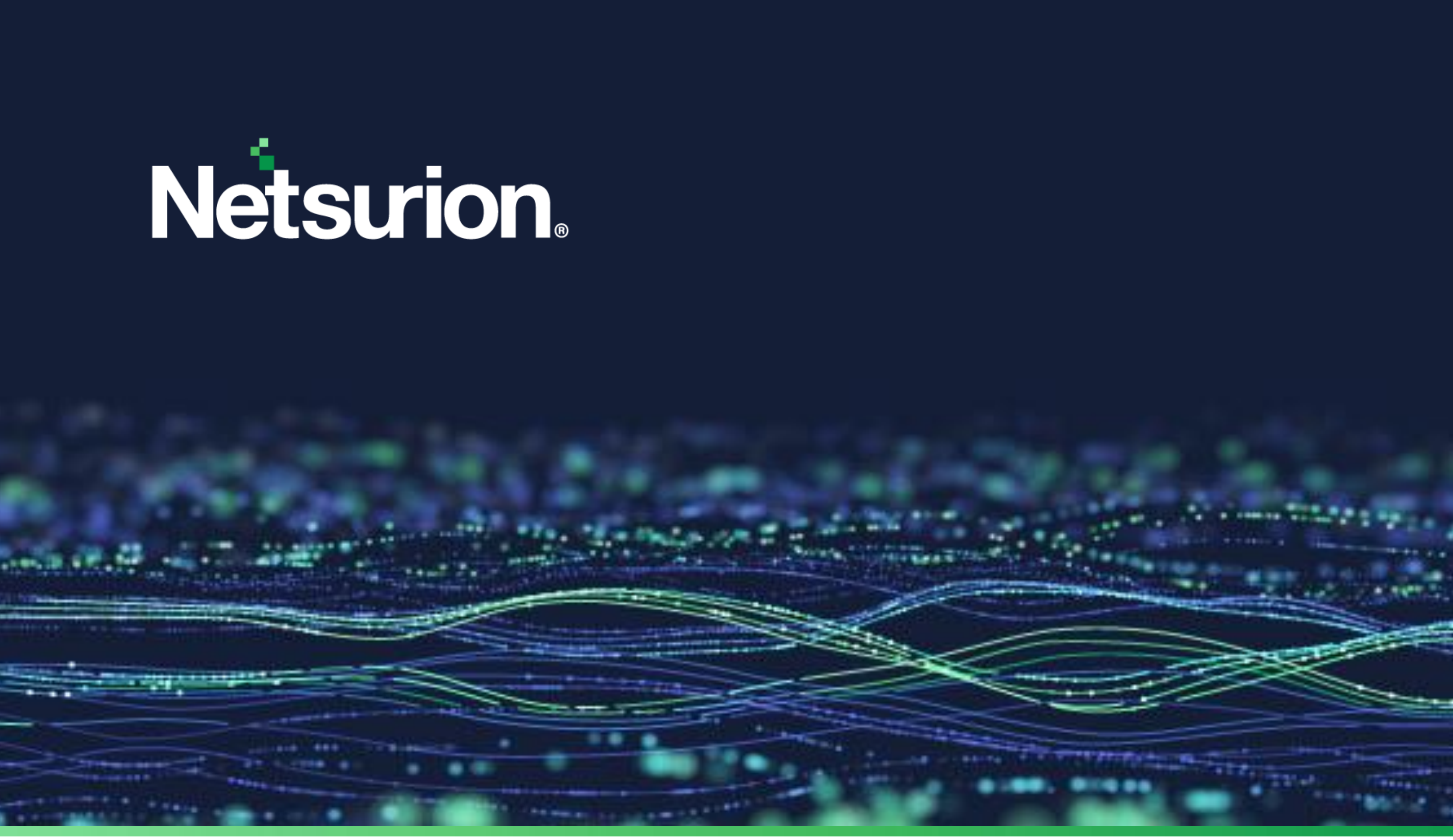


Integration Guide

Integrate Fortinet FortiGate with Netsurion Open XDR

Publication Date

October 04, 2023

Abstract

This guide provides instructions to configure and integrate Fortinet FortiGate with Netsurion Open XDR to retrieve its logs via syslog and forward them to Netsurion Open XDR.

