FortiGate 60F Setup Guide with SD-WAN for Multiple WAN Connections

This guide will help you configure your FortiGate 60F with the following features:

- **Introduction to SD-WAN**
- **Three WAN Connections**: Fiber (Primary), 5G, and Starlink
- **SD-WAN Configuration**: For load balancing and redundancy
- **Three VLANs**: Home, Guest, and IoT
- **Firewall Rules**: Optimized for streaming and gaming
- **Traffic Prioritization**: Using Quality of Service (QoS)

Prerequisites

- **FortiGate 60F**: Ensure your FortiGate device is powered on and connected to your network.
- **Access to FortiGate Management Interface**: Use a web browser to access the FortiGate interface at `https://<FortiGate-IP>`.
- **WAN Connections**: Have your Fiber, 5G, and Starlink connections physically connected to the FortiGate.
- **Basic Network Knowledge**: Familiarity with network configurations and terms.

Step-by-Step Setup

Step 1: Access FortiGate Management Interface

1. Open a web browser and navigate to the FortiGate's IP address.
2. Log in using your admin credentials.
   - **Default Username**: `admin`
   - **Default Password**: *(Leave blank initially; change immediately for security)*

Step 2: Configure WAN Interfaces

Navigate to **Network > Interfaces** to configure your WAN connections.

Configure Fiber Connection (Primary)

- **Interface Name**: `WAN_Fiber`
- **Physical Interface**: e.g., `port2`
- **Role**: `WAN`
- **Addressing Mode**: Configure according to your ISP (e.g., DHCP, Static, PPPoE)
- **Distance**: `5` *(Lower distance gives higher priority in routing)*

Configure 5G Connection

- **Interface Name**: `WAN_5G`
- **Physical Interface**: e.g., `port3`
- **Role**: `WAN`
- **Addressing Mode**: Configure according to your ISP
- **Distance**: `10`

Configure Starlink Connection

- **Interface Name**: `WAN_Starlink`
- **Physical Interface**: e.g., `port4`
- **Role**: `WAN`
- **Addressing Mode**: Configure according to your ISP
- **Distance**: `15`

Step 3: Configure SD-WAN

Navigate to **Network > SD-WAN** to set up load balancing and failover.

Add Member Interfaces

1. Click **Create New** to add WAN interfaces to SD-WAN.
2. **Add WAN_Fiber**
   - **Interface**: `WAN_Fiber`
   - **Weight**: `0`
   - **Priority**: `1`
3. **Add WAN_5G**
   - **Interface**: `WAN_5G`
   - **Weight**: `0`
   - **Priority**: `2`
4. **Add WAN_Starlink**
   - **Interface**: `WAN_Starlink`
   - **Weight**: `0`

- **Priority**: `3`

Configure SD-WAN Rules

1. Go to the **SD-WAN Rules** tab.
2. Click **Create New**.
   - **Name**: `Default_Rule`
   - **Incoming Interfaces**: `VLAN_Home`, `VLAN_Guest`, `VLAN_IoT`
   - **Source**: `All`
   - **Destination**: `All`
   - **Service**: `All`
   - **Outgoing Interfaces**: `Best Quality (SLA)` or `Manual (choose preferred interfaces)`
3. **Set Interface Preference**
   - **Preferred Interfaces**: `WAN_Fiber`, `WAN_5G`, `WAN_Starlink`
   - **Load Balancing Algorithm**: `Manual`

Step 4: Configure VLANs

Navigate to **Network > Interfaces** to set up VLANs.

Home VLAN

- **Interface Name**: `VLAN_Home`
- **VLAN ID**: `10`
- **Interface**: Physical interface connected to your switch (e.g., `port1`)
- **IP/Netmask**: `192.168.10.1/24`

Guest VLAN

- **Interface Name**: `VLAN_Guest`
- **VLAN ID**: `20`
- **Interface**: `port1`
- **IP/Netmask**: `192.168.20.1/24`

IoT VLAN

- **Interface Name**: `VLAN_IoT`
- **VLAN ID**: `30`
- **Interface**: `port1`
- **IP/Netmask**: `192.168.30.1/24`

Step 5: Configure DHCP for Each VLAN

Navigate to **Network > DHCP Servers**.

Home VLAN DHCP

- **Interface**: `VLAN_Home`
- **IP Range**: `192.168.10.2` to `192.168.10.100`

Guest VLAN DHCP

- **Interface**: `VLAN_Guest`
- **IP Range**: `192.168.20.2` to `192.168.20.100`

IoT VLAN DHCP

- **Interface**: `VLAN_IoT`
- **IP Range**: `192.168.30.2` to `192.168.30.100`

Step 6: Configure Security Policies

Navigate to **Policy & Objects > Firewall Policy**.

