流量解密概述

以下主题概述了传输层安全/安全套接字层 (TLS/SSL) 检查，讨论了 TLS/SSL 检查配置的先决条件，并详细介绍了部署场景。

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。

流量解密已说明

互联网上的大多数流量都是加密的，并且在大多数情况下您都不希望解密；即使您不这样做，您仍然可以收集有关它的一些信息，并在必要时从网络中阻止它。

您的选择包括：

- 解密流量并对其进行完整的深度检查：
  - 高级恶意软件防护
  - 安全情报
  - 威胁情报导向器
  - 应用检测器

- URL 和类别过滤

- 保持流量加密并设置访问控制和 SSL 策略 以查找并可能阻止：
  - 旧协议版本（例如安全套接字层）
  - 不安全的密码套件
  - 具有高风险和低业务关联性的应用
  - 不可信颁发者的可分辨名称

访问控制策略是一种可调用子策略和其他配置（包括 SSL 策略）的主配置。如果将 SSL 策略与访问控制相关联，则系统会在使用访问控制规则评估加密会话前使用该 SSL 策略对其进行处理。如果没有配置 TLS/SSL或设备不支持，则访问控制规则将处理所有加密流量。

当您的 TLS/SSL配置允许加密流量通过时，访问控制规则也会对其进行处理。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。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。

即使策略不需要解密流量，我们也建议将选择性解密作为最佳实践。换句话说，您应该设置一些 TLS/SSL 规则 来查找不需要的应用、密码套件和不安全的协议。这些类型的规则不需要对流量中的数据进行解密，而只用确定流量中是否包含这些不良特征即可。

备注

仅当托管设备处理加密流量时才设置解密规则。TLS/SSL 规则 需要处理可能会影响性能的开销。

只要托管设备启用了 Snort 3，系统就支持解密 TLS 1.3 流量。您可在 SSL 策略 的高级选项中启用 TLS 1.3 解密；有关详细信息，请参阅SSL 策略 高级选项。

Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第 10 页和已知密钥解密（传入流量），第 11 页。

如果使用 FlexConfig 设置 TCP 最大分段大小 (MSS) 的值，则观察到的 MSS 可能会小于您的设置。有关详细信息，请参阅关于 TCP MSS。

相关主题

TLS/SSL 握手处理，第 2 页
TLS/SSL 最佳实践，第 8 页

TLS/SSL 握手处理

在本文档中，术语 *TLS/SSL* 握手表示启动 SSL 协议及其后续协议 TLS 中的加密会话的双向握手。

在内联部署中，Firepower 系统处理可能会修改 ClientHello 消息并用作会话的 TCP 代理服务器的 TLS/SSL 握手。

下图显示了内联部署。

客户端确立与服务器的 TCP 连接后（成功完成 TCP 三向握手后），托管设备会监控 TCP 会话的任何启动加密会话的尝试。TLS/SSL 握手通过使用交换客户端与服务器之间的专门数据包来确立加密会话。在 SSL 和 TLS 协议中，这些专门数据包称为握手消息。握手消息传达客户端和服务器都支持的加密属性：

- ClientHello - 客户端为每个加密属性指定多个受支持的值。
- ServerHello - 服务器为每个加密属性指定一个受支持的值，而 ServerHello 响应会确定安全会话期间系统使用的加密方法。

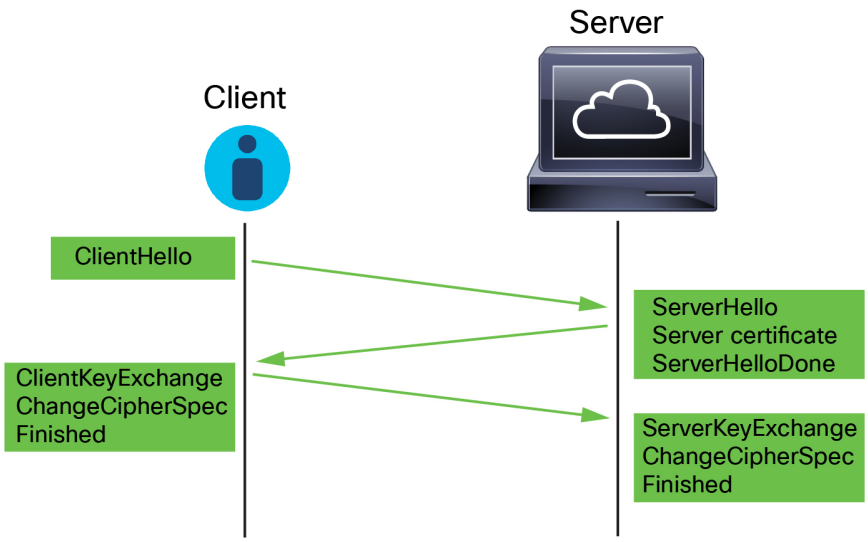
TLS/SSL 握手完成后，受管设备缓存加密会话数据，这允许在不需要完全握手的情况下进行会话恢复。受管设备还缓存服务器证书数据，这允许在使用相同证书的后续会话中更快速地处理握手。

