TLS/SSL 规则

以下主题概述了 TLS/SSL 规则 的创建、配置、管理和故障排除：

注释 由于 TLS 和 SSL 通常可以互换使用，因此我们使用 *TLS/SSL* 来指示所讨论的任一协议。IETF 已弃用 SSL 协议以支持更安全的 TLS 协议，因此您通常可将 *TLS/SSL* 解读为仅指代 TLS。

但 SSL 策略 是个例外。由于 管理中心 配置选项是 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**，我们使用术语 *SSL* 策略 ，尽管这些策略是用于定义 TLS 和 SSL 流量的规则。

有关 SSL 和 TLS 协议的更多信息，请参阅 SSL 与 TLS - 差别何在？ 等资源。

TLS/SSL 规则概述

TLS/SSL 规则 提供一种精细的方法来跨多台受管设备处理加密流量：阻止流量而不进一步检查；不解密流量并通过访问控制对其进行检查；或者解密流量以进行访问控制分析。

TLS/SSL 规则 准则和限制

在设置 TLS/SSL 规则 时，请记住以下要点。正确配置 TLS/SSL 规则 是一项复杂的任务，但是对于构建用于处理加密流量的有效部署至关重要。许多因素会影响您配置规则的方式，包括您无法控制的特定应用行为。

此外，规则可以互相抢占，需要其他许可证或包含无效配置。周全配置的 SSL 规则还可以减少处理网络流量所需的资源。创建过度复杂的规则和以错误方式对规则进行排序可能会对性能产生不利影响。

有关详细信息，请参阅访问控制规则的最佳实践。

有关 TLS 加密加速的具体准则，请参阅TLS 加密加速。

相关主题

使用 TLS/SSL 解密的准则

一般准则

仅当托管设备处理加密流量时，才设置**解密 - 重新签名**或**解密 - 已知密钥**规则。TLS/SSL 规则 需要处理可能会影响性能的开销。

您无法在具有被动或内联分流模式接口的设备上解密流量。

无法解密的流量准则

我们可以确定某些流量不可解密，要么是因为网站本身不可解密，要么是因为该网站使用了 SSL 锁定，这有效地阻止了用户访问其浏览器中没有错误的已解密网站。

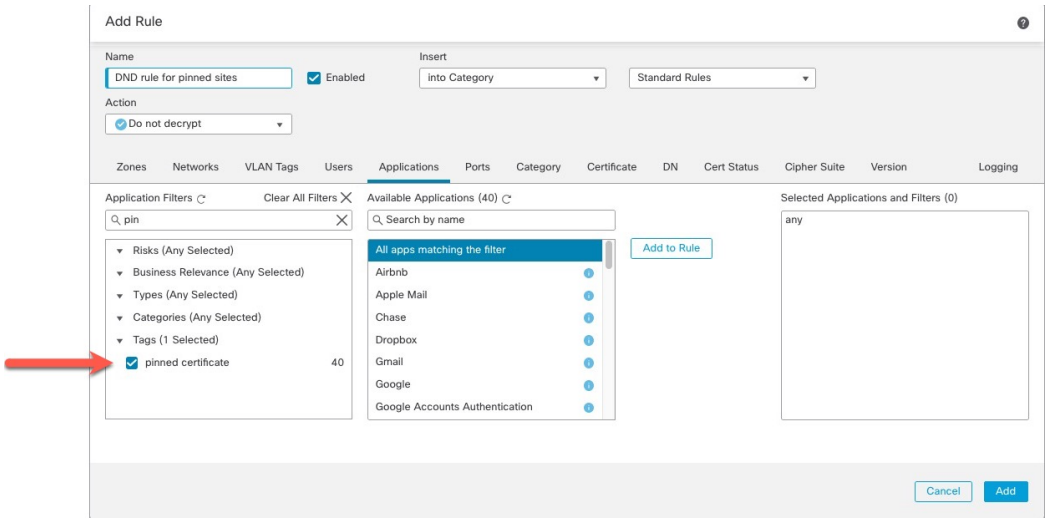
有关证书锁定的详细信息，请参阅关于 TLS/SSL 锁定，第 38 页。

我们维护的这些站点的列表如下：

- 名为 **Cisco-Undecryptable-Sites** 的可分辨名称 (DN) 组
- **已固定证书**应用过滤器

如果您正在解密流量，并且不希望用户在访问这些站点时在其浏览器中看到错误，我们建议您在 TLS/SSL 规则 底部设置**不解密规则**。

设置**已固定证书**应用过滤器的示例如下。



TLS/SSL 规则不支持的功能

不支持 RC4 密码套件

众所周知，Rivest Cipher 4（也称为 *RC4* 或 *ARC4*）密码套件存在漏洞，被认为是不安全的。SSL 策略 会将 RC4 密码套件识别为不受支持；应在策略的**无法解密的操作 (Undecryptable Actions)** 选项卡页面中配置**不支持的密码套件 (Unsupported Cipher Suite)** 操作，以满足您的组织的要求。有关详细信息，请参阅无法解密流量的默认处理选项。

不支持被动、内联分流模式以及 SPAN 接口

无法在被动、内联分流模式或 SPAN 接口上解密 TLS/SSL 流量。

规则名称中的字符不受支持

请勿在 TLS/SSL 规则 规则名称中使用带重音的字符（例如 Comunicación）；这样做可防止将策略部署到受管设备。

TLS/SSL 不解密准则

如果是以下情况，则不应对流量进行解密：

- 法律所禁止；例如，某些司法管辖区禁止解密财务信息
- 公司政策所禁止；例如，您的公司可能会禁止解密特权通信
- 隐私法规所禁止
- 使用证书固定（也称为*TLS/SSL*固定）的流量必须保持加密，以防止断开连接

加密流量可以在任何 TLS/SSL 规则 条件下被允许或阻止，包括但不限于：

- 证书状态（例如，证书已过期或无效）

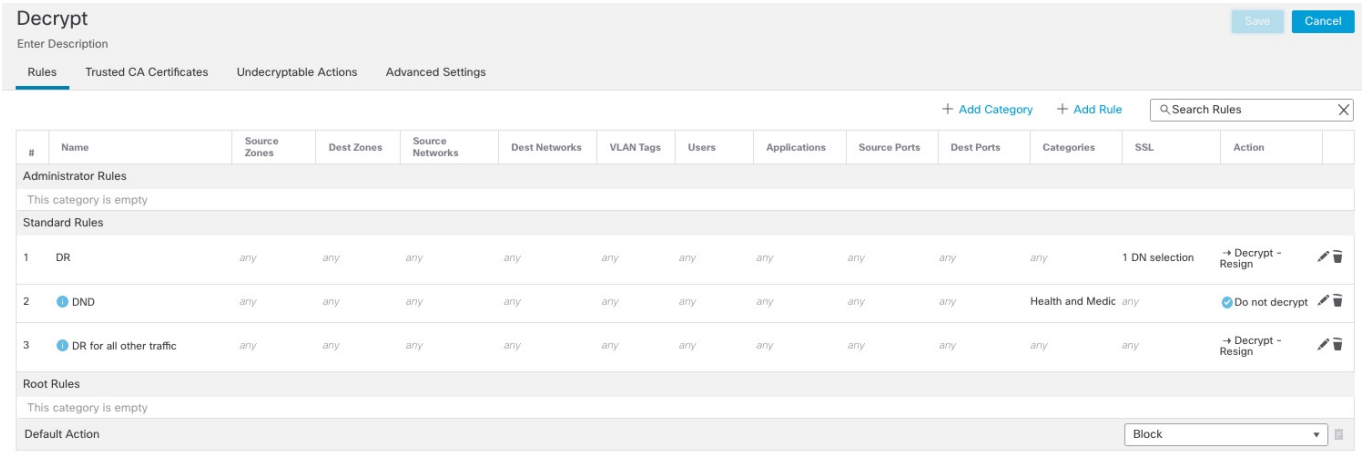
- 协议（例如，非安全 SSL 协议）
- 网络（安全区域、IP 地址、VLAN 标记等）
- 确切的 URL 或 URL 类别
- Port
- 用户组

“不解密”规则中的类别限制

您可以选择在 SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 情报组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进 URL 过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅 使用 TLS/SSL 解密的准则，第 2 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践。

TLS/SSL 解密 - 重新签名准则

您可以将一个内部证书颁发机构 (CA) 证书和私钥与**解密 - 重新签名 (Decrypt - Resign)** 操作相关联。如果流量与此规则相匹配，则系统会使用 CA 证书对服务器证书重新签名，然后充当中间人。它创建两个 TLS/SSL 会话，一个是客户端与受管设备之间的会话，一个是受管设备与服务器之间的会话。每个会话包含不同的加密会话详细信息，并且允许系统解密并重新加密流量。

最佳实践

我们的建议如下：

- 使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作解密传出流量，而不是建议使用**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作的传入流量。

  有关**解密 - 已知密钥**的详细信息，请参阅TLS/SSL 解密 - 已知密钥准则，第 6 页。

- 在设置**机密 - 重新签名 (Decrypt - Resign)** 规则操作时始终选中**仅更换密钥 (Replace Key Only)** 复选框。

  当用户浏览到使用自签名证书的网站时，他们会在 Web 浏览器中看到安全警告，并会意识到自己正在与不安全的站点通信。

  当用户浏览到使用受信任证书的网站时，他们不会看到安全警告。

详情

如果配置具有**Decrypt - Resign**操作的规则，则除任何已配置的规则条件外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您将一个 CA 证书与 **Decrypt - Resign** 操作相关联，因此无法创建用来解密使用不同签名算法加密的多种类型的传出流量的 TLS/SSL 规则。此外，添加到规则中的任何外部证书对象和密码套件都必须与关联的 CA 证书加密算法类型相匹配。

例如，仅当操作引用基于椭圆曲线 (EC) 的 CA 证书时，使用 EC 算法加密的传出流量才会与**解密 - 重新签名**规则相匹配；必须将基于 EC 的外部证书和密码套件添加到此规则，以创建证书和密码套件规则条件。

同样，引用基于 RSA 的 CA 证书的 **Decrypt - Resign** 规则仅与使用 RSA 算法加密的传出流量相匹配；使用 EC 算法加密的传出流量与该规则不匹配，即使所有其他已配置的规则条件都匹配也如此。

准则和限制

另请注意以下提示：

不支持的匿名密码套件

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为匿名密码套件不用于身份验证。

“解密 - 重新签名”规则操作和证书签名请求

要使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作，应创建证书签名请求 (CSR) 并由受信任的证书颁发机构签名。（您可以使用 FMC 创建 CSR：**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)**。）

要在解密 - 重新签名规则中使用，您的证书颁发机构 (CA) 必须至少具有以下扩展名之一：

- **CA: TRUE**

  有关详细信息，请参阅 RFC3280 第 4.2.1.10 节中对基本限制的讨论。

- **KeyUsage=CertSign**

  有关详细信息，请参阅 RFC 5280 第 4.2.1.3 节。

要验证您的 CSR 或 CA 是否至少具有上述扩展名之一，您可以按照 openssl 文档等参考资料中的说明来使用 **openssl** 命令。

这是必要的，因为要使**解密 - 重新签名 (Decrypt - Resign)** 检查工作，SSL 策略 中使用的证书会即时生成证书并对其进行签名，以便充当中间人并代理所有 TLS/SSL 连接。

