



PALO ALTO NETWORKS - EDU-210



Lab 9: User-ID

Document Version: 2021-08-24

Copyright © 2021 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
9 User-ID	6
9.0 Load Lab Configuration	6
9.1 Enable User-ID on the Inside Zone.....	9
9.2 Configure the LDAP Server Profile	10
9.3 Configure User-ID Group Mapping	12
9.4 Configure an Integrated Firewall Agent	13
9.5 Verify the User-ID Configuration.....	17
9.6 Review the Logs.....	20
9.7 Create a Security Policy Rule.....	20
9.8 Review Logs	24

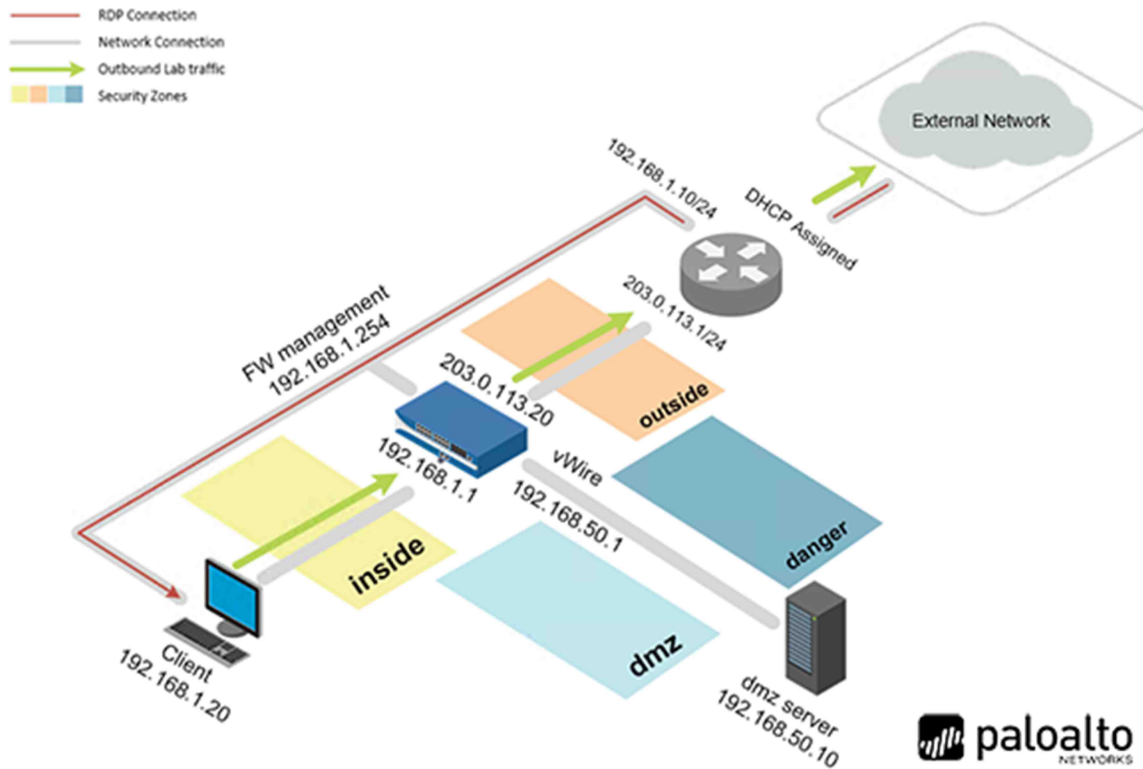
Introduction

Management would like to get reports on users for items such as which sites they have visited or if they have downloaded viruses. They would also like to restrict certain applications to specific users within the company. In order to provide management with those types of reports and to be able to restrict the applications, you will need to enable User-ID.

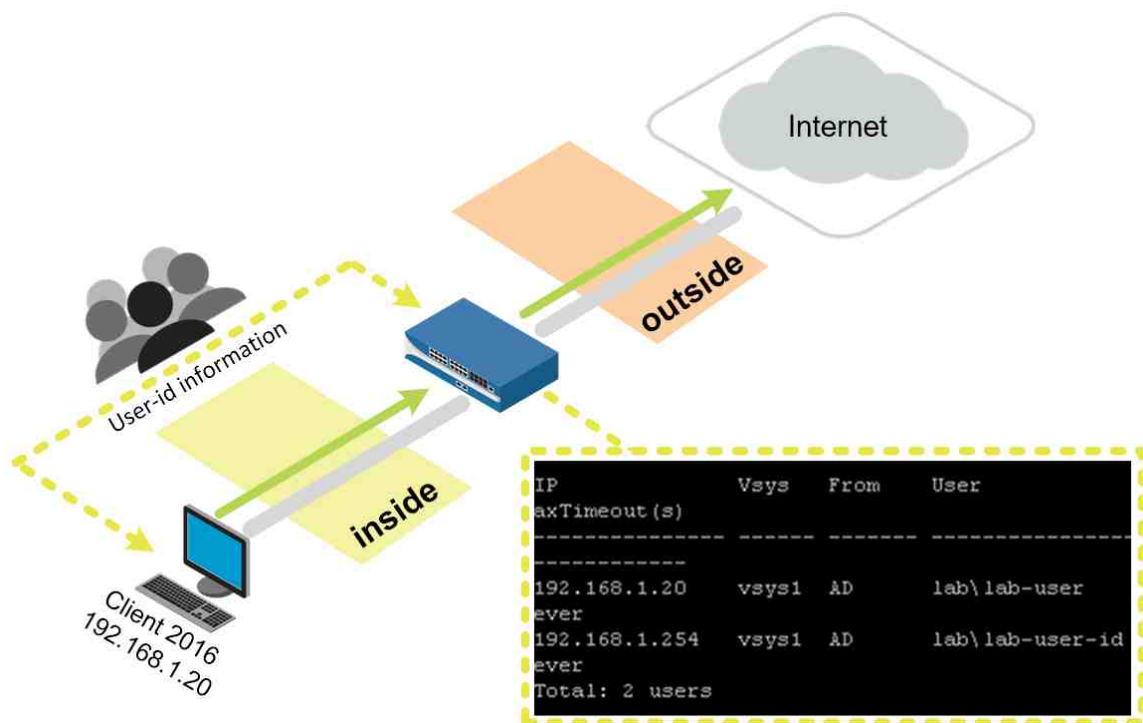
Objectives

-) Enable User-ID technology on the inside zone
-) Configure the LDAP Server Profile to be used in group mapping
-) Configure group mapping for User-ID
-) Configure and test the PAN-OS® integrated User-ID agent
-) Leverage User-ID information in a Security policy rule

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	Training\$
Firewall	192.168.1.254	admin	Training\$

9 User-ID

9.0 Load Lab Configuration

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. Log in as lab-user using the password **Training\$**.



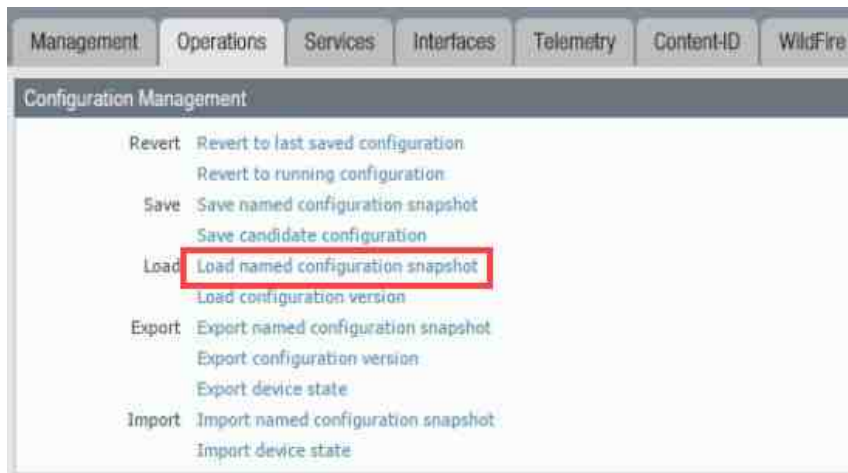
3. Launch the Chromium Web Browser and connect to `https://192.168.1.254`.
4. If a security warning appears, click Advanced and proceed by clicking on Proceed to 192.168.1.254 (unsafe).
5. Log in to the Palo Alto Networks firewall using the following:

Parameter	Value
Name	admin
Password	Training\$

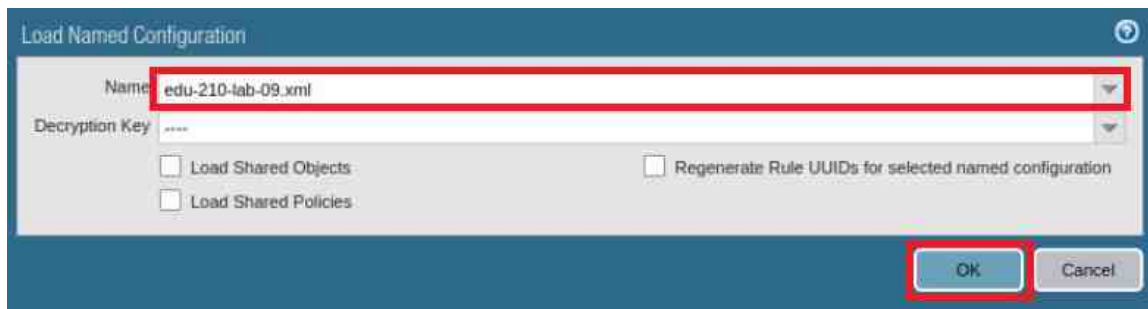
6. In the web interface, select Device > Setup > Operations.



