PALO ALTO NETWORKS - EDU-210

Lab 9: User-ID

Document Version: 2017-09-29

Contents

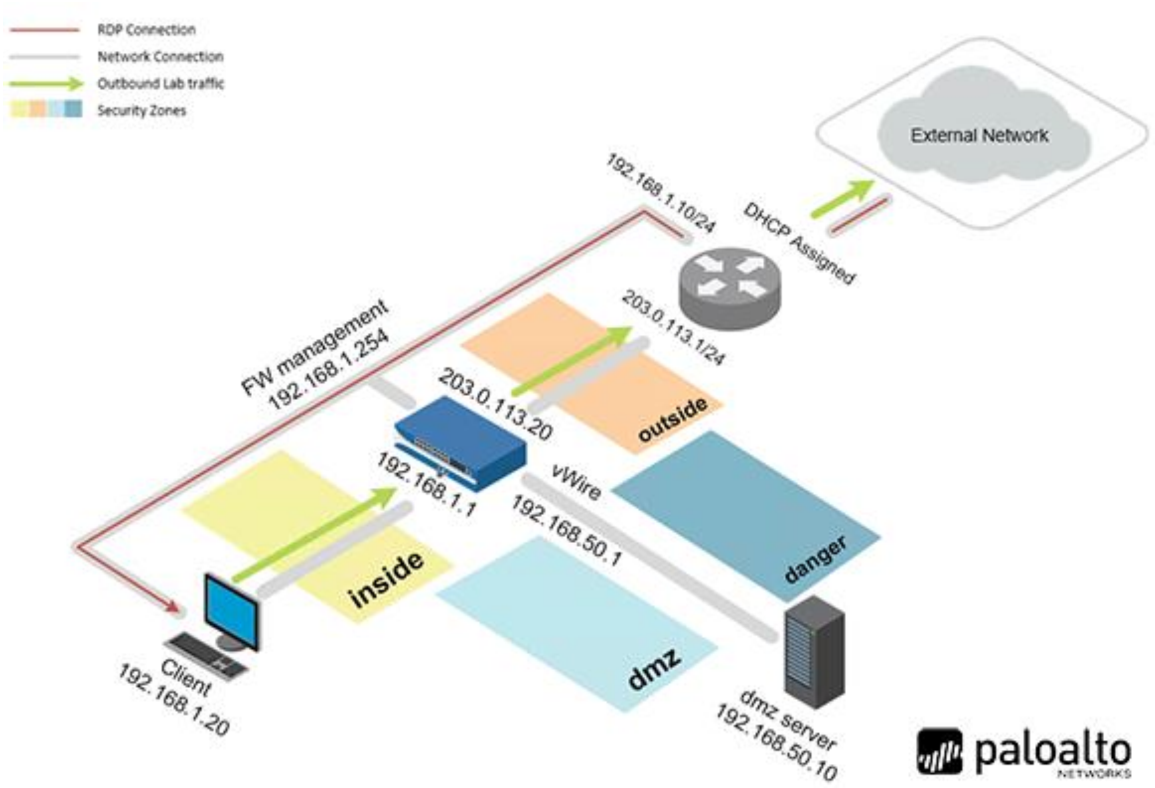
Introduction

Management would like to get reports on users for things like what 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 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



Lab Settings

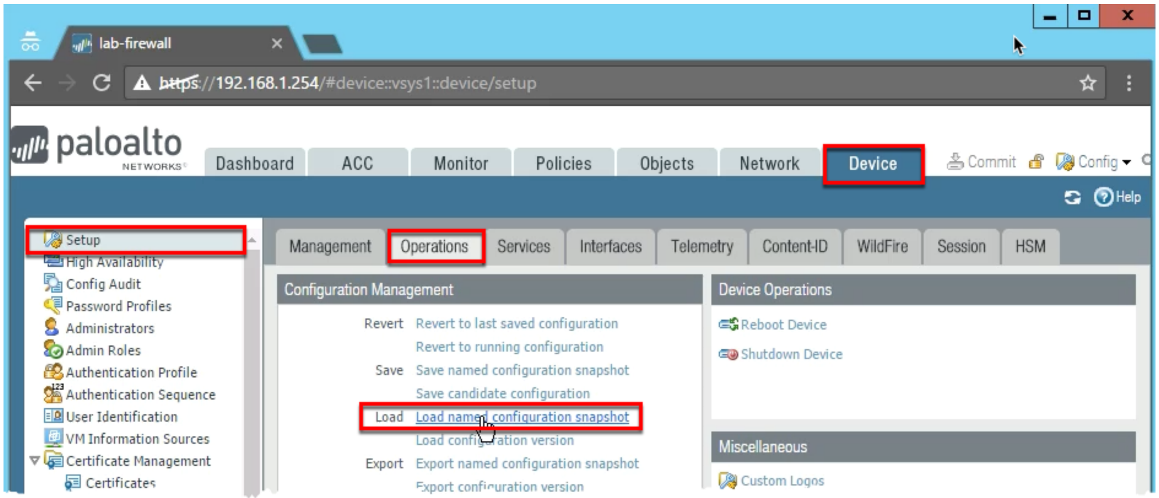
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client – Windows 2012 R2	192.168.1.20	lab-user	Pal0Alt0
Firewall – PA-VM	192.168.1.254	admin	admin

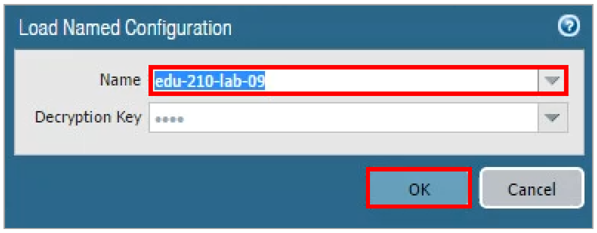
9 Lab: User-ID

9.0 Load Lab Configuration

1. In the WebUI select **Device > Setup > Operations**.
2. Click **Load named configuration snapshot**:



3. Select **edu-210-lab-09** and click **OK**.


Load Named Configuration

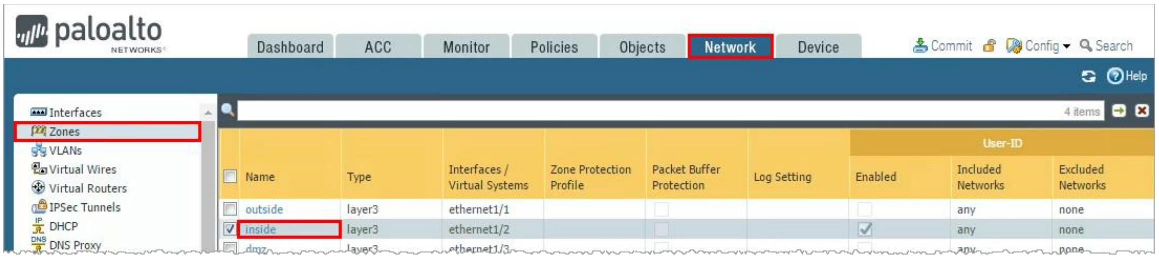
Name: edu-210-lab-09

Decryption Key: ••••

4. Click **Close**.
5. **Commit** all changes.

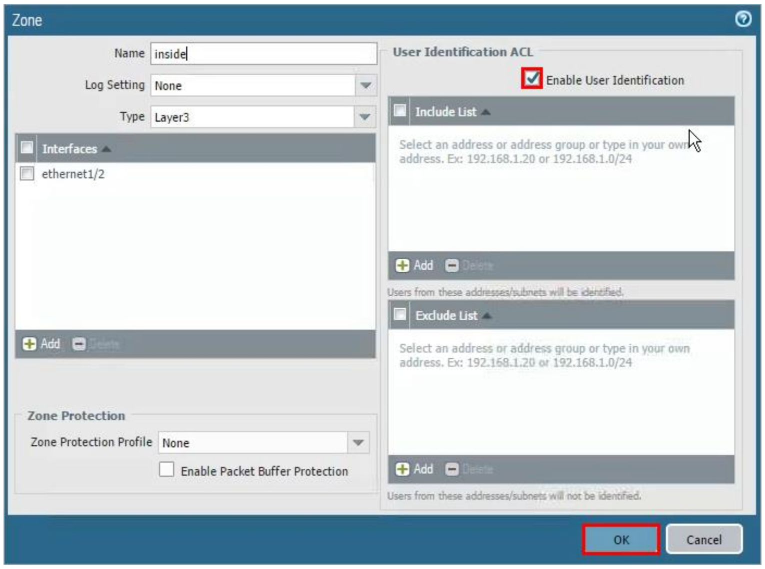
9.1 Enable User-ID on the Inside Zone

1. In the WebUI select **Network > Zones** then click **inside** to open the inside zone.



	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	User-ID Enabled	User-ID Included Networks	User-ID Excluded Networks
□	outside	layer3	ethernet1/1		□		□	any	none
☑	inside	layer3	ethernet1/2		□		☑	any	none
□	dmz	layer3	ethernet1/3		□		□	any	none

