Check Point Anti-Bot 소프트웨어 블레이드로 Umbrella 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

개요

기능

컨피그레이션 단계

- 서비스 중단 방지
- 1단계: Umbrella 스크립트 및 API 토큰 생성
- 2단계: Check Point Appliance에 사용자 지정 스크립트 구축
- 3단계. 새 스크립트에 게시할 검사점 경고 작성 또는 편집
- 4단계: 차단할 통합 테스트 및 검사점 이벤트 설정

"감사 모드"에서 검사점 보안 카테고리에 추가된 이벤트 관찰

- 대상 목록 검토
- 정책에 대한 보안 설정 검토

관리되는 클라이언트에 대한 정책에 "차단 모드"의 검사점 보안 설정 적용

Umbrella에서 Check Point 이벤트에 대한 보고

- Check Point 보안 이벤트 보고
- 도메인이 Check Point 대상 목록에 추가된 경우 보고

원치 않는 탐지 또는 오탐 처리

- 원치 않는 탐지에 대한 허용 목록 관리
- Check Point 대상 목록에서 도메인 삭제

소개

이 문서에서는 Cisco Umbrella를 Check Point Anti-Bot 소프트웨어 블레이드와 통합하는 방법에 대해 설명합니다.

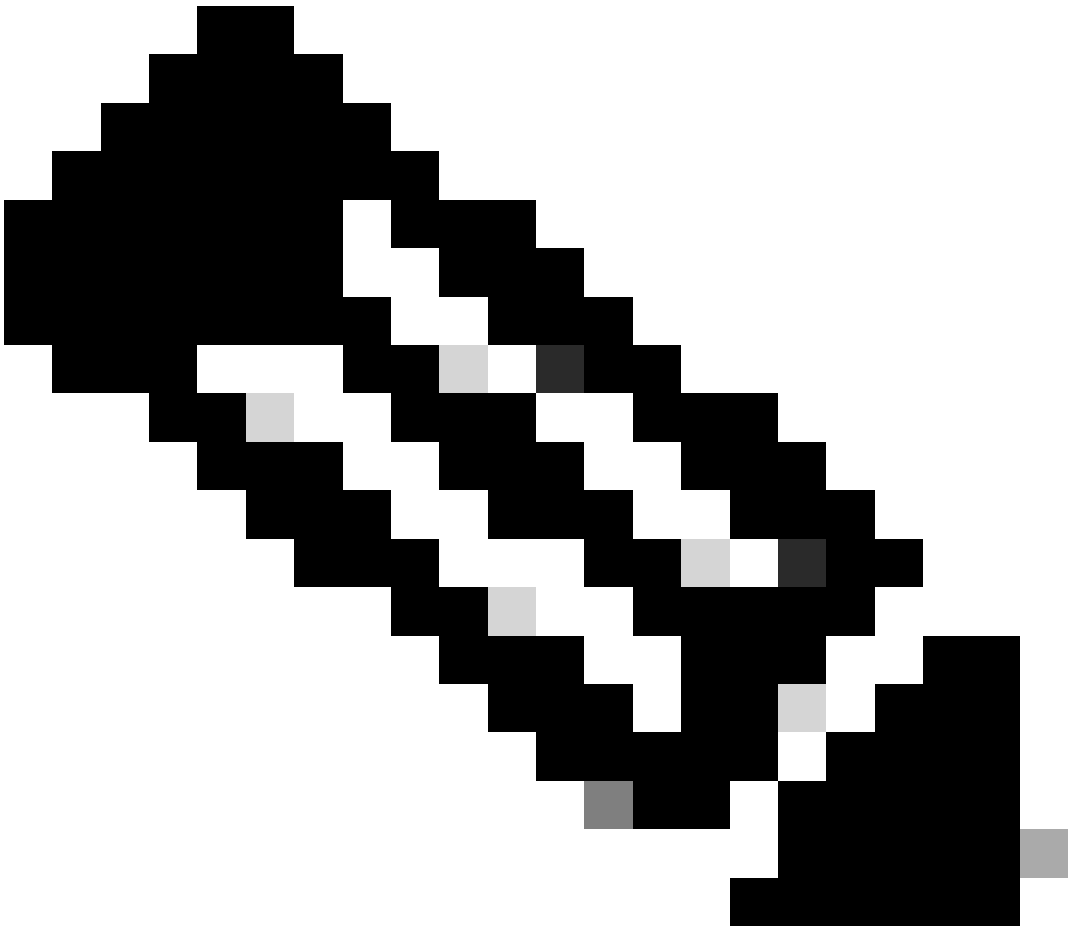
사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Anti-Bot 소프트웨어 블레이드가 있는 체크포인트 장치
- Check Point 소프트웨어 버전 R80.40 이상

- Check Point 디바이스가 "https://s-platform.api.opendns.com"에 아웃바운드 HTTP 요청을 수행할 수 있는지 확인합니다.
- DNS Essentials, DNS Advantage, SIG Essentials 또는 SIG Advantage와 같은 Cisco Umbrella 패키지
- Cisco Umbrella 대시보드 관리 권한



참고: Check Point 통합은 DNS Essentials, DNS Advantage, SIG Essentials 또는 SIG Advantage와 같은 Cisco Umbrella 패키지에만 포함됩니다. 이러한 패키지 중 하나가 없는 경우 Check Point 통합을 원할 경우 Cisco Umbrella Account Manager에게 문의하십시오. 올바른 Cisco Umbrella 패키지가 있지만 대시보드의 통합으로 Check Point가 표시되지 않는 경우 Cisco Umbrella Support에 문의하십시오.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

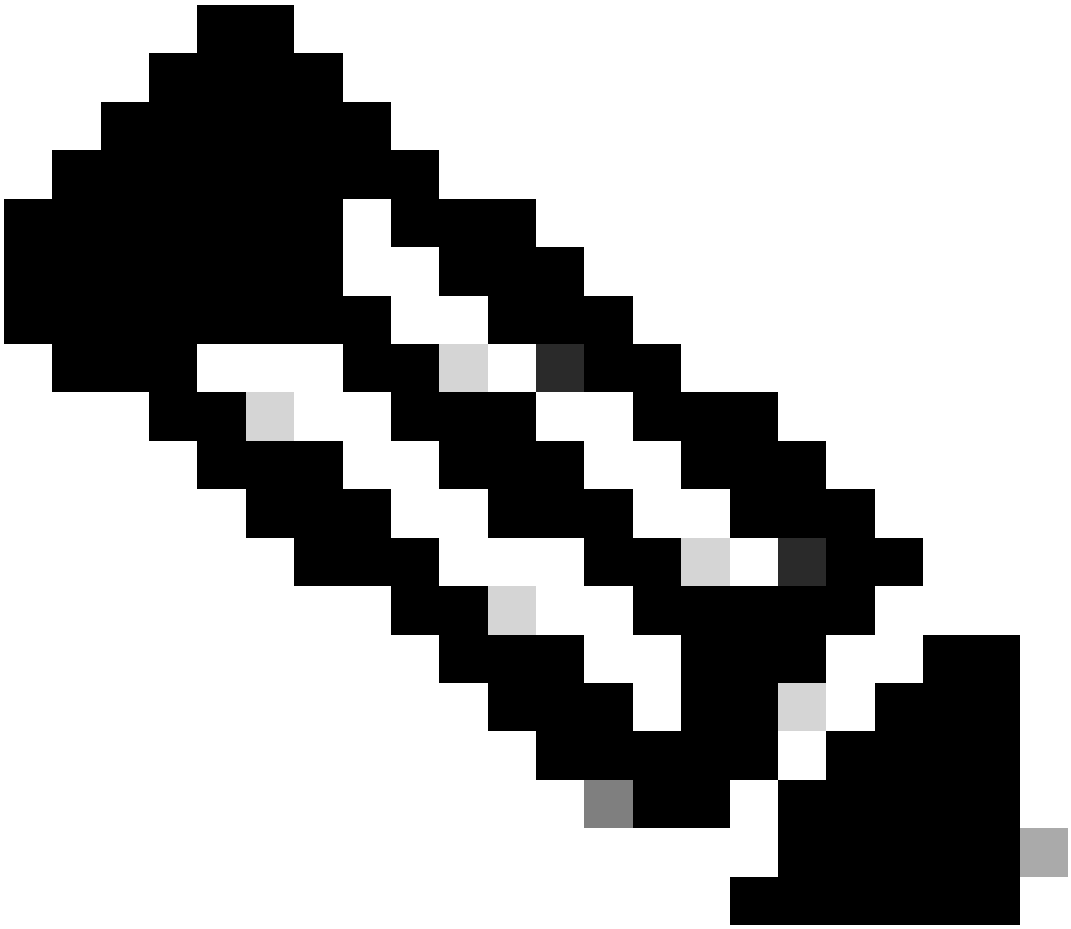
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Cisco Umbrella와 Check Point Anti-Bot Software Blade가 통합되어 검사하는 네트워크 트래픽에서 블레이드가 위협을 발견하면 Check Point 디바이스가 Anti-Bot Software Blade 알림을 Cisco Umbrella로 전송할 수 있습니다. Cisco Umbrella에서 수신한 알림은 Check Point Anti-Bot 소프트웨어 블레이드로 보호되지 않는 네트워크에서 로밍 중인 노트북 컴퓨터, 태블릿 및 전화기를 보호할 수 있는 차단 목록을 작성합니다.

