PALO ALTO NETWORKS EDU 210

Lab 14: Preventing Use of Stolen Credentials

Document Version: 2022-07-18

Contents

Introduction

Recently, numerous users in your organization have received phishing emails. Most employees have wisely ignored and deleted emails from unrecognized senders; however, an alarming number of people continue to open suspicious emails and click included links.

You suspect that several users have supplied their work credentials to phishing websites, so you will implement Credential Protection on the Palo Alto Networks firewall.

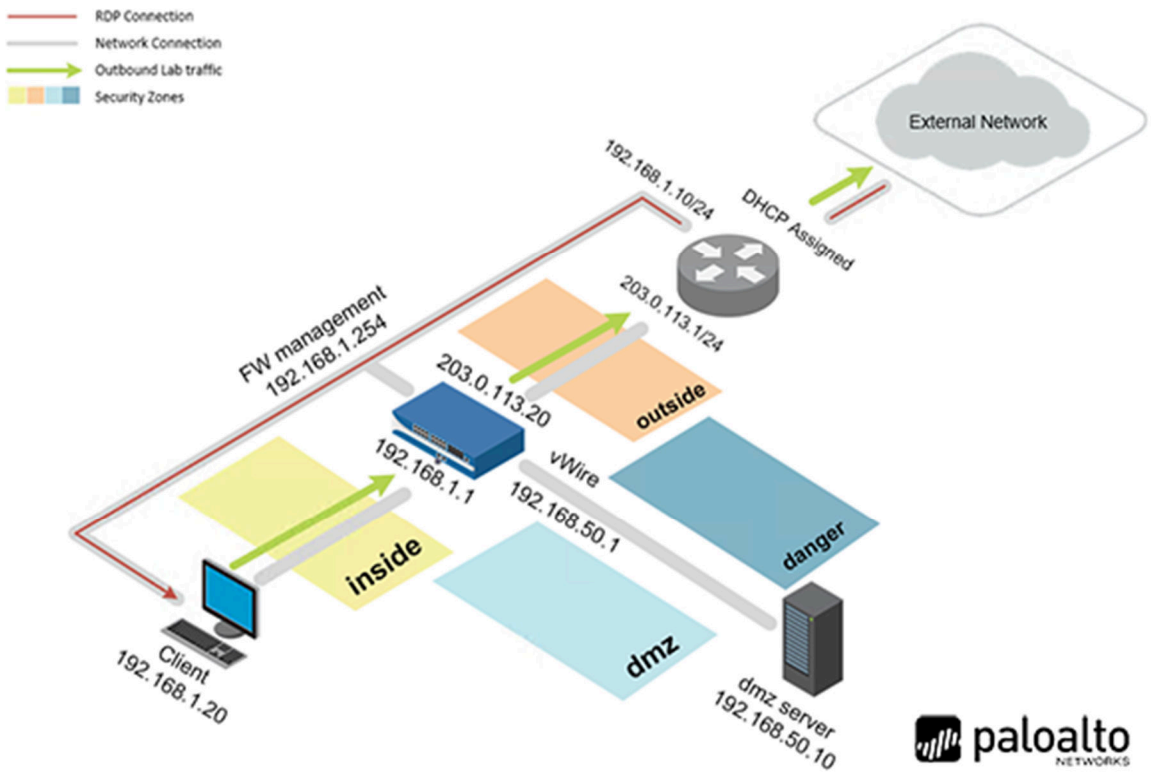
With Credential Protection in place, the firewall will block employees' attempts to enter work usernames into external websites.

Objective

In this lab, you will perform the following tasks:

- Create a self-signed certificate for trusted connections
- Create a self-signed certificate for untrusted connections
- Export the firewall certificate and import to Firefox
- Test the firewall behavior without credential detection
- Provide the firewall with User-ID information
- Test the firewall behavior with credential detection

Lab Topology



Lab Settings

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

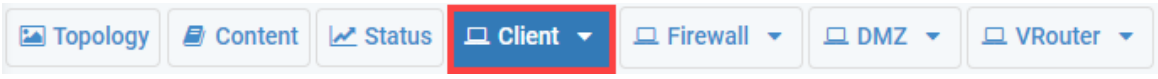
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	**Pal0Alt0!**
DMZ	192.168.50.10	root	**Pal0Alt0!**
Firewall	192.168.1.254	admin	**Pal0Alt0!**
VRouter	192.168.1.10	root	**Pal0Alt0!**

1 Preventing Use of Stolen Credentials

1.1 Apply a Baseline Configuration to the Firewall

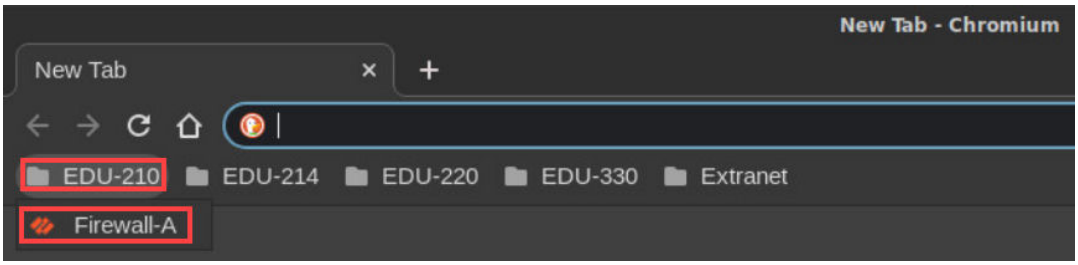
In this section, you will load the Firewall configuration file.

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

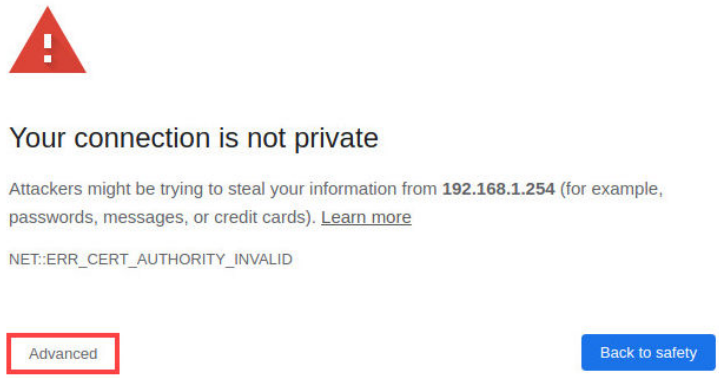


2. Double-click the **Chromium Web Browser** icon located on the desktop.

3. In the *Chromium* web browser, click on the **EDU-210** bookmark folder in the bookmarks bar and then click on **Firewall-A**.

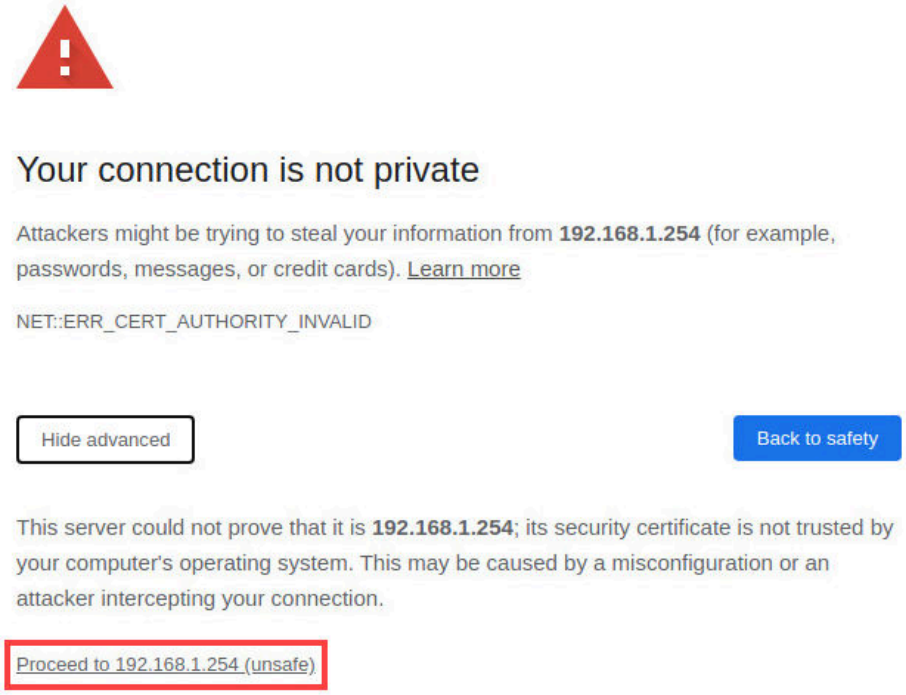


4. You will see a "*Your connection is not private*" message. Next, click on the **ADVANCED** link.



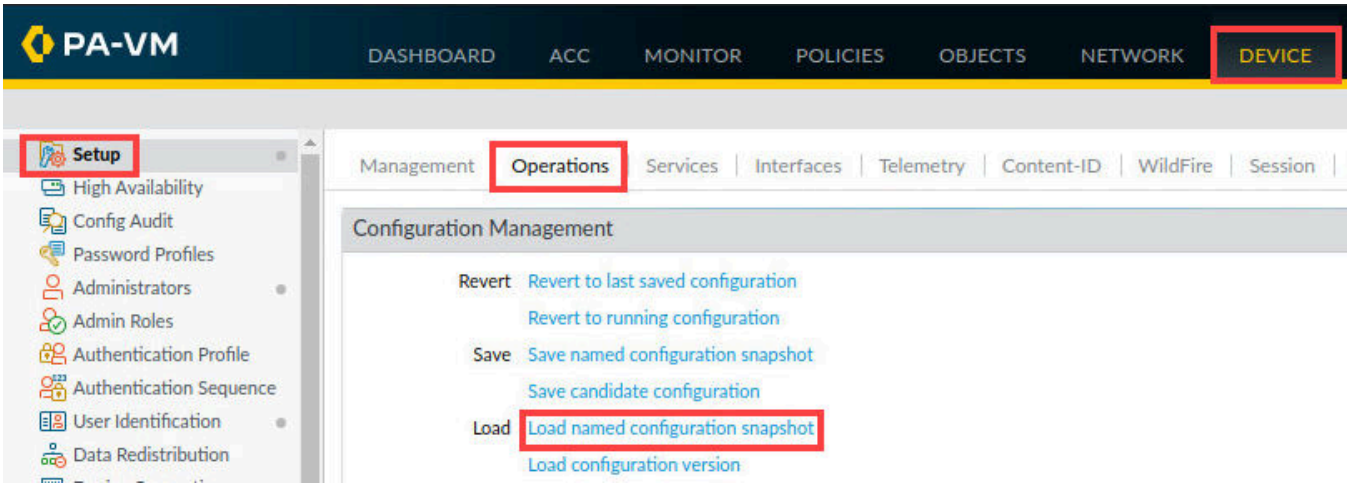
If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

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

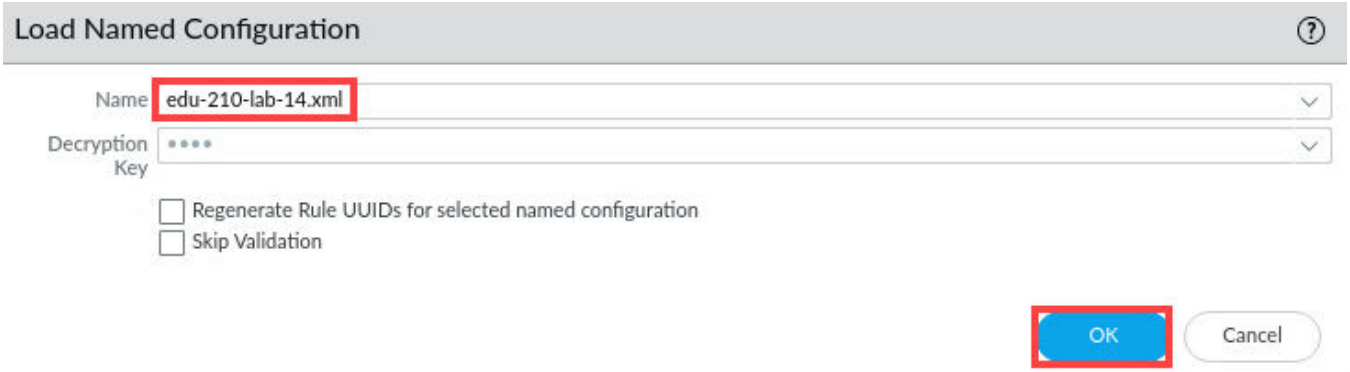


6. Log in to the firewall web interface as username **`admin`**, password **`Pal0Alt0!.`**

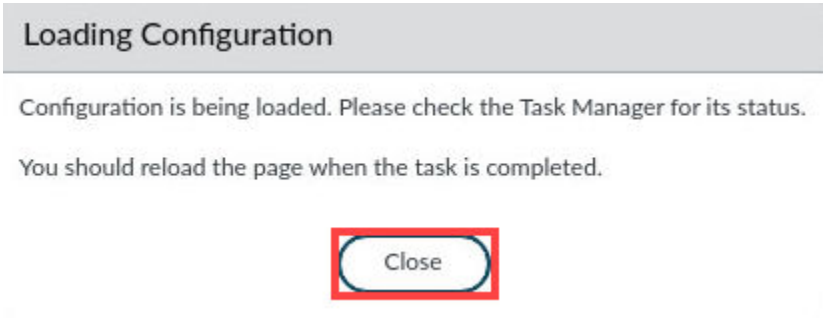
7. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



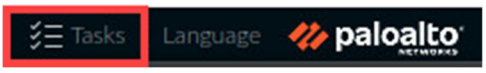
8. In the *Load Named Configuration* window, select **edu-210-lab-14.xml** from the *Name* dropdown box and click **OK**.



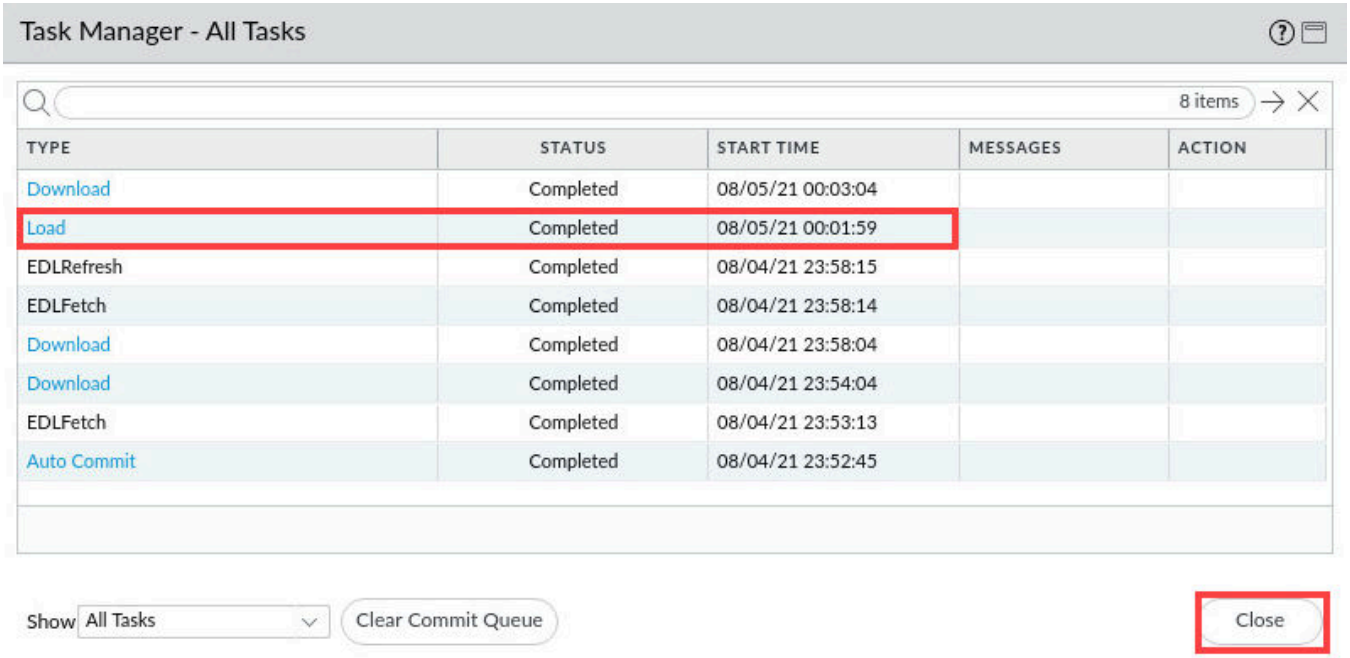
9. In the *Loading Configuration* window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



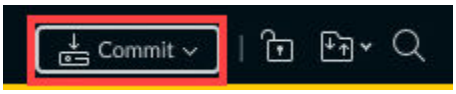
10. Click the **Tasks** icon located at the bottom-right of the web interface.



