

ASSIGNMENT

COURSE	PA Firewall	ASSIGNMENT NO	3
MODULE	Firewall	ASSIGNMENT DATE	26-Sep-24
STUDENT NAME	Konganti Chaithanya Kumar	SUBMIT DATE	26-Sep-24

1. Change the Firewall Name and Time

- **Access the PAN Web Interface:**
 - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
 - Device > Setup > Management tab.
- **Change Firewall Name:**
 - Under General Settings, click the gear icon to the right of Hostname.
 - Enter the new firewall name and click OK.
- **Change System Time:**
 - Under Operations in the same tab, click Set Time.
 - Update the time and time zone as needed.
 - Click OK to apply changes.

Screenshot: After changing the firewall name and time, take a screenshot from the Management tab.

General Settings

Hostname Batch22-Firewall

Domain

☐ Accept DHCP server provided Hostname

☐ Accept DHCP server provided Domain

Login Banner

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile None

Time Zone Asia/Kolkata

Locale en

Date 2024/09/27

Time 02:52:00

Latitude

Longitude

☐ Automatically Acquire Commit Lock

☐ Certificate Expiration Check

☒ Use Hypervisor Assigned MAC Addresses

☐ GTP Security

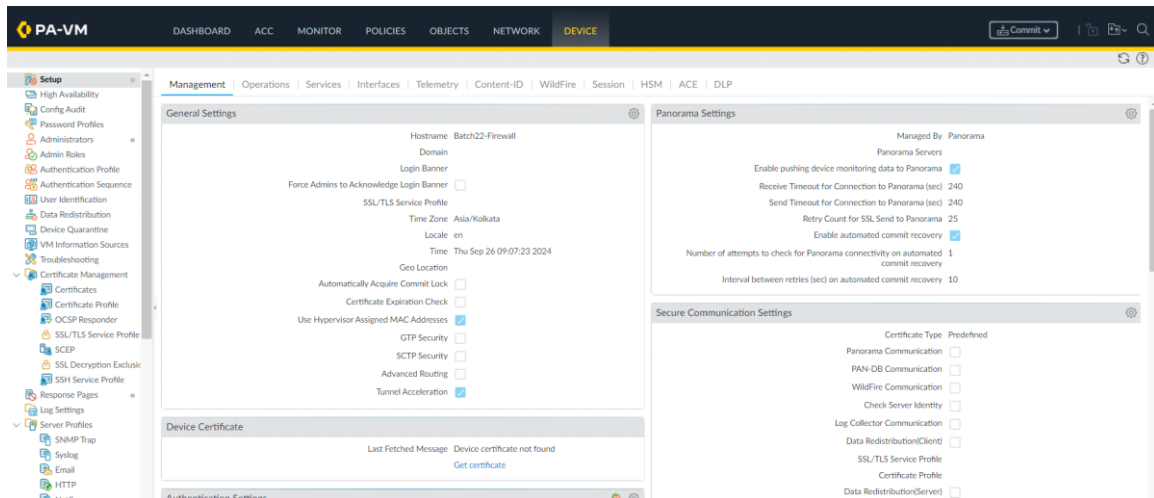
☐ SCTP Security

☐ Advanced Routing

☒ Tunnel Acceleration

OK

Cancel



The screenshot shows the Palo Alto Networks VM-Series configuration interface. The left sidebar contains a 'Setup' menu with various configuration options. The main content area is divided into three panels:

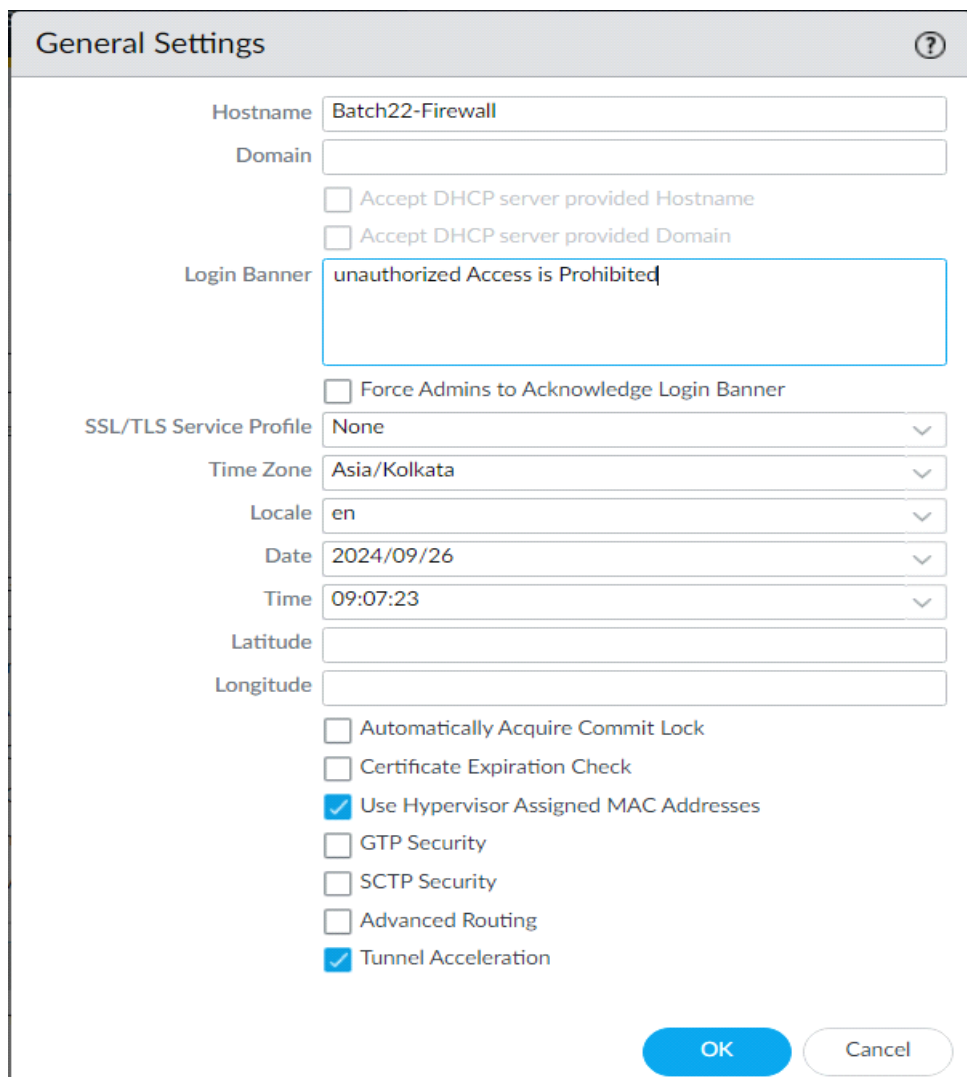
- General Settings:** This panel contains fields for Hostname (Batch22-Firewall), Domain, Login Banner, and SSL/TLS Service Profile (None). It also includes a section for Time Zone (Asia/Kolkata), Locale (en), Date (2024/09/27), and Time (02:52:00). There are checkboxes for Latitude, Longitude, Automatically Acquire Commit Lock, Certificate Expiration Check, Use Hypervisor Assigned MAC Addresses (checked), GTP Security, SCTP Security, Advanced Routing, and Tunnel Acceleration (checked).
- Panorama Settings:** This panel shows settings for Panorama Servers, including Enable pushing device monitoring data to Panorama (checked), Receive Timeout for Connection to Panorama (sec) (240), Send Timeout for Connection to Panorama (sec) (240), Retry Count for SSL Send to Panorama (25), Enable automated commit recovery (checked), Number of attempts to check for Panorama connectivity on automated commit recovery (1), and Interval between retries (sec) on automated commit recovery (10).
- Secure Communication Settings:** This panel shows settings for Certificate Type (Predefined), Panorama Communication, PAN-DB Communication, WildFire Communication, Check Server Identity, Log Collector Communication, Data Redistribution(Client), SSL/TLS Service Profile, Certificate Profile, and Data Redistribution(Server).

2. Write a Banner and Verify It

- **Access the PAN Web Interface:**
 - Log in to the PAN firewall using the web interface with your credentials.

- **Navigate to:**
 - Device > Setup > Management tab.
- **Write the Banner:**
 - Click the gear icon to the right of Login Banner.
 - Enter the text for your banner and click OK.
- **Verify the Banner:**
 - Logout of the web interface and re-login to see if the banner is displayed correctly.

Screenshot: After logging back in, capture a screenshot showing the banner at the login page.



General Settings

Hostname: Batch22-Firewall

Domain:

☐ Accept DHCP server provided Hostname

☐ Accept DHCP server provided Domain

Login Banner: unauthorized Access is Prohibited

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: None

Time Zone: Asia/Kolkata

Locale: en

Date: 2024/09/26

Time: 09:07:23

Latitude:

Longitude:

☐ Automatically Acquire Commit Lock

☐ Certificate Expiration Check

☒ Use Hypervisor Assigned MAC Addresses

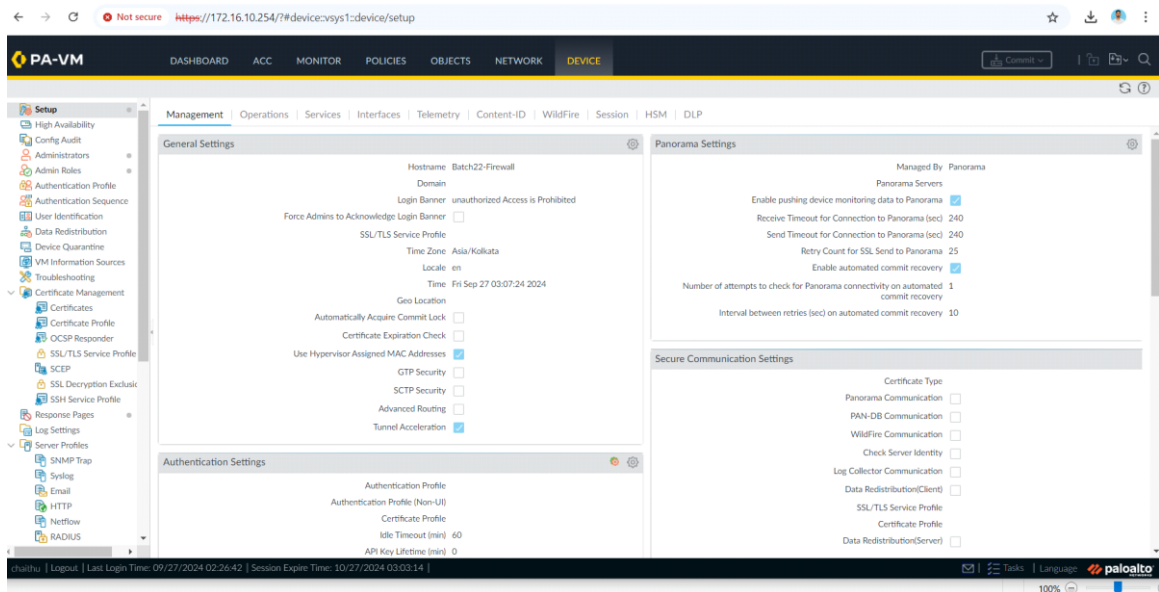
☐ GTP Security

☐ SCTP Security

☐ Advanced Routing

☒ Tunnel Acceleration

OK Cancel

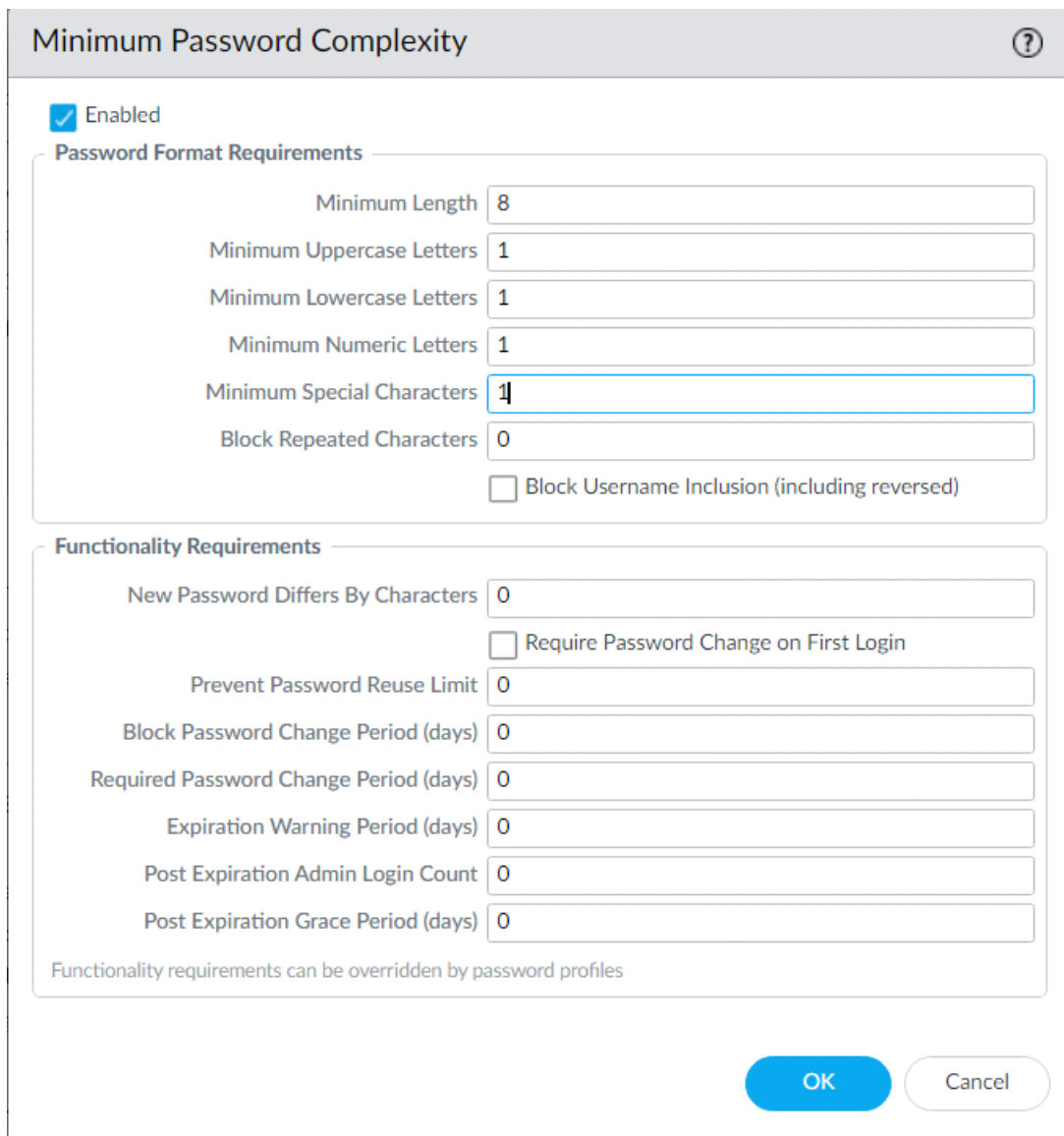


3. Configure a Complex Password Policy

- **Access the PAN Web Interface:**
 - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
 - Device > Setup > Management > Password Profile.
- **Create a Password Profile:**
 - Click Add and configure the following settings:
 - Minimum length: Set a value (8 characters).
 - Require at least one uppercase letter(1), one lowercase letter(1), one number(1), and one special character(1).
 - Set password expiration days (10).
 - Set the number of failed login attempts before logout.

- Click OK.
- **Test the Validity:**
 - Create a test user and attempt to set a password that doesn't meet the complexity requirements, and then one that does.

Screenshot: After configuring the policy, capture a screenshot showing the Password Profile screen.



The screenshot shows a configuration window titled "Minimum Password Complexity" with a help icon in the top right corner. The window is divided into two main sections: "Password Format Requirements" and "Functionality Requirements".

