

# **VPS PROXMOX**

# Job 1 : Membangun Infrastruktur Cloud

Anda bekerja sebagai Cloud Engineer di PT EduCloud Nusantara. Client meminta Anda membangun infrastruktur cloud untuk 2 layanan Web

## ANALISIS DAN PERANCANGAN INFRASTRUKTUR CLOUD

### 1. Ringkasan

Berdasarkan permintaan client untuk membangun infrastruktur cloud bagi layanan web. Infrastruktur akan dibangun menggunakan dua server virtual berbasis VM di atas hypervisor Proxmox. Untuk efisiensi dan konsistensi konfigurasi, deployment akan menggunakan metode **cloud-init**. Jaringan dirancang dengan model hibrida dimana server menggunakan IP Private untuk keamanan dan komunikasi internal, serta diakses dari publik melalui mekanisme NAT (Network Address Translation) dari IP Publik yang tersedia.

### 2. Analisis Kebutuhan dan Lingkungan

#### 2.1. Inventarisasi Perangkat

Berdasarkan data yang diberikan, lingkungan yang tersedia adalah:

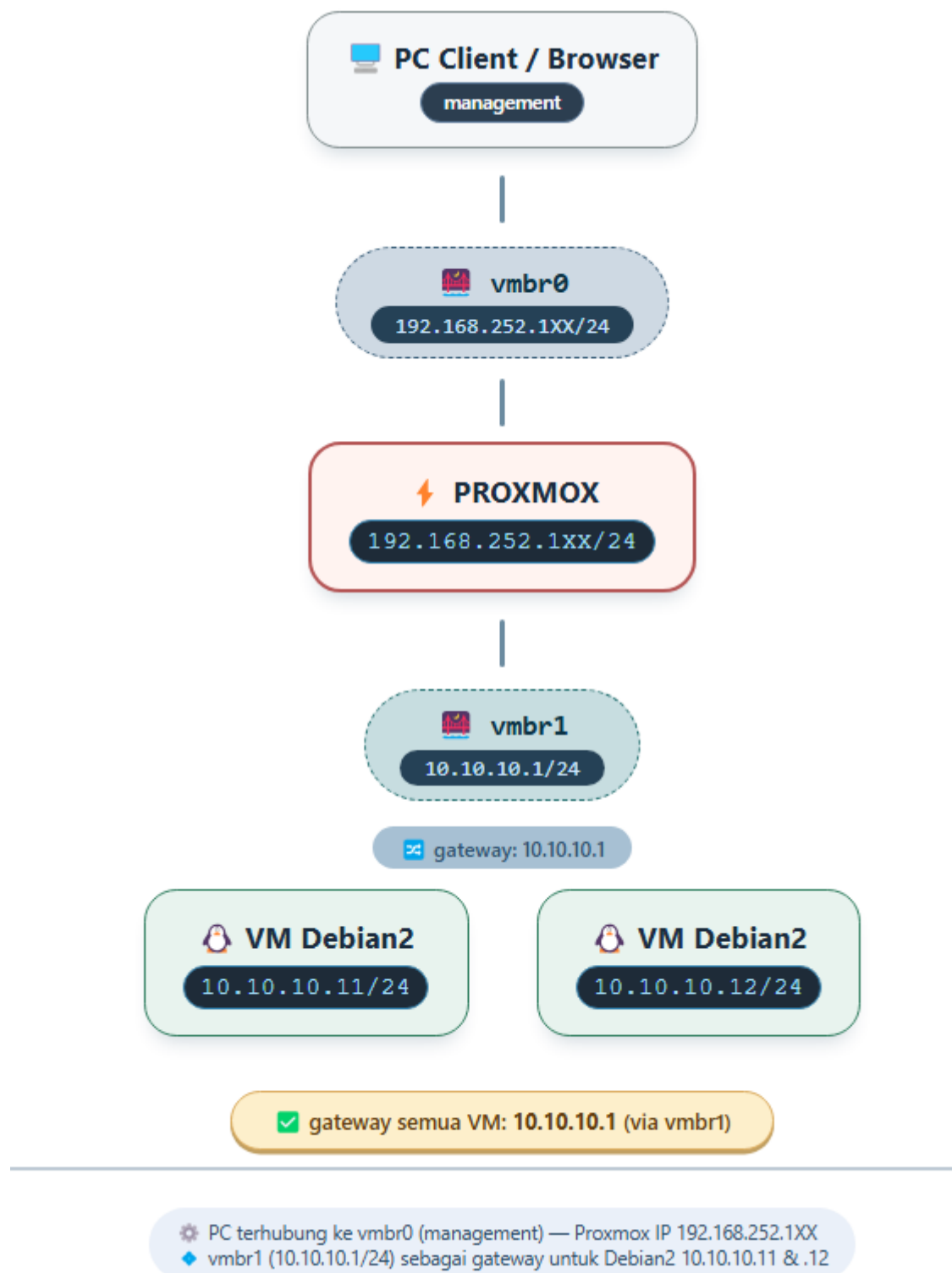
- **1 Unit PC Server:** Berfungsi sebagai host untuk hypervisor.
- **Hypervisor:** Proxmox VE (Virtual Environment).
- **Konektivitas Jaringan:**
  - **1 IP Publik:** IP ini statis dan dapat diakses dari internet (contoh: 192.168.252.1XX/24).
  - **Jaringan Private:** Jaringan internal yang akan digunakan untuk komunikasi antar VM.

#### 2.2. Identifikasi Masalah

Masalah utama yang perlu dipecahkan adalah bagaimana menghubungkan infrastruktur private (2 VM dengan IP Private) dengan aksesibilitas publik (user dari internet), dengan keterbatasan hanya memiliki 1 alamat IP Publik.

### 3. Desain Solusi Infrastruktur

#### 3.1. Topologi Jaringan



Untuk mengakomodasi keterbatasan IP Publik, akan diterapkan konsep **Port Forwarding (DNAT)** . Arsitektur jaringannya adalah sebagai berikut:

1. **Interface Publik (Bridge):** Proxmox akan menggunakan bridge, vmbr0, yang terhubung langsung ke jaringan publik. IP Publik akan dikonfigurasi pada interface Proxmox ini.
2. **Interface Private (Bridge):** Akan dibuat bridge kedua, vmbr1, yang berfungsi sebagai jaringan private (Contoh subnet: 10.10.10.0/24). Semua VM akan terhubung ke bridge private ini.
3. **Gateway dan Firewall:** Proxmox akan difungsikan sebagai router sederhana dan gateway bagi VM-VM. Fitur firewall dan NAT pada Proxmox akan diaktifkan untuk meneruskan lalu lintas dari publik ke VM private.

### 3.2. Skema Pengalamatan

- **Proxmox Host:**
  - IP Publik: 192.168.252.1XX (contoh)
  - IP Private (di vmbr1): 10.10.10.1/24 (bertindak sebagai gateway)
- **VM 1 (Debian1):**
  - Hostname: web-a
  - IP Private: 10.10.10.11/24
  - Gateway: 10.10.10..1
- **VM 2 (Debian2):**
  - Hostname: web-b
  - IP Private: 10.10.10.12/24
  - Gateway: 10.10.10..1
- **User (Dari Internet):** Mengakses IP Publik 192.168.252.1XX.

**Keterangan : XX adalah nomor urut siswa**

### 3.3. Mekanisme Akses (Port Forwarding)

Untuk mengarahkan user ke server yang tepat, akan dikonfigurasi aturan port forwarding pada firewall Proxmox. Karena hanya ada satu IP publik, pendekatan yang digunakan adalah membedakan berdasarkan port.

- **Contoh Aturan:**

- o Lalu lintas HTTP ke IP Publik (port 8011) akan diteruskan ke VM 1 (10.10.10.11:80).
- o Lalu lintas HTTP ke IP Publik (port 8012) akan diteruskan ke VM 2 (10.10.10.12:80).
- o Lalu lintas SSH ke IP Publik (port 2211) akan diteruskan ke VM 1 (10.10.10.11:22).
- o Lalu lintas SSH ke IP Publik (port 2212) akan diteruskan ke VM 2 (10.10.10.12:22).

## Langkah Kerja

**Tabel 1 - Setting Network VirtualBox sebagai berikut :**

| Node    | VirtualBox Interface | VirtualBox Network Type | Name |
|---------|----------------------|-------------------------|------|
| Proxmox | Adapter 1            | Bridge                  | -    |

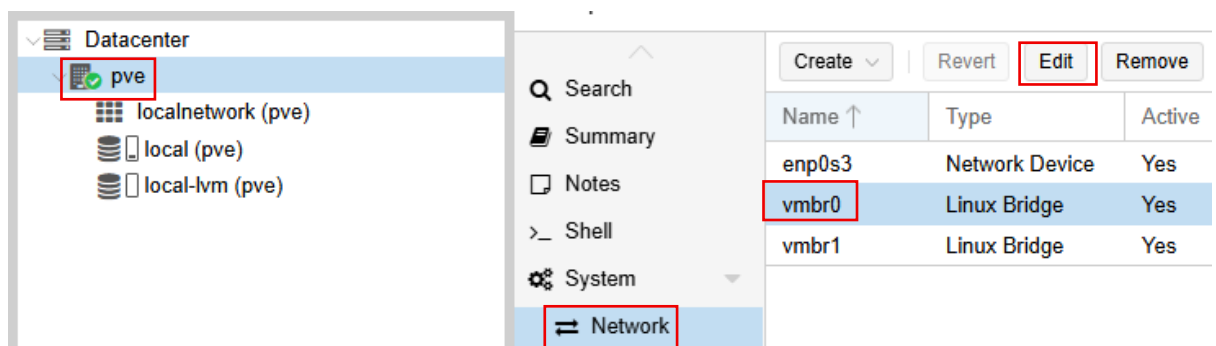
**Tabel 2 - Setting Network Proxmox sebagai berikut :**

| Bridge | IP Address         | Gateway         | DNS Server      |
|--------|--------------------|-----------------|-----------------|
| vmbr0  | 192.168.252.1XX/24 | 192.168.252.254 | 192.168.252.254 |
| Vmbr1  | 10.10.10.1/24      | -               | -               |

## 4. Setting Network di Proxmox

### 4.1. Konfigurasi IP Address di Proxmox (vmbr0)

1. Konfigurasi IP Address : Pilih **pve** => **Network** => **vmbr0** , Kemudian pilih **Edit**



**Edit: Linux Bridge**

|                 |                    |               |                                     |
|-----------------|--------------------|---------------|-------------------------------------|
| Name:           | vmbr0              | Autostart:    | <input checked="" type="checkbox"/> |
| IPv4/CIDR:      | 192.168.252.153/24 | VLAN aware:   | <input type="checkbox"/>            |
| Gateway (IPv4): | 192.168.252.254    | Bridge ports: | enp0s3                              |
| IPv6/CIDR:      |                    | Comment:      |                                     |
| Gateway (IPv6): |                    |               |                                     |

Advanced ☐ **OK**

Isi seperti gambar diatas, kemudian klik **OK**, kalau sudah sesuai klik **CLOSE**

## 2. Konfigurasi DNS : Pilih pve => DNS => Edit

Datacenter

- pve**
  - localnetwork (pve)
  - local (pve)
  - local-lvm (pve)

Search

Summary

Notes

Shell

System

Network

Certificates

**DNS**

**Edit**

|               |                 |
|---------------|-----------------|
| Search domain | example.net     |
| DNS server 1  | 192.168.252.254 |

**Edit: DNS**

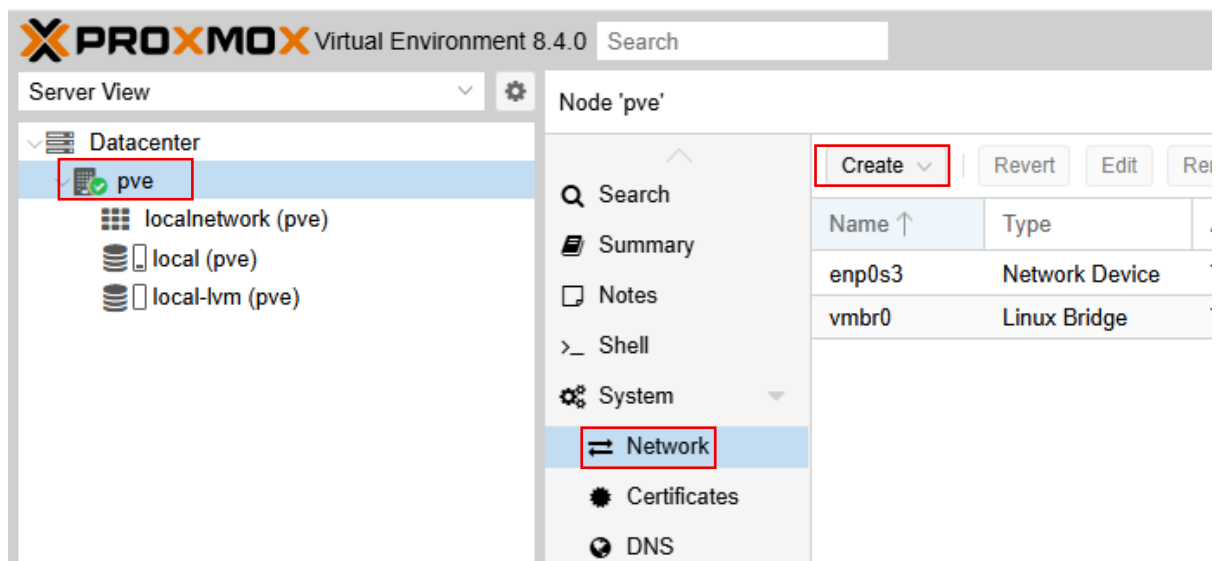
|                |                 |
|----------------|-----------------|
| Search domain: | example.net     |
| DNS server 1:  | 192.168.252.254 |
| DNS server 2:  |                 |
| DNS server 3:  |                 |

**OK**

Isi **DNS server 1** seperti gambar diatas, kemudian klik **OK**, kalau sudah sesuai klik **CLOSE**

## 4.2. Menambah vmbr1 bridge

1. Pilih pve => Network => Create, Kemudian pilih Linux Bridge



2. Isi IP Address untuk **vmbr1**, **10.10.10.1/24**, kemudian klik **Create**

Create: Linux Bridge

Name: **vmbr1** Autostart: ☒

IPv4/CIDR: **10.10.10.1/24** VLAN aware: ☐

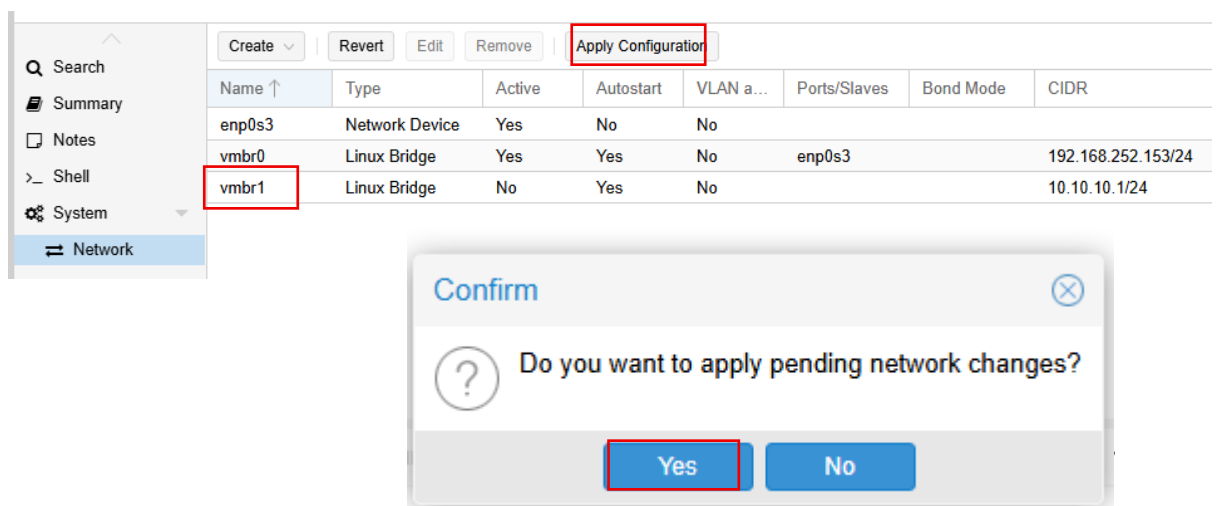
Gateway (IPv4): Bridge ports:

IPv6/CIDR: Comment:

Gateway (IPv6):

Help Advanced **Create**

3. Setelah muncul **vmbr1**, klik **Apply Configuration**, untuk mengaktifkan vmbr1. Setelah itu muncul kotak Konfirmasi (Confirm), kemudian klik **Yes**



## 5. Membuat Template VM Debian – Proxmox Cloud Init

cloud-init adalah mekanisme otomatisasi konfigurasi awal VM saat pertama kali dinyalakan (first boot). Dengan cloud-init, kita tidak perlu konfigurasi manual satu-satu (hostname, IP, user, SSH, dll).

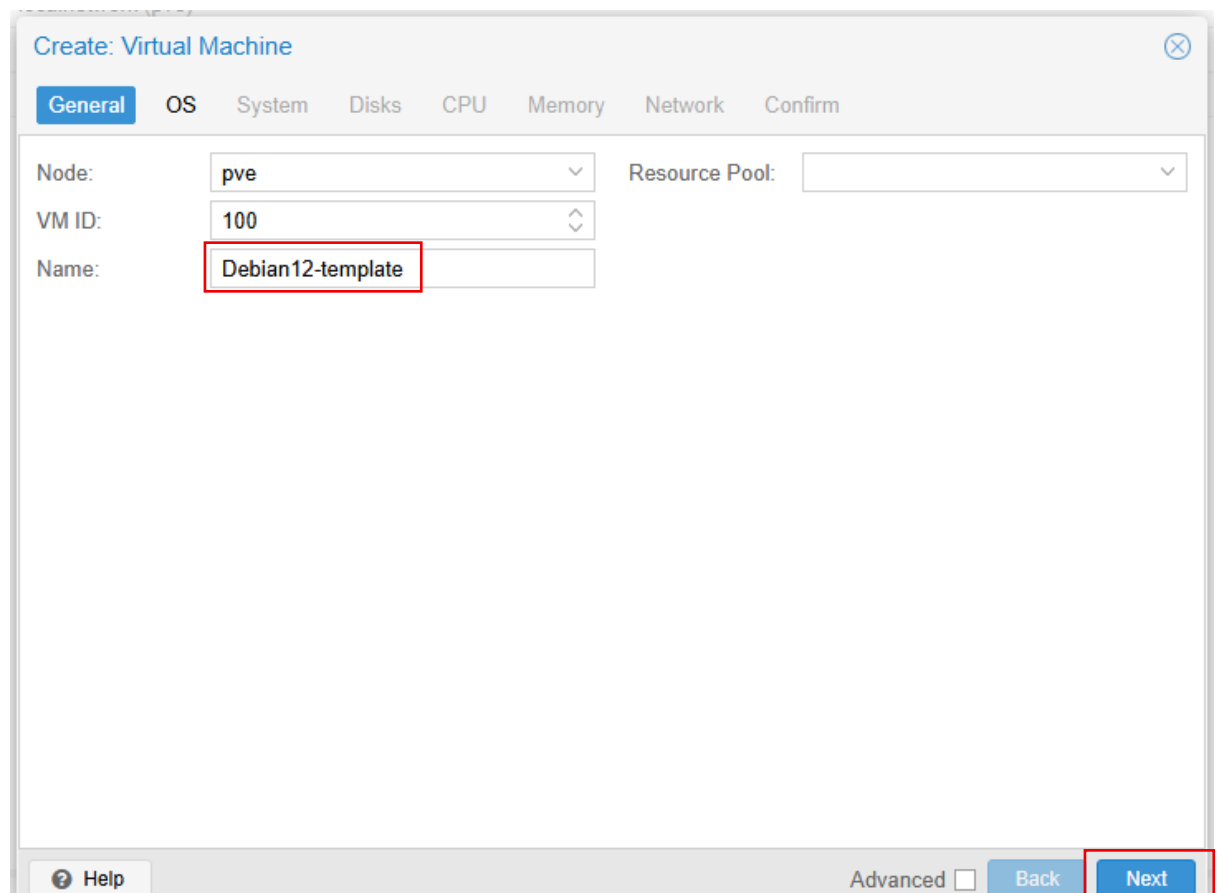
Dipakai luas di cloud & data center (AWS, OpenStack, Proxmox, dll).

