Paraplu configureren met Check Point Anti-Bot Software Blade

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Overzicht

Functionaliteit

Configuratiestappen

- Onderbrekingen van de service voorkomen
- Stap 1: Umbrella Script en API Token Generation
- Stap 2: Implementeer het aangepaste script op het controlepunttoestel
- Stap 3. Een controlepuntwaarschuwing maken of bewerken om naar het nieuwe script te posten
- Stap 4: Het testen van de integratie en het instellen van controlepuntgebeurtenissen die moeten worden geblokkeerd

Waarnemen van gebeurtenissen toegevoegd aan de categorie Check Point Security in "Audit Mode"

- Bestemmingslijst bekijken
- Beveiligingsinstellingen voor een beleid bekijken

De beveiligingsinstellingen van het controlepunt in de "blokmodus" toepassen op een beleid voor beheerde clients

Rapportage binnen Paraplu voor controlepuntgebeurtenissen

- Rapportage over beveiligingsgebeurtenissen bij controlepunten
- Rapporteren wanneer domeinen zijn toegevoegd aan de bestemmingslijst van controlepunten

Omgaan met ongewenste detecties of valse positieven

- Een lijst met machtigingen voor ongewenste detectie beheren
- Domeinen verwijderen uit de bestemmingslijst van controlepunten

Inleiding

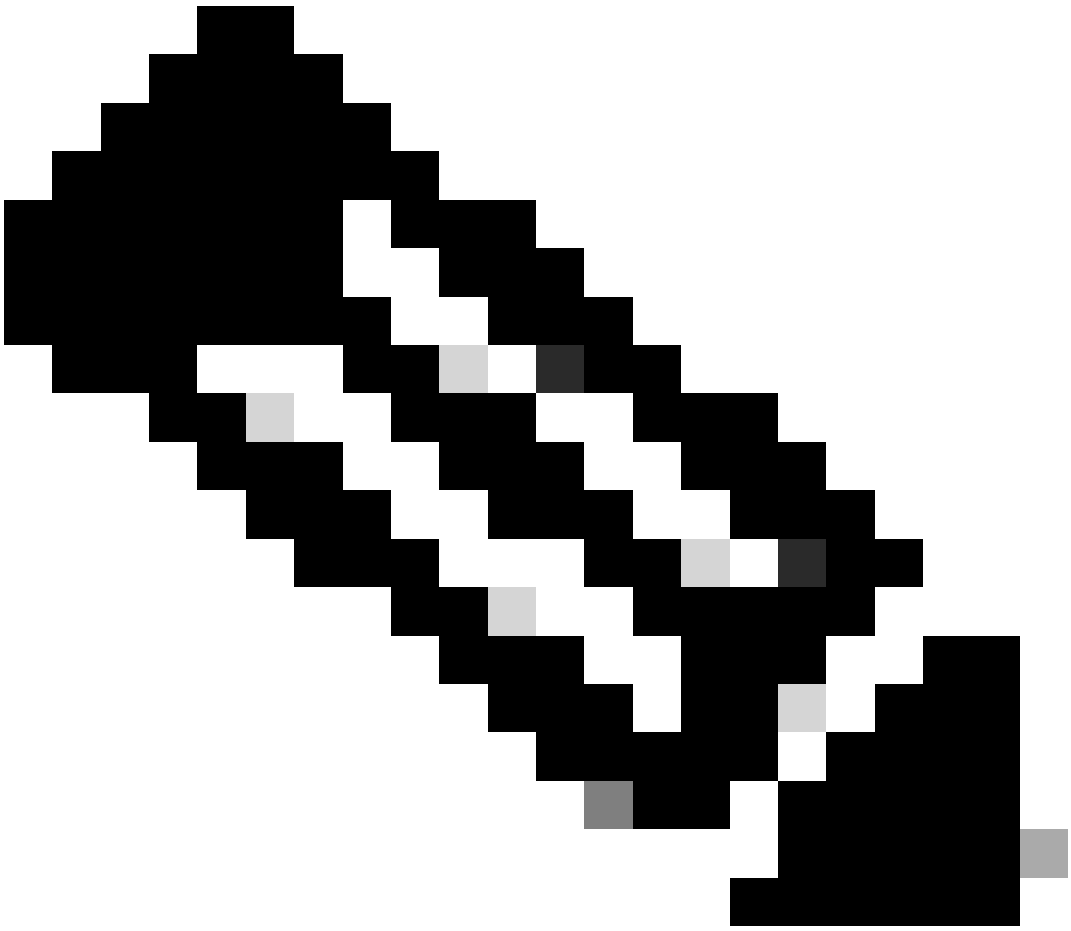
In dit document wordt beschreven hoe u Cisco Umbrella kunt integreren met de softwareblade Check Point Anti-Bot.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een controlepuntapparaat met de softwareblade Anti-Bot
- Check Point-softwareversie R80.40 of hoger
- Zorg ervoor dat het Check Point-apparaat uitgaande HTTP-verzoeken kan indienen bij "https://s-platform.api.opendns.com".
- Een Cisco Umbrella-pakket zoals DNS Essentials, DNS Advantage, SIG Essentials of SIG Advantage
- Administratieve rechten Cisco Umbrella Dashboard



Opmerking: de integratie van het controlepunt is alleen inbegrepen in Cisco Umbrella-pakketten zoals DNS Essentials, DNS Advantage, SIG Essentials of SIG Advantage. Als u niet over een van deze pakketten beschikt en de integratie van het controlepunt wilt hebben, neemt u contact op met uw Cisco Umbrella-accountmanager. Als u het juiste Cisco Umbrella-pakket hebt, maar Check Point niet ziet als een integratie voor uw dashboard, kunt u contact opnemen met Cisco Umbrella Support.

Gebruikte componenten

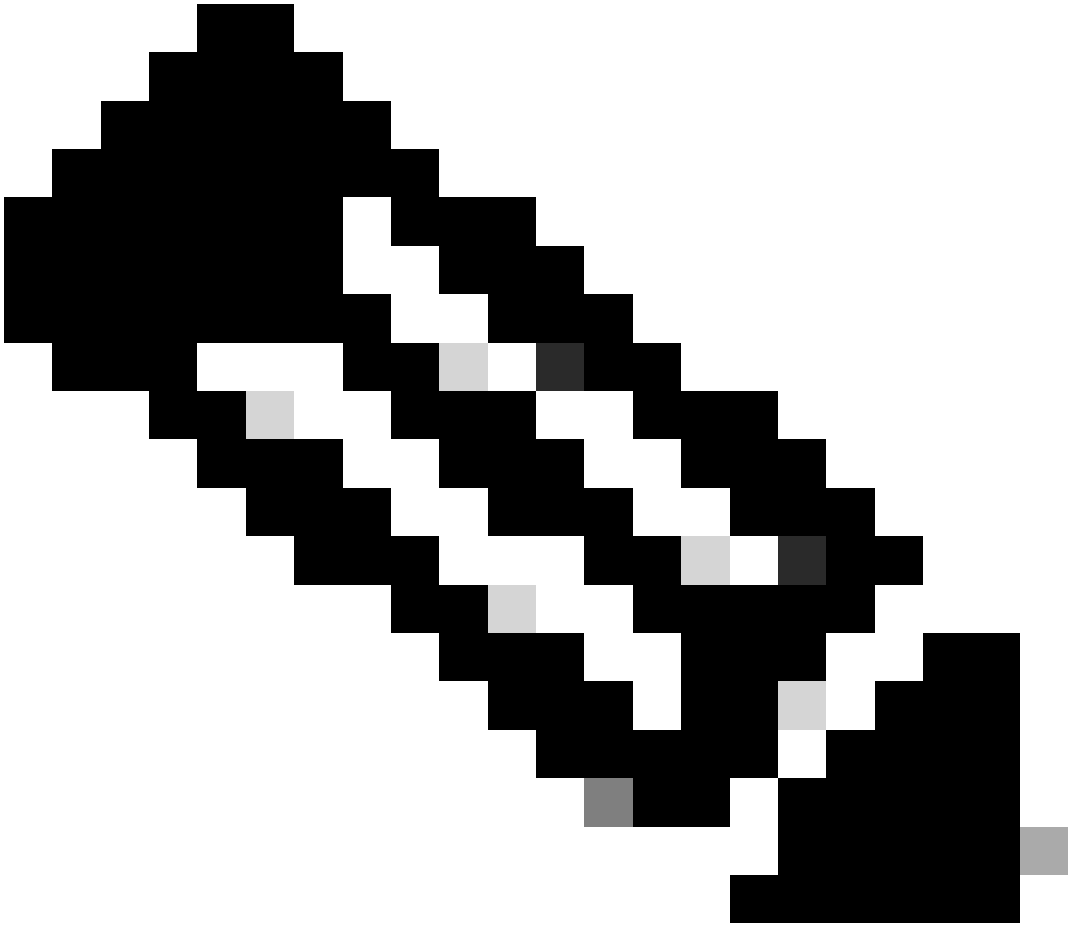
De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

De Cisco Umbrella-integratie met de Check Point Anti-Bot Software Blade maakt het voor een Check Point-apparaat mogelijk om zijn Anti-Bot Software Blade-waarschuwingen naar Cisco Umbrella te sturen wanneer de Blade bedreigingen ontdekt in het netwerkverkeer dat hij inspecteert. Waarschuwingen ontvangen door Cisco Umbrella bouwen een blokkeerlijst die roaminglaptops, tablets en telefoons kan beschermen op netwerken die niet worden beschermd door de Check Point Anti-Bot Software Blade.

