업데이트

다음 항목에서는 Firepower 구축을 업데이트 하는 방법을 설명합니다.

시스템 업데이트 정보

management center를 사용하여 자체 및 관리하는 디바이스의 시스템 소프트웨어를 업그레이드할 수 있습니다. 또한 고급 서비스를 제공하는 다양한 데이터베이스 및 피드를 업데이트할 수 있습니다.

인터넷에 액세스할 수 있는 management center의 경우, 시스템은 종종 Cisco에서 직접 업데이트를 가져올 수 있습니다. 가능한 경우 자동 업데이트를 예약하거나 활성화하는 것이 좋습니다. 일부 업데이트는 초기 설정 프로세스에서 또는 관련 기능을 활성화할 때 자동으로 활성화됩니다. 기타 업데이트는 직접 예약해야 합니다. 초기 설정 후 모든 자동 업데이트를 검토하고 필요한 경우 조정하는 것이 좋습니다.

표 *1:* 업그레이드 및 업데이트

구성 요소	설명	세부정보
시스템 소프트웨어	주요 소프트웨어 릴리스에는 새로운 기능과 향상된 기능이 포함되어 있습니다. 여기에는 인프라 또는 아키텍처 변경 사항이 포함될 수 있습니다. 유지 보수 릴리스에는 일반적인 버그 및 보안 관련 수정 사항이 포함되어 있습니다. 동작 변경은 거의 포함되지 않으며, 동작 변경이 포함되는 경우 이러한 수정과 관련이 있습니다. 패치는 온디맨드 업데이트로, 시급한 중요 수정 사항만을 제공합니다. 핫픽스는 특정 고객 문제를 해결할 수 있습니다.	직접 다운로드: 일부 릴리스만 해당 릴리스를 수동으로 다운로드할 수 있습니다. 지연되는 기간은 릴리스 유형, 릴리스 채택 및 기타 요인에 따라 달라집니다. 예약: 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**의 패치만 해당됩니다. 제거: 패치만 해당됩니다. 되돌리기/이미지 재설치: 주요 릴리스 및 유지 보수 릴리스에만 해당됩니다. 참조: 시스템 소프트웨어 업그레이드, 4 페이지
VDB(Vulnerability Database)	Cisco VDB(취약성 데이터베이스)는 호스트가 영향을 받기 쉬운 알려진 취약성의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. 시스템이 VDB를 사용하여 특정 호스트가 침해 위험을 높이는지 여부를 결정합니다.	직접 다운로드**:** 예. 예약**:** 예, 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**. 제거**:** 아니요. 참조**:** 취약성 데이터베이스(VDB) 업데이트, 4 페이지
GeoDB(Geolocation database)	Cisco 지리위치 데이터베이스(GeoDB)는 라우팅 가능한 IP 주소와 관련된 지리적 및 연결 관련 데이터의 데이터베이스입니다.	직접 다운로드**:** 예. 예약**:** 예, 시스템 (⚙) > **Updates(**업데이트**)**. 제거**:** 아니요. 참조**:** 지리위치 데이터베이스 업데이트, 6 페이지
침입 규칙(SRU/LSP)	침입 규칙은 업데이트된 새로운 침입 규칙과 전처리기 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 규칙 업데이트는 또한 규칙을 삭제하고, 새로운 규칙 카테고리와 기본 변수를 제공하며, 기본 변수 값을 변경할 수 있습니다.	직접 다운로드**:** 예. 예약**:** 예, 시스템 (⚙) > **Updates(**업데이트**)**. 제거**:** 아니요. 참조**:** 침입 규칙 업데이트, 8 페이지

구성 요소	설명	세부정보
보안 인텔리전스 피드	보안 인텔리전스 피드는 항목과 일치하는 트래픽을 빠르게 필터링하는 데 사용할 수 있는 IP 주소, 도메인 이름 및 URL의 모음입니다.	직접 다운로드: 예. 예약: 예, **Objects(개체)** > **Object Management(개체 관리)**. 제거: 아니요. 참조: Cisco Secure Firewall Management Center 디바이스 구성 가이드
URL 범주 및 평판	URL 필터링을 사용하면 URL의 일반 분류(범주) 및 위험 수준(평판)을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.	직접 다운로드: 예. 예약: 예, 요구 사항에 따라 **Integration(통합)** > **Other Integrations(기타 통합)**> **Cloud Services(클라우드 서비스)** 또는 시스템 (⚙) > **Tools(툴)** > **Scheduling(예약)**를 선택합니다. 제거: 아니요. 참조: Cisco Secure Firewall Management Center 디바이스 구성 가이드

시스템 업데이트 요구 사항 및 사전 요건

모델 지원

Any(모든)

지원되는 도메인

글로벌 달리 명시되지 않은 경우

사용자 역할

관리자

시스템 업데이트에 대한 가이드라인 및 제한 사항

업데이트 하기 전에

구축 구성 요소(침입 규칙, VDB 또는 GeoDB 포함)를 업데이트하기 전에 업데이트와 함께 제공되는 릴리스 정보 또는 권고 텍스트를 읽어 보십시오. 호환성, 사전 요구 사항, 새로운 기능, 동작 변경, 경고 등 중요 및 릴리스 별 정보를 제공합니다.

예약된 업데이트

시스템은 UTC 기준으로 작업을 예약합니다(업데이트 포함). 즉, 로컬에서 발생하는 시간은 날짜와 사용자의 특정 위치에 따라 달라집니다. 또한 업데이트는 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받는다면, 예약된 업데이트는 현지 시간에 따라 여름에는 겨울보다 1시간 '후'에 실행됩니다

중요 예약된 업데이트가 의도한 시점에 수행되는지 확인하기를 적극 권장합니다.

