访问控制

以下主题介绍访问控制规则。这些规则控制允许通过设备传递的流量，并会对流量应用入侵检测等高级服务。

访问控制最佳实践

访问控制策略是保护内部网络和防止用户访问不良外部网络资源（例如不良网站）的主要工具。因此，我们建议您特别注意此策略并对其进行调整，以实现所需的保护和连接级别。

以下程序概述您应对访问控制策略执行的基本操作。这只是一个概述，并不介绍执行每个任务的详尽步骤。

要进入访问控制策略，请选择**策略** > **访问控制**。

过程

步骤 1 配置策略的默认操作。

默认操作处理不与策略中的特定规则匹配的连接。默认情况下，此操作为**阻止**，以便阻止规则中遗漏的任何流量。因此，您只需要编写允许所需流量的访问控制规则。这是配置访问控制策略的传统方式。

您可以执行相反的操作，即在默认情况下允许流量，并编写丢弃已知不良流量的规则，这样您就无需为要允许的所有流量制定规则。这样更便于使用新服务，但会使新不良流量在您不经意间进入网络，构成风险。

步骤 2 点击**访问策略设置 (Access Policy Settings)** (⚙) 按钮，并启用 **TLS 服务器身份发现 (TLS Server Identity Discovery)** 选项。

此选项可改进 TLS 1.3 连接的初始应用检测以及 URL 类别和信誉识别。如果未启用此选项，则 TLS 1.3 流量将不与预期规则匹配。此选项还可以提高解密规则的效率。

步骤 3 尽可能少创建访问控制规则。

使用传统防火墙，您可能最终会获得数万条用于 IP 地址和端口的各种组合的规则。借助下一代防火墙，您可以使用高级检测功能并避免这其中的一些细化规则。您设置的规则越少，系统评估流量的速度就越快，您在规则集内查找和修复问题就越容易。

步骤 4 对访问控制规则启用日志记录。

仅当启用日志记录时，系统才会为匹配流量收集统计信息。如果不启用日志记录，您的监控控制面板信息将不准确。

步骤 5 将非常具体的规则放在策略前面，并确保具体规则位置高于任何可以匹配相同连接的更通用的规则。

系统自上而下地评估策略，并应用流量匹配的第一个策略。因此，如果您输入阻止所有流向特定子网的流量的规则，然后在此规则之后设置一条允许访问该子网内的单个 IP 地址的规则，则系统不会允许流量流向该地址，因为第一个规则将阻止它。

此外，应将仅基于传统条件（例如入向/出向接口和源/目标 IP 地址、端口或地理位置）来控制流量的规则放在需要深度检测的规则（例如应用于用户条件、URL 过滤或应用过滤的规则）前面。由于这些规则不需要执行检测，因此将它们放到前面可以让您更快地为与规则匹配的连接做出访问控制决策。

有关更多建议，请参阅访问控制规则顺序最佳实践，第 12 页。

步骤 6 将阻止规则和允许规则配对以控制部分流量。

例如，您可能希望允许大量 HTTP/HTTPS 流量，但需要阻止访问某些不良网站（例如色情或赌博网站）。您可以通过创建以下规则并使其在策略中保持相应先后顺序（例如，规则 11 和 12）来实现此目的。

- 将控制不良 URL 类别的 URL 过滤阻止规则应用于内部安全区（源）和外部安全区（目的地），以及任何 IP 地址、端口或地理位置。例如，阻止僵尸网络、虐待儿童的内容、挖矿劫持、DNS 隧道、电子银行欺诈、漏洞攻击、极端行为、过滤器规避行为、赌博、黑客攻击、仇恨言论、高风险站点和位置、非法活动、非法下载、违禁药物、恶意站点、恶意软件站点、移动威胁、P2P 恶意软件节点、网络钓鱼、色情、垃圾邮件、间谍软件和广告软件。
- 将适用于 HTTP 和 HTTPS 应用的应用过滤“允许”规则应用于内部安全区（源）和外部安全区（目的地）以及任何 IP 地址、端口或地理位置。在 URL 过滤规则“阻止”规则阻止对不良 Web 资源的访问后，此规则允许所有其他 HTTP/HTTPS 访问。

步骤 7 无论 IP 地址或端口如何，都可使用高级下一代防火墙功能来控制流量。

攻击者或其他恶意行为者可能会频繁更改 IP 地址和端口，以规避传统访问控制流量匹配条件。因此，请改用以下下一代功能：

- 用户条件 - 配置身份策略，以获取有关发起流量的用户的信息。理想情况下，您的 Active Directory 服务器会将用户分为不同的组，并且您可以创建基于用户组成员身份允许或阻止流量的访问控制规则。例如，允许工程师访问您的开发子网，但隐式阻止不属于工程师组的所有其他人访问此子网。使用组而不使用单个用户名，这样您就无需在向网络中添加人员时不断更新规则。
- 应用条件 - 使用应用过滤条件来允许或阻止某些类型的应用。这样，如果用户更改 HTTP 连接的端口，系统可以识别出它是 HTTP，即使它不连接到端口 80。有关更多建议，请参阅应用过滤最佳实践，第 5 页。
- URL 类别和信誉条件 - 使用基于类别的 URL 过滤来根据站点类型动态允许或阻止站点。在站点类型或类别中，您可以根据站点信誉的好坏来调整规则。通过使用类别和信誉，您无需在站点更改 URL 时不断调整规则，而如果您尝试按 URL 手动阻止站点，就必须执行此类调整。有关更多建议，请参阅有效 URL 过滤的最佳实践，第 9 页。

  您还可以将 URL 类别/信誉过滤规则应用于 DNS 查找请求中的 FQDN。系统可以阻止对被阻止的类别/信誉的 DNS 响应，从而有效地阻止用户的连接尝试。有关详细信息，请参阅基于 URL 类别和信誉过滤 DNS 请求，第 11 页。

步骤 8 将入侵检测应用于所有“允许”规则。

下一代防火墙的一个强大功能是，您可以使用同一设备应用入侵检测和访问控制。将入侵策略应用于每个“允许”规则，这样如果确实有攻击通过正常良性路径进入您的网络，您也可以捕获该攻击并丢弃攻击连接。

如果默认操作为“允许”，您还可以对与默认操作匹配的流量应用入侵保护。

步骤 9 此外，还应配置安全智能策略以阻止不良 IP 地址和 URL。

安全智能策略在访问控制策略之前应用，以便可以在系统评估访问控制规则之前阻止不良连接。这可以尽早阻止此类连接，并帮助您降低访问控制规则的复杂性。

步骤 10 考虑实施 SSL 解密策略。

系统不会对加密的流量进行深度检测。如果配置 SSL 解密策略，则访问控制策略将应用于已解密版本的流量。因此，深度检测可以识别攻击（使用入侵策略），并且规则匹配效果更好，因为应用和 URL 过滤会得到更高效的应用。然后，访问控制策略允许的所有流量都会在从设备发送出去之前重新加密，因此最终用户不会失去加密保护。

步骤 11 启用对象组搜索以简化规则的部署。

从版本 7.2 开始，默认情况下会在新部署上启用此功能，但不会在升级后的系统上自动启用。

启用对象组搜索可以降低包含网络对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

可执行 **object-group-search access-control** 命令来通过使用 FlexConfig 设置此选项；可在取消模板中使用该命令的 **no** 形式。

访问控制概述

以下主题介绍访问控制策略。

访问控制规则和默认操作

使用访问控制策略允许或阻止对网络资源的访问。该策略包含一系列有序的规则，按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。

您可以根据以下条件控制访问：

- 传统网络特征，例如源和目标 IP 地址、协议、端口和接口（以安全区形式）。
- 源或目标（以网络对象形式）的完全限定域名 (FQDN)。流量匹配基于从 DNS 查询为该名称返回的 IP 地址。
- 思科身份服务引擎 (ISE) 分配给源或目的地的安全组标记 (SGT)。
- 正在使用的应用。您可以基于特定应用控制访问，也可以创建涵盖应用类别、标记特定特征的应用、应用类型（客户端、服务器、Web）或应用风险或业务相关性评级的规则。
- Web 请求的目的 URL，包括 URL 的通用类别。您可以基于目标站点的公共信誉优化类别匹配。
- DNS 查找请求中 FQDN 的 URL 类别和信誉。您可以阻止不需要的类别或信誉不佳的 DNS 响应，从而有效防止后续连接尝试。
- 发出请求的用户或用户所属的用户组。

对于您允许的未加密流量，可以应用 IPS 检测来检查威胁并阻止看似攻击的流量。另外，您还可以使用文件策略来检查是否存在禁止文件或恶意软件。

与访问规则不匹配的流量由访问控制**默认操作**处理。默认情况下，如果允许流量，则可以对流量应用入侵检测。但您不能对默认操作处理的流量执行文件或恶意软件检测。

应用过滤

您可以使用访问控制规则基于连接中使用的应用过滤流量。系统会识别各种各样的应用，因此您不需要弄明白如何在不阻止所有 Web 应用的情况下阻止某个 Web 应用。

对于一些常用的应用，您可以根据应用的不同方面进行过滤。例如，您可以创建一个阻止 Facebook 游戏但不阻止所有 Facebook 功能的规则。

您还可以基于一般应用特点创建规则，通过选择风险或业务相关性、类型、类别或标记来阻止或允许整组应用。**但是，在应用过滤器中选择类别时，请查看匹配的应用列表，确保不包含非预期应用。**有关可能分组的详细说明，请参阅应用条件，第 21 页。

