

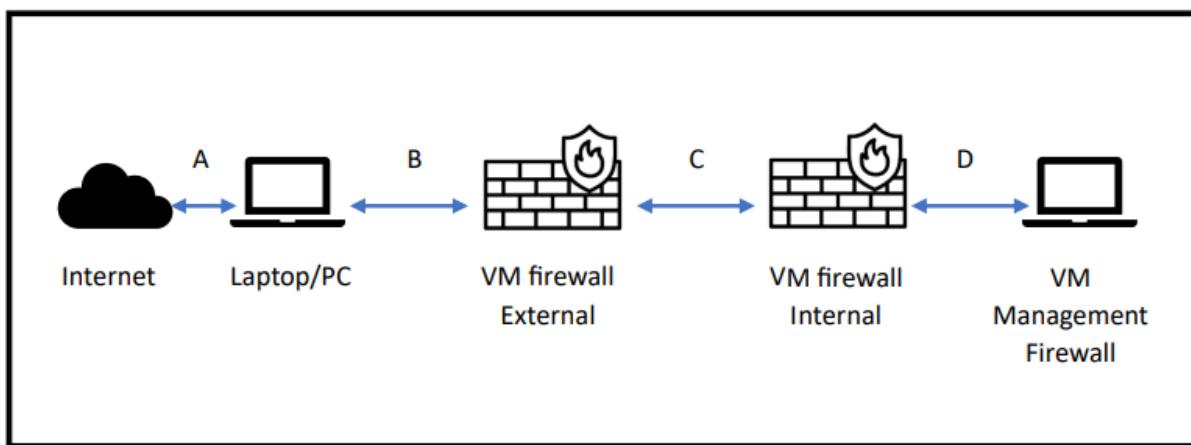
IMPLEMENTASI INTERNAL DAN EXTERNAL FIREWALL

I. PENDAHULUAN

Firewall adalah sistem keamanan jaringan yang berfungsi sebagai pengontrol akses antara jaringan internal (yang dianggap aman) dan jaringan eksternal (seperti internet, yang dianggap tidak aman). Firewall bekerja sebagai penghalang yang memeriksa dan memfilter lalu lintas jaringan berdasarkan aturan keamanan yang telah ditetapkan, mencegah akses yang tidak sah dan ancaman dari luar. Firewall melindungi jaringan dengan memonitor dan mengendalikan data yang masuk dan keluar berdasarkan kriteria tertentu seperti alamat IP, port, dan protokol. Cara kerjanya dapat bervariasi tergantung pada jenis firewall yang digunakan

II. ALAT DAN BAHAN

- Laptop dengan minimal RAM 8 GB dan Free Storage 100 GB
- Hypervisor: Virtualbox / VMWare Workstation / Hyper-V / Qemu/KVM
- PfSense
- OPNSense
- Alma Llinux / Rocky Linux / RHEL
- Topologi :



1. Merupakan koneksi antara internet dan laptop/PC, dapat berupa wired ataupun wireless
2. Merupakan koneksi antara Laptop dengan lingkungan virtual dengan koneksi tipe NAT
3. Merupakan koneksi antara VM Firewall External dan VM Firewall Internal dengan koneksi tipe "Internal Network (Virtualbox)" atau "LAN Segment (VMware)" dan subnet jaringan 10.10.10.0/24

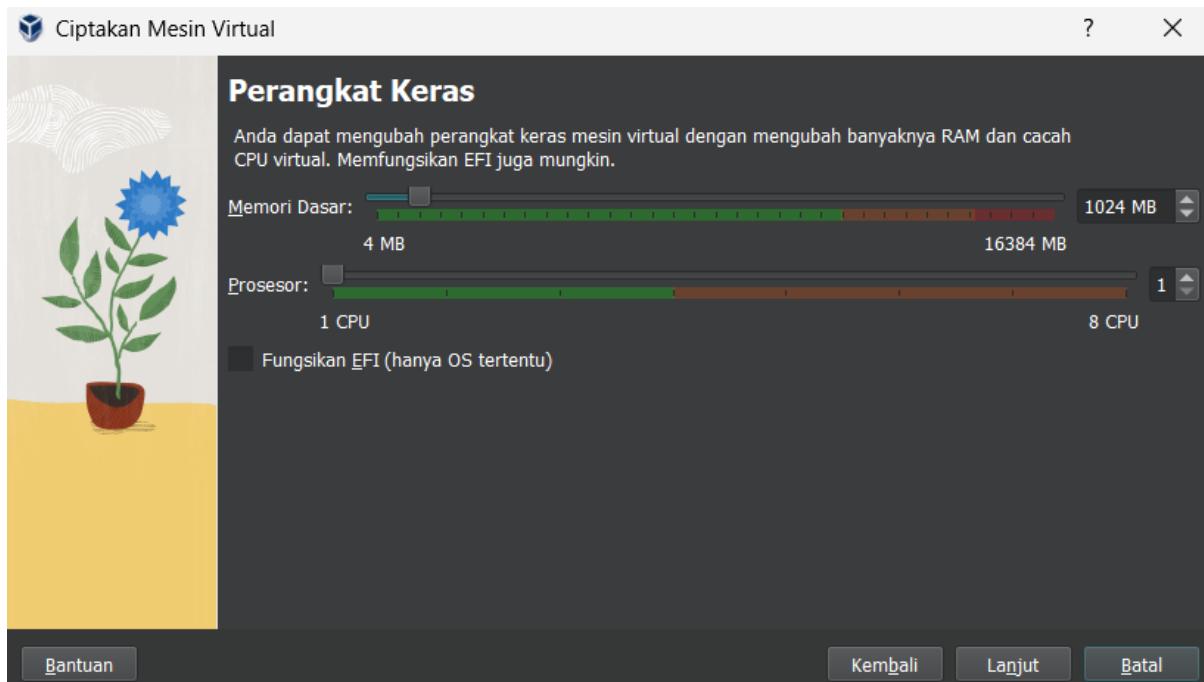
- Merupakan koneksi antara VM Firewall Internal dan VM Management Firewall dengan koneksi tipe "Internal Network (Virtualbox)" atau "LAN Segment (VMware)" dan subnet jaringan 10.10.20.0/24

III. Install pfSense – VM firewall external

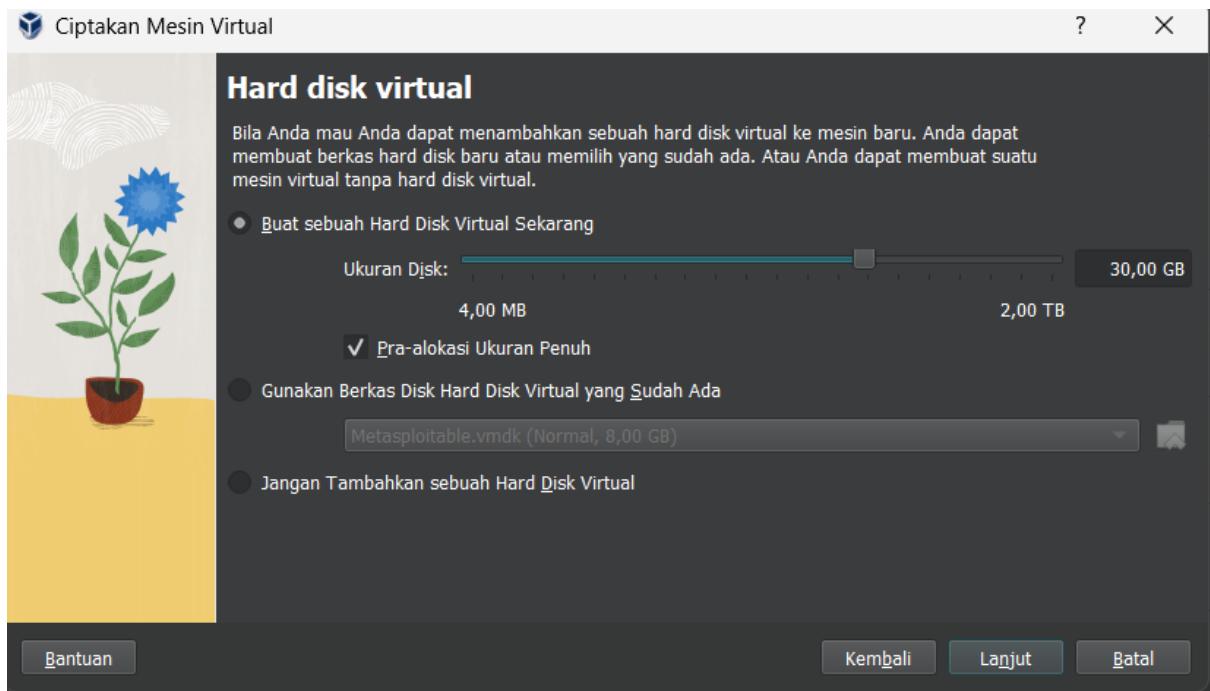
- Install pfSense pada virtual mesin



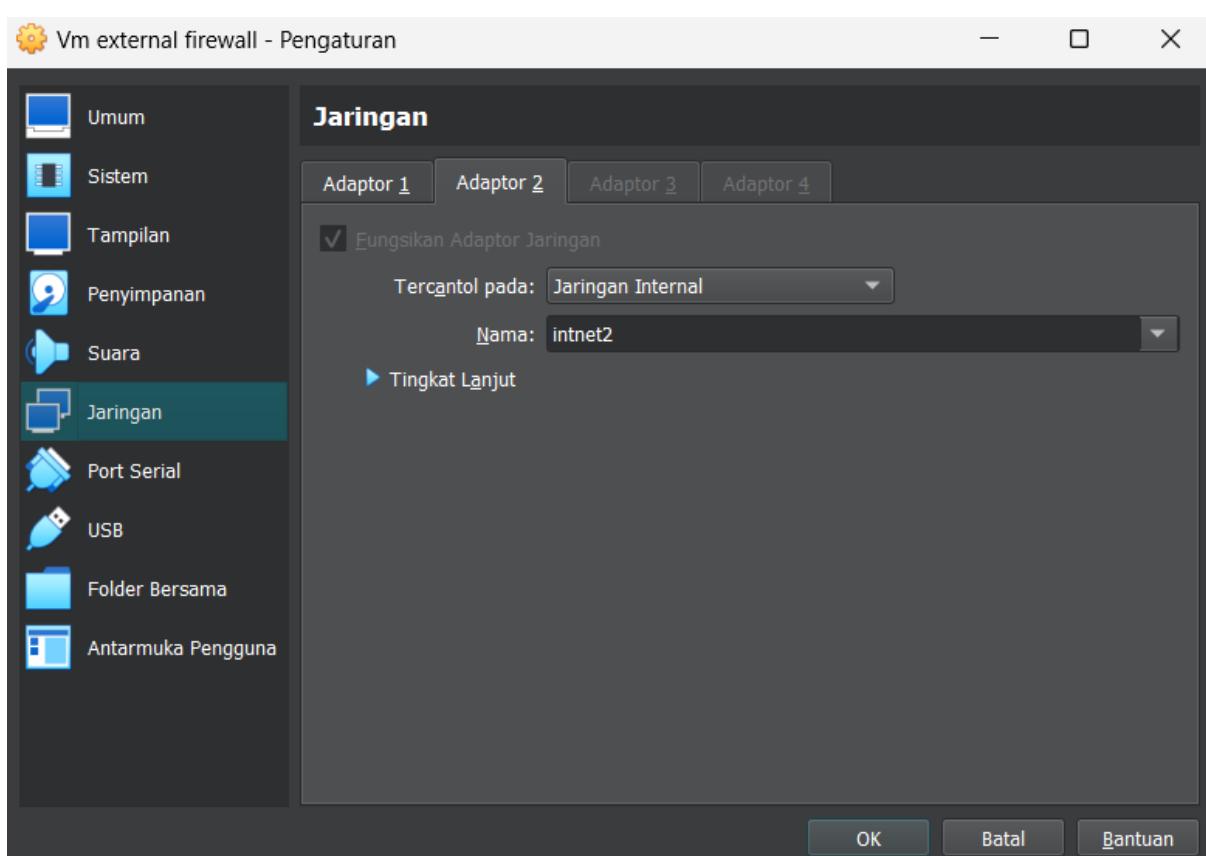
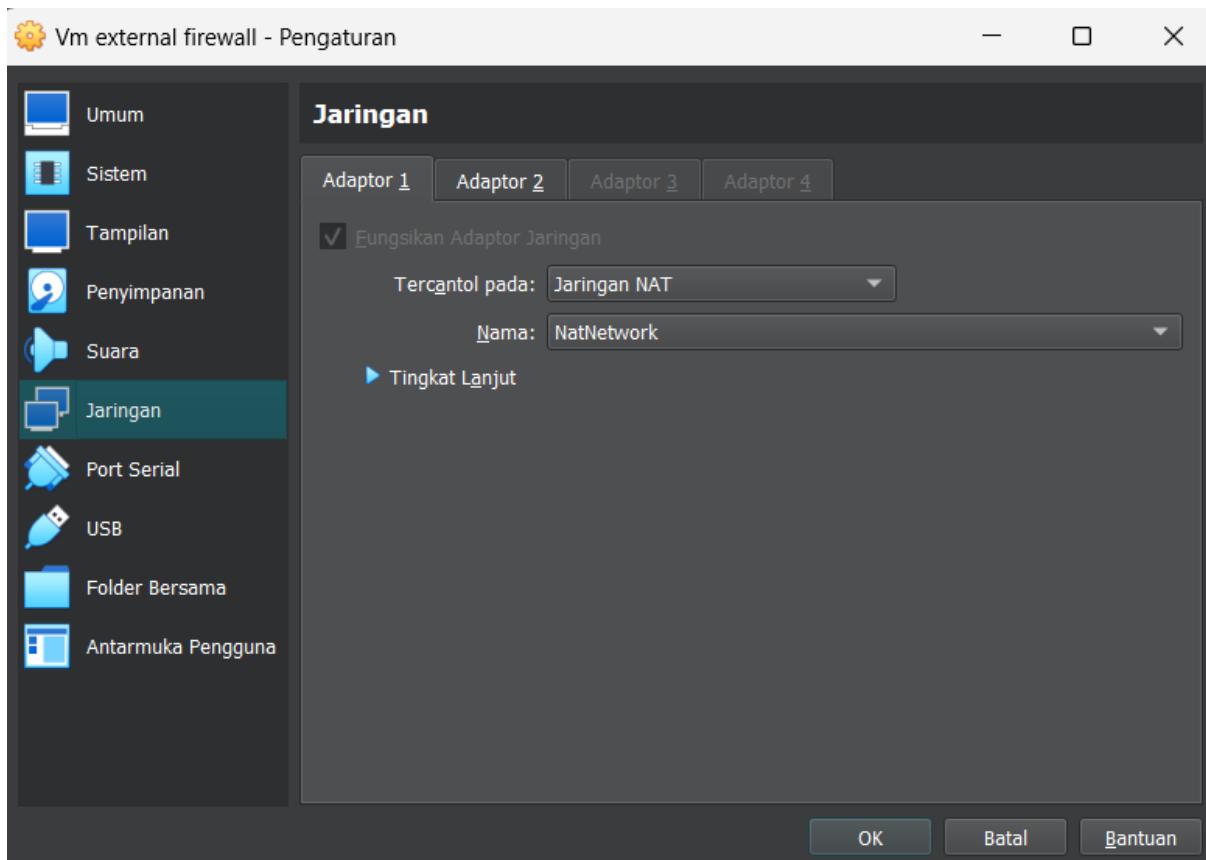
- Setting ram dan cpu vm firewall external



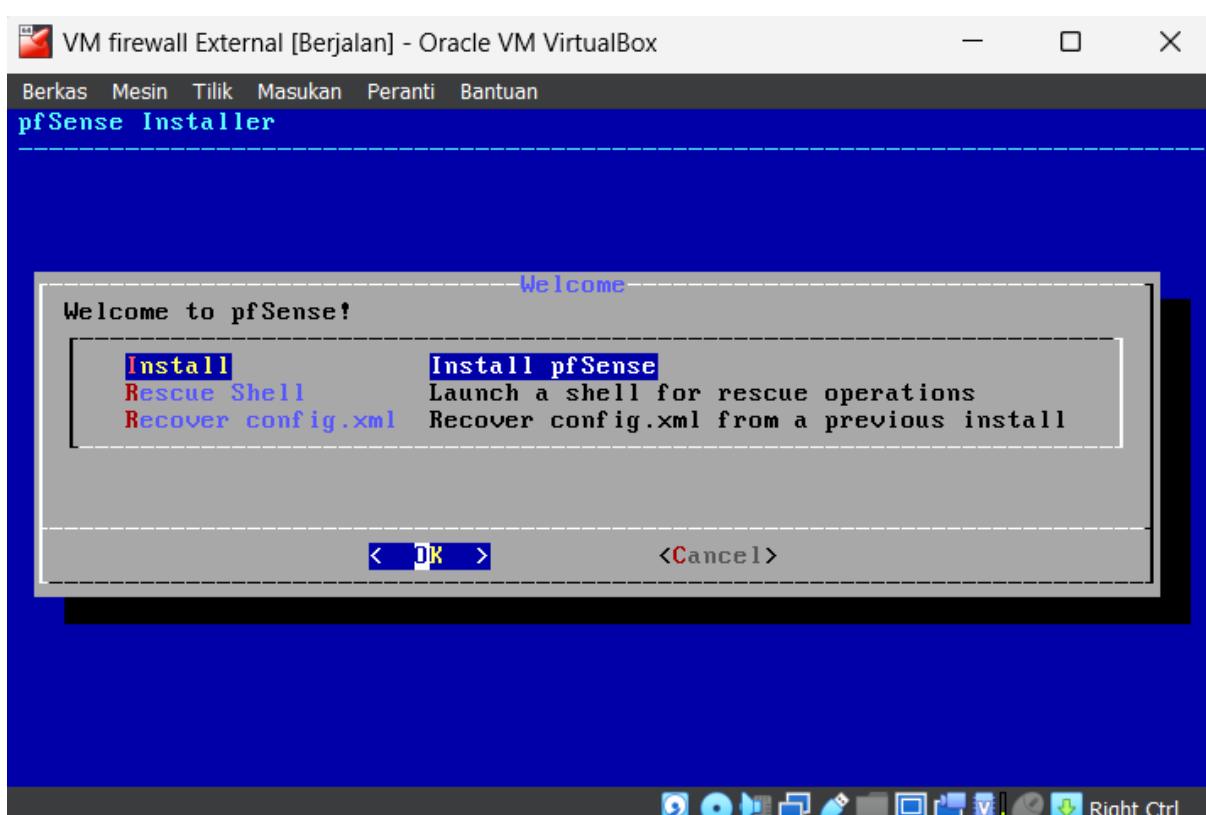
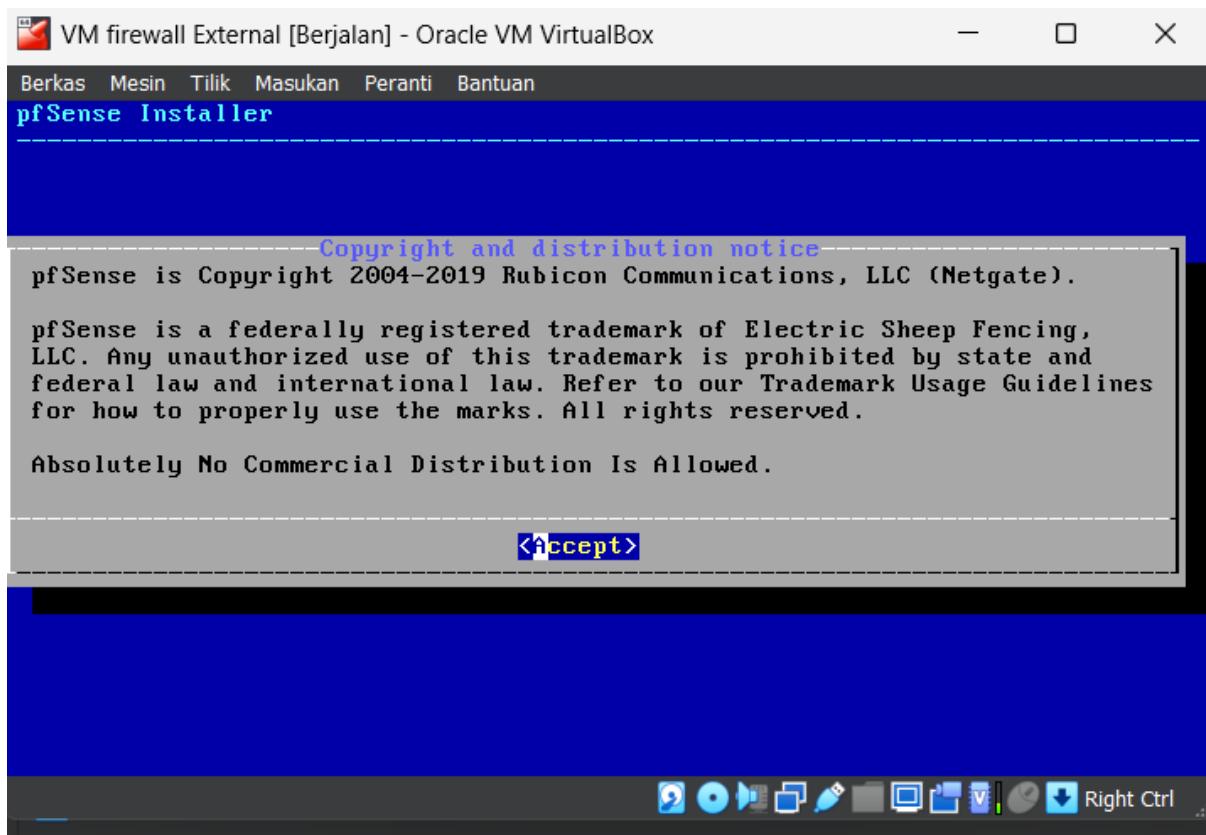
3. Setting penyimpanan sebesar 30gb

