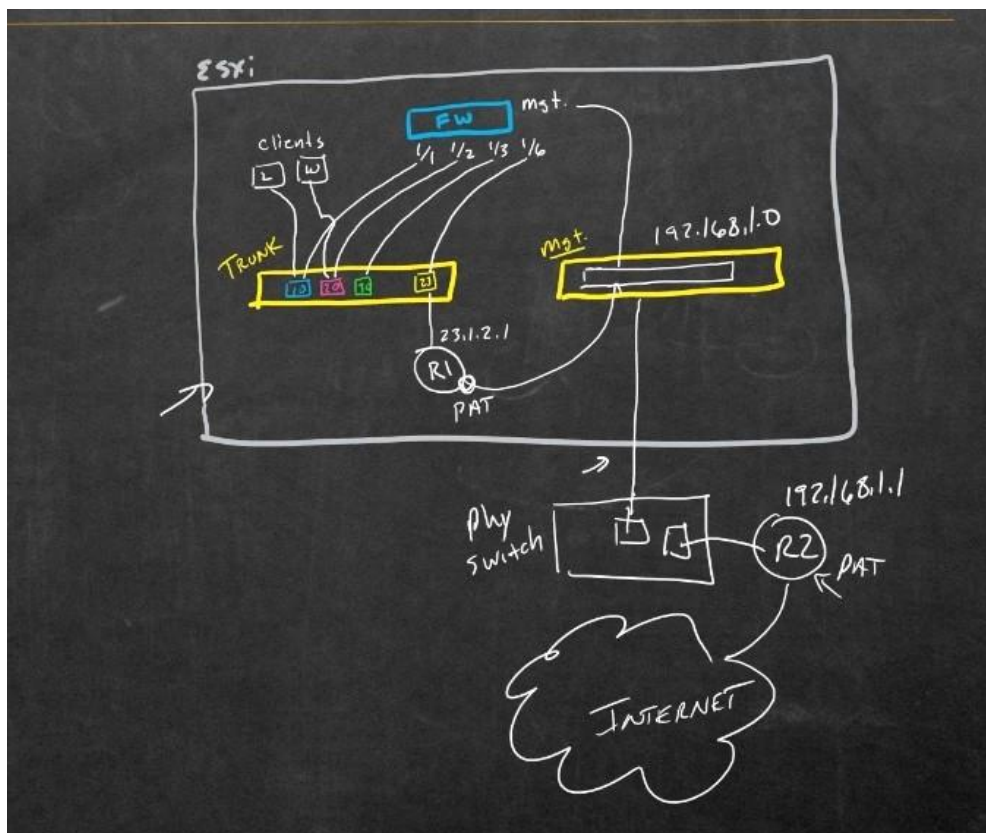
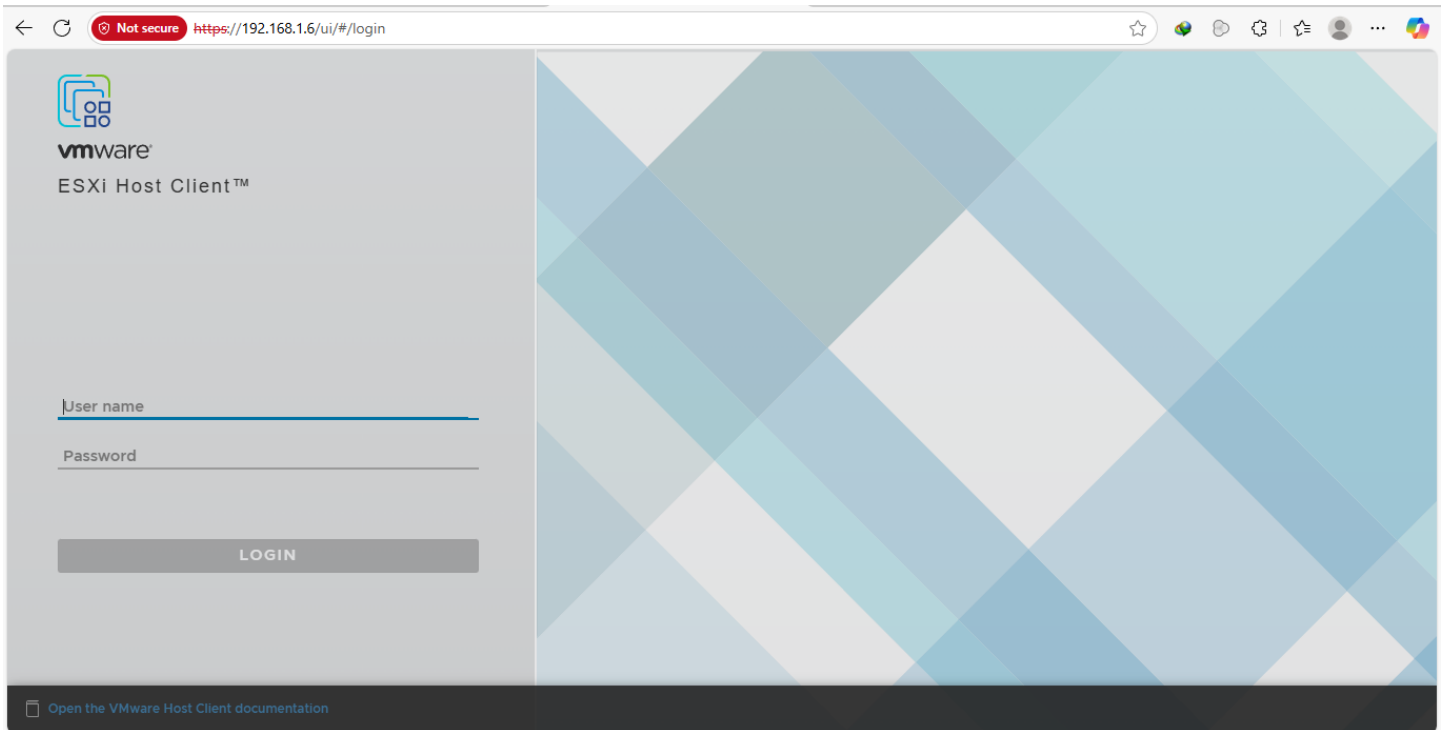
