

ASSIGNMENT

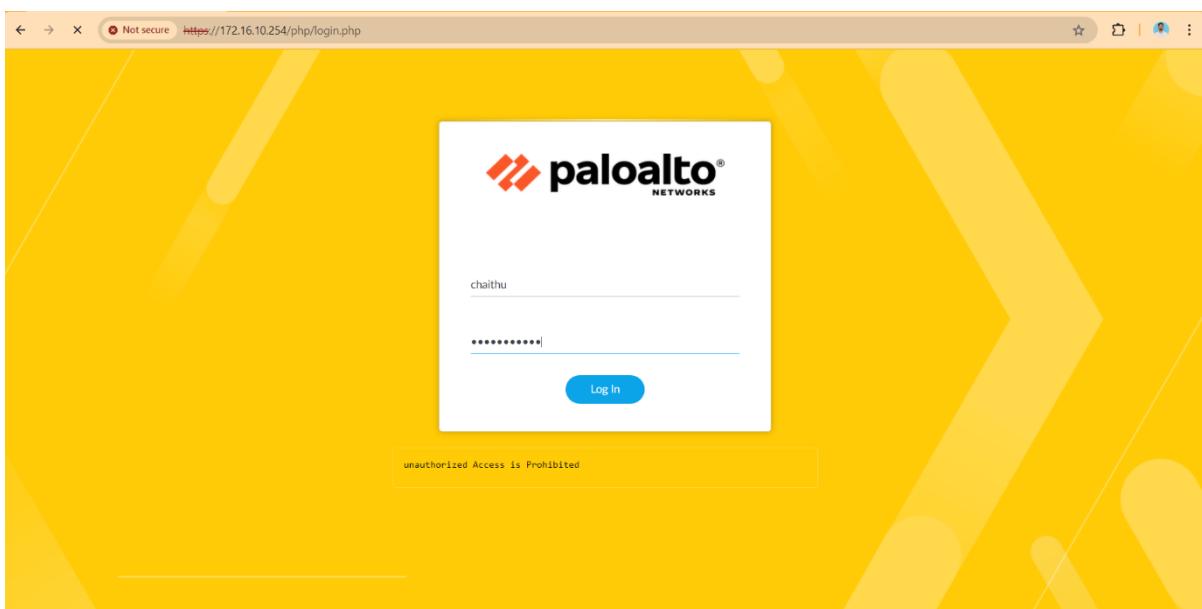
COURSE	PAN Firewall	ASSIGNMENT NO	4
MODULE	Firewall	ASSIGNMENT DATE	28-Sep-24
STUDENT NAME	Konganti Chaithanya Kumar	SUBMIT DATE	29-Sep-24

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:

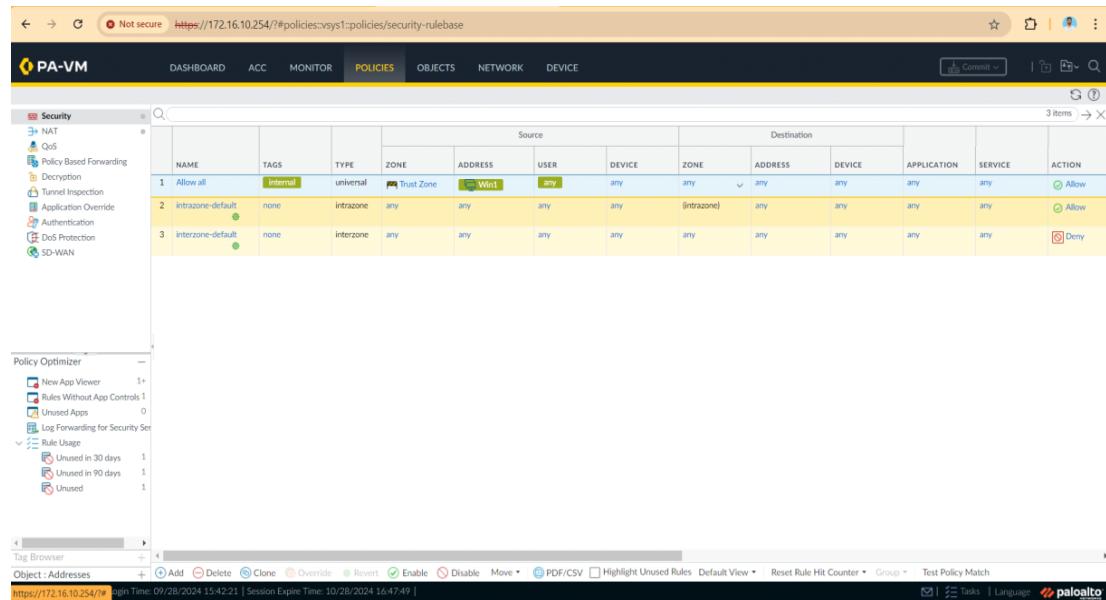
1. Log in to the Palo Alto Firewall:

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



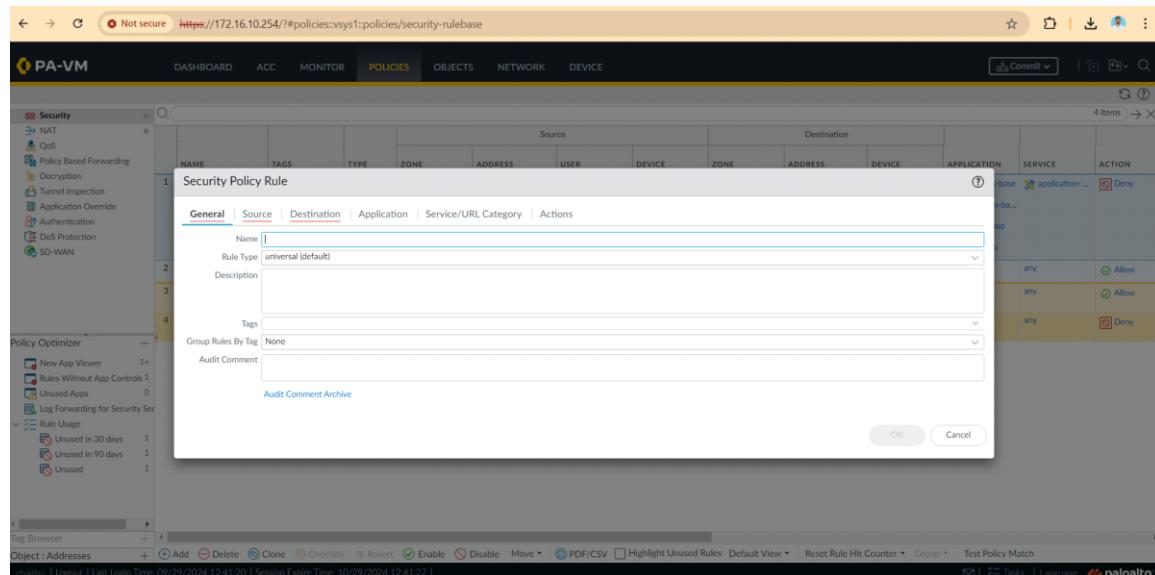
2. Navigate to the Security Policy:

- 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:

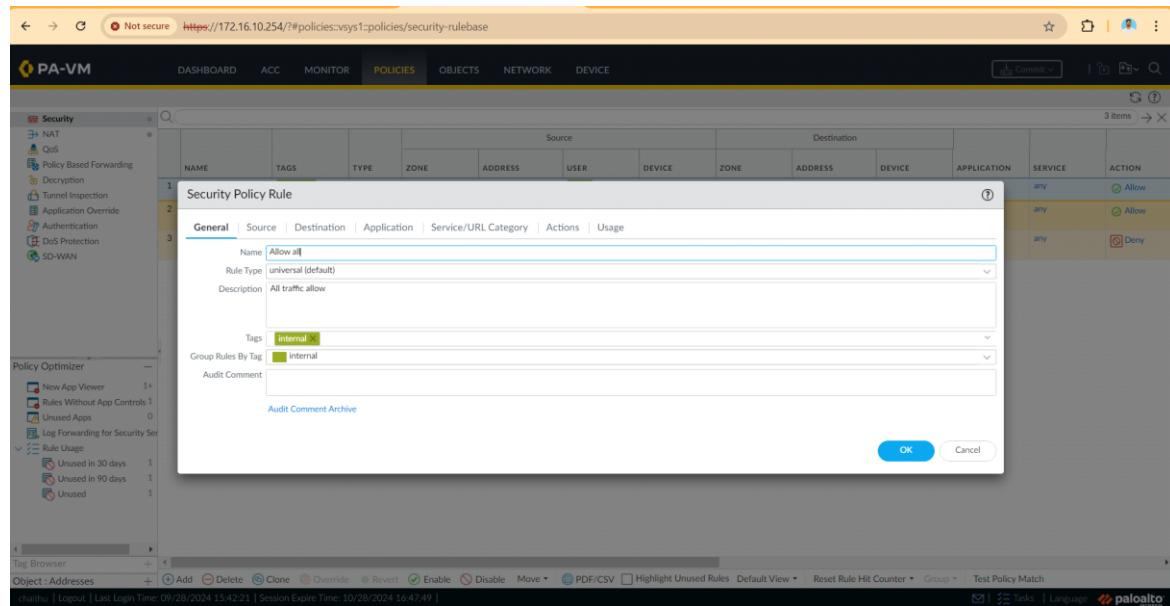
- Click the **Add** button at the bottom of the **Security Policies** list.
- This will open the security policy editor where you can define the rules for accessing the internet from the internal network.



4. Configure the Policy:

Name the Policy:

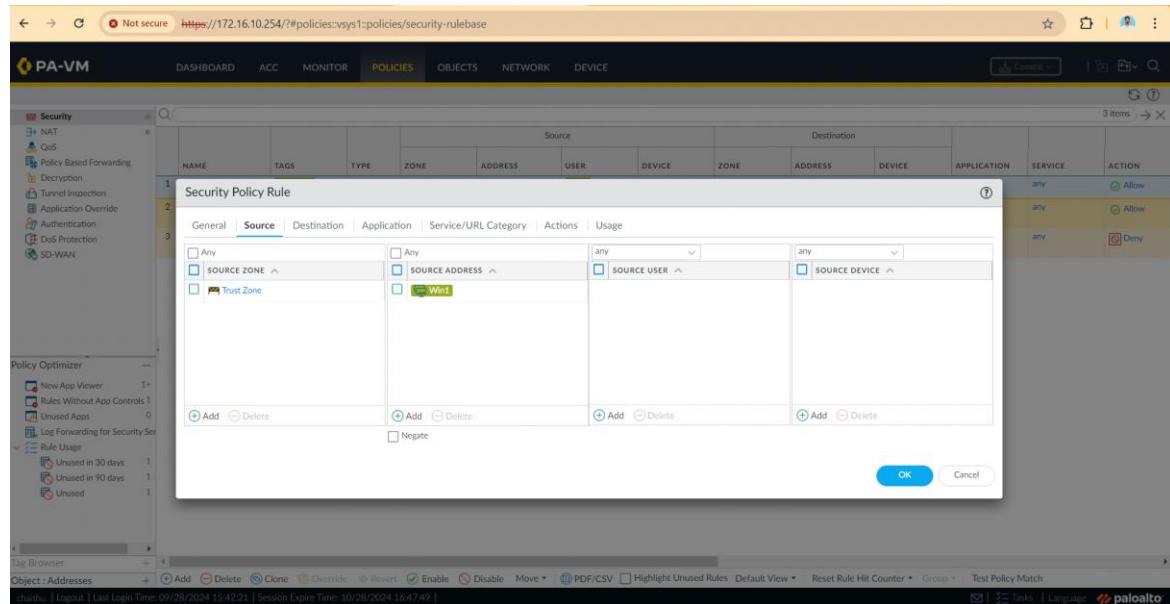
- In the **General** tab, provide a descriptive name for the policy such as **Allow-Internet**.
- Add a description for clarity like "**Allow all**".



The screenshot shows the Palo Alto Networks PA-VM interface. In the top navigation bar, the 'POLICIES' tab is selected. On the left sidebar, under the 'Security' section, 'Policy Based Forwarding' is expanded, showing options like NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DDoS Protection, and SD-WAN. Below this, 'Policy Optimizer' and 'Rule Usage' sections are visible. The main content area displays a table titled 'Security Policy Rule' with three items. The first item, 'Allow all', is currently selected. The 'General' tab is active, showing the rule name 'Allow all', rule type 'universal (default)', and description 'All traffic allow'. The 'Source' tab is also visible. The 'Tags' field contains 'internal'. The 'Audit Comment' field is empty. The 'ACTION' column shows 'Allow' for the first item. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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).



