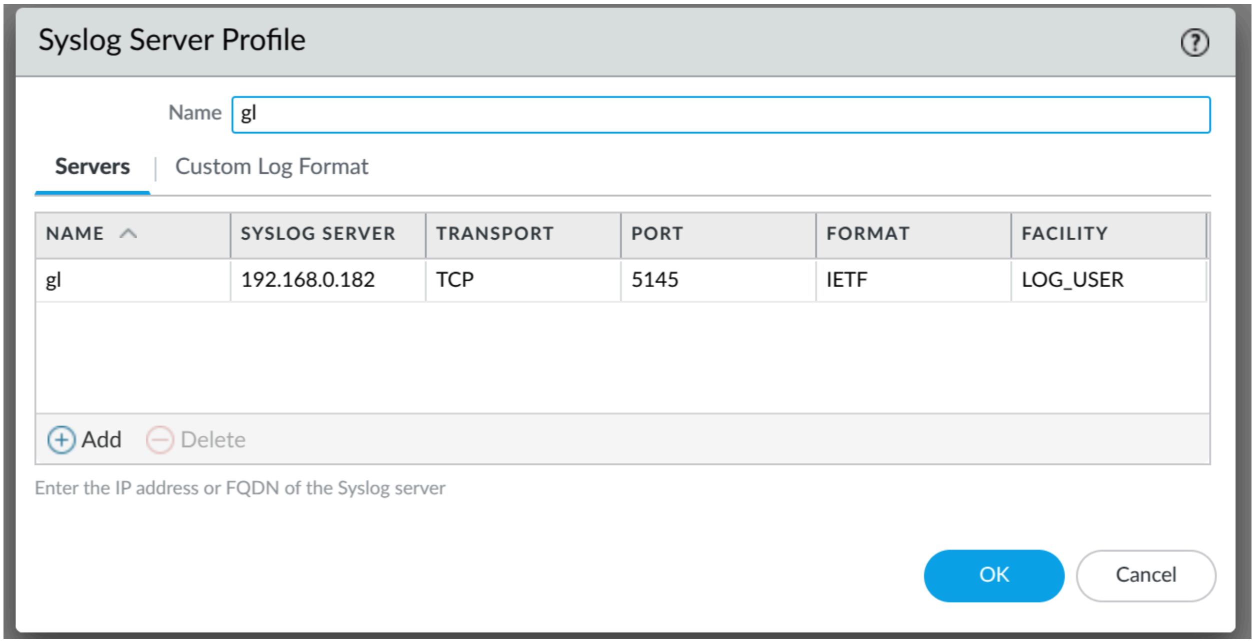
## Step 1: Configure the Syslog Server

1. Go to **Device > Server Profiles > Syslog**.
2. Click **Add** to create a new syslog server profile.
3. Fill in the required details:
   - **Name**: Enter a descriptive name for the syslog server (e.g., `Graylog-Syslog`).
   - **IP Address**: Enter the syslog server's IP address.
   - **Port**: Specify the port (e.g., `514` for UDP/TCP).
   - **Format**: Choose the format (e.g., `BSD` or `IETF`).
   - **Facility**: Set to **Loglevel 7** for detailed logs.
4. Click **OK** to save the configuration.

- This step establishes the connection between the Palo Alto firewall and your syslog server, allowing logs to be sent remotely.



