Configure Umbrella with Check Point Anti-Bot Software Blade

Contents

Introduction

This document describes how to Integrate Cisco Umbrella with Check Point Anti-Bot Software Blade.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- A Check Point device with the Anti-Bot Software Blade
- Check Point software version R80.40 or higher
- Ensure the Check Point device can make outbound HTTP requests to "https://s-platform.api.opendns.com".
- A Cisco Umbrella package like DNS Essentials, DNS Advantage, SIG Essentials, or SIG Advantage

- Cisco Umbrella Dashboard administrative rights

Note: The Check Point integration is included only in Cisco Umbrella packages like DNS Essentials, DNS Advantage, SIG Essentials, or SIG Advantage. If you do not have one of these packages and would like to have the Check Point integration, please contact your Cisco Umbrella Account Manager. If you have the correct Cisco Umbrella package but do not see Check Point as an integration for your dashboard, please contact Cisco Umbrella Support.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

The Cisco Umbrella integration with Check Point Anti-Bot Software Blade enables a Check Point device to send its Anti-Bot Software Blade alerts to Cisco Umbrella when the Blade discovers threats in the network traffic it inspects. Alerts received by Cisco Umbrella build a block list that can protect roaming laptops, tablets, and phoneson networks not protected by the Check Point Anti-Bot Software Blade.

This article provides instructions to configure a Check Point device to send Anti-Bot Software Blade alerts to Cisco Umbrella.

Note: This integration was deprecated by Check Point in version R81.20 after it was initially released in R80.40.

Functionality

The Cisco Umbrella integration with the Check Point Anti-Bot Software Blade appliance pushes threats that it has found (for example, domains that host malware, command and control for botnets, or phishing sites) to Cisco Umbrella for global enforcement.

Cisco Umbrella then validates the threat to ensure it can be added to a policy. If the information from the Check Point Anti-Bot Software Blade is confirmed to be a threat, the domain address is added to the Check

Point Destination List as part of a security setting that can be applied to any Cisco Umbrella policy. That policy is immediately applied to any requests made from devices assigned to that policy.

Going forward, Cisco Umbrella automatically parses Check Point alerts and adds malicious sites to the Check Point Destination List. This extends Check Point protection to all remote users and devices and provides another layer of enforcement to your corporate network.

Configuration Steps

Configuring the integration involves these steps:

1. Enable the integration in Cisco Umbrella to generate an API token with a custom script.
2. Deploy the API token and custom script on the Check Point appliance.
3. Build/Edit a Check Point alert to post to this new script.
4. Set Check Point events to be blocked within Cisco Umbrella.

Prevent Service Interruptions

To avoid unwanted service interruptions, Cisco Umbrella recommends adding mission-critical domain names that can never be blocked (for example, google.com or salesforce.com) to the Global Allow List (or other destination lists as per your policy) prior to configuring the integration.

Mission-critical domains can include:

- The home page for your organization
- Domains representing services you provide that can have both internal and external records. For example, "mail.myservicedomain.com" and "portal.myotherservicedomain.com".
- Lesser-known cloud-based applications that you depend on that Cisco Umbrella cannot include in automatic domain validation. For example, "localcloudservice.com".

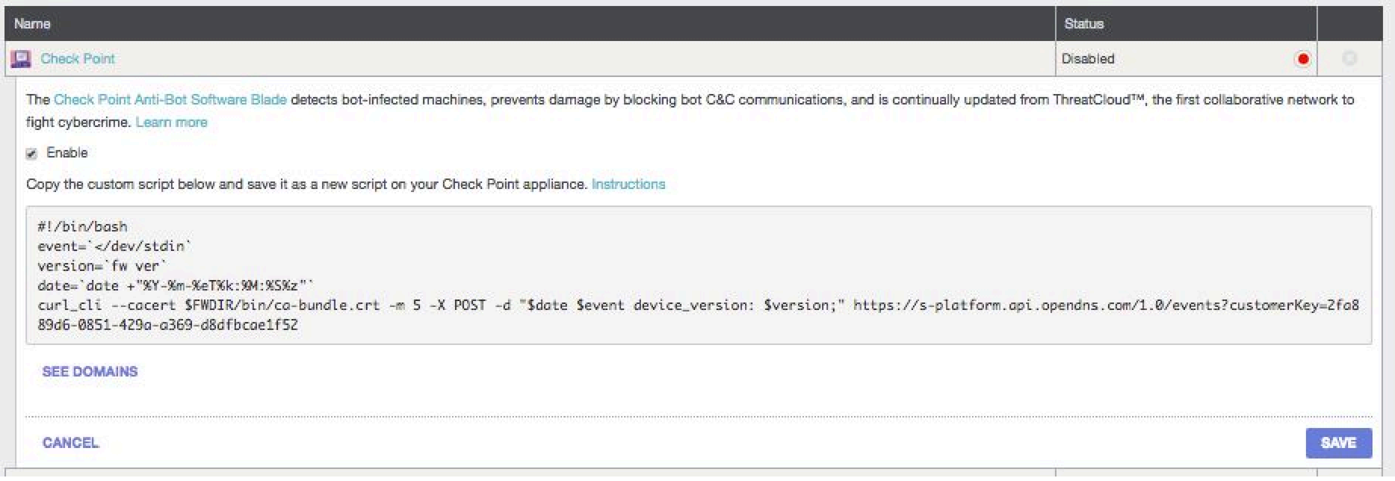
These domains must be added to the Global Allow List, which is found under **Policies > Destination Lists** in Cisco Umbrella.

Step 1: Umbrella Script and API Token Generation

1. Log into the Cisco Umbrella Dashboard as an Administrator.

2. Navigate to **Policies > Policy Components > Integrations** and select **Check Point** in the table to expand it.

3. Select the **Enable** option.



The Check Point Anti-Bot Software Blade detects bot-infected machines, prevents damage by blocking bot C&C communications, and is continually updated from ThreatCloud™, the first collaborative network to fight cybercrime. Learn more

☑ Enable

Copy the custom script below and save it as a new script on your Check Point appliance. Instructions

```
#!/bin/bash
event=`</dev/stdin`
version=`fw ver`
date=`date +"%Y-%m-%eT%k:%M:%S%z"`
curl_cli --cacert $FWDIR/bin/ca-bundle.crt -m 5 -X POST -d "$date $event device_version: $version;" https://s-platform.api.opendns.com/1.0/events?customerKey=2fa8
89d6-0851-429a-a369-d8dfbcae1f52
```

4. Copy the entire script, starting from the line with:

```
#!/bin/bash
```

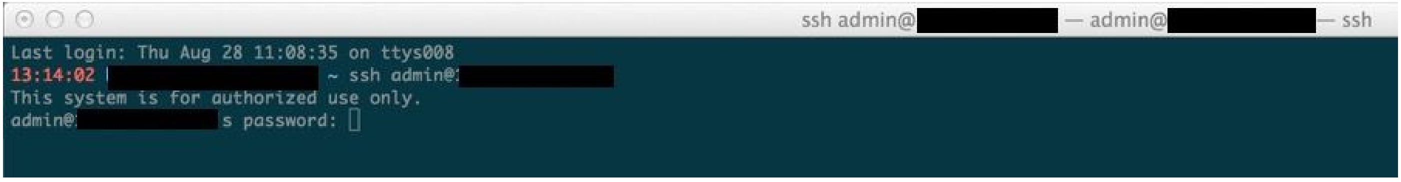
You can then use the script in later steps.

