Integration Guide

Integrate Palo Alto Firewall with the Netsurion Open XDR platform

Publication Date

April 04, 2023

Abstract

This guide provides instructions to configure and integrate the Palo Alto Firewall with the Netsurion Open XDR platform to retrieve its event logs via syslog and forward them to the Netsurion Open XDR platform.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Palo Alto Firewall and the Netsurion Open XDR platform version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Palo Alto Firewall in the Netsurion Open XDR platform.

Product Terminology

The following terms are used throughout this guide:

- The term “Netsurion’s Open XDR platform” or “the Netsurion Open XDR platform” or “the Open XDR platform” refers to EventTracker.
- The term “Data Source Integrations” refers to Knowledge packs.

Table of Contents

1 Overview

Palo Alto Networks, the next-generation firewalls provide a flexible networking architecture that includes support for dynamic routing, switching, and VPN connectivity, enabling you to deploy the firewall into nearly any networking environment. When configuring the Ethernet ports on your firewall, you can choose from virtual wire, Layer 2, or Layer 3 interface deployments. In addition, to allow you to integrate into a variety of network segments, you can configure different types of interfaces on different ports.

Netsurion's Open XDR platform seamlessly integrates SIEM, Log Management, File Integrity Monitoring, machine Analytics, and so forth. The Netsurion Open XDR platform facilitates monitoring events retrieved from Palo Alto Firewall. The alerts, reports, dashboards, and categories in the Netsurion Open XDR platform benefit in capturing important and critical activities in Palo Alto Firewall.

2 Prerequisites

- Palo Alto Appliance, PanOS version (2.0 - 8.1) must be installed.
- Appropriate access permissions to make configuration changes.
- PowerShell version 5.0 and above must be installed.
- Port 514 must be opened by Palo Alto Firewall (PanOS).
- The Data Source Integrator package.

> **Note**
>
> To get the Data Source Integrator package, contact your Netsurion Account Manager.

3 Integrating Palo Alto Firewall with the Netsurion Open XDR platform

> **IMPORTANT:**
>
> The Integration procedure does not cover all the configuration and Syslog-related features and functionality available in Palo Alto Networks (PanOS). Refer Palo Alto Networks (PanOS) Product Documentation for more information.

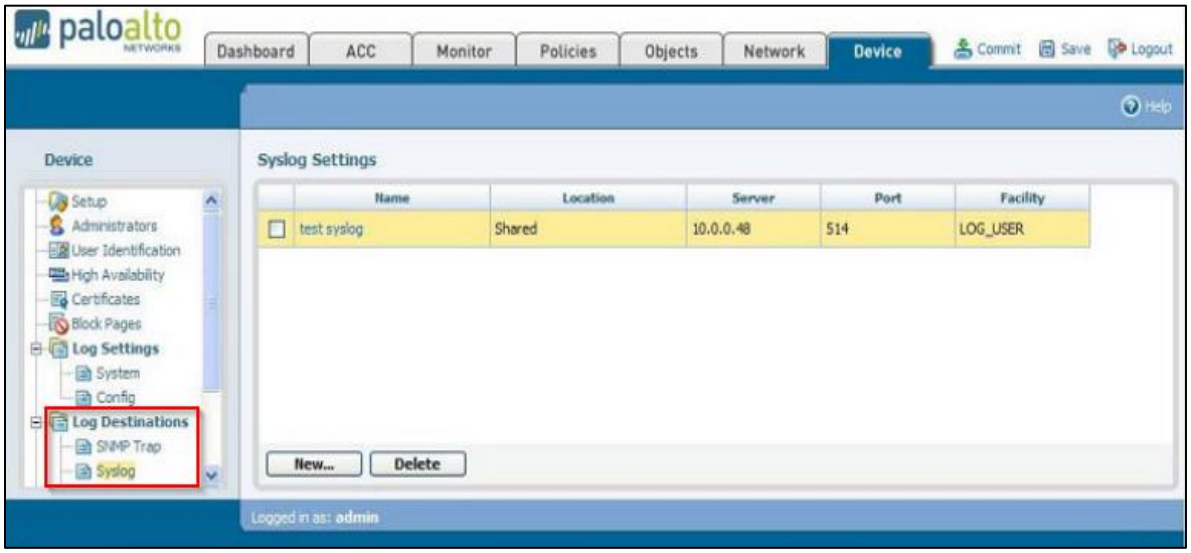
3.1 Defining Syslog Servers

To generate Syslog messages for systems, configurations, traffics, or threat log entries, it is necessary to specify one or more Syslog servers.

3.1.1 Defining the Syslog Server Profile

Perform the following procedure to define the syslog server profile.

1. In the **Palo Alto Networks** interface, from the **Device** tab on the left, go to **Log Destinations** > **Syslog** and open the **Syslog Settings**.



2. Click **New** to define a **New Syslog** and specify the following details.

   - **Name** - Specify a name for the syslog server (up to 31 characters).

     Note:

     The name is case- sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

   - **Server**-Enter the FQDN or the IP address of the Syslog server, that is, the Netsurion Open XDR Manager.

