



PAN8 CYBERSECURITY ESSENTIALS

Lab 2: Configuring Authentication

Document Version: **2018-07-02**

Copyright © 2018 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition, and NETLAB+ are registered trademarks 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
2 Lab: Configuring Authentication	6
2.0 Load Lab Configuration	6
2.1 Configure a Local User Account and Authentication Profile.....	9
2.2 Enable the Captive Portal and Enable Web-Form based Logins.....	13
2.3 Create an Authentication Policy.....	17
2.4 Commit and Test Authentication Policy.....	20

Introduction

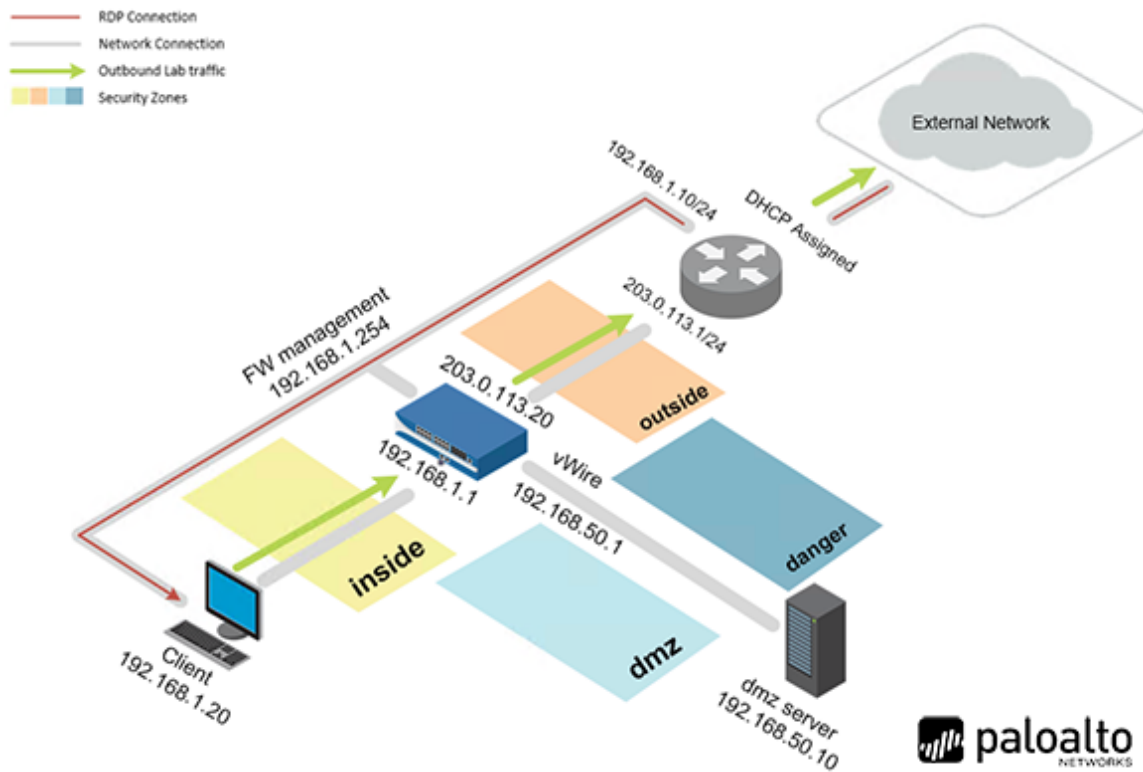
In this lab, you will configure the Firewall to use a Captive Portal to authenticate users by using a local user account and Authentication Policy.

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	Pal0Alt0
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	admin

2 Lab: Configuring Authentication

2.0 Load Lab Configuration

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

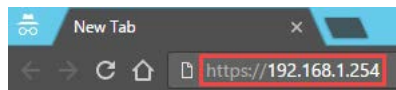
1. Click on the **Client** tab to access the Client PC.



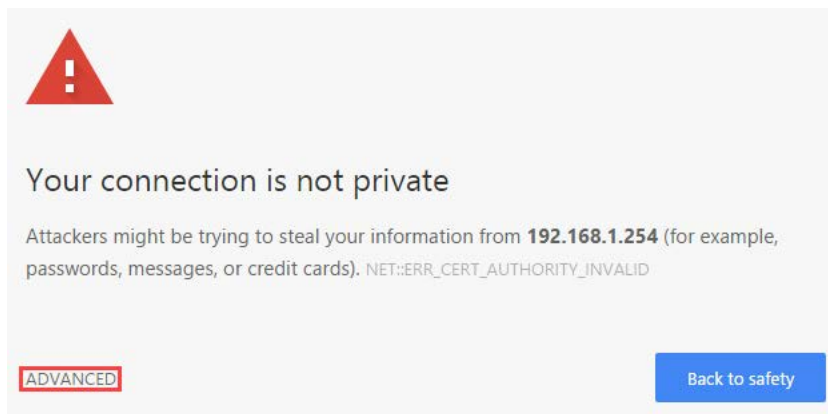
2. Login to the Client machine as username **lab-user**, password **Pa10A1t0**.
3. Double-click the **Google Chrome** icon located on the Desktop.