5. Select **Save** to enable the integration.

Step 2: Deploy the Custom Script on the Check Point Appliance

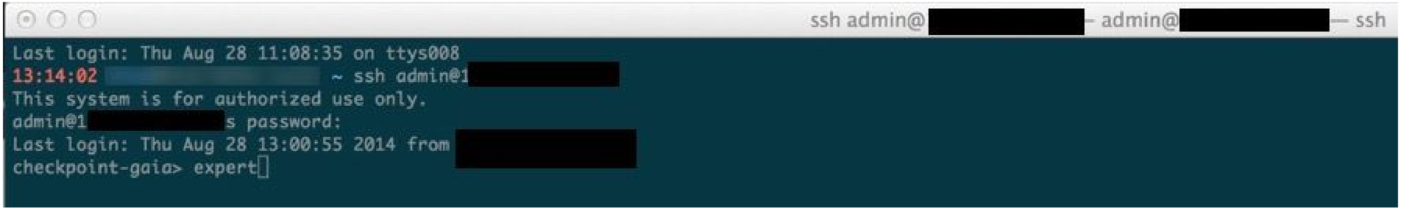
The next steps are to install the custom Cisco Umbrella script on your Check Point appliance, and then enable it in the SmartDashboard.

1. To install the custom script, SSH into the Check Point Appliance as an admin:



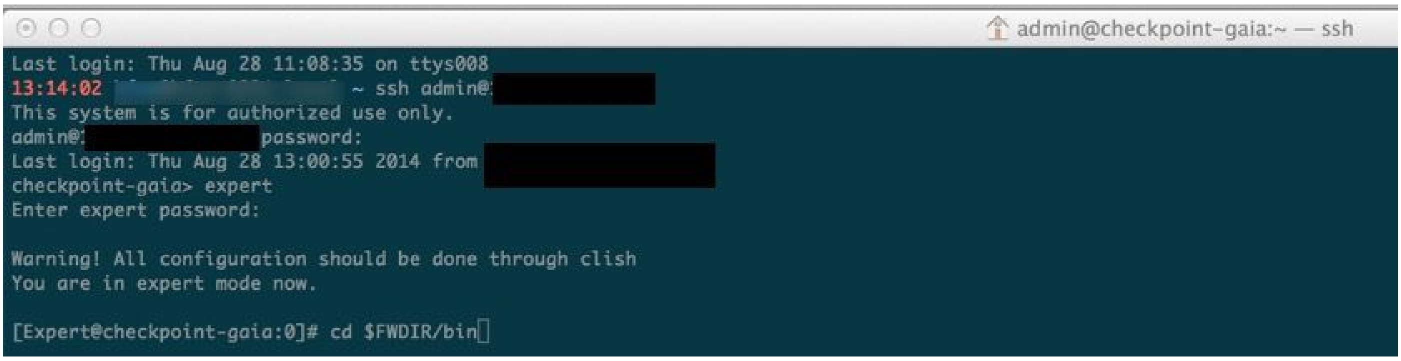
```
Last login: Thu Aug 28 11:08:35 on ttys008
13:14:02 [redacted] ~ ssh admin@[redacted]
This system is for authorized use only.
admin@[redacted]s password:
```

2. Next, launch "Expert Mode" by typing "expert" in the command line:



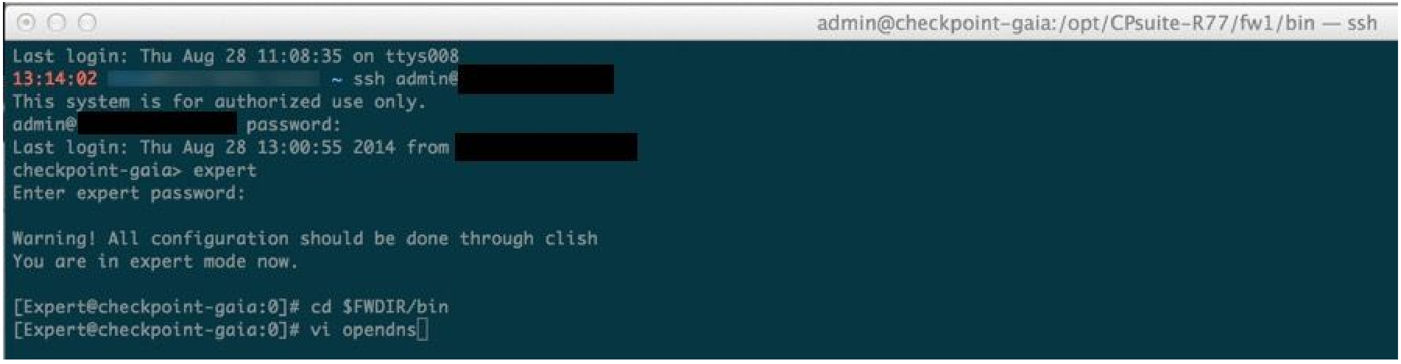
```
Last login: Thu Aug 28 11:08:35 on ttys008
13:14:02 [redacted] ~ ssh admin@1[redacted]
This system is for authorized use only.
admin@1[redacted]s password:
Last login: Thu Aug 28 13:00:55 2014 from [redacted]
checkpoint-gaia> expert
```

3. Change the working directory to `$FWDIR/bin`:



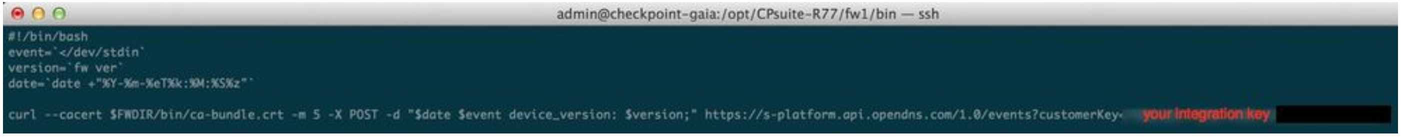
```
Last login: Thu Aug 28 11:08:35 on ttys008
13:14:02 [redacted] ~ ssh admin@[redacted]
This system is for authorized use only.
admin@[redacted]password:
Last login: Thu Aug 28 13:00:55 2014 from [redacted]
checkpoint-gaia> expert
Enter expert password:

Warning! All configuration should be done through clish
You are in expert mode now.

[Expert@checkpoint-gaia:0]# cd $FWDIR/bin
```

