Palo Alto Firewall Syslog Filter

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.

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**.

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

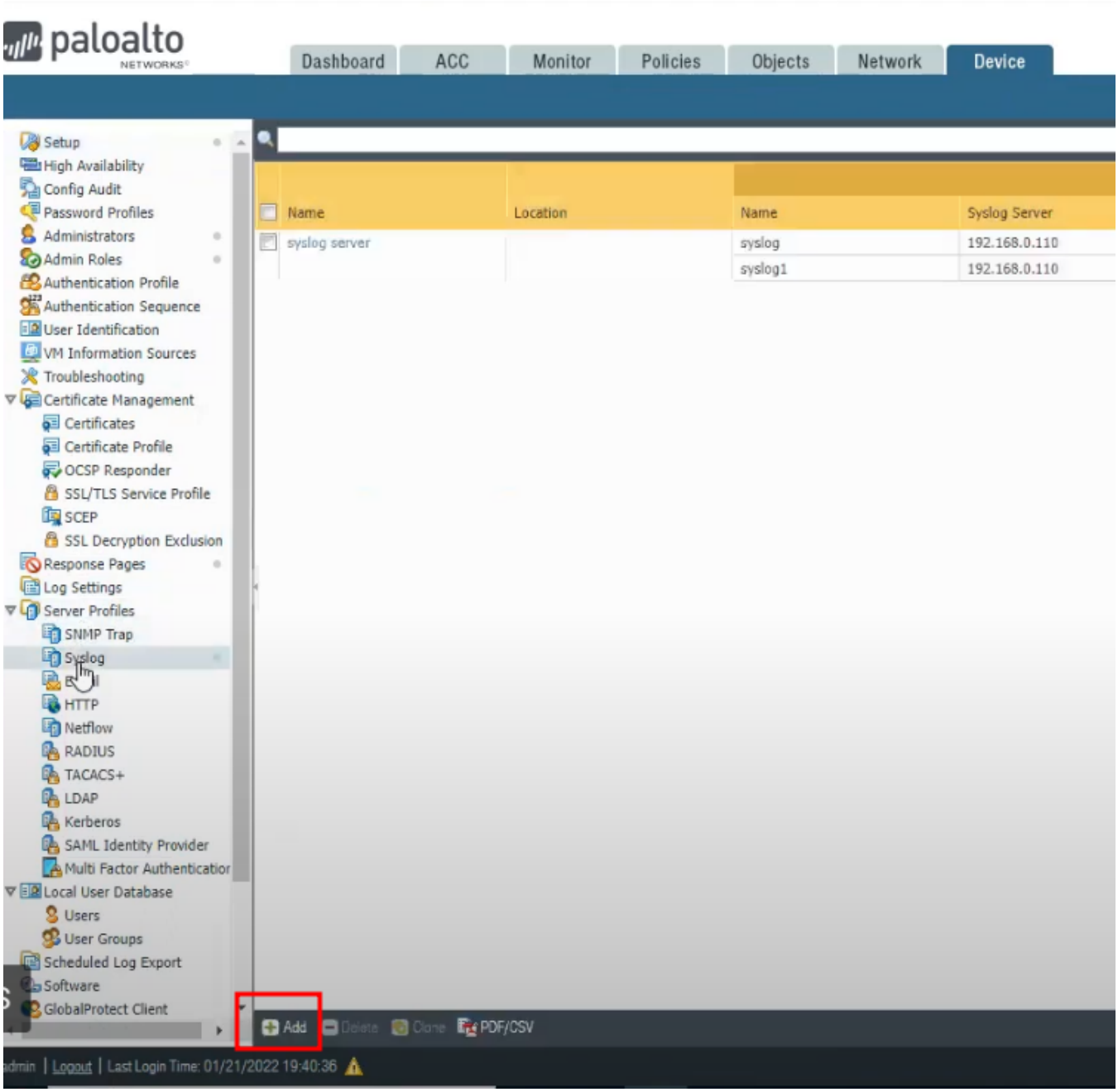