In dit artikel worden instructies gegeven voor het configureren van een controlepuntapparaat voor het verzenden van waarschuwingen voor de bladeservers van de Anti-Bot Software naar Cisco Umbrella.



Opmerking: deze integratie werd door Check Point in versie R81.20 afgeschreven nadat deze aanvankelijk in R80.40 was uitgebracht.

Functionaliteit

De Cisco Umbrella-integratie met het Check Point Anti-Bot Software Blade-apparaat duwt bedreigingen die het heeft gevonden (bijvoorbeeld domeinen die malware hosten, commando en controle voor botnets of phishingsites) naar Cisco Umbrella voor wereldwijde handhaving.

Cisco Umbrella valideert vervolgens de dreiging om ervoor te zorgen dat deze kan worden toegevoegd aan een beleid. Als wordt bevestigd dat de informatie van de Check Point Anti-Bot Software Blade een bedreiging vormt, wordt het domeinadres toegevoegd aan de Checkpoint Destination List als onderdeel van een beveiligingsinstelling die kan worden toegepast op elk Cisco Umbrella-beleid. Dat beleid wordt onmiddellijk toegepast op alle verzoeken die worden ingediend vanaf apparaten die aan dat beleid zijn toegewezen.

In de toekomst parseert Cisco Umbrella automatisch Check Point-waarschuwingen en voegt het

kwaadaardige sites toe aan de Check Point-bestemmingslijst. Dit breidt de Check Point-bescherming uit naar alle externe gebruikers en apparaten en biedt een andere laag van handhaving voor uw bedrijfsnetwerk.

Configuratiestappen

Het configureren van de integratie omvat de volgende stappen:

1. Schakel de integratie in Cisco Umbrella in om een API-token te genereren met een aangepast script.
2. Implementeer de API-token en het aangepaste script op het Check Point-toestel.
3. Maak/bewerk een checkpoint-waarschuwing om naar dit nieuwe script te posten.
4. Stel gebeurtenissen in het controlepunt in die moeten worden geblokkeerd in Cisco Umbrella.

Onderbrekingen van de service voorkomen

Om ongewenste onderbrekingen van de service te voorkomen, raadt Cisco Umbrella aan om bedrijfskritieke domeinnamen die nooit kunnen worden geblokkeerd (bijvoorbeeld google.com of salesforce.com) toe te voegen aan de Globale machtigingslijst (of andere bestemmingslijsten volgens uw beleid) voordat u de integratie configureert.

Bedrijfskritieke domeinen kunnen zijn:

- De homepage voor uw organisatie
- Domeinen die diensten vertegenwoordigen die u levert en die zowel interne als externe records kunnen hebben. Bijvoorbeeld "mail.myservicedomain.com" en "portal.myotherservicedomain.com".
- Minder bekende cloudgebaseerde toepassingen waarvan u afhankelijk bent en die Cisco Umbrella niet kan opnemen in automatische domeinvalidatie. Bijvoorbeeld "localcloudservice.com".

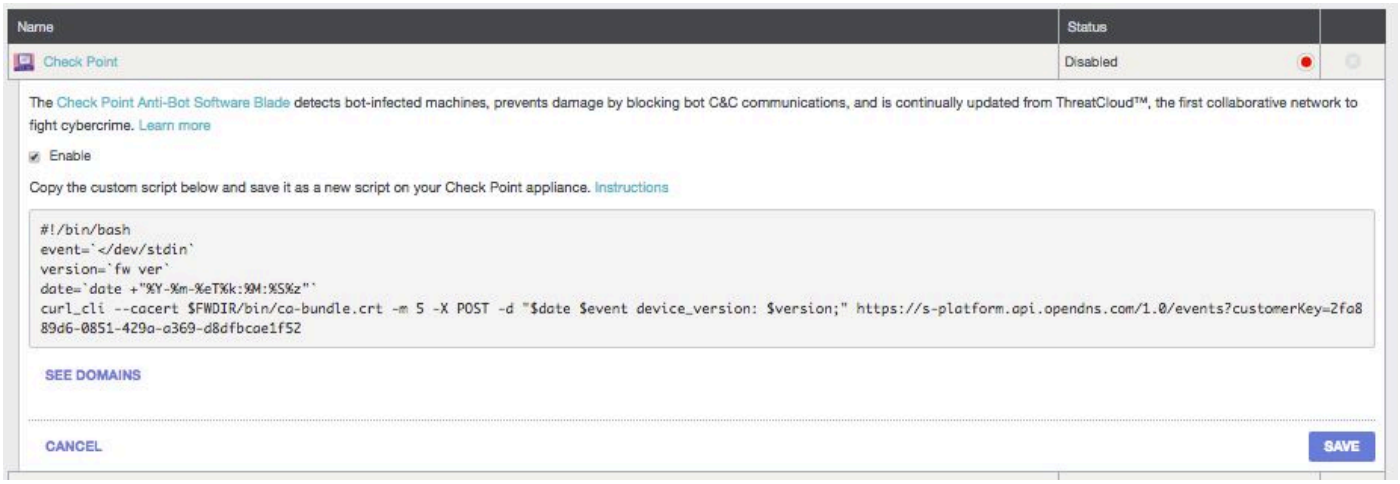
Deze domeinen moeten worden toegevoegd aan de Global Allow List, die te vinden is onder Beleid > Bestemmingslijsten in Cisco Umbrella.

Stap 1: Umbrella Script en API Token Generation

1. Meld u aan bij het Cisco Umbrella Dashboard als beheerder.

2. Navigeer naar Beleid > Beleidscomponenten > Integraties en selecteer Controlepunt in de tabel om deze uit te vouwen.

3. Selecteer de optie Inschakelen.



4. Kopieer het volledige script, beginnend vanaf de regel met:

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

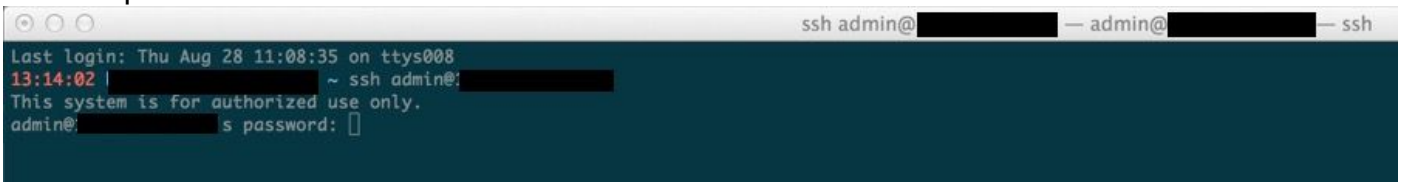
U kunt het script vervolgens in latere stappen gebruiken.

