ISE/ISE-PIC를 사용하여 사용자 제어

다음 주제는 ISE/ISE-PIC를 이용해 사용자 인식 및 사용자 제어를 수행하는 방법을 설명합니다.

ISE/ISE-PIC ID 소스

패시브 인증에 ISE/ISE-PIC를 사용하기 위해 Cisco Identity Services Engine(ISE) 또는 ISE Passive Identity Connector(ISE-PIC) 구축을 Firepower System에 통합할 수 있습니다.

ISE/ISE-PIC은 신뢰할 수 있는 ID 소스로서 액티브 디렉터리(AD), LDAP, RADIUS, RSA로 인증하는 사용자에 대한 사용자 인식 데이터를 제공합니다. 또한 액티브 디렉터리 사용자에 대한 사용자 제어를 수행할 수 있습니다. ISE/ISE-PIC에서는 실패한 로그인 시도 또는 ISE 게스트 서비스 사용자의 활동을 보고하지 않습니다.

참고

Firepower 시스템은 IEEE 802.1x 머신 인증을 구문 분석하지 않지만, 802.1x 사용자 인증은 구문 분석합니다. ISE에서 802.1x를 사용한다면 사용자 인증을 포함해야 합니다. 802.1x 머신 인증은 정책에서 사용할 수 있는 사용자 ID를 FMC에 제공하지 않습니다.

Cisco ISE/ISE-PIC에 대한 자세한 정보는 *Cisco Identity Services Engine* 관리자 설명서와 *Identity Services Engine Passive Identity Connector(ISE-PIC)* 설치 및 관리자 가이드을 참조하십시오.

참고 최신 기능 집합과 가장 많은 수의 문제를 해결하려면 최신 버전의 ISE/ISE-PIC를 사용하는 것이 좋습니다.

대상 SGT(Security Group Tag) 매칭

ISE를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 SGT(Security Group Tag)를 정의하고 사용하는 경우, SGT를 소스 및 대상 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 이렇게 하면 보안 그룹 멤버십에 따른 액세스를 IP 주소가 아니라 네트워크 개체를 기준으로 차단 또는 허용할 수 있습니다.

SGT 태그 매칭은 다음과 같은 이점을 제공합니다.

- FMC는 ISE에서 SXP(Security Group Tag eXchange Protocol) 매핑을 구독할 수 있습니다.

  ISE는 SXP를 사용하여 IP-to-SGT 매핑 데이터베이스를 매니지드 디바이스에 전파합니다. ISE 서버를 사용하도록 FMC를 구성한다면, ISE에서 SXP 항목을 수신 대기하려면 옵션을 활성화합니다. 이로 인해 FMC는 ISE에서 직접 보안 그룹 태그 및 매핑에 대해 학습합니다. 그런 다음 FMC는 매니지드 디바이스에 SGT 및 매핑을 게시합니다.

  SXP 주제는 ISE 및 기타 SXP 준수 디바이스(예: 스위치) 간의 SXP 프로토콜을 통해 학습한 정적 및 동적 매핑에 따라 보안 그룹 태그를 수신합니다.

  ISE에서 보안 그룹 태그를 생성하고 각 태그에 호스트 또는 네트워크 IP 주소를 할당할 수 있습니다. 또한 사용자 어카운트에 SGT를 할당할 수 있으며, SGT는 사용자의 트래픽에 할당됩니다. 네트워크의 스위치와 라우터가 이 작업을 수행하도록 구성된 경우, 이러한 태그는 ISE, Cisco TrustSec 클라우드로 제어되는 네트워크에 진입할 때 패킷에 할당됩니다.

  ISE-PIC는 SXP를 지원하지 않습니다.

- FMC 및 매니지드 FTD 디바이스는 추가 정책을 구축 없이 SGT 매핑을 학습할 수 있습니다. (즉 액세스 제어 정책을 구축하지 않고도 SGT 매핑에 대한 연결 이벤트를 볼 수 있습니다.)

- 네트워크를 분할해 중요한 비즈니스 자산을 보호하는 Cisco TrustSec를 지원합니다.

- SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가할 때, 매니지드 디바이스는 다음 우선순위를 사용합니다.

  1. 패킷에 정의된 소스 SGT 태그(있는 경우).

     SGT 태그를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.

     SGT 태그를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.

  2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. SGT는 소스 또는 대상과 일치할 수 있습니다.

3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있다면, 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.

예:

- ISE에서 Guest Users(게스트 사용자)라는 이름의 SGT 태그를 생성하고 192.0.2.0/24 네트워크에 연결합니다.

  예를 들어 액세스 제어 규칙에서 Guest Users(게스트 사용자)를 소스 SGT 조건으로 사용하고, 네트워크에 액세스하는 사람이 특정 URL, 웹 사이트 범주 또는 네트워크만 액세스하도록 제한할 수 있습니다.

- ISE에서 Restricted Networks(제한된 네트워크)라는 이름의 SGT 태그를 생성하고 198.51.100.0/8 네트워크에 연결합니다.

  예를 들어 Restricted Networks(제한된 네트워크)를 대상 SGT 규칙 조건으로 사용하고, Guest Users(게스트 사용자)와 네트워크 액세스 자격이 없는 사용자가 있는 네트워크에서의 액세스를 차단할 수 있습니다.

관련 항목

ISE/ISE-PIC 지침 및 제한 사항, 4 페이지

ISE/ISE-PIC의 라이선스 요구 사항

FTD 라이센스

Any(모든 상태)

기본 라이선스

제어

ISE/ISE-PIC 요구 사항 및 사전 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

- 관리자

- 액세스 관리자
- Network Admin(네트워크 관리자)

ISE/ISE-PIC 지침 및 제한 사항

Firepower System으로 ISE/ISE-PIC를 구성하는 경우에는 이 섹션에서 설명하는 지침을 사용하십시오.

