Cisco FireSIGHT システムの SSL 検査ポリシーの設定

内容

概要

この SSL 検査機能により、暗号化トラフィックを検査せずにブロックするか、暗号化/復号済みトラフィックをアクセス制御で検査するかを選択できるようになります。このドキュメントでは、Cisco FireSIGHT システムに SSL 検査ポリシーをセットアップするための設定手順を説明します。

前提条件

使用するコンポーネント

- Cisco FireSIGHT Management Center
- Cisco FirePOWER 7000 または 8000 アプライアンス
- ソフトウェア バージョン 5.4.1 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

警告： 管理対象デバイスで SSL 検査ポリシーを適用すると、ネットワークのパフォーマンスに影響を及ぼす可能性があります。

設定

以下の方法で、トラフィックを復号化するための SSL 検査ポリシーを設定することができます。

1.復号化と再署名：

- オプション 1：FireSIGHT Center をルート認証局（CA）として使用する
- オプション 2：内部 CA に証明書に署名してもらう
- オプション 3：CA 証明書とキーをインポートする

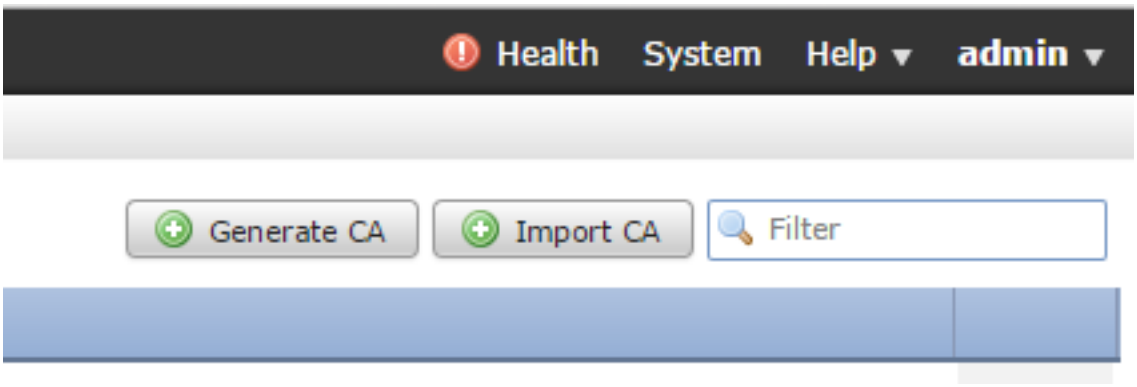
2.既知の証明書で復号化：

- FireSIGHT Management Center にログインし、[Objects] に移動します。
- [Objects] **ページで [PKI] を展開し、[Internal CAs] を選択します。**