证书固定

如果客户的浏览器使用证书锁定来验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。要允许此流量，请配置一个 TLS/SSL 规则，将**不解密**操作与服务器证书公用名或可分辨名称相匹配。

不匹配的密码套件

如果尝试使用与证书不匹配的密码套件保存 TLS/SSL 规则，则会显示以下错误。要解决此问题，请参阅验证 TLS/SSL 密码套件，第 42 页。

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

不受信任的证书颁发机构

如果客户端不信任用于对服务器证书重新签名的证书颁发机构 (CA)，则会警告用户不应信任该证书。为了避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织拥有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。

HTTP 代理限制

如果 HTTP 代理位于客户端和受管设备之间，并且客户端和服务器使用 CONNECT HTTP 方法建立隧道化 TLS/SSL 连接，则系统无法解密流量。**Handshake Errors** 无法解密操作将决定系统如何处理此流量。

上传签名的 CA

如果创建内部 CA 对象并选择生成证书签名请求 (CSR)，那么在将签名证书上传到对象之前，会无法对 **Decrypt - Resign** 操作使用此 CA。

不匹配的签名算法

如果配置具有 **Decrypt - Resign** 操作的规则，并且不匹配一个或多个外部证书对象或密码套件的签名算法类型，则策略编辑器在该规则旁边显示**信息**（  ）。如果所有外部证书对象或所有密码套件的签名算法类型不匹配，则策略在该规则旁边显示警告图标**警告**（  ），并且无法部署与 SSL 策略相关联的访问控制策略。

TLS/SSL 解密 - 已知密钥准则

当配置 **Decrypt - Known Key** 操作时，可以将一个或多个服务器证书和配对私钥与该操作相关联。如果流量与规则相匹配，并且用于加密流量的证书与操作的关联证书相匹配，则系统会使用相应的

私钥获取会话加密和解密密钥。由于您必须有权访问私钥，此操作最适合于解密传入到组织控制的服务器的流量。

另请注意以下提示：

不支持的匿名密码套件

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为匿名密码套件不用于身份验证。

无法匹配可分辨名称或证书

创建具有**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 TLS/SSL 规则 时，无法使用**可分辨名称 (Distinguished Name)** 或**证书 (Certificate)** 条件进行匹配。此限制基于这样一种假设：如果此规则与流量相匹配，则证书、使用者 DN 和颁发者 DN 已经与规则的关联证书相匹配。

椭圆曲线数字签名算法 (*ECDSA*) 证书会导致流量被阻止。

（仅启用 TLS 1.3 解密。）如果将 ECDSA 证书与**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作配合使用，则会阻止匹配的流量。要避免这种情况，请将证书与其他类型的证书配合使用。

TLS/SSL 阻止准则

如果解密流量与具有**交互式阻止 (Interactive Block)** 或**交互式阻止并重置 (Interactive Block with reset)** 操作的访问控制规则相匹配，则系统会显示可自定义的响应页面。

如果您在规则中启用了日志记录，则会显示两个连接事件（在**分析 (Analysis)** > **事件 (Events)** > **连接 (Connections)**）：一个事件用于交互式阻止，而另一个事件用于指示用户是否选择继续访问站点。

相关主题

配置 HTTP 响应页面

TLS/SSL 证书固定准则

某些应用使用称为 *TLS/SSL* 锁定或证书锁定的技术，其在应用自身中嵌入原始服务器证书的指纹。因此，如果您配置具有**解密 - 重签**操作的 TLS/SSL 规则，则应用从受管设备收到重签的证书时，验证会失败且连接会中止。

由于 TLS/SSL 锁定用于避免中间人攻击，因此无法不能将其阻止或绕过。您有以下选择：

- 为排在**解密 - 重签**规则之前的应用创建**不解密**规则。
- 指示用户使用网络浏览器访问应用。

有关规则排序的详细信息，请参阅SSL 规则顺序。

要确定应用是否正在使用 TLS/SSL 锁定，请参阅对 TLS/SSL 锁定进行故障排除 ， 第 39 页。

TLS/SSL 心跳准则

某些应用使用RFC6520定义的传输层安全(TLS)和数据报传输层安全(DTLS)协议的*TLS*心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

您可以在网络分析策略(NAP)中配置**最大心跳长度**，以便确定如何处理 TLS 心跳。有关详细信息，请参阅SSL 预处理器。

有关详细信息，请参阅关于 TLS 心跳，第 37 页。

TLS/SSL 匿名密码套件限制

本质上，匿名密码套件并不用于身份验证，也不使用密钥交换。匿名密码套件的用途有限；有关详细信息，请参阅 RFC 5246，附录 F.1.1.1。（TLS 1.3 已被替换为 RFC 8446 附录 C.5。）

无法在规则中使用**解密 - 重新签名 (Decrypt - Resign)**或**解密 - 已知密钥 (Derypt - Known Key)**操作，因为匿名密码套件不用于身份验证。

您可以将匿名密码套件添加到TLS/SSL规则的**密码套件**条件中，但系统会在ClientHello处理期间自动删除匿名密码套件。要让系统使用该规则，还必须配置TLS/SSL规则的顺序以阻止ClientHello处理。有关详细信息，请参阅SSL 规则顺序。

TLS/SSL 标准化程序准则

如果启用内联规范化预处理器中的**规范化多余负载**选项，则预处理器在规范化解密流量时，可能会丢弃数据包并将其替换为修整过的数据包。这不会结束 TLS/SSL 会话。如果允许流量，则修整过的数据包会作为 TLS/SSL 会话的一部分加密。

其他 TLS/SSL 规则 准则

用户和组

如果向规则中添加用户或组，然后更改领域设置以排除该组或用户，规则将不会生效。（同样适用于禁用领域。）有关领域的更多信息，请参阅创建 Active Directory 领域和领域目录。

TLS/SSL 规则 中的类别

如果您的 SSL 策略具有**解密 - 重新签名 (Decrypt - Resign)**操作，但网站不会被解密，请检查与该策略相关的规则的**类别 (Category)**页面。

在某些情况下，网站重定向到另一个站点进行身份验证或实现其他目的，而重定向的站点可能具有与您正在尝试解密的站点不同的 URL 分类。例如，`gmail.com`（**基于 Web 的电子邮件**类别）将重定向到`accounts.gmail.com`（**互联网门户**类别）进行身份验证。请务必在 SSL 规则中包含所有相关类别。

注释 为了根据 URL 类别完全处理流量，您还必须配置 URL 过滤。请参阅URL 过滤一章。

查询不在本地数据库中的 URL

如果您创建了一个**解密 - 重签**规则，并且用户浏览到其类别和信誉不在本地数据库中的网站，则数据可能不会被解密。某些网站未分类在本地数据库中，如果未分类，默认情况下不会解密来自这些网站的数据。

您可以通过**系统 (System) > 集成 (Integration) > 云服务** 设置来控制此行为，然后选中**向思科云查询未知 URL (Query Cisco cloud for unknown URLs)**。

有关此选项的详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的思科云。

TLS/SSL 规则 的要求和必备条件

支持的域

任意

用户角色

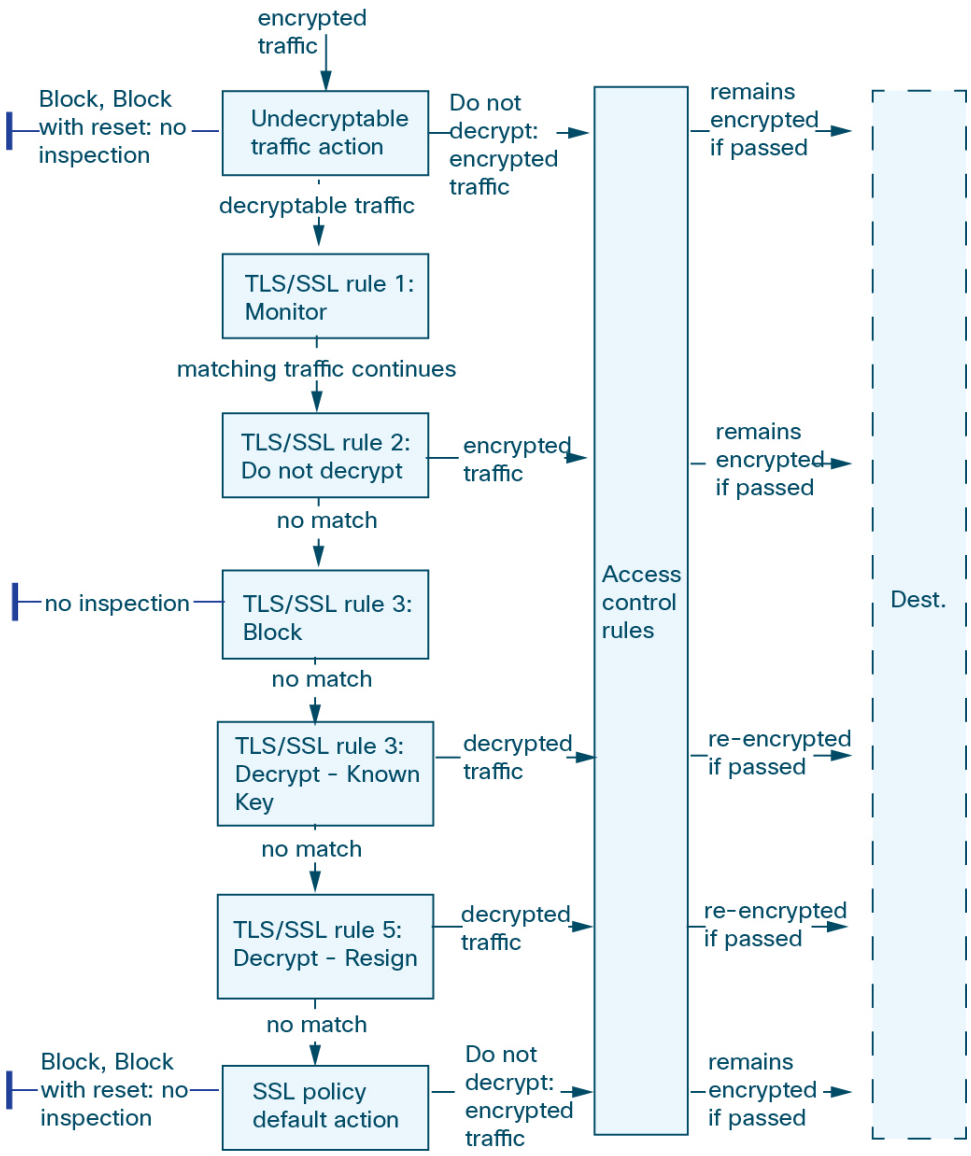
- 管理员
- 访问管理员
- 网络管理员

TLS/SSL 规则流量处理

系统会按照您所指定的顺序将流量与 TLS/SSL 规则规则相匹配。在大多数情况下，系统会根据第一个 TLS/SSL 规则（使用规则的所有条件来匹配流量）来处理加密流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，而是会通过访问控制来检查加密流量和无法解密的流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。

