ASA 和思科 TrustSec

本章介绍如何为 ASA 实施思科 TrustSec。

关于思科 TrustSec

以往，防火墙等安全功能根据预定义的 IP 地址、子网和协议执行访问控制。然而，随着企业不断向无边界网络过渡，用于连接人员和组织的技术取得了长足的进步，同时对数据保护和网络保护的安全要求也显著提高。同时，终端变得越来越具流动性，而且用户通常利用各种终端（例如，笔记本电脑（而非台式机）、智能手机或平板电脑），这样用户属性结合终端属性一起提供了关键特征（除了现有的基于 6 元组的规则以外），带防火墙功能的交换机和路由器或专用防火墙等实施设备能够可靠地利用这些关键特征制定访问控制决策。

因此，对于支持跨客户网络、在网络的接入层、分发层和核心层以及在数据中心实现安全性，终端属性或客户端身份属性的可用性和传送性已经成为越来越重要的要求。

思科 TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并集成平台上的安全访问服务。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。此信息的可用性和传送性支持在网络的接入层、分发层和核心层实现跨网络安全性。

在环境中实施思科 TrustSec 具备以下优势：

- 提供不断增加的移动和复杂劳动力，他们能够从任何设备进行适当和更安全的访问。
- 针对正在连接有线或无线网络的人员和设备，提供全面的可视性，降低安全风险
- 针对访问物理或云计算型的 IT 资源的网络用户的活动提供优越控制

- 通过高度安全的集中式访问策略管理和可扩展策略实施机制来降低总拥有成本
- 有关详细信息，请访问以下 URL：
  - 面向企业的 Cisco TrustSec 系统和架构的说明。

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
  - 有关在企业中部署 Cisco TrustSec 解决方案的说明，包含组件设计指南的链接。

    http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html
  - 搭配 ASA、交换机、无线 LAN (WLAN) 控制器和路由器使用的思科 TrustSec 解决方案概述。

    http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf
  - 思科 TrustSec 平台支持矩阵，其中列出支持 Cisco TrustSec 解决方案的思科产品。

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

关于思科 TrustSec 中的 SGT 和 SXP 支持

在 Cisco TrustSec 功能中，安全组访问可以将拓扑感知网络转换为基于角色的网络，支持在基于角色的访问控制 (RBAC) 的基础上实施端到端策略。在身份验证期间获得的设备和用户凭证用于按安全组对数据包进行分类。每个进入 Cisco TrustSec 云的数据包都被标记有安全组标记 (SGT)。这种标记有助于可信的中间设备确定数据包的源身份，沿着数据路径实施安全策略。当使用 SGT 定义安全组 ACL 时，SGT 可以指明域上的权限级别。

SGT 通过 IEEE 802.1X 身份验证、Web 身份验证或 MAC 身份验证绕行 (MAB) 分配到设备，被分配的同时带有 RADIUS 供应商特定属性。SGT 可以被静态地分配给特定 IP 地址或交换机接口。在成功进行身份验证之后，SGT 可以被动态地传送到交换机或访问点。

安全组交换协议 (SXP) 是一种为 Cisco TrustSec 开发的协议，用以在不具有（支持 SGT 的）硬件支持的网络设备上将 IP 到 SGT 的映射数据库传送到支持 SGT 和安全组 ACL 的硬件。SXP 为一种控制层面协议，可以将 IP-SGT 映射从身份验证点（例如，旧版接入层交换机）传送到网络中的上游设备。

SXP 连接为点到点的连接，使用 TCP 作为底层传输协议。SXP 使用 TCP 64999 端口启动连接。此外，SXP 连接唯一可通过源 IP 地址和目标 IP 地址被标识。

思科 TrustSec 功能中的角色

为了提供基于身份和策略的访问实施，思科 TrustSec 功能包含以下角色：

- 访问请求者 (AR) - 访问请求者指的是请求访问网络中受保护资源的终端设备。它们是架构的主要主体，其访问权限视身份凭证而定。

  访问请求者包括终端设备，例如计算机、笔记本电脑、移动电话、打印机、摄像机和支持 MACsec 功能的 IP 电话。

- 策略决定点 (PDP) - 策略决定点负责制定访问控制决策。PDP 可以提供 802.1x、MAB 和 Web 身份验证等功能。PDP 通过 VLAN、DACL 和安全组访问 (SGACL/SXP/SGT) 支持身份验证和实施。

  在思科 TrustSec 功能中，思科身份服务引擎 (ISE) 可充当 PDP。思科 ISE 提供身份和访问控制策略功能。

- 策略信息点 (PIP) - 策略信息点是向策略决策点提供外部信息（例如，信誉、位置和 LDAP 属性）的源。

  策略信息点包括 Session Directory、Sensor IPS 和通信管理器等设备。

- 策略管理点 (PAP) - 策略管理点定义策略并将策略插入授权系统。PAP 提供思科 TrustSec 标记到用户身份映射和思科 TrustSec 标记到服务器资源映射，充当一个身份资源库。

  在思科 TrustSec 功能中，思科安全访问控制系统（带集成式 802.1x 和 SGT 支持的策略服务器）充当 PAP。

- 策略实施点 (PEP) - 策略实施点是实施 PDP 为每个 AR 制定的决策（策略规则和操作）的实体。PEP 设备通过网络上的主要通信路径获悉身份信息。PEP 设备从多个来源获悉每个 AR 的身份属性，例如终端代理、授权服务器、对等实施设备和网络流量。反过来，PEP 设备使用 SXP 将 IP-SGT 映射传送到网络上相互信任的对等设备。

  策略实施点包括 Catalyst 交换机、路由器、防火墙（特别是 ASA）、服务器、VPN 设备和 SAN 设备等网络设备。

ASA 在身份架构中充当 PEP 角色。使用 SXP，ASA 可直接从身份验证点获悉身份信息并使用它们来实施基于身份的策略。

安全组策略实施

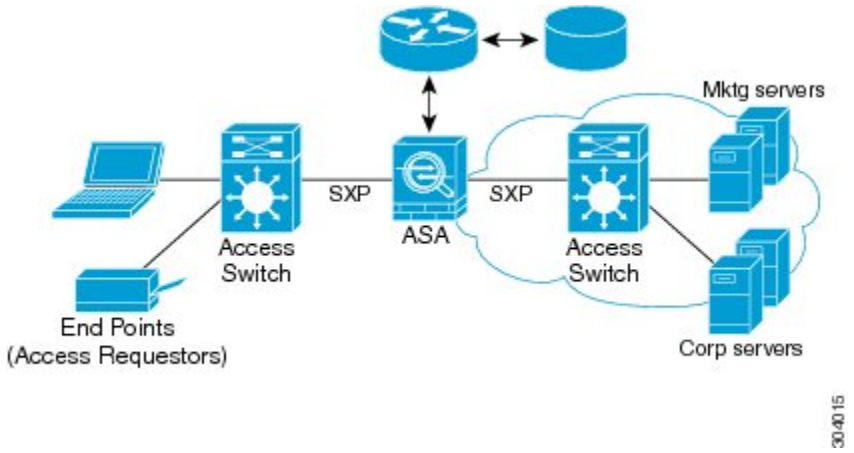
安全策略实施基于安全组名称进行。终端设备尝试访问数据中心中的资源。与在防火墙上配置的基于 IP 的传统策略相比，基于身份的策略基于用户和设备身份配置。例如，允许市场营销承包商访问市场营销服务器；允许市场营销公司用户访问市场营销服务器和公司服务器。

