Check Pointアンチボットソフトウェアブレードを使用したUmbrellaの設定

内容

はじめに

このドキュメントでは、Cisco UmbrellaをCheck Point Anti-Botソフトウェアブレードと統合する方法について説明します。

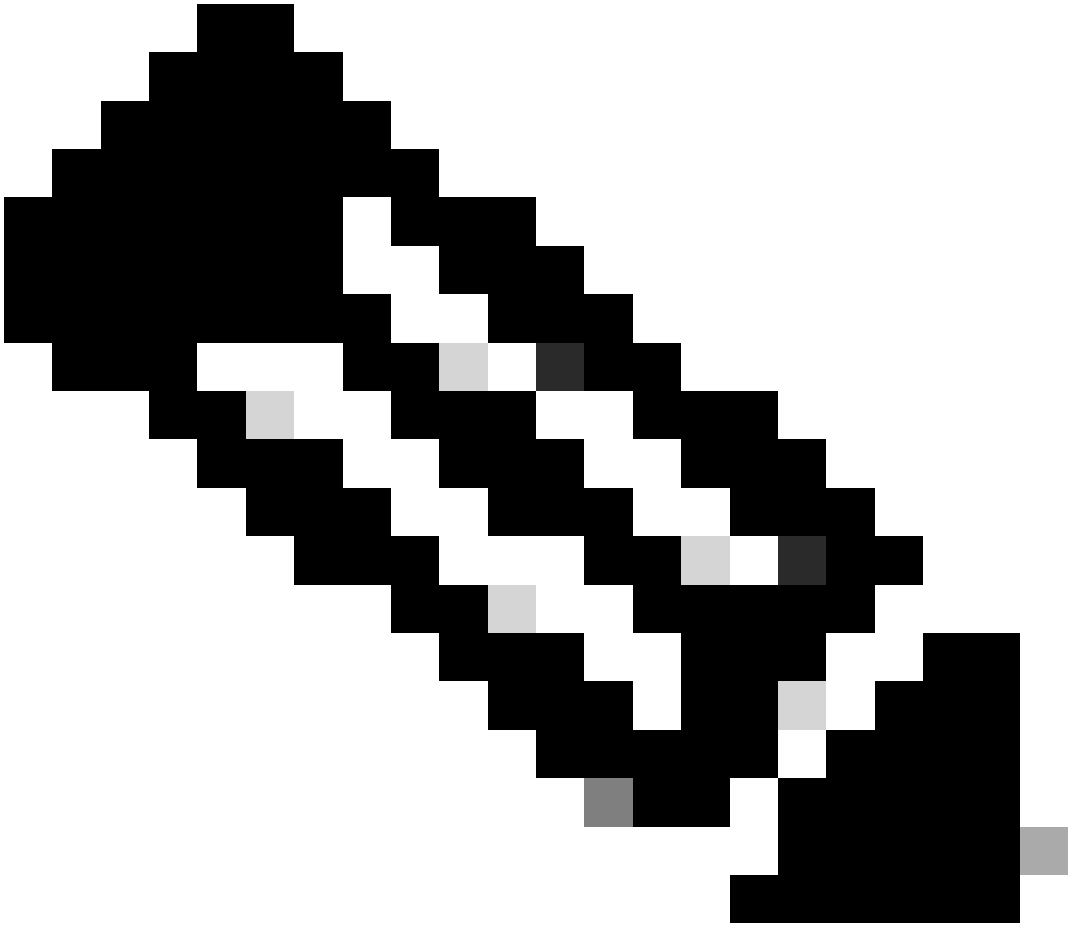
前提条件

要件

次の項目に関する知識があることが推奨されます。

- アンチボットソフトウェアブレードを備えたCheck Pointデバイス

- Check Pointソフトウェアバージョン R80.40以降
- Check Pointデバイスが「https://s-platform.api.opendns.com」に対して発信HTTP要求を実行できることを確認します。
- DNS Essentials、DNS Advantage、SIG Essentials、SIG AdvantageなどのCisco Umbrellaパッケージ
- Cisco Umbrellaダッシュボードの管理者権限



注：Check Pointの統合は、DNS Essentials、DNS Advantage、SIG Essentials、またはSIG AdvantageなどのCisco Umbrellaパッケージにのみ含まれています。これらのパッケージを所有しておらず、Check Point統合を希望する場合は、Cisco Umbrellaアカウントマネージャにお問い合わせください。正しいCisco Umbrellaパッケージがあっても、ダッシュボードの統合としてCheck Pointが表示されない場合は、Cisco Umbrellaサポートにお問い合わせください。

使用するコンポーネント

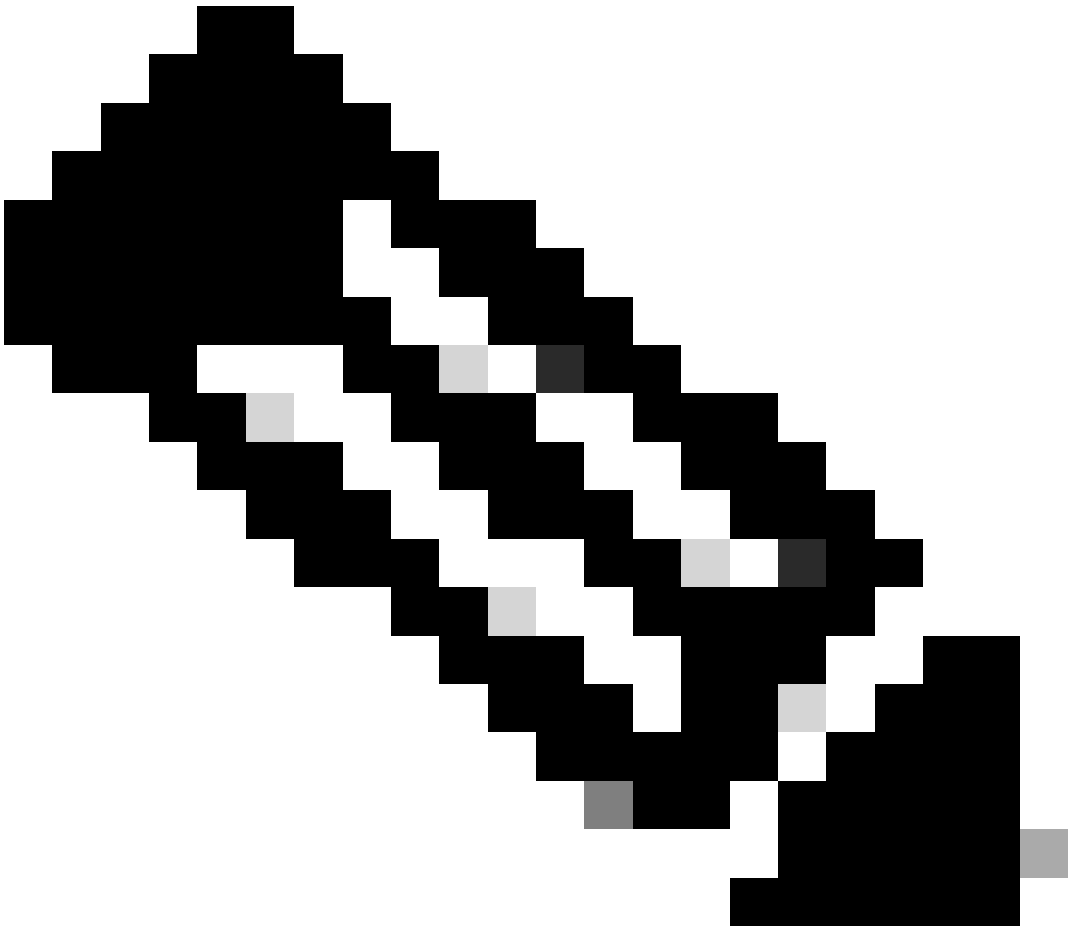
このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Cisco UmbrellaとCheck Point Anti-Bot Software Bladeの統合により、Check Pointデバイスは、検査しているネットワークトラフィック内の脅威を検出した場合、Cisco UmbrellaにAnti-Bot Software Bladeアラートを送信できます。Cisco Umbrellaが受信したアラートにより、ブロックリストが構築され、Check Point Anti-Bot Software Bladeで保護されていないローミング中のラップトップ、タブレット、および電話ネットワークを保護できます。

