رواد مصر الرقمية

Name: Mohamed Khalid Fathi Ibrahim

Track: Fortinet Cyber security

Groub ID: CAI1_ISS8_S1e

Student ID: 21027505

Project: IPsec VPN

IPsec VPN

Introduction:

A VPN (Virtual Private Network) in a firewall is a secure tunnel that encrypts and protects data traveling between devices or networks over the internet or other public networks. Firewalls integrated with VPN capabilities provide enhanced security by controlling and monitoring traffic and ensuring encrypted connections.

Types of VPN:

- **Site-to-Site VPN (used in this project)**
  - Links entire networks (e.g., branch offices to HQ).
  - Uses IPsec protocol for secure communication.
- **Remote Access VPN**
  - Provides secure access for individual users.
  - Commonly uses IPsec or SSL/TLS.
- **Client-to-Site VPN (SSL VPN)**
  - Remote access via a web browser using HTTPS.
  - Ideal for ad-hoc or temporary access.
- **Mobile VPN**

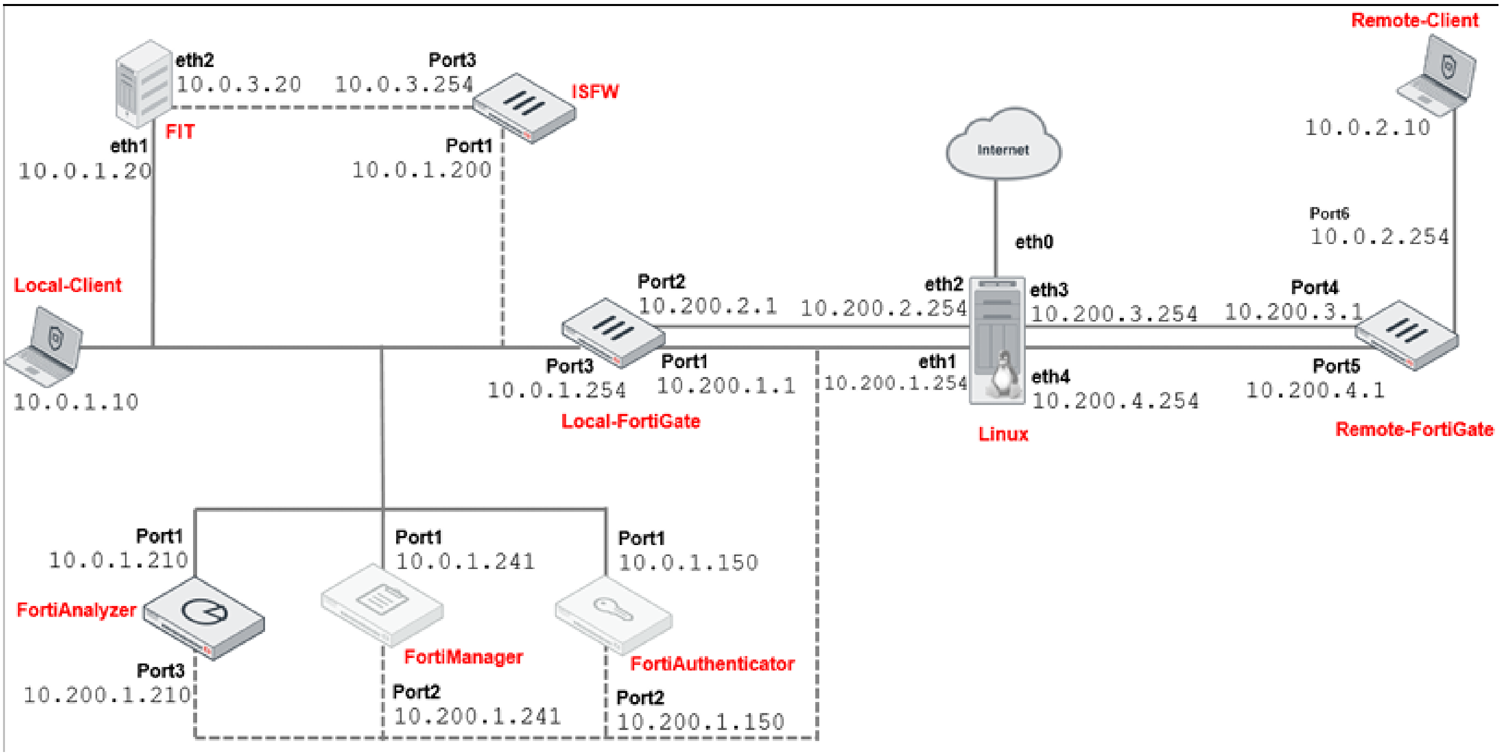
- Ensures stable connectivity for mobile devices across changing networks.