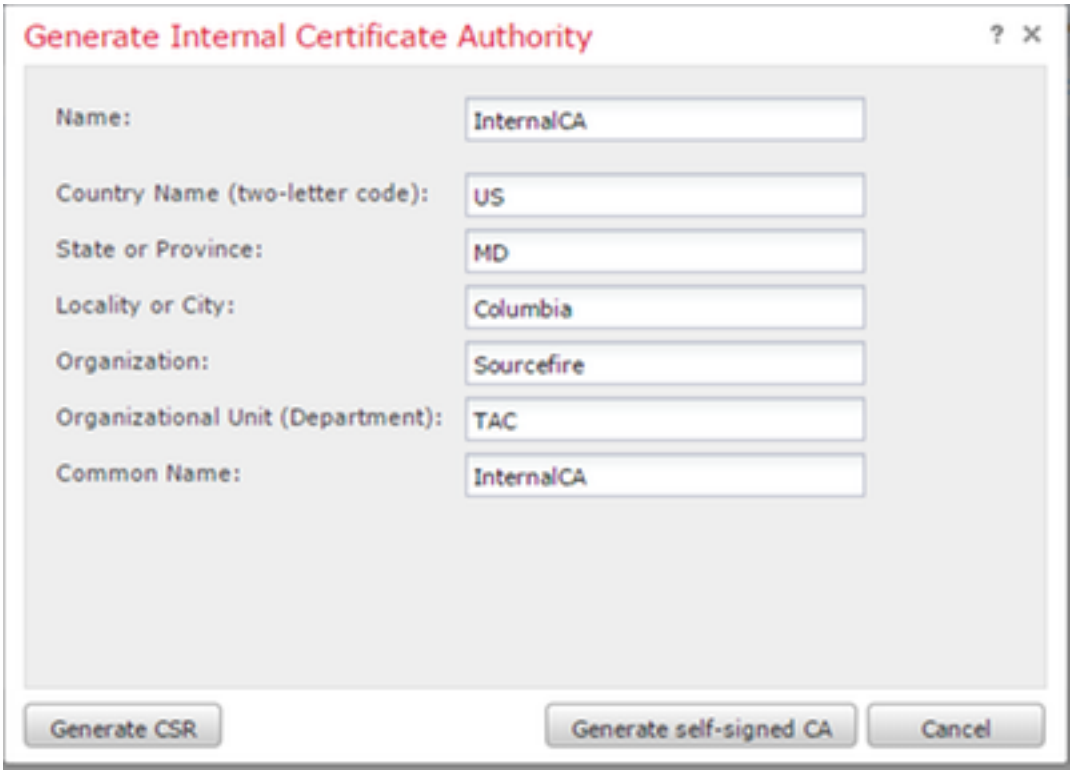
1.復号化と再署名

オプション 1：FireSIGHT Center をルート認証局（CA）として使用する

i. [Generate CA] をクリックします。



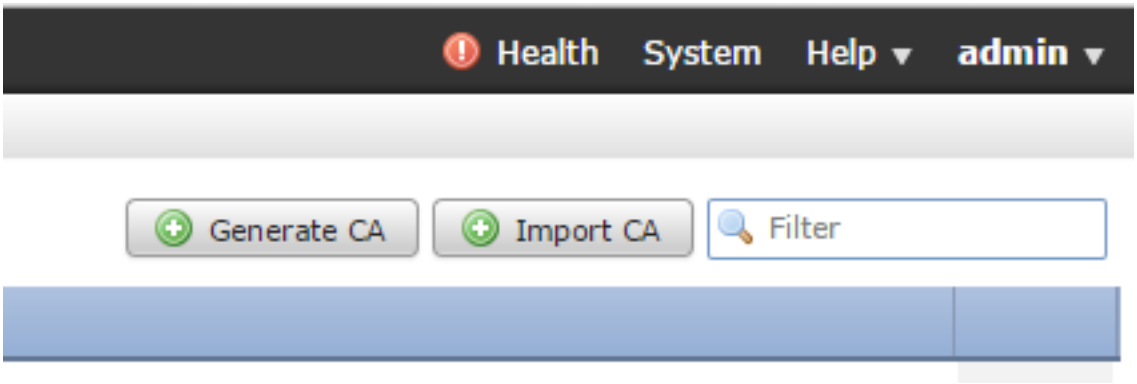
ii.関連情報を入力します



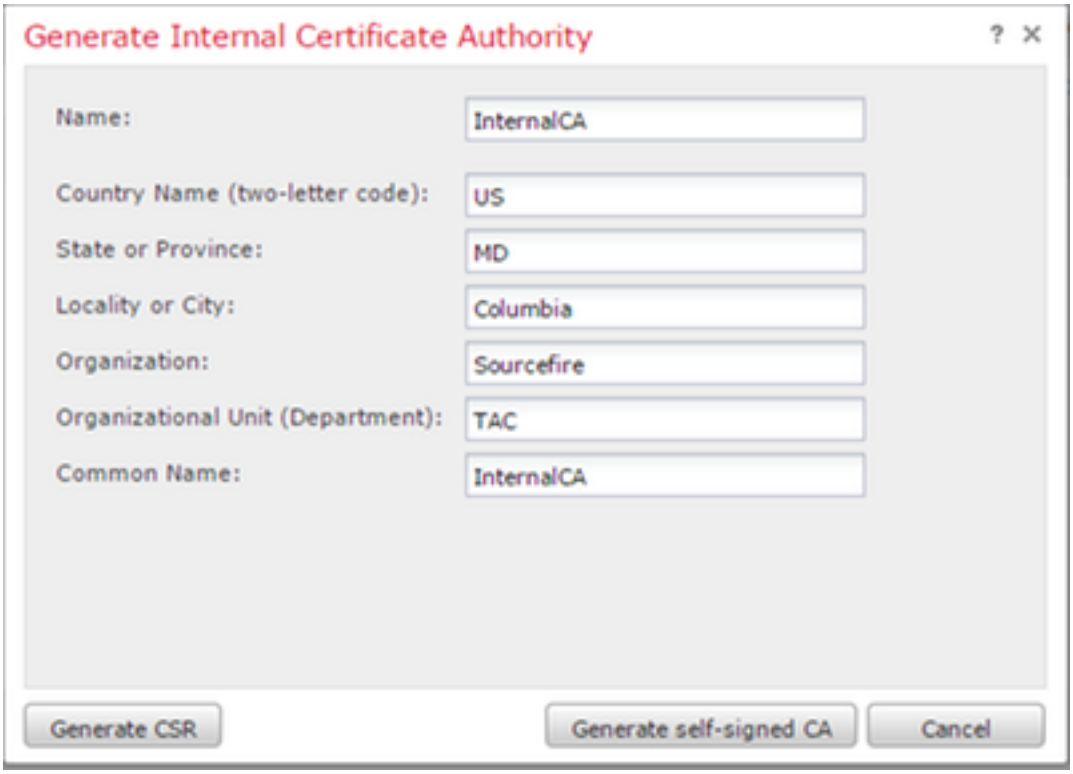
iii.[Generate self-signed CA]をクリックします。

オプション 2：内部 CA に証明書に署名してもらう

i.[Generate CA] をクリックします。

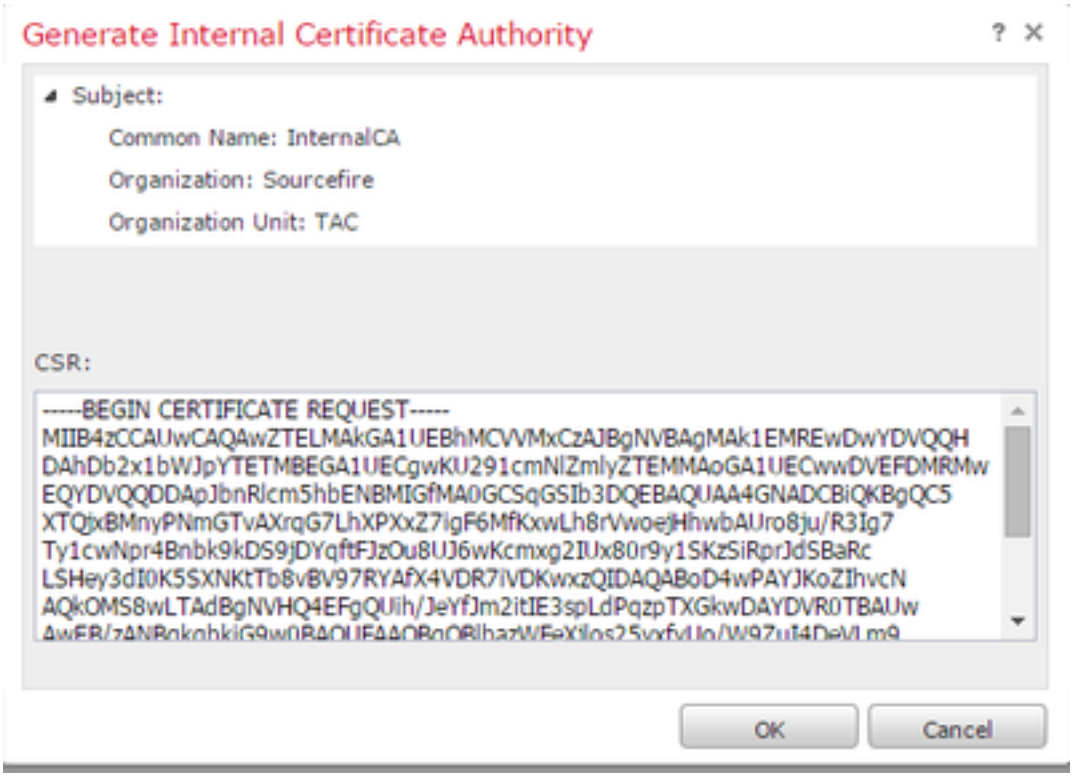


ii.関連情報を入力します。



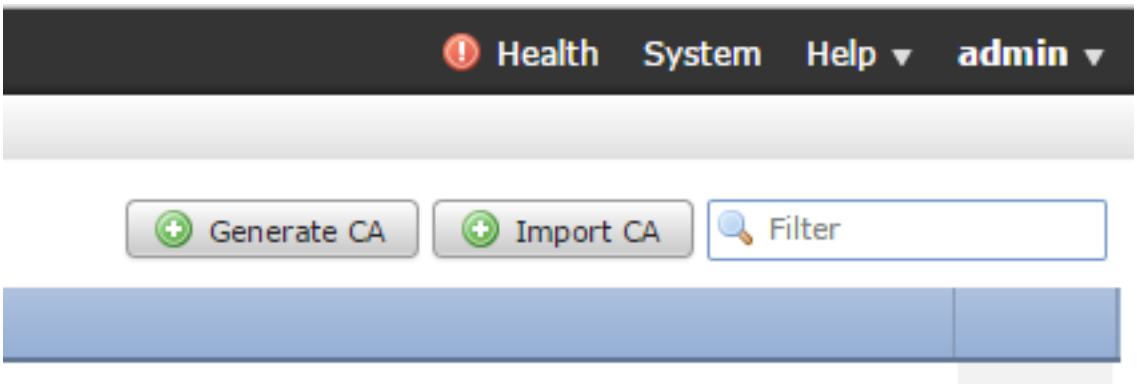
注：CA 管理者に問い合わせて、署名要求のテンプレートがあるかどうか確認する必要がある場合もあります。

iii.—BEGIN CERTIFICATE REQUESTと – END CERTIFICATE REQUESTを含む証明書全体をコピーして、.req拡張子を持つテキストファイルに保存します。