この記事では、アンチボットソフトウェアブレードのアラートをCisco Umbrellaに送信するようにCheck Pointデバイスを設定する手順について説明します。



注：この統合は、R80.40で最初にリリースされた後、バージョンR81.20のCheck Pointで廃止されました。

機能

Cisco UmbrellaとCheck Point Anti-Bot Software Bladeアプライアンスの統合により、検出された脅威（マルウェアをホストするドメイン、ボットネットのコマンドと制御、フィッシングサイトなど）がCisco Umbrellaにプッシュされ、グローバルに適用されます。

その後、Cisco Umbrellaは脅威を検証し、ポリシーに追加できることを確認します。Check Point Anti-Bot Software Bladeからの情報が脅威であることが確認されると、任意のCisco Umbrellaポリシーに適用できるセキュリティ設定の一部として、ドメインアドレスがCheck Point Destination Listに追加されます。このポリシーは、そのポリシーに割り当てられたデバイスから行われたすべての要求に対して即座に適用されます。

今後、Cisco UmbrellaはCheck Pointアラートを自動的に解析し、悪意のあるサイトをCheck Point Destination Listに追加します。これにより、すべてのリモートユーザとデバイスに対してCheck Point保護が拡張され、企業ネットワークに対してもう1つの適用レイヤが提供されます。

設定手順

統合を設定するには、次の手順を実行します。

1. Cisco Umbrellaの統合を有効にして、カスタムスクリプトでAPIトークンを生成します。
2. APIトークンとカスタムスクリプトをCheck Pointアプライアンスに展開します。
3. Check Pointアラートを作成/編集して、この新しいスクリプトに投稿します。
4. Cisco Umbrella内でCheck Pointイベントがブロックされるように設定します。

サービス中断の防止

不要なサービス中断を回避するため、Cisco Umbrellaでは、統合を設定する前に、ブロックされることのないミッションクリティカルなドメイン名(google.comやsalesforce.comなど)をグローバル許可リスト（またはポリシーに従ったその他の宛先リスト）に追加することを推奨しています。

ミッションクリティカルなドメインには、次のものが含まれます。

- 組織のホームページ
- 内部レコードと外部レコードの両方を持つことができる、提供するサービスを表すドメイン。たとえば、「mail.myservicedomain.com」や「portal.myotherservicedomain.com」などです。
- Cisco Umbrellaに依存しているあまり知られていないクラウドベースのアプリケーションは、ドメインの自動検証に含めることができません。例：「localcloudservice.com」。

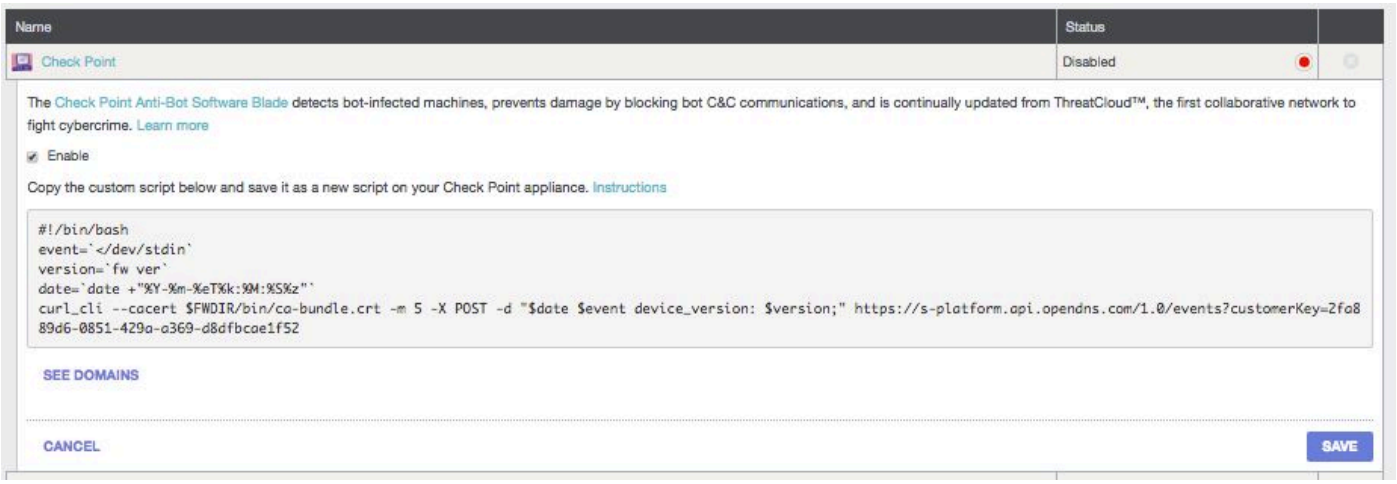
これらのドメインは、Cisco UmbrellaのPolicies > Destination ListsにあるGlobal Allow Listに追加する必要があります。

ステップ1:UmbrellaスクリプトとAPIトークンの生成

1. Cisco Umbrellaダッシュボードに管理者としてログインします。

2. 「ポリシー」>「ポリシー・コンポーネント」>「統合」に移動し、表の「チェック・ポイント」を選択して展開します。

3. 「使用可能」オプションを選択します。



4. 次の行からスクリプト全体をコピーします。

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

このスクリプトは、後の手順で使用できます。

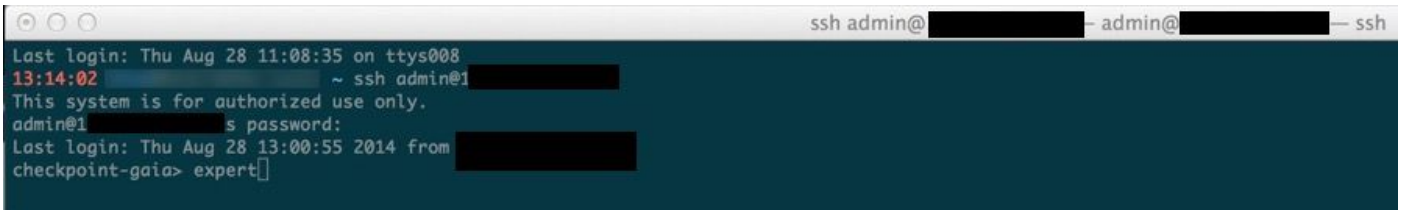
5. 「保存」を選択して統合を有効にします。

手順2: Check Pointアプライアンスにカスタムスクリプトを展開する

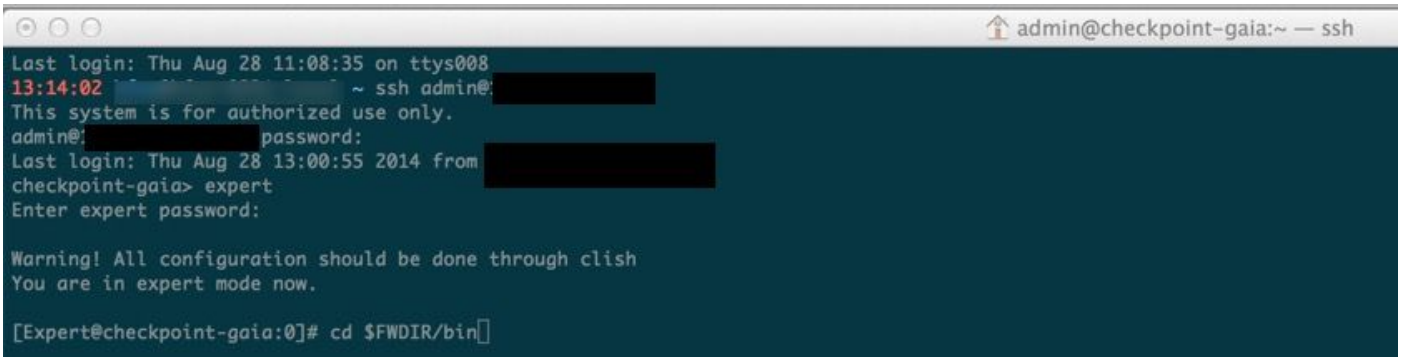
次の手順では、Check PointアプライアンスにカスタムCisco Umbrellaスクリプトをインストールし、SmartDashboardで有効にします。

