



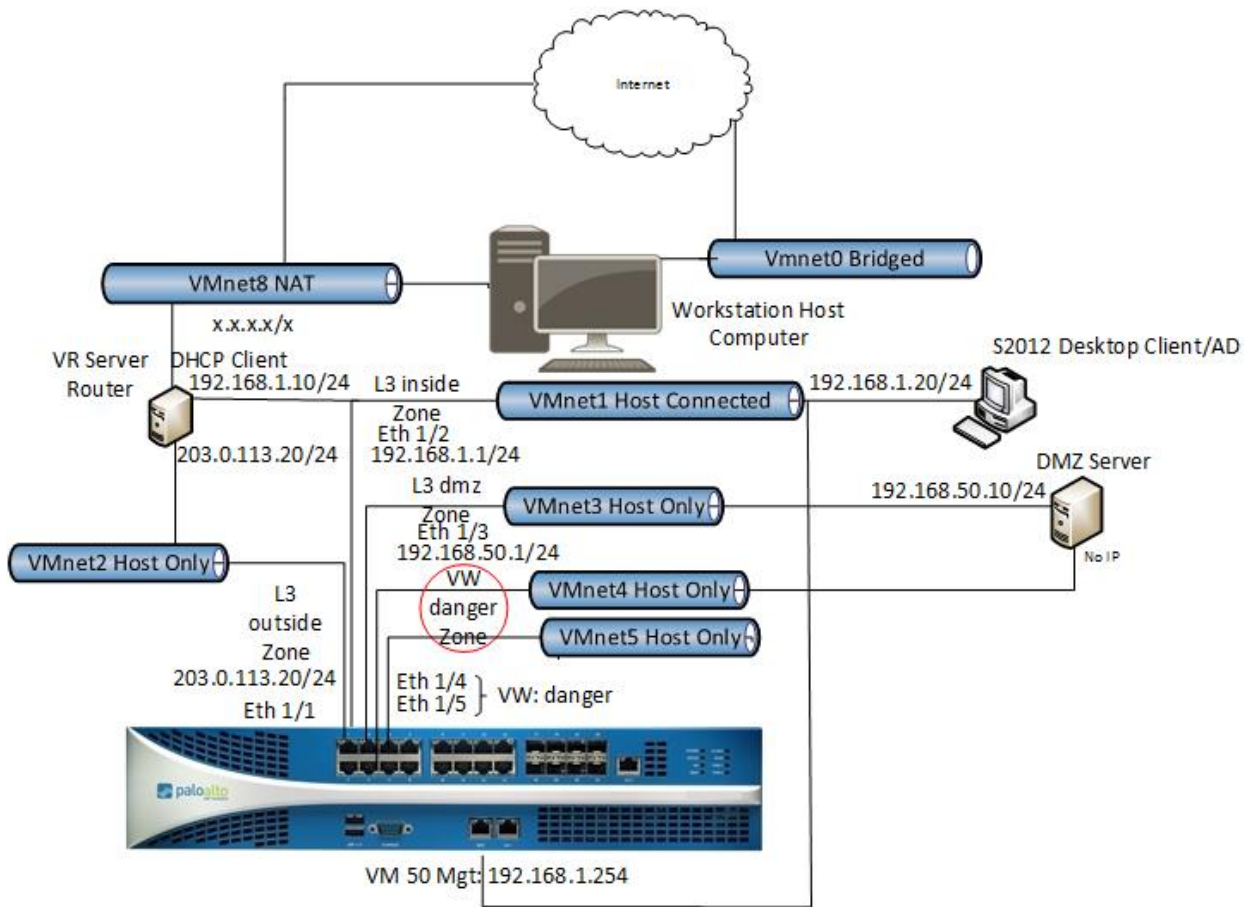
Palo Alto Networks Academy Labs Lab 1 Initial Configuration

