Configurer le parapluie avec la lame logicielle Check Point Anti-Bot

Table des matières

Introduction

Ce document décrit comment intégrer Cisco Umbrella avec Check Point Anti-Bot Software Blade.

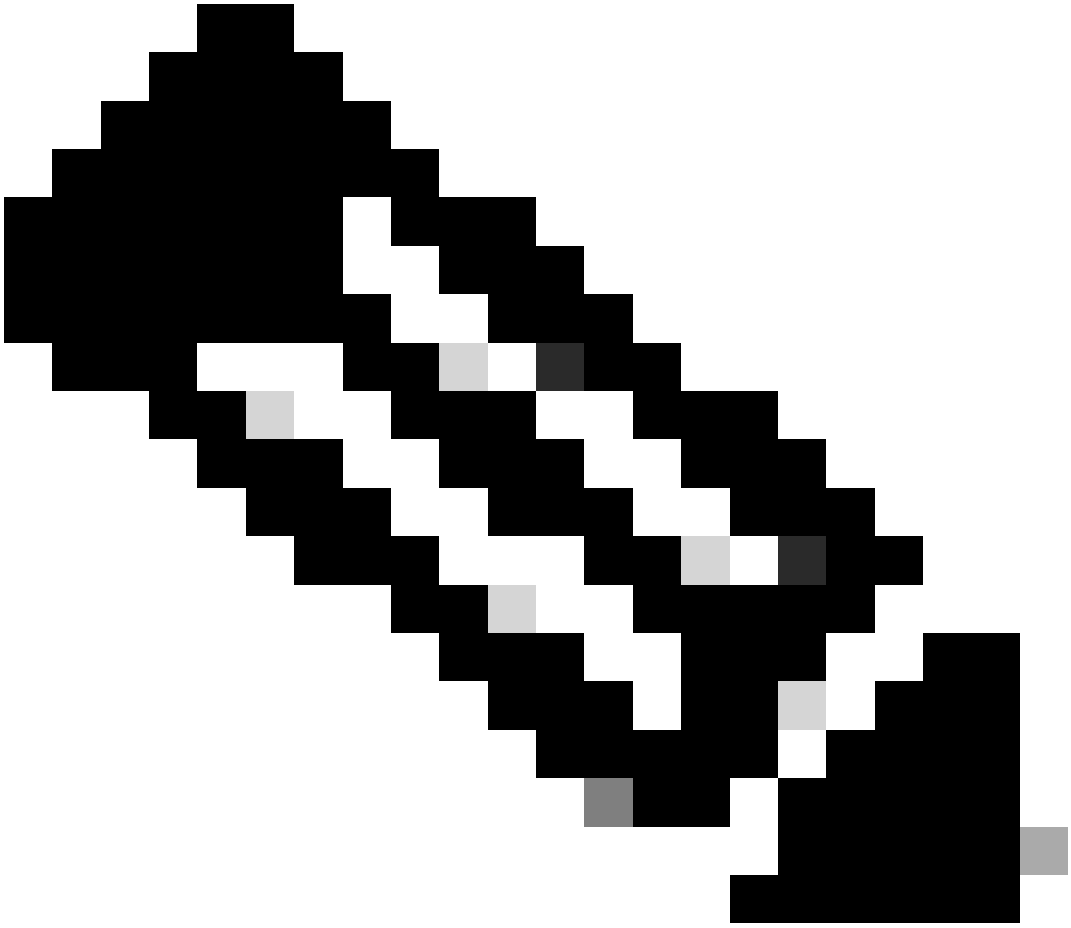
Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Périphérique Check Point avec la lame du logiciel anti-bot

- Logiciel Check Point version R80.40 ou ultérieure
- Assurez-vous que le périphérique Check Point peut effectuer des requêtes HTTP sortantes vers « https://s-platform.api.opendns.com ».
- Un package Cisco Umbrella comme DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage
- Droits d'administration de Cisco Umbrella Dashboard



Remarque : L'intégration Check Point est incluse uniquement dans les packages Cisco Umbrella tels que DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage. Si vous ne disposez pas de l'un de ces packages et souhaitez bénéficier de l'intégration Check Point, contactez votre responsable de compte Cisco Umbrella. Si vous disposez du package Cisco Umbrella approprié mais que Check Point ne s'affiche pas comme une intégration pour votre tableau de bord, contactez l'assistance Cisco Umbrella.

Composants utilisés

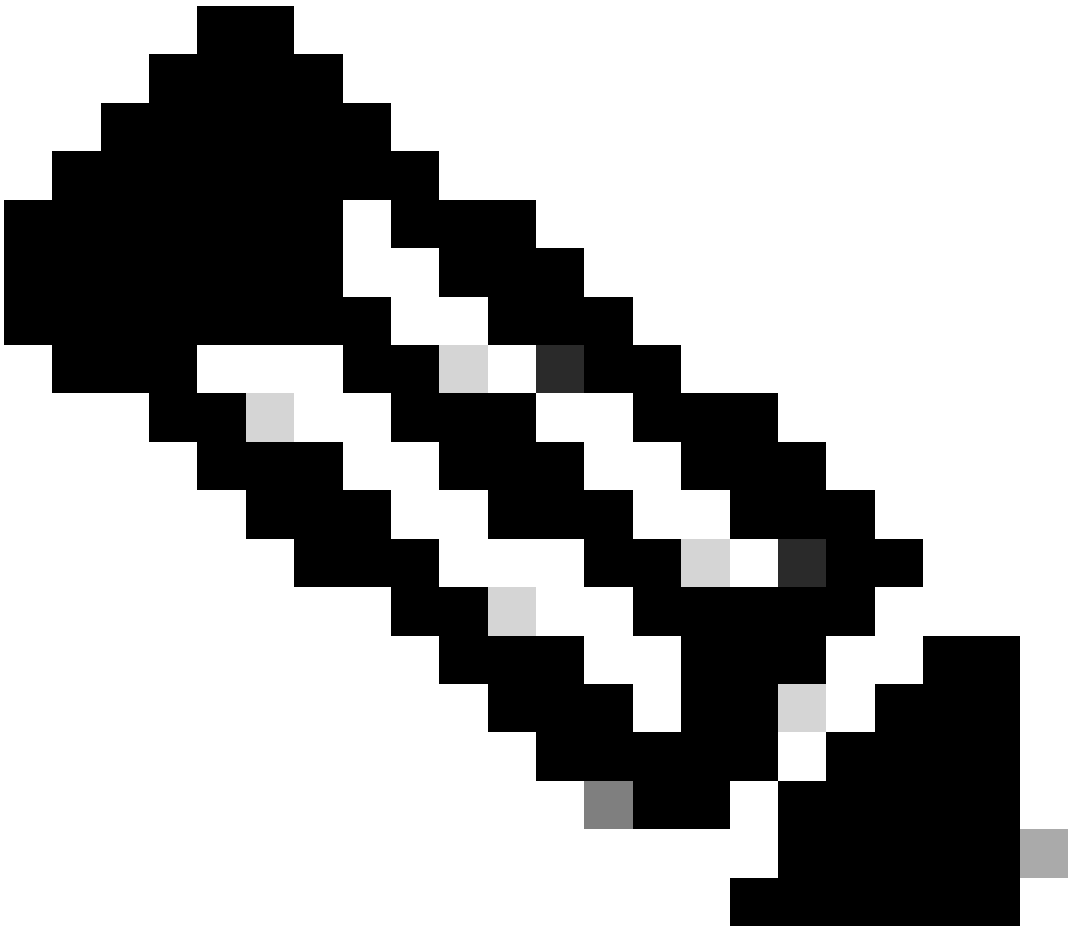
Les informations contenues dans ce document sont basées sur Cisco Umbrella.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

L'intégration de Cisco Umbrella avec la lame logicielle anti-bot Check Point permet à un périphérique Check Point d'envoyer ses alertes de lame logicielle anti-bot à Cisco Umbrella lorsque la lame détecte des menaces dans le trafic réseau qu'elle inspecte. Les alertes reçues par Cisco Umbrella constituent une liste de blocage capable de protéger les ordinateurs portables, tablettes et téléphones itinérants sur les réseaux non protégés par la lame logicielle Check Point Anti-Bot.