此类部署的优点包括：

- 使用单一对象 (SGT) 简化策略管理定义和实施用户组与资源。
- 在支持思科 TrustSec 的交换机基础设施中保留用户身份和资源身份。

下图显示基于安全组名称的策略实施的部署。

图 *1:* 基于安全组名称的策略实施部署



通过实施思科 TrustSec，可以配置支持服务器分类的安全策略，并且实现以下功能：

- 可以将 SGT 分配给服务器池，以简化策略管理。
- SGT 信息保留在支持思科 TrustSec 的交换机的基础设施中。
- ASA 可使用 IP-SGT 映射跨思科 TrustSec 域执行策略实施。
- 服务器强制要求 802.1x 授权，由此可能简化部署。

ASA 如何实施基于安全组的策略

注释 基于用户的安全策略和基于安全组的策略在ASA中可以共存。网络属性、基于用户的属性和基于安全组的属性的任意组合都能够在安全策略中配置。

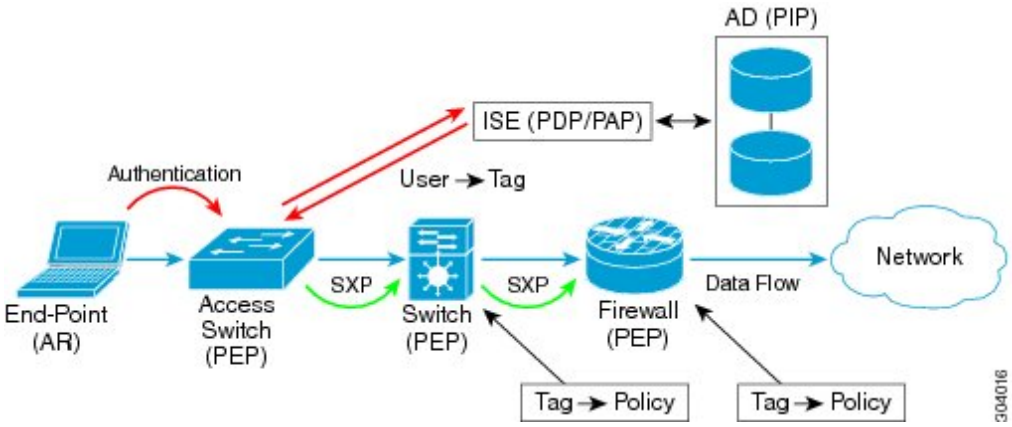
要将 ASA 配置为与思科 TrustSec 协同运行，必须从 ISE 导入受保护的访问凭证 (PAC) 文件。

将 PAC 文件导入到 ASA 会与 ISE 建立安全的通信通道。建立通道后，ASA 会使用 ISE 启动 PAC 安全 RADIUS 事务并下载思科 TrustSec 环境数据（即安全组表）。此安全组表将 SGT 映射到安全组名称。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。

ASA 第一次下载安全组表时会浏览表中的所有条目，并解析在其中配置的安全策略中包含的所有安全组名称；然后，ASA 将在本地激活这些安全策略。如果 ASA 无法解析安全组名称，则会对未知安全组名称生成系统日志消息。

下图显示如何在 Cisco TrustSec 实施安全策略。

图 2: 安全策略实施



1. 终端设备直接或通过远程访问连接到接入层设备，并使用思科 TrustSec 进行身份验证。
2. 通过使用 802.1X 或 Web 身份验证等身份验证方法，接入层设备可以利用 ISE 对终端设备进行身份验证。终端设备传送角色和组成员信息，将此设备划分至相应的安全组。
3. 接入层设备使用 SXP，将 IP-SGT 映射传送到上游设备。
4. ASA 接收数据包并使用 SXP 传送的 IP-SGT 映射查询源与目标 IP 地址的 SGT。

   如果该映射为新映射，ASA 将在其本地 IP-SGT 管理器数据库中记录该映射。IP-SGT 管理器数据库在控制层面中运行，为每个 IPv4 或 IPv6 地址跟踪 IP-SGT 映射。此数据库记录映射被获悉的源。SXP 连接的对等 IP 地址可用作映射源。每个 IP-SGT 映射条目都可以有多个源。

   如果 ASA 被配置为发言者，ASA 会将所有 IP-SGT 映射条目传输到其 SXP 对等体。
5. 如果在 ASA 上配置了包含 SGT 或安全组名称的安全策略，ASA 将实施该策略。（您可以在 ASA 上创建包含 SGT 或安全组名称的安全策略。要基于安全组名称实施策略，ASA 需要使用安全组表将安全组名称映射到 SGT。）

   如果 ASA 在安全组表中找不到安全组名称，但安全策略中包含安全组名称，ASA 会将安全组名称视为未知并生成一条系统日志消息。在 ASA 从 ISE 刷新安全组表并获得安全组名称后，ASA 将生成一条系统日志消息，指示安全组名称已知。

更改 ISE 上安全组的效果

ASA 通过从 ISE 下载更新表定期刷新安全组表。在不同的下载之间，ISE 上的安全组会发生更改。在刷新安全组表之前，ASA 中不会反映这些更改。

提示 我们建议您在维护时段安排在 ISE 上进行策略配置更改，然后手动刷新 ASA 上的安全组表，以确保执行安全组更改。

按这种方式处理策略配置更改，可以最大限度增加安全组名称获得解析和安全策略立即进入活动状态的几率。

当环境数据计时器过期时，系统会自动刷新安全组表。也可以按需触发安全组表刷新。

如果进行 ISE 中的安全组更改，当 ASA 刷新安全组表时会发生以下事件：

- 只有使用安全组名称配置的安全组策略才需要通过安全组表进行解析。包含安全组标记的策略始终处于活动状态。
- 当安全组表首次可用时，浏览所有包含安全组名称的策略，解析安全组名称，激活策略。浏览所有包含标记的策略，并为未知标记生成系统日志。
- 如果安全组表已过期，将继续根据最新下载的安全组表实施策略，直到您清楚或有新表变得可用为止。
- 当ASA上已解析的安全组名称变成未知时，安全策略将被禁用；不过，该安全策略仍然存在于 ASA 运行配置中。
- 如果在 PAP 上删除现有安全组，以前已知的安全组标记会变成未知，但在 ASA 上不会发生策略状态更改。以前已知的安全组名称会变成未解析，然后策略被停用。如果安全组名称被重用，则使用新标记重新编译策略。
- 如果在 PAP 上添加新安全组，以前未知的安全组标记会变成已知，会生成系统日志消息，但策略状态不会发生更改。以前未知的安全组名称变成已解析，然后相关联的策略被激活。
- 如果已在 PAP 上重命名标记，使用标记配置的策略会显示新的标记名称，策略状态不会发生更改。使用此新标记值重新编译使用安全组名称配置的策略。