ISE/ISE-PIC 버전 및 설정 호환성

ISE/ISE-PIC 버전과 설정은 다음과 같이 Firepower와의 통합 및 상호작용에 영향을 줍니다.

- 최신 기능 집합을 사용하려면 최신 버전의 ISE/ISE-PIC를 사용하는 것이 좋습니다.
- ISE/ISE-PIC 서버와 Firepower Management Center의 시간을 동기화합니다. 그렇지 않으면 시스템이 예기치 않은 간격으로 사용자 시간 제한을 수행할 수 있습니다.
- ISE 또는 ISE-PIC 데이터를 사용하여 사용자 제어를 구현하려면, 영역 생성에서 설명하는 것처럼 pxGrid 페르소나를 가정하는 ISE 서버의 영역을 설정하고 활성화합니다.
- ISE 서버에 연결되는 각 Firepower Management Center 호스트 이름은 고유해야 합니다. 그렇지 않으면 단일 Firepower Management Center에 대한 연결이 중단됩니다.
- 많은 사용자 그룹을 모니터링하도록 ISE/ISE-PIC를 설정하는 경우 시스템은 매니지드 디바이스 메모리 제한으로 인해 그룹을 기준으로 사용자 매핑을 삭제할 수 있습니다. 그 결과, 영역이 있는 규칙 또는 사용자 조건이 정상적으로 수행되지 않을 수 있습니다.

  FTD v6.7 이상을 실행하는 디바이스의 경우, 선택적으로 **configure identity-subnet-filter** 명령을 사용하여 매니지드 디바이스가 모니터링하는 서브넷을 제한할 수 있습니다. 자세한 내용은 *Firepower Threat Defense* 명령 참조에 나와 있습니다.

이 시스템 버전과 호환되는 특정 ISE/ISE-PIC 버전에 대한 자세한 내용은 *Cisco Firepower* 호환성 가이드를 참고하십시오.

ISE에서 클라이언트 승인

ISE 서버와 Firepower Management Center 디바이스 간의 연결에 성공하려면 ISE에서 클라이언트를 수동으로 승인해야 합니다. (일반적으로 클라이언트 두 개가 존재합니다. 하나는 연결 테스트용이며, 다른 하나는 ISE 에이전트용입니다.)

또한 *Cisco Identity Services Engine* 관리자 가이드의 사용자 및 외부 ID 소스 관리 장에서 설명하는 것처럼 ISE에서 **Automatically approve new accounts(**새 어카운트 자동 승인**)**를 활성화할 수도 있습니다.

SGT(Security Group Tag)

보안 그룹 태그(SGT)는 신뢰할 수 있는 네트워크 내의 트래픽 소스 권한을 지정합니다. Cisco ISE 및 Cisco TrustSec에서는 SGA(Security Group Access)라는 기능을 사용하여 네트워크로 들어오는 패킷에 SGT 속성을 적용합니다. 이러한 SGT는 ISE 또는 TrustSec 내에서 사용자가 할당한 보안 그룹에 해당합니다. ISE를 ID 소스로 구성하는 경우 Firepower System은 이러한 SGT를 사용하여 트래픽을 필터링할 수 있습니다.

보안 그룹 태그는 액세스 제어 규칙에서 소스 및 대상 일치 기준으로 사용할 수 있습니다.

소스 SGT 태그 외에 대상 SGT 태그도 매칭할 때는, 다음 사항이 적용됩니다.

필수 ISE 버전: 2.6 패치 6 이상, 2.7 패치 2 이상

라우터 지원: 이더넷을 통한 SGT 인라인 태깅을 지원하는 모든 Cisco 라우터 자세한 내용은 Cisco Group Based Policy Platform and Capability Matrix Release(Cisco Group 기반 정책 플랫폼 및 기능 매트릭스 릴리스) 등의 참조 자료에서 확인하십시오.

제한 사항:

- QoS(Quality Service) 정책은 소스 SGT 매칭만 사용합니다. 대상 SGT 매칭은 사용하지 않습니다.
- RA-VPN은 RADIUS에서 바로 SGT 매핑을 수신하지 않습니다.

FMC가 FirePOWER Services 디바이스를 이용해 ASA를 관리한다면, SXP 구독은 캡티브 포털 ID 규칙을 디바이스에 구축했을 때만 작동합니다.

ISE 및 고가용성

기본 Firepower Management Center가 실패하는 경우에는 다음이 발생합니다.

- 대기 상태가 기본으로 승격하지 않은 한, 보조 Firepower Management Center의 사용자 데이터베이스는 읽기 전용입니다.

  저장소(예: Active Directory)에 추가된 사용자는 Firepower Management Center에 다운로드되지 않으며 이러한 사용자는 Unknown(알 수 없음)으로 식별됩니다.

  새 SGT는 사용되지 않습니다.

- 대기 상태가 기본으로 승격되면, 모든 작업자는 다시 정상 상태가 됩니다. 즉 사용자가 다운로드되고, 새 SGT를 사용하며, 사용자는 가능한 경우 식별됩니다.

ISE 기본 서버가 실패한다면, 사용자는 보조를 기본으로 직접 승격해야 합니다. 자동 페일오버는 실행되지 않습니다.

엔드포인트 위치**(**또는 위치 **IP)**

엔드포인트 위치 속성은 ISE에서 식별된 사용자를 인증하기 위해 ISE를 사용한 네트워크 디바이스의 IP 주소입니다.

ISE 속성

ISE 연결을 구성하면 Firepower Management Center 데이터베이스에 ISE 속성 데이터가 입력됩니다. 사용자 인식 및 사용자 제어에 다음과 같은 ISE 속성을 사용할 수 있습니다. ISE-PIC에서는 이러한 작업이 지원되지 않습니다.

엔드포인트 프로파일**(**또는 디바이스 유형**)**

엔드포인트 프로파일 속성은 ISE에서 식별된 사용자의 엔드포인트 디바이스 유형입니다.