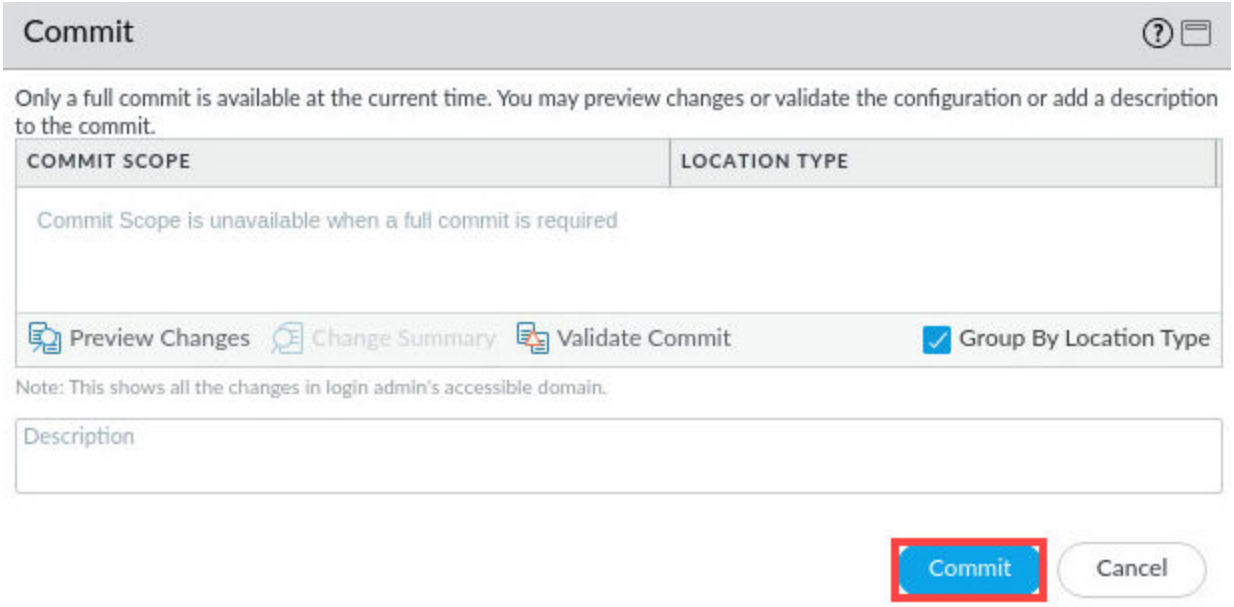
11. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.



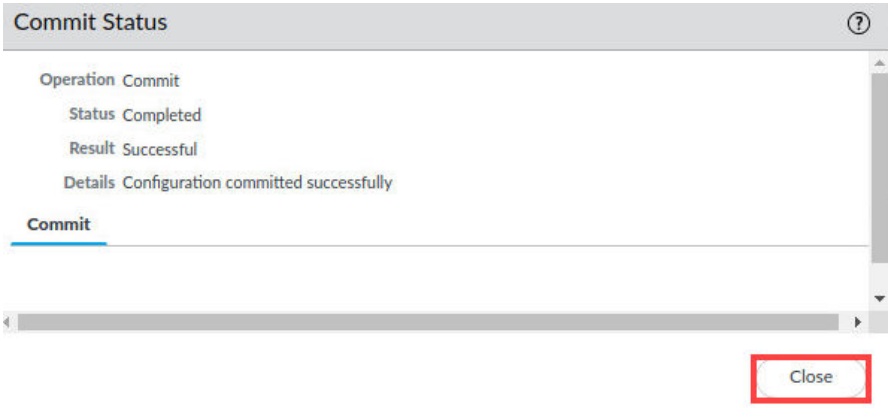
12. Click the **Commit** link located at the top-right of the web interface.



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



14. 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.

15. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

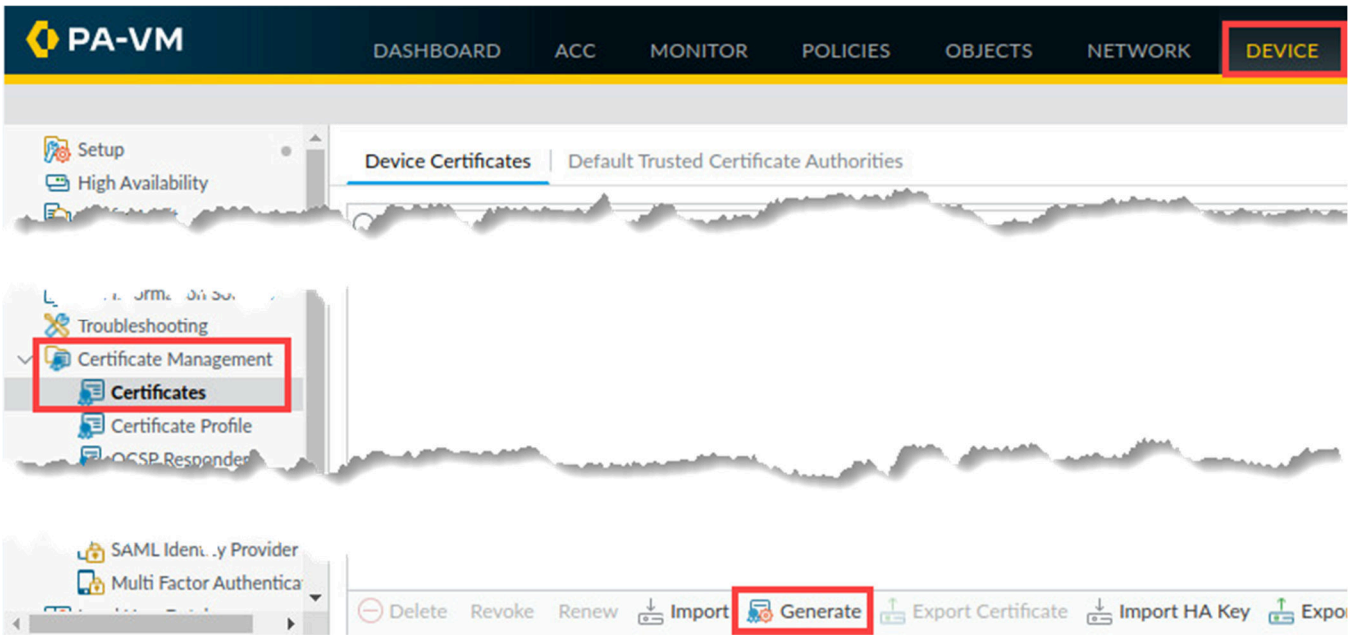
1.2 Prepare the Lab Environment

To start this lab exercise, you will continue from the configuration you completed in the previous lab on Decryption. This action will allow you to reconfigure the certificate needed for the firewall and import it to the Firefox browser.

You will re-generate a certificate on the firewall that will be used when clients connect to HTTPS websites that DO NOT have certificates issued by trusted certificate authorities - for example, sites that use self-signed certificates or certificates that have expired. You will also create a Decryption Policy to decrypt HTTPS traffic from the Users_Net security zone to the Internet security zone.

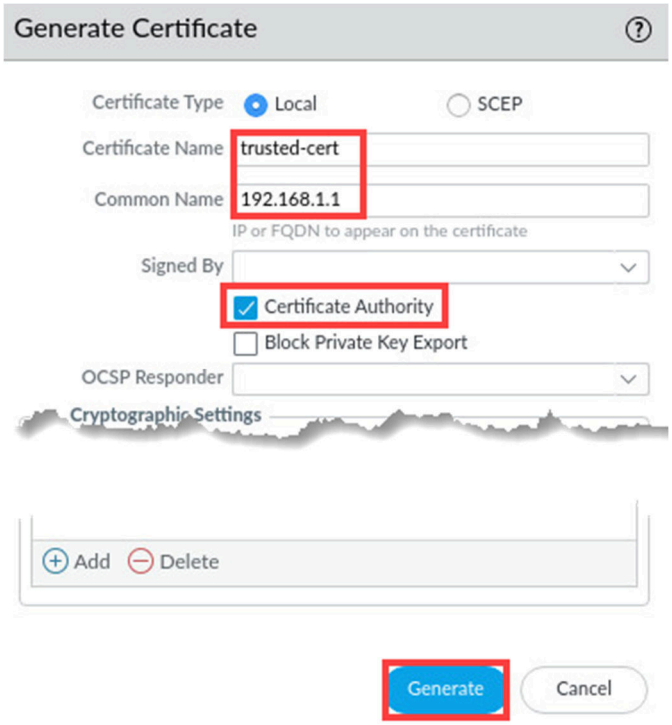
Remember that certificates are very important to help keep integrity between the client and the Palo Alto Networks Firewall. The firewall will use this certificate as part of the decryption process between clients and untrusted HTTPS websites.

1. Select **Device > Certificate Management > Certificates**. Click **Generate** to create a new *CA Certificate*.



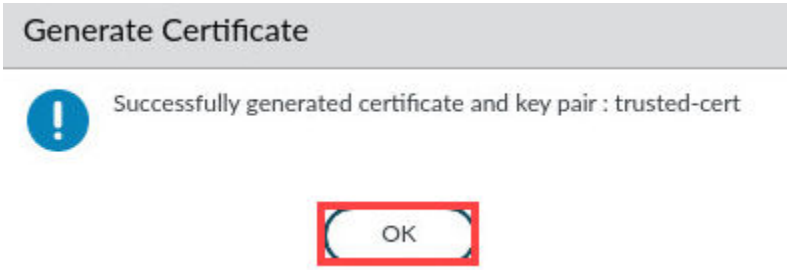
2. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`trusted-cert`
Common Name	`192.168.1.1`
Certificate Authority	**Certificate Authority**



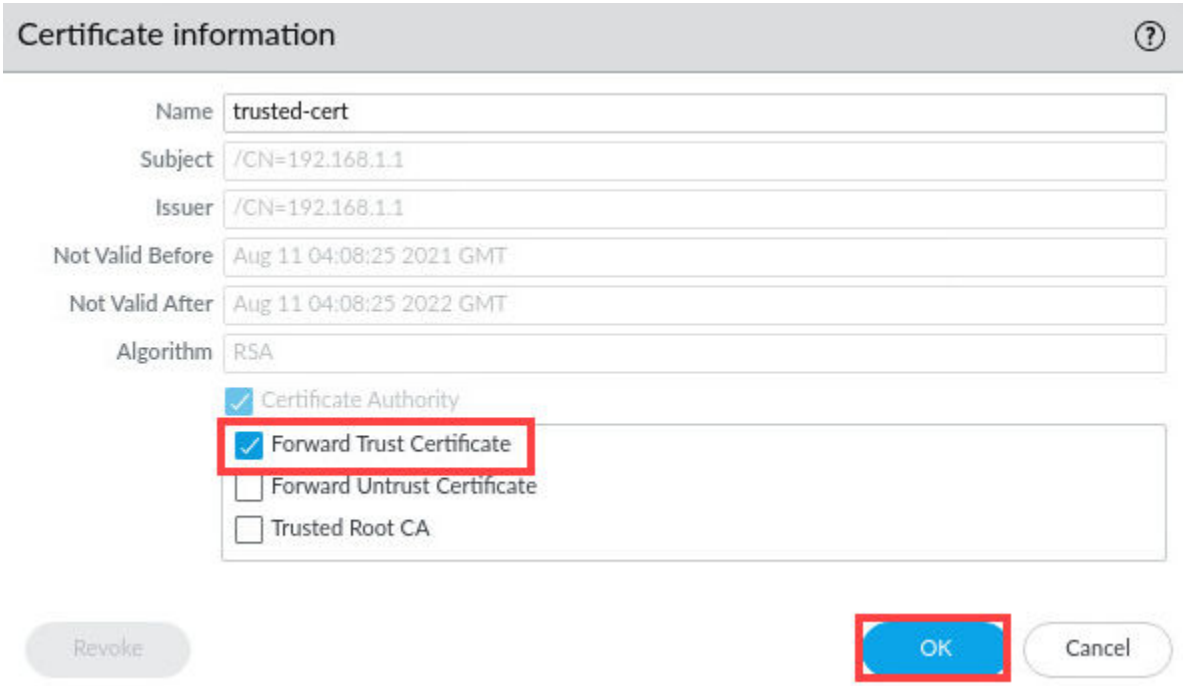
Please Note A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

3. In the *Generate Certificate* window, click **OK**.



4. You should have a new entry in the *Device Certificates* table. Click **trusted-cert**.

5. In the *Certificate information* window, place a **check** in the box for **Forward Trust Certificate**. Click **OK**.



> **Please Note**
> This action instructs the firewall to use this certificate to decrypt traffic between clients and trusted HTTPS sites.

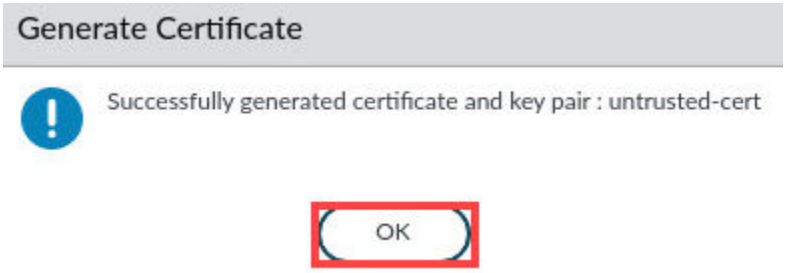
6. Click **Generate** to create a new *CA Certificate*.