ASA 中的发言者和收听者

ASA 支持通过 SXP 发送和接收进出其他网络设备的 IP-SGT 映射条目。SXP 允许安全设备和防火墙从访问交换机获悉身份信息，无需硬件升级或更改。SXP 还能够用来将上游设备（例如，数据中心设备）的 IP-SGT 映射条目重新传送到下游设备。ASA 可接受来自上游和下游方向的信息。

在 ASA 上配置 SXP 到 SXP 对等体的连接时，您必须将 ASA 指定为该连接的发言者或收听者，这样才能交换身份信息：

- 发言者模式 - 配置 ASA，使其可以将 ASA 中收集的所有活动 IP-SGT 映射条目转发到上游设备进行策略实施。
- 收听者模式 - 配置 ASA，使其可以接收来自下游设备（支持 SGT 的交换机）的 IP-SGT 映射条目，并可使用该信息创建策略定义。

如果将SXP连接的一端配置为说话者，必须将另一端配置为收听者，反之亦然。如果位于SXP连接两端的两个设备均配置为同一角色（同为发言者或同为收听者），则SXP连接失败，ASA将生成一条系统日志消息。

多个 SXP 连接能够获悉已从 IP-SGT 映射数据库下载的 IP-SGT 映射条目。在 ASA 上建立 SXP 到 SXP对等体的连接后，收听者将从发言者下载完整的IP-SGT映射数据库。此后发生的所有更改仅在网络上出现新设备时被发送。因此，SXP信息流速率与终端主机对网络进行身份验证的速率成比例。

已通过 SXP 连接获悉的IP-SGT 映射条目在 SXP IP-SGT 映射数据库中进行维护。可以通过不同 SXP 连接获悉相同映射条目。此映射数据库为每个已获悉的映射条目维护一个副本。同一IP-SGT映射值

的多个映射条目按获悉映射的连接的对等 IP 地址进行标识。SXP 请求 IP-SGT 管理器在首次获悉新映射时添加映射条目，并在删除 SXP 数据库中的最后副本时删除映射条目。

无论 SXP 连接何时被配置为说话者，SXP 都请求 IP-SGT 管理器将在设备上收集的所有映射条目转发给对等体。当在本地获悉新映射时，IP-SGT 管理器请求 SXP 通过已配置为说话者的连接转发此映射。

将 ASA 同时配置为 SXP 连接的发言者和收听者可能会导致形成 SXP 循环，这意味着最初传输 SXP 数据的 SXP 对等体可以接收这些数据。

将 ASA 注册到 ISE

在 ISE 中，必须首先将 ASA 配置为认可的思科 TrustSec 网络设备，ASA 才能成功导入 PAC 文件。要将 ASA 注册到 ISE，请执行以下步骤：

过程

步骤 1 登录 ISE。

步骤 2 依次选择 **Administration** > **Network Devices** > **Network Devices**。

步骤 3 点击 **Add**。

步骤 4 输入 ASA 的 IP 地址。

步骤 5 当 ISE 用于进行用户身份验证时，请在 Authentication Settings 区域输入一个共享密钥。

在 ASA 上配置 AAA 服务器时，需提供您此时在 ISE 上创建的共享密钥。ASA 上的 AAA 服务器要与 ISE 通信需使用此共享密钥。

步骤 6 为 ASA 指定设备名称、设备 ID、密码和下载间隔。有关如何执行这些任务的详细信息，请参阅 ISE 文档。

在 ISE 上创建安全组

在配置 ASA 以便与 ISE 通信时，需指定 AAA 服务器。在 ASA 上配置 AAA 服务器时，必须指定服务器组。必须配置安全组，使其使用 RADIUS 协议。要在 ISE 上创建安全组，请执行以下步骤：

过程

步骤 1 登录 ISE。

步骤 2 依次选择 **Policy** > **Policy Elements** > **Results** > **Security Group Access** > **Security Group**。

步骤 3 为 ASA 添加安全组。（安全组是全局性的，并非 ASA 特定的。）

ISE 在 Security Groups 下创建带有标记的条目。

步骤 4 在 Security Group Access 区域，为 ASA 配置设备 ID 凭证和密码。

生成 PAC 文件

要生成 PAC 文件，请执行以下步骤。

注释 PAC 文件包括允许 ASA 和 ISE 保护两者之间进行的 RADIUS 交易的共享密钥。因此，请确保将其安全地存储于 ASA 中。

过程

步骤 1 登录 ISE。

步骤 2 依次选择 **Administration** > **Network Resources** > **Network Devices**。

步骤 3 从设备列表中选择 ASA。

步骤 4 在 Security Group Access (SGA) 下方点击 **Generate PAC**。

步骤 5 要加密 PAC 文件，请输入密码。

为加密 PAC 文件而输入的密码（或加密密钥）独立于在 ISE 上被配置为设备凭证的一部分的密码。

ISE 生成 PAC 文件。ASA 可通过 TFTP、FTP、HTTP、HTTPS 或 SMB 从闪存或远程服务器导入 PAC 文件。（导入 PAC 文件之前，不必一定将其置于 ASA 闪存中。）

思科 TrustSec 准则

本节包括在配置思科 TrustSec 之前应查看的准则和限制。

故障转移

- 在主/主和主/备配置下，您可以在 ASA 上配置基于安全组的策略。
- 如果故障转移配置中涉及 ASA，则必须将 PAC 文件导入主 ASA 设备。另外，还必须刷新主设备上的环境数据。
- ASA 可与为实现高可用性 (HA) 而配置的 ISE 通信。
- 您可以在 ASA 上配置多个 ISE 服务器，如果无法连接第一个服务器，会继续连接下一个服务器，以此类推。然而，如果服务器列表被下载为 Cisco TrustSec 环境数据的一部分，它将被忽略。

- 如果 ASA 中从 ISE 下载的 PAC 文件到期且无法下载更新的安全组表，ASA 将继续基于上次下载的安全组表实施安全策略，直到 ASA 下载更新的表。

集群

- 如果故障转移配置中涉及 ASA，则必须将 PAC 文件导入控制单元。
- 如果故障转移配置中涉及 ASA，则必须刷新控制单元上的环境数据。

IPv6

对于 IPv6 和支持 IPv6 的网络设备，ASA 支持 SXP。AAA 服务器必须使用 IPv4 地址。

第 2 层 SGT 实施

- 仅支持物理接口、子接口、和 EtherChannel 接口。
- 不支持逻辑接口或虚拟接口，例如 BVI。
- 不支持采用 SAP 协商和 MACsec 的链路加密。
- 不支持故障转移链路。
- 不支持集群控制链路。
- 如果 SGT 更改，ASA 不会对现有的流量重新分类。任何根据以前 SGT 指定的策略决定对流量寿命依然有效。不过，ASA 可立即反映传出数据包上的 SGT 更改，即便数据包所属的流量是基于以前的 SGT 进行分类。
- Firepower 1010 交换机端口和 VLAN 接口不支持第 2 层安全组标记实施。