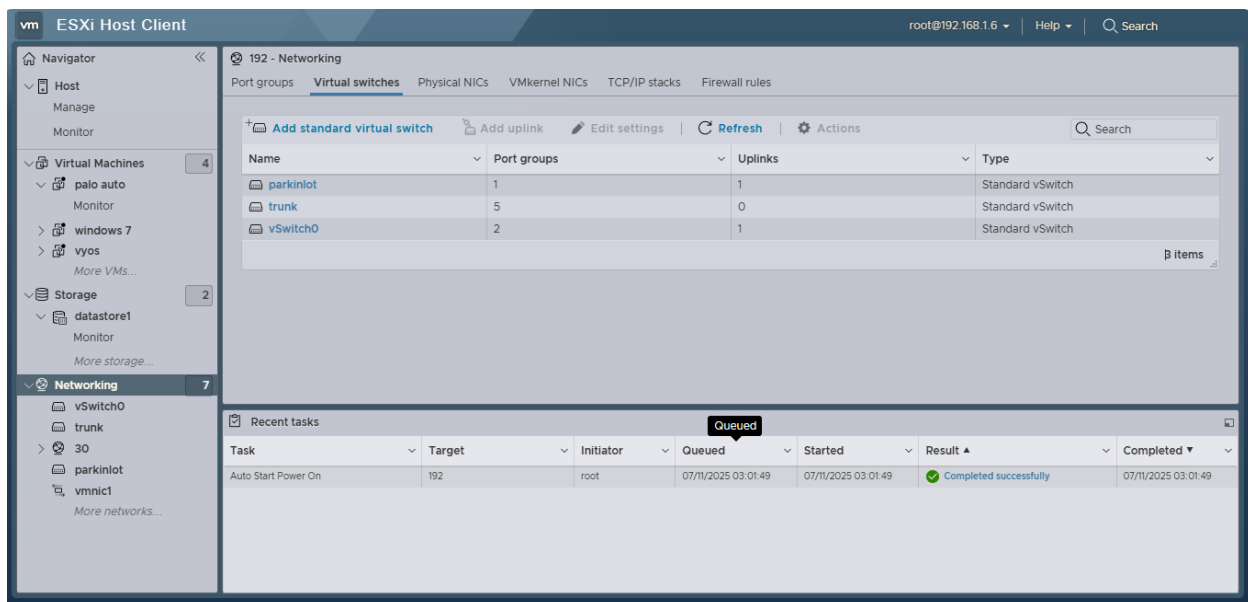


