



CYBERSECURITY FOUNDATION

Lab 4: Configuring Authentication

Document Version: 2021-01-22

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Palo Alto Networks and the Palo Alto Networks logo are trademarks or registered trademarks of Palo Alto Networks, Inc.

Contents

Introduction	3
Objective	3
Lab Topology	4
Lab Settings	5
4 Configuring Authentication.....	6
4.0 Load Lab Configuration	6
4.1 Configure a Local User Account and Authentication Profile	11
4.2 Enable the Captive Portal and Enable Web-Form based Logins	15
4.3 Create an Authentication Policy	19
4.4 Commit and Test Authentication Policy	22

Introduction

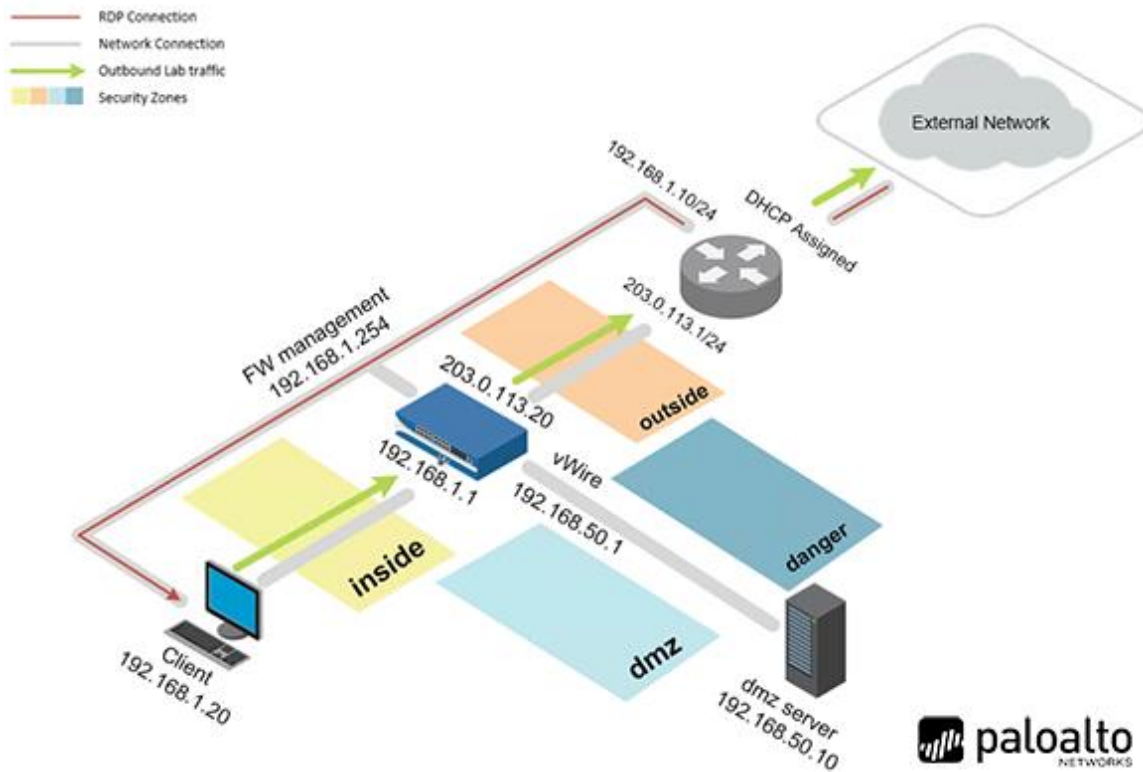
In this lab, you will configure the Firewall to use a Captive Portal to authenticate users by using a local user account and Authentication Policy.

Objective

In this lab, you will perform the following tasks:

- Configure a Local User Account and Authentication Profile
- Enable the Captive Portal and Enable Web-Form based Logins
- Create an Authentication Policy
- Commit and Test Authentication Policy

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

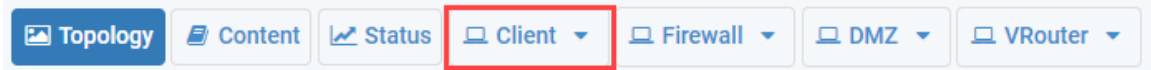
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng\$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng\$

4 Configuring Authentication

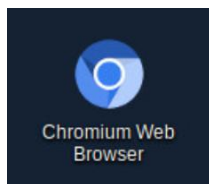
4.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

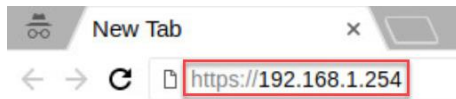
1. Click on the **Client** tab to access the Client PC.



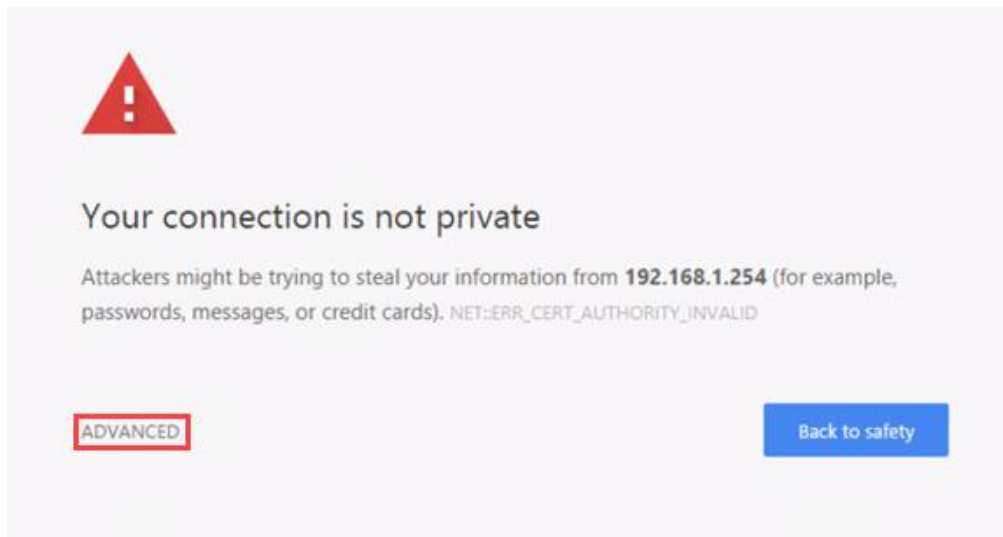
2. Log in to the Client PC as username **lab-user**, password **Train1ng\$**.
3. Double-click the **Chromium Web Browser** icon located on the Desktop.



4. In the *Chromium* address field, type **https://192.168.1.254** and press **Enter**.



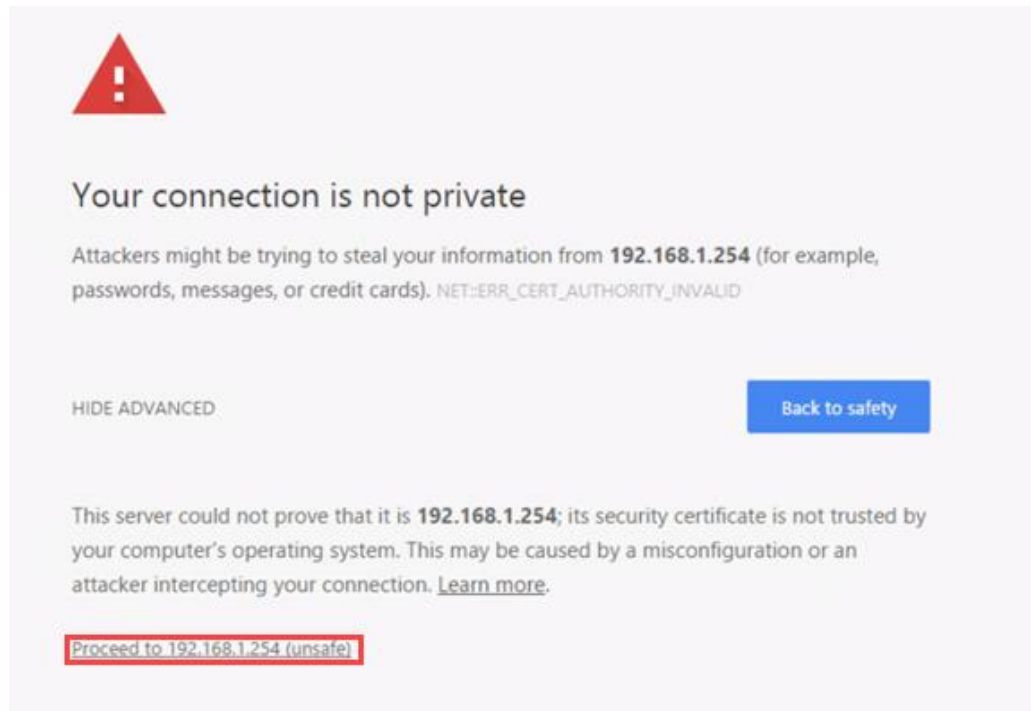
5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.





