

ASSIGNMENT

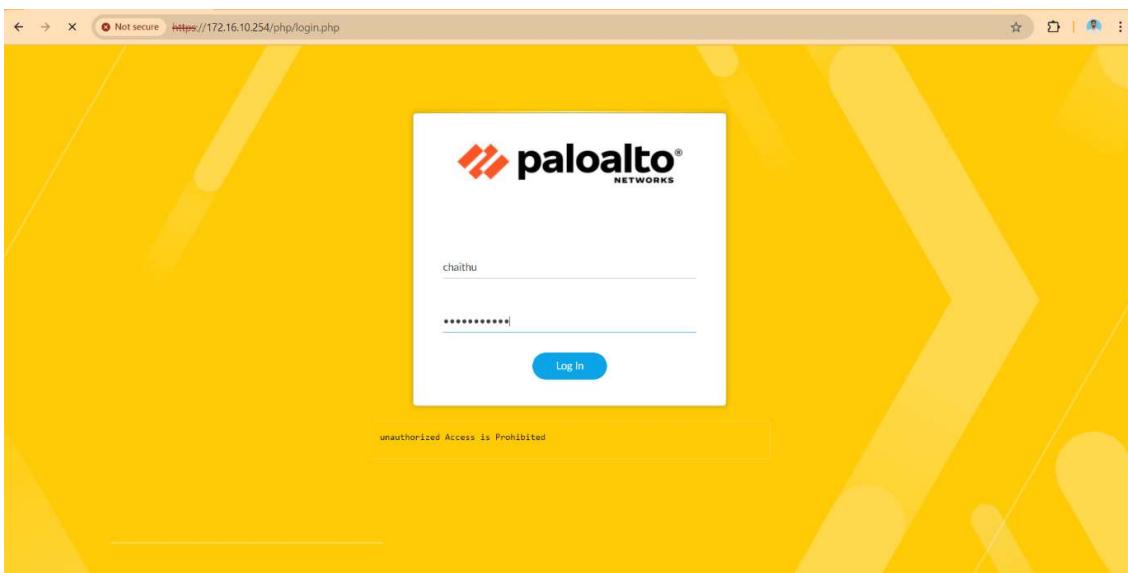
COURSE	PAN Firewall	ASSIGNMENT NO	4
MODULE	Firewall	ASSIGNMENT DATE	28-Sep-24
STUDENT NAME	Konganti Chaithanya Kumar	SUBMIT DATE	29-Sep-24

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:

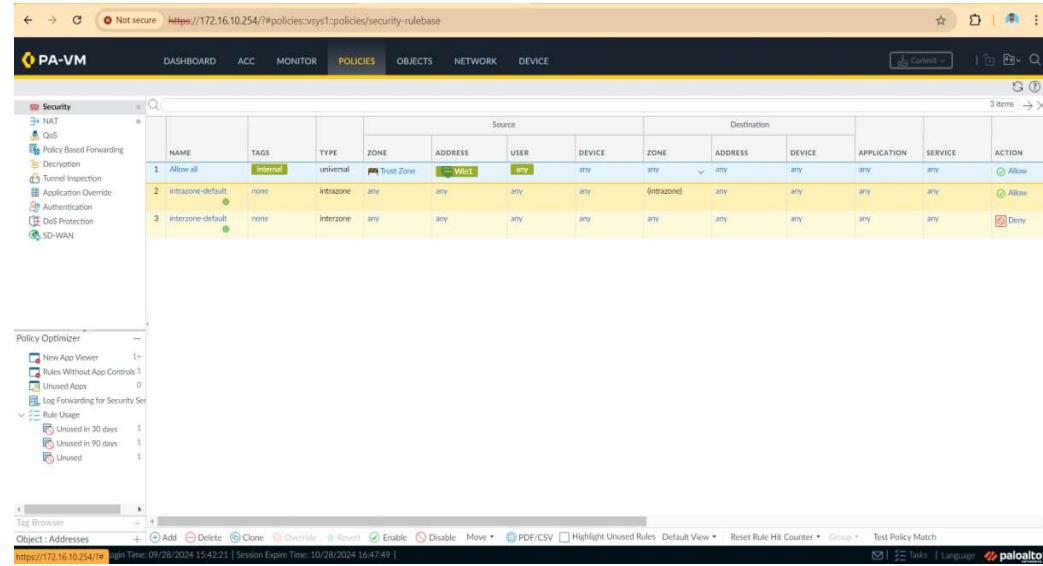
1. Log in to the Palo Alto Firewall:

- 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.



The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES (selected), OBJECTS, NETWORK, and DEVICE. The left sidebar under 'Security' lists NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. The main content area displays a table of security policies:

NAME	TAGS	TYPE	ZONE	Source			Destination			APPLICATION	SERVICE	ACTION
				ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1 Allow all	internal	universal	Trust Zone	(Wan)	any	any	any	(Intrazone)	any	any	any	
2 intrazone-default	none	Intrazone	any	any	any	any	any	any	any	any	any	
3 interzone-default	none	Interzone	any	any	any	any	any	any	any	any	any	

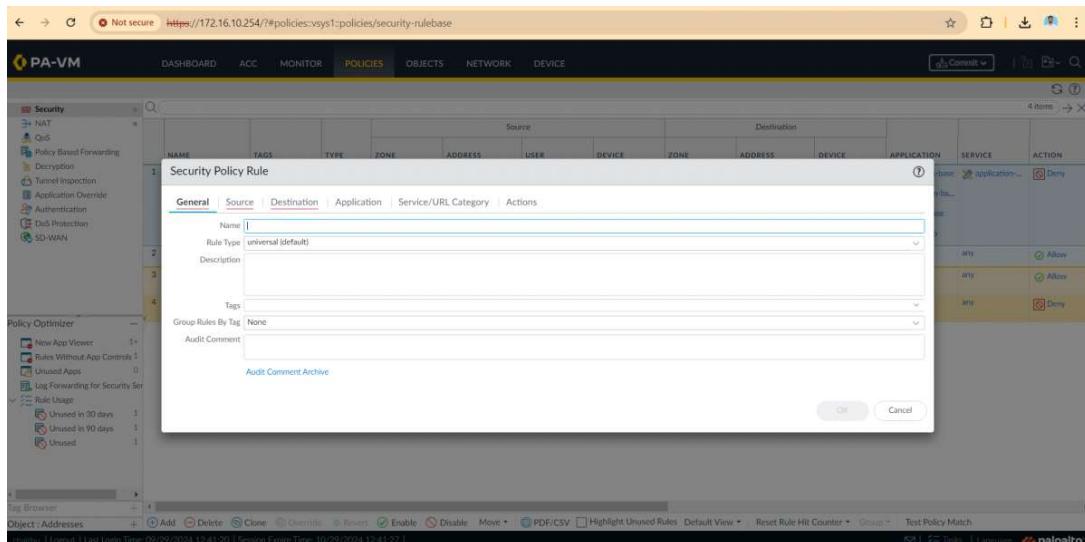
The 'Policy Optimizer' sidebar on the left shows the following rule usage statistics:

- New App Viewer: 1+
- Rules Without App Controls: 1
- Unused Apps: 0
- Log Forwarding for Security Services: 0
- Rule Usage:
 - Unused in 30 days: 1
 - Unused in 90 days: 1
 - Unused: 1

The bottom status bar indicates the URL as https://172.16.10.254/# and the current time as 09/28/2024 15:42:21.

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.



The screenshot shows the 'Security Policy Rule' dialog box in the foreground, overlaid on the main security policies list. The 'General' tab is active, containing the following fields:

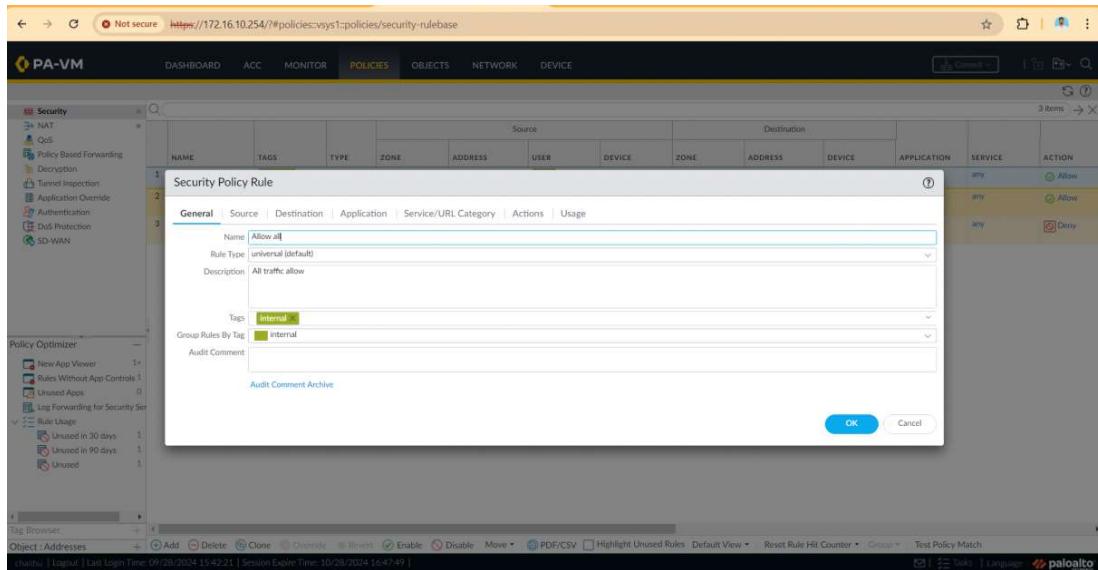
- Name:
- Rule Type: universal (default)
- Description:
- Tags:
- Group Rules By Tag: None
- Audit Comment:

The 'OK' and 'Cancel' buttons are visible at the bottom right of the dialog. In the background, the main security policies list is visible, showing the same three rules as the previous screenshot.

4. Configure the Policy:

Name the Policy:

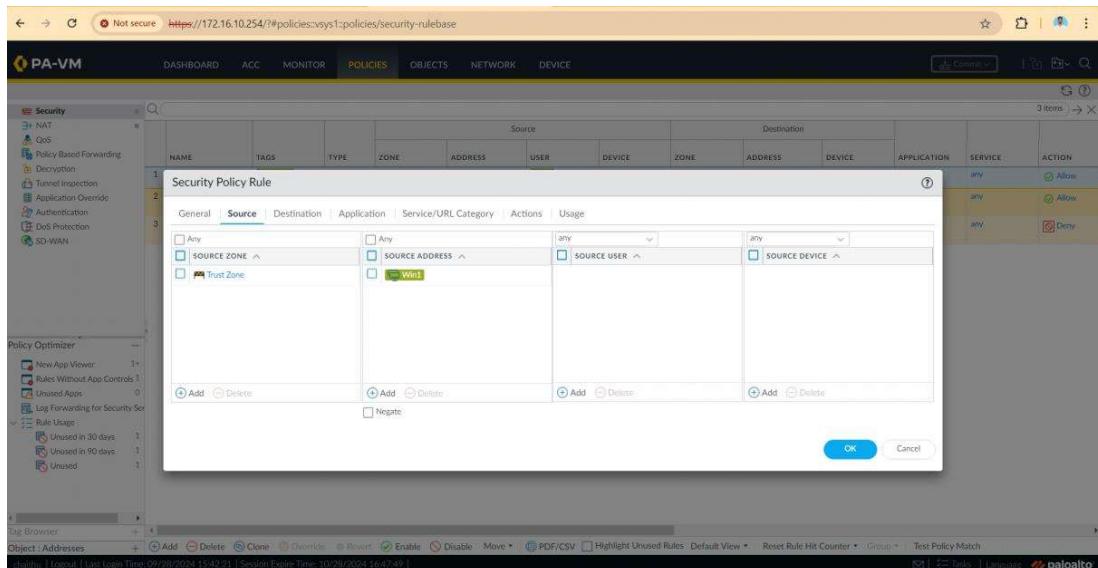
- In the **General** tab, provide a descriptive name for the policy such as **Allow-Internet**.
- Add a description for clarity like "**Allow all**".



