SECURITY OPERATIONS FUNDAMENTALS V2

Lab 4: Log Forwarding to Linux

Document Version: 2022-12-23

Contents

Introduction

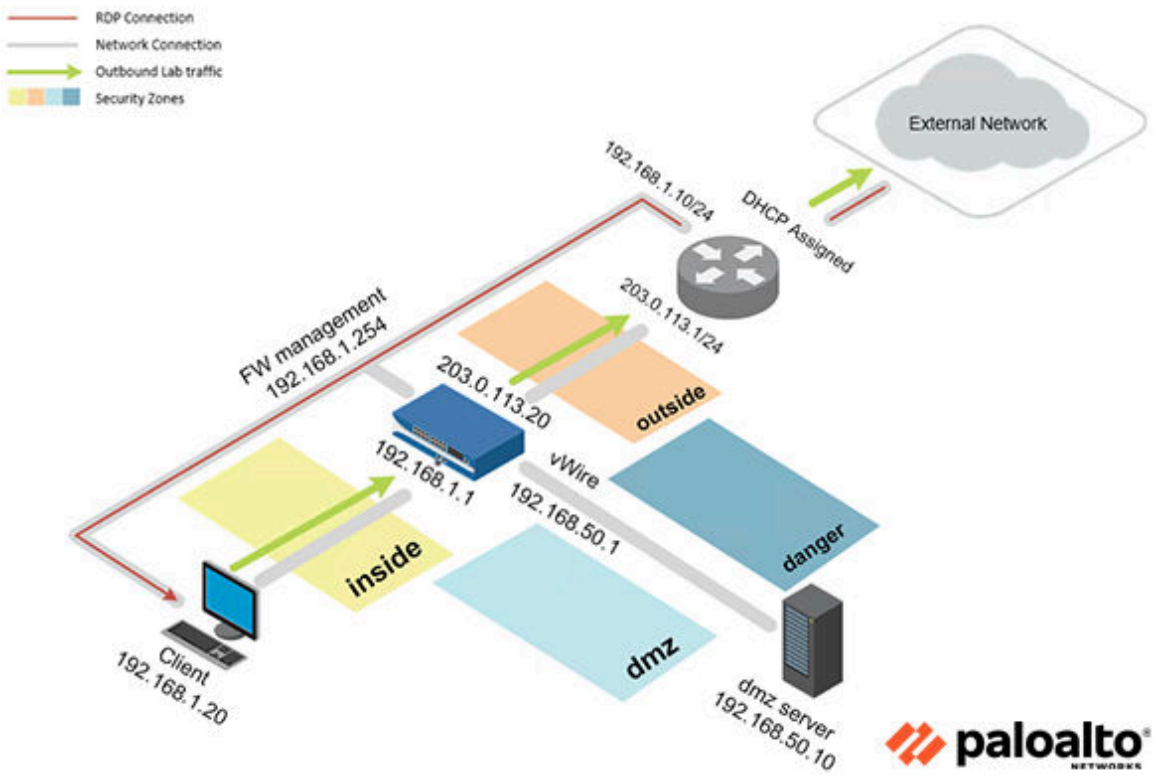
In this lab, you will configure Syslog Monitoring in the Palo Alto Networks Firewall. You will confirm the logs are being forwarded and view the files on the DMZ server.

Objective

In this lab, you will perform the following tasks:

- Configure Syslog Monitoring via Palo Alto Firewall
- Verify Syslog Forwarding

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.

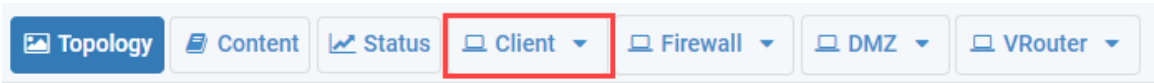
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	`lab-user`	`Pal0Alt0!`
DMZ	192.168.50.10	`root`	`Pal0Alt0!`
Firewall	192.168.1.254	`admin`	`Pal0Alt0!`

1 Log Forwarding to Linux

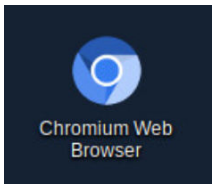
1.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

1. Click on the **Client** tab to access the client PC.

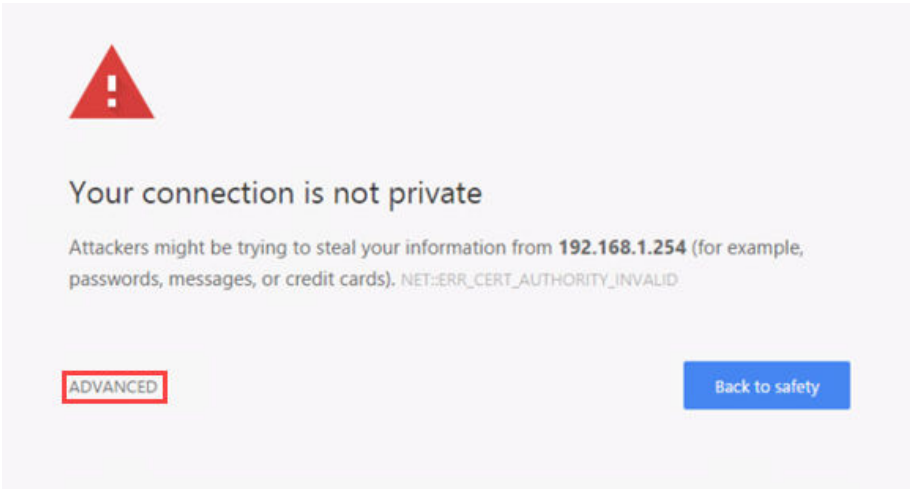


2. Log in to the client PC as username `lab-user`, password `Pal0Alt0!`.
3. Double-click the **Chromium** icon located on the desktop.



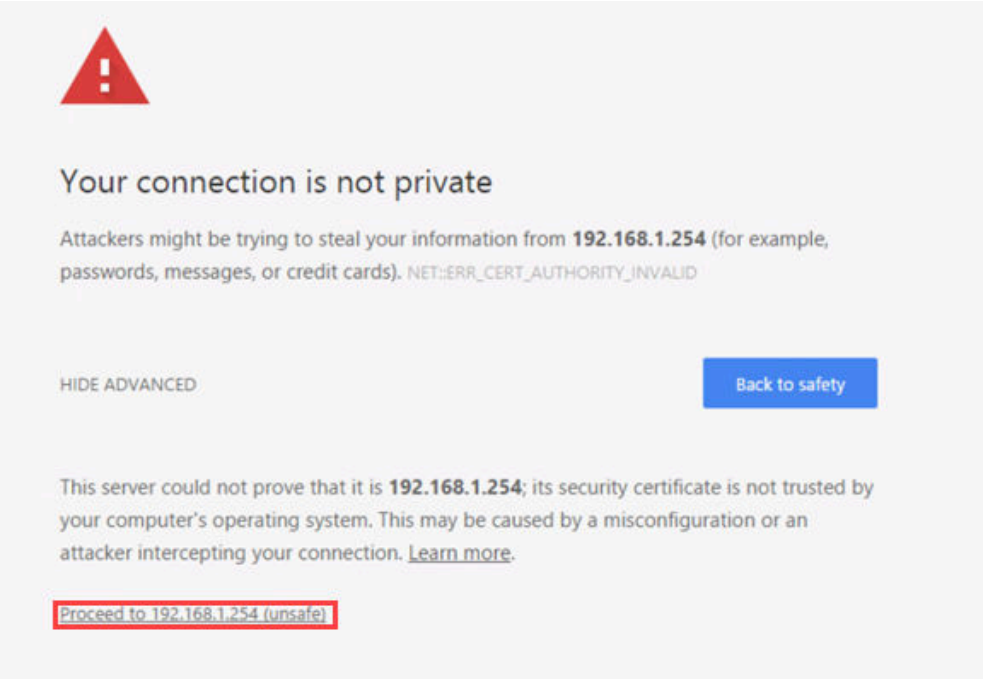
4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.