이 문서에서는 Cisco Umbrella에 안티봇 소프트웨어 블레이드 알림을 전송하도록 Check Point 디바이스를 구성하는 방법을 설명합니다.



참고: 이 통합은 R80.40에서 처음 릴리스된 이후 버전 R81.20의 Check Point에서 더 이상 사용되지 않습니다.

기능

Cisco Umbrella와 Check Point Anti-Bot Software Blade Appliance는 발견된 위협(예: 악성코드, 봇넷을 위한 명령 및 제어, 피싱 사이트를 호스팅하는 도메인)을 글로벌 시행을 위해 Cisco Umbrella로 푸시합니다.

그런 다음 Cisco Umbrella는 위협을 검증하여 정책에 추가할 수 있는지 확인합니다. Check Point Anti-Bot Software Blade의 정보가 위협으로 확인되면 도메인 주소가 Cisco Umbrella 정책에 적용할 수 있는 보안 설정의 일부로 Check Point Destination List에 추가됩니다. 해당 정책은 해당 정책에 할당된 디바이스에서 생성되는 모든 요청에 즉시 적용됩니다.

앞으로 Cisco Umbrella는 Check Point 알림을 자동으로 구문 분석하고 악의적인 사이트를 Check Point Destination List에 추가합니다. 따라서 모든 원격 사용자 및 장치에 대해 Check Point 보호 기능이 확대되고 기업 네트워크에 대한 또 다른 적용 계층이 제공됩니다.

컨피그레이션 단계

통합 구성에는 다음 단계가 포함됩니다.

1. Cisco Umbrella의 통합을 활성화하여 맞춤형 스크립트로 API 토큰을 생성합니다.
2. Check Point 어플라이언스에 API 토큰 및 사용자 지정 스크립트를 구축합니다.
3. 이 새 스크립트에 게시할 검사점 알림 작성/편집
4. Cisco Umbrella 내에서 Check Point 이벤트를 차단하도록 설정합니다.

서비스 중단 방지

원치 않는 서비스 중단을 방지하기 위해 Cisco Umbrella는 통합을 구성하기 전에 차단될 수 없는 미션 크리티컬 도메인 이름(예: google.com 또는 salesforce.com)을 전역 허용 목록(또는 정책에 따라 다른 대상 목록)에 추가할 것을 권장합니다.

미션 크리티컬 도메인은 다음과 같습니다.

- 조직의 홈 페이지
- 사용자가 제공하는 서비스를 나타내는 도메인으로서 내부 및 외부 레코드를 모두 포함할 수 있습니다. 예: "mail.myservicedomain.com" 및 "portal.myotherservicedomain.com"
- Cisco Umbrella에 의존하는 잘 알려지지 않은 클라우드 기반 애플리케이션은 자동 도메인 검증에 포함할 수 없습니다. 예: "localcloudservice.com".

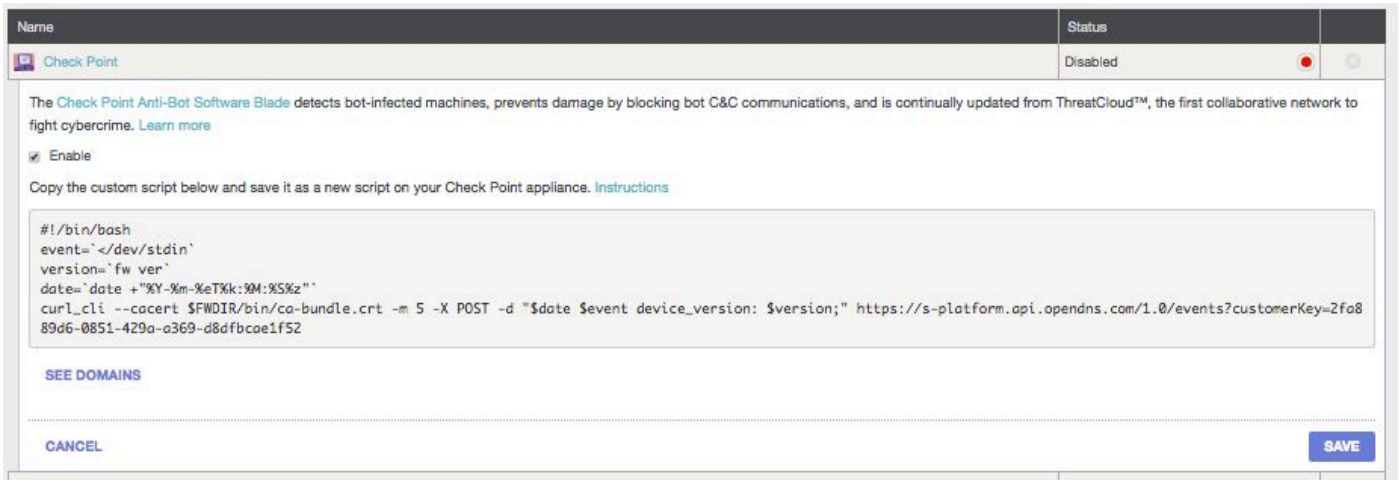
이러한 도메인은 Cisco Umbrella의 Policies(정책) > Destination Lists(대상 목록)에 있는 Global Allow List(전역 허용 목록)에 추가해야 합니다.

1단계: Umbrella 스크립트 및 API 토큰 생성

1. Cisco Umbrella 대시보드에 관리자로 로그인합니다.

2. Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동하고 테이블에서 Check Point(검사점)를 선택하여 확장합니다.

3. 사용가능 옵션을 선택합니다.



4. 다음 행부터 전체 스크립트를 복사합니다.

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

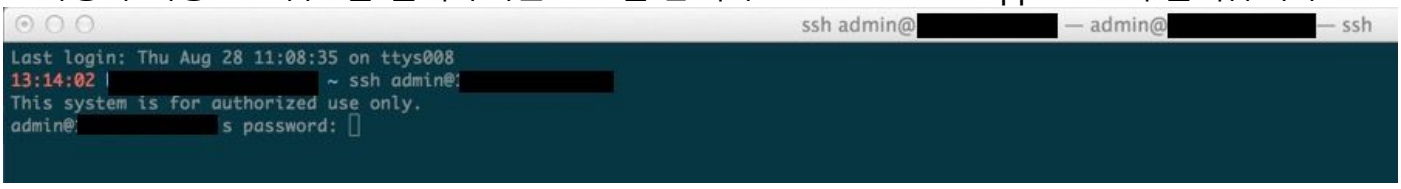
그런 다음 이후 단계에서 스크립트를 사용할 수 있습니다.

5. 저장을 선택하여 통합을 활성화합니다.

