标准解密 策略

以下主题详细介绍了 标准解密 政策。

关于标准解密策略

我们推荐使用 标准解密 策略类型，因为它设置更简单，且应能减少客户常遇到的问题。特别是，标准解密 策略可防止您在您的网络中解密过多流量。流量解密需要大量处理能力，解密过多流量会降低系统速度。

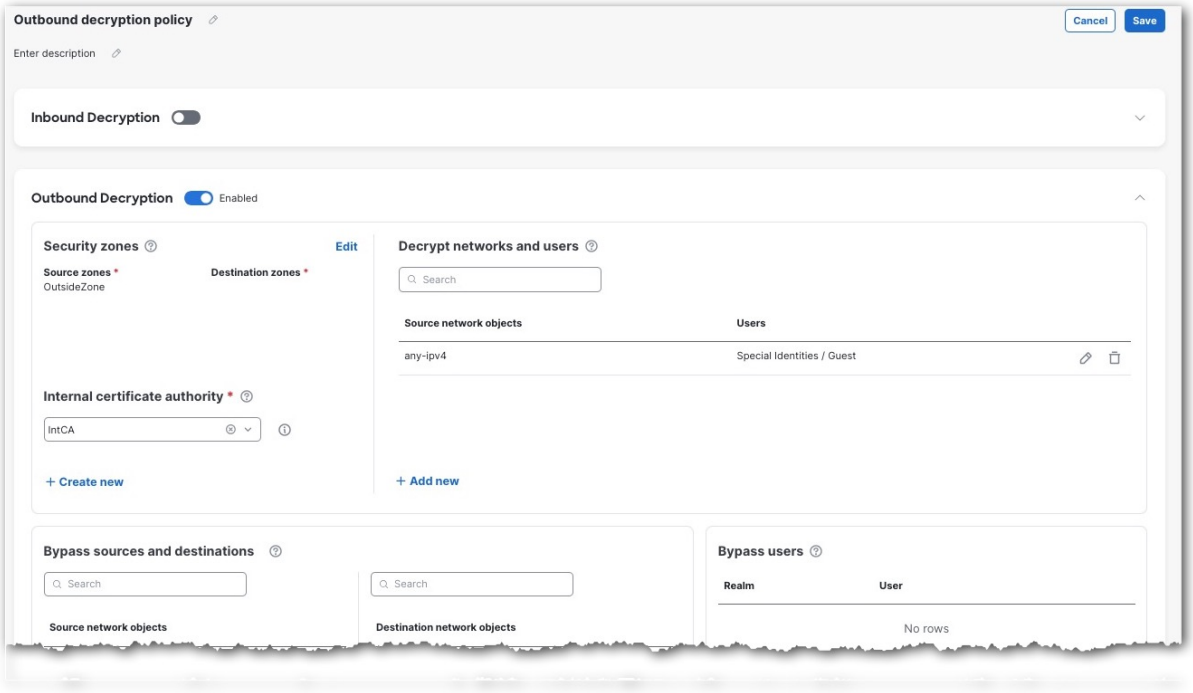
哪种类型的解密策略适合我？

本主题讨论 标准解密 策略和 基于规则的解密 策略。

标准解密策略

我们建议使用标准 解密策略类型，因为它具有向导式的外观，易于设置，使您能够轻松选择要在策略中使用的安全区、用户和网络以及其他对象。标准解密策略特别适合不熟悉解密策略细节的用户。

以下是设置标准解密策略的示例。



前述策略仅解密传出流量。来自任何 IPv4 网络上 OutsideZone 安全区域的所有流量均使用名为 `IntCA` 的内部 CA 解密。

请注意以下事项：

- 前面的规则是不完整的示例，还有更多可用选项
- 您可以配置入站条件和/或出站条件。
- 除了 对象，您还可以选择配置出站解密排除项，如：
  - 无法解密的应用（例如使用证书锁定的应用）。
  - URL 类别，例如医疗、贸易和财务。
- 您可以为证书状态和 TLS 版本配置出站阻止规则。
- 标准策略具有类似于旧版策略的高级策略选项。

基于规则的解密策略

使用向导创建的解密策略，引导您完成入站解密、出站解密或两者的可用选项。创建旧解密策略后，您可以向其添加更多规则、对规则重新排序或进行其他更改以满足您的需求。

基于规则的解密策略最灵活，但也最复杂。您可以随时将标准解密策略转换为基于规则的策略。

10.0.0 之前版本的标准解密策略部署问题

如果将标准解密策略部署到运行 10.0.0 之前版本的设备，您可能会遇到以下问题：

- 如果配置任何入站解密规则，则规则操作会在这些设备上更改为**解密 - 已知密钥**。有关传入解密操作类型的详细信息，请参阅传入流量解密。
- 高级策略选项**智能解密绕行**要求设备运行 7.7 或更高版本。默认情况下，此高级选项处于禁用状态，但如果启用此选项，并且设备运行的是 7.7 之前的版本，则策略部署会失败。

