업데이트

이 장에서는 콘텐츠 업데이트를 수행하는 방법을 설명합니다.

중요 management center 또는 threat defense 소프트웨어나 새시를 업그레이드하려면 *management center*가 현재 실행 중인 버전에 대한 업그레이드 설명서(http://www.cisco.com/go/ftd-fmc-upgradehttp://www.cisco.com/go/ftd-fmc-upgrade-74)를 참조하십시오.

매니지드 디바이스를 업그레이드하려면 클라우드 제공 Firewall Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드의 내용을 참조하십시오.

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 콘텐츠 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: 패치 및 유지 보수 릴리스만 선택합니다. 보통 릴리스 이후에 얼마간 수동으로 다운로드할 수 있습니다. 지연되는 기간은 릴리스 유형, 릴리스 채택 및 기타 요인에 따라 달라집니다. 온디맨드 다운로드 및 예약 다운로드가 모두 지원됩니다. 참고 버전 7.4.1에서는 모든 릴리스(핫픽스 제외)의 온디맨드 직접 다운로드 지원이 시작됩니다. 그러나 유지 보수 릴리스의 예약된 다운로드에 대한 지원은 중단됩니다. 설치 예약: 패치와 유지 보수 릴리스만 예약 작업으로 수행합니다. 제거: 패치만 해당됩니다. 되돌리기: threat defense를 위한 주요 릴리스 및 유지 보수 릴리스에만 해당됩니다. management center 또는 Classic 디바이스에서는 되돌리기가 지원되지 않습니다. 이미지 재설치: 주요 릴리스 및 유지 보수 릴리스에만 해당됩니다. 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
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. 예약된 작업으로 수행됩니다. 제거: VDB 357부터 management center에 대한 기준 VDB까지 모든 VDB를 설치할 수 있습니다. 참조: 취약성 데이터베이스(VDB) 업데이트, 4 페이지
GeoDB(지리위치 데이터베이스)	Cisco 지리위치 데이터베이스(GeoDB)는 라우팅 가능한 IP 주소와 관련된 지리적 및 연결 관련 데이터의 데이터베이스입니다.	직접 다운로드: 예. 예약: 예. 자체 업데이트 페이지에서 수행됩니다. 제거: 아니요. 참조: GeoDB(지리위치 데이터베이스) 업데이트, 6 페이지

구성 요소	설명	세부정보
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. 자체 업데이트 페이지에서 수행됩니다. 제거: 아니요. 참조: 침입 규칙 업데이트, 9 페이지
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. 개체 관리자에서 수행됩니다. 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. 통합/클라우드 서비스를 구성할 때 또는 예약된 작업으로 수행됩니다. 제거: 아니요. 참조: Cisco Secure Firewall Management Center 디바이스 구성 가이드

시스템 업데이트 요구 사항 및 사전 요건

모델 지원

모두

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(문제 해결 TechNote)

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.

management center의 초기 설정에서는 일회성 작업으로 Cisco에서 최신 VDB를 자동으로 다운로드하여 설치합니다. 또한 최신 VDB를 포함하여 사용 가능한 최신 소프트웨어 업데이트를 다운로드하는 매주 작업을 예약합니다. 이 주간 작업을 검토하고 필요한 경우 조정하는 것이 좋습니다. 선택적으로, 새로운 주간 작업을 예약하여 실제로 VDB를 업데이트하고 구성을 구축합니다. 자세한 내용은 취약성 데이터베이스 업데이트 자동화를 참조하십시오.

VDB 343 이상의 경우 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.

VDB 업데이트 예약

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

VDB 수동 업데이트

이 절차를 사용하여 VDB를 수동으로 업데이트합니다.VDB 357부터 management center에 대한 기준 VDB까지 모든 VDB를 설치할 수 있습니다.

⚠

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

management center가 인터넷에 액세스할 수 없는 경우 Cisco 지원 및 다운로드 사이트(https://www.cisco.com/go/firepower-software)에서 업데이트를 가져옵니다. 모델을 선택하거나 검색한 다음(또는 모든 management center에 대해 동일한 VDB를 사용하는 모델을 선택), *Coverage and Content Updates(*커버리지 및 콘텐츠 업데이트*)* 페이지로 이동합니다.

프로시저

단계 **1** VDB 업데이트 페이지로 이동합니다.

- 7.4.0 버전: 시스템 (⚙) > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)**
- 7.4.1 이상 버전: 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)** > **VDB Updates(VDB** 업데이트**)**

단계 **2** VDB를 management center로 가져오는 방법을 선택합니다.

- 직접 다운로드: **Download Updates(**업데이트 다운로드**)** 버튼.
- 수동 업로드: **Upload Update(**업데이트 업로드**)**를 클릭한 후, **Choose File(**파일 선택**)**을 클릭하고 VDB로 이동합니다. 파일을 선택한 후 **Upload(**업로드**)**를 클릭합니다.

참고 버전 7.4.0에서 **Download Updates(**업데이트 다운로드**)**를 클릭하여 최신 유지 보수 릴리스 및 구축을 위한 최신 중요 패치를 즉시 다운로드합니다.

단계 **3** VDB를 설치합니다.

a) 설치하려는 Vulnerability and Fingerprint Database(취약성 및 핑거프린트 데이터베이스) 업데이트 옆에 있는 **Install(**설치**)** 아이콘(새 VDB) 또는 **Rollback(**롤백**)** 아이콘(이전 VDB)을 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.

VDB 업데이트 페이지와 도움말( ) > 정보 에는 모두 현재 버전이 표시됩니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.
- 더 이상 사용할 수 없는 취약성, 애플리케이션 탐지기 또는 핑거프린트를 기반으로 하는 구성인 경우 해당 구성을 검토하여 트래픽을 정상적으로 처리하고 있는지 확인합니다. 또한 VDB를 업데이트하기 위해 예약된 작업이 롤백을 취소할 수 있다는 점에 유의하십시오. 이를 방지하려면 예약된 작업을 변경하거나 최신 VDB 패키지를 삭제하십시오.

GeoDB(지리위치 데이터베이스) 업데이트

GeoDB(지리위치 데이터베이스)는 지리적 위치를 기준으로 트래픽을 보고 필터링하는 데 사용할 수 있는 데이터베이스입니다. GeoDB 업데이트는 주기적으로 제공되므로, 정확한 지리위치 정보를 얻으려면 GeoDB를 정기적으로 업데이트해야 합니다. 최신 버전은 도움말( ) > 정보 에서 확인할 수 있습니다.

시스템은 IP 주소를 국가/대륙에 매핑하는 초기 GeoDB 국가 코드 패키지와 함께 제공되므로 정보를 항상 사용할 수 있습니다. 시스템은 GeoDB 업데이트(온디맨드 또는 일정에 따름)를 다운로드할 때 기본적으로 상황별 데이터가 있는 IP 패키지를 포함하여 설치합니다. 여기에는 추가 위치 세부 정보는 물론 ISP, 연결 유형, 프록시 유형, 도메인 이름 등의 연결 정보가 포함됩니다. 이 정보가 중요하지 않은 경우 IP 패키지를 비활성화하고 삭제하여 디스크 공간을 절약할 수 있습니다. VDB를 수동으로 업데이트하는 경우두 패키지를 모두 업데이트합니다.두 패키지 모두 있어야 합니다. 적어도 국가 코드 패키지가 필요합니다.

참고 시스템은 초기 구성의 일부로 매주 GeoDB 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 GeoDB 업데이트 예약, 7 페이지.

GeoDB 업데이트는 GeoDB의 이전 버전을 무시하고 즉시 적용됩니다. management center는 자동으로 매니지드 디바이스를 업데이트합니다. 재구축할 필요가 없습니다.

GeoDB를 업데이트하는 데 필요한 시간은 어플라이언스에 따라 다르지만, 업데이트 크기에 따라 최대 45분이 걸릴 수 있습니다. 시스템에서 전체 IP 패키지 집합을 다운로드하여 처리하는 경우를 예로 들 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 업데이트 예약

시스템은 초기 구성의 일부로 매주 GeoDB 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 이 절차.