대역폭 지침

시스템 소프트웨어를 업그레이드하거나 준비도 확인을 실행하려면 업그레이드 패키지가 어플라이언스에 있어야 합니다. 업그레이드 패키지 크기는 다양합니다. 관리되는 디바이스로 대량 데이터 전송을 수행할 수 있는 대역폭을 사용하고 있는지 확인합니다. Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)

시스템 소프트웨어 업그레이드

이 설명서에는 시스템 소프트웨어 또는 함께 제공되는 운영 체제에 대한 자세한 업그레이드 지침이 포함되어 있지 않습니다. 대신 버전에 맞는 Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드를 참조하십시오.

일부 업데이트의 다운로드 및 설치 예약에 대한 자세한 내용은 소프트웨어 업데이트 자동화 섹션을 참조하십시오. 초기 설정 프로세스에서는 자동으로 매주 다운로드를 예약합니다. 설정 후 자동 예약 구성을 검토하고 필요한 경우 조정해야 합니다.

취약성 데이터베이스(VDB) 업데이트

Cisco VDB(취약성 데이터베이스)는 호스트가 영향을 받기 쉬운 알려진 취약성의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. 시스템이 VDB를 사용하여 특정 호스트가 침해 위험을 높이는지 여부를 결정합니다.

Cisco는 VDB에 주기적인 업데이트를 제공합니다. management center에서 VDB 및 관련 매핑 업데이트에 걸리는 시간은 네트워크 맵에 있는 호스트 수에 따라 달라집니다. 호스트 수를 1000으로 나누면 업데이트 수행에 걸리는 대략적인 시간(분)이 나옵니다.

VDB 343부터는 Cisco Secure Firewall 애플리케이션 탐지기를 통해 모든 애플리케이션 탐지기 정보를 사용할 수 있습니다. 이 사이트에는 검색 가능한 애플리케이션 탐지기 데이터베이스가 포함되어 있습니다. 릴리스 노트에서는 특정 VDB 릴리스의 변경 사항에 대한 정보를 제공합니다.

참고 management center의 초기 설정에서는 일회성 작업으로 Cisco에서 최신 VDB를 자동으로 다운로드하여 설치합니다. 선택적으로, VDB 업데이트를 다운로드 및 설치하고 구성을 구축하는 작업을 예약합니다. 자세한 내용은 취약성 데이터베이스 업데이트 자동화를 참조하십시오.

VDB 수동 업데이트

이 절차를 사용하여 VDB를 수동으로 업데이트합니다.

주의 VDB가 업데이트되는 동안에는 매핑된 취약성과 관련된 작업을 수행하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

대부분의 경우 VDB 업데이트 후 첫 번째 구축은 Snort 프로세스를 재시작하여 트래픽 검사를 중단합니다. 이러한 상황이 발생하면 시스템에서 사용자에게 경고합니다(업데이트된 애플리케이션 탐지기 및 운영 체제 핑거프린트는 재시작이 필요하지만 취약성 정보는 그렇지 않음). 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작를 참조하십시오.

시작하기 전에

VDB를 management center에 수동으로 업로드하려는 경우 https://www.cisco.com/go/firepower-software에서 다운로드합니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)**를 선택한 후, **Product Updates(**제품 업데이트**)**를 클릭합니다.

단계 **2** management center에 VDB를 가져옵니다. 다음 중 하나를 수행할 수 있습니다.

- Cisco에서 직접 다운로드: 최신 VDB, 최신 유지 보수 릴리스 및 구축을 위한 최신 중요 패치를 즉시 다운로드하려면 **Download Updates(**업데이트 다운로드**)** 버튼을 클릭합니다.
- 수동 업로드: **Upload Update(**업데이트 업로드**)**를 클릭한 후, **Choose File(**파일 선택**)**을 클릭합니다. 업데이트를 찾은 다음 **Upload(**업로드**)**를 클릭합니다.

단계 **3** VDB를 설치합니다.

a) Vulnerability and Fingerprint Database update(취약성 및 지문 데이터베이스 업데이트) 옆에 있는 **Install(**설치**)** 아이콘을 클릭합니다
b) management center을(를) 선택합니다.
c) **Install(**설치**)**을 클릭합니다.

메시지 센터에서 업데이트 진행 상황을 모니터링합니다. 업데이트가 완료된 후, 시스템이 새 취약성 정보를 사용합니다. 그러나 구성을 구축해야 업데이트된 애플리케이션 탐지기 및 운영 체제 지문을 적용할 수 있습니다.

단계 **4** 업데이트 성공을 확인합니다.

도움말( ) > 소개 를 선택하고 VDB 현재 버전을 확인합니다.

다음에 수행할 작업

Deploy configuration changes(구성 변경 사항 구축)참조.

VDB 업데이트 예약

management center이 인터넷 액세스 권한이 있는 경우 정기적인 VDB 업데이트를 예약하는 것이 좋습니다. 취약성 데이터베이스 업데이트 자동화의 내용을 참조하십시오.

지리위치 데이터베이스 업데이트

GeoDB(지리위치 데이터베이스)는 지리적 위치를 기준으로 트래픽을 보고 필터링하는 데 사용할 수 있는 데이터베이스입니다.