### 5.1 Instalasi dan Konfigurasi

#### 1. Membuat Template Debian

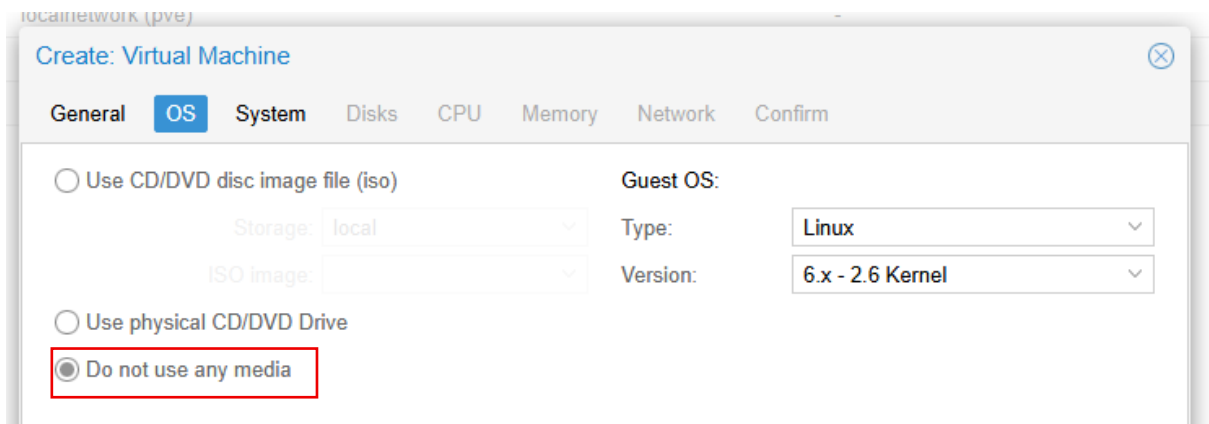
##### Create VM

Pada pojok kanan atas web klik **Create VM**, lalu masukan **VM Name (Debian12-template)** yang akan digunakan. Catat dan ingat VM ID karena akan kita gunakan di step-step selanjutnya. Kemudian klik **Next**



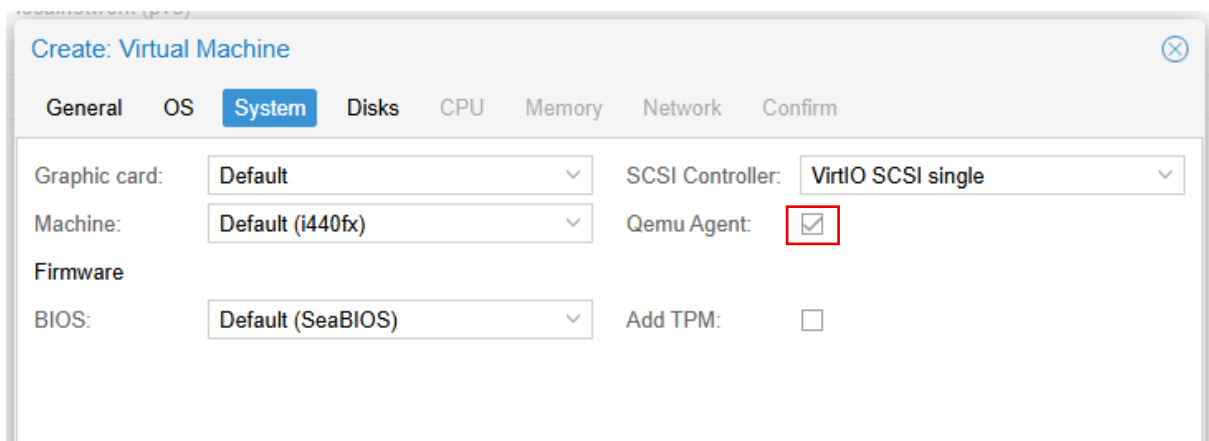
## Operation System:

Pada bagian OS pastikan Anda memilih **“Do not use any media”** karena kita akan menambahkan storagenya nanti dengan beberapa konfigurasi tambahan.



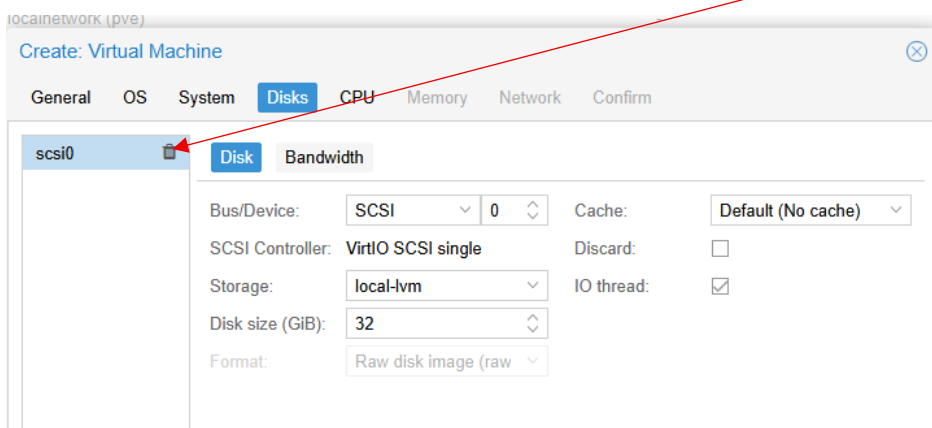
## System:

Dibagian system biarkan semua opsi default, kecuali bagian Qemu Agent, pastikan Anda mengaktifkannya.



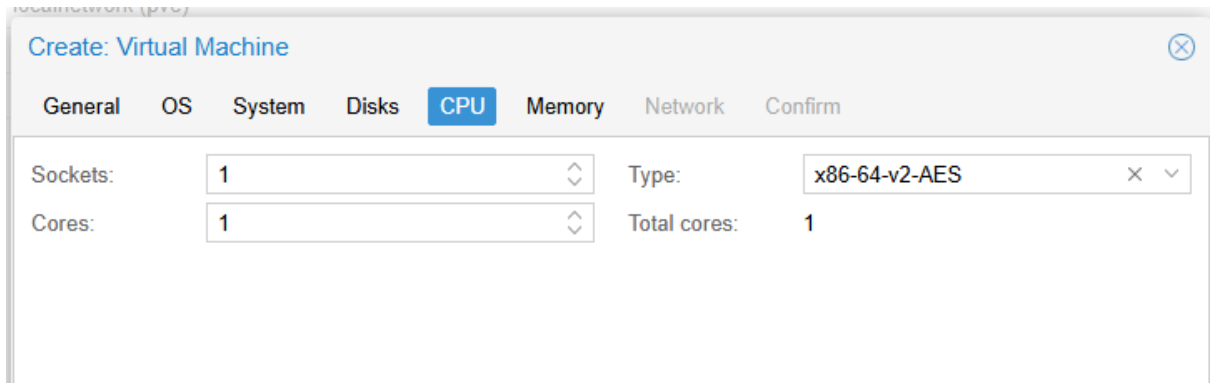
## Disk :

Selanjutnya pada bagian Disk pastikan menghapusnya dengan klik icon Trash, setelah di klik tampilan menjadi kosong, kemudian klik **Next**



### CPU:

Pada form ini kita menentukan jumlah core prosesor yang akan dialokasikan untuk menjalankan VM yang akan dibuat. Karena tidak ada yang perlu diubah jadi bisa langsung **Next** saja.

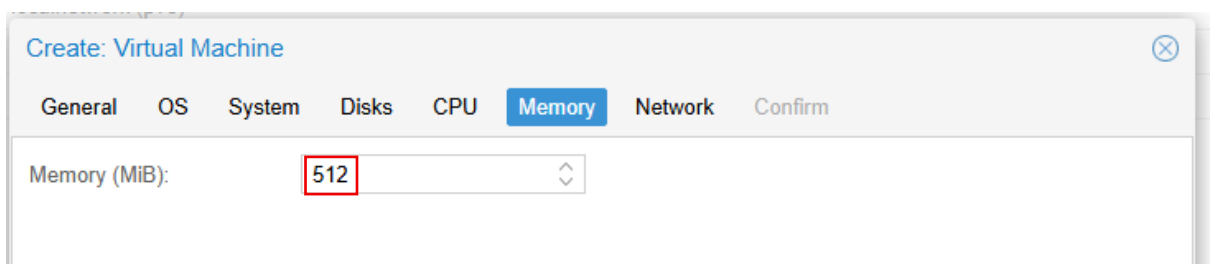


The screenshot shows the 'Create: Virtual Machine' dialog box with the 'CPU' tab selected. The 'Sockets' field is set to 1, and the 'Cores' field is set to 1. The 'Type' dropdown is set to 'x86-64-v2-AES'. The 'Total cores' is displayed as 1.

| Field       | Value         |
|-------------|---------------|
| Sockets     | 1             |
| Cores       | 1             |
| Type        | x86-64-v2-AES |
| Total cores | 1             |

### Memory:

Pada form ini kita menentukan jumlah memori (RAM) yang akan dialokasikan untuk menjalankan VM yang akan dibuat

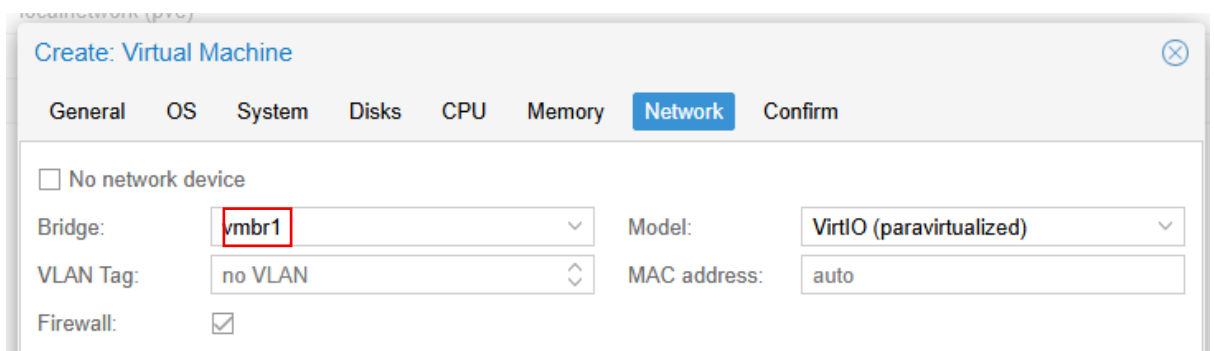


The screenshot shows the 'Create: Virtual Machine' dialog box with the 'Memory' tab selected. The 'Memory (MiB)' field is set to 512.

| Field        | Value |
|--------------|-------|
| Memory (MiB) | 512   |

### Network:

Pada form ini kita menentukan model koneksi jaringan VM dengan lingkungan sekitar, apakah bridge atau yang lainnya, pilih **vmbr1** (sesuai dengan perencanaan dan topologi, vm di koneksikan ke **vmbr1**)

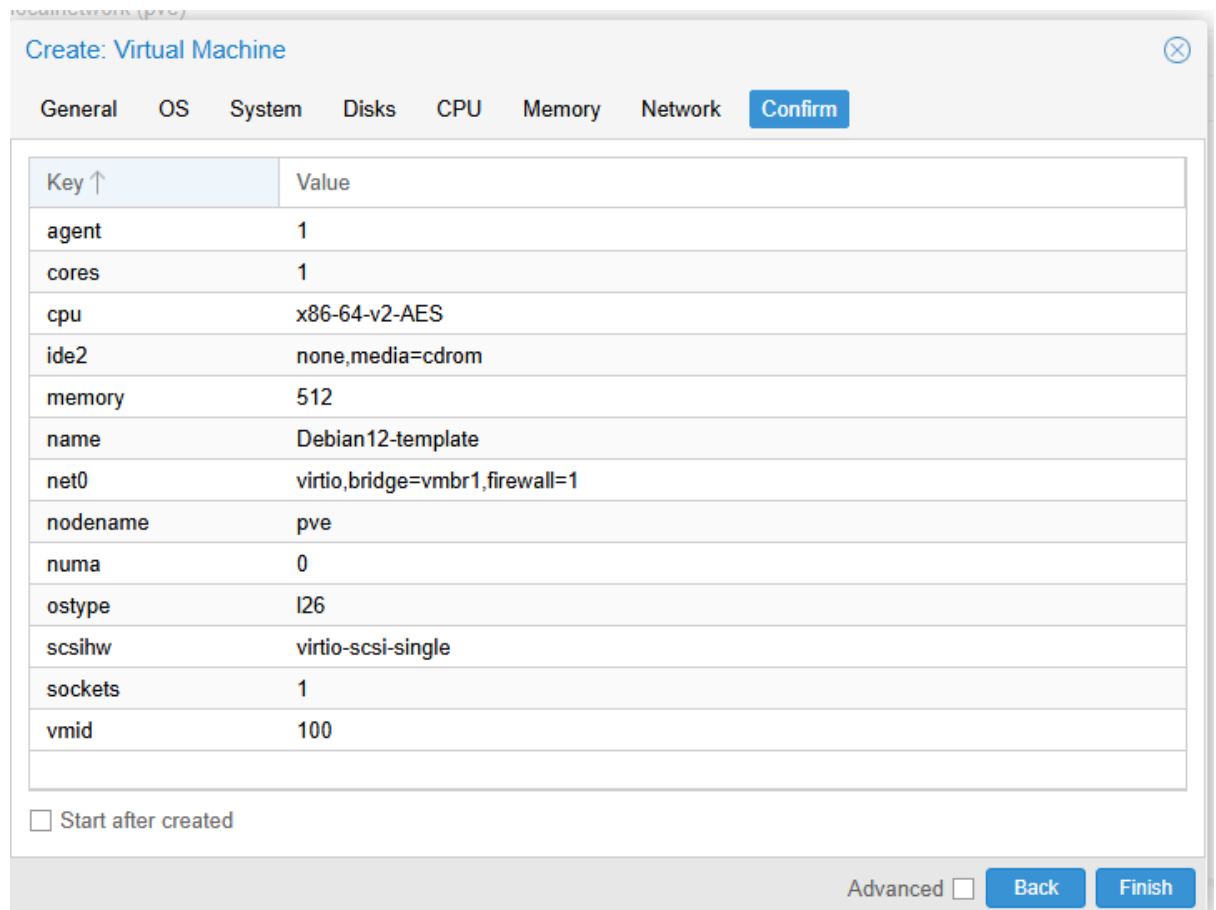


The screenshot shows the 'Create: Virtual Machine' dialog box with the 'Network' tab selected. The 'Bridge' dropdown is set to 'vmbr1'. The 'Model' dropdown is set to 'VirtIO (paravirtualized)'. The 'VLAN Tag' dropdown is set to 'no VLAN'. The 'MAC address' dropdown is set to 'auto'. The 'Firewall' checkbox is checked.

| Field       | Value                               |
|-------------|-------------------------------------|
| Bridge      | vmbr1                               |
| Model       | VirtIO (paravirtualized)            |
| VLAN Tag    | no VLAN                             |
| MAC address | auto                                |
| Firewall    | <input checked="" type="checkbox"/> |

## Confirm:

Pada form ini kita dapat mereview parameterparameter yang telah ditentukan sebelum proses pembuatan VM dilakukan. Setelah semua yakin parameterparameter sudah sesuai dengan yang kita inginkan, maka klik tombol **“Finish”**



**Create: Virtual Machine**

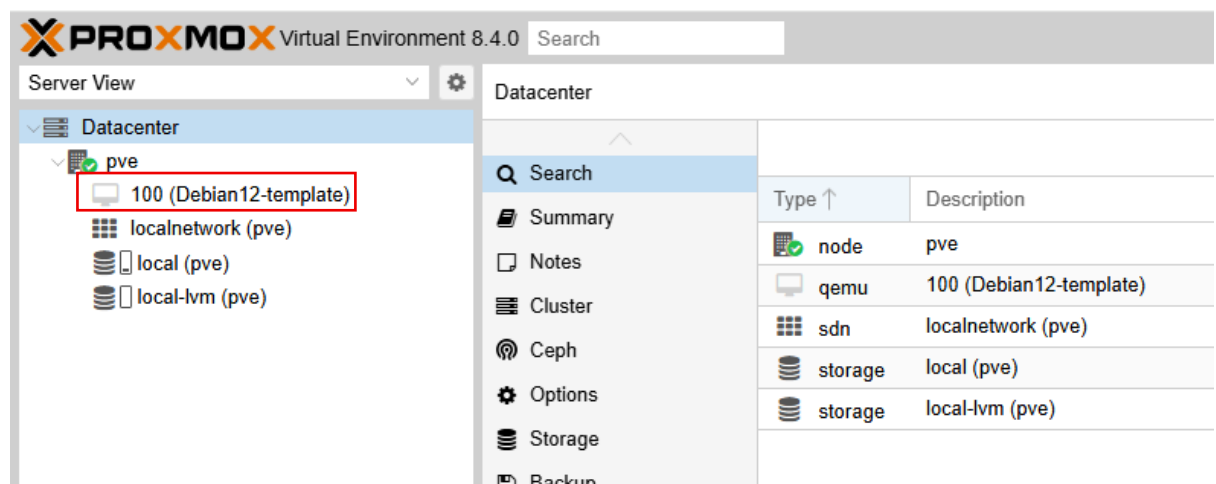
General OS System Disks CPU Memory Network **Confirm**

| Key ↑    | Value                          |
|----------|--------------------------------|
| agent    | 1                              |
| cores    | 1                              |
| cpu      | x86-64-v2-AES                  |
| ide2     | none,media=cdrom               |
| memory   | 512                            |
| name     | Debian12-template              |
| net0     | virtio,bridge=vmbr1,firewall=1 |
| nodename | pve                            |
| numa     | 0                              |
| ostype   | l26                            |
| scsihw   | virtio-scsi-single             |
| sockets  | 1                              |
| vmid     | 100                            |

☐ Start after created

Advanced ☐ **Back** **Finish**

## Tampilan setelah Finish



**PROXMOX** Virtual Environment 8.4.0 Search

Server View

**Datacenter**

- ▼ Datacenter
  - ▼ pve
    - 100 (Debian12-template)**
    - localnetwork (pve)
    - local (pve)
    - local-lvm (pve)

**Datacenter**

- Search
- Summary
- Notes
- Cluster
- Ceph
- Options
- Storage
- Backup

| Type ↑  | Description             |
|---------|-------------------------|
| node    | pve                     |
| qemu    | 100 (Debian12-template) |
| sdn     | localnetwork (pve)      |
| storage | local (pve)             |
| storage | local-lvm (pve)         |

## Storage:

Untuk membuat storage dan memilih image yang akan digunakan, silakan buka terminal Proxmox, kemudian jalankan beberapa command berikut:

Download image [debian-12-generic-amd64.qcow2](http://192.168.252.252/proxmox/debian-12-generic-amd64.qcow2) di alamat 192.168.252.252/proxmox

```
root@pve:~#  
root@pve:~# wget http://192.168.252.252/proxmox/debian-12-generic-amd64.qcow2  
  
--2026-02-22 14:51:28-- http://192.168.252.252/proxmox/debian-12-generic-amd64.qcow2  
Connecting to 192.168.252.252:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 446480384 (426M)  
Saving to: 'debian-12-generic-amd64.qcow2'  
  
debian-12-generic-amd64.qcow2 100%[=====]  
2026-02-22 14:51:29 (367 MB/s) - 'debian-12-generic-amd64.qcow2' saved [446480384/446480384]  
root@pve:~#
```

mengonfigurasi Mesin Virtual (VM) dengan ID 100 agar menggunakan konsol serial (Serial Terminal) sebagai output VGA/tampilan utamanya

```
root@pve:~#  
root@pve:~# qm set 100 --serial0 socket --vga serial0  
  
root@pve:~# qm set 100 --serial0 socket --vga serial0  
update VM 100: -serial0 socket -vga serial0
```

## Keterangan :

- **qm set 100:** Mengubah konfigurasi VM dengan nomor ID 100 (QM adalah singkatan dari QEMU Manager).
- **--serial0 socket** → menambahkan serial console
- **--vga serial0** → mengalihkan tampilan ke serial console

## Tujuan :

1. **Mengakses Konsol via CLI:** Memungkinkan akses login ke VM melalui terminal Proxmox (qm terminal 100) jika akses jaringan terputus atau VNC tidak tersedia.