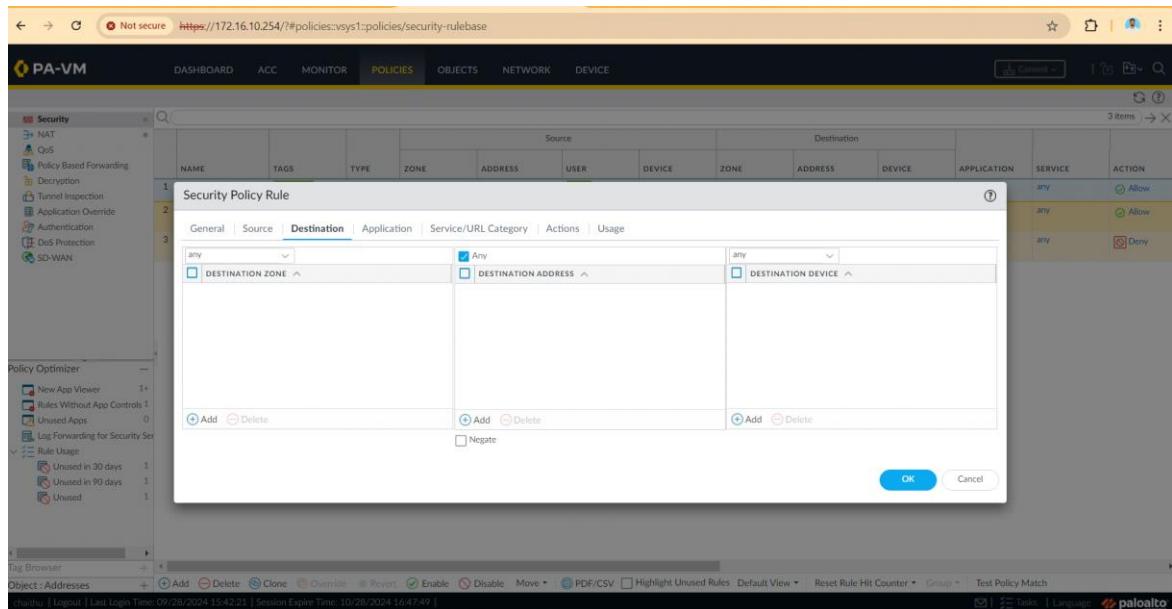
This screenshot shows the configuration of the 'Allow all' security policy rule. The 'Source' tab is selected, showing the following settings:

- Source Zone: Any
- Source Address: Any
- Source User: any
- Source Device: any

 The 'Destination' tab is also visible. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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.



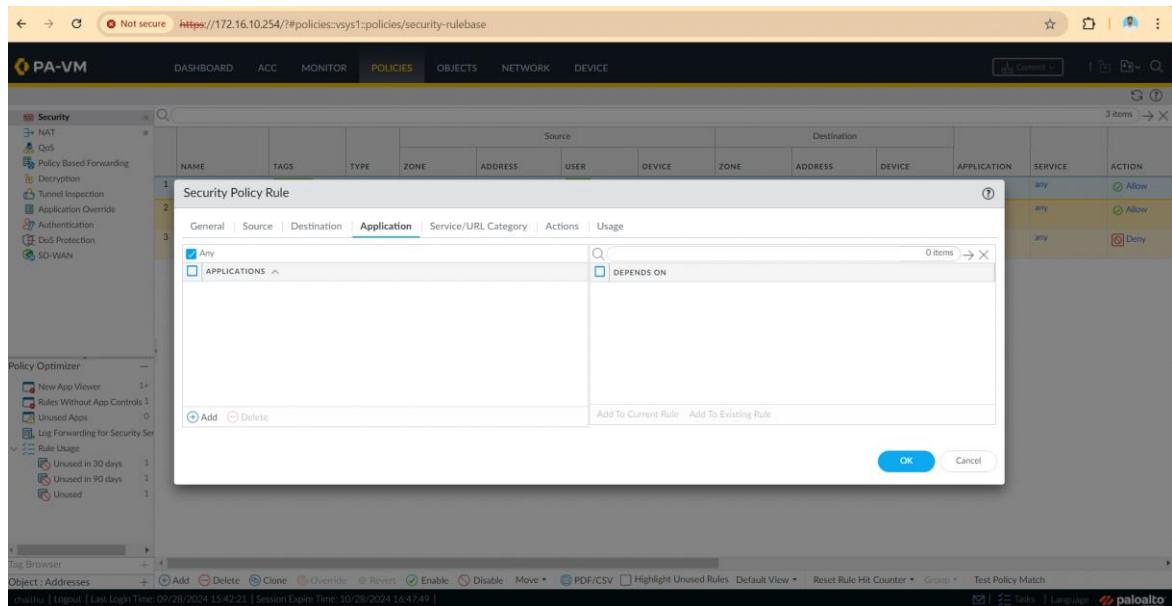
The screenshot shows the Palo Alto Networks Policy Manager interface. The main window displays a table titled "Security Policy Rule" with columns for Name, Tags, Type, Zone, Source, Destination, Application, Service, and Action. The "Destination" tab is selected. In the "Destination" section, there are three rows of rules:

- Row 1: Any → Any → Any (Allow)
- Row 2: Any → Any → Any (Allow)
- Row 3: Any → Any → Any (Deny)

Below the table, there are buttons for Add, Delete, and OK.

Application Tab:

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



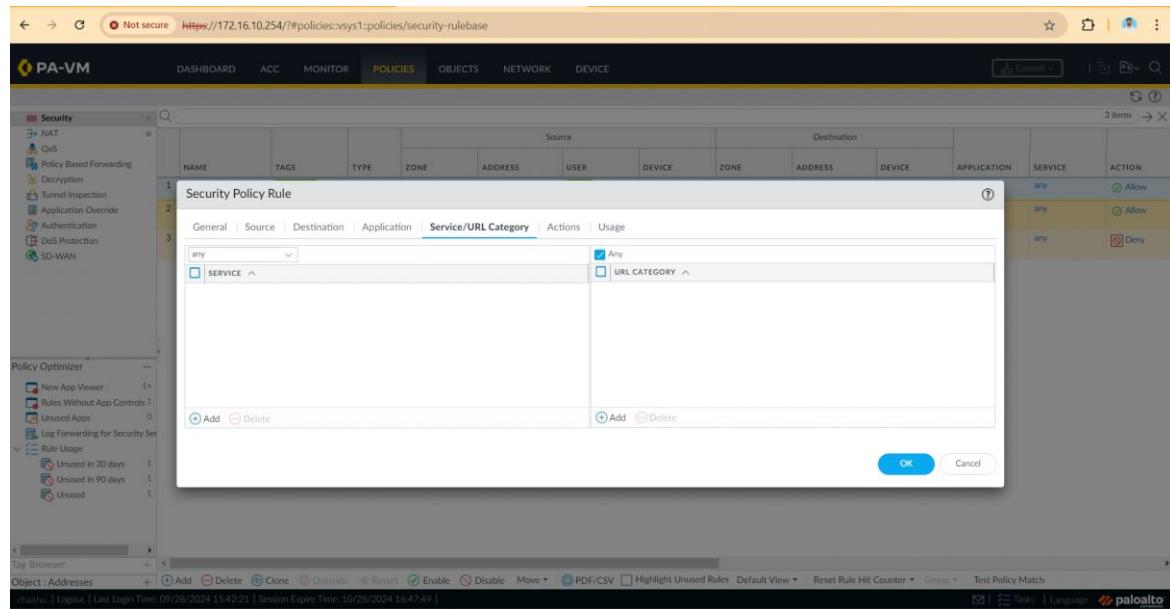
The screenshot shows the Palo Alto Networks Policy Manager interface. The main window displays a table titled "Security Policy Rule" with columns for Name, Tags, Type, Zone, Source, Destination, Application, Service, and Action. The "Application" tab is selected. In the "APPLICATION" section, there is one row of rules:

- Row 1: Any → Any → Any (Allow)
- Row 2: Any → Any → Any (Allow)
- Row 3: Any → Any → Any (Deny)

Below the table, there are buttons for Add, Delete, and OK.

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).



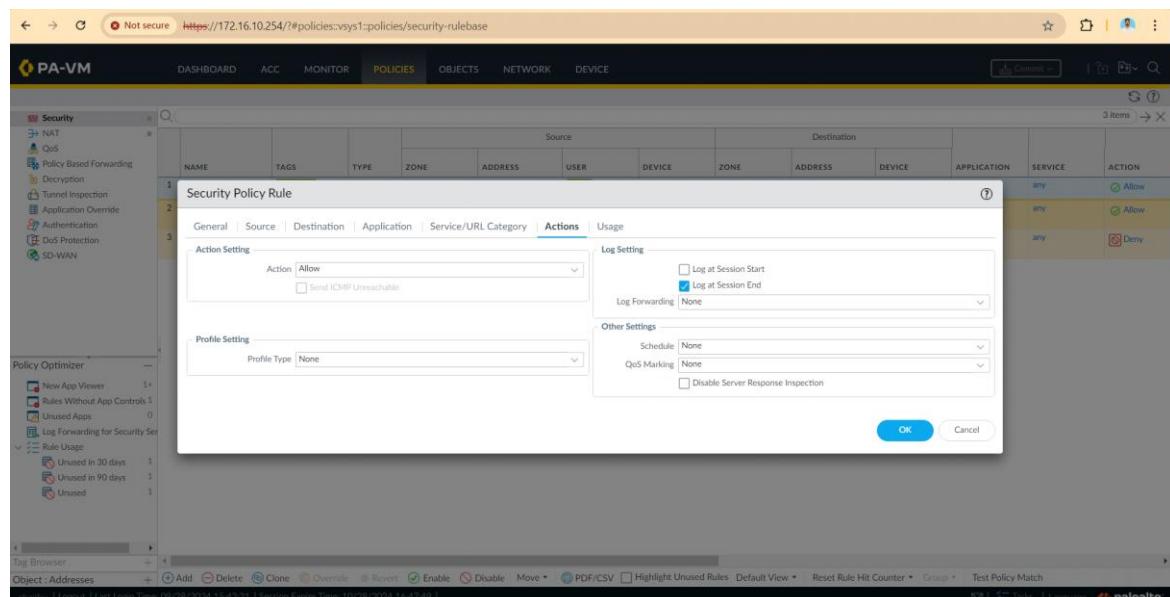
The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The POLICIES tab is selected. On the left, a sidebar lists various security features like NAT, QoS, and Policy Based Forwarding. The main panel displays a table for 'Security Policy Rule'. The 'Service/URL Category' tab is active. It contains three entries:

- 1: Any - Allow
- 2: Any - Allow
- 3: Any - Deny

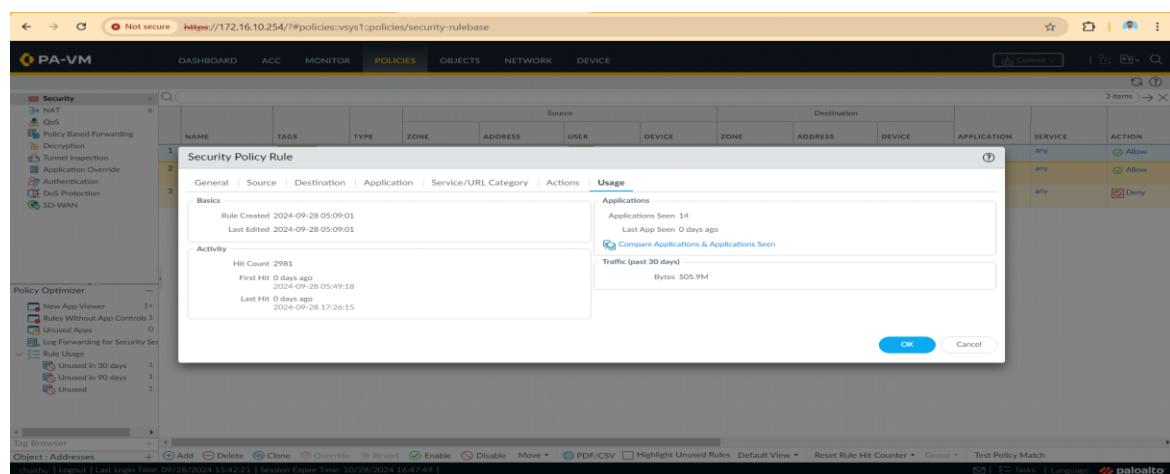
At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Action:

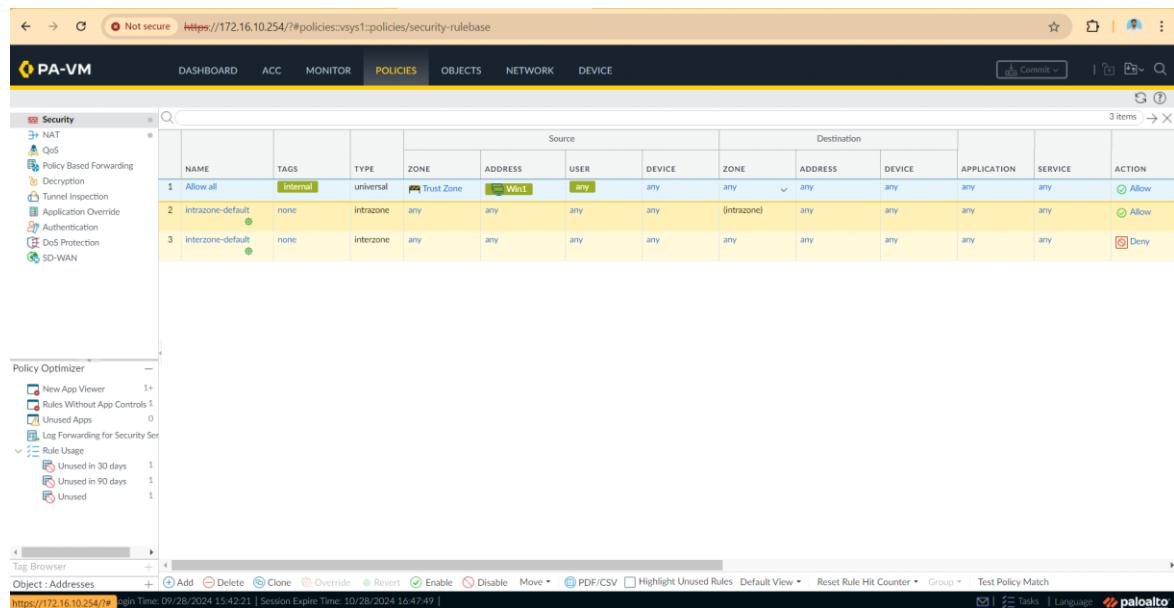
- In the Action tab, set the Action to Allow.



