使用Check Point Anti-Bot軟體刀片配置Umbrella

目錄

簡介

本檔案介紹如何將Cisco Umbrella與Check Point Anti-Bot軟體刀鋒整合。

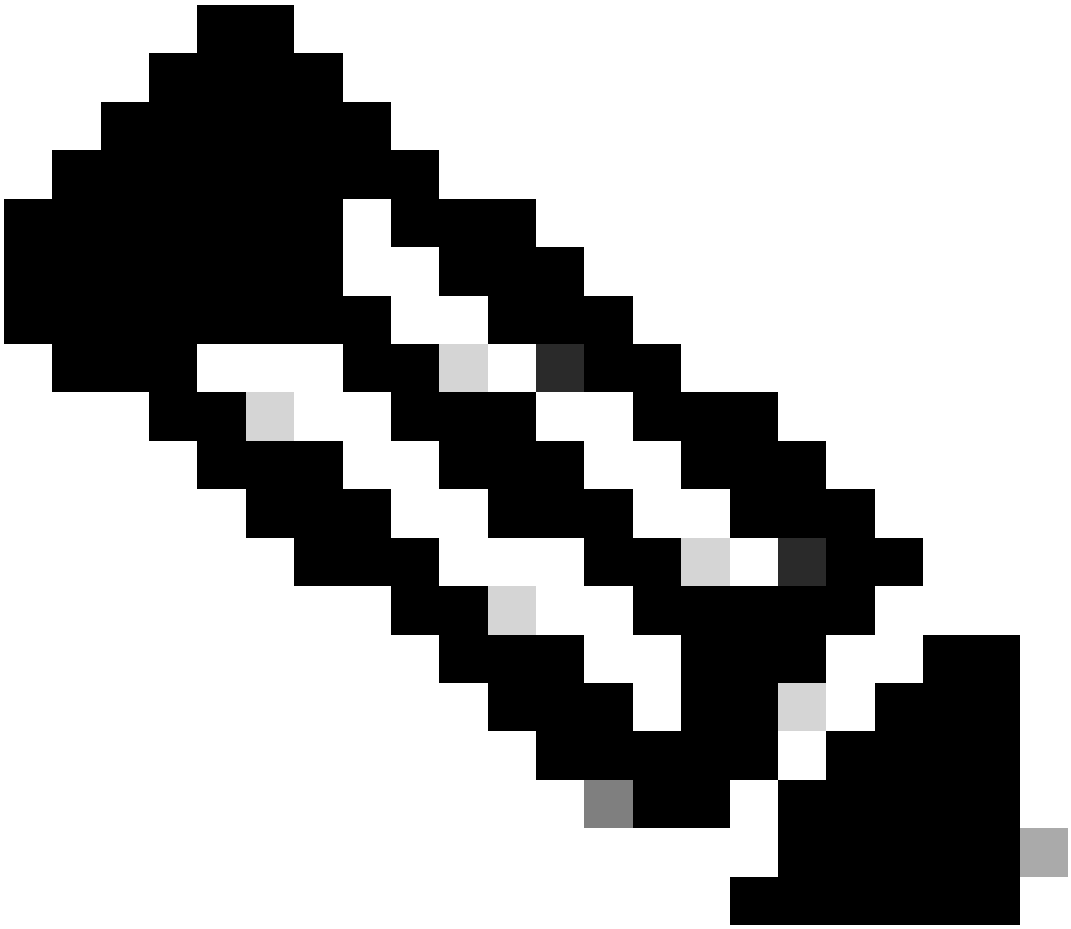
必要條件

需求

思科建議您瞭解以下主題：

- 具有防僵機器人軟體刀片的檢查點裝置
- Check Point軟體版本R80.40或更高版本
- 確保Check Point裝置可以向「https://s-platform.api.opendns.com」發出出站HTTP請求。
- Cisco Umbrella包，例如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage

- Cisco Umbrella Dashboard管理許可權



附註：Check Point整合僅包含在Cisco Umbrella包中，例如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage。如果您沒有這些軟體包之一，並且希望整合Check Point，請聯絡您的Cisco Umbrella客戶經理。如果您有正確的Cisco Umbrella軟體包，但是沒有將Check Point視為控制面板的整合，請與Cisco Umbrella支援聯絡。

採用元件

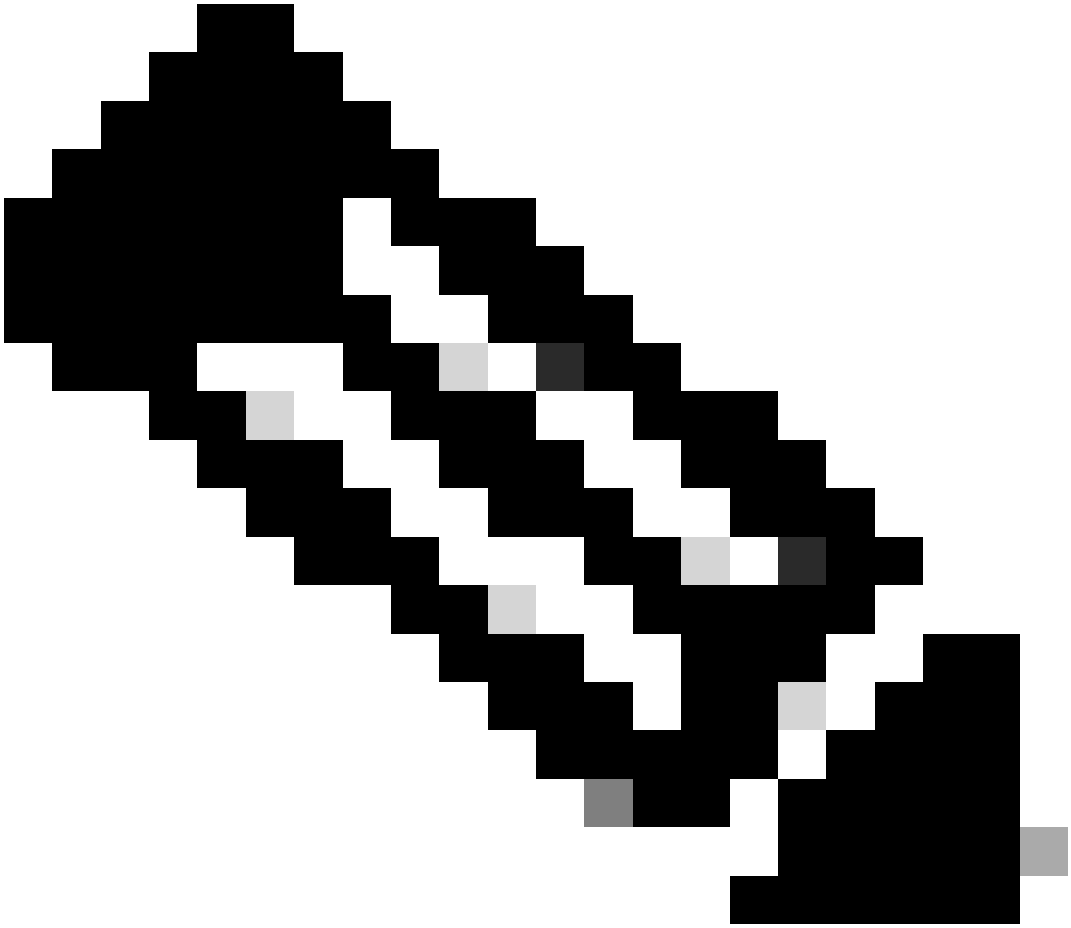
本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Cisco Umbrella與Check Point Anti-Bot Software Blade的整合使Check Point裝置能夠在刀片發現其檢查的網路流量中的威脅時，將其Anti-Bot Software Blade警報傳送到Cisco Umbrella。Cisco Umbrella收到的警報會構建阻止清單，該清單可以保護漫遊的筆記型電腦、平板電腦和電話網路（未受Check Point Anti-Bot軟體刀片保護）。

