by VPN wizard)


Edit Static Route

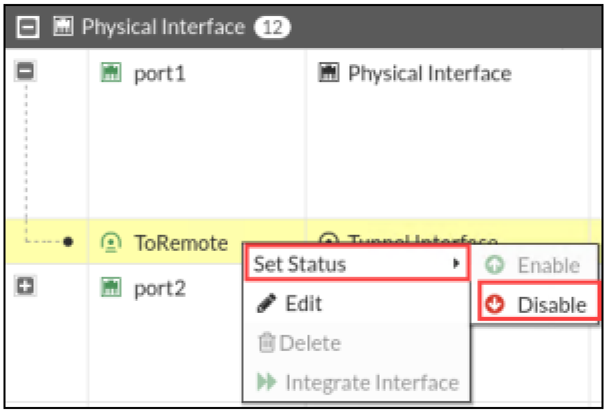
Destination	Subnet / Named Address / Internet Service ToRemoteBackup_remote
Interface	ToRemoteBackup
Administrative Distance	20
Comments	VPN: ToRemoteBackup (Created by VPN wizard) 43/255
Status	Enabled / Disabled

8. Test VPN Redundancy

I tested the VPN failover. I used the sniffer tool to monitor which VPN tunnel the traffic is using,The sniffer output is :

```
28.040086 port3 in 10.0.1.10 -> 10.0.2.10: icmp: echo request
28.040107 ToRemote out 10.0.1.10 -> 10.0.2.10: icmp: echo request
28.041188 ToRemote in 10.0.2.10 -> 10.0.1.10: icmp: echo reply
28.041196 port3 out 10.0.2.10 -> 10.0.1.10: icmp: echo reply
```

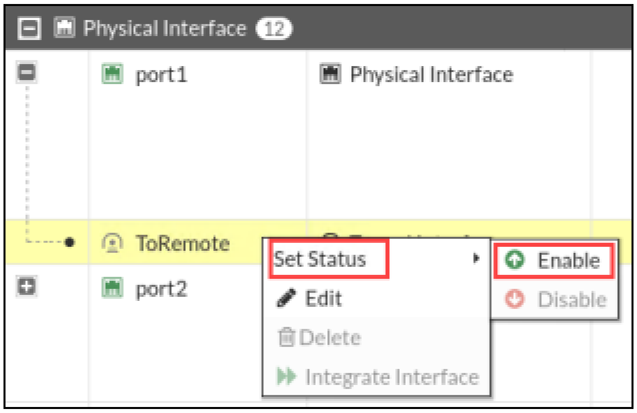
It shows that Local-FortiGate is routing the packets through the **ToRemote** VPN.
then, I simulated a failure in the ToRemote VPN, and observed how FortiGate started using the secondary ToRemoteBackup VPN.



view the sniffer output again. Notice that the **ToRemoteBackup** VPN is being used now

```
546.352063 port3 in 10.0.1.10 -> 10.0.2.10: icmp: echo request
546.352090 ToRemoteBackup out 10.0.1.10 -> 10.0.2.10: icmp: echo request
546.353546 ToRemoteBackup in 10.0.2.10 -> 10.0.1.10: icmp: echo reply
546.353560 port3 out 10.0.2.10 -> 10.0.1.10: icmp: echo reply
```

***Re-enable vpn interface again and see the result**



Use sniffer output again. Notice that **the ToRemote** VPN is being used again.

```
589.622935 port3 in 10.0.1.10 -> 10.0.2.10: icmp: echo request
589.622948 ToRemote out 10.0.1.10 -> 10.0.2.10: icmp: echo request
589.624057 ToRemote in 10.0.2.10 -> 10.0.1.10: icmp: echo reply
589.624072 port3 out 10.0.2.10 -> 10.0.1.10: icmp: echo reply
```