已加密和已解密流量的应用控制

如果应用使用加密，系统可能无法识别该应用。

系统可以检测使用 StartTLS 加密的应用流量，包括 SMTPS、POP、FTPS、TelnetS 和 IMAPS。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书中的使用者可分辨名称值来识别某些加密应用。

请使用应用过滤器对话框通过选择以下标记来确定应用是否需要解密，然后检查应用列表。

- **SSL 协议** - 不需要解密标记为“SSL 协议”的流量。系统可以识别此流量并应用您的访问控制操作。用于所列出应用的访问控制规则应与预期的连接匹配。
- **解密流量** - 只有先解密流量，系统才能识别此流量。配置用于此流量的 SSL 解密规则。

过滤通用工业协议 (CIP) 和 Modbus 应用 (ISA 3000)

可以在思科 ISA 3000设备上启用通用工业协议 (CIP) 和 Modbus 预处理器，并在访问控制规则中过滤 CIP 和 Modbus 应用。所有 CIP 应用名称均以“CIP”开头，例如 CIP Write。仅有一个应用适用于 Modbus。

要启用预处理器，必须在 CLI 会话（SSH 或控制台）中进入专家模式，并发出以下命令以启用其中一个或两个监控和数据采集 (SCADA) 应用。

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

例如，要启用两个预处理器：

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```

注释 必须在每次部署后发出此命令。部署期间禁用这些预处理器。

应用过滤最佳实践

设计应用过滤访问控制规则时，请牢记以下建议。

- 要处理网络服务器所推荐的流量（例如广告流量），请匹配被推荐的应用（而非推荐应用）。
- 避免将应用与 URL 标准组合在同一规则中，尤其是对于加密流量。
- 如果要为标记为**解密流量**的流量编写规则，请确保具有解密匹配流量的 SSL 解密规则。仅可在解密连接中识别这些应用。
- TLS 1.3 加密大多数握手消息，因此证书信息不容易获得。对于使用 TLS 1.3 加密的流量，要高效地匹配使用应用或URL过滤的访问规则，系统必须获取服务器的明文证书。我们建议您在访问控制设置中启用 **TLS 1.3 证书可视性** 。如果启用此选项，系统将根据客户端 Hello 数据包中的 IP 地址和服务器名称指示 (SNI) 检查站点的证书是否存储在缓存中。如果不可用，系统将使用 TLS 1.2 探测器获取证书，然后可将其用于应用/URL 类别和信誉识别，而无需解密连接。
- 系统可以检测多个类型的 Skype 应用流量。要控制 Skype 流量，请从应用过滤器列表中选择 Skype 标记（而不是选择个别应用）。这确保系统可以相同方式检测和控制所有 Skype 流量。
- 要控制 Zoho 邮件访问，请选择 Zoho 和 Zoho 邮件应用。

URL 过滤

您可以使用访问控制规则基于 HTTP 或 HTTPS 连接中使用的 URL 过滤流量。请注意，HTTP 的 URL 过滤比 HTTPS 更直接，因为 HTTPS 会被加密。

您可以使用以下方法实施 URL 过滤：

- 基于类别和信誉的 URL 过滤 - 使用 URL 过滤许可证，您可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。这是迄今为止阻止非必要网站的最简单、最有效的方法。
- 手动 URL 过滤 - 使用任何许可证均可手动指定各个 URL 和 URL 组，以便对网络流量实现精细的自定义控制。手动过滤的主要目的是创建基于类别的阻止规则的例外，但可以将手动规则用于其他目的。

以下主题提供了有关 URL 过滤的详细信息。

按照类别和信誉过滤 URL

通过 URL 过滤许可证，您可以基于所请求 URL 的类别和信誉控制对网站的访问：

- 类别 - URL 的一般分类。例如，ebay.com 属于“拍卖”类别，而 monster.com 属于“职位搜索”类别。URL 可以属于多个类别。
- 信誉 - URL 被用于可能违反组织安全策略之目的的可能性。范围可从“不受信任”（第 1 级）到“受信任”（第 5 级）。

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，您可以使用访问控制阻止“违禁药物”类别中不受信任的 URL。

有关类别说明，请参阅 https://www.talosintelligence.com/categories。

使用类别和信誉数据还会简化策略创建和管理。代表安全威胁的站点或提供不良内容的站点的出现和消失速度，可能比您更新和部署新策略的速度要快。由于思科使用新站点、已更改分类与信誉更新 URL 数据库，因此，规则会自动调整以适应新信息。无需为新站点编辑规则。

如果启用常规 URL 数据库更新，则可确保系统使用最新信息进行 URL 过滤。还可启用与思科 综合安全智能 (CSI) 的通信，获取类别和信誉已知的 URL 的最新威胁智能。有关详细信息，请参阅配置 URL 过滤首选项。

注释 要查看事件和应用详细信息中的 URL 类别和信誉信息，必须至少创建一条具有 URL 标准的规则。

查找 URL 的类别和信誉

您可以检查特定 URL 的类别和信誉。您可以转至访问控制规则或 SSL 解密规则的 URL 选项卡，或转至**设备** > **系统设置** > **URL 过滤首选项**。其中，您可以在**待检查的 URL** 字段中输入 URL，然后点击**前往**。

您将转至显示查询结果的网站。您可以使用此信息，帮助您查看基于类别和信誉的URL过滤规则的表现。

如果您对分类持不同意见，您可以点击 设备管理器 中的 **提交 URL 类别争议**，告诉我们您的想法。

手动 URL 过滤

您可以通过手动过滤各个 URL 或 URL 组，补充或选择性地覆盖基于类别和信誉的 URL 过滤。您可以在没有特殊许可证的情况下执行此类 URL 过滤。

例如，您可以使用访问控制阻止不适合于您组织的某类网站。但是，如果该类别包含适合的网站，且要为其提供访问权限，则可以为该站点创建手动“允许”规则，并将该规则置于适用于该类别的“阻止”规则前。

要配置手动 URL 过滤，请使用目标 URL 创建一个 URL 对象。基于如下规则解释该 URL：

- 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。

过滤 HTTPS 流量

由于 HTTPS 流量加密，所以直接对 HTTPS 流量执行 URL 过滤并不像对 HTTP 流量执行 URL 过滤那样直接。因此，应考虑使用 SSL 解密策略解密想要过滤的所有 HTTPS 流量。这样，URL 过滤访问控制策略可有效用于解密流量，并会获得与常规 HTTP 流量相同的结果。

但是，如果打算允许某些HTTPS流量在未加密情况下通过访问控制策略，则需了解规则匹配HTTPS流量与匹配 HTTP 流量的方式不同。要过滤加密流量，系统将根据 SSL 握手期间传递的信息确定请求的URL：用于加密流量的公钥证书中的使用者公用名。URL中的网站主机名与使用者公用名之间可能没有多大关系。

如果启用 DNS 请求过滤，则可以改进类别/信誉规则的 HTTPS 匹配。系统可以在 DNS 解析阶段确定类别和信誉，并在用户可以开始 HTTPS 连接尝试之前阻止对不需要的组合做出 DNS 回复。对于允许的 DNS 响应，系统将提供可用于后续 HTTPS 连接的类别/信誉信息。请参阅 DNS 请求过滤，第 10 页。

HTTPS 过滤与 HTTP 过滤不同，它不考虑使用者公用名内的子域。手动过滤 HTTPS URL 时，请勿包含子域信息。例如，使用 example.com 而不是 www.example.com。此外，请查看站点所使用的证书内容，以确保使用者公用名中使用的域名正确，且该名称不会与其他规则冲突（例如，想要阻止的站点名称可能与想要允许的站点名称重叠）。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）。

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。

按加密协议控制流量

在执行 URL 过滤时，系统会忽略加密协议（HTTP 和 HTTPS）。对于手动 URL 标准和基于信誉的 URL 标准均会发生此情况。换句话说，URL 过滤以相同方式处理发送到以下网站的流量：

- http://example.com
- https://example.com

要配置仅匹配HTTP流量或HTTPS流量（而不是同时匹配这两种流量）的规则，请在“目标”条件中指定 TCP 端口或在规则中添加应用条件。例如，可以通过构造两个访问控制规则（各规则具有 TCP 端口或应用和 URL 标准）来允许对某个站点进行 HTTPS 访问，同时禁止 HTTP 访问。

第一个规则允许 HTTPS 流量到达网站：

操作：允许
TCP 端口或应用：HTTPS（TCP 端口 443）
URL：example.com

第二个规则阻止对同一网站进行 HTTP 访问：

操作：阻止
TCP 端口或应用：HTTP（TCP 端口 80）

URL：example.com

比较 URL 和应用过滤

URL 和应用过滤具有许多相似之处。但应将其用于明显不同的目的：

- URL 过滤最好用于阻止或允许访问整个 Web 服务器。例如，如果不希望在网络上进行任何类型的赌博，则可创建用于阻止赌博类别的 URL 过滤规则。通过该规则，用户无法访问该类别内所有 Web 服务器上的任何页面。
- 应用过滤适用于阻止特定应用（无论托管站点如何），或阻止在其他方面受允许的其他网站的特定功能。例如，可以在不阻止所有 Facebook 功能的情况下阻止 Facebook 游戏应用。

由于组合应用与 URL 标准可能会导致非预期结果，尤其是对于加密流量，因此，分别创建用于 URL 和应用标准的单独规则是个好方法。如果需要将应用与 URL 标准合并到单个规则中，应将这些规则直接置于仅应用或仅 URL 规则后，除非应用+URL 规则作为更一般的仅应用或仅 URL 规则的例外。由于 URL 过滤阻止规则比应用过滤阻止规则更广泛，因此，您应将其置于仅应用规则之上。

