解密规则 和策略示例

本章以本指南中讨论的概念为基础，提供包含遵循我们的最佳实践和建议的 解密规则 的 SSL 策略具体示例。您应该能够将此示例应用于自己的情况，使其适应您的组织的需求。

简而言之：

- 对于受信任的流量（例如传输大型压缩服务器备份），可使用预过滤和流量分流完全绕过检查。
- 将可以快速评估的任何 解密规则 规则放在 最前面，例如适用于特定 IP 地址的规则。
- 将需要处理的任何规则、 **解密 - 重新签署**规则以及阻止不安全协议版本和密码套件的 解密规则 放在 最后 。

解密规则 示例

本 部分 提供说明最佳实践的 解密规则 规则示例。

有关详细信息，请参阅以下各节之一：

运行解密策略向导

此任务讨论如何为出站流量保护运行解密策略向导。此策略包含四个规则：

1. **不解密**规则，适用于已知无法解密的可分辨名称，这很可能是因为它们使用 TLS/SSL 固定。

2. 根据内容分类为敏感的 URL 类别（例如，医疗和金融）的**不解密**规则。
3. **不解密**规则，适用于已知无法解密的应用，这很可能是因为它们使用 TLS/SSL 固定。
4. **解密 - 重签** 规则，使用名为 **IntCA** 的证书颁发机构对象解密其余流量。

然后，您可以根据需要编辑规则，也可以手动添加：

- **解密 - 重新签名**流量规则，以监控和确定未来是否应阻止流量。
- 适用于其他类型流量的**不解密**规则
- 针对不良证书和不安全密码套件的**阻止**或**阻止并重置**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**。

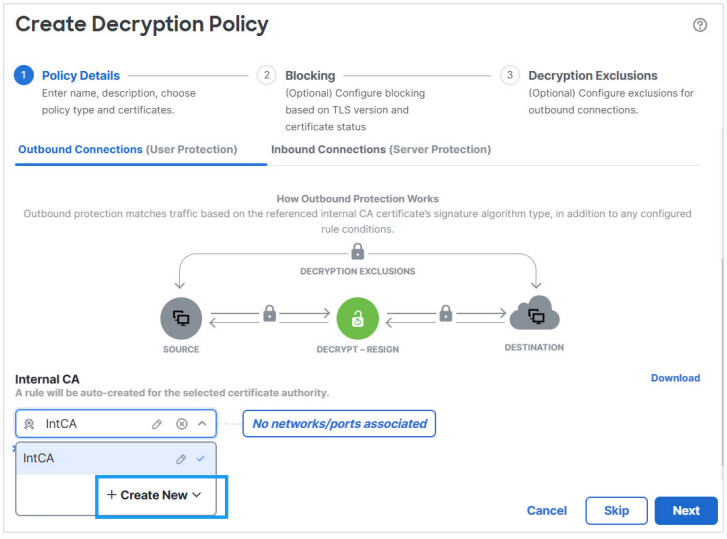
步骤 3 点击**创建解密策略 (Create Decryption Policy)**。

步骤 4 为解密策略提供一个**名称**，也可提供**说明**。

步骤 5 点击**出站保护 (Outbound Protection)** 选项卡。

步骤 6 从**内部 CA (Internal CA)** 列表中，点击内部证书颁发机构对象的名称，或者点击**新建 (Create New)** 以上传或生成证书颁发机构对象。

下图显示了一个示例。



有关创建或上传内部证书颁发机构对象的详细信息，请参阅：

- 为出站保护上传内部 CA
- 为出站保护生成内部 CA

步骤 7 （可选。）要限制流向源网络和目标网络的流量，请点击**点击以分配网络和端口 (Click to assign networks and ports)**。