1. カスタムスクリプトをインストールするには、管理者としてCheck PointアプライアンスにSSHで接続します。

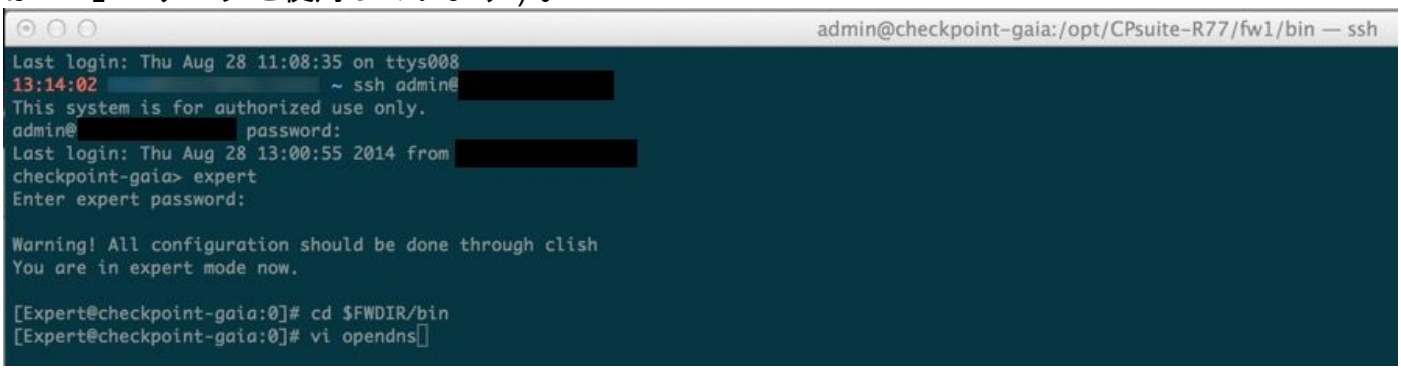
2. 次に、コマンドラインに「expert」と入力して「Expert Mode」を起動します。



3. 作業ディレクトリを$FWDIR/binに変更します。

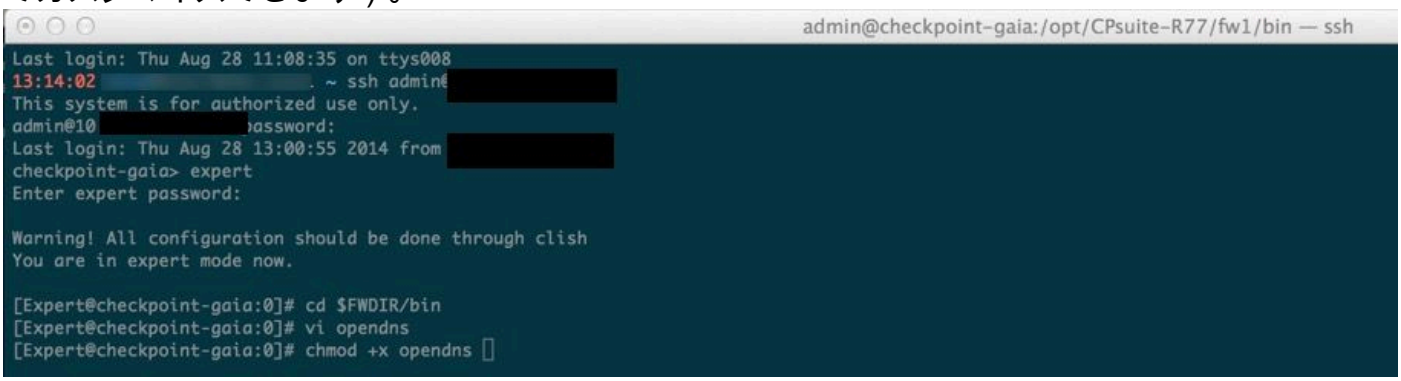


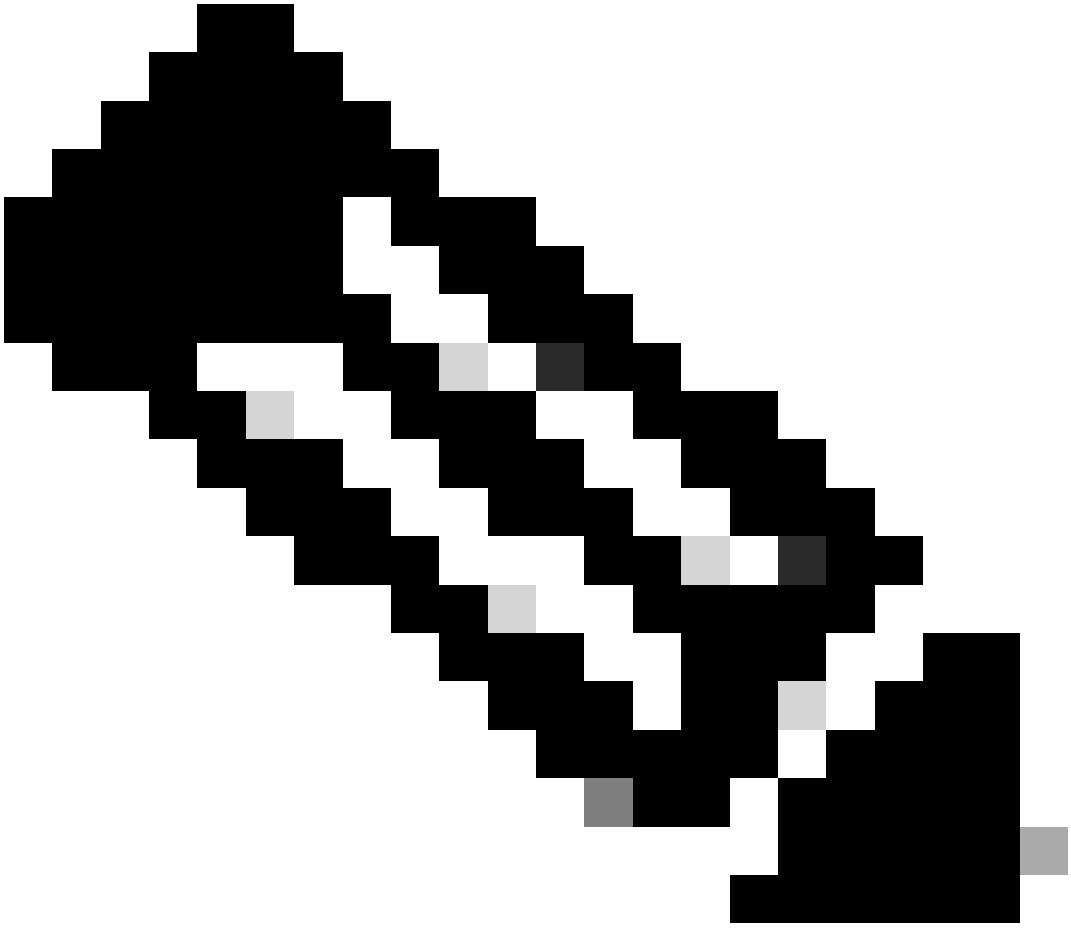
4. テキストエディタを使用して「opendns」という名前の新しいファイルを開きます（この例では「vi」エディタを使用しています）。



