PurpleSynapz™

ASSIGNMENT

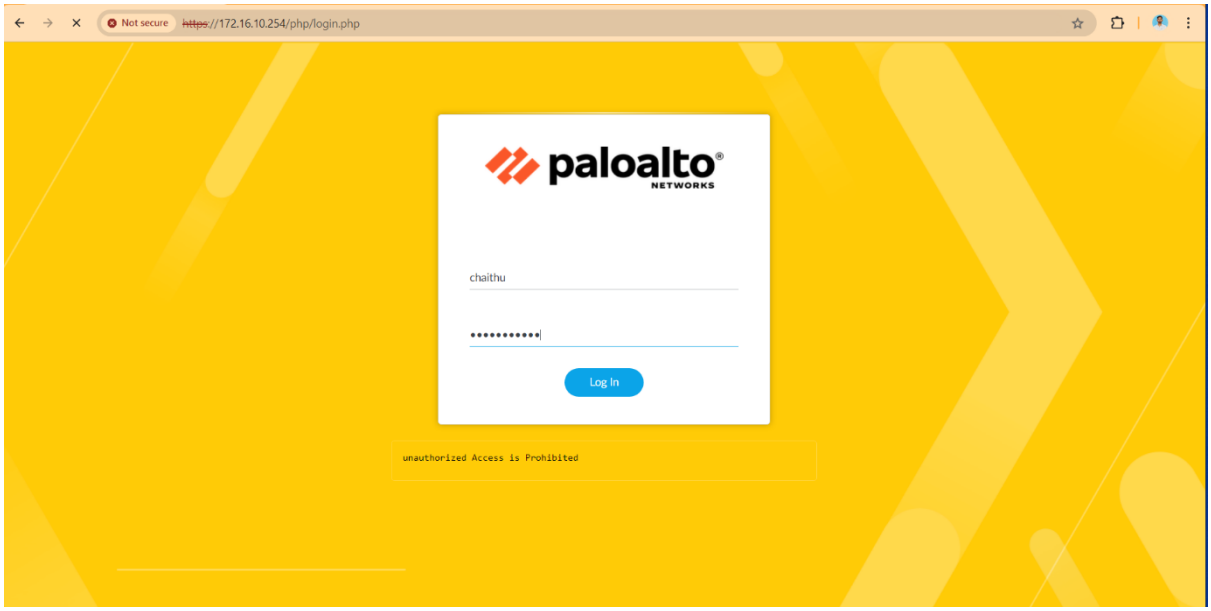
COURSE	PAN Firewall	**ASSIGNMENT NO**	4
MODULE	Firewall	**ASSIGNMENT DATE**	28-Sep-24
STUDENT NAME	Konganti Chaithanya Kumar	**SUBMIT DATE**	29-Sep-24

1. Configure a security Policy to access Internet from internal network, share and explain screenshots of logs, steps to configure the policy.

Step-by-Step:

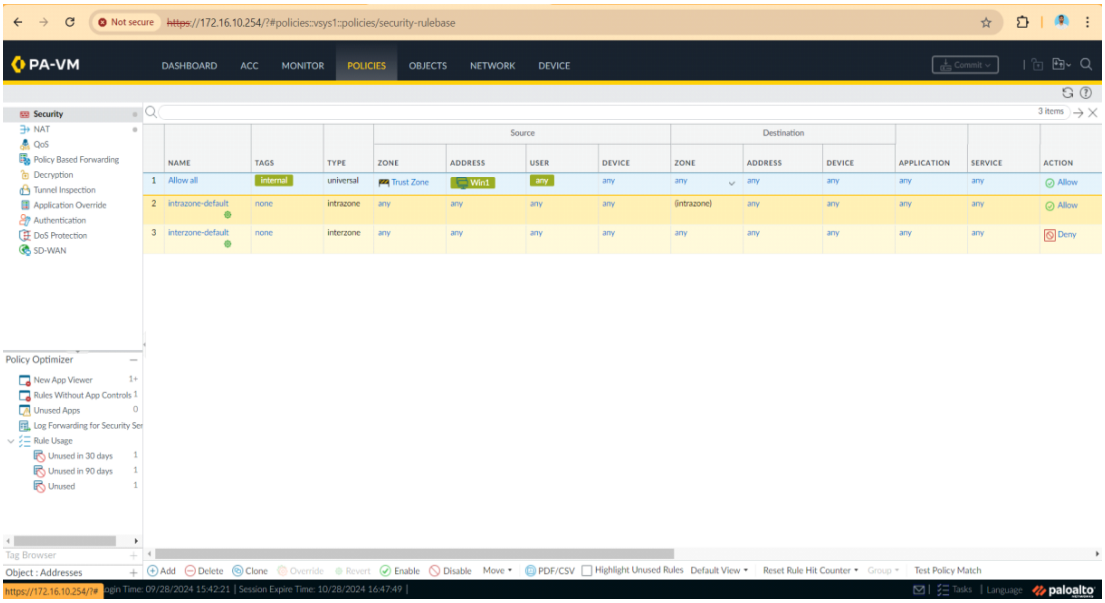
1. Log in to the Palo Alto Firewall:

- Open the web browser and navigate to the firewall's management IP.
- Log in using your **admin** credentials.



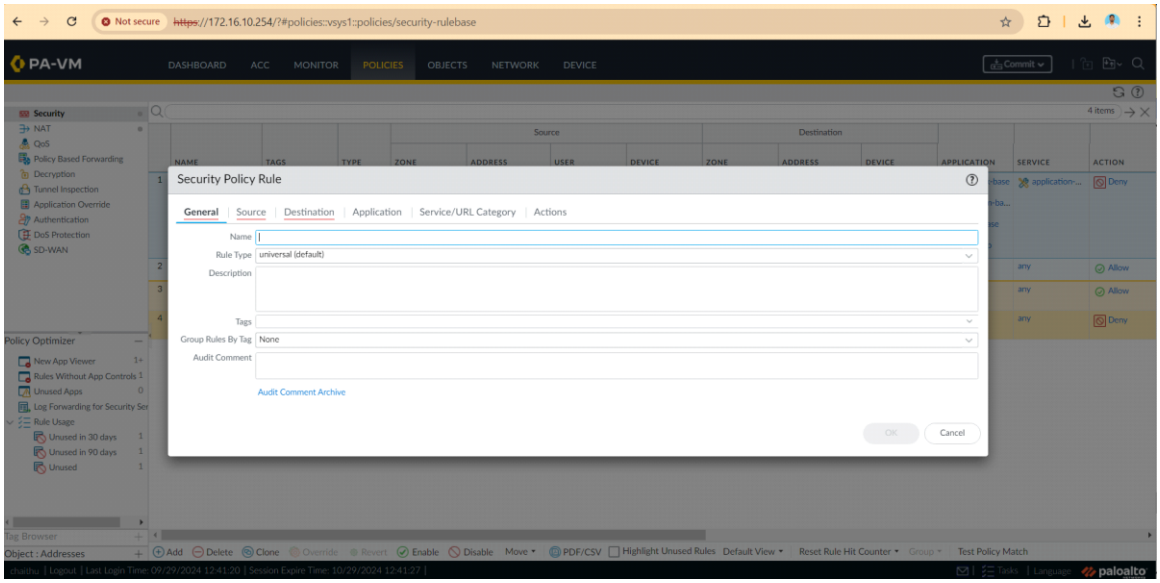
2. Navigate to the Security Policy:

- From the web interface, go to the **Policies** tab on the left sidebar.
- Click on **Security** under the **Policies** section.



3. Create a New Security Policy:

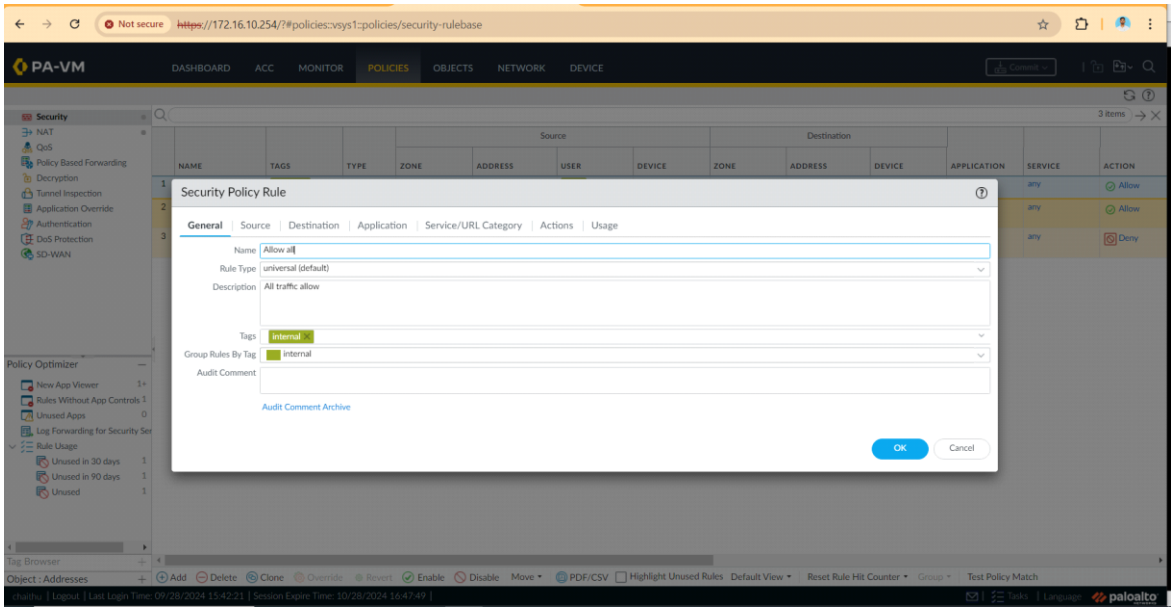
- Click the **Add** button at the bottom of the **Security Policies** list.
- This will open the security policy editor where you can define the rules for accessing the internet from the internal network.



4. Configure the Policy:

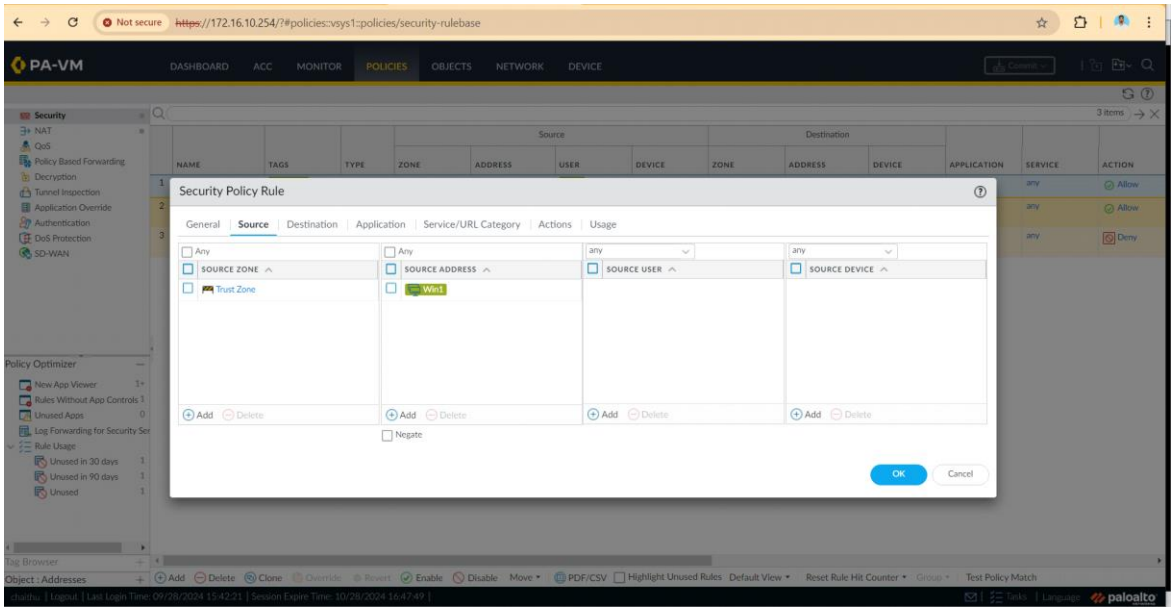
Name the Policy:

- In the **General** tab, provide a descriptive name for the policy such as Allow-Internet.
- Add a description for clarity like **"Allow all**".



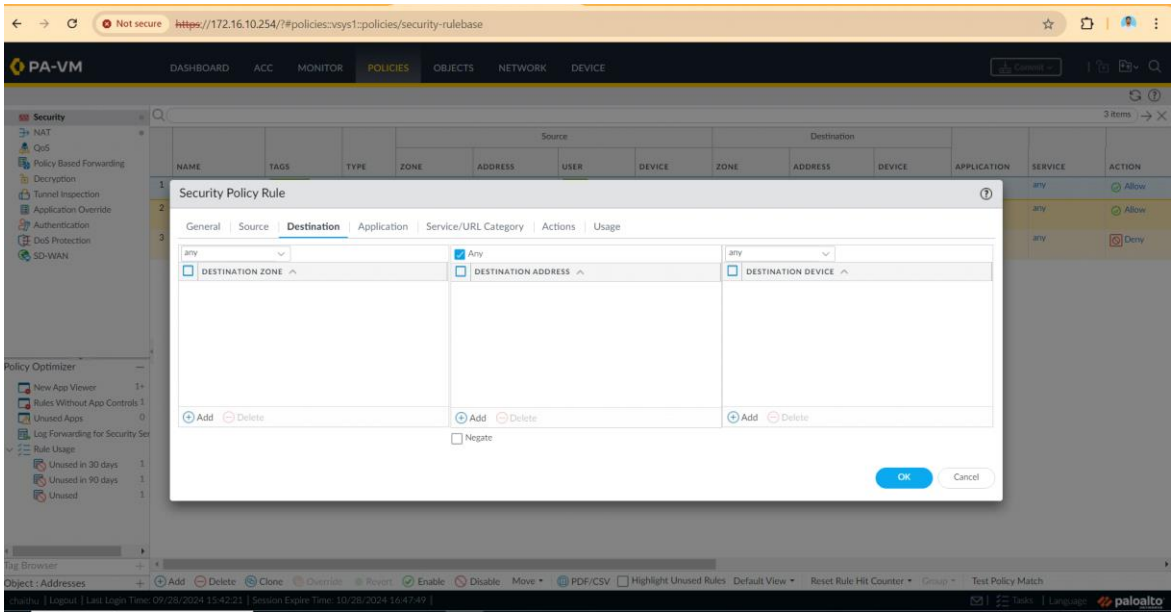
Source Configuration:

- **Source Zone:** Select the internal network zone **Trust**.
- **Source Address:** Specify the internal subnet (simply select **Any** if you want to allow all internal addresses).