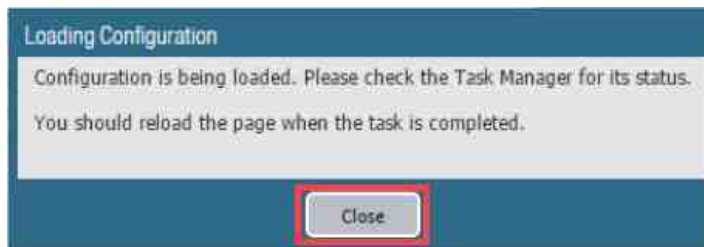
- Click Load named configuration snapshot:



- Click the dropdown list next to the Name text box and select edu-210-lab-09.xml. Click OK.



- Click Close.

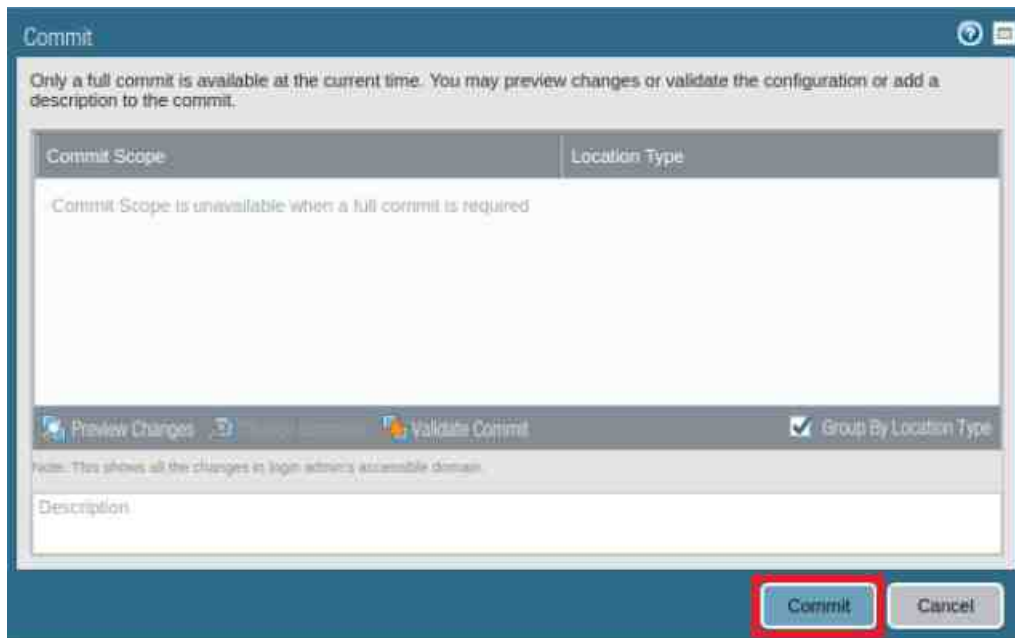


The following instructions are the steps to execute a "Commit All" as you will perform many times throughout these labs.

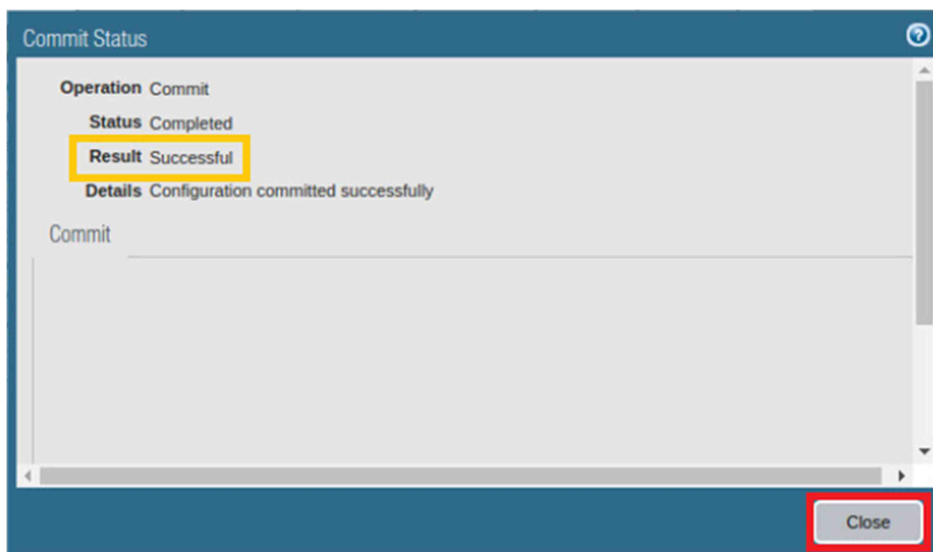
- Click the Commit link at the top-right of the web interface.



11. Click Commit and wait until the commit process is complete.



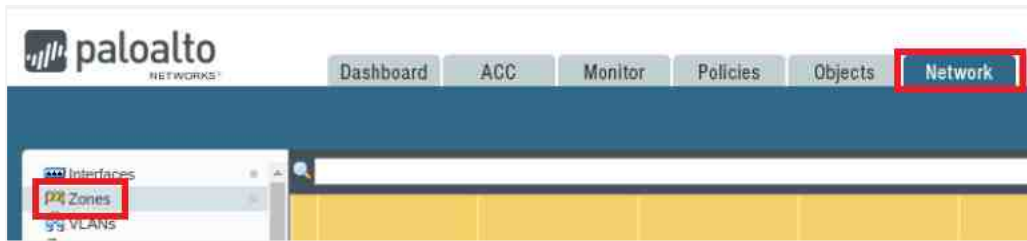
12. Once completed successfully, click Close to continue.



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

9.1 Enable User-ID on the Inside Zone

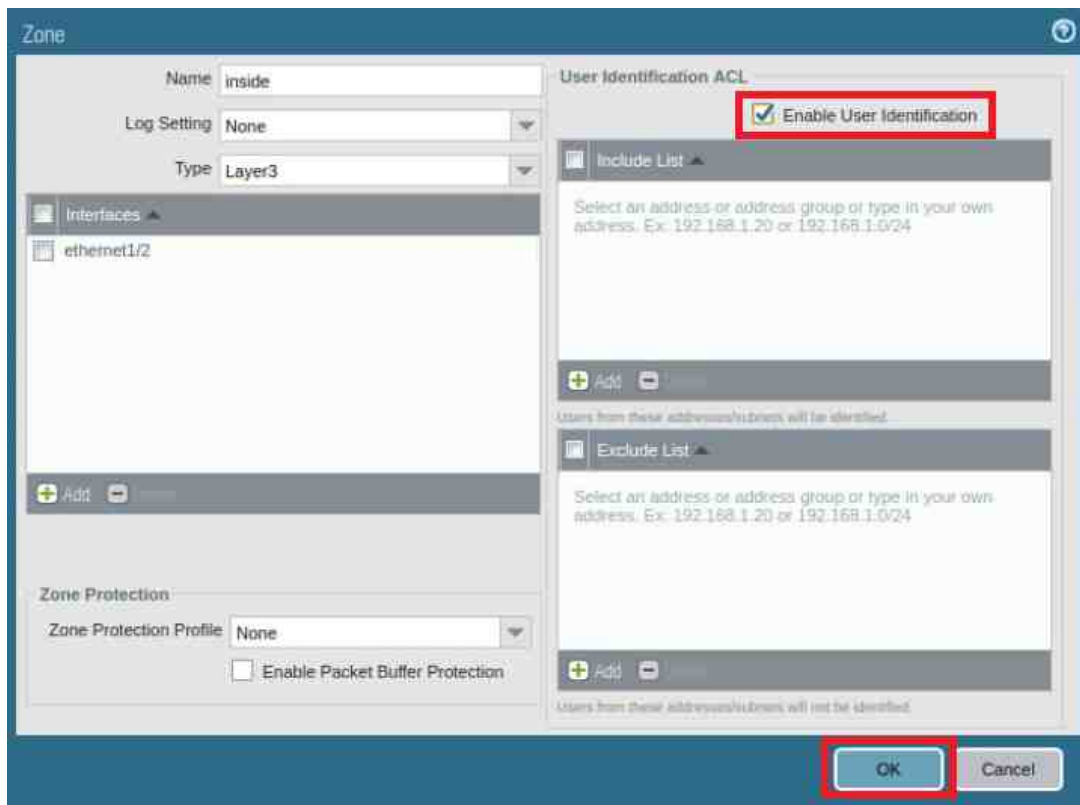
1. In the web interface, navigate to Network > Zones.