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

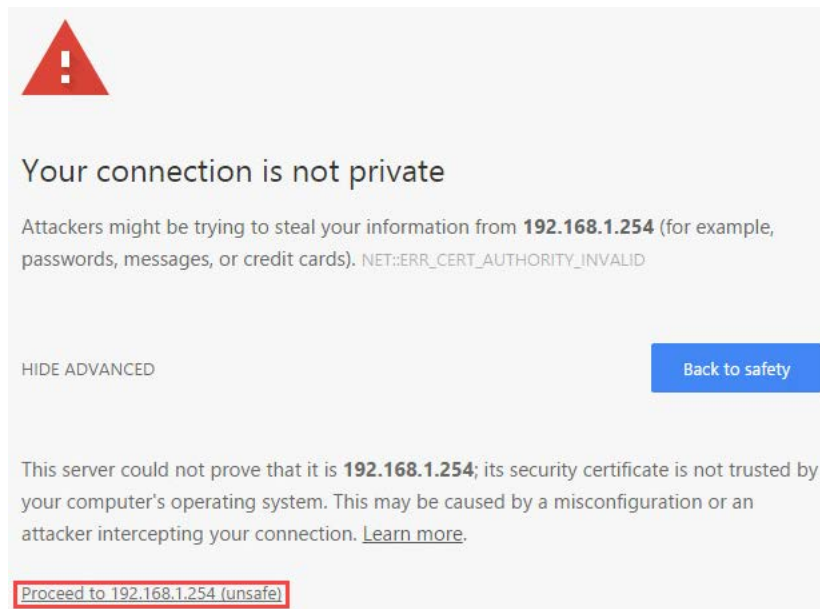


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

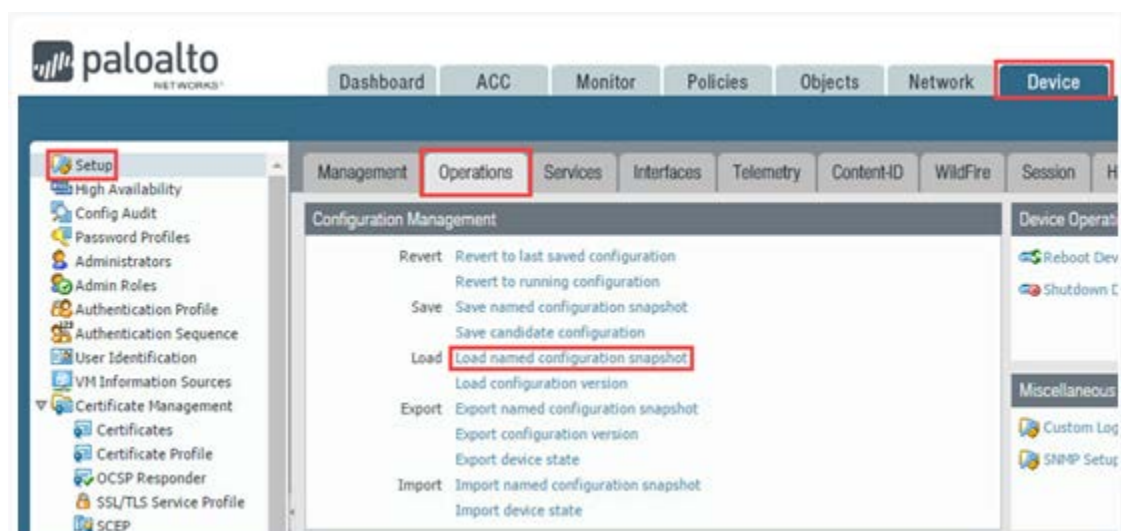
- Click on **Proceed to 192.168.1.254 (unsafe)**.



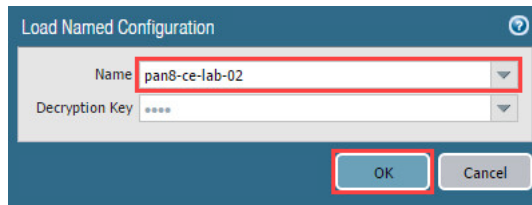
- Login to the Firewall web interface as username **admin**, password **admin**.



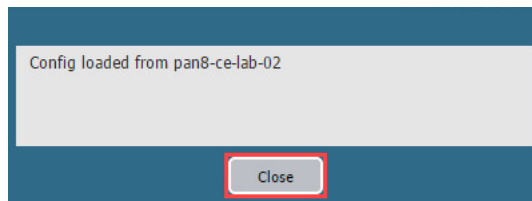
- Navigate to **Device > Setup > Operations > Load named configuration snapshot**.



9. In the *Load Named Configuration* window, select **pan8-ce-lab-02** from the *Name* dropdown box and click **OK**.



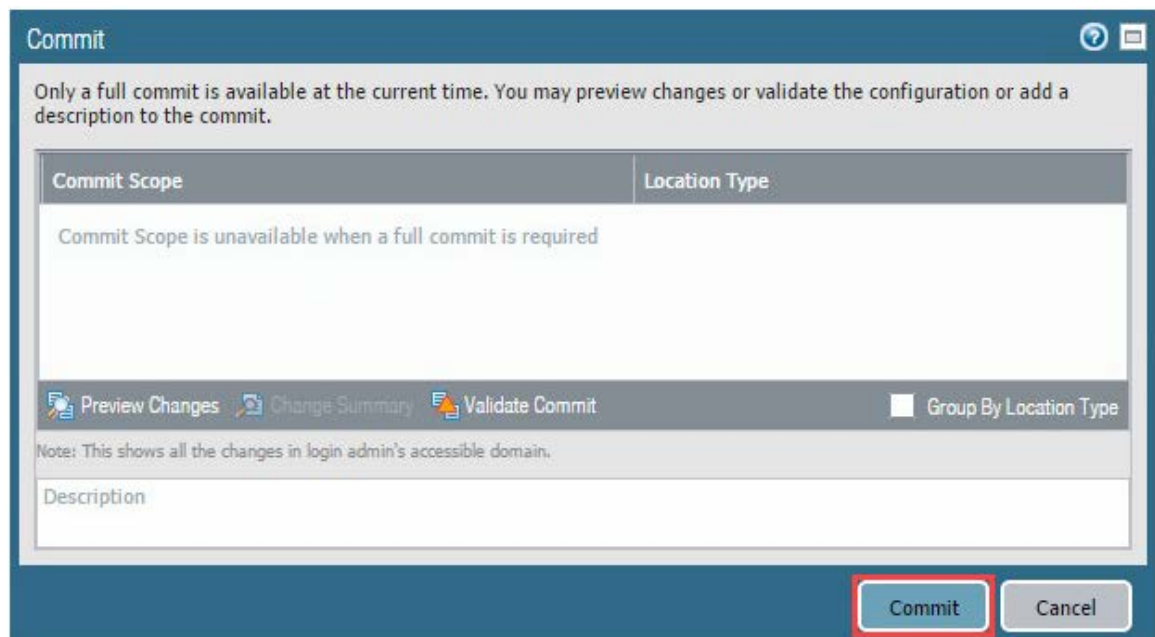
10. A message will confirm the configuration has loaded. Click **Close** to continue.



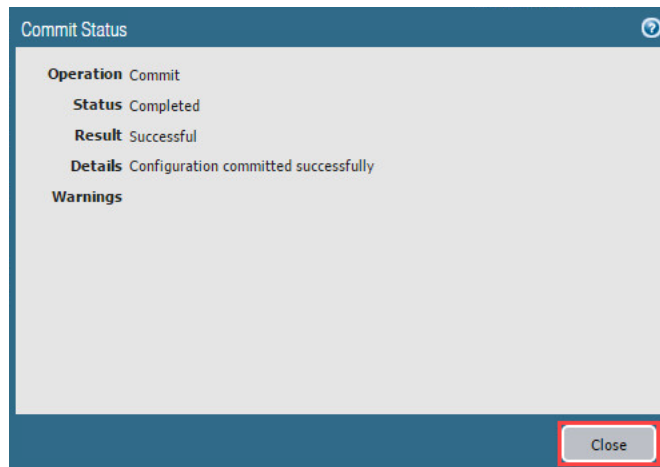
11. Click the **Commit** link located at the top-right of the web interface.



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



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

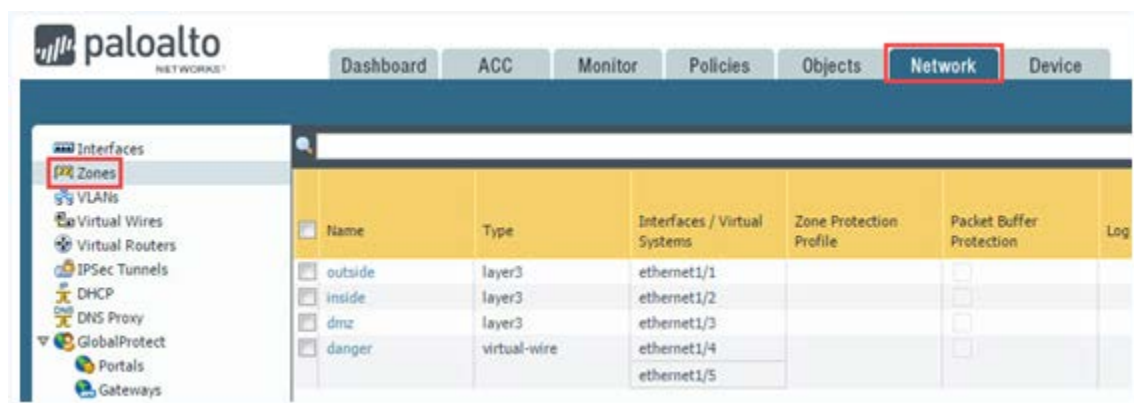


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

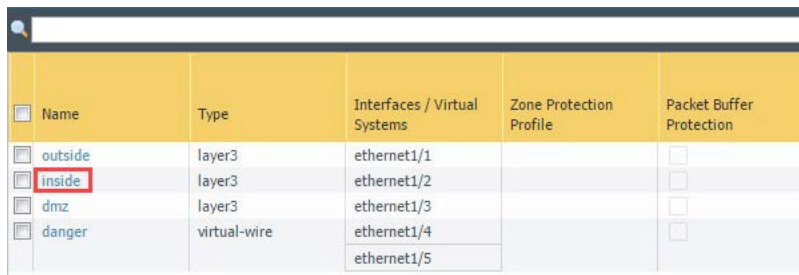
2.1 Configure a Local User Account and Authentication Profile

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**.

