



PALO ALTO NETWORKS - EDU 210



Lab 1: Initial Configuration

Document Version: 2019-11-12

Copyright © 2019 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
Objectives.....	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
1 Initial Configuration	6
1.0 Connect to Your Student Firewall	6
1.1 Apply a Baseline Configuration to the Firewall.....	6
1.2 Add an Admin Role Profile	8
1.3 Add an Administrator Account.....	10
1.4 Test the policy-admin User	11
1.5 Take a Commit Lock and Test the Lock	14
1.6 Verify the Update and DNS Servers	17
1.7 Schedule Dynamic Updates.....	19

Introduction

The long-awaited moment has arrived. Your new Palo Alto Networks Firewall appliance has been delivered, and the networking team has put it in the racks and wired it up. It is now your job as the Security Engineer to configure and test the firewall.

You have decided that the first thing you would like to do is create a new admin account that can only work with certain features of the firewall. To set up these restrictions, you are going to create an administrator role and then assign it to the new admin account you create.

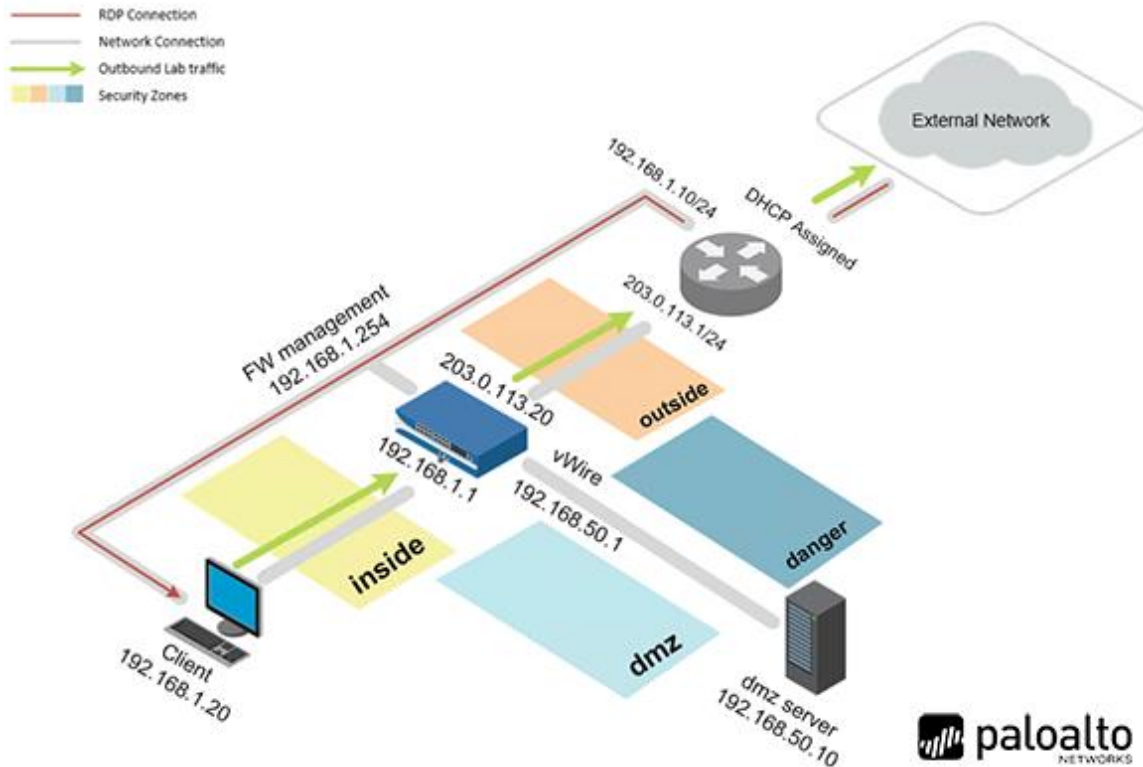
You also want to test the ability to prevent others from making or committing changes to the firewall while you are working. You have learned that this can be done with commit locks.

Finally, you need to make sure the firewall is updating with new signatures and updates on a regular basis, so you are going to configure the dynamic updates to do this for you.

