TLS/SSL 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 TLS/SSL 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：

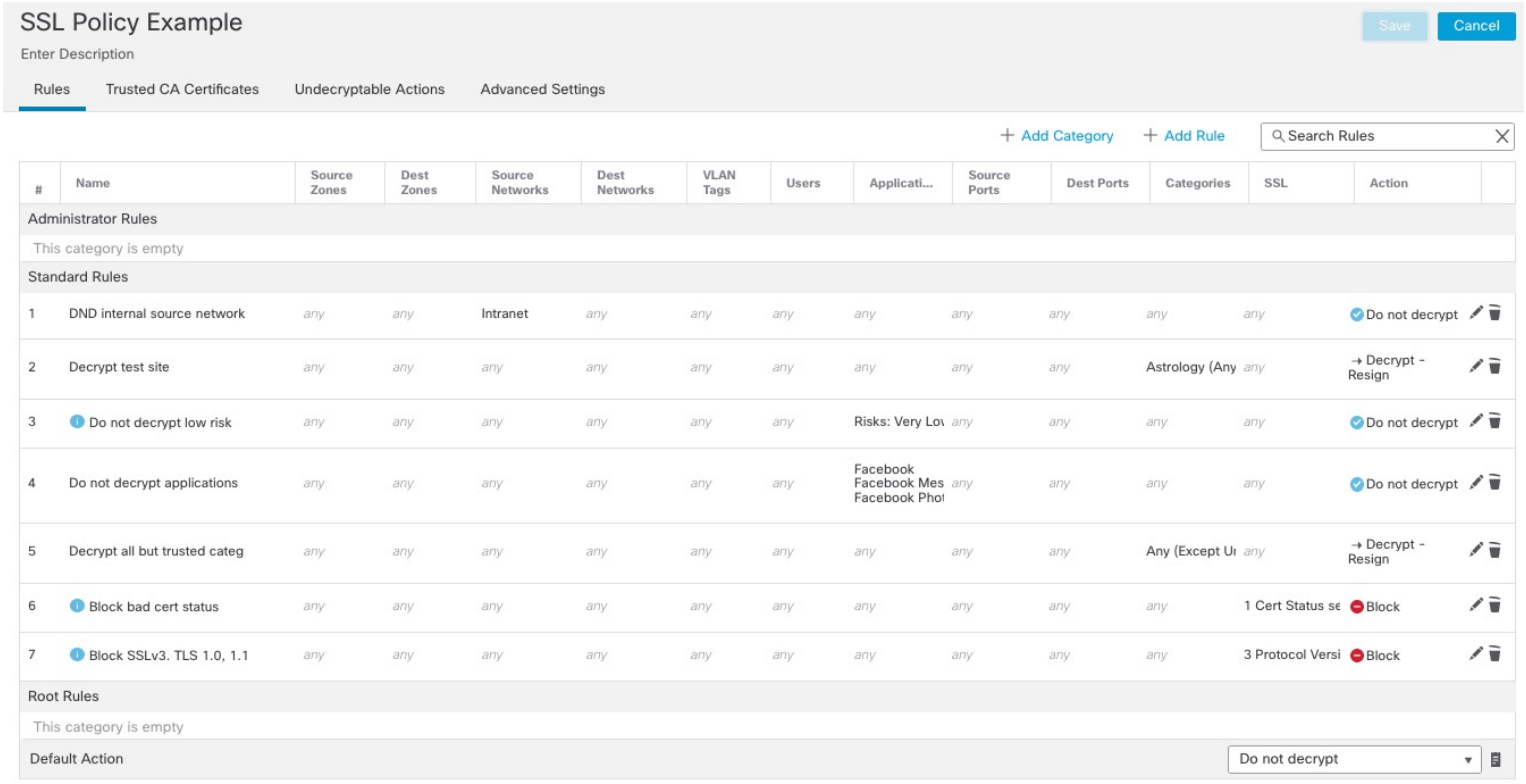
- 对于受信任的流量（例如传输大型压缩服务器备份），可使用预过滤和流量分流完全绕过检查。
- 将可以快速评估的任何 TLS/SSL 规则 规则放在 最前面 ， 例如适用于特定 IP 地址的规则。
- 将需要处理的任何规则、**解密 - 重新签署**规则以及阻止不安全协议版本和密码套件的 TLS/SSL 规则 规则放在 最后 。

- TLS/SSL 规则 最佳实践 ， 第 1 页
- SSL 策略 逐步指导 ， 第 4 页

TLS/SSL 规则 最佳实践

本章提供了 TLS/SSL 规则 的一个示例 SSL 策略，用于说明我们的最佳实践和建议。首先，我们将讨论 SSL 和访问控制策略的设置，然后再介绍所有规则以及我们建议以特定方式对其进行排序的原因。

以下是我们将在本章中讨论的 SSL 策略。



使用预过滤器和数据流分流绕过检测

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。预过滤非常简单、快速并且可以及早执行。预过滤使用有限的外部报头条件来快速处理流量。将此过滤操作与后续评估进行比较，后续评估使用内部报头并具有更强大的检测功能。

配置预过滤：

- 提高性能 - 越早排除不需要检查的流量，越好。您可以基于隧道的外部封装报头传递隧道为某些类型的明文设置快速路径或加以阻止，而不检查其封装的连接。您还可以为从及早处理中受益的其他任何连接设置快速路径或加以阻止。
- 为封装流量定制深度检查 - 您可以对某些类型的隧道重新分区，以便以后可以使用相同的检查标准处理其封装的连接。重新分区是必要的，因为在预过滤后，访问控制使用内部报头。

如果有可用的 Firepower 4100/9300，则可以使用大型流量分流，这种技术可以让受信任的流量绕过检测引擎以获得更好的性能。例如，您可以在数据中心使用它来传输服务器备份。

相关主题

大型流量分流

预过滤与访问控制

快速路径预过滤的最佳实践

不解密最佳实践

记录流量

我们建议不要创建未记录任何内容的**不解密**规则，因为这些规则在托管设备上仍需要处理时间。如果设置了任何类型的 TLS/SSL 规则，请启用日志记录，以便您可以查看匹配的流量。