注： CA 管理者が .req とは別のファイル拡張子を要求する場合があります。

オプション 3：CA 証明書とキーをインポートする

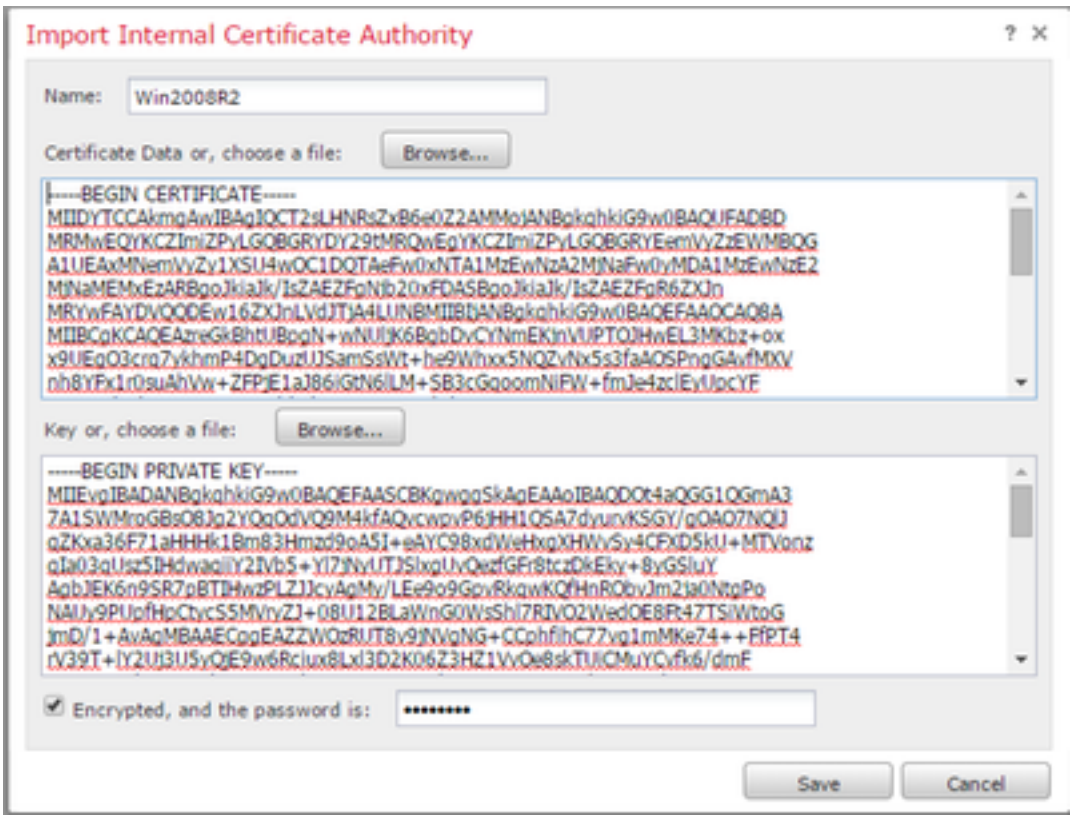


i.[Import CA] をクリックします。

ii.証明書を参照または貼り付けます。

iii.秘密キーを参照または貼り付けます。

iv.[Encrypted] チェックボックスをオンにして、パスワードを入力します。



注： パスワードがない場合は、[Encrypted] チェックボックスをオンにしてパスワード フィールドを空白のままにします。

2.既知のキーで復号化

既知の証明書のインポート（復号化と再署名の代替手段）

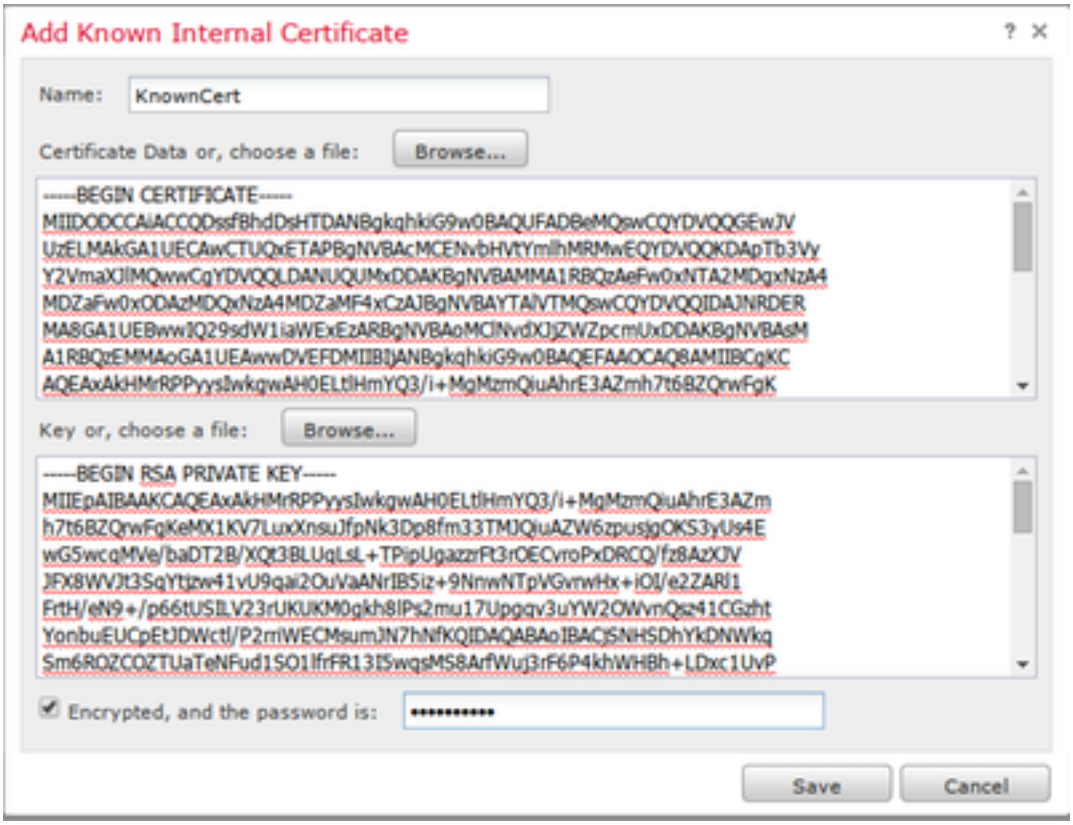
i.左側の [Objects] ページで [PKI] を展開し、[Internal Certs] を選択します。