Cet article fournit des instructions pour configurer un périphérique Check Point afin d'envoyer des alertes de lames logicielles anti-bot à Cisco Umbrella.



Remarque : Cette intégration a été déconseillée par Check Point dans la version R81.20 après sa sortie initiale dans R80.40.

Fonctionnalité

L'intégration de Cisco Umbrella à l'appliance lame logicielle Check Point Anti-Bot repousse les menaces détectées (par exemple, les domaines hébergeant des programmes malveillants, la commande et le contrôle de botnets ou les sites d'hameçonnage) vers Cisco Umbrella pour une application globale.

Cisco Umbrella valide ensuite la menace pour s'assurer qu'elle peut être ajoutée à une stratégie. Si les informations de la lame logicielle anti-bot Check Point sont confirmées comme étant une menace, l'adresse de domaine est ajoutée à la liste de destination Check Point dans le cadre d'un paramètre de sécurité qui peut être appliqué à n'importe quelle stratégie Cisco Umbrella. Cette stratégie est immédiatement appliquée à toutes les requêtes effectuées à partir des périphériques affectés à cette stratégie.

Par la suite, Cisco Umbrella analyse automatiquement les alertes Check Point et ajoute les sites malveillants à la liste de destinations Check Point. Cela étend la protection Check Point à tous les utilisateurs et périphériques distants et fournit une autre couche d'application à votre réseau d'entreprise.

Configuration Steps

La configuration de l'intégration comprend les étapes suivantes :

1. Activez l'intégration dans Cisco Umbrella pour générer un jeton API avec un script personnalisé.
2. Déployez le jeton API et le script personnalisé sur l'appliance Check Point.
3. Créez/modifiez une alerte Check Point pour publier sur ce nouveau script.
4. Définissez les événements Check Point à bloquer dans Cisco Umbrella.

Empêcher les interruptions de service

Pour éviter les interruptions de service indésirables, Cisco Umbrella recommande d'ajouter des noms de domaine critiques qui ne peuvent jamais être bloqués (par exemple, google.com ou salesforce.com) à la liste verte globale (ou à d'autres listes de destinations conformément à votre stratégie) avant de configurer l'intégration.

Les domaines critiques peuvent inclure :

- La page d'accueil de votre entreprise
- Domaines représentant des services que vous fournissez et pouvant avoir des enregistrements internes et externes. Par exemple, « mail.myservicedomain.com » et « portal.myotherservicedomain.com ».
- Les applications cloud moins connues dont vous dépendez et que Cisco Umbrella ne peut

pas inclure dans la validation automatique de domaine. Par exemple, « localcloudservice.com ».

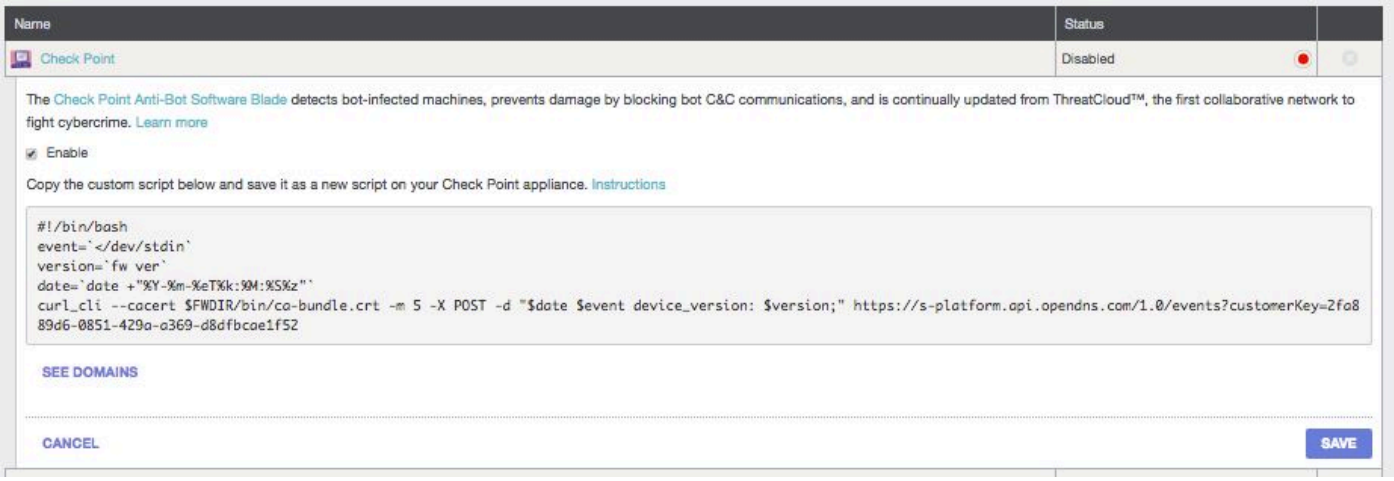
Ces domaines doivent être ajoutés à la liste verte globale, qui se trouve sous Politiques > Listes de destinations dans Cisco Umbrella.

Étape 1 : Génération de jetons de script et API Umbrella

1. Connectez-vous au tableau de bord Cisco Umbrella en tant qu'administrateur.

2. Accédez à Stratégies > Composants de stratégie > Intégrations et sélectionnez Point de contrôle dans le tableau pour le développer.

3. Sélectionnez l'option Activer.



4. Copiez l'intégralité du script, en commençant par la ligne avec :

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

Vous pouvez ensuite utiliser le script dans les étapes suivantes.

5. Sélectionnez Enregistrer pour activer l'intégration.

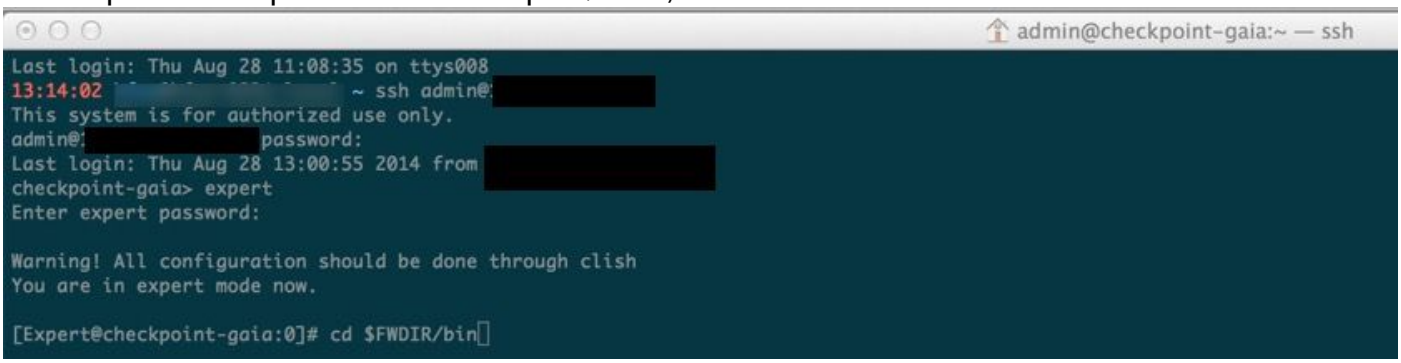
Étape 2 : Déployer le script personnalisé sur l'appliance Check Point

Les étapes suivantes consistent à installer le script Cisco Umbrella personnalisé sur votre appliance Check Point, puis à l'activer dans le tableau de bord intelligent.