无法解密的流量准则

我们可以确定某些流量不可解密，要么是因为网站本身不可解密，要么是因为该网站使用了 SSL 锁定，这有效地阻止了用户访问其浏览器中没有错误的已解密网站。

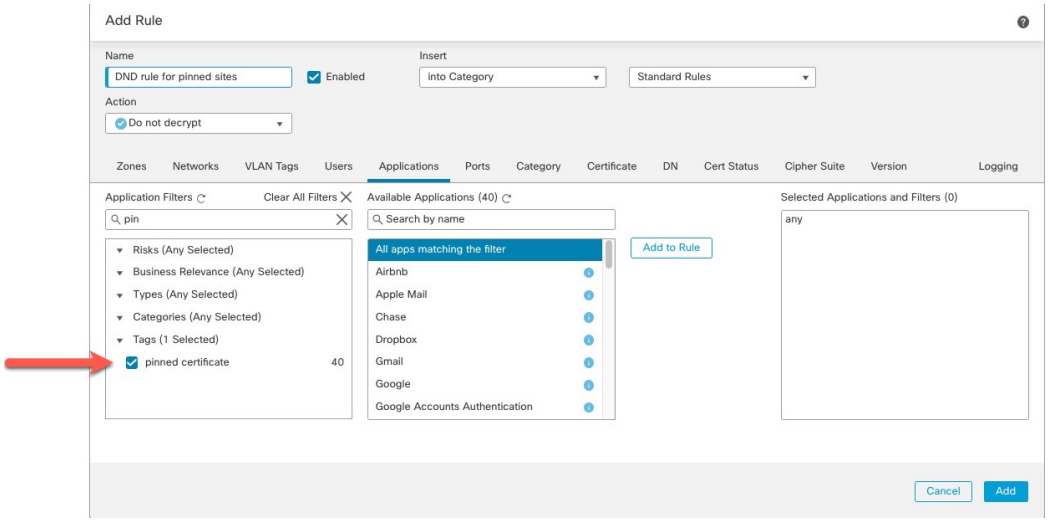
有关证书锁定的详细信息，请参阅关于 TLS/SSL 锁定。

我们维护的这些站点的列表如下：

- 名为 **Cisco-Undecryptable-Sites** 的可分辨名称 (DN) 组
- **已固定证书**应用过滤器

如果您正在解密流量，并且不希望用户在访问这些站点时在其浏览器中看到错误，我们建议您在 TLS/SSL 规则 底部设置**不解密规则**。

设置**已固定证书**应用过滤器的示例如下。



解密 - 重新签名和解密 - 已知密钥最佳实践

本主题讨论**解密 - 重新签名**和**解密 - 已知密钥** TLS/SSL 规则 的最佳实践。

解密 - 使用证书锁定的重新签名最佳实践

某些应用使用称为 *TLS/SSL* 锁定或证书锁定的技术，其在应用自身中嵌入原始服务器证书的指纹。因此，如果您配置具有**解密 - 重签**操作的 TLS/SSL 规则，则应用从受管设备收到重签的证书时，验证会失败且连接会中止。

由于 TLS/SSL 锁定用于避免中间人攻击，因此无法不能将其阻止或绕过。您有以下选择：

- 为排在**解密 - 重签**规则之前的应用创建**不解密**规则。
- 指示用户使用网络浏览器访问应用。

有关证书锁定的详细信息，请参阅关于 TLS/SSL 锁定。

解密 - 已知密钥最佳实践

由于**解密 - 已知密钥**规则操作用于流向内部服务器的流量，因此应始终将目标网络添加到这些规则（ **网络**规则条件）。这样，流量会直接进入服务器所在的网络，从而减少网络上的流量。

优先考虑 TLS/SSL 规则

将数据包的第一部分可以匹配的任何规则放在最前面；例如，引用IP地址的规则（**网络**规则条件）。

TLS/SSL 规则 放在最后

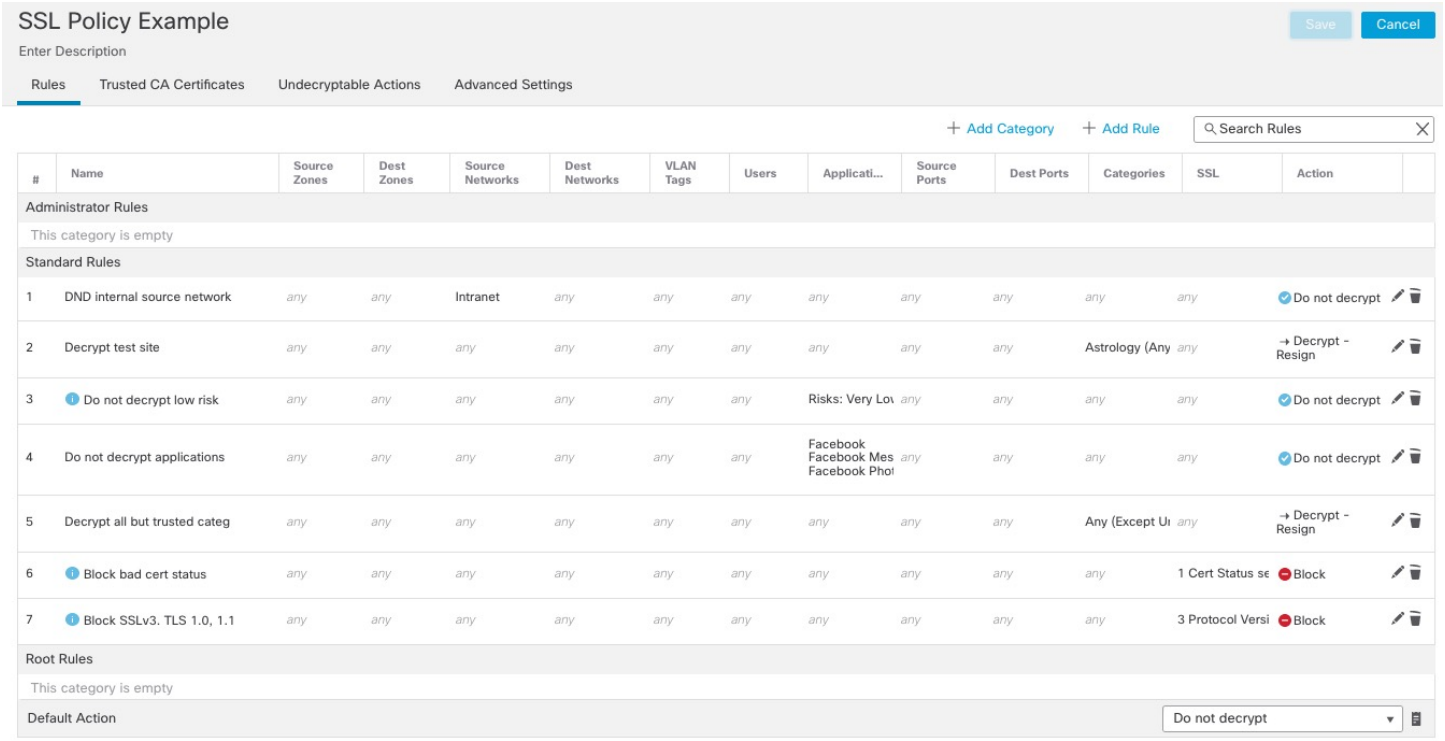
具有以下规则条件的规则应放在最后，因为这些规则要求系统在最长时间内检查流量：

- 应用
- 类别 (Category)
- 证书
- 可分辨名称 (DN)
- 证书状态
- 密码套件
- 版本

SSL 策略 逐步指导

本章提供有关如何使用我们的最佳实践规则来创建 SSL 策略的分步讨论和演练。您将看到 SSL 策略的预览，然后是最佳实践的概要，最后是对策略中规则进行的讨论。

以下是我们将在本章中讨论的 SSL 策略。



有关详细信息，请参阅以下各节之一：

相关主题

建议的策略和规则设置，第 5 页
要预过滤的流量，第 9 页
第一条 TLS/SSL 规则：不解密特定流量，第 9 页
下一条 TLS/SSL 规则：解密特定测试流量，第 10 页
创建解密 - 类别的重新签名规则，第 13 页
不解密低风险类别、信誉或应用，第 11 页
最后的 TLS/SSL 规则：阻止或监控证书和协议版本，第 14 页

