Firepower 사용자 ID:사용자 에이전트에서 Identity Services Engine으로 마이그레이션

소개

향후 릴리스에서는 Firepower User Agent를 더 이상 사용할 수 없습니다.ISE(Identity Services Engine) 또는 ISE-PIC(Identity Services Engine - 수동 ID 커넥터)로 교체됩니다. 현재 User Agent를 사용하고 ISE로 마이그레이션을 고려하고 있는 경우 이 문서에서는 마이그레이션을 위한 고려 사항 및 전략을 제공합니다.

사용자 ID 개요

현재 기존 ID 인프라에서 사용자 ID 정보를 추출하는 두 가지 방법이 있습니다.사용자 에이전트 및 ISE 통합.

사용자 에이전트

사용자 에이전트는 Windows 플랫폼에 설치된 애플리케이션입니다.WMI(Windows Management Instrumentation) 프로토콜을 사용하여 사용자 로그온 이벤트(이벤트 유형 4624)에 액세스한 다음 데이터를 로컬 데이터베이스에 저장합니다.사용자 에이전트가 로그온 이벤트를 검색하는 방법에는 두 가지가 있습니다.사용자가 로그인할 때 실시간으로 업데이트되거나(Windows Server 2008 및 2012에만 해당) 구성 가능한 간격마다 데이터를 폴링합니다.마찬가지로, 사용자 에이전트는 AD(Active Directory)에서 수신된 데이터를 실시간으로 FMC(Firepower Management Center)로 전송하고 로그온 데이터 배치를 FMC에 정기적으로 전송합니다.

사용자 에이전트에서 감지할 수 있는 로그인 유형에는 직접 또는 원격 데스크톱을 통해 호스트에 로그인하는 것이 포함됩니다.파일 공유 로그인;컴퓨터 계정 로그인Citrix, 네트워크 로그온 및 Kerberos 로그인과 같은 다른 유형의 로그인은 사용자 에이전트에서 지원되지 않습니다.

사용자 에이전트에는 매핑된 사용자가 로그오프되었는지 여부를 탐지하는 선택적 기능이 있습니다.로그오프 검사가 활성화된 경우 각 매핑된 엔드포인트에서 "explorer.exe" 프로세스가 실행 중인지 주기적으로 확인합니다.실행 중인 프로세스를 탐지할 수 없는 경우 72시간 후에 이 사용자에 대한 매핑이 제거됩니다.

Identity Services Engine

ISE(Identity Services Engine)는 사용자의 네트워크 로그인 세션을 관리하는 강력한 AAA 서버입니다.ISE는 스위치 및 무선 컨트롤러와 같은 네트워크 디바이스와 직접 통신하므로 사용자 활동에 대한 최신 데이터에 액세스할 수 있으므로 사용자 에이전트보다 더 나은 ID 소스가 됩니다.사용자가 엔드포인트에 로그온하면 일반적으로 네트워크에 자동으로 연결되며, 네트워크에 대해 dot1x 인증이 활성화된 경우 ISE는 이 사용자에 대한 인증 세션을 생성하고 사용자가 네트워크에서 로그오프할 때까지 이를 활성 상태로 유지합니다.ISE가 FMC와 통합된 경우 사용자-IP 매핑(ISE에서 수집한 다른 데이터 포함)을 FMC에 전달합니다.

ISE는 pxGrid를 통해 FMC와 통합할 수 있습니다.pxGrid는 ISE 서버 및 다른 제품 간의 세션 정보 분포를 중앙 집중화하기 위해 설계된 프로토콜입니다.이 통합에서 ISE는 pxGrid Controller의 역할을 하며 FMC는 컨트롤러에 가입하여 세션 데이터를 수신합니다(FMC는 나중에 논의된 교정 중에

외에는 어떤 데이터도 ISE에 게시하지 않음). 그리고 데이터를 센서에 전달하여 사용자 인식을 달성합니다.