2단계: Check Point Appliance에 사용자 지정 스크립트 구축

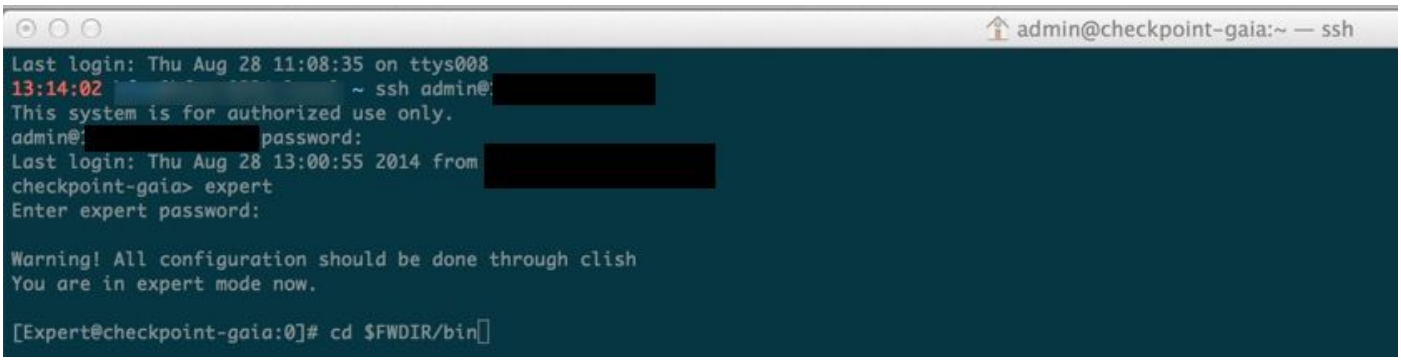
다음 단계는 Check Point 어플라이언스에 맞춤형 Cisco Umbrella 스크립트를 설치한 다음 SmartDashboard에서 활성화하는 것입니다.

1. 사용자 지정 스크립트를 설치하려면 SSH를 관리자로 Check Point Appliance에 설치합니다.

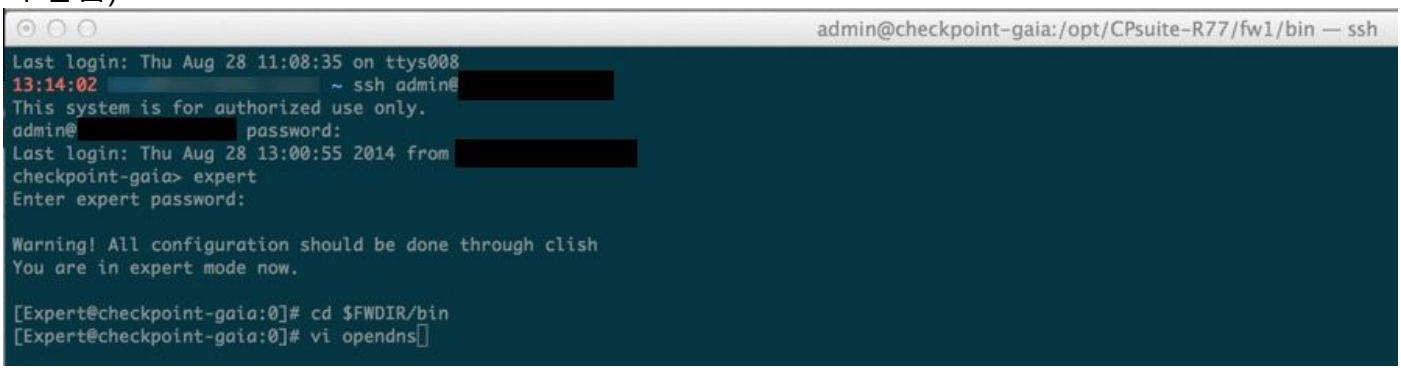


2. 다음 명령줄에 "expert"를 입력하여 "Expert Mode"를 시작합니다.

3. 작업 디렉토리를 `$FWDIR/bin`으로 변경합니다.

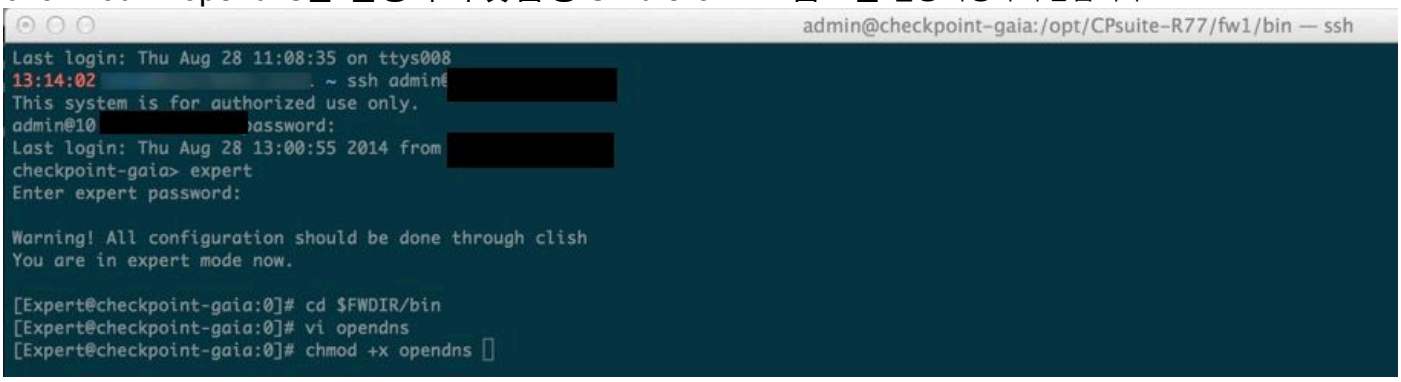


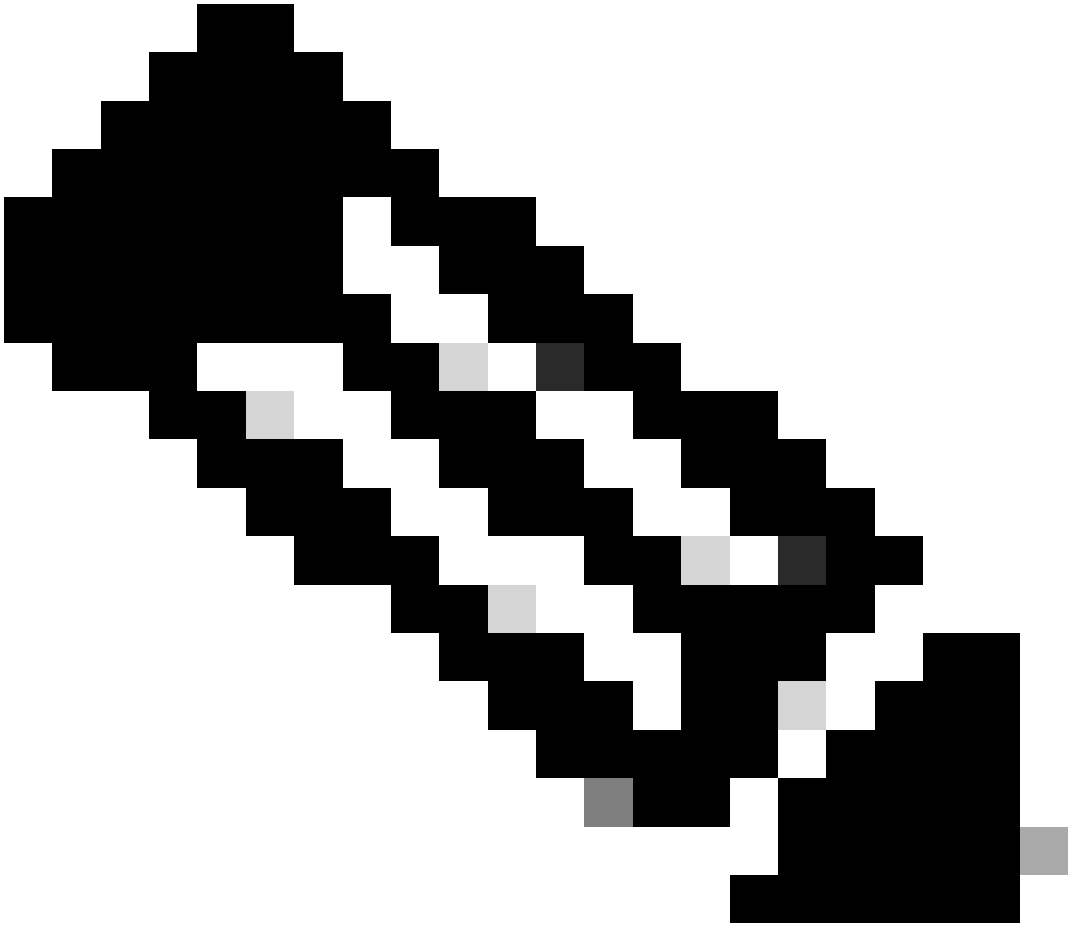
4. 텍스트 편집기를 사용하여 "opendns"라는 이름의 새 파일을 엽니다("vi" 편집기를 사용하는 예제와 같음).