建议的策略和规则设置

我们建议使用以下策略设置：

- SSL 策略：
  - 默认操作：**不解密**。
  - 启用日志记录。
  - 将 **SSL v2 会话 (SSL v2 Session)** 和压缩会话 **(Compressed Session)** 的无法解密的操作 **(Undecryptable Actions)** 同时设置为**阻止 (Block)**。
  - 在策略的高级设置中启用 TLS 1.3 解密。

- TLS/SSL 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。）
- 访问控制策略：
  - 将 SSL 策略 与访问控制策略关联。（如果不这样做， SSL 策略 和规则将不会起作用。）
  - 将默认策略操作设为**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)**。
  - 启用日志记录。

相关主题

SSL 策略 设置，第 6 页
TLS/SSL 规则 设置，第 21 页
访问控制策略设置，第 7 页

SSL 策略 设置

如何为 SSL 策略配置以下建议的最佳实践设置：

- 默认操作：**不解密**。
- 启用日志记录。
- 将 **SSL v2 会话 (SSL v2 Session)** 和**压缩会话 (Compressed Session)** 的**无法解密的操作 (Undecryptable Actions)** 同时设置为**阻止 (Block)**。
- 在策略的高级设置中启用 TLS 1.3 解密。

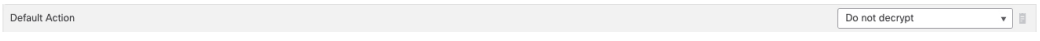
过程

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 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略 旁边的 **编辑**（）。

步骤 4 从页面底部的**默认操作 (Default Action)** 列表中，点击**不解密 (Do Not Decrypt)**。
下图显示了一个示例。



步骤 5 在行的末尾位置，点击 **日志记录**（）。

步骤 6 选中**在连接结束时记录 (Log at End of Connection)** 复选框。

步骤 7 点击**确定 (OK)**。

步骤 8 点击**保存 (Save)**。

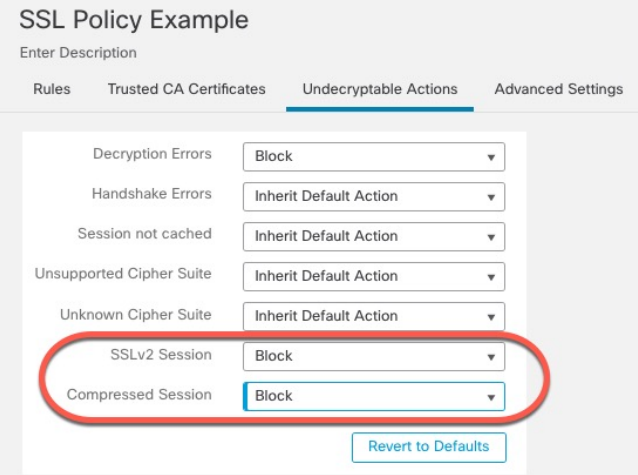
步骤 9 选择**无法解密的操作 (Undecryptable Actions)** 选项卡。

步骤 10 我们建议将 **SSLv2 会话 (SSLv2 Session)** 和**压缩的会话 (Compressed Session)** 的操作设置为**阻止 (Block)**。

您的网络上不应允许 SSL v2，并且不支持压缩的 TLS/SSL 流量，因此您也应阻止该流量。

有关设置每个选项的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》的部分。

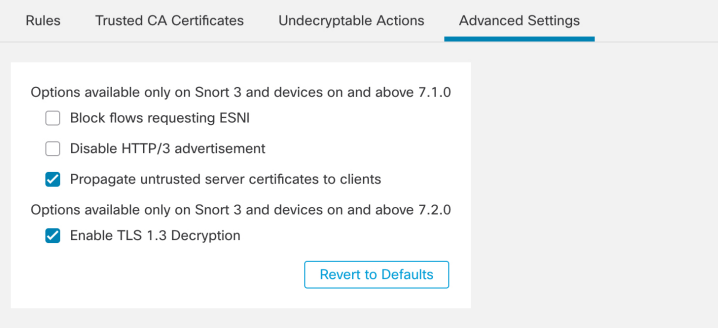
下图显示了一个示例。



步骤 11 点击**高级设置 (Advanced Settings)** 选项卡页面。

步骤 12 选中**启用 TLS 1.3 解密 (Enable TLS 1.3 Decryption)** 复选框。

以下为示例。



步骤 13 在该页面顶部，点击**保存**。

下一步做什么

配置 TLS/SSL 规则 规则并设置每个规则，如TLS/SSL 规则 设置，第 21 页中所述。

访问控制策略设置

如何为访问控制策略配置以下建议的最佳实践设置：

- 将 SSL 策略 与访问控制策略关联。（如果不这样做， SSL 策略 和规则将不会起作用。）
- 将默认策略操作设为**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)**。
- 启用日志记录。

过程

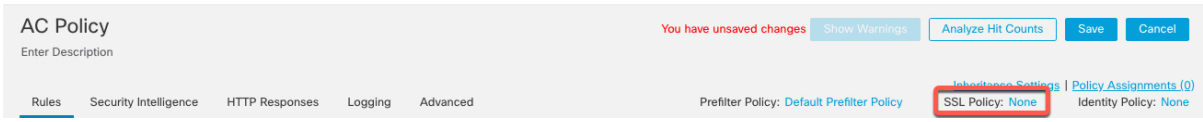
步骤 1 如果尚未登录，请登录Cisco Secure Firewall Management Center。

步骤 2 请点击 **策略** > **访问控制**。

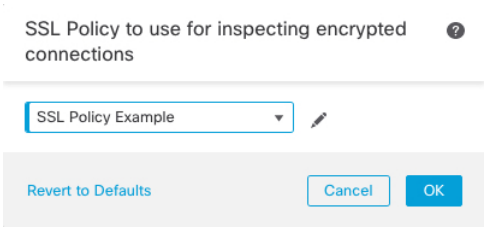
步骤 3 点击访问控制策略旁边的 **编辑**（）。

步骤 4 （如果尚未设置 SSL 策略，可以稍后再执行此操作。）

a) 点击页面顶部 **SSL 策略 (SSL Policy)** 旁边的**无 (None)**，如下图所示。



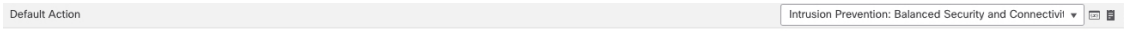
b) 从列表中，点击 SSL 策略的名称。下图显示了一个示例。



c) 点击**确定 (OK)**。

d) 在该页面顶部，点击**保存**。

步骤 5 从页面底部的**默认操作 (Default Action)** 列表中，点击**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)**。
下图显示了一个示例。



步骤 6 请点击 **日志记录**（）。

步骤 7 选中**在连接结束时记录 (Log at End of Connection)** 复选框并点击**确定 (OK)**。

步骤 8 点击**保存 (Save)**。

下一步做什么

请参阅TLS/SSL 规则 示例 ，第 9 页。

TLS/SSL 规则 示例

本部分提供阐述最佳实践的 TLS/SSL 规则 规则示例。

有关详细信息，请参阅以下各节之一：

相关主题

要预过滤的流量，第 9 页
第一条 TLS/SSL 规则：不解密特定流量，第 9 页
下一条 TLS/SSL 规则：解密特定测试流量，第 10 页
不解密低风险类别、信誉或应用，第 11 页
创建解密 - 类别的重新签名规则，第 13 页
最后的 TLS/SSL 规则：阻止或监控证书和协议版本，第 14 页