시작하기 전에

management center에서 Cisco 지원 및 다운로드 사이트에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** GeoDB 업데이트 페이지로 이동합니다.

- 7.4.0 버전: 시스템 (⚙) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**
- 7.4.1 이상 버전: 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**

단계 **2** **IP Package Configuration(IP** 패키지 구성**)**에서 **IP Package Download(IP** 패키지 다운로드**)** 옵션을 사용하여 필요한 국가 코드 패키지만 다운로드할지 아니면 IP 패키지도 다운로드할지 지정합니다.

IP 패키지를 사용하지 않으면 디스크 공간이 절약되지만, IP 주소의 상황적 지리위치 데이터가 제거됩니다. 이 구성을 변경하는 경우에는 **Save(**저장**)**를 클릭합니다.

단계 **3** **Recurring Geolocation Updates(**반복되는 지리위치 업데이트**)**에서 **Enable Recurring Weekly Updates(**반복되는 주간 업데이트 활성화**)**를 체크합니다..

단계 **4** **Update Start Time(**업데이트 시작 시간**)**을 지정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

GeoDB 수동 업데이트

온디맨드 GeoDB 업데이트를 수행하려면 이 절차를 사용합니다.

시작하기 전에

management center가 인터넷에 액세스할 수 없는 경우 Cisco 지원 및 다운로드 사이트(https://www.cisco.com/go/firepower-software)에서 업데이트를 가져옵니다. 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 코드 패키지와 선택 사항인 IP 패키지를 다운로드합니다.

프로시저

단계 **1** GeoDB 업데이트 페이지로 이동합니다.

- 7.4.0 버전: 시스템 (⚙) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**
- 7.4.1 이상 버전: 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**

단계 **2** **One-Time Geolocation Update(**일회성 지리위치 업데이트**)** 아래에서 GeoDB를 업데이트할 방법을 선택합니다.

- 직접 다운로드: **Download and install...(**다운로드 및 설치**...)**를 선택합니다..
- 수동 업로드: **Upload and install...(**업로드 및 설치**...)**을 선택한 다음, **Choose File(**파일 선택**)**을 클릭하고 이전에 다운로드한 국가 코드 패키지를 찾습니다.

단계 **3** **IP Package Configuration(IP** 패키지 구성**)**에서 **IP Package Download(IP** 패키지 다운로드**)** 옵션을 사용하여 국가 코드 패키지만 사용할지 아니면 IP 패키지도 사용할지 지정합니다.

IP 패키지를 누락하면 디스크 공간이 절약되지만, IP 주소의 상황적 지리위치 데이터가 제거됩니다. GeoDB 패키지를 수동으로 업로드하더라도 IP 패키지의 데이터가 필요하지 않은 경우에는 이 옵션을 비활성화해야 합니다. 이는 이 옵션을 비활성화하면 기존의/오래된 IP 패키지가 삭제되기 때문입니다.

이 구성을 변경하는 경우에는 **Save(**저장**)**를 클릭합니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

메시지 센터에서 업데이트 진행 상황을 모니터링합니다.

단계 **5** 업데이트 성공을 확인합니다.

GeoDB 업데이트 페이지와 도움말(?) > 정보 에는 모두 현재 버전이 표시됩니다.

단계 **6** (선택 사항) 수동으로 업데이트를 업로드하는 경우, IP 패키지에 대해 이 절차를 반복합니다.

침입 규칙 업데이트

새로운 취약성이 알려지면 Talos 인텔리전스 그룹에서 침입 규칙 업데이트를 릴리스합니다. 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 설정을 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.

- 시스템 제공 — 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.

주의 규칙 업데이트 자체는 구축 시 Snort 프로세스를 재시작하지 않지만 다른 변경 사항으로 인해 재시작될 수도 있습니다. Snort를 다시 시작하면 고가용성/확장성을 위해 구성된 디바이스를 포함하여 모든 디바이스의 트래픽 흐름 및 검사가 잠시 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다. Snort를 다시 시작하지 않고 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다.

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.

시스템은 초기 구성의 일부로 매일 침입 규칙 업데이트를 예약합니다. 이 작업을 검토하고 필요한 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 업데이트 예약

시스템은 초기 구성의 일부로 매일 침입 규칙 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 이 절차.

시작하기 전에

- 침입 규칙을 업데이트하는 프로세스가 보안 정책을 준수하는지 확인합니다.
- 대역폭 제한 및 Snort 재시작으로 인해 업데이트가 트래픽 플로우 및 검사에 미치는 영향을 고려합니다. 유지 보수 창에서 업데이트를 수행하는 것이 좋습니다.
- management center이 인터넷에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** 규칙 업데이트 페이지로 이동합니다.

- 7.4.0 버전: 시스템 (⚙) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**
- 7.4.1 이상 버전: 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)** > **Rule Updates(**규칙 업데이트**)**

단계 **2** **Recurring Rule Update Imports(**반복 규칙 업데이트 가져오기**)**에서 **Enable Recurring Rule Update Imports(**반복 규칙 업데이트 가져오기 활성화**)**를 선택합니다.

단계 **3** **Import Frequency(**가져오기 빈도**)** 및 시작 시간을 지정합니다.

단계 **4** (선택 사항) 각 업데이트 이후에 구축하려면 **Reapply all policies...(**모든 정책 재적용**...)**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

침입 규칙 수동 업데이트

온디맨드 침입 규칙 업데이트를 수행하려면 이 절차를 사용합니다.

시작하기 전에

- 침입 규칙을 업데이트하는 프로세스가 보안 정책을 준수하는지 확인합니다.
- 대역폭 제한 및 Snort 재시작으로 인해 업데이트가 트래픽 플로우 및 검사에 미치는 영향을 고려합니다. 유지 보수 창에서 업데이트를 수행하는 것이 좋습니다.
- management center가 인터넷에 액세스할 수 없는 경우 Cisco 지원 및 다운로드 사이트(https://www.cisco.com/go/firepower-software)에서 업데이트를 가져옵니다. 모델을 선택하거나 검색한 다음(또는 모든 management center에 대해 동일한 SRU 또는 LSP를 사용하는 모델을 선택), *Coverage and Content Updates(*커버리지 및 콘텐츠 업데이트*)* 페이지로 이동합니다.

프로시저

단계 **1** 규칙 업데이트 페이지로 이동합니다.

- 7.4.0 버전: 시스템 (⚙) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**
- 7.4.1 이상 버전: 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)** > **Rule Updates(**규칙 업데이트**)**

단계 **2** **One-Time Rule Update/Rules Import(**일회성 규칙 업데이트/규칙 가져오기**)**에서 침입 규칙을 업데이트할 방법을 선택합니다.

- 직접 다운로드: **Download new rule update...(**새 규칙 업데이트 다운로드**...)**를 선택합니다..
- 수동 업로드: **Rule update or text rule file...(**규칙 업데이트 또는 텍스트 규칙 파일**...)**을 선택한 다음, **Choose File(**파일 선택**)**을 클릭하고 침입 규칙 업데이트를 찾습니다.

단계 **3** (선택 사항) 업데이트 이후에 구축하려면 **Reapply all policies...(**모든 정책 재적용**...)**를 선택합니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

메시지 센터에서 업데이트 진행 상황을 모니터링합니다. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

단계 **5** 업데이트 성공을 확인합니다.

규칙 업데이트 페이지와 도움말(?) > 정보 에는 모두 현재 버전이 표시됩니다.

다음에 수행할 작업

업데이트의 일부로 구축하지 않은 경우에는 지금 구축합니다.Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

로컬 침입 규칙 가져오기

이 절차를 사용하여 로컬 침입 규칙을 가져옵니다. 가져온 침입 규칙이 로컬 규칙 카테고리에 비활성화된 상태로 나타납니다. 모든 도메인에서 이 작업을 수행할 수 있습니다.