本文提供配置Check Point裝置以向Cisco Umbrella傳送Anti-Bot軟體刀片警報的說明。



附註：R81.20版中的Check Point在R80.40中首次發佈此整合後不再支援。

功能

Cisco Umbrella與Check Point Anti-Bot Software Blade裝置的整合將其發現的威脅（例如，託管惡意軟體的域、殭屍網路的命令和控制或網路釣魚站點）推送至思科Umbrella進行全球實施。

然後，Cisco Umbrella驗證威脅以確保將其新增到策略中。如果確認來自Check Point Anti-Bot Software Blade的資訊是威脅，則域地址會作為安全設定的一部分新增到Check Point Destination List，該安全設定可以應用於任何Cisco Umbrella策略。該策略會立即應用於從分配給該策略的裝置

發出的任何請求。

接下來，Cisco Umbrella會自動分析Check Point警報並將惡意站點新增到Check Point Destination List。這會將Check Point保護擴展到所有遠端使用者和裝置，並為您的公司網路提供另一層實施。

設定步驟

配置整合涉及以下步驟：

1. 啟用在Cisco Umbrella中的整合，以使用自定義指令碼生成API令牌。
2. 在Check Point裝置上部署API令牌和自定義指令碼。
3. 生成/編輯Check Point警報以發佈到此新指令碼。
4. 設定要在Cisco Umbrella中阻止的Check Point事件。

防止服務中斷

為了避免不必要的服務中斷，Cisco Umbrella建議在配置整合之前將永遠無法阻止的任務關鍵型域名(例如google.com或salesforce.com)新增到全域性允許清單（或根據您的策略的其他目標清單）。

任務關鍵型域可包括：

- 您組織的首頁
- 表示您提供的服務的域，可以同時具有內部和外部記錄。例如，「mail.myservicedomain.com」和「portal.myotherservicedomain.com」。
- 您依賴於Cisco Umbrella的不太知名的基於雲的應用程式不能包含在自動域驗證中。例如，「localcloudservice.com」。

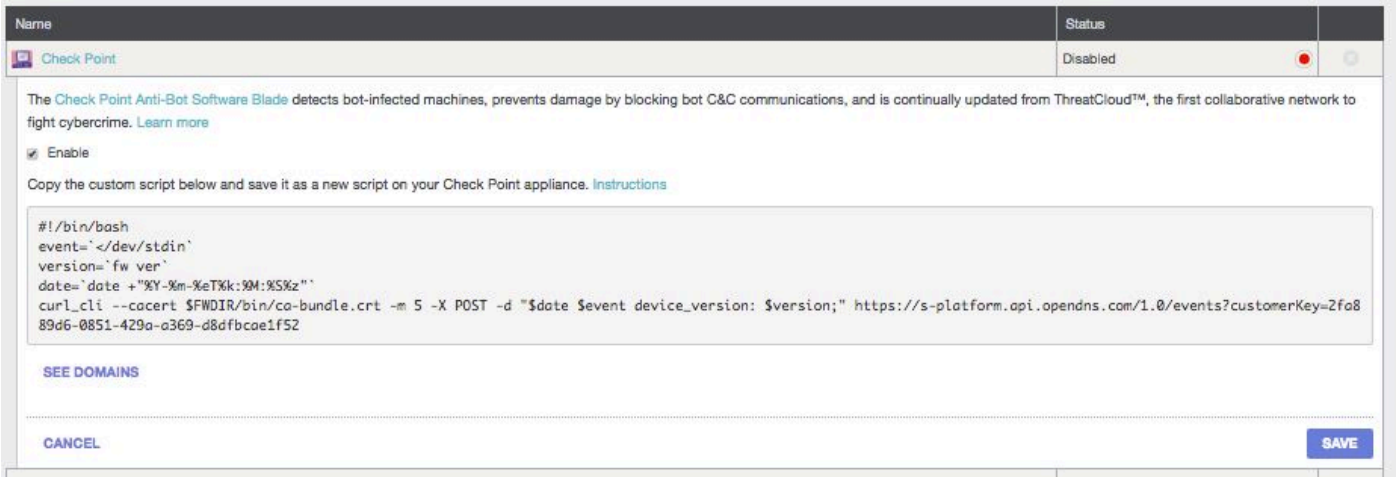
這些域必須新增到Global Allow List中，該清單位於Cisco Umbrella中的Policies > Destination Lists下。

步驟 1:Umbrella指令碼和API令牌生成

1.以管理員身份登入Cisco Umbrella Dashboard。

2.定位至Policies > Policy Components > Integrations，然後在表中選擇Check Point將其展開。

3.選擇Enable選項。



4.複製整個指令碼，從以下行開始：

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

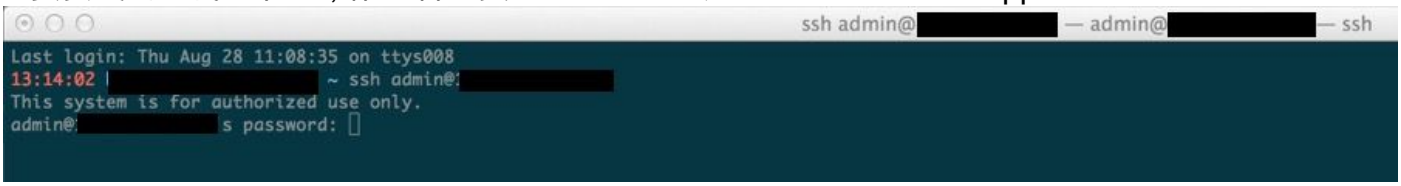
然後，可以在後續步驟中使用指令碼。

5.選擇儲存以啟用整合。

步驟 2:在Check Point裝置上部署自定義指令碼

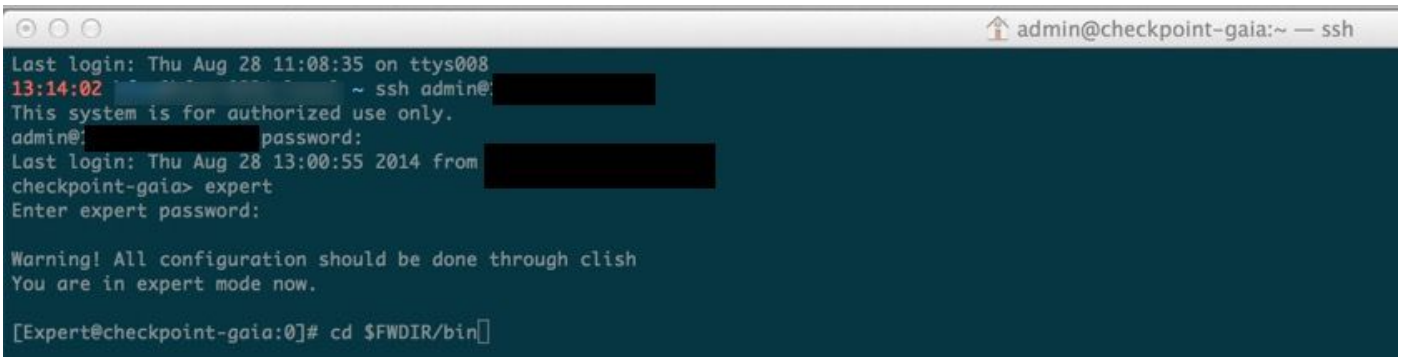
接下來的步驟是在您的Check Point裝置上安裝自定義Cisco Umbrella指令碼，然後在SmartDashboard中啟用該指令碼。