5. Selecteer Opslaan om de integratie in te schakelen.

Stap 2: Implementeer het aangepaste script op het controlepunttoestel

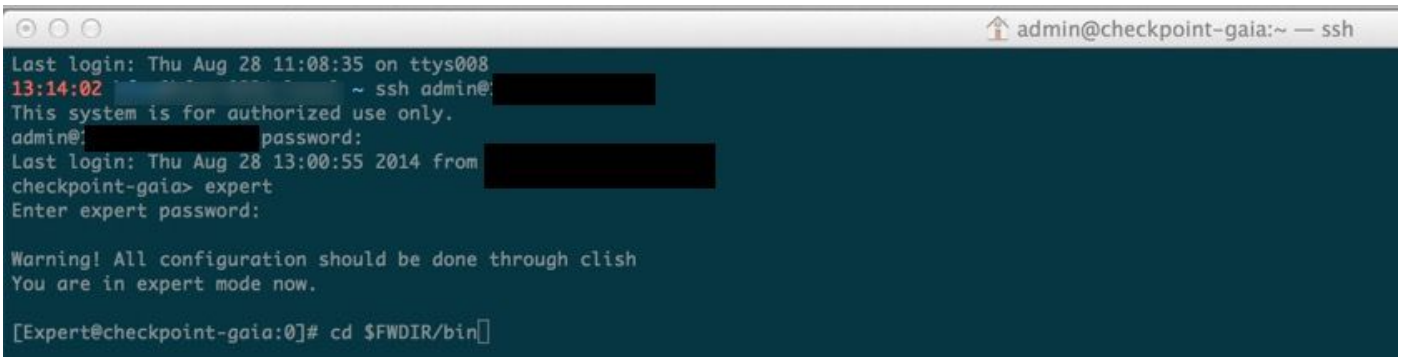
De volgende stappen zijn het installeren van het aangepaste Cisco Umbrella-script op uw Check Point-toestel en het vervolgens inschakelen in het SmartDashboard.

1. Als u het aangepaste script wilt installeren, gebruikt u SSH als beheerder in het Controlepunttoestel:

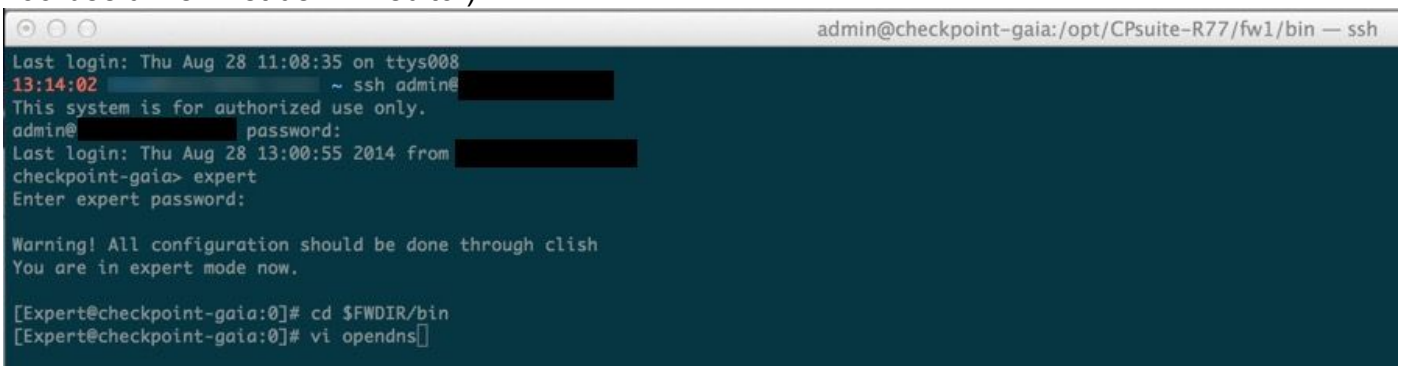


2. Start vervolgens "Expert Mode" door "expert" in de opdrachtregel te typen:

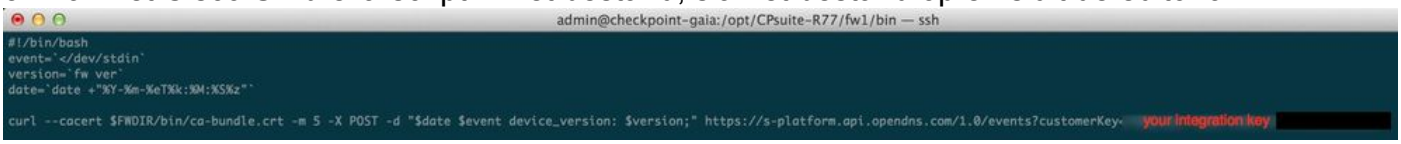
3. Wijzig de werkmap in `$FWDIR/bin`:



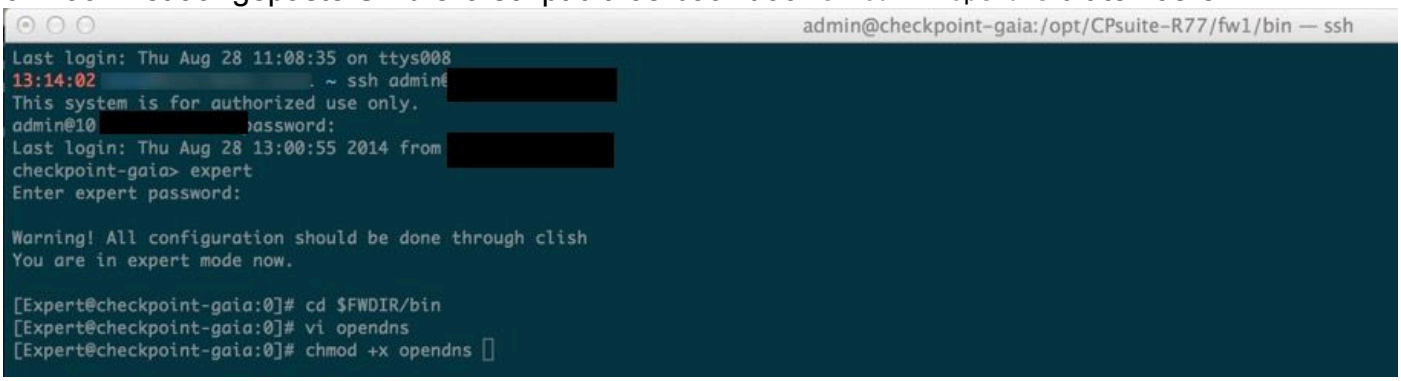
4. Open een nieuw bestand met de naam "opendns" met behulp van een teksteditor (zoals in het voorbeeld hier met de "vi" -editor):

