ASDM을 통해 Cisco Security Intelligence를 사용하는 동안 IP 블랙리스트 구성(온박스 관리)

목차

소개

이 문서에서는 Cisco Security Intelligence/IP 주소 평판 및 IP 블랙리스트(차단)의 컨피그레이션(Blocking)과 낮은 IP 주소의 사용자 지정/자동 피드에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA(Adaptive Security Appliance) 방화벽, ASDM(Adaptive Security Device Manager) 지식
- FirePOWER 어플라이언스 지식

  : .

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 5.4.1 이상을 실행하는 ASA FirePOWER 모듈(ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)
- 소프트웨어 버전 6.0.0 이상을 실행하는 ASA FirePOWER 모듈(ASA 5515-X, ASA 5525-X,

ASA 5545-X, ASA 555-X)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco Security Intelligence는 Cisco TALOS 팀에서 평판이 좋지 않은 것으로 확인된 여러 개의 정기적으로 업데이트되는 IP 주소 모음으로 구성됩니다.Cisco TALOS 팀은 스팸, 악성코드, 피싱 공격과 같은 IP 주소에서 악의적인 활동이 발생하는지 여부에 대해 낮은 평판을 결정합니다.

Cisco IP Security Intelligence 피드는 공격자, Bogon, Bots, CnC, Dga, ExploitKit, Malware, Open_proxy, Open_relay, Phishing, Response, Spam, Suspicious의 데이터베이스를 추적합니다.Firepower 모듈에서는 낮은 IP 주소의 사용자 지정 피드를 생성하는 옵션을 제공합니다.

보안 인텔리전스 피드 개요

보안 인텔리전스에서 다른 범주로 분류될 수 있는 IP 주소 수집 유형에 대한 자세한 내용은 다음과 같습니다.

공격자:취약성을 지속적으로 검사하거나 다른 시스템을 악용하려는 IP 주소 수집

악성코드:악성코드를 전파하려고 하거나 방문하는 모든 사람을 능동적으로 공격하는 IP 주소 수집

피싱:최종 사용자에게 사용자 이름 및 비밀번호와 같은 기밀 정보를 입력하도록 능동적으로 유도하려는 호스트의 모음입니다.

스팸:스팸 이메일 메시지 전송 소스로 식별된 호스트의 모음입니다.

봇은 다음과 같습니다.봇넷의 일부로서 활발히 사용되고 알려진 봇넷 컨트롤러에 의해 제어되고 있는 호스트의 모음입니다.

CNc:알려진 Botnet의 제어 서버로 식별된 호스트의 모음입니다.

프록시 열기: Open Web Proxies를 실행하고 익명 웹 브라우징 서비스를 제공하는 것으로 알려진 호스트의 모음입니다.

오픈 릴레이:스팸 및 피싱 공격자가 사용하는 익명 이메일 릴레이 서비스를 제공하는 것으로 알려진 호스트 모음입니다.

토르 종료 노드:토르 익명 장치 네트워크에 대한 종료 노드 서비스를 제공하는 것으로 알려진 호스트의 컬렉션입니다.

보곤:할당되지 않았지만 트래픽을 전송하는 IP 주소의 모음입니다.

