# PAN-OS 7.0 FIREWALL ESSENTIALS
# LAB SERIES

## Lab 15: Advanced Monitoring and Reporting

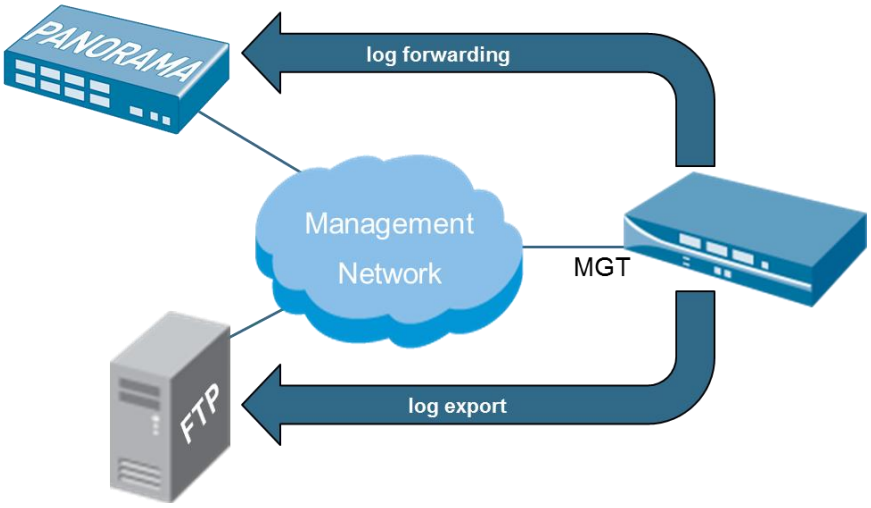
**Document Version: 2016-04-19**

# Contents



## Introduction




To have a complete view of network traffic and threats in your environment, you decide to centralize all logs on a Panorama server. Logs generated by the existing security polices and the system log must be forwarded to Panorama and an external syslog server. To reduce the amount of information in the logs, you decide that only threat logs of severity level High or Critical must be forwarded.

Additionally, the traffic log must be uploaded to an FTP server nightly to provide an additional backup of traffic data for historical reference.

You will also generate a PDF summary report to get a general idea of activity on your firewall.

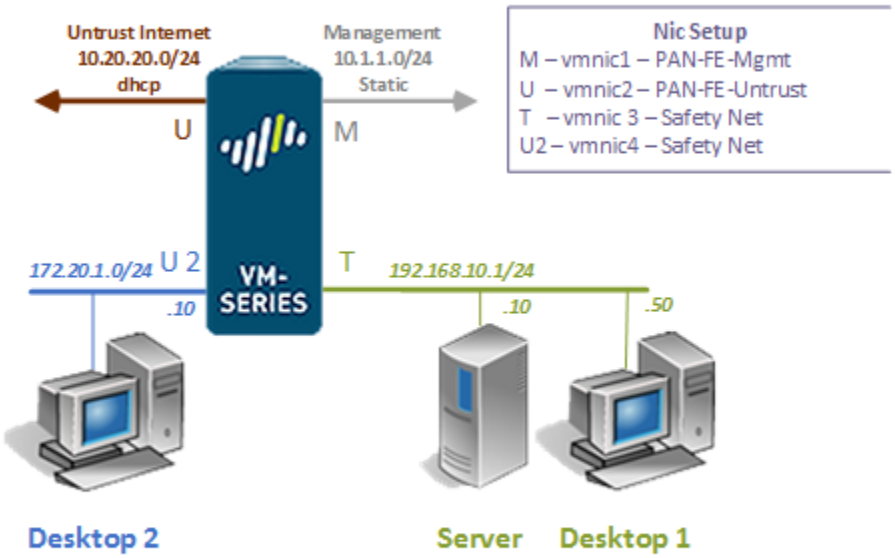
## Objective

In this lab, you will be utilizing Palo Alto technology to perform the following tasks:

1. Configure log-forwarding
2. Configure a service route to forward the logs

## Pod 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) |
|---|---|---|---|
| Ubuntu Desktop 1 | 192.168.10.50 | sysadmin | Train1ng$ |
| Ubuntu Server | 192.168.10.10 | sysadmin | Train1ng$ |
| Ubuntu Desktop 2 | 172.30.1.10 | sysadmin | Train1ng$ |
| Palo Alto Firewall | 192.168.10.1<br>172.30.1.1 | admin | paloalto |

# 1 Initial Firewall Configuration

1. Click on the **Desktop 1** graphic found on the *topology page*.
2. Login using **`sysadmin`** as the *username* and **`Train1ng$`** as the *password*. Click **Log In**.
3. Double-click on the **Firefox Web Browser** icon located on the *Desktop*.