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：

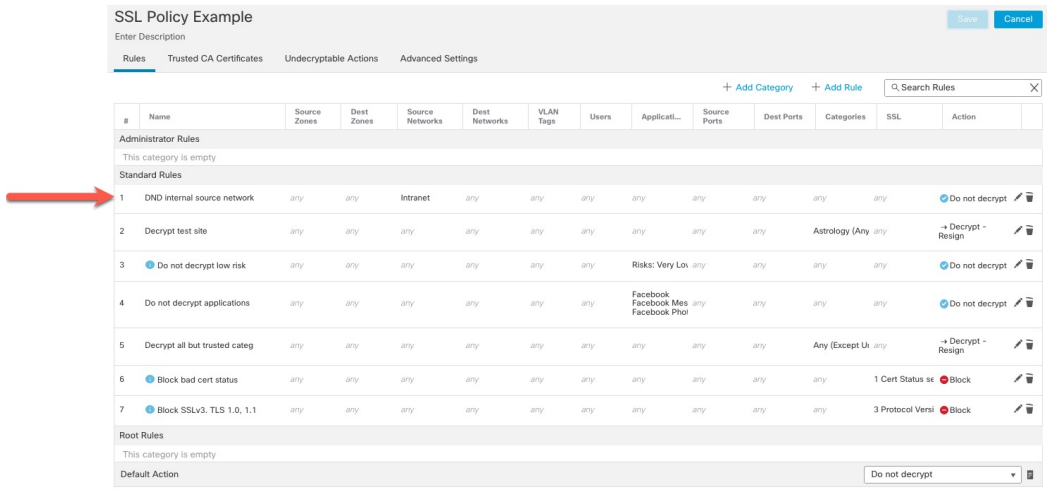
- 常见的办公室内应用，例如 Microsoft Outlook 365
- 大象流，例如服务器备份

相关主题

预过滤与访问控制
快速路径预过滤的最佳实践

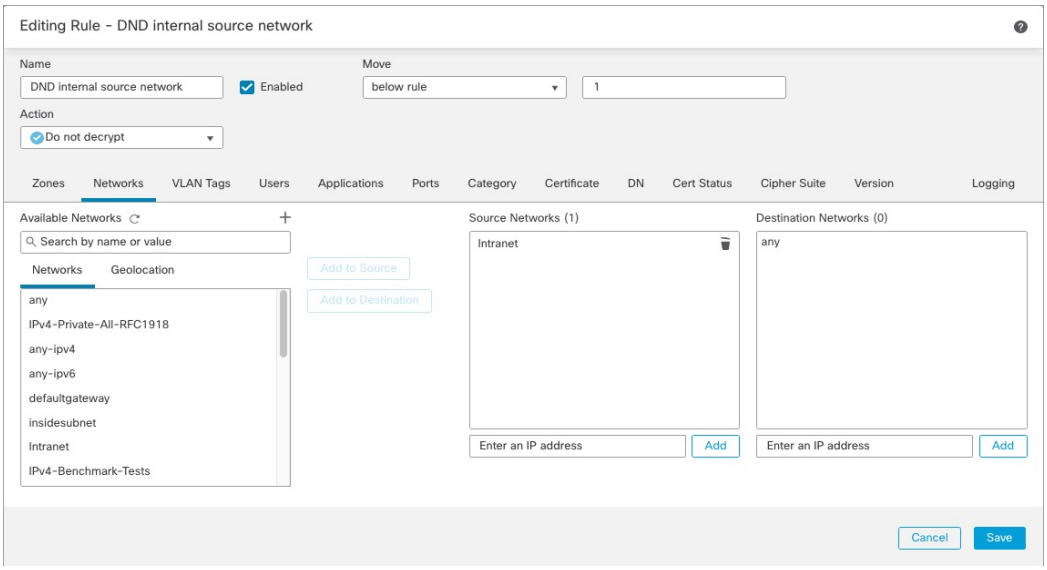
第一条 TLS/SSL 规则：不解密特定流量

示例中的第一条 TLS/SSL 规则 不会解密流向 内部网络（定义为 **intranet**）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。



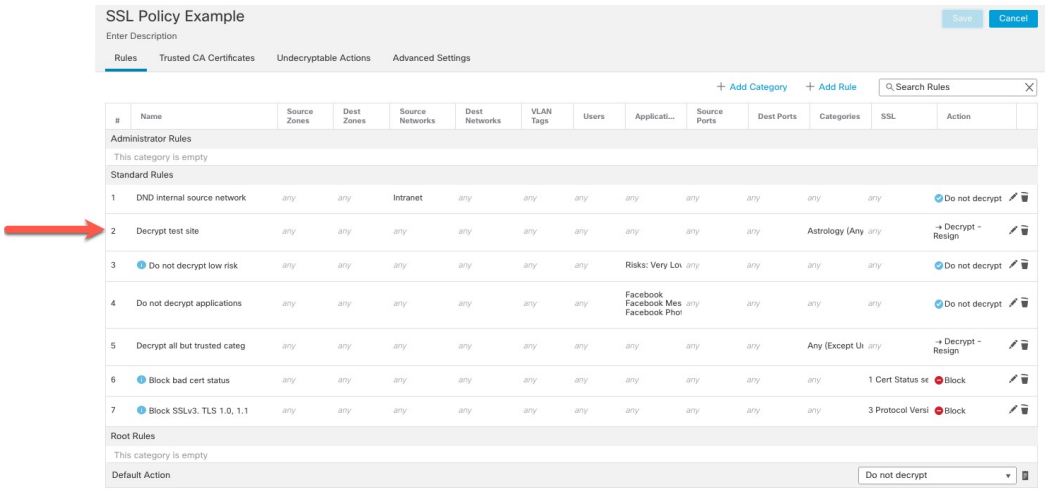
注释 如果您有从内部 DNS 服务器流向内部 DNS 解析器（例如思科 Umbrella 虚拟设备）的流量，则还可以为其添加**不解密规则**。如果内部DNS服务器会执行自己的日志记录，您甚至可以将这些添加到预过滤策略。