Password Format Requirements:

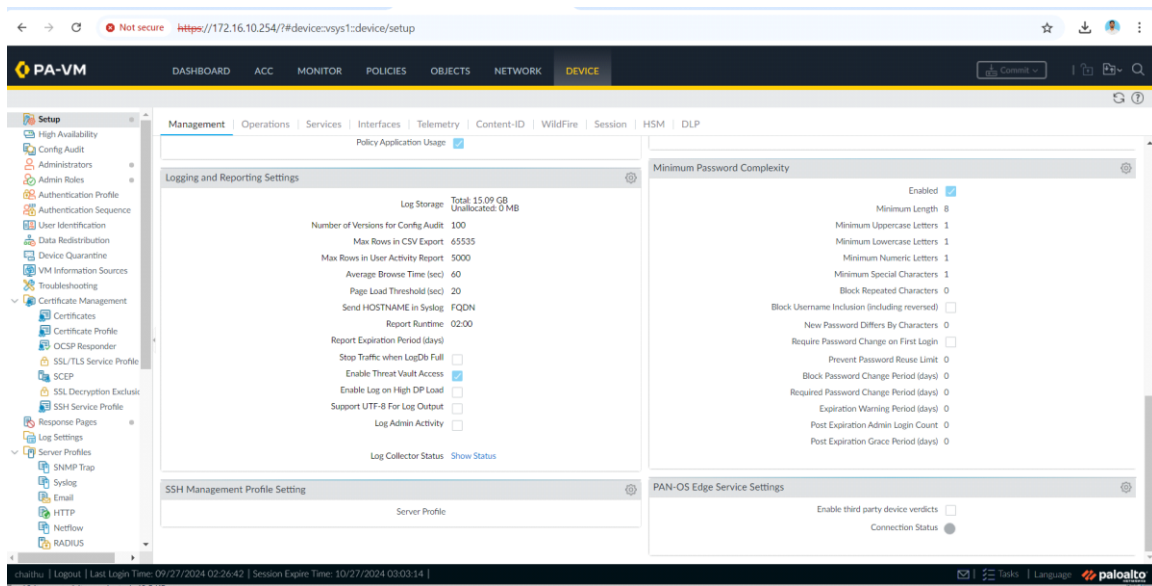
- ☒ Enabled
- Minimum Length: 8
- Minimum Uppercase Letters: 1
- Minimum Lowercase Letters: 1
- Minimum Numeric Letters: 1
- Minimum Special Characters: 1
- Block Repeated Characters: 0
- ☐ Block Username Inclusion (including reversed)

Functionality Requirements:

- New Password Differs By Characters: 0
- ☐ Require Password Change on First Login
- Prevent Password Reuse Limit: 0
- Block Password Change Period (days): 0
- Required Password Change Period (days): 0
- Expiration Warning Period (days): 0
- Post Expiration Admin Login Count: 0
- Post Expiration Grace Period (days): 0

Functionality requirements can be overridden by password profiles

At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).



4. Create a Role-Based Profile

- **Access the PAN Web Interface:**
 - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
 - Device > Admin Roles.
- **Create a New Role:**
 - Click Add and provide a name for the role.
 - Customize the permissions for various system components like Policies, Objects, Network, etc.
 - Save the role by clicking OK.

Screenshot: After creating the role, capture a screenshot showing the role settings.

⑦

Name	Read-Only Admin
------	-----------------

Description	Admin with read-only permissions
-------------	----------------------------------

[Web UI](#) | [XML API](#) | [Command Line](#) | [REST API](#)

- ✓ Dashboard
- ✓ ACC
- ✓ Monitor
 - ✓ Logs
 - ✓ Traffic
 - ✓ Threat
 - ✓ URL Filtering
 - ✓ WildFire Submissions
 - ✓ Data Filtering
 - ✓ HIP Match
 - ✓ GlobalProtect
 - ✓ IP-Tag
 - ✓ User-ID
 - ✓ Decryption
 - ✓ Tunnel Inspection

Legend: Enable Read Only Disable

OK

Cancel

← → 🔍 🔒 Not secure https://172.16.10.254/?#device:vsys1:device/admin-roles ☆ 🧑 👤 ⋮

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** [Commit](#) [📄](#) [🔍](#) [🔍](#)

🔍 4 items → ×

Admin Roles

NAME	DESCRIPTION	ROLE	CLI ROLE
<input type="checkbox"/> auditadmin	Audit Administrator for Common Criteria	device	
<input type="checkbox"/> cryptoadmin	Crypto Administrator for Common Criteria	device	
<input type="checkbox"/> securityadmin	Security Admin for Common Criteria	device	
<input type="checkbox"/> Read-Only Admin	Admin with read-only permissions	device	

🔍 Add Delete Clone PDF/CSV

chaitu | Logout | Last Login Time: 09/27/2024 02:26:42 | Session Expire Time: 10/27/2024 03:03:14 | 📧 📅 Tasks | Language 🌐 paloalto

5. Create a User and Assign the Role-Based Profile

- **Access the PAN Web Interface:**
 - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to the Administrators Section:**
 - Go to the PAN firewall's Web UI.
 - Navigate to Device > Administrators.
- **Add a New Administrator:**
 - In the Administrators section, click the Add button to create a new administrator account.
- **Enter User Details:**
 - **Username:** Enter a username for the new admin (chaithu).
 - **Password:** Enter and confirm a strong password for the user. Ensure the password complies with the complex password policy if you've set one.
- **Assign the Role-Based Profile:**
 - In the Admin Role Profile dropdown, select the role profile you created earlier.
- **Set the Authentication Profile:**
 - In the Authentication Profile section, choose the default profile or any existing authentication profile that is configured.
- **Save the Configuration:**
 - Click OK to save the new administrator.

Administrator

?

