CYBERSECURITY FOUNDATION V2

Lab 6: Allowing Only Trusted Applications

Document Version: 2022-12-22

Contents

Introduction

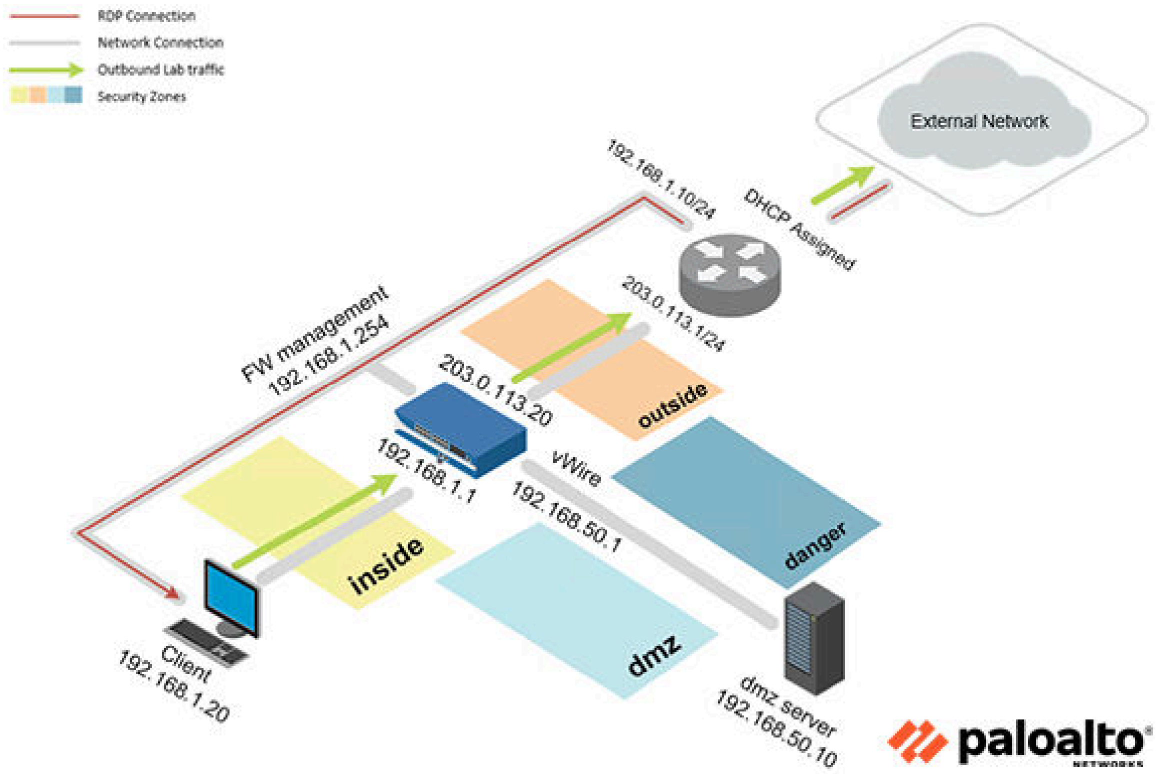
In this lab, you will configure the Firewall to only allow trusted applications by creating an application group and adding it to an existing security policy.

Objective

In this lab, you will perform the following tasks:

- Create an Application Group
- Modify Security Policy
- Commit and Test

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.

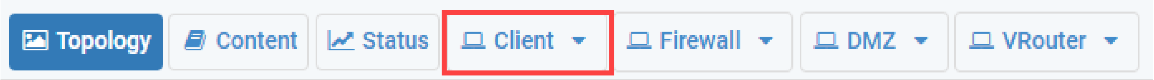
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Allowing Only Trusted Applications

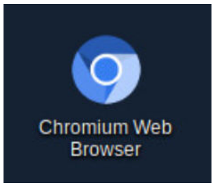
1.0 Load Lab Configuration

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

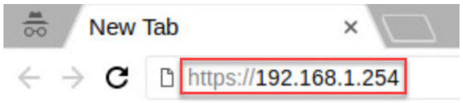
1. Click on the **Client** tab to access the Client PC.



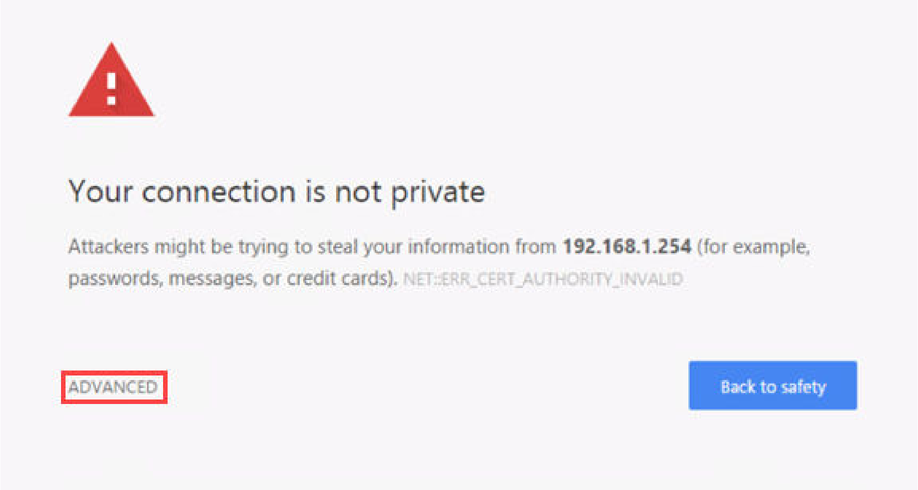
2. Log in to the Client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium Web Browser** icon located on the desktop.



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.

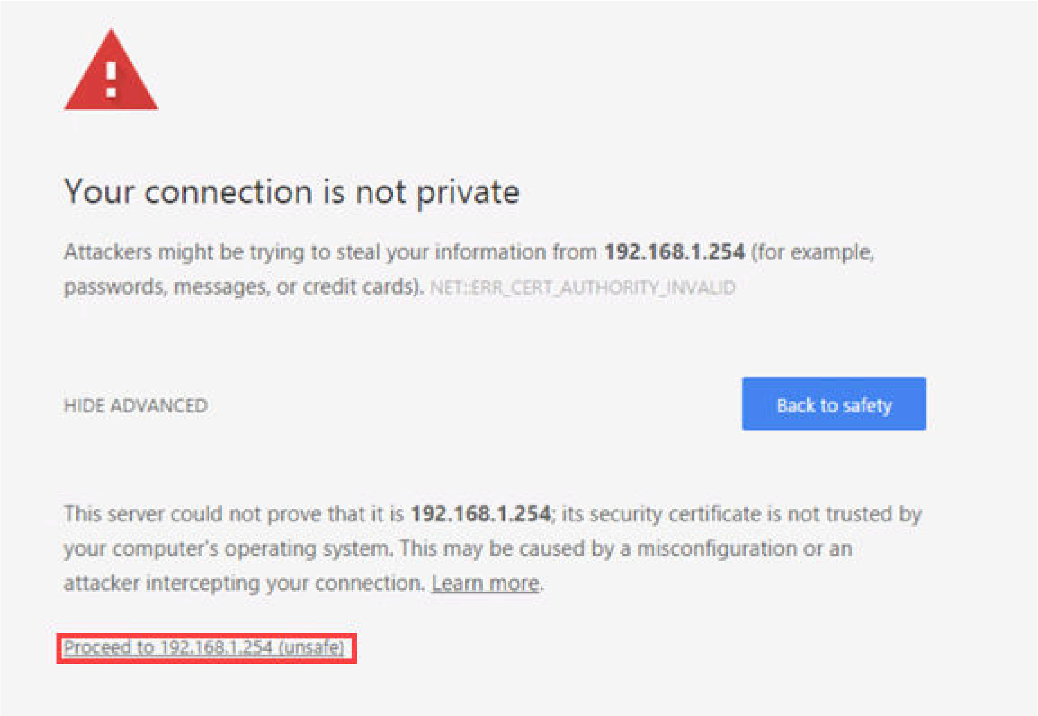


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

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)**.