     Note:

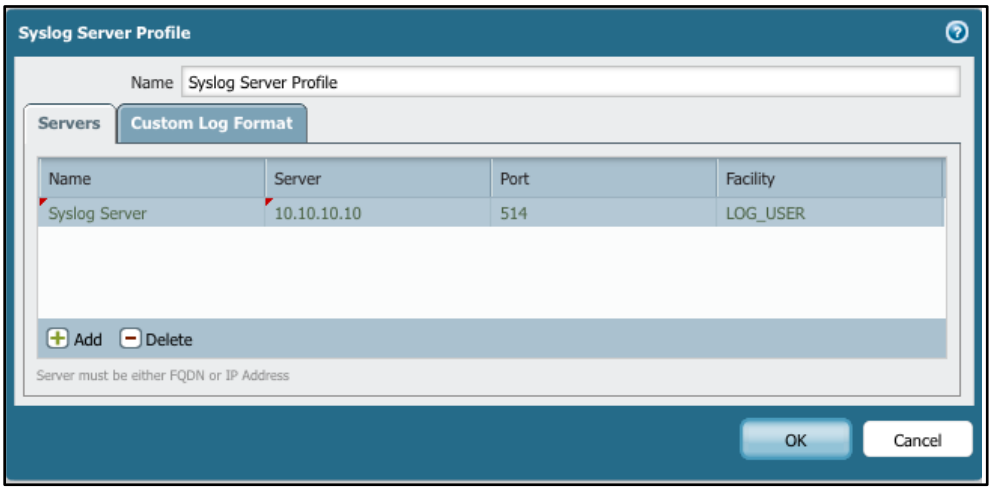
     Recommended using the FQDN.

   - **Port** -Enter the port number of the Syslog server.

     Note:

     The standard port is **514**.

- **Facility**-Choose the appropriate Facility level from the drop-down list.



3. After providing the necessary details, click **OK** to submit the new trap destination.

Note:

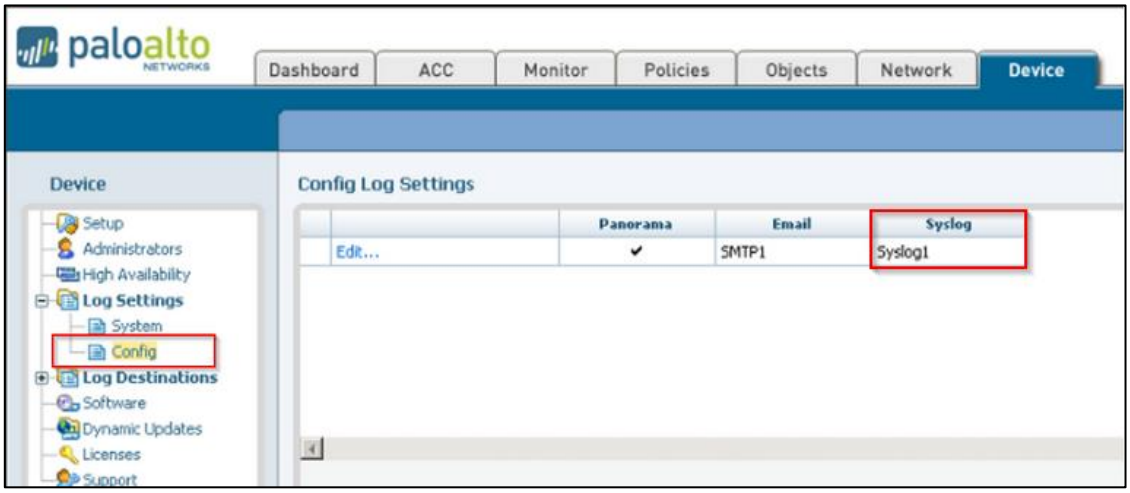
You may activate your changes immediately or save them for future activation.

3.1.2 Configuring the Log Settings

1. In the **Palo Alto Networks** interface, from the **Device** tab on the left, go to **Log Settings > Config** to configure the Log settings.
2. Click **Edit** to modify the existing the log settings.
3. In the **Syslog** field, select the syslog server profile that was created in the above step for the desired log-severity, and click **OK** to change the log settings.

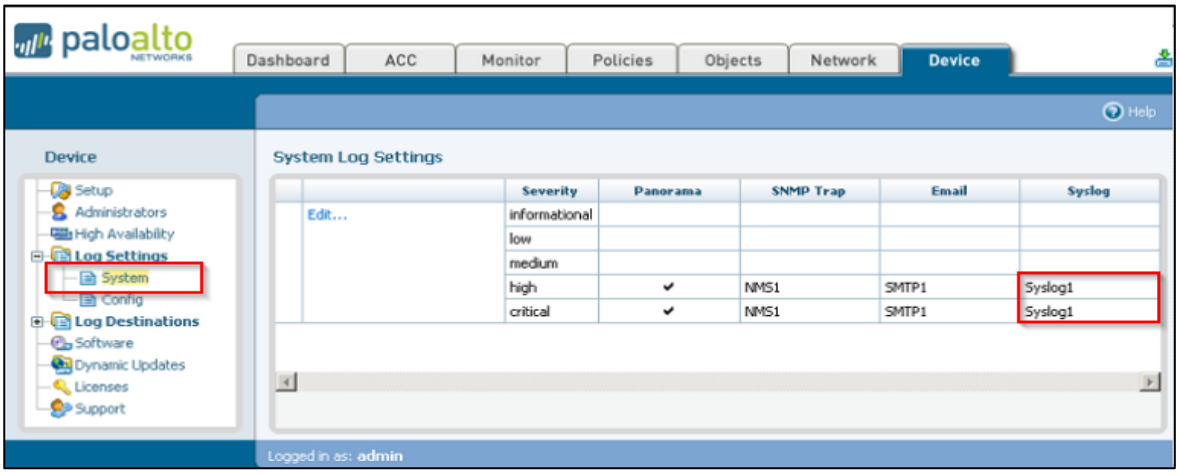
Note:

You may activate your changes immediately or save them for future activation.