Name

chaithu

Authentication Profile

None

☐ Use only client certificate authentication (Web)

Password

••••••••

Confirm Password

••••••••

Password Requirements

- Minimum Password Length (Count) 8
- Minimum Uppercase Characters 1
- Minimum Lowercase Characters 1
- Minimum Numeric Characters 1
- Minimum Special Characters 1

☐ Use Public Key Authentication (SSH)

Administrator Type

☐ Dynamic ☒ Role Based

Profile

Read-Only Admin

Password Profile

None

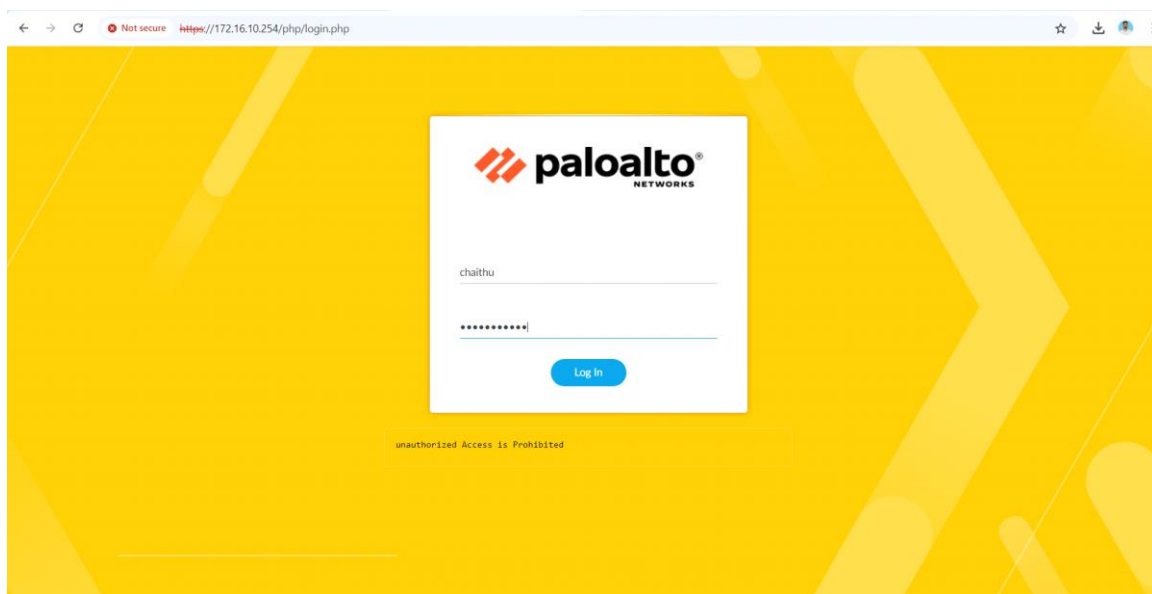
OK

Cancel

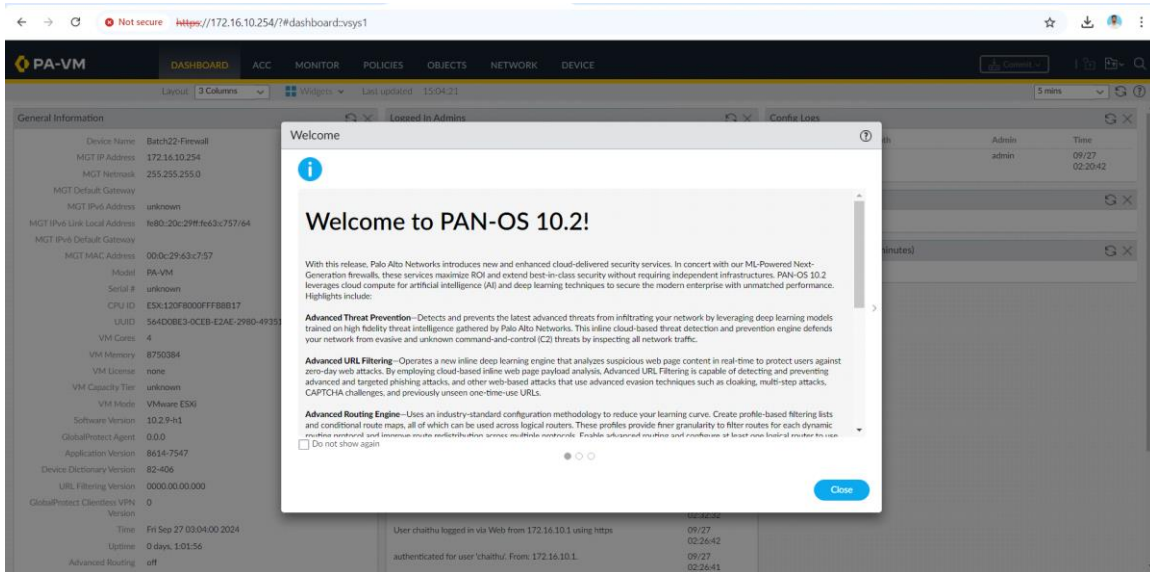
- **Test the Login:**

- Logout of the web interface and login using the new user's credentials to confirm it works.

Screenshot: Capture a screenshot after logging in with the new user.



A successful login with the new user's credentials.



The screenshot shows the Palo Alto VM dashboard with a 'Welcome' dialog box open. The dialog box contains the following text:

Welcome to PAN-OS 10.2!