2. Enable User-ID by selecting the Enable User Identification check box:


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

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

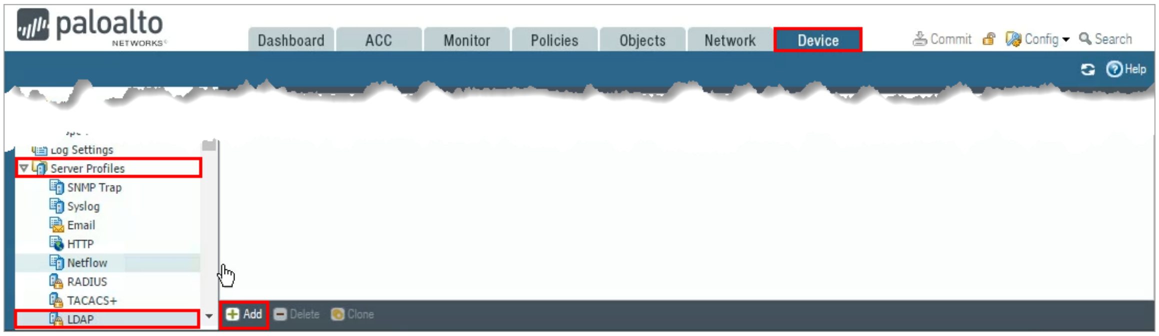
Users from these addresses/subnets will not be identified.

3. Click **OK**.

9.2 Configure the LDAP Server Profile

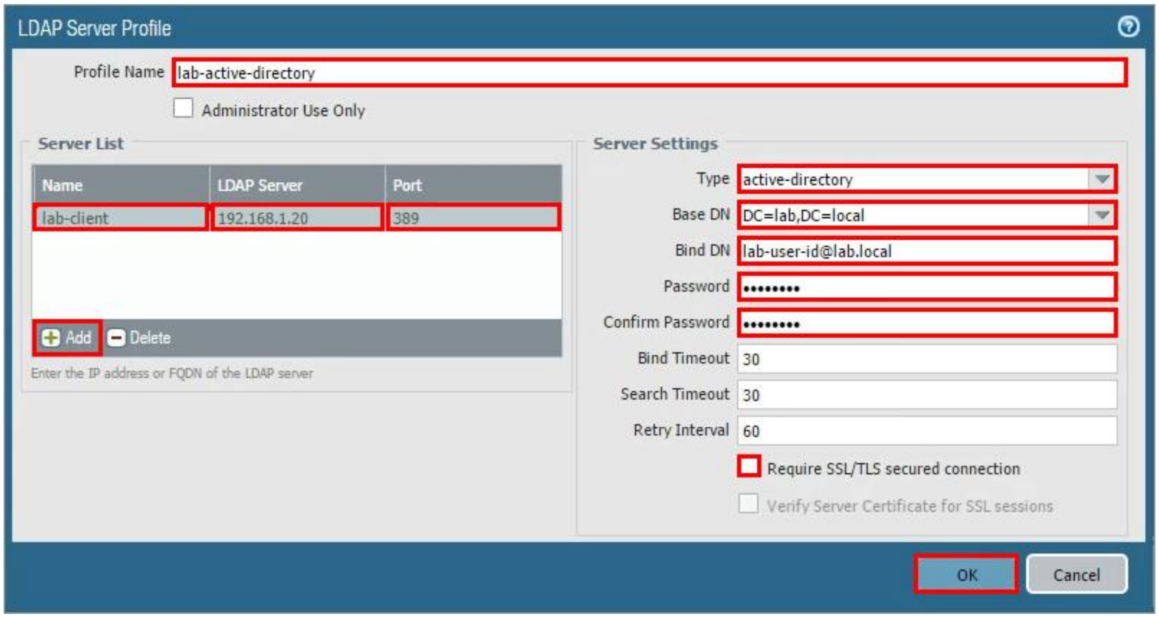
Create a Server profile so that the firewall can pull group and user information from Active Directory.

1. In the WebUI select **Device > Server Profiles > LDAP** then click **Add**.



2. Click **Add** and configure the following on the **LDAP Server Profile** window then click **OK**.

Parameter	**Value**
Profile Name	`lab-active-directory`
Server List	
Name	`lab-client`
LDAP Server	`192.168.1.20`
Port	`389`
Server Settings	
Require SSL/TLS secured connection (*make sure to do this first*)	`DESELECT the checkbox`
Type	`active-directory`
Base DN	`DC=lab,DC=local`
Bind DN	`lab-user-id@lab.local`
Password	`Pal0Alt0`



LDAP Server Profile

Profile Name: lab-active-directory

□ Administrator Use Only

Server List

Name	LDAP Server	Port
lab-client	192.168.1.20	389

Enter the IP address or FQDN of the LDAP server

Server Settings

Type: active-directory

Base DN: DC=lab,DC=local

Bind DN: lab-user-id@lab.local

Password: ••••••••

Confirm Password: ••••••••

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

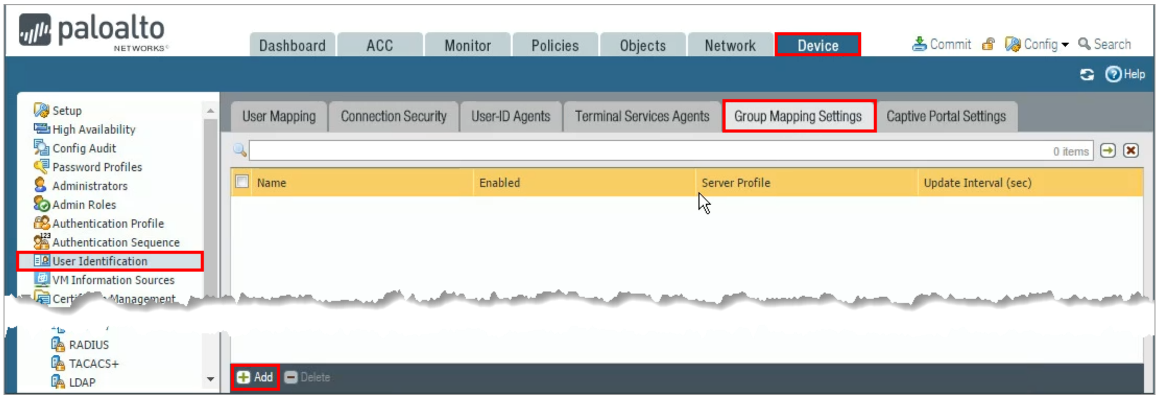
□ Require SSL/TLS secured connection

□ Verify Server Certificate for SSL sessions

9.3 Configure User-ID Group Mapping

Define which users and groups will be available when creating policy rules.

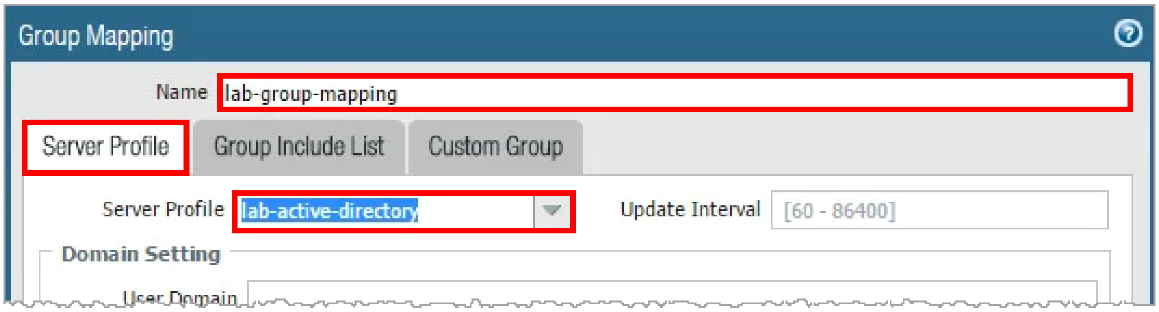
1. In the WebUI select **Device > User Identification > Group Mapping Settings** click **Add** to open the Group Mapping configuration window.