如果将应用标准与 URL 标准组合在一起，则可能需要更仔细地监控网络，以确保不允许访问不必要的站点和应用。

有效 URL 过滤的最佳实践

设计 URL 过滤访问控制规则时，请牢记以下建议。

- 尽可能使用类别和信誉阻止。这可以确保在将新站点添加到类别时自动将其阻止，且如果站点的信誉变得更佳（或更劣），则根据信誉对阻止情况进行调整。
- 使用 URL 类别匹配时，请注意，有时候站点登录页的类别与站点本身的类别不同。例如，Gmail 属于“基于 Web 的邮件”类别，而登录页面属于搜索引擎和门户 (Search Engines and Portals)类别。如果您为类别制定了包含不同操作的不同规则，可能会出现意想不到的结果。
- 使用 URL 对象定位整个网站，并对类别阻止规则进行例外处理。也就是说，允许特定网站（否则，该网站会被阻止于某个类别规则中）。
- 如果要手动阻止 Web 服务器（使用 URL 对象），则在安全智能策略中这样做更有效。评估访问控制规则前，安全智能策略丢弃连接，以便可获得更快、更有效的阻止。
- 为对 HTTPS 连接进行最有效的过滤，请使用 SSL 解密规则解密正在为其编写访问控制规则的流量。任何解密的 HTTPS 连接均会在访问控制策略中作为 HTTP 连接予以过滤，以避免 HTTPS 过滤的所有限制。
- TLS 1.3 加密大多数握手消息，因此证书信息不容易获得。对于使用 TLS 1.3 加密的流量，要高效地匹配使用应用或 URL 过滤的访问规则，系统必须获取服务器的明文证书。我们建议您在访问控制设置中启用 **TLS 1.3 证书可视性** 。如果启用此选项，系统将根据客户端 Hello 数据包中的 IP 地址和服务器名称指示 (SNI) 检查站点的证书是否存储在缓存中。如果不可用，系统将使用 TLS 1.2 探测器获取证书，然后可将其用于应用/URL 类别和信誉识别，而无需解密连接。
- 将 URL 阻止规则置于任何应用过滤规则前，因为 URL 过滤阻止整个 Web 服务器，而应用过滤将针对特定的应用使用，而不考虑 Web 服务器。

- 如果要阻止类别未知的高风险站点，请选择未分类类别，并将信誉滑块调整为“可疑”或“不受信任”。
- 您还可以通过启用 DNS 请求过滤来提高总体 URL 过滤效率。当使用 DNS 请求过滤时，系统会在执行 DNS 查找时确定 FQDN 的 URL 类别和信誉，以便在后续 HTTP/HTTPS 请求的目的地相同时提供这些信息。此外，如果阻止类别/信誉，则尝试连接将在 DNS 请求阶段停止，而不是在 Web 会话建立阶段停止。请参阅DNS 请求过滤，第 10 页。

阻止网站时用户看到的内容

使用 URL 过滤规则阻止网站时，用户所看到的内容视该站点是否加密而异。

- HTTP 连接 - 用户会看到系统默认阻止响应页面，而不是为超时或重置连接而正常显示的浏览器页面。此页面将明确指示，您有意阻止了该连接。
- HTTPS（已加密）连接 - 用户不会看到系统默认阻止响应页面。相反，用户会看到浏览器显示安全连接故障的默认页面。错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

此外，网站可能是被属于非显式URL过滤规则的其他访问控制规则，甚至是被默认操作而阻止。例如，如果阻止整个网络或地理位置，也会阻止该网络或该地理位置的任何网站。受这些规则阻止的用户可能（也可能不能）得到以下限制中所述的响应页面。

如果实施URL过滤，请考虑向最终用户说明他们在站点被有意阻止时可能会看到的内容，以及您将阻止的站点类型。否则，他们可能会花费大量时间来解决受阻止的连接故障。

HTTP 响应页面的限制

当系统阻止网络流量时，并不总是显示 HTTP 响应页面。

- 如果网络流量由于提升的访问控制规则（放在前面的仅包含简单网络条件的阻止规则）被阻止，系统则不显示响应页面。
- 如果网络流量在系统识别请求的 URL 之前被阻止，则系统不显示响应页面。
- 对于被访问控制规则阻止的已加密连接，系统不会显示响应页面。

DNS 请求过滤

您可以将 URL 类别和信誉数据库应用于 DNS 查找请求，即使是对于非 HTTP/HTTPS 的连接尝试也可以如此。

例如，如果用户尝试建立到 www.example.com 的 FTP 连接，您可以将系统配置为在看到针对该完全限定域名 (FQDN) 的 DNS 查找请求时查找 www.example.com 的类别和信誉。如果返回的类别/信誉的 DNS/URL 过滤规则是阻止规则，则系统会阻止 DNS 回复。因此，用户无法获取 FQDN 的 IP 地址，并且连接尝试失败。

通过启用 DNS 查找请求过滤，您可以将 URL 过滤规则扩展到除 HTTP/HTTPS 之外的协议，并防止 FTP、TFTP、SCP、ICMP 和任何其他协议与您阻止进行网络访问的站点建立连接。只要用户使用

FQDN 名称并因此需要进行 DNS 查找，此方法就有效。如果用户使用 IP 地址，就没有 DNS 请求，且无法阻止 DNS 请求。

对于 HTTP/HTTPS 流量，在 DNS 请求时执行类别/信誉查找可能会提高系统性能，因为它可以在尝试建立 Web 会话之前阻止连接。这对于加密的 HTTPS 可能特别有用。通过在 DNS 请求阶段拒绝，系统永远不会看到HTTPS连接，因此您的解密规则不需要评估，系统也不需要执行更困难的任务，即将加密会话与正确的访问控制规则进行匹配。

DNS 请求过滤准则

在配置 DNS 请求过滤时，请记住以下几点：

- DNS请求过滤仅适用于DNS会话。如果允许DNS回复（即，URL过滤规则操作为“允许”），则用户使用返回的IP地址建立的后续连接将单独与您的访问控制规则进行匹配。连接可能与其他规则匹配，因此由于其他原因而被阻止或允许。例如，如果允许 FTP 尝试通过 DNS 查找获取 IP 地址，则可能有另一个禁止 FTP 连接的访问控制规则，连接最终将被阻止。
- 将根据匹配规则允许或阻止与 URL/DNS 请求过滤规则之前的访问控制规则相匹配的 DNS 查找请求。将不会对这些连接执行类别/信誉查找。
- 此功能要求您根据类别/信誉实施 URL 过滤。您必须具有此类 URL 过滤的 URL 过滤许可证。如果没有基于类别/信誉的 URL 过滤规则，则 DNS 请求过滤不相关，因此不应启用。
- 由 DNS 过滤生成的连接事件包括以下特别需要关注的字段：DNS 查询、URL 类别和 URL 信誉。DNS 查询字段显示查找请求的完全限定域名 (FQDN)。对于 DNS 过滤事件，URL 字段将为空。
- DNS 请求过滤仅使用 URL 类别和信誉数据库。在匹配访问控制规则中定义的任何 URL 对象或其他手动 URL 过滤都将被忽略。如果要实施 DNS 名称手动阻止，请使用安全智能 DNS 策略。

基于 URL 类别和信誉过滤 DNS 请求

以下程序介绍如何实施 DNS 查找请求过滤。

开始之前

您必须启用 URL 许可证（如果尚未启用）。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 如有必要，请点击**访问策略设置** ( ) 按钮，选择 **DNS 流量的信誉实施**选项，然后点击**确定**。

此选项为访问控制策略启用 DNS 请求过滤。默认情况下，此选项已启用。

步骤 3 评估现有的 URL 过滤规则或创建新的规则，以根据也适用于 DNS 请求的 URL 类别和信誉实施过滤。

URL 过滤通常仅适用于 HTTP/HTTPS 流量，因此没有理由根据应用或端口限制这些规则。但是，如果有这些限制，请确保规则也适用于 DNS 请求：

- 在**源/目标**选项卡上，如果**目标端口**字段的值为**任何**，则无需更改。如果指定了端口，请将 **DNS over UDP** 和 **DNS over TCP** 添加到列表。
- 在**应用**选项卡上，如果应用列表仅包含**任何**，则无需更改。如果指定了任何应用或应用过滤器，请将 **DNS** 应用添加到列表或过滤器。其他与 DNS 相关的选项与此目的无关。

有关创建访问控制规则的信息，请参阅配置访问控制规则，第 18 页。

步骤 4 评估前面的规则，确保 DNS 请求与这些规则不匹配。

仅当 DNS 请求与具有类别和信誉指定的 URL 过滤规则匹配时，才会确定类别和信誉。任何与访问控制策略中的规则比 URL 过滤规则更早匹配的任何 DNS 请求都会绕过 DNS 请求过滤。此类 DNS 请求根据匹配规则（被阻止或允许）进行处理。

入侵、文件和恶意软件检测

入侵策略和文件策略共同发挥作用，作为允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。
- 文件策略监管系统的文件控制和恶意软件防御功能。

处理所有其他流量后，才会检验网络流量中是否存在入侵、禁止文件和恶意软件。通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

您只能对**允许**流量的规则配置入侵策略和文件策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是**允许**，则您可以配置入侵策略，但不能配置文件策略。