With this release, Palo Alto Networks introduces new and enhanced cloud-delivered security services. In concert with our ML-Powered Next-Generation firewalls, these services maximize ROI and extend best-in-class security without requiring independent infrastructures. PAN-OS 10.2 leverages cloud compute for artificial intelligence (AI) and deep learning techniques to secure the modern enterprise with unmatched performance. Highlights include:

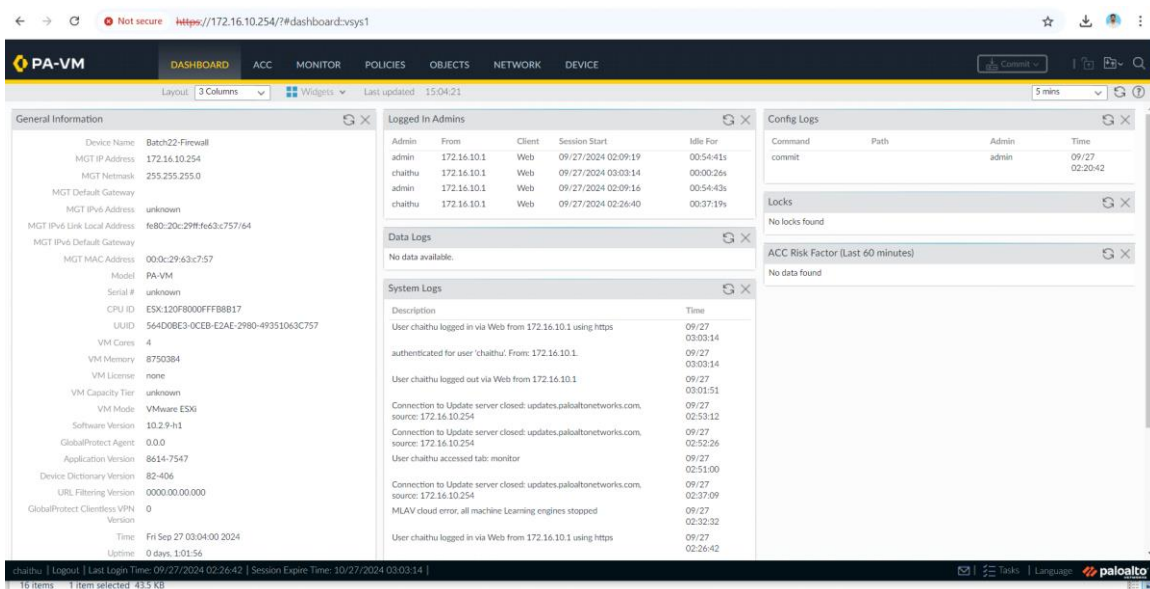
- Advanced Threat Prevention** - Detects and prevents the latest advanced threats from infiltrating your network by leveraging deep learning models trained on high fidelity threat intelligence gathered by Palo Alto Networks. This inline cloud-based threat detection and prevention engine defends your network from evasive and unknown command-and-control (C2) threats by inspecting all network traffic.
- Advanced URL Filtering** - Operates a new inline deep learning engine that analyzes suspicious web page content in real-time to protect users against zero-day web attacks. By employing cloud-based inline web page payload analysis, Advanced URL Filtering is capable of detecting and preventing advanced and targeted phishing attacks, and other web-based attacks that use advanced evasion techniques such as cloaking, multi-step attacks, CAPTCHA challenges, and previously unseen one-time-use URLs.
- Advanced Routing Engine** - Uses an industry-standard configuration methodology to reduce your learning curve. Create profile-based filtering lists and conditional route maps, all of which can be used across logical routers. These profiles provide finer granularity to filter routes for each dynamic machine endpoint and increase route redistribution across multiple networks. Enable advanced routing and monitor at least one logical router to use.

☐ Do not show again

Close

The background dashboard shows the 'General Information' tab for the device 'Batch22-Firewall'. The 'Logged In Admins' table shows a successful login for user 'chaitu' from 172.16.10.1 using https on 09/27/2024 at 02:26:42.

Verify the Role:



The screenshot shows the Palo Alto VM dashboard with the 'System Logs' tab selected. The 'System Logs' table shows the following events:

Description	Time
User chaitu logged in via Web from 172.16.10.1 using https	09/27 03:03:14
authenticated for user 'chaitu'. From: 172.16.10.1.	09/27 03:03:14
User chaitu logged out via Web from 172.16.10.1.	09/27 03:01:51
Connection to Update server closed: updates.paloaltonetworks.com, source: 172.16.10.254	09/27 02:53:12
Connection to Update server closed: updates.paloaltonetworks.com, source: 172.16.10.254	09/27 02:52:26
User chaitu accessed tab: monitor	09/27 02:51:00
Connection to Update server closed: updates.paloaltonetworks.com, source: 172.16.10.254	09/27 02:37:09
MLAV cloud error, all machine Learning engines stopped	09/27 02:32:32
User chaitu logged in via Web from 172.16.10.1 using https	09/27 02:26:42