의심스러움:의심스러운 활동을 표시하고 현재 조사 중인 IP 주소 수집

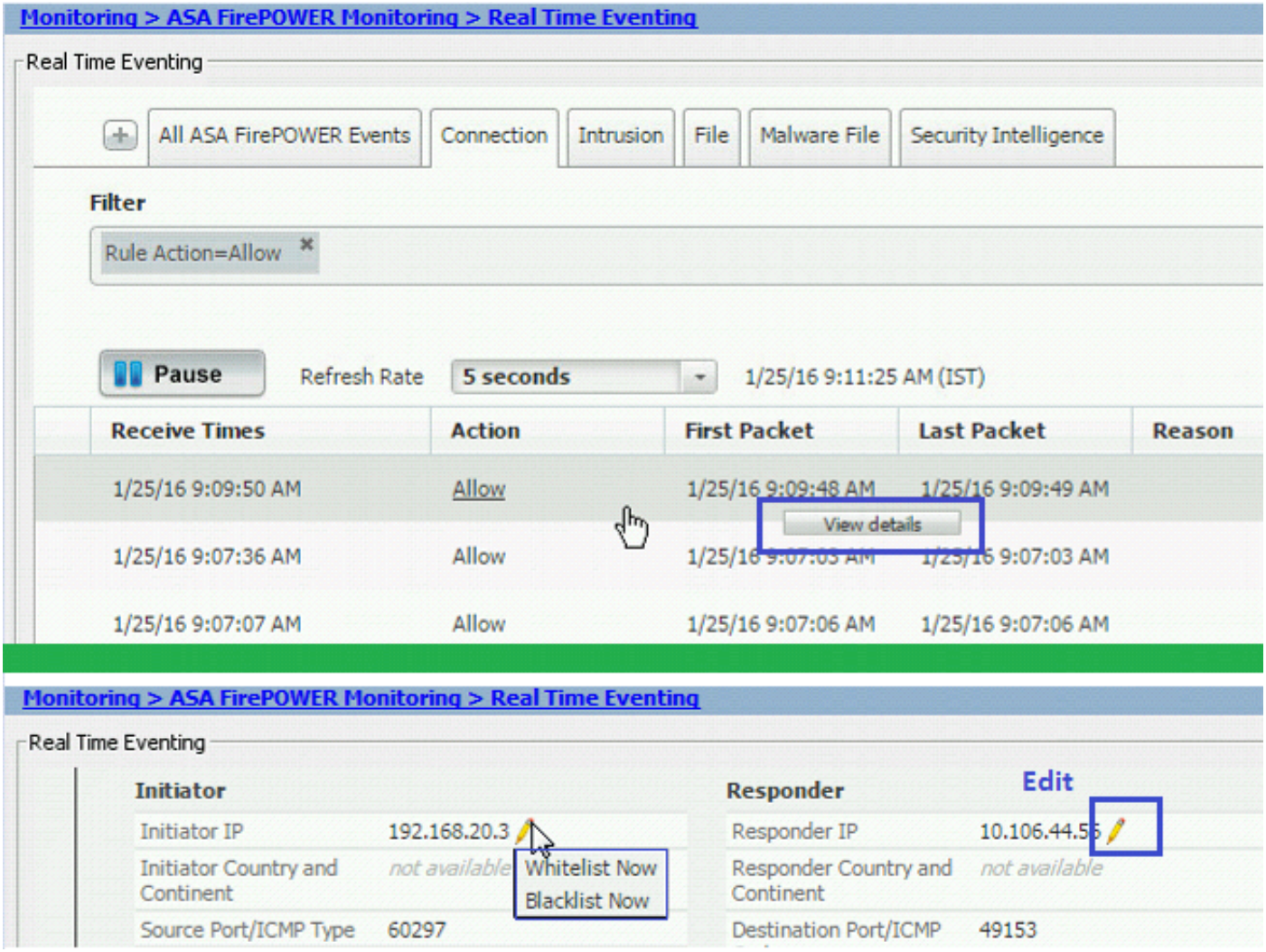
응답:의심스럽거나 악의적인 동작과 관련하여 반복적으로 관찰된 IP 주소 모음입니다.

Global-Blacklist 및 Global-Whitelist에 IP 주소 수동 추가

Firepower 모듈을 사용하면 특정 IP 주소가 일부 악의적인 활동의 일부임을 알고 있는 경우 Global-Blacklist에 추가할 수 있습니다.블랙리스트 IP 주소에 의해 차단된 특정 IP 주소에 대한 트래픽을 허용하려면 IP 주소를 Global-Whitelist에 추가할 수도 있습니다.Global-Blacklist/Global-Whitelist에 IP 주소를 추가하면 정책을 적용할 필요 없이 즉시 적용됩니다.