If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

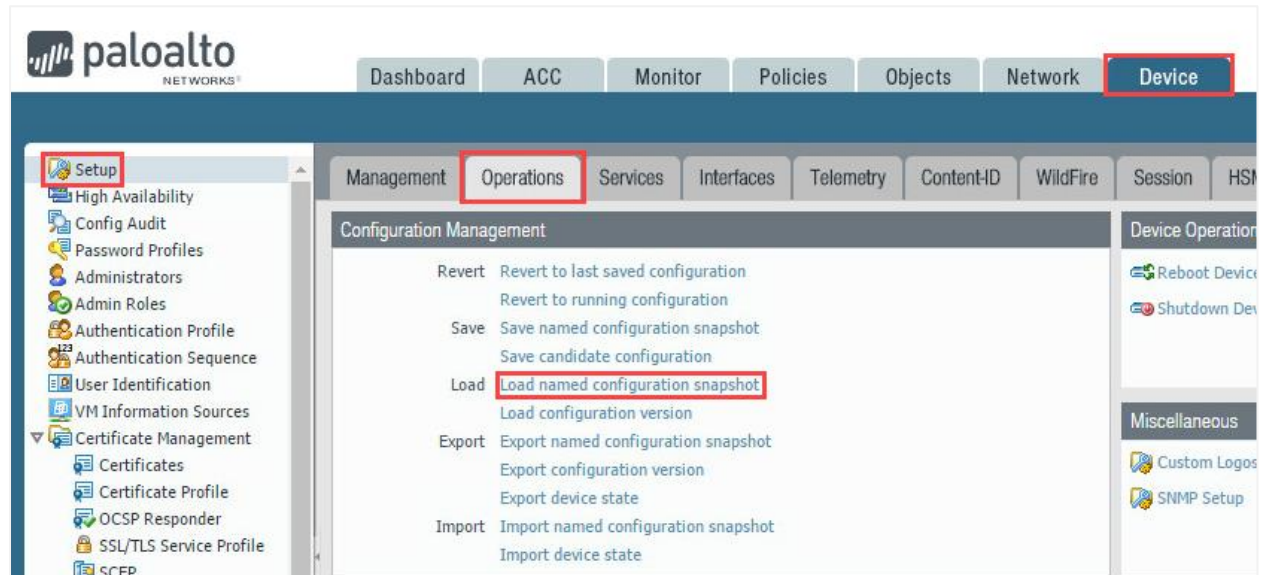
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



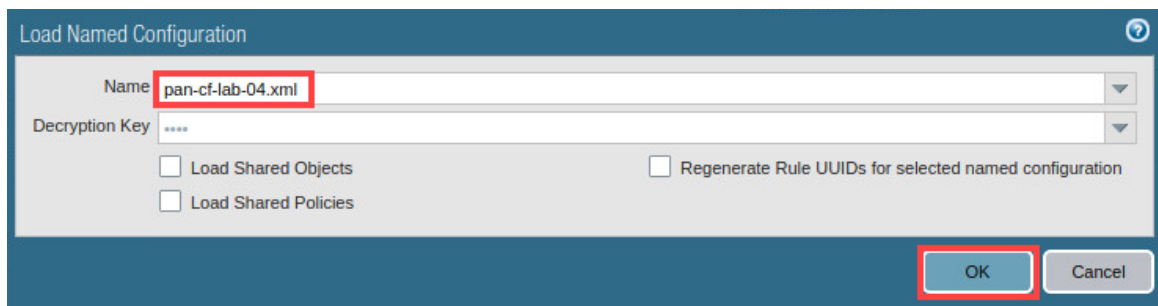
7. Log in to the Firewall web interface as username **admin**, password **Train1ng\$**.



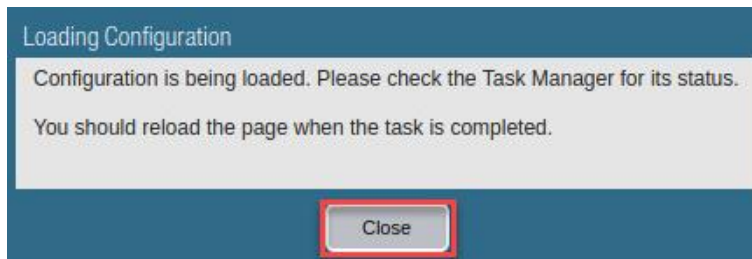
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



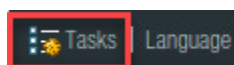
9. In the *Load Named Configuration* window, select **pan-cf-lab-04.xml** from the *Name* dropdown box and click **OK**.



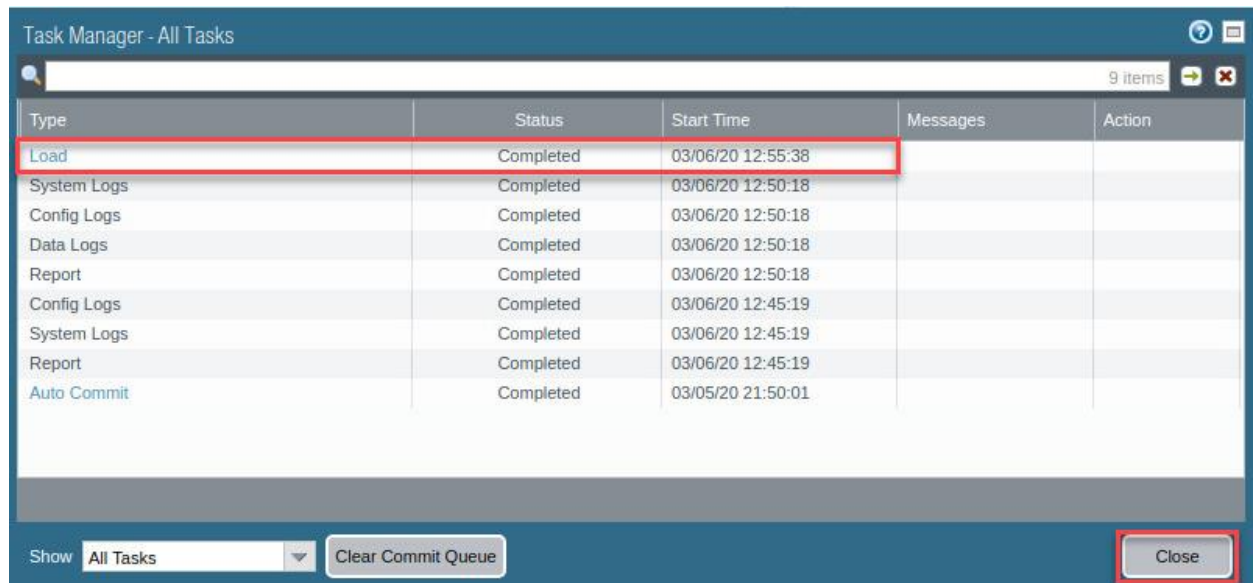
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



11. Click the **Tasks** icon located at the bottom-right of the web interface.



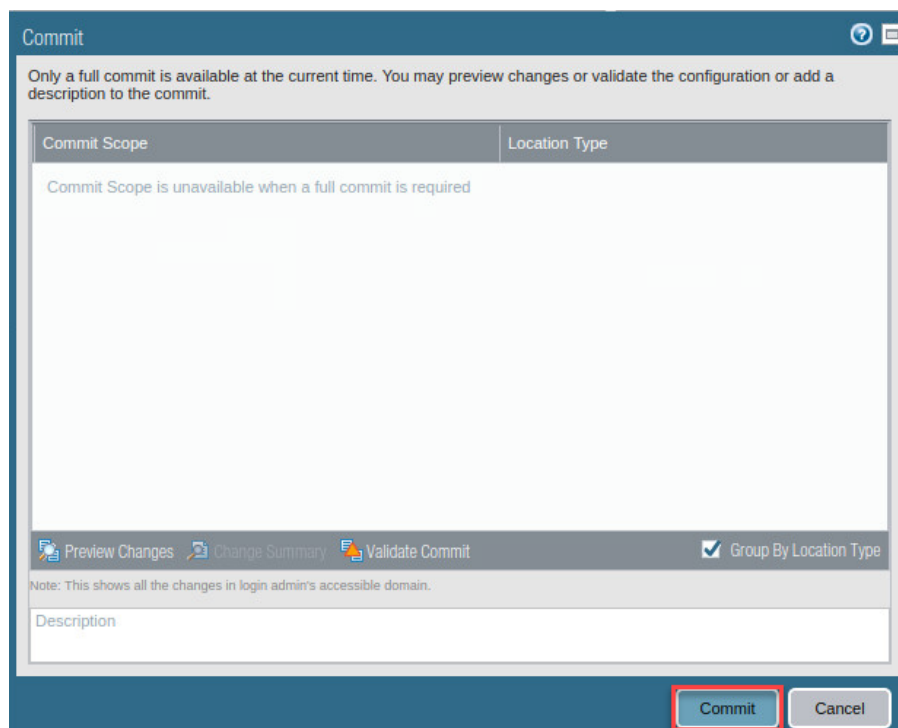
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



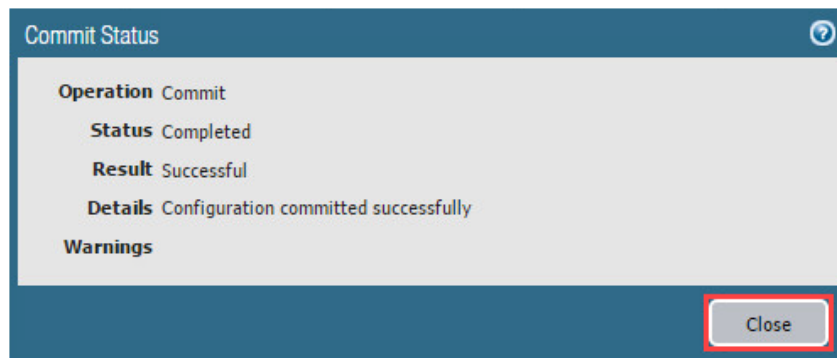
13. Click the **Commit** link located at the top-right of the web interface.



14. In the *Commit* window, click **Commit** to proceed with committing the changes.



15. When the commit operation successfully completes, click **Close** to continue.

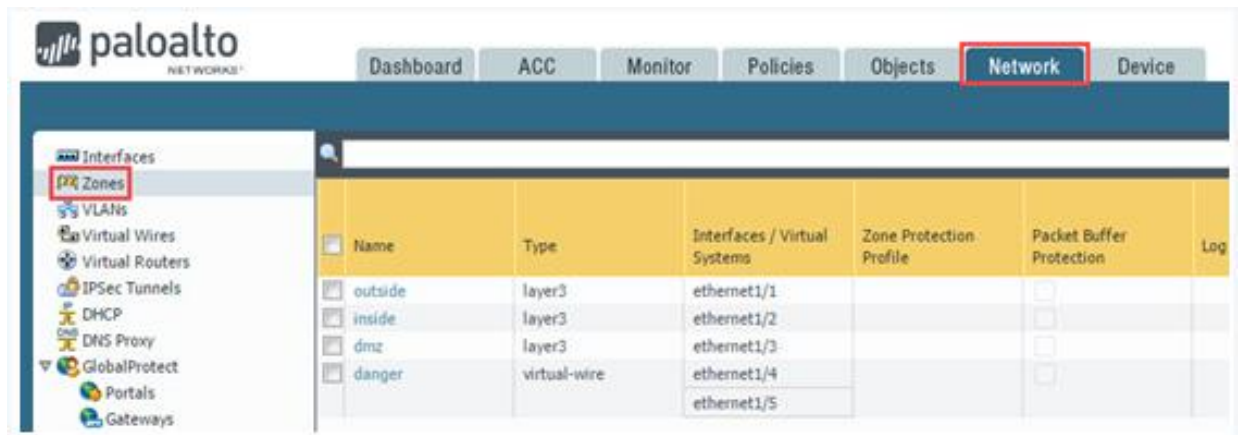


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

4.1 Configure a Local User Account and Authentication Profile

In this section, you will configure a local user account. Then, you will create a local authentication profile, which will later be assigned to a security policy.