ii.[Add Internal Cert]をクリックします。

iii.証明書を参照または貼り付けます。

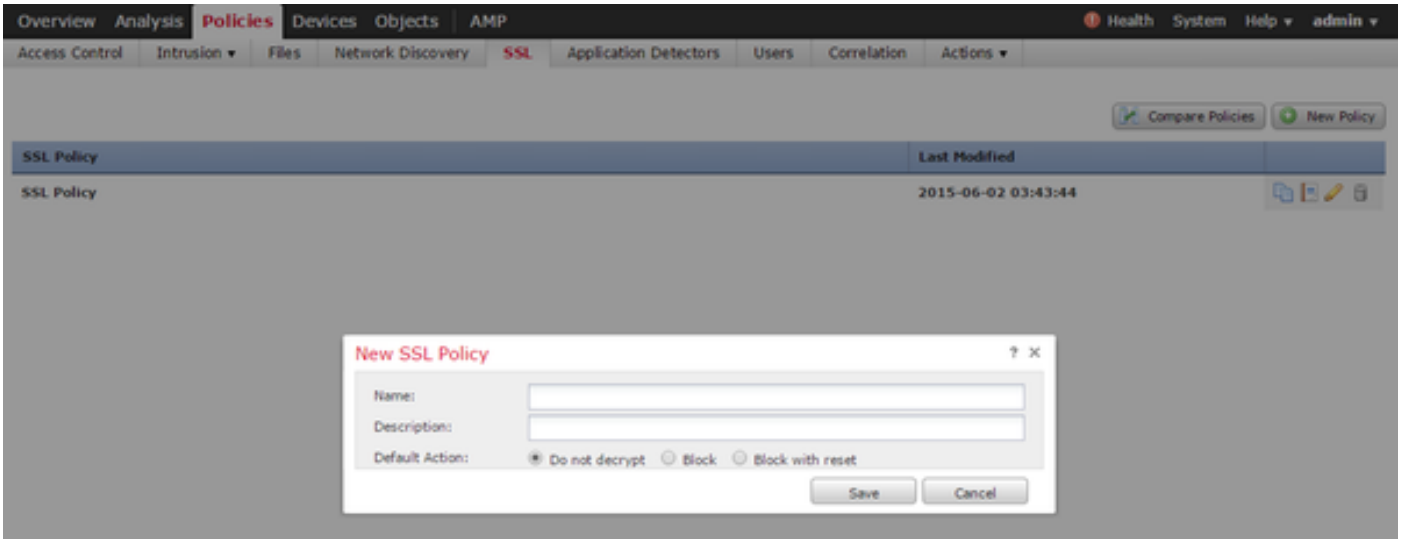
iv.秘密キーを参照または貼り付けます。

v. [Encrypted]ボックスにチェックを入れ、パスワードを入力します。



注： パスワードがない場合は、[Encrypted] ボックスを空白のままにします。

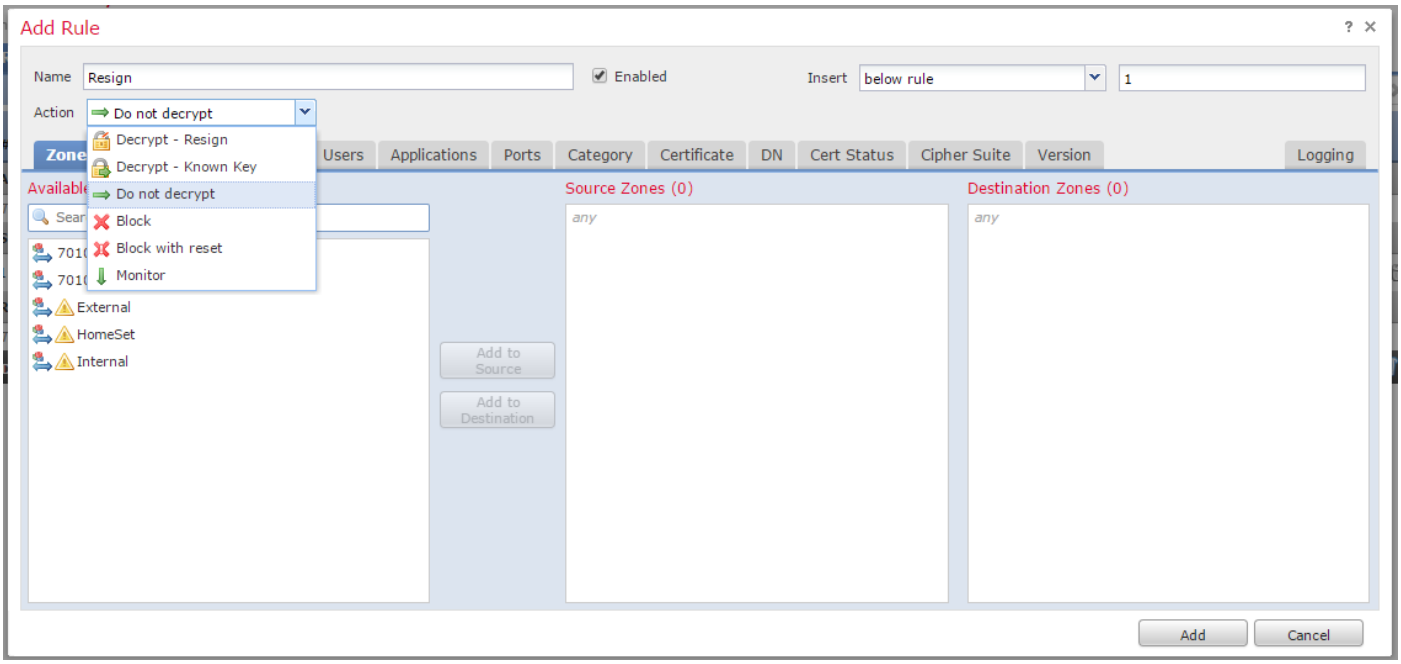
4. 「ポリシー」>「SSL」に移動し、「新規ポリシー」をクリックします。



5.名前を指定し、「デフォルト・アクション」**を選択します**。SSL ポリシー エディタ ページが表示されます。SSL ポリシー エディタ ページは、アクセス コントロール ポリシー エディタ ページと同じように機能します。

> **注：** [Default Action] に何を選択してよいかわからない場合、出発点として [Do not decrypt] をアクションとして選択することを推奨します。

6. SSLポリシーエディタページで、[ルールの追加]をクリ**ックします**。[Add Rule] ウィンドウで、ルールに名前を付けて、その他すべての該当する情報を入力します。



次のセクションで、[Add Rule] ウィンドウで提供されるさまざまなオプションについて説明します。：

アクション

Decrypt - Resign

- 中間者（MitM）として機能するセンサーが、ユーザとの接続を受け入れてから、サーバへの新しい接続を確立します。以下に、いくつかの例を示します。ユーザがブラウザに https://www.facebook.com と入力します。このトラフィックがセンサー

に到達すると、センサーは選択された CA 証明書を使用してユーザとネゴシエートし、SSL トンネル A を確立します。それと同時にセンサーは https://www.facebook.com に接続し、SSL トンネル B を確立します。
- 最終結果：ユーザには Facebook の証明書ではなく、ルールに含まれる証明書が表示されます。
- このアクションには内部CAが必要です。キーを置き換える場合は、「キーの置き換え」を選択します。ここで選択した証明書がユーザに送信されます。

注： このオプションはパッシブ モードでは使用できません。

Decrypt - Known Key

- トラフィックの復号化に使用するためのキーは、センサーが保持します。以下に、いくつかの例を示します。ユーザがブラウザに https://www.facebook.com と入力します。このトラフィックがセンサーに到達すると、センサーはトラフィックを復号化してから、トラフィックを検査します。
- 最終結果：ユーザには Facebook の証明書が表示されます
- このアクションには内部証明書が必要です。内部証明書を追加するには、[Objects] > [PKI] > [Internal Certs] の順に選択します。

