对象

对象是可重用容器，用于定义在策略或其他设置中要使用的条件。例如，网络对象定义主机和子网地址。

对象允许您定义条件，这样即可在不同策略中重新使用相同的条件。在更新对象时，将自动更新使用该对象的所有策略。

对象类型

可以创建以下类型的对象。在大多数情况下，如果策略或设置允许使用对象，则必须使用对象。

对象类型	主要用途	说明
AnyConnect 客户端配置文件	远程访问 VPN。	AnyConnect 客户端 配置文件随 AnyConnect 客户端 软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及是否允许最终用户更改 AnyConnect 客户端 首选项和高级设置中的选项。 请参阅配置并上传客户端配置文件。
应用过滤器	访问控制规则。	应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。 请参阅配置应用过滤器对象，第 8 页。
证书	身份策略。 远程访问 VPN。 SSL 解密规则。 管理 Web 服务器。	数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。 请参阅配置证书。

对象类型	主要用途	说明
DNS 组	管理和数据接口的 DNS 设置。	DNS 组定义 DNS 服务器列表和某些相关联的属性。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。 请参阅配置 DNS 组。
事件列表过滤器	选定日志记录目标的系统日志记录设置。	事件列表过滤器创建用于系统日志消息的过滤器列表。您可以使用它们来限制发送到特定日志记录位置（例如系统日志服务器或内部日志缓冲区）的消息。 请参阅配置事件列表过滤器。
地理位置	安全策略。	地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。 请参阅配置地理位置对象，第 11 页。
身份源	身份策略。 远程访问 VPN。 设备管理器访问。	身份源是定义用户账户的服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程访问 VPN 连接或到设备管理器的访问进行身份验证。 请参阅身份源。
IKE 策略	VPN。	互联网密钥交换 (IKE) 策略对象定义用于对 IPsec 对等体进行身份验证、协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的 IKE 提议。IKEv1 和 IKEv2 有单独的对象。 请参阅配置全局 IKE 策略。
IPsec 提议	VPN。	IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。 请参阅配置 IPsec 提议。
网络	安全策略和各种设备设置。	网络组和网络对象（统称为“网络对象”）定义主机或网络的地址。 请参阅配置网络对象和组，第 4 页。
端口	安全策略。	端口组和端口对象（统称为“端口对象”）定义流量的协议、端口或 ICMP 服务。 请参阅配置端口对象和组，第 6 页。
密钥	Smart CLI 和 FlexConfig 策略。	密钥对象定义要加密和隐藏的密码或其他身份验证字符串。 请参阅配置密钥对象。

对象类型	主要用途	说明
安全区	安全策略。	安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。 请参阅配置安全区，第 7 页。
SGT 组	访问控制策略。	Trustsec 安全组标记 (SGT) 定义思科身份服务引擎 (ISE) 中定义的流量标记。您必须先配置ISE，然后才能创建这些对象。接下来，您可以将对象用作访问控制规则中的源/目的地匹配条件。 请参阅配置安全组标记 (SGT) 组，第 13 页。
SLA 监控器	静态路由。	SLA 监控器定义用于监控静态路由的目标 IP 地址。如果监控器确定无法再访问目标 IP 地址，则系统可安装备用静态路由。 请参阅配置 SLA 监控器对象。
SSL 密码	SSL 设置。	SSL 密码对象定义在建立与 威胁防御的 SSL 连接时可以使用的安全级别、TLS/DTLS 协议版本和加密算法的组合。在系统设置中使用这些对象为与设备建立 TLS/SSL 连接的用户定义安全要求。 请参阅配置 TLS/SSL 密码设置。
系统日志服务器	访问控制规则。 诊断日志记录。 安全智能策略。 SSL 解密规则。 入侵策略。 文件/恶意软件策略	系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。 请参阅配置系统日志服务器，第 12 页。
URL	访问控制规则。 安全智能策略。	URL 对象和组（统称为“URL 对象”）定义网络请求的 URL 或 IP 地址。 请参阅配置 URL 对象和组，第 10 页。
用户	远程访问 VPN。	您可以直接在设备上创建与远程访问 VPN 搭配使用的用户账户。您可以使用本地用户账户代替外部身份验证源，或与后者搭配使用。 请参阅配置本地用户。