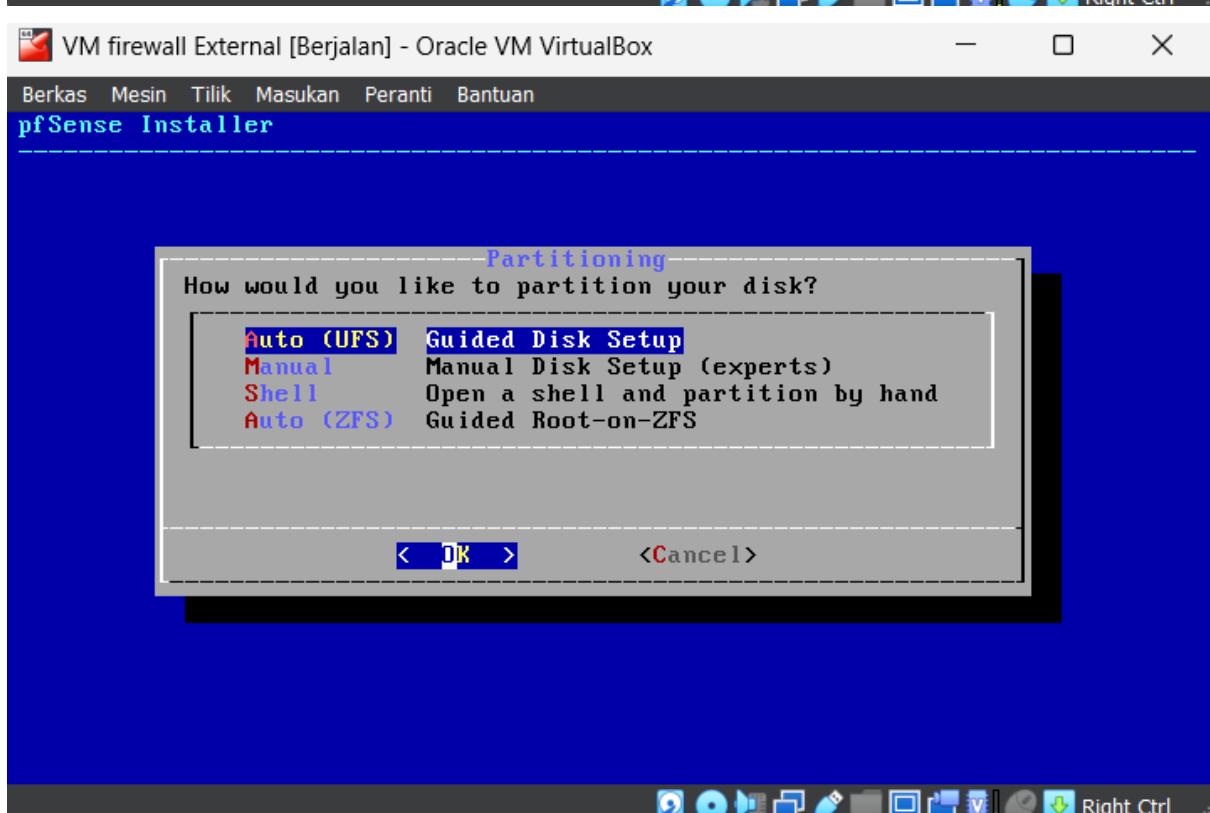
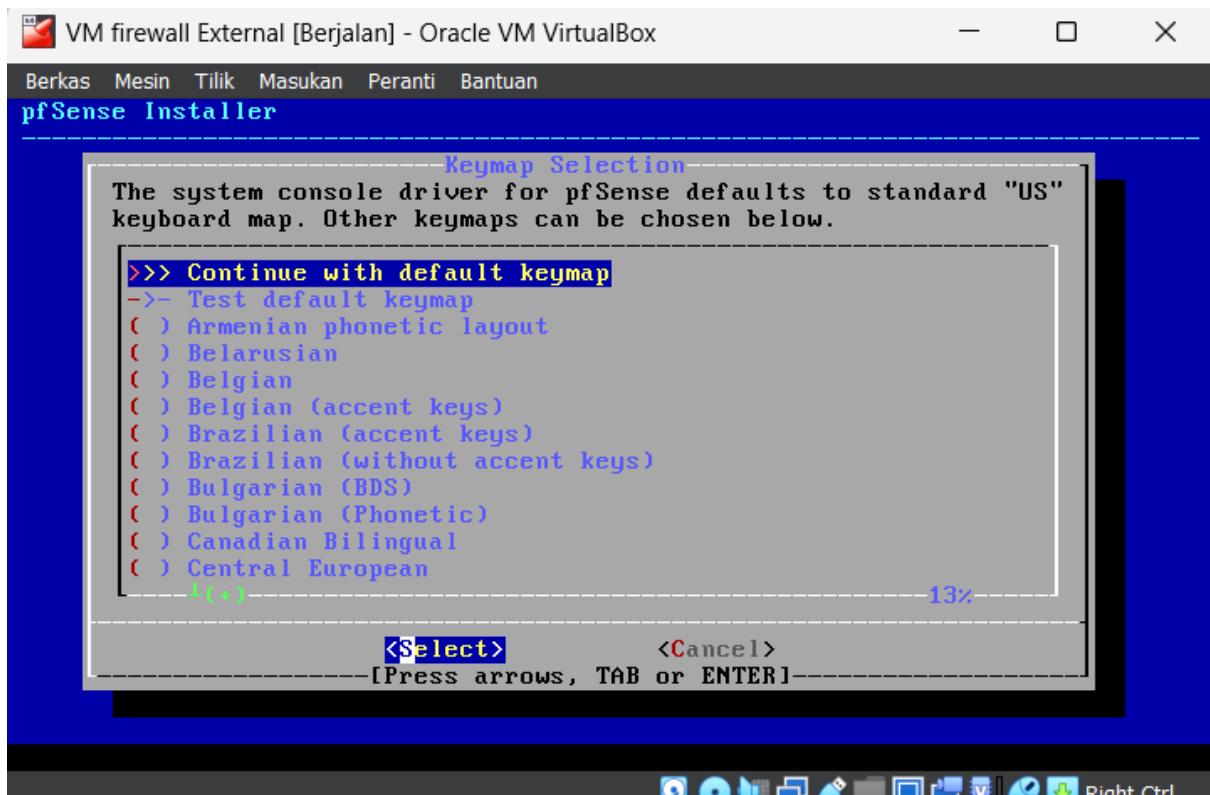


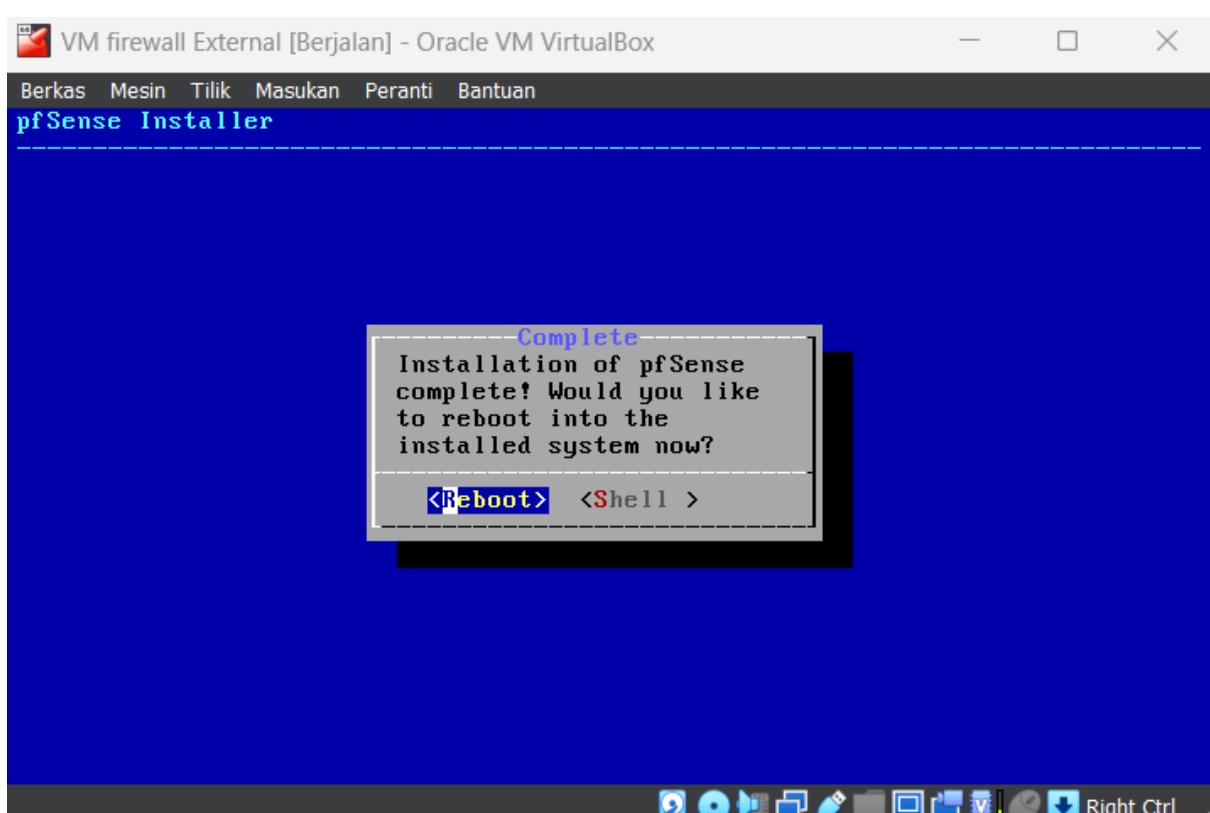
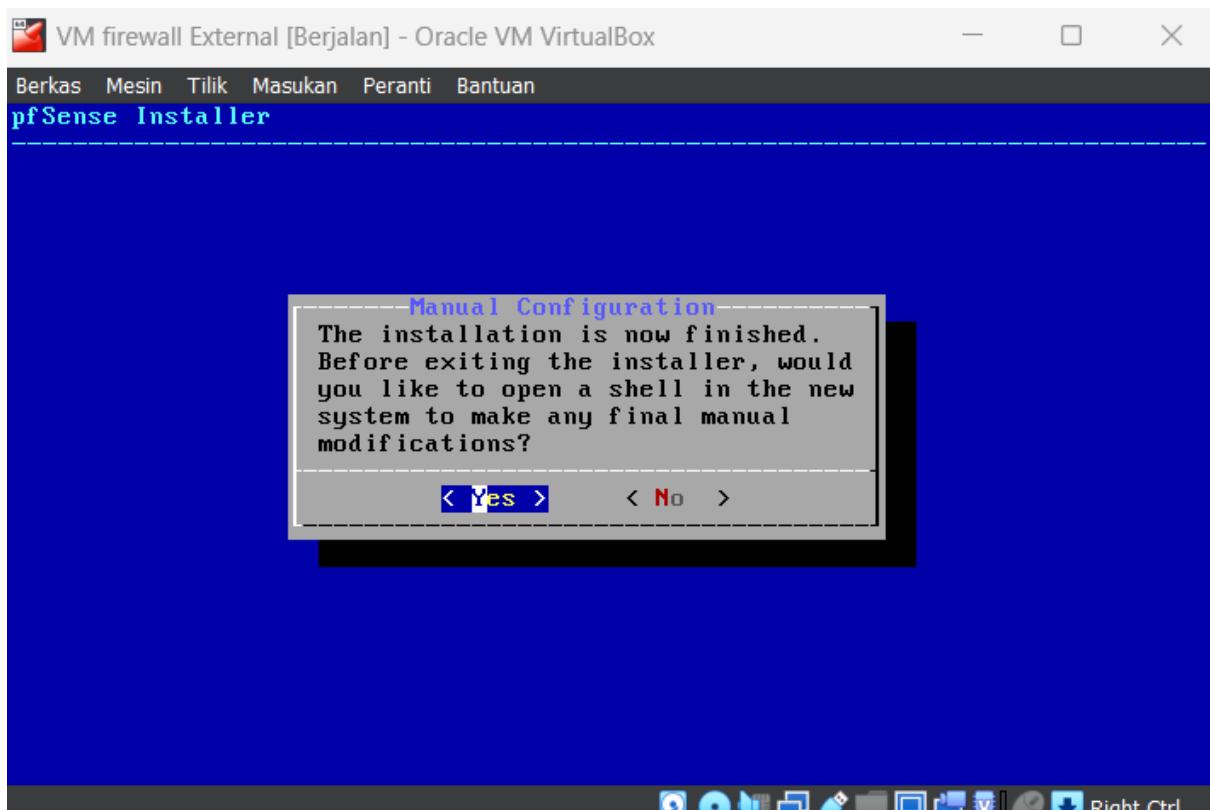
4. Setting jaringan firewall external menggunakan jaringan NAT dan jaringan internal intnet2



5. Instalasi pfSense







```

VM firewall External [Berjalan] - Oracle VM VirtualBox

Berkas Mesin Tilik Masukan Peranti Bantuan
5) Reboot system      14) Enable Secure Shell (sshd)
6) Halt system        15) Restore recent configuration
7) Ping host          16) Restart PHP-FPM
8) Shell

Enter an option: clear

VirtualBox Virtual Machine - Netgate Device ID: c4b4fab04ae5dc65aae1

*** Welcome to pfSense 2.4.5-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

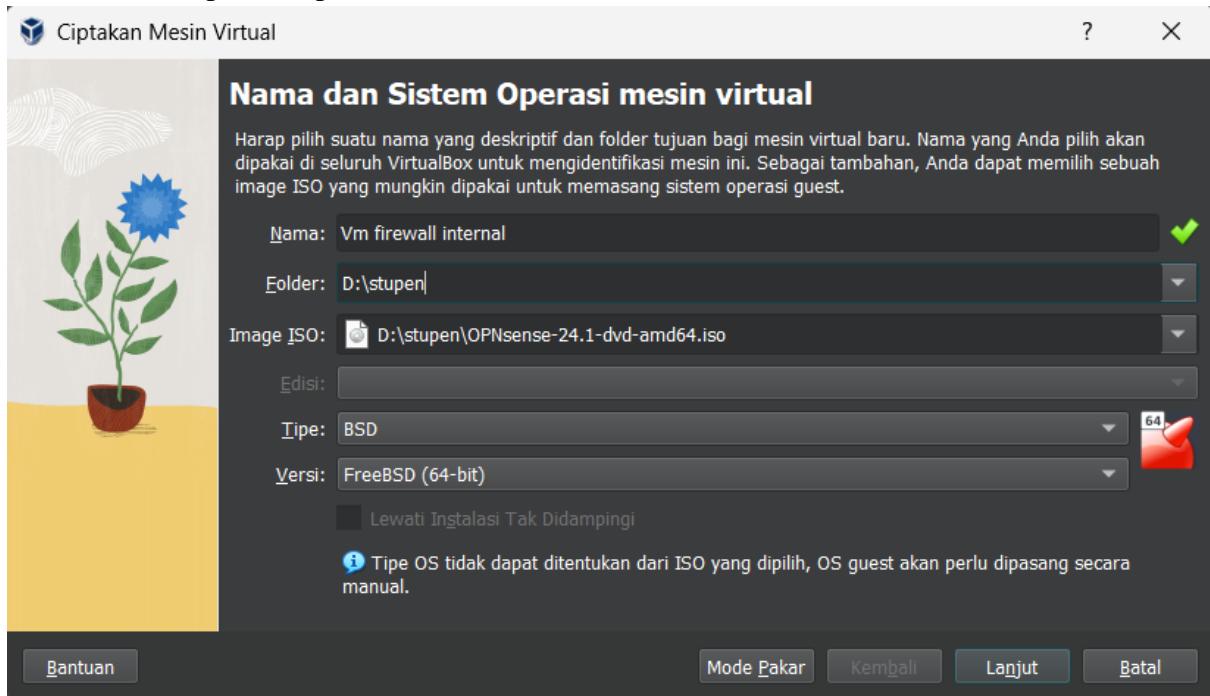
0) Logout (SSH only)      9) pfTop
1) Assign Interfaces       10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system          14) Enable Secure Shell (sshd)
6) Halt system            15) Restore recent configuration
7) Ping host              16) Restart PHP-FPM
8) Shell

Enter an option: 

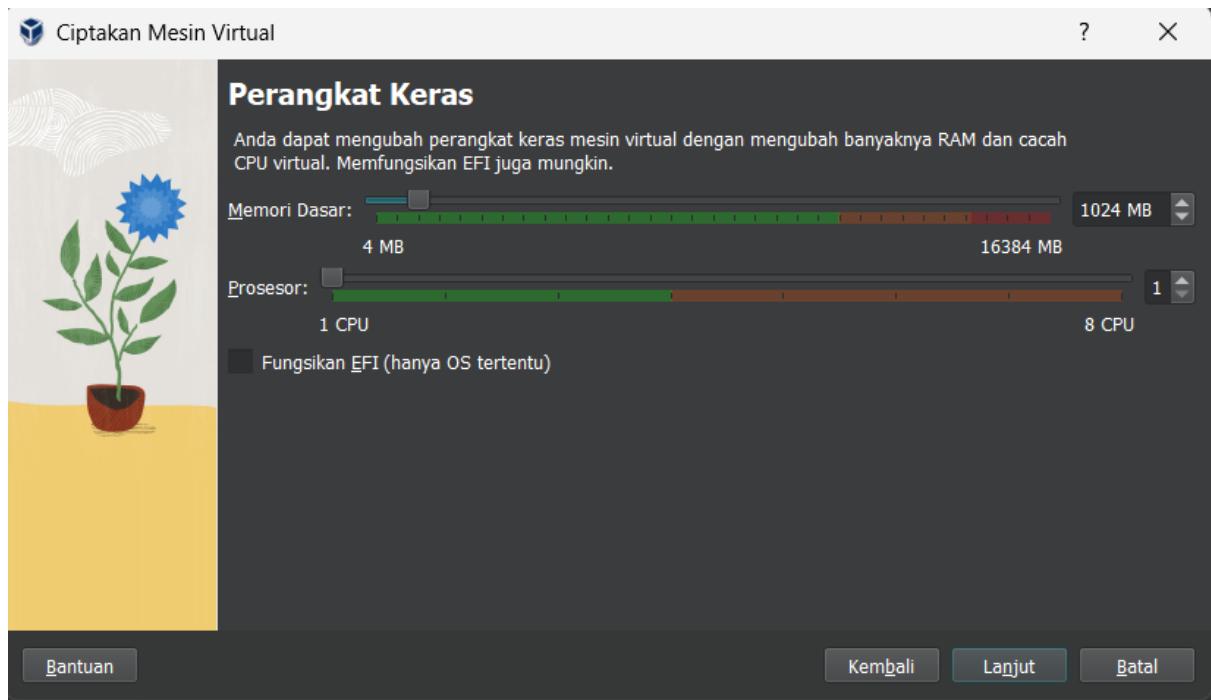
```

