Juniper Networks

Juniper setup guides and tutorials

- Router Setup
  - Juniper SRX320 Setup Guide (Basic Network)

Router Setup

Router setup guides

Juniper SRX320 Setup Guide (Basic Network)

This guide will help you configure your Juniper SRX320 router 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. **Juniper SRX320**: Ensure your SRX320 is powered on and connected to your network.
2. **J-Web Interface**: Access the router through a web browser at `http://<SRX320-IP>`.
3. **Basic Network Setup**: Have an existing internet connection and basic understanding of network configurations.

Step-by-Step Setup

Step 1: Access Juniper SRX320

1. **Open a web browser** and navigate to the SRX320's IP address.
2. **Log in** using the default credentials or your configured admin username and password.

Step 2: Configure VLANs

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

Home VLAN

- **VLAN ID**: 10
- **Interface**: `ge-0/0/1.10`
- **IP Address**: `192.168.10.1/24`

Guest VLAN

- **VLAN ID**: 20
- **Interface**: `ge-0/0/1.20`
- **IP Address**: `192.168.20.1/24`

IoT VLAN

- **VLAN ID**: 30
- **Interface**: `ge-0/0/1.30`
- **IP Address**: `192.168.30.1/24`

Step 3: Configure DHCP for Each VLAN

1. **Navigate to**: `Network > DHCP Server`.
2. **Configure DHCP** for each VLAN.

Home VLAN DHCP

- **Interface**: `ge-0/0/1.10`
- **Pool**: `192.168.10.10 to 192.168.10.100`

Guest VLAN DHCP

- **Interface**: `ge-0/0/1.20`
- **Pool**: `192.168.20.10 to 192.168.20.100`

IoT VLAN DHCP

- **Interface**: `ge-0/0/1.30`
- **Pool**: `192.168.30.10 to 192.168.30.100`

Step 4: Configure Security Zones

1. **Navigate to**: `Security > Security Zones`.
2. **Create security zones** for each VLAN.

Home Zone

- **Zone Name**: home
- **Interfaces**: Add `ge-0/0/1.10`

Guest Zone

- **Zone Name**: guest
- **Interfaces**: Add `ge-0/0/1.20`

IoT Zone

- **Zone Name**: iot
- **Interfaces**: Add `ge-0/0/1.30`

Step 5: Configure Firewall Policies

1. **Navigate to**: `Security > Policies`.
2. **Create policies** to manage traffic between zones.

Allow Traffic from Home to Internet

- **Source Zone**: home
- **Destination Zone**: untrust
- **Policy**: Allow

Allow Traffic from Guest to Internet

- **Source Zone**: guest
- **Destination Zone**: untrust
- **Policy**: Allow

Allow Traffic from IoT to Internet

- **Source Zone**: iot
- **Destination Zone**: untrust
- **Policy**: Allow

Deny Traffic Between VLANs

- **Source Zone**: home
- **Destination Zone**: guest, iot
- **Policy**: Deny
- **Source Zone**: guest
- **Destination Zone**: home, iot
- **Policy**: Deny
- **Source Zone**: iot
- **Destination Zone**: home, guest
- **Policy**: Deny

Step 6: Configure Traffic Prioritization (QoS)

1. **Navigate to**: `Network > Quality of Service`.
2. **Create QoS profiles** to prioritize gaming and streaming traffic.

Create Classifiers for Gaming and Streaming

- **Classifier Name**: gaming
  - **DSCP**: 46 (EF for low latency)

    - **Application**: Match traffic to gaming servers
- **Classifier Name**: streaming
    - **DSCP**: 34 (AF41 for streaming)
    - **Application**: Match traffic to streaming services

Apply Classifiers to Interfaces

- Apply the classifiers to the interfaces connected to your gaming and streaming devices.

Step 7: Apply and Test Configuration

1. **Review all configurations** and apply changes.
2. **Test the network**:
    - Verify that devices on each VLAN receive the correct IP addresses.
    - Test internet connectivity for devices on each VLAN.
    - Ensure that gaming and streaming traffic is prioritized as expected.

Additional Tips

- **Secure Access**: Change the default admin password and restrict management access to trusted IPs.
- **Regular Backups**: Backup your configuration regularly to prevent data loss.
- **Firmware Updates**: Keep the SRX320 firmware updated for security and performance enhancements.