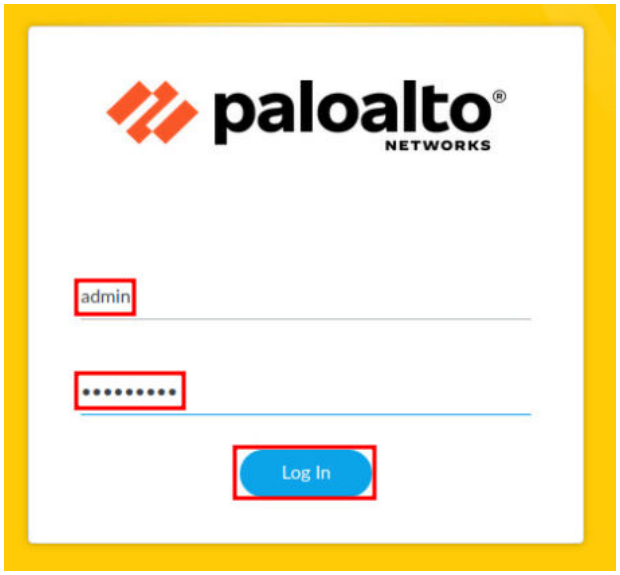


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

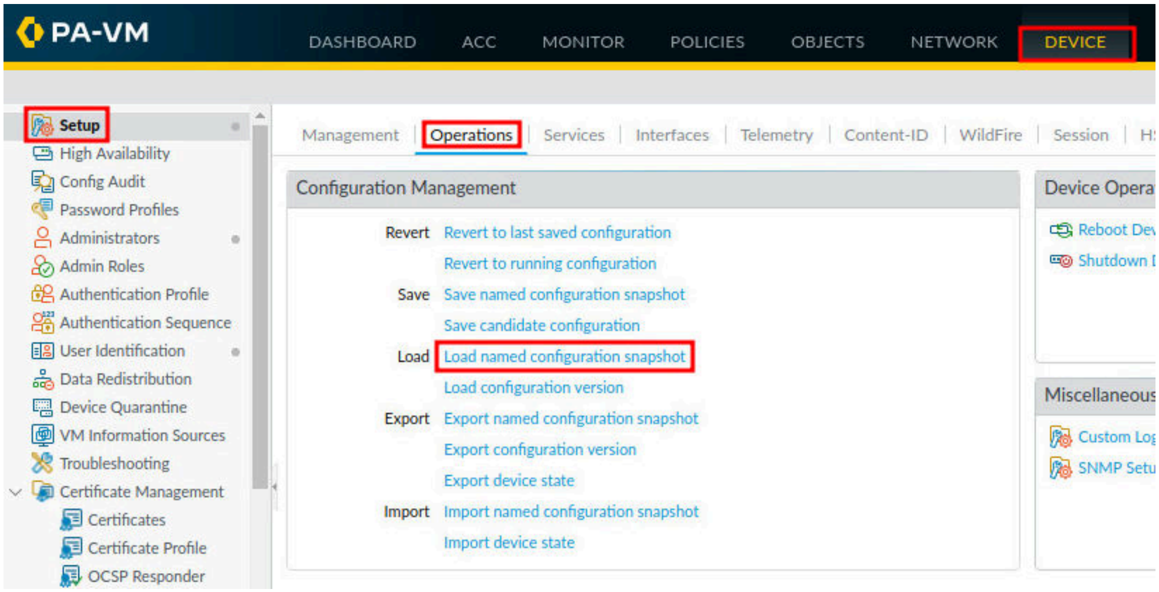
7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.



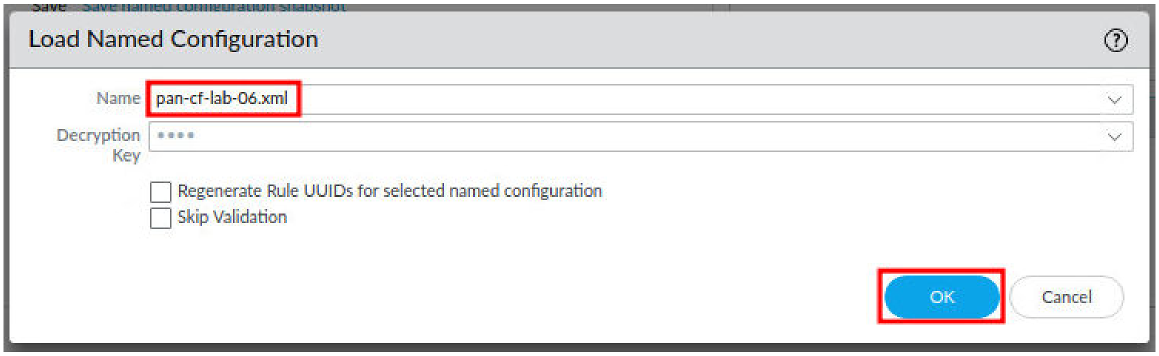
admin

•••••••••

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-06.xml** from the *Name* dropdown box and click **OK**.

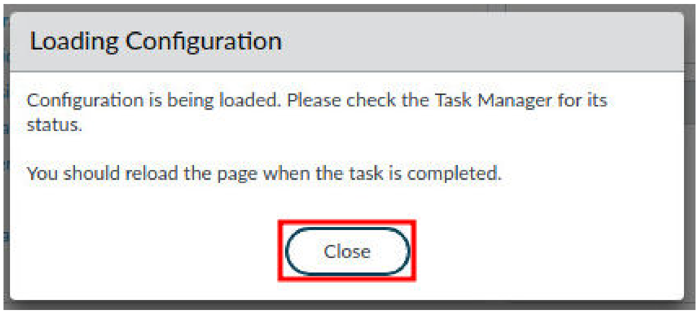


Load Named Configuration

Name: pan-cf-lab-06.xml

Decryption Key: ••••

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.

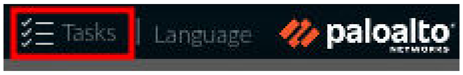


Loading Configuration

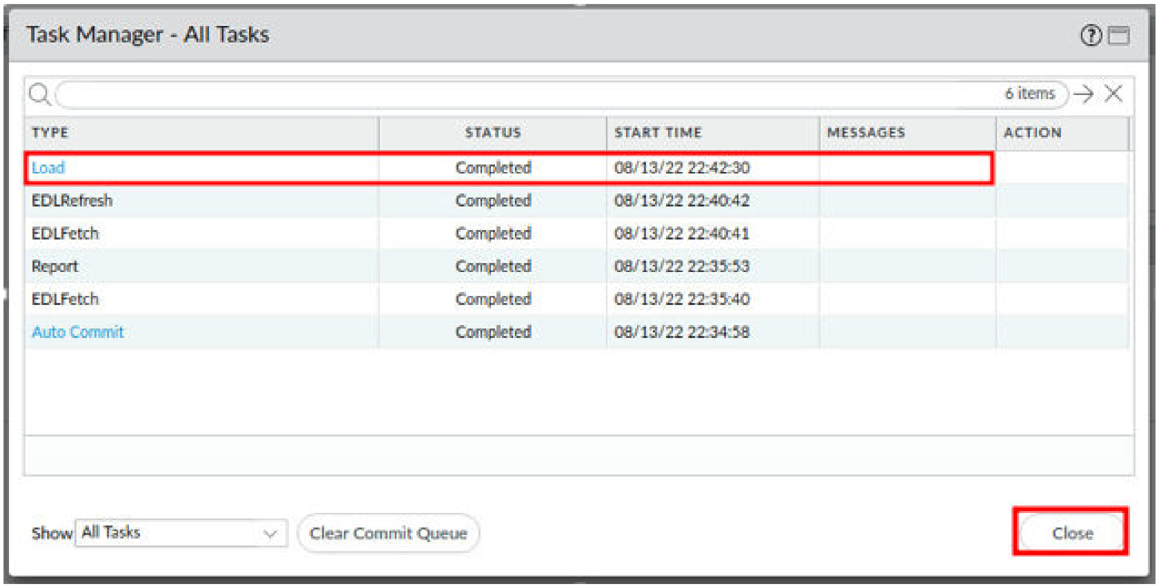
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

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



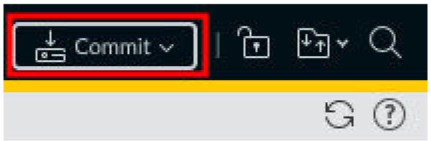
12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close.**


Task Manager - All Tasks

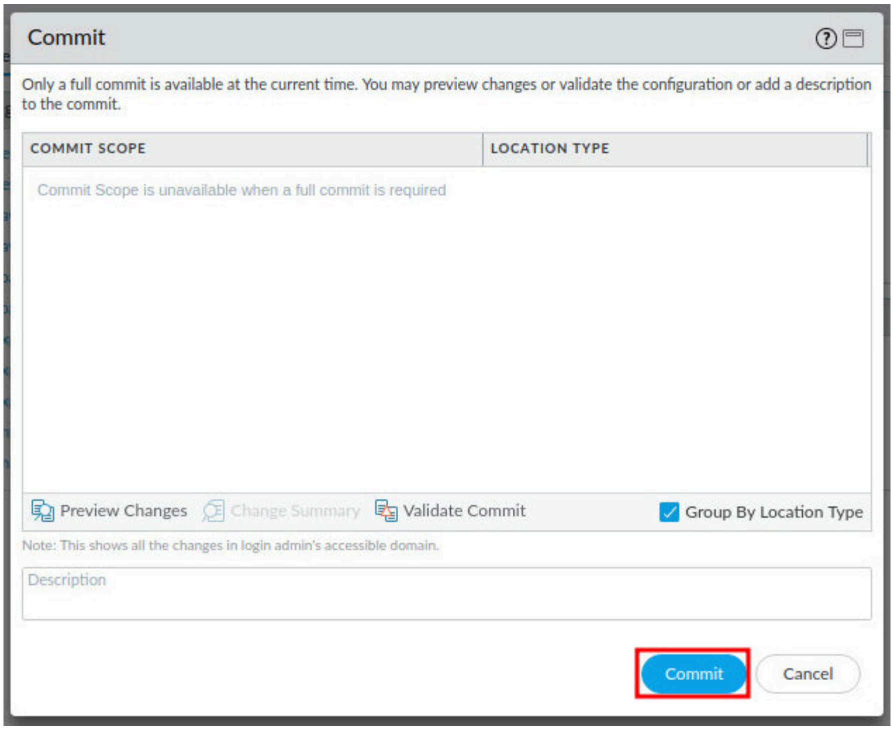
6 items

TYPE	STATUS	START TIME	MESSAGES	ACTION
Load	Completed	08/13/22 22:42:30		
EDLRefresh	Completed	08/13/22 22:40:42		
EDLFetch	Completed	08/13/22 22:40:41		
Report	Completed	08/13/22 22:35:53		
EDLFetch	Completed	08/13/22 22:35:40		
Auto Commit	Completed	08/13/22 22:34:58		

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.



Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

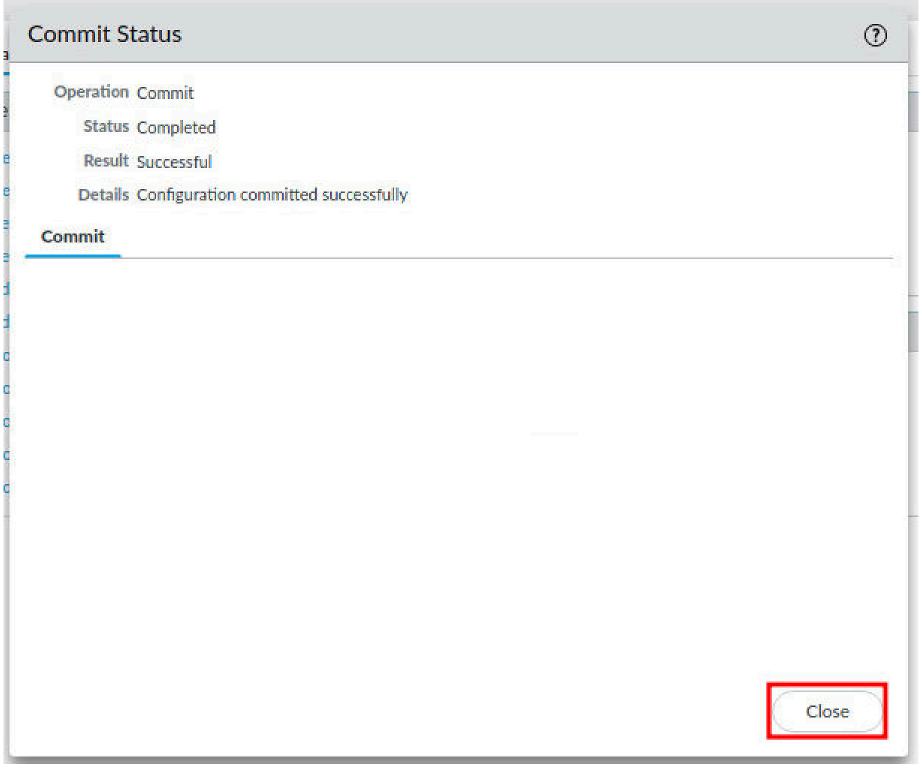
COMMIT SCOPE	LOCATION TYPE
Commit Scope is unavailable when a full commit is required	

Preview Changes | Change Summary | Validate Commit | ☑ Group By Location Type

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

Description

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



Commit Status

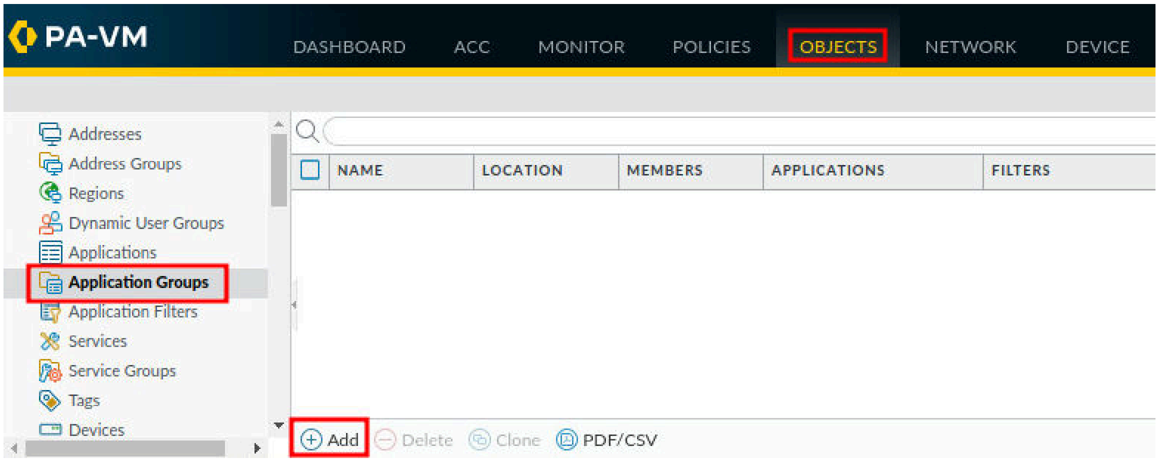
Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

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.

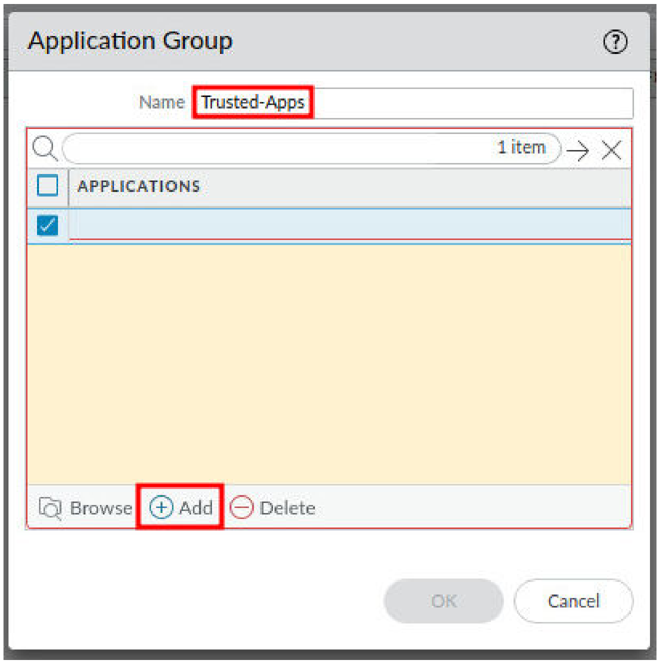
1.1 Create an Application Group

In this section, you will create an application group. To simplify the creation of security policies, applications requiring the same security settings can be combined by creating an application group.

1. Navigate to **Objects > Application Groups > Add.**

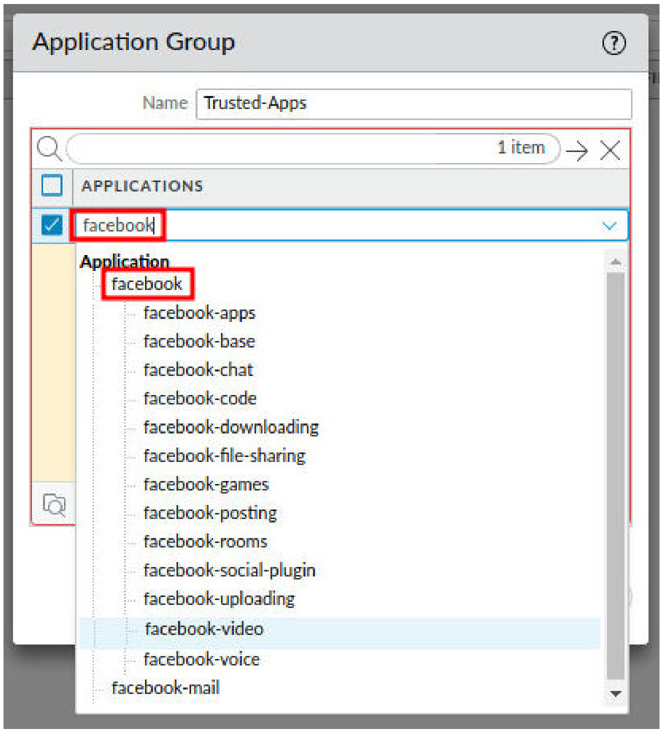


2. In the *Application Group* window, type `Trusted-Apps` in the *Name* field. Then, click the **Add** button.



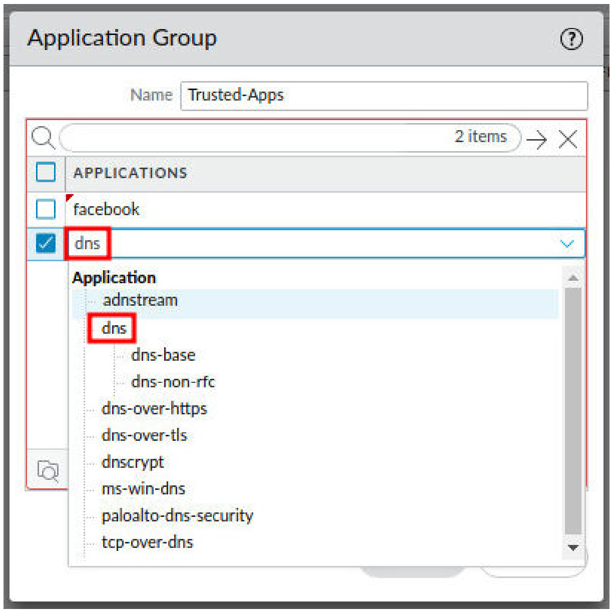
Name: Trusted-Apps

3. In the *Application Group* window, type `facebook` in the search box under the *Applications* column. Then, click on **facebook** under *Application*.

