



PALO ALTO NETWORKS - EDU-210



Lab 9: User-ID

Document Version: 2019-11-12

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Theoretical Lab Topology.....	4
Lab Settings	5
1 User-ID	6
1.0 Load Lab Configuration	6
1.1 Enable User-ID on the Inside Zone.....	8
1.2 Configure the LDAP Server Profile	9
1.3 Configure User-ID Group Mapping	12
1.4 Configure an Integrated Firewall Agent	13
1.5 Verify the User-ID Configuration.....	17
1.6 Review the Logs.....	19
1.7 Create a Security Policy Rule	20
1.8 Review Logs	24

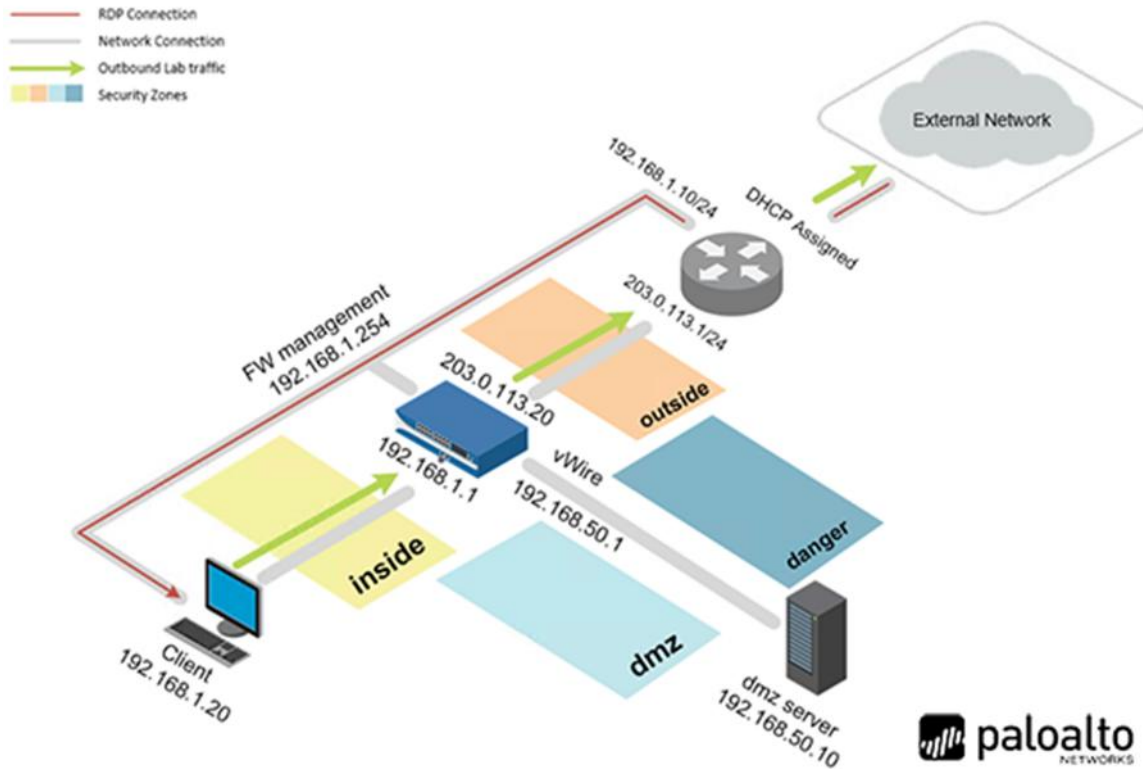
Introduction

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.

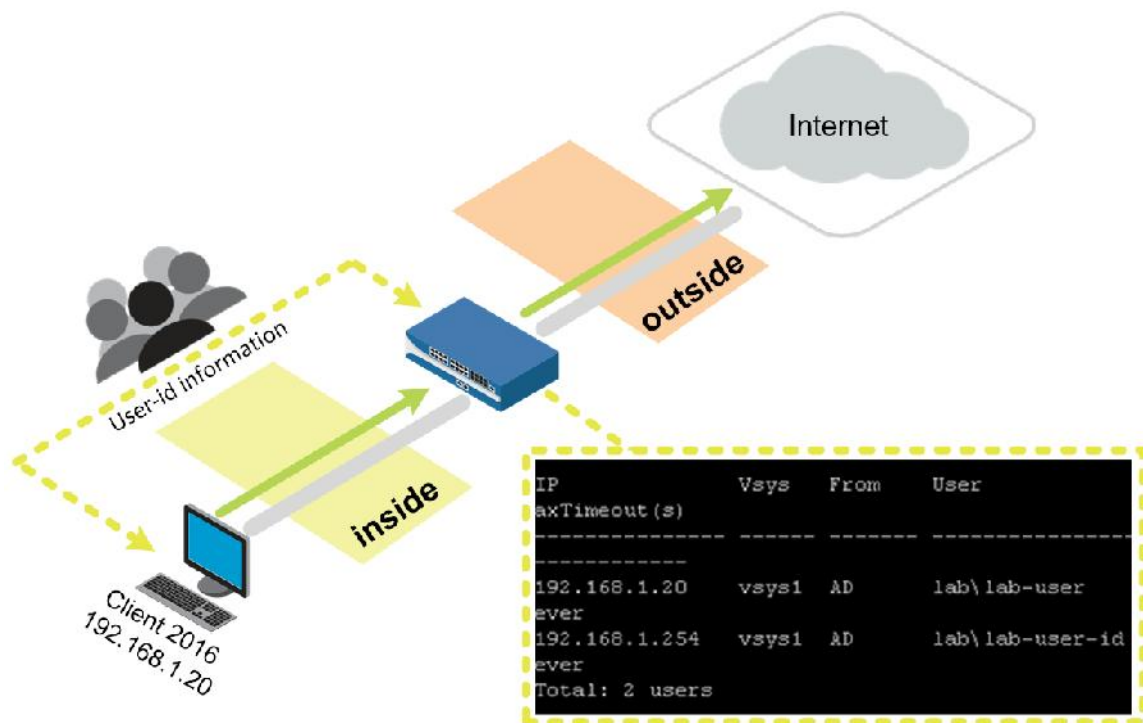
Objectives

-) 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	Pa10Alt0
Firewall	192.168.1.254	admin	admin

1 User-ID

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



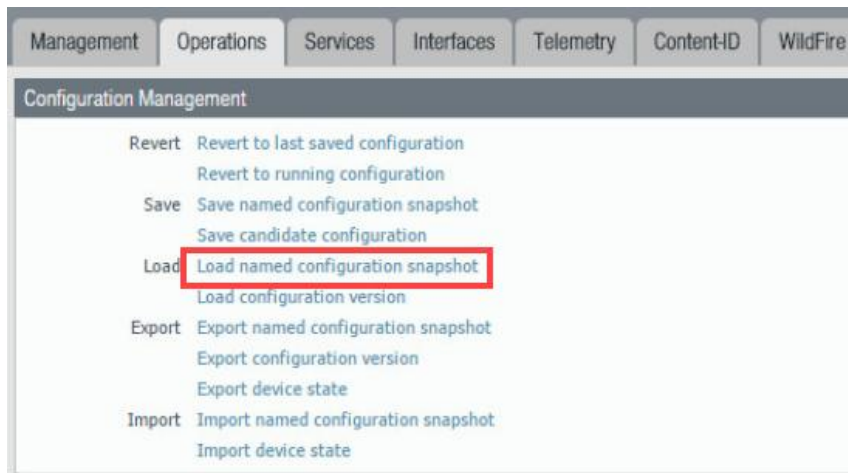
3. Launch the **Chrome** browser and connect to **https://192.168.1.254**.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	admin
Password	admin