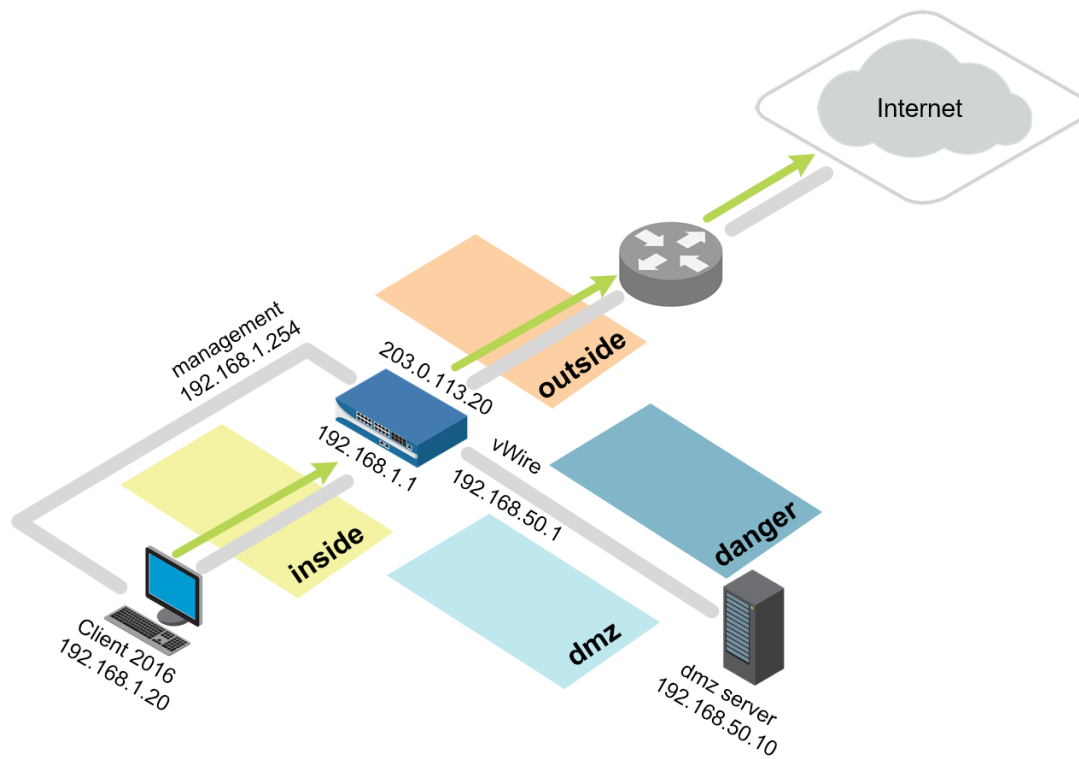
Document Version: 2018-11-10

Copyright © 2018 Palo Alto Networks, Inc.

www.paloaltonetworks.com

Lab Topology





Virtual Machine	Username	Password
Firewall	admin	admin
Server 2012	lab-user	Pa10Alt0
Centos AAC DMZ	root	Pa10Alt0
Centos Virtual Router	root	Pa10Alt0

Lab 1: Initial Configuration

Lab Objectives:

Your assignment is to integrate a new firewall into your environment.

- **Log into your firewall and load configuration snapshot**
- **Create an administrator role.**
- **Create a new administrator and apply an administrator role.**
- **Observe the newly created role permissions via the CLI and Web User Interface.**
- **Create and test a commit lock.**
- **Configure DNS servers for the firewall.**
- **Schedule dynamic updates.**