2. Configure the following:

Parameter	Value
Name	`lab-group-mapping`
Server Profile *(Tab)*	

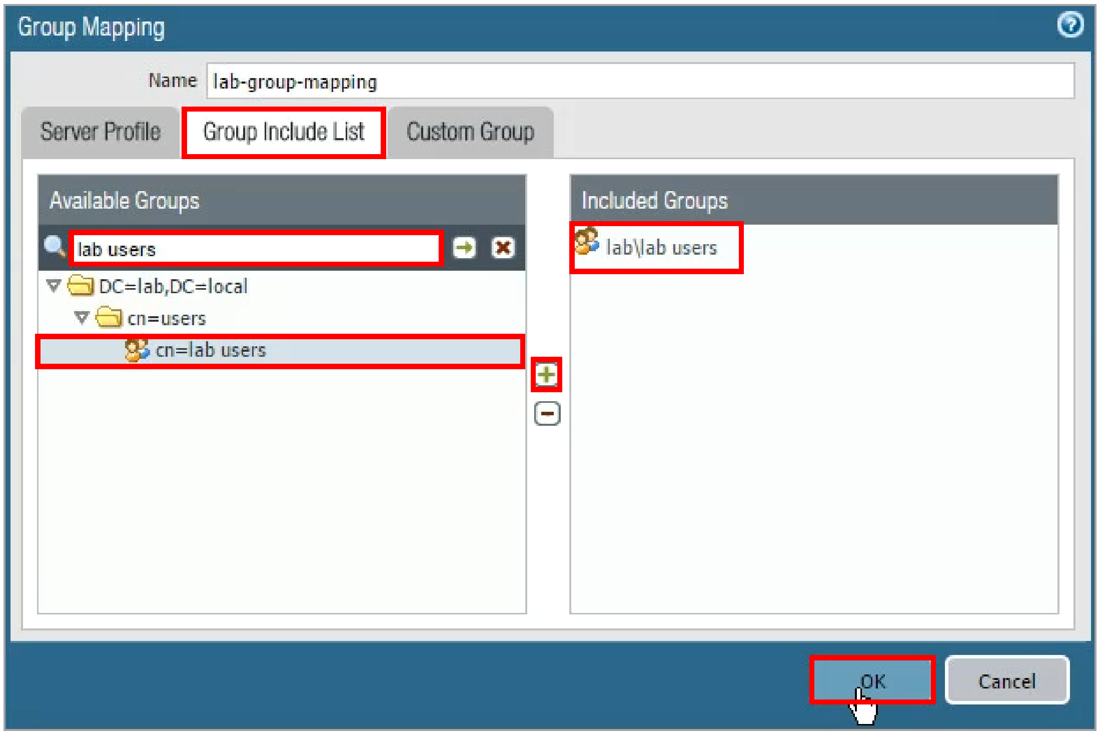
Server Profile	**`lab-active-directory`**
	`(all other fields will auto-populate)`



3. Click the **Group Include List** tab and configure the following:

Parameter	Value
Search Box	`lab users`

After running the search, select **`cn=lab users`** then click the **plus** icon to add the selected to the Included Groups, then click **OK**.

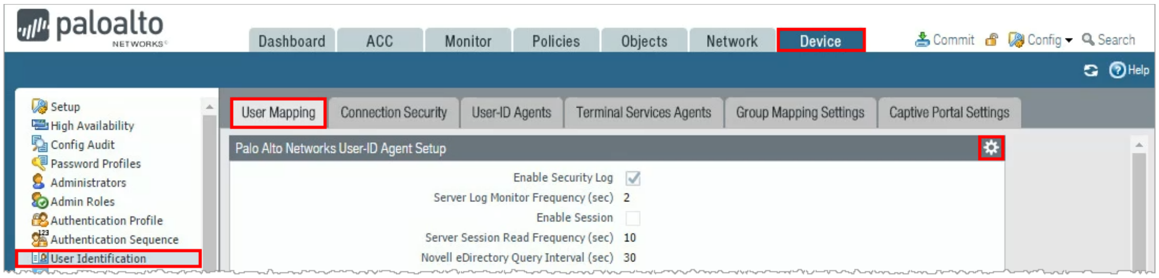


Group Mapping

Name lab-group-mapping

9.4 Configure Integrated Firewall Agent

1. Select **Device > User Identification > User Mapping** then click the **Gear** icon in the top-right of the Palo Alto Networks User-ID Agent Setup pane.

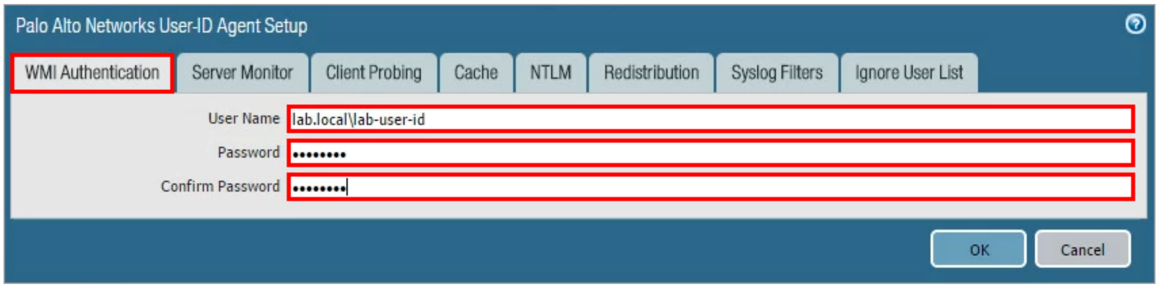


Palo Alto Networks User-ID Agent Setup

Enable Security Log	☑
Server Log Monitor Frequency (sec)	2
Enable Session	☐
Server Session Read Frequency (sec)	10
Novell eDirectory Query Interval (sec)	30

2. Configure the following:

Parameter	Value
User Name	`lab.local\lab-user-id`
Password	`Pal0Alt0`

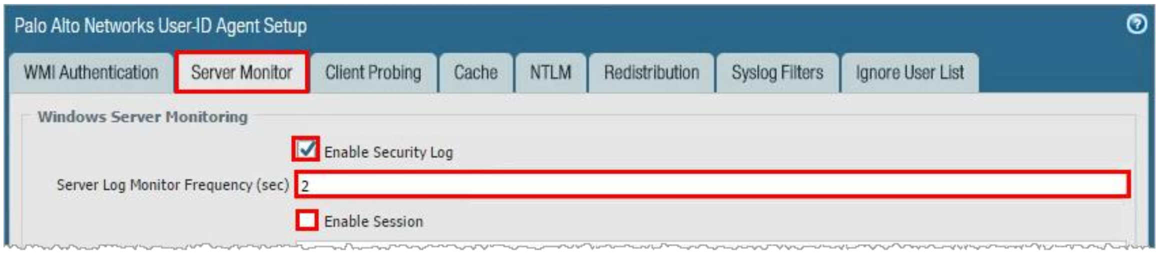


Palo Alto Networks User-ID Agent Setup

User Name	lab.local\lab-user-id
Password	••••••••
Confirm Password	••••••••

3. 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

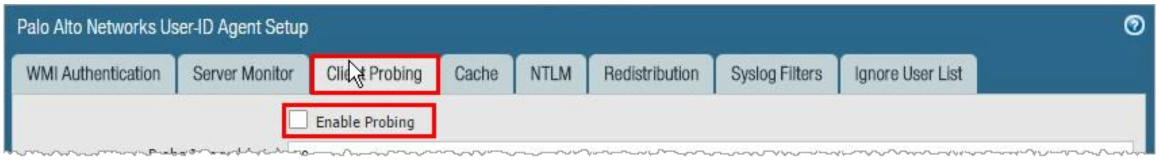
Windows Server Monitoring

☑ Enable Security Log

Server Log Monitor Frequency (sec) 2

☐ Enable Session

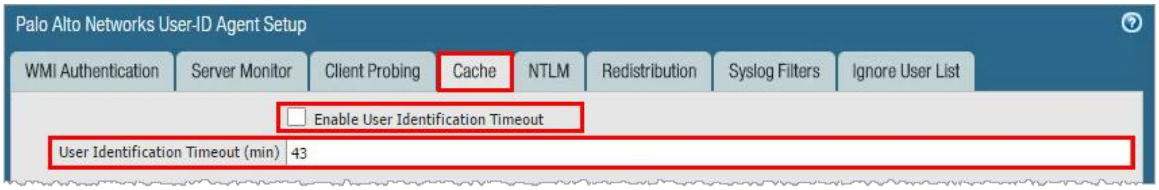
4. Click the **Client Probing** tab and verify that the **Enable Probing** check box is deselected.