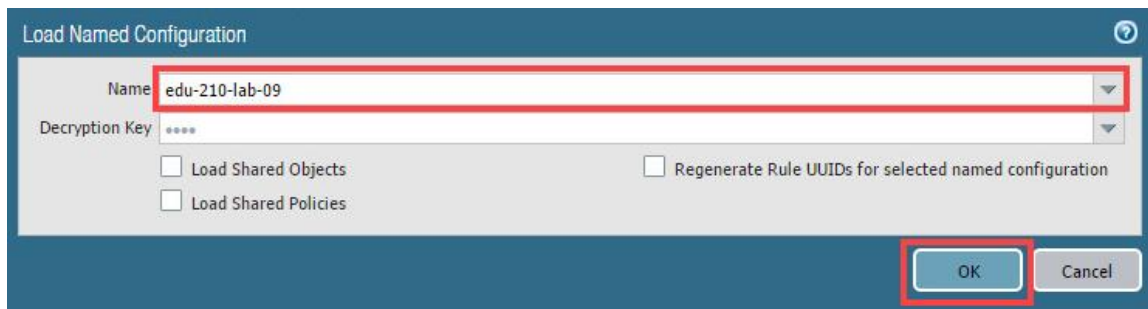
6. In the web interface, navigate to **Device > Setup > Operations**.



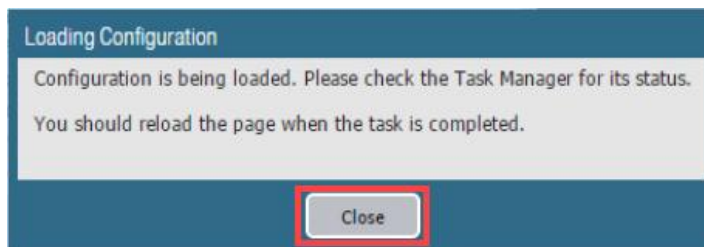
7. Click **Load named configuration snapshot**:



8. Click the drop-down list next to the *Name* text box and select **edu-210-lab-09**. Click **OK**.



9. Click **Close**.

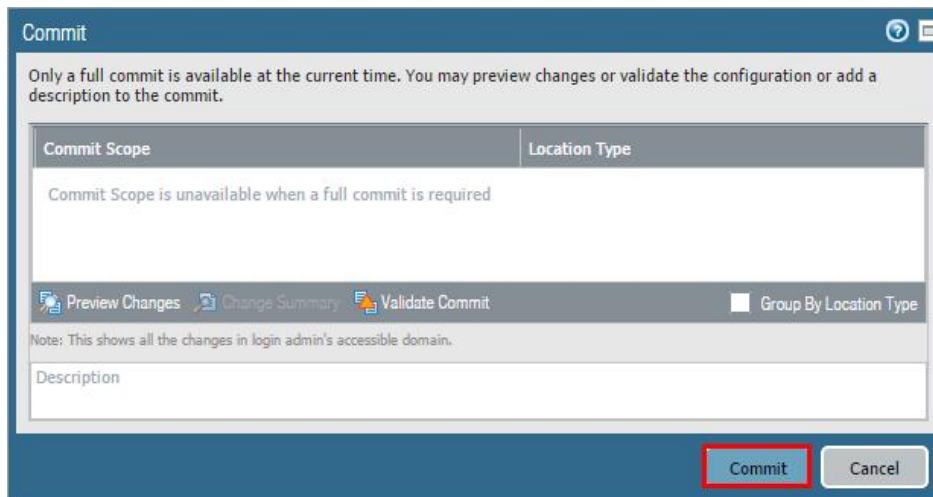


The following instructions are the steps to execute a **“Commit All”** as you will perform many times throughout these labs.

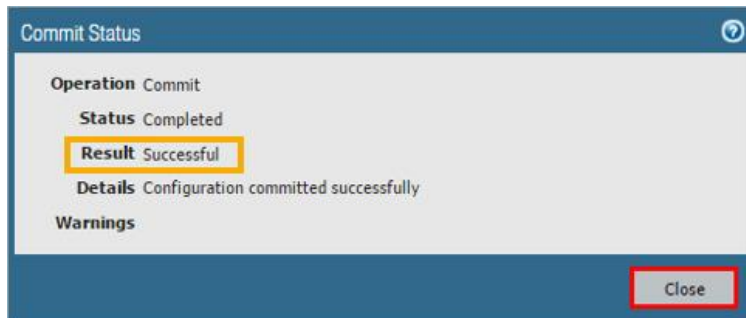
10. Click the **Commit** link at the top-right of the web interface.



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



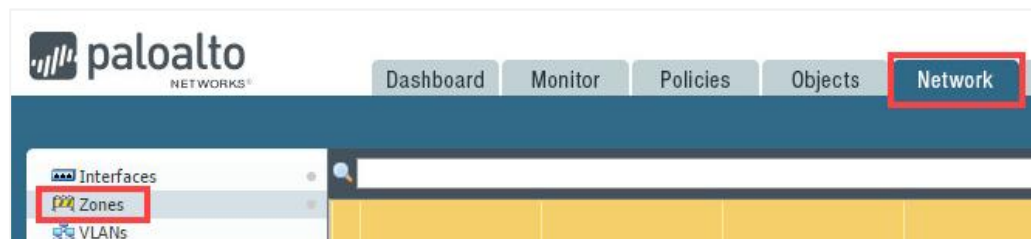
12. Once completed successfully, click **Close** to continue.



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

1.1 Enable User-ID on the Inside Zone

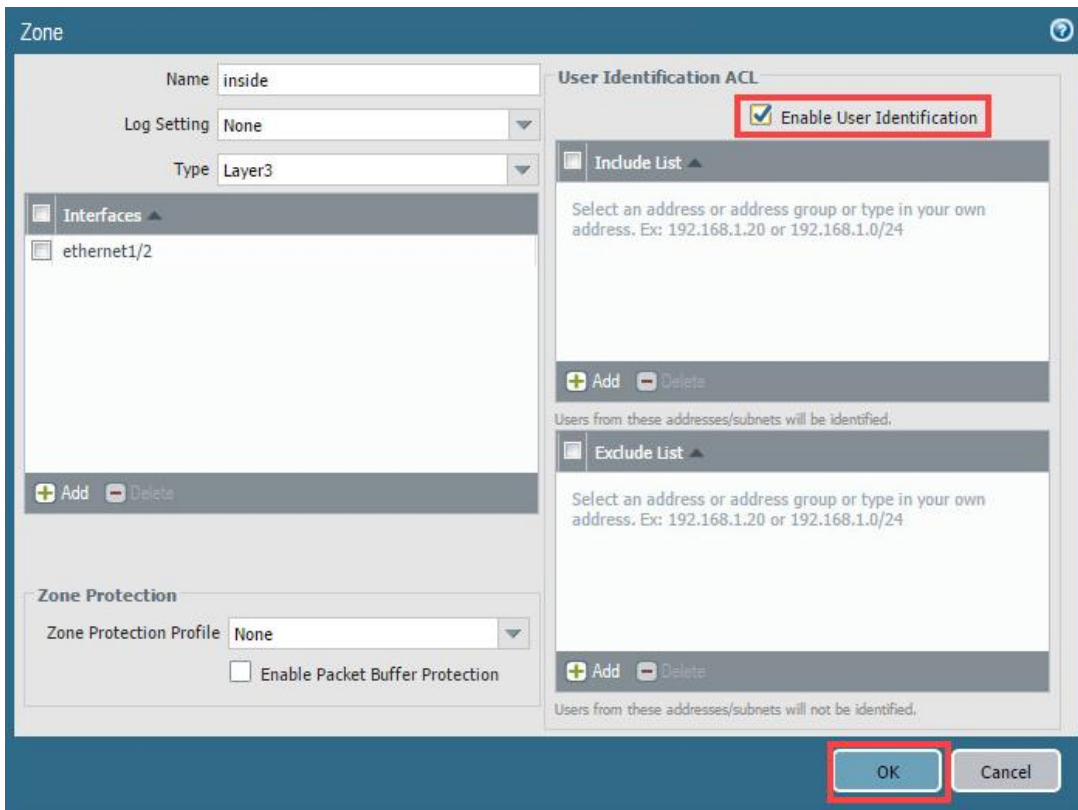
1. In the web interface, navigate to **Network > Zones**.