2. Click on inside from the list to open the Zone configuration window.

Name	Type	Interfaces / Virtual Systems
danger	virtual-wire	ethernet1/4 ethernet1/5
dmz	layer3	ethernet1/3
inside	layer3	ethernet1/2
outside	layer3	ethernet1/1

3. In the Zone window, enable User-ID by selecting the Enable User Identification checkbox. Click OK.

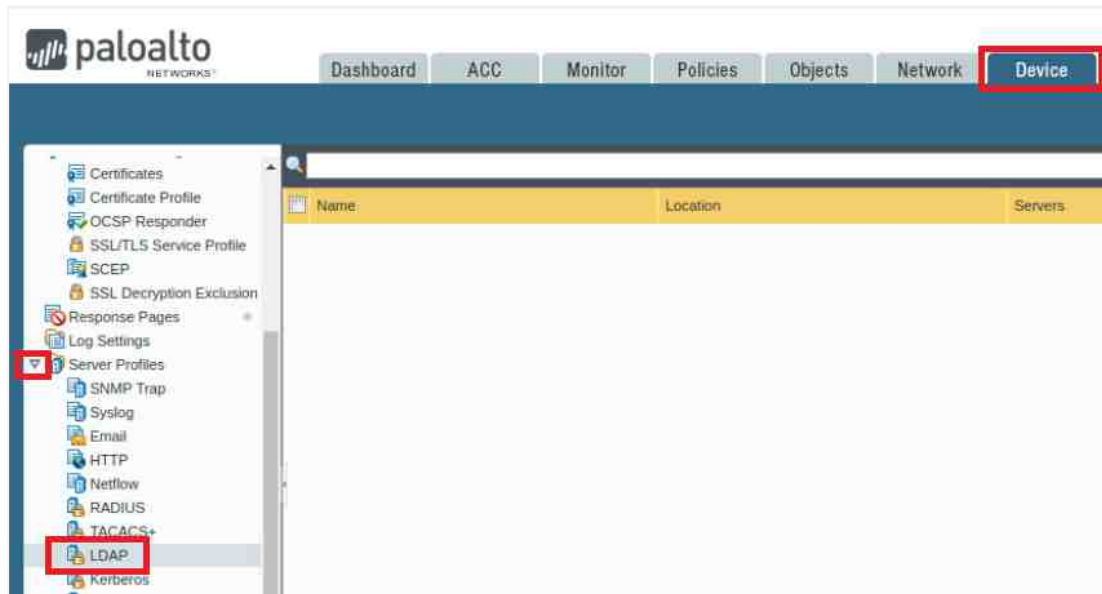


4. Leave the firewall web interface open to continue with the next task.

9.2 Configure the LDAP Server Profile

In this task, you will create a Server Profile so the firewall can pull user and group information from Active Directory.

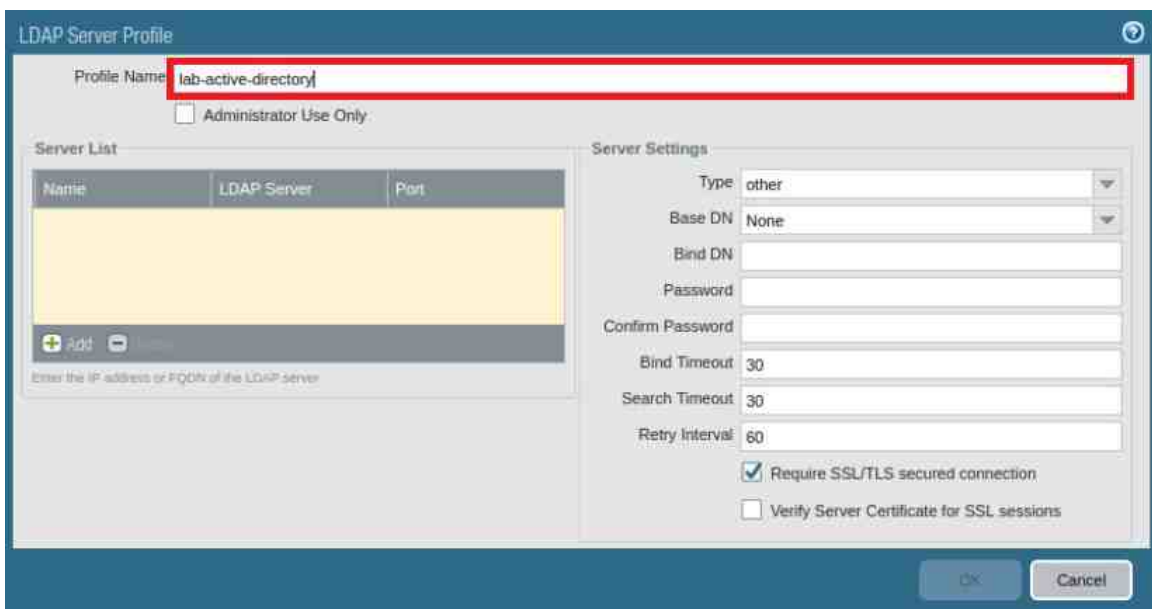
1. In the web interface, select Device > Server Profiles > LDAP.



2. Click Add to open the LDAP Server Profile configuration window.

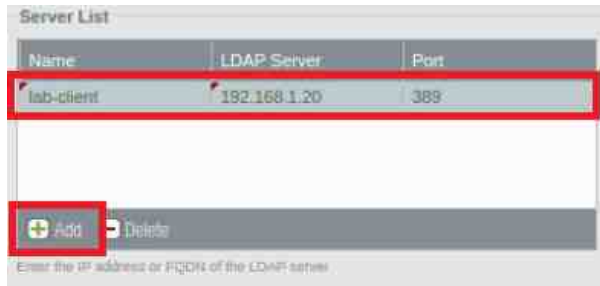


3. In the LDAP Server Profile window, type lab-active-directory into the Profile Name text field.



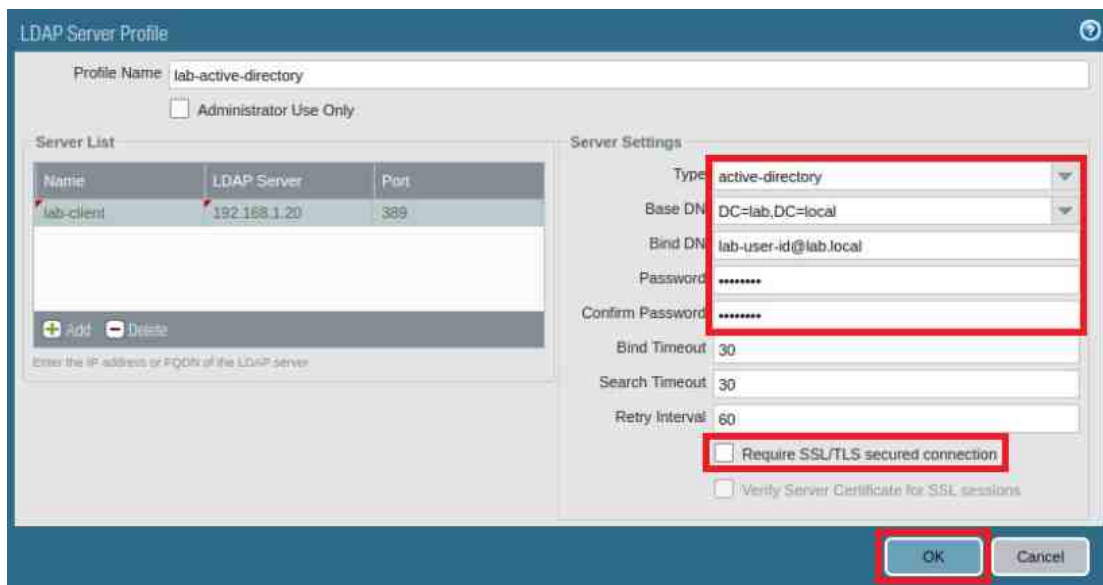
4. In the LDAP Server Profile window, locate the Server List on the left side, click Add, and configure the following.