Configuration Steps

1. Create Syslog Server Profile

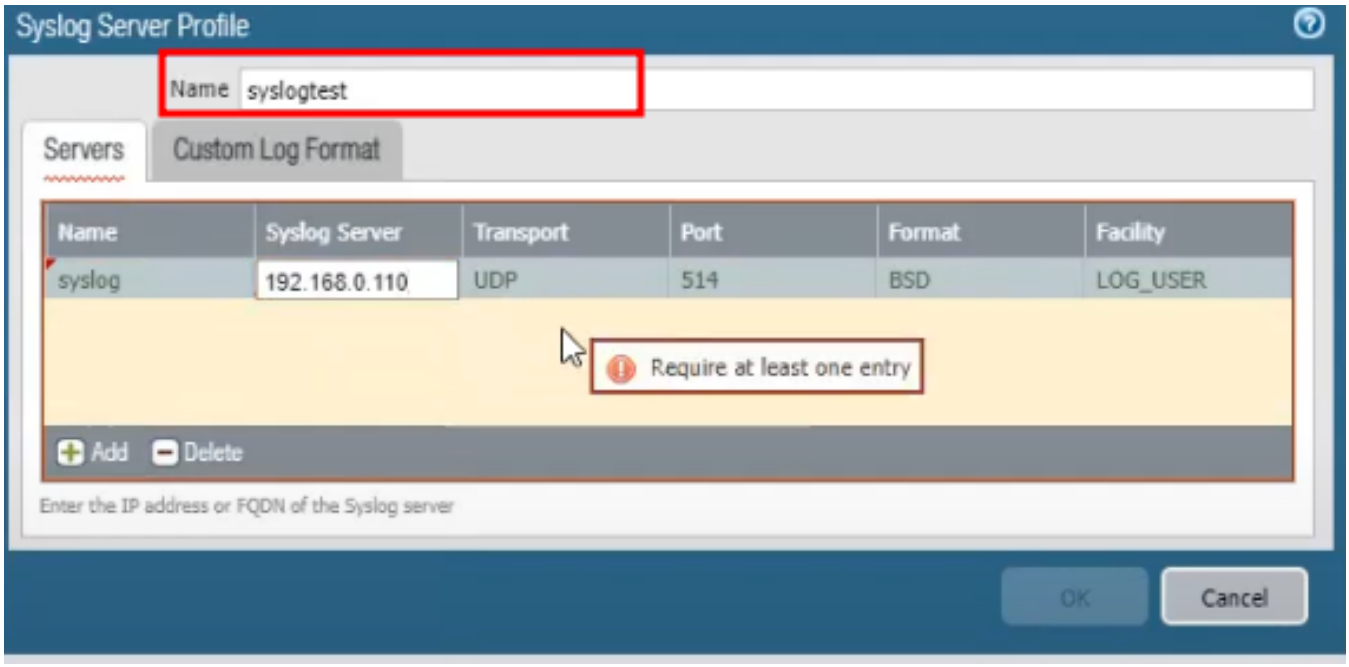
Navigate to: **Device** > **Server Profiles** > **Syslog**

Steps:

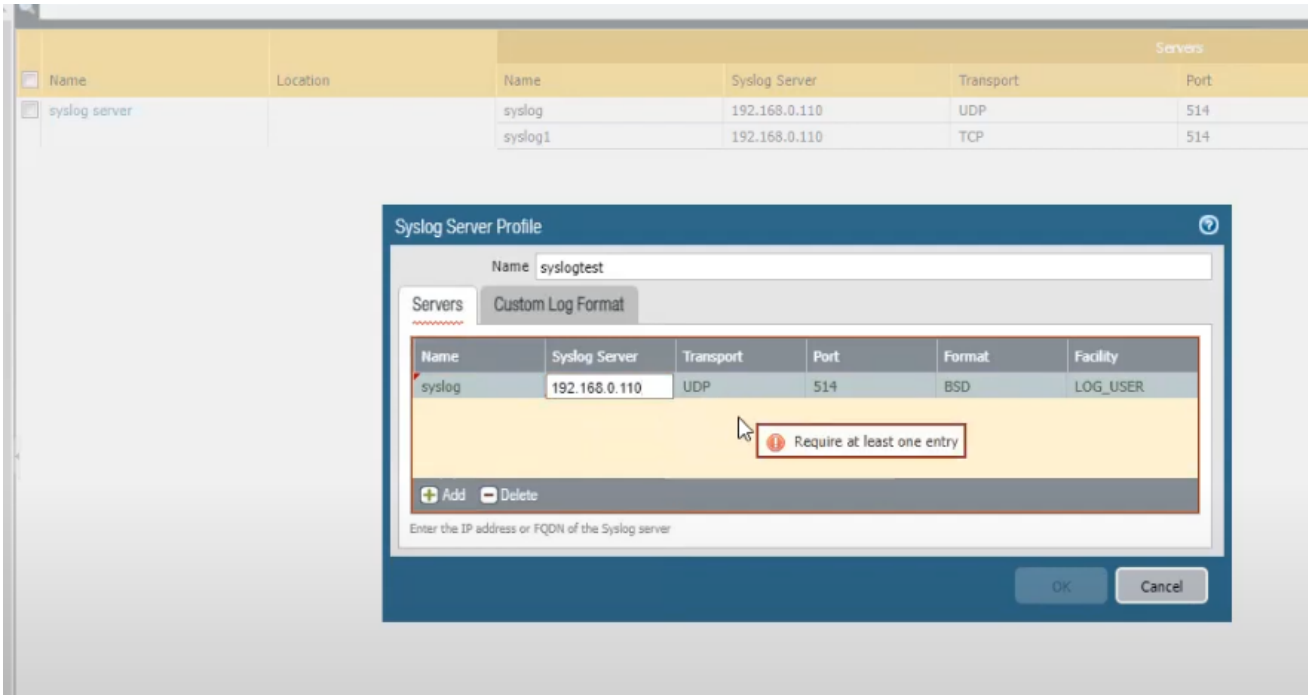
1. Click **Add** to create a new profile.