IV. Install OPNSense – VM firewall internal

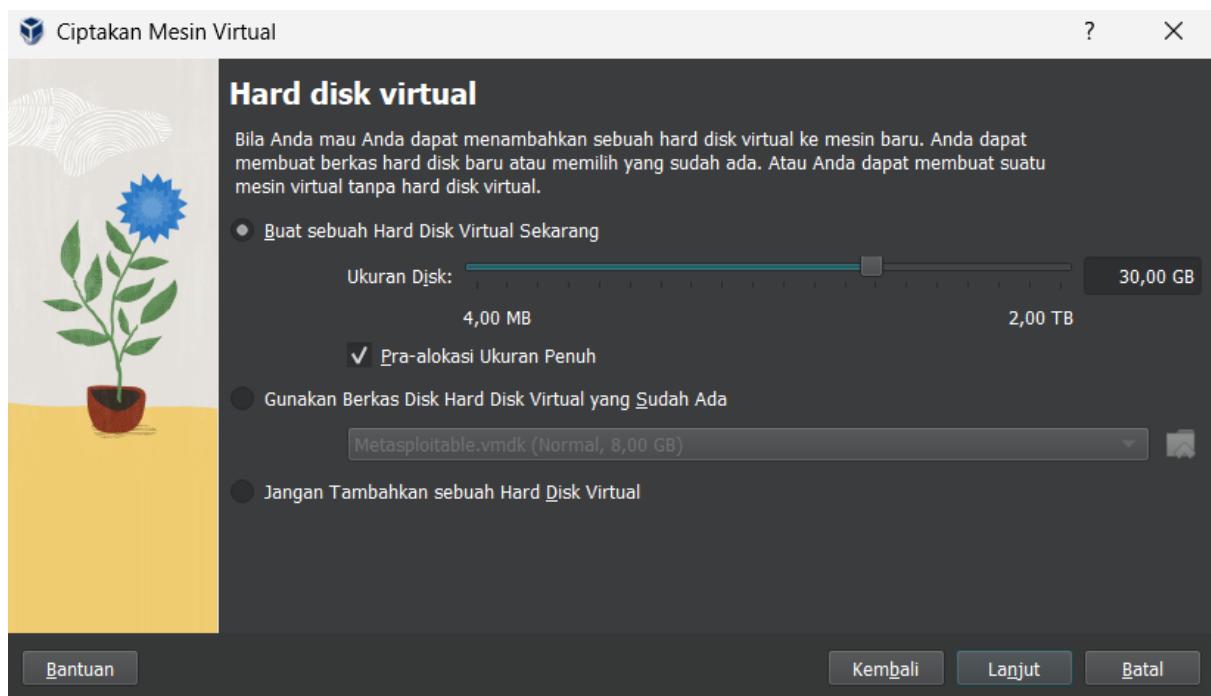
1. Install opnsense pada virtualbox



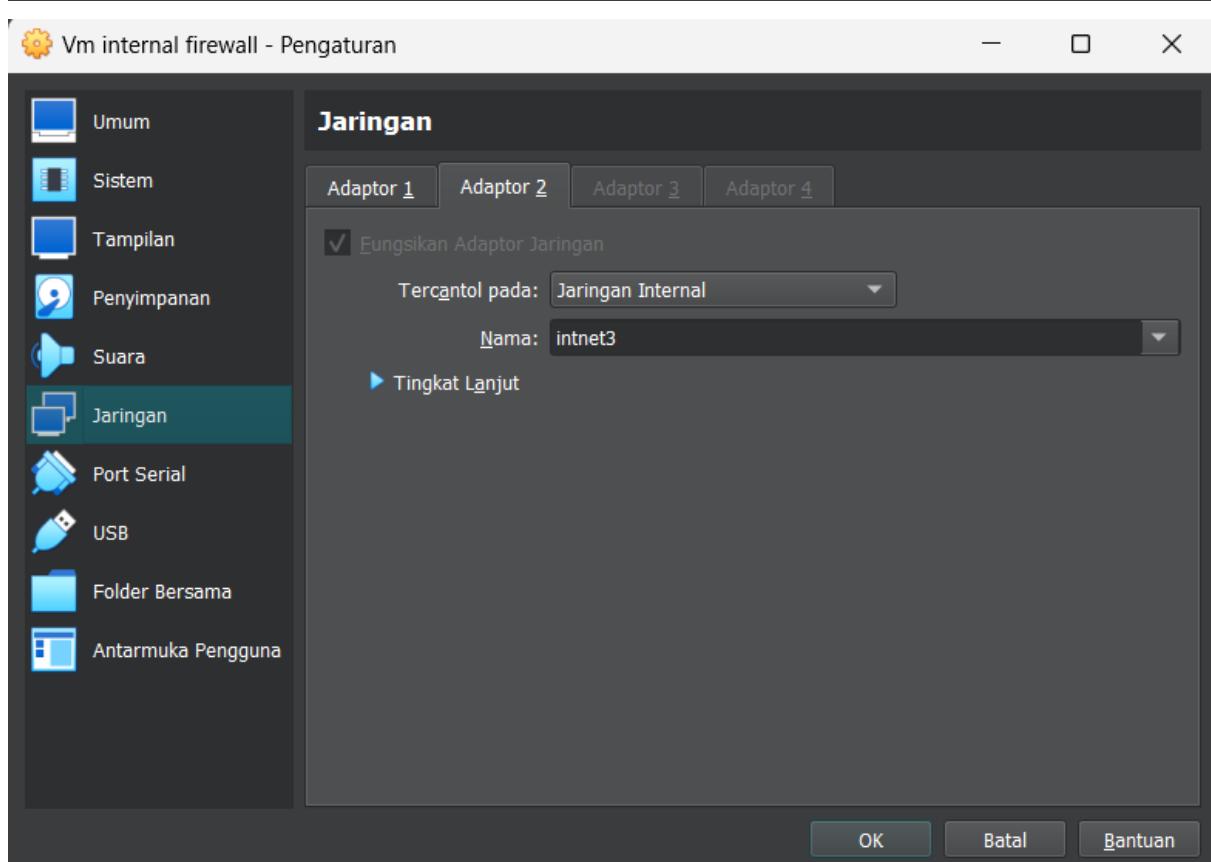
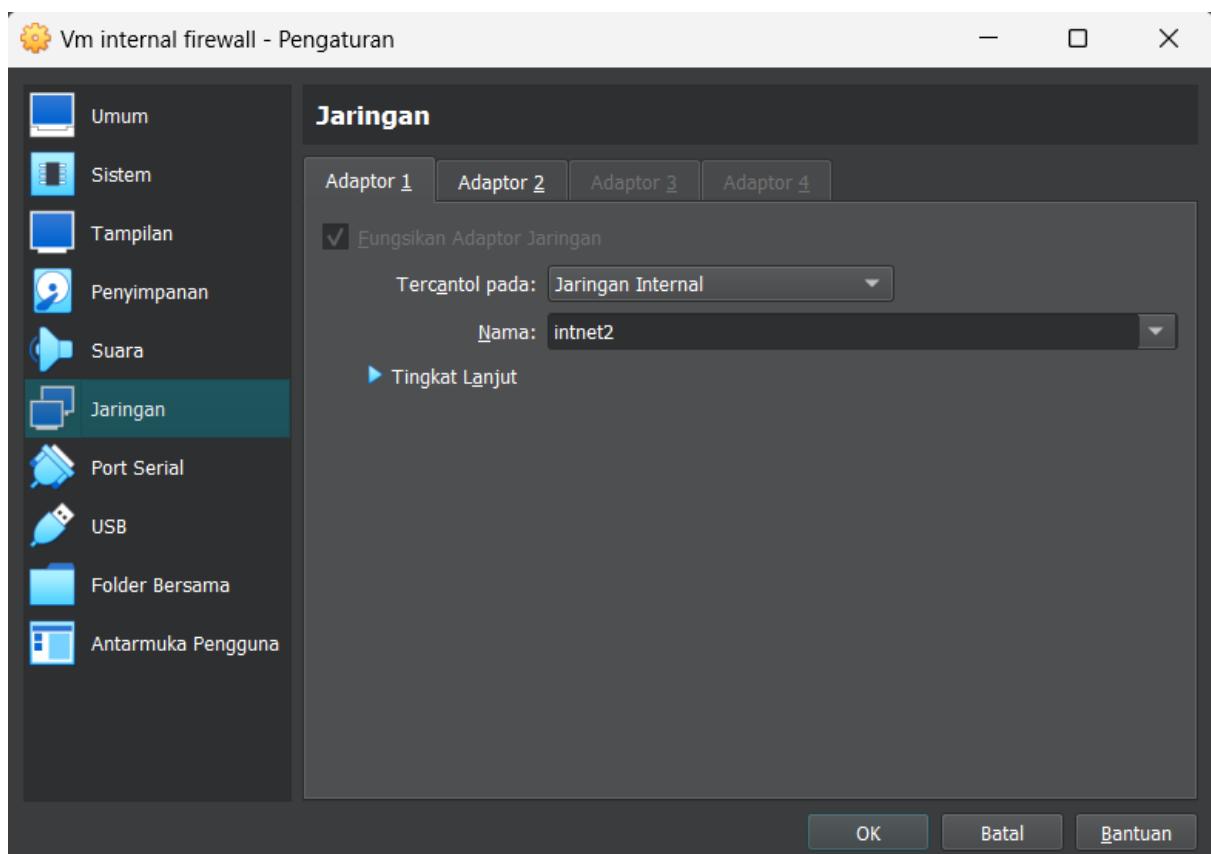
2. Setting ram dan cpu vm firewall external



3. Setting penyimpanan sebesar 30gb



4. Setting jaringan firewall Internal menggunakan jaringan internal pada adaptor 1 intnet2 dan adaptor 2 intnet3



5. Instalasi opnsense

```
Vm firewall internal [Berjalan] - Oracle VM VirtualBox  
Berkas Mesin Tilik Masukan Peranti Bantuan  
psm0: [GIANT-LOCKED]  
WARNING: Device "psm" is Giant locked and may be deleted before FreeBSD 14.0.  
psm0: model IntelliMouse Explorer, device ID 4  
prm0: <ISA Option ROMs> at iomem 0xc0000-0xc7fff,0xe2000-0xeffff pnpid 0RM0000 on isa0  
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff pnpid PNP0900 on isa0  
atrtc0: <AT realtime clock> at port 0x70 irq 8 on isa0  
atrtc0: registered as a time-of-day clock, resolution 1.000000s  
Event timer "RTC" frequency 32768 Hz quality 0  
Timecounter "TSC-low" frequency 1651198094 Hz quality 1000  
Timecounters tick every 10.000 msec  
usbus0: 12Mbps Full Speed USB v1.0  
usbus1: 480Mbps High Speed USB v2.0  
pcm0: measured ac97 link rate at 43799 Hz  
ugen1.1: <Intel EHCI root HUB> at usbus1  
uhub0 on usbus1  
uhub0: <Intel EHCI root HUB, class 9/0, rev 2.00/1.00, addr 1> on usbus1  
ugen0.1: <Apple OHCI root HUB> at usbus0  
uhub1 on usbus0  
uhub1: <Apple OHCI root HUB, class 9/0, rev 1.00/1.00, addr 1> on usbus0  
Trying to mount root from cd9660:/dev/iso9660/OPNSENSE_INSTALL [ro]...  
uhub1: 12 ports with 12 removable, self powered  
Root mount waiting for: CAM usbus1
```

```
Vm firewall internal [Berjalan] - Oracle VM VirtualBox  
Berkas Mesin Tilik Masukan Peranti Bantuan  
The interfaces will be assigned as follows:  
WAN -> em1  
LAN -> em0  
Do you want to proceed? [y/N]: y  
Writing configuration...done.  
Configuring loopback interface...lo0: link state changed to UP  
done.  
Configuring kernel modules...done.  
Setting up extended sysctls...done.  
Setting timezone: Etc/UTC  
Writing firmware settings: FreeBSD OPNsense  
Writing trust files...done.  
Scanning /usr/share/certs/blacklisted for certificates...  
Scanning /usr/share/certs/trusted for certificates...  
Scanning /usr/local/share/certs for certificates...  
Writing trust bundles...done.  
Setting hostname: OPNsense.localdomain  
Generating /etc/resolv.conf...done.  
Generating /etc/hosts...done.  
Configuring system logging...done.  
Configuring firewall.....done.  
Configuring hardware interfaces...■
```

Vm firewall internal [Berjalan] - Oracle VM VirtualBox

```
Berkas Mesin Tilik Masukan Peranti Bantuan
>>> Invoking start script 'sysctl'
Service `sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Sun Jun 23 20:07:48 UTC 2024

*** OPNsense.locaLdomain: OPNsense 24.1 ***

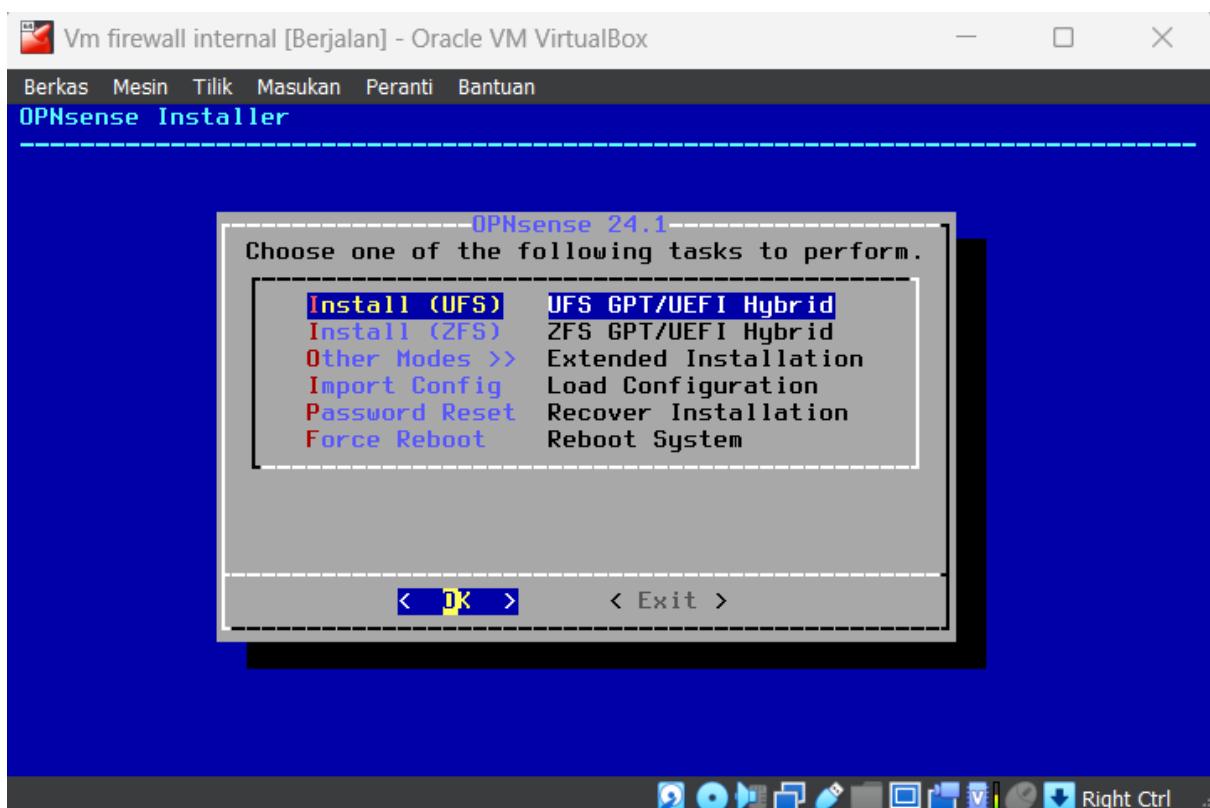
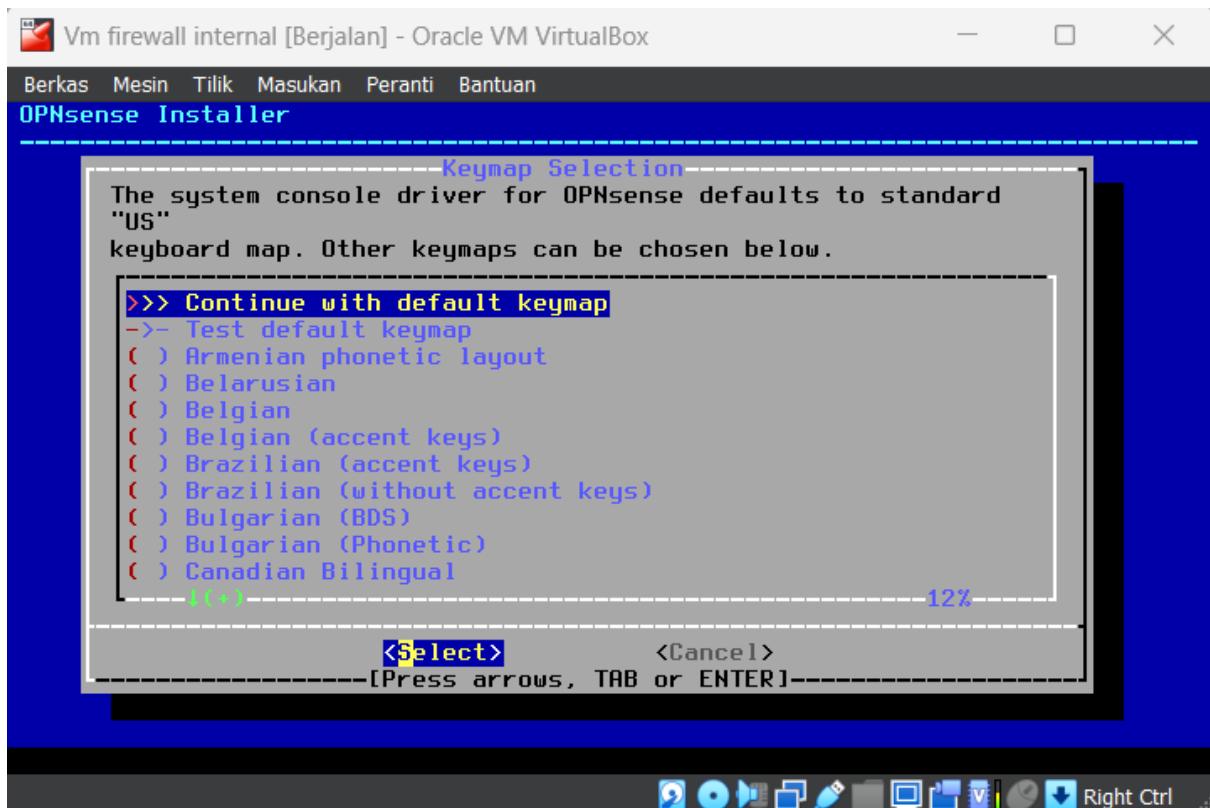
LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      -> v4/DHCP4: 192.168.1.100/24

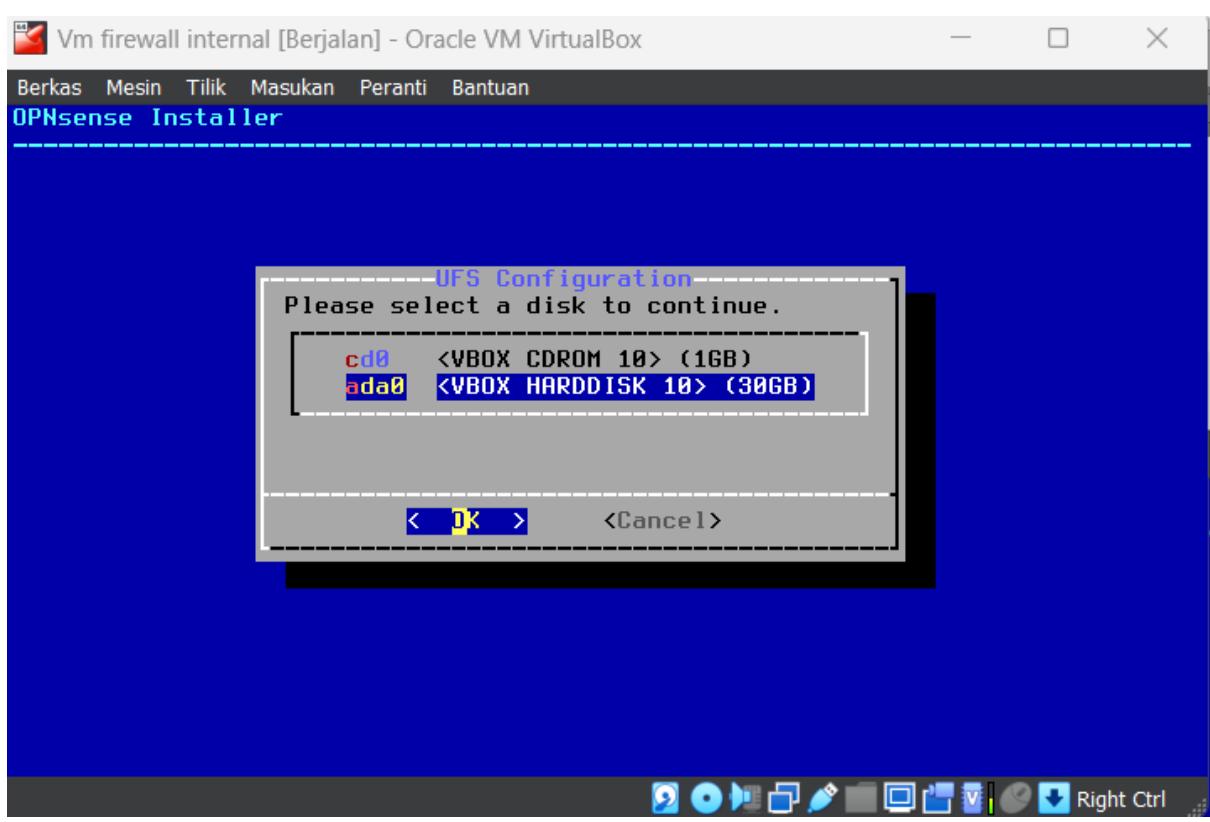
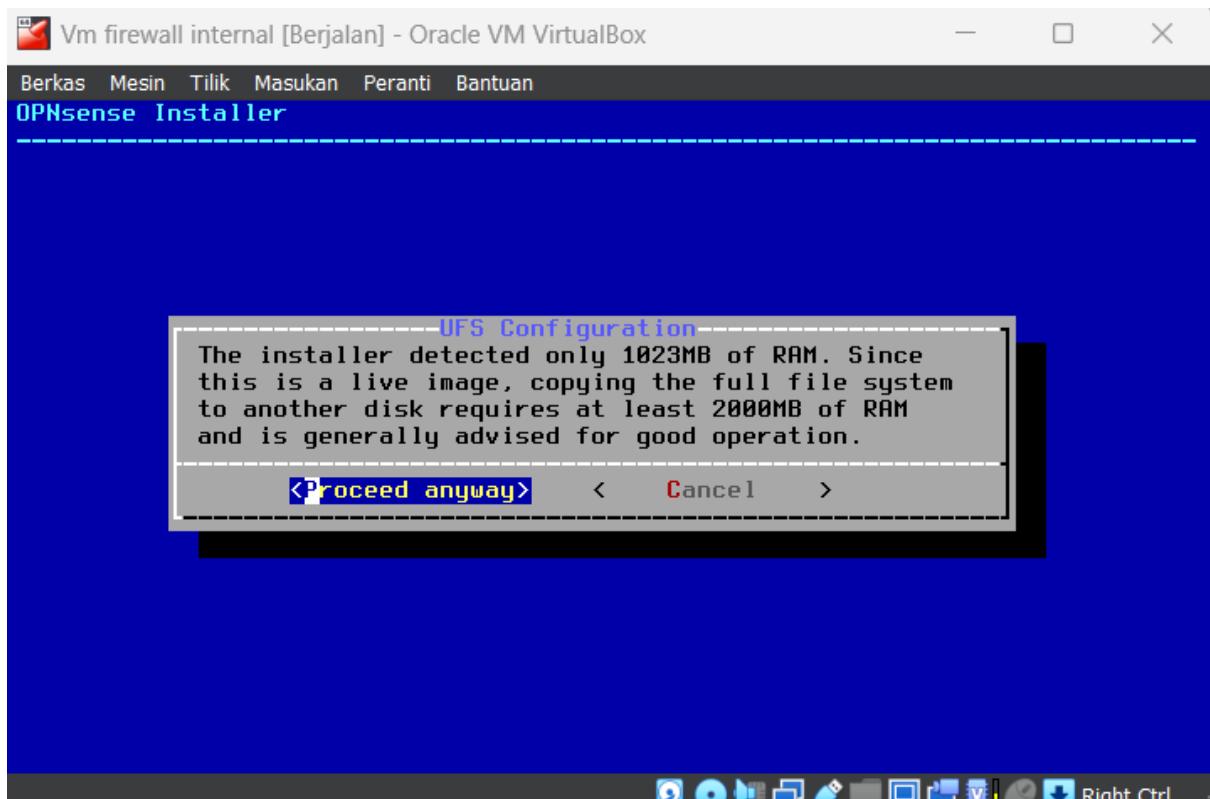
HTTPS: SHA256 79 67 3B 7E 1B 59 A2 62 41 11 F9 90 13 E2 36 84
        F9 2C 3D FA 71 06 84 00 4B 39 35 0A 3A 60 B6 BB
SSH:   SHA256 Ms1L61IR61f9+8UMH1591y2GsFeH7EpBSsis5RgU3gI (ECDSA)
SSH:   SHA256 U+YGDztHzvT5VXuxPXqpnq6M62zsVvAOi6U8XQrXk98 (ED25519)
SSH:   SHA256 DSMCDqJh09sQ4XAk9+xYrP7233DUbfVdhc2uNX5ldpQ (RSA)

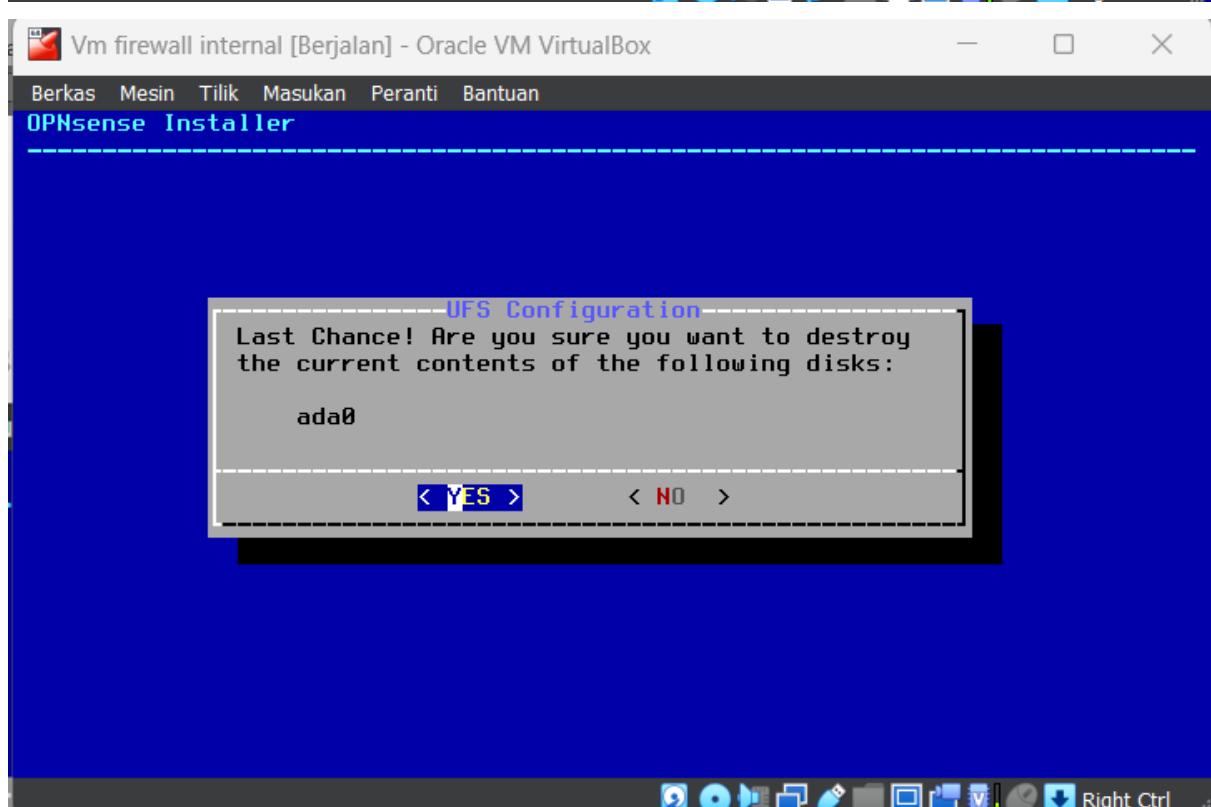
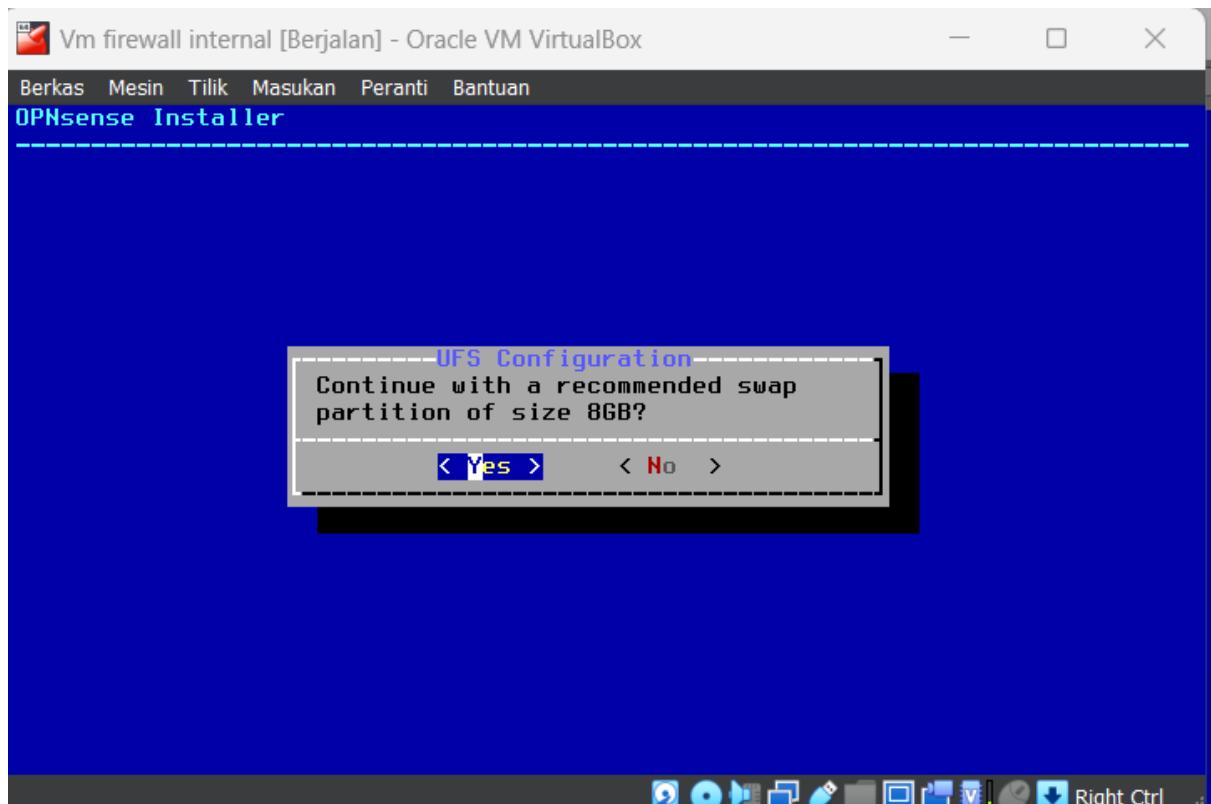
Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

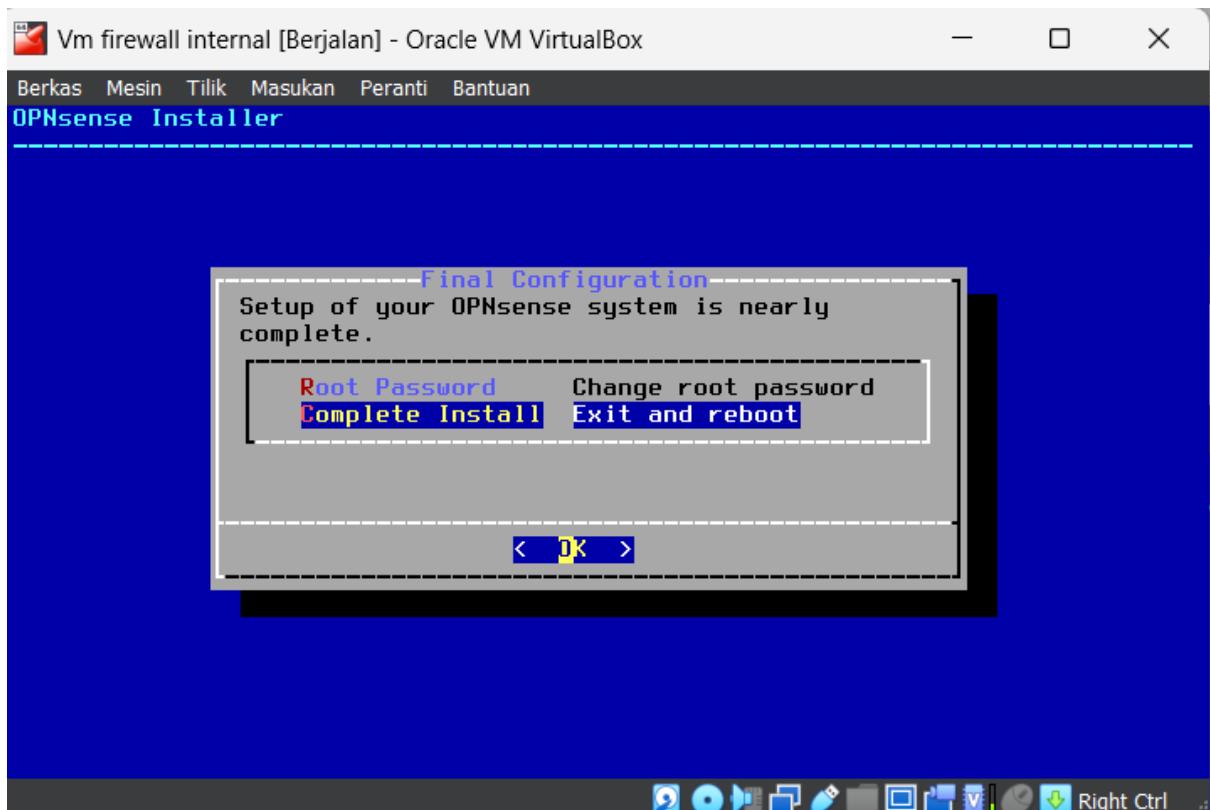
freeBSD/amd64 (OPNsense.locaLdomain) (ttyv0)

login: █
```