ClientHello 消息的处理

客户端将 ClientHello 消息发送到一台服务器，如果可以建立安全连接，则该服务器将作为数据包的目标。客户端发送信息以启动 TLS/SSL 握手，或者用于响应目标服务器的 ServerHello 消息。

概述

下图显示了一个示例。另请参阅 RFC 8446，第 4 节 。您还可以参考 cheapsslshop.com 上的了解 SSL/TLS 握手协议等资源。



该过程可汇总如下：

1. ClientHello 启动该过程。

ClientHello 消息包含服务器名称指示 (SNI)，其中包含服务器的完全限定域名。

2. 当受管设备处理 ClientHello 消息并将其传输到目标服务器后，服务器会确定其是否支持客户端在该消息中指定的解密属性。如果不支持这些属性，服务器将向客户端发送握手失败警报。如果支持这些属性，服务器将发送 ServerHello 信息。如果商定的密钥交换方法使用证书进行身份验证，则服务器证书消息会紧跟在 ServerHello 消息之后。

   服务器证书包含使用者可选名称 (SAN)，可以具有完全限定的域名和 IP 地址。有关 SAN 的详细信息，请参阅可分辨名称。

3. 当受管设备收到这些消息时，会尝试将其与系统上配置的 TLS/SSL 规则相匹配。这些消息包含 ClientHello 消息或会话数据缓存中缺少的信息。具体而言，系统可能会匹配关于 TLS/SSL 规则的可分辨名称、证书状态、密码套件和版本条件的这些消息。

整个过程都会别加密。

数据交换

如果配置 TLS/SSL 解密，则当托管设备收到 ClientHello 消息时，系统会尝试将此消息与进行**解密 - 重新签名 (Decrypt - Resign)** 或**解密 - 已知密钥 (Decrypt - Known Key)** 操作的 TLS/SSL 规则 规则进行匹配。该匹配依赖于来自 ClientHello 消息的数据，以及来自缓存服务器证书数据的数据。可能的数据包括：

表 *1: TLS/SSL* 规则 条件的数据可用性

TLS/SSL 规则 条件	数据所在位置
区域	ClientHello
网络	ClientHello
VLAN 标记	ClientHello
端口	ClientHello
用户	ClientHello
应用	ClientHello（服务器名称指示器扩展）
类别	ClientHello（服务器名称指示器扩展）
证书	服务器证书（可能已缓存）
可分辨名称	服务器证书（可能已缓存）
证书状态	服务器证书（可能已缓存）
密码套件	ServerHello
版本	ServerHello

注释 仅在具有**阻止**或**阻止并重置**规则操作的规则中使用**密码套件 (Cipher Suite)** 和**版本 (Version)** 规则条件。在具有其他规则操作的规则中使用这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

ClientHello 修改

如果 ClientHello 消息与**解密 - 重新签名 (Decrypt-Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** 规则匹配，则系统会按如下方式修改 ClientHello 消息：

- （仅 TLS 1.2；TLS 1.3 不支持压缩。）压缩方法 - 删除 `compression_methods` 元素（其指定客户端所支持的压缩方法）。系统无法解密压缩的会话。
- 密码套件 - 如果系统不支持密码套件，则从 `cipher_suites` 元素中删除它们。如果系统不支持任何指定的密码套件，则系统将传输原始的未经修改的元素。此修改会减少无法解密的流量的“未知密码套件”(Unknown Cipher Suite) 和“不受支持的密码套件”(Unsupported Cipher Suite) 类型。
- 会话标识符 - 删除 `Session Identifier` 元素和 SessionTicket extension (RFC 5077, sec 3.2) 中任何与缓存会话数据不匹配的值。如果 ClientHello 值与缓存数据相匹配，则中断的会话无需客户端和服务器执行完整的 TLS/SSL 握手操作也可恢复。此修改会增加会话恢复的机会，并减少无法解密的流量的“不缓存会话”(Session Not Cached) 类型。
- 椭圆曲线 - 如果系统不支持椭圆曲线，则从受支持的椭圆曲线扩展中删除它们。如果系统不支持任何指定的椭圆曲线，则受管设备将删除扩展，并从 `cipher_suites` 元素中删除任何相关的密码套件。
- ALPN 扩展 - 删除应用层协议协商 (ALPN) 扩展中不受系统支持的任意值（例如，HTTP/2 协议）。
- 其他扩展 - 删除下次协议协商 (NPN) 和 TLS 通道 ID 扩展。

