Configure static routes in FortiGate to enable communication between multiple networks.

**Step-by-Step Procedure**

**Step 1: Access FortiGate**

1. Connect to the FortiGate:
   * Using the Web GUI: Open a browser and log in to the FortiGate via its IP (e.g., https://192.168.1.99).
   * Using CLI: Use SSH or console access.

**Step 2: Configure Interfaces**

1. Go to **Network > Interfaces**.
2. Assign IP addresses to the interfaces:
   * Example:
     + **WAN Interface (port1)**: IP 192.168.1.1/24.
     + **LAN Interface (port2)**: IP 10.0.0.1/24.
3. Configure the administrative access for each interface if needed (e.g., HTTPS, SSH, PING).

**Step 3: Configure a Static Route**

1. Navigate to **Network > Static Routes** in the GUI.
2. Click **Create New** to add a route.
3. Input the following:
   * **Destination**: Specify the network you want to route to (e.g., 0.0.0.0/0 for default routing).
   * **Interface**: Select the outgoing interface (e.g., port1 for WAN).
   * **Gateway**: Enter the next-hop IP address provided by your ISP (e.g., 192.168.1.254 for WAN gateway).
   * **Distance**: Leave at default (usually 10).
4. Click **OK** to save.

**Step 4: Configure Firewall Policies**

1. Go to **Policy & Objects > Firewall Policy**.
2. Click **Create New**.
3. Configure the policy for LAN-to-WAN traffic:
   * **Incoming Interface**: Select the LAN interface (e.g., port2).
   * **Outgoing Interface**: Select the WAN interface (e.g., port1).
   * **Source**: Define the LAN subnet (e.g., 10.0.0.0/24).
   * **Destination**: Use all or specify external destinations.
   * **Service**: Use all or specify protocols (e.g., HTTP, HTTPS, DNS).
   * **Action**: Select **Accept**.
4. Enable NAT if routing to the internet.
5. Save the policy.

**Step 5: Test Connectivity**

1. Connect a device to the LAN (e.g., a PC with an IP like 10.0.0.2).
2. Try pinging:
   * The LAN gateway (10.0.0.1).
   * The WAN gateway (192.168.1.254).
   * An external site (e.g., 8.8.8.8).
3. If connectivity fails, check routing, interfaces, and policies.

**Step 6: View Routing Table**

1. In the GUI:
   * Navigate to **Network > Routing Monitor**.
   * Verify the static route is listed.
2. In the CLI:
   * Run the command: get router info routing-table all.

**CLI Example for Routing Configuration**

1. Configure WAN interface:

config system interface

edit "port1"

set ip 192.168.1.1 255.255.255.0

set allowaccess ping https ssh

next

1. Configure LAN interface:

config system interface

edit "port2"

set ip 10.0.0.1 255.255.255.0

set allowaccess ping https ssh

next

1. Add a static route:

config router static

edit 1

set dst 0.0.0.0 0.0.0.0

set gateway 192.168.1.254

set device "port1"

next

Topology for FortiGate Routing

**Description**

* **WAN Interface**: Connected to the ISP or an external network.
* **LAN Interface**: Connected to the internal network (e.g., a switch or directly to a client device like a PC).
* A **test client** (e.g., a PC or laptop) is connected to the LAN subnet to test connectivity.

**IP Address Details**

1. **WAN Interface (port1)**:
   * IP: 192.168.1.1/24
   * Gateway: 192.168.1.254 (ISP Router IP)
   * Destination for default route: 0.0.0.0/0.
2. **LAN Interface (port2)**:
   * IP: 10.0.0.1/24
   * Connected to internal devices (e.g., test PC with IP 10.0.0.2).

**Steps to Implement the Topology**

1. **Connect WAN Interface**:
   * Attach the WAN interface (port1) to the ISP router or external gateway using an Ethernet cable.
   * Assign an IP from the same subnet as the ISP router (e.g., 192.168.1.1/24).
2. **Connect LAN Interface**:
   * Connect the LAN interface (port2) to a switch or directly to a client device.
   * Assign an IP from a different subnet (e.g., 10.0.0.1/24).
3. **Test Client Configuration**:
   * Set the test PC's IP manually (e.g., 10.0.0.2/24) or use a DHCP server if configured.
   * Gateway for the test PC: 10.0.0.1.

**Components**

1. **ISP Router**:
   * Simulates the internet or upstream gateway.
   * IP Address: 192.168.1.254/24.
   * Gateway for FortiGate WAN interface traffic.
2. **FortiGate Firewall**:
   * Manages traffic between LAN and WAN (routes packets between networks).
   * Interfaces:
     + **WAN (port1)**: 192.168.1.1/24.
     + **LAN (port2)**: 10.0.0.1/24.
3. **LAN (Internal Network)**:
   * Devices connected to the LAN interface (e.g., PCs, servers, printers).
   * Example device: Test PC with IP 10.0.0.2/24 and Gateway 10.0.0.1.

**Details of Configuration**

**Step 1: ISP Router**

1. **Simulated Environment**:
   * Use an actual ISP connection or simulate it with another router.
   * Assign an IP address to the router (e.g., 192.168.1.254/24).
2. **Purpose**:
   * Acts as a gateway for all traffic leaving the FortiGate.

**Step 2: FortiGate Configuration**

1. **WAN Interface**:
   * Connect to the ISP router via Ethernet.
   * Assign the IP 192.168.1.1/24.
   * Gateway: 192.168.1.254.
   * **Configuration via GUI**:
     + Go to **Network > Interfaces**.
     + Edit port1:
       - Set IP/Netmask: 192.168.1.1/24.
       - Set **Administrative Access**: Enable PING and HTTPS.

**Firewall Policy**:

* Allow traffic from LAN to WAN.
* **Configuration via GUI**:
  + Go to **Policy & Objects > Firewall Policy**.
  + Create a policy:
    - Incoming Interface: port2 (LAN).
    - Outgoing Interface: port1 (WAN).
    - Source: 10.0.0.0/24.
    - Destination: all (or specify a range).
    - Action: Accept.
    - NAT: Enable.

**Configuration via CLI**:

config firewall policy

edit 1

set name "LAN-to-WAN"

set srcintf "port2"

set dstintf "port1"

set srcaddr "all"

set dstaddr "all"

set action accept

set schedule "always"

set service "ALL"

set nat enable

next

end

**Step 3: Test Client (PC)**

1. Assign a static IP to the PC:
   * IP Address: 10.0.0.2.
   * Subnet Mask: 255.255.255.0.
   * Default Gateway: 10.0.0.1.
2. Test connectivity:
   * Ping 10.0.0.1 (LAN Interface) → Success.
   * Ping 192.168.1.254 (ISP Router) → Success.
   * Ping 8.8.8.8 (Google DNS) → Success if routing is properly set up.

**Step 4: Troubleshooting**

* If connectivity fails:
  + Verify IP settings on all devices.
  + Check routing tables (get router info routing-table all).
  + Ensure firewall policies allow traffic.
  + Use CLI debugging:

diagnose debug enable

diagnose debug flow filter addr 10.0.0.2

diagnose debug flow trace start 10