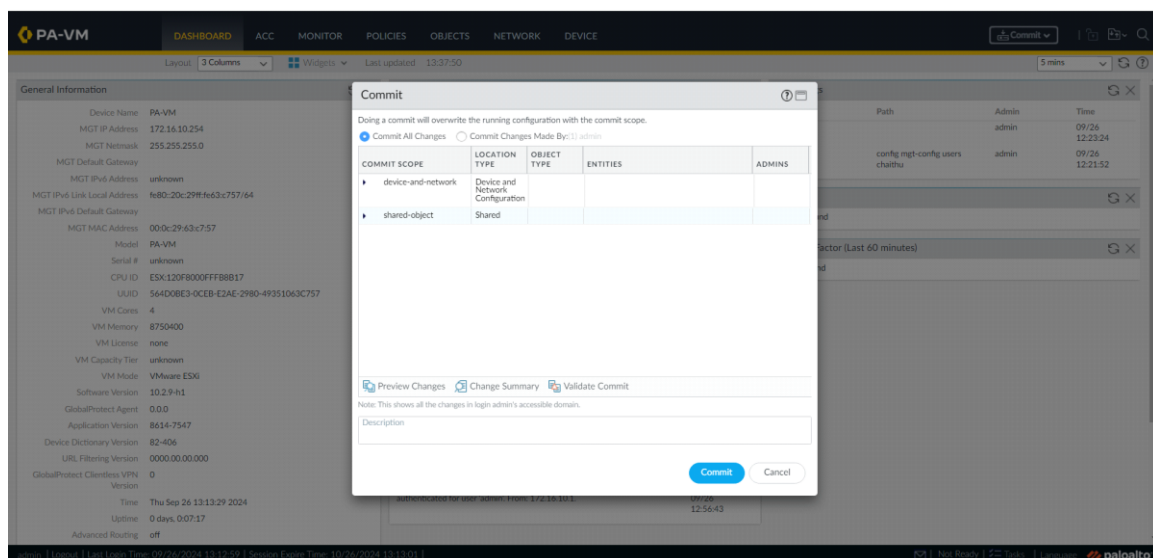
The 'General Information' tab on the left shows the device details for 'Batch22-Firewall'. The 'Config Logs' tab on the right shows a successful commit for user 'admin' on 09/27/2024 at 02:20:42.

6. Commit the Changes

- **Access the PAN Web Interface:**
 - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
 - Click Commit in the top-right corner of the web interface.
 - Review the changes and click Commit to apply.

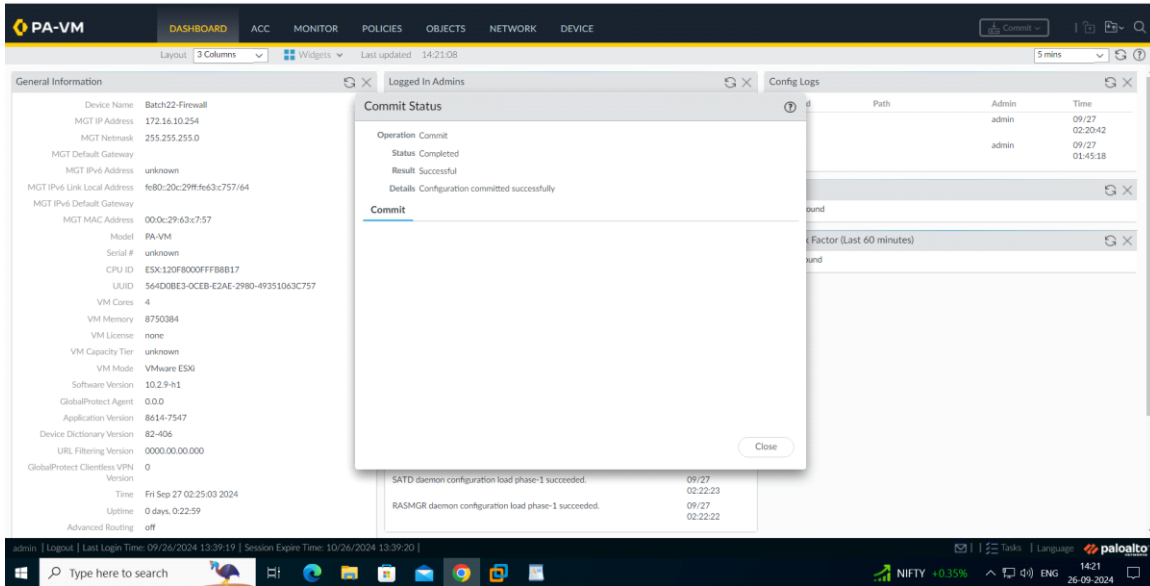
Screenshot: After committing the changes, take a screenshot of the Commit status.

Wait for the Commit to Complete:



Successfully completed commit:

- The commit process will take a few seconds to complete, depending on the size and complexity of the changes.
- You will see a notification when the commit is successful.



PA-VM | DASHBOARD | ACC | MONITOR | POLICIES | OBJECTS | NETWORK | DEVICE

Layout: 3 Columns | Widgets | Last updated: 14:21:08 | 5 mins

General Information

Device Name	Batch22-Firewall
MGT IP Address	172.16.10.254
MGT Netmask	255.255.255.0
MGT Default Gateway	unknown
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80:20c:29ff:fe63:c757/64
MGT IPv6 Default Gateway	unknown
MGT MAC Address	00:0c:29:63:c7:57
Model	PA-VM
Serial #	unknown
CPU ID	ESX:120F8000FFB8B17
UUID	564D0BE3-0CEB-E2AE-2980-49351063C757
VM Cores	4
VM Memory	8750384
VM License	none
VM Capacity Tier	unknown
VM Mode	VMware ESXi
Software Version	10.2.9-h1
GlobalProtect Agent	0.0.0
Application Version	8614-7547
Device Dictionary Version	82-406
URL Filtering Version	0000.00.00.000
GlobalProtect Clientless VPN Version	0
Time	Fri Sep 27 02:25:03 2024
Uptime	0 days, 0:22:59
Advanced Routing	off

