SSL 解密

某些协议（如 HTTPS）使用安全套接字层 (SSL) 或其后续版本传输层安全性 (TLS) 来加密流量以进行安全传输。由于系统无法检查加密连接，因此，如果要应用可考虑借助更高层流量特性进行访问决策的访问规则，则必须将其解密。

关于 SSL 解密

通常情况下，访问控制策略会评估连接以确定是允许还是阻止相应连接。但是，如果启用 SSL 解密策略，则连接将首先被发送至 SSL 解密策略，以确定应将其解密还是阻止。然后，访问控制策略评估所有未阻止连接（无论是否解密），作出最终的允许/阻止决策。

注释 您必须启用 SSL 解密策略，才能在身份策略中实施有效的身份验证规则。如果您启用 SSL 解密来启用身份策略，但不想另外实施 SSL 解密，请选择“不解密”作为默认操作，并且不要创建其他 SSL 解密规则。身份策略会自动生成所需的任何规则。

以下主题更详细地介绍了加密流量管理和解密。

为什么要实施 SSL 解密？

无法检查 HTTPS 连接等加密流量。

许多连接均是合法加密的连接，比如与银行和其他金融机构的连接。许多网站使用加密保护隐私或敏感数据。例如，您与 设备管理器 的连接已加密。

但是，用户也可能会隐藏加密连接中的不良流量。

通过实施 SSL 解密，可解密和检查连接，确保不含威胁或其他不良流量，然后重新加密后再允许继续连接。（解密流量通过访问控制策略，并根据检查的加密连接特征而不是加密特征匹配规则。）这平衡了应用访问控制策略的需求与用户保护敏感信息的需求。

还可以配置 SSL 解密规则，阻止明确不想要允许其进入网络的加密流量类型。

请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

可应用于加密流量的操作

配置 SSL 解密规则时，可应用以下主题中所述的操作。这些操作也可用于默认操作（适用于与显示规则不匹配的任何流量）。

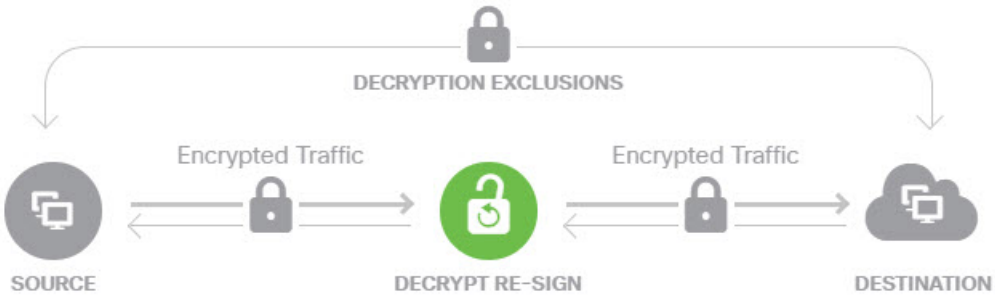
注释 通过 SSL 解密策略的任何流量均必须通过访问控制策略。除了 SSL 解密策略中丢弃的流量外，最终的允许或丢弃决定还取决于访问控制策略。

解密重签名

如果选择解密或重签流量，系统将扮演中间人的角色。

例如，用户在浏览器中键入 https://www.cisco.com。流量到达 威胁防御 设备，然后设备使用规则中指定的 CA 证书与用户进行协商，并在用户和 威胁防御 设备之间建立 SSL 隧道。同时，设备连接至 https://www.cisco.com ，并在服务器和 威胁防御 设备之间建立 SSL 隧道。

因此，用户将看到配置用于 SSL 解密规则的 CA 证书，而不是来自 www.cisco.com 的证书。用户必须信任该证书才能完成连接。威胁防御 设备随后对用户和目标服务器之间的流量执行双向解密/重新加密。



注释 如果客户端不信任用于对服务器证书重新签名的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。

如果使用解密重签名操作配置规则，则除了已配置的任何规则条件之外，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。由于您可以选择用于 SSL 解密策略的单个重签名证书，因此可以限制匹配重签规则的流量。

例如，仅当重签名证书是基于 EC 的 CA 证书时，使用椭圆曲线 (EC) 算法加密的出站流量才能匹配解密重签名规则。同样，仅当全局重签名证书为 RSA 时，使用 RSA 算法加密的流量才可与解密重签名规则匹配；即使所有其他配置的规则条件匹配，使用 EC 算法加密的出站流量也与规则不匹配。

解密已知密钥

如果您拥有目标服务器，则可使用已知密钥实现解密。在这种情况下，用户打开 https://www.cisco.com 的连接后，用户会看到 www.cisco.com 的实际证书，即使出示证书的是 威胁防御 设备。