其他准则

- ASA 支持 SXP 版本 3。ASA 与支持 SXP 的不同网络设备协商 SXP 版本。
- 您可以将 ASA 配置为在 SXP 调和计时器到期时刷新安全组表，也可以根据需要下载安全组表。从 ISE 更新 ASA 中的安全组表时，更改也会反映到相应的安全策略中。
- Cisco TrustSec 在单一情景和多情景模式中支持 Smart Call Home 功能，但在系统情景模式中不支持此功能。
- 只能将 ASA 配置为在单一思科 TrustSec 域中实现互通。
- ASA 不支持设备中 SGT-名称映射的静态配置。
- SXP 消息不支持 NAT。
- SXP 在网络中将 IP-SGT 映射传送到实施点。如果接入层交换机与实施点分属不同的 NAT 域，该交换机上传的 IP-SGT 映射则无效，而且在实施设备上进行的 IP-SGT 映射数据库查找不会显示有效的结果。因此，ASA 无法在实施设备上应用安全组感知型安全策略。

- 您可以为 ASA 配置默认密码以用于 SXP 连接，也可以选择不使用密码；不过 SXP 对等体不支持使用特定于连接的密码。配置的默认 SXP 密码应当在部署网络中保持一致。如果配置连接特定密码，连接可能会失败，并且显示警告消息。如果使用默认密码配置连接，但未配置默认密码，则结果与不使用密码配置连接时的结果相同。
- 可以将 ASA 配置为 SXP 发言者或收听者，或者同时配置为两者。但是，当某台设备与对等体之间存在双向连接，或是设备属于单向连接设备链的一部分时，可能会形成 SXP 连接循环。（ASA 可从数据中心的接入层获悉资源的 IP-SGT 映射。ASA 可能需要将这些标记传送到下游设备。）SXP 连接环路会导致 SXP 消息传输出现意外行为。如果 ASA 被配置为发言者和收听者，可能会形成 SXP 连接循环，导致最初发送 SXP 数据的对等体接收这些数据。
- 在更改 ASA 本地 IP 地址时，必须确保所有 SXP 对等体均已更新其对等体列表。另外，如果 SXP 对等体更改其 IP 地址，必须确保这些更改反映到 ASA 中。
- 不支持自动 PAC 文件调配。ASA 管理员必须从 ISE 管理界面请求 PAC 文件，再将其导入 ASA。
- PAC 文件有过期日期。在当前的 PAC 文件到期前必须导入更新的 PAC 文件，否则 ASA 将无法检索环境数据更新。如果 ASA 中从 ISE 下载的 PAC 文件到期且无法下载更新的安全组表，ASA 将继续基于上次下载的安全组表实施安全策略，直到 ASA 下载更新的表。
- 如果 ISE 中的安全组发生更改（例如被重命名或删除），ASA 不会更改包含与已更改安全组相关联的 SGT 或安全组名称的任何 ASA 安全策略之状态；但 ASA 会生成一条系统日志消息，指示这些安全策略已更改。
- 在 ISE 1.0 中不支持组播类型。
- SXP 连接在通过 ASA 互连的两个 SXP 对等体之间处于正在初始化的状态，如下例所示：

```
(SXP peer A) - - - - (ASA) - - - (SXP peer B)
```

因此，在将 ASA 配置为与思科 TrustSec 集成时，必须在 ASA 中启用 no-NAT、no-SEQ-RAND 和 MD5-AUTHENTICATION TCP 选项以便配置 SXP 连接。为 SXP 对等体之间以 SXP 端口 TCP 64999 为目标的流量创建 TCP 状态绕行策略。然后，在相应的接口上应用该策略。

例如，以下命令集显示如何为 TCP 状态绕行策略配置 ASA：

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
```

```
service-policy global_policy global
```

将 ASA 配置为与思科 Trustsec 集成

要配置 ASA 与思科 TrustSec 集成，请执行以下任务。

开始之前

在配置 ASA 与思科 TrustSec 集成之前，必须在 ISE 中完成以下任务：

- 将 ASA 注册到 ISE，第 7 页
- 在 ISE 上创建安全组，第 7 页
- 生成 PAC 文件，第 8 页

过程

步骤 1 配置 AAA 服务器以便与思科 TrustSec 集成，第 11 页

步骤 2 导入 PAC 文件，第 13 页

步骤 3 配置安全交换协议，第 14 页

此任务会为 SXP 启用和设置默认值。

步骤 4 添加 SXP 连接对等体，第 17 页

步骤 5 刷新环境数据，第 18 页

请根据需要执行任务。

步骤 6 配置安全策略，第 18 页

步骤 7 配置第 2 层安全组标记实施，第 20 页

配置 AAA 服务器以便与思科 TrustSec 集成

本节介绍如何为 Cisco TrustSec 集成 AAA 服务器。要在 ASA 上配置 AAA 服务器组以便与 ISE 通信，请执行以下步骤。

开始之前

- 引用的服务器组必须配置为使用 RADIUS 协议。如果向 ASA 中添加非 RADIUS 服务器，配置将会失败。

- 如果也使用 ISE 进行用户验证，请获取将 ASA 注册到 ISE 时在 ISE 上输入的共享密钥。请联系 ISE 管理员，以获取此信息。

过程

步骤 1 为 ASA 创建 AAA 服务器组并配置 AAA 服务器参数，以便与 ISE 服务器通信。

aaa-server *server-tag* **protocol radius**

示例：

```
ciscoasa(config)# aaa-server ISEserver protocol radius
```

server-tag 参数指定服务器组名称。

步骤 2 从 aaa 服务器组配置模式中退出。

exit

示例：

```
ciscoasa(config-aaa-server-group)# exit
```

步骤 3 将 AAA 服务器配置为 AAA 服务器组的一部分，设置主机特定连接数据。

```
ciscoasa(config)# aaa-server server-tag(interface-name) host server-ip
```

示例：

```
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
```

interface-name 参数指定 ISE 所驻留的网络接口。需要在此参数中使用圆括号。*server-tag* 参数是 AAA 服务器组的名称。*server-ip* 参数指定 ISE 服务器的 IP 地址。

步骤 4 指定向 ISE 服务器验证 ASA 的服务器密钥值。

key *key*

示例：

