FortiNAC

Check Point
Device Integration

Version: 9.1, 9.2, 9.4

Date: December 14, 2023

Rev: A

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM
http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview 4
L3 (ARP) Information Collection 5
Syslog Management 6
How it Works 6
Requirements 6
Step 1: Configure Check Point 7
Step 2: Add Check Point as a Pingable Device in FortiNAC 8
Step 3: Create "Catch All" Security Rule 9
Step 4: Generate and Evaluate Security Events 11
Step 5: Configure Security Rule 12
Validate 12
Troubleshooting 13
Related KB Articles 13
Debugging 13
Appendix 14
Add or Modify a Security Rule Trigger 14
Security Event Severity Level Mappings 16

Overview

The information in this document provides guidance for configuring the Check Point firewall to be managed by FortiNAC. This document details the items that must be configured.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

What it Does

The following features operate independently of each other. Both can be configured, if desired.

L3 (ARP) Information Collection
The Check Point firewall can also be used to collect L3 (ARP) information for network visibility.

Syslog Management

When FortiNAC receives an incoming security syslog event from a Check Point firewall, FortiNAC generates a security event. That security event can trigger a security alarm allowing FortiNAC to take action on the associated host, such as disabling the host or marking it at risk. See Security incidents in the Administration Guide for more information.

Click on the desired feature to proceed:
L3 (ARP) Information Collection
Syslog Management

L3 (ARP) Information Collection

How it Works
FortiNAC collects IP address to MAC address information by reading the Checkpoint's ARP cache regularly. For details, see L3 polling in the Administration Guide.

Check Point Requirements

- SNMP community or account

Procedure

1. In the FortiNAC Administration UI, navigate to **Network > Inventory.**
2. Add the Checkpoint using the management interface IP address. See Add or modify a device in the Administration Guide for instructions. Include the following:

    - **SNMP Settings:** SNMP v1 or v3 credentials used for device discovery and ARP collection/L3 polling

    Related KB Articles:
    Options for Devices Unable to Be Modeled in Topology

3. Once added, enable L3 Polling. Right click on the model in the left panel and select **Group Membership**.
4. Check the box next to **L3 Polling (IP→MAC)** and click **OK.**
5. Click the **Polling** tab.
    a. Check the box next to **L3 (IP→MAC) Polling**.
    b. Click **Save**.

Once the Checkpoint is discovered, IP address information should populate the adapter records.

Syslog Management

How it Works

Automated response by FortiNAC to security events sent by the firewall is achieved through the following steps:

1. Firewall sends a security syslog event to FortiNAC.
2. FortiNAC parses the information based on pre-defined security event parsers stored in FortiNAC's database. See Security event parsers in the Administration Guide for more information.
3. FortiNAC generates a security event that can contain any or all of the fields included in the message.
4. FortiNAC attempts to identify the host that is the target of the event. This is done by resolving the source IP address in the message to a MAC address in FortiNAC's database through L3 Polling.
    a. If the IP address is not able to be resolved, the event is held in memory until an associated host can be found.
    b. Once an associated host is found, the event is printed and searchable under **Logs > Security Incidents > Events** of the Administration UI. See Security events in the Administration Guide for more information.
5. If the Security Event is mapped to a Security Alarm, FortiNAC takes action based on the alarm configuration. The actions taken can range from sending an email to isolating the offending host. See Security alarms in the Administration Guide for more information.

Requirements

- **FortiNAC**
    - Endpoint License level PRO

Step 1: Configure Check Point

Add FortiNAC as a Syslog server. Use the eth0 management IP address. Refer to the Check Point documentation to configure the Check Point Gateway to enable logging of the specific Events (e.g., Anti-Malware, New Anti-Virus, etc.).

Step 2: Add Check Point as a Pingable Device in FortiNAC

1. Navigate to **Network > Inventory**.
2. Right-click and select **Add a Pingable Device** to add the Check Point to FortiNAC. The Physical Address (MAC) is required when creating pingable devices if the IP to MAC cannot be resolved when the ARP tables are read.
3. Configure using the table below. For instructions, see Add or modify a pingable device in the Administration Guide.

Element Tab Field Definitions

Some fields listed display only when modifying an existing pingable device or when viewing the device properties.