사용자 제어에 대한 ISE/ISE-PIC 설정 방법

다음 구성 중 하나에서 ISE/ISE-PIC를 사용할 수 있습니다.

- 영역, ID 정책 및 관련 액세스 제어 정책을 이용합니다.

  영역을 사용하여 정책 내 네트워크 리소스에 대한 사용자 액세스를 제어합니다. 정책에서 ISE/ISE-PIC SGT(Security Group Tags) 메타데이터를 계속 사용할 수 있습니다.

- 액세스 제어 정책만 사용할 수 있습니다. 영역 또는 ID 정책은 필요 없습니다.

  SGT 메타데이터만 사용하여 네트워크 액세스를 제어하려면 이 방법을 사용해야 합니다.

관련 항목

영역을 사용하지 않고 ISE를 구성하는 방법, 6 페이지
영역을 사용해 사용자 제어에 대한 ISE/ISE-PIC를 설정하는 방법, 7 페이지

영역을 사용하지 않고 ISE를 구성하는 방법

이 항목에서는 SGT 태그를 이용해 네트워크 액세스를 허용 또는 차단하도록 ISE를 구성하려면 수행해야 하는 작업을 개략적으로 설명합니다.

프로시저

	명령 또는 동작	목적
단계 1	SGT 매칭: ISE에서 SXP를 활성화합니다.	그러면 SGT 메타데이터 변경 시 FMC가 ISE에서 업데이트를 받게 됩니다.
단계 2	ISE/ISE-PIC에서 시스템 인증서를 내보냅니다.	ISE/ISE-PIC pxGrid, 모니터링(MNT) 서버 및 FMC를 안전하게 연결하려면 인증서가 있어야 합니다. FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 11 페이지의 내용을 참조하십시오.
단계 3	ISE/ISE-PIC ID 소스를 생성합니다.	ISE/ISE-PIC ID 소스를 사용하면 ISE/ISE-PIC가 제공하는 SGT(Security Group Tags)를 사용하여 사용자 활동을 제어할 수 있습니다. 사용자 제어를 위한 ISE/ISE-PIC 설정, 13 페이지의 내용을 참조하십시오.
단계 4	액세스 제어 규칙을 생성합니다.	액세스 제어 규칙은 트래픽이 규칙 기준과 일치할 때 수행할 작업(예: 허용 또는 차단)을 지정합니다. 액세스 제어 규칙에서는 소스 및 대상 SGT 메타데이터를 매칭 기준으로 사용할 수 있습니다. 액세스 제어 규칙 소개의 내용을 참조하십시오.

	명령 또는 동작	목적
단계 5	액세스 제어 정책을 매니지드 디바이스에 구축합니다.	효과를 발휘하려면 정책은 매니지드 디바이스에 구축해야 합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

다음에 수행할 작업

FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 11 페이지

영역을 사용해 사용자 제어에 대한 ISE/ISE-PIC를 설정하는 방법

시작하기 전에

이 항목에서는 사용자 제어를 위해 ISE/ISE-PIC를 구성하고 사용자나 그룹의 네트워크 액세스를 허용 또는 차단하려면 수행해야 하는 작업을 개략적으로 설명합니다. 사용자와 그룹은 영역에 지원되는 서버에 나열된 모든 서버에 저장할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	대상 SGT에만 해당: ISE에서 SXP를 활성화합니다.	그러면 SGT 메타데이터 변경 시 FMC가 ISE에서 업데이트를 받게 됩니다.
단계 2	ISE/ISE-PIC에서 시스템 인증서를 내보냅니다.	ISE/ISE-PIC pxGrid, 모니터링(MNT) 서버 및 FMC를 안전하게 연결하려면 인증서가 있어야 합니다. FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 11 페이지의 내용을 참조하십시오.
단계 3	영역을 생성합니다.	영역 생성의 유일한 목적은 선택한 사용자 및 그룹을 기준으로 네트워크 액세스를 제어하는 것입니다. 영역 생성의 내용을 참조하십시오.
단계 4	사용자 및 그룹을 다운로드하고 영역에서 활성화합니다.	사용자 및 그룹을 다운로드하면 액세스 제어 규칙에서 사용할 수 있습니다. 을 참조하십시오. 사용자 및 그룹 다운로드을 참조하십시오.
단계 5	ISE/ISE-PIC ID 소스를 생성합니다.	ISE/ISE-PIC ID 소스를 사용하면 ISE/ISE-PIC가 제공하는 SGT(Security Group Tags)를 사용하여 사용자 활동을 제어할 수 있습니다. 사용자 제어를 위한 ISE/ISE-PIC 설정, 13 페이지의 내용을 참조하십시오.

	명령 또는 동작	목적
단계 **6**	ID 정책을 생성합니다.	ID 정책은 하나 이상의 ID 규칙에 대한 컨테이너입니다. ID 정책 생성의 내용을 참조하십시오.
단계 **7**	ID 규칙을 생성합니다.	ID 규칙은 영역을 이용해 사용자 및 그룹의 네트워크 액세스를 제어하는 방법을 지정합니다. ID 규칙 생성의 내용을 참조하십시오.
단계 **8**	ID 정책을 액세스 제어 정책과 연결합니다.	이렇게 하면 액세스 제어 정책은 영역에 있는 사용자 및 그룹을 사용할 수 있습니다.
단계 **9**	액세스 제어 규칙을 생성합니다.	액세스 제어 규칙은 트래픽이 규칙 기준과 일치할 때 수행할 작업(예: 허용 또는 차단)을 지정합니다. 액세스 제어 규칙에서는 소스 및 대상 SGT 메타데이터를 매칭 기준으로 사용할 수 있습니다. 액세스 제어 규칙 소개의 내용을 참조하십시오.
단계 **10**	액세스 제어 정책을 매니지드 디바이스에 구축합니다.	효과를 발휘하려면 정책은 매니지드 디바이스에 구축해야 합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

다음에 수행할 작업

FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 11 페이지

ISE/ISE-PIC 구성

다음 항목에서는 FMC에서 ID 정책과 함께 사용하도록 ISE/ISE-PIC 서버를 구성하는 방법을 설명합니다.