5. Cisco Umbrellaスクリプトをファイルに貼り付け、ファイルを保存して エディタを終了します。

6. chmod +x opendnsを実行して、カスタムのUmbrellaスクリプトを実行可能にします（必要に応じてカスタマイズできます）。



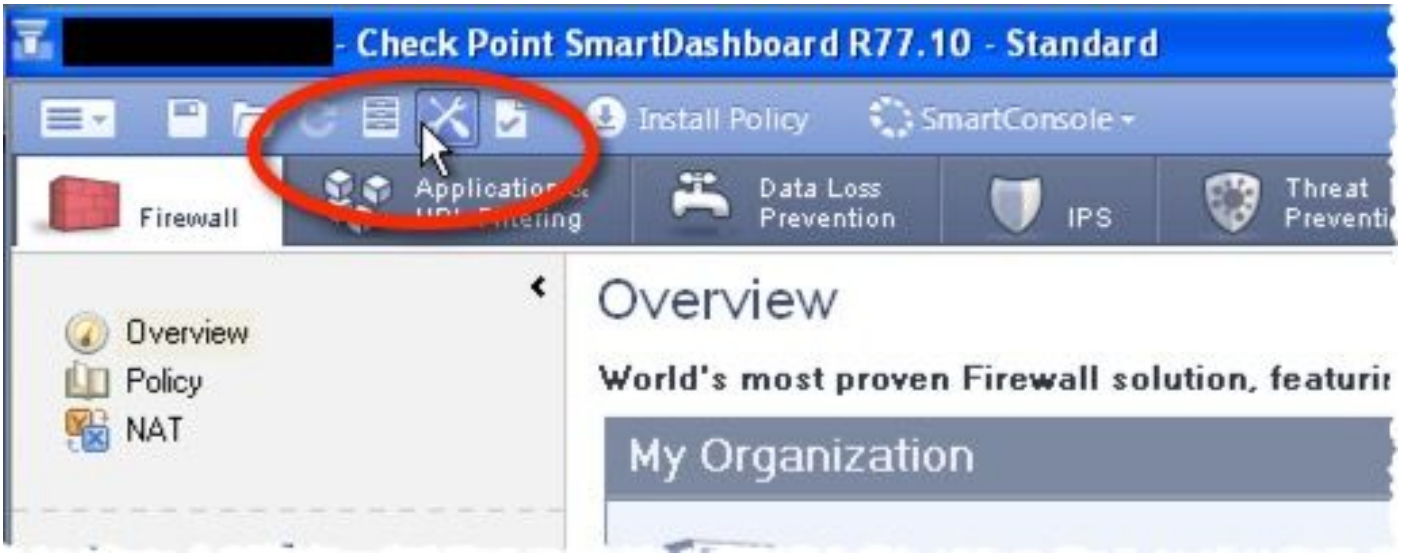


注：ブレードのバージョンをアップグレードまたは変更する場合は、新しいバージョンについてこれらの手順を繰り返す必要があります。

ステップ 3：新しいスクリプトに送信するチェックポイント・アラートの作成または編集

1. ログインしてSmartDashboardを起動し、SmartDashboardで新しいスクリプトをポストできるようにします。

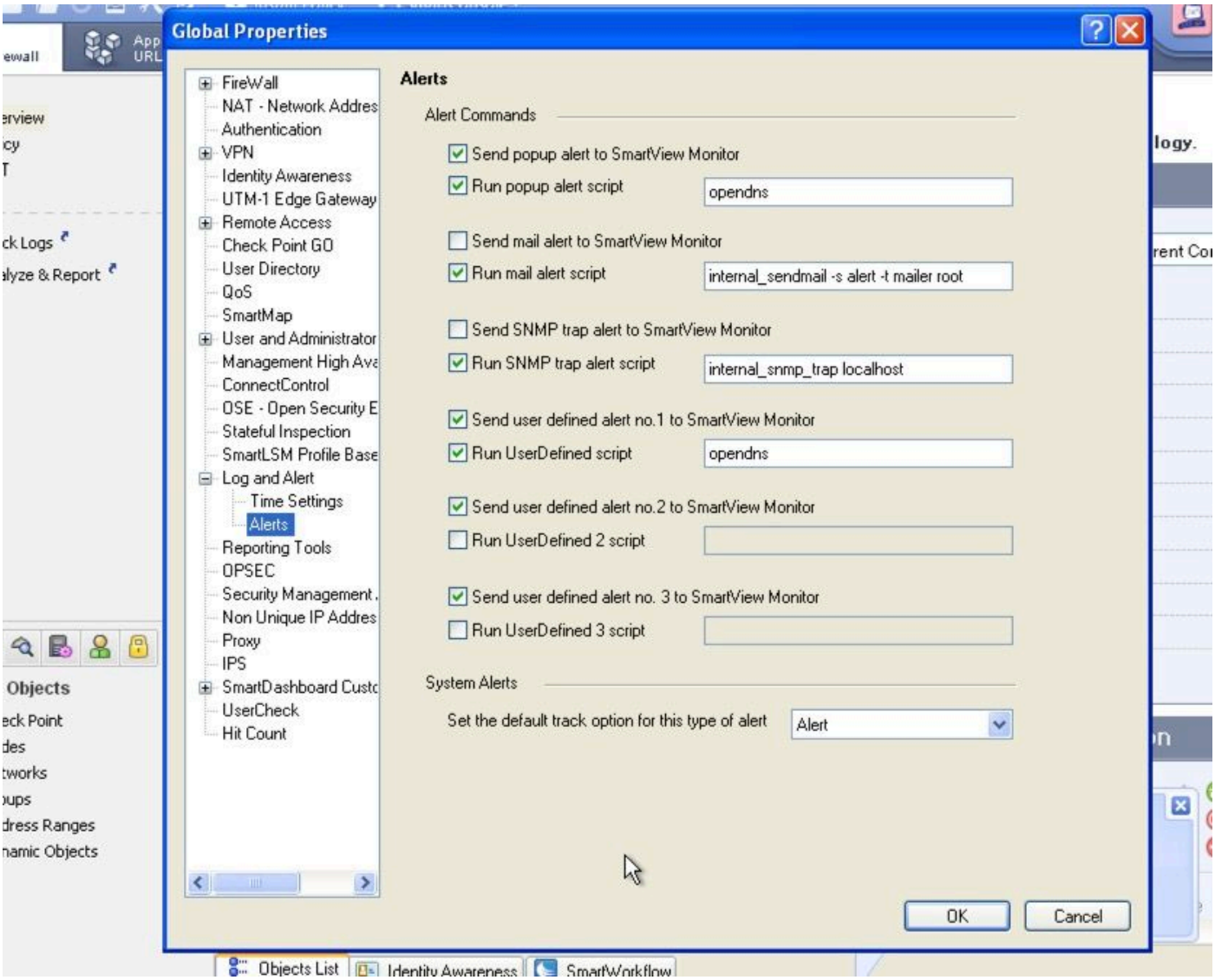
2. Global Propertiesを開きます。



3. Global Propertiesで、Log and Alert > Alertsの順に開き、次の手順を実行します。

- Send popup alertscriptおよびRun UserDefined scriptを選択します。
- 両方のスクリプトフィールドで「opendns」を定義します。