管理对象

您可以直接通过“对象”(Objects) 页面配置对象，也可以在编辑策略时进行配置。两种方法得到的结果相同：新对象或更新的对象，所以请使用当下符合您需求的方法。

以下程序介绍如何直接通过“对象”(Objects) 页面创建和管理对象。

注释 在编辑策略或设置时，如果属性需要对象，系统将会为您显示已定义的对象列表，从中您可以选择适当的对象。如果所需的对象不存在，只需点击列表中所示的**创建新对象 (Create New Object)** 链接即可。

过程

步骤 1 选择**对象**。

“对象”(Objects) 页面有一个目录，其中列出了可用的对象类型。在选择对象类型时，您会看到现有对象的列表，并可在此处创建新对象。另外，还可看到对象内容和类型。

步骤 2 从目录中选择对象类型，并执行以下任一操作：

- 要创建对象，请点击 **+** 按钮。对象的内容视类型而异；有关每个对象类型的具体信息，请参阅配置主题。
- 要创建组对象，请点击**添加组** () 按钮。组对象包含多个项目。
- 要编辑对象，请点击该对象的编辑图标 ()。无法编辑预定义对象的内容。
- 要删除对象，请点击该对象的删除图标 ()。如果某个策略或其他对象目前正在使用对象，或者对象为预定义对象，则无法将其删除。

配置网络对象和组

使用网络组和网络对象（统称为“网络对象”）可定义主机或网络的地址。然后，您可以在安全策略中使用这些对象来定义流量匹配条件，或在设置中使用它们来定义服务器或其他资源的地址。

网络对象定义单个主机或网络地址，而网络组对象可以定义多个地址。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑地址属性时，点击对象列表中所示的**创建新网络 (Create New Network)** 链接来创建网络对象。

过程

步骤 1 选择**对象**，然后从目录中选择**网络**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击**添加组** () 按钮。
- 要编辑某个对象或组，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 输入对象的名称和说明（后者为可选项），并定义对象内容。

我们建议不要单独使用 IP 地址作为名称，以便您可以轻松地从对象内容或独立 IP 地址中识别对象名称。如果您想要在名称中使用 IP 地址，请添加一个有意义的前缀，例如 host-192.168.1.2 或 network-192.168.1.0。如果您使用 IP 地址作为名称，系统会添加一条竖线作为前缀，例如 |192.168.1.2. 设备管理器 不会在对象选择器中显示这条竖线，但如果您在 CLI 中使用 **show running-config** 命令检查运行配置，您将看到此命名标准。

步骤 4 配置对象的内容。

网络对象

选择对象**类型**并配置内容：

- **网络** - 使用以下格式之一输入网络地址：
  - IPv4 网络（包含子网掩码），例如 10.100.10.0/24 或 10.100.10.0/255.255.255.0。
  - IPv6 网络（包括前缀），例如 2001:DB8:0:CD30::/60。
- **主机** - 使用以下格式之一输入主机 IP 地址：
  - IPv4 主机地址，例如 10.100.10.10。
  - IPv6 主机地址，例如 2001:DB8::0DB8:800:200C:417A 或 2001:DB8:0:0:0DB8:800:200C:417A。
- **范围** - 地址范围，起始地址和终止地址用连字符分隔。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。例如，192.168.1.10-192.168.1.250 或 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100。
- **FQDN** - 输入完全限定域名，例如 www.example.com。不能使用通配符。此外，请选择 **DNS 解析**确定是否要将 IPv4 地址、IPv6 地址，或这两个地址与 FQDN 关联。默认值为 IPv4 和 IPv6 这两个地址。只能在访问控制规则中使用这些对象。规则匹配通过 DNS 查找获取的 FQDN IP 地址。