ISE/ISE-PIC 서버에서 인증서를 내보내 FMC를 이용해 인증하고 SXP 주제를 게시해야 합니다. 이렇게 해야 ISE 서버에서 업데이트된 SGT(Security Group Tags)를 사용하여 FMC를 업데이트할 수 있습니다.

관련 항목

FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 11 페이지
ISE에서 보안 그룹 및 SXP 게시 구성, 8 페이지

ISE에서 보안 그룹 및 SXP 게시 구성

TrustSec 정책 및 SGT(Security Group Tag)를 생성하려면 Cisco ISE(Identity Services Engine)에서 수행해야 할 구성이 많이 있습니다. TrustSec을 구현하는 방법에 대한 더 자세한 내용은 ISE 설명서를 참조하십시오.

다음 절차에서는 ISE에서 FTD 디바이스에 대해 구성해야 하는 핵심 설정의 중요 사항을 골라서 설명하므로 이를 따라 정적 SGT-IP 주소 매핑을 다운로드하고 적용할 수 있습니다. 그러면 이 매핑을 액세스 제어 규칙에서 소스 및 대상 SGT 일치에 사용할 수 있습니다. 자세한 내용은 ISE 설명서를 참조하십시오.

이 절차의 스크린 샷은 ISE 2.4를 기준으로 합니다. 이러한 기능에 대한 정확한 경로는 이후 릴리스에서 변경될 수 있지만 개념 및 요구 사항은 동일합니다. ISE 2.4 이상 및 2.6 이상 버전이 권장되더라도 구성은 ISE 2.2 패치 1부터 작동해야 합니다.

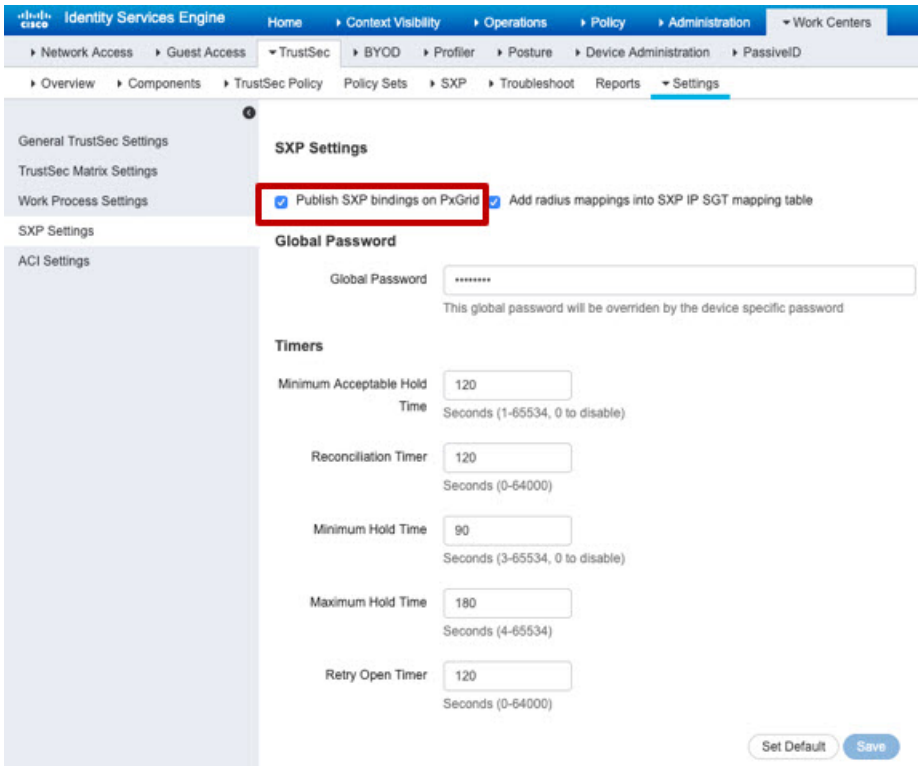
시작하기 전에

SGT-IP 주소 정적 매핑을 게시하고, 사용자 세션-SGT 매핑을 가져와 FTD 디바이스가 이를 수신할 수 있도록 하려면 ISE Plus 라이선스가 있어야 합니다.

프로시저

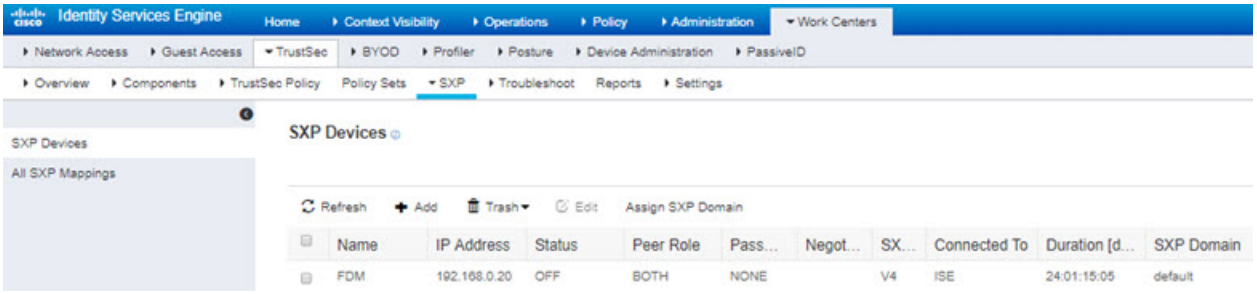
단계 **1** **Work Center(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **SXP Settings(SXP** 설정**)**를 선택하고 **Publish SXP Bindings on PxGrid(PxGrid**에서 **SXP** 바인딩 게시**)** 옵션을 선택합니다.