1.要安裝自定義指令碼，請以管理員身份通過SSH連線到Check Point Appliance:

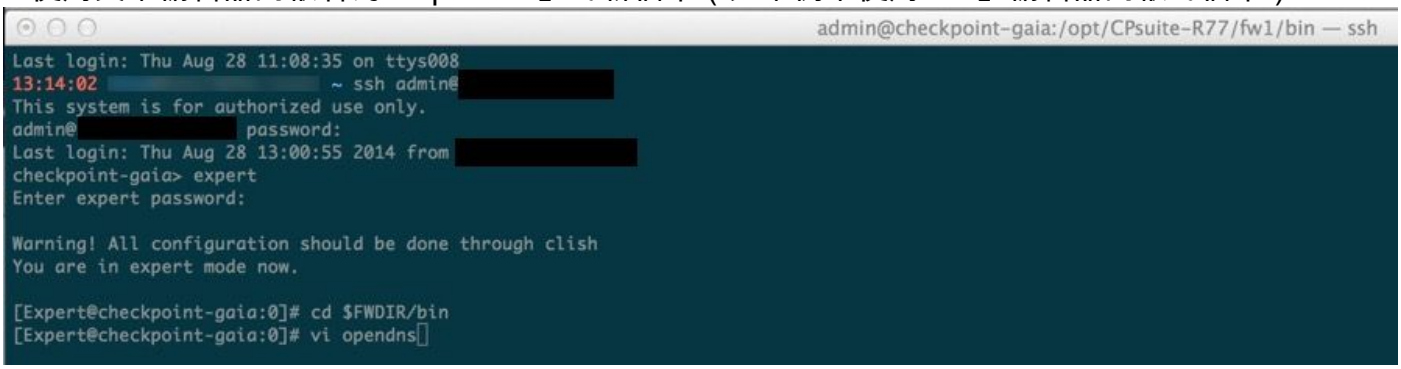


2.接下來，在命令列中鍵入「expert」，啟動「Expert Mode」：

3.將工作目錄更改為`$FWDIR/bin`:

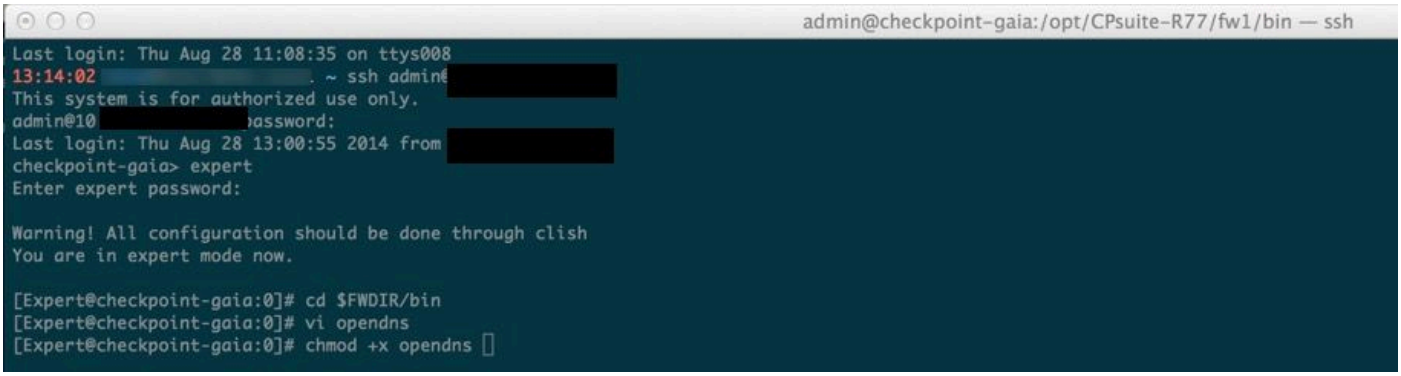


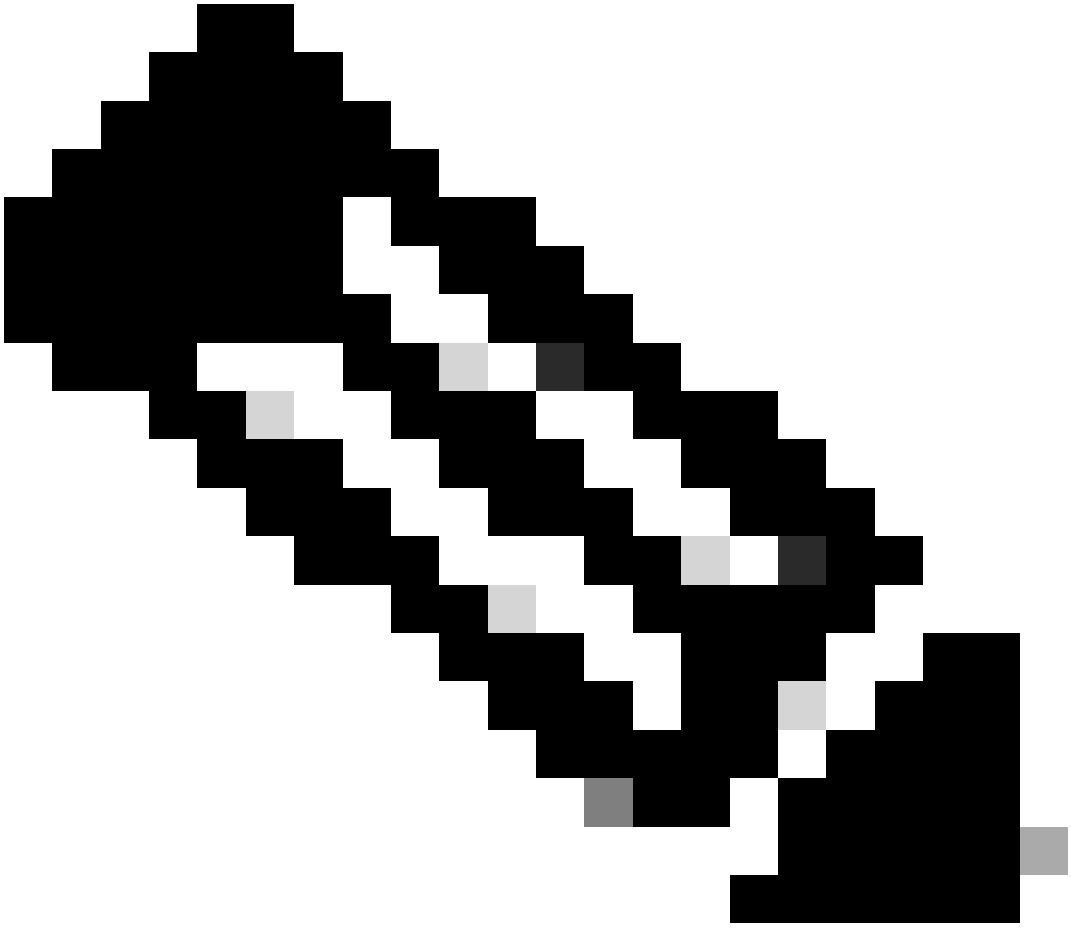
4.使用文本編輯器開啟名為「opendns」的新檔案（如本例中使用「vi」編輯器開啟的檔案）：