4. Open a new file named "opendns" using a text editor (like in the example here using the "vi" editor):



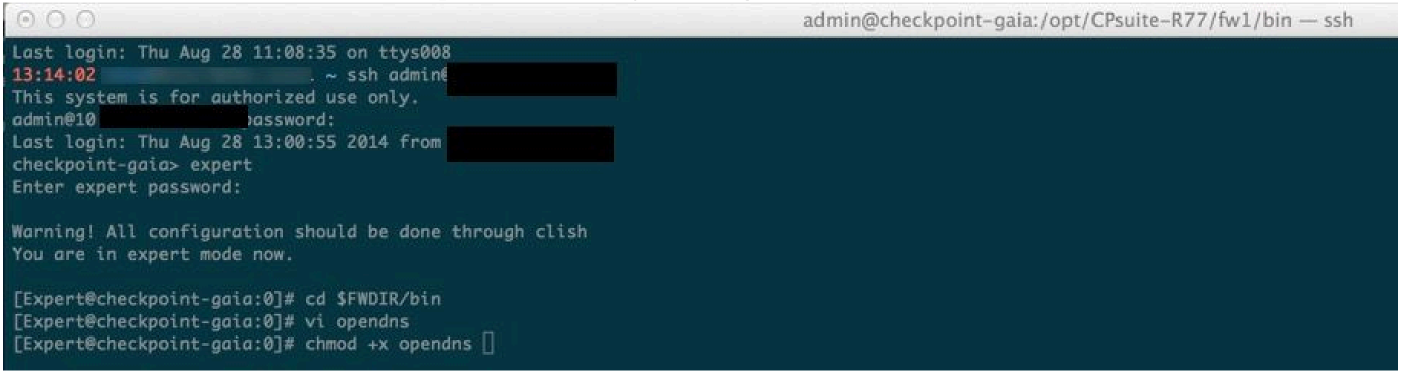
```
Last login: Thu Aug 28 11:08:35 on ttys008
13:14:02 [redacted] ~ ssh admin@[redacted]
This system is for authorized use only.
admin@[redacted] password:
Last login: Thu Aug 28 13:00:55 2014 from [redacted]
checkpoint-gaia> expert
Enter expert password:

Warning! All configuration should be done through clish
You are in expert mode now.

[Expert@checkpoint-gaia:0]# cd $FWDIR/bin
[Expert@checkpoint-gaia:0]# vi opendns
```

5. Paste the Cisco Umbrella script into the file, then save the file and exit your editor:



```
#!/bin/bash
event=`</dev/stdin`
version=`fw ver`
date=`date +"%Y-%m-%eT%k:%M:%S%z"`

curl --cacert $FWDIR/bin/ca-bundle.crt -m 5 -X POST -d "$date $event device_version: $version;" https://s-platform.api.opendns.com/1.0/events?customerKey= your integration key [redacted]
```

6. Make the custom Umbrella script executable by running `chmod +x opendns` :

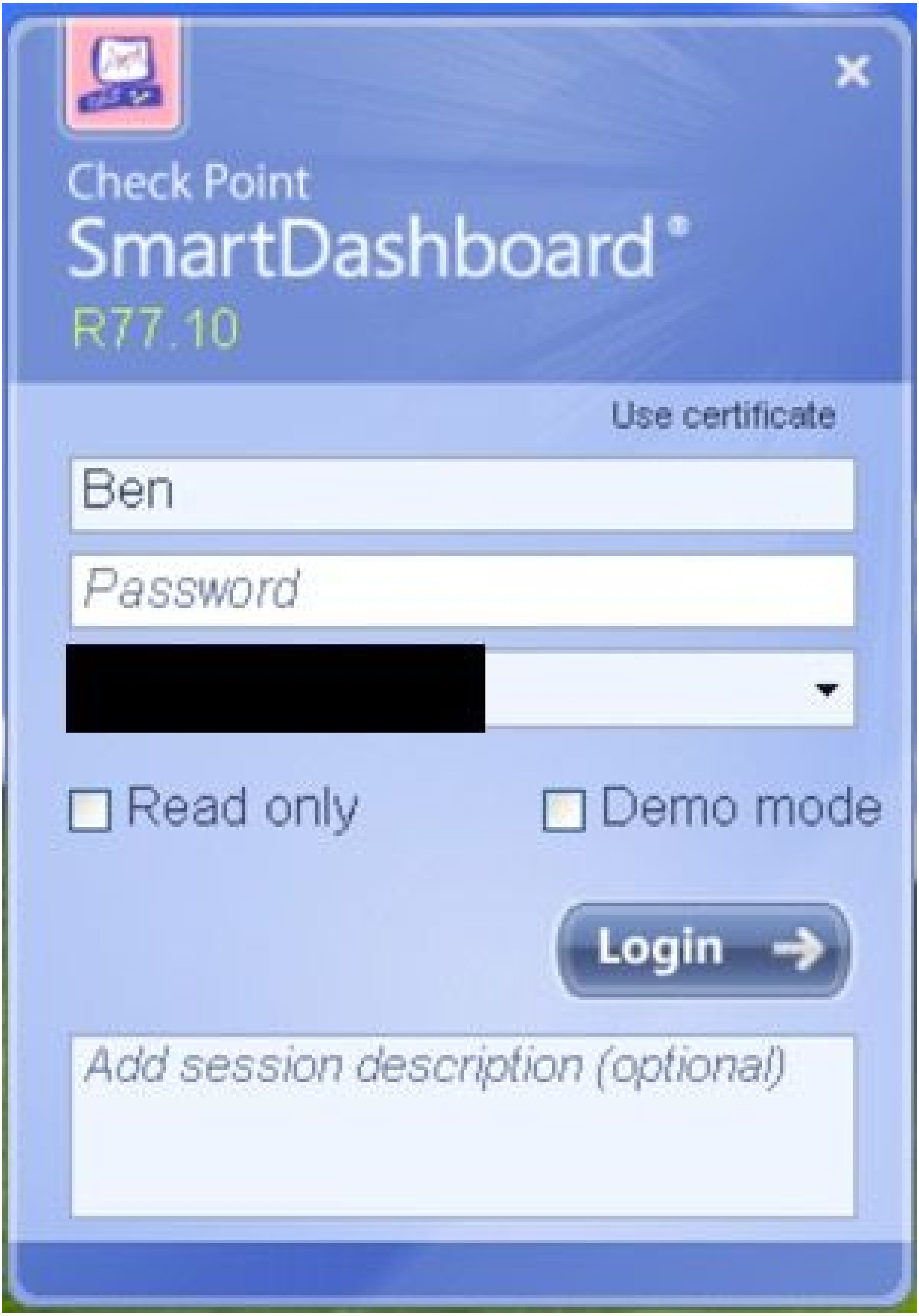


```
Last login: Thu Aug 28 11:08:35 on ttys008
13:14:02 [redacted] ~ ssh admin@[redacted]
This system is for authorized use only.
admin@10[redacted]password:
Last login: Thu Aug 28 13:00:55 2014 from [redacted]
checkpoint-gaia> expert
Enter expert password:

Warning! All configuration should be done through clish
You are in expert mode now.

[Expert@checkpoint-gaia:0]# cd $FWDIR/bin
[Expert@checkpoint-gaia:0]# vi opendns
[Expert@checkpoint-gaia:0]# chmod +x opendns
```

Note: If you upgrade or change Blade versions, then you must repeat these steps on that new version.