2. **Cloud-Init / Template:** Sering digunakan saat menyiapkan *image* cloud-init (seperti Ubuntu / Debian Cloud Image) agar konsol bisa diakses dengan baik sebelum jaringan dikonfigurasi.

### Resize disk ( menentukan ukuran disk) menjadi 30 GB

```
root@pve:~#  
root@pve:~# qemu-img resize debian-12-generic-amd64.qcow2 30G  
Image resized.
```

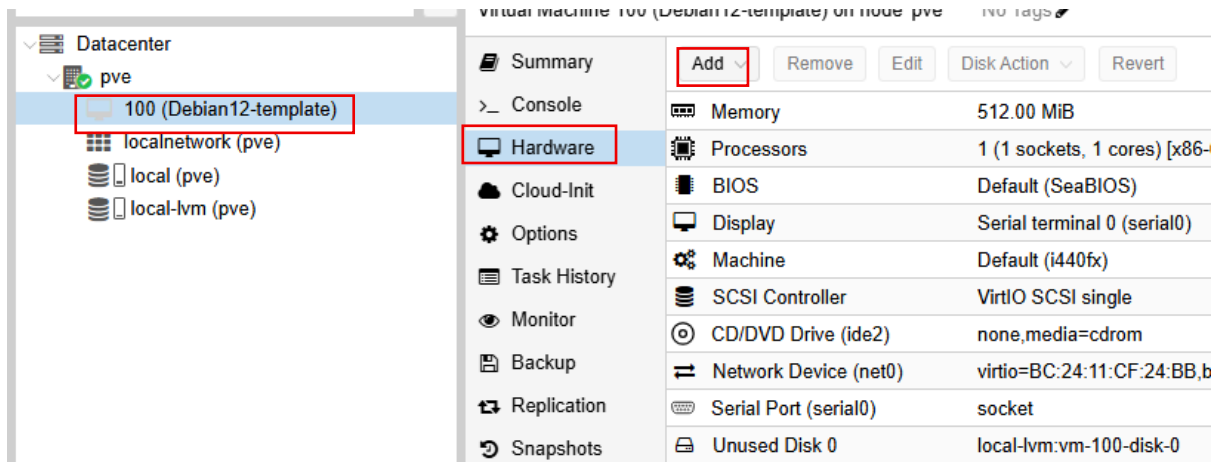
### Import disk

```
root@pve:~#  
root@pve:~# qm importdisk 100 debian-12-generic-amd64.qcow2 local-lvm
```

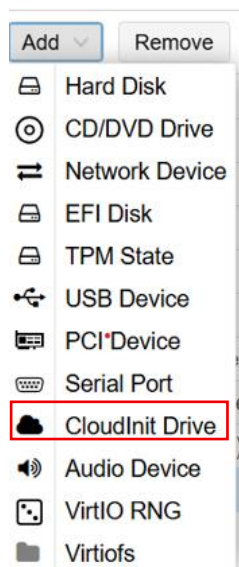
```
transferred 25.8 GiB of 30.0 GiB (85.99%)  
transferred 25.9 GiB of 30.0 GiB (86.35%)  
transferred 26.2 GiB of 30.0 GiB (87.36%)  
transferred 26.5 GiB of 30.0 GiB (88.36%)  
transferred 26.8 GiB of 30.0 GiB (89.37%)  
transferred 27.1 GiB of 30.0 GiB (90.37%)  
transferred 27.4 GiB of 30.0 GiB (91.37%)  
transferred 27.7 GiB of 30.0 GiB (92.38%)  
transferred 28.0 GiB of 30.0 GiB (93.39%)  
transferred 28.3 GiB of 30.0 GiB (94.40%)  
transferred 28.6 GiB of 30.0 GiB (95.45%)  
transferred 28.9 GiB of 30.0 GiB (96.45%)  
transferred 29.2 GiB of 30.0 GiB (97.46%)  
transferred 29.5 GiB of 30.0 GiB (98.46%)  
transferred 29.8 GiB of 30.0 GiB (99.47%)  
transferred 30.0 GiB of 30.0 GiB (100.00%)  
transferred 30.0 GiB of 30.0 GiB (100.00%)  
unused0: successfully imported disk 'local-lvm:vm-100-disk-0'  
root@pve:~#
```

## Hardware:

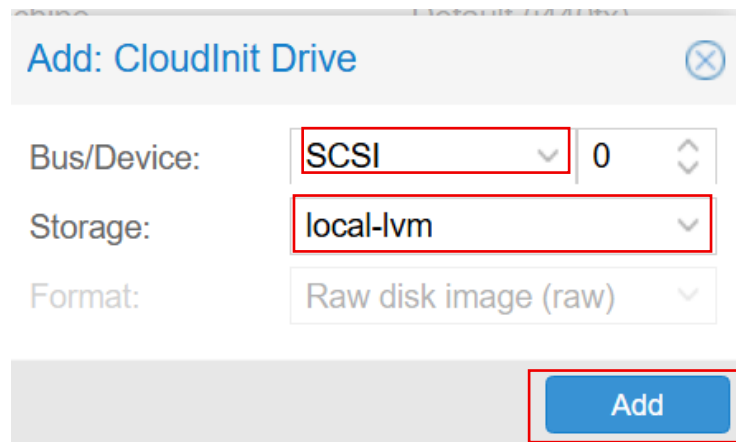
Setelah berhasil melakukan import disk, buka kembali Proxmox GUI **klik 100(Debian12-template) => Klik Hardware => Klik Add**



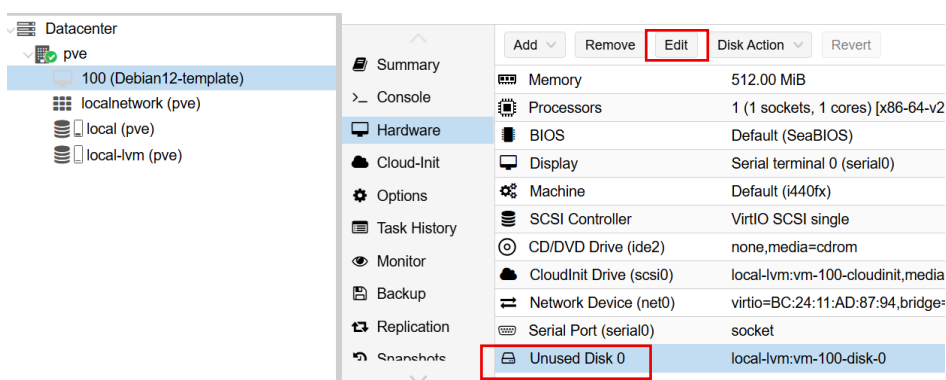
Kemudian pilih



**Bus/Device : scsi => Storage:local-lvm => Klik Add**



Langkah berikutnya klik **Unused Disk 0 => Klik Edit**



Setelah di klik **Edit** akan muncul tampilan sebagai berikut, kemudian ceklist **Discard**  
=> klik **Add**

**Add: Unused Disk**

**Disk** | Bandwidth

Bus/Device: SCSI | 1 | Cache: Default (No cache)

SCSI Controller: VirtIO SCSI single | Discard: ☒

Disk image: local-lvm:vm-100-disk-0 | IO thread: ☒

Help | Advanced ☐ | **Add**

Langkah berikutnya mengubah Boot Order, klik **Options** > **Klik Boot Order** > **Klik Edit**

**Options**

**Edit** | Revert

|                             |               |
|-----------------------------|---------------|
| Name                        | Debian12-te   |
| Start at boot               | No            |
| Start/Shutdown order        | order=any     |
| OS Type                     | Linux 6.x - 2 |
| <b>Boot Order</b>           | ide2, net0    |
| Use tablet for pointer      | Yes           |
| Hotplug                     | Disk, Netwo   |
| ACPI support                | Yes           |
| KVM hardware virtualization | Yes           |
| Freeze CPU at startup       | No            |

Langkah selanjutnya ceklist **scsi1**, kemudian klik **Ok**

**Edit: Boot Order**

| # | Enabled                             | Device | Description                                      |
|---|-------------------------------------|--------|--------------------------------------------------|
| 1 | <input type="checkbox"/>            | ide2   | none,media=cdrom                                 |
| 2 | <input type="checkbox"/>            | net0   | virtio=BC:24:11:AD:87:94,bridge=vmbri,firewall=1 |
| 3 | <input checked="" type="checkbox"/> | scsi1  | local-lvm:vm-100-disk-0,iosthread=1,size=30G     |

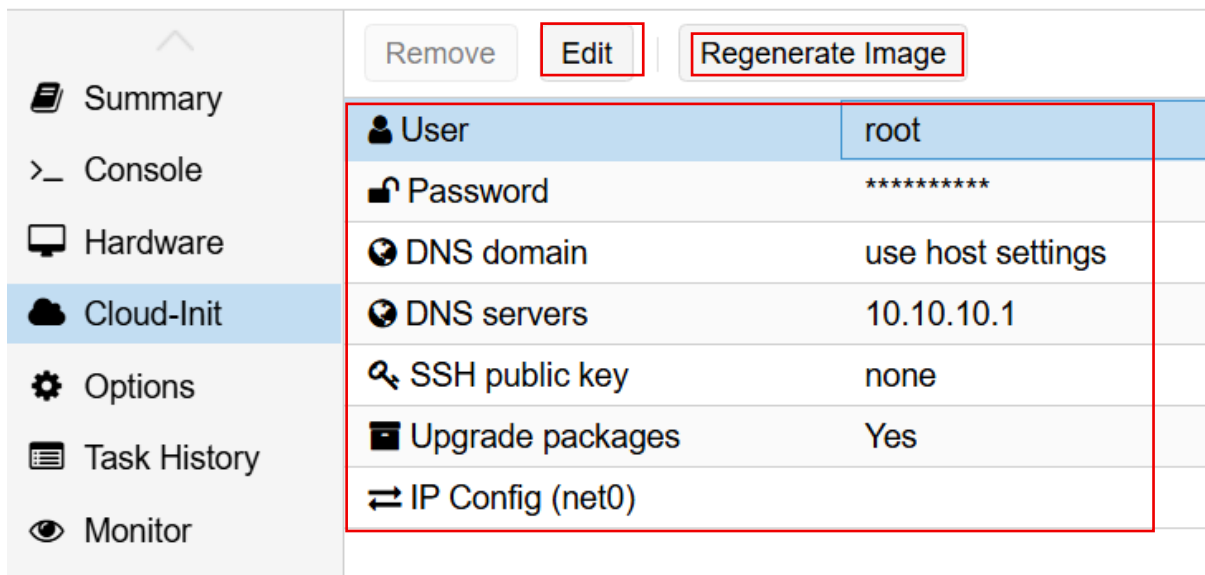
Drag and drop to reorder

Help | **OK**

### Cloud-Init:

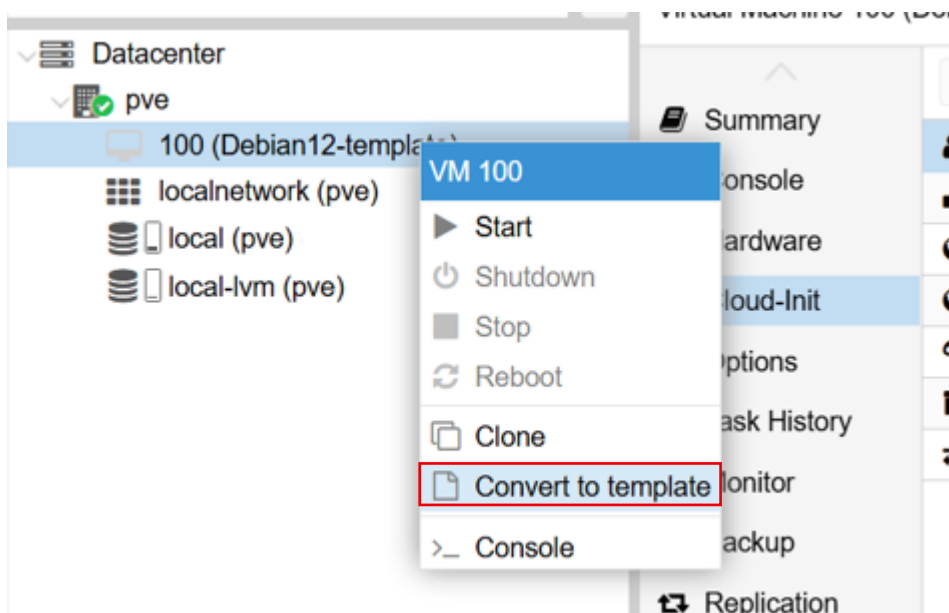
Selanjutnya masuk ke tab **Cloud-Init** dan **edit** User, Password, DNS Servers dan klik **Regenerate Image**.

|             |            |
|-------------|------------|
| User        | root       |
| Password    | 123456     |
| DNS Servers | 10.10.10.1 |



### Convert VM ke Template:

Jika semua langkah-langkah diatas telah berhasil di jalankan, maka VM sudah siap untuk di convert menjadi Template. Klik kanan pada VM **100 (Debian12-template)** dan pilih **Convert to template**.

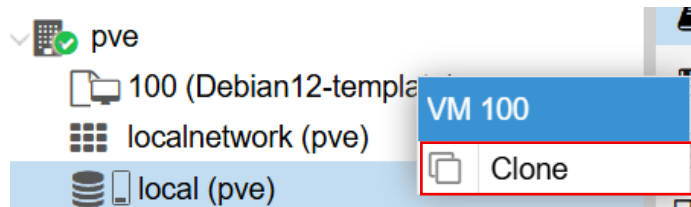


## Membuat VM dari Template Debian 12

Untuk membuat instance virtual (VM) dari template di Proxmox VE, dapat mengikuti langkah-langkah berikut:

### Buat VM dari Template:

Di Proxmox Web GUI, klik kanan VM **100 (Debian12-template)** dan pilih **Clone**



kemudian isikan VM ID dan Name. Pada bagian Mode pastikan memilih Full Clone dan klik **Clone**.

|       |            |
|-------|------------|
| VM ID | 101        |
| Name  | debian1    |
| Mode  | Full Clone |

### Clone VM Template 100

Target node: pve

VM ID: 101

Name: debian1

Resource Pool:

Mode: Full Clone

Target Storage: Same as source

Format: QEMU image format (qc

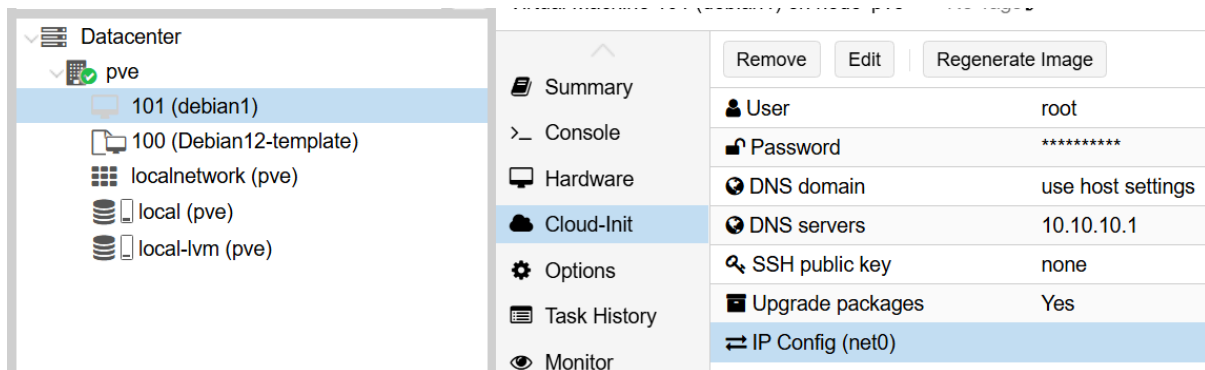
Help

Clone

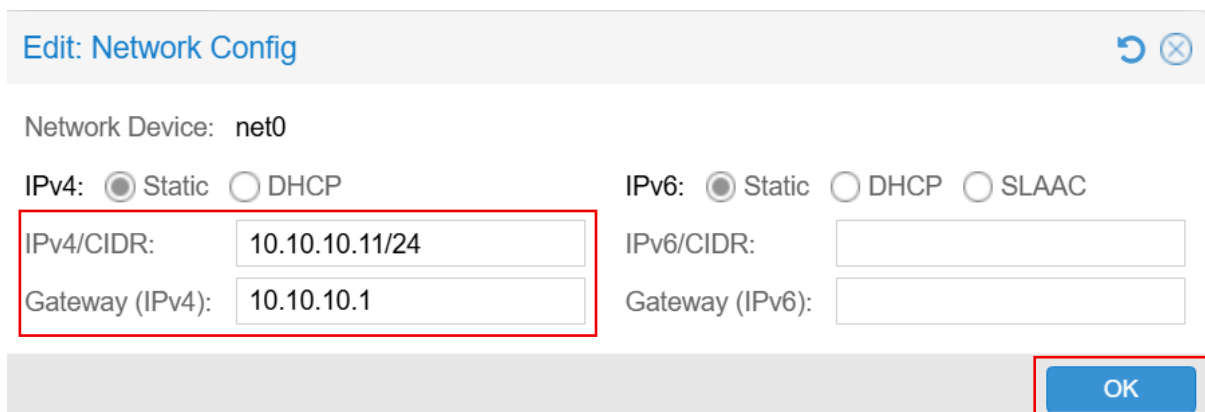
Sampai saat ini kita telah berhasil membuat 1 VM Debian dengan cara mengkloning dari Debian12-template. Langkah berikutnya adalah konfigurasi IP Address di Debian1, sesuai perencanaan dan topologi IP Adressnya adalah sebagai berikut :

| Debian1     |                |
|-------------|----------------|
| IP Address  | 10.10.10.11/24 |
| Gateway     | 10.10.10.1     |
| DNS Servers | 10.10.10.1     |