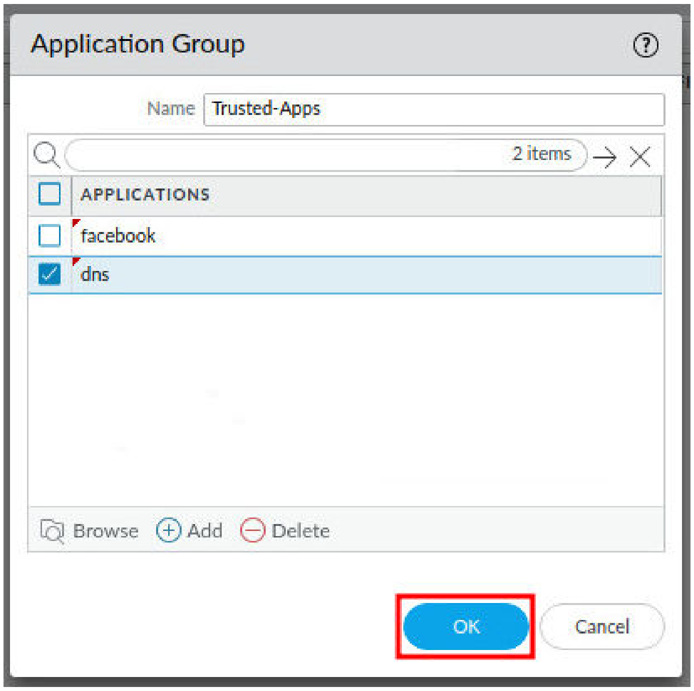


The Palo Alto Networks Firewall has many pre-defined applications. These applications have signatures that allow the Firewall to recognize traffic associated with that application.

4. In the *Application Group* window, click the **Add** button again. Then, type `dns` in the search box under the *Applications* column. Next, click on **dns** under *Application*.



5. In the *Application Group* window, click the **OK** button.



Name: Trusted-Apps

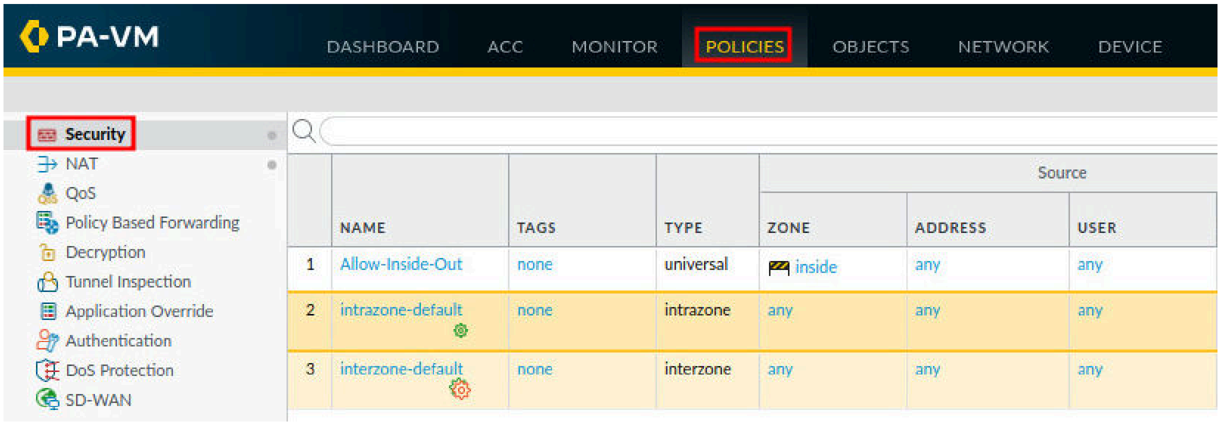
2 items

□	APPLICATIONS
□	facebook
☑	dns

1.2 Modify Security Policy

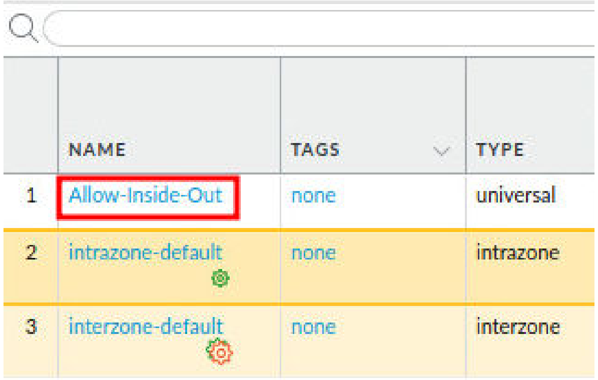
In this section, you will modify the **Allow-Inside-Out** security policy to only allow the applications in the application group, **Trusted-Apps**, you created earlier.

1. Navigate to **Policies > Security**.



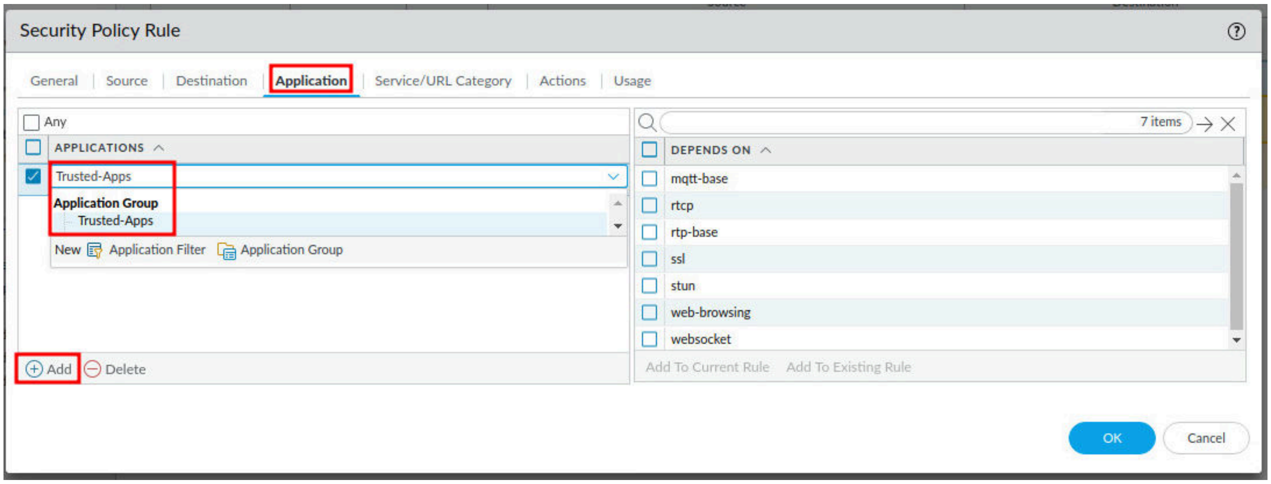
				Source		
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER
1	Allow-Inside-Out	none	universal	inside	any	any
2	intrazone-default	none	intrazone	any	any	any
3	interzone-default	none	interzone	any	any	any

2. Click on the **Allow-Inside-Out** policy.

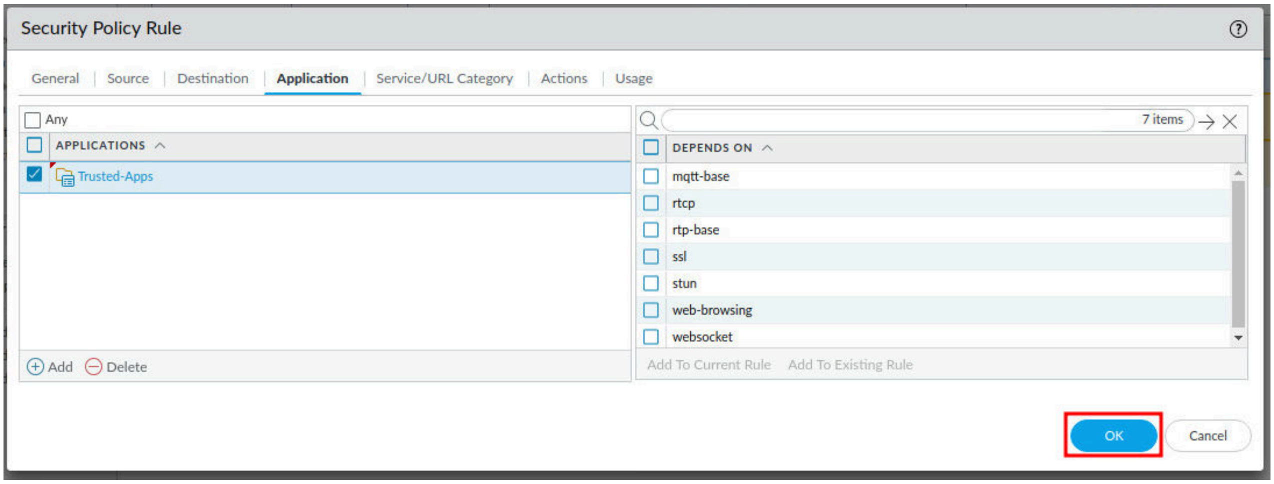


	NAME	TAGS	TYPE
1	Allow-Inside-Out	none	universal
2	intrazone-default	none	intrazone
3	interzone-default	none	interzone

3. In the *Security Policy Rule* window, click on the **Application** tab. Then, click the **Add** button. Next, type `Trusted-Apps` in the search box under the *Applications* column. Finally, select **Trusted-Apps** under *Application Group*.



