使用Check Point Anti-Bot Software Blade配置Umbrella

目录

简介

本文档介绍如何将Cisco Umbrella与Check Point Anti-Bot Software Blade集成。

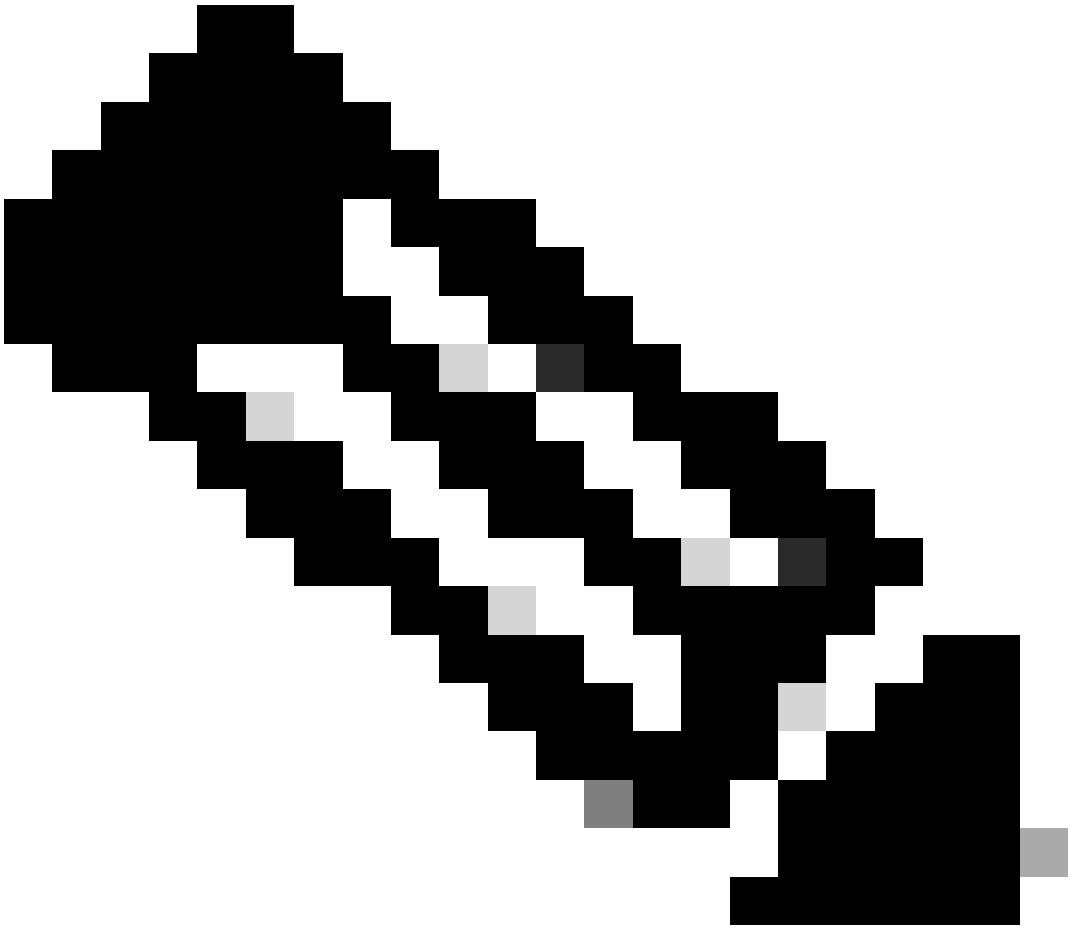
先决条件

要求

Cisco 建议您了解以下主题：

- 具有防僵尸软件刀片的检查点设备
- Check Point软件版本R80.40或更高版本
- 确保Check Point设备可以向“https://s-platform.api.opendns.com”发出出站HTTP请求。

- Cisco Umbrella软件包，如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage
- Cisco Umbrella Dashboard管理权限



注意：Check Point集成仅包含在Cisco Umbrella包中，如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage。如果您没有这些软件包之一，并且希望集成Check Point，请联系您的思科Umbrella客户经理。如果您有正确的Cisco Umbrella软件包，但是没有将Check Point视为控制面板集成，请与Cisco Umbrella支持联系。

使用的组件

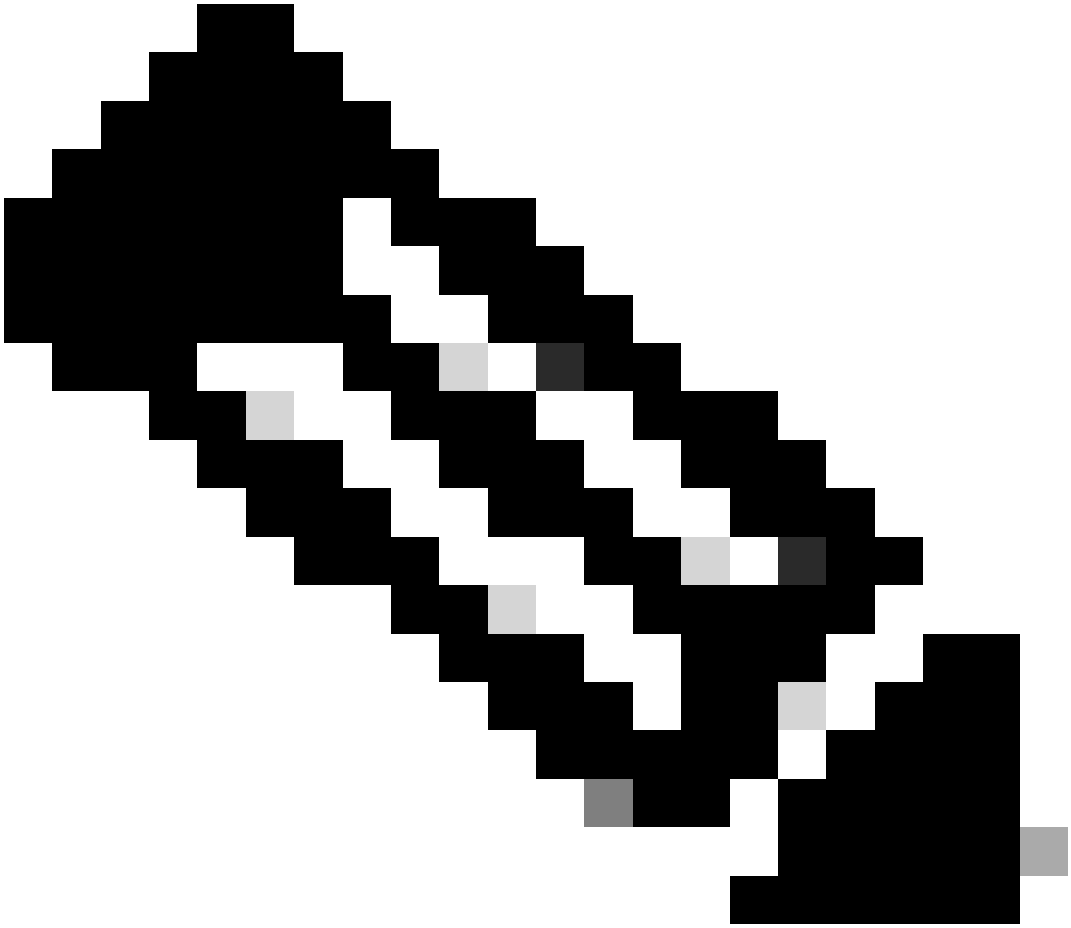
本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

Cisco Umbrella与Check Point防僵尸软件刀片的集成使Check Point设备能够在刀片发现其检查的网络流量中的威胁时向Cisco Umbrella发送其防僵尸软件刀片警报。Cisco Umbrella收到的警报会构建一个阻止列表，可以保护未受Check Point防僵尸软件刀片保护的漫游笔记本电脑、平板电脑和电话网络。