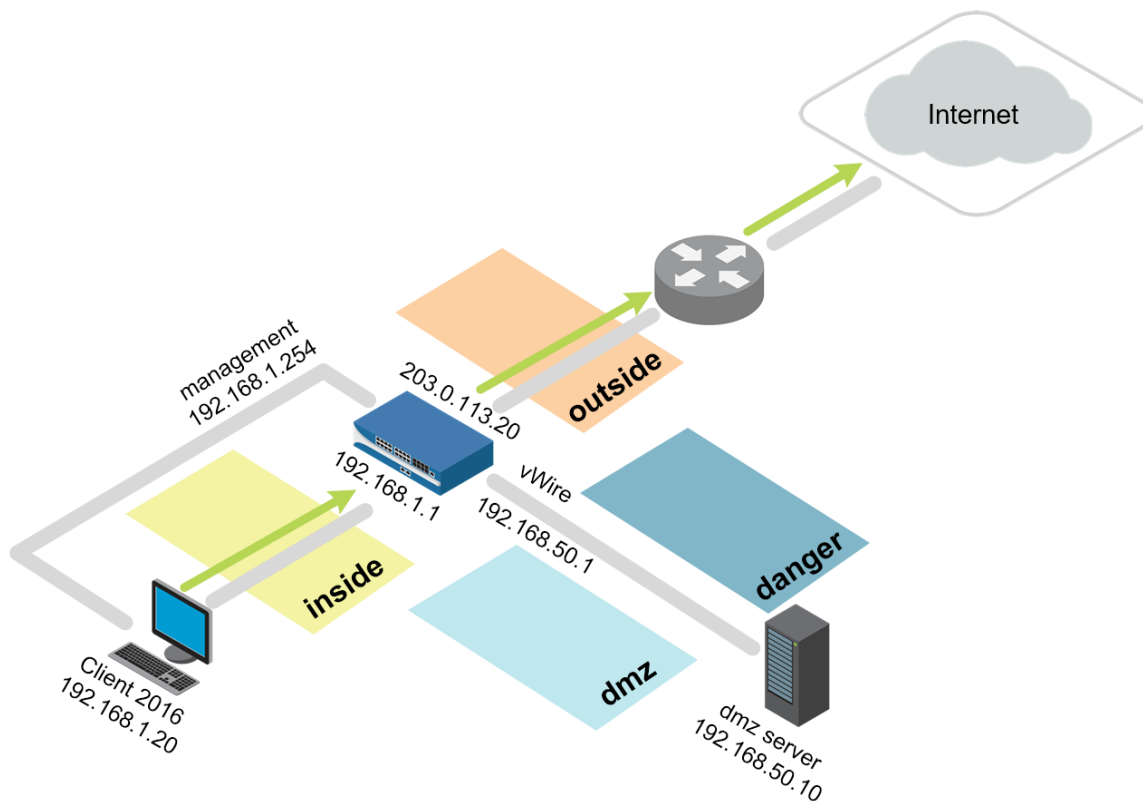
Objectives

- Load a configuration
- Create an administrator role
- Create a new administrator and apply an administrator role
- Observe the newly created role permissions via the CLI and web interface
- Create and test a commit lock
- Configure DNS servers for the firewall
- Schedule dynamic updates

Lab Topology



Theoretical 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	Pa10A1t0
Firewall	192.168.1.254	admin	admin

1 Initial Configuration

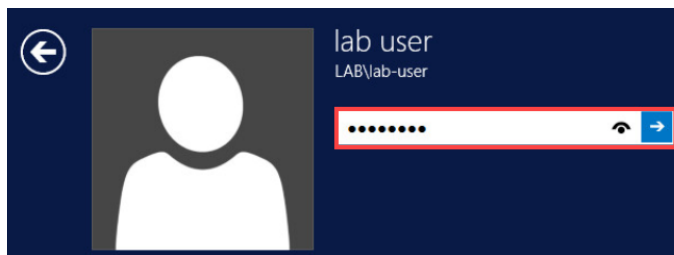
1.0 Connect to Your Student Firewall

1. Launch the **Client** virtual machine to access the graphical login screen.



To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

2. Click within the splash screen to bring up the login screen. Log in as **lab-user** using the password **Pa10A1t0**.



3. Launch the **Chrome** browser and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	admin

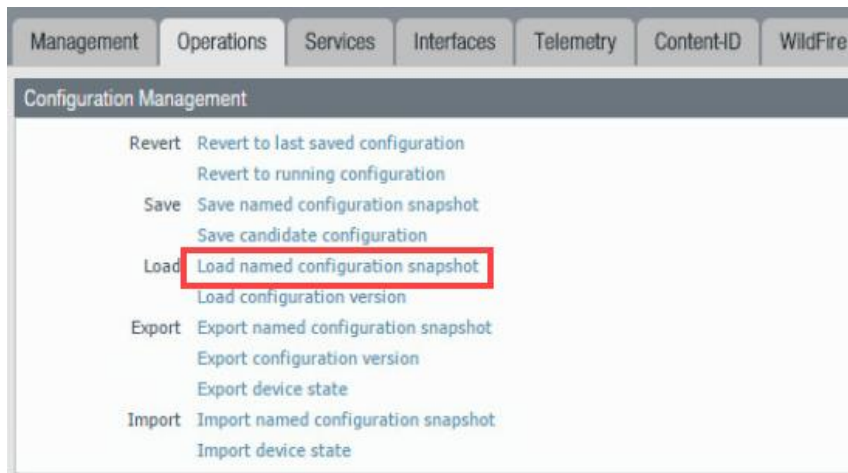
6. Leave the firewall web interface open to continue with the next task.

1.1 Apply a Baseline Configuration to the Firewall

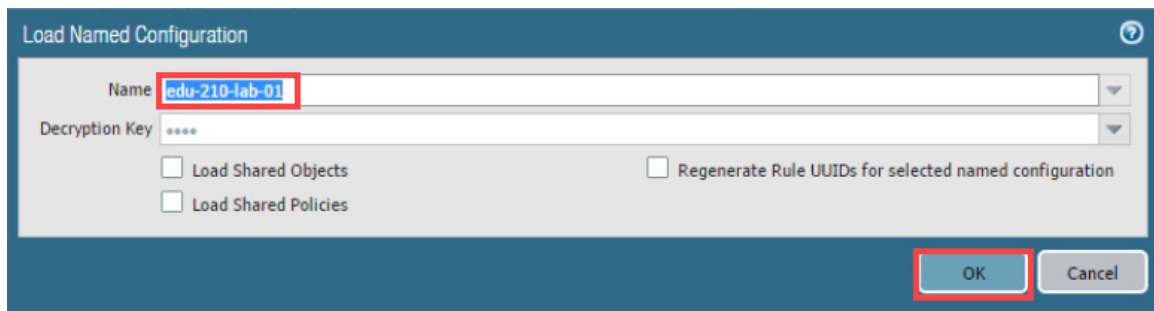
1. In the *Palo Alto Networks* firewall web interface, select **Device > Setup > Operations**.