创建新的 标准解密 策略

您可以创建以下任何类型的解密策略：

- 保护入站流量的策略：解密传入您网络的网络流量。执行此操作通常是为了解密和检查定向到内部服务器的流量。
- 保护出站流量的策略：解密从网络流向外部服务器的网络流量。

有关详细信息，请参阅以下主题之一：

相关主题

创建具有入站保护的 标准解密 策略，第 3 页
创建具有入站保护的 标准解密 策略，第 7 页

创建具有入站保护的 标准解密 策略

以下任务讨论如何创建 标准解密 策略以解密 传入 网络的网络流量。执行此操作通常是为了解密和检查定向到内部服务器的流量。此页面上的所有选项均为必填项。

开始之前

在 传入流量解密中查看入站保护解密策略的含义。

要创建具有出站保护的解密策略，请参阅创建具有入站保护的 标准解密 策略，第 7 页。

过程

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

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击 **创建新的** > **解密策略**

步骤 4 在提供的字段中，输入**名称**和可选**说明**。

解密策略名称中不支持使用以下字符：

- #,;,{,},=,$,<,>

步骤 5 点击**创建策略 (Create Policy)**。

步骤 6 将 “**入站解密**” 滑动到 “**启用**”，如下图所示。

步骤 7 将以下内容添加到解密策略中：

- 安全区，第 4 页
- 内部服务器详细信息（入站解密），第 6 页

安全区

安全区域对您的网络进行分段，通过对多个设备之间的接口进行分组来帮助您管理、分类和解密流量。

安全区域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。

尽可能将匹配条件减少，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。

了解更多信息：

- 入站解密：添加安全区域（入站解密），第 4 页
- 出站解密：添加安全区域（出站解密），第 8 页

添加安全区域（入站解密）

此任务讨论如何将安全区域添加到入站 标准解密 策略。安全区指定向内部服务器发送流量的Firewall Threat Defense设备接口。通常，对于入站保护，这是一个内部（或 *DMZ*）接口。

您必须同时选择源和和目标安全区域。

开始之前

完成 创建具有入站保护的 标准解密 策略，第 3 页中讨论的任务。

过程

步骤 1 点击安全区域旁边的**编辑区域**。

步骤 2 在安全区对话框中，执行以下任一操作：

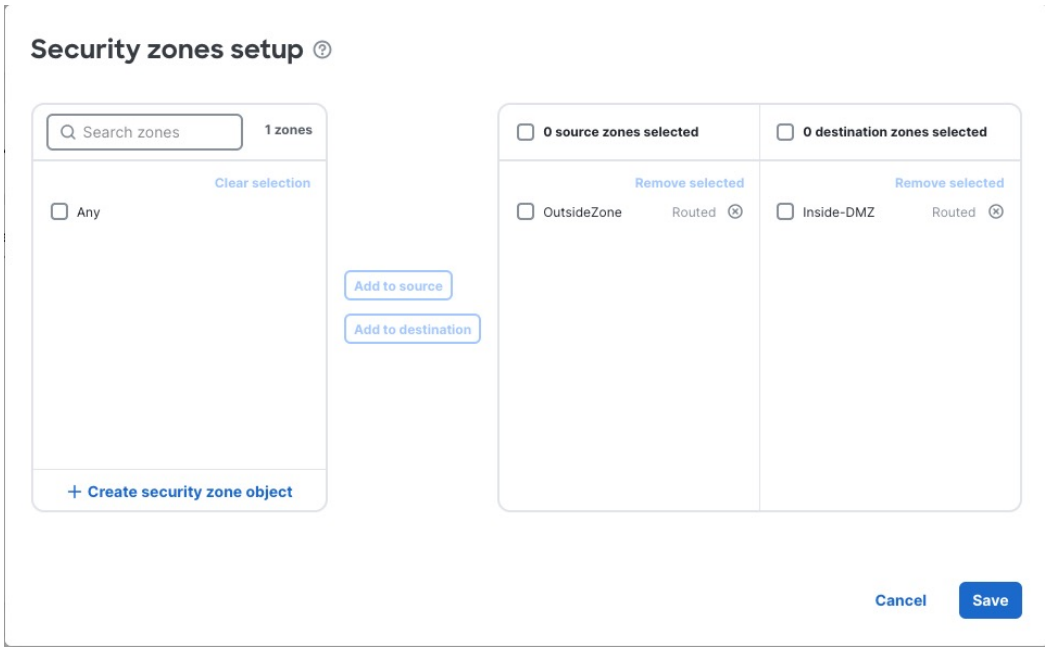
- 选中要添加到源或目标的安全区域旁边的复选框。
- 要创建新的安全区域，请点击 **创建安全区域对象 (Create security zone object)**。
- 在搜索区域字段中输入文本并按 Enter 键以搜索安全区。