IP 주소를 Global-Blacklist/Global-Whitelist에 추가하려면 Monitoring(모니터링) **> ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Real Time Eventing(실시간 이벤트)으로 이동하고** 연결 이벤트에 마우스를 올려 놓고 View Details(세부 정보 보기)를 선택합니다.

소스 또는 대상 IP 주소를 Global-Blacklist/ Global-Whitelist에 추가할 수 있습니다.Edit(**수정)** 버튼**을** 클릭하고 **Whitelist Now/Blacklist Now(지금 화이트리스트/블랙리스트)**를 선택하여 이미지에 표시된 대로 해당 목록에 IP 주소를 추가합니다.



소스 또는 대상 IP 주소가 Global-Blacklist/ Global-Whitelist에 추가되었는지 확인하려면 Configuration(구성) **> ASA Firepower Configuration(ASA Firepower 구성) > Object Management(개체 관리) > Security Intelligence(보안 인텔리전스) > Network Lists and Feeds(네트워크 목록 및 피드)로 이동하고 Global-Blacklist/ Global Whitelist(전역 화이트리스트)를 편집하고 편집합니다**.목록에서 IP 주소를 제거하려면 삭제 버튼을 사용할 수도 있습니다.

블랙리스트 IP 주소의 사용자 지정 목록 생성

Firepower를 사용하면 블랙리스트(차단)에 사용할 수 있는 맞춤형 네트워크/IP 주소 목록을 생성할

수 있습니다. 다음과 같은 세 가지 옵션이 있습니다.