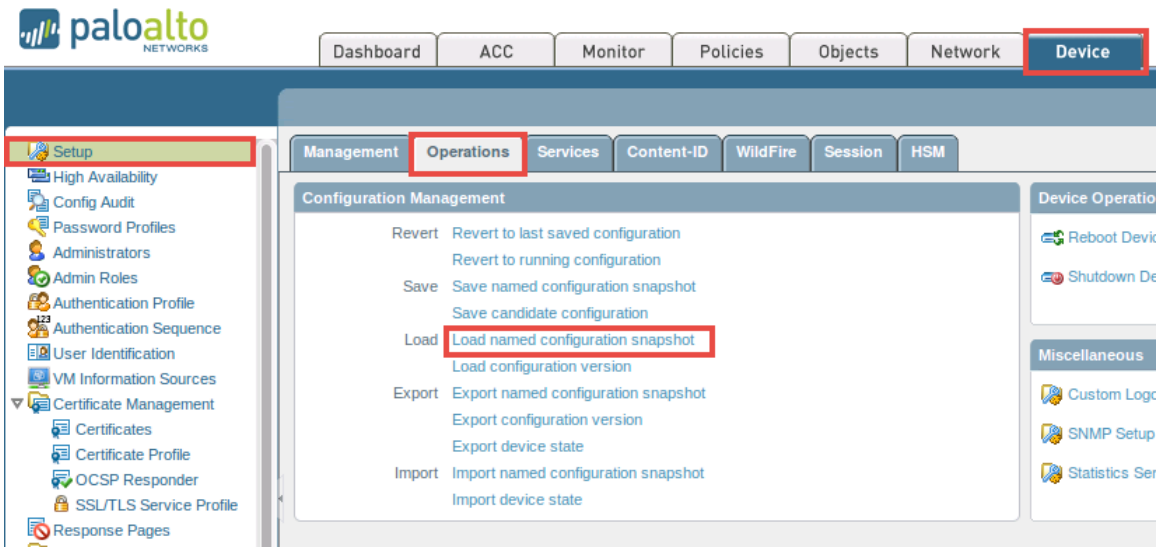

4. In the address field, type **`https://192.168.10.1`** and press **Enter**.

> If you experience the "*Unable to connect*" message while attempting to connect to the specified IP above, please wait an additional 3-5 minutes for the PA VM to fully initialize and refresh the page to continue.

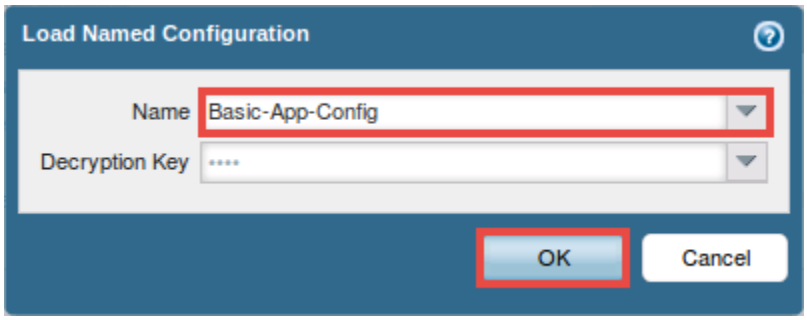
5. Login with the *username* **`admin`** and *password* **`paloalto`** on the firewall web interface.

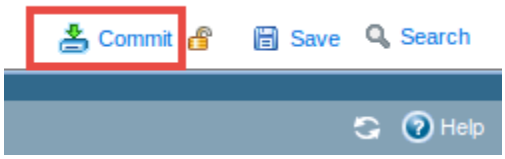
6. Using the *Palo Alto WebUI*, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.




7. In the *Load Named Configuration* window, select **Basic-App-Config** from the *Name* drop-down box. Click **OK**.

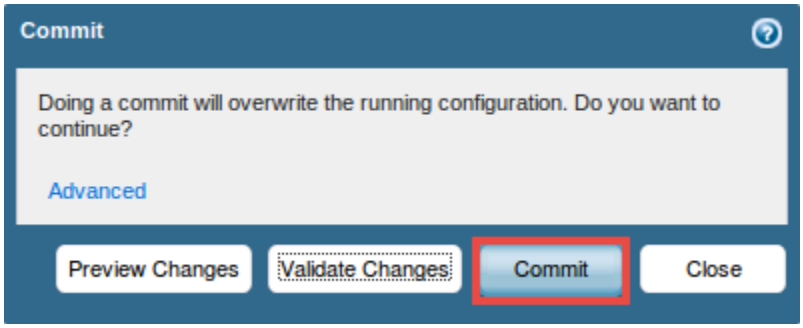



8. When prompted with the config loaded message, click on the **Close** button to continue.
9. Click on the **Commit** link located at the top-right of the *WebUI*.