步骤 8 点击**下一步 (Next)**。

步骤 9 完成 解密策略排除项中讨论的向导。

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：

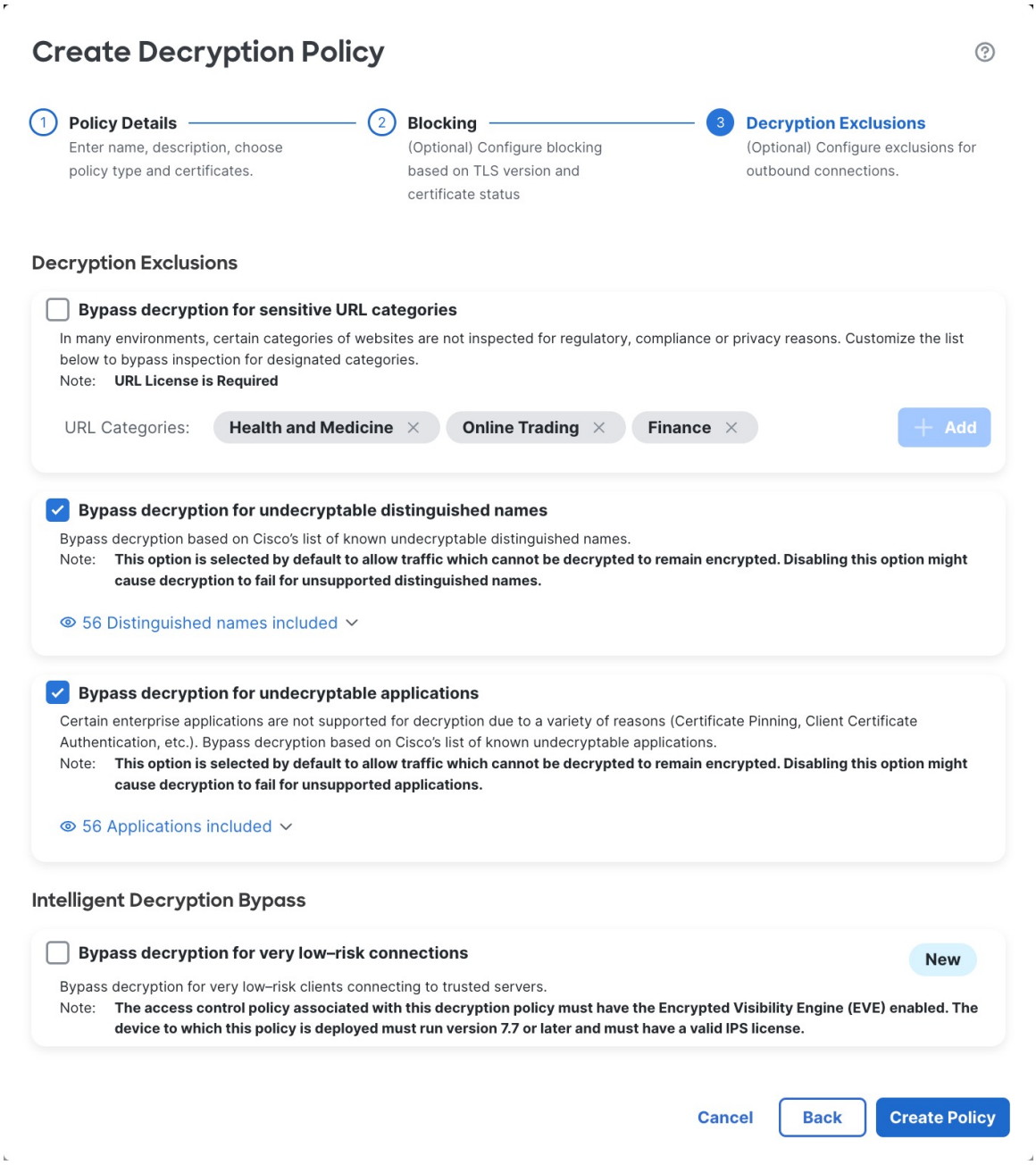
- 创建具有出站连接保护的解密策略
- 有关详细信息，请参阅创建具有入站连接保护的解密策略

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。

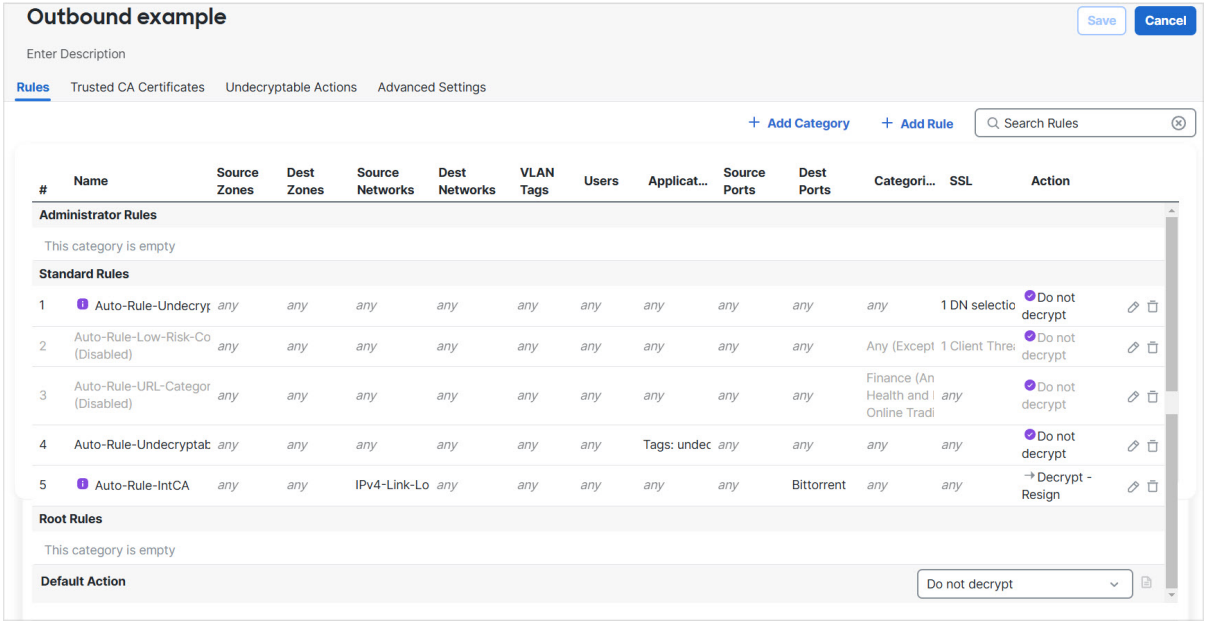
项目	说明
绕过对不可解密的可分辨名称的解密	选中此复选框可在重新签名证书可能导致连接失败时不解密流量。通常，此行为与证书锁定相关，《TLS/SSL 证书固定准则的证书锁定准则中对此进行了讨论。 无法解密的可分辨名称列表由思科维护。
绕过解密无法解密的应用	选中此复选框可在重新签名证书可能导致连接失败时不解密流量。 通常，此行为与证书锁定相关，《TLS/SSL 证书固定准则的证书锁定准则中对此进行了讨论。 无法解密的应用会在漏洞数据库 (VDB) 中自动更新。您可以在 Cisco Secure Firewall应用检测器 (Secure Firewall Application Detectors) 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。
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)**。