이 옵션을 선택하면 ISE에서 SXP를 사용하여 SGT 매핑을 전송합니다. FTD 디바이스에서 SXP 항목에 대한 목록의 내용을 "수신 대기"하도록 설정하려면 이 옵션을 선택해야 합니다. 정적 SGT-IP 주소 매핑에 대한 정보를 가져오려면 FTD 디바이스에 대해 이 옵션을 선택해야 합니다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 옵션이 필수 사항이 아닙니다.

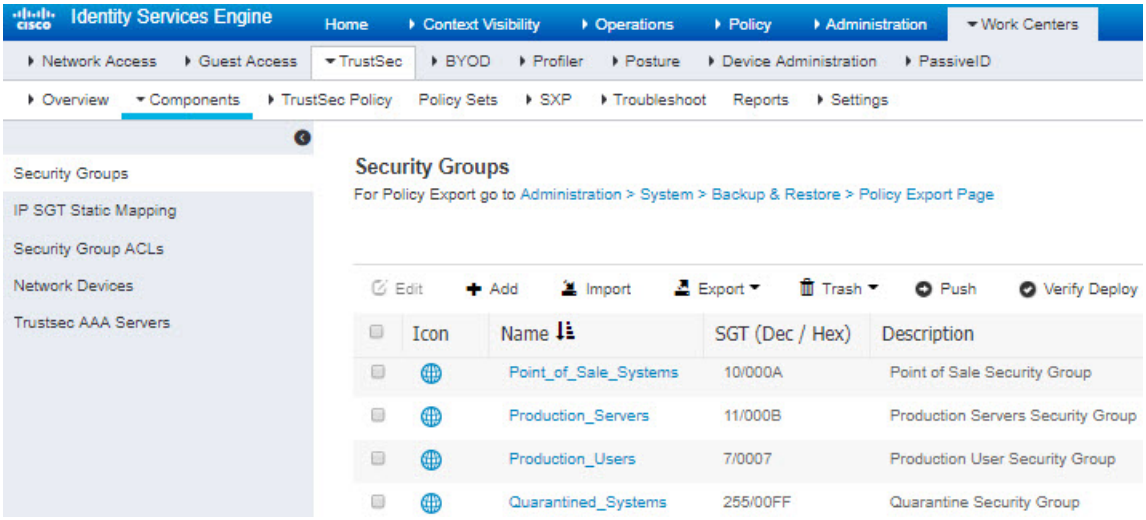


단계 **2** **Work Centers(**작업 센터**)** > **TrustSec** > **SXP** > **SXP Devices(SXP** 디바이스**)**를 선택하고 디바이스를 추가합니다.

이 디바이스가 실제 디바이스일 필요는 없으며, FTD 디바이스의 관리 IP 주소를 사용할 수도 있습니다. 이 표에는 ISE에서 정적 SGT-IP 주소 매핑을 게시하도록 유도하는 디바이스가 하나 이상 필요합니다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.

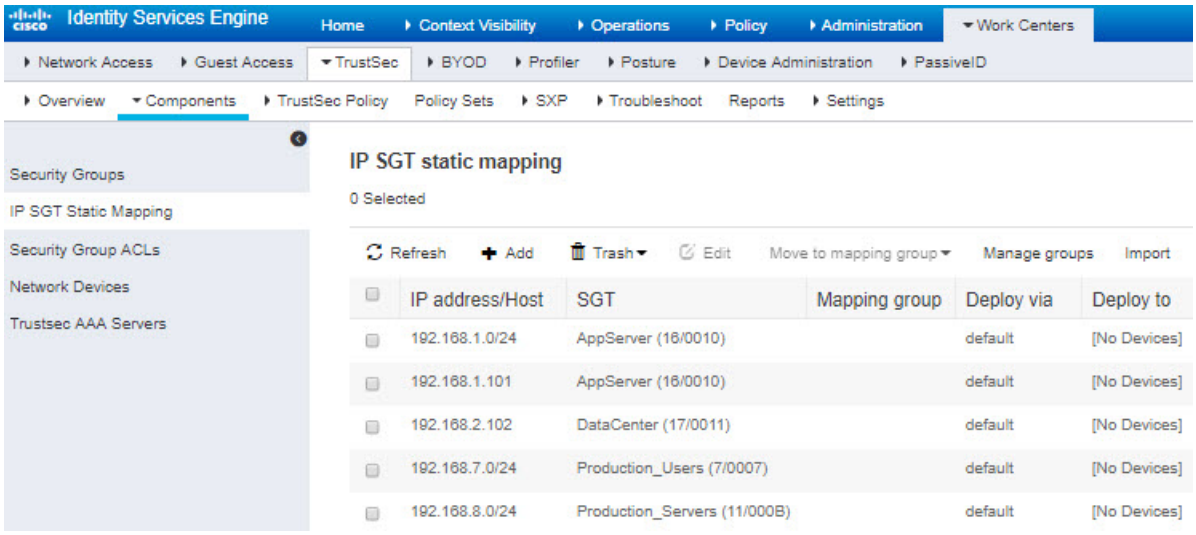


단계 **3** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **Security Groups(**보안 그룹**)**를 선택하고 SGT(Security Group Tag)가 정의되어 있는지 확인합니다. 필요에 따라 새로 생성합니다.



단계 **4** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **IPSGT Static Mapping(IPSGT** 정적 매핑**)**을 선택하고 호스트 및 네트워크 IP 주소를 SGT(Security Group Tag)에 매핑합니다.

단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.



FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기

아래 섹션에서는 다음을 수행하는 방법을 설명합니다.

- ISE/ISE-PIC 서버에서 시스템 인증서를 내보냅니다.

  이러한 인증서는 ISE/ISE-PIC 서버에 안전하게 연결하는 데 필요합니다. ISE 시스템 설정 방법에 따라 1개 또는 최대 3개의 인증서를 내보내야 합니다.

  - pxGrid 서버용 인증서 1개
  - 모니터링(MNT) 서버용 인증서 1개
  - FMC용 인증서 1개(개인 키 포함)

- 이러한 인증서를 FMC로 가져옵니다.

