使用ASDM（现场管理）在FirePOWER模块上配置SSL解密

目录

简介

本文档介绍使用ASDM（现场管理）在FirePOWER模块上配置安全套接字层(SSL)解密。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解ASA（自适应安全设备）防火墙、ASDM（自适应安全设备管理器）
- FirePOWER设备知识
- HTTPS/SSL协议知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本6.0.0及更高版本的ASA FirePOWER模块(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- 运行软件版本6.0.0及更高版本的ASA FirePOWER模块(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)

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。

> **注意**：确保FirePOWER模块具有保护许**可证**以配置此功能。要验证许可证，请导航至**Configuration > ASA FirePOWER Configuration > License**。

背景信息

Firepower模块解密并检查重定向到它的入站和出站SSL连接。一旦流量被解密，就会检测并控制隧道应用，如facebook聊天等。对解密的数据进行威胁、URL过滤、文件阻止或恶意数据检查。

出站SSL解密

firepower模块通过拦截出站SSL请求并为用户要访问的站点重新生成证书，充当出站SSL连接的转发代理。颁发机构(CA)是Firepower自签名证书。如果firepower的证书不是现有层次结构的一部分，或者未将其添加到客户端的浏览器缓存，客户端在浏览到安全站点时会收到警告。Decrypt-Resign方法用于执行出站SSL解密。

入站SSL解密

如果入站流量发往内部Web服务器或设备，管理员将导入受保护服务器的证书和密钥的副本。当SSL服务器证书加载到firepower模块上，并且为入站流量配置了SSL解密策略时，设备会在转发流量时解密并检查流量。然后，模块会检测通过此安全通道传输的恶意内容、威胁和恶意软件。此外，Decrypt-Known Keymethod用于执行入站SSL解密。