您的组织必须是域和证书的所有者。以 cisco.com 为例，让最终用户查看思科证书的唯一可能方式是，您实际拥有域 cisco.com（即您是思科系统公司）并拥有由公共 CA 签名的 cisco.com 证书。您仅可使用已知密钥对您的组织拥有的站点进行解密。

使用已知密钥进行解密的主要目的是对通往 HTTPS 服务器的流量进行解密，以保护服务器免受外部攻击。如要检查流向外部 HTTPS 站点的客户端流量，由于您不是服务器所有者，所以必须使用解密重签名。

注释 要使用已知密钥解密，必须将服务器证书和密钥上传为内部身份证书，再在 SSL 解密策略设置中将其添加至已知密钥证书。然后，可编写已知密钥解密规则，其中服务器地址为目标地址。有关将证书添加至 SSL 解密策略的信息，请参阅为已知密钥和重签解密配置证书，第 16 页。

不解密

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。系统会使加密流量继续进入访问控制策略，根据流量所匹配的访问控制规则对其执行允许或丢弃操作。

阻止

您可以简单地阻止匹配 SSL 解密规则的加密流量。阻止 SSL 解密策略可防止连接到访问控制策略。

阻止 HTTPS 连接后，用户看不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。

自动生成的 SSL 解密规则

无论您是否启用 SSL 解密策略，系统都会自动为实施主动身份验证的各身份策略规则生成解密重签名规则。这是为 HTTPS 连接启用主动身份验证的必然要求。

启用 SSL 解密策略后，您可以在“身份策略主动身份验证规则”标题下看到这些规则。这些规则归入 SSL 解密策略顶部。这些规则为只读格式。仅可通过更改身份策略进行更改。

处理不可解密流量

有几个特点使得连接不可解密。如果连接具有以下任何特征，则默认操作将应用于该连接，而不管该连接本可能会与哪个规则匹配。如果将“阻止”选作默认操作（而不是“不解密”），则可能会出问题，包括过度丢弃合法流量的问题。您可以更改默认行为，如配置高级和无法解密的流量设置，第 17 页中所述。

- 压缩会话 - 数据压缩应用于连接。
- SSLv2 会话 - 支持的最低 SSL 版本是 SSLv3。
- 未知密码套件 - 系统无法识别连接的密码套件。
- 不受支持的密码套件 - 系统不支持根据检测到的密码套件进行解密。
- 会话未缓存 - 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。
- 握手错误 - SSL 握手协商期间出错。
- 解密错误 - 解密操作期间出错。
- 被动接口流量 - 被动接口（被动安全区）上的所有流量均无法解密。

SSL 解密许可证要求

使用 SSL 解密策略无需特殊许可证。

但需要 **URL** 许可证创建将 URL 类别和信誉作为匹配标准的规则。有关配置许可证的信息，请参阅启用或禁用可选许可证。

SSL 解密准则

配置和监控 SSL 解密策略时，请注意以下事项：

- 对于与设置为信任或阻止的访问控制规则匹配的任何连接，如果这些规则满足以下条件，则绕过 SSL 解密策略：
  - 将安全区、网络、地理位置和端口仅用作流量匹配条件。

- 排在任何要求检测的其他规则之前，例如，基于应用或URL匹配连接的规则，或允许应用入侵或文件检测的规则。

- 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的类别是“基于网页的邮件”，而登录页的类别是“互联网门户网站”。要对到这些站点的连接解密，必须在规则中添加这两个类别。
- 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 SSL 解密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）”。
- 如果您有任何主动身份验证规则，将无法禁用 SSL 解密策略。要禁用 SSL 解密策略，您必须禁用身份策略，或者删除任何使用主动身份验证的身份规则。

如何实施和维护 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

与其他一些安全策略不同的是，您需要监控并积极维护 SSL 解密策略，这是因为目标服务器上的证书可能会过期甚至发生变更。此外，客户端软件的变更可能会改变解密某些连接的能力，这是因为解密重签名操作无法与中间人攻击区分开来。

以下程序介绍了实施和维护 SSL 解密策略的端到端流程。

过程

步骤 1 如果要实施解密重签名规则，请创建所需的内部 CA 证书。

必须使用内部证书颁发机构 (CA) 证书。有以下选项可供选择。由于用户必须信任证书，因此应上传客户端浏览器已配置为可信任的证书，或确保所上传的证书已添加到浏览器信任存储区。