3.1.3 Defining the System Log Settings

1. In the **Palo Alto Networks** interface, from the **Device** tab on the left, go to **Log Settings > System** to set the System Log Settings.
2. Click **Edit** to change the log settings.
3. In the **Syslog** field, select the syslog server profile created earlier (in the **Defining the Syslog Server Profile** section) for the required log-severity.



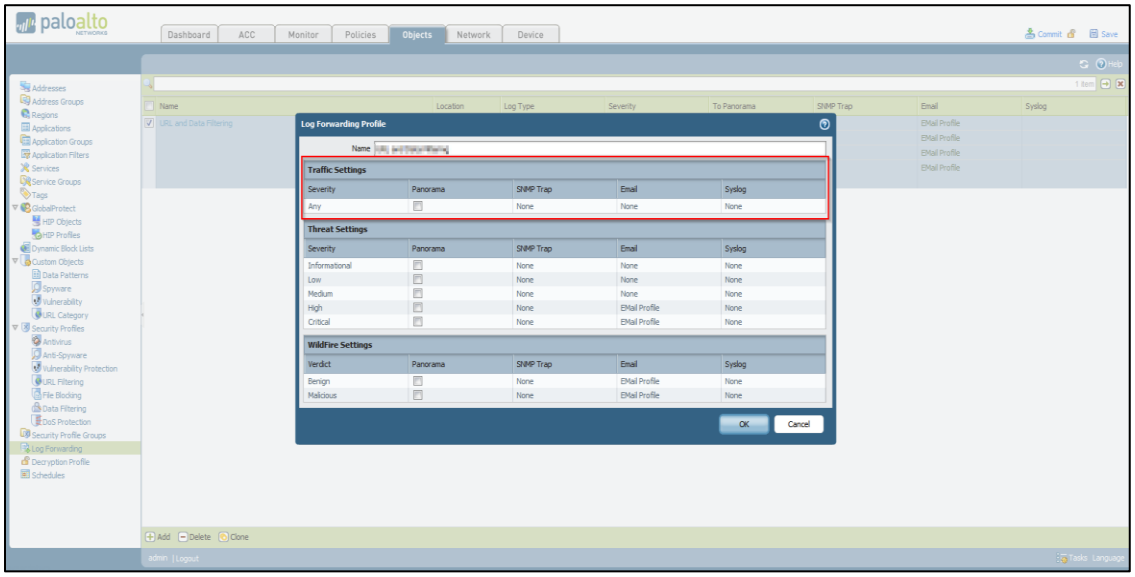
4. Click **OK** to change the log settings.

Note:

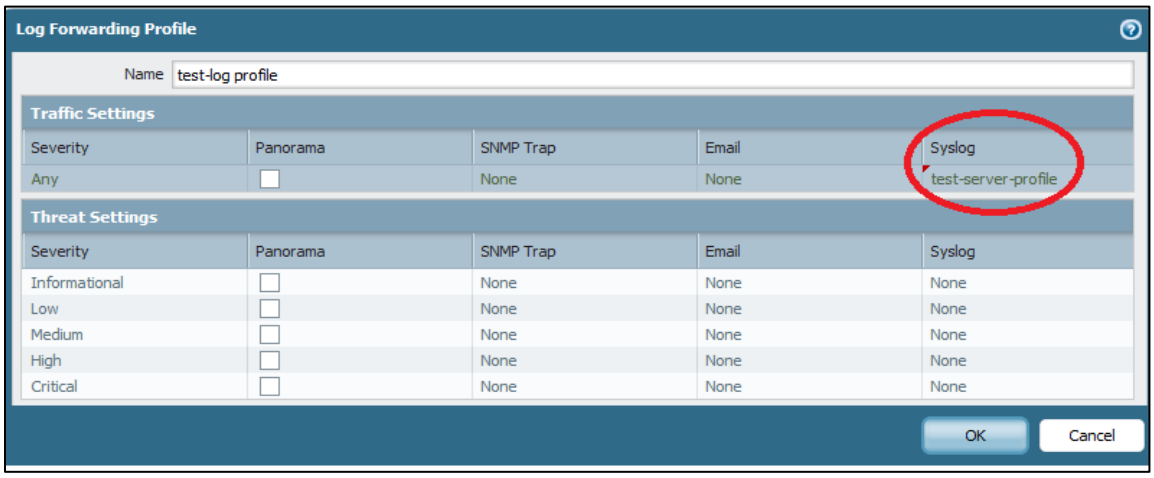
You may activate your changes immediately or save them for future activation.

3.1.4 Defining the Traffic log settings

1. In the **Palo Alto Networks** interface, go to **Objects > Log forwarding** and click **Add** to create a new profile.