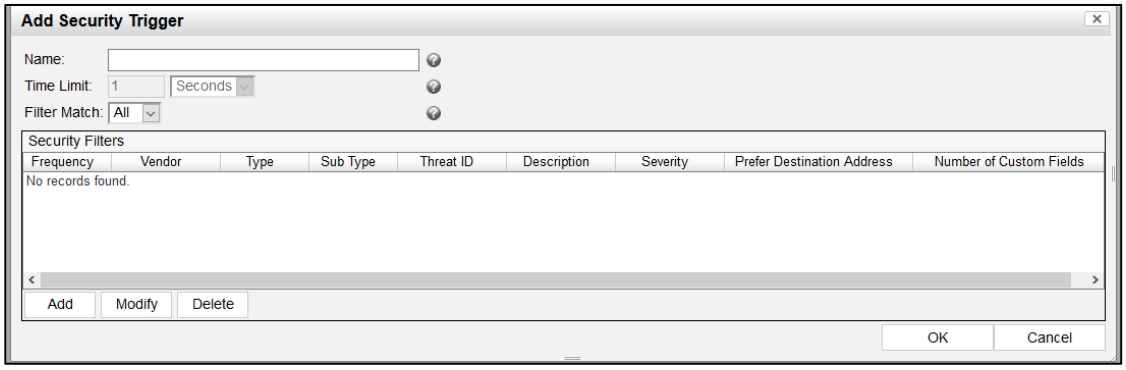
Container	Container in the Inventory tree where this device is stored.
Name	Name of the device. Enter Check Point.
IP Address	IP address of the Check Point.
Physical Address	The MAC address of the Check Point. Appears in the view only when the device is a pingable.
Device Type	Select **IPS/IDS**.
Incoming Events	Select **Security Events**, and then select **Check Point**.
SSO Agent	Select **Not Applicable**.
Role	The Role for this device. Available roles appear in the drop-down list.
Description	Description of the device entered by the Administrator.
Note	User specified notes about the device.
Contact Status Polling	Enable or disable contact status polling for the selected device.

Step 3: Create “Catch All” Security Rule

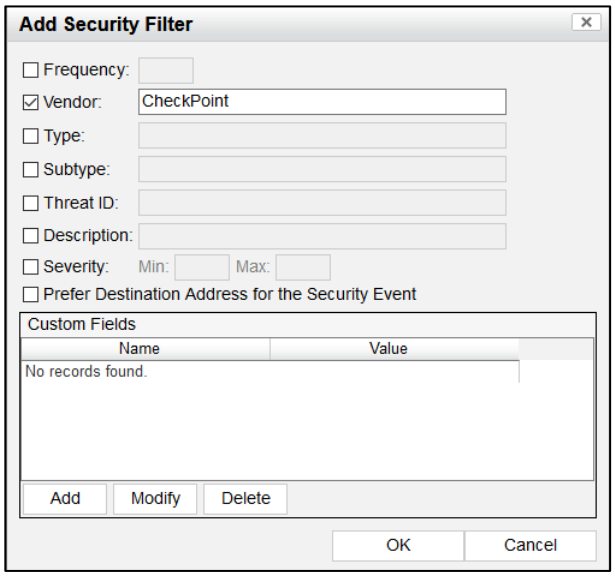
Create a "Catch All" security rule to enable logging of security events from a Check Point device. No security alarms are generated. Used to view all events that are being sent to FortiNAC.

Create “Catch All” Security Rule Trigger

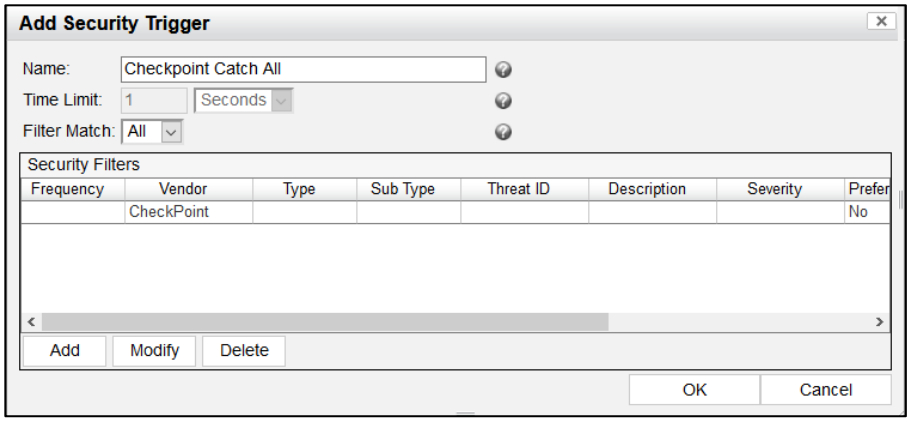
1. Select **Logs > Security Incidents**.
2. Select **Triggers**.
3. Click **Add** or select an existing trigger and click **Modify**.
4. Click in the **Name** field and enter a name for this security trigger (such as “Checkpoint Catch All”).