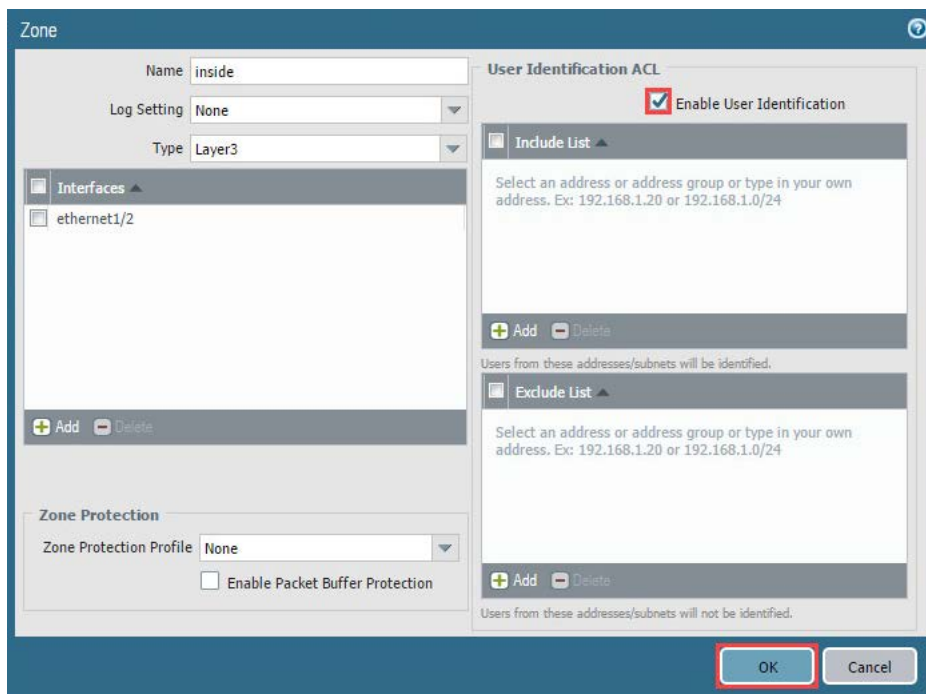


2. Click on the **inside** zone.



Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection
outside	layer3	ethernet1/1		<input type="checkbox"/>
inside	layer3	ethernet1/2		<input type="checkbox"/>
dmz	layer3	ethernet1/3		<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.

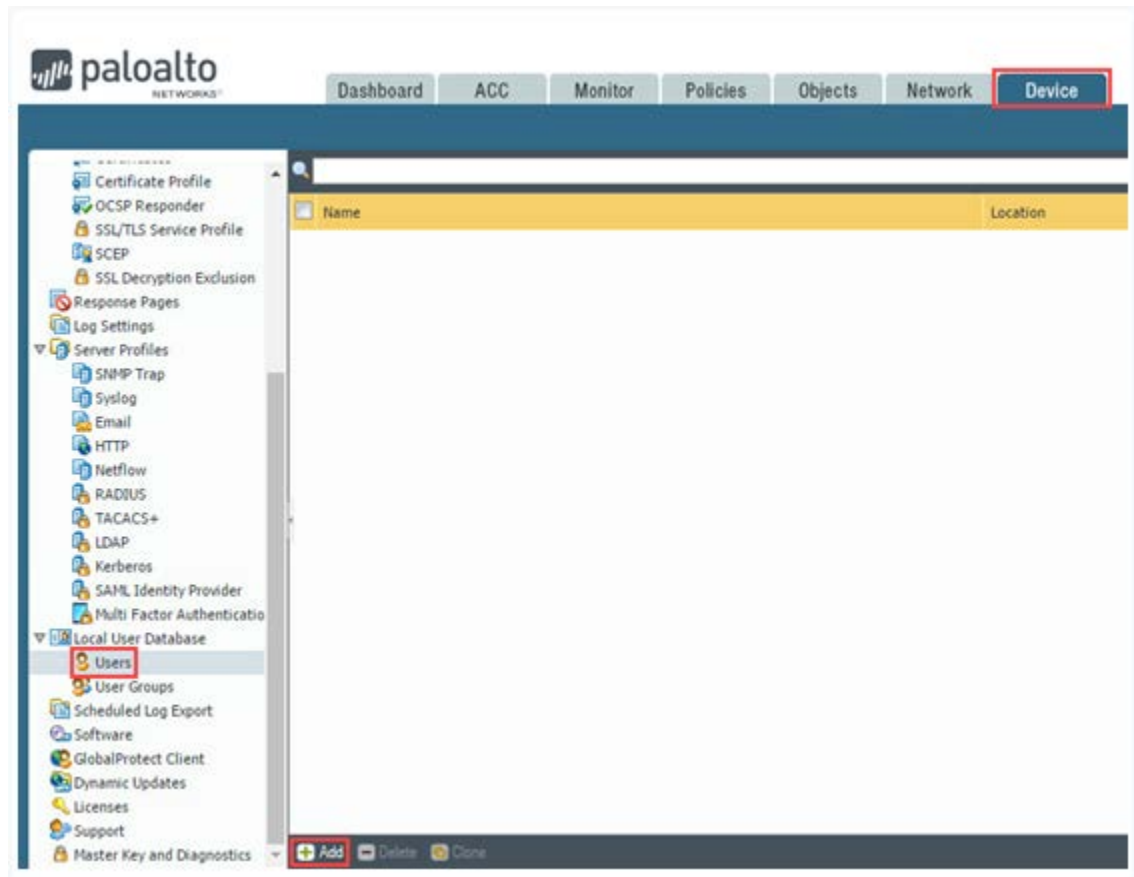


The screenshot shows the 'Zone' configuration window for the 'inside' zone. The 'Name' field is 'inside', 'Log Setting' is 'None', and 'Type' is 'Layer3'. The 'Interfaces' list contains 'ethernet1/2'. The 'Zone Protection' section shows 'Zone Protection Profile' as 'None' and 'Enable Packet Buffer Protection' as unchecked. The 'User Identification ACL' section has the 'Enable User Identification' checkbox checked. Below this are 'Include List' and 'Exclude List' sections, each with a description and 'Add'/'Delete' buttons. The 'OK' button at the bottom right is highlighted with a red box.

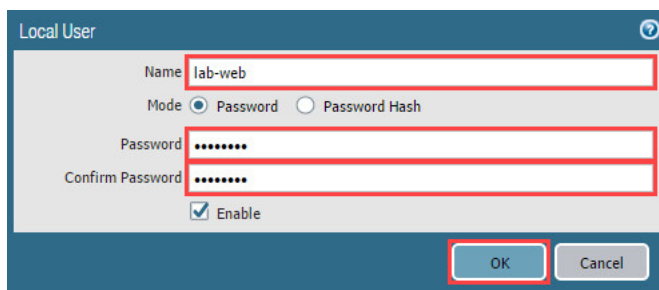


This will enable the inside zone to use a Username for authentication.