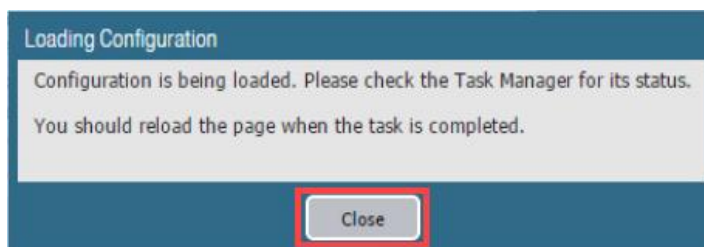
2. Click **Load named configuration snapshot**:



3. Click the drop-down list next to the *Name* text box and select **edu-210-lab-01**. Click **OK**.



4. Click **Close**.

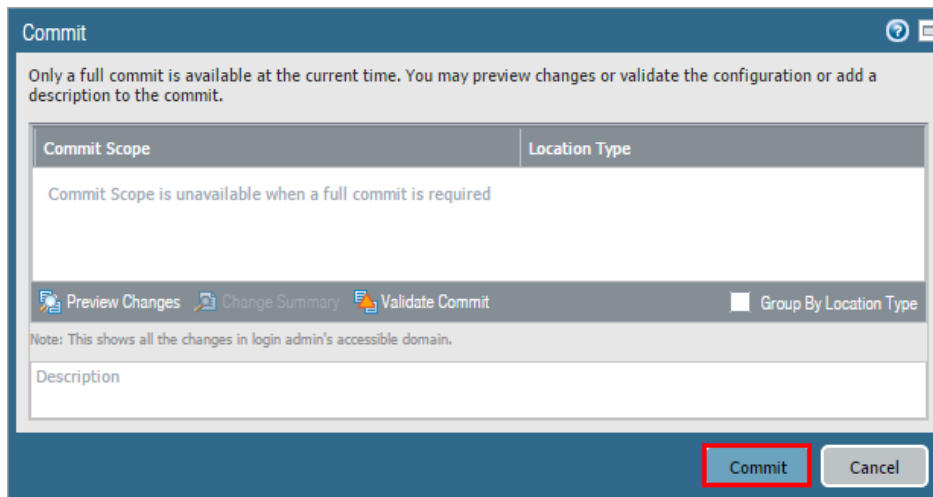


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

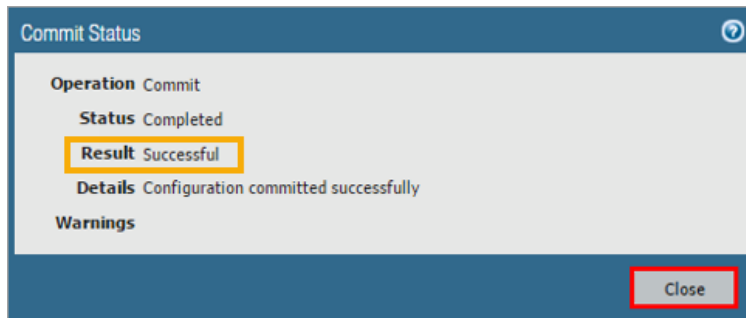
5. Click the **Commit** link at the top-right of the web interface.



- Click **Commit** and wait until the commit process is complete.



- Once completed successfully, click **Close** to continue.



- Leave the firewall web interface open to continue with the next task.

1.2 Add an Admin Role Profile

- In the *Palo Alto Networks* firewall web interface, select **Device > Admin Roles**.





- Click **Add** in the lower-left corner of the panel to create a new administrator role:








3. In the *Admin Role Profile* wizard, enter the following:

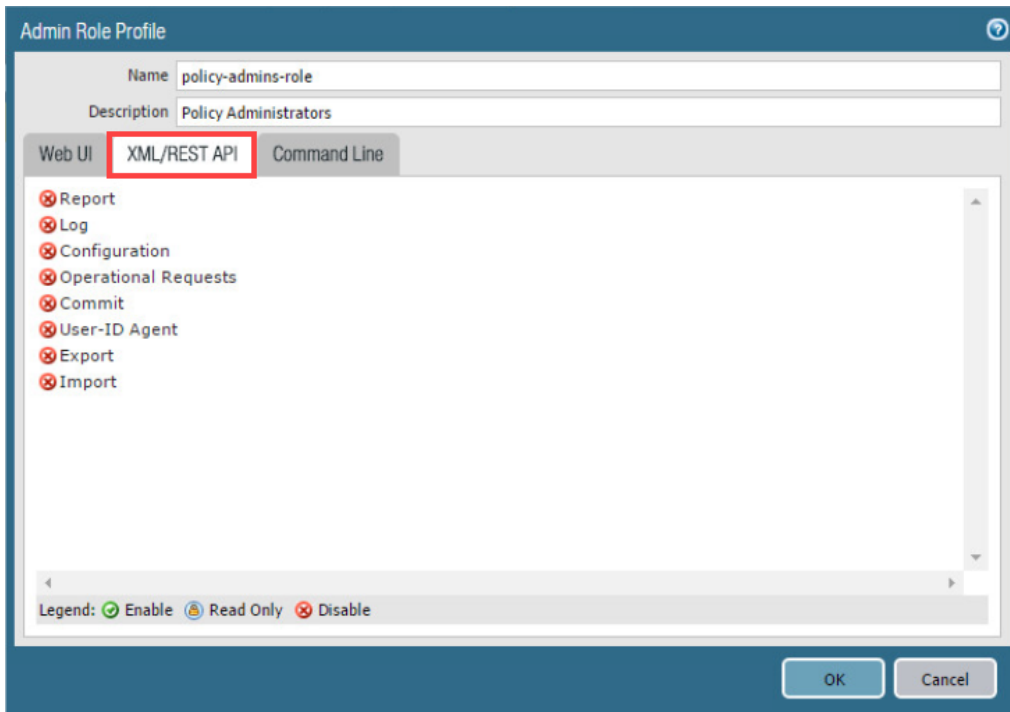
Parameter	Value
Name	policy-admins-role
Description	Policy Administrators




4. Under the *Web UI* tab, click the  icon to disable the following:

Parameter	Value
Monitor	
Network	
Device	
Privacy	

5. Click the **XML/REST API** tab and verify that all items are  disabled.



- Click the **Command Line** tab and verify that the selection is **None**, then click **OK** to continue.