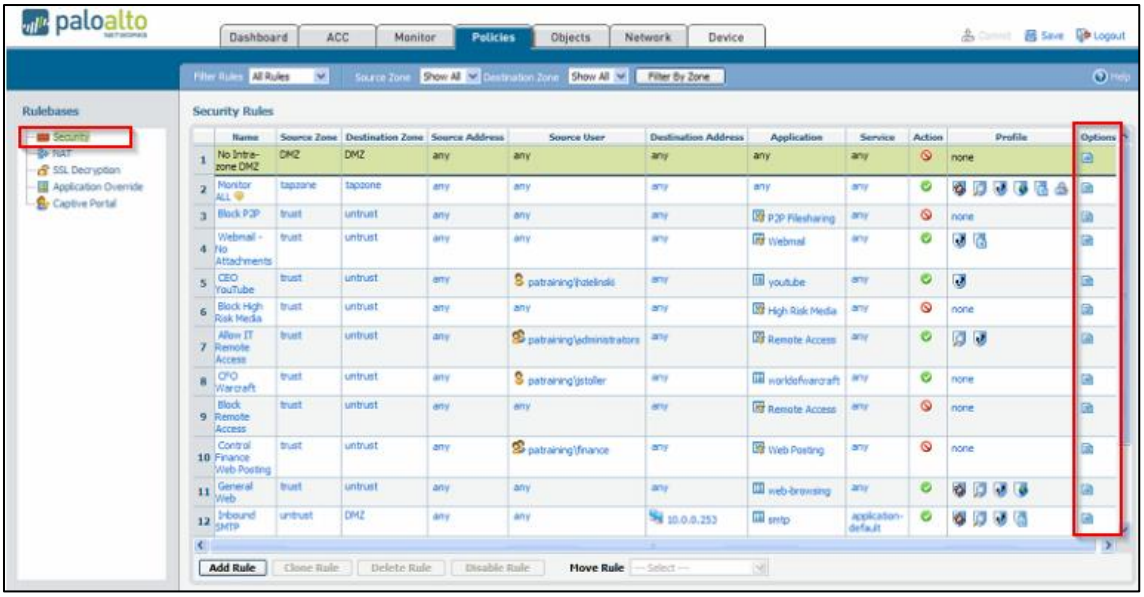


2. In the **Traffic Settings** > **Syslog**, select the syslog server profile created earlier for forwarding the traffic logs to the configured server.



3. Go to the **Policies** tab and click **Security** to go to the **Security Rules** page.

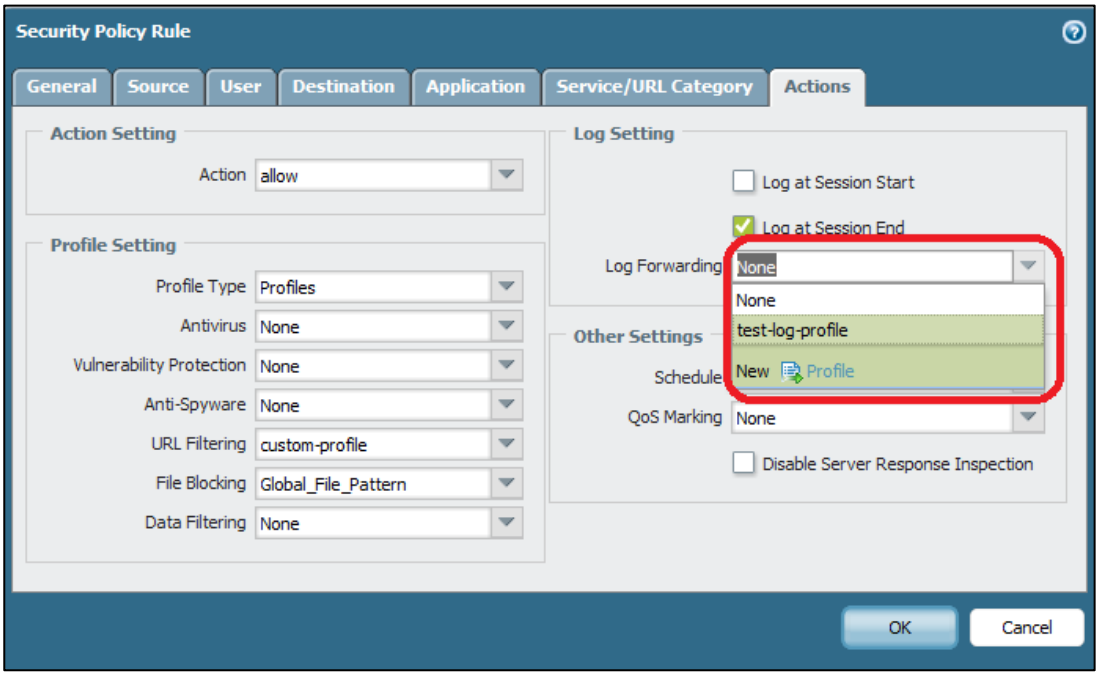
4. To view the rules for specific zones, select a zone from the **Source Zone** or **Destination Zone** drop-down list and click **Filter by Zone**.