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

<input type="checkbox"/>	Name	Type	Interfaces / Virtual Systems
<input type="checkbox"/>	danger	virtual-wire	ethernet1/4 ethernet1/5
<input type="checkbox"/>	dmz	layer3	ethernet1/3
<input type="checkbox"/>	inside	layer3	ethernet1/2
<input type="checkbox"/>	outside	layer3	ethernet1/1

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



Zone

Name: inside

Log Setting: None

Type: Layer3

Interfaces:

- ethernet1/2

Zone Protection:

Zone Protection Profile: None

☐ Enable Packet Buffer Protection

User Identification ACL:

☒ Enable User Identification

Include List:

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will be identified.

Exclude List:

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will not be identified.

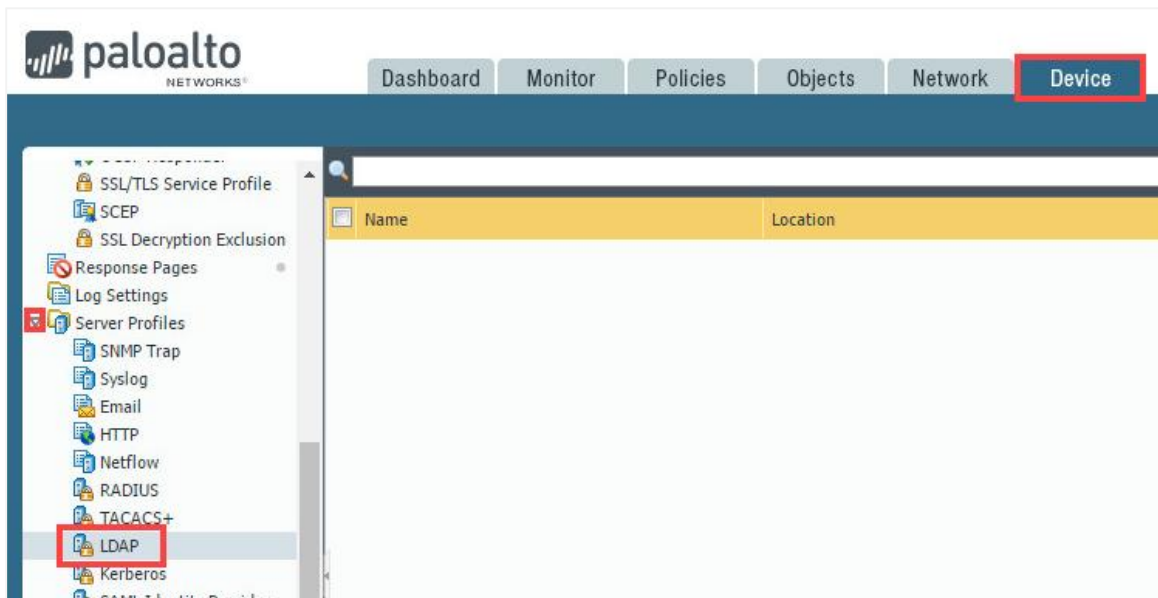
OK Cancel

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

1.2 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.

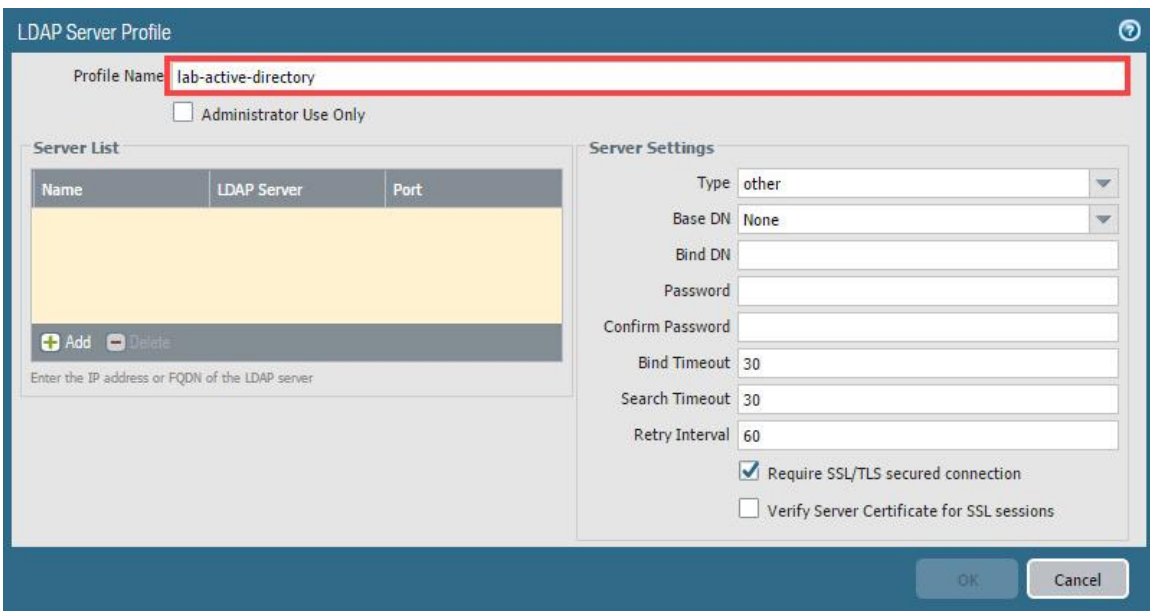
1. In the web interface, select **Device > Server Profiles > LDAP**.



