Lab 3: Routing

In this lab, I will configure the router settings and test scenarios to learn how FortiGate makes routing decisions.

Objectives

- Route traffic based on the destination IP address, as well as other criteria
- Balance traffic among multiple paths
- Implement route failover
- Diagnose a routing problem

Topology

```
          [ PC1 ]
             |
      [ Switch 1 ]
             |
       [ FortiGate ]
         /       \
    [ Router 1 ]  [ Router 2 ]
      /              \
 [ Network A ]    [ Network B ]
    (10.0.0.0/24)   (192.168.1.0/24)
```

Details of Topology Components:

End Devices:

PC1: A host device used for testing connectivity (e.g., using ping or traceroute).

Switches:

Switch 1: Connects PC1 to the FortiGate firewall.

FortiGate Firewall:

Acts as the central routing device.

Interfaces connected to Router 1 and Router 2.

Routers:

Router 1: Connects to Network A (e.g., 10.0.0.0/24).

Router 2: Connects to Network B (e.g., 192.168.1.0/24).

Networks/Subnets:

Network A: 10.0.0.0/24

Network B: 192.168.1.0/24

Firewall Internal Interface: E.g., 172.16.0.1/24 (for communication with PC1).

Components Used:

- FortiGate Firewall: Used to configure routing settings and enforce policies.
- Routers: Two or more routers for routing configuration and testing.
- End Devices: Computers or virtual machines to test connectivity (e.g., ping, traceroute).
- Switches: For interconnecting devices in the lab setup.
- Cables or Virtual Network Interfaces: For physical or virtual connections.
- Network Simulator or Emulator (Optional): GNS3, EVE-NG, or similar tools for virtualizing the lab.

Steps of the Lab:

1. **Initial Setup:**
    a. Power on the FortiGate firewall and routers.
    b. Connect the devices as per the topology (e.g., FortiGate connected to multiple routers).
2. **Configure Basic Interfaces:**
    a. Assign IP addresses to the interfaces on the FortiGate and routers.
    b. Ensure each interface has a unique subnet.
3. **Static Routing:**
    a. On the FortiGate, configure static routes for each destination network
        i. Similarly, configure static routes on the routers.
4. **4.Firewall Policies:**
    a. Configure appropriate firewall policies to allow traffic between the connected subnets.
5. **5.Testing Tools:**
    a. Use ping and traceroute commands from end devices to test connectivity and ensure correct routing.

Testing the lab

Static Routing Test:

Ping from one subnet to another through the FortiGate.

Verify if the traffic is taking the correct route by using traceroute.

Dynamic Routing Test (if configured):

Verify the routing table on FortiGate using the CLI

Check if dynamically learned routes appear in the routing table.

Failover Test (Optional):

If multiple routes are configured, test route failover by disconnecting one path and verifying connectivity through the alternate route.

The results

The Results:

1. **Routing Table Validation:**
   - The routing table on FortiGate and routers should show all static and dynamically learned routes.
2. **Successful Connectivity:**
   - End devices in different subnets should successfully ping each other.
3. **Traceroute Verification:**
   - Traceroute should display the correct routing path through the FortiGate and connected routers.

This lab demonstrates how FortiGate processes routing decisions and ensures correct traffic flow within a network.