本文提供配置检查点设备以向Cisco Umbrella发送防僵尸软件刀片警报的说明。



注意：在R80.40中首次发布此集成后，R81.20中的Check Point已弃用它。

功能

Cisco Umbrella与Check Point反僵尸软件刀片设备集成，将其发现的威胁（例如，托管恶意软件的域、僵尸网络的命令和控制或网络钓鱼站点）推送到Cisco Umbrella进行全球实施。

然后，Cisco Umbrella验证威胁以确保将其添加到策略中。如果确认来自Check Point Anti-Bot Software Blade的信息是威胁，则域地址将作为Check Point Destination List的安全设置的一部分添加到可以应用于任何Cisco Umbrella策略。该策略会立即应用于从分配给该策略的设备发出的任何请求。

接下来，Cisco Umbrella会自动解析Check Point警报并将恶意站点添加到Check Point Destination List。这会将Check Point保护扩展到所有远程用户和设备，并为您的公司网络提供另一层实施。

配置步骤

配置集成包括以下步骤：

1. 启用在Cisco Umbrella中的集成，以使用自定义脚本生成API令牌。
2. 在Check Point设备上部署API令牌和自定义脚本。
3. 生成/编辑Check Point警报以发布到此新脚本。
4. 将Check Point事件设置为在Cisco Umbrella中阻止。

防止服务中断

为避免不必要的服务中断，Cisco Umbrella建议在配置集成之前将永远无法阻止的任务关键域名(例如，google.com或salesforce.com)添加到全局允许列表（或根据策略的其他目标列表）。

任务关键型域可能包括：

- 您组织的主页
- 代表您提供的服务的域，可以同时具有内部和外部记录。例如，“mail.myservicedomain.com”和“portal.myotherservicedomain.com”。
- 您依赖于Cisco Umbrella的不太知名的基于云的应用不能包含在自动域验证中。例如，“localcloudservice.com”。

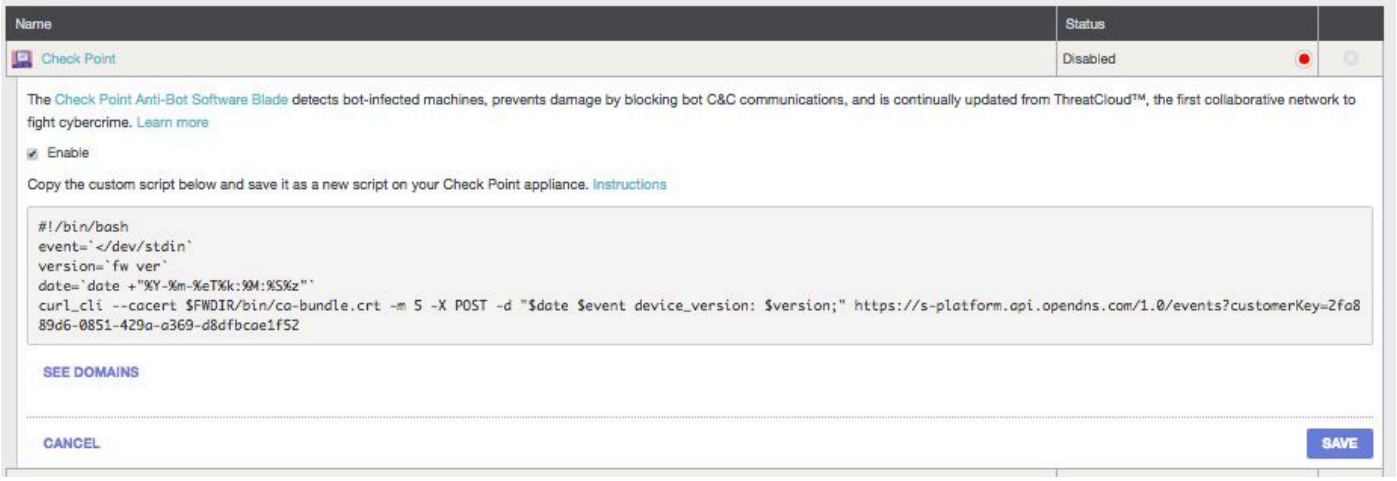
这些域必须添加到Global Allow List，该列表位于Cisco Umbrella的Policies > Destination Lists下。

步骤 1：Umbrella脚本和API令牌生成

1.以管理员身份登录Cisco Umbrella Dashboard。

2.定位至策略>策略组件>集成，然后在表中选择Check Point以展开它。

3.选择启用选项。



4.复制整个脚本，从以下行开始：

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

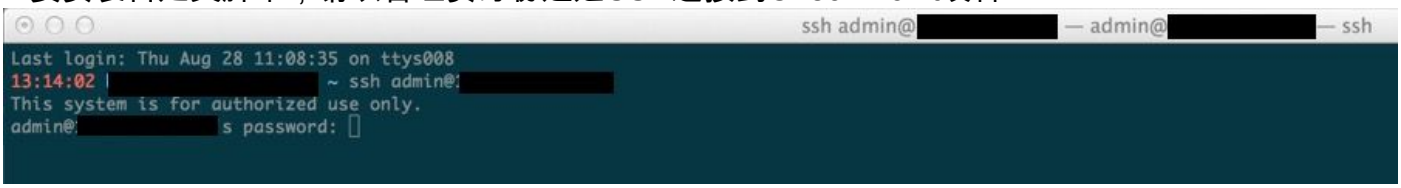
然后，您可以在后续步骤中使用该脚本。

5.选择保存以启用集成。

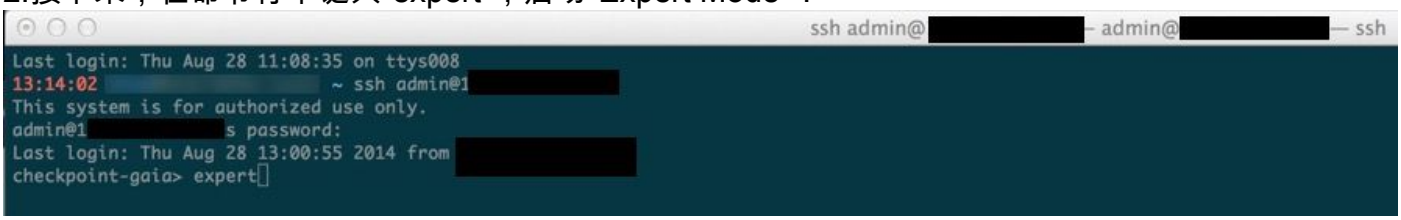
步骤 2：在Check Point设备上部署自定义脚本

下一步是在Check Point设备上安装自定义Cisco Umbrella脚本，然后在SmartDashboard中启用该脚本。

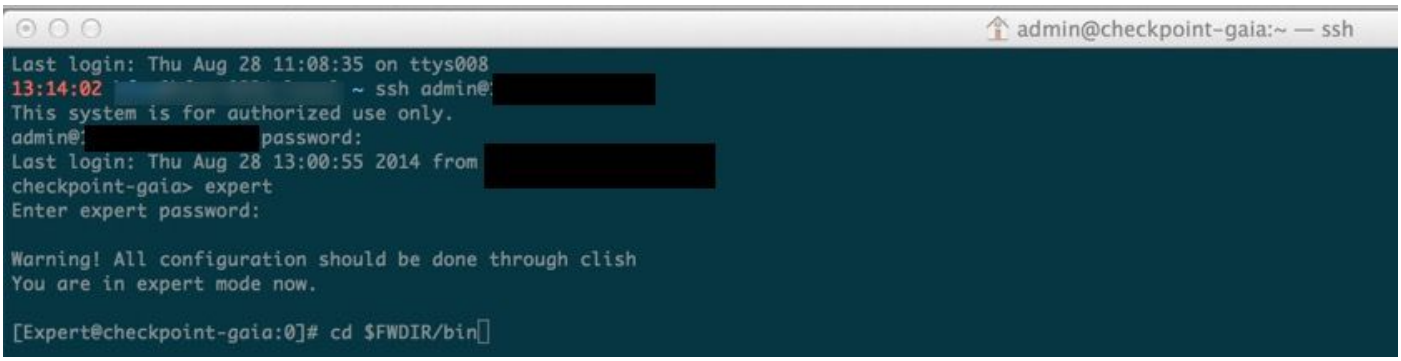
1.要安装自定义脚本，请以管理员身份通过SSH连接到Check Point设备：