下述场景概括说明了 TLS/SSL 规则在内联部署中处理流量的方式。



在这种情况中，流量评估如下：

- 首先，**Undecryptable Traffic Action** 评估加密流量。对于系统无法解密的流量，系统会将其阻止而不进一步检查，或者使其通过以进行访问控制检查。不匹配的加密流量继续根据下一规则进行评估。
- 其次，使用 **TLS/SSL 规则 1: Monitor** 评估加密流量。Monitor 规则跟踪和记录加密流量，但不对流量做出任何影响。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。
- 第三，使用 **TLS/SSL 规则 2: Do Not Decrypt** 评估加密流量。匹配流量未解密；系统通过访问控制检查此流量，但不执行文件或入侵检测。不匹配的流量继续根据下一规则进行评估。
- 第四，使用 **TLS/SSL 规则 3: Block** 评估加密流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据下一规则进行评估。

- 第五，使用 **TLS/SSL 规则 4: Decrypt - Known Key** 评估加密流量。系统使用您上传的私钥对传入网络的匹配流量进行解密。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 TLS/SSL 规则 不匹配的流量会继续根据下一规则进行评估。
- **TLS/SSL 规则 5: Decrypt - Resign** 是最终规则。如果流量与此规则相匹配，则系统使用已上传的 CA 证书对服务器证书重新签名，然后充当中间人解密流量。然后，根据访问控制规则评估解密流量。访问控制规则以相同方式处理已解密和未加密的流量。作为此额外检查的结果，系统可以阻止流量。所有剩余流量将被重新加密，才会被传输到目标。与 SSL 规则不匹配的流量继续根据下一规则进行评估。
- **SSL 策略 Default Action** 会处理与任何 TLS/SSL 规则 不匹配的所有流量。默认操作为以下两种方式之一：阻止加密流量，且不进一步检查；不解密流量而允许传输，以进行访问控制检查。

加密流量检查配置

您必须创建可重用公共密钥基础设施 (PKI) 对象才能基于加密会话特性控制加密流量并解密加密流量。可以在将受信任证书颁发机构 (CA) 证书上传到 an SSL 策略 并创建 TLS/SSL 规则，以及在此过程中创建关联对象时即时添加此信息。不过，提前配置这些对象可降低不正确创建对象的几率。

使用证书和配对密钥解密加密流量

如果通过上传用于会话加密的服务器证书和私钥来配置内部证书对象，则系统可以解密传入的加密流量。如果在包含**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 an SSL 策略 规则中引用该对象并且流量与该规则相匹配，则系统会使用上传的私钥来解密会话。

如果通过上传 CA 证书和私钥来配置内部 CA 对象，则系统还可以解密传出流量。如果在包含**解密 - 重新签名 (Decrypt - Resign)** 操作的 TLS/SSL 规则 规则中引用该对象并且流量与该规则相匹配，则系统会对传递到客户端浏览器的服务器证书重新签名，然后充当中间人来解密会话。您可以选择只替换自签名证书密钥，而不是整个证书，在这种情况下，用户可在浏览器中看到自签名证书密钥通知。

根据加密会话特性控制流量

系统可以根据用于协商会话的密码套件或服务器证书来控制加密流量。您可以从多个不同的可重用对象中选择一个进行配置，并在TLS/SSL规则 条件中参照该对象来匹配流量。下表介绍可以配置的不同类型的可重用对象：

如果配置.....	可以根据是否存在以下内容控制加密流量.....
包含一个或多个密码套件的密码套件列表	用于协商加密会话的密码套件与密码套件列表中的密码套件相匹配
受信任 CA 对象（通过上传组织信任的 CA 证书）	受信任 CA 根据以下情况来确定是否信任用于加密会话的服务器证书： • CA 直接颁发证书 • CA 向颁发服务器证书的中间 CA 颁发证书

如果配置.....	可以根据是否存在以下内容控制加密流量.....
外部证书对象（通过上传服务器证书）	用于加密会话的服务器证书与上传的服务器证书相匹配
包含证书使用者或颁发者可分辨名称的可分辨名称对象	用于加密会话的证书上的主题或颁发者通用名称、国家/地区、组织或组织单位与已配置的可分辨名称相匹配

相关主题

密码套件列表
可分辨名称
PKI

TLS/SSL 规则 顺序评估

在 SSL 策略 中创建 TLS/SSL 规则 时，您可以使用规则编辑器中的**插入 (Insert)** 列表来指定其位置。SSL 策略 中的 TLS/SSL 规则 会从 1 开始编号。系统按升序规则编号以自上而下的顺序将流量与 TLS/SSL 规则 相匹配。

在大多数情况下，系统根据第一个 TLS/SSL 规则（其中所有规则的条件都与流量相匹配）处理网络流量。除了 Monitor 规则（记录流量，但不影响流量）之外，系统在流量匹配一个规则后，不再继续根据其他低优先级规则评估流量。条件可以简单也可以复杂；可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书可分辨名称、证书状态、密码套件或加密协议版本来控制流量。

每个规则也具有操作，用于确定是使用访问控制监控、阻止还是检测匹配的已加密或已解密流量。请注意，系统不会进一步检查其阻止的加密流量，它会通过访问控制来检查加密流量和无法解密的流量。但是，访问控制规则条件需要未加密流量，因此，已加密流量匹配的规则更少。

使用特定条件（例如网络和 IP 地址）的规则应在使用一般条件（例如应用）的规则之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第 1 层、第 2 层和第 3 层（物理、数据链路和网络）条件的规则应首先在规则中排序。稍后应在规则中对第 5 层、第 6 层和第 7 层的条件（会话，表示和应用）进行排序。有关 OSI 模型的详细信息，请参阅此 维基百科文章。

提示 适当的 TLS/SSL 规则 顺序可减少处理网络流量所需的资源，并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。

相关主题

访问控制规则的最佳实践
无法解密流量的默认处理选项
SSL 规则顺序

TLS/SSL 规则 条件

TLS/SSL 规则 的条件识别此规则处理的加密流量的类型。条件可以简单也可以复杂，并且可以指定每个规则有多个条件类型。仅当流量满足规则中的所有条件时，该规则才适用于此流量。

如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，无论会话 SSL 或 TLS 版本如何，具有证书条件但不具有版本条件的规则根据用于协商会话的服务器证书来评估流量。

每个 TLS/SSL 规则 都具有对匹配的加密流量确定以下处理的关联操作：

- 处理：最重要的是，规则操作管理系统是监控、信任、阻止还是解密与规则条件匹配的加密流量
- 日志记录：规则操作确定何时及如何记录有关匹配的加密流量的详细信息。

您的 TLS/SSL 检查配置会处理、检查并记录解密流量：

- SSL 策略 的无法解密的操作处理系统无法解密的流量。
- 策略的默认操作处理不满足任何非监控器 TLS/SSL 规则 的条件的流量。

当系统阻止或信任加密会话时，可以记录连接事件。无论系统稍后如何处理或检查流量，您都可以强制系统记录其解密的连接，以通过访问控制规则进一步检查。已加密会话的连接日志包含有关加密的详细信息，例如用于加密该会话的证书。您可以仅记录连接结束事件，但是：

- 对于受阻连接（“阻止”、“阻止并重置”），系统会立即结束会话并生成事件
- 对于“不解密”连接，系统在会话结束时生成事件

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。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。

注意 在禁用了 TLS/SSL 解密（即，当访问控制策略不包括 an SSL 策略 时）时添加第一个主动身份验证规则或删除最后一个主动身份验证规则 在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为。

请注意，主动身份验证规则具有 **主动身份验证** 规则操作或 **被动身份验证** 规则操作，并且 **如果无法建立被动或 VPN 识别，则使用主动身份验证** 已选中。

相关主题

安全区域规则条件
网络规则条件
VLAN 标记规则条件
用户规则条件
应用规则条件
端口规则条件

类别规则条件，第 17 页
基于服务器证书的 TLS/SSL 规则条件，第 17 页

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

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。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。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

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。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。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

用户规则条件

用户规则条件会根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如将其他策略与访问控制相关联中所述。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。

- 未知：无法识别的用户；例如，配置的领域未下载的用户。

应用规则条件

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用程序规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅 应用检测器基础知识。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 *1:* 应用特征

特征	说明	示例
类型	应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。	HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。
风险	应用用于可能违反您的组织安全策略的用途的可能性。	点对点应用的风险通常很高。
业务相关性	应用用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。	游戏应用的业务相关性通常很低。
类别	说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。	Facebook 属于社交网络类别。

特征	说明	示例
标签	有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。	视频流网络应用通常标记为 `high bandwidth` 和 `displays ads`。

相关主题

配置应用控制的最佳实践

端口规则条件

通过端口条件，您可以按流量的源端口和目标端口控制该流量。

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。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。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。

应用过滤也建议用于动态打开单独通道的应用（如 FTD），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为源端口条件。

类别规则条件

您可以选择在 SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 情报组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。

有关详细信息，请参阅URL 过滤概述。

如果在具有 **不解密** 规则操作的规则的 SSL 策略 中使用类别规则条件，请参阅 TLS/SSL 规则 不解密操作 ， 第 31 页。

基于服务器证书的 TLS/SSL 规则条件

TLS/SSL 规则可以根据服务器证书特征来处理和解密已加密的流量。您可以根据以下服务器证书属性配置 TLS/SSL 规则：

- 通过可分辨名称，您可以根据颁发服务器证书的 CA 或证书使用者来处理和检查加密流量。根据颁发者可分辨名称，可以根据颁发站点服务器证书的 CA 处理流量。
- 通过 TLS/SSL 规则中的证书条件，可以根据用于对加密流量进行加密的服务器证书来处理和检查该流量。可以配置具有一个或多个证书的条件；如果证书与该条件的任何证书相匹配，则流量与规则相匹配。
- 通过 TLS/SSL 规则中的证书状态条件，可以根据用于对流量加密的服务器证书的状态（包括证书是否有效、已被吊销、已过期、尚未生效、自签署、由可信 CA 签署、证书吊销列表 (CRL) 是否有效；证书中的服务器名称指示 (SNI) 是否与请求中的服务器相匹配）处理和检查加密流量。
- 通过 TLS/SSL 规则中的密码套件条件，可以根据用于协商加密会话的密码套件来处理和检查加密流量。
- 通过 TLS/SSL 规则中的会话条件，可以根据用于加密流量的 SSL 或 TLS 版本来检查加密流量。

要检测规则、证书颁发者或证书持有者中的多个密码套件，可以创建可重用密码套件列表和可分辨名称对象并将其添加到规则中。要检测服务器证书和某些证书状态，必须为规则创建外部证书和外部 CA 对象。