Syslog Server Profile

Name: gl

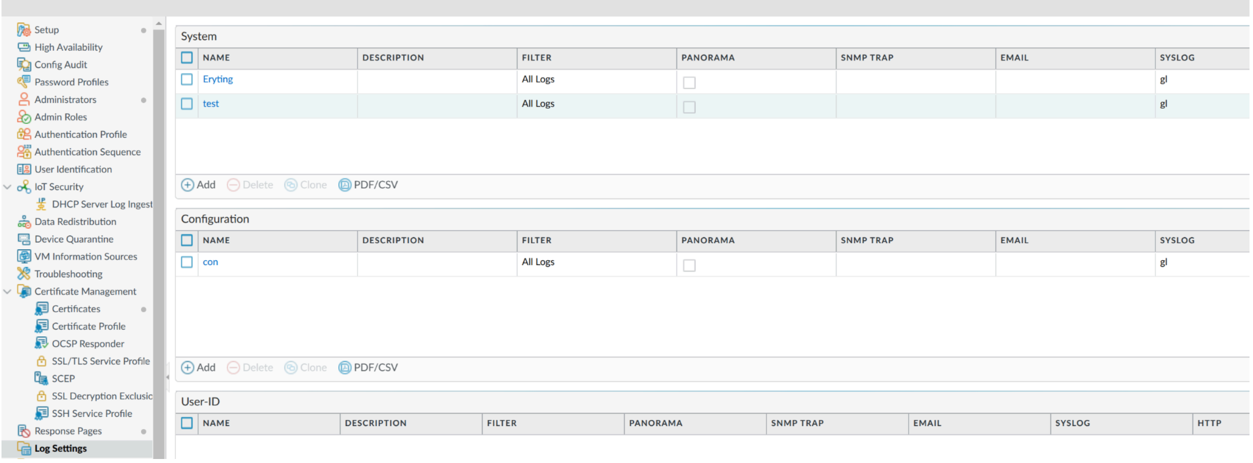
| NAME | SYSLOG SERVER | TRANSPORT | PORT | FORMAT | FACILITY |
|---|---|---|---|---|---|
| gl | 192.168.0.182 | TCP | 5145 | IETF | LOG_USER |

Enter the IP address or FQDN of the Syslog server

## Step 2: Link the Syslog Server to Log Settings

1. Go to **Device > Log Settings** (located above the Syslog option).
2. Select a log type, such as **System Logs** or **User Identification**.
3. Click **Add**, then:
   - Enter a name for the log setting.
   - Select the **Syslog Server** you created earlier.
4. Click **OK** to save.

- This step determines which logs (e.g., system events, user authentication, traffic) are sent to the syslog server.



System

| □ | NAME | DESCRIPTION | FILTER | PANORAMA | SNMP TRAP | EMAIL | SYSLOG |
|---|---|---|---|---|---|---|---|
| □ | Eryting | | All Logs | □ | | | gl |
| □ | test | | All Logs | □ | | | gl |

Configuration

| □ | NAME | DESCRIPTION | FILTER | PANORAMA | SNMP TRAP | EMAIL | SYSLOG |
|---|---|---|---|---|---|---|---|
| □ | con | | All Logs | □ | | | gl |