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。

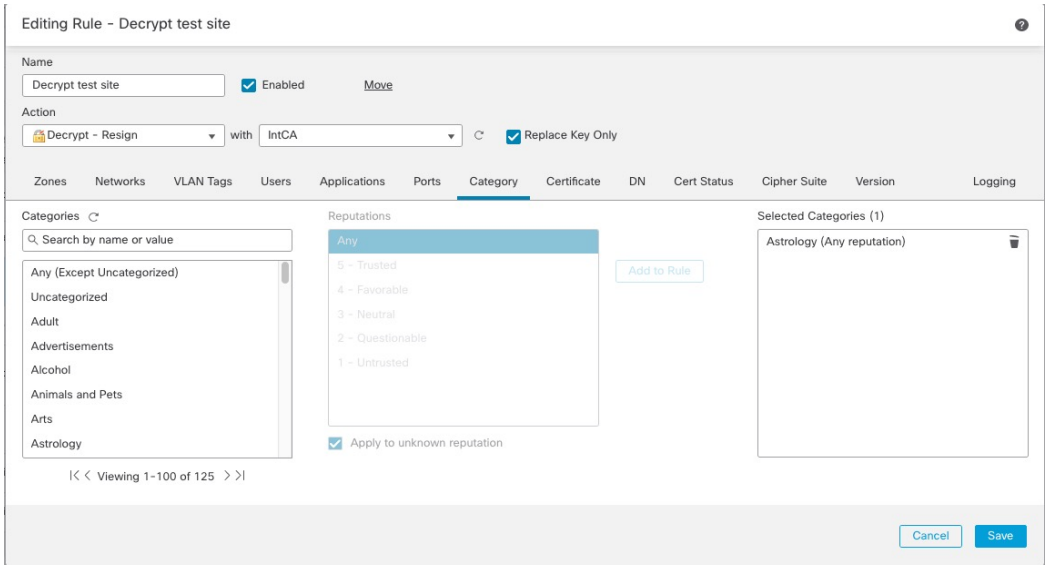


下一条 TLS/SSL 规则：解密特定测试流量

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。



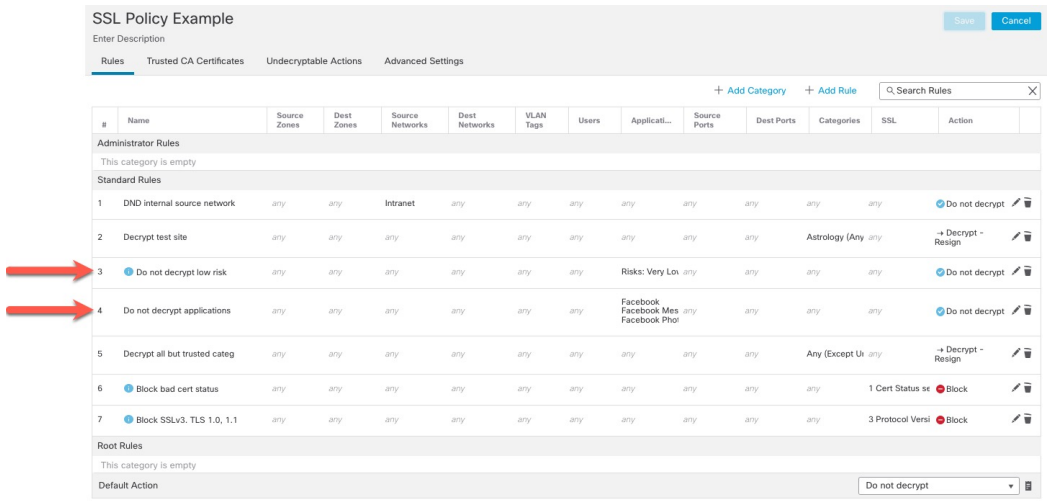
规则详细信息：



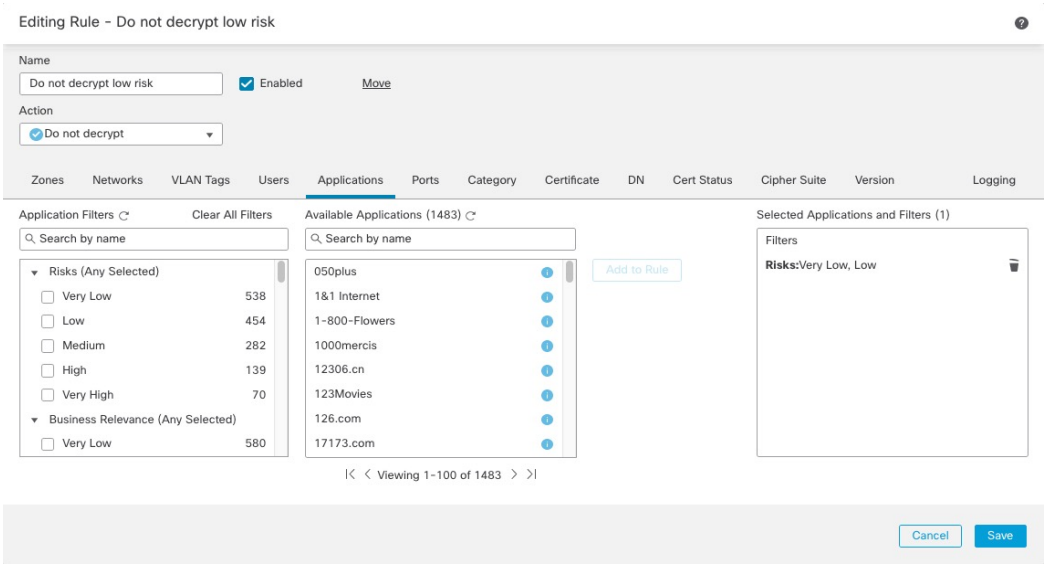
不解密低风险类别、信誉或应用

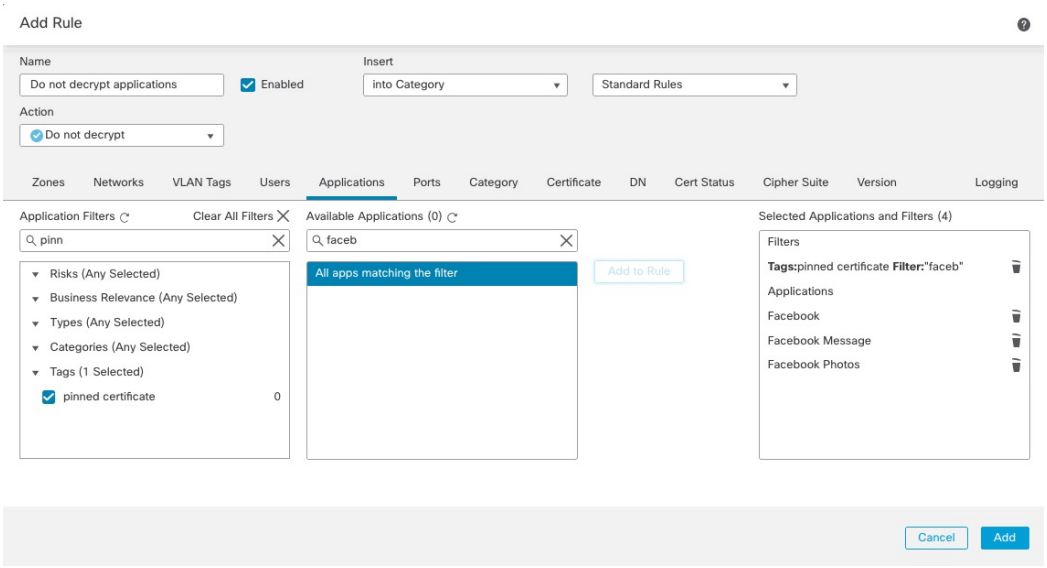
评估网络上的流量，以确定哪些流量与低风险类别、信誉或应用相匹配，并使用**不解密**操作来添加这些规则。将这些规则放在其他更具体的**不解密**规则之后，因为系统需要更多时间来处理流量。