5. You will see a "*Your connection is not private*" message. Click on the **ADVANCED** link.



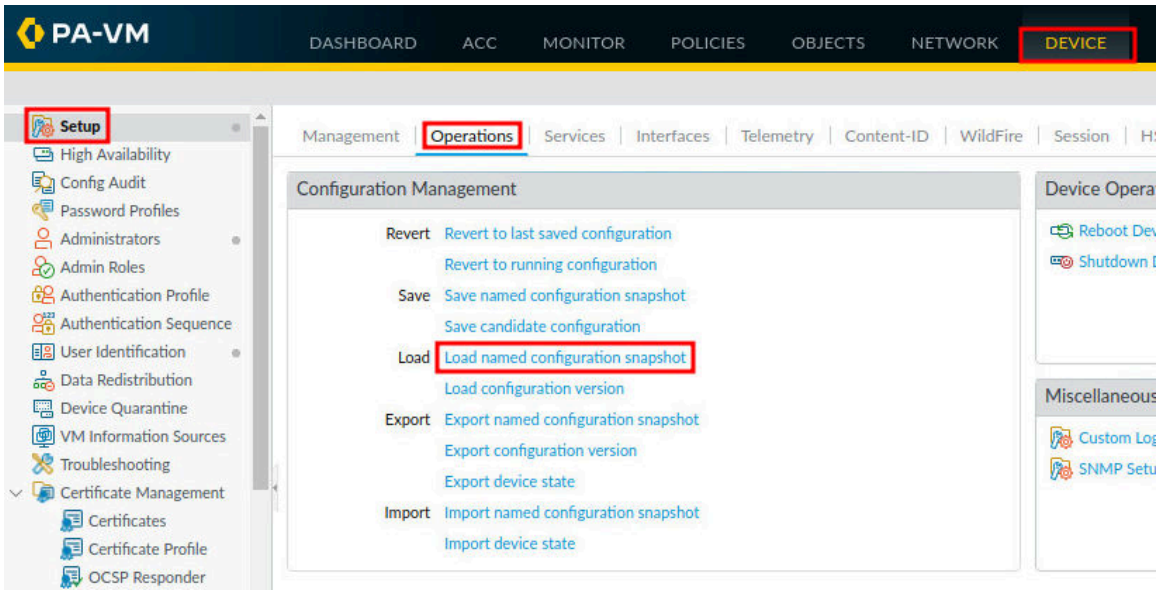
If you encounter the *"Unable to connect"* or *"502 Bad Gateway"* message while attempting to connect to the IP specified above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

6. Click on **Proceed to 192.168.1.254 (unsafe)**.

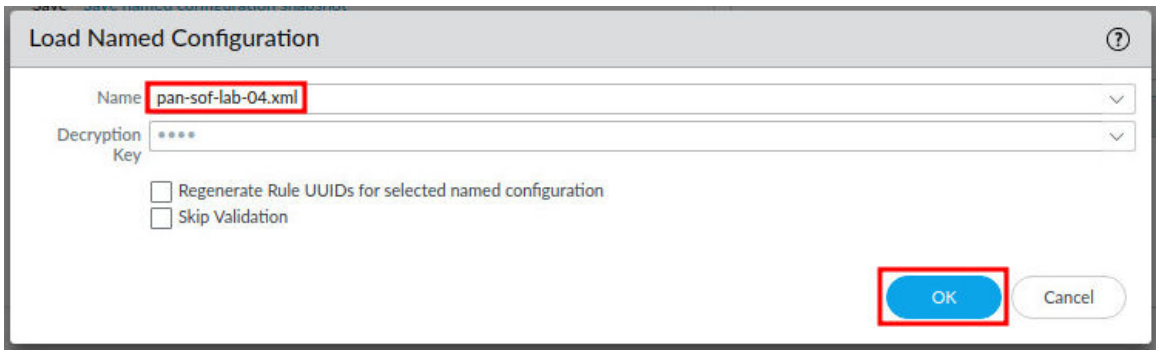


7. Log in to the Firewall web interface as username `admin`, password `Pal0Alt0!`.

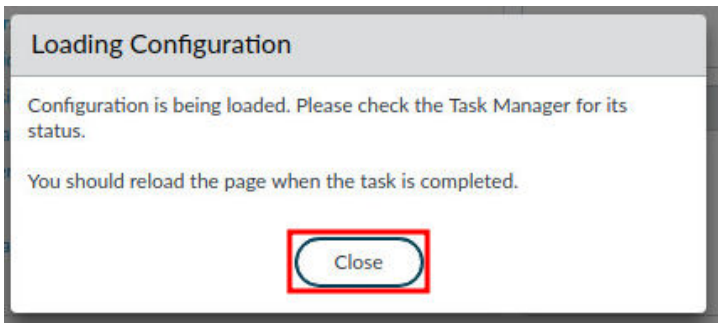
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan-sof-lab-04.xml** from the *Name* dropdown box and click **OK**.