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

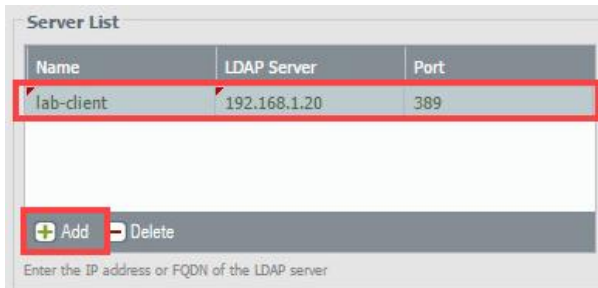


3. In the *LDAP Server Profile* window, type **lab-active-directory** into the *Profile Name* text field.



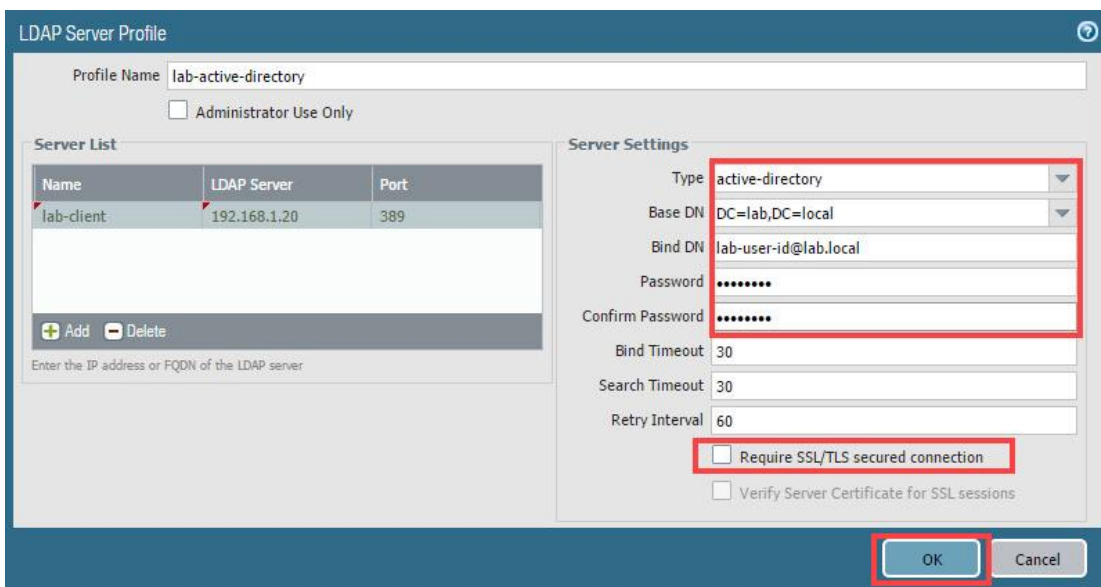
4. In the *LDAP Server Profile* window, locate the *Server List* on the left side, click **Add**, and configure the following.

Parameter	Value
Name	Type <code>lab-client</code>
LDAP Server	Type <code>192.168.1.20</code>
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 drop-down list
Base DN	Type <code>DC=lab,DC=local</code>
Bind DN	Type <code>lab-user-id@lab.local</code>
Password	Type <code>Pa10A1t0</code>
Confirm Password	Type <code>Pa10A1t0</code>

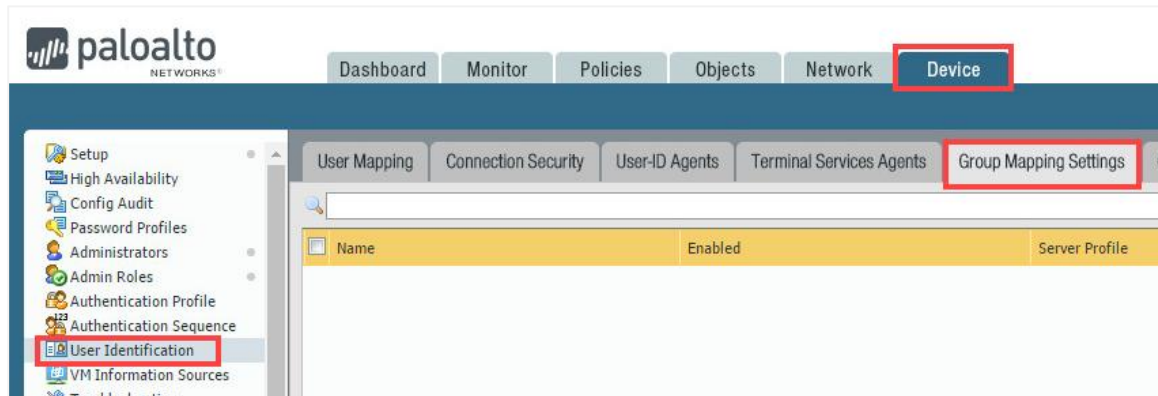


6. Leave the firewall web interface open to continue with the next task.

1.3 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**.