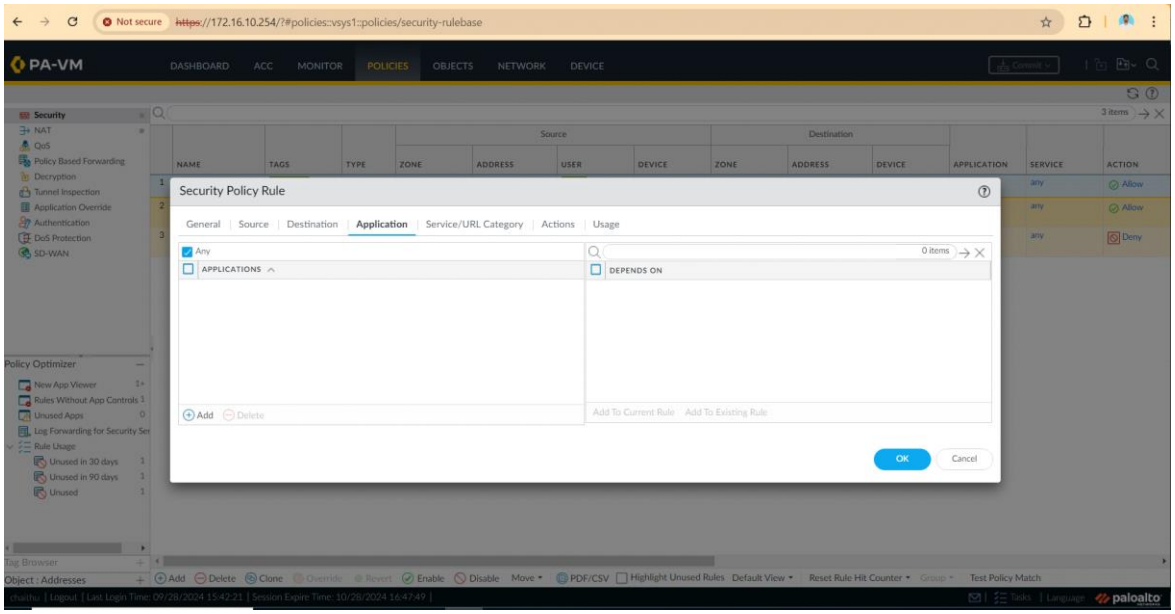
Destination Configuration:

- **Destination Zone:** Set the destination zone to **Untrust**, which represents the internet.
- **Destination Address:** You can use **Any** to allow access to any external IP on the internet.



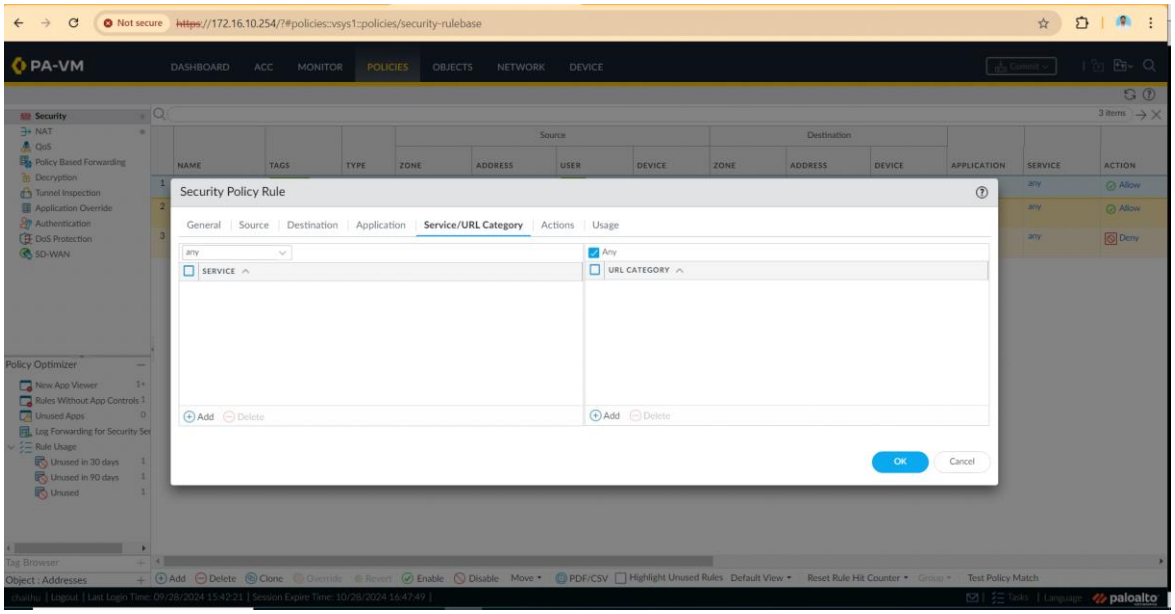
Application Tab:

- In the **Application** tab, select **Any**
- if you want to limit the policy to specific applications.



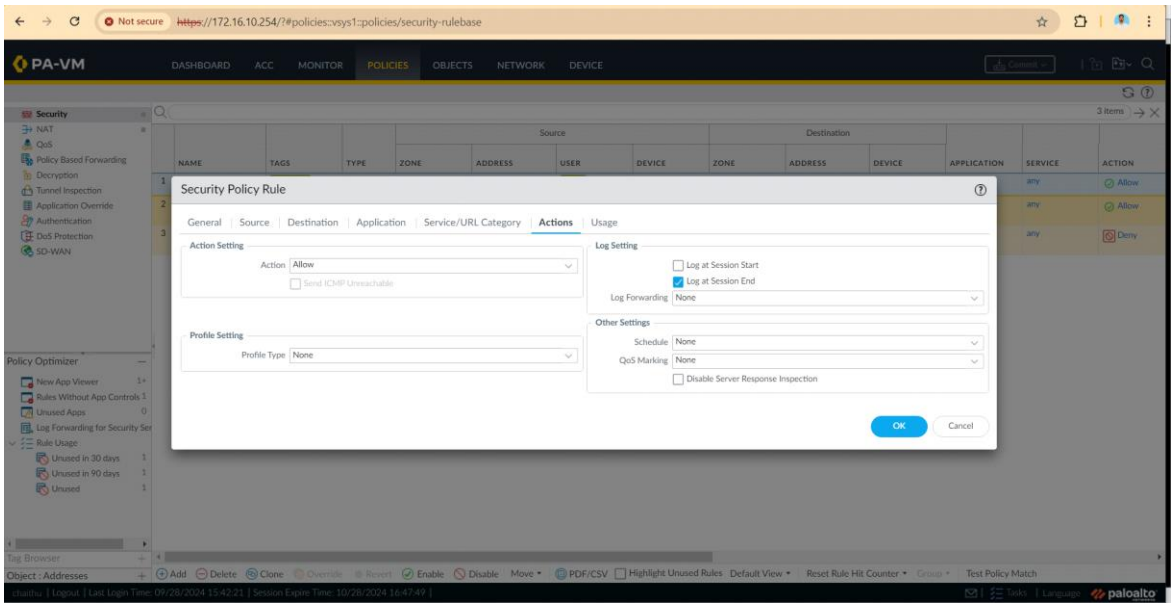
Service/URL Category:

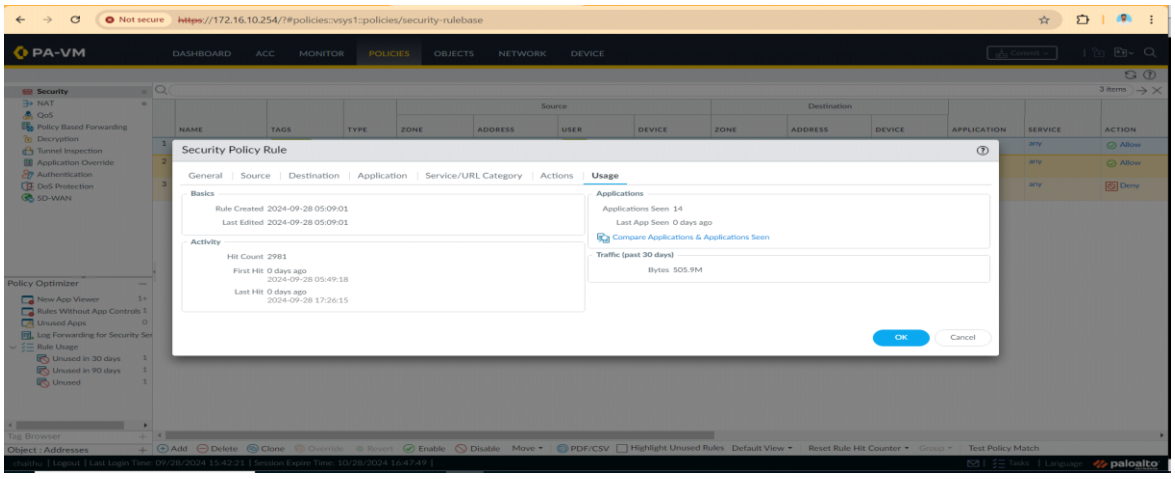
- In the **Service/URL Category** tab, set **Service** to **application-default** to allow internet traffic on the default ports (e.g., port 80 for HTTP, port 443 for HTTPS).

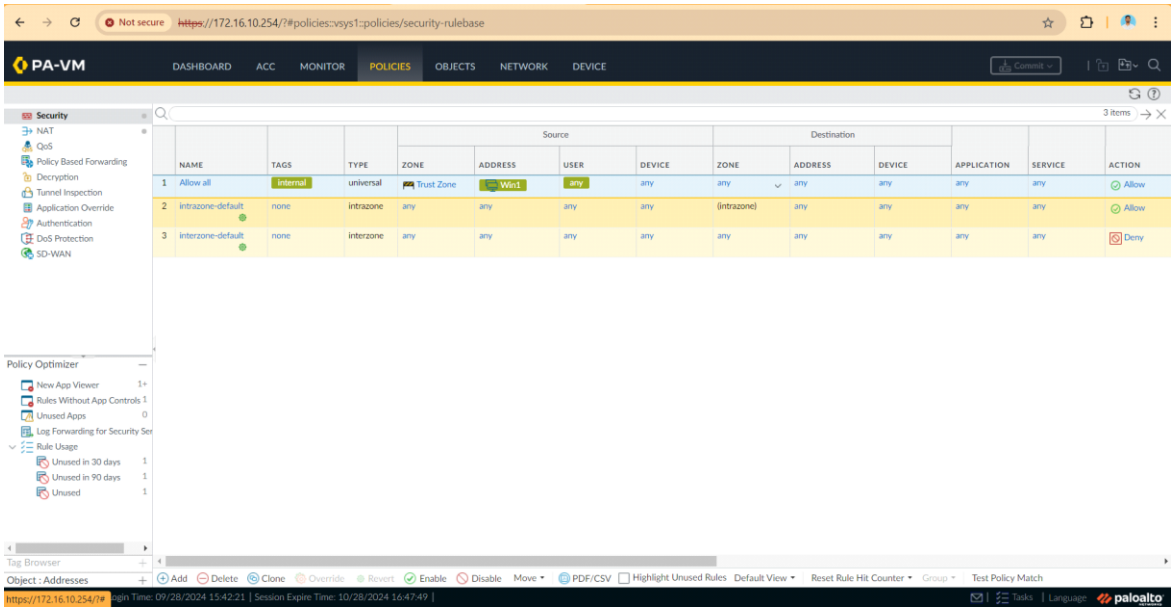


Action:

- In the **Action** tab, set the **Action** to **Allow**.

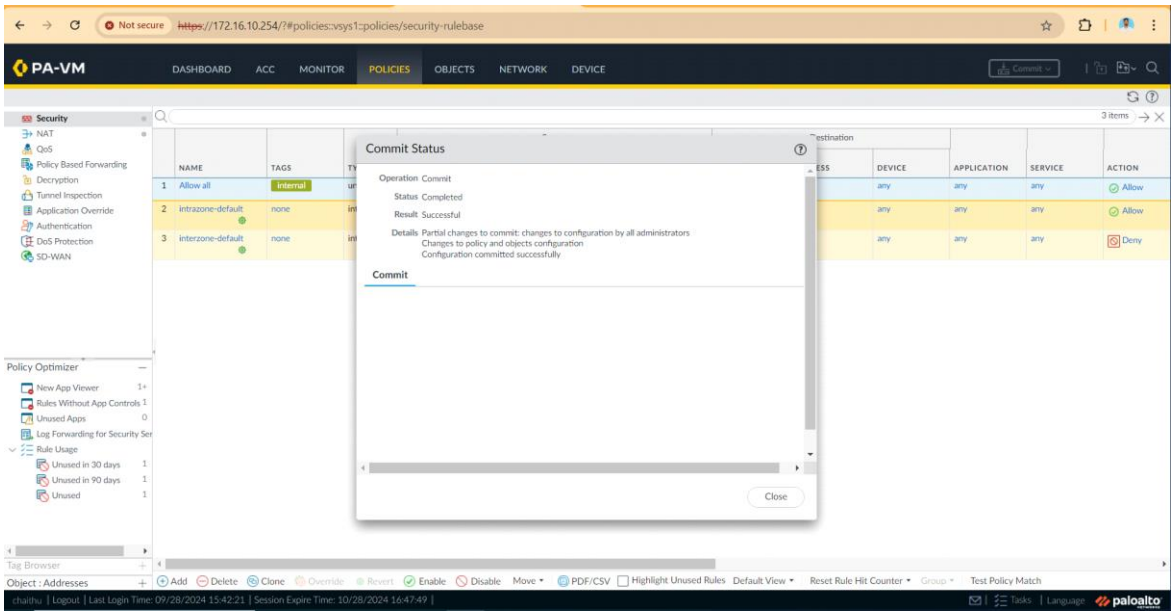






5. Commit the Policy:

- Once the policy configuration is complete, click **OK** to save the policy.
- In the top-right corner of the screen, click **Commit** to apply the new policy changes to the firewall.