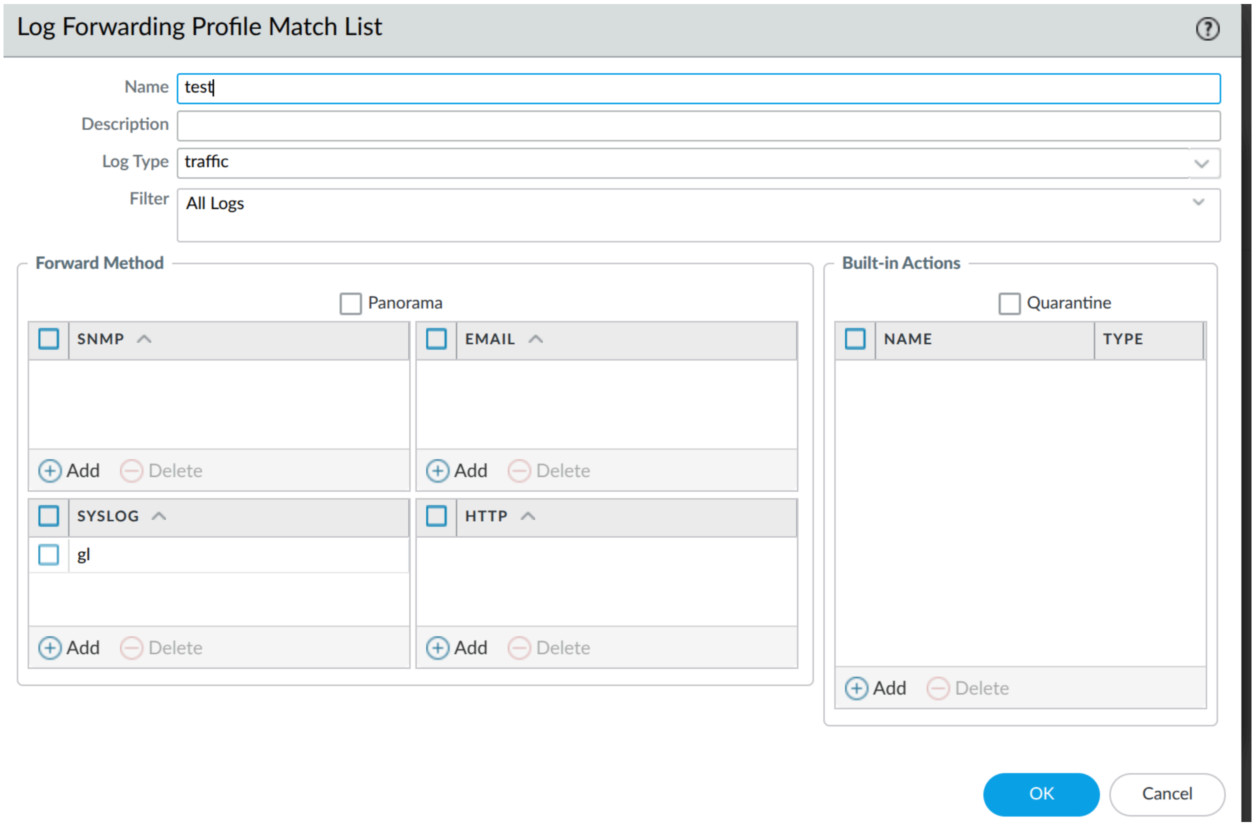
User-ID

| □ | NAME | DESCRIPTION | FILTER | PANORAMA | SNMP TRAP | EMAIL | SYSLOG | HTTP |
|---|---|---|---|---|---|---|---|---|

## Step 3: Create a Log Forwarding Profile

1. Go to **Objects > Log Forwarding**.
2. Click **Add** to create a new log forwarding profile.
3. Fill in the details:
   - **Name**: Provide a name for the profile (e.g., `Forward-All-Traffic`).
   - Under **Log Forwarding Matching**, click **Add**.
   - Choose the **Syslog Server** created in Step 1.
   - Select the type of traffic you want to forward (e.g., traffic logs, threat logs, or all).
4. Click **OK** to save.

- This step defines the log forwarding behavior, specifying what type of logs should be sent to the syslog server.



Log Forwarding Profile Match List

Name: test

Description:

Log Type: traffic

Filter: All Logs

Forward Method

□ Panorama

| □ | SYSLOG |
|---|---|
| □ | gl |

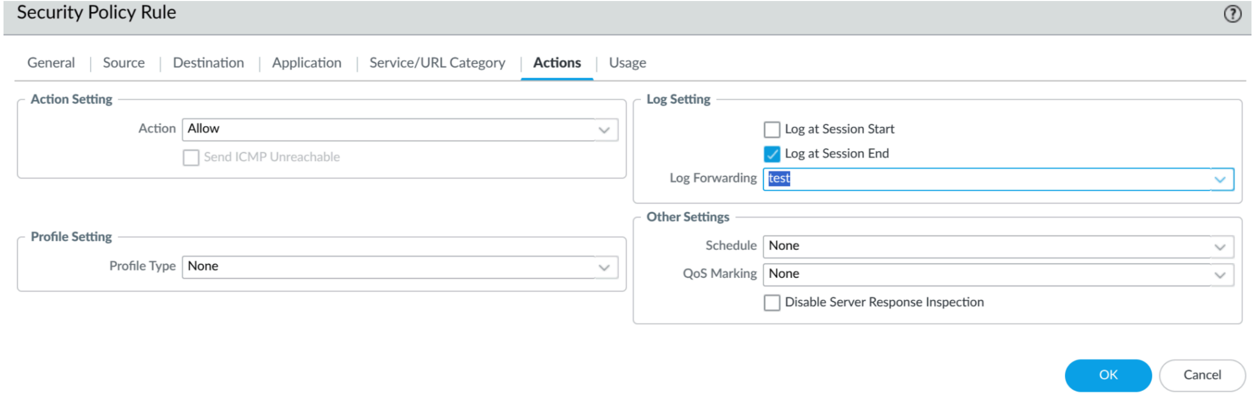
Built-in Actions

□ Quarantine

## Step 4: Apply Log Forwarding Profile to Policies

1. Go to **Policies > Security**.
2. Open the **existing policy** to which you want to attach log forwarding.
3. Scroll to the **Actions** tab of the policy.
4. In the **Log Forwarding** dropdown menu:
    - Select the log forwarding profile you created earlier.
5. Click **OK** to save the changes.