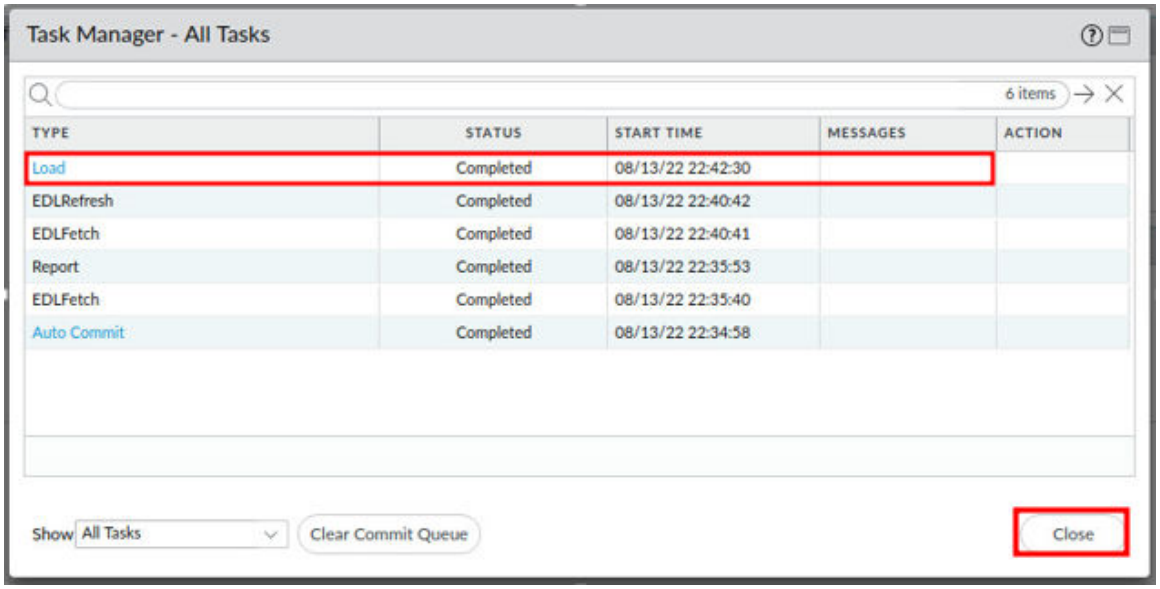


10. In the *Loading Configuration* window, a message will say *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.

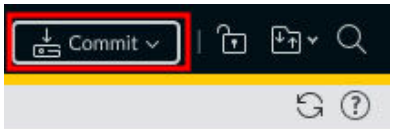


11. Click the **Tasks** icon located at the bottom-right of the web interface.

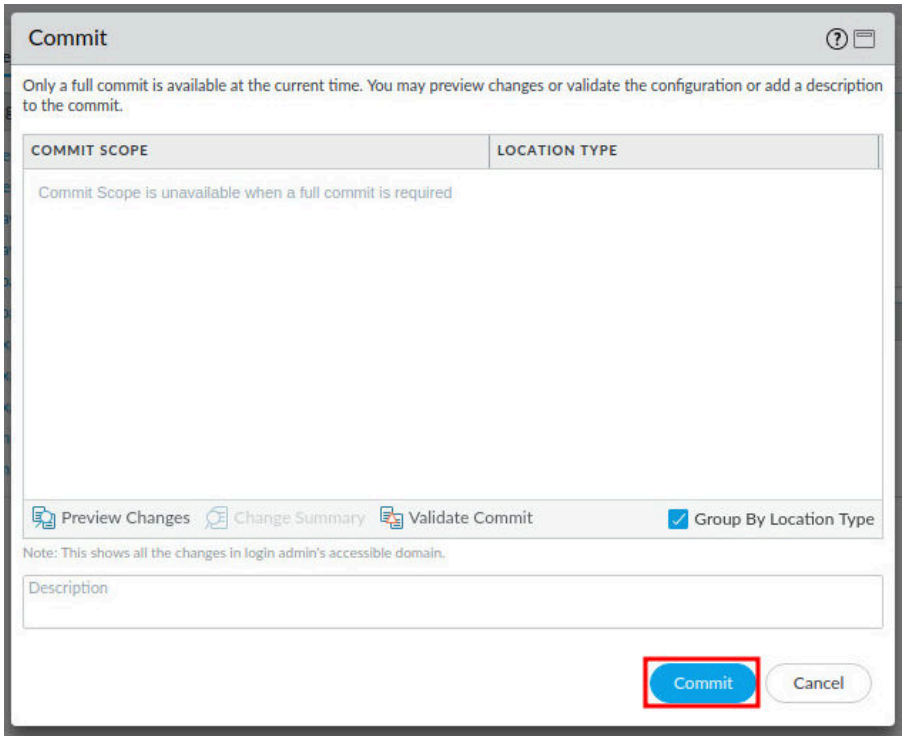
12. In the *Task Manager – All Tasks* window, verify that the *Load* type has successfully completed. Click **Close**.



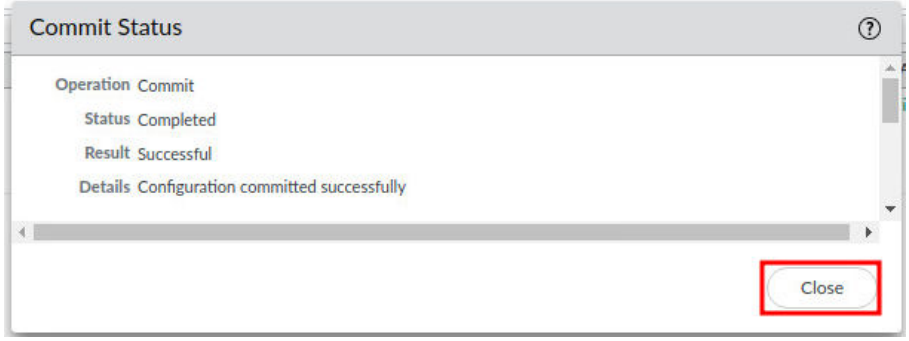
13. Click the **Commit** link located at the top-right of the web interface.