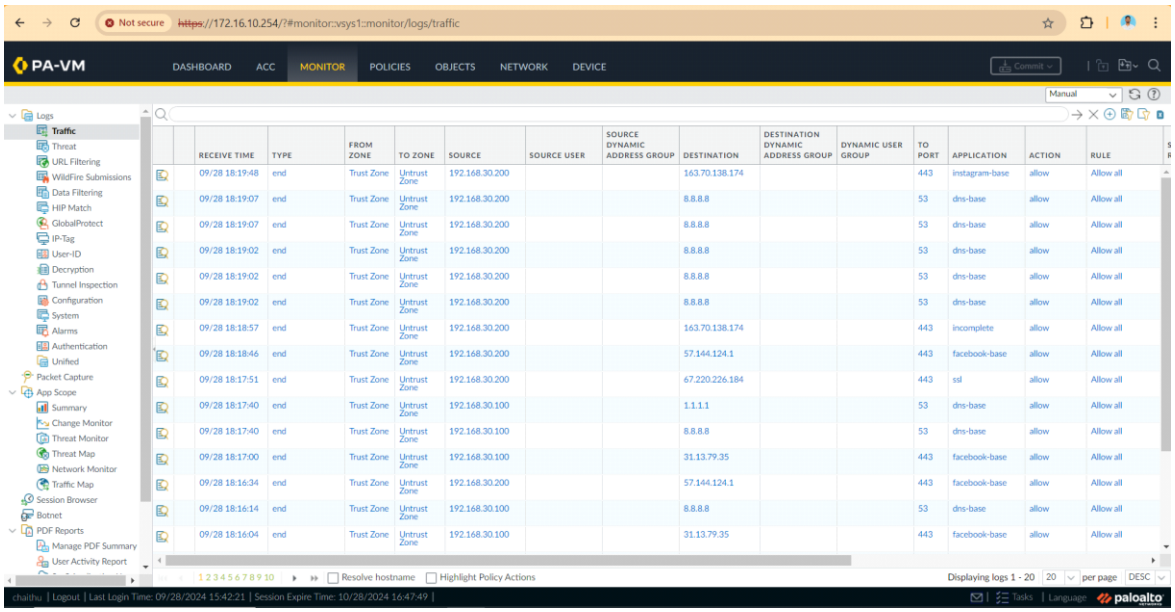


6. Verification and Logs:

Viewing Logs:

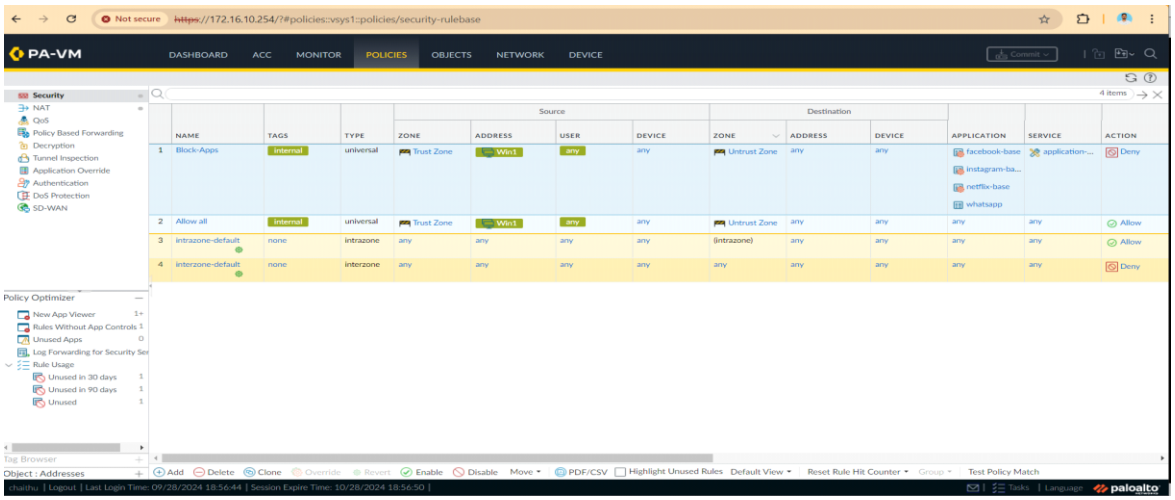
- After committing the policy, verify if traffic is allowed through the firewall.

- Navigate to **Monitor > Logs > Traffic** to view the logs.
- Filter the logs based on the security policy you just created (Allow-Internet) to see the allowed internet access from the internal network.



Screenshot of Logs:

- Take a screenshot showing:
  - The **Source IP** from the internal network.
  - The **Destination IP** (internet-based IP).
  - The **Action** column showing **Allow**.
  - The **Application** column showing **web-browsing** or any other relevant applications being allowed.



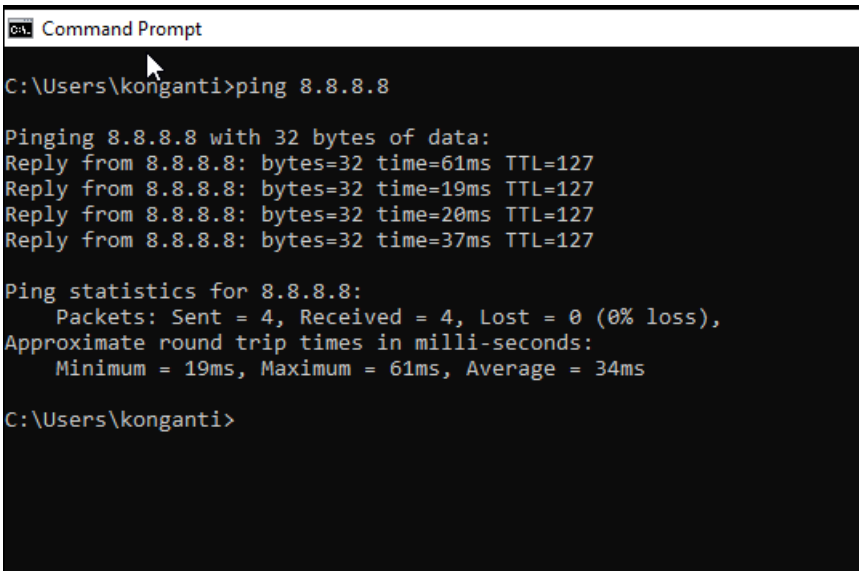
Ping and Web Access Test:

- From a machine in the internal network open a browser and try accessing an external website (www.google.com).
- Test **ping** to an external address to confirm outbound connectivity (if ICMP is allowed).

Command for Ping:

ping 8.8.8.8

- Check the traffic logs in the firewall again to ensure the traffic is being processed under the Allow-Internet rule.



Final Output:

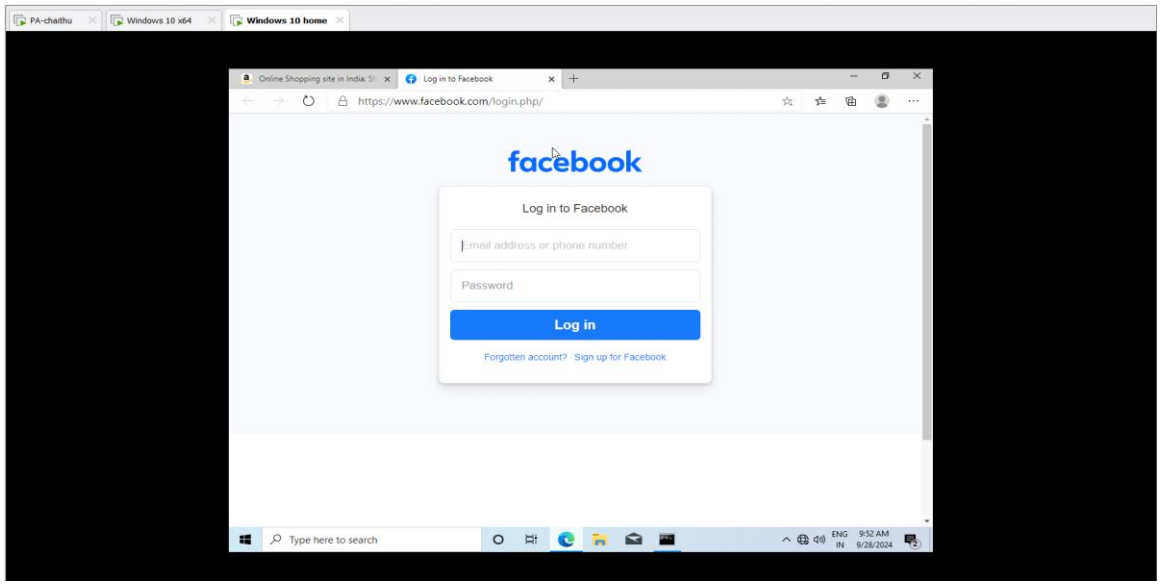
Steps to Check Internet Access with Webpages:

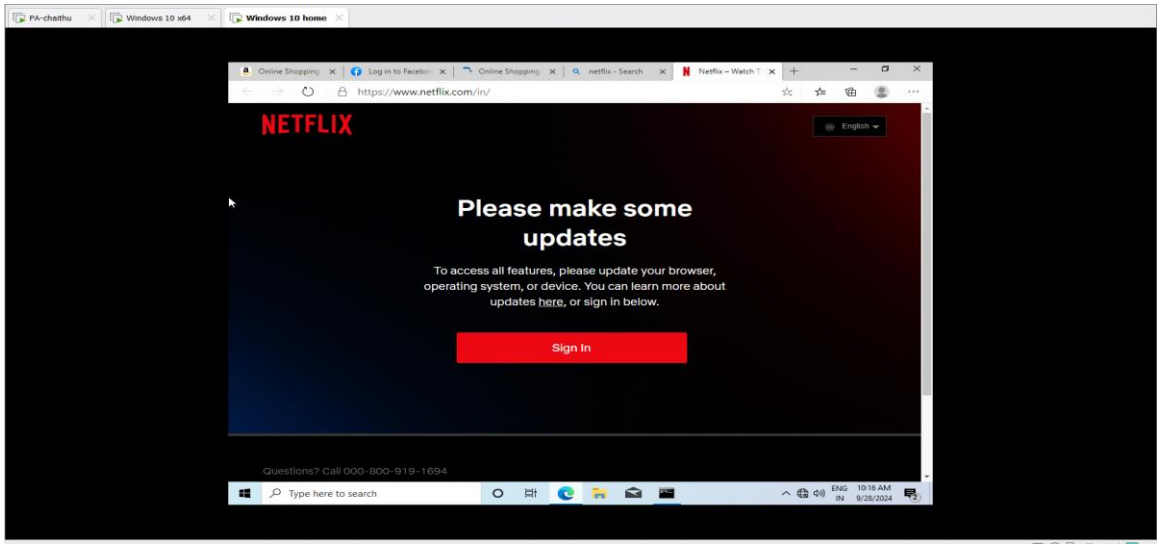
1. Webpage Access Test (Allow Internet Access):

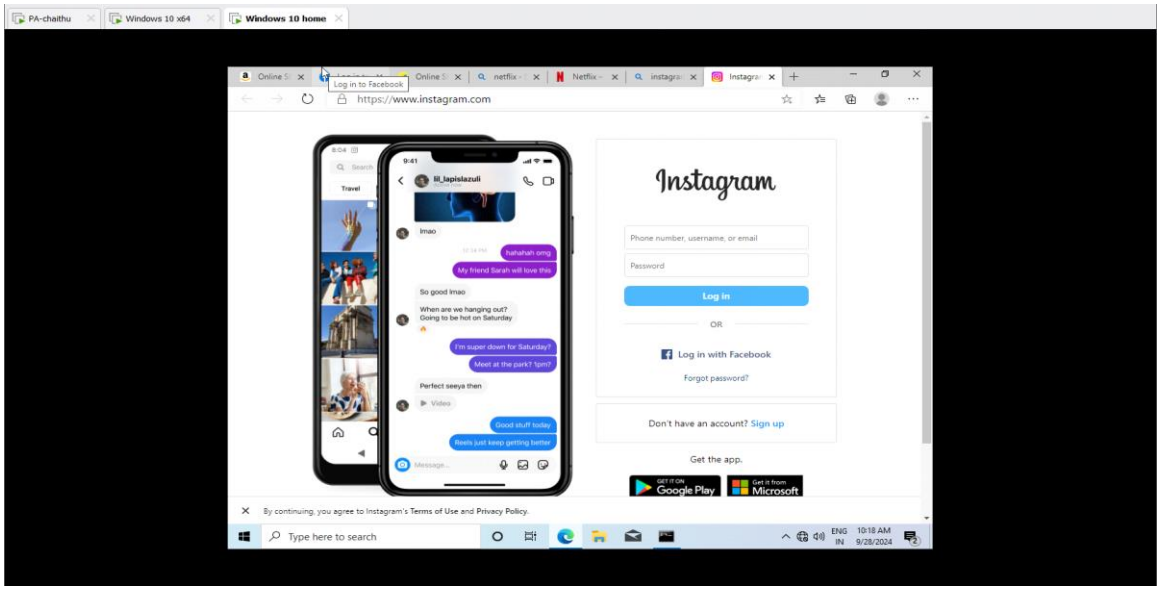
You can check whether the internet access policy is working by opening a browser on a machine in the internal network and accessing various websites.