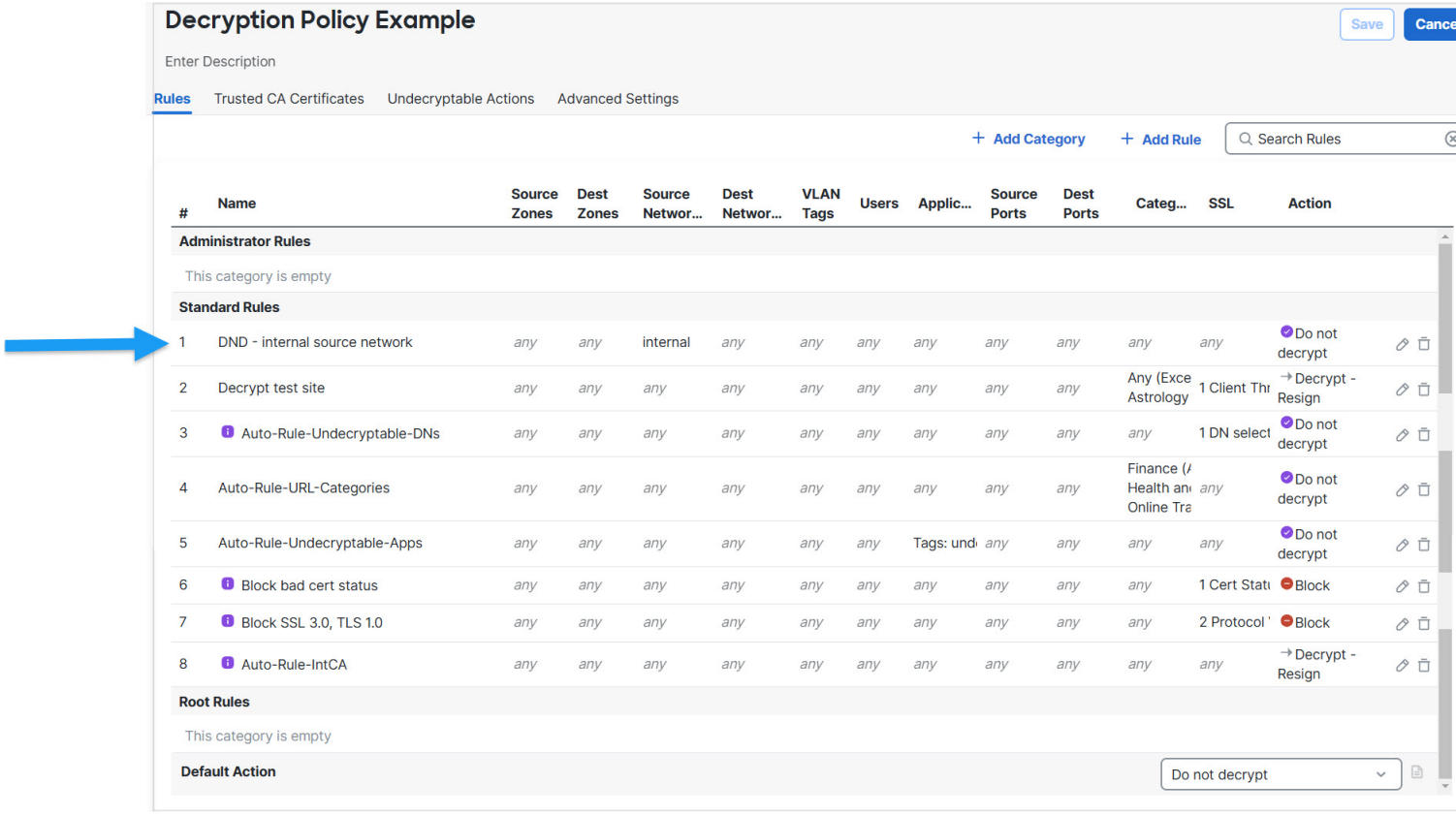
下一步做什么

- 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
- 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。
- 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。

第一个手动不解密规则：特定流量

示例中的第一条 解密规则 不会解密流向 内部网络（定义为 **internal**）的流量。**不解密**规则操作会在 ClientHello 期间进行匹配，因此处理速度非常快。

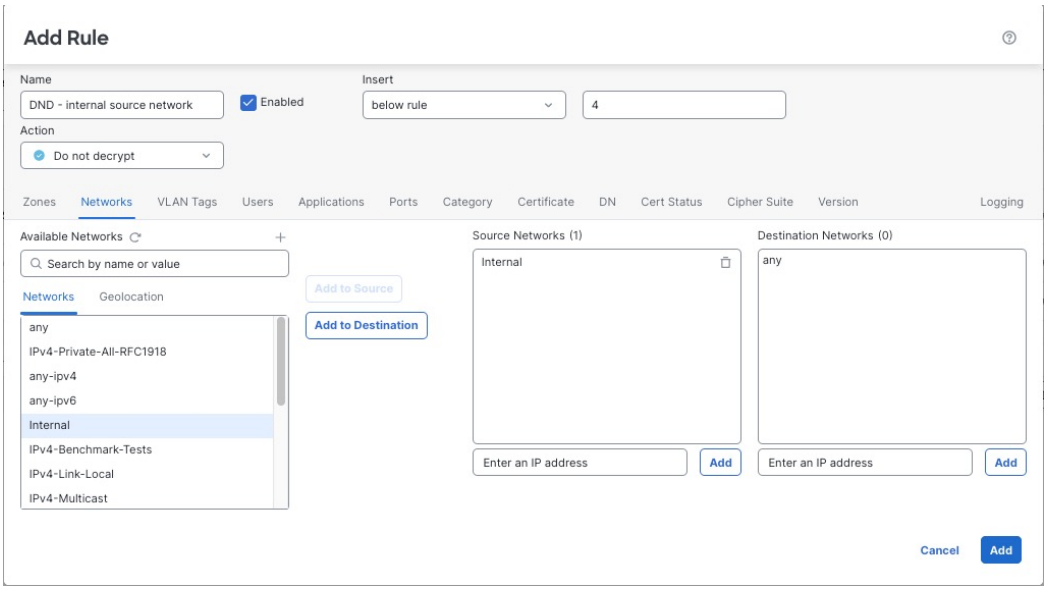
运行解密策略向导后，编辑策略以添加以下规则。将其拖动到规则列表的顶部，以便首先对其进行评估。