网络组

点击 + 按钮，以选择要添加到组中的网络对象或组。另外，也可以创建新对象。

步骤 5 点击**确定 (OK)**，保存更改。

配置端口对象和组

使用端口组和端口对象（统称为“端口对象”）可定义流量的协议、端口或 ICMP 服务。然后，可以在安全策略中使用这些对象来定义流量匹配条件，例如使用访问规则来允许流量传送至特定 TCP 端口。

端口对象定义单一协议、TCP/UDP 端口、端口范围或 ICMP 服务，而端口组对象可定义多项服务。

该系统中包括多个针对通用服务的预定义对象。您可以在策略中使用这些对象，但无法编辑或删除系统定义的对象。

注释 在创建端口组对象时，请确保合理组合对象。例如，如果在访问规则中使用某个对象指定源端口和目标端口，则不能在该对象中混合使用多个协议。在编辑已使用的对象时请务必小心，否则可能导致使用该对象的策略无效（和被禁用）。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑服务属性时，点击对象列表中所示的**创建新端口**链接来创建端口对象。

过程

步骤 1 选择**对象**，然后从目录中选择**端口**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击**添加组** ( ) 按钮。
- 要编辑某个对象或组，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的名称和说明（后者为可选项），并定义对象内容。

端口对象

选择**协议**，然后按以下所示配置该协议：

- **TCP**、**UDP** - 输入单一端口或端口范围编号，例如 80（适用于 HTTP）或 1-65535（涵盖所有端口）。
- **ICMP**、**IPv6-ICMP** - 选择 ICMP **类型**和**代码**（可选）。选择 **Any** 类型可应用于所有 ICMP 消息。有关类型和代码的信息，请参阅以下页面：
  - ICMP -http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6 -http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **其他** - 选择所需协议。

端口组

点击 + 按钮，以选择要添加至该组的端口对象。另外，也可以创建新对象。

步骤 4 点击**确定 (OK)**，保存更改。

配置安全区

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

系统将在初始配置期间创建以下区域。您可以编辑这些区域以添加或移除接口；如果不再使用这些区域，也可以删除它们。

- **inside_zone** - 包括内部接口。如果内部接口为网桥组，则此区域包括所有网桥组成员接口，而不是内部网桥虚拟接口 (BVI)。此区域用于表示内部网络。
- **outside_zone** - 包括外部接口。此区域用于表示在您控制之外的网络，例如互联网。

通常，按接口在网络中扮演的角色对它们分组。例如，可将连接至互联网的接口放在 **outside_zone** 安全区，并将内部网络的所有接口放在 **inside_zone** 安全区。然后，可以对来自外部区域和传至内部区域的流量应用访问控制规则。

在创建区域之前，请考虑要应用至网络的访问规则和其他策略。例如，无需将所有内部接口都放到同一个区域。如果您有 4 个内部网络，并希望将其中一个与另外三个区别对待，则可以创建两个区域（而不是一个区域）。如果有一个接口需允许外部访问公共 Web 服务器，您可能希望对该接口使用单独的区域。

以下步骤程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑安全区属性时，点击对象列表中所示的**创建新安全区**链接来创建安全区。

过程

步骤 1 选择**对象**，然后从目录中选择**安全区**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 选择区域的**模式**。