相关主题

证书 TLS/SSL 规则 条件，第 18 页
证书状态 TLS/SSL 规则 条件，第 25 页
信任外部证书颁发机构，第 24 页
按证书状态匹配流量
密码套件 TLS/SSL 规则 条件，第 27 页
加密协议版本 TLS/SSL 规则条件，第 30 页

证书 TLS/SSL 规则 条件

构建基于证书的 TLS/SSL 规则条件时，可以上传服务器证书；将证书另存为外部证书对象，该对象可重用并会将名称与服务器证书相关联。或者，可以使用现有外部证书对象和对象组来配置证书条件。

可以根据以下证书可分辨名称特性在外部证书对象或对象组所基于的规则条件中搜索**可用证书 (Available Certificates)** 字段：

- 使用者或颁发者公用名 (CN)，或者 URL 包含在证书的使用者可选名称 (SAN) 中

  用户在浏览器中输入的 URL 与通用名称 (CN) 匹配
- 使用者或颁发者组织 (O)
- 使用者或颁发者组织单位 (OU)

您可以选择根据单个证书规则条件中的多个证书进行匹配；如果用于加密流量的证书与上传的任何证书相匹配，则加密流量与规则相匹配。

在单个证书条件中，可以向**所选证书 (Selected Certificates)** 添加最多 50 个外部证书对象和外部证书对象组。

请注意以下事项：

- 如果还选择**解密 - 已知密钥 (Decrypt - Known Key)** 操作，则无法配置证书条件。由于该操作要求选择服务器证书来解密流量，因此结果是证书已经与流量相匹配。
- 如果使用外部证书对象配置证书条件，则添加到密码套件条件中的任何密码套件或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与外部证书的签名算法类型相匹配。例如，如果规则的证书条件引用基于 EC 的服务器证书，则添加的任何密码套件或与 **Decrypt - Resign** 操作相关联的 CA 证书也必须基于 EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告。
- 系统首次检测新服务器的加密会话时，证书数据不可用于 ClientHello 处理，因为这会导致首个会话不解密。在初始会话后，受管设备会缓存服务器证书消息中的数据。对于来自同一个客户端的后续连接，系统可将 ClientHello 消息与使用证书条件的规则进行决定性匹配，并处理消息以最大限度提高解密的可能性。

可分辨名称 (DN) 规则条件

本主题讨论如何在 TLS/SSL 规则 中使用可分辨名称条件。如果您不确定，可以使用 Web 浏览器查找证书的使用者可选名称 (SAN) 和公用名，然后可以将这些值作为可分辨名称条件添加到 TLS/SSL 规则。

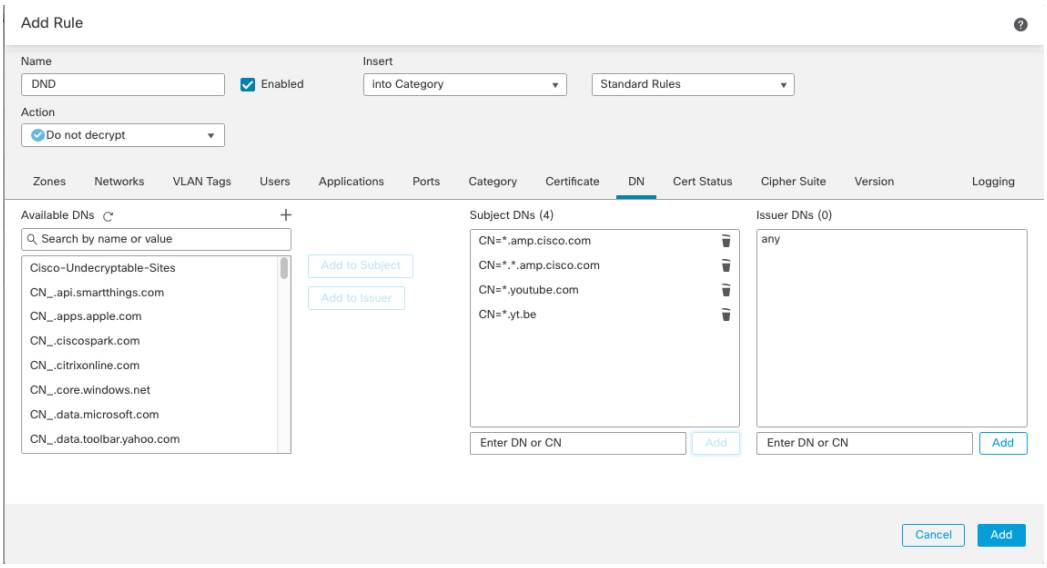
有关 SAN 的详细信息，请参阅 RFC 528 第 4.2.1.6 节。

以下各部分讨论：

- DN 规则匹配示例
- 系统如何使用 SNI 和 SAN
- 如何查找证书的通用名称和使用者可选名称
- 如何添加 DN 规则条件

DN 规则匹配示例

以下是不解密规则中 DN 规则条件的示例。假设您希望确保不解密流向 `amp.cisco.com` 或 YouTube 的流量。那么您可以按如下方式来设置 DN 条件：



前面的 DN 规则条件将与以下 URL 匹配，因此先前被规则阻止的流量会被解密：

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

前面的 DN 规则条件与以下任何 URL 都不匹配，因此，流量将不匹配“不解密”(Do Not Decrypt) 规则，但可能匹配同一 SSL 策略 中的任何其他 TLS/SSL 规则。

- amp.cisco.com
- youtube.com
- yt.be

要匹配上述任何主机名，请向规则中添加更多 CN（例如，添加 `CN=yt.be` 就会匹配该 URL。）

系统如何使用 SNI 和 SAN

客户端请求中 URL 的主机名部分是服务器名称指示 (SNI)。客户端会使用 TLS 握手中的 SNI 扩展名来指定要连接的主机名（例如，`auth.amp.cisco.com`）。然后，服务器会选择在单个 IP 地址上托管所有证书时建立连接所需的相应私钥及证书链。

如果证书中的 SNI 与 CN 或 SAN 匹配，则我们会在与规则中列出的 DN 进行比较时使用 SNI。如果没有 SNI 或它与证书不匹配，则我们将在与规则中列出的 DN 进行比较时使用证书的 CN。

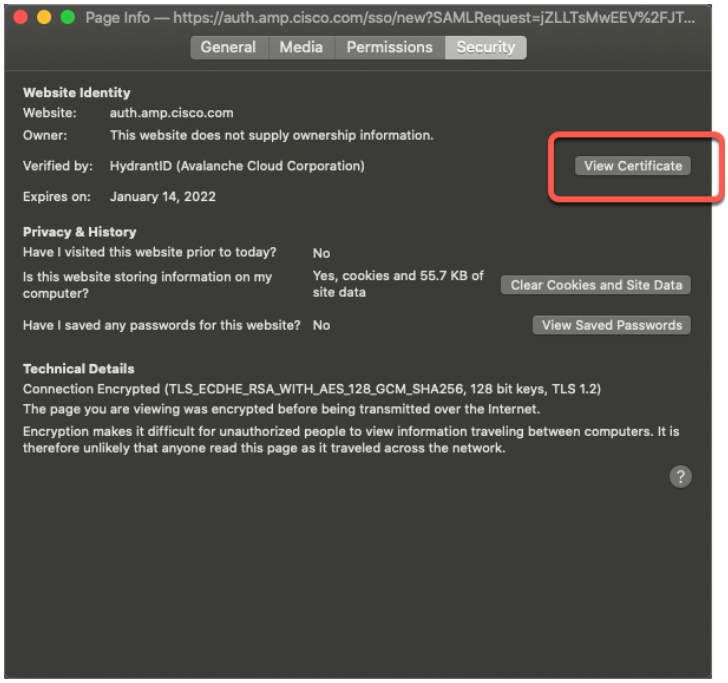
如何查找证书的通用名称和使用者可选名称

要查找任何证书的通用名称，请执行以下步骤。您甚至可以使用这些步骤来查找自签名证书的通用名称和 SAN。

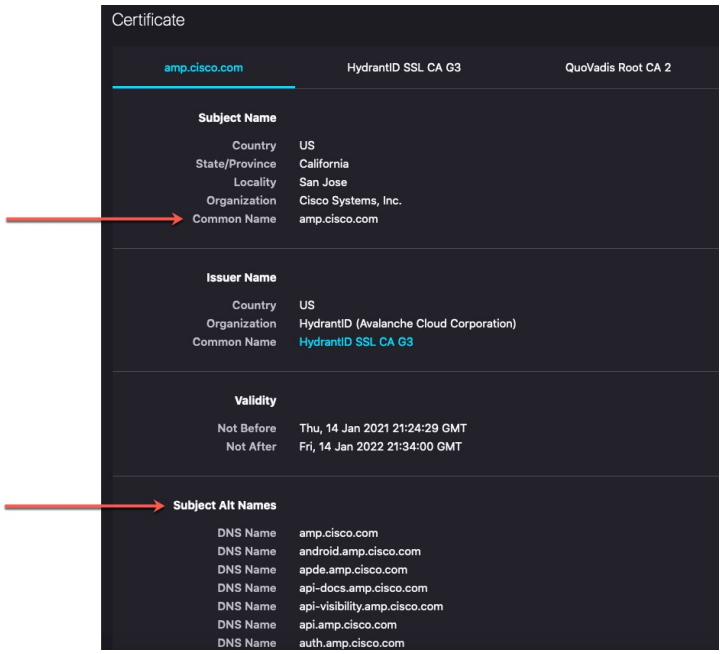
这些步骤适用于 Firefox，但其他浏览器也与之类似。以下程序以 `amp.cisco.com` 为例。

1. 在 Firefox 中浏览到 `amp.cisco.com`。
2. 在浏览器的地址栏中，点击 URL 左侧的 。
3. 点击**连接安全 (Connection secure)** > **更多信息 (More Information)**。

   （对于非安全或自签名证书，请点击**连接不安全 (Connection not secure)** > **详细信息 (More Information)**。）
4. 在页面信息对话框中，点击**查看证书 (View Certificate)**。



5. 下一页显示了证书详细信息。



请注意以下提示：

- `CN=auth.amp.cisco.com`，如果用作 DN 规则条件，则仅与该主机名（即 SNI）匹配。SNI `amp.cisco.com` 不匹配。
- 要匹配尽可能多的域名字段，请使用通配符。

  例如，要匹配 `auth.amp.cisco.com`，请使用 `CN=*.amp.cisco.com`。要匹配 `auth.us.amp.cisco.com`，请使用 `CN=*.*.amp.cisco.com`。

  像 `CN=*.example.com` 这样的 DN 与 `www.example.com` 匹配，但与 `example.com` 不匹配。要匹配两个 SNI，请在规则条件中使用两个 DN。

- 但不要过多使用通配符。例如，DN 对象（例如 `CN=*.google.com`）与大量的 SAN 匹配。使用 DN 对象（例如 `CN=*.youtube.com`）而不是 `CN=*.google.com`，使其与 `www.youtube.com` 等名称匹配。