Step 3. Build or Edit a Check Point Alert to Post to the New Script

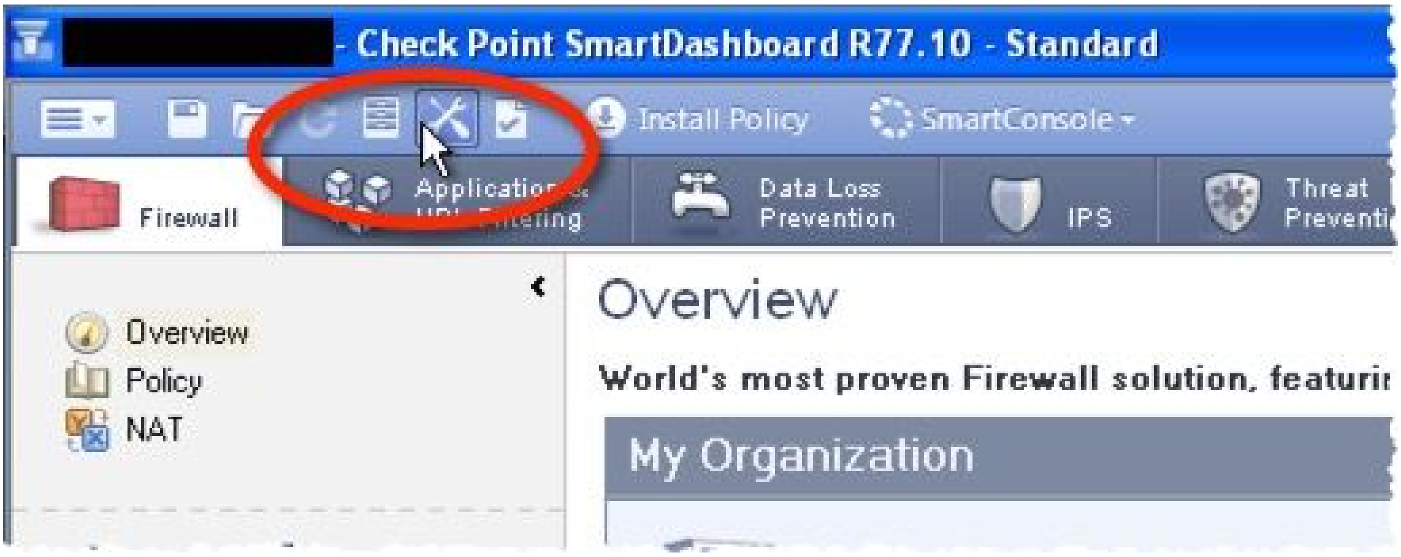
1. Enable the SmartDashboard to post the new script by logging in and launching the SmartDashboard:



Ben

[redacted]

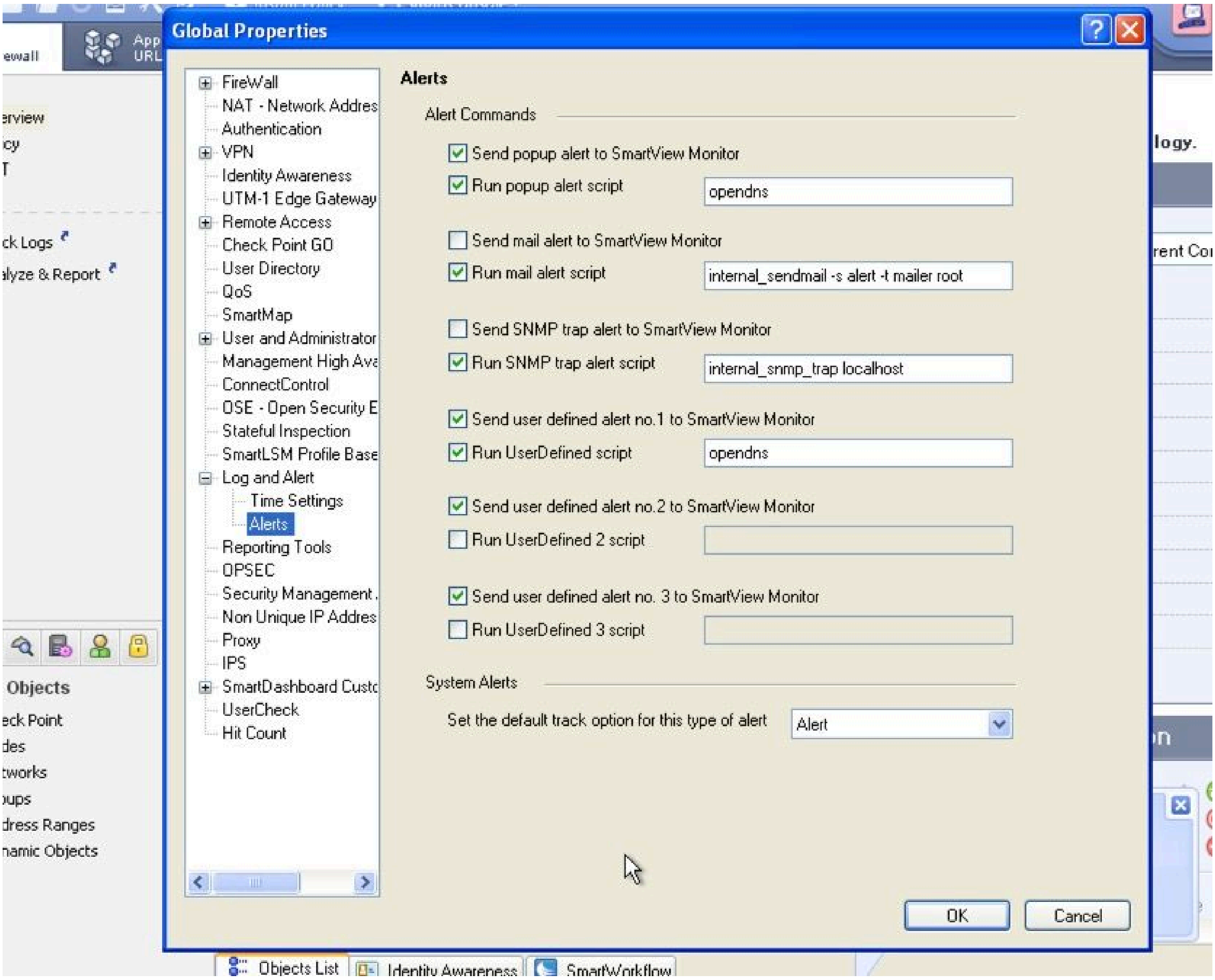
2. Open **Global Properties**:


[redacted] - Check Point SmartDashboard R77.10 - Standard
Install Policy
SmartConsole
Firewall
Application URL Filtering
Data Loss Prevention
IPS
Threat Preventi
Overview
Policy
NAT
Overview
World's most proven Firewall solution, featuri
My Organization

3. Within **Global Properties**, open **Log and Alert > Alerts** and complete these steps:

- Select **Send popup alertscript** and **Run UserDefined script**.
- Define "opendns" in the script fields for both.