- **Hybrid VPN**
    - Combines Site-to-Site and Remote Access features.

Objective:

- Deploy a site-to-site VPN between two FortiGate devices
- Set up dial-up and static remote gateways

Topology:



Components:

- Local FortiGate
- Remote FortiGate
- Local Client
- Remote Client

Steps:

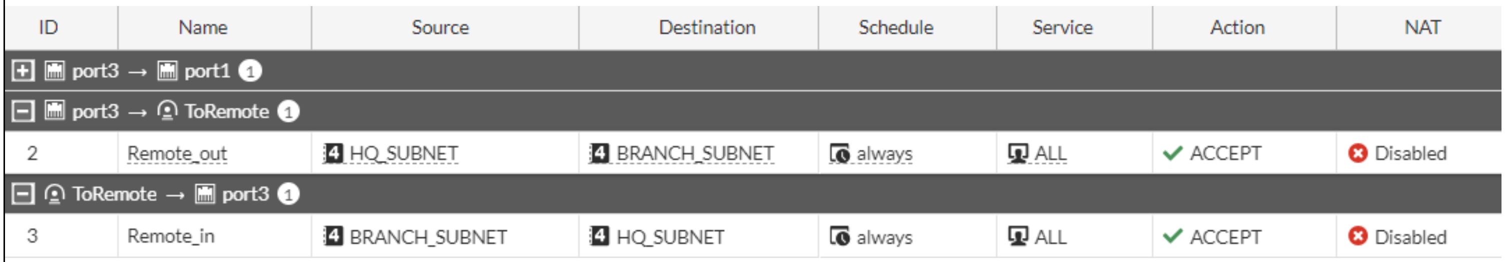
1) dial-up and static remote gateways

- ➢ Create Phase 1 and Phase 2 Negotiations on Local-FortiGate (Dial-Up Server)
  - Open Local FortiGate
  - Click VPN > ipsec tunnel > create new
  - Name : ToRemote , Template type: Custom ,
  - In the **Network** section
    - Remote Gateway: Dialup User
    - Interface: port1
    - Dead Peer Detection: on idel
  - In the **Authentication** section
    - Method: Pre-shared Key ,
    - Pre-shared Key: Fortinet
    - Version: 1
    - Mode: Aggressive
    - Accept Types: Specific peer ID
    - Peer ID: Remote-FortiGate

    - In the **Phase 2 Selectors section** section
        - Local Address : 10.0.1.0/24

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

- On the Local-FortiGate GUI, click Policy & Objects > Firewall Policy > create new
- Choose the next configurations
    - Name: Remote_out
    - Incoming Interface: port 3
    - Outgoing Interface: TORemote
    - Source: HQ_SUBNET
    - Destination: BRANCH_SUBNET
    - Schedule: always
    - Service: all
    - Action: Accept
    - Disable NAT.
- Right click on the policy > choose rverse policy
    - Name : Remote_in
    - Enable this policy



ID	Name	Source	Destination	Schedule	Service	Action	NAT
⊞ port3 → port1 1							
⊟ port3 → ToRemote 1							
2	Remote_out	HQ_SUBNET	BRANCH_SUBNET	always	ALL	✓ ACCEPT	✖ Disabled
⊟ ToRemote → port3 1							
3	Remote_in	BRANCH_SUBNET	HQ_SUBNET	always	ALL	✓ ACCEPT	✖ Disabled

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

- Open Remote-FortiGate GUI
    - Click VPN > ipsec tunnel > create new

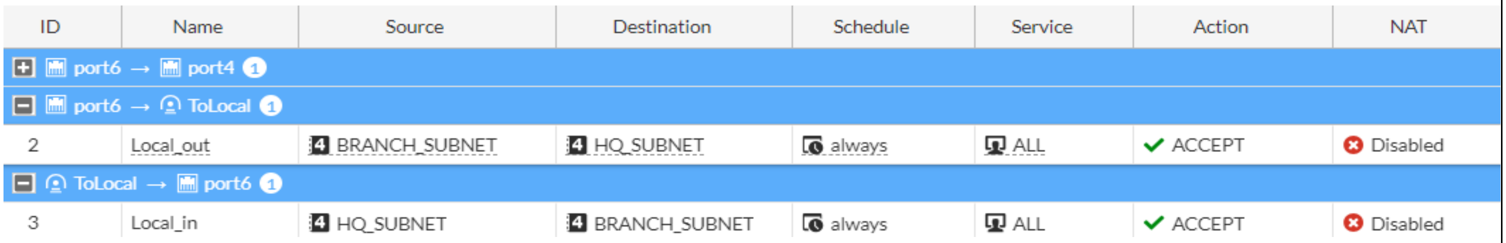
- Name : ToLocal , Template type: Custom ,
- In the **Network** section
  - Remote Gateway: Static IP Address
  - Ip address: 10.200.1.1
  - Interface: port4
  - Dead Peer Detection: on idel
- In the **Authentication** section
  - Method: Pre-shared Key ,
  - Pre-shared Key: Fortinet
  - Version: 1
  - Mode: Aggressive
  - Accept Types: any peer ID