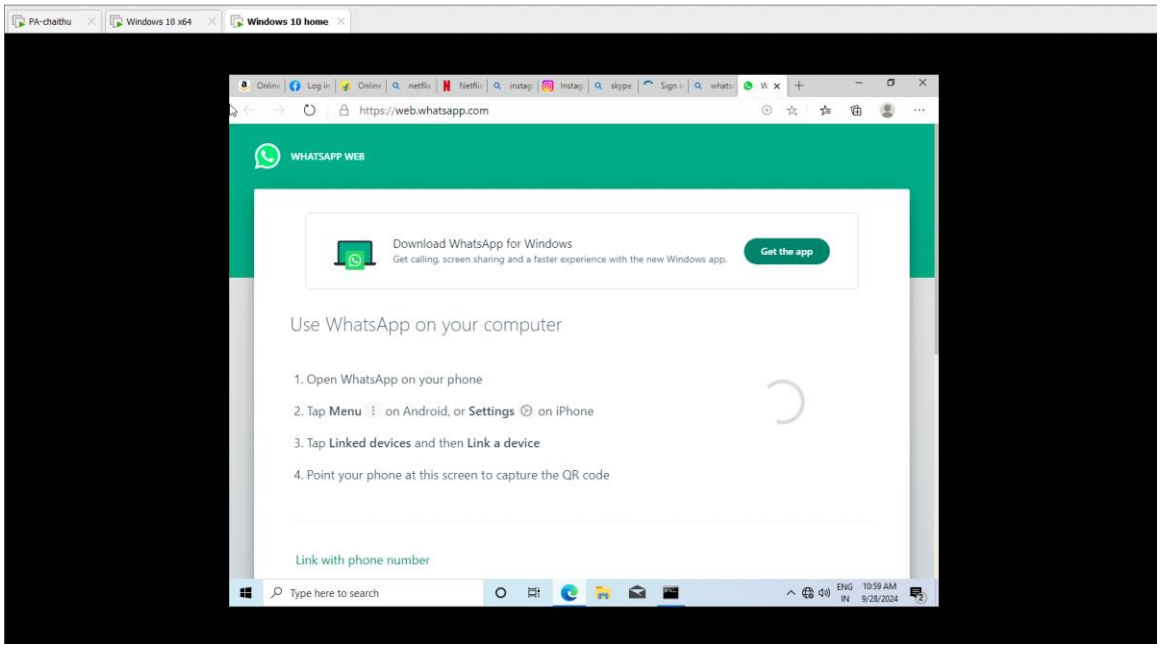
On a Windows or Ubuntu Host:

- Open a web browser (e.g., Google Chrome or Firefox).
- Try accessing an external website like:
- If the webpage loads, the internet access is working correctly, and your security policy is successfully allowing the traffic.
- You can also try opening another webpage like:


PA-chaithu
Windows 10 x64
Windows 10 home
Log in to Facebook
https://www.facebook.com/login.php/
facebook
Log in to Facebook
Email address or phone number
Password
Log in
Forgotten account? Sign up for Facebook
Type here to search


PA-chaithu
Windows 10 x64
Windows 10 home
https://www.netflix.com/in/
NETFLIX
English
Please make some updates
To access all features, please update your browser, operating system, or device. You can learn more about updates here, or sign in below.
Sign In
Questions? Call 000-800-919-1694
Type here to search

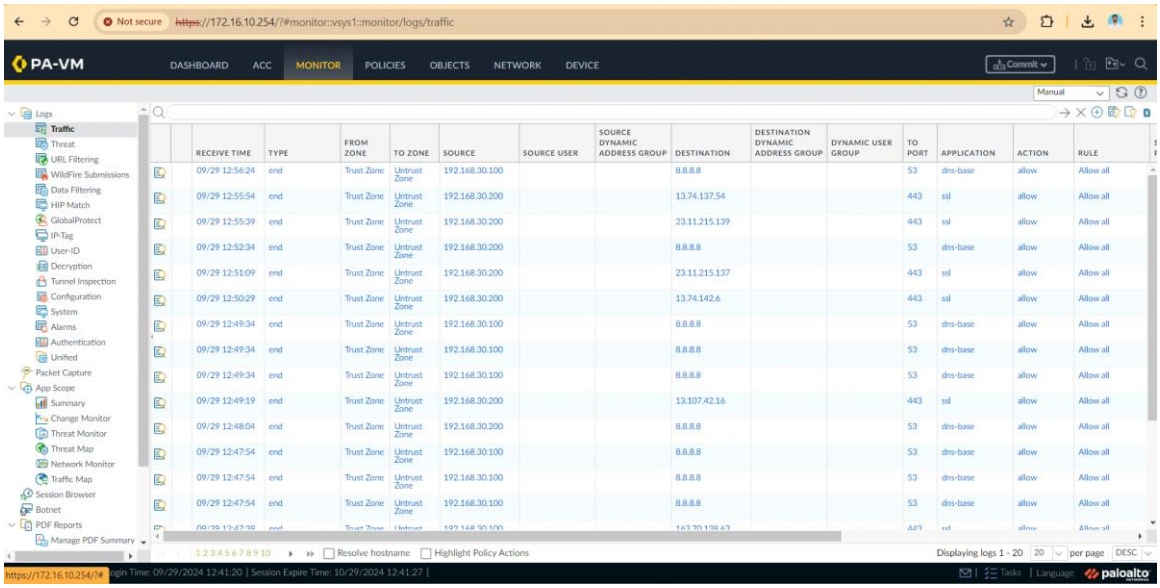

PA-chaithu
Windows 10 x64
Windows 10 home
Log in to Facebook
https://www.instagram.com
Instagram
Phone number, username, or email
Password
Log in
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app.
Google Play
Microsoft
By continuing, you agree to Instagram's Terms of Use and Privacy Policy.
Type here to search



Verifying Traffic on Palo Alto Firewall:

- Navigate to **Monitor > Logs > Traffic** in the firewall web interface.
- Apply a filter to see traffic logs related to your security policy.

To configure a **security policy** in Palo Alto Networks (PAN) firewall and block at least four applications, follow these steps:



Conclusion:

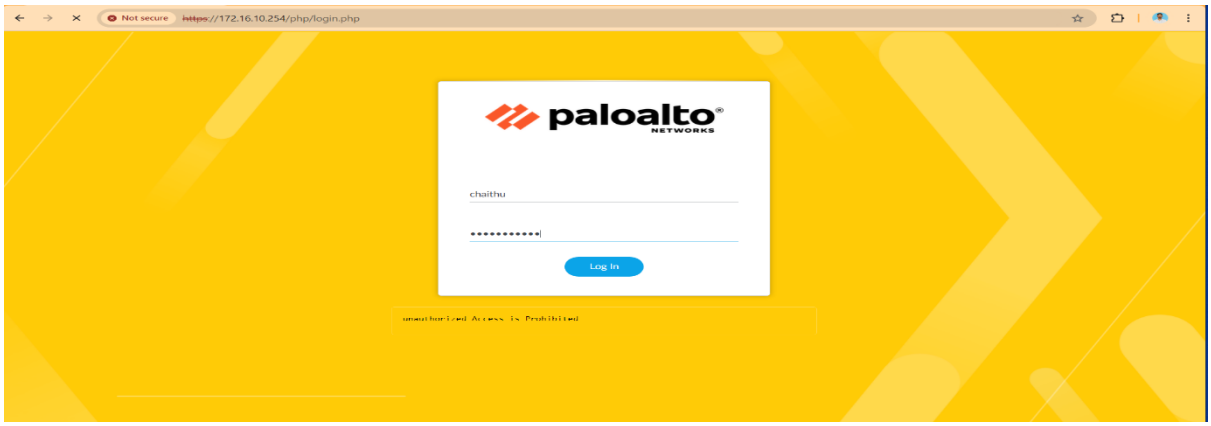
The security policy was successfully created to allow internet access from the internal network. Traffic logs confirm the policy is working, ensuring secure internet access with effective traffic monitoring.

2. Block at least 4 applications and explain logs and steps to configure the policy with the help of a screenshot?

Step-by-Step Process:

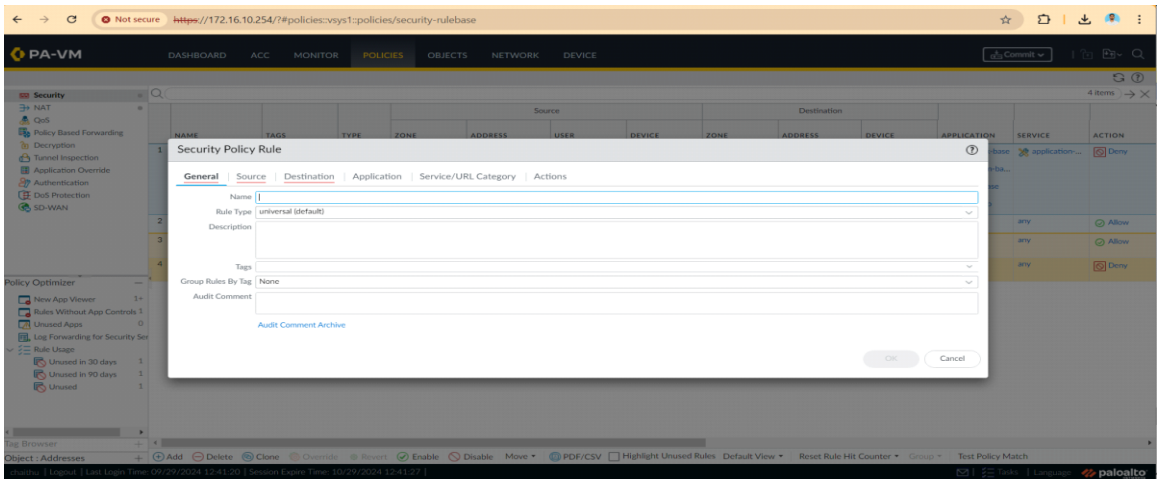
1. Login to Palo Alto Networks Firewall

- Open your web browser and access the firewall GUI by entering its IP address.
- Log in using your credentials (admin account or custom role-based account).



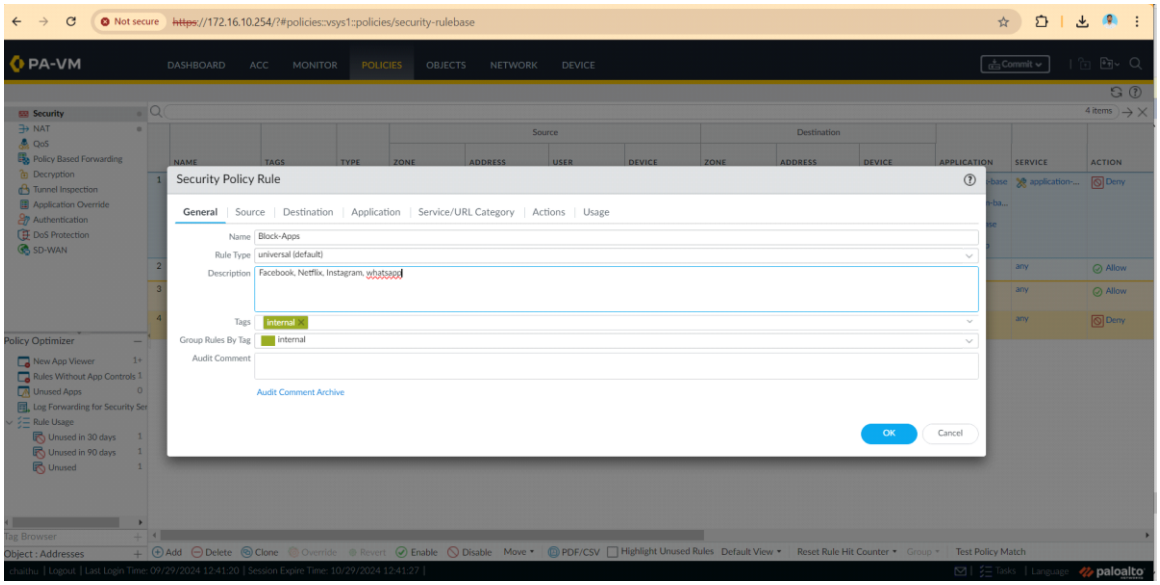
2. Navigate to the Security Policies

- Go to the **Policies** tab.
- Click on **Security** under the Policies section.



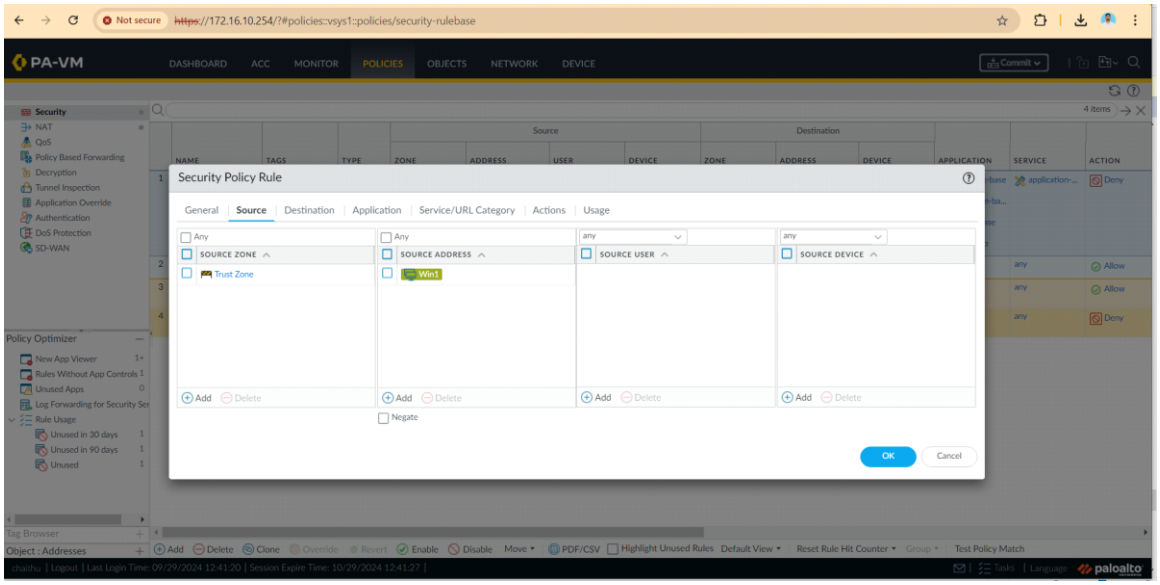
3. Create a New Security Policy

- Click on **Add** to create a new security policy.
- Give your policy a **Name**: Block App



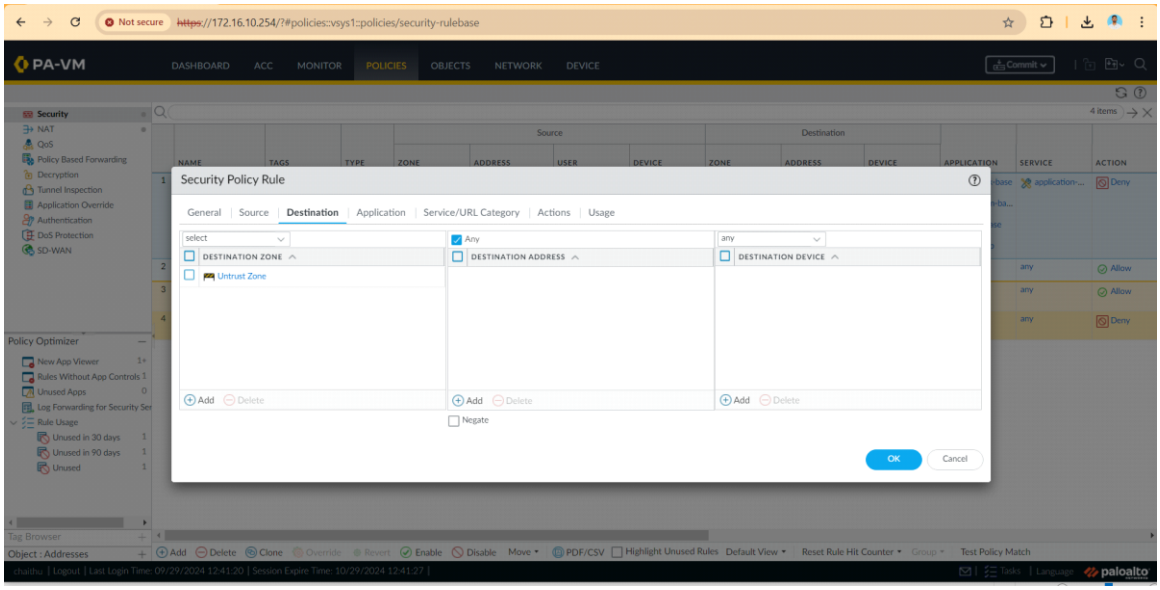
Source Zone:

- Define the source zone (**Trust** zone).
- Select internal devices or users as the source.