```
ciscoasa(config-aaa-server-host)# key myexclusivekey
```

key 参数为字母数字关键字，最长为 127 个字符。

如果也使用 ISE 进行用户验证，请输入将 ASA 注册到 ISE 时在 ISE 上输入的共享密钥。

步骤 5 从 AAA 服务器主机配置模式中退出。

exit

示例：

```
ciscoasa(config-aaa-server-host)# exit
```

步骤 6 标识被 Cisco TrustSec 用于环境数据检索的 AAA 服务器组。

cts server-group *AAA-server-group-name*

示例：

```
ciscoasa(config)# cts server-group ISEserver
```

AAA-server-group-name 参数为您在步骤 1 中在 *server-tag* 参数中指定的 AAA 服务器组的名称。

注释
您可以在 ASA 上只为思科 TrustSec 配置一个服务器组实例。

以下示例显示如何为思科 TrustSec 集成配置 ASA 以便与 ISE 服务器通信：

```
ciscoasa(config)#aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

导入 PAC 文件

本节介绍如何导入 PAC 文件。

开始之前

- ASA 在 ISE 中必须被配置为认可的思科 TrustSec 网络设备，才能生成 PAC 文件。
- 在 ISE 上生成 PAC 文件时，请获取用于加密此文件的密码。ASA 需要使用此密码来导入和解密 PAC 文件。
- 导入后，PAC 文件会驻留在 NVRAM 中。在 HA 模式下运行时，如果正确配置故障转移和有状态链路，将 PAC 文件导入活动单元后，就会复制到辅助单元。由于导入的文件驻留在 NVRAM 中，因此每当设备重启时，例如软件升级后，必须再次导入文件。
- 设备使用单个 PAC 文件。如果导入多个 PAC 文件，则每个导入的 PAC 文件都会替换之前导入的文件。
- ASA 需要访问 ISE 生成的 PAC 文件。ASA 可通过 TFTP、FTP、HTTP、HTTPS 或 SMB 从闪存或远程服务器导入 PAC 文件。（导入 PAC 文件之前，无需将其置于 ASA 闪存中。）
- 系统已为 ASA 配置服务器组。

过程

导入 Cisco TrustSec PAC 文件。

cts import-pac *filepath* **password** *value*

示例：

```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

value 参数指定用于加密 PAC 文件的密码。此密码与 ISE 上配置为设备凭证一部分的密码无关。输入 *filepath* 参数作为下列选项之一：

单模式

- **disk0**：disk0 上的路径和文件名
- **disk1**：disk1 上的路径和文件名
- **flash**：闪存上的路径和文件名
- **ftp**：FTP 上的路径和文件名
- **http**：HTTP 上的路径和文件名
- **https**：HTTPS 上的路径和文件名
- **smb**：SMB 上的路径和文件名
- **tftp**：TFTP 上的路径和文件名

多模式

- **http**：HTTP 上的路径和文件名
- **https**：HTTPS 上的路径和文件名
- **smb**：SMB 上的路径和文件名
- **tftp**：TFTP 上的路径和文件名

以下示例显示如何将 PAC 文件导入 ASA：

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

配置安全交换协议

您需要启用和配置安全交换协议 (SXP)，才能使用思科 Trustsec。

开始之前

至少必须有一个接口处于 UP/UP 状态。如果启用 SXP 时所有接口均处于关闭状态，ASA 不会显示消息来表示该 SXP 没有运行或无法启用。如果通过输入 **show running-config** 命令来检查配置，此命令输出则显示以下消息：

```
"WARNING: SXP configuration in process, please wait for a few moments and try again."
```

过程

步骤 1 在 ASA 上启用 SXP。默认情况下，SXP 被禁用。

cts sxp enable

示例：

```
ciscoasa(config)# cts sxp enable
```

步骤 2 （可选，不推荐。）为 SXP 连接配置默认源 IP 地址。

cts sxp default source-ip *ipaddress*

示例：

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

ipaddress 参数是 IPv4 或 IPv6 地址。

当为 SXP 配置默认源 IP 地址时，必须指定与 ASA 出站接口相同的地址。如果源 IP 地址不匹配出站接口的地址，SXP 连接将失败。

如果未配置 SXP 连接的源 IP 地址，ASA 将执行路由/ARP 查询来确定 SXP 连接的出站接口。我们建议您不要为 SXP 连接配置默认源 IP 地址，并允许 ASA 执行路由/ARP 查询来确定 SXP 连接的源 IP 地址。

步骤 3 （可选。）配置用于对 SXP 对等体进行 TCP MD5 身份验证的默认密码。默认情况下，SXP 连接无密码。

cts sxp default password [**0** | **8**] 密码

示例：

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

当且仅当配置 SXP 连接对等体来使用默认密码时配置一个默认密码。

密码的长度取决于解密级别，如果未指定，则默认为 0：

- **0**- 未加密的明文形式。密码最长为 80 个字符。
- **8**- 加密的文本。密码最长为 162 个字符。

步骤 4 （可选。）指定 ASA 尝试在 SXP 对等体之间设置新 SXP 连接的时间间隔。

cts sxp retry period *timervalue*

示例：

```
ciscoasa(config)# cts sxp retry period 60
```

ASA 将继续尝试进行连接，直到成功建立连接，尝试失败后则等待重试之前的重试间隔。您可以指定重试期间，范围介于 0 到 64000 秒之间。默认值为 120 秒。如果指定 0 秒，ASA 则不会尝试连接到 SXP 对等体。

我们建议您将重试计时器配置为不同于其 SXP 对等体的值。

步骤 5 （可选。）指定调和计时器的值。

cts sxp reconciliation period *timervalue*

示例：