SSL解密配置

SSL流量解密有两种方法。

- 解密 — 对出站SSL流量重新签名
- 解密 — 已知入站SSL流量

出站SSL解密（解密 — 重新签名）

Firepower模块充当MITM（中间人），用于公共SSL服务器的任何SSL协商。它使用在firepower模块上配置的中间CA证书重新签署公共服务器的证书。

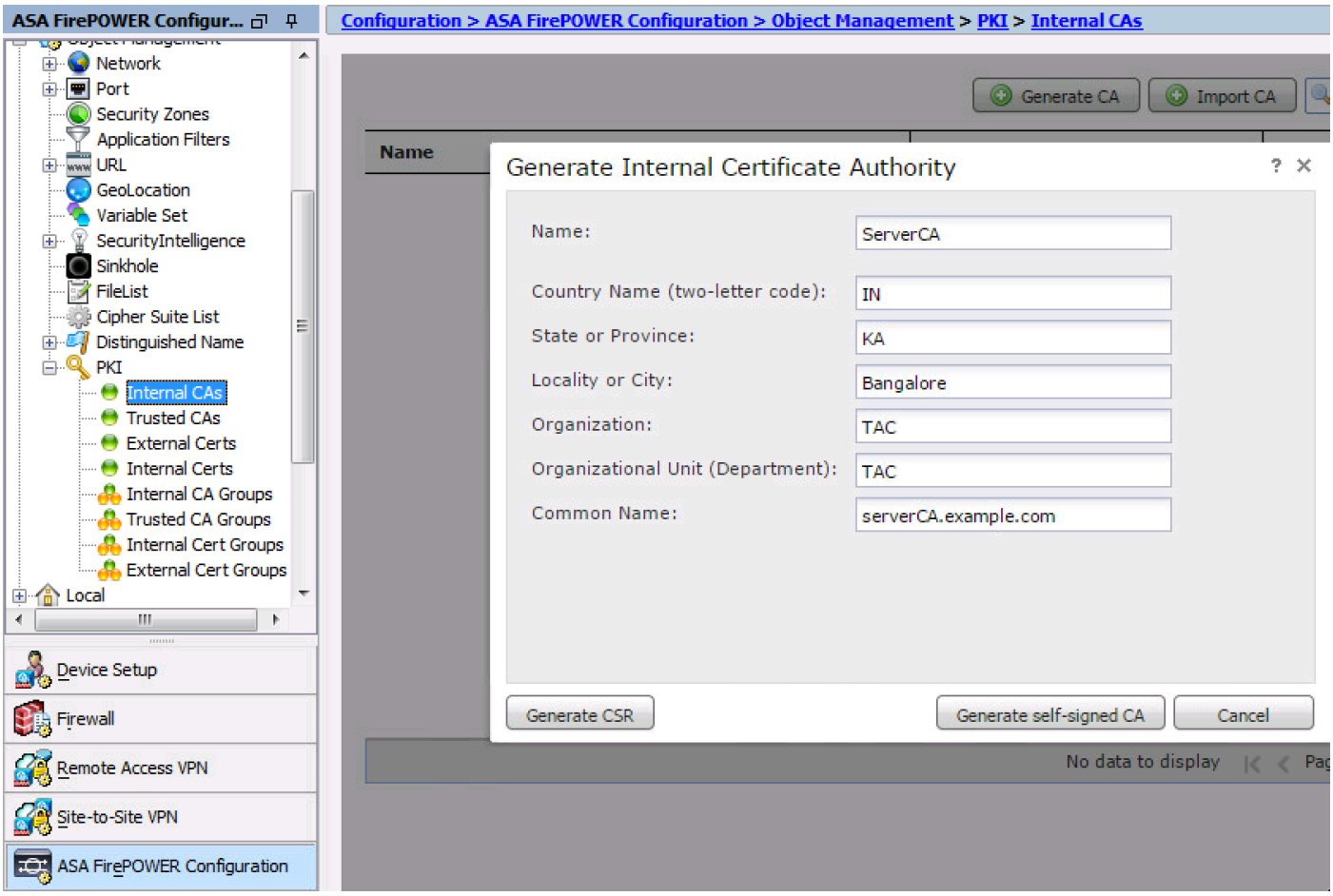
以下是配置出站SSL解密的三个步骤。

步骤1.配置CA证书。

配置自签名证书或中间受信任CA证书以重新签名证书。

配置自签名CA证书

要配置自签名CA证书，请导航至**Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs，然**后单击**Generate CA**。系统会提示输入CA证书的详细信息。如图所示，请根据您的要求填写详细信息。



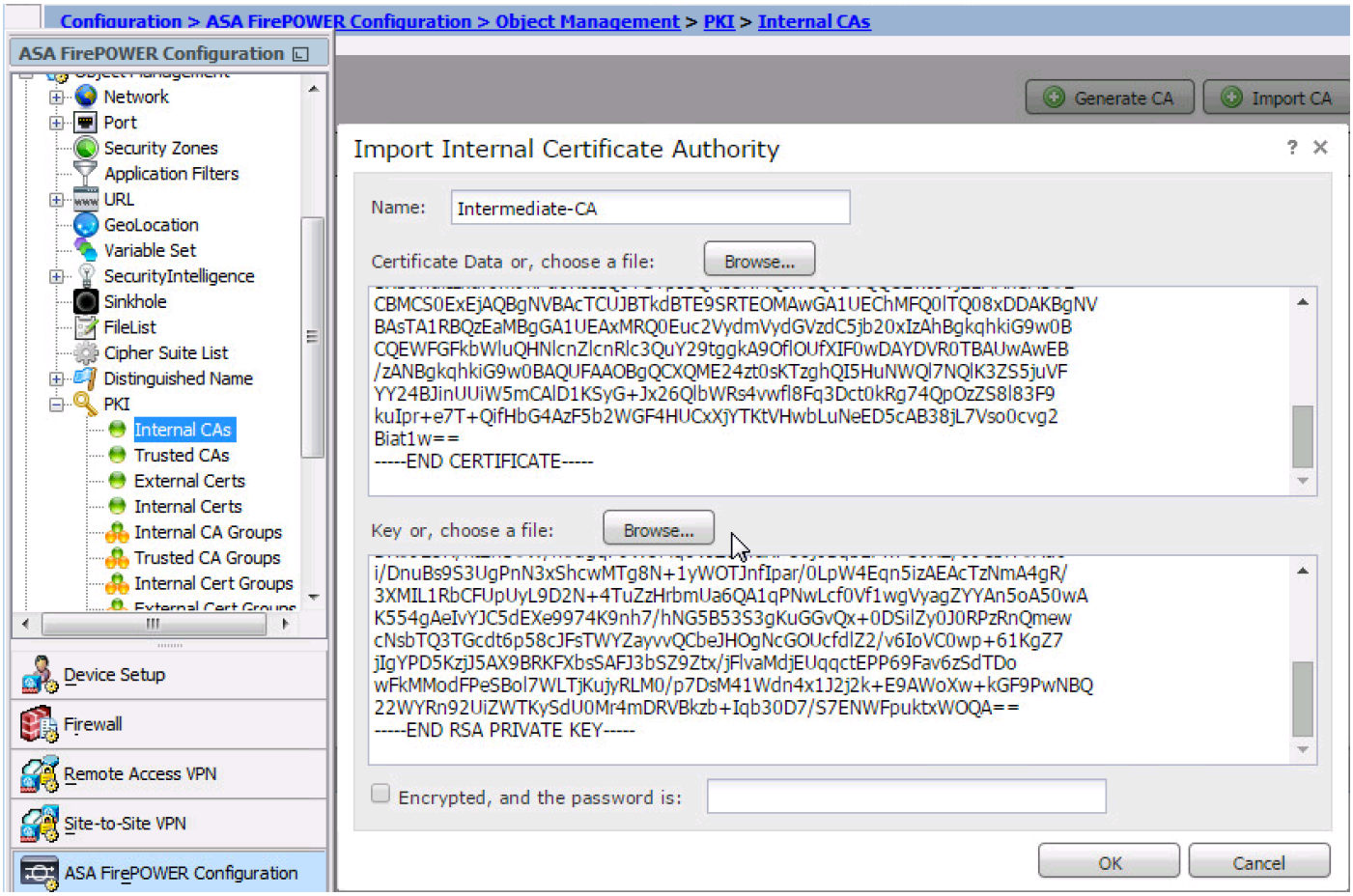
单击**Generate self-signed CA** 以生成内部CA证书。然后单击**Generate CSR**以生成证书签名请求，该请求随后与要签名的CA服务器共享。