시스템은 IP 주소를 국가/대륙에 매핑하는 초기 GeoDB 국가 코드 패키지와 함께 제공되므로 정보를 항상 사용할 수 있습니다. GeoDB를 업데이트하면 시스템은 상황 데이터가 포함된 IP 패키지도 다운로드합니다. 이 상황 데이터에는 추가 위치 세부 정보는 물론 ISP, 연결 유형, 프록시 유형, 도메인 이름 등의 연결 정보가 포함됩니다. 또한 GeoDB는 정기적으로 업데이트되므로 정확한 지리위치 정보를 얻으려면 GeoDB를 정기적으로 업데이트해야 합니다.

시스템은 초기 구성 중에 주 단위로 자동 GeoDB 업데이트를 구성합니다. 업데이트 구성에 실패하고 management center이 인터넷에 액세스할 수 있는 경우, GeoDB 업데이트 예약, 7 페이지.

GeoDB를 업데이트하는 데 필요한 시간은 어플라이언스에 따라 다르지만, 전체 GeoDB를 처음 다운로드하는 경우 등 업데이트 크기에 따라 최대 45분이 걸릴 수 있습니다. GeoDB 업데이트를 수행해도 지리위치 정보의 지속적인 수집을 비롯한 기타 시스템 기능이 중단되지는 않지만, 업데이트를 완료하는 동안 시스템 리소스가 사용됩니다. 업데이트를 예약하는 경우 이를 고려하십시오.

GeoDB 업데이트는 GeoDB의 이전 버전을 무시하고 즉시 적용됩니다. GeoDB를 업데이트할 때, management center는 매니지드 디바이스 관련 데이터를 자동으로 업데이트합니다. GeoDB 업데이트가 구축 전반에 적용되려면 몇 분 정도 걸릴 수 있습니다. 업데이트 후 다시 구축할 필요가 없습니다.

시스템 ( ) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)** 페이지와 도움말( ) > 소개 페이지 모두 현재 버전을 나열합니다.

GeoDB 업데이트 예약

시스템은 초기 구성 중에 주 단위로 자동 GeoDB 업데이트를 구성합니다. 업데이트 구성에 실패하고 management center이 인터넷에 액세스할 수 있는 경우, 이 절차.

시작하기 전에

management center이 인터넷에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**을(를) 선택합니다.

단계 **2** Recurring Geolocation Updates(반복되는 지리위치 업데이트)에서 **Enable Recurring Weekly Updates from the Support Site(**지원 사이트에서 반복되는 주간 업데이트 활성화**)**를 선택합니다.

단계 **3** **Update Start Time(**업데이트 시작 시간**)**을 지정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

GeoDB 수동 업데이트(인터넷 연결)

management center가 인터넷에 액세스할 수 있는 경우 이 절차를 사용하여 GeoDB의 온디맨드 업데이트를 수행합니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**을(를) 선택합니다.

단계 **2** One-Time Geolocation Update(일회성 지리위치 업데이트)에서 **Download and install geolocation update from the Support Site(**지원 사이트에서 지리위치 업데이트 다운로드 및 설치**)**를 선택합니다.

단계 **3** **Import(**가져오기**)**를 클릭합니다.

메시지 센터에서 업데이트 진행률을 모니터링할 수 있습니다.

단계 **4** 업데이트 성공을 확인합니다.

Geolocation Updates(지리위치 업데이트) 페이지와 도움말(?) > 소개 페이지 모두 현재 버전을 나열합니다.

GeoDB 수동 업데이트(인터넷 연결 없음)

management center가 인터넷에 액세스할 수 없는 경우 이 절차를 사용하여 GeoDB의 온디맨드 업데이트를 수행합니다.

프로시저

단계 **1** Cisco 지원 및 다운로드 사이트: https://www.cisco.com/go/firepower-software에서 GeoDB를 다운로드합니다.

모델을 선택하거나 검색한 다음(또는 모든 management center에 대해 동일한 GeoDB를 사용하는 모델을 선택) *Coverage and Content Updates*(커버리지 및 콘텐츠 업데이트) 페이지로 이동합니다.

국가 코드와 IP 패키지를 모두 다운로드해야 합니다.

단계 **2** 시스템 ( ) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**을(를) 선택합니다.

단계 **3** One-Time Geolocation Update(일회성 지리위치 업데이트)에서 **Upload and install geolocation update(**지리위치 업데이트 업로드 및 설치**)**를 선택합니다.

단계 **4** **Choose File(**파일 선택**)**을 클릭한 다음 이전에 다운로드한 국가 코드 패키지를 찾습니다.

단계 **5** **Import(**가져오기**)**를 클릭합니다.

메시지 센터에서 업데이트 진행률을 모니터링할 수 있습니다.

단계 **6** IP 패키지에 대해 4~5단계를 반복합니다.

단계 **7** 업데이트 성공을 확인합니다.

Geolocation Updates(지리위치 업데이트) 페이지와 도움말( ) > 소개 페이지 모두 현재 버전을 나열합니다.

침입 규칙 업데이트

새로운 취약성이 알려지면 Talos 인텔리전스 그룹은 가져올 수 있는 침입 규칙 업데이트를 management center로 릴리스하고, 그런 다음 변경된 구성을 매니지드 디바이스에 구축하여 구현합니다. 이러한 업데이트는 침입 규칙, 전처리기 규칙 및 규칙을 사용하는 정책에 영향을 줍니다.

규칙 업데이트는 누적되며, Cisco에서는 항상 최신 업데이트를 가져올 것을 권장합니다. 현재 설치된 규칙의 버전과 일치하거나 이전의 침입 규칙 업데이트는 가져올 수 없습니다.