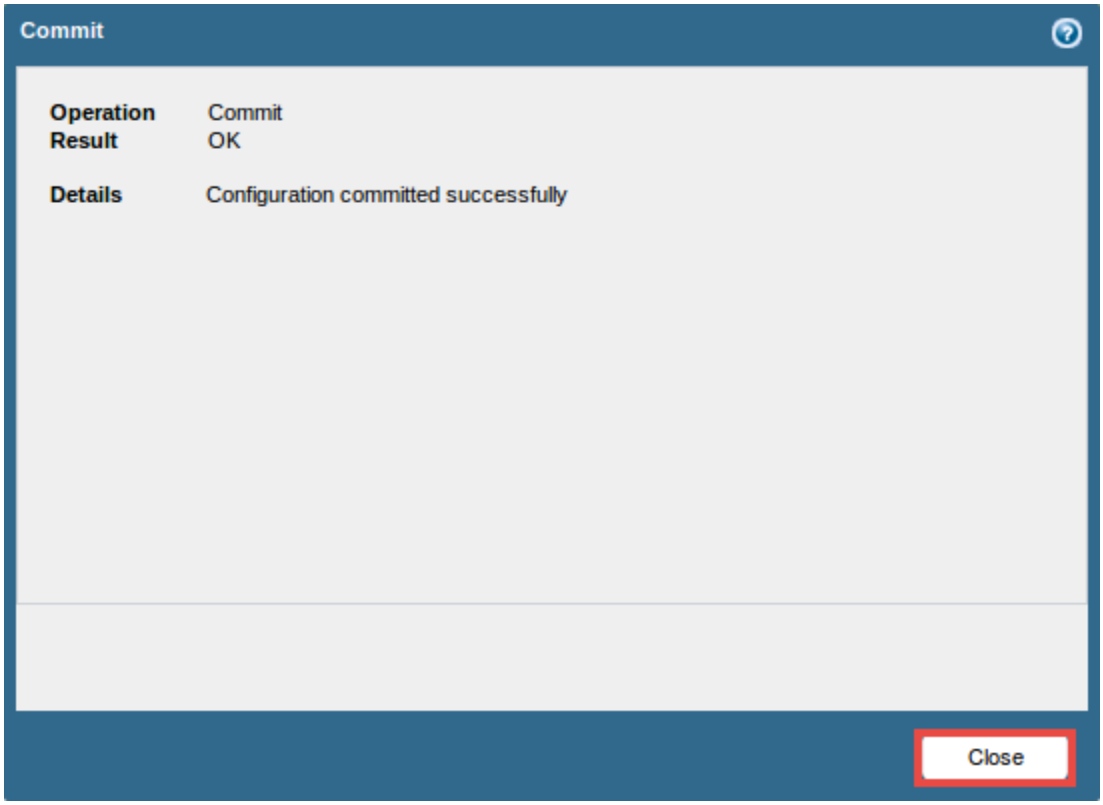


10. In the *Commit* window, click **Commit** to proceed with committing the changes.




11. Once the operation successfully completes, click **Close** to continue.



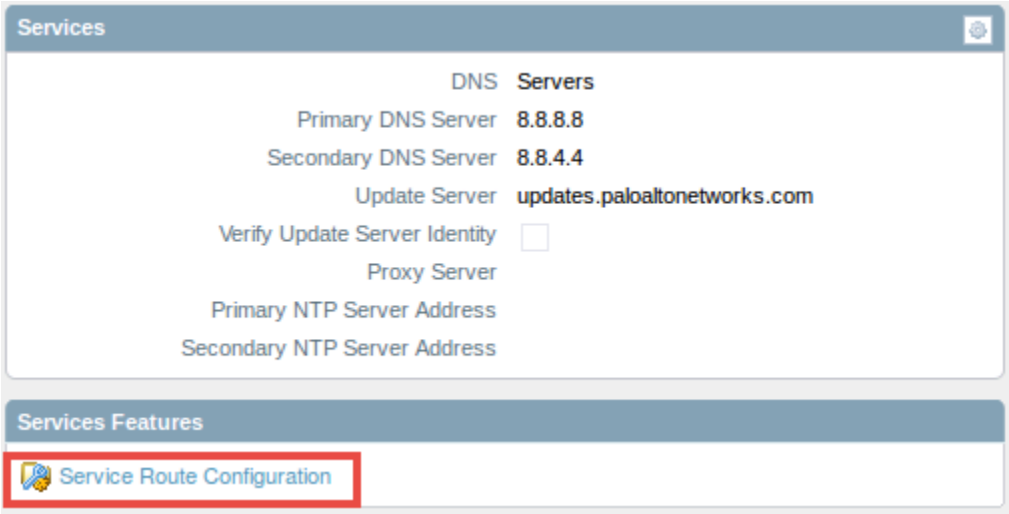

12. Leave the *WebUI* opened to continue with the next task.

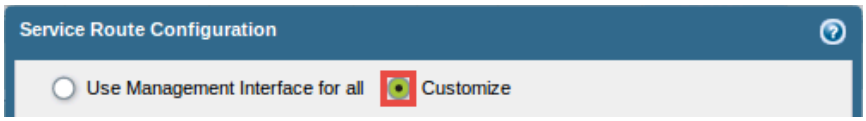
## 2 Prepare Service Route to Forward Syslog