  目前，具有**解密 - 重新签名**或**解密 - 已知密钥**操作的 TLS/SSL 规则 在 ClientHello 协商期间在本地支持扩展主密钥 (EMS) 扩展，从而实现更安全的通信。EMS 扩展由 RFC 7627 定义。

在系统修改 ClientHello 消息后，它会确定消息是否通过访问控制评估（可能包括深度检测）。如果消息通过评估，则系统会将其传输到目标服务器。

如果 ClientHello 消息与**解密 - 重新签名 (Decrypt-Resign)** 或**解密 - 已知密钥 (Decrypt - Known Key)** 规则不匹配，则系统不会修改消息。然后，它会确定消息是否通过访问控制评估（可能包括深度检查）。如果消息通过检查，则系统会将其传输到目标服务器。

如果流量与**监控**规则条件匹配，则不会修改 ClientHello。

中间人

在 TLS/SSL 握手过程中，客户端和服务器之间无法再进行直接通信，因为在消息修改之后，由客户端和服务器计算的消息身份验证代码 (MAC) 不再匹配。对于所有后续的握手消息（和已建立的加密

会话），托管设备将充当中间人。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。因此，每个会话包含不同的加密会话详细信息。

注释 系统可以解密的密码套件会频繁更新，且其无法直接对应于您可以在 TLS/SSL 规则 条件中使用的密码套件。有关可解密密码套件的当前列表，请联系思科 TAC。

相关主题

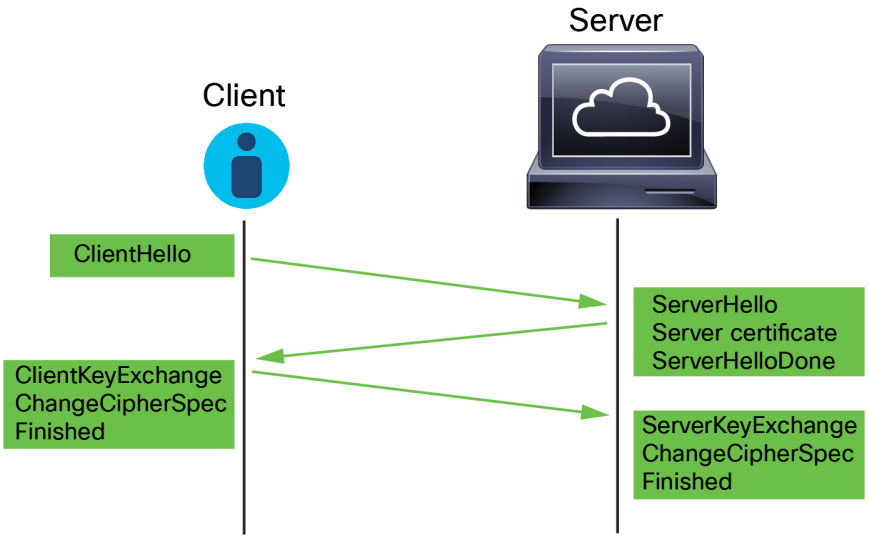
无法解密流量的默认处理选项

ServerHello 和服务器证书消息处理 ， 第 6 页

ServerHello 和服务器证书消息处理

概述

下图显示了一个示例。另请参阅 RFC 8446，第 4 节 。您还可以参考 cheapsslshop.com 上的了解 SSL/TLS 握手协议等资源。



该过程可汇总如下：

1. ClientHello 启动该过程。

   ClientHello 消息包含服务器名称指示 (SNI)，其中包含服务器的完全限定域名。

2. 当受管设备处理 ClientHello 消息并将其传输到目标服务器后，服务器会确定其是否支持客户端在该消息中指定的解密属性。如果不支持这些属性，服务器将向客户端发送握手失败警报。如果支持这些属性，服务器将发送 ServerHello 信息。如果商定的密钥交换方法使用证书进行身份验证，则服务器证书消息会紧跟在 ServerHello 消息之后。

   服务器证书包含使用者可选名称 (SAN)，可以具有完全限定的域名和 IP 地址。有关 SAN 的详细信息，请参阅可分辨名称。

3. 当受管设备收到这些消息时，会尝试将其与系统上配置的 TLS/SSL 规则相匹配。这些消息包含 ClientHello 消息或会话数据缓存中缺少的信息。具体而言，系统可能会匹配关于 TLS/SSL 规则的可分辨名称、证书状态、密码套件和版本条件的这些消息。

整个过程都会别加密。

TLS/SSL 规则 操作

如果消息与任何 TLS/SSL 规则 都不匹配，托管设备将执行 SSL 策略 默认操作。

如果消息与属于与访问控制策略关联的 SSL 策略 的规则匹配，则托管设备会根据需要继续：

操作：“监控”(Monitor)