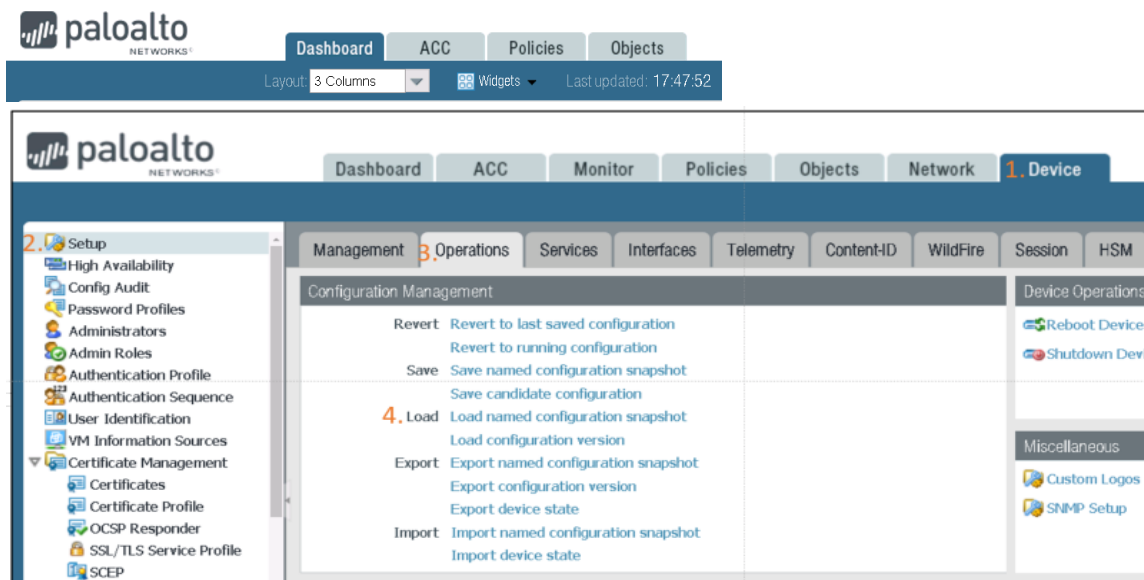
1.0 Connect to the Firewall

1. Launch a browser and connect to <https://192.168.1.254>.
2. Log in to the Palo Alto Networks firewall using the following:

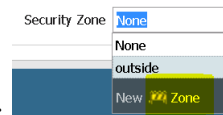
Parameter	Value
Name	Admin
Password	Admin

1.1 Apply a Baseline Configuration to the Firewall

3. In the Palo Alto Networks firewall web interface, select **Device > Setup > Operations**.
4. Click **Load named configuration snapshot**:



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



6. Click **OK**. A loading configuration dialog box soon appears:
7. Click **Close**.
8. Click the **Commit** link at the top right of the web interface. Click **Commit** and wait until the commit process is complete. Click **Close** to continue.



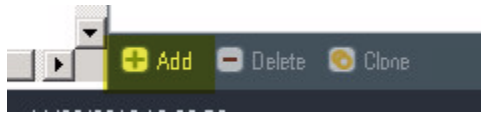
Note: Continue if you are warned about a full commit.

1.2 Add an Admin Role Profile


Admin Role Profiles are custom roles that determine the access privileges and responsibilities of administrative users.





9. Select **Device > Admin Roles**. 

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



11. Enter the name **policy-admins-role**.

12. Click the **Web UI** tab. Click the  icon to disable the following:

Parameter	Value
Monitor	
Network	
Device	
Privacy	

13. Click the **XML API** tab and verify that all items are  disabled.

14. Click the **Command Line** tab and verify that the selection is **None**.



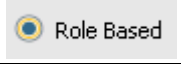
15. Click  to continue.

1.3 Add an Administrator Account

16. Select **Device > Administrators**. 

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

18. Configure the following:

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

19. Click **OK**.

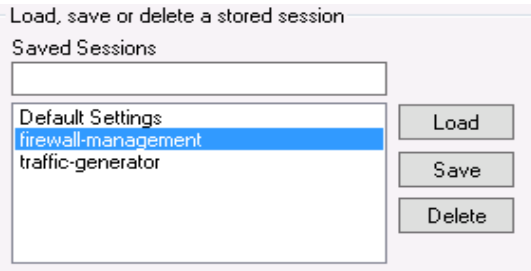
20. Click the **Commit** link at the top right of the web interface. Click **Commit** and wait until the commit process is complete. Click **Close** to continue.

1.4 Test the policy-admin User



21. Open **PuTTY** from the Windows desktop.

22. Double-click **firewall-management**:



23. 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.

```
admin@firewall-a>
```

24. Close the **PuTTY** window and then open **PuTTY** again.

25. Double-click **firewall-management**.

26. Log in using the following information (the window will close if authentication is successful):

Parameter	Value
Name	policy-admin
Password	paloalto

The **PuTTY** window closes because the Admin Role assigned to this account denies CLI access.

27. Open a *different* browser (not a tab) in private/incognito mode and browse to

<https://192.168.1.254>. A Certificate Warning might appear.

28. Click through any Certificate Warning. The Palo Alto Networks firewall login page opens.

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

Parameter	Value
Name	policy-admin
Password	paloalto

30. **Close** the **Welcome** window if one is presented.

31. Explore the available functionality of the web interface. Notice that several tabs and functions are excluded from the interface because of the Admin Role assigned to this user account:



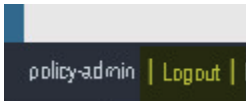
1.5 Take a Commit Lock and Test the Lock


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.