5. Under Security Filters, click the **Add** button
6. For the “Catch All” trigger, add a filter with **Vendor:** CheckPoint.



7. Click **OK** to save filter.



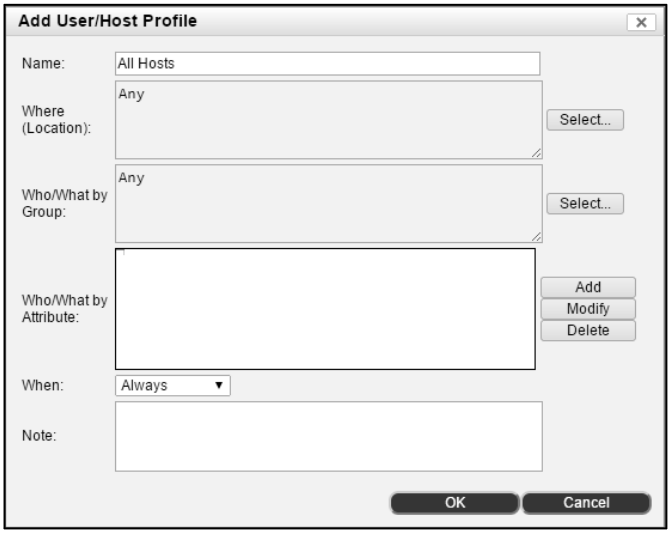
8. Click **OK** to save Trigger.

For more details on these views, see Add a trigger and Add or modify filters in the Administration Guide.

Add "All Hosts" User/Host Profile

Create a profile to apply to all hosts.

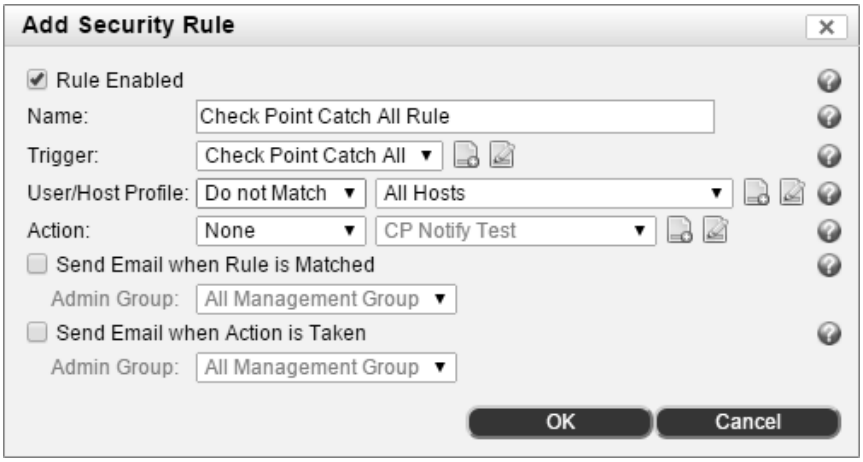
1. Select **Policy & Objects > User/Host Profiles.**
2. Click the **Add** button.
3. Click in the Name field and enter **All Hosts**.
4. Leave all other fields at default. Click **OK** to continue.



Create "Catch All" Security Rule

Create a "Catch All" Security Rule and associate the "Catch All" trigger.

1. Select **Logs > Security Incidents.**
2. Select **Rules**.
3. Click **Add.**



4. Click in the **Name** field and enter a name for this security rule.
5. Select the "Catch All" trigger from the drop down menu.
6. Select **Does Not Match** and **All Hosts** from the User/Host Profile drop-down lists. This enables Security Event Triggers but disables Security Alarms.
7. Click **OK** to save.