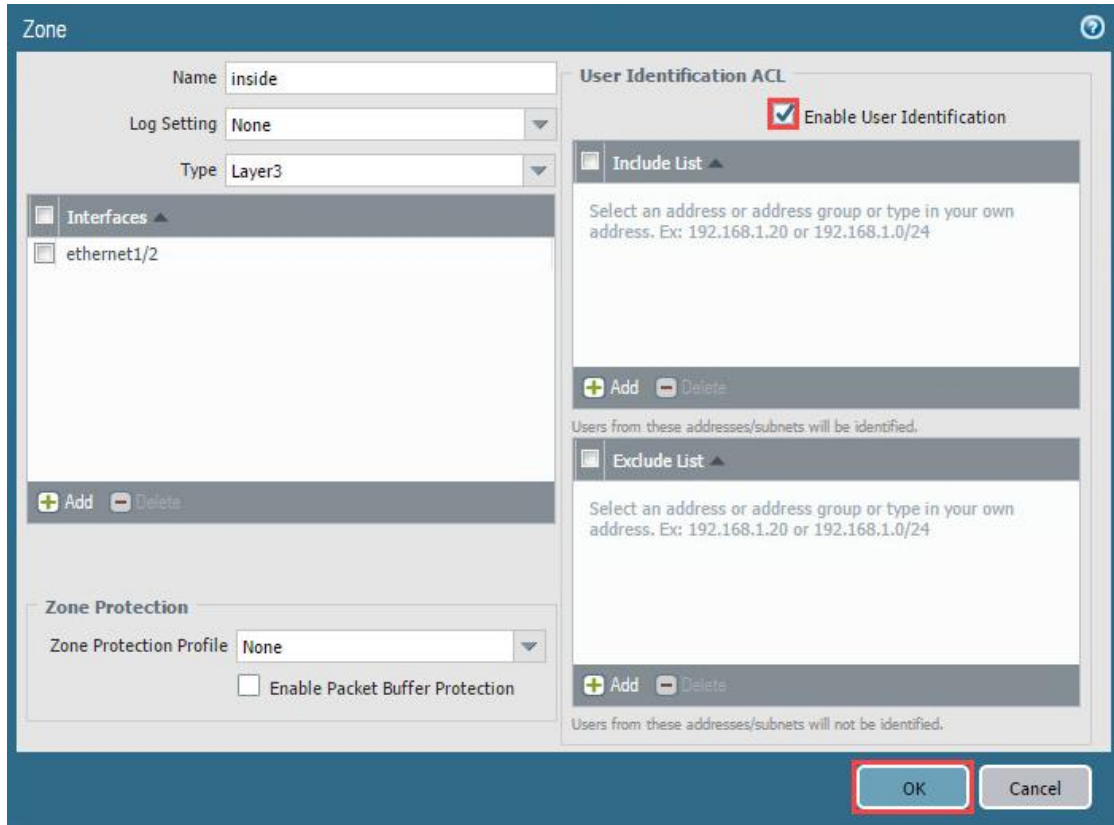
1. Navigate to **Network > Zones**.



2. Click on the **inside** zone.

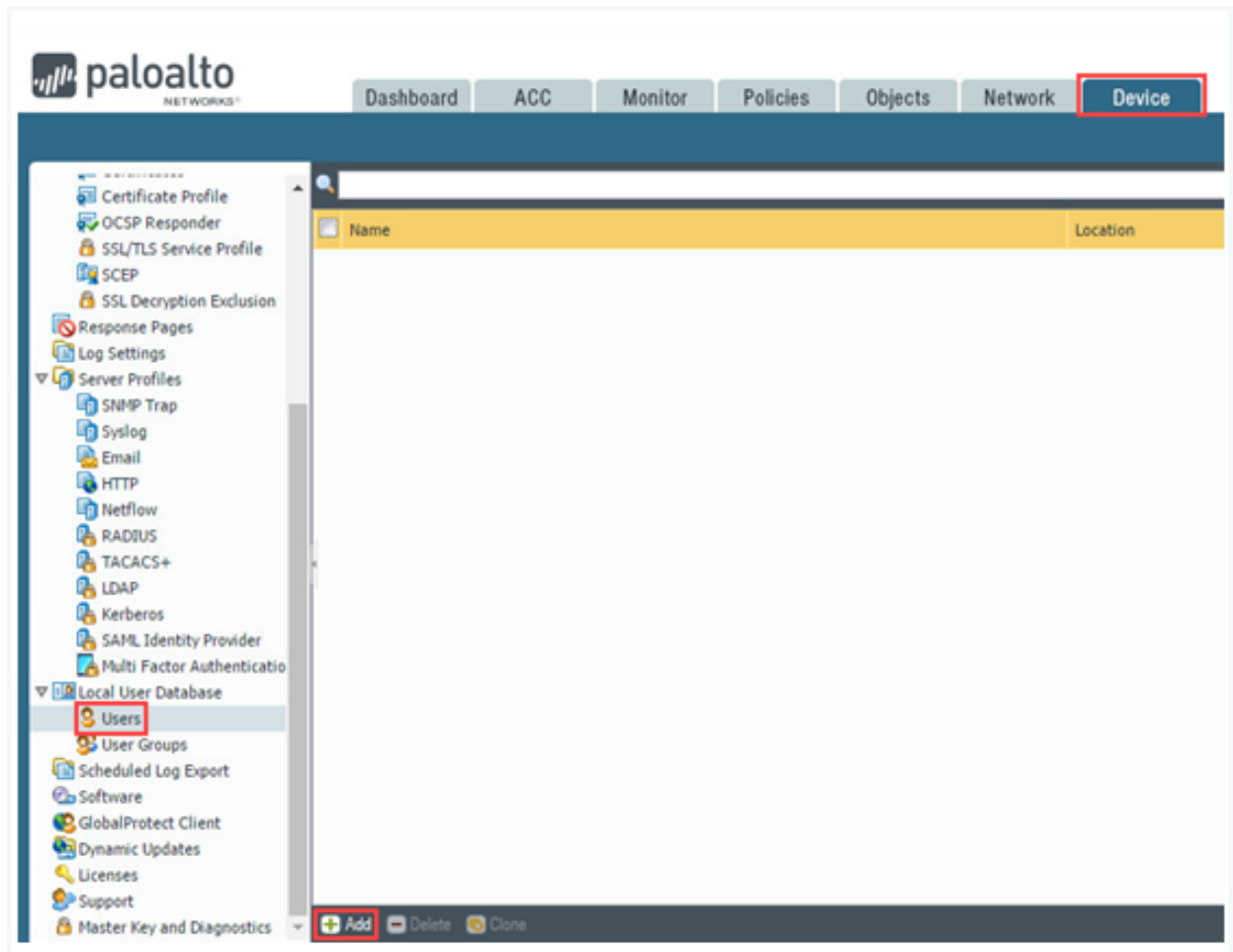
<input type="checkbox"/>	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection
<input type="checkbox"/>	outside	layer3	ethernet1/1		<input type="checkbox"/>
<input type="checkbox"/>	inside	layer3	ethernet1/2		<input type="checkbox"/>
<input type="checkbox"/>	dmz	layer3	ethernet1/3		<input type="checkbox"/>
<input type="checkbox"/>	danger	virtual-wire	ethernet1/4		<input type="checkbox"/>
			ethernet1/5		

3. In the *Zone* window, click the **Enable User Identification** checkbox under the *User Identification ACL*. Then, click the **OK** button.

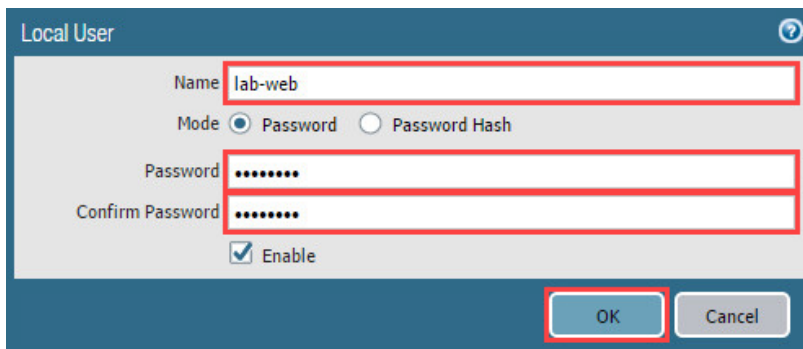


This will enable the inside zone to use a Username for authentication.