1. Using the *WebUI*, navigate to **Device > Setup > Services**.

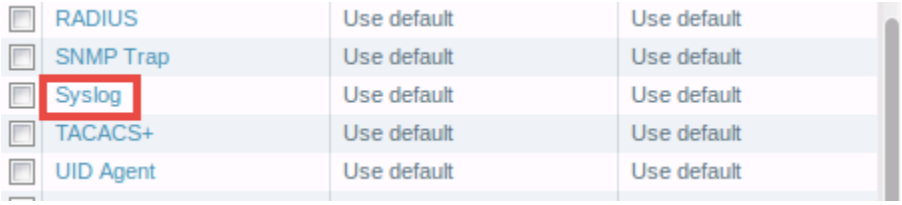

2. Click on the **Service Route Configuration** link, in the *Services Features* pane.




3. In the *Service Route Configuration* window, select the **Customize** radio button.



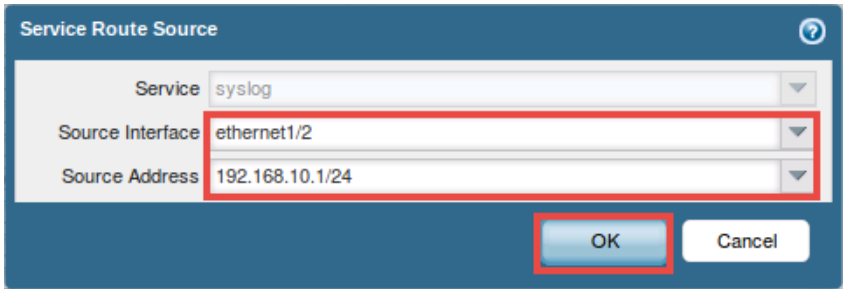

4. In the *Service Route Configuration* window, scroll down the service list and click on **Syslog** to open the *Service Route Source* configuration window.



5. In the *Service Route Source* window, use the information from the table below to make the appropriate configurations.

| Field | Data/Selection |
|---|---|
| *Source Interface* | Select **ethernet1/2** |
| *Source Address* | Select **192.168.10.1/24** |

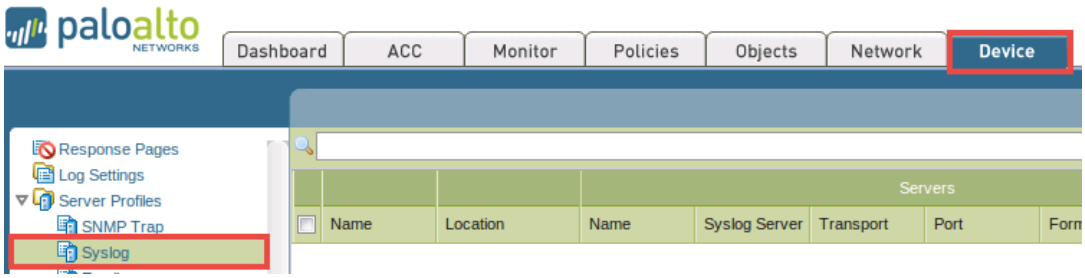



6. Click **OK** to save changes.
7. In the *Service Route Configuration* window, verify that **Syslog** is checked and click **OK**.
8. Leave the *WebUI* opened to continue with the next task.

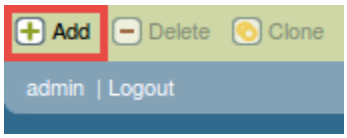
  

## 3 Configure a Security Policy for Log Forwarding

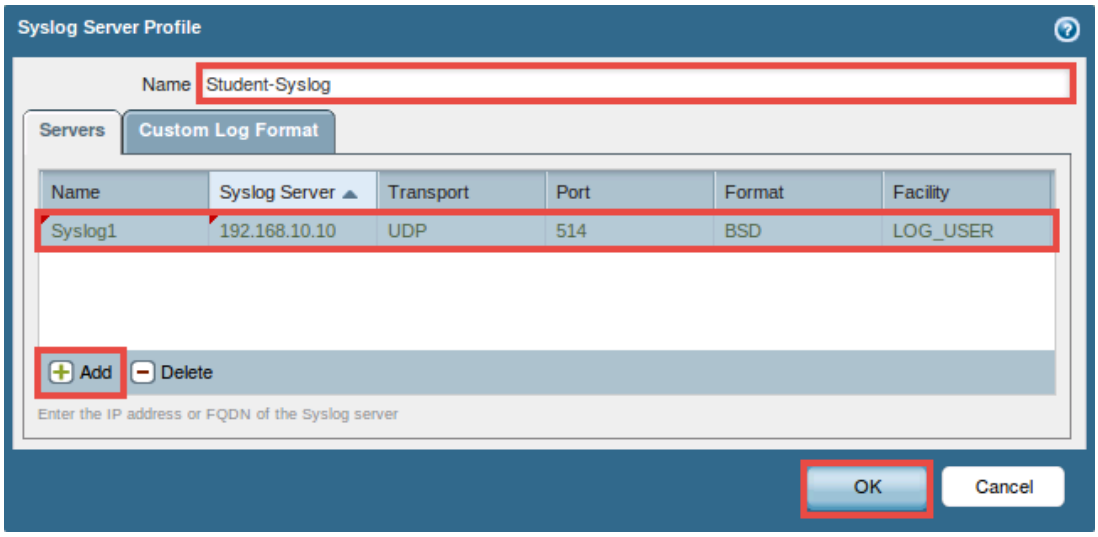
1. Using the *WebUI*, navigate to **Device > Server Profiles > Syslog**.