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



15. When the commit operation successfully completes, click **Close** to continue.

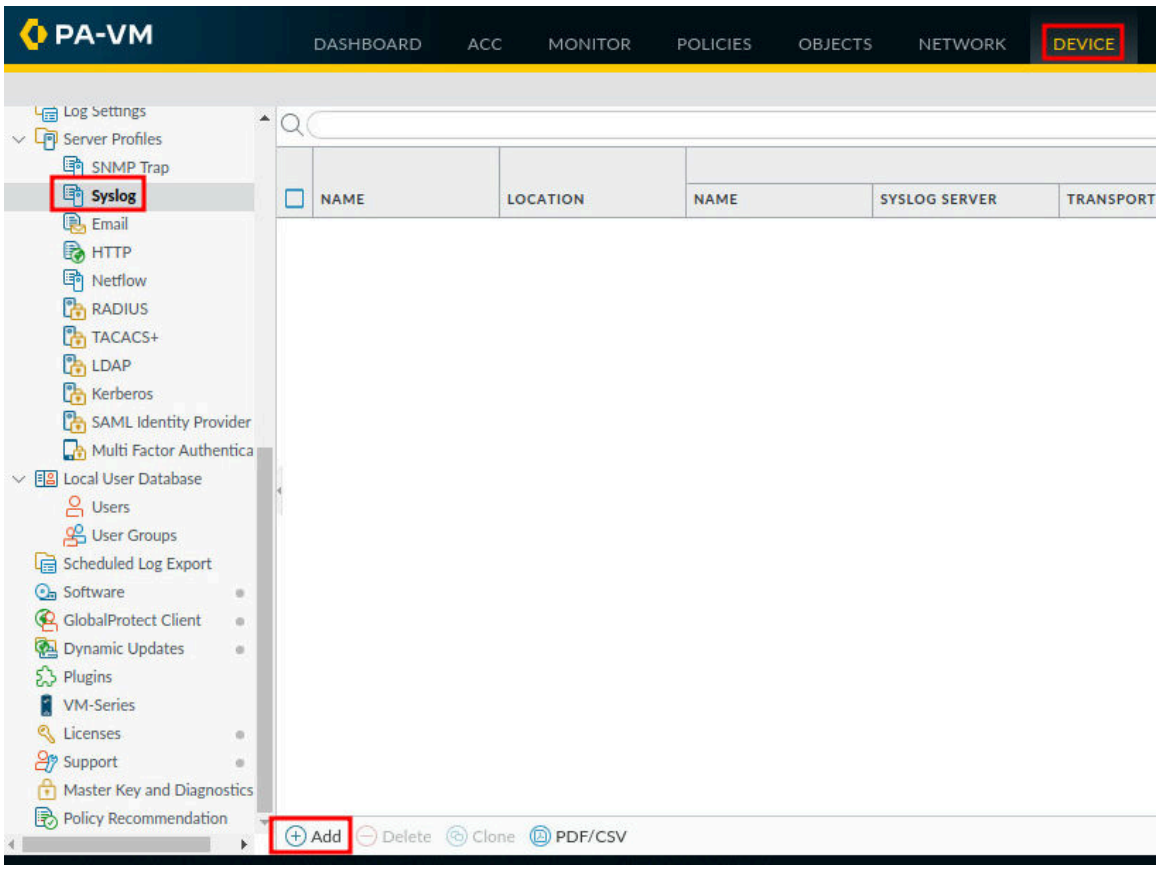


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

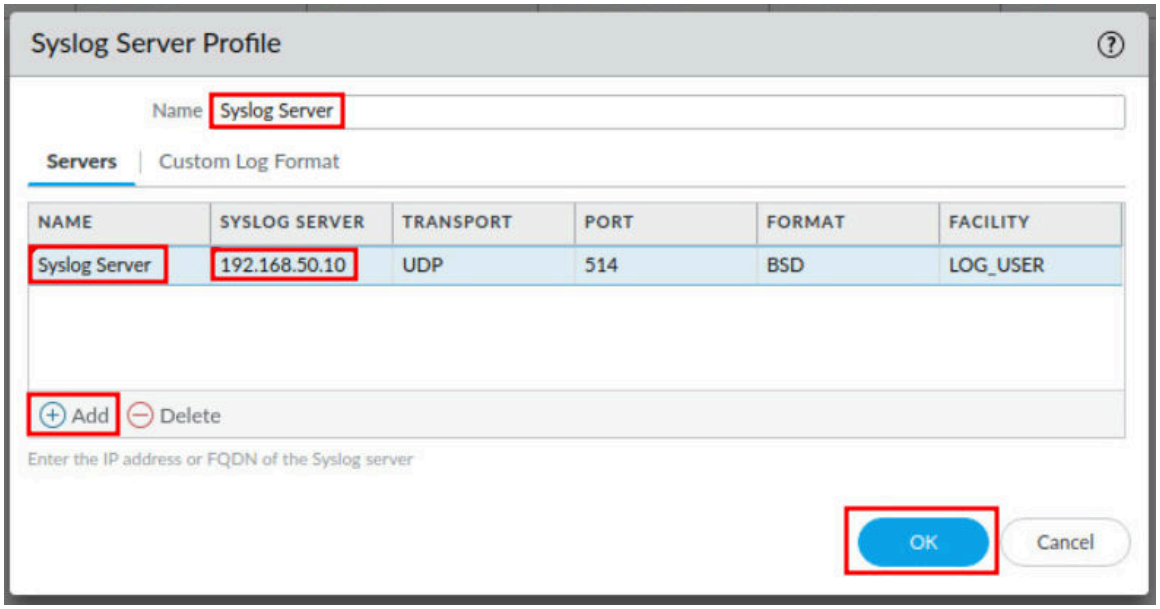
1.1 Configure Syslog Monitoring via Palo Alto Firewall

In this section, you will configure the Palo Alto Firewall for Syslog Monitoring. Syslog is a standard log transport mechanism that enables the aggregation of log data from different network devices - such as routers, firewalls, printers - from different vendors into a central repository for archiving, analysis, and reporting. Palo Alto Networks Firewalls can forward every type of log they generate to an external Syslog server. You can use TCP or SSL for reliable and secure log forwarding, or UDP for non-secure forwarding.

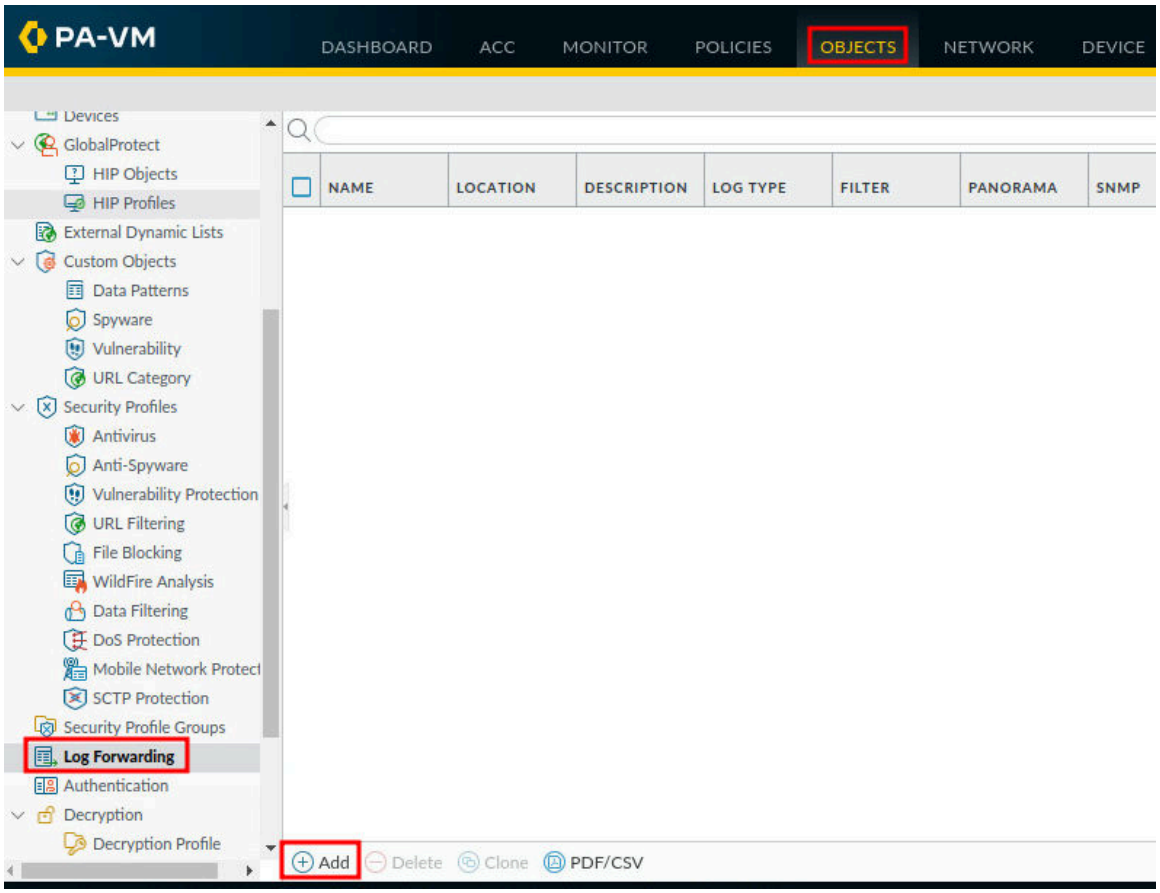
1. Navigate to **Device > Server Profiles > Syslog > Add**.



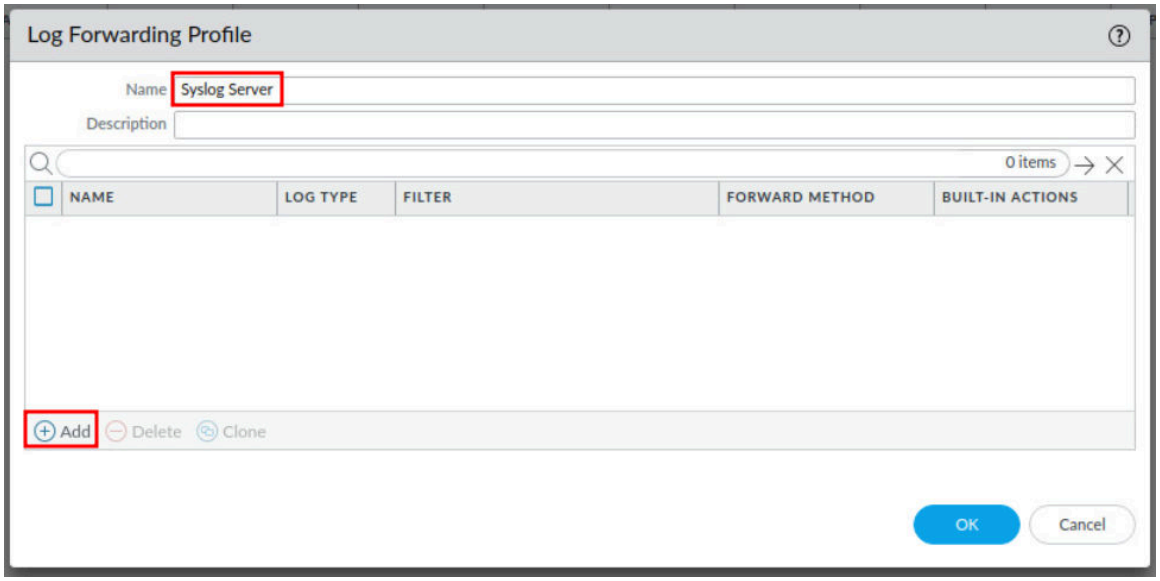
2. In the *Syslog Server Profile* window, type `Syslog Server` in the *Name* field. Next, click **Add**. Then, type `Syslog Server` in the *Name* column. Next, type `192.168.50.10` (the IP address of the DMZ server) in the *Syslog Server* column. Finally, click **OK**.