注释
点击任何对话框上的 **帮助** (⊙) 了解详细信息。

步骤 3 点击 **添加到源**以解密匹配源安全区域的流量，或点击**添加到目标**以解密匹配目标安全区域的流量。如果同时选择源网络和目标区域进行解密，则流量必须与两个区域匹配。

通常，您的内部服务器应是入站解密规则的目标。

下图显示了一个示例。



步骤 4 点击**保存**。

步骤 5 请参阅内部服务器详细信息（入站解密），第 6 页。

内部服务器详细信息（入站解密）

通过解密和（可选）检查流向内部服务器的流量来添加要保护的内部服务器。您可以使用网络对象和可选端口指定这些服务器。

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。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。

尽可能将匹配条件减少，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。

有关详细信息，请参阅添加内部服务器，第 6 页。

添加内部服务器

此任务讨论如何选择证书来解密到达要保护的内部服务器的流量。除了可以选择证书之外，还可以指定内部服务器所在的网络和端口，从而节省处理时间。

开始之前

完成 创建具有入站保护的 标准解密 策略，第 3 页中讨论的任务。

过程

步骤 1 点击内部服务器详情下的 **添加新的** 。

步骤 2 在内部服务器对话框中，执行以下任一操作：

- 在搜索字段中输入文本并按 Enter 键，从而搜索内部证书。
- 从 **内部证书对象** 列表中，选择现有证书，或点击 **新增 (Add New)** 以创建新证书。

  注释
  为流量提供服务的 Cisco Secure Firewall Threat Defense 设备必须信任您上传至规则的证书。如果上传自签名证书或不受证书颁发机构信任的证书，并且想要稍后替换证书，则必须通过以下任一方式更新策略的高级设置：

  - 将证书添加到**受信任 CA 证书**列表。
  - 选择**入站解密需要证书完全匹配**复选框。

  有关高级策略选项的详细信息，请参阅标准解密 策略高级选项，第 19 页。

  有关替换证书的详细信息，请参阅传入流量解密中有关替换证书的讨论。

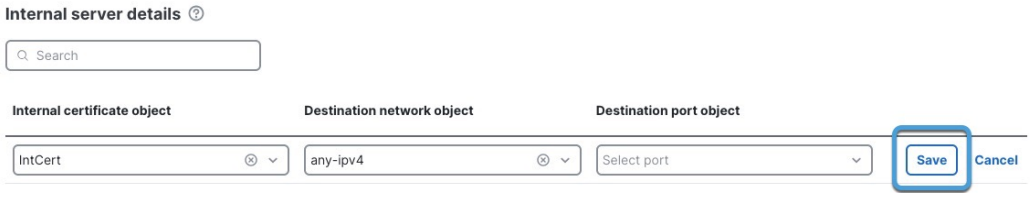
- 从**目标网络对象列表**中，点击内部服务器所在的网络，或点击**添加新网络**以创建新的网络。
- （可选。）从 **目标端口** 列表中，点击要应用解密规则的端口，或点击 **添加新的** 以创建新规则。

  有关详细信息，请参阅为入站保护上传内部证书。

注释
点击任何对话框上的 **帮助** (?) 了解详细信息。

步骤 3 点击**保存**。

下图显示了一个示例。



步骤 4 通过点击页面顶部的 **保存** 来保存解密策略。

步骤 5 如果您已完成策略配置，请参阅 解密策略操作 ， 第 22 页。

创建具有入站保护的 标准解密 策略

注释 有关将 标准解密 策略部署到运行 10.0.0 之前版本的设备时潜在问题的信息，请参阅10.0.0 之前版本的标准解密策略部署问题 ， 第 2 页。

以下任务讨论如何创建标准解密策略来保护内部网络外的服务器。要解密出站连接，除另有说明外，此页面上的所有选项均为必填项。要绕过或阻止某些出站连接，只需要安全区域以及绕过或阻止选项。