注释 如果您有从内部 DNS 服务器流向内部 DNS 解析器（例如思科 Umbrella 虚拟设备）的流量，则还可以为其添加**不解密规则**。如果内部DNS服务器会执行自己的日志记录，您甚至可以将这些添加到预过滤策略。

但是，我们强烈建议您不要对进入互联网的DNS流量使用**不解密**规则或预过滤，例如互联网根服务器（例如，Active Directory 中内置的 Microsoft 内部 DNS 解析器）。在这些情况下，您应该全面检查流量，甚至考虑阻止它。

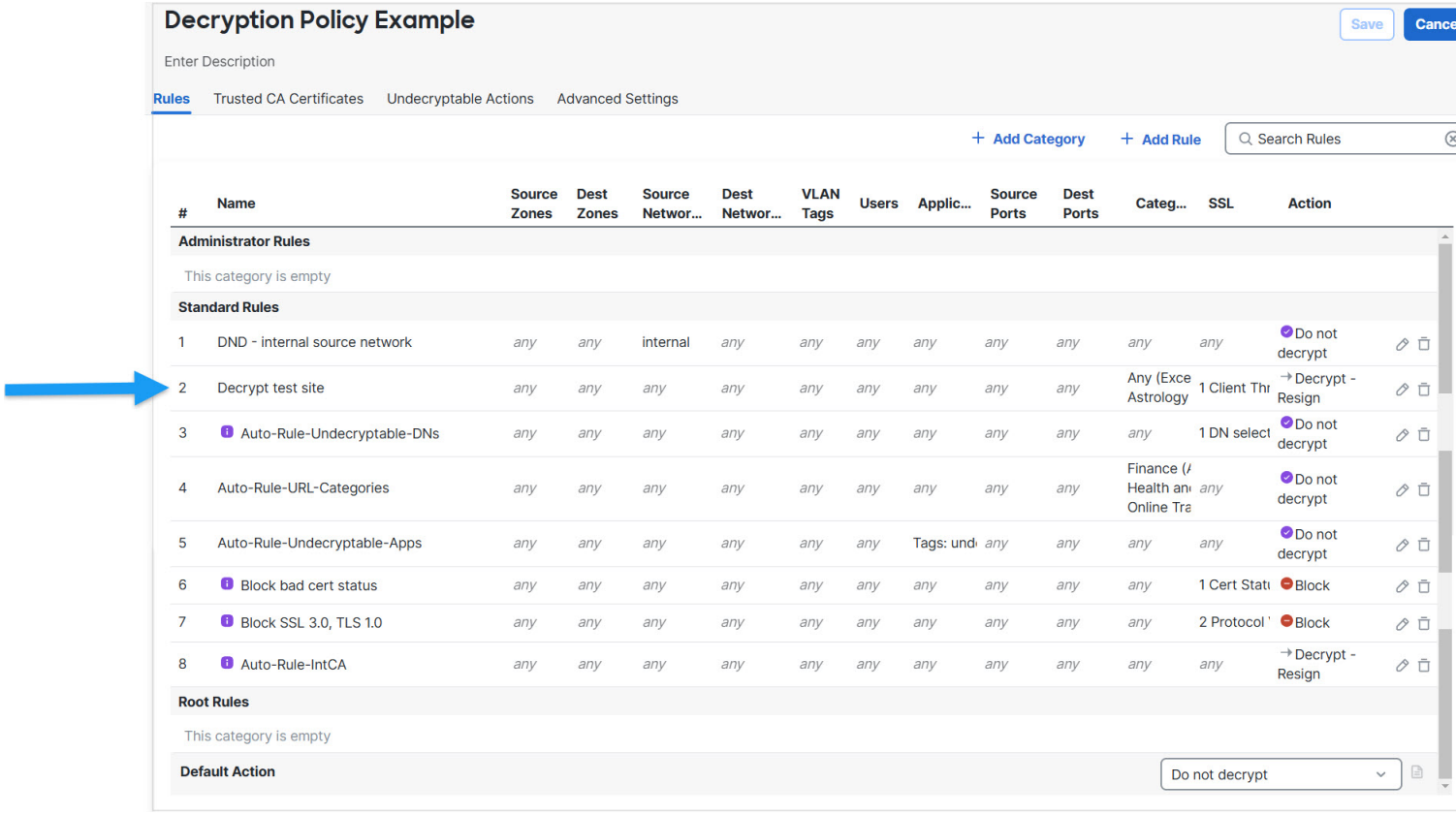
规则详细信息：



下一条手动规则：解密特定测试流量