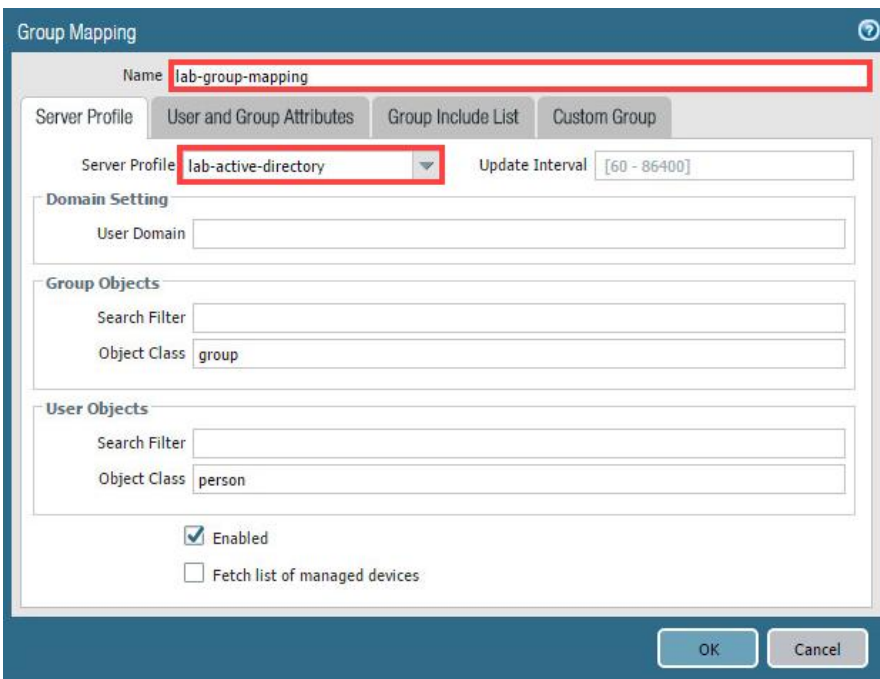


2. Click **Add** to open the *Group Mapping* configuration window.

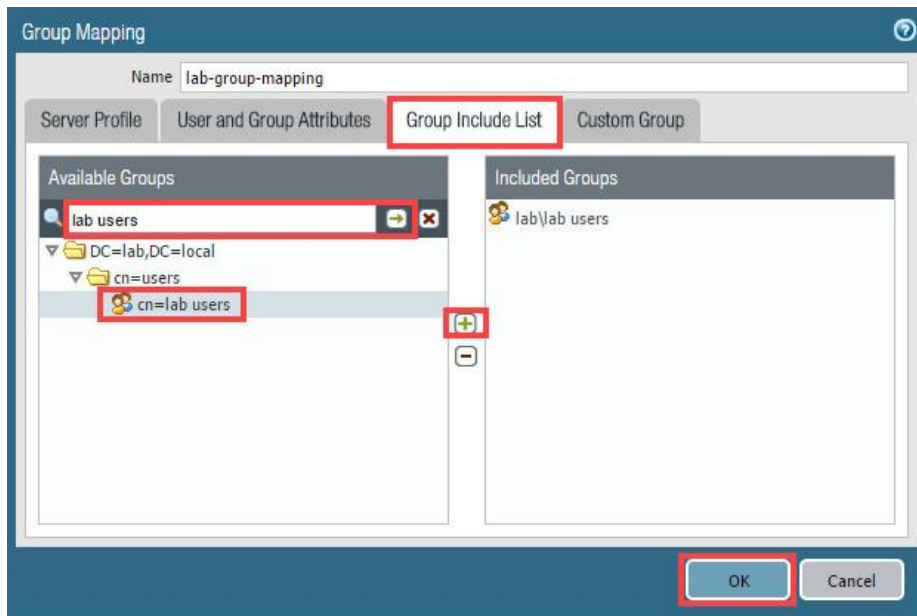


3. In the *Group Mapping* window, while on the *Server Profile* tab, configure the following.

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



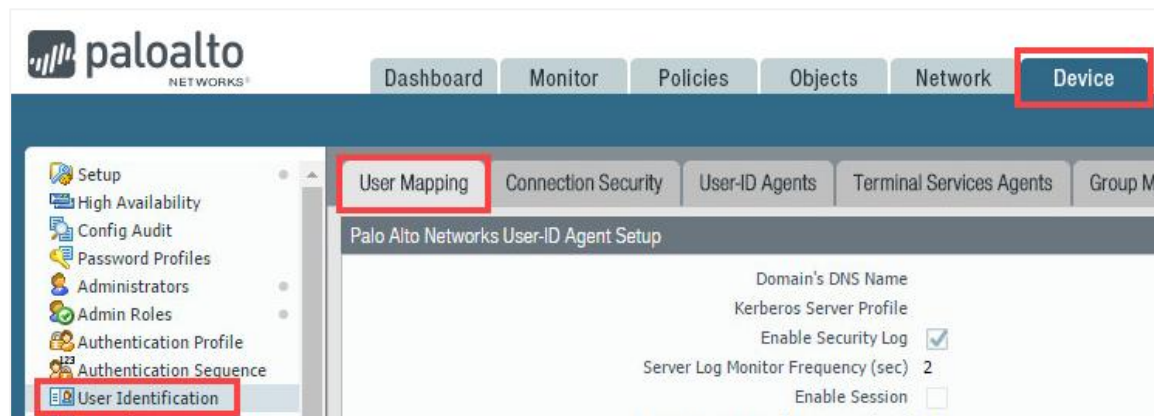
- In the *Group Mapping* window, click the **Group Include List** tab and type **lab users** into the search box, followed by pressing the **Enter** key. After running the search, select **cn=lab users** and then click the **plus** icon to add the selected to the Included Groups pane, then click **OK**.




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

1.4 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.

3. 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 Pa10A1t0



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: *****

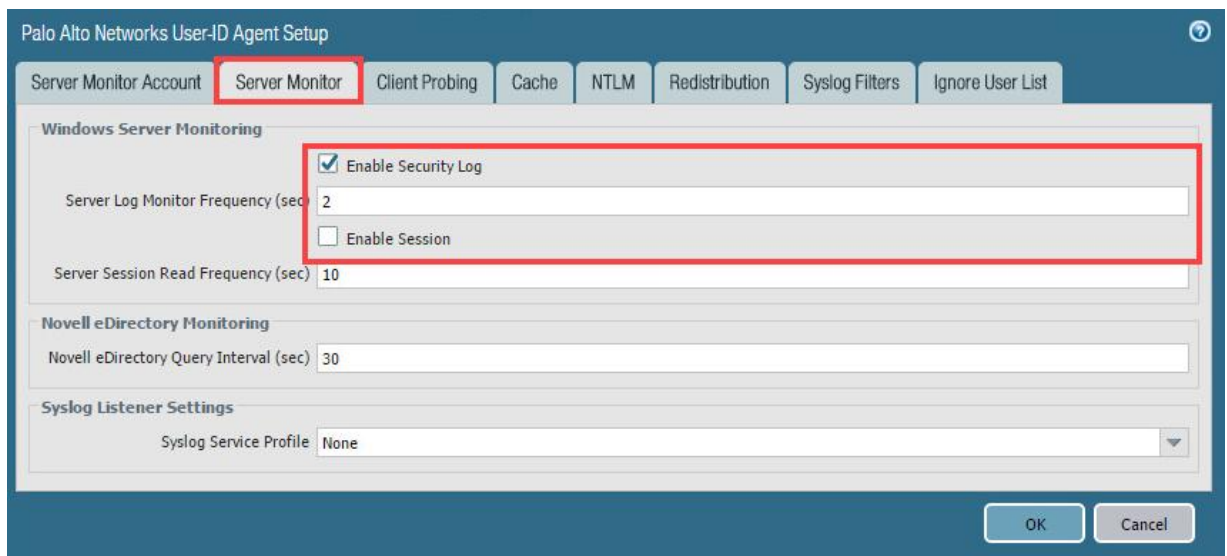
Confirm Password: *****

Kerberos Server Profile: None

OK Cancel

4. 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

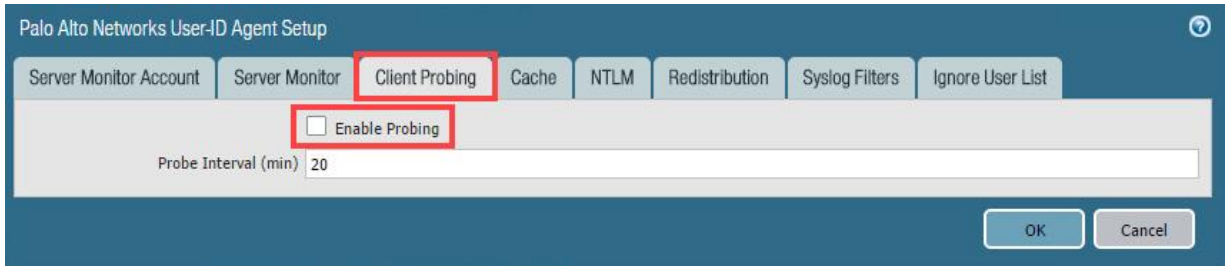
Novell eDirectory Query Interval (sec): 30

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.



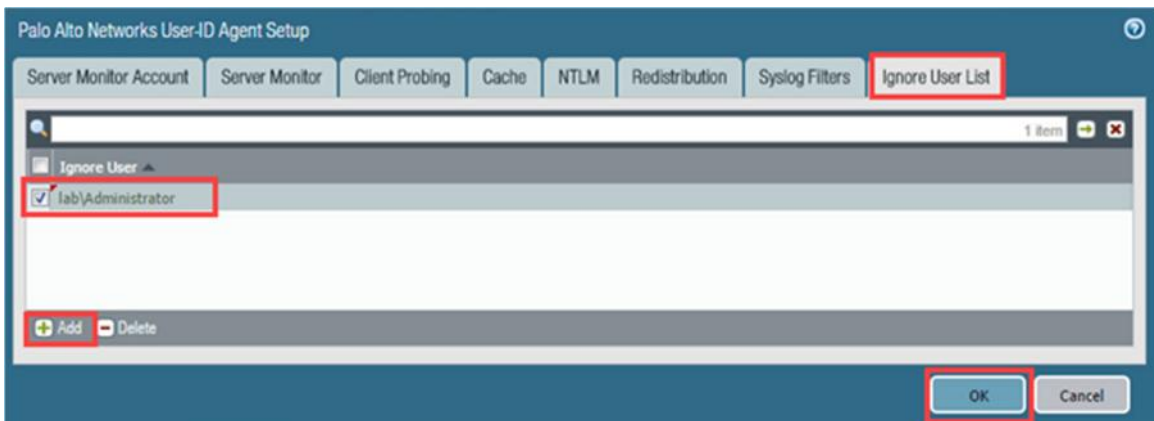
- In the *Palo Alto Networks User-ID Agent Setup* window, click the **Cache** tab and **uncheck** the **Enable User Identification Timeout** checkbox. Ensure that **45** is entered in the *User Identification Timeout (min)* text field.