配置中间CA证书

要配置由另一第三方CA签名的中间CA证书，请导航到**Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs，然**后单击**Import CA**。

指定证书的名称。选择**浏**览并从本地计算机上传证书，或在“证书数据”(Certificate Data)选项中复制并粘贴证**书的**内容。要指定证书的私钥，请浏览密钥文件或在“密钥”选项中复制粘贴**密钥**。

如果密钥已加密，请启用复选框“已加密”**并指**定密码。单击**OK**保存证书内容，如图所示：



步骤2.配置SSL策略。

SSL策略定义解密操作并标识应用解密的解密 — 重新签名方法的流量。根据业务需求和组织安全策略配置多个SSL规则。

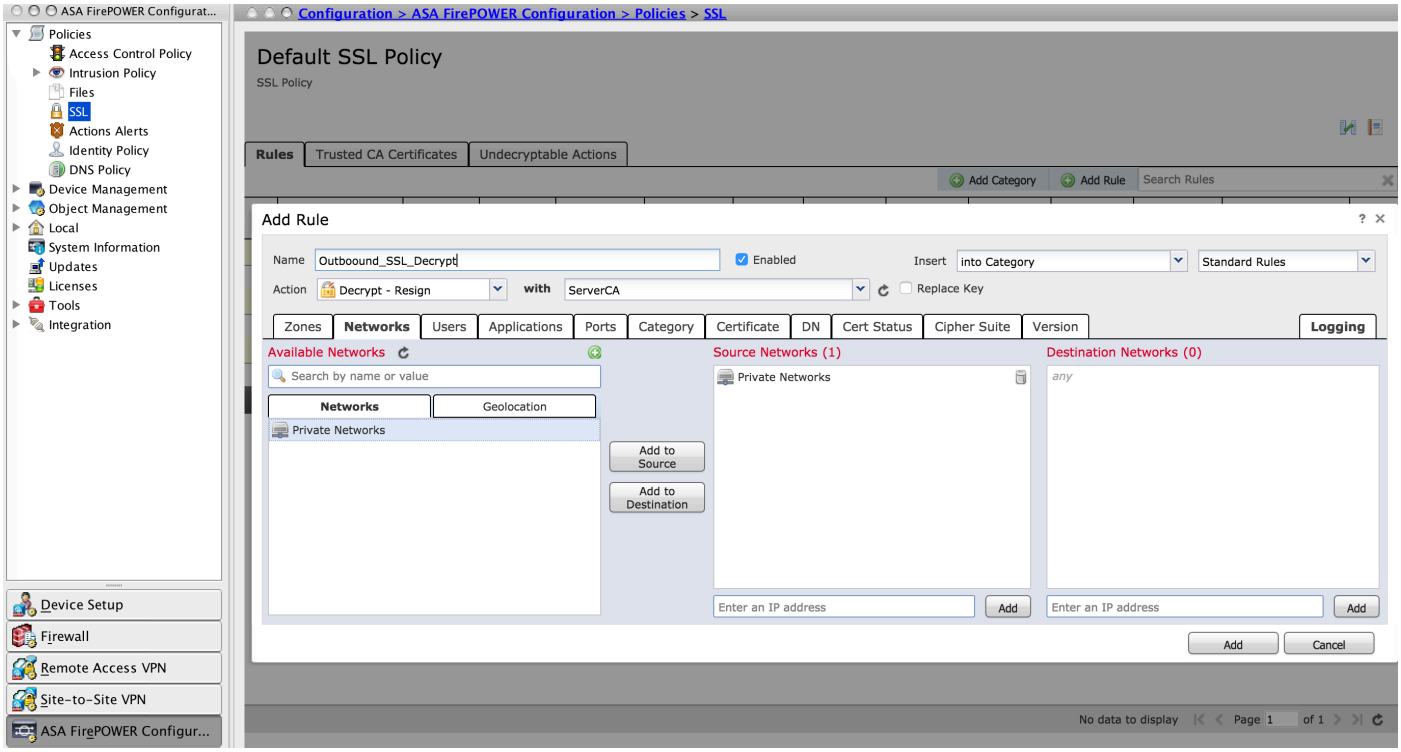
要配置SSL策略，请导航至**Configure > ASA FirePOWER Configuration > Policies > SSL，然**后点击**Add Rule**。