- 创建由设备自身签署的自签名内部 CA 证书。请参阅生成自签名的内部证书和内部 CA 证书。
- 上传由外部受信任 CA 或组织内部 CA 签署的内部 CA 证书和密钥。请参阅上传内部证书和内部 CA 证书。

步骤 2 如果要实施解密已知密钥规则，请从各内部服务器收集证书和密钥。

只可将解密已知密钥用于您所控制的服务器，这是因为必须从服务器中获取证书和密钥。上传这些证书和密钥，作为内部证书（而不是内部 CA 证书）。请参阅上传内部证书和内部 CA 证书。

步骤 3 启用 SSL 解密策略，第 8 页。

启用该策略时，还需要配置一些基本设置。

步骤 4 配置默认 SSL 解密操作，第 9 页。

如有疑问，请选择**不解密**作为默认操作。在适当的情况下，访问控制策略仍然可以丢弃与默认 SSL 解密规则匹配的流量。

步骤 5 配置 SSL 解密规则，第 10 页。

标识要解密的流量以及要应用的解密类型。

步骤 6 如要配置已知密钥解密，请编辑 SSL 解密策略设置，以加入这些证书。请参阅为已知密钥和重签解密配置证书，第 16 页。

步骤 7 如有需要，下载用于解密重签名规则的 CA 证书并将其上传到客户端工作站上的浏览器。

有关下载证书并将其分发给客户端的信息，请参阅为解密重签名规则下载 CA 证书，第 18 页。

步骤 8 定期更新重新和已知密钥证书。

- 重签名证书 - 在证书过期之前更新此证书。如果通过 设备管理器生成证书，则有效期为 5 年。要检查证书的有效期，请依次选择 **对象** > **证书**，在列表中查找该证书，然后在“操作”列中点击证书的信息图标 ( )。“信息”对话框显示有效期和一些其他属性。此外，也可从此页面上传替换证书。
- 已知密钥证书 - 对于任何已知密钥解密规则，需要确保已上传目标服务器的当前证书和密钥。只要所支持的服务器上的证书和密钥发生更改，就必须上传新的证书和密钥（作为内部证书）并更新 SSL 解密设置，以使用新证书。

步骤 9 上传外部服务器缺失的受信任 CA 证书。

系统包含各种由第三方颁发的受信任根证书和中间证书。为解密重签名规则协商威胁防御和目标服务器之间的连接时，需要这些证书。

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。在**对象 (Objects)** > **证书 (Certificates)** 页面上上传证书。请参阅上传受信任的 CA 证书。

配置 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

注释 VPN 隧道在 SSL 解密策略评估之前已解密，因此该策略永远不适用于隧道本身。但是，隧道内的任何加密连接都要通过 SSL 解密策略进行评估。

以下程序介绍了如何配置 SSL 解密策略。有关创建和管理 SSL 解密的端到端流程说明，请参阅如何实施和维护 SSL 解密策略，第 5 页。

开始之前

SSL 解密规则表包含两个部分：

- **身份策略主动身份验证规则** - 如果启用身份策略并创建使用主动身份验证的规则，系统将自动创建使这些策略生效所需的 SSL 解密规则。这些规则始终在您自己创建的 SSL 解密规则之前进行评估。只可通过更改身份策略来间接更改这些规则。
- **SSL 本机规则** - 这些是已经配置的规则。只能将规则添加到此部分。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

如果尚未启用该策略，请点击**启用 SSL 解密**并按启用 SSL 解密策略，第 8 页中的说明配置策略设置。

步骤 2 配置策略的默认操作。

最安全的选择是**不解密**。有关详细信息，请参阅配置默认 SSL 解密操作，第 9 页。

步骤 3 管理 SSL 解密策略。

在配置 SSL 解密设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要禁用该策略，请点击 **SSL 解密策略**开关。可以通过点击**启用 SSL 解密**重新启用该策略。
- 要编辑策略设置（包括策略中使用的证书列表），请点击 **SSL 解密设置** 按钮 (); 请参阅 配置 SSL 解密设置，第 16 页。此外，还可以下载与解密重签名规则一起使用的证书，以便将其分发给客户端。请参阅以下主题：
  - 为已知密钥和重签解密配置证书，第 16 页
  - 为解密重签名规则下载 CA 证书，第 18 页
- 要配置规则，请执行以下操作：
  - 要创建新规则，请点击 + 按钮。请参阅配置 SSL 解密规则，第 10 页。
  - 要编辑现有规则，请点击该规则的编辑图标 ()（在“操作”列中）。也可以选择在表中点击某规则属性来编辑该属性。

- 要删除不再需要的规则，请点击该规则的删除图标 ( )（在“操作”列中）。

- 要移动规则，请编辑规则并从**顺序**下拉列表中选择新位置。
- 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。