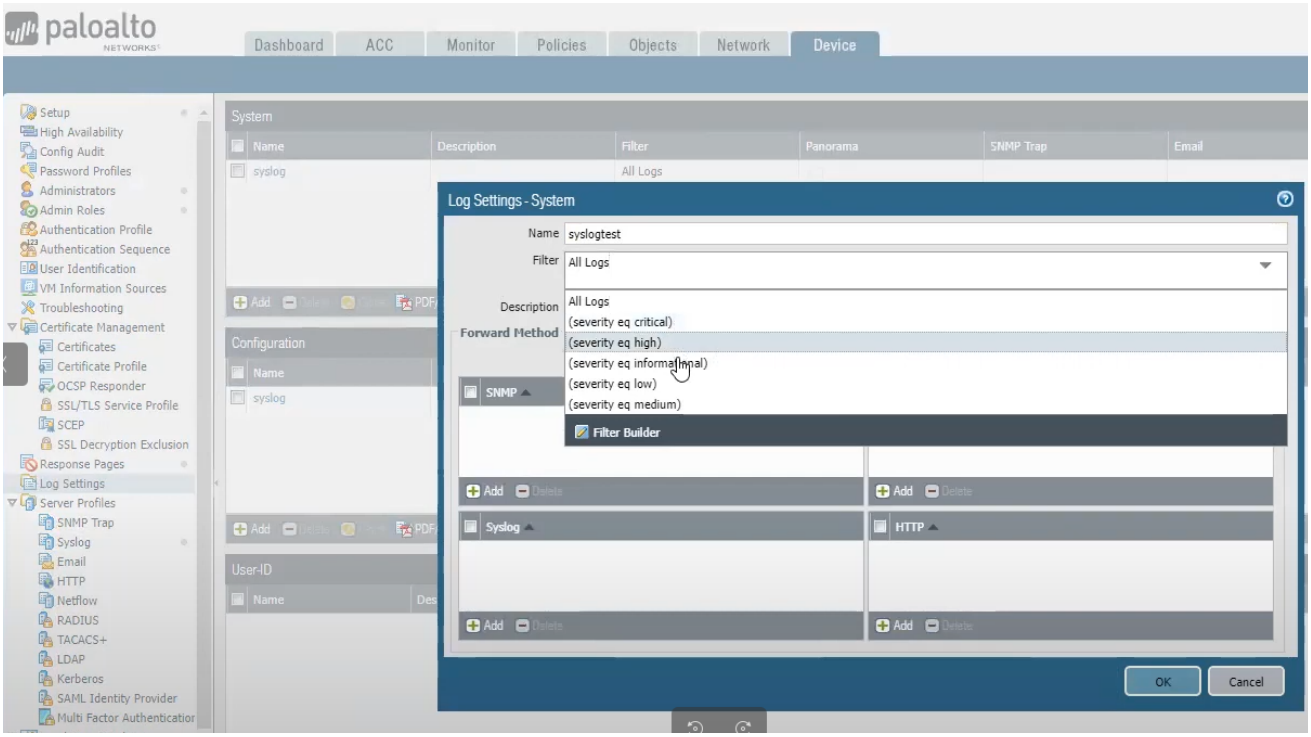
2. Enter a **Name (e.g., AQUILA-Syslog-Filter).**



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



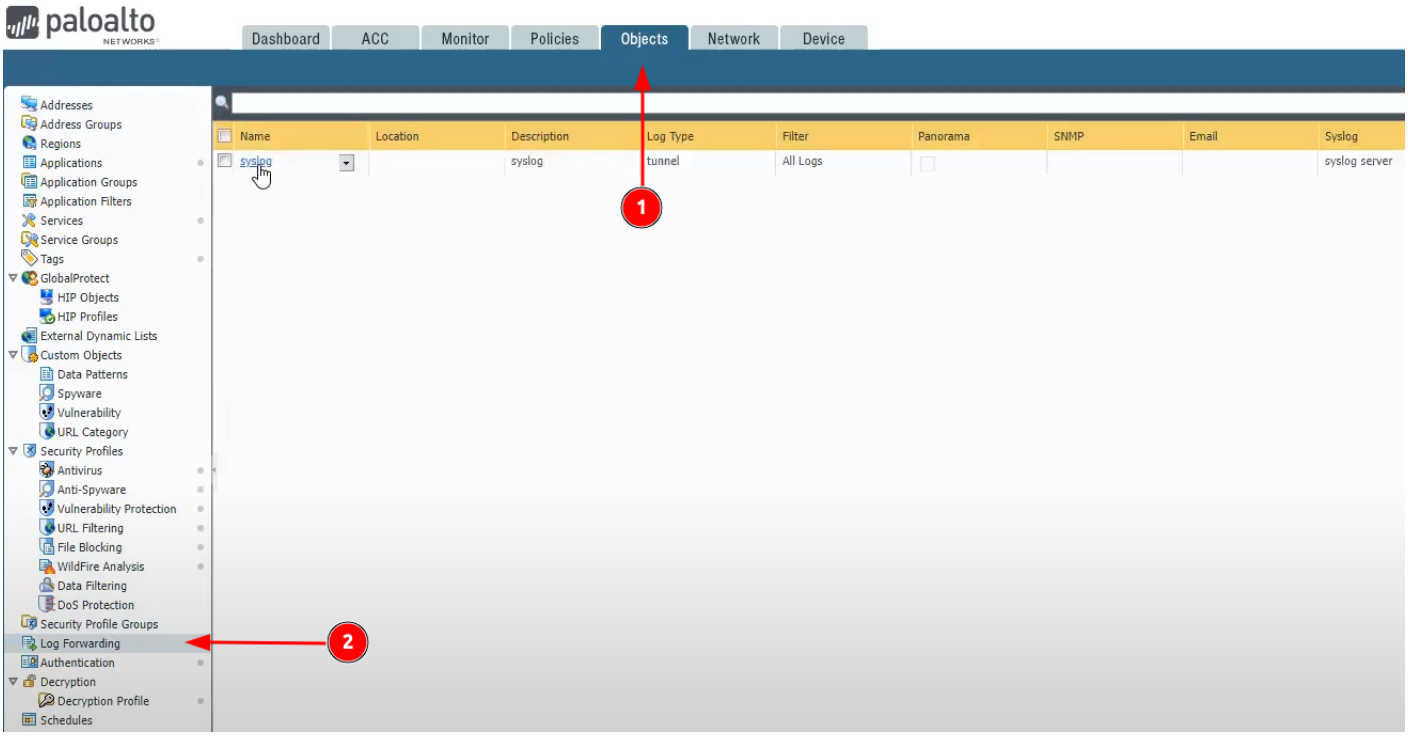
4. Add a **Filter** to specify:
   - **Log Type**: Threat
   - **Severity**: High