The screenshot shows the 'Admin Role Profile' configuration window. The 'Name' field is 'policy-admins-role' and the 'Description' is 'Policy Administrators'. The 'Command Line' tab is selected and highlighted with a red box. Below the tabs, a dropdown menu is set to 'None' and is also highlighted with a red box. At the bottom right, the 'OK' button is highlighted with a red box.

- Verify that the new role appears in the list.

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	auditadmin	Audit Administrator for Common Criteria
<input type="checkbox"/>	cryptoadmin	Crypto Administrator for Common Criteria
<input type="checkbox"/>	securityadmin	Security Admin for Common Criteria
<input type="checkbox"/>	policy-admins-role	Policy Administrators

- Leave the firewall web interface open to continue with the next task.

1.3 Add an Administrator Account

- In the *Palo Alto Networks* firewall web interface, select **Device > Administrators**.



- Click **Add** in the lower-left corner of the panel to open the *Administrator* configuration window.



- Configure the following and then click **OK**.

Parameter	Value
Name	policy-admin
Authentication Profile	None
Password	paloalto
Administrator Type	Role Based
Profile	policy-admins-role
Password Profile	None



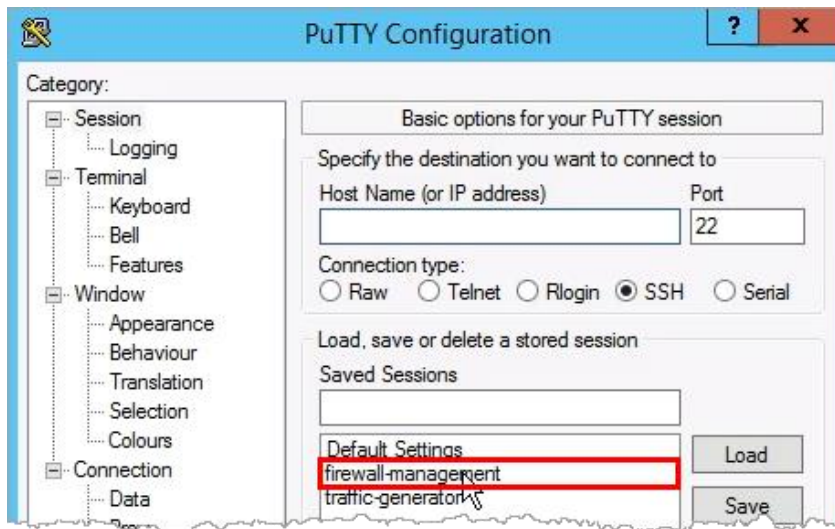
- Click the **Commit** link at the upper-right corner of the web interface.
- Click **Commit**.
- Once completed, click **Close**.

1.4 Test the policy-admin User

- Double click the **PuTTY** icon from the Windows desktop.



- Double-click **firewall-management** from the *Save Sessions* pane.



- Log in using the following information:

Parameter	Value
Name	admin
Password	admin



The role assigned to this account is allowed CLI access, so the connection should succeed.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Mon Jul 10 11:00:21 2017 from 192.168.1.20

Number of failed attempts since last successful login: 0

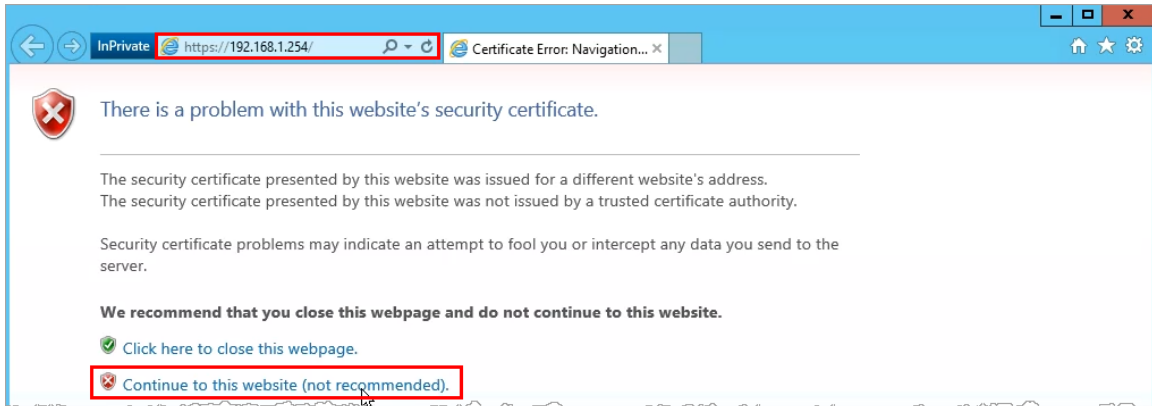
admin@lab-firewall> █
```

- Close the **PuTTY** window. When prompted, click **OK** to continue.
- Open **PuTTY** again.
- Open an SSH connection to **firewall-management**.
- Log in using the following information (*the window will close if authentication is successful*):

Parameter	Value
Name	policy-admin
Password	paltoalto