开始之前

在 解密和重新签名（传出流量）中查看出站保护解密策略的含义。

要改为创建具有入站保护的解密策略，请参阅创建具有入站保护的 标准解密 策略 ， 第 3 页。

过程

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

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 点击 **创建新的** > **解密策略**

步骤 4 在提供的字段中，输入**名称**和可选**说明**。

解密策略名称中不支持使用以下字符：

- #,;,{,},=,$,<,>

步骤 5 点击**创建策略 (Create Policy)**。

步骤 6 将**出站解密**滑动到**已启用**，如下图所示。

安全区

安全区域对您的网络进行分段，通过对多个设备之间的接口进行分组来帮助您管理、分类和解密流量。

安全区域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。

尽可能将匹配条件减少，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。

了解更多信息：

- 入站解密：添加安全区域（入站解密），第 4 页
- 出站解密：添加安全区域（出站解密），第 8 页

添加安全区域（出站解密）

此任务讨论如何将安全区域添加到出站 标准解密 策略。安全区指定向外部服务器发送流量的Firewall Threat Defense设备接口。

开始之前

完成 创建具有出站连接保护的 基于规则的解密策略中讨论的任务。

过程

步骤 1 点击安全区域旁边的**编辑区域**。

步骤 2 在安全区对话框中，执行以下任一操作：

- 选中要添加到源或目标的安全区域旁边的复选框。

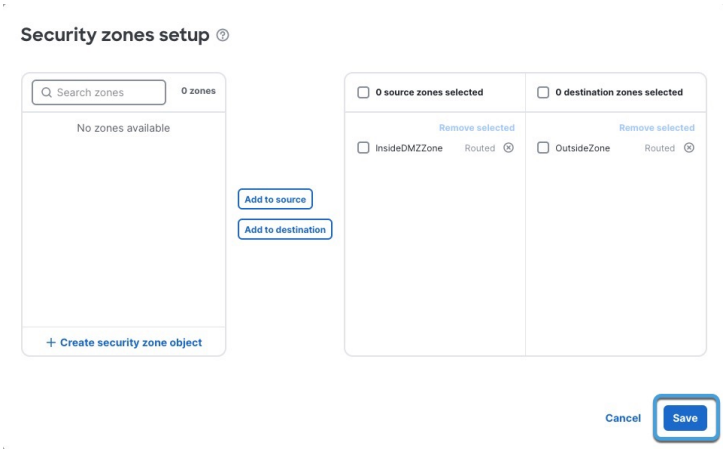
- 要创建新的安全区域，请点击 **创建安全区域对象 (Create security zone object)**。
- 在搜索区域字段中输入文本并按 Enter 键以搜索安全区。

注释
点击任何对话框上的 **帮助** (?) 了解详细信息。

步骤 3 点击 **添加到源 (Add to Source)** 以解密匹配源网络的流量，或点击 **添加到目标 (Add to Destination)** 以解密匹配目标网络的流量。如果同时选择源网络和目标网络进行解密，则流量必须与两个安全区匹配。

通常，要为其解密流量的服务器应在目标区域中。

下图显示了一个示例。



步骤 4 点击**保存**。

步骤 5 如果您已完成策略配置，请参阅 解密策略操作，第 22 页。

解密网络和用户

通过此选项，您可以对特定网络对象以及 Microsoft AD、LDAP 或本地领域中的特定用户和组实施解密和深度检查。

网络对象

网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。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来构建网络条件。

用户和组

您可以选择解密来自身份领域中一部分用户和组的流量，也可以选择解密来自以下特殊身份的流量：

- 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。

相关详细信息

有关详细信息，请参阅添加网络和用户 ， 第 10 页。

添加网络和用户

此任务讨论如何对来自特定网络的出站流量强制解密；以及来自 Microsoft Active Directory、LDAP 或本地领域中的用户和组的流量。

只会解密与您选择的所有网络和用户都匹配的流量。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 7 页中讨论的任务。

过程

步骤 1 完成 创建具有入站保护的 标准解密 策略 ， 第 7 页中讨论的任务。

步骤 2 点击“解密网络和用户”旁边的**新增**。

步骤 3 从**源网络对象**列表中，执行以下任一操作：

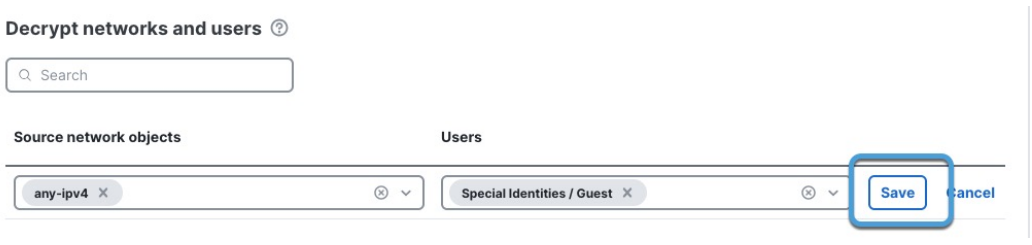
- 在提供的字段中，输入现有网络对象的全部或部分以过滤该对象。
- 选中要解密的网络旁边的复选框。要解密来自所有网络的流量，请点击**新增**和**保存**，而不选择任何网络。
- 点击**新增**以向列表中添加其他网络。