2. Click on **Add**, located near the bottom of the window, to create a syslog server profile.



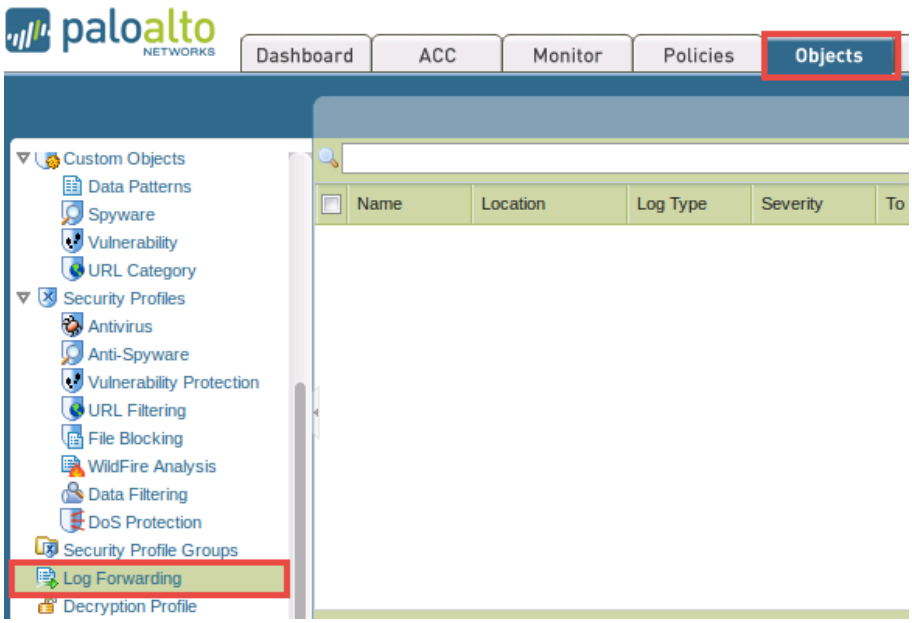

3. In the *Syslog Server Profile* window, enter `Student-Syslog` into the *Name* field.
4. In the *Syslog Server Profile* window, click on **Add** followed by typing `Syslog1` in the *Name* column and `192.168.10.10` in the *Syslog Server* column.



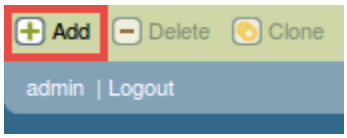

5. Click **OK** to save the configurations.
6. Verify that *Student-Syslog* appears in the list.

7. Using the *WebUI*, navigate to **Objects > Log Forwarding**.



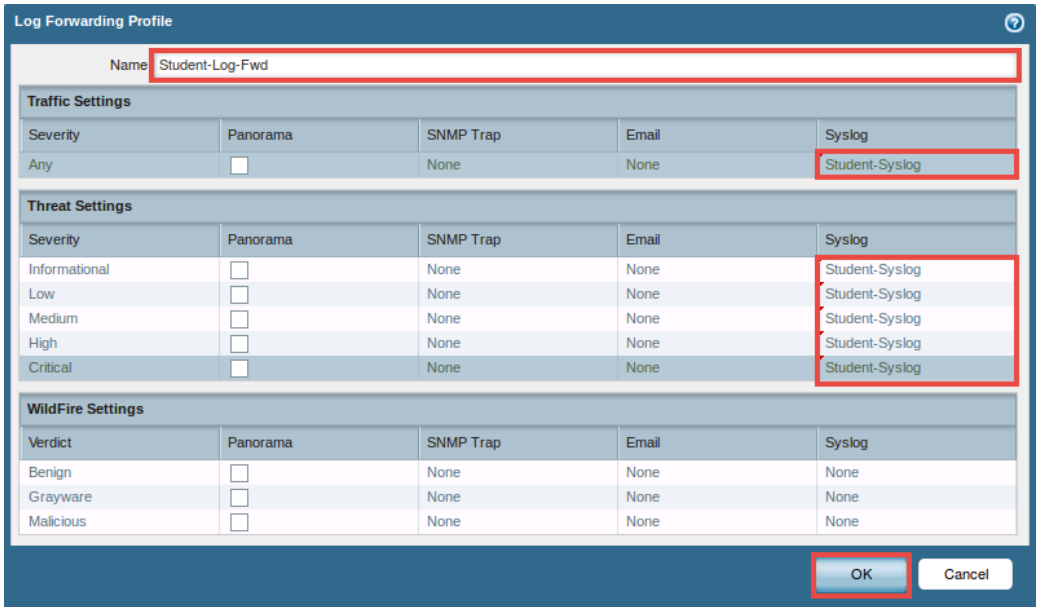

8. Click on **Add**, located near the bottom of the window, to create a log forwarding profile.



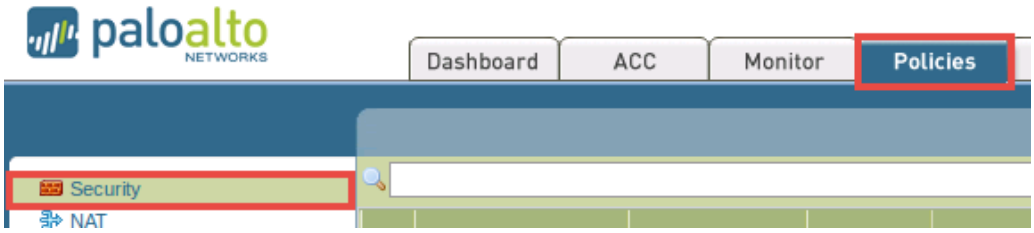

9. In the *Log Forwarding Profile* window, use the information from the table below to make the appropriate configurations.