관련 항목

시스템 인증서 내보내기, 11 페이지
ISE/ISE-PIC 인증서 가져오기, 12 페이지

시스템 인증서 내보내기

시스템 인증서 또는 인증서와 그 연결된 개인 키를 내보낼 수 있습니다. 인증서 및 해당 개인 키를 백업용으로 내보내는 경우 나중에 필요하면 인증서와 키를 다시 가져올 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

프로시저

단계 **1** 선택 . **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** 인증서만 내보낼지 아니면 인증서 및 연결된 개인 키를 내보낼지를 선택합니다.

팁 인증서와 연결된 개인 키의 값이 노출될 수 있으므로 개인 키는 내보내지 않는 것이 좋습니다. 노드 간 통신용으로 와일드카드 시스템 인증서를 다른 Cisco ISE 노드로 가져오기 위해 내보내는 등의 경우와 같이 개인 키를 내보내야 하는 경우에는 개인 키용 암호화 비밀번호를 지정합니다. 개인 키의 암호를 해독하려면 이 인증서를 다른 Cisco ISE 노드로 가져오는 동안 이 비밀번호를 지정해야 합니다.

단계 **4** 개인 키를 내보내도록 선택한 경우 비밀번호를 입력합니다. 비밀번호는 8자 이상이어야 합니다.

단계 **5** **Export(**내보내기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 파일 시스템에 인증서를 저장합니다.

인증서만 내보내는 경우에는 PEM 형식으로 인증서가 저장됩니다. 인증서와 개인 키를 모두 내보내는 경우에는 PEM 형식 인증서와 암호화된 개인 키 파일을 포함하는 .zip 파일로 인증서가 내보내집니다.

ISE/ISE-PIC 인증서 가져오기

이 절차는 선택사항입니다. 사용자 제어를 위한 ISE/ISE-PIC 설정, 13 페이지의 설명에 따라 ISE/ISE-PIC ID 소스를 생성할 때 ISE 서버 인증서를 가져올 수도 있습니다.

시작하기 전에

시스템 인증서 내보내기, 11 페이지의 설명에 따라 ISE/ISE-PIC 서버에서 인증서를 내보냅니다. FMC에 로그인하는 장치에 인증서와 키가 있어야 합니다.

다음 두 가지 유형의 인증서 개체를 가져옵니다.

- ISE/ISE-PIC를 사용하여 인증하는 데 필요한 FMC용 내부 인증서 및 개인 키
- pxGrid 및 ISE 모니터링(MNT) 서버를 위한 신뢰할 수 있는 인증 기관(CA) 1곳 이상

  ISE/ISE-PIC 시스템 설정 방법에 따라 별개의 인증서 2개가 필요할 수도 있고 1개만 필요할 수도 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 FMC에 로그인합니다.

단계 **2** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 클릭합니다.

단계 3 **PKI**를 확장합니다.
단계 4 **Internal Certs(**내부 인증서**)**를 클릭합니다.
단계 5 **Add Internal Cert**를 클릭합니다.
단계 6 화면에 표시되는 메시지에 따라 인증서와 개인 키를 가져옵니다.
단계 7 **Trusted CAs(**신뢰할 수 있는 **CA)**를 클릭합니다.
단계 8 **Add Trusted CA(**신뢰하는 **CA** 추가**)**를 클릭합니다.
단계 9 화면에 표시되는 메시지에 따라 pxGrid 서버 인증서를 가져옵니다.
단계 10 필요하다면 앞의 단계를 반복하여 MNT 서버의 신뢰할 수 있는 CA를 가져옵니다.

다음에 수행할 작업

사용자 제어를 위한 ISE/ISE-PIC 설정, 13 페이지

사용자 제어를 위한 ISE/ISE-PIC 설정

다음 절차에서는 ISE/ISE-PIC ID 소스를 구성하는 방법을 설명합니다. 이 작업을 수행하려면 전역 도메인에 있어야 합니다.

시작하기 전에

- Microsoft Active Directory 서버 또는 지원되는 LDAP 서버에서 사용자 세션을 가져오려면, 영역 생성의 설명에 따라 pxGrid 가상 사용자를 가정하여 ISE 서버에 대한 영역을 구성하고 활성화합니다.
- ISE 또는 ISE-PIC 연결을 구성합니다. 자세한 내용은 ISE/ISE-PIC ID 소스, 1 페이지 및 ISE/ISE-PIC 설정 필드, 15 페이지를 참조하십시오.
- SXP를 통해 게시된 SGT-IP 주소 매핑을 비롯한 ISE에 정의된 모든 매핑을 가져오려면 다음 절차를 따르십시오. 다음 옵션을 사용할 수도 있습니다.
  - 패킷에 있는 SGT 정보만 사용하고 ISE에서 다운로드한 매핑은 사용하지 않으려면, 액세스 제어 규칙 생성 및 수정에서 설명하는 단계는 건너뛰십시오. 이 경우에는 SGT 태그를 소스 조건으로만 사용할 수 있으며 이러한 태그는 대상 기준과 일치하지 않습니다.
  - 패킷과 사용자 대 IP 주소/SGT 매핑만 사용하려면, ISE ID 소스의 SXP 주제는 구독해선 안 되며, SXP 매핑을 게시하도록 ISE를 구성해선 안 됩니다. 소스 및 대상 일치 조건 둘 다에 이 정보를 사용할 수 있습니다.
- ISE/ISE-PIC 서버에서 인증서를 내보내고, 원한다면 FMC에서 사용할 인증서를 ISE/ISE-PIC 서버에서 내보내기, 11 페이지의 설명에 따라 FMC에 인증서를 가져옵니다.

프로시저

단계 1 Firepower Management Center에 로그인합니다.

단계 2 **System(**시스템**)** > **Integration(**통합**)** 버튼을 클릭합니다.