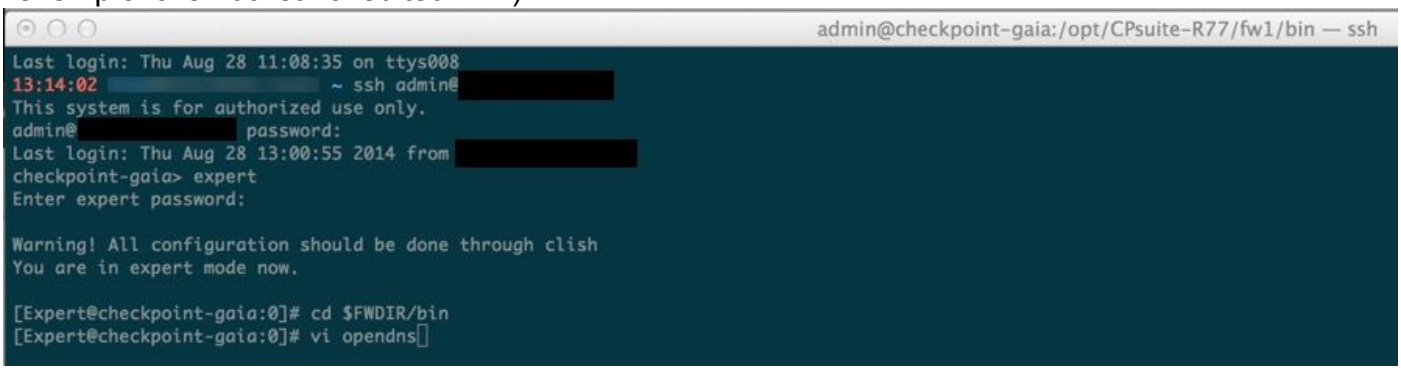
1. Pour installer le script personnalisé, installez SSH dans l'appliance Check Point en tant qu'administrateur :

2. Ensuite, lancez le « Mode expert » en tapant « expert » dans la ligne de commande :

3. Remplacez le répertoire de travail par `$FWDIR/bin` :

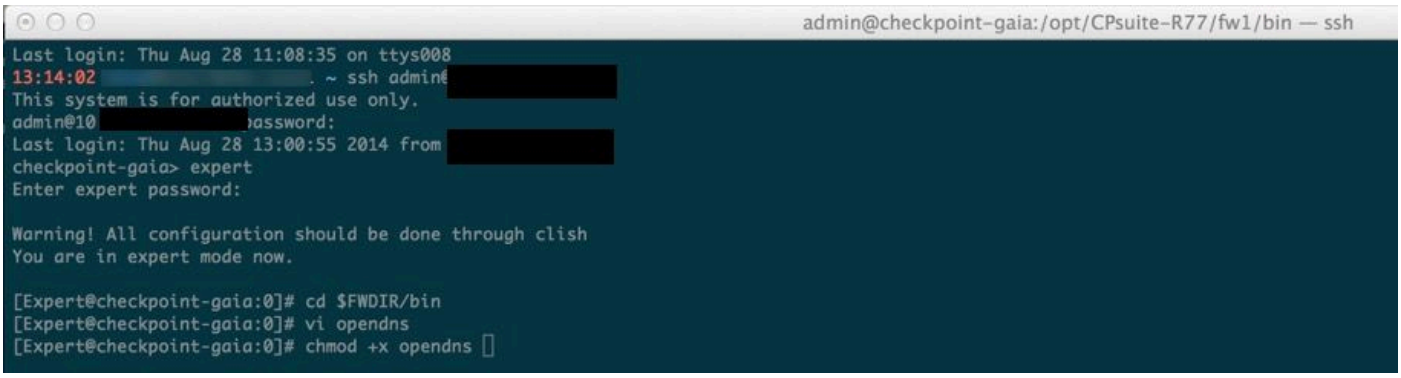


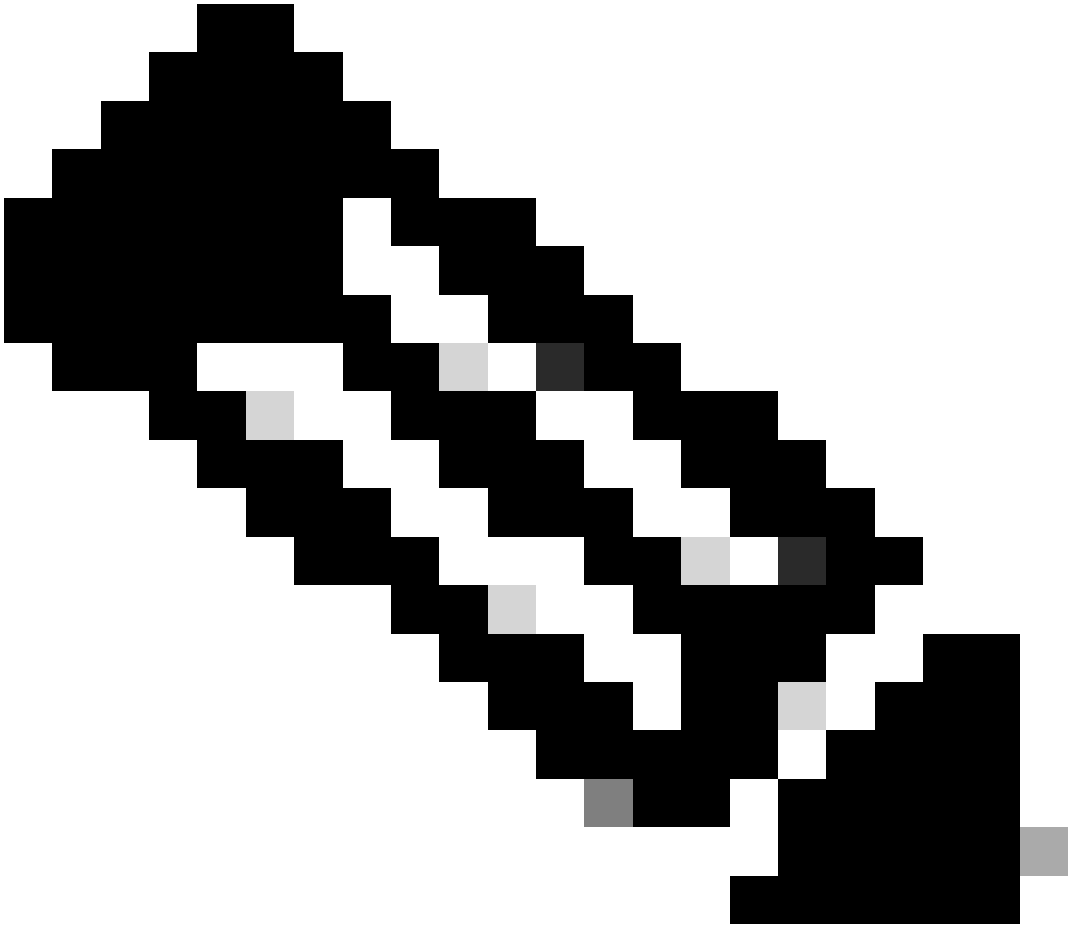
4. Ouvrez un nouveau fichier nommé "opendns" en utilisant un éditeur de texte (comme dans l'exemple ici en utilisant l'éditeur "vi") :