4. Navigate to **Device > Local User Database > Users > Add**. You may need to scroll down on the left pane.

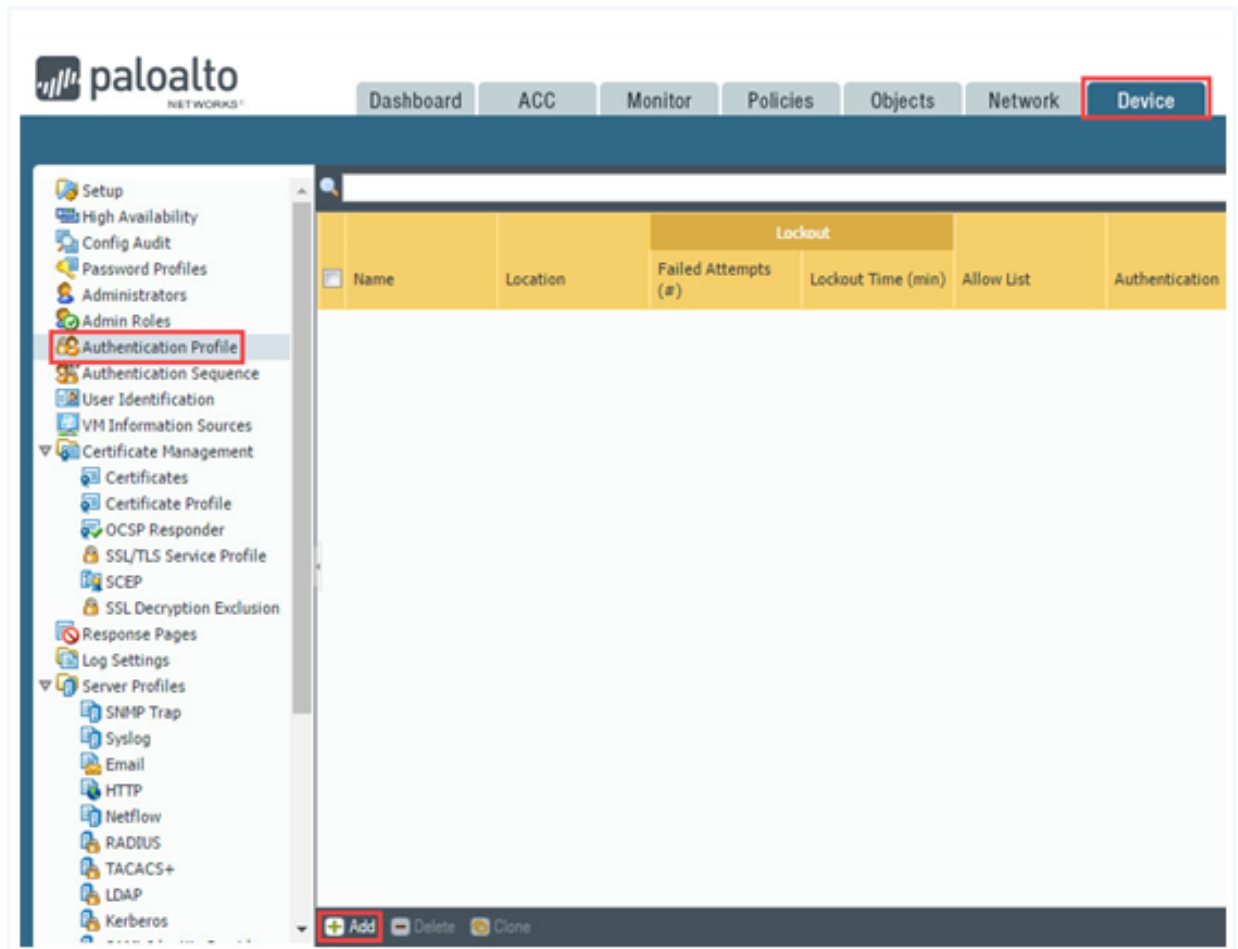


5. In the *Local User* window, type **lab-web** in the *Name* field. Then, type **pa10a1t0** in the *Password* and *Confirm Password* fields. Finally, click the **OK** button.

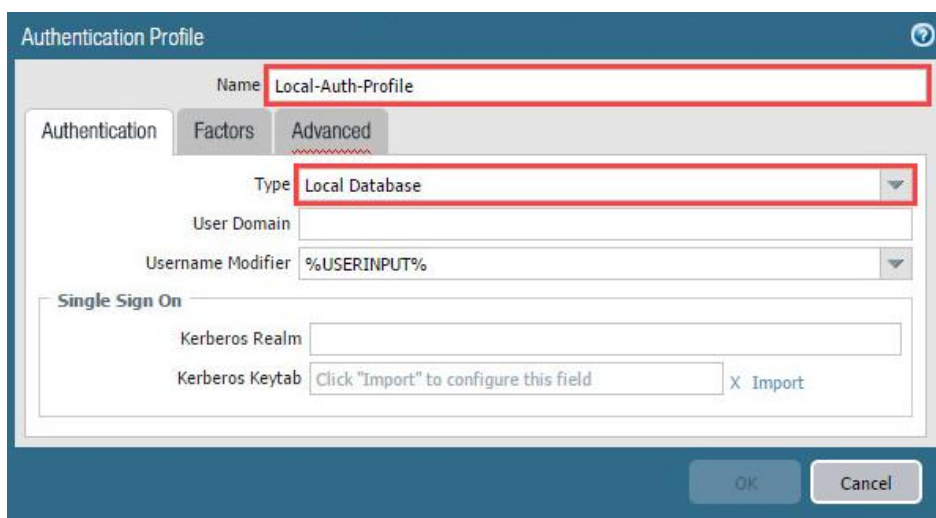


The screenshot shows the 'Local User' configuration window. The 'Name' field contains 'lab-web'. The 'Mode' is set to 'Password'. The 'Password' and 'Confirm Password' fields both contain 'pa10a1t0'. The 'Enable' checkbox is checked. The 'OK' button is highlighted with a red box.

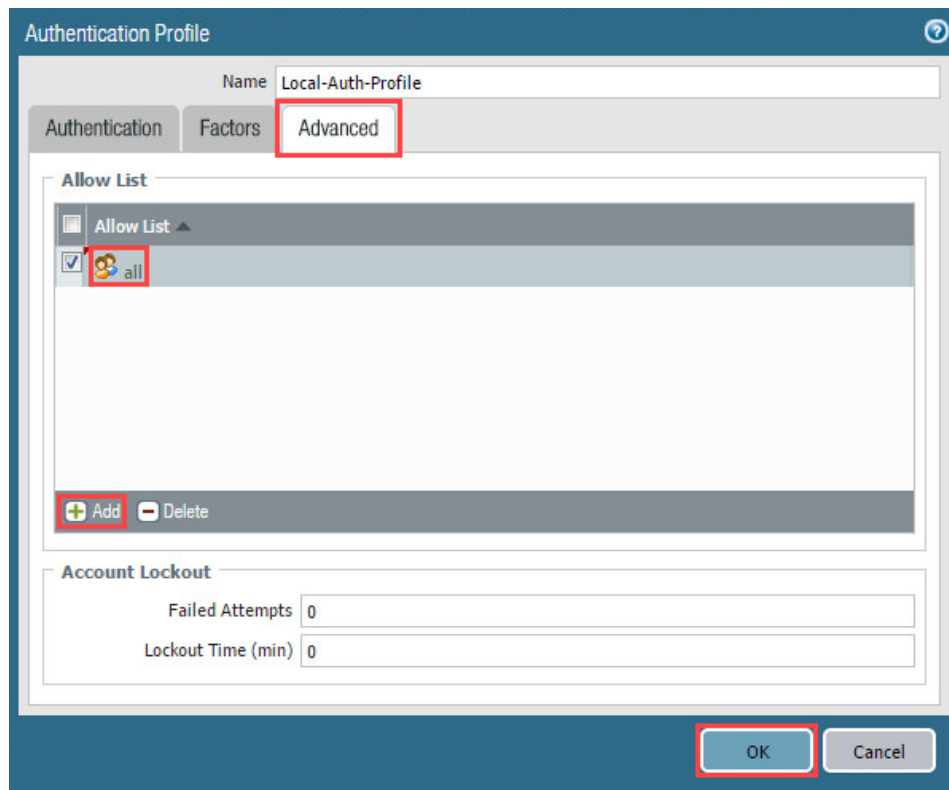
6. Navigate to **Device > Authentication Profile > Add**. You may need to scroll up on the left pane.



7. In the *Authentication Profile* window, type **Local-Auth-Profile** in the *Name* field. Then, select **Local Database** from the *Type* dropdown.



- In the *Authentication Profile* window, click on the **Advanced** tab. Then, click on the **Add** button. Next, select **all** from the dropdown in the *Allow List* column. Finally, click the **OK** button.



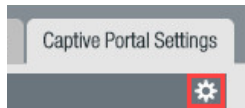
4.2 Enable the Captive Portal and Enable Web-Form based Logins

In this section, you will enable a captive portal. In that captive portal, you will use a web-form for login.

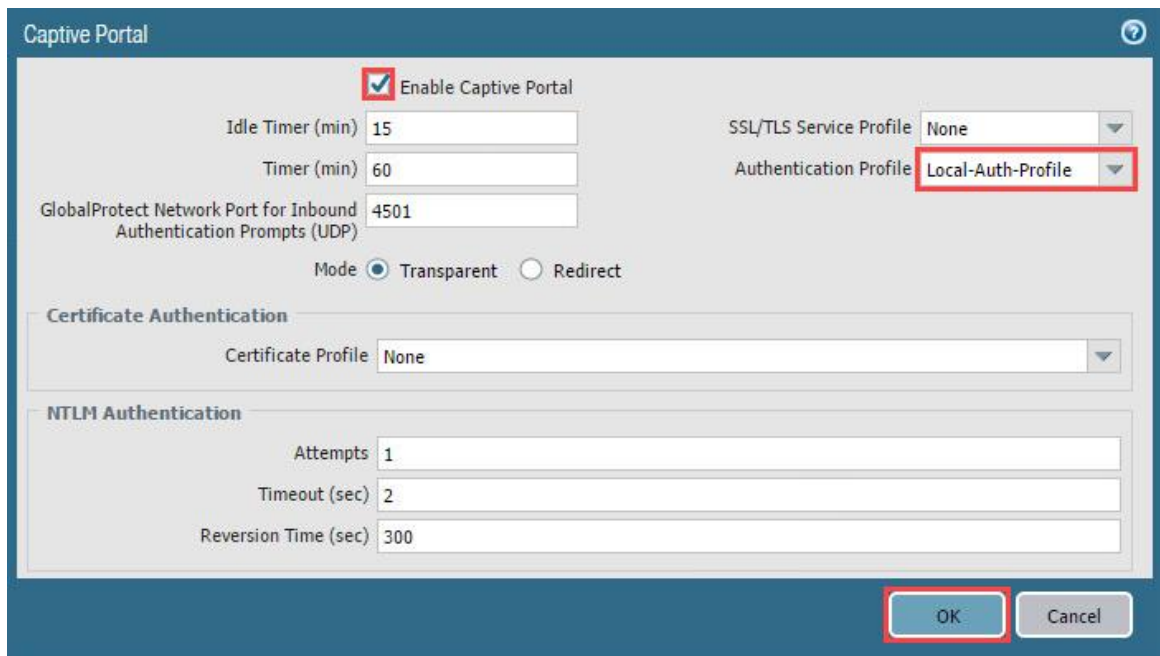
- Navigate to **Device > User Identification > Captive Portal Settings**.