7. In the *Generate Certificate* window, configure the following. Click **Generate**.

Parameter	Value
Certificate Name	`untrusted-cert`
Common Name	`untrusted`
Certificate Authority	**Certificate Authority**

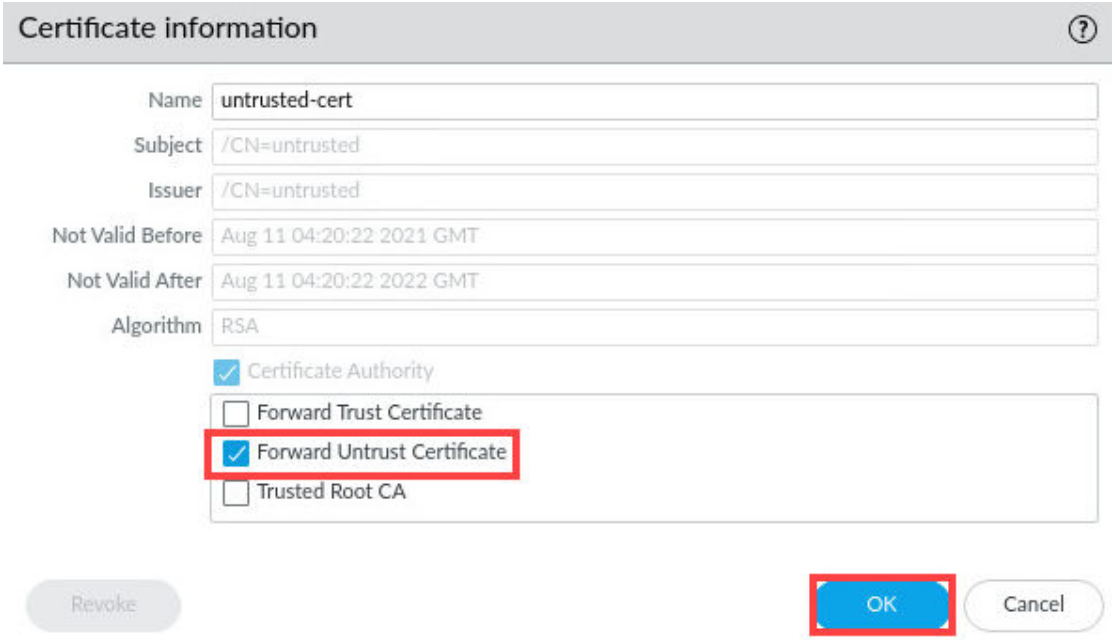
> **Please Note**
> A Generate Certificate status window should open that confirms that the certificate and key pair were generated successfully.

8. In the *Generate Certificate* window, click **OK**.



9. You should have a new entry in the *Device Certificates* table. Click **untrusted-cert**.

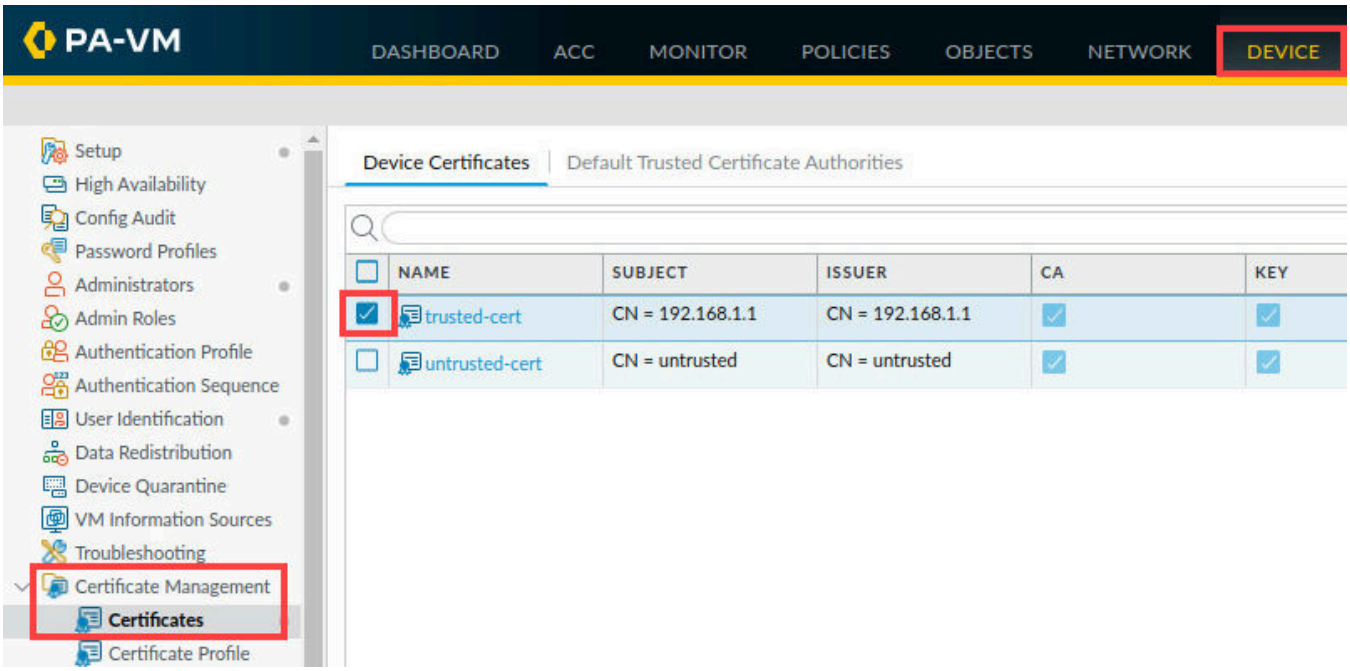
10. In the *Certificate information* window, place a **check** in the box for **Forward untrust Certificate**. Click **OK**.



Please Note

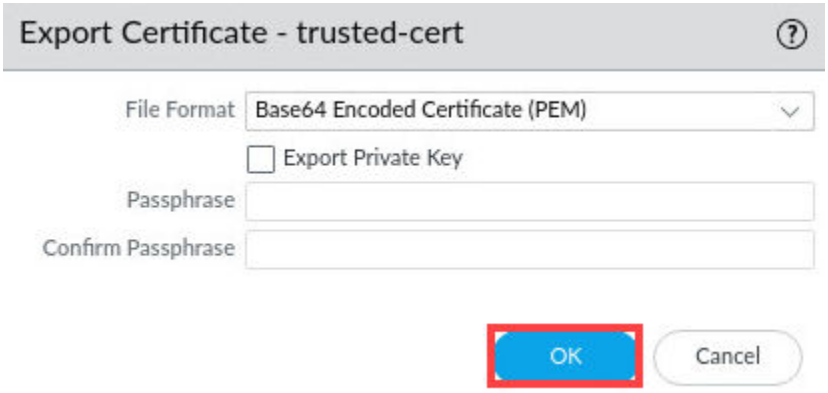
This action instructs the firewall to use this certificate to decrypt traffic between clients and HTTPS sites that are not trustworthy (expired certificates, self-signed certificates, etc.).

11. Select **Device > Certificate Management > Certificates**. **Highlight** but do not open *trusted-cert*.



12. At the bottom of the window, click **Export Certificate** to open the *Export Certificate* configuration window.

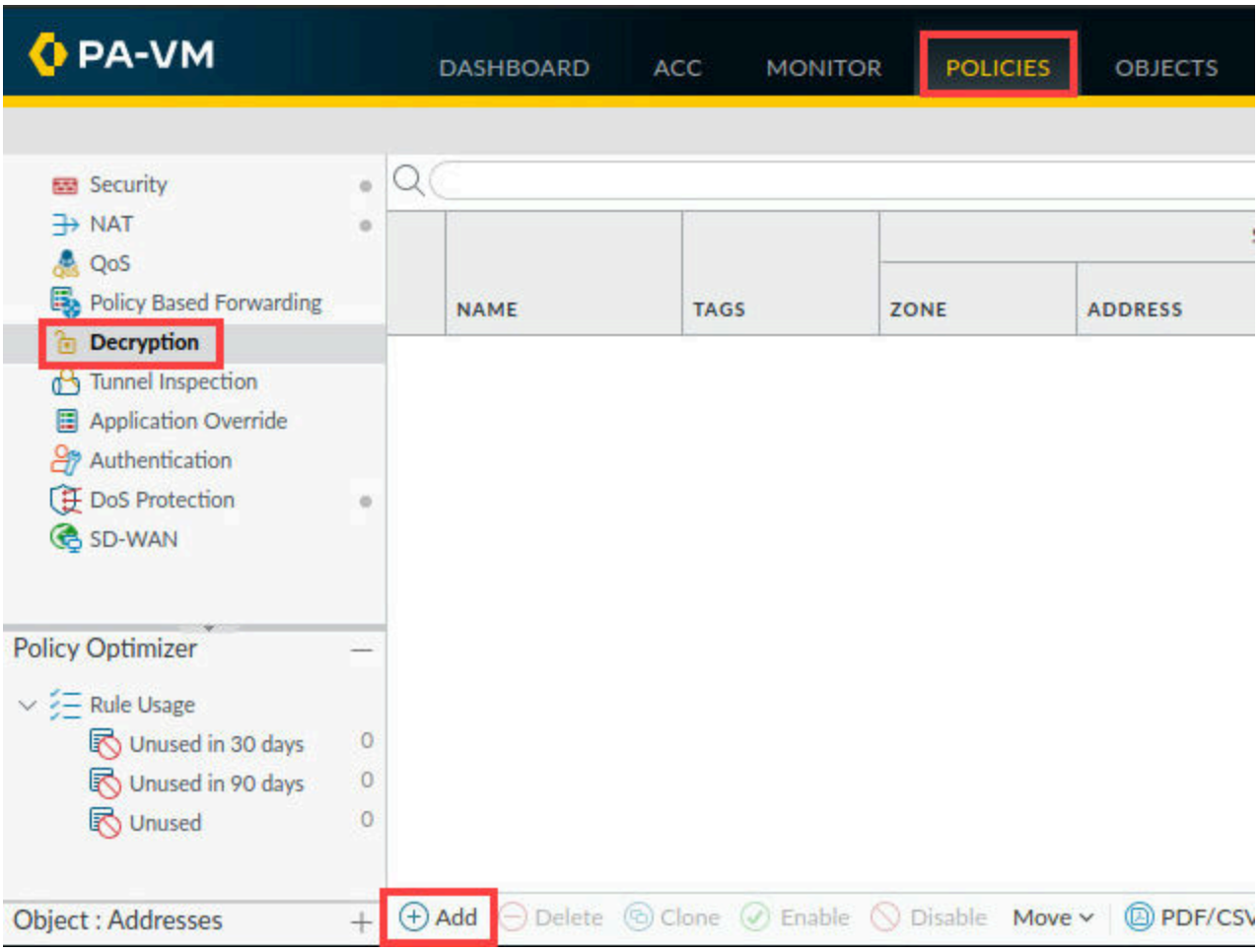
13. In the *Export Certificate – trusted-cert* window, leave all settings unchanged. Click **OK** to export the *trusted-cert* certificate.



Please Note

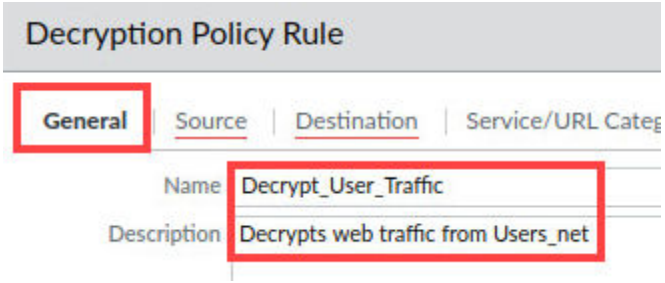
The file will be saved to the workstation's Downloads folder.

14. Select **Policies > Decryption**. Click **Add**.



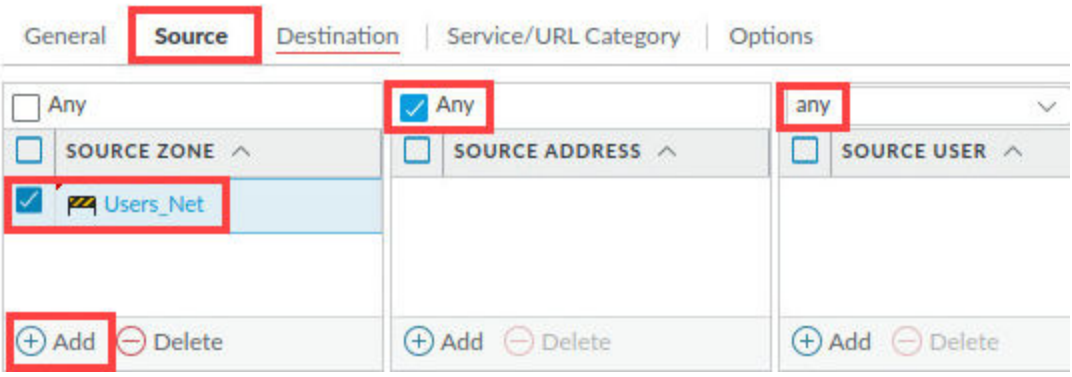
15. In the *Decryption Policy Rule* window, under the *General* tab, configure the following.

Parameter	Value
Name	`Decrypt_User_Traffic`
Description	`Decrypts web traffic from Users_Net.`



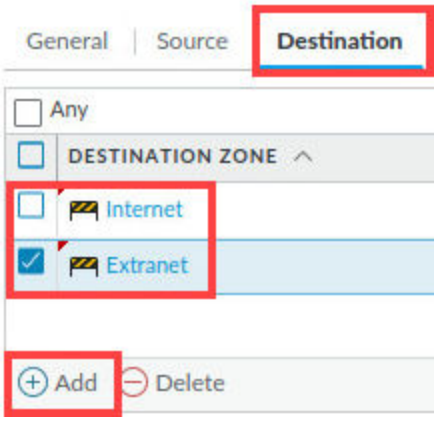
16. Click the **Source** tab and configure the following.

Parameter	Value
Source Zone	**Users_Net**
Source Address	**Any**
Source User	**any**

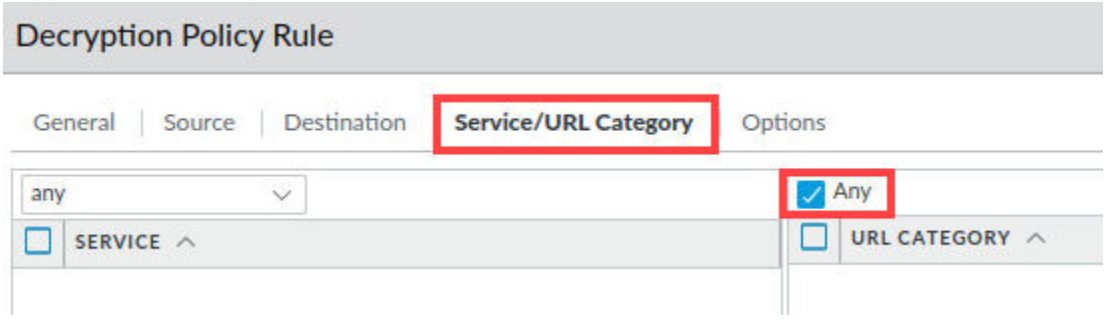


17. Click the **Destination** tab and configure the following.

Parameter	Value
Destination Zone	**Internet** **Extranet**
Destination Address	**Any**



18. Click the **Service/URL Category** tab and verify that the **Service** is set to **any** and that the box for **Any** above *URL Category* is **checked**.