Allow Traffic from VLANs to SD-WAN

1. **Home VLAN to Internet**
   - **Name**: `Allow_Home_to_Internet`
   - **Incoming Interface**: `VLAN_Home`
   - **Outgoing Interface**: `SD-WAN`
   - **Source**: `All`
   - **Destination**: `All`
   - **Service**: `All`
   - **Action**: `Accept`
   - **NAT**: Enable
2. **Guest VLAN to Internet**
   - **Name**: `Allow_Guest_to_Internet`
   - **Incoming Interface**: `VLAN_Guest`
   - **Outgoing Interface**: `SD-WAN`
   - **Source**: `All`
   - **Destination**: `All`
   - **Service**: `All`
   - **Action**: `Accept`
   - **NAT**: Enable
3. **IoT VLAN to Internet**
   - **Name**: `Allow_IoT_to_Internet`
   - **Incoming Interface**: `VLAN_IoT`
   - **Outgoing Interface**: `SD-WAN`
   - **Source**: `All`
   - **Destination**: `All`
   - **Service**: `All`
   - **Action**: `Accept`
   - **NAT**: Enable

Deny Inter-VLAN Traffic

- **Name**: `Deny_InterVLAN`
- **Incoming Interface**: `VLAN_Home`, `VLAN_Guest`, `VLAN_IoT`
- **Outgoing Interface**: `VLAN_Home`, `VLAN_Guest`, `VLAN_IoT`
- **Source**: `All`
- **Destination**: `All`
- **Service**: `All`
- **Action**: `Deny`

Step 7: Configure Traffic Prioritization (QoS)

Navigate to **Policy & Objects > Traffic Shapers**.

Create Traffic Shapers

1. **Gaming Traffic Shaper**
   - **Name**: `Priority_Gaming`
   - **Type**: `Per Policy`
   - **Priority**: `High`
   - **Bandwidth**: Set according to your requirements
2. **Streaming Traffic Shaper**
   - **Name**: `Priority_Streaming`
   - **Type**: `Per Policy`
   - **Priority**: `Medium`
   - **Bandwidth**: Set according to your requirements

Apply Traffic Shapers to Policies

1. Edit the **Allow_Home_to_Internet** policy.
2. Under **Traffic Shaping**, enable **Apply Shaper Per Policy**.
3. Select the appropriate traffic shaper based on the service.

Step 8: Configure SD-WAN Performance SLA (Optional)

Navigate to **Network > SD-WAN > Performance SLA**.

Create SLA Targets

1. Click **Create New**.
2. **Name**: `SLA_Fiber`
   - **Members**: `WAN_Fiber`
   - **Latency**, **Jitter**, **Packet Loss**: Set thresholds
   - **Protocol**: `Ping` or `HTTP`
   - **Server**: Reliable external IP (e.g., 8.8.8.8)

Repeat for `WAN_5G` and `WAN_Starlink` if desired.

Configure SD-WAN Rules with SLA

1. Go back to **SD-WAN Rules**.
2. Edit `Default_Rule`.
3. Under **SLA**, select the SLA targets you created.
4. Set the **SLA Mode** to `Best Quality`.

Step 9: Test Configuration

- **Connectivity**: Verify that devices on each VLAN receive the correct IP addresses and can access the internet.
- **Failover**: Disconnect the Fiber connection to test if traffic fails over to 5G or Starlink.
- **Load Balancing**: Monitor traffic to see if load balancing is functioning as configured.
- **QoS**: Test streaming and gaming applications to ensure they receive priority bandwidth.

Additional Tips

- **Secure Access**: Change the default admin password and enable HTTPS-only access under **System > Settings**.
- **Regular Backups**: Go to **System > Maintenance > Backup & Restore** to back up your configuration.
- **Firmware Updates**: Check **System > Firmware** for updates to keep your FortiGate secure and up-to-date.

By following this guide, you should have a robust network setup that leverages SD-WAN to manage multiple WAN connections, provides separate VLANs for different device types, and prioritizes critical traffic like gaming and streaming. The Fiber connection is set as the primary link, ensuring the best performance under normal conditions, with 5G and Starlink as backups for redundancy.

Revision #1
Created 11 October 2024 05:09:13 by Jarryd
Updated 11 October 2024 05:10:58 by Jarryd