启用 SSL 解密策略

在可以配置 SSL 解密规则之前，必须启用该策略并配置一些基本设置。以下程序介绍了如何直接启用该策略。此外，还可在启用身份策略时启用该策略。身份策略要求启用 SSL 解密策略。

开始之前

如果从未设置 SSL 解密策略的版本进行升级，但已使用主动身份验证规则配置身份策略，则 SSL 解密策略已启用。确保已选择要使用的解密重签名证书，并且可以选择启用预定义规则。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

步骤 2 点击**启用 SSL 解密 (Enable SSL Decryption)** 配置策略设置。

- 如果是第一次启动该策略，系统将打开“SSL 解密配置”对话框。继续进行后续步骤。
- 如果已对策略进行过一次配置然后禁用了策略，则只需使用之前的设置和规则即可再次启动该策略。可以点击 **SSL 解密设置 (SSL Decryption Settings)** 按钮 ( ) 并按照为已知密钥和重签解密配置证书，第 16 页中所述的方式配置设置。

步骤 3 在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击下载按钮 ( ) 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书，第 18 页。

步骤 4 （可选。）点击**受信任 CA 证书**下的 **+**，并选择您希望策略信任的证书或证书组。

默认组 Cisco-Trusted-Authorities 包括所有系统定义的受信任 CA 证书。如果您已上传其他证书，则可以在此处添加这些证书，或者将其收集到您自己的组中并在此处选择该组。您可以替换 Cisco-Trusted-Authorities 组，也可以直接添加组。系统将提示用户接受其列表中未显示证书签名机构的任何站点的证书：系统不会仅仅因为证书不受信任而阻止访问此类站点。

如果将列表留空或仅选择空证书组，则 SSL 解密策略将信任所有证书。

步骤 5 选择初始 SSL 解密规则。

系统包含可能对您有用的下列预定义规则：

- **Sensitive_Data** - 该规则不对与金融服务和医疗 URL 类别（包括银行、医疗服务等）网站匹配的流量进行解密。必须启用 URL 许可证才能实现该规则。

步骤 6 点击**启用 (Enable)**。

配置默认 SSL 解密操作

如果加密连接没有匹配特定 SSL 解密规则，则由 SSL 解密策略的默认操作来处理。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

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。

- **不解密** - 允许加密连接。然后，访问控制策略将评估加密连接，并根据访问控制规则丢弃或允许该连接。
- **阻止** - 立即丢弃连接。连接将不传递到访问控制策略。

步骤 4 （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。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
  - **将连接事件发送到** - 如果要将事件副本发送至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。

- **无日志记录** - 不生成任何事件。

步骤 5 单击**保存**。

配置 SSL 解密规则

使用 SSL 解密规则确定如何处理加密连接。SSL 解密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。

只可在“SSL 本机规则”部分创建和编辑规则。

注释 在 SSL 解密策略评估连接之前，系统将对 VPN 连接（站点间和远程访问）流量进行解密。因此，SSL 解密规则永远不会应用于 VPN 连接，且在创建这些规则时不需要考虑 VPN 连接。但是，系统会对 VPN 隧道中使用的所有加密连接进行评估。例如，SSL 解密规则将对通过 RA VPN 连接到内部服务器的 HTTPS 连接进行评估，即使 RA VPN 隧道本身没有接受评估（原因在于其已解密）。

开始之前

如要创建解密已知密钥规则，请确保上传目标服务器的证书和密钥（作为内部证书），并编辑 SSL 解密策略设置，以使用该证书。已知密钥规则通常在该规则目标网络条件中指定目标服务器。有关详细信息，请参阅为已知密钥和重签解密配置证书，第 16 页。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

如果未配置任何 SSL 解密规则（不是为主动身份验证的身份规则自动生成的规则），可以点击**添加预定义规则**来添加预定义规则。系统将提示您选择所需的规则。

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。

只可将规则插入 **SSL 本机规则**部分。身份策略主动身份验证规则将根据身份策略自动生成并且为只读形式。

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。

有关每个选项的详细讨论，请参阅下列内容：

- 解密重签名，第 2 页
- 解密已知密钥，第 3 页
- 不解密，第 3 页
- 阻止，第 3 页

步骤 6 使用以下选项卡的任意组合，定义流量匹配标准：

- **源/目标** - 流量通过的安全区（接口）、IP 地址或该 IP 地址的国家/地区或大洲（地理位置）或者流量中使用的 TCP 端口。默认设置为任何区域、地址、地理位置和 TCP 端口。请参阅 SSL 解密规则的源/目标条件，第 12 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。默认设置为任何加密应用。请参阅 SSL 解密规则的应用标准，第 13 页。
- **URL** - Web 请求的 URL 类别。默认情况下，进行匹配时不考虑 URL 类别和信誉。请参阅 SSL 解密规则的 URL 标准，第 14 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 SSL 解密规则的用户条件，第 14 页。
- **高级** - 从连接中使用的证书派生的特性，例如 SSL/TLS 版本和证书状态。请参阅 SSL 解密规则的高级条件，第 15 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 SSL 解密规则中添加条件时，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，可以使用单一规则来基于 URL 类别对流量进行解密。
- 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。
- 匹配 URL 类别需要 URL 过滤许可证。