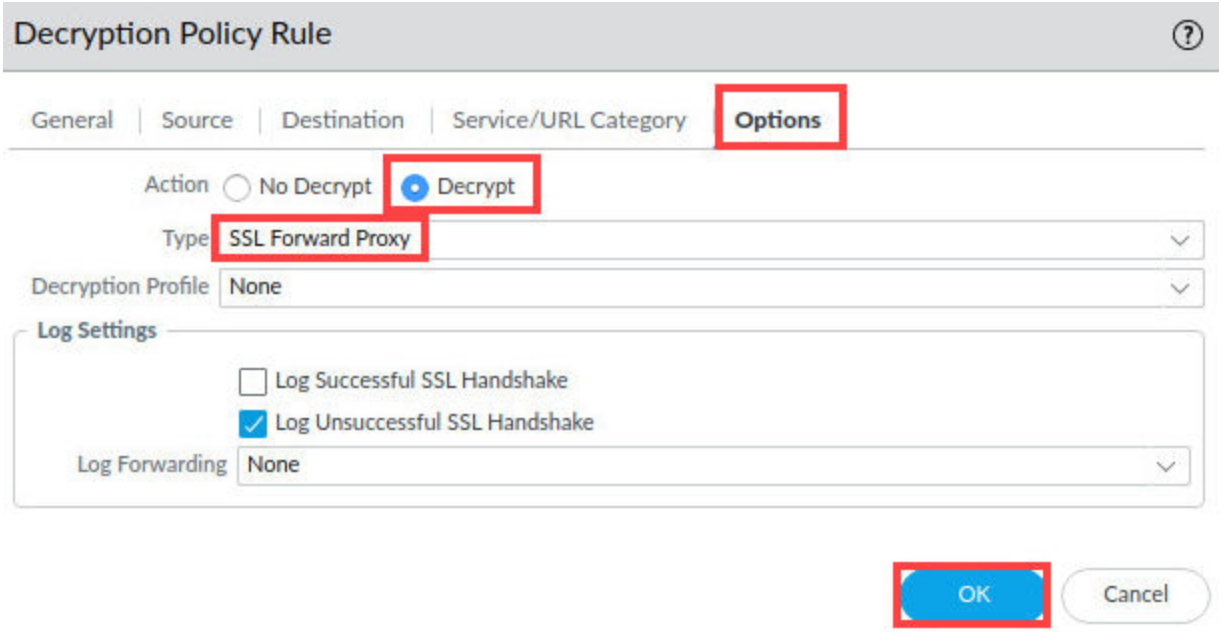
Please Note

Note that the Any setting for URL category instructs the firewall to decrypt all HTTPS traffic, regardless of the type of website users are accessing. Decrypting traffic from users to website categories such as Health and Medicine, Shopping or Government can expose Personally Identifiable Information (PII). In a production environment, you will need to make sure you only decrypt traffic which is appropriate.

Later in this lab, you will exclude several categories of websites as an illustration.

19. Click the **Options** tab and configure the following. Click **OK**.

Parameter	Value
Action	**Decrypt**
Type	**SSL Forward Proxy**
Decryption Profile	**None**



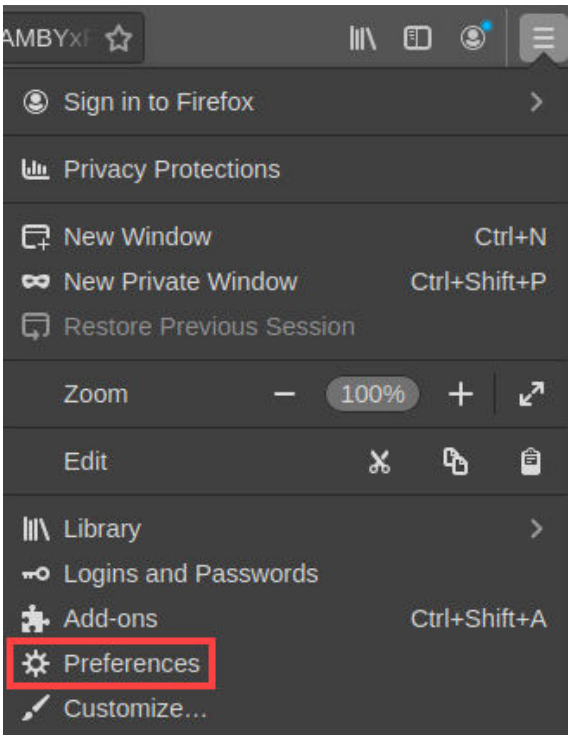
20. Verify the Decryption policy is visible, and the configuration matches the following.

		Source	Destination				
	NAME	ZONE	ZONE	URL CATEGORY	SERVICE	ACTION	TYPE
1	Decrypt_User_Traffic	Users_Net	Extranet Internet	any	any	decrypt	ssl-forward-proxy

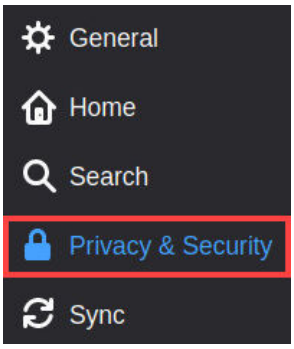
21. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

22. On the *client desktop*, open the **Firefox Web Browser** application.

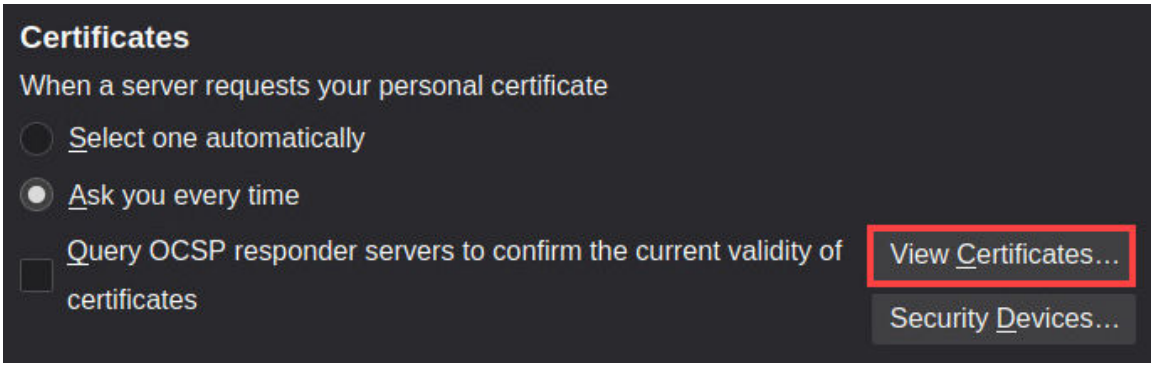
23. In the upper-right corner of the window, click the "**hamburger**" button and choose **Preferences**.



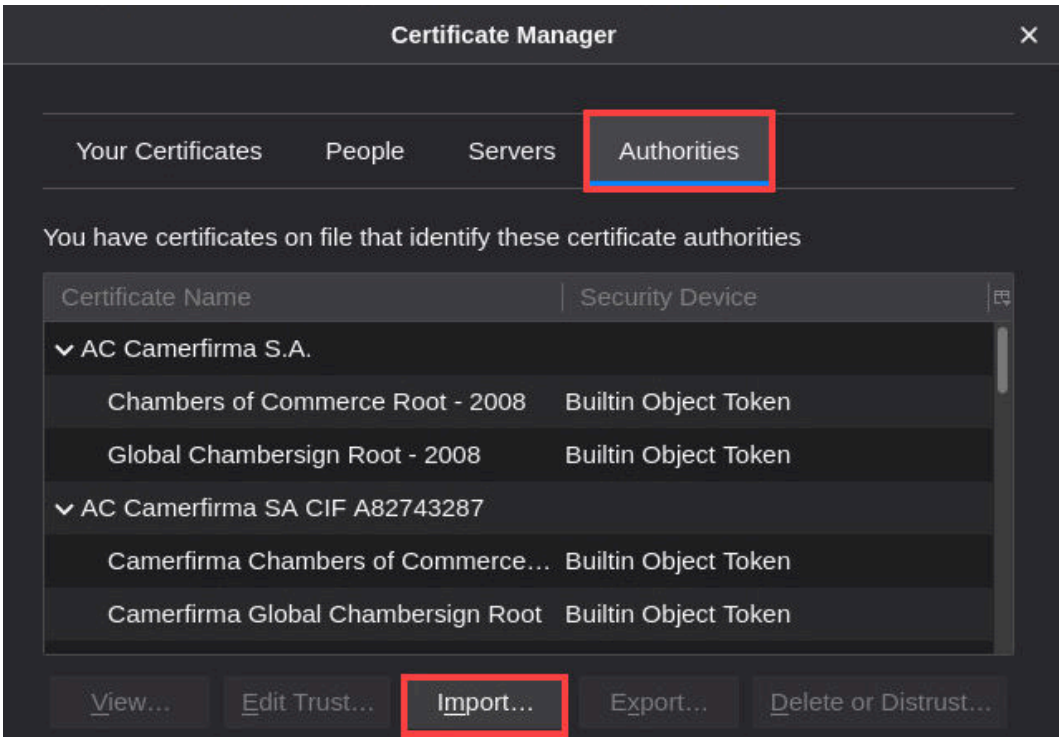
24. On the left side of the *Preferences* screen, select **Privacy & Security**.



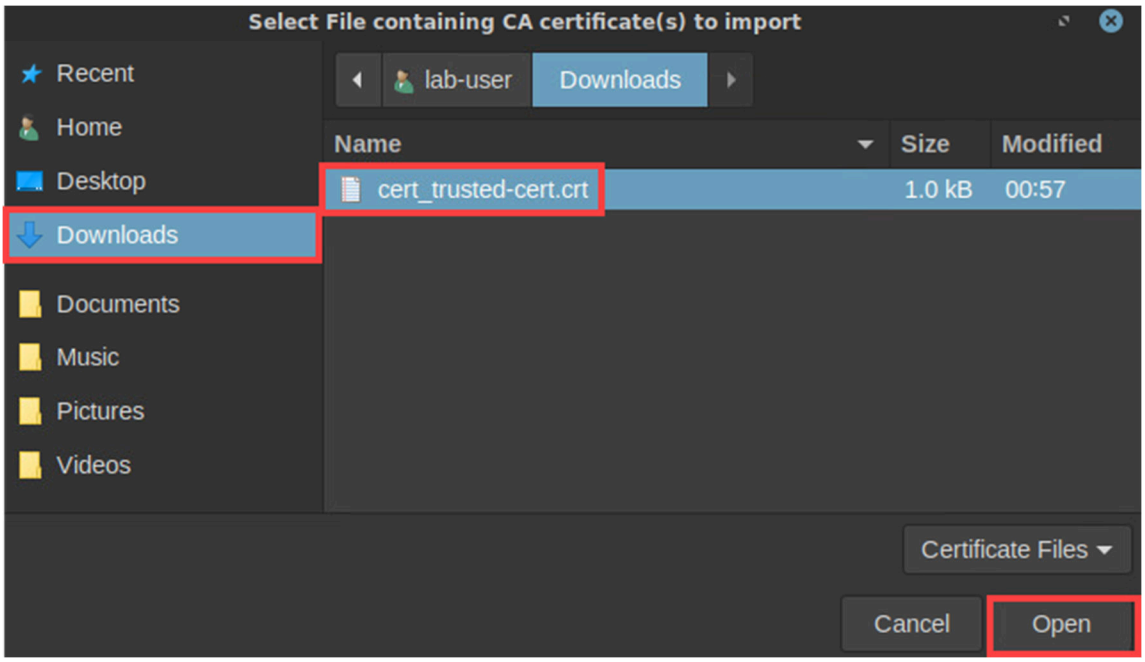
25. Scroll to the bottom of the screen and locate the *Certificates* section. Click **View Certificates**.



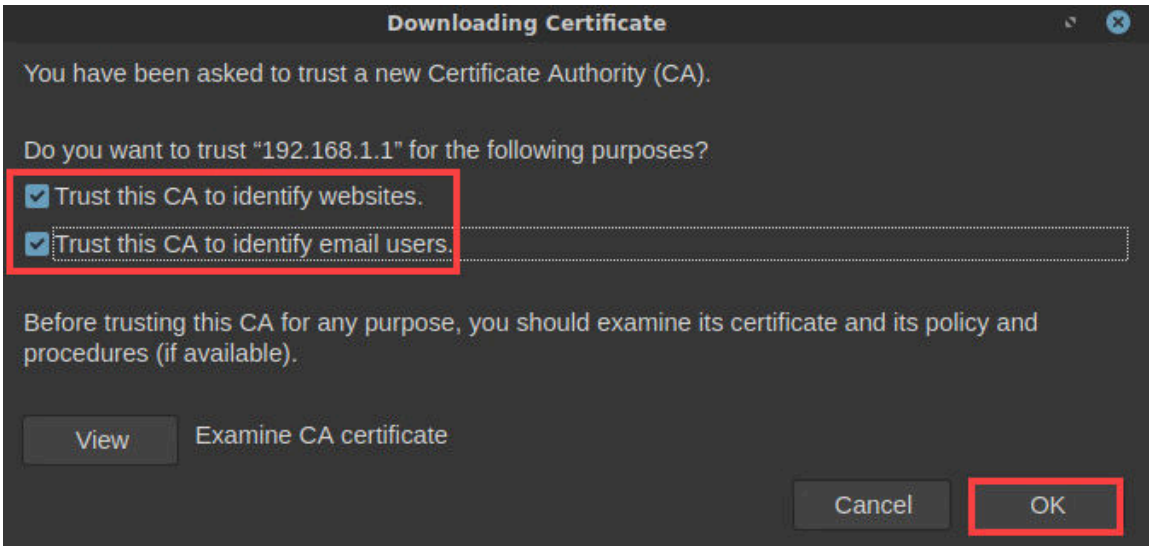
26. In the *Certificate Manager* window, select the **Authorities** tab. Click **Import**.



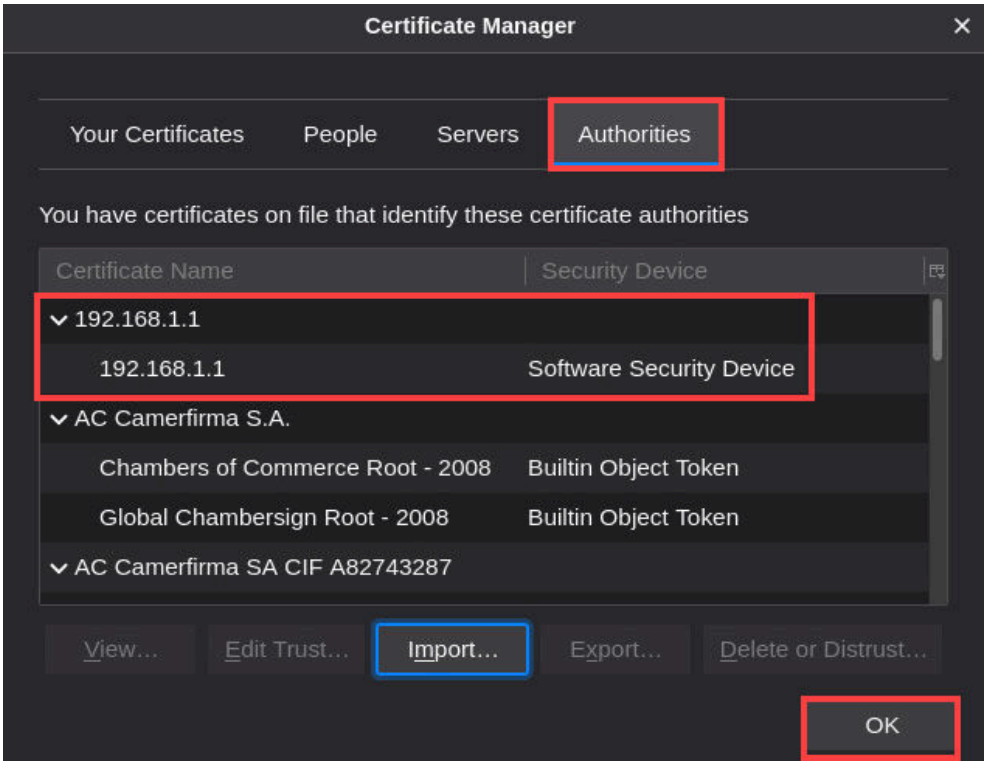
27. In the *Select File containing CA certificate(s) to import* window, click **Downloads**. Select **cert_trusted-cert.crt** and click **Open**.



28. In the *Downloading Certificate* window, place **checks** in both boxes for **Trust this CA**. Click **OK**.



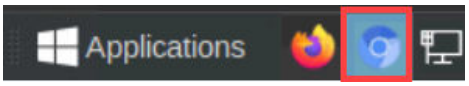
29. The firewall **trusted-cert** entry appears in the list of certificate authorities. Click **OK**.



