



How-To Guide

Integrate Check Point NGFW with Netsurion Open XDR

Publication Date

August 25, 2023

Abstract

This guide provides instructions to configure and integrate Check Point NGFW 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 Check Point NGFW and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Check Point NGFW in Netsurion Open XDR.

Table of Contents

1	Overview	4
2	Prerequisites	4
3	Integrating Check Point NGFW with Netsurion Open XDR	4
3.1	Forwarding Syslog Data to Netsurion Open XDR	4
3.1.1	Enabling Syslog Reporting on Check Point Firewall Gaia Portal	4
3.1.2	Enabling Syslog Reporting on Check Point Firewall R80.10 Gaia CLISH	5
4	Data Source Integration (DSI) in Netsurion Open XDR	6
4.1	Alerts	6
4.2	Reports	7
4.3	Dashboards	8
4.4	Saved Searches	8

1 Overview

Check Point is a cyber security architecture which offers security, easy deployment, and effective management by consolidating key security applications (Firewall, VPN, Intrusion Prevention, Antivirus and more).

Netsurion Open XDR manages logs retrieved from Check Point. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Check Point.

2 Prerequisites

- Admin access to Check Point Smart Console.
- Check Point Firewall version R80.10 and later.
- Port 514 must be set to allow in the firewall.
- The Data Source Integration package.

Note

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

3 Integrating Check Point NGFW with Netsurion Open XDR

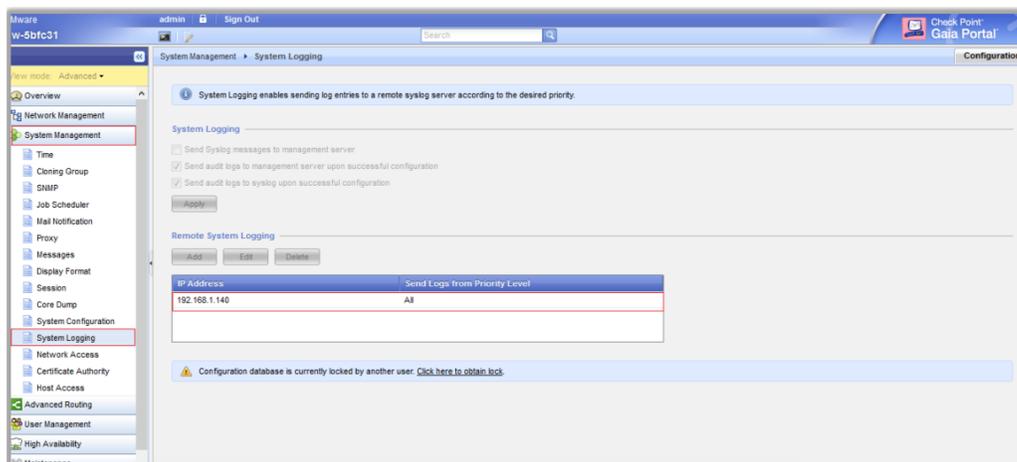
To configure syslog for Check Point R80.10, you can follow any one type of configuration method.

- Configuring via Gaia Portal.
- Configuring via Gaia CLISH.

3.1 Forwarding Syslog Data to Netsurion Open XDR

3.1.1 Enabling Syslog Reporting on Check Point Firewall Gaia Portal

1. In the Main menu, from the left panel, go to **System Management > System Logging**.



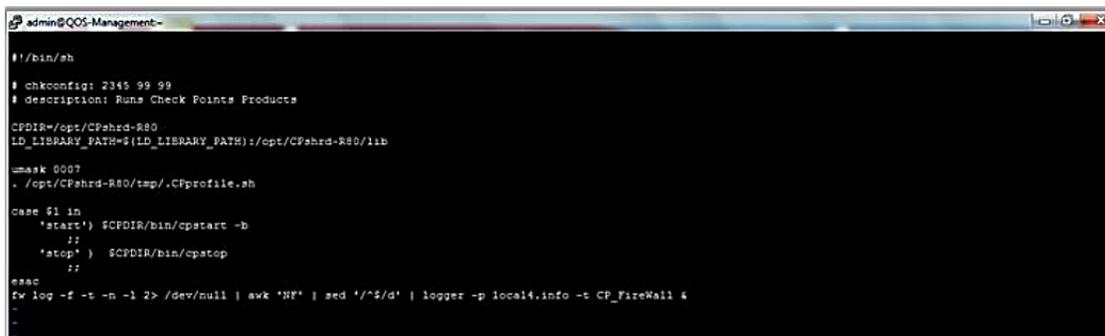
2. In the **System Logging** interface, click **Add** and specify the following details.
 - **IP Address:** Specify Netsurion Open XDR IP address or FQDN. (Recommended to specify FQDN).
 - **Port:** Specify the syslog server port number 514.
3. After providing the details, click **Apply** to forward the logs to Netsurion Open XDR

3.1.2 Enabling Syslog Reporting on Check Point Firewall R80.10 Gaia CLISH

The following configuration runs on Check Point Firewall system.

