

NetWitness[®] Platform XDR

Fortinet FortiGate Event Source Log Configuration Guide

Fortinet FortiGate

Event Source Product Information:

Vendor: [Fortinet](#)

Event Source: FortiGate

Versions: FortiOS v 2.8, 3.0, 4.0 MR1, 4.0 MR2, 5.x, 6.x

Note: NetWitness is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.5 or later

Event Source Log Parser: fortinet

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 and 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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2022

Contents

Configure Syslog Output on Fortinet FortiGate	6
Configure CEF Logging for Fortinet FortiGate 6.4.9	6
Configure Fortinet FortiGate 5.x or higher	6
Configure Fortinet FortiGate 4.0 MR1 or 4.0 MR2	6
Configure Firewall Policy Logging	7
Configure Protection Profile Logging	7
Configure Log Setting	7
Configure Fortinet FortiGate 3.0	7
Enable Traffic Logging	8
Configure Firewall Policy Logging	8
Configure Protection Profile Logging	8
Configure Log Setting	8
Configure Fortinet FortiGate 2.8	9
Enable Traffic Logging	9
Configure Log Settings	9
Configure NetWitness Platform XDR for Syslog Collection	10
Enable the Parser	10
Configure Syslog Collection	10
Getting Help with NetWitness Platform XDR	12
Self-Help Resources	12
Contact NetWitness Support	12
Feedback on Product Documentation	13

To configure the Fortinet FortiGate event source, you must:

- I. [Configure Syslog Output on Fortinet FortiGate](#)
- II. [Configure NetWitness Platform XDR for Syslog Collection.](#)

Configure Syslog Output on Fortinet FortiGate

Configure your version of FortiGate:

- [Configure CEF Logging for Fortinet FortiGate 6.4.9](#)
- [Configure Fortinet FortiGate 5.x or higher](#)
- [Configure Fortinet FortiGate 4.0 MR1 or 4.0 MR2](#)
- [Configure Fortinet FortiGate 3.0](#)
- [Configure Fortinet FortiGate 2.8](#)

Configure CEF Logging for Fortinet FortiGate 6.4.9

To enable CEF logging to the Syslog server:

Log into the FortiGate Command Line Interface as Administrator and enter the following commands:

```
config log syslogd setting
set format cef
end
```

Configure Fortinet FortiGate 5.x or higher

To enable logging to the Syslog server:

Log into the FortiGate Command Line Interface as Administrator and enter the following commands:

```
config log syslogd setting
set status enable
set server NW-IP-address
set csv disable
set facility facility-name
end
```

Where:

- **NW-IP-address** is the IP address of the NetWitness Log Decoder or Remote Log Collector.
- **facility-name** is a name of your choice.

Note: For the facility option, NetWitness supports loca.l0, local1, and so on.

Configure Fortinet FortiGate 4.0 MR1 or 4.0 MR2

To configure logging for version 4.0 MR1 or 4.0 MR2, you must complete these tasks:

Note: If you are using FortiGate 4.0 MR2, you must enable logging for each component and only complete task III.

- I. Configure firewall policy logging.
- II. Configure protection profile logging.
- III. Configure log settings.

Configure Firewall Policy Logging

1. Click **Firewall > Policy**.
2. Edit each policy by selecting **Log Allowed Traffic**.
3. Click **OK**.

Configure Protection Profile Logging

1. Click **Firewall > Protection Profile**.
2. Select the protection profile that you want to use and select **Edit**.
3. Click the blue arrow next to **Logging** and select the features that you want to log.
4. Click **OK**.

Configure Log Setting

1. Click **Log&Report > Log Config > Log Setting**.
2. Select **Remote Logging and Archiving**.
3. Select **Syslog** and follow these steps:
 - a. Enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
 - b. In the port number field, type **514**.
 - c. Select the logging severity level except **Debug**.
 - d. Select the log facility.
 - e. Make sure the **Enable CSV format** option is not selected.
4. Click **Apply**.

Configure Fortinet FortiGate 3.0

To configure logging for version 3.0, you must complete these tasks:

- I. Enable traffic logging per interface.
- II. Configure firewall policy logging.
- III. Configure protection profile logging.
- IV. Configure log settings.

Enable Traffic Logging

1. Click **System > Network > Interface**.
2. Select the **Edit** icon for an interface.
3. Select **Log**.
4. Click **OK**.
5. Repeat steps 1 through 4 for each interface you want to enable logging.

Configure Firewall Policy Logging

1. Click **Firewall > Policy**.
2. Edit each policy by selecting **Log Allowed Traffic**.

Configure Protection Profile Logging

1. Click **Firewall > Protection Profile**.
2. For the protection profile that you want to use, select **Edit**.
3. Click the blue arrow next to **Logging** and select all necessary settings.

Configure Log Setting

1. Click **Log&Report > Log Config > Log Setting**.
2. Select the locations to which you want to log.
3. Select the blue arrow next to the location and follow these steps:
 - a. If you are logging to a remote location, enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
 - b. If you are logging to a remote syslog server, in the port number field, type **514**.
 - c. Select the logging severity level.
 - d. Select the log facility.
 - e. If you are logging to the local disk, configure the log roll settings.
 - f. Make sure the **Enable CSV format** option is not selected.
4. Repeat step 3 to configure additional logging locations.
5. Click **Apply**.

Configure Fortinet FortiGate 2.8

To configure logging for version 2.8, you must complete these tasks:

- I. Enable traffic logging.
- II. Configure log settings.

Enable Traffic Logging

You can enable traffic logging for an interface or VLAN subinterface (if available). All connections to and through the interface are recorded in the traffic log.

To enable traffic logging:

1. Click **System > Network > Interface**.
2. Select the **Edit** icon for an interface.
3. Select **Log**.
4. Click **OK**.
5. Repeat steps 1 through 4 for each interface you want to enable logging.

Configure Log Settings

Log setting configuration is organized by log location. Configure log settings for each location you want to record logs. If you want to log traffic, you must also enable traffic logging for specific interfaces and firewall policies.

To configure log setting:

1. Click **Log&Report > Log Config > Log Setting**.
2. Select the locations you want to log.
3. Select the blue arrow next to the location, and follow these steps:
 - a. If you are logging to a remote location, enter the IP address of the NetWitness Log Decoder or Remote Log Collector.
 - b. If you are logging to a remote syslog server, in the port number field, type **514**.
 - c. Select the logging severity level.
 - d. If you are logging to the local disk, configure the log roll settings.
 - e. Make sure the **Enable CSV format** option is not selected.
4. Repeat step 3 to configure additional logging locations.
5. Click **Apply**.

Configure NetWitness Platform XDR for Syslog Collection


Perform the following steps in NetWitness Platform XDR:

- Enable the parser
- Configure Syslog Collection.

Enable the Parser

If you do not see your parser in the list while performing this procedure, you need to download it in NetWitness Platform XDR 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: The required parser is **fortinet**.

Configure Syslog Collection


Note: Syslog collection must be configured only for the first time when you set up an event source which uses Syslog to send its output to NetWitness.

For Syslog, you can configure either the Log Decoder or the Remote Log Collector. You do not need to configure both.

To configure Log Decoder for Syslog Collection

1. In the **NetWitness** 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  **Start Capture**, click the icon to start capturing Syslog.
 - If you see  **Stop Capture**, 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** 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.

Getting Help with NetWitness Platform XDR

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 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 XDR 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 nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.