5. Collez le script Cisco Umbrella dans le fichier, puis enregistrez le fichier et quittez votre éditeur :

6. Rendez le script Umbrella personnalisé exécutable en exécutant `chmod +x opendns` :





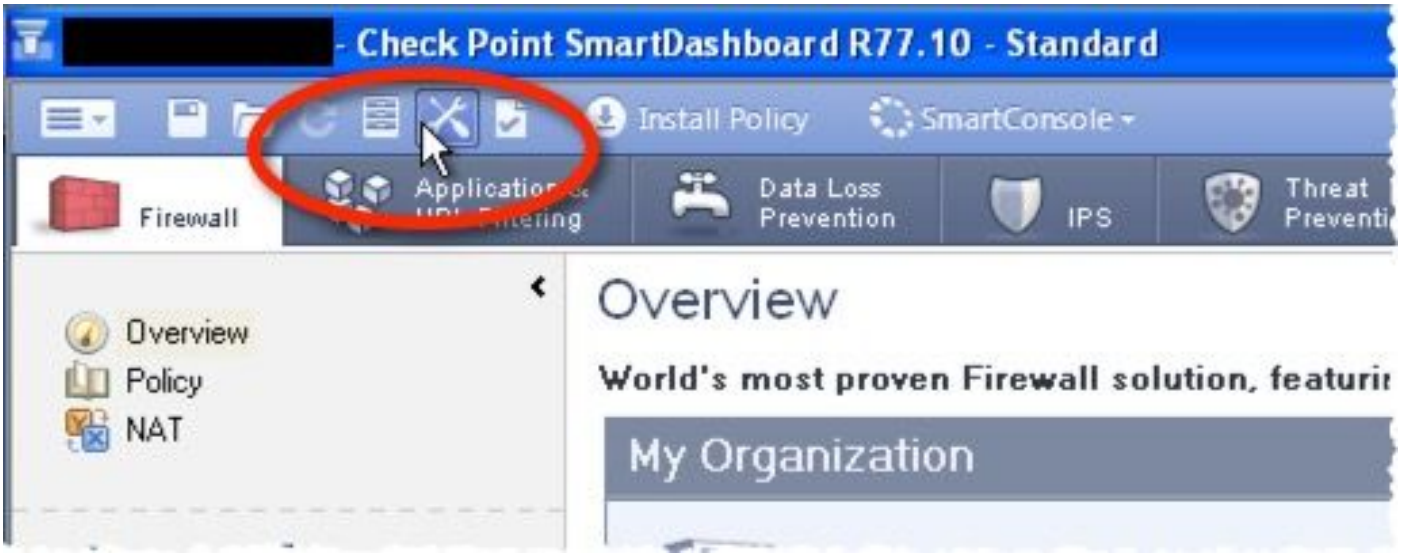
Remarque : Si vous mettez à niveau ou modifiez des versions de lame, vous devez répéter ces étapes sur cette nouvelle version.

Étape 3. Création ou modification d'une alerte Check Point à publier dans le nouveau script

1. Activez le SmartDashboard pour publier le nouveau script en vous connectant et en lançant le

SmartDashboard :

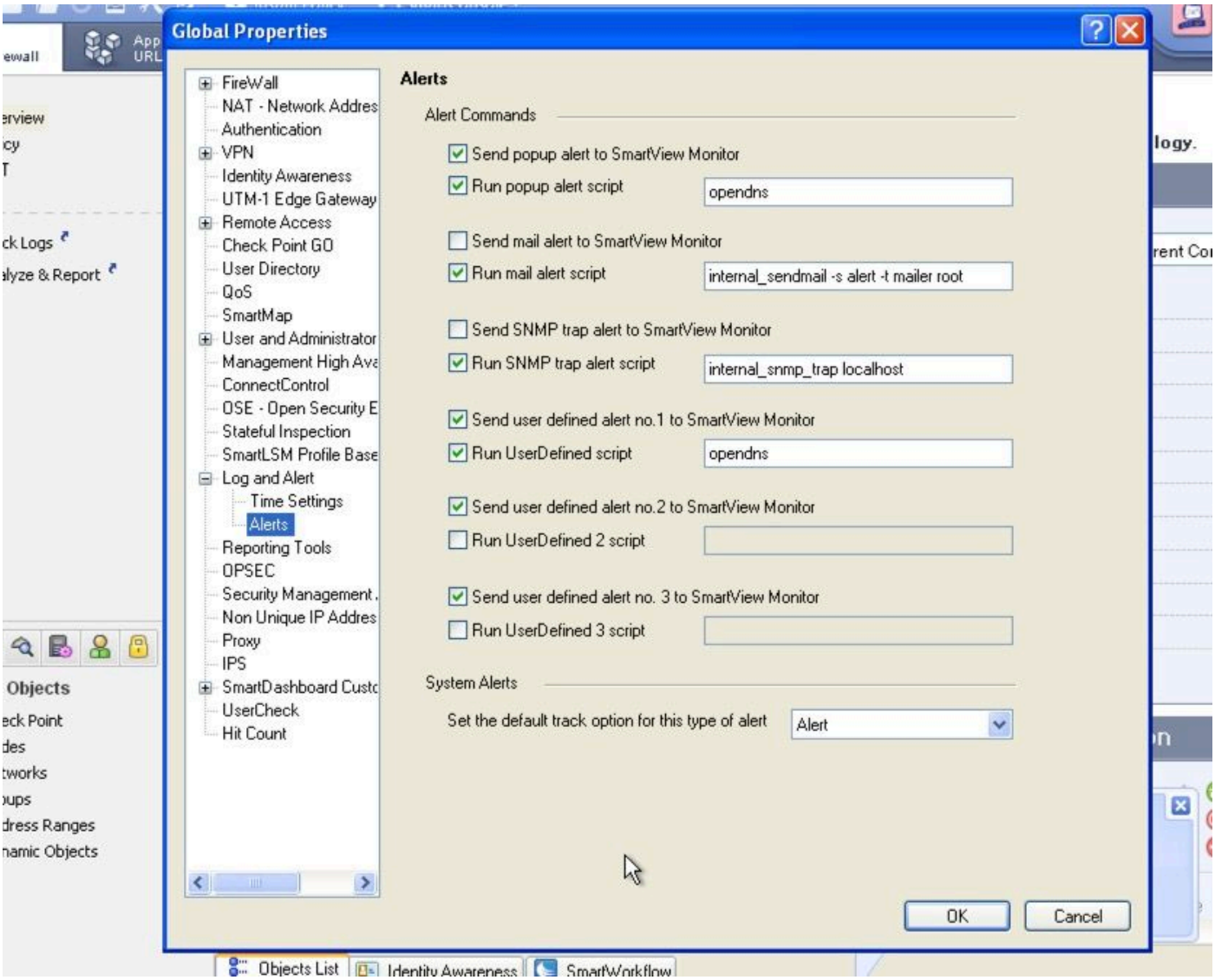
2. Ouvrez Propriétés globales :



3. Dans Propriétés globales, ouvrez Journal et alertes > Alertes et procédez comme suit :

- Sélectionnez Send popup alertscript et Run UserDefined script.
- Définissez « opendns » dans les champs de script pour les deux.

4. Sélectionnez OK. Dans SmartDashboard, enregistrez et installez votre stratégie mise à jour.



Étape 4 : Test de l'intégration et définition des événements de point de contrôle à bloquer

Tout d'abord, générez un événement de lame anti-bot de test qui apparaîtra dans le tableau de bord Cisco Umbrella :

1. À partir de n'importe quel périphérique du réseau protégé par votre appliance Check Point, chargez cette URL dans votre navigateur :

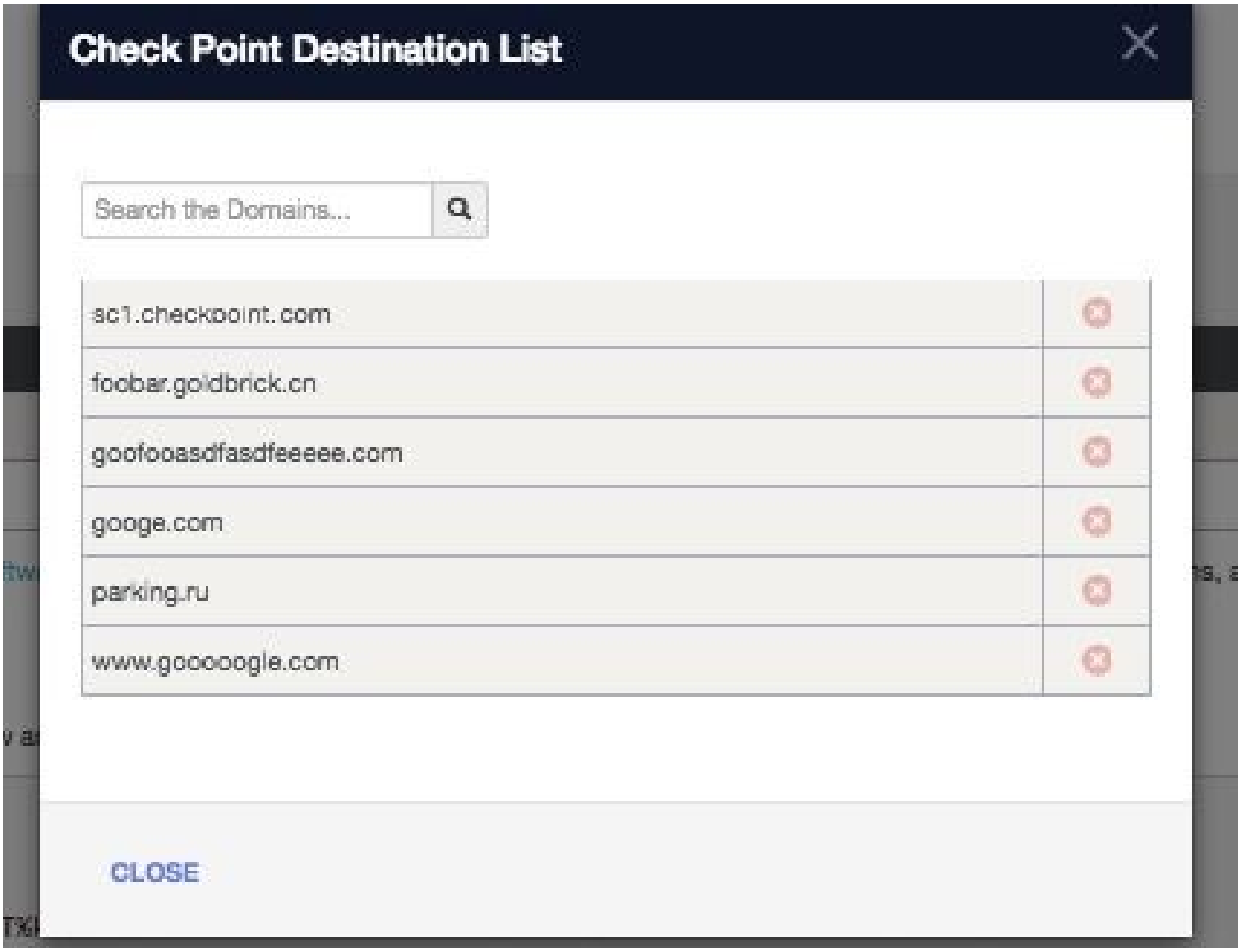
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