  有关详细信息，请参阅创建网络对象。

步骤 4 从**用户**列表中，选中每个要解密的用户名或组名旁边的复选框。

要解密来自所有用户的流量，请点击**新增**和**保存**，而不选择任何用户。

下图显示选择要解密的网络和用户的示例。



步骤 5 点击**保存**。

步骤 6 如果您已完成策略配置，请参阅 解密策略操作，第 22 页。

内部证书颁发机构

本主题讨论如何将内部证书颁发机构 (CA) 添加到 标准解密 策略的出站部分。内部证书颁发机构用于在解密流量后对流量进行重新签名。内部 CA 必须受到网络上的用户的信任，以避免在其网络浏览器中看到不受信任的证书错误。

有关详细信息，请参阅为出站保护添加内部 CA，第 11 页。

为出站保护添加内部 CA

此任务讨论如何添加内部 CA 以重新签发传出流量。

开始之前

完成 创建具有入站保护的 标准解密 策略，第 7 页中讨论的任务。

过程

在**内部证书颁发机构**列表中，执行以下任一操作：

- 点击内部 CA 的名称。
- 点击**新建**以创建新的内部 CA。

  点击**帮助**以获取更多信息。

  如果您还没有内部 CA，请参阅：

  - 为出站保护生成内部 CA，第 11 页
  - 为出站保护上传内部 CA，第 12 页

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

步骤 2 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 3 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。

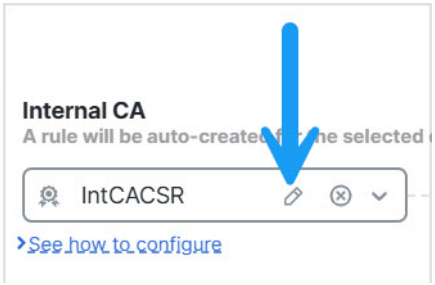
步骤 4 在提供的字段中输入请求的信息。

步骤 5 点击**保存**。

步骤 6 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 7 按照 创建具有出站连接保护的 基于规则的解密策略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**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 从**内部 CA (Internal CA)** 列表中，点击**新建 (Create New）** > **上传 CA (Upload CA)**。

步骤 2 为内部 CA 指定一个**名称**。

步骤 3 粘贴或在提供的字段中浏览找到证书及其私钥。

步骤 4 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 5 按照 创建具有出站连接保护的 基于规则的解密策略中的说明继续创建策略。

解密时绕过流量

本主题讨论您可以选择绕过解密流量的方法（即，流量通过设备加密）。您可以在此处查看对流量保持加密的一些原因：何时解密流量以及何时不解密。绕过某些流量还有一个额外的优势，即解密流量时不会消耗系统资源。

我们提供以下方法在解密时绕过流量：

- 绕过源和目标网络：例如，无需解密来自您可信的内部/DMZ 网络上内部服务器的流量。
- 绕过用户：您可以为信任的用户和组绕过解密。
- 绕过无法解密的应用：（推荐。）绕过流向应用的传出流量的典型原因是此类流量可能使用无法解密的证书锁定。

  有关详细信息，请参阅关于 TLS/SSL 锁定。
- 绕过类别：（推荐。）由于以下原因，绕过解密站点的 URL 类别：
  - 类别代表可能非法解密和检查的应用（例如个人财务或健康）。
  - 思科确定为低风险的网站类别。
- 智能解密绕过：根据客户端的威胁置信度绕过服务器，该置信度由加密可见性引擎 (EVE) 和 URL 类别信誉确定。

  所有部署了启用此选项的 标准解密 策略的设备都必须运行 7.7 或更高版本；否则，策略部署会失败。

绕过源和目的地

（可选。）绕过来自源或目标网络对象的流量。例如，如果流量来自拥有受信任设备的内部网络，您可以选择不解密该流量。 网络使用内部信头按流量的源和目标 IP 地址来控制或解密流量。