5. Click **Options**; specify any combination of the following options:

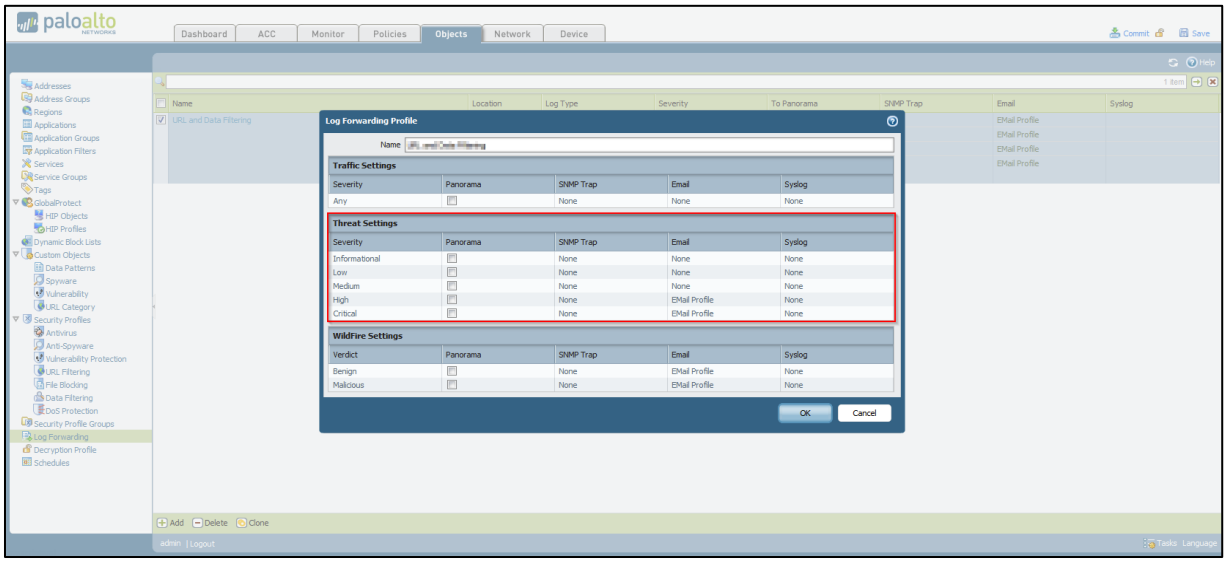
   - Ensure **Send Traffic Log** at session end for action is set to **allow** (by default, it is set to allow).
   - Ensure **Send Traffic Log** at session start for action is set to **deny.**

6. In the **Actions** tab, from the **Log Forwarding** drop-down list select the earlier created syslog server profile and click **OK** to save.

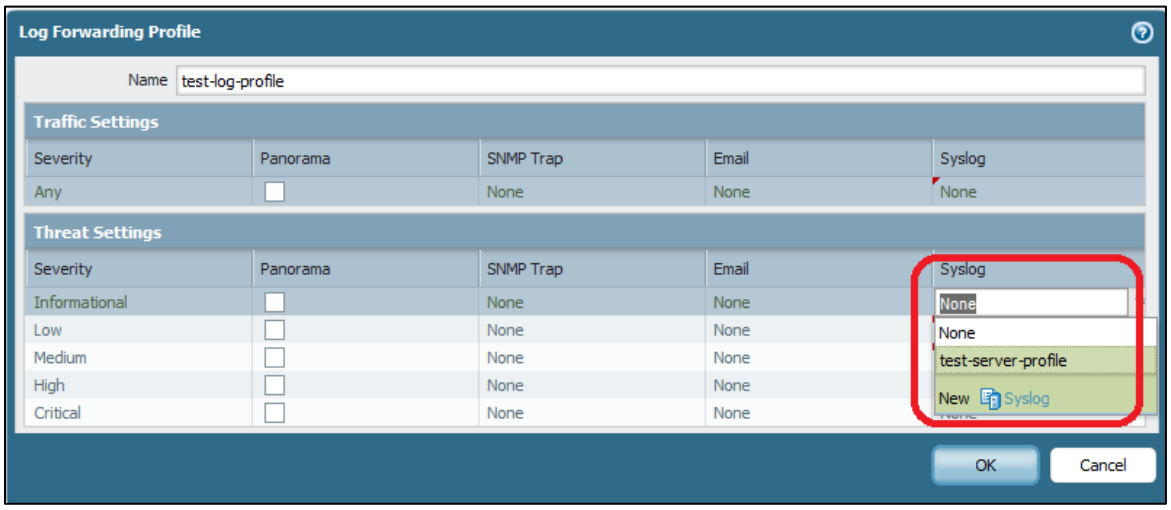


3.1.5 Defining the Threat log settings

1. In the **Palo Alto Networks** interface, go to **Objects** > **Log forwarding** and click **Add** to create a new profile.