5. Cisco Umbrella 스크립트를 파일에 붙여넣은 다음 파일을 저장하고 편집기를 종료합니다.

6. chmod +x opendns를 실행하여 맞춤형 Umbrella 스크립트를 실행 가능하게 만듭니다.





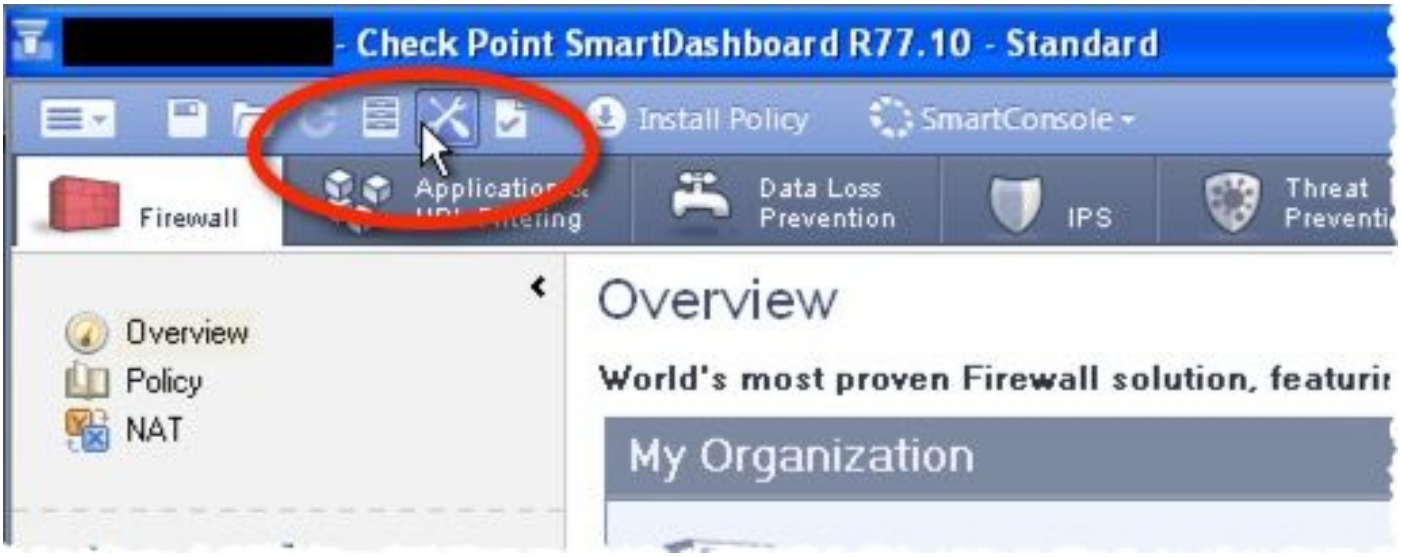
참고: 블레이드 버전을 업그레이드하거나 변경할 경우, 해당 새 버전에 대해 이 단계를 반복해야 합니다.

3단계. 새 스크립트에 게시할 검사점 경고 작성 또는 편집

1. SmartDashboard에 로그인하고 SmartDashboard를 시작하여 새 스크립트를 게시하도록 SmartDashboard를 활성화합니다.


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

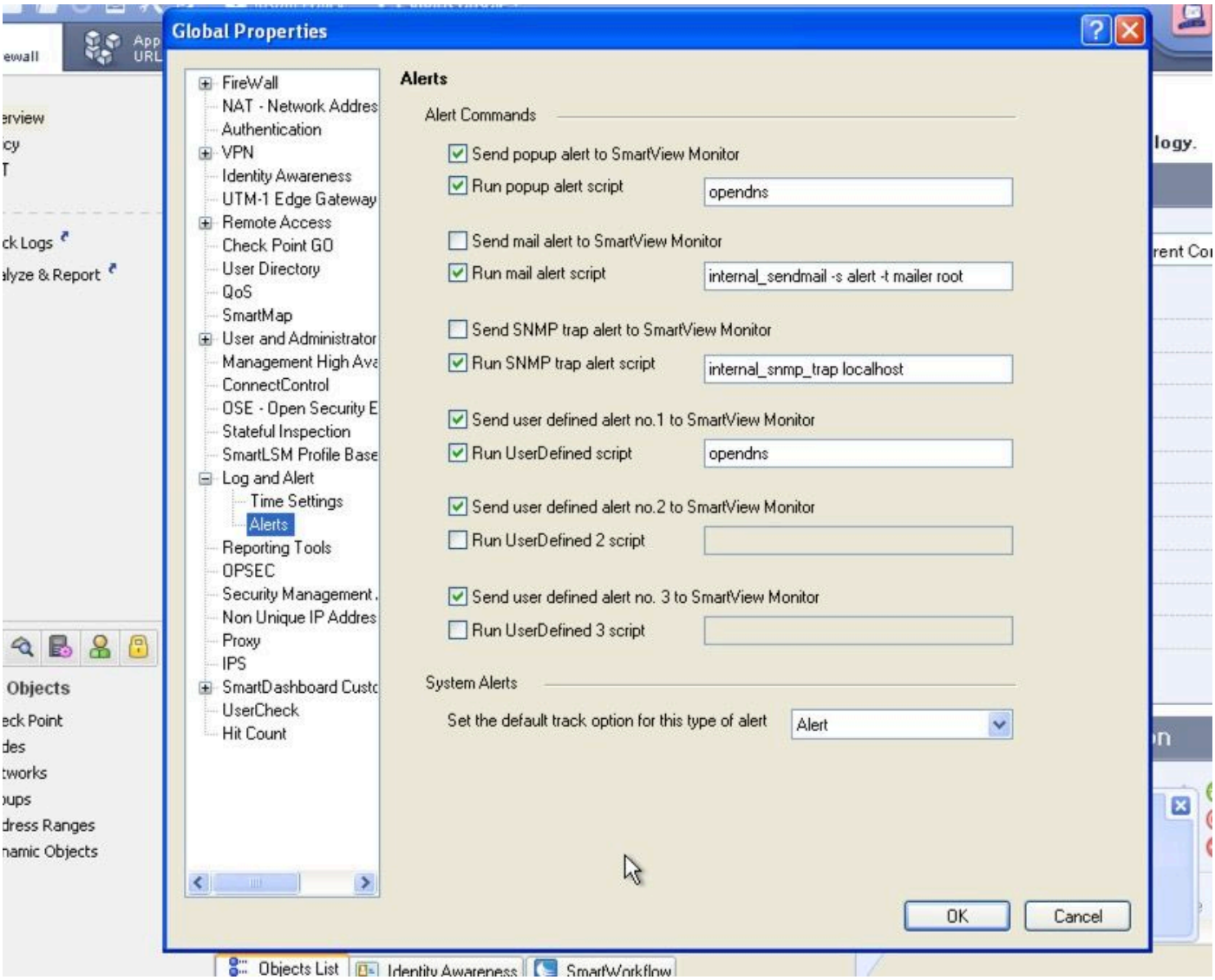
2. 글로벌 등록 정보 열기



3. Global Properties(전역 속성)에서 Log and Alert(로그 및 경고) > Alerts(경고)를 열고 다음 단계를 완료합니다.

- Send popup alertscript and Run UserDefined script를 선택합니다.
- 스크립트 필드에서 둘 모두에 대해 "opendns"를 정의합니다.

4. 확인을 선택합니다. SmartDashboard에서 갱신된 정책을 저장하고 설치합니다.



4단계: 차단할 통합 테스트 및 검사점 이벤트 설정

먼저 Cisco Umbrella Dashboard에 나타날 테스트 안티봇 블레이드 이벤트를 생성합니다.