Step 4: Generate and Evaluate Security Events

1. Create conditions that generate events from the Check Point so they can be evaluated.
2. Under **Logs > Security Incidents**, select **Events**.
3. Review the security events received. Use these security events as a starting point to filter on specific fields in order to create the appropriate security filters for security event triggers.

   An event rule can be created from this view based upon a received event. For details on this view, see Security events in the Administration Guide.

Step 5: Configure Security Rule

Create security alarms for these security events. Once alarms are created, admin and/or users can be notified, and take the primary action, secondary action, etc.

1. Define a security trigger that consists of one or many security filters and optional time limit/frequency. See Add a Trigger.
2. Define a security action that consists of one or many activities to be executed once a trigger is satisfied. Each activity consists of a primary task and an optional secondary task that can be executed after a period of time. See Add or modify an action.
3. Add the security rule.
    a. Select the security trigger created in the previous step.
    b. Define hosts to which the security rule applies (see User/host profiles in the Administration Guide).
    c. Select the security action created in the previous step.
    d. Notify administrators/users.

For details, see Add or modify a rule in the Administration Guide.

Validate

1. Connect a host to the network.
2. Reproduce a condition on the host to trigger the firewall to send a security event.
3. Verify the event is generated in FortiNAC by navigating to **Logs > Security Incidents > Events** and clicking the **Update** button.
4. If alarm is also configured, verify the alarm was generated by clicking **Alarms** and clicking the **Update** button.
5. If an action was configured, verify the action executed.

If any of the above do not work as expected, refer to the Troubleshooting section of this document.

Troubleshooting

Related KB Articles

Refer to the applicable KB article(s):
Troubleshooting SNMP Communication Issues
Troubleshooting Poll Failures
Wired hosts displaying incorrect status
Online wireless hosts displaying offline status
Rogue Wireless Clients Cannot Connect to SSID
Troubleshooting RADIUS clients not connecting
Troubleshooting Wireless Clients Moved to the Wrong VLAN
Packets not processed when source IP address does not match Device Model
Troubleshooting security events

Debugging

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

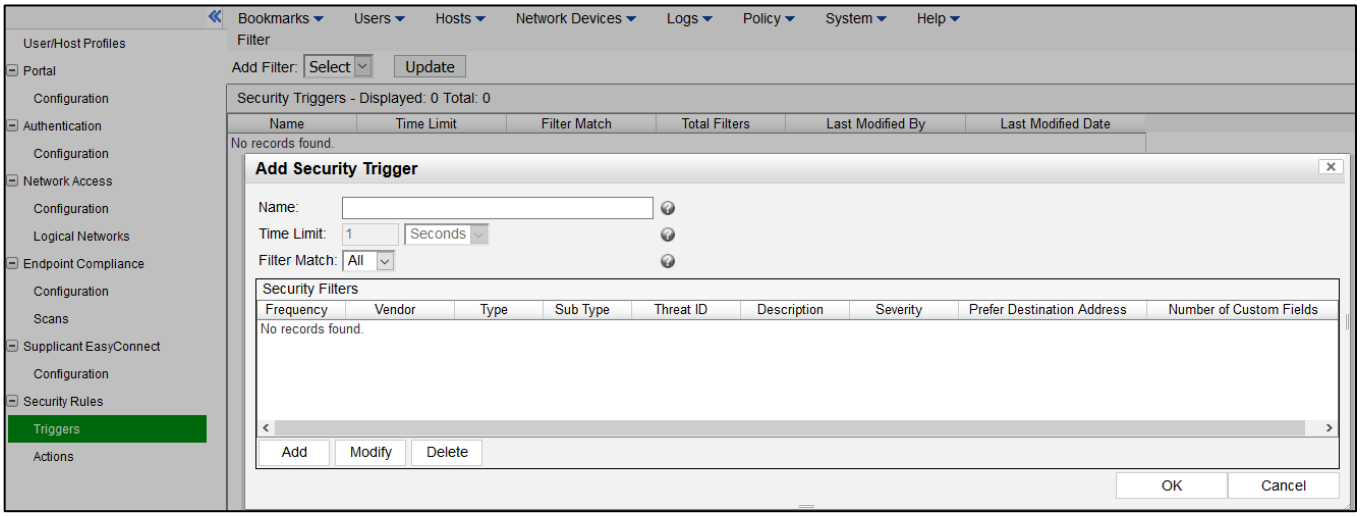
Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
Syslog activity	`nacdebug -name SyslogServer true`	/bsc/logs/output.master
Security Event syslog parsing	`nacdebug -name SecurityEventManager true`	/bsc/logs/output.master
SNMP activity	`nacdebug -name SnmpV1 true`	/bsc/logs/output.master
Disable debug	`nacdebug -name <debug name> false`	N/A