단계 3 **Identity Sources(ID** 소스**)**를 클릭합니다.

단계 4 ISE 연결을 활성화하려면 **Service Type(**서비스 유형**)**으로 **Identity Services Engine(ID** 서비스 엔진**)**을 클릭합니다.

참고 연결을 비활성화하려면 **None(**없음**)**을 클릭합니다.

단계 5 **Primary Host Name/IP Address(**기본 호스트 이름**/IP** 주소**)**를 입력하고 필요에 따라 **Secondary Host Name/IP Address(**보조 호스트 이름**/IP** 주소**)**를 입력합니다.

단계 6 **PxGrid Server CA** 및 **MNT** 서버 **CA** 목록에서 적절한 인증서 인증 기관과 **FMC** 서버 인증서 목록에서 적절한 인증서를 클릭합니다. 추가(+)을 클릭하여 인증서를 추가할 수도 있습니다.

참고 **FMC Server Certificate(FMC** 서버 인증서**)**에는 **clientAuth** 확장된 키 사용 값을 포함해야 하거나, 확장된 키 사용 값을 포함하지 않아야 합니다.

단계 7 (선택 사항). CIDR 블록 표기법을 사용하려면 **ISE Network Filter(ISE** 네트워크 필터**)**를 입력합니다.

단계 8 Subscribe To(구독 대상) 섹션에서 다음을 확인합니다.

- ISE 서버에서 ISE 사용자 세션 정보를 가져오는 **Session Directory Topic(**세션 디렉터리 주제
- ISE 서버에서 제공하는 SGT-to-IP 매핑에 대한 업데이트를 수신하는 **SXP** 주제 이 옵션은 액세스 제어 규칙에서 목적지 SGT 태깅을 사용할 때 필요합니다.

단계 9 연결을 테스트하려면 **Test(**테스트**)**를 클릭합니다.

다음에 수행할 작업

- ID 정책 생성에 설명된 대로 ID 정책을 사용하여 제어할 사용자 및 기타 옵션을 지정합니다.
- 액세스 제어에 다른 정책 연결에 설명된 대로 ID 규칙을 트래픽을 필터링하고 필요에 따라 검사하는 액세스 제어 규칙과 연결합니다.
- 컨피그레이션 변경 사항 구축에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- 워크플로 사용에 설명된 대로 사용자 활동을 모니터링합니다.

관련 항목

ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결, 16 페이지
신뢰할 수 있는 인증 기관 개체
내부 인증서 개체

ISE/ISE-PIC 설정 필드

다음 필드를 사용하여 ISE/ISE-PIC에 대한 연결을 구성합니다.

Primary and Secondary Host Name/IP Address(기본 및 보조 호스트 이름**/IP** 주소**)**

기본과 보조 pxGrid ISE 서버(선택 사항)의 호스트 이름 또는 IP 주소입니다.

사용자가 지정한 호스트 이름이 사용한 포트는 ISE와 Firepower Management Center 모두가 연결할 수 있어야 합니다.

pxGrid 서버 **CA**

PxGrid 프레임워크용 인증 증명입니다. 구축에 기본 및 보조 pxGrid 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.

MNT 서버 **CA**

벌크 다운로드 수행 시의 ISE 인증서용 인증 증명입니다. 구축에 기본 및 보조 MNT 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.

FMC 서버 인증서

ISE/ISE-PIC에 연결하거나 벌크 다운로드를 수행하려면 Firepower Management Center에서 ISE/ISE-PIC에 제공해야 하는 인증서와 키입니다.

참고 **FMC Server Certificate(FMC** 서버 인증서**)**에는 clientAuth 확장된 키 사용 값을 포함해야 하거나, 확장된 키 사용 값을 포함하지 않아야 합니다.

ISE 네트워크 필터

ISE가 Firepower Management Center에 보고하는 데이터를 제한하기 위해 설정할 수 있는 선택적 필터입니다. 네트워크 필터를 제공하는 경우 ISE는 필터 내의 네트워크에서 데이터를 보고합니다. 다음과 같은 방법으로 필터를 지정할 수 있습니다.

- **any (**모두**)** 를 지정하려면 필드를 비워 둡니다.
- CIDR 표기법을 사용하여 단일 IPv4 주소 블록을 입력합니다.
- CIDR 표기법을 사용하여 IPv4 주소 블록 목록을 쉼표로 구분해 입력합니다.

참고 이 Firepower System 버전에서는 ISE 버전에 관계없이 IPv6 주소를 사용한 필터링을 지원하지 않습니다.

구독**:**

Session Directory Topic(세션 디렉토리 주제**)**:이 확인란을 선택하면 ISE 서버에서 사용자 세션 정보를 구독할 수 있습니다. SGT 및 엔드포인트 메타데이터를 포함합니다.
SXP Topic(SXP 주제**)**: 이 확인란을 선택하면 ISE 서버에서 SXP 매핑을 구독합니다.

관련 항목

신뢰할 수 있는 인증 기관 개체
내부 인증서 개체

ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결

Cisco TrustSec 문제 해결

디바이스 인터페이스는 ISE/ISE-PIC 또는 네트워크의 Cisco 디바이스(Cisco TrustSec이라고 함)에서 SGT(Security Group Tag)를 전파하도록 설정할 수 있습니다. Device Management(디바이스 관리) 페이지(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**)에서 디바이스를 재부팅하고 나면 인터페이스에 대한 **Propagate Security Group Tag(**보안 그룹 태그 전파**)** 확인란이 선택됩니다. 인터페이스에서 TrustSec 데이터를 전파하지 않도록 하려면 확인란의 선택을 취소합니다.

ISE/ISE-PIC 문제 해결

기타 관련 문제 해결 정보를 보려면 영역 및 사용자 다운로드 문제 해결 및 사용자 제어 문제 해결을 참조하십시오.

ISE 또는 ISE-PIC 연결에 문제가 발생한 경우 다음을 확인하십시오.