Virtual Network Lab





1. vSwitch0 – Home Network Switch

Purpose:

- Provides a connection between the virtual environment and the physical network.
- Allows virtual machines to access the internet and communicate with the home LAN.
- Enables remote management of the ESXi host and connected VMs.
- Used for VMs that require external connectivity, such as the Palo Alto firewall's WAN interface or a VPN server.

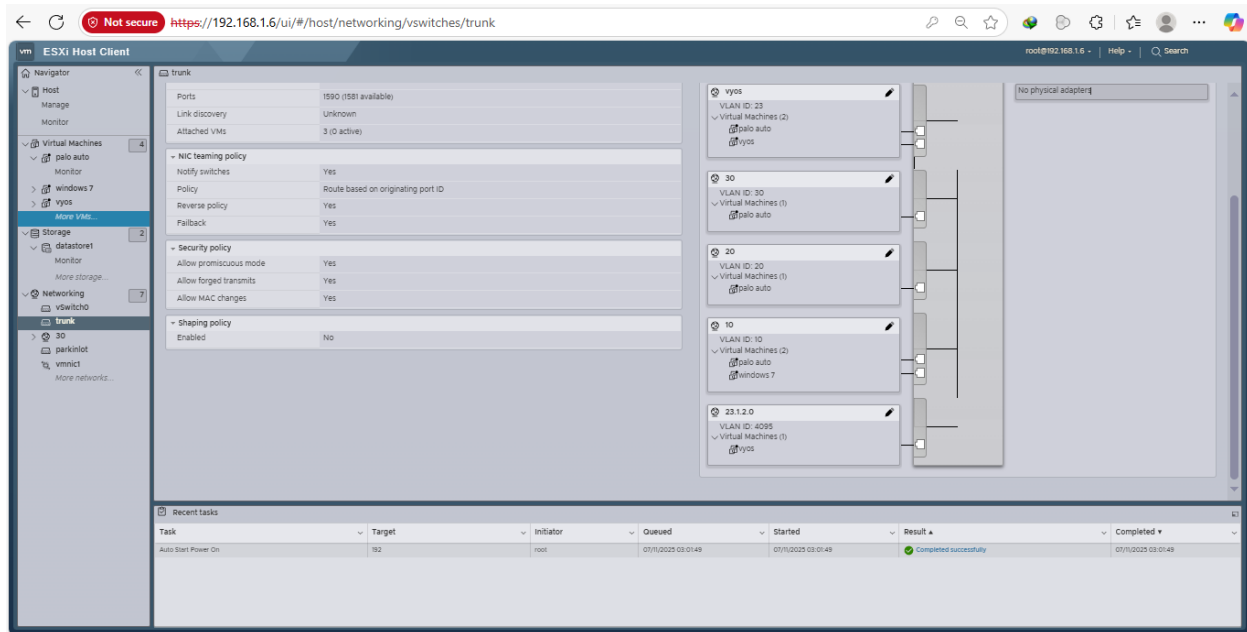
2. Trunking Switch – Internal Lab Switch

Purpose:

- Isolates internal virtual machines for secure and controlled communication.
- Used for VLAN-based network segmentation and inter-VLAN routing experiments.
- Does not connect directly to the physical network.
- Ideal for testing firewall rules, routing configurations, and security scenarios in a controlled environment.

P Unassigned Interfaces – Empty Parking Slots

- When a VM is created but **not yet connected to a switch**, it's like a **car without a parking spot**.
- I assign these VMs to a virtual switch later depending on what **traffic zone** they belong to.



Trunking Virtual Switch – Purpose and Port Group Configuration

The **Trunking Switch** in my ESXi lab is a dedicated virtual switch used for internal VM communication, VLAN segmentation, and firewall testing. It does **not connect to the physical network** directly. Instead, it provides isolated environments for advanced networking scenarios.

Purpose of Trunking Switch

- Enables communication between internal VMs using **VLAN-tagged traffic**.
- Isolates different traffic types (e.g., LAN, DMZ, WAN zones) for **firewall testing**.
- Allows **inter-VLAN routing** through a virtual router like VyOS.
- Helps simulate real-world enterprise segmentation for security and performance.

Port Group Configuration (Total: 5)

The Trunking Switch includes **five port groups**, each assigned to a specific VLAN or function. These port groups define how each VM's virtual NIC is tagged and how traffic is handled.

