



Check Point
SOFTWARE TECHNOLOGIES LTD.

18 November 2020

INFINITY NEXT

Security Solutions

Administration Guide

[Classification: Protected]



STEP UP TO
5TH GENERATION
CYBER SECURITY

Important Information



Latest Software

Infinity Next software components update automatically. We recommend that you always stay with the most recent software release to benefit from the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



Latest Version of this Document in English

Open the latest version of this [document in a Web browser](#).

Download the latest version of this [document in PDF format](#).

You can find the Important Updates and Release Notes in the Infinity Next Management Portal > **Support** > **Release Notes**.



Feedback

Check Point is engaged in a continuous effort to improve its documentation.

[Please help us by sending your comments.](#)

Revision History

Date	Description
27 October 2020	First release of this document

Table of Contents

Overview of Infinity Next	6
Introduction	6
In This Release	8
Infinity Next CloudGuard WAAP Practice	9
Deploying Infinity Next WAAP	10
Infinity Next Access Control	10
Management Overview	12
Navigating the Infinity Next Web UI	12
Managing the Portal Overview	13
Environment	13
Assets	13
Zones	16
Policy	16
Rules	16
Practices	17
Parameters	17
Triggers	17
Enforcement	17
Profiles	17
Agents	18
Operation	18
Support	19
Release Notes	19
Support	19
Downloads	19
Infinity Next Deployment and Configuration	20
Configuring Infinity Next Policy	20
Assets and Zones	20
Policy Configuration Practices	20
Triggers	20

Infinity Next Policy Rules	28
Deploying Nano-Agents	29
Agent Profile and Registration Tokens	29
Supported Deployments	30
Basic Nano-Agent Deployment	31
Deploying a Nano-Agent as a Container	31
CloudGuard Infinity Next Gateway	32
Deploying CloudGuard Infinity Next Gateway	33
Configuring the Dedicated Check Point Reverse Proxy	41
How to Manually Upload Certificates	45
Infinity Next Events	47
WAAP Management	50
Configuring WAAP Assets	50
Configuring WAAP Policy	52
WAAP Practices	53
Defining Practices	53
Web API Protection	54
Web Application Protection	55
WAAP Parameters	55
Schema Configuration	56
Overrides	56
Trusted Sources	57
Web Anti-Bot	58
Analyzing WAAP Events	60
Using the WAAP Dashboard	60
WAAP Best Practices	63
Initial Learning Period	63
Moving to Prevent Mode	63
Access Control	64
Supported environments	64
Access Control Management	64
Defining Practices	64
Incoming/Outgoing Access Control Practice	65

By Zone Access Control Practice	66
Zone configuration	66
Advanced Nano-Agent Configuration	70
Software Update Window	70
More Advanced Settings for Nano-Agents	71
Troubleshooting	72
CP-NANO Tool	72
Agent Uninstall	73
Support	75
Product Evaluation and Licensing	75

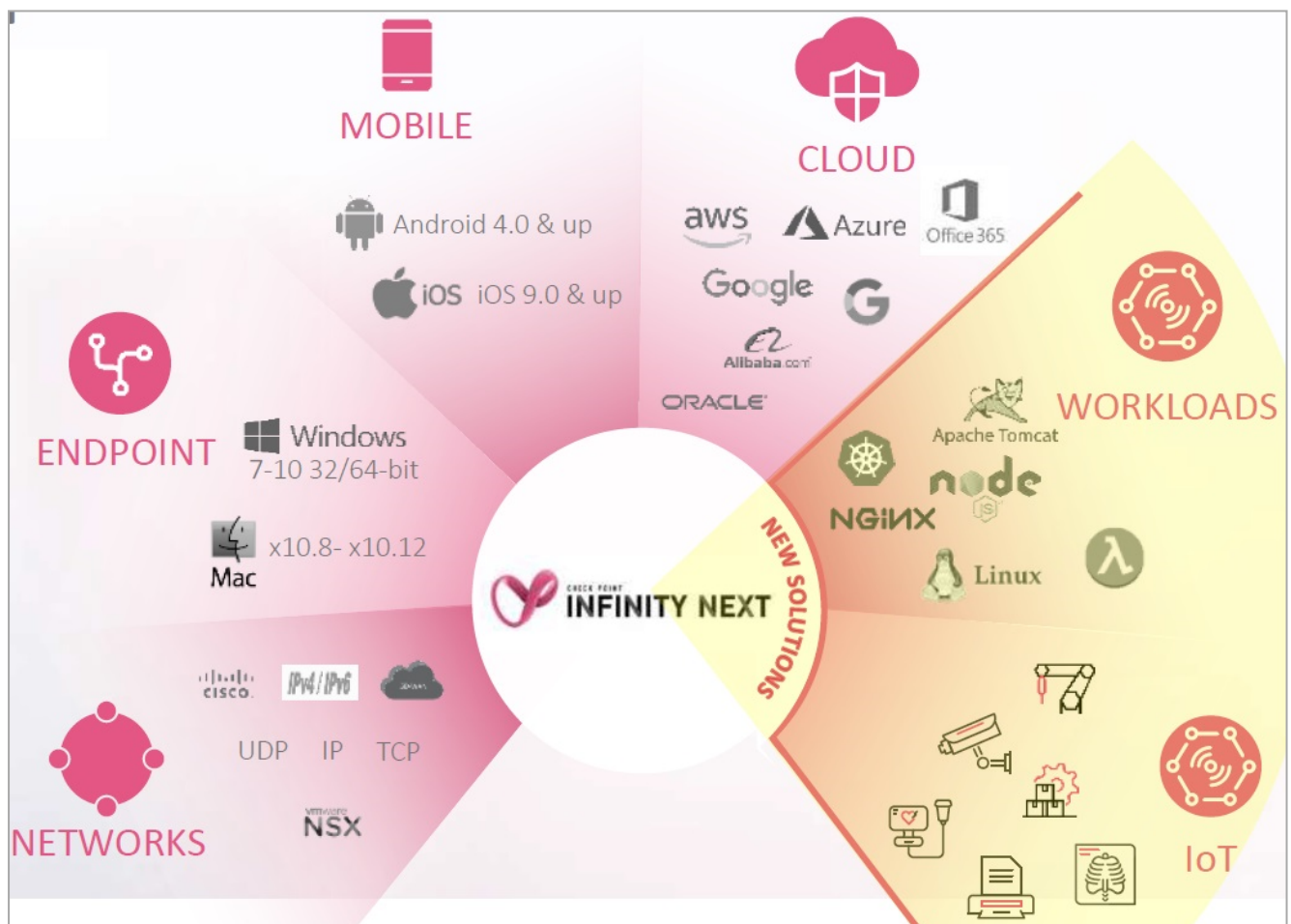
Overview of Infinity Next

Introduction

Infinity Next protects and controls access to and from assets.

- Infinity Next is a Check Point Gen VI security framework that protects modern digital blueprints. It adopts a straight forward approach that puts the digital Asset you want to protect in the center.
- Infinity Next can obtain inventory of assets and their attributes from various sources, and lets Security Teams and DevOps to apply applicable security practices:
 - Access Control
 - Threat Prevention
 - Web Application and API Protection
 - IoT Protection

Infinity Next covers more than fifty families of assets across Cloud, Network, Endpoint, Mobile, and IoT:



The Infinity Next Platform has three primary layers:

- Agents
- Fog
- Infinity Next Cloud and Management

Agents

Agents implement security monitoring and enforcement with either code developed by Check Point or by controlling native capabilities of the environment. In addition, Agents can include components of, or even fully developed by 3rd parties.

Examples:

- A Check Point software code that runs as an NGINX module and provides WAAP (Web Application and API Protection). This is called an "NGINX **Embedded** Nano-Agent".
- A Check Point Virtual Machine that runs in the Public or Private Cloud and provides multiple security practices. This is called an "Infinity Next Gateway **Dedicated** Agent".
- A Check Point software code that utilizes AWS or Azure APIs to provide Access Control by Public Cloud native means. This is called a "Public Cloud **Control** Agent".
- A Check Point software code that runs inside Nvidia SmartNIC to provide Access Control for servers. This is called a "SmartNic Embedded Nano-Agent".
- A Check Point Nano-Agent that runs as Kubernetes Ingress and provide Web API Protection and Threat Prevention. This is called a "Kubernetes Ingress **Embedded** Nano-Agent".
- A very small Check Point software code injected into Lambda function and provides Web Application Protection. This is called an "**Injected** Nano-Agent".
- A Nano-Agent that runs on a Smart Thermostat and provides Run Time IoT Workload Protection and Virtual Patching. This is called an "IoT **Embedded** Nano-Agent".

All types of Agents automatically update themselves. Manual updates are possible. But, as a best practice we do not recommend this method. Automatic updates make sure that the Agents have the latest security updates.

To deploy an Embedded Nano-Agent efficiently, it starts with a "Nano-Egg" - a very small piece of code, less than 100 KB. The Nano-Egg connects to its master. The Nano-Egg master provides only the necessary software components.

Note - The size of a basic Embedded Nano-Agent is less than 10 MB.

Fog

"Fog" is a term from the Edge Computing paradigm.

Fog is the master for all Agents.

By default, Agents connect to the Check Point Public Fog hosted in the Cloud, which is highly-available and secure.

The Check Point Fog provides multiple services to Agents:

- Software updates.
- Setting and Policy updates.

- Real-Time Asset and Security Intelligence.
- Cross-Agent Machine Learning Functions.
- Channel for Event Logs and Telemetry (Fog sends this data for storage to the Infinity Next Cloud).

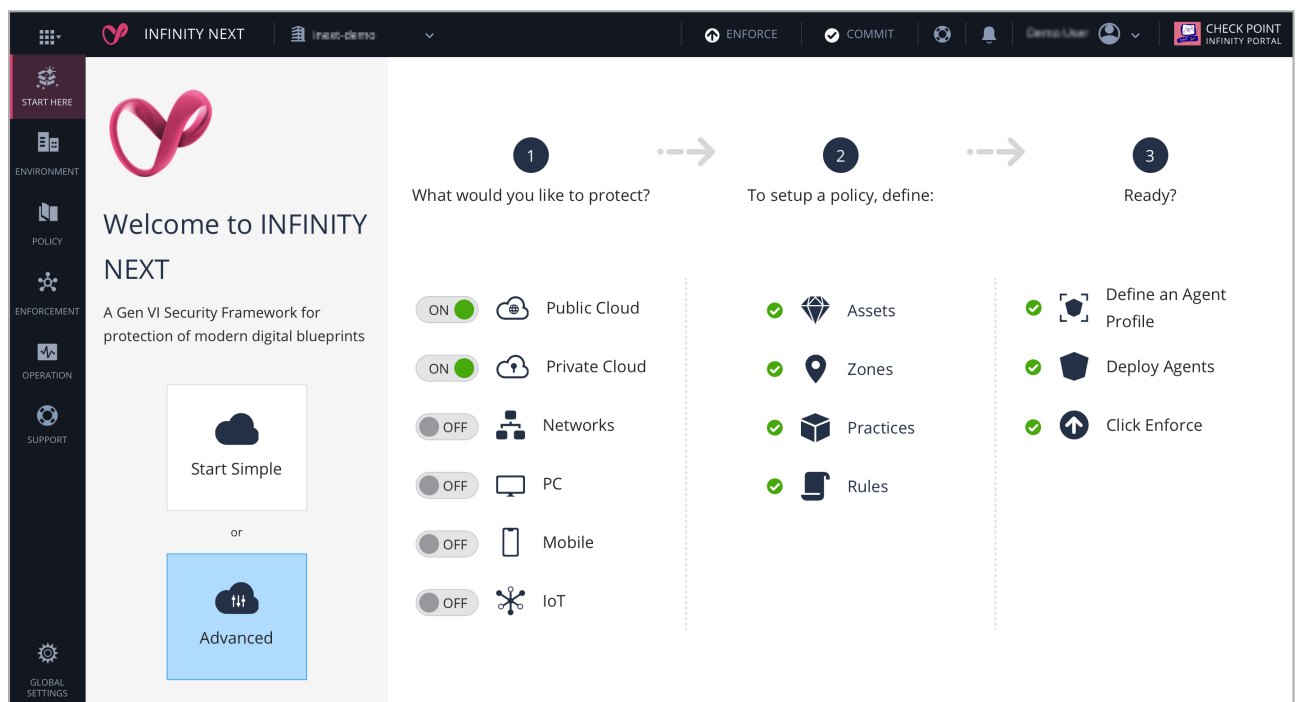
Note - By default, the Fog is transparent to users of Infinity Next technology.

Infinity Next Cloud and Management

Infinity Next Cloud is a highly-available and secure public service that hosts the Infinity Next Management Web Portal and RESTful API Server.

In addition, Infinity Next Fogs use Infinity Next.

Infinity Next is 100% API-ready for modern DevOps deployments. Infinity Next has a Web UI, which is asset-centric and shows the policies in human readable terms that are understood by different audiences (as in DevOps, Security, Auditors, and Executives).



In This Release

Available Security Practices:

1. WAAP (Web Application and API Protection).

- Prevention of attacks in Web Application and API requests.
- Validation of Web API conformance to the OpenAPI schema (Swagger).
- Protection against Web Bots.

The WAAP Security Practice uses Machine Learning. It requires almost zero configuration and has very high accuracy rate.

2. Access Control - Incoming and Outgoing access, and "Access by zone".

Layer 4 Access Control solution for Linux-based workloads - Public Cloud, Private Cloud, and IoT.

You can configure policies with rules, or with an intuitive graphical diagram.



Roadmap - Additional Security Practices are planned such as IPS, Virtual Patching, IOT Workload Protection, Access Control for Kubernetes, Public Cloud, and more.

Infinity Next CloudGuard WAAP Practice

The Infinity Next CloudGuard WAAP solution secures an organization's web applications.

WAAP analyzes web transactions with a set of Artificial Intelligence engines that operate in unison to protect against sophisticated attacks.

CloudGuard WAAP has three primary security components:

- Web Application Protection (WAF)
- API Security
- Anti-Bot Protection

Web Application Protection: OWASP Top 10 and Advanced Attacks

The first component of WAAP, the WAF, does a two-stage request analysis.

The first stage is very fast, where usually 95% of the requests are determined as non-suspicious. The suspicious requests go to a second stage, in which the requests undergo a deeper analysis that uses three patent-pending AI engines (User Reputation Scoring, Application Awareness Scoring, and Indicator Scoring).

This three-score combination, with the addition of pattern learning, leads to a very accurate decision that has these benefits:

1. Superior false-positive rate than traditional WAF (decisions are mainly based on matches to signatures).
2. Blocks different attack scenarios that are not blocked with a signature-only approach.
3. Reduction in administration time because it is not constantly necessary to tune the engine, create exceptions, disable signatures, and so on.

API Security: Validate Schema and Prevent Attacks

Frequently, software developers do not include verification of API input in their code.

The WAAP API security component provides two protection models - positive and negative. Administrators can enable one of them, or the two of them.

- The **positive model** delivers preemptive protection for possible API vulnerabilities through a schema validation procedure.

API schemas in OpenAPI ("Swagger") are uploaded to WAAP.

Incoming API requests are validated against these schemas to block all invalid API requests.

- The **negative model** uses the WAF and automatically detects and blocks malicious payloads in the API.

Anti-Bot Protection: Distinguish Humans from Bots

WAAP Anti-Bot protection component performs a three-step procedure:

1. Inject scripts into web application pages, such as login pages.
2. Collect data about input patterns and make the analysis of key stroke sequences, mouse moves, and finger touches.

Bots do not use such patterns. If a bot artificially creates such patterns, WAAP identifies them.

3. Make a decision if the input is entered by a human or by an automatic script (such as a bot), and block this activity.

Deploying Infinity Next WAAP

Infinity Next WAAP deployment options:

1. Infinity Next Gateway - a Virtual Machine that runs Check Point Gaia Operating System with a Reverse Proxy and Check Point Nano-Agent.

Available for:

- a. Amazon Web Services (AWS) - available in the AWS Marketplace.
 - b. Microsoft Azure - available in the Azure Marketplace.
 - c. Standalone Virtual Machine for VMware.
2. Infinity Next Container for Docker and Kubernetes environments.
 3. An Embedded Nano-Agent on top of any NGINX Web Server or NGINX Reverse Proxy.
 4. On the roadmap: An Embedded Nano-Agent on top of Apache, Envoy, and other Web Servers, API Servers, and Reverse Proxies.

Infinity Next Access Control

Access Control is the most basic Security Practice for any Asset.

