Firepower用户身份：从用户代理迁移到身份服务引擎

简介

在未来版本中，Firepower用户代理不再可用。替换为身份服务引擎(ISE)或身份服务引擎 — 被动ID连接器(ISE-PIC)。 如果您当前使用用户代理并考虑迁移到ISE，本文档将提供迁移的注意事项和策略。

用户身份概述

目前有两种方法可以从现有身份基础设施中提取用户身份信息：用户代理和ISE集成。

用户代理

用户代理是安装在Windows平台上的应用程序。它依靠Windows管理规范(WMI)协议访问用户登录事件（事件类型4624），然后将数据保存到本地数据库。用户代理通过两种方式检索登录事件：在用户登录时实时更新（仅限Windows Server 2008和2012），或轮询每个可配置间隔的数据。同样，用户代理会实时将从Active Directory(AD)收到的数据发送到Firepower管理中心(FMC)，并定期向FMC发送大量登录数据。

用户代理可检测的登录类型包括直接或通过远程桌面登录主机；文件共享登录；计算机帐户登录。用户代理不支持其他类型的登录，如Citrix、网络登录和Kerberos登录。

用户代理具有可选功能来检测映射用户是否已注销。如果启用注销检查，它会定期检查“explorer.exe”进程是否在每个映射的终端上运行。如果无法检测到72小时后运行的进程，则删除此用户的映射。

身份服务引擎

身份服务引擎(ISE)是管理用户网络登录会话的强大AAA服务器。由于ISE直接与网络设备（如交换机和无线控制器）通信，因此它可以访问有关用户活动的最新数据，使其成为比用户代理更好的身份源。当用户登录终端时，它通常会自动连接到网络，如果为网络启用dot1x身份验证，ISE会为此用户创建身份验证会话并保持其活动状态，直到用户注销网络。如果ISE与FMC集成，它会将用户IP映射（以及ISE收集的其他数据）数据转发到FMC。

ISE可以通过pxGrid与FMC集成。pxGrid是一种协议，旨在集中ISE服务器之间以及与其他产品之间的会话信息分发。在此集成中，ISE充当pxGrid控制器，FMC订用控制器以接收会话数据(FMC不向ISE发布任何数据，除非在补救期间（稍后会讨论）)，并将数据传递到传感器以实现用户感知。

身份服务引擎被动身份连接器(ISE-PIC)实质上是具有受限许可证的ISE实例。ISE-PIC不执行任何身份验证，而是充当网络中各种身份源的中心集线器，收集身份数据并将其提供给用户。ISE-PIC类似于用户代理，因为它还使用WMI从AD收集登录事件，但具有更强大的功能，称为被动身份。它还通过pxGrid与FMC集成。

迁移注意事项

许可要求

FMC不需要额外的许可证。如果身份服务引擎尚未部署在基础设施中，则需要许可证。请参阅思科ISE许可模式文档了解详细信息。ISE被动ID连接器是完整ISE部署中已存在的功能集，因此，如果存在现有ISE部署，则无需其他许可证。有关ISE-PIC的新部署或单独部署，请参阅思科ISE-PIC许可文档以了解详细信息。

SSL证书

虽然用户代理不需要公共密钥基础设施(PKI)来与FMC和Active Directory通信，但ISE或ISE-PIC集成需要ISE和FMC之间共享的SSL证书，仅用于身份验证。集成支持证书颁发机构签名和自签名证书，前提是"服务器身份验证"和"客户端身份验证"EKU（扩展密钥用法）都添加到证书。

身份源覆盖

用户代理仅涵盖来自Windows桌面的Windows登录事件，并提供基于轮询的注销检测。ISE-PIC涵盖Windows桌面登录以及其他身份源，如AD代理、Kerberos SPAN、系统日志解析器和终端服务代理(TSA)。 完整ISE具有ISE-PIC的所有覆盖范围以及来自非Windows工作站和移动设备的网络身份验证和其他功能。

	用户代理	ISE-PIC	ISE
Active Directory桌面登录	Yes	Yes	Yes
网络登录	无	无	Yes
终端探测	Yes	Yes	Yes
InfoBlox/IPAM	无	Yes	Yes
LDAP	无	Yes	Yes
安全Web网关	无	Yes	Yes
REST API源	无	Yes	Yes
系统日志解析器	无	Yes	Yes
网络范围	无	Yes	Yes

用户代理寿命终止

支持用户代理的Firepower的最新版本是6.6，它提供警告，在升级到更高版本之前必须禁用用户代理。如果需要升级到高于6.6的版本，则必须在升级之前完成从用户代理到ISE或ISE-PIC的迁移。有关详细信息，请参阅《用户代理配置指南》。

兼容性

请查看Firepower产品兼容性指南，确保集成中涉及的软件版本兼容。请注意，对于未来的Firepower版本，支持更高的ISE版本可能需要特定的补丁级别。

迁移策略

从用户代理迁移到ISE或ISE-PIC需要仔细的规划、执行和测试，以确保FMC的用户身份源平稳过渡并避免对用户流量产生任何影响。本节提供本练习的最佳实践和建议。

准备迁移

在从用户代理切换到ISE集成之前，可以执行后续步骤。

步骤1.配置ISE或ISE-PIC以启用PassiveID，并与Active Directory建立WMI连接。请参阅《ISE-PIC管理指南》。

步骤2.准备FMC的身份证书。它可以是由FMC颁发的自签名证书或在FMC上生成的证书签名请求(CSR)，由专用或公共证书颁发机构(CA)签名。 ISE上必须安装CA的自签名证书或根证书。有关详细信息，请参阅ISE和FMC集成指南。

步骤3.在FMC上安装签署ISE的pxGrid证书(或pxGrid证书（如果自签名）的CA根证书。有关详细信息，请参阅ISE和FMC集成指南。

切换流程

如果不禁用FMC上的用户代理配置，则无法配置FMC-ISE集成，因为这两种配置是互斥的。这可能会影响更改期间的用户。建议在维护窗口期间执行这些步骤。

步骤1.启用并验证FMC-ISE集成。有关详细信息，请参阅ISE和FMC集成指南。

步骤2.确保用户活动报告给FMC，并导航至FMC上的**Analysis > User > User Activities**页面。

步骤3.检查用户IP映射和用户组映射在上的受管设备上可用
分析>连接>事件>连接事件的表视图。

步骤4.修改访问控制策略，将操作临时更改为“监控”(**Monitor**)，以根据用户名或用户组条件将任何阻止流量的规则更改为“监控”(Monitor)。对于允许基于发起方用户或组的流量的规则，请创建允许不带用户条件的流量的重复规则，然后禁用原始规则。此步骤的目的是确保在维护窗口后的测试阶段不影响关键业务流量。

步骤5.在维护窗口后，在正常工作时间内观察FMC上的连接事件以监控用户IP映射。请注意，只有在启用规则需要用户数据时，连接事件才显示用户信息。因此，在上一步中建议使用监控器操作。

步骤6.达到所需状态后，只需恢复对访问控制策略所做的更改，并将策略部署推送到受管设备。

其他信息

- 视频教程：用户代理过渡到ISE-PIC
- 思科ISE 2.4管理指南：许可
- 身份服务引擎被动身份连接器(ISE-PIC)安装和管理员指南，版本2.2
- 用户代理配置指南
- 思科Firepower兼容性指南
- 配置ISE 2.4和FMC 6.2.3 pxGrid集成