名称：指定规则的名称。

操作：将操作指定**为解密 —** 重新签名，然后从上一步中配置的下拉列表中选择CA证书。

在规则中定义条件以匹配流量，因为有多个选项（区域、网络、用户等），指定这些选项以定义需要解密的流量。

要生成SSL解密事件，请启用loggingat **logging**选项，如图所示：



单击**Add**以添加SSL规则。

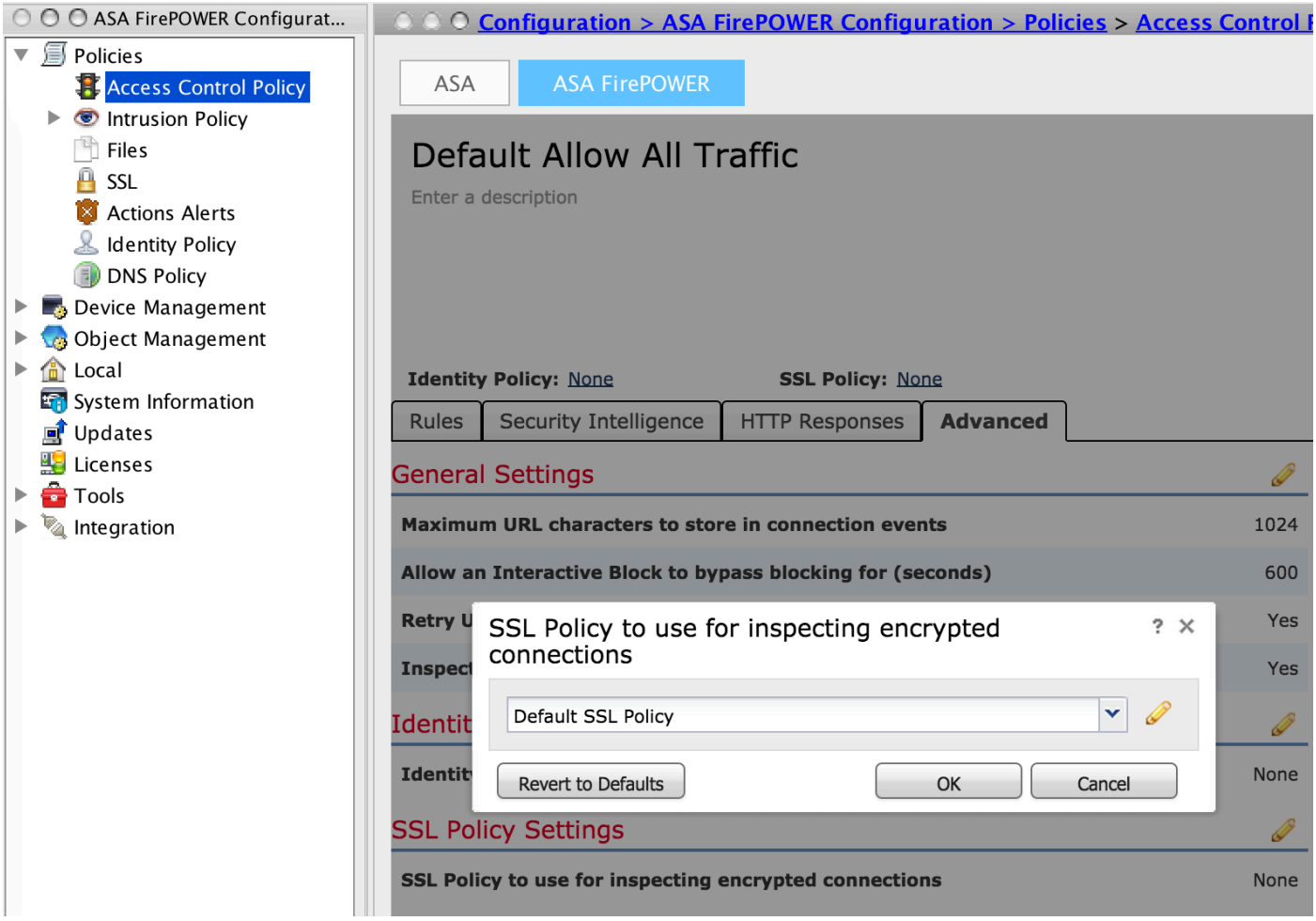
单击**Store ASA Firepower Changes**以保存SSL策略的配置。

步骤3.配置访问控制策略

使用适当的规则配置SSL策略后，必须在访问控制中指定SSL策略以实施更改。

要配置访问控制策略，请导航至**Configuration > ASA Firepower Configuration > Policies > Access Control。**