Port Group Name VLAN ID Purpose

Inside-Zone	10	LAN traffic behind the firewall
--------------------	----	---------------------------------

Port Group Name VLAN ID Purpose

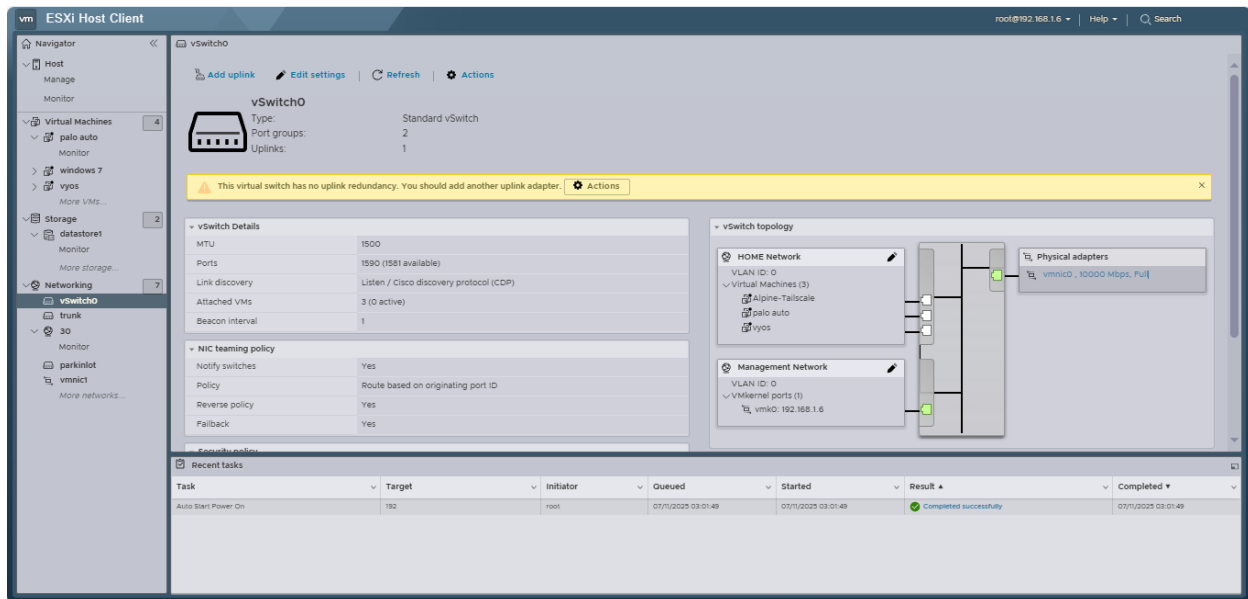
DMZ-Zone	20	Public-facing services for testing
Outside-Zone	30	WAN-side or internet-simulated traffic
Monitor-Zone	40	Used for packet capture and log analysis
All-Traffic (SPAN)	4095	Special mode to receive all VLAN traffic (promiscuous mode)

Special Note on VLAN 4095

- **VLAN ID 4095** is a special VLAN setting in ESXi that puts the port group in "**promiscuous mode.**"
 - It allows the connected VM (e.g., a firewall or packet sniffer) to **capture traffic from all VLANs** on that virtual switch.
 - This is used to **inspect, monitor, or log all internal traffic**, similar to a SPAN/mirror port in physical switches.
-

Use Case with Palo Alto Firewall

- Each port group is connected to a different interface (eth1, eth2, etc.) on the Palo Alto firewall.
- The firewall policies are applied between these zones to simulate enterprise-grade **zone-based security**.
- VLAN 4095 helps the firewall inspect all inter-VLAN traffic for **deep packet inspection and rule enforcement**.