Please Note

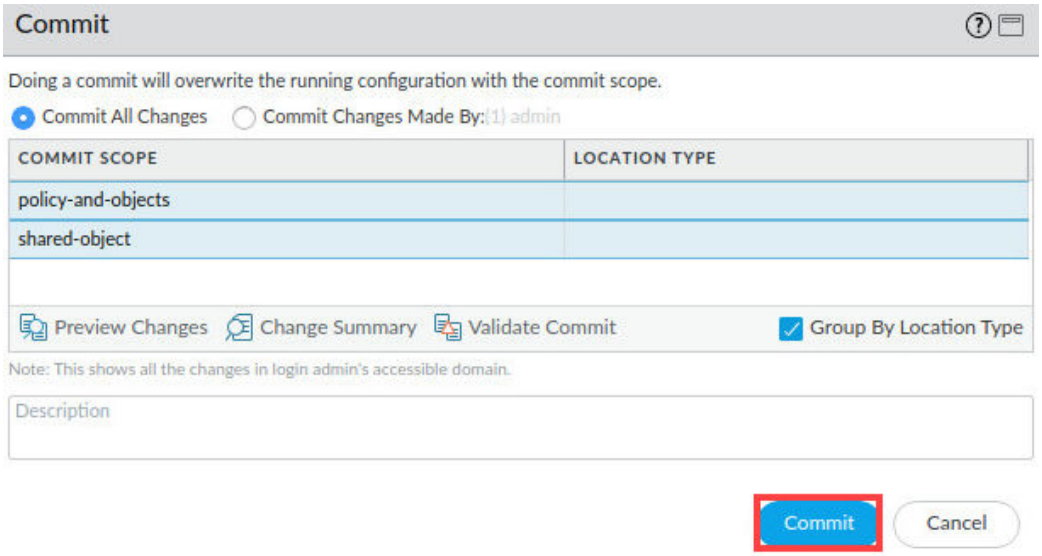
The Firefox browser will trust any certificate issued by the entities in this Authorities list. By adding the firewall certificate to this list, the Firefox browser will trust any certificates issued by the firewall. Note that the process of importing certificates to client workstations varies based on the browser type and the operating system.

30. Reopen the *PA-VM firewall* web interface by clicking on the **Chromium** icon in the taskbar.

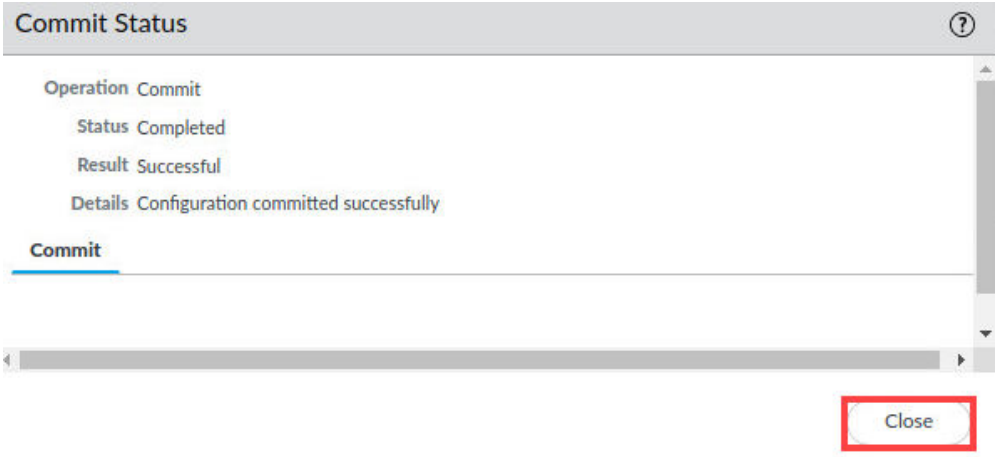


31. Click the **Commit** link located at the top-right of the web interface.

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



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



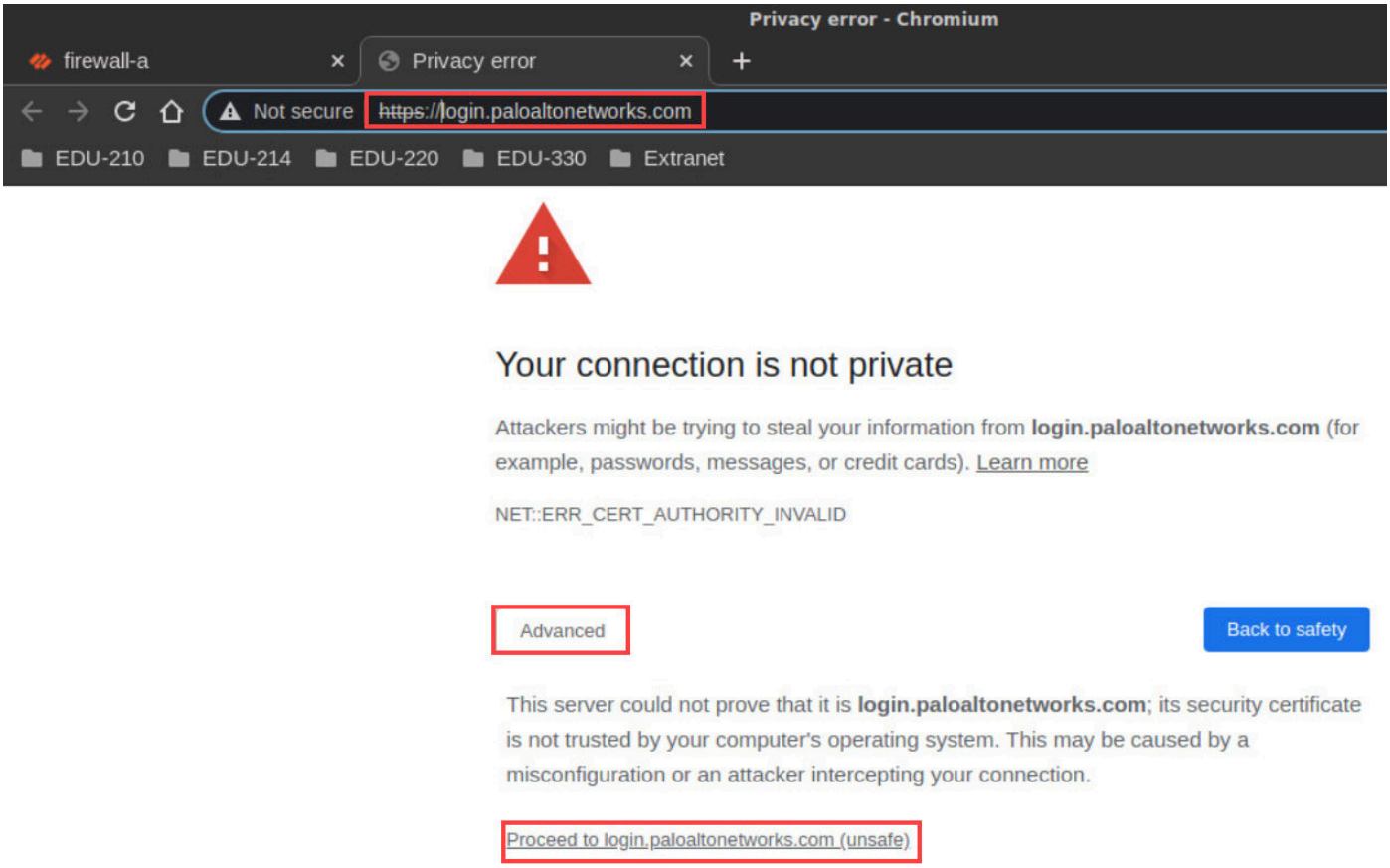
34. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

1.3 Test the Firewall Behavior Without Credential Detection

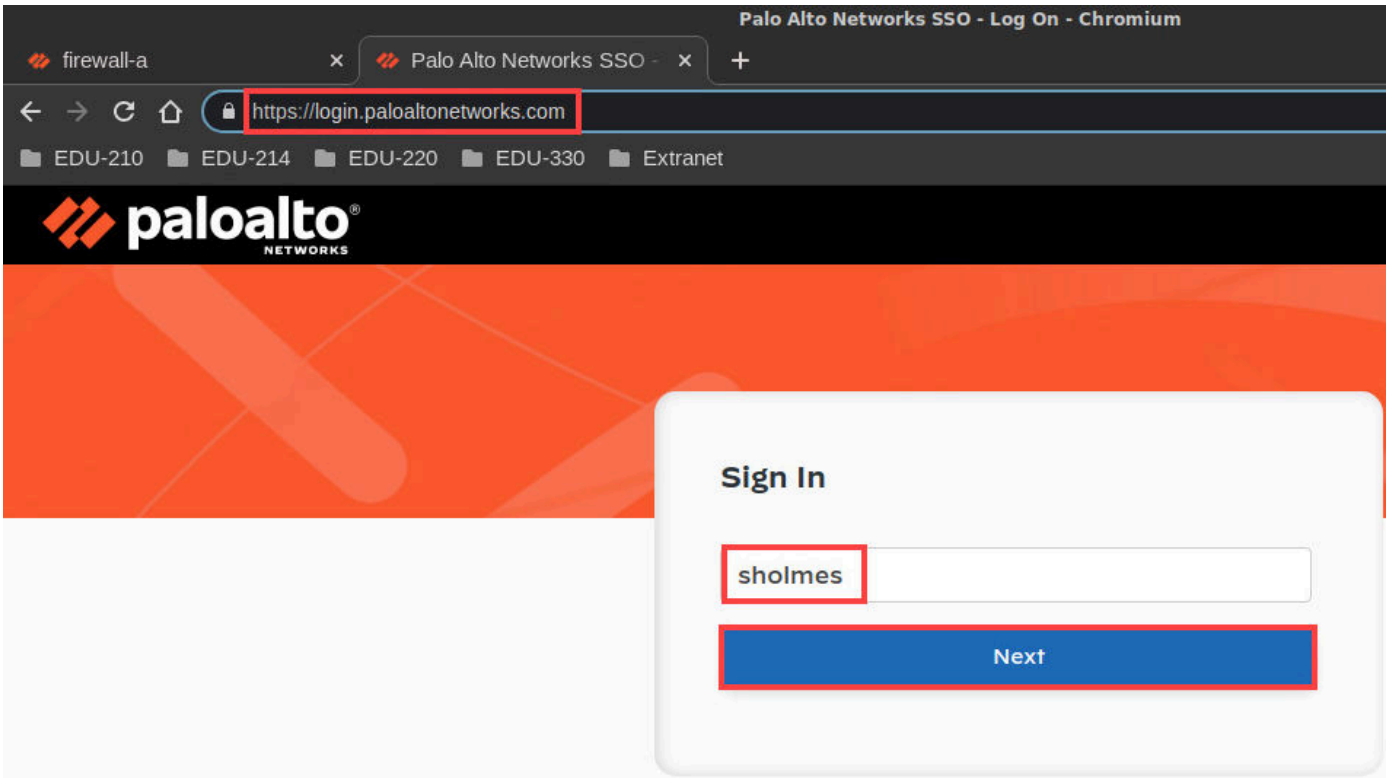
In this section, you will connect to an internet website and enter a fictitious user's domain credentials. This action will allow you to see how the firewall behaves without Credential Detection configured.

1. Open a new tab in **Chromium**.

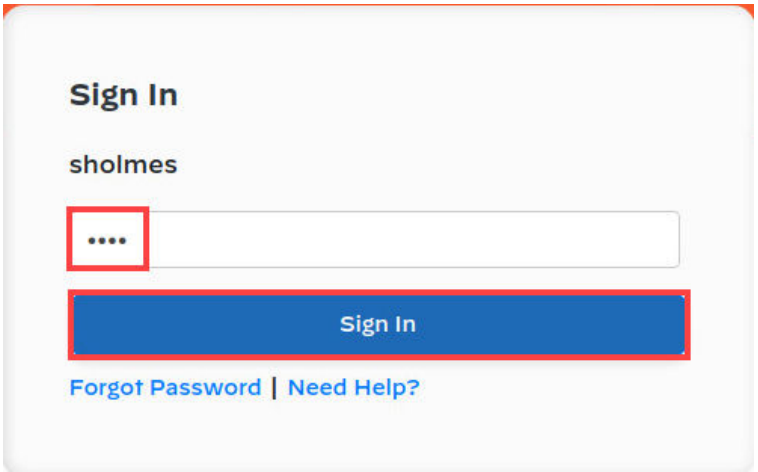
2. Type **`https://login.paloaltonetworks.com`** and press **Enter**. Click **Advanced** and **Proceed to login.paloaltonetworks.com (unsafe)**.



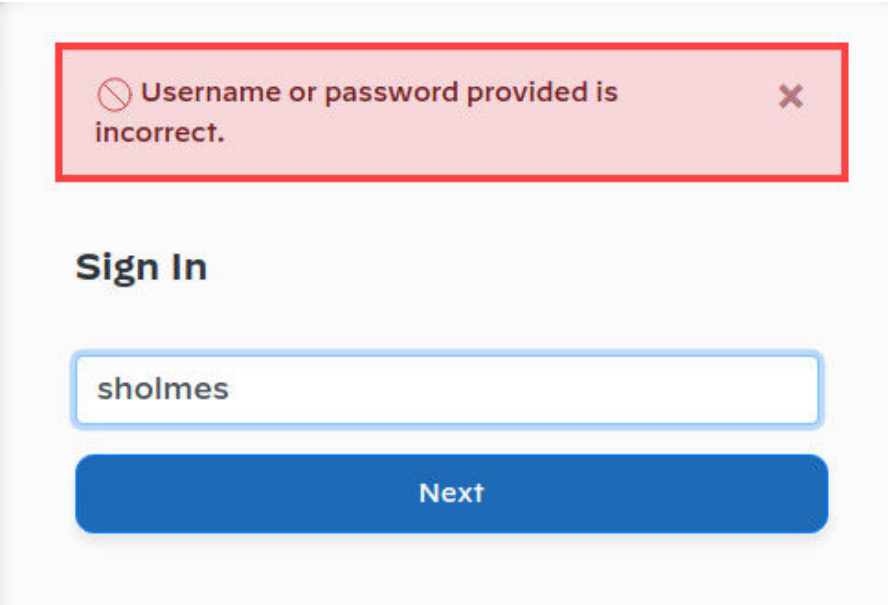
3. For *Username*, enter **sholmes.** Click **Next.**



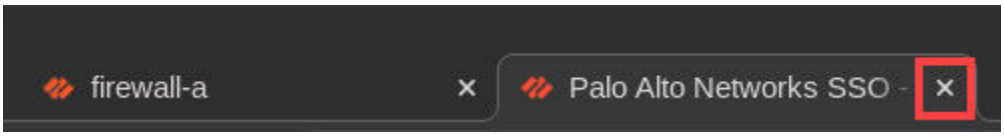
4. In the *Sign In* window, enter **1234** as the *password*. Click **Sign In**.