注： ドメインおよび証明書の所有者は、所属組織でなければなりません。facebook.com を例として取り上げると、エンドユーザに Facebook の証明書が表示されるのは、組織が実際にドメイン facebook.com の所有者であり (つまり、所属企業が Facebook, Inc であること)、パブリック CA によって署名された facebook.com 証明書の所有権を持っている場合のみです。復号化できるのは、所属組織が所有するサイトの既存のキーを使用する場合のみです。

既知のキーを使用して復号化する主な目的は、HTTPS サーバへのトラフィックを復号化して、社内サーバを外部の攻撃から保護することです。外部 HTTPS サイトへのクライアント側トラフィックを検査する場合は、外部サーバに対する所有権はなく、ネットワーク内で外部の暗号化サイトに接続するクライアント トラフィックを検査することが目的であるため、復号化および再署名を使用します。

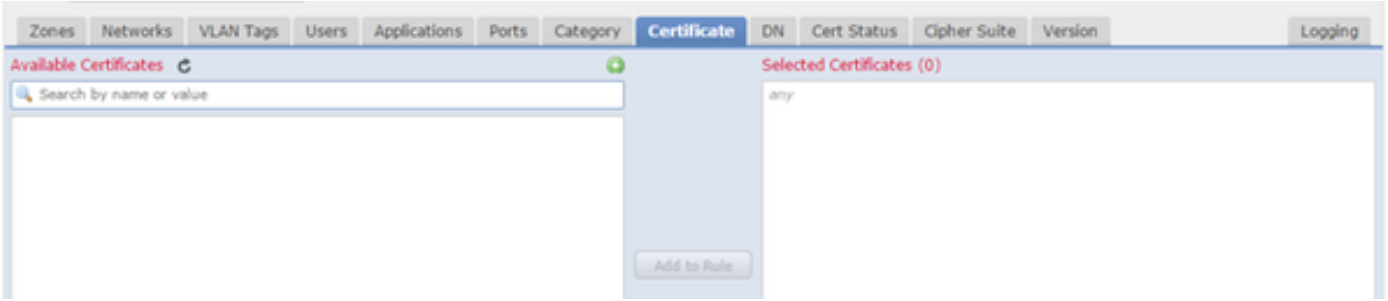
注： DHE と ECDHE で復号化するには、双方の協力が必要です。

Do Not Decrypt

SSL ポリシーはバイパスしてアクセス コントロール ポリシーをトラフィックに適用します。

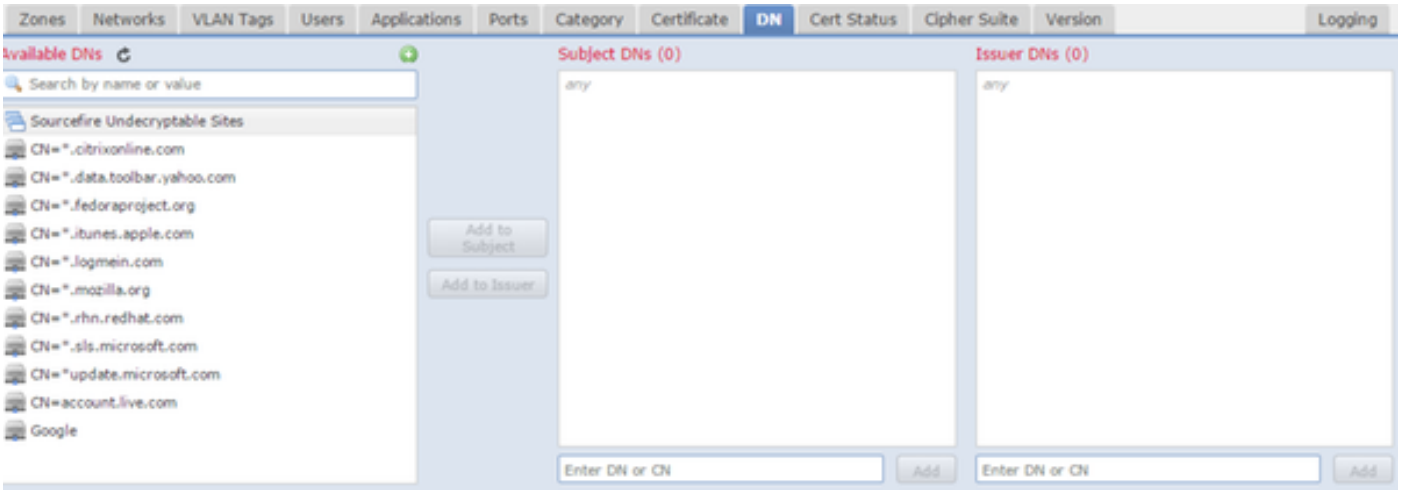
証明書

特定の証明書を使用して、SSL トラフィックにルールが適用されます。



DN

証明書内の特定のドメイン名を使用して、SSL トラフィックにルールが適用されます。

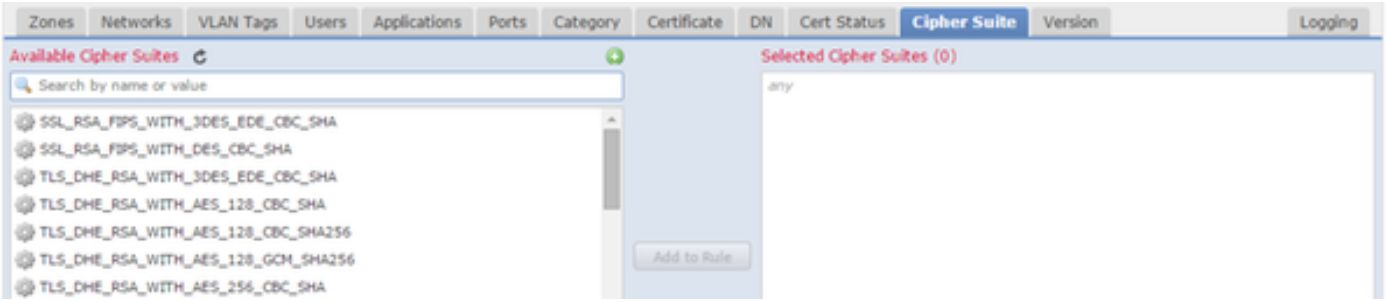


Cert Status

以下の証明書ステータスに基づいて、SSL トラフィックにルールが適用されます。

Cipher Suite

以下の暗号スイートを使用して、SSL トラフィックにルールが適用されます。



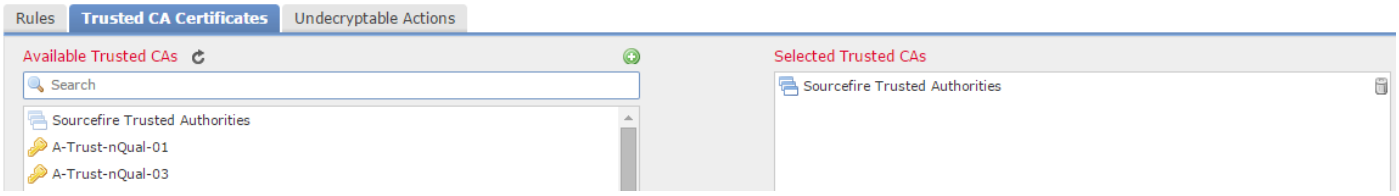
バージョン