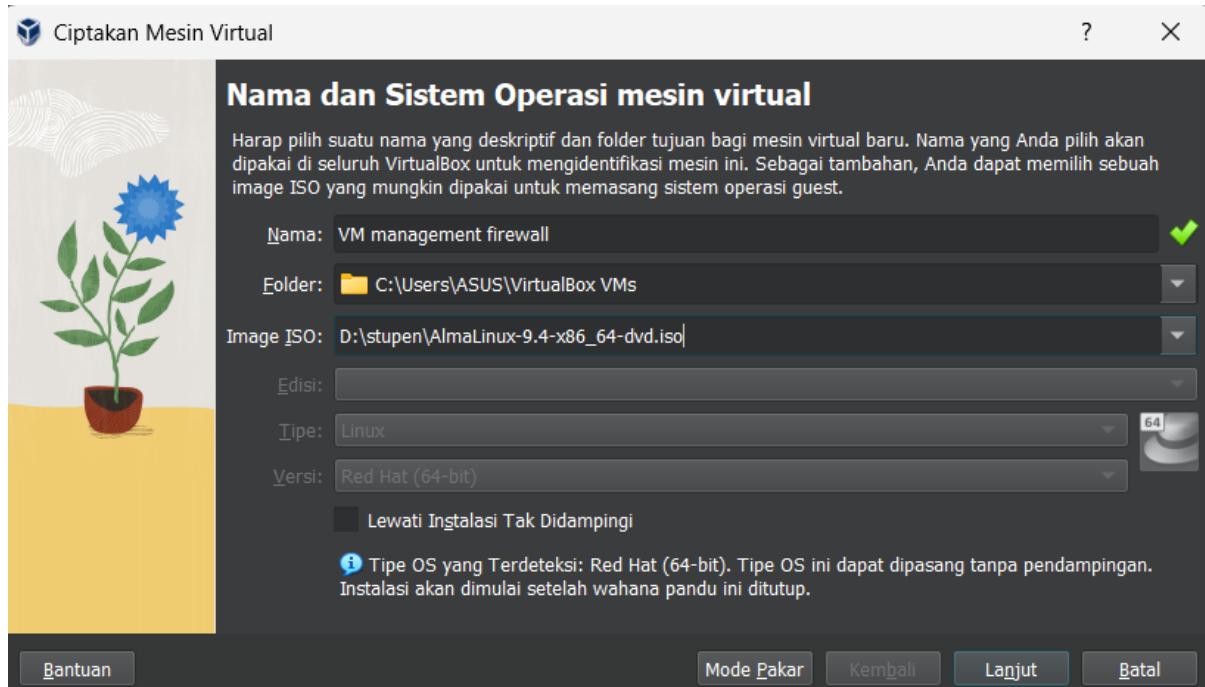




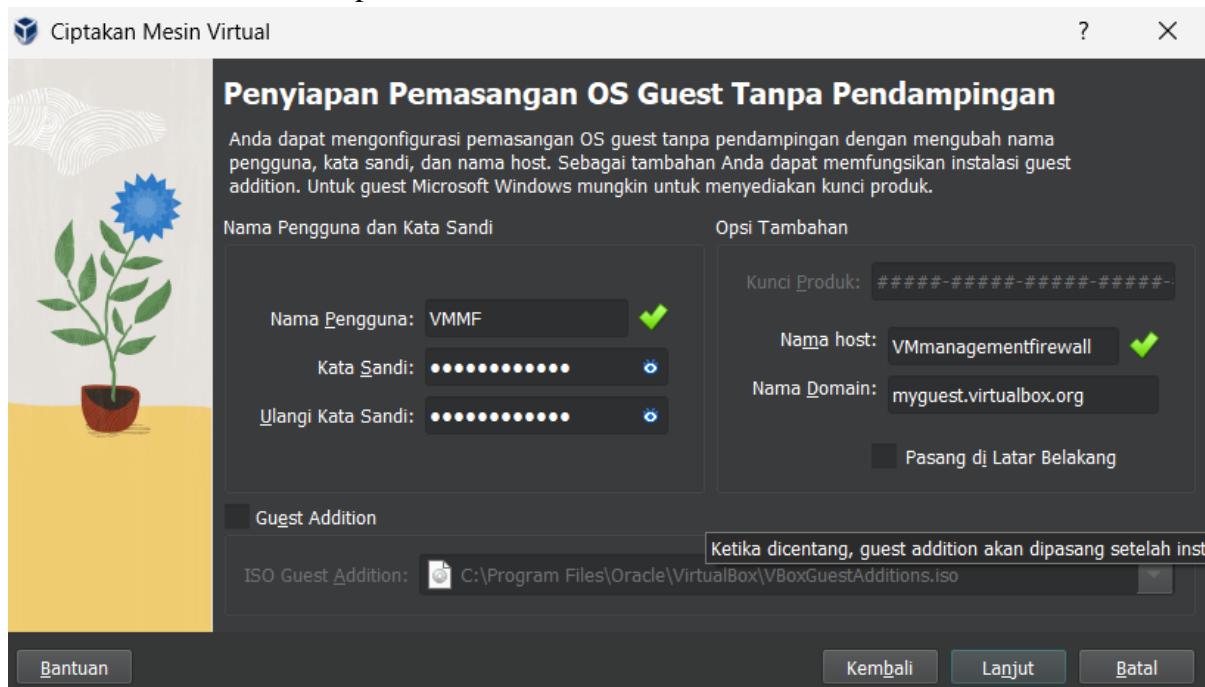


V. Install Alma linux – VM Management Firewall

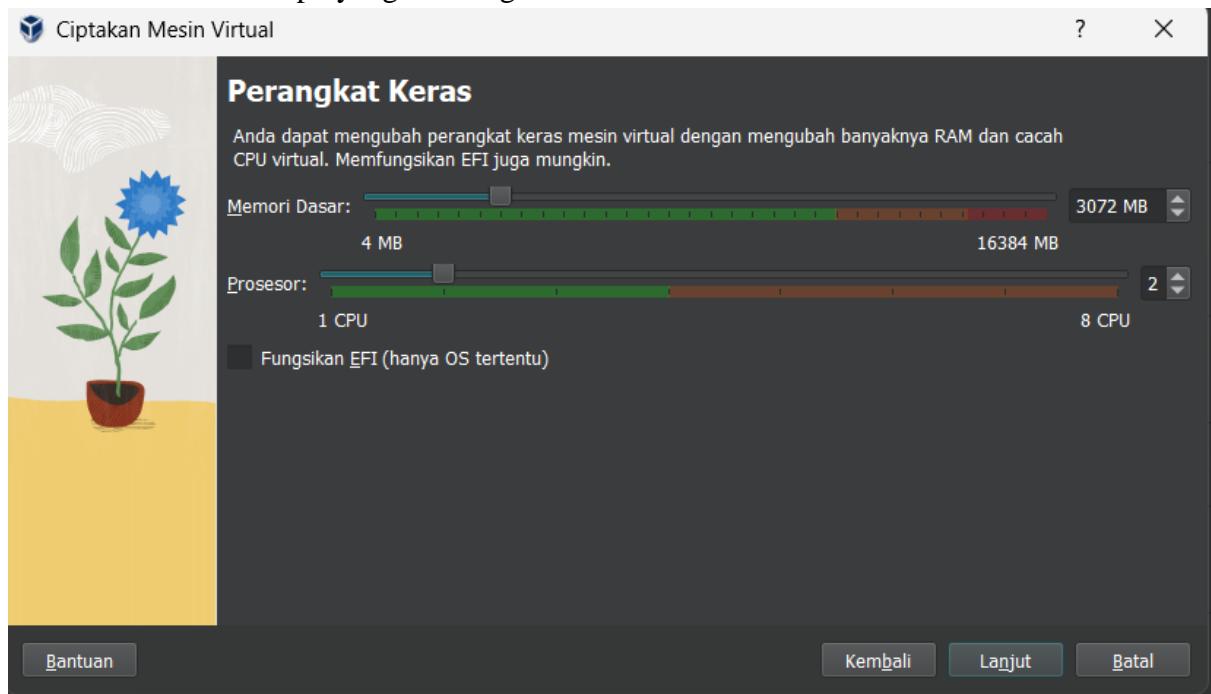
1. Install vm management firewall menggunakan alma linux



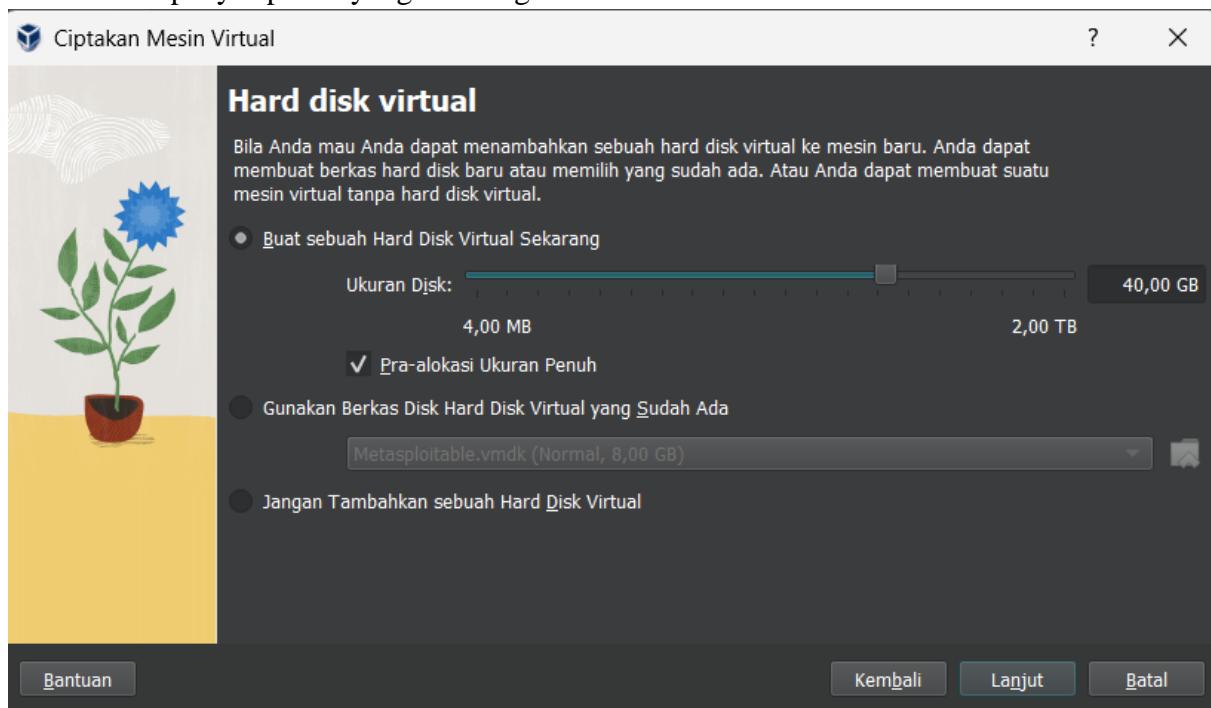
2. Atur username dan password dan nama host



