在Cisco FireSIGHT系统上配置SSL检查策略

目录

简介
先决条件
使用的组件
配置
1.解密和重新签名
选项 1：将FireSIGHT中心用作根证书颁发机构(CA)
选项 2：让内部CA签署您的证书
选项 3：导入CA证书和密钥
2.使用已知密钥解密
导入已知证书（解密和重新签名的替代选项）
其他配置
确认
解密 — 重新签名
解密 — 已知证书
故障排除
问题 1:某些网站可能未加载到Chrome浏览器上
问题 2:在某些浏览器中获取不受信任的警告/错误
参考
相关的思科支持社区讨论

简介

SSL检查功能允许您阻止加密流量而不对其进行检查，或使用访问控制检查加密或解密的流量。本文档介绍在Cisco FireSIGHT系统上设置SSL检查策略的配置步骤。

先决条件

使用的组件

- 思科FireSIGHT管理中心
- Cisco Firepower 7000或8000设备
- 软件版本5.4.1或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

> **警告：** 如果在受管设备上应用SSL检查策略，可能会影响网络性能。

配置

可以配置SSL检查策略以通过以下方式解密流量：

1.解密和重新签名：

- 选项 1：将FireSIGHT中心用作根证书颁发机构(CA)，或
- 选项 2：让内部CA签署您的证书，或
- 选项 3：导入CA证书和密钥

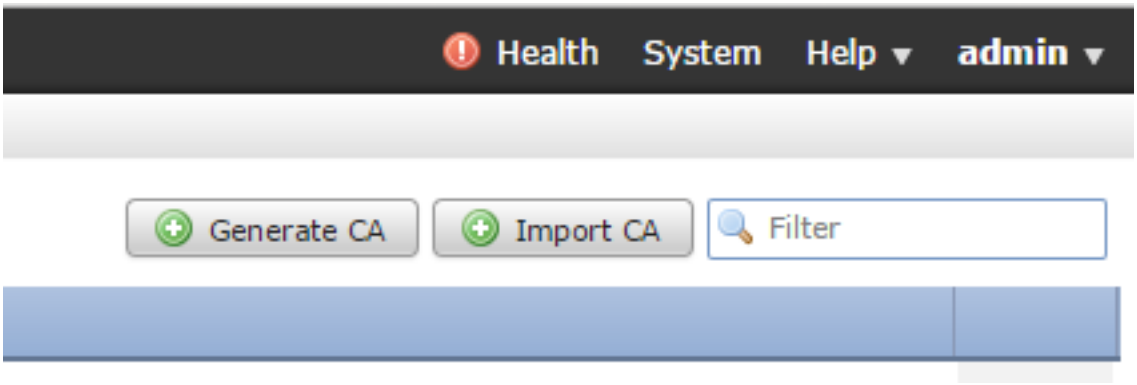
2.使用已知证书解密：

- 登录FireSIGHT管理中心，然后导航至“对**象**”。
- 在“对**象**”页上，展开**PKI**并选择**内部CA**。

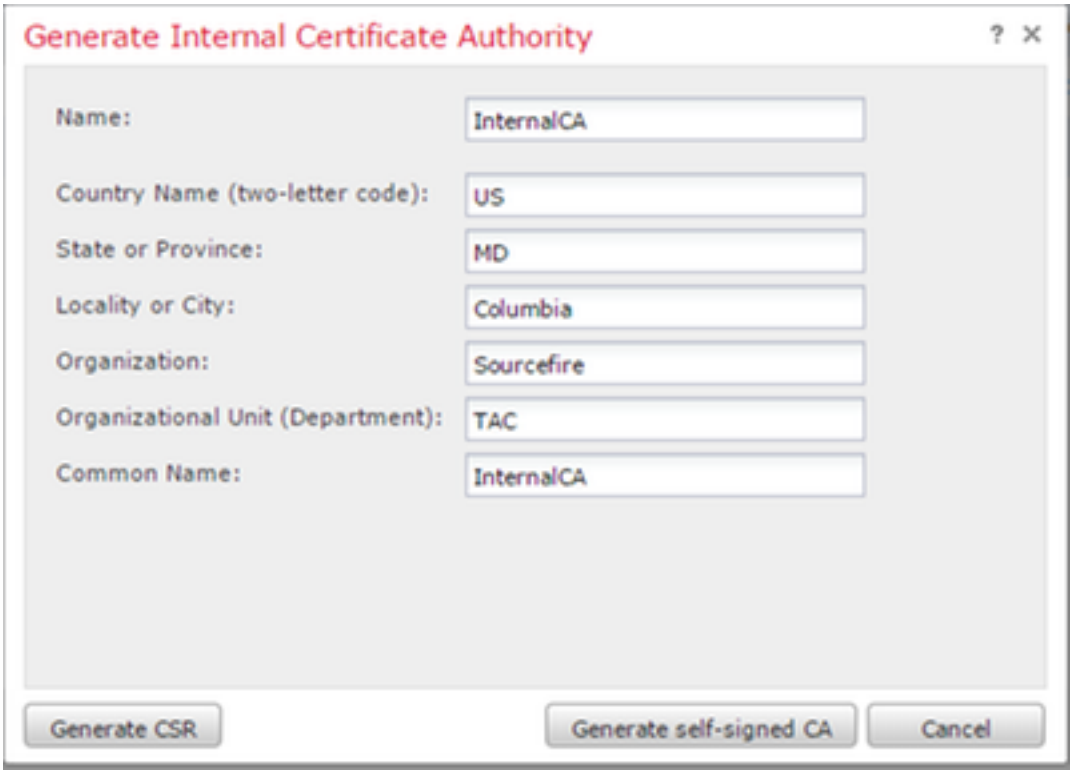
1.解密和重新签名

选项 1：将FireSIGHT中心用作根证书颁发机构(CA)