選択したバージョンの SSL を使用した SSL トラフィックだけにルールが適用されます。

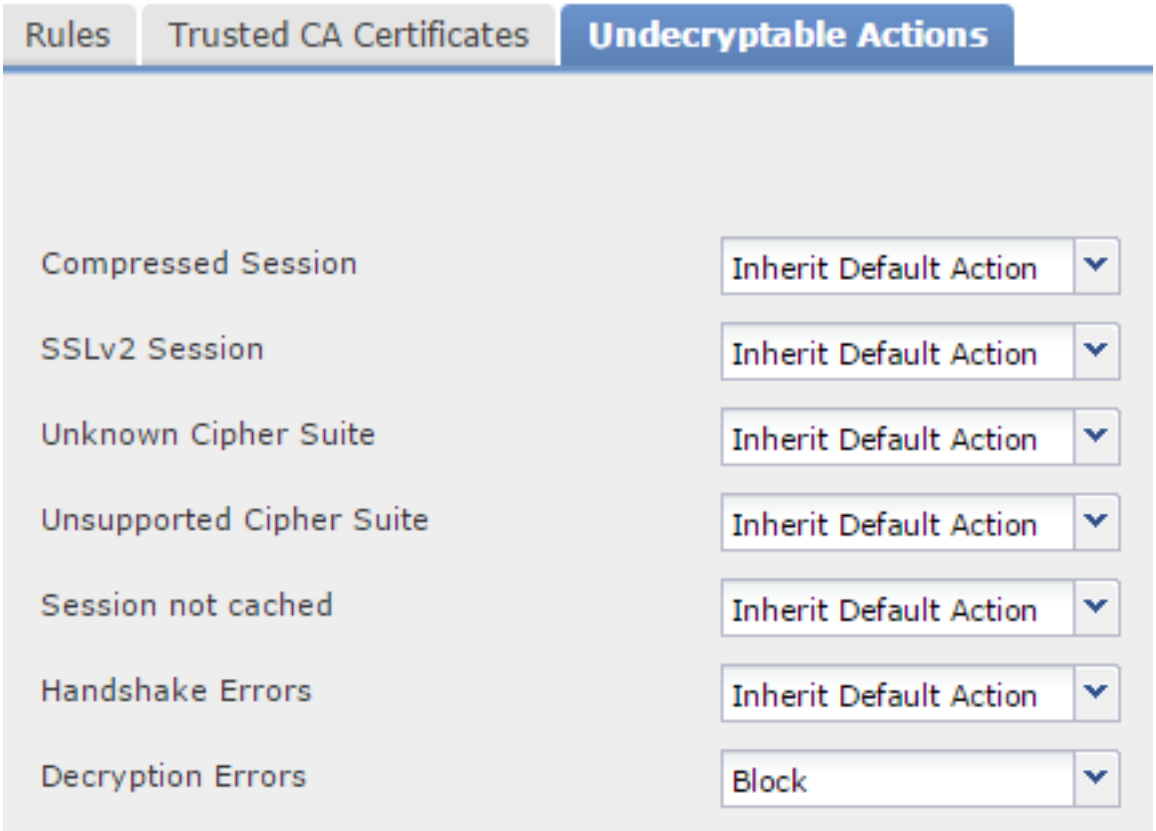
Logging

SSL トラフィックの接続イベントを確認するには、ロギングを有効にします。

7.[Trusted CA Certificate] をクリックします。ここで、信頼された CA をポリシーに追加します。



8.[Undecryptable Actions] をクリックします。これらのアクションは、センサーがトラフィックを復号化できない場合に適用されます。定義については、FireSIGHT Management Center のオンライン ヘルプ（[Help] > [Onlinie]）を参照してください。



- **Compressed Session**：SSL セッションでデータ圧縮方式が適用されます。
- **SSLv2 Session**：セッションはSSLバージョン2で暗号化されます。クライアントのhelloメッセージがSSL 2.0の場合はトラフィックが復号化され、送信されたトラフィックの残りがSSL 3.0であることに注意してください。
- **Unknown Cipher Suite**：システムが暗号スイートを認識しません。

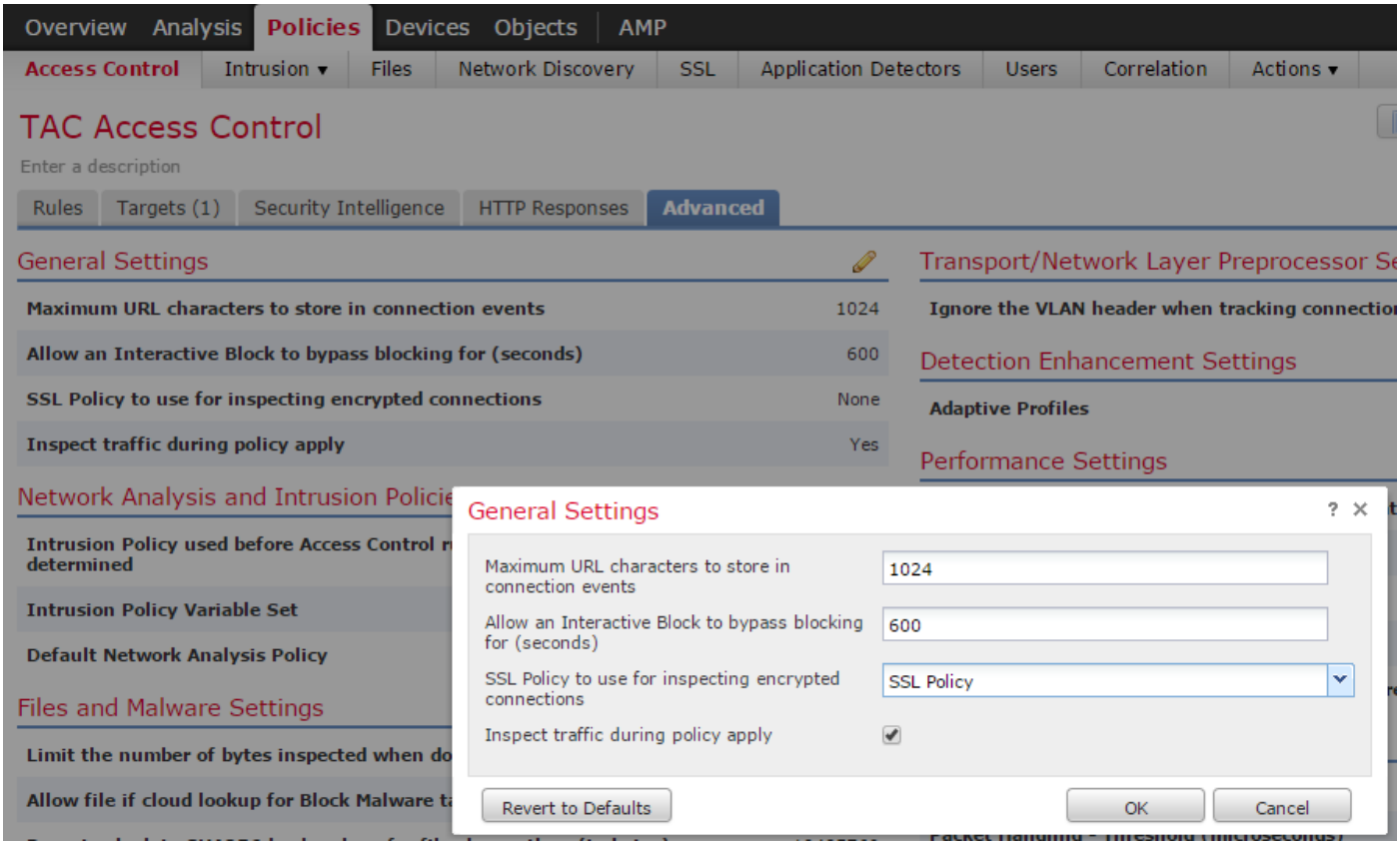
- **Unsupported Cipher Suite**：システムが、検出された暗号スイートに基づく復号化をサポートしません。
- **Session not cached**：SSL セッションにおいてセッションの再利用が可能になっていて、クライアントとサーバがセッション ID でセッションを再確立したときに、システムがそのセッション ID をキャッシュに入れなかったことを意味します。
- **Handshake Errors**：SSL ハンドシェーク ネゴシエーション中にエラーが発生しました。
- **Decryption Errors**：トラフィックの復号化中にエラーが発生しました。

