SSL 策略

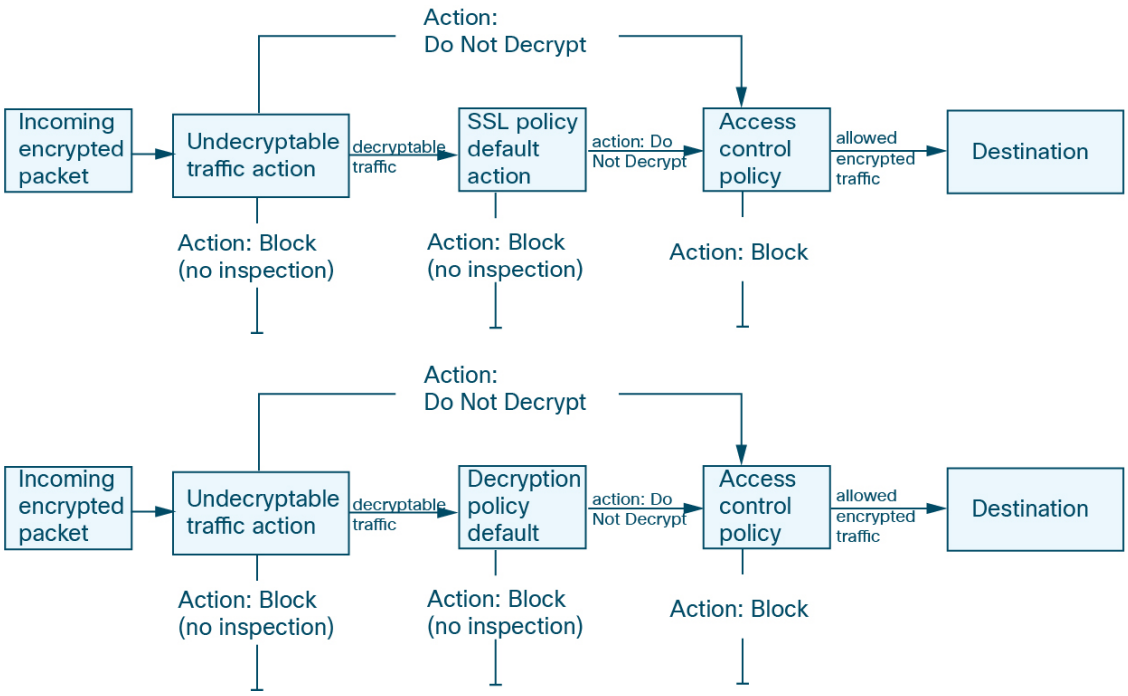
以下主题概述 SSL 策略 的创建、部署、管理和日志记录。

SSL 策略概述

An SSL 策略 确定系统如何处理网络上的加密流量。可以配置一个或多个 SSL 策略，将 an SSL 策略与访问控制策略关联起来，然后将访问控制策略部署到受管设备。当设备检测到 TCP 握手时，访问控制策略首先处理并检查流量。如果它随后识别出通过 TCP 连接建立的 TLS/SSL加密会话，则 SSL 策略将接管、处理和解密已加密的流量。

注意 仅*Snort 2*。添加或删除构件SSL 策略 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。

最简单的 SSL 策略（如下图所示）引导其部署所在设备，以使用单个默认操作处理加密流量。可将默认操作设置为阻止可解密流量（无需进一步检查），或者使用访问控制检查未解密的可解密流量。然后系统可以允许或阻止已加密的流量。如果设备检测到无法解密的流量，它会阻止该流量，无需进一步检查或不对其进行解密，而是使用访问控制对其进行检查。



更为复杂的 SSL 策略可通过不同的操作处理不同类型无法解密的流量，根据证书颁发机构 (CA) 是否颁发或信任加密证书而控制流量，以及使用 TLS/SSL 规则 规则对已加密流量的日志记录和处理进行精细控制。这些规则可能很简单，也可能很复杂，使用多个条件匹配和检查已加密的流量。