With Access Control it is possible to refer to an Asset or group of Assets by any attribute that describes them, rather than by only traditional keys such as IP addresses, Ports, Protocol, Applications, and so on.










These practices are supported for Access Control:

■ Incoming/Outgoing Access Practice

Note - This practice is in the *Early Availability* stage.

Infinity Next Agents allow or block communication to and from a specific Asset or a dynamic group of Assets called **Zones**.

Example:

Incoming		
* New x Delete v ^		
#	Action	From
1	 Accept	 My clients 
2	 Drop	 Any Zone 
Outgoing		
* New x Delete v ^		
#	Action	To
1	 Accept	 Any Zone 

■ Zone-Based Access Practice

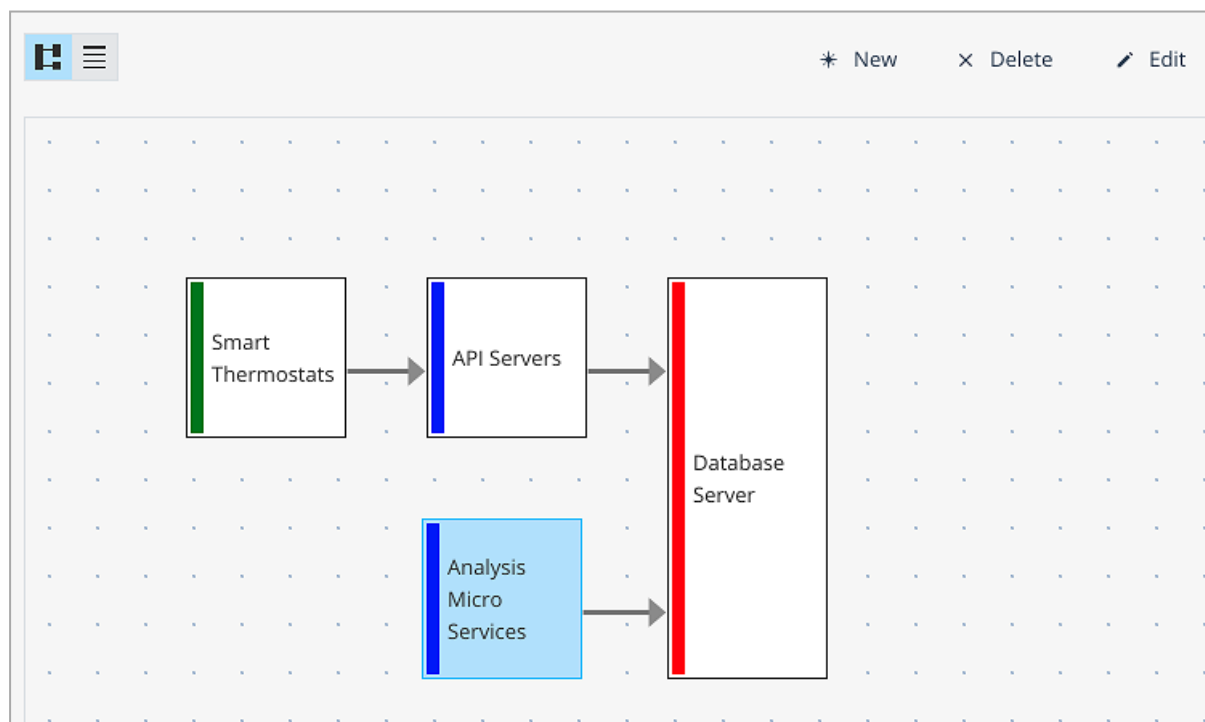
Note - This practice is in the Early Availability stage.

Infinity Next Agents allow or block communication to and from a specific Asset based on a definition of the access relationship called **Adjacency**.

This graphical interface is a simpler way to configure access than a large number of rules in a Rule Base.


This release supports Access Control with an Embedded Nano-Agent for Linux Servers (Private Cloud and Public Cloud) and IoT Devices.

Example:

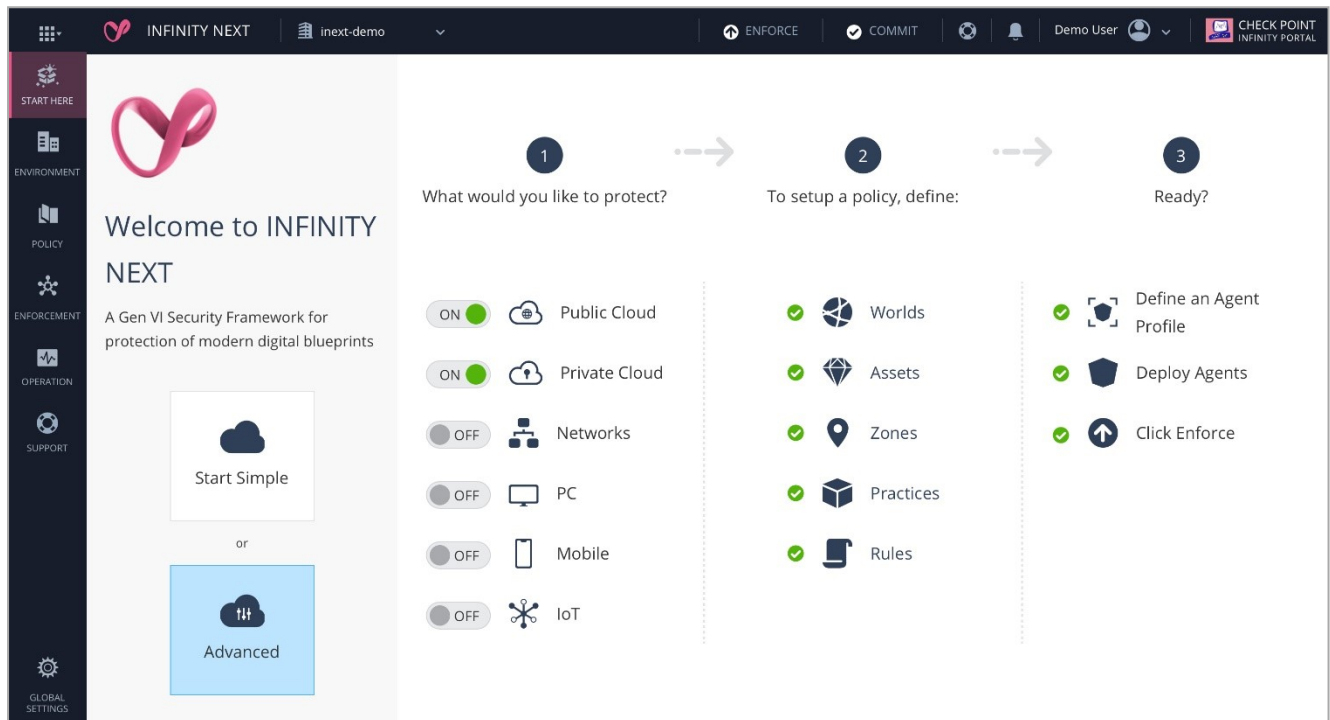


Management Overview

The Infinity Next Portal is accessed from Check Point's Portal. To gain access, create a new account or log

in to an existing account. To select the Infinity Next application, click the  icon at the top left part of the screen.

Navigating the Infinity Next Web UI



When you log in, the Start Here page open. You need to select one of these modes:

- **Start Simple** - For small environments and few security Practices.



Roadmap - This Mode will be available in a future release.


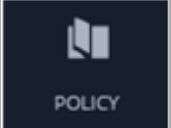

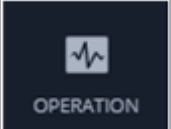
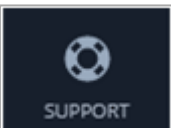
- **Advanced Mode** - Allow for a creation of advanced policies covering different classes of Asset and different Security Practices. In this release you can protect Web Applications and APIs, Linux Servers and IOT devices.



Roadmap - Additional types of assets will be added in a future release.

This table gives a brief overview of each button and its role. A more detailed description is in the related section of this guide.

Overview of Infinity Next Navigation Toolbar Options:

Navigation bar	Content
 ENVIRONMENT	<ul style="list-style-type: none"> ■ Assets ■ Zones
 POLICY	<ul style="list-style-type: none"> ■ Rules ■ Practices ■ Parameters ■ Triggers
 ENFORCEMENT	<ul style="list-style-type: none"> ■ Profile ■ Agents
 OPERATION	<ul style="list-style-type: none"> ■ Events ■ Access Control Dashboard ■ WAAP Dashboard
 SUPPORT	<ul style="list-style-type: none"> ■ Release Notes ■ Support ■ Downloads

Note - Infinity Next Web User Interface shows time according to your local web browser time zone.

Managing the Portal Overview


In this section, terms used to manage Infinity Next security capabilities.

Environment

Assets

Infinity Next refers to Assets by attributes that may be different according to the asset Class, Family and Type. For example, see the AWS VM. In Infinity Next, we can refer to it using any of its attributes:

DETAILS


Ingestion-1

Class	Workload	IP	172.30.21.4	Tags	Type: Tomcat Phase: Production
Family	AWS	Name	Ingestion-1	Location	us-west-2
First Known Time	2019-02-17T15:55:12.012	Public DNS Name	Ec2-4-21-us-west-2.compute.amazonaws.com		

Additional Information

Instance Type	a1.medium	Image	ami-05e1b2aec3b47890f	ID	i-08d061c47fac
Platform	linux	Function	VM	First Seen	2019-02-17T14:35:20Z
VPC	ae3ab311	Type	EC2		
Cloud Account ID	d4de5847-f3d0-40d3-943c-	Source	Dome9		

In Infinity Next the inventory of assets is obtained automatically from different sources. In the **Ingestion-1** example, it is obtained through Check Point's Dome9 connectors to the Public Cloud. Also, you can Assets through API or manually in the Web Management Portal.

For example:

EDIT ACME JUICE SHOP CUSTOMER PORTAL

×

General

Reverse proxy

Parameters

Name *

Acme Juice Shop Customer Portal

Comment

Add a comment...

Class *

Workload

Category *

Cloud

Family *

Web Application

Stage

Production

Application URLs *

e.g. <https://www.example.com/path>

+

<https://www.acme-juiceshop.com>

CANCEL

SAVE

Note - This release supports Assets of Family Web Application, Web API, and Generic TCP/UDP service.



Roadmap - More types of Assets are planned.

Zones

To make things scalable, we can dynamically group assets into Zones. For example, “Zone Ingestion” will include all the Assets that correspond to the following key/values:

Name *

Ingestion App Zone

Comment

Add a comment...

Query *

cloudVpc : vpc-0d892598ae9912af2

+

Adjacent Zones

+
Add Adjacent Zone

CANCEL SAVE

Note - For the supported key:value pairs used to define assets, see ["Zone configuration" on page 66](#).

Policy

Rules

Infinity Next Policy contains rules that describes which Practices must be applied to different Assets/Zones.

For example:

Name	Assets & Zones	Practices	Parameters	Triggers	Priority
Acme Power Web App	Acme Power Web...	Web Application Protection Best Practice (Thre... Web Attack Mitigation: Prevent Minimum Severity: High Bot Protection: Prevent	Example: WAAP ...	Log - Standard Web - Block Page	1
Smart Meters	SmartMeters	IoT Workload Protection Best Practice (Threat Prev...		Log - Standard	1

Note - Several rules can have the same Priority. The most restrictive action prevails (as in **Detect & Prevent -> Prevent**).

Practices

Practices defines the expected behavior for a set of security engines. In the **Rules** screenshot, we apply a **Web Application Practice** to a **Web Application Asset**.

Infinity Next comes with a set of Best Practices, or administrators can define their own.

Rules	* New x Delete Search...		
Practices			
Parameters			
Triggers			
	Name	Type	Sub-Type
	IoT Workload Protection Best Practice	Threat Prevention	IoT Workload
	Web API Protection Best Practice	Threat Prevention	Web API
	Web Application Protection Best Practice	Threat Prevention	Web Application
	Zone Oriented Access Control Best Practice	Access Control	Zone Oriented

Parameters

Parameters are often optional. They allow refinement of settings and creation of exceptions. They allow you to use the same Practice in two different rules, but for each rule a different particular setting.

Triggers

Triggers are operations that happen when there is a match on a rule. For example, send event log.

Enforcement

Profiles

Policy enforcement is done by Agents. To provision and manage groups of Agents with similar functions and settings use the default **Profile**, or define your own.

Profiles	* New x Delete Tokens... Manual Upgrade... Search...		
Agents			
R&D			
Object Explorer			
	Name	Type	Comments
	Default Agents Pro...	Agent	Up to 10 agents, usi...

GENERAL

SETTINGS

Name *

Comment

Agent Type *

Number of Agents *

Agent Authentication:
☒ Reusable Token
☐ Unique Token per agent

Agent Upgrade

Upgrade Mode

To get a token to associate your Agents with a profile, click **Token** (the Token is entered when the Agent is deployed).



Agents

Provides a view of all deployed agents, their details and status.

Profiles
Agents

Delete
Delete All
Refresh
Search...

Type	UID	Host	First Installed	Last Update	Last Known IP	Policy Version
Embedded	aa9ab928-64d1-4728-bf09-f81465e7565b	ubuntu-amd	10/2/2020, 5:59:05 PM	10/2/2020, 9:33:20 PM	77.248.1	3

GENERAL

Type
Embedded

Last Known IP
77.248.1

UID
aa9ab928-64d1-4728-bf09-f81465e7565b

Policy Version
3

Host
ubuntu-amd

Agent Tags
agent_version: 110044

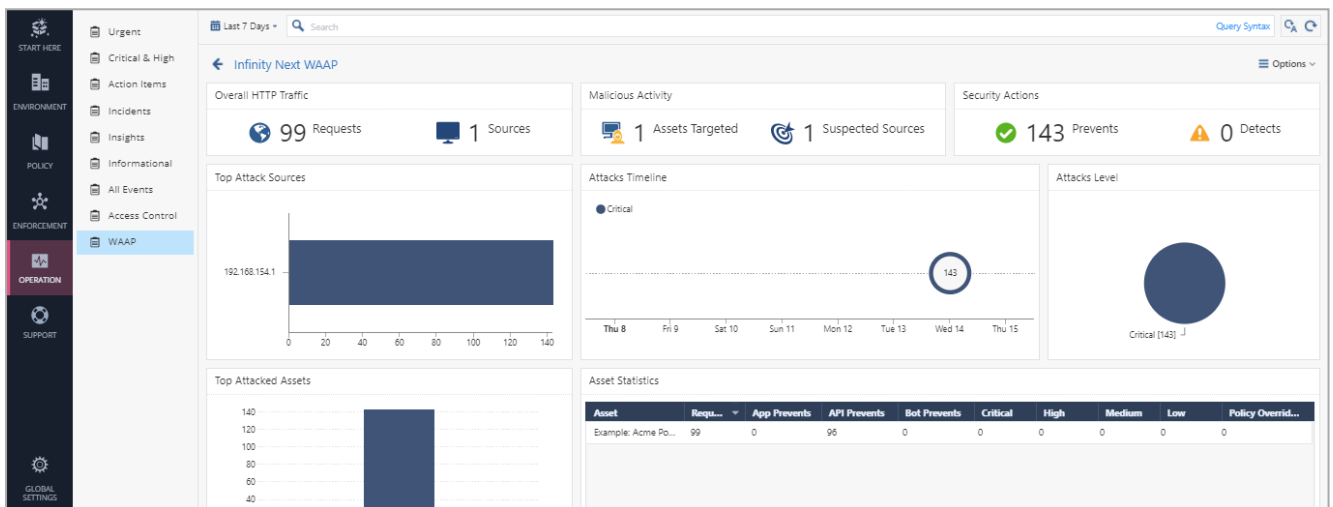
First Installed
10/2/2020, 5:59:05 PM

Last Update
10/2/2020, 9:33:20 PM

Operation

Provides log views and dashboard of events reported by the product.

START HERE	Urgent	Last 7 Days	Search	Query Syntax	Options
ENVIRONMENT	Critical & High	Time	Event Sever...	Asset Name	Security Act...
POLICY	Action Items	Oct 14, 2020 8:49:59 PM	Critical	Example: Acme Power SmartMeters API	Prevent
ENFORCEMENT	Incidents	Oct 14, 2020 8:49:57 PM	Critical	Example: Acme Power SmartMeters API	Prevent
OPERATION	Insights	Oct 14, 2020 8:49:55 PM	Critical	Example: Acme Power SmartMeters API	Prevent
SUPPORT	Informational	Oct 14, 2020 8:49:53 PM	Critical	Example: Acme Power SmartMeters API	Prevent
GLOBAL SETTINGS	All Events	Oct 14, 2020 8:49:50 PM	Critical	Example: Acme Power SmartMeters API	Prevent
	Access Control	Oct 14, 2020 8:49:48 PM	Critical	Example: Acme Power SmartMeters API	Prevent
	WAAP	Oct 14, 2020 8:49:46 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:44 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:42 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:40 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:38 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:35 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:33 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:31 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:29 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:27 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:25 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:23 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:21 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:18 PM	Critical	Example: Acme Power SmartMeters API	Prevent
		Oct 14, 2020 8:49:16 PM	Critical	Example: Acme Power SmartMeters API	Prevent



Support

Release Notes

Provides a location to view “What’s new” for the latest version, a list of known limitations and limits, and FAQ.

Support

Provides the necessary information to contact Check Point support.

Downloads

Provides a central page from which to download all Infinity Next essentials, mainly Agent installation, deployment, files, and links.

Infinity Next Deployment and Configuration

This section details how to configure the policy and install Nano-Agents to enforce it.

Configuring Infinity Next Policy

Assets and Zones

Note - The details for the configuration of assets and zones to apply security to and use for configuration in your security settings are describe for each security in other parts of this guide.

If you plan to use, as your enforcement point, the CloudGuard Infinity Next Gateway (explained later in this guide), it is necessary to define web application assets to configure the reverse proxy functionality of the product. See ["CloudGuard Infinity Next Gateway" on page 32](#).

Policy Configuration Practices

A **Practice** is the general form of security services then can be activated, and might lead to an action upon detection of events.

Practices specify the security services applied on asset(s).

To create a new practice(s):

1. From the Navigation Toolbar, select **Policy > Practices**.
2. Select **New**. A window opens to define the new practice.

The exact practices are detailed in the section for each security solution later in this guide.

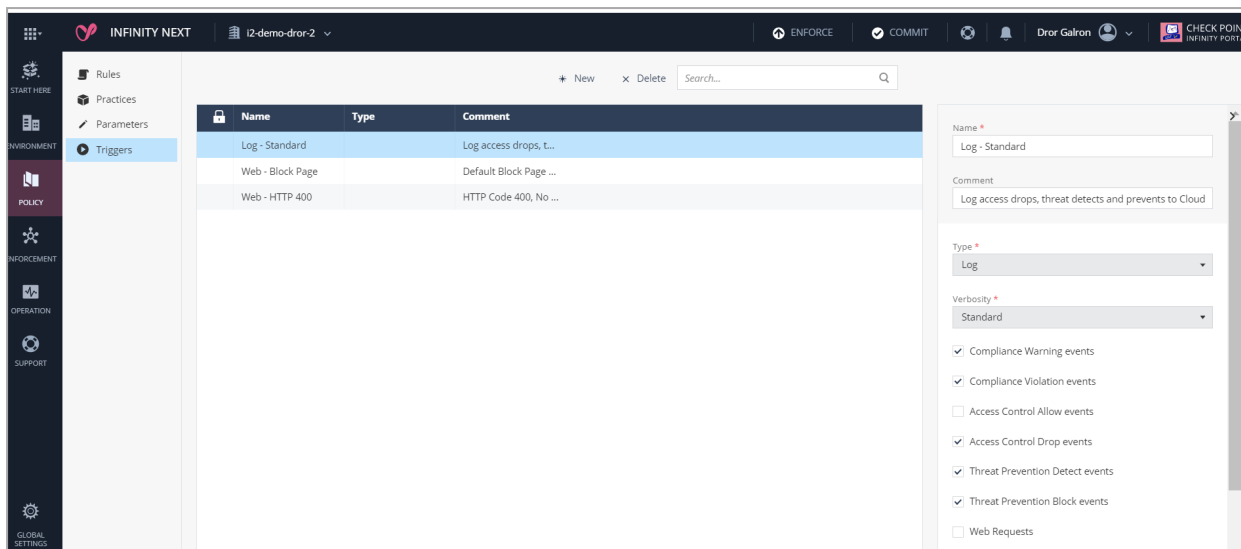
Triggers

A **Trigger** is another action bound to a rule that occurs upon a security practice match on its relevant event.

When a rule is fired and the security practice found a match, it starts a trigger.

To configure a trigger:

1. Click on **Triggers**.
A trigger configuration window opens.



2. Select **New**.

A window open with tabs to defining a new trigger.

Example:

The screenshot shows a configuration form for a trigger object. It has a light gray background and a vertical scrollbar on the right. The form contains the following fields and options:

- Name ***: A text input field with a blue border.
- Comment**: A text input field.
- Type ***: A dropdown menu with "Log" selected.
- Verbosity ***: A dropdown menu with "Standard" selected.
- Event Selection**: A list of checkboxes for selecting event types:
 - ☒ Compliance Warning events
 - ☒ Compliance Violation events
 - ☐ Access Control Allow events
 - ☒ Access Control Drop events
 - ☒ Threat Prevention Detect events
 - ☒ Threat Prevention Block events
 - ☐ Web Requests
- Buttons**: "CANCEL" and "SAVE" buttons at the bottom right.

Name - Required. Give your trigger object a useful name.

Comment - Optional

Type - There are two types of triggers:

- **Log** - Used to send a log message.

The **Verbosity** parameter defines the events to log and specific fields in these events to include.

Note - When you select a Log trigger, the verbosity parameter defines the events to log and which specific fields in these events to include.

- **Web Response** - Modifies the response of the initial request relevant to practices that are activated on web traffic (as in WAAP).

Note - When you select a **Web Response** trigger, you can select between one of these modes:

- **Block Page**
- **Response Code Only**
- **Redirect**

Description:

- Block Page

Name *

Comment

Type *

Web User Response ▼

Mode *

Block Page ▼

Message Title *

Message Body *

HTTP Response Code *

CANCEL

SAVE

Message Title - Text that appears in the **message title** of a WAAP block page.

Message Body - Text that appears in the **message body** of a WAAP block page.

HTTP Response Code - The HTTP response code returned in case the WAAP engine blocked the request.

- **Response Code Only**

Name *

Comment

Type *

Web User Response ▼

Mode *

Response Code Only ▼

HTTP Response Code *

CANCEL

SAVE

- **Redirect**

Redirect URL - The URL, to which to redirect.

Name *

Comment

Type *

Web User Response ▼

Mode *

Redirect ▼

Redirect URL *

☐ Add X-Event-ID to header

CANCEL

SAVE

3. Click **Save**.

Infinity Next Policy Rules

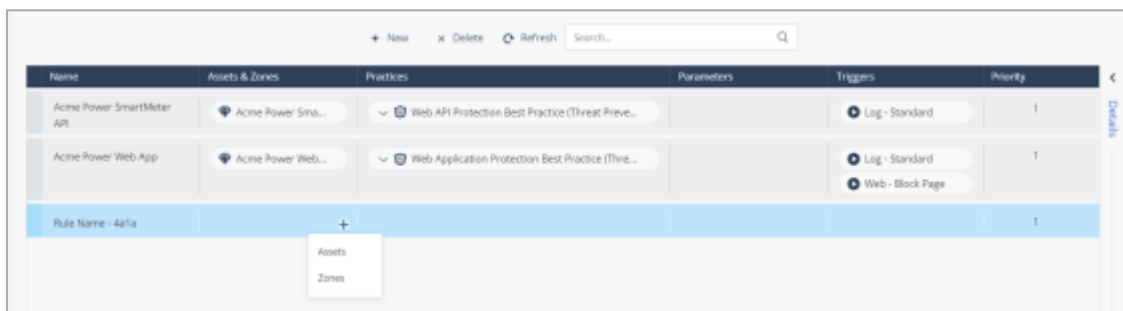
Rules bind the security practices and other specific actions, referred to as triggers, when an applicable condition (matched asset) occurs. The rule allows the user to decide which security to use and when to apply it, as in on which asset(s). Assets are defined either explicitly or through an asset Zone object that defines a dynamic group of assets that use a key:value based query.

To update a rule:

1. Navigate to **Policy > Rules**. Select the rule to update.
2. Click **New**.
3. To change the rule's name, click on the rule name.

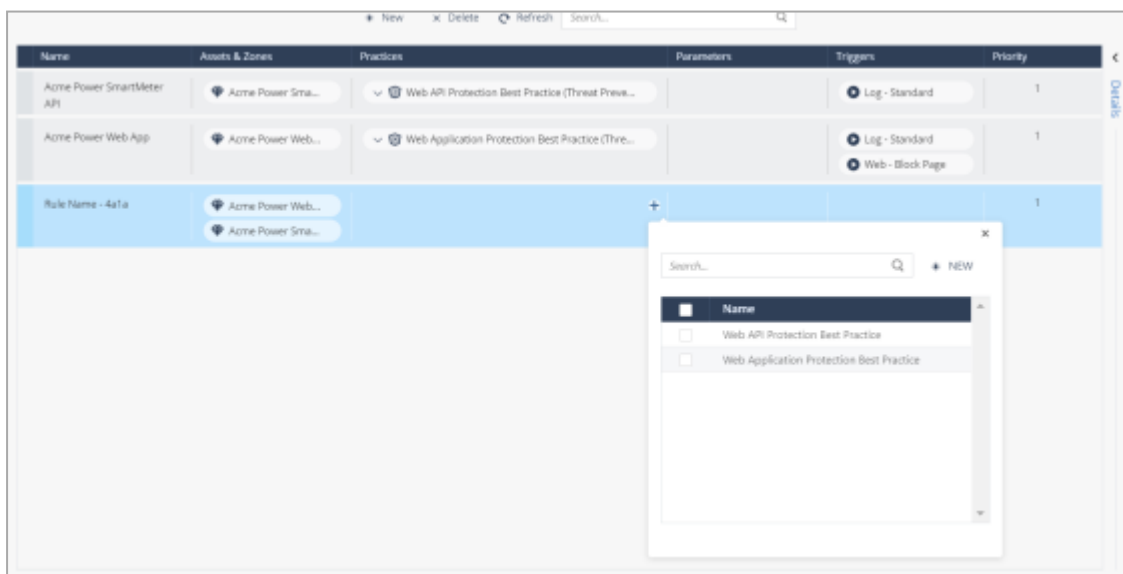
To bind the rule to an asset:

1. Click the **Assets & Zone**. This highlights the column.
2. To bind the rule to an asset, from the **assets** list click the plus sign.



See the specific methods to define the assets for each security practice described in this guide .

3. Click on the **Practices** column. To set the rule security function (s) from the list of the Practices, click the plus sign.



4. Click on the **Parameters** column. To add parameters from the parameters list, click the plus sign. Parameter objects provide additional specific configuration to allow more granularity, and are explained for each security solution and their own practices.
5. Click on the **Triggers** column. To set more rule actions upon a security practice match, from the **Triggers** list, click the plus sign.
6. Set the rule priority to set the sequence of execution, as the rules are in first-match logic.

Note - Rules of the same priority are matched from specific to general. Meaning, if there are two rules, one is matched on the definition of a specific asset and the second matches on the asset being part of an asset zone, then the first rule will apply.

Deploying Nano-Agents

The Infinity Next platform provides a variety of Nano-Agents that can attach to complex hybrid and dynamic environments. Installation usually uses a simple binary, called a *Nano-Egg*, that creates a trust with Infinity Next's platform in the cloud. It then deploys (the egg "hatches", in a manner of speaking) the relevant Nano-Agent services according to policy and the environment in which it is installed, and updates it automatically to the latest version (according to configuration).

Note - Not all security capabilities are available in all Nano-Agents. See the relevant section and security capability to learn where agents to install to enforce a specific capability.

Agent Profile and Registration Tokens

To create a Nano-Agent profile:

1. Connect to the Check Infinity Portal and navigate to Infinity Next.
2. From the **Navigation Toolbar**, select **Enforcement**.
3. Select **Profiles > New**.
 - a. Give the profile a name.
 - b. Select **Agent** as the profile's type.
 - c. Enter the number of agents to represent the maximum quantity of Nano-Agents that can register with this profile.
 - d. Select **Token** as the registration attribute.
 - e. Select how to create the token - either one unique token for each Nano-Agent or one reusable token for all Nano-Agents.
 - f. Save the profile.

- g. Select the new profile > click **Tokens** to receive your token(s):
 - i. For a profile defined with one token for each Nano-Agent, download a CSV file with all tokens.
 - ii. For profile defined with a reusable token, a window opens with the token information. You can use this type of token multiple times, until the limit in the **Number of Agents** field.

Important - Keep the tokens secure as they serve as a method to establish a trust between the Nano-Agent and the Fog. Also, it connects the Nano-Agent to the specific tenant in which the token was generated.

Supported Deployments

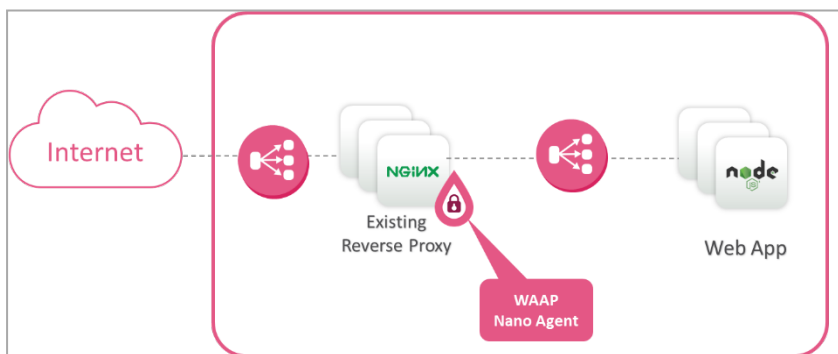
Deployment options for Check Point Infinity Next Nano-Agent:


- Infinity Next Gateway - provided as a Virtual Machine that runs on a Check Point Gaia Operating System with a Reverse Proxy and Check Point Nano-Agent. This options is available for:
 - Amazon Web Services (AWS) - available in the AWS Market Place
 - Microsoft Azure - available in the Azure Market Place
 - Stand Alone Virtual Machine that can be deployed in VMWare
- Infinity Next Container deployed in Docker Environments
- An Embedded Nano-Agent deployed:

Linux machine (for access control)

Linux machines with any NGINX Webserver/Reverse Proxy (for WAAP).

Example:



-  **Roadmap** - An Embedded Nano-Agent deployed on top of Apache, Envoy and other Web Servers, API Servers, and Reverse Proxies.

Note - For downloads and up-to-date information about Deployment Options and supported environments, see the Infinity Next Portal >> **Support > Release Notes and Support > Downloads**.

Basic Nano-Agent Deployment

To install the Nano-Agent:

1. Prepare a token to use with this Nano-Agent installation.
2. Start an SSH connection to the VM that you want to protect with a Nano-Agent.
3. Download the Nano-Egg from **Support > Downloads** page.
4. Provide execution privileges to the Nano-Egg run:

```
chmod +x cp-nano-egg.
```

5. Run the Nano-Egg installation file with this common usage:

```
./cp-nano-egg [--uninstall] | [--install --token <token>
[options...]
```

Or, for a full list of proprieties, see these options:

--uninstall - Removes the Nano-Agent installation

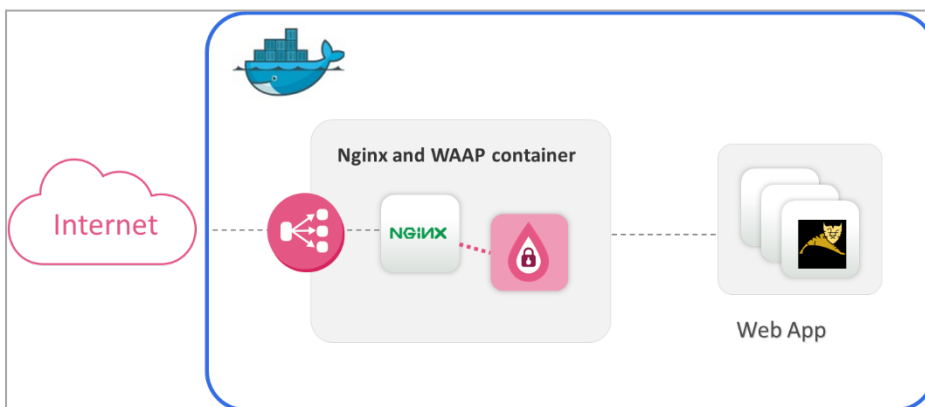
install - Selects the properties to install on a new Nano-Agent.

--token <token> - Registration token taken from the profile in the Infinity Portal.

--proxy [user:pass@]<proxy URL>:<proxy port> - Define the proxy details that you want to use. Or, select **none** if you do not want to use a proxy (default is taken from the OS configuration).

6. Monitor the Nano-Agent's status with this command: `cpnano -s`
7. Navigate to the Infinity Portal > **Enforcement**, go to the (nano) **Agents** page and make sure it shows a new Nano-Agent.

Deploying a Nano-Agent as a Container



Prerequisite:

- Linux host machine

This solution supports environment either with or without a NGINX container that is on.



Best Practice - If you do not already have a NGINX container in your environment, download Check Point's image with these steps.

In environments where the NGINX server is a container that acts as a reverse proxy for upstream locations and, or containers. You can use a Nano-Agent as a different container to receive a stream of all HTTP data from the NGINX container. To do this, the NGINX server loads a standard loadable module that communicates with Nano-Agent container.

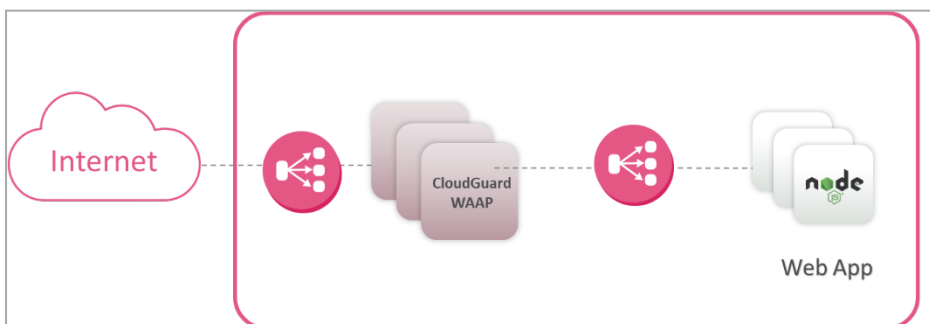
To Install the Nano-Agent as a container:

1. Add the Nano-Agent container image to the deployment CI's applicable container management system.
2. As part of your CI, use the registry that follows (in Docker Hub) to pull the Nano-Agent image:
checkpoint/infinity-next-nano-agent.
3. Prepare a token in advance to use in the Nano-Agent installation.
4. Run the Nano-Agent with this command (-e https_proxy parameter is **optional**):

```
docker run -d --name=agent-container --ipc=host -v=<path to persistent location for agent config>:/etc/cp/conf -v=<path to persistent location for agent data files>:/etc/cp/data -v=<path to persistent location for agent debugs and logs>:/var/log/nano_agent -e https_proxy=<user:password@Proxy address:port> -it <agent-image> /cp-nano-agent --token <token>
```

5. Create or replace the NGINX container using the registry that follows (in Docker Hub) to pull the following NGINX image for this deployment:
checkpoint/infinity-next-nginx
6. Change the NGINX docker "\run" command, add the "--ipc=host" parameter.
7. Run the execution commands for the two containers and make sure that it is running, use `docker ps`.
8. Navigate to the Infinity Portal > **Enforcement** > go to the (nano) **Agents** page and make sure that the new Nano-Agent is added.

CloudGuard Infinity Next Gateway



You can deploy a full machine with a reverse proxy that contains a Nano-Agent already in it. This product is called CloudGuard Infinity Next Gateway and runs on Check Point's Gaia operating system.

You can define multiple web applications with their reverse proxy configuration in the Infinity Next app, and bind them to a specialized profile for CloudGuard Infinity Next Gateway deployments. To scale the machines with the same configuration, connect all instances in a scaling group to the same profile.

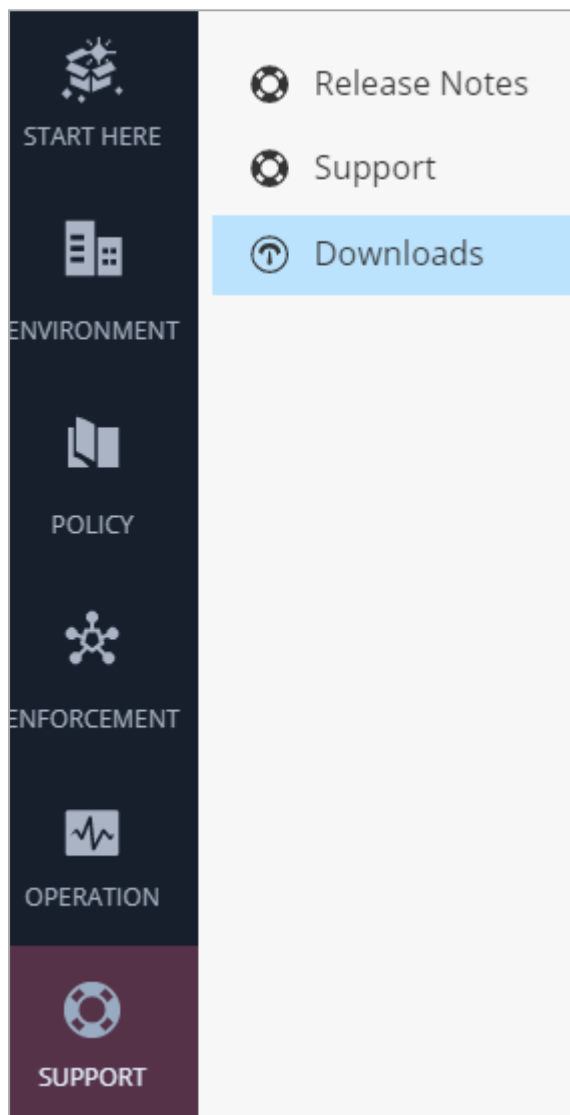
Deploying CloudGuard Infinity Next Gateway

Deployment options for the CloudGuard Infinity Next Gateway:

- As a VM on VMware ESXi 6.7 and later
- Through Microsoft Azure's Marketplace
- Through AWS

VM on VMware deployment

1. Go to the Infinity Next app >**Support**>**Downloads** page.



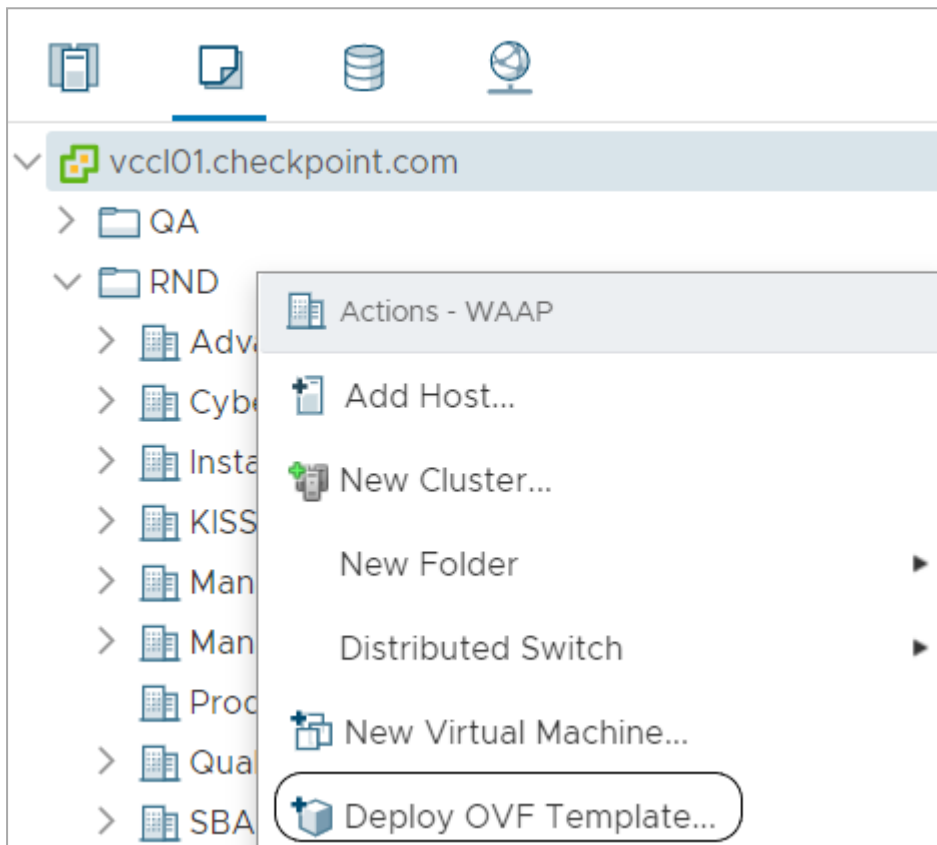
2. Click the **VM Deployment** The Down Details window opens.
3. Click **Download**, the download begins.

The size of the downloaded item is approx. 4.7 GB (this includes the operating system).

4. Extract the downloaded tgz archive, these are the files:

Name	Date modified	Type	Size
CloudGuard_Infinity_Next_Gateway_V1_0.cert	29/09/2020 12:09	CERT File	3 KB
CloudGuard_Infinity_Next_Gateway_V1_0.mf	29/09/2020 12:09	MF File	1 KB
CloudGuard_Infinity_Next_Gateway_V1_0.ovf	29/09/2020 12:09	Open Virtualization Format Package	14 KB
CloudGuard_Infinity_Next_Gateway_V1_0-disk1.vmdk	29/09/2020 12:09	VMware virtual disk file	5,004,635 KB

5. Open a Web browser and enter the URL for the vSphere Web Client:
https://<vcenter_server_ip_address_or_fqdn>/vsphere-client
6. Go to either the **Hosts and Clusters** or **VMs and Templates** tab and right-click on the data center in which you want to deploy the VM.
7. Click **Deploy OVF Template**.



8. Go to **Local file** and select the four extracted files.

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

http | https://remoteserver-address/filetoinstall.ovf | .ova

☒ Local file

Choose Files 4 files

CloudGuard_Infinity_Next_Gateway_V1_0.cert
CloudGuard_Infinity_Next_Gateway_V1_0.mf
CloudGuard_Infinity_Next_Gateway_V1_0.ovf
CloudGuard_Infinity_Next_Gateway_V1_0-disk1.vmdk

9. Click **Next** until you get to **Review details** where you can find details about the certificate, product version, and more.
10. Customize the template options.

Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 Select storage
✓ 6 Select networks
7 Customize template
8 Ready to complete

Customize template

Customize the deployment properties of this software solution.

✓ All properties have valid values

Check Point Configuration	6 settings
Hostname	<input type="text"/>
Default Gateway Address	<input type="text"/>
Password Type	Plain <input type="button" value="v"/>
Admin Password	Password <input type="text"/> Confirm Password <input type="text"/>
Ether 0 IP Address	<input type="text"/>
Ether 0 Subnet Mask Length	24 <input type="button" value="v"/>
DNS Configuration	1 settings
Primary DNS	<input type="text"/>

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Select networks

7 Customize template

8 Ready to complete

▼ DNS Configuration

1 settings

Primary DNS

▼ Proxy Configuration

2 settings

Proxy port

Proxy address

▼ NTP Server Configuration

2 settings

NTP Server

NTP Server Version

4 ▼

▼ Advanced Configuration

3 settings

Infinity Next Agent Token

Password

Confirm Password

Additional Clish Commands

Advanced Configuration Settings

CANCEL

BACK

NEXT

Primary DNS - Optional field for to set a primary DNS server.

Proxy address and port - Optional field to set a Proxy server.

NTP Server and version - Optional field to set a NTP server and its version.

Infinity Next Agent Token - A <registration token> that is obtained when you create a Profile in the **Enforcement/Profile** page. After that, click **Enforce**, then click **Tokens**.

Additional Clish Commands - Optional field for to set additional clish commands to run on first boot. Commands must be separated by "&" delimiter.

Advanced Configuration Settings - Optional field for to set additional environment variables on first boot (as in key=value). Assignments must be separated by "&" delimiter.

11. Click **Finish**. The deployment starts.
12. Power on your deployed VM. On the first boot it setups the template configurations and reboots.

Microsoft Azure Marketplace deployment

1. Go to the Infinity Next app > **Support > Downloads** page and click **Azure deployment**. Or, go directly to the Azure Marketplace > go to Check Point's solutions and select the offer: **CloudGuard Infinity Next Gateway - Access Control and Protection**.
2. Click **Get Now > Continue**.
3. The ARM Template give steps required for deployment of the CloudGuard Infinity Next Gateway.

a. Basics

Subscription - The subscription account where you want to deploy the solution

Resource group - Must create a new Resource Group.

A resource group contains the resources required to successfully deploy a VM in Azure. It is a container that holds related resources for an Azure solution. In Azure, you logically group related resources such as storage accounts, virtual networks, and virtual machines (VMs) to deploy, manage, and maintain them as a single entity.

Region - The Azure region you want to deploy the solution

VM name - The Azure name of the VM

Authentication type - Password or a SSH Public Key

b. Check Point CloudGuard Settings

Basics **Check Point CloudGuard settings** Network settings Review + create

Virtual machine size * ⓘ **1x Standard D2 v2**
2 vcpus, 7 GB memory
[Change size](#)

Bootstrap script ⓘ Select a file

Auto Assign Public IP address ⓘ ☒ Yes
☐ No

Infinity Next Agent Token * ⓘ

Confirm Infinity Next Agent Token * ⓘ

Virtual machine size - The machine size of the VM. Each machine size has its own compute price - <https://docs.microsoft.com/en-us/azure/virtual-machines/sizes>

Auto Assign Public IP address - If **Yes** is selected, then the solution has public IP address.

Bootstrap script - An optional script to run on the initial boot (**Optional** field)

Use development image uri - Set to **NO** (Default selection is "NO").

Infinity Next Agent Token - A <registration token> can be obtained with the creation of a Profile in the **Enforcement/Profile** page. Next, click **Enforce** > click **Tokens**.

c. Network Setting

Basics	Check Point CloudGuard settings	<u>Network settings</u>	Review + create
Configure virtual networks			
Virtual network *		(new) vnet01	▼
		Create new	
Frontend subnet *		(new) Frontend (10.6.0.0/24)	▼
Backend subnet *		(new) Backend (10.6.1.0/24)	▼

Virtual network - Azure VNET name

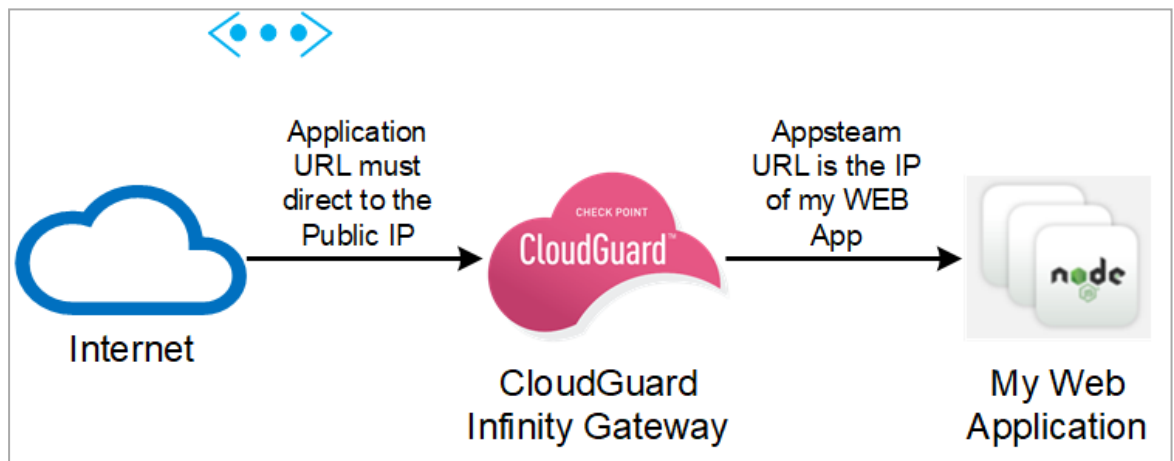
Frontend subnet - The Frontend Subnet CIDR

Backend subnet - The Backend Subnet CIDR

d. Review and Create

This step verifies the Templates input and allows you to review the summary and click create to start the deployment process.

Solution diagram:

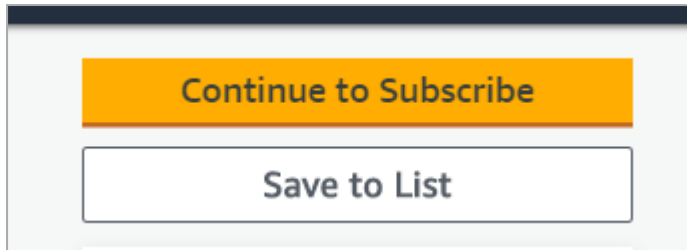


These ports are created as part of the Template deployment:

- SSH Port 22 - For SSH
- TCP Port 443 - For HTTPS
- TCP Port 30443 - Web UI of the CloudGuard Infinity Next Gateway
- TCP Port 80 for HTTP

AWS deployment

1. Go to the Infinity Next app > **Support** > **Downloads** page > click **AWS deployment**. Or, go directly to the AWS Marketplace > go to Check Point's solutions > select the offer: **CloudGuard Infinity Next Gateway - Access Control and Threat Prevention**.
2. To make sure that you are subscribed to the solution, click **Continue to Subscribe**:



3. After successful subscription, you must deploy the CloudGuard Infinity Next Gateway from a Cloud Formation Template developed by Check Point available at the [link](#).
4. Look for the CloudGuard Infinity Gateway section and solution the solution appropriate for your needs:

CloudGuard Infinity Next Gateway				
#	Description	Notes	Download	Direct Launch
22	CloudGuard Infinity Next Gateway	Creates a new VPC and deploys a CloudGuard InInfinity Next Gateway into it.		Launch Stack
23	Deploys and configures a CloudGuard Infinity Next Gateway	Deploys a CloudGuard InInfinity Next Gateway into an existing VPC.		Launch Stack

5. CFT deployment in a New VPC created by the Template.

The template deploys the CloudGuard Infinity Next Gateway in the region the portal is set.

a. VPC Network Configuration

VPC Network Configuration
 Availability zone
 The availability zone in which to deploy the instance

VPC CIDR
 The CIDR block of the VPC.

Public subnet CIDR
 The public subnet of the Security Gateway

Private subnet CIDR
 The private subnet of the Security Gateway

Availability Zone - The availability zone in which to deploy the instance

VPC CIDR - If you select the CFT, to create a new VPC - The CIDR of the new VPC

Public Subnet CIDR - The Public (Frontend) subnet of the CloudGuard Infinity Next Gateway

Private Subnet CIDR - The Private (Backend) subnet of the CloudGuard Infinity Next Gateway

b. EC2 Instance Configuration

EC2 Instance Configuration

Gateway Name

Gateway Instance type
The instance type of the Security Gateways

Key name
The EC2 Key Pair to allow SSH access to the instance

Auto Assign Public IP

Enable AWS Instance Connect
Ec2 Instance Connect is not supported with versions prior to R80.40

Gateway Name - EC2 name

Gateway Instance type - The machine size of the VM. Each machine size has its own compute price. See [Amazon EC2 Instance Types](#).

Key name - The EC2 Key Pair you created for this region

Auto Assign Public IP - If selected **Yes**, then the solution has a public IP address.

Enable AWS Instance Connect - Amazon EC2 Instance Connect is a simple and secure way to connect to your instances using Secure Shell (SSH). See the [AWS EC2 User Guide](#).

c. Check Point Settings

Check Point Settings

Gateway Password hash
Admin user's password hash (use command "openssl passwd -1 PASSWORD" to get the PASSWORD's hash) (optional)

Infinity Next Agent Token
Register/Login to "https://portal.checkpoint.com/" IN ENFORCEMENT Tab go to: Profiles -> Create an agent, and press "tokens"

Gateway Password hash - Admin user's password hash of the GAIA machine.

To provide the password hash, invoke the command in your shell:

```
"openssl passwd -1 <Password>"
```

Infinity Next Agent Token - A <registration token> can be obtained with the creation of a Profile in the **Enforcement/Profile** page. Next, click **Enforce** > click **Tokens**.

d. Advanced Settings

Advanced Settings

Gateway Hostname
(optional)

Bootstrap Script
An optional script with semicolon (;) separated commands to run on the initial boot (optional)

Gateway Hostname (Optional) - The Gaia Hostname

Bootstrap Script (Optional)

*The default Security Group associated to the VPC created is defined with these ports for Inbound:

- SSH 22
- HTTP 80 is enabled by default in the NSG
- HTTPS 443
- TCP 30443 (Download)

Configuring the Dedicated Check Point Reverse Proxy

A Nano-Agent profile object (with a unique web application configuration) must be created for each Reverse Proxy.

1. Go to **Enforcement > Profiles**.
2. Create a profile for **Type:Agent** and **Agent Type:Infinity Next Gateway**.

GENERAL
SETTINGS
REVERSE PROXY

Name *

Comment

Type *
Agent

Agent Type *
Infinity Next Gateway

Note - The action adds a **Reverse proxy** tab.

3. Do the steps in "Deployment and Configuration" -> "Agent Profile and Registration Tokens" that describe how to define the registration tokens of the agents installed as part of the deployment to the Infinity Next cloud.

In addition to the regular instructions used to define a Nano-Agent's profile, the "Reverse Proxy" tab allows you to bind the reverse proxy to multiple web application definitions that can be created in the **Environment > Assets** page.

GENERAL SETTINGS **REVERSE PROXY**

Web Assets *

Search...

<input type="checkbox"/>	Name
No data	

CANCEL SAVE

Go to **Environment -> Assets** and define web applications similarly to the explanation in the "Configuring WAAP Assets" section in this guide.

But, for "Web application" type assets, on top of that, go to **New Asset > Reverse Proxy** and add the Reverse proxy configuration for that specific app. Each asset of this type can now be added to the appropriate Nano-Agent profile you created via the "Reverse Proxy" tab list.

NEW ASSET
X

General
Reverse proxy
Parameters

Upstream URL

Server Certificate

Upload...
No file selected

Certificate Key

Upload...
No file selected

Proxy Settings

* New
X Delete

Key	Value
No Content	

CANCEL
SAVE

Upstream URL - The defined upstream URL for this specific web application (the URL the external URL is translated into - the external URL was defined in the "General" tab)

Server certificate and certificate key - Means to authenticate vs the target server behind the reverse proxy.
Note -for a manual upload of certificates, see ["How to Manually Upload Certificates" on page 45](#).

Proxy Settings:

Supported Keys	Purpose	Allowed Values
<code>setHeader</code>	Allows to redefine or append fields to the request header passed to the proxied server. The value can contain text, variables, and their combinations.	<Header name>:<Header value> For host header: Host:<value> Example: Host:\$host
<code>connectTimeout</code>	Defines a timeout to establish a connection with a proxied server.	Positive number

Supported Keys	Purpose	Allowed Values
<code>readTimeout</code>	Defines a timeout to read a response from the proxied server. The timeout is set only between two successive read operations, not for the transmission of the whole response. If the proxied server does not transmit anything within this time, the connection is closed.	Positive number
<code>proxySendTimeout</code>	Sets a timeout to transmit a request to the proxied server. The timeout is set only between two successive write operations, not for the transmission of the whole request. If the proxied server does not receive anything within this time, the connection is closed.	Positive number
<code>keepAliveTimeout</code>	Sets a timeout in which a keep-alive client connection stays open on the server side. The zero value disables keep-alive client connections.	Positive number
<code>accessLog</code>	Activates the access.	true/false
<code>additionalLocationConfig</code>	Adds content of file with additional configurations inside the server block of Nginx configuration.	File name
<code>additonalServerConfig</code>	Adds content of file with additional configurations outside the server block of Nginx configuration.	File name
<code>healthCheck</code>	Checks proxied server status, each minute.	true/false
<code>dnsServer</code>	Configures name servers used to resolve names of upstream servers into addresses.	Ip/<IP>:<Port> For example: 172.15.14.8090
<code>ProxySslName</code>	Lets you override the server name used to verify the certificate of the proxied HTTPS server. And, allow it to pass through SNI when you establish a connection with the proxied HTTPS server	String of server name
<code>ProxySSLVerify</code>	Enables or disabled verification of the proxied HTTPS server certificate.	On/off
<code>nginxIncludeLines</code>	Set of NGINX configuration lines separated by a ; to be added to this asset configuration file.	<line>; <line>;
<code>certificateFilePath</code>	Path to manually uploaded certificate file.	Full path
<code>certificateKeyPath</code>	Path to manually uploaded certificate key file.	Full path

How to Manually Upload Certificates

To manually upload your certificates to the VM manually, do these steps:

1. Log in to the CloudGuard Infinity Next Gateway machine.
2. Transfer the certificate and key files to the machine.
3. If you did not create a Nano-Agent profile object configured as the Infinity Next Gateway in the Check Point Portal, then create a new Nano-Agent profile before you do step 4. See ["Configuring the Dedicated Check Point Reverse Proxy" on page 41](#).

Important - Keep the name used in the -o flag. It is used again.

4. In the Check Point Portal, go to **Environment** > **Assets** > select the asset you want to edit.
5. From the **Reverse proxy** tab, make sure that the check box **Deploy certificate manually** is selected.
6. From **Proxy Settings**, click **New**.
7. In the **Key** column, select **certificateFilePath**, and in the **Value** column enter the full path of the certificate file you uploaded to the machine..
8. Again, click **New**.
9. In the **Key** column, select **certificateKeyPath**, and in the **Value** column enter the full path of the certificate key file you uploaded to the machine.

EDIT BENCHMARK SERVER

General

Reverse proxy

Parameters

Upstream URL

http://127.0.0.1:3000

☒ Deploy certificate manually

Server Certificate

Upload...

Certificate Key

Upload...

Proxy Settings

* New

x Delete

Key		Value
certificateFilePath	▼	/home/admin/test.pem
certificateKeyPath	▼	/home/admin/test.key

CANCEL

SAVE

10. Click **Save** and then **Enforce**.

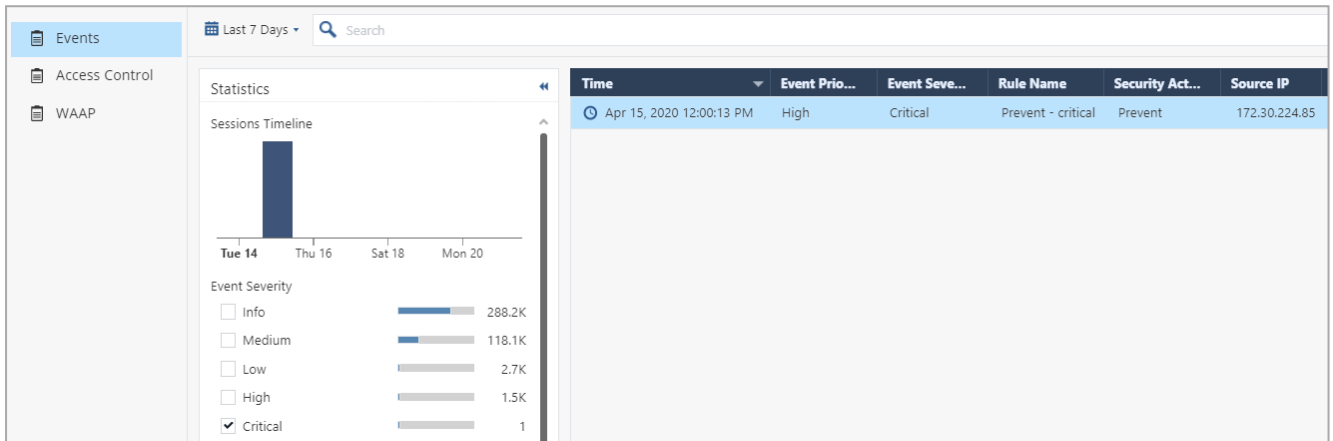
Infinity Next Events

Use the Event log to see the list of events and get details about specific events.

To see the Event log:

From the Navigation Toolbar, select **Operation > Events**.

Or, you can drill down on a field in the WAAP dashboard.



When you click on an event, a Log Card shows details about the specific transaction based on the trigger used.

Example Log Card:

Event Severity Classification	Protect Web Service Name	HTTP Transaction Information	Threat Prevention
<div>Event Info</div> <div>Event Time: 2020-04-15T12:00:13.000Z</div> <div>Event Type: Critical</div> <div>Event Priority: High</div> <div>Event Source: Rule Engine</div> <div>Event Action: Log</div> <div>Event Category: Security</div> <div>Event Description: A</div> <div>Agent ID: 0020180-0000-0000-0000-000000000000</div> <div>Product Type: Threat Prevention</div> <div>Product Subtype: Web Application</div>	<div>Web Service Name</div> <div>Web Service Name: /api/v1/insertintoelectricity_meters_readings</div>	<div>Transaction</div> <div>Source IP: 37.142.6.162</div> <div>Source Port: 606K</div> <div>Source Identifier: 37.142.6.162</div> <div>HTTP Host: 34.96.201.236</div> <div>HTTP Method: GET</div> <div>HTTP Path: /user-app/getLatestReadData</div> <div>HTTP URI Query: uid=1%27%3BINSERT%20INTO%20electricity_meters_readings%20(uid%2C%20count_number%2C%20delta%2C%20reading_time%2C%20reading_value)%20VALUES(%27e5488905-0af3-40aa-bd64-932a3b0f5017%27%2C4000%2C0%2C%272020-04-16%2018:58:17.236523%27%2C0%20SELECT%20%20FROM%20electricity_meters_readings%20WHERE%20%271%27%3D%271</div>	<div>Threat Prevention</div> <div>WAAP Final Score: 890</div> <div>WAAP Indicators Score: 805</div> <div>WAAP URI Score: 864</div> <div>WAAP User Reputation Score: 451</div> <div>Malicious Content: 1';insertintoelectricity_meters_readings(uid,count_number,delta,reading_time,reading_value)values('2b65f779-3d7e-4d84-b5d9-2a23dd9b2bd2',4000,0,'2020-04-0113:31:35.534763',0);select'fromelectricity_meters_readingswhere'1='1</div> <div>WAAP Found Indicators: quotes_ev_fast_reg_4</div> <div>WAAP Override: None</div>

The part of the request that has the malicious content

To filter the table:

- 1. Right-click on a specific value in the table in the **Log Card**.

Time	Event Prio...	Event Seve...	Rule Name
Apr 16, 2020 9:26:48 PM	Medium	Info	
Apr 16, 2020 9:25:57 PM	High	Critical	Protecting API
Apr 16, 2020 7:23:47 PM	Medium	Info	
Apr 16, 2020 7:23:47 PM	Low		ing Applica
Apr 16, 2020 7:23:46 PM	Low		Protecting Applica
Apr 16, 2020 7:23:46 PM	High	High	Protecting Applica
Apr 16, 2020 7:23:45 PM	Low	Info	Protecting Applica

2. Click **Enter**. The filtered **Log Card** window opens.

Card

Threat Prevention

Malicious Content:

vqlweb.js:12,391001mnh
is.\$2\$3=null;this.\$2\$4
=null;this.\$2\$5=null;th
is.\$2\$6=null;hi.call(thi
s,e,newif(mp.toString()
,0));this.\$c=ex;this.\$e=
ne

WAAP Found

Indicators:

toString(
this.
code_execution_fast_re
g_1
=
null
;

WAAP Override:

None

IDs

Log Id:

775.9K

Practice Id:

5e5e2e146329ed0017372bc8

Asset Id:

5e3b34146906db75b4393fbb

WAAP Management

Check Point Infinity Next application can manage multiple security products, among them is CloudGuard WAAP.



Best Practices - To configure security for your web applications we recommend that you do these steps:

1. Configure your web application and, or API assets.
2. Create a rule to protect the applications.

Optional:

- Customize your security practices and parameters.
- Customize your triggers (to control reports).

In "Configuring WAAP Assets", we demonstrate how to configure WAAP assets, practices, and rules to secure your web applications.

Configuring WAAP Assets

Check Point's Infinity Next application protects your assets. An "Asset" maps to a physical object (such as a Virtual Machine's IP address), or an abstract entity (such as URL).

To see your assets:

1. From the Navigation Toolbar, click the **Enforcement** tab > **Assets**. The Asset table opens.
The Asset table lists the assets currently configured in the system.
2. To view details about asset, click on an asset.

The screenshot shows the Check Point Infinity Next interface. The left sidebar contains navigation options: START HERE, ENVIRONMENT, POLICY, ENFORCEMENT, OPERATION, SUPPORT, GLOBAL SETTINGS, and APPROVERS. The main area displays the 'Assets' table under the 'Enforcement' tab. The table lists two assets: 'Acme Power SmartMeters API' and 'Acme Power Web App'. Below the table, the details for 'Acme Power SmartMeters API' are shown under the 'GENERAL' tab.

Status	Name	Namespace	Node	Instance Type	Host	Listening Address	Vendor	Account Id	VPC Id
✓	Acme Power SmartMeters API	N/A	N/A	N/A	192.168.238.128/In...	*:8000	N/A	N/A	N/A
✓	Acme Power Web App	N/A	N/A	N/A	192.168.238.128/us...	*:80	N/A	N/A	N/A

GENERAL

Acme Power SmartMeters API

Host 192.168.238.128/In...	Phase production	Category cloud
Listening Address *:8000	Class workload	Family webAPI

To edit an asset:

1. Click on the asset. Make sure it shows the asset as highlighted.
2. Click **Enter**.

To create a new asset:

1. Click **New**.

2. In each of the fields, enter the required information:

Field	Description
Name	Required. Give your asset a useful name.
Comment	Optional
Class	Select Workload .
Category	Select Cloud .

Field	Description
Family	Select either: <ul style="list-style-type: none"> ■ Web Application: A website that facilitates users browsing -or- ■ Web API: A web service that delivers applications that use specific REST APIs
Stage	Select either Production or Staging . This property is used later to query the assets in the course of zone definition.
Application URLs	Required - Add at least one host address with an option listening port. <ul style="list-style-type: none"> ■ Example: <code>www.acme.com</code> (listen to inbound traffic to this address on all ports) ■ Example: <code>www.acme.com:80</code> (only listen to inbound traffic to this address on port 80) ■ Example: <code>www.acme.com/api1</code>
Parameters	Use the Parameters tab to bind the parameters to a specific asset. See "WAAP Parameters" on page 55 .

Configuring WAAP Policy

In Policy Configuration, you configure the rules that enforce the security for the assets.

Each rule applies a unique set of assets that apply a condition and an action.

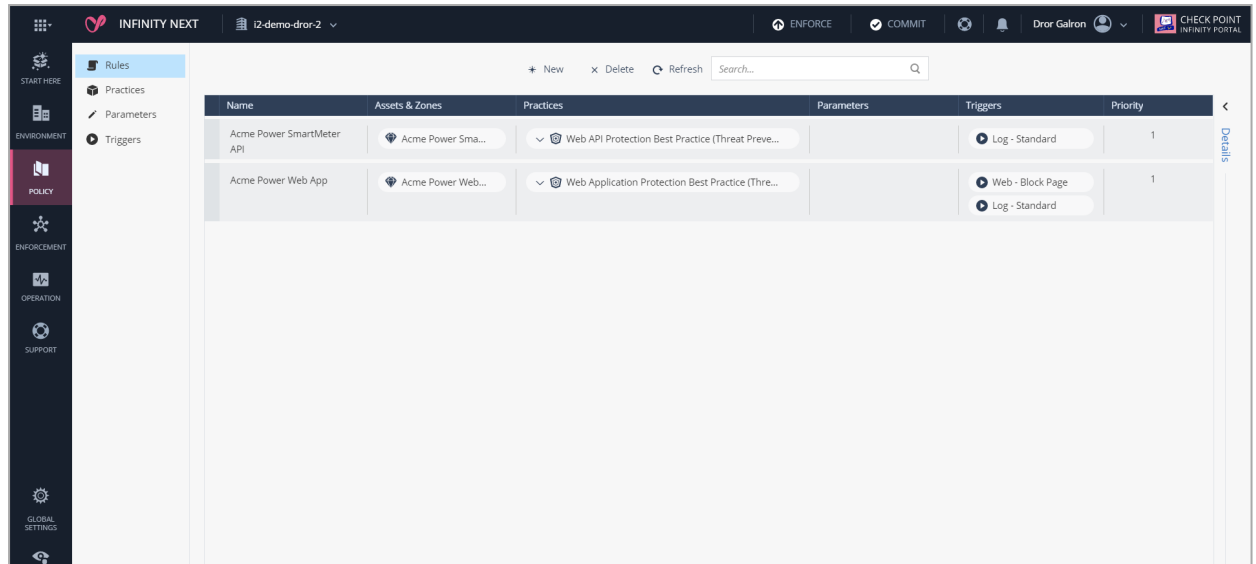
If the condition is met, then it triggers an action.

Notes:

- A *Condition* is a practice that combines with parameters
- An Action is defined as a "trigger"

To see the Policy Configuration rules for a specific asset:

1. From the Navigation Toolbar, click **Policy > Rules**.
2. On the right-side of the Rule table, click the left arrow or **Details**.



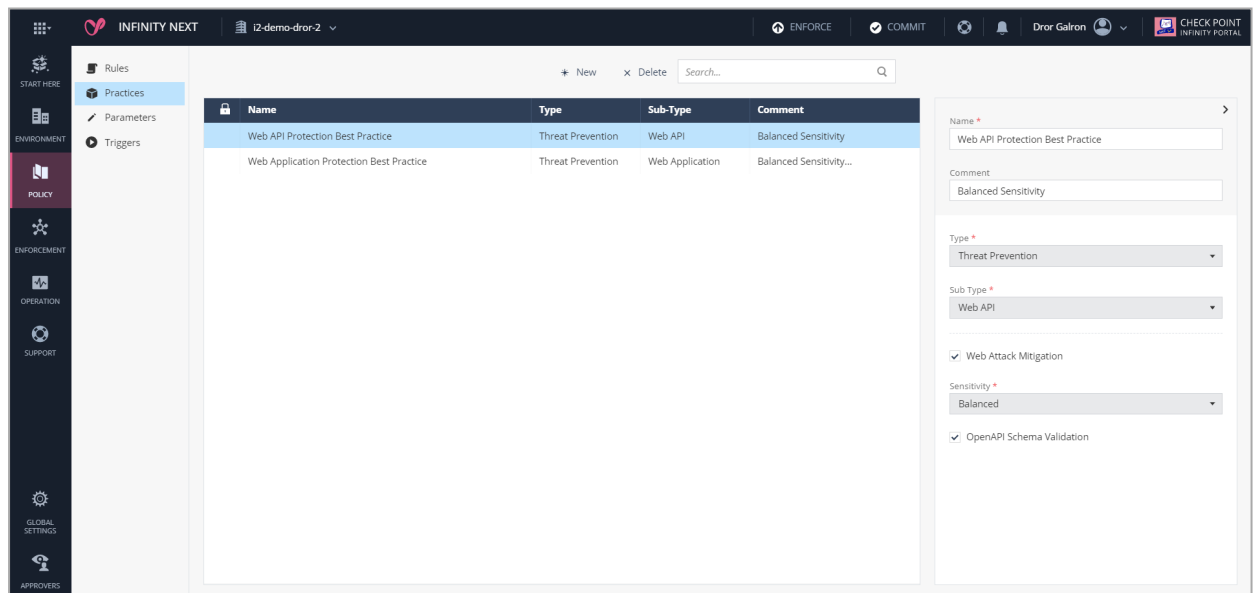
WAAP Practices

Defining Practices

A Practice is the general form of a security function. They specify the security services that applied on asset(s).

To create a new practice(s):

1. From the Navigation Toolbar, select **Policy > Practices**.



2. Select **New**. A window opens to define the new practice.

The form is used to define a new practice. It contains the following fields and options:

- Name ***: A text input field.
- Comment**: A text input field.
- Type ***: A dropdown menu with the selected value "Threat Prevention".
- Sub Type ***: A dropdown menu with the selected value "Web Application".
- Web Attack Mitigation**: A checkbox that is checked.
- Sensitivity ***: A dropdown menu with the selected value "Transparent".
- Bot Protection**: A checkbox that is checked.
- Buttons**: "CANCEL" and "SAVE" buttons at the bottom right.

Web API Protection

For Web **API** protection, you can turn on OpenAPI schema validation for specific pages. To set the practice as Web application API protection:

- For **Type**, select **Threat Prevention**.
- For **Subtype**, select **Web API**.

Web Application Protection

For Web **Application** protection, you can turn on bot protection for specific pages. Also, you must add additional bot protection parameters to your asset rule.

WAAP Parameters

Parameters specify more information that the WAAP ML (Machine Learning) engine uses to enforce security practices. In some cases, when a specific security service is applied, a parameter assignment is a must (to turn on an OpenAPI Schema validation requires OpenAPI schema parameters). In some cases, the parameters are optional and help Check Point to configure the security service behavior (as in a parameter override that can change the engine behavior in specific cases).

To create or edit a new parameter:

1. From the Navigation Toolbar, select **Policy > Parameter > New**.
To edit a parameter, double-click on the parameter or click **Details**.
2. Click either the left arrow on right-side of the table, or click **Details** on the left side of the table
3. To create new parameter, click **New**.
4. To delete a parameter, select the parameter and click **Delete**.

Notes about WAAP parameters:

- Each parameter has a name, description, and a type.
- Each type has specific configuration fields. This is a description of the parameter types applicable to WAAP:

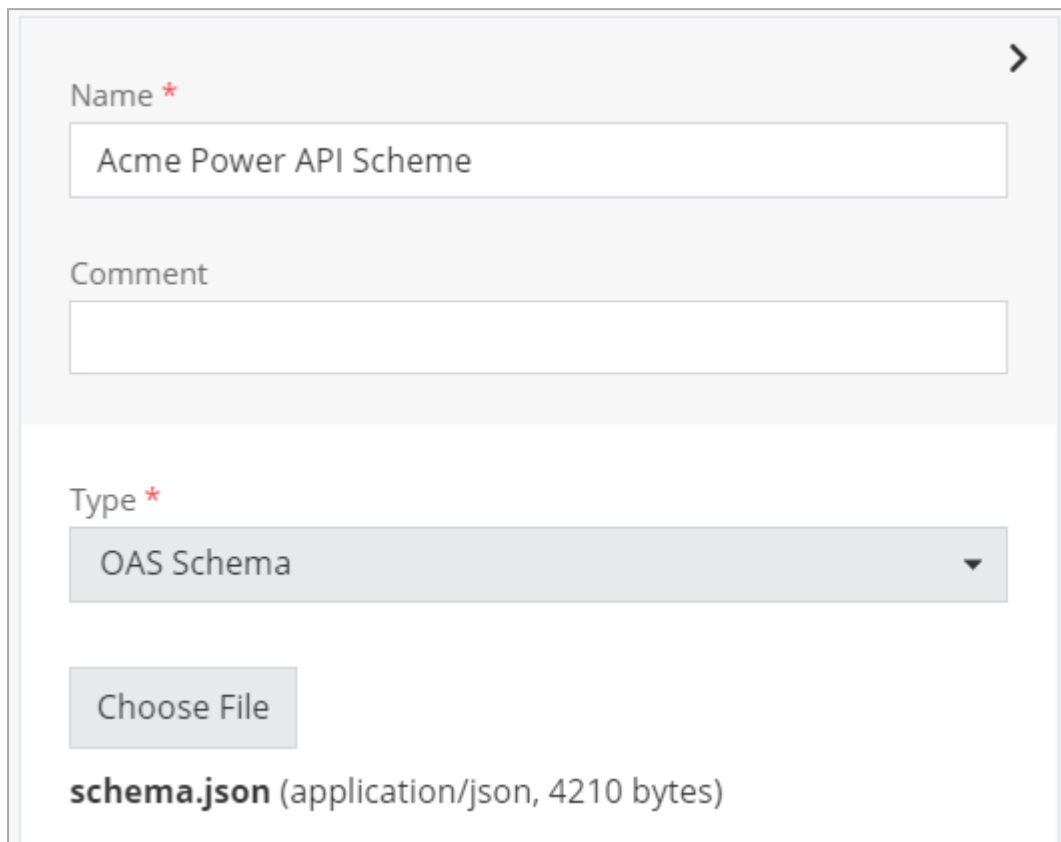
The screenshot displays a web form for configuring WAAP parameters. It includes the following elements:

- Name ***: A text input field with a red asterisk indicating it is required.
- Comment**: A text input field.
- Type ***: A dropdown menu with a red asterisk indicating it is required. The menu is open, showing a list of parameter types:
 - Overrides**: This option is selected and highlighted in grey.
 - Web Anti-Bot**
 - OAS Schema**
 - Trusted Sources**
 - WAAP Parameters**

- Each parameter has a different type.

Schema Configuration

If you have an API server and require validation for your API schema, we recommend that you create a new parameter called "OAS Schema". Next, upload your schema file (OpenAPI 3).



The form is titled "Schema Configuration" and is enclosed in a light gray border. It contains the following fields and elements:

- Name ***: A text input field containing "Acme Power API Scheme".
- Comment**: A text input field, currently empty.
- Type ***: A dropdown menu with "OAS Schema" selected.
- Choose File**: A button to upload a file.
- schema.json (application/json, 4210 bytes)**: A label indicating the uploaded file name, type, and size.

WAAP supports both YAML and JSON schema files.

Note - In most cases, you must give this parameter to a specific asset - and not to a rule.

Overrides

The Overrides parameter permits you to override the WAAP ML engine decision based on specific parameters.

In the **Match** section, select the condition that must be matched for the override behavior to apply. The override expressions are Boolean. This allows you to create a complex expression that uses **and/or/not** options with the combination of these expressions. To add more conditions with **and/or/not** relations, click the double quotes symbol `"`.

- **uri** - Regular expression that determines the uri to match. For example: `/login/.*`
- **sourceidentifier** - Regular expression and CIDR that determines the source identifier to match. For example: `192.168.24.0/24` or `.*@acme.com`
- **sourceip** - CIDR that determines the physical source IP to match. For example:
`192.168.24.0/16`
- **paramname** - Regular expression that determines the parameter name to match (For Example: `.*password.*`).
- **paramvalue** - Regular expression that determines the parameter value to match. For example: `^[0-9]{12}(:[0-9]{3})?$`
- **indicator** - The indicator that needs to be matched. This can be a list separated by commas.

In the behavior section, select the behavior to apply to the selected parameter.

- **action** - Overrides the WAAP engine behavior because it accepts and, or rejects traffic based on criteria defined in the Match section.
- **log** - Does not send a log to the management based on criteria defined in the Match section.
- **httpSourceId** - Overrides the logical source to allow the engine to understand the real source of the traffic.

Note - You must give this parameter to a specific rule, and not to an asset.

Trusted Sources

To increase the product's capability to learn, specify the Trusted Sources. Use this parameter configuration to automatically whitelist some of the indicators if they were hit by one or more trusted sources.

To specify trusted sources, add lines to the table below, each line can represent one or more trusted sources.

Parameter	Definition
Source IP	Physical source IP or CIDR of the trusted source
X-Forwarded-For	IP address or CIDR of the trusted source received in the X-Forwarded-For header
Cookie:_oauth2_proxy	Email address or RegEx of email addresses received in the <code>_oauth2_proxy</code> cookie header fields (for example: <code>.*@acme.com</code>)

In the **trusted sources to learn from** you can set the minimal number of trusted sources that can whitelist an indicator.

Note - You must give this parameter to a specific rule, and not to an asset.

Web Anti-Bot

The web Anti-Bot parameter defines the web pages' URLs. It injects Java script and validates the URL. You can add multiple URLs for Anti-Bot parameter.

Type *

Web Anti-Bot

Injected URIs

* New

Name
No Content

Validated URIs

* New

Name
No Content

Analyzing WAAP Events

The WAAP ML engine classifies each request and decides its attack possibilities through the smart AI engine. The engine class show in the **Event Severity** field.

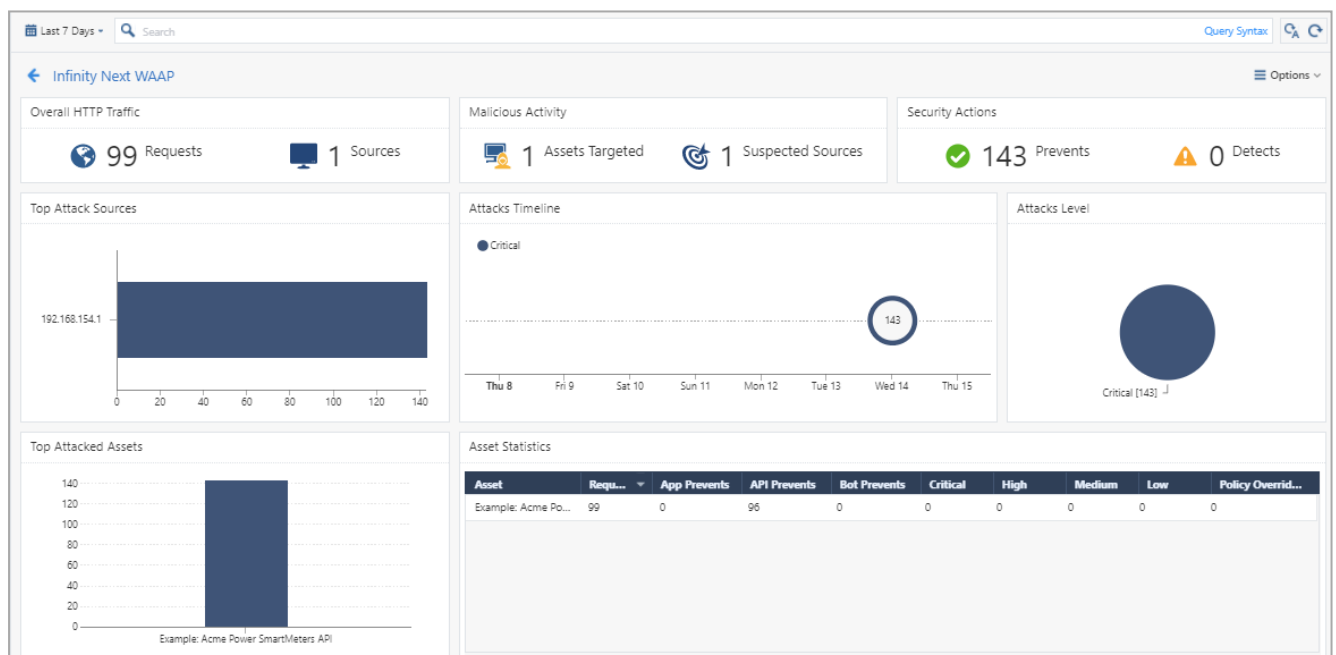
Event Severity	Description
None & Low	Unlikely to be an attack
Medium	Small chance that this is an attack. Check it occasionally.
High	A strong chance that this is an attack
Critical	Most probably an attack - check it out

Using the WAAP Dashboard

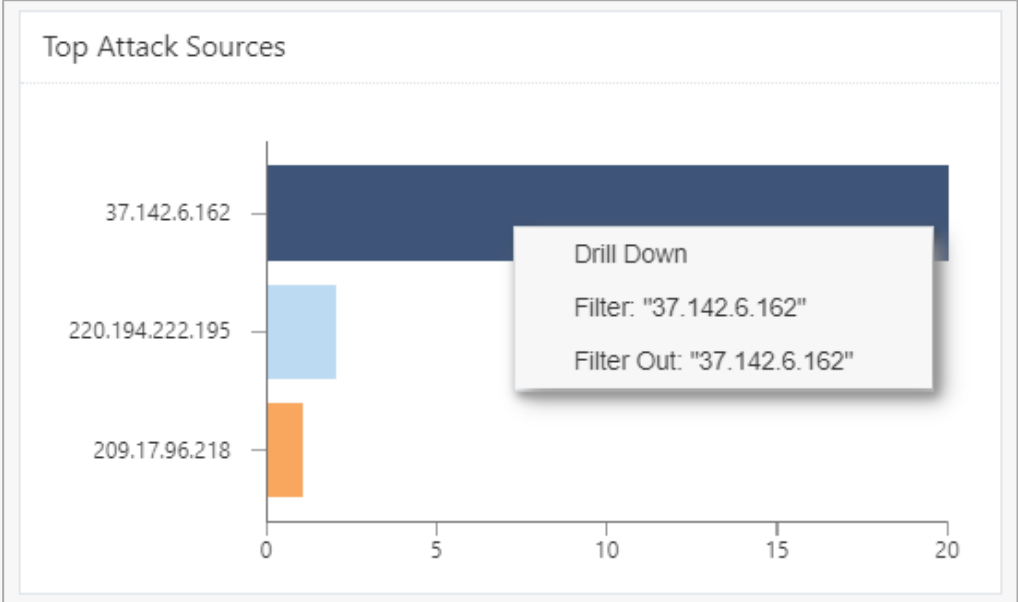
The WAAP dashboard is a single-pane view of all your security events.

To see the WAAP dashboard:

From the Navigation Toolbar, select **OPERATION > WAAP**. The WAAP dashboard opens:

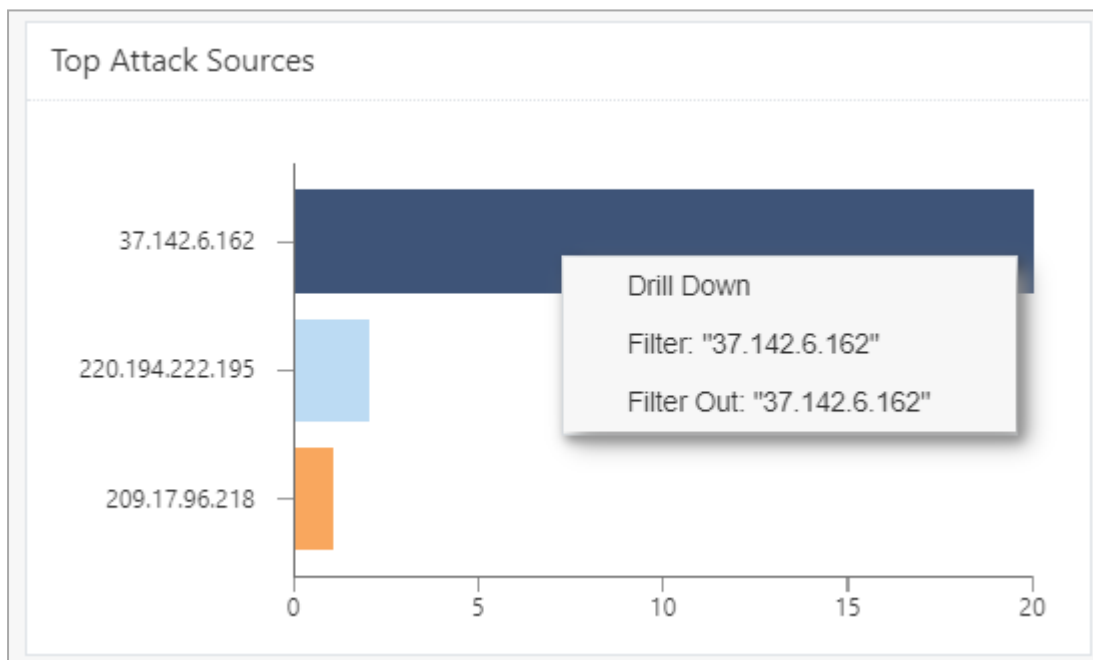


Field	Description
Overall HTTP Traffic	Statistics show the number of overall request for the time period and unique number of users and, or identities that use the protected web servers.

Field	Description
Malicious Activity	Overall statistics of the number of attackers (users and, or identities) and the number of attacks on web servers.
Security Actions	Overall number of events that where prevented and detected.
Top Attack Sources	<ul style="list-style-type: none"> ■ A chart of the top attackers by number of events. ■ Number of events on a time line, gives visibility to the changes in the security posture. 
Attacks Level	Chart of the number of attack by severity.
Top Attack Assets	Chart of the most attacked web servers.
Asset Statistics	Table of protected web server(s) and it statistics.

Field	Description																												
Attacks Timeline	<p>Give a specific period that you need the dashboard to show.</p> <div> <div>Last 7 Days</div> <div>Search</div> </div> <p>Select a time filter</p> <table> <tr> <th colspan="2">Presets</th></tr> <tr> <td>Today</td><td>(Apr 27, 2020)</td></tr> <tr> <td>Yesterday</td><td>(Apr 26, 2020)</td></tr> <tr> <td>This Week</td><td>(Since Apr 27, 2020)</td></tr> <tr> <td>This Month</td><td>(Since Apr 1, 2020)</td></tr> <tr> <td>This Year</td><td>(Since Jan 1, 2020)</td></tr> <tr> <td>Last Hour</td><td>(Since 2:45 PM)</td></tr> <tr> <td>Last 24 Hours</td><td>(Since Apr 26, 2020 3:45 PM)</td></tr> <tr> <td>Last 7 Days</td><td>(Since Apr 20, 2020)</td></tr> <tr> <td>Last Week</td><td>(Apr 20, 2020 - Apr 26, 2020)</td></tr> <tr> <td>Last 30 Days</td><td>(Since Mar 28, 2020)</td></tr> <tr> <td>Last Month</td><td>(Mar 2020)</td></tr> <tr> <td>Last 365 Days</td><td>(Since Apr 28, 2019)</td></tr> <tr> <td>Last Year</td><td>(2019)</td></tr> </table> <p>Relative Time Range</p> <p>Date Range</p> <p>Date and Time Range</p>	Presets		Today	(Apr 27, 2020)	Yesterday	(Apr 26, 2020)	This Week	(Since Apr 27, 2020)	This Month	(Since Apr 1, 2020)	This Year	(Since Jan 1, 2020)	Last Hour	(Since 2:45 PM)	Last 24 Hours	(Since Apr 26, 2020 3:45 PM)	Last 7 Days	(Since Apr 20, 2020)	Last Week	(Apr 20, 2020 - Apr 26, 2020)	Last 30 Days	(Since Mar 28, 2020)	Last Month	(Mar 2020)	Last 365 Days	(Since Apr 28, 2019)	Last Year	(2019)
Presets																													
Today	(Apr 27, 2020)																												
Yesterday	(Apr 26, 2020)																												
This Week	(Since Apr 27, 2020)																												
This Month	(Since Apr 1, 2020)																												
This Year	(Since Jan 1, 2020)																												
Last Hour	(Since 2:45 PM)																												
Last 24 Hours	(Since Apr 26, 2020 3:45 PM)																												
Last 7 Days	(Since Apr 20, 2020)																												
Last Week	(Apr 20, 2020 - Apr 26, 2020)																												
Last 30 Days	(Since Mar 28, 2020)																												
Last Month	(Mar 2020)																												
Last 365 Days	(Since Apr 28, 2019)																												
Last Year	(2019)																												

Note - To filter the dashboard and drill down to the log events, right-click on a graph, chart, or table item.



WAAP Best Practices

Check Point recommends that customers use these WAAP best practices.

Initial Learning Period

The WAAP engine learning-model decreases the quantity of Critical and High events over time as it learns the site traffic and understands the user's behavior. It learns in a continuous manner. *Note* - There is no "learning-mode".

When a new asset is added, we recommend, that the WAAP run in detect/transparent mode to allow an initial baseline. The learning period is 3-4 days with substantial quantity of traffic.

Moving to Prevent Mode

Use WAAP in transparent mode for the first 3-4 days. The number of day depends on the traffic volume.

Notes:

- Low sensitivity web attack mitigation policy blocks only critical events
- Balanced sensitivity web attack mitigation policy blocks only high and critical events
- High sensitivity web attack mitigation policy block only medium, high & critical events

The move to prevent mode must be gradual. We recommend that you use these guidelines.

- Analyze the critical severity events from the start of the initial Machine Learning
- Add overrides for traffic that the WAAP ML engine has misclassified (based on the `uri`, source identifier, parameter, and more)
- Repeat the procedure until you have a zero false critical events
- At this time you can move to "low" prevent mode sensitivity
- Do the procedure again with high severity events and move to balanced sensitivity

For some sites, low sensitivity is best. Other sites, based on site content, may need a higher level of sensitivity.

Access Control

Infinity Next offers security based on asset properties. Access control is defined by a list of keys (that is expected to grow with the supported of more environments and asset inventories).

The asset-centric policy of Infinity Next allows you to define dynamic groups of assets (Zones), and the allowed connections between them (adjacency). This creates a defined zone-based access diagram that the policy enforces.

You can also define a more traditional access control policy, but still asset-centric. To define this kind of policy, define incoming/outgoing access practices, and then activate them on specific assets of asset groups with the use of rules.

Note - Rules of the same priority are matched from specific to general. This means, if there are two rules, one is matched on the definition of a specific asset and the second matches on the asset being part of an asset zone, then the first rule will apply.

Supported environments

Infinity Next access control is enforced through Linux Nano-Agents. The Linux Nano-Agents attach to the Linux kernel and the network attachment to enforce the access policy at the lowest level possible.

For the full, updated, list of supported Linux distributions and kernels go to the Infinity Next the app > **Support** > **Release Notes** page.

Access Control Management

Step 1: Use a query of supported keys to define dynamic groups of assets called *Zones*.

Step 2: Use one these asset-centric methods to define an access policy in Infinity Next.

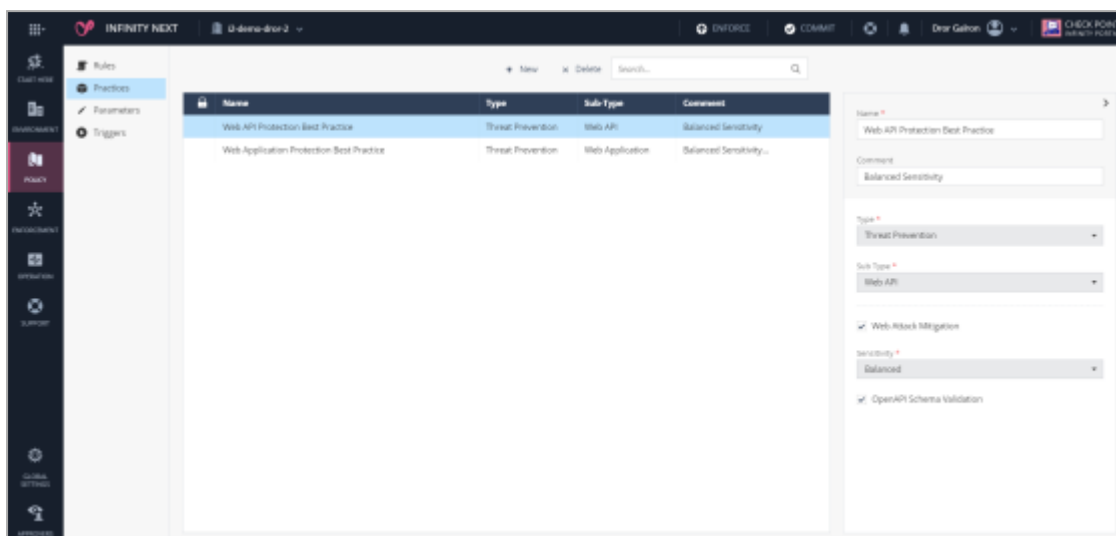
- Create an incoming/outgoing rule base, and assign each such rule base pair to an asset, an asset list, or a group of assets (Zone). The incoming and outgoing rule bases will use assets or asset zones to determine sources (for incoming) and destinations (for outgoing) to and from the matched assets
- or-
- When you define the assets' zones, define the connections and the direction of connections between each pair of zones. This is called the *adjacency configuration*. Then configure the system to apply this access policy on a group of assets (which is usually all the zones).

Defining Practices

A Practice is the general form of a security function. They specify the security services applied on asset(s). A practice means security logic is provided upon the rule's defined assets, and can result in actions as defined in the practice.

To create a new practice(s):

1. From the Navigation Toolbar, select **Policy > Practices**.



2. Select **New**. A window opens to define the new practice.

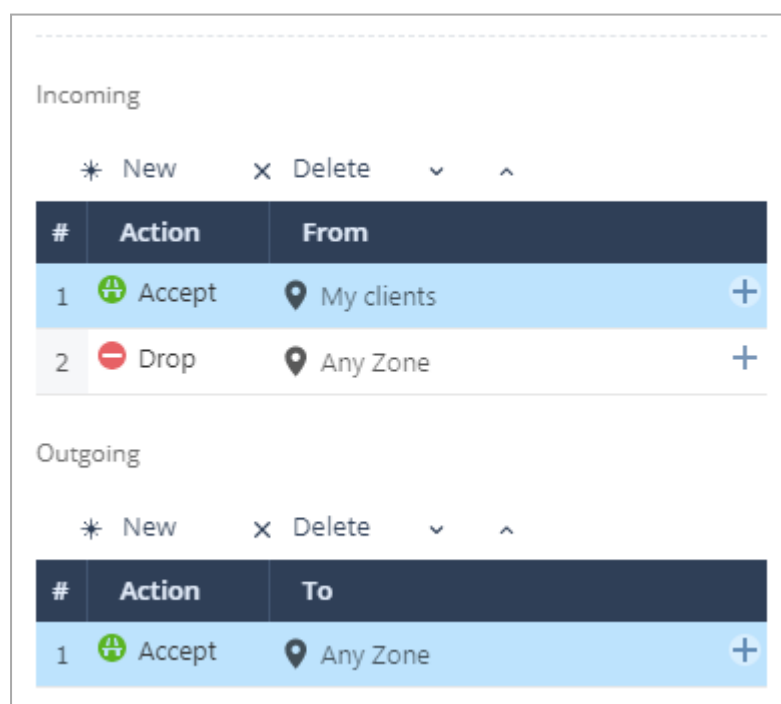
Incoming/Outgoing Access Control Practice

Provides a manual rule base for incoming traffic and outgoing traffic. The **Assets** column in a rule determines what is the destination matched for incoming rules and the source matched for outgoing rules.

In each rule that you define, the source zone (for incoming rules) and the destination zone (for outgoing rules) uses supported key:value pairs to define assets.

A *Zone* definition is explained in ["Zone configuration" on the next page](#). A *Zone* defines a group of assets, usually a dynamic group that uses a variety of properties that the system supports.

The rules are matched in order. The arrows above the rule base table change the order of the rules.



By Zone Access Control Practice

This practice, that enforces the access policy, is defined in the ["Zone configuration" below](#) for the matched assets in the rule. This means the entire access is based on zone object definition which includes the groups of assets (the Zones) defined by a query, and the defined connections between those groups (adjacency between zones).

Name *

My By Zone Access control practice

Comment

Type *

Access Control

Sub Type *

By Zone

The Zone Access Control Practices enforces these rules:

+

Accept

between adjacent zones

-

Block

between non-adjacent zones

+

Accept

within the same zone

Zone configuration

Zones are asset groups (usually dynamic asset groups). A Zone is defined by a logical query (that used AND/OR/NOT) of "key:value" pairs that use supported keys of asset properties that the system recognizes through various ways. Note - As Infinity Next continues to expand and support more environments, the number of supported keys is expected to increase and more asset inventories to draw data from.

To define zones:

1. Go to **Environment > Zones** page.
2. Click New, and enter the new Zone's name.
3. Create a Boolean query using AND/OR/NOT and key:value pairs. See list of supported key value pairs.

The screenshot displays a configuration window for 'My Servers'. It includes a 'Name' field with the value 'My Servers' and a 'Comment' field with the placeholder 'Add a comment...'. Below these is a 'Query' section with two conditions: 'ipAddress' set to '192.168.1.0/24' and 'port' set to '80', connected by an 'AND' operator. A plus sign icon indicates the ability to add more conditions. Under the 'Adjacent Zones' section, there is a table with columns 'Allow traffic' and 'Zone'. The first row shows 'From' in the 'Allow traffic' column and 'Any Zone' in the 'Zone' column. A plus sign icon and the text 'Add Adjacent Zone' are located below the table.

Name *

My Servers

Comment

Add a comment...

Query *

ipAddress 192.168.1.0/24

AND

port 80

+

Adjacent Zones

Allow traffic	Zone
From	Any Zone

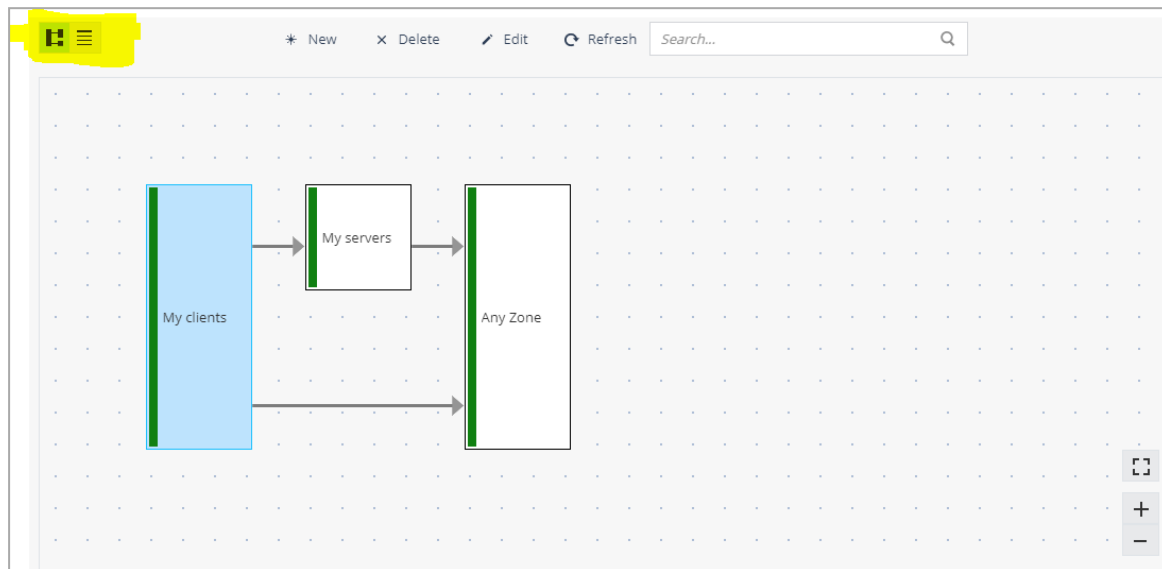
+

Add Adjacent Zone

4. If you plan to use the "By Zone Access Control" Practice:

- a. Define adjacent zones > click the plus sign at the bottom of the edit window.
- b. Define the adjacent zone and if traffic is allowed **From** it, **To** it, or if traffic can flow in a **Bidirectional** way between the two zones.

You can configure a difference access flow direction for each adjacent zone object. When you define an adjacency to another zone, this automatically creates the opposite definition in the other zone as well.



Note - To change to a graph view, click the top left button (highlighted). The graph is automatically created by the adjacency definition between the zones.



Important - Except for the predefined **Any Zone**, the zones' queries must create mutually exclusive groups of assets for the policy to be enforced correctly.

Supported Keys for Zone definition:

Note - This list is regularly updated. Make sure to read the latest documentation file for the most current list.

Supported Keys	Description	Allowed Values	Support dependency on additional configuration
<code>ipAddress</code>	The IP address of the asset/s in this zone	Single IPv4 IPv4 range (separated by '-') IPv4 network (CIDR format, e.g. "192.168.1.0/24") IPv6 single IP address and ranges in IPv6 format	No

Supported Keys	Description	Allowed Values	Support dependency on additional configuration
port	The ports used by this asset according to the context where the zone is configured. (If the zone is in the source of an "incoming" rule base, then the port is a source port, otherwise it is a destination port)	A valid port number (1-65535) A port range separated by '-'	No
ipProtocol	The IP protocol used by this asset	A valid IP protocol number (1-255)	No

Advanced Nano-Agent Configuration

After registration to the system, each Nano-Agent is associated with a Nano-Agent profile. Configuration of a Nano-Agent's profile object lets you control the Nano-Agents' settings associated with this profile.

Software Update Window

By default, the system is set to automatically and seamlessly update software and Nano-Agents. To update manually, or to set a specific schedule, go to **Agent Profile > Global > Agent Upgrade**.

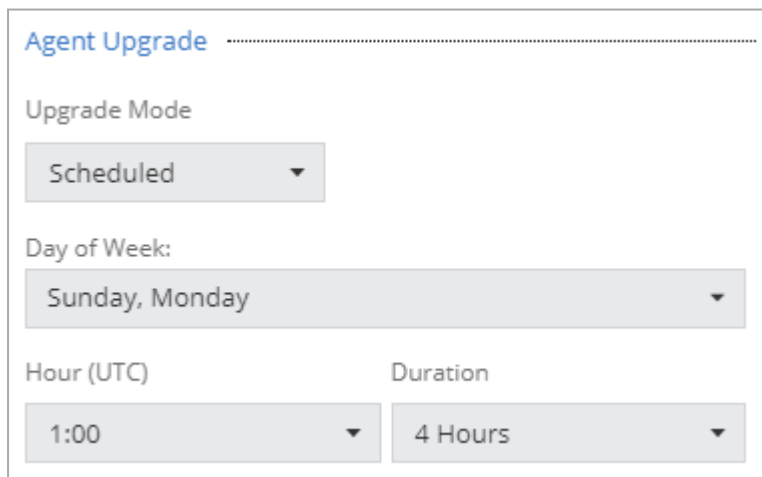
Note - The Nano-Agent can change its binaries if the policy changes and requires more components, or if the Nano-Agent's environment changes requires a different component version. The configuration of an upgrade time frame does not prevent such infrequent changes, as without them the system cannot operate. The time frame prevents an upgrade in the Nano-Agent component's version not included in the time frame.

The default mode is **Automatic**. This means that the upgrade occurs with the release of a new software.




The screenshot shows the 'Agent Upgrade' configuration window. The title 'Agent Upgrade' is at the top. Below it, the 'Upgrade Mode' is set to 'Automatic' in a dropdown menu.

The **Scheduled** allows you to define a time schedule which occurs periodically every week on a specific day(s), and that starts at a specific hour and lasts a defined duration of time



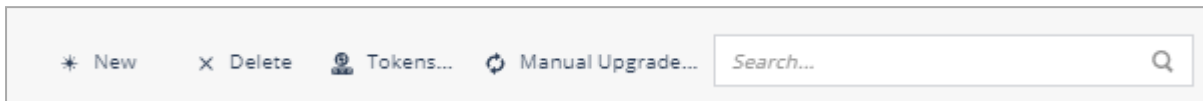
The screenshot shows the 'Agent Upgrade' configuration window with 'Upgrade Mode' set to 'Scheduled'. Below this, 'Day of Week' is set to 'Sunday, Monday'. 'Hour (UTC)' is set to '1:00' and 'Duration' is set to '4 Hours'.

Alternatively, change the option to Manual to stop automatic updates



The screenshot shows the 'Agent Upgrade' configuration window with 'Upgrade Mode' set to 'Manual' in a dropdown menu.

To allow all Nano-Agents in this profile to update to the latest version, select the requested profile and click **Manual Upgrade** at the top of the table. This choice is not recommended, as the system operates in continuous deployment of updates. If the Nano-Agent is not updated for a long period (three to four months), it is not supported. This choice gives you full control of the Nano-Agent's software component update events.



More Advanced Settings for Nano-Agents

The **Settings** tab allows you to configure advanced settings for a Nano-Agent.

The current optional keys that is used for support purposes and documented internally.

Troubleshooting

CP-NANO Tool

To connect to the agent with CLI, you must use the **cpnano** tool.

The connection gives agent details, such as the agent's status, settings, policy, and more.

In addition, use the **cpnano** tool to change the agent's configuration.

Syntax:

```
cpnano -s
cpnano {-ds | --display-settings}
cpnano --start-agent
cpnano --stop-agent
cpnano {-d | --debug} <Option>
cpnano {-gp | --set-gradual-policy} <Option>
```

Parameters

Description of Parameters

Parameter	Description
-s	Shows the agent status: <ul style="list-style-type: none">■ Path to all policy files■ Nano-Agent, Profile and Tenant ID■ Registration details■ Fog address■ Nano-Agent's policy version■ Nano-Agent's connectivity state■ Configuration update status, and last update attempt date and time■ Software update status, and last update attempt date and time■ Nano-Agent's service status (version and state)
-ds --display-settings	Shows the Nano-Agent complete configuration - settings, debug, and policy.
--start-agent	Starts the Nano-Agent.
--stop-agent	Stops the Nano-Agent.

Parameter	Description																
<code>-d <Option></code> <code>--debug <Option></code>	<p>Shows and configures the Nano-Agent debug settings.</p> <p>The options:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><code>--show</code></td><td>Shows the current debug configuration.</td></tr> <tr> <td><code>--show available-flags</code></td><td>Shows the available debug flags and debug levels.</td></tr> <tr> <td><code>--add [<Output Stream>]</code></td><td>Adds more debug configuration. This command does not change current debug configuration.</td></tr> <tr> <td><code>--set [<Output Stream>]</code></td><td>Changes the debug configuration. This command replaces the current debug configuration.</td></tr> <tr> <td><code>--delete [<Output Stream>]</code></td><td>Removes the current debug configuration.</td></tr> <tr> <td><code>--service <List of Nano Services></code></td><td>Specifies the Nano service, whose debug configuration to change.</td></tr> <tr> <td> <code>--flags</code> <code><Flag1=Level></code> <code>>,<Flag2=Level></code> <code>>,...,<FlagN=Level></code> </td><td>Specifies the list of debug flags and debug levels to configure.</td></tr> </table>	Option	Description	<code>--show</code>	Shows the current debug configuration.	<code>--show available-flags</code>	Shows the available debug flags and debug levels.	<code>--add [<Output Stream>]</code>	Adds more debug configuration. This command does not change current debug configuration.	<code>--set [<Output Stream>]</code>	Changes the debug configuration. This command replaces the current debug configuration.	<code>--delete [<Output Stream>]</code>	Removes the current debug configuration.	<code>--service <List of Nano Services></code>	Specifies the Nano service, whose debug configuration to change.	<code>--flags</code> <code><Flag1=Level></code> <code>>,<Flag2=Level></code> <code>>,...,<FlagN=Level></code>	Specifies the list of debug flags and debug levels to configure.
Option	Description																
<code>--show</code>	Shows the current debug configuration.																
<code>--show available-flags</code>	Shows the available debug flags and debug levels.																
<code>--add [<Output Stream>]</code>	Adds more debug configuration. This command does not change current debug configuration.																
<code>--set [<Output Stream>]</code>	Changes the debug configuration. This command replaces the current debug configuration.																
<code>--delete [<Output Stream>]</code>	Removes the current debug configuration.																
<code>--service <List of Nano Services></code>	Specifies the Nano service, whose debug configuration to change.																
<code>--flags</code> <code><Flag1=Level></code> <code>>,<Flag2=Level></code> <code>>,...,<FlagN=Level></code>	Specifies the list of debug flags and debug levels to configure.																
<code>-gp <Option></code> <code>--set-gradual-policy <Option></code>	<p>Configures a gradual policy (whitelist).</p> <p>The options:</p> <ul style="list-style-type: none"> ■ <code><List of IP strings or Range strings></code> ■ <code>{Access-Control HTTP-Manager} <List of IP strings or Range strings></code> 																

Agent Uninstall

To uninstall your Nano-Agent, you must use a special flag on the agent's installation package. After two - three seconds, all of the agent's content is removed from your system.

Note - There is not token replacement - when you uninstall an agent all the files are deleted. No change is needed.

To Uninstall the Agent on a Virtual Machine:

1. Start an SSH connection to the Virtual Machine, where the agent is installed.
2. Run the Egg installation file with the "`--uninstall`" flag.

To Uninstall the Agent in container environment:

1. Remove the Check Point container from your environment (and from your CI/CD).
2. Remove the Check Point NGINX attachment plugin.
 - Replace the Check Point provided NGINX container (if in use) and replace it with an official one.
 - If the attachment is an add-on to your modified NGINX container, then revert it back to the version - without Check Point content added to it.

To Uninstall the Agent in k8s environment:

1. Remove the Check Point container from your deployment yaml (and from your CI/CD).
2. Remove the Check Point NGINX attachment plugin with these steps:
 - a. If the attachment is an add-on to your modified NGINX container, then revert it back to the version - without Check Point content added to it.
 - b. If the attachment is an add-on to your modified NGINX container, revert it back to the version without Check Point content added to it.
 - c. From the NGINX configuration primary template, remove the command to install the attachment plugin.
 - d. From the NGINX site(s) configuration, remove the attachment activation annotations.

3. Delete the agent deployment, run:

```
kubectl delete <nginx ingress pod name>
```

4. Get the name of the volume mount claimed by the NGINX ingress deployment, run:

```
kubectl get persistentvolumeclaim
```

5. Delete the volume claim, run:

```
kubectl delete persistentvolumeclaim <volume claim name>
```

6. Apply the old/modified deployment YAML (the one that does not include the agent in it), run:

```
kubectl apply -f <path to the deployment yaml without the agent>
```

7. Monitor the deployment and make sure the NGINX ingress pod starts, run:

```
kubectl get pods
```

8. Make sure that **only** the NGINX container is part of the pod, run:

```
kubectl describe <name of the nginx ingress pod>
```

Support

If the troubleshooting tools have not provided an answer and the product does not behave as you expect it, contact Check Point's Infinity Next support:

infinity-next-support@checkpoint.com

Product Evaluation and Licensing

When activating the Infinity Next application from the Infinity Portal, you can evaluate the WAAP capabilities as explained in this documentation.

After you finished the evaluation, contact Check Point sales to inquire about a license purchase for use in your environment.

Check Point Copyright Notice

© 2020 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c) (1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.