i.单击“生**成CA**”。



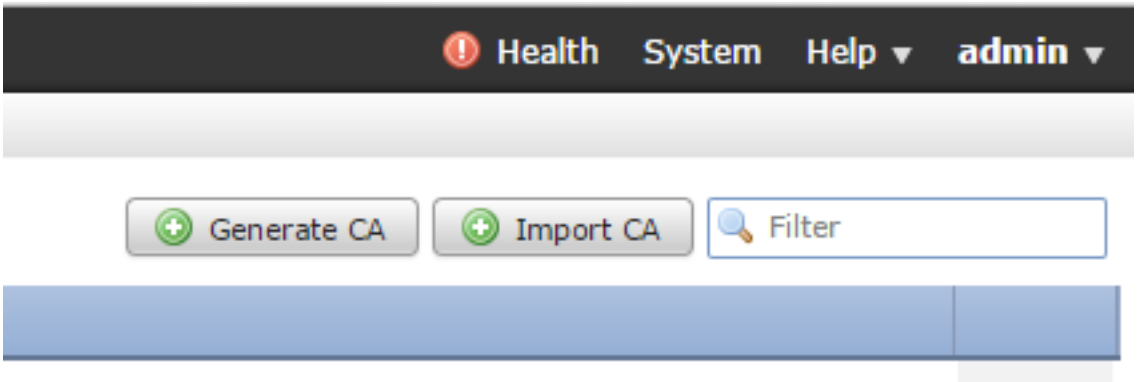
ii。填写相关信息



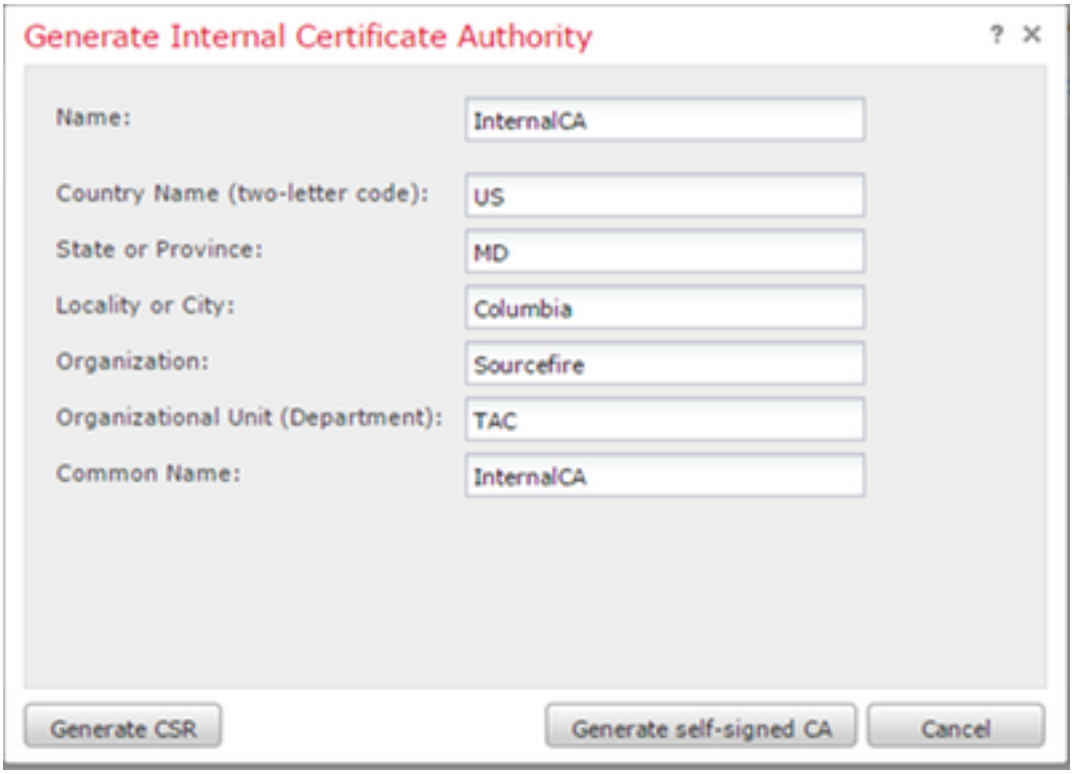
三、单击Generate self-signed CA。

选项 2：让内部CA签署您的证书

我。单击Generate CA。

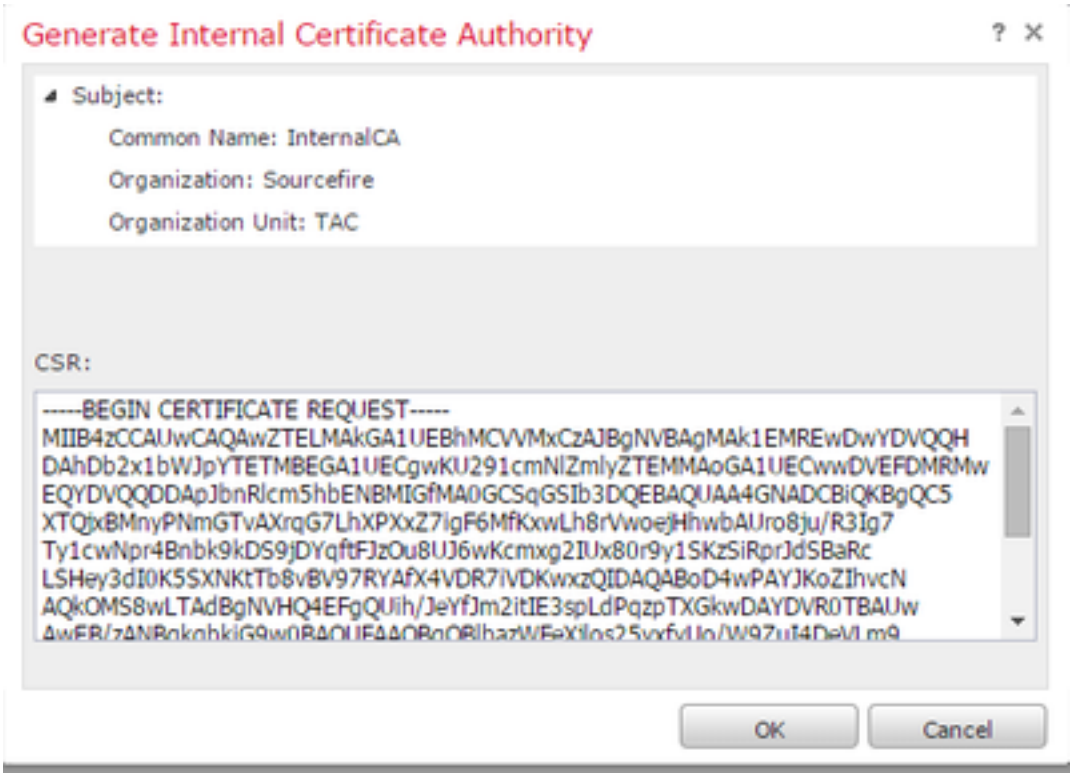


ii。填写相关信息。



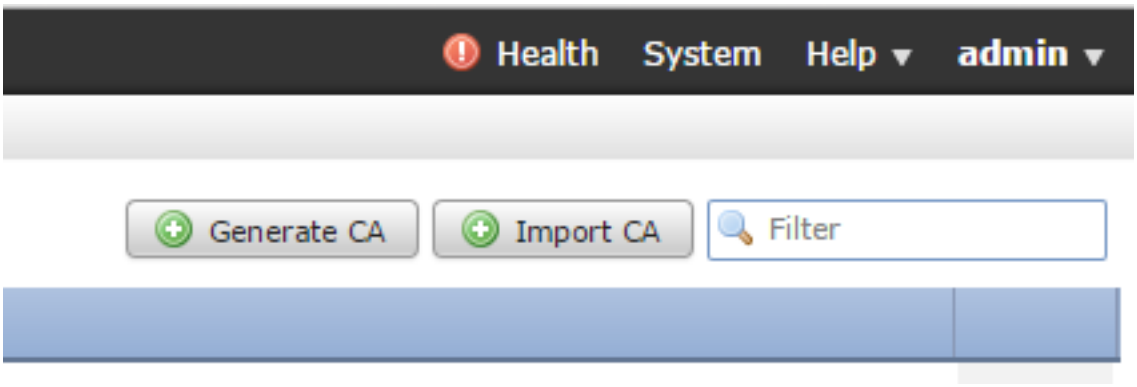
注意：您可能需要联系您的CA管理员以确定他们是否具有用于签名请求的模板。

三、复制整个证书，包括— BEGIN CERTIFICATE REQUEST -和—END CERTIFICATE REQUEST -,然后将其保存到扩展名为.req的文本文件中。



