解密策略

以下主题概述解密策略的创建、部署、管理和日志记录。

关于解密策略

A 解密策略 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 解密策略，将 a 解密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托管设备。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 解密策略将接管、处理和解密已加密的流量。

使用向导创建解密策略

您可以使用向导创建以下类型的解密策略：

- 出站保护（**解密 - 重新签名** 规则操作）。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。

  系统同时将三个具有 **不解密** 操作的规则添加到策略中，省去了以后再添加的麻烦。这些规则对应于您在创建策略时配置的任何解密排除项（例如，对于已知使用证书锁定的应用，您可以选择绕过解密。

  有关详细信息，请参阅创建具有出站连接保护的解密策略。

- 入站保护（**解密 - 已知密钥** 规则操作）。您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。

同时将三个具有**不解密**操作的规则添加到策略中，但默认情况下会禁用这些规则。这些规则对应于您在创建策略时配置的任何解密排除项（例如，对于已知使用证书锁定的应用，您可以选择绕过解密。

有关详细信息，请参阅 创建具有入站连接保护的旧版解密策略。

- 任何其他解密规则操作（例如阻止或监控）。

  有关详细信息，请参阅创建具有其他规则操作的解密策略，第 15 页。

向导会自动为您指定的每个证书创建单独的规则。例如，入站保护规则可能为传入财务部门内部网络的流量指定一个证书，为传入工程网络的流量指定另一个证书。

该向导会为出站和入站保护策略创建其他规则，如下所示：

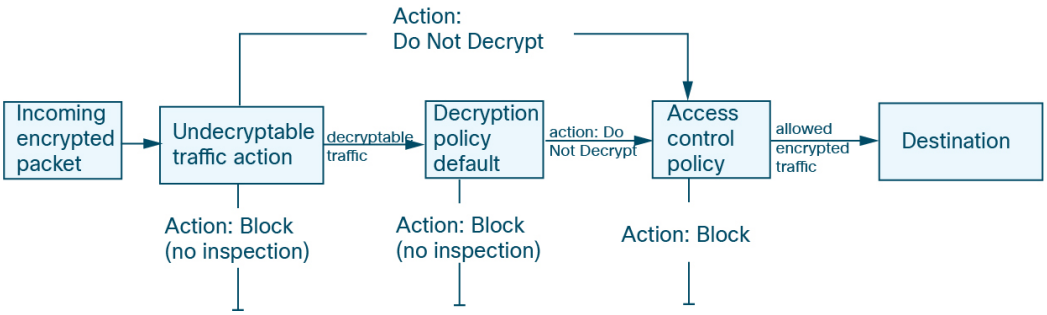
- 出站保护（**解密 - 重新签名** 规则操作）：向导为匹配您在向导中指定的例外的流量创建“不解密”规则。例如，您可以选择不解密来自无法解密的应用的流量，通常是使用证书锁定的应用。

  不解密规则放置在解密策略的第一个位置，以便流量通过防火墙时以最少的处理方式传输。

- 入站保护（**解密 - 已知密钥** 规则操作）：该向导不允许您选择任何例外，但它会将“不解密”规则添加到策略中并禁用它们；这样，您可以在以后需要时启用这些例外。

不解密策略示例

以下是具有**不解密 (Do Not Decrypt)** 规则操作的解密策略示例：



最简单的 解密策略（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。

要开始使用，请参阅 创建解密策略，第 3 页

解密策略 的要求和前提条件

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

创建解密策略

您可以创建以下任何类型的解密策略：

- 出站保护 策略具有保护出站连接的规则；也就是说，目标服务器位于受保护的网络外。此类规则具有 **解密 - 重新签名** 规则操作。我们还使用 **“不解密”** 操作创建其他规则，排除您指定的流量（例如使用证书锁定的流量）。

  请参阅创建具有出站连接保护的解密策略， 第 3 页

- 入站保护 策略具有保护入站连接的规则；也就是说，目标服务器位于受保护的网络内。此类规则具有**解密 - 已知密钥**规则操作。我们还使用 **“不解密”** 操作创建其他规则，排除您指定的流量（例如使用证书锁定的流量）。这些规则最初处于禁用状态，但您可以根据需要在以后修改和启用它们。

  请参阅创建具有入站连接保护的解密策略， 第 6 页

- 其他操作（包括 **“不解密”**、**“ 阻止”**和**“ 阻止并重置”**）。

  请参阅创建具有其他规则操作的解密策略， 第 15 页

创建具有出站连接保护的解密策略

此任务讨论如何使用保护出站连接的规则来创建解密策略；也就是说，目标服务器位于受保护的网络外。此类规则具有 **解密 - 重新签名** 规则操作。

创建解密策略时，您可以同时创建多条规则，包括多条**解密 - 已知密钥**规则、多条**解密 - 替换证书**规则和多条**解密 - 重新签名**规则。

如果启用了变更管理，则必须先创建并分配通知单，然后才能创建解密策略。在使用解密策略之前，必须先批准票证和所有关联对象（如证书颁发机构）。有关详细信息，请参阅创建变更管理故障单和支持变更管理的策略和对象。

开始之前

您必须先上传或生成出站服务器的内部证书颁发机构 (CA)，然后才能创建保护出站连接的解密策略。您可以通过以下任何一种方式执行此操作：

- 通过转至 **对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)** 并引用 PKI 来创建内部 CA 证书对象。
- 在创建此解密策略时。

过程

步骤 1 如果尚未登录，请登录 Cisco Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **访问控制标题** > **解密**。