TLS/SSL 握手继续完成。托管设备会跟踪和记录已加密的流量，但不会对其进行解密。

操作：“阻止”(Block) 或“阻止并重置”(Block with reset)

托管设备会阻止 TLS/SSL 会话，并重置 TCP 连接（如已配置）。

操作：“不解密”(Do Not Decrypt)

TLS/SSL 握手继续完成。受管设备不解密 TLS/SSL 会话期间交换的应用数据。

操作：“解密 - 已知密钥”(Derypt - Known Key)

托管设备尝试将服务器证书数据与先前导入管理中心的内部证书对象进行匹配。由于您无法生成内部证书对象，并且您必须拥有其私钥，因此假设您拥有在其上使用已知密钥解密的服务器。

如果此证书与已知证书匹配，则 TLS/SSL 握手将继续完成。受管设备使用上传的私钥解密并重新加密 TLS/SSL 会话期间交换的应用数据。

如果服务器在与客户端的初始连接和后续连接之间更改其证书，则必须在管理中心中导入新服务器证书，以便用于将来解密连接。

操作：“解密 - 重新签名”(Decrypt - Resign)

托管设备将处理服务器证书消息并使用之前上传或生成的证书颁发机构(CA)证书重签服务器证书。TLS/SSL 握手继续完成。托管设备随手会使用上传的私钥解密并重新加密 TLS/SSL 会话期间交换的应用数据。

注释 Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第 10 页和已知密钥解密（传入流量），第 11 页。

相关主题

ClientHello 消息的处理，第 3 页

TLS/SSL 最佳实践

本节讨论创建 SSL 策略 和规则时应牢记的信息。

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。

相关主题

解密案例，第 8 页
何时解密流量以及何时不解密，第 9 页
其他 TLS/SSL 规则 操作，第 11 页
TLS/SSL 规则 组件，第 12 页
TLS/SSL 规则 顺序评估，第 13 页
TLS 1.3 解密最佳实践

解密案例

只能允许或阻止通过系统时加密的流量，但不能对其进行深度检查或全面的策略实施（例如入侵防御）。

所有已加密的连接：

- 通过 SSL 策略 发送，以确定是否应解密或阻止它们。

  您还可以配置 TLS/SSL 规则 以阻止您知道不想在网络上传输的类型的加密流量，例如使用非安全 SSL 协议的流量或具有过期或无效证书的流量。

- 如果未被阻止，无论是否解密，流量都要经过访问控制策略，以做出最终的允许或阻止决定。

只有已解密的流量才能利用系统的威胁防御和策略实施功能，例如：

- 高级恶意软件防护
- 安全情报
- 威胁情报导向器
- 应用检测器
- URL 和类别过滤

请记住，解密并重新加密流量会增加设备的处理负载，从而会降低整体系统性能。

我们建议选择性地解密流量，以充分利用访问控制策略和深度检查。

总结：

- 可以通过策略允许或阻止已加密的流量；无法检查已加密的流量
- 已解密的流量受威胁防御和策略实施的约束；可以通过策略允许或阻止已解密的流量

相关主题

使用文件和入侵策略的深度检测

何时解密流量以及何时不解密

本节提供有关何时应解密流量以及何时应允许其通过加密防火墙的准则。

何时不解密流量

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

（Snort 2。）如果选择绕行某些类型的流量的解密，则不会对流量进行任何处理。加密流量会首先由 SSL 策略 进行评估，然后进入访问控制策略，在其中做出最终的允许或阻止决策。

（Snort 3。）对于任何符合访问控制规则的信任、阻止或阻止并重置的连接，除非流量被预先过滤，否则 SSL 策略 不会被绕过。加密流量会首先由 SSL 策略 进行评估，然后进入访问控制策略，在其中做出最终的允许或阻止决策。

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

TLS/SSL 规则 为此流量提供**不解密**操作；有关详细信息，请参阅TLS/SSL 规则 不解密操作。

注释 本主题末尾的相关信息链接解释了规则评估的某些方面是如何运作的。URL 和应用过滤等条件对加密流量存在限制。请确保您了解这些限制。

有关在 **不解密** 规则中使用 URL 过滤的详细信息，请参阅 TLS/SSL 规则 不解密操作。

何时解密流量

系统的威胁防护和策略实施功能必须在解密所有加密流量后才能发挥作用。如果托管设备允许解密流量（取决于其内存和处理能力），则应解密法律或法规未禁止的流量。如果您必须决定哪些流量要解密，请根据网络上允许流量的风险做出决定。系统提供了一个灵活框架，它会利用规则条件（包括 URL 信誉、密码套件、协议和许多其他因素）来对流量进行分类。

