소개 ISE-PIC

무단 위협으로부터 네트워크를 보호하려면 사용자 ID를 인증해야 합니다. 이를 위해 보안 제품이 네트워크에서 구현됩니다. 각 보안 제품에는 필요한 인증을 검색하는 고유한 방법이 있으며, 대개 인증된 사용자가 아닌 인증된 IP 주소를 식별합니다. 따라서 이러한 제품은 사용자 로그인 정보를 기반으로 인증을 제공하는 여러 외부 서버 및 방법을 참조하므로 네트워크가 분산됩니다. Cisco ISE(Identity Services Engine) Passive Identity Connector(ISE-PIC)는 중앙 집중식 설치 및 구현을 제공하므로 다양한 소스에서 패시브 인증 데이터를 수집하고 이러한 ID를 보안 제품 가입자와 공유할 수 있습니다.

Cisco ISE-PIC 용어

이 설명서에서는 Cisco ISE-PIC를 다룰 때 다음 용어를 사용합니다.

용어	정의
GUI	그래픽 유저 인터페이스. GUI는 ISE-PIC의 소프트웨어 설치에서 화면 및 탭 중 하나를 가리킵니다.
NIC	Network Interface Card(네트워크 인터페이스 카드).
노드	개별 물리적 또는 가상 Cisco ISE-PIC 어플라이언스.
PAN	ISE-PIC 구축의 기본 노드는 PAN(기본 관리 노드)이며 사용 가능한 모든 작업을 수행할 수 있는 노드입니다. ISE-PIC에서 최대 2개의 노드를 설치할 수 있습니다. 두 번째 노드를 설치하는 경우 이를 보조 관리 노드(보조 PAN)라고 합니다.

용어	정의
파서	시스템 로그 메시지를 수신하고 입력을 ISE-PIC에 관리, 매핑 및 게시할 수 있는 부분으로 나누는 ISE-PIC 백엔드 구성 요소입니다. 파서는 시스템 로그 메시지가 도착할 때마다 각 정보 라인을 통과하여 주요 정보를 찾습니다. 예를 들어 "mac ="를 찾도록 파서가 구성된 경우 파서는 각 구문을 구문 분석하면서 해당 구문을 찾습니다. 구성된 구문을 발견하면 파서가 정의된 정보를 ISE에 전달하도록 설정됩니다.
기본 노드	ISE-PIC 구축의 기본 노드는 PAN(기본 관리 노드)이며 사용 가능한 모든 작업을 수행할 수 있는 노드입니다. ISE-PIC에서 최대 2개의 노드를 설치할 수 있습니다. 두 번째 노드를 설치하는 경우 이를 보조 관리 노드(보조 PAN)라고 합니다.
프로브	프로브는 지정된 소스에서 데이터를 수집하는 메커니즘입니다. 프로브는 메커니즘을 설명하는 일반적인 용어이지만 데이터가 수집되는 방법 또는 수집되는 내용을 구체적으로 설명하지는 않습니다. 예를 들어 AD(Active Directory) 프로브는 ISE-PIC가 AD에서 데이터를 수집하는 데 도움을 주는 한편, 시스템 로그 프로브는 시스템 로그 메시지를 읽는 파서에서 데이터를 수집합니다.
사업자	ISE-PIC가 사용자 ID 정보를 수신, 매핑 및 게시하는 클라이언트 또는 소스입니다.
보조 노드	ISE-PIC 구축의 기본 노드는 PAN(기본 관리 노드)이며 사용 가능한 모든 작업을 수행할 수 있는 노드입니다. ISE-PIC에서 최대 2개의 노드를 설치할 수 있습니다. 두 번째 노드를 설치하는 경우 이를 보조 관리 노드(보조 PAN)라고 합니다.
가입자	사용자 ID 정보를 수신하기 위해 ISE-PIC 서비스를 구독하는 시스템입니다.

ISE-PIC 개요

Passive Identity Connector(ISE-PIC)는 중앙 집중식 원스톱 설치 및 구현을 제공하기 때문에, 사용자는 네트워크를 쉽고 간단하게 구성해 사용자 ID 정보를 받고 Cisco FMC(Firepower Management Center)나 Stealthwatch 같은 다양한 보안 제품 가입자와 공유할 수 있습니다. 수동 식별의 전체 브로커로서 ISE-PIC는 AD DC(Active Directory Domain Controller) 같은 다양한 제공자 소스로부터 사용자 ID를 수집하고, 사용자 로그인 정보를 사용 중인 관련 IP 주소에 매핑한 다음 매핑 정보를 사용자가 구성한 가입자 보안 제품과 공유합니다.

Passive Identity(패시브 **ID**)란?

AAA(인증, 권한 부여 및 계정 관리) 서버를 제공하며 802.1X나 Web Authentication(웹 인증) 같은 기술을 활용하고, 사용자 또는 엔드포인트와 직접 통신해 네트워크 액세를 요청한 다음 관련 로그인 자격 증명을 이용해 ID를 확인하고 활성 인증합니다.