Parameter	Value
Name	Type lab-cl i ent
LDAP Server	Type 192. 168. 1. 20
Port	Verify that port 389 is selected



5. In the LDAP Server Profile window, locate Server Settings on the right side and configure the following. Once finished, click OK.

Parameter	Value
Require SSL/TLS secured connection	Deselect the checkbox (make sure to do this task first)
Type	Select active-directory from the dropdown list
Base DN	Type DC=l ab, DC=l ocal
Bind DN	Type l ab-user-i d@l ab. l ocal
Password	Type P a l O A I t o
Confirm Password	Type P a l O A I t o



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

9.3 Configure User-ID Group Mapping

In this task, you will define which users and groups will be available when policy rules are created.

1. In the web interface, select Device > User Identification > Group Mapping Settings.

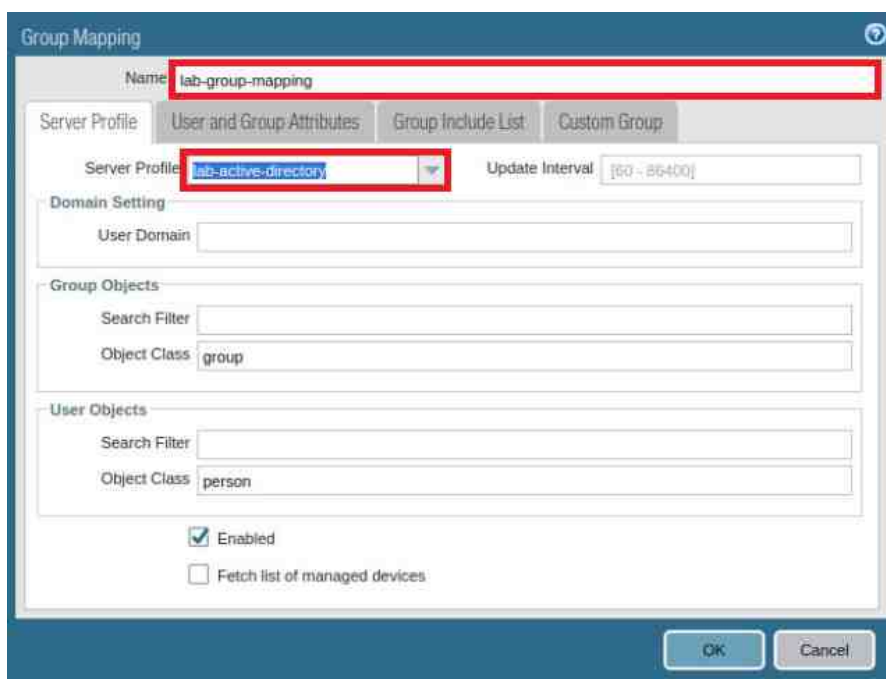


2. Click Add to open the Group Mapping configuration window.

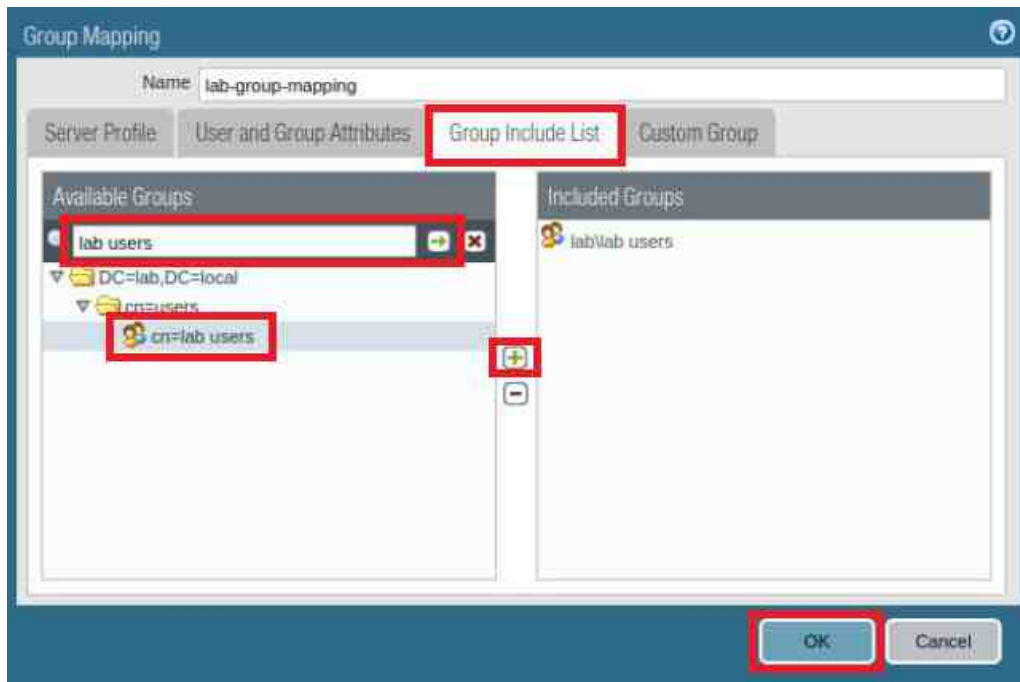


3. In the Group Mapping window, while on the Server Profile tab, configure the following.

Parameter	Value
Name	Type lab-group-mapping
Server Profile	Select lab-active-directory from the dropdown list



- In the Group Mapping window, click the Group Include List tab and type `lab users` into the search box, followed by pressing the Enter key. After running the search, select `cn=lab users` and then click the plus icon to add the selected to the Included Groups pane, then click OK.



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

9.4 Configure an Integrated Firewall Agent

- In the web interface, select Device > User Identification > User Mapping.



- Click the gear icon in the top-right of the Palo Alto Networks User-ID Agent Setup pane.

- In the Palo Alto Networks User-ID Agent Setup window, while on the Server Monitor Account tab, configure the following.

Parameter	Value
User Name	Type lab.local\lab-user-id
Password	Type Palo Alto



Palo Alto Networks User-ID Agent Setup

Server Monitor Account | Server Monitor | Client Probing | Cache | NTLM | Redistribution | Syslog Filters | Ignore User List

User Name: lab.local\lab-user-id

Domain's DNS Name:

Password:

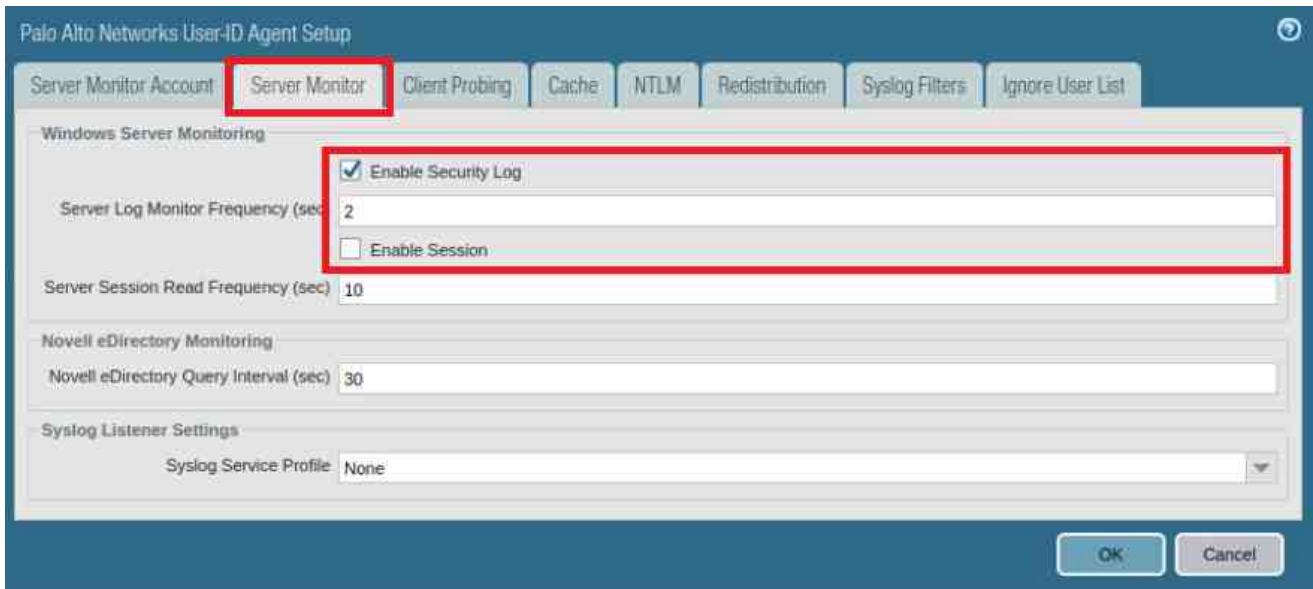
Confirm Password:

Kerberos Server Profile: None

OK Cancel

- In the Palo Alto Networks User-ID Agent Setup window, click the Server Monitor tab and verify the following:

Parameter	Value
Enable Security Log	Checked
Server Log Monitor Frequency (sec)	2
Enable Session	Unchecked



Palo Alto Networks User-ID Agent Setup

Server Monitor Account | Server Monitor | Client Probing | Cache | NTLM | Redistribution | Syslog Filters | Ignore User List

Windows Server Monitoring

☒ Enable Security Log

Server Log Monitor Frequency (sec): 2

☐ Enable Session

Server Session Read Frequency (sec): 10

Novell eDirectory Monitoring

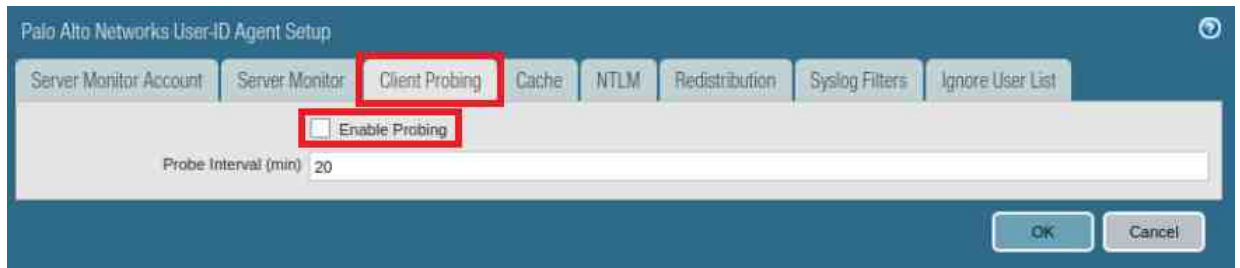
Novell eDirectory Query Interval (sec): 30

Syslog Listener Settings

Syslog Service Profile: None

OK Cancel

- In the Palo Alto Networks User-ID Agent Setup window, click the Client Probing tab and verify that the Enable Probing checkbox is deselected.



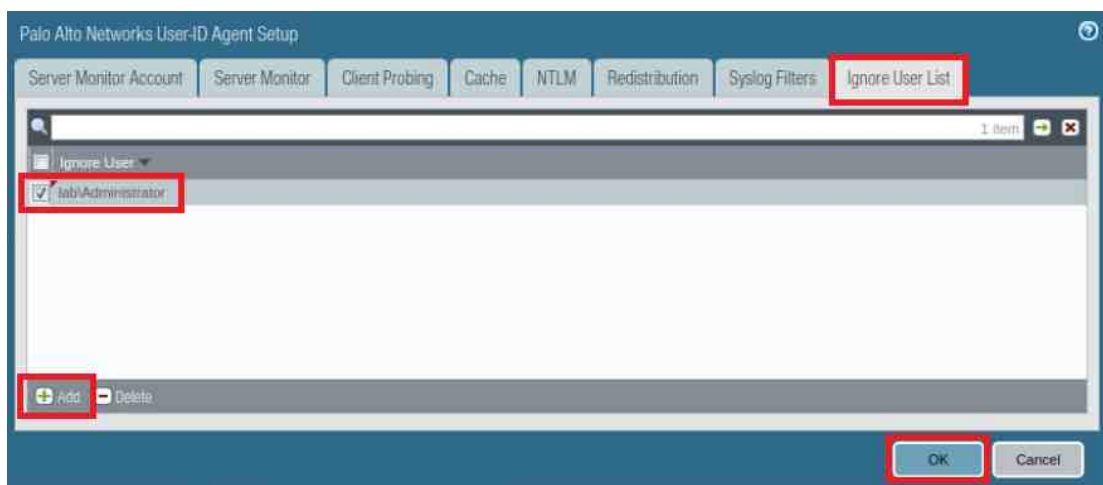
- In the Palo Alto Networks User-ID Agent Setup window, click the Cache tab and uncheck the Enable User Identification Timeout checkbox. Ensure that 45 is entered in the User Identification Timeout (min) text field.



You do not need to time out the IP address associated with the lab-user-id because the IP never changes. In a production environment, the timeout is recommended to be half the DHCP lease time.

- In the Palo Alto Networks User-ID Agent Setup window, click the Ignore User List tab, then click Add and configure the following. Once finished, click OK.

Parameter	Value
Ignore User	Type Lab\Administrator





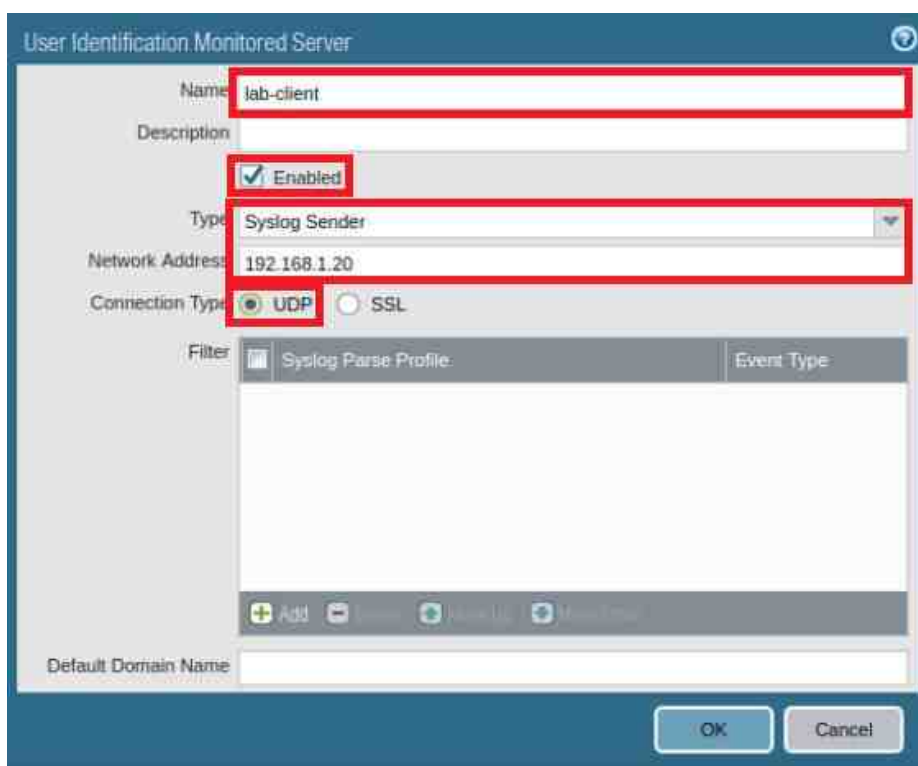
Addition of the Administrator to the Ignore User List prevents the firewall from assuming that Administrator is associated with 192.168.1.20.