침입 규칙 업데이트는 다음을 제공할 수 있습니다.

- 신규 및 수정된 규칙 및 규칙 상태 — 규칙 업데이트는 신규 및 업데이트된 침입 규칙과 전처리기 규칙을 제공합니다. 새 규칙의 경우, 규칙 상태는 각 시스템이 제공하는 침입 정책에서 다를 수 있습니다. 예를 들어, 새 규칙은 Security Over Connectivity(연결성에 우선하는 보안) 침입 정책에서 활성화되며 Connectivity Over Security(보안에 우선하는 연결성) 침입 정책에서는 비활성화됩니다. 규칙 업데이트는 기존 규칙의 기본 상태를 변경하거나, 기존 규칙을 완전히 삭제할 수 있습니다.
- 새 규칙 카테고리 — 규칙 업데이트에는 새 규칙 카테고리가 포함될 수 있는데, 이는 항상 추가됩니다.

- 수정된 프리프로세서 및 고급 설정 — 규칙 업데이트는 시스템이 제공한 침입 정책에 있는 고급 설정 및 시스템이 제공한 네트워크 분석 정책에 있는 전처리기 구성을 변경할 수 있습니다. 이들은 또한 액세스 제어 정책의 고급 전처리 및 성능 옵션에 대한 기본값을 업데이트할 수 있습니다.
- 신규 및 수정된 변수 — 규칙 업데이트는 기존의 기본 변수에 대한 기본값을 변경할 수 있지만, 변경 사항을 재정의하지 않습니다. 새로운 변수는 항상 추가됩니다.

다중 도메인 구축에서는 로컬 침입 규칙을 모든 도메인에 가져올 수 있지만 Talos의 침입 규칙 업데이트는 전역 도메인에만 가져올 수 있습니다.

침입 규칙 업데이트가 정책을 수정하는 시점에 대한 이해

침입 규칙 업데이트는 모든 액세스 제어 정책뿐만 아니라 시스템이 제공한 네트워크 분석 정책 및 사용자 지정 네트워크 분석 정책 모두에도 영향을 미칠 수 있습니다.

- 시스템제공—시스템이 제공한 네트워크 분석 및 침입 정책에 대한 변경 사항뿐만 아니라 고급 액세스 제어 설정에 대한 모든 변경 사항은 업데이트한 후 정책을 다시 구축할 때 자동으로 적용됩니다.
- 사용자 지정 — 각 사용자 지정 네트워크 분석 및 침입 정책은 시스템이 제공한 정책을 자체 기반으로, 또는 정책 체인의 궁극적인 기반으로 사용하므로 규칙 업데이트는 사용자 지정 네트워크 분석 및 침입 정책에 영향을 미칠 수 있습니다. 하지만, 규칙 업데이트가 자동으로 해당 변경 사항을 적용하는 것을 방지할 수 있습니다. 이를 통해 규칙 업데이트를 가져오는 것과 별개로 시스템 제공 기본 정책을 수동으로 업데이트할 수 있습니다. (사용자 지정 정책별 기반으로 실행되는) 선택 사항과 관계없이, 시스템이 제공한 정책에 대한 업데이트는 사용자 지정한 어떤 설정도 재지정하지 않습니다.

규칙 업데이트를 가져오면 네트워크 분석 및 침입 정책에 캐시된 변경 사항이 모두 제거된다는 점에 유의하십시오. 사용자의 편의를 위해, Rule Updates(규칙 업데이트) 페이지는 캐시된 변경 사항이 있는 정책및 변경한 사용자을 나열합니다.

침입 규칙 업데이트 구축

침입 규칙 업데이트를 통해 수행된 변경 사항을 적용하려면 구성을 재구축해야 합니다. 규칙 업데이트를 가져올 때 영향을 받는 디바이스에 자동으로 재구축하도록 시스템을 구성할 수 있습니다. 이 접근법은 침입 규칙 업데이트가 시스템이 제공하는 기본 침입 정책을 수정할 수 있는 경우에 특히 유용합니다.

반복 침입 규칙 업데이트

Rule Updates(규칙 업데이트) 페이지를 사용하여 일 단위, 주 단위 또는 월 단위로 규칙 업데이트를 가져올 수 있습니다.

management center의 고가용성 쌍이 배포에 포함된 경우, 기초 수준의 업데이트만 가져옵니다. 이차적 management center는 일반 동기화 프로세스의 일부로 규칙 업데이트를 수신합니다.

침입 규칙 업데이트 가져오기에서 적용 가능한 하위 태스크는 다운로드, 설치, 기본 정책 업데이트 및 구성 구축 순서로 수행됩니다. 1개의 하위 태스크가 완료되면, 다음 하위 태스크가 시작됩니다.

시스템은 이전 단계에서 지정한 대로 예약된 시간에 규칙 업데이트를 설치하고 변경된 구성을 구축합니다. 가져오기 작업 중 또는 작업 이전에 로그 오프하거나 웹 인터페이스를 사용하여 다른 작업을 수행할 수 있습니다. 가져오기 작업 중에 액세스된 경우, Rule Update Log(규칙 업데이트 로그)는 **Red Status(**빨간색 상태**)** ( )를 표시하며, Rule Update Log(규칙 업데이트 로그) 상세 보기에서 메시지가 나타나면 이를 확인할 수 있습니다. 규칙 업데이트 크기 및 콘텐츠에 따라, 몇 분이 지난 후에 상태 메시지가 표시될 수 있습니다.