5. Click **OK**

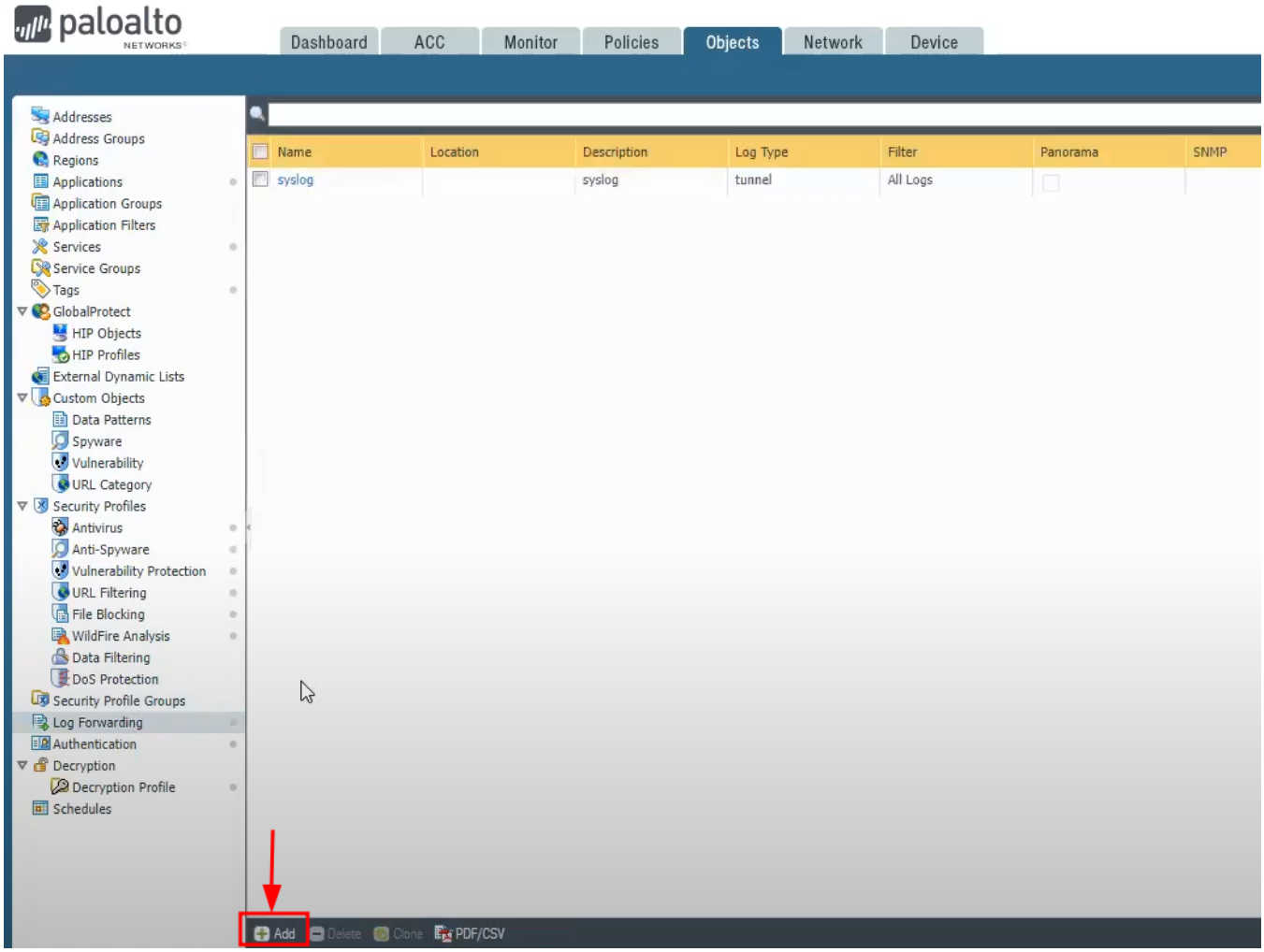
2. Create Log Forwarding Profile

Navigate to: **Objects** > **Log Forwarding**