2. Under the *Captive Portal Settings* tab, click on the **gear** icon.

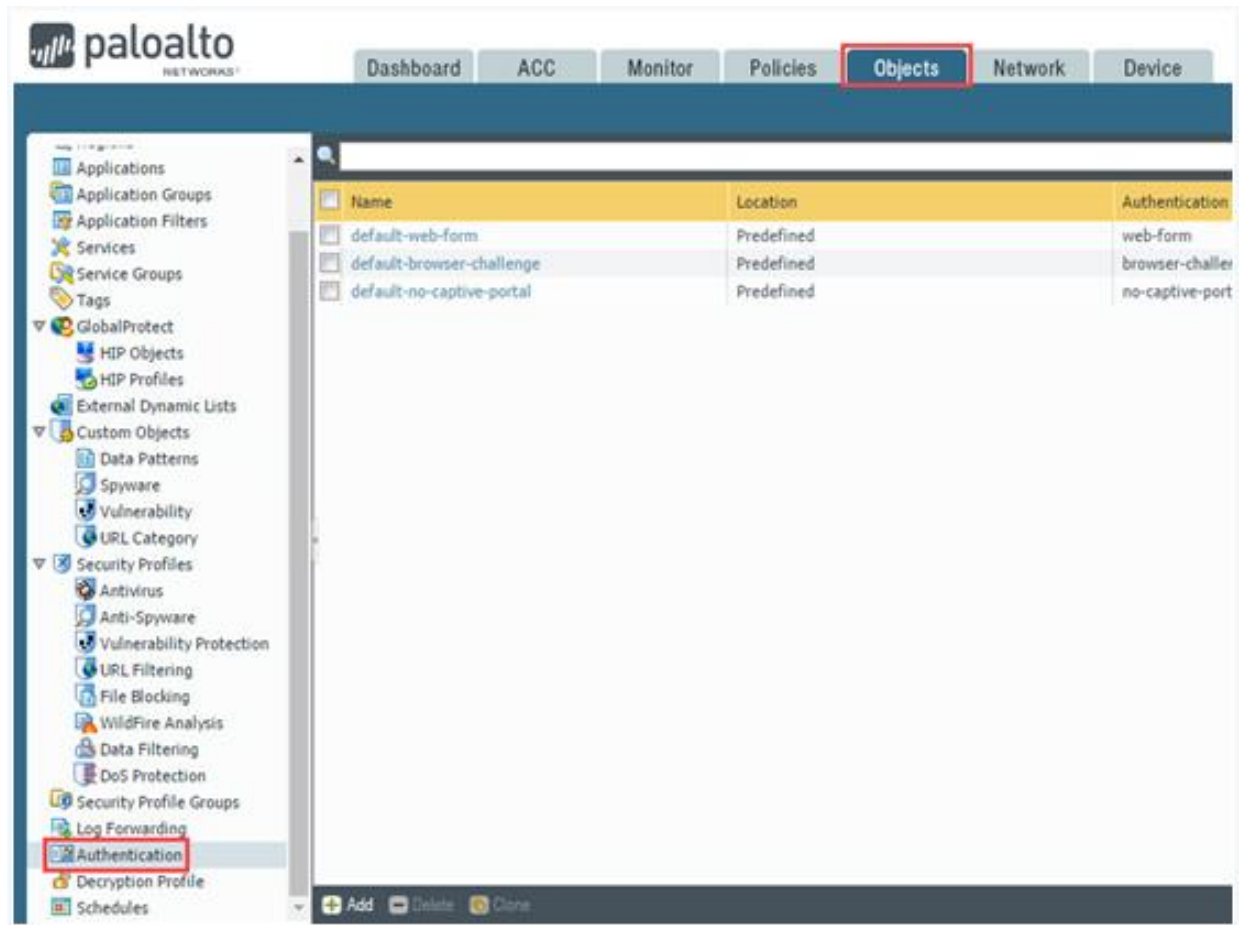


3. In the *Captive Portal* window, click the **Enable Captive Portal** checkbox. Then, select **Local-Auth-Profile** from the *Authentication Profile* dropdown. Finally, click the **OK** button.

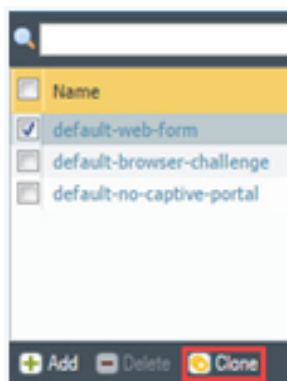
A screenshot of the 'Captive Portal' configuration window. The 'Enable Captive Portal' checkbox is checked and highlighted with a red box. The 'Authentication Profile' dropdown menu is open, showing 'Local-Auth-Profile' selected, also highlighted with a red box. Other fields include 'Idle Timer (min)' set to 15, 'Timer (min)' set to 60, 'GlobalProtect Network Port for Inbound Authentication Prompts (UDP)' set to 4501, 'Mode' set to 'Transparent', 'Certificate Profile' set to 'None', 'Attempts' set to 1, 'Timeout (sec)' set to 2, and 'Reversion Time (sec)' set to 300. The 'OK' button at the bottom right is highlighted with a red box.

This will turn on the Captive Portal for web-form logins and associate it with the **Local-Auth-Profile** you created earlier.

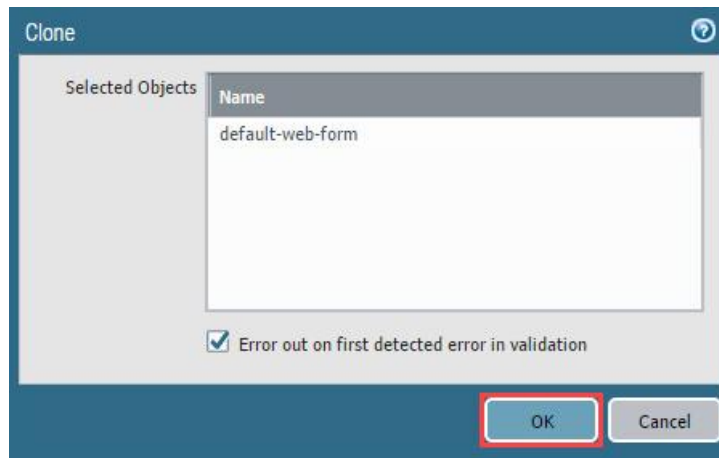
4. Navigate to **Objects > Authentication**. You may need to scroll down on the left pane.



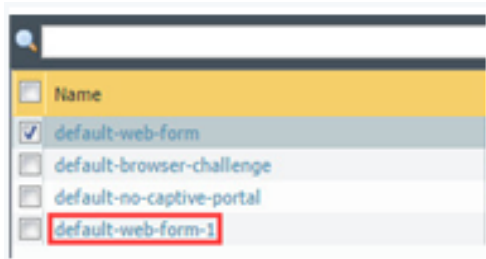
5. Click the checkbox beside the **default-web-form** and click **Clone**.



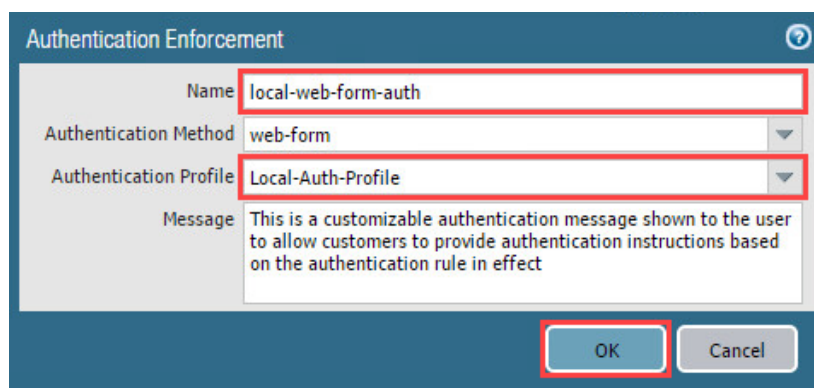
6. In the *Clone* window, click the **OK** button to confirm the clone.