注意： 您的CA管理员请求除.req外的其他文件扩展名。

选项 3：导入CA证书和密钥

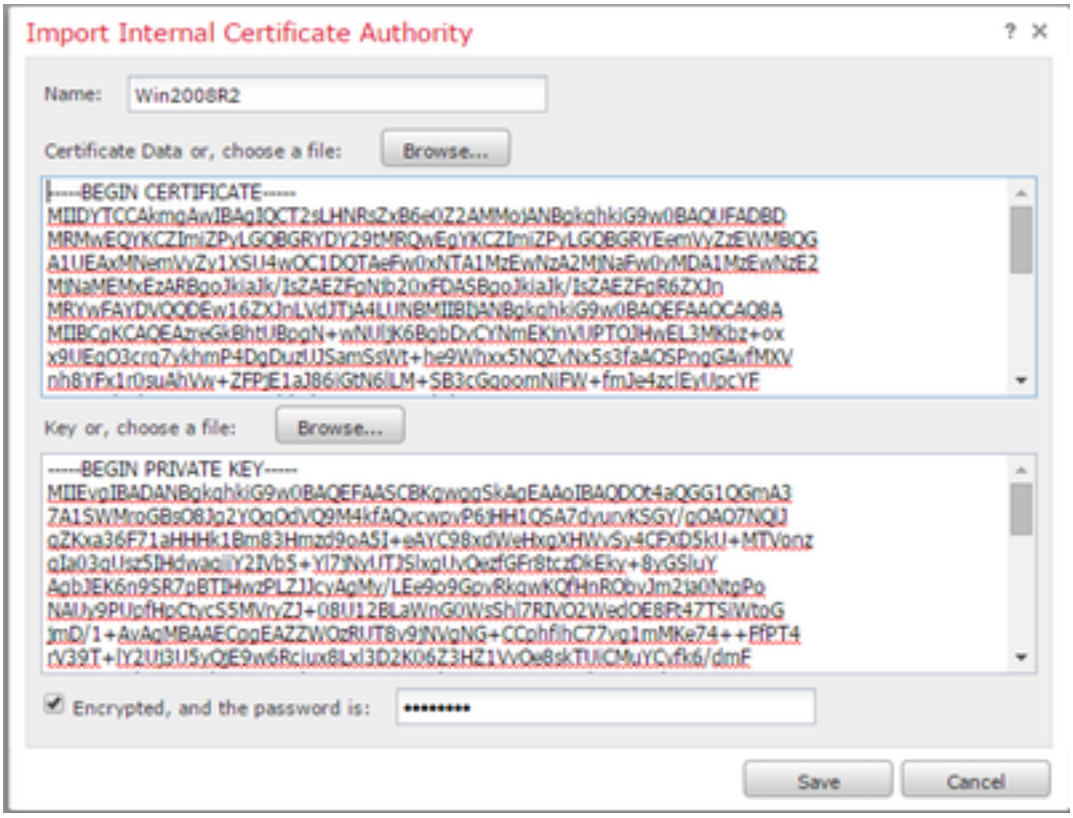


我。单击Import CA。

ii。浏览或粘贴证书。

三、浏览或粘贴私钥。

四。选中加密框并键入密码。



注意： 如果没有密码，请选中加密框并将其留空。

2.使用已知密钥解密

导入已知证书（解密和重新签名的替代选项）

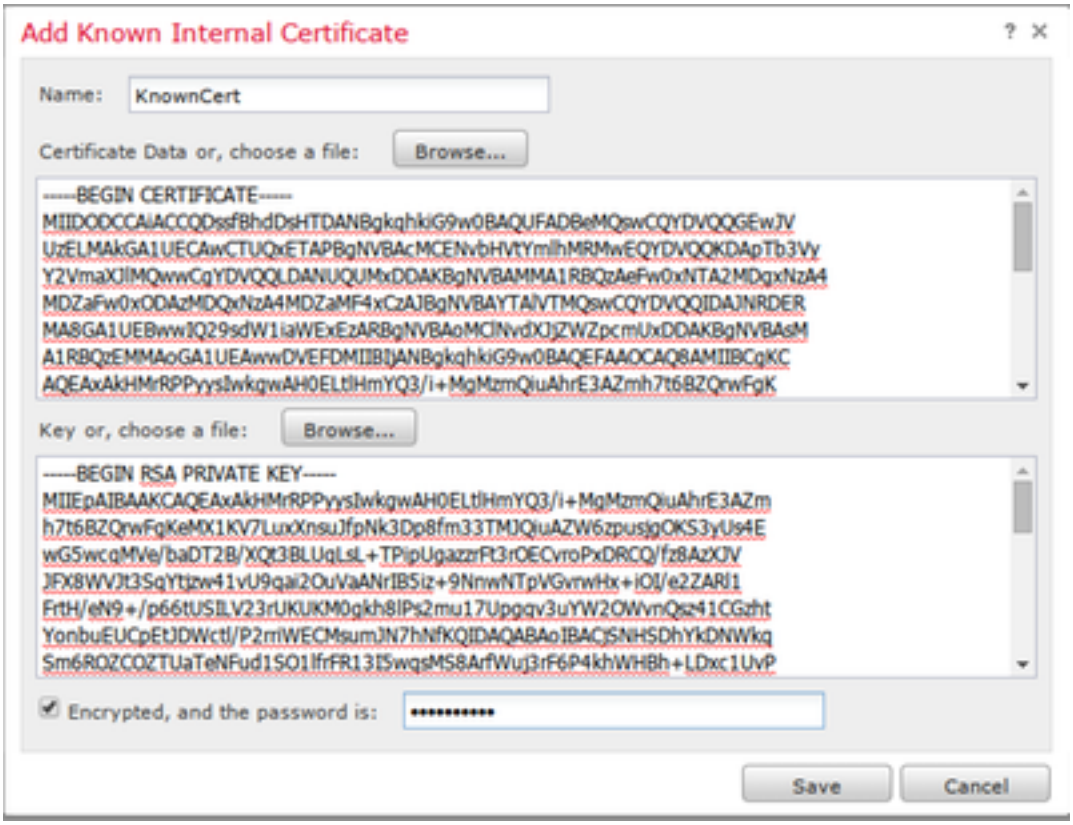
我。从左侧的“对象”(Objects)页面展开PKI并选择内部证书(Internal Certs)。