The screenshot shows the 'Actions' tab of the Security Policy Rule dialog. The 'Action Setting' section is open, showing 'Action: Allow' and 'Send ICMP Unreachable' checked. Other sections include 'Log Setting' (with 'Log at Session End' checked), 'Profile Setting' (with 'Profile Type: None'), and 'Other Settings' (with 'Schedule: None' and 'QoS Marking: None'). At the bottom are 'OK' and 'Cancel' buttons.



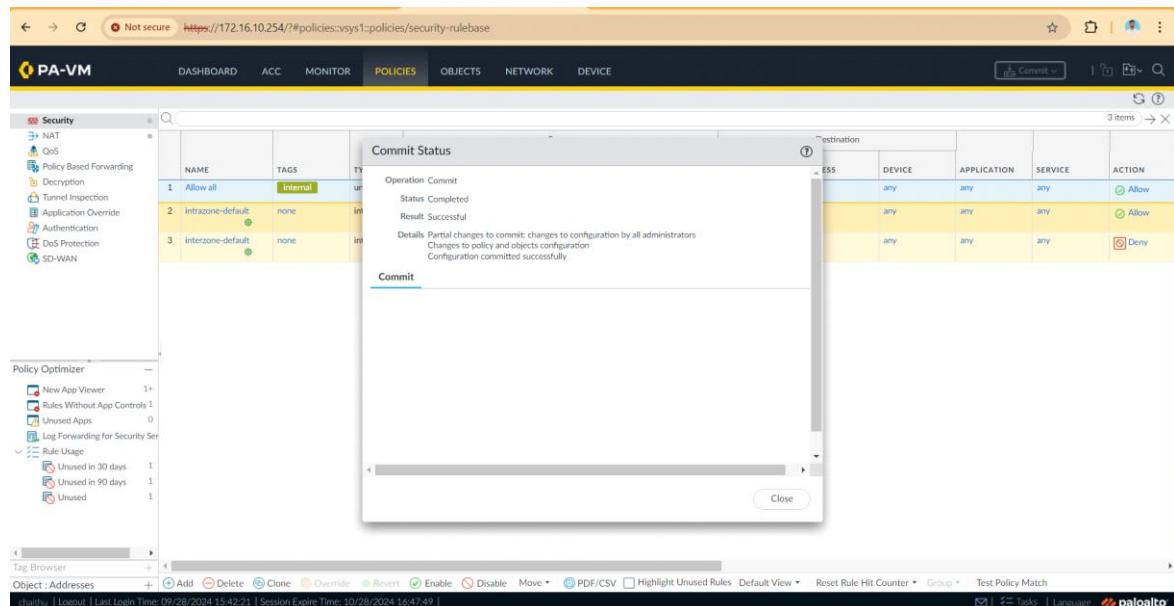
The screenshot shows the 'Usage' tab of the Security Policy Rule dialog. The 'Basics' section displays creation and edit times. The 'Activity' section shows a hit count of 2981, first hit on 2024-09-28 05:49:18, last hit on 2024-09-28 17:26:15, and traffic statistics for the past 30 days (Bytes: 505.9M). At the bottom are 'OK' and 'Cancel' buttons.



NAME	TAGS	TYPE	ZONE	Source			Destination			APPLICATION	SERVICE	ACTION
				ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1 Allow all	internal	universal	Trust Zone	Win1	any	any	(inzone)	any	any	any	any	Allow
2 intrazone-default	none	intrazone	any	any	any	any	any	any	any	any	any	Allow
3 interzone-default	none	interzone	any	any	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.



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

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.

Not secure https://172.16.10.254/?#policies:vsys1:policies/security-rulebase

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE Commit

Security

- DNAT
- QoS
- Policy Based Forwarding
- Decryption
- Tunnel Inspection
- Application Override
- Authentication
- Dos Protection
- SD-WAN

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1 Block-Apps	internal	universal	Trust Zone	Wan1	any	any	Untrust Zone	any	any	facebook-base	application...	Deny	
2 Allow all	internal	universal	Trust Zone	Wan1	any	any	Untrust Zone	any	any	Instagram-ba...		Allow	
3 Intra-zone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	netflix-base		Allow	
4 Inter-zone-default	none	interzone	any	any	any	any	any	any	any	whatsapp		Deny	

Policy Optimizer

- New App Viewer
- Search App Controls
- Unused Apps
- Log Forwarding for Security Services
- Rule Usage
 - Unused in 30 days 1
 - Unused in 90 days 1
 - Unused 1

Tag Browser

Object : Addresses Add Delete Clone Override Revert Enable Disable Move PDF/CSV Highlight Unused Rules Default View Reset Rule Hit Counter Group Test Policy Match

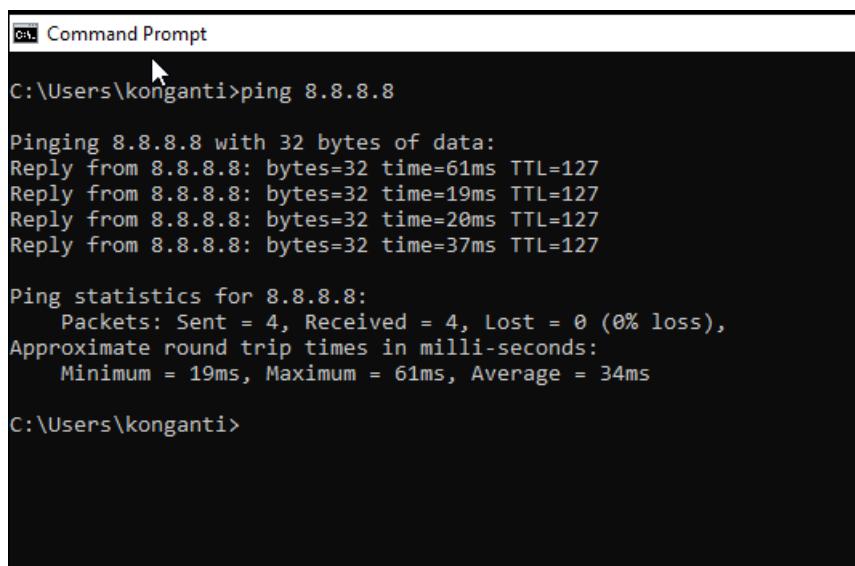
Ping and Web Access Test:

- 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:

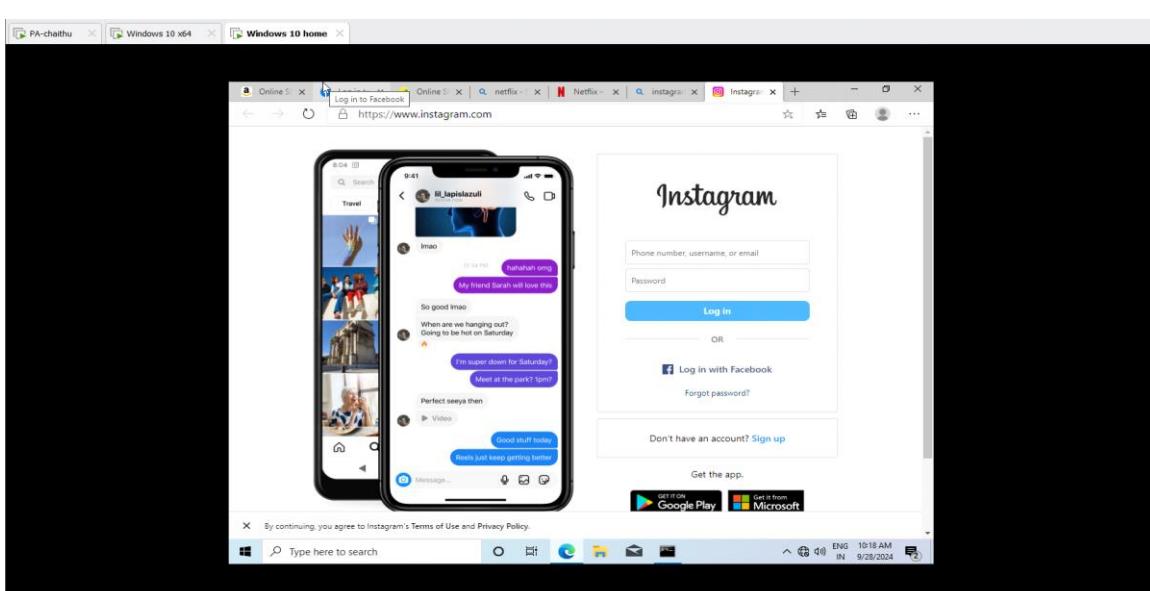
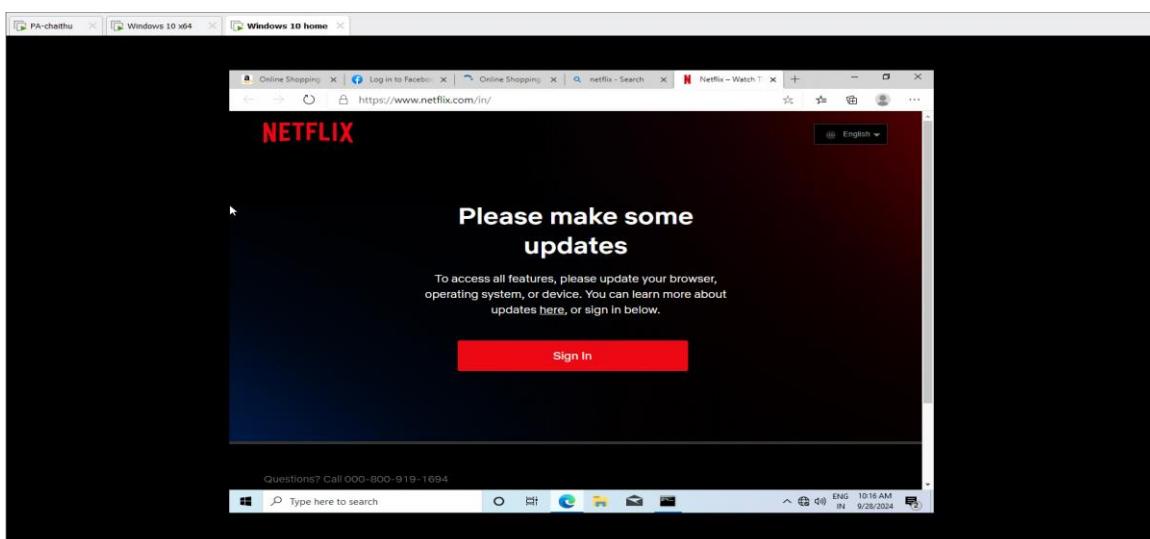
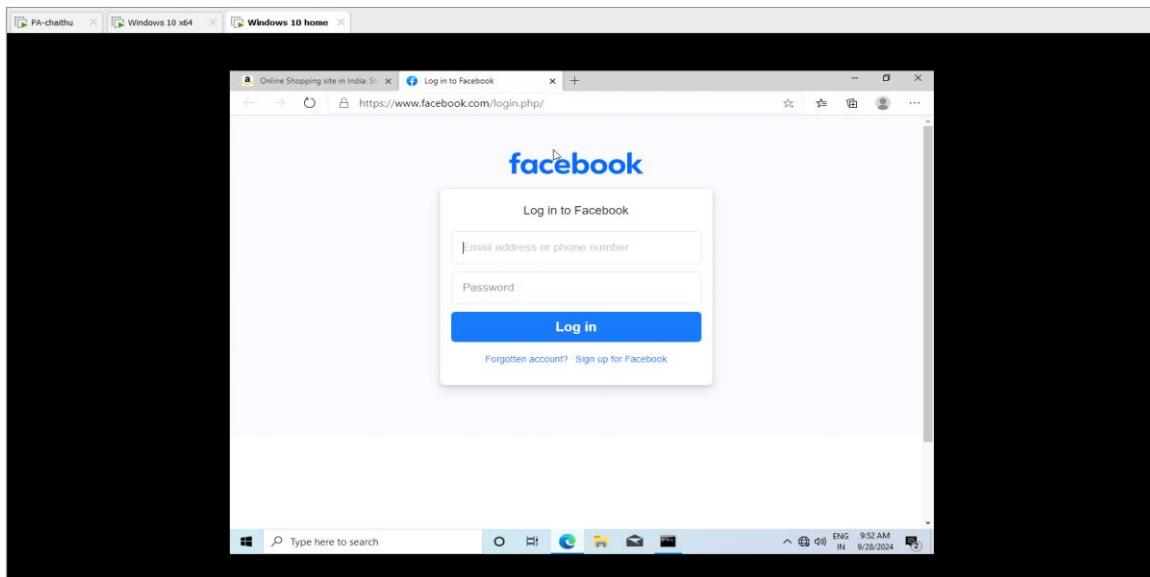
Steps to Check Internet Access with Webpages:

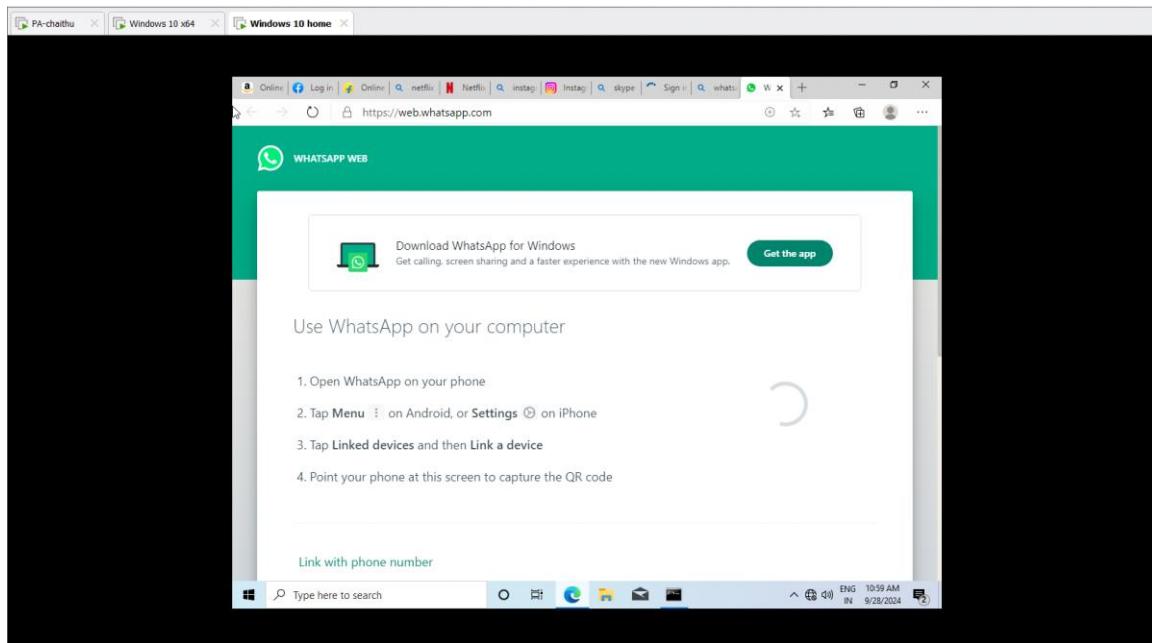
1. Webpage Access Test (Allow Internet Access):

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:

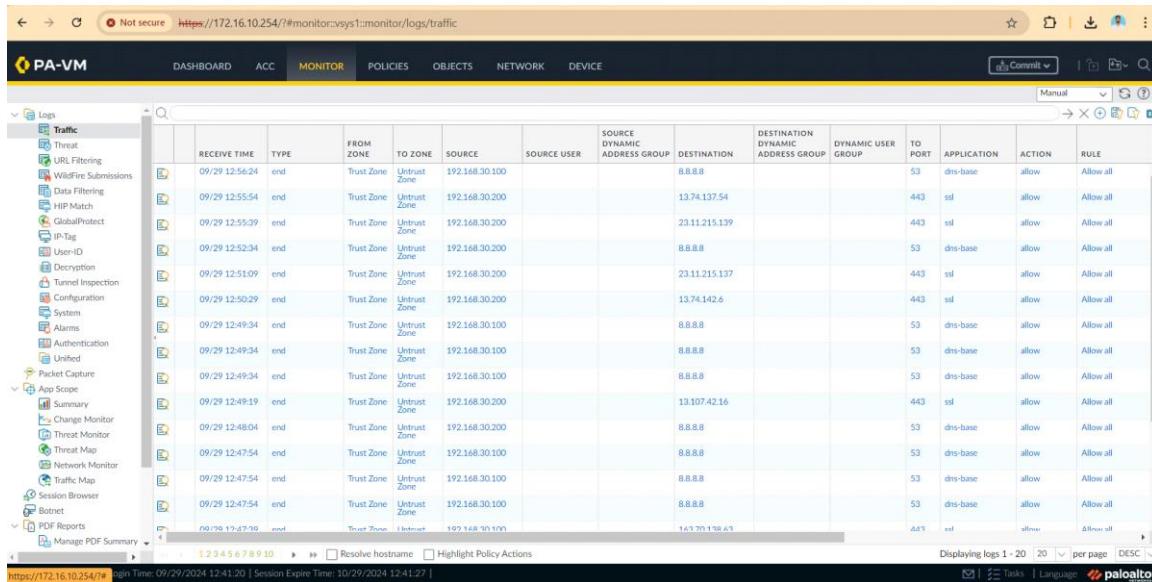




Verifying Traffic on Palo Alto Firewall:

- 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:



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	RULE
09/29 12:56:24	end	Trust Zone	Untrust Zone	192.168.30.100		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:55:54	end	Trust Zone	Untrust Zone	192.168.30.200		13.74.137.54				443	ssl	allow	Allow all
09/29 12:55:39	end	Trust Zone	Untrust Zone	192.168.30.200		23.11.215.139				443	ssl	allow	Allow all
09/29 12:52:34	end	Trust Zone	Untrust Zone	192.168.30.200		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:51:09	end	Trust Zone	Untrust Zone	192.168.30.200		23.11.215.137				443	ssl	allow	Allow all
09/29 12:50:29	end	Trust Zone	Untrust Zone	192.168.30.200		13.74.142.6				443	ssl	allow	Allow all
09/29 12:49:34	end	Trust Zone	Untrust Zone	192.168.30.100		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:49:34	end	Trust Zone	Untrust Zone	192.168.30.100		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:49:34	end	Trust Zone	Untrust Zone	192.168.30.100		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:49:19	end	Trust Zone	Untrust Zone	192.168.30.200		13.107.42.16				443	ssl	allow	Allow all
09/29 12:48:04	end	Trust Zone	Untrust Zone	192.168.30.200		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:47:54	end	Trust Zone	Untrust Zone	192.168.30.100		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:47:54	end	Trust Zone	Untrust Zone	192.168.30.100		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:47:54	end	Trust Zone	Untrust Zone	192.168.30.100		8.8.8.8				53	dns-base	allow	Allow all
09/29 12:47:54	end	Trust Zone	Untrust Zone	192.168.30.100		14.9.70.198.8.9				443	ed	allow	Allow all

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:

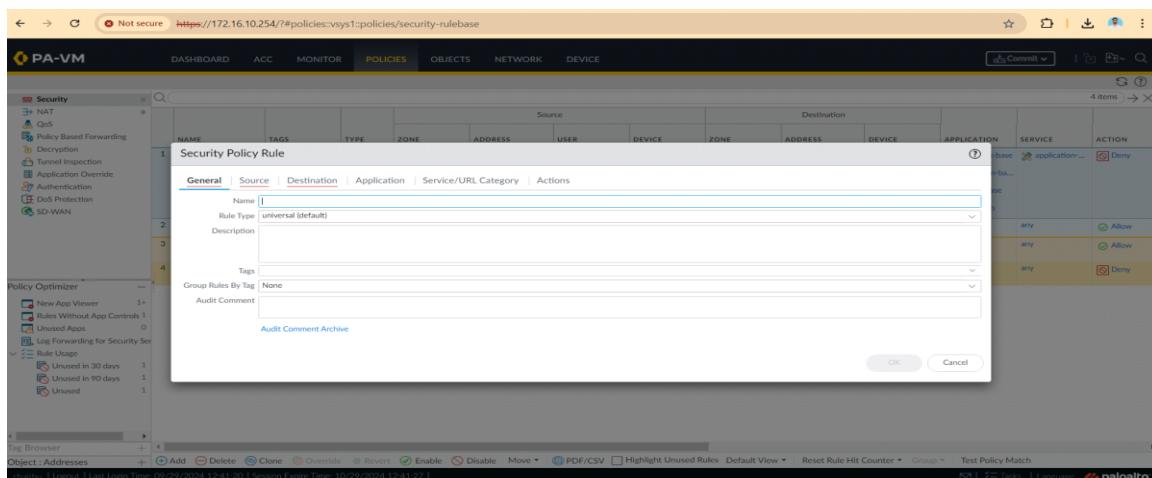
1. Login to Palo Alto Networks Firewall

- 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).



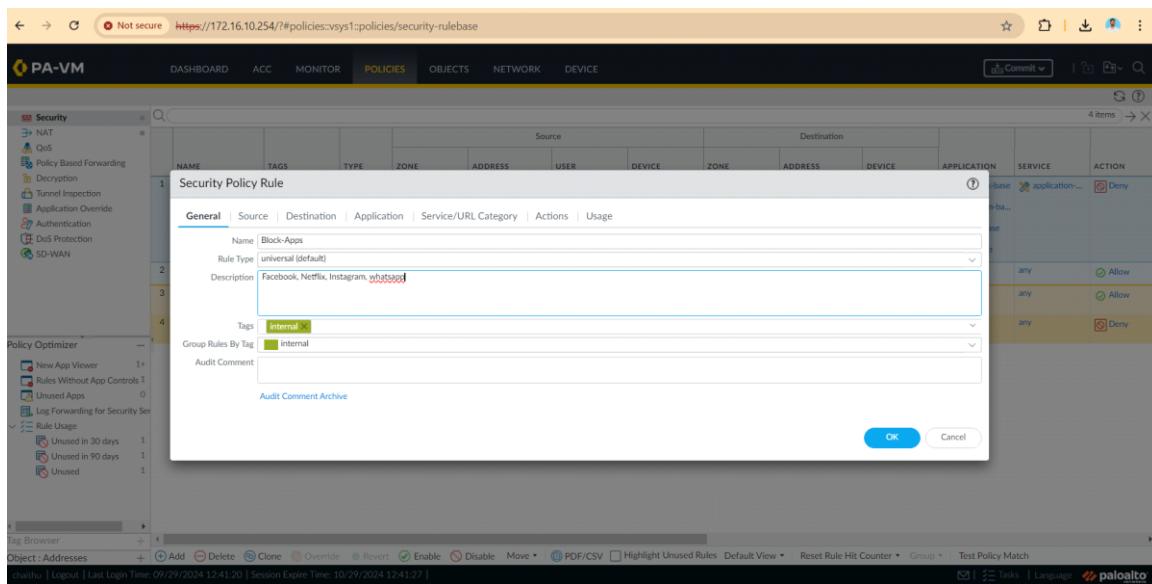
2. Navigate to the Security Policies

- 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**

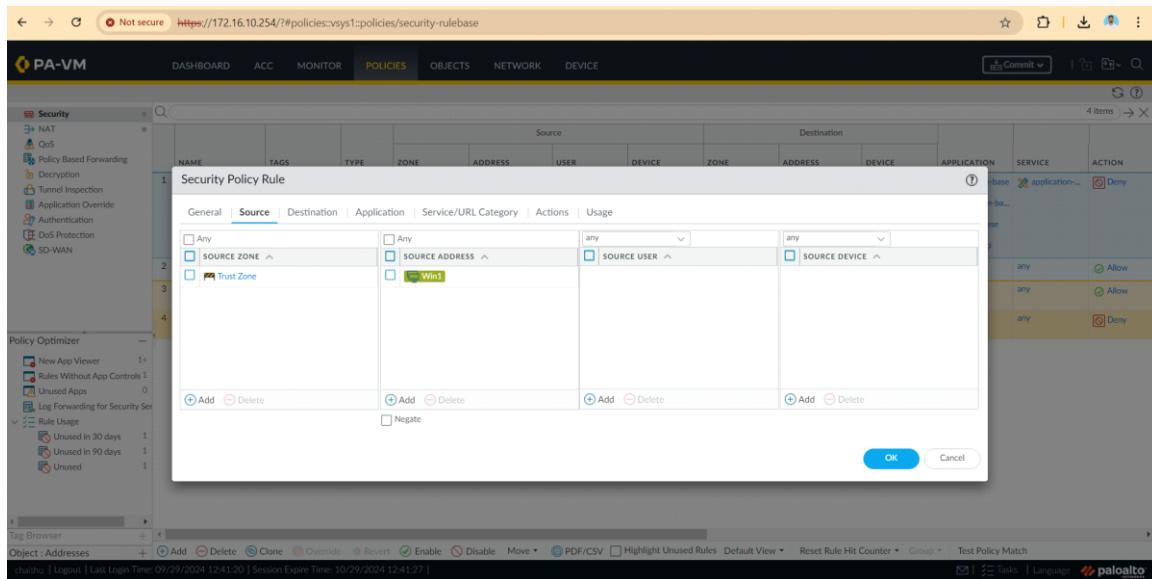


The screenshot shows the Palo Alto Networks PA-VM interface. A modal window titled "Security Policy Rule" is open, showing the "General" tab. The rule is named "Block-Apps" and has a description of "Facebook, Netflix, Instagram, whatsapp". It is tagged as "internal". The rule base is set to "application-based". The rule table contains three entries:

Source	Destination	Action
any	any	Allow
any	any	Allow
any	any	Deny

Source Zone:

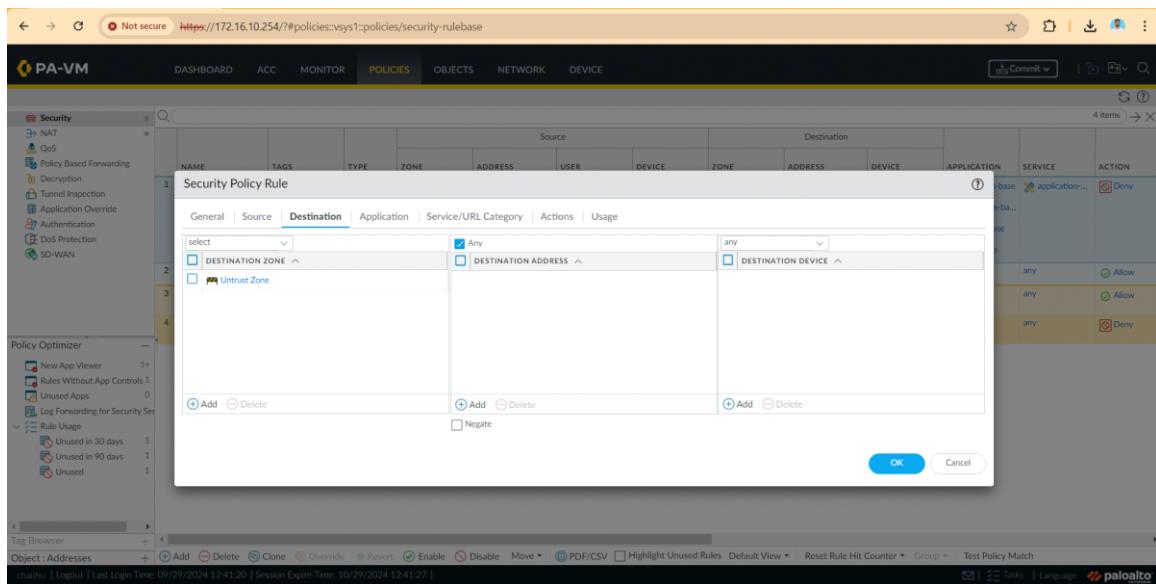
- Define the source zone (**Trust** zone).
- Select internal devices or users as the source.