☐ Enable Probing

5. Click the **Cache** tab and configure the following:

Parameter	Value
Enable User Identification Timeout	`Unchecked`
User Identification Timeout (min)	`43`



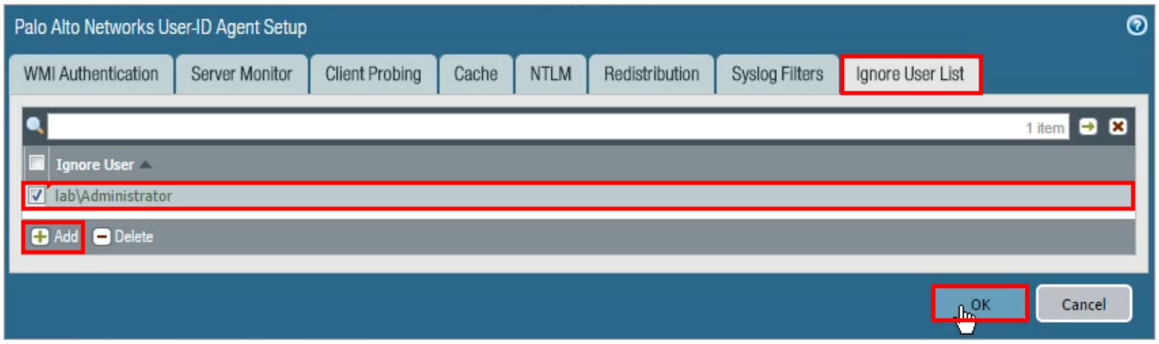
☐ Enable User Identification Timeout

User Identification Timeout (min) 43

6. Click the **Ignore User List** tab then click **Add** and configure the following:

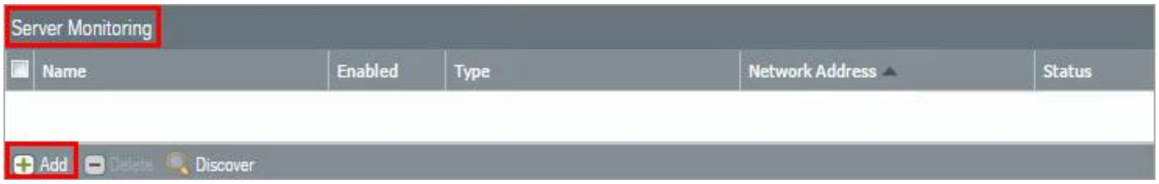
Parameter	Value

Ignore User	`lab\Administrator`
	`Prevents the firewall from assuming that Administrator is associated with 192.168.1.20`



☐	Ignore User
☑	lab\Administrator

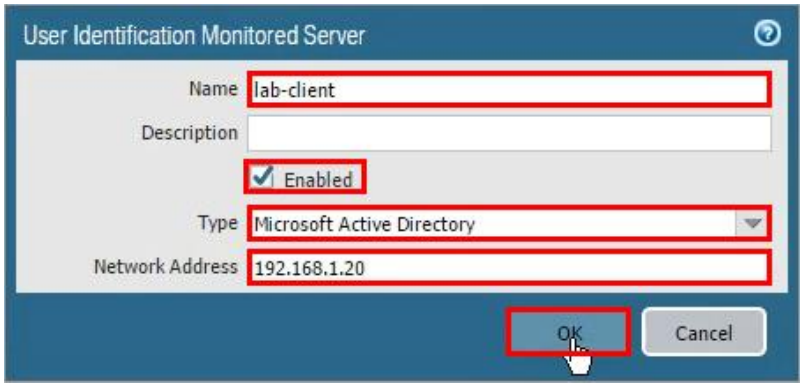
7. Click **OK**.
8. Scroll down to the **Server Monitoring** pane then click **Add**.



☐	Name	Enabled	Type	Network Address	Status

9. Configure the parameters in the following table then click **OK**.

Parameter	Value
Name	`lab-client`
Enabled	`Checked`
Type	**`Microsoft Active Directory`**
Network Address	`192.168.1.20`



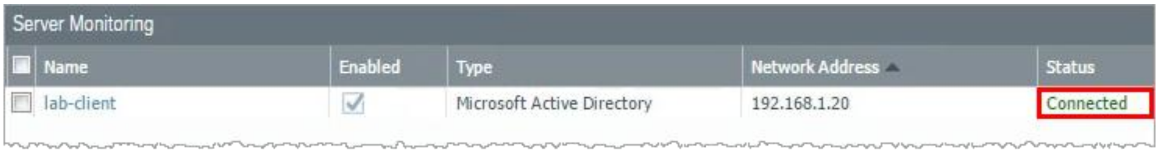
User Identification Monitored Server

Name	lab-client
Description	
	☑ Enabled
Type	Microsoft Active Directory
Network Address	192.168.1.20

10. **Commit** all changes.

9.5 Verify User-ID Configuration

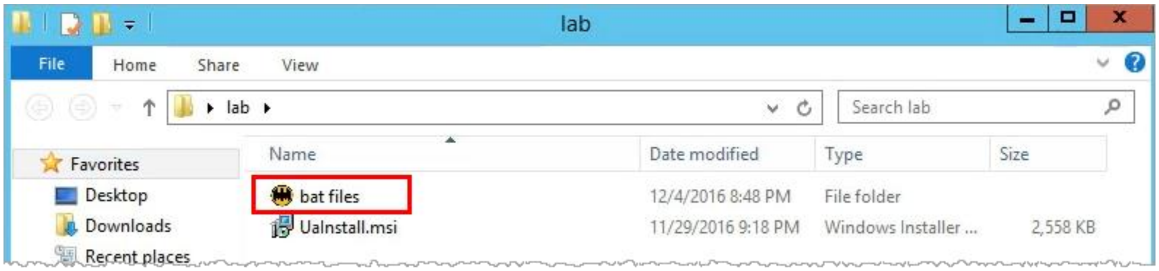
1. Under the **Server Monitoring** section, verify the status as **Connected.**



Server Monitoring

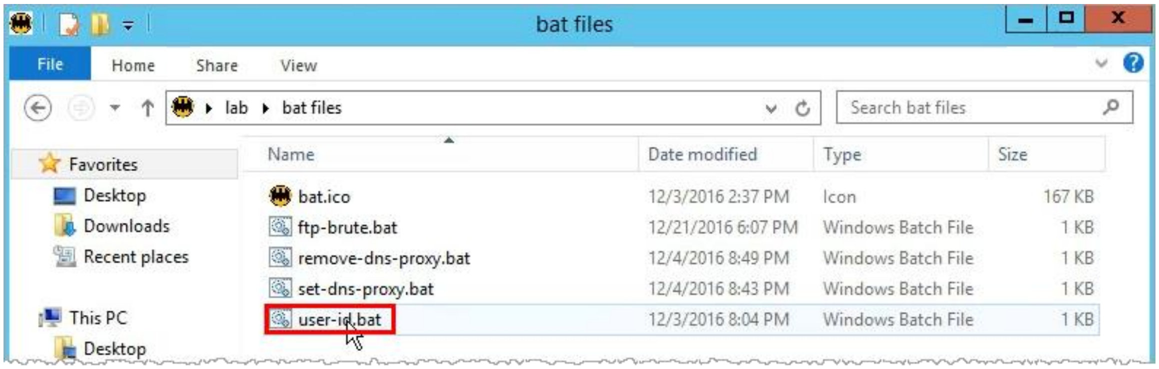
☐	Name	Enabled	Type	Network Address ▲	Status
☐	lab-client	✓	Microsoft Active Directory	192.168.1.20	Connected

2. On the Windows desktop, double-click the **lab** folder and then double-click the **bat files** folder.



Name	Date modified	Type	Size
bat files	12/4/2016 8:48 PM	File folder	
UaInstall.msi	11/29/2016 9:18 PM	Windows Installer ...	2,558 KB