4. Select **OK**. From SmartDashboard, save and install your updated policy.



Alerts

Alert Commands

☑ Send popup alert to SmartView Monitor

☑ Run popup alert script: opendns

□ Send mail alert to SmartView Monitor

☑ Run mail alert script: internal_sendmail -s alert -t mailer root

□ Send SNMP trap alert to SmartView Monitor

☑ Run SNMP trap alert script: internal_snmp_trap localhost

☑ Send user defined alert no.1 to SmartView Monitor

☑ Run UserDefined script: opendns

☑ Send user defined alert no.2 to SmartView Monitor

□ Run UserDefined 2 script

☑ Send user defined alert no. 3 to SmartView Monitor

□ Run UserDefined 3 script

System Alerts

Set the default track option for this type of alert: Alert

Step 4: Testing the Integration and Setting Check Point Events to be Blocked

First, generate a test anti-bot blade event to appear in the Cisco Umbrella Dashboard:

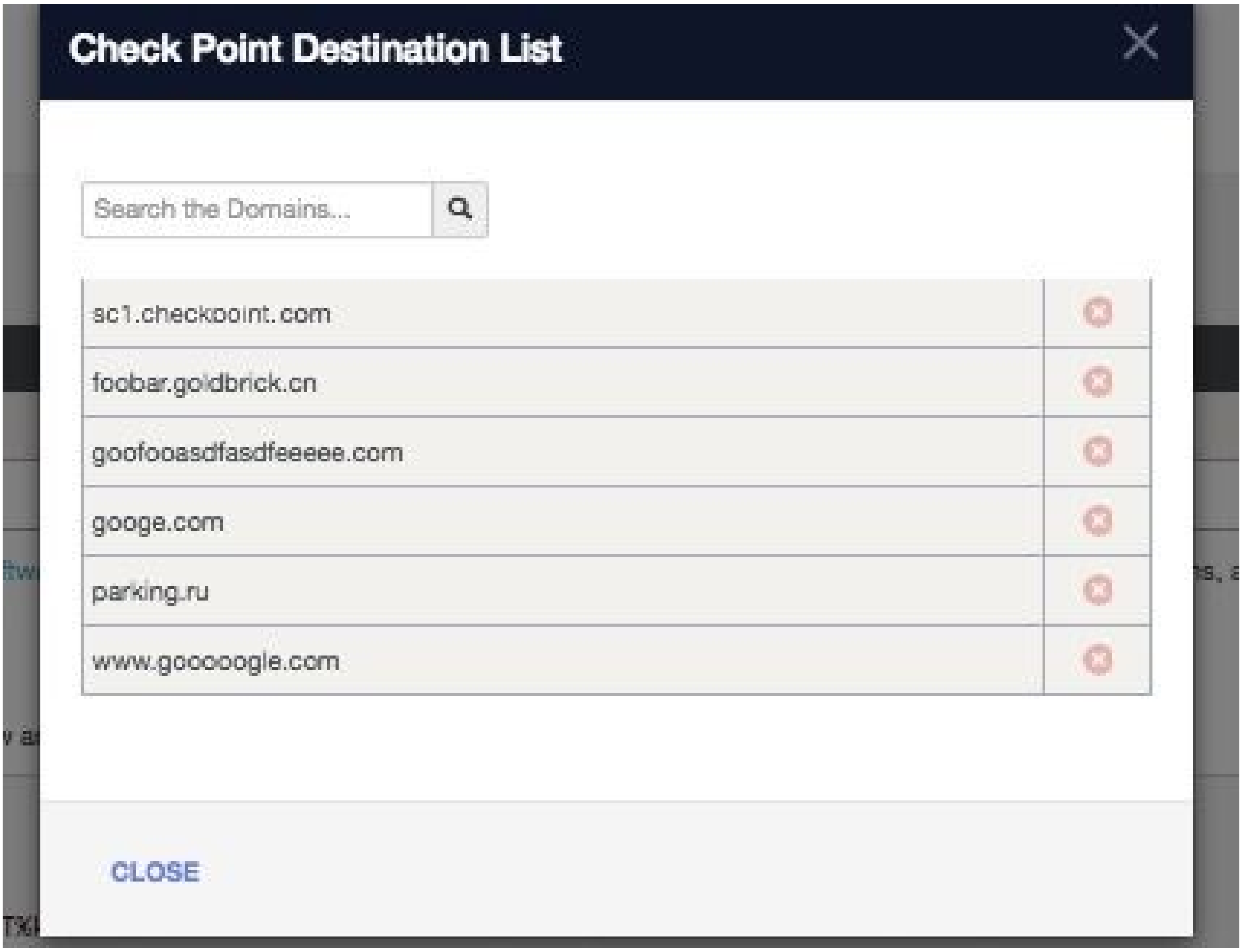
1. From any device on the network protected by your Check Point appliance, load this URL in your browser:

```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

2. Log into the Cisco Umbrella dashboard as an administrator.

3. Navigate to **Policies** > **Policy Components** > **Integrations** and select **Check Point** in the table to expand it.

4. Select **See Domains**. This opens a window displaying the Check Point Destination List that can include "sc1.checkpoint.com." From that point on, a searchable list begins to be populated and grow.



sc1.checkpoint.com

foobar.goldbrick.cn

goofooasdfasdfeeeee.com

googe.com

parking.ru

www.gooooogle.com

Note: You can also alter this destination list if there is a domain appearing here that you do not wish to enforce policy on. Select the **Delete** icon to remove the domain.

Observing Events Added to the Check Point Security Category in "Audit Mode"

The next step is to observe and audit the events added to your new Check Point security category.

The events from your Check Point appliance begin to populate a specific destination list that can be applied to policies as a Check Point security category. By default, the destination list and the security category are in "audit mode" and are not applied to any policies and cannot result in any change to your existing Cisco Umbrella policies.

Note: "Audit mode" can be enabled for however long is necessary based on your deployment profile and network configuration.

Review Destination List

You can review the Check Point Destination List at any time in Cisco Umbrella:

1. Navigate to **Policies > Policy Components > Integrations**.

2. Expand **Check Point** in the table and select **See Domains**.

Review Security Settings for a Policy