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 Fortinet FortiGate and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Fortinet FortiGate in Netsurion Open XDR.

Table of Contents

1 Overview

Fortinet FortiGate firewall provides protection in various areas with other key security features such as anti-virus, intrusion prevention system (IPS), web filtering, anti-spam, and traffic shaping to deliver multi-layered security for the IT environment.

Netsurion Open XDR manages logs retrieved from Fortinet FortiGate firewall. The alerts, reports, dashboard, and saved searches in Netsurion Open XDR are enhanced by detecting any suspicious activities like security violations, user behavior, and traffic anomalies.

2 Prerequisites

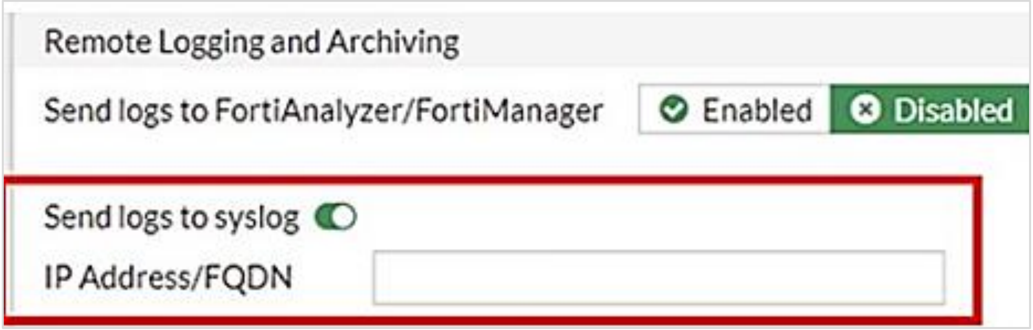
- Fortinet FortiGate firewall with FortiOS v6.0 and above must be installed.
- Port **514 (TCP)** must be open and dedicated to syslog communication.
- The Data Source Integration package.

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

3 Integrating Fortinet FortiGate with Netsurion Open XDR

3.1 Forwarding the Logs from FortiGate to Syslog Server

1. Log in to the FortiGate web interface and go to **Log & Report** > **Log Settings**
2. In **Remote Logging and Archiving**, toggle to enable **Send logs to syslog.**



Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager ○ Enabled [✓ ☒ Disabled]

Send logs to syslog ●

IP Address/FQDN

3. Specify the **IP Address/FQDN** (recommended using FQDN) of the Netsurion Open XDR manager.
4. After providing the appropriate details, click the **Apply** button.

> **Note:**
>
> The only way to verify the log format status is through the Command Line Interface. Refer to [Enabling Syslog Forwarding using CLI]() section for more details.

3.2 Configuring Syslog over TLS

Refer to the Configure syslog over TLS in Netsurion Open XDR document to configure syslog over TLS in Netsurion Open XDR.

3.3 Enabling Syslog Forwarding using CLI

The Fortinet unit can be configured to send logs to a remote computer that is running a syslog server. Using the CLI, you can send the logs up to three different syslog servers.

The following commands are used to configure the log settings for logging into a remote syslog server (available only in the CLI).

You can also configure additional syslog servers using syslogd2 and syslogd3 commands.

Syntax: `Config log {syslogd | syslogd2 | syslogd3} setting`

1. Set status to enable logging to a remote syslog server.

   Example: `set status enable`

2. Enable default format to allow the Fortinet unit to produce the logs in default format. If default format is not enabled, then the Fortinet unit produces plain text files.

   Example: `set default enable`

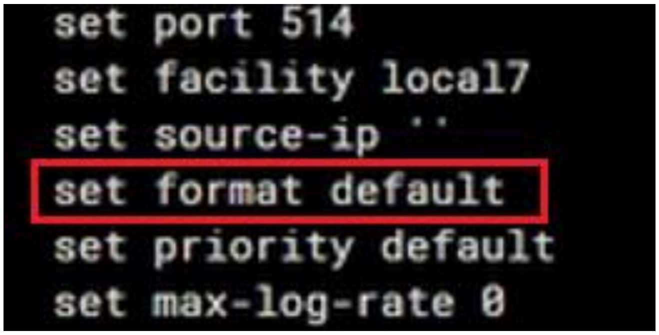
For a specific syslog server, if the log format is configured to something other than **default**, use the following command to set it to default.