The screenshot shows the 'Security Policy Rule' configuration window. The 'General' tab is selected. The 'Name' field contains 'Allow all'. The 'Rule Type' dropdown is set to 'universe (default)'. The 'Description' field contains 'All traffic allow'. Under 'Tags', there is a single tag named 'internal'. The 'Audit Comment' field is empty. The 'OK' button is visible at the bottom right.

Source Configuration:

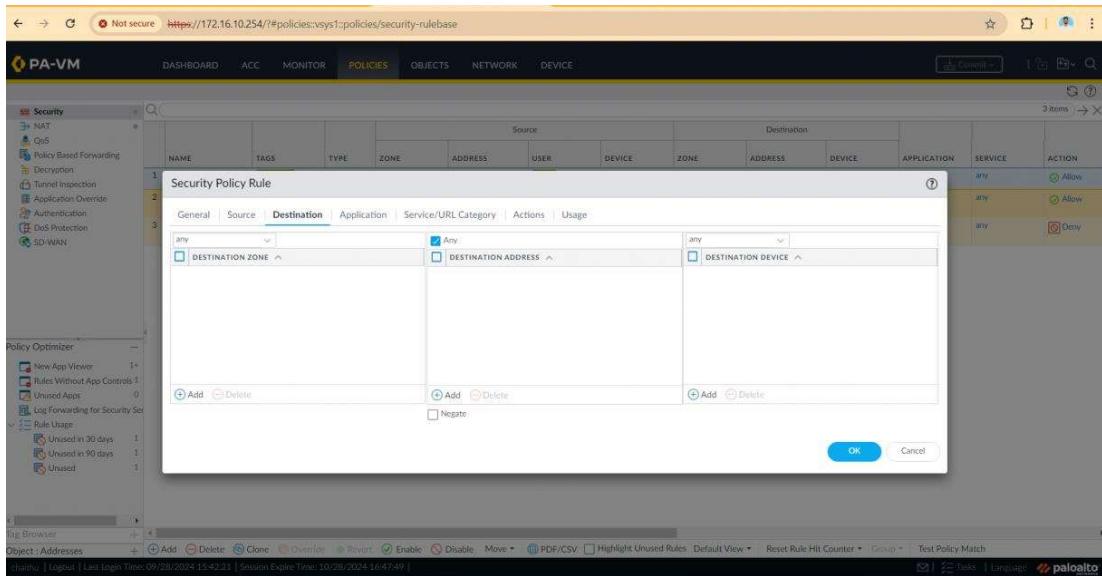
- Source Zone:** Select the internal network zone **Trust**.
- Source Address:** Specify the internal subnet (simply select **Any** if you want to allow all internal addresses).



The screenshot shows the 'Source' tab of the 'Security Policy Rule' configuration window. The 'SOURCE ZONE' dropdown is set to 'Trust Zone'. The 'SOURCE ADDRESS' dropdown is set to 'Any'. The 'SOURCE USER' and 'SOURCE DEVICE' dropdowns are both set to 'any'. The 'OK' button is visible at the bottom right.

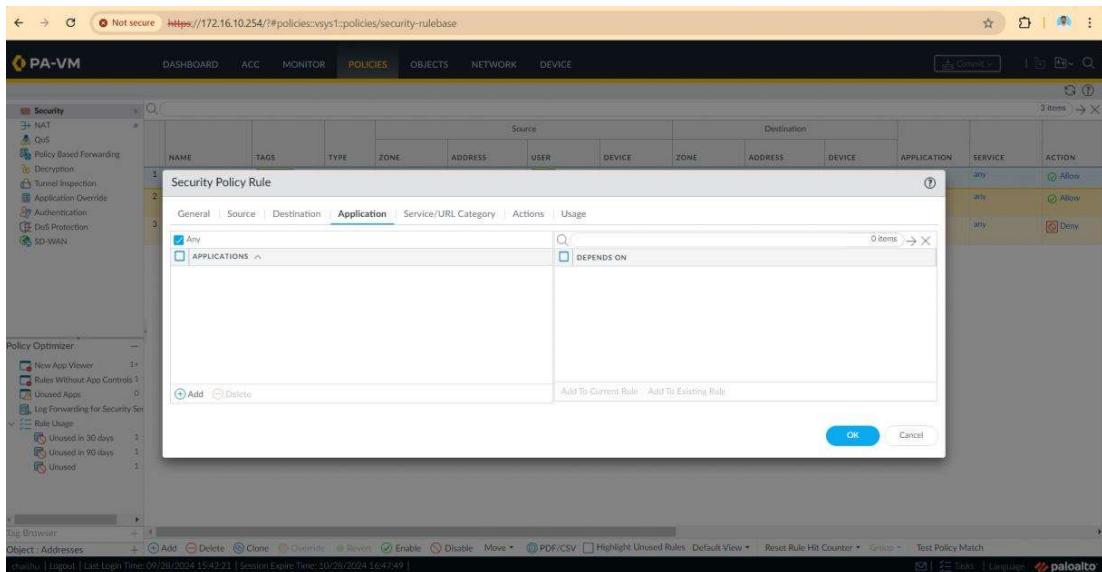
Destination Configuration:

- 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.



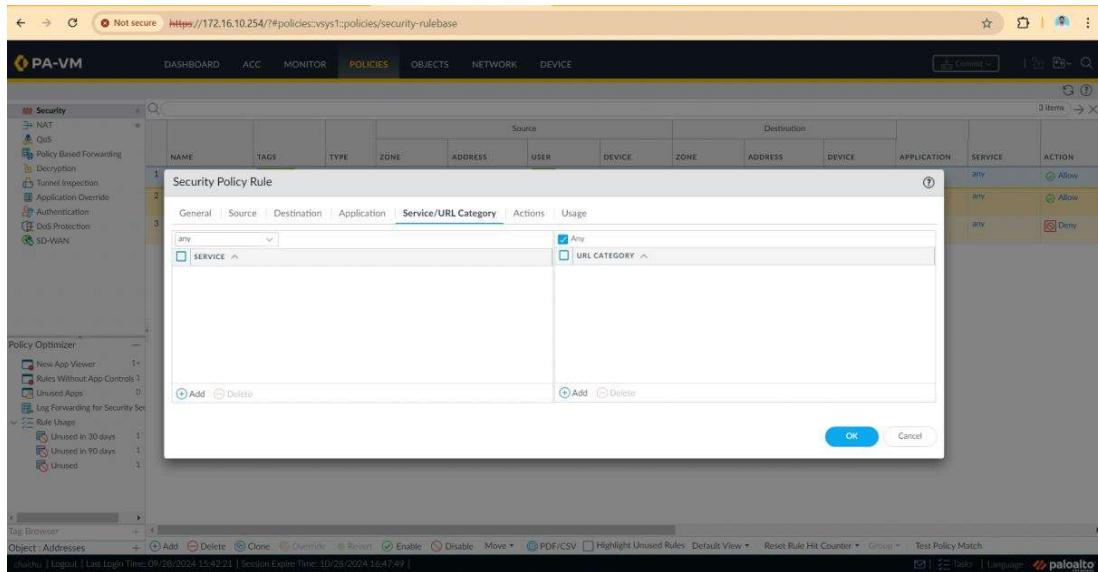
Application Tab:

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



Service/URL Category:

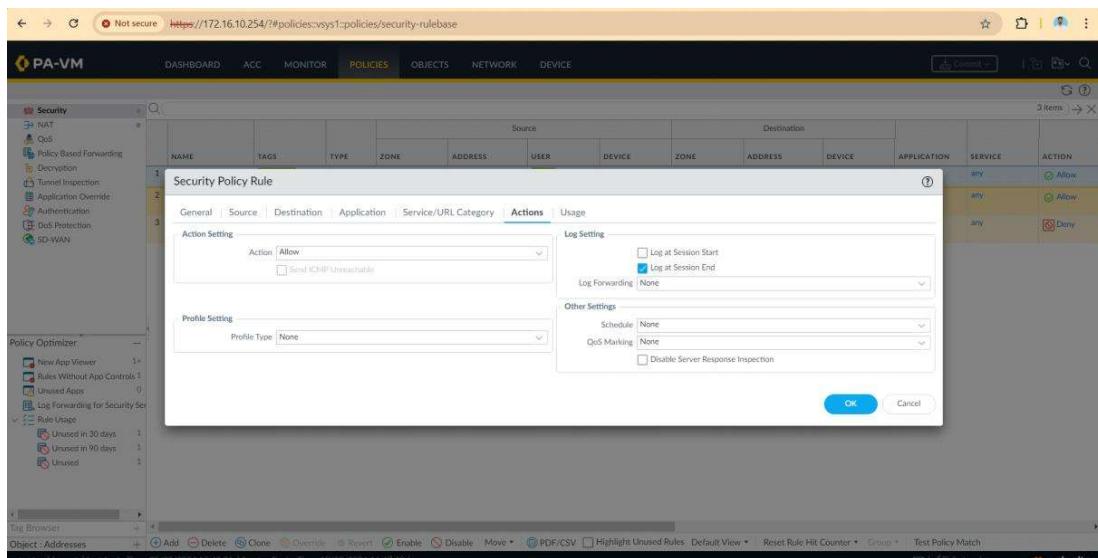
- In the **Service/URL Category** tab, set **Service** to **application-default** to allow internet traffic on the default ports (e.g., port 80 for HTTP, port 443 for HTTPS).



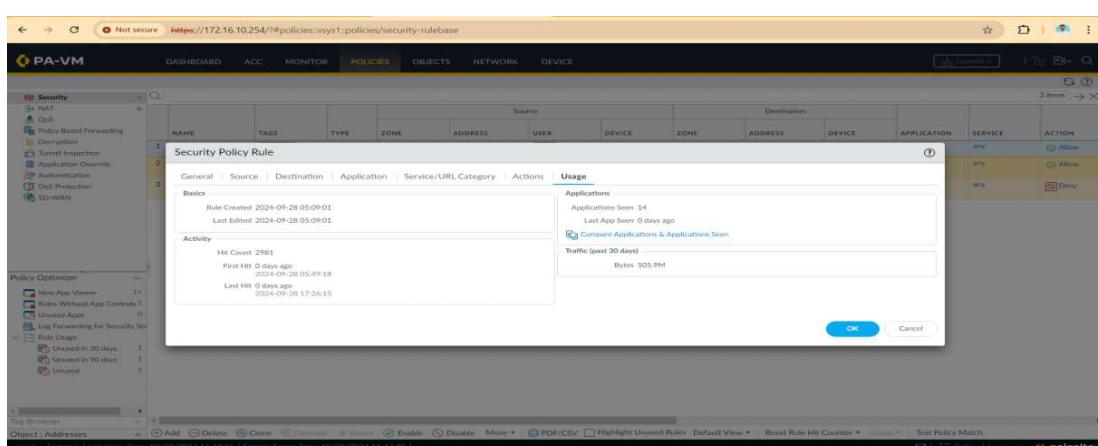
The screenshot shows the 'Security Policy Rule' configuration dialog in the Palo Alto Networks interface. The 'Service/URL Category' tab is selected. Under the 'Source' section, there is a dropdown menu set to 'any'. Below it, there is a 'SERVICE' dropdown with an option 'Any' selected. To the right of the source section, there is a 'URL CATEGORY' dropdown with an option 'None' selected. At the bottom of the dialog, there are 'Add' and 'Delete' buttons, and a large 'OK' button.