시작하기 전에

- 로컬 규칙 파일이 로컬 침입 규칙 가져오기 모범 사례, 13 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.

프로시저

단계 **1** 규칙 업데이트 페이지로 이동합니다.

- 7.4.0 버전: 시스템 (⚙) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**
- 7.4.1 이상 버전: 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)** > **Rule Updates(**규칙 업데이트**)**
- 모든 버전: **Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**

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.

Message Center의 가져오기 진행 상황을 모니터링할 수 있습니다. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업데이트에서 장애가 발생했다고 나타나더라도 가져오기를 재시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

다음에 수행할 작업

- 침입 정책을 수정하고 가져온 규칙을 활성화합니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

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 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.

침입 규칙 업데이트 로그 보기

시스템에서 타임스탬프, 사용자, 각 업데이트의 성공 또는 실패 여부를 기준으로 나열되는 규칙 업데이트/가져오기 로그를 생성합니다. 이러한 로그에는 업데이트된 모든 규칙 및 구성 요소에 대한 자세한 가져오기 정보가 포함됩니다. 침입 규칙 업데이트 로그 세부 정보, 15 페이지의 내용을 참고하십시오. 규칙 가져오기 로그를 보려면 이 절차를 사용합니다. 가져오기 로그를 삭제해도 가져온 개체는 삭제되지 않습니다. 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** 규칙 업데이트 페이지로 이동합니다.

- 7.4.0 버전: 시스템 ( ) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**
- 7.4.1 이상 버전: 시스템 ( ) > **Content Updates(**콘텐츠 업데이트**)** > **Rule Updates(**규칙 업데이트**)**

단계 **2** **Rule Update Log(**규칙 업데이트 로그**)**를 클릭합니다.

단계 **3** (선택 사항) 로그 파일 옆에 있는 **View(**보기**)** ( )을 클릭하여 규칙 업데이트의 세부 정보를 봅니다.

침입 규칙 업데이트 로그 세부 정보

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 *2:* 침입 규칙 업데이트 로그 세부 정보

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.) • `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.

에어-갭(Air-Gapped) 구축 유지 관리

management center이 인터넷에 연결되어 있지 않으면, 필수 업데이트가 자동으로 발생하지 않습니다. 이러한 업데이트를 수동으로 가져오고 설치해야 합니다.

자세한 내용은 다음 링크를 참조하십시오.

- 소프트웨어 업그레이드 가이드: https://cisco.com/go/ftd-fmc-upgrade
- VDB 수동 업데이트, 5 페이지
- 침입 규칙 수동 업데이트, 11 페이지
- GeoDB 수동 업데이트, 7 페이지

시스템 업데이트 히스토리

표 *3:* 버전 *7.4.1* 기능

기능	최소 **Management Center**	최소 **Threat Defense**	설명
업그레이드 시작 페이지 및 패키지 관리 개선.	Any(모든)	모두	

기능	최소 **Management Center**	최소 **Threat Defense**	설명
			새로운 업그레이드 페이지를 사용하면 업그레이드를 더 쉽게 선택하고, 다운로드하고, 관리하고, 전체 구축에 적용할 수 있습니다. 여기에는 Management Center, Threat Defense 디바이스 및 모든 이전 NGIPSv/ASA FirePOWER 디바이스가 포함됩니다. 이 페이지에는 현재 구축에 적용되는 모든 업그레이드 패키지가 나열되며, 제안된 릴리스는 특별히 표시됩니다. Cisco에서 패키지를 쉽게 선택하고 직접 다운로드할 수 있으며 수동으로 패키지를 업로드하고 삭제할 수 있습니다. 업그레이드 패키지 목록을 검색하고 직접 다운로드하려면 인터넷 액세스가 필요합니다. 그렇지 않으면 수동 관리로 제한됩니다. 해당 유지 보수 릴리스에 적어도 하나의 어플라이언스가 있는 경우(또는 패치를 수동으로 업로드한 경우) 패치는 나열되지 않습니다. 핫픽스를 수동으로 업로드해야 합니다. 신규/수정된 화면: • 시스템 (⚙) > 제품 업그레이드를 통해 이제 Management Center와 모든 매니지드 디바이스를 업그레이드하고 업그레이드 패키지를 관리할 수 있습니다. • 시스템 (⚙) > **Content Updates(**콘텐츠 업데이트**)**에서는 이제 침입 규칙, VDB, GeoDB를 업데이트할 수 있습니다. • **Devices(**디바이스**)** > **Threat Defense Upgrade(Threat Defense** 업그레이드**)**를 사용하면 Threat Defense 업그레이드 마법사로 바로 이동합니다. • 시스템 (⚙) > **Users(**사용자**)** > **User Role(**사용자 역할**)** > **Create User Role(**사용자 역할 생성**)** > **Menu-Based Permissions(**메뉴 기반 권한**)**를 사용하면 **Product Upgrades(**제품 업그레이드**)(**시스템 소프트웨어) 액세스 허용 없이 **Content Updates(**콘텐츠 업데이트**)(**VDB, GeoDB, 침입 규칙)에 대한 액세스 권한을 부여할 수 있습니다. 지원이 중단된 화면/옵션: • 시스템 (⚙) > **Updates(**업데이트**)**는 더 이상 사용되지 않습니다. 이제 모든 Threat Defense 업그레이드가 마법사를 사용합니다. • Threat Defense 업그레이드 마법사의 **Add Upgrade Package(**업그레이드 패키지 추가**)** 버튼이 새 업그레이드 페이지로 연결되는 **Manage Upgrade Packages(**업그레이드 패키지 관리**)** 링크로 교체되었습니다.

기능	최소 **Management Center**	최소 **Threat Defense**	설명
			참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
Threat Defense 업그레이드 마법사에서 되돌리기 활성화.	모두	모두 - 7.1 이상으로 업그레이드하는 경우	이제 Threat Defense 업그레이드 마법사에서 되돌리기를 활성화할 수 있습니다. 기타 버전 제한: Threat Defense를 버전7.1이상으로 업그레이드해야 합니다. 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
Threat Defense 업그레이드 마법사에서 자세한 업그레이드 상태 보기.	모두	모두	이제 Threat Defense 업그레이드 마법사의 마지막 페이지에서 업그레이드 진행 상황을 모니터링할 수 있습니다. 이 기능은 Device Management(디바이스 관리) 페이지의 Upgrade(업그레이드) 탭 및 Message Center에서 기존 모니터링 기능으로 추가됩니다. 새 업그레이드 플로우를 시작하지 않은 경우 **Devices(**디바이스**)** > **Threat Defense Upgrade(Threat Defense** 업그레이드**)**를 사용하면 현재(또는 가장 최근에 완료된) 디바이스 업그레이드의 세부 상태를 확인할 수 있는 마지막 마법사 페이지로 돌아갑니다. 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
Management Center 업그레이드 후 구성 변경 보고서를 자동으로 생성합니다.	모두	모두	주요 및 유지 보수 Management Center 업그레이드 후 구성 변경에 대한 보고서를 자동으로 생성할 수 있습니다. 이렇게 하면 구축하려는 변경 사항을 파악할 수 있습니다. 시스템에서 보고서를 생성한 후에는 메시지 센터의 Tasks(작업) 탭에서 다운로드할 수 있습니다. 기타 버전 제한: 버전 7.4.1 이상에서 Management Center를 업그레이드하는 경우에만 지원됩니다. 버전 7.4.1 또는 이전 버전으로의 업그레이드는 지원되지 않습니다. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)** > **Upgrade Configuration(**구성 업그레이드**)** > **Enable Post-Upgrade Report(**업그레이드 후 보고서 활성화**)**
제안된 릴리스 알림.	모두	모두	새로운 제안 릴리스가 제공되면 Management Center에서 알림을 보냅니다. 지금 업그레이드하지 않으려면 시스템에서 나중에 알림을 보내도록 하거나 다음 제안 릴리스까지 알림을 연기할 수 있습니다. 새 업그레이드 페이지에는 제안된 릴리스도 표시됩니다. 참조: Cisco Secure Firewall Management Center의 릴리스별 새로운 기능