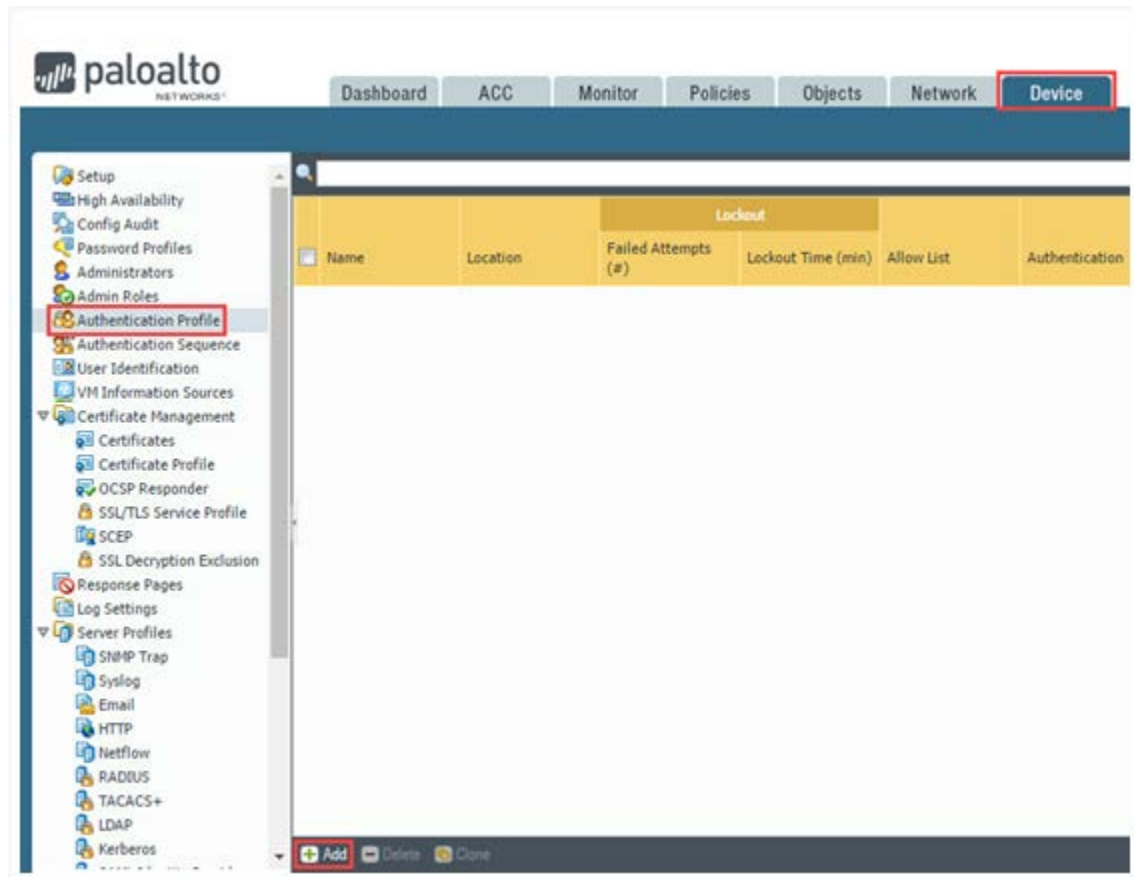
4. Navigate to **Device > Local User Database > Users > Add**. You may need to scroll down on the left pane.



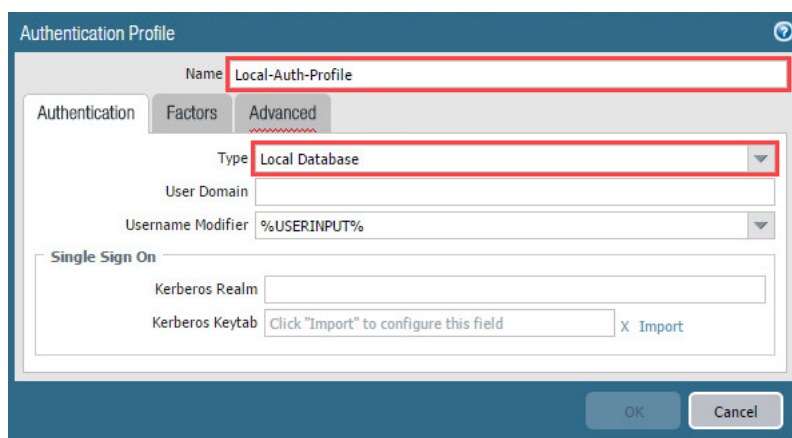
5. In the *Local User* window, type **lab-web** in the Name field. Then, type **Pa10A1t0** in the Password and Confirm Password fields. Finally, click the **OK** button.

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.

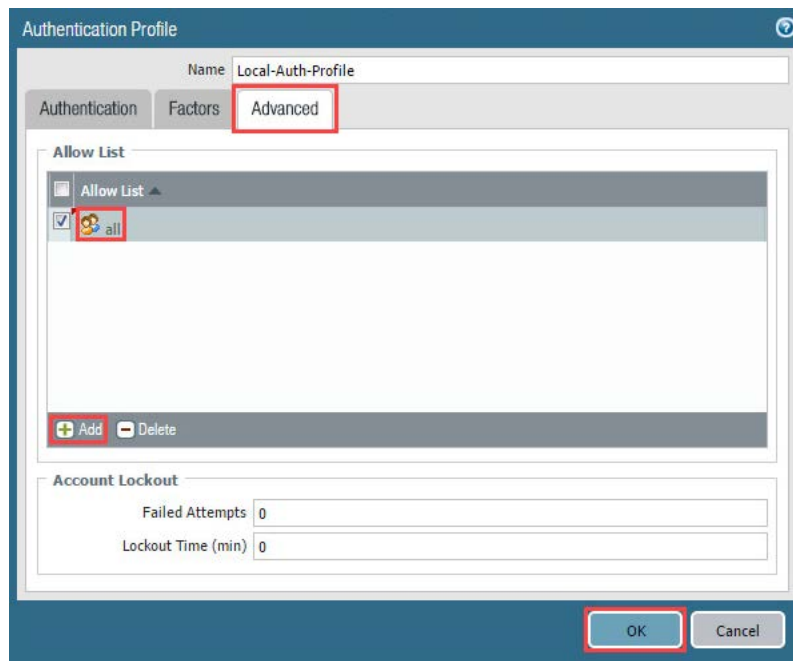
6. Navigate to **Device > Authentication Profile > Add**. You may need to scroll up on the left pane.



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



8. 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.



2.2 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.