초기 구성 중에 시스템은 Cisco 지원 및 다운로드 사이트에서 매일 Snort 2 디바이스용 자동 침입 규칙 업데이트(SRU) 를 구성합니다. 업데이트 구성에 실패하고 management center이 인터넷에 액세스할 수 있는 경우, 침입 규칙 업데이트 예약, 11 페이지.

로컬 침입 규칙 가져오기

로컬 침입 규칙은 로컬 컴퓨터에 ASCII 또는 UTF-8로 인코딩한 일반 텍스트 파일로 가져오는 맞춤형 표준 텍스트 규칙입니다. Snort 사용자 설명서의 지침을 사용하여 로컬 규칙을 생성할 수 있습니다. 지침은 http://www.snort.org에서 다운로드할 수 있습니다.

다중 도메인 구축에서 로컬 침입 규칙을 모든 도메인으로 가져올 수 있습니다. 현재 도메인 및 상위 도메인에서 가져온 로컬 침입 규칙을 볼 수 있습니다.

침입 규칙 일회성 수동 업데이트

management center이 인터넷 액세스할 수 없는 경우, 새로운 침입 규칙 업데이트를 수동으로 가져옵니다.

프로시저

단계 **1** Cisco 지원 사이트(http://www.cisco.com/cisco/web/support/index.html)에서 업데이트를 수동으로 다운로드합니다.

단계 **2** 시스템 ( ) > **Updates(**업데이트**)**를 선택한 후, **Rule Updates(**규칙 업데이트**)** 탭을 클릭합니다.

단계 **3** 사용자가 생성했거나 가져온 사용자 정의 규칙을 삭제된 폴더로 옮기려는 경우, 툴바에 있는 **Delete All Local Rules(**모든 로컬 규칙 삭제**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** **Rule Update or text rule file to upload and install(**규칙 업데이트 또는 업로드 및 설치할 텍스트 규칙 파일**)**을 선택하고 **Browse(**검색**)**를 클릭하여 규칙 업데이트 파일을 탐색하고 선택합니다.

단계 **5** 업데이트가 완료된 후 매니지드 디바이스에 정책을 자동으로 다시 구축하려는 경우, **Reapply all policies after the rule update import completes(**규칙 업데이트 가져오기가 완료된 후 모든 정책 재적용**)**을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다. 시스템에 규칙 업데이트가 설치되고 Rule Update Log(규칙 업데이트 로그) 상세 보기가 표시됩니다.

참고 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 Support(지원팀)에 문의하십시오.

침입 규칙 일회성 자동 업데이트

참고 이 섹션은 Snort 2에만 적용됩니다.

새 침입 규칙 업데이트를 자동으로 가져오려면 어플라이언스가 인터넷에 액세스해야 지원 사이트에 연결할 수 있습니다.

시작하기 전에

- management center에서 인터넷에 액세스할 수 있는지 확인합니다. 보안, 인터넷 액세스 및 통신 포트의 내용을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)**를 선택합니다.

참고 침입 규칙 편집기 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다 (**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**).

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** 사용자가 생성했거나 가져온 사용자 정의 규칙을 삭제된 폴더로 옮기려는 경우, 툴바에 있는 **Delete All Local Rules(**모든 로컬 규칙 삭제**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** **Download new Rule Update from the Support Site(**지원 사이트에서 새로운 규칙 업데이트 다운로드**)**를 선택합니다.

단계 **5** 업데이트가 완료된 후 매니지드 디바이스에 변경된 구성을 자동으로 다시 구축하려는 경우, **Reapply all policies after the rule update import completes(**규칙 업데이트 가져오기가 완료된 후 모든 정책 재적용**)** 확인란을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.
시스템에 규칙 업데이트가 설치되고 Rule Update Log(규칙 업데이트 로그) 상세 보기가 표시됩니다.

주의 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 Support(지원팀)에 문의하십시오.

침입 규칙 업데이트 예약

참고 이 섹션은 Snort 2에만 적용됩니다.

초기 구성 중에 시스템은 Cisco 지원 및 다운로드 사이트에서 매일 Snort 2 디바이스용 자동 침입 규칙 업데이트(SRU) 를 구성합니다. 업데이트 구성에 실패하고 management center이 인터넷에 액세스할 수 있는 경우, 이 섹션.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)**를 선택합니다.

참고 침입 규칙 편집기 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다 (**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**).

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** 사용자가 생성했거나 가져온 사용자 정의 규칙을 삭제된 폴더로 옮기려는 경우, 툴바에 있는 **Delete All Local Rules(**모든 로컬 규칙 삭제**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** **Enable Recurring Rule Update Imports from the Support Site(**지원 사이트에서 반복 규칙 업데이트 가져오기 활성화**)** 확인란을 선택합니다.

Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기**)** 섹션 제목 아래에 가져오기 상태 메시지가 나타납니다.

단계 **5** **Import Frequency(**가져오기 빈도**)** 필드에서 다음을 지정합니다.

- 업데이트 빈도(**Daily(**매일**)**, **Weekly(**매주**)**, or **Monthly(**매월**)**)
- 업데이트를 수행할 주나 월의 날짜
- 업데이트를 시작하려는 시간

단계 **6** 업데이트가 완료된 후 매니지드 디바이스에 변경된 구성을 자동으로 다시 구축하려는 경우, **Deploy updated policies to targeted devices after rule update completes(**규칙 업데이트 완료 후 업데이트된 정책을 대상 디바이스에 구축**)** 확인란을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

주의 침입 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 지원팀에 문의하십시오.

Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기) 섹션 제목 아래의 상태 메시지가 변경되어 규칙 업데이트가 아직 실행되지 않았음을 나타냅니다.

로컬 침입 규칙 가져오기 모범 사례

로컬 규칙 파일을 가져올 때 다음 지침을 따르십시오.

- 규칙 가져오기 도구를 사용하려면 모든 맞춤형 규칙을 ASCII 또는 UTF-8로 인코딩된 일반 텍스트로 가져와야 합니다.
- 텍스트 파일 이름은 영숫자 및 공백을 포함할 수 있지만 밑줄(_), 마침표(.) 및 대시(-)를 제외한 특수 문자는 포함할 수 없습니다.

- 시스템이 단일 파운드 문자(#)로 시작되는 로컬 규칙을 가져오지만, 삭제된 것으로 플래그 표시됩니다.
- 시스템이 단일 파운드 문자(#)로 시작하는 로컬 규칙을 가져오지만, 파운드 문자 2개(##)로 시작하는 로컬 규칙은 가져오지 않습니다.
- 규칙은 확장 문자를 사용할 수 없습니다.
- 다중 도메인 구축에서 시스템은 전역 도메인으로 가져오거나 생성된 규칙에 GID 1을 할당하고 다른 모든 도메인에서는 도메인 별 GID를 1000과 2000 사이로 할당합니다.
- 로컬 규칙을 가져올 때 GID(Generator ID)를 지정할 필요가 없습니다. 이렇게 하면 표준 텍스트 규칙에 GID 1만 지정됩니다.
- 처음으로 규칙을 가져오는 경우, Snort ID (SID) 또는 개정 번호를 지정하지 마십시오. 이렇게 하면 삭제된 규칙을 포함해 다른 규칙의 SID와 충돌을 피할 수 있습니다. 시스템은 해당 규칙에 다음으로 사용 가능한 1000000 이상의 사용자 지정 규칙 SID와 수정 번호 1을 자동으로 할당합니다.

  SID가 있는 규칙을 가져와야 하는 경우, SID는 1,000,000 이상의 고유 숫자가 될 수 있습니다.

  다중 도메인 구축에서 여러 관리자가 동시에 로컬 규칙을 가져오는 경우, 시스템이 시퀀스의 중간 숫자를 다른 도메인에 할당했기 때문에 개별 도메인 내의 SID가 비순차적으로 보일 수 있습니다.
- 이전에 가져온 로컬 규칙의 업데이트된 버전을 가져올 경우 또는 삭제한 로컬 규칙을 되돌리는 경우, 반드시 시스템이 할당한 SID와 현재 개정 번호보다 큰 개정 번호를 포함해야 합니다. 규칙을 편집하여 현재 또는 삭제된 규칙의 개정 번호를 결정할 수 있습니다.

참고 로컬 규칙을 삭제하면 자동으로 개정 번호가 증가합니다. 이 디바이스를 통해 로컬 규칙을 복원할 수 있습니다. 삭제된 모든 로컬 규칙은 로컬 규칙 카테고리에서 삭제된 규칙 카테고리로 이동합니다.

- 고가용성 쌍으로 된 기본 Firepower Management Center의 로컬 규칙을 가져오고 SID 번호 매기기 문제를 방지합니다.
- 규칙에 다음 중 하나가 포함되는 경우 가져오기가 실패합니다.
  - 2147483647 보다 큰 SID.
  - 64자를 초과하는 소스 또는 대상 포트의 목록.
  - 다중 도메인 구축에서 전역 도메인으로 가져오는 경우, GID:SID 조합은 GID 1과 이미 다른 도메인에 있는 SID를 사용합니다. 이는 해당 조합이 버전 6.2.1 이전에 존재했음을 나타냅니다. GID 1과 고유한 SID를 사용하여 규칙을 다시 가져올 수 있습니다.
- 더 이상 사용되지 않는 `threshold` 키워드를 침입 정책의 침입 이벤트 임계값 설정 기능과 조합하여 사용하는, 가져온 로컬 규칙을 활성화하는 경우 정책 인증이 실패합니다.
- 가져온 모든 로컬 규칙은 로컬 규칙 카테고리에 자동으로 저장됩니다.

- 시스템은 사용자가 가져오는 로컬 규칙을 항상 비활성화된 규칙 상태로 설정합니다. 로컬 규칙을 침입 정책에서 사용하기 전에 상태를 수동으로 설정해야 합니다.

로컬 침입 규칙 가져오기

- 로컬 규칙 파일이 로컬 침입 규칙 가져오기 모범 사례, 12 페이지에 설명된 지침을 따르는지 확인합니다.
- 로컬 침입 규칙을 가져오는 프로세스가 보안 정책을 준수하는지 확인합니다.
- 대역폭 제한 및 Snort 재시작으로 인해 가져오기가 트래픽 흐름 및 검사에 미치는 영향을 고려합니다. 유지 보수 기간 중 규칙 업데이트를 예약하는 것이 좋습니다.
- 모든 도메인에서 이 작업을 수행할 수 있습니다.

이 절차를 사용하여 로컬 침입 규칙을 가져옵니다. 가져온 침입 규칙이 로컬 규칙 카테고리에 비활성화된 상태로 나타납니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)**를 선택한 후, **Rule Updates(**규칙 업데이트**)** 탭을 클릭합니다.

단계 **2** (선택 사항) 기존 로컬 규칙을 삭제합니다.