기능	최소 **Management Center**	최소 **Threat Defense**	설명
Management Center용 새 업그레이드 마법사.	모두	모두	새로운 업그레이드 시작 페이지 및 마법사를 통해 Management Center 업그레이드를 더욱 쉽게 수행할 수 있습니다. 시스템 (⚙) > **Product Upgrades(**제품 업그레이드**)**를 사용하여 Management Center에 적절한 업그레이드 패키지를 가져온 다음, **Upgrade(**업그레이드**)**를 클릭하여 시작합니다. 기타 버전 제한: 버전 7.4.1 이상에서 Management Center를 업그레이드하는 경우에만 지원됩니다. Management Center를 원하는 버전으로 업그레이드하려면 사용 중인 Management Center가 현재 실행 중인 버전에 대한 업그레이드 설명서를 참조하십시오(: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드). 버전 7.4.0을 실행하는 경우, 버전 7.3.x 설명서를 참조하면 됩니다.
동기화를 일시 중지하지 않고 고가용성 Management Center를 핫픽스합니다.	모두	모두	핫픽스 릴리스 노트 또는 Cisco TAC에 달리 명시되어 있지 않은 한, 고가용성 Management Center에 핫픽스를 설치하기 위해 동기화를 일시 중지할 필요가 없습니다.
FXOS 업그레이드에 포함되는 펌웨어 업그레이드.	모두	모두	새시/**FXOS** 업그레이드 영향**.** 펌웨어 업그레이드로 인해 추가 재부팅이 발생합니다**.** Firepower 4100/9300의 경우, 이제 버전 2.14.1로의 FXOS 업그레이드에는 펌웨어 업그레이드가 포함됩니다. 디바이스의 펌웨어 구성 요소가 FXOS 번들에 포함된 것보다 오래된 경우, FXOS 업그레이드 시 펌웨어도 업데이트됩니다. 펌웨어가 업그레이드되면 디바이스가 두 번(FXOS용으로 한 번, 펌웨어용으로 한 번) 재부팅됩니다. 소프트웨어 및 운영 체제를 업그레이드할 때와 마찬가지로 펌웨어 업그레이드 중에는 구성을 변경하거나 구축하지 마십시오. 시스템이 비활성 상태로 나타나더라도 펌웨어 업그레이드 중에 수동으로 재부팅하거나 종료하지 마십시오. 참조: Cisco Firepower 4100/9300 업그레이드 가이드

기능	최소 **Management Center**	최소 **Threat Defense**	설명
다중 인스턴스 모드에서 Secure Firewall 3100에 대한 섀시 업그레이드.	7.4.1	7.4.1	다중 인스턴스 모드 내 Secure Firewall 3100의 경우, 컨테이너 인스턴스(*Threat Defense* 업그레이드)와 별도로 운영 체제 및 펌웨어를 업그레이드합니다(섀시 업그레이드). 신규/수정된 화면: • 섀시 업그레이드: **Devices(**디바이스**)** > **Chassis Upgrade(**섀시 업그레이드**)** • 위협 방어 업그레이드: **Devices(**디바이스**)** > **Threat Defense Upgrade(**위협 방어 업그레이드**)** 지원되는 플랫폼: Secure Firewall 3100(Secure Firewall 3105 제외) 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
소프트웨어 업그레이드 직접 다운로드에 대한 인터넷 액세스 요구 사항을 업데이트했습니다.	모두	모두	업그레이드 영향. 시스템이 새 리소스에 연결됩니다. Management Center 소프트웨어 업그레이드 패키지의 직접 다운로드 위치를 sourcefire.com에서 amazonaws.com으로 변경했습니다.
예약된 작업은 패치와 VDB 업데이트만 다운로드합니다.	모두	모두	업그레이드 영향. 예약된 다운로드 작업이 유지 보수 릴리스 검색을 중지합니다. **Download Latest Update(**최신 업데이트 다운로드**)** 예약 작업은 유지 보수 릴리스를 더 이상 다운로드하지 않습니다. 이제 적용 가능한 최신 패치와 VDB 업데이트만 다운로드합니다. 유지 보수(및 주요) 릴리스를 Management Center에 직접 다운로드하려면 시스템 (⚙) > **Product Upgrades(**제품 업그레이드**)**를 사용하십시오.

표 ***4:*** 버전 ***7.4.0*** 기능

기능	최소 **Management Center**	최소 **Threat Defense**	설명
콘텐츠 업데이트			

기능	최소 **Management Center**	최소 **Threat Defense**	설명
국가 코드 지리위치 패키지만다운로드합니다.	모두	모두	업그레이드 영향**.** 업그레이드하면 **IP** 패키지를 삭제할 수 있습니다**.** 이제 IP 주소를 국가/대륙에 매핑하는 지리위치 데이터베이스(GeoDB)의 국가 코드 패키지만 다운로드하도록 시스템을 구성할 수 있습니다. 추가 위치 세부 정보 및 연결 정보를 포함한 상황별 데이터를 포함하는 더 큰 IP 패키지는 이제 선택 사항입니다. 기본적으로 시스템은 IP 패키지만 다운로드합니다(기본적으로 두 패키지를 모두 다운로드하는 버전 7.4.0 및 7.4.1 제외). 신규/수정된 화면: 시스템 (⚙) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**

표 ***5:*** 버전 ***7.3.0*** 기능

기능	최소 **Management Center**	최소 **Threat Defense**	설명
제품 업그레이드			
Cisco에서 업그레이드 패키지를 선택하고 Management Center로 직접 다운로드합니다.	모두	모두	이제 관리 센터로 직접 다운로드할 위협 방어 업그레이드 패키지를 선택할 수 있습니다. > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)**에서 새 **Download Updates(**업데이트 다운로드**)**를 사용합니다. 기타 버전 제한: 버전 7.4.1에서 이 기능은 개선된 패키지 관리 시스템으로 대체됩니다. 참조: Management Center를 사용하여 업그레이드 패키지 다운로드
Threat Defense 마법사에서 업그레이드 패키지를 Management Center에 업로드합니다.	모두	모두	이제 마법사를 사용하여 Threat Defense 업그레이드 패키지를 업로드하거나 위치를 지정할 수 있습니다. 이전에는 시스템 (⚙) > **Updates(**업데이트**)**를 사용했습니다. 최소 Management Center: 7.3.0. 버전 7.4.1 이상에서 이 기능은 개선된 패키지 관리 시스템으로 대체됩니다. 참조: Threat Defense 업그레이드