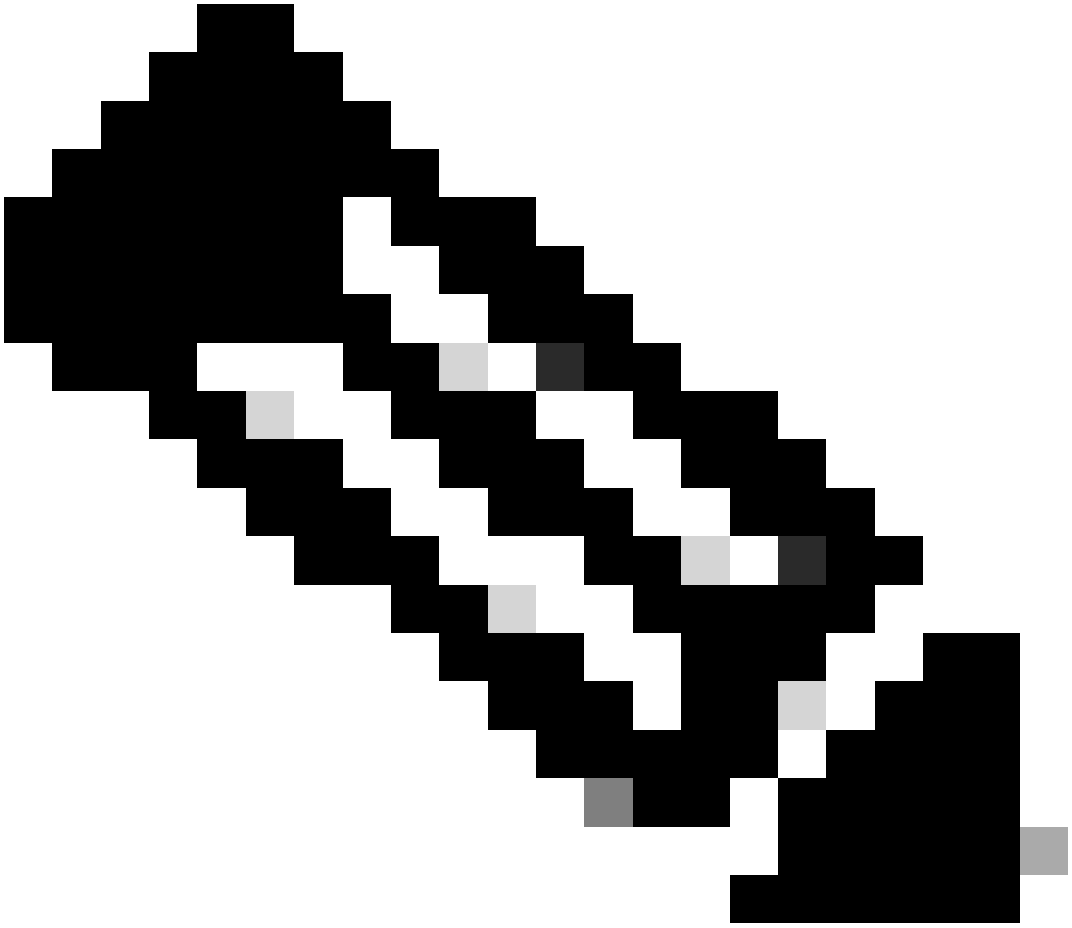
2. Connectez-vous au tableau de bord Cisco Umbrella en tant qu'administrateur.

3. Accédez à Stratégies > Composants de stratégie > Intégrations et sélectionnez Point de contrôle dans le tableau pour le développer.

4. Sélectionnez Voir Domaines. Une fenêtre s'ouvre et affiche la liste de destinations Check Point

pouvant inclure « sc1.checkpoint.com ». À partir de ce moment, une liste consultable commence à être remplie et s'agrandit.



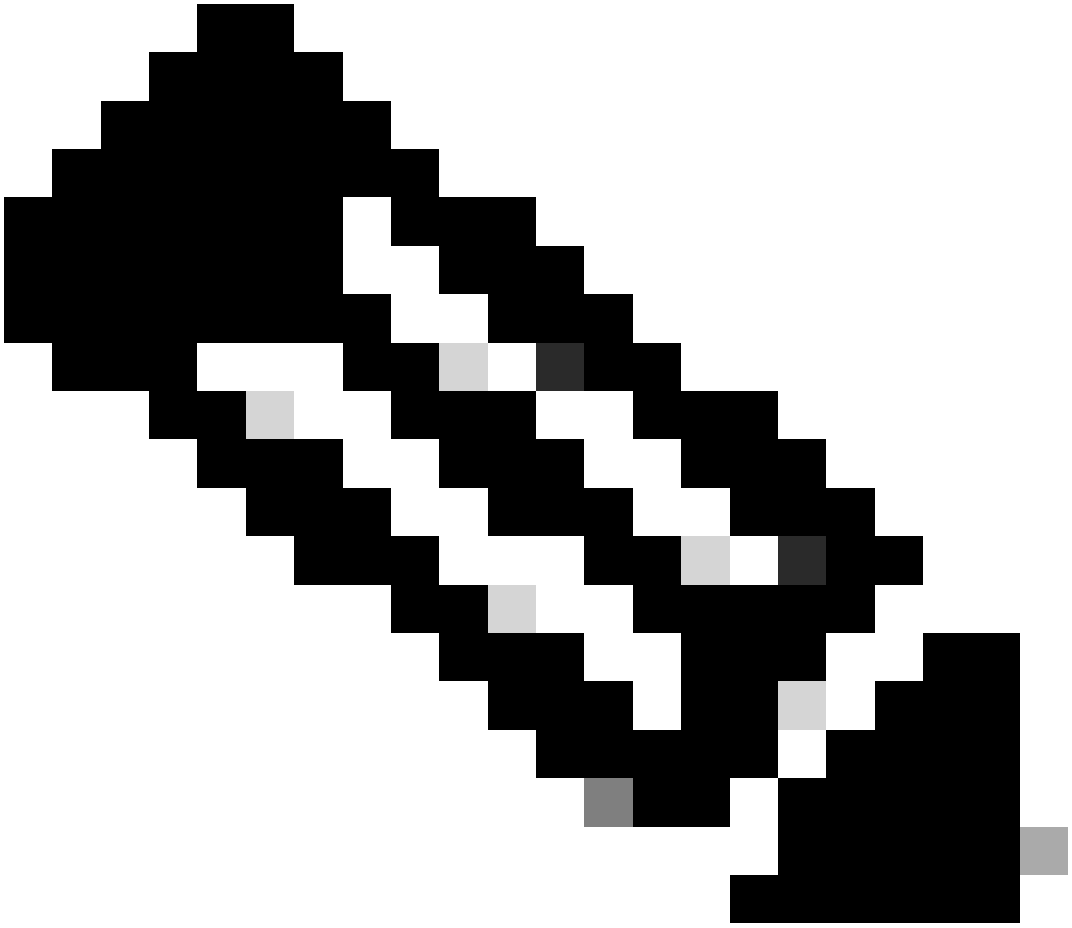


Remarque : Vous pouvez également modifier cette liste de destinations si un domaine apparaît ici sur lequel vous ne souhaitez pas appliquer de stratégie. Sélectionnez l'icône Delete pour supprimer le domaine.