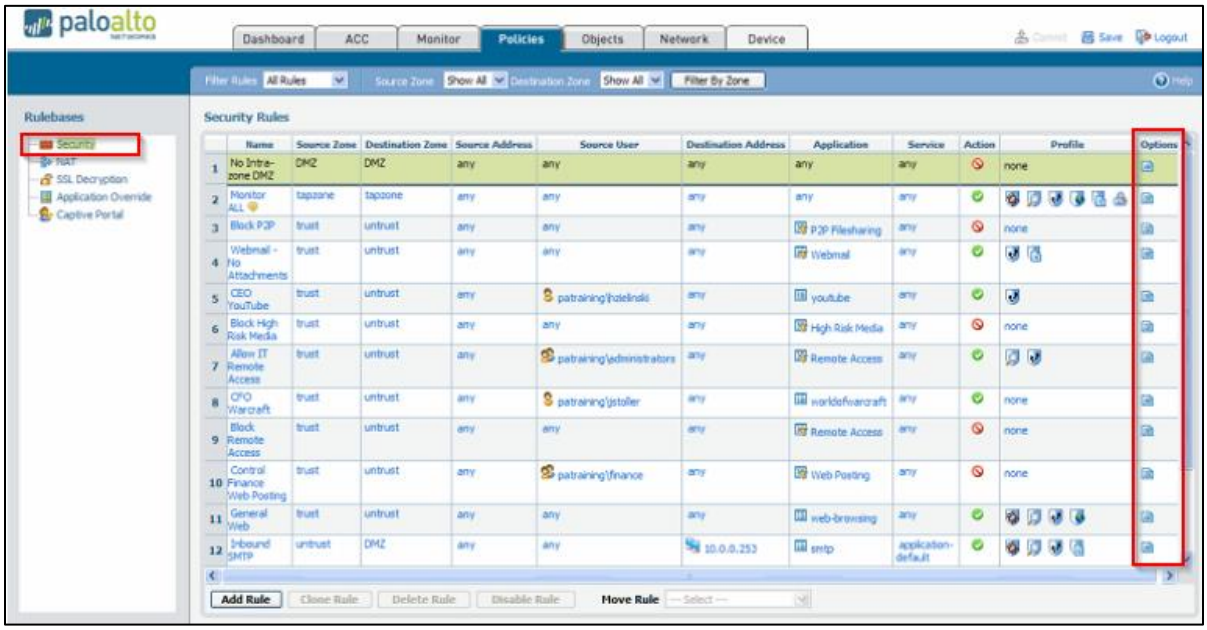
2. Select the syslog server profile created in **Threat Settings** > **Syslog** for forwarding threat logs to the configured server.



3. Go to the **Policies** tab, click **Security** to go to the **Security Rules**.

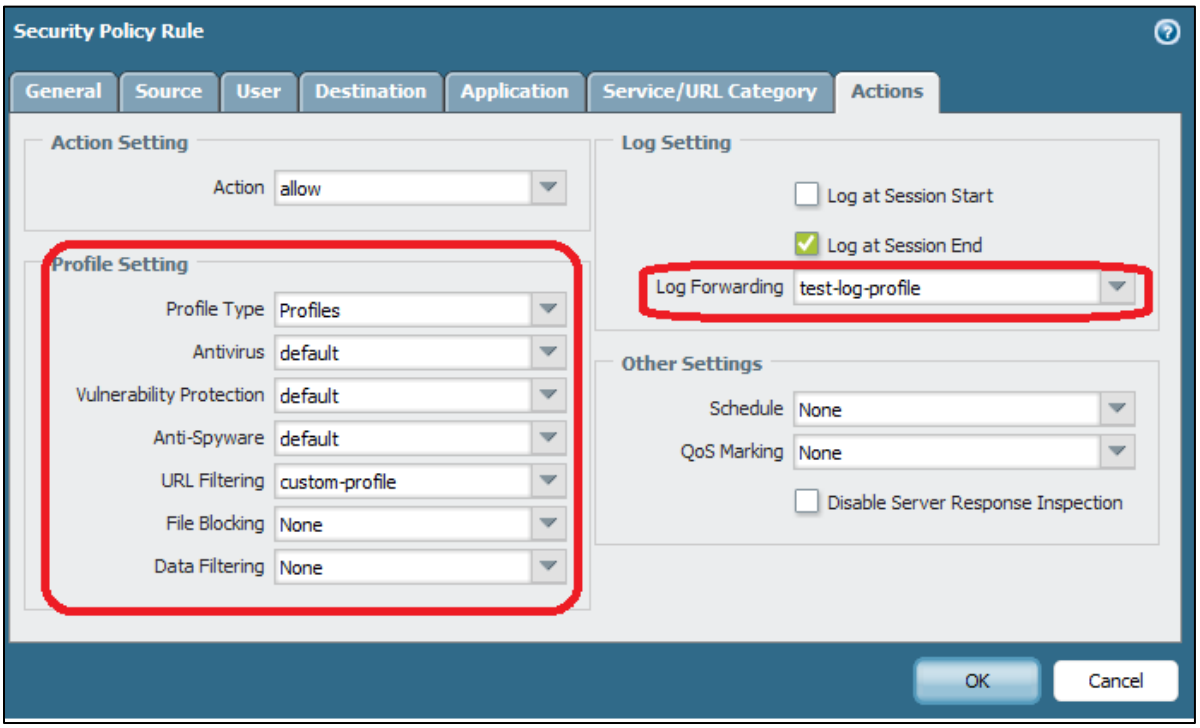
4. To view the rules for specific zones, select a zone from the Source Zone or Destination Zone drop-down list, and click **Filter by Zone**.

5. Select the rule for which you require to forward the logs.



6. Click **Options** to apply the security profiles to the selected rule.

7. In the **Actions** tab, from the **Log Forwarding** drop-down, select the created syslog server profile menu, and click **OK** to save.



3.2 Enable Syslog Forwarding in Palo Alto Firewall version 8.0

3.2.1 Configure a Syslog server profile.

1. In the **Palo Alto Networks** interface, go to **Device** > **Server Profiles** > **Syslog**.
2. In the **Syslog** interface, 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 following information for the firewall to connect.
   - **Name** - Unique name for the server profile.
   - **Syslog Server** - Enter the **Open XDR Manager's** FQDN or the IP Address.