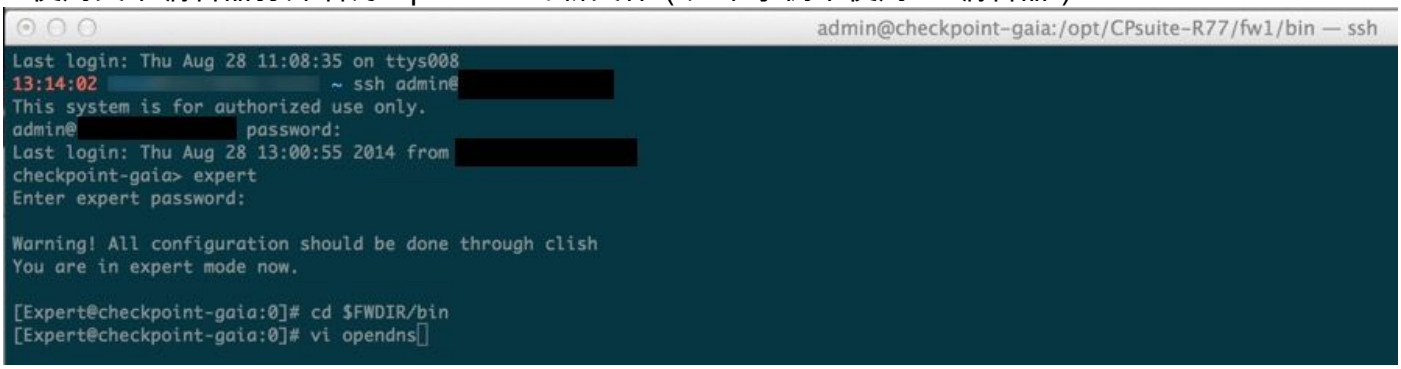
2.接下来，在命令行中键入“expert”，启动“Expert Mode”：



3.将工作目录更改为`$FWDIR/bin`:

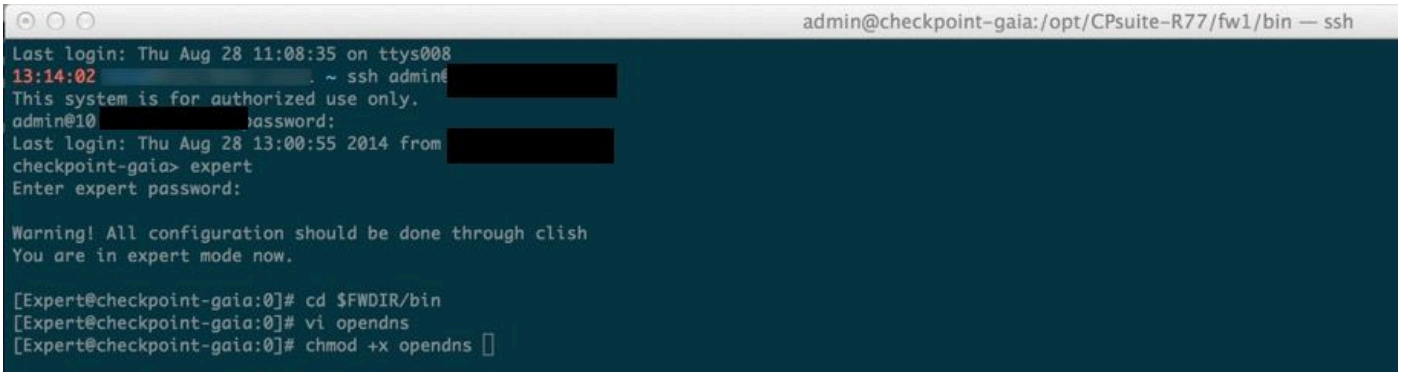


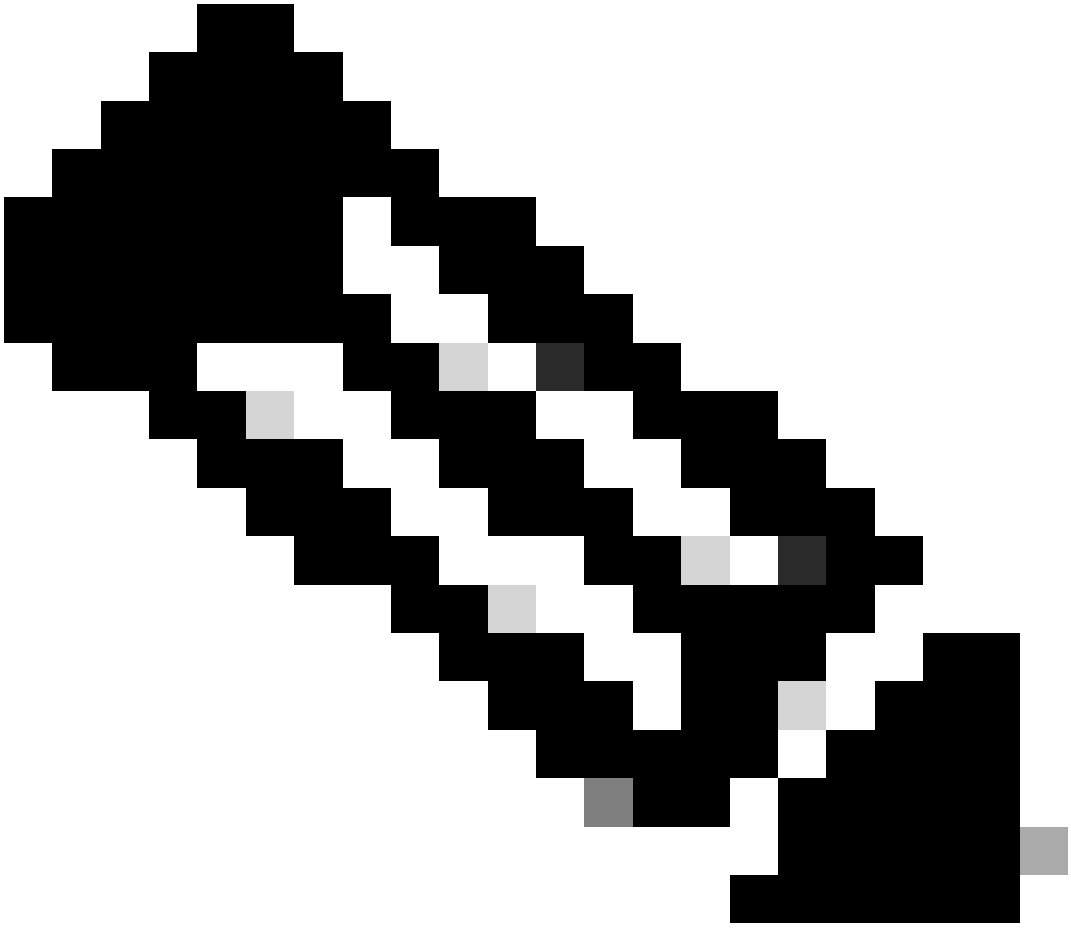
4.使用文本编辑器打开名为“opendns”的新文件（如本示例中使用“vi”编辑器）：