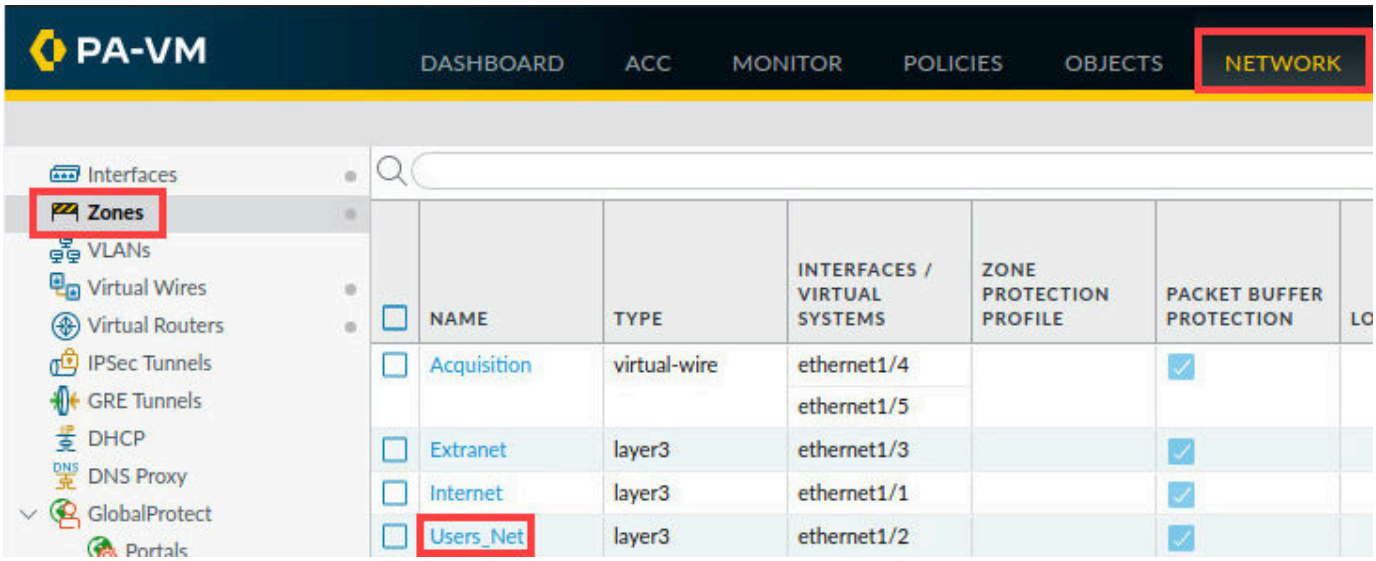
5. Because there is no account for **sholmes**, the site will present you with the *Username or password provided is incorrect* message.



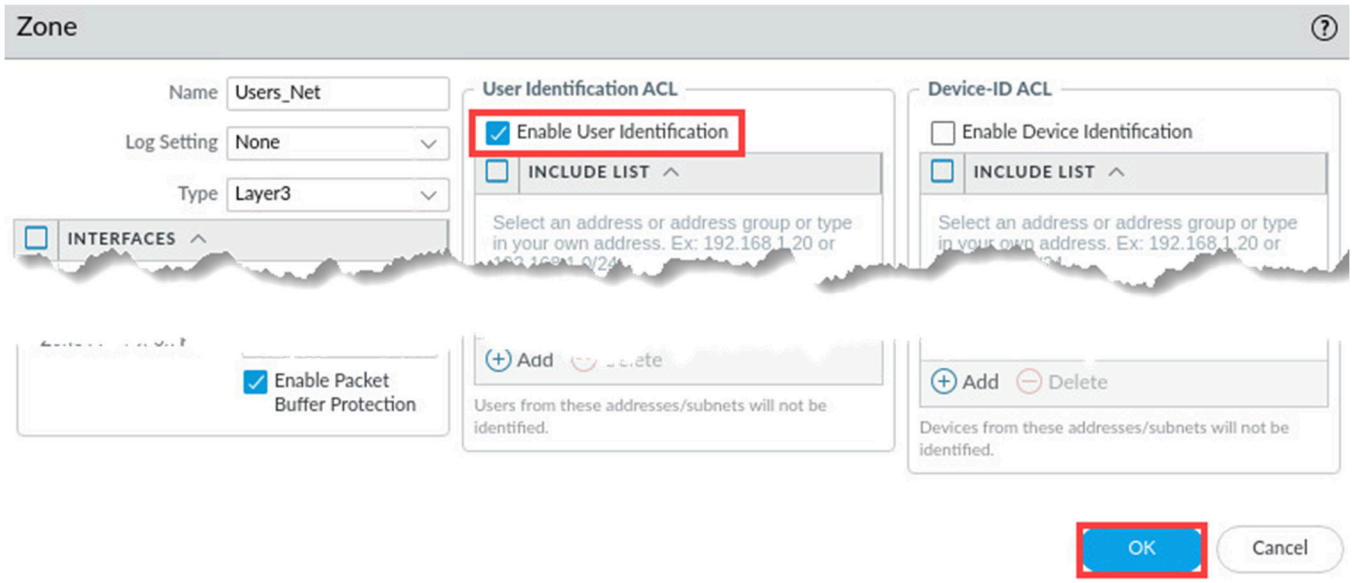
6. Close the *Chromium tab* for the *Palo Alto Networks SSO* by clicking the **X** icon.



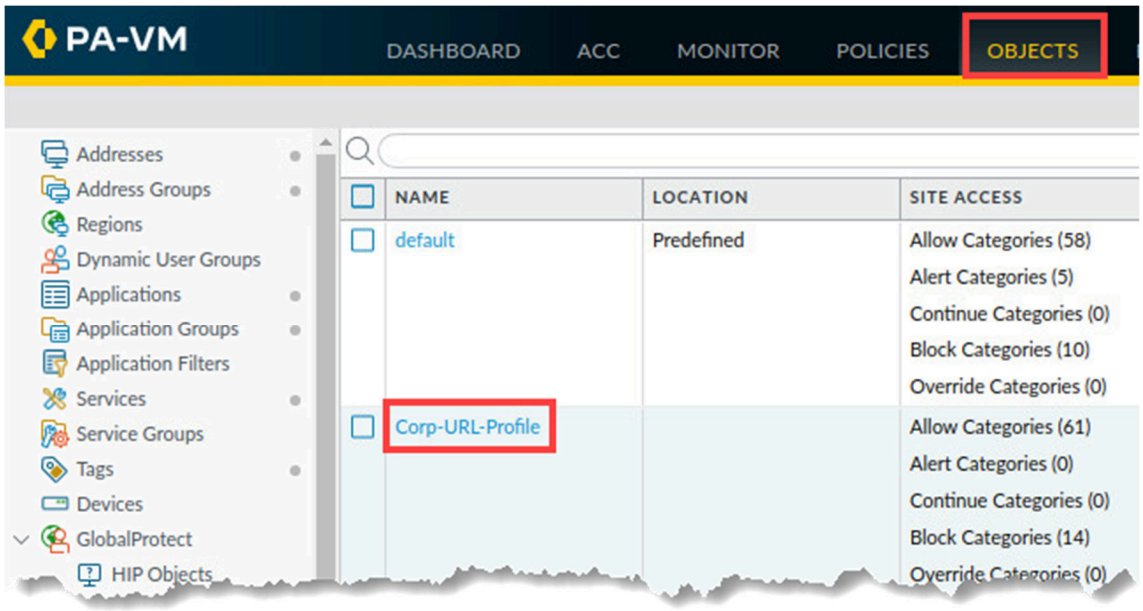
7. In the firewall web interface, select **Network > Zones**. Click the entry for the **Users_Net** to edit it.

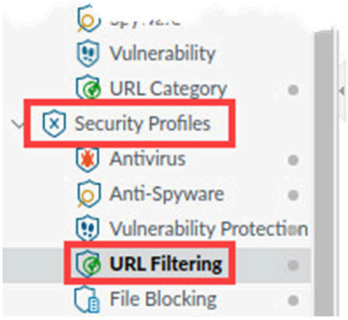


8. In the *Zone* window, click **Enable User Identification**. Click **OK**.

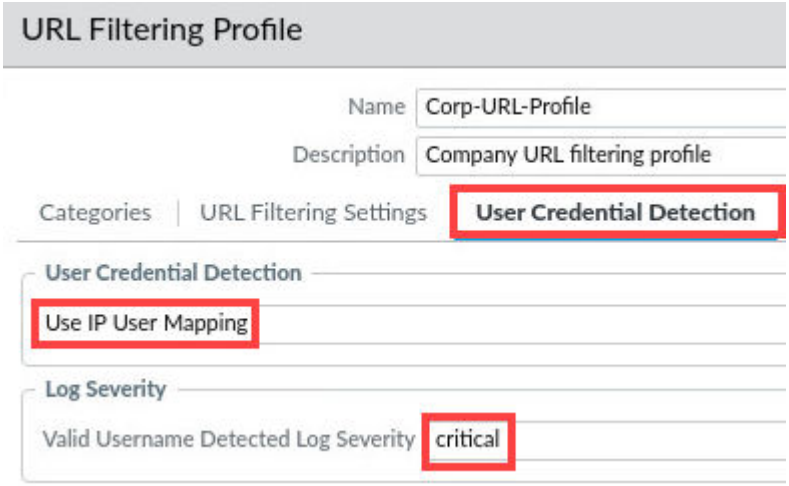


9. Select **Objects > Security Profiles > URL Filtering**. Click the entry for **Corp-URL-Profile**.

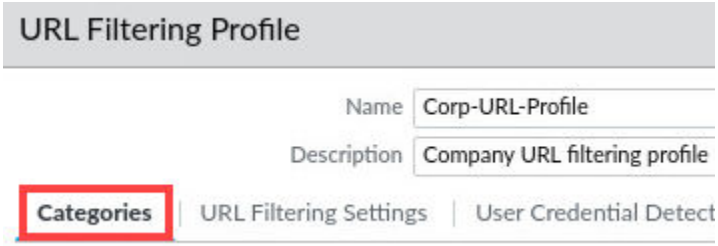




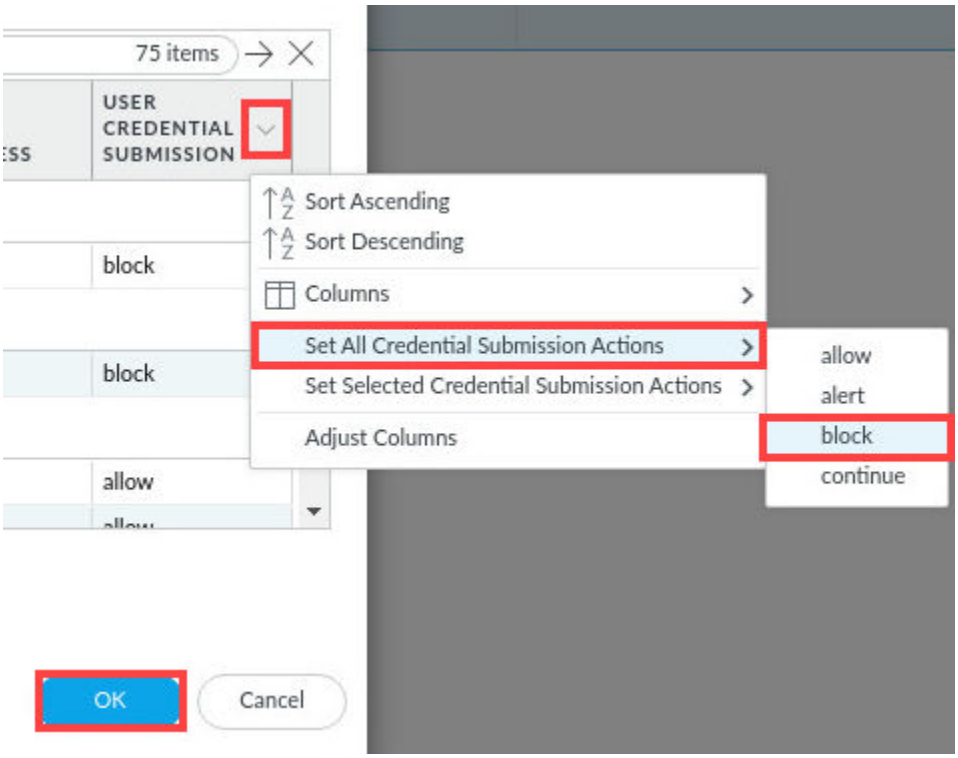
10. Select the tab for **User Credential Detection**. Select **Use IP User Mapping** for *User Credential Detection***.** Change the dropdown for *Valid Username Detected Log Severity* to **critical**.



11. In the *URL Filtering Profile*, select **Categories**.



12. Select set all **Credential Submission** actions to **block**. Click the small triangle next to the column header for *User Credential Submission***.** Hover your mouse over **Set All Credential Submission Actions** and select **block**. Click **OK**.



Please Note

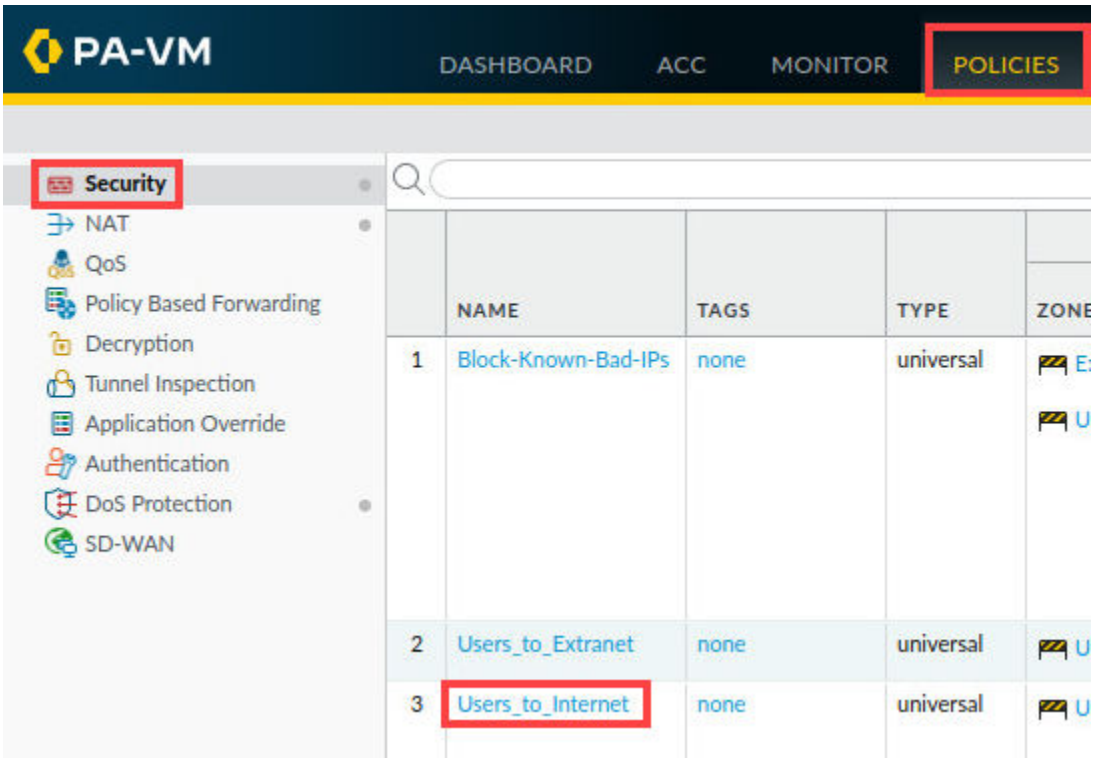
Note that setting all URL categories to block credential submissions is not a good idea in a production environment because no users would be able to submit any credentials to any website. In this lab, you will use this setting so that you do not have to select individual categories and change the option.