     Note:

     Recommended using the FQDN.
   - **Transport** - Select UDP as the protocol for communicating with the syslog server.
   - **Port** - The port number on which to send syslog messages (default is UDP on port 514); you must use the same port number on the firewall and the syslog server.
   - **Format** - Select the syslog message format to use: **BSD** (the default) or **IETF**. Traditionally, **BSD** format is over **UDP** and **IETF** format is over TCP or SSL/TLS.

- **Facility** - Select a syslog standard value (default is **LOG_USER**) to calculate the priority (PRI) field in your syslog server implementation. Select the value that maps to how you use the PRI field to manage your syslog messages.

5. After providing the necessary details, click **OK** to save the server profile.

3.2.2 Configure Log Forwarding

The profile defines the destinations for Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, Tunnel and Authentication logs.

1. In the **Palo Alto Networks** interface, go to **Objects** -> **Log Forwarding** and click **Add** profile.
2. Enter a **Name** to identify the profile.

   Note:

   If you want the firewall to automatically assign the profile to new security rules and zones, provide default. If you do not want a default profile, or you want to override an existing default profile, provide a Name that will help you identify the profile when assigning it to security rules and zones.

3. Then, click **Add** to add one or more match list profiles.
   a. Enter a **Name** to identify the profile.
   b. Select the **Log Type**.
   c. In the **Filter** drop-down list, select **Filter Builder** and **Add** the following parameters.
      - **Connector** logic.
      - Log **Attribute.**
      - **Operator** to define inclusion or exclusion logic.
      - Attribute **Value** for the query to match.
   d. Select Panorama if you want to forward the logs to Log Collectors or the Panorama management server.
   e. For each type of external service that you use for monitoring (SNMP, Email, Syslog, and HTTP), **Add** one or more server profiles.
4. Click **OK** to save the Log Forwarding profile.

3.2.3 Assign the Log Forwarding profile to policy rules and network zones.

Perform the following steps for each rule that you want to trigger log forwarding.

1. In the **Palo Alto Networks** interface, go to **Policies** -> **Security** and click **Edit** to edit the rules.
2. Select **Actions** and select the **Log Forwarding profile** you created.
3. Set the **Profile Type** to **Profiles** or **Group**, and then select the **security profiles** or **Group Profile** to which the log generation and forwarding must be triggered.
   - **Threat logs** - Traffic must match any security profile assigned to the rule.
   - **WildFire Submission logs** - Traffic must match a WildFire Analysis profile assigned to the rule.

4. For Traffic logs, select **Log At Session Start** and/or **Log At Session End**.
5. Click **OK** to save the rule.

3.2.4 Configure syslog forwarding for Traffic, Threat, and WildFire Submission logs.

1. In the **Palo Alto Networks** interface, go to **Objects** > **Log Forwarding**, click **Add** and enter a **Name** to identify the profile.
2. For each log type and each severity level or WildFire verdict, select the **Syslog** server profile and click **OK**.

3.2.5 Configure syslog forwarding for System, Config, HIP Match, and Correlation logs.

1. In the **Palo Alto Networks** interface, go to **Device** -> **Log Settings**.
2. For **System and Correlation logs**, click each Severity level and select the **Syslog** server profile, and then click **OK**.
3. For **Config, HIP Match, and Correlation logs**, edit the section, select the **Syslog** server profile, and then click **OK**.

3.2.6 Create a certificate to secure syslog communication over TLSv1.2

The syslog server uses the certificate to verify that the firewall is authorized to communicate with the syslog server.

Note:

This is required only if the syslog server uses client authentication.

Ensure the following conditions are met:

- The private key must be available on the sending firewall; the keys cannot reside on a Hardware Security Module (HSM).
- The subject and the issuer for the certificate must not be identical.
- The syslog server and the sending firewall must have certificates that the same trusted certificate authority (CA) signed. Alternatively, you can generate a self-signed certificate on the firewall, export the certificate from the firewall, and import it into the syslog server.

1. In the **Palo Alto Networks** interface, go to **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and click **Generate**.
2. Enter a **Name** for the certificate.
3. In the **Common Name** field, enter the IP address of the firewall that forwards the logs to the syslog server.
4. In **Signed by**, select the trusted CA or the self-signed CA that both the syslog server and the firewall (the firewall that forwards the logs to the syslog server) trusts

5. The certificate cannot be a **Certificate Authority** nor an **External Authority** (certificate signing request [CSR]).
6. Click **Generate**. The firewall generates the certificate and key-pair.
7. Click the certificate Name to edit it, select the **Certificate for Secure Syslog** check box, and click **OK**.

4 Data Source Integrations (DSIs) in the Netsurion Open XDR platform

After the logs are received by the Netsurion Open XDR platform, configure the Data Source Integrations in the Netsurion Open XDR platform.

The Data Source Integrations package contains the following files for the Palo Alto Firewall.

- Categories_Palo Alto Firewall.iscat
- Alerts_Palo Alto Firewall.isalt
- Reports_Palo Alto Firewall.etcrx
- KO_Palo Alto Firewall.etko
- Dashboards_Palo Alto Firewall.etwd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in the Netsurion Open XDR platform.