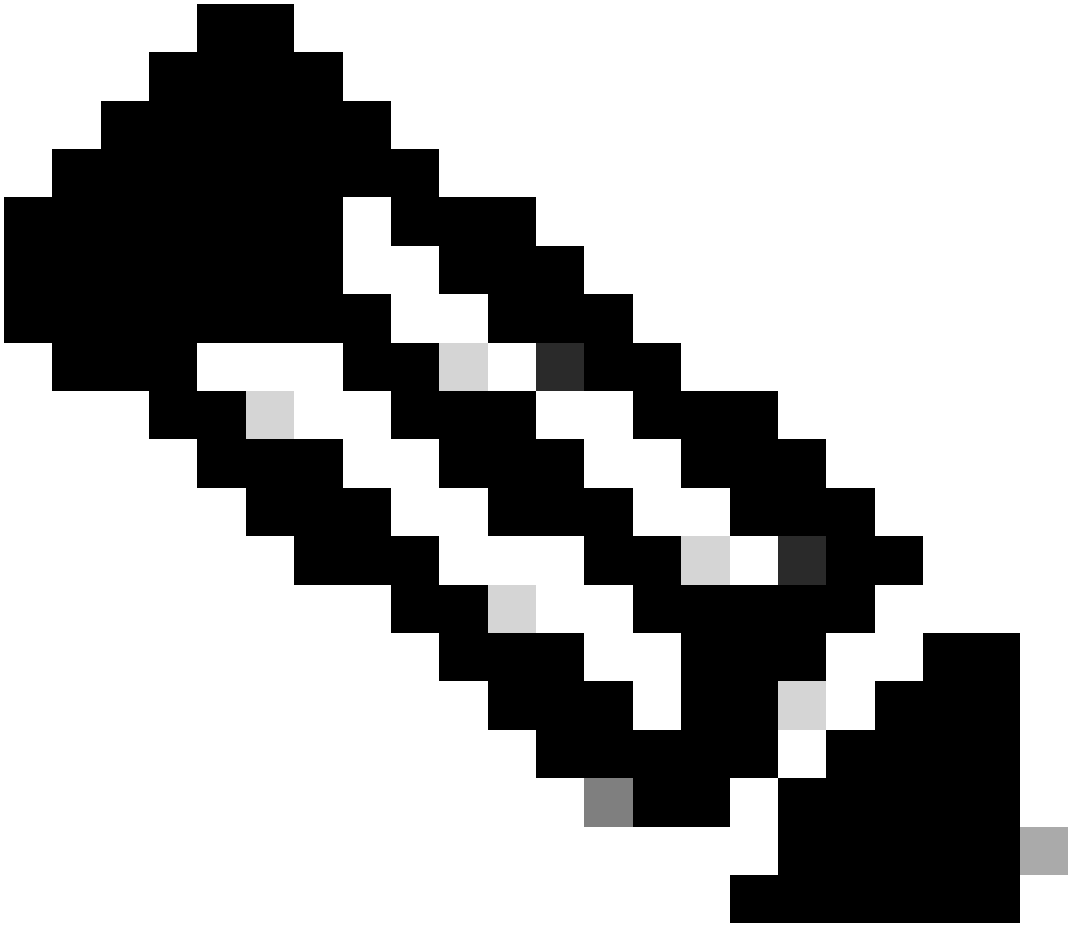


5. Plak het Cisco Umbrella-script in het bestand, sla het bestand op en sluit de editor af:



6. Maak het aangepaste Umbrella script uitvoerbaar door `chmod +x opendns` uit te voeren:



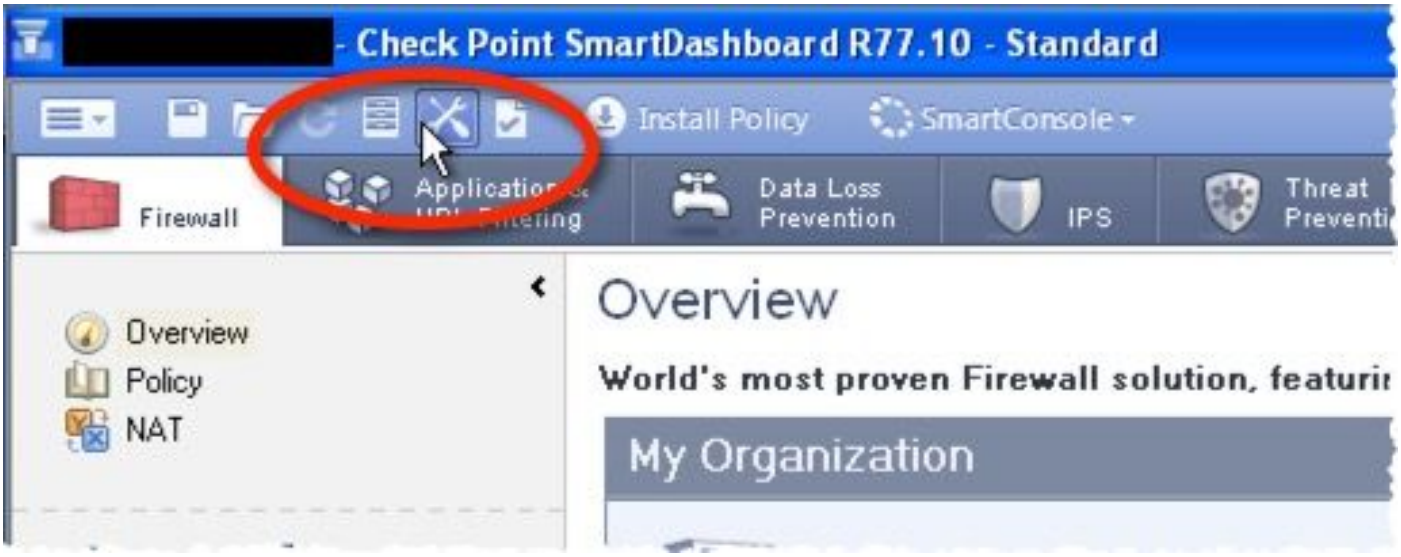


Opmerking: als u bladeversies bijwerkt of wijzigt, moet u deze stappen herhalen voor die nieuwe versie.

Stap 3. Een controlepuntwaarschuwing maken of bewerken om naar het nieuwe script te posten

1. Schakel het SmartDashboard in om het nieuwe script te posten door in te loggen en het SmartDashboard te starten:

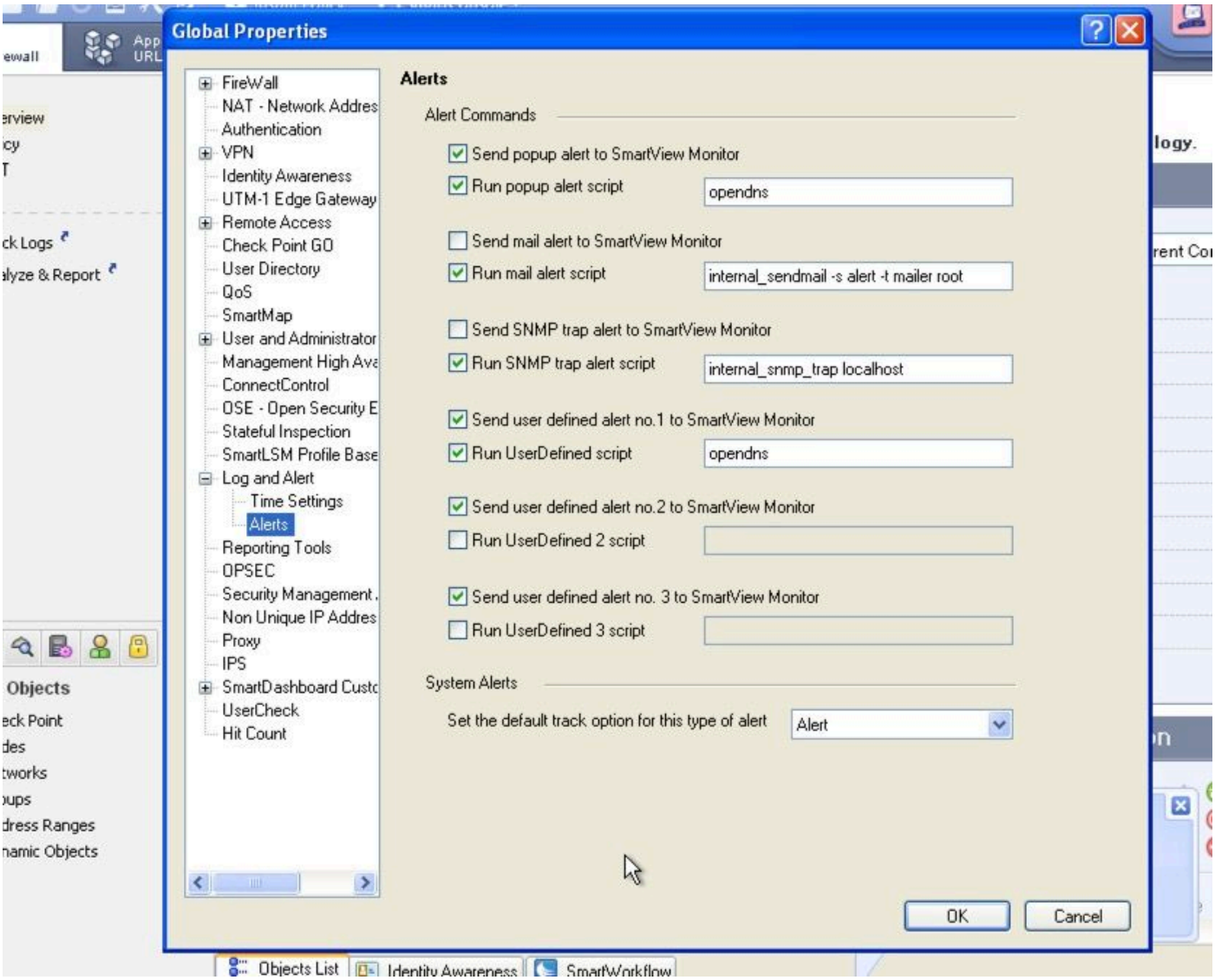
2. Open globale eigenschappen:



3. Open Log en waarschuwing > Waarschuwingen in Globale eigenschappen en voer de volgende stappen uit:

- Selecteer Pop-upwaarschuwingsscript verzenden en Door gebruiker gedefinieerd script uitvoeren.
- Definieer "opendns" in de scriptvelden voor beide.