Observation des événements ajoutés à la catégorie de sécurité Check Point en mode audit

L'étape suivante consiste à observer et à auditer les événements ajoutés à votre nouvelle catégorie de sécurité Check Point.

Les événements de votre appliance Check Point commencent à remplir une liste de destinations spécifique qui peut être appliquée aux stratégies en tant que catégorie de sécurité Check Point. Par défaut, la liste de destinataires et la catégorie de sécurité sont en « mode audit » et ne s'appliquent à aucune stratégie. Elles ne peuvent pas entraîner de modification de vos stratégies Cisco Umbrella existantes.



Remarque : Le « mode audit » peut être activé pendant la durée nécessaire, en fonction de votre profil de déploiement et de la configuration du réseau.

Vérifier la liste de destinations

Vous pouvez consulter la liste des destinations Check Point à tout moment dans Cisco Umbrella :

1. Accédez à Stratégies > Composants de stratégie > Intégrations.

2. Développez Check Point dans le tableau et sélectionnez Voir Domaines.

Vérifier les paramètres de sécurité d'une stratégie

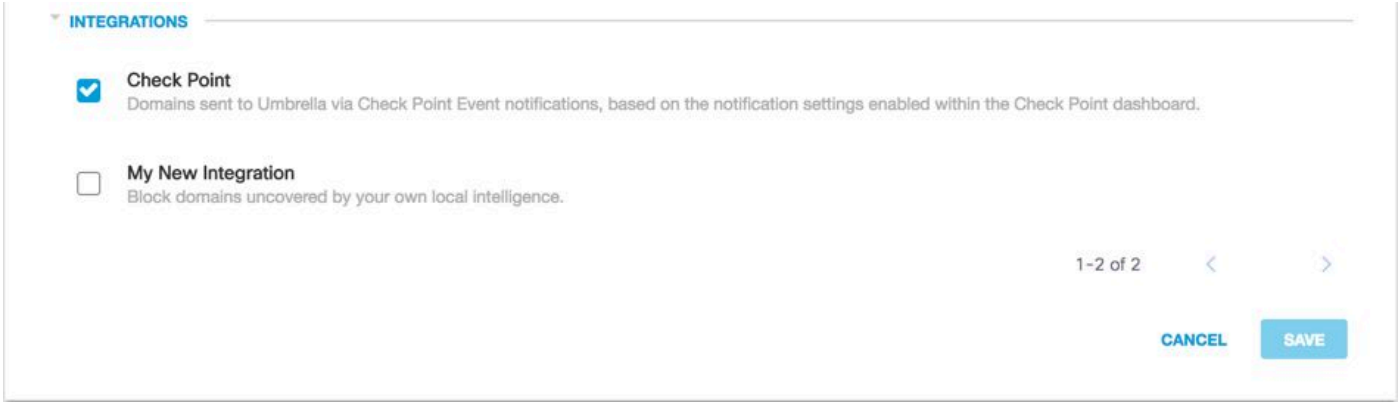
Vous pouvez consulter à tout moment les paramètres de sécurité pouvant être activés pour une stratégie dans Cisco Umbrella :

1. Accédez à Stratégies > Composants de stratégie > Paramètres de sécurité.

2. Sélectionnez un paramètre de sécurité dans la table pour le développer.

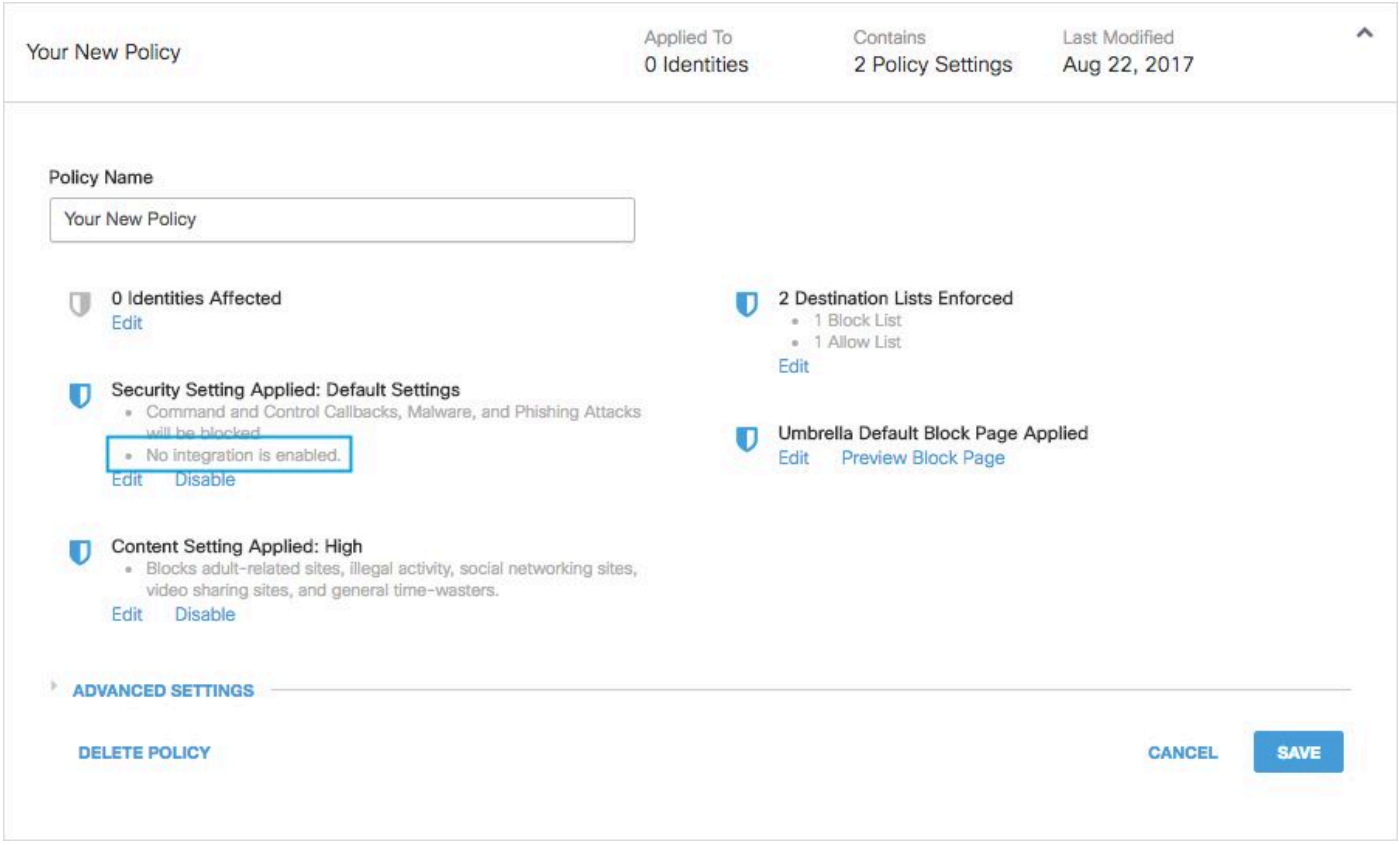
3. Faites défiler jusqu'à la section Integrations et développez la section pour afficher l'intégration Check Point.