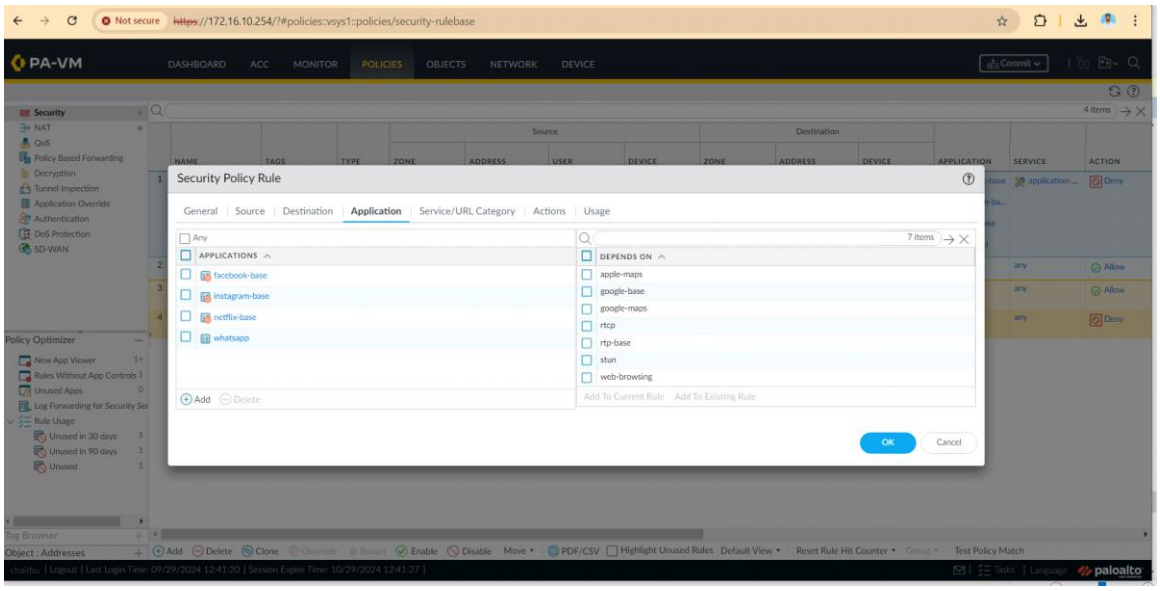
Destination Zone:

- Define the destination zone as **Untrust** (external network).



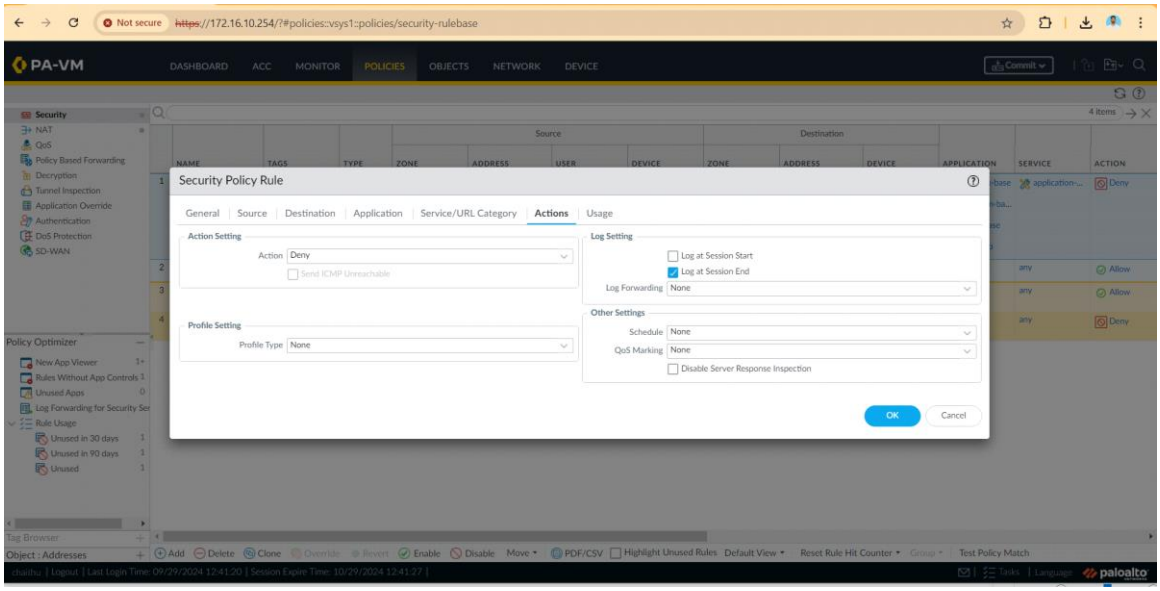
4. Define Applications to Block

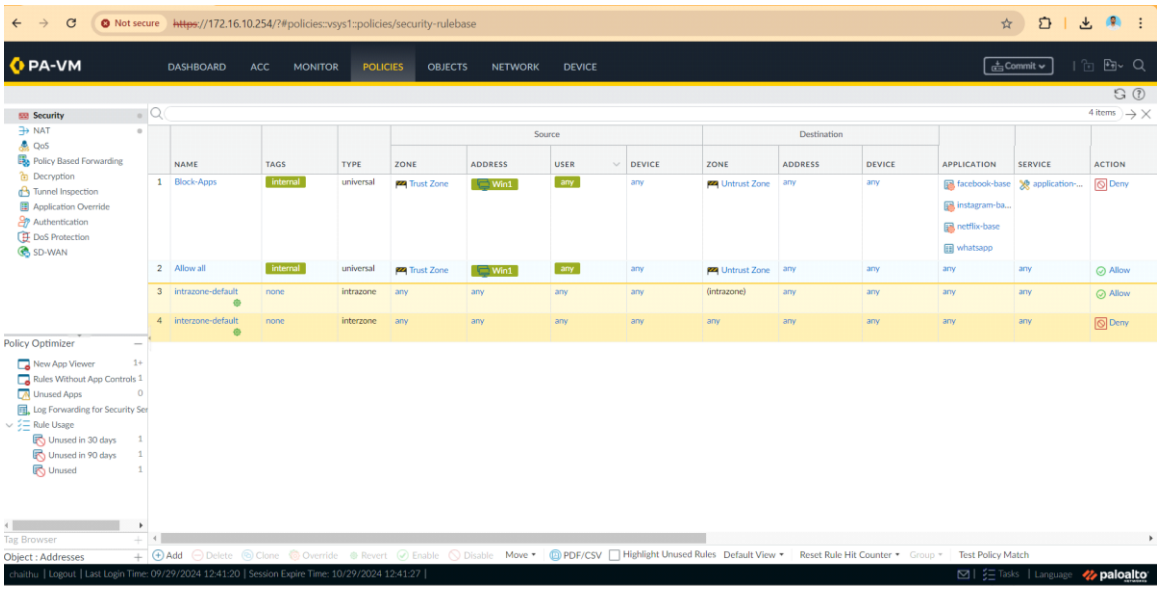
- Go to the **Application** tab.
- Click **Add** and search for the applications you want to block. For this example, block the following four applications:
  - **Facebook**
  - **Instagram**
  - **Netflix**
  - **WhatsApp**
- Select each application and add it to the blocked list.



5. Action Configuration

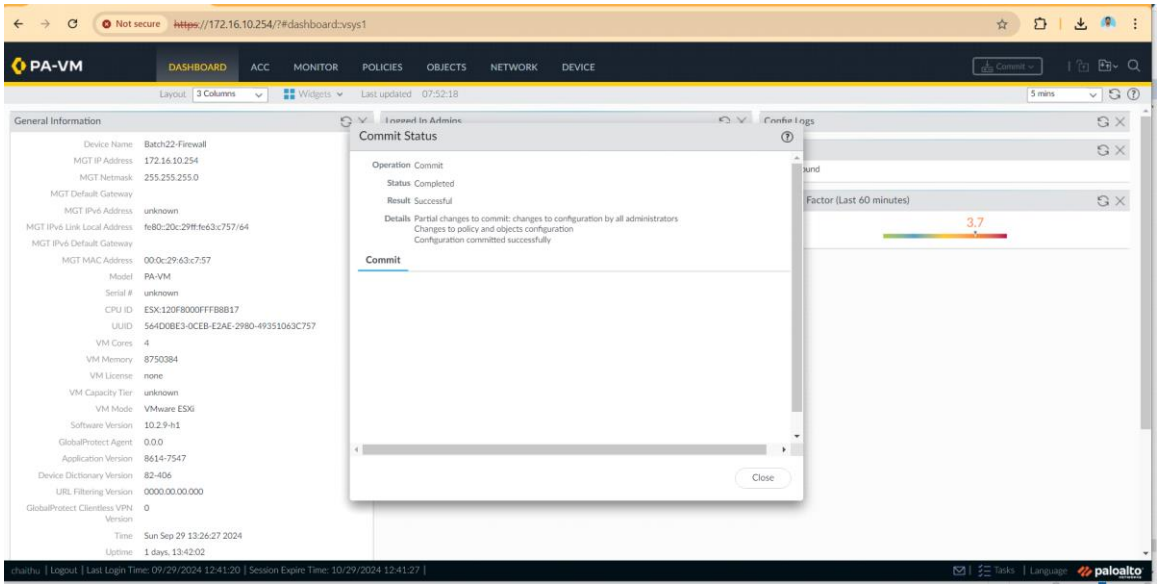
- Under the **Actions** tab, set the **Action** to **Deny** to block traffic for these applications.
- You can also configure **Logging** to capture traffic related to these applications in the logs.





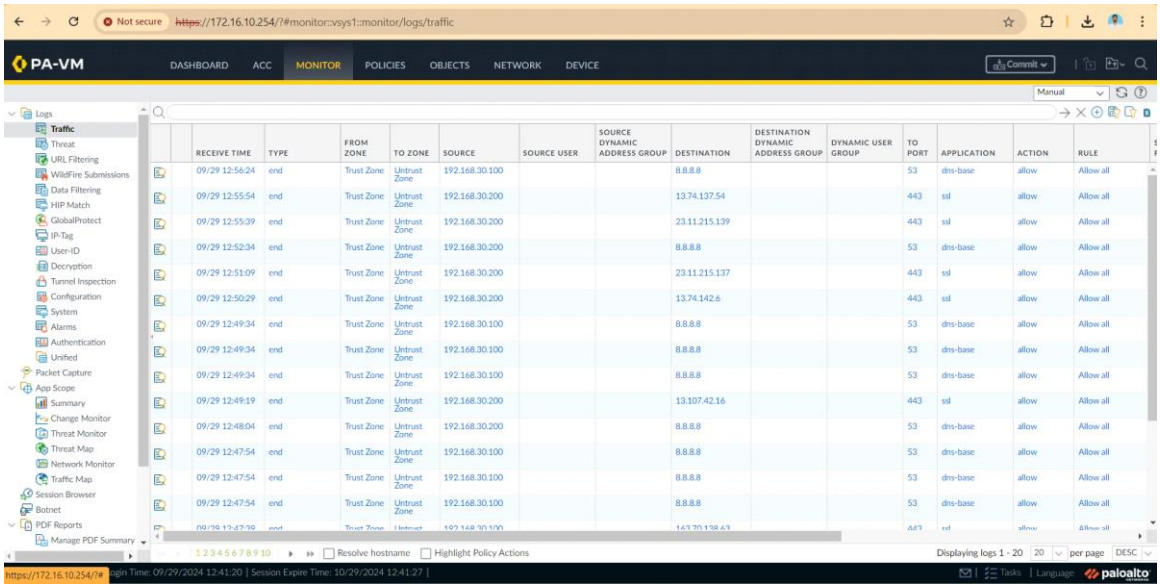
6. Commit the Changes

- After configuring the security policy, click **OK**.
- Click **Commit** at the top-right corner of the screen to apply the policy.



7. Check Logs for Blocked Applications

- Navigate to the **Monitor** tab and select **Logs > Traffic**.
- Filter the logs by application name (e.g., Facebook, Instagram) to verify that the applications are being blocked.
- The logs should show that traffic from these applications is denied by your policy.



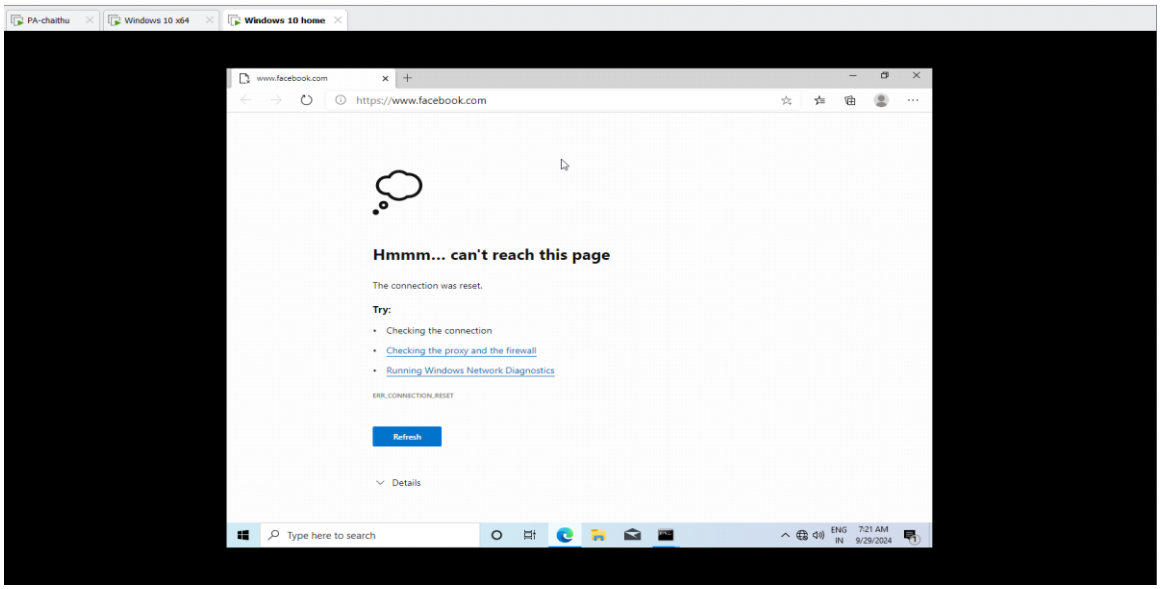
Final Output:

Screenshot Documentation:

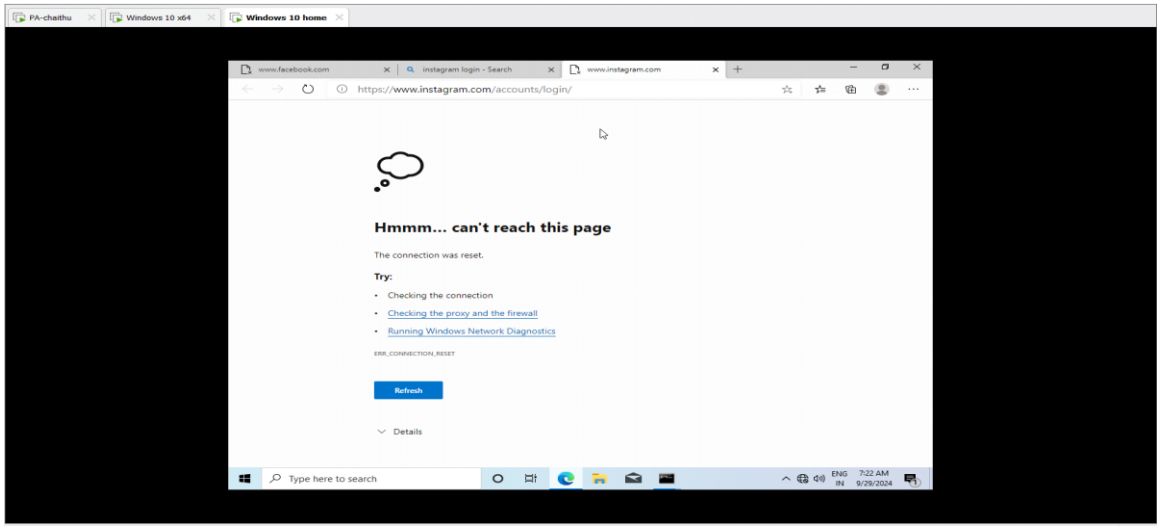
- **Login Page**: Capture a screenshot of the login page showing access to the PAN firewall.