4. Selecteer OK. Vanuit SmartDashboard slaat u het bijgewerkte beleid op en installeert u het.



Stap 4: Het testen van de integratie en het instellen van controlepuntgebeurtenissen die moeten worden geblokkeerd

Genereer eerst een test-antibotbladegebeurtenis die in het Cisco Umbrella Dashboard wordt weergegeven:

1. Laad vanaf elk apparaat op het netwerk dat wordt beschermd door uw Check Point-toestel deze URL in uw browser:

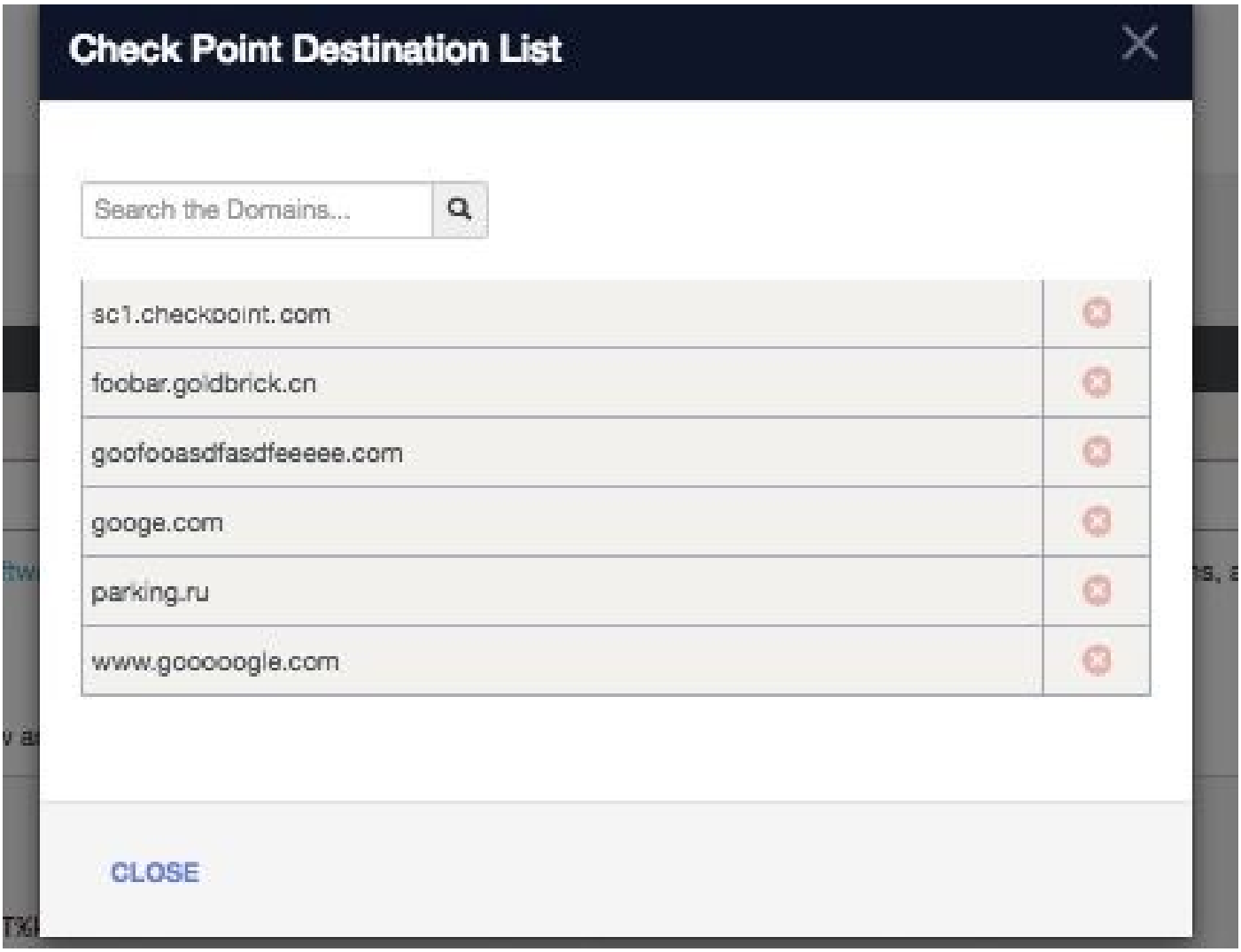
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

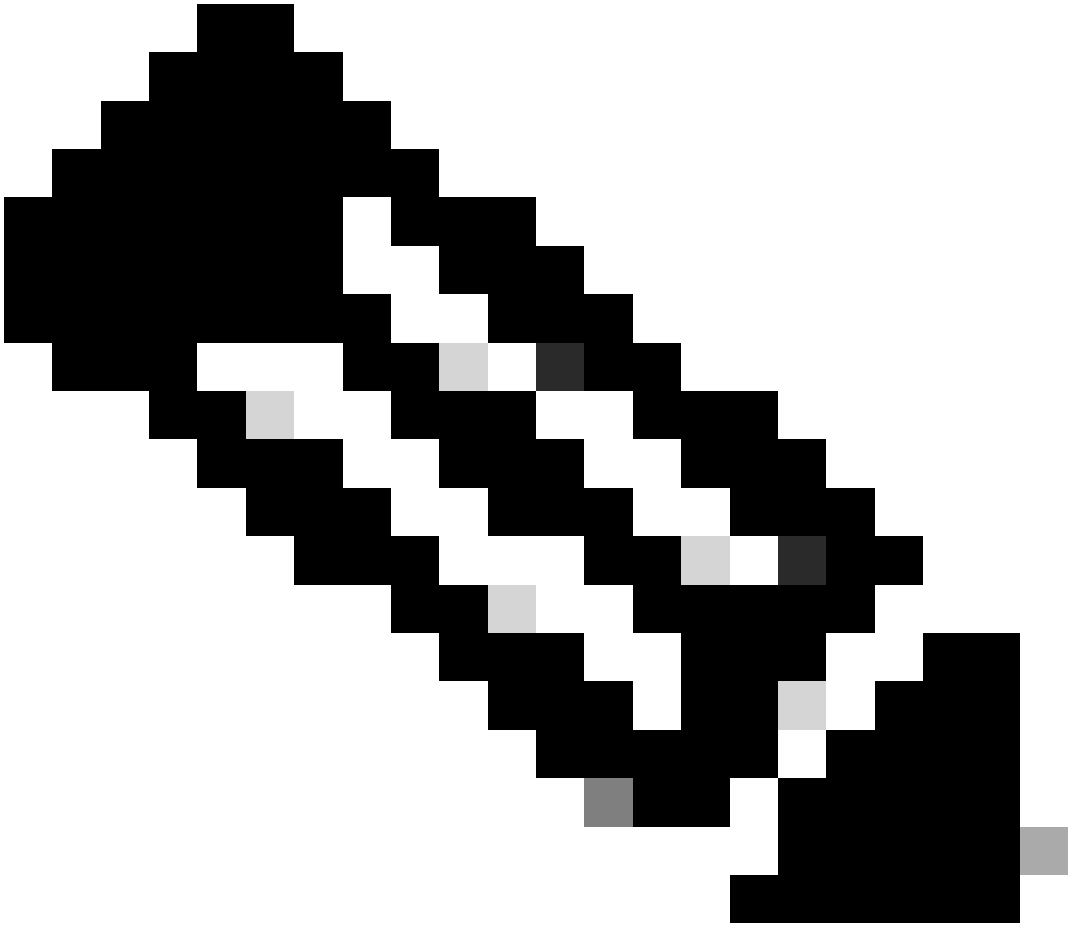
2. Meld u aan bij het Cisco Umbrella-dashboard als beheerder.

3. Navigeer naar Beleid > Beleidscomponenten > Integraties en selecteer Controlepunt in de tabel om deze uit te vouwen.

4. Selecteer Zie domeinen. Dit opent een venster met de bestemmingslijst van controlepunten die

"sc1.checkpoint.com" kan bevatten. Vanaf dat moment begint een doorzoekbare lijst te worden gevuld en te groeien.



