通过 ISE/ISE-PIC 的用户控制

以下主题介绍如何通过 ISE/ISE-PIC 执行用户感知和用户控制：

ISE/ISE-PIC 身份源

您可以将思科身份服务引擎 (ISE) 或 ISE 被动身份连接器 (ISE-PIC) 部署与 Firepower 系统集成到一起，以便将 ISE/ISE-PIC 用于被动身份验证。

ISE/ISE-PIC 是一个授权身份源，并为使用 Active Directory (AD)、LDAP、RADIUS 或 RSA 进行身份验证的用户提供用户感知数据。此外，您还可以对 Active Directory 用户执行用户控制。ISE/ISE-PIC 不报告 ISE 访客服务用户的失败登录尝试或活动。

注释 Firepower 系统不会解析 IEEE 802.1x 计算机身份验证，但会解析 802.1x 用户身份验证。如果将 802.1x 与 ISE 配合使用，则必须包括用户身份验证。802.1x 计算机身份验证不会向可在策略中使用的 FMC 提供用户身份。

有关 Cisco ISE/ ISE-PIC的详细信息，请参阅 Cisco Identity Services Engine Passive Identity Connector 管理员指南。

注释 我们强烈建议您使用最新版本的ISE/ ISE-PIC 获取最新功能集和最多数量的问题修复程序。

源和目标安全组标记 (SGT) 匹配

如果使用 ISE 定义并使用安全组标记 (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。这允许您可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址或网络。

匹配 SGT 标签具有以下优势：

- 管理中心 可以从 ISE 订阅安全组标记交换协议 (SXP) 映射。

  ISE 使用 SXP 将 IP 到 SGT 映射数据库传播到受管设备。当您将 管理中心 配置为使用 ISE 服务器时，必须打开该选项才能从 ISE 侦听 SXP 主题。这会导致 管理中心 直接从 ISE 了解安全组标记和映射。然后，FMC 将 SGT 和映射发布到受管设备。

  SXP 主题接收基于 ISE 与其他 SXP 兼容设备（例如交换机）之间通过 SXP 协议获取的静态和动态映射的安全组标记。

  您可以在 ISE 创建安全组标记，并将主机或网络 IP 地址分配至各标记。您还可以将 SGT 分配给用户账户，并将 SGT 分配给用户流量。如果网络中的交换机和路由器配置为执行此操作，则在数据包进入 ISE（Cisco TrustSec 云) 控制的网络时，这些标记会分配给数据包。

  ISE-PIC 不 支持 SXP。

- 管理中心 和受管设备可以了解 SGT 映射，而无需部署其他策略。（换句话说，您可以在不部署访问控制策略的情况下查看 SGT 映射的连接事件。）

- 支持 Cisco TrustSec，使您能够对网络进行分段，以保护关键业务资产。

- 受管设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

  1. 数据包中定义的源 SGT 标记（如有）。

     对于数据包中的 SGT 标记，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。

     对于数据包中的 SGT 标记，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。

  2. 分配给用户会话的 SGT，从 ISE 会话目录下载。 SGT 可以与源或目标相匹配。

  3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

示例：

- 在 ISE 中，创建名为 Guest Users 的 SGT 标记并将其与 192.0.2.0/24 网络关联。

  例如，您可以将访客用户用作访问控制规则中的源 SGT 条件，并限制访问您网络的任何人对某些 URL、网站类别或网络的访问。

- 在 ISE 中，创建名为 Restricted Networks 的 SGT 标记并将其与 198.51.100.0/8 网络关联。

  例如，您可以使用“受限网络”作为目标 SGT 规则条件，并阻止来自访客用户和具有未经授权访问网络的用户的其他网络的访问。

相关主题

ISE/ISE-PIC 指南和限制，第 3 页

ISE/ISE-PIC 的许可证要求

威胁防御 许可证

任意

经典许可证

控制

ISE/ISE-PIC 的要求和必备条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

ISE/ISE-PIC 指南和限制

请在配置 ISE/ISE-PIC 时使用本节所讨论的准则。

ISE/ISE-PIC 版本和配置兼容性

您的ISE /ISE-PIC 版本和配置会影响其与 Firepower 的集成和交互，如下所示：

- 我们强烈建议您使用最新版本的 ISE/ ISE-PIC 来获取最新的功能集。
- 同步 ISE/ISE-PIC 服务器和 Cisco Secure Firewall Management Center上的时间。否则，系统可能会以意外间隔执行用户超时。
- 要使用 ISE 或 ISE-PIC 数据实施用户控制，请配置并启用担任 pxGrid 角色的 ISE 服务器的领域，如创建 Active Directory 领域和领域目录中所述。
- 每个连接到 ISE 服务器的 Cisco Secure Firewall Management Center主机名必须是唯一的；否则，将丢弃与其中一个 Cisco Secure Firewall Management Center的连接。