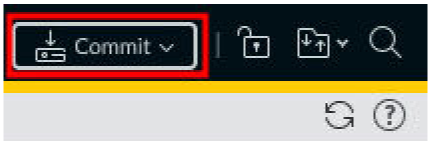
4. In the *Security Policy Rule* window, click the **OK** button.



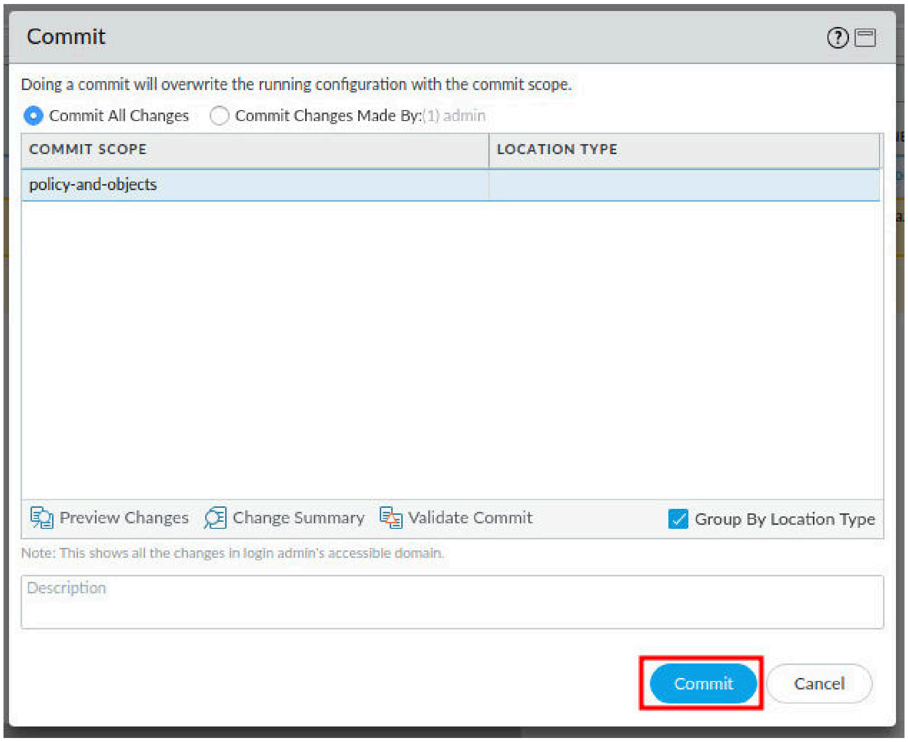
1.3 Commit and Test

In this section, you will commit changes to the Firewall. Then, you will test the security policy you modified earlier. Next, you will add an additional application to the application group, **Trusted-Apps**. Finally, you will verify the additional application is allowed.

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.



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	

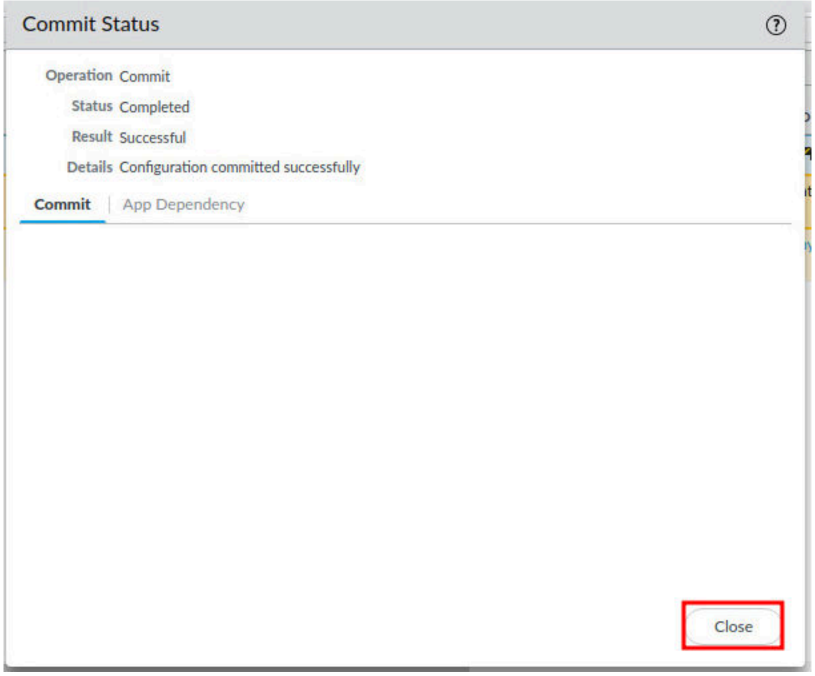
Preview Changes Change Summary Validate Commit ☑ Group By Location Type

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

Description

Commit Cancel

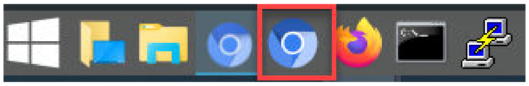
3. When the commit operation successfully completes, click **Close** to continue.



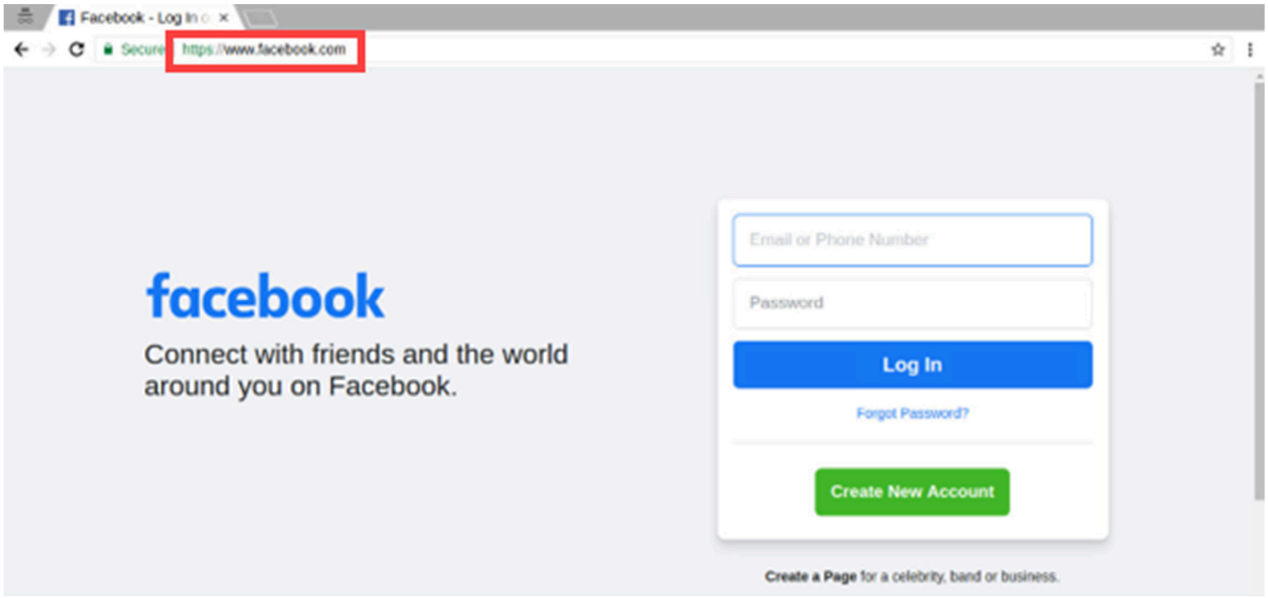
Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