The screenshot shows the "Source" tab of the "Security Policy Rule" configuration. Under "SOURCE ZONE", the "Trust Zone" is selected. Under "SOURCE ADDRESS", the IP address "Win1" is listed. The "Source" tab also includes fields for "Any", "SOURCE USER", and "SOURCE DEVICE".

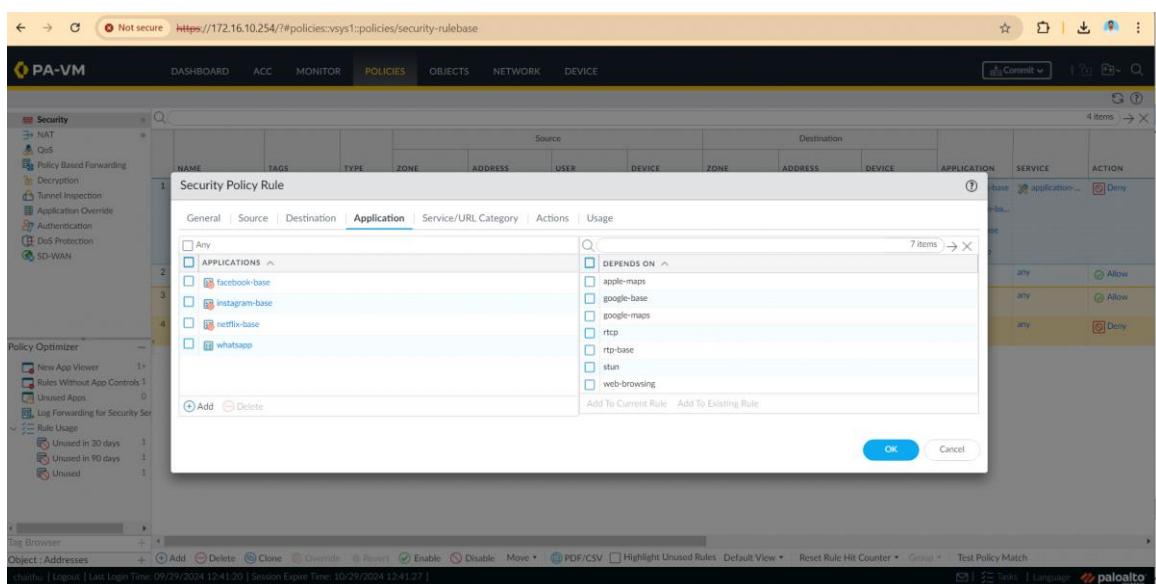
Destination Zone:

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



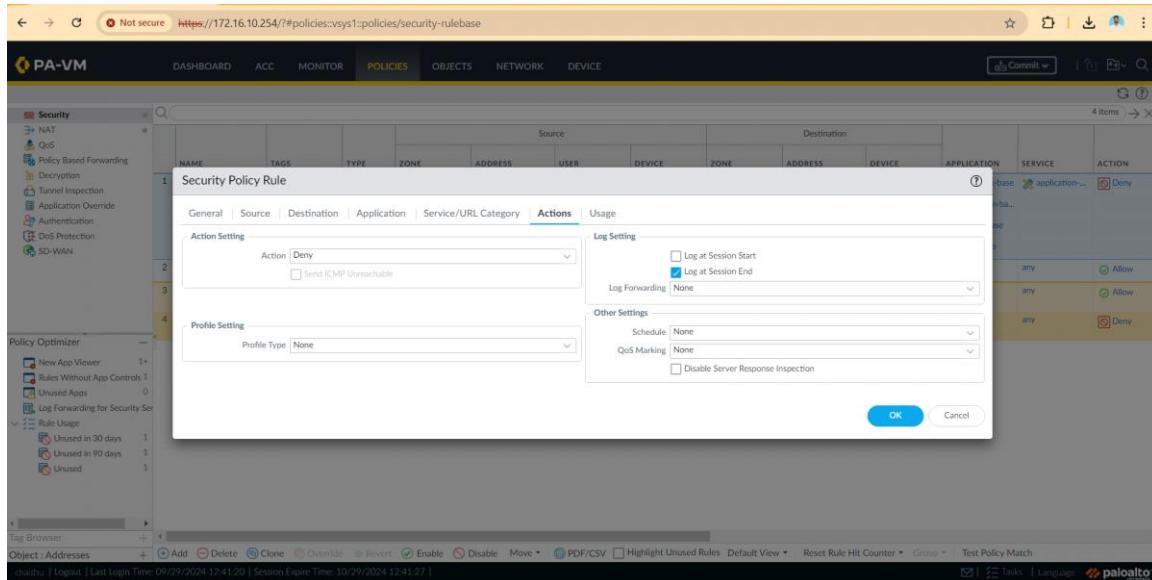
4. Define Applications to Block

- 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.

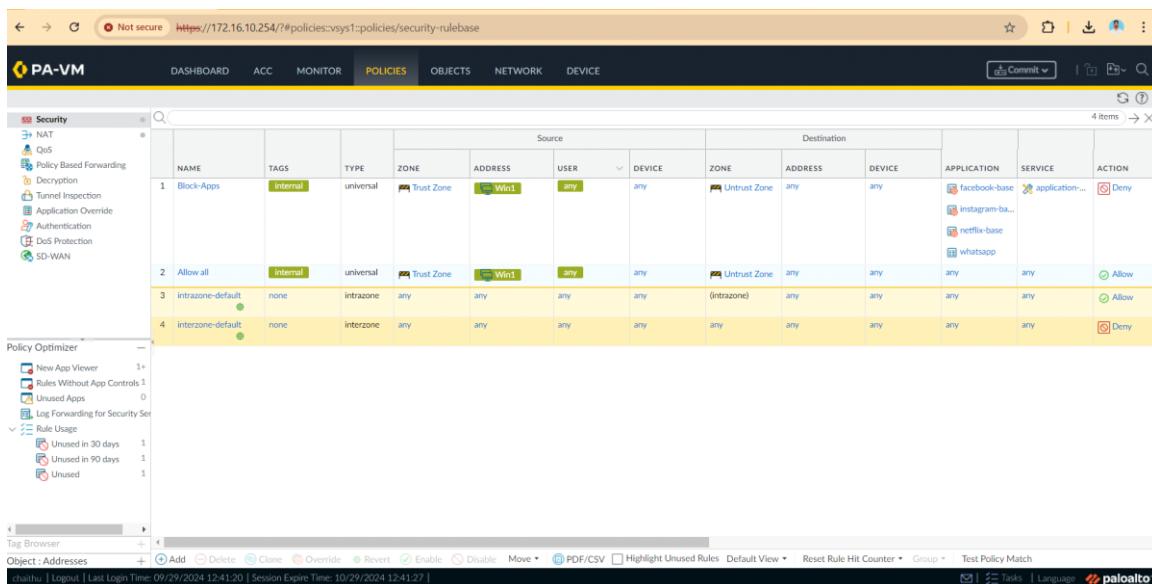


5. Action Configuration

- 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.



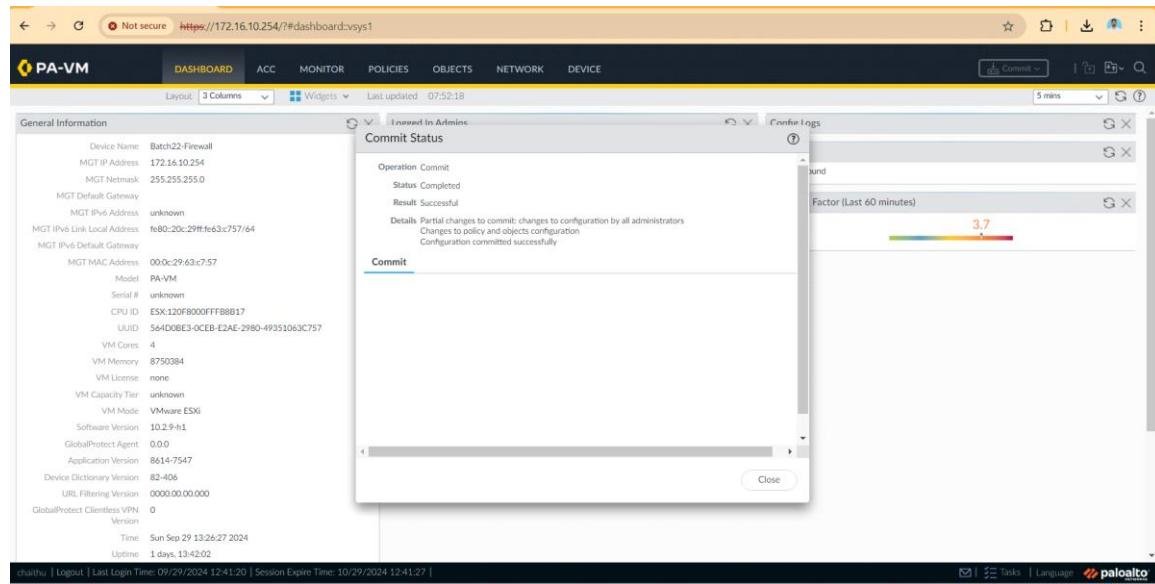
The screenshot shows the Palo Alto Networks UI for configuring a security policy rule. The 'Actions' tab is active, displaying the 'Action' dropdown set to 'Deny'. Other tabs include General, Source, Destination, Application, Service/URL Category, and Usage. The 'Log Setting' section has checkboxes for 'Log at Session Start' and 'Log at Session End', both of which are checked. The 'Profile Setting' section shows 'Profile Type: None'. The main table lists four items, with the last item having its 'ACTION' column set to 'Deny'.



The screenshot shows the list of security policy rules. Rule 1, named 'Block-Apps', is configured to block specific applications (facebook-base, instagram-base, netflix-base, whatsapp) and is set to 'Deny'. Rule 2, named 'Allow all', is set to 'Allow'. Rules 3 and 4 are 'intrazone-default' and 'interzone-default' respectively, both set to 'Allow'. The 'ACTION' column for these rules is also visible.

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.



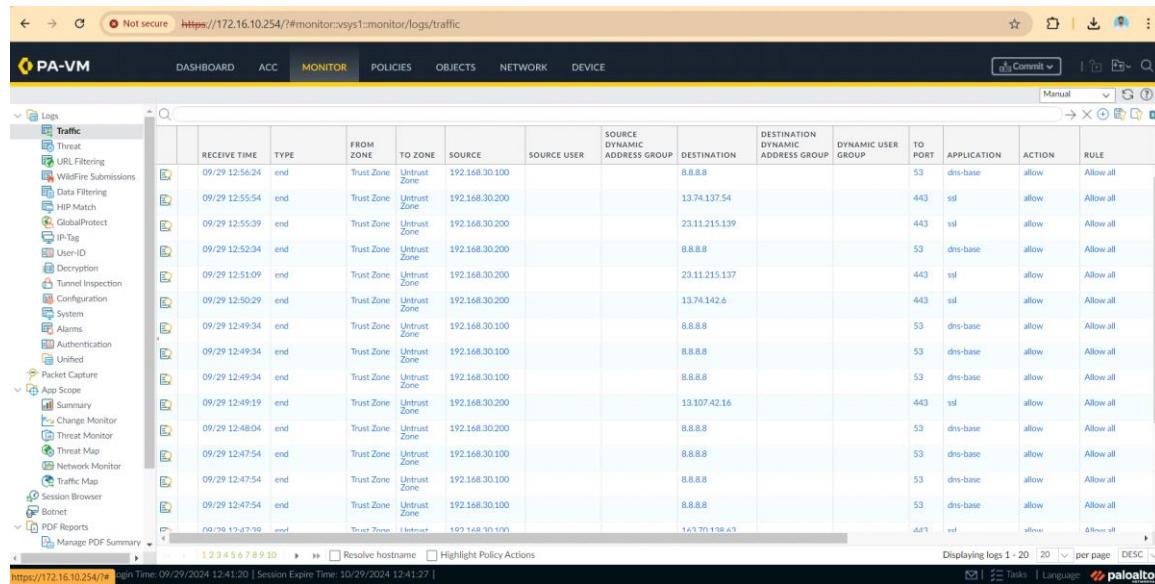
The screenshot shows the PurpleSynapz interface with a 'Commit Status' dialog open. The dialog displays the following information:

- 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.
- Commit:** A button labeled 'Commit'.

The main dashboard area shows general device information for 'PA-VM' including Device Name, MGT IP Address, MGT Netmask, MGT Default Gateway, MGT IPv6 Address, MGT IPv6 Link Local Address, MGT IPv6 Default Gateway, MGT MAC Address, Model, Serial #, CPU ID, UUID, VM Cores, VM Memory, VM License, VM Capacity Tier, VM Mode, Software Version, GlobalProtect Agent, Application Version, Device Dictionary Version, URL Filtering Version, GlobalProtect Clientless VPN Version, and Time. The status bar at the bottom indicates the session is still active.

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 'Logs' section under the 'Traffic' category in the monitor. The table displays the following columns: 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 list various traffic entries, mostly from 'Trust Zone' to 'Untrust Zone' or vice versa, involving IP addresses like 192.168.30.100, 192.168.30.200, and 192.168.30.10. The actions shown are 'allow' or 'allow all' with 'dns-base' as the application. The interface includes a sidebar with other log categories like Threat, URL Filtering, and WildFire Submissions, and a bottom navigation bar with links for Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map, Session Browser, Botnet, PDF Reports, and Manage PDF Summary.