- 如果将 ISE/ISE-PIC 配置为监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。

  对于运行版本 6.7 或更高版本的任何设备，您可以选择使用 **configure identity-subnet-filter** 命令限制受管设备监控的子网。有关详细信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。

  或者，您可以配置网络对象并将该对象应用为身份策略中的身份映射过滤器。请参阅创建身份策略。

有关与此版本的系统兼容的 ISE/ISE-PIC 的特定版本，请参阅 思科 Firepower 兼容性指南。

IPv6 支持

- 兼容版本的 ISE/ISE-PIC 版本 2.x 包括对支持 IPv6 的终端的支持。
- 版本 3.0（补丁 2）及更高版本的 ISE/ISE-PIC 启用 ISE/ISE-PIC 与 管理中心 之间的 IPv6 通信。

代理序列

代理序列 是一个或多个可用于与 LDAP、 Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当 思科防御协调器 （CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如， CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。）

虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。

在 ISE 中批准客户端

在 ISE 服务器与 管理中心 成功建立连接之前，您必须手动在 ISE 中批准客户端。（通常有两个客户端：一个用于连接测试，另一个用于 ISE 代理。）

您还可以按照《思科身份服务引擎管理员指南》中关于管理用户和外部身份源的章节中所述，在 ISE 中启用**自动批准新帐户**。

删除无法访问的会话

如果 ISE/ISE-PIC 中的用户会话被报告为无法访问，则 Cisco Secure Firewall Management Center 会删除该会话，因此具有相同 IP 的其他用户无法匹配不可访问的用户的身份规则。
您可以在 ISE/ISE-PIC 中控制此行为，方法是转至**提供程序 (Providers)** > **终端探测器 (Endpoint Probes)** 并点击以下选项之一：

- **启用 (Enabled)**，ISE/ISE-PIC 将监控终端连接，从而导致 Cisco Secure Firewall Management Center 删除无法访问的用户的会话。
- **禁用 (Disabled)**，可导致 ISE/ISE-PIC 忽略终端连接。

安全组标记 (SGT)

安全组标记 (SGT) 指定受信任网络中的流量源的权限。思科 ISE 和思科 TrustSec 使用称为安全组访问 (SGA) 的功能将 SGT 属性实时应用于进入网络的数据包。这些 SGT 对应于 ISE 或 TrustSec

中的用户分配的安全组。如果将 ISE 配置为身份源，则 Firepower 系统可以使用这些 SGT 过滤流量。

安全组标记可以用于源匹配条件和目标匹配访问控制规则的标准。

注释 要仅使用 ISE SGT 属性标记实施用户控制，则无需为 ISE 服务器配置领域。SGT ISE 属性条件可在具有或不具有关联身份策略的策略中进行配置。

注释 在某些规则中，自定义 SGT 条件可匹配带有非 ISE 分配的 SGT 属性标记的流量。这不属于用户控制，并且仅在不使用 ISE/ISE-PIC 作为身份源时才起作用；请参阅自定义 SGT 条件。

除源 SGT 标记外，要匹配目标 SGT 标记，请执行以下操作：

所需的 ISE 版本： 2.6 补丁 6 或更高版本，2.7 补丁 2 或更高版本

路由器支持：任何支持通过以太网 SGT 内联标记的 Cisco 路由器。有关详细信息，请参阅 《Cisco 基于组的策略平台和功能列表》

限制：

- 服务质量（QoS）策略仅使用源 SGT 匹配；它 不 使用目标 SGT 匹配
- RA-VPN 不直接通过 RADIUS 接收 SGT 映射

ISE 和高可用性

当主 ISE / ISE-PIC 服务器发生故障时，会发生以下情况：

由于与 pxGrid v2 集成， 管理中心 已配置 ISE 主机之间的轮询，直到一台主机接受连接。

如果连接丢失， 管理中心 会恢复对连接主机的轮询尝试。

终端位置（或位置 IP）

终端位置属性为 ISE 识别的使用了 ISE 验证用户的网络设备的 IP 地址。

您必须配置和部署身份策略，才能根据**终端位置（位置 IP）**控制流量。

ISE 属性

配置 ISE 连接会使用 ISE 属性数据填充 Cisco Secure Firewall Management Center数据库。对于用户感知和用户控制，可以使用以下 ISE 属性。 SE-PIC 不支持这样做。