ISE-PIC(Identity Services Engine Passive Identity Connector)는 기본적으로 제한된 라이센스가 있는 ISE의 인스턴스입니다.ISE-PIC는 어떤 인증도 수행하지 않고 대신 네트워크의 다양한 ID 소스에 대한 중앙 허브 역할을 하여 ID 데이터를 수집하고 가입자에게 제공합니다.ISE-PIC는 WMI를 사용하여 AD에서 로그인 이벤트를 수집하지만 패시브 ID라고 하는 더 강력한 기능을 가지고 있다는 점에서 사용자 에이전트와 유사합니다.또한 pxGrid를 통해 FMC와 통합됩니다.

마이그레이션 고려 사항

라이센싱 요구 사항

FMC에는 추가 라이센스가 필요하지 않습니다.Identity Services Engine이 인프라에 아직 구축되어 있지 않은 경우 라이센스가 필요합니다.자세한 내용은 Cisco ISE 라이센싱 모델 문서를 참조하십시오. ISE 패시브 ID 커넥터는 전체 ISE 구축에 이미 존재하는 기능 집합이므로 기존 ISE 구축이 있는 경우 추가 라이센스가 필요하지 않습니다.ISE-PIC의 신규 또는 개별 구축은 Cisco ISE-PIC 라이센싱 문서를 참조하십시오.

SSL 인증서

사용자 에이전트는 FMC 및 Active Directory와의 통신에 PKI(Public Key Infrastructure)를 필요로 하지 않지만, ISE 또는 ISE-PIC 통합에는 인증 목적으로만 ISE와 FMC 간에 공유되는 SSL 인증서가 필요합니다.이 통합은 인증서에 "Server Authentication(서버 인증)" 및 "Client Authentication(클라이언트 인증)" EKU(Extension Key Usage) 모두 추가되는 경우 CA(Certificate Authority) 서명 및 자체 서명 인증서를 지원합니다.

ID 소스 커버리지

사용자 에이전트는 폴링 기반 로그아웃 탐지와 함께 Windows 데스크톱의 Windows 로그인 이벤트만 다룹니다.ISE-PIC는 Windows 데스크톱 로그인과 AD 에이전트, Kerberos SPAN, Syslog 파서, TSA(Terminal Services Agent)와 같은 추가 ID 소스를 다룹니다. 전체 ISE는 ISE-PIC의 모든 커버리지와 Windows 이외의 워크스테이션 및 모바일 장치에서 네트워크 인증을 제공합니다.

	사용자 에이전트	ISE-PIC	ISE
Active Directory 데스크톱 로그온	예	예	예
네트워크 로그온	아니요	아니요	예
엔드포인트 프로브	예	예	예
InfoBlox/IPAM	아니요	예	예
LDAP	아니요	예	예
보안 웹 게이트웨이	아니요	예	예
REST API 소스	아니요	예	예
Syslog 파서	아니요	예	예
네트워크 범위	아니요	예	예

사용자 에이전트 단종

User Agent를 지원하는 Firepower의 마지막 버전은 6.6입니다. 이 버전은 이후 릴리스로 업그레이드하기 전에 User Agent를 비활성화해야 한다는 경고를 제공합니다.6.6 이상 버전으로 업그레이드

해야 하는 경우 업그레이드 전에 사용자 에이전트에서 ISE 또는 ISE-PIC로 마이그레이션해야 합니다.자세한 내용은 사용자 에이전트 구성 가이드를 참조하십시오.

호환성

통합과 관련된 소프트웨어 버전이 호환되는지 확인하려면 Firepower 제품 호환성 가이드를 검토하십시오.향후 Firepower 릴리스의 경우, 최신 ISE 버전을 지원하려면 특정 패치 수준이 필요할 수 있습니다.