4. 「OK」を選択します。SmartDashboardで、更新したポリシーを保存してインストールします。



ステップ4：統合のテストおよびブロックするチェックポイントイベントの設定

最初に、Cisco Umbrellaダッシュボードに表示するテストアンチボットブレードイベントを生成します。

1. Check Pointアプライアンスで保護されているネットワーク上の任意のデバイスから、ブラウザに次のURLをロードします。

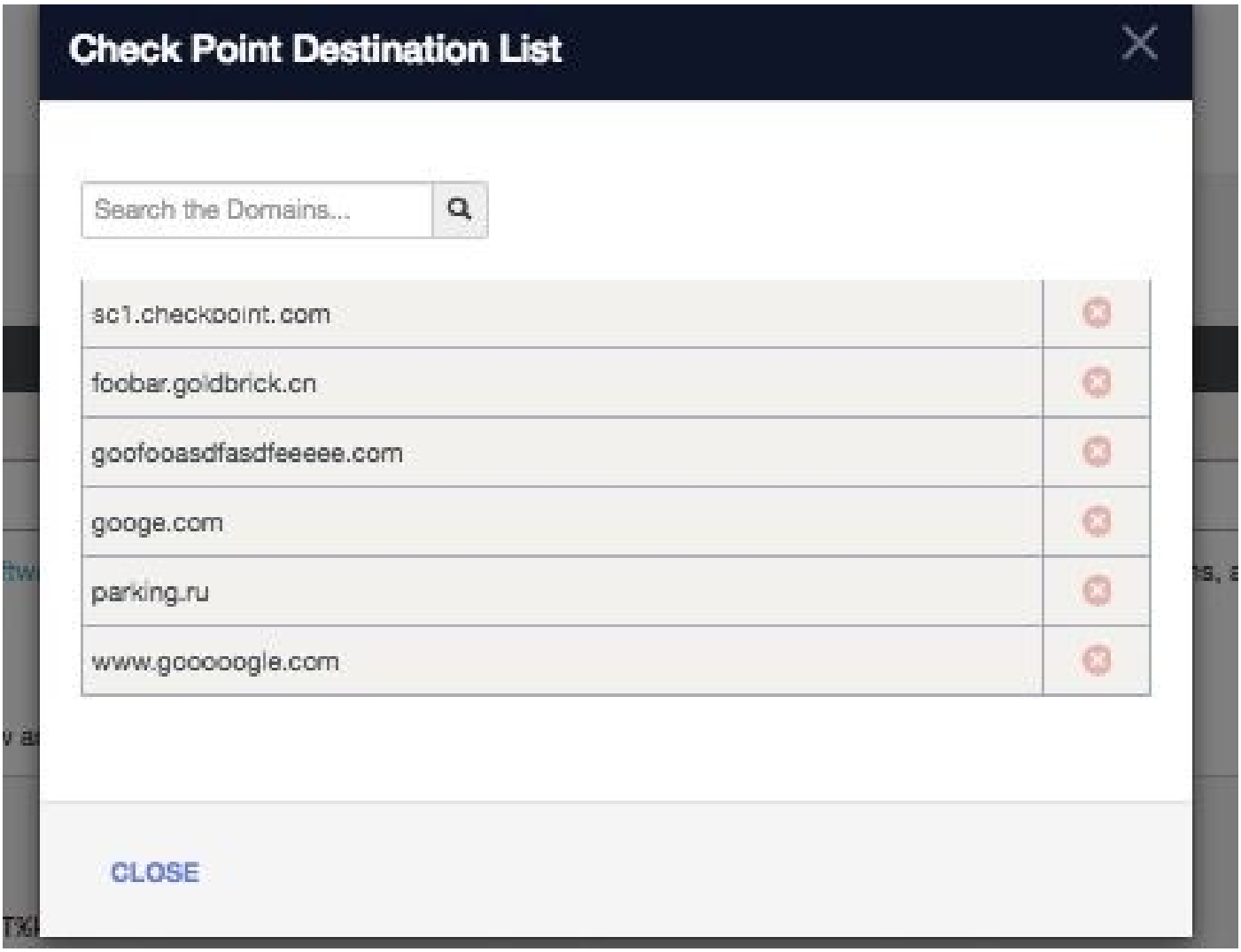
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

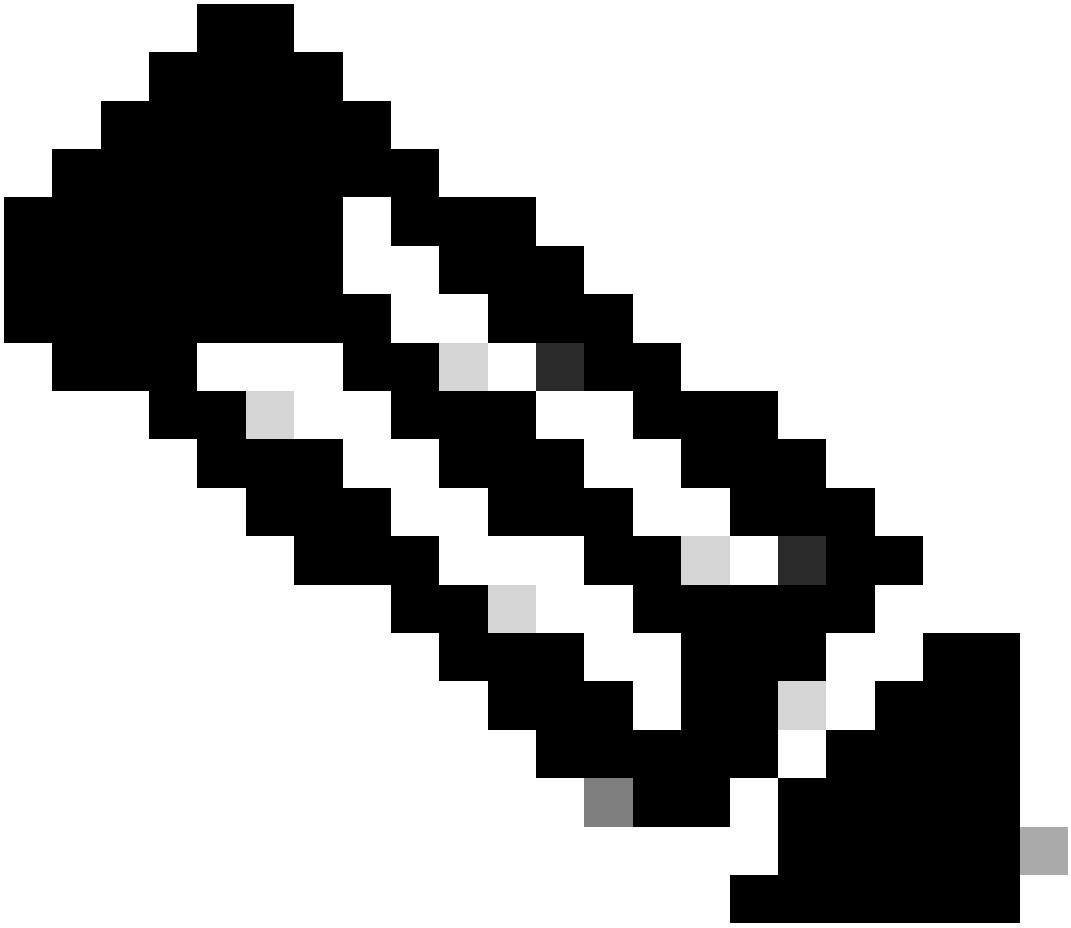
2. Cisco Umbrellaダッシュボードに管理者としてログインします。

3. 「ポリシー」>「ポリシー・コンポーネント」>「統合」に移動し、表の「チェック・ポイント」を選択して展開します。

4. 「ドメインを表示」を選択します。ウィンドウが開き、「sc1.checkpoint.com」を含むCheck Point Destination Listが表示されます。 その時点から、検索可能なリストにデータが入力され始