相关主题

解密和重新签名（传出流量），第 10 页
已知密钥解密（传入流量），第 11 页
TLS/SSL 规则 准则和限制
SSL 规则顺序
URL 条件（URL 过滤）
应用规则顺序
TLS 1.3 解密最佳实践

解密和重新签名（传出流量）

解密 - 重新签名 (Decrypt - Resign) TLS/SSL 规则 操作使系统能够充当中间人，拦截、解密以及（如果允许流量通过）检查和重新加密。**解密 - 重新签名 (Decrypt - Resign)** 规则操作用于传出流量；也就是说，目的服务器在受保护的网络之外。

威胁防御 设备会使用规则中指定的内部证书颁发机构 (CA) 对象来与客户端协商，并在客户端和 威胁防御 设备之间建立 TLS/SSL 隧道。同时，设备连接至目标网站，并在服务器和 威胁防御 设备之间建立 SSL 隧道。

因此，客户端将看到配置用于 TLS/SSL 规则 的 CA 证书，而不是来自目标服务器的证书。客户端必须信任防火墙的证书才能完成连接。威胁防御 设备随后会对客户端和目标服务器之间的流量执行双向解密/重新加密。

前提条件

要使用**解密 - 重新签名 (Decrypt - Resign)** 规则操作，您必须使用 CA 文件和配对的私钥文件创建内部 CA 对象。如果您还没有 CA 和私钥，则可以在系统中生成它们。

注释 Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第 10 页和已知密钥解密（传入流量），第 11 页。

相关主题

TLS/SSL 规则 解密操作
外部证书对象

已知密钥解密（传入流量）

解密 - 已知密钥 (Decrypt - Known Key) TLS/SSL 规则 操作使用服务器的私钥解密流量。**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作用于传入流量；也就是说，目的服务器位于受保护的网络内。

使用已知密钥进行解密的主要目的是保护服务器免受外部攻击。

前提条件

要使用**机密 - 已知密钥 (Decrypt - Known Key)** 规则操作，您必须使用服务器的证书文件和配对的私钥文件来创建内部证书对象。

注释 Firepower 系统不支持相互身份验证；也就是说，不能将客户端证书上传到 管理中心 并将其用于**解密 - 重新签名 (Decrypt - Resign)** 或 **解密 - 已知密钥 (Decrypt - Known Key)** TLS/SSL 规则 操作。有关详细信息，请参阅解密和重新签名（传出流量），第 10 页和已知密钥解密（传入流量），第 11 页。

相关主题

已知密钥解密（传入流量），第 11 页
TLS/SSL 规则 解密操作
内部证书对象

其他 TLS/SSL 规则 操作

以下各部分讨论其他 TLS/SSL 规则 操作。

相关主题

TLS/SSL 规则 阻止操作
TLS/SSL 规则 监控操作

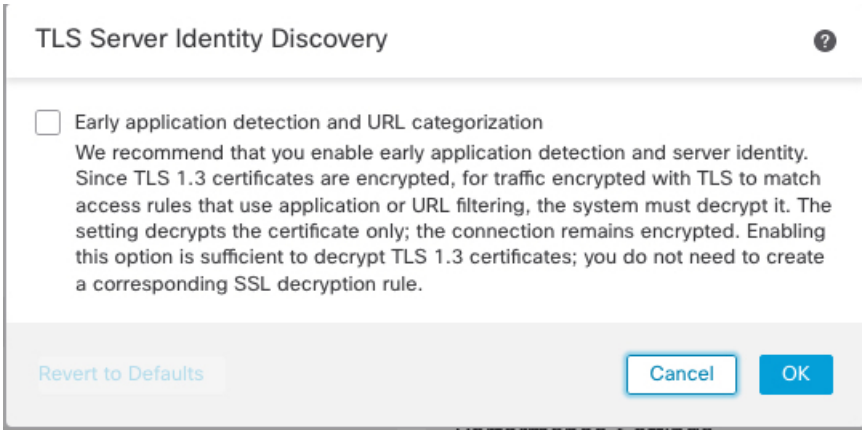
TLS 1.3 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

在为访问控制策略配置高级设置时，可以启用此功能，称为 *TLS* 服务器身份发现。

我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。SSL 策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

下图显示在访问控制策略的高级设置中启用 TLS 服务器身份发现的示例。



相关主题

创建基本 SSL 策略

将其他策略与访问控制相关联

TLS/SSL 规则 组件

每个 TLS/SSL 规则 都有以下组件。

状态

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

SSL 策略 中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

条件

条件指定规则处理的特定流量。条件可以按安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL、用户、证书、证书使用者或颁发者、证书状态、密码套件或加密协议版本来匹配流量。使用条件取决于目标设备许可证。

