Cisco FireSIGHT 시스템의 보안 인텔리전스에 의해 IP 주소가 차단되거나 블랙리스트에 추가됨

목차

소개

보안 인텔리전스 기능을 사용하면 소스 또는 대상 IP 주소를 기반으로 네트워크를 통과할 수 있는 트래픽을 지정할 수 있습니다.이 기능은 특히 트래픽이 액세스 제어 규칙으로 분석되기 전에 특정 IP 주소로 드나드는 트래픽을 블랙리스트에 추가하려는 경우 유용합니다.이 문서에서는 Cisco FireSIGHT System에서 IP 주소를 차단하거나 블랙리스트에 추가할 때 시나리오를 처리하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 Cisco FireSIGHT Management Center에 대한 지식을 보유하고 있는 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco FireSIGHT Management Center
- Cisco Firepower 어플라이언스
- Cisco ASA with Firepower (SFR) 모듈
- 소프트웨어 버전 5.2 이상

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 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

인텔리전스 피드 및 인텔리전스 목록의 차이

FireSIGHT 시스템에서 보안 인텔리전스 기능을 사용하는 방법에는 두 가지가 있습니다.

보안 인텔리전스 피드

보안 인텔리전스 피드는 Defense Center가 HTTP 또는 HTTPS 서버에서 다운로드하는 IP 주소의 동적 컬렉션입니다.블랙리스트 구축을 돕기 위해 Cisco는 *보안 인텔리전스 피드를* 제공합니다. 이는 VRT(Vulnerability Research Team)에서 평판이 좋지 않은 IP 주소를 나타냅니다.

보안 인텔리전스 목록

피드와 달리 보안 인텔리전스 목록은 FireSIGHT Management Center에 수동으로 업로드하는 간단한 정적 IP 주소 목록입니다.

합법적인 IP 주소가 차단되거나 블랙리스트에 추가됨

IP 주소가 보안 인텔리전스 피드에 있는지 확인

보안 인텔리전스 피드 블랙리스트에 의해 IP 주소가 차단되는 경우 다음 단계에 따라 이를 확인할 수 있습니다.

1단계:Firepower 어플라이언스 또는 서비스 모듈의 CLI에 액세스합니다.

2단계:다음 명령을 실행합니다.<IP_Address>를 검색할 IP 주소로 바꿉니다.

```
admin@Firepower:~$ grep
```

예를 들어 IP 주소 198.51.100.1을 검색하려면 다음 명령을 실행합니다.

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

이 명령은 제공한 IP 주소에 대한 일치 항목을 반환하면 IP 주소가 보안 인텔리전스 피드 블랙리스트에 있음을 나타냅니다.

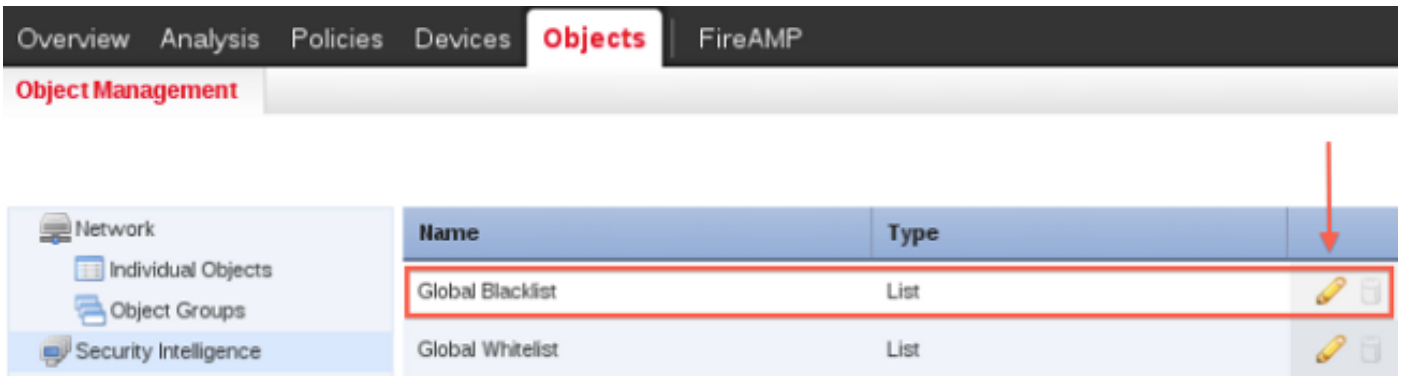
블랙리스트 확인

블랙리스트에 포함될 수 있는 IP 주소의 목록을 찾으려면 다음 단계를 수행하십시오.