め、リストが拡大し始めます。



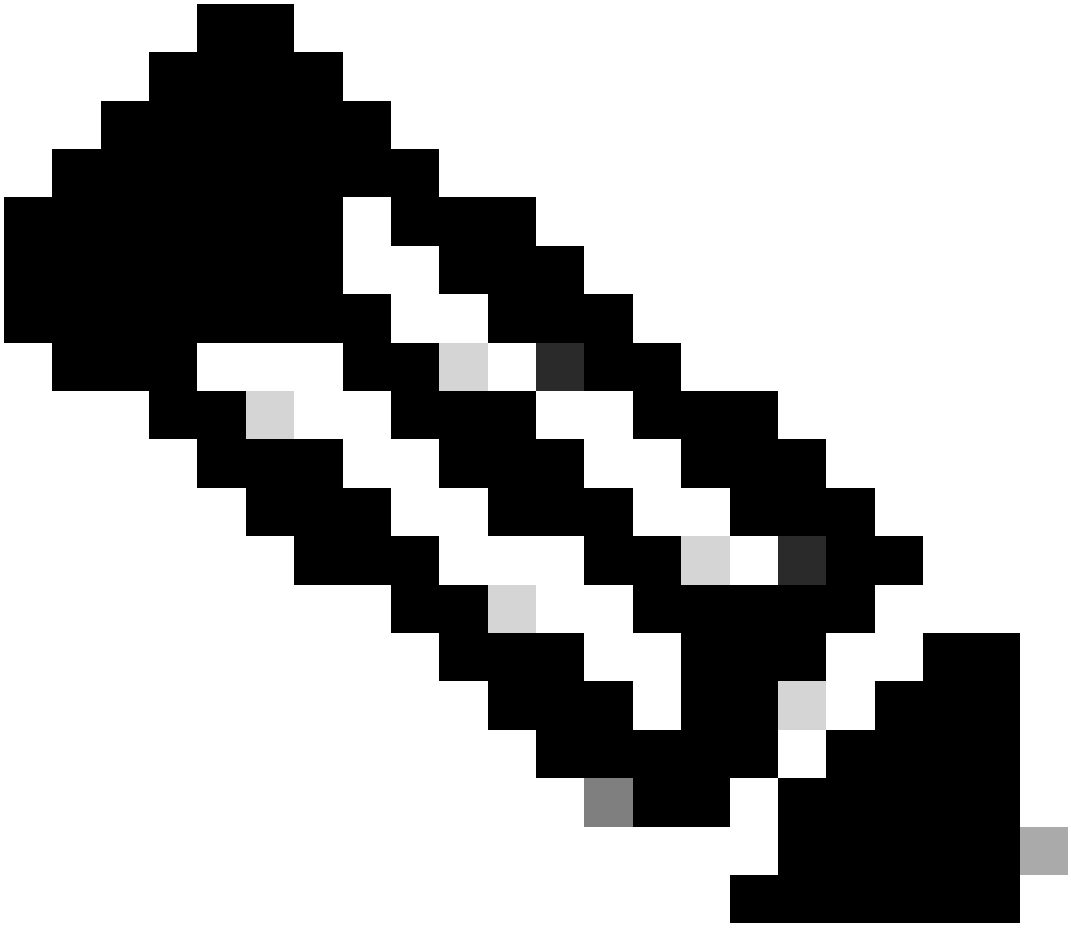


注：ポリシーを適用したくないドメインが表示されている場合は、この宛先リストを変更することもできます。削除アイコンを選択して、ドメインを削除します。

「監査モード」で「チェックポイント・セキュリティ」カテゴリに追加されたイベントの監視

次の手順では、新しいCheck Pointセキュリティカテゴリに追加されたイベントを確認し、監査します。

Check Pointアプライアンスからのイベントは、Check Pointセキュリティカテゴリとしてポリシーに適用できる特定の宛先リストの入力を開始します。デフォルトでは、宛先リストとセキュリティカテゴリは「監査モード」であり、ポリシーには適用されず、既存のCisco Umbrellaポリシーを変更することはできません。



注:「監査モード」は、導入プロファイルとネットワーク設定に基づいて、必要な期間だけ有効にできます。

宛先リストの確認

Check Point Destination Listは、Cisco Umbrellaでいつでも確認できます。

1. [ポリシー] > [ポリシーコンポーネント] > [統合] に移動します。

2. テーブルのCheck Pointを展開し、See Domainsを選択します。

ポリシーのセキュリティ設定の確認

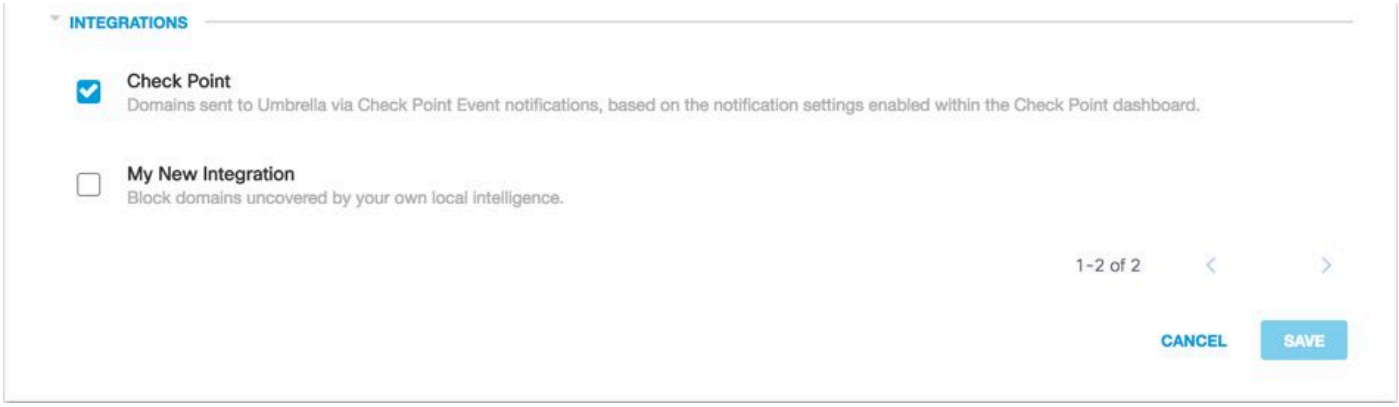
ポリシーに対して有効にできるセキュリティ設定は、Cisco Umbrellaでいつでも確認できます。

1. [ポリシー] > [ポリシーコンポーネント] > [セキュリティ設定] に移動します。

2. 表内のセキュリティ設定を選択して展開します。

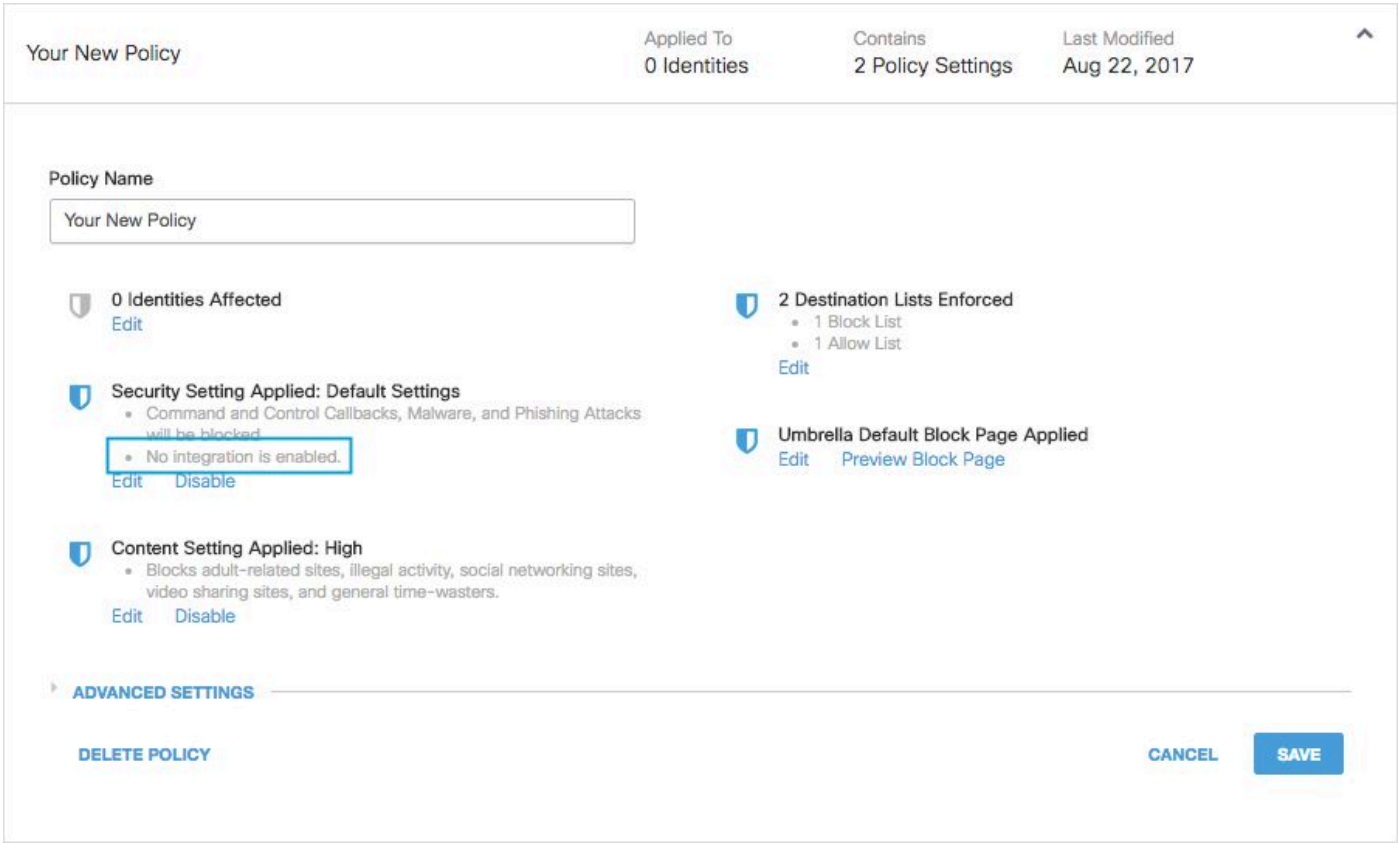
3. 「統合」セクションまでスクロールし、セクションを展開してCheck Point統合を表示します。