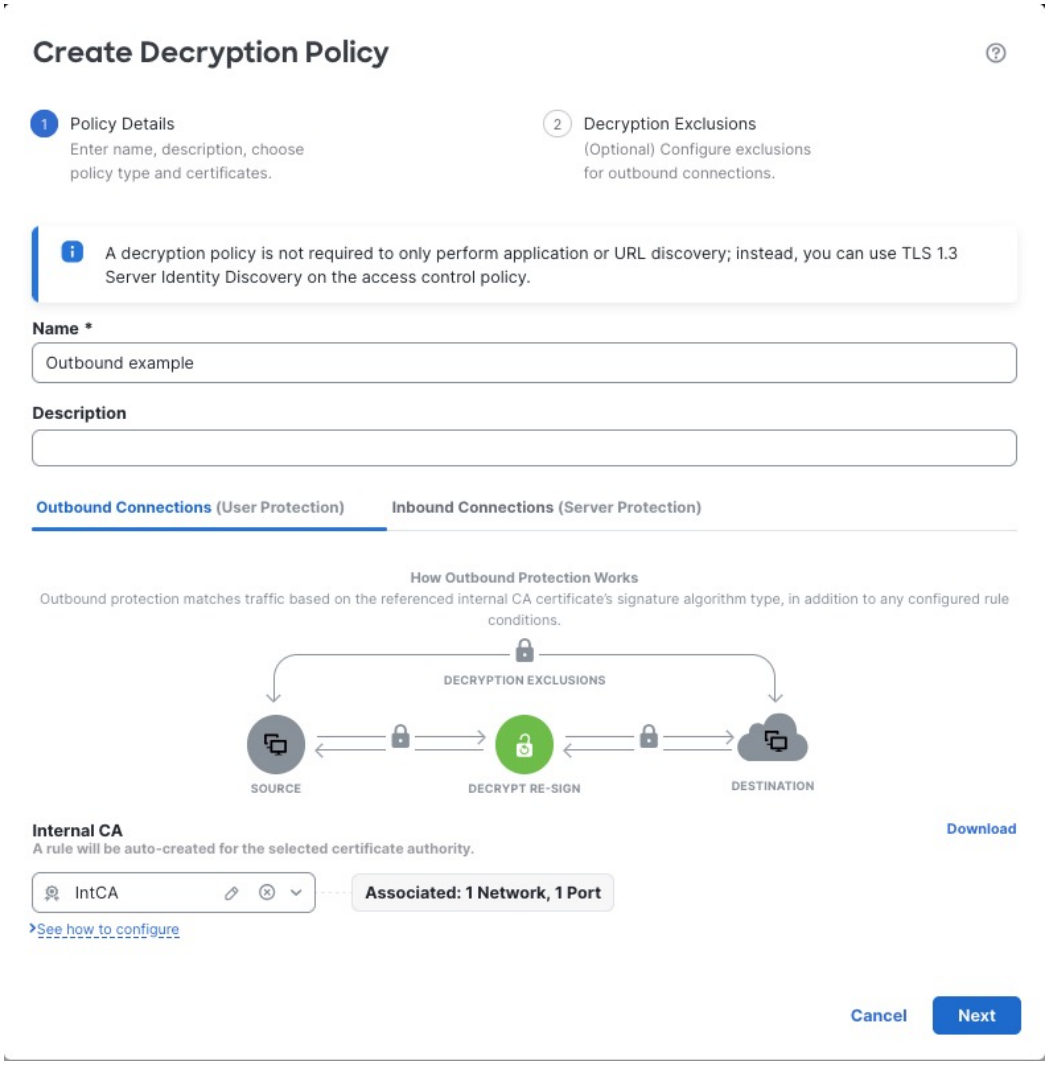
步骤 3 点击**创建解密策略 (Create Decryption Policy)**。