Action:

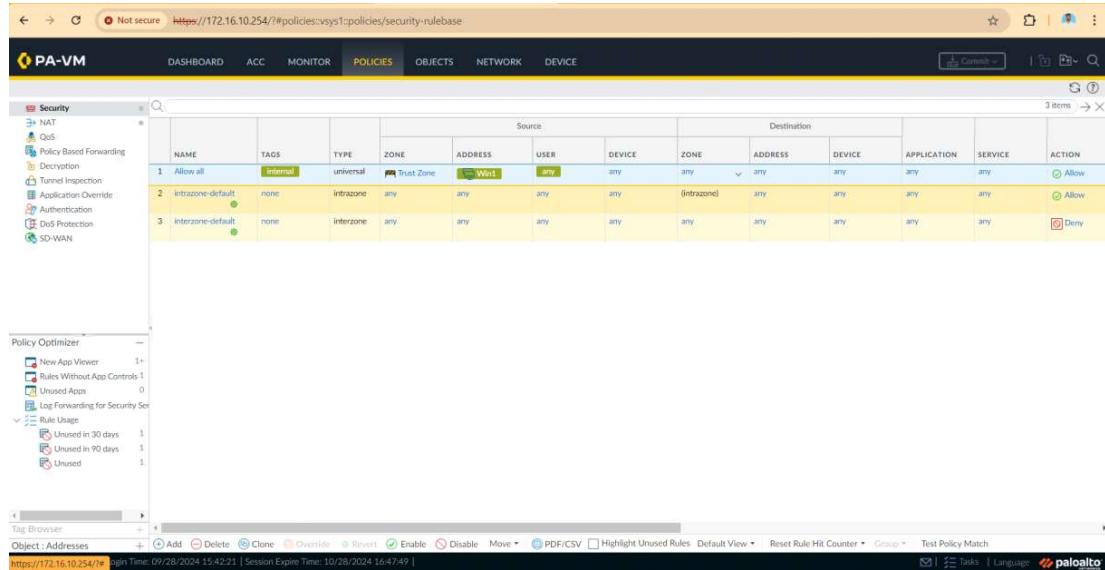
- In the Action tab, set the Action to Allow.



The screenshot shows the 'Actions' tab of the 'Security Policy Rule' configuration dialog. In the 'Action Setting' section, the 'Action' dropdown is set to 'Allow'. Below it, there is a checkbox for 'Send ICMP Unreachable'. In the 'Log Setting' section, the 'Log at Session Start' checkbox is unchecked, while 'Log at Session End' is checked. The 'Log Forwarding' dropdown is set to 'None'. In the 'Profile Setting' section, the 'Profile Type' dropdown is set to 'None'. In the 'Other Settings' section, the 'Schedule' dropdown is set to 'None', and the 'QoS Marking' dropdown is set to 'None'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.



The screenshot shows the 'Usage' tab of the 'Security Policy Rule' configuration dialog. It displays basic information about the rule: 'Rule Created: 2024-09-28 05:09:01' and 'Last Edited: 2024-09-28 05:09:01'. It also shows activity statistics: 'Hit Count: 2981', 'First Hit: 2024-09-28 05:09:18', and 'Last Hit: 2024-09-28 17:26:15'. The 'Applications' section shows 'Applications Seen: 14' and 'Last App Seen: 0 days ago'. There is a link to 'Compare Applications & Applications Seen'. The 'Traffic' section shows 'Bytes: 505.9M'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

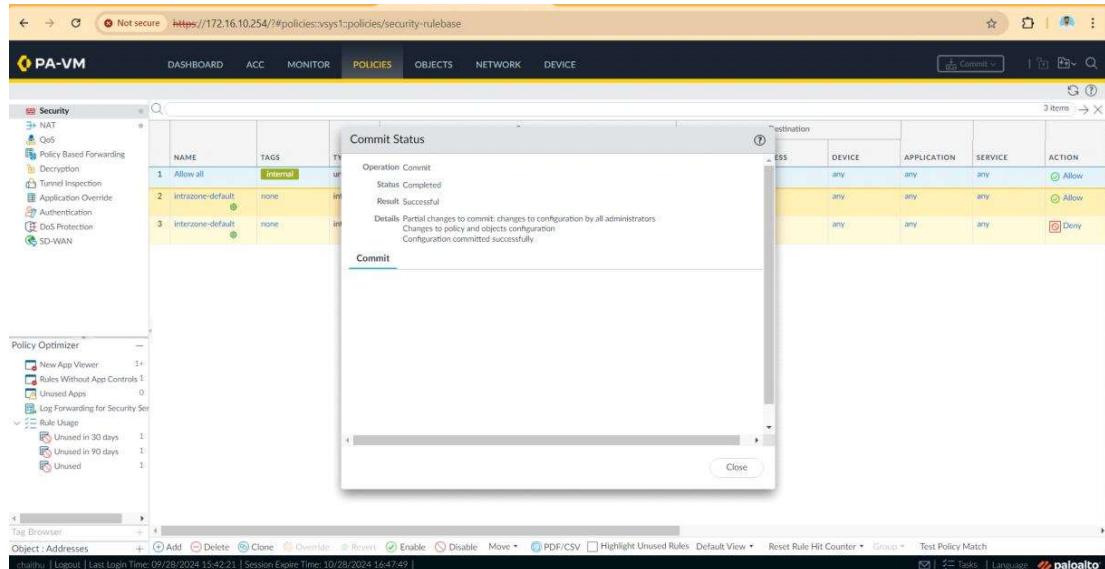


The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The POLICIES tab is selected. On the left, a sidebar titled "Security" lists various features like NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DDoS Protection, and SD-WAN. Below this is the "Policy Optimizer" section, which displays rule usage statistics. The main content area shows a table of security rules. The table columns are: NAME, TAGS, TYPE, ZONE, ADDRESS, USER, DEVICE, DESTINATION, APPLICATION, SERVICE, and ACTION. The rules listed are:

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	DESTINATION	APPLICATION	SERVICE	ACTION
Allow all	Internal	universal	Trust Zone	any	any	any	any	any	any	Allow
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	Allow
interzone-default	none	interzone	any	any	any	any	any	any	any	Deny

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.



The screenshot shows the Palo Alto Networks PA-VM interface after committing the policy. A modal dialog box titled "Commit Status" is displayed in the center. It shows the following information:

- Operation: Commit
- Status: Completed
- Result: Successful
- Details: Partial changes to commit: changes to configuration by all administrators
Changes to policy and objects configuration
Configuration committed successfully.

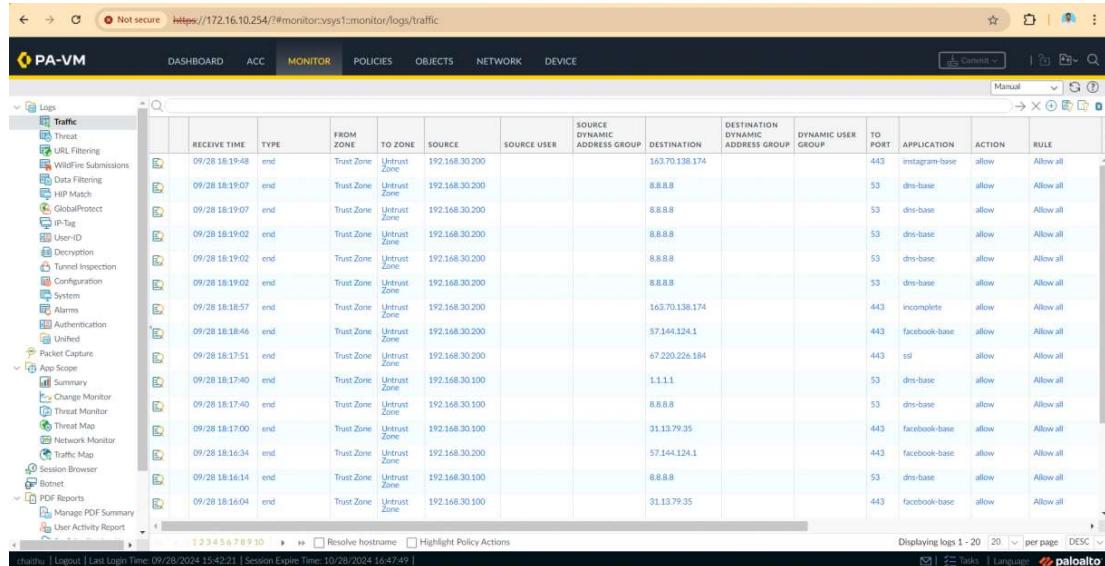
At the bottom of the dialog box, there is a "Close" button. The main interface remains the same as the previous screenshot, showing the security policy configuration table.

6. Verification and Logs:

Viewing Logs:

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

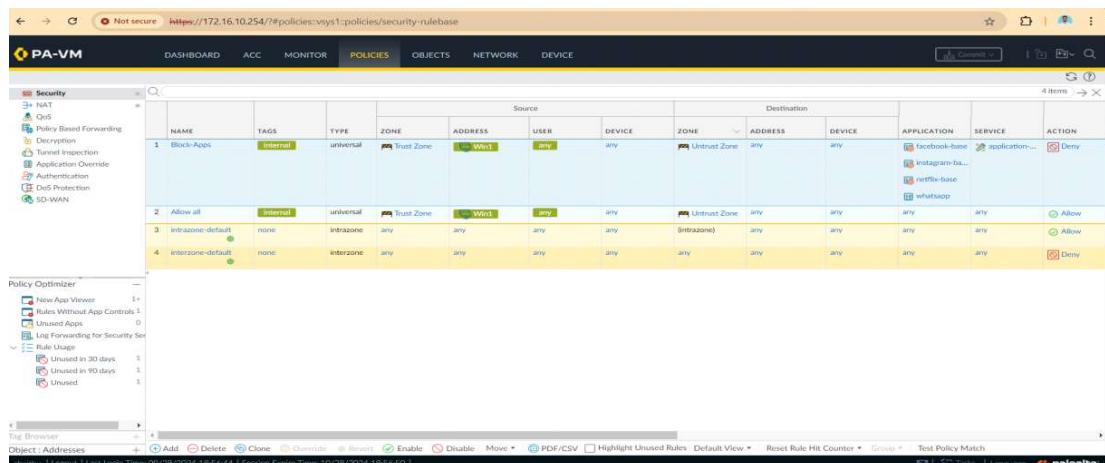
- Navigate to **Monitor > Logs > Traffic** to view the logs.
- Filter the logs based on the security policy you just created (Allow-Internet) to see the allowed internet access from the internal network.



The screenshot shows the Palo Alto Networks PA-VM interface with the URL <https://172.16.10.254/#monitor:sys1:monitor/logs/traffic>. The left sidebar has a 'Logs' section expanded, showing various log types like Threat, URL Filtering, and Traffic. The main area displays a table of traffic logs. The columns include: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION, DESTINATION DYNAMIC ADDRESS GROUP, DYNAMIC USER GROUP, TO PORT, APPLICATION, ACTION, and RULE. The logs show multiple entries for port 80 (HTTP) from internal IP 192.168.30.200 to external IP 163.70.138.174, with applications like instagram-base, facebook-base, and netflix-base, all labeled 'allow' under ACTION.

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.



The screenshot shows the Palo Alto Networks PA-VM interface with the URL <https://172.16.10.254/#policies:sys1:policies/security:rulebase>. The left sidebar has a 'Security' section expanded, showing rules for NAT, Policy Based Forwarding, and SD-WAN. The main area displays a table of security rules. The columns include: NAME, TAGS, TYPE, ZONE, ADDRESS, USER, DEVICE, Source, Destination, APPLICATION, SERVICE, and ACTION. There are four rules listed: 1. Block-App (universal, Trust Zone, Win1, any, Untrust Zone, any, Deny), 2. Allow-all (universal, Trust Zone, Win1, any, Untrust Zone, any, Allow), 3. Intrazone-default (intrazone, any, any, any, any, any, any, any, any, any, Allow), and 4. interzone-default (interzone, any, any, any, any, any, any, any, any, any, Deny).