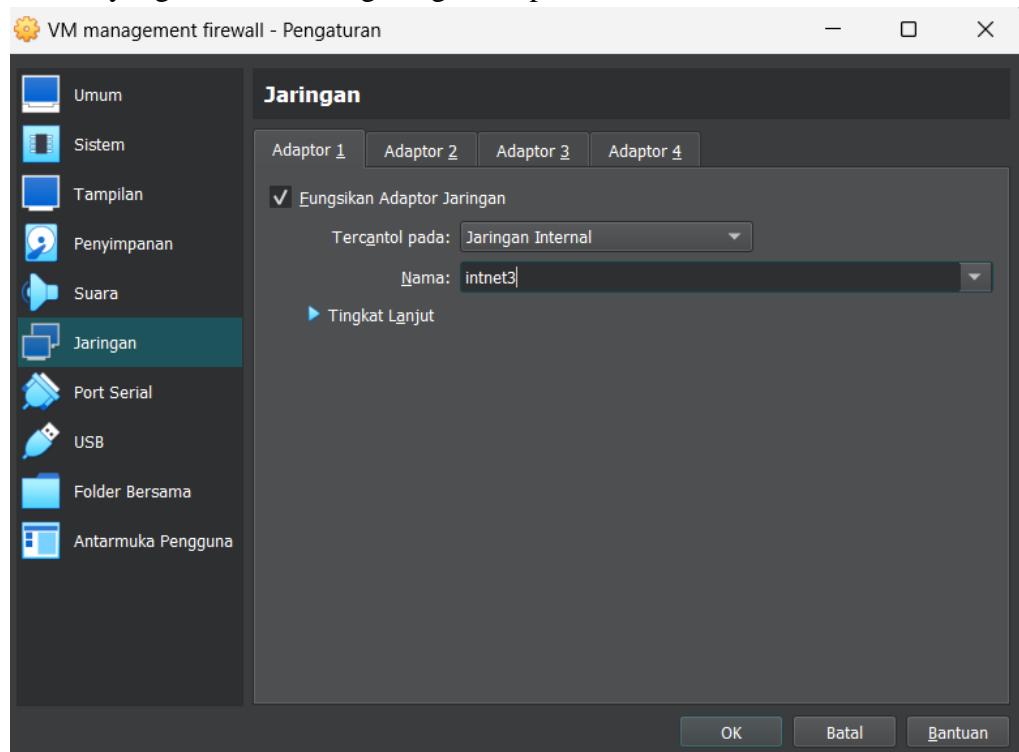
3. Atur ram dan cpu yang akan digunakan



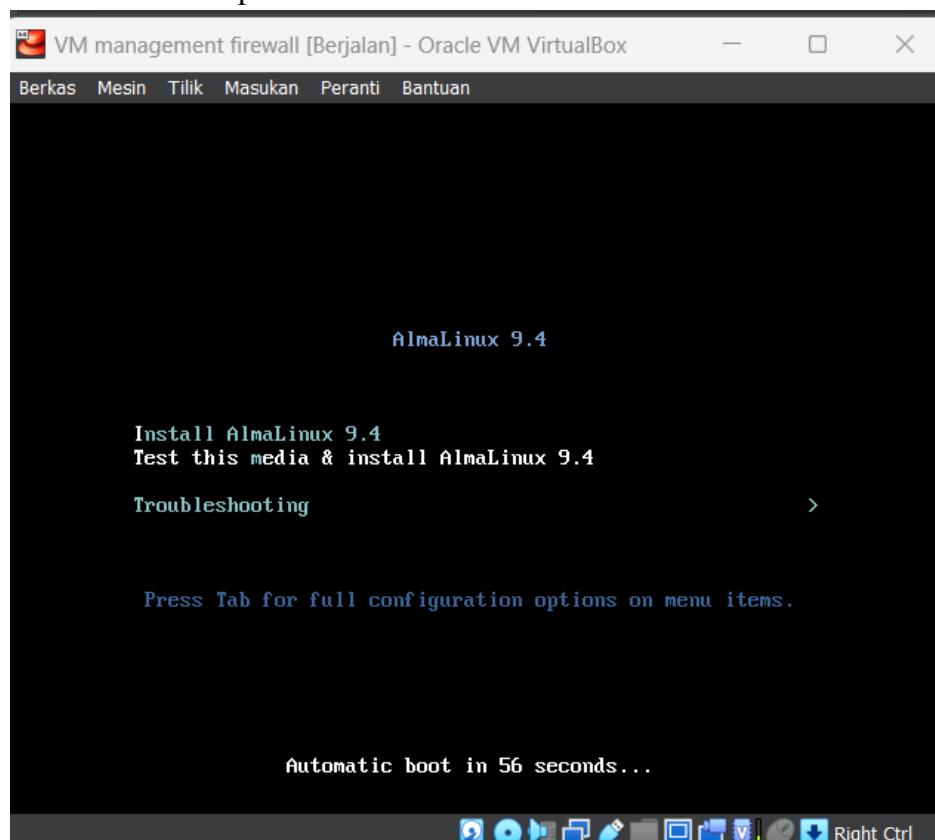
4. Atur penyimpanan yang akan digunakan



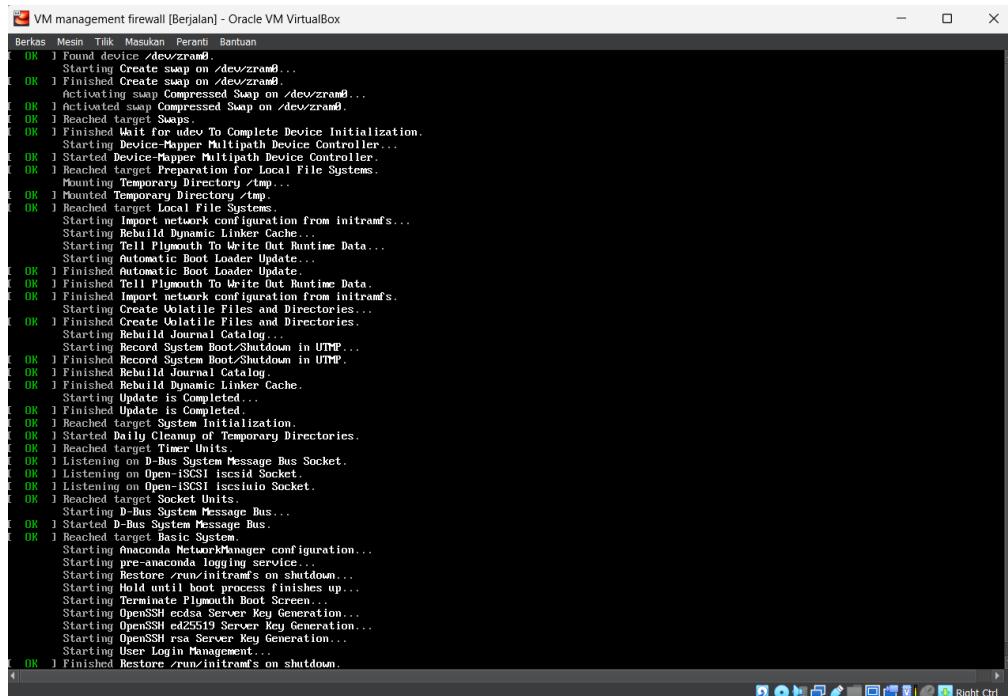
5. Atur jaringan yang akan digunakan pada adaptor 1 menggunakan jaringan internal intnet3 yang akan terhubung dengan adaptor 2 intnet3 internal firewall



6. Instalasi alma linux pilih install Almalinux 9.4

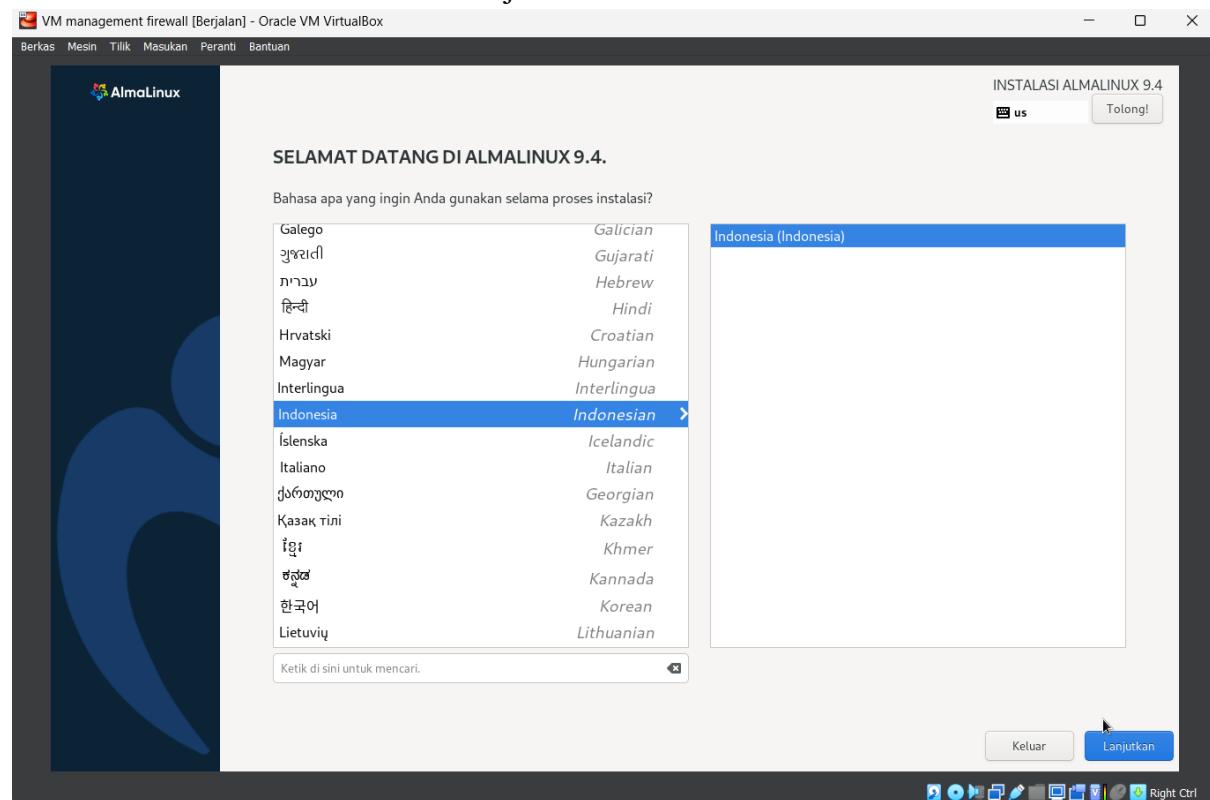


7. Tunggu sedang proses pengecekan os

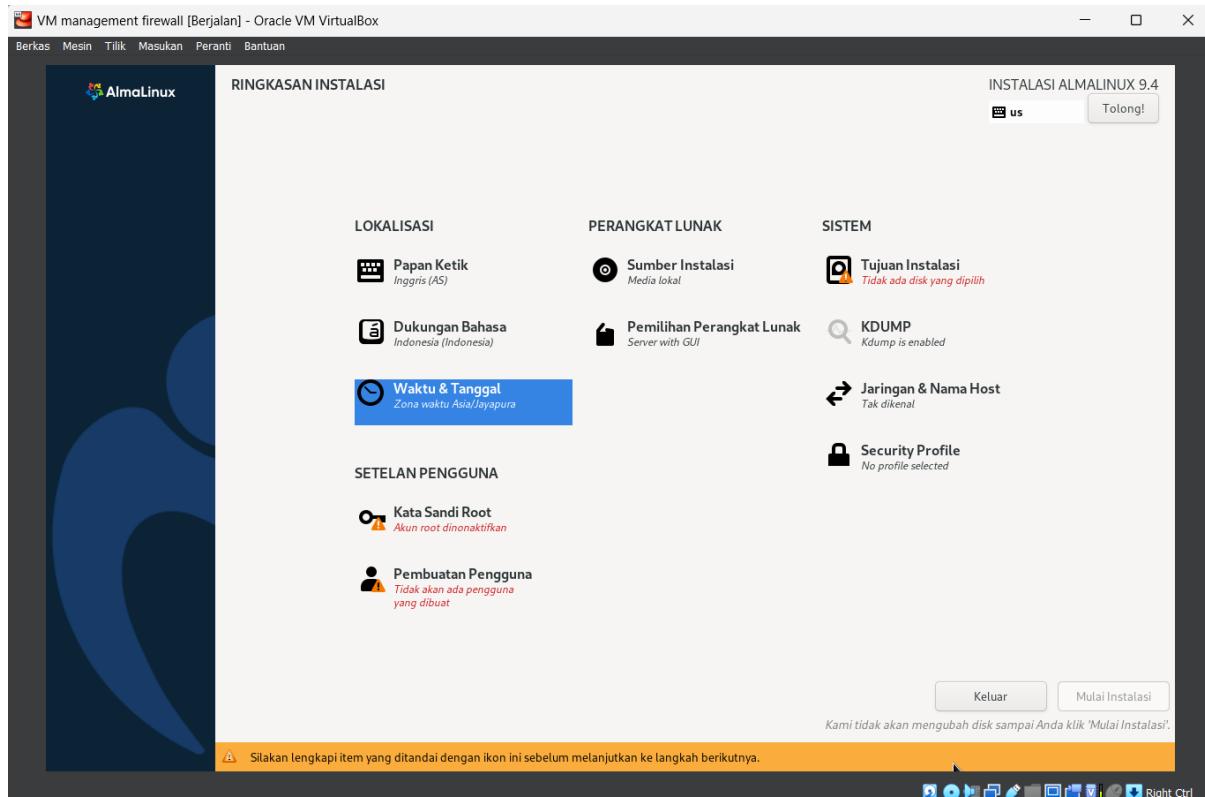


```
VM management firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tisk Masukan Peranti Bantuan
OK J Found device /dev/zram0.
OK J Starting Create swap on /dev/zram0...
OK J Finished Create swap on /dev/zram0...
OK J Writing Compressed Swap on /dev/zram0...
OK J Activated swap Compressed Swap on /dev/zram0.
OK J Reached target Swap.
OK J Finished Wait for udev To Complete Device Initialization.
OK J Starting Device-Mapper Multipath Device Controller...
OK J Started Device-Mapper Multipath Device Controller.
OK J Reached target Preparation for Local File Systems.
OK J Mounting Temporary Directory /tmp...
OK J Mounted Temporary Directory /tmp.
OK J Reached target Local File Systems.
OK J Importing network configuration from initramfs...
OK J Starting Rebuild Dynamic Linker Cache.
OK J Starting Tell Plymouth To Write Out Runtime Data...
OK J Starting automatic Root Loader Update...
OK J Finished automatic Root Loader Update.
OK J Finished Tell Plymouth To Write Out Runtime Data.
OK J Finished Import network configuration from initramfs.
OK J Starting Create Volatile Files and Directories...
OK J Finished Create Volatile Files and Directories.
OK J Starting Rebuild Journal Catalog.
OK J Finished Rebuild Dynamic Linker Cache.
OK J Starting Update is Completed...
OK J Finished Update is Completed.
OK J Reached target System Initialization.
OK J Started Daily Cleanup of Temporary Directories.
OK J Reached target Timer Units.
OK J Listening on D-Bus System Message Bus Socket.
OK J Listening on D-Bus Open-SCSI Iscsiid Socket.
OK J Listening on Open-SCSI Iscsiio Socket.
OK J Reached target Socket Units.
OK J Starting D-Bus System Message Bus...
OK J Started D-Bus System Message Bus.
OK J Reached target Basic System.
OK J Starting anaconda NetworkManager configuration...
OK J Starting pre-anacoda logging service...
OK J Starting Restore /run/initramfs on shutdown...
OK J Starting Hold until boot process finishes up...
OK J Generating Public Boot Keys...
OK J Starting OpenSSH ecdsa Server Key Generation...
OK J Starting OpenSSH ed25519 Server Key Generation...
OK J Starting OpenSSH rsa Server Key Generation...
OK J Starting User Login Management...
OK J Finished Restore /run/initramfs on shutdown.
```

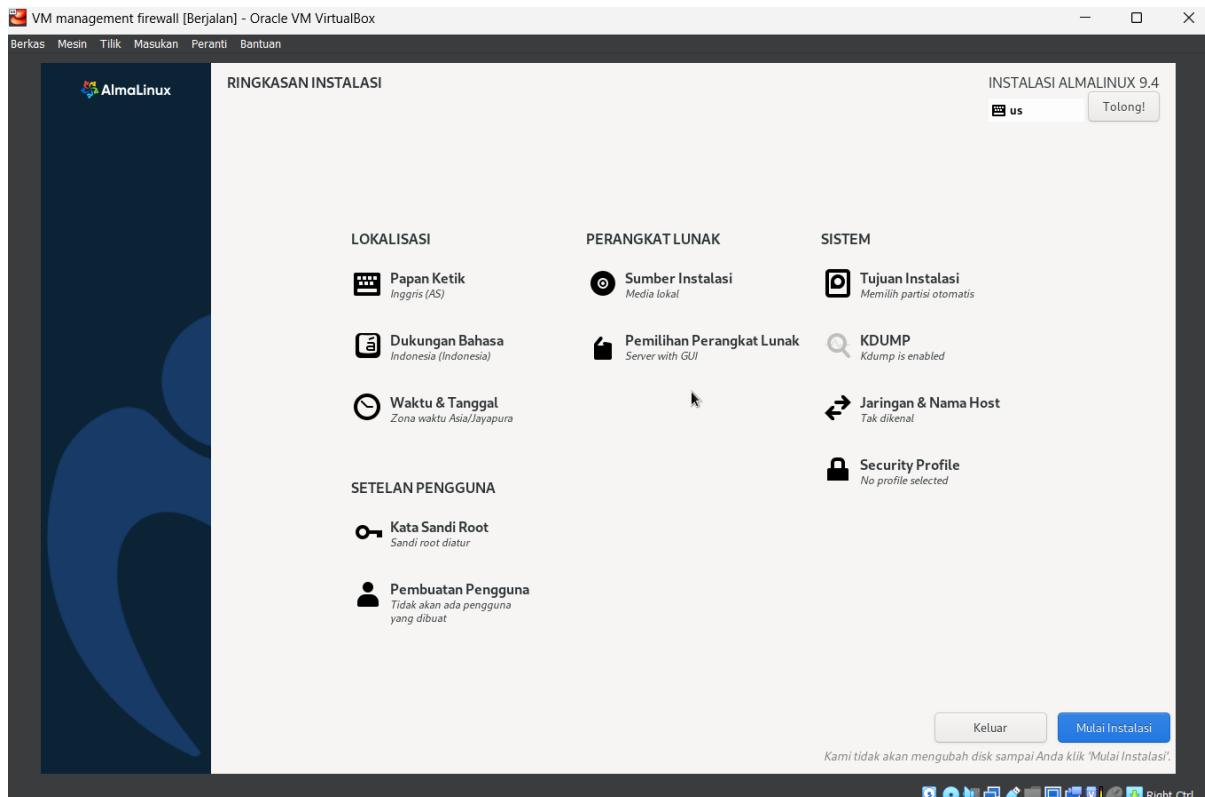
8. Pilih bahasa indonesia dan klik lanjutkan



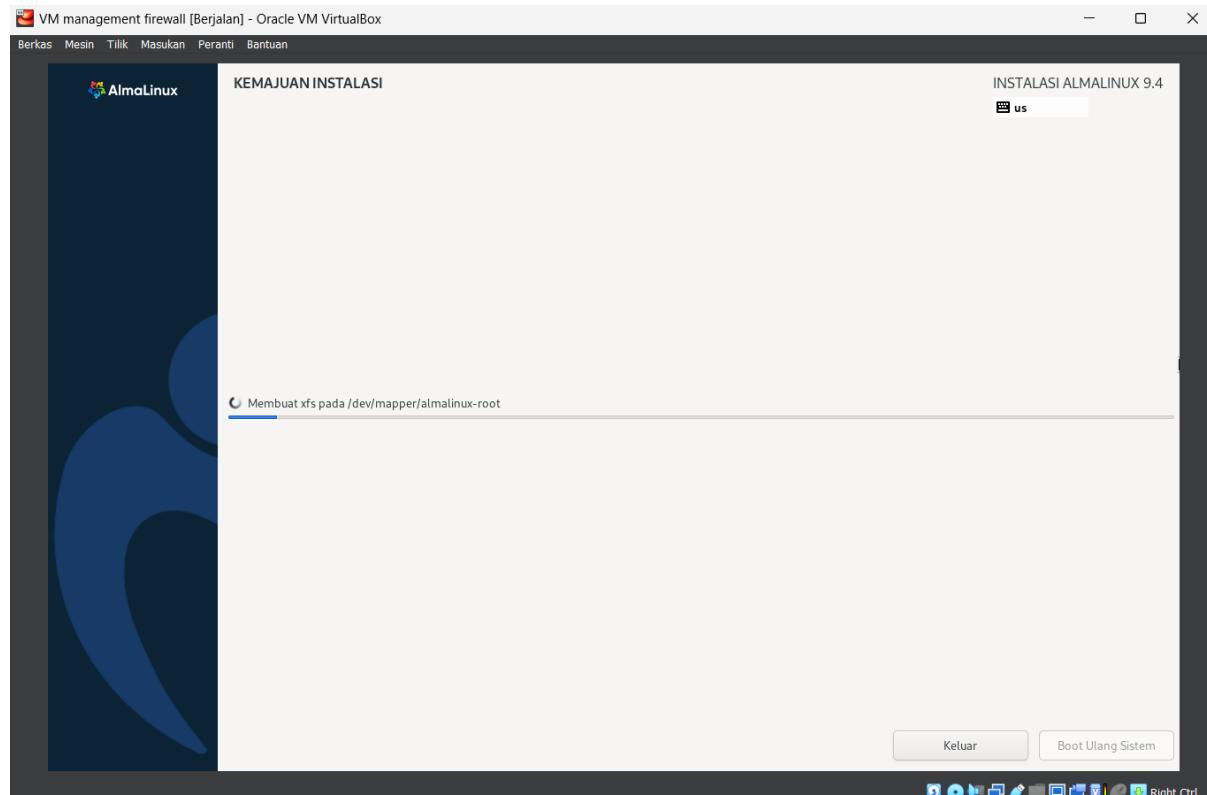
9. Atur kata sandi admin/root dan atur disk penyimpanan yg digunakan



