

# 在Cisco FireSIGHT系統上配置SSL檢查策略

## 目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[組態](#)

[1.解密並辭職](#)

[選項1:使用FireSIGHT中心作為根證書頒發機構\(CA\)](#)

[選項2:讓內部CA對您的證書簽名](#)

[選項3:匯入CA證書和金鑰](#)

[2.使用已知金鑰解密](#)

[匯入已知證書 \( 解密和重新簽名的替代方法 \)](#)

[其他配置](#)

[驗證](#)

[解密 — 重新簽名](#)

[解密 — 已知證書](#)

[疑難排解](#)

[問題1:某些網站可能無法在Chrome瀏覽器上載入](#)

[問題2:在某些瀏覽器中收到不可信的警告/錯誤](#)

[參考資料](#)

[相關思科支援社群討論](#)

## 簡介

SSL檢查功能可讓您封鎖加密流量而不對其進行檢查，或者使用存取控制檢查加密或解密的流量。本文檔介紹在Cisco FireSIGHT系統上設定SSL檢查策略的配置步驟。

## 必要條件

### 採用元件

- Cisco FireSIGHT管理中心
- Cisco Firepower 7000或8000裝置
- 軟體版本5.4.1或更高版本

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。

**警告：** 如果在受管裝置上應用SSL檢查策略，可能會影響網路效能。

## 組態

您可以通過以下方式配置SSL檢查策略來解密流量：

### 1.解密並辭職：

- 選項1:使用FireSIGHT中心作為根證書頒發機構(CA)，或
- 選項2:讓內部CA對您的證書簽名，或者
- 選項3:匯入CA證書和金鑰

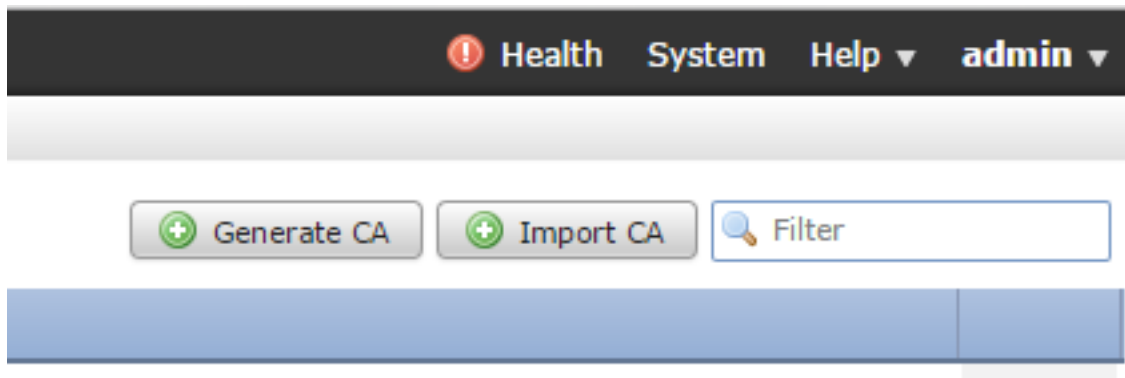
### 2.使用已知證書解密：

- 登入到FireSIGHT管理中心，然後導航到對象。
- 在Objects頁面上，展開PKI，然後選擇Internal CAs。

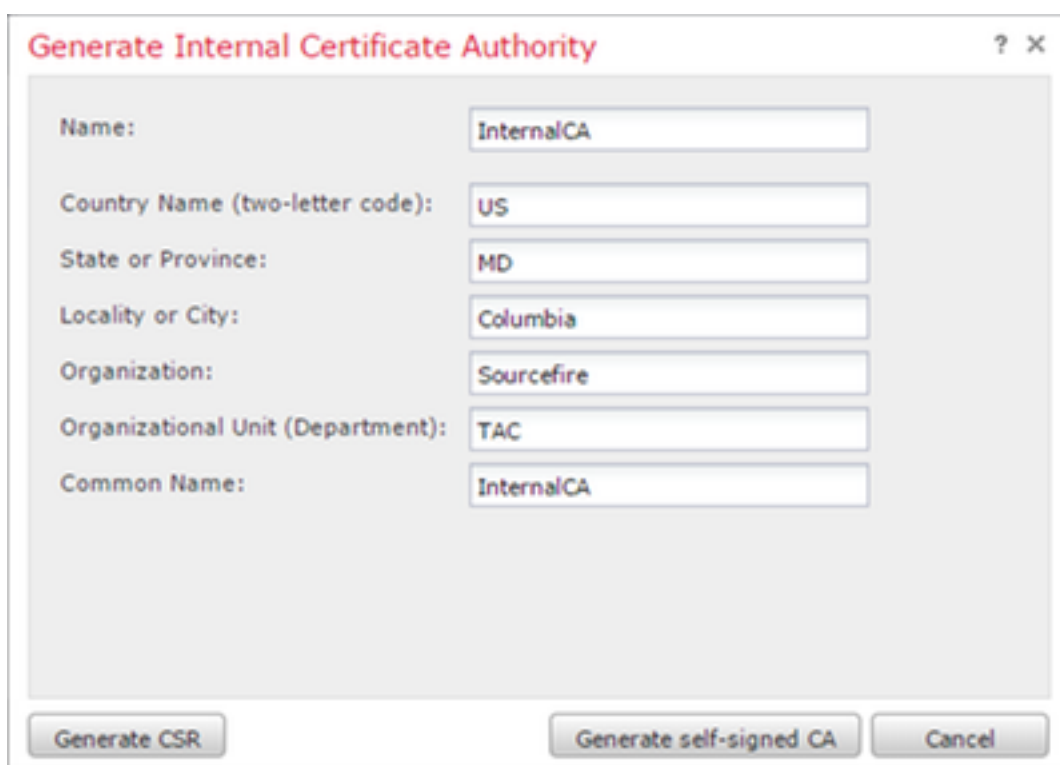
## 1.解密並辭職

### 選項1:使用FireSIGHT中心作為根證書頒發機構(CA)

i.按一下生成CA。



二。填寫相關資訊

A screenshot of a dialog box titled 'Generate Internal Certificate Authority'. The dialog has a title bar with a question mark and a close button. It contains several input fields for certificate information:

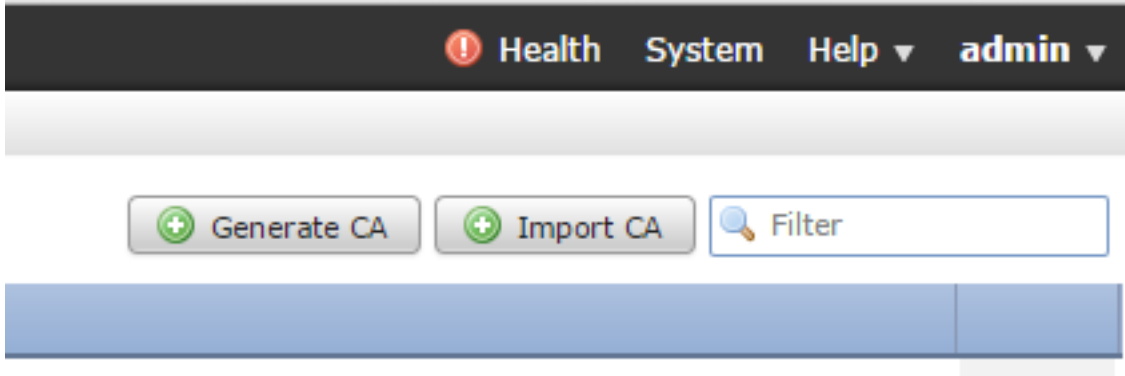
- Name: InternalCA
- Country Name (two-letter code): US
- State or Province: MD
- Locality or City: Columbia
- Organization: Sourcefire
- Organizational Unit (Department): TAC
- Common Name: InternalCA

At the bottom of the dialog, there are three buttons: 'Generate CSR', 'Generate self-signed CA', and 'Cancel'.

三。按一下「Generate self-signed CA」。

## 選項2:讓內部CA對您的證書簽名

i.按一下「Generate CA」。

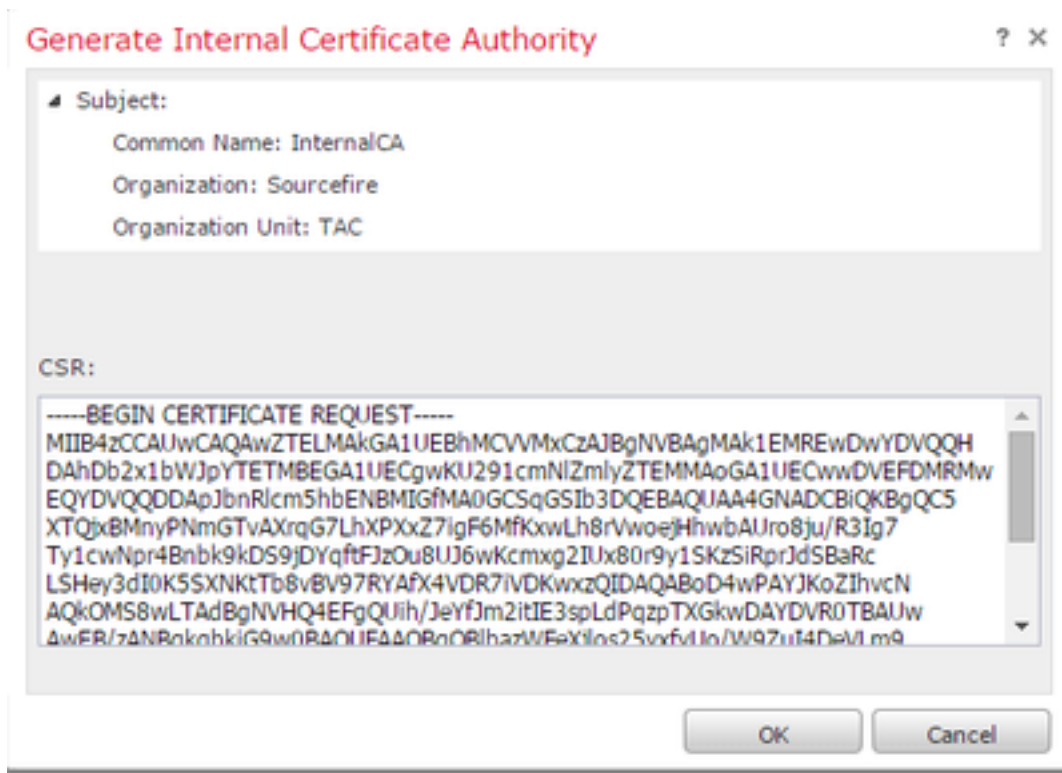


二。填寫相關資訊。

A screenshot of a dialog box titled 'Generate Internal Certificate Authority'. The dialog box has a title bar with a question mark and a close button. It contains several text input fields with labels: 'Name:' (InternalCA), 'Country Name (two-letter code):' (US), 'State or Province:' (MD), 'Locality or City:' (Columbia), 'Organization:' (Sourcefire), 'Organizational Unit (Department):' (TAC), and 'Common Name:' (InternalCA). At the bottom of the dialog box, there are three buttons: 'Generate CSR', 'Generate self-signed CA', and 'Cancel'.

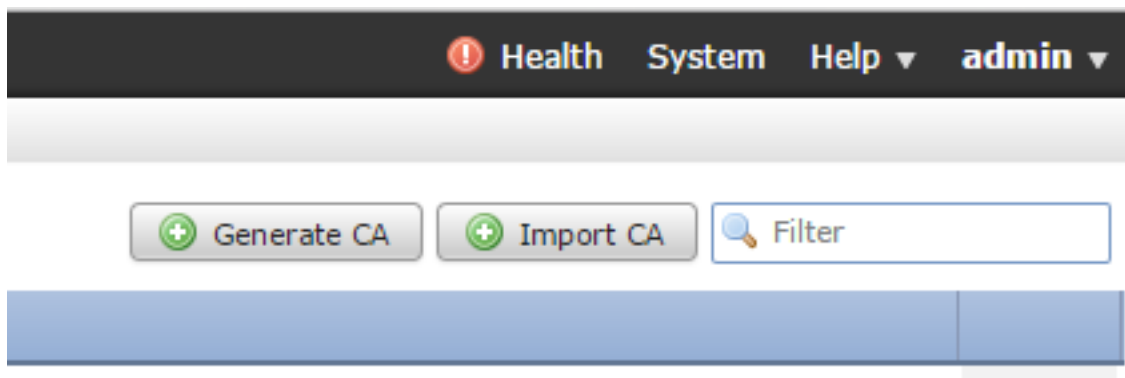
**附註：**您可能需要聯絡您的CA管理員以確定他們是否具有簽名請求的模板。

三。複製包括—BEGIN CERTIFICATE REQUEST—和—END CERTIFICATE REQUEST在內的整個證書，然後將其儲存到副檔名為.req 的文本檔案中。



附註：您的CA管理員請求除.req之外的其他副檔名。

### 選項3:匯入CA證書和金鑰

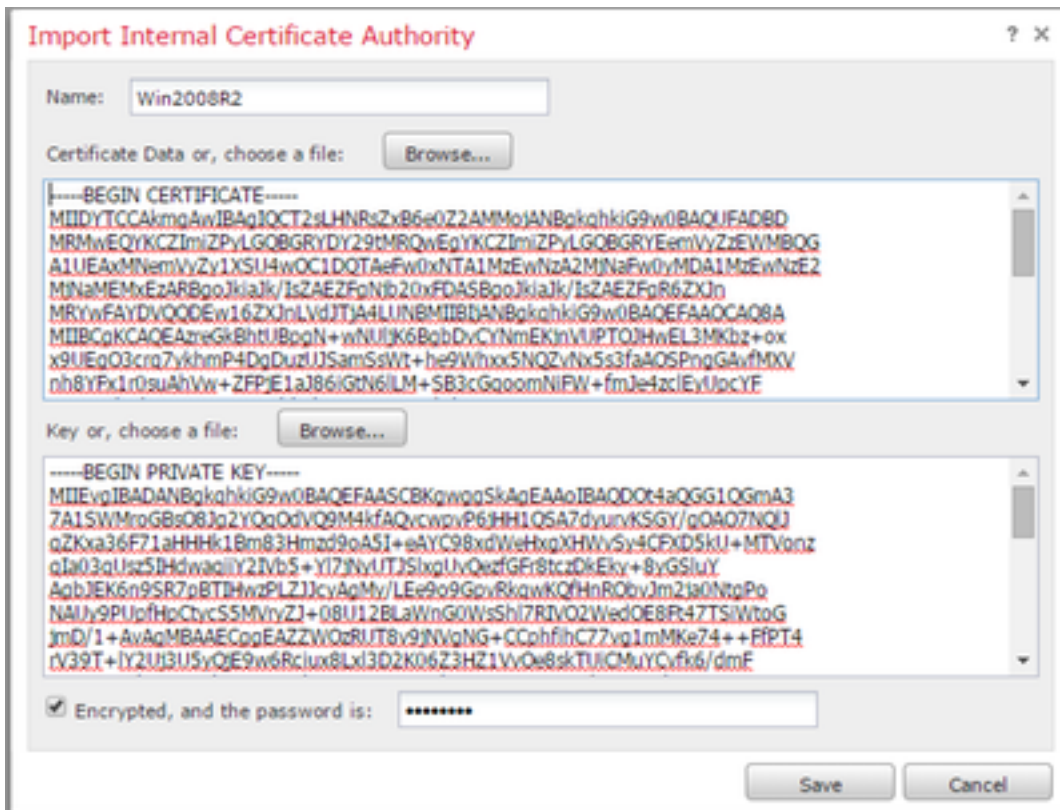


i. 按一下「Import CA」。

二。瀏覽到或貼上到證書。

三。瀏覽到私鑰或貼上到私鑰中。

四。選中加密框並鍵入密碼。



附註：如果沒有密碼，請選中加密框並將其留空。

## 2. 使用已知金鑰解密

### 匯入已知證書（解密和重新簽名的替代方法）

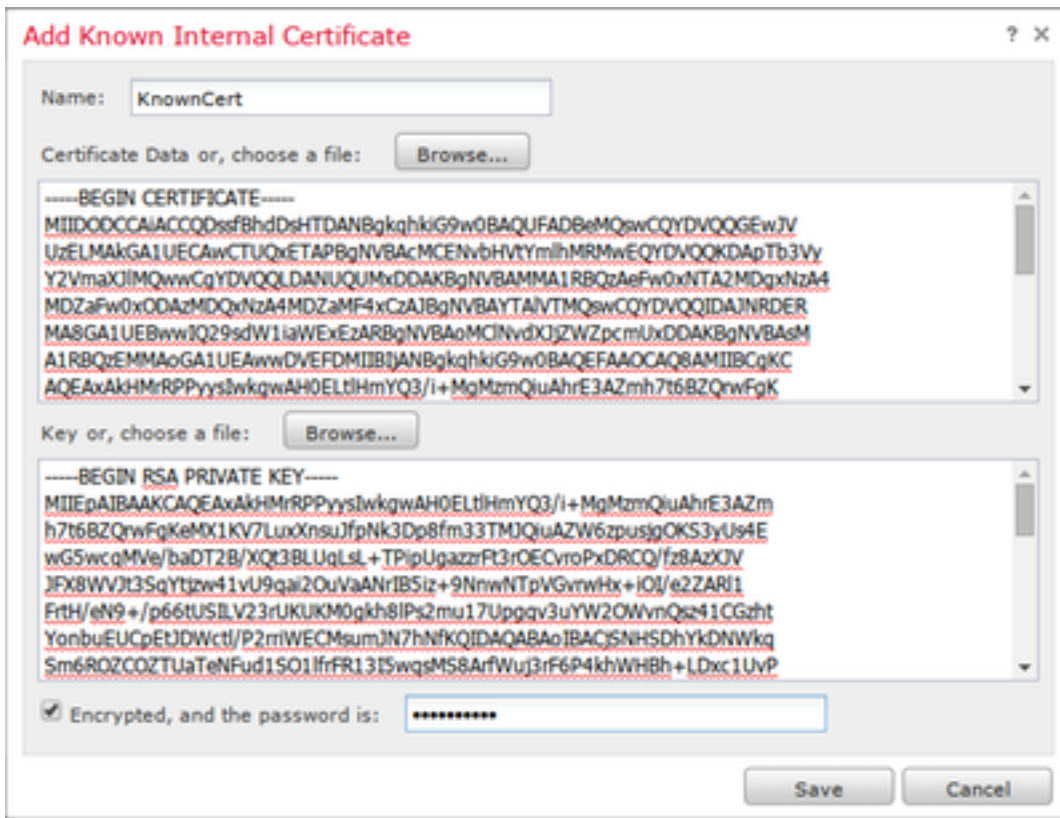
i. 從左側的「對象」(Objects)頁面中展開PKI，然後選擇「內部證書」(Internal Certs)。

二。按一下Add Internal Cert。

三。瀏覽到或貼上到證書。

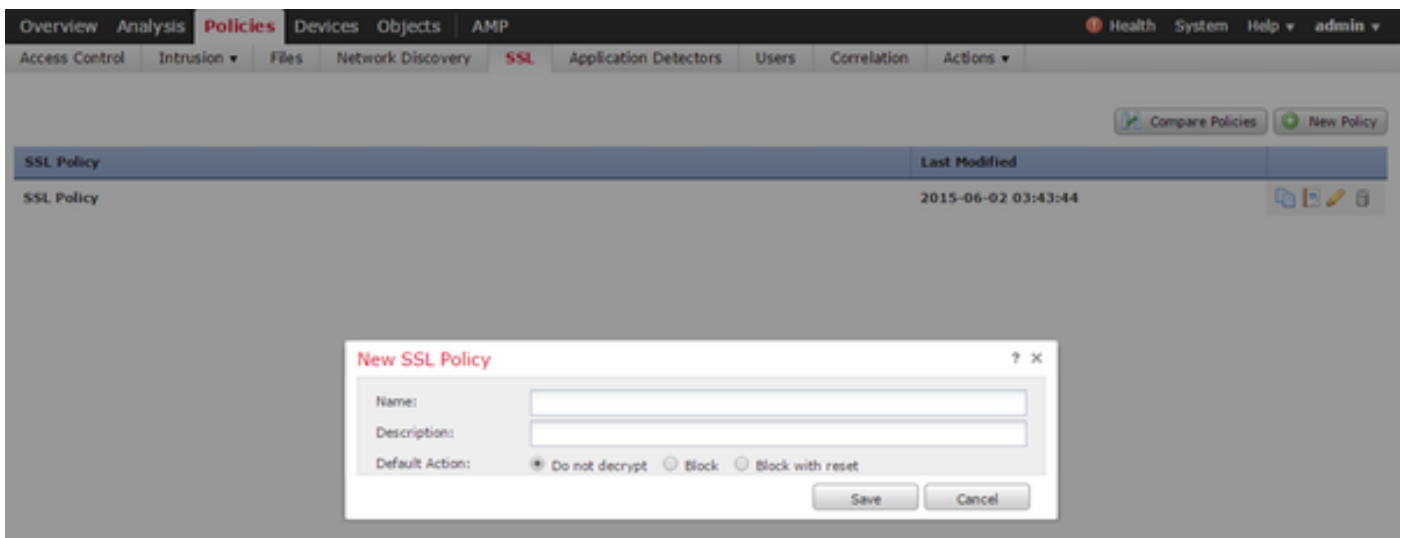
四。瀏覽到私鑰或貼上到私鑰中。

v. 選中Encrypted框並鍵入密碼。



附註：如果沒有密碼，請將Encrypted框留空。

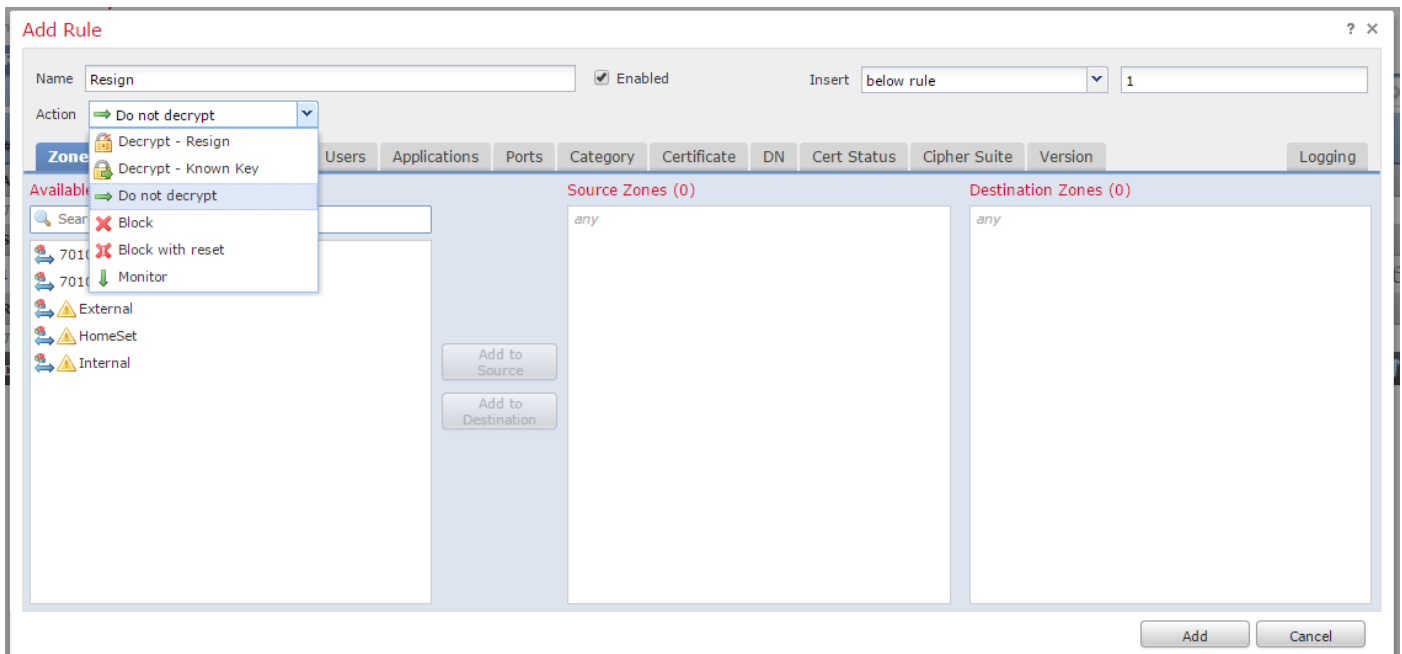
4. 定位至Policies > SSL，然後按一下New Policy。



5. 提供名稱並選擇預設操作。系統將顯示SSL策略編輯器頁面。SSL策略編輯器頁的工作方式與「訪問控制策略編輯器」頁的工作方式相同。

附註：如果不確定Default Action，則建議從Do not decrypt開始。

6. 在SSL策略編輯器頁面上，按一下Add Rule。在Add Rule視窗中，提供規則的名稱，並填寫所有其他相關資訊。



以下部分介紹「新增規則」(Add Rule)視窗中的各種選項：

#### 動作

### 解密 — 重新簽名

- 感測器充當中間人(MitM)，接受與使用者的連線，然後建立與伺服器的新連線。例如：瀏覽器中https://www.facebook.com中的使用者型別。通訊量到達感測器，然後感測器使用選定的CA證書與使用者協商並建立SSL隧道A。同時，感測器連線到https://www.facebook.com並建立SSL隧道B。
- 最終結果：使用者可以在規則中檢視證書，而不是facebook的證書。
- 此操作需要內部CA。如果您希望替換金鑰，請選擇「替換金鑰」。使用者會收到您選擇的憑證。

**附註：** 不能在被動模式下使用。

### 解密 — 已知金鑰

- 感測器具有用於解密流量的金鑰。例如：瀏覽器中https://www.facebook.com中的使用者型別。通訊量到達感測器，感測器解密通訊量，然後檢查通訊量。
- 最終結果：使用者檢視facebook的證書
- 此操作需要內部證書。這會新增到Objects > PKI > Internal Certs中。

**附註：** 您的組織必須是域和證書的所有者。例如，facebook.com讓終端使用者看到facebook證書的唯一可能方式是，您實際擁有域facebook.com（即，您的公司是Facebook，Inc），並且擁有由公共CA簽名的facebook.com證書的所有權。您只能使用組織擁有的站點的已知金鑰解密。

解密已知金鑰的主要目的是解密指向https伺服器的流量，以保護您的伺服器免受外部攻擊。要檢查到外部https站點的客戶端流量，您將使用decrypt resign，因為您沒有伺服器，並且您對檢查連線到外部加密站點的網路中的客戶端流量感興趣。

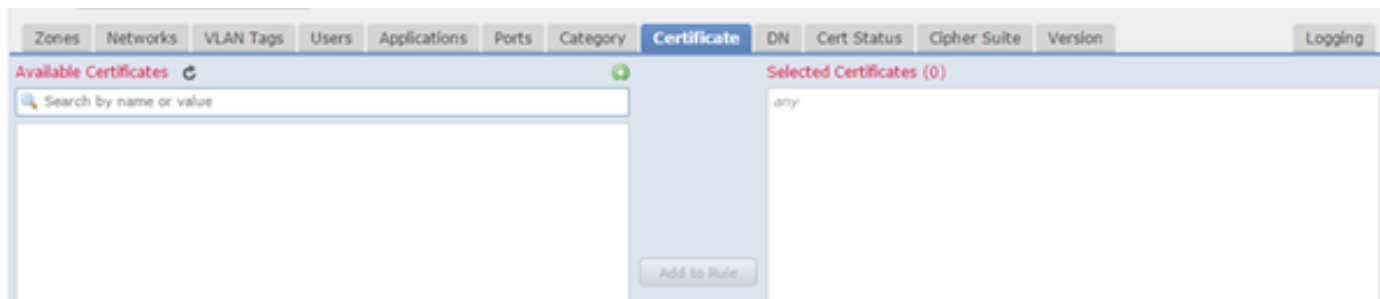
**附註：** DHE和ECDHE要想解密，我們必須線上。

### 不解密

流量會繞過SSL策略並繼續執行訪問控制策略。

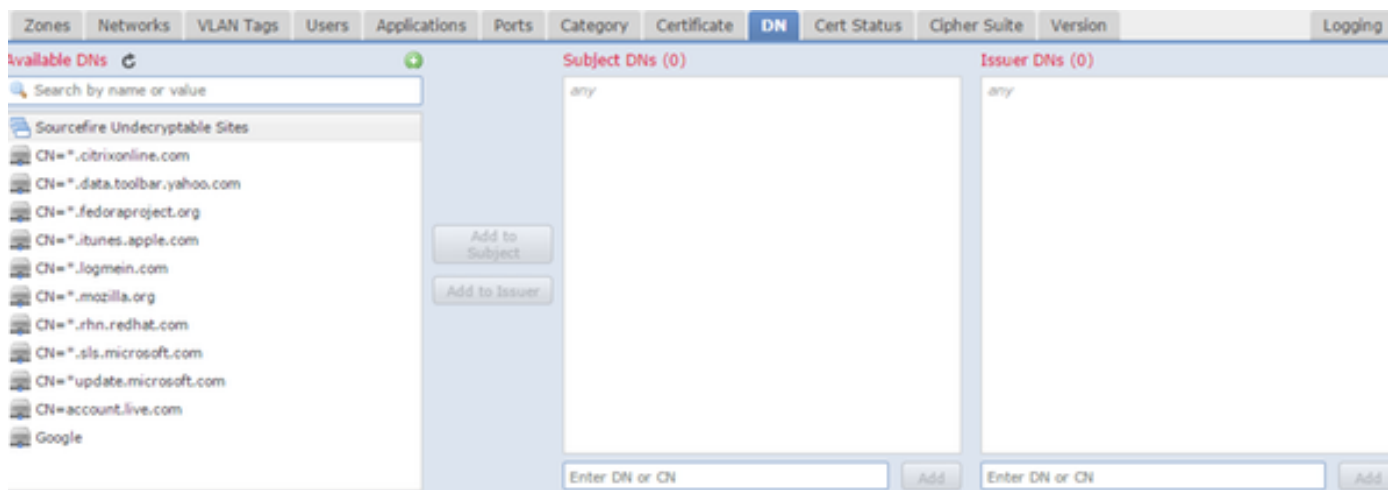
### 憑證

規則匹配使用此特定證書的SSL流量。



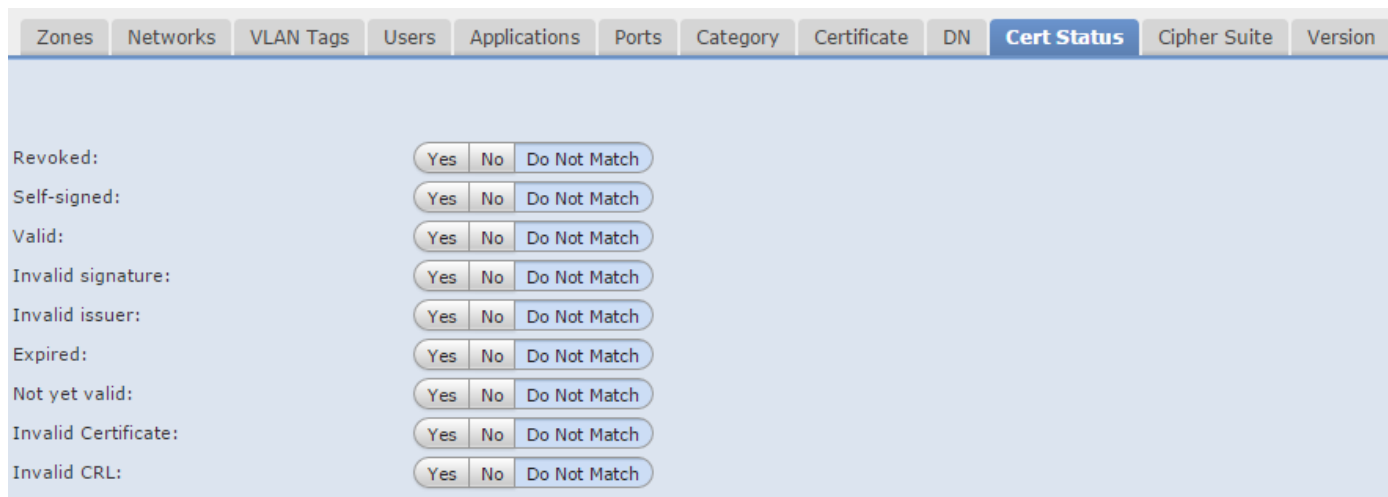
### DN

規則使用證書中的某些域名匹配SSL流量。



### 證書狀態

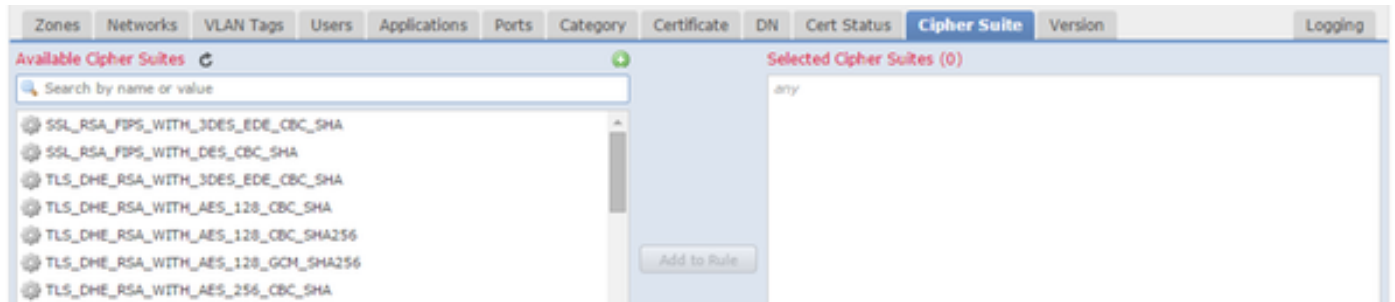
規則匹配具有以下證書狀態的SSL流量。



### 密碼套件

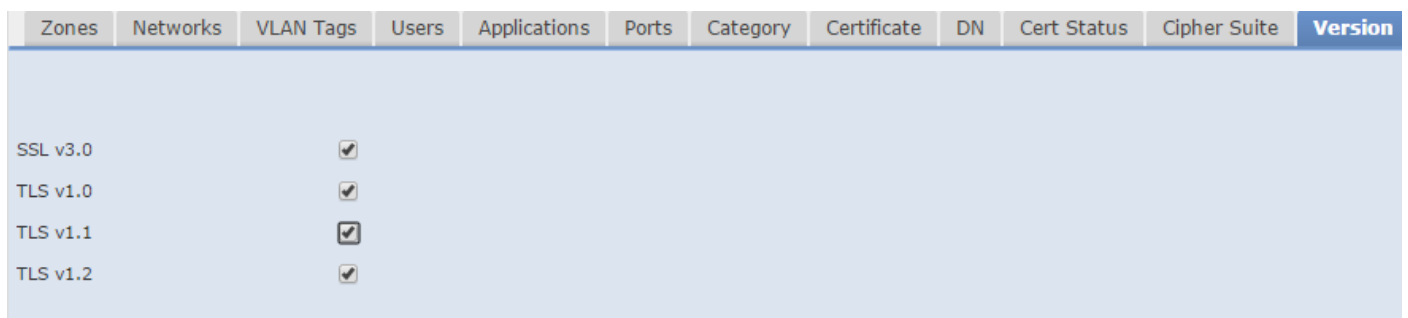


規則使用這些密碼套件匹配SSL流量。



版本

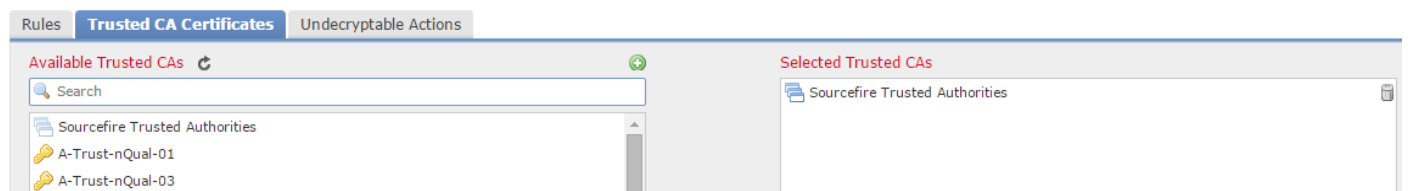
規則僅適用於具有選定版本的SSL的SSL流量。



記錄

啟用日誌記錄以檢視SSL流量的連線事件。

7. 按一下**Trusted CA Certificate**。這是將受信任的CA新增到策略的位置。



8. 按一下**無法解密的操作**。以下是感測器無法解密通訊量的操作。您可以在FireSIGHT管理中心的聯機幫助([幫助](#)>[線上](#))中找到這些定義。

Rules	Trusted CA Certificates	Undecryptable Actions
Compressed Session		Inherit Default Action ▼
SSLv2 Session		Inherit Default Action ▼
Unknown Cipher Suite		Inherit Default Action ▼
Unsupported Cipher Suite		Inherit Default Action ▼
Session not cached		Inherit Default Action ▼
Handshake Errors		Inherit Default Action ▼
Decryption Errors		Block ▼

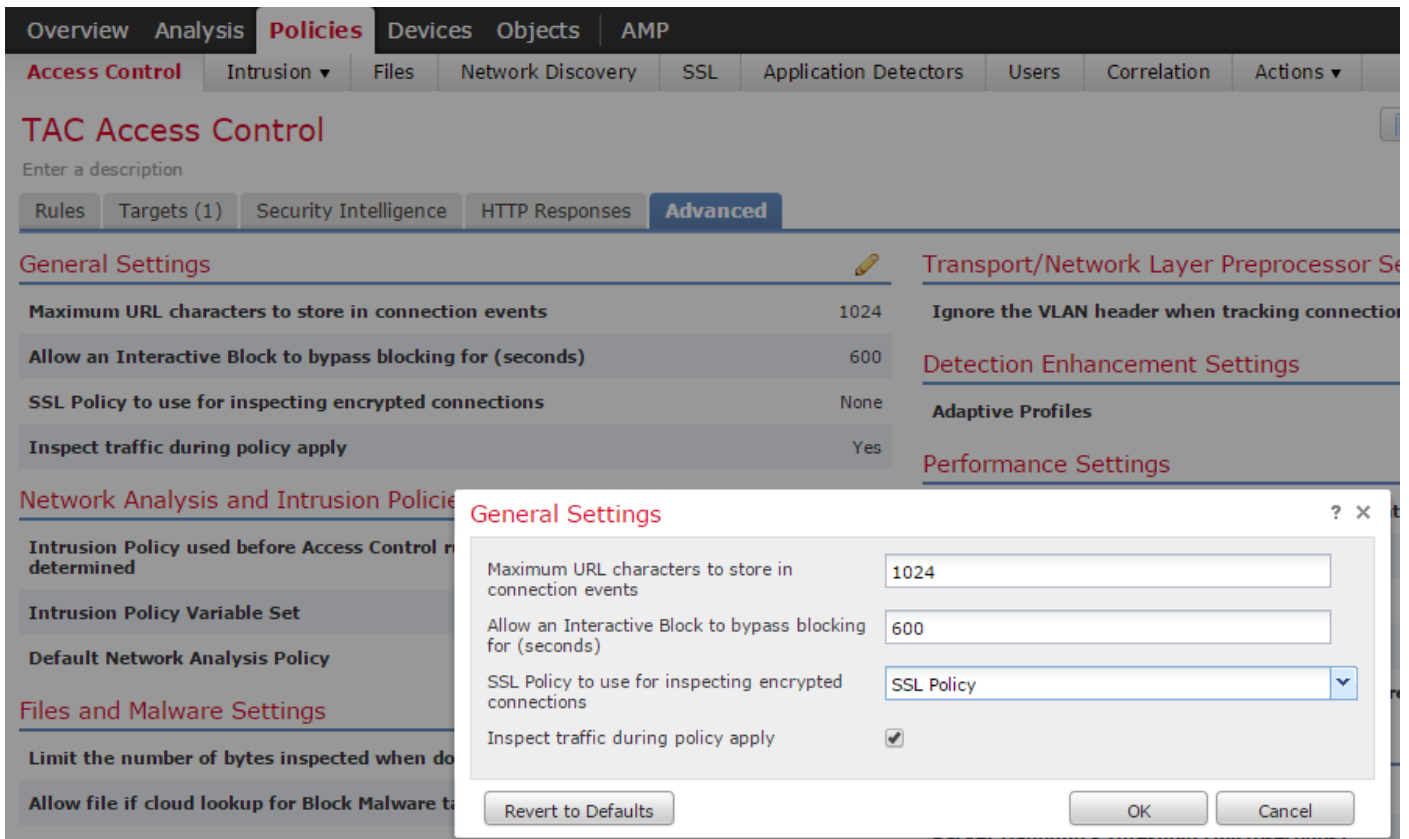
- **壓縮會話**:SSL會話應用資料壓縮方法。
- **SSLv2會話**:使用SSL版本2對會話進行加密。請注意，如果客戶端hello消息是SSL 2.0，並且傳輸的流量的其餘部分是SSL 3.0，則流量可解密。
- **未知密碼套件**:系統無法識別密碼套件。
- **不支援的密碼套件**：系統不支援基於檢測到的密碼套件進行解密。
- **未快取會話**:SSL會話已啟用會話重用，客戶端和伺服器使用會話識別符號重新建立了會話，系統未快取該會話識別符號。
- **握手錯誤**:SSL握手協商期間出錯。
- **解密錯誤**:流量解密期間出錯。

**附註：**預設情況下，這些操作將繼承「預設操作」。如果預設操作為「阻止」，則可能會遇到意外問題

9.儲存策略。

10.導覽至Policies > Access Control。編輯策略或建立新的訪問控制策略。

11.按一下Advanced，然後編輯General Settings。



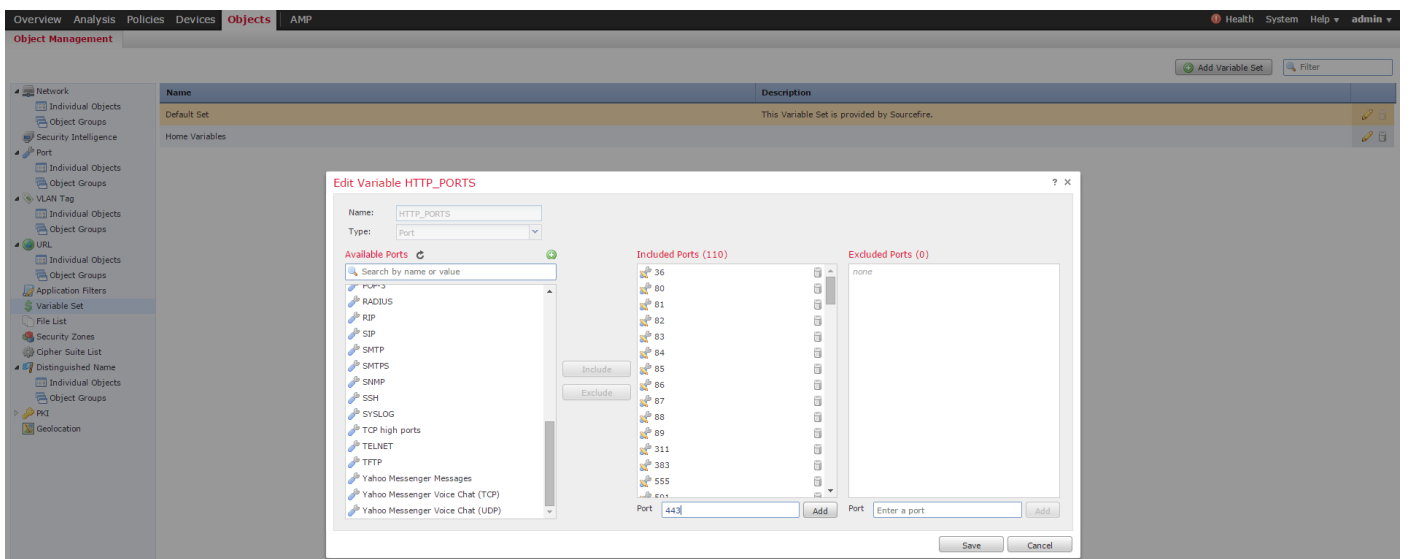
12. 從下拉選單中選擇您的SSL策略。

13. 按一下OK儲存。

## 其他配置

為了正確識別，應對入侵策略進行以下更改：

i.\$HTTP\_PORTS變數應包括埠443以及具有將被策略解密的https流量的任何其他埠(Objects > Object Management > Variable Set > Edit變數集)。



二。檢查加密流量的網路分析策略必須在HTTP前處理器設定的埠欄位中包含埠443 ( 以及具有將被策略解密的https流量的任何其他埠 ) ，否則將不會觸發任何具有http內容修飾符的http規則(即

http\_uri、http\_header等)，因為這依賴於定義的http埠，並且將不會為未通過指定埠的流量填充snort中的http緩衝區。

三。（可選，但建議使用，以便更好地檢查）將https埠新增到在兩個埠上執行資料流重組欄位中的TCP資料流配置中。

四。在計畫的維護時段重新應用修訂的訪問控制策略。

**警告：**此修改策略可能會導致嚴重的效能問題。這應在生產時間之外進行測試，以減少網路中斷或效能風險。

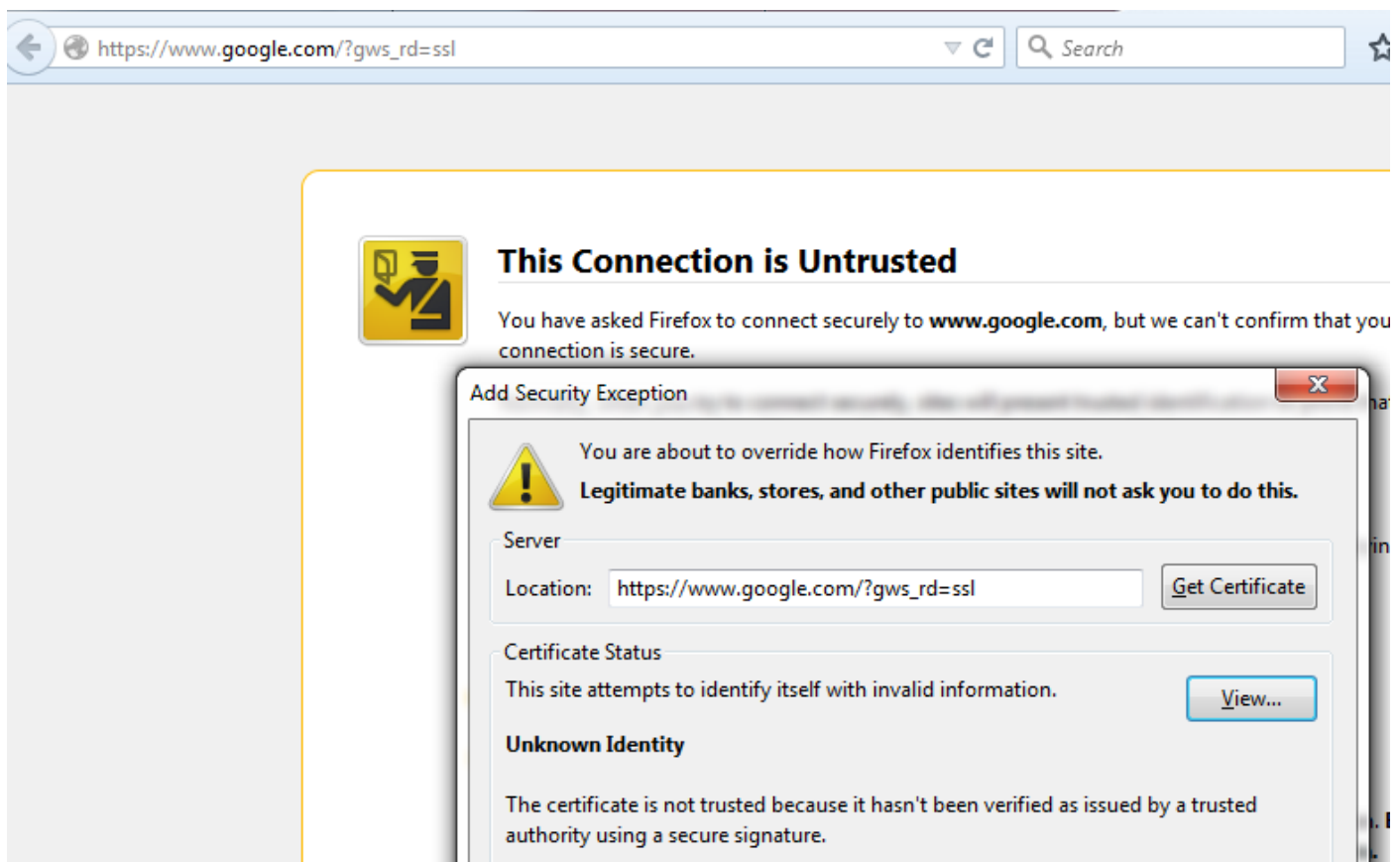
## 驗證

解密 — 重新簽名

1. 開啟Web瀏覽器。

**注意：**以下示例中使用的是Firefox瀏覽器。此示例在Chrome中可能不起作用。有關詳細資訊，請參閱故障排除部分。

2. 導航至SSL網站。在使用https://www.google.com下面的示例中，金融機構的網站也將正常工作。您將看到以下頁面之一：



**附註：**如果憑證本身不受信任，且瀏覽器不信任簽名CA憑證，則會看到上頁。要瞭解瀏覽器如何確定受信任的CA證書，請參閱下面的「受信任的證書頒發機構」部分。

# Google

Google Search I'm Feeling Lucky

Page Info - https://www.google.com/?gws\_rd=ssl

General Media Permissions Security

**Website Identity**

Website: **www.google.com**  
Owner: **This website does not supply ownership information.**  
Verified by: **Sourcefire**

[View Certificate](#)

**Privacy & History**

Have I visited this website prior to today?	<b>Yes, 277 times</b>	
Is this website storing information (cookies) on my computer?	<b>Yes</b>	<a href="#">View Cookies</a>
Have I saved any passwords for this website?	<b>No</b>	<a href="#">View Saved Passwords</a>

**Technical Details**

附註：如果顯示此頁面，則您已成功對流量重新簽名。注意Verified by: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

附註：這是對同一證書的特寫。

3.在管理中心中，轉至分析>連線>事件。

4.根據您的工作流程，您可能會看到SSL解密選項，也可能看不到。按一下**Table View of Connection Events**。

[Connections with Application Details](#) > [Table View of Connection Events](#)

No Search Constraints ([Edit Search](#))

Jump to... ▼	<input type="checkbox"/>	▼ <a href="#">First Packet</a>	<a href="#">Last Packet</a>	<a href="#">Action</a>	<a href="#">Reason</a>
--------------	--------------------------	--------------------------------	-----------------------------	------------------------	------------------------

5.滾動到右側並查詢SSL狀態。您應該會看到類似以下的選項：

443 (https) / tcp	Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> Secure Web browser	<input type="checkbox"/> Skype Tunneling
443 (https) / tcp	Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> Secure Web browser	<input type="checkbox"/> Google

解密 — 已知證書

1. 在FireSIGHT管理中心，導航至分析>連線>事件。
2. 根據您的工作流程，您可能會看到SSL解密選項，也可能不會看到。按一下Table View of Connection Events。

[Connections with Application Details](#) > [Table View of Connection Events](#)

No Search Constraints ([Edit Search](#))

Jump to... ▼	<input type="checkbox"/>	▼ <a href="#">First Packet</a>	<a href="#">Last Packet</a>	<a href="#">Action</a>	<a href="#">Reason</a>
--------------	--------------------------	--------------------------------	-----------------------------	------------------------	------------------------

3. 滾動到右側並查詢SSL狀態。您應該會看到類似以下的選項：

443 (https) / tcp	Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> Secure Web browser	<input type="checkbox"/> Skype Tunneling
443 (https) / tcp	Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> Secure Web browser	<input type="checkbox"/> Google

## 疑難排解

### 問題1:某些網站可能無法在Chrome瀏覽器上載入

#### 範例

www.google.com不能載入解密 — 使用Chrome重新簽名。

#### 原因

Google Chrome瀏覽器能夠檢測google屬性的欺詐證書，以防止中間人攻擊。如果Chrome瀏覽器（客戶端）嘗試連線到google.com域（伺服器），並且返回的證書不是有效的google證書，瀏覽器將拒絕連線。

#### 解決方案

如果您遇到這種情況，請為DN=\*.google.com、\*.gmail.com和\*.youtube.com新增不解密規則。然後清除瀏覽器快取和歷史記錄。

### 問題2:在某些瀏覽器中收到不可信的警告/錯誤

## 範例

當您使用Internet Explorer和Chrome連線到站點時，不會收到安全警告，但是當您使用Firefox瀏覽器時，每次關閉並重新開啟瀏覽器時，都必須信任該連線。

## 原因

受信任CA的清單取決於瀏覽器。當您信任證書時，它不會跨瀏覽器傳播，並且受信任條目通常僅在瀏覽器開啟時繼續存在，因此，關閉證書後，所有受信任的證書都會被修剪，並且下次您開啟瀏覽器並訪問站點時，必須再次將其新增到受信任證書清單中。

## 解決方案

在這種情況下，IE和Chrome都使用作業系統中的受信任CA清單，但Firefox維護自己的清單。因此，CA證書已匯入到OS應用商店，但未匯入到Firefox瀏覽器。為了避免在Firefox中收到安全警告，您必須將CA證書作為受信任的CA匯入到瀏覽器中。

## 受信任的證書頒發機構

建立SSL連線時，瀏覽器首先檢查此證書是否受信任（即，您之前曾訪問過此站點，並手動通知瀏覽器信任此證書）。如果證書不受信任，瀏覽器會檢查驗證此站點證書的證書頒發機構(CA)證書。如果CA證書受瀏覽器信任，則它將其視為受信任證書並允許連線。如果CA證書不受信任，瀏覽器將顯示安全警告，並強制您將證書手動新增為受信任證書。

瀏覽器中受信任CA的清單完全取決於瀏覽器的實現，並且每個瀏覽器可以與其他瀏覽器不同的方式填充其受信任清單。通常，當前瀏覽器填充受信任CA清單的方式有兩種：

1. 它們使用作業系統信任的受信任CA的清單
2. 他們隨軟體傳送一個受信任CA的清單，該清單內建在瀏覽器中。

對於最常見的瀏覽器，可信任的CA填充如下：

- **Google Chrome:**作業系統的受信任CA清單
- **Firefox:**維護自己的受信任CA清單
- **Internet Explorer:**作業系統的受信任CA清單
- **Safari:**作業系統的受信任CA清單

瞭解不同之處很重要，因為客戶端上看到的行為會因這一點而有所不同。例如，為了為Chrome和IE新增受信任CA，您必須將CA證書匯入到作業系統的受信任CA儲存中。如果將CA證書匯入OS的受信任CA儲存，則在連線到具有此CA簽名的證書的站點時，將不再收到警告。在Firefox瀏覽器上，必須手動將CA證書匯入瀏覽器本身的受信任CA儲存中。執行此操作後，在連線到由該CA驗證的站點時，將不再收到安全警告。

## 參考資料

- [SSL規則入門](#)