  您还可以使用与 SAN 匹配的 SNI 变体，例如 `CN=*.youtube.com`、`CN=youtu.be`、`CN=*.yt.be` 等。

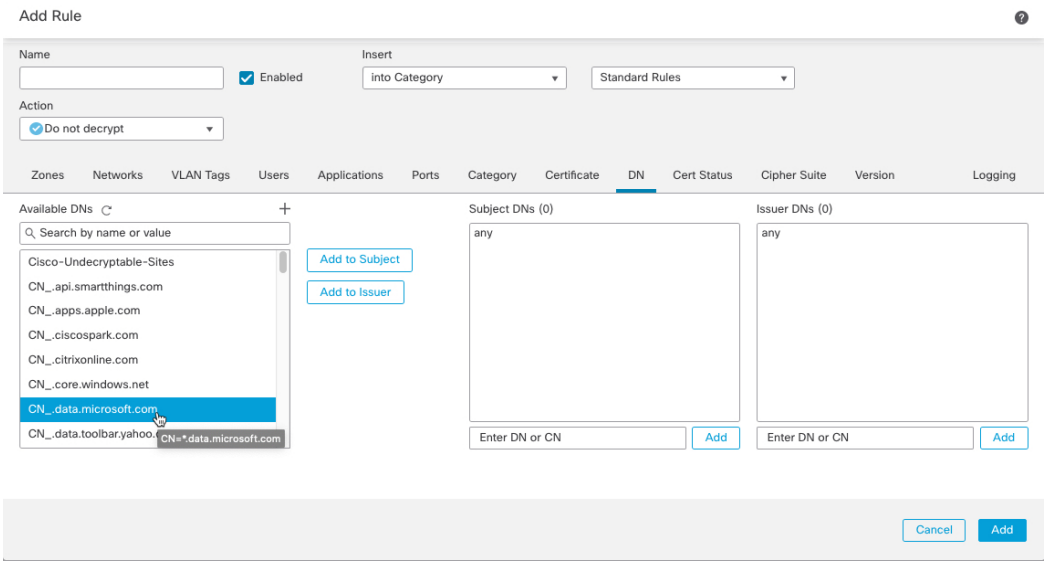
- 自签名证书应以相同的方式工作。您可以通过颁发者 DN 与使用者 DN 是否相同来确认它是否为自签名证书。

如何添加 DN 规则条件

在知道要匹配的 CN 后，请通过以下方式之一编辑 TLS/SSL 规则：

- 使用现有 DN。

  点击 DN 的名称，然后点击**添加到使用者 (Add to Subject)** 或**添加到颁发者 (Add to Issuer)**。（**添加到使用者 (Add to Subject)** 更为常用。）要查看 DN 对象的值，请将鼠标指针悬停在它上面。）

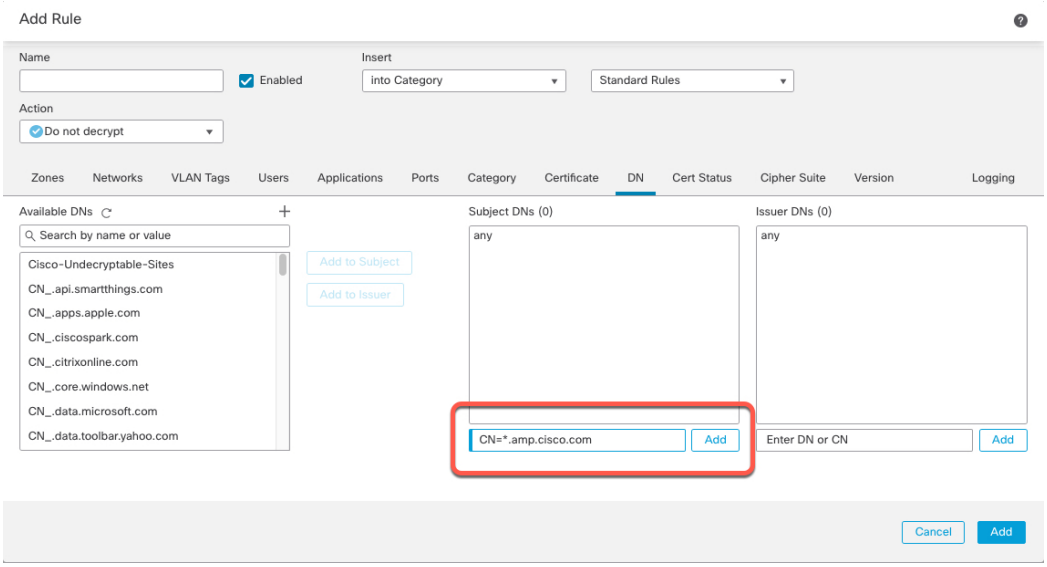


- 创建新的 DN 对象。

  点击可用 DN 右侧的 **添加**（+）。DN 对象必须包含名称和值。

- 直接添加 DN。

  在**使用者 DN (Subject DNs)** 字段或**颁发者 DN (Issuer DNs)** 字段底部的字段中输入 DN。（**使用者 DN (Subject DNs)** 更为常用。）输入 DN 后，点击**添加 (Add)**。



相关主题

可分辨名称

信任外部证书颁发机构

您可以通过向 SSL 策略中添加根 CA 证书和中间 CA 证书来信任 CA，然后使用这些受信任 CA 验证用于加密流量的服务器证书。

如果受信任 CA 证书包含上传的证书撤销列表 (CRL)，则还可以验证受信任 CA 是否已撤销加密证书。

提示 将根 CA 的信任链链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。此外，如果将证书状态条件配置为根据根颁发者 CA 来信任流量，则可以允许而不解密受信任 CA 的信任链中的所有流量，而不是不必要地将其解密。

有关详细信息，请参阅受信任的 CA 对象。

注释 创建 an SSL 策略时，策略的 **受信任 CA 证书** 选项卡页面将填充多个受信任 CA 证书，包括添加到 **选择受信任 CA** 列表中的 **Cisco-Trusted-Authorities** 组。

过程

步骤 1 如果尚未登录，请登录管理中心。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略 旁边的 **编辑**（ ） 进行编辑。

步骤 4 点击**添加规则 (Add Rule)** 以添加新的 TLS/SSL 规则，或者点击 **编辑**（ ） 以编辑现有的规则。

步骤 5 点击**证书 (Certificates)** 选项卡。

步骤 6 从**可用证书 (Available Certificates)** 中查找要添加的受信任 CA，如下所示：

- 要即时添加可随后添加到条件中的受信任 CA 对象，请点击**可用证书 (Available Certificates)** 列表上方的 **添加**（ ）。
- 要搜索将添加的受信任 CA 对象和组，请点击 **可用证书** 列表上方的 **按名称或值搜索** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 7 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后选择**全选 (Select All)**。

步骤 8 点击 **Add to Rule**（**添加至规则**）。

提示 您也可以拖放选定对象。

步骤 9 添加或继续编辑规则。

下一步做什么

- 将证书状态 TLS/SSL 规则条件添加到 SSL 规则。有关详细信息，请参阅按证书状态匹配流量。
- 部署配置更改；请参阅部署配置更改。

证书状态 TLS/SSL 规则 条件

对于配置的每个证书状态 TLS/SSL 规则，您可以根据给定状态存在还是缺失来匹配流量。可以在一个规则条件中选择若干状态，如果证书与任何所选状态相匹配，则规则与流量相匹配。

可以选择根据单个证书状态规则条件中多个证书状态的存在或缺失进行匹配；证书只需匹配其中一个标准即可与规则相匹配。

设置此参数时，应考虑是配置解密规则还是阻止规则。通常情况下，应对阻止规则点击**是**，对解密规则点击**否**。示例：

- 如果要配置**解密 - 重新签名**规则，则默认行为是使用过期的证书解密流量。要更改此行为，请对**过期**点击**否**，以确保不会解密并重签具有过期证书的流量。
- 如果要配置**阻止**规则，则默认行为是允许具有过期证书的流量。要更改此行为，请对**过期**点击**是**，以阻止具有过期证书的流量。

下表介绍系统如何根据加密服务器证书的状态评估加密流量。

表 *2:* 证书状态规则条件标准

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
已撤销	策略信任颁发服务器证书的 CA，并且上传到策略的 CA 证书包含用于撤销服务器证书的 CRL。	策略信任颁发服务器证书的 CA，并略的 CA 证书不包含用于撤销证书的
自签名	检测到的服务器证书包含相同的使用者和颁发者可分辨名称。	检测到的服务器证书包含不同的使用可分辨名称。
有效	以下所有情况都成立： • 策略信任颁发证书的 CA。 • 签名则是有效的。 • 颁发者有效。 • 策略的受信任 CA 未撤销证书 • 当前日期介于证书的有效期开始日期和有效期结束日期之间。	至少以下情况之一成立： • 策略不信任颁发证书的 CA。 • 签名无效。 • 颁发者无效。 • 策略中的受信任 CA 已撤销证书 • 当前日期在证书的有效期开始日 • 当前日期在证书的有效期结束日
签名无效	无法根据证书的内容正确验证证书的签名。	根据证书的内容正确验证证书的签名
颁发者无效	颁发者 CA 证书未存储在策略的受信任 CA 证书列表中。	颁发者 CA 证书存储在策略的受信任表中。

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
到期	当前日期在证书的有效期结束日期之后。	当前日期在证书的有效期结束日期之前
尚未生效	当前日期在证书的有效期开始日期之前。	当前日期在证书的 Valid From 日期之后
无效的证书	证书无效。至少以下情况之一成立： • 证书扩展名无效或不一致；即，证书扩展名具有无效值（例如，编码不正确）或某些值与其他扩展名不一致。 • 证书无法用于指定用途。 • 已超出基本约束路径长度参数。 有关详细信息，请参阅 RFC 5280 第 4.2.1.9 节。 • 证书的“有效起始日期”或“有效终止日期”值无效。这些日期可以编码为 UTC 时间或通用时间 有关详细信息，请参阅 RFC 5280 第 4.1.2.5 节。 • 无法识别名称限制的格式；例如 RFC 5280 第 4.2.1.10 节中未提及表单的邮件地址格式。这可能是由于扩展名不正确或当前不支持的某些新功能导致的。 遇到了不受支持的名称限制类型。OpenSSL 目前仅支持目录名称、DNS 名称、邮件和 URI 类型。 • 根证书颁发机构不受信任，不可用于指定用途。 • 根证书颁发机构拒绝指定的用途。	证书有效。以下所有情况都成立： • 验证证书扩展名。 • 证书可用于指定用途。 • 基本约束路径长度有效。 • “有效起始日期”和“有效终止日有效。 • 名称限制有效。 • 根证书受信任，可用于指定用途。 • 根证书接受指定的用途。