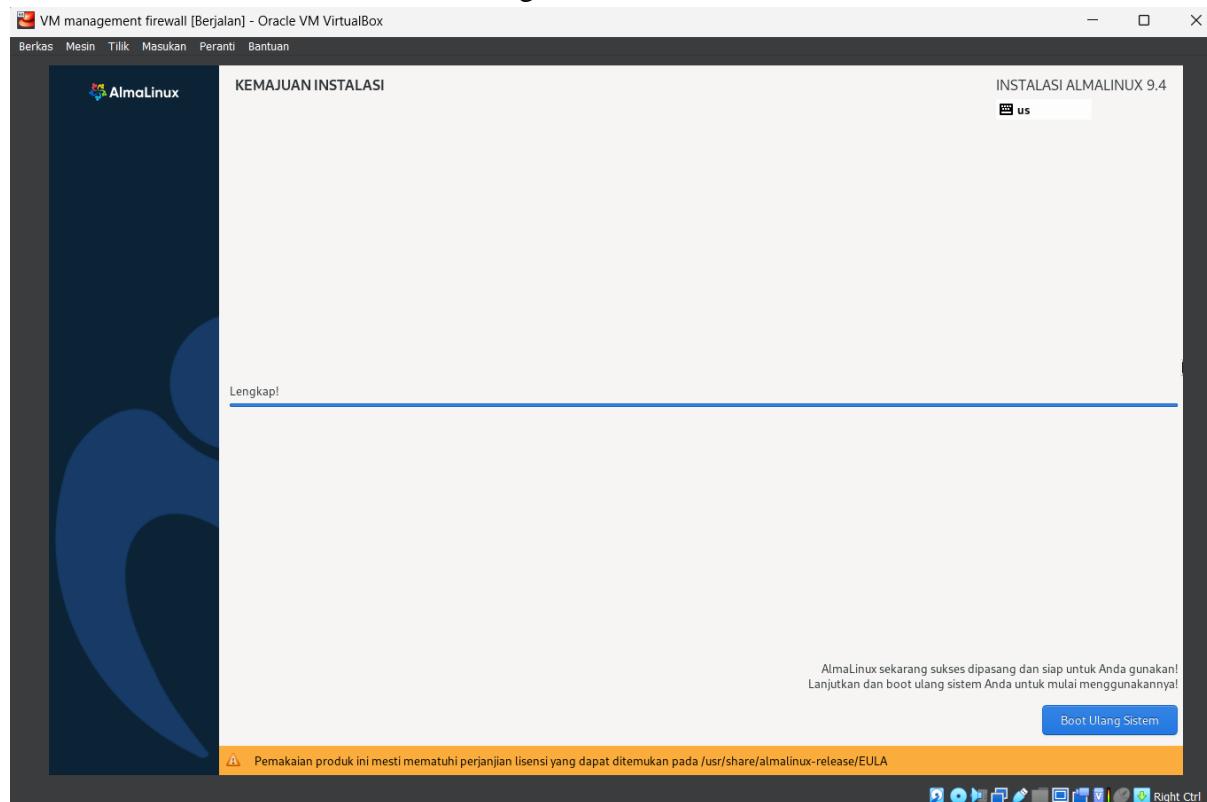
10. Jika sudah klik mulai instalasi



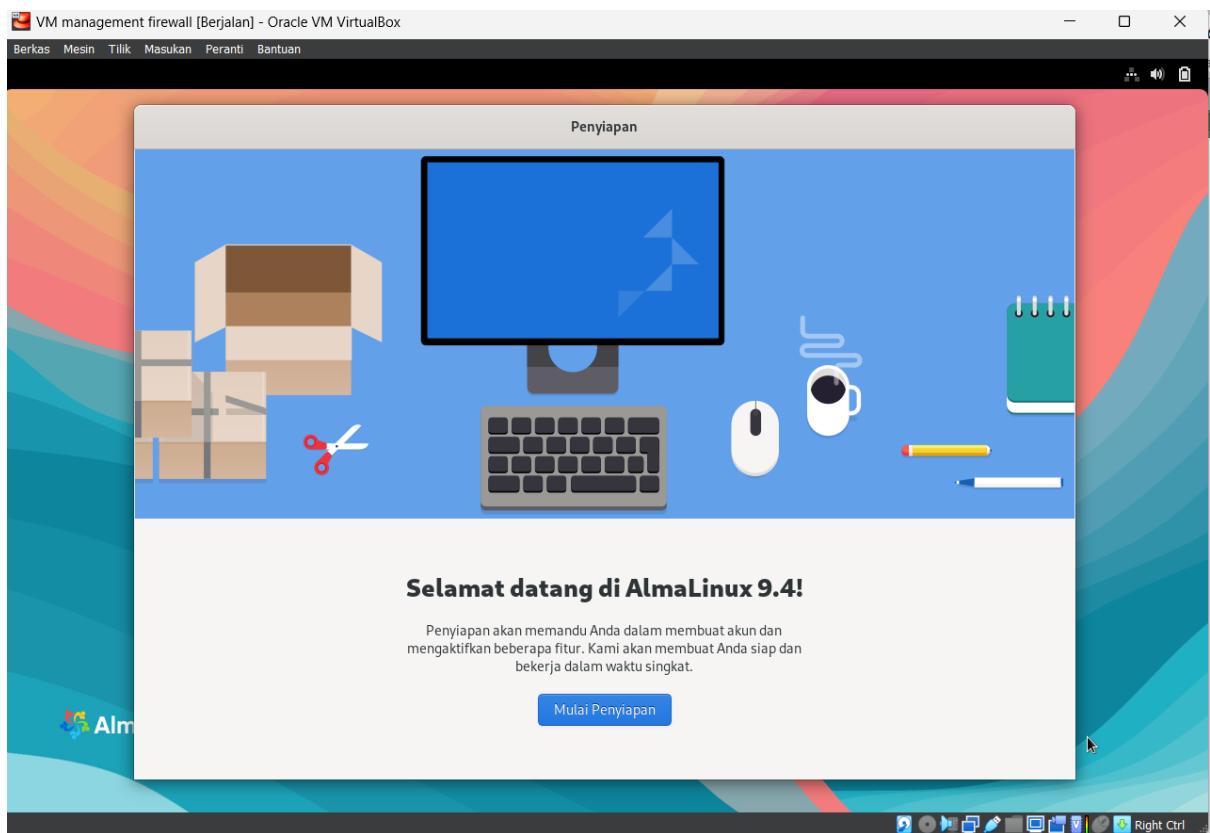
11. Tunggu instalasi selesai



12. Jika sudah selesai klik boot ulang sistem



13. Alma linux berhasil ter install



VI. Konfigurasi firewall external dengan laptop dan internet

1. Mengatur interface pada external firewall untuk wan menggunakan dhcp nat network dan pada LAN menggunakan static dengan ip address 10.10.10.1/24 dan gateway 10.10.10.2

```
Vm external firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan

Available interfaces:
1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.10.10.2

Enter the new LAN IPv6 address. Press <ENTER> for none:
> 
```

2. Uji konektifitas pada external untuk ping 8.8.8.8 dns google.com

```
Vm external firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan

1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address    11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults     13) Update from console
5) Reboot system                 14) Enable Secure Shell (sshd)
6) Halt system                   15) Restore recent configuration
7) Ping host                      16) Restart PHP-FPM
8) Shell

Enter an option: 7

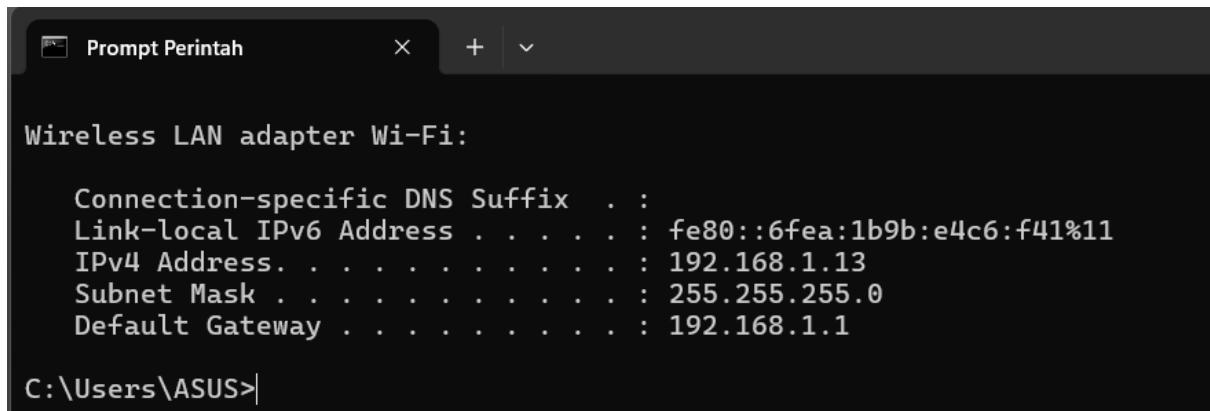
Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=113 time=30.076 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=34.629 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=27.127 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 27.127/30.611/34.629/3.086 ms

Press ENTER to continue.
```

3. Uji konektifitas dengan jaringan laptop menggunakan ping dari eksternal firewall

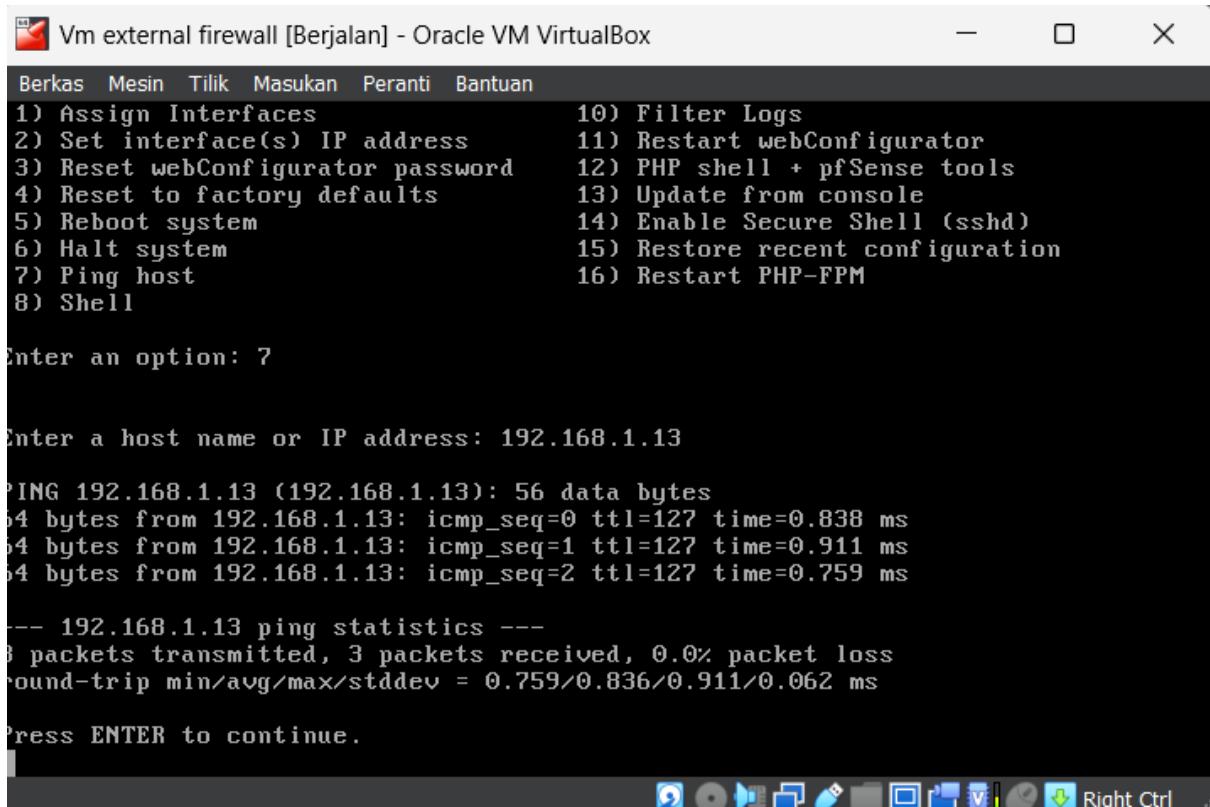


```
Prompt Perintah
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::6fea:1b9b:e4c6:f41%11
IPv4 Address. . . . . : 192.168.1.13
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\Users\ASUS>
```

(ip address laptop)



```
Vm external firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell

Enter an option: 7

Enter a host name or IP address: 192.168.1.13

PING 192.168.1.13 (192.168.1.13): 56 data bytes
64 bytes from 192.168.1.13: icmp_seq=0 ttl=127 time=0.838 ms
64 bytes from 192.168.1.13: icmp_seq=1 ttl=127 time=0.911 ms
64 bytes from 192.168.1.13: icmp_seq=2 ttl=127 time=0.759 ms

--- 192.168.1.13 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.759/0.836/0.911/0.062 ms

Press ENTER to continue.
```

VII. Konfigurasi firewall Internal dengan firewall eksternal

1. Mengatur interface pada wan interface internal firewall memasukan ip address submask dan gateway untuk terhubung dengan eksternal firewall

```
Vm internal firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan

1 - LAN (em1 - static)
2 - WAN (em0 - static)

Enter the number of the interface to configure: 2
Configure IPv4 address WAN interface via DHCP? [Y/n] n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.10.10.2

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0    = 16
     255.0.0.0      = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.10.10.1

Do you want to use it as the default IPv4 gateway? [Y/n] ■
```

2. Mengatur interface pada LAN interface internal firewall memasukan ip address submask

```
Vm internal firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan

1 - LAN (em1 - static)
2 - WAN (em0 - static)

Enter the number of the interface to configure: 1
Configure IPv4 address LAN interface via DHCP? [y/N] n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.20.1

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0    = 16
     255.0.0.0      = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? [y/N] ■
```

3. Uji konektifitas dari internal firewall ke eksternal firewall

```
Vm internal firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan
0) Logout 7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: 7

Enter a host name or IP address: 10.10.10.1

PING 10.10.10.1 (10.10.10.1): 56 data bytes
4 bytes from 10.10.10.1: icmp_seq=0 ttl=64 time=0.535 ms
4 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.542 ms
4 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.818 ms

-- 10.10.10.1 ping statistics --
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.535/0.631/0.818/0.132 ms

Press ENTER to continue.
```

4. Uji konektifitas dari eksternal firewall ke internal firewall

```
Vm external firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM

Enter an option: 7

Enter a host name or IP address: 10.10.10.2

PING 10.10.10.2 (10.10.10.2): 56 data bytes
64 bytes from 10.10.10.2: icmp_seq=0 ttl=64 time=0.183 ms
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.550 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.603 ms

-- 10.10.10.2 ping statistics --
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.183/0.445/0.603/0.187 ms

Press ENTER to continue.
```

5. Uji konektifitas dari internal firewall ke dns google.com

```
Vm internal firewall [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan
0) Logout 7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: 7

Enter a host name or IP address: 8.8.8.8

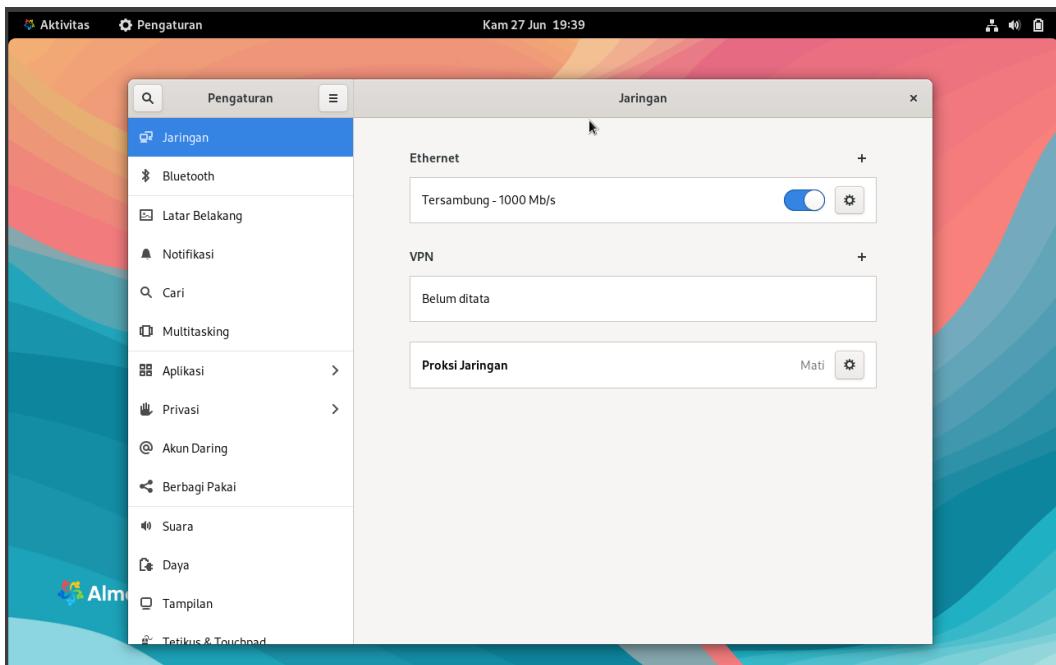
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=114 time=28.569 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=77.882 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=27.656 ms

-- 8.8.8.8 ping statistics --
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 27.656/44.702/77.882/23.464 ms

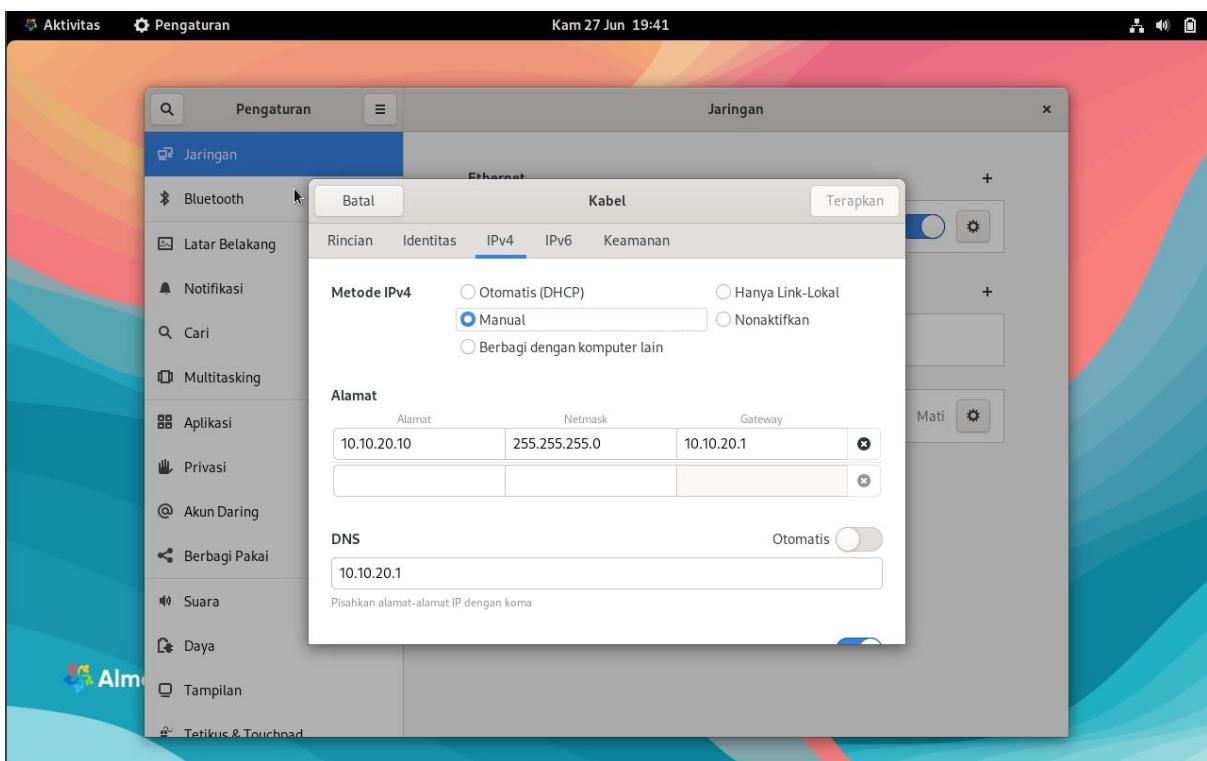
Press ENTER to continue.
```

VIII. Konfigurasi VM management firewall dengan firewall internal

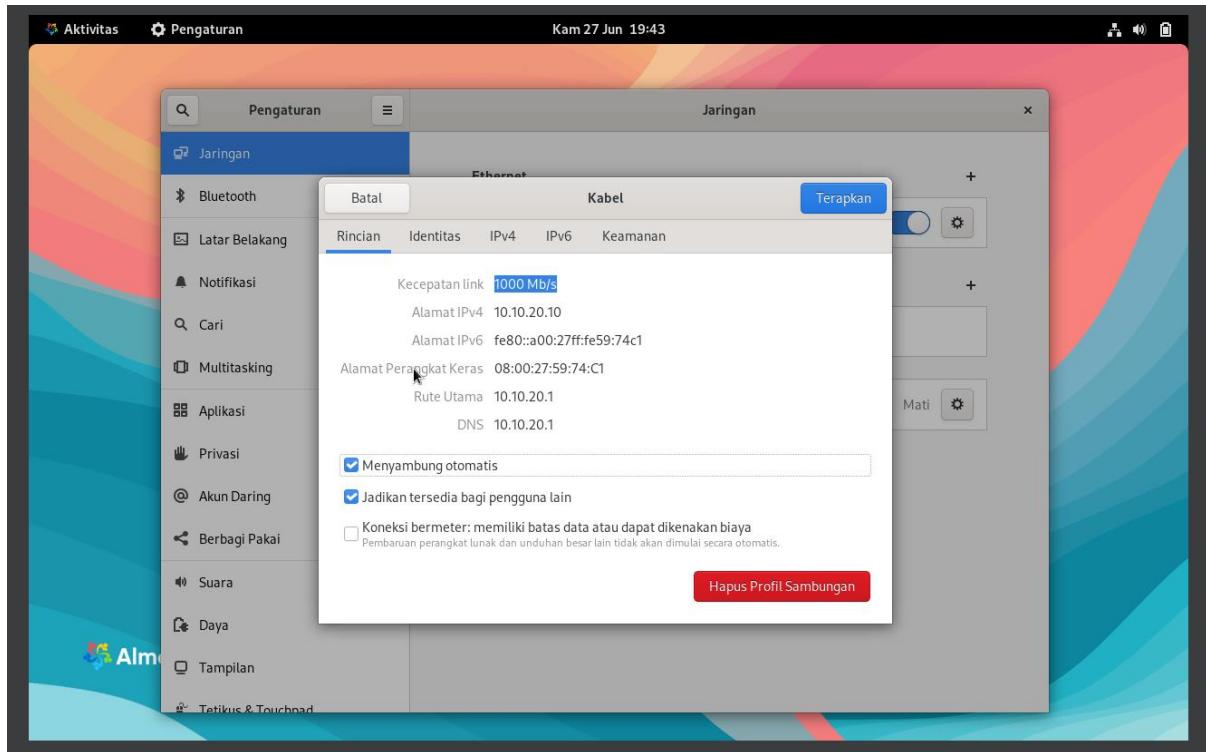
1. Masuk ke menu network



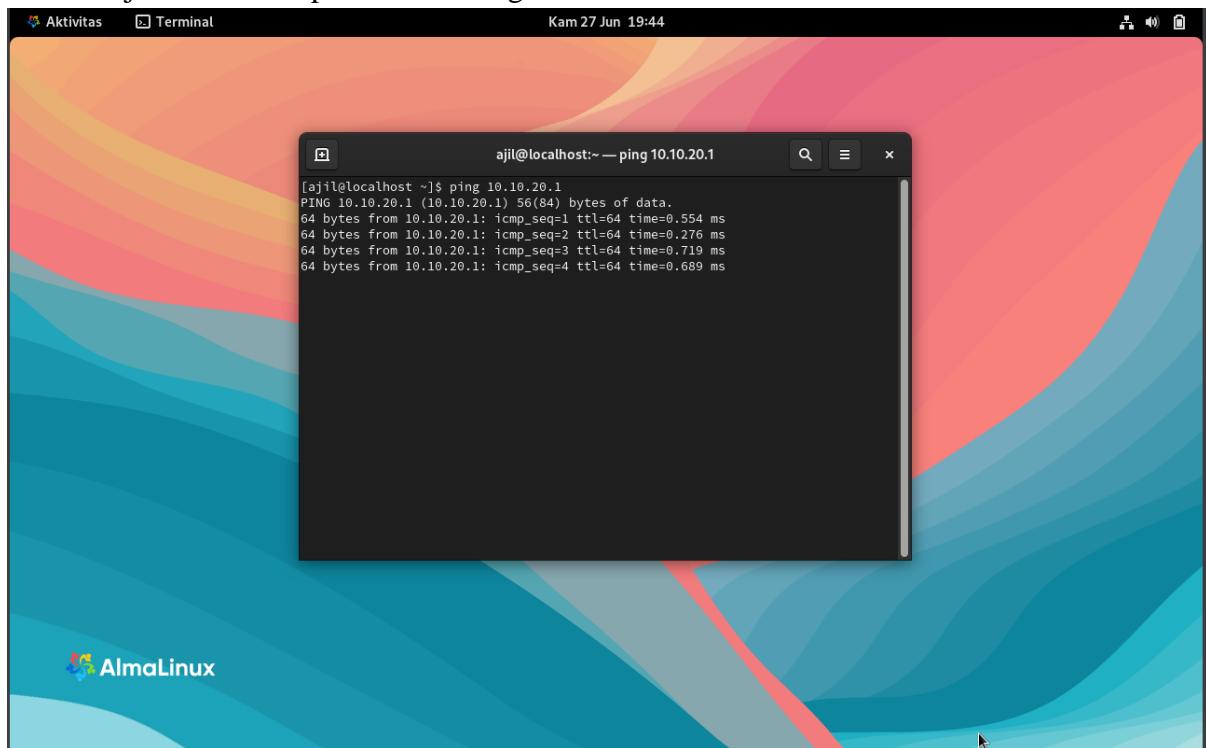
2. Klik setting pada ethernet dan pilihli ipv4 manual masukan ip address 10.10.20.10/24 lalu gateway 10.10.20.1 dan masukan dns 10.10.20.1 jika sudah klik terapkan dan restart