3. Double-click the **user-id.bat** file.

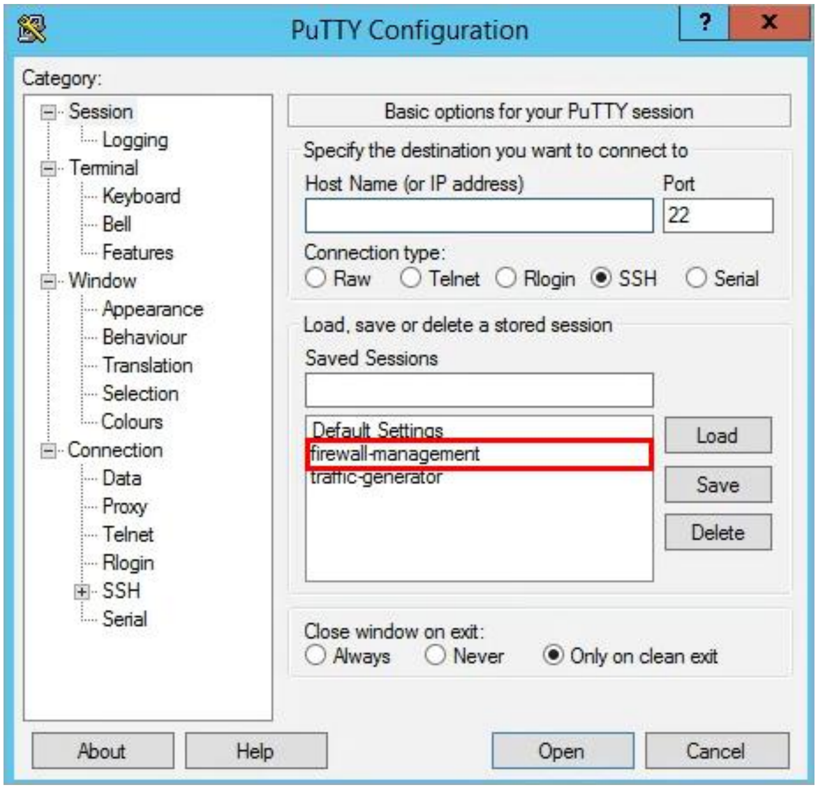


Name	Date modified	Type	Size
bat.ico	12/3/2016 2:37 PM	Icon	167 KB
ftp-brute.bat	12/21/2016 6:07 PM	Windows Batch File	1 KB
remove-dns-proxy.bat	12/4/2016 8:49 PM	Windows Batch File	1 KB
set-dns-proxy.bat	12/4/2016 8:43 PM	Windows Batch File	1 KB
user-id.bat	12/3/2016 8:04 PM	Windows Batch File	1 KB

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

4. On the Windows desktop, double-click the **PuTTY** icon.

5. Double-click firewall-management:



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

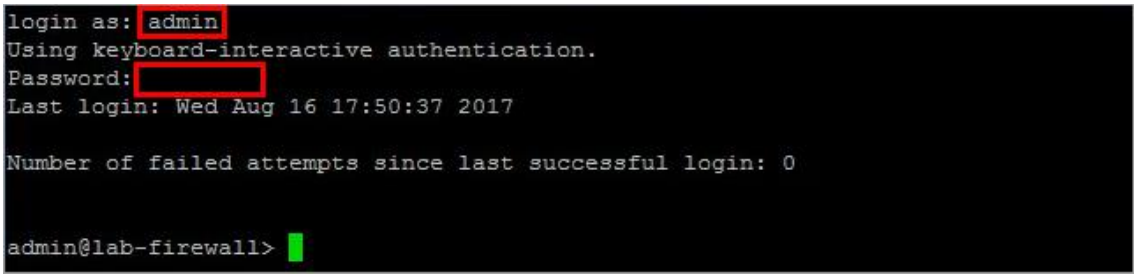
Load, save or delete a stored session

Saved Sessions

Default Settings
firewall-management
traffic-generator

Close window on exit:
○ Always ○ Never ● Only on clean exit

6. Log in to the firewall with the username `admin` and password `admin`.

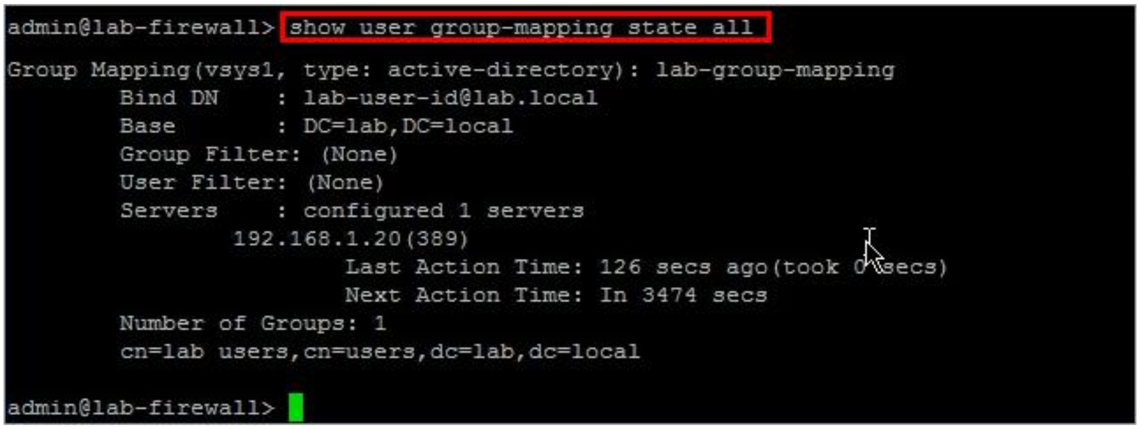


```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 16 17:50:37 2017

Number of failed attempts since last successful login: 0

admin@lab-firewall>
```

7. Type the following CLI command:

```
show user group-mapping state all.
```

The output should be similar to the following:

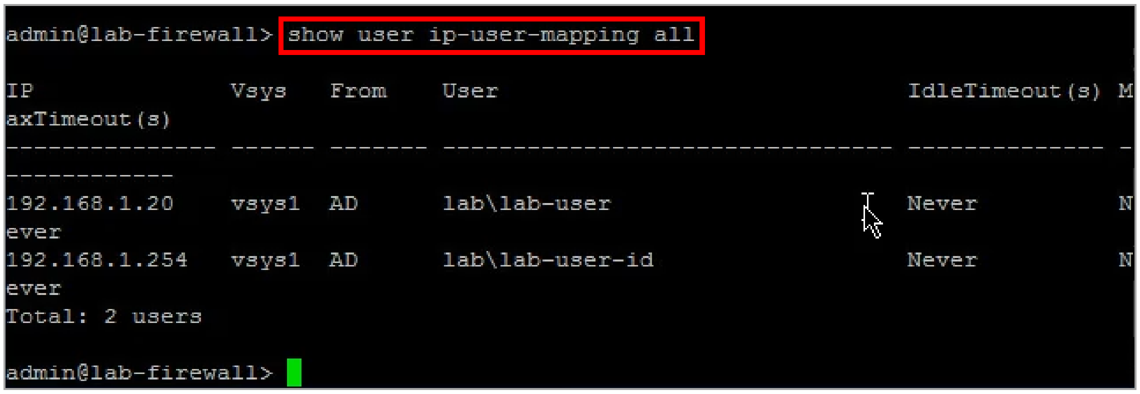


```
admin@lab-firewall> show user group-mapping state all

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: 126 secs ago(took 0 secs)
                        Next Action Time: In 3474 secs
        Number of Groups: 1
        cn=lab users,cn=users,dc=lab,dc=local

admin@lab-firewall>
```

8. Type the following CLI command:

```
show user ip-user-mapping all.
```

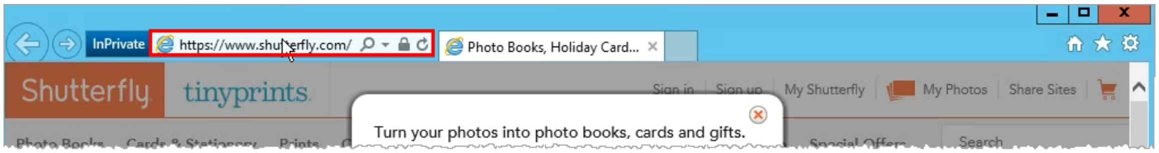
The output should be similar to the following:



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

IP              Vsys   From    User                             IdleTimeout(s) M
axTimeout(s)
--------------- ------ ------- -------------------------------- -------------- -
------------
192.168.1.20    vsys1  AD      lab\lab-user                     Never          N
ever
192.168.1.254   vsys1  AD      lab\lab-user-id                  Never          N
ever
Total: 2 users

admin@lab-firewall>
```

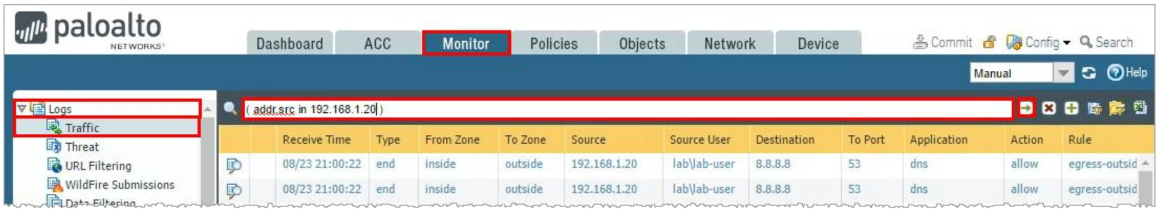
Note: lab\lab-user must have the IP address of 192.168.1.20. If that IP address is not listed, do not proceed. Contact your instructor or lab partner for assistance.

9. Open a **browser** and browse to **`shutterfly.com`** and **`google.com`** in order to generate some traffic.



9.6 Review Logs

1. Select **Monitor > Logs > Traffic** then type the filter **`(addr.src in 192.168.1.20`**) in the filter text box and depress **Enter**.



(addr.src in 192.168.1.20)

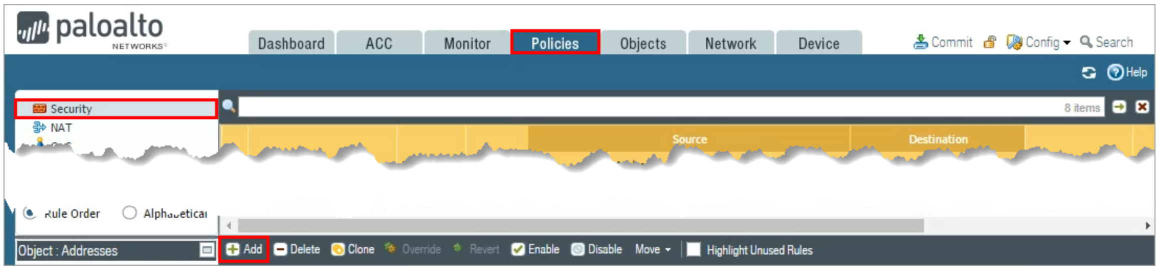
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
08/23 21:00:22	end	inside	outside	192.168.1.20	lab\lab-user	8.8.8.8	53	dns	allow	egress-outsid
08/23 21:00:22	end	inside	outside	192.168.1.20	lab\lab-user	8.8.8.8	53	dns	allow	egress-outsid

Notice that the Source User column now shows the lab-user.

Note: This user-id references could take up to **three** minutes. Click the **refresh** icon to update the log entries.

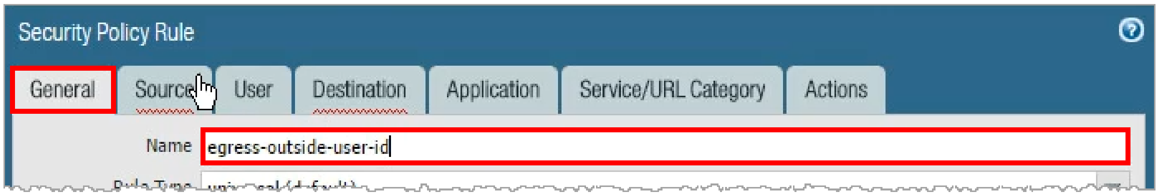
9.7 Create Security Policy Rule

1. Select **Policies > Security** then click **Add** to open the Security Policy Rule configuration window.



2. Under the **General** tab configure the following:

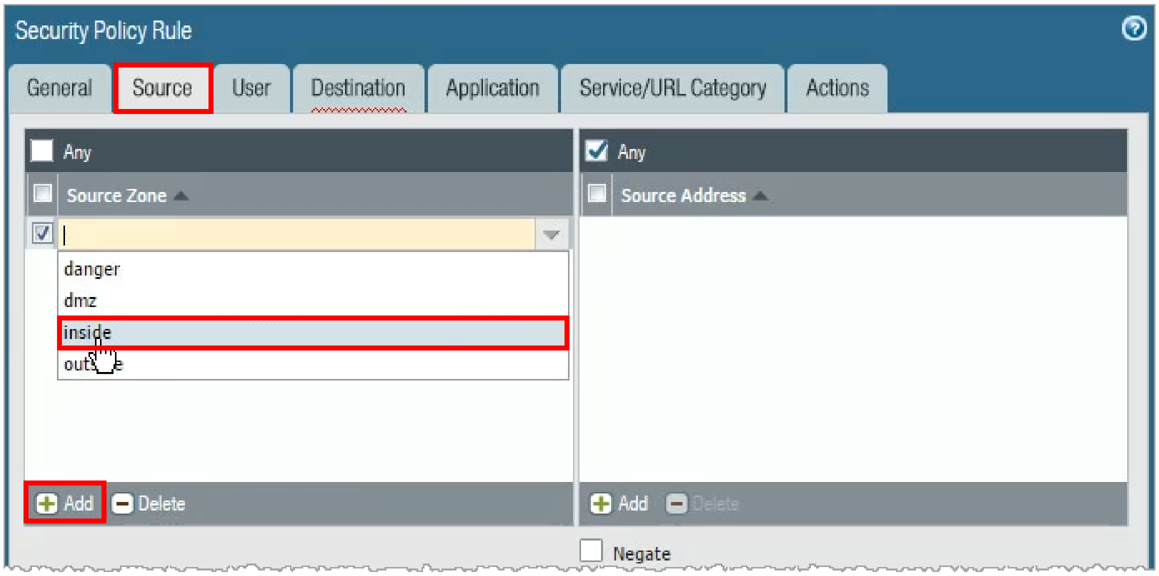
Parameter	Value
Name	`egress-outside-user-id`



Name: egress-outside-user-id

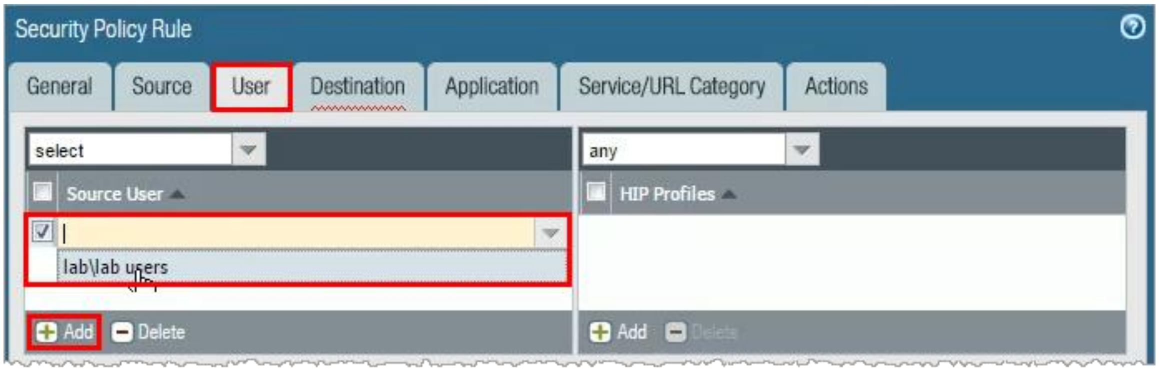
3. Click the **Source** tab and configure the following:

Parameter	Value
Source Zone	☑ inside



4. Click the **User** tab and configure the following:

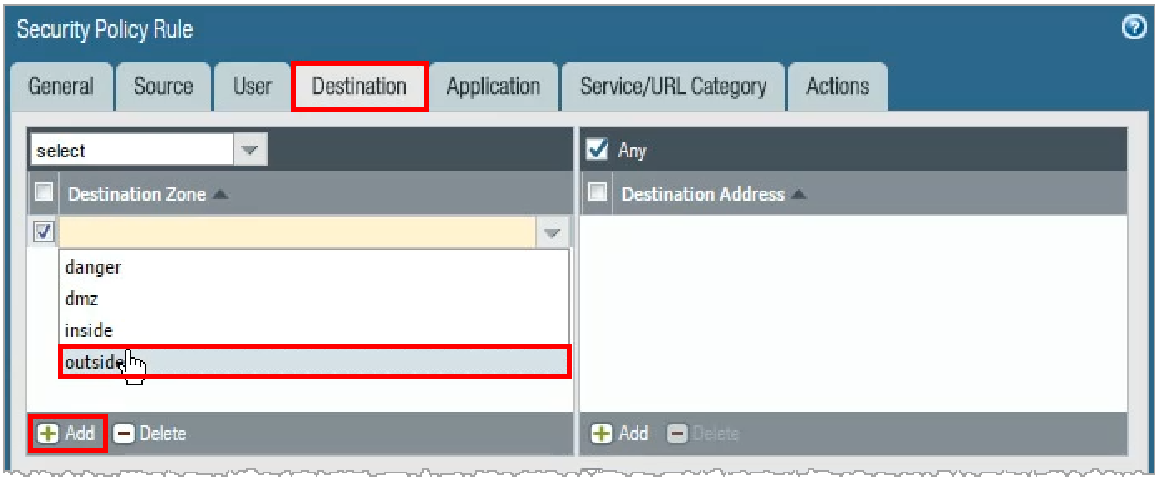