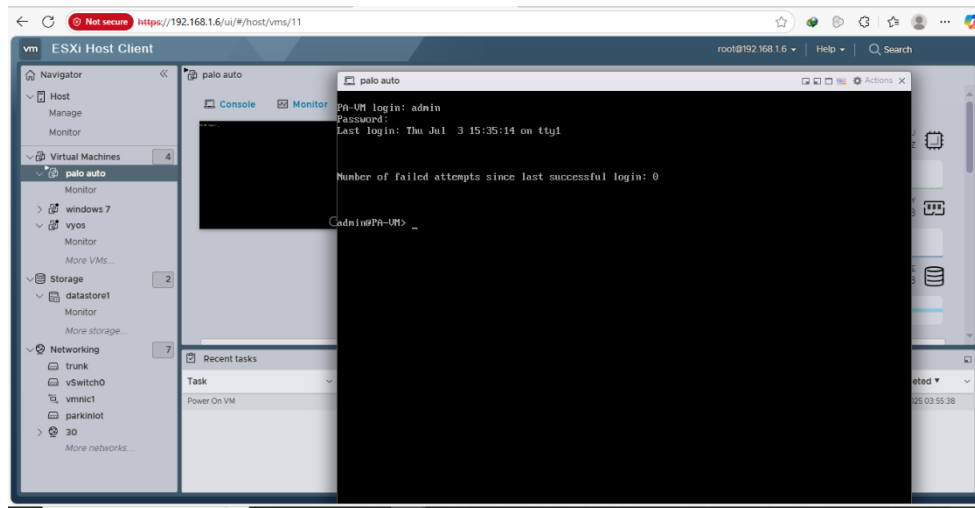


In my ESXi setup, **vSwitch0** is the virtual switch responsible for connecting the virtual environment to the **external physical network**. It includes a single port group called **Home Network**, which is used to provide **internet access** and **remote management** for the ESXi host and selected virtual machines.

The **Home Network Port Group** is bridged to the **physical NIC** of the host machine, allowing traffic to pass between the virtual machines and the real home network (LAN). This setup enables VMs like the **Palo Alto firewall's WAN interface** and the **APLinux VPN jump host** to reach the internet or be accessed remotely.

vSwitch0 is essential for external connectivity, secure remote access, and integrating the virtual lab with the physical world.

Palo Alto



In my virtual lab, I deployed a **Palo Alto Next-Generation Firewall (NGFW)** as a virtual machine on ESXi to simulate enterprise-grade security. The firewall is used to control and inspect traffic between different virtual zones, enabling deep packet inspection, NAT, and advanced threat prevention.

The firewall is connected to **multiple port groups** across two virtual switches:

- **WAN/Untrust Interface** is connected to the **Home Network Port Group** on vSwitch0 for internet access.
- **LAN, DMZ, and other zone interfaces** are connected to port groups on the **Trunking Switch**, each assigned to different VLANs (e.g., 10, 20, 30).

With this configuration, the firewall acts as a **central security device**, enforcing **zone-based policies**, performing **inter-VLAN routing**, and allowing **packet capture and monitoring**.

This setup allows me to simulate real-world firewall deployments and test access control, NAT, logging, and security rules across isolated environments.

In my ESXi setup, **vSwitch0** is the virtual switch responsible for connecting the virtual environment to the **external physical network**. It includes a single port group called **Home Network**, which is used to provide **internet access** and **remote management** for the ESXi host and selected virtual machines.

The **Home Network Port Group** is bridged to the **physical NIC** of the host machine, allowing traffic to pass between the virtual machines and the real home network (LAN). This setup enables VMs like the **Palo Alto firewall's WAN interface** and the **APLinux VPN jump host** to reach the internet or be accessed remotely.

vSwitch0 is essential for external connectivity, secure remote access, and integrating the virtual lab with the physical world.

←↻🔒 Not secure https://192.168.1.20/?#dashboard:vsys1

PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Commit

Layout3 ColumnsWidgetsLast updated04:05:245 mins

General Information

Device Name

PA-VM

MGT IP Address

192.168.1.20

MGT Netmask

255.255.255.0

MGT Default Gateway

192.168.1.1

MGT IPv6 Address

unknown

MGT IPv6 Link Local Address

fe80:20c:29ff:fe8:688b/64

MGT IPv6 Default Gateway

MGT MAC Address

00:0c:29:a8:68:8b

Model

PA-VM

Serial #

unknown

CPU ID

ESX:100F8700FFB8B17

UUID

14C24D56-B673-CB44-FEE1-D3DD01A8688B

VM Cores

2

VM Memory

5.32 GB

VM License

none

VM Capacity Tier

unknown

VM Mode

VMware ESXi

Software Version

11.1.4

GlobalProtect Agent

0.0.0

Logged In Admins

Admin	From	Client	Session Start	Idle For
_openconfig	127.0.0.1	Web	07/10/2025 15:27:34	00:07:49s
admin	192.168.1.10	Web	07/10/2025 15:35:03	00:00:03s
admin	Console	CLI	07/10/2025 15:32:12	00:03:11s

Data Logs

No data available.