有关详细信息，请参阅添加绕过源和目的地 ， 第 13 页。

添加绕过源和目的地

以下任务讨论如何选择性地绕过来自源网络或前往目标网络的出站流量。通常，只有在您信任来自这些网络的流量时才执行此操作。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 7 页中讨论的任务。

过程

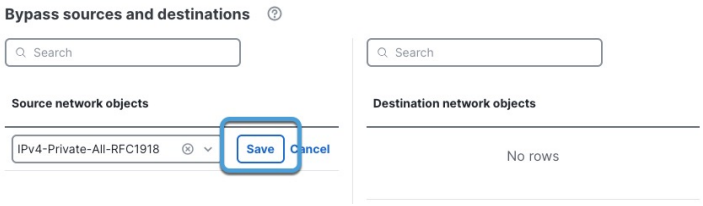
步骤 1 对于源网络对象或目标网络对象，点击“绕过源和目标”下的**新增**。

步骤 2 在显示的对话框中，执行以下任一操作：

- 在搜索字段中输入文本并按 Enter 键，即可搜索网络对象。
- 从**源网络对象**或**目标网络对象**列表中，选择现有的网络对象，或点击**新增**以创建一个新的网络对象。

注释
点击任何对话框上的 **帮助** (⊙) 了解详细信息。

下图显示了一个示例。



步骤 3 点击**保存**。

步骤 4 如果您已完成策略配置，请参阅 解密策略操作，第 22 页。

绕过用户

（可选。）您可以在 Microsoft Active Directory、LDAP 和本地领域中为特定用户绕过解密；通常，这些是您信任的用户。

您可以选择绕过身份领域中的一部分用户和组，也可以选择从以下特殊身份绕过：

- 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。

有关详细信息，请参阅添加绕过用户，第 14 页。

添加绕过用户

为选定的 Microsoft AD、LDAP 和本地领域中的用户和组绕过解密。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 7 页中讨论的任务。

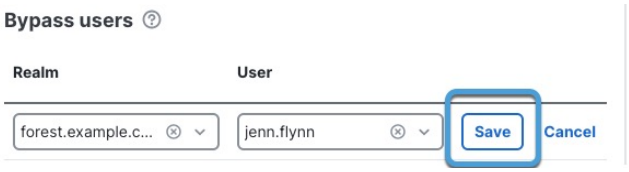
过程

步骤 1 点击绕过用户下的**新增**。

步骤 2 在显示的对话框中：

- 在**领域**列表中，点击领域名称。
- 从**用户**列表中，选中要绕过解密的一个或多个用户或组旁边的复选框。

下图显示了一个示例。



步骤 3 点击**保存**。

步骤 4 根据需要多次重复上述步骤，以绕过更多用户和组。

绕过应用

（可选。）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。

有关详细信息，请参阅添加绕过应用程序 ， 第 15 页。

添加绕过应用程序

此任务讨论如何绕过应用程序的解密（通常是因为这些应用程序使用证书锁定，如关于 TLS/SSL 锁定中所述，无法解密）。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 7 页中讨论的任务。

过程

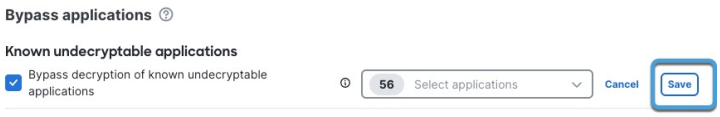
步骤 1 选中**绕过已知不可解密应用程序的解密**复选框。

步骤 2 点击**编辑应用程序**。

步骤 3 从列表中执行以下任一操作：

- 点击**全选**以选择思科确定的所有不可解密的应用程序。
- 选中要绕过解密的某个应用程序名称旁的复选框。
- 清除要解密连接的某个应用程序名称旁的复选框。

下图显示了一个示例。



步骤 4 在选定的应用程序和过滤器下，点击**新增**以添加要绕过的应用程序或应用程序过滤器。点击**帮助**以获取更多信息。

步骤 5 点击**保存**。

步骤 6 如果您已完成策略配置，请参阅 解密策略操作 ， 第 22 页。

绕过 URL 类别和信誉

（可选。）选择不解密的类别和信誉，例如个人财务或健康信息。根据您所在地区的法律，解密此类流量可能被禁止。有关详细信息，请咨询您所在地区的权威机构。

URL 类别和信誉由 Cisco Talos 维护。

有关类别的详细信息，请参阅智能类别。

有关信誉的详细信息，请参阅 Web 信誉级别。

要将 URL 类别和信誉添加到您的解密策略，请参阅添加绕过 URL 类别和信誉 ， 第 16 页。

添加绕过 *URL* 类别和信誉

（可选。）此任务讨论如何根据 Cisco Talos 提供的评级绕过类别和信誉解密。

下图显示了我们建议的类别和信誉列表。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 7 页中讨论的任务。

