FireSIGHT 시스템에 설치할 수 있는 업데이트 파일 유형

목차

소개

이 문서에서는 시스템을 최신 상태로 유지하기 위해 FireSIGHT System에서 설치하는 다양한 유형의 업데이트 파일에 대해 간략하게 설명합니다.일부 파일은 FireSIGHT System의 소프트웨어 및 운영 체제를 업데이트하지만, 일부 파일은 보안을 강화합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Sourcefire FirePOWER 7000 Series 어플라이언스, 8000 Series 어플라이언스 및 NGIPS 가상 어플라이언스
- Sourcefire 소프트웨어 버전 5.0 이상

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.

업데이트 유형

FireSIGHT Systems에서 다음과 같은 유형의 업데이트를 설치할 수 있습니다.

	설명	예
업그레이드	• 새로운 기능 및 구성 요소를 소개합니다. • 버그 픽스를 포함합니다. • 알려진 문제를 해결합니다.	`Sourcefire_3D_Defense_Center_S3_`**`Upgrade`**`-5.4.0-763.sh`
패치	• 이전 핫픽스에 제공된 해상도를 포함합니다. • 소프트웨어 버전 5.0 이상에 설치할 수 있습니다.	`Sourcefire_3D_Defense_Center_S3_`**`Patch`**`-5.4.1-59.sh`
SRU(Sourcefire Rule Update)	• Snort 규칙 및 공유 객체 규칙을 업데이트합니다.	`Sourcefire_Rule_Update-2015-05-20-001-vrt.sh`
취약성 데이터베이스(VDB)	• 애플리케이션 및 운영 체제에 대한 핑거프린트, 탐지기 및 취약성 정보를 업데이트합니다.	`Sourcefire_`**`VDB`**`_Fingerprint_Database-4.5.0-241.sh`
SourceFire GeoLocation 데이터베이스 업데이트(GeoDB)	• 라우팅 가능한 IP 주소와 관련된 지리적 데이터를 업데이트합니다.	`Sourcefire_`**`Geodb`**`_Update-2015-05-09-001.sh`
보안 인텔리전스 피드	• IP 주소를 블랙리스트에 추가하는	피드는 FireSIGHT Management Center에서 정기적으로 클라우드에서 자동으로 다운로드됩니다.

URL 필터링 데이터	데 사용되는 IP 주소 목록을 업데이트합니다. • 액세스 제어 규칙에서 URL 필터링에 사용되는 데이터를 업데이트합니다.	피드는 FireSIGHT Management Center에서 정기적으로 클라우드에서 자동으로 다운로드됩니다.

웹 인터페이스의 업데이트 페이지

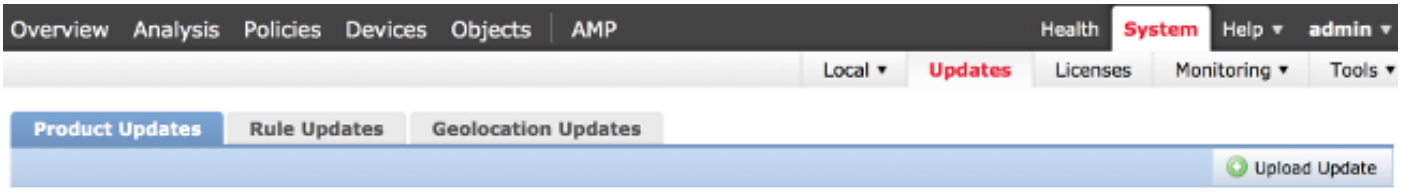
FireSIGHT Management Center를 업데이트하려면 웹 인터페이스의 다양한 페이지로 이동해야 할 수 있습니다.다운로드할 업데이트 유형에 따라 다릅니다.이 섹션에서는 다양한 업데이트 페이지로 이동하는 방법을 설명합니다.

제품 업데이트

이러한 구성 요소를 업로드하거나 설치하려면 **시스템 > 업데이트**를 선택하고 **제품 업데이트** 탭을 선택합니다.

- 업그레이드
- 패치
- VDB

Cisco 지원 사이트에서 업그레이드, 패치 또는 VDB 파일을 직접 다운로드하려면 Download Updates(**업데이트 다운로드)를** 클릭합니다.이 버튼은 페이지 하단에 있습니다.또는 Cisco 지원 사이트에서 파일을 수동으로 다운로드한 후 FireSIGHT 시스템에 업로드하려면 Upload **Update**를 클릭합니다.



규칙 업데이트

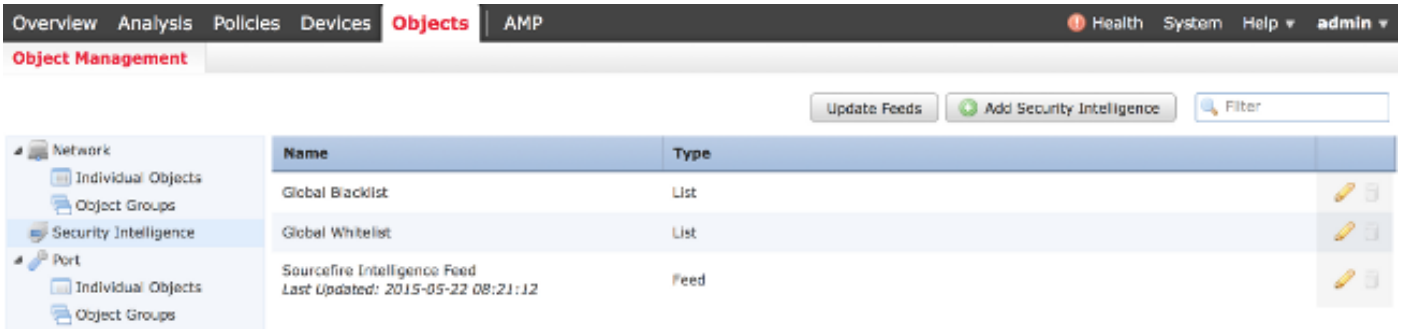
SRU를 업데이트하려면 **System > Updates**를 선택하고 **Rule Updates** 탭을 선택합니다.

GeoDB 업데이트

GeoDB를 업데이트하려면 **System > Updates**를 선택하고 Geolocation Updates 탭을 선택합니다.

보안 인텔리전스 업데이트

보안 인텔리전스 피드를 업데이트하려면 Objects(개체) **> Object Management(개체 관리)를** 선택합니다.왼쪽 패널에서 **Security Intelligence(보안 인텔리전스)** 옵션을 선택하고 Update Feeds(피드 **업데이트)**를 클릭합니다.사용자 지정 피드를 업데이트하거나 사용자 지정 목록을 만들려면 **Add Security Intelligence(보안 인텔리전스 추가)를** 클릭합니다.



URL 필터링 업데이트

URL 필터링 데이터베이스를 업데이트하려면 **System > Local > Configuration을** 선택합니다.Cloud **Services(클라우드 서비스)를** 선택하고 **Update Now(지금 업데이트)**를 클릭합니다.