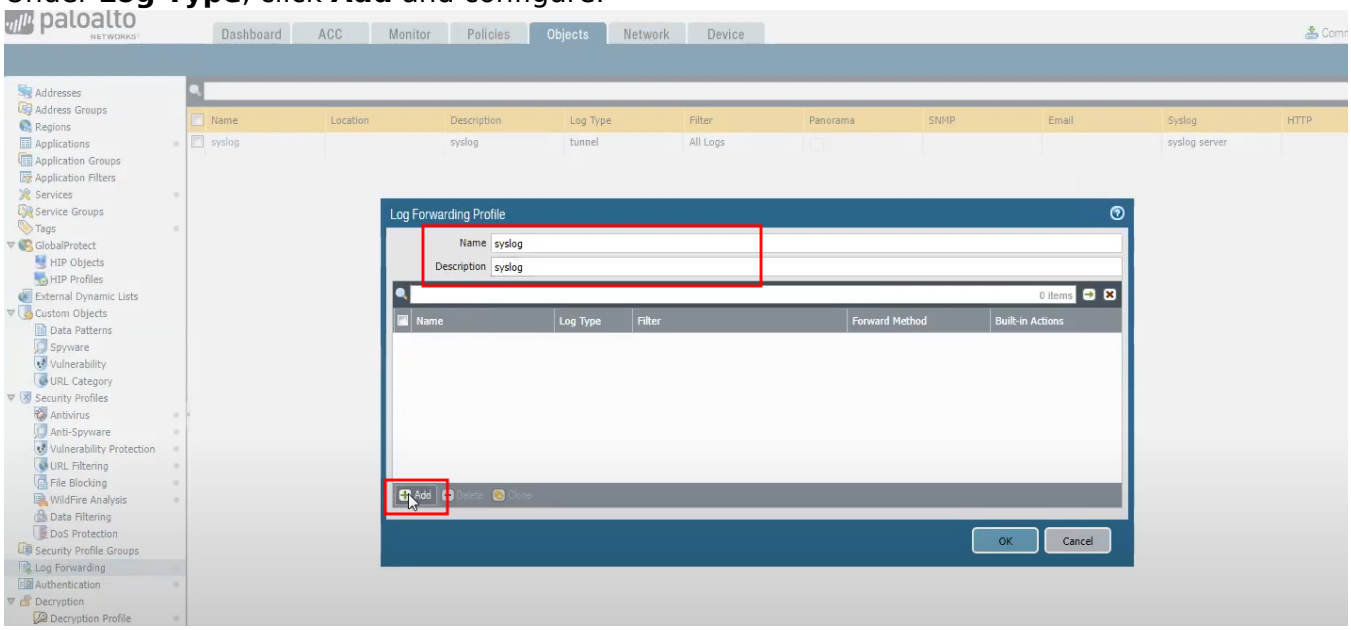


Steps:

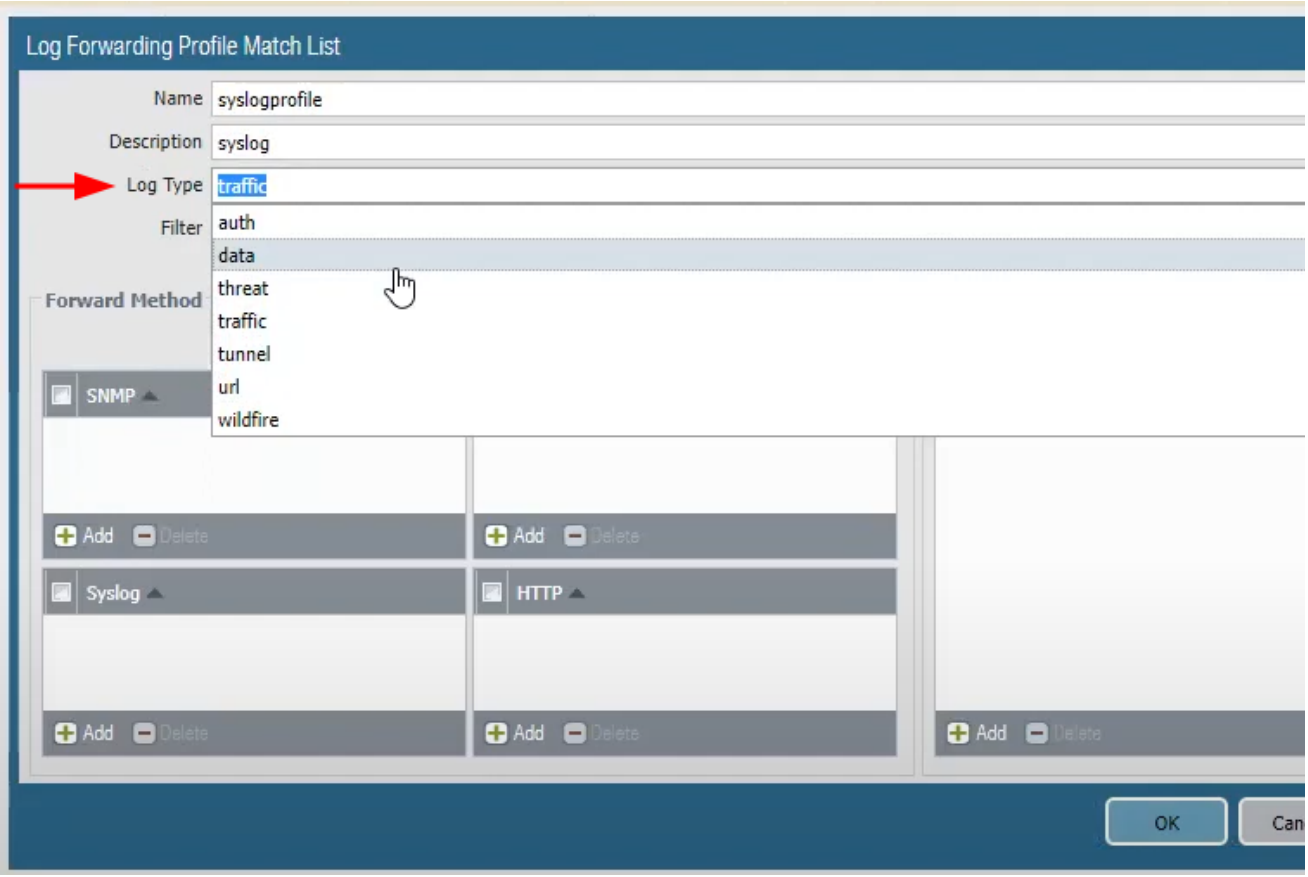
1. Click **Add** to create a new log forwarding profile.



