使用ASDM（機箱內管理）在FirePOWER模組上配置SSL解密

目錄

簡介

本文檔介紹使用ASDM（機上管理）在FirePOWER模組上配置安全套接字層(SSL)解密。

必要條件

需求

思科建議您瞭解以下主題：

- ASA（自適應安全裝置）防火牆、ASDM（自適應安全裝置管理器）知識
- FirePOWER裝置知識
- 瞭解HTTPS/SSL協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本6.0.0及更高版本的ASA FirePOWER模組(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- 運行軟體版本6.0.0及更高版本的ASA FirePOWER模組(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 555-X)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

> **附註**：確保FirePOWER模組具有**保護**許可證以配置此功能。要驗證許可證，請導航到**Configuration > ASA FirePOWER Configuration > License**。

背景資訊

Firepower模組解密並檢查重定向到它的入站和出站SSL連線。一旦流量被解密，就會檢測並控制諸如facebook聊天等隧道應用。將檢查解密的資料是否存在威脅、URL過濾、檔案阻止或惡意資料。

傳出SSL解密

Firepower模組通過攔截出站SSL請求並為使用者想要訪問的站點重新生成證書，充當出站SSL連線的轉發代理。頒發機構(CA)是Firepower自簽名證書。如果firepower的證書不屬於已存在的層次結構的一部分，或者未新增到客戶端的瀏覽器快取中，則客戶端在瀏覽到安全站點時收到警告。Decrypt-Resignmethod用於執行出站SSL解密。

傳入SSL解密

如果入站流量流向內部Web伺服器或裝置，管理員將匯入受保護伺服器的證書和金鑰的副本。當SSL伺服器證書載入到firepower模組上，並且為入站流量配置了SSL解密策略時，裝置會在轉發流量時對流量進行解密和檢查。然後，模組會檢測流經此安全通道的惡意內容、威脅和惡意軟體。此外，解密已知金鑰方法用於執行入站SSL解密。

SSL解密的配置

SSL流量解密有兩種方法。

- 解密 — 為出站SSL流量重新簽名
- 解密 — 已知傳入SSL流量

出站SSL解密（解密 — 重新簽名）

對於公共SSL伺服器的任何SSL協商，Firepower模組均充當MITM（中間人）。它使用在firepower模組上配置的中間CA證書來重新簽署公共伺服器的證書。