Parameter	Value
Source User	☑ lab\lab-user



You must start typing before usernames become available on the drop-down list.

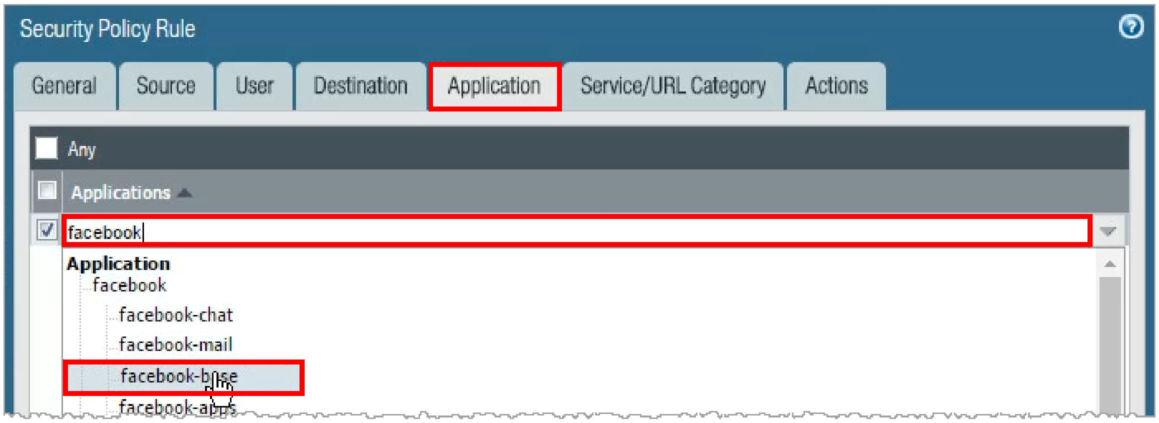
5. Click the **Destination** tab and configure the following:

Parameter	Value
Destination Zone	☑ outside



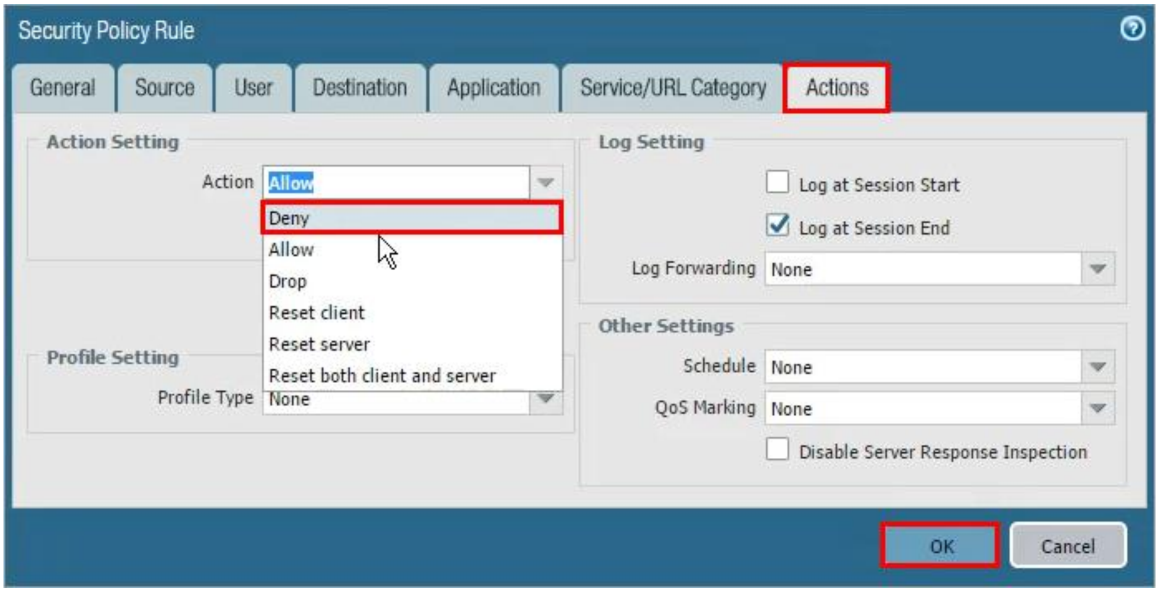
6. Click the **Application** tab and configure the following:

Parameter	Value
Applications	`facebook-base`



7. Click the **Actions** tab and configure the following then click **OK** to close the window.

Parameter	Value
Action	**`Deny`**



Action Setting

Action: Allow

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

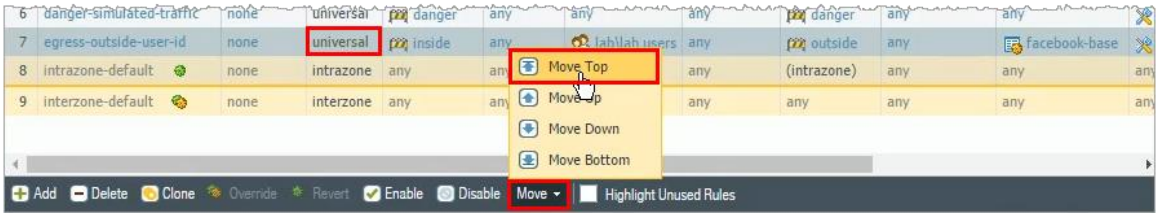
Other Settings

Schedule: None

QoS Marking: None

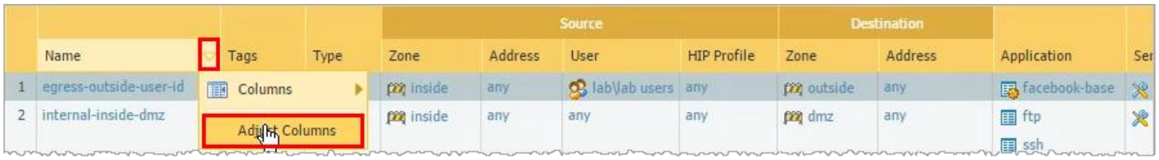
□ Disable Server Response Inspection

8. Select but do not open the **egress-outside-user-id** Security policy rule. Then click **Move** and select **Move Top** to move the rule to the top of the list.



6	danger-simulated-traffic	none	universal	danger	any	any	any	danger	any	any
7	egress-outside-user-id	none	universal	inside	any	lab\lab users	any	outside	any	facebook-base
8	intrazone-default	none	intrazone	any	any		any	(intrazone)	any	any
9	interzone-default	none	interzone	any	any		any	any	any	any

9. You may need to adjust the columns. Click the drop arrow by **Name** and select **Adjust Columns**.



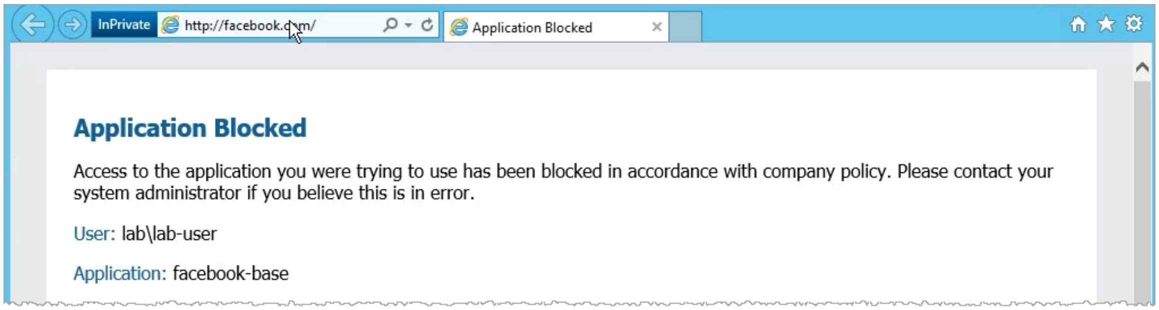
				Source				Destination			
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Ser
1	egress-outside-user-id			inside	any	lab\lab users	any	outside	any	facebook-base	
2	internal-inside-dmz			inside	any	any	any	dmz	any	ftp ssh	

10. **Commit** all changes.

9.8 Review Logs

1. Open a new browser in private/incognito mode and browse to www.facebook.com.

   The connection is denied based on the egress-outside-user-id Security policy rule:



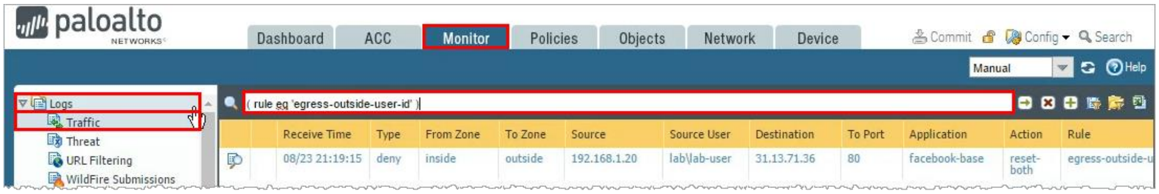
Application Blocked

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