4. Open **Chromium** from the taskbar.

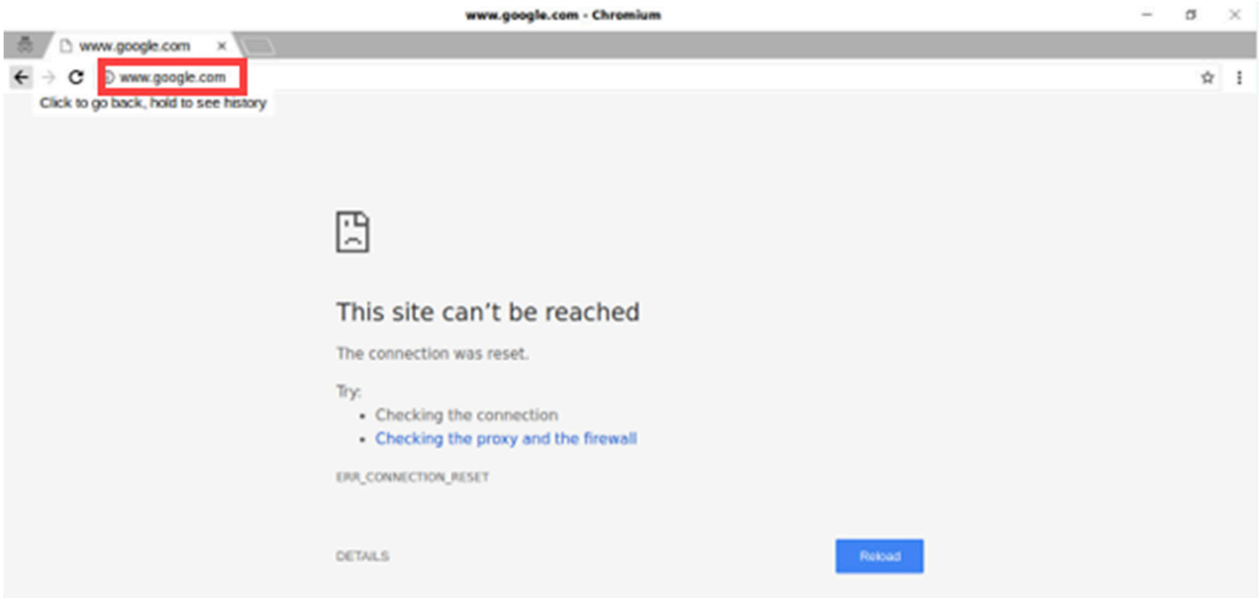


5. In the address bar, type `https://www.facebook.com` and press **Enter**.



> The Firewall recognizes the traffic and matches it to the application, **facebook**. As **facebook** is part of the application group, **Trusted-Apps**, you created earlier, the Firewall allows the traffic based on the security policy you modified.

6. In the address bar, type `http://www.google.com` and press **Enter**.


www.google.com - Chromium
www.google.com
www.google.com
Click to go back, hold to see history
DETAILS
Reload

This site can't be reached

The connection was reset.

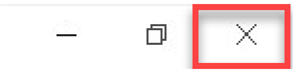
Try:

- Checking the connection
- Checking the proxy and the firewall

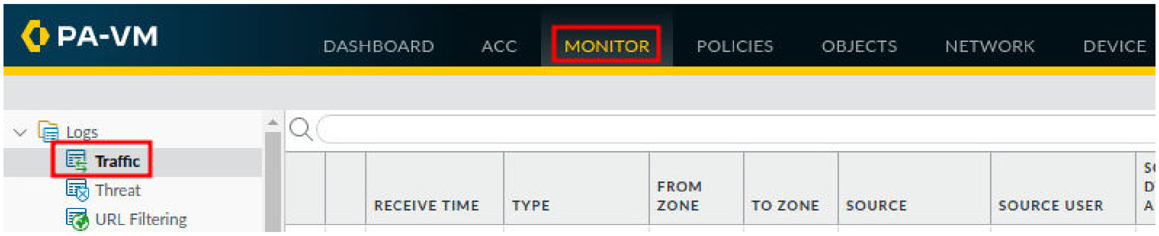
ERR_CONNECTION_RESET

> The Firewall recognizes the traffic and matches it to the application, **google**. As **google** is NOT part of the application group, **Trusted-Apps**, you created earlier, the Firewall blocks the traffic based on the security policy you modified.

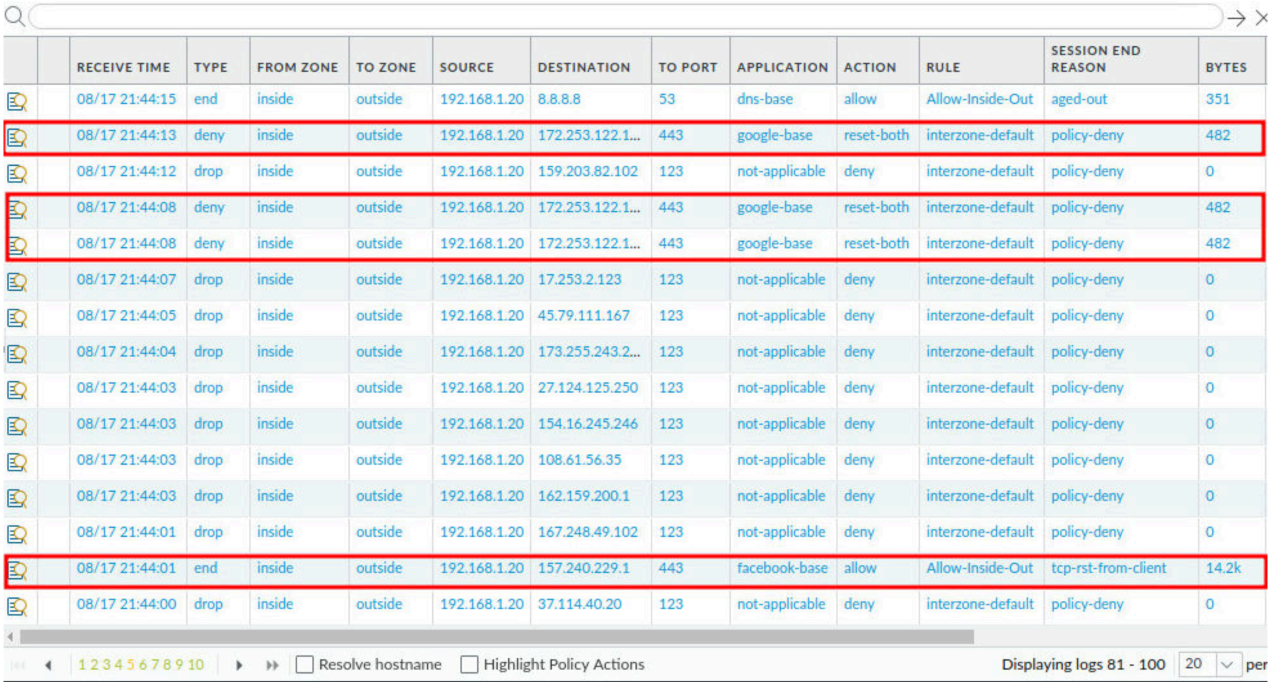
7. Click the **X** in the upper-right to close *Chromium*.



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



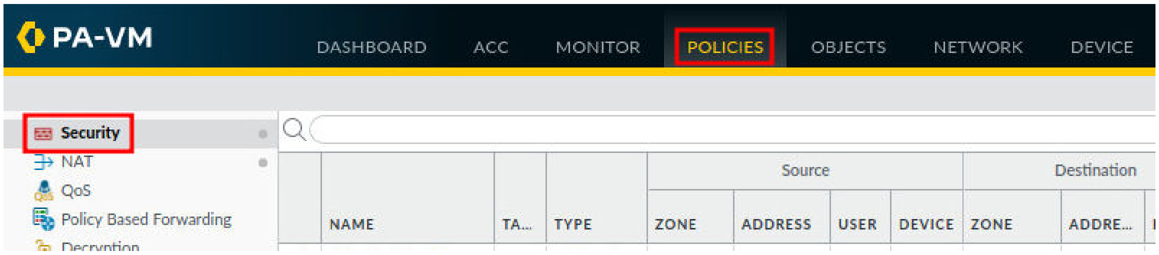
9. Scroll through the traffic logs, notice the application **facebook-base** has the action of **allow** based on rule **Allow-Inside-Out.** Then, notice the application **google-base** has the action **reset-both** based on the rule **interzone-default**, which has a session end reason of **policy-deny**. Next, notice the application **dns** has the action of **allow** based on the rule **Allow-Inside-Out.** You may need to refresh the Traffic logs by clicking refresh in the top-right of the firewall interface.