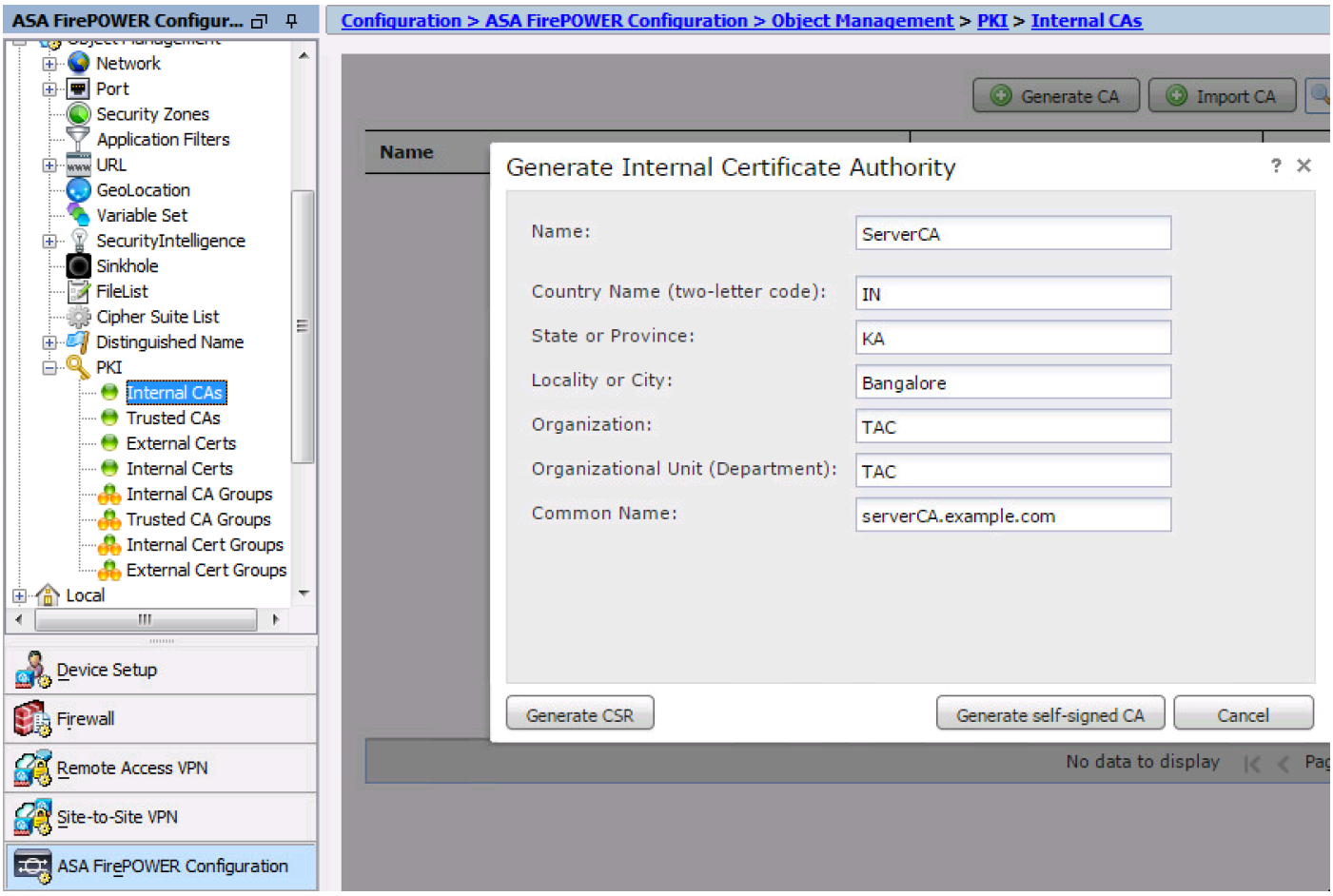
以下是設定傳出SSL解密的三個步驟。

步驟1.配置CA證書。

為證書重新簽名配置自簽名證書或中間受信任CA證書。

配置自簽名CA證書

要配置自簽名CA證書，請導航到**Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs**，然後按一下**Generate CA**。系統會提示CA證書的詳細資訊。如圖所示，根據您的要求填寫詳細資訊。



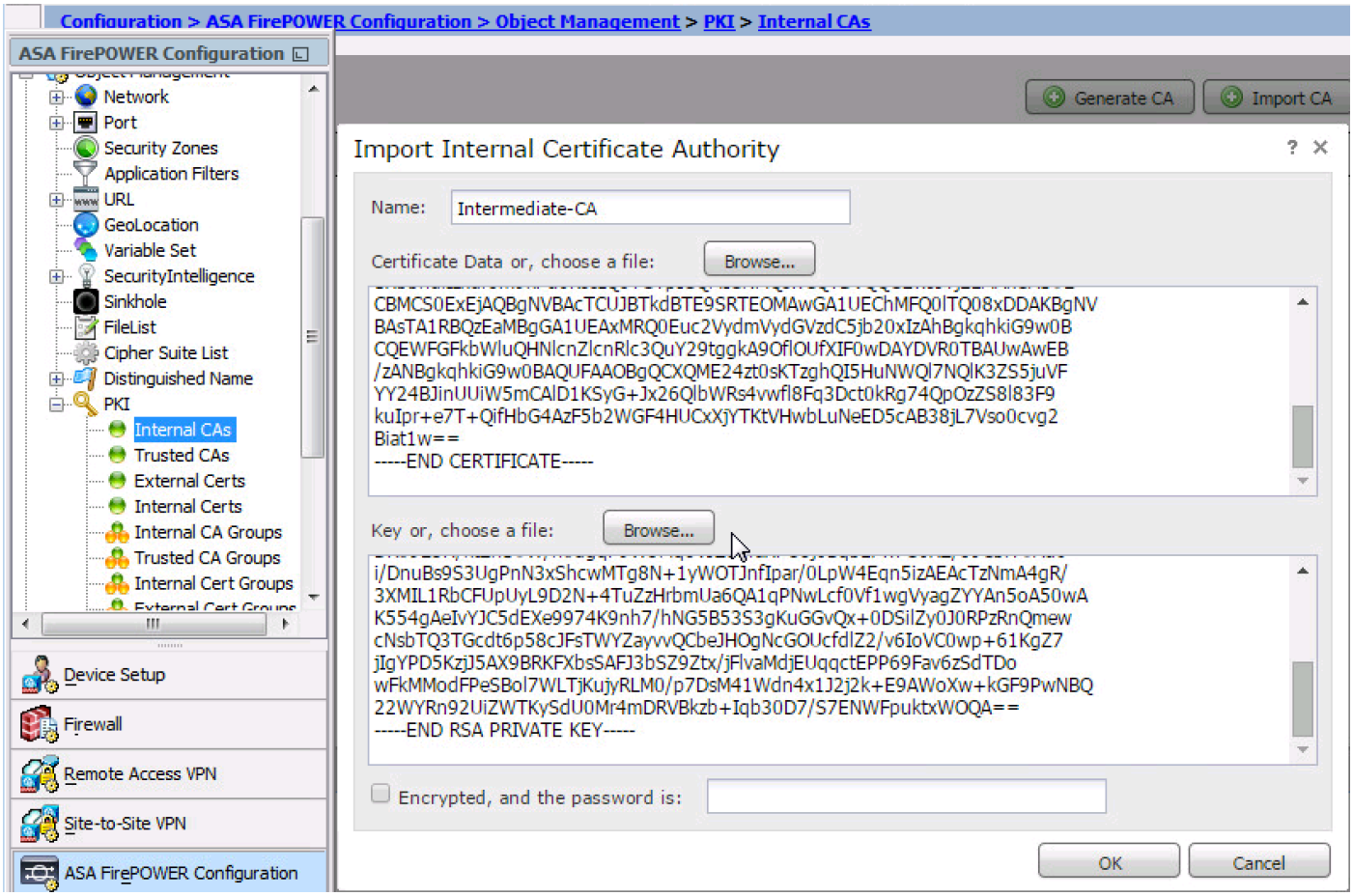
按一下**Generate self-signed CA**以生成內部CA證書。然後按一下**產生CSR** 以產生憑證簽署請求，該要求隨後會與要簽署的CA伺服器共用。