对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。

注释 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。检测仅适用于未加密的流量。

访问控制规则顺序最佳实践

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。请考虑以下建议：

- 特定规则应在一般规则之前，特别当特定规则是一般规则的例外时。
- 仅基于第 3/4 层标准丢弃流量的任何规则（如 IP 地址、安全区和端口号）应尽早出现。我们建议这些规则应在需要检查的任何规则前，如具有应用或 URL 标准的规则，因为可快速评估第 3/4 层标准而无需检查。当然，这些规则的任何例外必须置于这些规则之上。
- 尽可能将特定丢弃规则置于策略顶部附近。这确保了对非预期流量尽可能做出最早的决定。
- 包括应用和 URL 标准的任何规则应直接位于仅应用或仅 URL 规则前，除非应用+URL 规则作为更一般仅应用或仅 URL 规则的例外。组合应用和 URL 标准可能会导致非预期结果，尤其是对于加密流量，因此，我们建议您尽可能创建单独的 URL 和应用过滤规则。

NAT 和访问规则

在确定访问规则匹配时，访问规则始终将使用真实 IP 地址，即使您已配置 NAT。例如，如果已为内部服务器 (10.1.1.5) 配置 NAT，以使该服务器在外部拥有公共可路由的 IP 地址 209.165.201.5，则用于允许外部流量访问内部服务器的访问规则需要引用该服务器的真实 IP 地址 (10.1.1.5)，而非映射地址 (209.165.201.5)。

其他安全策略如何影响访问控制

其他安全策略可能影响访问控制规则的运行和对连接的匹配。配置访问规则时，请记住以下几点：

- **SSL 解密**策略 - 访问控制前评估 SSL 解密规则。因此，如果加密连接与应用某类型解密的 SSL 解密规则相匹配，则该连接为通过访问控制策略评估的纯文本（解密）连接。访问规则无法查看加密版本的连接。此外，访问控制策略绝不会看到任何与丢弃流量的 SSL 解密规则相匹配的连接。最后，匹配“不解密”规则的任何加密连接将以其加密状态接受评估。
- **身份**策略 - 仅当存在用于源 IP 地址的用户映射时，连接才与用户（以及用户组）匹配。侧重于用户或组成员关系的访问规则可能仅匹配身份策略成功收集的用户身份的那些连接。
- **安全智能**策略 - 访问控制策略绝不会看到任何被丢弃的连接。匹配“不阻止”列表的连接随后会与访问控制规则相匹配，最终，访问控制规则决定如何处理（允许或丢弃）连接。
- **VPN**（站点间或远程访问）- 始终根据访问控制策略对 VPN 流量进行评估，并根据匹配规则允许或丢弃连接。但在评估访问控制策略前，VPN 隧道本身将被解密。访问控制策略评估嵌入 VPN 隧道中的连接，而不是隧道本身。

访问控制许可证要求

使用访问控制策略无需特殊许可证。

但若要使用访问控制策略中的特定功能，则需以下许可证。有关配置许可证的信息，请参阅启用或禁用可选许可证。

- **URL** 许可证 - 创建将 URL 类别和信誉作为匹配标准的规则。

- **威胁**许可证 - 为访问规则或默认操作配置入侵策略。还需要此许可证才能使用文件策略（还需要恶意软件许可证）。
- **恶意软件**许可证 - 在访问规则上配置文件策略。文件策略还需要 威胁。

访问控制策略的准则和限制

以下是访问控制的一些其他限制。请在评估是否会从规则中获取预期结果时考虑这些内容。

- 如果URL数据库更新包括已添加（新增、传入）、已弃用（传出）或已删除的类别，则您可以在一个宽限期内对受影响的访问控制规则进行更改。受影响的规则都标有信息性消息，包含对影响规则的问题的说明，以及思科 Talos 情报小组 (Talos) 网站的链接，其中包含有关类别更改的详细信息。您需要更新规则，以便它可以使用最新 URL 数据库中相应的类别。

  要适应宽限期，请将新添加的传入类别添加到适当的规则，同时不删除已弃用的传出类别：规则应包含新的和旧的类别。当旧类别标记为删除时，新类别才会生效。当旧类别最终被删除时，您需要编辑规则来移除已删除的类别并重新部署配置。只有在修复所有使用旧类别的规则后，系统才不会阻止您部署配置。点击表格上方的**查看问题规则**链接，过滤出需要注意的规则。

- 设备管理器 可以从目录服务器下载多达 50,000 个用户的信息。如果您的目录服务器上有超过 50,000 个用户账户，则在访问规则中选择用户时或查看基于用户的控制面板信息时，您不会看到所有可能的名称。您仅可以对已下载的名称编写规则。

  此 50,000 个用户的限制也适用于与组相关联的名称。如果组成员超过 50,000 个，则只能将下载的 50,000 个名称与组成员身份进行匹配。

- 如果漏洞数据库 (VDB) 更新删除（弃用）应用，则必须对使用已删除应用的任何访问控制规则或应用过滤器进行更改。修复这些规则前，您无法部署更改。此外，您无法在解决问题之前安装系统软件更新。在“应用过滤器对象”页面上或规则的“应用”选项卡上，这些应用在应用名称后显示“（已弃用）”。

- 要将完全限定域名 (FQDN) 网络对象用作源或目标条件，您还必须在**设备** > **系统设置** > **DNS 服务器**上配置适用于数据接口的 DNS。系统不使用管理 DNS 服务器设置查找访问控制规则中使用的 FQDN 对象。有关排除 FQDN 解析问题的信息，请参阅常规 DNS 问题故障排除。

  请注意，通过 FQDN 控制访问是尽力而为机制。考虑以下几点：

  - 由于 DNS 回复可能具有欺骗性，因此只能使用完全受信任的内部 DNS 服务器。
  - 有些FQDN，特别是非常受欢迎的服务器，可能有成百上千个 IP 地址，而且这些地址经常都会变化。由于系统使用的是缓存的 DNS 查询结果，用户可能会获得尚未在缓存中的地址，因此他们的连接将与 FQDN 规则不匹配。使用 FQDN 网络对象的规则只对解析为 100 个以内地址的名称有效。

    建议您不要为解析为超过 100 个地址的 FQDN 创建网络对象规则，因为连接中的地址是设备DNS缓存中已解析和可用地址的可能性很低。对于这些情况，请使用基于URL的规则，而不是 FQDN 网络对象规则。

  - 对于受欢迎的 FQDN，不同的 DNS 服务器可以返回一组不同的 IP 地址。因此，如果您的用户使用的DNS服务器与您所配置的不同，基于FQDN的访问控制规则可能不适用于客户端对于该站点使用的所有 IP 地址，而您的规则也不会实现预期结果。
  - 一些 FQDN DNS 条目的生存时间 (TTL) 值非常小。这会导致查询表频繁地进行重新编译，从而可能会影响总体系统性能。

- 如果编辑的规则正在使用中，所做的更改不会应用于Snort不再检查的已建连接。此新规则用于根据未来的连接进行匹配。此外，如果Snort当前正在检查连接，它可以将更改的匹配或操作条件应用于现有连接。如果您需要确保将所做的更改应用于当前的所有连接，您可以登录设备CLI并使用 **clear conn** 命令终止已建连接，但前提是，连接源稍后将尝试重新建立连接，并根据新规则进行相应匹配。
- 系统需要 3 至 5 个数据包才能识别连接中的应用或 URL。因此，正确的访问控制规则可能不会立即匹配给定连接。但是，一旦应用/URL 已知，系统会根据匹配规则处理连接。对于加密连接，这发生于 SSL 握手中的服务器证书交换之后。
- 对于在用于应用识别的连接中没有负载的数据包，系统会应用默认策略操作。
- 尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。例如，如果仅将安全区条件留空，而不是创建包含所有接口的区域，则系统可以更有效地匹配所有接口的流量。指定多个条件时，系统必须匹配您指定的条件内容的各组合。
- 如果为源或目标条件指定 IP 地址，请不要在同一规则中混合使用 IPv4 和 IPv6 地址。而是为 IPv4 和 IPv6 地址创建单独的规则。
- 运行时，威胁防御设备会根据访问规则中使用的任何网络对象的内容，将访问控制规则扩展为多个访问控制列表条目。您可以通过启用对象组搜索来减少搜索访问规则所需的内存。启用对象组搜索后，系统不会扩展网络对象，而是根据这些组定义在访问规则中搜索匹配项。对象组搜索不会影响访问规则的定义方式或它们在 设备管理器中的显示方式，而只会影响将连接与访问控制规则匹配时设备如何对其进行解释和处理。

  启用对象组搜索可以降低包含网络对象的访问控制策略的内存要求。但是，请务必注意，对象组搜索还可能会降低规则查找性能，从而提高 CPU 利用率。您应该在 CPU 影响与降低特定访问控制策略的内存要求之间取得平衡。在大多数情况下，启用对象组搜索可提高网络运营性能。

  可执行 **object-group-search access-control** 命令来通过使用 FlexConfig 设置此选项；可在取消模板中使用该命令的 **no** 形式。

  从版本 7.2 开始，默认情况下会在新部署上启用此功能，但不会在升级后的系统上自动启用。
- 违反相关 RFC 的 GRE 隧道将被丢弃。例如，如果 GRE 隧道在保留位中包含非零值，则与 RFC 相反，它将被丢弃。如果需要允许不合规的GRE隧道，则需要使用远程管理器并配置信任会话的预过滤器规则。不能使用 设备管理器配置预过滤器规则。

