FortiGate

Site-to-Site VPN

1- Objective of the Lab:

The primary objective of this lab is to establish a secure Site-to-Site VPN connection between two geographically separated .networks using FortiGate devices

Goals:

-Configure IPsec VPN tunnels on both FortiGate devices to allow secure communication.

-Test the VPN connection to ensure devices in both sites can communicate securely.

-Demonstrate the use of encryption to protect data between the two sites**.**

2-**Topology**

Description:

Site A: A FortiGate device with a local subnet 192.168.1.0/24 .connected to the WAN using a public IP (1.1.1.1)

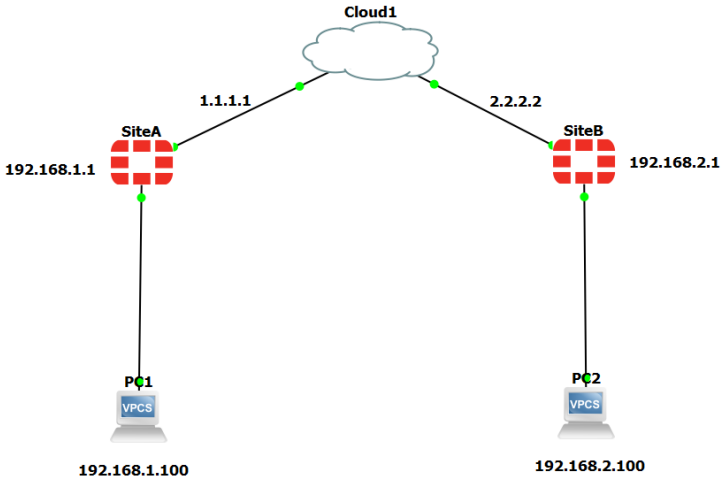
Site B: Another FortiGate device with a local subnet 192.168.2.0/24, also connected to the WAN using a public IP (2.2.2.2).

Network Diagram:

Site A LAN: 192.168.1.0/24

Site B LAN: 192.168.2.0/24

WAN Connection: Public IPs (1. 1.1.1 and 2.2.2.2)



3. Components Used

Hardware: Two FortiGate devices (Physical or Virtual)

Software: (FortiOS 7.4)

Testing Tools:

Ping and traceroute for connectivity verification.

FortiGate’s diagnostic tools (logs and traffic monitoring)

4-Steps of the Lab：

Step 1: Configuring VPN on Site A

Access the FortiGate GUI using the management IP

Navigate to VPN > IPsec Tunnels and click Create New

Select Custom and configure as follows:

Name: SiteA-to-SiteB.

Remote Gateway: Public IP of Site B (2.2.2.2).

Authentication: Pre-shared Key (same key to be used in Site B).

Local Subnet: 192.168.1.0/24.

Remote Subnet: 192.168.2.0/24.

Save the settings and ensure the phase 1 and phase 2 configurations are completed.

Add a firewall policy to allow traffic from LAN A to the VPN tunnel.

Step 2: Configuring VPN on Site B

Repeat the steps above on the FortiGate device in Site B, with the following adjustments:

Name: SiteB-to-SiteA.

Remote Gateway: Public IP of Site A (1.1.1.1).

Local Subnet: 192.168.2.0/24.

Remote Subnet: 192.168.1.0/24.

Step 3: Configuring Firewall Policies

Create bidirectional policies on both FortiGates to allow traffic .between the VPN tunnel and the LANs

Step 4: Verification

Ensure the VPN status is Up on both devices (check under Monitor > IPsec Tunnels).

Test connectivity using ping between devices in both LANs.

5-Testing the Lab:

Scenario 1:

Ping from a PC in Site A (192.168.1.100) to a PC in Site B (192.168.2.100).

Verify that traffic is routed through the VPN tunnel.

Scenario 2:

Verify logs in both FortiGates for encrypted traffic (under Log & Report > Event Logs > VPN).

6-The Results:

Outcome:

A fully operational VPN tunnel was established between Site A and Site B

Devices in both subnets communicated securely through the tunnel

Logs confirmed successful traffic encryption.