1단계:FireSIGHT Management Center의 웹 인터페이스에 액세스합니다.

2단계:Objects > **Object Management > Security Intelligence로 이동합니다**.

3단계: *연필* 아이콘을 클릭하여 **전역 블랙리스트**를 열거나 **편집합니다**.IP 주소 목록이 있는 팝업 창이 나타납니다.



차단 또는 블랙리스트 IP 주소 작업

보안 인텔리전스 피드에 의해 특정 IP 주소가 차단되거나 블랙리스트에 추가된 경우 다음 옵션 중 하나를 선택하여 허용할 수 있습니다.

옵션 1:보안 인텔리전스 화이트리스트

보안 인텔리전스에 의해 블랙리스트에 추가된 IP 주소를 화이트리스트에 추가할 수 있습니다.화이트리스트는 블랙리스트를 재정의합니다.FireSIGHT 시스템은 IP 주소도 블랙리스트에 추가된 경우에도 액세스 제어 규칙을 사용하여 화이트리스트에 있는 소스 또는 대상 IP 주소로 트래픽을 평가합니다.따라서 블랙리스트가 여전히 유용하지만 범위가 너무 넓고 검사하려는 트래픽을 잘못 차단하는 경우 화이트리스트를 사용할 수 있습니다.

예를 들어, 평판이 좋은 피드가 중요한 리소스에 대한 액세스를 부적절하게 차단하지만 조직에 전반적으로 유용한 경우, 블랙리스트에서 전체 피드를 제거하는 대신 부적절하게 분류된 IP 주소만 화이트리스트할 수 있습니다.

주의:액세스 제어 정책을 변경한 후 관리되는 디바이스에 정책을 다시 적용해야 합니다.

옵션 2:보안 영역별 보안 인텔리전스 필터 적용

세분화를 위해 연결의 소스 또는 대상 IP 주소가 특정 보안 영역에 있는지 여부에 따라 보안 인텔리전스 필터링을 적용할 수 있습니다.

위의 화이트리스트 예를 확장하려면 잘못 분류된 IP 주소를 화이트리스트에 추가한 다음 해당 IP 주소에 액세스해야 하는 조직의 보안 영역에서 사용하는 화이트리스트 객체를 제한할 수 있습니다.이렇게 하면 비즈니스 요구 사항이 있는 사용자만 화이트리스트에 있는 IP 주소에 액세스할 수 있습니다.또 다른 예로, 서드파티 스팸 피드를 사용하여 이메일 서버 보안 영역에서 트래픽을 블랙리스트에 추가할 수 있습니다.

옵션 3:차단 목록 대신 모니터

특정 IP 주소 또는 주소 집합을 블랙리스트에 추가할지 확실하지 않은 경우, "monitor-only" 설정을 사용할 수 있습니다. 이 설정을 사용하면 시스템은 일치하는 연결을 액세스 제어 규칙에 전달하되,

매칭도 블랙리스트에 로깅할 수 있습니다.전역 블랙리스트는 모니터링 전용으로 설정할 수 없습니다

해당 피드를 사용하여 차단을 구현하기 전에 서드파티 피드를 테스트하려는 시나리오를 고려해 보십시오.피드를 모니터링 전용으로 설정하면 시스템에서 차단한 연결을 추가로 분석하도록 허용하지만 평가를 위해 각 연결의 레코드도 로깅합니다.

"모니터링 전용" 설정으로 보안 인텔리전스를 구성하는 단계:

1. 액세스 제어 정책의 **Security Intelligence** 탭에서 로깅 아이콘을 클릭합니다.Blacklist Options 대화 상자가 나타납니다.
2. 트래픽이 보안 인텔리전스 조건을 충족할 때 연결 시작 이벤트를 로깅하려면 **Log Connections** 확인란을 선택합니다.
3. 연결 이벤트를 보낼 위치를 지정합니다.
4. OK(**확인**)를 클릭하여 로깅 옵션을 설정합니다.Security Intelligence 탭이 다시 나타납니다.
5. 저장을 **클릭합니다**.변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다.

옵션 4:Cisco 기술 지원 센터에 문의

다음과 같은 경우 언제든지 Cisco Technical Assistance Center에 문의할 수 있습니다.

- 위 옵션 1, 2 또는 3과 관련된 질문이 있습니다.
- 보안 인텔리전스에 의해 블랙리스트에 추가된 IP 주소에 대한 추가 연구 및 분석을 원하게 됩니다.
- 보안 인텔리전스에 의해 IP 주소가 블랙리스트에 추가되는 이유에 대해 설명하고자 합니다.