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。

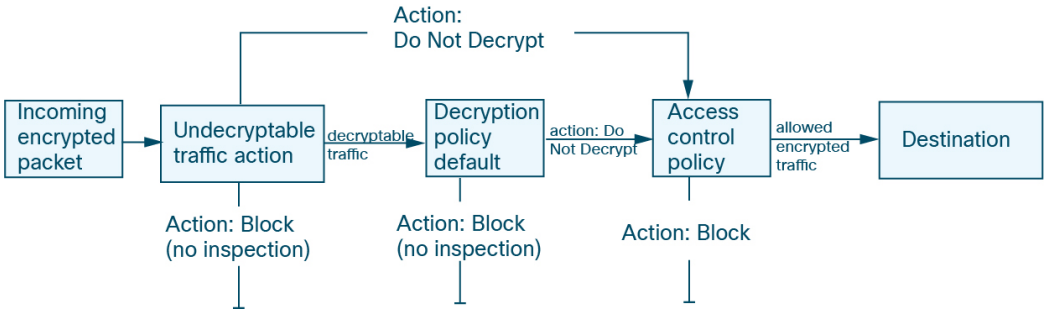
关于解密策略

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 解密策略将接管、处理和解密已加密的流量。

您可以同时创建多个规则，包括用于解密传入流量的规则（**解密 - 已知密钥 (Decrypt - Known Key)** 规则操作）和传出流量（**解密 - 重新签名 (Decrypt - Resign)** 规则操作）。要创建具有**不解密 (Do Not Decrypt)** 或其他规则操作（例如**阻止 (Block)** 或**监控 (Monitor)**）的规则，请创建一个空解密策略，然后再添加该规则。

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。

解密策略 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。

  请参阅创建具有出站连接保护的解密策略，第 2 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 (Decrypt - Known Key)** 规则操作。

  请参阅创建具有入站连接保护的解密策略，第 5 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 7 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，可以同时创建多个规则，包括多个**解密 - 已知密钥 (Decrypt - Known Key)** 规则和多个**解密 - 重新签名 (Decrypt - Resign)** 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 如果尚未登录，请登录Ciso Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。

步骤 3 点击 **创建解密策略**。

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 从 **内部证书** 列表中，上传或选择规则的证书。

系统会根据 CA 和网络/端口的组合创建一条规则（如适用）。

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 4 页 和 为出站保护上传内部 CA，第 4 页。

步骤 6 （可选。）选择网络和端口。

更多详情：

- 网络规则条件
- 端口规则条件

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 8 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 10 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Ciso Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。

步骤 3 点击 **创建解密策略**。

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 (Save)**。

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 创建具有入站连接保护的解密策略， 第 5 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Ciso Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。

步骤 3 点击 **创建解密策略**。

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 2 页中的说明继续创建策略。

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 (Decrypt - Known Key)** 规则操作。

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 (Decrypt - Known Key)** 规则和多个**解密 - 重新签名 (Decrypt - Resign)** 规则。

开始之前

您可选必须首先上传内部服务器的内部证书，然后才能创建保护入站连接的解密策略。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。

过程

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

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。

步骤 3 点击 **创建解密策略**。

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 从 **内部 CA** 列表中，上传或选择规则的证书。

系统会根据 CA 和网络/端口的组合创建一条规则（如适用）。

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。

更多详情：

- 网络规则条件
- 端口规则条件

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 8 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 10 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Ciso Secure Firewall Management Center。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。

步骤 3 点击 **创建解密策略**。

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 CA 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 5 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 (Decrypt - Known Key)** 规则和多个**解密 - 重新签名 (Decrypt - Resign)** 规则。

过程

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

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。

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）。

步骤 4 等待策略创建。

步骤 5 点击解密策略名称旁边的 **编辑**（ ）。

步骤 6 点击**添加规则 (Add Rule)**。

步骤 7 为规则 **命名**。

步骤 8 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 9 点击**保存 (Save)**。

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 8 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 10 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，请登录管理中心。
2. 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。
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

类型	说明	默认操作	可用操作
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
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 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。

相关主题

设置无法解密的流量的默认处理 ，第 10 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，请登录管理中心。

步骤 2 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **解密 (Decryption)**。

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 8 页和解密策略 默认操作，第 8 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；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 配置的所有受管设备的全局设置。

在运行以下命令的任何受管设备上，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 12 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管理的此类受管设备，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。

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 10 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
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 威胁防御上的所有 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。