設定中間CA憑證

若要設定由另一個第三方CA簽署的中間CA憑證，請導覽至**Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs**，然後按一下**Import** CA。

指定證書的名稱。選擇**browse**，並從本地電腦上傳證書，或者在**Certificate Data**選項中複製貼上證書的內容。若要指定憑證的私密金鑰，請瀏覽金鑰檔案或在**Key**選項中複製貼上金鑰。

如果金鑰已加密，請啟用**Encrypted**覈取方塊並指定密碼。按一下**OK**以儲存憑證內容，如下圖所示：



步驟2.配置SSL策略。

SSL策略定義解密操作，並標識對其應用Decrypt-Resign解密方法的流量。根據您的業務需求和組織安全策略配置多個SSL規則。

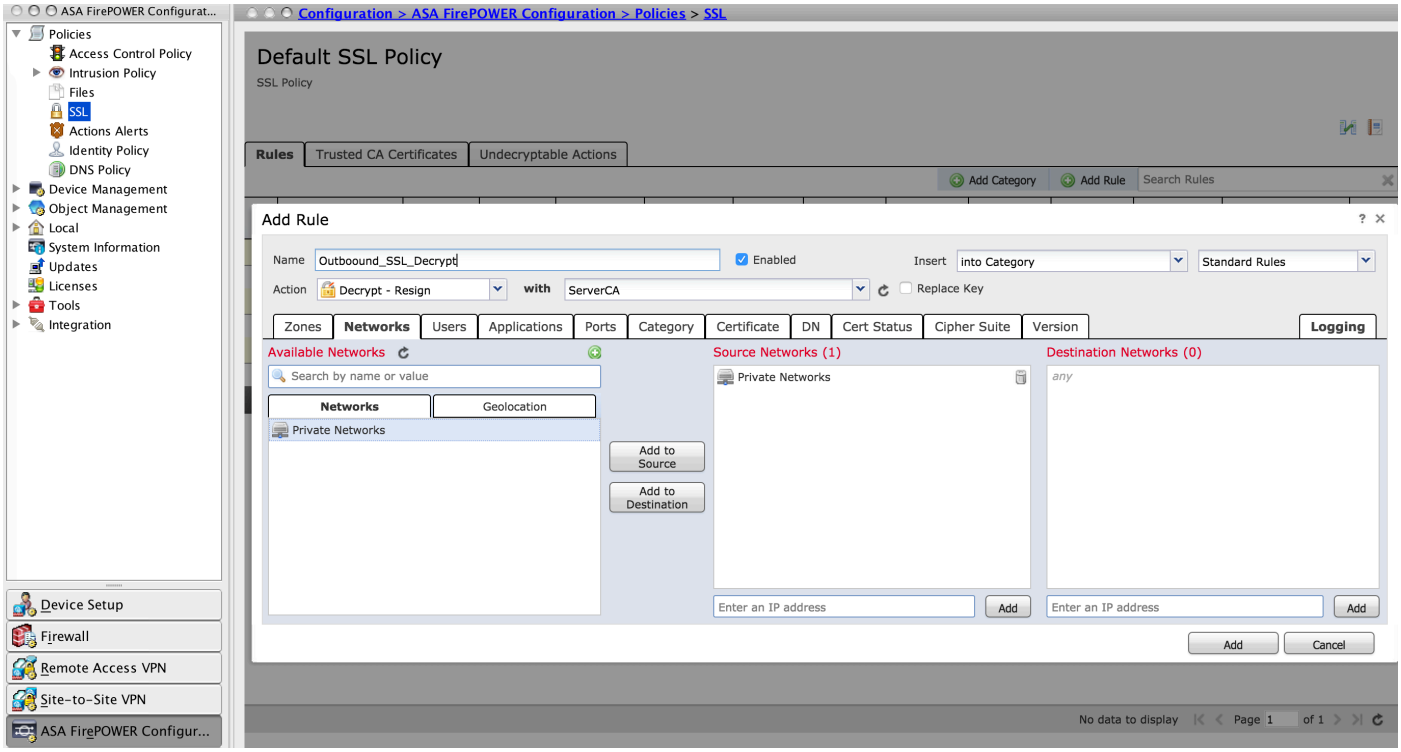
要配置SSL策略，請導航到**Configure > ASA FirePOWER Configuration > Policies > SSL**，然後點選**Add Rule**。