7. You will notice a new entry named default-web-form-1 has been created; click on **default-web-form-1**.



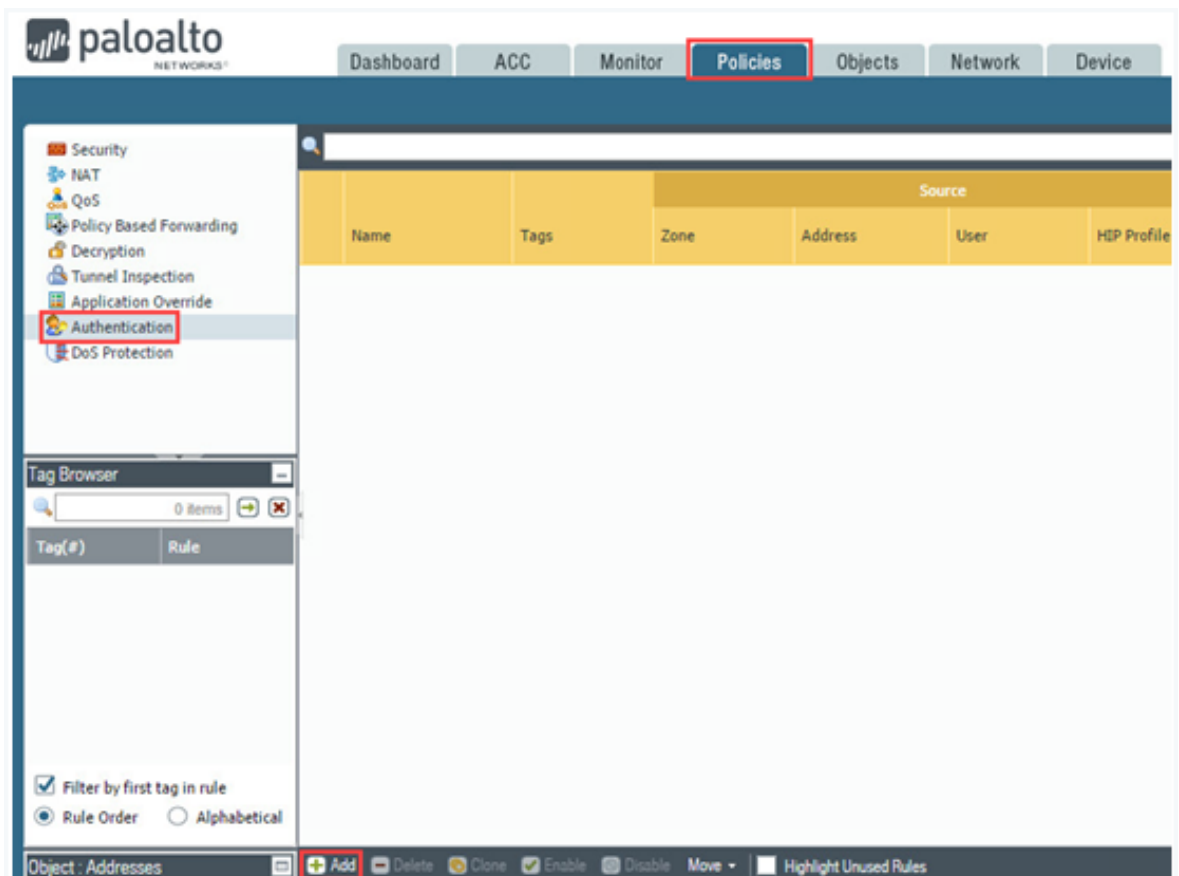
8. In the *Authentication Enforcement* window, type **local-web-form-auth** in the *Name* field. Then, select **Local-Auth-Profile** in the *Authentication Profile* dropdown. Next, click the **OK** button.



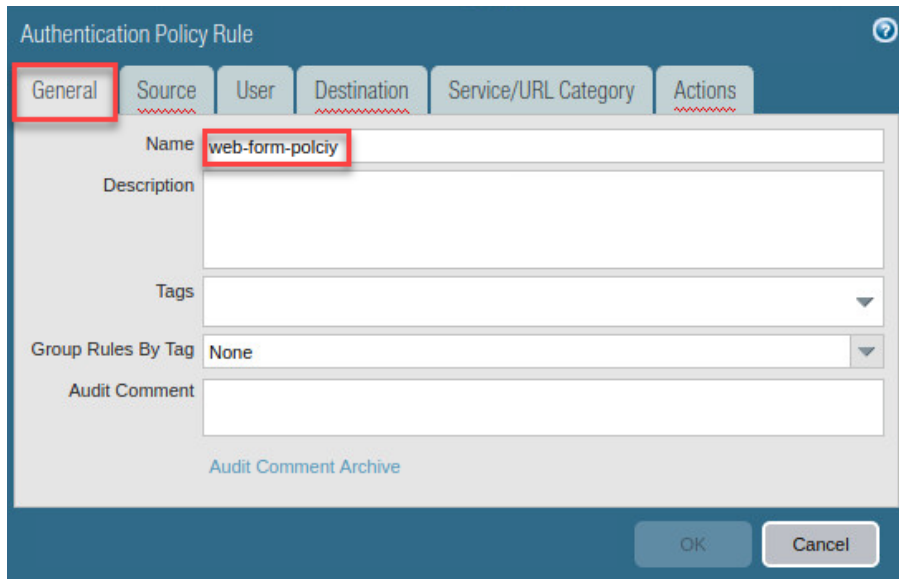
4.3 Create an Authentication Policy

In this section, you will enable a captive portal. A captive portal redirects web requests that match the authentication policy and forces the user to use a login to continue. This is typically seen in corporate guest networks, hotels, and Wi-Fi hotspots. In this captive portal, you will use a web-form for login.

1. Navigate to **Policies > Authentication > Add**.

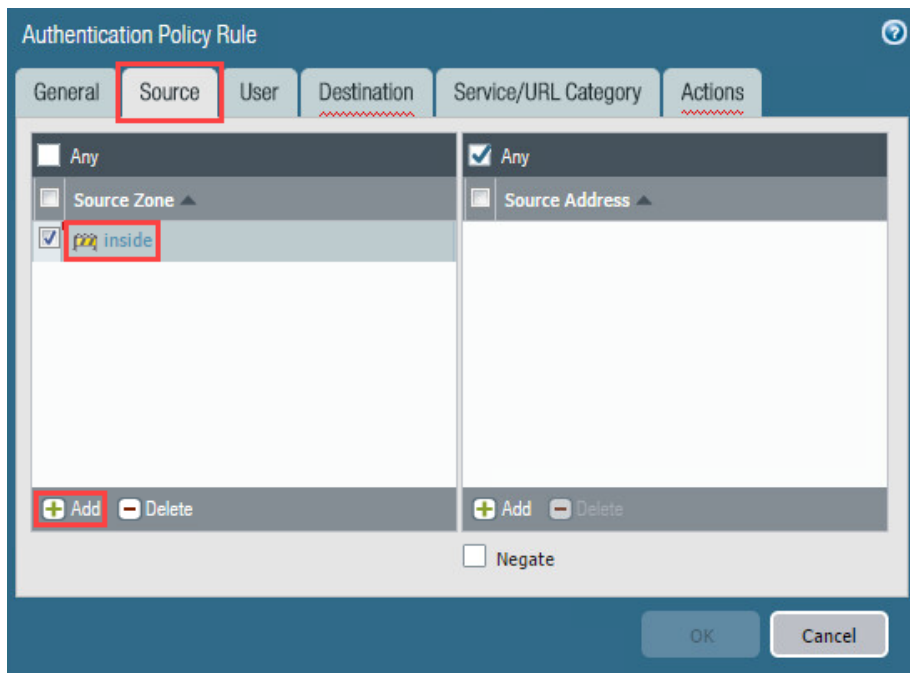


2. In the *Authentication Policy Rule* window, type `web-form-policy` in the *Name* field.



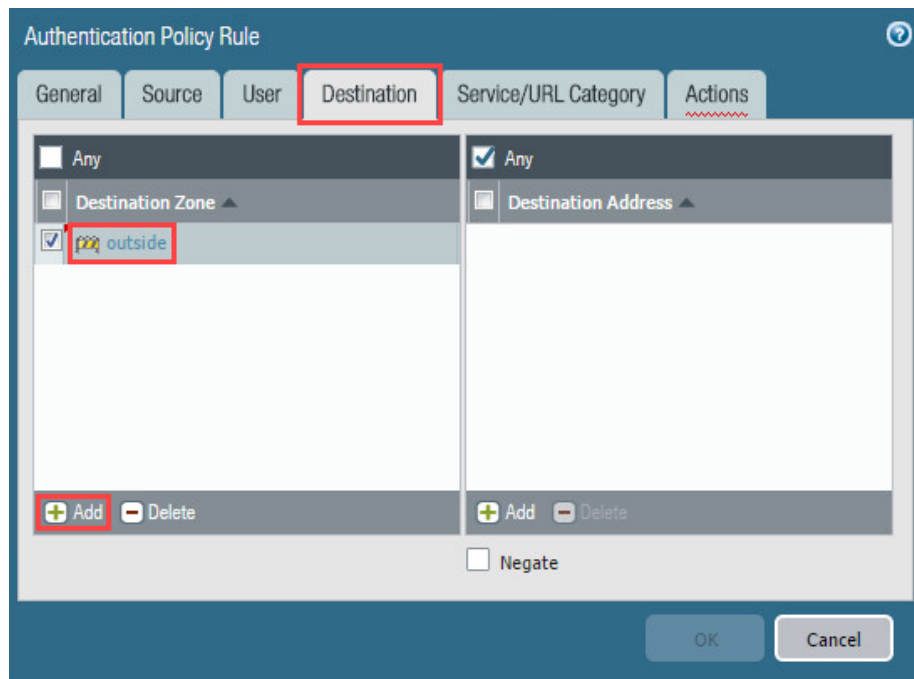
The screenshot shows the 'Authentication Policy Rule' window with the 'General' tab selected. The 'Name' field contains the text 'web-form-policy'. The 'Description' field is empty. The 'Tags' field is empty. The 'Group Rules By Tag' dropdown is set to 'None'. The 'Audit Comment' field is empty. There is a link for 'Audit Comment Archive' below the field. At the bottom right are 'OK' and 'Cancel' buttons.

3. In the *Authentication Policy Rule* window, click on the **Source** tab. Then, click the **Add** button in the *Source Zone* section. Next, select **inside**.