패시브 ID 서비스는 사용자를 직접 인증하는 대신 서비스 제공자로 확인된 (Active Directory 같은) 외부 인증 서버에서 사용자 ID와 IP 주소를 수집한 다음 이 정보를 가입자와 공유합니다. ISE-PIC는 먼저 서비스 제공자로부터 (대부분 사용자 로그인 및 암호를 바탕으로) 사용자 ID 정보를 수신한 다음 필요한 확인 작업과 서비스를 수행하여 사용자 ID를 관련 IP 주소와 매치함으로써 인증된 IP 주소를 가입자에게 전달합니다.

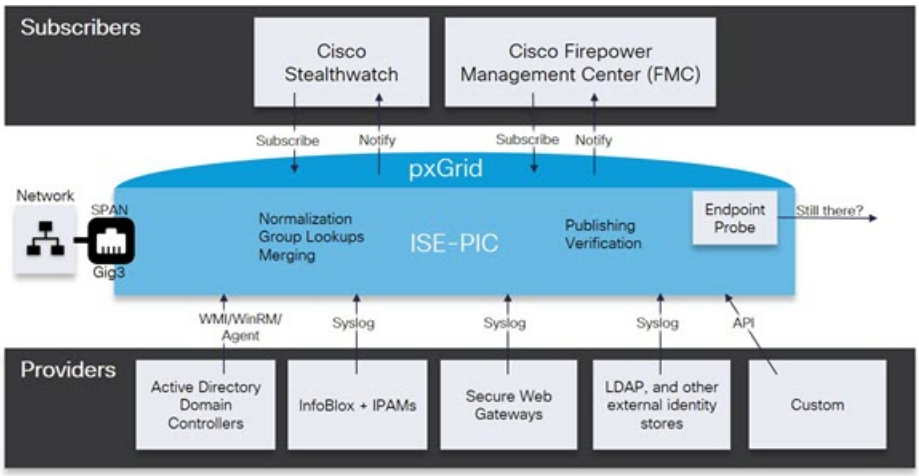
Passive Identity Connector(ISE-PIC) 흐름

ISE-PIC의 흐름은 다음과 같습니다.

1. 서비스 제공자가 사용자 또는 엔드포인트의 인증을 수행합니다.
2. 서비스 제공자가 인증된 사용자 정보를 ISE-PIC에 전송합니다.
3. ISE-PIC는 사용자 정보를 정규화하고 관련 조회와 병합 및 구문 분석을 수행하며 IP 주소에 매핑하고, 매핑한 세부 정보를 pxGrid에 게시합니다.
4. pxGrid 가입자는 매핑된 사용자 세부 정보를 수신합니다.

다음 다이어그램에서는 ISE-PIC에서 제공되는 개괄적인 플로우에 대해 설명합니다.

그림 ***1:*** 고수준 흐름



Cisco ISE-PIC 아키텍처, 구축 및 노드

Cisco ISE-PIC 아키텍처는 다음 구성 요소를 포함합니다.

- 노드 - Cisco ISE-PIC 구축에서 아래 설명된 대로 최대 2개의 노드를 구성할 수 있습니다.

- 네트워크 리소스
- 엔드포인트

단일 Cisco ISE-PIC 노드가 있는 구축을 독립형 구축이라고 합니다.

두 개의 Cisco ISE-PIC 노드가 있는 구축을 고가용성 구축이라고하며, 여기서 하나의 노드는 기본 어플라이언스(기본 관리 노드 또는 PAN)로 작동합니다. 고가용성 구축은 서비스 가용성을 개선합니다.

PAN이 이 네트워크 모델에 필요한 모든 컨피그레이션 기능을 제공합니다. 보조 Cisco ISE 노드(보조 PAN)는 백업의 역할을 합니다. 보조 노드는 기본 노드를 지원하며 기본 노드와의 연결이 끊길 때마다 기능을 다시 시작합니다.

Cisco ISE-PIC는 기본 Cisco ISE-PIC 노드에 있는 모든 콘텐츠를 보조 Cisco ISE-PIC 노드와 동기화하거나 복제하여 보조 노드가 기본 노드의 상태와 최신 상태를 유지하도록 합니다(따라서 백업으로 사용할 수 있음).

ISE 커뮤니티 리소스

구축 및 확장에 대한 자세한 내용은 ISE 구축 여정을 참조하십시오.

장점 ISE-PIC

ISE-PIC 다음을 제공합니다.