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）。

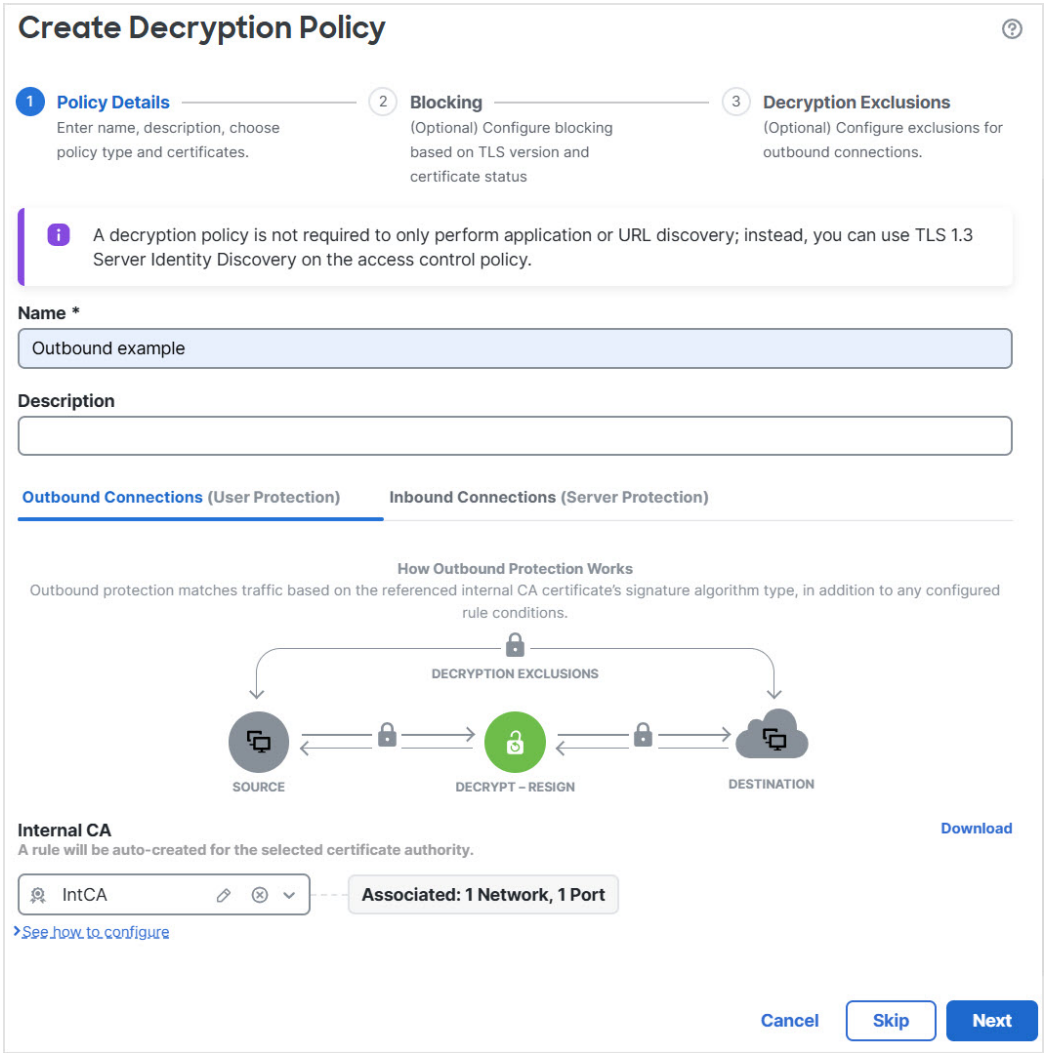
解密策略名称中不支持使用以下字符：

- 前导句点
- `#,;,{,},=,$,<,>`

步骤 5 点击**出站连接 (Outbound Connections)** 选项卡。



步骤 6 点击**出站连接 (Outbound Connections)** 选项卡。



步骤 7 从**内部 CA (Internal CA)** 列表中，上传或选择规则的证书。

有关内部证书的更多信息，请参阅 为出站保护生成内部 CA，第 12 页 和 为出站保护上传内部 CA，第 13 页。

步骤 8 （可选。）选择网络和端口。

了解更多信息：

- 网络规则条件
- 端口规则条件

步骤 9 点击**下一步 (Next)**。

步骤 10 继续执行解密策略阻止连接，第 8 页。

下一步做什么

- 添加规则条件： 解密规则 条件
- 添加默认策略操作： 解密策略 默认操作 ， 第 16 页
- 为默认操作配置日志记录选项，如《Cisco Secure Firewall Management Center 管理指南》 中的使用策略默认操作记录连接所述。
- 设置高级策略属性：解密策略 高级选项 ， 第 19 页。
- 将 解密策略 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；请参阅 部署配置更改。

创建具有入站连接保护的解密策略

此任务讨论如何使用保护入站连接的规则来创建解密策略；也就是说，目标服务器位于受保护的网络内。此类规则具有**解密 - 已知密钥**规则操作。

创建解密策略时，您可以同时创建多条规则，包括多条“**解密 - 已知密钥**”规则和多条“**解密 - 重新签名**”规则。。

开始之前

在创建用于保护入站连接的解密策略之前，可以选择为内部服务器上传内部证书。您可以通过以下任何一种方式执行此操作：

- 通过转至 **对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部证书 (Internal Certs)** 并引用 PKI 来创建内部证书对象。
- 在创建此解密策略时。

如果启用了变更管理，则必须先创建并分配通知单，然后才能创建解密策略。在使用解密策略之前，必须先批准票证和所有关联对象（如证书颁发机构）。有关详细信息，请参阅创建变更管理故障单和支持变更管理的策略和对象。

过程

步骤 1 如果尚未登录，请登录 Cisco Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **访问控制标题** > **解密**。