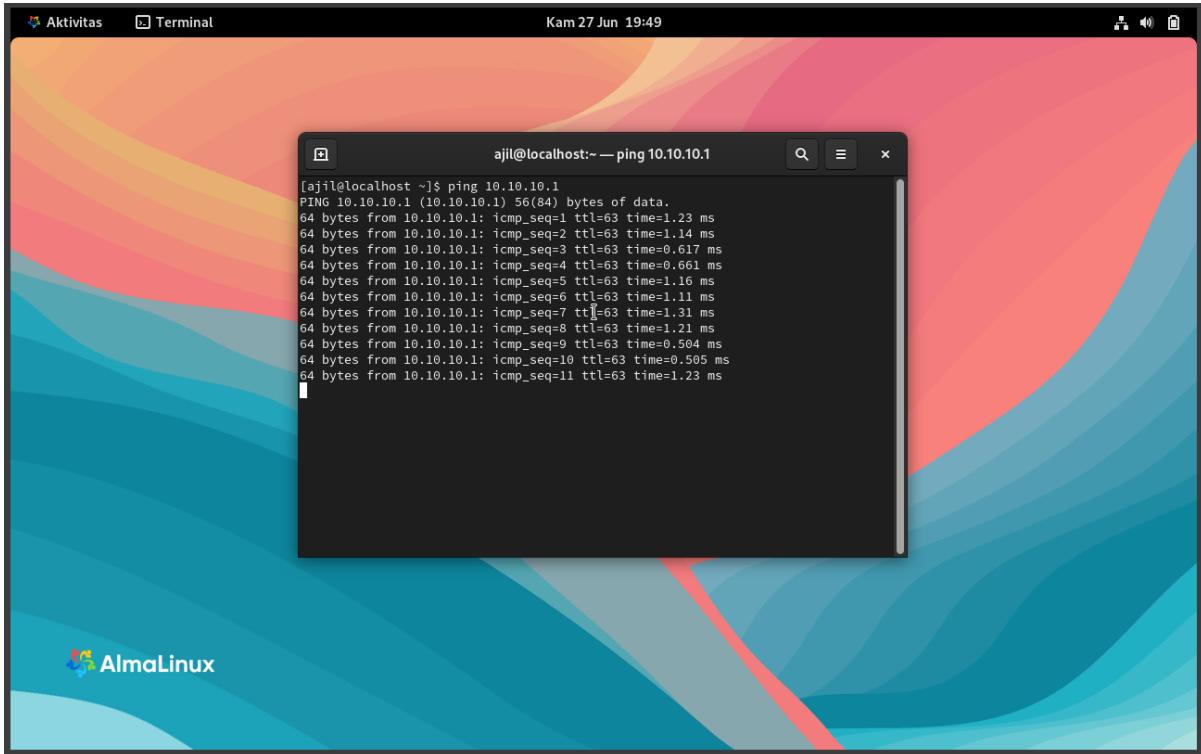
3. Jika sudah akan seperti gambar dibawah ini



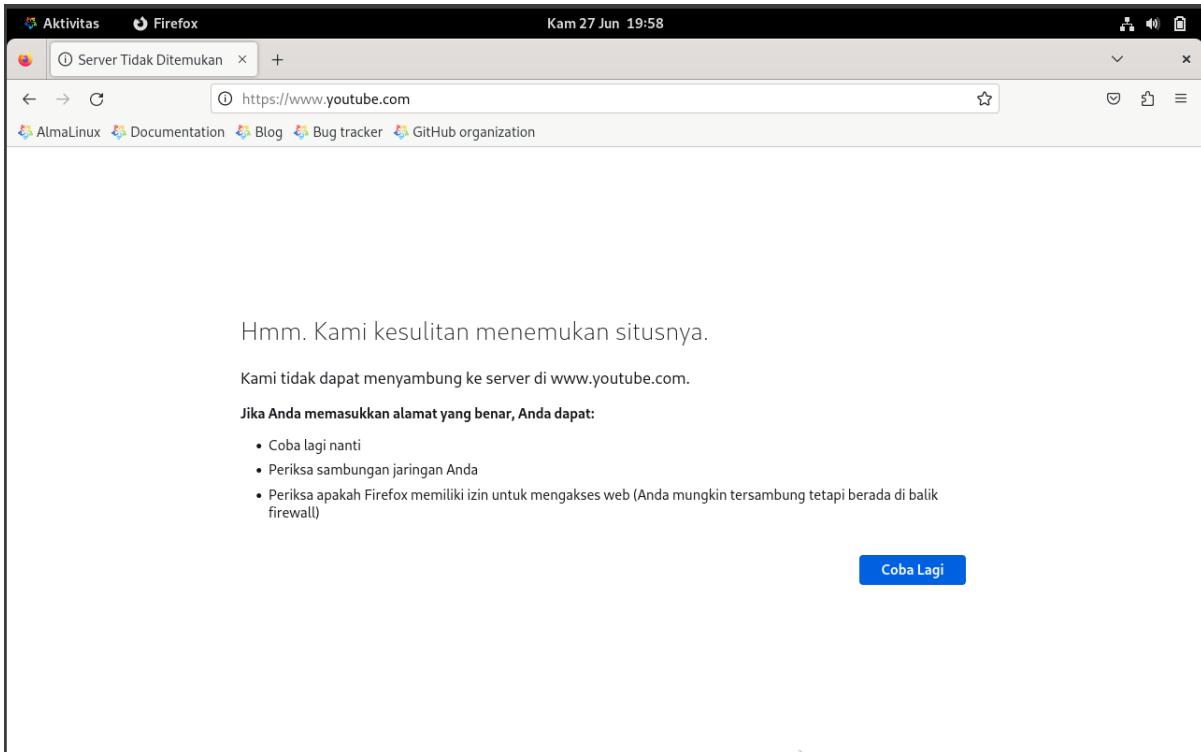
4. Uji konektifitas pada VM management firewall ke internal firewall



5. Uji konektifitas pada VM management firewall ke eksternal firewall

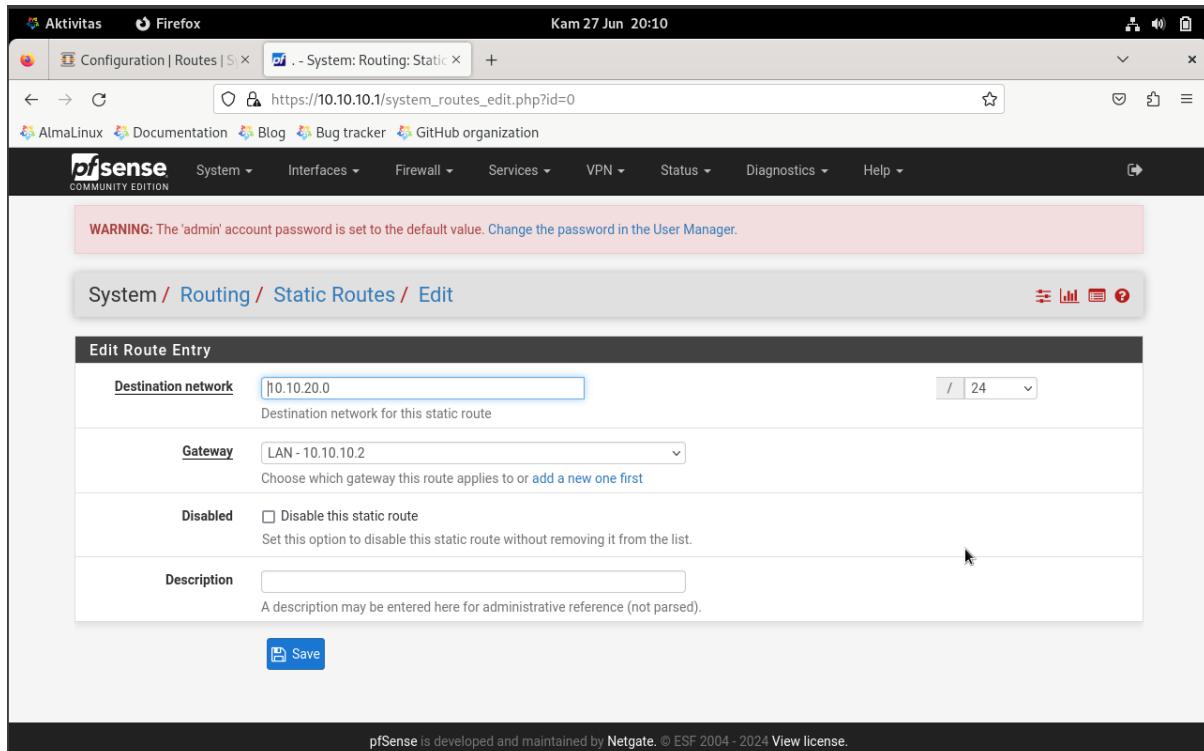


6. Uji vm management firewall terhubung ke internet, masih belum terhubung karena aturan default pada opnsense memblokir semua jaringan yang masuk, jadi perlu menambahkan rules baru.



IX. Konfigurasi VM management firewall terhubung internet

1. Masuk pada web gui pfsense lalu pada system->routing->static route->add , lalu isikan pada destination network pada subnet 10.10.20.0 dan gateway 10.10.10.2 lalu save



2. Uji konektifitas pada eksternal firewall ping ke vm management firewall

```
Berkas Mesin Tilik Masukan Peranti Bantuan
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell

Enter an option: 7

Enter a host name or IP address: 10.10.20.10

PING 10.10.20.10 (10.10.20.10): 56 data bytes
64 bytes from 10.10.20.10: icmp_seq=0 ttl=63 time=1.272 ms
64 bytes from 10.10.20.10: icmp_seq=1 ttl=63 time=1.163 ms
64 bytes from 10.10.20.10: icmp_seq=2 ttl=63 time=1.012 ms

--- 10.10.20.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.012/1.149/1.272/0.107 ms

Press ENTER to continue.
SS
```

3. Masuk ke firewall->NAT->outbound dan pilih hybrid outbound nat rule generation klik save

The screenshot shows the pfSense web interface. The top navigation bar includes 'Aktivitas', 'Firefox', 'Configuration | Routes | S', 'Firewall: NAT: Outbound', 'terjemahan - Penelusuran', and a '+' button. Below the navigation is a toolbar with links to 'AlmaLinux', 'Documentation', 'Blog', 'Bug tracker', and 'GitHub organization'. The main content area has a header 'Firewall / NAT / Outbound'. Below it, tabs for 'Port Forward', '1:1', 'Outbound' (which is selected), and 'NPT' are shown. A red warning message 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' is displayed. The 'Outbound NAT Mode' section contains four radio buttons: 'Automatic outbound NAT rule generation. (IPsec passthrough included)', 'Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)' (which is selected), 'Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)', and 'Disable Outbound NAT rule generation. (No Outbound NAT rules)'. At the bottom of this section is a blue 'Save' button.

4. Lalu pada bagian mapping klik add masukan interface WAN, protocol any, source network 10.10.10.0/24, destination any, dan address interface address lalu klik save

The screenshot shows the pfSense 'firewall_nat_out_edit.php?id=0' configuration page. The top navigation and toolbar are identical to the previous screenshot. The main form has sections for 'Disabled' (unchecked), 'Do not NAT' (unchecked), 'Interface' (set to 'WAN'), 'Address Family' (set to 'IPv4+IPv6'), 'Protocol' (set to 'any'), 'Source' (Type 'Network' with '10.10.10.0 / 24'), 'Destination' (Type 'Any'), and 'Not' (unchecked). The 'Translation' section has 'Address' set to 'Interface Address'. A note at the bottom states: 'Connections matching this rule will be mapped to the specified Address. The Address can be an Interface, a Host-type Alias, or a Virtual IP address.'

5. Hasil akan seperti gambar dibawah ini

The screenshot shows a Firefox browser window with the URL https://10.10.10.1/firewall_nat_out.php. The page title is "Firewall / NAT / Outbound". Below the title, there are tabs: Port Forward, 1:1, Outbound (which is selected), and NPT. Under "Outbound NAT Mode", the "Hybrid Outbound NAT rule generation" option is selected. A "Save" button is visible. The "Mappings" section contains a table with one entry: WAN (Interface) with Source 10.10.10.0/24, Destination * (Source Port *), Destination Port 500 (Destination Port *), NAT Address WAN address, NAT Port *, Static Port *, Description "Auto created rule for ISAKMP". Below this is a table titled "Automatic Rules:" with two entries: WAN (Interface) with Source 127.0.0.0/8 :1/128 10.10.20.0/24, Destination * (Source Port *), Destination Port 500 (Destination Port *), NAT Address WAN address, NAT Port *, Static Port *, Description "Auto created rule".

6. Selanjutnya masuk ke web gui internal firewall ke menu firewall->rules->wan lalu klik add pada bagian action pilih pass, interface wan, direction in, protocol any, source pilih single host or network lalu masukan network 10.10.10.0/24 , dan pada destination pilih any, lalu klik save

The screenshot shows a web-based configuration interface for OPNsense. The left sidebar has a "WAN" section selected. The main area is titled "Firewall: Rules: WAN" and shows the "Edit Firewall rule" form. The form fields are: Action (Pass), Disabled (unchecked), Quick (checked), Interface (WAN), Direction (in), TCP/IP Version (IPv4), Protocol (any), Source / Invert (unchecked), and Source (empty). At the bottom of the form, it says "OPNsense (c) 2014-2024 Deciso B.V."

Aktivitas Firefox Kam 27 Jun 20:24

WAN | Rules | Firewall - Services: DHCP Server + https://10.10.20.1/firewall_rules_edit.php?if=wan&id=0

AlmaLinux Documentation Blog Bug tracker GitHub organization

OPNsense

Protocol: any
Source / Invert: Use this option to invert the sense of the match.
Source: Single host or Network
10.10.10.0 24
Source: Advanced
Destination / Invert: Use this option to invert the sense of the match.
Destination: any
Destination port range: from: any to: any
Log: Log packets that are handled by this rule
Category:

OPNsense (c) 2014-2024 Deciso B.V.

Aktivitas Firefox Kam 27 Jun 20:27

WAN | Rules | Firewall - Services: DHCP Server + https://10.10.20.1/firewall_rules.php?f=wan

AlmaLinux Documentation Blog Bug tracker GitHub organization

OPNsense

Firewall: Rules: WAN

Select category: Automatically generated rules

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	Action
IPv4 *	10.10.10.0/24	*	*	*	*	*		
pass	block	reject	reject	log	log	in	first match	
pass (disabled)	block (disabled)	reject (disabled)	reject (disabled)	log (disabled)	log (disabled)	out	last match	

Active/Inactive Schedule (click to view/edit)
Alias (click to view/edit)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

OPNsense (c) 2014-2024 Deciso B.V.

- Setting routing pada internal firewall klik add masukan network 0.0.0.0/0 dan gateway 10.10.10.1

System: Routes: Configuration

Disabled	Network	Gateway	Description	Commands
<input type="checkbox"/>	0.0.0.0/0	pfsense_gw - 10.10.10.1		Edit Delete Details

Showing 1 to 1 of 1 entries

Do not enter static routes for networks assigned on any interface of this firewall. Static routes are only used for networks reachable via a different router, and not reachable via your default gateway.

Apply

- Lalu konfigurasi pada outbound pilih mode hybrid, lalu add rules interface wan lalu konfigurasi seperti gambar dibawah ini lalu klik save

Firewall: NAT: Outbound

Mode

- Automatic outbound NAT rule generation (no manual rules can be used)
- Hybrid outbound NAT rule generation (automatically generated rules are applied after manual rules)
- Manual outbound NAT rule generation (no automatic rules are being generated)
- Disable outbound NAT rule generation (outbound NAT is disabled)

Save

Manual rules

Select category	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
	WAN	10.10.20.0/24	*	*	*	Interface address	*	NO	

Automatic rules

OPNsense (c) 2014-2024 Deciso B.V.

Kam 27 Jun 20:41

Outbound | NAT | Firewall . - Services: DHCP Server +

AlmaLinux Documentation Blog Bug tracker GitHub organization

root@OPNsense.localdomain

Firewall: NAT: Outbound

Edit Advanced Outbound NAT entry

full help

Disabled	<input type="checkbox"/> Disable this rule
Do not NAT	<input type="checkbox"/>
Interface	WAN
TCP/IP Version	IPv4
Protocol	any
Source invert	<input type="checkbox"/>
Source address	Single host or Network 10.10.20.0 24
Source port	any

OPNsense (c) 2014-2024 Deciso B.V.

This screenshot shows the 'Edit Advanced Outbound NAT entry' configuration page. The 'Source address' field is set to 'Single host or Network' with the value '10.10.20.0' and a subnet mask of '24'. Other fields include 'Interface' (WAN), 'TCP/IP Version' (IPv4), 'Protocol' (any), and 'Source port' (any). There are also sections for 'Do not NAT', 'Source invert', and 'Translation / target'.

Kam 27 Jun 20:41

Outbound | NAT | Firewall . - Services: DHCP Server +

AlmaLinux Documentation Blog Bug tracker GitHub organization

root@OPNsense.localdomain

Firewall: NAT: Outbound

Source port	10.10.20.0 24
Destination invert	<input type="checkbox"/>
Destination address	any
Destination port	any
Translation / target	Interface address
Log	<input type="checkbox"/> Log packets that are handled by this rule
Translation / port:	<input type="text"/>
Static-port:	<input type="checkbox"/>
Pool Options:	Default

OPNsense (c) 2014-2024 Deciso B.V.

This screenshot shows the 'Edit Advanced Outbound NAT entry' configuration page. The 'Source port' field is set to '10.10.20.0 24'. Other fields include 'Destination address' (any), 'Translation / target' (Interface address), and 'Log' (checked). There are also sections for 'Destination port', 'Translation / port:', 'Static-port:', and 'Pool Options'.

9. Lalu pada menu firewall tambahkan aturan baru pada LAN seperti gambar dibawah ini dengan action pass dimana semua alamat dari semua lan network ke semua destination di bolehkan.

Screenshot 1: Firewall: Rules: LAN (Basic Rule)

Action	Pass
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	any
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	any

Screenshot 2: Firewall: Rules: LAN (Advanced Rule)

Source	LAN net
Source	Advanced
Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination	any
Destination port range	from: any to: any
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule
Category	any
Description	access valid
No XMLRPC Sync	<input type="checkbox"/>
Schedule	any

10. Cek koneksi vm management firewall dengan internet dan terhubung

11. Cek pada log files pada lan dan berhasil.

The screenshot shows the OPNsense Firewall Log Files interface. The left sidebar menu includes Firewall, Aliases, Automation, Categories, Groups, NAT, Rules, Shaper, Settings, Log Files (selected), General, Live View, Overview, Plain View, Diagnostics, VPN, Services, Power, and Help. The main content area displays a table of log entries for the 'lan' interface. The table columns are Interface, Time, Source, Destination, Proto, and Label. The logs show various network interactions, such as TCP and UDP connections to and from the LAN interface at different times on June 28, 2024. A filter bar at the top allows for interface selection and other search criteria. A status bar at the bottom indicates the session is running on root@OPNsense.localdomain.