状态检查	状态设置为“是”(Yes)	状态设置为“否”(No)
无效 CRL	证书撤销列表 (CRL) 的数字签名无效。至少以下情况之一成立： • CRL 的“下次更新”或“上次更新”字段的值无效。 • CRL 尚未生效。 • CRL 已过期。 • 尝试验证 CRL 路径时出错。仅在启用扩展 CRL 检查时才会发生此错误。 • 找不到 CRL。 • 唯一可以找到的CRL 与证书的范围不匹配。	CRL 有效。以下所有情况都成立： • “下次更新”和“上次更新”字 • CRL 日期有效。 • 路径有效。 • 已找到 CRL。 • CRL 与证书的范围相匹配。
服务器不匹配	服务器名称与服务器的服务器名称指示 (SNI) 名称不匹配，这可能表示尝试欺骗服务器名称。	服务器名称与客户端请求访问的服务称匹配。

请注意，即使证书可能匹配多个状态，但是该规则导致仅对流量执行一次操作。

检查颁发或撤销证书的 CA 是否要求将根 CA 证书和中间 CA 证书以及关联的 CRL 作为对象进行上传。然后，将这些受信任 CA 对象添加到 SSL 策略 的受信任 CA 证书列表。

密码套件 TLS/SSL 规则 条件

系统提供可向密码套件规则条件中添加的预定义密码套件。您还可以添加包含多个密码套件的密码套件列表对象。

注释 不能添加新的密码套件。不能修改和删除预定义密码套件。

在单个密码套件条件中，可以向**所选密码套件 (Selected Cipher Suites)** 添加最多 50 个密码套件和密码套件列表。系统支持向密码套件条件添加以下密码套件：

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

请注意以下提示：

- 如果添加部署不支持的密码套件，则无法部署配置。例如，被动部署不支持使用任何短 Diffie-Hellman (DHE) 或短椭圆曲线 Diffie-Hellman (ECDHE) 密码套件来解密流量。使用这些密码套件创建规则将会阻止部署访问控制策略。
- 如果使用密码套件配置密码套件条件，则添加到证书条件中的任何外部证书对象或与 **Decrypt - Resign** 操作相关联的内部 CA 对象必须与密码套件的签名算法类型相匹配。例如，如果规则的密码套件条件引用基于 EC 的密码套件，则添加的任何服务器证书或与 **Decrypt - Resign** 操作相关联的 CA 证书也必须基于 EC。如果在此情况下签名算法类型不匹配，则策略编辑器会在规则旁边显示警告图标。
- 您可以在 SSL 规则中的**密码套件 (Cipher Suite)** 条件中添加一个匿名密码套件，但请记住：
  - 系统会在 ClientHello 处理期间自动删除匿名密码套件。要让系统使用该规则，还必须配置顺序以阻止 ClientHello 处理。有关详细信息，请参阅SSL 规则顺序。
  - 在该规则中无法使用**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Derypt - Known Key)** 操作，因为系统无法解密使用匿名密码套件加密的流量。

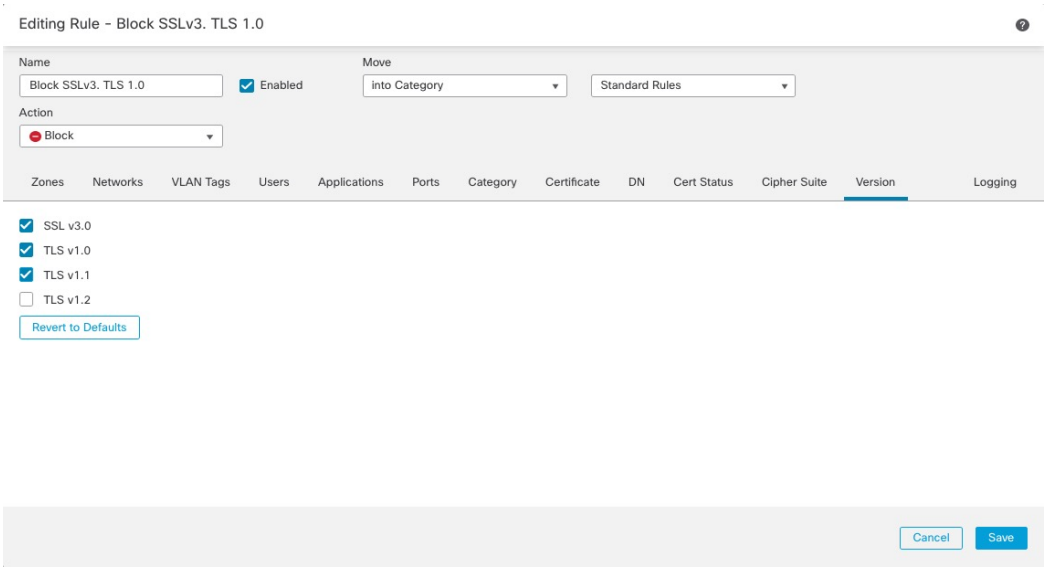
- 指定密码套件作为规则条件时，应该考虑使用 ServerHello 消息中协商的密码套件进行匹配的规则，而不是使用 ClientHello 消息中指定的整个密码套件列表进行匹配的规则。在 ClientHello 处理期间，受管设备从 ClientHello 消息中删除不受支持的密码套件。但如果这会导致所有指定的密码套件被删除，系统会保留原始列表。如果系统保留不受支持的密码套件，后续评估会导致会话不解密。

加密协议版本 TLS/SSL 规则条件

可以选择根据使用 SSL V3.0 或 TLS V1.0、V1.1 或 V1.2 加密的流量进行匹配。默认情况下，在创建规则时会选择所有协议版本；如果选择多个版本，则与任何所选版本相匹配的加密流量都与该规则相匹配。保存规则条件时，必须至少选择一个协议版本。

您无法在版本规则条件中选择 SSL V2.0；系统不支持解密使用 SSL V2.0 加密的流量。可以配置无法解密的操作来允许或阻止此流量而不进一步检查。

例如，要阻止所有 SSL v1.0、TLS v1.0 和 TLS v1.1 流量，请按如下所示设置选项：



TLS/SSL 规则 操作

以下各部分讨论 TLS/SSL 规则 可用的操作。

TLS/SSL 规则 监控操作

监控 (Monitor) 操作不能允许或拒绝流量。相反，它的主要目的是强制连接日志记录，而不会考虑最终如何处理匹配的流量。如果流量与**监控**规则条件匹配，则不会修改 ClientHello 消息。

系统随后会根据其他规则（如果有）来匹配流量，以确定信任、阻止还是解密该流量。所匹配的第一个非“监控”(Monitor) 规则确定流量和任何进一步的检测。如果没有其他匹配的规则，系统使用默认操作。

由于“监控”规则的主要目的是跟踪网络流量，因此系统会自动将受监控流量的连接结束事件记录到 Cisco Secure Firewall Management Center数据库，而无论稍后处理该连接的规则或默认操作的日志记录配置如何。

TLS/SSL 规则 不解密操作

不解密操作会让加密流量通过，以通过访问控制策略的规则和默认操作进行评估。由于某些访问控制规则条件需要未加密的流量，因此该流量可能与较少的规则相匹配。系统无法对加密流量执行深入检查，例如入侵或文件检查。

不解密规则操作的常见原因包括：

- 法律禁止解密 TLS/SSL 流量。
- 确定可以信任的站点。
- 通过检查流量（如 Windows Update）可以中断的站点。
- 使用连接事件查看 TLS/SSL 字段的值。（您无需解密流量即可查看连接事件字段。）有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的填充连接事件字段的要求。

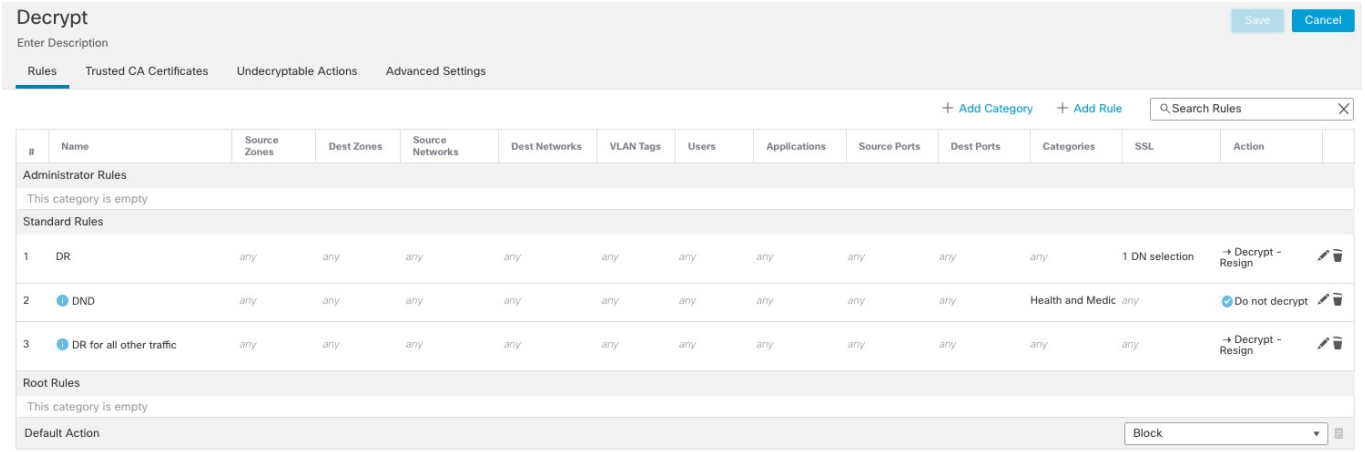
有关详细信息，请参阅无法解密流量的默认处理选项

“不解密”规则中的类别限制

您可以选择在 SSL 策略中包含类别。这些类别也称为 *URL* 过滤，由思科 Talos 情报组更新。更新基于机器学习和人工分析，这些内容可从网站目的地检索，有时也可从其托管和注册信息检索。分类不 基于所声明的公司行业、意图或安全性。虽然我们努力不断更新和改进 URL 过滤类别，但这并不是一门精确的科学。有些网站根本没有分类，有些网站可能分类不当。

避免在不解密规则中过度使用类别，以避免无故解密流量；例如，“健康和医学”类别包括不会威胁到患者隐私的 WebMD 网站。

以下是一个解密策略示例，它可以阻止解密“健康”和“医学”类别的网站，但允许解密 WebMD 和其他所有内容。有关解密规则的一般信息，请参阅 使用 TLS/SSL 解密的准则 ，第 2 页。



注释 不要将 URL 过滤与应用检测混淆，后者依赖于从网站读取数据包来更具体地确定其内容（例如，Facebook Message 或 Salesforce）。有关详细信息，请参阅配置应用控制的最佳实践。

TLS/SSL 规则 阻止操作

系统为您不希望通过系统的流量提供以下 TLS/SSL 规则 操作：

- **阻止 (Block)**，此操作可终止连接，从而导致客户端浏览器出错。

  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。

- **阻止并重置 (Block with reset)**，此操作可终止并重置连接，从而导致客户端浏览器出错。

  该错误会指明连接已重置，但未指明具体原因。

提示 在被动或内联（触点模式）部署中不能使用 **阻止 (Block)** 或**阻止并重置 (Block with reset)** 操作，因为设备不会直接检查流量。如果创建具有**阻止 (Block)** 或**阻止并重置 (Block with reset)** 操作的规则，该规则在安全区域条件内包含被动或内联（触点模式）接口，则策略编辑器在该规则旁边显示警告 ( )。