操作

规则操作确定系统如何处理匹配的流量。您可以对加密的匹配流量执行监控、允许、阻止或解密操作。解密和允许的加密流量会受到进一步检查。请注意，系统不对被阻止的加密流量执行检查。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。您可以在系统阻止加密会话或允许其未经解密便通过（取决于 SSL 策略中的设置）时记录连接。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。您可以将连接记录到Cisco Secure Firewall Management Center数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器中。

有关日志记录的详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 连接日志记录最佳实践。

提示 正确创建 TLS/SSL 规则 并对其排序是一项复杂的任务。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，SSL 策略接口具有功能强大的规则警告和错误反馈系统。

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。

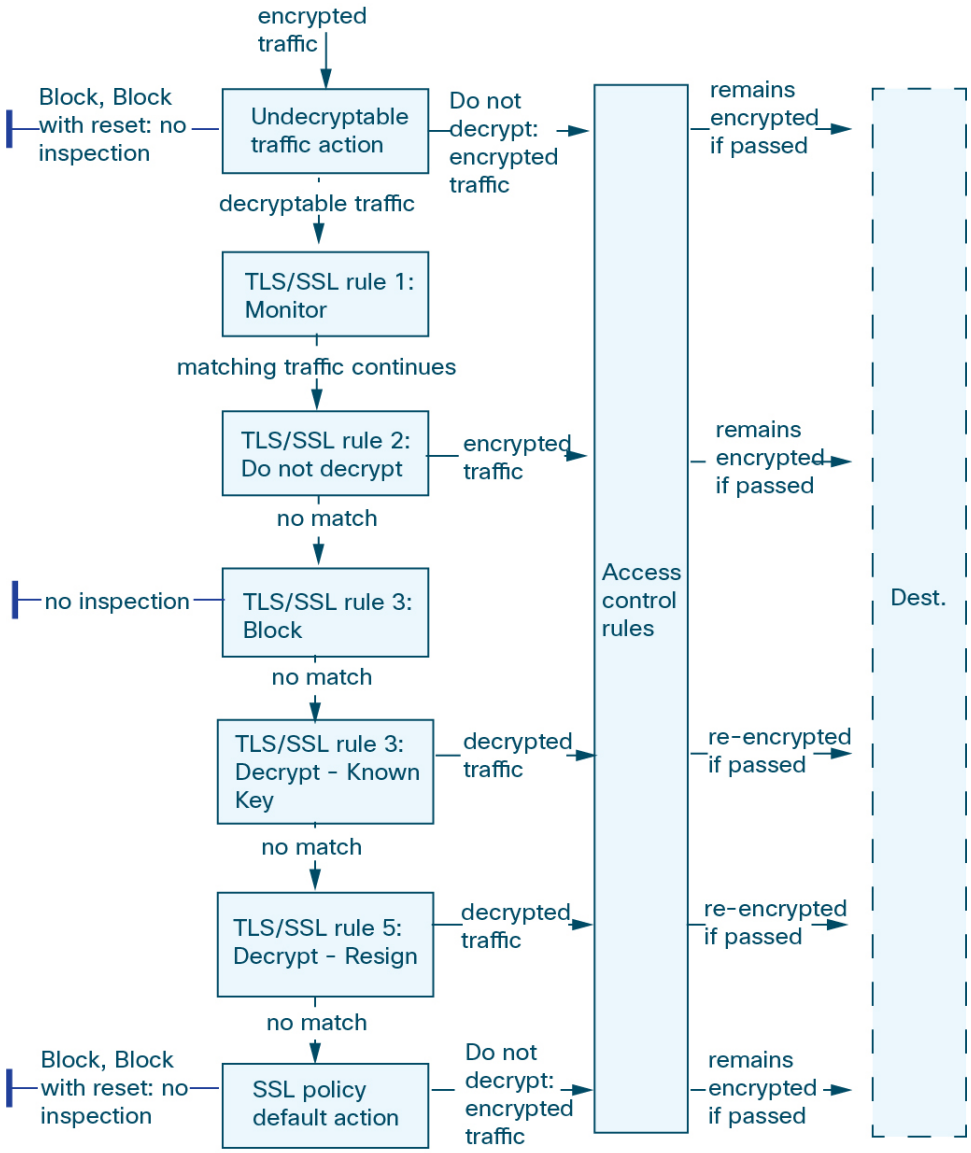
除了按照编号排序规则之外，还可按类别对规则进行分组。默认情况下，系统提供三个类别：管理员、标准和根。您可以添加自定义类别，但是不能删除系统提供的类别或更改类别的顺序。

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

多规则示例

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。

TLS 加密加速

TLS 加密加速 加快以下操作：

- TLS/SSL 加密和解密。
- VPN，包括TLS/SSL和 IPsec

支持的硬件

以下硬件型号支持 TLS 加密加速：

- Firepower 3100 和 Cisco Secure Firewall Threat Defense
- 采用 Cisco Secure Firewall Threat Defense 的 Firepower 2100
- 采用 Cisco Secure Firewall Threat Defense的 Firepower 4100/9300