2. Select **Monitor > Logs > Traffic**.
3. Type the filter (`rule eq 'egress-outside-user-id')` in the filter text box.



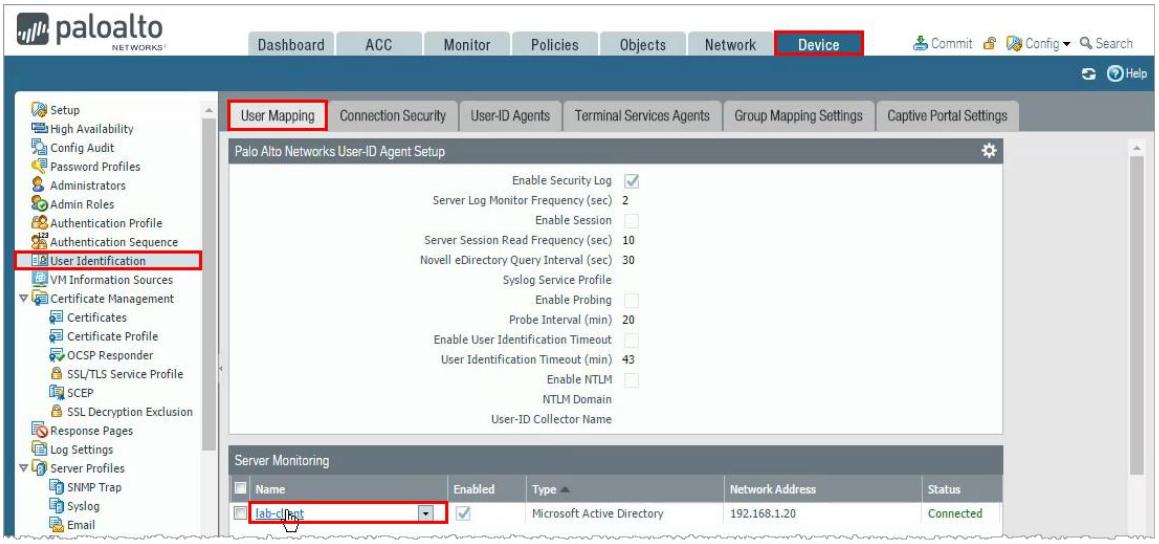
```
( rule eq 'egress-outside-user-id' )
```

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	08/23 21:19:15	deny	inside	outside	192.168.1.20	lab\lab-user	31.13.71.36	80	facebook-base	reset-both	egress-outside-u

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

9.9 Disable Integrated Firewall Agent

1. Select **Device > User Identification > User Mapping** then click the **lab-client** item under **Server Monitoring**.



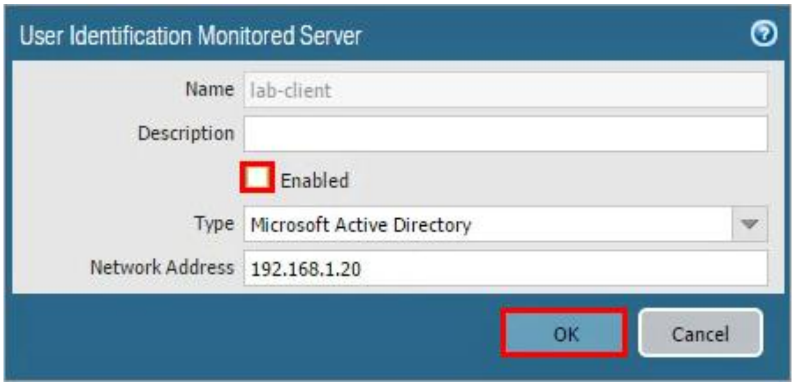
Palo Alto Networks User-ID Agent Setup

Enable Security Log	☑
Server Log Monitor Frequency (sec)	2
Enable Session	☐
Server Session Read Frequency (sec)	10
Novell eDirectory Query Interval (sec)	30
Syslog Service Profile	
Enable Probing	☐
Probe Interval (min)	20
Enable User Identification Timeout	☐
User Identification Timeout (min)	43
Enable NTLM	☐
NTLM Domain	
User-ID Collector Name	

Server Monitoring

☐	Name	Enabled	Type	Network Address	Status
☐	lab-client	☑	Microsoft Active Directory	192.168.1.20	Connected

2. Deselect the **Enabled** check box then click **OK**.



User Identification Monitored Server

Name: lab-client

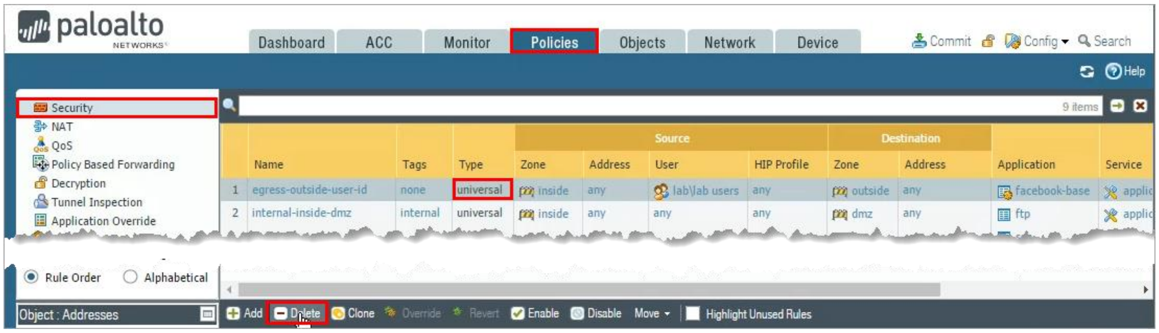
Description:

☐ Enabled

Type: Microsoft Active Directory

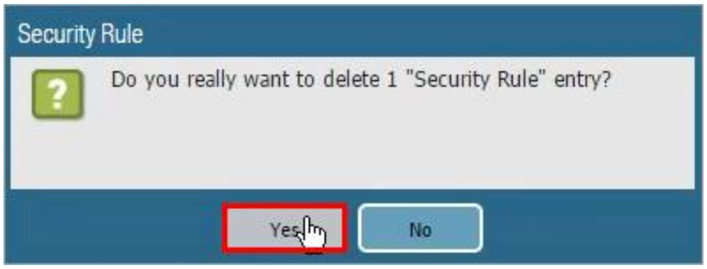
Network Address: 192.168.1.20

3. Select **Policies > Security**. Select but do not open the Security policy rule named **egress-outside-user-id** then click **Delete**.



				Source				Destination			
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service
1	egress-outside-user-id	none	universal	inside	any	lab\lab users	any	outside	any	facebook-base	applic
2	internal-inside-dmz	internal	universal	inside	any	any	any	dmz	any	ftp	applic

4. Click **Yes**.



Security Rule

Do you really want to delete 1 "Security Rule" entry?

5. **Commit** all changes.

Stop. This is the end of the User-ID lab.