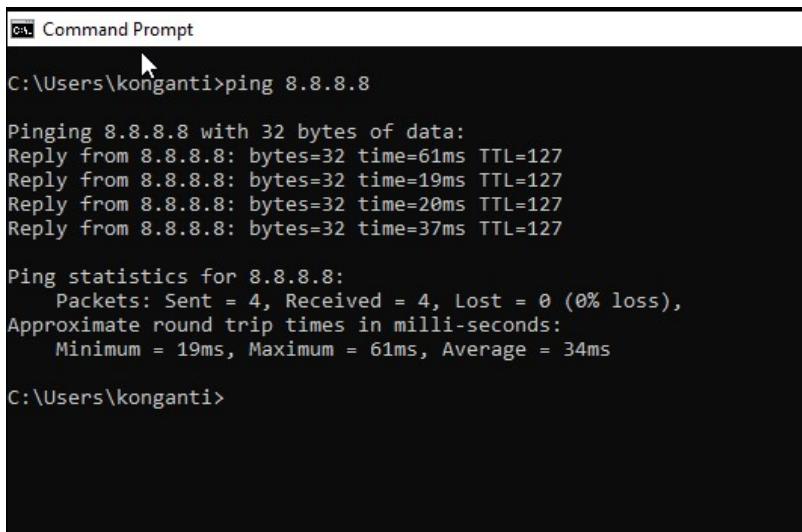
Ping and Web Access Test:

- 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.



```
C:\> Command Prompt
C:\Users\konganti>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=61ms TTL=127
Reply from 8.8.8.8: bytes=32 time=19ms TTL=127
Reply from 8.8.8.8: bytes=32 time=20ms TTL=127
Reply from 8.8.8.8: bytes=32 time=37ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 61ms, Average = 34ms

C:\Users\konganti>
```

Final Output:

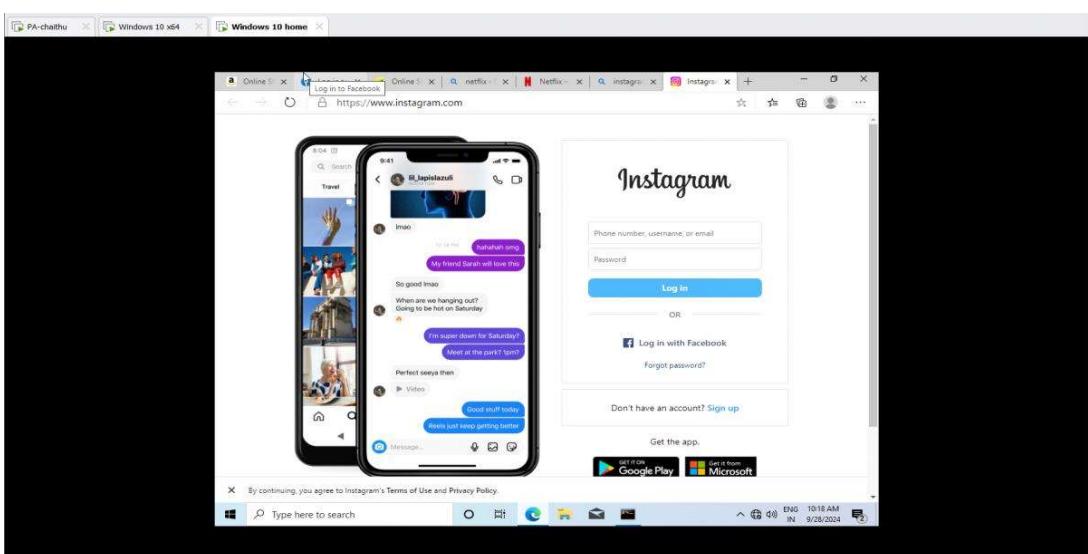
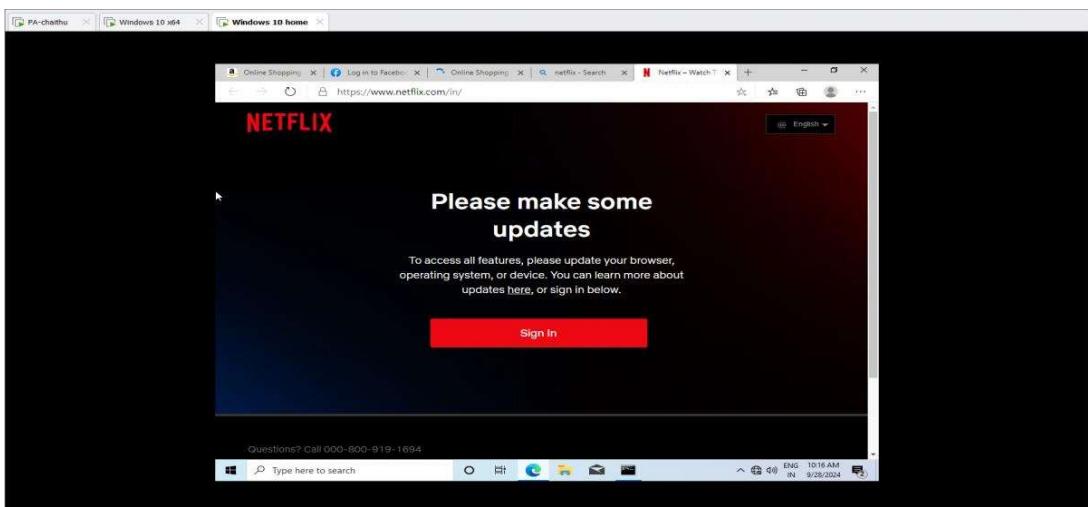
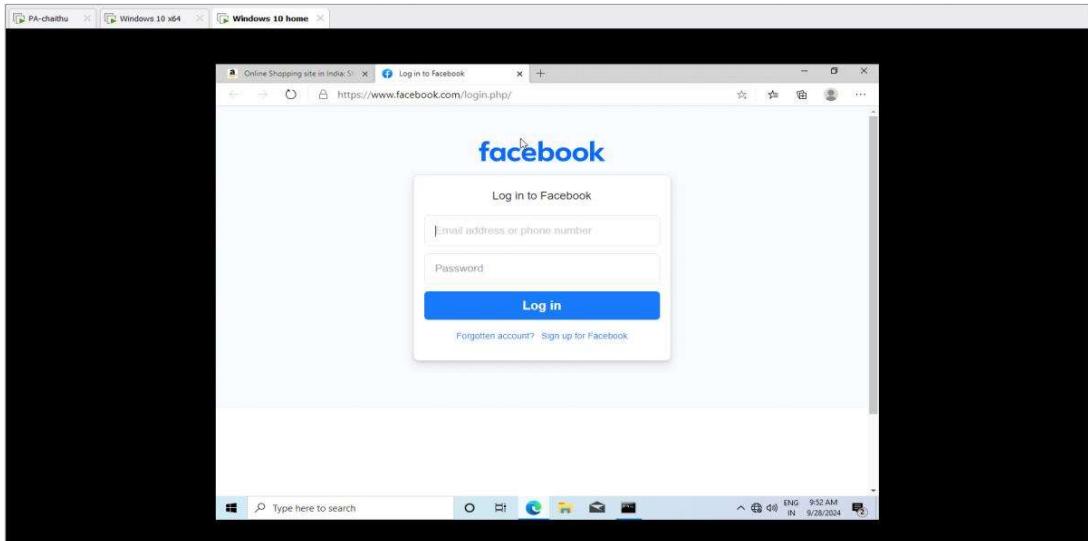
Steps to Check Internet Access with Webpages:

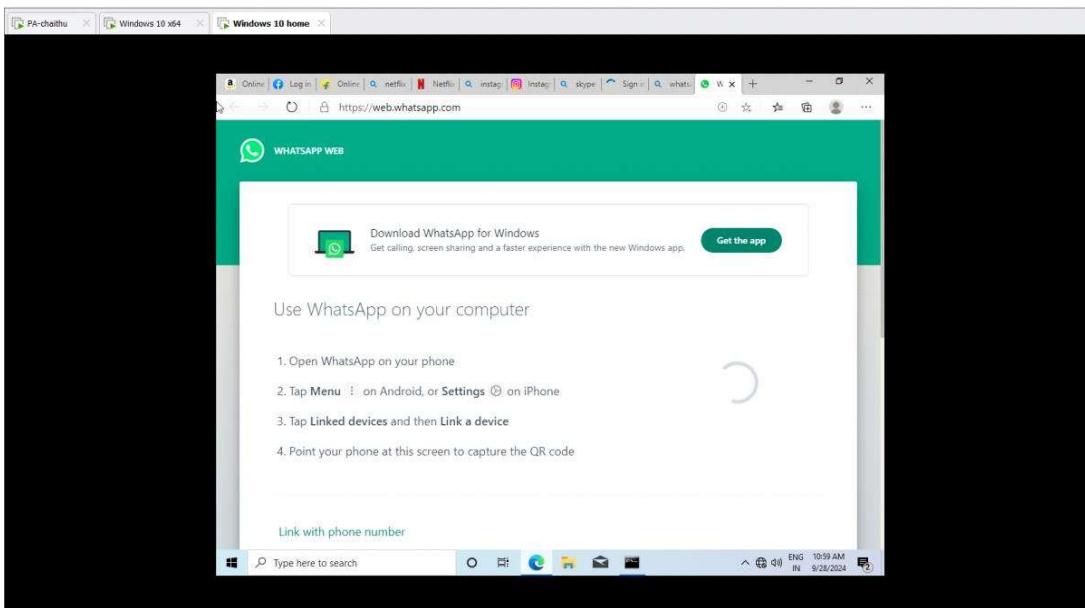
1. Webpage Access Test (Allow Internet Access):

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:

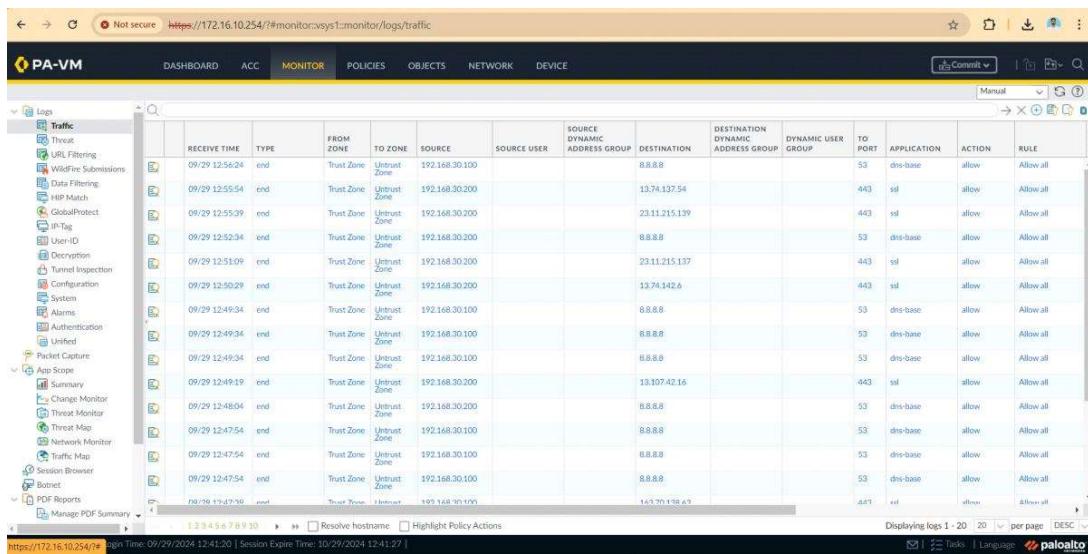




Verifying Traffic on Palo Alto Firewall:

- 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:

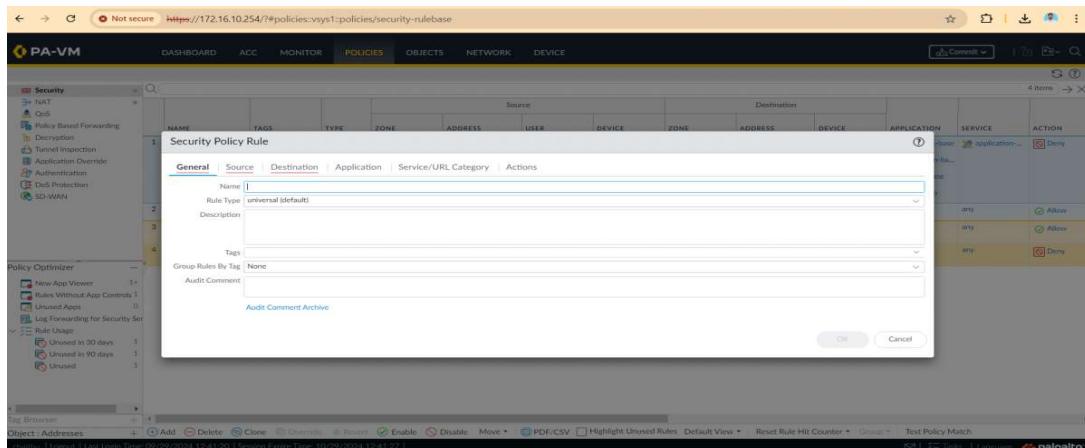
1. Login to Palo Alto Networks Firewall

- 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).