单击**None(SSL策略)**或导**航至Advanced(高**级)**> SSL Policy Setting（SSL策略设置）。**从下拉列表中指定SSL策略，然后单击**OK**以保存该策略，如图所示：



单击 **存储ASA Firepower更改** 保存SSL策略的配置。

您必须将访问控制策略部署到传感器。在应用策略之前，模块上会显示**访问控制策略已过**时。若要将更改部署到传感器，请单击**部署**并选择**部署FirePOWER更改选项。**验证所做的更改，然后单击**Deploy。**

> **注意**：在版本5.4.x中，如果需要将访问策略应用于传感器，请单击**Apply ASA FirePOWER Changes。**

> **注意**：导航至**Monitoring > ASA Firepower Monitoring > Task Status。**然后，您应用配置更改以确保任务完成。

入站SSL解密（解密 — 已知）

入站SSL解密（解密 — 已知）方法用于解密已为其配置服务器证书和私钥的入站SSL流量。您需要将服务器证书和私钥导入Firepower模块。当SSL流量到达Firepower模块时，它会解密流量并对解密的流量执行检查。检查后，Firepower模块会重新加密流量并将其发送到服务器。

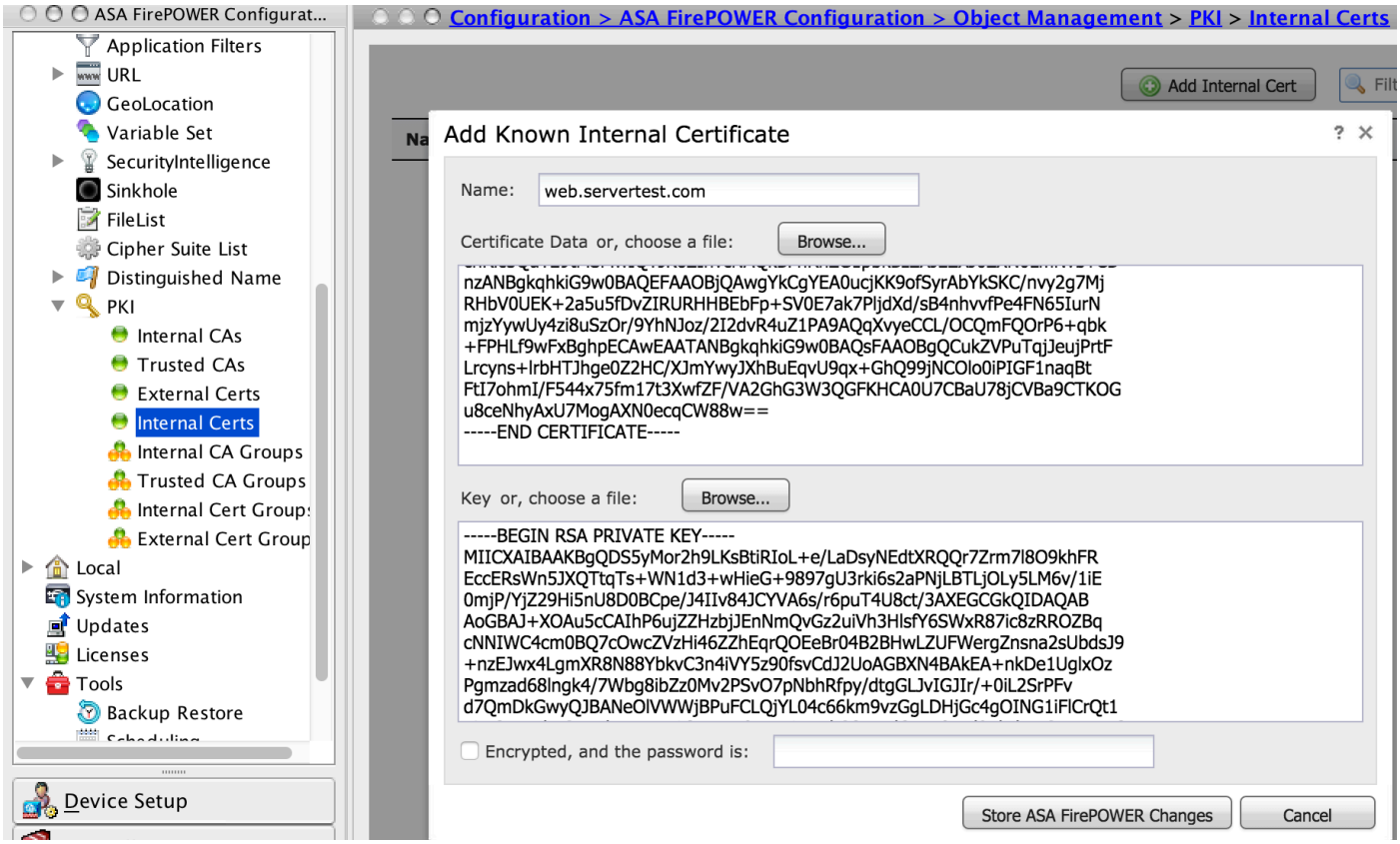
以下是配置出站SSL解密的四个步骤：

步骤1.导入服务器证书和密钥。

要导入服务器证书和密钥，请导航至**Configuration > ASA Firepower Configuration > Object Management > PKI > Internal Certs，然**后点击**Add Internal Cert**。