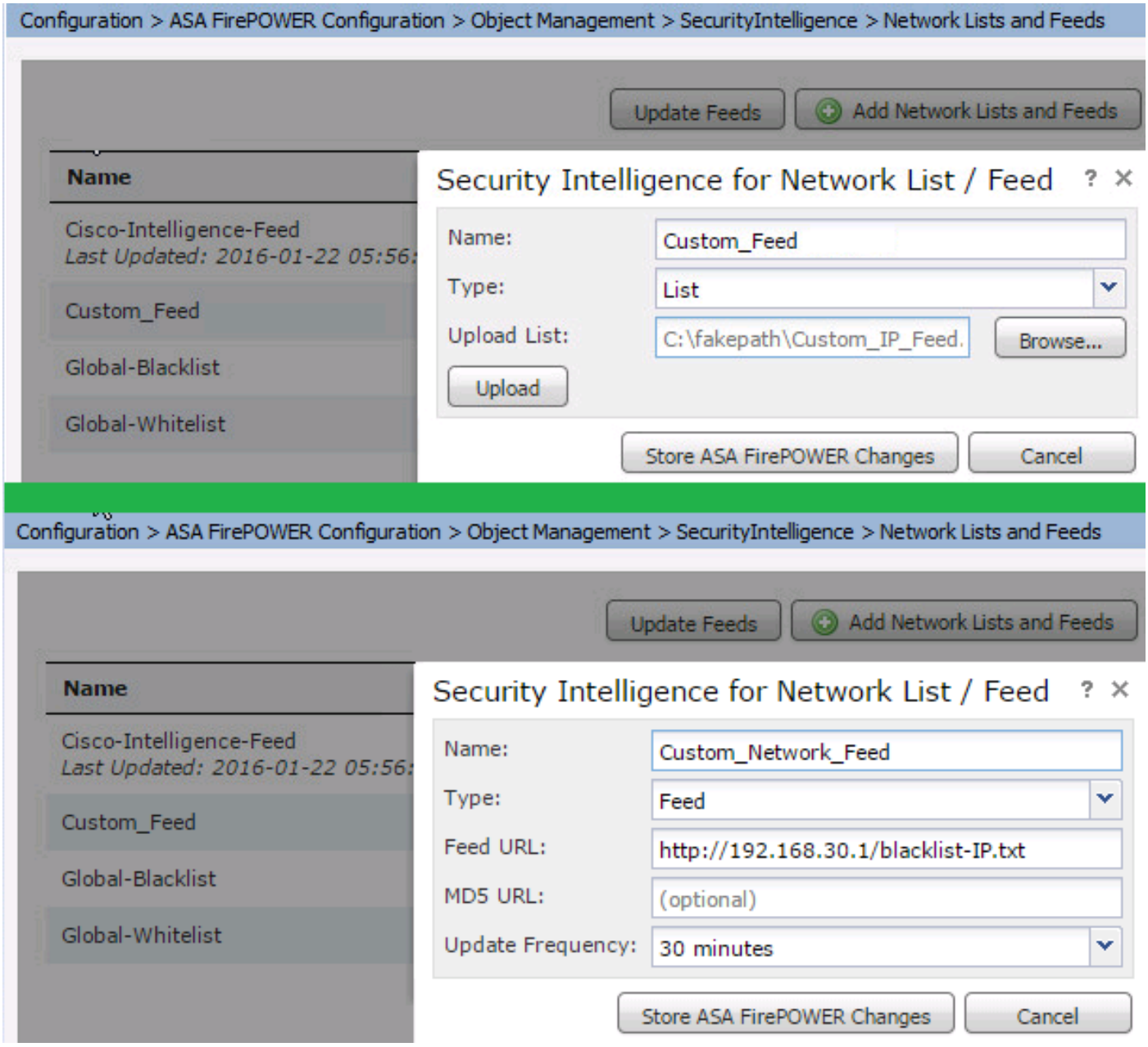
1. IP 주소를 텍스트 파일(한 줄에 하나씩 IP 주소)에 쓰고 파일을 Firepower Module에 업로드할 수 있습니다.파일을 업로드하려면 Configuration(구성) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Object Management(개체 관리) > Security Intelligence(보안 인텔리전스) > Network Lists and Feeds(네트워크 목록 및 피드 추가)로** 이동한 다음 **Add Network Lists and Feeds(네트워크 목록 및 피드 추가)를** 클릭합니다. 이름: 사용자 지정 목록의 이름을 지정합니다. 유형: 드롭다운 목록에서 List를 선택합니다. **업로드 목록:** Browse(**찾아보기**)를 선택하여 시스템에서 텍스트 파일을 찾습니다.파일을 업로드하려면 **업로드** 옵션을 선택합니다.
2. Firepower 모듈이 타사 서버에 연결하여 IP 주소 목록을 가져오는 사용자 지정 목록에 대해 서드파티 IP 데이터베이스를 사용할 수 있습니다.이 구성 하려면 Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) **> Object Management(개체 관리) > Security Intelligence(보안 인텔리전스) > Network Lists and Feeds(네트워크 목록 및 피드 추가)로 이동한** 다음 **Add Network Lists and Feeds(네트워크 목록 및 피드 추가)를** 클릭합니다.
   이름:사용자 지정 피드의 이름을 지정합니다.

   유형:드롭다운 목록에서 옵션 Feed를 선택합니다.

   피드 URL: Firepower 모듈이 연결하고 피드를 다운로드할 서버의 URL을 지정합니다.

   MD5 URL:피드 URL 경로를 검증할 해시 값을 지정합니다.

   업데이트 빈도:시스템이 URL 피드 서버에 연결하는 시간 간격을 지정합니다.