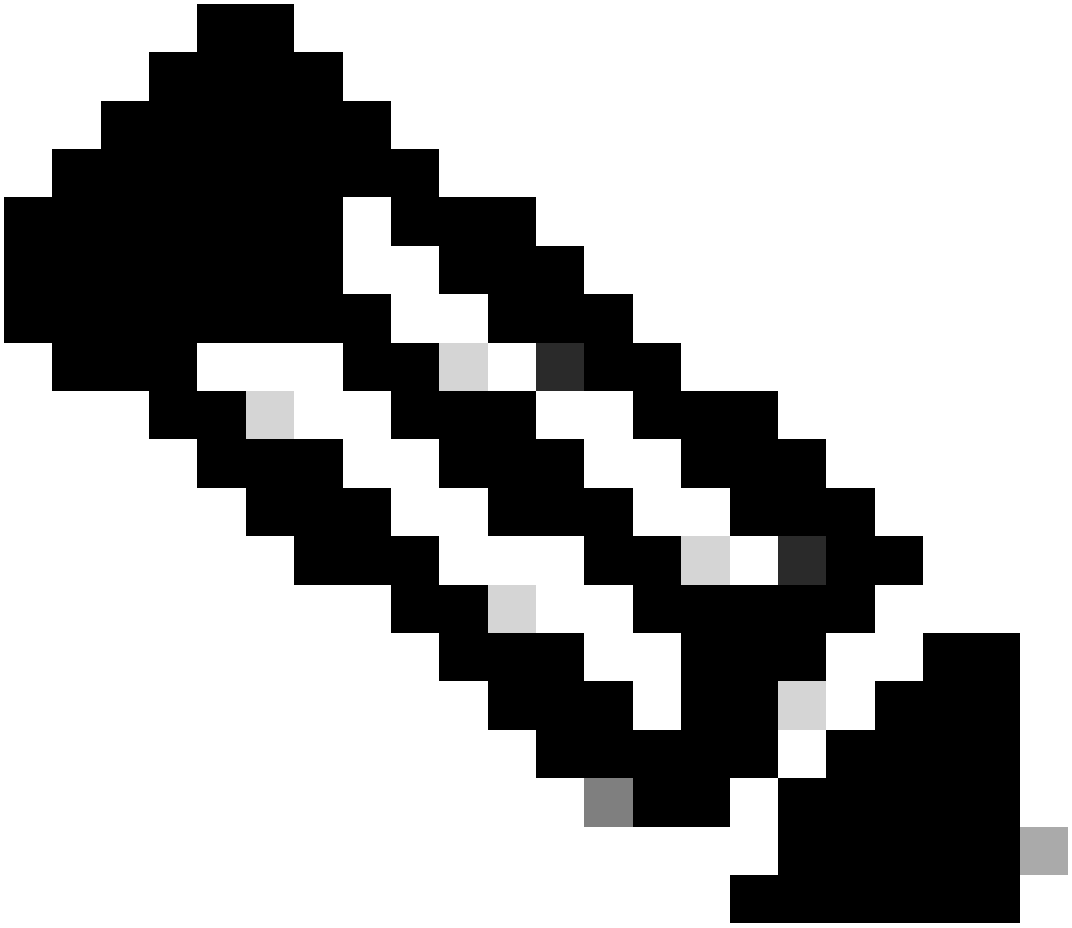


Opmerking: U kunt deze bestemmingslijst ook wijzigen als er een domein verschijnt waarop u het beleid niet wilt afdwingen. Selecteer het pictogram Verwijderen om het domein te verwijderen.

Waarnemen van gebeurtenissen toegevoegd aan de categorie Check Point Security in "Audit Mode"

De volgende stap is het observeren en controleren van de gebeurtenissen die zijn toegevoegd aan uw nieuwe beveiligingscategorie Check Point.

De gebeurtenissen uit uw Check Point-toestel beginnen een specifieke bestemmingslijst te vullen die kan worden toegepast op beleid als een Check Point-beveiligingscategorie. De doellijst en de beveiligingscategorie bevinden zich standaard in de "controlemodus" en worden niet toegepast op beleidsregels. Dit kan niet leiden tot wijzigingen in uw bestaande Cisco-beleidsregels.



Opmerking: de "Controlemodus" kan worden ingeschakeld zolang dit nodig is op basis van uw implementatieprofiel en netwerkconfiguratie.

Bestemmingslijst bekijken

U kunt de bestemmingslijst van controlepunten op elk gewenst moment bekijken in Cisco Umbrella:

1. Ga naar Beleid > Beleidscomponenten > Integraties.

2. Vouw Checkpoint in de tabel uit en selecteer Zie domeinen.

Beveiligingsinstellingen voor een beleid bekijken

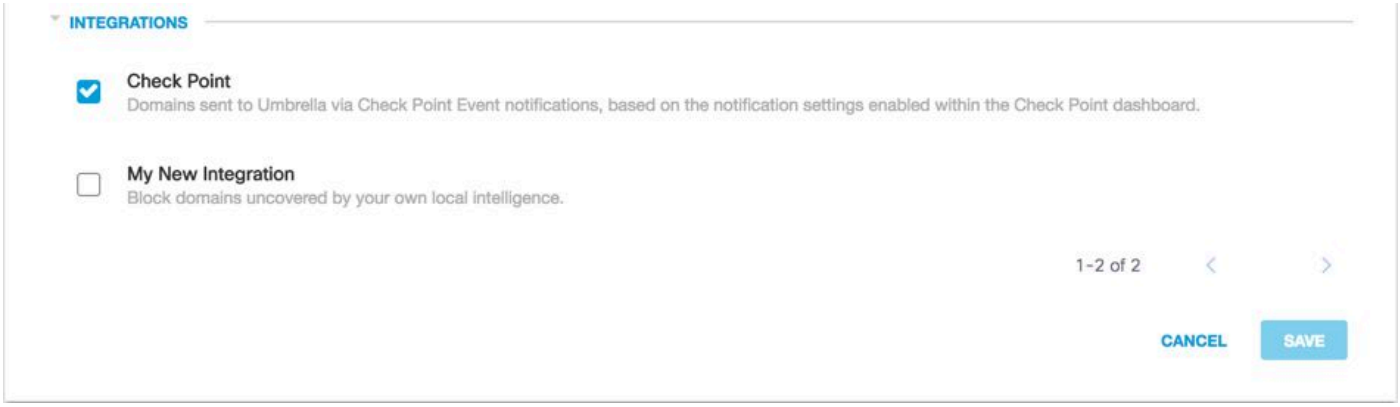
U kunt de beveiligingsinstellingen bekijken die op elk gewenst moment voor een beleid kunnen worden ingeschakeld in Cisco Umbrella:

1. Navigeer naar Beleid > Beleidscomponenten > Beveiligingsinstellingen.

2. Selecteer een beveiligingsinstelling in de tabel om deze uit te vouwen.

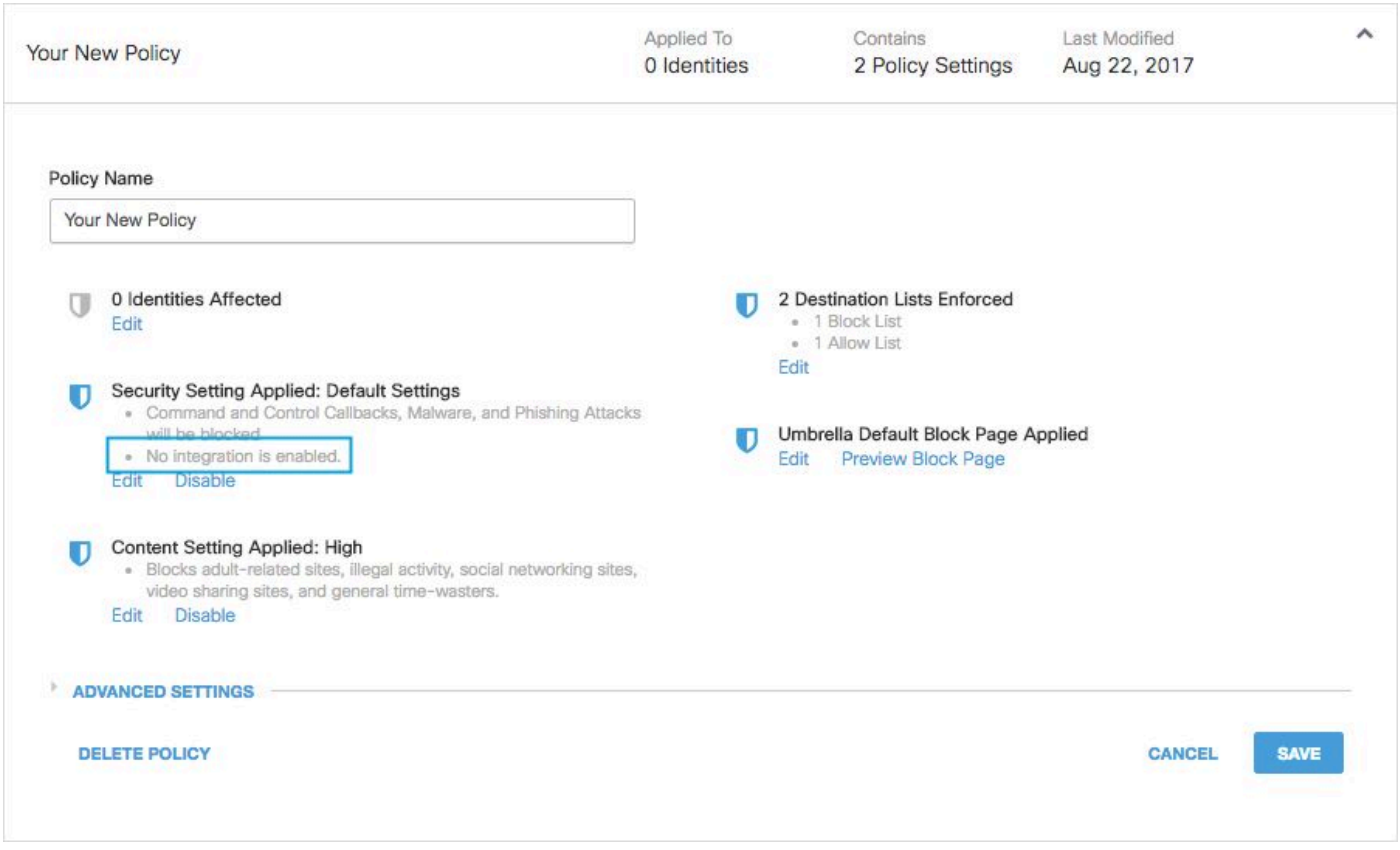
3. Blader naar de sectie Integraties en vouw de sectie uit om de integratie van het controlepunt weer te geven.