以下为示例。


SSL Policy Example
Enter Description
Save
Cancel
Rules
Trusted CA Certificates
Undecryptable Actions
Advanced Settings
Add Category
Add Rule
Search Rules
Name Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applicati... Source Ports Dest Ports Categories SSL Action
Administrator Rules
This category is empty
Standard Rules
1 DND internal source network Intranet Do not decrypt
2 Decrypt test site Astrology (Any → Decrypt - Resign
3 Do not decrypt low risk Risks: Very Lo Do not decrypt
4 Do not decrypt applications Facebook Facebook Mes Facebook Phot Do not decrypt
5 Decrypt all but trusted categ Any (Except Ur → Decrypt - Resign
6 Block bad cert status 1 Cert Status se Block
7 Block SSLv3. TLS 1.0, 1.1 3 Protocol Versi Block
Root Rules
This category is empty
Default Action
Do not decrypt

规则详细信息：


Editing Rule - Do not decrypt low risk
Name
Do not decrypt low risk
Enabled
Move
Action
Do not decrypt
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging
Application Filters
Clear All Filters
Search by name
Risks (Any Selected)
Very Low 538
Low 454
Medium 282
High 139
Very High 70
Business Relevance (Any Selected)
Very Low 580
Available Applications (1483)
Search by name
050plus
1&1 Internet
1-800-Flowers
1000mercis
12306.cn
123Movies
126.com
17173.com
Viewing 1-100 of 1483
Add to Rule
Selected Applications and Filters (1)
Filters
Risks:Very Low, Low
Cancel
Save



相关主题

配置应用控制的最佳实践

应用控制的建议

创建解密 - 类别的重新签名规则

本主题展示为除未分类站点外的所有站点创建包含 **解密 - 重新签名** 操作的 TLS/SSL 规则 的示例。该规则使用可选的**仅替换密钥 (Replace Key Only)** 选项，我们始终建议将其与**解密 - 重新签名 (Decrypt-Resign)** 规则操作配合使用。

当用户浏览到使用自签名证书的站点时，**仅替换密钥 (Replace Key Only)** 会导致用户在 Web 浏览器中看到安全警告，使用户知道他们正在与不安全的站点通信。

通过将此规则放在底部附近，您可以兼顾两者：您可以解密和（可选）检查流量，同时不会影响性能，就像您将规则放在策略中一样。

过程

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

步骤 2 如果尚未执行此操作，请将内部证书颁发机构 (CA) 上传到 Cisco Secure Firewall Management Center（**对象** > **对象管理**，然后 **PKI** > **内部 CA (Internal CAs)**）。

步骤 3 请点击 **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 4 点击 SSL 策略旁边的 **编辑**（）。