5.将Cisco Umbrella脚本粘贴到文件中，然后保存文件并退出编辑器：

6.通过运行`chmod +x opendns`使自定义Umbrella脚本可执行：





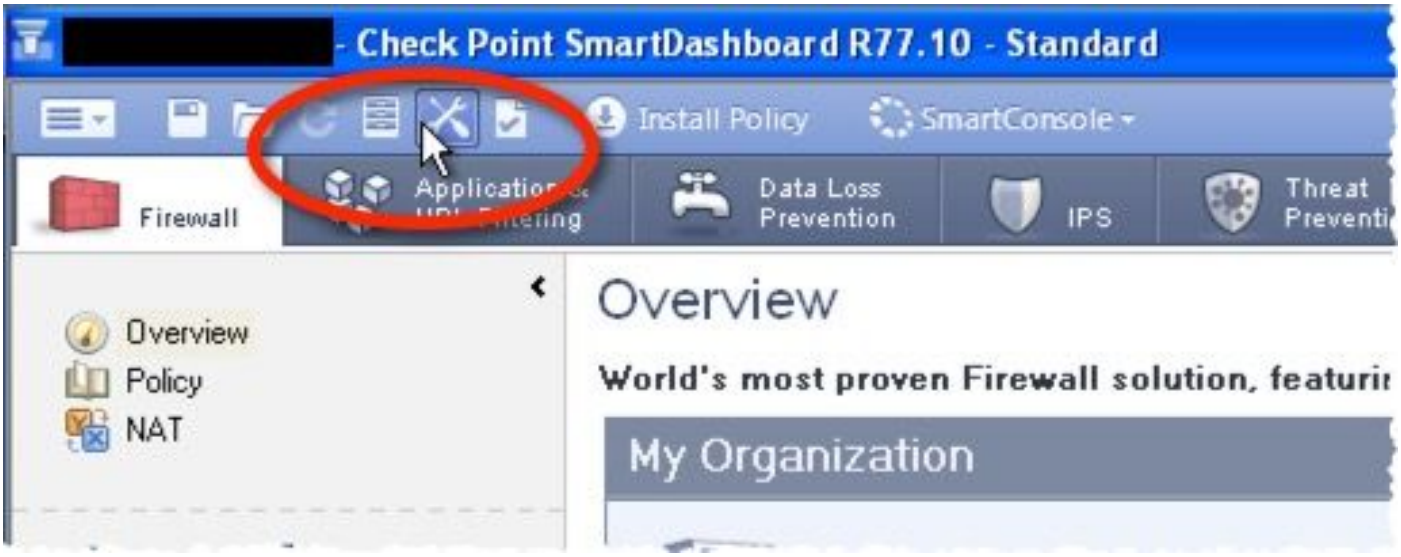
注意：如果您升级或更改刀片版本，则必须在该新版本上重复这些步骤。

步骤3.生成或编辑Check Point警报以发布到新脚本

1.通过登录和启动SmartDashboard，使SmartDashboard发布新脚本：


Check Point
SmartDashboard
R77.10
Use certificate
Ben
Password
Read only
Demo mode
Login
Add session description (optional)

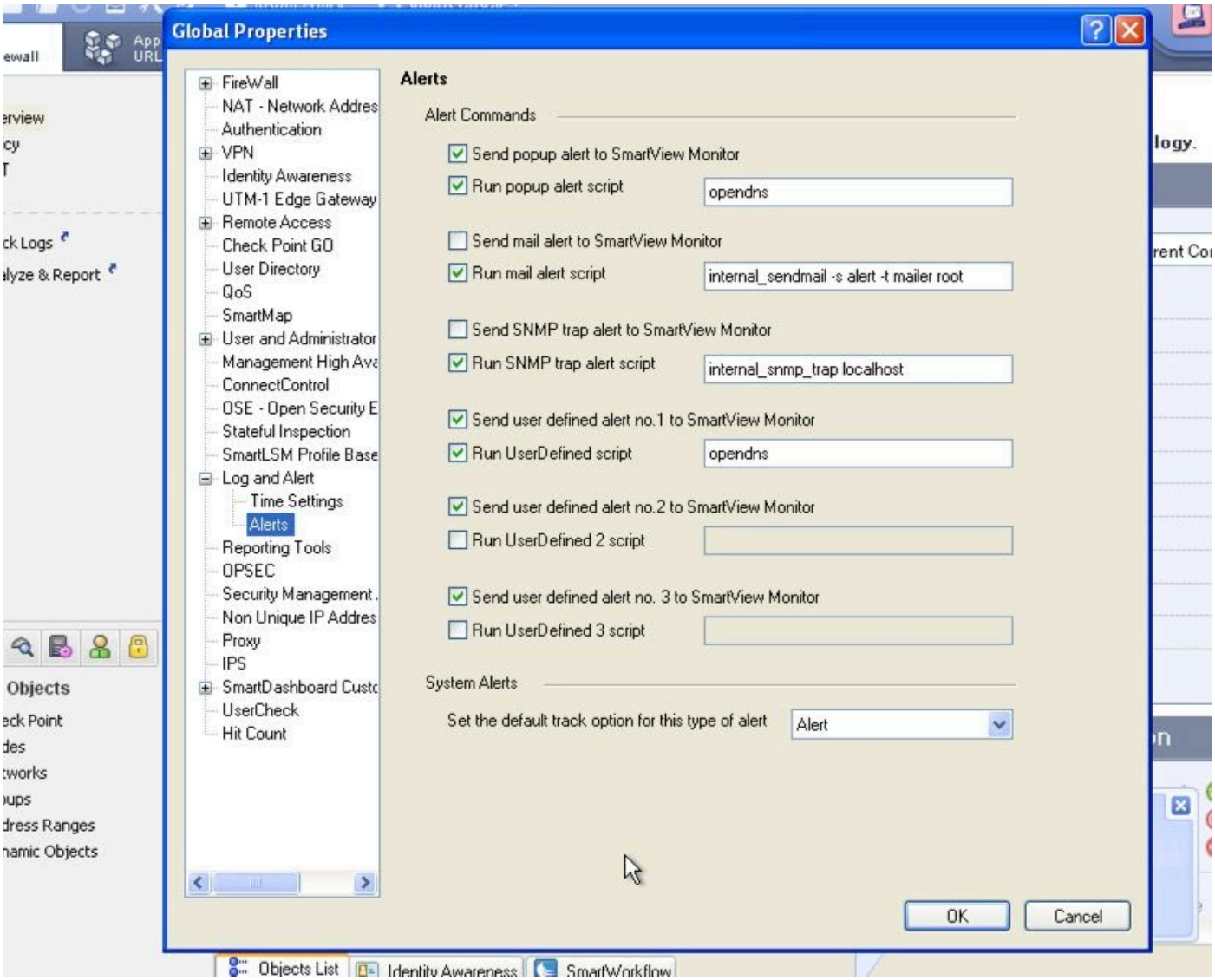
2.打开全局属性:



3.在全局属性中，打开Log and Alert > Alerts 并完成以下步骤：

- 选择发送弹出窗口alertscript和运行用户定义脚本。
- 在两个脚本字段中均定义“opendns”。

4.选择确定。从SmartDashboard保存并安装更新的策略。



步骤 4：测试集成并设置要阻止的Check Point事件

首先，生成测试反僵尸刀片事件，使其显示在Cisco Umbrella控制面板中：

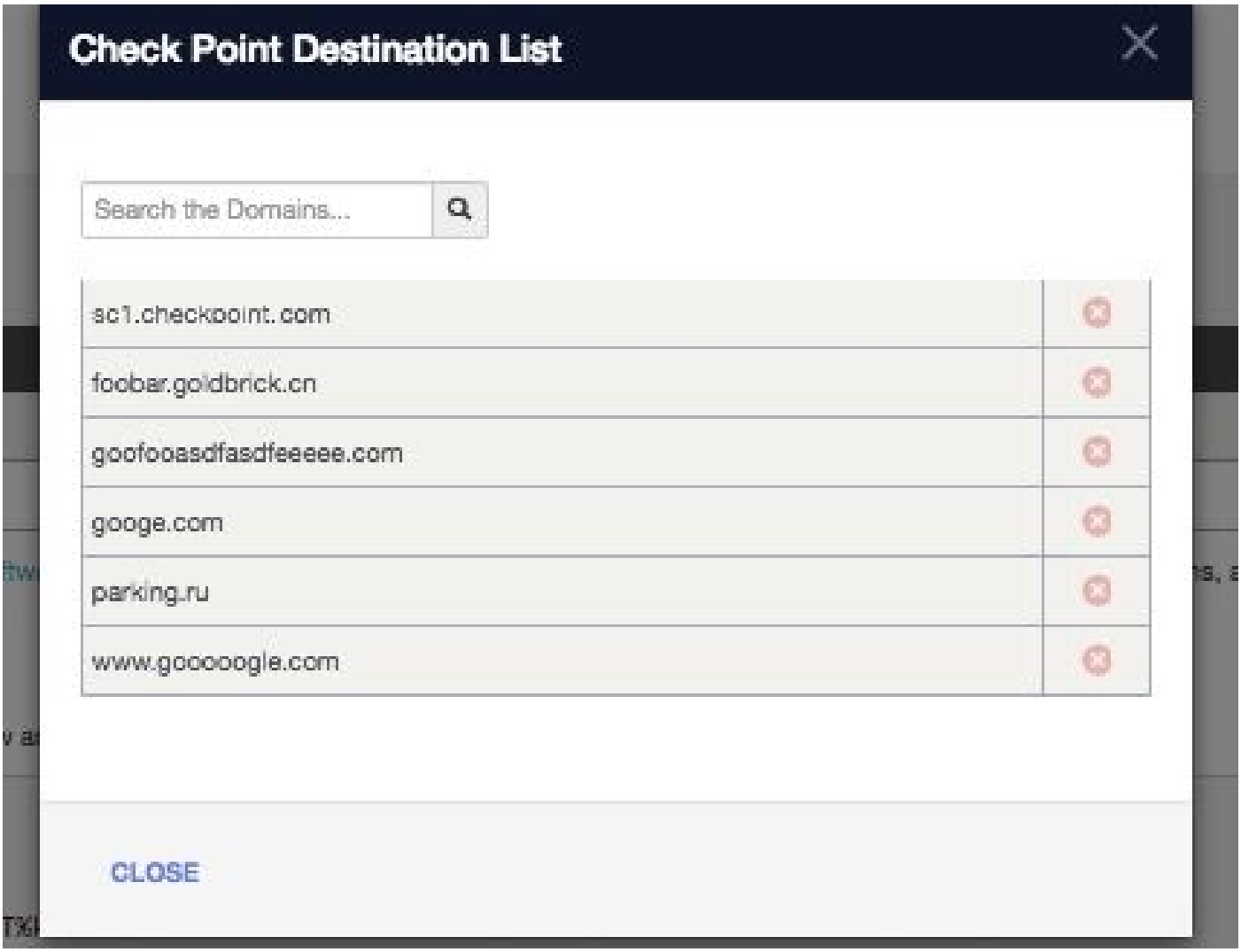
1.从网络上受Check Point设备保护的任何设备将此URL加载到浏览器中：

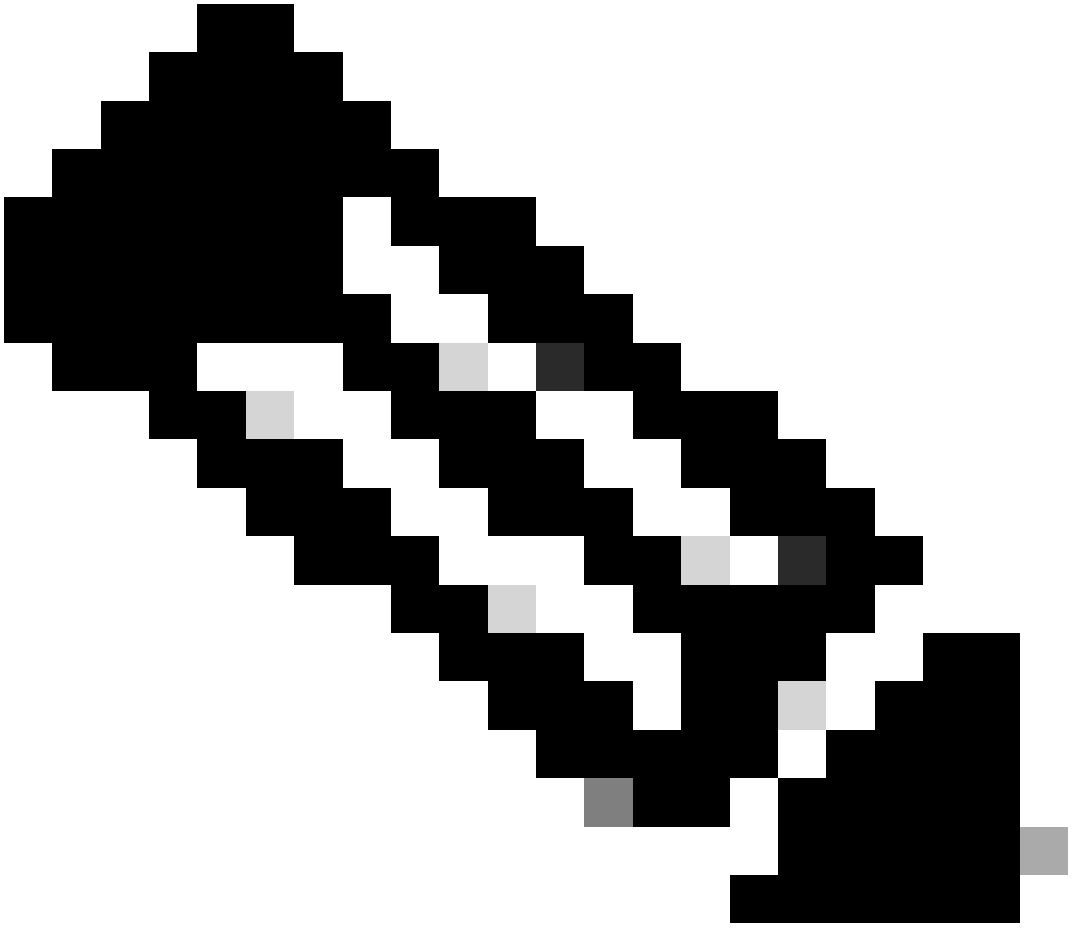
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

2.以管理员身份登录Cisco Umbrella控制面板。

3.定位至策略>策略组件>集成，然后在表中选择Check Point以展开它。

4.选择查看域。这将打开一个窗口，其中显示可以包括“sc1.checkpoint.com”的Check Point Destination List。 从那时起，可搜索列表开始填充和增长。


Check Point Destination List
Search the Domains...
sc1.checkpoint.com
foobar.goldbrick.cn
goofooasdfasdfeeeee.com
googe.com
parking.ru
www.goooogle.com
CLOSE