4. Check Point統合のオプションを選択し、Saveを選択します。



115013984226

統合情報は、「セキュリティ設定の概要」ページでも確認できます。



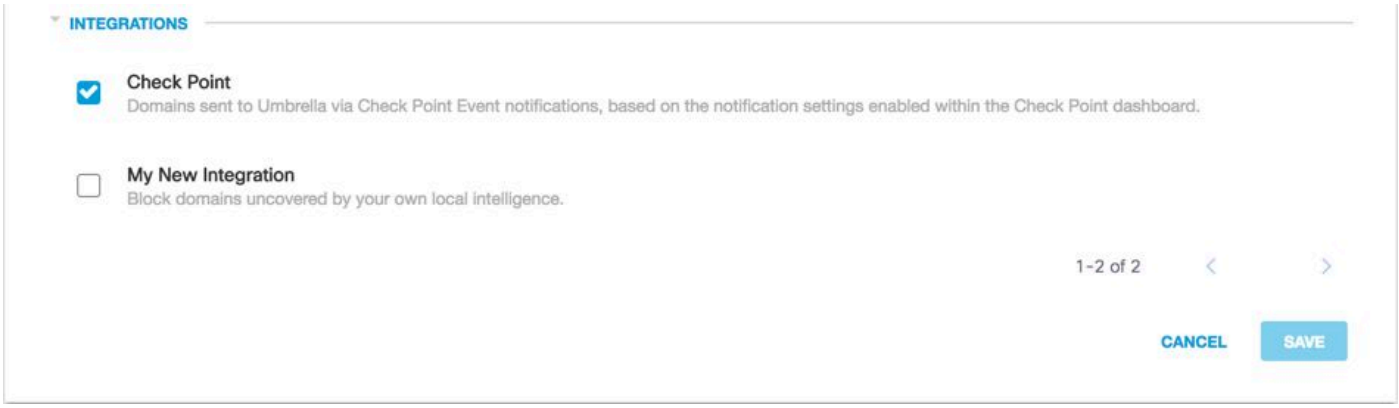
19916943300244

「ブロックモード」でのCheck Pointセキュリティ設定の管理対象クライアントのポリシーへの適用

Cisco Umbrellaで管理されるクライアントによってこれらの追加のセキュリティ脅威を適用する準備ができたら、既存のポリシーのセキュリティ設定を変更するか、デフォルトポリシーの上に配置する新しいポリシーを作成して、最初に適用されるようにします。

1. 前のセクションで行ったように、Check Point統合が引き続き有効になっていることを確認します。Policies > Policy Components > Security Settingsの順に移動し、関連する設定を開きます。

2. 「統合」で、「チェック・ポイント」オプションが選択されていることを確認します。保存されていない場合は、オプションを選択してSaveを選択します。



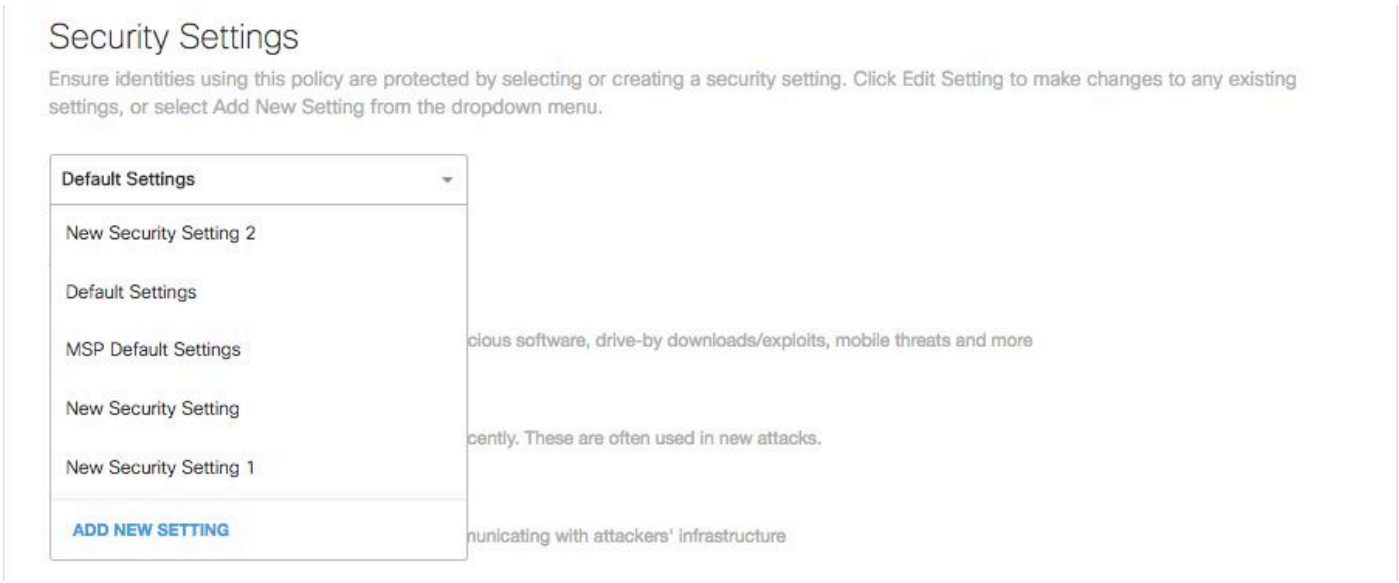
115013984226

次に、Cisco Umbrellaポリシーウィザードで、編集中のポリシーにこのセキュリティ設定を追加します。

1. ポリシー(Policies > DNS PoliciesまたはPolicies > Web Policy)に移動します。

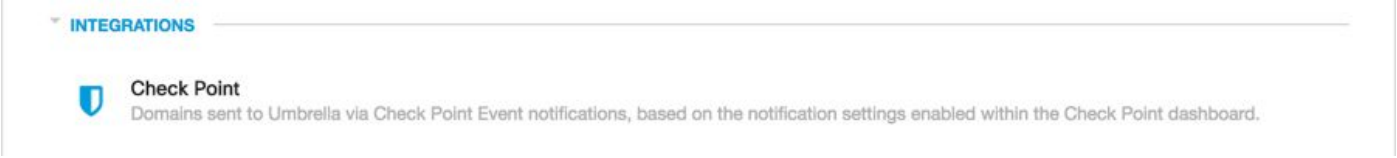
2. ポリシーを展開し、Security Setting Applied (DNS Policies)またはSecurity Settings (Web Policy)の下で、Editを選択します。