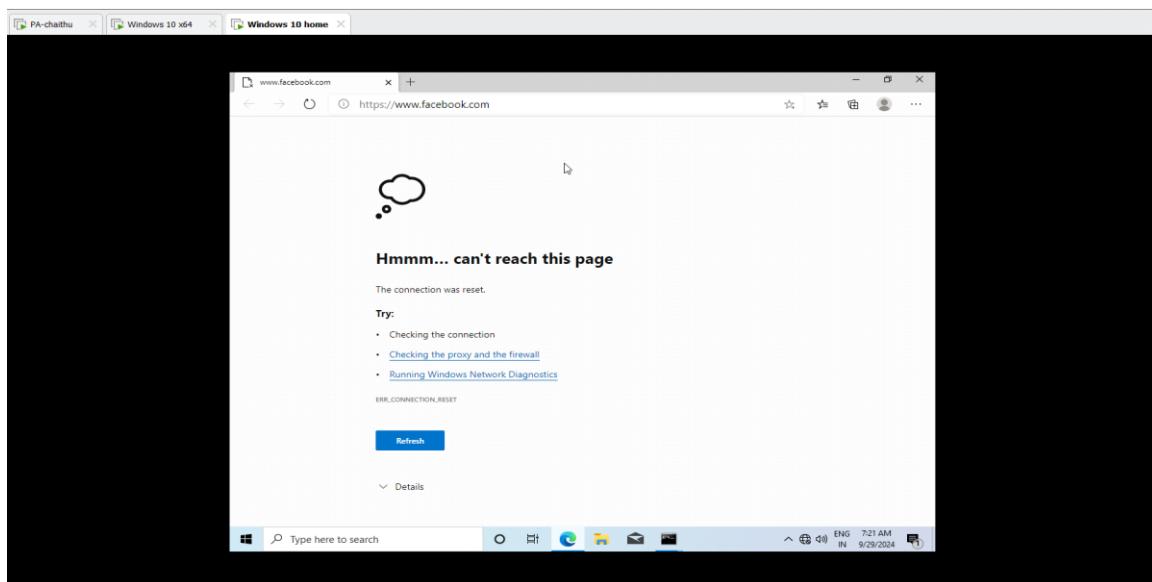
Final Output:

Screenshot Documentation:

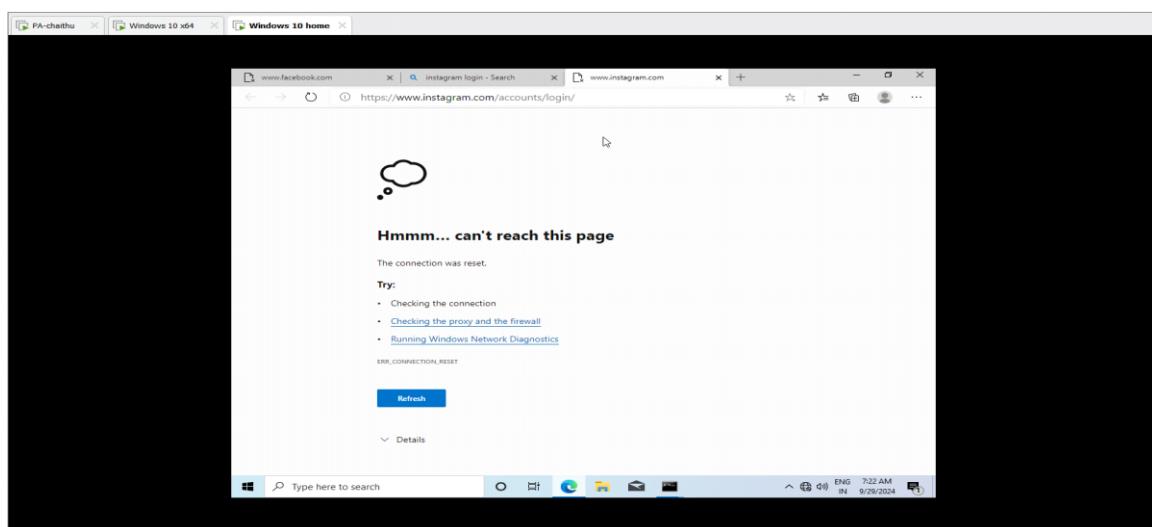
- **Login Page:** Capture a screenshot of the login page showing access to the PAN firewall.

- **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.

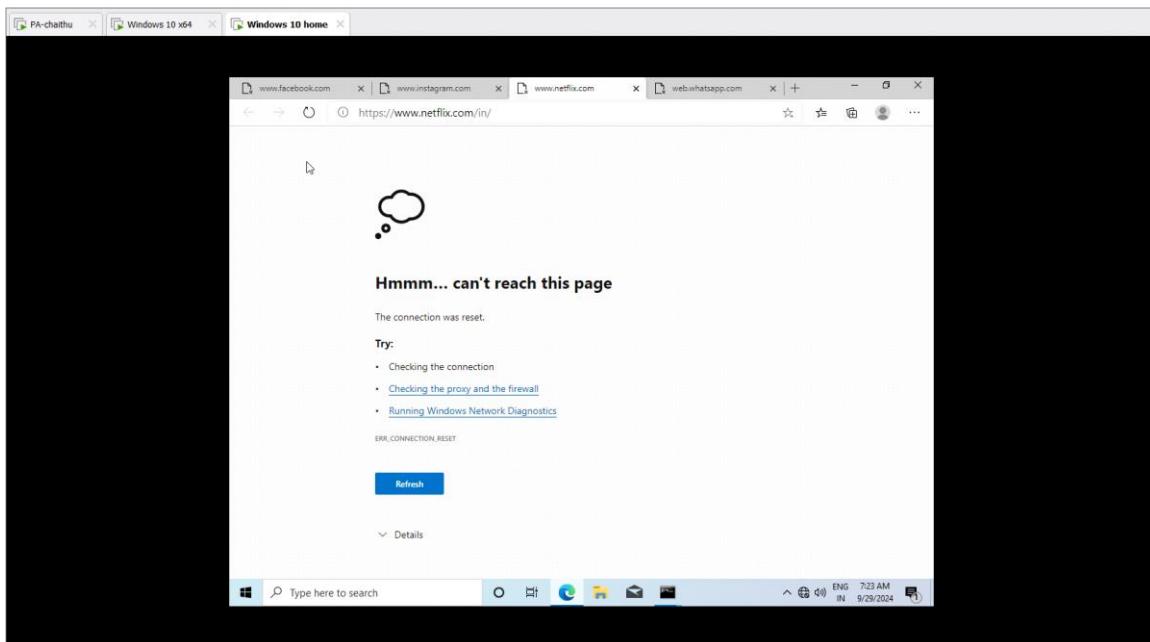
Facebook:



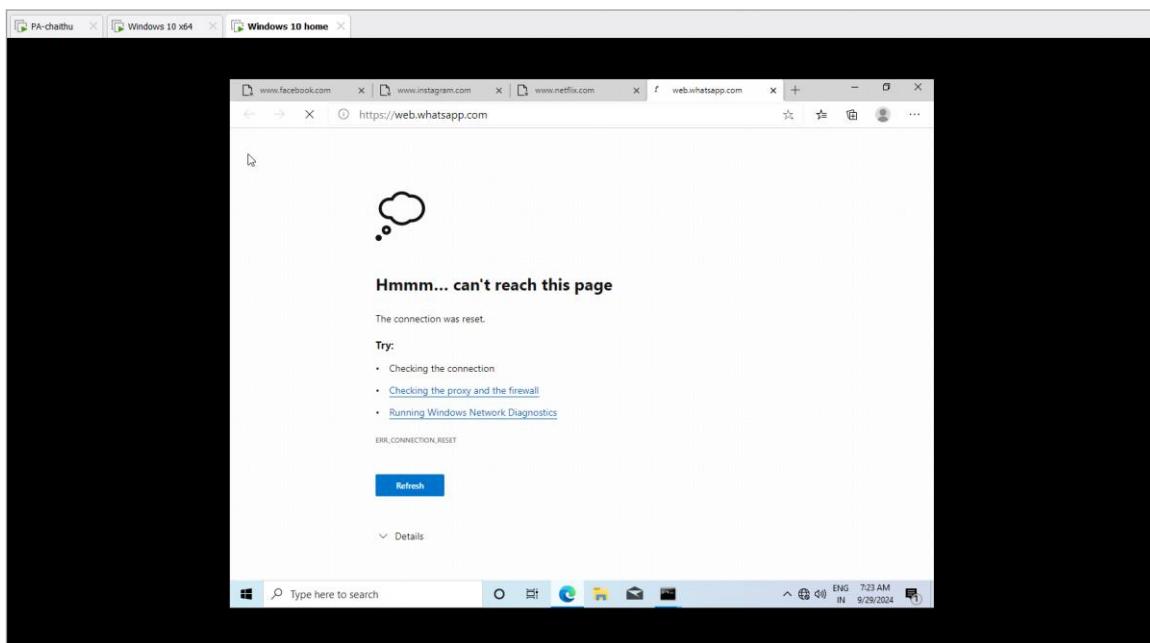
Instagram:



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.

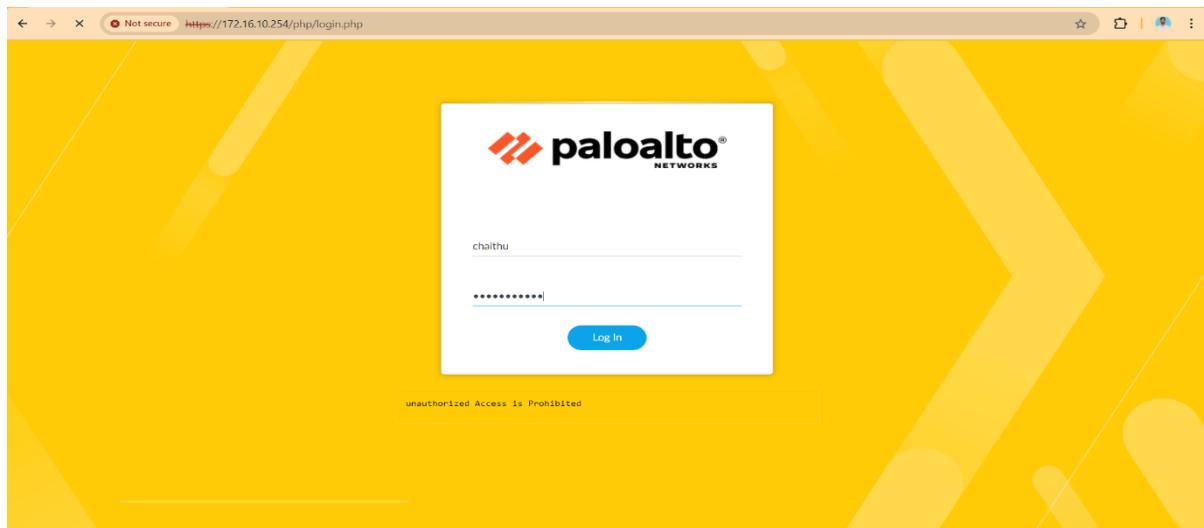
3.Configuring Zones, Interfaces, Virtual Router, and Source NAT?

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:sys1:network/zones>

Zone

Name	Type	Log Setting	INTERFACES	User Identification ACL	Device-ID ACL
Trust Zone	Layer3	None	ethernet1/1	<input type="checkbox"/> Enable User Identification <input checked="" type="checkbox"/> INCLUDE LIST	<input type="checkbox"/> Enable Device Identification <input checked="" type="checkbox"/> INCLUDE LIST
Untrust Zone	Layer3	None	ethernet1/2	<input type="checkbox"/> EXCLUDE LIST	<input type="checkbox"/> EXCLUDE LIST

Zone Protection

Zone Protection Profile	Log Setting	INTERFACES	User Identification ACL	Device-ID ACL
None	None	ethernet1/2	<input type="checkbox"/> EXCLUDE LIST	<input type="checkbox"/> EXCLUDE LIST

Zone Protection Profile

Profile	Log Setting	INTERFACES	User Identification ACL	Device-ID ACL
None	None	ethernet1/2	<input type="checkbox"/> EXCLUDE LIST	<input type="checkbox"/> EXCLUDE LIST

OK **Cancel**

Not secure <https://172.16.10.254/#network:sys1:network/zones>

Zone

Name	Type	Log Setting	INTERFACES	User Identification ACL	Device-ID ACL
Untrust Zone	Layer3	None	ethernet1/2	<input type="checkbox"/> Enable User Identification <input checked="" type="checkbox"/> INCLUDE LIST	<input type="checkbox"/> Enable Device Identification <input checked="" type="checkbox"/> INCLUDE LIST
Trust Zone	Layer3	None	ethernet1/1	<input type="checkbox"/> EXCLUDE LIST	<input type="checkbox"/> EXCLUDE LIST

Zone Protection

Zone Protection Profile	Log Setting	INTERFACES	User Identification ACL	Device-ID ACL
None	None	ethernet1/2	<input type="checkbox"/> EXCLUDE LIST	<input type="checkbox"/> EXCLUDE LIST

Zone Protection Profile

Profile	Log Setting	INTERFACES	User Identification ACL	Device-ID ACL
None	None	ethernet1/2	<input type="checkbox"/> EXCLUDE LIST	<input type="checkbox"/> EXCLUDE LIST

OK **Cancel**

Not secure <https://172.16.10.254/#network:sys1:network/zones>

Network

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	User-ID	Device-ID				
Trust Zone	layer3	ethernet1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
Untrust Zone	layer3	ethernet1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS

OK **Cancel**

B. Configure Network Interfaces

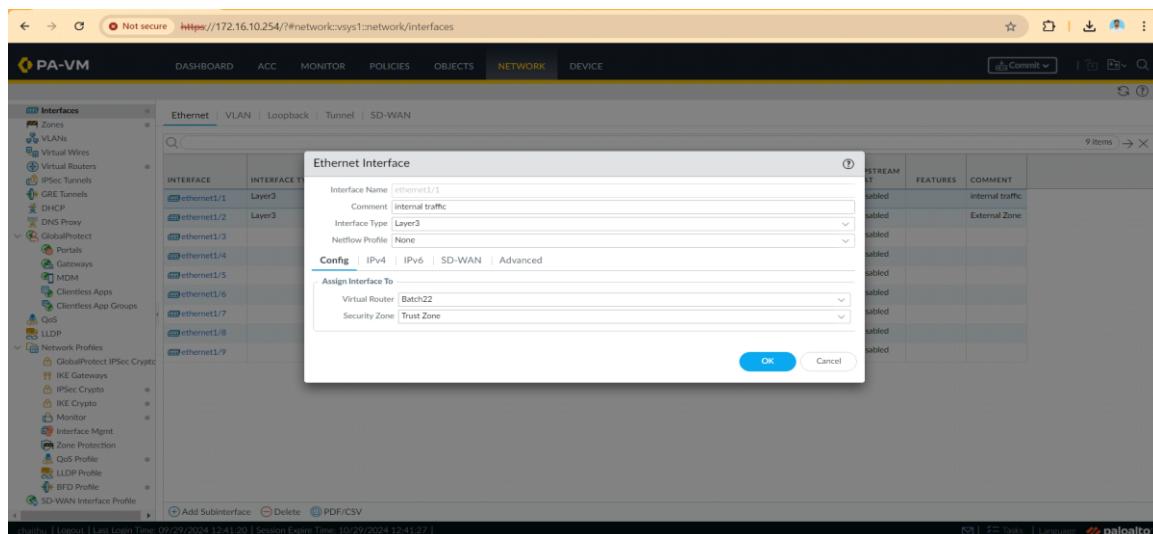
Assign the firewall's physical interfaces to the zones you created.

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.



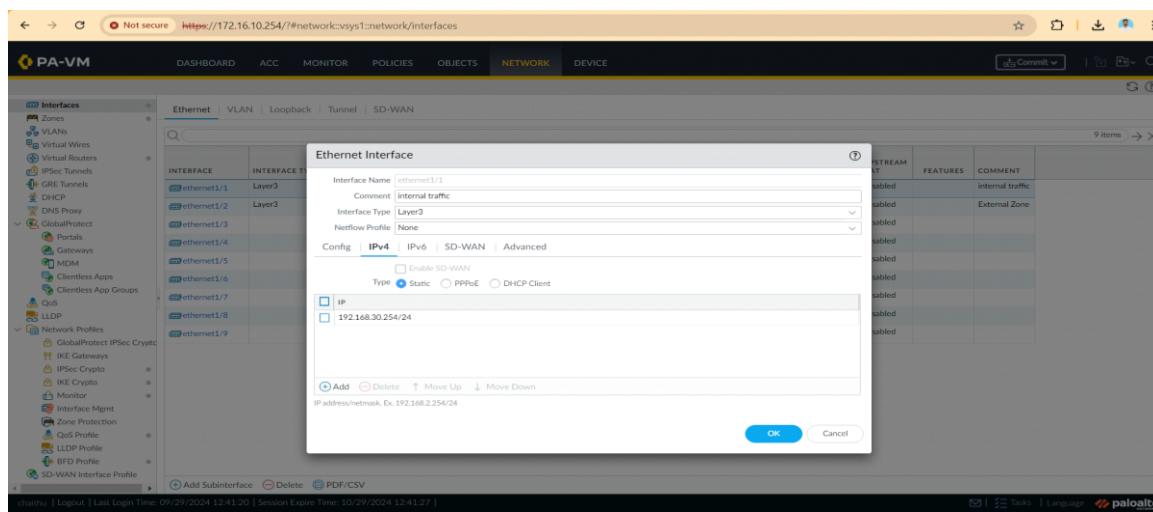
The screenshot shows the 'Interfaces' section of the Palo Alto Networks management interface. The 'ethernet1/1' interface is selected and configured as follows:

- Interface Name:** ethernet1/1
- Comment:** internal traffic
- Interface Type:** Layer3
- Netflow Profile:** None
- Config:** IPv4 | IPv6 | SD-WAN | Advanced
- Assign Interface To:**
 - Virtual Router:** Batch22
 - Security Zone:** Trust Zone

The 'IPv4' tab is active, showing the static IP configuration:

- Type:** Static
- IP:** 192.168.30.254/24

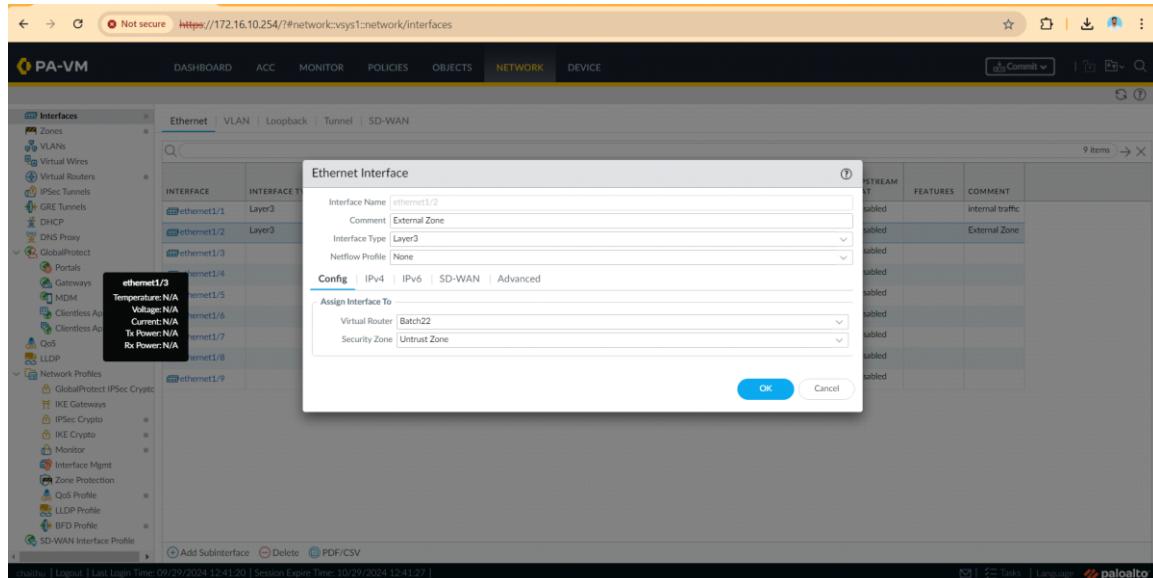
The 'SD-WAN' tab is also visible in the configuration dialog.



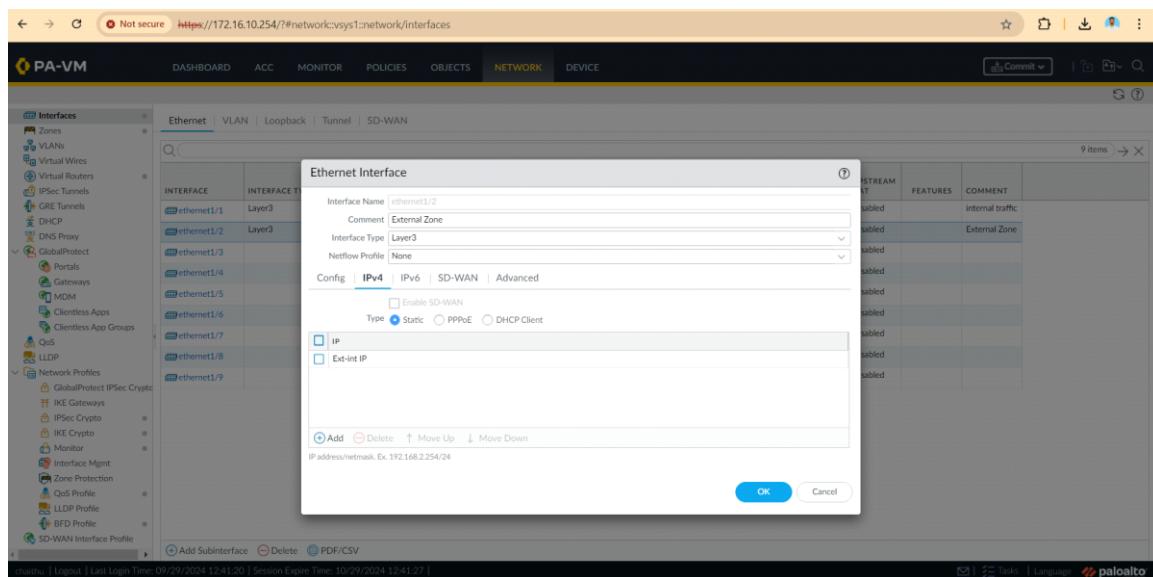
This screenshot is identical to the one above, showing the configuration of the 'ethernet1/1' interface. The key difference is that the 'IPv4' tab is highlighted, indicating it is the active configuration tab.

3. Configure Internal (LAN) Interface:

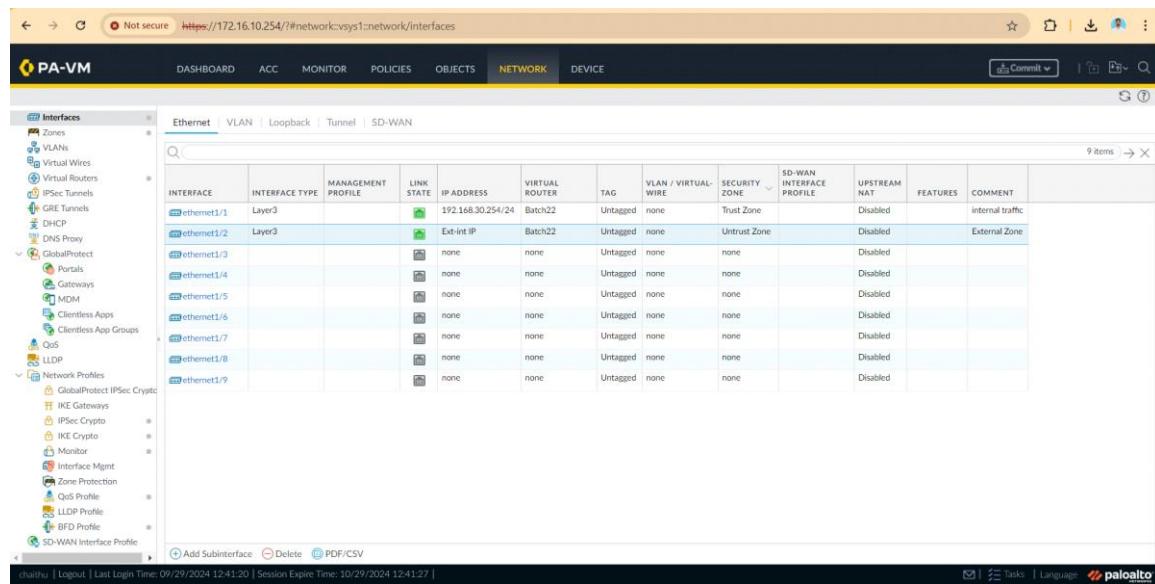
- Select another available interface (**ethernet1/2**).
- Set Interface Type to **Layer 3**.
- **Virtual Router:** Assign the same virtual router.
- **Security Zone:** Choose LAN.
- Under **IPv4 tab**, add the IP address range for your LAN.
- Click **OK**.



The screenshot shows the Palo Alto Networks VM interface configuration screen. The 'Ethernet' tab is selected. The interface 'ethernet1/2' is selected for configuration. The 'Config' tab is active, showing 'Virtual Router' set to 'Batch22' and 'Security Zone' set to 'Untrust Zone'. The 'IPv4' tab is also visible. A table on the right shows interface statistics.



The screenshot shows the Palo Alto Networks VM interface configuration screen. The 'Ethernet' tab is selected. The interface 'ethernet1/2' is selected for configuration. The 'Config' tab is active, showing 'IPV4' selected. The 'Type' dropdown is set to 'Static'. The 'IP' checkbox is checked. The 'Comment' field is set to 'External Zone'. The 'Interface Type' is set to 'Layer3'. The 'Netflow Profile' is set to 'None'. The 'Assign Interface To' section shows 'Virtual Router' set to 'Batch22' and 'Security Zone' set to 'Untrust Zone'. The 'IPv4' tab is also visible. A table on the right shows interface statistics.



C. Configure the Virtual Router

A virtual router is responsible for routing traffic between zones.