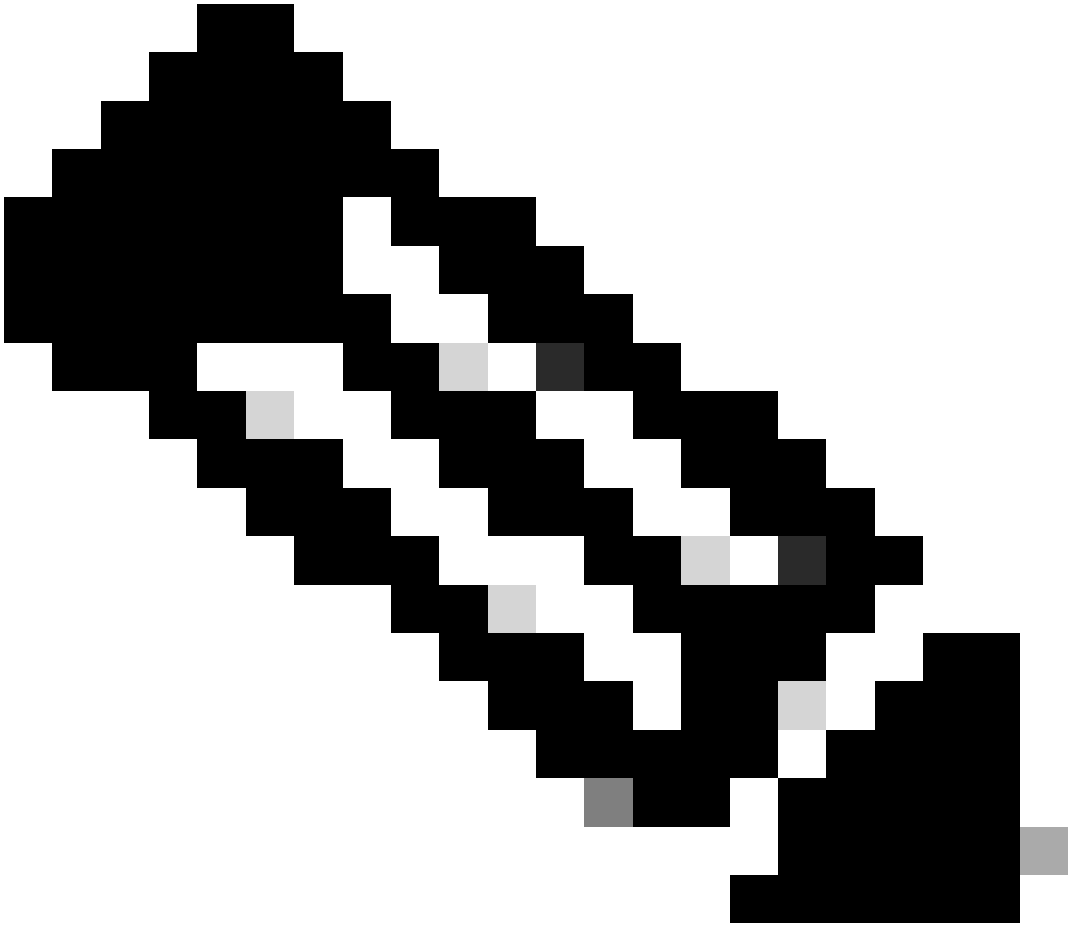


注意：如果此处显示了一个您不想对其实施策略的域，您也可以更改此目标列表。选择删除图标以删除域。

观察在“审核模式”下添加到Check Point安全类别的事件

下一步是观察和审核添加到新的Check Point安全类别的事件。

Check Point设备中的事件开始填充可以作为Check Point安全类别应用到策略的特定目标列表。默认情况下，目标列表和安全类别处于“审核模式”，不应用于任何策略，且不会导致对现有Cisco Umbrella策略进行任何更改。



注意：根据您的部署配置文件和网络配置，可以启用“审核模式”，但必须持续很长时间。

查看目标列表

您可以随时在Cisco Umbrella中查看Check Point Destination List:

1.定位至策略>策略组件>集成。

2.展开表中的Check Point并选择See Domains。

查看策略的安全设置

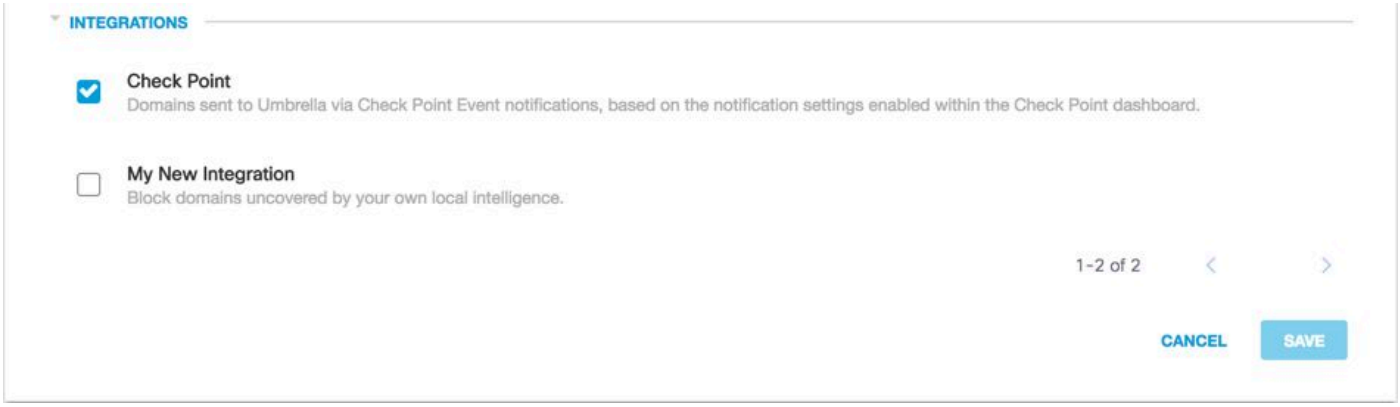
您可以随时在Cisco Umbrella中查看可以为策略启用的安全设置：

1.导航到策略>策略组件>安全设置。

2.选择表中的安全设置将其展开。

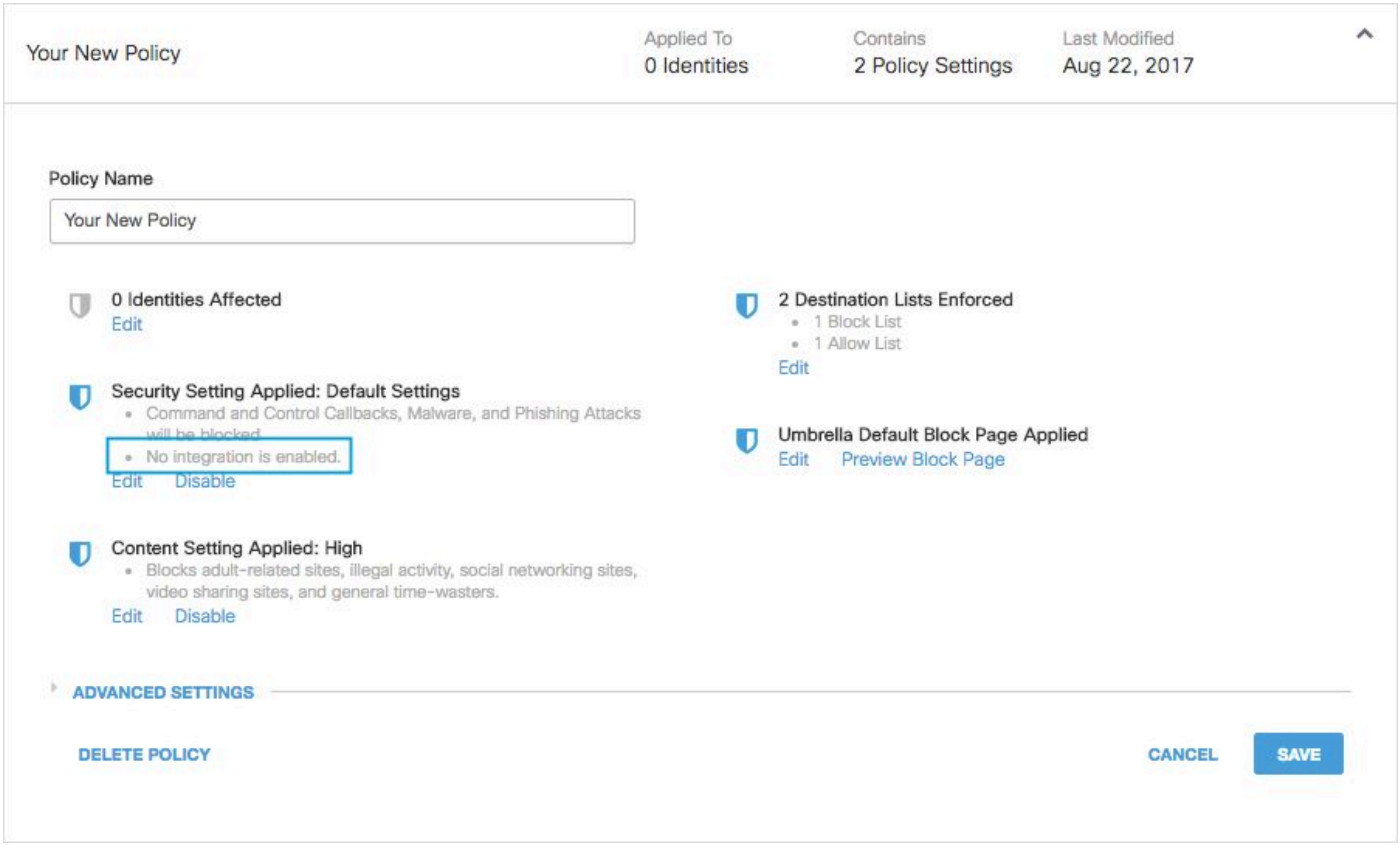
3.滚动到集成部分并展开该部分以显示Check Point集成。

4.选择Check Point集成的选项，然后选择保存。



115013984226

您还可以通过Security Settings Summary页查看集成信息：



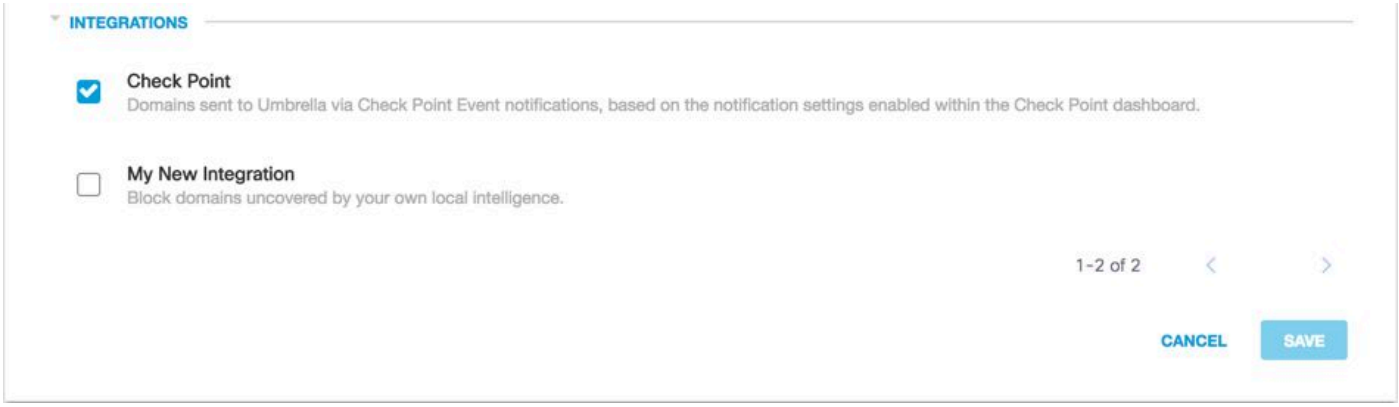
19916943300244

将“阻止模式”下的Check Point安全设置应用于托管客户端的策略

当您准备好让这些附加安全威胁由Cisco Umbrella管理的客户端实施后，请更改现有策略的安全设置，或创建位于默认策略之上的新策略，以确保首先实施该策略：

1.确保Check Point集成仍按上一节中的步骤启用。导航到策略>策略组件>安全设置，然后打开相关设置。

2.在Integrations下，验证Check Point选项是否已选中。否则，请选择该选项并选择保存。



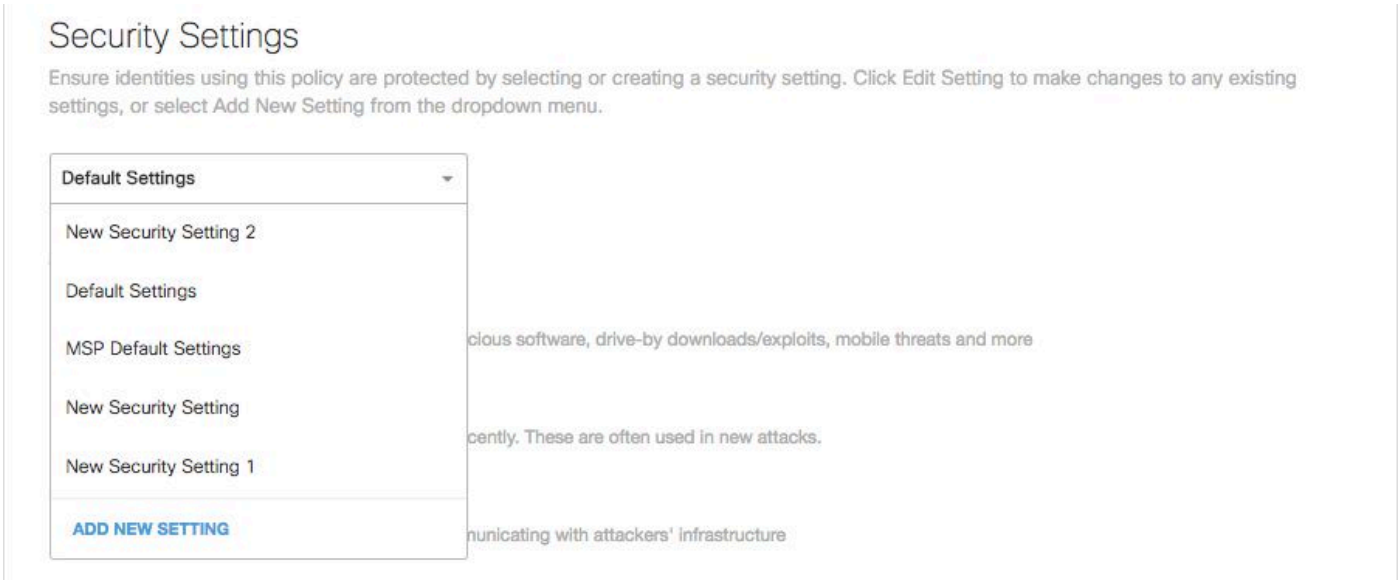
115013984226

接下来，在Cisco Umbrella Policy向导中，将此安全设置添加到正在编辑的策略中：

1.定位至策略：Policies > DNS Policies或Policies > Web Policy。

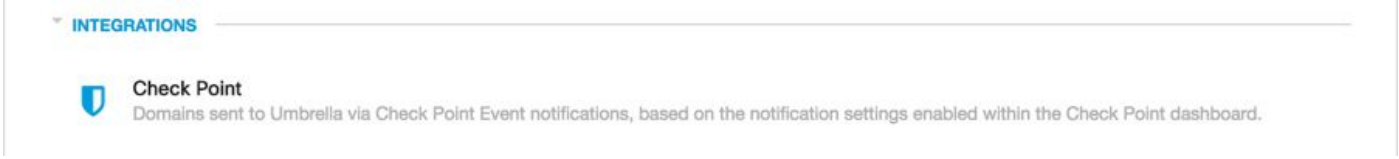
2.展开策略，然后在Security Setting Applied(DNS Policies)或Security Settings(Web Policy)下选择Edit。

