FortiNAC - FortiDeceptor Integration Guide

Version 7.2 F

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

December 7, 2023
FortiNAC 7.2 F FortiDeceptor Integration Guide
49-922-769106-20211216

TABLE OF CONTENTS

Overview

This document provides guidance on integrating FortiDeceptor with FortiNAC.

What it Does

FortiDeceptor is based on deception technology that complements an organization's existing breach protection strategy designed to deceive, expose, and eliminate attacks originating from either external or internal sources before any real damage occurs.

FortiNAC is the Fortinet network access control solution. It enhances the overall Fortinet Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events.

FortiDeceptor from V.3.2 provides the capability to integrate with third-party security tools using the GEN WEBHOOK as part of the "integrated devices" feature for alert mitigation.

The integration between FortiDeceptor and FortiNAC allows us to automatically isolate any infected device from the network based on FortiDeceptor alert detection.

One of the compelling use cases for this integration is Ransomware mitigation using SMB Deception Token by luring the ransomware to encrypt fake files and raise alerts. Fortideceptor will use FortiNAC to isolated the infected endpoint from the network automatically and save the network damage.

Requirements

FortiNAC

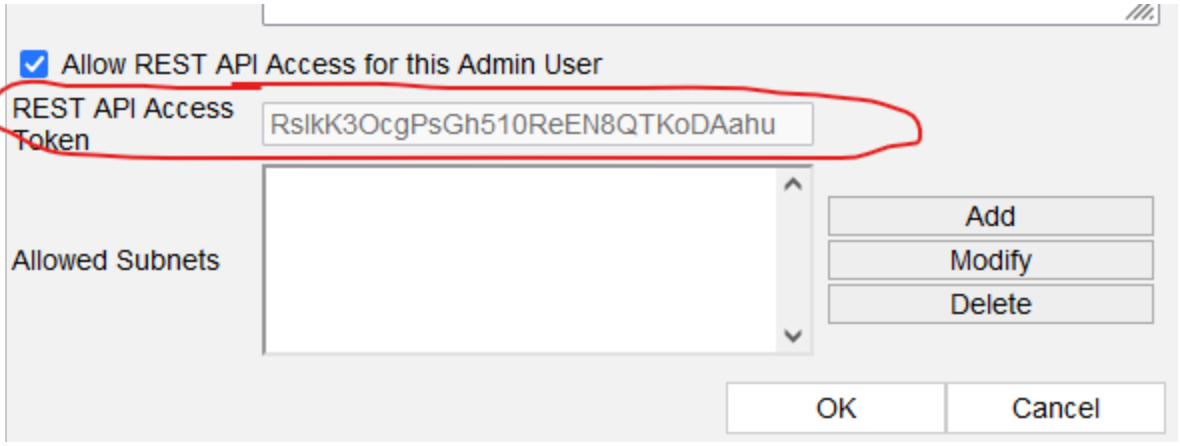
Minimum software version: 8.8 and greater

FortiDeceptor

Supported firmware version: v3.2 and greater

Step 1: Generate the Authorization Token in FortiNAC

1. Log in to the FortiNAC Administration UI.
2. Navigate to **Users & Hosts > Hosts.**
3. Create a new Admin User with REST API access and copy the Authorization token. For instructions see Add an Administrator in the Administration Guide.