Delete All Local Rules(모든 로컬 규칙 삭제**)**를 클릭한 후, 생성했거나 가져온 모든 침입 규칙을 삭제된 폴더로 옮기는지 확인합니다.

단계 **3** **One-Time Rule Update/Rules Import(**일회성 규칙 업데이트/규칙 가져오기**)** 아래에서 **Rule update or text rule file to upload and install(**업로드 및 설치할 규칙 업데이트 또는 텍스트 규칙 파일**)**을 선택한 다음 **Choose File(**파일 선택**)**을 클릭하여 로컬 규칙 파일을 찾습니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

단계 **5** Message Center의 가져오기 진행 상황을 모니터링합니다.

Message Center를 표시하려면, 메뉴 바에서 System Status(시스템 상태)를 클릭합니다. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 가져오기가 실패했다고 나타나더라도 가져오기를 재시작하지 마십시오. 대신 Cisco TAC에 문의하십시오.

다음에 수행할 작업

- 침입 정책을 수정하고 가져온 규칙을 활성화합니다.
- 구성 변경 사항 구축. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 구성 변경 사항 구축

규칙 업데이트 로그

management center은 사용자가 가져오는 각 규칙 업데이트 및 로컬 규칙 파일에 대한 레코드를 생성합니다.

각 레코드에는 파일을 가져온 사용자의 타임 스탬프, 이름 및 가져오기가 성공 또는 실패되었음을 나타내는 상태 아이콘이 포함됩니다. 가져온 모든 규칙 업데이트 및 로컬 파일 규칙의 목록을 유지할 수 있고, 목록에서 가져온 모든 레코드를 삭제할 수 있으며, 가져온 모든 규칙 및 규칙 업데이트 구성 요소에 대한 세부 레코드에 액세스할 수 있습니다.

Rule Update Import Log(규칙 업데이트 가져오기 로그) 상세 보기에서는 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 개체에 대한 세부 레코드가 나열됩니다. 특정 요건에 일치하는 정보만 포함하는 나열된 레코드로부터 사용자 지정 워크플로 또는 보고서를 생성할 수도 있습니다.

침입 규칙 업데이트 로그 테이블

표 *2:* 침입 규칙 업데이트 로그 필드

필드	설명
요약	가져오기 파일의 이름입니다. 가져오기가 실패한 경우, 실패 이유에 대한 간략한 설명이 파일 이름 아래에 나타납니다.
시간	가져오기가 시작된 날짜 및 시간입니다.
사용자 ID	가져오기를 시작한 사용자의 사용자 이름입니다.
상태	가져오기 여부: • **Succeeded(**성공함**)** ( ) • 실패 또는 현재 진행 중 **Red Status(**빨간색 상태**)** ( ) 가져오기 작업 진행 중에는 실패했거나 완료되지 않은 가져오기를 나타내는 빨간색 상태 아이콘이 Rule Update Log(규칙 업데이트 로그) 페이지에 나타나고 가져오기가 성공적으로 완료된 경우에만 이 아이콘이 녹색으로 바뀝니다.

팁 침입 규칙 업데이트 가져오기가 진행되는 동안 나타나는 가져오기 세부사항을 볼 수 있습니다.

침입 규칙 업데이트 로그 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 시스템 ( ) > **Updates(**업데이트**)**를 선택합니다.

팁 침입 규칙 편집기 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다 (**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**).

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** **Rule Update Log(**규칙 업데이트 로그**)**를 클릭합니다.

단계 **4** 다음 2가지 옵션을 사용할 수 있습니다.

- View(보기) - 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 개체에 대한 세부 사항을 보려면 확인하려는 파일 옆에 있는 **View(**보기**)** ( )를 클릭합니다. 침입 규칙 업데이트 가져오기 로그 세부 정보 보기, 18 페이지의 내용을 참조하십시오.
- Delete(삭제) - 파일에 포함된 모든 개체에 대한 세부 레코드를 포함하여 가져오기 파일 레코드를 가져오기 로그에서 삭제하려면 가져오기 파일 이름 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.

  참고 로그에서 파일을 삭제해도 가져오기 파일에서 가져온 모든 개체를 삭제하는 것은 아니며, 가져오기 로그 레코드만 삭제합니다.

침입 규칙의 필드에 로그를 업데이트합니다.

팁 단일 가져오기 파일에 대한 레코드만 표시된 Rule Update Import Log(규칙 업데이트 가져오기 로그) 상세 보기의 툴바에서 **Search(**검색**)**를 클릭하여 검색을 시작하는 경우에도 Rule Update Import Log(규칙 업데이트 가져오기 로그) 데이터베이스 전체를 검색합니다. 검색에 포함할 모든 개체를 포함하도록 시간 제약 조건을 설정해야 합니다.