TLS/SSL 规则 解密操作

Decrypt - Known Key 和 **Decrypt - Resign** 操作会对加密流量进行解密。系统通过访问控制来检查解密流量。访问控制规则以相同方式处理已解密和未加密的流量，您可以检查该流量来获得发现数据，并检测和阻止入侵、禁止的文件及恶意软件。系统在将允许的流量传递到其目标之前会将其重新加密。

建议使用来自受信任证书颁发机构 (CA) 的证书来解密流量。这可以防止**Invalid Issuer**显示在连接事件的“SSL 证书状态”列中。

有关添加受信任对象的详细信息，请参阅受信任证书颁发机构对象。

相关主题：TLS 1.3 解密最佳实践。

监控 TLS/SSL 硬件加速

以下主题讨论如何监控 TLS/SSL 状态

信息计数器

如果负载的系统运行良好，您应会看到以下计数器的计数较大。由于跟踪器进程的每个连接有2端，所以您会看到每个连接的这些计数器呈 2 倍增长。PRIV_KEY_RECV 和 SECU_PARAM_RECV 计数器最为重要，并会突出显示。CONTEXT_CREATED 和 CONTEXT_DESTROYED 计数器与加密芯片内存的分配相关。

```
> show counters
Protocol      Counter                          Value   Context
SSLENC        CONTEXT_CREATED                 258225   Summary
SSLENC        CONTEXT_DESTROYED               258225   Summary
TLS_TRK       OPEN_SERVER_SESSION             258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION             258225   Summary
TLS_TRK       UPSTREAM_CLOSE                  516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE                516450   Summary
TLS_TRK       FREE_SESSION                    516450   Summary
TLS_TRK       CACHE_FREE                      516450   Summary
TLS_TRK       PRIV_KEY_RECV                   258225   Summary
TLS_TRK       NO_KEY_ENABLE                   258225   Summary
TLS_TRK       SECU_PARAM_RECV                 516446   Summary
TLS_TRK       DECRYPTED_ALERT                 258222   Summary
TLS_TRK       DECRYPTED_APPLICATION         33568976   Summary
TLS_TRK       ALERT_RX_CNT                    258222   Summary
TLS_TRK       ALERT_RX_WARNING_ALERT          258222   Summary
TLS_TRK       ALERT_RX_CLOSE_NOTIFY           258222   Summary
TCP_PRX       OPEN_SESSION                    516450   Summary
TCP_PRX       FREE_SESSION                    516450   Summary
TCP_PRX       UPSTREAM_CLOSE                  516450   Summary
TCP_PRX       DOWNSTREAM_CLOSE                516450   Summary
TCP_PRX       FREE_CONN                       258222   Summary
TCP_PRX       SERVER_CLEAN_UP                 258222   Summary
TCP_PRX       CLIENT_CLEAN_UP                 258222   Summary
```

警报计数器

我们按照 TLS 1.2 规范实施了以下计数器。FATAL 或 BAD 警报可能表明存在问题；但是，ALERT_RX_CLOSE_NOTIFY 表明正常。

有关详细信息，请参阅 RFC 5246 第 7.2 节。

```
TLS_TRK       ALERT_RX_CNT                          311   Summary
TLS_TRK       ALERT_TX_CNT                            2   Summary
TLS_TRK       ALERT_TX_IN_HANDSHAKE_CNT               2   Summary
```

```
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT                    2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT                     308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                         3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                         2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY                      308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC                      2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC                      2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE                     1   Summary
```

错误计数器

这些计数器指示系统错误。这些计数在运行状况正常的系统上应较低。BY_PASS 计数器指示不经解密便直接传递到检测引擎 (Snort) 进程（在软件中运行）或从其传递的数据包。以下示例中列出了一些错误计数器。