8. Scroll down to the Server Monitoring pane, then click Add.

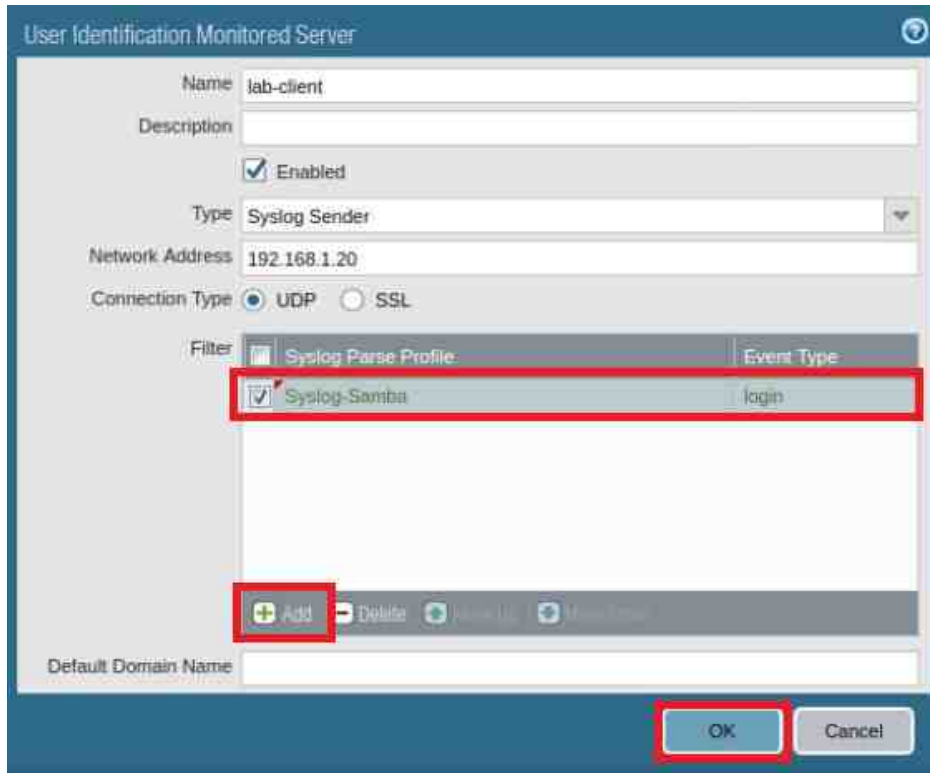


9. In the User Identification Monitored Server window, configure the parameters in the following table.

Parameter	Value
Name	Type lab-client
Enabled	Select the checkbox
Type	Verify that Syslog Sender is selected
Network Address	Type 192. 168. 1. 20
Connection Type	Verify that UDP is selected



10. In the User Identification Monitored Server window Filter section, click Add and select Syslog-Samba, then click OK.



The screenshot shows the 'User Identification Monitored Server' configuration window. The 'Name' field is set to 'lab-client'. The 'Type' is 'Syslog Sender' and the 'Network Address' is '192.168.1.20'. The 'Connection Type' is 'UDP'. In the 'Filter' section, a table lists 'Syslog Parse Profile' and 'Event Type'. The 'Syslog-Samba' profile is selected with a checkmark, and its event type is 'login'. Below the table, the 'Add' button is highlighted with a red box. At the bottom right, the 'OK' button is also highlighted with a red box.

Syslog Parse Profile	Event Type
<input checked="" type="checkbox"/> Syslog-Samba	login

11. Commit all changes.
12. Leave the firewall web interface open to continue with the next task.

9.5 Verify the User-ID Configuration

1. Under the Server Monitoring section, verify that the lab-client user is listed.



The screenshot shows the 'Server Monitoring' section of the firewall web interface. It contains a table with the following data:

Name	Enabled	Type	Network Address	Status
lab-client	<input checked="" type="checkbox"/>	Syslog Sender	192.168.1.20	



2. On the Windows desktop, double-click the lab folder.
3. Within the lab folder, double-click the scripts folder.

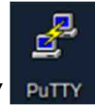


user-id.sh

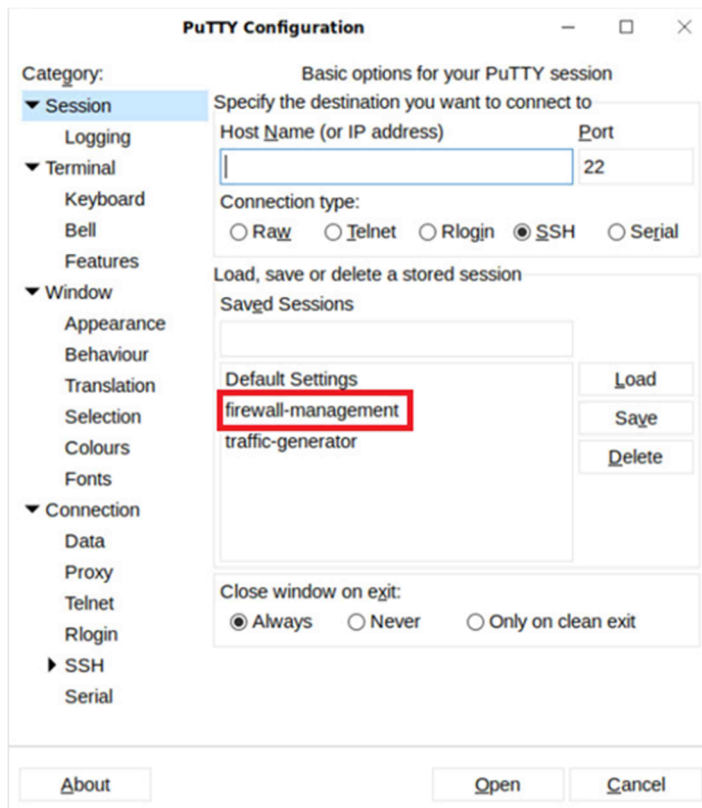
4. Double-click the user-id.sh file to launch the file.



This action will force a login event for the firewall to parse.



5. On the Windows desktop, double-click the PuTTY icon.
6. In the PuTTY window, double-click firewall-management.



7. When prompted for credentials, log in to the firewall with the username `admin` and password `Tra1n1ng$`.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 27 21:11:02 2020

Number of failed attempts since last successful login: 0

admin@firewall-a>
```

8. At the prompt, enter the command below.

```
admin@firewall-a> show user group-mapping state all
```

```
admin@firewall-a> show user group-mapping state all

Group Mapping(vsys1, type: active-directory): lab-group-mapping
  Bind DN      : lab-user-id@lab.local
  Base        : DC=lab,DC=local
  Group Filter : (None)
  User Filter  : (None)
  Servers      : configured 1 servers
                  192.168.1.20(389)
                  Last Action Time: 1781 secs ago(took 1 secs)
                  Next Action Time: In 1819 secs
  Number of Groups: 1
  cn=lab users,cn=users,dc=lab,dc=local

admin@firewall-a>
```

9. Enter the following command:

```
admin@firewall-a> show user ip-user-mapping all
```

```
admin@firewall-a> show user ip-user-mapping all

IP (s)          Vsys      From      User          IdleTimeout(s) MaxTimeout
-----
192.168.1.20    vsys1     SYSLOG    lab\lab-user   Never          Never
Total: 1 users