ii。单击Add Internal Cert。

三、浏览或粘贴证书。

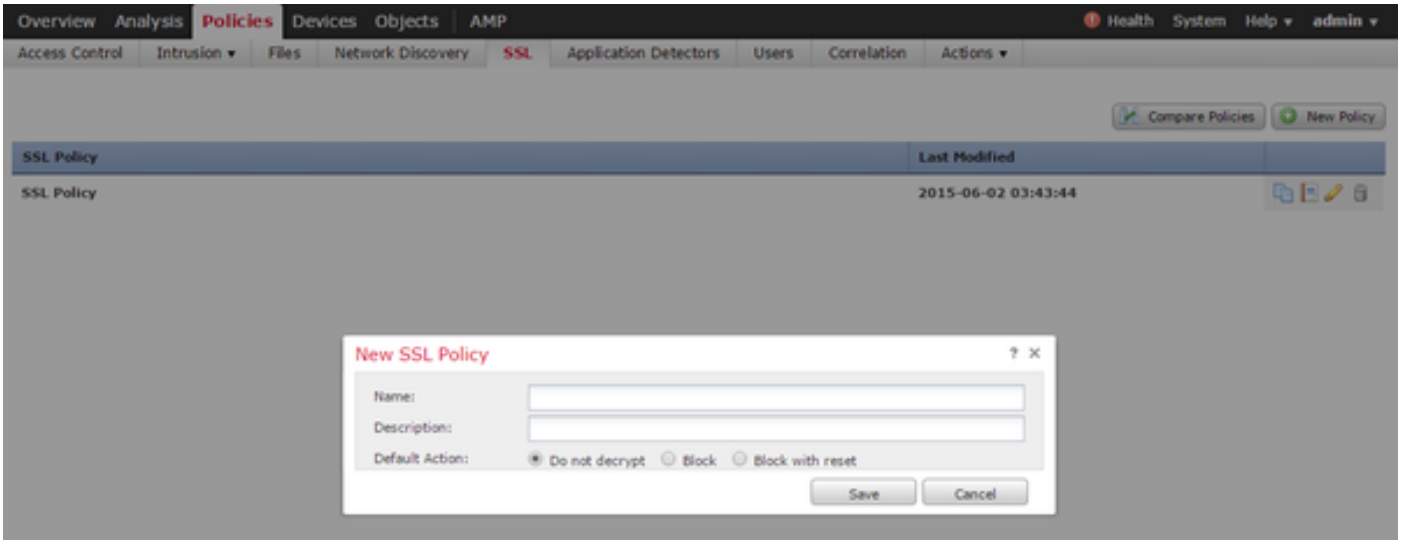
四。浏览或粘贴私钥。

v.选中Encrypted**框**并键入密码。



注意： 如果没有密码，请将**Encrypted**框留空。

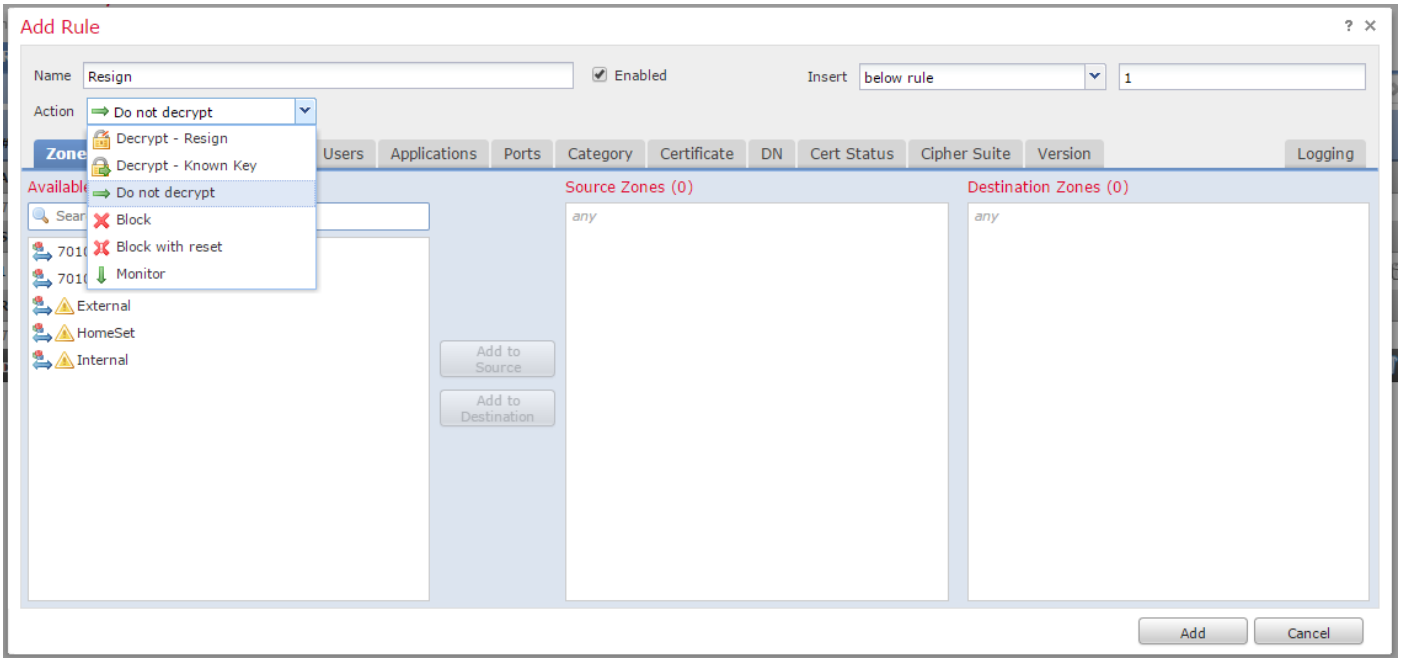
4.导航至Policies(策**略)> SSL(SSL)**，然后单**击New Policy(新建策**略)。



5.提供名称并选择“默认**操作”**。系统将显示SSL策略编辑器页面。SSL策略编辑器页面与访问控制策略编辑器页面的工作方式相同。

注意： 如果不确定**默认操**作，**建议**从“不解密”开始。

6.在SSL策略编辑器页面上，单击“添**加规则”**。在“添加规则”窗口中，为规则提供名称，并填写所有其他相关信息。



以下部分介绍“添加规则”(Add Rule)窗口中的各种选项：

操作

解密 — 重新签名

- 传感器充当中间人(MitM)，接受与用户的连接，然后与服务器建立新连接。例如：用户在浏览器中键入https://www.facebook.com。流量到达传感器，然后传感器使用所选CA证书与用户协商，并建立SSL隧道A。同时，传感器连接到https://www.facebook.com并创建SSL隧道B。
- 最终结果：用户在规则中看到证书，而不是facebook的证书。
- 此操作需要内部CA。如果希望替换密钥，请选择“替换密钥”。用户将收到您选择的证书。

注意： 在被动模式下不能使用。

解密 — 已知密钥

- 传感器具有用于解密流量的密钥。例如：用户在浏览器中键入https://www.facebook.com。流量到达传感器，传感器解密流量，然后检查流量。
- 最终结果：用户查看Facebook的证书
- 此操作需要内部证书。这将添加到“对**象**”>“**PKI**”>“**内部证书**”。

注意： 您的组织必须是域和证书的所有者。对于facebook.com的示例，让最终用户查看facebook证书的唯一可能方法是，您实际拥有域facebook.com（即您的公司是Facebook，Inc），并拥有由公共CA签名的facebook.com证书。您只能使用组织拥有的站点的已知密钥解密。

解密已知密钥的主要目的是解密流向https服务器的流量，以保护服务器免受外部攻击。对于检查到外部https站点的客户端流量，您将使用解密重新签名，因为您不拥有服务器，并且您有兴趣检查连接到外部加密站点的网络中的客户端流量。