  有关 TLS 加密加速Firepower 4100/9300 支持威胁防御 容器实例的信息，请参阅 *FXOS* 配置指南。

所有虚拟设备或除前面所述设备之外的任何硬件上都不支持 TLS 加密加速。

注释 有关 TLS 加密加速 和 4100/9300 的详细信息，请参阅 *FXOS* 配置指南。

以下方不支持的功能 TLS 加密加速

TLS 加密加速不支持的功能包括：

- 启用了 威胁防御 容器实例 的托管设备。
- 如果检测引擎配置为保留连接，并且检测引擎意外出现故障，则 TLS/SSL流量将被丢弃，直到引擎重启。

  此行为受 **configure snort preserve-connection {enable | disable}** 命令控制。

TLS 加密加速 准则和限制

如果受管设备启用了 TLS 加密加速，请记住以下几点。

仅 HTTP 性能

在不对流量进行解密的受管设备上使用 TLS 加密加速可能会影响性能。

联邦信息处理标准 (FIPS)

如果同时启用了 TLS 加密加速 和联邦信息处理标准 (FIPS)，则与以下选项的连接会失败：

- 大小小于 2048 字节的 RSA 密钥
- Rivest 密码 4 (RC4)
- 单一数据加密标准（单一 DES）
- Merkle – Damgard 5 (MD5)
- SSL v3

当您将 管理中心 和受管设备配置为以安全认证合规模式运行时，FIPS 会被启用。在这些模式下运行时，要允许连接，则可配置 Web 浏览器以接受更为安全的选项。

更多详情：

- FIPS 支持的密码：关于 SSL 设置。
- 安全认证合规性模式。
- 通用标准。

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

有关详细信息，请参阅无法解密流量的默认处理选项。

要确定应用是否正在使用 TLS 心跳，请参阅对 TLS 心跳进行故障排除。

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。

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。

如果出现大量超订用，有以下选项可供选择：

- 升级受管设备以提高 TLS/SSL 处理能力。
- 更改您的 SSL 策略，为不具有较高解密优先级的流量添加**不解密**规则。

查看 TLS 加密加速的状态

本主题讨论如何确定是否已启用 TLS 加密加速。

请执行 管理中心 中的下列任务。

过程

步骤 1 登录管理中心。

步骤 2 点击**设备** > **设备管理**。

步骤 3 点击 **编辑**（ ） 以编辑受管设备。

步骤 4 单击**设备 (Device)**页面。TLS 加密加速 状态显示在“常规”(General) 部分中。

如何配置 SSL 策略 和规则

本主题简要概述要在这些策略中配置 SSL 策略和 TLS/SSL 规则而必须完成的任务，以便阻止、监控或允许网络上的 TLS/SSL 流量。

您必须是 管理员、访问管理员 或 网络管理员 才能执行此任务。

过程

	命令或操作	目的
步骤 1	创建an SSL 策略。	An SSL 策略 是一个或多个规则的容器。要使用 an SSL 策略 及其规则进行访问控制，您必须稍后将 SSL 策略 与访问控制策略关联。有关详细信息，请参阅创建基本 SSL 策略。
步骤 2	为您的 SSL 策略 设置默认操作。	当流量与 SSL 策略 定义的规则不匹配时将采取默认操作。请参阅SSL 策略 默认操作。
步骤 3	指定应如何处理无法解密的流量。	流量无法解密的原因有很多，包括协议不安全、使用和未知的密码套件，或者在握手或解密错误的情况下。请参阅无法解密流量的默认处理选项。
步骤 4	对于**解密 - 已知密钥 (Decrypt - Known Key)**（用于解密流向网络中服务器的入站流量）TLS/SSL 规则，请创建内部证书对象。	内部证书对象使用您的服务器的证书和私钥。请参阅内部证书对象。
步骤 5	对于**解密 - 重新签名 (Decrypt - Resign)**（解密流向网络外部服务器的出站流量）TLS/SSL 规则，请创建内部证书颁发机构 (CA) 对象。	内部 CA 对象会使用 CA 和私钥。请参阅内部证书颁发机构对象。
步骤 6	创建您的 TLS/SSL 规则。	
步骤 7	将 SSL 策略 与访问控制策略关联。	除非您将 SSL 策略 与访问控制策略相关联，否则它不会起作用。在执行此操作后，您可以选择允许或阻止与访问控制规则匹配的流量并执行其他操作。请参阅将其他策略与访问控制相关联。
步骤 8	配置访问控制规则，以便允许或阻止已解密的流量。	请参阅访问控制策略组件。
步骤 9	将访问控制策略部署到托管设备。	在策略生效之前，必须将其部署到托管设备。请参阅部署配置更改。