配置访问控制策略

使用访问控制策略可监控对网络资源的访问。该策略包含一系列有序的规则，按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。如果没有匹配流量的规则，则应用页面底部显示的默认操作。

要配置访问控制策略，请依次选择**策略** > **访问控制**。

访问控制表将按顺序列出所有规则。对于每条规则：

- 点击最左列规则编号旁边的>按钮，可打开规则图表。图表可帮助您查看规则控制流量的方式。再次点击该按钮可关闭图表。
- 大多数单元格允许行内编辑。例如，您可以点击操作选择不同的操作，或者点击某个源网络对象以添加或更改源条件标准。
- 要移动规则，请将鼠标悬停在规则上，直到显示移动图标 ()，然后点击规则并将其拖放到新位置。您还可以通过编辑规则并在**顺序**列表中选择新位置来移动规则。一定要按您想要处理它们的顺序排列这些规则。特定规则应该靠近顶部，特别是定义一般规则例外情况的规则
- 最右列包含规则的操作按钮；将鼠标悬停在该单元格上可查看按钮。您可以编辑 () 或删除 () 规则。
- 点击**访问控制设置** () 按钮，以配置应用于访问控制策略而不是策略中特定规则的设置。
- 点击表格上方的**切换命中计数**图标 ()，添加或删除表中的命中计数列。命中计数列位于名称列的右侧，显示规则的总命中计数以及最后一次命中的日期和时间。点击切换按钮可即刻获取命中计数信息。点击**刷新**图标 () 可获取最新信息。
- 如果有任何规则存在问题，例如，因为删除或更改了URL类别而出现问题，请点击搜索框旁边的**查看问题规则**链接，对表格进行过滤，仅显示存在问题的规则。请编辑并更正（或删除）这些规则，以便它们可提供所需的服务。

以下主题介绍如何配置策略。

配置默认操作

如果连接未匹配特定访问规则，则由访问控制策略的默认操作来处理该连接。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**默认操作**字段的任意位置。

步骤 3 选择应用于匹配流量的操作。

- **信任** - 允许流量，而无需进行任何类型的进一步检测。

- **允许** - 允许流量接受入侵策略检测。
- **阻止** - 无条件地丢弃流量。不检测流量。

步骤 4 如果操作为**允许**请选择一条入侵策略。

有关策略选项的说明，请查看入侵策略设置，第 24 页。

步骤 5 （可选。）针对默认操作配置日志记录。

要在控制面板数据或事件查看器中包括匹配默认操作的流量，必须对匹配默认操作的流量启用日志记录。请参阅日志记录设置，第 25 页。

步骤 6 点击**确定 (OK)**。

配置访问控制策略设置

您可以配置应用于访问控制策略而不是策略中特定规则的设置。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**访问策略设置** (⚙) 按钮。

步骤 3 配置设置：

- **TLS 服务器身份发现**- TLS 1.3 加密大多数握手消息，因此证书信息不容易获得。对于使用 TLS 1.3 加密的流量，要匹配使用应用或 URL 过滤的访问规则，系统必须获取服务器的明文证书。如果启用此选项，系统将根据客户端 Hello 数据包中的 IP 地址和服务器名称指示 (SNI) 检查站点的证书是否存储在缓存中。如果不可用，系统将使用 TLS 1.2 探测器获取证书，然后可将其用于应用/URL 类别和信誉识别。建议您启用此选项，以确保将加密连接与正确的访问控制规则进行匹配。此设置仅获取证书；连接保持加密状态。启用此选项即可获取 TLS 1.3 证书；您无需创建相应的 SSL 解密规则。但是，除了访问控制处理之外，缓存的证书还用于更有效的解密规则处理。
- **DNS 流量的信誉实施** - 启用此选项可将 URL 过滤类别和信誉规则应用于 DNS 查找请求。如果查找请求中的完全限定域名 (FQDN) 具有要阻止的类别和信誉，系统会阻止 DNS 回复。由于用户未收到 DNS 解析，因此用户无法完成连接。使用此选项可将 URL 类别和信誉过滤应用于非 Web 流量。有关详细信息，请参阅DNS 请求过滤，第 10 页。

步骤 4 点击**确定 (OK)**。

配置访问控制规则

使用访问控制规则可监控对网络资源的访问。访问控制策略中的规则按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

要删除不再需要的规则，请点击该规则的删除图标 ( )。

步骤 3 在**顺序**中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在**名称**中输入规则的名称。

名称不能包含空格。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 5 选择应用于匹配流量的操作。

- **信任** - 允许流量，而无需进行任何类型的进一步检测。
- **允许** - 允许流量，不受策略中的入侵及其他检测设置约束。
- **阻止** - 无条件地丢弃流量。不检测流量。

步骤 6 使用以下选项卡的任意组合，定义流量匹配标准：

- **源/目的地** - 流量传输所用的安全区（接口）、IP 地址或该 IP 地址的国家/地区或大洲（地理位置）、分配给该地址的安全组标记(SGT)或者流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、SGT、协议和端口。请参阅 源/目标条件，第 19 页。
- **应用** - 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。默认设置为任何应用。请参阅应用条件，第 21 页。
- **URL** - Web 或 DNS 查找请求的 URL 或 URL 类别。默认设置为任何 URL。请参阅 URL 标准，第 22 页。
- **用户** - 身份源，用户或用户组。身份策略决定了用户和组的信息是否可用于流量匹配。只有配置身份策略，才能使用此条件标准。请参阅 用户条件，第 23 页。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击**确定(OK)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的**x**，可将其从策略中移除。

向访问控制规则中添加条件时，请考虑以下提示：

- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则对特定主机或网络执行 URL 过滤。
- 最多可以为规则中的每个条件添加50个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多50个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的和应用之间）为 AND 关系。
- 有些功能需要您启用适当的许可证。

步骤 7 （可选。）对于使用“允许”操作的策略，可以对未加密流量配置进一步的检测。点击以下任一链接：

- **入侵策略** - 依次选择**入侵策略** > **开**，然后选择入侵检测策略，可检测流量中是否存在入侵和漏洞攻击。请参阅入侵策略设置，第 24 页。
- **文件策略** - 选择文件策略可检测流量中是否存在包含恶意软件的文件和应被阻止的文件。请参阅文件策略设置，第 24 页。

步骤 8 （可选。）针对规则配置日志记录。

默认情况下，对于匹配规则的流量不会生成连接事件，但如果选择了文件策略，则默认生成文件事件。您可以更改此行为。要在控制面板数据或事件查看器中包括匹配策略的流量，必须对匹配策略的流量启用日志记录。请参阅日志记录设置，第 25 页。

无论匹配访问规则的日志记录配置如何，系统始终为设置为丢弃或发送警报的入侵规则生成入侵事件。

步骤 9 点击**确定 (OK)**。

源/目标条件

访问规则的“源/目标”条件定义用于传递流量的安全区（接口）、IP 地址或 IP 地址的国家/地区或大洲（地理位置）、分配给地址的安全组标记 (SGT) 或流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、SGT、协议和端口。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

您可以通过以下标准来标识规则中要匹配的源和目标。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至**目标区域**。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至**源区域**。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保到达内部主机的所有流量均进行入侵检测，则应将内部区域选为**目标区域**，同时将源区域保留为空。要在规则中实施入侵过滤，则规则操作必须为**允许**，并且必须在该规则中选择入侵策略。

注释 不能在同一规则中搭配使用被动和路由安全区。此外，被动安全区只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置**源网络**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络**。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。
- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

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)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。对于 ICMP，可包括代码和类型。

- 要匹配来自协议或端口的流量，请配置**源端口**。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置**目标端口/协议**。如果仅将目标端口添加至条件，则可以添加使用不同传输协议的端口。ICMP 和其他非 TCP/UDP 规格仅可用于目标端口，不允许用于源端口。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

源 SGT 组、目的地 SGT 组

从身份服务引擎 (ISE) 下载的标识分配给流量的安全组标记 (SGT) 的 SGT 组对象。仅当定义 ISE 身份源时，才能使用这些对象；否则，此部分将不会显示。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 ，第 29 页。

- 要匹配源具有组中定义的一个 SGT 的流量，请配置**源 SGT 组**。
- 要匹配流向具有组中定义的一个 SGT 的目的地的流量，请配置**目的地 SGT 组**。
- 如果同时向一条规则添加源和目的地 SGT 条件，匹配规则的流量必须来自具有其中一个指定标记的源并流向其中一个标记目的地。

应用条件

访问规则的“应用”条件对 IP 连接中使用的应用进行定义，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何应用。

虽然您可以在规则中指定个别应用，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。

另外，思科会通过系统和漏洞数据库 (VDB) 更新频繁更新和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。

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。

要修改应用和过滤器列表，请点击该条件内的 + 按钮，选择在单独选项卡中列出的相应应用或应用过滤器对象，然后在弹出对话框中点击**确定**。在任一选项卡中，您可以点击**高级过滤器**选择过滤器条件或帮助您搜索特定应用。点击应用、过滤器或对象的 **x**，可将其从策略中移除。点击**另存为过滤器**链接，可将尚不是对象的组合条件另存为新应用过滤器对象。

注释 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。

您可以使用以下**高级过滤器**条件来标识规则中要匹配的应用或过滤器。这些元素与应用过滤器对象中使用的元素相同。

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。

URL 标准

访问规则中的 URL 标准对 Web 请求中使用的 URL 或请求的 URL 所属的类别进行定义。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。默认设置为允许所有 URL。