기능	최소 **Management Center**	최소 **Threat Defense**	설명
Threat Defense 업그레이드 마법사에서 업그레이드할 디바이스 선택.	모두	모두	마법사를 사용하여 업그레이드할 디바이스를 선택합니다. 이제 Threat Defense 업그레이드 마법사를 사용하여 업그레이드할 디바이스를 선택하거나 세분화할 수 있습니다. 마법사에서 선택한 디바이스, 남은 업그레이드 후보, 부적격 디바이스(이유 포함), 업그레이드 패키지가 필요한 디바이스 간 보기를 전환할 수 있습니다. 이전에는 디바이스 관리 페이지만 사용할 수 있었으며 프로세스의 유연성이 훨씬 낮았습니다. 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
무인 위협 방어 업그레이드.	모두	모두	위협 방어 업그레이드 마법사는 이제 새로운 무인 모드 메뉴를 사용하여 무인 업그레이드를 지원합니다. 업그레이드할 대상 버전 및 디바이스를 선택하고 몇 가지 업그레이드 옵션을 지정한 다음 단계를 수행하면 됩니다. 로그아웃하거나 브라우저를 닫을 수도 있습니다. 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
여러 사용자의 동시 Threat Defense 업그레이드 워크플로우.	모두	모두	이제 서로 다른 디바이스를 업그레이드하는 경우에 한해 서로 다른 사용자의 동시 업그레이드 워크플로우를 허용합니다. 시스템은 이미 다른 사람의 워크플로우에 있는 디바이스를 업그레이드하는 것을 방지합니다. 이전에는 모든 사용자에게 한 번에 하나의 업그레이드 워크플로우만 허용되었습니다. 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드
Threat Defense 디바이스에 대한 업그레이드 전 문제 해결 생성을 건너뜁니다.	모두	모두	새로운 **Generate troubleshooting files before upgrade begins(**업그레이드 시작 전에 문제 해결 파일 생성**)** 옵션을 비활성화하여 주요 및 유지 보수 업그레이드 전에 문제 해결 파일을 자동으로 생성하는 작업을 건너뛸 수 있습니다. 이렇게 하면 시간과 디스크 공간이 절약됩니다. 위협 방어 디바이스에 대한 문제 해결 파일을 수동으로 생성하려면 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**을 선택하고 왼쪽 패널에서 디바이스를 클릭한 다음 **View System & Troubleshoot Details(**시스템 및 문제 해결 세부 정보 보기**), Generate Troubleshooting Files(**문제 해결 파일 생성**)**를 선택합니다. 참조: Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드

기능	최소 **Management Center**	최소 **Threat Defense**	설명
위협 방어 업그레이드에 성공한 후 Snort 3으로의 자동 업그레이드는 더 이상 선택 사항이 아닙니다.	모두	모두	업그레이드 영향. 위협 방어에서 버전 7.3 이상으로 업그레이드하는 경우 더 이상 **Snort 2**를 **Snort 3**으로 업그레이드 옵션을 비활성화할 수 없습니다. 소프트웨어 업그레이드 후에는 설정을 구축할 때 모든 적격 디바이스가 Snort 2에서 Snort 3으로 업그레이드됩니다. 개별 디바이스를 다시 전환할 수는 있지만 Snort 2는 향후 릴리스에서 더 이상 사용되지 않으므로 지금 사용을 중지하는 것이 좋습니다. 맞춤형 침입 또는 네트워크 분석 정책 사용으로 인한 자동 업그레이드 부적격 디바이스의 경우, 향상된 탐지 및 성능을 위해 Snort 3으로 수동 업그레이드하는 것이 좋습니다. 마이그레이션 지원은 버전에 맞는 Cisco Secure Firewall Management Center Snort 3 구성 가이드의 내용을 참조하십시오.

기능	최소 **Management Center**	최소 **Threat Defense**	설명
Secure Firewall 3100용 통합 업그레이드 및 설치 패키지.	모두	7.3.0	

기능	최소 **Management Center**	최소 **Threat Defense**	설명
			이미지 재설치 영향. 버전 7.3에서는 다음과 같이 Secure Firewall 3100에 대한 위협 방어 설치 및 업그레이드 패키지를 통합했습니다. • 버전 7.1–7.2 설치 패키지: cisco-ftd-fp3k.*version*.SPA • 버전 7.1–7.2 업그레이드 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • 버전 7.3 이상 통합 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar 문제 없이 위협 방어를 업그레이드할 수 있지만, 이전 위협 방어 및 ASA 버전에서 직접 위협 방어 버전 7.3 이상으로 이미지 재설치할 수는 없습니다. 이는 새 이미지 유형에 필요한 ROMMON 업데이트 때문입니다. 이러한 이전 버전에서 이미지를 재설치하려면 이전 ROMMON에서 지원되지만 새 ROMMON으로 업데이트되는 ASA 9.19 이상을 "처리"해야 합니다. 별도의 ROMMON 업데이터는 없습니다. 위협 방어 버전 7.3 이상을 사용하기 위한 옵션은 다음과 같습니다. • Threat Defense 버전 7.1 또는 7.2에서 업그레이드 - 일반 업그레이드 프로세스를 사용합니다. 해당 업그레이드 가이드를 참조하십시오. • Threat Defense 버전 7.1 또는 7.2에서 이미지 재설치 - 먼저 ASA 9.19 이상으로 이미지 재설치한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *Threat Defense(*위협 방어*)→ASA: Firepower 1000, 2100; Secure Firewall 3100* 및 *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode(Firepower 1000, 2100* 어플라이언스 모드*) Secure Firewall 3100*을 참조하십시오. • ASA 9.17 또는 9.18에서 이미지 재설치 - ASA 9.19 이상으로 먼저 업그레이드한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 업그레이드 가이드를 참조한 다음 Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *ASA→*위협 방어*: Firepower 1000, 2100* 어플라이언스 모드*, Secure Firewall 3100*을 참조하십시

기능	최소 **Management Center**	최소 **Threat Defense**	설명
			오. • 위협 방어 버전 7.3 이상에서 이미지 재설치 - 일반 이미지 재설치 프로세스를 사용합니다. Firepower Threat Defense를 사용하는 Firepower 1000/2100 및 Secure Firewall 3100/4200용 Cisco FXOS 문제 해결 가이드에서 새 소프트웨어 버전으로 시스템 이미지 재설치를 참조하십시오.
콘텐츠 업데이트			
자동 VDB 다운로드.	모두	모두	관리 센터의 초기 설정에서는 사용 가능한 최신 소프트웨어 업데이트를 다운로드하는 주간 작업을 예약합니다. 여기에는 최신 VDB(취약성 데이터베이스)가 포함되어 있습니다. 이 주간 작업을 검토하고 필요한 경우 조정하는 것이 좋습니다. 선택적으로, 새로운 주간 작업을 예약하여 실제로 VDB를 업데이트하고 구성을 구축합니다. 신규/수정된 화면: 이제 시스템에서 생성한 **Weekly Software Download(**주간 소프트웨어 다운로드**)** 예약 작업에서 **Vulnerability Database(**취약성 데이터베이스**)** 확인란이 기본적으로 활성화됩니다.
VDB를 설치합니다.	모두	모두	이제 VDB 357부터 해당 관리 센터에 대한 베이스라인 VDB까지 모든 VDB를 설치할 수 있습니다. VDB를 업데이트한 후 구성 변경 사항을 구축합니다. 더 이상 사용할 수 없는 취약성, 애플리케이션 탐지기 또는 핑거프린트를 기반으로 하는 구성인 경우 해당 구성을 검토하여 트래픽을 정상적으로 처리하고 있는지 확인합니다. 또한 VDB를 업데이트하기 위해 예약된 작업이 롤백을 취소할 수 있다는 점에 유의하십시오. 이를 방지하려면 예약된 작업을 변경하거나 최신 VDB 패키지를 삭제하십시오. 신규/수정된 화면: 에서시스템 (⚙) > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)** > **Available Updates(**사용 가능한 업데이트**)**에서 이전 VDB를 업로드하면 **Install(**설치**)** 아이콘 대신 새 **Rollback(**롤백**)** 아이콘이 나타납니다.