- Use the following command to change the log format to default.

  ```
  # config log syslogd setting
  # set format default
  # end
  ```

- Use the following command to verify the change by listing parameters. The following command shows the full configuration of syslog setting. Check for the parameter,

  ```
  # set format default
  ```



```
  set port 514
  set facility local7
  set source-ip ''
  set format default
  set priority default
  set max-log-rate 0
```

3. Specify the facility type. Facility identifies the source of the log message to syslog.

```
Set facility {alert | audit | auth | authpriv | clock | cron |
daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4
| local5 | local6 | local7 | lpr | mail | news | ntp | syslog |
user | uucp}
```

Example: `set facility local3`

4. Specify the port number for communication with the syslog server.

Example: `set port 514`

5. Specify the reliable delivery of syslog messages to the syslog server.

Example: `set reliable enable`

6. Specify the IP address of the syslog server that stores the logs.

Example: `set server 172.168.22.54`

7. Specify the source IP address for syslogd, syslog2, and syslog3.

Example: `set source-ip 172.168.22.50`

Note:

If you need to enable the TLS, follow the below steps that are optional.

8. Specify the reliable syslog with the TLS encryption.

Example: `set enc-algorithm high`

9. Specify the TLS version to send logs securely.

Example: `set ssl-min-proto-version TLSv1-2`

Note:

Use the below command to set the certificate path.

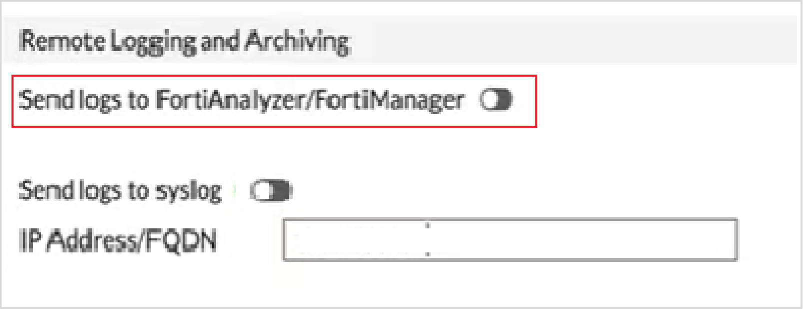
10. Specify the certificate to communicate with the Syslog server.

```
set certificate "<certificate local path>"
```

Example: `set certificate “/root/CACert.crt”`

3.4 Forwarding the Logs via FortiManager or FortiAnalyzer to Netsurion Open XDR

1. Log in to the FortiGate web interface and go to **Log & Report** > **Log Settings**
2. In **Remote Logging and Archiving**, specify the following details.



Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager

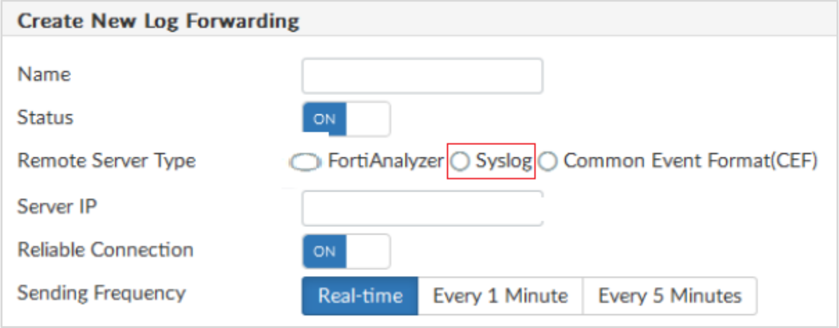
Send logs to syslog

IP Address/FQDN

   a. Toggle to enable **Send logs to FortiAnalyzer/FortiManager.**

   b. Specify the **FQDN/IP address** (recommended using FQDN) of the FortiAnalyzer/FortiManager device.

3. After providing the appropriate details, click the **Apply** button.
4. Log in to FortiAnalyzer Web GUI console and go to **System Settings** > **Advanced** > **Syslog Server.**
5. Click **Create New** in the toolbar to configure the New Syslog Server Settings.