终端配置文件（或设备类型）

终端配置文件属性为 ISE 识别的用户终端设备类型。

您必须配置和部署身份策略，才能根据**终端配置文件（设备类型）**控制流量。

如何为用户控制配置 ISE/ISE-PIC

您可以在以下任何配置中使用 ISE/ISE-PIC：

- 具有领域、身份策略和关联的访问控制策略。

  在策略中使用领域来控制用户对网络资源的访问。您仍可以在策略中使用 ISE/ISE-PIC 安全组标记 (SGT) 元数据。

- 仅使用一个访问控制策略。不需要领域或身份策略。

  使用此方法可单独使用 SGT 元数据来控制网络访问。

相关主题

如何在没有领域的情况下配置 ISE， 第 6 页
如何为无领域的用户控制配置 ISE/ISE-PIC， 第 7 页

如何在没有领域的情况下配置 ISE

本主题简要介绍了配置 ISE 以允许或阻止使用 SGT 标记访问网络时所必须完成的任务。

过程

	命令或操作	目的
步骤 1	SGT 匹配：在 ISE 上启用 SXP。	这使 管理中心 能够在 SGT 元数据更改时从 ISE 接收更新。
步骤 2	从 ISE/ISE-PIC 导出系统证书。	在 ISE/ISE-PIC pxGrid、监控 (MNT) 服务器和管理中心之间进行安全连接需要证书。请参阅 从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用， 第 11 页
步骤 3	将证书导入 管理中心。	必须按如下方式导入证书： • pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)**) 的内部证书 • pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部证书 (Internal Certs)**) • MNT 证书：受信任 CA

	命令或操作	目的
步骤 4	创建 ISE/ISE-PIC 身份源。	通过 ISE/ISE-PIC 身份源，您可以使用由 ISE/ISE-PIC 提供的安全组标记 (SGT) 控制用户活动。请参阅配置用户控制 ISE/ISE-PIC，第 14 页。
步骤 5	创建访问控制规则。	访问控制规则指定了在流量与规则条件匹配时要采取的操作（例如，允许或阻止）。您可以将源和目标 SGT 元数据用作访问控制规则中的匹配条件。请参阅访问控制规则简介。
步骤 6	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改。

下一步做什么

从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 11 页

如何为无领域的用户控制配置 ISE/ISE-PIC

开始之前

本主题简要介绍为配置 ISE/ISE-PIC 进行用户控制并允许或阻止用户或组访问网络而必须完成的任务。用户和组可以存储在 领域支持的服务器 中列出的任何服务器上。

过程

	命令或操作	目的
步骤 1	仅目标 SGT：在 ISE 上启用 SXP。	这使 管理中心 能够在 SGT 元数据更改时从 ISE 接收更新。
步骤 2	从 ISE/ISE-PIC 导出系统证书。	在 ISE/ISE-PIC pxGrid、监控 (MNT) 服务器和 管理中心 之间进行安全连接需要证书。请参阅以下内容： • pxGrid 服务器和 MNT 服务器证书：从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 11 页 • pxGrid 客户端证书：生成自签证书，第 13 页
步骤 3	将证书导入 管理中心。	必须按如下方式导入证书： • pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object**

	命令或操作	目的
		Management) > **PKI** > 内部 **CA (Internal CAs)**) 的内部证书 • pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > 内部证书 **(Internal Certs)**) • MNT 证书：受信任 CA
步骤 4	（可选。）创建用于该领域以及 ISE/ISE-PIC 的代理序列。	代理序列 是一个或多个可用于与 LDAP、Active Directory 或 ISE / ISE-PIC 服务器通信的受管设备。仅当思科防御协调器（CDO）无法与 Active Directory 或 ISE / ISE-PIC 服务器通信时，才需要执行此操作。（例如，CDO 可能在公共云中，但 Active Directory 或 ISE / ISE-PIC 可能在私有云中。） 虽然您可以使用一台受管设备作为代理序列，但我们强烈建议您设置两台或更多设备，以便在受管设备无法与 Active Directory 或 ISE / ISE-PIC 通信时，另一台受管设备可以接管。
步骤 5	创建领域。	您必须仅创建一个领域来控制所选择的用户和组对网络的访问。 请参阅创建 Active Directory 领域和领域目录。
步骤 6	下载用户和组并启用领域。	下载用户和组让您能够在访问控制规则中使用它们。请参阅同步用户和组。
步骤 7	创建 ISE/ISE-PIC 身份源。	通过 ISE/ISE-PIC 身份源，您可以使用由 ISE/ISE-PIC 提供的安全组标记 (SGT) 控制用户活动。请参阅配置用户控制 ISE/ISE-PIC，第 14 页。
步骤 8	创建身份策略。	身份策略是一个或多个身份规则的容器。请参阅创建身份策略。
步骤 9	创建身份规则。	身份规则指定了如何使用领域来控制用户和组对网络的访问。请参阅创建身份规则。
步骤 10	将身份策略与访问控制策略相关联。	这会让访问控制策略能够使用领域中的用户和组。

	命令或操作	目的
步骤 11	创建访问控制规则。	访问控制规则指定了在流量与规则条件匹配时要采取的操作（例如，允许或阻止）。您可以将源和目标 SGT 元数据用作访问控制规则中的匹配条件。请参阅访问控制规则简介。
步骤 12	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改。