13. Leave the *Palo Alto Networks Firewall* open and continue to the next task.

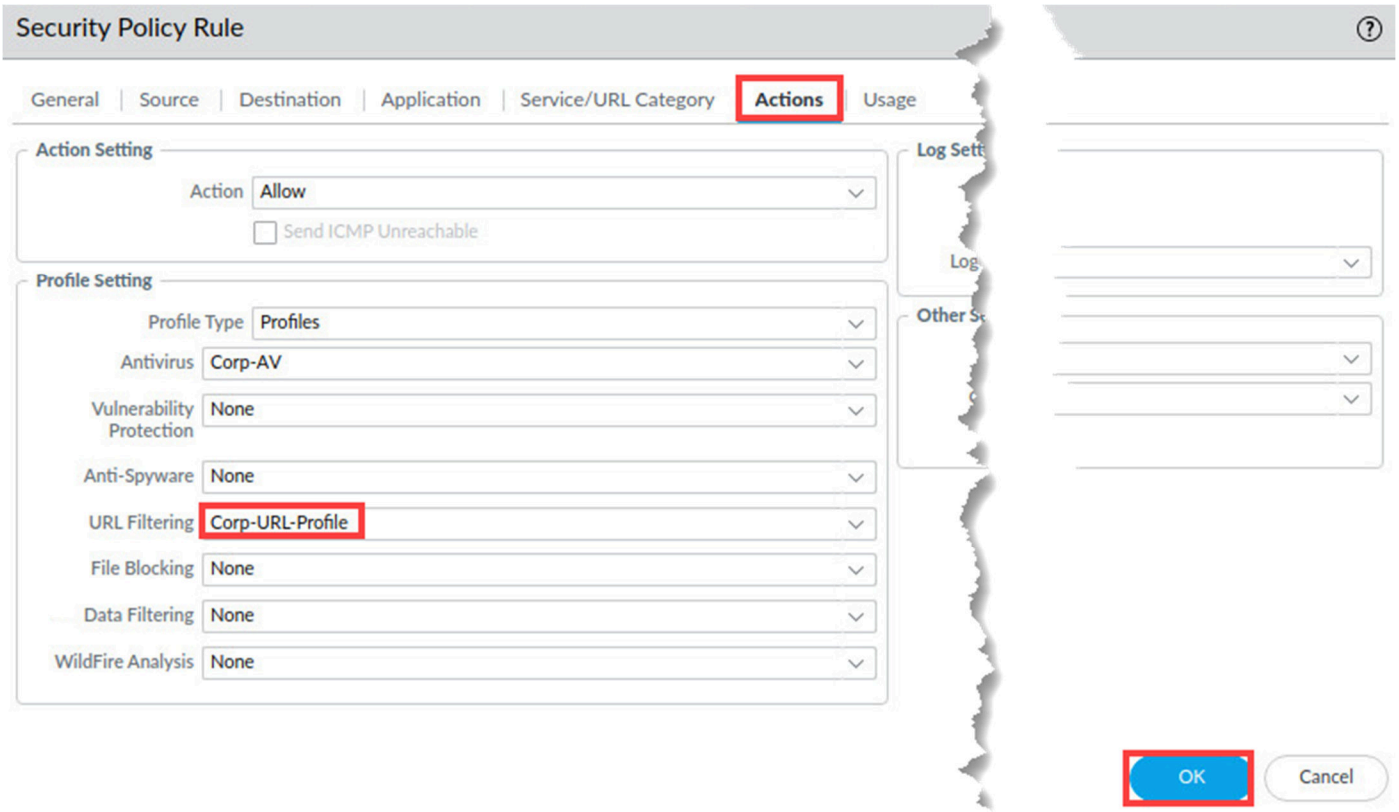
1.4 Apply the Corp-URL-Profile to Security Policy

In this section, you will apply the Corp-URL-Profile to the security policy rule, which allows user traffic to reach the internet.

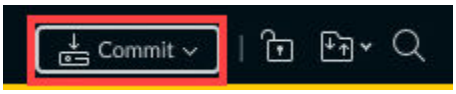
1. Select **Policies > Security**. Click the **Users_to_Internet** security policy.



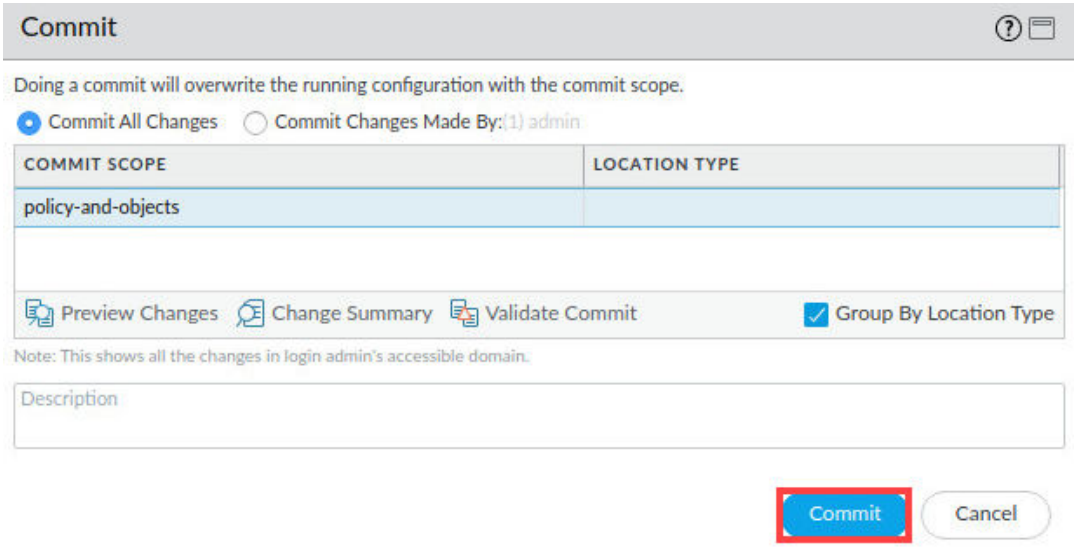
2. In the *Security Policy Rule* window, click the **Actions** tab. Under *Profile Settings*, use the dropdown list to select **Profiles**. For *URL Filtering*, select **Corp-URL-Profile**. Click **OK**.



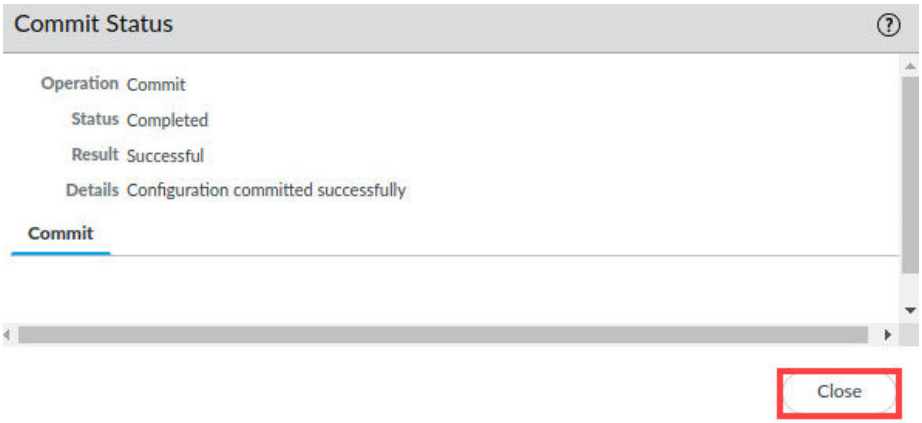
3. Click the **Commit** link located at the top-right of the web interface.



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



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



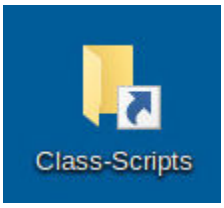
6. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

7. Close the *Preferences – Mozilla Firefox* window by clicking the **X** icon.

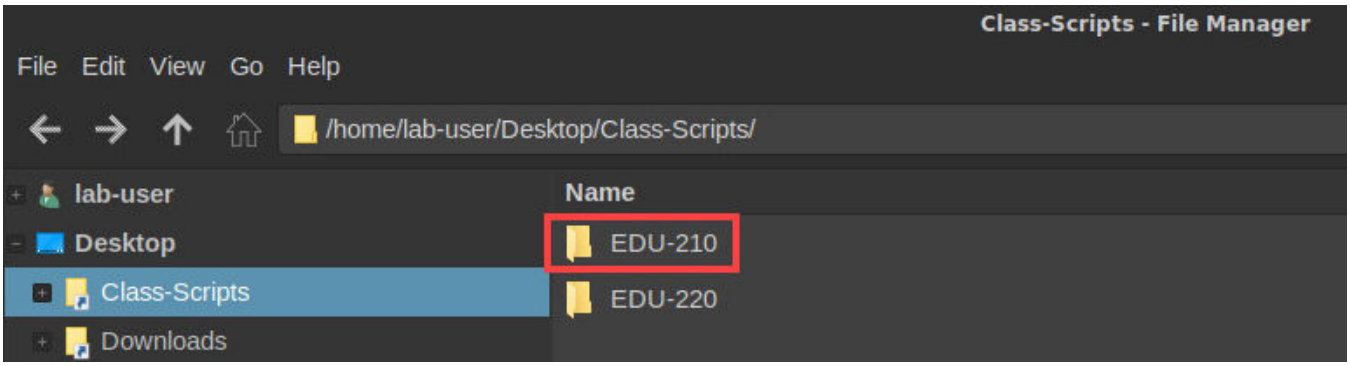
1.5 Provide the Firewall with User-ID Information

In this section, you will run a short script that generates application traffic from your client workstation to hosts in the internet and Extranet security zones.

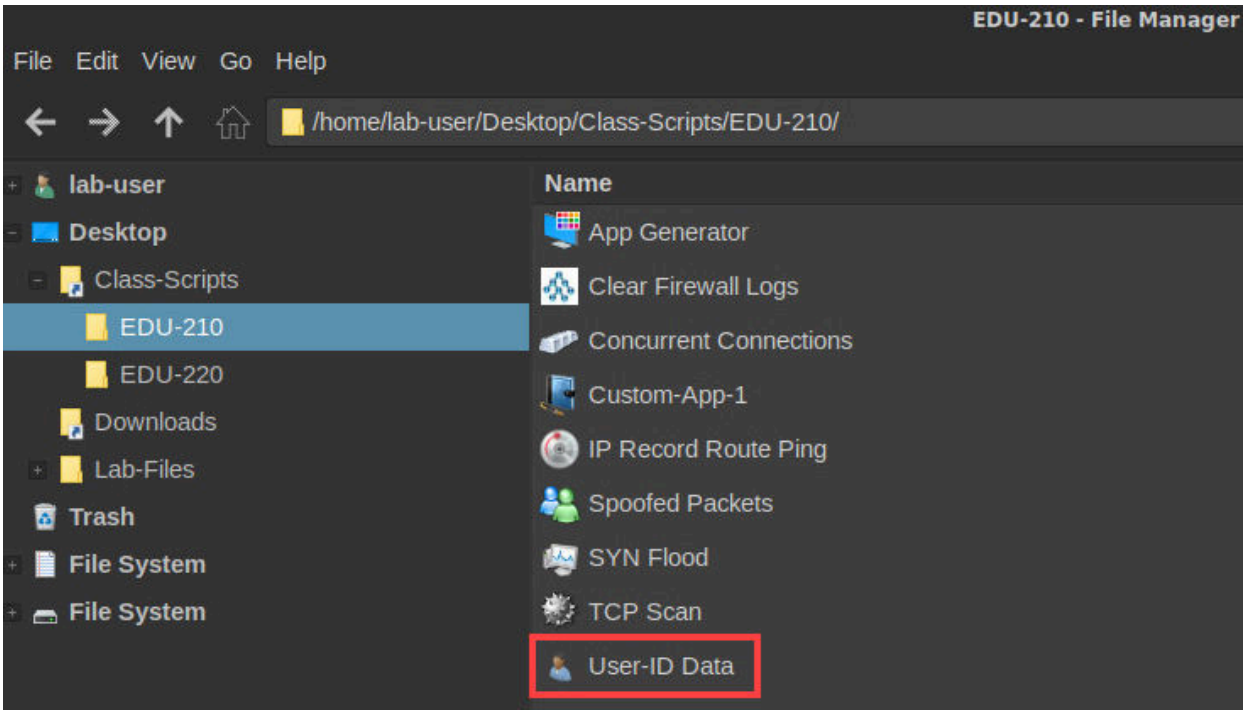
1. On the *client* desktop, double-click the folder for **Class-Scripts**.



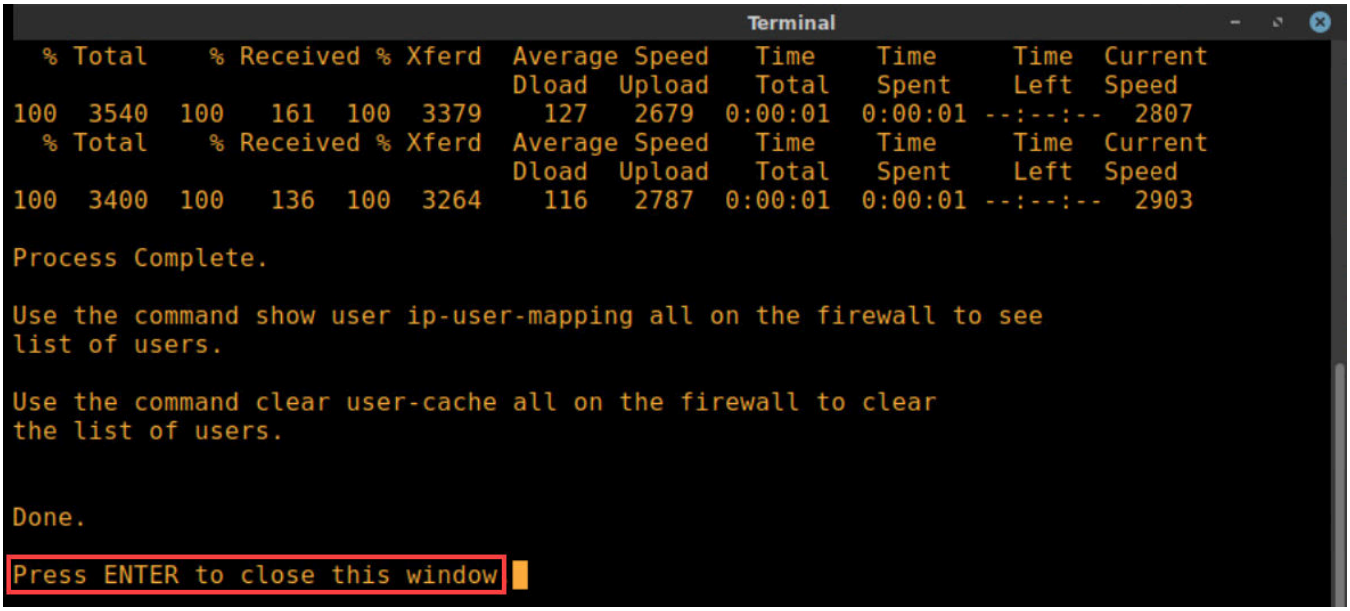
2. Open the **EDU-210** folder.



3. Execute the **User-ID Data** script by double-clicking it.



4. Notice the *Terminal* window will pop up. Allow the *User-ID Data* script to finish before moving to the next step. Press **Enter**.