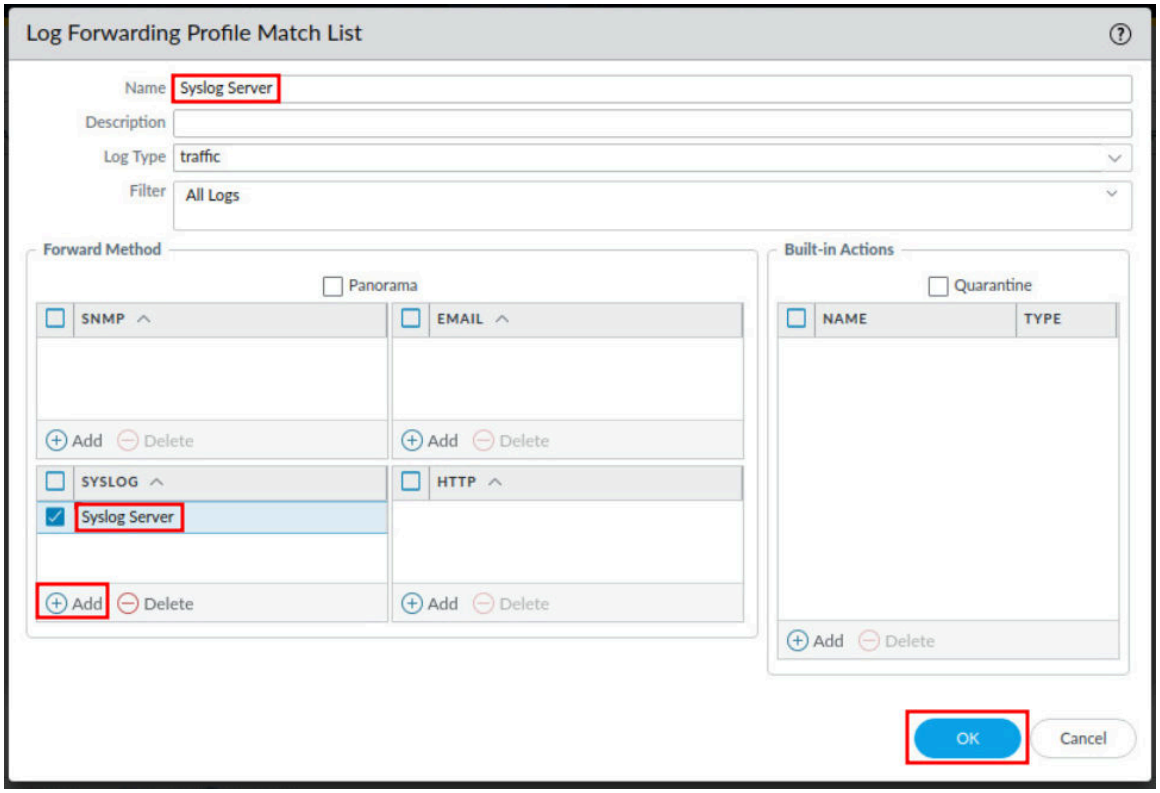
3. Navigate to **Objects > Log Forwarding > Add**.



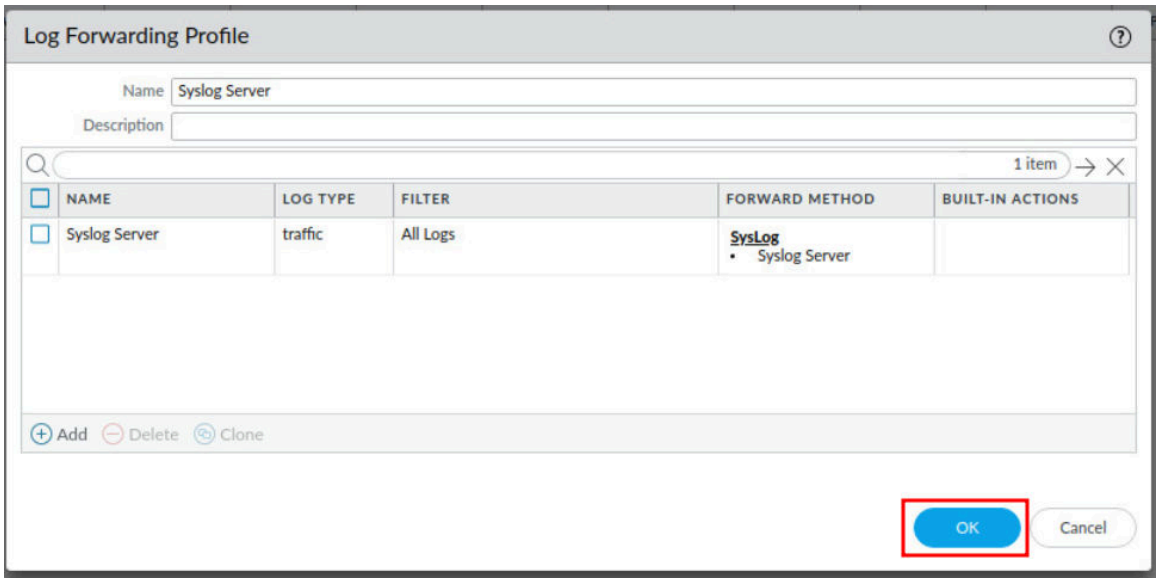
4. In the *Log Forwarding Profile* window, type `Syslog Server` in the *Name* field. Next, click **Add** in the lower-left corner.



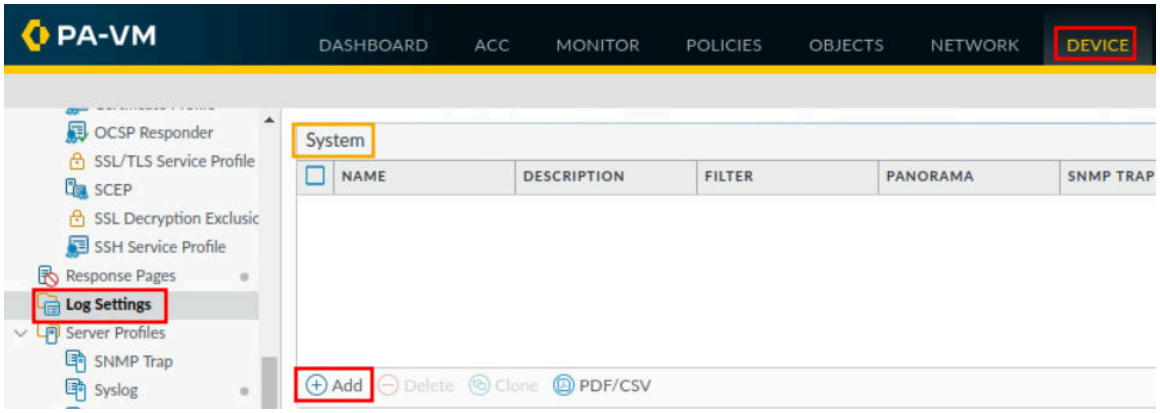
5. In the *Log Forwarding Profile Match List* window, type `Syslog Server` in the *Name* field. Next, confirm **traffic** is selected in the *Log Type* field and **All Logs** is selected in the *Filter* field. Then, under the *Syslog* section, click **Add**. Finally, select **Syslog Server** (the profile you created earlier) and click **OK**.