下一步做什么

从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用 ， 第 11 页

配置 ISE/ISE-PIC

以下主题讨论如何配置 ISE/ISE-PIC 服务器，以便与 管理中心 中的身份策略配合使用。

您必须从 ISE/ISE-PIC 服务器导出证书，以使用 管理中心 进行身份验证并发布 SXP 主题，以便使用 ISE 服务器上的安全组标记 (SGT) 来更新 管理中心。

相关主题

在 ISE 中配置安全组和 SXP 发布 ， 第 9 页
从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用 ， 第 11 页

在 ISE 中配置安全组和 SXP 发布

您必须在思科身份服务引擎 (ISE) 中执行许多配置，才能创建 TrustSec 策略和安全组标记 (SGT)。有关实施 TrustSec 的更完整信息，请参阅 ISE 文档。

以下操作步骤将挑选出必须在 ISE 中配置的核心设置的要点，以便 威胁防御 设备能够下载和应用静态 SGT-IP 地址映射，然后在访问控制规则中用于源 SGT 和目标 SGT 匹配。有关详细信息，请参阅 ISE 文档。

此操作步骤的屏幕截图基于 ISE 2.4。在后续版本中，这些功能的确切路径可能会发生变化，但概念和要求是相同的。虽然建议使用 ISE 2.4 或更高版本（最好是 2.6 或更高版本），但配置应从 ISE 2.2 补丁 1 开始。

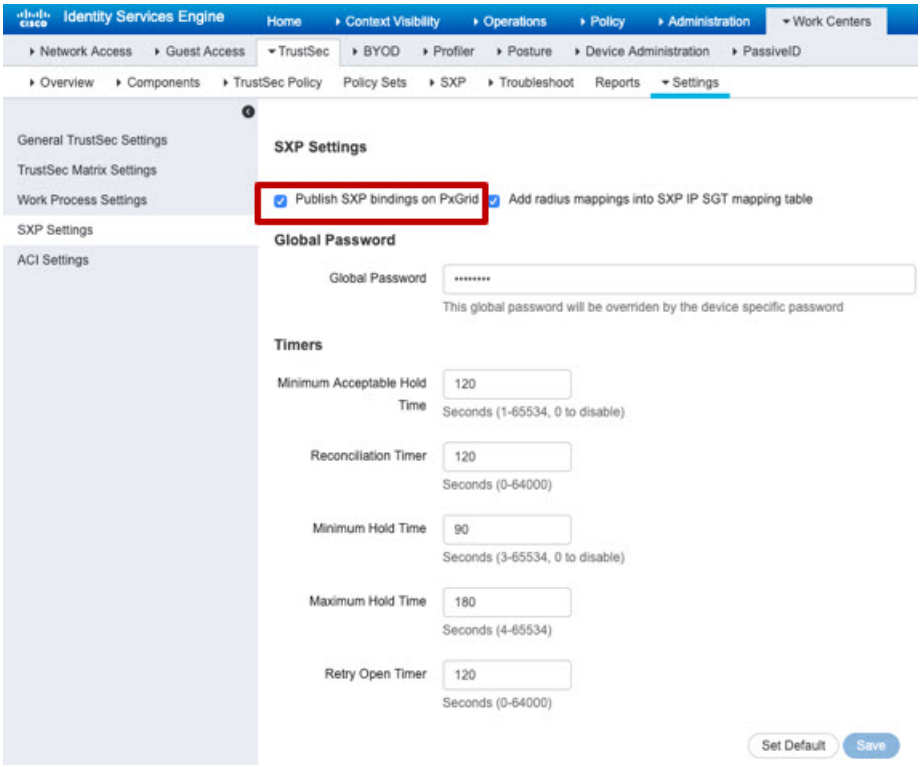
开始之前

您必须拥有 ISE Plus 许可证，才能发布从 SGT 到 IP 地址的静态映射和获取从用户会话到 SGT 的映射，以便 威胁防御 设备可以接收这些映射。

过程

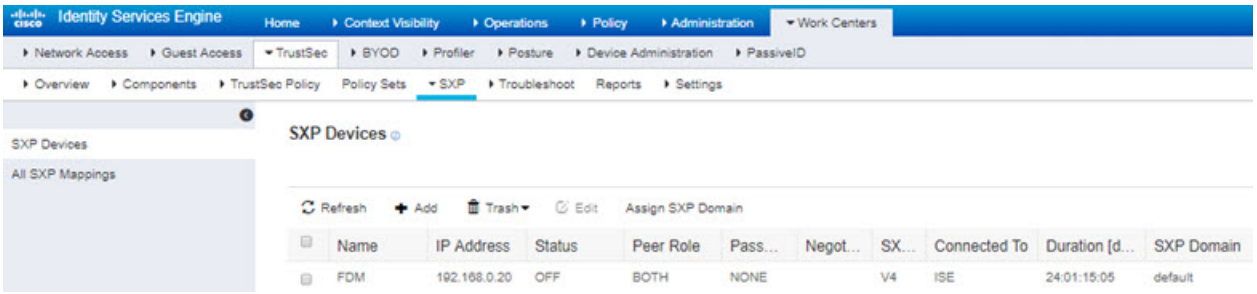
步骤 1 选择工作中心 > **TrustSec** > **设置** > **SXP 设置**，然后选择**在 PxGrid 上发布 SXP 绑定**选项。