步骤 7 （可选。）针对规则配置日志记录。

对于与控制面板或事件查看器中包括的规则匹配的流量，必须为其启用日志记录。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
  - **将连接事件发送到** - 如果要将事件副本发送至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。

- **无日志记录** - 不生成任何事件。

步骤 8 点击**确定 (OK)**。

SSL 解密规则的源/目标条件

SSL 解密规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的 TCP 端口。默认设置为任何区域、地址、地理位置、协议和任何 TCP 端口。TCP 是与 SSL 解密规则匹配的唯一协议。

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，如果要确保从外部主机到内部主机的所有流量均被解密，则应将外部区域选为**源区域**，并将内部区域选为**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。

注释 对于解密已知密钥规则，请选择使用目标服务器 IP 地址的对象（该对象使用您上传的证书和密钥）。

- **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。

源端口、目标端口/协议

定义流量中所用协议的端口对象。仅可指定用于 SSL 解密规则的 TCP 协议和端口。

- 要匹配来自 TCP 端口的流量，请配置**源端口**。
- 要匹配流向 TCP 端口的流量，请配置**目标端口/协议**。
- 要同时匹配来自特定 TCP 端口的流量和流向特定 TCP 端口的流量，请配置源端口和目标端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

SSL 解密规则的应用标准

SSL 解密规则的应用标准定义 IP 连接中使用的应用，或定义按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认为任何具有 SSL 协议标记的应用。您无法将 SSL 解密规则与任何未加密应用相匹配。

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 SSL 解密规则，用于解密或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意一个，系统会解密或阻止会话。

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，高风险应用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。

有关应用标准以及如何配置高级过滤器和选择应用的更多信息，请参阅配置应用过滤器对象。

在 SSL 解密规则中使用应用标准时，请考虑以下提示。

- 系统可以识别使用 StartTLS 进行加密的未加密应用。这包括诸如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS 之类的应用。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使用者可分辨名称值来识别某些加密应用。
- 仅在服务器证书交换后，系统才可识别使用。如果在 SSL 握手期间交换的流量与包含应用条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许完成握手，以便可以识别应用。在系统完成其识别后，系统将 SSL 规则操作应用于与其应用条件相匹配的剩余会话流量。
- 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。

SSL 解密规则的 URL 标准

SSL 解密规则的 URL 标准定义了 Web 请求中的 URL 所属的类别。还可以指定要解密、阻止或允许不解密的站点的相对信誉。默认不基于 URL 类别匹配连接。

例如，您可以阻止所有加密的赌博网站，或解密不受信任社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止或解密。有关 URL 类别匹配的详细信息，请参阅按照类别和信誉过滤 URL。

“类别”选项卡

点击 **+**，选择所需的类别，然后点击**确定**。点击类别或对象的 **x**，可将其从策略中删除。

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**复选框，然后使用**信誉**滑块选择信誉级别。信誉滑块的左侧指明待允许而不解密的站点，右侧是要解密或阻止的站点。如何使用信誉取决于规则操作：

- 如果该规则解密或阻止连接，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，如果配置规则以解密或阻止**问题站点**（第 2 级），系统还会自动解密或阻止**不受信任**（第 1 级）站点。
- 如果规则允许连接而不解密（不解密），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，如果配置规则不解密**可靠站点**（第 4 级），该规则还会自动不解密**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。

SSL 解密规则的用户条件

SSL 解密规则的“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，您可以创建规则，对从外部网络发往工程组的流量进行解密，并单独创建一个不会对从该组传出的流量进行解密的规则。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解密处理。

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用户或用户组。点击用户或组对应的 **x**，或将其从策略中移除。