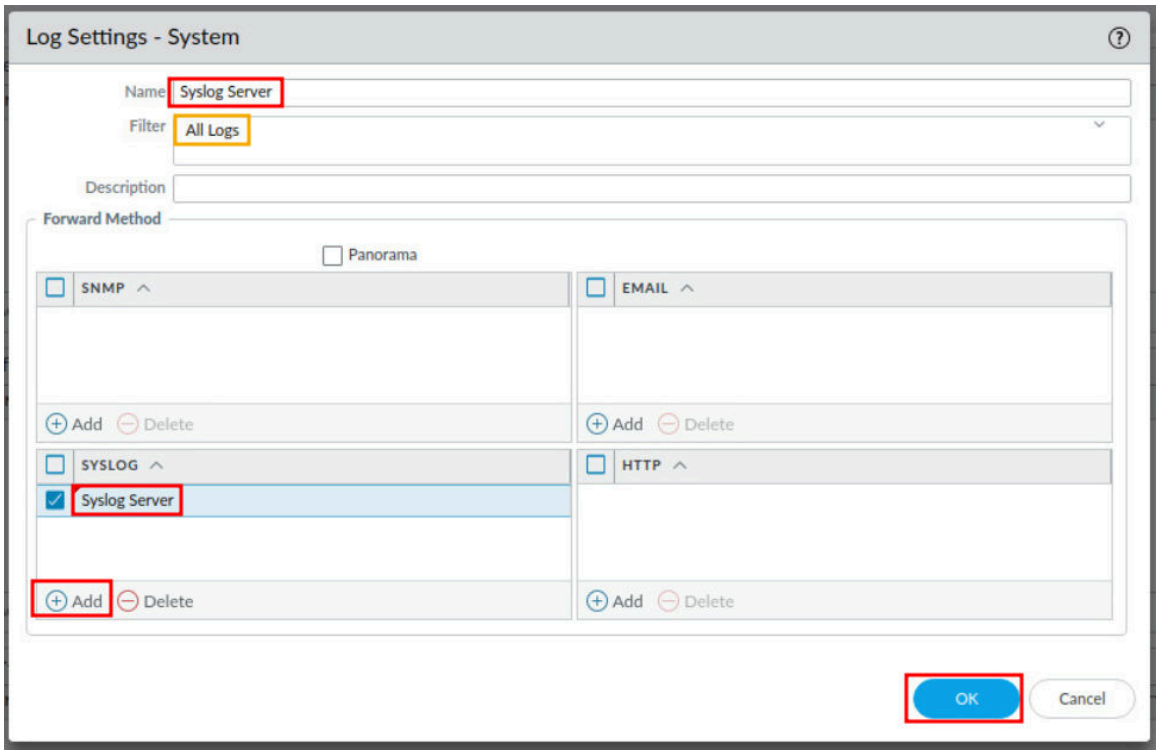
6. Verify that your screen matches the screenshot below, then click **OK**.



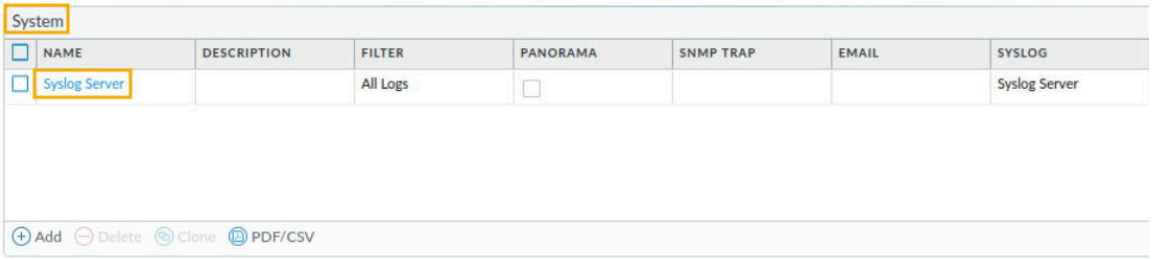
7. Navigate to **Device > Log Settings**, and in the *System* section, click **Add**.

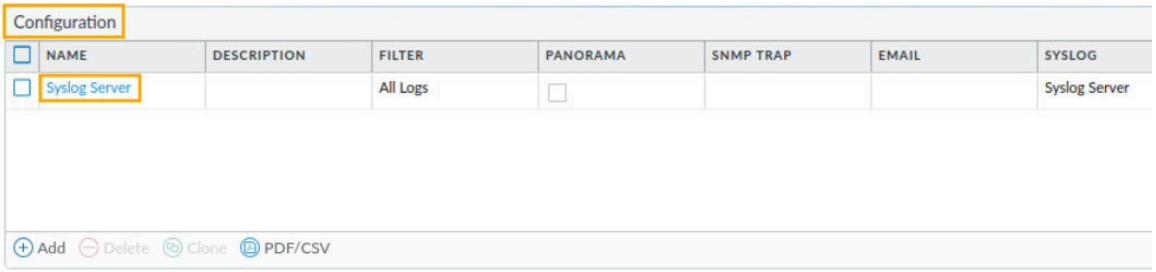


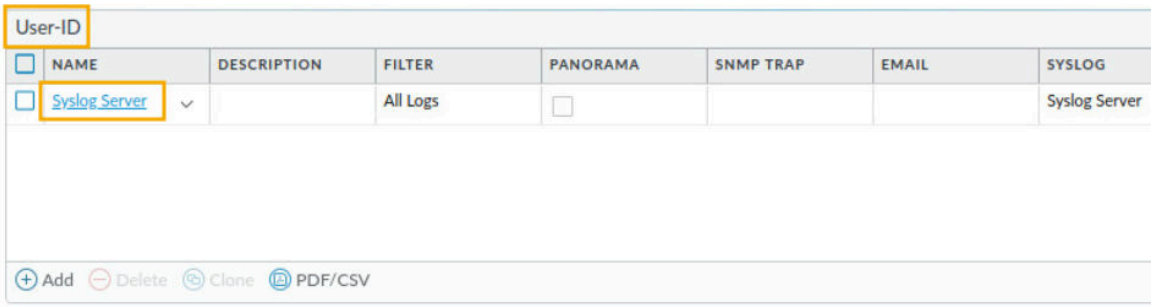
8. In the *Log Settings – System* window, type `Syslog Server` in the *Name* field. Next, confirm **All Logs** is selected in the *Filter* field. Then, in the *Syslog* section, click **Add**. Finally, select **Syslog Server** from the dropdown and click **OK**.

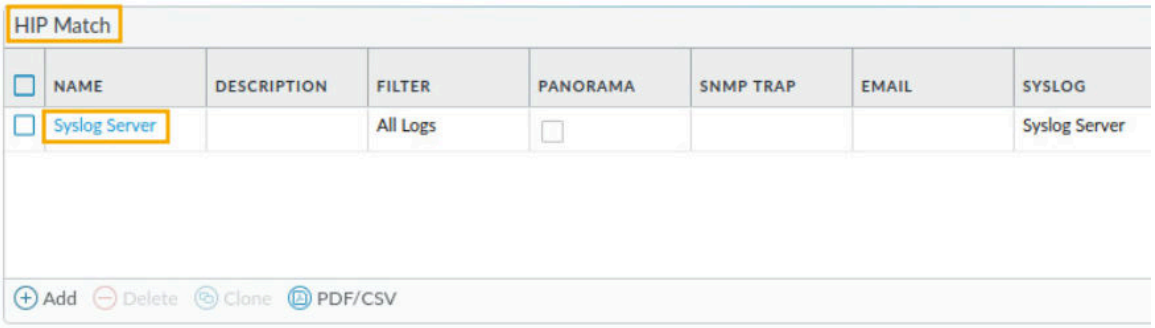


9. Repeat the previous step by clicking **Add** for *Configuration*, *User-ID*, and *HIP Match* sections. You may need to scroll down on the right. Confirm each section matches the pictures below.