```
ciscoasa(config)# cts sxp reconciliation period 60
```

在 SXP 对等体终止其 SXP 连接后，ASA 将启动抑制计时器。如果 SXP 在抑制计时器运行时进行连接，ASA 将启动调和计时器；然后，ASA 将更新 SXP 映射数据库来获取最新映射。

在调和计时器过期后，ASA 将扫描 SXP 映射以识别过时的映射条目（以前的连接会话获取的内容）。ASA 会将这些连接标记为过时。在调和计时器过期后，ASA 将从 SXP 映射数据中删除过时的条目。

您可以指定调和期间，范围介于 1 到 64000 秒之间。默认值为 120 秒。

步骤 6 （可选。）配置在 SXP 对等体终止其 SXP 连接后从某个对等体获知的 IP-SGT 映射的删除抑制计时器。

cts sxp delete-hold-down period *timervalue*

计时器的值指定了在删除从非活动状态的 SXP 连接获知的 IP-SGT 映射之前将其保留的秒数 (120-64000)。

示例：

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

每个 SXP 连接都与一个删除抑制计时器相关联。当侦听程序端的 SXP 连接不活动时，就会触发此计时器。从该 SXP 连接获知的 IP SGT 映射不会被立即删除。相反，它们将被保留，直到删除抑制计时器到期。此计时器到期时删除该映射。

步骤 7 （可选。）配置 IPv4 子网在充当使用 SXPv2 或更低版本的对等体的发言者时的扩展深度。

cts sxp mapping network-map *maximum_hosts*

如果对等体使用 SXPv2 或更低版本，则该对等体无法将 SGT 扩展至子网绑定。ASA 可以将 IPv4 子网绑定扩展到各个主机绑定（IPv6 绑定不进行扩展）。此命令指定一个子网绑定可生成的最大主机绑定数。

您可以指定最大数量，范围介于0到65535之间。默认值为0，意味着子网绑定未扩展至主机绑定。

添加 SXP 连接对等体

如要添加 SXP 连接对等体，请执行以下步骤：

过程

建立与 SXP 对等体的 SXP 连接。

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **none**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

示例：

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

SXP 连接按 IP 地址设置；一个设备对可以服务于多个 SXP 连接。

peer_ip_address 参数为 SXP 对等体的 IPv4 或 IPv6 地址。对等体 IP 地址必须可从 ASA 传出接口访问。

source_ip_ad 参数是 SXP 连接的本地 IPv4 或 IPv6 地址。源 IP 地址必须与 ASA 出站接口相同，否则连接将失败。

我们建议您不要为 SXP 连接配置源 IP 地址，并允许 ASA 执行路由/ARP 查询来确定 SXP 连接的源 IP 地址。

指示是否使用 SXP 连接的身份验证密钥：

- **default** - 使用为 SXP 连接配置的默认密码。
- **none** - 对 SXP 连接不使用密码。

指示 SXP 连接模式：

- **local** - 使用本地 SXP 设备。
- **peer** - 使用对等 SXP 设备。

指示 ASA 是作为 SXP 连接的发言者还是收听者。

- **speaker** - ASA 可将 IP-SGT 映射转发到上游设备。
- **listener** - ASA 可接收来自下游设备的 IP-SGT 映射。

以下示例显示如何在 ASA 上配置 SXP 对等体：

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default
```

```
mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default
mode peer speaker
```

刷新环境数据

ASA 从 ISE 下载环境数据，ISE 中包括安全组标记 (SGT) 名称表。在 ASA 上完成以下任务后，ASA 将自动刷新从 ISE 获取的环境数据：

- 将 AAA 服务器配置为与 ISE 通信。
- 从 ISE 导入 PAC 文件。
- 标识 ASA 用于检索思科 TrustSec 环境数据的 AAA 服务器组。

通常，无需手动刷新来自 ISE 的环境数据；然而，安全组会在 ISE 上发生更改。在刷新 AAA 安全组表中的数据之前，这些更改不会反映到 ASA 上，所以在 ASA 上刷新数据可确保将在 ISE 上进行的任何安全组更改都反映到 ASA 上。

注释 我们建议您在 ISE 上安排策略配置更改，并于维护期间在 ASA 上手动刷新数据。按这种方式处理策略配置更改，可尽可能地提高安全组名称被解析以及安全策略在 ASA 上立即处于活动状态的可能性。

要刷新环境数据，请执行以下步骤：

过程

刷新来自 ISE 的环境数据，将协调计时器重置为已配置的默认值。

```
cts refresh environment-data
```

示例：

```
ciscoasa(config)# cts refresh environment-data
```

配置安全策略

可以在许多 ASA 功能中加入思科 TrustSec 策略。任何使用扩展 ACL（除非在本章列为不支持）的功能都能够利用思科 TrustSec。可以将安全组参数添加到扩展 ACL 以及基于网络的传统参数中。

- 要配置扩展 ACL，请参阅添加扩展 ACE 执行基于安全组的匹配（思科 TrustSec）。

- 要配置可在 ACL 中使用的安全组对象组，请参阅配置安全组对象组。

例如，访问规则通过网络信息允许或拒绝接口上的流量。通过思科 TrustSec，可以根据安全组控制访问。例如，可以为 sample_securitygroup1 10.0.0.0 255.0.0.0 创建访问规则，这意味着，安全组可以拥有 10.0.0.0/8 子网上的任何 IP 地址。

可以根据安全组名称（服务器、用户、非受管设备等等）、基于用户的属性和基于 IP 地址的传统对象（IP 地址、Active Directory 对象和 FQDN）构成的组合配置安全策略。安全组成员能够扩展到角色以外，将设备和位置属性包含在内，并且不受用户组成员约束。

以下示例显示如何创建一个使用在本地定义的安全对象组的 ACL：

```
object-group security objgrp-it-admin
   security-group name it-admin-sg-name
   security-group tag 1
object-group security objgrp-hr-admin
   security-group name hr-admin-sg-name  // single sg_name
   group-object it-admin     // locally defined object-group as nested object
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
object-group security objgrp-hr-network
security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

通过配置访问组或模块化策略框架，可激活上一个示例中配置的 ACL。

其他示例：

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53

!match src hr-admin-sg-name from host 10.1.1.1 to dst any
access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any

!match src tag 22 from any network to dst hr-servers-sg-name any network
access-list idfw-acl permit ip security-group tag 22 any security-group
name hr-servers-sg-name any

!match src user mary from any host to dst hr-servers-sg-name any network
access-list idfw-acl permit ip user CSCO\mary any security-group
name hr-servers-sg-name any

!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
access-list idfw-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers any

!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24
! to dst objgrp-hr-servers any network
access-list idfw-acl permit ip user CSCO\Jack object-group-security
objgrp-hr-network 10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

!match src user Tom from security-group mktg any google.com
object network net-google
fqdn google.com
access-list sgacl permit ip sec name mktg any object net-google

! If user Tom or object_group security objgrp-hr-admin needs to be matched,
! multiple ACEs can be defined as follows:
```

```
access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin
    10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any
```