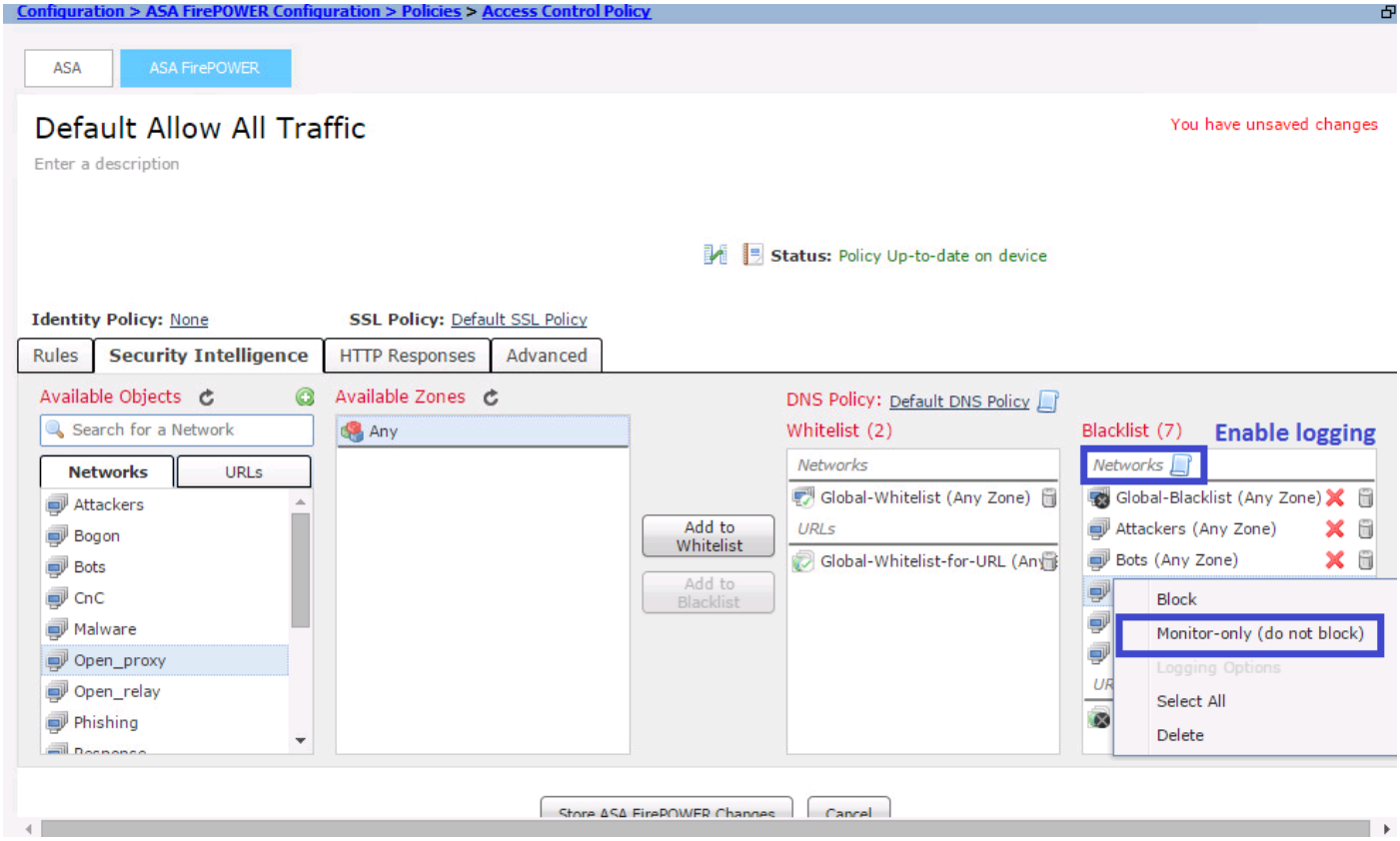
보안 인텔리전스 구성

Security Intelligence(보안 인텔리전스)를 구성하려면 Configuration(컨피그레이션) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Access Control Policy(액세스 제어 정책)로 이동하여 Security Intelligence(보안 인텔리전스)** 탭을 선택합니다.