如图所示，指定证书的名称。选择“**浏览**”以从本地计算机中选择证书，或在“证书数据”中复制粘贴证书**内容**。要指定证书的私钥，请浏览密钥文件或将密钥复制粘贴到选项**Key**中。

如果密钥已加密，请启用复选框“已加密”并指定密码，如图所示：



单击“**Store ASA FirePOWER Changes(存储ASA FirePOWER更改)**”以保存证书内容。

步骤2.导入CA证书（可选）。

对于由内部中间或根CA证书签名的服务器证书，您需要将CA证书的内部链导入firepower模块。执行导入后，firepower模块可以验证服务器证书。

要导入CA证书，请导航至**Configuration > ASA Firepower Configuration > Object Management > Trusted CAs，然**后单**击Add Trusted CA**以添加CA证书。

步骤3.配置SSL策略。

SSL策略定义要为其配置解密已知方法以解密入站流量的操作和服务器详细信息。如果您有多个内部服务器，请根据不同的服务器及其处理的流量配置多个SSL规则。

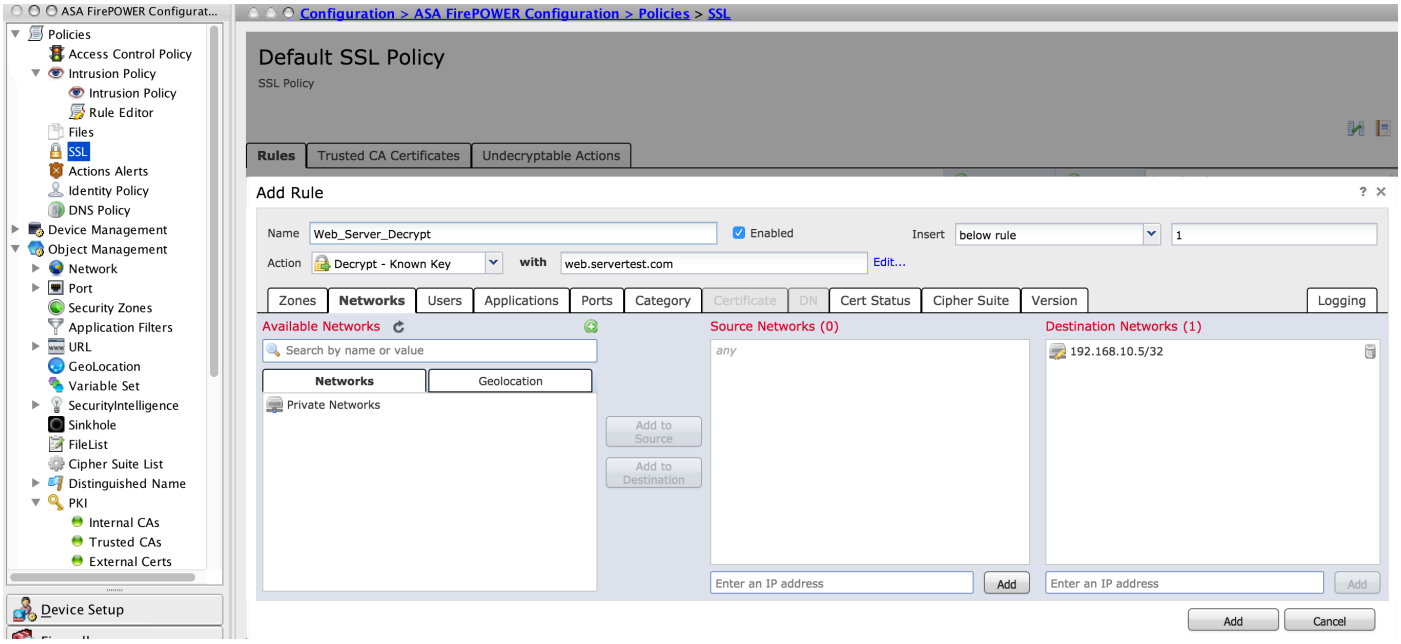
要配置SSL策略，请导航至**Configure > ASA FirePOWER Configuration > Policies > SSL，然**后点击**Add Rule**。

名称：指定规则的名称。

操作：将操作指定**为解**密 — 已知，然后从上一步配置的下拉列表中选择CA证书。

定义与此规则匹配的条件，因为指定了多个选项（网络、应用程序、端口等）来定义要为其启用SSL解密的服务器的相关流量。在“受信任CA”证书选项卡的“选**定受信任CA”中指**定内部CA。