1. Log in to Check Point Firewall R80.10 server console.
2. Enable then expert mode by using **expert** command.
3. Add the specified lines in the **/etc/rc.d/init.d/cpboot** file.

```
fw log -f -t -n -l 2> /dev/null | awk 'NF' | sed '/^$/d' | logger -p local4.info -t CP_FireWall &
```



```
admin@QOS-Management-
#!/bin/sh
# chkconfig: 2345 99 99
# description: Runs Check Points Products

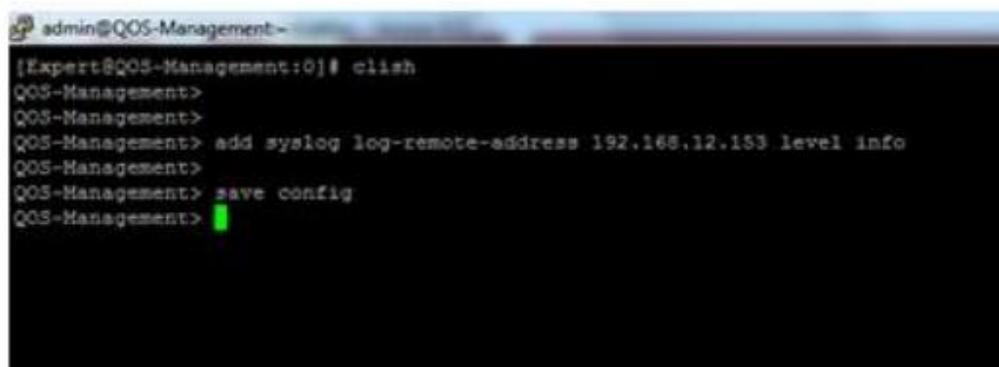
CPDIR=/opt/CPshrd-R80
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CPshrd-R80/lib

#mask 0007
# /opt/CPshrd-R80/tmp/.CPprofile.sh

case $1 in
  'start') $CPDIR/bin/cpstart -b
           ;;
  'stop' ) $CPDIR/bin/cpatop
           ;;
  *)
  esac
fw log -f -t -n -l 2> /dev/null | awk 'NF' | sed '/^$/d' | logger -p local4.info -t CP_FireWall &
```

4. Exit from the expert mode and configure syslog using the following command.

```
> add syslog log-remote-address level info
```



```
admin@QOS-Management-
[Expert@QOS-Management:0]# clish
QOS-Management>
QOS-Management>
QOS-Management> add syslog log-remote-address 192.168.12.153 level info
QOS-Management>
QOS-Management> save config
QOS-Management>
```

5. After providing the specified details, save the configuration details.

4 Data Source Integration (DSI) in Netsurion Open XDR

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

The Data Source Integrations package contains the following files for Check Point.

- Categories_Check Point NGFW.iscat
- Alerts_Check Point NGFW.isalt
- Reports_Check Point NGFW.etcrx
- KO_Check Point NGFW.etko
- Dashboards_Check Point NGFW.etwd

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
Check Point NGFW: Attacks detected	Generated when an event associated with intrusion prevention is logged by Check Point.
Check Point NGFW: Configuration changes detected	Generated when a user performs configuration changes in Check Point.
Check Point NGFW: DLP event has been detected	Generated when an event associated with data Loss and prevention is logged by Check Point.
Check Point NGFW: Failed login attempt detected	Generated when an endpoint user or machine had a failed login attempt.