Create New Log Forwarding

Name

Status: ON

Remote Server Type: ○ FortiAnalyzer ○ Syslog ○ Common Event Format(CEF)

Server IP

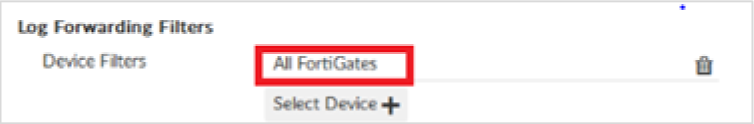
Reliable Connection: ON

Sending Frequency: [✓ Real-time] Every 1 Minute Every 5 Minutes

   a. Choose the **Syslog** option for **Remoter Server Type**

   b. For **Server IP**, specify Netsurion Open XDR FQDN/IP address (recommended using FQDN).

   c. Apply the **Device Filters** as **All FortiGate** in **log Forwarding Filter** section to send the FortiGate logs only to the specific Syslog server.



Log Forwarding Filters

Device Filters: All FortiGates

6. After providing the appropriate details, click the **Apply** button to save the configuration.

3.5 Applying Filters on FortiGate through CLI

3.5.1 Logs Sent Directly to Syslog Server

1. Log in to the FortiGate command line interface via root.
2. Execute the following command to forward logs to syslog for particular events instead of collecting for the entire category.

For example,

```
    # config log syslogd filter
    Set filter-type exclude
    Set filter
       “logid(00002,00011,00012,00013,00014,13312,13056,37127,
    54000,54400,54401,54802,54803,54804,54805)”
end
```

Note:

By setting **`filter-type exclude`** will exclude the logs that match the filter while forwarding it. For further information kindly go through the link Syslog filter to send specific logs.

3.5.2 Logs Sent via FortiAnalyzer to Syslog Server

1. Log in to the FortiGate command line interface via root.
2. Execute the following command to forward logs to syslog for specific events instead of collecting for the entire category.

For example,

```
    # config log fortianalyzer filter
    Set filter-type exclude
    Set filter
       “logid(00002,00011,00012,00013,00014,13312,13056,37127,
    54000,54400,54401,54802,54803,54804,54805)”
end
```

Note:

The parameter **`filter-type exclude`** will exclude the logs that match the filter while forwarding it. For further information, refer to Syslog filter to send specific logs.

4 Data Source Integrations (DSIs) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the DSIs in Netsurion Open XDR.

The Data Source Integrations package contains the following files for the Fortinet FortiGate.

- Categories_Fortinet FortiGate.iscat
- Alerts_Fortinet FortiGate.isalt
- Reports_Fortinet FortiGate.etcrx
- Template_Fortinet FortiGate.ettd
- KO_Fortinet FortiGate.etko
- Dashboards_Fortinet FortiGate.etwd
- Filters_Fortinet FortiGate.isfil

Note

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

4.1 Alerts

Name	Description
Fortinet FortiGate: Admin authentication failure	Generated when admin authentication failure event has been detected.
Fortinet FortiGate: Device reboot activity	Generated when the device reboot or restart event detected.
Fortinet FortiGate: DLP event detected	Generated when a potential DLP event has been detected.
Fortinet FortiGate: Firewall configuration change detected	Generated when the system detects change in firewall configuration.
Fortinet FortiGate: Intrusion or anomaly detected	Generated when a potential anomaly has been detected.
Fortinet FortiGate: Log deleted by user	Generated when the log is deleted by user.
Fortinet FortiGate: SSL VPN login failure detected	Generated when an SSL VPN login failure event has been detected while accessing the connection.
Fortinet FortiGate: User authentication failure	Generated when a user authentication failure has been detected.
Fortinet FortiGate: Virus detected	Generated when a potential malicious file is detected.

Name	Description
Fortinet FortiGate: User login activities	Generated when the successful login activity is detected.
Fortinet FortiGate: User added or deleted	Generated when new user added or existing one deleted like activities detected.