표 ***6:*** 버전 ***7.2.0*** 기능

기능	설명
Threat Defense 업그레이드	

기능	설명
디바이스 간에 업그레이드 패키지("peer-to-peer sync")를 복사합니다.	management center 또는 내부 웹 서버에서 각 디바이스로 업그레이드 패키지를 복사하는 대신 threat defense CLI를 사용하여 디바이스 간에 업그레이드 패키지를 복사할 수 있습니다("피어 간 동기화"). 이 안전하고 신뢰할 수 있는 리소스 공유는 관리 네트워크를 통해 이루어지지만 management center에 의존하지 않습니다. 각 디바이스는 5개의 패키지 동시 전송을 수용할 수 있습니다. 이 기능은 동일한 독립형 management center에서 관리하는 버전 7.2 이상의 독립형 디바이스에서 지원됩니다. 다음에 대해서는 지원되지 않습니다. • 컨테이너 인스턴스. • 디바이스 고가용성 쌍 및 클러스터. 이러한 디바이스는 일반 동기화 프로세스의 일부로 서로 패키지를 가져옵니다. 업그레이드 패키지를 한 그룹 멤버에 복사하면 모든 그룹 멤버에 자동으로 동기화됩니다. • 고가용성 management center에서 관리하는 디바이스. • 클라우드 사용 Firewall Management Center에서 관리하지만, 분석 모드에서 온프레미스 management center에 추가된 디바이스. • 서로 다른 도메인에 있는 디바이스 또는 NAT 게이트웨이로 분리된 디바이스. • management center 버전에 관계없이 버전 7.1 이하에서 업그레이드하는 디바이스 신규/수정된 CLI 명령: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
위협 방어 업그레이드가 완료되면 Snort 3으로 자동 업그레이드됩니다.	버전 7.2 이상 관리 센터를 사용하여 위협 방어를 업그레이드하는 경우 이제 **Snort 2**를 **Snort 3**으로 업그레이드할지 여부를 선택할 수 있습니다. 소프트웨어 업그레이드 후에는 설정을 구축할 때 적격 디바이스가 Snort 2에서 Snort 3으로 업그레이드됩니다. 맞춤형 침입 또는 네트워크 분석 정책 사용으로 인한 부적격 디바이스의 경우, 향상된 탐지 및 성능을 위해 Snort 3으로 수동 업그레이드하는 것이 좋습니다. 마이그레이션 지원은 버전에 맞는 Cisco Secure Firewall Management Center Snort 3 구성 가이드의 내용을 참조하십시오. 이 옵션은 버전 7.2 이상에 대한 주요 및 유지 관리 Threat Defense 업그레이드에 지원됩니다. 버전 7.0 또는 7.1로의 위협 방어 업그레이드 또는 모든 버전의 패치에는 지원되지 않습니다.

기능	설명
단일 노드 클러스터를 업그레이드합니다.	이제 디바이스 업그레이드 페이지(디바이스 > 디바이스 업그레이드)를 사용하여 활성 노드가 하나뿐인 클러스터를 업그레이드할 수 있습니다. 비활성화된 노드도 업그레이드됩니다. 이전에는 이러한 유형의 업그레이드가 실패했습니다. 이 기능은 시스템 업데이트 페이지(시스템 (⚙)**Updates(**업데이트**)**)에서 지원되지 않습니다. 이 경우 무중단 업그레이드도 지원되지 않습니다. 트래픽 흐름 및 검사 중단은 독립형 디바이스와 마찬가지로 단독 액티브 유닛의 인터페이스 구성에 따라 달라집니다. 지원되는 플랫폼: Firepower 4100/9300, Secure Firewall 3100
CLI에서 위협 방어 업그레이드를 되돌립니다.	이제 관리 센터와 디바이스 간의 통신이 중단되는 경우 디바이스 CLI에서 위협 방어 업그레이드를 되돌릴 수 있습니다. 고가용성/확장성 구축에서는 모든 유닛이 동시에 복귀될 때 복귀가 더 성공적입니다. CLI를 사용하여 되돌릴 때는 모든 유닛에서 세션을 열고 각 유닛에서 되돌리기가 가능한지 확인한 다음 프로세스를 동시에 시작합니다. 주의 CLI에서 되돌리면 업그레이드 후 변경한 내용에 따라 디바이스와 관리 센터 간의 구성이 동기화되지 않을 수 있습니다. 이로 인해 추가 통신 및 구축 문제가 발생할 수 있습니다. 신규/수정된 CLI 명령: **upgrade revert**, **show upgrade revert-info**.
Management Center 업그레이드	
Management Center 업그레이드가 문제 해결 파일을 자동으로 생성하지 않습니다.	시간과 디스크 공간을 절약하기 위해 업그레이드가 시작되기 전에 관리 센터 업그레이드 프로세스에서 더 이상 문제 해결 파일을 자동으로 생성하지 않습니다. 디바이스 업그레이드는 영향을 받지 않으며 계속해서 문제 해결 파일을 생성합니다. 관리 센터에 대한 문제 해결 파일을 수동으로 생성하려면 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택하고 왼쪽 패널에서 **Firewall Management Center**를 클릭한 다음 **View System & Troubleshoot Details(**시스템 및 문제 해결 세부 정보 보기**)**, **Generate Troubleshooting Files(**문제 해결 파일 생성**)**를 클릭합니다.
콘텐츠 업데이트	

기능	설명
GeoDB는 두 개의 패키지로 나뉩니다.	버전 7.2 릴리스 직전인 2022년 5월에 GeoDB를 두 개의 패키지로 분할했습니다. IP 주소를 국가/대륙에 매핑하는 국가 코드 패키지와 라우팅 가능한 IP 주소와 관련된 추가 상황 데이터를 포함하는 IP 패키지입니다. IP 패키지의 상황 데이터에는 추가 위치 세부 정보는 물론 ISP, 연결 유형, 프록시 유형, 도메인 이름 등의 연결 정보가 포함될 수 있습니다. 버전 7.2 이상 관리 센터에서 인터넷에 액세스할 수 있고 반복 업데이트를 활성화하거나 Cisco 지원 및 다운로드 사이트에서 일회성 업데이트를 수동으로 시작하는 경우, 시스템은 자동으로 두 패키지를 모두 얻어 가져옵니다. 그러나 업데이트를 수동으로 다운로드하는 경우(예: 에어 갭(air-gapped) 구축의 경우) 두 GeoDB 패키지를 모두 가져와야 합니다. • 국가 코드 패키지: Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP 패키지: Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar Geolocation Updates(시스템 (⚙)**> Updates(**업데이트**) > Geolocation Updates(**지리위치 업데이트**)**) 페이지 및 About(정보) 페이지(**Help(**도움말**) > About(**정보**)**)에는 시스템에서 현재 사용 중인 패키지의 버전이 나열됩니다.

표 ***7:*** 버전 ***7.1.0*** 기능

기능	설명
제품 업그레이드	
성공한 디바이스 업그레이드 되돌리기	이제 주요 및 유지 보수 업그레이드를 FTD로 되돌릴 수 있습니다. 되돌리면 소프트웨어가 마지막 업그레이드 직전의 상태로 돌아갑니다(스냅샷이라고도 함). 패치를 설치한 후 업그레이드를 되돌리면 패치는 물론 주요 업그레이드 및/또는 유지 보수 업그레이드도 되돌립니다. 중요 되돌릴 필요가 있다고 생각되면 .시스템 (⚙) > **Updates(**업데이트**)**를 사용하여 FTD를 업그레이드해야 합니다. System Updates(시스템 업데이트) 페이지에서는 업그레이드를 시작할 때 되돌리기 스냅샷을 저장하도록 시스템을 구성하는 **Enable revert after successful upgrade(**업그레이드 후 되돌리기 활성화**)** 옵션을 활성화할 수 있는 유일한 곳입니다. 이는 **Devices(**디바이스**) > Device Upgrade(**디바이스 업그레이드**)** 페이지에서 마법사를 사용하는 일반적인 권장 사항과 다릅니다. 이 기능은 컨테이너 인스턴스에는 지원되지 않습니다. 최소 FTD: 7.1 최소 Threat Defense: 7.1

기능	설명
클러스터링된 디바이스 및 고가용성 디바이스에 대한 업그레이드 워크플로우가 개선되었습니다.	클러스터링된 디바이스 및 고가용성 디바이스에 대한 업그레이드 워크플로우가 다음과 같이 개선되었습니다. • 이제 업그레이드 마법사에서 클러스터링된 고가용성 유닛을 개별 디바이스가 아닌 그룹으로 올바르게 표시합니다. 시스템은 사용자에게 발생할 수 있는 그룹 관련 문제를 식별하고, 보고하고, 사전에 수정을 요구할 수 있습니다. 예를 들어 Firepower Chassis Manager에서 동기화되지 않은 변경 사항을 적용한 경우 Firepower 4100/9300에서 클러스터를 업그레이드할 수 없습니다. • 업그레이드 패키지를 클러스터 및 고가용성 쌍으로 복사하는 속도와 효율성을 개선했습니다. 이전에는 FMC에서 패키지를 각 그룹 멤버에 순차적으로 복사했습니다. 이제 그룹 멤버는 일반 동기화 프로세스의 일부로 서로 패키지를 가져올 수 있습니다. • 이제 클러스터에서 데이터 유닛의 업그레이드 순서를 지정할 수 있습니다. 제어 유닛은 항상 마지막에 업그레이드됩니다.