名稱：指定規則的名稱。

操作：將操作指定為**Decrypt - Resign，並從在上一步中配置的下拉選單中選擇CA證書。**

定義規則中的條件以匹配流量，因為有多個選項（區域、網路、使用者等）指定用於定義需要解密的流量。

若要產生SSL解密的事件，請啟用**logging at logging**選項，如下圖所示：



按一下**Add**以新增SSL規則。

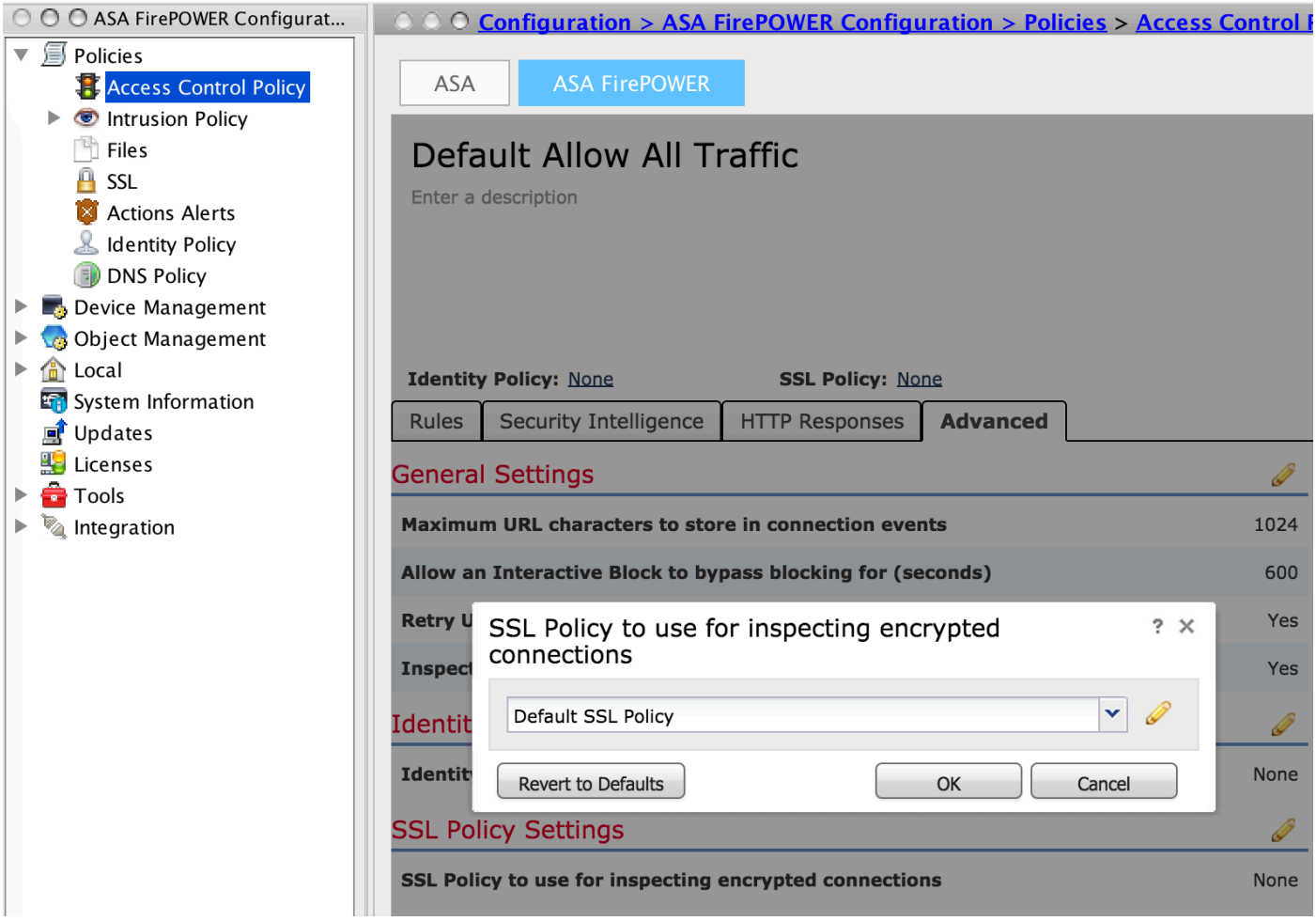
按一下**Store ASA Firepower Changes**儲存SSL策略的配置。

步驟3.配置訪問控制策略

使用適當的規則配置SSL策略後，必須在訪問控制中指定SSL策略以實施更改。

要配置訪問控制策略，請導航到**Configuration > ASA Firepower Configuration > Policies > Access Control**。