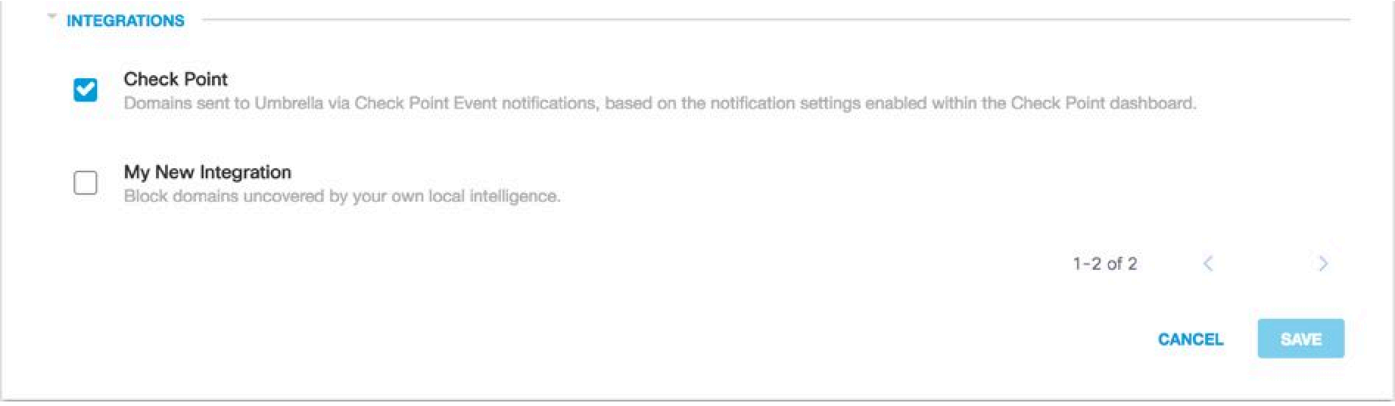
You can review the security settings that can be enabled for a policy at any time in Cisco Umbrella:

1. Navigate to **Policies > Policy Components > Security Settings**.

2. Select a security setting in the table to expand it.

3. Scroll to the **Integrations** section and expand the section to display the Check Point integration.

4. Select the option for the **Check Point** integration, then select **Save**.



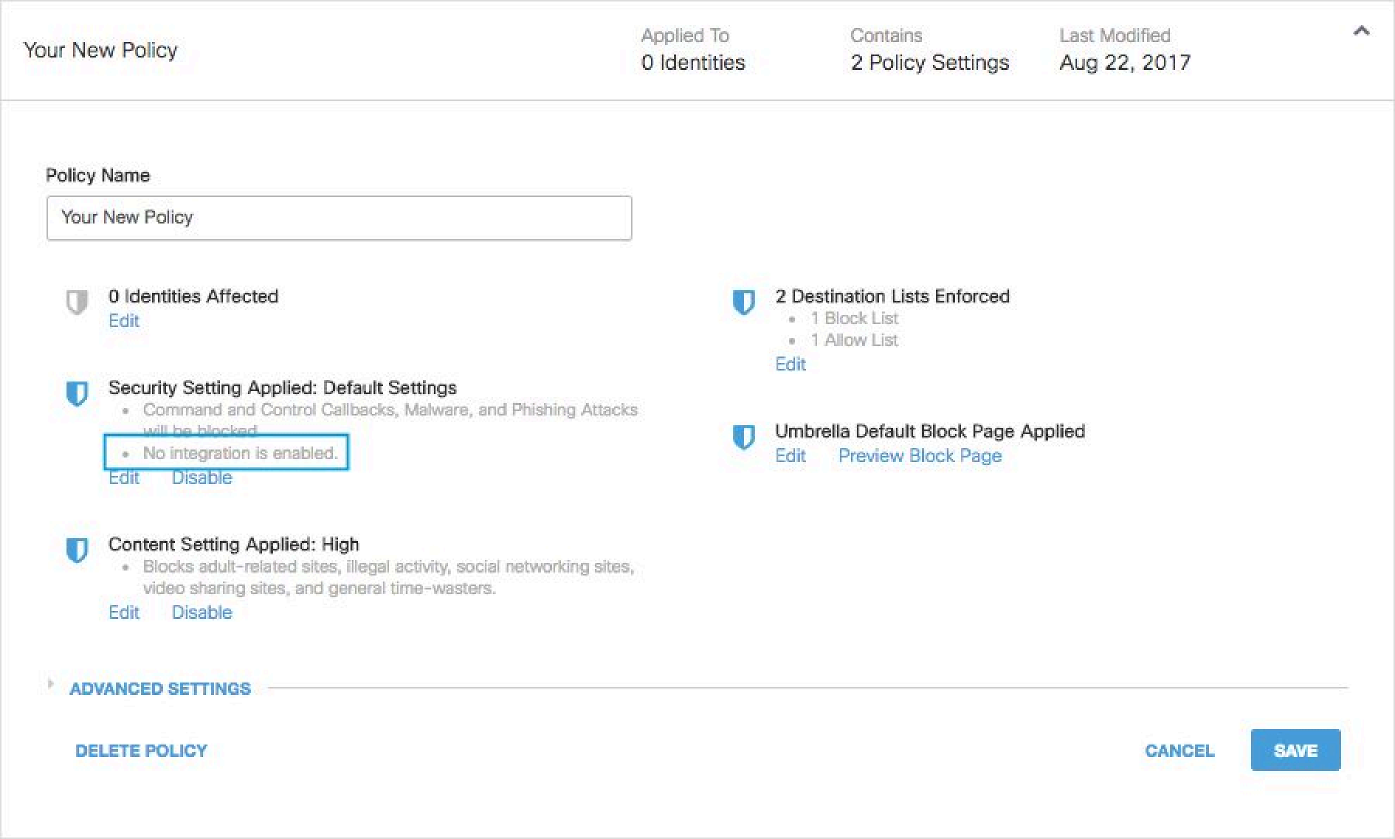
INTEGRATIONS

☑ Check Point
Domains sent to Umbrella via Check Point Event notifications, based on the notification settings enabled within the Check Point dashboard.

□ My New Integration
Block domains uncovered by your own local intelligence.

115013984226

You can also review integration information through the **Security Settings Summary** page:



Your New Policy	Applied To 0 Identities	Contains 2 Policy Settings	Last Modified Aug 22, 2017

Policy Name: Your New Policy

0 Identities Affected
Edit

Security Setting Applied: Default Settings
- Command and Control Callbacks, Malware, and Phishing Attacks will be blocked.
- No integration is enabled.

Edit Disable

Content Setting Applied: High
- Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

Edit Disable

2 Destination Lists Enforced
- 1 Block List
- 1 Allow List

Edit

Umbrella Default Block Page Applied
Edit Preview Block Page

19916943300244

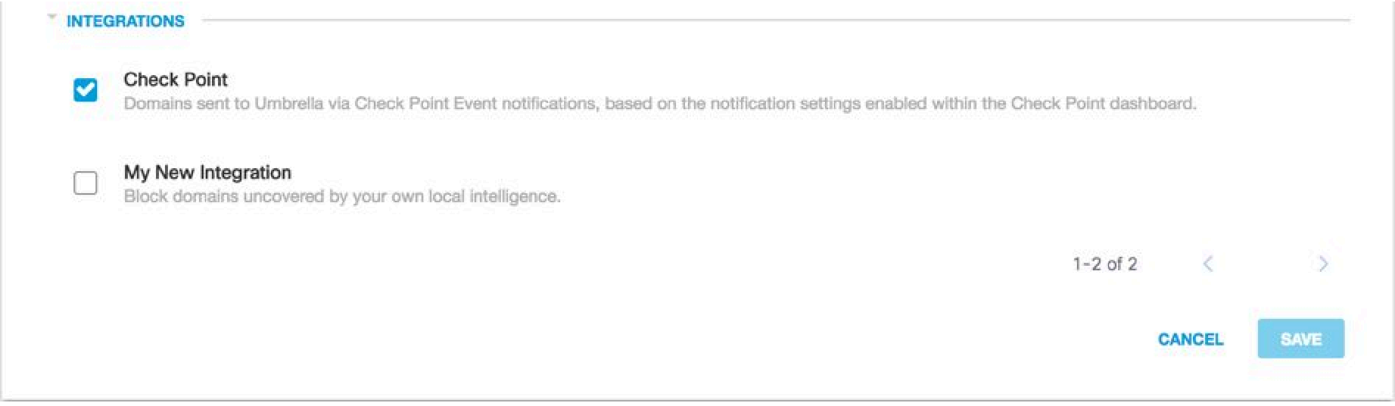
Applying the Check Point Security Settings in "Block Mode" to a Policy for Managed Clients

Once you are ready to have these additional security threats enforced by clients managed by Cisco

Umbrella, change the security setting on an existing policy or create a new policy that sits above your default policy to ensure that it is enforced first:

1. Ensure that the Check Point integration is still enabled as done in the previous section. Navigate to **Policies > Policy Components > Security Settings** and open the relevant setting.

2. Under **Integrations**, verify that the **Check Point** option is selected. If not, select the option and select **Save**.



INTEGRATIONS

☑ Check Point
Domains sent to Umbrella via Check Point Event notifications, based on the notification settings enabled within the Check Point dashboard.

□ My New Integration
Block domains uncovered by your own local intelligence.

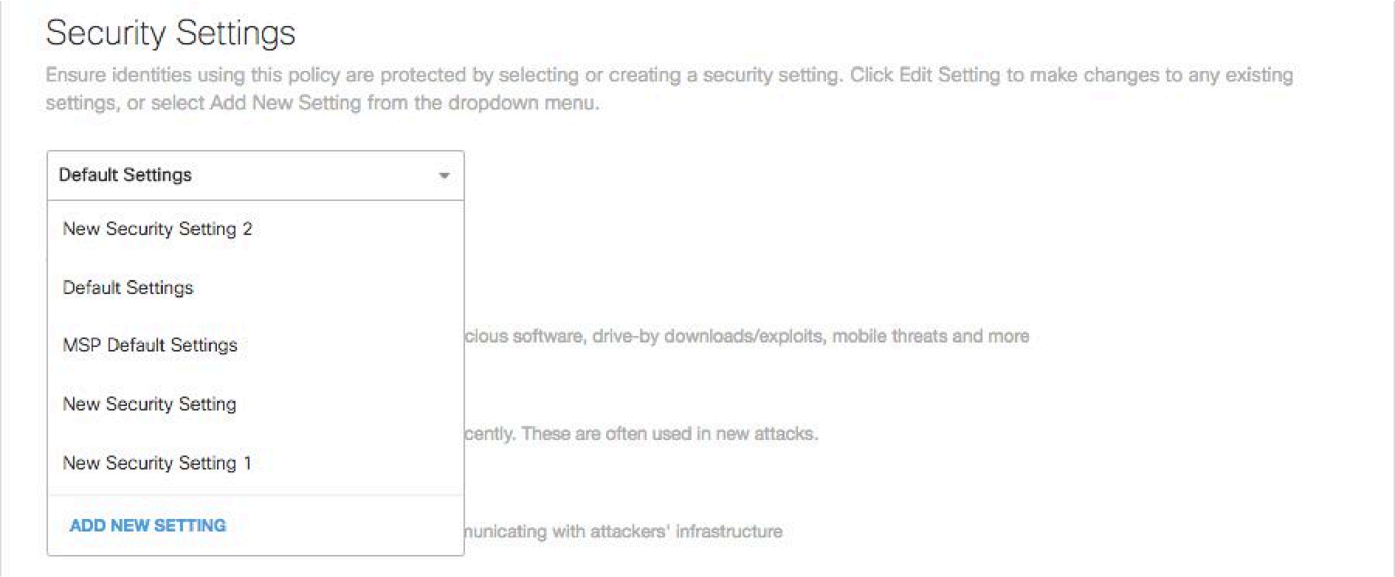
115013984226

Next, in the Cisco Umbrella Policy wizard, add this security setting to a policy that you are editing:

1. Navigate to a policy: either **Policies > DNS Policies** or **Policies > Web Policy**.

2. Expand a policy and under **Security Setting Applied** (DNS Policies) or **Security Settings** (Web Policy), then select **Edit**.