- 다양한 제공자와 상호 작용하는 단일 ID 솔루션입니다.
- 간편한 컨피그레이션, 모니터링 및 문제 해결을 지원하는 친숙한 GUI
- 간단한 설치 및 구성
- 활성 인증을 위해 ISE로 쉽게 업그레이드할 수 있습니다. ISE-PIC에서 전체 ISE 구축으로 업그레이드하고 ISE-PIC 노드를 사용하여 독립형 ISE 구축을 생성할 때 또는 이 노드를 기존 구축에 기본 노드로 추가할 경우 ISE는 업그레이드 이전에 ISE-PIC에서 제공되었던 모든 기능을 계속 제공하고 기존 컨피그레이션이 보존됩니다.

참고 ISE로 업그레이드하려면 평가판을 다운로드하거나 Cisco 담당자에게 문의하여 라이선싱 옵션에 대해 논의하십시오.

기본 노드가 아닌 기존 ISE 구축에 업그레이드된 ISE-PIC를 추가하면 이전 ISE-PIC 컨피그레이션을 덮어 씁니다.

업그레이드 흐름에 대한 자세한 내용은 전체 ISE 설치로 ISE-PIC 업그레이드를 참조하십시오.

ISE-PIC와 ISE/CDA 비교

ISE-PIC ISE로 쉽고 원활하게 업그레이드하는 기능 등의 다양한 혜택을 제공합니다. Cisco는 ISE-PIC 및 ISE 외에 추가 보안 메커니즘인 CDA도 제공합니다. 이 섹션의 아래 표에서는 세 제품을 비교한 결과를 확인할 수 있습니다.

ISE-PIC와 ISE의 자세한 비교

ISE-PIC 는 패시브 ID만 공유하도록 설계되었고, AAA(인증, 권한 부여 및 계정 관리) 서버를 제공하며 ISE가 제공하는 권한 부여 또는 인증 서비스는 제공하지 않습니다. 다음 표에서는 두 제품 간의 차이를 자세히 확인할 수 있습니다.

표 *1: ISE-PIC*와 *ISE* 비교

카테고리	기능	ISE-PIC	ISE
Smart Licensing		—	√
인증 및 권한 부여 유형	권한 부여 정책	—	√
	TrustSec	—	√
	WMI를 포함한 Active Directory 수동 인증	√	√

카테고리	기능	**ISE-PIC**	**ISE**
패시브 ID 소스		√	√
	Easy Connect	—	√
	SysLog 소스	√	√
	REST API 소스	√	√
	SPAN	√	√
	Security Group eXchange Protocol (SXP)	—	√
	RADIUS 프록시를 포함한 RADIUS	—	√
	BYOD	—	√
	게스트	—	√
	포스처	—	√
	Device Administration(TACACS+)	—	√
pxGrid	pxGrid 컨트롤러	√ Cisco 가입자 전용	√
	pxGrid 컨트롤러 이중화	√	√
	주제 확장성	—	√
CA(Certificate Authority)	pxGrid 인증서 템플릿	√	√
	엔드포인트 CA	—	√
	보안 전송을 통한 등록(EST)	—	√
	기타 인증서 템플릿	—	√
가시성 및 상황	컨텍스트 디렉토리	—	√
	프로파일링	—	√

카테고리	기능	**ISE-PIC**	**ISE**
리포트		! 참고 ISE-PIC에서는 시스템 상태를 모니터링하고 네트워크 문제를 해결하는 데 사용할 수 있는 보고서를 제공합니다. 하지만 ISE-PIC에서는 ISE와는 달리 기능 하위 집합을 제공하며, 따라서 ISE 보고서 중 일부는 ISE-PIC에서는 사용할 수 없습니다.	√

ISE-PIC와 **ISE/CDA**의 개략적인 비교

CDA는 보안 게이트웨이가 네트워크에서 어떤 사용자가 어떤 IP 주소를 사용하는지 확인할 수 있도록 IP 주소를 사용자 이름에 매핑하며, 따라서 이제 이러한 보안 게이트웨이는 사용자(또는 사용자가 속한 그룹)를 기준으로 결정을 내릴 수 있습니다. 그러나 ISE-PIC에서는 사용자 이름, MAC 주소 및 포트 같은 추가 데이터에 액세스하여 사용자 ID를 훨씬 더 정확하게 수집합니다. 다음 표에서는 ISE-PIC, ISE와 CDA의 고수준 비교 결과를 확인할 수 있습니다.

표 ***2: ISE-PIC***와 ***ISE/CDA*** 비교

패시브 인증 세부 정보	전체 **ISE**	**ISE-PIC**	**CDA**
도메인 컨트롤러 숫자	100	100	80
가입자 수	20	20	—
WMI(에이전트 없음)	예	예	예
사용 가능한 Windows 서버 에이전트	예	예	—
DCOM 필수	아니요(SPAN)	아니요(SPAN)	예
Easy Connect	예	—	—

패시브 인증 세부 정보	전체 **ISE**	**ISE-PIC**	**CDA**
SPAN을 이용한 Kerberos 탐지	예	예	—
결합(IP 주소, MAC 주소 및 사용자 이름)	300,000	300,000	64,000