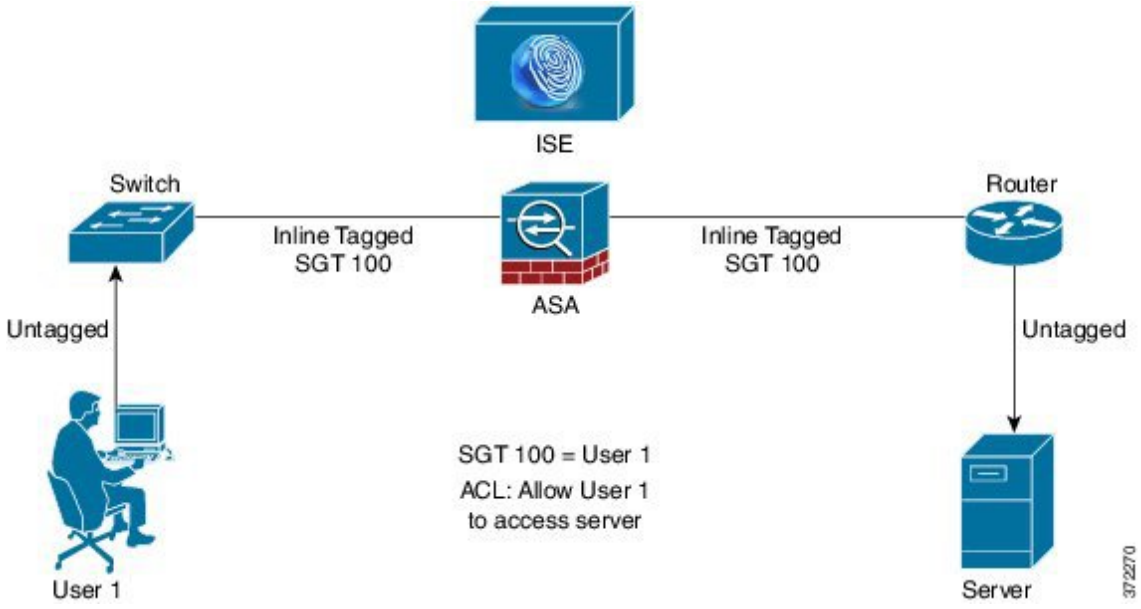
配置第 2 层安全组标记实施

Cisco TrustSec 可以对每个网络用户和资源进行标识和身份验证，并分配一个称为安全组标记 (SGT) 的 16 位数字。转而，此标识符会传送到网络跃点之间，从而允许 ASA、交换机和路由器等中间设备基于此身份标记实施策略。

SGT 加以太网标记（也称为第 2 层 SGT 实施）使 ASA 能够使用思科专有的以太网帧 (EtherType 0x8909)（允许向纯文本以太网帧中插入源安全组标记）在以太网接口上收发安全组标记。ASA 可基于手动每接口配置在传出数据包中插入安全组标记，并处理传入数据包中的安全组标记。此功能允许跨网络设备对终端身份进行内联逐跳传送，在每个跃点之间提供无缝的第 2 层 SGT 实施。

下图显示第 2 层 SGT 实施的典型示例。

图 *3:* 第 *2* 层 *SGT* 实施



使用场合

下表介绍配置此功能时入口流量的预期行为。

表 *1:* 入口流量

接口配置	收到的已标记数据包	收到的未标记数据包
未发出命令。	数据包被丢弃。	SGT 值来自 IP-SGT 管理器。
发出 **cts manual** 命令。	SGT 值来自 IP-SGT 管理器。	SGT 值来自 IP-SGT 管理器。

接口配置	收到的已标记数据包	收到的未标记数据包
同时发出 **cts manual** 命令和 **policy static sgt** *sgt_number* 命令。	SGT 值来自 **policy static sgt** *sgt_number* 命令。	SGT 值来自 **policy static sgt** *sgt_number* 命令。
同时发出 **cts manual** 命令和 **policy static sgt** *sgt_number* **trusted** 命令。	SGT 值来自数据包中的内联 SGT。	SGT 值来自 **policy static sgt** *sgt_number* 命令。

注释 如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为“Unknown”使用预留 SGT 值“0x0”。

下表介绍配置此功能时出口流量的预期行为。

表 *2:* 出口流量

接口配置	发送的已标记或未标记数据
未发出命令。	未标记
发出 **cts manual** 命令。	已标记
同时发出 **cts manual** 命令和 **propagate sgt** 命令。	已标记
同时发出 **cts manual** 命令和 **no propagate sgt** 命令。	未标记

下表介绍配置此功能时流向设备的流量和流出设备的流量的预期行为。

表 *3:* 传入和传出流量

接口配置	接收的已标记或未标记数据包
未在进口接口上为流向设备的流量发出命令。	数据包被丢弃。
在进口接口上为流向设备的流量发出 **cts manual** 命令。	数据包已被接受，但没有策略实施或 SGT 传送
未发出 **cts manual** 命令，或者在出口接口上为流出设备的流量同时发出 **cts manual** 命令和 **no propagate sgt** 命令。	未标记数据包被发送，但没有策略实施。SGT 号管理器。
已发出 **cts manual** 命令，或者在出口接口上为流出设备的流量发出 **cts manual** 命令和 **propagate sgt** 命令。	已标记数据包被发送。SGT 号来自 IP-SGT 管理

注释 如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为“Unknown”使用预留 SGT 值“0x0”。

在接口上配置安全组标记

要在接口上配置安全组标记，请执行以下步骤：

过程

步骤 1 指定接口并输入接口配置模式。

interface *id*

示例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

步骤 2 启用第 2 层 SGT 实施，然后进入 cts 手动接口配置模式。

cts manual

示例：

```
ciscoasa(config-if)# cts manual
```

步骤 3 在接口上启用安全组标记传送。默认情况下，传送被启用。

propagate sgt

示例：

```
ciscoasa(config-if-cts-manual)# propagate sgt
```

步骤 4 将策略应用于手动配置的 CTS 链路中。

policy static sgt *sgt_number* [**trusted**]

示例：

```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

static 关键字指定应用到链路上的传入流量的 SGT 策略。

sgt *sgt_number* 关键字参数对指定要应用于来自对等体的传入流量的 SGT 号。有效值为 2 到 65519。

trusted 关键字指明接口上具有在命令中指定的 SGT 的进口流量不应使其 SGT 被覆盖。默认设置为 Untrusted。

以下示例为第 2 层 SGT 实施启用接口并定义此接口是否可信：

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

手动配置 IP-SGT 绑定

要手动配置 IP-SGT 绑定，请执行以下步骤：

过程

手动配置 IP-SGT 绑定。

cts role-based sgt-map {*IPv4_addr*[/*mask*] | *IPv6_addr*[/*prefix*]} **sgt** *sgt_value*

示例：

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

可以指定 IPv4 或 IPv6 主机地址。另外，也可以通过包含子网掩码或前缀值（对于 IPv6）指定网络地址，例如 10.100.10.0/24。*sgt_value* 是 SGT 编号，范围介于 2 到 65519 之间。

故障排除提示

使用 **packet-tracer** 命令确定为何特定会话被允许或被拒绝，正在使用哪个 SGT 值（来自数据包中的 SGT，来自 IP-SGT 管理器，或来自在接口上配置的 **policy static sgt** 命令），以及应用了哪些基于安全组的安全策略。

以下示例显示 **packet-tracer** 命令的输出，以显示到 IP 地址的安全组标记映射：

```
ciscoasa# packet-tracer input inside tcp inline-tag 100
security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

使用 **capture** *capture-name* **type inline-tag** *tag* 命令仅捕获带或不带特定 SGT 值的思科 CMD 数据包 (EtherType 0x8909)。