| Field | Data/Selection |
|---|---|
| *Name* | Enter **Student-Log-Fwd** |
| *Traffic Settings* | In the *Syslog* column, select **Student-Syslog** |
| *Threat Settings* | Select **Student-Syslog** in the *Syslog* column for **all** *Severity* levels |

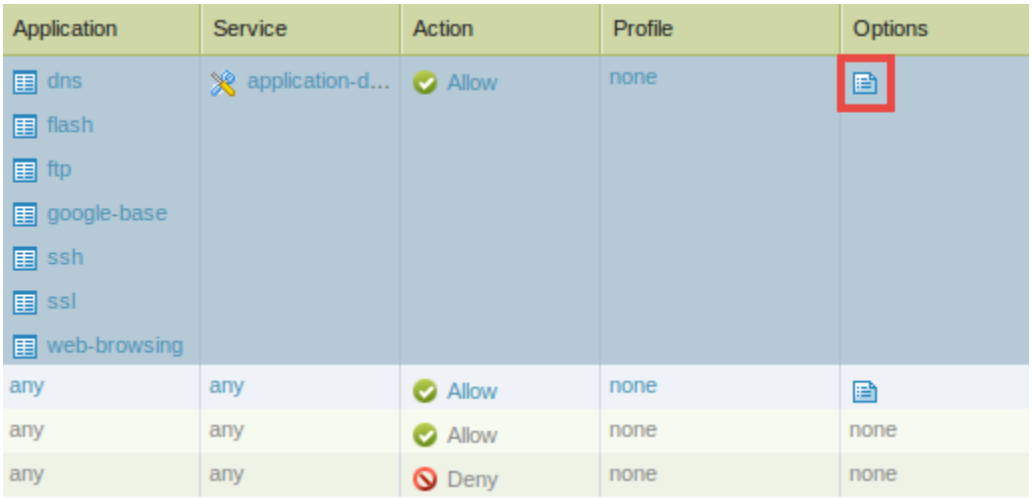
  




10. Click **OK** to save changes.
11. Verify that the *Student-Log-Fwd* appears in the list.
12. Using the *WebUI*, navigate to **Policies > Security**.

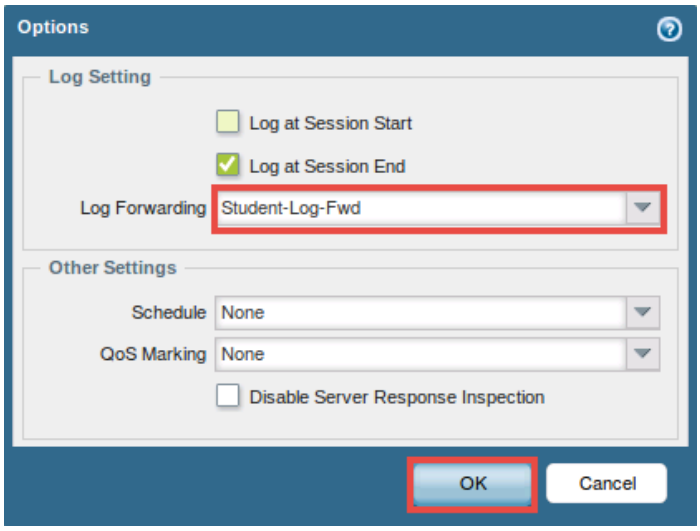



13. Scroll to the right within the list and click on the **icon** in the **Options** column for the **Basic-Allowed-Apps** security policy.