Commit Status

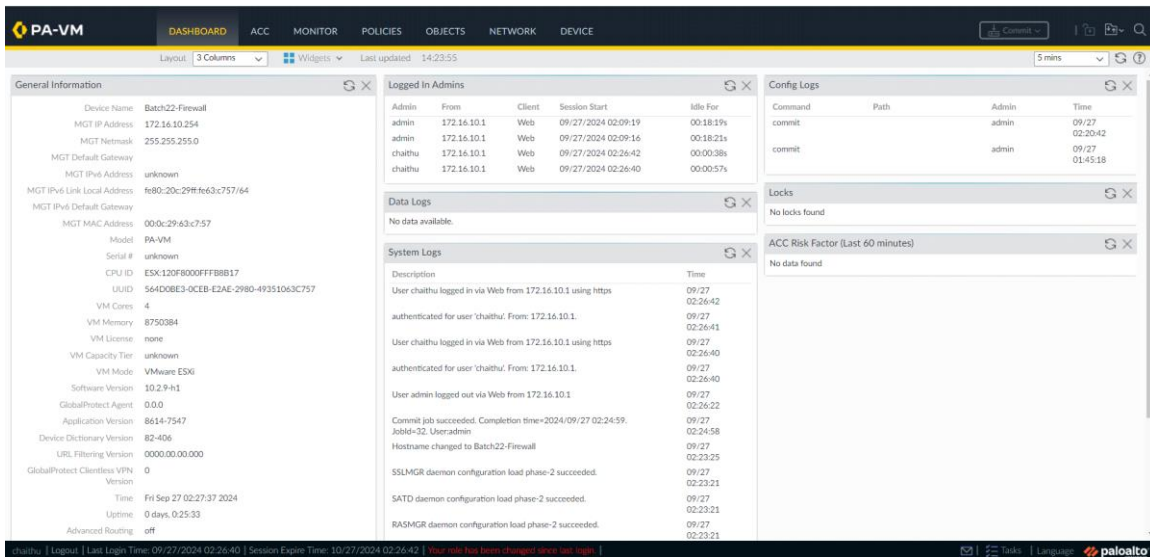
Operation: Commit
Status: Completed
Result: Successful
Details: Configuration committed successfully

Commit

SATD daemon configuration load phase-1 succeeded. 09/27 02:22:23
RASMGR daemon configuration load phase-1 succeeded. 09/27 02:22:22

admin | Logout | Last Login Time: 09/26/2024 13:09:19 | Session Expires Time: 10/26/2024 13:39:20 | NIFTY +0.35% | Tasks | Language | paloalto 14:21 26-09-2024

After Completed welcome page:



PA-VM | DASHBOARD | ACC | MONITOR | POLICIES | OBJECTS | NETWORK | DEVICE

Layout: 3 Columns | Widgets | Last updated: 14:23:55 | 5 mins

General Information

Device Name	Batch22-Firewall
MGT IP Address	172.16.10.254
MGT Netmask	255.255.255.0
MGT Default Gateway	unknown
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80:20c:29ff:fe63:c757/64
MGT IPv6 Default Gateway	unknown
MGT MAC Address	00:0c:29:63:c7:57
Model	PA-VM
Serial #	unknown
CPU ID	ESX:120F8000FFB8B17
UUID	564D0BE3-0CEB-E2AE-2980-49351063C757
VM Cores	4
VM Memory	8750384
VM License	none
VM Capacity Tier	unknown
VM Mode	VMware ESXi
Software Version	10.2.9-h1
GlobalProtect Agent	0.0.0
Application Version	8614-7547
Device Dictionary Version	82-406
URL Filtering Version	0000.00.00.000
GlobalProtect Clientless VPN Version	0
Time	Fri Sep 27 02:27:37 2024
Uptime	0 days, 0:25:33
Advanced Routing	off

Logged In Admins

Admin	From	Client	Session Start	Idle For
admin	172.16.10.1	Web	09/27/2024 02:09:19	00:18:19s
admin	172.16.10.1	Web	09/27/2024 02:09:16	00:18:21s
chalthu	172.16.10.1	Web	09/27/2024 02:26:42	00:00:38s
chalthu	172.16.10.1	Web	09/27/2024 02:26:40	00:00:57s

Data Logs

No data available.

System Logs

Description	Time
User chalthu logged in via Web from 172.16.10.1 using https	09/27 02:26:42
authenticated for user 'chalthu'. From: 172.16.10.1	09/27 02:26:41
User chalthu logged in via Web from 172.16.10.1 using https	09/27 02:26:40
authenticated for user 'chalthu'. From: 172.16.10.1	09/27 02:26:40
User admin logged out via Web from 172.16.10.1	09/27 02:26:22
Commit job succeeded. Completion time: 2024/09/27 02:24:59.	09/27 02:24:58
Hostname changed to Batch22-Firewall	09/27 02:23:25
SSLMGR daemon configuration load phase-2 succeeded.	09/27 02:23:21
SATD daemon configuration load phase-2 succeeded.	09/27 02:23:21
RASMGR daemon configuration load phase-2 succeeded.	09/27 02:23:21

Config Logs

Command	Path	Admin	Time
commit		admin	09/27 02:20:42
commit		admin	09/27 01:45:18

Locks

No locks found

ACC Risk Factor (Last 60 minutes)

No data found

chalthu | Logout | Last Login Time: 09/27/2024 02:26:40 | Session Expires Time: 10/27/2024 02:26:42 | Your role has been changed since last login. | Tasks | Language | paloalto 14:21 26-09-2024

Thank You