- **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。

SSL 解密规则的高级条件

高级流量匹配标准与根据连接中使用的证书派生的属性有关。您可以配置以下任何或全部选项。

证书属性

如果流量与任何选定属性匹配，则它与相应规则的证书属性选项匹配。您可以配置以下内容：

证书状态

证书**无效**还是**有效**。如果您不关心证书状态，请选择**任意**（默认）。

如果满足以下所有条件，证书即视为有效，否则视为无效：

- 策略信任颁发证书的 CA。
- 可根据证书的内容对证书的签名进行适当的验证。
- 颁发者 CA 证书存储在策略的受信任 CA 证书列表中。
- 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。

自签名

服务器证书是否包含相同的使用者和颁发者可分辨名称。选择以下一个选项：

- **自签名** - 服务器证书自签名。
- **CA 签名** - 服务器证书由证书颁发机构签名。也就是说，颁发者和使用者不同。
- **任意** - 不考虑按照匹配标准，证书是否为自签名。

支持的版本

要匹配的 SSL/TLS 版本。该规则适用于仅使用任何选定版本的流量。默认设置是所有版本。选项包括： **SSL 3.0**、 **TLS 1.0**、 **TLS 1.1**、 **TLS 1.2**、 **TLS 1.3**。

例如，如果仅希望允许 TLSv1.2/3 连接，则可创建用于更低版本的阻止规则。

您必须使用 Snort 3 才能匹配 TLS 1.3 连接。

使用任何未列出版本（例如 SSL v2.0）的流量均由 SSL 解密策略的默认操作处理。

配置 SSL 解密设置

如果您有任何解密流量的规则，则必须配置证书设置。您还可以修改设置，以更改将解密应用于加密流量的方式。下面的主题介绍了几个选项。

为已知密钥和重签解密配置证书

如果通过重签或使用已知密钥实施解密，则需要确定 SSL 解密规则可以使用的证书。确保所有证书均有效且未过期。

特别是对于已知密钥的解密，需要确保系统拥有要解密连接的各目标服务器的当前证书和密钥。通过解密已知密钥规则，可以使用目标服务器的实际证书和密钥进行解密。因此，必须确保 威胁防御设备始终拥有当前证书和密钥，否则将无法成功解密。

只要在已知密钥规则中更改目标服务器上的证书或密钥，就要上传新的内部证书和密钥。将上述证书作为内部证书（而不是内部 CA 证书）上传。可以在下列程序中上传证书，也可以转到**对象 (Objects)** > **证书 (Certificates)**页面并在此页面中上传。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

步骤 2 点击 **SSL 解密设置**按钮 ( )。

如有必要，请选择 **基本** 选项卡。

步骤 3 在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击下载按钮 ( ) 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书，第 18 页。

步骤 4 对于使用已知密钥解密的每条规则，上传目标服务器的内部证书和密钥。

a) 点击**解密已知密钥证书**下的 +。

b) 选择内部身份证书，或点击**创建新的内部证书**以便立即上传。

c) 点击**确定 (OK)**。

步骤 5 （可选。）点击**受信任 CA 证书**下的 +，并选择您希望策略信任的证书或证书组。

默认组 Cisco-Trusted-Authorities 包括所有系统定义的受信任 CA 证书。以下是您可能希望更改此设置的主要情况：

- 您希望使用不在默认组中的受信任 CA 证书。然后，您可以在 SSL 解密策略设置中选择默认组和新组。如果您已上传其他受信任 CA 证书，可以执行此操作。
- 您希望使用的受信任 CA 证书列表比默认组中限制更严格。然后，您将创建一个具有受信任证书的完整列表（而不只是您所增加的受信任证书）的组，并将其选择为 SSL 解密策略设置中的唯一组。

系统将提示用户接受其列表中未显示证书签名机构的任何站点的证书：系统不会仅仅因为证书不受信任而阻止访问此类站点。

如果将列表留空或仅选择空证书组，则 SSL 解密策略将信任所有证书。

步骤 6 单击**保存**。

配置高级和无法解密的流量设置

如果不想使用默认行为，可以配置高级解密设置和无法解密的流量的设置。

过程

步骤 1 选择 **策略 > SSL 解密**。

步骤 2 点击 **SSL 解密设置**按钮 ( )。

步骤 3 在 **高级** 选项卡上，选择是否启用 **TLS 1.3 解密**。

如果启用 TLS 1.3 解密，则还必须在应用于 TLS 1.3 的每个规则的高级选项卡上选择 TLS 1.3 选项。您必须运行 Snort 3 才能解密 TLS 1.3。