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

TLS/SSL 规则 条件

SSL 策略 默认操作

an SSL 策略的默认操作确定系统如何处理与策略中任何非监控规则都不匹配的可解密的已加密流量。当部署不包含任何 TLS/SSL 规则 规则的 an SSL 策略时，默认操作确定如何处理网络上所有无法解密的流量。请注意，对于默认操作阻止的已加密流量，系统不会执行任何类型的检查。

表 *1: SSL* 策略 默认操作

默认操作	对已加密流量的影响
阻止	阻止 TLS/SSL 会话，无需进一步检查。
阻止并重置	阻止 TLS/SSL 会话并且无需进一步检查，然后重置 TCP 连接。如果流量使用的是像 UDP 一样的无连接协议，请选择此选项。在这种情况下，无连接协议将尝试重新建立连接，直到被重置。 执行此操作时，浏览器中还会显示连接重置错误，以便用户知道连接被阻止。
不解密	使用访问控制检查已加密的流量。

相关主题

创建基本 SSL 策略，第 6 页

无法解密流量的默认处理选项

表 *2:* 无法解密的流量类型

类型	说明	默认操作	可用操作
压缩的会话	TLS/SSL 会话应用数据压缩方法。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
SSLv2 会话	此会话使用 SSL V2 加密。 请注意，如果 ClientHello 消息为 SSL 2.0，并且已传输流量的剩余部分为 SSL 3.0，则流量可解密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
未知密码套件	系统无法识别该密码套件。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作

类型	说明	默认操作	可用操作
不支持的密码套件	系统不支持根据检测到的密码套件进行解密。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
会话无法缓存	TLS/SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
握手错误	TLS/SSL 握手协商期间出错。	继承默认操作	不解密 阻止 阻止并重置 继承默认操作
解密错误	在流量解密时出错。	阻止	阻止 阻止并重置

首次创建 an SSL 策略时，默认情况下将禁用记录默认操作所处理的连接。由于默认操作的日志记录设置也适用于无法解密的流量处理，默认情况下也将禁用记录无法解密的流量操作所处理的连接。

请注意，如果浏览器使用证书锁定验证服务器证书，则无法通过对服务器证书重新签名来解密此流量。有关详细信息，请参阅TLS/SSL 规则 准则和限制。

相关主题

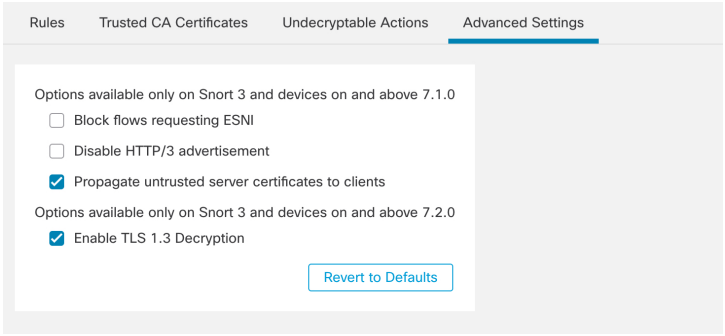
设置无法解密的流量的默认处理 ，第 6 页

SSL 策略 高级选项

An SSL 策略 的 **高级设置** 选项卡页面具有适用于为应用策略的 Snort 3 配置的所有受管设备的全局设置。 在运行以下命令的任何受管设备上，这些设置都将被忽略：

- 早于 7.1 的版本
- Snort 2

以下为示例。



阻止请求 ESNI 的流

加密服务器名称指示（ESNI [建议草案的链接]）是客户端告知 TLS 1.3 服务器其请求内容的一种方式。由于 SNI 会被加密，因此您可以选择阻止这些连接，因为系统无法确定服务器是什么。

禁用 HTTP/3 通告

此选项会从 TCP 连接中的 ClientHello 删除 HTTP/3 (RFC 9114)，因为：

- 如 RFC 9114 中所述，HTTP/3 是 QUIC 传输协议的一部分，而不是 TCP 传输协议
- Firepower 系统尚不支持 QUIC
- 阻止这些客户端通告 HTTP/3 提供了对攻击和规避企图的保护。