4. Sélectionnez l'option d'intégration Check Point, puis sélectionnez Enregistrer.



115013984226

Vous pouvez également consulter les informations d'intégration via la page Résumé des paramètres de sécurité :



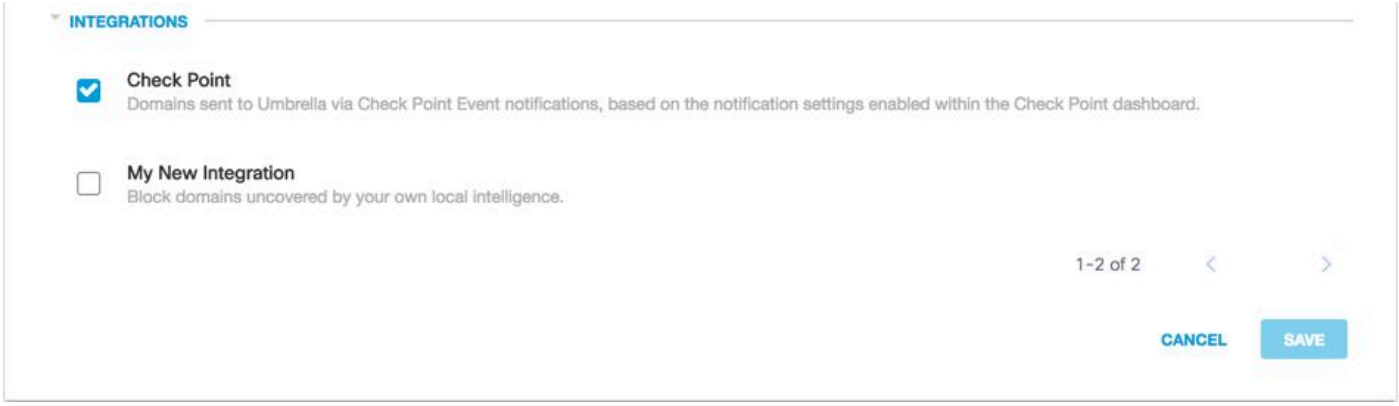
19916943300244

Application des paramètres de sécurité du point de contrôle en « mode blocage » à une stratégie pour les clients gérés

Une fois que vous êtes prêt à faire appliquer ces menaces de sécurité supplémentaires par les clients gérés par Cisco Umbrella, modifiez le paramètre de sécurité sur une stratégie existante ou créez une nouvelle stratégie qui se trouve au-dessus de votre stratégie par défaut pour vous assurer qu'elle est appliquée en premier :

1. Assurez-vous que l'intégration Check Point est toujours activée, comme indiqué dans la section précédente. Accédez à Policies > Policy Components > Security Settings et ouvrez le paramètre approprié.

2. Sous Intégrations, vérifiez que l'option Check Point est sélectionnée. Si ce n'est pas le cas, sélectionnez l'option et sélectionnez Enregistrer.



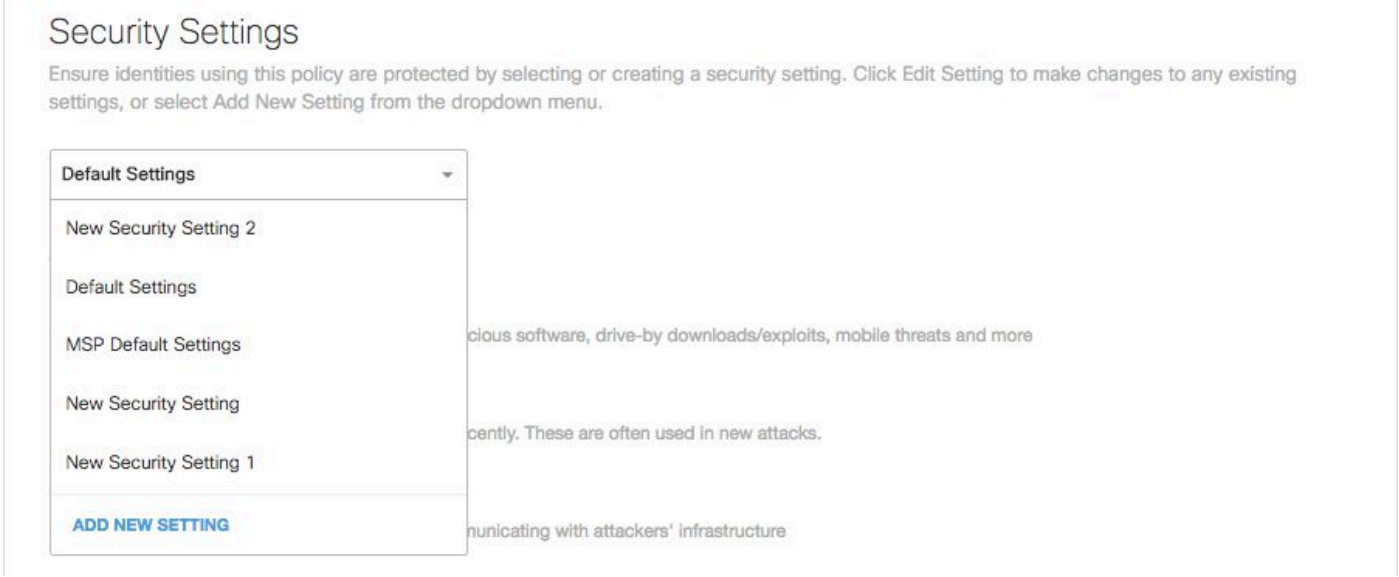
115013984226

Ensuite, dans l'assistant Cisco Umbrella Policy, ajoutez ce paramètre de sécurité à une stratégie que vous modifiez :

1. Accédez à une règle : soit Politiques > Politiques DNS ou Politiques > Politique Web.

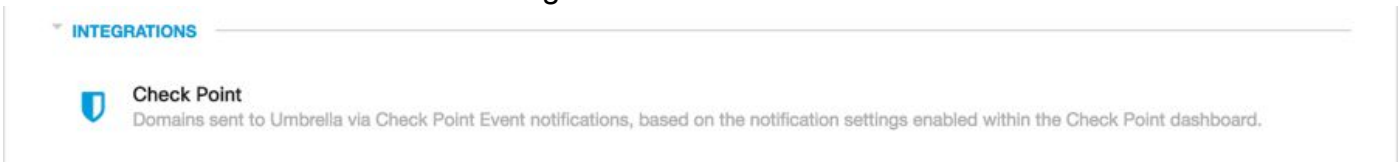
2. Développez une stratégie et sous Paramètres de sécurité appliqués (stratégies DNS) ou Paramètres de sécurité (stratégie Web), puis sélectionnez Modifier.

3. Dans la liste déroulante Paramètres de sécurité, sélectionnez un paramètre de sécurité qui inclut le paramètre Check Point.



19916943316884

L'icône en forme de bouclier sous Intégrations devient bleue.



115014149783

4. Sélectionnez Set & Return (DNS Policies) ou Save (Web Policy).

Les domaines Check Point contenus dans le paramètre de sécurité de Check Point peuvent ensuite être bloqués pour ces identités à l'aide de la stratégie.