- In the **Phase 1 Proposal** section
  - Local ID : Remote-FortiGate

- In the **Phase 2 Selectors section** section
  - Local Address : 10.0.2.0/24
  - Remote Address: 10.0.1.0/24

- **Create a Static Route for VPN Traffic on Remote-FortiGate (Dial-Up Client)**
  - Remote-FortiGate GUI
  - Network > Static Routes
    - Destination: Subnet 10.0.1.0/24
    - Interface: ToLocal
    - Ok

- **Create the Firewall Policies for VPN Traffic on Remote-FortiGate (Dial-Up Client)**
  - Remote-FortiGate GUI, click Policy & Objects > Firewall Policy.
  - Create new
    - Name : Local_out
    - Incoming Interface: Port 6
    - Outgoing Interface: ToLocal
    - Source: BRANCH_SUBNET
    - Destination: HQ_SUBNET
    - Schedule: always
    - Service: all
    - Action: Accept
    - Disable NAT
    - Ok
- Right Click in the previous Policy and choose Make reverese policy
  - Name : Local_in
  - Enable policy
  - Ok



ID	Name	Source	Destination	Schedule	Service	Action	NAT
⊞ port6 → port4 1							
⊟ port6 → ToLocal 1							
2	Local_out	BRANCH_SUBNET	HQ_SUBNET	always	ALL	✓ ACCEPT	✖ Disabled
⊟ ToLocal → port6 1							
3	Local_in	HQ_SUBNET	BRANCH_SUBNET	always	ALL	✓ ACCEPT	✖ Disabled

Test and Monitor the VPN:

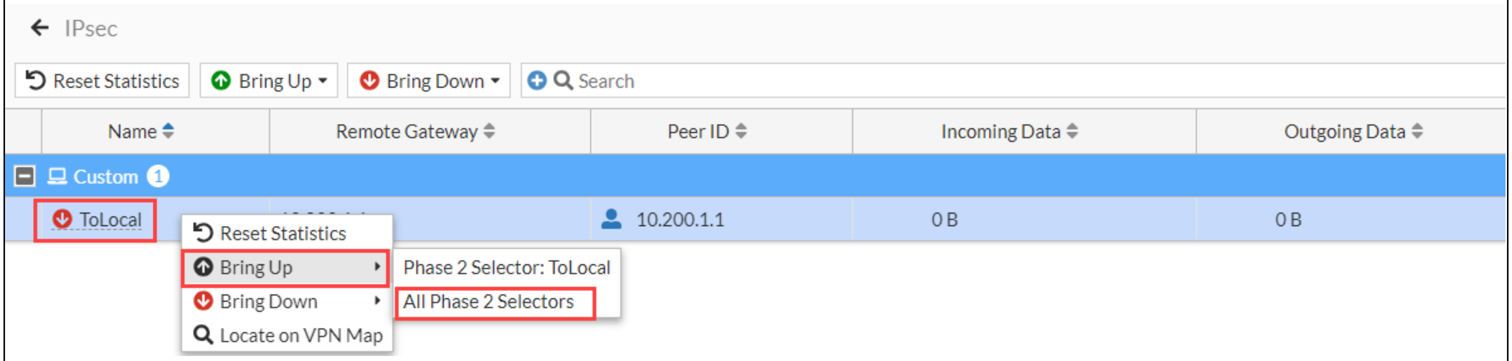
1. On the Remote-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.

2. Click **+** beside **Custom** to expand the custom VPN tunnel section
3.

Notice that the **ToLocal** VPN is currently down.

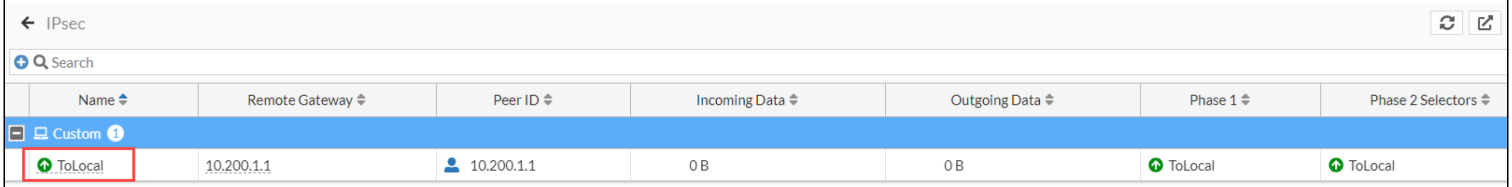
1. Right-click the VPN, and then click **Bring Up** > **All Phase 2 Selectors** to bring up the tunnel.

