Setting Up Port Forwarding for IPSEC IKE Tunnel

Introduction

- Port forwarding, also known as tunnelling, is a network technology procedure that enables external devices to access services on a private network. This is achieved by rerouting communication requests from one address and port number combination to another while packets traverse a network gateway.
- It is extensively used in scenarios where certain applications or services need to be accessible from the internet, including online gaming, torrent downloads, and hosting web servers. These applications typically require direct communication with devices on your private network, which isn't possible due to NAT (Network Address Translation) mechanisms used by most routers.
- While port forwarding can grant outside access and improve connectivity, it also presents a potential risk as it exposes your internal network to the internet. As such, it's crucial to exercise due caution by only forwarding necessary ports and implementing robust security measures such as using strong, complex passwords and up-to-date firewall settings.

Method

Step 1: Access MikroTik Router

1. Open Winbox or your web browser and connect to your MikroTik router.
2. Log in using your credentials.

Step 2: Configure Port Forwarding

1. **Go to IP > Firewall > NAT**.
2. Click on the **+** to add a new rule.

1. Port Forwarding for UDP Port 500 (IKE)

- **General Tab**:
  - **Chain**: dstnat

- **Protocol**: udp
- **Dst. Port**: 500 (this may change, request from the client what is needed. Also ensure that it does not interfere with any existing ports configured)

- **Action Tab**:
  - **Action**: dst-nat
  - **To Addresses**: Internal IP address (e.g., 192.168.1.2)
  - **To Ports**: 500 (this may change, request from the client what is needed. Also ensure that it does not interfere with any existing ports configured)

2. Port Forwarding for UDP Port 4500 (NAT-T)

- **General Tab**:
  - **Chain**: dstnat
  - **Protocol**: udp
  - **Dst. Port**: 4500 (this may change, request from the client what is needed. Also ensure that it does not interfere with any existing ports configured)

- **Action Tab**:
  - **Action**: dst-nat
  - **To Addresses**: Internal IP address (e.g., 192.168.1.2)
  - **To Ports**: 4500 (this may change, request from the client what is needed. Also ensure that it does not interfere with any existing ports configured)

Step 3: Configure Firewall Rules

1. **Go to IP > Firewall > Filter Rules**.
2. Click on the **+** to add new rules.

1. Allow UDP Port 500 (IKE)

- **General Tab**:
  - **Chain**: forward
  - **Protocol**: udp
  - **Dst. Port**: 500 (this may change, request from the client what is needed. Also ensure that it does not interfere with any existing ports configured)

- **Action Tab**:
  - **Action**: accept

2. Allow UDP Port 4500 (NAT-T)

- **General Tab**:
  - **Chain**: forward

    - **Protocol**: udp
    - **Dst. Port**: 4500 (this may change, request from the client what is needed. Also ensure that it does not interfere with any existing ports configured)

- **Action Tab**:
    - **Action**: accept

Step 4: Sort the Filter Rules

- Drag and drop the filter rules you have created in **Step 3** so that they are above any existing 'drop rules'.

Step 5: Ensure IP Forwarding is Enabled

1. **Go to IP > Settings**.
2. Make sure **IP Forwarding** is enabled.

Step 6: Verify Configuration

1. **Check the NAT Rules**:

- Ensure the NAT rules are correctly set up and active.
- Go to **IP > Firewall > NAT** and verify that the new rules are listed and active.
- **Check the Firewall Rules**:

- Ensure the firewall rules are correctly set up and active.
- Go to **IP > Firewall > Filter Rules** and verify that the new rules are listed and active.
- **Test the VPN Connection**:

- Attempt to establish the VPN connection from the internal router to Azure.
- Verify the connection by checking the VPN status on the internal router.

Revision #1
Created 9 August 2024 06:41:29 by Jarryd
Updated 9 August 2024 06:42:12 by Jarryd