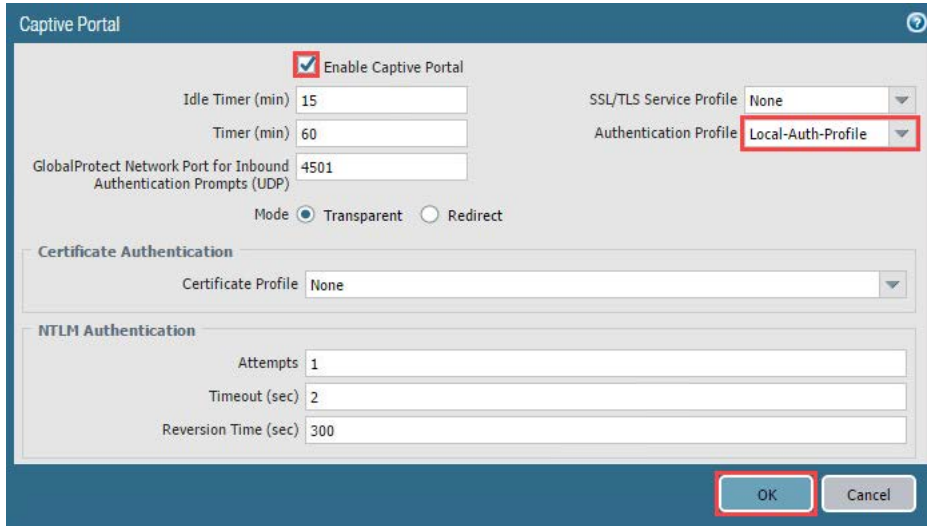
1. Navigate to **Device > User Identification > Captive Portal Settings**.



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

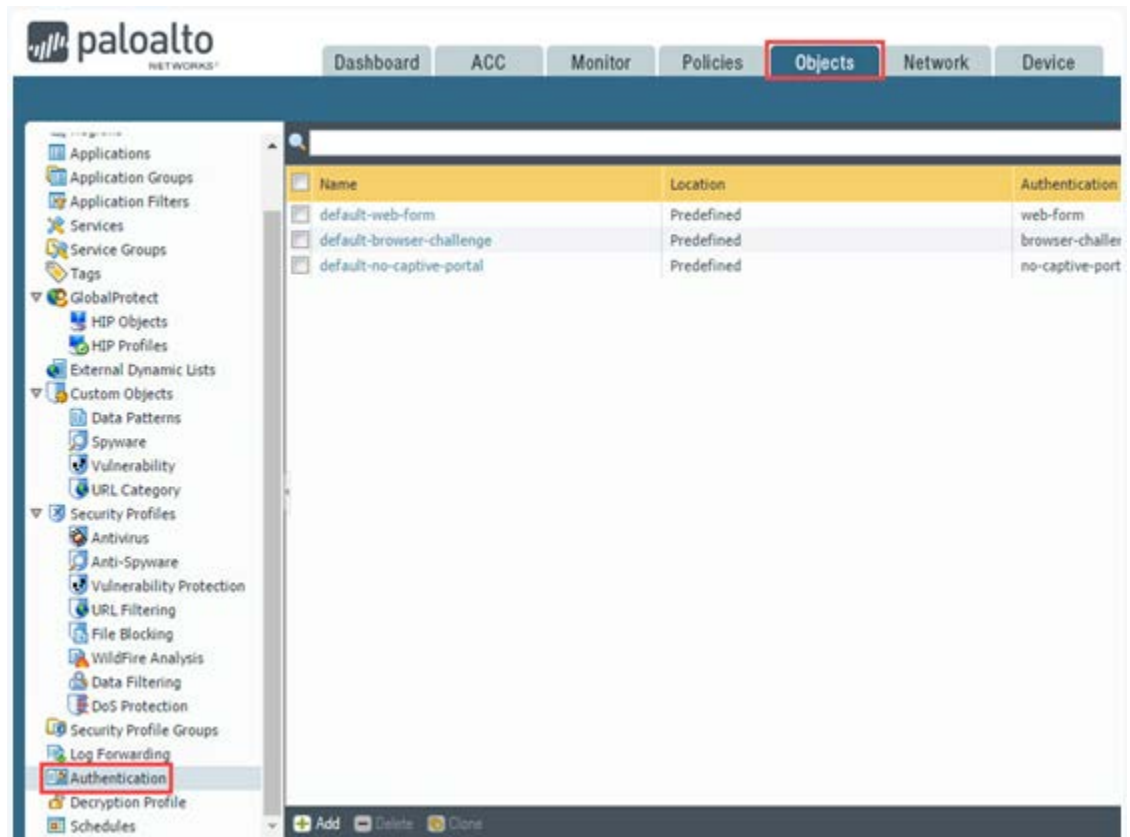


3. In the *Captive Portal* window, click the **Enable Captive Portal** checkbox. Then, select **Local-Auth-Profile** from the Authentication Profile dropdown. Finally, click the **OK** button.

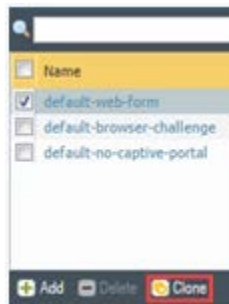
A screenshot of the 'Captive Portal' configuration window. The 'Enable Captive Portal' checkbox is checked. The 'Authentication Profile' dropdown is set to 'Local-Auth-Profile'. The 'OK' button is highlighted with a red box. Other settings include Idle Timer (15 min), Timer (60 min), GlobalProtect Network Port (4501), Mode (Transparent), Certificate Profile (None), and NTLM Authentication settings (Attempts: 1, Timeout: 2, Reversion Time: 300).

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

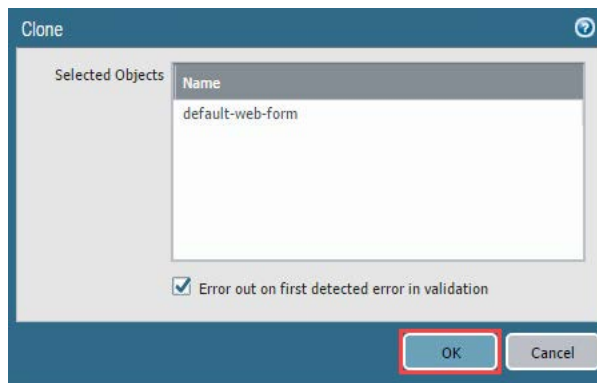
4. Navigate to **Objects > Authentication**. You may need to scroll down on the left pane.



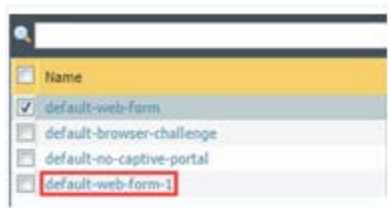
- Click the checkbox beside the **default-web-form** and click **Clone**.



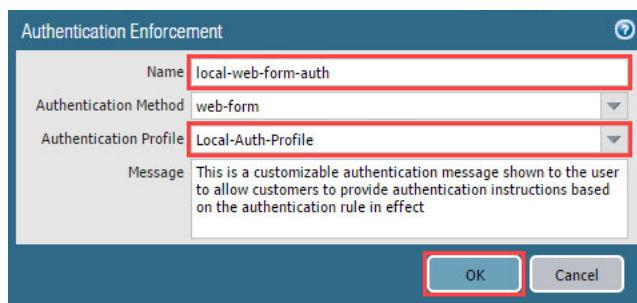
- In the *Clone* window, click the **OK** button to confirm the clone.