Step 2: Configure the GEN-WEBHOOK in FortiDeceptor

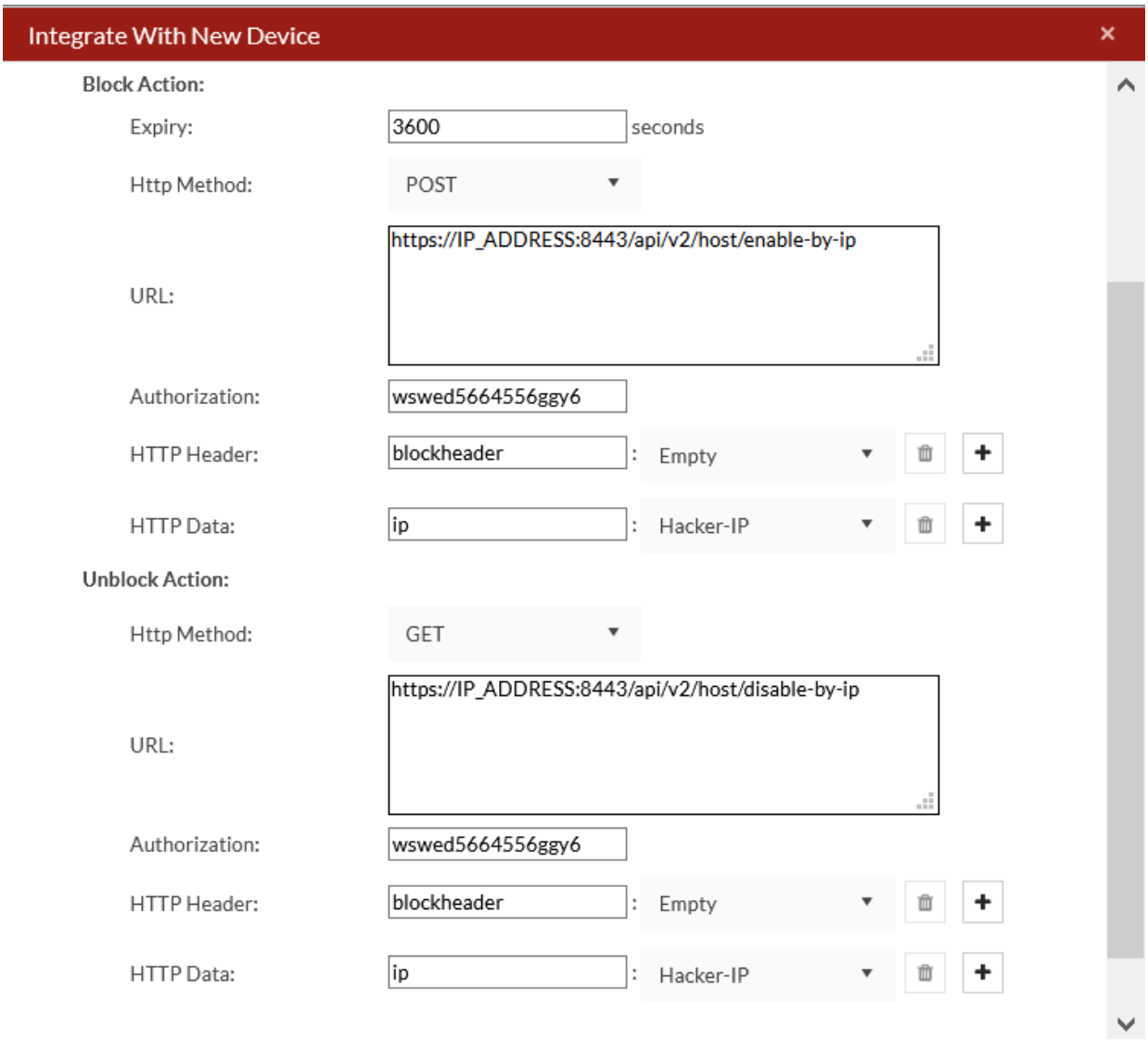
1. Access the FortiDeceptor Admin console. (https://IP_ADDRESS)
2. Click on **Fabric-> Integration Devices** to configure the gen-webhook.
3. Click on “+integrate with new device”.
4. Configure the WEBHOOK parameters for FortiNAC using the table below.