Appendix

Add or Modify a Security Rule Trigger

1. Select **Policy > Policy Configuration**.
2. In the menu on the left expand **Security Rules**.
3. Click **Triggers**.
4. Click **Add** or select an existing trigger and click **Modify**.
5. Click in the **Name** field and enter a name for this security trigger.

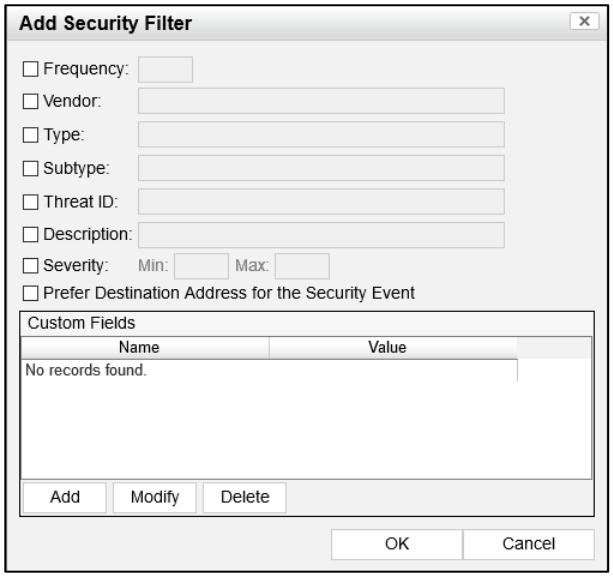


6. Use the table of field definitions below to enter the security trigger information.

Add Security Rule Trigger - Field Definitions

Name	A name for this security trigger.
Time Limit	The amount of time within which the incoming events must occur before satisfying the trigger.
Filter Match	Select whether any size subset of the security filters must be matched in order to satisfy the trigger.
Frequency	The number of times the security event must occur from the vendor in order to satisfy the trigger.
Vendor	The name of the vendor that is sending the security event.
Type	Specifies the type of security event.
Sub Type	Specifies the subtype of security event.
Threat ID	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Description	A textual description supplied by the security appliance of the event.
Severity	The range within which the threat level must be defined in order to satisfy the trigger. See Security Event Severity Level Mappings.
Number of Custom Fields	The number of custom fields that were added to the filter.
Add button	Click to add a filter.
Modify button	Click to modify a selected filter.
Delete button	Click to delete a selected filter.
Not currently in use/In use by	Indicates whether the action is in use, and the number of rules currently associated with the action.

7. To create a Security Filter for the Security Trigger, under **Security Filters**, click the **Add** button.



8. Use the table of field definitions below to enter the Security Filter information. Click **OK** to save.

Security Filters – Field Definitions

Frequency	The number of times the security event must occur from the vendor in order to satisfy the trigger.
Vendor	The name of the vendor that is sending the security event. Select **Check Point**.
Type	Specifies the type of security event.
Sub Type	Specifies the subtype of security event.
Threat ID	The code generated by the vendor for the security event threat level.
Description	Additional details about the security event.
Severity Range	The range within which the threat level must be defined in order to satisfy the trigger.
Custom Fields	The custom fields that were added to the filter. Click **Add** to add a custom field. Click **Modify** to modify a selected field. Click **Delete** to delete a selected field.

Add a Custom Field

Security Event Severity Level Mappings

Each vendor defines its own severity levels for syslog messages. These severity levels are normalized within FortiNAC to provide additional filtering options for incoming security events. The following table provides severity level mappings between the vendor and FortiNAC.

Check Point Vendor Severity Level	FortiNAC Severity Level
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10