5.將Cisco Umbrella指令碼貼上到檔案中，然後儲存檔案並退出編輯器：

6.通過運行`chmod +x opendns`使自定義Umbrella指令碼可執行：





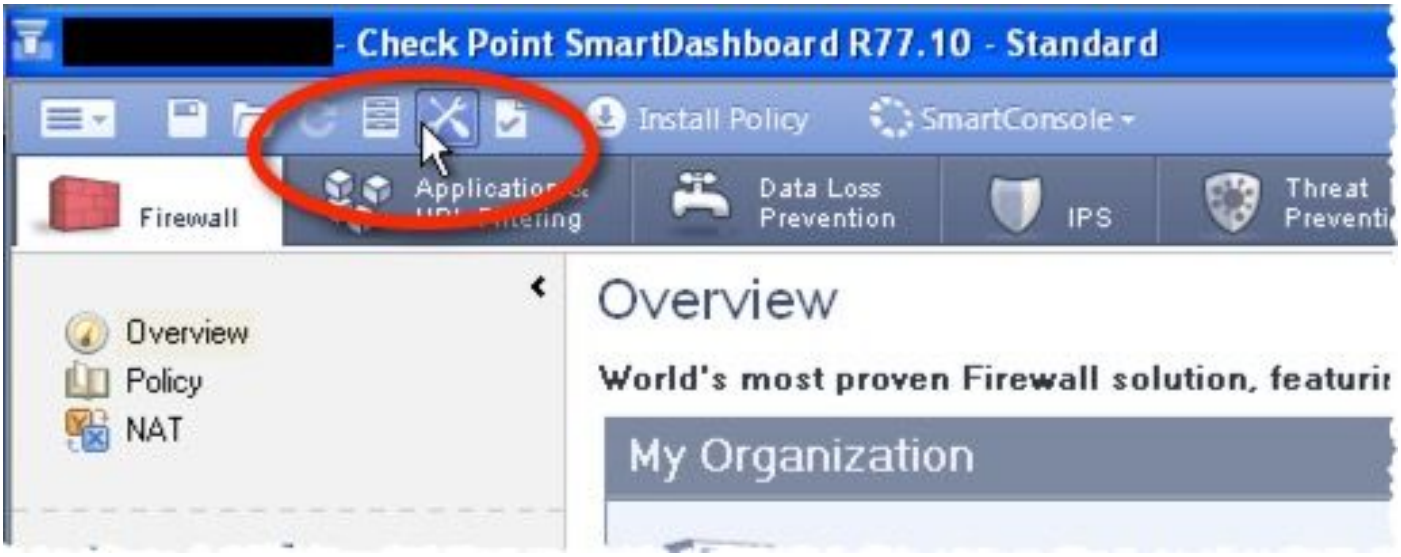
附註：如果您升級或更改刀片版本，則必須在該新版本上重複這些步驟。

步驟3.生成或編輯Check Point警報以發佈到新指令碼

1.通過登入並啟動SmartDashboard，啟用SmartDashboard來發佈新指令碼：


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

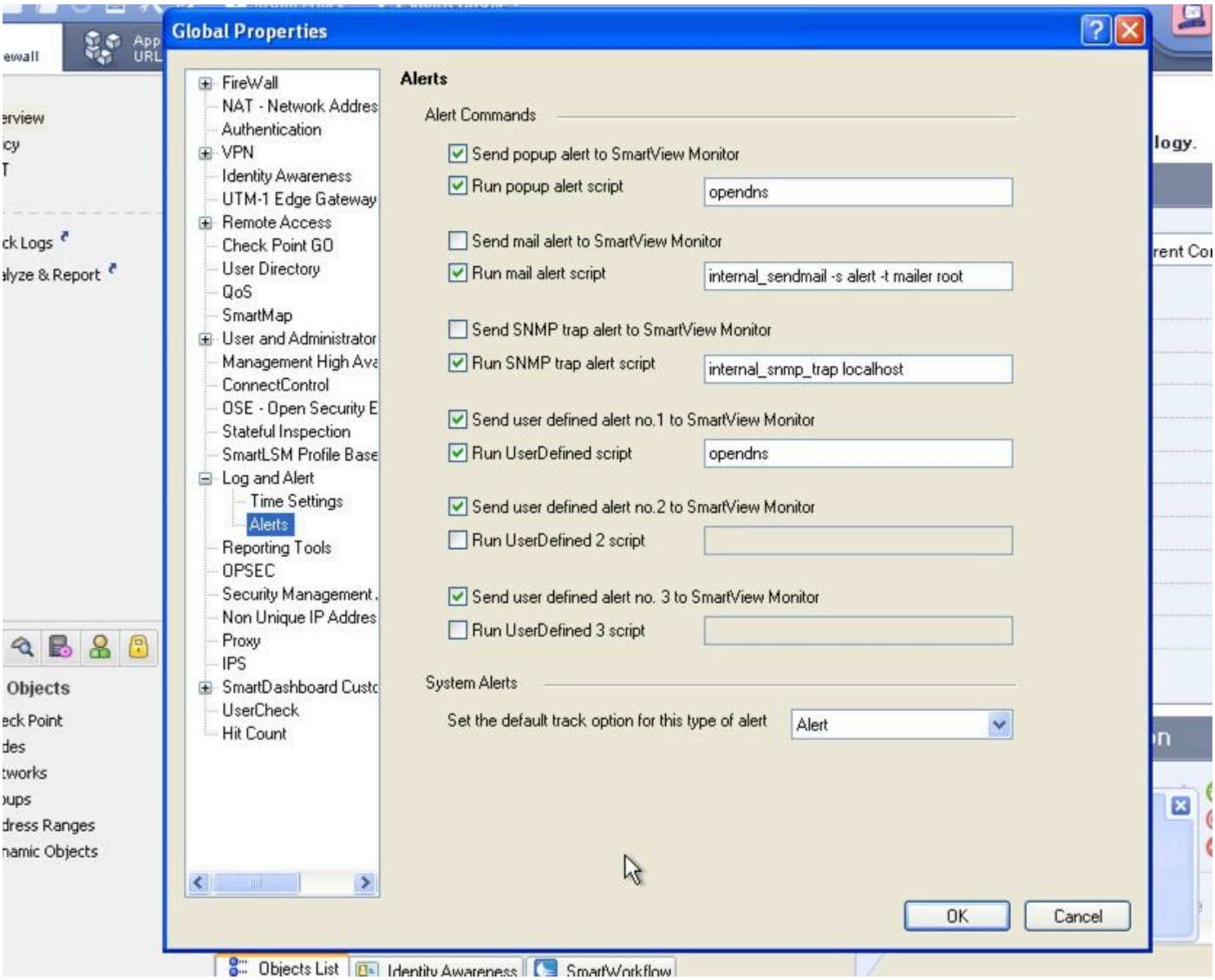
2.開啟全局屬性:



3.在全域性屬性中，開啟Log and Alert > Alerts，然後完成以下步驟：

- 選擇Send popup alertscript和Run UserDefined script。
- 在兩個指令碼欄位中定義「opendns」。

4.選擇確定。從SmartDashboard儲存並安裝更新的策略。



步驟 4:測試整合並設定要阻止的Check Point事件

首先，生成要顯示在Cisco Umbrella控制面板中的測試anti-bot刀片事件：

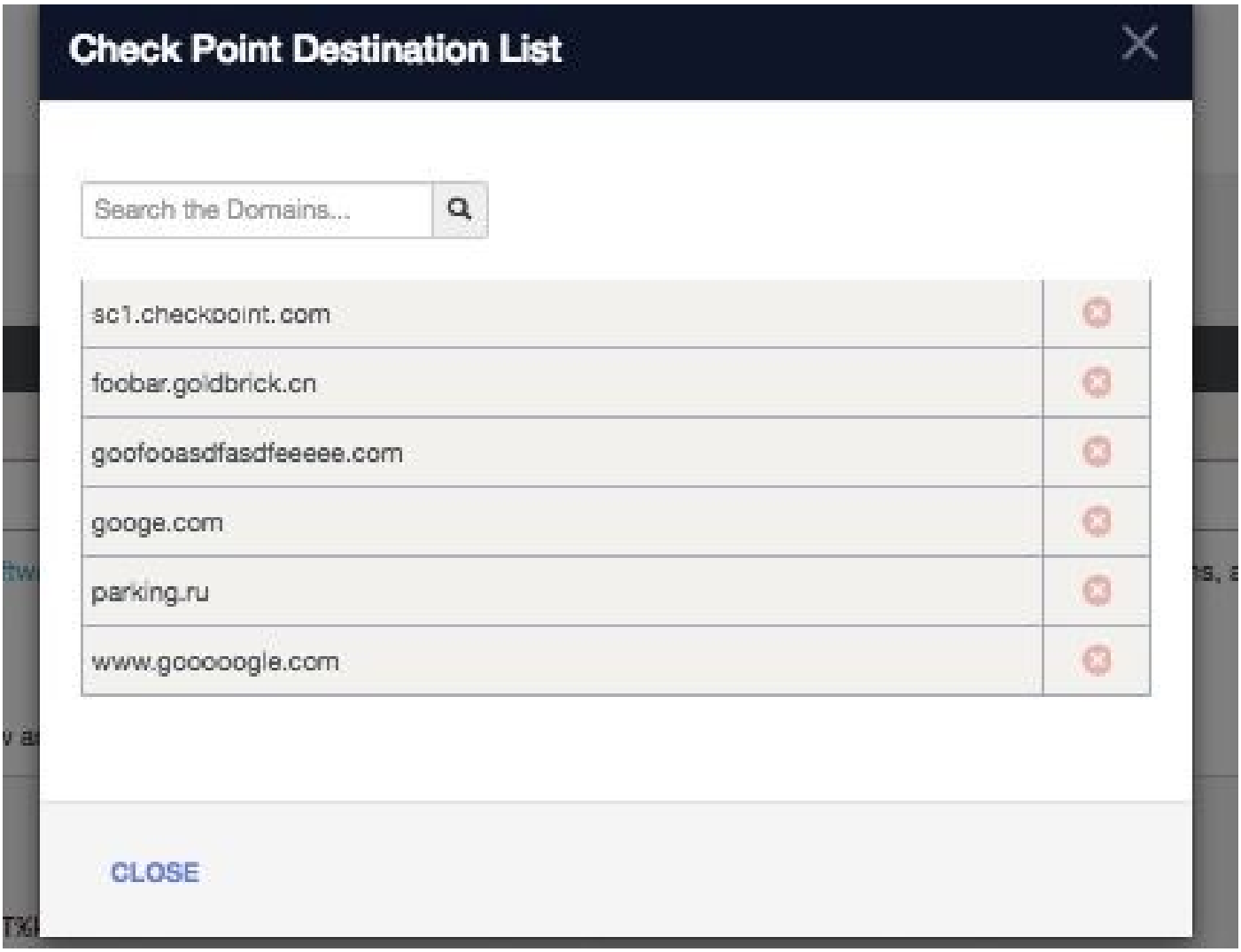
1.從受Check Point裝置保護的網路上的任何裝置，在瀏覽器中載入此URL:

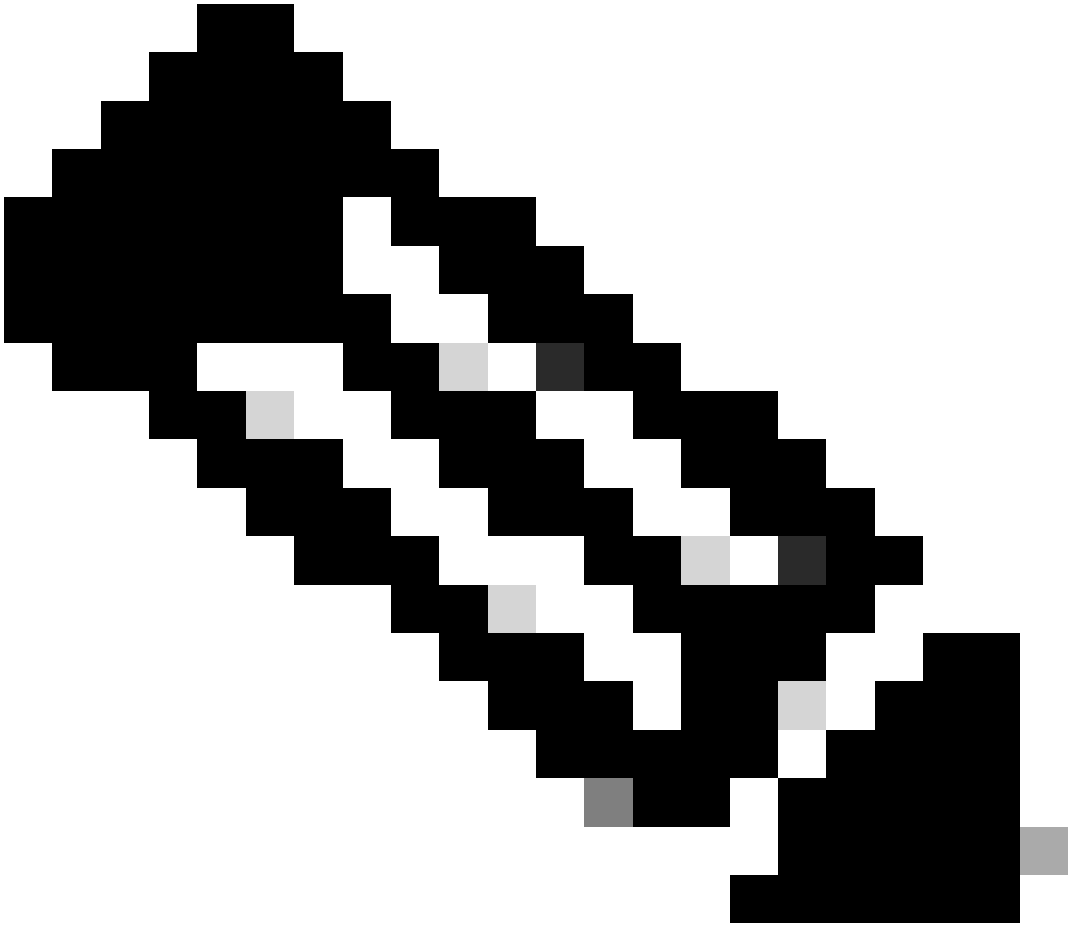
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

2.以管理員身份登入Cisco Umbrella控制面板。

3.定位至「策略」>「策略元件」>「整合」，然後在表中選擇Check Point將其展開。

4.選擇檢視域。這將開啟一個視窗，其中顯示Check Point Destination List（檢查點目標清單），該清單可以包括「sc1.checkpoint.com」。 從那時起，一個可搜尋的清單開始被填充和增長。