```
login as: policy-admin
Using keyboard-interactive authentication.
Password: █
```

8. Open the **Internet Explorer** browser in **private/incognito mode** and browse to **https://192.168.1.254**. A *Certificate Warning* might appear.
9. Click through the *Certificate Warning*. The *Palo Alto Networks* firewall login page opens.



10. Log in using the following information (this action must be done in a different browser):

Parameter	Value
Name	policy-admin
Password	paloalto



11. **Close** the *Welcome* window if one is presented.
12. Explore the available functionality of the web interface. Notice that several tabs and functions are excluded from the interface because of the modified *Admin Role* assigned to this user account.
13. Leave the firewall web interface open to continue with the next task.

1.5 Take a Commit Lock and Test the Lock

The web interface supports multiple concurrent administrator sessions by enabling an administrator to lock the candidate or running configuration so that other administrators cannot change the configuration until the lock is removed.

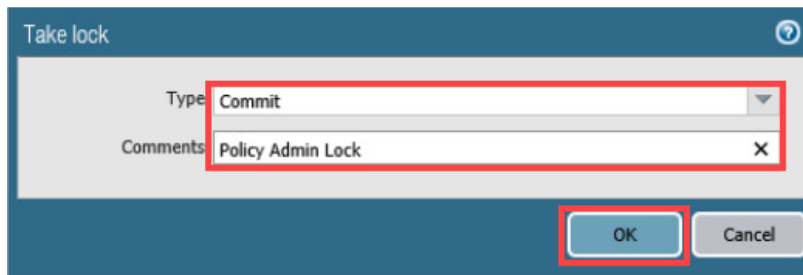
1. From the web interface where you are logged in as *policy-admin*, click the **transaction lock** icon to the right of the *Commit* link.



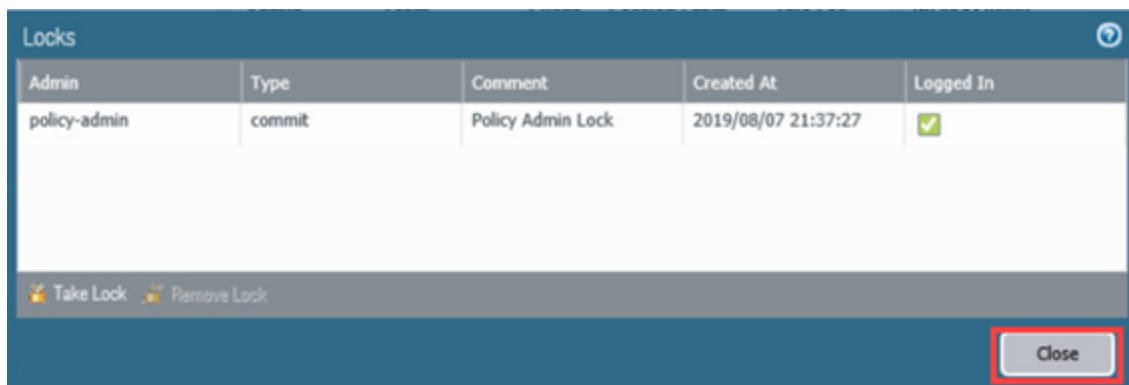
2. Notice that the *Locks* window opens. Click **Take Lock**.



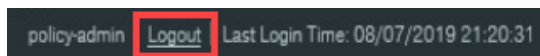
3. A *Take lock* window opens. Set the *Type* to **Commit** and type **Policy Admin Lock** in the *Comments* text field. Click **OK**. The policy-admin lock is listed in the *Locks* window.



4. Click **Close** to close the *Locks* window.



5. Click the **Logout** button on the bottom-left corner of the web interface:

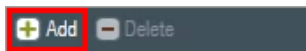


6. Close the *policy-admin* browser window.

7. Return to the *Chrome* browser in the web interface where you are logged in as *admin*.