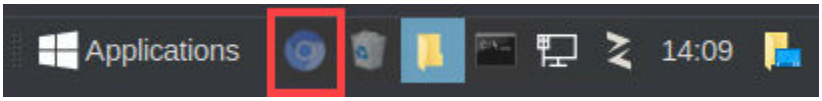


Please Note

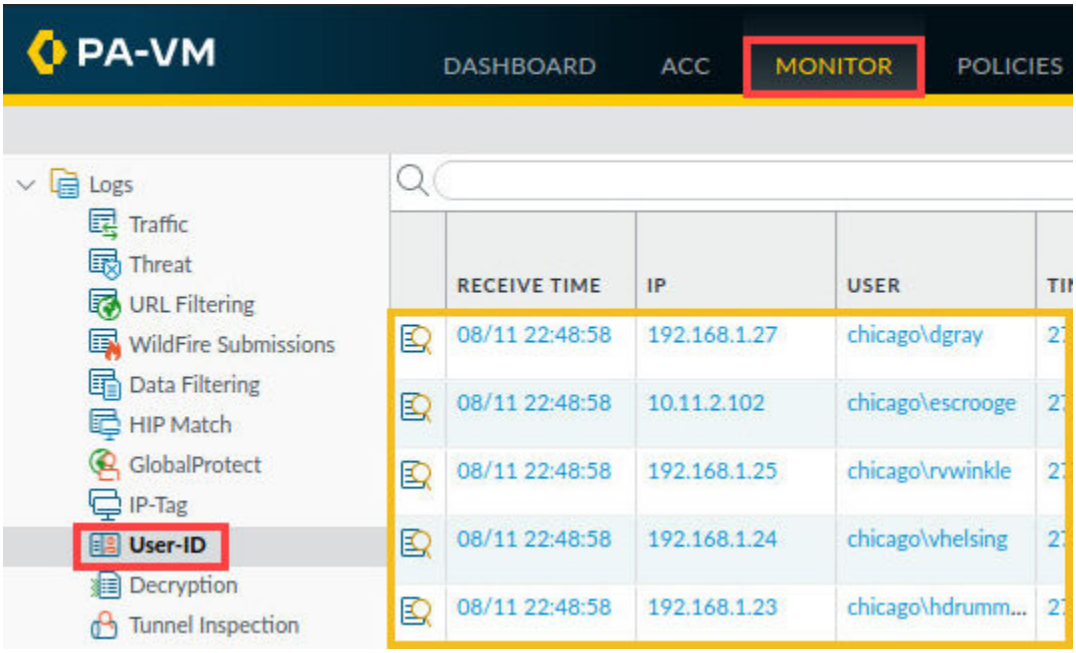
This script uses the XML API to send a list of users, IP addresses and groups to the firewall.

5. Close the *EDU-210 - File Manager* window by clicking the **X** icon.

6. Reopen the *PA-VM firewall* by clicking on the **Chromium** icon in the taskbar.



7. Select **Monitor > User-ID**. You should see numerous entries indicating that the firewall has User-to-IP mappings.



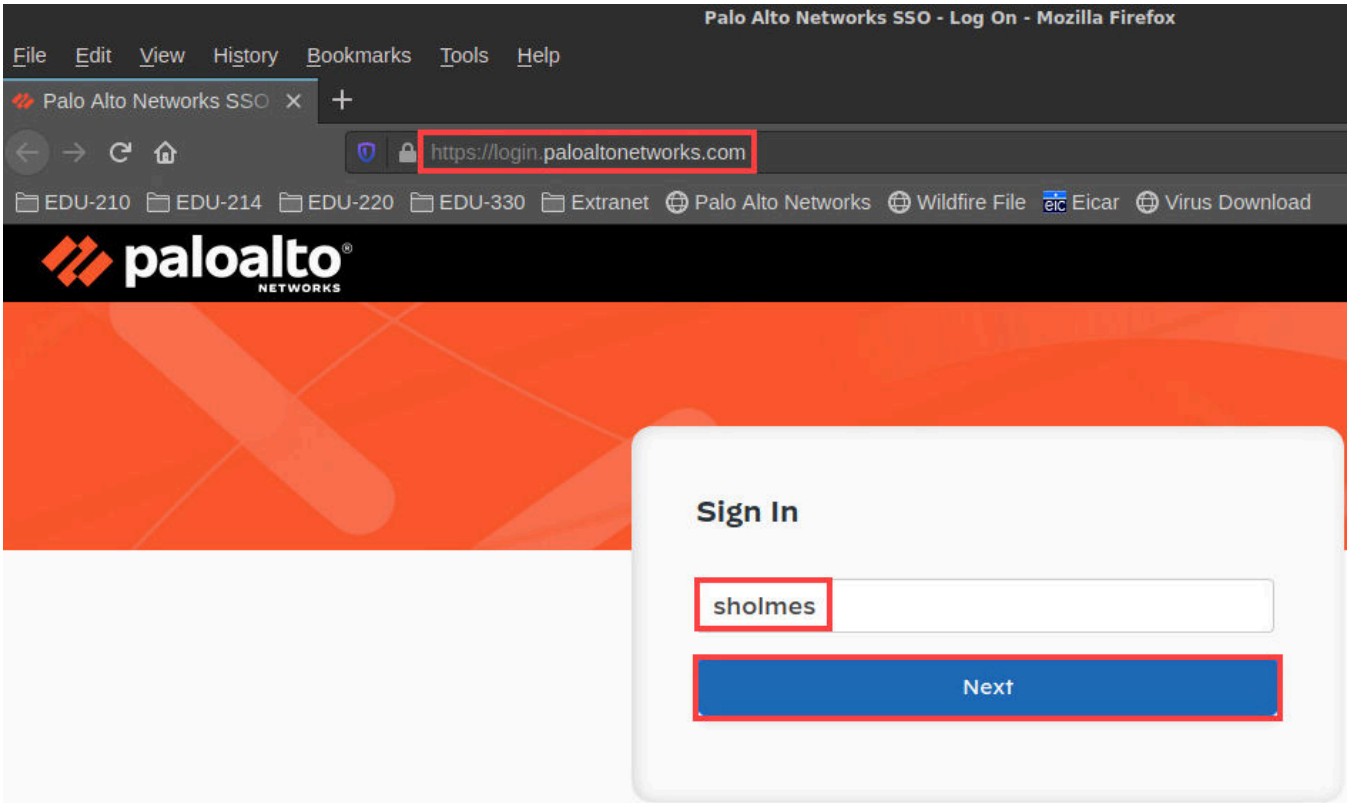
8. Minimize the *Palo Alto Networks Firewall* and continue to the next task.

1.6 Test the Firewall Behavior with Credential Detection

In this section, you will test the firewall behavior with credential detection.

1. On the *client desktop*, open the **Firefox Web Browser** application.

2. Type **`https://login.paloaltonetworks.com`** and press **Enter**. For *Username*, enter **`sholmes`**. Click **Next.**

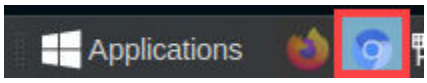


3. The firewall will present a window indicating that you have submitted your credentials to a blocked site. Close the *Firefox browser* using the **X** icon.

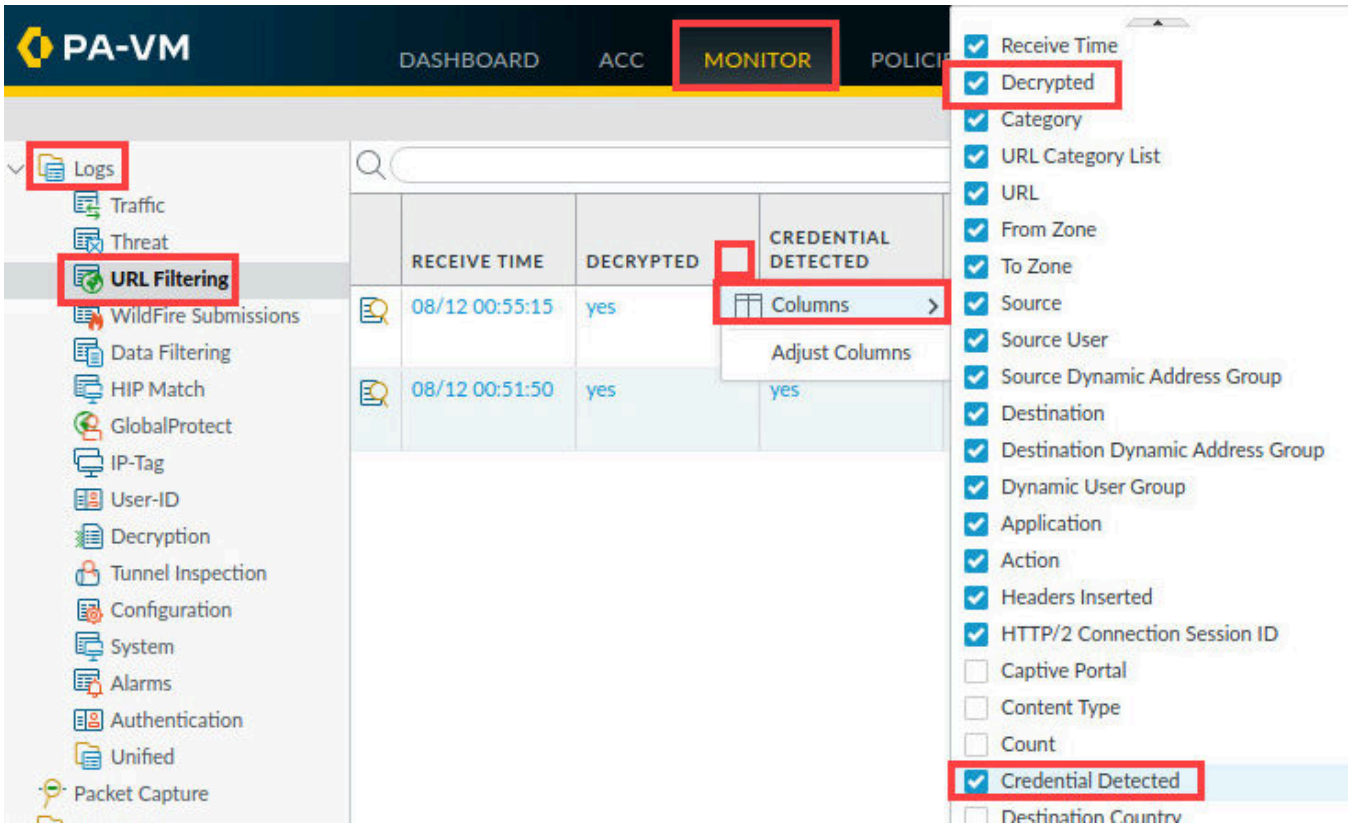
Please Note

Recall that before configuring Credential Detection, the firewall allowed you to submit the username and even a password to the website. With Credential Detection enabled, the firewall blocks the session when you submit a username which belongs to the domain.

4. Reopen the *firewall* web interface by clicking on the **Chromium** icon in the taskbar.

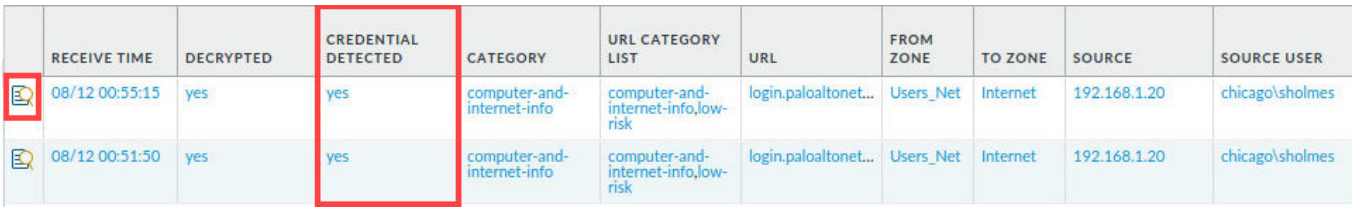


5. Select **Monitor > URL Filtering**. Modify the URL Filtering table by adding the **Credential Detected** and **Decrypted** columns.

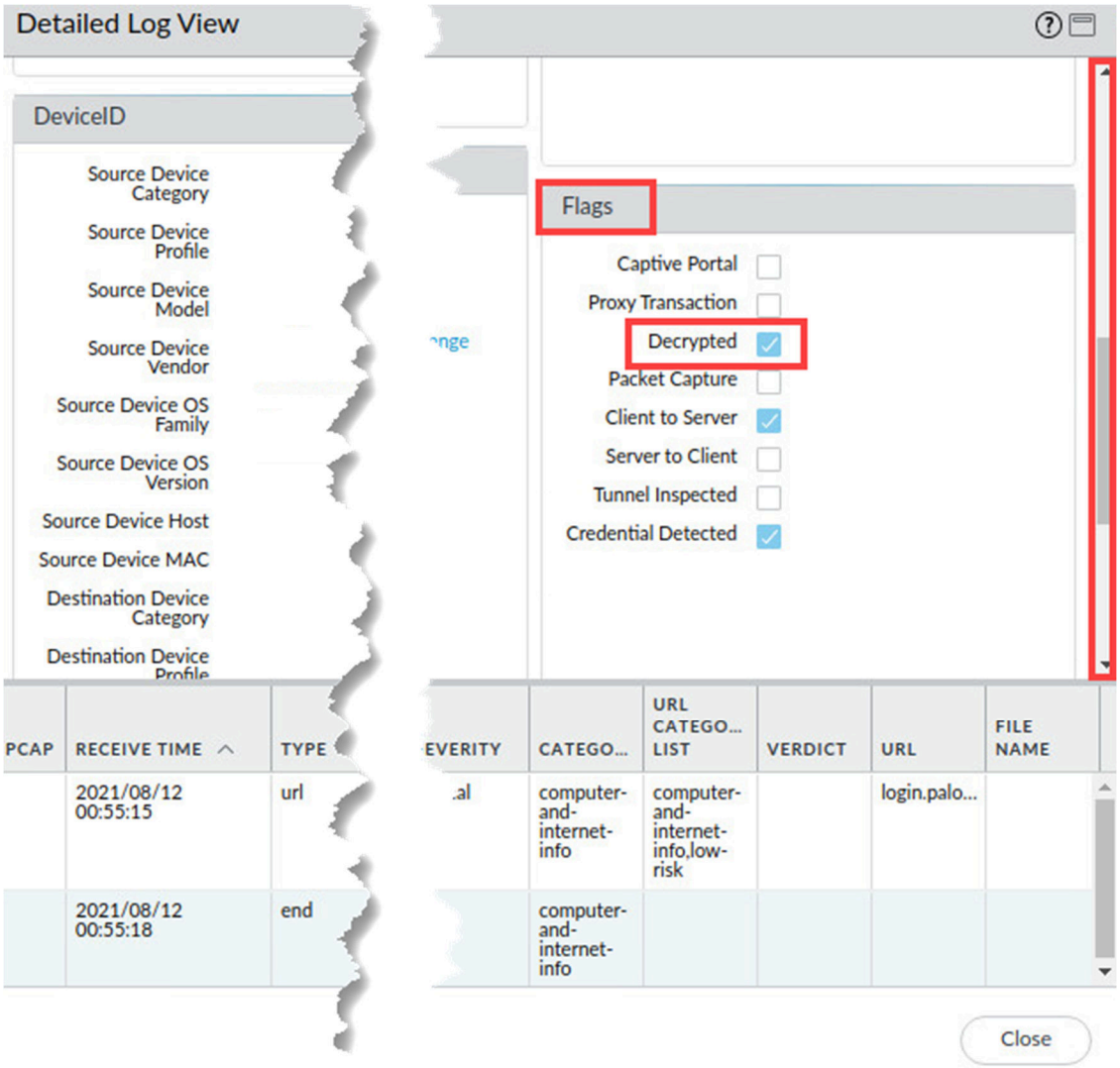


6. Clear any filters you may have in place. In the *filter* field, enter the following filter **`( action eq block-url )`** to display only entries that have been blocked. Press **Enter** to apply the filter.

7. Note the information displayed under the *Credential Detected* column. Click the **magnifying glass** icon to see more detailed information about this entry.



8. In the *Detailed Log View* window, scroll down and locate the *Flags* section. Note the checkbox for **Decrypted,** which indicates that the firewall decrypted this traffic and was able to detect an attempted credential submission.



9. The lab is now complete; you may end your reservation.