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 <code>lab\Administrator</code>





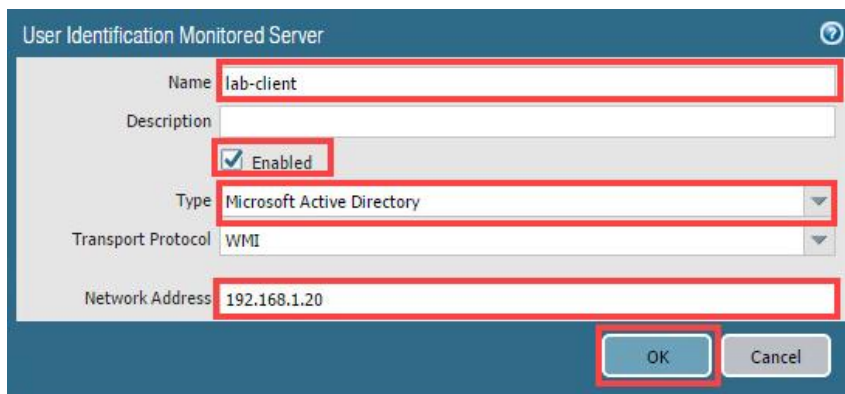
Addition of the Administrator to the Ignore User List prevents the firewall from assuming that Administrator is associated with 192.168.1.20.

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 and then click **OK**.

Parameter	Value
Name	Type lab-client
Enabled	Select the checkbox
Type	Verify that Microsoft Active Directory is selected
Network Address	Type 192.168.1.20



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

1.5 Verify the User-ID Configuration

- Under the *Server Monitoring* section, verify the status as *Connected*.


Server Monitoring				
<input type="checkbox"/> Name	Enabled	Type	Network Address ▲	Status
<input type="checkbox"/> lab-client	<input checked="" type="checkbox"/>	Microsoft Active Directory	192.168.1.20	Connected

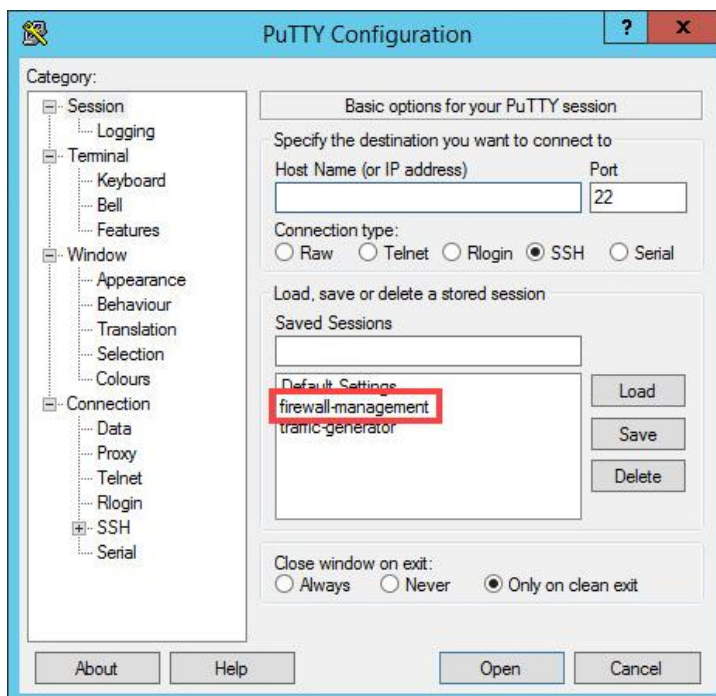
+ Add - Delete Discover

- On the Windows desktop, double-click the **lab**  folder.
- Double-click the **bat files**  folder.
- Double-click the **user-id.bat**  file.



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

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



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

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

Number of failed attempts since last successful login: 0

admin@firewall-a>
```

- 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: 2557 secs ago(took 0 secs)
                  Next Action Time: In 1043 secs
  Number of Groups: 1
  cn=lab users,cn=users,dc=lab,dc=local

admin@firewall-a>
```

- Enter the following command:

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

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

IP	Vsys	From	User	IdleTimeout(s)	MaxTimeout(s)
192.168.1.20	vsys1	AD	lab\lab-user	Never	Never
192.168.1.254	vsys1	AD	lab\lab-user-id	Never	Never
Total: 2 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.

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

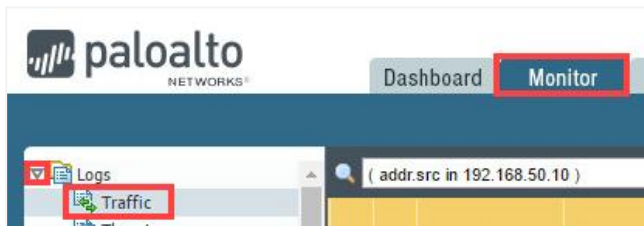
- Open a new **Internet Explorer** browser window in **private/incognito** mode and browse to **msn.com** and **google.com** to generate some traffic.



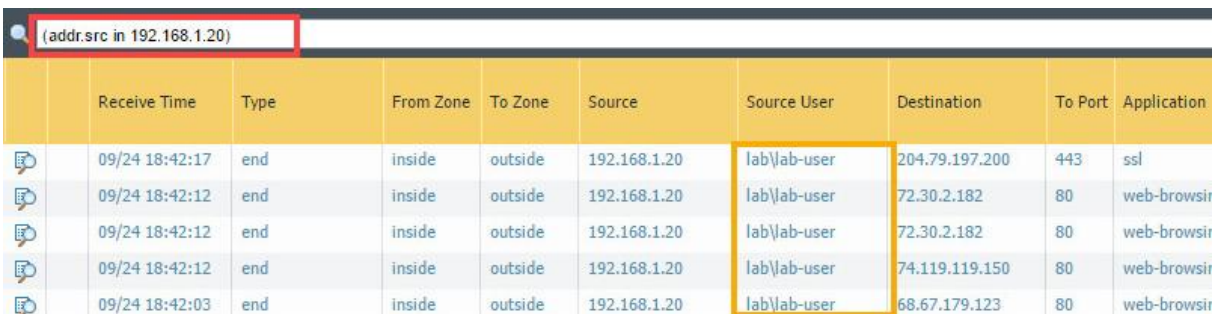
- Close the **IE** browser.

1.6 Review the Logs

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



- 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	To Port	Application
	09/24 18:42:17	end	inside	outside	192.168.1.20	lab\lab-user	204.79.197.200	443	ssl
	09/24 18:42:12	end	inside	outside	192.168.1.20	lab\lab-user	72.30.2.182	80	web-browsir
	09/24 18:42:12	end	inside	outside	192.168.1.20	lab\lab-user	72.30.2.182	80	web-browsir
	09/24 18:42:12	end	inside	outside	192.168.1.20	lab\lab-user	74.119.119.150	80	web-browsir
	09/24 18:42:03	end	inside	outside	192.168.1.20	lab\lab-user	68.67.179.123	80	web-browsir

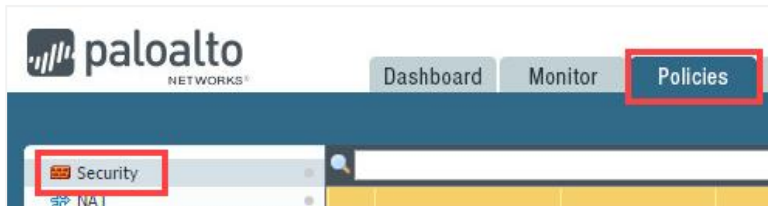


Notice that the *Source User* column now shows the *lab-user*. This user-id reference could take up to three minutes to show on the logs. Click **refresh** to update the log entries.