步骤 3 点击**创建解密策略 (Create Decryption Policy)**。

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）。

解密策略名称中不支持使用以下字符：

- 前导句点
- #,;,{,},=,$,<,>

步骤 5 从**内部证书 (Internal Certificates)** 列表中，上传或选择规则的证书。

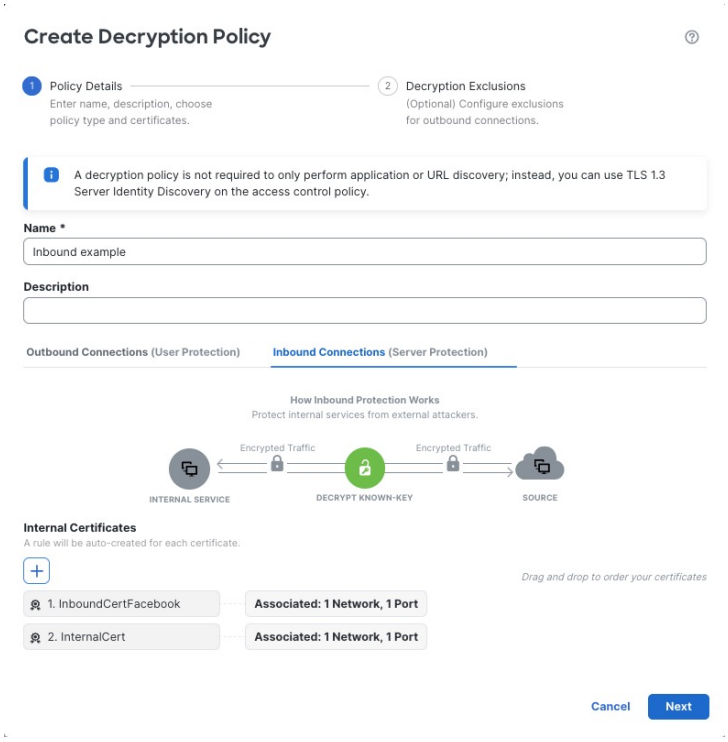
有关内部 CA 证书的详细信息，请参阅内部证书颁发机构对象。

步骤 6 （可选。）选择网络和端口。

了解更多信息：

- 网络规则条件
- 端口规则条件

步骤 7 点击**入站连接 (Inbound Connections)** 选项卡。



步骤 8 点击**下一步 (Next)**。

步骤 9 继续执行 解密策略阻止连接， 第 8 页

步骤 10 继续执行解密策略排除项， 第 8 页。

下一步做什么

- 添加规则条件： 解密规则 条件
- 添加默认策略操作： 解密策略 默认操作， 第 16 页
- 为默认操作配置日志记录选项，如中的 使用策略默认操作记录连接《Cisco Secure Firewall Management Center 管理指南》所述。

- 设置高级策略属性：解密策略 高级选项， 第 19 页。
- 将 解密策略 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；请参阅 部署配置更改。

解密策略阻止连接

此主题提供以下详细信息：如何在创建解密策略时阻止与 TLS 版本和服务器证书状态不安全的服务器连接。您的解密策略中创建默认禁用的 **阻止并重置 (Block with Reset)** 规则。

过程

步骤 1 完成以下提到的任务：

- 创建具有出站连接保护的解密策略， 第 3 页
- 创建具有入站连接保护的解密策略， 第 6 页

步骤 2 **阻止 (Blocking)** 页面提供以下选项。默认情况下，会为解密策略操作禁用所有选项。

- **基于 TLS 版本阻止连接 (Block connections based on TLS version)** - 选中此复选框可阻止与使用不安全 TLS 版本的服务器的连接。默认情况下，系统会选择已知易受攻击的 **SSL v3.0**、**TLS v1.0** 和 **TLS v1.1**。您可以从下拉列表中选择其他版本。
- **基于服务器证书状态阻止连接 (Block connections based on server certificate status)** - 选中此复选框可阻止与服务器证书状态为不安全的服务器的连接。默认情况下，**无效签名 (Invalid Signature)**、**过期 (Expired)**、**尚未生效 (Not Yet Valid)** 和**无效证书 (Invalid Certificate)** 处于选中状态。您可以从下拉列表中选择其他状态。

点击 **删除** (✕) 以删除选择，或点击**重置为默认值 (Reset to default)** 恢复为默认选择。

步骤 3 点击**下一步 (Next)**。

下一步做什么

继续执行解密策略排除项， 第 8 页。

解密策略排除项

此任务讨论如何将某些类型的流量排除在解密之外。虽然最初仅为出站解密策略（即，使用**解密 - 重新签名**策略操作的策略）启用这些规则，但我们会在解密策略中为这些策略创建**不解密**规则。

开始之前

您必须先上传出站服务器的内部证书颁发机构(CA)，然后才能创建保护出站连接的解密策略。您可以通过以下任何一种方式执行此操作：

- 通过转至 **对象 (Objects)** > **对象管理 (Object Management)** > **PKI** > **内部 CA (Internal CAs)** 并引用 PKI 来创建内部 CA 证书对象。
- 在创建此解密策略时。

过程

步骤 1 完成以下讨论的任务：

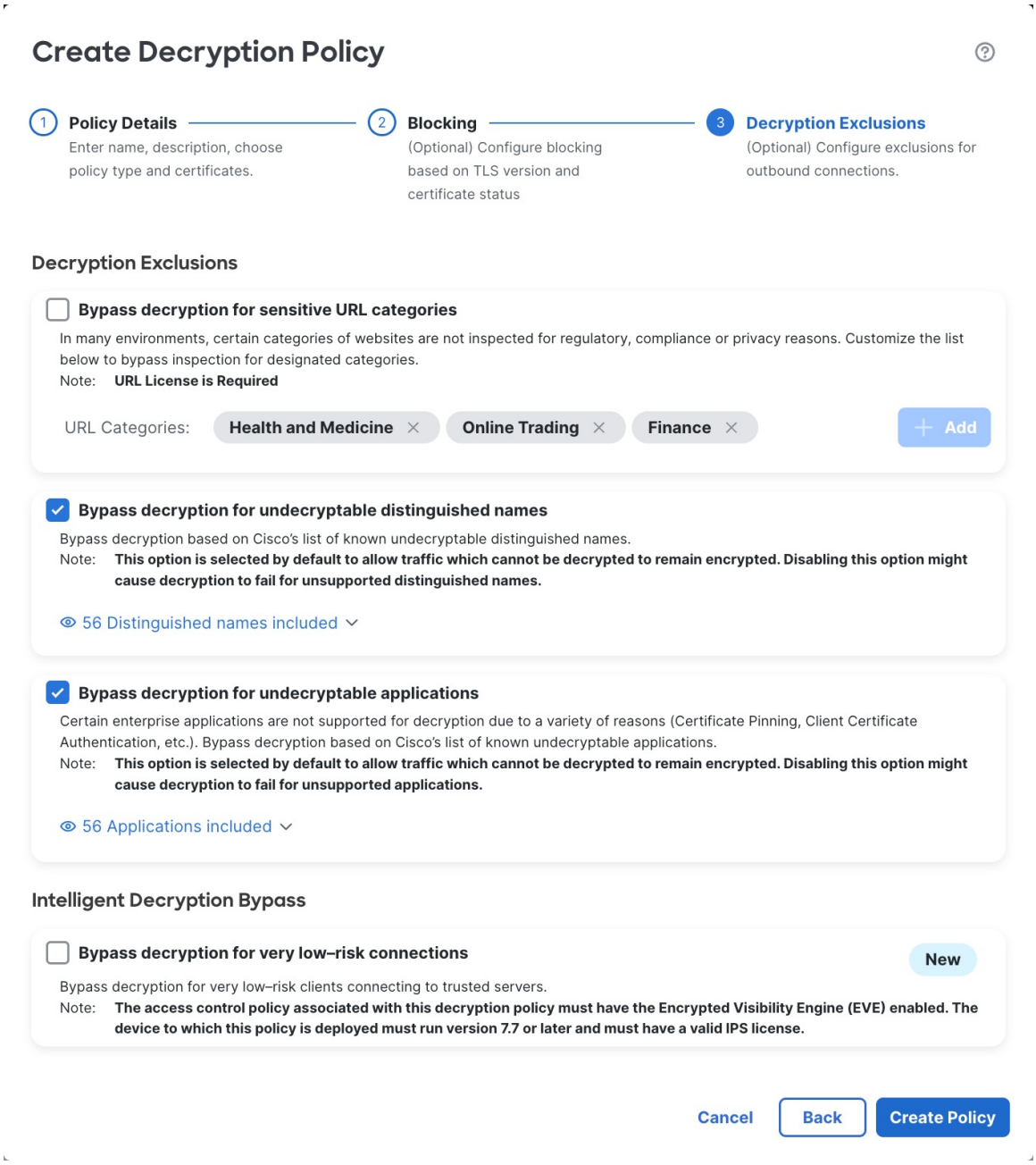
- 创建具有出站连接保护的解密策略， 第 3 页
- 有关详细信息，请参阅创建具有入站连接保护的解密策略， 第 6 页

步骤 2 排除项页面提供以下选项。为出站保护策略（**解密 - 重新签名**规则操作）启用 所有选项，并为所有其他解密策略操作禁用所有选项。

项目	说明
绕过解密敏感 URL 类别	选中此复选框可不解密来自指定类别的流量。根据您所在地区的法律，可能会禁止解密某些流量，例如与金融或健康相关的流量。有关详细信息，请咨询您所在地区的权威机构。 点击**添加 (Add)** 以添加更多类别。 点击 **删除** (✕) 以删除类别。
绕过对不可解密的可分辨名称的解密	选中此复选框可在重新签名证书可能导致连接失败时不解密流量。通常，此行为与证书锁定相关，《TLS/SSL 证书固定准则的证书锁定准则中对此进行了讨论。 无法解密的可分辨名称列表由思科维护。
绕过解密无法解密的应用	选中此复选框可在重新签名证书可能导致连接失败时不解密流量。 通常，此行为与证书锁定相关，《TLS/SSL 证书固定准则的证书锁定准则中对此进行了讨论。 无法解密的应用会在漏洞数据库 (VDB) 中自动更新。您可以在 Cisco Secure Firewall应用检测器 (Secure Firewall Application Detectors) 页面上找到所有应用的列表；**undecryptable** 标记会标识思科确定为无法解密的应用。 无法解密的应用列表由思科维护。

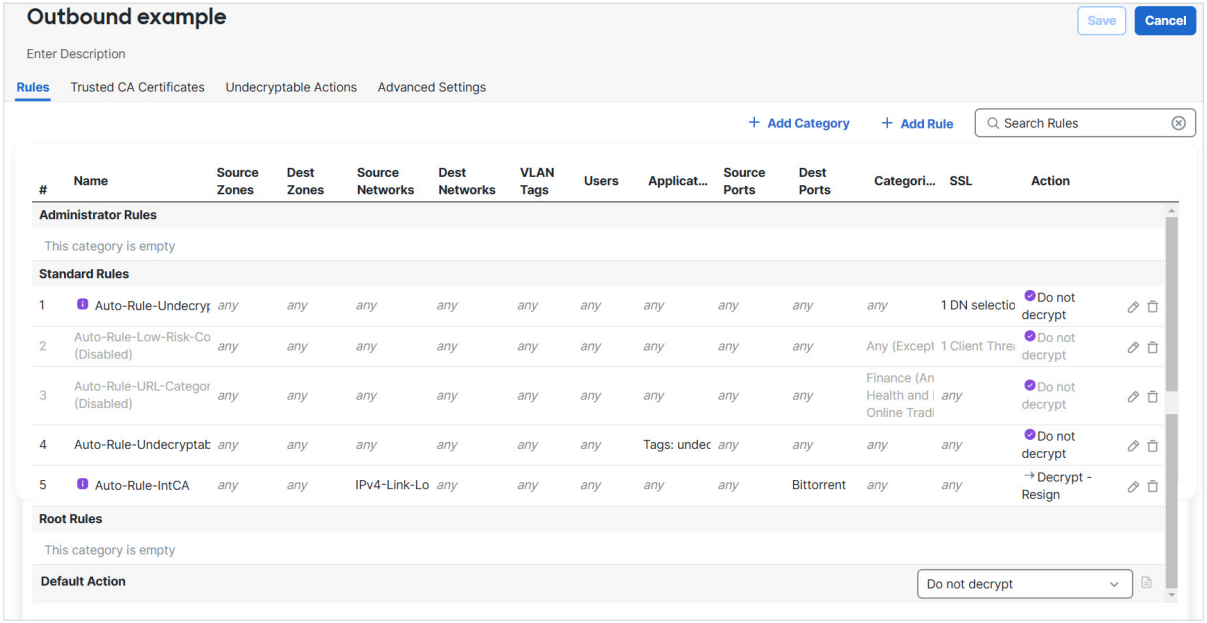
项目	说明
对风险极低的连接绕过解密	选中此复选框，根据客户端的威胁置信度（由加密可见性引擎（EVE）和URL类别声誉决定），不解密连接到受信任服务器的极低风险客户端的流量。在新的解密策略中创建并启用了 **Auto-Rule-Low-Risk-Connections** 不解密规则。 要使用**对风险极低的连接绕过解密**选项，必须在对应地访问控制策略中启用加密可视性引擎 (EVE)，并且托管设备必须使用有效的 IPS 许可证运行版本 7.7 或更高版本。

下图显示了默认选项。



步骤 3 点击**创建策略 (Create Policy)**。

下图显示了出站保护策略示例。



在前面的示例中，与您的规则排除项选择相对应的**不解密**规则会自动添加到**解密 - 重新签名**规则之前。敏感URL类别的规则已被禁用，因为默认情况下，该排除项已被禁用。如果您选中了**绕过敏感 URL 类别的解密 (Bypass decryption for sensitive URL categories)** 复选框，则该规则将被启用。

步骤 4 点击**创建策略 (Create Policy)**。

下一步做什么

- 添加规则条件： 解密规则 条件
- 添加默认策略操作： 解密策略 默认操作 ， 第 16 页
- 为默认操作配置日志记录选项，如《Cisco Secure Firewall Management Center 管理指南》 中的使用策略默认操作记录连接所述。
- 设置高级策略属性：解密策略 高级选项 ， 第 19 页。
- 将 解密策略 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；请参阅 部署配置更改。

为出站保护生成内部 CA

此任务讨论在创建保护出站连接的解密规则时如何选择性地生成内部证书颁发机构。您也可以使用上传为响应 CSR 而颁发的签名证书中所述的**对象** > **对象管理**来执行这些任务。

开始之前

确保您了解生成内部证书颁发机构对象的要求，如内部证书颁发机构对象中所述。

过程

步骤 1 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略** > **访问控制标题** > **解密**。

步骤 3 点击**创建解密策略（旧版）**。

步骤 4 在**名称 (Name)** 字段中输入策略的名称，在**说明 (Description)** 字段中输入可选的描述。

步骤 5 点击**出站连接 (Outbound Connections)** 选项卡。

步骤 6 从**内部 CA (Internal CA)** 列表中，点击**新建 (Create New)** > **生成 CA (Generate CA)**。

步骤 7 为内部 CA 提供一个**名称**，然后提供一个由两个字母组成的**国家/地区名称**。

步骤 8 点击**字签名 (Self-Signed)** 或**CSR**。

有关这些选项的详细信息，请参阅内部证书颁发机构对象。

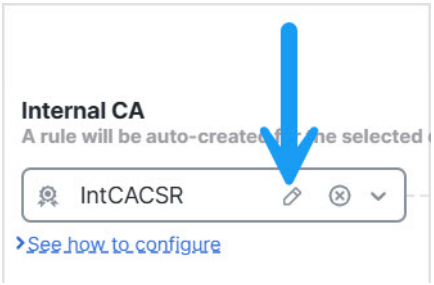
步骤 9 在提供的字段中输入请求的信息。

步骤 10 点击**保存**。

步骤 11 如果您选择了 **CSR**，则在签名请求完成后，点击**安装证书 (Install Certificate)**，如下所示：

a) 重复此程序中的上述步骤。

b) 从**内部 CA (Internal CA)** 列表编辑 CA，如下所示。



c) 点击 **Install Certificate**。

d) 按照屏幕提示完成任务。

步骤 12 按照 创建具有出站连接保护的解密策略，第 3 页中的说明继续创建策略。

为出站保护上传内部 CA

此任务讨论在创建保护出站连接的解密规则时如何选择性地上传内部证书颁发机构。您也可以使用上传为响应 CSR 而颁发的签名证书中所述的**对象** > **对象管理**来执行这些任务。

开始之前

确保您了解生成内部证书颁发机构对象的要求，如内部证书颁发机构对象中所述。

过程

步骤 1 如果尚未登录，请登录 Cisco Secure Firewall Management Center 。
步骤 2 请点击 **策略** > **访问控制标题** > **解密**。
步骤 3 点击**创建解密策略 (Create Decryption Policy)**。
步骤 4 在**名称 (Name)** 字段中输入策略的名称，在**说明 (Description)** 字段中输入可选的描述。
步骤 5 点击**出站连接 (Outbound Connections)** 选项卡。
步骤 6 从**内部 CA (Internal CA)** 列表中，点击**新建 (Create New**） > **上传 CA (Upload CA)**。
步骤 7 为内部 CA 指定一个**名称**。
步骤 8 粘贴或在提供的字段中浏览找到证书及其私钥。
步骤 9 如果 CA 有密码，请选中**已加密 (Encrypted)** 复选框并在相邻字段中输入密码。
步骤 10 按照 创建具有出站连接保护的解密策略， 第 3 页中的说明继续创建策略。

为入站保护上传内部证书

此任务讨论在创建保护出站连接的解密规则时如何上传内部证书颁发机构。您还可以使用**对象** > **对象管理**上传内部 CA，如导入 CA 证书和私钥中所述。

开始之前

确保您具有中内部证书颁发机构对象所讨论的一种格式的内部证书颁发机构。

过程

步骤 1 如果尚未登录，请登录 Cisco Secure Firewall Management Center。
步骤 2 请点击 **策略** > **访问控制标题** > **解密**。
步骤 3 点击**创建解密策略 (Create Decryption Policy)**。
步骤 4 在**名称 (Name)** 字段中输入策略的名称，在**说明 (Description)** 字段中输入可选的描述。
步骤 5 点击**入站连接 (Inbound Connections)** 选项卡。
步骤 6 从 **内部证书** 列表中，点击 **添加** (+)。
步骤 7 点击**上传**。
步骤 8 为内部证书指定一个**名称**。
步骤 9 粘贴或在提供的字段中浏览找到证书及其私钥。
步骤 10 如果证书有密码，请选中 **已加密** 复选框并在相邻字段中输入密码。
步骤 11 按照 创建具有入站连接保护的解密策略， 第 6 页中的说明继续创建解密策略。

创建具有其他规则操作的解密策略

要使用**不解密**、**阻止**、**阻止并重置**或**监控**规则操作来创建解密规则，请创建解密策略并编辑该策略以添加该规则。

创建解密策略时，可以同时创建多个规则，包括多个**解密 - 已知密钥**规则、多个**解密 - 替换证书**规则和多个**解密 - 重新签名**规则。

如果启用了变更管理，则必须先创建并分配通知单，然后才能创建解密策略。在使用解密策略之前，必须先批准票证和所有关联对象（如证书颁发机构）。有关详细信息，请参阅创建变更管理故障单和支持变更管理的策略和对象。

过程

步骤 1 如果尚未登录，请登录 Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略** > **访问控制标题** > **解密**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

解密策略名称中不支持使用以下字符：

- 前导句点
- `#,;,{,},=,$,<,>`

步骤 4 点击**下一步 (Next)**。

步骤 5 旁路页面仅供参考；您无法绕过其他类型解密（如**屏蔽**）的流量。

步骤 6 点击**创建策略 (Create Policy)**。

步骤 7 等待策略创建。

步骤 8 点击解密策略名称旁边的 **编辑** ()。

步骤 9 点击**添加规则**。

步骤 10 为规则 **命名**。

步骤 11 从**操作 (Action)** 列表中，点击规则操作，并参阅以下部分以了解详细信息：

- 解密规则 不解密操作
- 解密规则 阻止操作
- 解密规则 监控操作

步骤 12 点击**保存**。

下一步做什么

- 添加规则条件： 解密规则 条件

- 添加默认策略操作： 解密策略 默认操作 ， 第 16 页
- 为默认操作配置日志记录选项， 如 《Cisco Secure Firewall Management Center 管理指南》 中的使用策略默认操作记录连接 所述。
- 设置高级策略属性：解密策略 高级选项 ， 第 19 页。
- 将 解密策略 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；请参阅 部署配置更改。

解密策略 默认操作

a解密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 解密规则 规则的 a 解密策略时，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。

要设置 解密策略 默认操作：

1. 如果尚未登录，请登录 Cisco Secure Firewall Management Center 。
2. 请点击 **策略** > **访问控制标题** > **解密**。
3. 点击 解密策略名称旁边的 **编辑** (✎) 。
4. 在“默认操作”行中，点击列表中的以下操作之一。

表 *1:* 解密策略 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。

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	会话使用 SSL 版本 2 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
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

类型	说明	默认操作	可用操作
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 a 解密策略时，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，请参阅解密规则 准则和限制。

如果解密策略与使用 TCP 状态绕行的访问控制策略关联，则系统会根据策略为**握手错误**配置的**无法解密的操作**对匹配的流量执行操作。

例如，如果解密策略的**握手错误**被设置为**阻止 (Block)**，则匹配规则的流量会被阻止，并且连接事件的操作会报告为握手错误。

有关 TCP 状态绕行的详细信息，请参阅：

- 配置 TCP 状态绕行
- 绕过非对称路由的 TCP 状态检查（TCP 状态绕行）

相关主题

设置无法解密的流量的默认处理 ， 第 18 页

设置无法解密的流量的默认处理

您可以在解密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 解密规则 的a解密策略 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 解密策略 的默认操作。

过程

步骤 1 如果尚未登录，请登录 Cisco Secure Firewall Management Center 。

步骤 2 请点击 **策略** > **访问控制标题** > **解密**。

步骤 3 点击 解密策略名称旁边的 **编辑** (✎) 。

步骤 4 在 解密策略 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解密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 17 页和解密策略 默认操作，第 16 页。

步骤 6 点击**保存**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；请参阅《Cisco Secure Firewall Management Center 管理指南》。
- 部署配置更改；请参阅 部署配置更改。

解密策略 高级选项

A 解密策略 的 **高级设置 (Advanced Settings)** 页面具有适用于为应用策略的 Snort 3 配置的所有托管设备的全局设置。

在运行以下命令的任何托管设备上，A 解密策略 高级设置都将被忽略：

- 早于 7.1 的版本
- Snort 2

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)。HTTP/3 是 QUIC 传输协议的一部分，而不是 TCP 传输协议。阻止客户端通告 HTTP/3，可以防止可能隐藏在 QUIC 连接中的攻击和规避企图。

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

是否将解密规则应用于 TLS 1.3 连接。如果不启用此选项，则解密规则仅适用于 TLS 1.2 或更低版本的流量。请参阅TLS 1.3 解密最佳实践，第 21 页。

启用自适应 TLS 服务器身份探测

启用 TLS 1.3 解密时自动启用。 探测 是与服务器的部分 TLS 连接，其目的是获取服务器证书并将其缓存。（如果证书已缓存，则永远不会建立探测。）

如果在与解密策略关联的访问控制策略上禁用了 TLS 1.3 服务器身份发现，我们将尝试使用服务器名称指示 (SNI)，这并不可靠。

自适应 TLS 服务器身份探测发生在以下任何情况下，而不是在早期版本中的每个连接上发生：

- 证书颁发者 - 当解密规则的 DN 规则条件中的 **颁发者 DN** 值匹配时匹配。

  有关详细信息，请参阅可分辨名称 (DN) 规则条件。

- 证书状态 - 当解密规则中的任何 **证书状态** 条件匹配时匹配。

  有关详细信息，请参阅证书状态 解密规则 条件。

- 内部/外部证书 - 内部证书可以通过 **解密 - 已知密钥** 规则操作中使用的证书进行匹配；可以在 **证书** 规则条件中匹配外部证书。

  有关详细信息，请参阅已知密钥解密（传入流量）和证书 解密规则 条件。

- 应用 ID - 可以通过访问控制策略或解密策略中的 **应用** 规则条件进行匹配。

  有关详细信息，请参阅应用规则条件。

- URL 类别 - 可以通过访问控制策略中的 **URL** 规则条件进行匹配。

  有关详细信息，请参阅URL 规则条件。

注释 任何部署到 AWS 的设备都不支持启用自适应 TLS 服务器发现模式。Cisco Secure Firewall Threat Defense Virtual如果您有任何由 Cisco Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。

启用 QUIC 解密

是否将解密规则应用于通过 QUIC 协议使用 HTTP/3 的连接。解密 QUIC 连接时，系统可以检查会话内容是否存在入侵、恶意软件或其他问题。您还可以根据访问控制策略中的特定条件来对已解密的 QUIC 连接应用精细控制和过滤。QUIC 支持符合 RFC 9000、9001、9002、9114、9204 的要求。

实施 QUIC 解密时，请考虑以下事项：

- 在 高可用性或集群设备上，QUIC 解密只有在连接保持位于同一节点时才有效。如果对连接进行故障转移或将其转发到另一个节点，则连接会断开，必须重新建立。支持多实例而无限制。
- 适用于 QUIC 流量的规则将包括具有目的端口 443 的 UDP 协议。

- 适用于 QUIC 流量的访问控制规则将包括 HTTP/3 或 QUIC 协议（显式或隐式）。

以下限制适用于 QUIC 解密：

- QUIC 解密仅适用于 7.6+。运行较低版本的设备无法解密 QUIC 连接。
- 无法为出站流量解密来自使用 Chromium 堆栈的浏览器（Google Chrome、Opera 和 Edge）的连接。但可以解密来自相同浏览器的入站流量。
- 不支持 RFC 9000 中所述的连接迁移。QUIC 中的连接 ID 概念允许终端在地址更改时保留相同的连接。
- 不支持密钥更新、会话恢复和 QUIC 版本 2。
- 不支持交互式阻止和交互式阻止并重置（在访问控制规则中）。这些操作将作为“阻止”和“阻止并重置”。
- 每个连接的活动连接 ID 限制为 5。如有必要，您可以使用设备 CLI 中的**system support quic-tuning**和**system support quic-tuning-reset**命令修改这些限制。

TLS 1.3 解密最佳实践

建议：何时启用高级选项

解密策略 和访问控制策略都具有影响流量处理方式的高级选项，无论流量是否被解密。

高级选项包括：

- 解密策略：
  - TLS 1.3 解密
  - TLS 自适应服务器身份探测
- 访问控制策略：TLS 1.3 服务器身份发现

  访问控制策略设置优先于解密策略设置。

使用下表确定要启用的选项：

TLS 自适应服务器身份探测设置（解密策略）	**TLS 1.3** 服务器身份发现设置（访问控制策略）	结果	建议使用条件
已启用	已禁用	如果解密策略包含解密策略 高级选项，第 19 页中指定的任何规则条件 并且服务器证书未被缓存，则发送自适应探测。	• 您未在访问控制规则中使用应用或 URL 条件 • 您正在解密流量
已启用	已启用	如果服务器证书未缓存，则始终发送探测。	仅当访问控制规则具有 URL 或应用条件时使用

TLS 自适应服务器身份探测设置（解密策略）	TLS 1.3 服务器身份发现设置（访问控制策略）	结果	建议使用条件
已禁用	已启用	如果服务器证书未缓存，则始终发送探测。	不推荐。
Disabled	Disabled	从不发送探测。	用途非常有限；仅在不解密流量且不在访问控制规则中使用应用或 URL 条件时使用

注释 缓存的 TLS 服务器证书可用于特定 上的所有 Snort 实例。可以使用 CLI 命令清除缓存，并在设备重新启动时自动清除缓存。

参考

有关详细信息，请参阅 secure.cisco.com 上有关 TLS 服务器身份发现 的讨论。

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。