在本例中，下一条规则为可选；使用它来解密和监控有限类型的流量，然后再确定是否允许它在您的网络上使用。

运行解密策略向导后，编辑策略以添加以下规则。将其拖动到规则列表中的第二个位置。



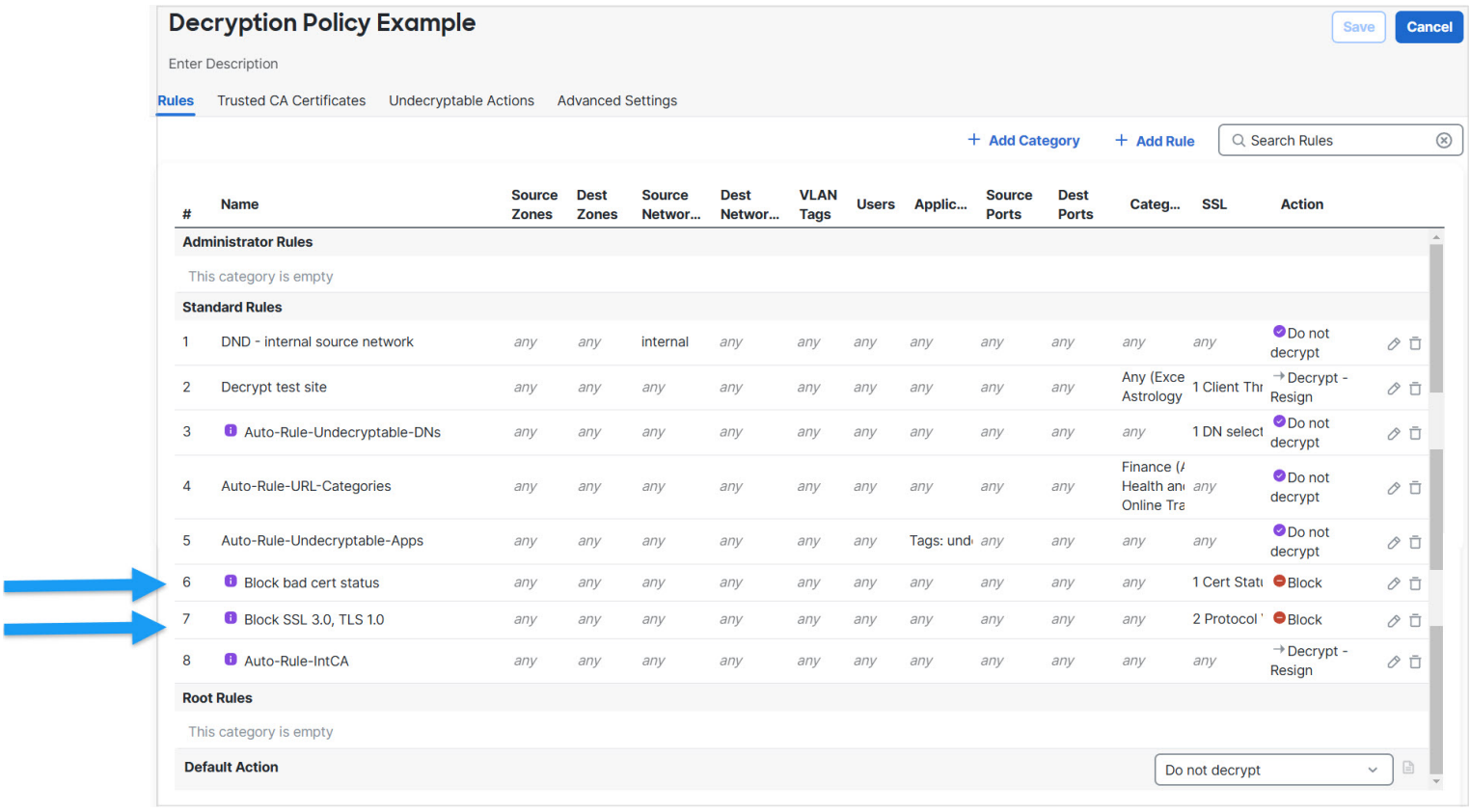
规则详细信息：

最后的 解密规则：阻止或监控证书和协议版本

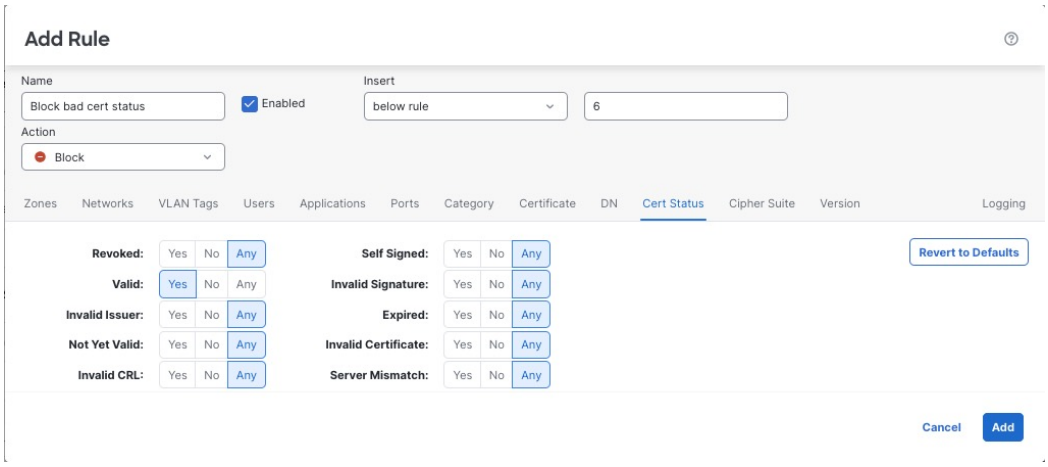
由于最后的 解密规则最具体且需要最多的处理，因此它们是监控或阻止不良证书和不安全协议版本的规则。

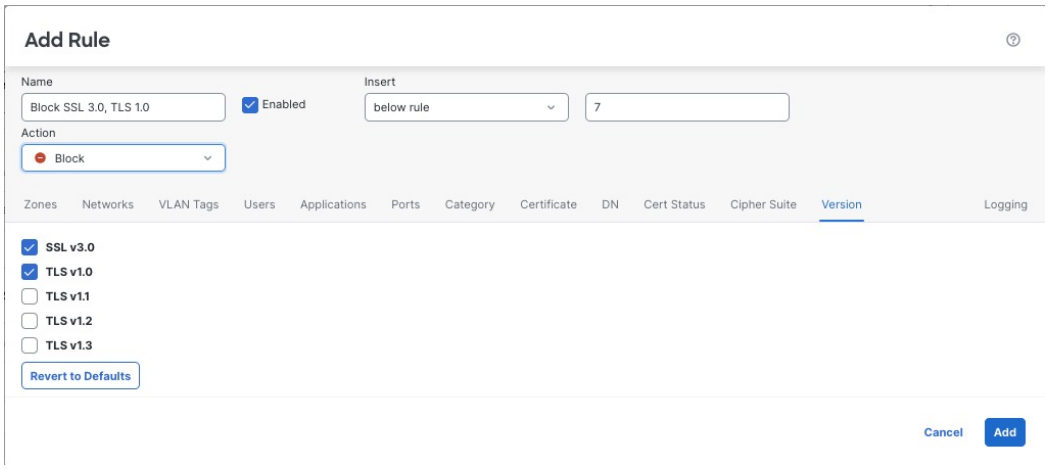
运行解密策略向导后，编辑策略以添加以下规则。将它们拖动到**解密 - 重新签名**规则之前 的位置。