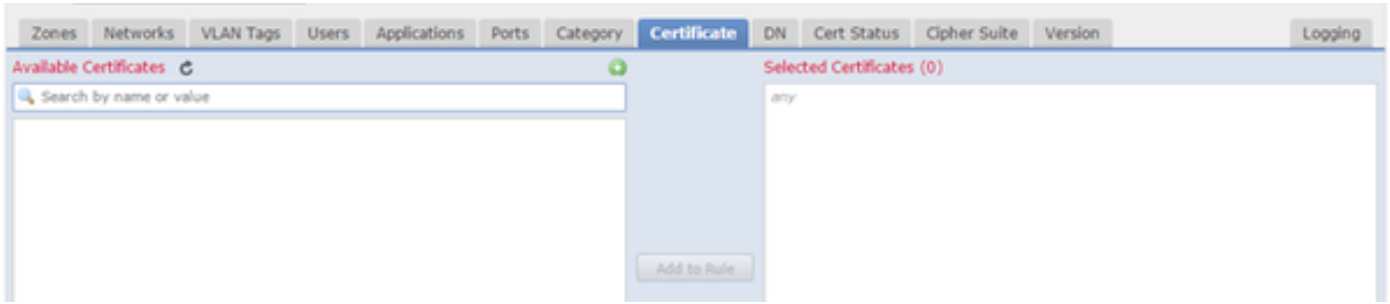
注意： DHE和ECDHE要解密，必须处于串联状态。

不解密

流量绕过SSL策略并继续进入访问控制策略。

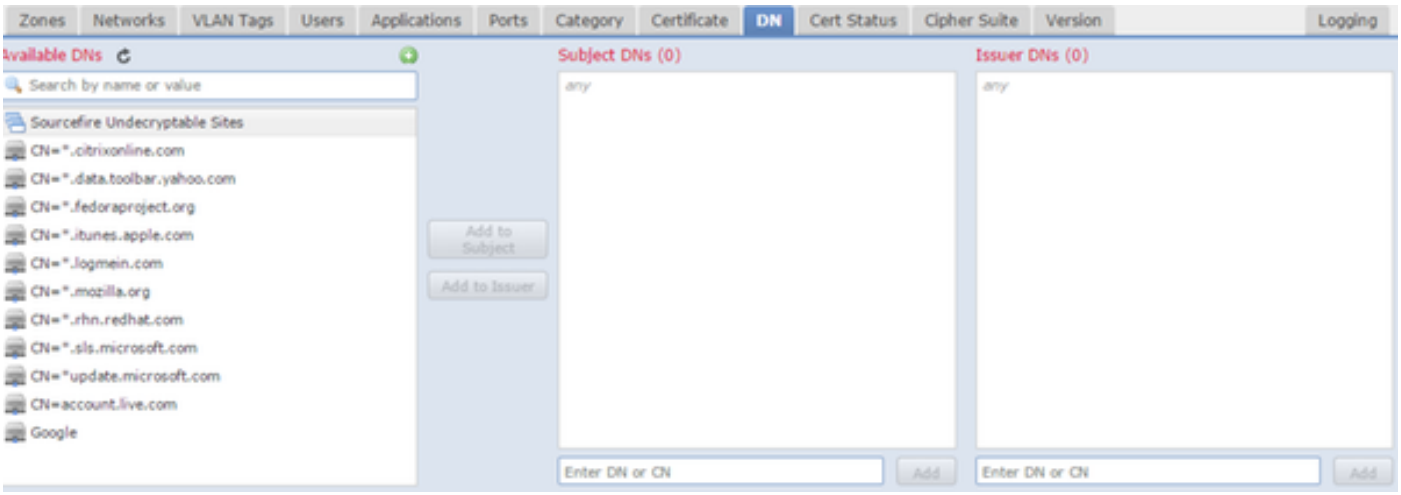
证书

规则使用此特定证书匹配SSL流量。



DN

规则使用证书中的某些域名匹配SSL流量。



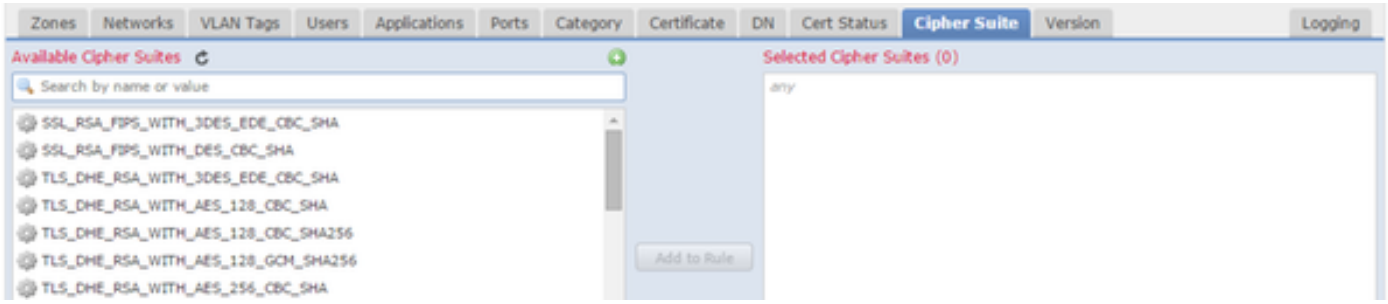
证书状态

规则将SSL流量与这些证书状态匹配。



密码套件

规则使用这些密码套件匹配SSL流量。



version

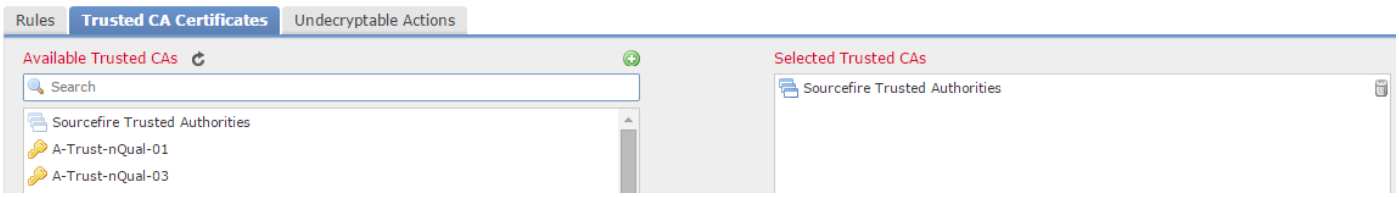
规则仅适用于具有选定SSL版本的SSL流量。



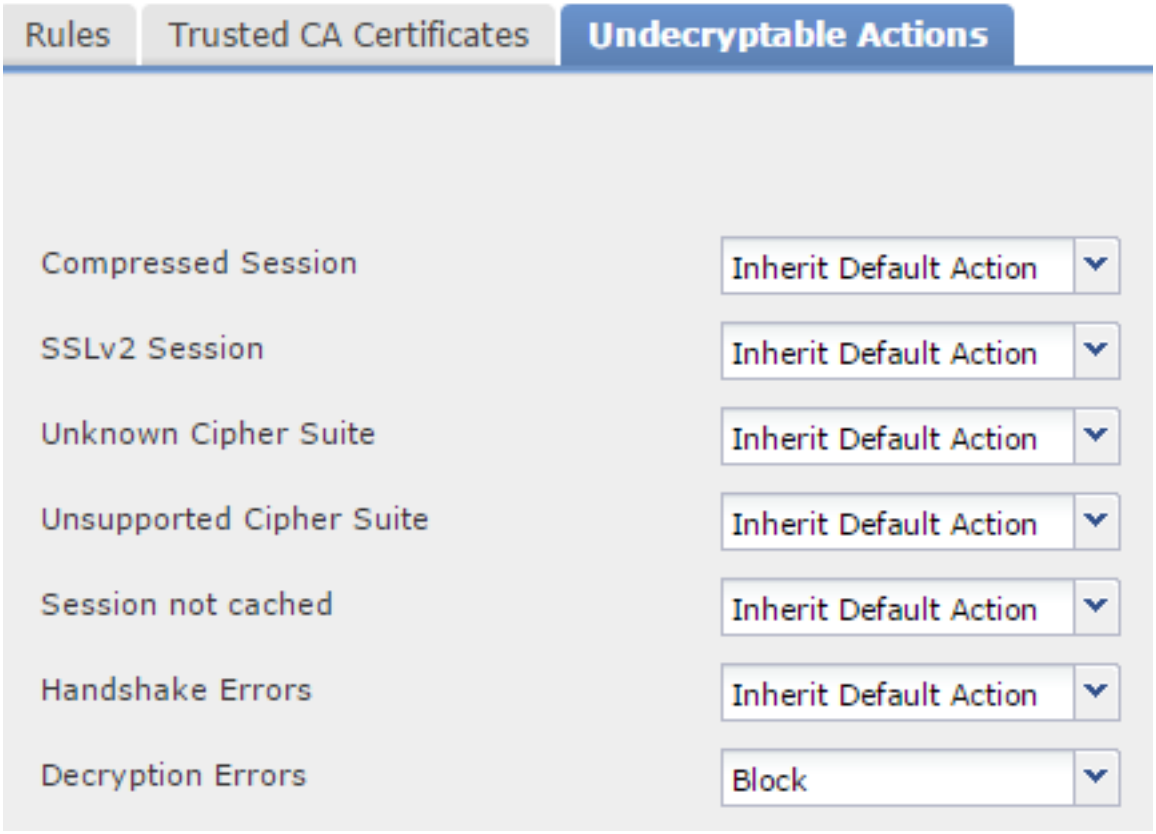
日志记录

启用日志记录以查看SSL流量的连接事件。

7.单击“受信**任CA证书”**。这是向策略添加受信任CA的位置。



8.单击“无法解**密的操作”**。以下是传感器无法解密流量的操作。您可以从FireSIGHT管理中心的联机帮助(“**帮助”>“联**机”)中找到定义。



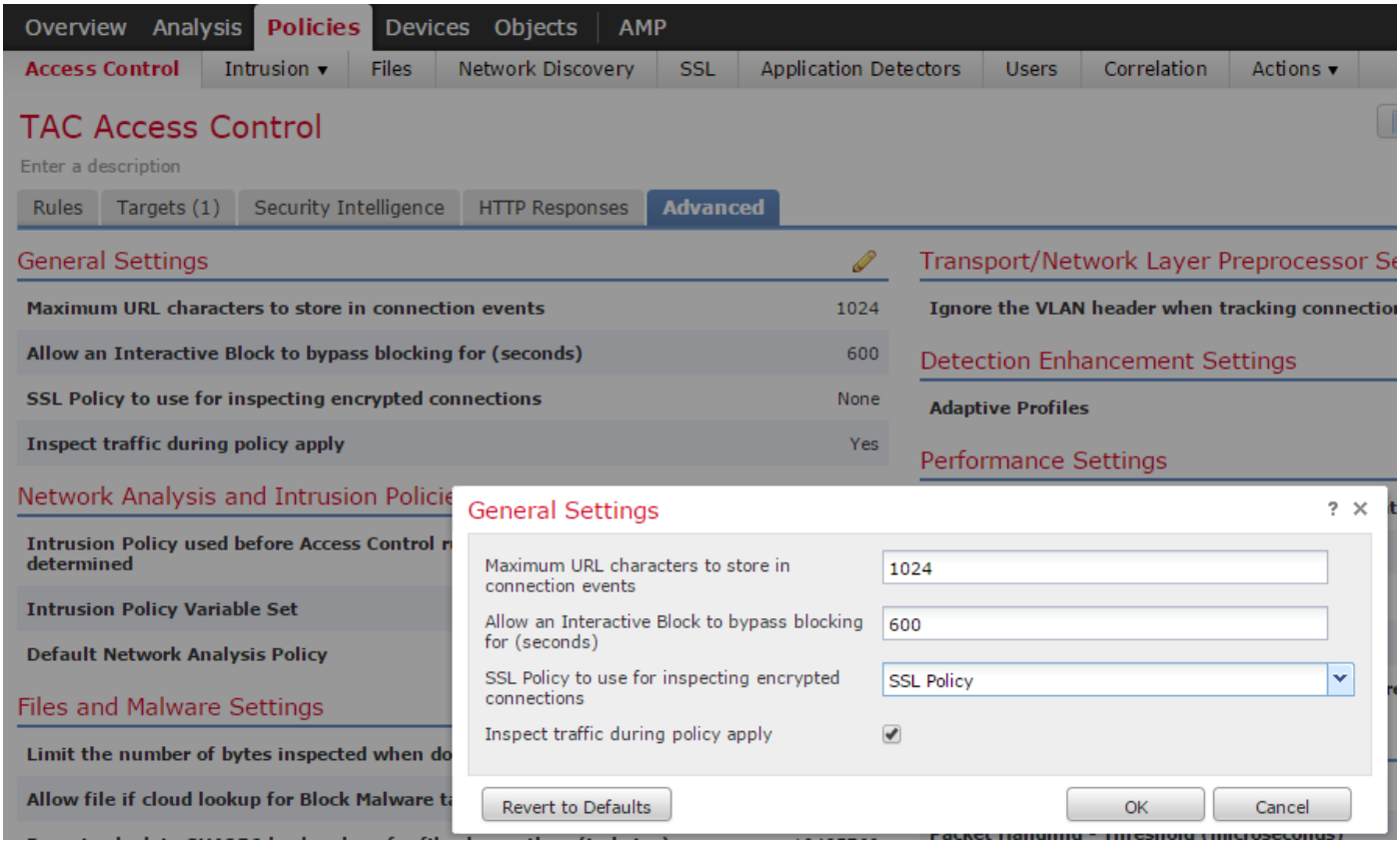
- **压缩会话**:SSL会话应用数据压缩方法。
- **SSLv2会话**:会话使用SSL版本2进行加密。请注意，如果客户端hello消息为SSL 2.0，而传输的流量的其余部分为SSL 3.0，则可解密流量。