System Logs

Description	Time
User admin logged in via Web from 192.168.1.10 using https	07/10 15:35:02
authenticated for user 'admin'. From: 192.168.1.10.	07/10 15:35:02
MLAV: Authentication or Client Certificate failure.	07/10 15:33:05
User admin logged in via CLI from Console	07/10 15:32:11
authenticated for user 'admin'. From: Console or telnet.	07/10 15:32:11
DHCP server auto-probe finished, turn on DHCP server since no offer received. Interface ethernet1/1	07/10 15:28:10

Config Logs

No data available.

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

No data found

admin | Logout | Last Login Time: 07/10/2025 15:32:11 | Session Expire Time: 08/09/2025 15:35:03 | Tasks | Language | paloalto

PA-VM

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICE

Commit

InterfacesZonesVLANsVirtual WiresVirtual RoutersIPSec TunnelsGRE TunnelsDHCPDNS ProxyProxyGlobalProtectPortalsGatewaysMDMClientless AppsClientless App GroupsQoSLLDPNetwork ProfilesGlobalProtect IPSec GryIKE GatewaysIPSec CryptoIKE Crypto

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

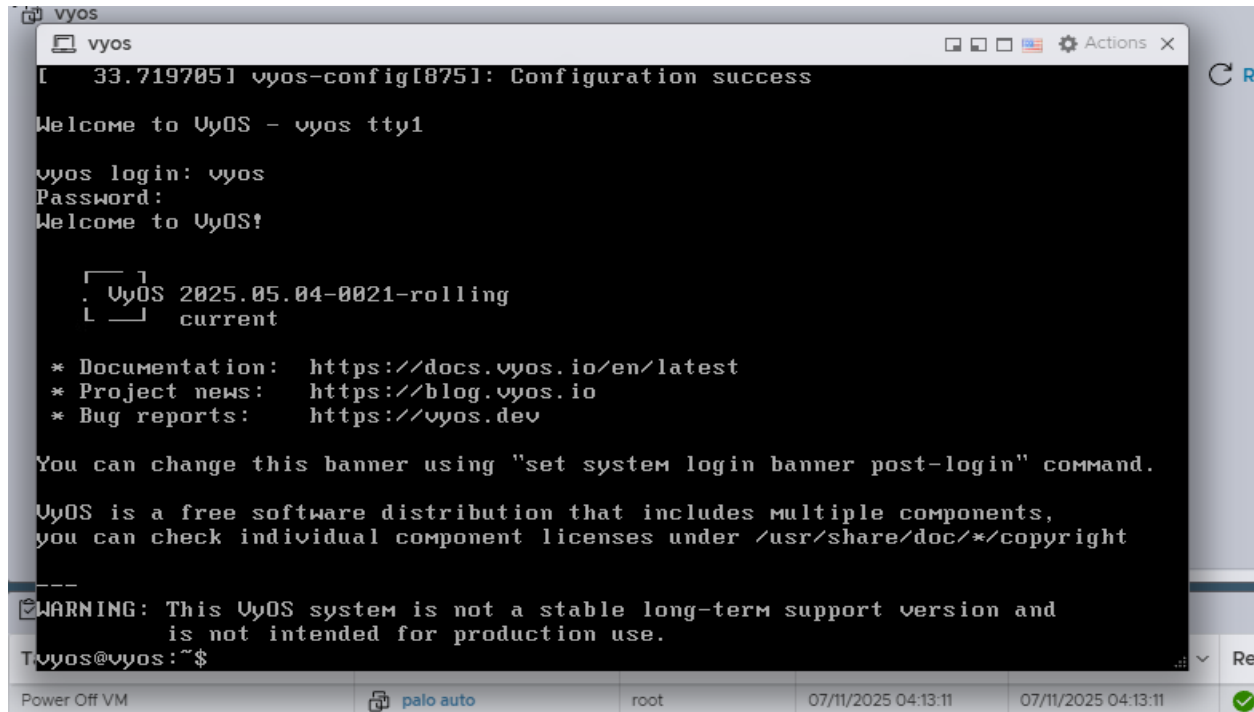
9 items

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT
ethernet1/1	Layer3	Allow-Ping And Https		10.10.0.15/24	our router	Untagged	none	inside		Disabled
ethernet1/2	Layer3	Allow-Ping And Https		10.20.0.15/24	our router	Untagged	none	inside		Disabled
ethernet1/3	Layer3	Allow-Ping And Https		10.30.0.15/24	our router	Untagged	none	inside		Disabled
ethernet1/4	Layer3			none	our router	Untagged	none	inside		Disabled
ethernet1/5	Layer3			none	our router	Untagged	none	inside		Disabled
ethernet1/6	Layer3	Allow-Ping And Https		23.1.2.15/24	our router	Untagged	none	out side		Disabled
ethernet1/7	Layer3			none	our router	Untagged	none	inside		Disabled
ethernet1/8				none	none	Untagged	none	none		Disabled
ethernet1/9				none	none	Untagged	none	none		Disabled

Add SubinterfaceAdd Aggregate GroupDeletePDF/CSV

admin | Logout | Last Login Time: 07/10/2025 15:32:11 | Session Expire Time: 08/09/2025 15:35:03 | Tasks | Language | paloalto

Vyos



```
vyos
[ 33.719705] vyos-config[8751]: Configuration success

Welcome to VyOS - vyos tty1

vyos login: vyos
Password:
Welcome to VyOS!

[ ] VyOS 2025.05.04-0021-rolling
[ ] current

* Documentation: https://docs.vyos.io/en/latest
* Project news: https://blog.vyos.io
* Bug reports: https://vyos.dev

You can change this banner using "set system login banner post-login" command.

VyOS is a free software distribution that includes multiple components,
you can check individual component licenses under /usr/share/doc/*/copyright

---
[WARNING: This VyOS system is not a stable long-term support version and
is not intended for production use.]
Tvyos@vyos:~$
```