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

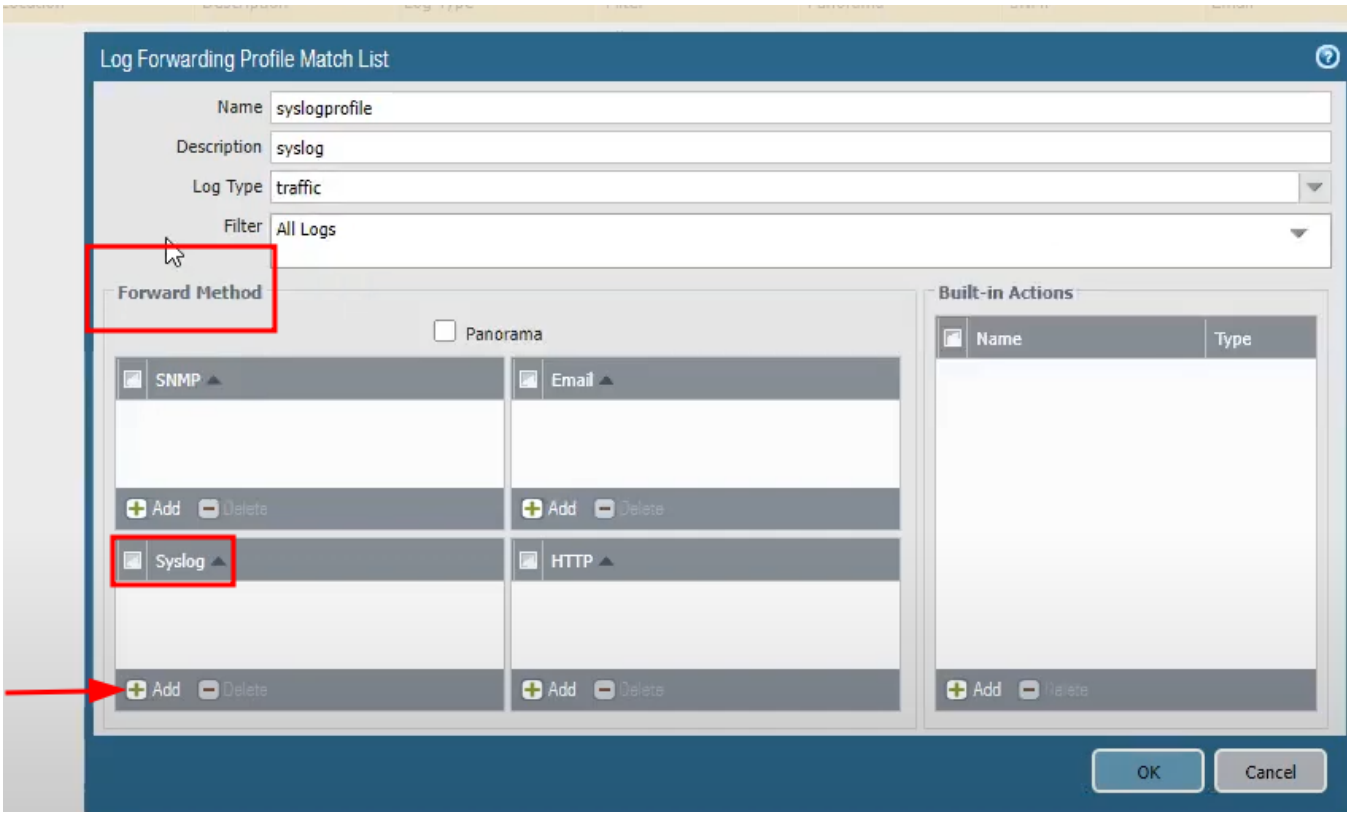


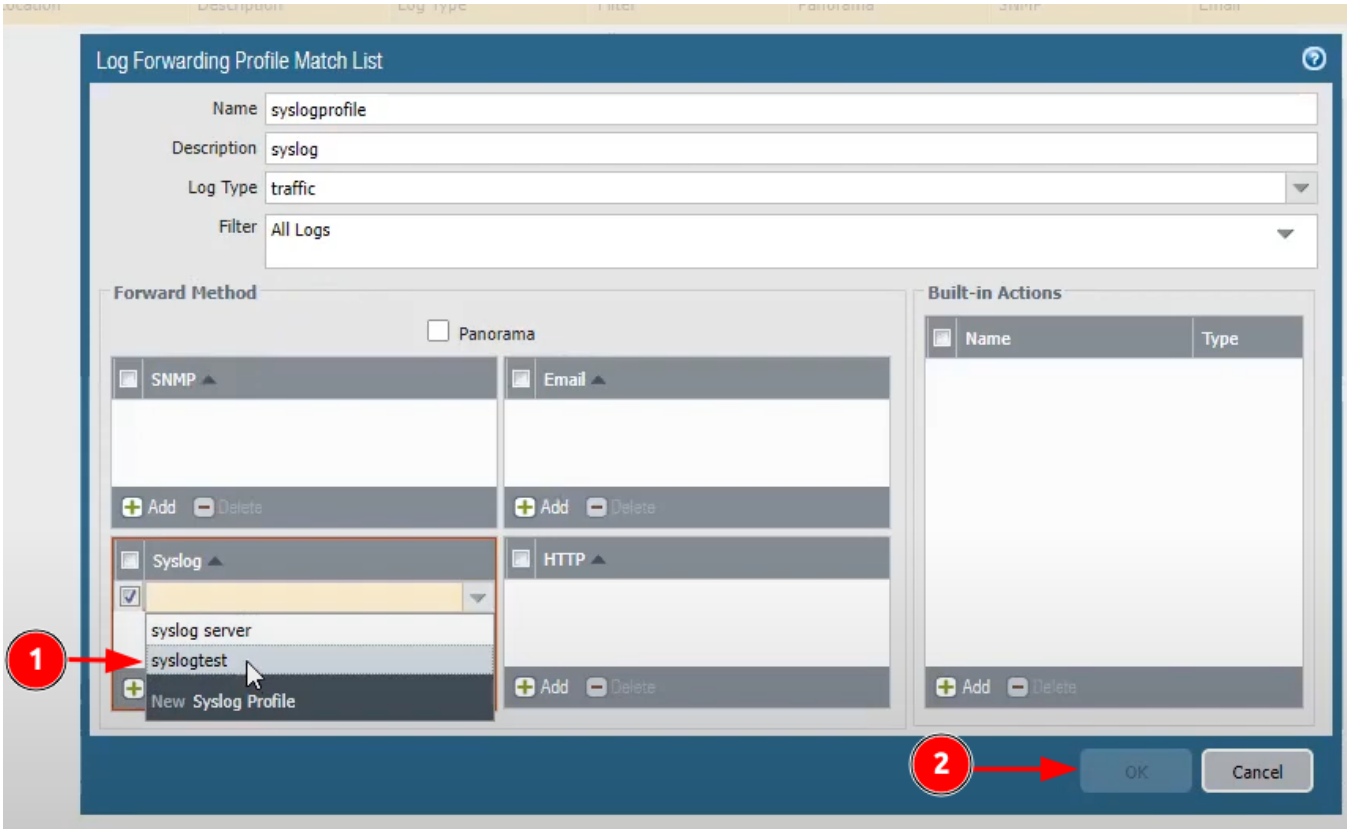
- **Log Type**: Select Threat



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

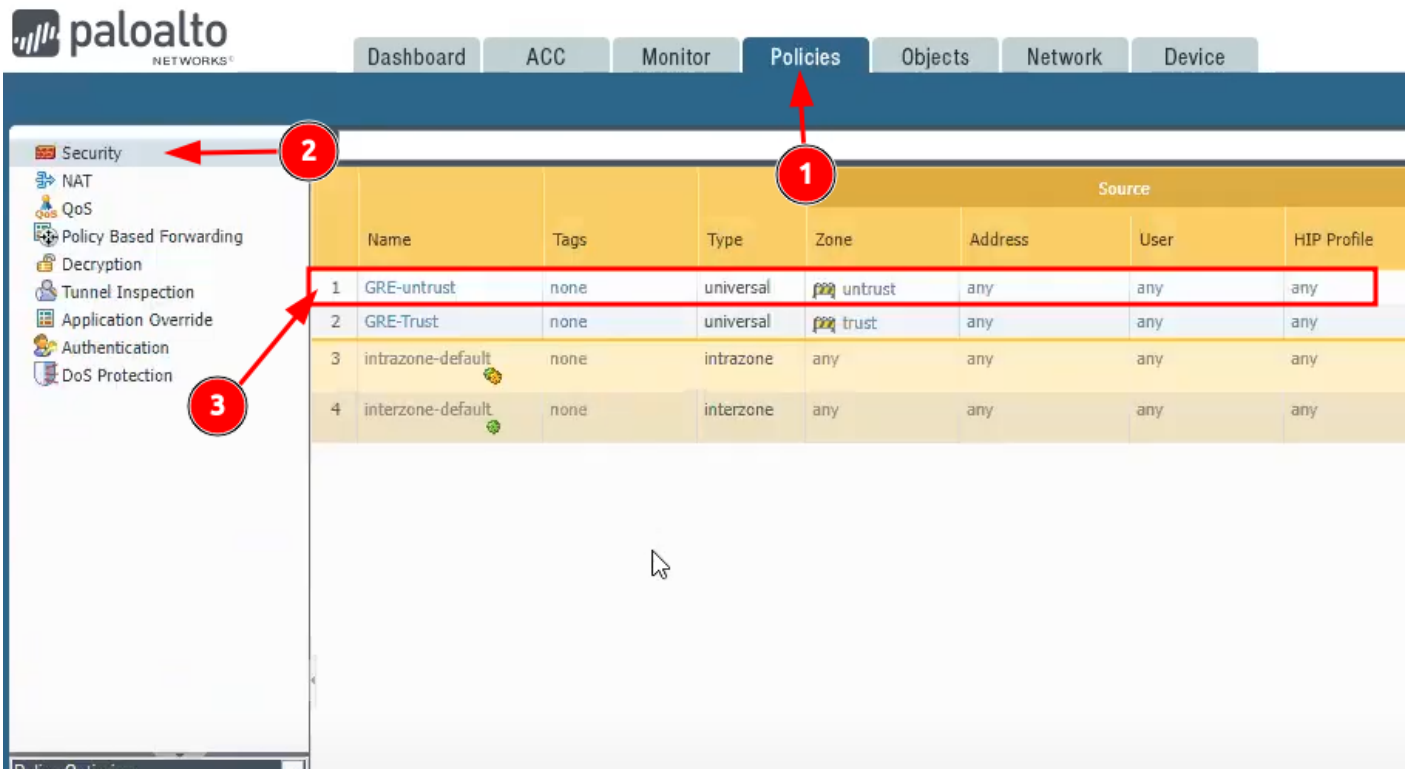
4. Click **OK**





3. Apply Log Forwarding to Security Policy

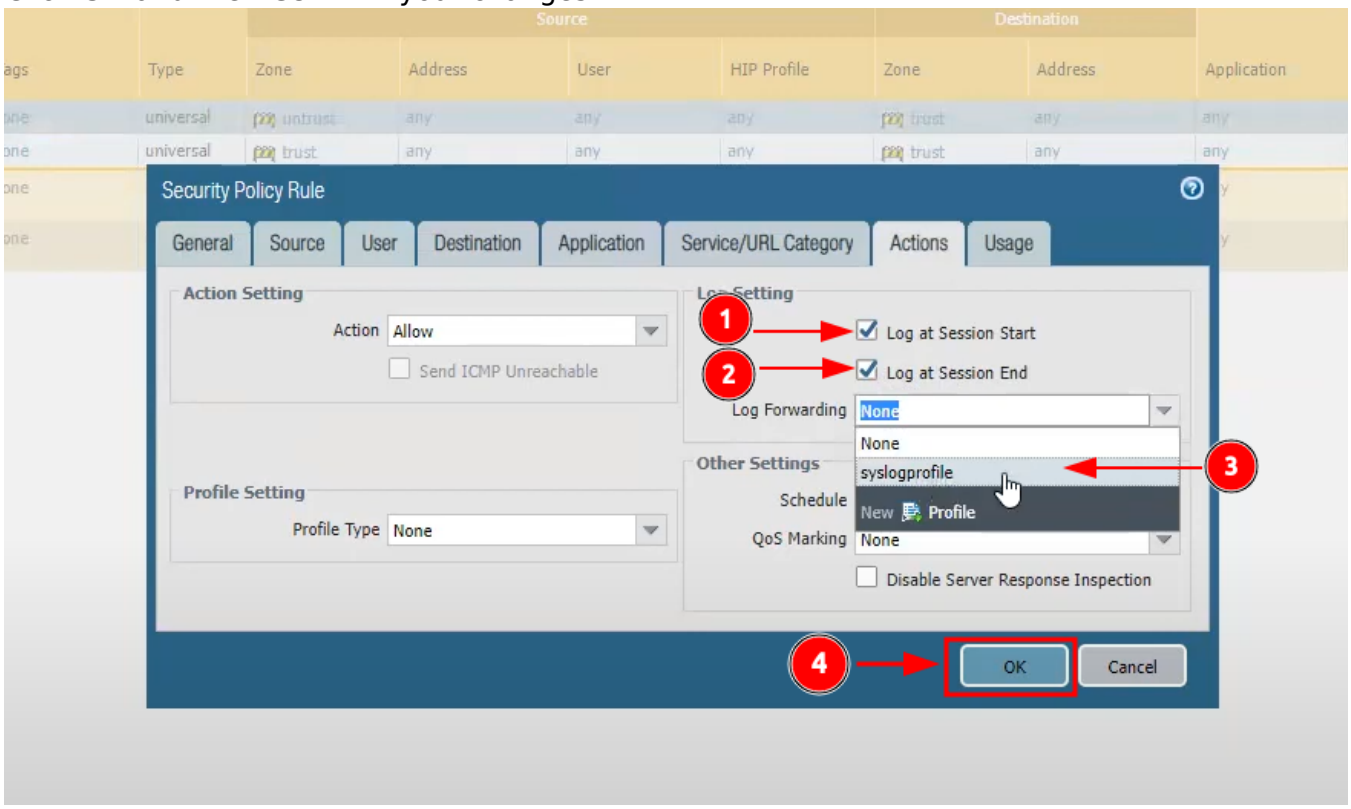
Navigate to: Policies > Security



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.



Please provide the following information to CyTech:

Requirements:Collect logs via syslog over UDP or TCP

*__Syslog Host__-> Syslog Collector IP address where the Elastic-Agent is installed.
*__Syslog Port__-> Port Number (Please identify if TCP or UDP)

Reference Links:

- *https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring*
- *https://www.youtube.com/watch?v=ftR3DU2MtjY&t=137s*

If you need further assistance, kindly contact our support at __support@cytechint.com__ for prompt assistance and guidance.

Revision #15
Created 18 June 2025 06:50:23
Updated 19 June 2026 08:35:39 by Benjie Janlay Jr.