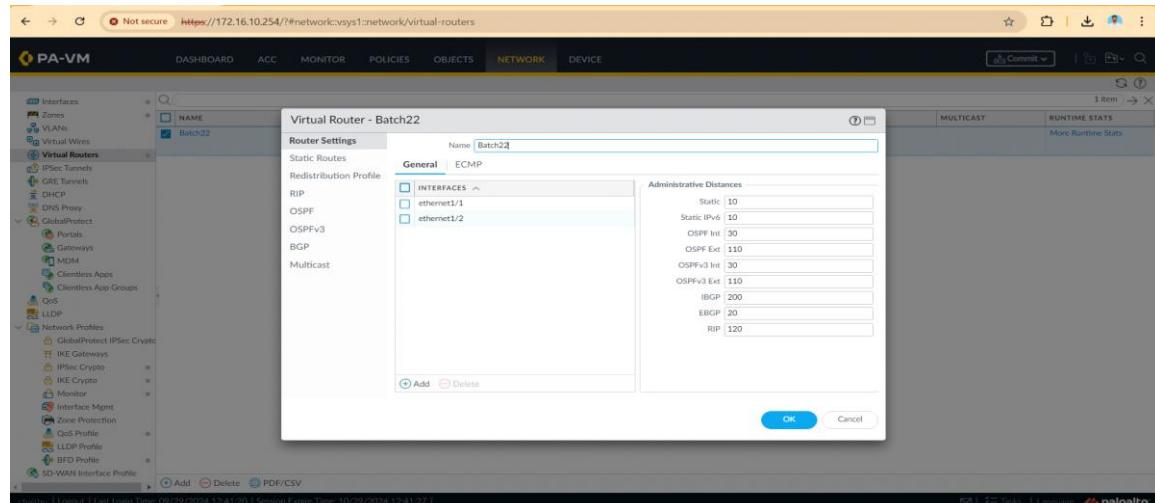
1. Navigate to the Virtual Router:

- 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)

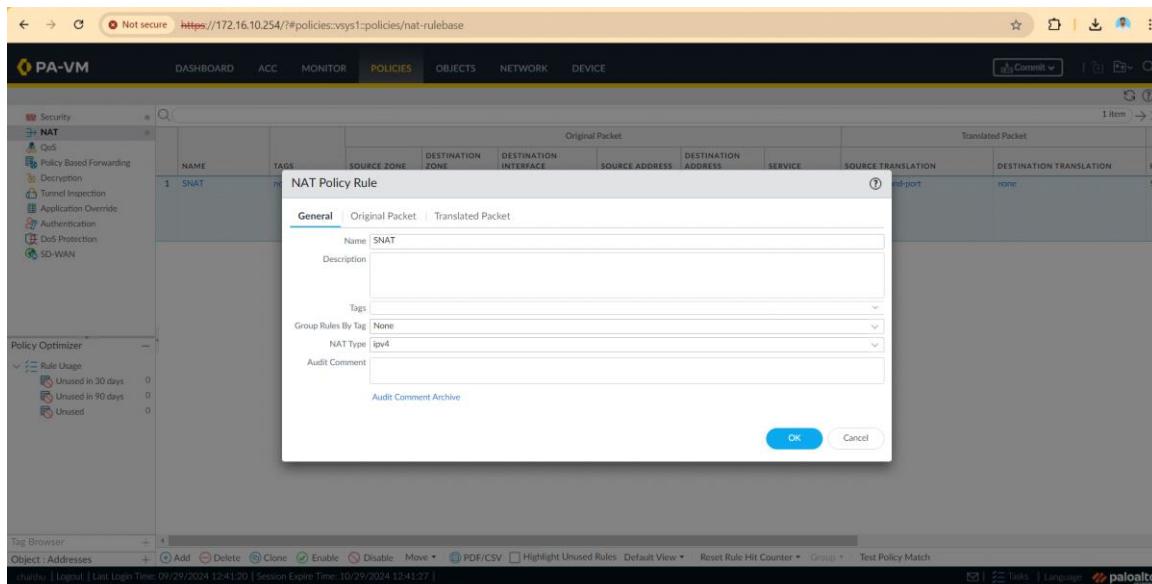


D. Configure Source NAT

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

1. Navigate to the NAT Configuration:

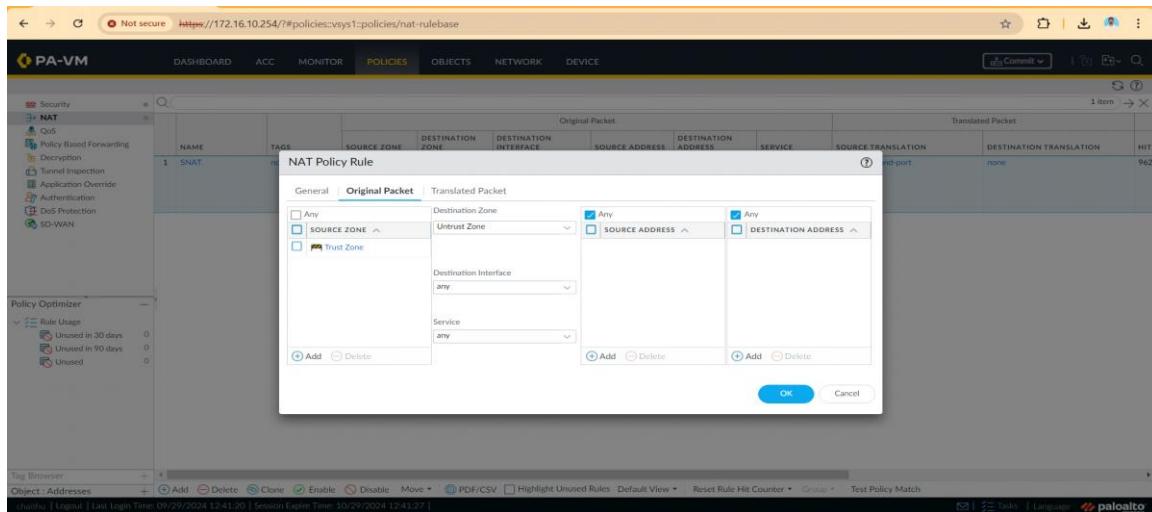
- Go to Policies > NAT.
- Click Add to create a new NAT policy.
- NAT Rule General Settings:
- Name: Give your rule a name (**SNAT**).



The screenshot shows the Palo Alto VM interface with the URL <https://172.16.10.254/#/policies:vsys1:policies/nat-rulebase>. The left sidebar has 'NAT' selected. A modal window titled 'NAT Policy Rule' is open, showing the 'General' tab. The 'Name' field is set to 'SNAT'. Other fields include 'Description', 'Tags', 'Group Rules By Tag: None', 'NAT Type: ipv4', and 'Audit Comment'. At the bottom right of the modal are 'OK' and 'Cancel' buttons. The main pane shows a table with one row for the 'SNAT' rule, and the bottom status bar indicates '1 item'.

2. Original Packet Tab:

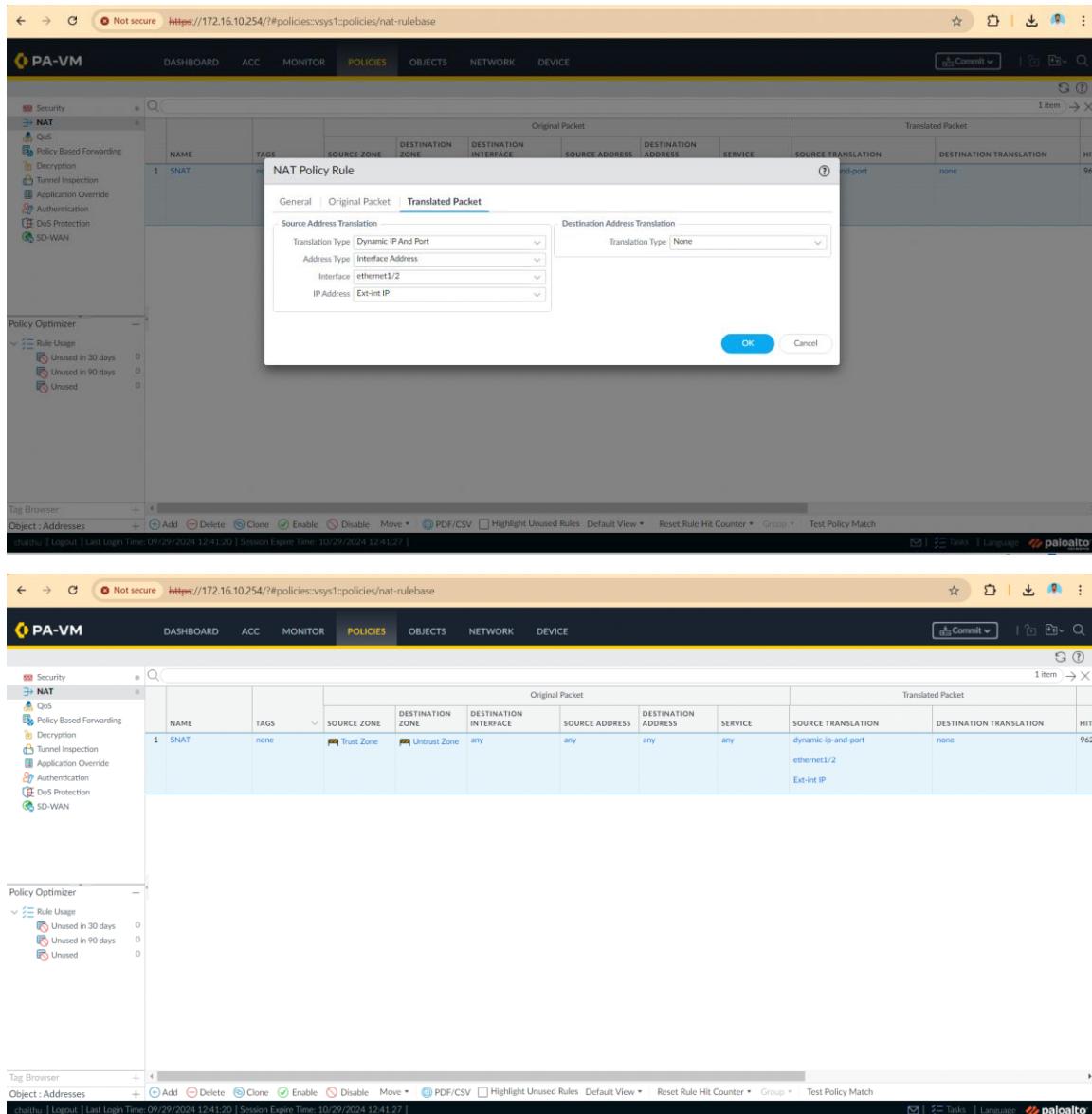
- **Source Zone:** Select your LAN zone (the zone from where traffic originates).
- **Destination Zone:** Select WAN.
- **Destination Interface:** Select your WAN interface (**ethernet1/1**).



The screenshot shows the same interface as the previous one, but the 'Original Packet' tab is selected in the modal. Under 'Destination Zone', 'Untest Zone' is selected. Under 'Source Address', 'Any' is selected. Under 'Destination Address', 'Any' is selected. The bottom status bar indicates '1 item'.

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.



The screenshot shows the Palo Alto Networks PA-VM web interface. The user is configuring a NAT Policy Rule named "SNAT". The "Translated Packet" tab is selected. Under "Source Address Translation", the "Translation Type" is set to "Dynamic IP And Port", "Address Type" to "Interface Address", "Interface" to "ethernet1/2", and "IP Address" to "Ext-int IP". Under "Destination Address Translation", the "Translation Type" is set to "None". The "OK" button is visible at the bottom right of the dialog.

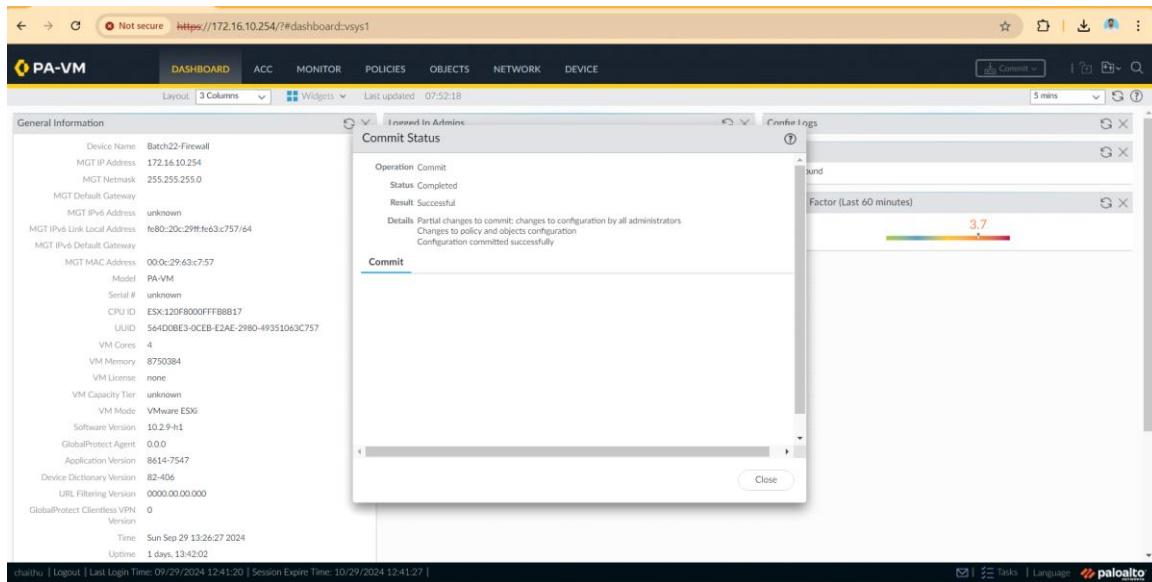
Original Packet		Translated Packet								
NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION	HIT
1 SNAT	none	Trust Zone	Untrust Zone	any	any	any	any	dynamic-ip-and-port	none	962

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.



The screenshot shows the Palo Alto Networks PA-VM dashboard. On the left, there's a sidebar with 'General Information' containing various device details like Device Name (Batch22-Firewall), MGT IP Address (172.16.10.254), and Model (PA-VM). In the center, a modal window titled 'Commit Status' is open, showing 'Operation Commit' completed successfully with no errors. To the right, there's a 'Configure Logs' section with a chart titled 'Factor (Last 60 minutes)' showing a value of 3.7.

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