- **未知密码套件**:系统无法识别密码套件。
- **不支持的密码套件**:系统不支持基于检测到的密码套件的解密。
- **会话未缓存**:SSL会话已启用会话重用，客户端和服务器使用会话标识符重新建立会话，并且系统未缓存该会话标识符。
- **握手错误**:SSL握手协商期间出错。
- **解密错误**:流量解密期间出错。

注意： 默认情况下，这些操作继承默认操作。如果默认操作为Block，则可能遇到意外问题

9.保存策略。

10.导航至“策**略**”>“**访问控制**”。编辑策略或创建新的访问控制策略。

11.单击“高**级**”并编辑“**常规设置**”。



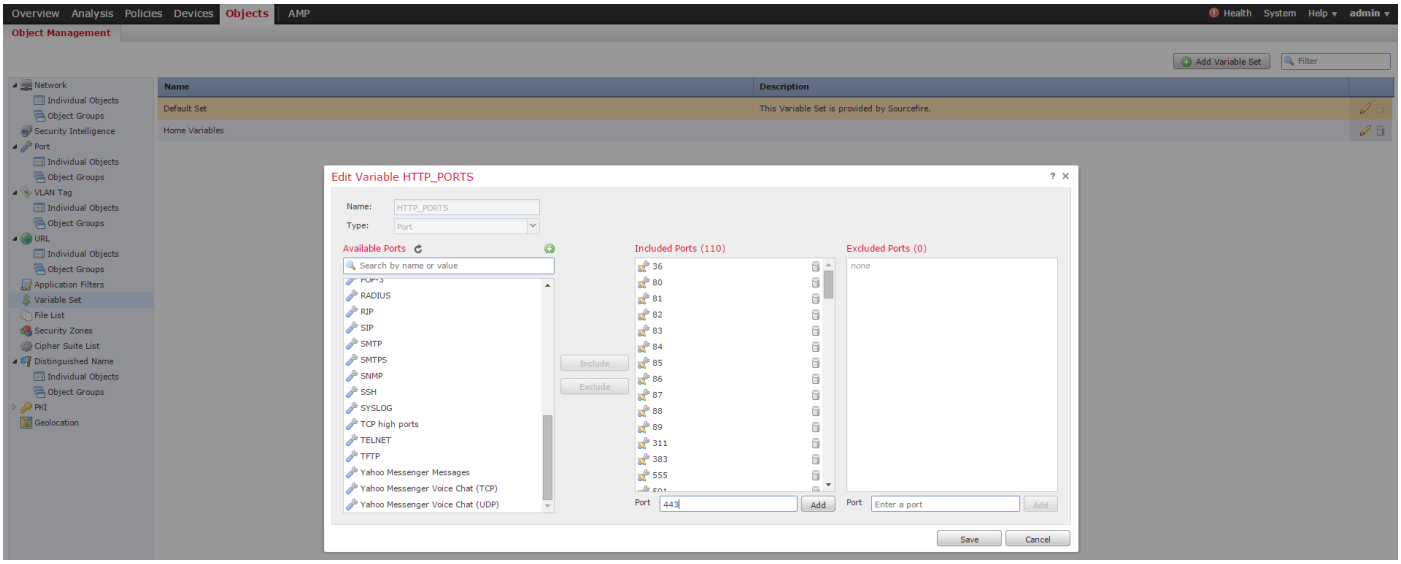
12.从下拉菜单中选择您的**SSL策略**。

13.单击“**确定**”保存。

其他配置

应对入侵策略进行以下更改以正确识别：

我。$HTTP_PORTS变量应包括端口443和任何具有https流量的其他端口，这些流量将由您的策略(**Objects** > Object Management > Variable Set > Edit the variable set)。



ii。检查已加密流量的网络分析策略必须将端口443（以及任何其他具有https流量且将由策略解密的端口）包含在HTTP预处理器设置的端口字段中，否则，不会触发具有http内容修饰符(即http_uri、