Power Off VM	palo auto	root	07/11/2025 04:13:11	07/11/2025 04:13:11	Re
--------------	-----------	------	---------------------	---------------------	----

In my virtual lab, I use the **VyOS router VM** to manage internal network routing and provide **Network Address Translation (NAT)** services. It routes traffic between different VLANs inside the virtual environment and connects the internal network to the firewall.

The typical traffic flow is:

- Internal host machines send their traffic to the **Palo Alto firewall** for security inspection.
- The firewall forwards allowed traffic to the **VyOS router**.
- VyOS applies **NAT** and routes the traffic to the internet via the firewall's WAN interface.
- Incoming return traffic from the internet goes through the firewall and VyOS back to the internal hosts.

This design separates routing and security functions, enabling flexible network segmentation and controlled internet access for internal machines.


```
vyos
* Documentation: https://docs.vyos.io/en/latest
* Project news:  https://blog.vyos.io
* Bug reports:   https://vyos.dev

You can change this banner using "set system login banner post-login" command.

VyOS is a free software distribution that includes multiple components,
you can check individual component licenses under /usr/share/doc/*/copyright

---
WARNING: This VyOS system is not a stable long-term support version and
         is not intended for production use.
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface  IP Address      MAC                VRF      MTU    S/L    Descripti
on
-----
eth0       192.168.1.3/24   00:0c:29:85:3b:fc  default  1500   u/u
eth1       -               00:0c:29:85:3b:06  default  1500   u/u
eth1.10    -               00:0c:29:85:3b:06  default  1500   u/u
eth2       23.1.2.1/24     00:0c:29:85:3b:10  default  1500   u/u
lo         127.0.0.1/8     00:00:00:00:00:00  default  65536  u/u
::1/128

vyos@vyos:~$
```

Power Off VM | palo auto | root | 07/11/2025 04:13:11 | 07/11/2025 04:13:11 | ✓

VyOS Router Interface Configuration

In my virtual lab setup, the VyOS router has two main network interfaces with distinct roles:

- **eth0 (WAN interface):**
 - Connected to the outside network (ISP router).
 - Configured in **DHCP mode**, so it automatically obtains an IP address from the ISP or upstream router.
- **eth1 (LAN interface):**
 - Serves as the **NAT server** interface.
 - Handles traffic from internal VMs or networks, performing **Network Address Translation** to allow multiple internal hosts to share a single public IP address on eth0.

This configuration allows VyOS to act as a gateway between the internal virtual network and the external internet, managing IP addressing dynamically on the WAN side and providing NAT services for internal hosts.