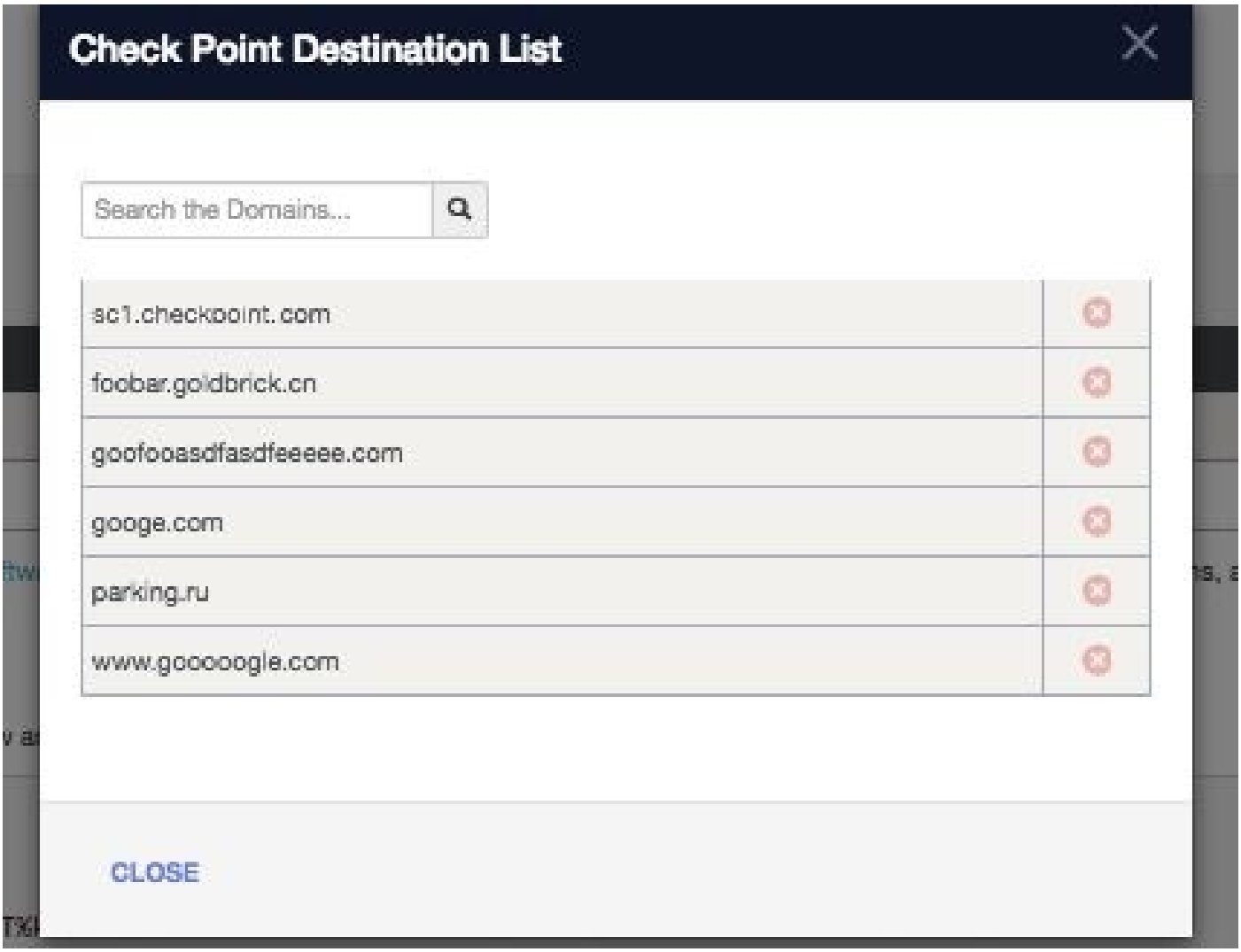
1. Check Point Appliance로 보호되는 네트워크의 모든 디바이스에서 다음 URL을 브라우저에 로드합니다.

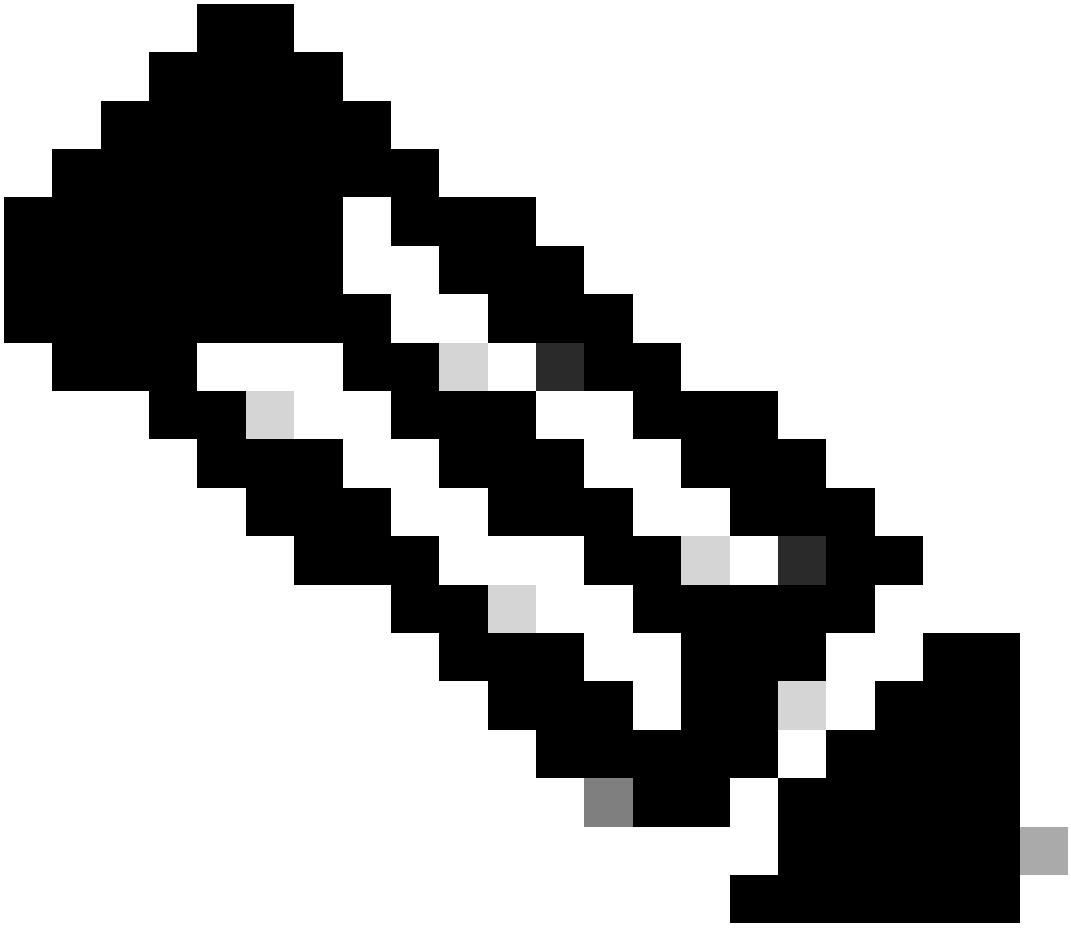
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

2. Cisco Umbrella 대시보드에 관리자로 로그인합니다.

3. Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동하고 테이블에서 Check Point(체크포인트)를 선택하여 확장합니다.

4. 도메인 보기를 선택합니다. 그러면 "sc1.checkpoint.com"를 포함할 수 있는 Check Point Destination List(체크포인트 대상 목록)가 표시된 창이 열립니다. 그 시점부터 검색 가능한 목록이 채워지고 확장되기 시작합니다.