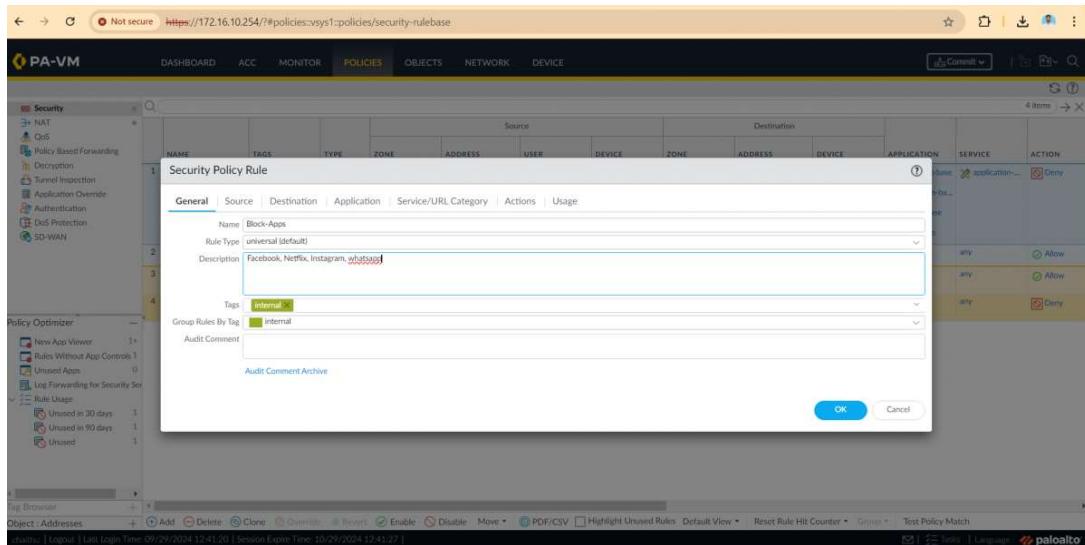
2. Navigate to the Security Policies

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



3. Create a New Security Policy

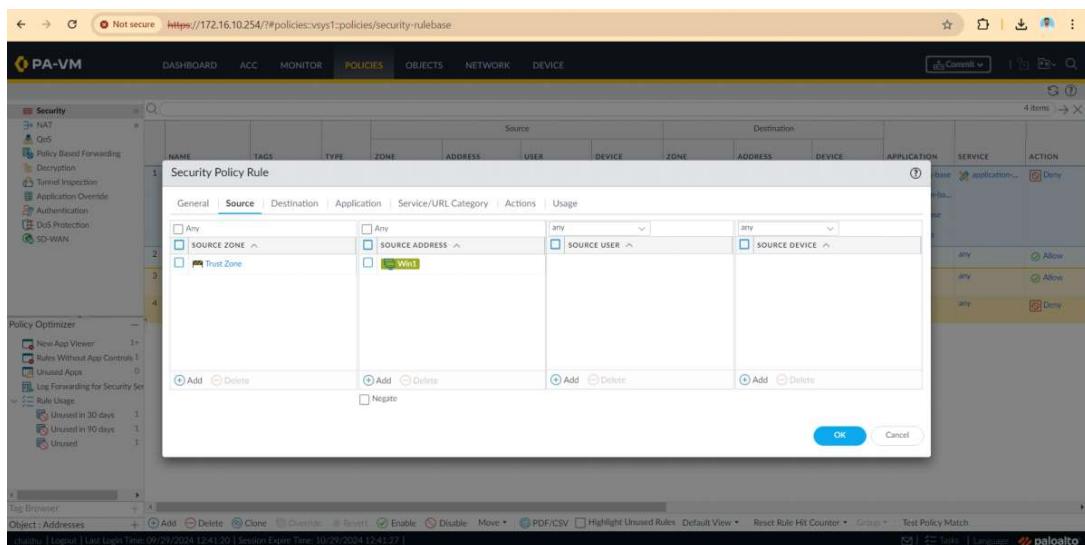
- Click on **Add** to create a new security policy.
- Give your policy a **Name**: **Block App**



The screenshot shows the Palo Alto Networks PA-VM interface for creating a Security Policy Rule. The rule is named "Block-Apps" and has a "universal (default)" rule type. The description is set to "Facebook, Netflix, Instagram, whatsaap". Under the "Tags" section, "internal" is selected. The "Source" tab is active, showing "Any" as the source. The "Destination" tab shows "any" as the destination. The "Actions" tab indicates "Deny". The "Audit Comment" field is empty. The "OK" button is highlighted.

Source Zone:

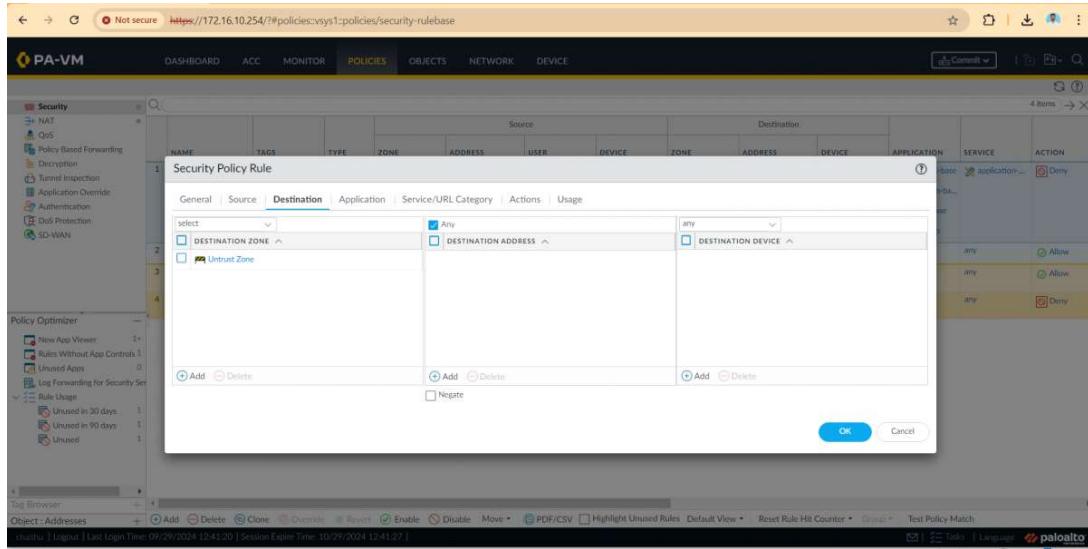
- Define the source zone (**Trust** zone).
- Select internal devices or users as the source.



The screenshot shows the "Source" tab of the Security Policy Rule configuration. The "Any" source is selected. Under "SOURCE ZONE", "Trust Zone" is chosen. The "OK" button is highlighted.

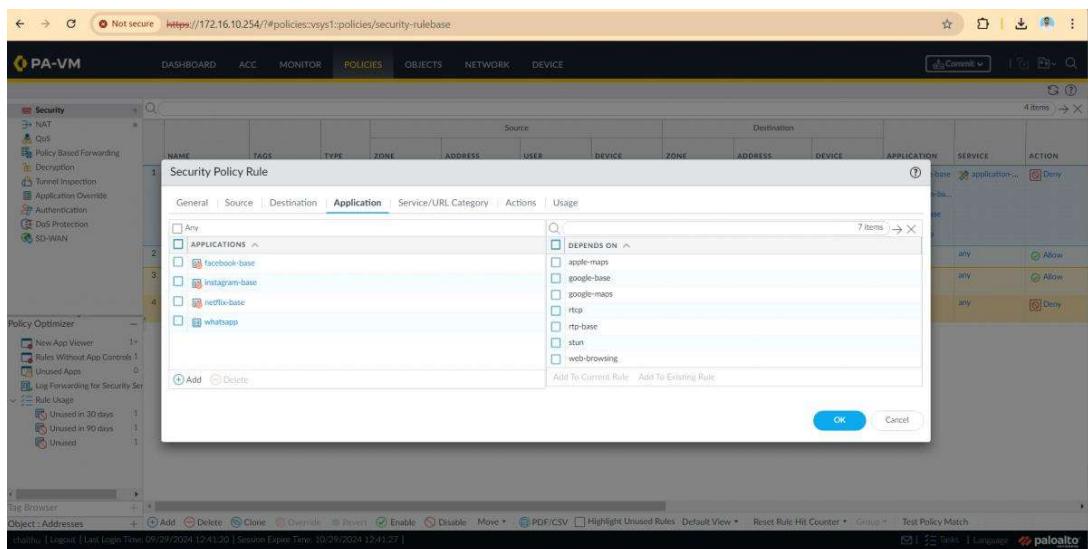
Destination Zone:

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



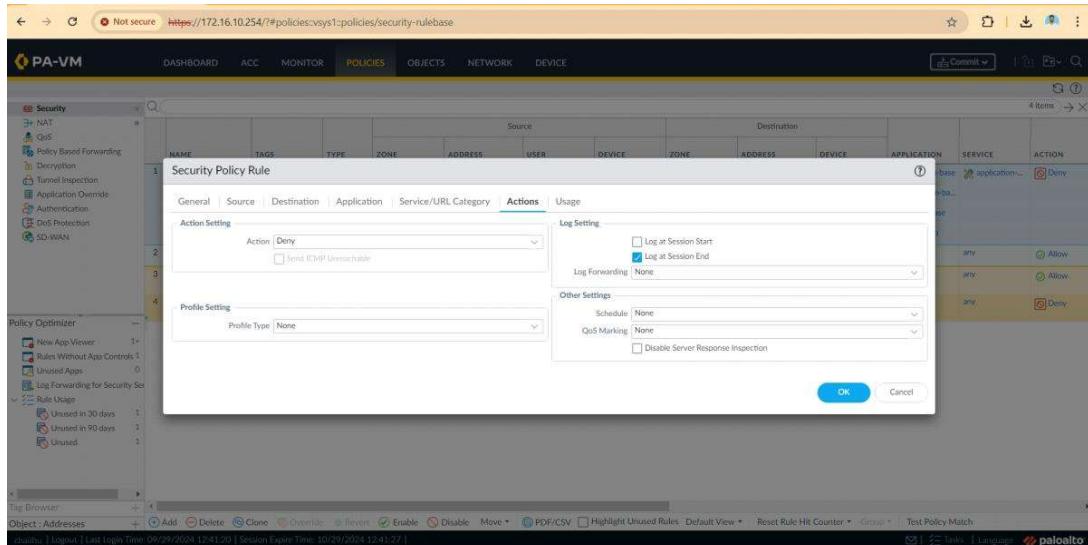
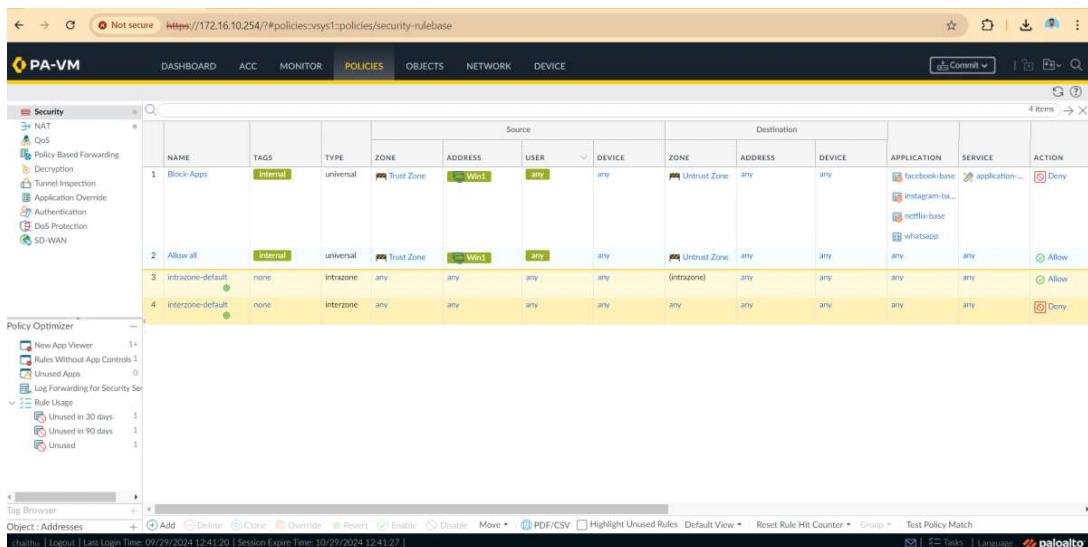
4. Define Applications to Block

- 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.