将不受信任的服务器证书传播到客户端

这仅适用于匹配**解密 - 重新签名 (Decrypt - Resign)** 规则操作的流量。

启用此选项可在服务器证书不受信任的情况下，使用托管设备上的证书颁发机构 (CA) 来替换服务器证书。不受信任的服务器证书是指未在 Cisco Secure Firewall Management Center 中列为受信任 CA 的证书。（**对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **受信任 CA (Trusted CAs)**）。

启用 TLS 1.3 解密

（仅限 Snort 3。）移动滑块可让由 管理中心 管理的 威胁防御 设备能够解密 TLS 1.3 流量。

如果滑块移至禁用位置，则系统仅解密 TLS 1.2 流量。

相关信息

TLS/SSL 规则 最佳实践

SSL 策略 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

创建基本 SSL 策略

要配置 an SSL 策略，您必须为策略提供唯一的名称并指定默认操作。

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**新建策略**。
步骤 4 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。
步骤 5 指定**默认操作 (Default Action)**；请参阅SSL 策略 默认操作 ， 第 2 页。
步骤 6 为默认操作配置日志记录选项，。
步骤 7 点击**保存 (Save)**。

后续操作

- 为无法解密的流量设置默认处理，请参阅设置无法解密的流量的默认处理 ， 第 6 页。
- 为默认处理无法解密的流量配置日志记录选项。
- 设置高级策略属性：SSL 策略 高级选项 ， 第 4 页。
- 将 SSL 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。
- 部署配置更改。

设置无法解密的流量的默认处理

您可以在 SSL 策略 级别设置无法解密的流量操作以处理系统无法解密或检查的某些类型的已加密流量。部署不包含任何 TLS/SSL 规则 的 an SSL 策略 时，无法解密的流量操作确定如何处理网络上的所有无法解密的已加密流量。

视乎无法解密的流量类型，您可以选择：

- 阻止连接。

- 阻止连接，然后重置连接。对于UDP等一直尝试连接直到连接被阻止的无连接协议，最好选择此选项。
- 使用访问控制检查已加密的流量。
- 继承 SSL 策略 的默认操作。

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 策略名称旁边的 **编辑**（ ）。

步骤 4 在 SSL 策略 编辑器中，点击**无法解密的操作 (Undecryptable Actions)**。

步骤 5 对于每个字段，请选择要对无法解密的流量类型执行的SSL 策略 的默认操作或其他操作。有关详细信息，请参阅无法解密流量的默认处理选项，第 3 页和SSL 策略 默认操作，第 2 页。

步骤 6 点击**保存 (Save)** 保存策略。

下一步做什么

- 为无法解密的流量操作所处理的连接配置默认日志记录。
- 部署配置更改。

管理SSL 策略

在 SSL 策略 编辑器中，您可以：

- 添加、编辑、删除、启用、禁用和整理 TLS/SSL 规则。
- 添加受信任 CA 证书。
- 确定系统无法解密的已加密流量的处理。
- 记录由默认操作和无法解密的流量操作处理的流量。
- 设置高级选项。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。

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 管理 SSL 策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略。
- 复制 - 点击 **复制**（）。
- 创建 - 点击**新建策略 (New Policy)**；请参阅创建基本 SSL 策略，第 6 页。
- 删除 - 点击 **删除**（）。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 报告 - 点击**报告**（）；请参阅生成当前策略报告。
- 编辑 - 点击 **编辑**（）。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。
- 要将受信任 CA 证书添加到 SSL 策略，请参阅信任外部证书颁发机构。
- 要配置您的 SSL 策略 如何处理无法解密的流量，请参阅设置无法解密的流量的默认处理，第 6 页。
- SSL 策略 高级设置 - 请参阅SSL 策略 高级选项，第 4 页。
- 导入/导出 - 请参阅Cisco Secure Firewall Management Center 和威胁防御管理网络管理中有关导入和导出配置的部分。
- 要为无法解密的流量处理以及不匹配 SSL 规则的流量记录连接，请参阅《Cisco Secure Firewall Management Center 管理指南》中的使用策略默认操作记录连接 。
- 部署 - 选择**部署** > **部署**；请参阅部署配置更改。

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。