步骤 4 在**无法解密的操作**选项卡上，修改系统处理与实施解密的规则匹配的连接的方式，但对于连接无法解密的情况。

默认设置是对这些连接应用与默认操作相同的操作。例外情况是解密错误，您可以选择阻止或仅阻止并重置。

有关这些类别的说明，请参阅处理不可解密流量，第 4 页。

步骤 5 点击**确定 (OK)**。

为解密重签名规则下载 CA 证书

如果决定对流量进行解密，则用户必须拥有加密流程中使用的内部CA证书，该证书由使用TLS/SSL的应用中被定义为受信任根证书颁发机构所颁发。通常，当生成证书或即使导入证书后，证书不会立即在这些应用中定义为受信任。默认情况下，在大多数网络浏览器中，当用户发送 HTTPS 请求时，他们将看到一条来自客户端应用的警告消息，告知他们网站的安全证书有问题。通常，错误消息表明网站的安全证书并非由受信任证书颁发机构所颁发或网站由未知机构所认证，但该警告可能还表明可能存在中间人攻击。一些其他客户端应用不会向用户显示此警告消息，也不允许用户接受无法识别的证书。

可以通过以下方式为用户提供所需的证书：

通知用户接受根证书

可以通知您组织中的用户，告知其公司的新策略并指示其接受组织提供的根证书作为受信任来源。用户应接受该证书并将其保存在受信任根证书颁发机构存储区，以确保在下次访问该站点时系统不会再次提示。

注释 用户需要接受并信任创建替换证书的 CA 证书。如果仅信任替换服务器证书，用户访问各个不同 HTTPS 站点时将继续看到警告。

将根证书添加到客户端设备

能够以受信任根证书颁发机构身份将根证书添加到网络上的所有客户端设备。这样，客户端应用将自动接受包含根证书的事务。

可以通过以下方式向用户提供证书：通过邮件发送或将其放在共享站点上，将证书整合到企业工作站映像中并使用应用更新工具将其自动分发给用户。

以下程序介绍了如何下载内部 CA 证书并将其安装在 Windows 客户端上。

过程

步骤 1 从 设备管理器下载证书。

a) 选择 **策略** > **SSL 解密**。

b) 点击 **SSL 解密设置**按钮 ( )。

c) 点击**下载**按钮 ( )。

d) 选择一个下载位置，或者更改文件名（但是不要更改扩展名），然后点击**保存 (Save)**。

此时可以取消“SSL 解密设置”对话框。

步骤 2 在客户端系统上，在网络浏览器的受信任根证书颁发机构存储区安装证书，或向客户端提供证书，以便用户自行安装。

该流程因操作系统和浏览器类型的不同而不同。例如，对于 Windows 上运行的 Internet Explorer 和 Chrome 浏览器，可以采用以下流程。（对于 Firefox，请依次选择**工具 (Tools)** > **选项 (Options)** > **高级 (Advanced)** 页面，进行安装。）

a) 从**开始**菜单中，依次选择**控制面板** > **Internet 选项**。
b) 选择**内容**选项卡。
c) 点击**证书**按钮，打开“证书”对话框。
d) 选择**受信任根证书颁发机构**选项卡。
e) 点击**导入**，然后根据向导找到并选择下载的文件 (<uuid>_internalCA.crt) 并将其添加到受信任根证书颁发机构存储区。
f) 点击**完成**。

系统应显示消息，指示已成功导入。您可能会看到一个中间对话框，警告：如果生成自签名证书而不是从知名第三方证书颁发机构获取证书，则 Windows 无法验证该证书。

此时，可以关闭“证书”和“Internet 选项”对话框。

示例：从网络阻止较旧的 SSL/TLS 版本

某些组织需要通过政府法规或公司策略来阻止使用较旧版本的 SSL 或 TLS。可以使用 SSL 解密策略来阻止使用您禁止的 SSL/TLS 版本的流量。请考虑将此规则置于 SSL 解密策略的顶部，以确保立即捕获禁止的流量。

以下示例阻止所有 SSL 3.0 和 TLS 1.0 连接。

开始之前

此过程假定已启用 SSL 解密策略，如启用 SSL 解密策略，第 8 页中所述。

过程

步骤 1 依次选择**策略** > **SSL 解密**。

步骤 2 点击 **+** 按钮创建新规则。

步骤 3 按顺序选择 **1** 将规则置于策略的顶部，或选择最适合您网络的数字。

默认情况下，会将该规则添加到策略的末尾。

步骤 4 在**标题**中，输入规则名称，例如，Block_SSL3.0_and_TLS1.0。

步骤 5 在**操作**中，选择**阻止**。这将立即丢弃与该规则匹配的任何流量。

步骤 6 保留以下选项卡上所有选项的默认值：**源/目标**、**应用**、 **URL** 和 **用户**。

步骤 7 点击 **高级** 选项卡，并在 **受支持版本**下，选择 SSL 3.0 和 TLS 1.0，但取消选中 TLS1.1、TLS1.2、TLS 1.3。

步骤 8 （可选）如果希望控制面板和事件反映阻止连接，请点击**日志记录**选项卡并选择**在连接结束时**。如果正在使用外部系统日志服务器，还可以选择该服务器。

步骤 9 点击**确定**。

您现在可以部署策略。部署后，通过系统的任何 SSL 3.0 或 TLS 1.0 连接均将弃用。

注释 SSL 2.0 连接由策略的默认操作处理。如果要确保已弃用这些，请将默认操作更改为阻止。

下一步做什么

如果实施此规则，我们具有以下建议：

- 对于任何类型的解密规则，请包括“高级”选项卡的默认设置，其中，所有 SSL/TLS 选项均已选中。通过应用至所有版本，可以简化握手过程。但是，您的初始阻止规则仍将阻止 SSL 3.0 和 TLS 1.0 连接。
- 通常建议使用“不解密”作为策略的默认操作。但是，由于 SSL 2.0 连接始终由默认操作处理，因此您可能希望改用“阻止”。但是，如果要将“不解密”应用为所有可解密流量的默认操作，请在策略末尾创建“不解密”规则，其中，您接受所有流量匹配条件的默认值。此规则将匹配与表中的较早规则不匹配的任何受支持 TLS 连接，并作为这些 TLS 版本的默认值。

SSL 解密监控和故障排除

以下主题介绍如何对 SSL 解密策略进行监控和故障排除。

监控 SSL 解密

您可以在控制面板和事件中查看有关匹配日志记录已启用的规则（或默认操作）的流量解密信息。

SSL 解密控制面板

要评估整体解密统计信息，请查看**监控** > **SSL 解密**控制面板。控制面板显示以下信息：

- 加密流量与纯文本流量百分比。
- 按照 SSL 规则的流量解密百分比。

事件

除了控制面板，事件查看器（**监控** > **事件**）包括加密流量 SSL 信息。以下是评估事件的一些提示：

- 对于因匹配阻止匹配流量的 SSL 规则（或默认操作）而被丢弃的连接，**操作**应为“阻止”，**原因**应指示“SSL 阻止”。
- **SSL 实际操作**字段指示系统应用于连接的实际操作。这可能与 **SSL 预期操作**有所不同，SSL 预期操作指示在匹配规则上定义的操作。例如，连接可能与应用解密的规则匹配，但出于某些原因不能被解密。

处理解密重签名适用于浏览器而非应用的 Web 站点（SSL 或证书颁发机构锁定）

智能手机和其他设备的某些应用使用 SSL（或证书颁发机构）锁定技术。SSL 锁定技术将原始服务器证书的散列值嵌入到应用本身内部。因此，当应用收到来自 威胁防御设备的重签名证书时，散列验证会失败并中止连接。

主要表现是，用户使用站点应用无法连接到网站，但可以使用网络浏览器连接，即使在应用无法正常工作的同一台设备上使用浏览器也可以连接。例如，用户不能使用 Facebook iOS 或 Android 应用，但可以通过 https://www.Facebook.com 转至 Safari 或 Chrome，进行成功连接。

由于 SSL 锁定专用于避免中间人攻击，因此此问题无法解决。必须从以下选项中选择一项：

- 支持应用用户，在这种情况下无法解密流向网站的任何流量。为站点应用创建“Do Not Decrypt”规则（在 SSL 解密规则的“应用”选项卡上），并确保该规则排在应用于连接的任何解密重签名规则前面。
- 强制用户只使用浏览器。如果必须解密流向网站的流量，需要向用户说明，通过您的网络连接时，他们无法使用站点应用，只能使用浏览器。

更多详细信息

如果站点在浏览器中可用，但不能在同一设备的应用中使用，几乎可以肯定这是一个 SSL 锁定实例。但是，如果您想要更深入地挖掘，除了浏览器测试之外，还可以使用连接事件确定 SSL 锁定。

应用可能会通过两种方式处理散列验证失败：

- 第 1 组应用，例如 Facebook，从服务器收到 SH、CERT、SHD 消息后立即发送 SSL 警告消息。警告通常是一个表示 SSL 锁定的“Unknown CA (48)”警告。紧接着警告消息发送 TCP 重置。在事件详细信息中，您应看到以下现象：
  - SSL 流标志包括 ALERT_SEEN。
  - SSL 流标志不包括 APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE。
- 第 2 组应用，例如 Dropbox，不会发送任何警告。而是，等到完成握手后发送 TCP 重置。在事件中，您应看到以下现象：
  - SSL 流标志不包括 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。

- SSL 流消息通常是：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。

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。