- **Security Policy Creation**: Capture a screenshot of the new security policy settings, especially under the Application tab where you select the applications to block.
- **Application Block**: Show a screenshot of the applications being added to the block list.
- **Action Deny**: Screenshot the action being set to "Deny."
- **Logs**: Provide screenshots of the traffic logs showing the denied traffic for each blocked application.

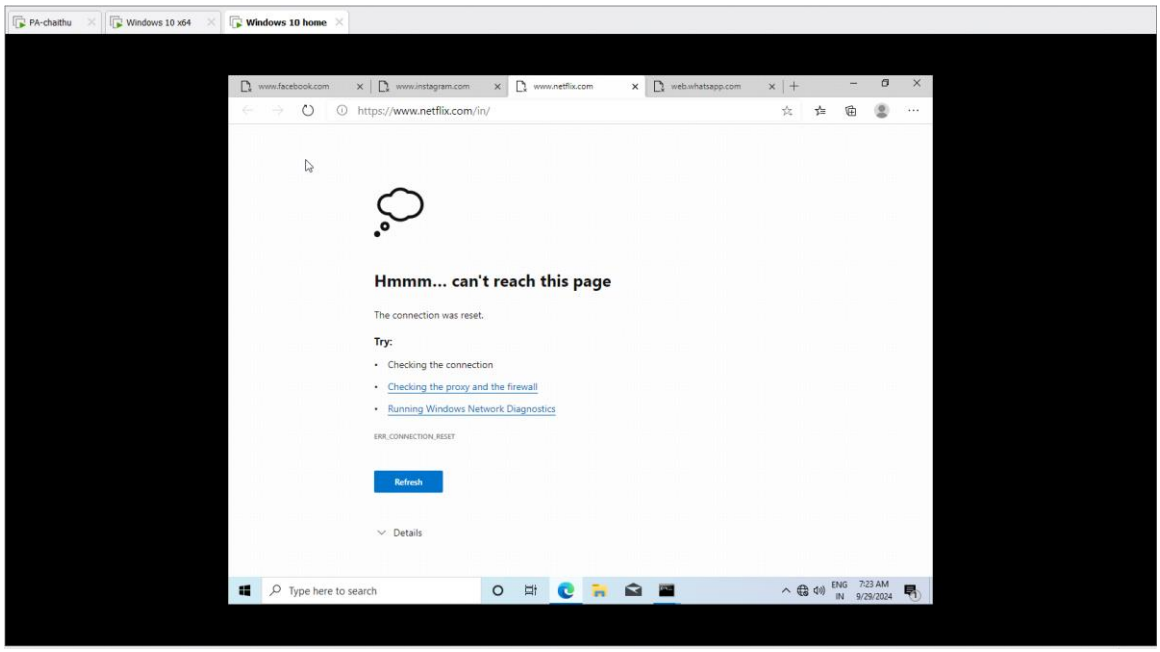
Facebook:



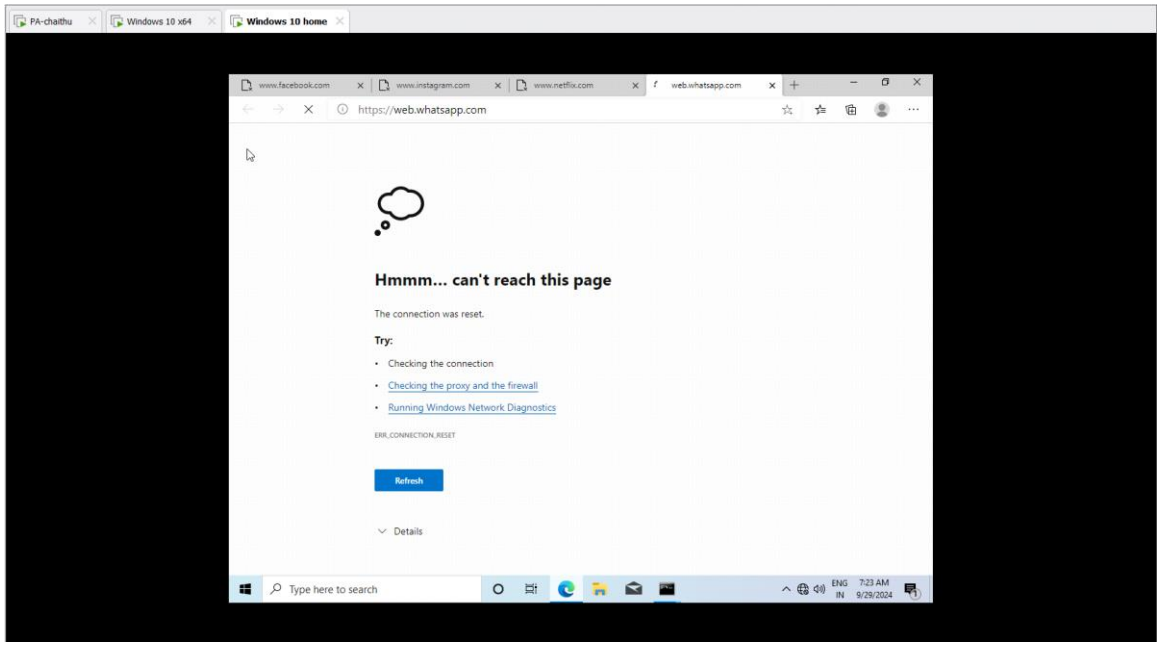
Instagram:



Netflix:



WhatsApp:



Conclusion:

The policy was successfully configured to block Facebook, Instagram, Netflix, and WhatsApp. Firewall logs confirm that the applications are being blocked, ensuring effective control and monitoring.

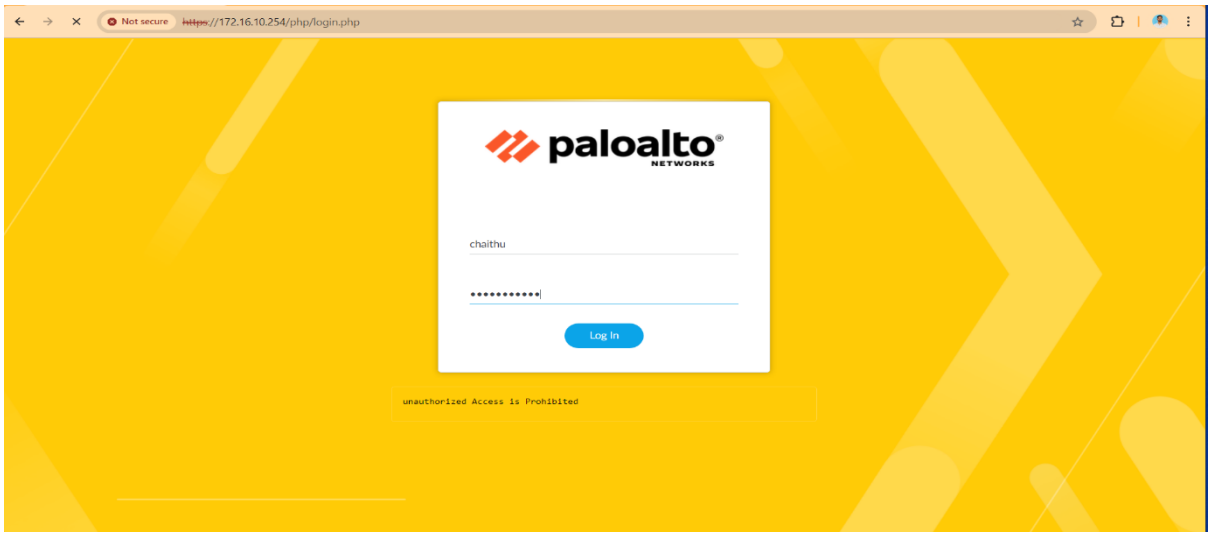
3.Configuring Zones, Interfaces, Virtual Router, and Source NAT?

A. Configure Security Zones:

- Security zones logically segment your network to apply security policies to different types of traffic.

1.Login to PAN Firewall:

- Open your browser and navigate to the PAN firewall management IP.
- Enter the admin credentials and log in to the web interface.

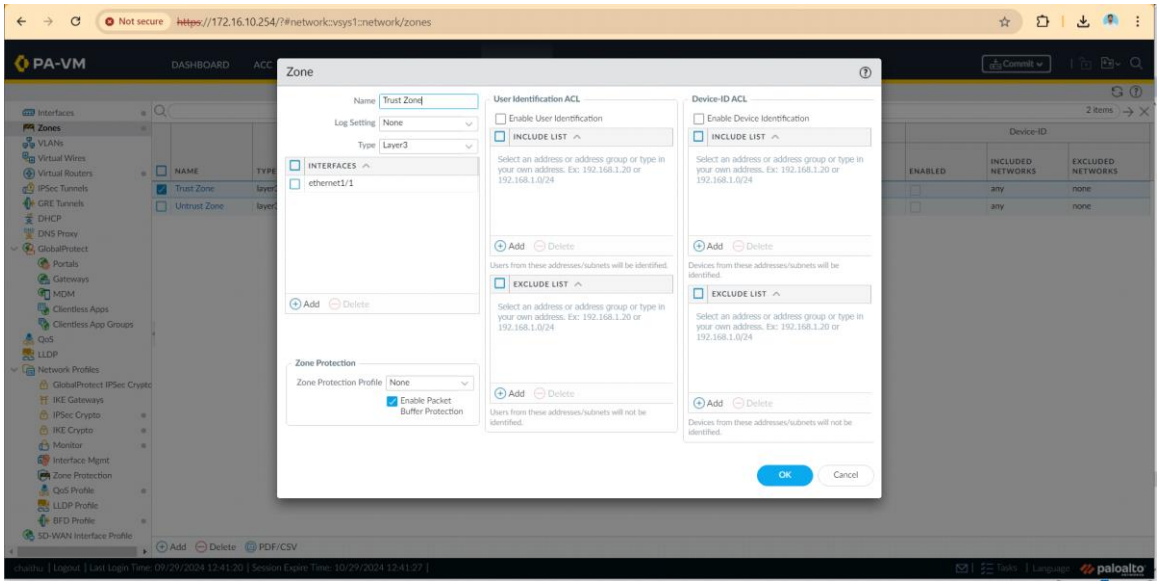


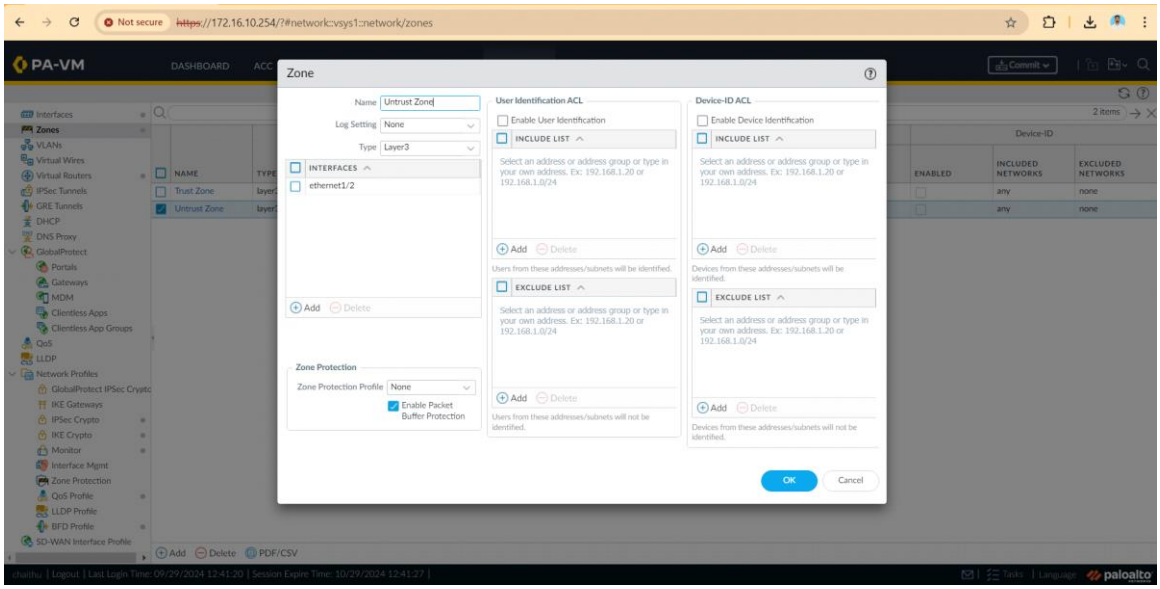
2.Navigate to the Zones Configuration:

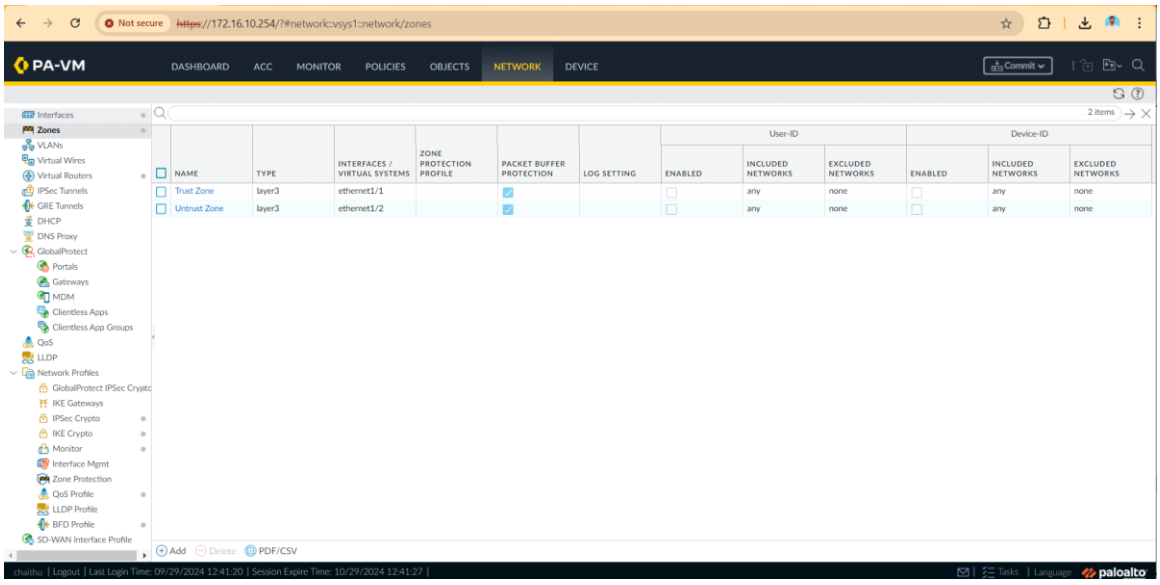
- In the top menu, click on **Network.**
- From the left-hand panel, select **Zones**.