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 information.



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

It will be green ..



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

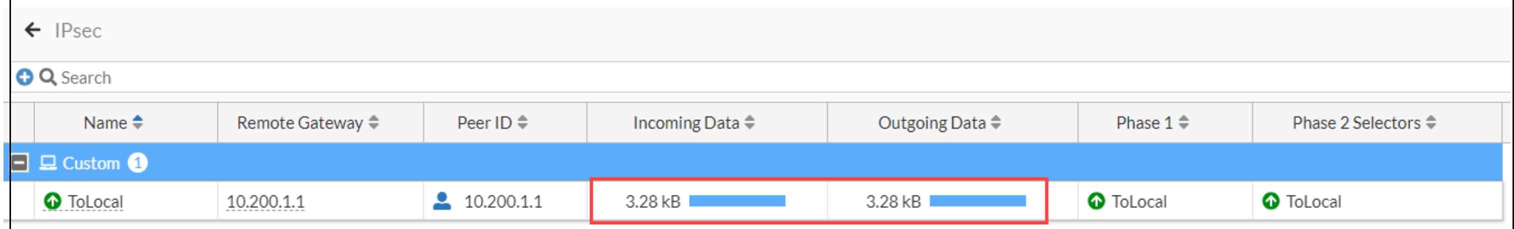
After that

Open remote client vm and ping on 10.0.1.10

It should be work if the tunnel is up

And to Make sure

5. On the Remote-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.

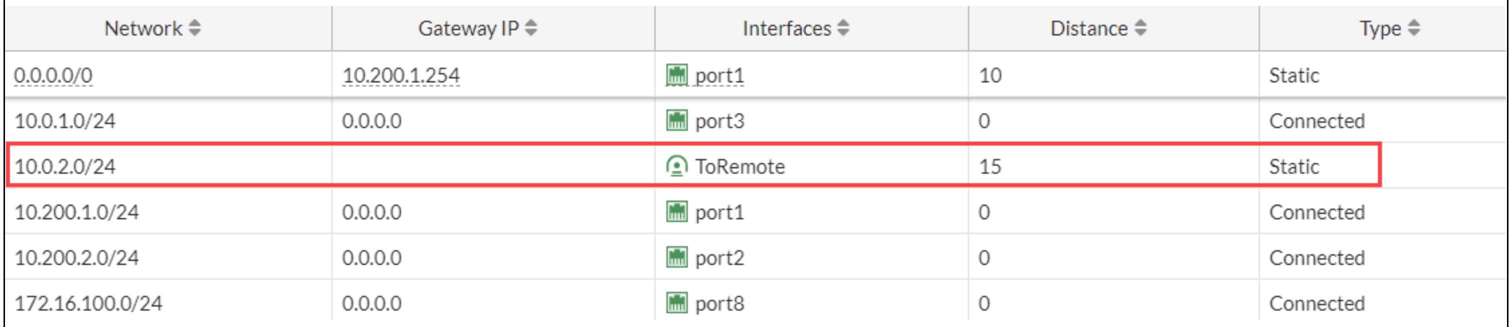


Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Custom 1						
ToLocal	10.200.1.1	10.200.1.1	3.28 kB	3.28 kB	ToLocal	ToLocal

Notic that

You will notice that the counters in the **Incoming Data** and **Outgoing Data** columns increase over time. This indicates that the traffic between 10.0.1.10 and 10.0.2.10 is being encrypted successfully and routed through the tunnel.

.On the Local-FortiGate GUI, click Dashboard > Network > Static & Dynamic Routing.



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.0.2.0/24		ToRemote	15	Static
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

Notice the address listed in the **Gateway IP** column for that route

Finally if you want to Convert it to be between 2 static FortiGate devices

You will repeat this steps but with small changes

As the following

You will change only

- In the local FortiGate
  - In **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**
  - In the **Network** section
    - Remote Gateway: Static IP Address
    - IP Address: 10.200.3.1
  - In the **Authentication** section
    - Accept Types: any peer ID
  - In the **Phase 2 Selectors** section
    - Local Address: 10.0.1.0/24

- Remote Address: 10.0.2.0/24

And any step other is like to dial up configuration