如果启用 DNS 查找请求过滤，则类别和信誉设置也会应用于查找请求中的完全限定域名 (FQDN)。仅类别和信誉设置适用于 DNS 请求过滤。忽略手动 URL 过滤。

URL 类别和信誉可供您快速创建访问控制规则的 URL 标准。例如，您可阻止所有赌博网站或不受信任的社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于思科的威胁智能会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的恶意站点出现和消失的速度可能比您更新和部署新策略的速度要快。

要修改 URL 列表，请点击该条件内的 + 按钮，使用以下任一方法选择所需的类别或 URL。点击类别或对象的 **x**，可将其从策略中删除。

URL 选项卡

点击 +，选择 URL 对象或组，然后点击**确定 (OK)**。如果所需的对象不存在，可以点击**创建新 URL (Create New URL)**。

注释 在配置特定目标站点的 URL 对象之前，请仔细阅读有关手动 URL 过滤的信息。

“类别”选项卡

点击 +，选择所需的类别，然后点击**确定 (OK)**。

有关类别说明，请参阅 https://www.talosintelligence.com/categories。

默认为将规则应用于每个选定类别的所有 URL，不考虑信誉。要根据信誉限制规则，请点击每个类别的向下箭头，取消选中**任何 (Any)** 复选框，然后使用**信誉 (Reputation)** 滑块选择信誉级别。信誉滑块的左侧指示要允许的站点，右侧是要阻止的站点。如何使用信誉取决于规则操作：

- 如果该规则阻止或监控网络访问，则选择某个信誉级别也会选择高于该级别的所有信誉。例如，如果将规则配置为阻止或监控**问题站点**（第 2 级），该规则还会自动阻止或监控**不受信任**（第 1 级）站点。
- 如果该规则允许网络访问，则选择某个信誉级别也会选择低于该级别的所有信誉。例如，如果您将规则配置为允许**可靠站点**（第 4 级），该规则还会自动允许**受信任**（第 5 级）站点。

选择**包含信誉未知的站点**选项，可使具有未知信誉的URL包括在信誉匹配项中。新站点通常未评级，并且站点的信誉可能会由于其他原因而未知或无法确定。

检查 URL 的类别

您可以检查特定 URL 的类别和信誉。在**待检查的 URL** 框中输入 URL，然后点击**前往**。系统会将您转至外部网站以查看结果。如果您对分类持有不同意见，请点击**提交 URL 类别争议**链接，将您的想法反馈给我们。

用户条件

访问规则的“用户”条件对IP连接的用户或用户组进行了定义。只有配置身份策略和相关联的目录服务器，才能在访问规则中包括用户或用户组条件。

您的身份策略决定是否收集某个特定连接的用户身份。如果建立了身份，则主机的IP地址与所识别的用户相关联。因此，源IP地址映射到用户的流量将被视为来自该用户。IP数据包本身不包含用户身份信息，所以此 IP 地址到用户的映射是最接近的近似值。

由于最多可以向规则中添加50个用户或组，所以选择组比选择单个用户通常更有意义。例如，您可以创建一条规则允许“工程”组访问开发网络，并创建一条后续规则拒绝对该网络的所有其他访问。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

您还可以选择身份源，以应用于该源中的所有用户。因此，如果您支持多个 Active Directory 域，您可以根据域提供不同的资源访问。

要修改用户列表，请点击该条件内的 + 按钮，并使用以下任一方法选择所需的身份。点击身份对应的 **x**，可将其从策略中删除。

- **身份源** - 选择身份源，例如 AD 领域或本地用户数据库，以将规则应用于从所选源获取的所有用户。如果所需的领域尚不存在，请点击**创建新身份领域**并立即创建。
- **组** - 选择所需的用户组。只有在目录服务器中配置了组，才能使用组。如果您选择了某个组，规则将应用于该组的所有成员，包括子组。如果要区别对待某个子组，您需要针对该子组创建一条单独的访问规则，并将其置于访问控制策略中适用于父组的规则之上。
- **用户** - 选择单个用户。用户名使用身份源作为前缀，例如“领域\用户名”。

  特殊身份领域中存在一些内置用户：

  - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。
  - **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
  - **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。
  - **未知** - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。

入侵策略设置

Cisco 通过防火墙系统提供多种入侵策略。Cisco 思科 Talos 情报小组 (Talos) 交付的一些入侵策略由 Cisco.Talos 设计，其设定了入侵和预处理器规则的状态和高级设置。对于允许流量的访问控制规则，您可以选择入侵策略来检测流量中是否存在入侵和攻击程序。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。

运行 Snort 2 时，这些是唯一可用的策略，并且您无法修改这些策略。不过，您可以更改要对给定规则执行的操作，如更改入侵规则操作 (Snort 2)中所述。

运行 Snort 3 时，您可以选择其中一个策略，也可以创建自己的入侵策略。

要启用入侵检测，请选择**入侵策略** > **开**，然后选择所需策略。点击下拉列表中策略的信息图标，可查看每个策略的说明。

有关预定义策略的详细信息，请参阅系统定义的网络分析和入侵策略。

文件策略设置

使用文件策略来检测恶意软件，或 恶意软件，使用恶意软件防御。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

恶意软件防御使用 Cisco Secure Malware Analytics 云 检索网络流量中检测到的潜在恶意软件的处置，并获取本地恶意软件分析和文件预分类更新。管理接口必须可连接互联网，以便访问 Cisco Secure

Malware Analytics 云 并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 Cisco Secure Malware Analytics 云 中是否存在该文件的处置。可能的处置包括：

- 恶意软件 - Cisco Secure Malware Analytics 云 将文件归类为恶意软件。如果其中的任何文件为恶意软件，存档文件（例如 zip 文件）会被标记为恶意软件。
- 安全 - Cisco Secure Malware Analytics 云 将文件归类为安全，不含恶意软件。如果其中的所有文件都安全，存档文件将会标记为安全。
- 未知 - Cisco Secure Malware Analytics 云 尚未指定该文件的处置。如果其中的任何文件属于未知状态，存档文件会被标记为未知。
- 不可用 - 系统无法通过查询 Cisco Secure Malware Analytics 云 来确定文件的处置。您可能看到很少一部分事件为此处置；这是预期行为。如果您连续看到许多“不可用”事件，请确保管理地址的互联网连接正常运行。

可用的文件策略

您可以选择下列文件策略之一：

- **无** - 不评估传输的文件中是否存在恶意软件，且不阻止特定的文件。对于文件传输受信任或不可能传输文件的规则或您相信自己的应用或URL过滤可适当保护网络的规则，请选择此选项。
- **阻止所有恶意软件**- 查询 Cisco Secure Malware Analytics 云 以确定通过网络传输的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **全部执行云查找**- 查询 Cisco Secure Malware Analytics 云以获取和记录通过网络传输的文件的处置，同时仍允许文件传输。
- （**自定义文件策略**）- 可以使用 威胁防御 API filepolicies 资源和其他 FileAndMalwarePolicies 资源（例如 filetypes、filetypecategories、ampcloudconfig、ampservers 和 ampcloudconnections）创建您自己的文件策略。创建策略并部署更改后，可以在编辑 设备管理器中的访问控制规则时选择策略。选择策略说明后，策略说明会显示在策略下方。

日志记录设置

访问规则的日志记录设置确定是否对匹配规则的流量发出连接事件。只有启用日志记录，才能在事件查看器中查看与该规则相关的事件。另外，您还必须启用日志记录，才能使匹配流量反映到可用于监控系统的各种控制面板中。

您应该根据您组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。

注意 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口。

您可以配置以下日志记录操作。

选择日志操作

可以选择下列操作之一：

- **在连接开始和结束时记录** - 在连接开始和结束时发出事件。由于连接结束事件包含连接开始事件所含的一切，以及连接期间可能收集的所有信息，所以思科建议不要对允许的流量选择此选项。记录两种事件可能会影响系统性能。但是，这是针对阻止的流量唯一允许的选项。
- **在连接结束时记录** - 如果要在连接结束时启用连接日志记录（建议对允许或受信任的流量执行此操作），请选择此选项。
- **在连接时不执行日志记录** - 选择此选项，可对规则禁用日志记录。这是默认值。

注释 当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，系统会在发生入侵的位置自动记录连接终止，无论该规则的日志记录配置如何。对于入侵受阻的连接，连接日志中的连接操作为**阻止**，原因为**入侵阻止**，即使执行入侵检测，也必须使用“允许”规则。

文件事件

如果要对禁止文件或恶意软件事件启用日志记录，请选择**日志文件**。只有在规则中选择了文件策略，才能配置此选项。如果对规则选择了文件策略，则该选项默认处于启用状态。思科建议您将此选项保留为已启用。

当系统检测到受禁文件时，它会自动记录以下类型的事件之一：

- 文件事件，代表检测到或阻止的文件，包括恶意软件文件。
- 恶意软件事件，仅代表检测到或阻止的恶意软件文件。
- 可追溯的恶意软件事件，在之前检测到的文件的恶意软件处置变更时生成。

对于文件受阻的连接，连接记录中的连接操作为**阻止**，即便要执行文件和恶意软件检测，也必须使用“允许”规则。连接原因是**文件监控**（检测到某种文件类型或恶意软件）或者是**恶意软件阻止**或**文件阻止**（文件被阻止）。

将连接事件发送到

如果要将事件副本发送到外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择**任何**）。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

此设置仅适用于连接事件。要将入侵事件发送到系统日志，请在入侵策略设置中配置服务器。要将文件/恶意软件事件发送到系统日志，请在**设备** > **系统设置** > **日志记录设置**中配置服务器。