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

1.7 Create a Security Policy Rule

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

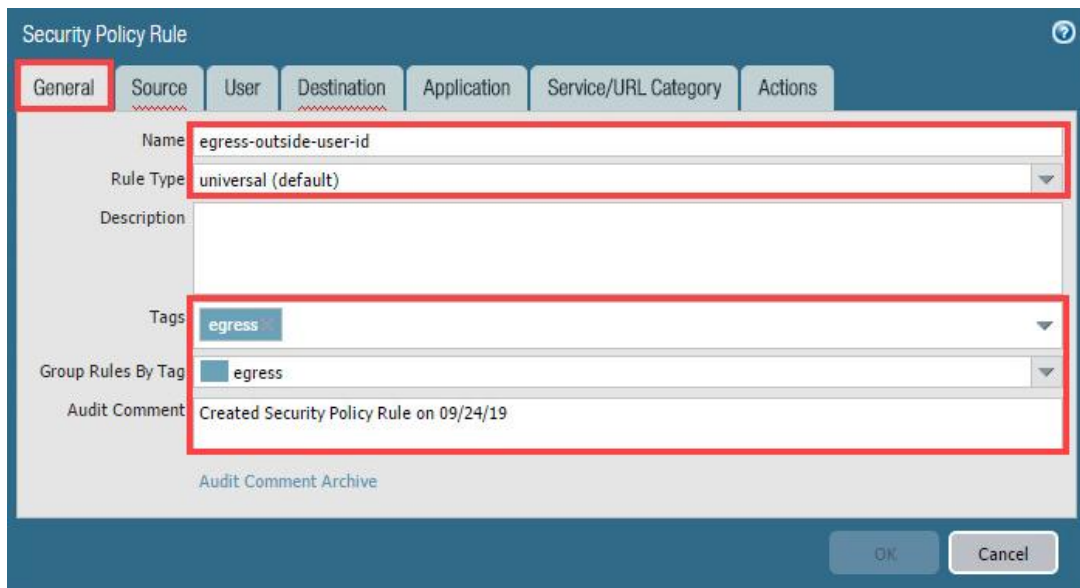


2. Click **Add** to open the *Security Policy Rule* configuration window.



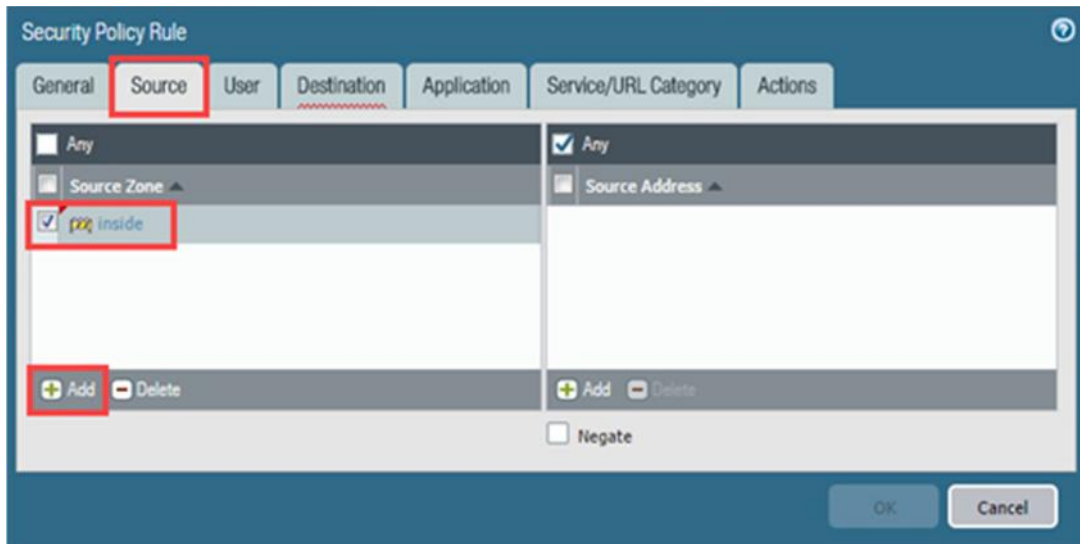
3. In the *Security Policy Rule* window, while on the *General* tab, configure the following:

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



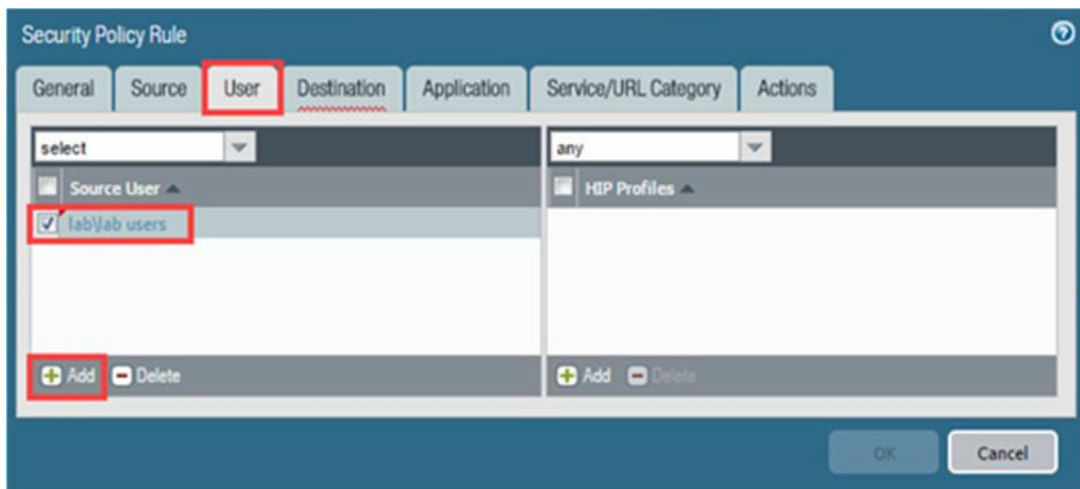
4. In the *Security Policy Rule* window, click the **Source** tab and configure the following.