以下示例显示 **show capture** 命令针对指定的 SGT 值的输出：

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

思科 TrustSec 示例

以下示例显示如何配置 ASA 以使用思科 TrustSec：

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
cts server-group cts-server-list
// Configure SXP peers
cts sxp enable
cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
security-group name hr-admin-sg-name
group-object it-admin
object-group security objgrp-hr-servers
security-group name hr-servers-sg-name
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
   interface gi0/1
   cts manual
   propagate sgt
   policy static sgt 100 trusted
   cts role-based sgt-map 10.1.1.100 sgt 50
```

Secure Client VPN 支持思科 TrustSec

ASA 支持对 VPN 会话应用安全组标记。可以使用外部 AAA 服务器向 VPN 会话分配安全组标记 (SGT)，也可以通过为本地用户或 VPN 组策略配置安全组标记来向 VPN 会话分配安全组标记。然后，可以在第 2 层以太网上通过思科 TrustSec 系统传送此标记。安全组标记适用于组策略，当 AAA 服务器无法提供 SGT 时可用于本地用户。

以下是向 VPN 用户分配 SGT 的典型步骤：

1. 用户连接到使用 AAA 服务器组（包含 ISE 服务器）的远程访问 VPN。
2. ASA 从 ISE 请求可能包括 SGT 的 AAA 信息。ASA 也为用户通过隧道传输的流量分配 IP 地址。
3. ASA 使用 AAA 信息对用户进行身份验证，并创建隧道。
4. ASA 使用 AAA 信息中的 SGT 和分配的 IP 地址向第 2 层报头中添加一个 SGT。
5. 包含 SGT 的数据包传递到 Cisco TrustSec 网络中的下一个对等设备。

如果来自 AAA 服务器的属性中没有可分配给 VPN 用户的 SGT，ASA 将使用组策略中的 SGT。如果组策略中也没有 SGT，则会分配标记 0x0。

注释 此外，您也可以通过 ISE 授权变更 (CoA) 将 ISE 用于策略实施。有关如何配置策略实施的信息，请参阅 VPN 配置指南。

向远程访问 VPN 组策略和本地用户添加 SGT

要在远程访问 VPN 组策略中配置 SGT 属性，或在 VPN 策略中为 LOCAL 用户数据库中定义的用户配置 SGT 属性，请执行以下步骤。

没有用于组策略或本地用户的默认 SGT。

过程

步骤 1 要在远程访问 VPN 组策略上配置 SGT，请执行以下操作：

a) 进入组策略配置模式：

group-policy *name*

示例：

```
ciscoasa(config)# group policy Grpolicy1
```

b) 为组策略配置 SGT。

security-group-tag {**none** | **value** *sgt*}

如果使用 **value**设置标记，该标记的范围可介于 2 到 65519 之间。指定 **none** 可设置无 SGT。

示例：

```
ciscoasa(config-group-policy# security-group-tag value 101
```

步骤 2 要为 LOCAL 数据库中的用户配置 SGT，请执行以下操作：

a) 如果需要，请创建用户。

username *name* {**nopassword** | **password** *password* [**encrypted**]} [**privilege** *priv_level*]}

示例：

```
ciscoasa(config)# username newuser password changeme encrypted privilege 15
```

b) 进入用户名配置模式。

username *name* **attributes**

示例：

```
asa3(config)# username newuser attributes
```

```
asa3(config-username)#
```

c) 为用户配置 SGT。

security-group-tag {**none** | **value** *sgt*}

如果使用 **value**设置标记，该标记的范围可介于 2 到 65519 之间。指定 **none** 可设置无 SGT。

示例：

```
ciscoasa(config-username)# security-group-tag value 101
```

监控 Cisco TrustSec

请参阅以下commands来监控思科 TrustSec：

- **show running-config cts**
- **show running-config** [**all**] **cts role-based** [**sgt-map**]

  此命令显示用户定义的 IP-SGT 绑定表条目。
- **show cts sxp connections**

  此命令显示使用多情景模式时，ASA 上特定用户情景的 SXP 连接。
- **show conn security-group**

  显示所有 SXP 连接的数据。
- **show cts environment-data**

  显示 ASA 上安全组表中包含的思科 TrustSec 环境信息。
- **show cts sgt-map**

  显示控制路径中的 IP 地址安全组表管理器条目。
- **show asp table cts sgt-map**

  此命令显示数据路径内维护的 IP 地址安全组表映射数据库中的 IP 地址安全组表映射条目。
- **show cts pac**

  显示从 ISE 导入到 ASA 的 PAC 文件的相关信息，并包括 PAC 文件已过期或 30 天内即将过期的警告消息。

思科 TrustSec 的历史记录

表 *4:* 思科 *TrustSec* 的历史记录

功能名称	平台版本	说明
思科 TrustSec	9.0(1)	Cisco TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并将集成平台上的安全访问服务集成在一个平台上。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。 在此版本中，ASA 与思科 TrustSec 集成提供基于安全组的策略实施。Cisco TrustSec 域中的访问策略不受拓扑影响，基于源和目标设备的角色，而非基于网络 IP 地址。 ASA 可对其他类型的基于安全组的策略（例如应用检测）使用思科 TrustSec，例如可配置包含基于安全组的访问策略的类映射。 引入或修改了以下命令：**access-list extended**、 **cts sxp enable**、 **cts server-group**、**cts sxp default**、**cts sxp retry period**、**cts sxp reconciliation period**、**cts sxp connection peer**、**cts import-pac**、**cts refresh environment-data**、**object-group security**、**security-group**、**show running-config cts**、**show running-config object-group**、**clear configure cts**、**clear configure object-group**、**show cts pac**、**show cts environment-data**、**show cts environment-data sg-table**、**show cts sxp connections**、**show object-group**、**show configure security-group**、**clear cts environment-data**、**debug cts,** 和 **packet-tracer**。
第 2 层安全组标记实施	9.3(1)	现在，可以使用结合了以太网标记的安全组标记来实施策略。SGT 加以太网标记（也称为第 2 层 SGT 实施）使 ASA 能够使用思科专有的以太网帧 (EtherType 0x8909)（允许向纯文本以太网帧中插入源安全组标记）在以太网接口上收发安全组标记。 引入或修改了以下命令：**cts manual**、**policy static sgt**、**propagate sgt**、**cts role-based sgt-map**、**show cts sgt-map**、**packet-tracer**、**capture**、**show capture**、**show asp drop**、**show asp table classify**、**show running-config all**、**clear configure all** 和 **write memory**。
思科 Trustsec 支持安全交换协议 (SXP) 版本 3。	9.6(1)	ASA 上的思科 Trustsec 现在实施 SXPv3，其中启用了比主机绑定更加高效的 SGT 到子网绑定。 引入或修改了以下命令：**cts sxp mapping network-map**、**cts role-based sgt-map**、**show cts sgt-map**、**show cts sxp sgt-map**、**show asp table cts sgt-map**。

功能名称	平台版本	说明
Trustsec SXP 连接可配置删除抑制计时器	9.8(3)	默认 SXP 连接抑制计时器为 120 秒。现在，您可以配置此计时器，范围介于 120 到 64000 秒之间。 新增/修改的命令：**cts sxp delete-hold-down period**、**show cts sxp connection brief** 和 **show cts sxp connections**

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。