마이그레이션 전략

사용자 에이전트에서 ISE 또는 ISE-PIC로 마이그레이션하려면 FMC용 사용자 ID 소스를 원활하게 전환하고 사용자 트래픽에 영향을 미치지 않도록 신중하게 계획, 실행 및 테스트를 수행해야 합니다.이 섹션에서는 이 활동에 대한 모범 사례 및 권장 사항을 제공합니다.

마이그레이션 준비

다음 단계는 사용자 에이전트에서 ISE 통합으로 컷오프하기 전에 수행할 수 있습니다.

1단계. PassiveID를 사용하도록 ISE 또는 ISE-PIC를 구성하고 Active Directory와 WMI 연결을 설정합니다.ISE-PIC 관리 설명서를 참조하십시오.

2단계. FMC의 ID 인증서를 준비합니다.FMC에서 발급한 자체 서명 인증서 또는 FMC에서 생성된 CSR(Certificate Signing Request)일 수 있으며, CA(Private 또는 Public Certificate Authority)에서 서명할 수 있습니다. CA의 자체 서명 인증서 또는 루트 인증서가 ISE에 설치되어 있어야 합니다.자세한 내용은 ISE 및 FMC 통합 가이드를 참조하십시오.

3단계. ISE의 pxGrid 인증서(또는 자체 서명된 경우 pxGrid 인증서)에 서명한 CA 루트 인증서를 FMC에 설치합니다.자세한 내용은 ISE 및 FMC 통합 가이드를 참조하십시오.

컷오버 프로세스

두 컨피그레이션은 상호 배타적이므로 FMC에서 사용자 에이전트 컨피그레이션을 비활성화하지 않으면 FMC-ISE 통합을 구성할 수 없습니다.이는 변경 중에 사용자에게 영향을 미칠 수 있습니다.이러한 단계는 유지 보수 기간 동안 수행하는 것이 좋습니다.

1단계. FMC-ISE 통합을 활성화하고 확인합니다.자세한 내용은 ISE 및 FMC 통합 가이드를 참조하십시오.

2단계. 사용자 활동이 FMC에 보고되어 FMC의 **Analysis > User > User Activities** 페이지로 이동하는지 확인합니다.

3단계. 사용자-IP 매핑 및 사용자-그룹 매핑을 의 관리되는 디바이스에서 사용할 수 있는지 검토합니다.
Analysis > Connections > Events > Table View of Connection Events.

4단계. Access Control Policy(액세스 제어 정책)를 수정하여 사용자 이름 또는 사용자 그룹 조건에 따라 트래픽을 차단하는 모든 규칙으로 일시적으로 작업을 **Monitor(모니터링)**로 변경합니다.개시자 사용자 또는 그룹을 기반으로 트래픽을 허용하는 규칙의 경우 사용자 기준 없이 트래픽을 허용하는 중복 규칙을 만든 다음 원래 규칙을 비활성화합니다.이 단계는 유지 보수 기간 후 테스트 단계에서

비즈니스 크리티컬 트래픽이 영향을 받지 않도록 하는 것입니다.

5단계. 유지 보수 기간 후 정상 업무 시간 동안 FMC의 Connection Events(연결 이벤트)를 관찰하여 사용자-IP 매핑을 모니터링합니다.연결 이벤트는 사용자 데이터를 필요로 하는 활성화된 규칙이 있는 경우에만 사용자 정보를 표시합니다.따라서 이전 단계에서 모니터 작업이 제안되는 이유입니다.

6단계. 원하는 상태가 되면 액세스 제어 정책에 대한 변경 사항을 되돌리고 정책을 관리되는 디바이스에 푸시하면 됩니다.

추가 정보

- 비디오 자습서:ISE-PIC로 사용자 에이전트 전환
- Cisco ISE 2.4 관리 가이드:라이센싱
- ISE-PIC(Identity Services Engine Passive Identity Connector) 설치 및 관리자 가이드, 릴리스 2.2
- 사용자 에이전트 컨피그레이션 가이드
- Cisco Firepower 호환성 가이드
- ISE 2.4 및 FMC 6.2.3 pxGrid 통합 구성