14. In the *Options* window, select **Student-Log-Fwd** in the *Log Forwarding* drop-down menu.

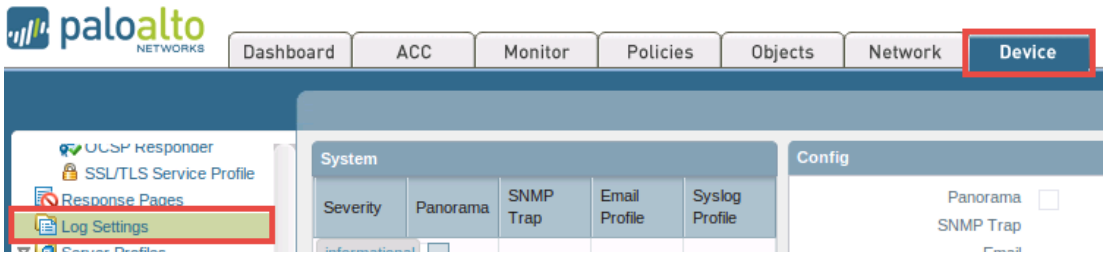



15. Click **OK** to save changes.
16. Leave the *WebUI* opened to continue with the next task.

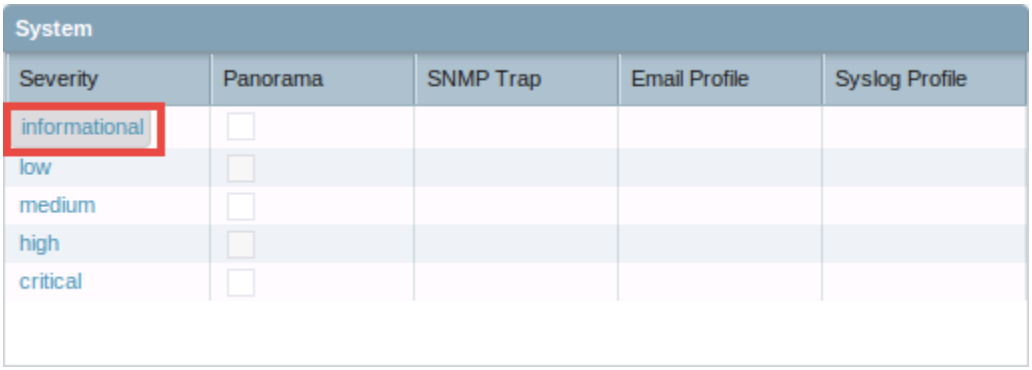
  

## 4 Configure System Log Forwarding

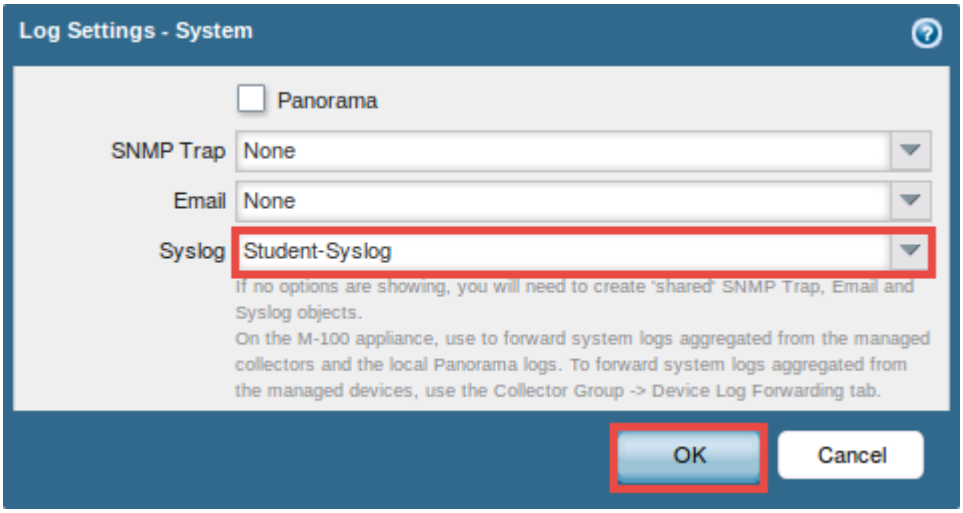
1. Using the *WebUI*, navigate to **Device > Log Settings**.




2. In the *System* panel, click on **informational** underneath the *Severity* column.



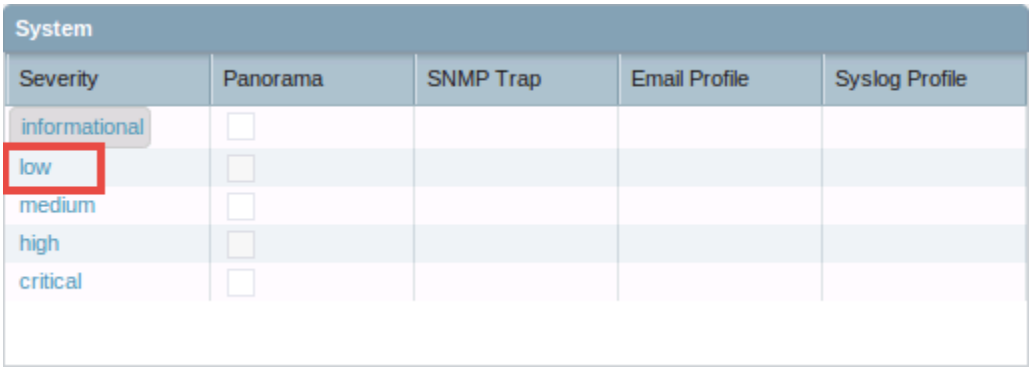

3. In the *Log Settings – System* window, select **Student-Syslog** from the *Syslog* drop-down menu.



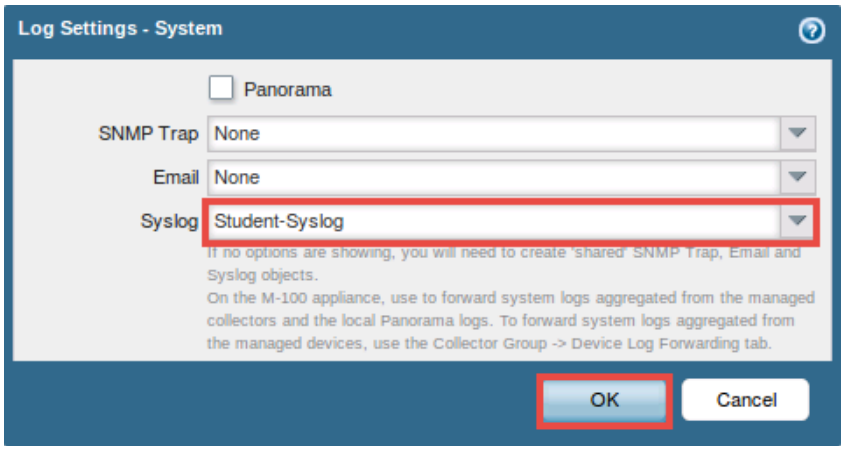

4. Click **OK** to save changes.

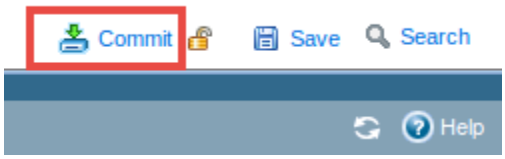
5. In the *System* panel, click on **low** underneath the *Severity* column.