按一下**SSL Policy**中的**無**，或導航到**Advanced > SSL Policy Setting**。**從下拉選單中指定SSL策略，然後按一下OK**將其儲存，如下圖所示：



按一下 **儲存ASA Firepower更改** 儲存SSL策略的配置。

必須將訪問控制策略部署到感測器。在應用策略之前，模組上顯示**訪問控制策略已過**期。若要將更改部署到感測器，請按一下**部署**，然後選擇**部署FirePOWER更改選項。驗證所做的更改，然後按一下Deploy（部署）。**

> **附註**：在5.4.x版本中，如果需要將訪問策略應用到感測器，請按一下Apply ASA FirePOWER Changes。

> **附註**：導航到**監控> ASA Firepower監控>任務狀態。**然後應用配置更改以確保任務完成。

傳入SSL解密（解密 — 已知）

入站SSL解密(Decrypt-Known)方法用於解密已為其配置了伺服器證書和私鑰的入站SSL流量。您需要將伺服器證書和私鑰匯入Firepower模組。當SSL流量到達Firepower模組時，會解密流量並對解密的流量執行檢查。檢查後，Firepower模組重新加密流量並將其傳送到伺服器。

以下是設定傳出SSL解密的四個步驟：

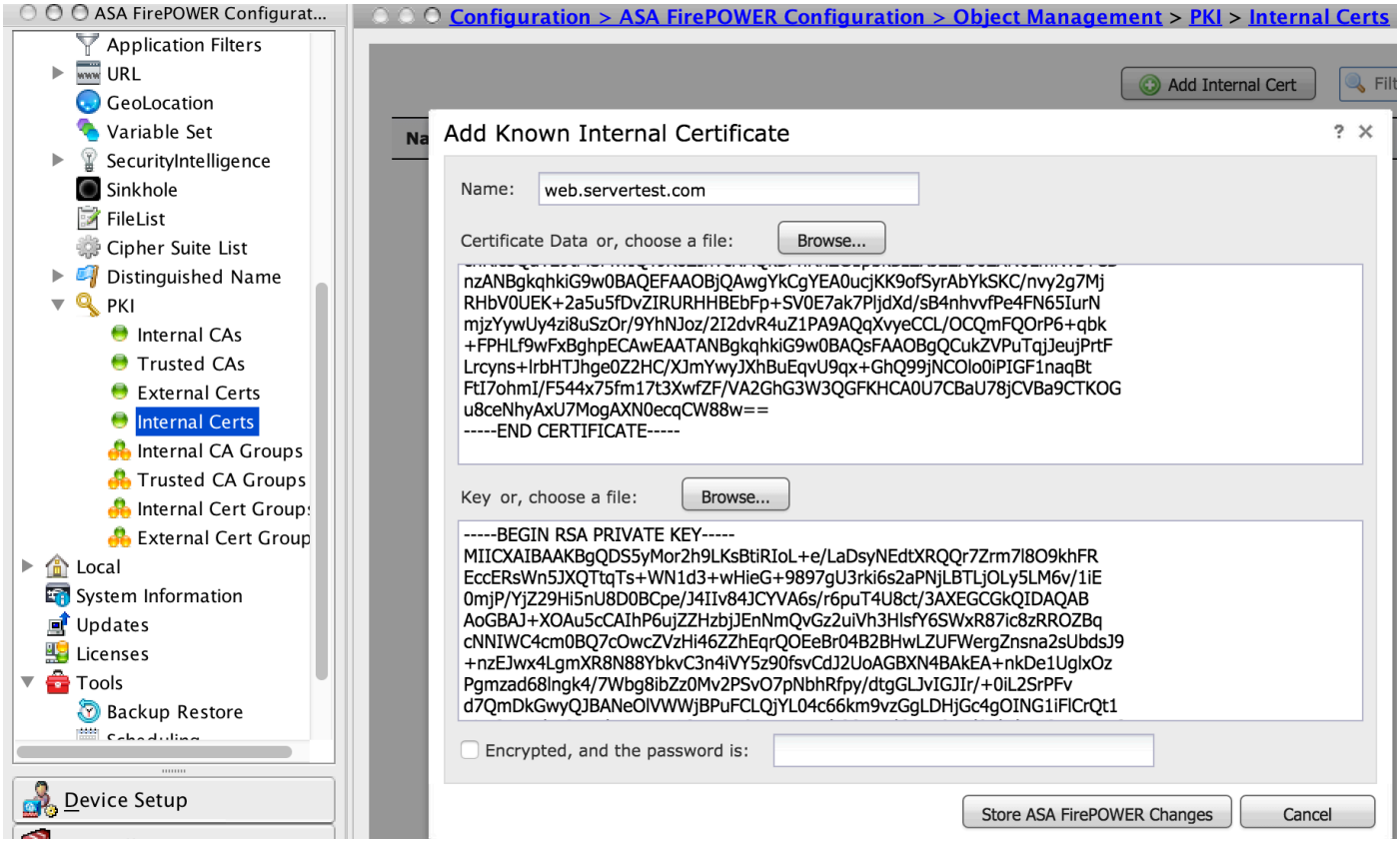
步驟1. 匯入伺服器憑證和金鑰。

要匯入伺服器證書和金鑰，請導航到Configuration > ASA Firepower Configuration > Object

Management > PKI > Internal Certs，然後點選Add Internal Cert。

如圖所示，指定憑證的名稱。選擇browse以從本地電腦中選擇證書，或者複製貼上證書資料中的**證書內容**。若要指定憑證的私密金鑰，請瀏覽金鑰檔案，或者在Key選項中複製貼上金鑰。