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





33. Click **Take Lock** in the lower-left corner of the panel. A **Take lock** window opens.
34. Set the Type to **Commit**, and click **OK**. The policy-admin lock is listed in the **Locks** window.
35. Click **Close** to close the **Locks** window.
36. Click the **Logout** button on the lower-left corner of the web interface:

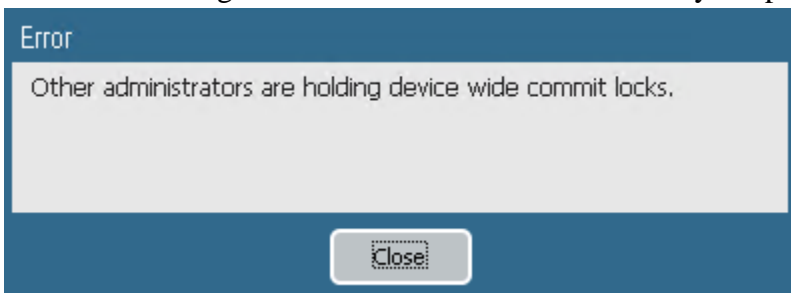


37. Close the **policy-admin** browser window.
38. Return to the web interface where you are logged in as the *admin* account.
39. Click the **Device > Administrators** link. The web interface refreshes. Notice the **lock** icon in the upper-right corner of the web interface.  (1)

40. Click  to add another administrator account.
41. Configure the following:

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

42. Click **OK**. The new test-lock user is listed.
43.  **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:



44. Click **Close**.
45. Click the **transaction lock** icon in the upper-right corner:



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



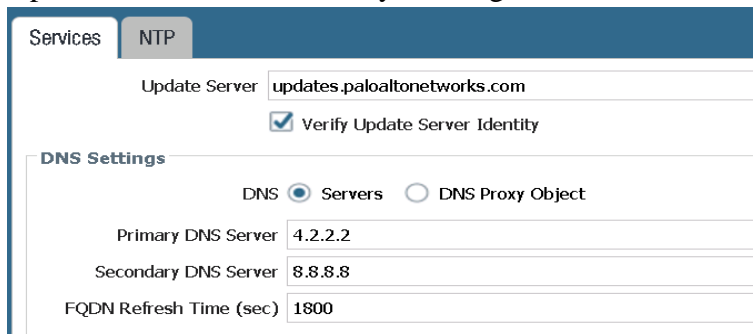
Note: The user that took the lock or any superuser can remove a lock.

47. Click **OK** and the lock is removed from the list.
48. Click **Close**.
49. Now that the lock is removed, changes can be committed. **Commit** all changes.
50. Select the **test-lock** user and then click **Delete** to delete the test-lock user.
51. Click **Yes** to confirm the deletion.
52. **Commit** all changes.

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.

53. Select **Device > Setup > Services**.
54. Open the **Services** window by clicking the icon in the upper-right corner of the **Services** panel:



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

1.7 Schedule Dynamic Updates

Palo Alto Networks regularly posts updates for application detection, threat protection, and GlobalProtect data files through dynamic updates.

58. Select **Device > Dynamic Updates**.
59. Locate and click the **Schedule** hyperlink on the far right of **Antivirus**:

▼ **Antivirus** **Last checked:** 2017/03/05 23:53:54 UTC **Schedule:** **None**

The scheduling window opens. Antivirus signatures are released daily.

60. Configure the following:

Parameter		Value
Recurrence		Daily
Time		01:02
Action		download-and-install

61. Click **OK**.

62. Locate and click the **Schedule** hyperlink on the far right of **Application and Threats**. The scheduling window opens. Application and Threat signatures are released weekly.

63. Configure the following:

Parameter	Value
Recurrence	Weekly
Day	Wednesday
Time	01:05
Action	download-and-install

64. Click **OK**.

65. Locate and click the **Schedule** hyperlink on the far right of **WildFire**. The scheduling window opens. WildFire® signatures can be available within five minutes.

66. Configure the following:

Parameter	Value
Recurrence	Every Minute
Action	download-and-install

67. Click **OK**.

68.  **Commit** all changes.



Stop. This is the end of the Initial Configuration lab.