admin@firewall-a>
```



The lab\lab-user must have the IP address of 192.168.1.20. If that IP address is not listed, do not proceed. Contact your instructor or lab partner for assistance.

10. Type `exit` followed by pressing the Enter key to close the PuTTY session.

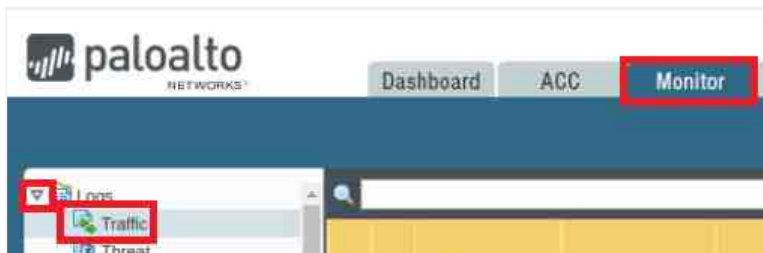
11. Open a new tab in Chromium Web Browser and browse to `msn.com` and `google.com` to generate some traffic.



12. Close the browser tab.

9.6 Review the Logs

1. Change focus to the firewall's web interface and navigate to Monitor > Logs > Traffic.



2. Clear any existing filter and type the filter (addr.src in 192.168.1.20) in the filter text box. Press Enter.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	Dynamic User Group	To Port	Application
	03/16 20:18:21	end	inside	outside	192.168.1.20	lab/lab-user	72.30.35.88		123	ntp
	03/16 20:18:20	end	inside	outside	192.168.1.20	lab/lab-user	46.4.34.242		123	ntp
	03/16 20:18:19	end	inside	outside	192.168.1.20	lab/lab-user	213.5.39.34		123	ntp
	03/16 20:18:18	end	inside	outside	192.168.1.20	lab/lab-user	74.121.138.36		443	ssl
	03/16 20:18:17	end	inside	outside	192.168.1.20	lab/lab-user	213.251.53.217		123	ntp

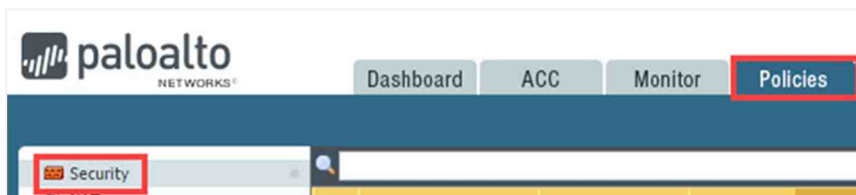


Notice that the Source User column now shows the lab-user. This user-id reference could take up to three minutes to show on the logs. Click refresh to update the log entries.

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

9.7 Create a Security Policy Rule

1. In the web interface, navigate to Policies > Security.



2. Click Add to open the Security Policy Rule configuration window.



3. In the Security Policy Rule window, while on the General tab, configure the following:

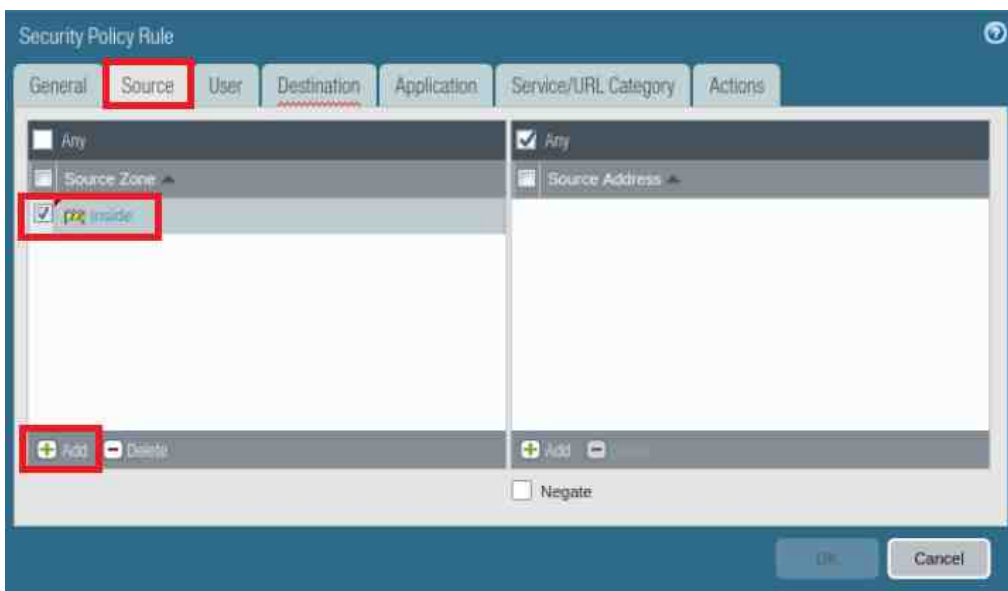
Parameter	Value
Name	Type egress-outside-user-id
Rule Type	Verify that universal (default) is selected
Tags	Select egress from the dropdown list
Group Rules By Tag	Select egress from the dropdown list
Audit Comment	Type Created Security Policy on <date> by admin



The screenshot shows the 'Security Policy Rule' window with the 'General' tab selected. The 'Name' field is 'egress-outside-user-id', 'Rule Type' is 'universal (default)', 'Tags' is 'egress', and 'Group Rules By Tag' is 'egress'. The 'Audit Comment' field contains 'Created Security Policy on 03/16/2020 by admin'. The 'General' tab is highlighted with a red box.

4. In the Security Policy Rule window, click the Source tab and configure the following.

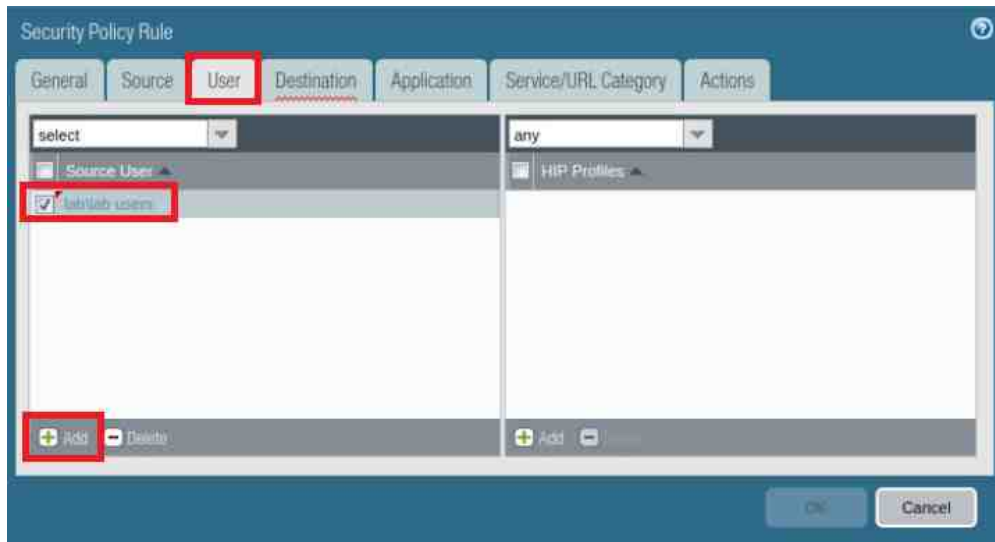