如果金鑰已加密，請啟用Encrypted覈取方塊並指定密碼，如下圖所示：



按一下Store ASA FirePOWER Changes以儲存證書內容。

步驟2.匯入CA證書（可選）。

對於由內部中間CA證書或根CA證書簽名的伺服器證書，需要將CA證書的內部鏈匯入firepower模組。執行匯入後，firepower模組能夠驗證伺服器證書。

要匯入CA證書，請導航到Configuration > ASA Firepower Configuration > Object Management > Trusted CAs，然後點選Add Trusted CA以新增CA證書。

步驟3.配置SSL策略。

SSL策略定義您要配置解密已知方法以對入站流量進行解密的操作和伺服器詳細資訊。如果有多個內部伺服器，請根據不同的伺服器及其處理的流量配置多個SSL規則。

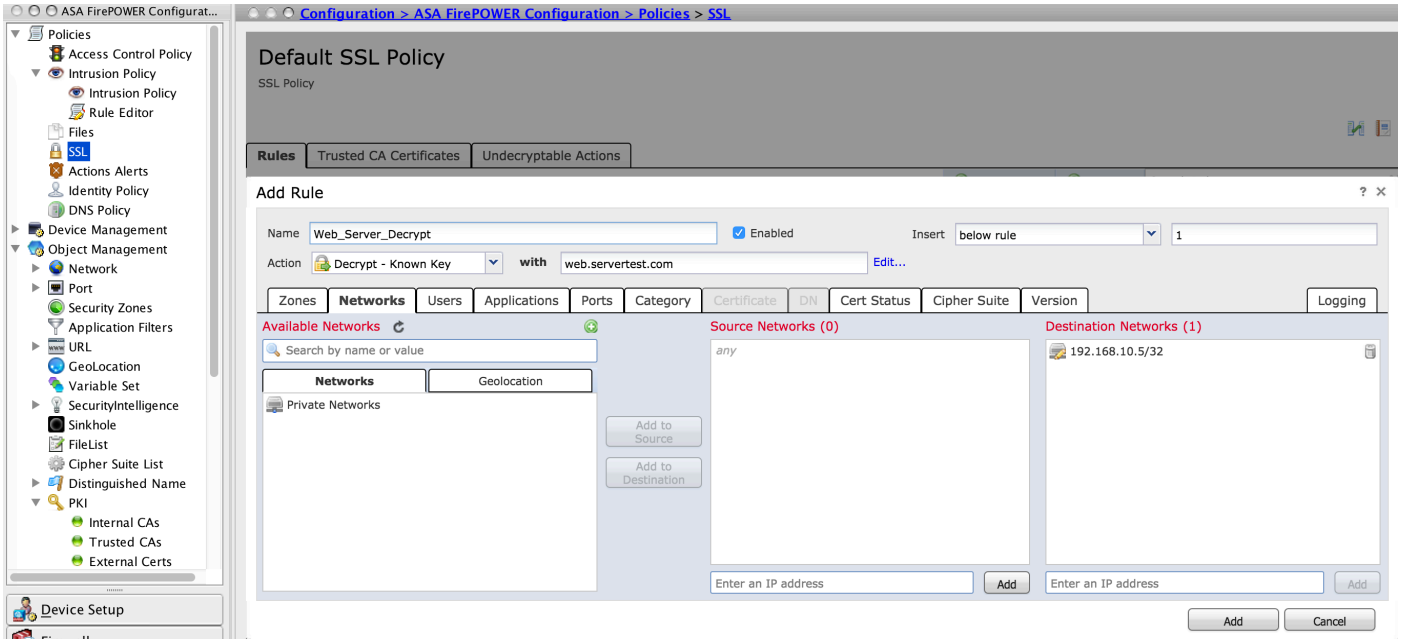
要配置SSL策略，請導航到Configure > ASA FirePOWER Configuration > Policies > SSL，然後點選Add Rule。

名稱：指定規則的名稱。

操作：將操作指定為Decrypt - known，並從在上一步中配置的下拉選單中選擇CA證書。

定義條件以匹配此規則，因為有多個選項（網路、應用程式、埠等）指定用於定義要為其啟用SSL解密的伺服器相關流量。在「受信任CA證書中的選定受信任CA」頁籤中指定內部CA。