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

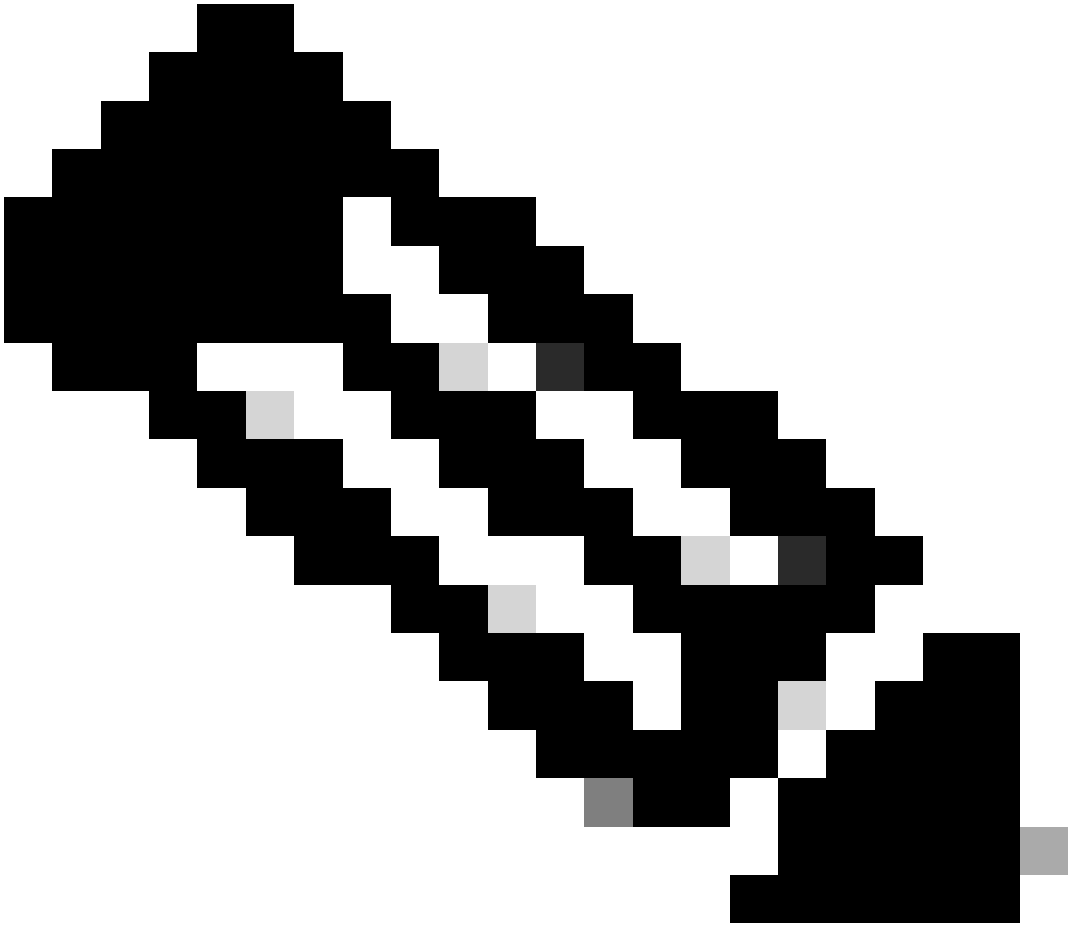


참고: 여기에 정책을 적용하지 않으려는 도메인이 표시되면 이 대상 목록을 변경할 수도 있습니다. 도메인을 제거하려면 삭제 아이콘을 선택합니다.

"감사 모드"에서 검사점 보안 카테고리에 추가된 이벤트 관찰

다음 단계는 새로운 Check Point 보안 카테고리에 추가된 이벤트를 관찰하고 감사하는 것입니다.

Check Point 어플라이언스의 이벤트가 특정 대상 목록을 채우기 시작합니다. 이 목록은 정책에 Check Point 보안 카테고리로 적용할 수 있습니다. 기본적으로 대상 목록 및 보안 카테고리는 "감사 모드"에 있으며 어떤 정책에도 적용되지 않으며 기존 Cisco Umbrella 정책을 변경할 수 없습니다.



참고: "감사 모드"는 구축 프로파일 및 네트워크 컨피그레이션에 따라 얼마든지 활성화할 수 있습니다.

대상 목록 검토

Cisco Umbrella에서 언제든지 Check Point Destination List(체크 포인트 대상 목록)를 검토할 수 있습니다.

1. Policies(정책) > Policy Components(정책 구성 요소) > Integrations(통합)로 이동합니다.

2. 테이블에서 Check Point를 확장하고 See Domains(도메인 보기)를 선택합니다.

정책에 대한 보안 설정 검토

Cisco Umbrella에서 언제든지 정책에 대해 활성화할 수 있는 보안 설정을 검토할 수 있습니다.

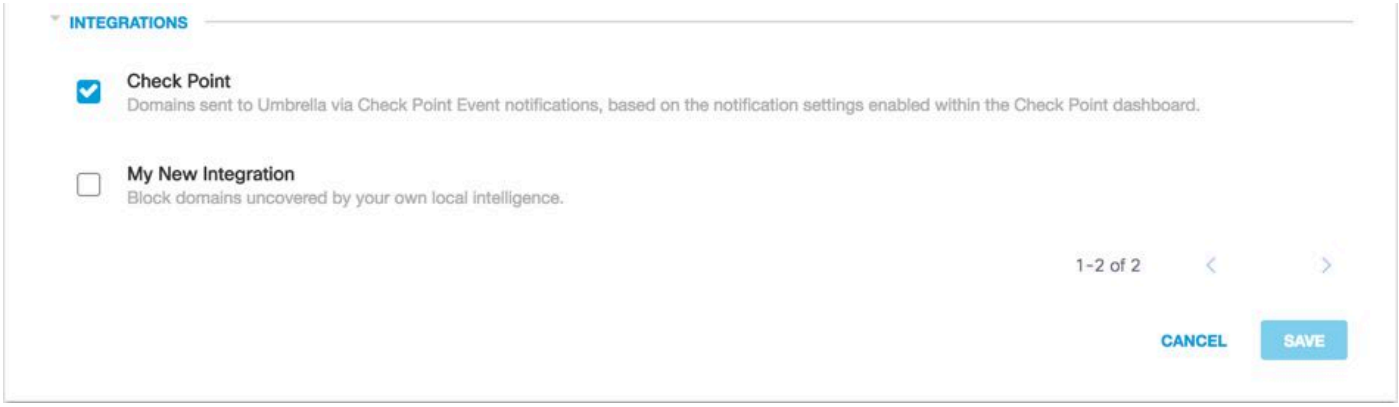
1. Policies(정책) > Policy Components(정책 구성 요소) > Security Settings(보안 설정)로 이동합니

다.

2. 테이블에서 보안 설정을 선택하여 확장합니다.

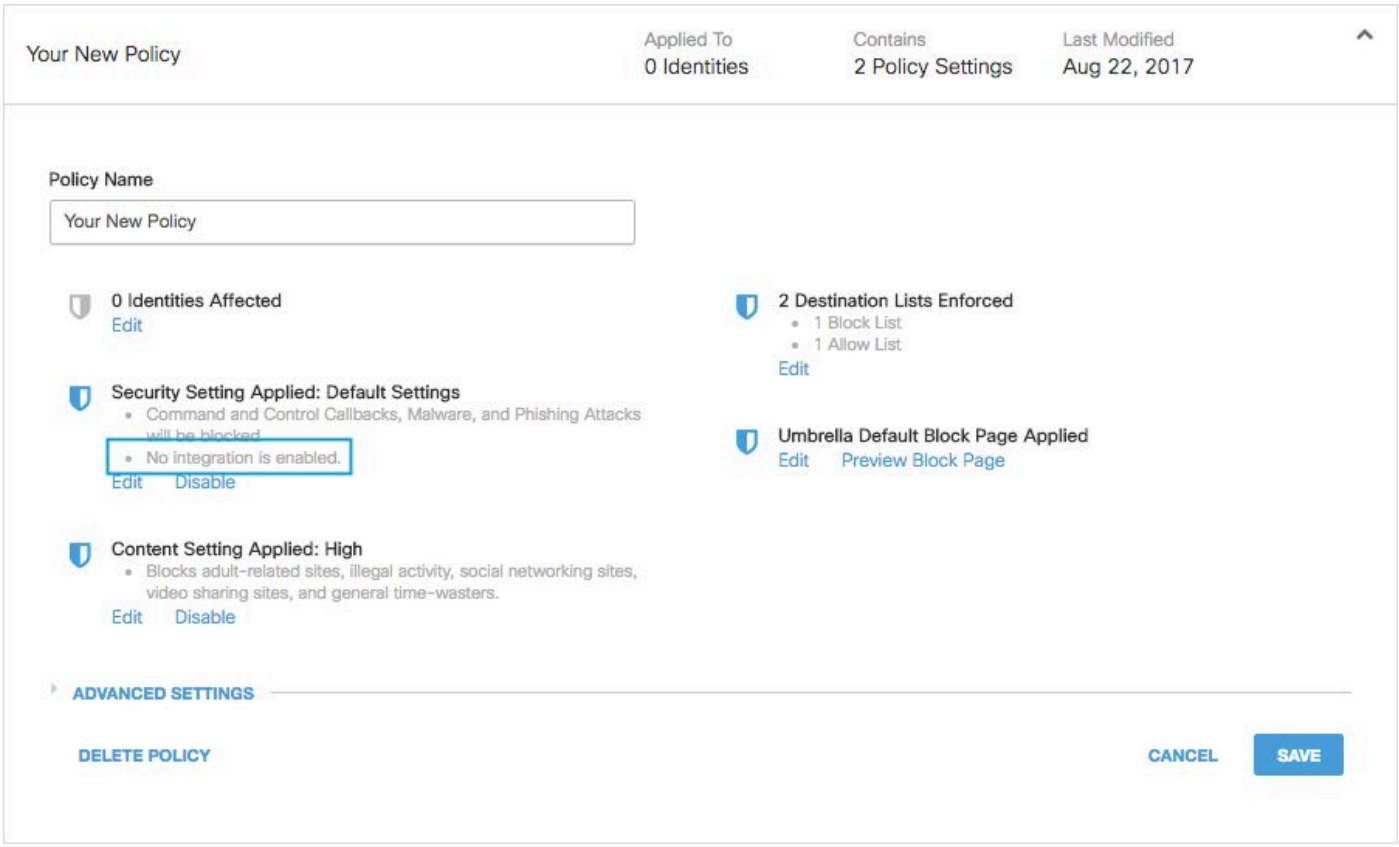
3. 통합 섹션으로 스크롤하고 섹션을 확장하여 체크포인트 통합을 표시합니다.