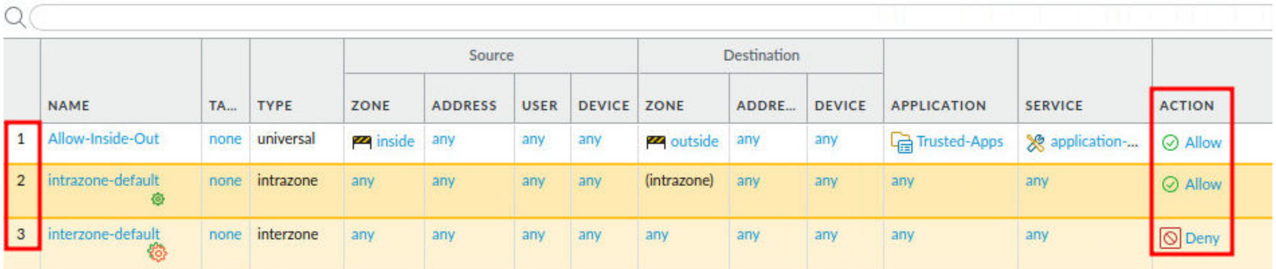
	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
	08/17 21:44:15	end	inside	outside	192.168.1.20	8.8.8.8	53	dns-base	allow	Allow-Inside-Out	aged-out	351
	08/17 21:44:13	deny	inside	outside	192.168.1.20	172.253.122.1...	443	google-base	reset-both	interzone-default	policy-deny	482
	08/17 21:44:12	drop	inside	outside	192.168.1.20	159.203.82.102	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:08	deny	inside	outside	192.168.1.20	172.253.122.1...	443	google-base	reset-both	interzone-default	policy-deny	482
	08/17 21:44:08	deny	inside	outside	192.168.1.20	172.253.122.1...	443	google-base	reset-both	interzone-default	policy-deny	482
	08/17 21:44:07	drop	inside	outside	192.168.1.20	17.253.2.123	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:05	drop	inside	outside	192.168.1.20	45.79.111.167	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:04	drop	inside	outside	192.168.1.20	173.255.243.2...	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:03	drop	inside	outside	192.168.1.20	27.124.125.250	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:03	drop	inside	outside	192.168.1.20	154.16.245.246	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:03	drop	inside	outside	192.168.1.20	108.61.56.35	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:03	drop	inside	outside	192.168.1.20	162.159.200.1	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:01	drop	inside	outside	192.168.1.20	167.248.49.102	123	not-applicable	deny	interzone-default	policy-deny	0
	08/17 21:44:01	end	inside	outside	192.168.1.20	157.240.229.1	443	facebook-base	allow	Allow-Inside-Out	tcp-rst-from-client	14.2k
	08/17 21:44:00	drop	inside	outside	192.168.1.20	37.114.40.20	123	not-applicable	deny	interzone-default	policy-deny	0

Remember, reviewing the traffic logs is an excellent way to troubleshoot and confirm traffic is being matched to the appropriate policy. Because the traffic to **www.google.com** is not part of the **Trusted-Apps** application group, which is applied to the **Allow-Inside-Out** security policy, the Firewall matches that traffic to the next appropriate policy. In this case, the traffic will match to **interzone-default**, which has an explicit deny action.

10. Navigate to **Policies > Security.**

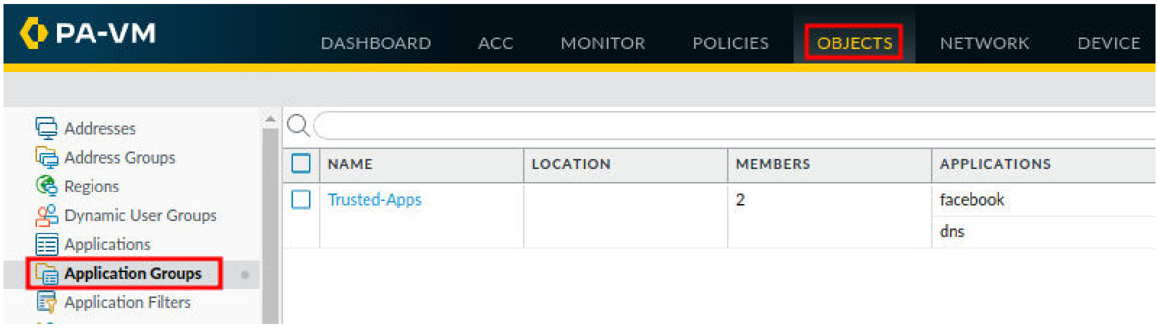


11. Confirm the order of the policies and their action.



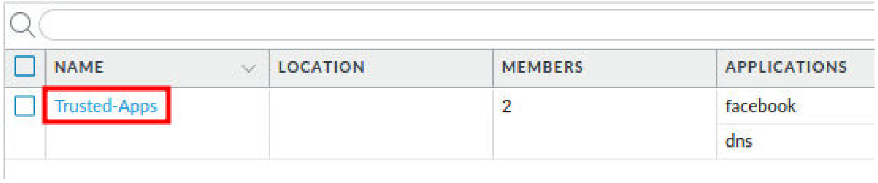
				Source				Destination					
	NAME	TA...	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRE...	DEVICE	APPLICATION	SERVICE	ACTION
1	Allow-Inside-Out	none	universal	inside	any	any	any	outside	any	any	Trusted-Apps	application-...	Allow
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
3	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

12. To add the application, **google-base** application to the *Trusted-Apps* group you created, navigate to **Objects > Application Groups**.



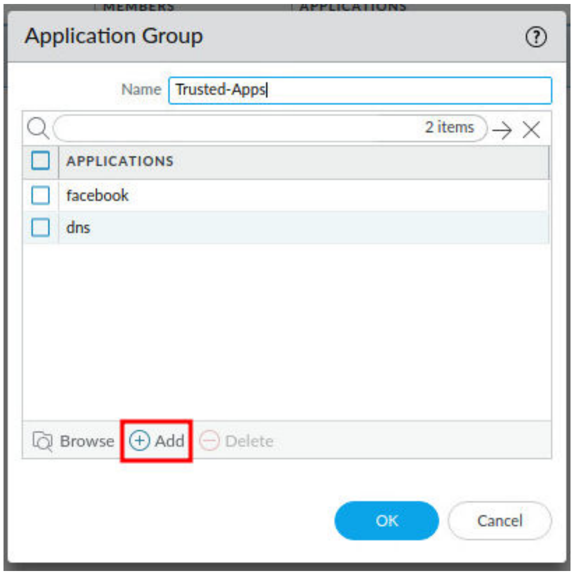
NAME	LOCATION	MEMBERS	APPLICATIONS
Trusted-Apps		2	facebook dns

13. Click on the **Trusted-Apps** Application Group.



NAME	LOCATION	MEMBERS	APPLICATIONS
Trusted-Apps		2	facebook dns

14. In the *Application Group* window, click the **Add** button.



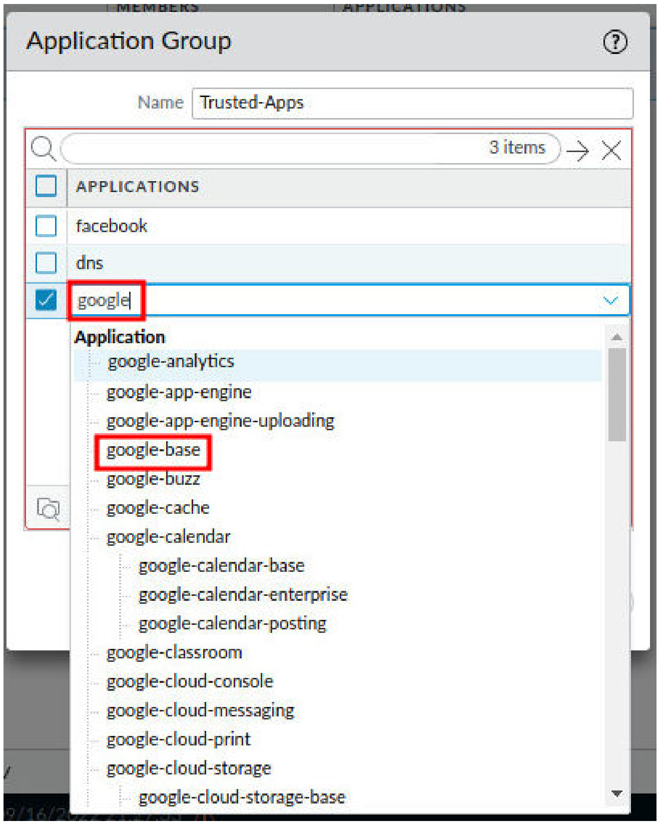
Application Group

Name Trusted-Apps

2 items

APPLICATIONS
facebook
dns

15. In the *Application Group* window, type `google` in the search box under the *Applications* column. Then, click on **google-base** under *Application*.