표 ***8:*** 버전 ***7.0.0*** 기능

기능	설명
제품 업그레이드	
FTD 업그레이드 성능 및 상태 보고 기능이 개선되었습니다.	이제 FTD 업그레이드가 더 쉽고 빠르고 안정적이며 디스크 공간을 덜 차지합니다. 메시지 센터의 새로운 **Upgrades(**업그레이드**)** 탭은 업그레이드 상태 및 오류 보고에 대한 추가 개선 사항을 제공합니다.

기능	설명
FTD 디바이스를 위한 따르기 쉬운 업그레이드 워크플로우.	FMC의 새 디바이스 업그레이드 페이지(**Devices(**디바이스**) > Device Upgrade(**디바이스 업그레이드**)**)에서는 버전 6.4 이상 FTD 디바이스를 업그레이드하기 위한 따라하기 쉬운 마법사를 제공합니다. 업그레이드할 디바이스 선택, 디바이스에 업그레이드 패키지 복사, 호환성 및 준비 확인 등 중요한 업그레이드 전 단계를 안내합니다. 시작하려면 Device Management(디바이스 관리) 페이지(**Devices(**디바이스**) > Device Management(**디바이스 관리**) > Select Action(**작업 선택**)**)에서 새로운 **Upgrade Firepower Software(Firepower** 소프트웨어 업그레이드**)** 작업을 사용합니다. 계속 진행하면 선택한 디바이스에 대한 기본 정보와 현재 업그레이드 관련 상태가 표시됩니다. 여기에는 업그레이드할 수 없는 모든 이유가 포함됩니다. 디바이스가 마법사의 단계를 "통과"하지 않으면 다음 단계에 표시되지 않습니다. 마법사에서 빠져나가도 진행 상황은 유지되지만 관리자 액세스 권한이 있는 다른 사용자는 마법사를 재설정, 수정 또는 계속할 수 있습니다. 참고 FTD 업그레이드 패키지의 위치를 업로드하거나 지정하려면 여전히 시스템 (⚙) > **Updates(**업데이트**)**를 사용해야 합니다. FMC 자체는 물론 모든 비 FTD 매니지드 디바이스를 업그레이드하려면 System Updates(시스템 업데이트) 페이지를 사용해야 합니다. 참고 버전 7.0에서는 마법사가 클러스터 또는 고가용성 쌍의 디바이스를 올바르게 표시하지 않습니다. 이러한 디바이스를 하나의 유닛으로 선택하고 업그레이드해야 하지만 마법사에서는 이러한 디바이스를 독립형 디바이스로 표시합니다. 디바이스 상태 및 업그레이드 준비 상태는 개별적으로 평가 및 보고됩니다. 즉, 한 유닛은 다음 단계로 "전달"되는 것으로 표시되지만 다른 유닛은 그렇지 않을 수 있습니다. 그러나 이러한 디바이스는 여전히 그룹화됩니다. 하나에서 준비 확인을 실행하면 모두에서 실행됩니다. 하나에서 업그레이드를 시작하면 모두에서 시작됩니다. 시간이 오래 걸리는 업그레이드 실패를 방지하려면 **Next(**다음**)**를 클릭하기 전에 모든 그룹 멤버가 마법사의 다음 단계로 이동할 준비가 되었는지 수동으로 확인합니다.

기능	설명
한 번에 더 많은 FTD 디바이스를 업그레이드합니다.	FTD 업그레이드 마법사는 다음 제한을 해제합니다. • 동시 디바이스 업그레이드. 한 번에 업그레이드할 수 있는 디바이스의 수가 이제 동시 업그레이드를 관리하는 시스템의 기능이 아니라 관리 네트워크 대역폭에 의해 제한됩니다. 이전에는 한 번에 5개 이상의 디바이스를 업그레이드하지 않는 것을 권장했습니다. 중요 FTD 버전 6.7 이상으로 업그레이드하는 경우에만 이 개선 사항이 표시됩니다. 디바이스를 이전 FTD 릴리스로 업그레이드하는 경우(새 업그레이드 마법사를 사용하는 경우에도) 한 번에 5개의 디바이스로 제한하는 것이 좋습니다. • 디바이스 모델별 업그레이드 그룹화 이제 시스템이 적절한 업그레이드 패키지에 액세스할 수 있는 한 모든 FTD 모델을 동시에 대기열에 넣고 업그레이드를 호출할 수 있습니다. 이전에는 업그레이드 패키지를 선택한 다음 해당 패키지를 사용하여 업그레이드할 디바이스를 선택했습니다. 즉, 업그레이드 패키지를 공유하는 경우에만 여러 디바이스를 동시에 업그레이드할 수 있었습니다. 예를 들어 Firepower 2100 Series 디바이스 2개를 동시에 업그레이드할 수 있지만 Firepower 2100 Series와 Firepower 1000 Series는 업그레이드할 수 없었습니다.

표 ***9:*** 버전 ***6.7.0*** 기능

기능	설명
제품 업그레이드	

기능	설명
FTD 업그레이드 상태 보고 및 취소/재시도 옵션이 개선되었습니다.	이제 Device Management(디바이스 관리) 페이지에서 진행 중인 FTD 디바이스 업그레이드 및 준비도 확인 상태와 7일간의 업그레이드 성공/실패 기록을 볼 수 있습니다. 메시지 센터는 향상된 상태 및 오류 메시지도 제공합니다. 클릭 한 번으로 디바이스 관리 및 메시지 센터에서 액세스할 수 있는 새로운 Upgrade Status(업그레이드 상태) 팝업에 남은 비율/시간, 특정 업그레이드 단계, 성공/실패 데이터, 업그레이드 로그 등의 자세한 업그레이드 정보가 표시됩니다. 또한 이 팝업에서 실패 또는 진행 중인 업그레이드를 수동으로 취소하거나(**Cancel Upgrade(**업그레이드 취소**)**) 실패한 업그레이드를 재시도 할 수 있습니다(**Retry Upgrade(**업그레이드 재시도**)**). 업그레이드를 취소하면 디바이스가 업그레이드 전 상태로 돌아갑니다. 참고 수동으로 취소하거나 실패한 업그레이드를 재시도하려면 FMC를 사용하여 FTD 디바이스를 업그레이드할 때 나타나는 새로운 자동 취소 옵션을 비활성화해야 합니다. **Automatically cancel on upgrade failure and roll back to the previous version(**업그레이드 실패 시 자동으로 취소하고 이전 버전으로 롤백합니다**)**. 이 옵션을 활성화하면 업그레이드 실패시 디바이스가 자동으로 업그레이드 전 상태로 돌아갑니다. 패치에 대해서는 자동 취소가 지원되지 않습니다. HA 또는 클러스터형 구축에서는 자동 취소가 각 디바이스에 개별적으로 적용됩니다. 즉, 한 디바이스에서 업그레이드에 실패하면 해당 디바이스만 복귀됩니다. 신규/수정된 화면: • FTD 업그레이드 패키지의 시스템 (⚙) > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)** > **Available Updates(**사용 가능한 업데이트**)** > **Install(**설치**)** 아이콘 • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Upgrade(**업그레이드**)** • **Message Center(**메시지 센터**) > Tasks(**작업**)** 신규/수정된 CLI 명령: **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**
업그레이드는 디스크 공간을 절약하기 위해 PCAP 파일 제거.	업그레이드시 이제 로컬에 저장된 PCAP 파일이 제거됩니다. 업그레이드하려면 사용 가능한 디스크 공간이 충분해야 합니다. 그렇지 않으면 업그레이드에 실패합니다.
콘텐츠 업데이트	