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



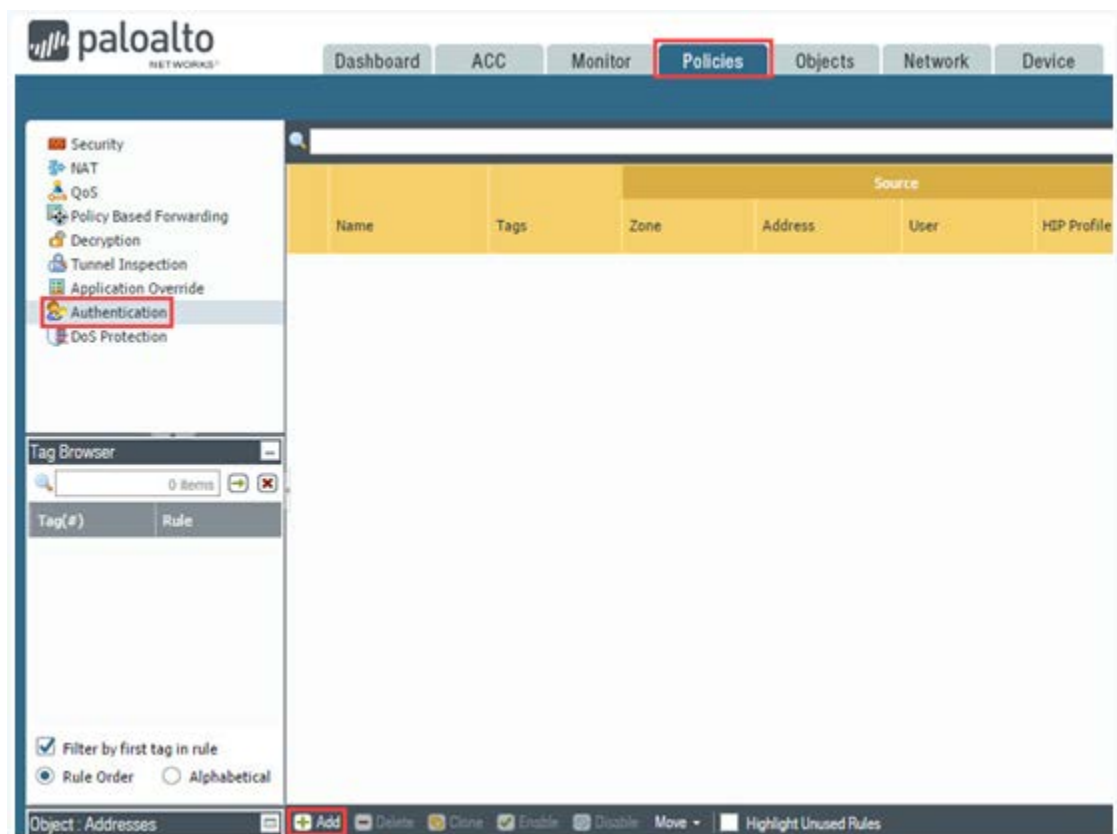
- In the *Authentication Enforcement* window, type **local-web-form-auth** in the Name field. Then, select **Local-Auth-Profile** in the Authentication Profile dropdown. Next, click the **OK** button.



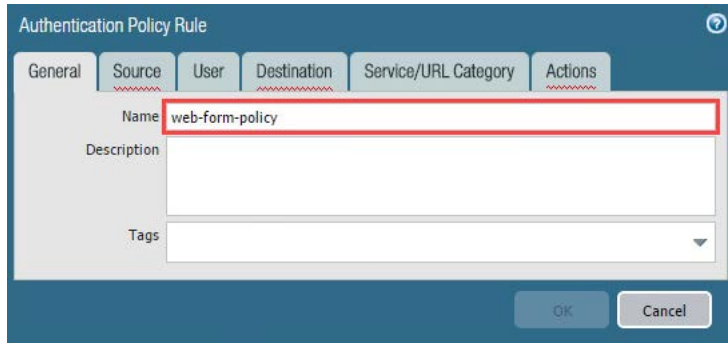
2.3 Create an Authentication Policy

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**.

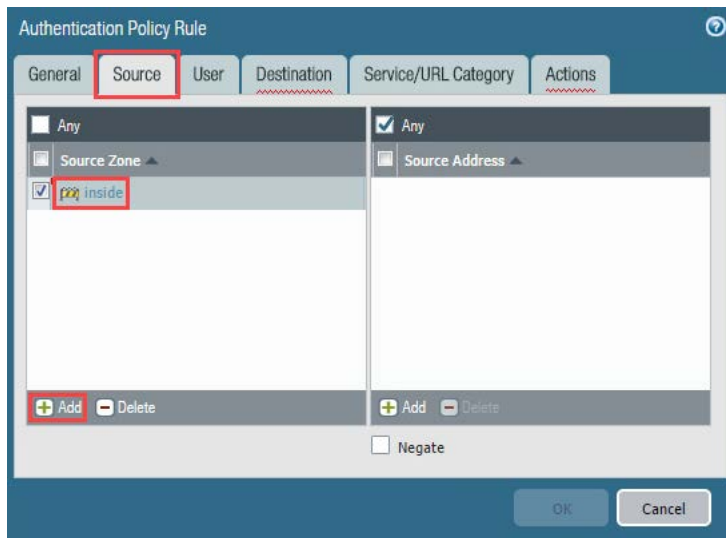


2. In the *Authentication Policy Rule* window, type **web-form-policy** in the Name field.



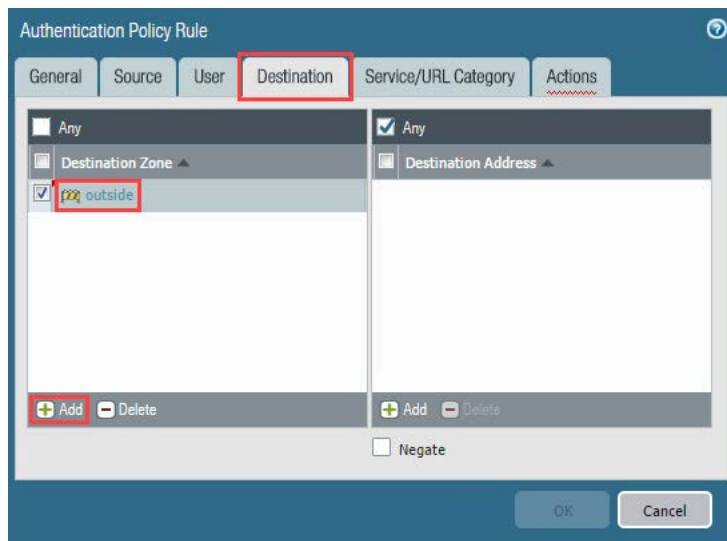
The screenshot shows the 'Authentication Policy Rule' window with the 'General' tab selected. The 'Name' field is highlighted with a red box and contains the text 'web-form-policy'. The 'Description' field is empty. The 'Tags' field is a dropdown menu. At the bottom right are 'OK' and 'Cancel' buttons.

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**.

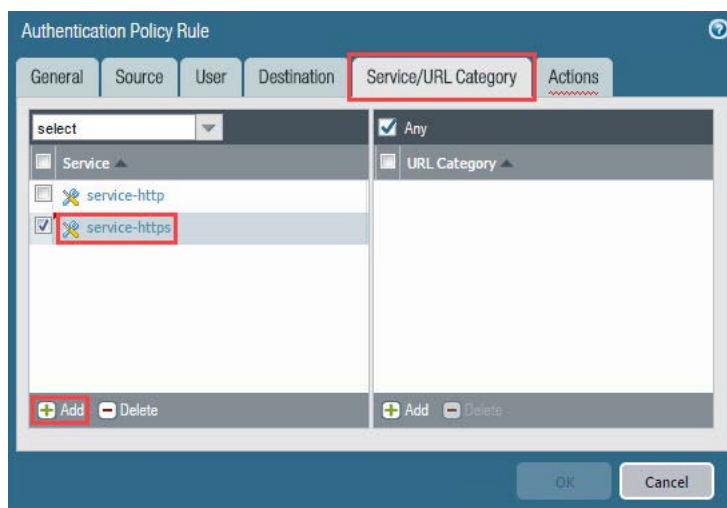


The screenshot shows the 'Authentication Policy Rule' window with the 'Source' tab selected. The 'Source Zone' section on the left has a red box around the 'Add' button. Below it, the 'inside' option is selected and highlighted with a red box. The 'Source Address' section on the right has a 'Negate' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