Untuk konfigurasi langkahnya sebagai berikut : Klik **101(debian1)** => pilih **Cloud-Init** => **IP Config (net0)** => klik **Edit**



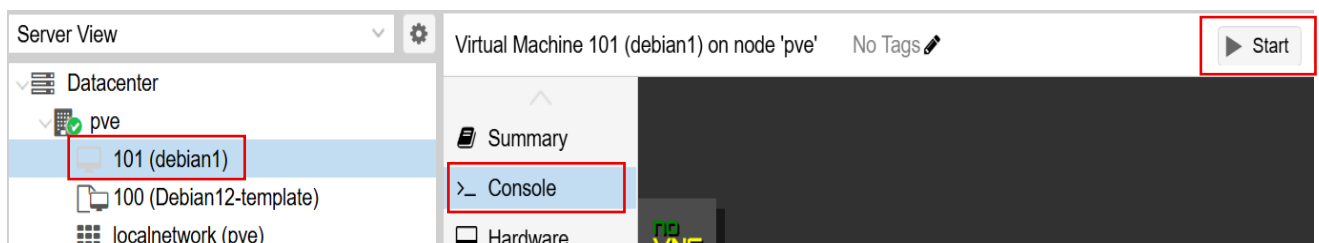
Setelah klik **Edit** akan muncul tampilan sebagai berikut, isikan IP Address sesuai dengan ketentuan diatas, kemudian klik **OK**

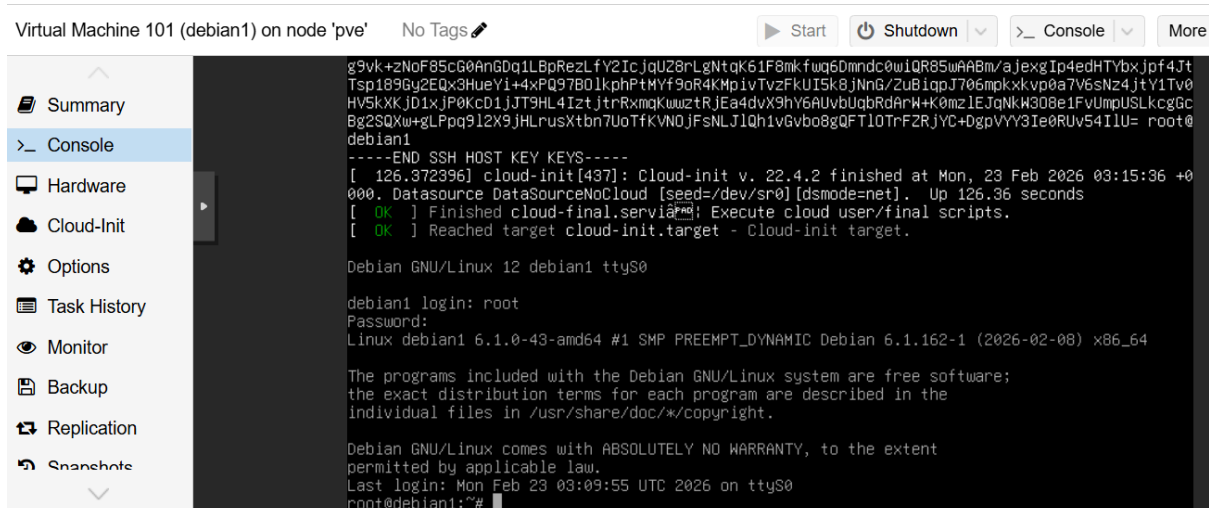


Untuk DNS Servers tidak perlu di isi, karena sudah di isi ketika membuat debian12-template.

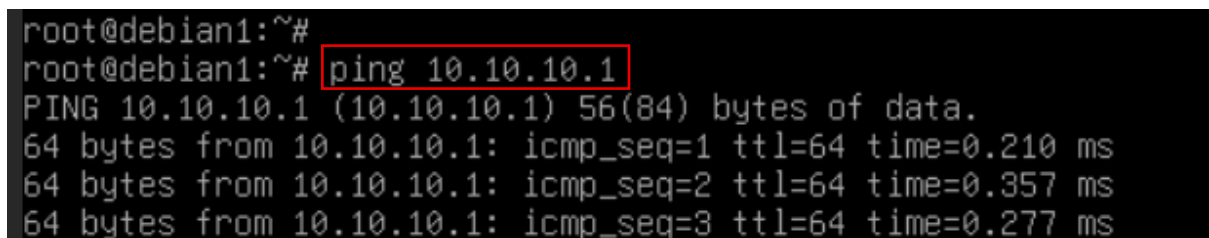
### Akses VM:

Setelah berhasil clone VM dari Templates, klik ke **VM 101 (debian1)** dan akses tab **Console**, kemudian **start** VM dan login dengan user dan password yang sudah dibuat di Cloud-Init sebelumnya.





Kalau **Console** sudah terbuka, uji koneksi ke 10.10.10.1 (vmbri) dari **VM 101 (debian1)**



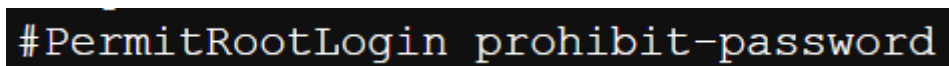
**Konfigurasi SSH supaya dapat diakses dengan user dan password dari Client**

1. Masuk ke **Console 101(debian1)**
2. Buka file **/etc/ssh/sshd\_config**

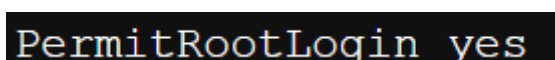


3. Cari baris **#PermitRootLogin prohibit-password** ubah menjadi **PermitRootLogin yes** dan hilangkan tanda # didepanya.

Sebelum



Sesudah



4. Memberikan tanda pagar di depan baris **PasswordAuthentication no**

```
# To disable tunneled clear text
#PasswordAuthentication no
#PermitEmptyPasswords no
```

5. Setelah selesai di konfigurasi simpan, kemudian restart **SSH**

```
root@debian1:~# /etc/init.d/ssh restart
Restarting ssh (via systemctl): ssh.service.
root@debian1:~#
```

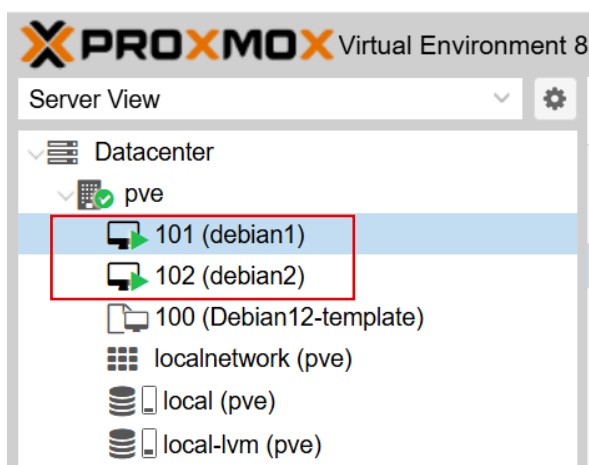
## VM DEBIAN

Tugas berikutnya Adalah membuat **VM Debian2** dengan mengkloning dari **debian12-template**, caranya sama dengan cara membuat **VM Debian1**, mulai dari Langkah **Membuat VM dari Template Debian 12**. Dengan ketentuan sebagai berikut

|       |            |
|-------|------------|
| VM ID | 102        |
| Name  | Debian2    |
| Mode  | Full Clone |

| Debian1     |                |
|-------------|----------------|
| IP Address  | 10.10.10.12/24 |
| Gateway     | 10.10.10.1     |
| DNS Servers | 10.10.10.1     |

Jika berhasil kita akan mempunyai 2 buah VM **debian1** dan **debian2** di Proxmox, Seperti pada gambar dibawah ini



## KONFIGURASI NAT SUPAYA VM DAPAT MENGAKSES JARINGAN INTERNET/EXTERNAL

1. Masuk ke Terminal Proxmox
2. Membuat supaya proxmox dapat melewati/memforward IP  
Karena computer kita di gunakan untuk memforwardkan/melewatkan paket IP maka hilangkan tanda #  
pada baris **net.ipv4.ip\_forward=1** di dalam file **/etc/sysctl.conf**.  
**nano /etc/sysctl.conf**  
Sebelum  
**# net.ipv4.ip\_forward=1**  
sesudah  
**net.ipv4.ip\_forward=1**
3. Berikutnya adalah bagaimana Komputer-komputer VM dapat mengakses Internet/external. kita harus membuat konfigurasi NAT pada Proxmox dengan menggunakan MASQUERADING. Untuk mengatur masquerading, gunakan perintah berikut:

**iptables -t nat -A POSTROUTING -s 10.10.10.0/24 -j MASQUERADE**

Perintah diatas dapat diartikan setiap paket-paket data yang berasal (-s) dari alamat jaringan 10.10.10.0/24 setelah melalui router (POSTROUTING) IP addressnya akan diganti (MASQUERADE) menjadi IP Address pada sisi luar dari router.

4. Simpan Rules agar Permanen  
Install iptables-persistent di Proxmox  
**apt install iptables-persistent**  
Untuk menyimpan Rules, gunakan perintah dibawah ini setelah membuat iptables  
**iptables-save > /etc/iptables/rules.v4**
5. Setelah selesai konfigurasi NAT, dilanjutkan dengan cek jaringan menggunakan ping ke Alamat gateway sekolah (**192.168.252.254**) dan ke internet (**8.8.8.8**), misalnya dari **VM debian2**

```
root@debian2:~# ping 192.168.252.254
PING 192.168.252.254 (192.168.252.254) 56(84) bytes of data.
64 bytes from 192.168.252.254: icmp_seq=1 ttl=63 time=0.538 ms
64 bytes from 192.168.252.254: icmp_seq=2 ttl=63 time=2.21 ms
64 bytes from 192.168.252.254: icmp_seq=3 ttl=63 time=0.893 ms
64 bytes from 192.168.252.254: icmp_seq=4 ttl=63 time=1.53 ms
64 bytes from 192.168.252.254: icmp_seq=5 ttl=63 time=1.95 ms
```

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=95.5 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=189 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=140 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=164 ms
```

## INSTALASI DAN KONFIGURASI DNS FORWARD

Fungsi dari DNS Forward Adalah meneruskan (forward) query ke DNS internet. Client **cukup pakai 1 DNS saja**, yaitu DNS lokal (Proxmox), jadi kalau nanti Proxmox mempunyai DNS lokal sendiri cukup di isi IP DNS lokal saja (10.10.10.1) dan akan meneruskan ke DNS Publik (internet), jadi tidak perlu mengisi Alamat DNS 8.8.8.8.

DNS Server yang akan digunakan praktek di sini menggunakan **dnsmasq**, karena lebih ringan dan konfigurasinya lebih sederhana dibandingkan **bind9**.

### Masuk ke terminInstalasal Proxmox

1. Instal **dnsmasq** di **Proxmox**

**apt install dnsmasq**

```
root@pve:~#  
root@pve:~# apt install dnsmasq
```

2. Konfigurasi **dnsmasq** sebagai DNS Forwarder

**nano /etc/dnsmasq.conf**

Hilangkan tanda pagar di depan ke tiga baris dibawah ini

**domain-needed**

**bogus-priv**

**no-resolv**

```
# Never forward plain  
domain-needed  
# Never forward address  
bogus-priv
```

```
# uncomment this.  
no-resolv
```

Kemudian pada bagian paling bawah tambahkan baris berikut :

**server=8.8.8.8**

```
#dhcp-ignore-names=tag:wpad-ignore
```

```
server=8.8.8.8
```

Setelah selesai simpan dan keluar

### Restart dnsmasq

systemctl restart dnsmasq

3. Uji konfigurasi dengan cara ping dari **vm debian1** dan **debian2** ke salah satu domain yang ada di internet misalnya **google.com**

#### VM debian1

```
root@debian1:~#  
root@debian1:~# ping google.com  
PING google.com (142.250.4.101) 56(84) bytes of data.  
64 bytes from sm-in-f101.1e100.net (142.250.4.101): icmp_seq=1 ttl=97 time=162 ms  
64 bytes from sm-in-f101.1e100.net (142.250.4.101): icmp_seq=2 ttl=97 time=47.1 ms  
64 bytes from sm-in-f101.1e100.net (142.250.4.101): icmp_seq=3 ttl=97 time=113 ms
```

#### VM debian2

```
root@debian2:~#  
root@debian2:~# ping google.com  
PING google.com (64.233.170.138) 56(84) bytes of data.  
64 bytes from sg-in-f138.1e100.net (64.233.170.138): icmp_seq=1 ttl=97 time=163 ms  
64 bytes from sg-in-f138.1e100.net (64.233.170.138): icmp_seq=2 ttl=97 time=172 ms  
64 bytes from sg-in-f138.1e100.net (64.233.170.138): icmp_seq=3 ttl=97 time=181 ms
```

## INSTALASI DAN KONFIGURASI WEB SERVER

Pada bagian ini kita akan menginstall Web Server (Apache2) sesuai permintaan dari Client untuk membuat layanan Web.

1. Install **apache2** di **VM debian1** dan **debian2**

#### apt install apache2

```
root@debian1:~#  
root@debian1:~# apt install apache2
```

2. Mengubah halman web di **VM debian1** dan **debian2**

Masuk ke direktori **/var/www/html**

**cd /var/www/html**

Backup **index.html** menjadi **index.html.bak**

**mv index.html index.html.bak**

Membuat tampilan halaman web

**nano index.html**

```
<html>  
<body>  
<h1>SELAMAT DATANG DI WEB SERVER DEBIAN1</h1>  
</body>  
</html>
```

Untuk halaman web **VM debian2** sama seperti diatas **DEBIAN1** diganti **DEBIAN2**

## PORT FORWARDING

Pada bagian ini kita akan mencoba untuk mengakses service-service yang ada di **debian1** dan **debian2** tidak menggunakan IP Address **debian1** dan **debian2** tetapi dari IP Address external yaitu vmbr0 Proxmox 192.168.252.1XX, hal ini diperlukan jika data center kita hanya mempunyai satu IP Publik, padahal kita mempunyai lebih dari satu server.

Langkah-langkahnya sebagai berikut :

1. Buka **terminal** di **Proxmox**
2. Selanjutnya kita akan mencoba kalau mengakses **debian1** dan **debian2** menggunakan web browser dengan alamat 192.168.252.1XX yang muncul adalah bukan halaman webnya Proxmox tapi halaman web **debian1** dan **debian2**

Mengakses Halaman web **debian1**

Kalau dari web browser di ketik http://192.168.252.1XX:8011, akan dibelokan ke IP Address **debian1** (10.10.10.11), maka halaman web yang harus muncul halaman web **debian1**



Mengakses Halaman web **debian2**

Kalau dari web browser di ketik http://192.168.252.1XX:8012, akan dibelokan ke IP Address **debian1** (10.10.10.12), maka halaman web yang harus muncul halaman web **debian2**



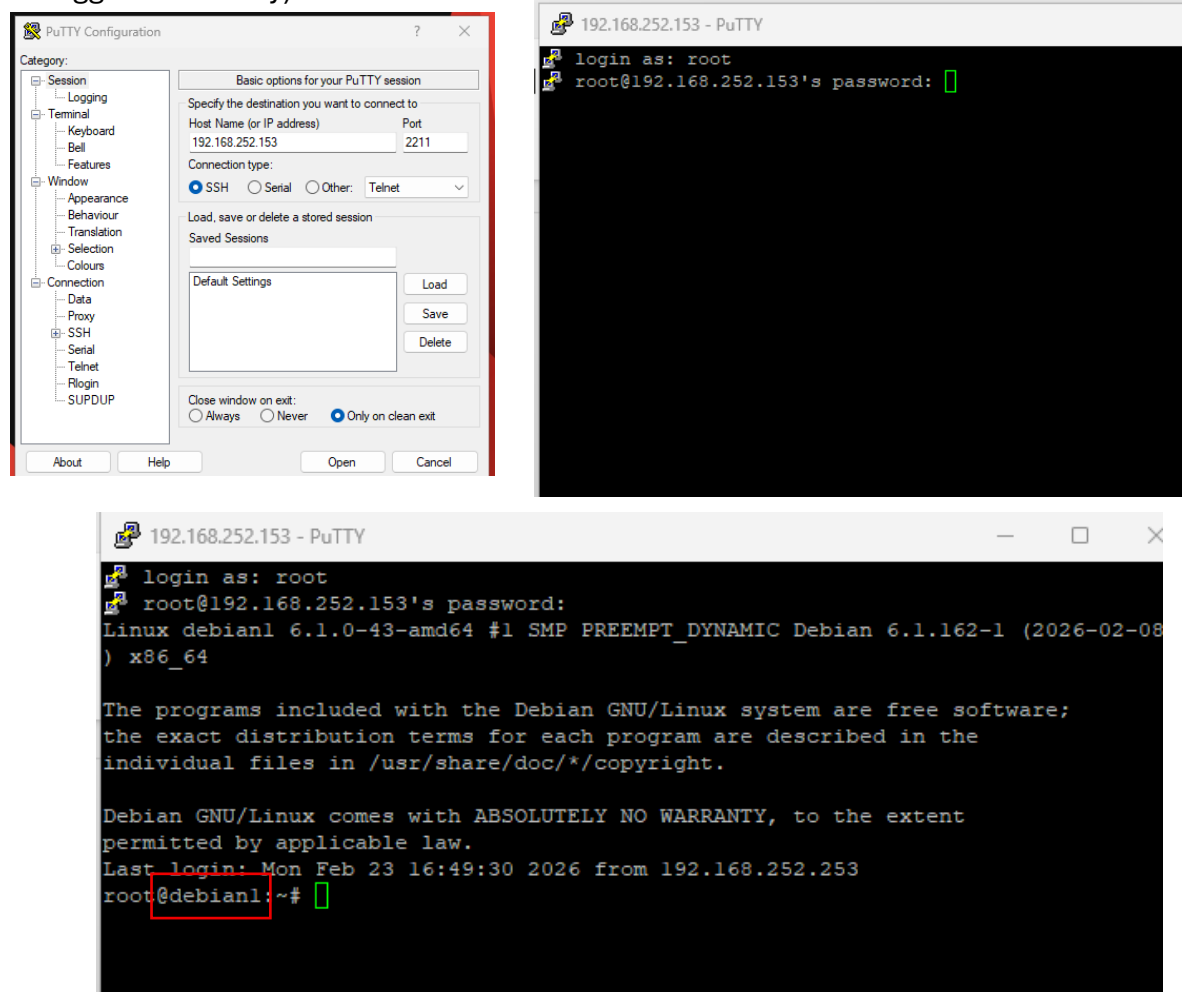
3. Perintah di Proxmox supaya bisa mengakses halaman web **debian1** dan **debian2**  
Mengakses halaman web **debian1**

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.252.1xx --dport 8011 -j DNAT --to 10.10.10.11:80
```