3. In the **Security Settings** dropdown, select a security setting that includes the Check Point setting.



Security Settings

Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

Default Settings

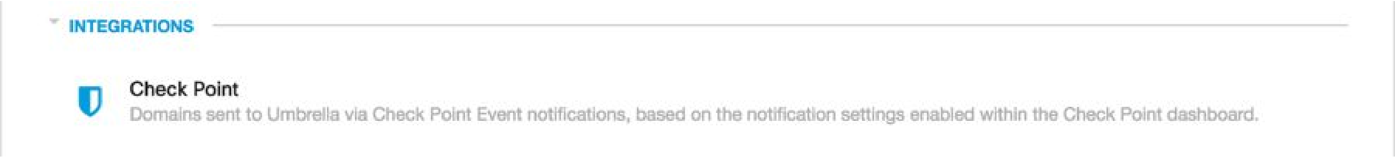
cious software, drive-by downloads/exploits, mobile threats and more

cently. These are often used in new attacks.

nunicating with attackers' infrastructure

19916943316884

The shield icon under Integrations updates to blue.


INTEGRATIONS

Check Point

Domains sent to Umbrella via Check Point Event notifications, based on the notification settings enabled within the Check Point dashboard.

115014149783

4. Select **Set & Return** (DNS Policies) or **Save** (Web Policy).

Check Point domains contained within the security setting for Check Point can then be blocked for those identities using the policy.

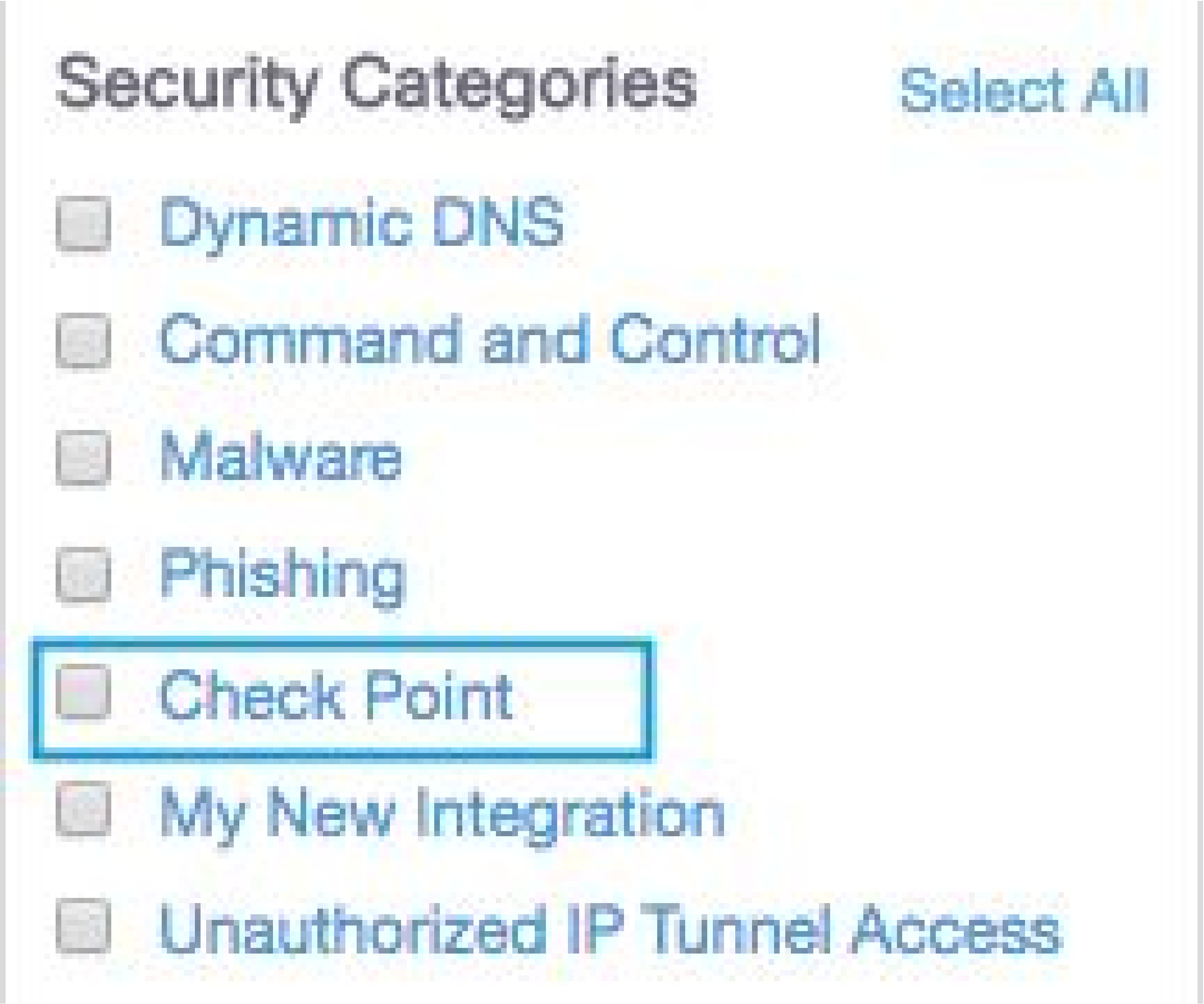
Reporting within Umbrella for Check Point Events

Reporting on Check Point Security Events

The Check Point Destination List is one of the security categories available for reports. Most or all of the reports use the Security Categories as a filter. For instance, you can filter security categories to only show Check Point-related activity:

1. Navigate to **Reporting** > **Core Reports** > **Activity Search**.

2. Under **Security Categories**, select **Check Point** to filter the report to only show the security category for Check Point.



Security Categories

Select All

□ Dynamic DNS

□ Command and Control

□ Malware

□ Phishing

□ Check Point

□ My New Integration

□ Unauthorized IP Tunnel Access

115014197623

Note: If the Check Point integration is disabled, it cannot appear in the Security Categories filter.

3. Select **Apply** to see Check Point-related activity for the period selected in the report.

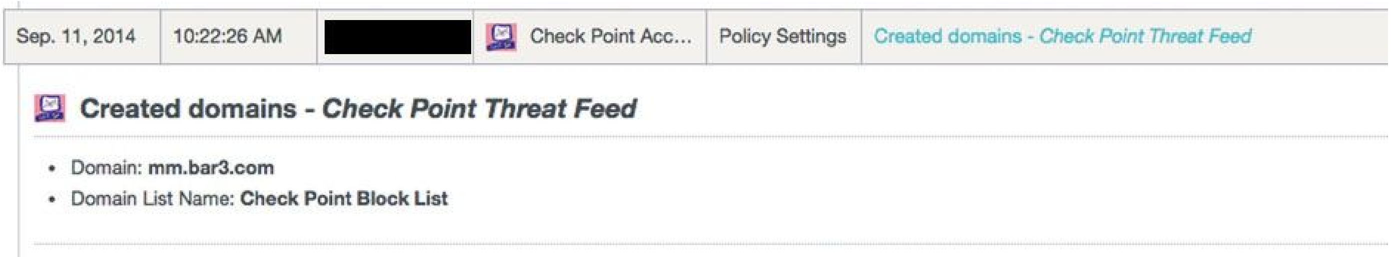
Reporting when Domains Were Added to the Check Point Destination List

The Cisco Umbrella Admin Audit log includes events from the Check Point appliance as it adds domains to the destination list. These domains appear to be added by a "Check Point account" label, under the **User** column of the Audit log.

To find the Umbrella Admin Audit log, navigate to **Reporting > Admin Audit Log**.

To report on when a domain was added, filter to only include Check Point changes by applying a **Filter by Identities & Settings** filter for the **Check Point Block List.**

Once you run the report, you can see a list of domains added to the Check Point destination list.



Sep. 11, 2014	10:22:26 AM	[redacted]	Check Point Acc...	Policy Settings	Created domains - *Check Point Threat Feed*