要生成SSL解密事件，請啟用loggingat **logging**選項。



按一下**Add**以新增SSL規則。

然後點選**儲存ASA Firepower更改**以儲存SSL策略的配置。

步驟4.配置訪問控制策略。

使用適當的規則配置SSL策略後，必須在訪問控制中指定SSL策略以實施更改。

要配置訪問控制策略，請導航到**Configuration > ASA Firepower Configuration > Policies > Access Control。**

按一下**SSL Policy** 旁邊的**None** 選項，或導覽至**Advanced > SSL Policy Setting**，從下拉選單中指定SSL策略，然後按一下**OK**進行儲存。

按一下 **儲存ASA Firepower更改** 儲存SSL策略的配置。

您必須部署訪問控制策略。在應用策略之前，可以在模組上看到指示訪問控制策略已過期。若要將更改部署到感測器，請按一下**部署**，然後選擇**部署FirePOWER更改選項。驗證所做的變更，然後在快顯視窗中按一下Deploy。**

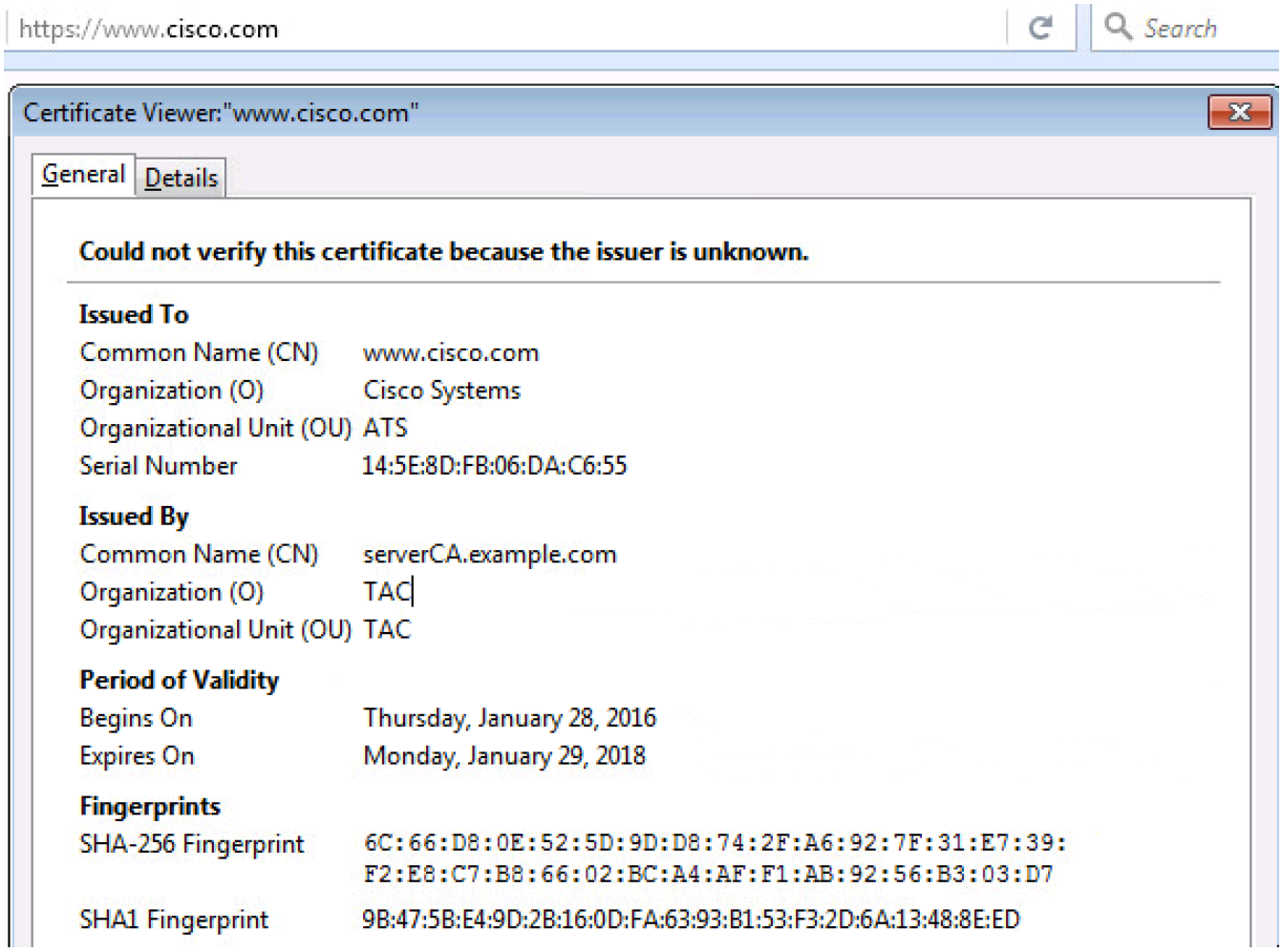
> **附註**：在5.4.x版本中，如果需要將訪問策略應用到感測器，請按一下**Apply ASA FirePOWER Changes。**