The screenshot shows the PA-VM dashboard interface. The top navigation bar includes links for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. A floating alert box in the center-right area displays a red warning icon, the text "sound", and a progress bar labeled "Factor (Last 60 minutes)" with a value of "3.7". The main content area is divided into sections: General Information, Commit Status, and a large central pane for configuration changes.

General Information

- Device Name: Batch22-Firewall
- MGT IP Address: 172.16.10.254
- MGT Network: 255.255.255.0
- MGT Default Gateway: MGT IPv4 Address: unknown
- MGT IPv6 Default Gateway: MGT IPv6 Default Gateway: fe80::20c:29ff%eth3<757/64
- MGT MAC Address: 00:0c:29:63:c7:57
- Model: PA-VM
- Serial #: unknown
- CPU ID: E5K120F8000FFB88E7
- UUID: 56400BE3-0CEB-E2AE-2980-49351069C757
- VM Cores: 4
- VM Memory: 8790384
- VM License: none
- VM Capacity Tier: unknown
- VM Mode: VMware ESXi
- Software Version: 10.2.9-81
- GlobalProtect Agent: 0.0.0
- Application Version: 8614-7547

Device Dictionary Version: 82-406
URL Filtering Version: 0000.00.00.00
GlobalProtect Clientless VPN Version: 0

Time: Sun Sep 29 13:26:27 2024
Uptime: 1 days, 13:42:02

Commit Status

Operation: Commit
Status: Completed
Result: Successful
Details: Partial changes to commit: changes to configuration by all administrators
Changes to policy and objects configuration
Configuration committed successfully

Commit

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.

The screenshot shows the Palo Alto Networks PA-VM interface for monitoring network traffic. The top navigation bar includes links for Dashboard, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, and a Commit button. The left sidebar has a 'Logs' section with a 'Traffic' category selected, listing various log types like Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, IP-Tag, User-ID, Decryption, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, and Packet Capture. Below this is an 'App Scope' section with Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map, Session Browser, Botnet, PDF Reports, and Manage PDF Summary.

The main content area displays a table of network logs. The columns are: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION, DESTINATION DYNAMIC ADDRESS GROUP, DYNAMIC USER GROUP, TO PORT, APPLICATION, ACTION, and RULE. The table contains 20 rows of log entries, each with a timestamp ranging from 09/29 12:54:24 to 09/29 12:57:10, and various destination ports like 8.8.8, 443, 23.11.215.137, and 192.168.30.100.

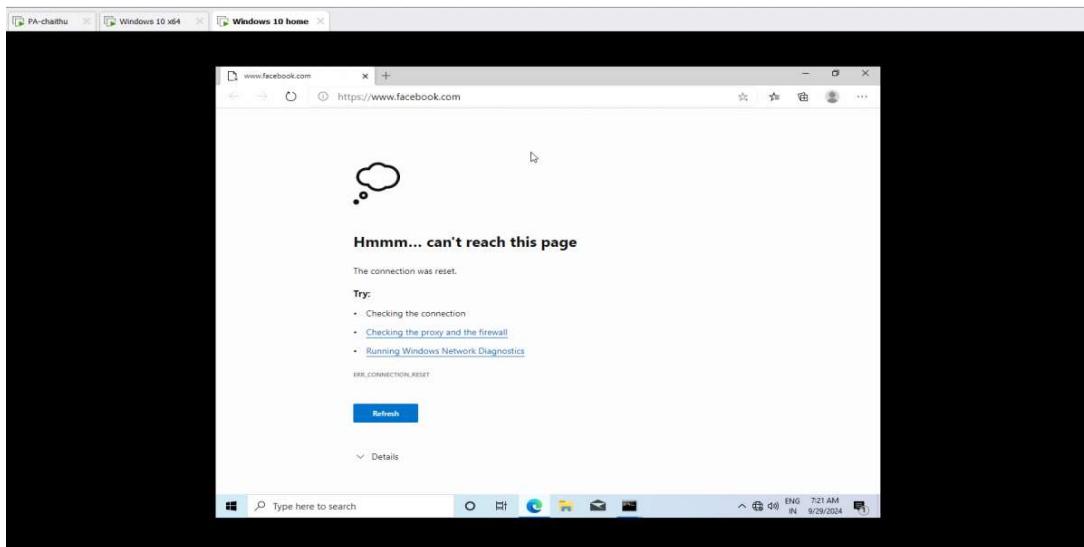
Final Output:

Screenshot Documentation:

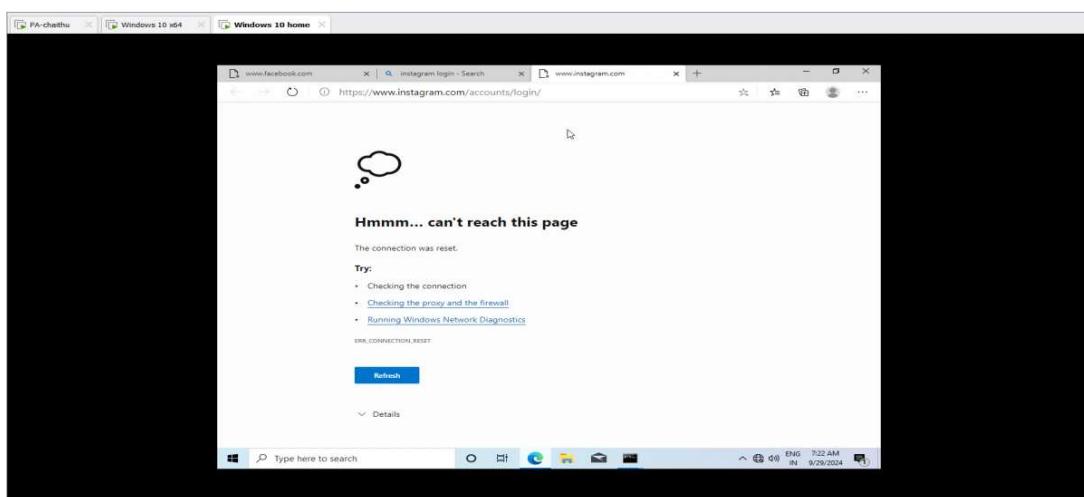
- **Login Page:** Capture a screenshot of the login page showing access to the PAN firewall.

- **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.

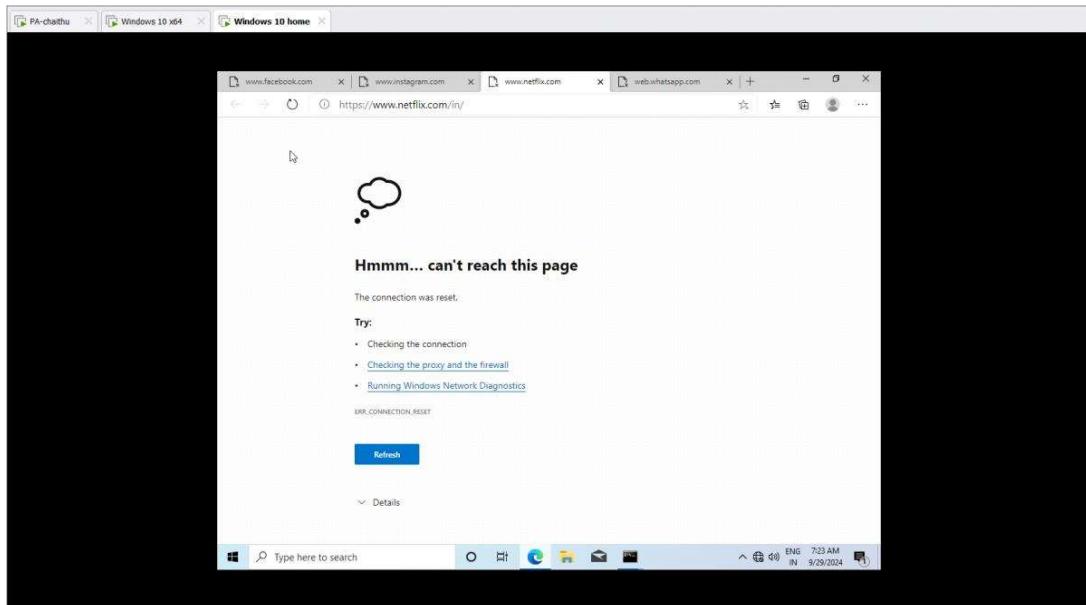
Facebook:



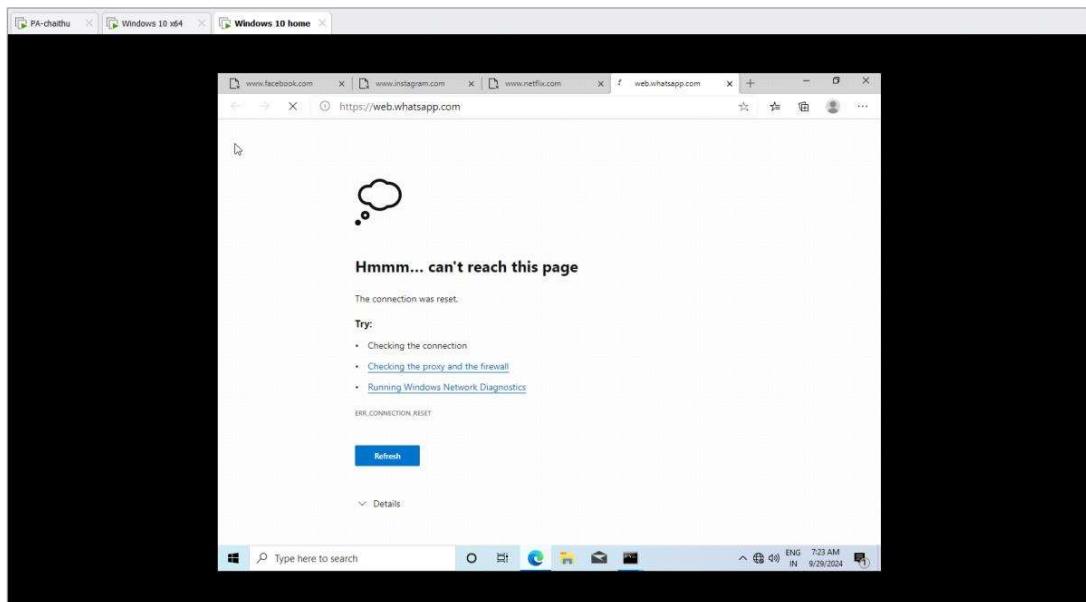
Instagram:



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.

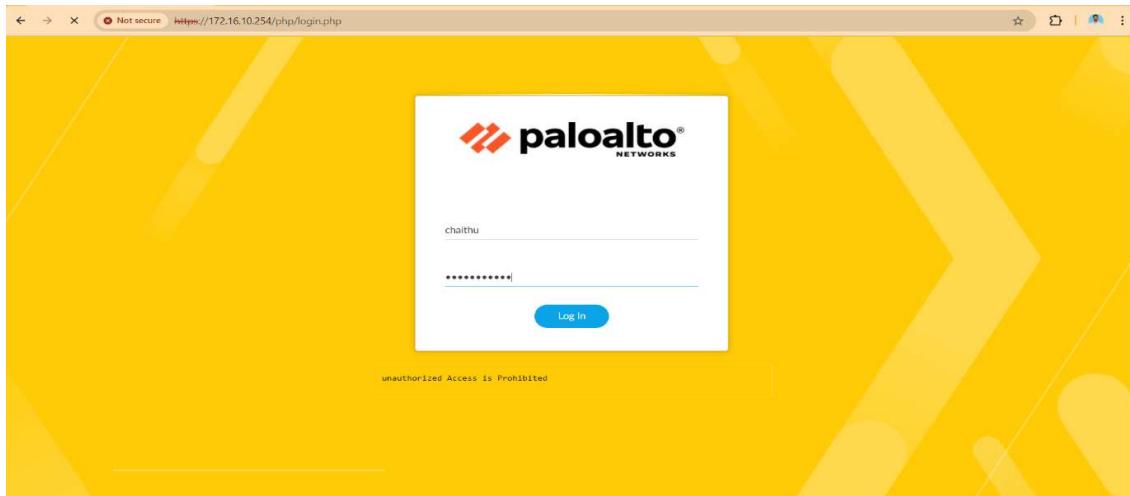
3. Configuring Zones, Interfaces, Virtual Router, and Source NAT?