Network Available Object(네트워크 사용 가능한 개체)에서 피드를 선택하고 Whitelist **/ Blacklist(화이트리스트/블랙리스트)** 열로 이동하여 악성 IP 주소에 대한 연결을 허용/차단합니다.

아이콘을 클릭하고 이미지에 지정된 대로 로깅을 활성화할 수 있습니다.

연결을 차단하는 대신 악의적인 IP 연결에 대한 이벤트를 생성하려는 경우 피드를 마우스 오른쪽 버튼으로 클릭하고 이미지에 표시된 대로 **Monitor-only(Monitor-only(Monitor-only)(차단 안 함)**를 선택합니다.

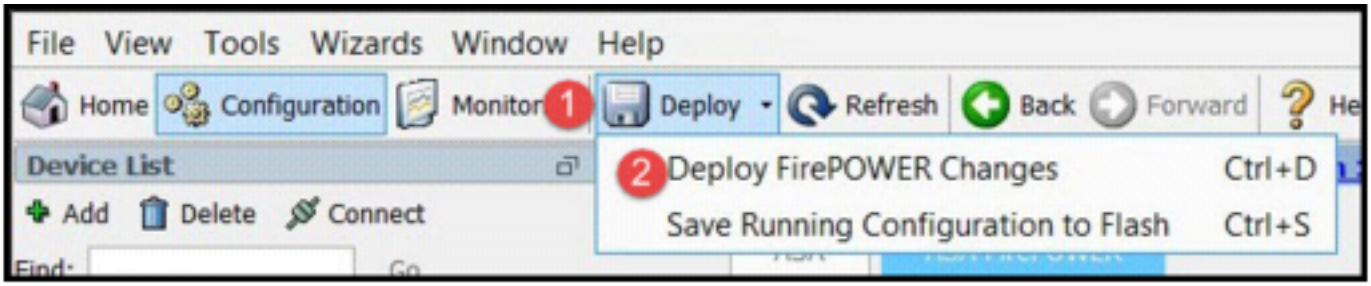


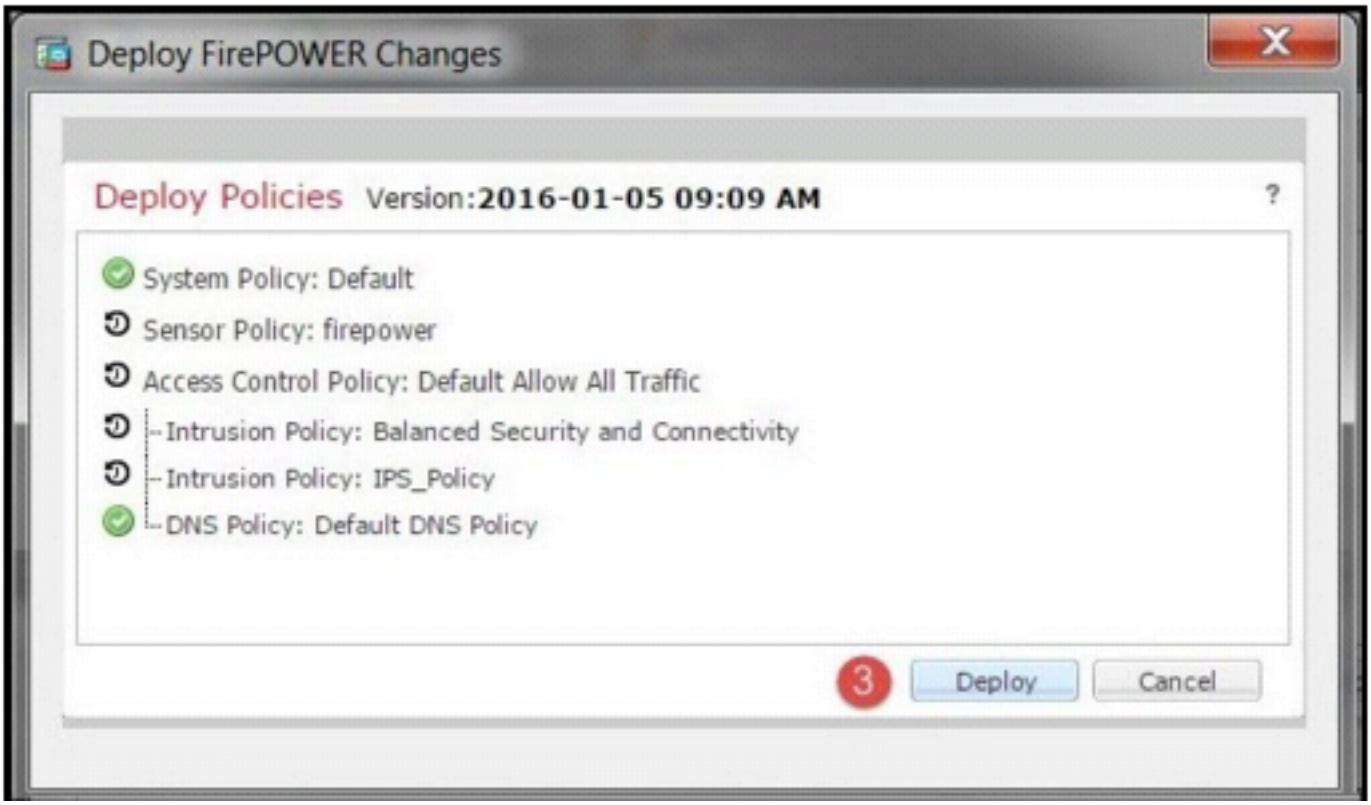
Store ASA Firepower Changes(ASA Firepower 변경 사항 저장) 옵션을 선택하여 AC 정책 변경 사항을 저장합니다.