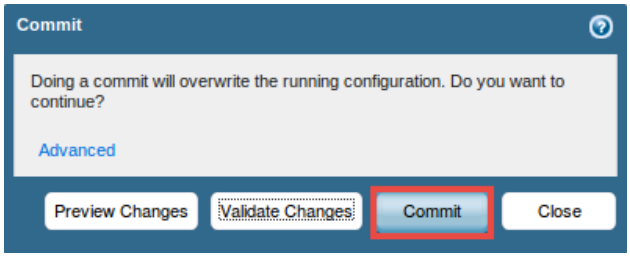

6. In the *Log Settings – System* window, select **Student-Syslog** from the *Syslog* drop-down menu.




7. Click **OK** to save changes.
8. Click on the **Commit** link located at the top-right of the *WebUI*.




9. In the *Commit* window, click **Commit** to proceed with committing the changes.




10. Once the operation successfully completes, click **Close** to continue.

## 5 Test the Remote Logging

1. While on the *Desktop 1* VM, open a new terminal by clicking on the **LXTerminal** icon, located in the bottom tool panel.

2. Using the terminal, type the command below followed by pressing the **Enter** key.

```
ssh sysadmin@192.168.10.10
```

3. When prompted for a password, enter **`Train1ng$`**.
4. Once in the server, enter the command below and analyze the logs.

```
tail -f /var/log/192.168.10.1/syslog.log
```

```
sysadmin@ubuntu:~$ tail /var/log/192.168.10.1/syslog.log
Nov  9 13:02:04 PA-VM 1,2015/11/09 13:02:04,007000007144,SYSTEM,ras,0,2015/11/09 13:02:04,,rasmgr-config-p1-success,,0,0,general,inf
ormational,RASMGR daemon configuration load phase-1 succeeded.,1780,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:04 PA-VM 1,2015/11/09 13:02:04,007000007144,SYSTEM,sslmgr,0,2015/11/09 13:02:04,,sslmgr-config-p1-success,,0,0,general,
informational,SSLMGR daemon configuration load phase-1 succeeded.,1781,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:04 PA-VM 1,2015/11/09 13:02:04,007000007144,SYSTEM,satd,0,2015/11/09 13:02:04,,satd-config-p1-success,,0,0,general,info
rmational,SATD daemon configuration load phase-1 succeeded.,1782,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:10 PA-VM 1,2015/11/09 13:02:10,007000007144,SYSTEM,routing,0,2015/11/09 13:02:10,,routed-config-p2-success,,0,0,general
,informational,Route daemon configuration load phase-2 succeeded.,1783,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:10 PA-VM 1,2015/11/09 13:02:10,007000007144,SYSTEM,vpn,0,2015/11/09 13:02:10,,ike-config-p2-success,,0,0,general,inform
ational,IKE daemon configuration load phase-2 succeeded.,1784,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:10 PA-VM 1,2015/11/09 13:02:10,007000007144,SYSTEM,satd,0,2015/11/09 13:02:10,,satd-config-p2-success,,0,0,general,info
rmational,SATD daemon configuration load phase-2 succeeded.,1785,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:10 PA-VM 1,2015/11/09 13:02:10,007000007144,SYSTEM,sslmgr,0,2015/11/09 13:02:10,,sslmgr-config-p2-success,,0,0,general,
informational,SSLMGR daemon configuration load phase-2 succeeded.,1786,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:10 PA-VM 1,2015/11/09 13:02:10,007000007144,SYSTEM,ras,0,2015/11/09 13:02:10,,rasmgr-config-p2-success,,0,0,general,inf
ormational,RASMGR daemon configuration load phase-2 succeeded.,1787,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:12 PA-VM 1,2015/11/09 13:02:12,007000007144,SYSTEM,dhcp,0,2015/11/09 13:02:12,,if-release-trigger,ethernet1/1,0,0,gener
al,informational,DHCP client triggered release on interface:ethernet1/1 from server: 10.20.20.254,1788,0x0,0,0,0,0,,PA-VM
Nov  9 13:02:12 PA-VM 1,2015/11/09 13:02:12,007000007144,SYSTEM,general,1,2015/11/09 13:02:12,,general,,0,0,general,informational,Co
nfig installed,1790,0x0,0,0,0,0,,
```

> If you do not see the */var/log/192.168.10.1* directory, wait for an additional 2-3 minutes for the system to update.

5. Open a **new tab** in the *Firefox* browser and then navigate to **`www.yahoo.com`**. Once the page loads, go back to the terminal window. You should see the syslog file updating on the screen.
6. Close the **Desktop 1** PC viewer to end the lab.