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

PA-VM DASHBOARD ACC

[Not secure https://172.16.10.254/#/network:sys1:network/zones](#)

Zone

Name	Type	INTERFACES	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
Trust Zone	Layer3	ethernet1/1	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	any	none
Untrust Zone	layer3	ethernet1/2	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	any	none

User Identification ACL

Enable User Identification
 INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Users from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Users from these addresses/subnets will not be identified.

Device-ID ACL

Enable Device Identification
 INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Devices from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Devices from these addresses/subnets will not be identified.

[OK](#) [Cancel](#)

PA-VM DASHBOARD ACC

[Not secure https://172.16.10.254/#/network:sys1:network/zones](#)

Zone

Name	Type	INTERFACES	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
Trust Zone	Layer3	ethernet1/1	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	any	none
Untrust Zone	layer3	ethernet1/2	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	any	none

User Identification ACL

Enable User Identification
 INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Users from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Users from these addresses/subnets will not be identified.

Device-ID ACL

Enable Device Identification
 INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Devices from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

[Add](#) [Delete](#)

Devices from these addresses/subnets will not be identified.

[OK](#) [Cancel](#)

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

[Not secure https://172.16.10.254/#/network:sys1:network/zones](#)

Zone

Name	Type	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
Trust Zone	layer3	ethernet1/1	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
Untrust Zone	layer3	ethernet1/2	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none

B. Configure Network Interfaces

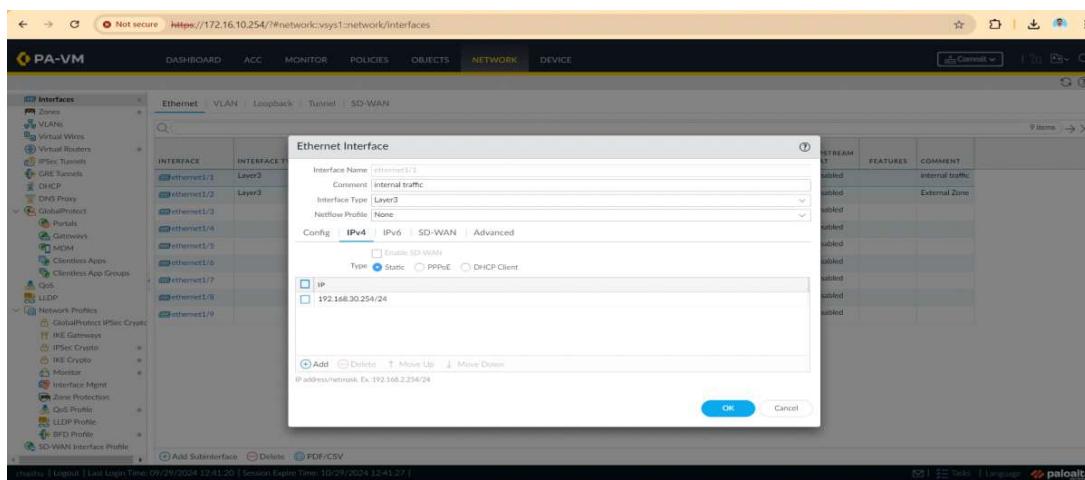
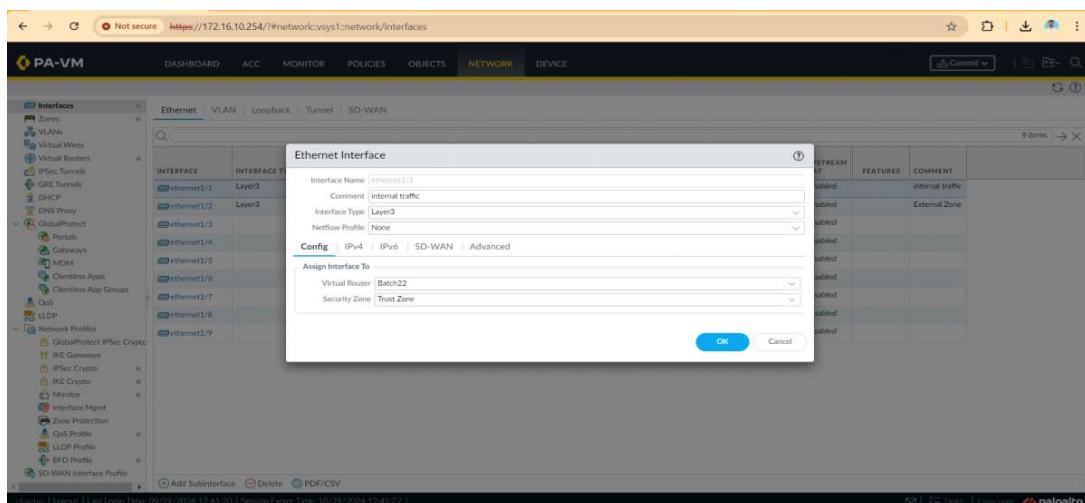
Assign the firewall's physical interfaces to the zones you created.

1. Navigate to the Interfaces:

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

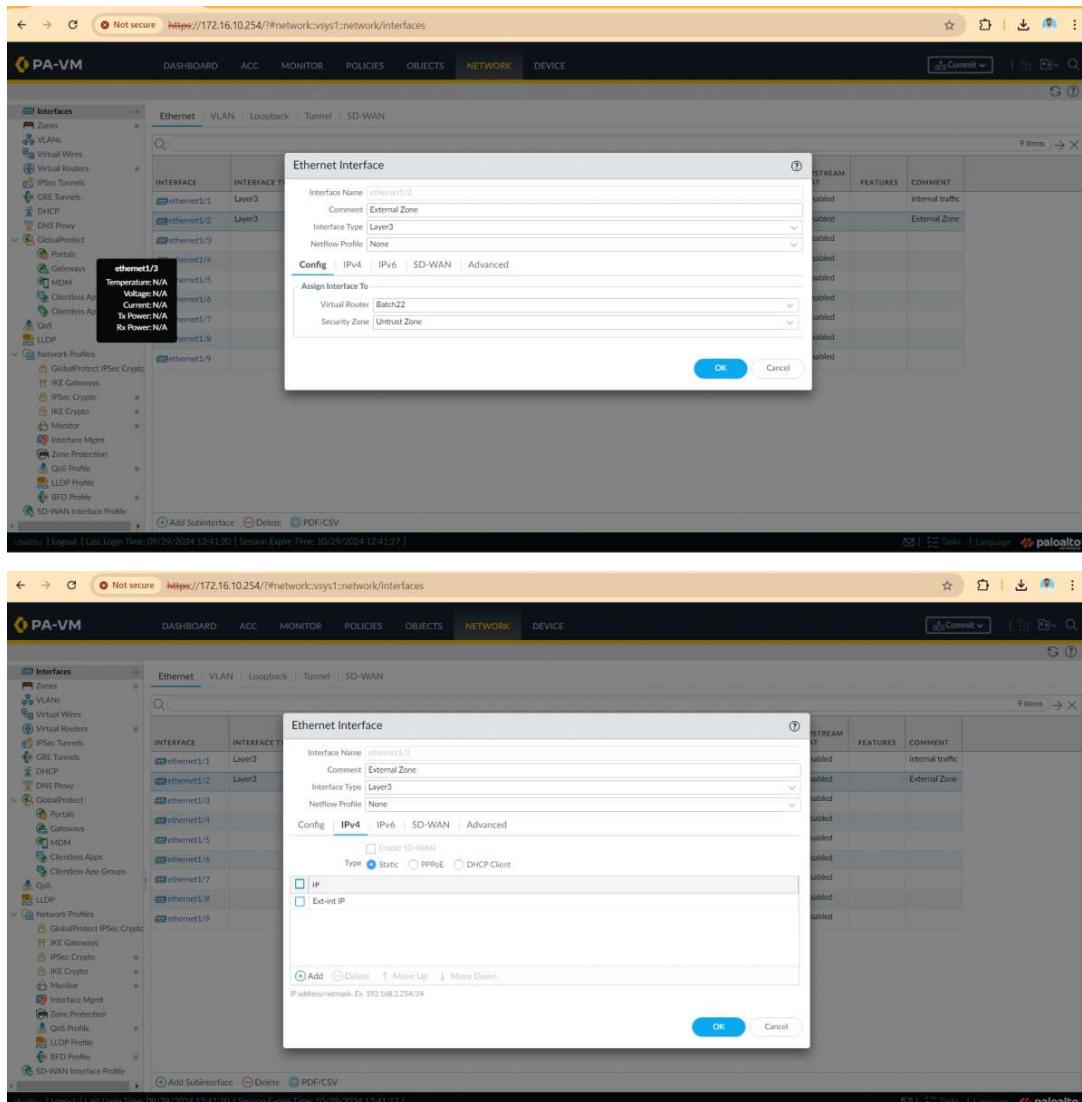
2. Configure External (WAN) Interface:

- 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.

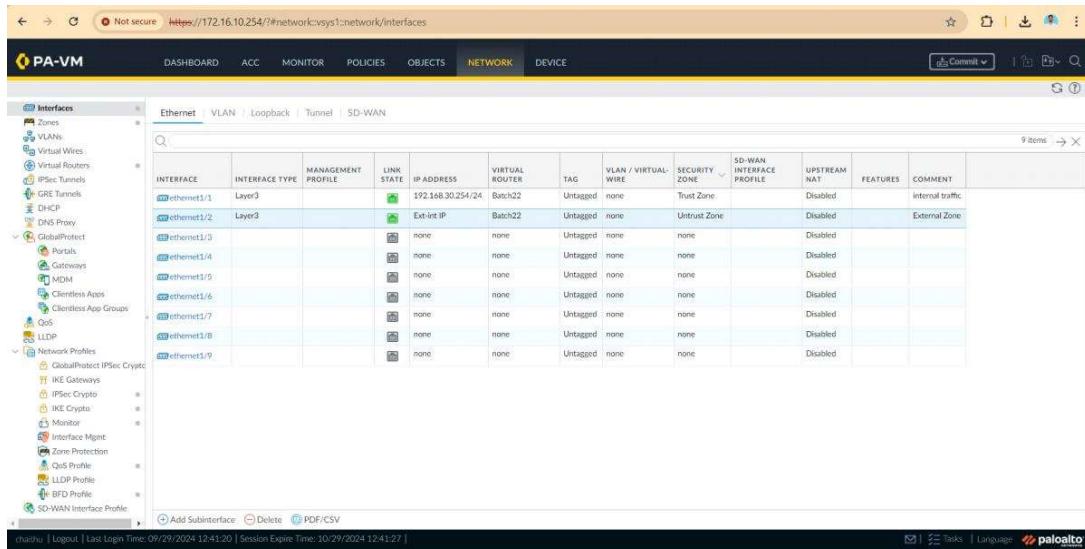


3. Configure Internal (LAN) Interface:

- 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**.



The screenshot shows the Palo Alto Networks PA-VM interface configuration screen. The left sidebar navigation includes: Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, and SD-WAN Interface Profile. The main pane displays the 'Ethernet' tab under 'Interfaces'. A table lists interfaces: ethernet1/3 (selected), ethernet1/4, ethernet1/5, ethernet1/6, ethernet1/7, ethernet1/8, and ethernet1/9. The interface details for ethernet1/3 show it is Layer3, assigned to 'External Zone' (Virtual Router), and 'Internal traffic' (Security Zone). The 'Config' tab is selected, showing the 'IPV4' tab is active. The 'IP' section has 'Type' set to 'Static' and 'IP address/netmask' set to '192.168.2.254/24'. The 'OK' button is visible at the bottom right of the configuration dialog. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (highlighted in yellow), and DEVICE. The bottom status bar shows session information: User: [redacted] Last Login Time: 09/29/2024 12:41:20 Session Expire Time: 10/29/2024 12:41:20, and the paloalto logo.



