Palo Alto Next Generation Firewall

Configure Syslog Monitoring

STEP 1 - Configure a Syslog server profile.

1. Select **Device**-->**Server**-->**Profiles**-->**Syslog**.
2. Click **Add** and enter a **Name** for the profile.
3. If the firewall has more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where this profile is available.
4. For each syslog server, click **Add** and enter the information that the firewall requires to connect to it:
    - **Name** - Unique name for the server profile.
    - **Syslog Server** - IP address of the syslog server.
    - **Transport** - Select TCP or UDP as the protocol for communicating with the syslog server.
    - **Port** - The port number on which to send syslog messages; you must use the same port number on the firewall and the syslog server.
5. Click **OK** to save the server profile.

STEP 2 - Configure syslog forwarding for Traffic, Threat, and WildFire Submission logs.

1. Configure the firewall to forward logs.
    - Select **Objects**-->**Log Forwarding**, click **Add**, and enter a **Name** to identify the profile.

- For each log type and each severity level or WildFire verdict, select the **Syslog server profile** and click **OK**.

2. Assign the log forwarding profile to a security policy to trigger log generation and forwarding.

   - Select **Policies**-->**Security** and select a policy rule.
   - Select the **Actions** tab and select the **Log Forwarding** profile you created.
   - For Traffic logs, select one or both **Log at Session Start** and **Log at Session End** check boxes, and click **OK**.

STEP 3 - Configure syslog forwarding for System, Config, HIP Match, and Correlation logs.

1. Select **Device**-->**Log Settings**.
2. For System and Correlation logs, click each Severity level, select the **Syslog server profile**, and click **OK**.
3. For Config, HIP Match, and Correlation logs, edit the section, select the **Syslog server profile**, and click **OK**.

Source: *https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring*

Palo Alto Next Generation Firewall Integration Procedures

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)

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

Revision #4
Created 16 January 2025 03:08:50 by Richmond Abella
Updated 17 January 2025 09:43:33 by Richmond Abella