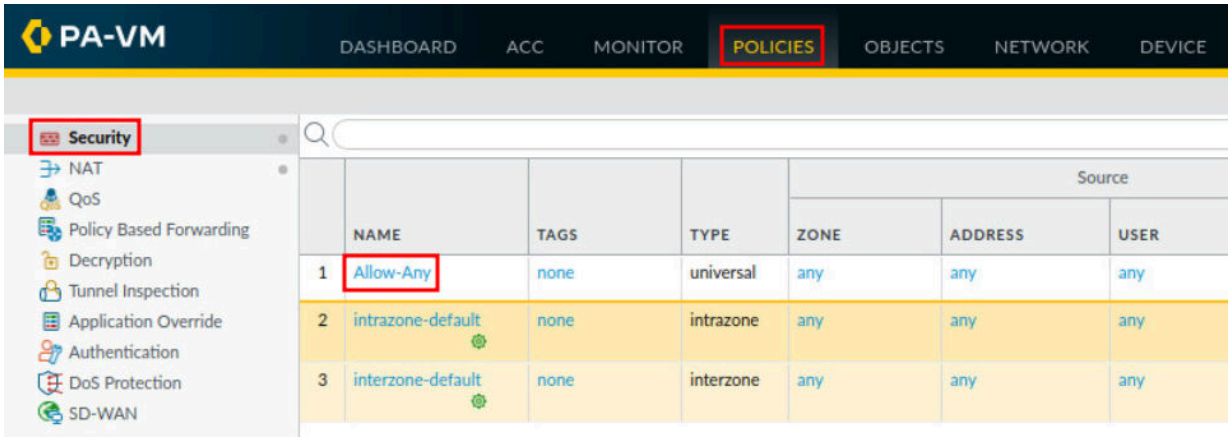




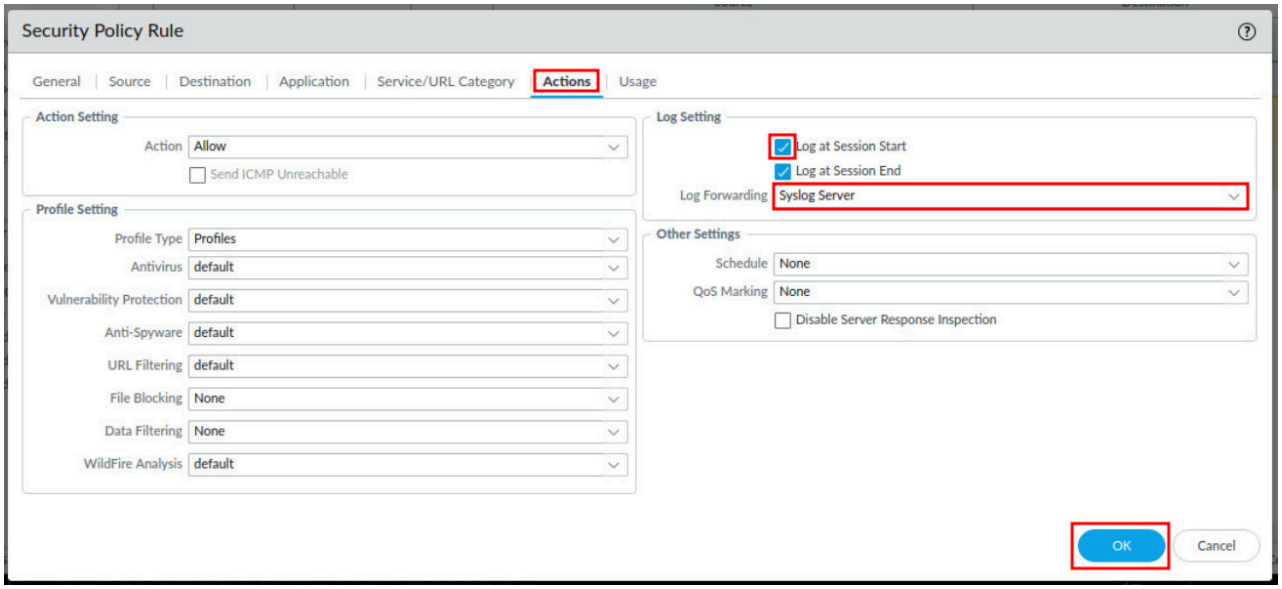




10. Navigate to **Policies > Security > Allow-Any.**

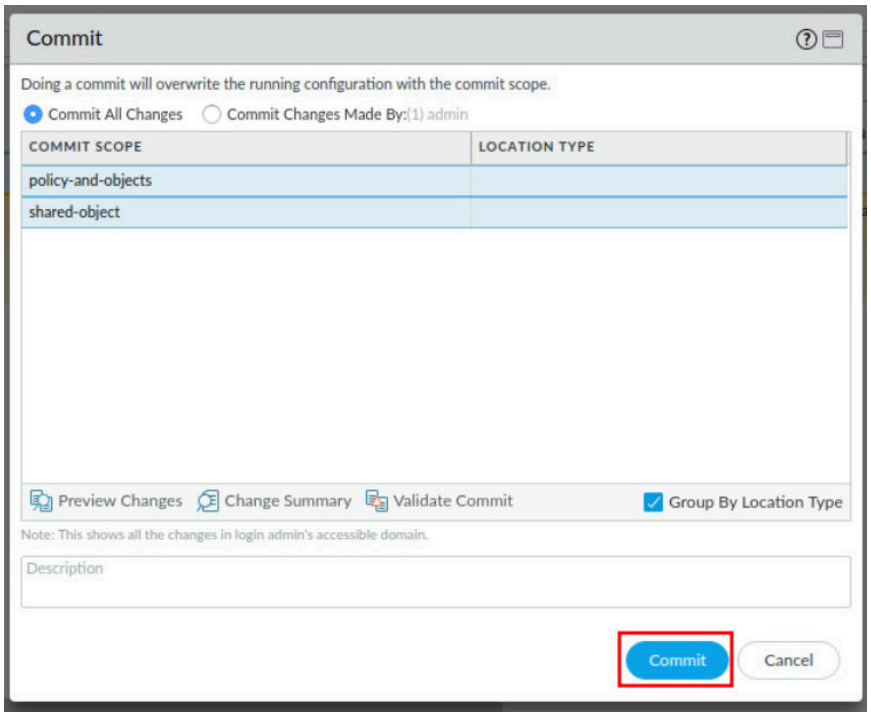


11. In the *Security Policy Rule* window, click on the **Actions** tab. Next, click the checkbox for **Log at Session Start**. Then, select **Syslog Server** in the *Log Forwarding* dropdown. Finally, click **OK**.

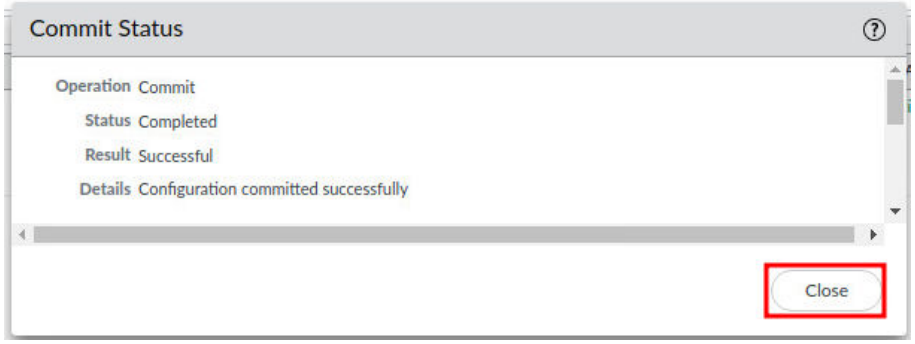


12. Click the **Commit** link located at the top-right of the web interface.

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



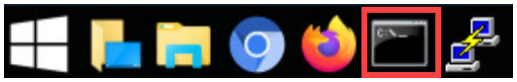
14. When the commit operation successfully completes, click **Close** to continue.



1.2 Verify Syslog Forwarding

In this section, you will connect to the DMZ server and verify that the syslogs are being forwarded.