4.2 Reports

Name	Description
Check Point NGFW - System attack detections	Provides information about system attack detections.
Check Point NGFW - URL filtering activities	<p>Provides information about the summary of events that are related to URL filtering that controls access to millions of web sites by category, users, groups, and machines to protect users from malicious sites.</p> <p>It includes, URL accessed, endpoint IP, user agent, log datetime, and more.</p>
Check Point NGFW - Application control activities	Provides information about Application control activities.
Check Point NGFW - HTTPS inspection activities	<p>Provides information about the summary of events related to traffic that are encrypted by HTTPS.</p> <p>It includes, URL, endpoint IP address, source port, action type, application category, and more.</p>
Check Point NGFW - DLP activities	<p>Provides information about summary of data loss and prevention events.</p> <p>It includes, action type, sender address, recipient address, email subject, scanning direction, and more.</p>
Check Point NGFW - Anti malware events	<p>Provides information about the summary of events that are associated with anti-malware activities, that is, events where viruses, spyware, keystroke loggers, trojans and rootkits are identified using signatures, behavior blockers and heuristic analysis.</p> <p>It includes, endpoint username, anti-virus name, event type, OS name or version, scan status, and more.</p>
Check Point NGFW - Denied traffic activities	<p>Provides information about the summary of denied traffic in Check Point firewall.</p> <p>It includes, source IP address, destination address, action type, service Id, and more.</p>
Check Point NGFW - User login and logout activities	<p>Provides information about the summary of endpoint user's or machine's failed login activity.</p> <p>It includes, username, source IP address, authentication type, Identity type, log datetime, and more.</p>
Check Point NGFW - VPN login and logout activities	<p>Provides information about the summary of VPN or SSLVPN login and logout activities.</p> <p>It includes endpoint IP address, login option, and failure reason.</p>

Name	Description
Check Point NGFW - All VPN activities	Provides information about all VPN activities
Check Point NGFW - Allowed traffic activities	Provides information about allowed traffic in Check Point firewall. It includes, source IP address, destination address, action type, service Id, and more.

4.3 Dashboards

Name	Description
Check Point NGFW - Events by attack detection score	Displays all the events by attack detection score captured by Check Point NGFW.
Check Point NGFW - VPN log in by source IP address	Displays all the VPN login by source IP address.
Check Point NGFW - Login activities object type	Displays all the login activities object type captured by Check Point NGFW.
Check Point NGFW - Login fails	Displays all the Login fails captured by Check Point NGFW.
Check Point NGFW - Event log types	Displays all the log types captured by Check Point NGFW.
Check Point NGFW - Event by action performed	Displays all the event by action performed by Check Point NGFW.
Check Point NGFW - Traffic denied	Displays all the denied traffic captured by Check Point NGFW.
Check Point NGFW - Events traffic allowed	Displays all the events traffic allowed by Check Point NGFW.

4.4 Saved Searches

Name	Description
Check Point NGFW - Attacks detected	Provides information about system attack detections.
Check Point NGFW - URL filtering	Provides information about the summary of events related to URL filtering that controls access to millions of web sites by category, users, groups, and machines to protect users from malicious sites. It includes, URL accessed, endpoint IP, user agent, log datetime, and more.

Name	Description
Check Point NGFW - Application control	Provides information about Application control activities.
Check Point NGFW - HTTPS inspection	<p>Provides information about the summary of events related to traffic that are encrypted by HTTPS.</p> <p>It includes, URL, endpoint IP address, source port, action type, application category, and more.</p>
Check Point NGFW - DLP events	<p>Provides information about summary of data loss and prevention events.</p> <p>It includes, action type, sender address, recipient address, email subject, scanning direction, and more.</p>
Check Point NGFW - Anti malware events	<p>Provides information about the summary of events that are associated with anti-malware activities, events where viruses, spyware, keystroke loggers, trojans and rootkits are identified using signatures, behavior blockers and heuristic analysis.</p> <p>It includes, endpoint username, anti-virus name, event type, OS name/version, scan status, and more.</p>
Check Point NGFW - Configuration changes	Provides information about the configuration changes activities.
Check Point NGFW - Login and logout activities	<p>Provides information about the summary of endpoint user or machine failed login activity.</p> <p>It includes, username, source IP address, authentication type, Identity type, log datetime, and more.</p>
Check Point NGFW - VPN login and logout activities	<p>Provides information about the summary of VPN or SSLVPN login and logout activities.</p> <p>It includes, endpoint IP address, login option, failure reason, and more.</p>
Check Point NGFW - Login failed activities	Provides information about all the login failed activities.
Check Point NGFW - Allowed traffic	<p>Provides information about allowed traffic in Check Point firewall.</p> <p>It includes, source IP address, destination address, action type, service Id, and more.</p>
Check Point NGFW - Denied traffic	<p>Provides information about the summary of denied traffic in Check Point firewall.</p> <p>It includes, source IP address, destination address, action type, service Id, and more.</p>

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>