值为 0 的计数器不会显示。要查看计数器的完整列表，请使用命令 **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                          Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM             2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET           2   Summary
TLS_TRK      ENC_FAIL                            82   Summary
TLS_TRK      DEC_FAIL                           211   Summary
TLS_TRK      DEC_CKE_FAIL                     43194   Summary
TLS_TRK      ENC_CB_FAIL                       4335   Summary
TLS_TRK      DEC_CB_FAIL                        909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                    818   Summary
TLS_TRK      RECORD_PARSE_ERR                   123   Summary
TLS_TRK      IN_ERROR                         44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD            43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE               123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR           123   Summary
TLS_TRK      DECRYPT_FAIL                     43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                   127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                 127   Summary
```

重大错误计数器

重大错误计数器表示严重的错误。这些计数器在正常运行的系统中应达到或接近于 0。以下示例列出了重大错误计数器。

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

RING_FULL 计数器不是重大错误计数器，但表明系统中加密芯片过载的频率。
ACCELERATOR_RESET 计数器指示 TLS 加密加速进程意外失败的次数，该进程意外失败也导致挂起的操作失败，即您在 ACCELERATOR_CORE_TIMEOUT 和 RSA_PRIVATE_DECRYPT_FAILED 中看到的数字。

如果问题仍未解决，请禁用 TLS 加密加速（ 或 **config hwCrypto disable**）并配合思科 TAC 来解决问题。

注释 您可以使用 **show snort tls-offload** 和 **debug snort tls-offload** 命令进行其他的故障排除。使用 **clear snort tls-offload** 命令可将 **show snort tls-offload** 命令中显示的计数器重置为零。

对TLS/SSL 规则进行故障排除

以下主题讨论如何对 TLS/SSL 规则 进行故障排除。

关于 TLS/SSL 超订用

TLS/SSL 超订用是受管设备过载 TLS/SSL 流量的状态。任何受管设备都可能会遇到 TLS/SSL 超订用，但只有支持 TLS 加密加速的受管设备才提供可配置的方式对其进行处理。

启用了 TLS 加密加速 的受管设备在超订用时，受管设备接收的任何数据包都根据 SSL 策略 的**无法解密的操作**中**握手错误**设置进行处理：

- 继承默认操作
- 不解密
- 阻止
- 阻止并重置

如果 SSL 策略的**无法解密的操作**中**握手错误**的设置为**不解密**，且相关的访问控制策略配置为检查流量，则检查会发生；但是解密不会发生。

对 TLS/SSL 超订用进行故障排除

如果您的受管设备已启用 TLS 加密加速，您可以查看连接事件，以确定设备是否遇到了 SSL 超订用。您必须至少将 **SSL 流标志**事件添加到连接事件的表视图。

开始之前

- 配置一个 an SSL 策略，其中包含一项针对**无法解密的操作 (Undecryptable Actions)** 页面上的**握手错误 (Handshake Errors)** 的设置。

  有关详细信息，请参阅设置无法解密的流量的默认处理。

- 为 SSL 规则启用日志记录，如 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中有关 TLS/SSL 规则 中记录可解密连接的部分所述。

过程

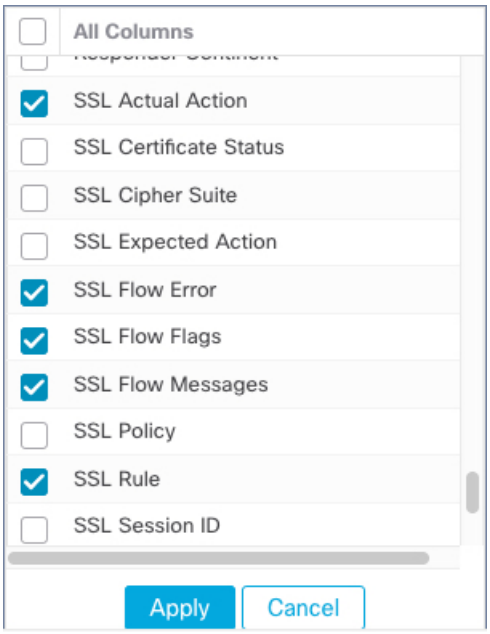
步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 依次单击 **分析** > **连接** > **事件**。

步骤 3 单击**连接事件的表视图**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。

以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。（查看对话框的“禁用列”部分。）



列按 《Cisco Secure Firewall Management Center 管理指南》 中的 连接和安全情报事件字段 中讨论的顺序添加。

步骤 5 单击 **Apply**。

TLS/SSL 超订用通过 **SSL 流标志**列中的 `ERROR_EVENT_TRIGGERED` 和 `OVER_SUBSCRIBED` 的值指示。

步骤 6 如果出现 TLS/SSL 超订用，请登录到受管设备并输入以下命令之一：

命令	结果
show counters	如果 **TCP_PRX BYPASS_NOT_ENOUGH_MEM** 的值较大，请考虑将设备升级到容量更大的可以容纳 SSL 流量的设备，或使用**不解密**规则以获得优先级较低的加密流量。

命令	结果
show snort tls-offload	如果 **BYPASS_NOT_ENOUGH_MEM** 的值较大，请考虑将设备升级到容量更大的可以容纳 SSL 流量的设备，或使用**不解密**规则以获得优先级较低的加密流量。

关于 TLS 心跳

某些应用使用 RFC6520 定义的传输层安全 (TLS) 和数据报传输层安全 (DTLS) 协议的 *TLS* 心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

当启用 TLS 加密加速的受管设备遇到使用 SSL 检测信号扩展的数据包时，受管设备将执行 SSL 策略 的**无法解密的操作**中**解密错误**的设置所指定的操作：

- 阻止
- 阻止并重置

相关主题

对 TLS 心跳进行故障排除，第 37 页

对 TLS 心跳进行故障排除

如果您的受管设备已启用 TLS 加密加速，则您可以查看连接事件，以确定设备是否看到了具有 SSL 心跳扩展的流量。您必须至少将 **SSL 流消息**事件添加到连接事件的表视图。

开始之前

SSL 心跳由连接事件的表视图中 **SSL 流消息**列内的心跳值来指示。要确定您的网络中的应用是否会使用 SSL 心跳，请先执行以下任务：

- 配置一个 SSL 策略，其中包含一项针对**无法解密的操作 (Undecryptable Actions)** 选项卡页面上的**解密错误 (Decryption Errors)** 的设置。

  有关详细信息，请参阅设置无法解密的流量的默认处理。

- 为 SSL 规则启用日志记录，如Cisco Secure Firewall Management Center 和威胁防御管理网络管理中所述。

过程

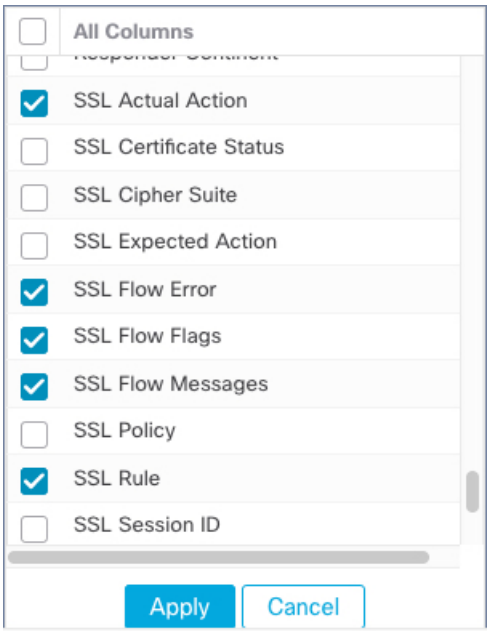
步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 依次单击**分析** > **连接** > **事件**。

步骤 3 单击**连接事件的表视图**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。

以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。



列按 《Cisco Secure Firewall Management Center 管理指南》 中的 连接和安全情报事件字段 中讨论的顺序添加。

步骤 5 单击 **Apply**。

TLS 心跳由 **SSL 流消息**列中的心跳值来指示。

步骤 6 如果您网络中的应用使用 SSL 心跳检测信号，请参阅TLS/SSL 规则 准则和限制，第 1 页。

关于 TLS/SSL 锁定

某些应用使用称为 *TLS/SSL* 锁定或证书锁定的技术，其在应用自身中嵌入原始服务器证书的指纹。因此，如果您配置具有**解密 - 重签**操作的 TLS/SSL 规则，则应用从受管设备收到重签的证书时，验证会失败且连接会中止。

要确认是否出现 TLS/SSL 锁定，请尝试登录到 Facebook 等移动应用。如果显示网络连接错误，则使用网络浏览器进行登录。（例如，您无法登录到 Facebook 移动应用，但可以使用 Safari 或 Chrome 登录到 Facebook。）您可以使用 Firepower 管理中心连接事件来进一步证明 TLS/SSL 锁定

注释 TLS/SSL 锁定不限于移动应用。

如果您网络中的应用使用 SSL 锁定，请参阅TLS/SSL 证书固定准则，第 7 页。

相关主题

对 TLS/SSL 锁定进行故障排除，第 39 页

对 TLS/SSL 锁定进行故障排除

通过查看连接事件，可以确定设备是否遇到 SSL 锁定。您必须至少向连接事件的表视图中添加 **SSL 流标志**和 **SSL 流消息**列。

开始之前

- 为 TLS/SSL 规则 启用日志记录，如 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中有关 TLS/SSL 规则中记录可解密连接的部分所述。
- 登录 Facebook 等移动应用；如果显示网络连接错误，请使用 Chrome 或 Safari 登录 Facebook。如果可以使用网络浏览器登录，但不是本机应用程序，则可能发生 SSL 锁定。

过程

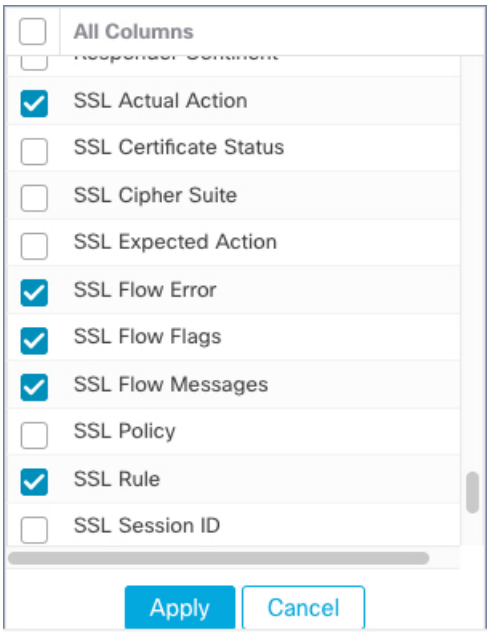
步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 依次单击 **分析** > **连接** > **事件**。

步骤 3 单击**连接事件的表视图**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。

以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。



这些列将按 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中的连接和安全智能事件字段中讨论的顺序进行添加。

步骤 5 点击**应用**。

步骤 6 以下内容介绍如何识别 SSL 锁定行为。

步骤 7 如果您确定网络中的应用使用 SSL 锁定，请参阅TLS/SSL 规则 准则和限制，第 1 页。

下一步做什么

您可以使用 TLS/SSL 连接事件，通过查找以下任何项目来确认发生 TLS/SSL 锁定：

- 在客户端收到来自服务器的 SERVER_HELLO，SERVER_CERTIFICATE、SERVER_HELLO_DONE 消息后立即发送 SSL ALERT 消息并后跟 TCP 重置的应用会出现以下症状。（使用数据包捕获可查看警报：`Unknown CA (48)`。）
  - “SSL 流标志”列显示 `ALERT_SEEN`，但不显示 `APP_DATA_C2S` 或 `APP_DATA_S2C`。
  - 如果受管设备已启用 SSL 硬件加速，则“SSL 流消息”列通常显示：`CLIENT_ALERT`、`CLIENT_HELLO`、`SERVER_HELLO`、`SERVER_CERTIFICATE`、`SERVER_KEY_EXCHANGE`、`SERVER_HELLO_DONE`。
  - 如果托管的设备不支持 SSL 硬件加速或该功能被禁用，则“SSL 流消息”(SSL Flow Messages) 列通常会显示：`CLIENT_HELLO`、`SERVER_HELLO`、`SERVER_CERTIFICATE`、`SERVER_KEY_EXCHANGE`、`SERVER_HELLO_DONE`。
  - “SSL 流错误”列将显示 `Success`。
- 在执行 SSL 握手后不是发送警报而是“TCP 重置”的应用会出现以下症状：

- “SSL 流标志”列不显示 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。
- 如果受管设备已启用 SSL 硬件加速，则“SSL 流消息”列通常显示：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。
- 如果托管的设备不支持SSL硬件加速或该功能被禁用，则“SSL流消息”(SSL Flow Messages)列通常会显示：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED,SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。
- “SSL 流错误”列将显示 Success。

相关主题

对未知或错误的证书或证书颁发机构进行故障排除，第 41 页

对未知或错误的证书或证书颁发机构进行故障排除

您可以查看连接事件，以确定设备是否遇到未知证书颁发机构、错误证书或未知证书。如果已固定TLS/SSL 证书，则也可以使用此程序。您必须至少向连接事件的表视图中添加 **SSL 流标志**和 **SSL 流消息**列。

开始之前

- 设置一个 TLS/SSL 规则。
- 为 TLS/SSL 规则 启用日志记录，如 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中有关 TLS/SSL 规则中记录可解密连接的部分所述。

过程

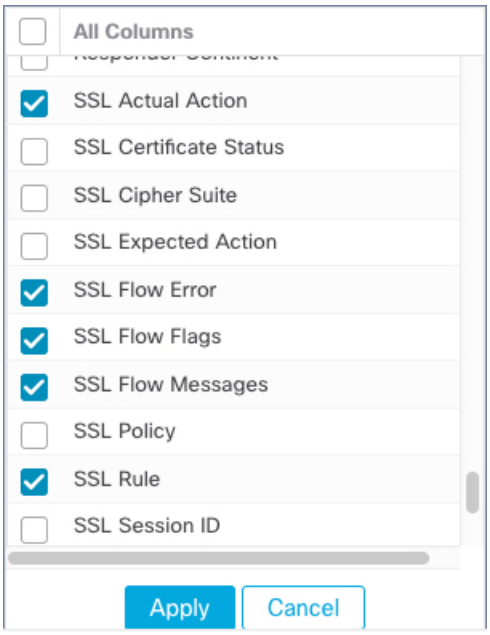
步骤 1 如果尚未登录，请登录 管理中心。

步骤 2 依次单击 **分析** > **连接** > **事件**。

步骤 3 单击**连接事件的表视图**。

步骤 4 点击连接事件表任意列中的 **x**，向至少包含 **SSL 流标志**和 **SSL 流消息**列的其他列。

以下示例显示如何向连接事件表中添加 **SSL 实际操作**、**SSL 流错误**、**SSL 流标志**、**SSL 流消息**、**SSL 策略**和 **SSL 规则**列。



这些列将按 Cisco Secure Firewall Management Center 和威胁防御管理网络管理 指南中的连接和安全智能事件字段中讨论的顺序进行添加。

步骤 5 点击**应用**。

步骤 6 下表讨论如何确定证书或证书颁发机构是否出错或缺失。

SSL 流量标志	含义
CLIENT_ALERT_SEEN_UNKNOWN_CA	表示 SSL 客户端应用收到了有效的证书链或部分证书链，但由于无法找到CA证书或者无法与已知的受信任CA匹配，因此该证书未被接受。此消息始终表示不可恢复的错误。
CLIENT_ALERT_SEEN_BAD_CERTIFICATE	证书已损坏、包含未正确验证的签名或存在其他问题。
CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN	处理证书时出现了一些其他（未指定的）问题，使得其无法被接受。

验证 TLS/SSL 密码套件

开始之前

本主题讨论在保存具有密码套件条件的 TLS/SSL 规则时看到以下错误时必须执行的操作：

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature
algorithm that the resigning CA's signature algorithm
```

此错误表示您为 TLS/SSL 规则条件选择的一个或多个密码套件与此 TLS/SSL 规则中使用的证书不兼容。要解决此问题，必须有权访问正在使用的证书。

注释 本主题中的任务假定了解 TLS/SSL 加密的工作原理。

过程

步骤 1 当您尝试使用指定的密码套件保存具有**解密 - 重新签名**或**解密 - 已知密钥**的 SSL 规则时，系统会显示以下错误：

示例：

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

步骤 2 找到将用于解密流量的证书，并在必要时将证书复制到可以运行 openssl 命令的系统。

步骤 3 运行以下命令，以显示证书使用的签名算法：

openssl x509 -in *CertificateName* **-text -noout**

输出的前几行显示内容类似于以下各项：

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

步骤 4 **Signature algorithm** 显示以下内容：

- 所使用的加密函数（在上述示例中，**ECDSA** 表示椭圆曲线数字签名算法）。
- 用于创建加密消息摘要的散列函数（上述示例中为 **SHA256**）。

步骤 5 搜索与这些值匹配的密码套件资源（如犹他大学的 OpenSSL）。密码套件必须采用 RFC 格式。您还可以搜索各种其他站点，例如 Mozilla Wiki 上的服务器端 TLS 或 RFC 5246 的附录 C。Microsoft 文档格式的 TLS/SSL (Schannel SSP) 中的密码套件对密码套件进行了详细说明。

步骤 6 如有必要，请将 OpenSSL 名称转换为 Firepower 管理系统使用的 RFC 名称。请参阅 `https://testssl.sh` 站点上的 RFC 映射列表。

步骤 7 上述示例 **ecdsa-with-SHA256** 可以在 Mozilla Wiki 上的现代兼容性列表中找到。

a) 仅选择名称中包含 **ECDSA** 和 **SHA-256** 的密码套件。这些密码套件遵循以下原则：

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) 在 RFC 映射列表中找到相应的 RFC 密码套件。这些密码套件遵循以下原则：

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

步骤 8 将上述密码套件添加到 TLS/SSL 规则中。

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。