步骤 5 点击**添加规则 (Add Rule)**。

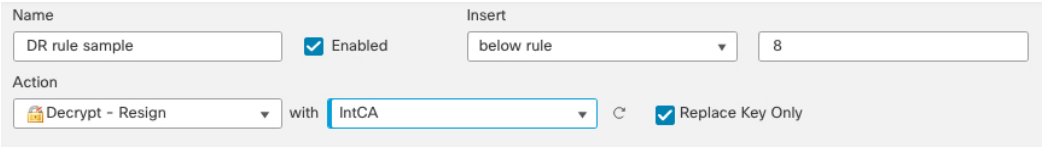
步骤 6 在**名称 (Name)** 字段中，输入用于标识规则的名称。

步骤 7 从**操作 (Action)** 列表中，点击**解密 - 重新签名 (Decrypt - Resign)**。

步骤 8 从**与 (with)** 列表中，点击内部 CA 的名称。

步骤 9 选中**仅替换密钥 (Replace Key Only)** 框。

下图显示了一个示例。



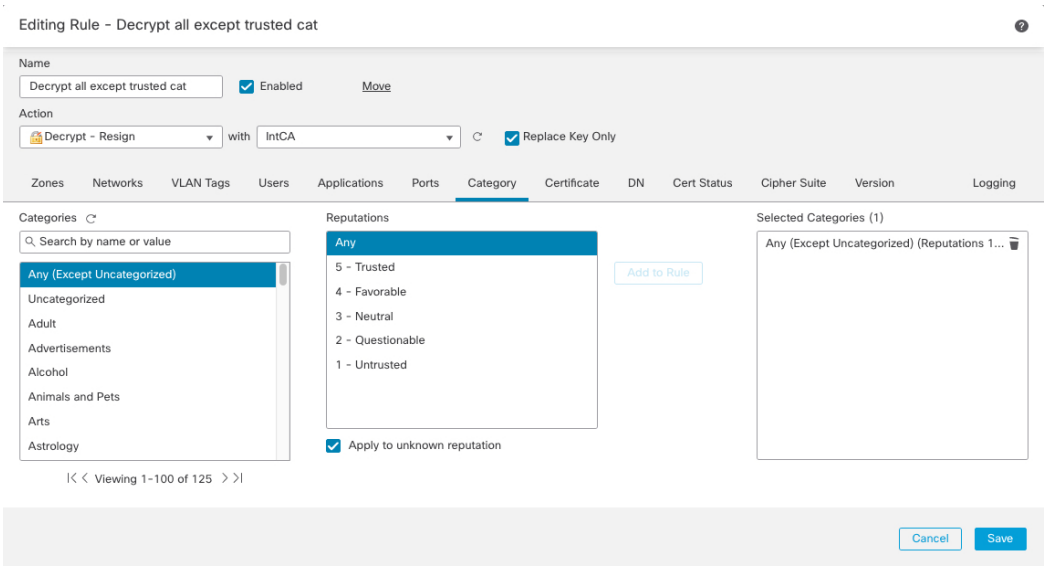
步骤 10 点击**类别 (Category)** 选项卡页面。

步骤 11 从**类别 (Categories)** 列表的顶部，点击**任何（未分类除外）(Any [Except Uncategorized])**。

步骤 12 从**信誉 (Reputations)** 列表中，点击**任意 (Any)**。

步骤 13 点击**添加至规则**。

下图显示了一个示例。

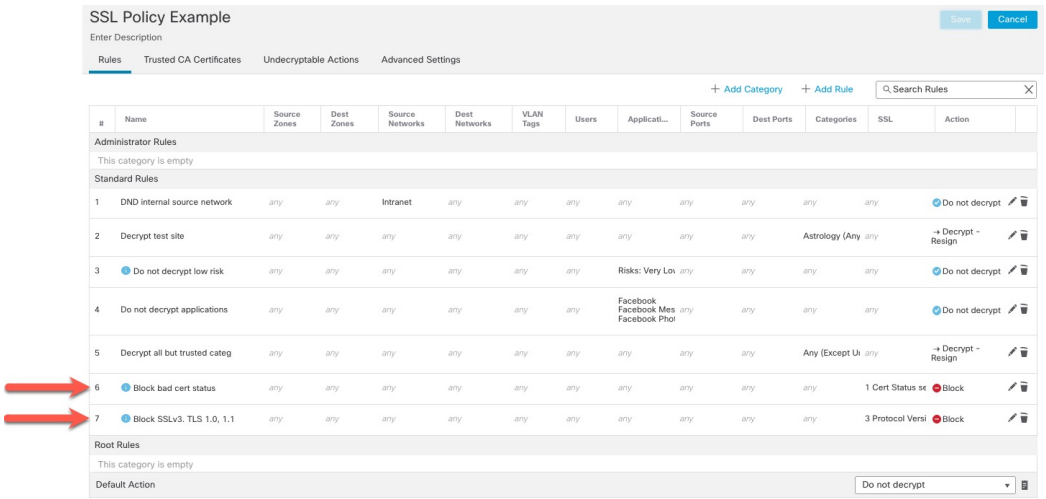


相关主题

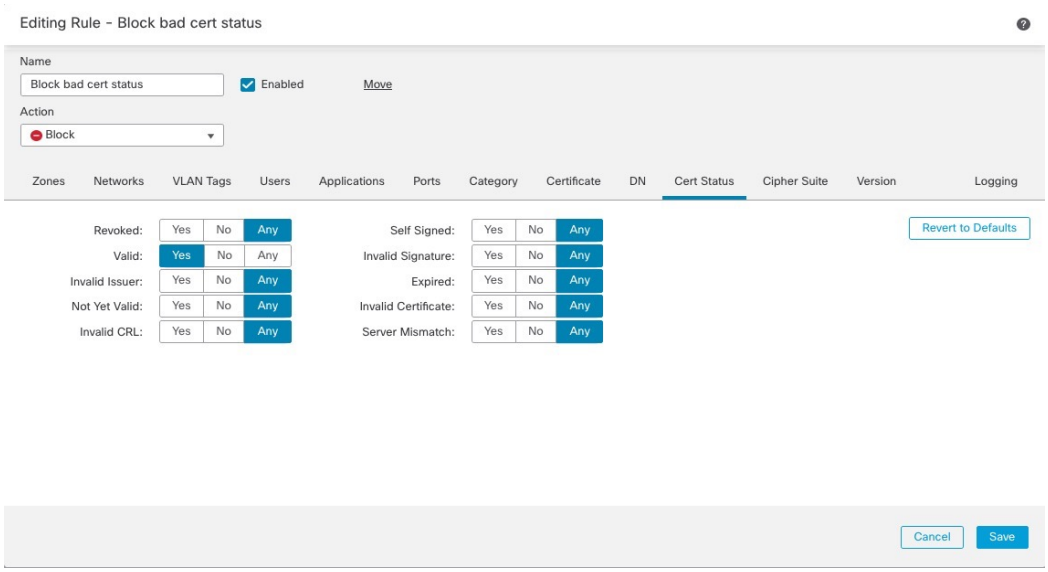
内部证书颁发机构对象

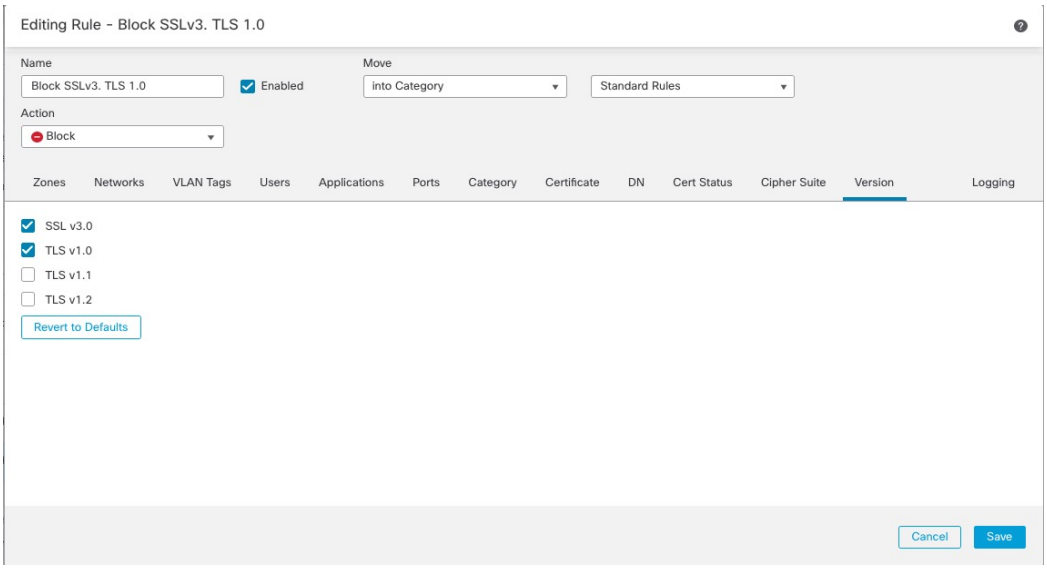
最后的 TLS/SSL 规则：阻止或监控证书和协议版本

由于最后的 TLS/SSL 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。


SSL Policy Example
Enter Description
Save
Cancel
Rules
Trusted CA Certificates
Undecryptable Actions
Advanced Settings
Add Category
Add Rule
Search Rules
Name Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applicati... Source Ports Dest Ports Categories SSL Action
Administrator Rules
This category is empty
Standard Rules
1 DND internal source network Intranet Do not decrypt
2 Decrypt test site Astrology (Any → Decrypt - Resign
3 Do not decrypt low risk Risks: Very Lo Do not decrypt
4 Do not decrypt applications Facebook Facebook Mes Facebook Phot Do not decrypt
5 Decrypt all but trusted categ Any (Except U → Decrypt - Resign
6 Block bad cert status 1 Cert Status se Block
7 Block SSLv3. TLS 1.0, 1.1 3 Protocol Versi Block
Root Rules
This category is empty
Default Action
Do not decrypt

规则详细信息：


Editing Rule - Block bad cert status
Name
Block bad cert status
Enabled
Move
Action
Block
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging
Revoked: Yes No Any
Valid: Yes No Any
Invalid Issuer: Yes No Any
Not Yet Valid: Yes No Any
Invalid CRL: Yes No Any
Self Signed: Yes No Any
Invalid Signature: Yes No Any
Expired: Yes No Any
Invalid Certificate: Yes No Any
Server Mismatch: Yes No Any
Revert to Defaults
Cancel
Save



相关主题

示例： TLS/SSL 规则 监控或阻止证书状态的规则 ， 第 16 页
示例：用于监控或阻止协议版本的 TLS/SSL 规则 ， 第 18 页
可选示例：监控或阻止证书可分辨名称的 TLS/SSL 规则 ， 第 19 页

示例： TLS/SSL 规则 监控或阻止证书状态的规则

由于最后的 TLS/SSL 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。

注释 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。在具有其他规则操作的规则中使用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 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（） 。

步骤 5 点击**添加规则 (Add Rule)**。

步骤 6 在“添加规则”(Add Rule) 对话框中，在**名称 (Name)** 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 (Yes)** 可根据该证书状态是否存在进行匹配。
- 点击**否 (No)** 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**保存 (Save)**。

步骤 11 要保存对策略的更改，请点击页面顶部的**保存 (Save)**。

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。

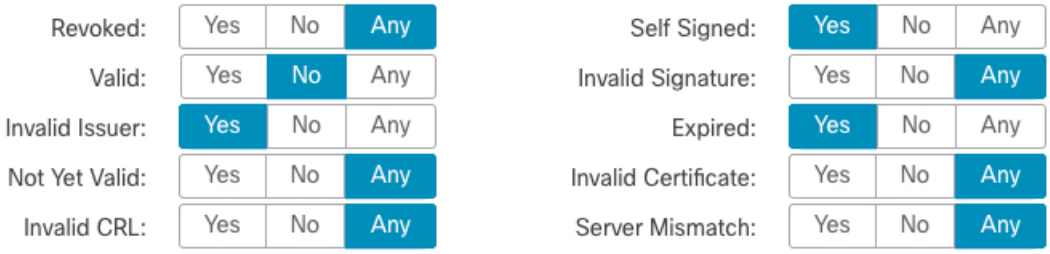
下图说明用于检查有效证书、由“已验证颁发机构”颁发的证书、不在 CRL 上的证书以及仍在有效开始日期和有效结束日期内的证书的证书状态规则条件。受配置原因的影响，未通过访问控制来解密和检查使用这些证书加密的流量。