选择该选项后，ISE 使用 SXP 发送 SGT 映射。您必须选择此选项， 威胁防御 设备才能“收听”从列表至 SXP 主题等一切内容。必须选择此选项， 威胁防御 设备才能获取静态 SGT-IP 地址映射信息。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则没有必要。

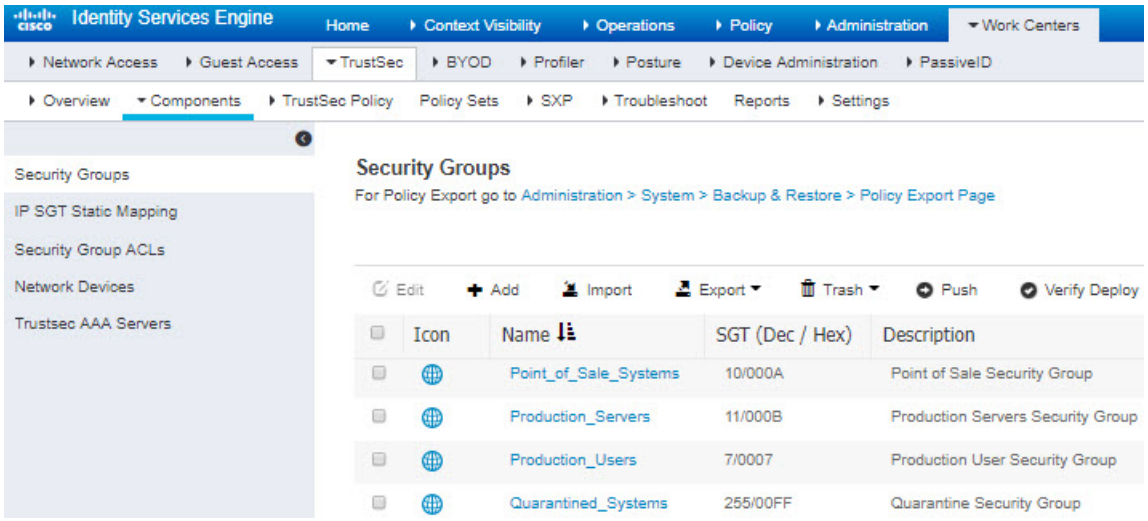


步骤 2 选择工作中心 > **TrustSec** > **SXP** > **SXP 设备**，然后添加设备。

这并不一定是真正的设备，您甚至可以使用 威胁防御 设备的管理 IP 地址。该表只需要至少一台设备来促使 ISE 发布静态 SGT-IP 地址映射。如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。