C. Configure the Virtual Router

A virtual router is responsible for routing traffic between zones.

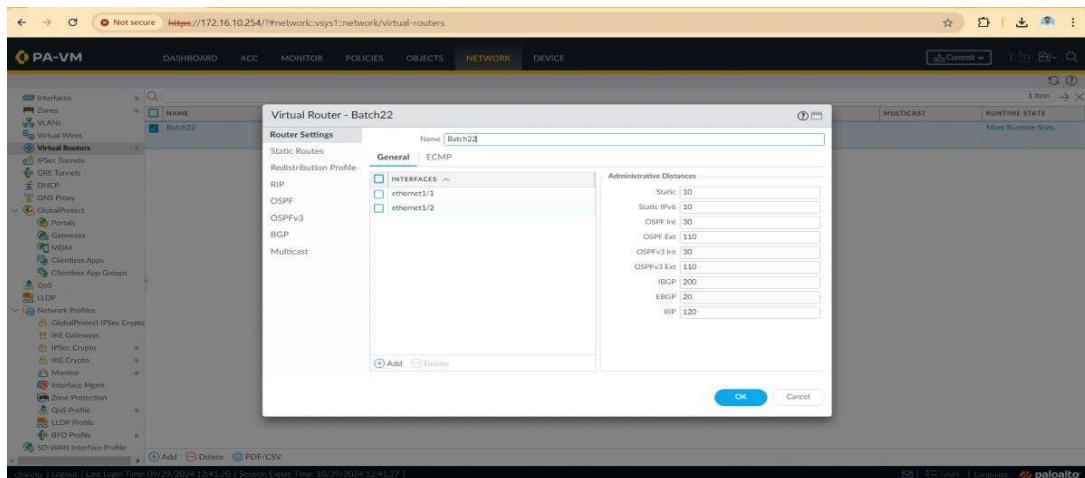
1. Navigate to the Virtual Router:

- 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)

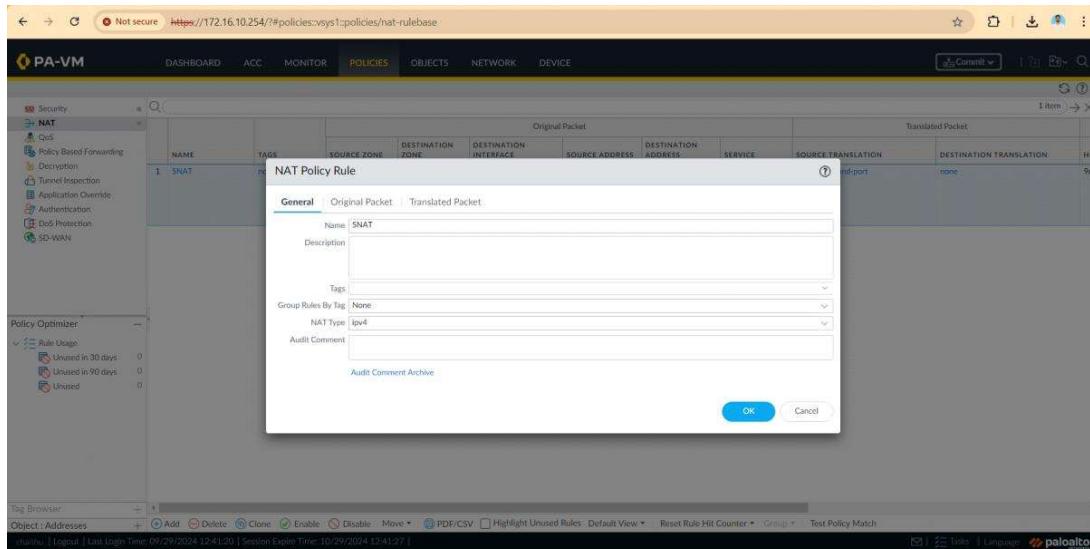


D. Configure Source NAT

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

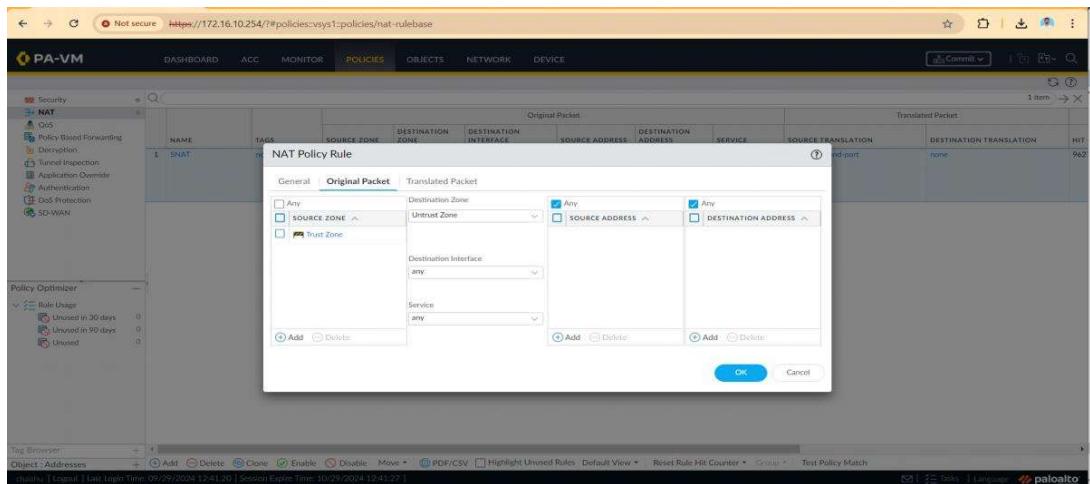
1. Navigate to the NAT Configuration:

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



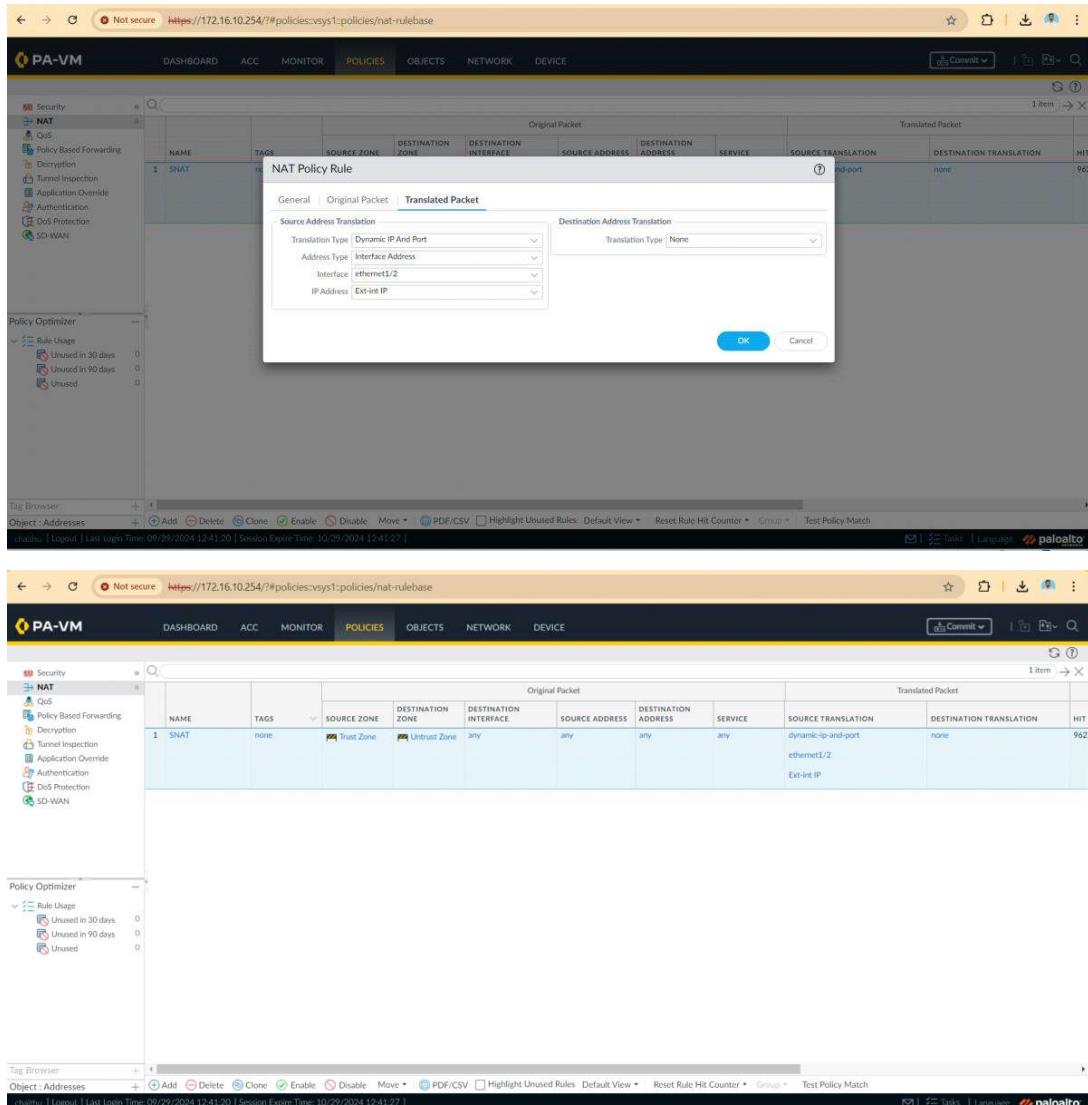
2. Original Packet Tab:

- **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.**



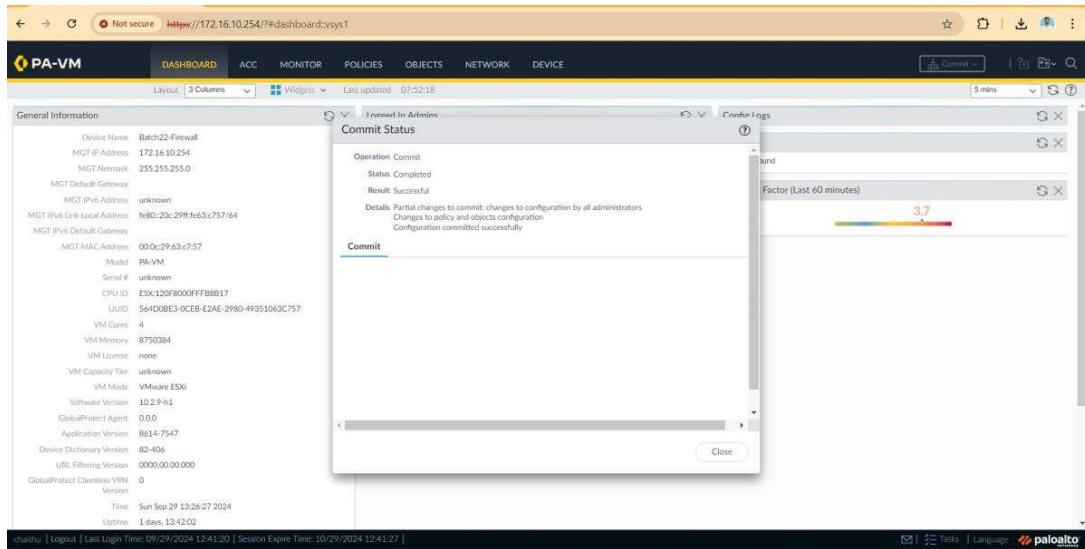
NAME	TAGS	Original Packet				Translated Packet				HIT
		SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	
1 SNAT	none	Trust Zone	Untrust Zone	any	any	any	any	dynamic-ip-and-port	none	962
								ethernet1/2		
								Ext-int IP		

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