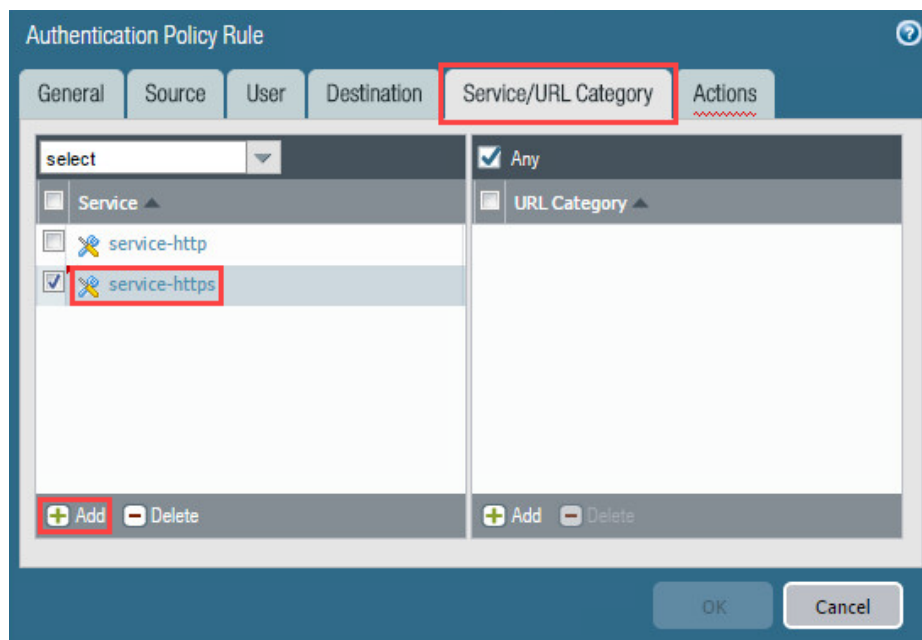


The screenshot shows the 'Authentication Policy Rule' window with the 'Source' tab selected. The 'Source Zone' section has a list with 'Any' and 'inside'. The 'inside' item is selected and highlighted. Below the list are 'Add' and 'Delete' buttons. The 'Source Address' section has a list with 'Any' and is checked. Below it are 'Add' and 'Delete' buttons. At the bottom is a 'Negate' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

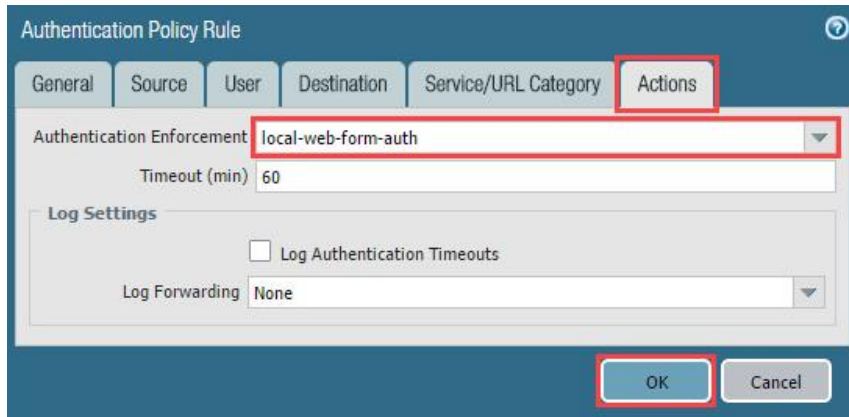
4. In the *Authentication Policy Rule* window, click on the **Destination** tab. Then, click the **Add** button in the *Destination Zone* section. Next, select **outside**.



5. In the *Authentication Policy Rule* window, click on the **Service/URL Category** tab. Then, click on the **Add** button in the *Service* section. Next, select **service-https**.



- In the *Authentication Policy Rule* window, click on the **Actions** tab. Then, select **local-web-form-auth** from the *Authentication Enforcement* dropdown. Then, click the **OK** button.



Authentication Policy Rule

General Source User Destination Service/URL Category **Actions**

Authentication Enforcement: local-web-form-auth

Timeout (min): 60

Log Settings

☐ Log Authentication Timeouts

Log Forwarding: None

OK Cancel

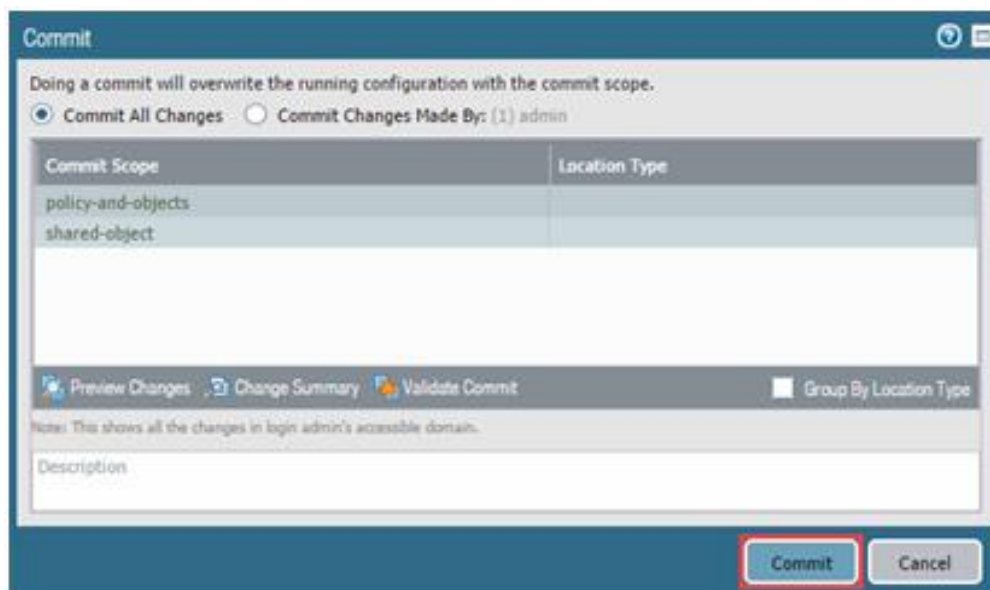
4.4 Commit and Test Authentication Policy

In this section, you will commit your changes and test the authentication policy with the captive portal.

- Click the **Commit** link located at the top-right of the web interface.



- In the *Commit* window, click **Commit** to proceed with committing the changes.



Commit

Doing a commit will overwrite the running configuration with the commit scope.

☒ Commit All Changes ☐ Commit Changes Made By: (1) admin

Commit Scope	Location Type
policy-and-objects	
shared-object	

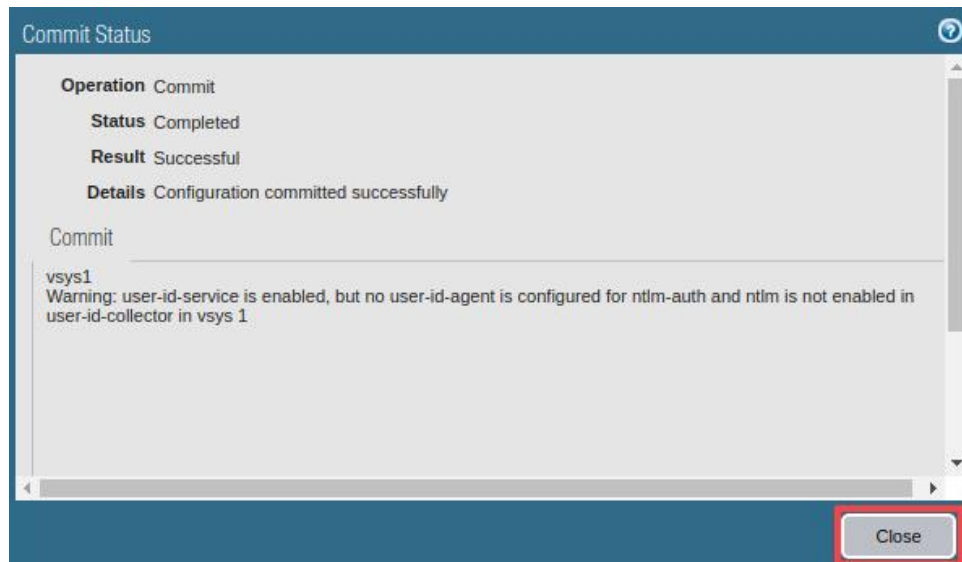
Preview Changes Change Summary Validate Commit ☐ Group By Location Type

Note: This shows all the changes in login admin's accessible domain.

Description

Commit Cancel

- When the commit operation successfully completes, click **Close** to continue.

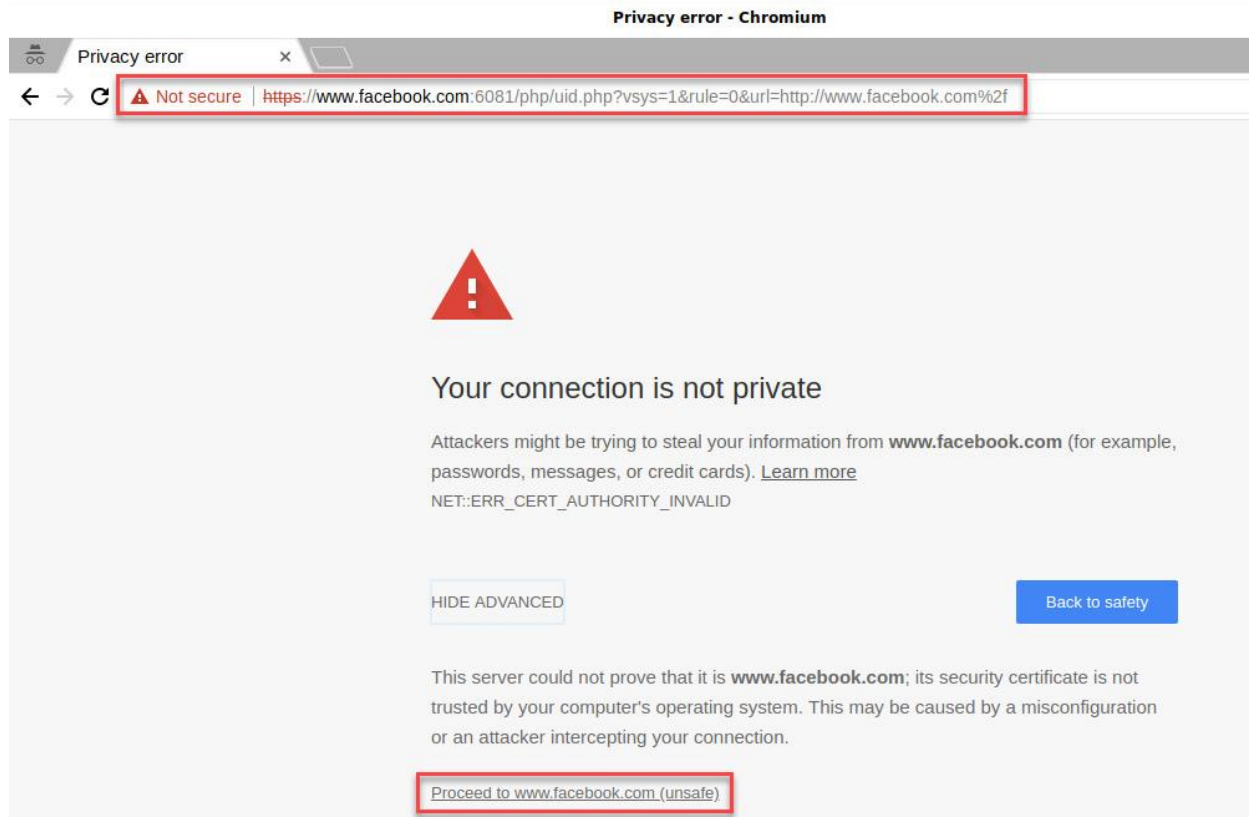


You will see a **vsys1** in Warnings, which refers to a virtual system in the Firewall. You can ignore it in this lab environment.