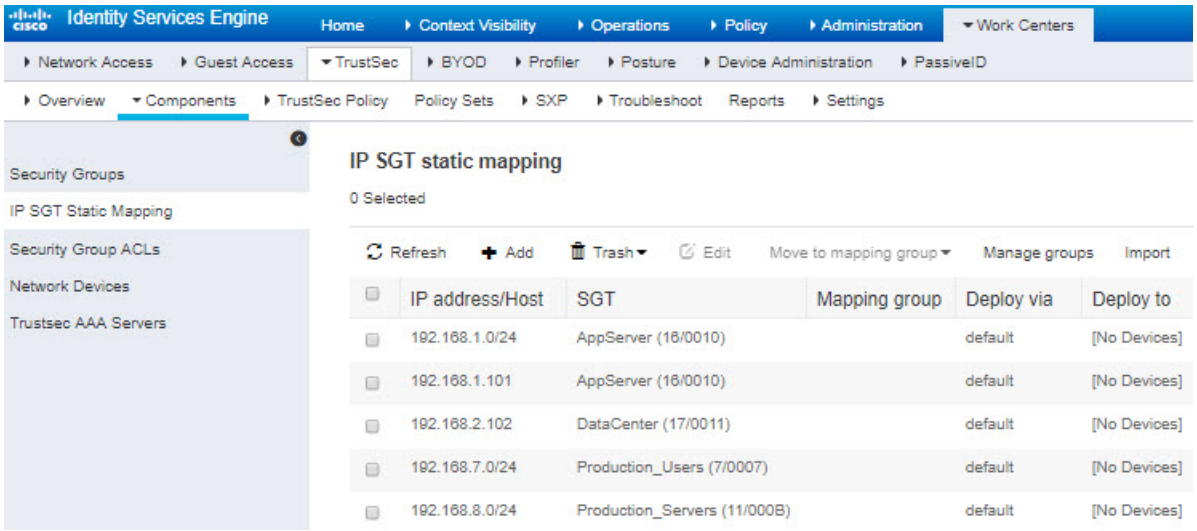


步骤 3 选择工作中心 > **TrustSec** > **组件** > **安全组**并验证是否定义了安全组标记。按需新建。



步骤 4 选择**工作中心** > **TrustSec** > **组件** > **IP SGT 静态映射**，并将主机和网络 IP 地址映射至安全组标记。

如果您仅想使用数据包中定义的 SGT 标记或分配给用户会话的 SGT，则无需执行此步骤。



从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用

以下各节介绍如何：

- 从 ISE / ISE-PIC 服务器导出系统证书。

  这些证书是安全连接到 ISE / ISE-PIC 服务器所必需的。您可能需要导出一个或多达三个证书，具体取决于 ISE 系统的设置方式：

  - pxGrid 服务器的一个证书

- 监控（MNT）服务器一个证书
- 一个证书，包括私钥，用于 pxGrid 客户端（即 管理中心）

  与前两个证书不同，这是一个自签名证书。

- 将这些证书导入 管理中心：
  - pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > 内部 **CA (Internal CAs)**) 的内部证书
  - pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部证书 (Internal Certs)**)
  - MNT 证书：受信任 CA

相关主题

导出系统证书，第 12 页
导入 ISE/ISE-PIC 证书，第 13 页

导出系统证书

您可以导出系统证书或某个证书及其关联的专用密钥。如果您导出证书及其私钥以进行备份，如有必要，您以后也可以重新导入此证书与私钥。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

过程

步骤 1 在思科 ISE GUI 中，点击**菜单**图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 2 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。

步骤 3 选择是仅导出证书，还是导出证书及其关联的私钥。

提示 由于可能会暴露专用密钥值，我们不建议导出与证书关联的专用密钥。如果您必须导出专用密钥（例如，导出要导入其他思科 ISE 节点以用于节点间通信的通配符系统证书时），请指定专用密钥加密密码。在将此证书导入另一思科 ISE 节点时，必须指定此密码以解密专用密钥。

步骤 4 如果您已选择导出私钥，请输入此密码。此密码至少必须包含 8 个字符。

步骤 5 点击 **Export** 以将证书保存至运行客户端浏览器的文件系统。

如果仅导出证书，证书将以 PEM 的格式进行存储。如果同时导出证书和专用密钥，则证书会导出为 .zip 文件，其中包含 PEM 格式的证书和已加密的专用密钥文件。

生成自签证书

通过生成自签证书添加新的本地证书。思科建议仅采用自签证书，以满足内部测试和评估需求。如果计划在生产环境中部署思科 ISE，尽可能使用 CA 签名证书，确保生产网络中更统一地接受。

注释 如果您使用自签名证书并且必须更改思科 ISE 节点的主机名，请登录思科 ISE 节点的管理门户，删除采用旧主机名的自签证书，然后生成新的自签证书。否则，思科 ISE 会继续使用采用旧主机名的自签证书。

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

过程

步骤 1 选择在思科 ISE GUI 中，点击**菜单**图标 (☰) 并选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。

要从辅助节点生成自签证书，请选择**管理 (Administration)** > **系统 (System)** > **服务器证书 (Server Certificate)**。

步骤 2 在 ISE-PIC GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **证书 (Certificates)** > **系统证书 (System Certificates)**。

步骤 3 点击**生成自签证书 (Generate Self Signed Certificate)** 并在显示的窗口中输入详细信息。

步骤 4 根据想要对其使用此证书的服务，选中 **Usage** 区域的复选框。

步骤 5 点击**提交 (Submit)** 生成证书。

要从 CLI 重新启动辅助节点，则按给定顺序输入以下命令：

a) **application stop ise**
b) **application start ise**

导入 ISE/ISE-PIC 证书

此步骤为可选。您还可以在创建 ISE/ISE-PIC 身份源时导入 ISE 服务器证书，如配置用户控制 ISE/ISE-PIC，第 14 页中所述。

开始之前

从 ISE/ISE-PIC 服务器导出证书，如导出系统证书，第 12 页中所述。证书和密钥必须存在于您登录管理中心 的计算机上。

您必须按如下方式导入证书：

- pxGrid 客户端证书：带密钥 (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > 内部 **CA (Internal CAs)**) 的内部证书
- pxGrid 服务器证书：受信任 CA (**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > 内部证书 **(Internal Certs)**)
- MNT 证书：受信任 CA