Création de rapports dans Umbrella pour les événements Check Point

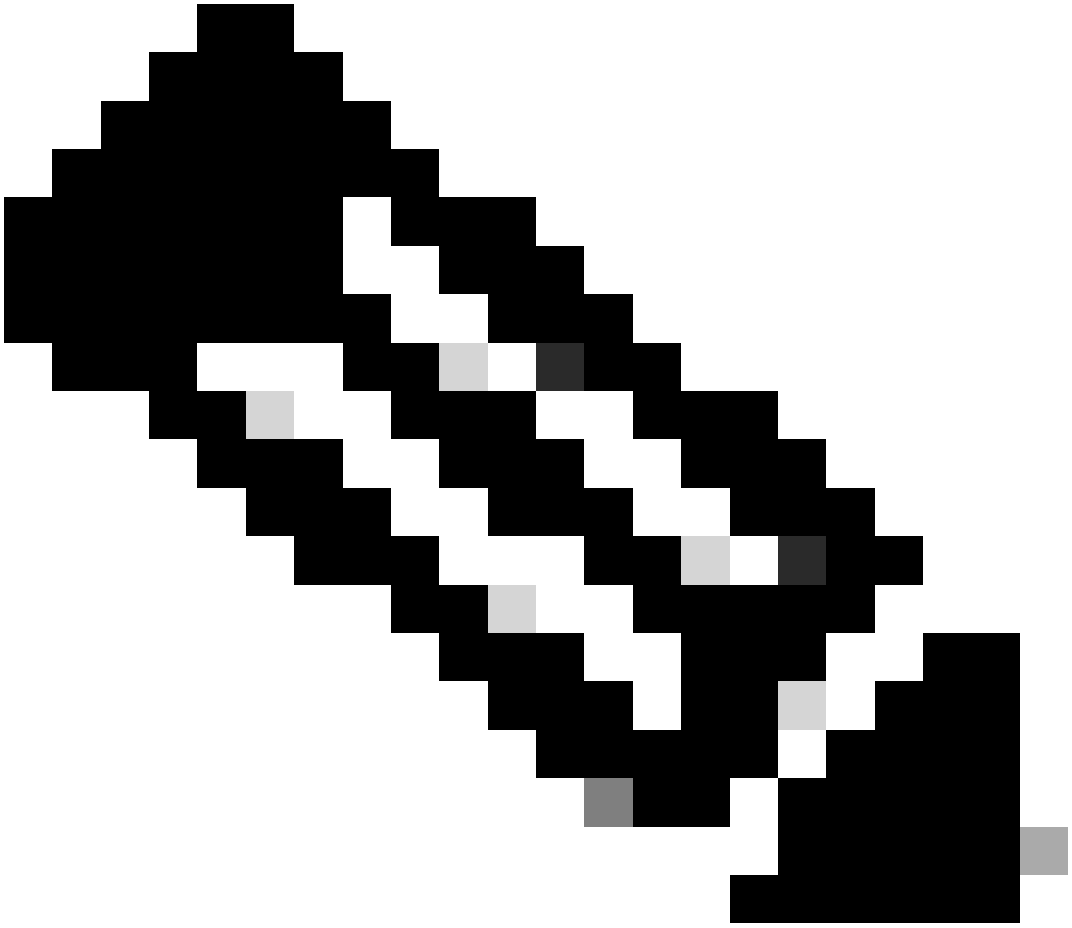
Rapports sur les événements de sécurité Check Point

La liste de destinations Check Point est l'une des catégories de sécurité disponibles pour les rapports. La plupart ou la totalité des rapports utilisent les catégories de sécurité comme filtre. Par exemple, vous pouvez filtrer les catégories de sécurité pour n'afficher que les activités liées à Check Point :

1. Accédez à Reporting > Core Reports > Activity Search.

2. Sous Security Categories, sélectionnez Check Point pour filtrer le rapport afin d'afficher uniquement la catégorie de sécurité pour Check Point.

115014197623



Remarque : Si l'intégration Check Point est désactivée, elle ne peut pas apparaître dans le filtre Catégories de sécurité.

3. Sélectionnez Appliquer pour voir l'activité liée aux points de contrôle pour la période sélectionnée dans l'état.

Création de rapports lorsque des domaines ont été ajoutés à la liste de destinations de point de contrôle

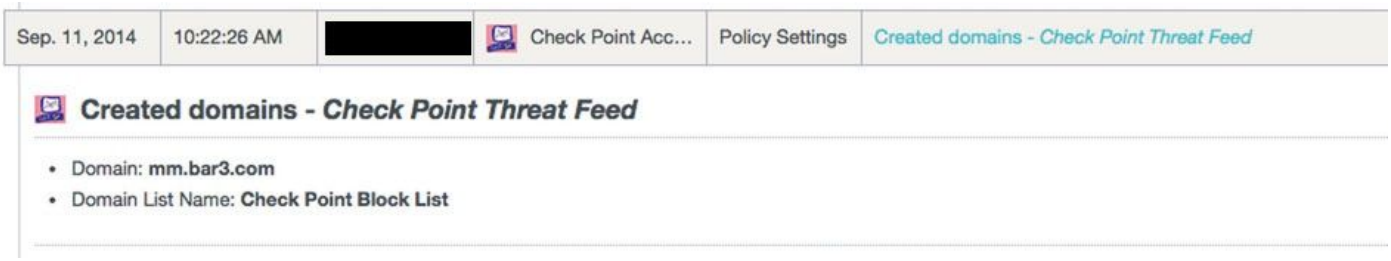
Le journal d'audit de l'administrateur Cisco Umbrella inclut les événements de l'appliance Check Point lors de l'ajout de domaines à la liste de destination. Ces domaines semblent être ajoutés par une étiquette « Compte Check Point », sous la colonne Utilisateur du journal d'audit.

Pour rechercher le journal d'audit d'admin. Umbrella, accédez à Reporting > Admin Audit Log.

Pour générer un rapport sur l'ajout d'un domaine, filtrez pour inclure uniquement les modifications de point de contrôle en appliquant un filtre Filtrer par identités et paramètres pour la liste de

blocage de point de contrôle.

Une fois que vous avez exécuté le rapport, vous pouvez voir une liste de domaines ajoutés à la liste de destinations Check Point.



Gestion des détections indésirables ou des faux positifs

Gestion d'une liste verte pour la détection indésirable

Bien qu'improbable, il est possible que les domaines ajoutés automatiquement par votre appliance Check Point déclenchent un blocage indésirable qui peut empêcher vos utilisateurs d'accéder à des sites Web particuliers. Dans une situation comme celle-ci, Cisco Umbrella recommande d'ajouter le ou les domaines à une liste d'autorisation, qui est prioritaire sur tous les autres types de listes de blocage, y compris les paramètres de sécurité. Une liste verte est prioritaire sur une liste rouge lorsqu'un domaine est présent dans les deux.

Cette approche est privilégiée pour deux raisons :

- Tout d'abord, si l'appliance Check Point devait ajouter à nouveau le domaine après sa suppression, la liste d'autorisation se prémunit contre ce problème, ce qui provoquerait d'autres problèmes.
- Ensuite, la liste verte affiche un historique des domaines problématiques pour des analyses ou des rapports d'audit ultérieurs.

Par défaut, une liste verte globale est appliquée à toutes les stratégies. L'ajout d'un domaine à la liste verte globale entraîne l'autorisation du domaine dans toutes les stratégies.

Si le paramètre de sécurité Check Point en mode Bloquer est appliqué uniquement à un sous-ensemble de vos identités Cisco Umbrella gérées (par exemple, il est appliqué uniquement aux ordinateurs et périphériques mobiles itinérants), vous pouvez créer une liste d'autorisation spécifique pour ces identités ou stratégies.

Pour créer une liste verte :

1. Accédez à Politiques > Listes de destinations et sélectionnez l'icône Ajouter.

2. Sélectionnez Autoriser et ajoutez votre domaine à la liste.

3. Sélectionnez Enregistrer.

Une fois la liste enregistrée, vous pouvez l'ajouter à une stratégie existante couvrant les clients qui

ont été affectés par le blocage indésirable.

Suppression de domaines de la liste de destinations de point de contrôle

À côté de chaque nom de domaine dans la liste de destination Check Point se trouve une icône Delete. La suppression de domaines vous permet de nettoyer la liste de destinations Check Point en cas de détection indésirable.

Cependant, la suppression n'est pas permanente si l'appliance Check Point renvoie le domaine à Cisco Umbrella.

Pour supprimer un domaine :

1. Accédez à Paramètres > Intégrations, puis sélectionnez Point de contrôle pour le développer.

2. Sélectionnez Voir Domaines.

3. Recherchez le nom de domaine que vous souhaitez supprimer.

4. Cliquez sur l'icône Supprimer.

5. Sélectionnez Fermer.

6. Sélectionnez Enregistrer.

En cas de détection indésirable ou de faux positif, Cisco Umbrella recommande de créer immédiatement une liste verte dans Cisco Umbrella, puis de corriger le faux positif dans l'appliance Check Point. Vous pourrez ensuite supprimer le domaine de la liste de destinations Check Point.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.