4. 체크포인트 통합에 대한 옵션을 선택한 다음 저장을 선택합니다.



115013984226

보안 설정 요약 페이지를 통해 통합 정보를 검토할 수도 있습니다.



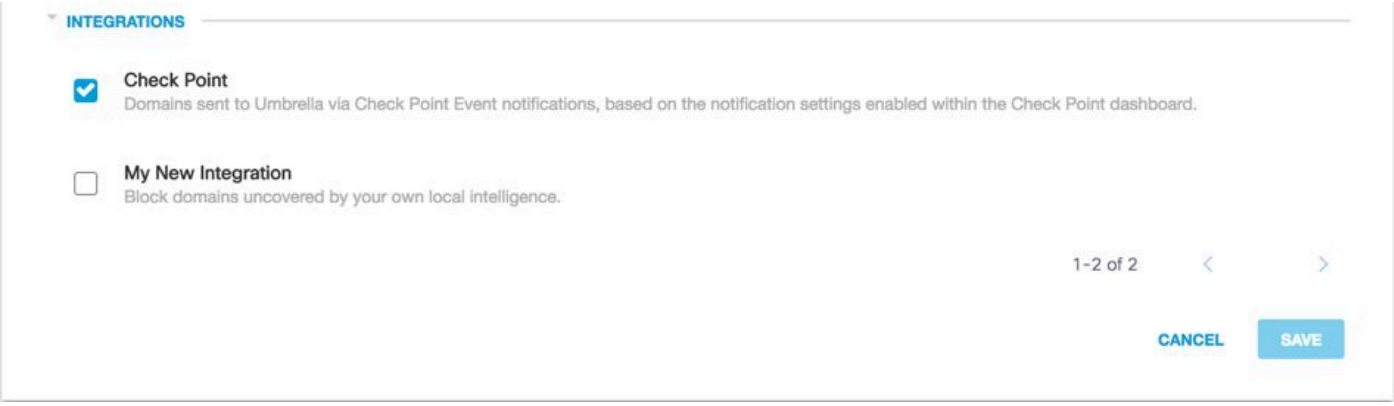
19916943300244

관리되는 클라이언트에 대한 정책에 "차단 모드"의 검사점 보안 설정 적용

Cisco Umbrella에서 관리하는 클라이언트에 의해 이러한 추가 보안 위협이 시행될 준비가 되면 기존 정책의 보안 설정을 변경하거나 기본 정책 위에 있는 새 정책을 생성하여 해당 정책이 먼저 시행되도록 합니다.

1. 이전 섹션에서 수행한 것처럼 검사점 통합이 계속 활성화되어 있는지 확인합니다. Policies(정책) > Policy Components(정책 구성 요소) > Security Settings(보안 설정)로 이동하고 관련 설정을 엽니다.

2. 통합 아래에서 Check Point 옵션이 선택되었는지 확인합니다. 그렇지 않은 경우 옵션을 선택하고 저장을 선택합니다.



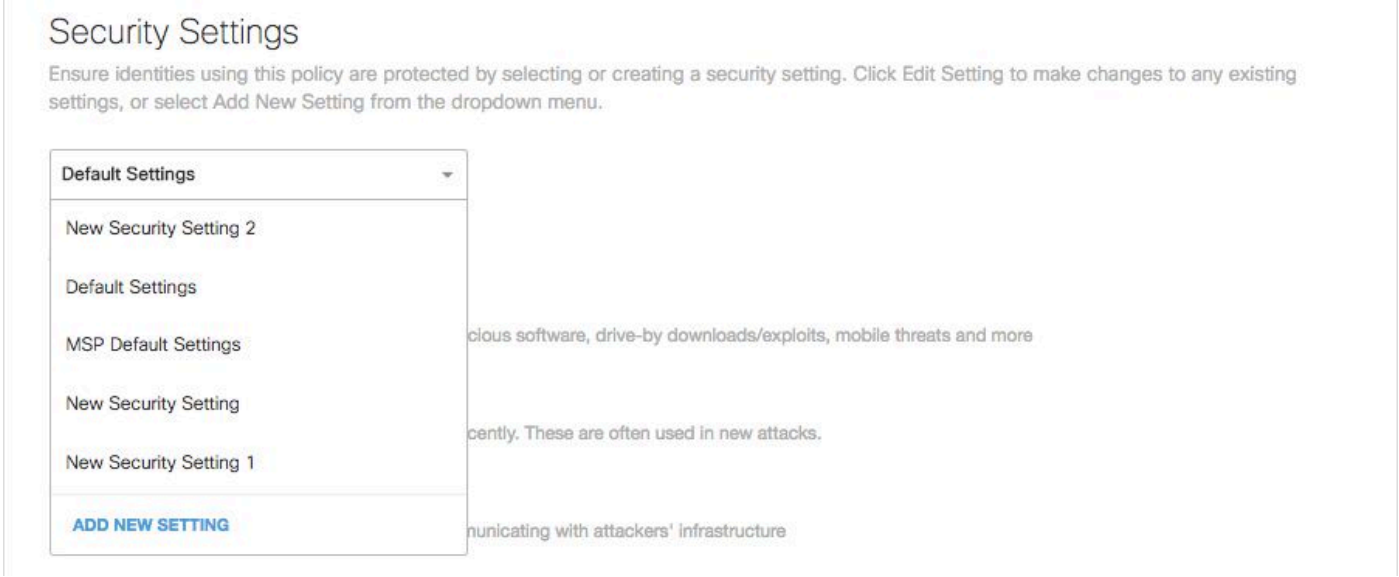
115013984226

다음으로, Cisco Umbrella Policy(Cisco Umbrella 정책) 마법사에서 수정 중인 정책에 이 보안 설정을 추가합니다.

1. 정책으로 이동합니다. Policies(정책) > DNS Policies(DNS 정책) 또는 Policies(정책) > Web Policy(웹 정책).

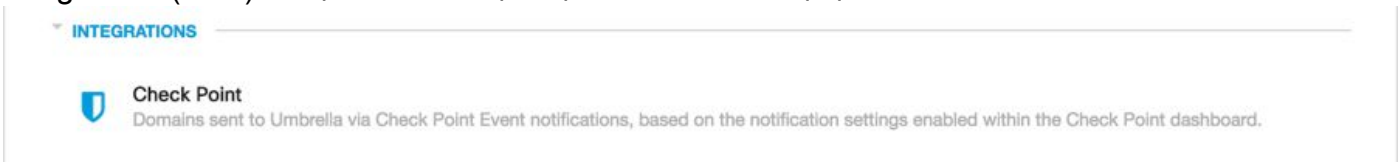
2. 정책을 확장하고 Security Setting Applied (DNS Policies)(보안 설정 적용됨(DNS 정책)) 또는 Security Settings (Web Policy)(보안 설정(웹 정책))에서 Edit(수정)를 선택합니다.

3. Security Settings(보안 설정) 드롭다운에서 Check Point(검사점) 설정이 포함된 보안 설정을 선택합니다.



19916943316884

Integrations(통합) 아래의 실드 아이콘이 파란색으로 업데이트됩니다.



115014149783

4. 설정 및 반환(DNS 정책) 또는 저장(웹 정책)을 선택합니다.