过程

步骤 1 如果尚未登录，请登录 管理中心。
步骤 2 点击**对象 (Objects)** > **对象管理 (Object Management)**。
步骤 3 展开 **PKI**。
步骤 4 点击 **内部证书**。
步骤 5 点击 **Add Internal Cert**。
步骤 6 按照屏幕上的提示导入证书和私钥。
步骤 7 点击**受信任 CA (Trusted CAs)**。
步骤 8 点击**添加可信 CA**。
步骤 9 按照屏幕上的提示导入 pxGrid 服务器证书。
步骤 10 如有必要，请重复上述步骤，以便导入 MNT 服务器的受信任 CA。

下一步做什么

配置用户控制 ISE/ISE-PIC， 第 14 页

配置用户控制 ISE/ISE-PIC

以下程序讨论如何配置 ISE/ ISE-PIC 身份源。您必须在全局域中才能执行此任务。

开始之前

- 要从 Microsoft Active Directory 服务器或受支持的 LDAP 服务器获取用户会话，请配置并启用 ISE 服务器的领域（假设为 pxGrid 角色），如 创建 Active Directory 领域和领域目录中所述。
- 配置到 ISE 或 ISE-PIC 的连接。有关详细信息，请参阅ISE/ISE-PIC 身份源， 第 1 页和ISE/ISE-PIC 配置字段， 第 16 页。
- 要获得 ISE 中定义的所有映射，包括通过 SXP 发布的 SGT 到 IP 地址的映射，请使用以下程序。或者，您可以选择以下选项：
  - 要想只使用数据包中的 SGT 信息，而不使用从 ISE 下载的映射，请跳过 创建和编辑访问控制规则中讨论的步骤。请注意，在这种情况下，您只能使用 SGT 标记作为源条件；这些标记永远不会匹配目标标准。

- 要仅在数据包和用户-IP-地址/SGT 映射中使用 SGT，请不要订阅 ISE 身份源中的 SXP 主题，也不要将 ISE 配置为发布 SXP 映射。您可以将此信息用于源匹配条件和目标匹配条件。

- 从 ISE/ ISE-PIC 服务器导出证书，也可以选择将其导入到 管理中心 中，如 从 ISE / ISE-PIC 服务器导出证书以在 管理中心 中使用，第 11 页中所述。

过程

步骤 1 登录管理中心。

步骤 2 请点击 **集成** > **其他集成** > **身份源**。

步骤 3 为**服务类型**点击**身份服务引擎**以启用 ISE 连接。

注释 要禁用连接，请点击**无**。

步骤 4 输入**主要主机名/IP 地址**以及**辅助主机名/IP 地址**（后者为可选）。

步骤 5 从 **pxGrid 服务器 CA** 和 **MNT 服务器 CA** 列表中点击相应的证书颁发机构，然后从 **pxGrid 客户端证书** 列表中点击相应的证书。也可以点击 **添加**（+） 来添加证书。

注释 **pxGrid 客户端证书** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

步骤 6 （可选。）使用 CIDR 块符号输入 **ISE 网络过滤器**。

步骤 7 在“订阅”部分中，选中以下项：

- **会话目录主题**，用于从 ISE 服务器接收 ISE 用户会话信息。
- **SXP 主题**，用于接收来自 ISE 服务器的 SGT 到 IP 映射的更新。要在访问控制规则中使用目标 SGT 标记，需要使用此选项。

步骤 8 （可选。）从 **代理** 列表中，点击受管设备或代理序列。
如果 CDO 无法与您的 ISE / ISE-PIC 服务器通信，您可以选择受管设备或代理序列来执行此操作。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

步骤 9 要测试操作，请点击**测试**。

如果测试失败，请点击**其他日志 (Additional Logs)** 以了解有关连接失败的详细信息。

下一步做什么

- 使用创建身份策略中所述的身份策略指定要控制的用户和其他选项。
- 按将其他策略与访问控制相关联中所述，将身份规则与可以过滤和选择性检查流量的访问控制策略相关联。

- 将身份和访问控制策略部署到受管设备，如部署配置更改中所述。
- 监控用户活动，。

相关主题

排除 ISE / ISE-PIC 或 Cisco TrustSec 问题 ，第 17 页
受信任证书颁发机构对象
内部证书对象

ISE/ISE-PIC 配置字段

以下字段用于配置与 /ISE-PIC的连接。

主要和辅助主机名/IP 地址 (Primary and Secondary Host Name/IP Address)

主要和辅助（可选）pxGrid ISE 服务器的主机名或 IP 地址。

您指定的主机名所使用的端口必须可由 ISE 和 管理中心访问。

pxGrid 服务器 CA (pxGrid Server CA)

可信 pxGrid 框架的证书颁发机构。如果部署包括主要和辅助 pxGrid 节点，则两个节点的证书必须由同一证书颁发机构签署。

MNT 服务器 CA (MNT Server CA)

当执行批量下载时 ISE 证书的可信证书颁发机构。如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

pxGrid 客户端证书

Cisco Secure Firewall Management Center 必须向 /ISE-PIC 提供的内部证书和密钥，以连接到 /ISE-PIC 或进行批量下载。