Parameter	Value
Source Zone	Click Add and select inside from the drop-down list



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

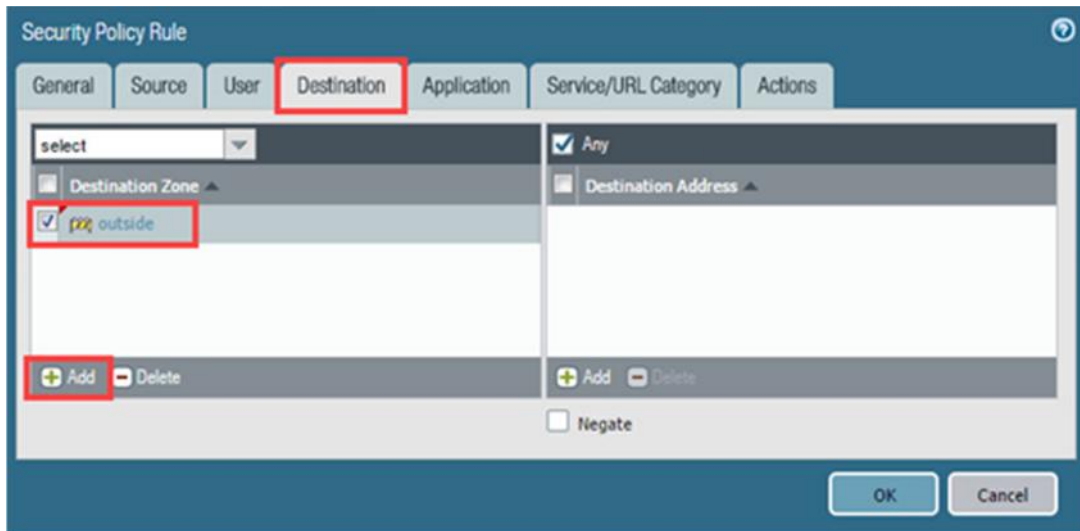
Parameter	Value
Source User	Click Add and select lab\lab users from the drop-down list



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

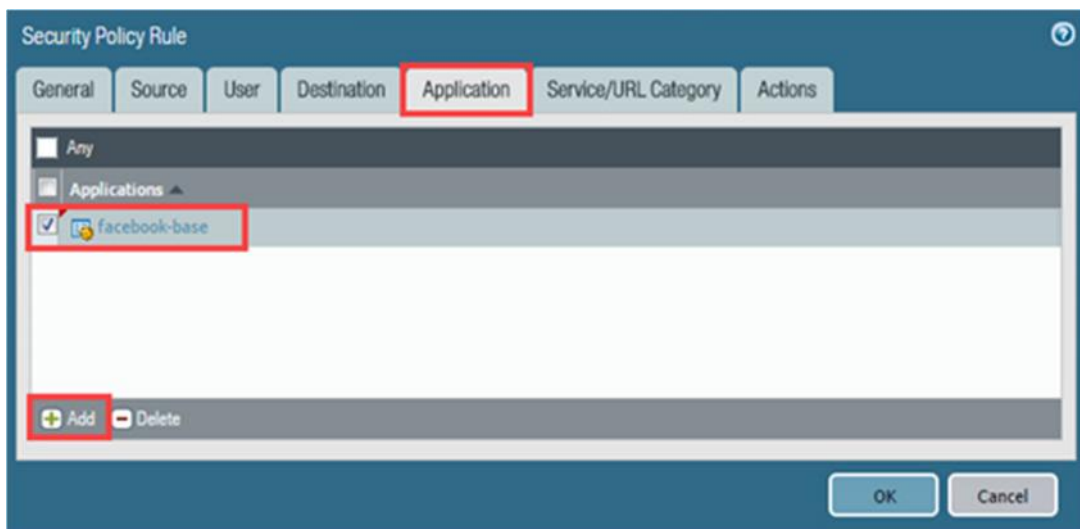
6. In the *Security Policy Rule* window, click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	Click Add and select outside from the drop-down list



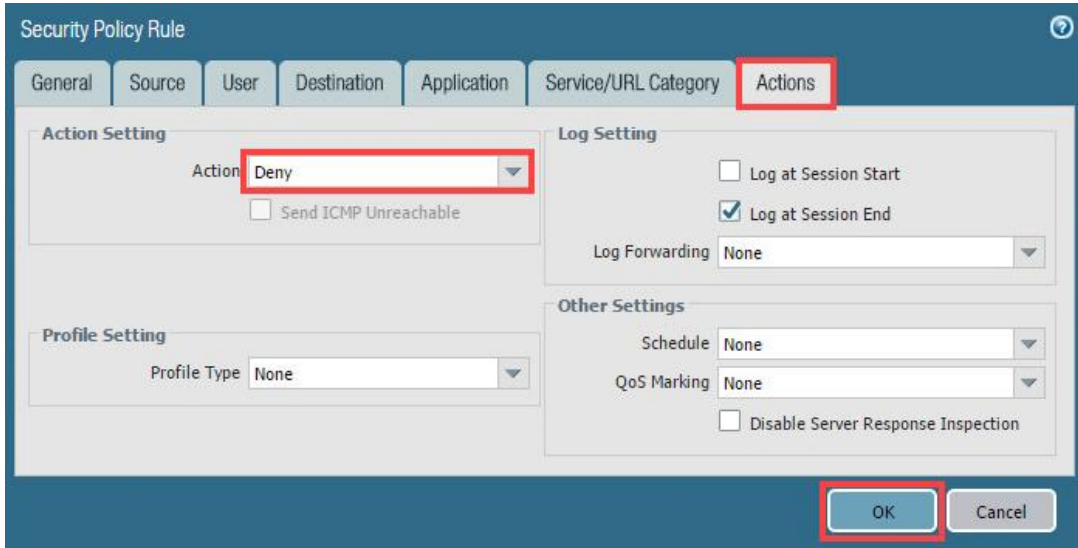
7. In the *Security Policy Rule* window, click the **Application** tab and configure the following:

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



Security Policy Rule

General Source User Destination Application Service/URL Category **Actions**

Action Setting

Action: **Deny**

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

OK Cancel

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.

	Name	Tags	Type	Zone	Address
1	internal-inside-dmz	internal	universal	inside	any
2	egress-outside	egress	universal	inside	any
3	egress-outside-content-id	egress	universal	inside	any
4	danger-simulated-traffic	none	universal	danger	any
5	egress-outside-user-id	egress	universal	inside	any
6	intrazone-default	none	intrazone	any	any
7	interzone-default	none	interzone	any	any

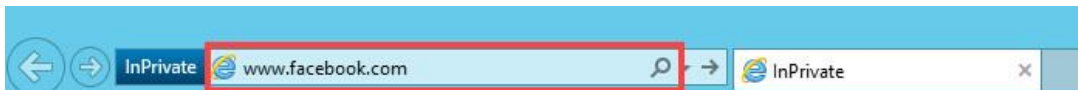
Move Top
Move Up
Move Down
Move Bottom

Add Delete Clone Override Revert Enable Disable Move PDF/CSV

10. **Commit** all changes.

1.8 Review Logs

1. Open a new **Internet Explorer** browser window in **private/incognito** mode 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 **IE** browser.

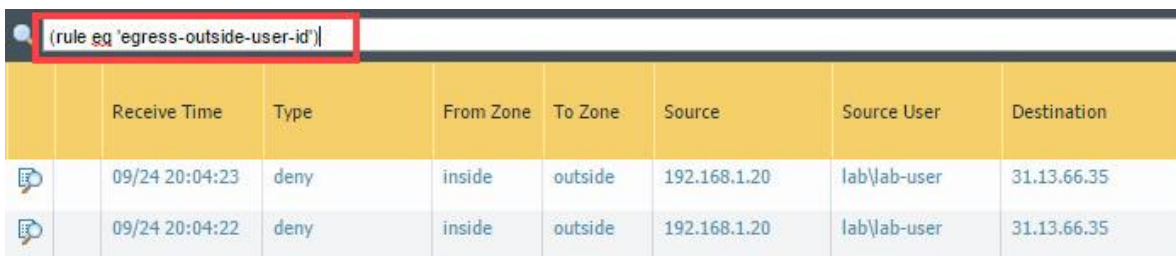
Application Blocked


Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: lab\lab-user

Application: facebook-base

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**.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
	09/24 20:04:23	deny	inside	outside	192.168.1.20	lab\lab-user	31.13.66.35
	09/24 20:04:22	deny	inside	outside	192.168.1.20	lab\lab-user	31.13.66.35



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.