监控访问控制策略

以下主题介绍如何监控访问控制策略。

在控制面板中监控访问控制统计信息

监控控制面板上的大多数数据与您的访问控制策略直接相关。请参阅监控流量和系统控制面板。

- **监控 (Monitoring)** > **访问和 SI 规则 (Access And SI Rules)**显示点击量最高的访问规则及安全智能规则等效对象和相关统计信息。
- 可以在**网络概述**、**目标**和**区域**控制面板找到常规统计信息。
- 可以在 **URL 类别**和**目标**控制面板找到 URL 过滤结果。必须至少有一个 URL 过滤策略，才可在 **URL 类别**控制面板看到任何信息。
- 可以在**应用**和 **Web 应用**控制面板找到应用过滤结果。
- 还可以在**用户**控制面板找到基于用户的统计信息。只有实施身份策略才能收集用户信息。
- 可以在**攻击者**和**目标**控制面板找到入侵策略统计信息。必须将入侵策略应用于至少一个访问控制规则，才能在这些控制面板上看到任何信息。
- 可以在**文件日志**和**恶意软件**控制面板找到文件策略和恶意软件过滤统计信息。必须将文件策略应用于至少一个访问控制规则，才能在这些控制面板上看到任何信息。
- **监控** > **事件**还显示与访问控制规则相关的连接和数据的事件。

检查规则命中计数

您可以查看每个访问控制规则的命中计数。命中计数表示连接与规则匹配的频率。可以使用此信息来确定最活跃的规则和不活跃的规则。

通过重新启动和升级，计数仍然存在。

您还可以使用 **show rule hits** 命令在设备 CLI 中查看规则命中计数信息。

过程

步骤 1 依次选择**策略** > **访问控制**。

步骤 2 点击**切换命中计数**图标 ( )。

命中计数列位于名称列的右侧，显示规则的总命中计数以及最后一次命中的日期和时间。点击切换按钮可即刻获取命中计数信息。

您可以使用命中计数信息执行以下操作：

- 在按钮左侧，您将看到有关命中次数最后更新时间的信息。点击**刷新**图标( )可获取最新数字。

- 要打开给定规则命中计数的详细视图，请点击表中的命中计数数字，打开命中计数对话框。命中计数信息包括命中数和与规则匹配的最后一次连接的日期和时间。点击**重置**链接可将计数器重置为零。

  如果您想要一次性重置所有规则的命中计数，请打开与设备的 SSH 会话并发布 **clear rule hits** 命令。

- 再次点击**切换命中计数**图标 ()，从表中删除命中计数列。

监控访问控制系统日志消息

除了在事件查看器中查看事件外，您还可以配置访问控制规则、入侵策略、文件/恶意软件策略和安全智能策略，以将事件发送到系统日志服务器。事件使用以下消息 ID：

- 430001 - 入侵事件。
- 430002 - 连接开始时记录的连接事件。
- 430003 - 在连接结束时记录的连接事件。
- 430004 - 文件事件。
- 430005 - 恶意软件事件。

在 CLI 中监控访问控制策略

您还可以打开 CLI 控制台或登录设备 CLI，使用以下命令获取有关访问控制策略和统计信息的更多详细信息。

- **show access-control-config** 显示访问控制规则的摘要信息以及每个规则的命中计数。
- **show access-list** 显示基于访问控制规则生成的访问控制列表 (ACL)。ACL 提供初始过滤器并尝试尽可能提供快速决策，以使应丢弃的连接不需要接受检测（从而避免不必要的资源消耗）。此信息包括命中计数。
- **show rule hits** 显示汇总命中计数，这比使用 **show access-control-config** 和 **show access-list** 显示的计数更加准确。如果您想要重置命中次数，请使用 **clear rule hits** 命令。
- **show snort statistics** 显示 Snort 检测引擎（主要检测程序）的相关信息。Snort 实施应用过滤、URL 过滤、入侵防护以及文件和恶意软件过滤。
- **show conn** 显示当前通过接口建立的连接的相关信息。
- **show traffic** 显示流过每个接口的流量的相关统计信息。
- **show ipv6 traffic** 显示流过设备的 IPv6 流量的相关统计信息。

访问控制示例

使用案例章节涵盖多个实施访问控制规则的示例。请参阅下面的示例：

- 如何深入了解您的网络流量。此示例展示收集整体的连接和用户信息的一些基本概念。
- 如何阻止威胁。此示例展示如何应用入侵策略。
- 如何阻止恶意软件。此示例展示如何应用文件策略。
- 如何实施可接受使用策略（URL 过滤）。此示例展示如何执行 URL 过滤。
- 如何控制应用的使用。此示例展示如何执行应用过滤。
- 如何添加子网。此示例展示如何将新的子网集成到整个网络，包括允许流量所需的访问规则。
- 如何被动监控网络上的流量

以下是其他示例。

如何使用 TrustSec 安全组标记控制网络访问

如果使用思科身份服务引擎 (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。因此，可以基于安全组成员身份阻止或允许访问，而不是直接使用 IP 地址。

关于安全组标记 (SGT)

在思科身份服务引擎(ISE)中，可以创建安全组标记(SGT)，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。

在 设备管理器中配置 ISE 身份源时， 威胁防御 系统会自动从 ISE 下载 SGT 列表。然后，可以使用 SGT 作为访问控制规则中的流量匹配条件。

例如，可以创建生产用户标记，并将 192.168.7.0/24 网络与标记相关联。如果将该网络用于用户终端（例如笔记本电脑、Wi-fi 客户端等），这将适用。可以创建用于生产服务器的单独标记，并将相关服务器或子网的IP地址分配给该标记。然后，在威胁防御中，可以根据标记允许或阻止从用户网络到生产服务器的访问。如果稍后修改 ISE 中标记所关联的主机或网络地址，则无需更改定义用于 威胁防御 设备的访问控制规则。

威胁防御 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。
2. 分配给用户会话的 SGT，从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息，但是，当您首次创建 ISE 身份源时，此选项会默认打开。SGT 可以与源或目标相匹配。尽管非必需，但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则，以收集用户身份信息。

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。

   ISE 使用安全组交换协议 (SXP) 将 IP 到 SGT 的映射数据库传播至网络设备。当您将 威胁防御 设备配置为使用 ISE 服务器时，必须打开该选项才能从 ISE 侦听 SXP 主题。因此，威胁防御 设备直接从 ISE 了解安全组标记和映射，且每当 ISE 发布更新的安全组标记和映射时均会收到通知。这可确保安全组标签和映射列表在设备上保持最新状态，以便 威胁防御 能够有效地实施 ISE 中定义的策略。

基于安全组标记 (SGT) 配置访问控制

要配置使用安全组标记 (SGT) 作为匹配条件的访问控制规则，必须先配置设备以从 ISE 服务器获取 SGT 映射。

以下程序根据您想要获取 ISE 中定义的所有映射（包括通过 SXP 发布的 SGT 到 IP 地址映射）来解释端到端流程。或者：

- 如果要仅使用数据包中的 SGT 信息，而不使用从 ISE 下载的映射，只需创建 SGT 组动态对象并将其用作访问控制规则中的源 SGT 标准。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。
- 如果仅希望在数据包中使用 SGT 和用户会话 SGT 映射，则无需打开该选项以订阅 ISE 身份源中的 SXP 主题，也无需配置 ISE 以发布 SXP 映射。您可以将此信息用于源匹配条件和目标匹配条件。

开始之前

假设您已在网络中配置 Cisco TrustSec，而您只是将 威胁防御 设备作为策略实施点添加。如果尚未部署 Cisco TrustSec，请从 ISE 开始并配置您的网络，然后返回至此过程。说明 Cisco TrustSec 超出本文档范围。

过程

步骤 1 确保已定义 SGT，已正确配置 ISE 以发布 SXP 主题，并且所有所需的静态映射都已部署到位。

请参阅在 ISE 中配置安全组和 SXP 发布 ， 第 32 页。

步骤 2 更新身份服务引擎对象以侦听 SXP 主题。

您可以使用 ISE 通过 SXP 获取用户会话 SGT 映射和/或静态 SGT 到 IP 地址映射。默认情况下，配置 ISE 身份源时，仅获取用户会话映射；必须打开该选项才能从 ISE 侦听 SXP 主题。

a) 依次选择**对象** > **身份源**。
b) 编辑 ISE 对象。如果尚未配置，请点击 + > **身份服务引擎**，并查看配置身份服务引擎。
c) 在**订用**下，选择 **SXP 主题**。

   如果您正在使用被动身份验证或需要“用户到 SGT”映射，请确保还选择了**会话目录主题**。

d) 点击**确定 (OK)**。

步骤 3 部署更改并等待系统从 ISE 下载标记和映射。

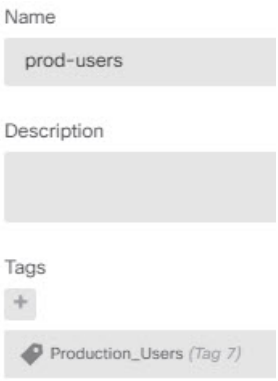
配置 ISE 身份源并部署更改后，系统会从 ISE 服务器检索安全组标记 (SGT) 信息。在部署更改之前，无法进行下载。

