简介 ISE-PIC

注释 此产品的文档集力求使用无偏见语言。在本文档集中，无偏见定义为不暗示基于年龄、残障、性别、种族身份、族群身份、性取向、社会经济地位和交叉性的歧视的语言。由于产品软件的用户界面中使用的硬编码语言，基于 RFP 文档使用的语言或引用的第三方产品使用的语言，文档中可能存在例外情况。

用户身份必须经过身份验证，以保护网络免受未经授权的威胁。为此，需要在网络上实施安全产品。每个安全产品都有自己的检索必要身份验证的方法，通常用于识别授权的 IP 地址，而不是授权的用户。因此，这些产品指的是基于用户登录信息提供身份验证的不同外部服务器和方法，从而形成分散网络。思科身份识别服务引擎 (ISE) 被动身份连接器 (ISE-PIC) 提供集中的一站式安装和实施，让您轻松地从各种来源收集用户的被动身份验证数据，并与安全产品用户共享这些用户身份。

思科 ISE-PIC 术语

本指南在讨论 Cisco ISE-PIC 时使用以下术语：

术语	定义
GUI	图形用户界面。GUI 是指 ISE-PIC 软件安装中的任何屏幕和选项卡。
网卡	网络接口卡。
节点	单个物理或虚拟思科 ISE-PIC 设备。

术语	定义
PAN	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在ISE-PIC中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
解析器	接收系统日志消息，并将输入拆分为可管理、映射并发布到 ISE-PIC 的各部分的 ISE-PIC 后端组件。解析器将在系统日志消息到达时解析每行信息，查找关键信息。例如，如果解析器配置为查找“mac=”，则解析器会在查找此短语时解析每行信息。解析器设置为在找到已配置的关键短语后，将定义的信息传送到 ISE。
主节点	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在ISE-PIC中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
探测功能	探测器是从给定源收集数据的机制。探测器是一个说明任何机制的通用术语，但不具体描述如何收集数据或收集什么。例如，Active Directory (AD) 探测器有助于 ISE-PIC 从 AD 收集数据，而系统日志探测器则从读取系统日志消息的解析器收集数据。
提供程序	ISE-PIC 从中接收、映射和发布用户身份信息的客户端或源。
辅助节点	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在ISE-PIC中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
用户	订用 ISE-PIC 服务以接收用户身份信息的系统。

ISE-PIC 概述

被动身份连接器 (ISE-PIC) 提供集中的一站式安装和实施，使您能够轻松简单地配置网络，以便接收用户身份信息并与各种不同的安全产品用户（例如思科 Firepower 管理中心 [FMC] 和 Stealthwatch）进行共享。作为用于被动识别的全面代理，ISE-PIC 从不同提供程序源（例如 Active Directory 域控制器 [AD DC]）收集用户身份，将用户登录信息映射到使用中的相关 IP 地址，然后将该映射信息与已配置的任何用户安全产品进行共享。

什么是被动身份？

思科身份服务引擎 (ISE) 之类的产品，用于提供身份验证、授权和记账 (AAA) 服务器，并利用 802.1X 或 Web 身份验证之类的技术，直接与用户或终端进行通信，从而请求访问网络，然后使用其登录凭证来确认其身份并主动进行身份验证。

被动身份服务不直接对用户进行身份验证，而是从 Active Directory 之类的外部身份验证服务器（称为提供程序）收集用户身份和 IP 地址，然后与用户共享该信息。ISE-PIC首先从提供程序接收用户身份信息（通常根据用户登录名和密码），然后执行必要的检查和服务，以便将用户身份与相关 IP 地址进行匹配，从而向用户传送经过身份验证的 IP 地址。

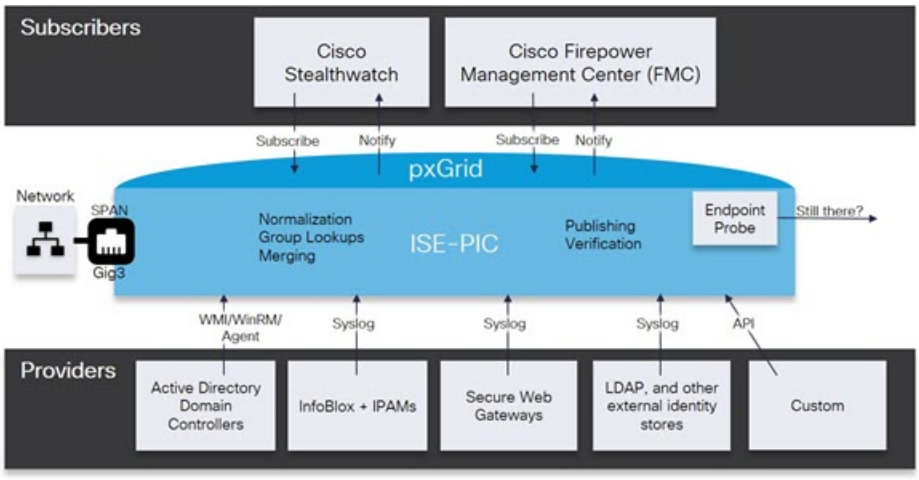
被动身份连接器 (ISE-PIC) 流程

ISE-PIC 的流程如下：

1. 提供程序对用户或终端执行身份验证。
2. 提供程序将经过身份验证的用户信息发送到思科 ISE-PIC。
3. ISE-PIC 将用户信息规范化，执行查找、合并、解析并将其映射到 IP 地址，然后将映射的详细信息发布到 pxGrid。
4. pxGrid 用户接收映射的用户详细信息。