注： デフォルトでは、デフォルト アクションが継承されます。デフォルト アクションが [Block] である場合、予期しない問題が発生する可能性があります。

9.ポリシーを保存します。

10.[Policies] > [Access Control] に移動します。ポリシーを編集するか、新しいアクセス コントロール ポリシーを作成します。

11．[Advanced]をクリックし、一般的な設定を編集します。



12.ドロップダウンメニューからSSLポリシーを選択します。

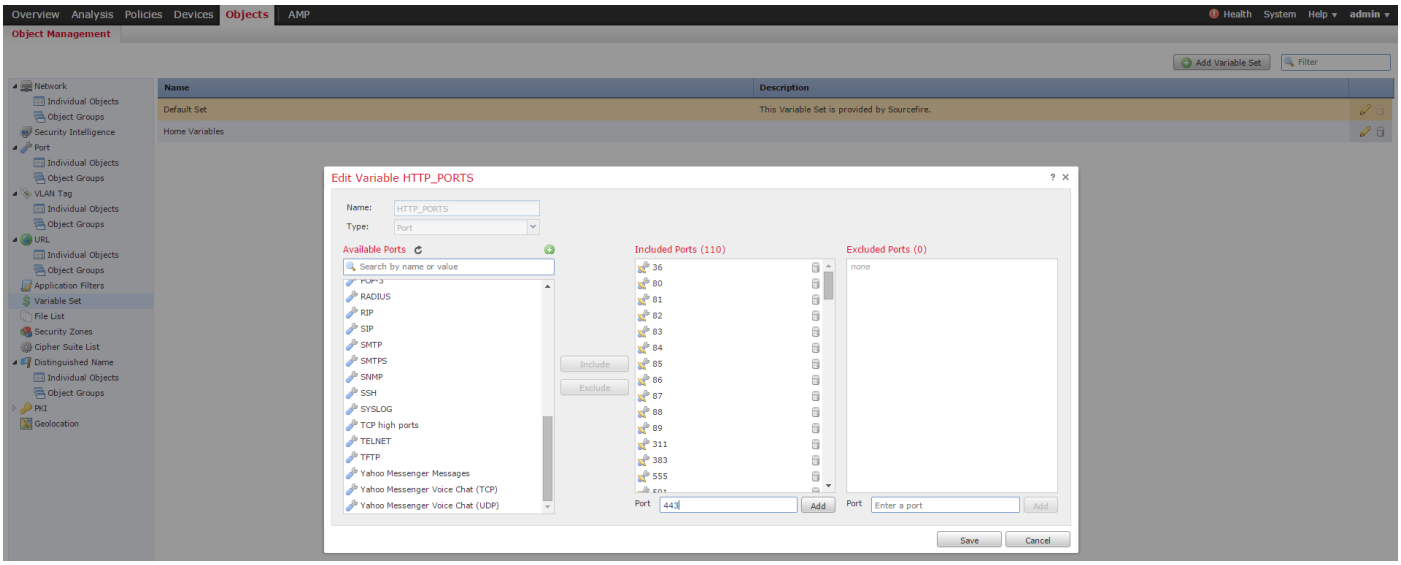
13.「OK」をクリックして保存してください。

その他の設定

適切に識別するためには、侵入ポリシーに以下の変更を加える必要ががあります。

i.$HTTP_PORTS 変数に、ポート 443 と、ポリシーで復号化する HTTPS トラフィックを受け入れるその他すべてのポートを含める必要があります（ [Objects] > [Object Management] >

[Variable Set] > [Edit] の順に移動して変数セットを編集します）。



ii.暗号化トラフィックを検査するネットワーク分析ポリシーで、HTTP プリプロセッサ設定のポート フィールドにポート 443（およびポリシーで復号化する HTTPS トラフィックを受け入れるその他すべてのポート）が設定されている必要があります。そうでないと、HTTP コンテンツ修飾子（例として、http_uri、http_header）付きの HTTP ルールがトリガーされません。なぜなら、ネットワーク分析ポリシーは定義済み HTTP ポートに依存することから、指定されたポートで送受信されないトラフィックについては Snort の HTTP バッファに入れられないためです。

iii.（オプションですが、より良い検査のために推奨）両方のポートでストリームの再構成を実行するフィールドのTCPストリームの構成設定にhttpsポートを追加します。

iv.スケジュールされたメンテナンス時間帯に、変更されたアクセスコントロールポリシーを再適用します。

> **警告：この変更**されたポリシーは、パフォーマンスの重大な問題を引き起こす可能性があります。実稼働時間外にポリシーをテストして、ネットワークの停止やパフォーマンスのリスクを減らしてください。