4. Selecteer de optie voor de Check Point-integratie en selecteer Opslaan.



115013984226

U kunt ook integratiegegevens bekijken via de pagina Overzicht van beveiligingsinstellingen:



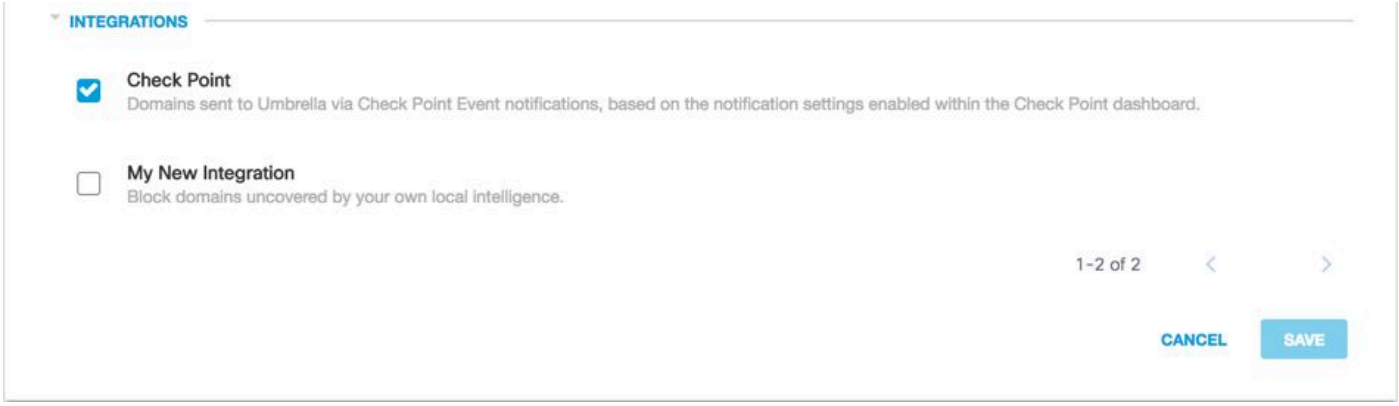
19916943300244

De beveiligingsinstellingen van het controlepunt in de "blokmodus" toepassen op een beleid voor beheerde clients

Zodra u klaar bent om deze extra beveiligingsbedreigingen te laten afdwingen door clients die worden beheerd door Cisco Umbrella, wijzigt u de beveiligingsinstelling voor een bestaand beleid of maakt u een nieuw beleid dat boven uw standaardbeleid staat om ervoor te zorgen dat het eerst wordt afgedwongen:

1. Zorg ervoor dat de integratie van het controlepunt nog steeds is ingeschakeld, zoals in de vorige sectie is gebeurd. Navigeer naar Beleid > Beleidscomponenten > Beveiligingsinstellingen en open de betreffende instelling.

2. Controleer onder Integraties of de optie Controlepunt is geselecteerd. Als dit niet het geval is, selecteert u de optie en selecteert u Opslaan.



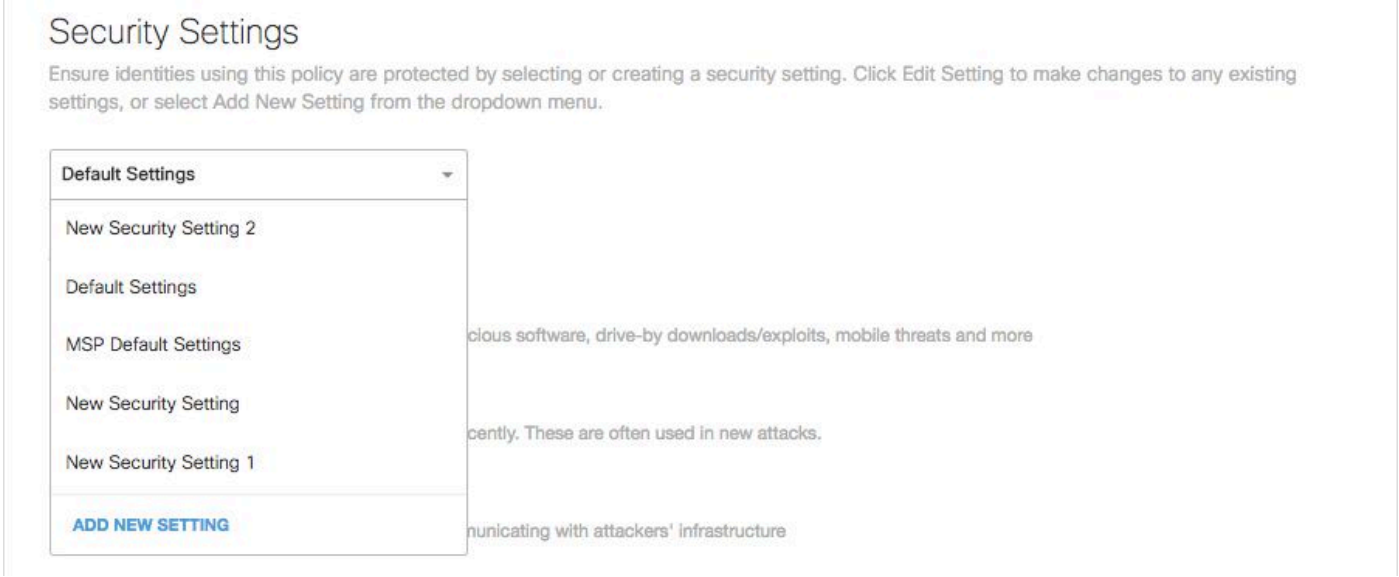
115013984226

Voeg vervolgens in de wizard Cisco Umbrella Policy deze beveiligingsinstelling toe aan een beleid dat u bewerkt:

1. Navigeer naar een beleid: Beleid > DNS-beleid of Beleid > Webbeleid.

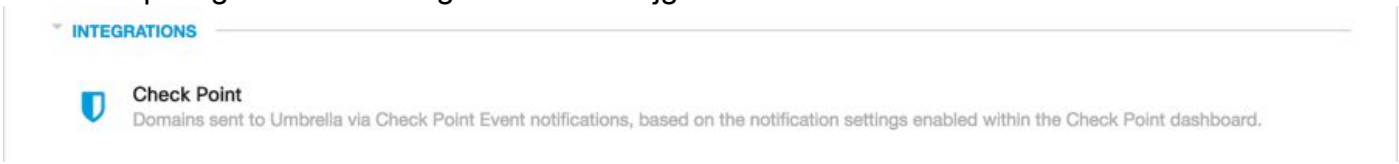
2. Vouw een beleid uit en selecteer Bewerken onder Beveiligingsinstellingen toegepast (DNS-beleid) of Beveiligingsinstellingen (Webbeleid).

3. Selecteer in de vervolgkeuzelijst Beveiligingsinstellingen een beveiligingsinstelling die de instelling Check Point bevat.



19916943316884

Het schildpictogram onder Integraties wordt bijgewerkt naar blauw.



115014149783

4. Selecteer Set & Return (DNS-beleid) of Save (webbeleid).

Check Point-domeinen in de beveiligingsinstelling voor Check Point kunnen vervolgens worden geblokkeerd voor die identiteiten die het beleid gebruiken.