要生成SSL解密事件，请启用loggingat logging**选**项。



单击**Add**以添加SSL规则。

然后单击“Store **ASA Firepower Changes”(存**储ASA Firepower更改)以保存SSL策略的配置。

步骤4.配置访问控制策略。

使用适当的规则配置SSL策略后，必须在访问控制中指定SSL策略以实施更改。

要配置访问控制策略，请导航至**Configuration > ASA Firepower Configuration > Policies > Access Control。**

单击**SSL Policy**旁边的**None**选项，或导航至**Advanced > SSL Policy Setting**，从下拉列表中指定SSL策略，然后单击**OK**保存该策略。

单击 **存储ASA Firepower更改** 保存SSL策略的配置。

您必须部署访问控制策略。在应用策略之前，您可以在模块上看到指示访问控制策略已过期。要将更改部署到传感器，请单击**部署**并选择**部署FirePOWER更改选项。验证所做的更改，然后在弹出窗口中Deploy。**

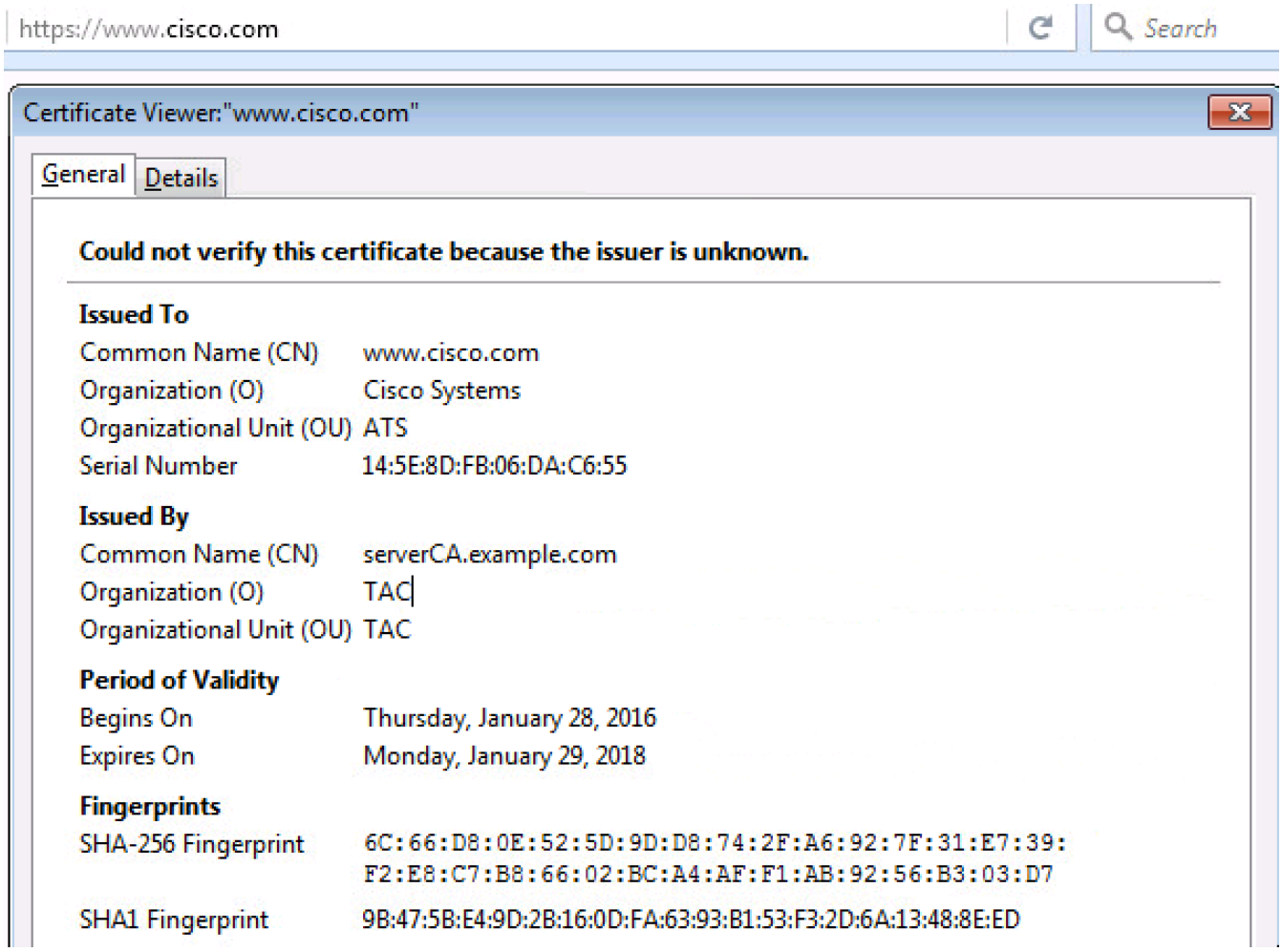
> **注意**：在版本5.4.x中，如果需要将访问策略应用于传感器，请单击“应用ASA FirePOWER更改”(Apply ASA FirePOWER Changes)。