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

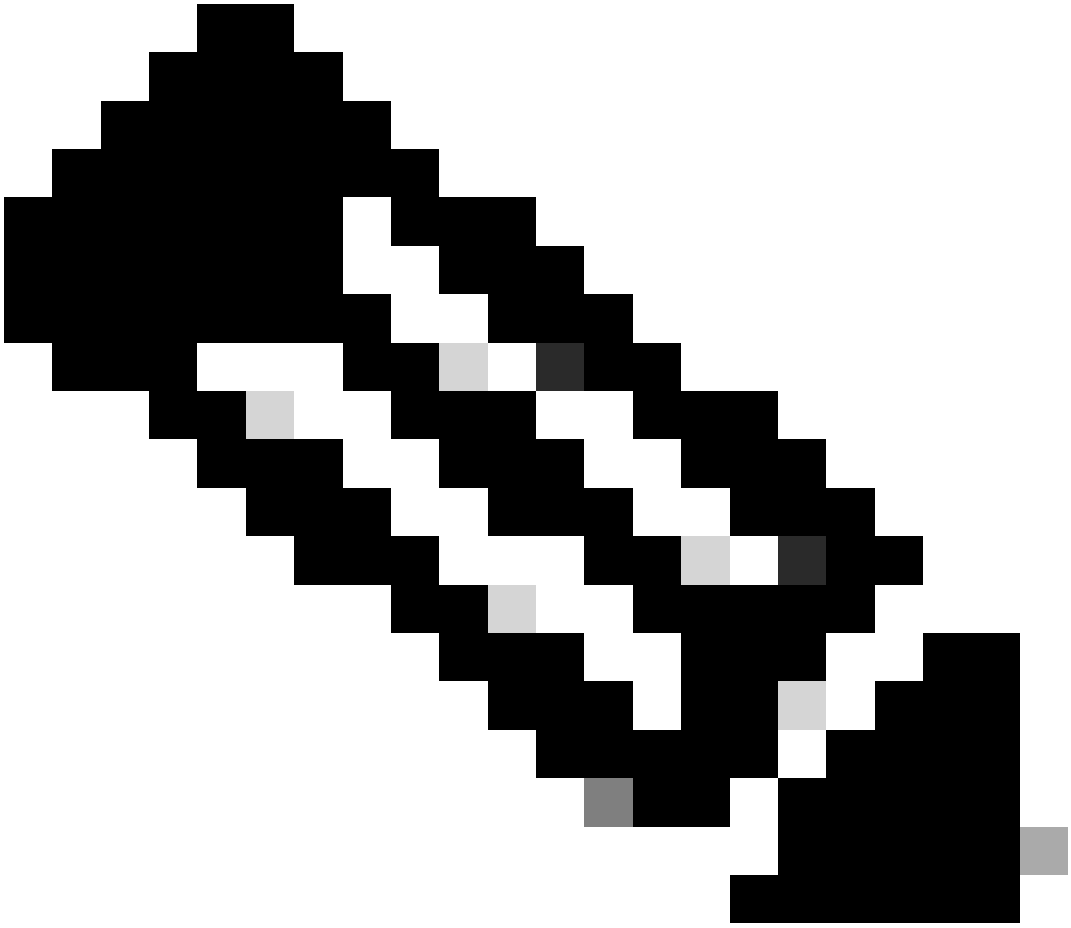


附註：如果此處顯示您不希望在其上實施策略的域，您還可以修改此目標清單。選擇刪除圖示以刪除域。

觀察在「稽核模式」下新增到Check Point安全類別的事件

下一步是觀察和稽核新增到您的新Check Point安全類別的事件。

Check Point裝置中的事件開始填充特定目標清單，該清單可以作為Check Point安全類別應用於策略。預設情況下，目標清單和安全類別處於「稽核模式」，不應用於任何策略，並且不能導致對現有Cisco Umbrella策略進行任何更改。



附註：根據您的部署配置檔案和網路配置，可以啟用「稽核模式」，無論需要多長時間。

檢視目標清單

您可以隨時在Cisco Umbrella中檢視Check Point Destination List:

1.定位至策略>策略元件>整合。

2.展開表中的Check Point，然後選擇See Domains。

檢視策略的安全設定

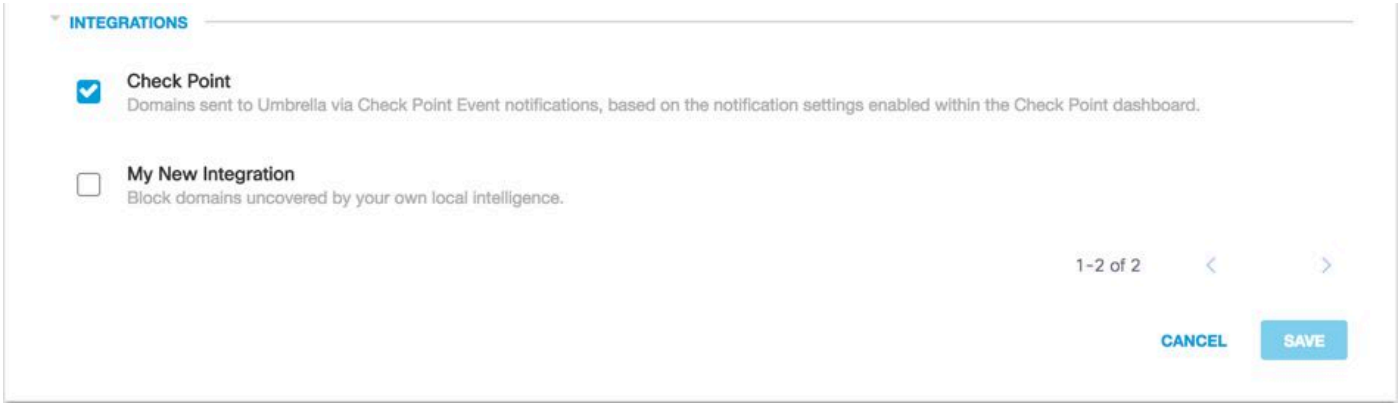
您可以檢視可在Cisco Umbrella中隨時為策略啟用的安全設定：

1.導航至策略>策略元件>安全設定。

2.選擇表中的安全性設定將其展開。

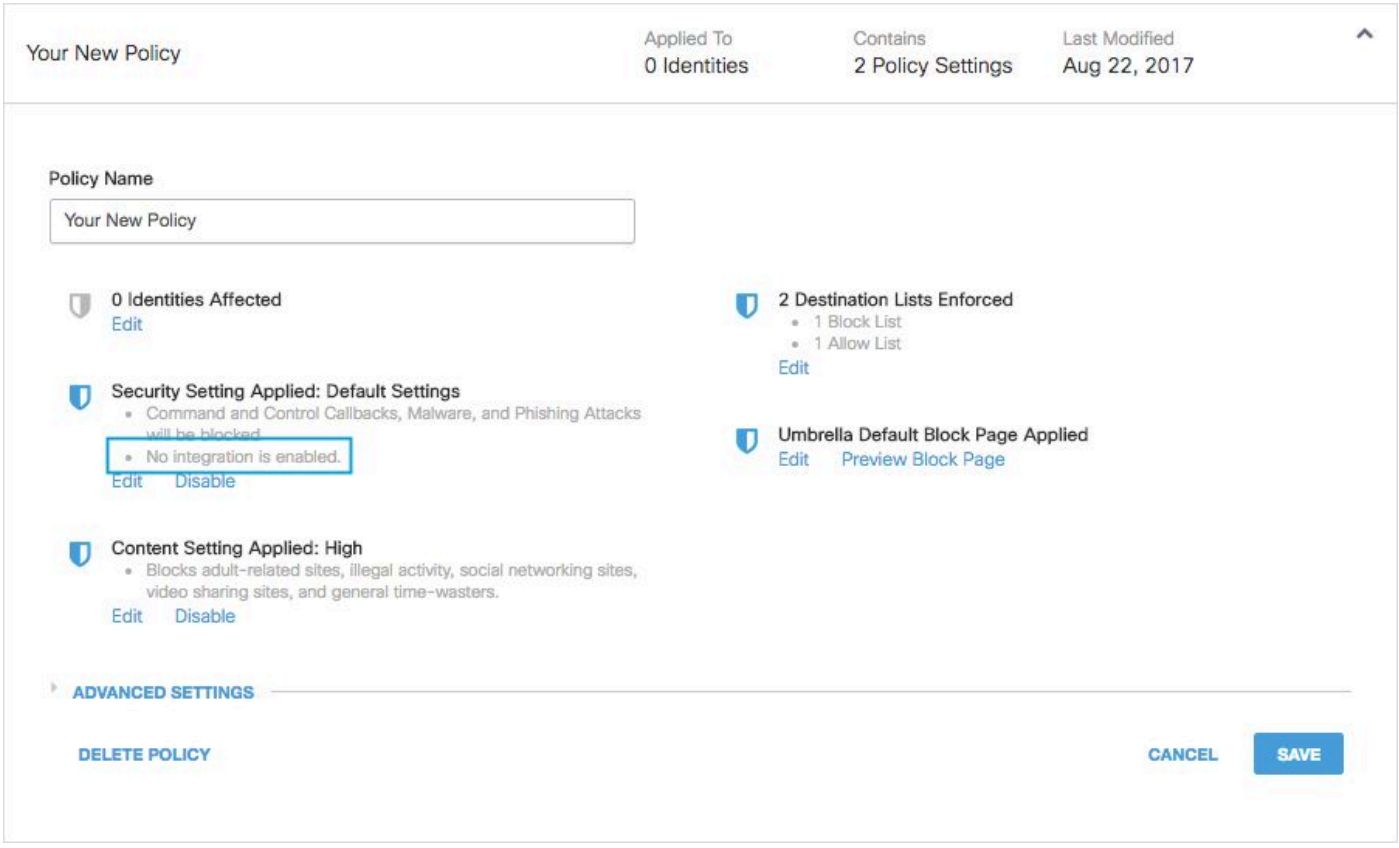
3.滾動至整合部分，然後展開該部分以顯示Check Point整合。

4.為「檢查點」整合選項，然後選擇「儲存」。



115013984226

您還可以通過「安全設定摘要」頁檢視整合資訊：



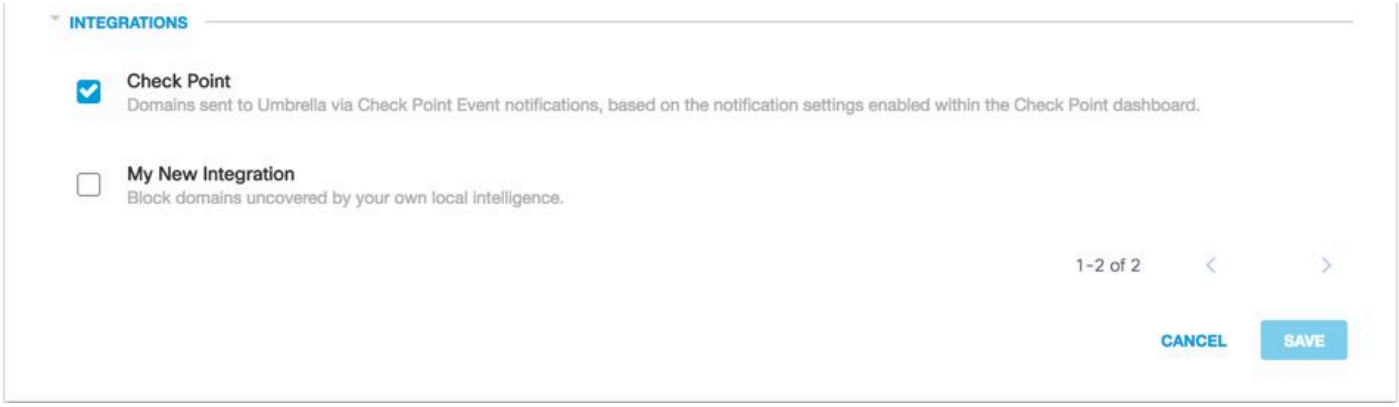
19916943300244

將「阻止模式」下的Check Point安全設定應用於託管客戶端的策略

當您準備好讓這些附加安全威脅由Cisco Umbrella管理的客戶端實施後，請更改現有策略的安全設定，或建立位於預設策略上方的新策略，以確保首先實施該策略：

1.確保Check Point整合仍按上一節中的步驟啟用。導航到Policies > Policy Components > Security Settings，然後開啟相關設定。

2.在Integrations下，驗證是否選擇了Check Point選項。否則，請選擇該選項並選擇儲存。



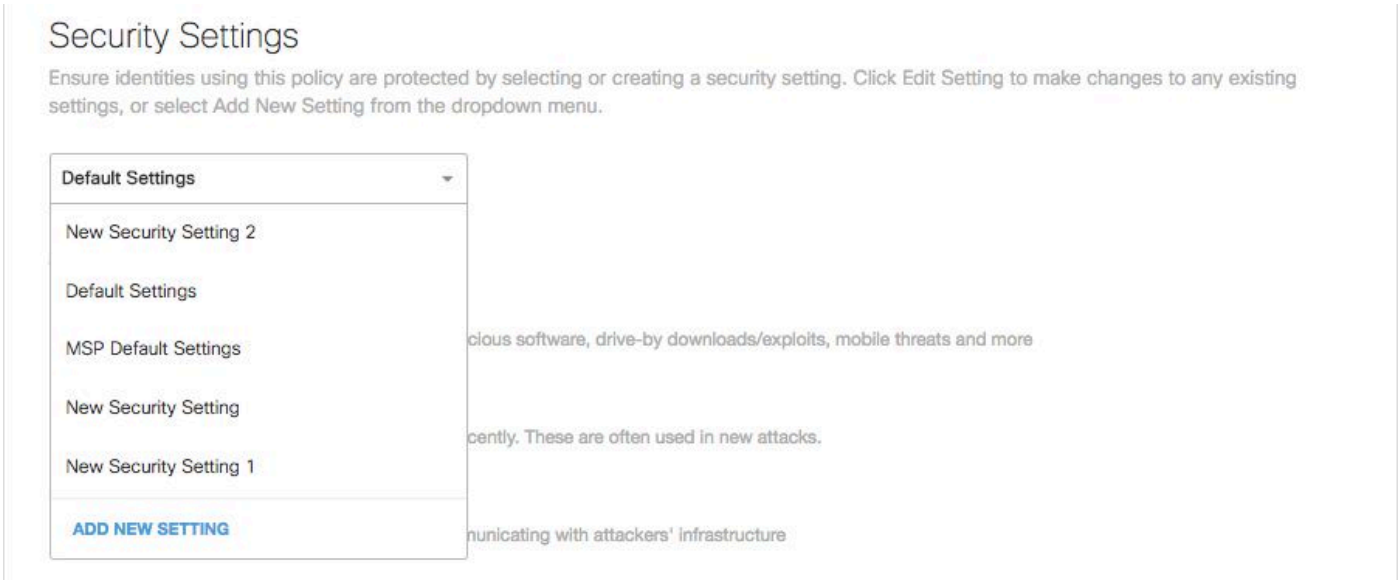
115013984226

接下來，在Cisco Umbrella策略嚮導中，將此安全設定新增到正在編輯的策略中：

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

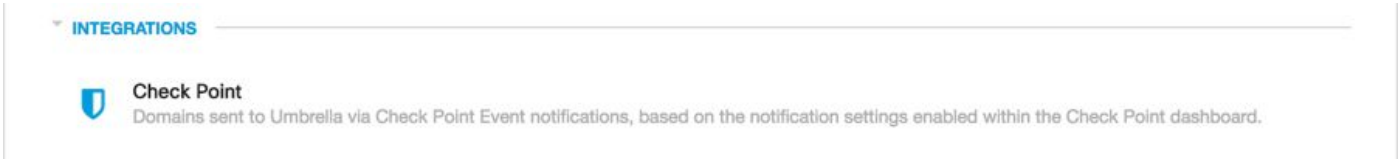
2.展開策略，然後在Security Setting Applied（DNS策略）或Security Settings（Web策略）下選擇Edit。