注释 **pxGrid 客户端证书** 必须包含 clientAuth 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。

ISE 网络过滤器 (ISE Network Filter)

一个可选过滤器，可以将其设置为限制 ISE 报告给 Cisco Secure Firewall Management Center的数据。如果提供网络过滤器，则 ISE 会报告来自该过滤器中的网络的数据。可通过以下方式指定过滤器：

- 将此字段留空以指定**任意 (any)** 值。
- 使用 CIDR 符号输入单一 IPv4 地址块。
- 使用由逗号分隔的 CIDR 符号输入 IPv4 地址块列表。

注释 无论您的 ISE 是何版本，此版本的系统均不支持使用 IPv6 地址进行过滤。

订用：

会话目录主题：选中此复选框可从 ISE 服务器订阅用户会话信息。包括 SGT 和终端元数据。

SXP 主题：选中此复选框可从 ISE 服务器订阅 SXP 映射。

代理

如果 CDO 无法与 ISE / ISE-PIC 通信，您可以选择选择受管设备或代理序列。例如，您的 CDO 可能在公共云中，但 ISE / ISE-PIC 服务器可能在内部内联网上。

相关主题

受信任证书颁发机构对象

内部证书对象

排除 ISE / ISE-PIC 或 Cisco TrustSec 问题

排除 Cisco TrustSec 问题

设备接口可以配置为从 ISE/ ISE-PIC 或从网络上的 Cisco 设备（称为 Cisco TrustSec）传播安全组标记 (SGT)。在设备管理页面（**设备** > **设备管理**）上，在设备重新启动后，选中接口的 **传播安全组标记** 复选框。 如果您不希望接口传播 TrustSec 数据，请取消选中此复选框。

排除 ISE/ ISE-PIC 问题

有关其他相关故障排除信息，请参阅领域和用户下载故障排除和用户控制故障排除。

如果您遇到 ISE 或 ISE-PIC 连接问题，请检查以下事项：

- 必须启用 ISE 中的 pxGrid 身份映射功能，才能将 ISE 与 Firepower 系统成功集成。
- 当主服务器出现故障时，您必须手动将辅助服务器升级为主服务器；不会进行自动故障切换。
- 在 ISE 服务器与 管理中心 成功建立连接之前，您必须手动在 ISE 中批准客户端。（通常有两个客户端：一个用于连接测试，另一个用于 ISE 代理。）

  您还可以按照 《思科身份服务引擎管理员指南》中"管理用户和外部身份源"的章节中所述，在 ISE 中启用 **自动批准新帐户** 。
- **pxGrid 客户端证书** 必须包含 **clientAuth** 扩展密钥使用值，或者禁止包含任何扩展密钥使用值。
- ISE 服务器上的时间必须与 Cisco Secure Firewall Management Center上的时间同步。如果设备不同步，系统可能会在非预期时间间隔时执行用户超时。
- 如果部署包括主要和辅助 pxGrid 节点，
  - 则两个节点的证书必须由同一个证书颁发机构签名。
  - ISE 服务器和 管理中心必须可以访问主机名使用的端口。

- 如果部署包括主要和辅助 MNT 节点，则两个节点的证书必须由同一证书颁发机构签署。

要从接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网，请使用 **configure identity-subnet-filter** {**add** | **remove**} 命令。您通常应对内存较低的受管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。

如果您遇到 ISE 或 ISE-PIC 报告的用户数据问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的 ISE 用户的活动后，会从服务器检索其相关信息。ISE 用户发现的活动并非由访问控制规则处理，而且在系统于用户下载中检索到它们的相关信息之前，它们不会显示在 Web 界面中。
- 不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。
- 管理中心不会收到 ISE 访客服务用户的用户数据。
- 如果 ISE 与 TS 代理监控的用户相同，则 管理中心 会划分 TS 代理数据的优先级。如果 TS 代理和 ISE 报告来自同一 IP 地址的相同活动，则仅会将 TS 代理数据记录到 管理中心。
- 您的 ISE 版本和配置会影响您在 Firepower 系统中使用 ISE 的方式。有关详细信息，请参阅 ISE/ISE-PIC 身份源，第 1 页。
- 如果您配置了 管理中心 高可用性并且主管理中心出现故障，请参阅 ISE/ISE-PIC 指南和限制，第 3 页中有关“ISE 和高可用性”的部分。
- ISE-PIC 不提供 ISE 属性数据。
- ISE-PIC 无法执行 ISE ANC 补救。
- 活动 FTP 会话在事件中显示为**Unknown**用户。此为正常现象，因为在活动 FTP 中，会由服务器（而非客户端）发起连接，而 FTP 服务器则不应具有关联的用户名。有关活动 FTP 的详细信息，请参阅 RFC 959。

如果您遇到支持的功能问题，请参阅 ISE/ISE-PIC 身份源，第 1 页 了解版本兼容性的详细信息。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。