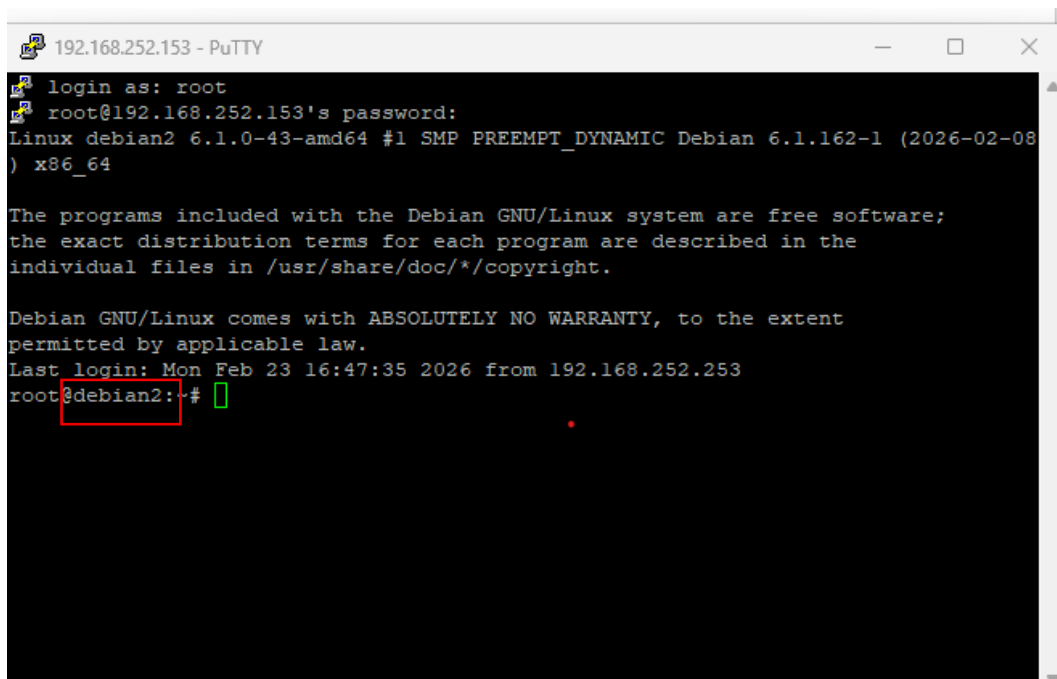
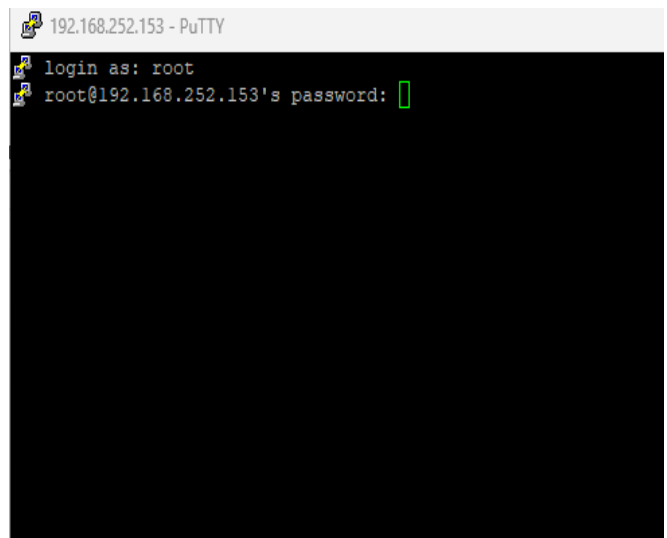
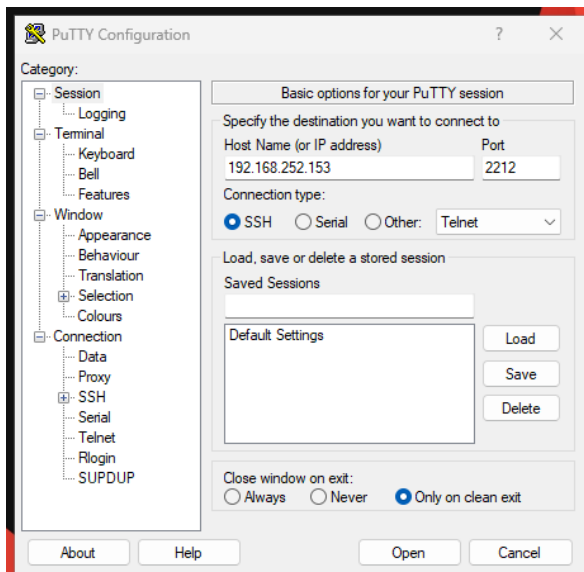
Mengakses halaman web **debian2**

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.252.1xx --dport 8012 -j DNAT --to 10.10.10.12:80
```

4. Konfigurasi Proxmox untuk SSH yang menggunakan port 2211 dari PC Client dengan mengakses IP 192.168.252.1XX diarahkan ke **debian1** (Cek menggunakan Putty)



5. Konfigurasi Proxmox untuk SSH yang menggunakan port 2212 dari PC Client dengan mengakses IP 192.168.252.1XX diarahkan ke **debian2** (Cek menggunakan Putty)



### Catatan :

Jangan lupa setelah membuat iptables, jangan lupa disimpan dengan perintah seperti pada gambar dibawah ini

```
root@pve:~# iptables -t nat -A PREROUTING -p tcp -d 1
root@pve:~# iptables -t nat -A PREROUTING -p tcp -d 1
root@pve:~# iptables -t nat -A PREROUTING -p tcp -d 1
root@pve:~# iptables -t nat -A PREROUTING -p tcp -d 1
root@pve:~# iptables-save > /etc/iptables/rules.v4
root@pve:~#
```

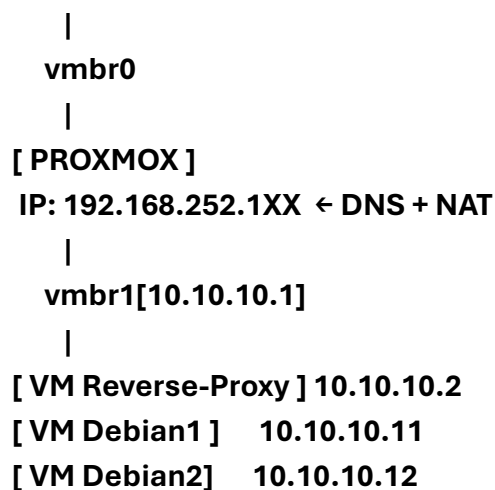
## Job 2 : DNS Lokal di Proxmox untuk Reverse Proxy dan Virtual Machine

Kalau sebelumnya Client mengakses web dengan menggunakan IP Address, pada perkembangan berikutnya Client ingin mengakses Web menggunakan domain, permasalahannya Client hanya mempunyai 1 IP Public dan masing – masing Virtual Machine harus bisa diakses dengan domain yang berbeda.

Untuk mengatasi permasalahan tersebut masing-masing domain tetap di mapping ke satu IP Public (192.168.252.1XX) dan permintaan domain tersebut akan diserahkan ke Reverse Proxy (nginx) untuk kemudian di teruskan ke Virtual Machine yang sesuai.

### TOPOLOGI

#### PC Client / Browser



Langkah kerjanya Adalah sebagai berikut :

1. Membuat VM satu lagi untuk **Reverse Proxy**, dengan cara mengkloning dari **debian12-template**, dengan ketentuan sebagai berikut:

|       |            |
|-------|------------|
| VM ID | 103        |
| Name  | proxy      |
| Mode  | Full Clone |

| proxy       |               |
|-------------|---------------|
| IP Address  | 10.10.10.2/24 |
| Gateway     | 10.10.10.1    |
| DNS Servers | 10.10.10.1    |

Catatan : cara mengkloning dapat dilihat di job sebelumnya

## 2. Konfigurasi DNS Server

Ketentuan Domain

| DOMAIN           | IP ADDRESS      | TUJUAN     |
|------------------|-----------------|------------|
| www.cepotxx.net  | 192.168.252.1XX | VM debian1 |
| www.dawalaxx.net | 192.168.252.1XX | VM debian2 |

Keterangan : xx Adalah nomor urut siswa

Konfigurasi DNS

**Masuk ke terminal Proxmox**

Membuat file konfigurasi DNS dengan nama misalnya **domain.conf**

**nano /etc/dnsmasq.d/domain.conf**

```
root@pve:~#  
root@pve:~# nano /etc/dnsmasq.d/domain.conf
```

```
GNU nano 7.2  
address=/www.cepot53.net/192.168.252.153  
address=/www.dawala53.net/192.168.252.153
```

**53 diganti nomor urut siswa**

Setelah selesai jangan lupa di simpan kemudian keluar

Restart **dnsmasq**

**systemctl restart dnsmasq** dari

Uji DNS Server dari salah satu VM dengan ping ke domain yang baru dibuat.

```
root@debian1:~#  
root@debian1:~# ping www.cepot53.net  
PING www.cepot53.net (192.168.252.153) 56(84) bytes of data.  
64 bytes from pve.example.net (192.168.252.153): icmp_seq=1 ttl=64 time=0.911 ms  
64 bytes from pve.example.net (192.168.252.153): icmp_seq=2 ttl=64 time=0.492 ms  
64 bytes from pve.example.net (192.168.252.153): icmp_seq=3 ttl=64 time=1.60 ms
```

```
root@debian1:~#  
root@debian1:~# ping www.dawala53.net  
PING www.dawala53.net (192.168.252.153) 56(84) bytes of data.  
64 bytes from pve.example.net (192.168.252.153): icmp_seq=1 ttl=64 time=0.338 ms  
64 bytes from pve.example.net (192.168.252.153): icmp_seq=2 ttl=64 time=1.02 ms  
64 bytes from pve.example.net (192.168.252.153): icmp_seq=3 ttl=64 time=0.707 ms
```

### 3. Konfigurasi **Revers Proxy**

#### Konfigurasi **Revers Proxy**

Masuk ke console **proxy**

Membuat file konfigurasi **Revers Proxy** dengan nama misalnya **proxy**  
**nano /etc/nginx/sites-available/proxy**

```
root@proxy:~#  
root@proxy:~# nano /etc/nginx/sites-available/proxy
```



```
GNU nano 7.2 /etc/nginx/sites-available/proxy  
server {  
    listen 80;  
    server_name www.cepot53.net;  
  
    location / {  
        proxy_pass http://10.10.10.11;  
        proxy_set_header Host $host;  
    }  
}  
  
server {  
    listen 80;  
    server_name www.dawala53.net;  
  
    location / {  
        proxy_pass http://10.10.10.12;  
        proxy_set_header Host $host;  
    }  
}
```

Setelah selesai jangan lupa disimpan kemudian keluar

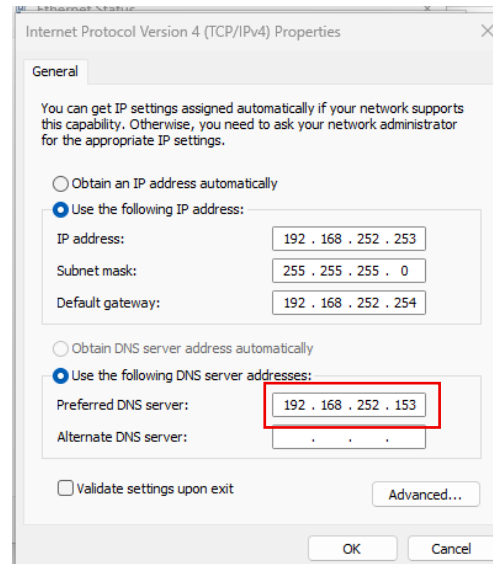
Aktifkan konfigurasi diatas

```
ln -s /etc/nginx/sites-available/proxy /etc/nginx/sites-enabled  
systemctl reload nginx
```

Konfigurasi port forwarding (NAT) di Proxmox supaya dapat mengakses port 80 (HTTP) **Revers Proxy**.

**iptables -t nat -A PREROUTING -p tcp -d 192.168.252.1XX --dport 80 -j DNAT --to-destination 10.10.10.2**

Cek akses web dari Client /Windows, ubah Alamat DNS menjadi IP address vmbr0 (192.168.252.1XX)



53 diganti nomor urut siswa

Cek koneksi ke domain lokal kita (www.cepotxx.net dan www.dawalaxx.net) dan domain yang ada di internet misalnya google.com.

```
C:\Users\admin>ping www.cepot53.net

Pinging www.cepot53.net [192.168.252.153] with 32 bytes of data:
Reply from 192.168.252.153: bytes=32 time<1ms TTL=64
Reply from 192.168.252.153: bytes=32 time<1ms TTL=64
Reply from 192.168.252.153: bytes=32 time<1ms TTL=64
Reply from 192.168.252.153: bytes=32 time<1ms TTL=64
```

```
C:\Users\admin>ping www.dawala53.net

Pinging www.dawala53.net [192.168.252.153] with 32 bytes of data:
Reply from 192.168.252.153: bytes=32 time<1ms TTL=64
Reply from 192.168.252.153: bytes=32 time=1ms TTL=64
Reply from 192.168.252.153: bytes=32 time<1ms TTL=64
Reply from 192.168.252.153: bytes=32 time<1ms TTL=64
```

```
C:\Users\admin>ping google.com

Pinging google.com [172.217.194.100] with 32 bytes of data:
Reply from 172.217.194.100: bytes=32 time=46ms TTL=98
Reply from 172.217.194.100: bytes=32 time=69ms TTL=98
Reply from 172.217.194.100: bytes=32 time=191ms TTL=98
Reply from 172.217.194.100: bytes=32 time=63ms TTL=98
```

**www.cepotxx.net**



**www.dawala.net**



## Job 3 : Instalasi *Control Panel Hosting* di Virtual Machine

Admin merasa kesulitan dalam mengelola Server secara manual, Kita akan menginstal *Control Panel Hosting* untuk admin agar mudah dan cepat dalam deploy dan mengatur web, domain, email, DNS, dan database dari satu dashboard terpusat tanpa harus melakukan instalasi dan konfigurasi secara manual yang rumit.

Kita akan menggunakan **HestiaCP** sebagai control panel untuk mengelola server hosting. HestiaCP dipilih karena ringan, gratis, dan cocok untuk pembelajaran sebelum nantinya mengenal control panel komersial seperti cPanel di dunia industri.

HestiaCP adalah solusi **control panel server yang gratis dan open source**, sehingga penggunaannya legal untuk praktik maupun produksi ringan tanpa perlu membeli lisensi seperti cPanel.

Dari sisi performa, panel ini sangat **ringan dan cepat**, bahkan dapat berjalan lancar di VPS dengan spesifikasi kecil (cukup RAM 1–2 GB). Proses instalasinya pun singkat, sehingga waktu belajar lebih fokus ke praktik langsung.

Dari segi fitur, HestiaCP sudah **lengkap untuk kebutuhan hosting**—mencakup manajemen domain, DNS, web server (Nginx + Apache), database MySQL/MariaDB, email server, SSL otomatis dari Let's Encrypt, serta FTP dan file manager. Alur kerjanya pun hampir mirip dengan cPanel yang umum dipakai di industri.

Yang tak kalah penting, HestiaCP **mudah dipahami pemula**. Antarmukanya sederhana, strukturnya jelas (USER → DOMAIN → WEB → DB), sehingga cocok sebagai jembatan dari teori ke praktik nyata.

Dari sisi keamanan, panel ini sudah cukup **aman** dengan dukungan firewall, SSL otomatis, dan bisa dikombinasikan dengan hardening dasar.

Namun perlu dicatat, HestiaCP memiliki **beberapa keterbatasan**: belum sepopuler cPanel di perusahaan besar, fitur enterprisennya terbatas, dan kurang cocok untuk kebutuhan shared hosting skala besar.

### Langkah-langkah Instalasi HestiaCP

Instalasi **HestiaCP** dilaksanakan di **debian1** dan **debian2**. Untuk contoh dibawah ini misalnya di **debian1**, setelah **HestiaCP** berhasil diinstal di **debian1**, kemudian ulangi menginstalasi **HestiaCP** di **debian2**.

#### Langkah 1: Instal Paket yang Diperlukan

```
root@debian1:~# apt install ca-certificates software-properties-common apt-transport-https gnupg wget unzip -y
```

## Langkah 2: Instal HestiCP

Unduh skrip instalasi HestiaCP terbaru dari repositori GitHub resmi menggunakan perintah `wget` berikut .

```
root@debian1:~# wget https://raw.githubusercontent.com/hestiacp/hestiacp/release/install/hst-install.sh
```

Jalankan skrip instalasi dan ikuti petunjuk di layar.

```
root@debian1:~# bash hst-install.sh
```

Selama proses instalasi, Anda akan diminta untuk mengkonfirmasi instalasi dan memilih paket perangkat lunak yang akan diinstal.

**Would you like to remove the conflicting packages? [y/N] y**

```
Hestia Control Panel
1.9.4
www.hestiacp.com

=====

Thank you for downloading Hestia Control Panel! In a few moments,
we will begin installing the following components on your server:

- NGINX Web / Proxy Server
- Apache Web Server (as backend)
- PHP-FPM Application Server
- Bind DNS Server
- Exim Mail Server
- Dovecot POP3/IMAP Server
- MariaDB Database Server
- Vsftpd FTP Server
- Firewall (iptables) + Fail2Ban Access Monitor

=====

Would you like to continue with the installation? [y/N]: y
```

Pada bagian diatas diinformasikan proses instalasi dari script installer yang sebelumnya didownload akan melakukan instalasi aplikasi-aplikasi seperti list yang tampil. Tekan tombol Y dan kemudian Enter untuk melanjutkan.

```
Please use a valid username (ex. user).
Please enter administrator username: admin
Please enter administrator password: 123456
```

```
Please use a valid emailaddress (ex. info@domain.tld).
Please enter admin email address: admin@cepot53.net
Please enter FQDN hostname [debian1]: server.cepot53.net
Installation backup directory: /root/hst_install_backups/010320260447
Installation log file: /root/hst_install_backups/hst_install-010320260447.log
```

Kita diminta memasukkan alamat email dan juga mengisi hostname. Jika hostname telah sesuai dengan yang kita kehendaki, silahkan tekan enter. Namun Kita juga bisa mengubah hostname sesuai kebutuhan. (53 diganti nomor urut)

### Langkah 3: Akses Panel Kontrol Hestia

Setelah instalasi selesai, HestiaCP akan memberi Anda URL login, nama pengguna, dan kata sandi.

```
Congratulations!

You have successfully installed Hestia Control Panel on your server.

Ready to get started? Log in using the following credentials:

Admin URL: https://server.cepot53.net:8083
Backup URL: https://182.2.68.36:8083
Username: admin
Password: The password you chose during installation.

Thank you for choosing Hestia Control Panel to power your full stack web server,
we hope that you enjoy using it as much as we do!

Please feel free to contact us at any time if you have any questions,
or if you encounter any bugs or problems:

Documentation: https://docs.hestiacp.com/
Forum: https://forum.hestiacp.com/
GitHub: https://www.github.com/hestiacp/hestiacp

Note: Automatic updates are enabled by default. If you would like to disable them,
please log in and navigate to Server > Updates to turn them off.