Data Source Integrations Details

4.1 Alerts

Name	Description
Palo Alto Firewall: Configuration success and failure	This alert is generated whenever any configuration succeeds or fails in the Palo Alto Firewall.
Palo Alto Firewall: VPN configuration changes	This alert is generated whenever any VPN configuration is modified in the Palo Alto Firewall.
Palo Alto Firewall: Logon failure	This alert is generated whenever any logon failure occurs in the Palo Alto Firewall.
Palo Alto Firewall: VPN login failures	This alert is generated whenever any VPN login failure occurs in the Palo Alto Firewall.
Palo Alto Firewall: User login success outside US	This alert is generated when any logon failure has occurred outside the US region.

Name	Description
Palo Alto Firewall: Virus detected	This alert is generated whenever Palo Alto Firewall detects any virus in the traffic.
Palo Alto Firewall: Vulnerability detected	This alert is generated whenever Palo Alto Firewall detects any vulnerability in the traffic.

4.2 Reports

Name	Description
Palo Alto Firewall - Traffic details	This report provides information related to the traffic flow. It includes session id, source address, source port, source location, destination address, destination port, destination location, protocol type, total bytes, bytes sent, bytes received, total packets, packets sent, and packets received.
Palo Alto Firewall - Configuration success and failure	This report provides information related to any modifications in the Palo Alto firewall configuration. It includes user, source IP, console type, and configuration path.
Palo Alto Firewall - VPN configuration changes	This report provides information related to any modifications in Palo Alto firewall's VPN configuration. It includes user, source IP, console type, and configuration path.
Palo Alto Firewall - VPN activities	This report provides information related to all VPN activities of Palo Alto firewall.
Palo Alto Firewall - Logon failure	This report provides information related to the user logon failures in the Palo Alto firewall. It includes source IP, user, and reason.
Palo Alto Firewall - Logon success	This report provides information related to the successful user login in Palo Alto firewall. It includes source IP and user.
Palo Alto Firewall - VPN login failures	This report provides information related to VPN logon failure in Palo Alto firewall. It includes source IP, user, and reason.
Palo Alto Firewall - VPN login and logout activity	This report provides information specific to all VPN login and logout activity of Palo Alto firewall.

Name	Description
Palo Alto Firewall - Threat details	This report provides information related to the threat detection. It includes threat id, protocol type, action taken, source address, source port, source location, destination address, destination port, and destination location.

4.3 Dashboards

Name	Description
Palo Alto Firewall - Traffic by Source IP address	This dashlet displays data of the Traffic by source IP address.
Palo Alto Firewall - Traffic by Destination IP address	This dashlet displays the data of the Traffic by destination IP address.
Palo Alto Firewall - Traffic by Source IP Geo-Location	This dashlet displays data of the Traffic by source IP location.
Palo Alto Firewall - Traffic by Destination IP Geo-Location	This dashlet displays the data of the Traffic by destination IP location.
Palo Alto Firewall - Login Activities by User	This dashlet displays the data of the Login Activities by username.
Palo Alto Firewall - Login by Source IP Geo-location	This dashlet displays the data of the Logins by source IP location.
Palo Alto Firewall - Login Failed by Source IP	This dashlet displays the data of the Login Failures by source IP.
Palo Alto Firewall - Login Failed by Geo-Location	This dashlet displays the data of the Login Failures by source IP location.
Palo Alto Firewall - Login Failed by User	This dashlet displays data about login failure by user.
Palo Alto Firewall - Intrusion Detection by Destination IP Geo-Location	This dashlet displays data of the Intrusion Detection by destination IP location.
Palo Alto Firewall - Intrusion Detection by Destination IP	This dashlet displays the data of the Intrusion Detection by destination IP.
Palo Alto Firewall - Intrusion Detection by Source IP	This dashlet displays the data of the Intrusion Detection by source IP.
Palo Alto Firewall - Intrusion Detection by Threat Name and Action	This dashlet displays the data of the Intrusion Detection by threat name and action.

Name	Description
Palo Alto Firewall - Intrusion Detection by Source IP Geo-Location	This dashlet displays the data of the Intrusion Detection by source IP location.

4.4 Saved Search

Name	Description
Palo Alto Firewall - Allowed traffic	This saved search provides detailed information of the allowed traffics into the organization via firewall.
Palo Alto Firewall - Configuration success and failure	This saved search provides the information about all the configurational changes (success or failure) that happened in firewall console.
Palo Alto Firewall - Denied traffic	This saved search provides detailed information of the denied traffics.
Palo Alto Firewall - VPN activities	This saved search provides detailed information about all the firewall VPN activities.
Palo Alto Firewall - VPN configuration changes	This saved search provides the information about all the VPN configurational changes.
Palo Alto Firewall - Logon failures	This saved search provides detailed information of the failed logins to the firewall console.
Palo Alto Firewall - Logon success	This saved search provides detailed information of the successful logins to the firewall console.
Palo Alto Firewall - URL filtering	This saved search provides information about the URL details filtered by the firewall.
Palo Alto Firewall - VPN login and logout activity	This saved search provides the information about the VPN login and logout activities.
Palo Alto Firewall - VPN login failures	This saved search provides the information about the VPN login failures.
Palo Alto Firewall - Vulnerability detected	This saved search provides the information of any vulnerability detected by the firewall.
Palo Alto Firewall - Virus detected	This saved search provides information about the Virus details detected by the firewall.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials-Support@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support