- This ensures that logs for specific traffic handled by your security policies are forwarded to the syslog server.


Security Policy Rule
General | Source | Destination | Application | Service/URL Category | Actions | Usage
OK
Cancel

Action Setting

Action: Allow

□ Send ICMP Unreachable

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: test

Profile Setting

Profile Type: None

Other Settings

Schedule: None

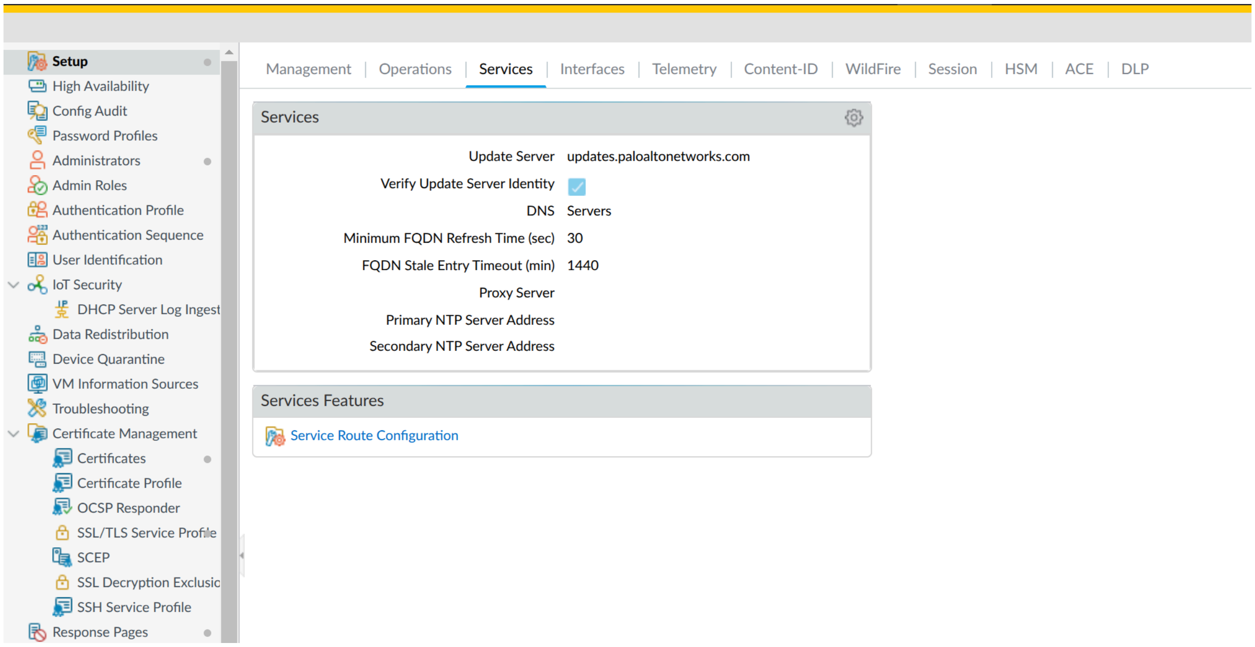
QoS Marking: None

□ Disable Server Response Inspection

## Step 5: Configure Service Route for Syslog

1. Go to **Device > Setup > Services**.
2. Click **Service Route Configuration**.
3. In the list of services, find **Syslog**.
4. Select the **source interface** and **source address** used to connect to the syslog server.
   - Example: Choose the **interface** where the syslog server is reachable (e.g., `ethernet1/1` for WAN or another appropriate interface).
5. Click **OK** and save the configuration.
6. Click **Commit** to apply all changes.

- This step ensures that the firewall uses the correct interface to send logs to the syslog server.
- Without this, the firewall might use the **management interface** (by default), which could be on a separate network and unable to reach the syslog server.