Revoked:	Yes	No	**Any**	Self Signed:	Yes	No	**Any**
Valid:	**Yes**	No	Any	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	Yes	No	**Any**	Expired:	Yes	No	**Any**
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	Yes	No	**Any**	Server Mismatch:	Yes	No	**Any**

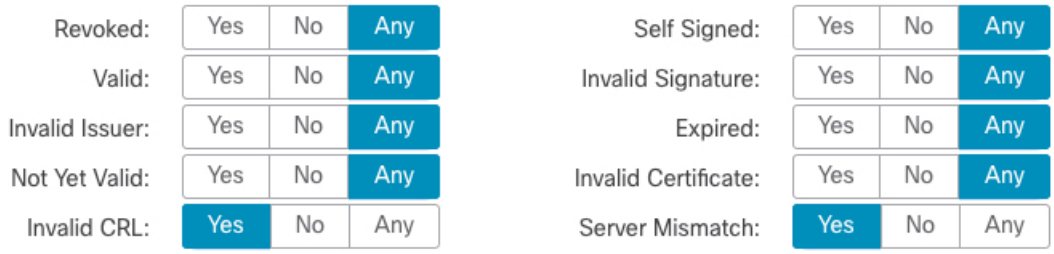
下图显示用于检查状态是否缺失的证书状态规则条件。在此情况下，由于配置原因，它与使用尚未到期的证书加密的流量相匹配并监控该流量。

Revoked:	Yes	No	**Any**	Self Signed:	Yes	No	**Any**
Valid:	Yes	No	**Any**	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	Yes	No	**Any**	Expired:	Yes	**No**	Any
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	Yes	No	**Any**	Server Mismatch:	Yes	No	**Any**

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 TLS/SSL 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 SSL 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 SSL 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。

注释 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。在具有其他规则操作的规则中使用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 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（） 。

步骤 5 点击**添加规则 (Add Rule)**。

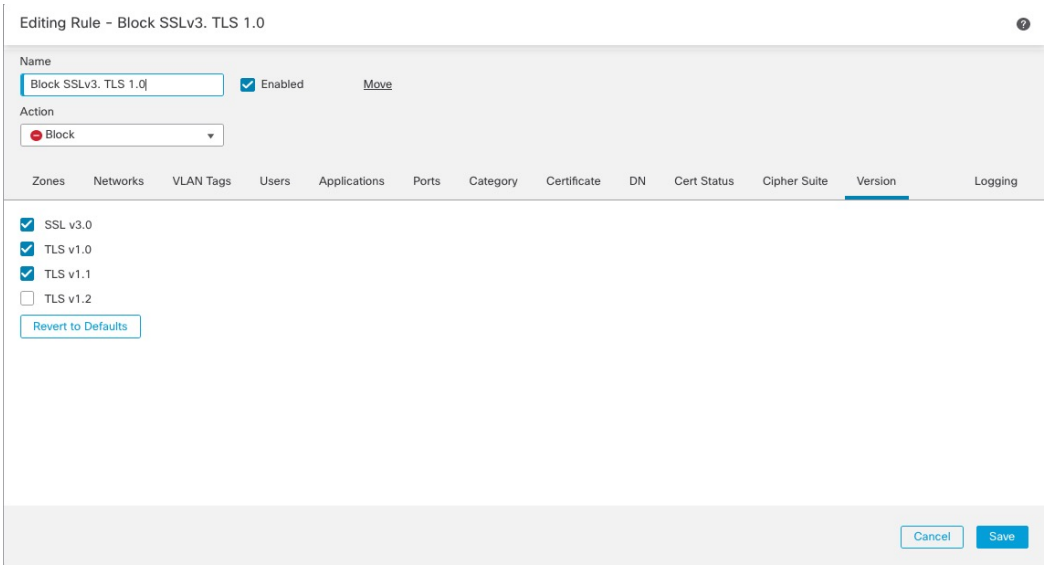
步骤 6 在“添加规则”(Add Rule) 对话框中，在**名称 (Name)** 字段中输入规则的名称。

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**保存 (Save)**。

可选示例：监控或阻止证书可分辨名称的 TLS/SSL 规则

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；可分辨名称 (DN) 规则条件中的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 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（✎）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（✎）。

步骤 5 点击**添加规则 (Add Rule)**。

步骤 6 在“添加规则”(Add Rule) 对话框中，在**名称 (Name)** 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，然后选择**全选 (Select All)**。

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。

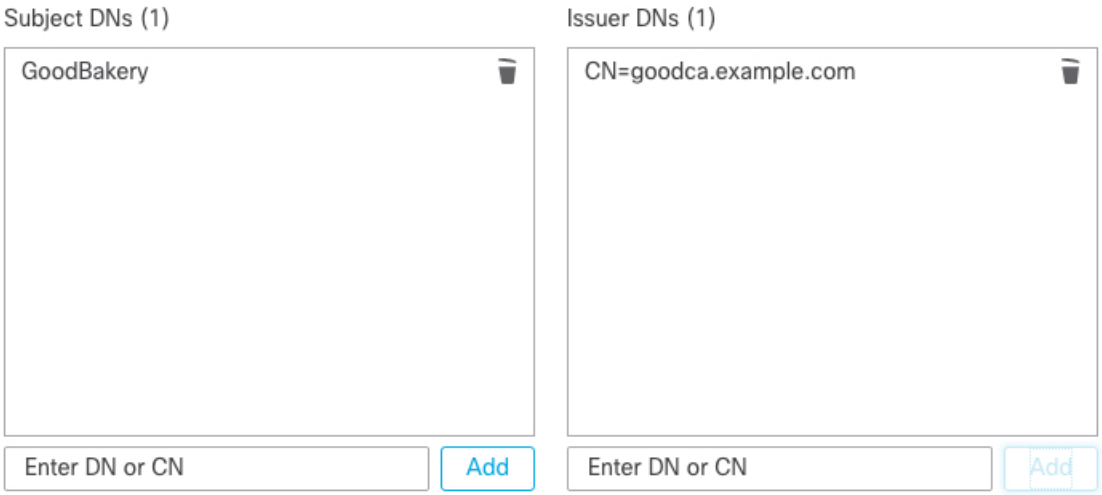
步骤 13 添加或继续编辑规则。

步骤 14 完成后，要保存对规则的更改，请点击页面底部的**保存 (Save)**。

步骤 15 要保存对策略的更改，请点击页面顶部的**保存 (Save)**。

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。



TLS/SSL 规则 设置

如何为TLS/SSL 规则配置建议的最佳实践设置。

TLS/SSL 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 (Policies)** > **访问控制 (Access Control)** > **SSL**。

步骤 3 点击 SSL 策略旁边的 **编辑**（）。

步骤 4 点击 TLS/SSL 规则旁的 **编辑**（） 。

步骤 5 点击**日志记录 (Logging)**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 (Save)**。

步骤 8 点击页面顶部的 **Save**。

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。