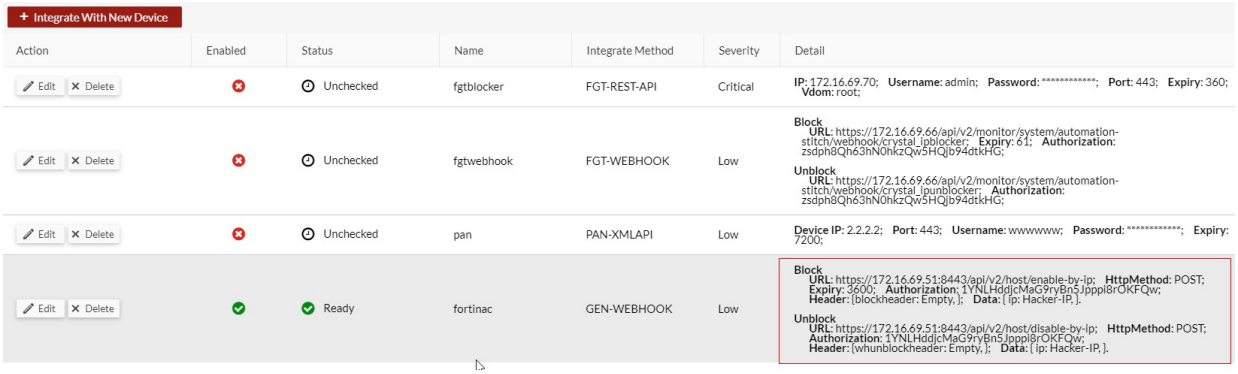
Block Action

Expiry	3600
Http Method	POST
URL	'https://IP_ADDRESS:8443/api/v2/host/enable-by-ip
Authorization	<Insert the Authorization token here>
HTTP Header	blockheader :: Empty
HTTP Data	ip :: Hacker-IP

Unblock Action

Expiry	3600
Http Method	POST
URL	'https://IP_ADDRESS:8443/api/v2/host/disable-by-ip
Authorization	<Insert the Authorization token here>
HTTP Header	blockheader :: Empty
HTTP Data	ip :: Hacker-IP


Integrate With New Device
Block Action:
Expiry:
3600
seconds
Http Method:
POST
URL:
https://IP_ADDRESS:8443/api/v2/host/enable-by-ip
Authorization:
wswed5664556ggy6
HTTP Header:
blockheader
Empty
HTTP Data:
ip
Hacker-IP
Unblock Action:
Http Method:
GET
URL:
https://IP_ADDRESS:8443/api/v2/host/disable-by-ip
Authorization:
wswed5664556ggy6
HTTP Header:
blockheader
Empty
HTTP Data:
ip
Hacker-IP


+ Integrate With New Device
Action
Enabled
Status
Name
Integrate Method
Severity
Detail
Edit
Delete
Unchecked
fgtblocker
FGT-REST-API
Critical
IP: 172.16.69.70; Username: admin; Password: **********; Port: 443; Expiry: 360; Vdom: root;
Unchecked
fgtwebhook
FGT-WEBHOOK
Low
Block
URL: https://172.16.69.66/api/v2/monitor/system/automation-stitch/webhook/crystal_ipblocker; Expiry: 61; Authorization: zsdph8Qh63hN0hkzQw5HQjb94dtkHG;
Unblock
URL: https://172.16.69.66/api/v2/monitor/system/automation-stitch/webhook/crystal_ipunblocker; Authorization: zsdph8Qh63hN0hkzQw5HQjb94dtkHG;
Unchecked
pan
PAN-XMLAPI
Low
Device IP: 2.2.2.2; Port: 443; Username: wwwwww; Password: **********; Expiry: 7200;
Ready
fortinac
GEN-WEBHOOK
Low
Block
URL: https://172.16.69.51:8443/api/v2/host/enable-by-ip; HttpMethod: POST; Expiry: 3600; Authorization: 1YNLHddjcMaG9ryBn5Jpppl8rOKFQw; Header: [blockheader: Empty,]; Data: [ip: Hacker-IP,].
Unblock
URL: https://172.16.69.51:8443/api/v2/host/disable-by-ip; HttpMethod: POST; Authorization: 1YNLHddjcMaG9ryBn5Jpppl8rOKFQw; Header: [whunblockheader: Empty,]; Data: [ip: Hacker-IP,].

Validate

FDC <-> FNAC - Attack Simulation

Use two network desktops: One for accessing the Fortideceptor & FortiNAC and the second for the attack simulation.

1. Access the FortiDeceptor Admin console. (https://IP_ADDRESS)
2. Click **Deception > Decoy & Lure Status** and identify a Decoy IP you are willing to attack (example: choose a windows decoy with SMB enabled).
3. Log in the FortiNAC Administration UI.
4. Navigate to **Users & Hosts > Hosts.**
5. Search for the “attacker endpoint” IP address and confirm it is connected to a port or SSID that is under enforcement.
6. Log into the “attacker endpoint” machine and access the windows Decoy IP network share to generate an alert.

   The “attacker endpoint” will get isolated from the network automatically by the FortiNAC.

In the FortiDeceptor Admin console, verify that Fortideceptor raised an alert under incident analysis. Navigate to Fabric > quarantine status to confirm that FortiDeceptor sent a quarantine command to FortiNAC.