3. 「セキュリティ設定」ドロップダウンで、「チェック・ポイント」設定を含むセキュリティ設定を選択します。



19916943316884

「統合」の下のシールドアイコンが青色に更新されます。



115014149783

4. Set & Return(DNS Policies)またはSave(Web Policy)を選択します。

Check Pointのセキュリティ設定内に含まれるCheck Pointドメインは、ポリシーを使用してこれらのIDに対してブロックできます。

Check Pointイベントに関するUmbrella内のレポート

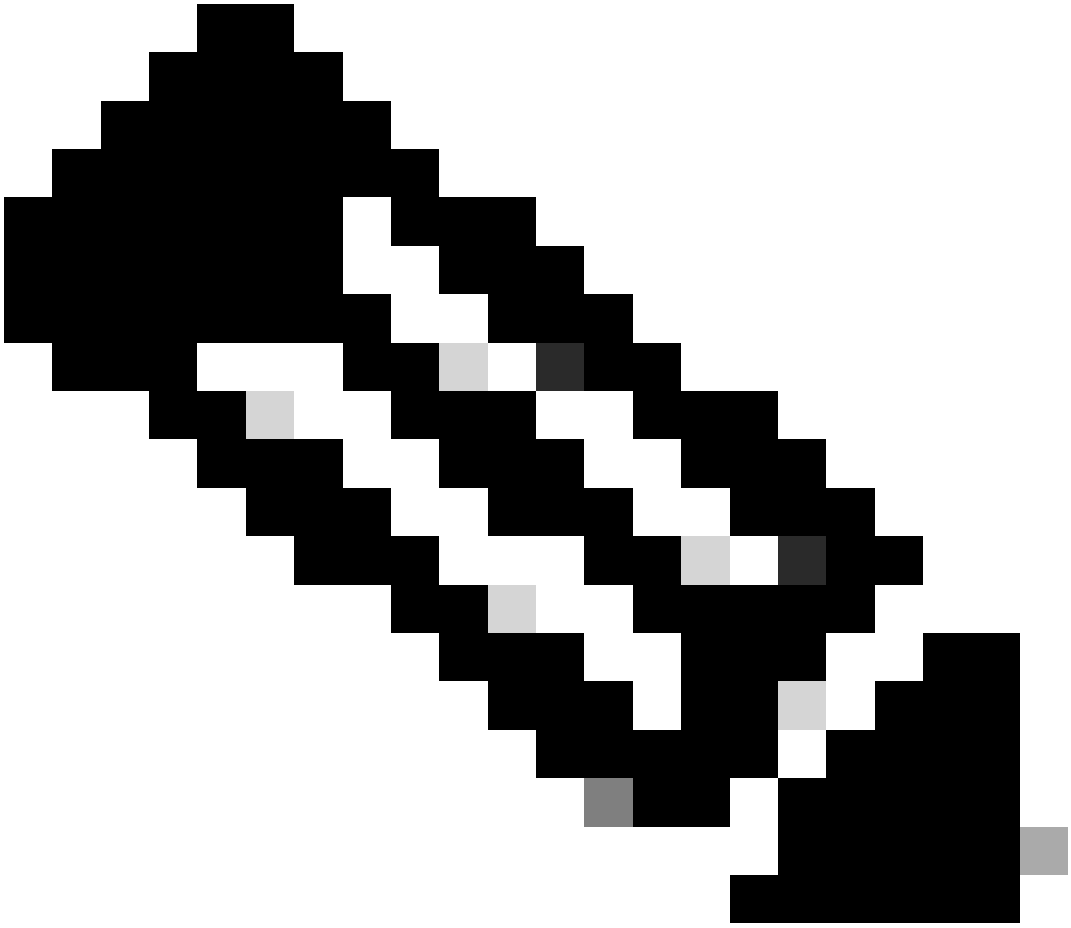
Check Pointセキュリティイベントのレポート

Check Point Destination Listは、レポートに使用できるセキュリティカテゴリの1つです。ほとんどのレポートまたはすべてのレポートでは、セキュリティカテゴリがフィルタとして使用されます。たとえば、セキュリティカテゴリをフィルタして、Check Point関連のアクティビティのみを表示できます。

1.「レポート」>「コア・レポート」>「活動検索」にナビゲートします。

2.「セキュリティ・カテゴリ」で、「チェック・ポイント」を選択して、レポートをフィルタし、「チェック・ポイント」のセキュリティ・カテゴリのみを表示します。

115014197623



注:Check Point統合が無効になっている場合は、[セキュリティカテゴリ]フィルタに表示されません。

3.「適用」を選択して、レポートで選択した期間のチェック・ポイント関連アクティビティを表示します。

Check Point宛先リストにドメインが追加されたときのレポート

Cisco Umbrella管理監査ログには、宛先リストにドメインを追加する際のCheck Pointアプライアンスからのイベントが含まれます。これらのドメインは、監査ログのUser列の下に、「Check Point account」ラベルが追加されているように見えます。

Umbrella管理監査ログを見つけるには、Reporting > Admin Audit Logの順に移動します。

ドメインがいつ追加されたかをレポートするには、[IDと設定によるフィルタ]フィルタを[CHECK POINTブロックリスト]に適用して、CHECK POINTの変更のみを含めるようにフィルタを適用します。

レポートを実行すると、Check Point宛先リストに追加されたドメインのリストが表示されます。

不要な検出や誤検出の処理

不要な検出の許可リストの管理

まれに、Check Pointアプライアンスによって自動的に追加されたドメインによって不要なブロックがトリガーされ、ユーザが特定のWebサイトにアクセスできなくなる可能性があります。このような状況では、Cisco Umbrellaは、許可リストにドメインを追加することを推奨します。許可リストは、セキュリティ設定を含む他のすべてのタイプのブロックリストよりも優先されます。ドメインが両方に存在する場合、許可リストはブロックリストよりも優先されます。

このアプローチが推奨される理由は、次の2つです。

- まず、Check Pointアプライアンスがドメインの削除後にドメインを再度追加する場合、許可リストは、この問題を引き起こすさらなる問題に対する防御策となります。
- 2番目に、許可リストは、後の調査または監査レポートで問題のあるドメインの履歴レコードを表示します。

デフォルトでは、すべてのポリシーに適用されるグローバル許可リストがあります。グローバル許可リストにドメインを追加すると、ドメインはすべてのポリシーで許可されます。

ブロックモードのCheck Pointセキュリティ設定が、管理対象のCisco Umbrellaアイデンティティのサブセットにのみ適用される（たとえば、ローミングコンピュータやモバイルデバイスにのみ適用される）場合、それらのアイデンティティまたはポリシーの特定の許可リストを作成できます。

許可リストを作成するには、次の手順を実行します。

1. Policies > Destination Listsの順に移動し、Addアイコンを選択します。

2. Allowを選択し、リストにドメインを追加します。

3. Saveを選択します。

リストを保存したら、不要なブロックの影響を受けるクライアントをカバーする既存のポリシーに追加できます。

チェックポイント宛先リストからのドメインの削除

Check Point宛先リストの各ドメイン名の横には、削除アイコンが表示されます。ドメインを削除

すると、不要な検出が発生した場合にチェックポイントの宛先リストをクリーンアップできます。

ただし、Check Pointアプライアンスがドメインをに再送信する場合、この削除は永続的にはありません。

ドメインを削除するには

1. 「設定」>「統合」に移動し、「チェック・ポイント」を選択して展開します。

2. 「ドメインを表示」を選択します。

3. 削除するドメイン名を検索します。

4. 「削除」アイコンを選択します。

5. Closeを選択します。

6. 「保存」を選択します。

不必要な検出または誤検出の場合、Cisco Umbrellaで即座に許可リストを作成し、Check Point Appliance内で誤検出を修復することをお勧めします。後で、Check Point宛先リストからドメインを削除できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。