模式与接口模式直接关联。区域可以包含一种类型的接口。

- **路由 (Routed)** - 路由接口是可应用安全策略的直通流量的正常接口。

- **被动 (Passive)** - 被动接口不影响流经设备的流量。

步骤 5 在**接口**列表中，点击 **+** 并选择要添加到该区域的接口。

列表中将显示当前不在该区域的所有已命名接口。只有配置接口并为其指定了名称，才能将其添加到该区域。

如果所有已命名接口均已在该区域内，则列表为空。如果要尝试将某个接口移到其他区域，则首先必须将其从当前区域中删除。

注释 您不能将网桥组接口 (BVI) 添加到某个区域，而只能添加成员接口。您可以将成员接口放到不同的区域中。

步骤 6 点击**确定 (OK)**，保存更改。

配置应用过滤器对象

应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。

虽然您可以指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

您可以直接在策略中选择应用和应用过滤器，而不使用应用过滤器对象。但是，如果要为同一组应用或过滤器创建多个策略，使用对象则非常方便。该系统包括多个预定义的应用过滤器，您不能编辑或删除它们。

注释 思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑访问控制规则时，在向“应用”(Applications) 选项卡中添加应用条件后点击**另存为过滤器 (Save As Filter)** 链接来创建应用过滤器对象。

开始之前

编辑过滤器时，如果所选应用已由 VDB 更新删除，则会在应用名称后显示“（已弃用）”。必须从过滤器中删除这些应用，否则将阻止后续部署和系统软件升级。

过程

步骤 1 选择**对象**，然后从目录中选择**应用过滤器**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 在**应用 (Applications)** 列表中，点击**添加 +** 并选择要添加到该对象的应用和过滤器。

初始列表将在连续滚动的列表中显示应用。点击**高级过滤器 (Advanced Filter)** 可查看过滤器选项，可更加方便地查看和选择应用。完成选择后，点击**添加 (Add)**。您可以重复该过程，以添加更多应用或过滤器。

注释 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。

风险

应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性

在组织的业务运营环境（非娱乐性）下使用应用的可能性，从非常低到非常高。

类型

应用类型：

- **应用协议** - 应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议** - 客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。
- **Web 应用** - Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别

说明应用的最基本功能的应用通用分类。

标记

关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 **SSL 协议**的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将**已解密的流量**标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表（显示屏底部）

在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。如果您计划添加特定应用，请从此列表中选择它们。

步骤 5 点击**确定 (OK)**，保存更改。

配置 URL 对象和组

使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全智能策略中进行阻止。

URL 对象定义单个 URL 或 IP 地址，而 URL 组对象可以定义多个 URL 或地址。

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配。然后，如果满足以下任一条件，则 URL 被视为匹配项：
  - 字符串位于 URL 的开头。
  - 字符串后面有一个点。
  - 字符串开头包含一个点。
  - 字符串后面跟有 :// 字符。

  例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。

注释 我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站（即，带有 / 字符的 URL），因为这样可能会重组服务器并将页面移至新路径。

- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

  但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑 URL 属性时，点击对象列表中所示的**创建新 URL** 链接来创建 URL 对象。

过程

步骤 1 选择**对象**，然后从目录中选择 **URL**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击**添加组** () 按钮。
- 要编辑某个对象或组，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 定义对象内容。

URL 对象

在 **URL** 框中输入 URL 或 IP 地址。在 URL 中不能使用通配符。

URL 组

点击 + 按钮选择要添加到组中的 URL 对象。另外，也可以创建新对象。

步骤 5 点击**确定 (OK)**，保存更改。

配置地理位置对象

地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。例如，使用地理位置可以很容易地将访问权限限制为特定国家/地区，而无需知道此处使用的所有潜在 IP 地址。

通常，可以直接在策略中选择地理位置，而无需使用地理位置对象。但是，如果要为同一组国家/地区或大洲创建多个策略，使用对象则非常方便。

注释 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑网络属性时，点击对象列表中所示的**创建新地理位置 (Create New Geolocation)** 链接来创建地理位置对象。

过程

步骤 1 选择**对象**，然后从目录中选择**地理位置**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 在**大洲/国家/地区 (Continents/Countries)** 列表中，点击**添加 + (Add +)** 并选择要添加到该对象的大洲和国家/地区。