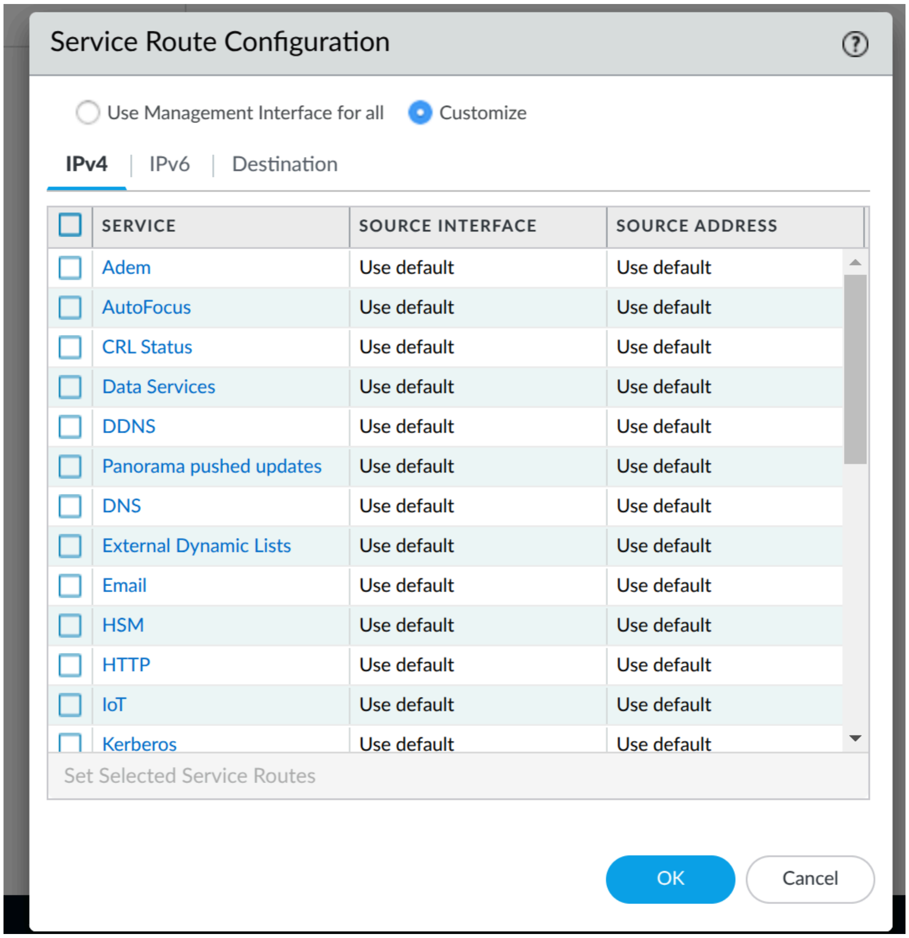


Services

| | |
|---|---|
| Update Server | updates.paloaltonetworks.com |
| Verify Update Server Identity | ☑ |
| DNS | Servers |
| Minimum FQDN Refresh Time (sec) | 30 |
| FQDN Stale Entry Timeout (min) | 1440 |
| Proxy Server | |
| Primary NTP Server Address | |
| Secondary NTP Server Address | |

