NetWitness® Platform

Palo Alto Networks Enterprise Firewall Event Source Log Configuration Guide

NETWITNESS
Platform

Palo Alto Networks Enterprise Firewall

Last Modified: Monday, September 30, 2024

Event Source Product Information:

Vendor: Palo Alto

Event Source: Networks Firewall

Versions: PAN OS 3.0, 4.0.7, 5.0, 6.0, 6.1, 6.1.x, 7.0, 7.1, 8.x, 9.x,10.x

Note: NetWitness supports the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case in the NetWitness Community Portal for support.

NetWitness Product Information:

Supported On: NetWitness Platform 12.3 and later

Event Source Type: paloaltonetworks, cef

Collection Method: Syslog

Event Source Class.Subclass: Security.Firewall

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

September 2024

Contents

To configure the Palo Alto Networks Enterprise Firewall event source, you must:

I. Configure Syslog Output on Palo Alto Networks Enterprise Firewall

II. Configure NetWitness Platform for Syslog Collection

Configure Syslog Output on Palo Alto Networks Enterprise Firewall

Configuration instructions are provided for the following versions:

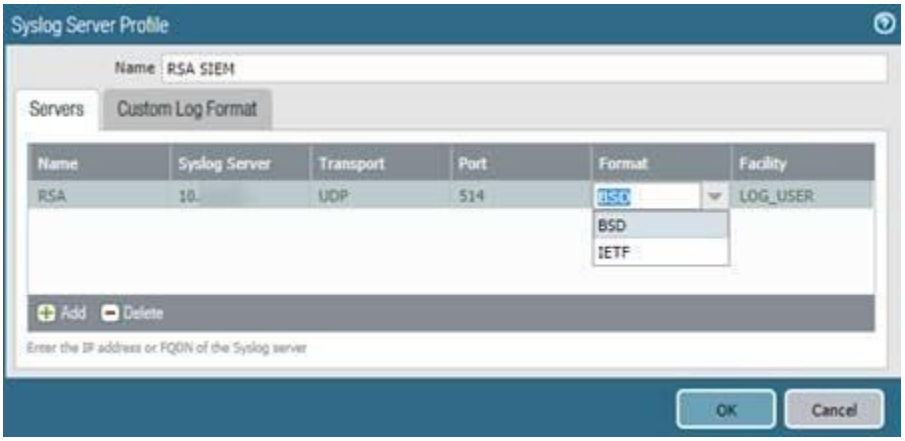
- Configure Palo Alto Networks Enterprise Firewall on PAN OS 9.x, 10.x
- Configure Palo Alto Networks Enterprise Firewall on PAN OS 5.0 and later
- Configure Palo Alto Networks Enterprise Firewall on PAN OS 4.0 and earlier

Note: For paloalto PAN-OS version 4.x or later, we recommend to use cef configuration steps and send logs in CEF format to Netwitness. Please refer the document for more details: https://docs.paloaltonetworks.com/resources/cef

Configure Palo Alto Networks Enterprise Firewall on PAN OS 9.x, 10.x

To configure Palo Alto Networks Enterprise Firewall:

1. Log on to the Palo Alto Networks Enterprise Firewall with administrative credentials.
2. To add the NetWitness Platform to Palo Alto Networks Enterprise Firewall, follow these steps:
   a. Click the **Device** tab.
   b. From the navigation menu, click **Server Profiles** > **Syslog**.
   c. Click **New**.
   d. In the **Name** field, enter a name for your NetWitness Platform.
   e. In the **Server** field, enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
   f. Select a log format, either BSD or IETF.



g. Ensure that the port is set to **514** and that the facility value is set to **LOG_USER**.

h. Click **OK**.

3. To configure Palo Alto Networks Enterprise Firewall to send system logs to the NetWitness Platform, follow these steps:

a. Click the 

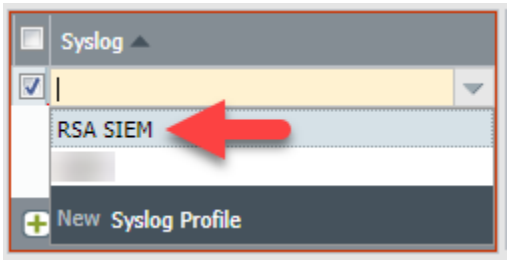
button.

b. Give the configuration a name.

c. Under the Syslog box, click 

.

d. Select the name of the Device you configured in Step 1 above.



e. Click the **Device** tab.

f. From the navigation menu, click **Log Settings** > **System**.

g. Click **Edit**.

h. From the **Syslog** drop-down list of each category of messages that you want to forward to the NetWitness Platform, select the name of the RSA NetWitness Platform that you specified in step 2.

i. Click **OK**.

4. To configure Palo Alto Networks Enterprise Firewall to send configuration logs to the NetWitness Platform, follow these steps:

a. Click the **Device** tab.

b. From the navigation menu, click **Log Settings** > **Config**.

c. Click the  button.

d. From the **Syslog** drop-down list, select the name of the RSA NetWitness Platform that you specified in step 2.

e. Click **OK**.

5. To forward logs to the NetWitness Platform based on specified rules, follow these steps:

a. Click the **Objects** tab.

b. From the **Log Forwarding** icon, click **Add** at the bottom of the central window pane.

c. Enter the name of your NetWitness Platform appliance.

d. For **Traffic Settings** section, select under the Syslog tab and choose your appliance name.

e. Under **Threat Settings** section, for all **Severity** select the name of your appliance under the Syslog tab.

f. Click **Ok**.

6. To forward logs to the NetWitness Platform based on specified rules, follow these steps:

a. Click the **Device** tab.

b. From the navigation menu, click **Log Settings** > **HIP Match**.

c. Click **Edit**.

d. From the Syslog drop-down list, select the name of the RSA NetWitness Platform appliance that you specified in Step 2.

e. Click **Ok**.

7. From the top menu, click **Save**.

8. From the top menu, click **Commit** to confirm all the changes.

Configure Palo Alto Networks Enterprise Firewall on PAN OS 5.0 and later

To configure Palo Alto Networks Enterprise Firewall:

1. Log on to the Palo Alto Networks Enterprise Firewall with administrative credentials.
2. To add the RSA NetWitness Platform to Palo Alto Networks Enterprise Firewall, follow these steps:

a. Click the **Device** tab.

b. From the navigation menu, click **Server Profiles** > **Syslog**.

c. Click **New**.

d. In the **Name** field, enter a name for your RSA NetWitness Platform.

e. In the **Server** field, enter the IP address of the NetWitness Log Decoder or Remote Log Collector.

f. Ensure that the port is set to **514** and that the facility value is set to **LOG_USER**.

g. Click **OK**.

3. To configure Palo Alto Networks Enterprise Firewall to send system logs to the RSA NetWitness Platform, follow these steps:

   a. Click the **Device** tab.

   b. From the navigation menu, click **Log Settings** > **System**.

   c. Click **Edit**.

   d. From the **Syslog** drop-down list of each category of messages that you want to forward to the RSA NetWitness Platform, select the name of the NetWitness Platform that you specified in step 2.

   e. Click **OK**.

4. To configure Palo Alto Networks Enterprise Firewall to send configuration logs to the RSA NetWitness Platform, follow these steps:

   a. Click the **Device** tab.

   b. From the navigation menu, click **Log Settings** > **Config**.

   c. Click **Edit**.

   d. From the **Syslog** drop-down list, select the name of the NetWitness Platform that you specified in step 2.

   e. Click **OK**.

5. To forward logs to the NetWitness Platform based on specified rules, follow these steps:

   a. Click the **Objects** tab.

   b. From the **Log Forwarding** icon, click **Add** at the bottom of the central window pane.

   c. Enter the name of your NetWitness Platform appliance.

   d. For **Traffic Settings** section, select under the Syslog tab and choose your appliance name.

   e. Under **Threat Settings** section, for all **Severity** select the name of your appliance under the Syslog tab.

   f. Click **Ok**.

6. To forward logs to the NetWitness Platform based on specified rules, follow these steps:

   a. Click the **Device** tab.

   b. From the navigation menu, click **Log Settings** > **HIP Match**.

   c. Click **Edit**.

   d. From the Syslog drop-down list, select the name of the RSA NetWitness Platform appliance that

you specified in Step 2.

e. Click **Ok**.

7. From the top menu, click **Save**.
8. From the top menu, click **Commit** to confirm all the changes.

Configure Palo Alto Networks Enterprise Firewall on PAN OS 4.0 and earlier

To configure Palo Alto Networks Enterprise Firewall:

1. Log on to the Palo Alto Networks Enterprise Firewall with administrative credentials.
2. To add the RSA NetWitness Platform to Palo Alto Networks Enterprise Firewall, follow these steps:
   a. Click the **Device** tab.
   b. From the navigation menu, click **Server Profiles** > **Syslog**.
   c. Click **Add**.
   d. In the **Name** field, enter a name for your [[[Undefined variable SAVariables.ProductSuiteName]]].
   e. In the **Server** field, enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
   f. Ensure that the port is set to **514** and that the facility value is set to **LOG_USER**.
   g. In the top right menu bar, click **Save**.
3. To configure Palo Alto Networks Enterprise Firewall to send system logs to the RSA NetWitness Platform, follow these steps:
   a. Click the **Device** tab.
   b. From the navigation menu, click **Log Settings** > **System**.
   c. From the **Syslog** drop-down list of each category of messages that you want to forward to the RSA NetWitness Platform, select the name of the RSA NetWitness Platform that you specified in step 2.
   d. Click **OK**.
   e. Click **Apply**.
   f. Click **Save**.
5. From the top menu, click **Save**.
6. From the top menu, click **Commit** to confirm all the changes.

Configure NetWitness Platform

Perform the following steps in NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in NetWitness Platform Live.

Ensure that the parser for your event source is available:

1. In the **NetWitness** menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions (** **)** menu, choose **View** > **Config**.
3. In the **Service Parsers Configuration** panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: If you send logs in CEF format to Netwitness, the required parser is **cef**. Otherwise, the required parser is **paloaltonetworks**.

Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness. You only need to configure either the Log Decoder or the Remote Log Collector for Syslog, not both.

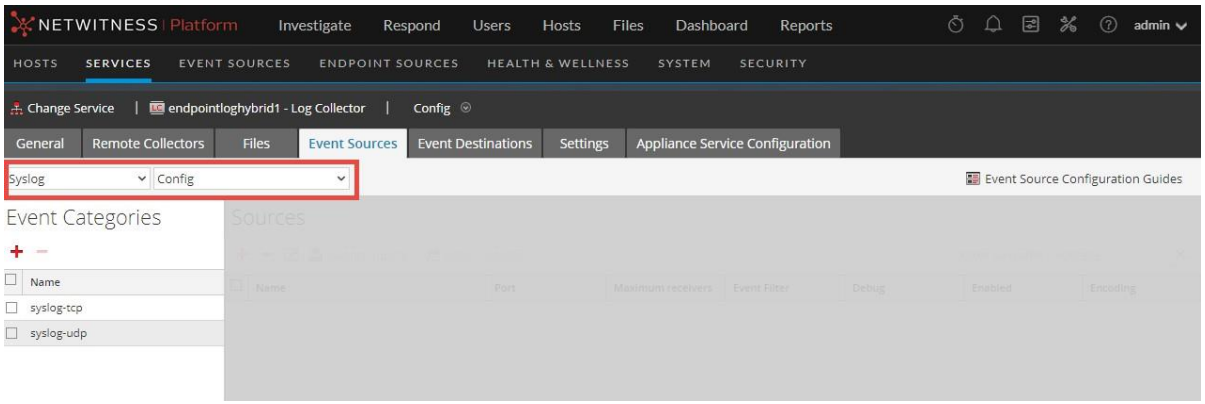
To configure Log Decoder for Syslog Collection

1. In the NetWitness Platform menu, select  (Admin) > **Services**.
2. In the **Services** grid, choose a Log Decoder and from the **Actions (** **)** menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see  , click the icon to start capturing Syslog.
   - If you see  , you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure Remote Log Collector for Syslog Collection

1. In the NetWitness Platform menu, go to (Admin) > **Services**.
2. In the **Services** grid, select a Remote Log Collector and from the **Actions** ( ) menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog / Config** from the drop-down menu.

   The **Event Categories** panel displays the Syslog event sources that are configured, if any.

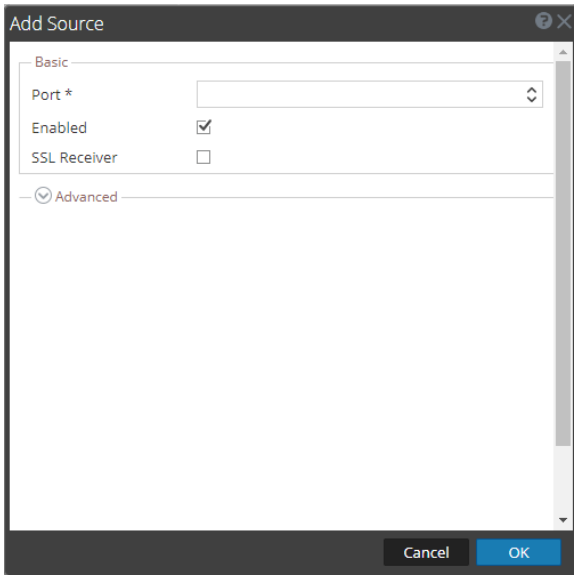


4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog will appear.

5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Choose the **New Type** in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog will appear.



7. Enter **514** for the port and choose **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

After you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. You can continue to add Syslog event sources to your system without a need to do any further configuration in NetWitness Platform.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.