Created domains - *Check Point Threat Feed*

- Domain: **mm.bar3.com**
- Domain List Name: **Check Point Block List**

Handling Unwanted Detections or False Positives

Managing an Allow List for Unwanted Detection

Although unlikely, it is possible that domains added automatically by your Check Point appliance can trigger an unwanted block that can cause your users to be blocked from accessing particular websites. In a situation like this, Cisco Umbrella recommends adding the domain(s) to an allow list, which takes precedence over all other types of block lists, including Security Settings. An allow list takes precedence over a block list when a domain is present in both.

There are two reasons why this approach is preferred:

- First, in case the Check Point appliance was to re-add the domain again after it was removed, the allow list safeguards against this causing further issues.
- Second, the allow list shows a historical record of problematic domains for later forensics or audit reports.

By default, there is a Global Allow List that is applied to all policies. Adding a domain to the Global Allow List results in the domain being allowed in all policies.

If the Check Point Security Setting in Block mode is only applied to a subset of your managed Cisco Umbrella identities (for instance, it is only applied to roaming computers and mobile devices), you can create a specific allow list for those identities or policies.

To create an allow list:

1. Navigate to **Policies > Destination Lists,** and select the **Add** icon.

2. Select **Allow**, and add your domain to the list.

3. Select **Save**.

Once the list has been saved, you can add it to an existing policy covering those clients that have been affected by the unwanted block.

Deleting Domains from the Check Point Destination List

Next to each domain name in the Check Point destination list is a **Delete** icon. Deleting domains lets you clean up the Check Point destination list in the event of unwanted detection.

However, the delete **is not** permanent if the Check Point appliance resends the domain to Cisco Umbrella.

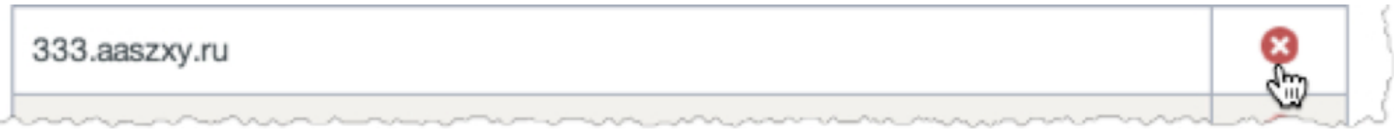
To delete a domain:

1. Navigate to **Settings > Integrations**, then select **Check Point** to expand it.

2. Select **See Domains.**

3. Search for the domain name you want to delete.

4. Select the **Delete** icon.



333.aaszxy.ru

5. Select **Close**.

6. Select **Save**.

If an unwanted detection or false positive, Cisco Umbrella recommends creating an allow list in Cisco Umbrella immediately and then remediating the false positive within the Check Point Appliance. Later, you can remove the domain from the Check Point destination list.