最后的 解密规则：阻止或监控证书和协议版本



规则详细信息：





示例： 解密规则 监控或阻止证书状态的规则

由于最后的 解密规则最具体且需要最多的处理，因此它们是监控或阻止不良证书和不安全协议版本的规则。本部分中的示例显示如何按证书状态监控或阻止流量。

重要事项 仅在具有**阻止**或**阻止并重置**规则操作的规则中使用**密码套件 (Cipher Suite)** 和**版本 (Version)** 规则条件。不要将**密码套件**和**版本**与**解密 - 重新签名**或**解密 - 已知密钥**规则操作一起使用。在具有其他规则操作的规则中，这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

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 解密策略旁边的 **编辑** (✎) 。

步骤 4 点击 解密规则旁的 **编辑** (✎) 。

步骤 5 点击**添加规则**。

步骤 6 在“添加规则” 对话框中，在**名称**字段中输入规则的名称。

步骤 7 点击**证书状态 (Cert Status)**。

步骤 8 就每个证书状态而言，有以下选项：

- 点击**是**可根据该证书状态是否存在进行匹配。
- 点击**否**可根据该证书状态是否缺失进行匹配。
- 点击**任意 (Any)** 可在匹配规则时跳过条件。换言之，选择**任意**意味着无论证书状态是否存在都与该规则匹配。

步骤 9 从**操作 (Action)** 列表中，点击**监控 (Monitor)** 以仅监控和记录与规则匹配的流量，或点击**阻止 (Block)** 或**阻止并重置 (Block with Reset)** 以阻止流量并选择性地重置连接。

步骤 10 要保存对规则的更改，请点击页面底部的**添加 (Add)**。

步骤 11 要保存对策略的更改，请点击页面顶部的**保存**。

示例

组织信任 Verified Authority 证书颁发机构。组织不信任 Spammer Authority 证书颁发机构。系统管理员将 Verified Authority 证书和由 Verified Authority 颁发的中间 CA 证书上传到系统。由于“已验证颁发机构”已撤销它以前颁发的证书，因此系统管理员上传该“已验证颁发机构”提供的 CRL。

下图说明用于检查有效证书、由“已验证颁发机构”颁发的证书、不在 CRL 上的证书以及仍在有效开始日期和有效结束日期内的证书的证书状态规则条件。受配置原因的影响，未通过访问控制来解密和检查使用这些证书加密的流量。

下图显示用于检查状态是否缺失的证书状态规则条件。在此情况下，由于配置原因，它与使用尚未到期的证书加密的流量相匹配。

在下面的示例中，如果传入流量使用的证书具有无效的颁发者、自签名、已过期且是无效证书，则流量会与此规则条件匹配。

下图展示了一个证书状态规则条件，如果请求的 SNI 与服务器名称匹配或者 CRL 无效，则会与该规则条件匹配。

示例：用于监控或阻止协议版本的 解密规则

本示例显示了如何阻止网络上不再被视为安全的 TLS 和 SSL 协议，例如 TLS 1.0、TLS 1.1 和 SSLv3。包含这些内容是为了让您更详细地了解协议版本规则的工作方式。

您应该从网络中排除不安全的协议，因为它们都可能会被利用。在本例中：

- 您可以使用 解密规则上的**版本 (Version)** 页面来阻止某些协议。
- 由于系统会将 SSLv2 视为无法解密，因此您可以对 解密策略使用 **无法解密的操作** 来阻止它。
- 同样，由于不支持压缩的 TLS/SSL，因此您也应将其阻止。

重要事项 仅在具有**阻止**或**阻止并重置**规则操作的规则中使用**密码套件 (Cipher Suite)** 和**版本 (Version)** 规则条件。不要将**密码套件**和**版本**与**解密 - 重新签名**或**解密 - 已知密钥**规则操作一起使用。在具有其他规则操作的规则中，这些条件可能会干扰系统的 ClientHello 处理，从而导致不可预测的性能。