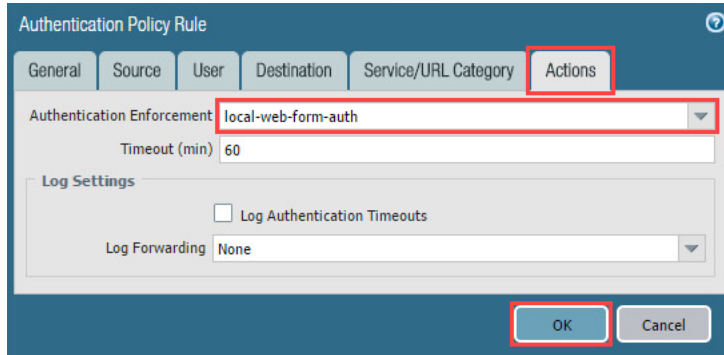
4. In the *Authentication Policy Rule* window, click on the **Destination** tab. Then, click the **Add** button in the Destination Zone section. Next, select **outside**.



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**.



6. 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.



The screenshot shows the 'Authentication Policy Rule' window with the 'Actions' tab selected. The 'Authentication Enforcement' dropdown is set to 'local-web-form-auth'. The 'Timeout (min)' is set to 60. Under 'Log Settings', the 'Log Authentication Timeouts' checkbox is unchecked, and 'Log Forwarding' is set to 'None'. The 'OK' button is highlighted with a red box.

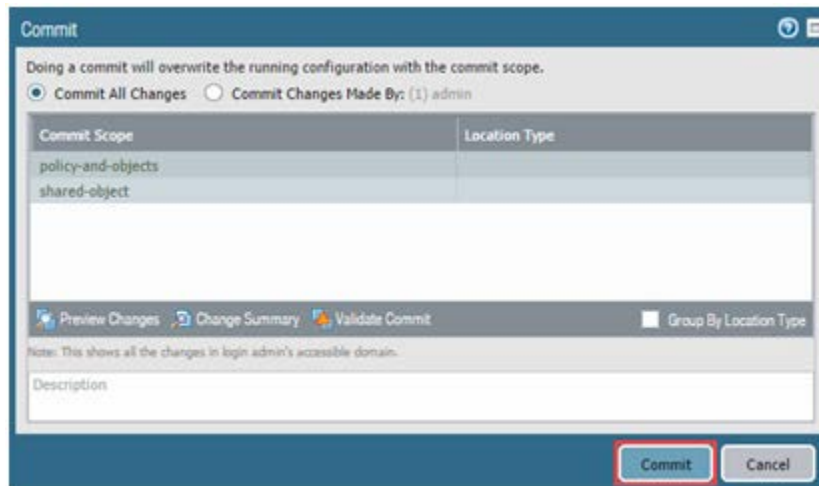
2.4 Commit and Test Authentication Policy

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

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



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

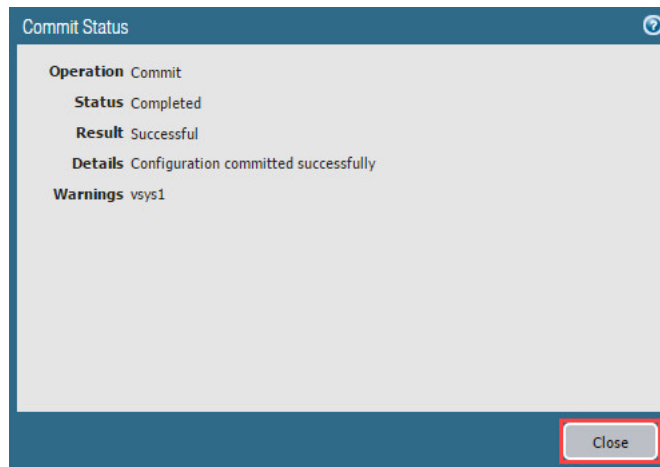


The screenshot shows the 'Commit' window. It displays a warning: 'Doing a commit will overwrite the running configuration with the commit scope.' Below this, there are two radio buttons: 'Commit All Changes' (selected) and 'Commit Changes Made By: (1) admin'. A table lists the commit scope and location type:

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

At the bottom, there are buttons for 'Preview Changes', 'Change Summary', and 'Validate Commit'. A checkbox for 'Group By Location Type' is also present. A note states: 'Note: This shows all the changes in login admin's accessible domain.' The 'Commit' button is highlighted with a red box.

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

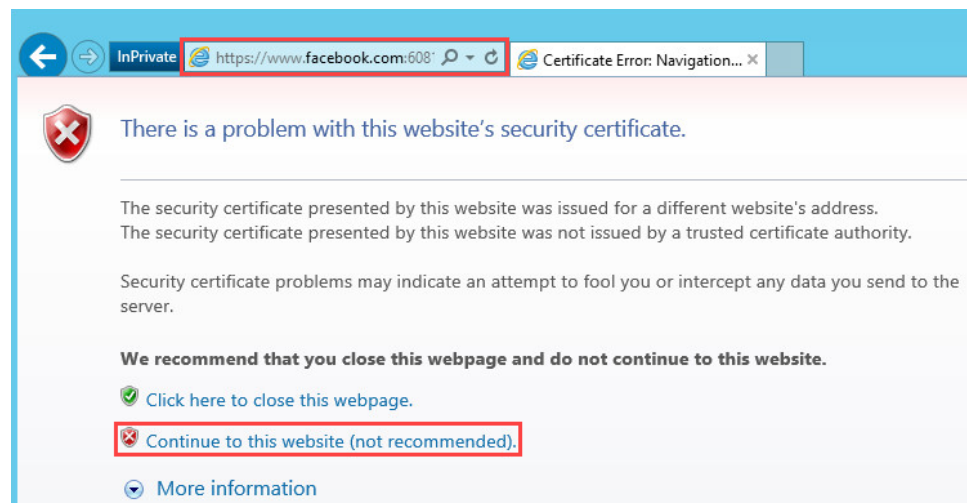


You will see a **vsys1** in Warnings, which refers to a virtual system in the Firewall. You can ignore it in this lab environment.

- Open **Internet Explorer** from the taskbar.

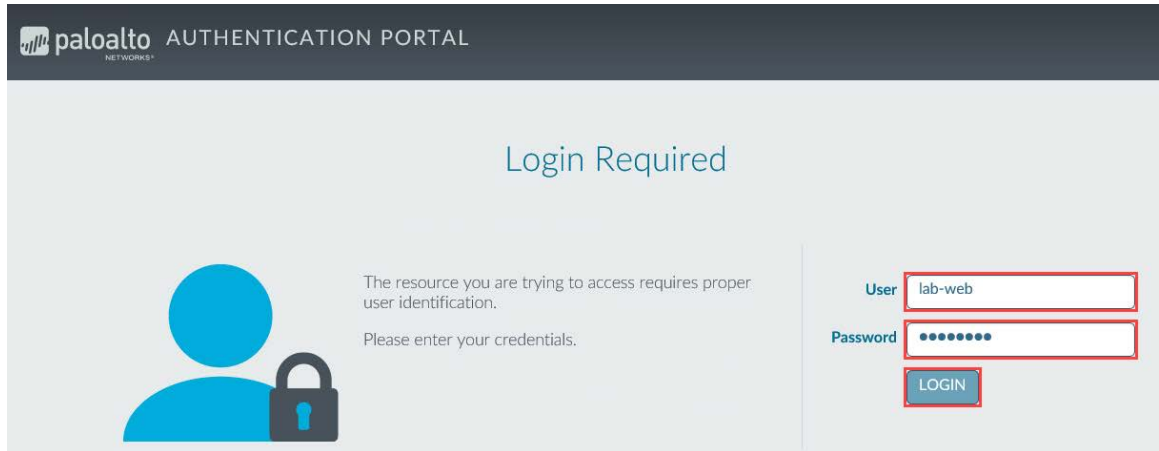


- In the address bar, type **http://www.facebook.com** and press **Enter**. You will need to confirm the certificate error, and click **Continue to this website (not recommended)**.