> **注意**：导航至**Monitoring > ASA Firepower Monitoring > Task Status。**然后，您应用配置更改以确保任务完成。

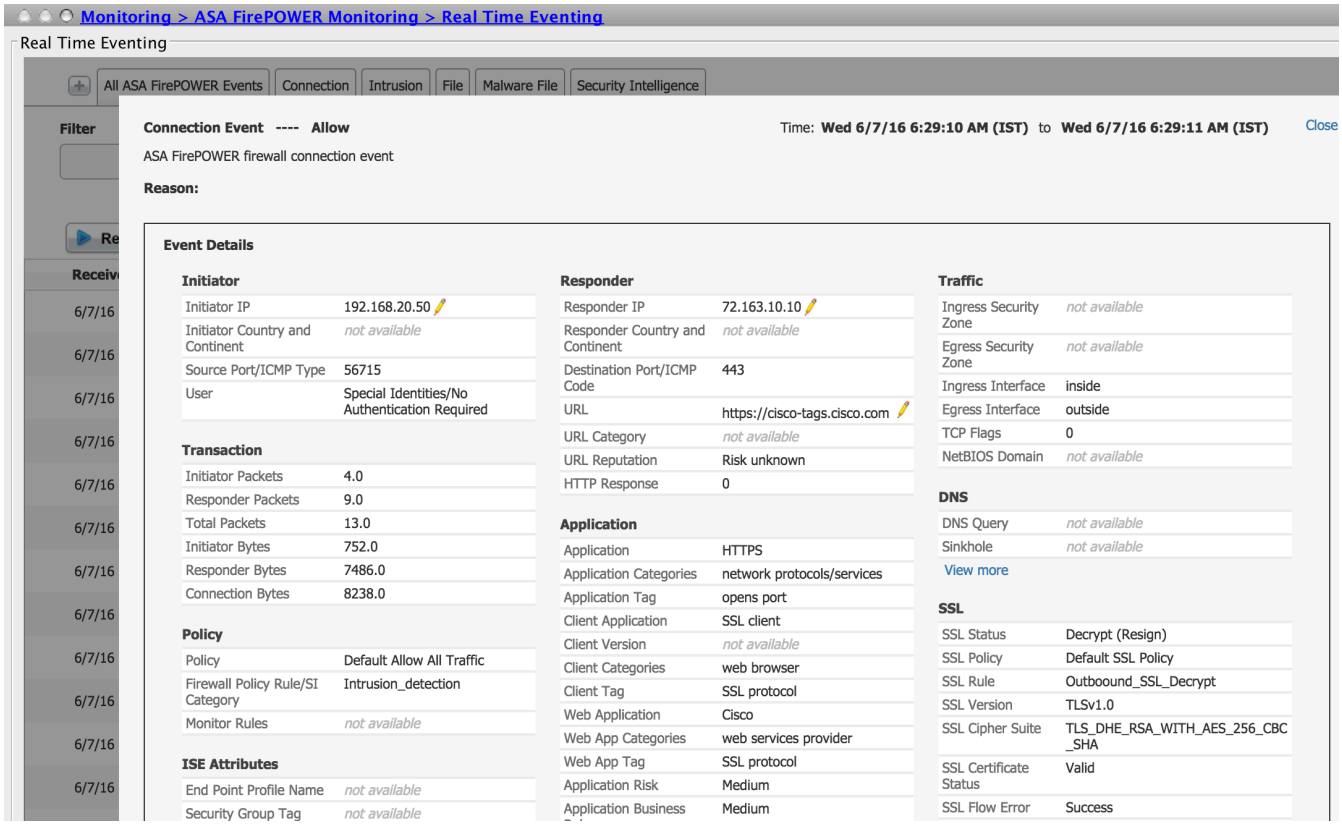
验证

使用本部分可确认配置能否正常运行。

- 对于出站SSL连接，从内部网络浏览公共SSL网站后，系统会提示证书的错误消息。检查证书内容并验证CA信息。系统将显示您在Firepower模块中配置的内部CA证书。接受错误消息以浏览SSL证书。要避免出现错误消息，请将CA证书添加到浏览器受信任CA列表。



- 检查连接事件，以验证流量所命中的SSL策略和SSL规则。导航至**Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing。选**择一个事件，然后单击**View Details**。验证SSL解密统计信息。



- 确保访问控制策略部署成功完成。
- 确保SSL策略包含在访问控制策略中。
- 确保SSL策略包含适当的入站和出站方向规则。
- 确保SSL规则包含定义相关流量的适当条件。
- 监控连接事件以验证SSL策略和SSL规则。
- 验证SSL解密状态。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems