

# Palo Alto Firewall Syslog Filter Documentation

## 1. Introduction

This guide outlines how to configure **Syslog filters** on Palo Alto Networks firewalls to control which logs are sent to external Syslog servers. Proper filtering reduces noise, focuses on relevant events, and improves SIEM performance.

## 2. Syslog Overview

Syslog is a protocol used to send logs from network devices to centralized logging systems. Palo Alto firewalls support syslog forwarding for various log types: **traffic**, **threat**, **system**, and **configuration**.

## 3. Components Involved

Component	Description
Syslog Server Profile	Defines the destination server and syslog transport type
Log Forwarding Profile	Specifies what logs to forward and to whom
Security Policy	Determines when logs are generated and which are forwarded

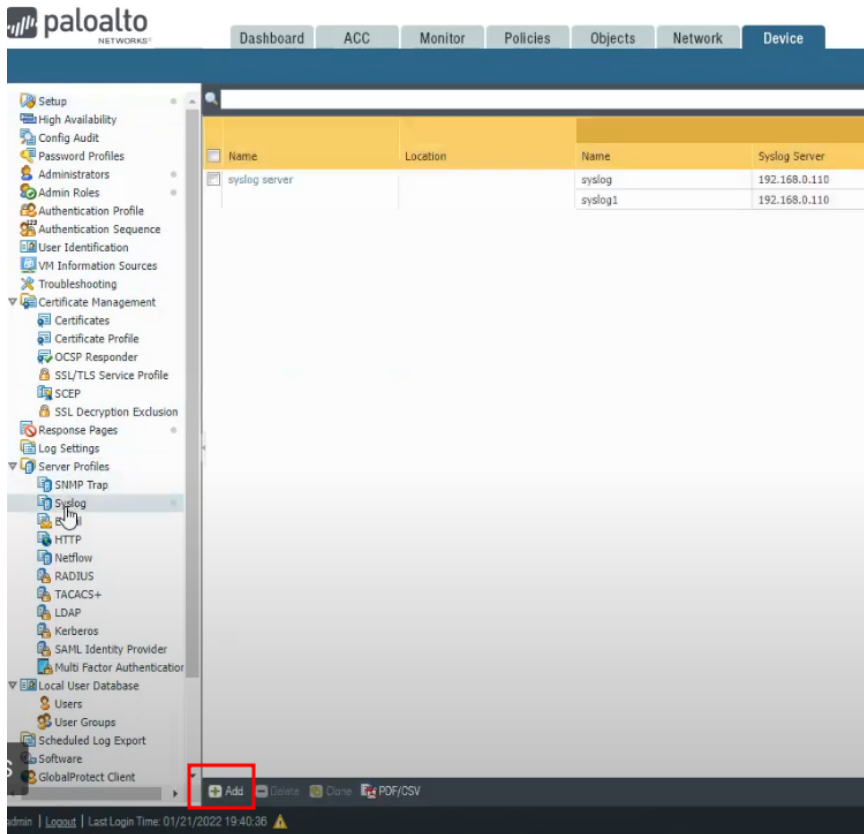
## 4. Configuration Steps

### 4.1 Create Syslog Server Profile

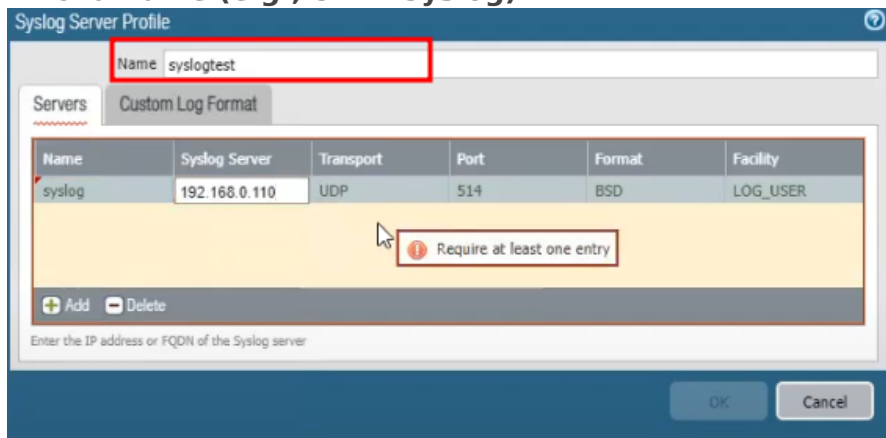
Navigate to: **Device > Server Profiles > Syslog**

## Steps:

1. Click **Add** to create a new profile.

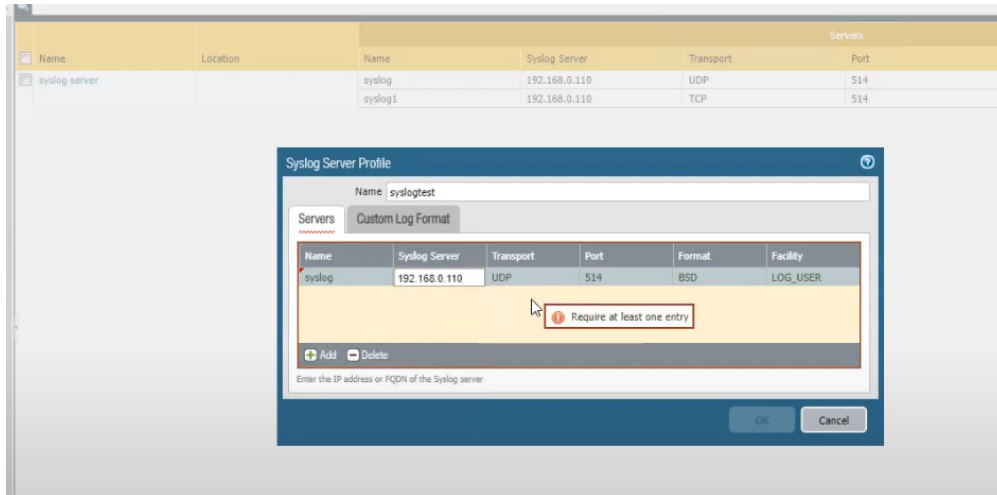


2. Enter a **Name (e.g., SIEM-Syslog)**.



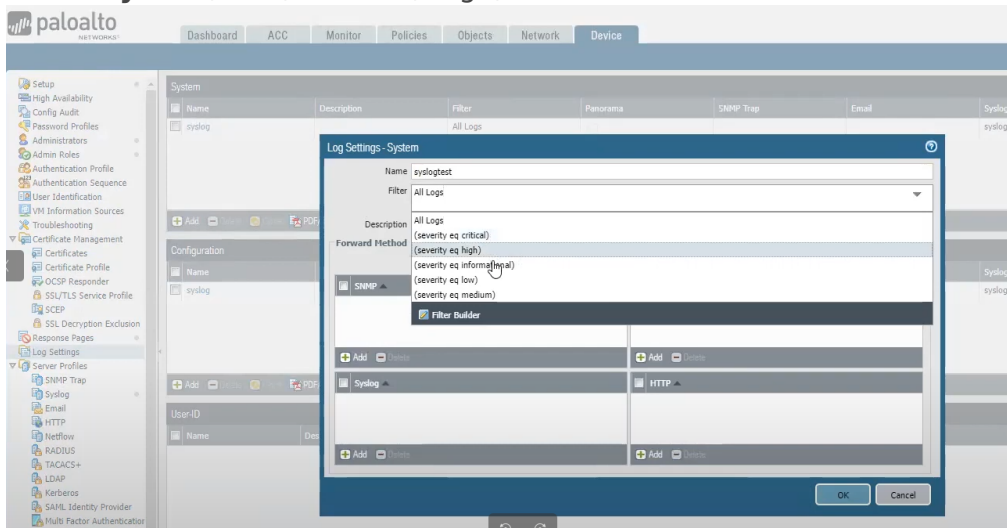
3. Under **Syslog Server**, click **Add** and enter:
  - **Name:** e.g., SIEM-Server
  - **Server:** IP or hostname of your syslog server
  - **Transport:** UDP, TCP, or SSL
  - **Port:** Default is 514 (UDP)
  - **Facility:** e.g., local4

- **Format:** BSD or IETF



4. (Optional) Add a **Filter** to specify:

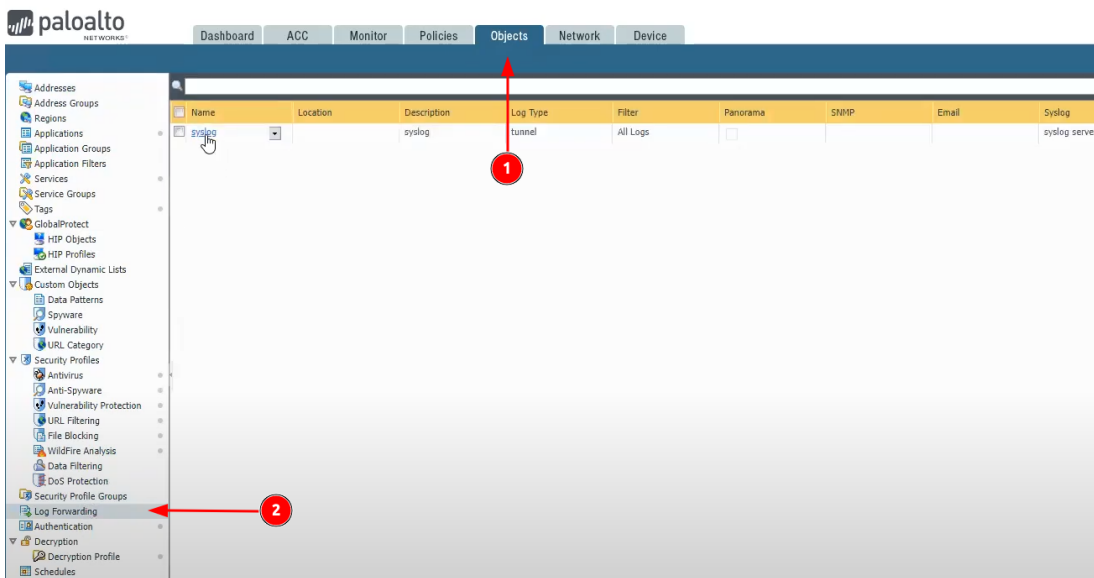
- **Log Type:** Threat, Traffic, System, Config
- **Severity:** Info, Low, Medium, High, Critical



5. Click **OK**

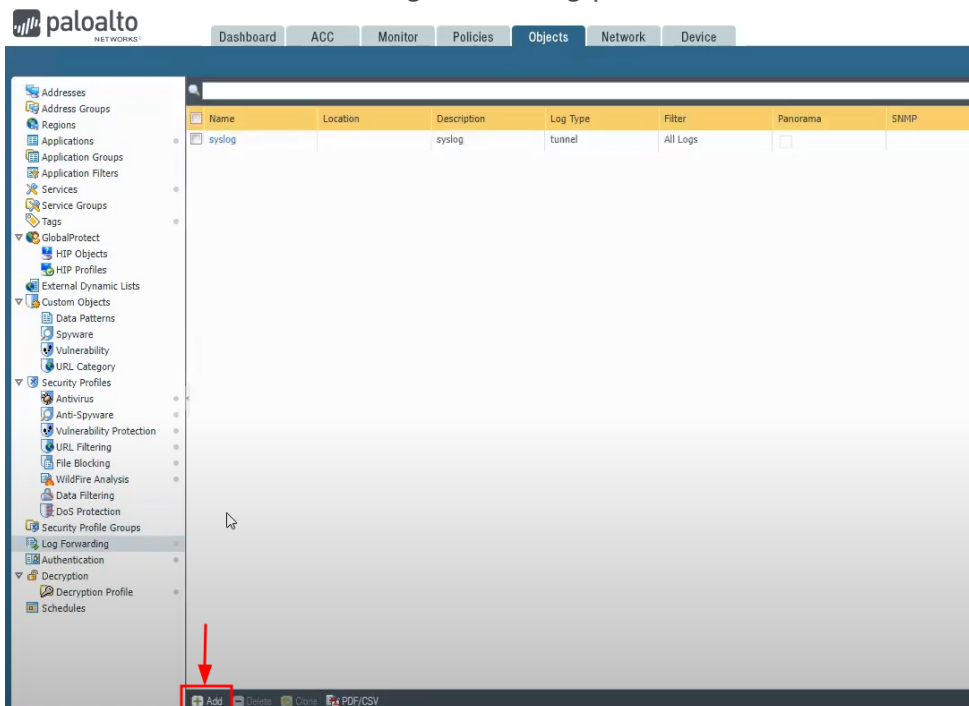
## 4.2 Create Log Forwarding Profile

Navigate to: **Objects > Log Forwarding**

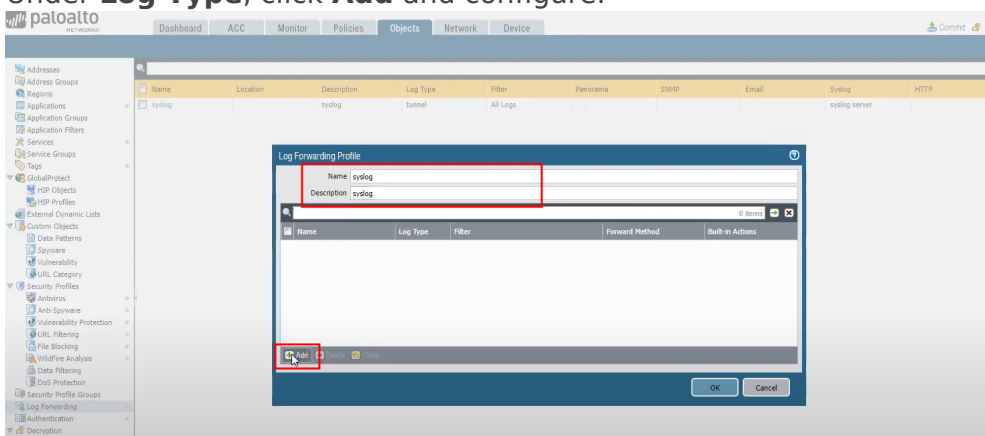


## Steps:

1. Click **Add** to create a new log forwarding profile.



2. Name it (example: syslog)
3. Under **Log Type**, click **Add** and configure:



- **Log Type:** Select Threat or Traffic

Log Forwarding Profile Match List

Name: syslogprofile

Description: syslog

Log Type: traffic

Filter: data

Forward Method: syslog

Buttons: Add, Delete, Syslog, HTTP, Add, Delete, Add, Delete

OK Cancel

- **Filter** (optional): For example, (severity eq high)
- **Forward Method:** Select the Syslog Server Profile you created, click **Add** then select the one you **created**

4. Click **OK**

Log Forwarding Profile Match List

Name: syslogprofile

Description: syslog

Log Type: traffic

Filter: All Logs

Forward Method: Syslog

Buttons: Add, Delete, Syslog, HTTP, Add, Delete, Add, Delete

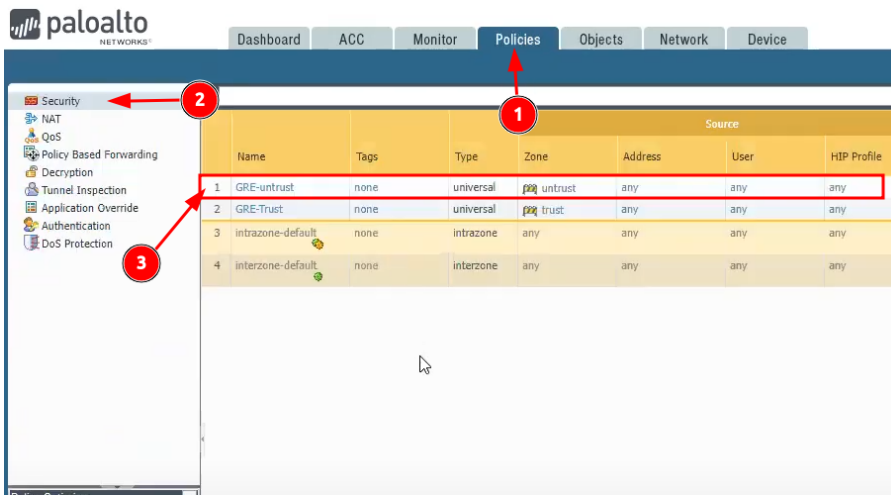
OK Cancel

1

2

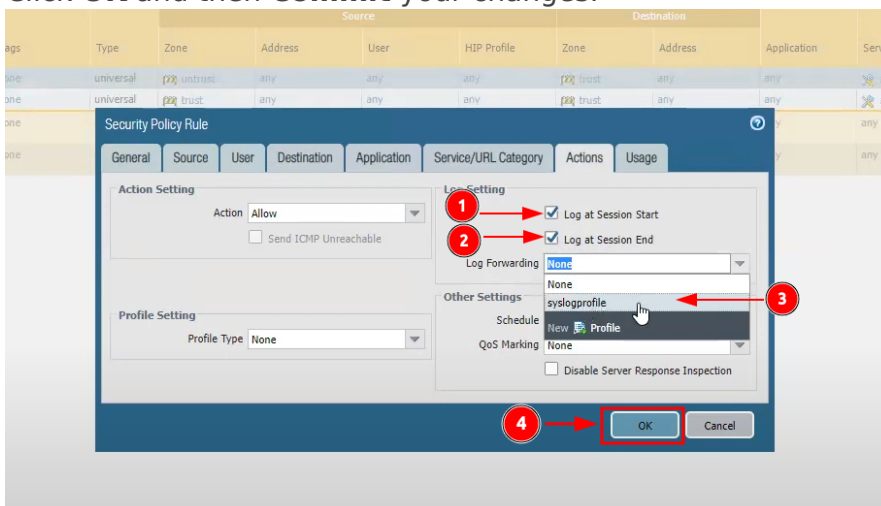
## 4.3 Apply Log Forwarding to Security Policy

Navigate to: **Policies > Security**



## Steps:

1. Locate and **edit** the security policy you want to apply logging to.
2. Click the **Actions** tab.
3. In the **Log Forwarding** field, select the log forwarding profile you created.
4. (Optional) Enable logging at session start/end.
5. Click **OK** and then **Commit** your changes.



Reference Links: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring>

Reference Video: <https://www.youtube.com/watch?v=ftR3DU2MtjY&t=137s>

Revision #11

Created 18 June 2025 06:50:23 by Albert Alombro

Updated 19 June 2025 05:57:27 by Albert Alombro