기능	설명
사용자 정의 침입 규칙 가져오기에서 규칙 충돌 경고	FMC에서는 이제 사용자 지정(로컬) 침입 규칙을 가져올 때 규칙 충돌을 경고합니다. 이전에는 충돌이 발생한 규칙 가져오기가 완전히 실패하는 버전 6.6.0.1을 제외하고 시스템은 충돌을 일으키는 규칙을 자동으로 건너 뛰었습니다. Rule Updates(규칙 업데이트) 페이지에서 규칙 가져오기에 충돌이 발생한 경우 Status(상태) 열에 경고 아이콘이 표시됩니다. 자세한 내용을 보려면 경고 아이콘 위에 포인터를 올려 놓고 툴팁을 확인하십시오. 기존 규칙과 동일한 SID/수정 번호를 가진 침입 규칙을 가져오려고 할 때 충돌이 발생합니다. 항상 업데이트된 버전의 사용자 지정 규칙에 새 수정 번호가 포함되어 있는지 확인해야 합니다. 신규/수정된 화면: 시스템 (⚙) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**에 경고 아이콘이 추가되었습니다

표 ***10:*** 버전 ***6.6.0*** 기능

기능	설명
제품 업그레이드	
내부 웹 서버에서 FTD 업그레이드 패키지를 가져옵니다.	이제 FTD 디바이스가 FMC가 아닌 자체 내부 웹 서버에서 업그레이드 패키지를 가져올 수 있습니다. 이는 FMC와 해당 디바이스 간의 대역폭이 제한된 경우 특히 유용합니다. 또한 FMC의 공간을 절약합니다. 참고 이 기능은 버전 6.6 이상을 실행하는 FTD 디바이스에서만 지원됩니다. 버전 6.6으로의 업그레이드에는 지원되지 않으며, FMC 또는 클래식 디바이스에서는 지원되지 않습니다. 신규/수정된 화면: 업그레이드 패키지를 업로드하는 페이지에 **Specify software update source(**소프트웨어 업데이트 소스 지정**)** 옵션이 추가되었습니다.
콘텐츠 업데이트	
초기 설정 중 자동 VDB 업데이트	새 이미지 또는 재이미징된 FMC를 설정하면 시스템이 자동으로 VDB(취약점 데이터베이스) 업데이트를 시도합니다. 이 작업은 한 번만 수행하면 됩니다. FMC에서 인터넷에 액세스할 수 있는 경우 자동 반복 VDB 업데이트 다운로드 및 설치를 수행하도록 작업을 예약하는 것이 좋습니다.

표 ***11:*** 버전 ***6.5.0*** 기능

기능	설명
콘텐츠 업데이트	

기능	설명
자동 소프트웨어 다운로드 및 GeoDB 업데이트.	새 이미지 또는 재이미징된 FMC를 설정하면 시스템에서 다음 일정을 자동으로 예약합니다. • FMC 및 매니지드 디바이스의 소프트웨어 업데이트를 다운로드하는 주간 작업. • GeoDB 주간 업데이트 이런 작업은 UTC 기준으로 예약되므로, 사용자가 있는 위치와 날짜에 따라 지역적으로 실행됩니다. 또한 작업은 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받을 경우 예약된 작업은 현지 시간에 따라 여름에는 겨울보다 1시간 '늦게' 실행됩니다. 자동 예약 구성을 검토하고 필요한 경우 조정할 것을 강력하게 권장합니다.

표 ***12:*** 버전 ***6.4.0*** 기능

기능	설명
업그레이드가 예약된 작업을 연기합니다.	management center업그레이드 프로세스가 이제 예약된 작업을 연기합니다. 업그레이드 중에 시작하도록 예약된 모든 작업은 업그레이드 후 재부팅하고 5분 후에 시작됩니다. 참고 업그레이드를 시작하기 전에 실행 중인 작업이 완료되었는지 확인해야 합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 이 기능은 지원되는 버전에서 모든 업그레이드를 지원합니다. 여기에는 버전 6.4.0.10 이상 패치, 버전 6.6.3 이상 유지 보수 릴리스, 버전 6.7.0 이상이 포함됩니다. 이 기능은 지원되지 않는 버전에서 지원되는 버전으로 업그레이드 할 때는 지원되지 않습니다.
콘텐츠 업데이트	

기능	설명
서명된 SRU, VDB 및 GeoDB 업데이트	따라서 시스템에서는 올바른 업데이트 파일을 사용하고 있는지 확인할 수 있습니다. 버전 6.4 이상에서는 SRU(침입 규칙), VDB(취약점 데이터베이스) 및 GeoDB(지리위치 데이터베이스)에 서명된 업데이트를 사용합니다. 이전 버전은 서명되지 않은 패키지를 계속 사용합니다. Cisco 지원 및 다운로드 사이트에서 업데이트를 수동으로 다운로드하지 않는 한 (예: 무선 연결 구축) 기능에 차이가 있어서는 안 됩니다. 그러나 SRU, VDB 및 GeoDB 업데이트를 수동으로 다운로드하여 설치하는 경우 현재 버전에 맞는 패키지를 다운로드해야 합니다. 서명된 업데이트 파일은 다음과 같이 'Sourcefire' 대신 'Cisco'로 시작하고 .sh 대신 .sh.REL.tar로 끝납니다. • SRU: Cisco_Firepower_SRU-날짜-빌드-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-버전.sh.REL.tar • GeoDB: Cisco_GEODB_Update-날짜-빌드.sh.REL.tar 서명되지 않은 업데이트가 필요한 버전의 경우 지원이 종료될 때까지 서명된 업데이트와 서명되지 않은 업데이트가 모두 제공됩니다. 서명된(.tar) 패키지의 압축을 풀지 마십시오. 서명된 업데이트를 이전의 FMC 또는 ASA FirePOWER 디바이스에 실수로 업로드한 경우에는 수동으로 삭제해야 합니다. 패키지를 그대로 두면 디스크 공간을 차지하여 향후 업그레이드에 문제가 발생할 수 있습니다.

표 ***13:*** 버전 ***6.2.3*** 기능

기능	설명
제품 업그레이드	
업그레이드 전에 관리되는 디바이스에 업그레이드 패키지 복사	이제 실제 업그레이드를 실행하기 전에 FMC에서 업그레이드 패키지를 매니지드 디바이스로 복사 또는 푸시할 수 있습니다. 이는 업그레이드 유지 보수 기간이 아닌 낮은 대역폭 사용 시간 동안 푸시할 수 있으므로 유용합니다. 고가용성, 클러스터형 또는 스택형 디바이스로 푸시할 경우, 시스템은 먼저 업그레이드 패키지를 액티브/컨트롤/기본에 전송한 다음 스탠바이/데이터/보조에 전송합니다. 신규/수정된 화면: 시스템 (⚙) > **Updates(**업데이트**)**
콘텐츠 업데이트	

기능	설명
FMC에서 VDB 업데이트 전에 Snort 재시작을 경고합니다.	이제 FMC에서 VDB(Vulnerability Database) 업데이트 시 Snort 프로세스가 재시작된다는 경고가 표시됩니다. 이렇게 하면 트래픽 검사가 중단되며, 매니지드 디바이스가 트래픽을 처리하는 방식에 따라 트래픽 흐름이 중단될 수 있습니다. 유지 보수 기간과 같이 편리한 시간까지 설치를 취소할 수 있습니다. 다음과 같은 경고가 표시될 수 있습니다. • VDB를 다운로드하고 수동으로 설치한 후 • VDB를 설치하기 위해 예약된 작업을 생성할 때 • 이전에 예약 된 작업이나 소프트웨어 업그레이드의 일부로 VDB가 백그라운드에서 설치되는 경우