过程

步骤 1 在“绕过 URL 类别”部分中，执行以下任一操作：

- 要编辑现有的类别/信誉，请点击 **编辑** ()。
- 要删除现有类别/信誉，请点击 **删除** ()。
- 要添加新的类别/信誉，请点击**新增**。
- 要将类别和信誉列表返回到思科建议的类别和信誉列表，请点击**应用建议的设置**。

步骤 2 要添加或编辑类别/信誉，请从第一个列表中点击类别的名称。

有关类别的详细信息，请参阅智能类别。

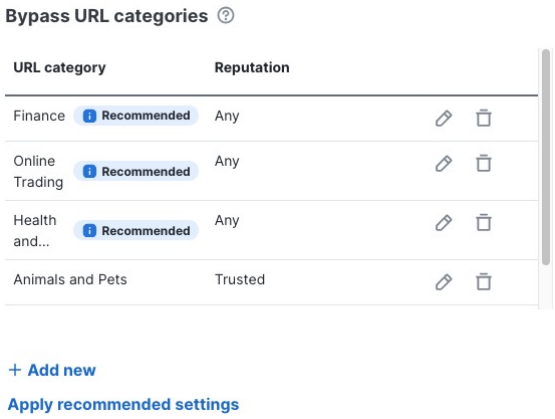
步骤 3 从第二个列表中，点击信誉的名称。

有关信誉的详细信息，请参阅 Web 信誉级别。

下图显示了使用思科的默认设置并添加信誉为“受信任”的“动物和宠物”类别的示例。

步骤 4 点击**保存**。

下图显示了一个示例。



步骤 5 如果您已完成策略配置，请参阅 解密策略操作，第 22 页。

绕过智能解密

您可以将EVE设置为绕过解密前往受信任连接的流量。绕过行为广泛，涵盖许多一般浏览活动。例如，与 www.cnn.com 的连接不会被解密，但从 CNN 的内容交付网络 (CDN) 获取资产的其他连接如果未被分类为受信任，则可能会被解密。

客户端分类基于 EVE 的风险评估，该风险评估使用机器学习来识别流量风险级别。URL 分类基于 Talos URL 信誉。系统会绕过且不解密从风险极低的客户端到受信任 URL 的任何连接。所有其他连接（包括与不受信任的 URL 的连接或来自分类为较高风险级别的客户端的连接）均须遵守解密策略。

绕过受信任连接可减少不必要的解密处理，节省系统资源。这也尊重用户隐私，不会解密分类为低风险和受信任的流量。

要为出站解密规则设置智能解密绕过，请找到**智能解密绕过**并将其设置为**滑块已启用**( )，以便根据加密可见性引擎 (EVE) 确定的客户端威胁置信度和URL类别信誉，不对连接到受信任服务器的极低风险客户端的流量进行解密。

要查看按信任级别分类的当前客户端列表，请转至 Cisco Secure Firewall 应用检测器。例如，cnn.com 被分类为“非常低”。确保您了解选择不解密的流量。

阻止连接

（可选。）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。

您可以选择阻止以下任一项：

- SSL 和 TLS 版本，因为有些被视为不安全。
- 证书状态；例如，可以阻止流向证书过期的服务器的出站流量，因为该服务器可能不可信任。

有关详细信息，请参阅添加阻止连接，第 19 页。

添加阻止连接

此任务讨论如何根据旧的 SSL 或 TLS 版本阻止连接；或基于服务器证书状态阻止连接。

注释 阻止会影响所有出站连接，并优先于您选择的所有其他绕过和解密条件。

开始之前

完成 创建具有入站保护的 标准解密 策略 ， 第 7 页中讨论的任务。

过程

步骤 1 找到“阻止连接”部分。

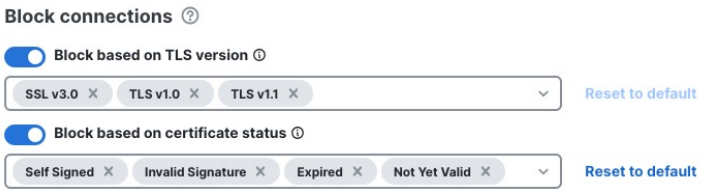
步骤 2 要根据 SSL 或 TLS 协议版本阻止出站流量，请将**基于 TLS 版本阻止**滑动到 **滑块已启用** ( )。

