Setting Up an Azure Server

Setting up a server on Microsoft Azure and configuring it to open specific ports is essential for various applications, including hosting services, proxies, and more. This guide will walk you through the process of creating an Azure Virtual Machine (VM) and configuring the firewall to open port 1080.

Table of Contents

Prerequisites

Before you begin, ensure you have the following:

- An active Microsoft Azure account.
- Basic knowledge of using the Azure Portal.
- SSH client (like Terminal on macOS/Linux or PuTTY on Windows) for accessing the VM.

Creating an Azure Virtual Machine

1. Log into the Azure Portal: Navigate to the Azure Portal and sign in with your credentials.

2. Create a New Virtual Machine:

   - Click on “Create a resource” in the upper-left corner.
   - Select “Virtual Machine” from the list of available resources.

3. Configure VM Basics:

   - Subscription: Choose your Azure subscription.
   - Resource Group: Create a new resource group or select an existing one.
   - Virtual Machine Name: Enter a name for your VM (e.g., `AzureServer`).
   - Region: Select the region closest to your target audience.
   - Image: Choose an OS image (e.g., Ubuntu 22.04 LTS).
   - Size: Select a VM size based on your performance needs.
   - Authentication: Choose SSH public key for secure access. Upload your public SSH key.

4. Configure Networking:

- Ensure the VM is placed in the appropriate Virtual Network and Subnet.
- Leave the Public IP enabled to allow external access.

5. Review and Create:

   - Review your configurations.
   - Click “Create” to deploy the VM. Deployment may take a few minutes.

Configuring the Firewall to Open Port 1080

Once your VM is up and running, you’ll need to configure Azure’s Network Security Group (NSG) to allow traffic on port 1080.

1. Navigate to Your VM’s Networking Settings:
   - In the Azure Portal, go to “Virtual Machines”.
   - Select your VM (`AzureServer`).
   - Click on “Networking” in the left sidebar.
2. Identify the Network Security Group (NSG):
   - Under “Network Interface”, locate the associated NSG.
   - Click on the NSG to manage its rules.
3. Add an Inbound Security Rule:
   - In the NSG settings, go to “Inbound security rules”.
   - Click “Add” to create a new rule.
4. Configure the Rule:
   - Source: Any (or specify a range for enhanced security).
   - Source port ranges: `*`
   - Destination: Any
   - Destination port ranges: `1080`
   - Protocol: TCP
   - Action: Allow
   - Priority: `1000` (ensure it doesn’t conflict with existing rules).
   - Name: `Allow-1080-TCP`
5. Save the Rule:
   - Click “Add” to apply the new rule.

Testing the Configuration

After configuring the firewall, it’s essential to verify that port 1080 is open and accessible.

1. Use Telnet to Verify Port Accessibility: From your local machine, run:

```
telnet <YOUR_VM_IP> 1080
```

   - Replace `<YOUR_VM_IP>` with your VM’ s public IP address.
   - If the connection is successful, the port is open and accessible.

2. Alternative Port Checking Tools:

   - Netcat (`nc`):

     ```
     nc -zv <YOUR_VM_IP> 1080
     ```

   - Online Port Checkers: Use online services like canyouseeme.org to check if port 1080 is open.

3. Troubleshooting:

   - Connection Issues: Verify that the NSG rules are correctly set and that any local firewalls on the VM are configured to allow traffic on port 1080.
   - Incorrect IP: Ensure you’ re using the correct public IP address of your VM.

Conclusion

By following this guide, you’ ve successfully set up an Azure Virtual Machine and configured the firewall to open port 1080. This setup lays the foundation for deploying various applications or services that require specific port access.

For further configurations, such as setting up proxy services or other applications on port 1080, refer to our dedicated posts on V2Ray Proxy Setup and Generating a Custom vmess URL.