



SECURITY OPERATIONS FUNDAMENTALS V2

Lab 4: Log Forwarding to Linux

Document Version: **2022-12-23**

Copyright © 2022 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark 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
Objective	3
Lab Topology	4
Lab Settings	5
1 Log Forwarding to Linux.....	6
1.0 Load Lab Configuration	6
1.1 Configure Syslog Monitoring via Palo Alto Firewall	11
1.2 Verify Syslog Forwarding.....	18

Introduction

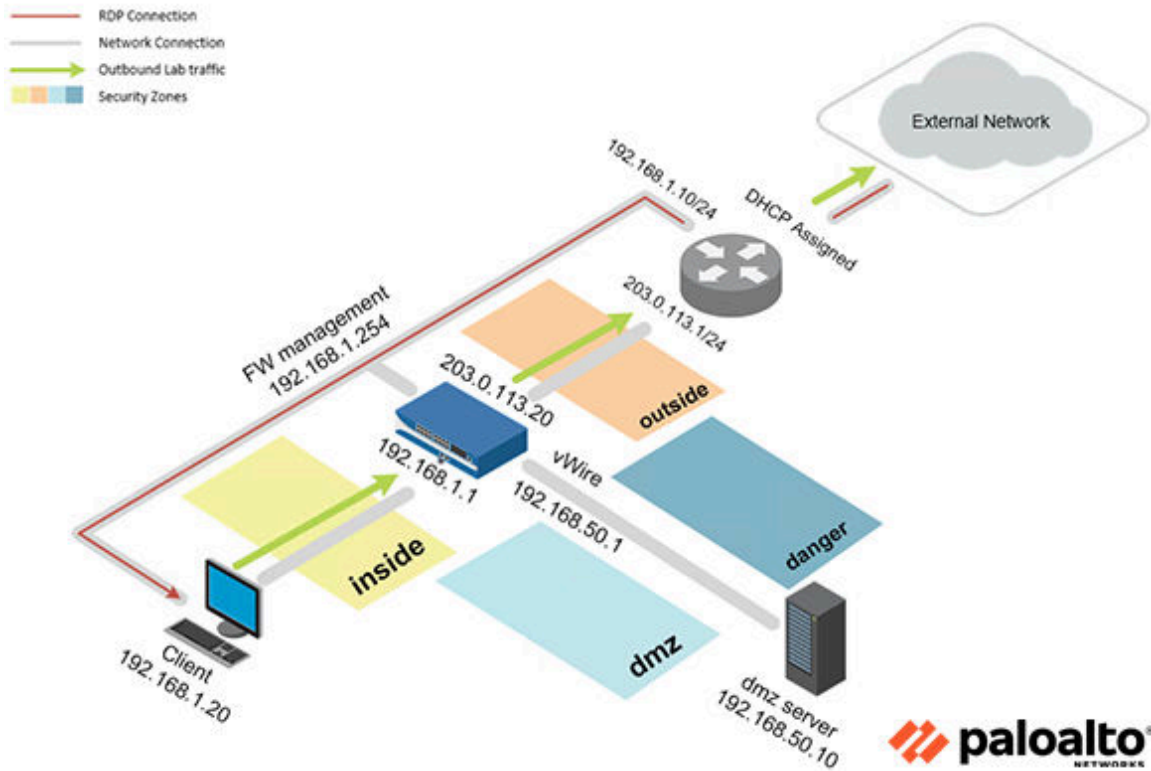
In this lab, you will configure Syslog Monitoring in the Palo Alto Networks Firewall. You will confirm the logs are being forwarded and view the files on the DMZ server.

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.

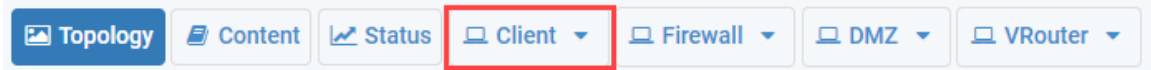
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Pal0Alt0!
DMZ	192.168.50.10	root	Pal0Alt0!
Firewall	192.168.1.254	admin	Pal0Alt0!

1 Log Forwarding to Linux

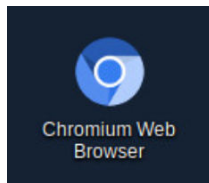
1.0 Load Lab Configuration

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

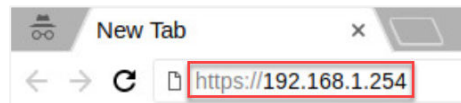
1. Click on the **Client** tab to access the client PC.



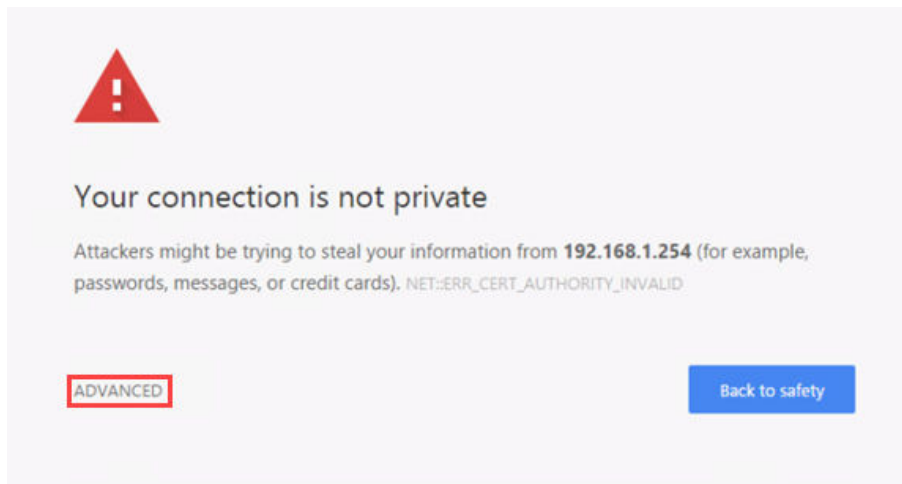
2. Log in to the client PC as username `lab-user`, password `Pa10Alt0!`.
3. Double-click the **Chromium** icon located on the desktop.



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

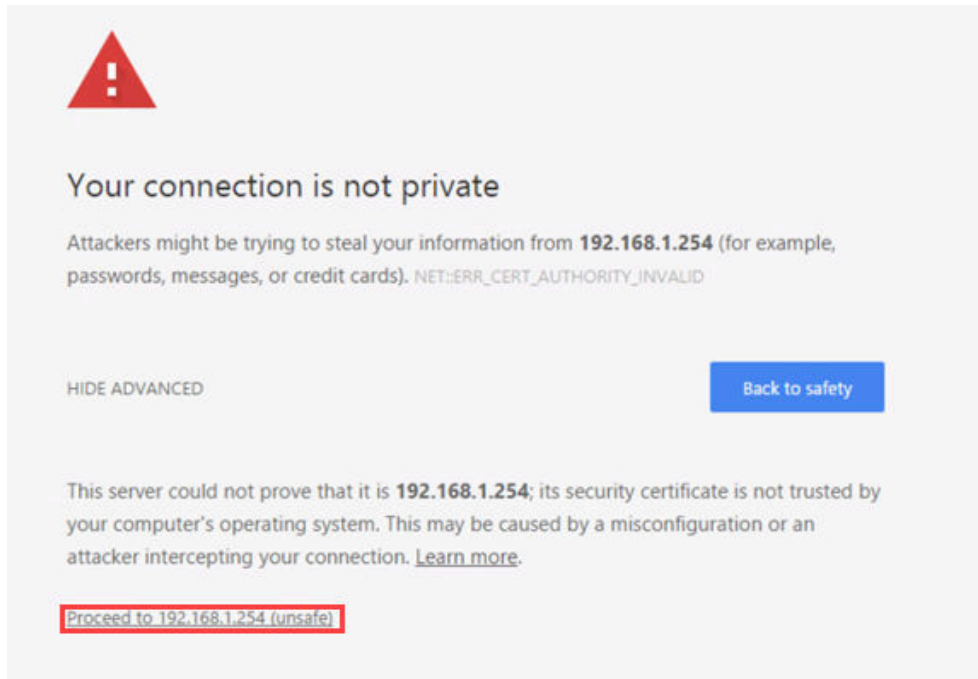


5. You will see a “Your connection is not private” message. Click on the **ADVANCED** link.



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.

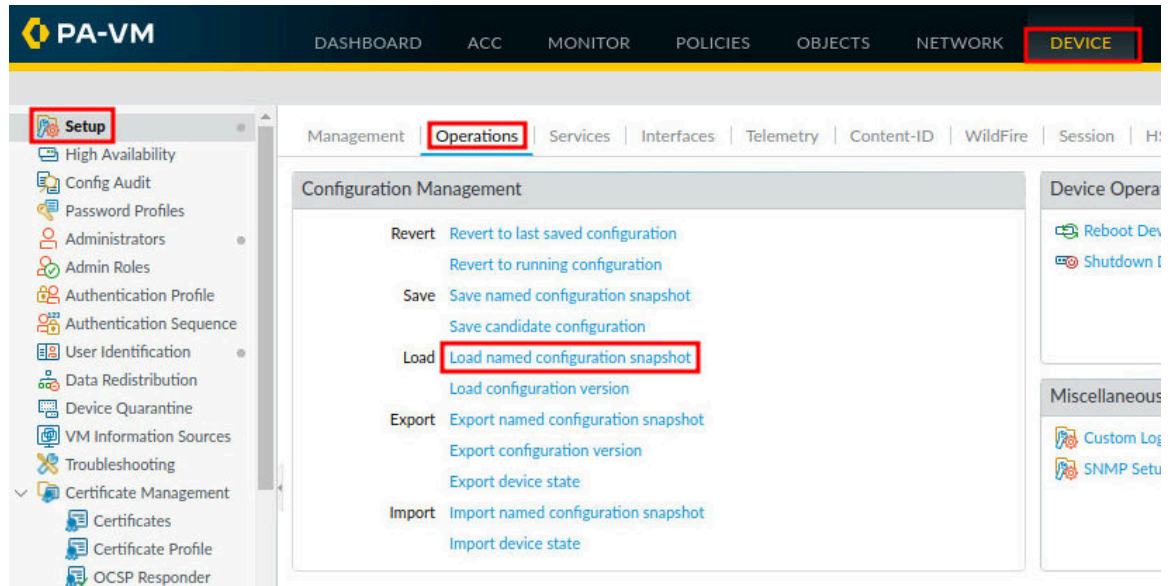
6. Click on **Proceed to 192.168.1.254 (unsafe)**.



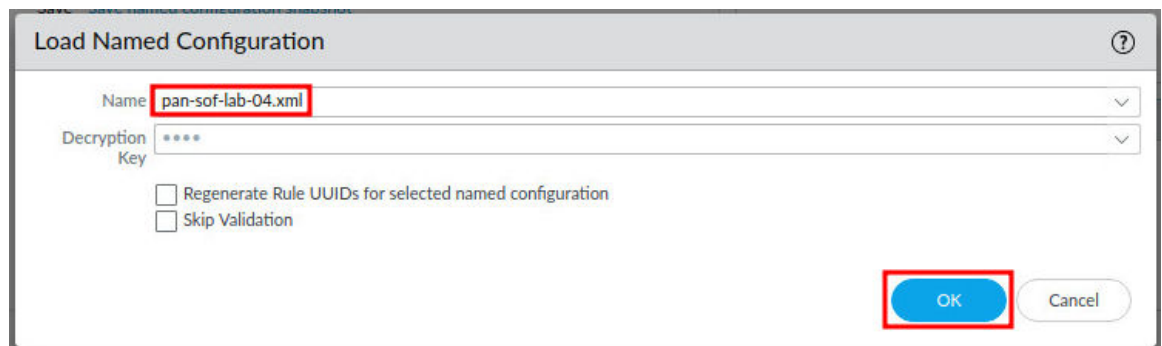
7. Log in to the Firewall web interface as username admin, password Pal0Alt0!.



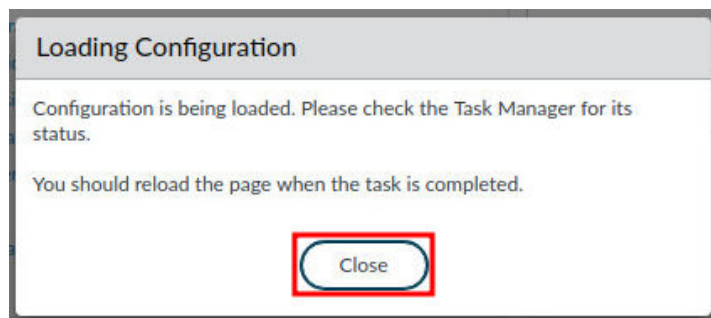
8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load** named configuration snapshot underneath the *Configuration Management* section.



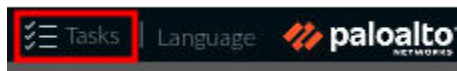
9. In the *Load Named Configuration* window, select **pan-sof-lab-04.xml** from the *Name* dropdown box and click **OK**.



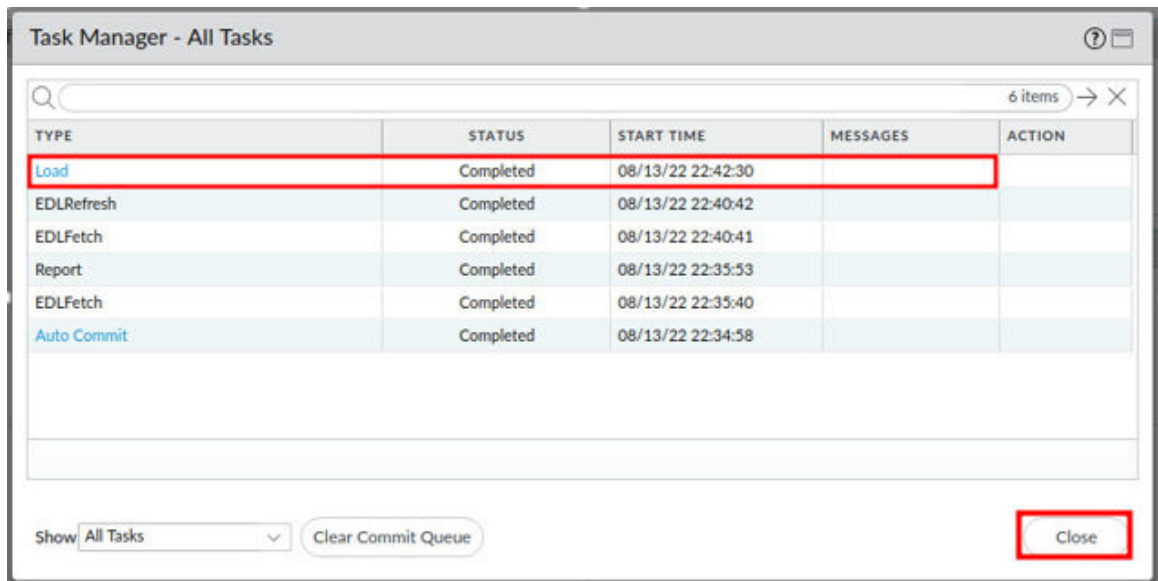
10. In the *Loading Configuration* window, a message will say *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.



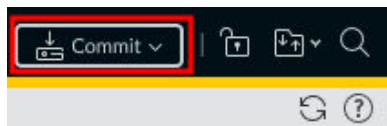
11. Click the **Tasks** icon located at the bottom-right of the web interface.



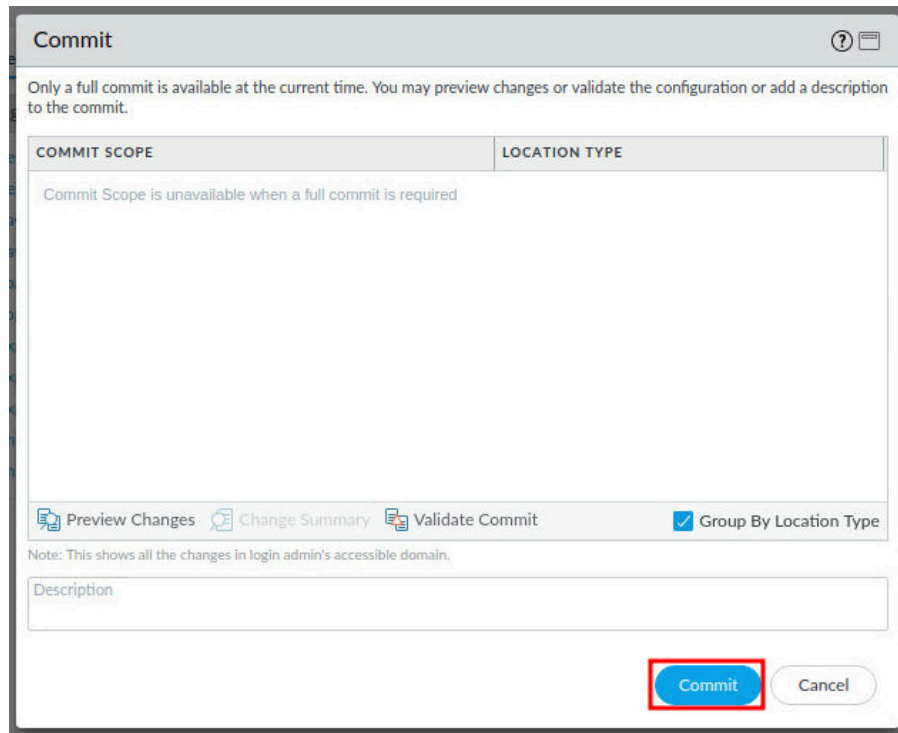
12. In the *Task Manager – All Tasks* window, verify that the *Load* type has successfully completed. Click **Close**.



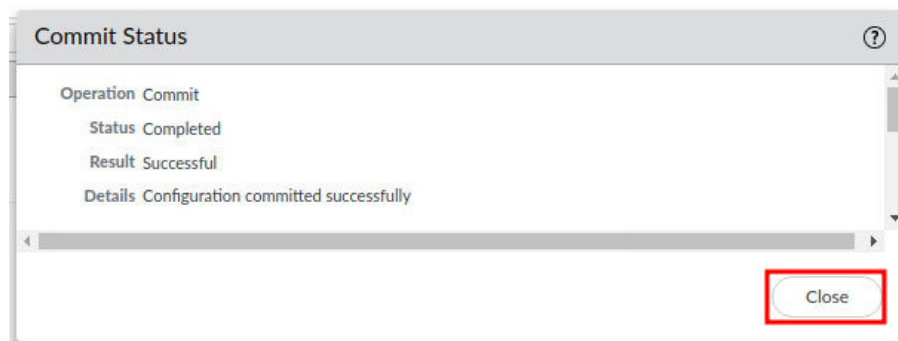
13. Click the **Commit** link located at the top-right of the web interface.



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



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

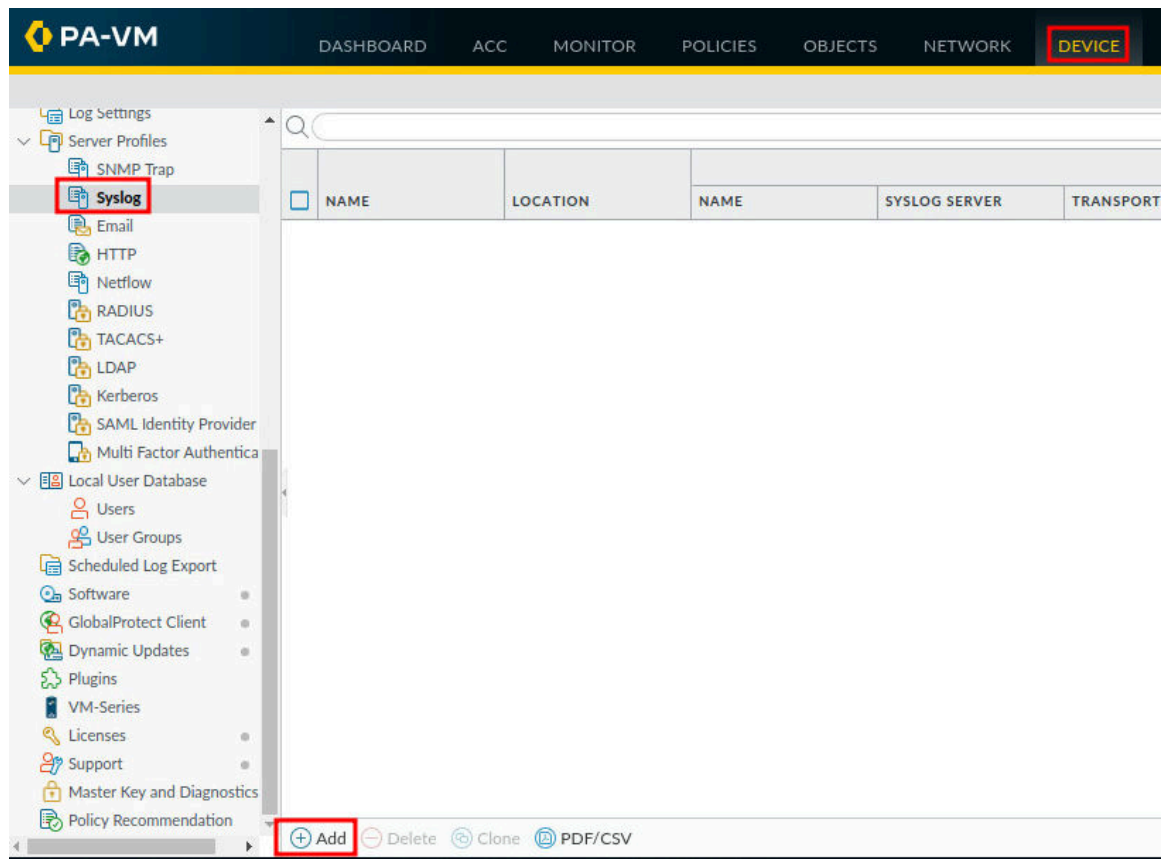


The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

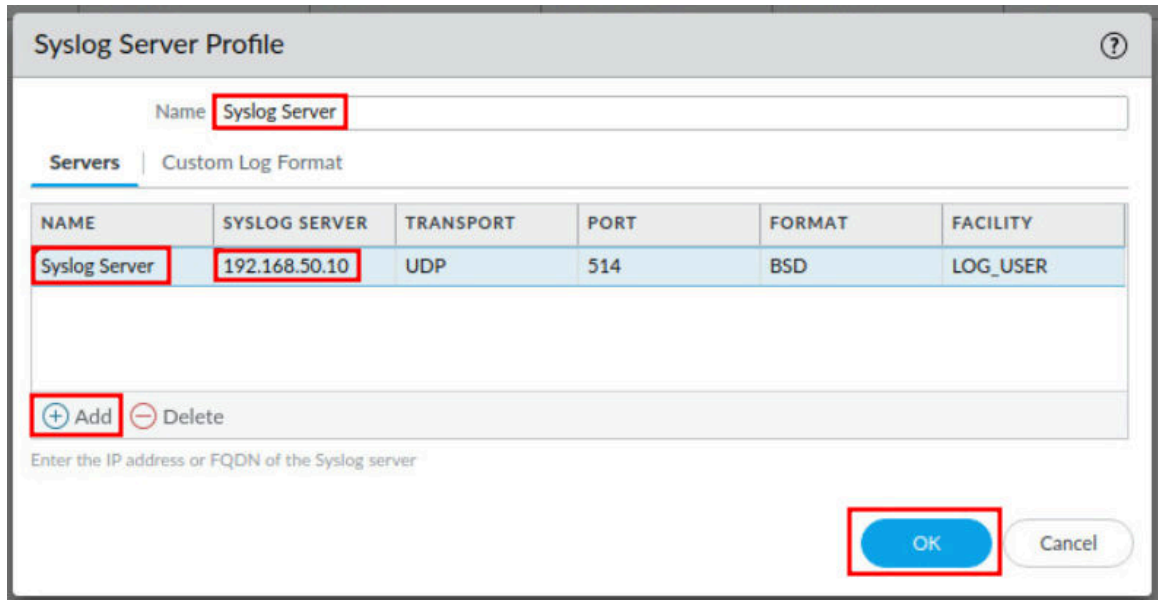
1.1 Configure Syslog Monitoring via Palo Alto Firewall

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**.

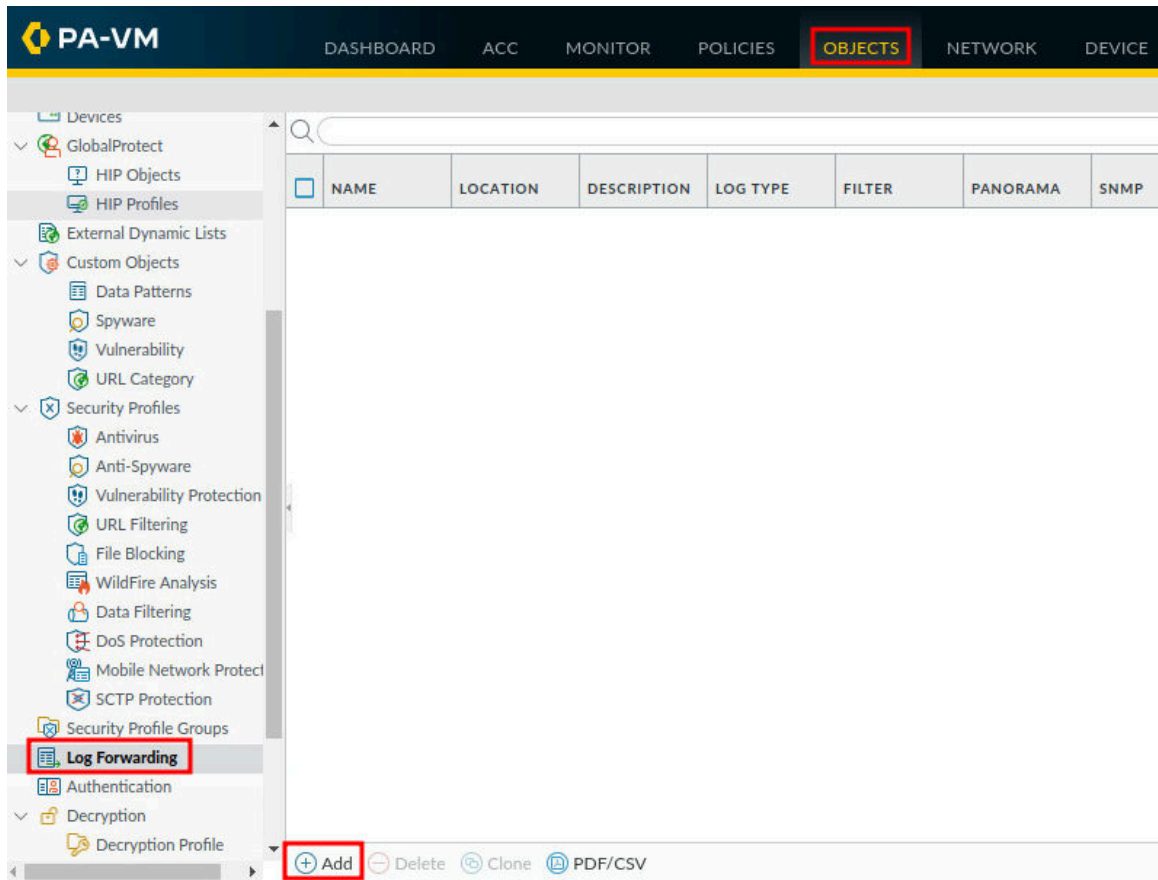


The Syslog Server Profile window shows the configuration for a Syslog server. The Name field is set to "Syslog Server". The Servers tab is active, displaying a table with the following data:

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
Syslog Server	192.168.50.10	UDP	514	BSD	LOG_USER

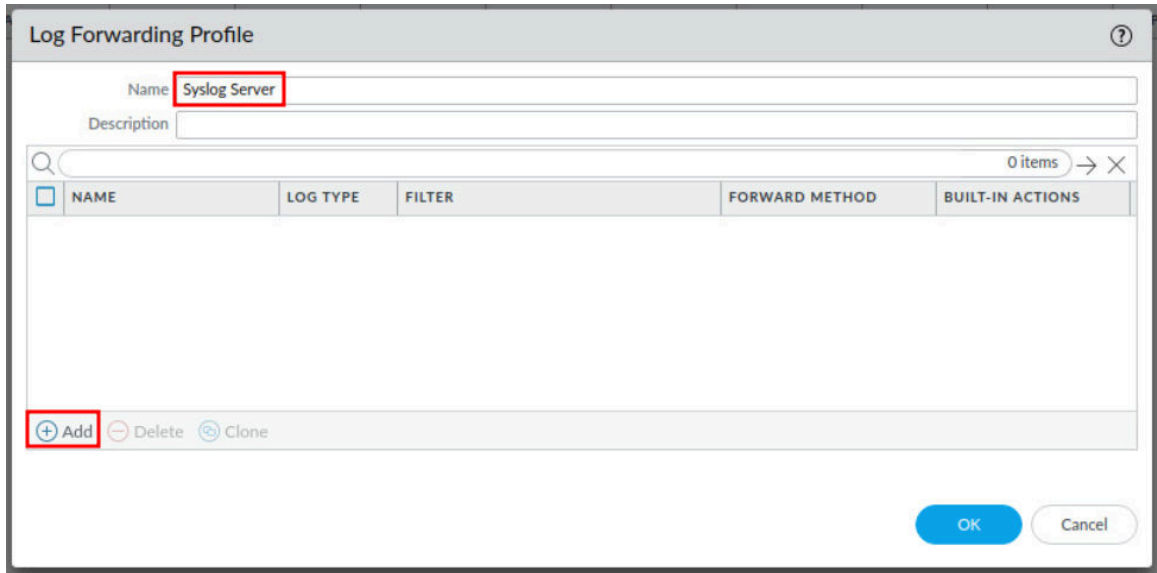
Below the table, there is an "Add" button (indicated by a red box) and a "Delete" button. A text prompt below the buttons says "Enter the IP address or FQDN of the Syslog server". At the bottom right, there are "OK" and "Cancel" buttons, with the "OK" button highlighted by a red box.

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



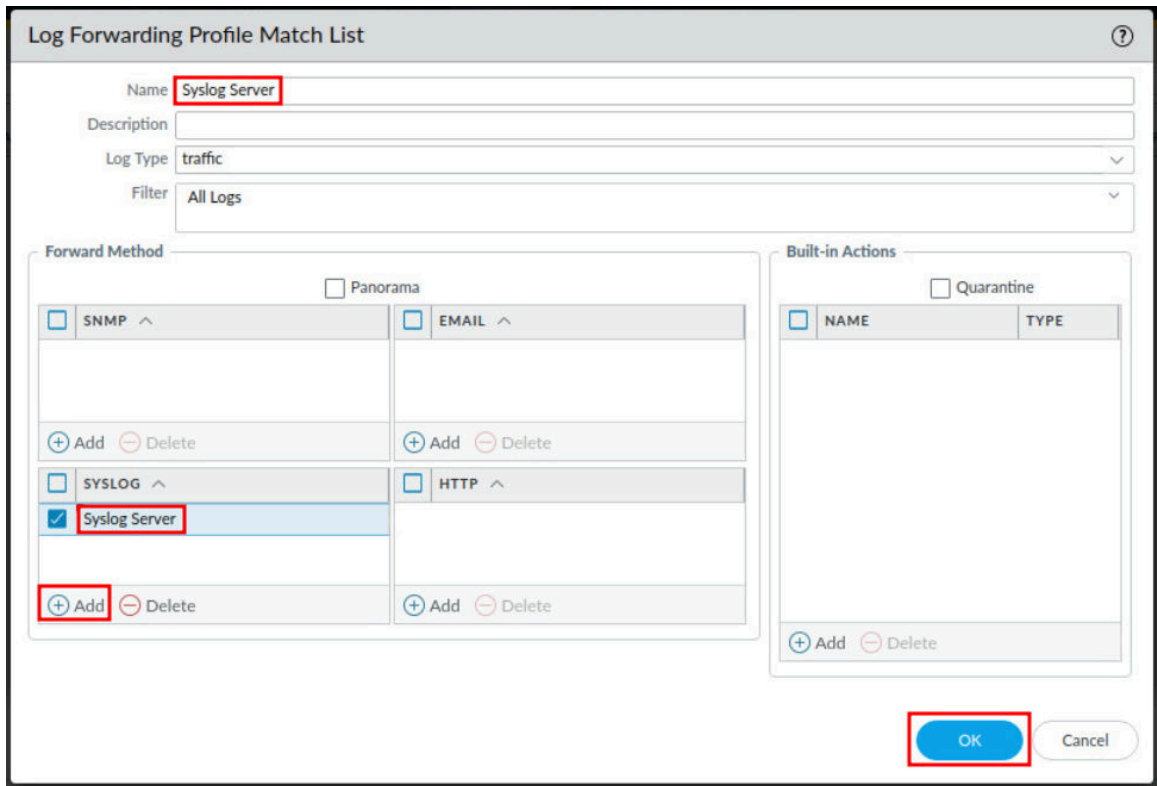
The PA-VM interface shows the navigation menu on the left with "Log Forwarding" highlighted by a red box. The main pane displays a table with the following columns: NAME, LOCATION, DESCRIPTION, LOG TYPE, FILTER, PANORAMA, and SNMP. At the bottom of the main pane, there is an "Add" button (indicated by a red box) and other buttons: "Delete", "Clone", and "PDF/CSV".

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



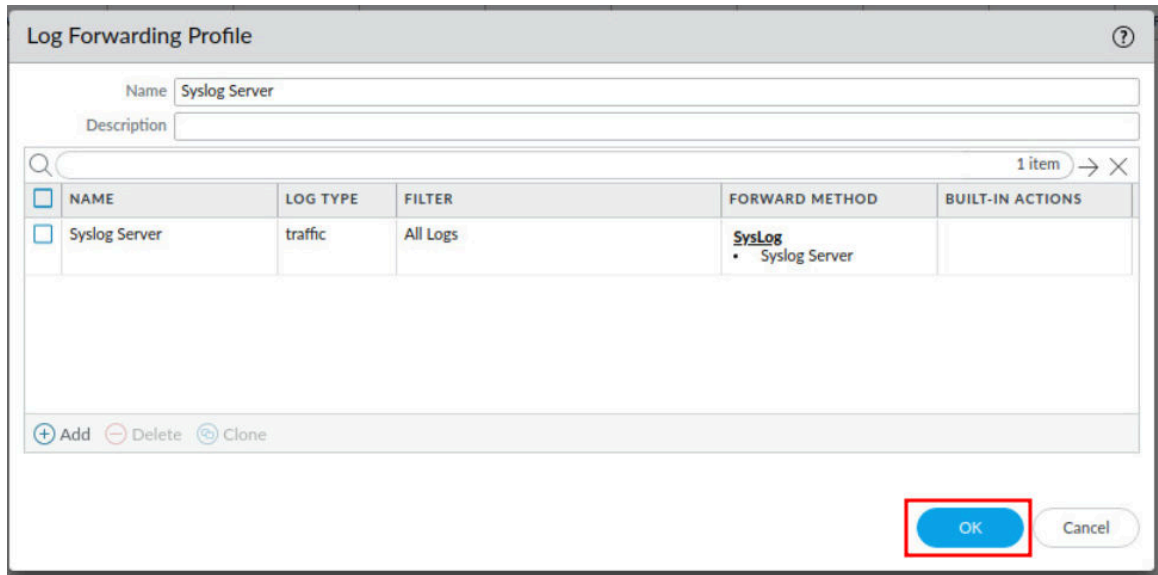
The screenshot shows the 'Log Forwarding Profile' window. The 'Name' field contains 'Syslog Server'. Below the fields is a table with columns: NAME, LOG TYPE, FILTER, FORWARD METHOD, and BUILT-IN ACTIONS. The table is currently empty. At the bottom left, there are three buttons: '+ Add', '- Delete', and 'Clone'. The '+ Add' button is highlighted with a red box. At the bottom right, there are 'OK' and 'Cancel' buttons.

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**.



The screenshot shows the 'Log Forwarding Profile Match List' window. The 'Name' field contains 'Syslog Server'. The 'Log Type' dropdown is set to 'traffic' and the 'Filter' dropdown is set to 'All Logs'. Below these are two sections: 'Forward Method' and 'Built-in Actions'. The 'Forward Method' section has a 'Panorama' checkbox and a table with columns: NAME, LOG TYPE, FILTER, FORWARD METHOD, and BUILT-IN ACTIONS. The table has two rows: 'SNMP' and 'SYSLOG'. The 'SYSLOG' row is expanded, showing a list of profiles. The 'Syslog Server' profile is selected, and the '+ Add' button is highlighted with a red box. The 'Built-in Actions' section has a 'Quarantine' checkbox and a table with columns: NAME and TYPE. The table is currently empty. At the bottom right, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red box.

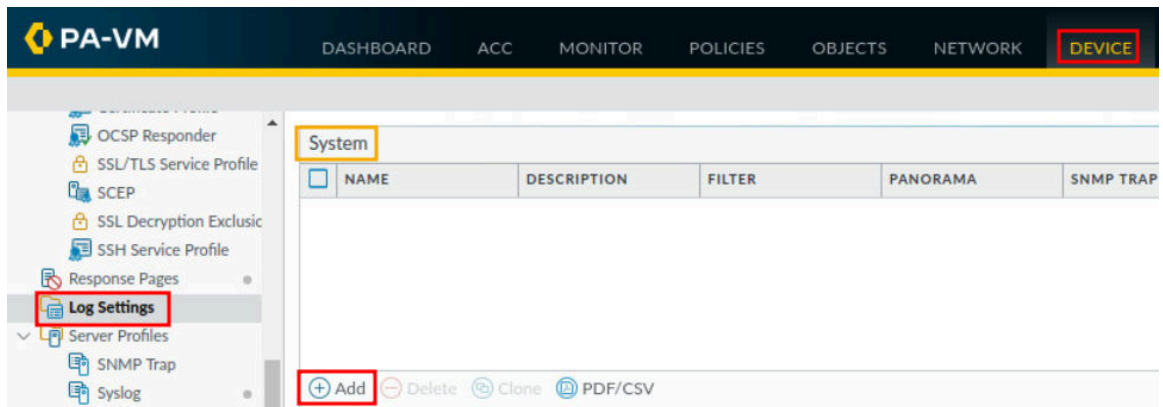
6. Verify that your screen matches the screenshot below, then click **OK**.



The screenshot shows the 'Log Forwarding Profile' configuration window. The 'Name' field is set to 'Syslog Server'. The 'Description' field is empty. Below the fields is a table with one item. The table has columns: NAME, LOG TYPE, FILTER, FORWARD METHOD, and BUILT-IN ACTIONS. The row shows 'Syslog Server' with LOG TYPE 'traffic' and FILTER 'All Logs'. The FORWARD METHOD is 'SysLog' with a sub-item 'Syslog Server'. At the bottom right, the 'OK' button is highlighted with a red box.

NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
Syslog Server	traffic	All Logs	SysLog • Syslog Server	

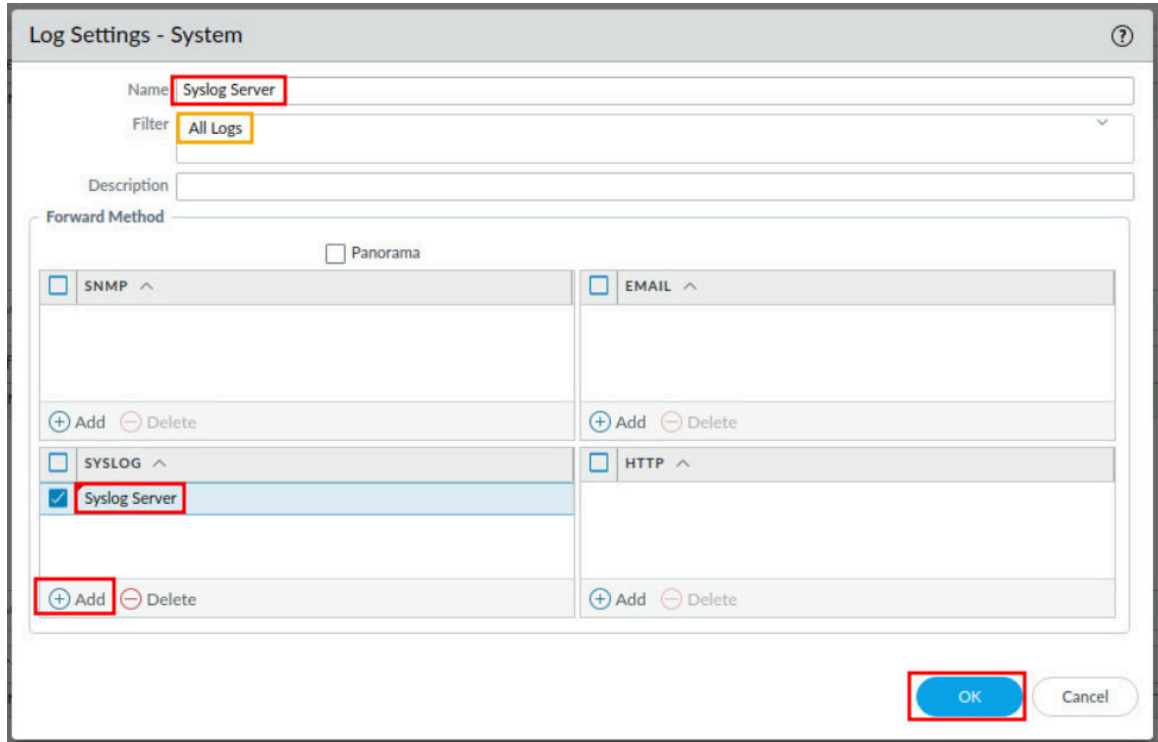
7. Navigate to **Device > Log Settings**, and in the *System* section, click **Add**.



The screenshot shows the PA-VM interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE' (highlighted with a red box). The left sidebar shows 'Log Settings' (highlighted with a red box) under the 'Server Profiles' section. The main content area shows the 'System' section with a table. The table has columns: NAME, DESCRIPTION, FILTER, PANORAMA, and SNMP TRAP. At the bottom left, the 'Add' button is highlighted with a red box.

NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP
------	-------------	--------	----------	-----------

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**.



The screenshot shows the "Log Settings - System" window. The "Name" field is set to "Syslog Server" and the "Filter" dropdown is set to "All Logs". The "Forward Method" section is expanded, showing four categories: SNMP, EMAIL, SYSLOG, and HTTP. Under the SYSLOG category, the "Syslog Server" option is selected. The "Add" button in the bottom left of the SYSLOG section is highlighted. The "OK" button is highlighted in the bottom right corner.

Forward Method	Configuration
SNMP	Empty list with Add/Delete buttons
EMAIL	Empty list with Add/Delete buttons
SYSLOG	Contains "Syslog Server" (checked). Includes Add/Delete buttons.
HTTP	Empty list with Add/Delete buttons

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.

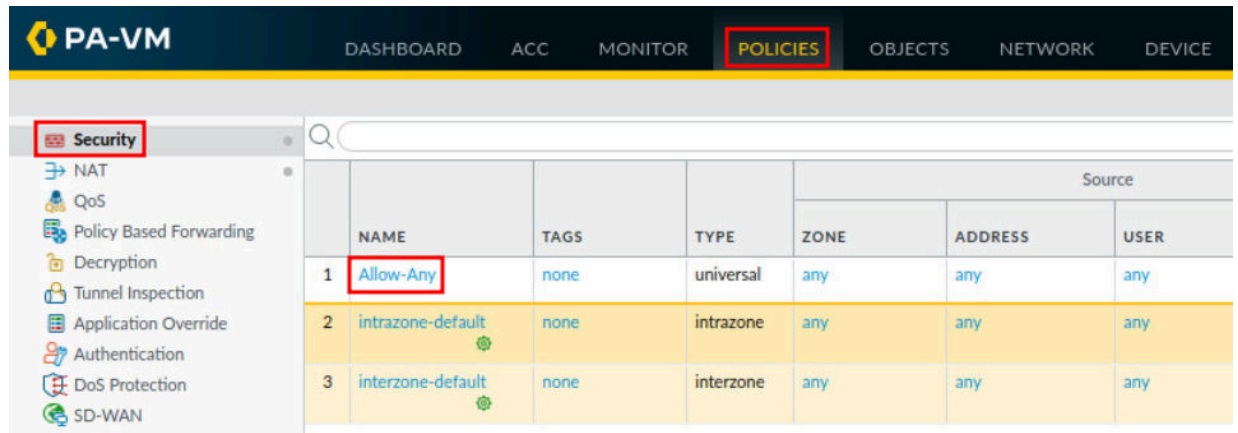
System							
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG
<input type="checkbox"/>	Syslog Server		All Logs	<input type="checkbox"/>			Syslog Server
<div> + Add - Delete 🔄 Clone 📄 PDF/CSV </div>							

Configuration							
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG
<input type="checkbox"/>	Syslog Server		All Logs	<input type="checkbox"/>			Syslog Server
<div> + Add - Delete 🔄 Clone 📄 PDF/CSV </div>							

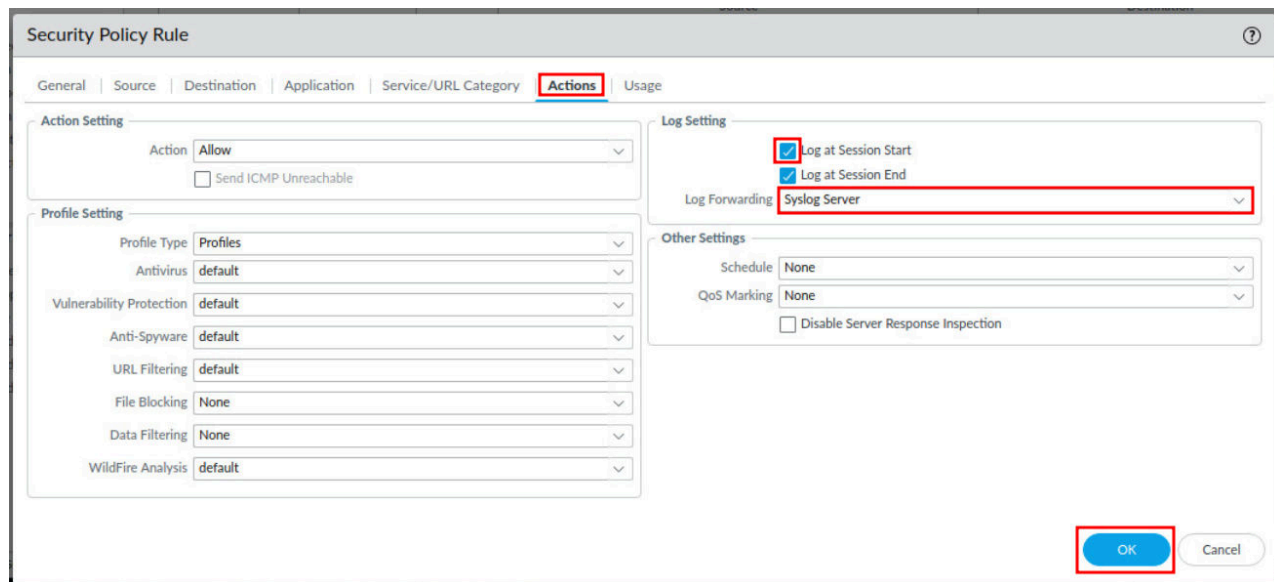
User-ID							
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG
<input type="checkbox"/>	Syslog Server		All Logs	<input type="checkbox"/>			Syslog Server
<div> + Add - Delete 🔄 Clone 📄 PDF/CSV </div>							

HIP Match							
<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP	EMAIL	SYSLOG
<input type="checkbox"/>	Syslog Server		All Logs	<input type="checkbox"/>			Syslog Server
<div> + Add - Delete 🔄 Clone 📄 PDF/CSV </div>							

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



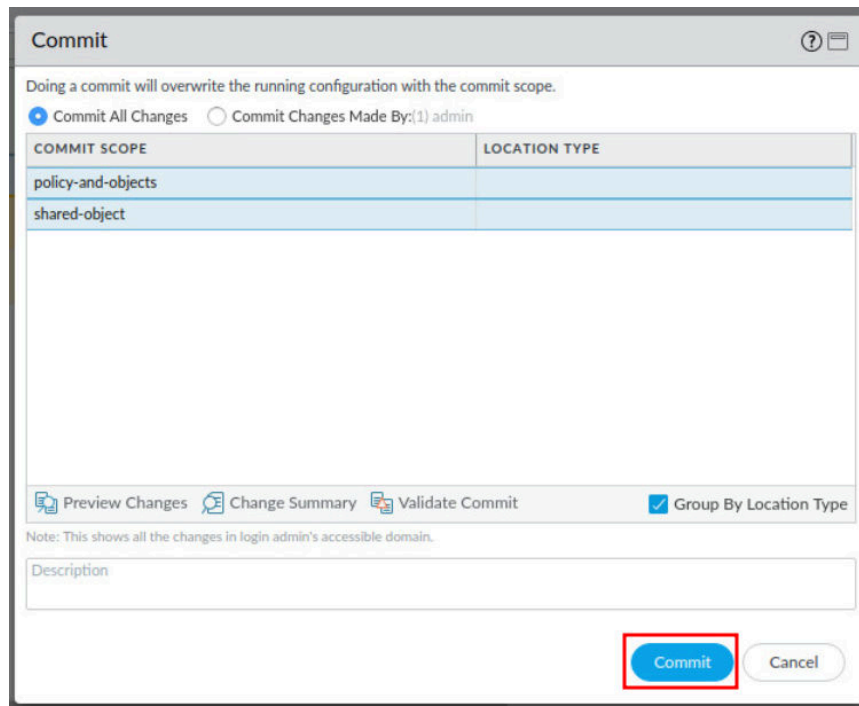
11. In the *Security Policy Rule* window, click on the **Actions** tab. Next, click the checkbox for **Log at Session Start**. Then, select **Syslog Server** in the *Log Forwarding* dropdown. Finally, click **OK**.



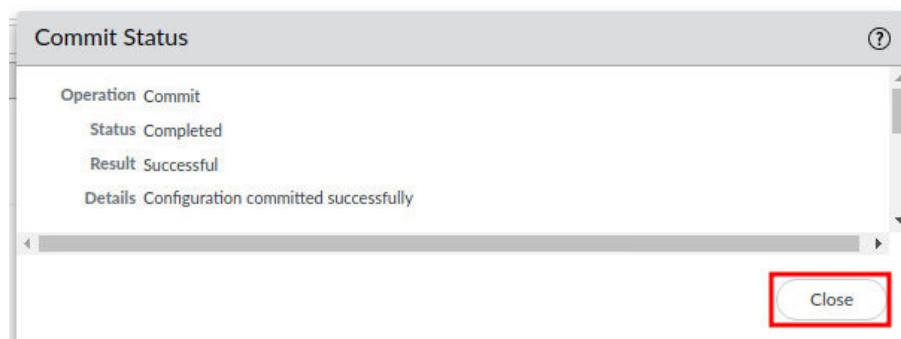
12. Click the **Commit** link located at the top-right of the web interface.



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>
```

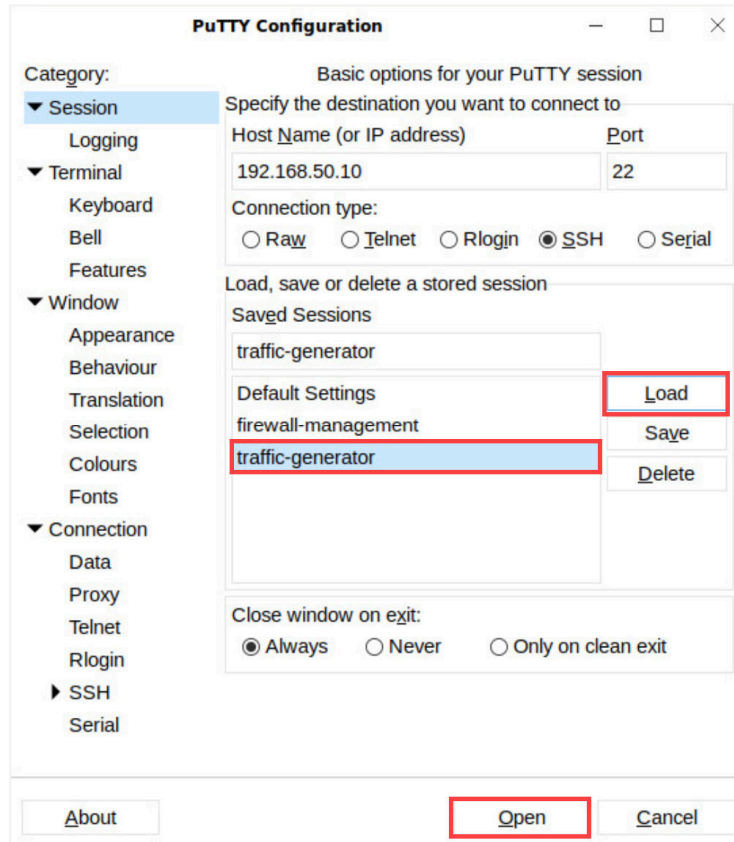
3. To close the *Xfce Terminal* window, type `exit` and press **Enter**.
4. You will need to generate traffic for the Firewall to populate the logs. Minimize *Chromium* in the upper-right corner.



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.



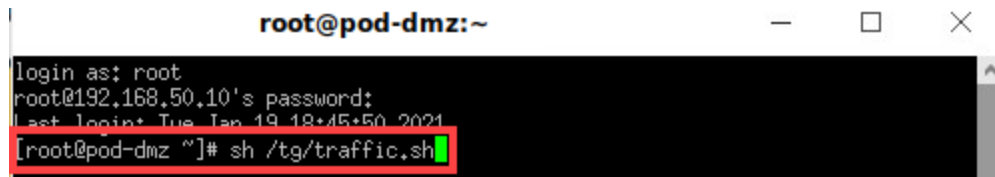
7. At the *login as:* prompt, type **root**. Type **Pa10Alt0!** for the password, and press **Enter**.



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
```



```
root@pod-dmz:~  
login as: root  
root@192.168.50.10's password:  
Last login: Tue Jan 19 18:45:50 2021  
[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.

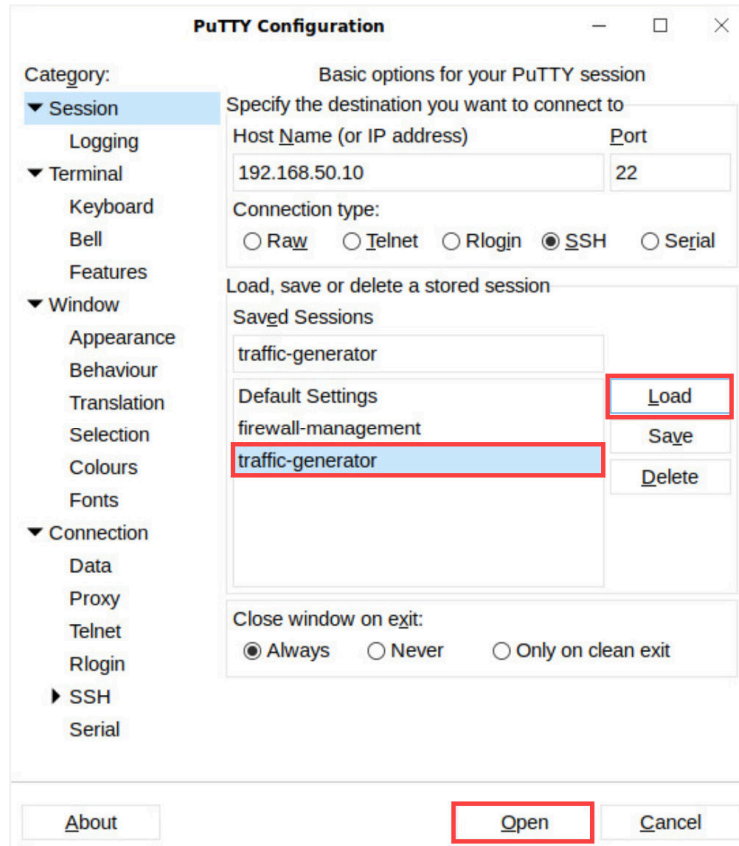


```
root@pod-dmz:~  
login as: root  
root@192.168.50.10's password:  
Last login: Mon Jan 25 21:35:44 2021  
[root@pod-dmz ~]# sh /tg/traffic.sh  
-- THIS WILL TAKE LESS THAN 90 SECONDS --
```

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 **Pa10Alt0!** 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
```

```
root@pod-dmz:~  
login as: root  
root@192.168.50.10's password:  
Last login: Mon Jan 25 21:42:45 2021 from 192.168.1.20  
[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.

```
root@pod-dmz:~  
Jan 25 21:13:06 lab-firewall.lab.local 1,2021/01/25 21:13:05,015351000056630,TRAFFIC,start,2305,2021/01/25 21:13:05,192.168.3.131,  
72.14.213.102,0,0,0,0,0,0,Allow-Any,,,google-base,vssys1,danger,danger,ethernet1/5,ethernet1/4,Syslog Server,2021/01/25 21:13  
:05,48641,1,55950,80,0,0,x68,tcp,allow,1058,1058,0,2,2021/01/25 20:11:05,3720,search-engines,0,119197,0x0,192.168.0.0-192.168.25  
5,255,United States,0,2,0,tcp-reuse,0,0,0,0,,lab-firewall,from-policy,,,0,0,,N/A,0,0,0,0,3834b9ba-2844-4636-a358-8c5f4df6eb1e,0,  
  
Jan 25 21:13:06 lab-firewall.lab.local 1,2021/01/25 21:13:05,015351000056630,TRAFFIC,start,2305,2021/01/25 21:13:05,10.2,15,91,  
103,140,2,0,0,0,0,0,0,Allow-Any,,,web-browsing,vssys1,danger,danger,ethernet1/4,ethernet1/5,Syslog Server,2021/01/25 21:13:05,  
20874,1,2546,80,0,0,0,x68,tcp,allow,578,578,0,1,2021/01/25 20:00:22,4363,business-and-economy,0,119198,0x0,10.0,0,0,10-10.255,255  
5,France,0,1,0,tcp-reuse,0,0,0,0,,lab-firewall,from-policy,,,0,0,,N/A,0,0,0,0,3834b9ba-2844-4636-a358-8c5f4df6eb1e,0,,,,,  
Jan 25 21:13:06 lab-firewall.lab.local 1,2021/01/25 21:13:05,015351000056630,TRAFFIC,start,2305,2021/01/25 21:13:05,192.168.204.1  
34,64,202,116,124,0,0,0,0,0,0,Allow-Any,,,web-browsing,vssys1,danger,danger,ethernet1/4,ethernet1/5,Syslog Server,2021/01/25 2  
1:13:05,405,1,49221,80,0,0,0,x68,tcp,allow,312,312,0,1,2021/01/25 19:59:33,4412,high-risk,0,119199,0x0,192.168.0.0-192.168.255,255  
5,United States,0,1,0,tcp-reuse,0,0,0,0,,lab-firewall,from-policy,,,0,0,,N/A,0,0,0,0,3834b9ba-2844-4636-a358-8c5f4df6eb1e,0,0,,,,,  
  
Jan 25 21:13:06 lab-firewall.lab.local 1,2021/01/25 21:13:05,015351000056630,TRAFFIC,start,2305,2021/01/25 21:13:05,10.2,15,96,  
17,8,49,0,0,0,0,0,0,0,Allow-Any,,,web-browsing,vssys1,danger,danger,ethernet1/4,ethernet1/5,Syslog Server,2021/01/25 21:13:05,98  
7,1,2547,5480,0,0,0,x100068,tcp,allow,669,669,0,3,2021/01/25 20:00:39,4346,business-and-economy,0,119200,0x0,10.0,0,0,10-10.255,255,2  
55,United States,0,3,0,tcp-reuse,0,0,0,0,,lab-firewall,from-policy,,,0,0,,N/A,0,0,0,0,3834b9ba-2844-4636-a358-8c5f4df6eb1e,0,0,,  
,,,,,  
Jan 25 21:13:06 lab-firewall.lab.local 1,2021/01/25 21:13:05,015351000056630,TRAFFIC,start,2305,2021/01/25 21:13:05,10.2,15,91,  
103,140,2,0,0,0,0,0,0,0,Allow-Any,,,web-browsing,vssys1,danger,danger,ethernet1/4,ethernet1/5,Syslog Server,2021/01/25 21:13:05,  
731,1,2546,5480,0,0,0,x100068,tcp,allow,638,638,0,2,2021/01/25 20:00:38,4347,business-and-economy,0,119201,0x0,10.0,0,0,10-10.255,255  
2,55,France,0,2,0,tcp-reuse,0,0,0,0,,lab-firewall,from-policy,,,0,0,,N/A,0,0,0,0,3834b9ba-2844-4636-a358-8c5f4df6eb1e,0,0,,,,,
```

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