Create New Zones:

- Click the **Add** button to create a new zone.
- **Name:** Enter a descriptive name for your zone.
- **Type:** Select **Layer 3** (since we will configure **Layer 3** routing).
- Leave the Interfaces section blank for now, as we'll assign them later.
- Click **OK**.
- Repeat the process for each additional zone


Not secure https://172.16.10.254/?#network::vsys1::network/zones
PA-VM
DASHBOARD
Zone
Name Trust Zone
Log Setting None
Type Layer3
INTERFACES
ethernet1/1
User Identification ACL
Enable User Identification
INCLUDE LIST
EXCLUDE LIST
Device-ID ACL
Enable Device Identification
Zone Protection
Zone Protection Profile None
Enable Packet Buffer Protection
OK
Cancel


Not secure https://172.16.10.254/?#network::vsys1::network/zones
PA-VM
DASHBOARD
Zone
Name Untrust Zone
Log Setting None
Type Layer3
INTERFACES
ethernet1/2
User Identification ACL
Enable User Identification
INCLUDE LIST
EXCLUDE LIST
Device-ID ACL
Enable Device Identification
Zone Protection
Zone Protection Profile None
Enable Packet Buffer Protection
OK
Cancel


Not secure https://172.16.10.254/?#network::vsys1::network/zones
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
NAME
TYPE
INTERFACES / VIRTUAL SYSTEMS
ZONE PROTECTION PROFILE
PACKET BUFFER PROTECTION
LOG SETTING
User-ID
Device-ID
ENABLED
INCLUDED NETWORKS
EXCLUDED NETWORKS
Trust Zone layer3 ethernet1/1 any none any none
Untrust Zone layer3 ethernet1/2 any none any none
Add
Delete
PDF/CSV

B. Configure Network Interfaces

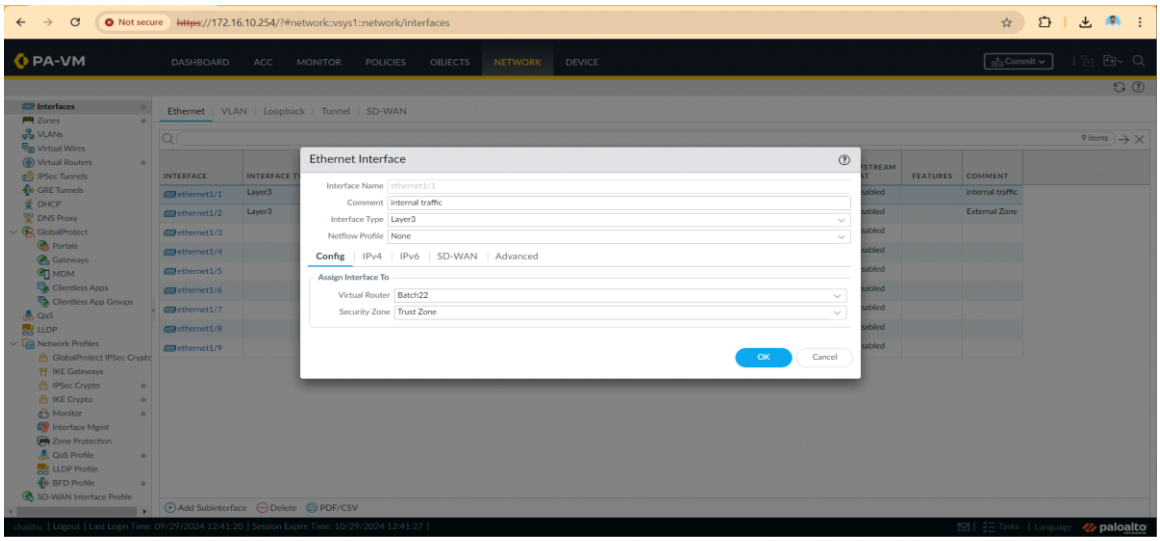
Assign the firewall's physical interfaces to the zones you created.

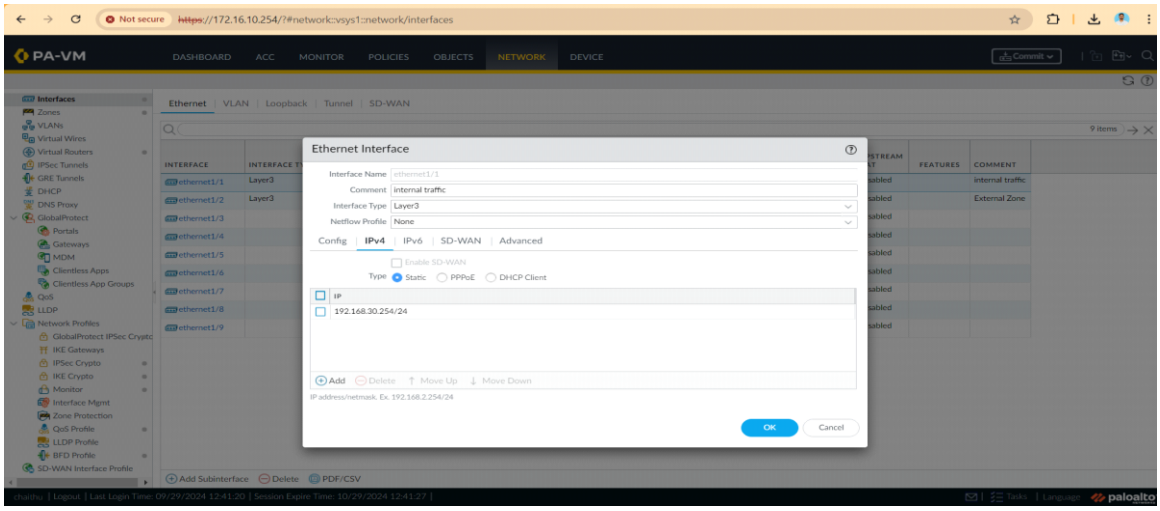
1.Navigate to the Interfaces:

- Go to Network > **Interfaces**.
- You'll see a list of available interfaces (**ethernet1/1, ethernet1/2**).

2.Configure External (WAN) Interface:

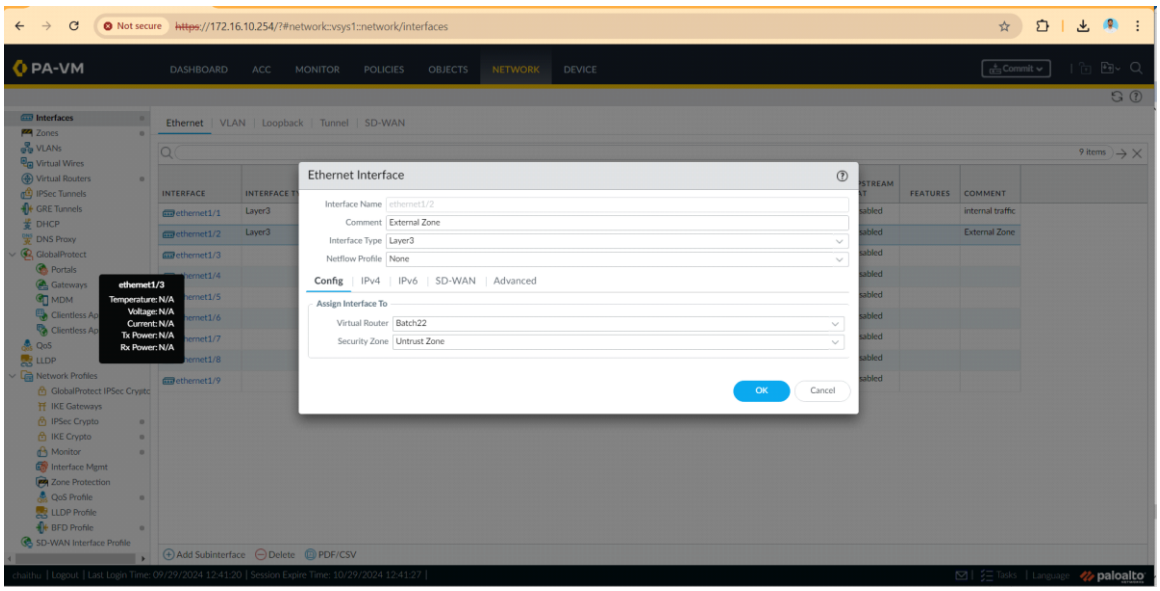
- Click on the interface you'll use for WAN (**ethernet1/1**).
- Set Interface Type to **Layer 3**.
- **Virtual Router:** Select the virtual router (we'll configure this next).
- **Security Zone:** Select the WAN zone that you created earlier.
- Under **IPv4 tab**, add the IP address for your WAN connection (static).
- Click **OK** to apply changes.

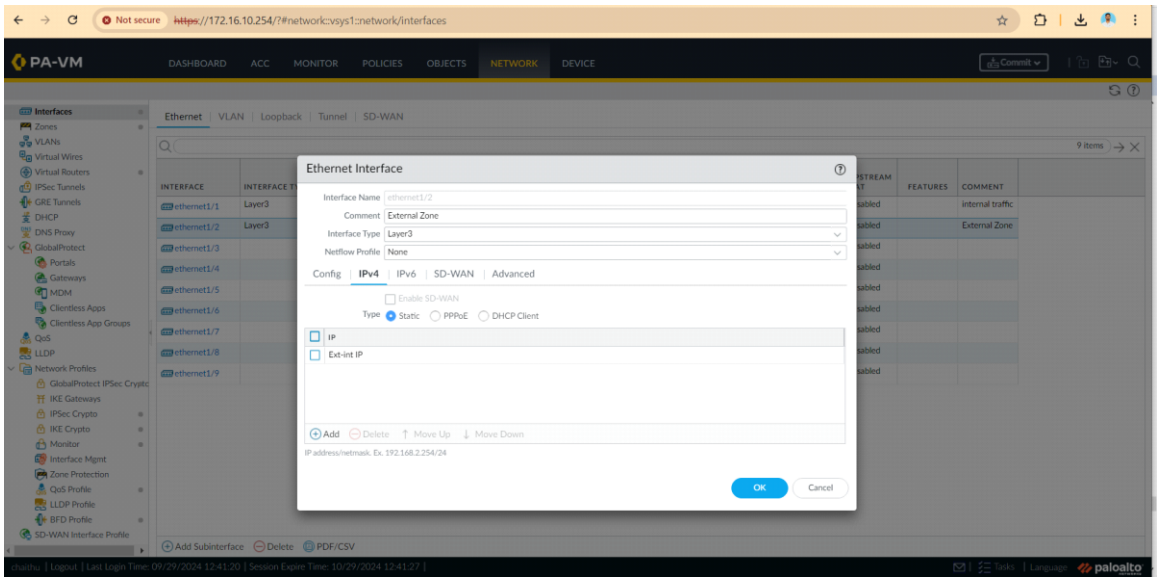


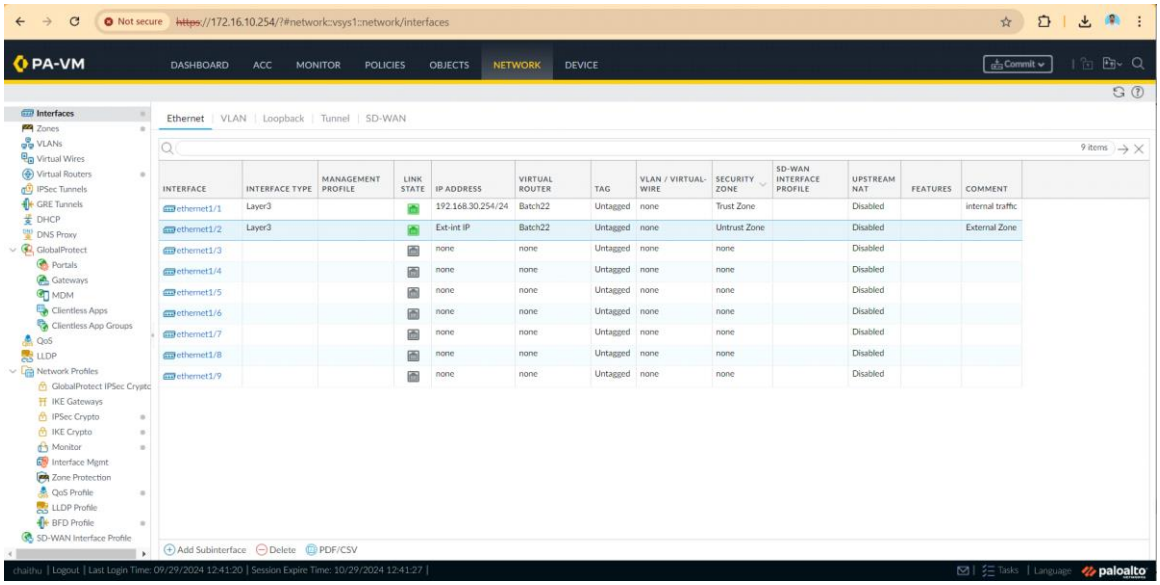


3.Configure Internal (LAN) Interface:

- Select another available interface (**ethernet1/2**).
- Set Interface Type to **Layer 3**.
- **Virtual Router:** Assign the same virtual router.
- **Security Zone:** Choose LAN.
- Under **IPv4 tab**, add the IP address range for your LAN.
- Click **OK**.