下图说明了ISE-PIC 提供的概要流程。

图 *1:* 概要流程



思科 ISE-PIC 架构、部署和节点

Cisco ISE-PIC 架构包括以下组件：

- 节点 - 在思科 ISE-PIC 部署中，最多可以配置两个节点，如下所述
- 网络资源
- 终端

具有单个 Cisco ISE-PIC 节点的部署称为独立部署。

具有两个思科 ISE-PIC 节点的部署称为高可用性部署，其中一个节点用作主要设备（主管理节点，即 PAN）。高可用性部署可提高服务可用性。

PAN 提供此网络模型所需的所有配置功能，并提供备份角色的辅助思科 ISE 节点（辅助 PAN）功能。辅助节点支持主节点，并在与主节点失去连接时恢复功能。

思科 ISE-PIC 会将位于主思科 ISE-PIC 节点上的所有内容与辅助思科 ISE-PIC 节点同步或进行复制，以确保您的辅助节点与主节点的状态一致（因此可用作备份）。

ISE 社区资源

有关部署和扩展的信息，请参阅ISE 部署历程。

注释 从思科 ISE 版本 3.1开始，所有 pxGrid 连接都必须基于 pxGrid 2.0。基于 pxGrid 1.0（基于 XMPP）的集成将从版本 3.1 开始在思科 ISE 上停止使用。

基于 WebSockets 的 pxGrid 版本 2.0 在思科 ISE 版本 2.4 中引入。我们建议将您的其他系统计划并升级到与 pxGrid 2.0 兼容的版本，以防止对集成造成可能的中断（如有）。

ISE-PIC 的优势

ISE-PIC 为您提供：

- 与各种不同提供程序交互的单一身份解决方案。
- 支持简单配置、监控和故障排除的友好 GUI
- 简单安装和配置
- 轻松升级到 ISE 以进行主动身份验证。从 ISE-PIC 升级到完整 ISE 部署并使用 ISE-PIC 节点创建独立 ISE 部署时，或者将此节点作为主节点添加到现有部署时，ISE 将继续提供升级之前在 ISE-PIC 中可用的所有功能，并将保留您的现有配置。

注释 要升级到 ISE，请下载试用版，或联系您的思科代表以讨论许可选项。

将已升级 ISE-PIC 添加到现有 ISE 部署，但不将其用作主节点时，将覆盖之前的 ISE-PIC 配置。

有关升级流程的完整说明，请参阅将 ISE-PIC 升级到完整 ISE 安装。

比较 ISE-PIC 与 ISE 和 CDA

ISE-PIC 具备许多优势，包括能够平稳轻松地升级到 ISE。除 ISE-PIC 和 ISE 以外，思科还提供一种额外的安全机制，即 CDA。本节在下列表格中对这三种产品进行比较：

- ISE-PIC 与 ISE 的详细比较，第 5 页
- ISE-PIC 与 ISE 和 CDA 的概括比较，第 6 页

ISE-PIC 与 ISE 的详细比较

ISE-PIC 设计为仅共享被动身份，并且不提供任何授权或身份验证服务，这两种服务均由 ISE 提供，ISE 可提供身份验证、授权和记账 (AAA) 服务器。下表中对这两种产品之间的差异进行了详细说明。

表 *1:* 比较 *ISE-PIC* 与 *ISE*

类别	特性	ISE-PIC	ISE
智能许可		-	√
身份验证和授权类型	授权策略	-	√
	TrustSec	-	√
	Active Directory 被动身份验证，包括 WMI	√	√
被动身份源		√	√
	Easy Connect	-	√
	系统日志源	√	√
	REST API 源	√	√
	SPAN	√	√
	安全组交换协议 (SXP)	-	√
	RADIUS，包括 RADIUS 代理	-	√
	自带设备	-	√
	访客	-	√
	安全评估	-	√
	设备管理 (TACACS+)	-	√

类别	特性	ISE-PIC	ISE
pxGrid	pxGrid 控制器	√ 仅适用于思科用户	√
	pxGrid 控制器冗余	√	√
	主题可扩展性	-	√
证书颁发机构 (CA)	pxGrid 证书模板	√	√
	终端 CA	-	√
	安全传输注册 (EST)	-	√
	其他证书模板	-	√
可视性与情景	Context Directory	-	√
	分析	-	√
报告		! **注释** ISE-PIC 提供报告，可用于监控系统运行状况并排除网络中的问题。但是，与 ISE 相比，ISE-PIC 提供一部分功能，因此在 ISE-PIC 中不提供某些 ISE 报告。	√

ISE-PIC 与 ISE 和 CDA 的概括比较

CDA 是一种机制，用于将 IP 地址映射到用户名，以便允许安全网关了解哪个用户使用网络中的哪个 IP 地址，因此这些安全网关现在可根据这些用户（或用户所属的组）制定决策。但是，ISE-PIC 通过访问用户名、MAC 地址和端口等其他数据，可以更精确地收集用户身份。下表概括比较了 ISE-PIC、ISE 和 CDA。

表 *2:* 比较 *ISE-PIC* 与 *ISE* 和 *CDA*

被动身份验证详细信息	完整 ISE	ISE-PIC	CDA
域控制器数量	100	100	80
用户数	20	20	-
WMI（无代理）	是	是	是
Windows 服务器代理可用	是	是	—
需要 DCOM	无 (SPAN)	无 (SPAN)	是
Easy Connect	是	—	-
使用 SPAN 的 Kerberos 嗅探	是	是	—
绑定（IP地址、MAC地址和用户名）	300,000	300,000	64,000