Services Features

Service Route Configuration

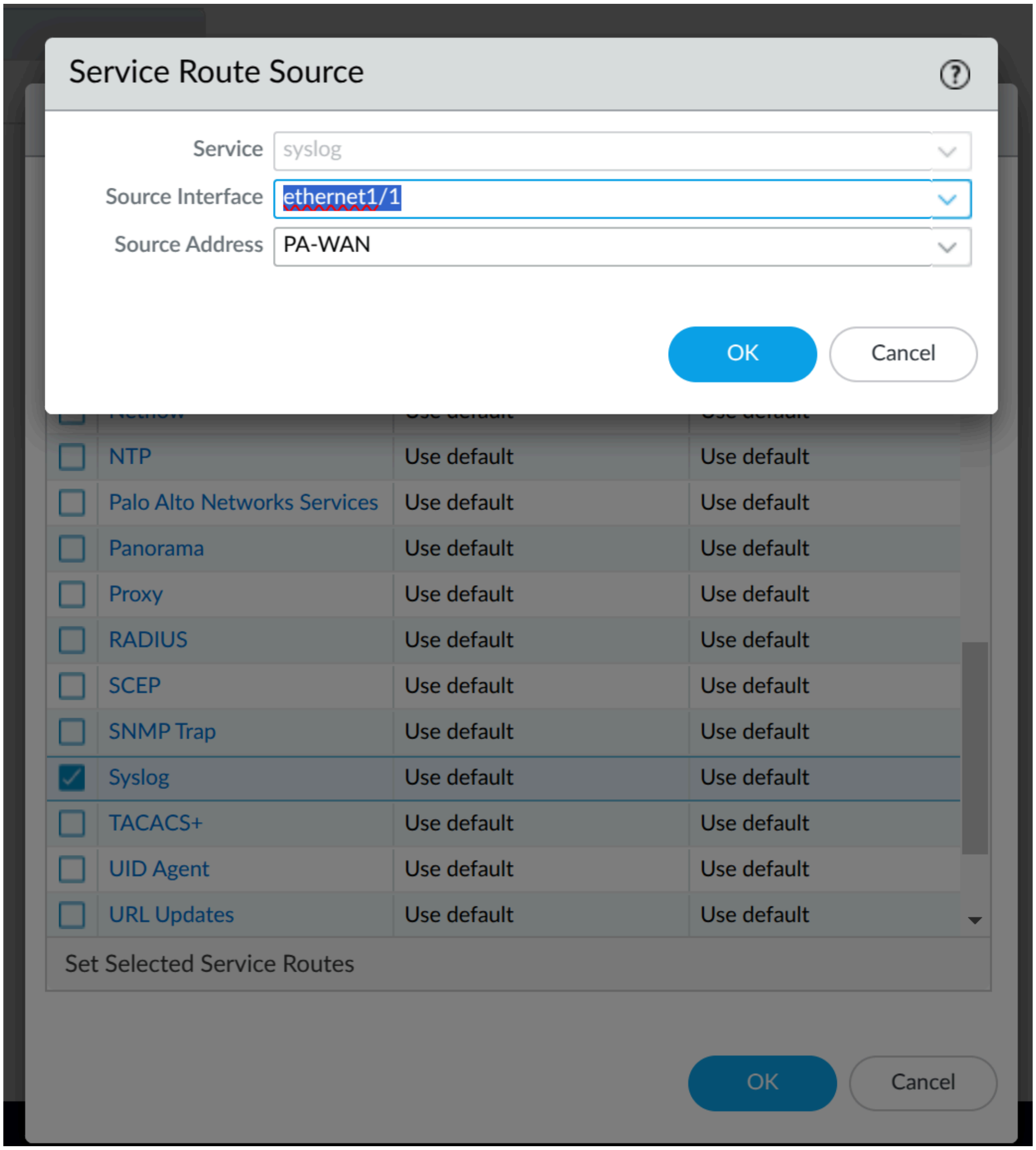


Service Route Configuration

○ Use Management Interface for all ● Customize

**IPv4** | IPv6 | Destination

| □ | SERVICE | SOURCE INTERFACE | SOURCE ADDRESS |
|---|---|---|---|
| □ | Adem | Use default | Use default |
| □ | AutoFocus | Use default | Use default |
| □ | CRL Status | Use default | Use default |
| □ | Data Services | Use default | Use default |
| □ | DDNS | Use default | Use default |
| □ | Panorama pushed updates | Use default | Use default |
| □ | DNS | Use default | Use default |
| □ | External Dynamic Lists | Use default | Use default |
| □ | Email | Use default | Use default |
| □ | HSM | Use default | Use default |
| □ | HTTP | Use default | Use default |
| □ | IoT | Use default | Use default |
| □ | Kerberos | Use default | Use default |



Service Route Source

Service: syslog

Source Interface: ethernet1/1

Source Address: PA-WAN

| | | | |
|---|---|---|---|
| □ | NTP | Use default | Use default |
| □ | Palo Alto Networks Services | Use default | Use default |
| □ | Panorama | Use default | Use default |
| □ | Proxy | Use default | Use default |
| □ | RADIUS | Use default | Use default |
| □ | SCEP | Use default | Use default |
| □ | SNMP Trap | Use default | Use default |
| ☑ | Syslog | Use default | Use default |
| □ | TACACS+ | Use default | Use default |
| □ | UID Agent | Use default | Use default |
| □ | URL Updates | Use default | Use default |

## Final Verification

1. Generate test traffic to match the policy with log forwarding.
2. Log in to the syslog server and confirm that logs are being received.
3. Check **Monitor > Logs** in Palo Alto to ensure the logs are correctly forwarded.