C. Configure the Virtual Router

A virtual router is responsible for routing traffic between zones.

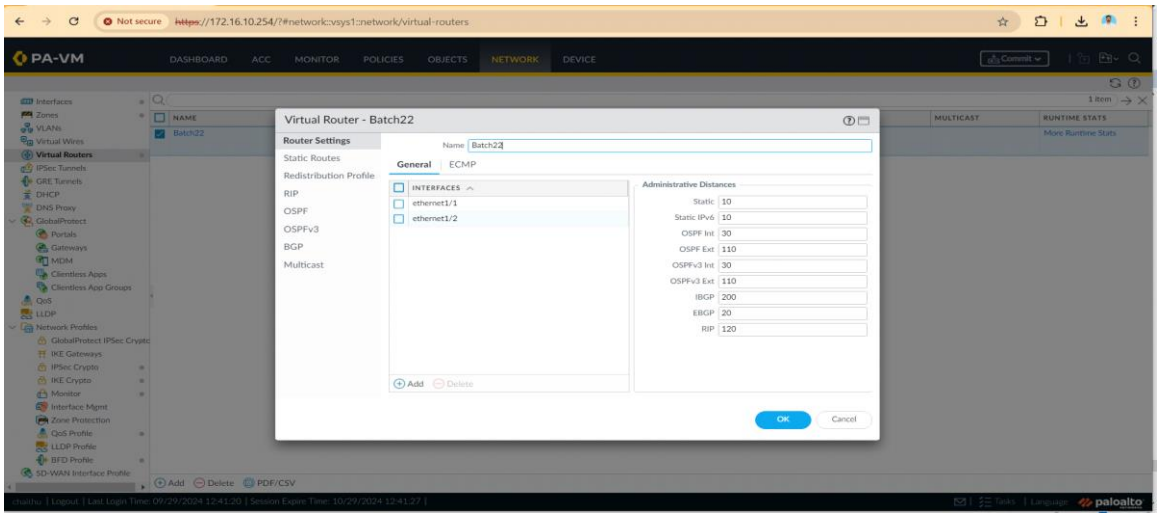
1.Navigate to the Virtual Router:

- Go to Network > **Virtual Routers**.
- Click **Add** to create a new virtual router.

2.Create a Virtual Router:

- Name: Enter a name (**Batch22**).
- Interfaces: Click **Add** to assign the WAN and LAN interfaces to this virtual router.
- Click **OK**.

Routing: (Optional)

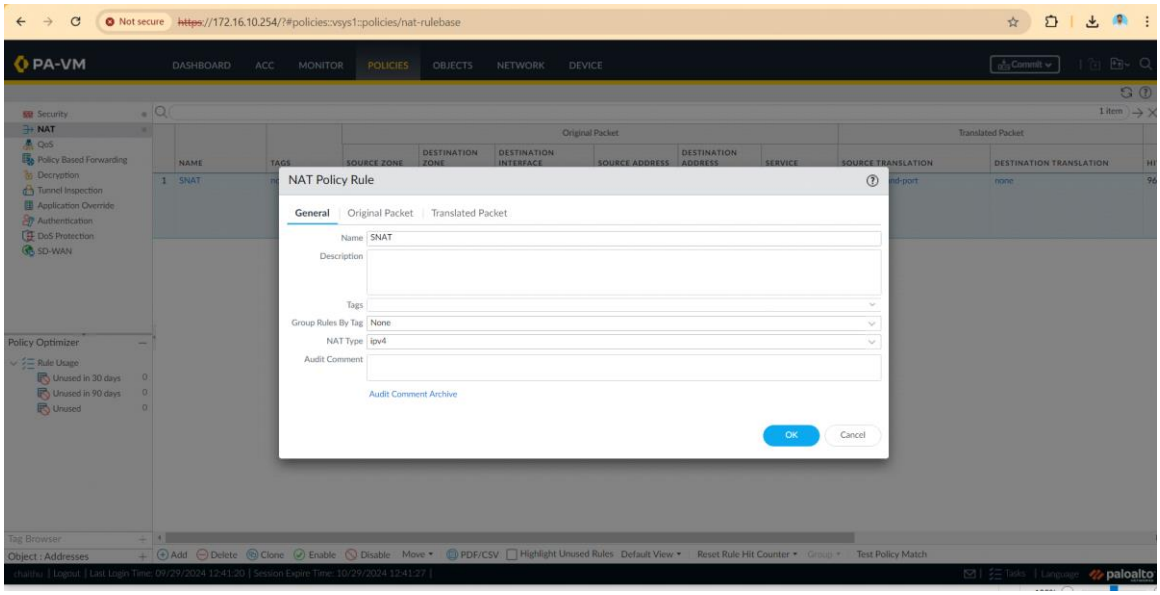


D. Configure Source NAT

Source NAT is essential for translating internal (private) IP addresses to a public IP when accessing the internet.

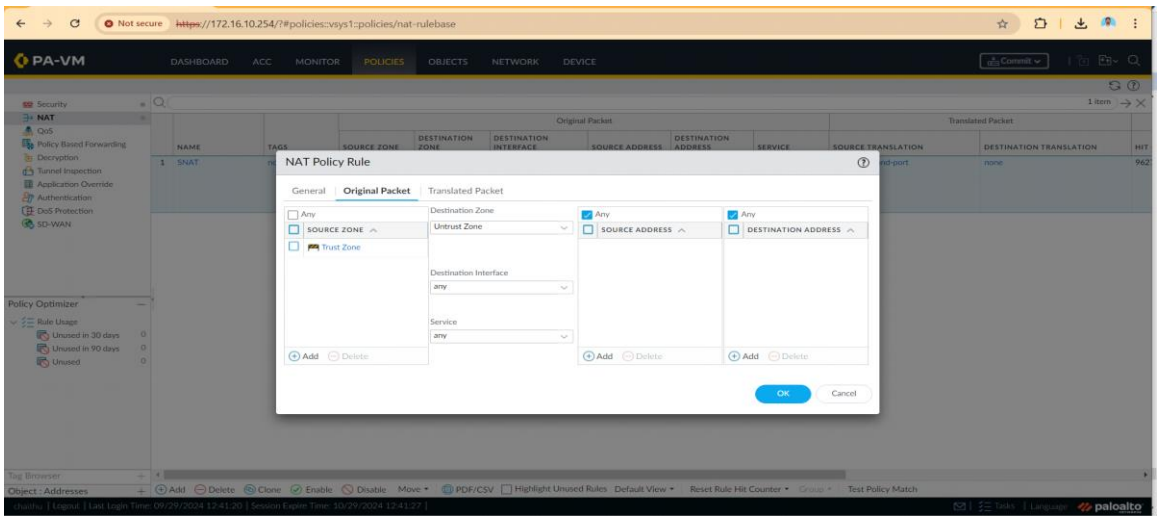
1.Navigate to the NAT Configuration:

- Go to Policies > **NAT.**
- Click **Add** to create a new NAT policy.
- **NAT** Rule General Settings:
- **Name:** Give your rule a name (**SNAT**).



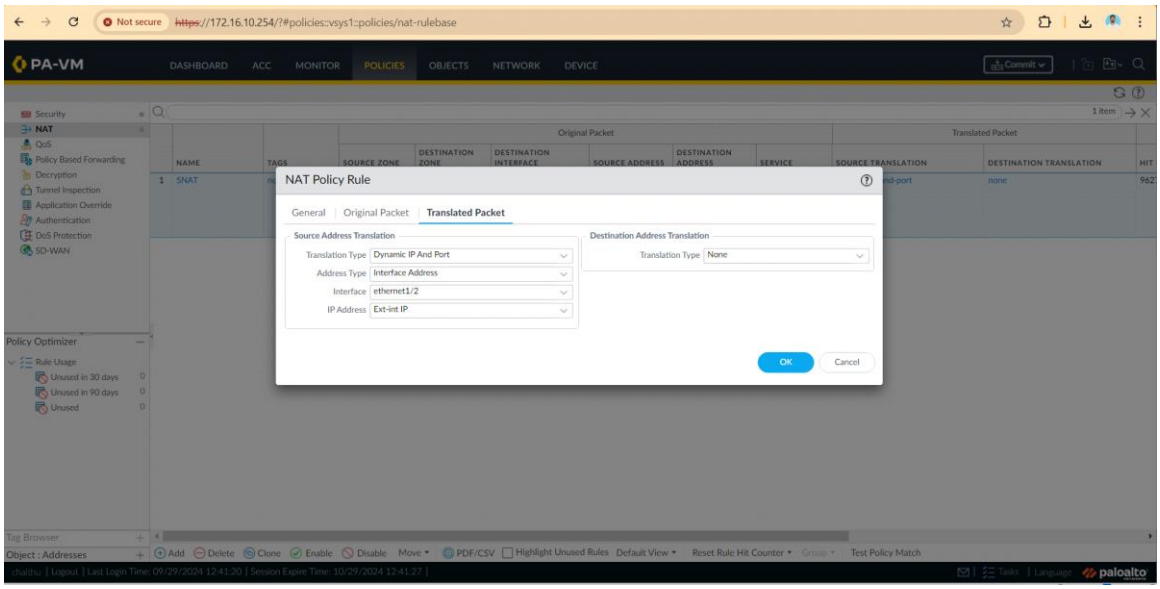
2.Original Packet Tab:

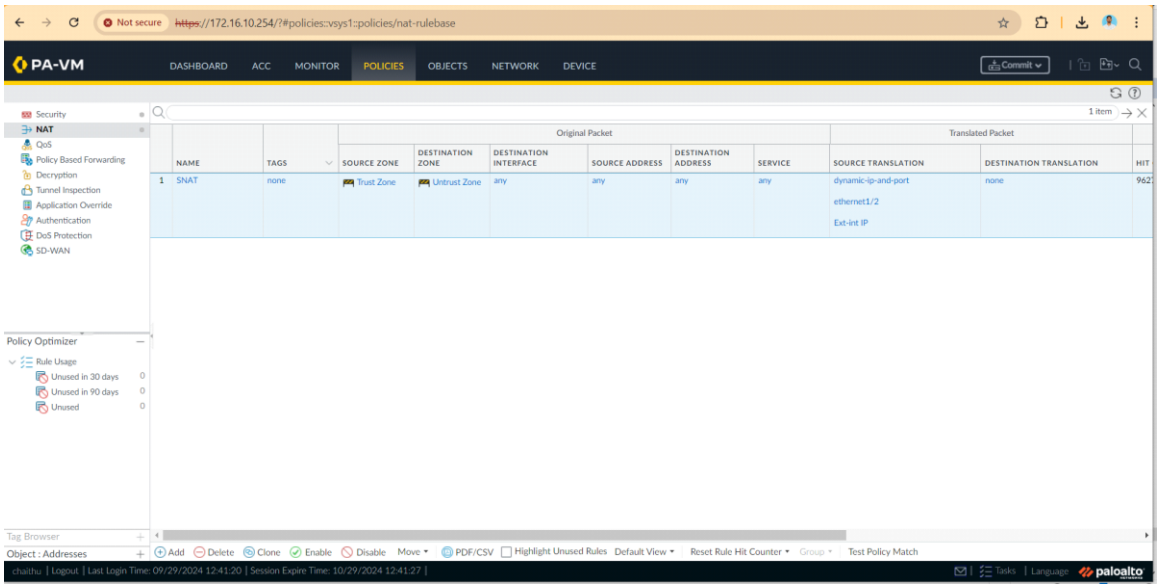
- **Source Zone:** Select your LAN zone (the zone from where traffic originates).
- **Destination Zone:** Select WAN.
- **Destination Interface:** Select your WAN interface (**ethernet1/1**).



3. Translation Tab:

- **Dynamic IP and Port:** Choose this option if you're using PAT (Port Address Translation).
- **Interface Address:** Choose the WAN interface and assign the public IP address or interface IP.
- Click OK.



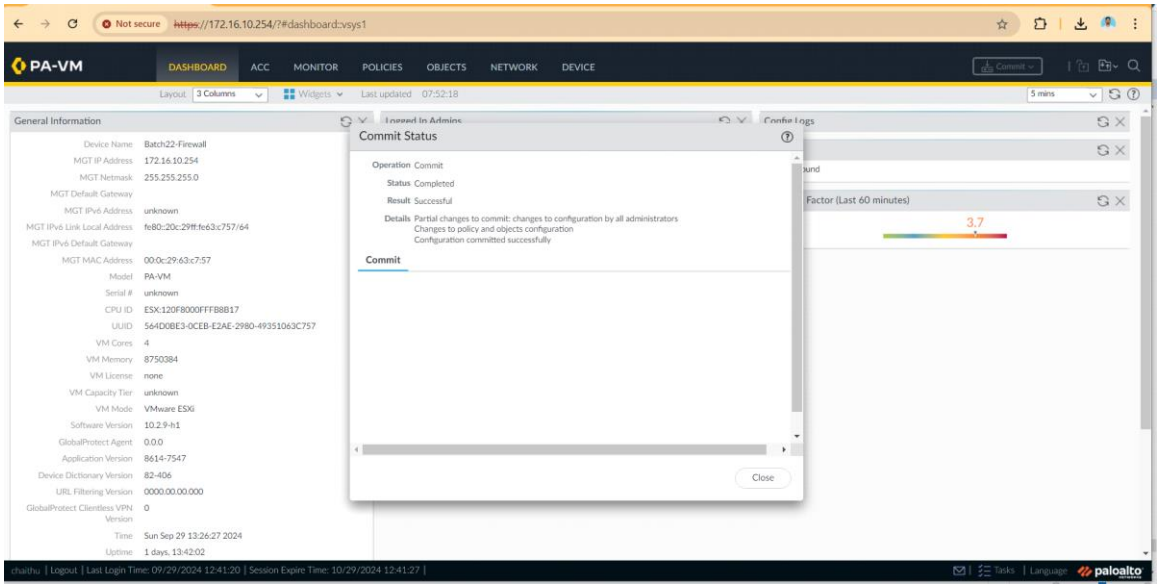


4.Commit the Configuration

Once all the changes have been made, you must commit them to apply.

Commit the Changes:

- In the upper-right corner, click the Commit button.
- Review the changes and click Commit again to finalize.



Conclusion:

Zones, interfaces, the virtual router, and Source NAT were configured successfully, allowing traffic flow between internal and external networks with proper address translation.

Thank You