- ISE를 Firepower System과 성공적으로 통합하려면 우선 ISE에서 pxGrid Identity Mapping(pxGrid ID 매핑) 기능을 활성화해야 합니다.
- 기본 서버가 실패하는 경우, 사용자는 보조를 기본으로 직접 승격해야 합니다. 자동 페일오버는 실행되지 않습니다.
- ISE 서버와 Firepower Management Center 디바이스 간의 연결에 성공하려면 ISE에서 클라이언트를 수동으로 승인해야 합니다. (일반적으로 클라이언트 두 개가 존재합니다. 하나는 연결 테스트용이며, 다른 하나는 ISE 에이전트용입니다.)

  또한 *Cisco Identity Services Engine* 관리자 가이드의 사용자 및 외부 ID 소스 관리 장에서 설명하는 것처럼 ISE에서 **Automatically approve new accounts(**새 어카운트 자동 승인**)**를 활성화할 수도 있습니다.
- **FMC Server Certificate(FMC** 서버 인증서**)**에는 **clientAuth** 확장된 키 사용 값을 포함해야 하거나, 확장된 키 사용 값을 포함하지 않아야 합니다.
- ISE 서버의 시간은 Firepower Management Center의 시간과 동기화되어야 합니다. 어플라이언스가 동기화되지 않은 경우, 시스템이 예기치 않은 간격으로 사용자 시간 초과를 수행할 수 있습니다.
- 구축에 기본 및 보조 pxGrid 노드가 포함되는 경우,
  - 두 노드의 인증서에 같은 인증 기관이 서명해야 합니다.
  - 호스트 이름이 사용한 포트는 ISE 서버와 Firepower Management Center 모두가 연결할 수 있어야 합니다.

- 구축에 기본 및 보조 MNT 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.

ISE에서 사용자-IP 및 SGT(Security Group Tag)-IP 매핑을 수신하는 서브넷을 제외하려면 **configure identity-subnet-filter** {**add** | **remove**} 명령을 사용합니다. 일반적으로 Snort ID 상태 모니터 메모리 오류를 방지하기 위해 메모리 부족 관리 디바이스에 대해 이 작업을 수행해야 합니다.

ISE 또는 ISE-PIC에서 보고된 사용자 데이터에 문제가 발생한 경우 다음을 참고하십시오.

- 데이터베이스에 데이터가 아직 없는 ISE 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. 시스템이 사용자 다운로드에서 사용자에 대한 정보를 성공적으로 검색할 때까지 ISE 사용자가 보여준 활동이 액세스 제어 규칙으로 처리되지 않으며, 웹 인터페이스에 표시되지도 않습니다.
- LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.
- Firepower Management Center는 ISE 게스트 서비스 사용자의 데이터를 수신하지 않습니다.
- ISE 버전 및 컨피그레이션은 Firepower System에서 ISE를 사용할 수 있는 방법에 영향을 미칩니다. 자세한 정보는 ISE/ISE-PIC ID 소스, 1 페이지의 내용을 참고하십시오.
-
- ISE-PIC는 ISE 속성 데이터를 제공하지 않습니다.
- ISE-PIC는 ANC 교정을 수행할 수 없습니다.
- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 RFC 959를 참조하십시오.

지원되는 기능에 문제가 발생할 경우 ISE/ISE-PIC ID 소스, 1 페이지에서 버전 호환성에 대한 자세한 내용을 참조하십시오.

ISE/ISE-PIC 기록

기능	버전	세부 사항
pxGrid 2.0은 지원되는 ISE/ISE-PIC 버전의 기본값입니다.	6.7.0	다음에 유의하십시오. • 지원되는 ISE/ISE-PIC 버전: 2.6 패치 6 이상, 2.7 패치 2 이상 • 적응형 네트워크 제어(ANC) 정책은 EPS(Endpoint Protection Service) 교정을 대체합니다. FMC에 EPS 정책이 구성된 경우 ANC를 사용하려면 마이그레이션해야 합니다.

기능	버전	세부 사항
선택적으로 ISE에서 사용자-IP 및 SGT(Security Group Tag)-IP 매핑을 수신하는 서브넷을 제외합니다. 일반적으로 Snort ID 상태 모니터 메모리 오류를 방지하기 위해 메모리 부족 관리 디바이스에 대해 이 작업을 수행해야 합니다.	6.7.0	새 명령: **configure identity-subnet-filter** {**add** | **remove**}
대상 SGT 매칭(Security Group Tag)	6.5.0	기능이 도입되었습니다. 액세스 제어 규칙의 소스 및 대상 매칭 기준 모두에 대해 ISE SGT 태그를 사용할 수 있습니다. SGT 태그는 ISE에서 얻은 태그-호스트/네트워크 매핑입니다. 신규/수정된 화면: • 대상 SGT 매칭을 구성하는 방법: **System(**시스템**)** > **Integration(**통합**)** > **Identity Sources(ID** 소스**)** > **ISE/ISE-PIC** • **Session Directory Topic(**세션 디렉토리 주제**)**:ISE 서버 세션 정보를 구독합니다. • **SXP Topic(SXP** 주제**)**: ISE 서버에서 SGT 태그 업데이트를 구독합니다. • **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**의 신규 및 이름 변경된 열 • 이름 변경: 보안 그룹 태그가 소스 SGT로 변경되었습니다. • 신규: 대상 SGT
ISE-PIC와의 통합	6.2.1	이제 ISE-PIC의 데이터를 사용할 수 있습니다.

기능	버전	세부 사항
ISE와 통합되었습니다.	6.0	기능이 도입되었습니다. Cisco의 PxGrid(Platform Exchange Grid)를 구독하면, Firepower Management Center는 추가적인 사용자 데이터, 디바이스 유형 데이터, 디바이스 위치 데이터 및 SGT(Security Group Tag, 네트워크 액세스 제어 기능을 제공하기 위해 ISE에서 사용하는 방법)를 다운로드할 수 있습니다.