Help support the Hestia Control Panel project by donating via PayPal:
https://www.hestiacp.com/donate

--
Sincerely yours,
The Hestia Control Panel development team

Made with love & pride by the open-source community around the world.
[ ! ] IMPORTANT: The system will now reboot to complete the installation process.
Press any key to continue
```

Untuk mengakhiri instalasi tekan **enter**

Instalasi **HestiaCP** di **debian1** sudah selesai, ulangi instalasi **HestiaCP** untuk **debian2** untuk email: **admin@dawalaxx.net** dan domain: **server.dawalaxx.net**

Setelah **HestiaCP** berhasil di instal di **debian1** dan **debian2**, sekarang Adalah bagaimana caranya kita mengakses **HestiaPC**. Untuk mengakses nya kita bisa menggunakan **web browser ( misalnya Chrome)** dengan protocol **HTTPS** dan **Port 8083**, masalah kita Adalah

untuk mengakses **debian1** dan **debian2** adalah hanya menggunakan **1 IP Publik (192.168.252.1XX)** dan **1 Port (8083)**, untuk mengatasinya kita akan menggunakan **Port Forwarding**

Untuk mengakses **hestiaCP** di **debian1** Menggunakan **8311** diteruskan ke **Port: 8083** di **debian1**

Untuk mengakses **hestiaCP** di **debian2** Menggunakan **8312** diteruskan ke **Port: 8083** di **debian2**

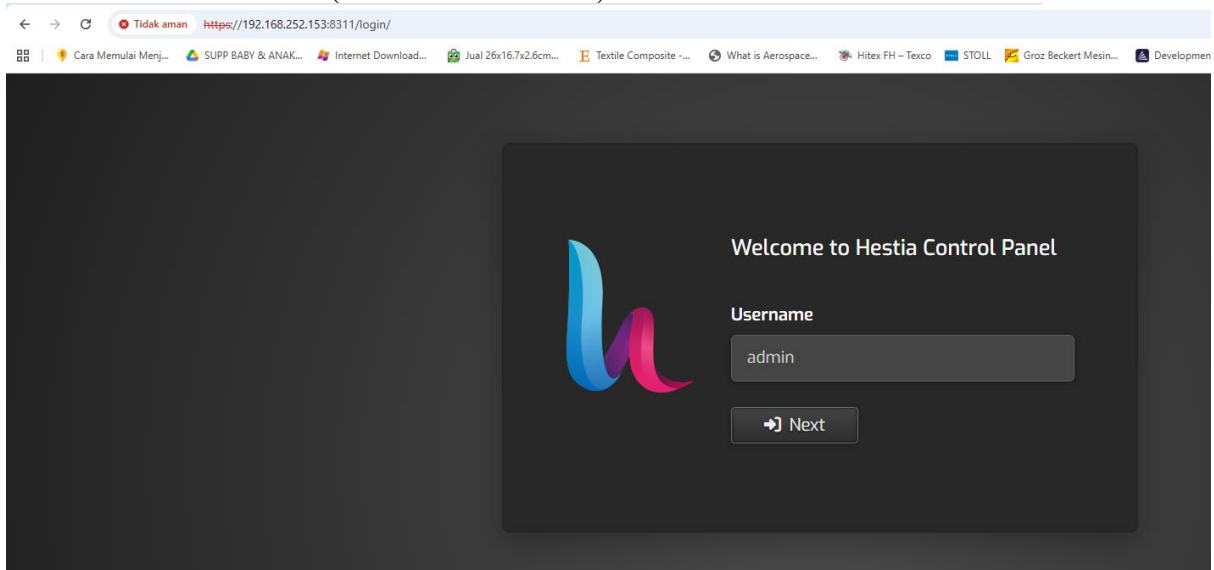
## Langkah untuk setting Port Forwarding

1. Masuk ke terminal **Proxmox**
2. Konfigurasi **NAT Port Forwarding**  

```
root@pve:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.252.153 --dport 8311 -j DNAT --to 10.10.10.11:8083
```

```
root@pve:~# iptables -t nat -A PREROUTING -p tcp -d 192.168.252.153 --dport 8312 -j DNAT --to 10.10.10.12:8083
```

```
root@pve:~# iptables-save > /etc/iptables/rules.v4
```
3. Akses dari Web Browser (Chrome), misalnya mengakses **HestiaCP** di **debian1** → ketik **https://192.168.252.1XX:8311** pada address bar web browser (Chrome). Kemudian isi Username dan Password (lihat ketika instalasi)



Setelah di klik **Next**, muncul tampilan dibawah ini, tampilan ini bukan error, tapi peringatan keamanan.



## Penjelasan Teknis

Apa yang terjadi ketika kita menggunakan perintah ini?

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.252.153 --dport 8311 -j DNAT --to 10.10.10.11:8083
```

Perintah di atas melakukan **penerusan alamat (DNAT)**. Cara kerjanya:

1. User mengakses `192.168.252.153:8311` melalui browser
2. Server meneruskan koneksi tersebut ke `10.10.10.11:8083` (HestiaCP)
3. Halaman HestiaCP terbuka di browser user

Tapi kenapa muncul error "**Potential CSRF use detected**"?

Ada 3 alasan teknis:

### 1. Host Header Tidak Cocok

- Browser user mengirimkan header "Host: 192.168.252.153:8311"
- HestiaCP menerima koneksi, tapi melihat header Host yang dikirim adalah `192.168.252.153:8311`
- Padahal HestiaCP mengenali dirinya sebagai `10.10.10.11:8083`
- Karena tidak cocok, HestiaCP curiga ada yang tidak beres

## 2. Cookie Domain Tidak Sesuai

- Saat pertama login, HestiaCP membuat cookie untuk domain `10.10.10.11`
- Saat user mengirim request berikutnya dari `192.168.252.153`, cookie tersebut ikut dikirim
- Tapi HestiaCP melihat cookie itu untuk domain `10.10.10.11`, bukan untuk alamat yang sekarang digunakan user
- Akibatnya cookie dianggap tidak valid

## 3. Token CSRF Bermasalah

- HestiaCP membuat token CSRF yang dikaitkan dengan alamat `10.10.10.11:8083`
- User mengirimkan token itu kembali dari alamat `192.168.252.153:8311`
- Karena alamatnya berbeda, token dianggap tidak sah

## Kesimpulan

DNAT hanya memindahkan koneksi ke alamat tujuan, tapi **tidak mengubah informasi di dalam koneksi** (seperti header Host, cookie, dan token). Akibatnya informasi yang dikirim user tidak cocok dengan yang diharapkan server, sehingga sistem keamanan HestiaCP bereaksi.

## Solusi Teknis yang Tepat:

1. **Gunakan VPN** - User terhubung ke jaringan internal dulu, baru akses langsung ke `10.10.10.11:8083`
2. **Gunakan Reverse Proxy** (Nginx/Apache) - Server perantara yang bisa mengubah header Host dan informasi lain agar sesuai dengan yang diharapkan HestiaCP

## Job 4 : Konfigurasi VPN (Virtual Private Server ) Untuk mengakses HestiaCP

Seperti penjelasan sebelumnya untuk mengakses **HestiaCp** yang terinstal di **VM debian1** dan **debian2** tidak bisa diakses langsung dari jaringan luar/internet dengan metode **Port Forwarding**, untuk mengatasinya bisa menggunakan **VPN** atau **Reverse Proxy**. Di sini kita akan menggunakan **VPN** untuk mengakses **HestiaCp**.

### KONSEP DASAR VPN

Secara sederhana, VPN adalah teknologi yang menciptakan jalur komunikasi pribadi dan aman di atas jaringan internet publik. Mari kita lihat perbedaannya:

- Tanpa VPN (Akses Langsung):
  - Cara kerja: Administrator mencoba mengakses server kantor secara langsung dari luar.
  - Risiko: Koneksi ini rentan karena dilakukan melalui jaringan publik. Akibatnya, jalur akses ke server (port) menjadi terbuka dan bisa saja dimanfaatkan oleh pihak tidak bertanggung jawab.
- Dengan VPN (Akses via Tunnel):
  - Cara kerja: Administrator pertama-tama terhubung ke jaringan internal kantor melalui VPN. Setelah terhubung, barulah ia bisa mengakses server.
  - Keuntungan: Kini, server sepenuhnya privat dan tidak terekspos ke internet publik. Administrator seolah-olah berada dalam satu jaringan lokal (LAN) yang sama dengan server, meskipun jaraknya ribuan kilometer.

Jadi, Kita bisa membayangkan VPN sebagai sebuah **jembatan aman** yang menghubungkan perangkat Kita langsung ke jaringan internal, dalam hal ini jaringan **vmbr1**, sehingga komunikasi dengan server di dalamnya menjadi aman dan eksklusif.

## Mengapa Memilih WireGuard untuk VPN?

Sekarang kita sudah paham pentingnya VPN, pertanyaan selanjutnya adalah: VPN mana yang sebaiknya digunakan? Salah satu pilihan terbaik saat ini adalah **WireGuard**. Ada tiga alasan utama mengapa WireGuard sangat direkomendasikan, terutama untuk pembelajaran:

### 1. Mudah (Kesederhanaan):

WireGuard dirancang agar tidak rumit. Tidak seperti VPN lain yang membutuhkan banyak konfigurasi dan aturan, WireGuard hanya memerlukan sedikit pengaturan. Ini membuat proses instalasi dan konfigurasinya jauh lebih cepat dan mudah dipahami, terutama bagi pemula.

### 2. Cepat (Performa Tinggi):

Dengan kode program yang ramping dan efisien, WireGuard mampu beroperasi dengan sangat cepat. Ia tidak membebani perangkat dan mampu memanfaatkan kecepatan internet secara maksimal, sehingga koneksi Anda tetap lancar.

### 3. Aman (Keamanan Modern):

WireGuard menggunakan teknologi kriptografi (ilmu tentang pengamanan data) terkini dan terbaik. Ia menggunakan kunci-kunci kriptografi modern yang sangat kuat untuk memastikan data Anda dienkripsi dengan aman dan tidak bisa disadap oleh siapa pun.

## Mengamankan Akses ke Panel HestiaCP dengan WireGuard

Setelah memahami konsep dasar VPN, mari kita lihat penerapannya dalam situasi nyata. Bayangkan kita memiliki sebuah server yang menjalankan **HestiaCP**, sebuah panel kontrol untuk mengelola website. Biasanya, panel ini bisa diakses melalui browser di alamat **https://ip\_server:8083**.

Namun, membuka akses panel kontrol langsung ke internet adalah praktik yang berisiko. Port 8083 akan terbuka untuk siapa saja, dan panel bisa menjadi sasaran serangan brute-force atau peretasan.

Dengan VPN, kita bisa membuat akses ke panel ini menjadi **jauh lebih aman** tanpa perlu repot mengatur konfigurasi yang rumit.

## Rancangan Jaringan

Mari kita lihat dulu bagaimana jaringan akan dibangun. Kita akan menggunakan sebuah server utama dengan **Proxmox** (platform virtualisasi) yang di dalamnya terdapat dua jaringan (bridge):

### 1. **vmbr0 (Jaringan Publik / NAT):**

- Ini adalah jembatan yang menghubungkan server ke internet melalui IP publik.
- Jaringan ini bersifat publik dan bisa diakses dari luar.

### 2. **vmbr1 (Jaringan Private 10.10.10.0/24):**

- Ini adalah jembatan untuk jaringan internal yang bersifat tertutup.
- Alamatnya menggunakan IP private, misalnya 10.10.10.x.
- Di jaringan inilah kita akan meletakkan layanan-layanan yang ingin kita lindungi.

Di dalam jaringan private vmbr1 ini, kita akan menjalankan dua mesin virtual (VM):

- **VM HestiaCP:** Berisi panel kontrol HestiaCP yang akan kita akses, dengan alamat IP 10.10.10.11 dan port 8083.
- **VM WireGuard Server:** Berfungsi sebagai "pintu gerbang" VPN. VM inilah yang akan menerima koneksi dari luar dan menghubungkannya ke jaringan private.

## Langkah – langkah Instalasi dan Konfigurasi Wireguard (VPN)

1. Membuat VM satu lagi untuk **vpn**, dengan cara mengkloning dari **debian12-template**, dengan ketentuan sebagai berikut:

|       |            |
|-------|------------|
| VM ID | 104        |
| Name  | vpn        |
| Mode  | Full Clone |

| vpn         |               |
|-------------|---------------|
| IP Address  | 10.10.10.5/24 |
| Gateway     | 10.10.10.1    |
| DNS Servers | 10.10.10.1    |

Catatan : cara mengkloning dapat dilihat di job 1

## 2. Konfigurasi IP Forwarding

nano /etc/sysctl.conf

Hilangkan tanda pagar pada baris

# net.ipv4.ip\_forward=1

Sesudah tanda pagar dihilangkan

net.ipv4.ip\_forward=1

Kemudian simpan, dan aktifkan dengan perintah

**Sysctl -p**

## 3. Instalasi Iptables

```
root@vpn:~# apt install iptables iptables-persistent
```

## 4. Instalasi Wireguard

```
root@vpn:~# apt update
```

```
root@vpn:~# apt install wireguard -y
```

## 5. Membuat (Generate) Key

Generate Key untuk Server

```
root@vpn:~# wg genkey | tee server_private.key | wg pubkey > server_public.key
```

Setelah generate key di atas akan muncul dua file **server\_private.key** dan **server\_public.key**

```
root@vpn:~# ls
server_private.key server_public.key
```

Generate Key untuk Client

```
root@vpn:~# wg genkey | tee client_private.key | wg pubkey > client_public.key
```

Setelah generate key di atas akan muncul dua file **client\_private.key** dan **client\_public.key**

```
root@vpn:~# ls
client_private.key client_public.key server_private.key server_public.key
root@vpn:~#
```

## 6. Konfigurasi Server

- Buka file **server\_private.key**

```
root@vpn:~# cat server_private.key
```

- Setelah terbuka muncul **key** yang akan digunakan untuk **private key** untuk server **Wireguard**, kemudian copy kan key tersebut dengan cara memblok key kemudian klik kanan pada menu, pilih **copy/salin**

```
root@vpn:~# cat server_private.key
mKO1/EZeR3fryoIGVNOSTAd2yJv97L2VHiCHzd7omHk=
root@vpn:~#
```

- Buka file konfigurasi **Wireguard**

```
root@vpn:~# nano /etc/wireguard/wg0.conf
```

Setelah terbuka ketikkan baris – baris perintah dibawah ini, pada baris **privatekey** isi **key** dengan cara mem **paste** dari **key** yang tadi kita copy. (cara mem **paste** : klik kanan pada baris **privatekey** kemudian pilih **paste/tempel**)

```
GNU nano 7.2 /etc/wireguard/wg0.conf *
[Interface]
Address = 10.20.20.1/24
ListenPort = 51820

PrivateKey = mKO1/EZeR3fryoIGVNOSTAd2yJv97L2VHiCHzd7omHk=

PostUp = sysctl -w net.ipv4.ip_forward=1
PostUp = iptables -t nat -A POSTROUTING -s 10.20.20.0/24 -j MASQUERADE

PostDown = iptables -t nat -D POSTROUTING -s 10.20.20.0/24 -j MASQUERADE
```

#### Keterangan :

##### [Interface]

Bagian ini digunakan untuk **konfigurasi interface WireGuard pada server**.

Jika dianalogikan dengan jaringan biasa:

**eth0**

**wlan0**

maka WireGuard membuat **interface virtual bernama wg0**.

Fungsi bagian ini:

- mengatur IP VPN
- port VPN
- private key server
- aturan tambahan saat VPN aktif

**Address = 10.20.20.1/24**

Artinya server VPN memiliki alamat IP 10.20.20.1 di Alamat jaringan VPN 10.20.20.0/24

**ListenPort = 51820**

Artinya server WireGuard mendengarkan koneksi pada port UDP 51820.

Client akan menghubungi server melalui: IP Address:51820

WireGuard menggunakan UDP arena:

- lebih cepat
- lebih ringan
- cocok untuk VPN

**PrivateKey = mKO1/EZeR3fryoIGVNOSTAd2yJv97L2VHiCHzd7omHk=**

Ini adalah **private key milik server**, fungsinya untuk proses enkripsi dan autentikasi VPN Konsepnya seperti **password server VPN**.

private key tidak boleh dibagikan, pasangannya Adalah **Public Key** yang digunakan oleh **client**.

**PostUp = sysctl -w net.ipv4.ip\_forward=1**

Perintah ini dijalankan **ketika WireGuard aktif**, fungsinya untuk mengaktifkan IP forwarding, artinya server boleh meneruskan paket jaringan.

Tanpa ini:

VPN hanya bisa connect

tapi tidak bisa mengakses jaringan lain

**PostUp = iptables -t nat -A POSTROUTING -s 10.20.20.0/24 -j MASQUERADE**

Perintah ini membuat NAT (Network Address Translation).

Fungsinya:

**mengubah IP client VPN menjadi IP server**

Contoh:

Sebelum NAT:

**Client VPN → 10.20.20.2**

Setelah NAT:

**Server melihat trafik dari 10.10.10.5**

Manfaat:

Client VPN bisa mengakses:

**Internet**

atau

**Jaringan internal**

```
PostDown = iptables -t nat -D POSTROUTING -s 10.20.20.0/24 -j MASQUERADE
```

Perintah ini dijalankan **ketika VPN dimatikan**. Fungsinya Adalah menghapus aturan NAT yang sebelumnya dibuat

- **Start Wireguard**

```
root@vpn:~# systemctl enable wg-quick@wg0
root@vpn:~# systemctl start wg-quick@wg0
```

- **Cek konfigurasi Wireguard**

```
root@vpn:~# wg show
```

```
interface: wg0
  public key: xoc+SNAdGwyPG4/g1Xrv4mcQ8Ib+tThwuC+FgD3rt3g=
  private key: (hidden)
  listening port: 51820
```

```
root@vpn:~# ip a
```

```
inet6 fe80::be24:11ff:fe96:1d58/64 scope link
    valid_lft forever preferred_lft forever
4: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue
    link/none
    inet 10.20.20.1/24 scope global wg0
        valid_lft forever preferred_lft forever
root@vpn:~#
```

## 7. Buka Port di Proxmox

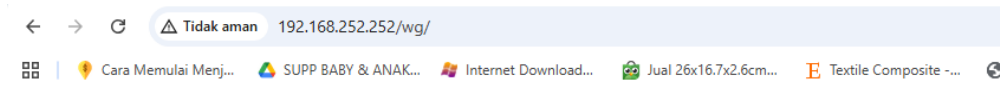
```
root@pve:~# iptables -t nat -A PREROUTING -p udp --dport 51820 -j DNAT --to 10.10.10.5:51820
```

```
root@pve:~# iptables-save > /etc/iptables/rules.v4
```

Rule ini untuk port forwarding yang akan digunakan untuk mengakses server VPN di jaringan internal ketika server VPN berada di VM atau jaringan private

## 8. Instalasi dan konfigurasi Wireguard di Client (Windows)

- Download installer **wireguard** (wireguard-amd64-0.5.3.msi) di Alamat **192.168.252.252/wg** melalui **web browser**.