步骤 4 创建访问控制规则所需的 SGT 组对象。

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。

对象的数量和内容取决于要编写的访问控制规则。重复以下过程，创建您所需的所有对象。

a) 依次选择**对象** > **SGT 组**。
b) 点击 **+** 以添加新对象，或编辑现有对象。
c) 为新对象输入名称和说明（后者为可选项）。
d) 在**标记 (Tags)** 下，点击 **+** 并选择应包含在组中的所有标记。



e) 点击**确定 (OK)**。

步骤 5 创建使用 SGT 组对象的访问控制规则。

例如，以下规则允许从生产用户到生产服务器的流量。该规则完全取决于 SGT；不受源/目标接口或任何其他条件的限制。因此，该规则将动态应用于来自不同接口的流量，且在 ISE 中更改安全组成员身份。如果数据包未明确包含源 SGT，则源/目的地匹配将基于数据包 IP 地址，与从用户会话信息或从 SXP 发布的映射获取的“SGT 到 IP 地址”映射进行比较。

a) 依次选择**策略** > **访问控制**。
b) 点击 **+** 新建一条规则或编辑现有规则。
c) 输入规则名称并选择**允许**作为操作。
d) 在**源/目的地 (Source/Destination)** 选项卡上，点击**源 (Source)** > **SGT 组 (SGT Groups)**下的 **+**，然后选择为生产用户创建的对象。

e) 在**源/目的地 (Source/Destination)** 选项卡上，点击**目的地 (Destination)** > **SGT 组 (SGT Groups)**下的 **+**，然后选择为生产服务器创建的对象。

f) 请根据需要配置其他选项。例如，您可以启用日志记录并应用入侵策略。

g) 点击**确定 (OK)**。

步骤 6 部署配置。

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。

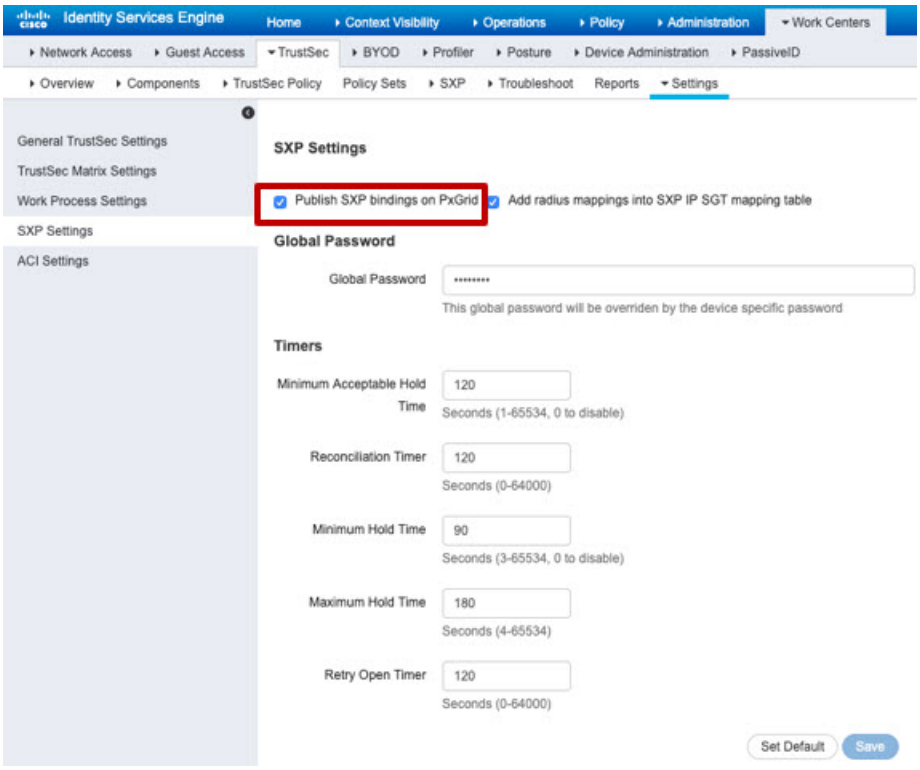
开始之前

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

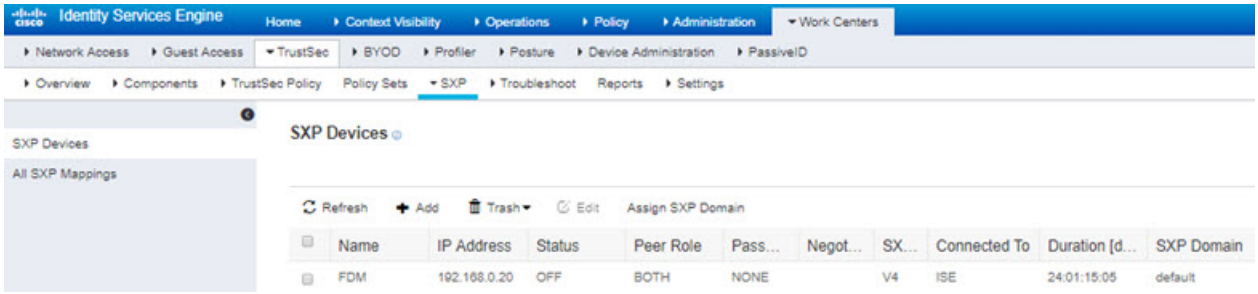
步骤 1 选择**工作中心** > **TrustSec** > **设置** > **SXP 设置**，然后选择**在 PxGrid 上发布 SXP 绑定**选项。

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。

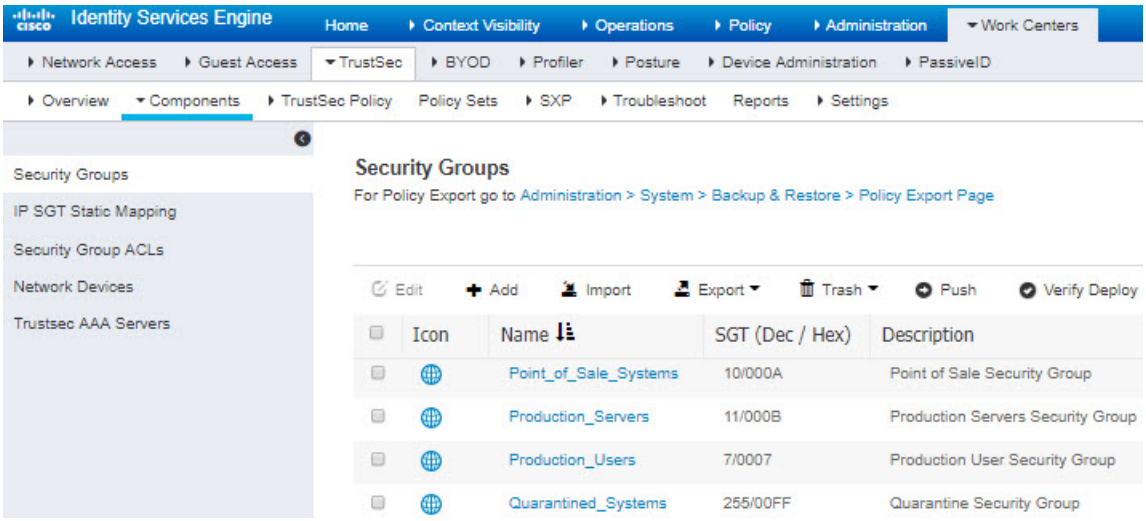


步骤 2 选择**工作中心** > **TrustSec** > **SXP** > **SXP 设备**，然后添加设备。

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。

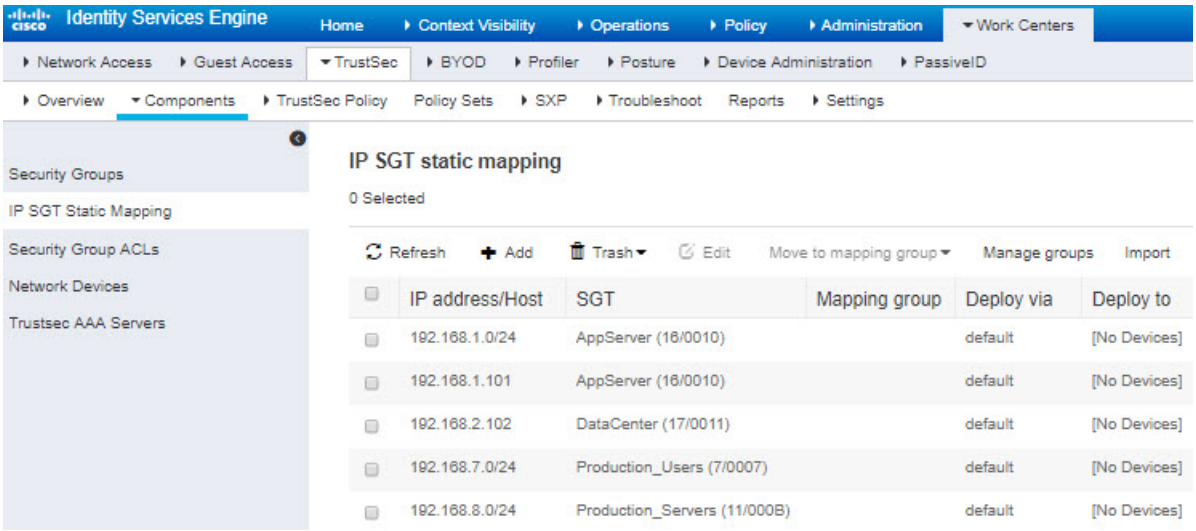


步骤 3 选择**工作中心** > **TrustSec** > **组件** > **安全组**并验证是否定义了安全组标记。按需新建。



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。



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。