Interface	Time	Source	Destination	Proto	Label
lan	2024-06-28T10:24:58	10.10.20.10:52508	10.10.20.1:443	tcp	anti-lockout rule
lan	2024-06-28T10:24:55	10.10.20.10:57717	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:24:55	10.10.20.10:42752	172.217.194.103:443	tcp	access valid
lan	2024-06-28T10:24:55	10.10.20.10:48437	172.217.194.105:443	udp	access valid
lan	2024-06-28T10:24:55	10.10.20.10:42750	172.217.194.103:443	tcp	access valid
lan	2024-06-28T10:24:55	10.10.20.10:38848	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:24:55	10.10.20.10:46025	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:24:54	10.10.20.10:42258	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:24:46	10.10.20.10:34375	172.217.194.157:443	udp	access valid
lan	2024-06-28T10:24:46	10.10.20.10:55810	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:24:41	10.10.20.10:60160	203.89.31.10:123	udp	access valid
lan	2024-06-28T10:24:12	10.10.20.10:46793	103.155.196.116:123	udp	access valid
lan	2024-06-28T10:23:57	10.10.20.10:38233	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:23:57	10.10.20.10:56582	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:23:35	10.10.20.10:35573	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:23:35	10.10.20.10:46274	10.10.20.1:53	udp	access valid

X. Update seluruh VM

1. Update opnsense internal firewall

The screenshot shows the OPNsense web interface with the URL <https://10.10.20.1/ui/core/firmware#updates>. The left sidebar has a 'Firmware' section selected. The main content area displays a table of updates:

Paket	Versi Saat Ini	Versi Terbaru	Status	Aksi
py311-ujson	N/A	5.10.0	new	OPNsense
py311-urllib3	N/A	1.26.18_1,1	new	OPNsense
py311-vici	N/A	5.9.11	new	OPNsense
py311-yaml	N/A	6.0.1	new	OPNsense
python39	3.9.18_1	N/A	obsolete	OPNsense
python311	N/A	3.11.9	new	OPNsense
radvd	2.19_2	2.19_3	upgrade	OPNsense
readline	8.2.7_1	8.2.10	upgrade	OPNsense
rrdtool	1.8.0_3	1.8.0_4	upgrade	OPNsense
sqlite3	3.45.0_1,1	3.46.0_1	upgrade	OPNsense
strongswan	5.9.13	5.9.14	upgrade	OPNsense
sudo	1.9.15p5_3	1.9.15p5_4	upgrade	OPNsense
suricata	7.0.2_3	7.0.5_1	upgrade	OPNsense
syslog-ng	4.4.0	4.7.1	upgrade	OPNsense
unbound	1.19.0	1.20.0_1	upgrade	OPNsense

Message at the bottom: There are 176 updates available, total download size is 297.5MB. This update requires a reboot.

2. Update pfSense internal firewall

The screenshot shows the pfSense web interface with the URL https://10.10.10.1/pkg_mgr_install.php?id=firmware. The left sidebar has a 'System' section selected. A warning message at the top says: WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

The main content area shows the 'System / Update / System Update' page. It has two tabs: 'System Update' (selected) and 'Update Settings'. A confirmation dialog box is open:

Confirmation Required to update pfSense system.

Branch: Current Stable Release (2.7.0-RELEASE)

Please select the branch from which to update the system firmware.
Use of the development version is at your own risk!

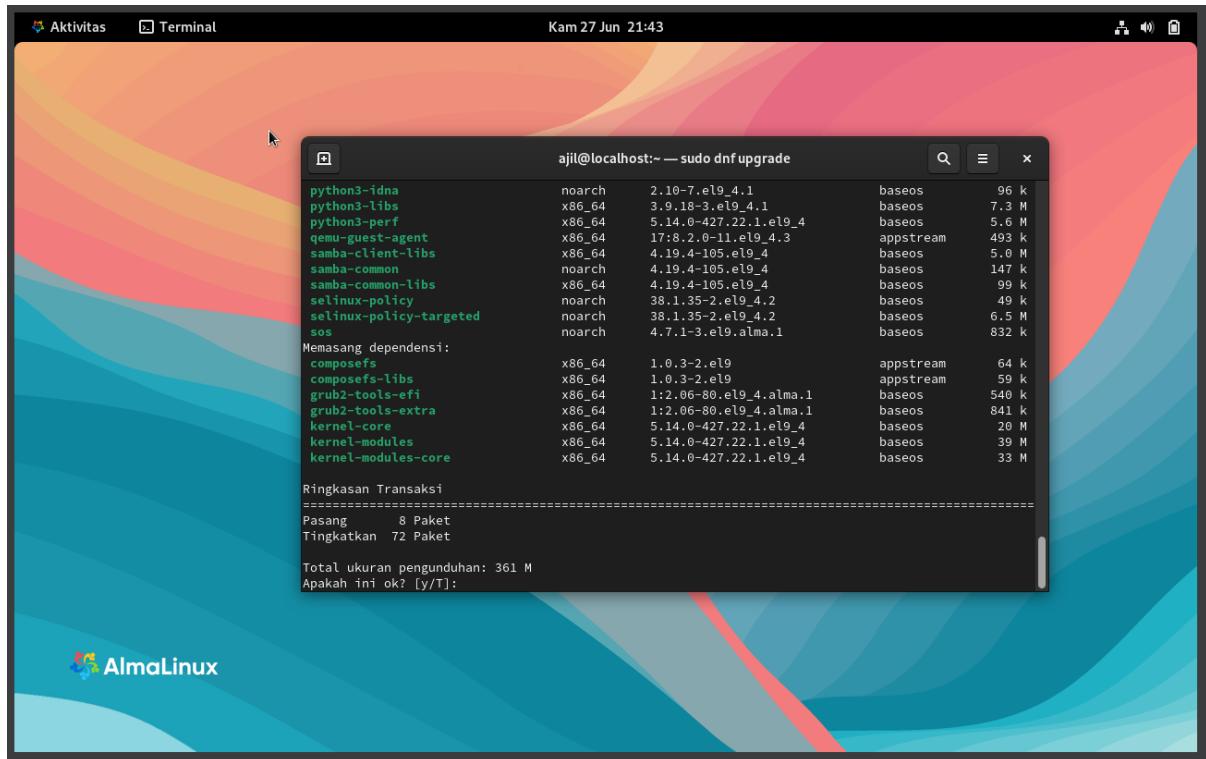
Current Base System: 2.4.5

Latest Base System: 2.7.0

Confirm Update: Confirm

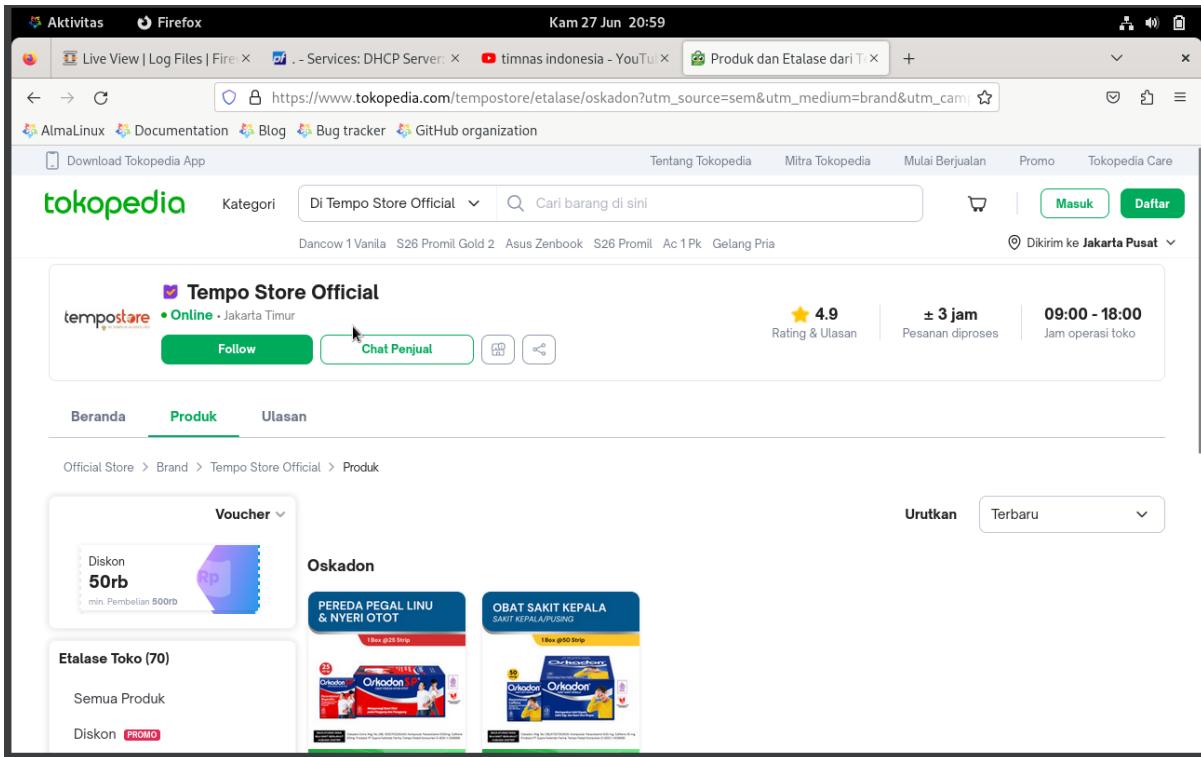
At the bottom: 10.10.10.1 and pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).

3. Update vm management firewall alma linux



XI. Membuat contoh rule baru yang di set pada internal firewall

- Disini mencoba untuk menambahkan rule baru untuk akses sites contoh menggunakan tokopedia pada halaman ini masih bisa kita akses untuk memblokir akses tersebut kita menambahkan rule baru



Aktivitas Firefox Kam 27 Jun 20:59

Live View | Log Files | Fire . - Services: DHCP Server: timnas indonesia - YouT Produk dan Etalase dari Tokopedia +

AlmaLinux Documentation Blog Bug tracker GitHub organization

Download Tokopedia App Tentang Tokopedia Mitra Tokopedia Mulai Berjualan Promo Tokopedia Care

tokopedia Kategori Di Tempo Store Official Cari barang di sini Masuk Daftar

Dancow 1 Vanila S26 Promil Gold 2 Asus Zenbook S26 Promil Ac 1Pk Gelang Pria Dikirim ke Jakarta Pusat

Tempo Store Official tempo store • Online • Jakarta Timur Follow Chat Penjual Rating & Ulasan ± 3 jam Pesanan diproses 09:00 - 18:00 Jam operasi toko

Beranda Produk Ulasan

Official Store > Brand > Tempo Store Official > Produk

Voucher

Diskon 50rb min. Pembelian 500rb

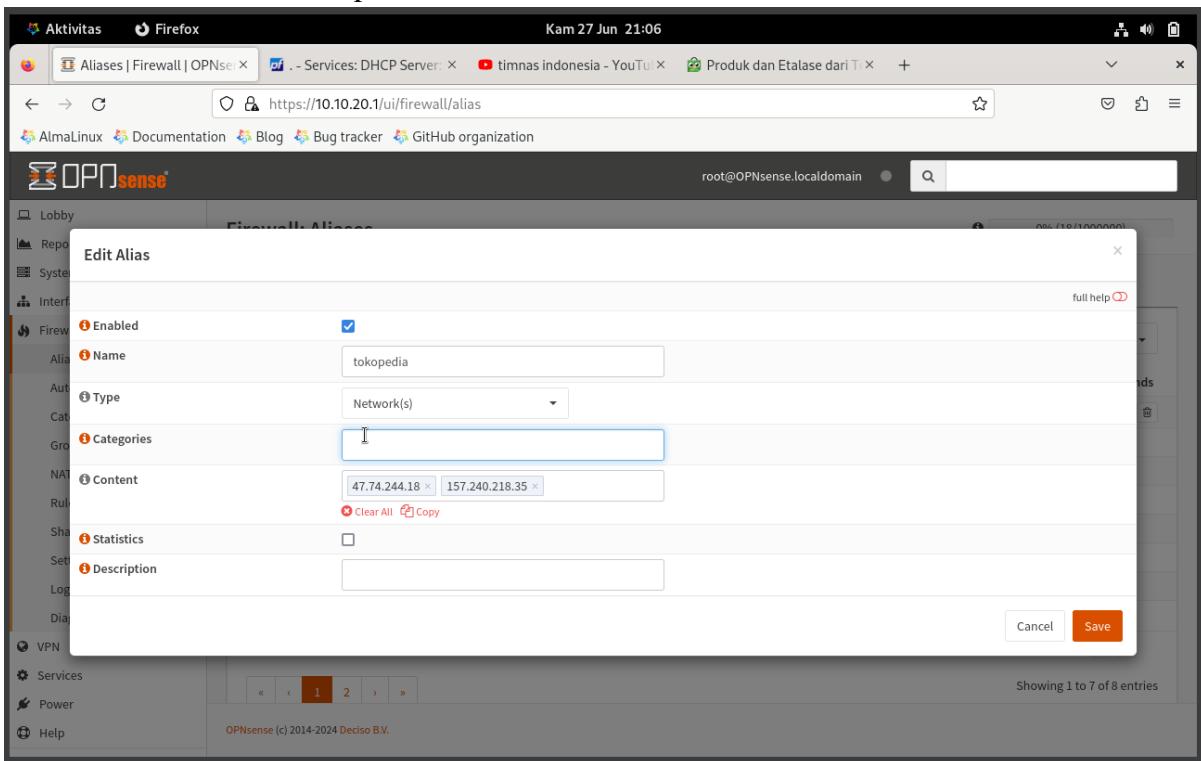
Etalase Toko (70)

Semua Produk Diskon PROMO

Oskadon PEREDA PEGAL LINU & NYERI OTOT OBAT SAKIT KEPALA SAKIT KEPALA/PUSING

Urutkan Terbaru

- Pada menu firewall->aliases lalu klik add dan masukan type network dengan content berisi address tokopedia lalu klik save



Aktivitas Firefox Kam 27 Jun 21:06

Aliases | Firewall | OPNsense . - Services: DHCP Server: timnas indonesia - YouT Produk dan Etalase dari Tokopedia +

AlmaLinux Documentation Blog Bug tracker GitHub organization

Lobby Firewall Aliases

Edit Alias

Enabled

Name: tokopedia

Type: Network(s)

Categories:

Content: 47.74.244.18 157.240.218.35

Statistics

Description

Cancel Save

Showing 1 to 7 of 8 entries

OPNsense (c) 2014-2024 Deciso B.V.

Kam 27 Jun 21:07

Aliases | Firewall | OPNsense | . - Services: DHCP Server | timnas indonesia - YouTube | Produk dan Etalase dari T... | +

AlmaLinux Documentation Blog Bug tracker GitHub organization

root@OPNsense.localdomain

Firewall: Aliases

Enabled	Name	Type	Description	Content	Loaded#	Last up...	Commands
<input type="checkbox"/>	<input checked="" type="checkbox"/> tokopedia	Network(s)	47.74.244.1...	2	2024-06-26 ...		
<input type="checkbox"/>	<input checked="" type="checkbox"/> bogons	External (advanced)	bogon net...	10			
<input type="checkbox"/>	<input checked="" type="checkbox"/> bogonsv6	External (advanced)	bogon net...				
<input type="checkbox"/>	<input checked="" type="checkbox"/> virusprot	External (advanced)	overload ta...	0			
<input type="checkbox"/>	<input checked="" type="checkbox"/> sshlockout	External (advanced)	abuse lock...	0			
<input type="checkbox"/>	<input checked="" type="checkbox"/> __wan_network	Internal (automatic)	wan net	1			
<input type="checkbox"/>	<input checked="" type="checkbox"/> __lan_network	Internal (automatic)	lan net	1			

Showing 1 to 7 of 8 entries

OPNsense (c) 2014-2024 Deciso B.V.

3. Lalu masuk pada rules->lan lalu klik add tambahkan rules seperti gambar dibawah ini, lalu klik save

Kam 27 Jun 20:43

LAN | Rules | Firewall | OPNsense | . - Services: DHCP Server | +

AlmaLinux Documentation Blog Bug tracker GitHub organization

root@OPNsense.localdomain

Firewall: Rules: LAN

Edit Firewall rule

Action	Block
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	any
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	

full help

OPNsense (c) 2014-2024 Deciso B.V.

The screenshot shows the OPNsense Firewall Rules Edit interface. On the left, a sidebar lists various firewall categories: Firewall, Aliases, Automation, Categories, Groups, NAT, Rules (selected), Floating, LAN (selected), Loopback, WAN, Shaper, Settings, Log Files, and Diagnostics. The main panel displays a configuration form for a rule:

- Source / Invert:** Use this option to invert the sense of the match.
- Source:** LAN net
- Source port range:** from: any to: any
- Destination / Invert:** Use this option to invert the sense of the match.
- Destination:** tokopedia
- Destination port range:** from: any to: any
- Log:** Log packets that are handled by this rule
- Category:** (empty)
- Description:** tokopedia is blocked

At the bottom of the main panel, it says "OPNsense (c) 2014-2024 Deciso B.V."

4. Mencoba ulang akses masuk ke halaman tokopedia tidak berhasil

The screenshot shows a Google search results page for the query "tokopedia". The search bar at the top contains "tokopedia". Below the search bar, there are several sponsored links and organic search results. On the right side of the page, there is a detailed information box for Tokopedia:

- Bersponsor:**
 - Tokopedia (<https://www.tokopedia.com>)
 - Tokopedia | Karena Tokopedia Selalu Ada**
Belanja Apa Aja Pasti Hemat di Tokopedia! Selalu Ada, Selalu Bisa. Apapun Kebutuhanmu, Tokopedia Selalu Ada & Selalu Bisa Hemat. Bisa Same Day Delivery. Bebas Ongkir.
 - Official Store**
Berbagai Official Store Ada Disini Diskon Spesial Dari Brand Ternama
 - Promo Hari Ini**
Dapatkan Promo Hari Ini Di Sini Di Jamin Ada Promo dan Cashback
- Tokopedia**
Perusahaan :
PT Tokopedia merupakan perusahaan teknologi Indonesia dengan misi pemerataan ekonomi secara digital di Indonesia. Visi perusahaan adalah untuk menciptakan ekosistem di mana siapa pun bisa memulai dan menemukan apa pun. [Wikipedia](#)
- Pendiri:** William Tanuwijaya, Leontinus Alpha Edison
- Organisasi induk:** GoTo Group, TikTok
- Didirikan:** 17 Agustus 2009
- Pembuat:** William Tanuwijaya dan Leontinus Alpha Edison
- Pemilik:** GoTo (25%), TikTok (75%)
- Tipe:** Perdagangan

Below the information box, it says "Orang lain juga menelusuri" followed by a list of related queries. At the very bottom of the page, there is a URL: <https://www.googleadservices.com/pagead/aclick?sa=L&ai=DChcSEwiiq7Tkjv6GAxUipGYC...o1rBwxMl0vzKIQ&q&adurl&ved=2ahUKEwj0q7Dkjv6GAxXuhGMGH5dbAHUQ0Qx6BAgGEAE&nis=8>.

5. Tampilan log ketika akses tokopedia

The screenshot shows the OPNsense Firewall Log Files: Live View interface. The left sidebar menu includes Firewall, Aliases, Automation, Categories, Groups, NAT, Rules, Shaper, Settings, Log Files (with Live View selected), Overview, Plain View, and Diagnostics. The main panel displays a table of log entries with the following columns: Interface, Time, Source, Destination, Proto, and Label. A search bar at the top allows filtering by interface (set to 'lan'), contains ('lan'), and a dropdown for choosing a template. There are also checkboxes for 'Auto refresh' and 'Lookup hostnames'. The log table shows several entries, mostly in red, indicating blocked traffic from the LAN interface (lan) to various external IP addresses (e.g., 10.10.20.10, 47.74.244.18:443, 172.217.194.147:443) on port 443 (tcp). Some entries are in green, indicating valid access (e.g., 10.10.20.10:56148 to 172.217.194.147:443 on udp).

Interface	Time	Source	Destination	Proto	Label
lan	2024-06-28T10:48:03	10.10.20.10:53950	47.74.244.18:443	tcp	tokopedia is blocked
lan	2024-06-28T10:48:03	10.10.20.10:53936	47.74.244.18:443	tcp	tokopedia is blocked
lan	2024-06-28T10:48:01	10.10.20.10:53950	47.74.244.18:443	tcp	tokopedia is blocked
lan	2024-06-28T10:48:01	10.10.20.10:53936	47.74.244.18:443	tcp	tokopedia is blocked
lan	2024-06-28T10:48:01	10.10.20.10:56148	172.217.194.147:443	udp	access valid
lan	2024-06-28T10:48:00	10.10.20.10:53950	47.74.244.18:443	tcp	tokopedia is blocked
lan	2024-06-28T10:48:00	10.10.20.10:53936	47.74.244.18:443	tcp	tokopedia is blocked
lan	2024-06-28T10:48:00	10.10.20.10:56309	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:47:49	10.10.20.10:47326	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:47:49	10.10.20.10:42346	10.10.20.1:53	udp	access valid
lan	2024-06-28T10:47:47	10.10.20.10:45342	47.74.244.18:443	tcp	tokopedia is blocked

XII. Kesimpulan

Menggunakan kombinasi dua firewall, yaitu pfSense dan OPNsense, dengan konfigurasi seperti yang dijelaskan, menawarkan lapisan perlindungan dan pengaturan jaringan yang lebih tersegmentasi dan aman. Di pfSense, jaringan diatur untuk menghubungkan jaringan internal ke internet dengan NAT dan berfungsi sebagai firewall utama yang mengelola lalu lintas dari dan ke internet. OPNsense, ditempatkan sebagai firewall tambahan antara pfSense dan VM Management Firewall di jaringan 10.10.10.0/24 dan 10.10.20.0/24, memperketat kontrol akses internal dengan aturan spesifik seperti memblokir akses ke situs tertentu seperti Tokopedia. Dengan cara ini, OPNsense memberikan kontrol granular pada lalu lintas internal dan memastikan kebijakan keamanan yang lebih ketat untuk lalu lintas antar-semen, sedangkan pfSense mengelola akses dan konektivitas yang lebih luas ke dan dari internet. Kombinasi ini memungkinkan pemisahan tanggung jawab antara konektivitas umum dan keamanan spesifik, meningkatkan fleksibilitas, manajemen, dan keamanan jaringan keseluruhan.

Daftar pustaka

[OPNsense® a true open source security platform and more - OPNsense® is a true open source firewall and more](#)

[pfSense CE RELEASE amd64 : pfSense : Free Download, Borrow, and Streaming : Internet Archive](#)

[AlmaLinux OS - Forever-Free Enterprise-Grade Operating System](#)

[ChatGPT](#)

<https://youtu.be/NE5xzb-qJgA?si=tuZBhVKk1ki8FsKr>

https://youtu.be/CcXYiFj9mBA?si=Ya6v1mtO1dD_Z7YT

<https://youtu.be/o12a2cFGopQ?si=HqQzZI0fTeiYI2KF>

Certified Network Defender (CND) Version 2 w/ iLabs (Volumes 1 through 4), 2nd Edition