http_header等)的http规则，因为这取决于定义的http端口和http缓冲区不会为不通过指定端口的流量填充snort。

三、（可选，但建议进行更好的检查）将https端口添加到“在两个端口上执**行数据流重**组”字**段中的“TCP数据流配置**”设置。

四。在计划的维护窗口期间重新应用修订的访问控制策略。

> **警告：此**修改的策略可能导致严重的性能问题。这应在生产时间之外进行测试，以降低网络中断或性能风险。

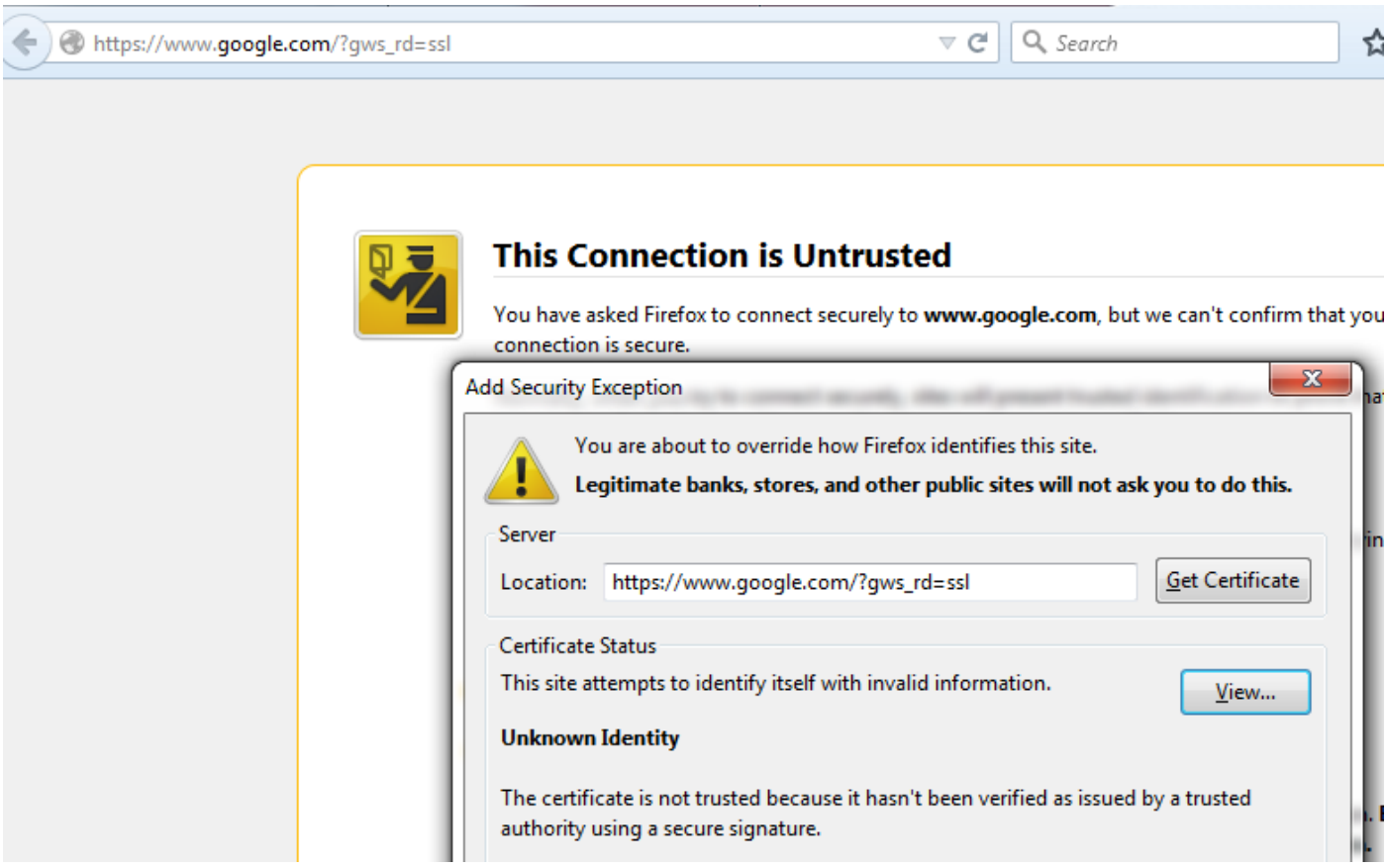
确认

解密 — 重新签名

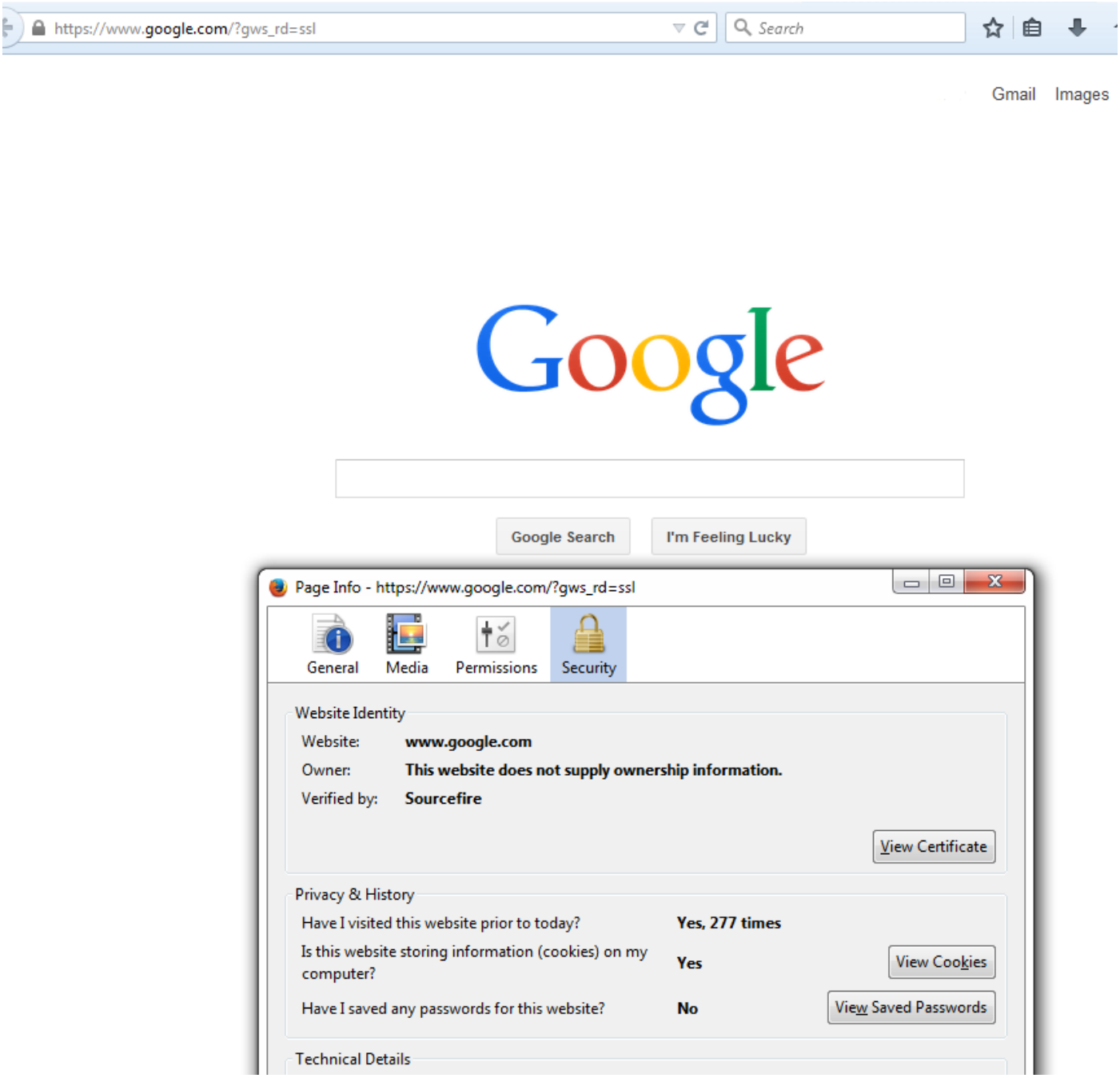
1.打开Web浏览器。

> **注意：**以下示例中使用Firefox浏览器。 此示例在Chrome中可能不起作用。有关详细信息，请参阅故障排除部分。

2.导航至SSL网站。在以下示例中，使用https://www.google.com，金融机构的网站也将工作。您将看到以下页面之一：



> **注意：**如果证书本身不受信任，且浏览器不信任签名CA证书，您将看到上面的页面。要了解浏览器如何确定受信任CA证书，请参阅下面的“受信任证书颁发机构”部分。



注意： 如果看到此页面，您已成功重新签名流量。请注意“验**证者：Sourcefire**。

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	www.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	13:E3:D5:7D:4E:5F:8F:E7

Issued By

Common Name (CN)	Sourcefire TAC
Organization (O)	Sourcefire
Organizational Unit (OU)	Tac