그러면 Check Point에 대한 보안 설정에 포함된 Check Point 도메인이 정책을 사용하여 이러한 ID에 대해 차단될 수 있습니다.

Umbrella에서 Check Point 이벤트에 대한 보고

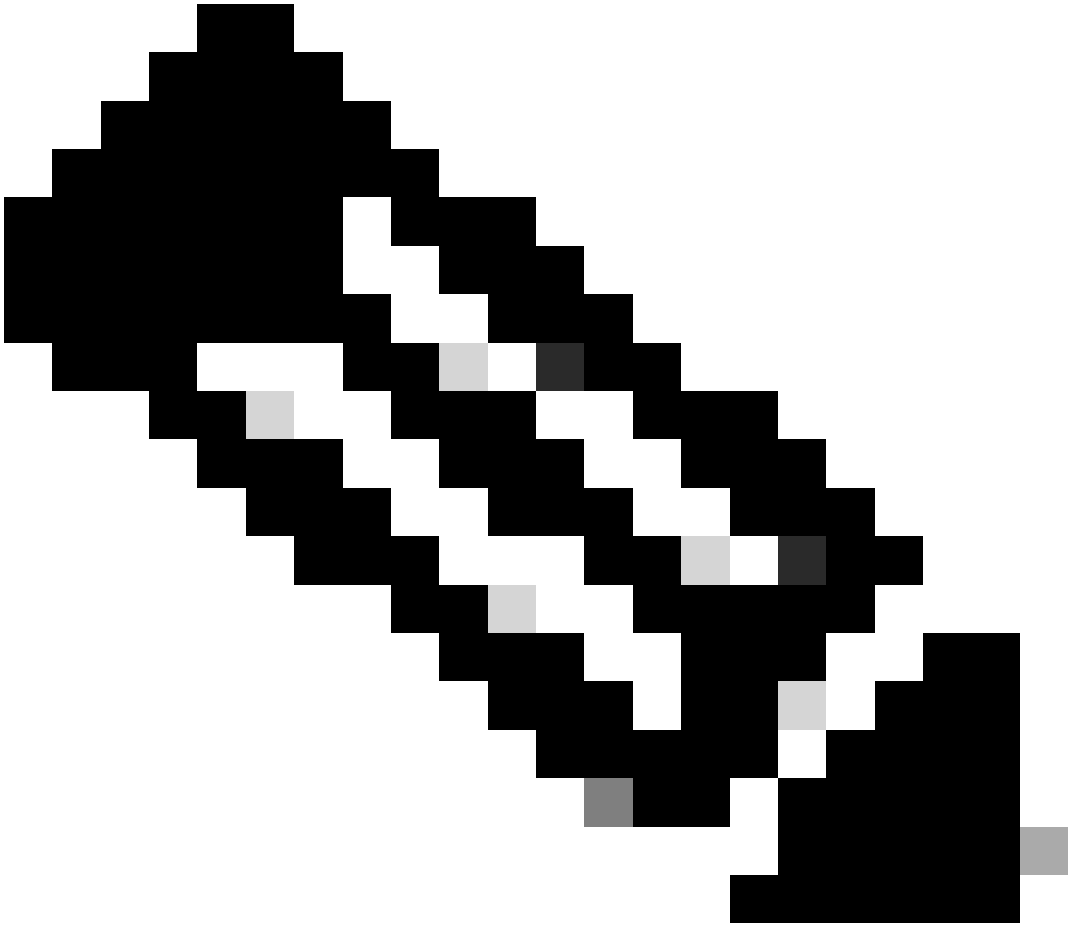
Check Point 보안 이벤트 보고

Check Point Destination List(검사점 대상 목록)는 보고서에 사용할 수 있는 보안 범주 중 하나입니다. 보고서의 대부분 또는 모두가 보안 카테고리를 필터로 사용합니다. 예를 들어, Check Point 관련 활동만 표시하도록 보안 카테고리를 필터링할 수 있습니다.

1. 보고 > 핵심 보고서 > 활동 검색으로 이동합니다.

2. Security Categories(보안 범주)에서 Check Point(검사점)를 선택하여 검사점에 대한 보안 범주만 표시하도록 보고서를 필터링합니다.

115014197623



참고: Check Point 통합이 비활성화된 경우 Security Categories(보안 카테고리) 필터에 표시되지 않습니다.

3. 적용을 선택하여 보고서에서 선택한 기간에 대한 체크포인트 관련 활동을 확인합니다.

도메인이 Check Point 대상 목록에 추가된 경우 보고

Cisco Umbrella Admin Audit(Cisco Umbrella 관리 감사) 로그는 목적지 목록에 도메인을 추가할 때 Check Point 어플라이언스의 이벤트를 포함합니다. 이러한 도메인은 감사 로그의 User 열에 있는 "Check Point account" 레이블에 의해 추가된 것으로 나타납니다.

Umbrella Admin Audit(Umbrella 관리자 감사) 로그를 찾으려면 Reporting(보고) > Admin Audit Log(관리자 감사 로그)로 이동합니다.

도메인이 추가된 시기를 보고하려면 Check Point Block List에 대해 Filter by Identities & Settings 필터를 적용하여 Check Point 변경 내용만 포함하도록 필터링합니다.

보고서를 실행하면 Check Point 대상 목록에 추가된 도메인 목록을 볼 수 있습니다.

원치 않는 탐지 또는 오탐 처리

원치 않는 탐지에 대한 허용 목록 관리

Check Point Appliance에 의해 자동으로 추가된 도메인이 원치 않는 차단을 트리거하여 사용자가 특정 웹 사이트에 액세스하지 못하도록 차단할 수 있습니다. 이와 같은 경우 Cisco Umbrella에서는 허용 목록에 도메인을 추가할 것을 권장합니다. 이는 보안 설정을 포함하여 다른 모든 유형의 차단 목록보다 우선합니다. 허용 목록은 둘 모두에 도메인이 있을 때 차단 목록보다 우선합니다.

이 접근 방식을 선호하는 이유는 두 가지입니다.

- 먼저, Check Point 어플라이언스가 제거된 후 도메인을 다시 추가해야 하는 경우 허용 목록은 추가 문제를 일으키지 않도록 보호합니다.
- 둘째, 허용 목록에는 이후 포렌식 또는 감사 보고서에 대해 문제가 있는 도메인의 기록 레코드가 표시됩니다.

기본적으로 모든 정책에 적용되는 전역 허용 목록이 있습니다. 전역 허용 목록에 도메인을 추가하면 모든 정책에서 도메인이 허용됩니다.

차단 모드의 Check Point 보안 설정이 관리되는 Cisco Umbrella ID의 하위 집합에만 적용되는 경우(예: 로밍 컴퓨터 및 모바일 디바이스에만 적용되는 경우) 이러한 ID 또는 정책에 대한 특정 허용 목록을 만들 수 있습니다.

허용 목록을 생성하려면

1. Policies(정책) > Destination Lists(대상 목록)로 이동하고 Add(추가) 아이콘을 선택합니다.

2. 허용을 선택하고 목록에 도메인을 추가합니다.

3. 저장을 선택합니다.

목록이 저장되면 원치 않는 블록의 영향을 받은 클라이언트를 다루는 기존 정책에 추가할 수 있습니다.

Check Point 대상 목록에서 도메인 삭제

Check Point 대상 목록의 각 도메인 이름 옆에는 Delete(삭제) 아이콘이 있습니다. 도메인을 삭제하면 원치 않는 탐지가 발생할 경우 Check Point 대상 목록을 정리할 수 있습니다.

그러나 Check Point 어플라이언스가 도메인을 Cisco Umbrella에 재전송하는 경우 삭제가 영구적이지 않습니다.

도메인을 삭제하려면

1. 설정 > 통합으로 이동한 다음 체크포인트를 선택하여 확장합니다.

2. 도메인 보기를 선택합니다.

3. 삭제할 도메인 이름을 검색합니다.

4. 삭제 아이콘을 선택합니다.

5. 마감을 선택합니다.

6. 저장을 선택합니다.

원치 않는 탐지 또는 오탐이 발생한 경우 Cisco Umbrella는 Cisco Umbrella에서 즉시 허용 목록을 생성한 다음 Check Point Appliance 내에서 오탐을 제거할 것을 권장합니다. 나중에 체크 포인트 대상 목록에서 도메인을 제거할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.