> **附註**：導航到**監控> ASA Firepower監控>任務狀態。**然後應用配置更改以確保任務完成。

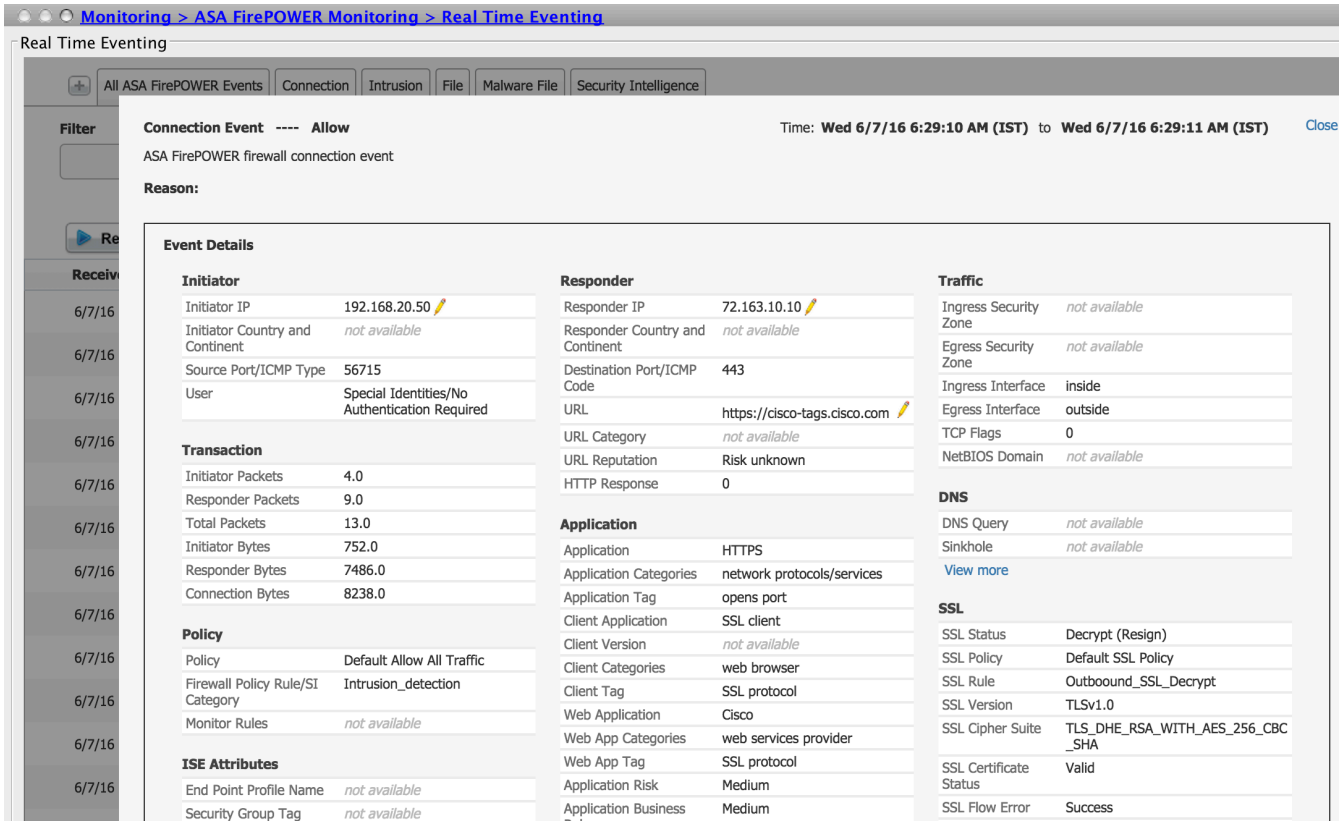
驗證

使用本節內容，確認您的組態是否正常運作。

- 對於出站SSL連線，一旦從內部網路瀏覽公共SSL網站，系統就會提示證書的錯誤消息。檢查證書內容並驗證CA資訊。系統將顯示在Firepower模組中配置的內部CA證書。接受錯誤消息以瀏覽SSL證書。若要避免此錯誤訊息，請將CA憑證新增到您的瀏覽器受信任CA清單中。



- 檢查連線事件以驗證流量所中斷的SSL策略和SSL規則。導航到**Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing。選擇**事件並按一下**View Details**。驗證SSL解密統計資訊。



- 確保訪問控制策略部署成功完成。
- 確保SSL策略包含在訪問控制策略中。
- 確保SSL策略包含入站和出站方向的適當規則。
- 確保SSL規則包含用於定義相關流量的適當條件。
- 監控連線事件以驗證SSL策略和SSL規則。
- 驗證SSL解密狀態。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 技術支援與文件 - Cisco Systems