OS-Management
Networked Project

Author: Severin Mikesch

Datum: 10.06.2020

1 Introduction

This is a simple guide to show the steps needed to set up virtual machines in Proxmox and install an SSH daemon and NGINX. Furthermore a VPN connection between two VMs will be established and a firewall set up.
I will be using following tools and environments:

- Proxmox
- OpenSSH
- Ubuntu server 20.04 LTS
- tinc
- nginx
- iptables

2 Setup of VMs in Proxmox

Proxmox VE (Virtual Environment) is an open-source solution for enterprise virtualization utilizing the KVM hypervisor running on Debian. I will skip the setup of the Proxmox server as it is a rather long an tedious process and I already have a Proxmox server running at home.
At first we will upload the ISO of Ubuntu server to the proxmox server in order to start our VMs from it.

2.1 VM Configuration

Before setting up the two VMs we have to make sure that there is a network bridge configured for the LAN in which the client will be placed.
We can leave the defaults of Proxmox when creating the VMs. We just have to define following things:

- ISO Image: ubuntu server
- Disk Size: 10GB
- CPU Cores: 2
- RAM: 2048 MB
- Network Bridge: your LAN Bridge

Now the settings can be confirmed and the VMs be started.

2.2 Ubuntu server installation on VM1

After the first VM was started a installer will guide you through the process.

2.2.1 Language selection

Select an appropriate language. We will select english.

2.2.2 optional installer upgrade

When prompted with an optional installer upgrade this should be accepted. The installer will continue here with the newest version.

2.2.3 Keyboard layout

Select the appropriate keyboard layout. We will use the German (Austria) layout.

2.2.4 Network connections

Here the previously selected LAN Bridge should be shown. Configure a static IPv4 address. In this example the address 192.168.1.91/24 will be used.

2.2.5 Proxy configuration

If needed a proxy can be defined here. In this example this field will be left blank.

2.2.6 Archive mirror configuration

If needed a different archive mirror can be selected. This example will use the default one.

2.2.7 Storage configuration

Here the previously defined storage should be shown. In this example the entire disk will be used for the VM. Confirm the selection two times to start writing to the disk.

2.2.8 Profile setup

Enter your preferred login credentials and give your vm a name. In this example it will be named virtualmachine1.

2.2.9 SSH setup

As we need a ssh daemon on this vm we will install the openssh server here, although we will not import any ssh identities.

2.2.10 Server snaps

If needed special services can simply be installed from here. This example will not need any.

2.2.11 Installation

Wait for the installation to finish and then reboot.

2.3 Ubuntu server installation on VM2

Follow subsection 2.2 a second time with some minor differences:

- subsubsection 2.2.4: use address 192.168.1.92/24.
- subsubsection 2.2.8: Change login credentials accordingly and change the servers name to virtualmachine2.
- subsubsection 2.2.9: Skip this as we only need an ssh daemon on one VM.

3 SSH Daemon configuration auf VM1

The open ssh server must be configured to listen on port 41500, allow only unpriviliged users and to use only public key authentication.

After logging in with a sudo user (user with access to root actions) open the config file with the command (enter the password if prompted):

```
sudo nano /etc/ssh/sshd_config
```

3.1 Port Configuration

Change following line to change the listening port of the ssh server.

```
#Port 22
```

to

```
Port 41500
```

In order to reflect the changes the server must be restarted with the command:

```
sudo service ssh restart
```

3.2 User access configuration

Change following line to allow only unpriviliged users to access to the server.

```
#PermitRootLogin prohibit-password
```

to

```
PermitRootLogin no
```

In order to reflect the changes the server must be restarted with the command:

```
sudo service ssh restart
```

3.3 Enable only public key authentication

Change following line to disallow password authentication in favour of public key authentication for the ssh server.

```
#PasswordAuthentication yes
```

to

```
PasswordAuthentication no
```

and

```
#PubkeyAuthentication yes
```

to

```
PubkeyAuthentication yes
```

In order to reflect the changes the server must be restarted with the command:

```
sudo service ssh restart
```

4 NGINX Setup

Example text

5 VPN Setup

Example text

6 Firewall Setup

Example text