步骤 3 要根据服务器证书状态阻止出站流量，请将**基于证书状态阻止**滑动到 **滑块已启用** ( )。

步骤 4 您有以下选择：

- 从列表中选中选项旁边的复选框，以将该协议或状态添加到策略中。
- 点击项目旁边的 **x** 可将其从列表中移除。
- 点击**重置为默认值**，可将列表条目恢复为其原始值。

下图显示使用 TLS 版本和服务器证书状态阻止流量的示例。自签名已添加到要阻止的服务器证书列表。



步骤 5 如果您已完成策略配置，请参阅 解密策略操作 ， 第 22 页。

标准解密 策略高级选项

（可选。）要设置高级解密策略选项，请创建或编辑一个标准解密 策略，然后展开**高级选项**。高级选项将在以下段落中讨论。

建议将所有高级选项设置为其默认值。

绕过思科旧版不可解密的站点

启用此选项可绕过对思科已确定无法解密的可分辨名称 (DN) 的网站进行解密。要查看 DN 列表，请转至 **对象** > **可分辨名称** > **对象组**。

入站解密需要证书完全匹配

启用此选项以要求在解密策略中使用内部服务器的证书（此选项称为已知密钥解密）。默认为使用其他证书，这样更便于在需要时替换策略的证书。有关详细信息，请参阅 传入流量解密操作。

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。Secure Firewall Threat Defense Virtual如果您有任何由 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。

解密事件日志记录选项

为了加快故障排除速度并了解解密策略的运行情况，建议您启用所有日志记录选项：绕过的流量、已解密的流量和被阻止的流量。

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 Firewall Threat Defense 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。

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。

保存策略

在配置高级策略选项后，请参阅解密策略操作 ， 第 22 页。

添加受信任 CA 证书

（可选。）此任务讨论如何将受信任 CA 证书添加到解密策略。我们强烈建议为组织的证书添加颁发者 CA，以避免解密流量出现问题。

开始之前

完成以下讨论的任务：

- 创建具有入站保护的 标准解密 策略 ， 第 3 页

- 创建具有出站连接保护的 基于规则的解密策略

过程

步骤 1 在策略中，展开**高级选项**。

步骤 2 在**受信任的 CA 证书**列表中，执行以下任一操作：

- 点击列表中受信任 CA 证书的名称。
- 要从列表中删除所有证书，请点击 。
- 要将列表恢复为原始值，请点击**添加推荐**。

解密策略操作

以下主题讨论如何：

- 复制解密策略
- 将 标准解密 策略转换为 基于规则的解密 策略
- 生成有关解密策略的报告

相关主题

将 标准解密 策略转换为 基于规则的解密 策略 ， 第 22 页
复制解密策略 ， 第 23 页
生成解密策略报告 ， 第 23 页

将 标准解密 策略转换为 基于规则的解密 策略

以下任务讨论如何将 标准解密 策略转换为 基于规则的解密 策略。转换为 基于规则的解密 策略后，您无法再转换回 标准解密 策略。此外，您无法将任何 基于规则的解密 策略转换为 标准解密 策略。

我们提供此功能，让您可以使用基于规则的解密策略中可用的其他自定义选项。有关详细信息，请参阅关于基于规则的解密策略。

开始之前

创建解密策略，如本指南中所述。

过程

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

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在要转换的解密策略旁边，在操作列中，点击 更多图标 （ ··· ），然后点击**转换策略模式**。

步骤 4 您需要确认操作。

系统将创建一个备份策略，并在原始策略的名称后附加 **-backup**。原始策略保留其名称。

复制解密策略

以下任务讨论如何复制解密策略。复制策略会复制策略中的任何规则以及所有策略的设置。

开始之前

创建解密策略，如本指南中所述。

过程

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

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在要复制的解密策略旁边的操作列中，点击 更多图标 （ ··· ），然后点击**复制策略**。

步骤 4 当出现提示时，请为策略提供名称。

步骤 5 点击**保存**。

生成解密策略报告

本主题讨论如何创建包含以下内容（以及其他内容）的解密策略报告：

- 规则列表
- 密码套件列表
- 策略的默认操作
- 受信任 CA 证书

开始之前

创建解密策略，如本指南中所述。

过程

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

步骤 2 请点击 **策略** > **安全策略** > **解密**。

步骤 3 在要创建报告的解密策略旁边，在操作列中，点击 更多图标 （ ··· ），然后点击**生成报告**。

系统会创建一个 PDF 报告，并使用默认的 PDF 应用程序将其打开。

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。

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。

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。