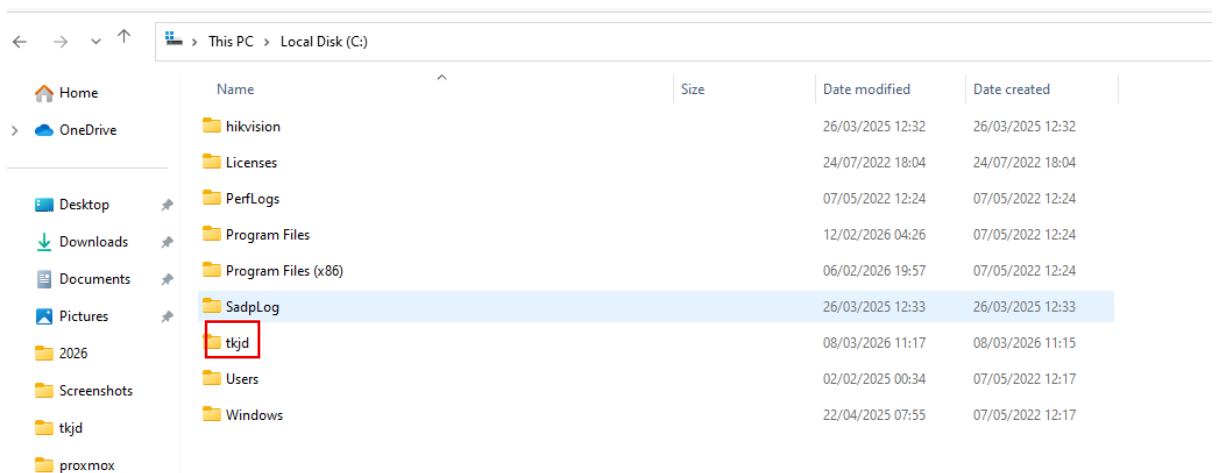


# Index of /wg

| <a href="#">Name</a>                      | <a href="#">Last modified</a> | <a href="#">Size</a> | <a href="#">Description</a> |
|-------------------------------------------|-------------------------------|----------------------|-----------------------------|
| <a href="#">Parent Directory</a>          |                               | -                    |                             |
| <a href="#">wireguard-amd64-0.5.3.msi</a> | 2026-03-09 09:15              | 2.7M                 |                             |
| <a href="#">wireguard-installer.exe</a>   | 2026-03-09 09:15              | 85K                  |                             |

*Apache/2.4.52 (Ubuntu) Server at 192.168.252.252 Port 80*

- Setelah berhasil di download instal **wireguard-amd64-0.5.3.msi**
- Buat folder di drive C, dengan nama kelas masing-masing misalnya kelas XII TKJ D, buat folder dengan nama **tkjd**. Folder ini digunakan untuk menyimpan file konfigurasi **Wierguard**.



- Untuk konfigurasi bisa menggunakan **notepad** atau **text editor** lainnnnya denga isi sperti gambar dibawah ini.

Pengisian **key** di baris **PrivatKey**, dapat dengan cara **copy/paste** dari **key** yang berada di dalam file **client\_private.key** di **vpn**.

Pengisian **key** di baris **PublicKey**, dapat dengan cara **copy/paste** dari **key** yang berada di dalam file **server\_public.key** di **vpn**.

Pada baris Endpoint = 192.168.252.153:51820, **53** diganti XX (no Urut siswa). 192.168.252.1XX => Alamat proxmox masing-masing

```
File Edit View

[Interface]
PrivateKey = OLQMUM5TNJNLBPkvwuUf5kKAesfm2mxx2ojsrUNC8Wg=
Address = 10.20.20.2/24
DNS = 10.10.10.5

[Peer]
PublicKey = xoc+SNAdGwyPG4/g1Xrv4mcQ8Ib+tThwuC+FgD3rt3g=
Endpoint = 192.168.252.153:51820
AllowedIPs = 10.10.10.0/24, 10.20.20.0/24
PersistentKeepalive = 25
```

Kalau sudah selesai **save** dengan nama file **wg0.conf** di folder **tkjx** (x = abjad kelas)

- Tambahkan **client** ke server vpn  
Di **wg0.conf** Server VPN tambahkan seperti gambar dibawah ini.

Pengisian **key** di baris **PublicKey**, dapat dengan cara **copy/paste** dari **key** yang berada di dalam file **client\_public.key** di **vpn**.

```
GNU nano 7.2 /etc/wireguard/wg0.conf *
[Interface]
Address = 10.20.20.1/24
ListenPort = 51820

PrivateKey = mK01/EZeR3fryoIGVNOSTAd2yJv97L2VHiCHzd7omHk=

PostUp = sysctl -w net.ipv4.ip_forward=1
PostUp = iptables -t nat -A POSTROUTING -s 10.20.20.0/24 -j MASQUERADE

PostDown = iptables -t nat -D POSTROUTING -s 10.20.20.0/24 -j MASQUERADE

[Peer]
PublicKey = Zq9E/vr//TDKEDp8ILzb6arRJLrOGYmETsfBHsZmcWc=
AllowedIPs = 10.20.20.2/32
```

Keterangan :

**[Peer]**  
Bagian ini digunakan untuk **mendaftarkan client VPN**.  
Setiap client VPN harus memiliki:  
**Public Key**

Jika ada 5 client:  
akan ada 5 bagian [Peer]

**PublicKey = Zq9E/vr//TDKEDp8ILzb6arRJLrOGYmETsfBHsZmcWc=**

Ini adalah **public key milik client**, fungsinya Adalah untuk mengidentifikasi client yang boleh masuk VPN.

Konsepnya sama seperti **username**

**AllowedIPs = 10.20.20.2/32**

Artinya client ini hanya boleh menggunakan IP 10.20.20.2, CIDR /32 maksudnya hanya untuk 1 IP saja.

Jika ada 3 client:

client1 = 10.20.20.2

client2 = 10.20.20.3

client3 = 10.20.20.4

maka server config menjadi:

[Peer]

AllowedIPs = 10.20.20.2/32

[Peer]

AllowedIPs = 10.20.20.3/32

[Peer]

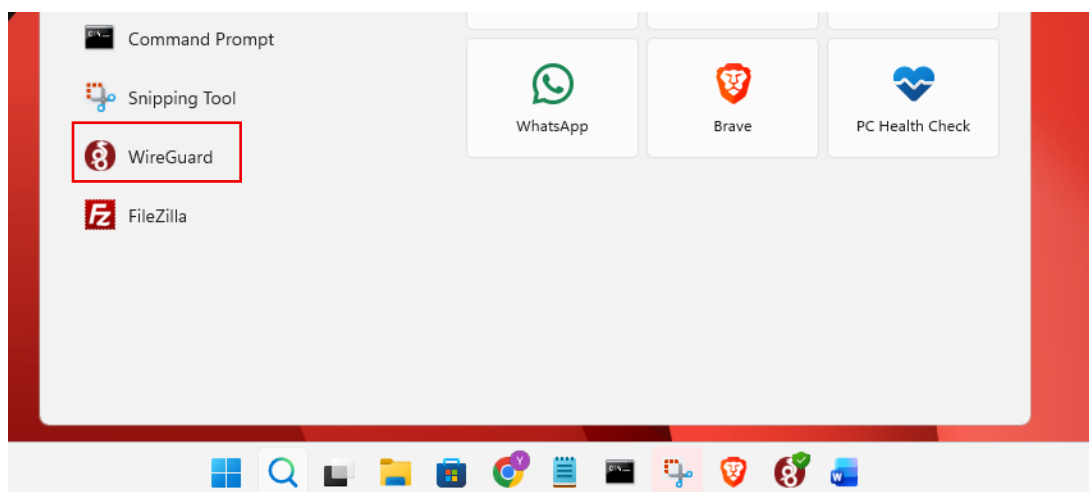
AllowedIPs = 10.20.20.4/32

- **Restart Konfigurasi Wireguard di Server VPN**

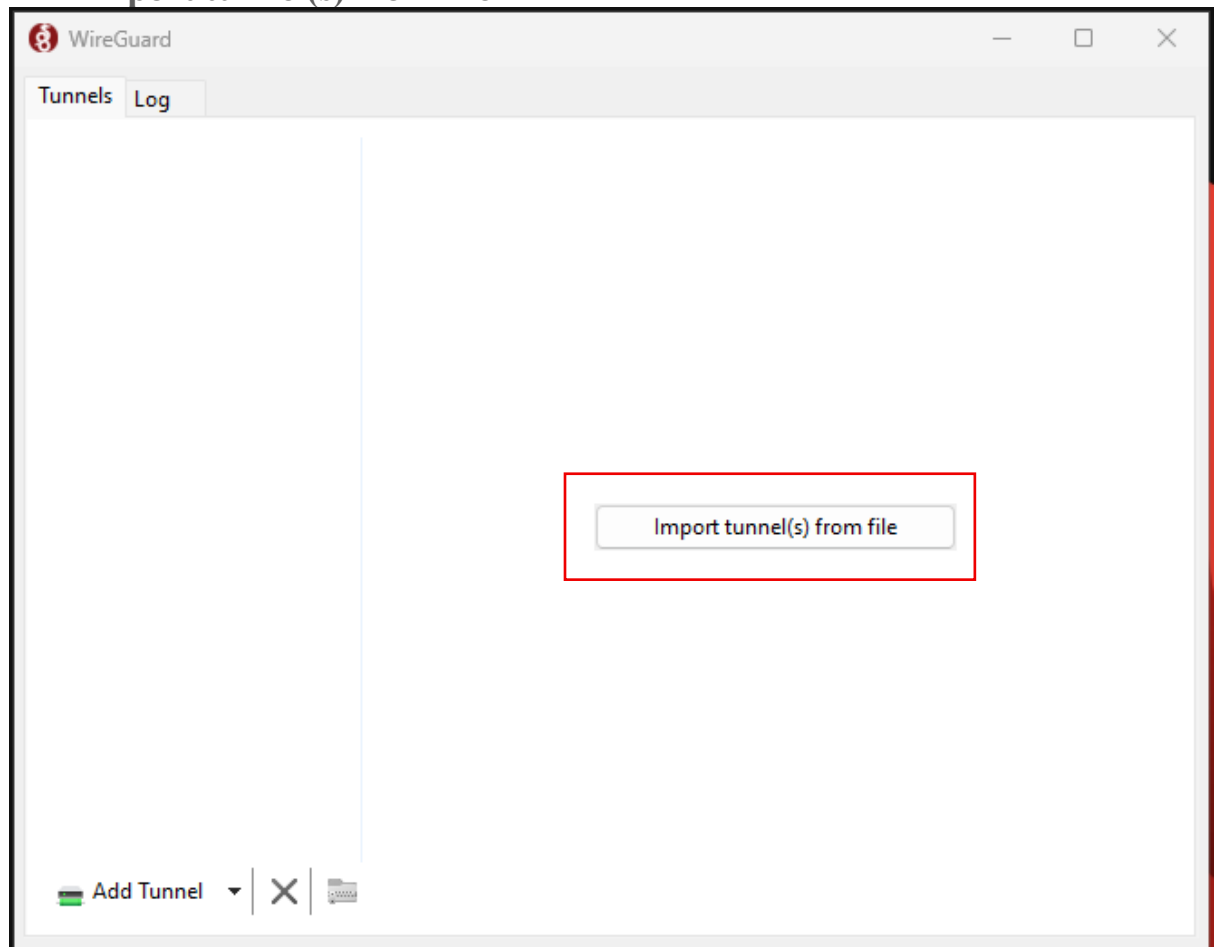
```
root@vpn:~# systemctl restart wg-quick@wg0
```

## 9. Test Hasil Konfigurasi

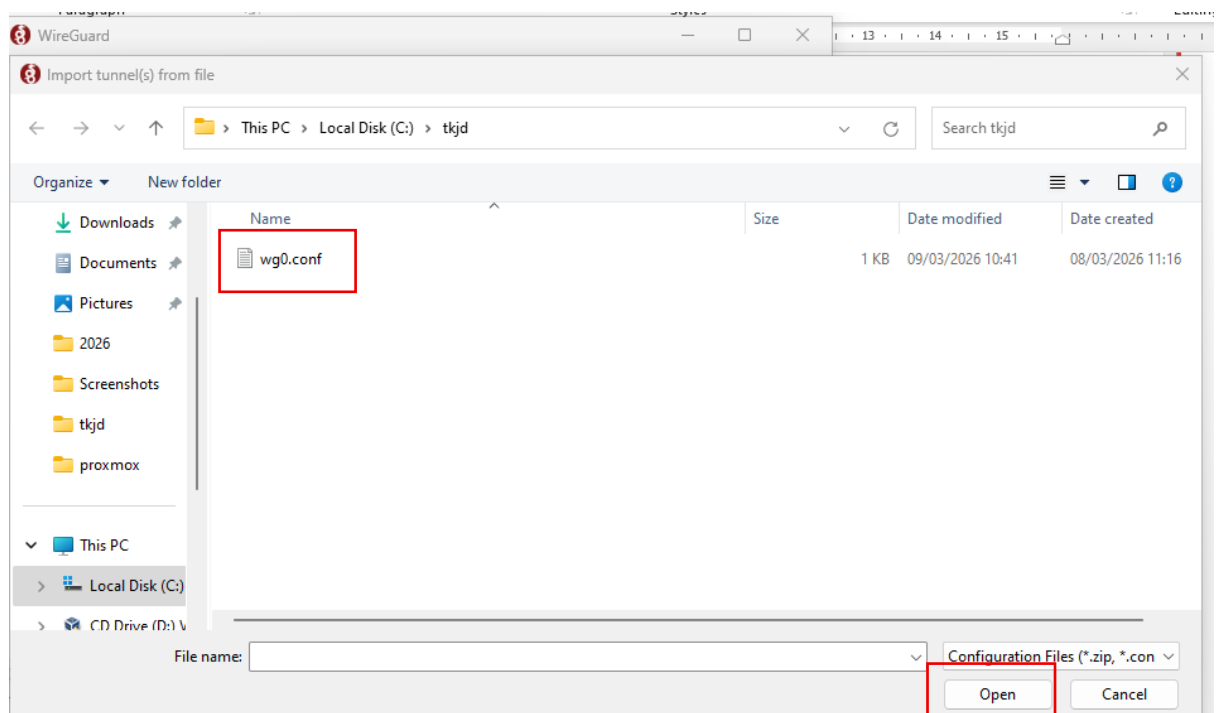
- **Jalankan WireGuard**



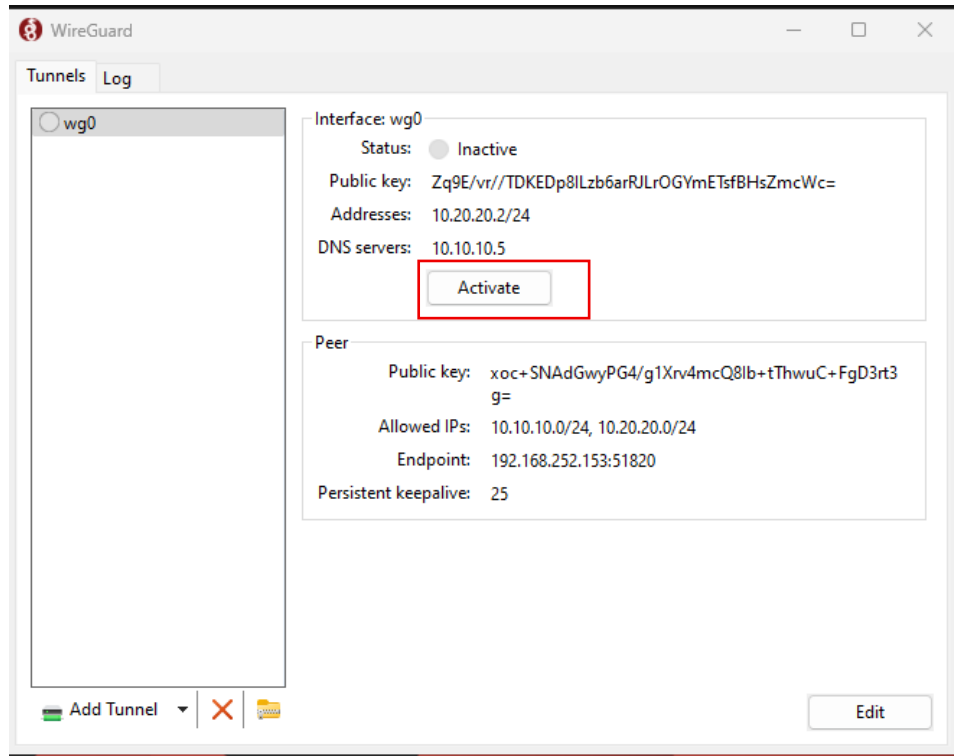
- Klik **import tunnel(s) from file**



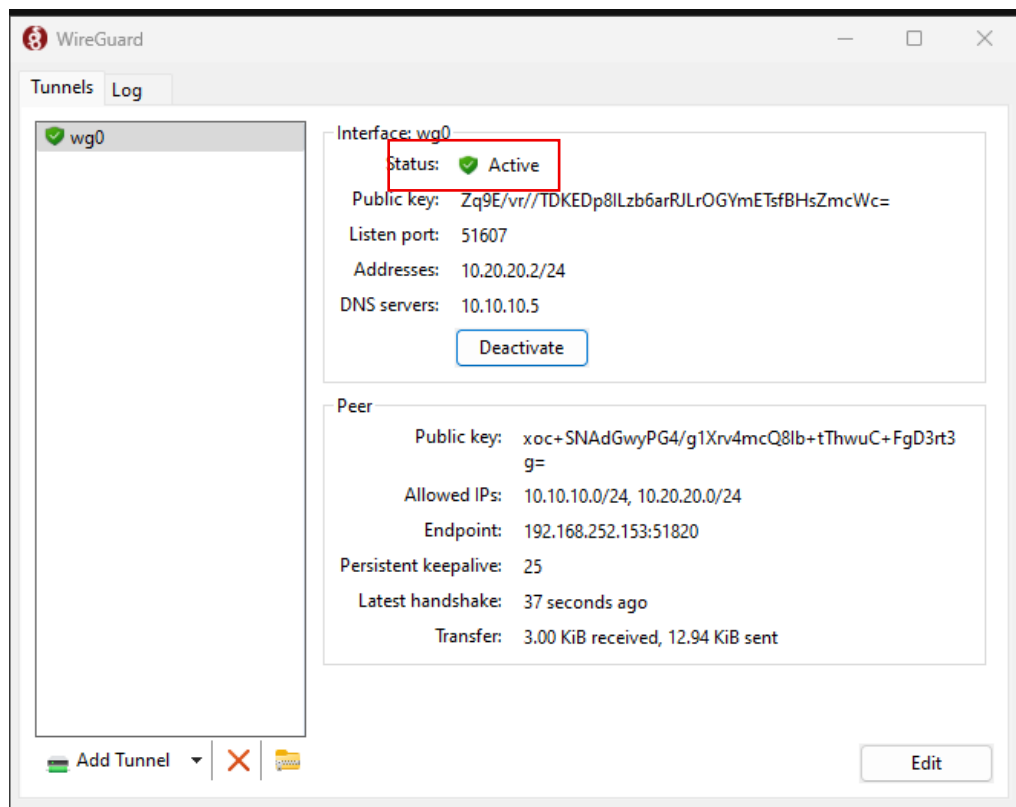
- Pilih file konfigurasi di folder **tkjx** kemudian klik **open**



- Aktifkan WireGuard



Tampilan setelah diaktifkan



- Ping ke IP address Server VPN (10.20.20.1)

```
C:\Users\admin>ping 10.20.20.1

Pinging 10.20.20.1 with 32 bytes of data:
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
Reply from 10.20.20.1: bytes=32 time=1ms TTL=64
```

- Ping ke IP local (VM) misalnya **debian1** (10.10.10.11)

```
C:\Users\admin>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=5ms TTL=63
Reply from 10.10.10.11: bytes=32 time=1ms TTL=63
Reply from 10.10.10.11: bytes=32 time=1ms TTL=63
Reply from 10.10.10.11: bytes=32 time=1ms TTL=63
```