8. Click the **Device > Administrators** link. The web interface refreshes. Notice the lock icon in the upper-right corner of the web interface.

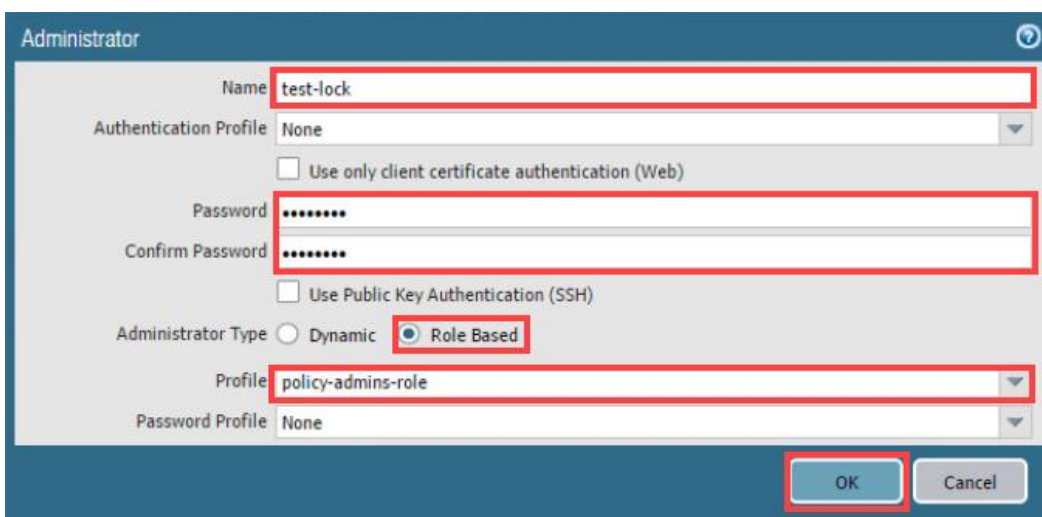


9. Click **Add** to add another administrator account.



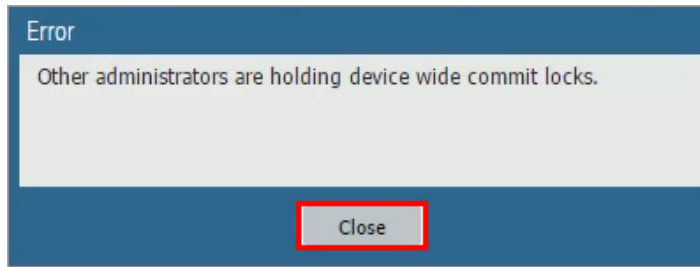
10. Configure the following:

Parameter	Value
Name	test-lock
Authentication Profile	None
Password	paloalto
Administrator Type	Role Based
Profile	policy-admins-role
Password Profile	None



11. Click **OK**. Notice the new *test-lock* user is listed.

12. **Commit** all changes. Although you could add a new administrator account, you are not allowed to commit the changes because of the *Commit lock* set by the *policy-admin* user:

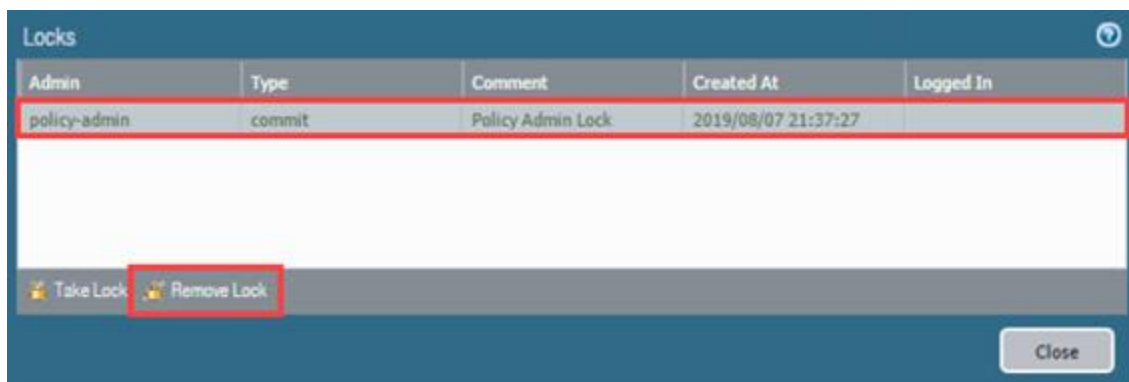


13. Click **Close**.

14. Click the **transaction lock** icon in the upper-right corner:

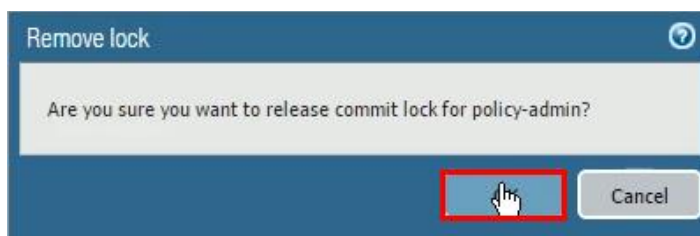


15. Select the **policy-admin** lock and click **Remove Lock**:



A lock may be removed by the user that took the lock or by any superuser.

16. Click **OK**, and the lock is removed from the list.



17. Back on the *Locks* window, click **Close**.

18. **Commit** all changes. Notice you can now commit the changes.

19. Select the test-lock user and then click **Delete** to delete the test-lock user.

<input type="checkbox"/>	Name	Role	Authentication Profile	Password Profile	Client Certificate Authentication (Web)	Public Key Authentication (SSH)	Profile	Locked User
<input type="checkbox"/>	admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	policy-admin	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	policy-admins-role	
<input checked="" type="checkbox"/>	test-lock	Custom role-based administrator			<input type="checkbox"/>	<input type="checkbox"/>	policy-admins-role	

20. Click **Yes** to confirm the deletion.

21. **Commit** all changes.

22. Leave the firewall web interface open to continue with the next task.

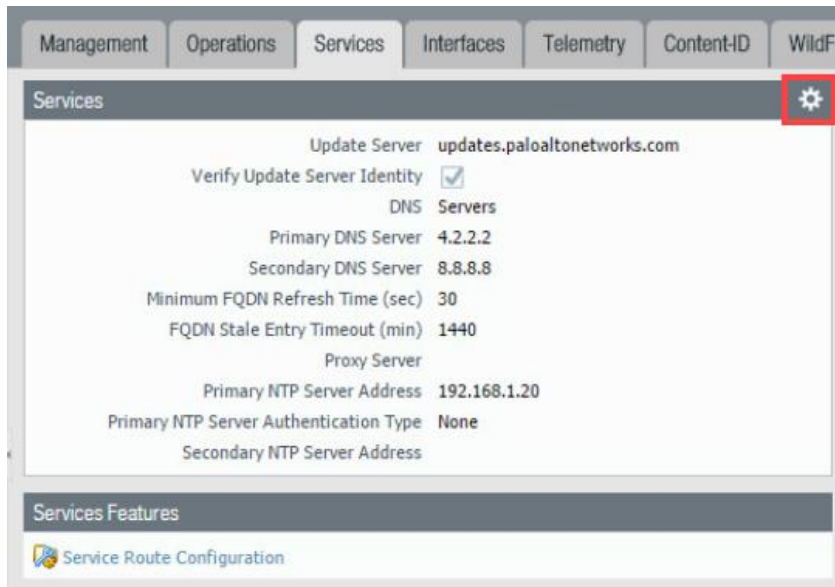
1.6 Verify the Update and DNS Servers