选择大洲将会选择该大洲内的所有国家/地区。

步骤 5 点击**确定 (OK)**，保存更改。

配置系统日志服务器

系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。如果已为日志收集和分析设置一台系统日志服务器，请创建对象以进行定义并在相关策略中使用这些对象。

可以将下列类型的事件发送至系统日志服务器：

- 连接事件。根据下列策略类型配置系统日志服务器对象：访问控制规则和默认操作、SSL 解密规则和默认操作、安全智能策略。
- 入侵事件。根据入侵策略配置系统日志服务器对象。
- 诊断事件。请参阅配置系统将日志记录发送到远程系统日志服务器。
- 文件/恶意软件事件。在**设备** > **系统设置** > **日志记录设置**中配置系统日志服务器。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑系统日志服务器属性时，点击对象列表中所示的**添加系统日志服务器**链接来创建系统日志服务器对象。

过程

步骤 1 选择**对象**，然后从目录中选择**系统日志服务器**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。

- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 配置系统日志服务器的属性：

- **IP 地址** - 输入系统日志服务器的 IP 地址。
- **协议类型、端口号** - 选择用于系统日志的协议并输入端口号。默认值为 UDP/514。如果您选择 **TCP**，系统可以识别何时系统日志服务器不可用，并停止发送事件，直至服务器再次可用。默认 UDP 端口为 514，默认 TCP 端口为 1470。如果您更改默认值，端口范围必须介于 1025 至 65535 之间。

  注释 如果您使用 TCP 作为传输协议，系统会打开与系统日志服务器的 4 个连接，以确保消息不会丢失。如果您使用系统日志服务器从大量设备收集消息，并且合并的连接开销对该服务器来说太大，请改用 UDP。

- **用于设备日志的接口** - 选择应使用哪个接口发送诊断系统日志消息。以下类型的事件始终使用管理接口：连接、入侵、文件和恶意软件。接口选择决定与系统日志消息关联的 IP 地址。选择以下选项之一：
  - **数据接口** - 选择用于诊断系统日志消息的数据接口。如果可以通过网桥组成员接口访问该服务器，请改而选择该网桥组接口 (BVI)。如果通过诊断接口（物理管理接口）访问，我们建议您选择**管理接口**，而不是此选项。您不能选择被动接口。

    对于连接、入侵、文件和恶意软件系统日志消息，源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。请注意，路由表中必须有适当的路由，以便将流量从选定接口引导至系统日志服务器，以获取这些事件类型。
  - **管理接口** - 对所有类型的系统日志消息使用虚拟管理接口。源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。

步骤 4 点击**确定 (OK)**，保存更改。

配置安全组标记 (SGT) 组

使用安全组标记 (SGT) 组对象以根据身份服务引擎 (ISE) 分配的 SGT 识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。

您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

有关如何使用 SGT 进行访问控制的详细信息，请参阅如何使用 TrustSec 安全组标记控制网络访问。

开始之前

在创建 SGT 组之前，必须配置 ISE 身份源以订用 SXP 映射并部署更改。然后，系统从 ISE 服务器检索 SGT 信息。只有在下载 SGT 后，您才能创建 SGT 组。

过程

步骤 1 选择**对象**，然后从目录中选择 **SGT 组**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ()。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 为对象输入**名称**和说明（后者为可选项）。

步骤 4 在**标记**下，点击 + 并选择要包含在对象中的已下载 SGT。

要删除 SGT，请点击标记名称右侧的 **x**。

如果列表为空，则系统无法下载任何 SGT 映射。如果发生这种情况，请采取以下措施：

- 确保 ISE 身份对象订用 SXP 主题。您必须订用 SXP，才能获取映射。
- 验证 ISE 中是否定义了静态映射，以及 ISE 是否配置为发布这些映射。如果不存在任何映射，就没有任何内容可供下载。请参阅在 ISE 中配置安全组和 SXP 发布。

步骤 5 点击**确定 (OK)**。

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。