액세스 제어 정책 구축

변경 사항을 적용하려면 액세스 제어 정책을 구축해야 합니다.정책을 적용하기 전에 액세스 제어 정책이 디바이스에서 최신 상태가 아닌지 여부를 나타내는 표시를 참조하십시오.

센서에 변경 사항을 배포하려면 cDeploy(**구축**)를 클릭하고 **Deploy FirePOWER Changes(FirePOWER 변경 사항 구축)를** 선택한 다음 팝업 창에서 Deploy(구축)를 선택하여 변경 사항을 구축합니다.



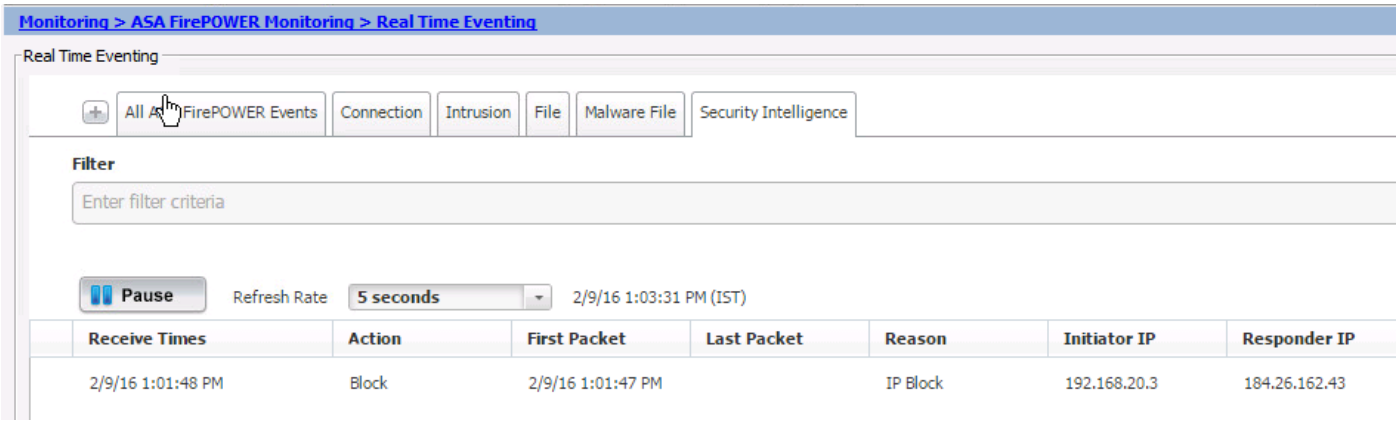


: 5.4.x Apply ASA FirePOWER Changes(**ASA FirePOWER)** .