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 解密策略旁边的 **编辑** (✎) 。

步骤 4 点击 解密规则旁的 **编辑** (✎) 。

步骤 5 点击**添加规则**。

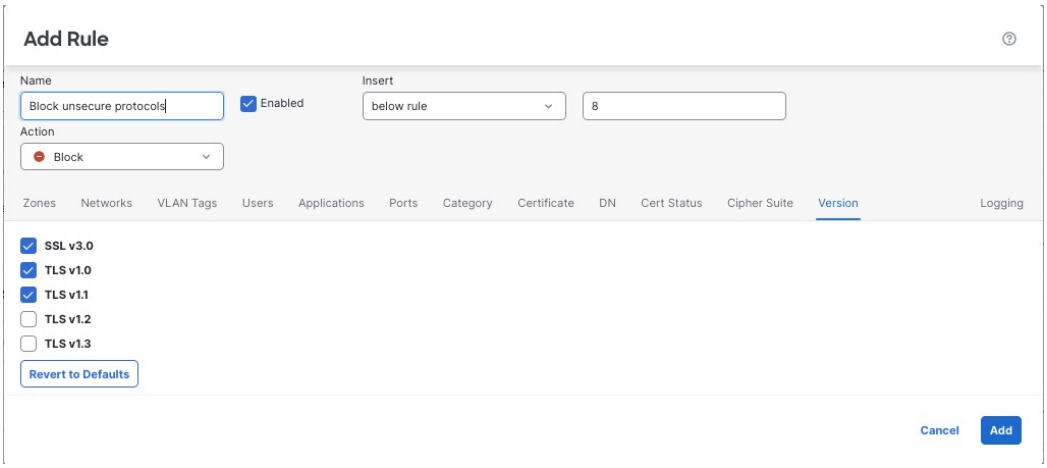
步骤 6 在“添加规则”对话框中，在**名称**字段中输入规则的名称。

步骤 7 从**操作 (Action)** 列表中，点击**阻止 (Block)** 或**阻止并重置 (Block with reset)**。

步骤 8 点击**版本 (Version)** 页面。

步骤 9 选中不再安全的协议的复选框，例如 **SSL v3.0**、**TLS 1.0** 和 **TLS 1.1**。取消选中仍被视为安全的任何协议的复选框。

下图显示了一个示例。



步骤 10 根据需要选择其他规则条件。

步骤 11 点击**添加 (Add)**。

可选示例：手动 解密规则 以监控或阻止证书可分辨名称

包含此规则是为了让您了解如何根据服务器证书的可分辨名称来监控或阻止流量。将其包含在内是为了向您提供更多详细信息。

可分辨名称可以包含国家/地区代码、公用名、组织和组织单位，但通常只会包含一个公用名。例如，`https://www.cisco.com` 的证书中的公用名为 `cisco.com`。（但这并非总是那么简单；《*Cisco Secure Firewall Management Center* 设备配置指南》可分辨名称规则条件部分介绍了如何查找常用名称。）

客户端请求中 URL 的主机名部分是服务器名称指示 (SNI)。客户端会使用 TLS 握手中的 SNI 扩展名来指定要连接的主机名（例如，`auth.amp.cisco.com`）。然后，服务器会选择在单个 IP 地址上托管所有证书时建立连接所需的相应私钥及证书链。

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 解密策略旁边的 **编辑** (✎) 。

步骤 4 点击 解密规则旁的 **编辑** (✎) 。

步骤 5 点击**添加规则**。

步骤 6 在“添加规则”对话框中，在**名称**字段中输入规则的名称。

步骤 7 从**操作 (Action)** 列表中，点击**阻止 (Block)** 或**阻止并重置 (Block with reset)**。

步骤 8 点击 **DN**。

步骤 9 从**可用 DN (Available DNs)** 中查找要添加的可分辨名称，如下所示：

- 要即时添加可随后添加到条件中的可分辨名称，请点击**可用 DN (Available DNs)** 列表上方的 **添加** (+)。
- 要搜索将添加的可分辨名称对象和组，请点击**可用 DN (Available DNs)** 列表上方的**按名称或值搜索 (Search by name or value)** 提示，然后键入对象的名称或对象中的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 10 要选择对象，请点击该对象。要选择所有对象，请点击右键，然后是 **全选**。

步骤 11 点击**添加到使用者 (Add to Subject)** 或**添加到颁发者 (Add to Issuer)**。

提示
您也可以拖放选定对象。

步骤 12 添加要手动指定的所有文本公用名或可分辨名称。点击**使用者 DN (Subject DNs)** 或**颁发者 DN (Issuer DNs)** 列表下方的**输入 DN 或 CN (Enter DN or CN)** 提示，然后键入公用名或可分辨名称并点击**添加 (Add)**。

虽然您可以将 CN 或 DN 添加到任一列表，但更常见的是将它们添加到**使用者 DN (Subject DNs)** 列表。

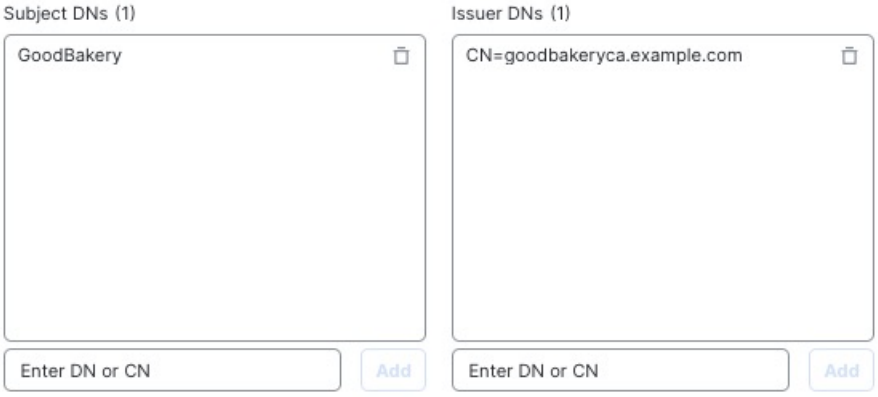
步骤 13 添加或继续编辑规则。

步骤 14 完成后，要保存对规则的更改，请点击页面底部的**添加**。

步骤 15 要保存对策略的更改，请点击页面顶部的**保存**。

示例

下图显示了用于搜索向 goodbakery.example.com 颁发或由 goodca.example.com 颁发的证书的可分辨名称规则条件。根据访问控制，允许通过这些证书加密的流量。



将 解密策略 与访问控制策略和高级设置关联

此任务讨论如何将 解密策略 与访问控制策略相关联，以及如何为访问控制策略设置建议的高级设置。

要使系统使用您的 解密策略，您必须将其与访问控制策略相关联。

开始之前

创建本指南中讨论的解密策略样本。

有关 解密策略 高级选项的更多信息，请参阅《*Cisco Secure Firewall Management Center* 设备配置指南》中的 解密策略 高级选项。