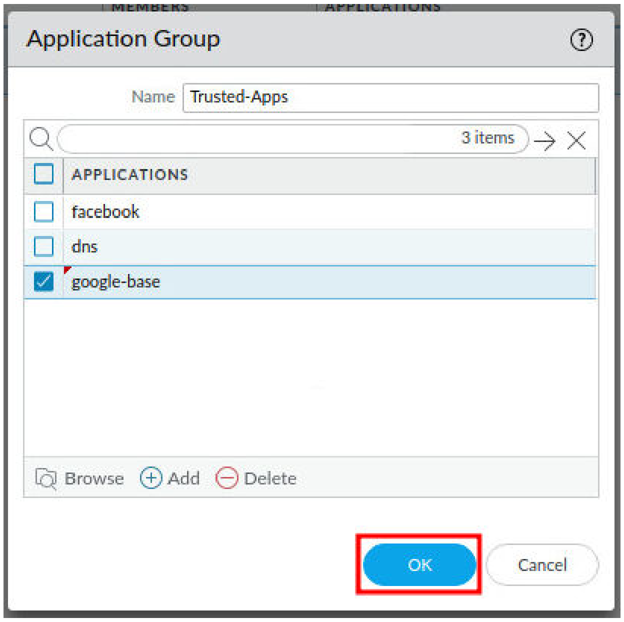
Application Group

Name: Trusted-Apps

3 items

	APPLICATIONS
□	facebook
□	dns
☑	google

16. In the *Application Group* window, click the **OK** button.



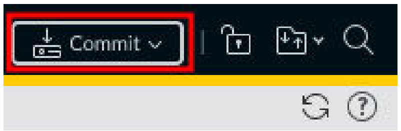
Application Group

Name: Trusted-Apps

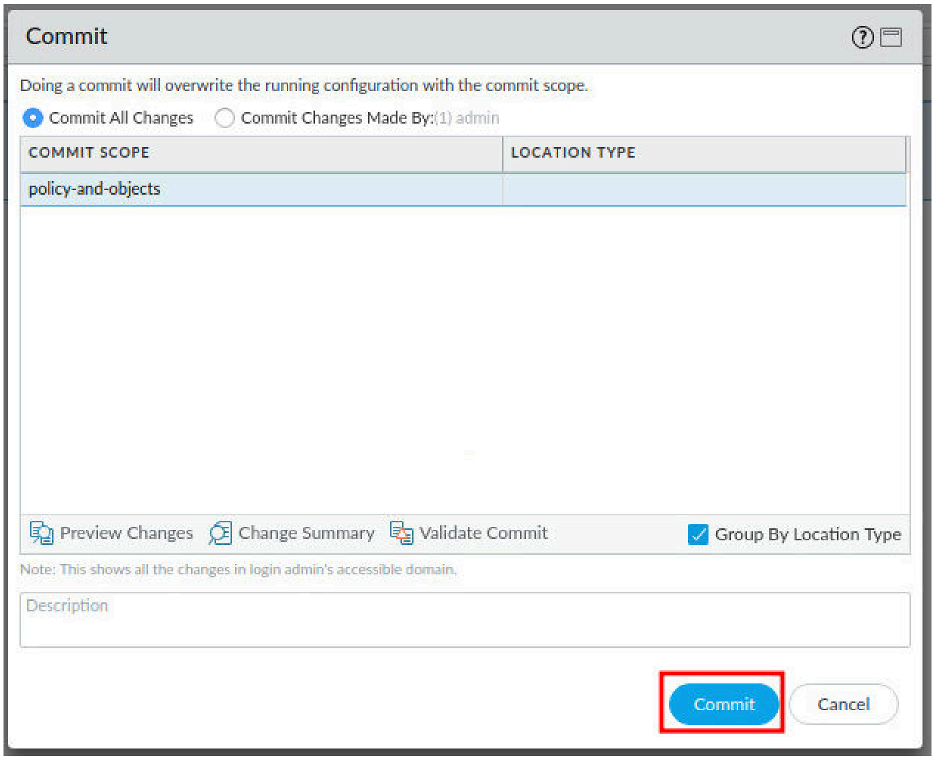
3 items

	APPLICATIONS
□	facebook
□	dns
☑	google-base

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



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



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

● Commit All Changes ○ Commit Changes Made By:(1) admin

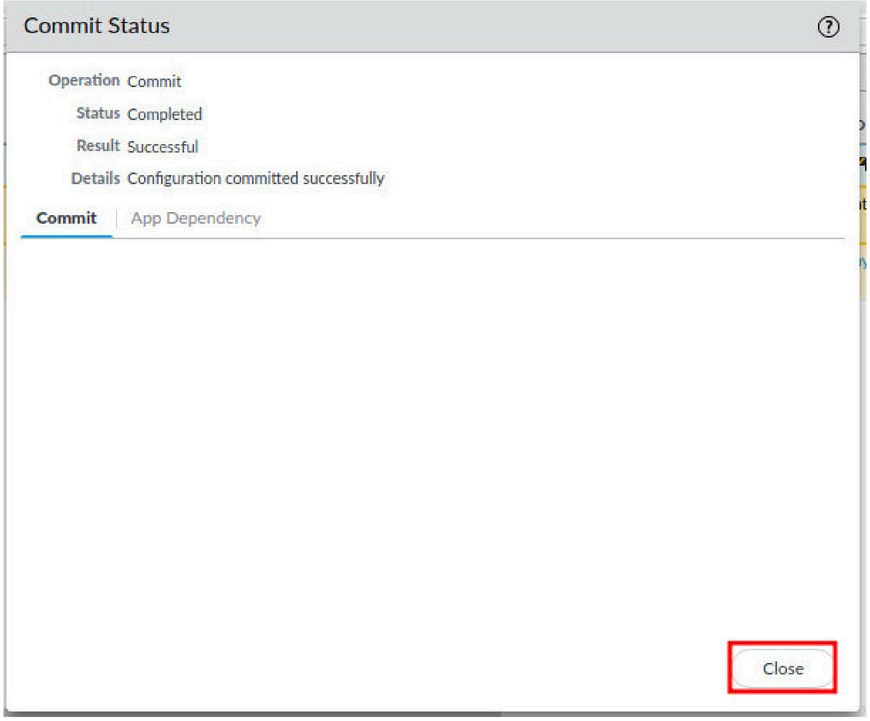
COMMIT SCOPE	LOCATION TYPE
policy-and-objects	

☑ Group By Location Type

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

Description

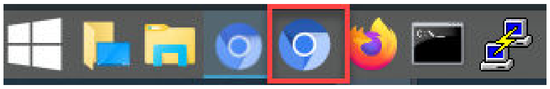
19. When the commit operation successfully completes, click **Close** to continue.



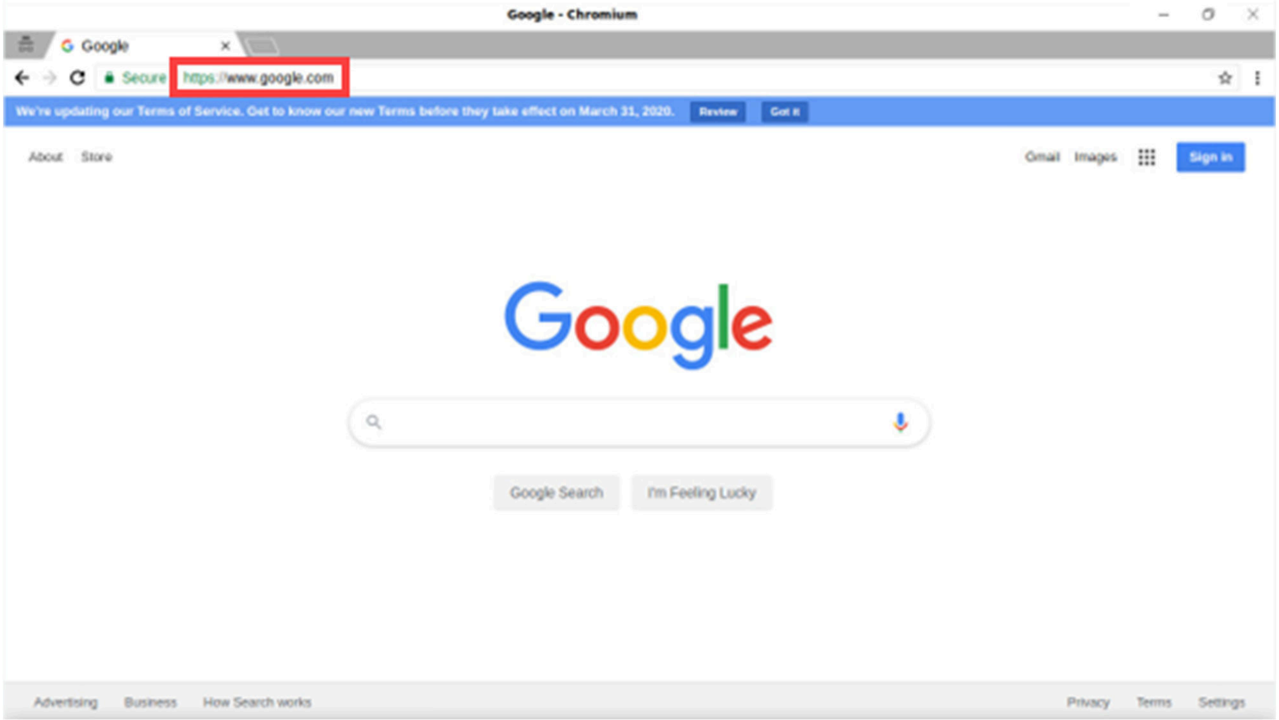
Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

20. Open **Chromium** from the taskbar.



21. In the address bar, type `https://www.google.com` and press **Enter**.



Notice that **https://www.google.com** now works because it was added to the **Trusted-Apps** application group.

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