Parameter	Value
Source Zone	Click Add and select inside from the dropdown list



The screenshot shows the 'Security Policy Rule' window with the 'Source' tab selected. The 'Source Zone' dropdown is open, showing 'Any' and 'Source Zone'. The 'Add' button is highlighted with a red box.

5. In the Security Policy Rule window, click the User tab and configure the following:

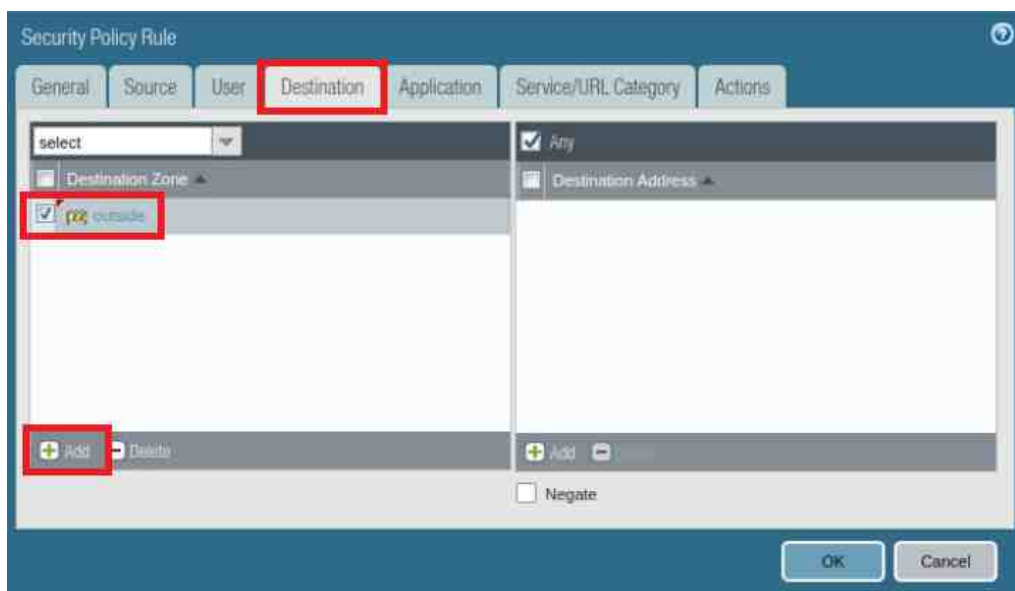
Parameter	Value
Source User	Click Add and select lab\lab users from the dropdown list



If the list of usernames does not appear from the dropdown list, start to type the username and the list should then populate.

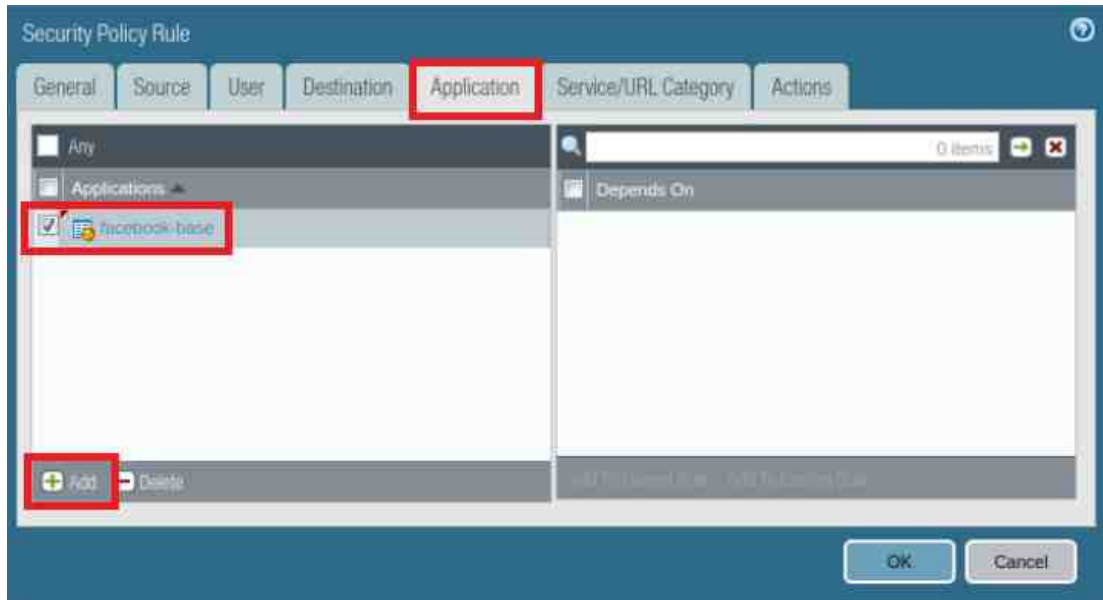
6. In the Security Policy Rule window, click the Destination tab and configure the following:

Parameter	Value
Destination Zone	Click Add and select outside from the dropdown list



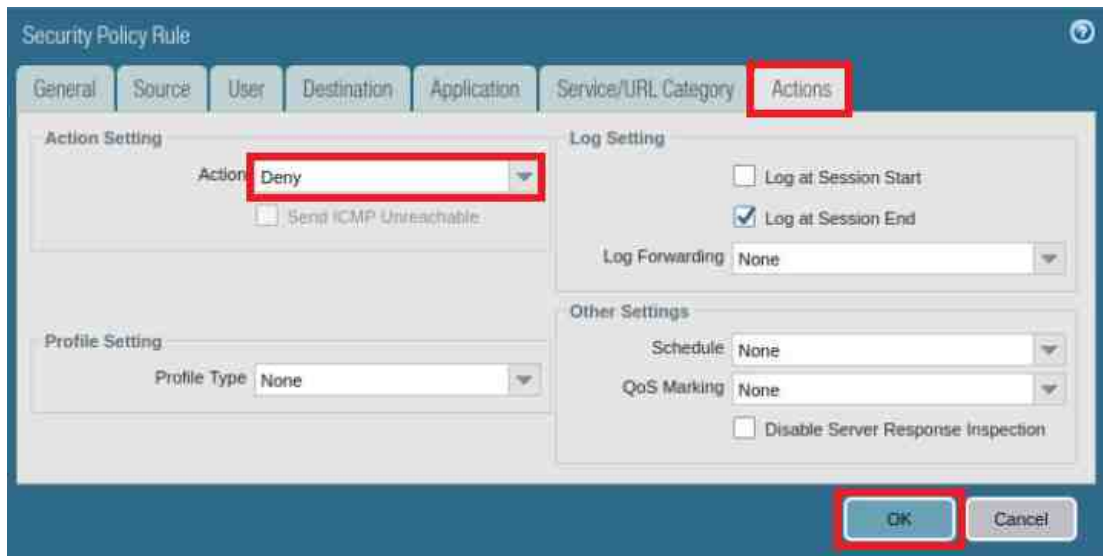
7. In the Security Policy Rule window, click the Application tab and configure the following:

Parameter	Value
Applications	Click Add and select facebook-base from the dropdown list

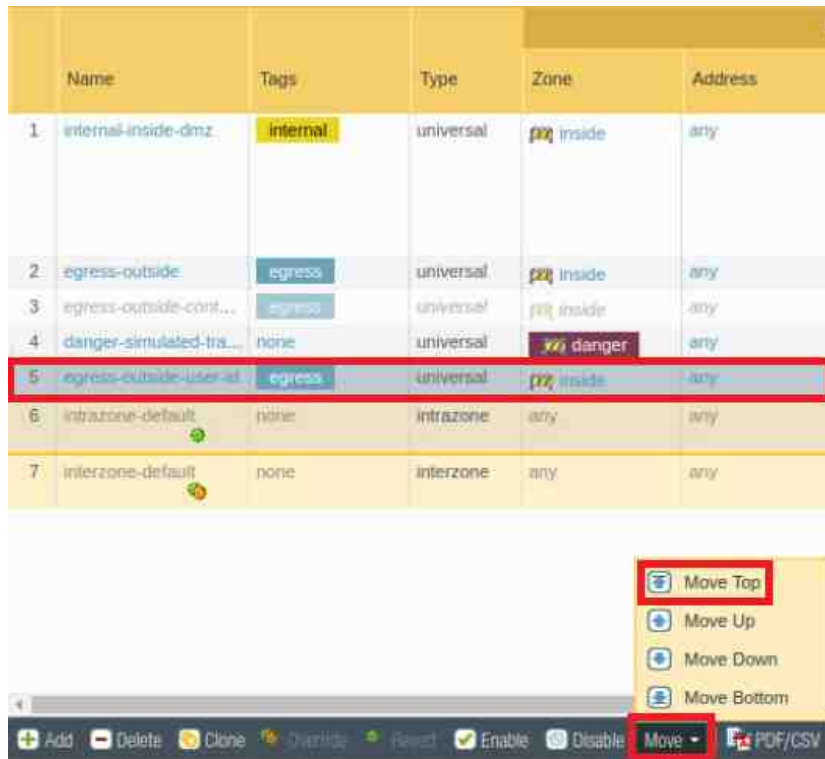


8. In the Security Policy Rule window, click the Actions tab and configure the following, then click OK to close the window.

Parameter	Value
Action	Select Deny from the dropdown list



9. Select, but do not open the egress-outside-user-id Security policy rule. Click Move and select Move Top to move the rule to the top of the list.



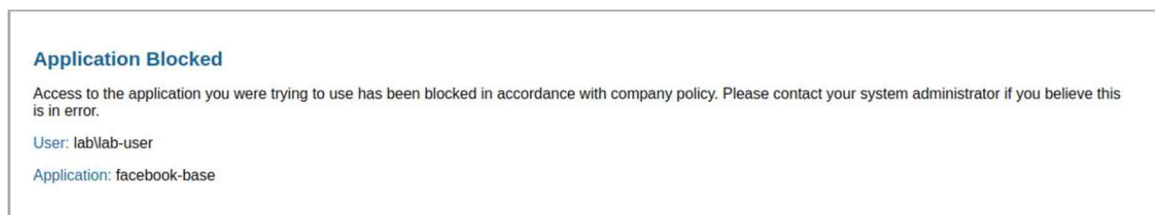
10. Commit all changes.

9.8 Review Logs

1. Open a new tab in Chromium Web Browser and browse to www.facebook.com.



2. Notice that the connection is denied based on the egress-outside-user-id Security policy rule. Close the browser tab.



3. Change focus to the firewall's web interface and navigate to Monitor > Logs > Traffic.

4. Clear any existing filters and type the filter `(rule eq 'egress-outside-user-id')` in the search criteria. Press Enter.

`(rule eq 'egress-outside-user-id')`

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	Dynamic User Group	To Port	Application
	03/16 20:33:35	deny	inside	outside	192.168.1.20	lab\lab-user	31.13.71.36		80	facebook-base
	03/16 20:33:35	deny	inside	outside	192.168.1.20	lab\lab-user	31.13.71.36		80	facebook-base
	03/16 20:33:35	deny	inside	outside	192.168.1.20	lab\lab-user	31.13.71.36		80	facebook-base



Notice that the Source User column shows the lab\lab-user and the Action column is reset-both.

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