The DNS server configuration settings are used for all DNS queries that the firewall initiates in support of FQDN address objects, logging, and firewall management.

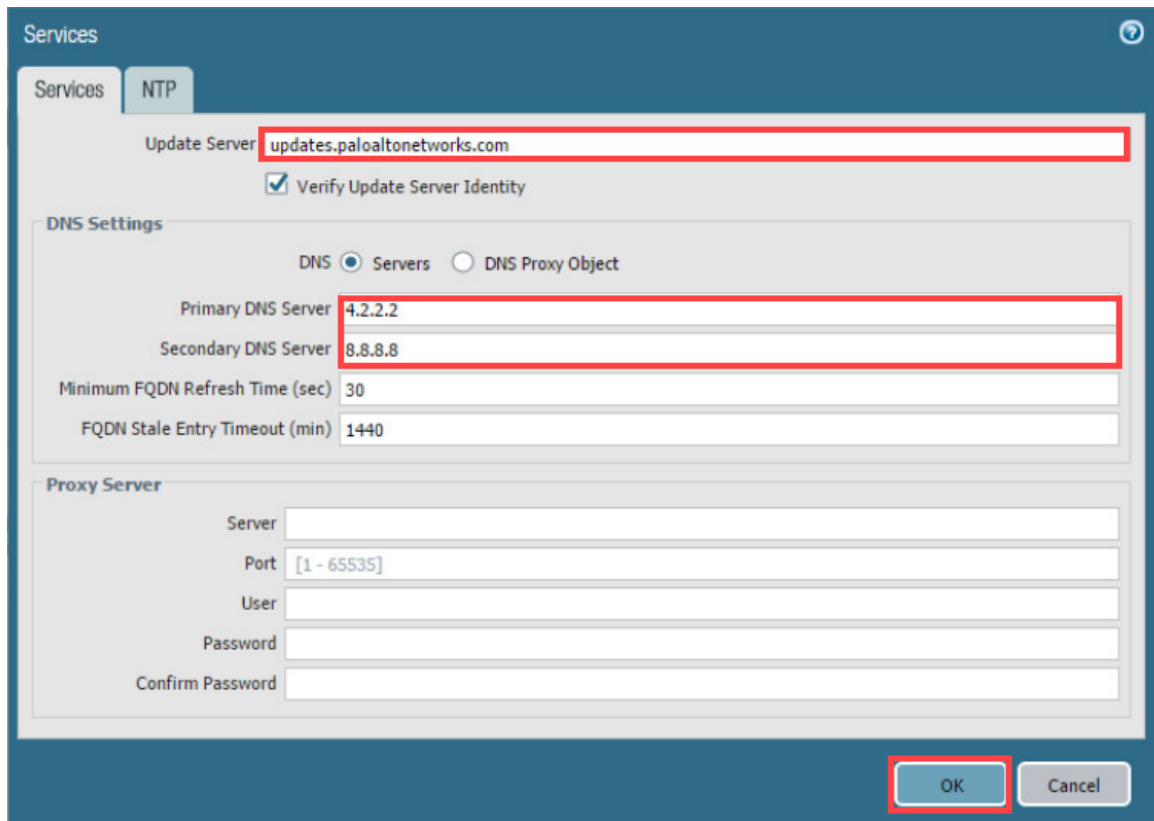
1. In the web interface, navigate to **Device > Setup > Services**.



- Open the *Services* window by clicking the **gear icon** in the upper-right corner of the *Services* panel.



- Verify that **4.2.2.2** is the *Primary DNS Server* and that **8.8.8.8** is the *Secondary DNS Server*. Verify that **updates.paloaltonetworks.com** is the *Update Server*. Click **OK**.

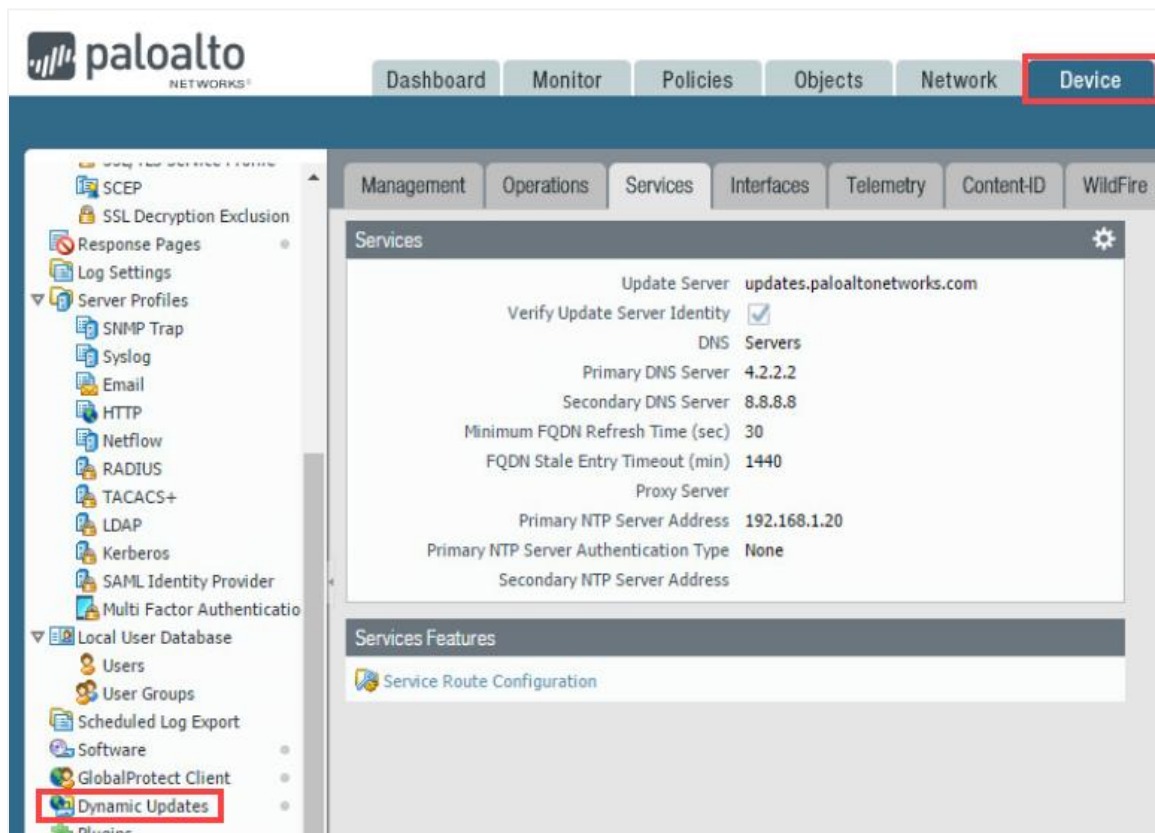


- Leave the firewall web interface open to continue with the next task.

1.7 Schedule Dynamic Updates

Palo Alto Networks regularly posts updates for new and modified application detection, threat protection, and *GlobalProtect* data files through dynamic updates. Even though these definitions are published at predefined intervals (daily or weekly), *Palo Alto Networks* often releases emergency updates to address newly discovered threats. These definitions should be downloaded and applied to the firewall as soon as possible. If you set schedules, you can automate this process so that the firewall has the latest protection definitions.

1. In the web interface, select **Device > Dynamic Updates**.

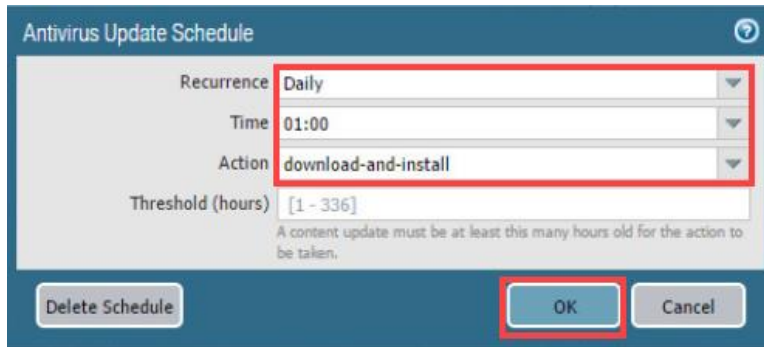


2. Locate and click the **Schedule** hyperlink on the far right of *Antivirus*.

Version ▲	File Name	Features	Type
▼ Antivirus	Last checked: 2019/08/06 18:54:27 UTC	Schedule:	None

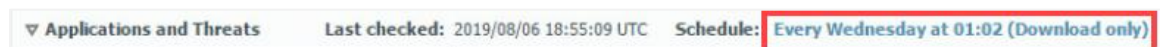
3. The scheduling window opens. Antivirus signatures are released daily. Configure the following and then click **OK**.

Parameter	Value
Recurrence	Daily
Time	01:00
Action	download-and-install



The screenshot shows the 'Antivirus Update Schedule' dialog box. The 'Recurrence' dropdown is set to 'Daily', 'Time' is '01:00', and 'Action' is 'download-and-install'. The 'Threshold (hours)' is set to '[1 - 336]'. A note below the threshold states: 'A content update must be at least this many hours old for the action to be taken.' The 'OK' button is highlighted with a red box.

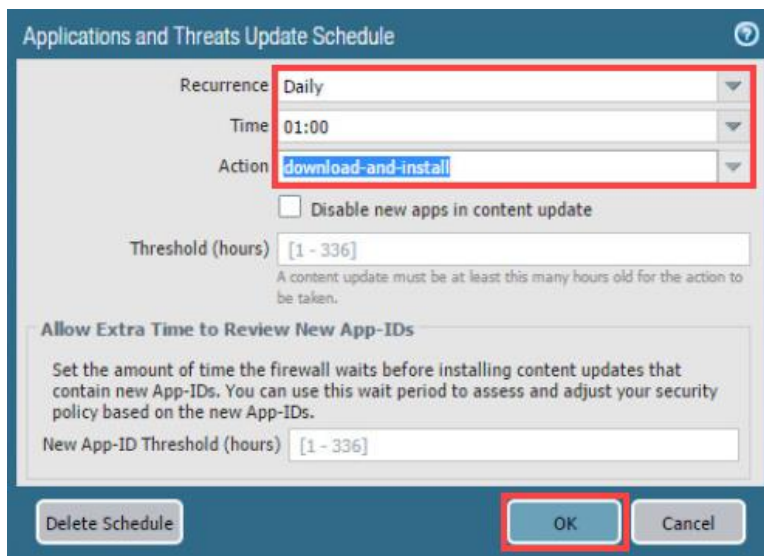
4. Locate and click the **Schedule** hyperlink on the far right of *Application and Threats*.



The screenshot shows the 'Applications and Threats' status bar. The 'Schedule' field is highlighted with a red box and contains the text 'Every Wednesday at 01:02 (Download only)'.

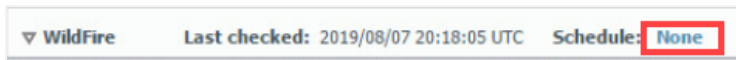
5. The scheduling window opens. *Application and Threat* signatures are released weekly. Configure the following and then click **OK**.

Parameter	Value
Recurrence	Daily
Time	01:00
Action	download-and-install



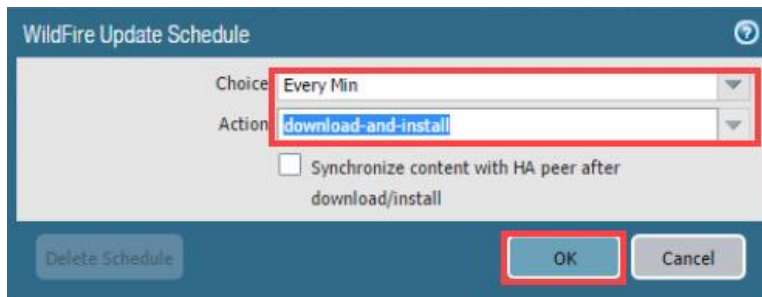
The screenshot shows the 'Applications and Threats Update Schedule' dialog box. The 'Recurrence' dropdown is set to 'Daily', 'Time' is '01:00', and 'Action' is 'download-and-install'. The 'Threshold (hours)' is set to '[1 - 336]'. A note below the threshold states: 'A content update must be at least this many hours old for the action to be taken.' There is a checkbox for 'Disable new apps in content update' which is unchecked. Below this is a section titled 'Allow Extra Time to Review New App-IDs' with a description: 'Set the amount of time the firewall waits before installing content updates that contain new App-IDs. You can use this wait period to assess and adjust your security policy based on the new App-IDs.' The 'New App-ID Threshold (hours)' is set to '[1 - 336]'. The 'OK' button is highlighted with a red box.

6. Scroll down to locate and click the **Schedule** hyperlink on the far right of *WildFire*.



7. The scheduling window opens. *WildFire* signatures can be available within five minutes. Configure the following and then click **OK**.

Parameter	Value
Recurrence	Every Minute
Action	download-and-install



8. **Commit** all changes.
9. The lab is now complete; you may end the reservation.