FortiGate 60F Setup Guide (Basic Home Network Setup)

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

- **Three VLANs**: Home, Guest, and IoT
- **Firewall Rules**: Optimized for streaming and gaming
- **Traffic Prioritization**: Using Quality of Service (QoS)

Prerequisites

1. **FortiGate 60F**: Ensure your FortiGate device is powered on and connected to your network.
2. **Access to FortiGate Management Interface**: Use a web browser to access the FortiGate interface at `http://<FortiGate-IP>`.
3. **Basic Network Setup**: Have an existing internet connection and basic knowledge of network configurations.

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. The default username is `admin`, and there is no password initially (change this immediately for security).

Step 2: Configure VLANs

1. **Navigate to**: `Network > Interfaces`.
2. **Create VLANs** for Home, Guest, and IoT.

Home VLAN

- **Interface Name**: VLAN_Home
- **VLAN ID**: 10
- **Interface**: Select the physical interface (e.g., `port1`) to assign the VLAN.
- **IP/Netmask**: `192.168.10.1/24`

Guest VLAN

- **Interface Name**: VLAN_Guest
- **VLAN ID**: 20
- **Interface**: Select the physical interface (e.g., `port1`) to assign the VLAN.
- **IP/Netmask**: `192.168.20.1/24`

IoT VLAN

- **Interface Name**: VLAN_IoT
- **VLAN ID**: 30
- **Interface**: Select the physical interface (e.g., `port1`) to assign the VLAN.
- **IP/Netmask**: `192.168.30.1/24`

Step 3: Configure DHCP for Each VLAN

1. **Navigate to**: `Network > DHCP Servers`.
2. **Create DHCP servers** for each VLAN.

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 4: Configure Security Policies

1. **Navigate to**: `Policy & Objects > IPv4 Policy`.
2. **Create policies** to manage traffic between zones.

Allow Traffic from Home to Internet

- **Name**: Allow_Home_to_Internet
- **Incoming Interface**: VLAN_Home
- **Outgoing Interface**: WAN
- **Source**: All
- **Destination**: All
- **Action**: Accept

Allow Traffic from Guest to Internet

- **Name**: Allow_Guest_to_Internet
- **Incoming Interface**: VLAN_Guest
- **Outgoing Interface**: WAN
- **Source**: All
- **Destination**: All
- **Action**: Accept

Allow Traffic from IoT to Internet

- **Name**: Allow_IoT_to_Internet
- **Incoming Interface**: VLAN_IoT
- **Outgoing Interface**: WAN
- **Source**: All
- **Destination**: All
- **Action**: Accept

Deny Traffic Between VLANs

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

Step 5: Configure Traffic Prioritization (QoS)

1. **Navigate to**: `Policy & Objects > Traffic Shapers`.
2. **Create traffic shapers** to prioritize gaming and streaming traffic.

Create Traffic Shapers for Gaming and Streaming

- **Name**: Priority_Gaming
  - **Priority**: High
  - **Traffic Type**: Custom
  - **Bandwidth**: Define based on gaming traffic requirements
- **Name**: Priority_Streaming
  - **Priority**: Medium
  - **Traffic Type**: Custom
  - **Bandwidth**: Define based on streaming traffic requirements

3. **Apply Traffic Shapers** to the relevant policies by editing the policies and assigning the appropriate traffic shaper.

Step 6: Test Configuration

1. **Verify device connectivity** on each VLAN.
2. **Test internet access** from each VLAN to ensure policies are correctly applied.
3. **Monitor traffic** to ensure streaming and gaming traffic are prioritized as expected.

Additional Tips

- **Secure Access**: Change the default admin password and enable HTTPS access only.
- **Regular Backups**: Regularly backup your configuration to prevent data loss.
- **Firmware Updates**: Keep your FortiGate firmware updated for the latest features and security patches.

Revision #1
Created 9 August 2024 13:00:15 by Jarryd
Updated 9 August 2024 13:41:26 by Jarryd