- Open a second **Chromium Web Browser** from the taskbar.

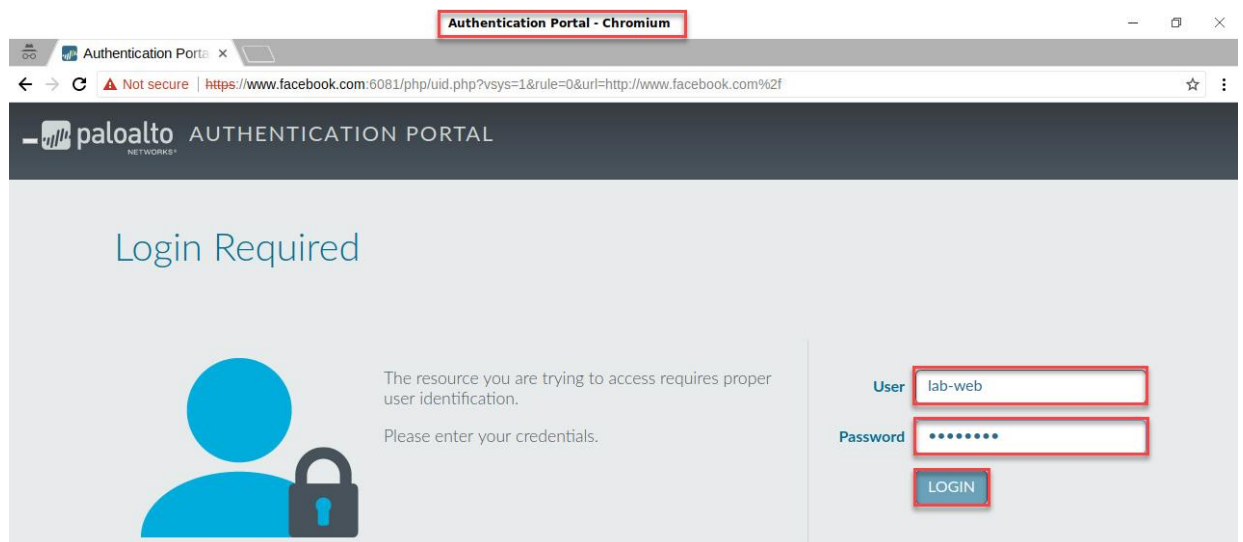


5. In the address bar, type `http://www.facebook.com` and press **Enter**. You will need to confirm the certificate error, click **Advanced** and then click **Proceed to `www.facebook.com(unsafe)`**.

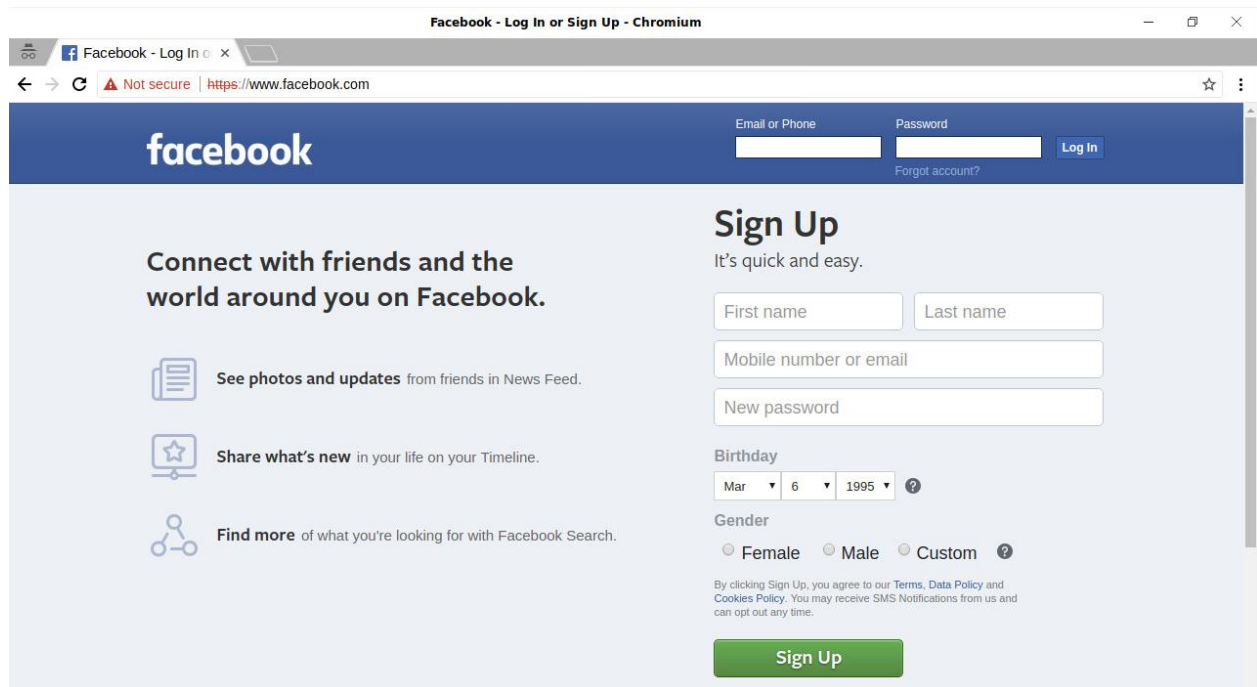


You are seeing this error because the Firewall is intercepting traffic coming from the inside zone to the outside zone. The Firewall serves as a man-in-the-middle until authenticated.

6. You will see a web-form login, type **lab-web** as the username. Then, type **Pa10A1t0** as the password. Finally, click the **Login** button.



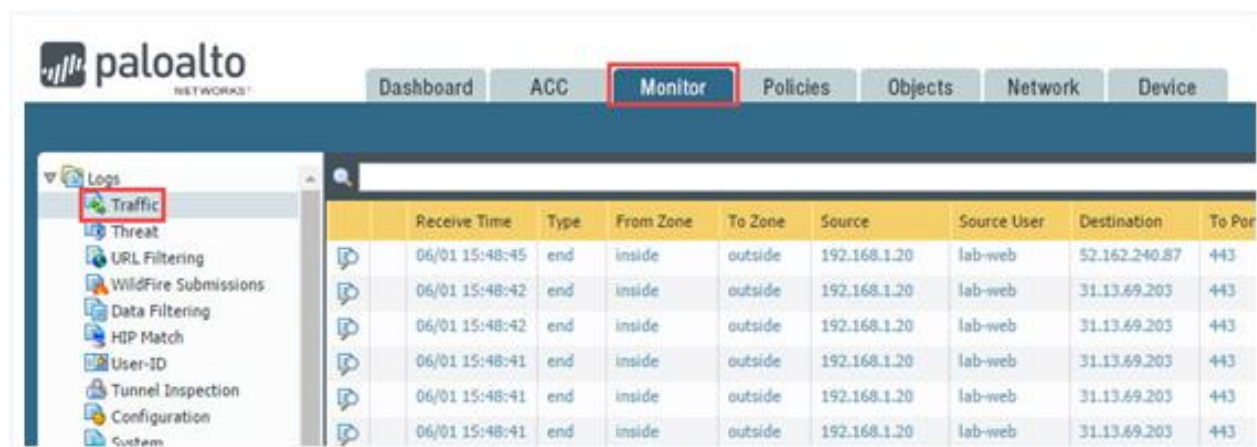
7. You will then see Facebook after you successfully authenticate to the Firewall as **lab-web**.

















8. Click the **X** in the upper-right to close **Chromium**.



9. Navigate to **Monitor > Logs > Traffic**.



10. In the logs, you will see that the entries to **facebook-base** are associated with the **lab-web** user. You may need to manually refresh logs or check additional pages at the bottom.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	Dynamic User Group	To Port	Application
	01/18 05:28:07	end	inside	outside	192.168.1.20	lab-web	66.175.211.68		123	ntp
	01/18 05:28:07	end	inside	outside	192.168.1.20	lab-web	162.159.200.1		123	ntp
	01/18 05:28:05	end	inside	outside	192.168.1.20	lab-web	8.8.8.8		53	dns
	01/18 05:28:05	end	inside	outside	192.168.1.20	lab-web	8.8.8.8		53	dns
	01/18 05:28:01	end	inside	outside	192.168.1.20	lab-web	91.189.89.199		123	ntp
	01/18 05:27:57	end	inside	outside	192.168.1.20	lab-web	8.8.8.8		53	dns
	01/18 05:27:56	end	inside	outside	192.168.1.20	lab-web	8.8.8.8		53	dns
	01/18 05:27:56	end	inside	outside	192.168.1.20	lab-web	8.8.8.8		53	dns
	01/18 05:27:56	end	inside	outside	192.168.1.20	lab-web	8.8.8.8		53	dns
	01/18 05:27:56	end	inside	outside	192.168.1.20	lab-web	8.8.8.8		53	dns
	01/18 05:27:51	end	inside	outside	192.168.1.20	lab-web	31.13.66.19		443	facebook-base
	01/18 05:27:51	end	inside	outside	192.168.1.20	lab-web	31.13.66.19		443	facebook-base
	01/18 05:27:51	end	inside	outside	192.168.1.20	lab-web	31.13.66.19		443	facebook-base
	01/18 05:27:51	end	inside	outside	192.168.1.20	lab-web	35.232.111.17		80	web-browsing

11. The lab is now complete; you may end the reservation.