相关主题

TLS/SSL 规则

的历史记录SSL 策略

功能	版本	详细信息
TLS 1.3 解密	7.2	现在，您可以在 SSL 策略的高级操作中启用 TLS 1.3 解密。TLS 1.3 解密需要托管设备运行 Snort 3。 同时还有其他选项；有关详细信息，请参阅SSL 策略 高级选项。 **新增/更改的屏幕：SSL 策略 (SSL Policy) > 高级设置 (Advanced Settings)**
SSL 策略高级设置	7.1	SSL 策略高级设置 **新增/更改的屏幕：SSL 策略 (SSL Policy) > 高级设置 (Advanced Settings)**
能够指定具有未知信誉的 URL 的处理方式	6.7	有关详细信息，请参阅URL 过滤历史记录。
用于**解密的 ClientHello 修改 - 已知**密钥规则	6.7	有关详细信息，请参阅ClientHello 消息的处理 ， 第 3 页。
能够提取 TLS 1.3 流量中的证书，以便让流量能够匹配访问控制规则中的 URL 和应用条件。	6.7	新增/修改的屏幕：**策略 (Policies) > 访问控制 (Access Control) >（编辑访问控制策略） > 高级 (Advanced)**链接。 有关详细信息，请参阅TLS 1.3 服务器身份发现 ， 第 11 页。
对基于类别和信誉的URL过滤的更改	6.5	有关详细信息，请参阅URL 过滤历史记录。
TLS 加密加速 无法被禁用	6.4	TLS 加密加速 会在所有支持的设备上启用。 在具有本地接口的托管设备上，无法禁用 TLS 加密加速。 对 威胁防御 容器实例 上 TLS 加密加速 的支持是有限的，如此表的下一行所述。 删除的命令： **system support ssl-hw-accel enable** **system support ssl-hw-accel disable** **system support ssl-hw-status**
支持将 TLS 加密加速 用于 Firepower 4100/9300 模块/安全引擎上的一个 威胁防御 容器实例	6.4	您现在可以在模块/安全引擎上为一个 威胁防御 容器实例 启用 TLS 加密加速。TLS 加密加速 对其他容器实例禁用，但对本地实例启用。 新增/修改的命令： **config hwCrypto enable** **show crypto accelerator status** 取代 **system support ssl-hw-status**）

功能	版本	详细信息
TLS/SSL 硬件加速 现在称为 *TLS* 加密加速	6.4	名称更改体现了可在更多设备上支持 TLS/SSL 加密和解密加速。根据设备的不同，加速可以在软件或硬件中执行。 受影响的屏幕：要查看 TLS 加密加速的状态，**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)**，常规 (General) 页面。
支持扩展主密钥扩展（请参阅 RFC 7627）	6.3.0.1	SSL 策略支持 TLS 扩展主密钥扩展；具体而言，是指具有**解密 - 重新签名**或**解密 - 已知密钥**规则操作的策略。
不支持扩展主密钥扩展	6.3	在 ClientHello 修改**解密 - 重新签名**规则期间删除此扩展。
TLS/SSL 硬件加速 默认为已启用	6.3	TLS/SSL 硬件加速 默认为在所有支持的设备上启用，但是如有需要，可以禁用它。
支持扩展主密钥扩展（请参阅 RFC 7627）	6.2.3.9	SSL 策略支持 TLS 扩展主密钥扩展；具体而言，是指具有**解密 - 重新签名**或**解密 - 已知密钥**规则操作的策略。
积极的 TLS 1.3 降级	6.2.3.7	使用 **system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** CLI 命令，可以确定将 TLS 1.3 流量降级到 TLS 1.2 的行为。有关详细信息，请参阅 Cisco Secure Firewall Threat Defense 命令参考。
TLS/SSL 硬件加速 已引入	6.2.3	某些受管设备型号会在硬件中执行 TLS/SSL 加密和解密，从而提高性能。默认情况下，此功能处于启用状态。 受影响的屏幕：要查看 TLS/SSL 硬件加速的状态，**设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)**，常规 (General) 页面。
支持类别和信誉条件	6.2.2	具有类别/信誉条件的访问控制规则或 SSL 规则。
支持安全搜索。	6.1.0	• 系统可为先被 SSL 策略加密然后被访问控制规则或访问控制策略默认操作阻止（或交互式阻止）的 HTTP 响应页面。在这些情况下，系统会加密响应页面并在重新加密的 SSL 数据流最后发送该页面。 • SafeSearch 可过滤掉令人不快内容，并阻止用户搜索成人站点。
TLS/SSL 策略。	6.0	引入的功能。

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。