3.在「安全設定」下拉選單中，選擇包含「檢查點」設定的安全設定。



19916943316884

「整合」(Integrations)下的遮蔽圖示將更新為藍色。



115014149783

4.選擇Set & Return（DNS策略）或Save（Web策略）。

然後，可以使用策略為這些身份阻止Check Point的安全設定中包含的Check Point域。

在Umbrella內報告Check Point事件

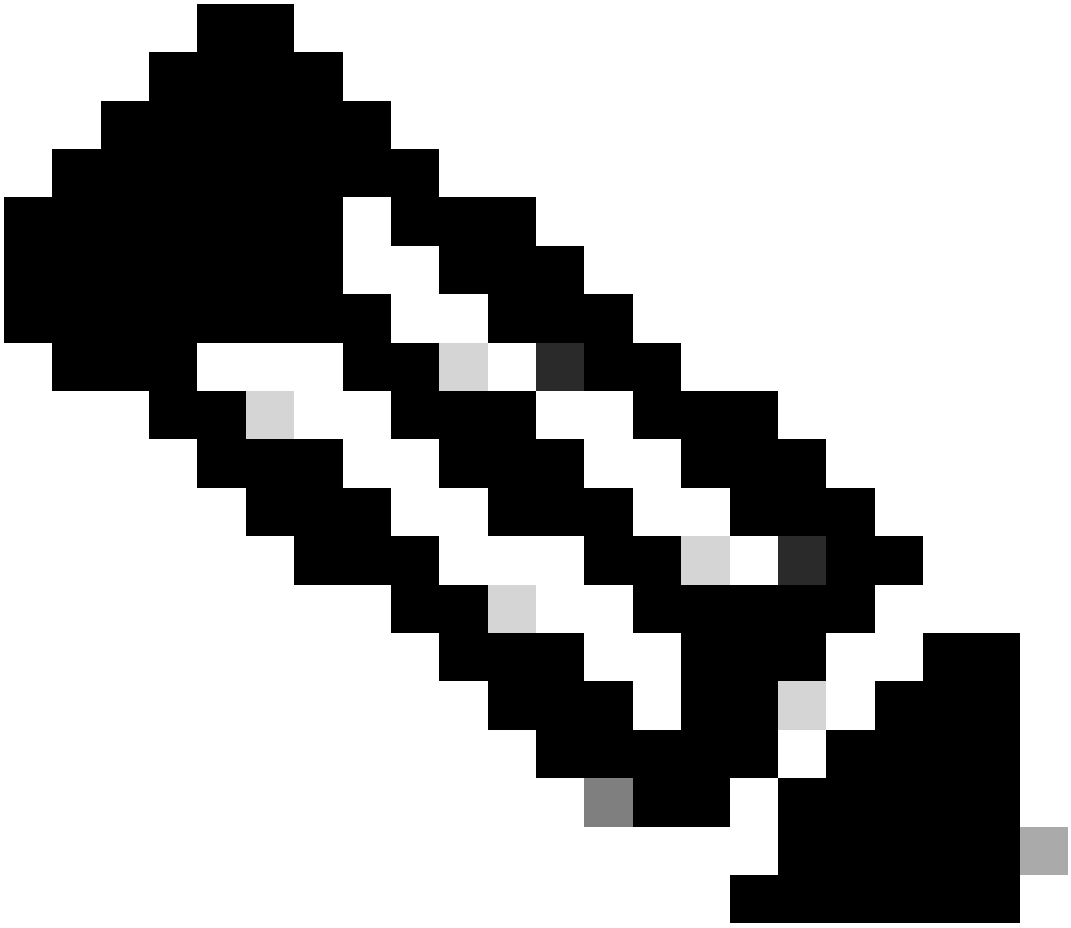
報告Check Point安全事件

Check Point Destination List是報告可用的安全類別之一。大多數或全部報告使用安全類別作為過濾器。例如，您可以過濾安全類別，以便只顯示Check Point相關的活動：

1.定位至報告>核心報表>活動搜尋。

2.在安全類別下，選擇檢查點以篩選報表，以便僅顯示「檢查點」的安全類別。

115014197623



附註：如果Check Point整合被禁用，則它不能出現在Security Categories篩選器中。

3.選擇應用以檢視報表中所選期間的「檢查點」相關活動。

報告將域新增到檢查點目標清單的時間

Cisco Umbrella Admin Audit日誌在檢查點裝置向目標清單新增域時包含其中的事件。這些域似乎通過「Check Point account」（檢查點帳戶）標籤新增到稽核日誌的User列下。

要查詢Umbrella Admin Audit日誌，請導航到Reporting > Admin Audit Log。

要報告何時新增域，請對Check Point Block List應用Filter by Identities & Settings過濾器，篩選為僅包括Check Point更改。

運行報告後，您可以看到新增到Check Point目標清單的域清單。

處理不需要的檢測或誤報

管理用於不需要的檢測的允許清單

儘管可能性不大，但您的Check Point裝置自動新增的域可能會觸發不需要的阻止，從而阻止您的使用者訪問特定網站。在這種情況下，Cisco Umbrella建議將網域新增到允許清單中，此清單優先於所有其他型別的封鎖清單，包括安全設定。當兩個域中都存在域時，允許清單優先於阻止清單。

這一方法更受歡迎的原因有兩個：

- 首先，如果Check Point裝置在域被移除後要重新新增域，則允許清單可防止出現進一步的問題。
- 其次，允許清單顯示有問題的域的歷史記錄，以供以後的調查分析或審計報告使用。

預設情況下，全域性允許清單應用於所有策略。將域新增到全域性允許清單會導致在所有策略中允許該域。

如果阻止模式中的Check Point Security Setting in Block僅應用於受管Cisco Umbrella標識的子集（例如，它僅適用於漫遊電腦和流動裝置），則可以為這些標識或策略建立特定的允許清單。

要建立允許清單，請執行以下操作：

1.定位至策略>目標清單，然後選擇新增圖示。

2.選擇Allow，然後將您的域新增到清單中。

3.選擇儲存。

儲存該清單後，可以將其新增到一個現有策略中，該策略將覆蓋那些受到該不需要的阻止影響的客戶端。

從檢查點目標清單中刪除域

在Check Point目標清單中的每個域名旁邊都有一個Delete圖示。通過刪除域，可以在出現不需要的檢測時清除Check Point目標清單。

但是，如果Check Point裝置將域重新傳送到Cisco Umbrella，則刪除操作不是永久性的。

刪除域：

1.定位至「設置」>「整合」，然後選擇「檢查點」將其展開。

2.選擇檢視域。

3.搜尋要刪除的域名。

4.選擇刪除圖示。

5.選擇關閉。

6.選擇「儲存」。

如果檢測到不需要的檢測或誤報，Cisco Umbrella建議立即在Cisco Umbrella中建立允許清單，然後在Check Point Appliance中修正誤報。稍後，您可以從Check Point目標清單中刪除該域。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。