Rapportage binnen Paraplu voor controlepuntgebeurtenissen

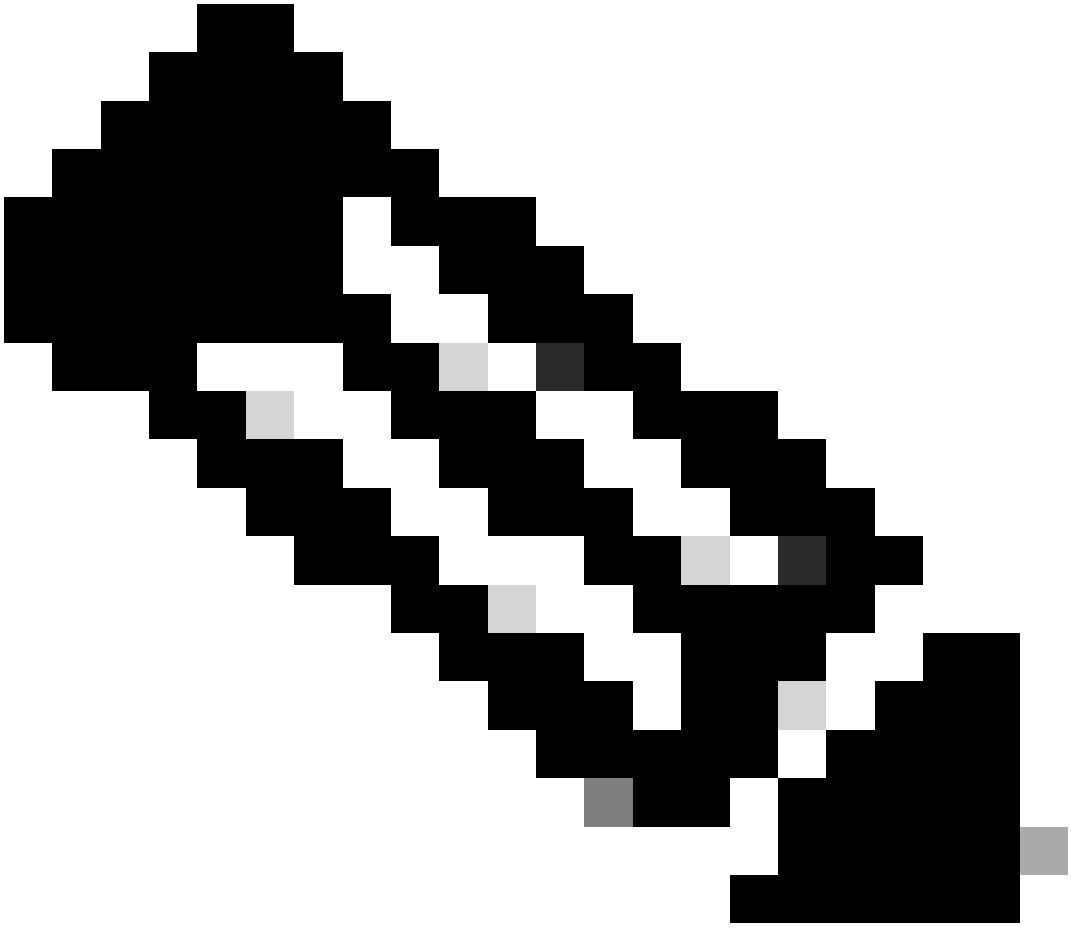
Rapportage over beveiligingsgebeurtenissen bij controlepunten

De bestemmingslijst van controlepunten is een van de beveiligingscategorieën die beschikbaar zijn voor rapporten. De meeste of alle rapporten gebruiken de beveiligingscategorieën als filter. U kunt bijvoorbeeld beveiligingscategorieën filteren om alleen activiteiten met betrekking tot controlepunten weer te geven:

1. Ga naar Rapportage > Kernrapporten > Zoeken naar activiteiten.

2. Selecteer onder Beveiligingscategorieën de optie Controlepunt om het rapport te filteren zodat alleen de beveiligingscategorie voor Controlepunt wordt weergegeven.

115014197623



Opmerking: Als de integratie van controlepunten is uitgeschakeld, kan deze niet worden weergegeven in het filter Beveiligingscategorieën.

3. Selecteer Toepassen om de activiteit met betrekking tot controlepunten voor de in het rapport geselecteerde periode te bekijken.

Rapporteren wanneer domeinen zijn toegevoegd aan de bestemmingslijst van controlepunten

Het controlelogboek van Cisco Umbrella Admin bevat gebeurtenissen uit het toestel Check Point, omdat het domeinen aan de bestemmingslijst toevoegt. Deze domeinen lijken te worden toegevoegd door een label "Check Point account", onder de kolom Gebruiker van het Audit-logboek.

Als u het controlelogboek van de Umbrella Admin wilt vinden, gaat u naar Rapportage > Controlelogboek van de beheerder.

Als u wilt rapporteren wanneer een domein is toegevoegd, filtert u om alleen wijzigingen in controlepunten op te nemen door een filter Filter op identiteit en instellingen toe te passen voor de blokkeringslijst van controlepunten.

Nadat u het rapport hebt uitgevoerd, ziet u een lijst met domeinen die zijn toegevoegd aan de bestemmingslijst van controlepunten.

Omgaan met ongewenste detecties of valse positieven

Een lijst met machtigingen voor ongewenste detectie beheren

Hoewel onwaarschijnlijk, is het mogelijk dat domeinen die automatisch door uw Check Point-toestel worden toegevoegd, een ongewenste blokkering kunnen veroorzaken waardoor uw gebruikers worden geblokkeerd voor toegang tot bepaalde websites. In een situatie als deze raadt Cisco Umbrella aan om de domeinnamen toe te voegen aan een lijst met machtigingen, die voorrang heeft op alle andere soorten bloklijsten, inclusief beveiligingsinstellingen. Een allow-lijst heeft voorrang op een block-lijst wanneer een domein in beide aanwezig is.

Er zijn twee redenen waarom deze aanpak de voorkeur heeft:

- Ten eerste, in het geval dat het Check Point-apparaat het domein opnieuw zou toevoegen nadat het was verwijderd, staat de lijst beveiligingen toe om dit te voorkomen en verdere problemen te veroorzaken.
- Ten tweede toont de allow-lijst een historisch record van problematische domeinen voor later forensisch onderzoek of controleverslagen.

Standaard is er een algemene lijst met toegestane items die wordt toegepast op alle beleidsregels. Als u een domein toevoegt aan de algemene machtigingslijst, wordt het domein toegestaan in alle beleidsregels.

Als de beveiligingsinstelling voor controlepunten in de blokmodus alleen wordt toegepast op een subset van uw beheerde Cisco Umbrella-identiteiten (deze wordt bijvoorbeeld alleen toegepast op zwervende computers en mobiele apparaten), kunt u een specifieke machtigingslijst maken voor die identiteiten of beleidsregels.

U maakt als volgt een lijst met machtigingen:

1. Navigeer naar Beleid > Bestemmingslijsten en selecteer het pictogram Toevoegen.

2. Selecteer Toestaan en voeg uw domein toe aan de lijst.

3. Selecteer Opslaan.

Zodra de lijst is opgeslagen, kunt u deze toevoegen aan een bestaand beleid voor die clients die zijn getroffen door het ongewenste blok.

Domeinen verwijderen uit de bestemmingslijst van controlepunten

Naast elke domeinnaam in de bestemmingslijst van Check Point staat een pictogram Verwijderen. Als u domeinen verwijdert, kunt u de bestemmingslijst van het controlepunt opschonen in het geval van ongewenste detectie.

De verwijdering is echter niet permanent als het Check Point-toestel het domein opnieuw doorstuurt naar Cisco Umbrella.

Een domein verwijderen:

1. Navigeer naar Instellingen > Integraties en selecteer Check Point om het uit te vouwen.

2. Selecteer Zie domeinen.

3. Zoek naar de domeinnaam die u wilt verwijderen.

4. Selecteer het pictogram Verwijderen.

5. Selecteer Sluiten.

6. Selecteer Opslaan.

Als er een ongewenste detectie of fout-positief is, raadt Cisco Umbrella aan om onmiddellijk een lijst met machtigingen in Cisco Umbrella te maken en vervolgens het fout-positieve in het Check Point Appliance te herstellen. Later kunt u het domein verwijderen uit de bestemmingslijst van het controlepunt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.