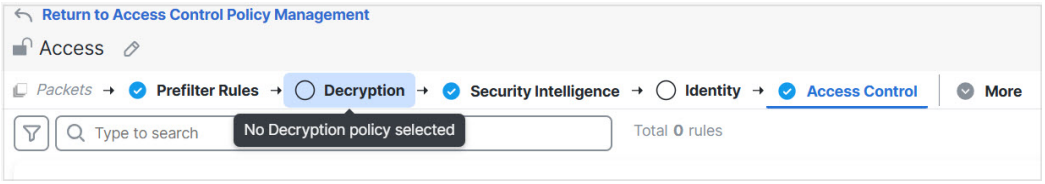
过程

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

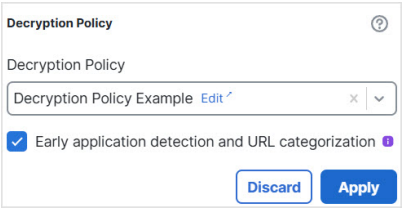
步骤 2 请点击 **策略** > **访问控制标题** > **访问控制**。

步骤 3 创建新的访问控制策略，或者点击 **编辑** (✎) 以编辑现有策略。

步骤 4 点击“解密”(Decryption) 字样，如下图所示。

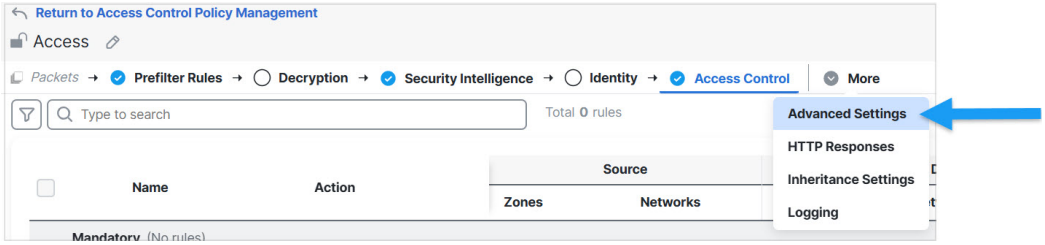


步骤 5 从列表中，点击解密策略的名称，并选中**早期应用检测和 URL 分类 (Early application detection and URL categorization)**，如下图所示。



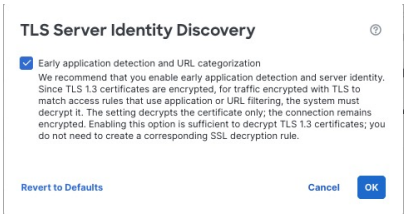
步骤 6 点击**应用 (Apply)**。

步骤 7 点击**更多 (More)** > **高级设置 (Advanced Settings)**，如下图所示。



步骤 8 点击 **TLS 服务器身份发现 (TLS Server Identity Discovery)** 旁的 **编辑** ()。

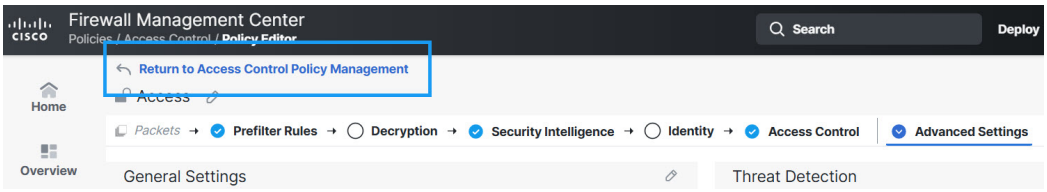
步骤 9 选中复选框，如下图所示。



步骤 10 点击**确定**。

步骤 11 在该页面顶部，点击**保存**。

步骤 12 在页面顶部，点击**返回到访问控制策略管理 (Return to Access Control Policy Management)**，如下图所示



步骤 13 点击 **编辑** () 以编辑的访问控制规则。

步骤 14 在页面底部的默认操作旁边，点击  （默认日志记录和检测）。

步骤 15 选中**连接开始时的日志 (Log at beginning of connection)** 和您选择的任何其他选项。

有关详细信息，请参阅《*Cisco Secure Firewall Management Center* 设备配置指南》中的 访问控制策略的日志记录设置访问控制策略的日志记录设置。

步骤 16 点击**应用 (Apply)**。

步骤 17 在该页面顶部，点击**保存**。

下一步做什么

- 解密规则 条件。

- 添加默认策略操作：《*Cisco Secure Firewall Management Center* 设备配置指南》中的 解密策略默认操作。
- 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。
- 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。

要预过滤的流量

在系统执行更多资源密集型评估之前，预过滤是访问控制的第一阶段。与后续评估相比，预过滤简单、快速、及时，它使用内部报头并具有更强大的检测功能。

根据您的安全需求和流量量变曲线，您应该考虑使用预过滤，以便从任何策略和检查中排除以下内容：

- 常见的办公室内应用，例如 Microsoft Outlook 365
- 大象流，例如服务器备份

解密规则 设置

如何为 解密规则配置建议的最佳实践设置。

解密规则：为每个规则启用日志记录，但具有 **不解密** 规则操作的规则除外。（这取决于您；如要查看有关未解密的流量的信息，请同时启用这些规则的日志记录。）

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 解密策略旁边的 **编辑** (✎) 。
步骤 4 点击 解密规则旁的 **编辑** (✎) 。
步骤 5 点击**日志记录**选项卡。
步骤 6 点击**在连接结束时记录 (Log at End of Connection)**。
步骤 7 点击**保存**。
步骤 8 点击页面顶部的**保存**。

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。