1. Click on the **Xfce Terminal** icon in the taskbar.



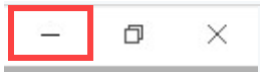
2. In the *CMD* window, ping the DMZ server address by typing `ping -c4 192.168.50.10` and pressing **Enter**.

```
C:\home\lab-user> ping -c4 192.168.50.10
```

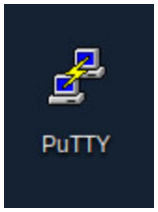
```
C:\home\lab-user> ping -c4 192.168.50.10
PING 192.168.50.10 (192.168.50.10) 56(84) bytes of data.
64 bytes from 192.168.50.10: icmp_seq=1 ttl=63 time=40.4 ms
64 bytes from 192.168.50.10: icmp_seq=2 ttl=63 time=0.785 ms
64 bytes from 192.168.50.10: icmp_seq=3 ttl=63 time=1.01 ms
64 bytes from 192.168.50.10: icmp_seq=4 ttl=63 time=0.862 ms

--- 192.168.50.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
rtt min/avg/max/mdev = 0.785/10.770/40.416/17.116 ms
C:\home\lab-user>
```

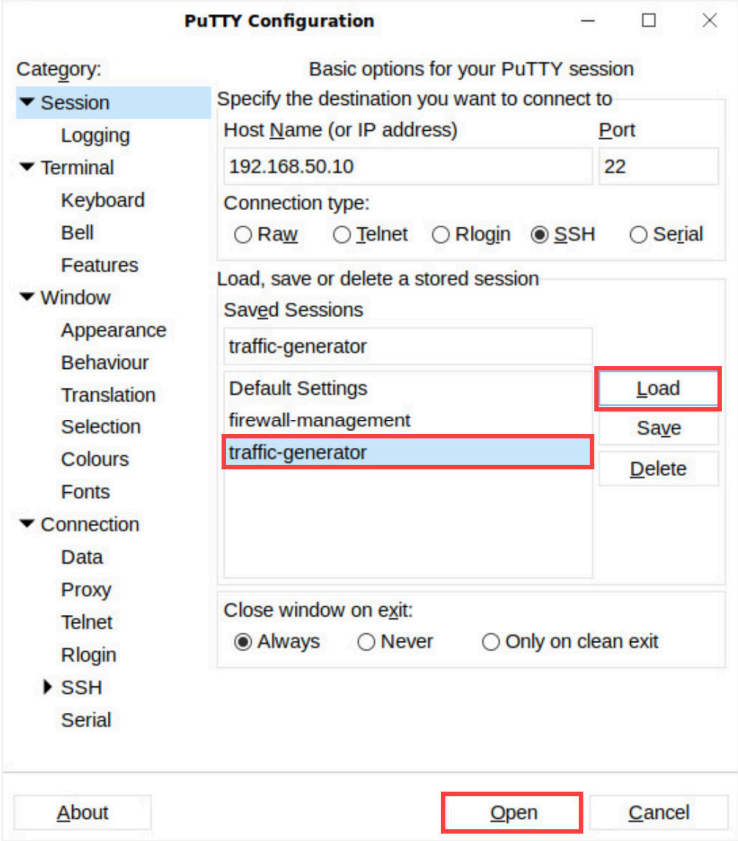
3. To close the *Xfce Terminal* window, type `exit` and press **Enter.**
4. You will need to generate traffic for the Firewall to populate the logs. Minimize *Chromium* in the upper-right corner.



5. Double-click the **PuTTY** application on the desktop.



6. From the *PuTTy Configuration* window, select **traffic-generator** from the *Saved Sessions* section. Then, click the **Load** button. Finally, click the **Open** button.



7. At the *login as:* prompt, type `root`. Type `Pal0Alt0!` for the password, and press **Enter**.

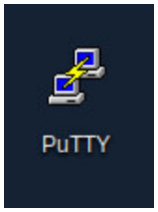
The cursor will not move while you type the password.

8. Type `sh /tg/traffic.sh` and press **Enter**.

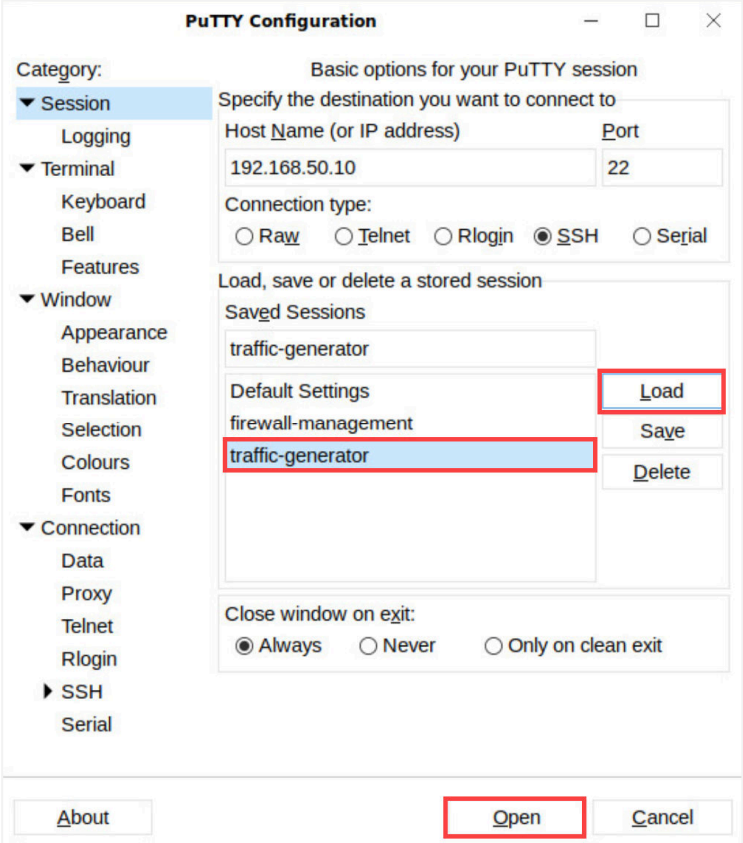
```
[root@pod-dmz ~]# sh /tg/traffic.sh
```

9. Allow the script to generate traffic. Notice it says it will take less than 90 seconds to complete. You may experience different time spans when doing this step. It is important that you allow the *traffic.sh* script to finish.

10. A second **PuTTY** session will need to be opened. To verify traffic for the Firewall, double-click the **PuTTy** icon on the desktop.



11. From the *PuTTY Configuration* window, select **traffic-generator** from the *Saved Sessions* section. Then, click the **Load** button. Finally, click the **Open** button.

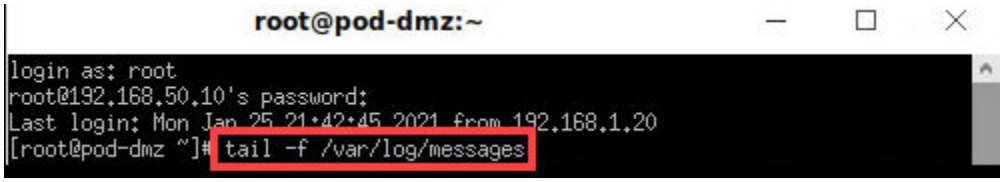


12. At the *login as:* prompt, type `root`. Type `Pal0Alt0!` for the password, and press **Enter**.

Note that the cursor will not move while you type the password.

13. To verify that logs are processing, type `tail -f /var/log/messages` and press **Enter.**

```
[root@pod-dmz ~]# tail -f /var/log/messages
```



By default, syslog stores the files in the **/var/log/messages** file. By utilizing the **`tail -f`** command, you can connect to this file and watch any changes that are occurring.

14. You should see the flow of traffic information occurring. The information to verify within the output should clearly describe the date, source of the syslog data, and information about the traffic.

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