3.在安全设置下拉列表中，选择包含“检查点”设置的安全设置。



19916943316884

“集成”(Integrations)下的屏蔽图标将更新为蓝色。



115014149783

4.选择Set & Return(DNS Policies)或Save(Web Policy)。

然后，对于使用策略的那些身份，可以阻止Check Point的安全设置中包含的Check Point域。

在Umbrella中报告Check Point事件

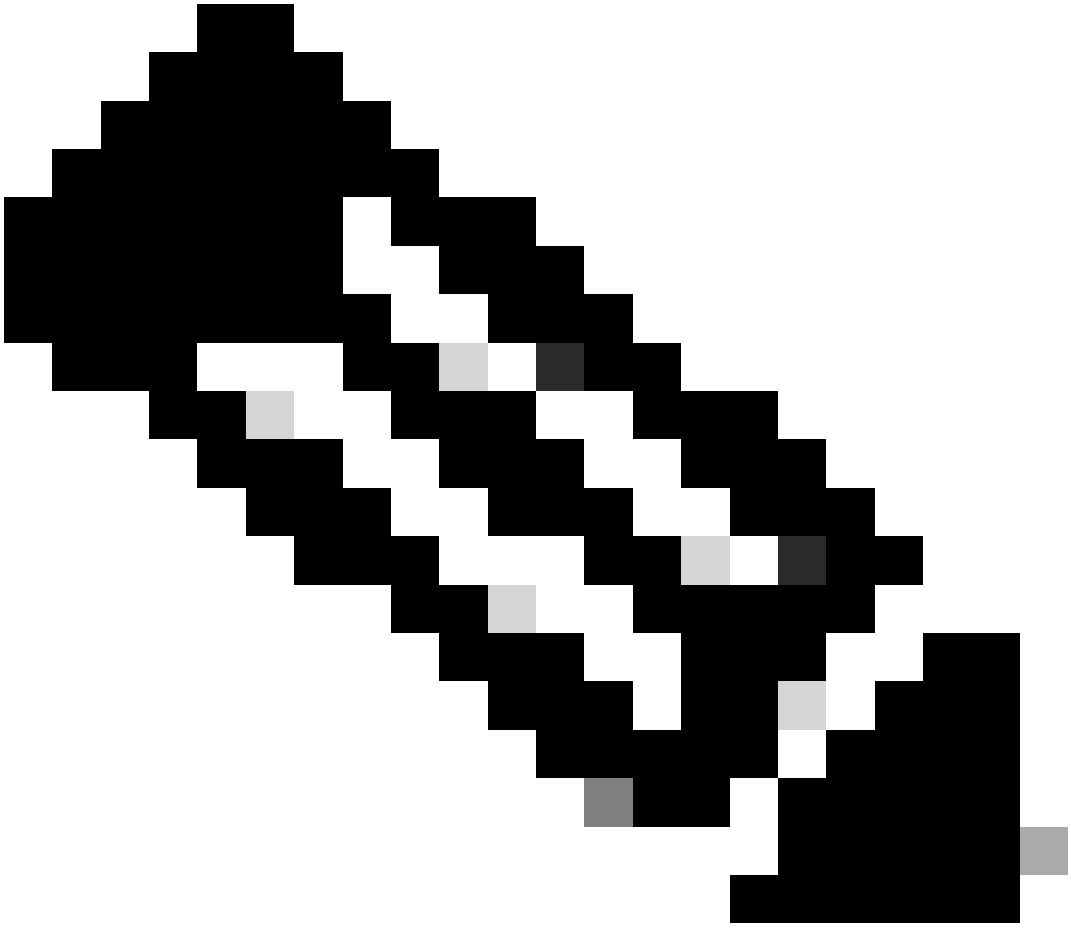
报告Check Point安全事件

Check Point Destination List是可用于报告的一种安全类别。大多数或全部报告将安全类别用作过滤器。例如，您可以过滤安全类别，以仅显示与Check Point相关的活动：

1.定位至报告>核心报表>活动搜索。

2.在Security Categories下，选择Check Point以过滤报表，以便仅显示Check Point的安全类别。

115014197623



注意：如果Check Point集成被禁用，则它不能出现在安全类别过滤器中。

3.选择应用以查看报表中所选期间的“检查点”相关活动。

报告域添加到Check Point目标列表的时间

Cisco Umbrella管理员审核日志包含检查点设备的事件，因为它将域添加到目标列表。这些域似乎通过“审核日志”User列下的“Check Point帐户”标签添加。

要查找Umbrella Admin Audit日志，请导航至报告>管理员审核日志。

要报告添加域的时间，请通过应用Check Point Block List的Filter by Identities & Settings过滤器来筛选仅包含Check Point更改。

运行报告后，您可以看到添加到Check Point目标列表的域列表。

处理不需要的检测或误报

管理不需要的检测的允许列表

虽然可能性不大，但您的Check Point设备自动添加的域可能会触发不需要的阻止，从而导致您的用户被阻止访问特定网站。在这种情况下，Cisco Umbrella建议将域添加到允许列表，该列表优先于所有其他类型的阻止列表，包括安全设置。当两个域中都存在域时，允许列表优先于阻止列表。

首选此方法的原因有两个：

- 首先，如果Check Point设备在删除域后再次重新添加域，则允许列表可防止导致进一步的问题。
- 其次，允许列表显示有问题的域的历史记录，以供以后的调查分析或审计报告使用。

默认情况下，全局允许列表应用于所有策略。将域添加到全局允许列表(Global Allow List)会导致在所有策略中允许该域。

如果Check Point Security Setting in Block模式仅适用于受管Cisco Umbrella身份的子集（例如，它仅适用于漫游计算机和移动设备），则可以为这些身份或策略创建特定的允许列表。

要创建允许列表，请执行以下操作：

1.定位至策略>目标列表，然后选择添加图标。

2.选择允许，然后将您的域添加到列表中。

3.选择保存。

保存该列表后，您可以将其添加到现有策略中，该策略涵盖了那些受不需要的阻止影响的客户端。

从检查点目标列表中删除域

Check Point目标列表中的每个域名旁边都有一个Delete图标。通过删除域，您可以在不需要的检测时清除Check Point目标列表。

但是，如果Check Point设备将域重新发送到Cisco Umbrella，则删除不是永久性的。

删除域的步骤：

1.定位至“设置”>“集成”，然后选择“检查点”将其展开。

2.选择查看域。

3.搜索要删除的域名。

4.选择删除图标。

5.选择关闭。

6.选择保存。

如果检测到不需要的检测或误报，Cisco Umbrella建议立即在Cisco Umbrella中创建允许列表，然后在Check Point设备中修复误报。之后，您可以从Check Point目标列表中删除该域。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。