: Monitoring() **> ASA Firepower Monitoring(ASA Firepower) > Task Status( ) .** .

보안 인텔리전스의 이벤트 모니터링

Firepower Module에서 보안 인텔리전스를 보려면 Monitoring(모니터링) **> ASA Firepower Monitoring(ASA Firepower 모니터링) > Real Time Eventing(실시간 이벤트)으로 이동합니다** .**Security Intelligence** 탭을 선택합니다.그러면 이미지에 표시된 대로 이벤트가 표시됩니다.

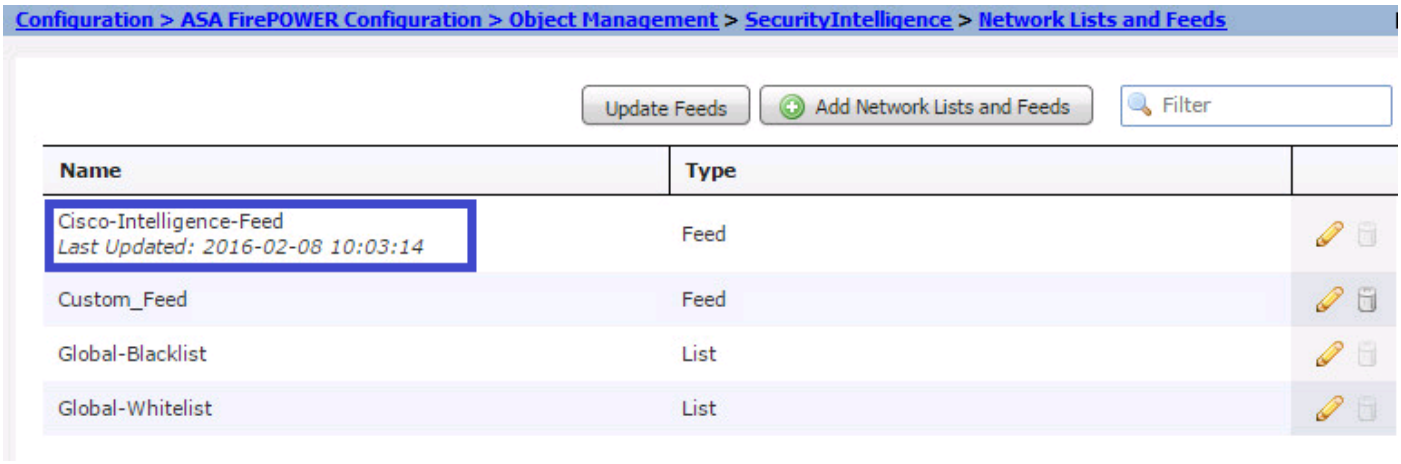


다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

보안 인텔리전스 피드가 최신 상태인지 확인하려면 Configuration(구성) > **ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리) > Security Intelligence(보안 인텔리전스) > Network Lists and Feeds(네트워크 목록 및 피드)로 이동하여** 피드가 마지막으로 업데이트된 시간을 확인합니다.편집 버튼을 선택하여 피드 업데이트 빈도를 설정할 수 있습니다.



액세스 제어 정책 배포가 성공적으로 완료되었는지 확인합니다.

보안 인텔리전스를 모니터링하여 트래픽이 차단되는지 확인합니다.

- Cisco ASA FirePOWER
- – Cisco Systems