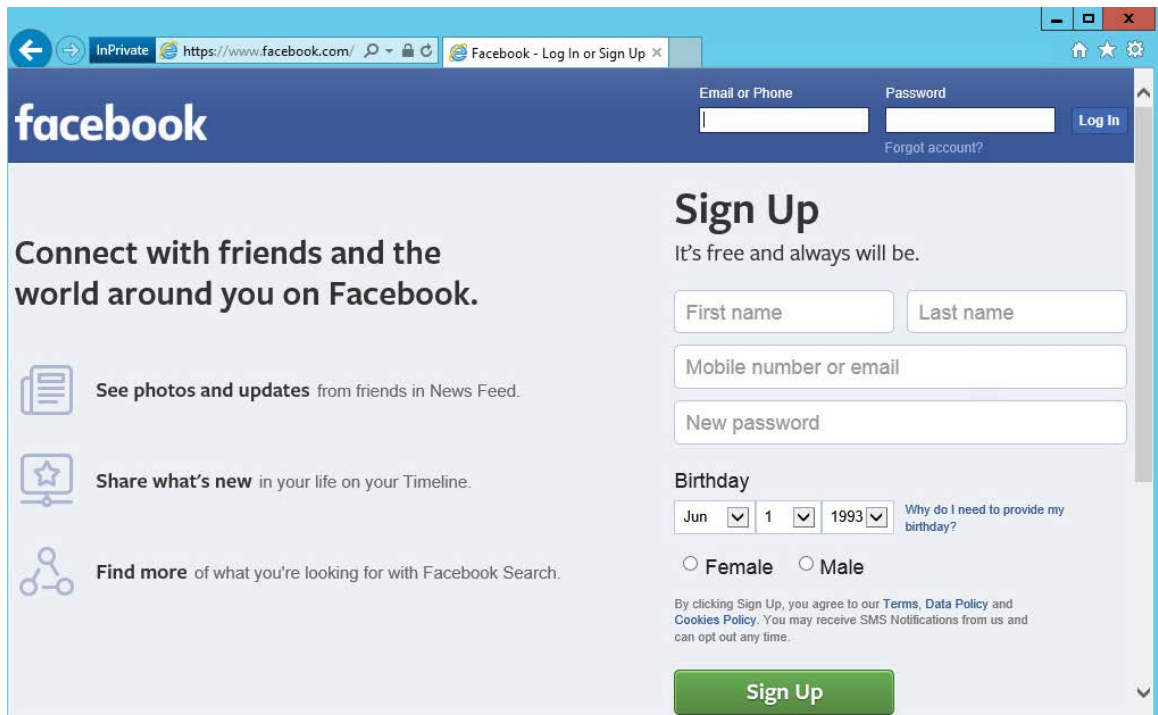
You are seeing this error because the Firewall is intercepting traffic coming from the inside zone to the outside zone. The Firewall serves as a man-in-the-middle until authenticated.

- You will see a web-form login, type **lab-web** as the username. Then, type **Pal0Alt0** as the password. Finally, click the **Login** button.



The image shows the Palo Alto Authentication Portal login page. At the top, the Palo Alto Networks logo and 'AUTHENTICATION PORTAL' are displayed. The main heading is 'Login Required'. Below this, a message states: 'The resource you are trying to access requires proper user identification. Please enter your credentials.' To the left of this message is a blue silhouette of a person with a padlock. On the right, there is a login form with two input fields: 'User' containing 'lab-web' and 'Password' containing a series of dots. Below the password field is a red 'LOGIN' button.

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

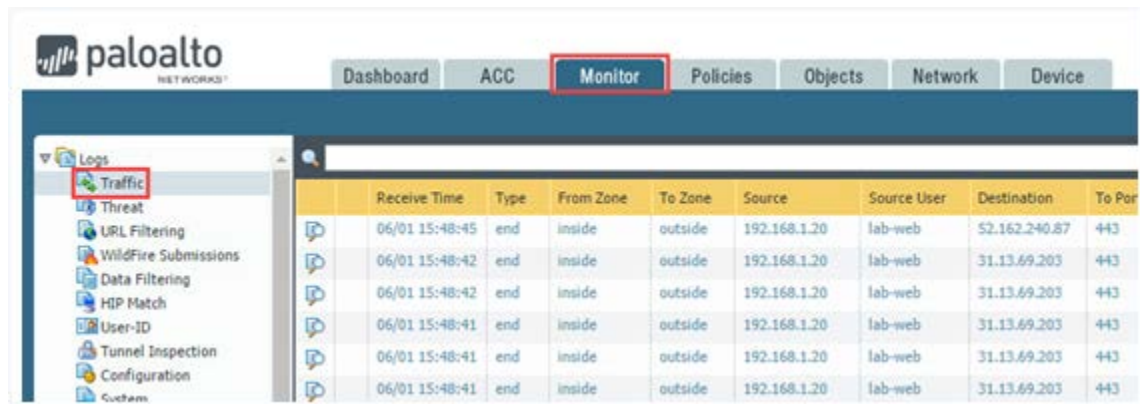


The image shows the Facebook Sign Up page in a web browser. The browser's address bar shows 'https://www.facebook.com/'. The Facebook logo is at the top left. To the right of the logo are input fields for 'Email or Phone' and 'Password', with a 'Log In' button and a 'Forgot account?' link. The main heading is 'Sign Up' with the subtext 'It's free and always will be.' Below this are input fields for 'First name', 'Last name', 'Mobile number or email', and 'New password'. There is a 'Birthday' section with dropdown menus for month (Jun), day (1), and year (1993), and a link 'Why do I need to provide my birthday?'. Below the birthday section are radio buttons for 'Female' and 'Male'. At the bottom, there is a green 'Sign Up' button. A disclaimer at the bottom states: 'By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.'

- Click the **X** in the upper-right to close Internet Explorer.



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



10. You will see in the logs the entries to **facebook-base** are associated to 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	To Port	Application
	06/01 15:48:45	end	inside	outside	192.168.1.20	lab-web	52.162.240.87	443	ssl
	06/01 15:48:42	end	inside	outside	192.168.1.20	lab-web	31.13.69.203	443	facebook-base
	06/01 15:48:42	end	inside	outside	192.168.1.20	lab-web	31.13.69.203	443	facebook-base
	06/01 15:48:41	end	inside	outside	192.168.1.20	lab-web	31.13.69.203	443	facebook-base
	06/01 15:48:41	end	inside	outside	192.168.1.20	lab-web	31.13.69.203	443	facebook-base
	06/01 15:48:41	end	inside	outside	192.168.1.20	lab-web	31.13.69.203	443	facebook-base