Period of Validity

Begins On	5/6/2015
Expires On	8/3/2015

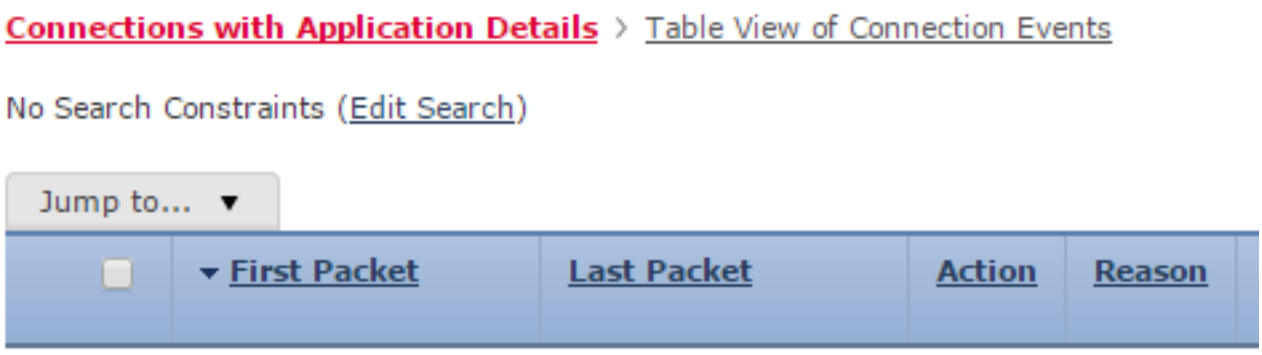
Fingerprints

SHA-256 Fingerprint	20:00:CB:25:13:8B:1F:89:4D:4A:CF:C5:E2:21:38:92: 06:66:00:2E:B7:83:27:72:98:EA:B1:6A:10:B3:67:A1
SHA1 Fingerprint	1B:C2:30:D9:66:84:DB:97:CF:A9:5E:5F:29:DA:4C:3F:13:E9:DE:5D

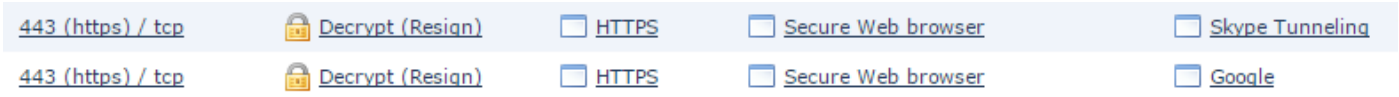
注意： 这是同一证书的特写。

3.在管理中心中，转到“分析”>“连**接”>“事件”**。

4.根据工作流程，您可能看到或看不到SSL解密选项。单击**连接事件的表视图**。



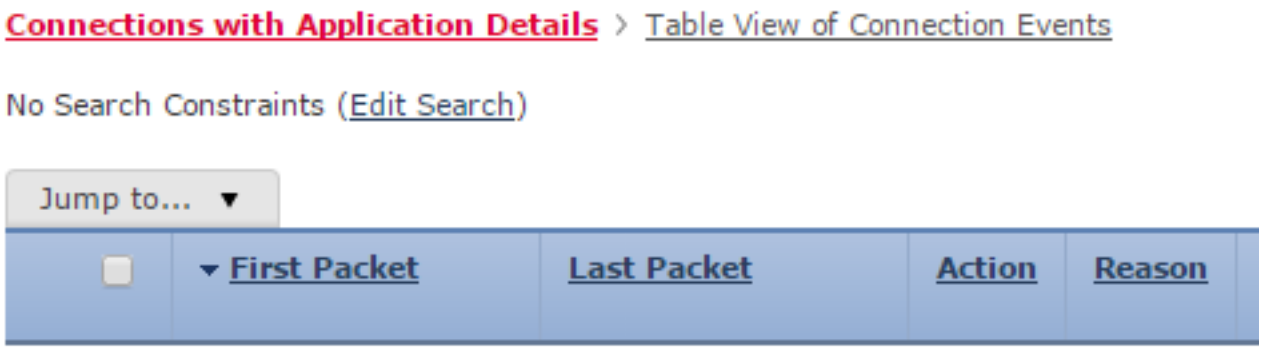
5.滚动到右侧并查找SSL状态。您应看到类似以下的选项：



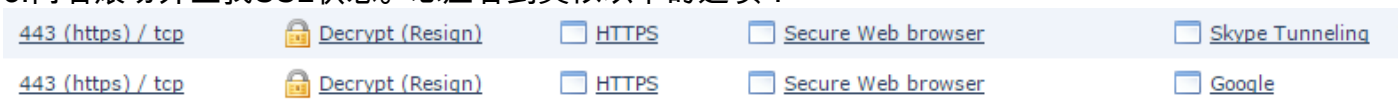
解密 — 已知证书

1.在FireSIGHT管理中心中，导航至“分析”**>“连接”>“事件”**。

2.根据您的工作流程，您可能看到或看不到SSL解密选项。单击**连接事件的表视图**。



3.向右滚动并查找SSL状态。您应看到类似以下的选项：



故障排除

问题 1:某些网站可能未加载到Chrome浏览器上

示例

www.google.com不能使用Chrome加载“解密 — 重新签名”。

原因

Google Chrome浏览器能够检测Google属性的欺诈证书，以防止中间人攻击。如果Chrome浏览器（客户端）尝试连接到google.com域（服务器），并且返回的证书不是有效的google证书，则浏览器将拒绝连接。

解决方案

如果遇到此情况，请为**DN=*.google.com**、*.gmail.com、*.youtube.com添加“不解密”规则。然后清除浏览器缓存和历史记录。

问题 2:在某些浏览器中获取不受信任的警告/错误

示例

使用Internet Explorer和Chrome连接到站点时，不会收到安全警告，但是，使用Firefox浏览器时，每次关闭并重新打开浏览器时，您都必须信任连接。

原因

受信任CA的列表取决于浏览器。当您信任证书时，这不会跨浏览器进行属性管理，受信任条目通常仅在浏览器打开时继续存在，因此一旦关闭，所有受信任的证书都将被删除，下次打开浏览器并访问站点时，您必须将其再次添加到受信任证书列表。

解决方案

在此场景中，IE和Chrome都使用操作系统中的受信任CA列表，但Firefox会维护自己的列表。因此，CA证书已导入到OS存储，但未导入到Firefox浏览器。为避免在Firefox中获得安全警告，您必须将CA证书作为受信任CA导入浏览器。

受信任证书颁发机构

当建立SSL连接时，浏览器首先检查此证书是否受信任（例如，您之前已访问过此站点，并手动告知浏览器信任此证书）。 如果证书不受信任，浏览器将检查验证此站点证书的证书颁发机构(CA)证书。如果浏览器信任CA证书，则它会将其视为受信任证书并允许连接。如果CA证书不受信任，浏览器将显示安全警告，并强制您手动将证书添加为受信任证书。

浏览器中的受信任CA列表完全取决于浏览器的实施，每个浏览器可以以不同于其他浏览器的方式填充其受信任列表。通常，当前浏览器填充受信任CA列表的方法有2种：

1. 它们使用操作系统信任的受信任CA列表
2. 他们随软件一起发送受信任CA列表，并将其内置到浏览器中。

对于最常见的浏览器，可信CA填充如下：

- Google Chrome:操作系统的受信任CA列表
- Firefox:维护自己的受信任CA列表
- Internet Explorer:操作系统的受信任CA列表
- Safari:操作系统的受信任CA列表

了解差异非常重要，因为客户端上看到的行为会因此而有所不同。例如，为了为Chrome和IE添加受信任CA，您必须将CA证书导入操作系统的受信任CA存储。如果将CA证书导入操作系统的受信任CA存储，则当连接到具有此CA签名的证书的站点时，将不再收到警告。在Firefox浏览器上，必须手动将CA证书导入浏览器本身的受信任CA存储。执行此操作后，在连接到该CA验证的站点时，您将不再收到安全警告。

参考

- SSL规则入门

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。