4.2 Reports

Name	Description
Fortinet FortiGate - SSL VPN user authentication events	Provides detailed information of SSL VPN user authentication events triggered on FortiGate device.
Fortinet FortiGate - User authentication events	Provides the information of authentication related events trigger on FortiGate device.
Fortinet FortiGate - Anomaly or IPS attack detected	Captures all the anomaly or IPS attack related events triggered on FortiGate device.
Fortinet FortiGate - Suspicious web content detected	Capture suspicious web related traffic triggered on FortiGate device.
Fortinet FortiGate - Suspicious email content detected	Fetches details on traffic related to the email communication triggered on FortiGate device.
Fortinet FortiGate - Data leak detected	Captures DLP events detected on FortiGate device.
Fortinet FortiGate - Traffic events	Fetches traffic events triggered on FortiGate device.
Fortinet FortiGate - Application control events	Capture details for intrusion attempts while matching the application pattern triggers on FortiGate device.
Fortinet FortiGate - Web application firewall events	Fetches information related to the web application firewall events.
Fortinet FortiGate - Virus detected	Captures events categorized as virus or malicious by FortiGate device.
Fortinet FortiGate - Administrator authentication events	Captures administrator authentication events triggered on respective FortiGate device.
Fortinet FortiGate - Firewall configuration change	Captures any configuration change related activity triggered on FortiGate device.

4.3 Dashboard

Name	Description
Fortinet FortiGate - Login and authentication success events.	Displays login and authentication success events triggered on respective FortiGate device.
Fortinet FortiGate - Login and authentication failed events.	Captures login and authentication failed events triggered on respective FortiGate devices.
Fortinet FortiGate - Intrusion detection by source IP	Displays Intrusion detection by source IP.
Fortinet FortiGate - Login failed by source Geo-location	Captures the geo location of source IP address who triggered login failed events on respective FortiGate device.
Fortinet FortiGate - Intrusion detection by log type	Detects the intrusion and display the message of respective threat type.
Fortinet FortiGate - Intrusion detection by source IP Geo-location	Displays source IP geo location where intrusion attack has been detected.
Fortinet FortiGate - Login or authentication events by source IP Geo-location	Displays the geo location of the source IP from where login or authenticate event have triggered.
Fortinet FortiGate - Traffic by source IP Geo-location	Displays the geo location of source IP from where traffic is originated.
Fortinet FortiGate - Login and authentication success events.	Displays the login and authentication success events triggered on respective FortiGate device.

4.4 Saved Search

Name	Description
Fortinet FortiGate - Admin login failures	Provides the information on Admin login failures activities which includes information like IP address, location, console type used by user.
Fortinet FortiGate - Allowed traffic	Provides information of the allowed traffic with related information like source and destination IP address and location.
Fortinet FortiGate - Application control	Provides information of the application control events.
Fortinet FortiGate - Data leak detected	Provides information on DLP events detected by FortiGate device.
Fortinet FortiGate - Denied traffic	Provides information of the denied traffic with related information like source and destination IP address, location and reason for the violation or denied.

Name	Description
Fortinet FortiGate - IPS attacks detected	Provides information on anomalies or IPS events detected by FortiGate device.
Fortinet FortiGate - SSL VPN user login failure	Provides the information on users who are failed to login through SSL VPN which includes information like IP address, location, etc.
Fortinet FortiGate - Suspicious email content detected	Provides information on suspicious email content detected on the Email category which included sender's and receiver's address, any attachments in the mail, etc.
Fortinet FortiGate - Suspicious web content detected	Provides information on suspicious web content detected by FortiGate device.
Fortinet FortiGate - User authentication failures	Provides the information on user login failures activities which includes information like IP address, location etc.
Fortinet FortiGate - User authentication success	Provides the information on user who can trigger successful authentication event which includes information like IP address, location, console type used by user.
Fortinet FortiGate - Virus detected	Provides information on events where any suspicious or malicious file detected by FortiGate device.
Fortinet FortiGate - VPN user tunnel status	Provides information on events whenever FortiGate detect the change of VPN tunnel status by respective user.
Fortinet FortiGate - Web application firewall activities	Provides information on web application firewall events detected by FortiGate device.
Fortinet FortiGate - Admin login and logout	Provides detailed information on admin login and logout activities which includes IP address, console type information.
Fortinet FortiGate - Configuration changes	Provides information on the firewall configuration changes detected on respective FortiGate device.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC 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 & Response (MXDR). 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@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support