표 *3:* 규칙 업데이트 가져오기 로그 상세 보기 필드

필드	설명
조치	다음 중 하나가 개체 유형에 발생했음을 나타냅니다. • `new(신규)` (해당 규칙이 어플라이언스에 처음 저장된 경우) • `changed(변경됨)`(규칙 업데이트 구성 요소 또는 규칙의 경우, 규칙 업데이트 구성 요소가 변경되었거나 규칙이 더 높은 수정 번호 및 동일한 GID 및 SID를 지닙니다.) • `collision(충돌)` (규칙 업데이트 구성 요소 또는 규칙의 경우, 해당 수정 버전이 기존 구성 요소 또는 규칙과 충돌하여 가져오기를 건너뛰었습니다.) • `deleted(탐지됨)`(규칙의 경우, 규칙이 규칙 업데이트에서 삭제되었습니다.) • `enabled(활성화됨)`(규칙 업데이트 수정에서 전처리기, 규칙 또는 다른 기능이 시스템 제공 기본 정책에서 활성화되었습니다.) • `disabled(비활성화됨)` (규칙의 경우, 시스템 제공 기본 정책에서 규칙이 비활성화되었습니다.) • `drop(삭제)`(규칙의 경우, 시스템 제공 기본 정책에서 규칙이 Drop and Generate Events(삭제 후 이벤트 생성)로 설정되었습니다.) • `error(오류)`(규칙 업데이트 또는 로컬 규칙 파일의 경우, 가져오기가 실패했습니다.) • `apply(적용)`(해당 가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes(**규칙 업데이트 가져오기가 완료된 후 침입 정책 다시 적용**)** 옵션이 활성화되었습니다.)
기본 작업	규칙 업데이트에 의해 정의된 기본 작업. 가져온 개체 유형이 `rule(규칙)`인 경우, 기본 작업은 `Pass(통과)`, `Alert(경고)` 또는 `Drop(삭제)`입니다. 다른 모든 가져온 개체 유형의 경우, 기본 작업이 없습니다.
세부 사항	구성 요소 또는 규칙에 고유한 문자열. 규칙의 경우, 변경된 규칙의 GID, SID 및 이전 수정 번호이며, `previously (GID:SID:Rev)(이전(GID:SID:Rev))`로 표시됩니다. 변경되지 않은 규칙의 경우 이 필드는 비어 있습니다.
도메인	침입 정책이 업데이트된 규칙을 사용할 수 있는 도메인. 하위 도메인의 침입 정책도 규칙을 사용할 수 있습니다. 이 필드는 다중 도메인 구축에서만 나타납니다.
GID	규칙에 대한 생성기 ID. 예를 들어, `1` (표준 텍스트 규칙, 전역 도메인 또는 레거시 GID) 또는 `3` (공유 개체 규칙).
이름	규칙 Message(메시지) 필드에 해당하는 규칙 및 규칙 업데이트 구성 요소에 대해 가져온 개체의 이름이 구성 요소 이름입니다.
정책	가져온 규칙의 경우, 이 필드는 `All(모두)`로 표시됩니다. 이는 해당 규칙 가져오기가 성공하였고 모든 적절한 기본 침입 정책에서 활성화될 수 있다는 의미입니다. 가져온 개체의 다른 유형의 경우, 이 필드는 비어 있습니다.
Rev	규칙의 수정 번호.
규칙 업데이트	규칙 업데이트 파일 이름.

필드	설명
SID	규칙의 SID.
시간	가져오기가 시작된 날짜 및 시간입니다.
유형	가져온 개체 유형. 다음 중 하나일 수 있습니다. • `rule update component(규칙 업데이트 구성 요소)`(규칙 팩 또는 정책 팩과 같은 가져온 구성 요소) • `rule(규칙)`(규칙의 경우, 신규 또는 업데이트된 규칙입니다. 버전 5.0.1에서 이 값이 더 이상 사용되지 않는 `update(업데이트)` 값을 대체했다는 점에 유의하십시오.) • `policy apply(정책 적용)`(해당 가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes(**규칙 업데이트 가져오기가 완료된 후 침입 정책 다시 적용**)** 옵션이 활성화되었습니다.)
개수	각 레코드의 개수(`1`). 표를 제한할 때 표 보기에 Count(개수) 필드가 나타나며, Rule Update Log(규칙 업데이트 로그) 상세 보기는 기본적으로 규칙 업데이트 레코드에 제한됩니다. 이 필드는 검색할 수 없습니다.

침입 규칙 업데이트 가져오기 로그 세부 정보 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)**를 선택합니다.

팁 침입 규칙 편집기 페이지에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다 (**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**).

단계 **2** **Rule Updates(**규칙 업데이트**)**를 클릭합니다.

단계 **3** **Rule Update Log(**규칙 업데이트 로그**)**를 클릭합니다.

단계 **4** 보려는 상세 레코드의 파일 옆에 있는 **View(**보기**)** (👁)를 클릭합니다.

단계 **5** 다음 작업을 수행할 수 있습니다.

- Bookmark(즐겨찾기) — 현재 페이지를 즐겨찾기 하려면 **Bookmark This Page(**이 페이지 즐겨찾기에 등록**)**를 클릭합니다.
- Edit Search(검색 편집) — 현재 단일 제약조건이 미리 입력된 검색 페이지를 열려면 Search Constraints(검색 제약조건) 옆에 있는 **Edit Search(**검색 편집**)** 또는 **Save Search(**검색 저장**)**를 선택합니다.
- Manage bookmarks(즐겨찾기 관리) — 즐겨찾기 관리 페이지로 이동하려면 **Report Designer(**리포트 디자이너**)**를 클릭합니다.

- Report(보고서) — 현재 보기의 데이터를 기반으로 보고서를 생성하려면 **Report Designer(**리포트 디자이너**)**를 클릭합니다.
- Search(검색) — 규칙 업데이트 가져오기 로그 데이터베이스 전체에서 규칙 업데이트 가져오기 레코드를 검색하려면 **Search(**검색**)**를 클릭합니다.
- Sort(정렬) — 현재 워크플로 페이지에서 레코드를 정렬하고 유지하려면 .
- Switch workflows(워크플로 전환) — 일시적으로 다른 워크플로를 사용하려면 **(**워크플로 전환**)**을 클릭합니다.