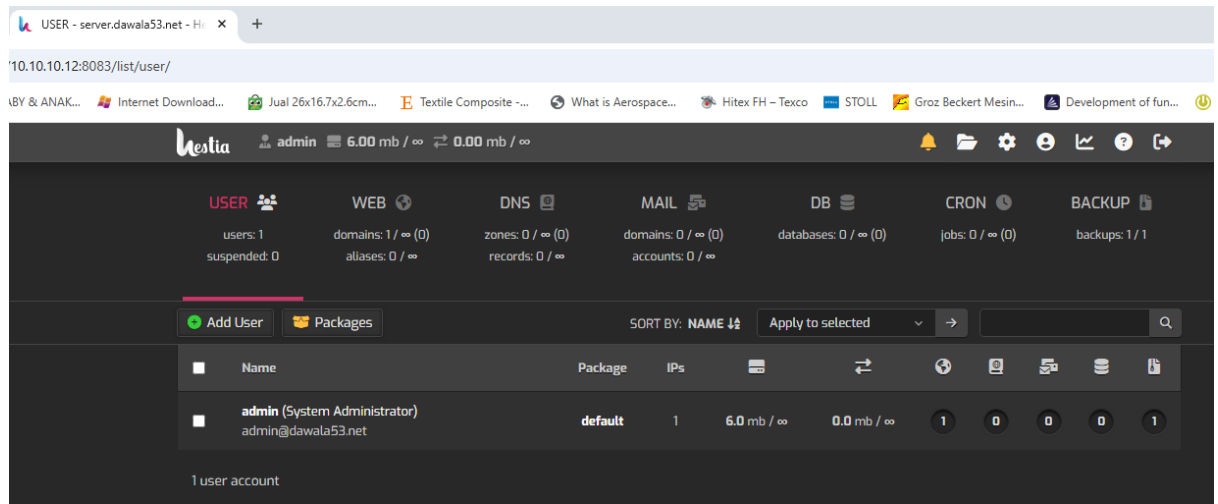
- Akses ke HestiaCP di **debian1** (10.10.10.11) dari web browser :  
[https ://10.10.10.11:8083](https://10.10.10.11:8083)  
**user: admin**  
**password: 123456**

The screenshot shows the HestiaCP web interface. At the top, there's a navigation bar with the Hestia logo and user information (admin, 6.00 mb / ∞, 0.00 mb / ∞). Below this, there are several status cards for different services: USER (1 user, 0 suspended), WEB (1 domain, 0 aliases), DNS (0 zones, 0 records), MAIL (0 domains, 0 accounts), DB (0 databases), CRON (0 jobs), and BACKUP (1 backup). Below these cards, there are buttons for 'Add User' and 'Packages'. A table lists the user accounts, with one user 'admin' (System Administrator) shown. The table has columns for Name, Package, IPs, and various resource usage metrics.

| Name                                              | Package | IPs | 1          | 6.0 mb / ∞ | 0.0 mb / ∞ | 1 | 0 | 0 | 0 | 1 |
|---------------------------------------------------|---------|-----|------------|------------|------------|---|---|---|---|---|
| admin (System Administrator)<br>admin@cepot53.net | default | 1   | 6.0 mb / ∞ | 0.0 mb / ∞ | 1          | 0 | 0 | 0 | 0 | 1 |

1 user account

- Akses ke **HestiaCP** di **debian1 (10.10.10.12)** dari web browser :  
**https ://10.10.10.12:8083**  
**user: admin**  
**password: 123456**



Jika seluruh pengujian berhasil, seperti ping ke IP server VPN (10.20.20.1), ping ke IP Debian1 (10.10.10.11) dan Debian2 (10.10.10.12), serta akses ke panel HestiaCP melalui alamat IP lokal (10.10.10.11 dan 10.10.10.12) dapat dilakukan dengan baik, maka dapat disimpulkan bahwa konfigurasi VPN WireGuard telah berhasil dan client sudah dapat terhubung ke jaringan internal server dengan aman melalui tunnel VPN.

## Job 5 : Konfigurasi HestiaCP

Pada job ini kita akan belajar bagaimana mengelola server / hosting menggunakan **Control Panel**, seperti mengelola domain website, mail, dan database

### KONFIGURASI DI DEBIAN1 (10.10.10.11)

Menambah domain [www.cepotxx.net](http://www.cepotxx.net)

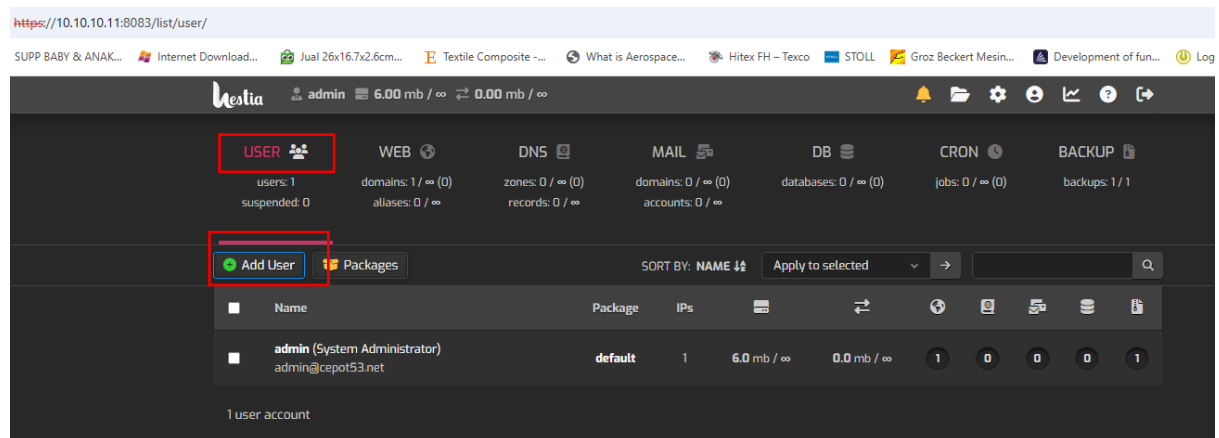
1. Akses ke **Control Panel HestiaCP** di **debian1** (10.10.10.11)

<https://10.10.10.11:8083>

masuk dengan user: **admin**, password: **123456**

2. Menambah user baru

klik menu **users** kemudian **add user** seperti gambar berikut.



Silahkan tambahkan user baru di HestiaCP untuk kebutuhan add domain Kita.

User : **userxx** (xx : nomor urut siswa)

Password: **Tekaje2026**

Setelah selesai membuat user kemudian klik **save**

**Save**

## Add User

**Username**

user53

**Contact Name**

**Email**

yuwana@smkn1gmb.net

**Password** 

Tekaje2026

Password must include:

- 8 characters minimum
- 1 uppercase & 1 lowercase character
- 1 number

☐ Do not allow user to log in to Control Panel

☐ Send welcome email

### 3. Masuk ke user **admin**

| USER  | WEB  | DNS  |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| users: 2<br>suspended: 0                                                                 | domains: 1 / ∞ (0)<br>aliases: 0 / ∞                                                    | zones: 0 / ∞ (0)<br>records: 0 / ∞                                                      |

**Add User** **Packages**

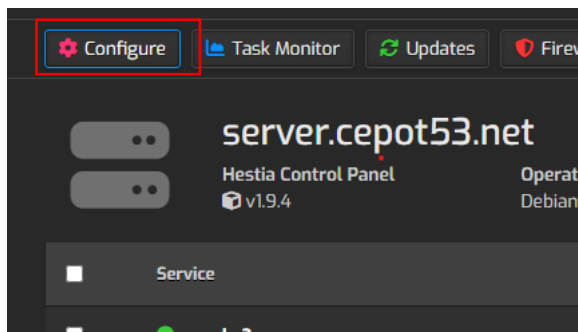
| Name                                                     |
|----------------------------------------------------------|
| <b>admin</b> (System Administrator)<br>admin@cepot53.net |
| user1 (user1)<br>yuwana@smkn1gmb.net                     |

Kemudian pilih **server setting**, di menu bagian atas

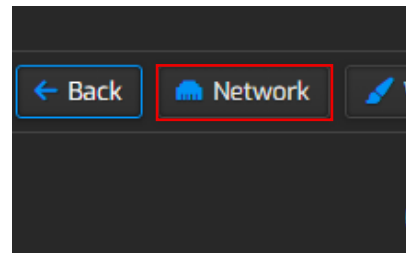
      

| DB  | CRON  | BACKUP  |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| databases: 0 / ∞ (0)                                                                   | jobs: 0 / ∞ (0)                                                                          | backups: 1 / 1                                                                             |

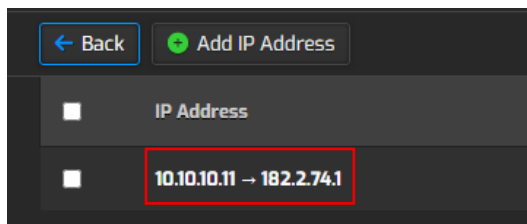
Klik **Configure**



Klik **Network**



Edit IP Address



Kosongkan IP pada bagian **NAT IP -Association** kemudian klik **Save**

**Edit IP Address**

IP Address  
10.10.10.11

Netmask  
255.255.255.0

Interface  
eth0

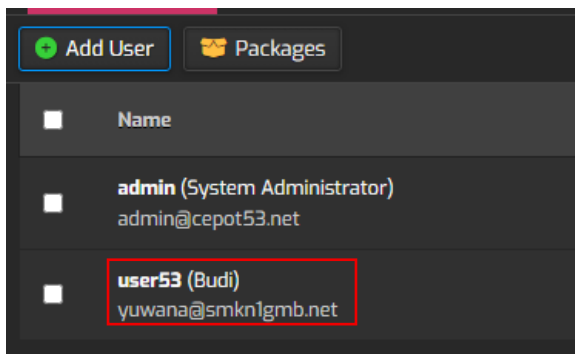
☒ Shared

Assigned Domain (Optional)

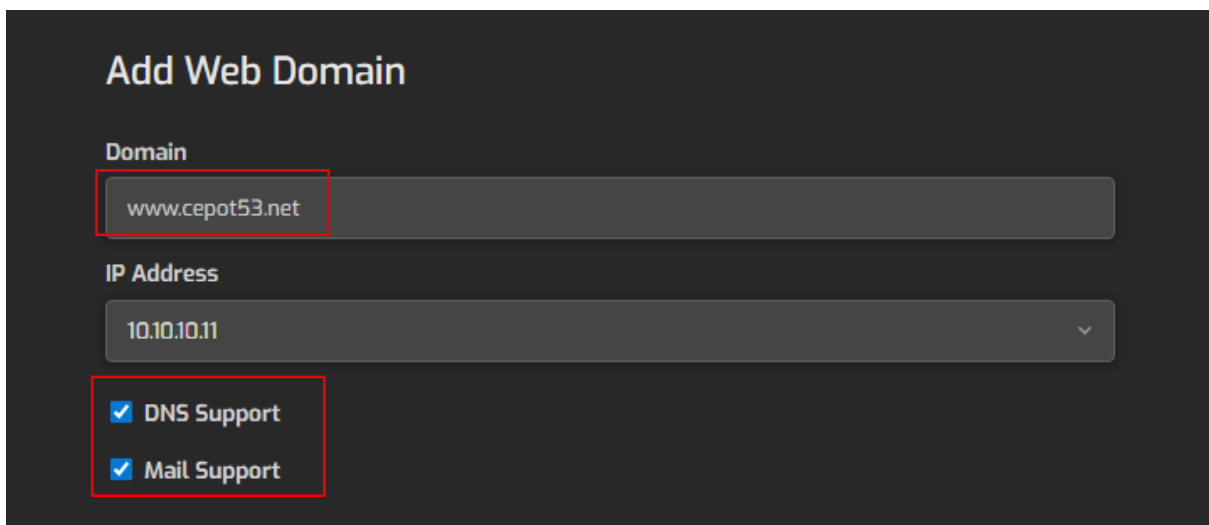
NAT IP Association (Optional)

Save

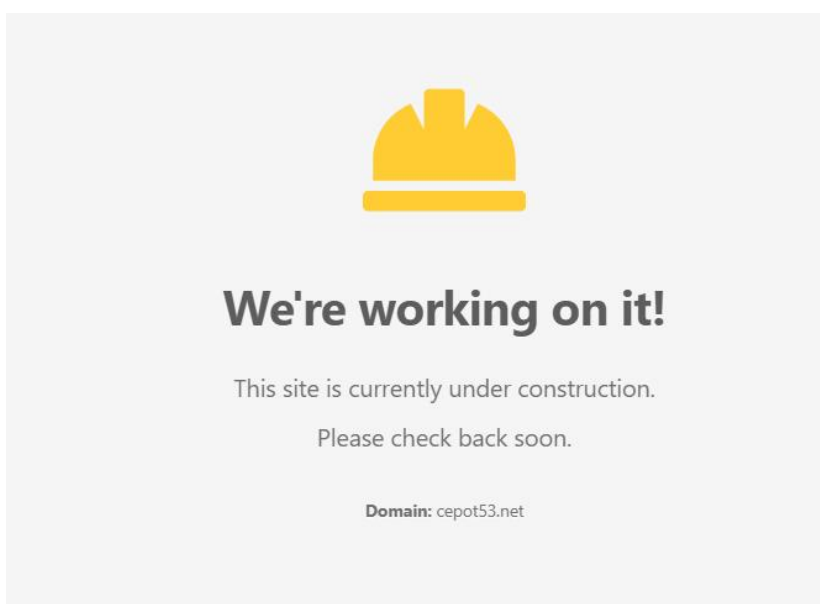
4. Login dengan **userxx**



5. klik **Add Web Domain**, kemudian isikan nama domain dan centang seperti gambar dibawah ini, setelah selesai klik **Save**

A screenshot of the 'Add Web Domain' form. The title 'Add Web Domain' is at the top. Below it are three fields: 'Domain' (containing 'www.cepot53.net'), 'IP Address' (containing '10.10.10.11'), and two checkboxes: 'DNS Support' and 'Mail Support', both of which are checked. A red rectangular box highlights the 'Domain' field, the 'IP Address' field, and the two checked checkboxes.

[www.cepot53.net](http://www.cepot53.net)



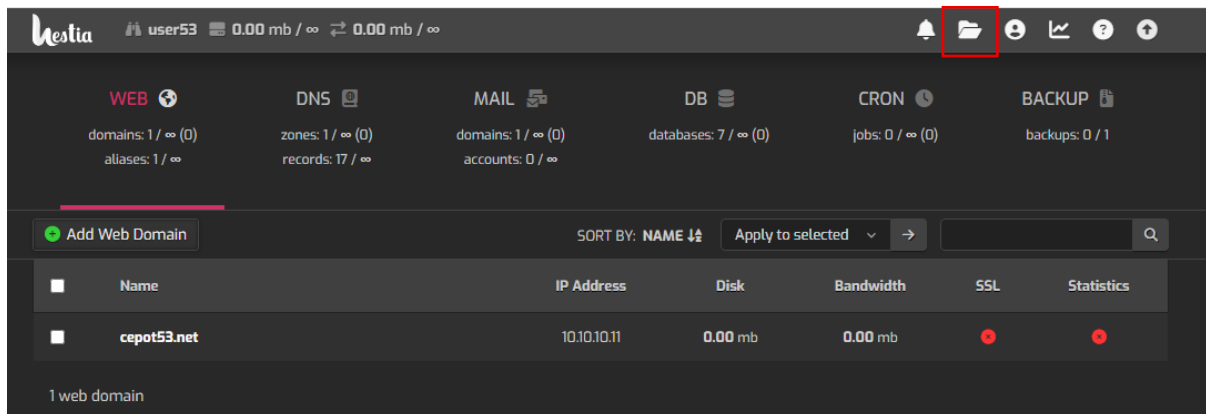
# TUGAS :

## TUGAS 1

Ubah tampilan website : [www.cepot53.net](http://www.cepot53.net)

Tampilan bebas ,

Untuk upload halaman web, bisa menggunakan **file manager** HestiaCP



Di upload ke direktori **/home/web/cepoxx.net/public\_html**

Bisa diupload melalui **filezilla**, kalau yang mau di upload bebebrapa file sekaligus.

Kalau mau menggunakan **FileZila**:

**Host : sftp://10.10.10.11**

**Username: userxx**

**Pasword: Tekaje2026**

**Port: 22**

Di upload ke **/home/user53/web/cepot53.net/public\_html**

Dapat nilai lebih jika halaman web yang diakses Adalah halaman web + database, jadi bisa untuk input data misalnya dan hasilnya ditampilkan di web ( bisa di cari di internet contohnya yang sudah jadi)

Boleh juga menggunakan web aplikasi bawaan hestiaCP, caranya bisa lihat link dibawah ini:

<https://www.rumahweb.com/journal/cara-add-domain-dan-install-website-di-hestiacp/>

catatan :

Kalau mau menggunakan database di HestiaCP, harus mengedit file **apache2.conf**, supaya bisa menggunakan **phpMyAdmin**

Langkahnya sebagai berikut :

Buka file **apache2.conf**

```
root@server:~# nano /etc/apache2/apache2.conf
```

Tambahkan baris **IncludeOptional conf.d/phpmyadmin.inc**

Pada bagian dibawah ini

```
IncludeOptional conf.d/*.conf
IncludeOptional conf.d/domains/webmail/*.conf
IncludeOptional conf.d/domains/*.conf
IncludeOptional conf.d/phpmyadmin.inc
```

Simpan kemudian restart

```
root@server:~# /etc/init.d/apache2 restart
```

## TUGAS 2

Setting **Mail Server di HestiaCP**, minimal membuat dua user dan bisa saling kirim.

### Petunjuk1:

Tambahkan domain **mail.cepot53.net** di **dnsmasq**

Langkahnya :

Masuk ke terminal **proxmox**, kemudian buka file konfigurasi **dnsmasq**

```
root@pve:~# nano /etc/dnsmasq.d/domain.conf
```

Tambahkan baris dibawah ini

```
address=/www.cepot53.net/192.168.252.153
address=/www.dawala53.net/192.168.252.153
address=/mail.cepot53.net/192.168.252.153
```

Simpan kemudian restart **dnsmasq**

```
root@pve:~# systemctl restart dnsmasq.service
```

## Petunjuk2

Masuk ke terminal **Proxy**

Buka file konfigurasi **nginx**

```
root@proxy:~# nano /etc/nginx/sites-available/proxy
```

Setelaha terbuka tambahkan baris – baris ini pada bagian bawah

```
server {  
    listen 80;  
    server_name mail.cepote53.net;  
  
    location / {  
        proxy_pass http://10.10.10.11;  
        proxy_set_header Host $host;  
    }  
}
```

Restart nginx

```
root@proxy:~# systemctl restart nginx.service
```

**mail.cepote53.net**

mail.cepote53.net

SUPP BABY & ANAK... Internet Download... Jual 26x16.7x2.6cm... E Textile Composite -... What is Aerospace... Hitex FH – Texco STOLL



LOGIN

Roundcube Webmail

S

### TUGAS 3

- Menambahkan domain [www.](#) di **hestiaCP** Debian2
- Ubah tampilan webnya, tampilan bebas.
- Setting Mail Server sampai bisa saling mengirim
- Tambahkan satu domain lagi **tkj. dawalaxx.net**, tampilan web bebas.