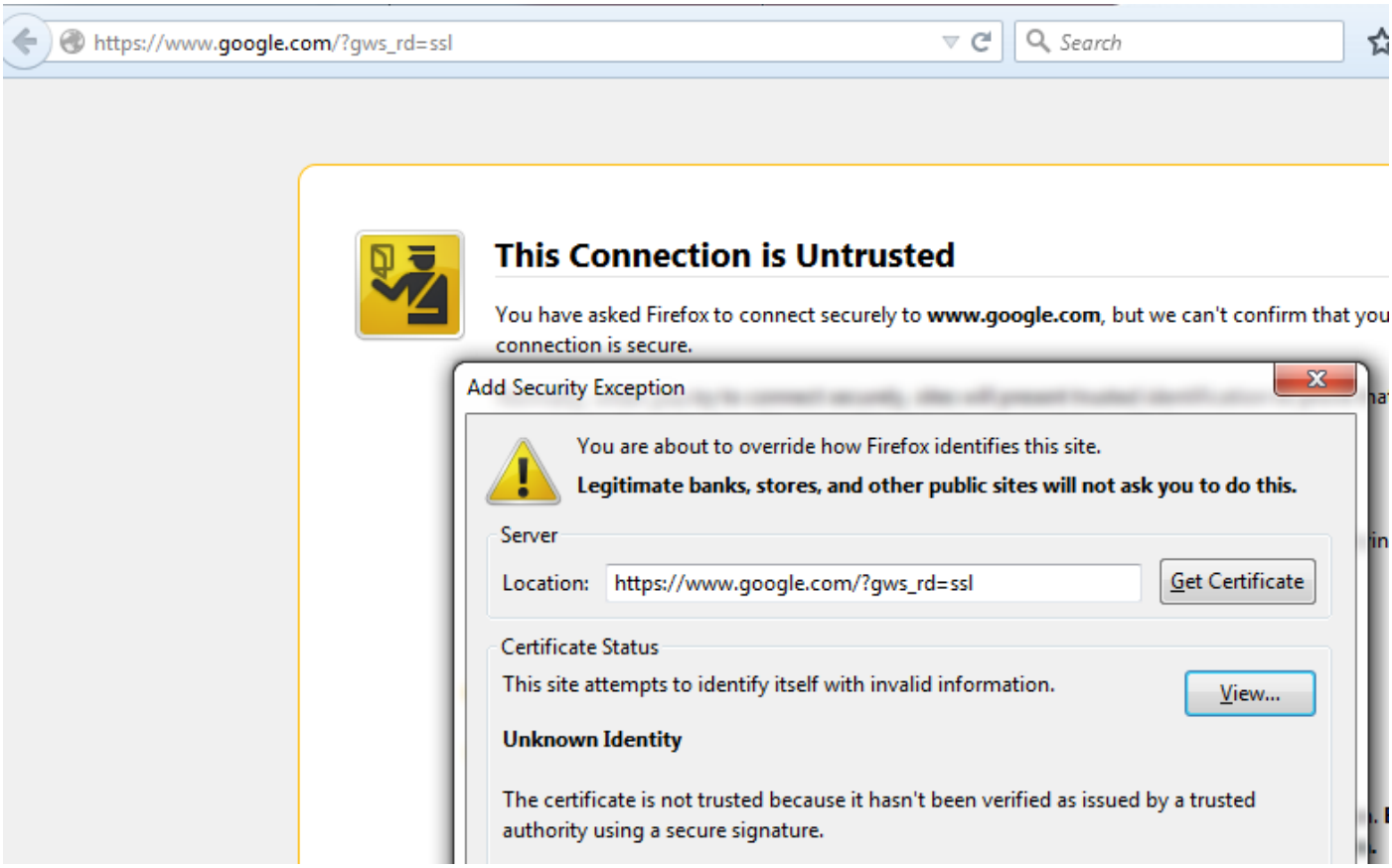
確認

Decrypt - Resign

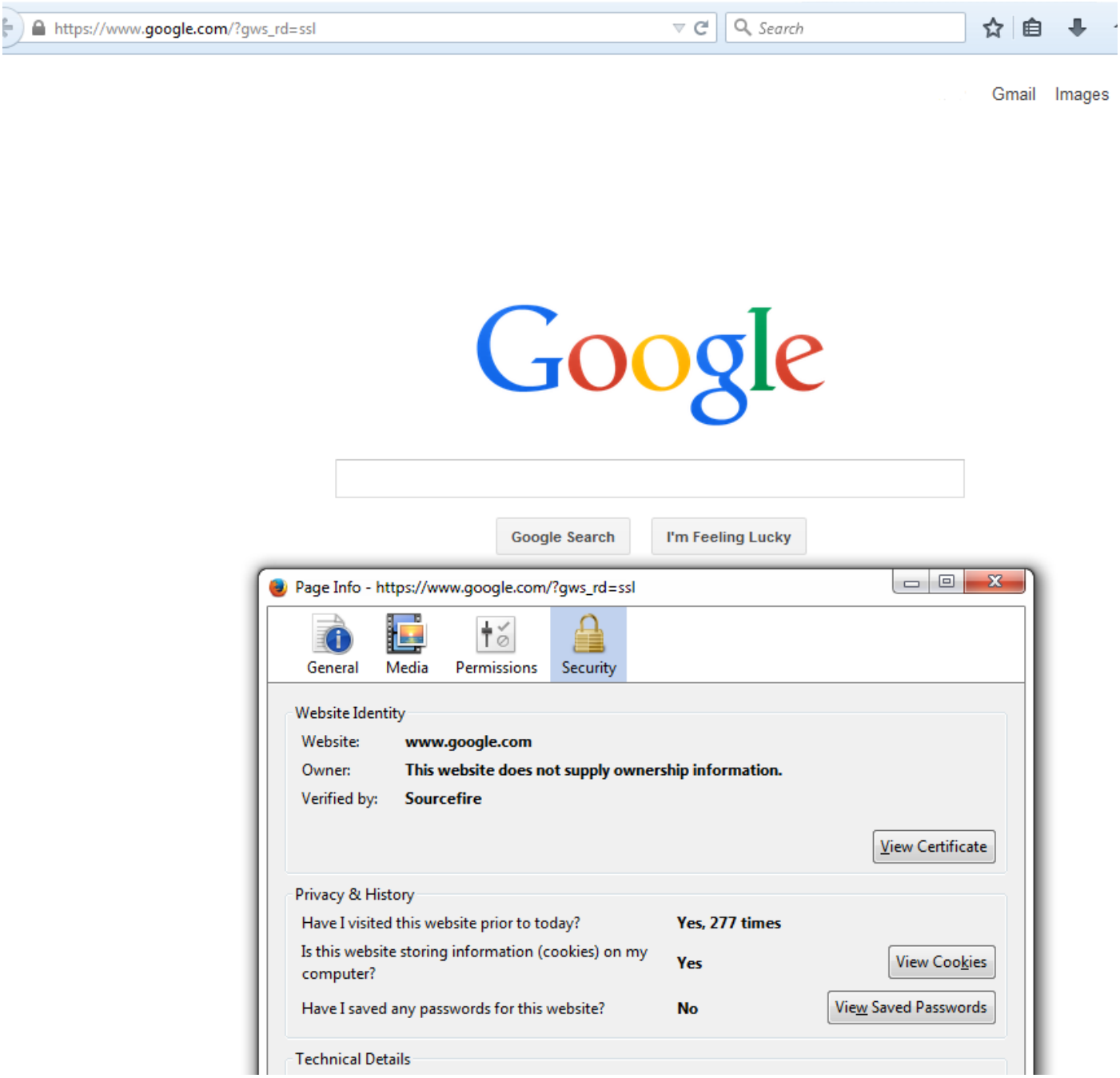
1. Webブラウザを開きます。

> **注：次**の例では、Firefoxブラウザを使用しています。 この例は、Chrome では機能しない可能性があります。詳細については、「トラブルシューティング」のセクションを参照してください。

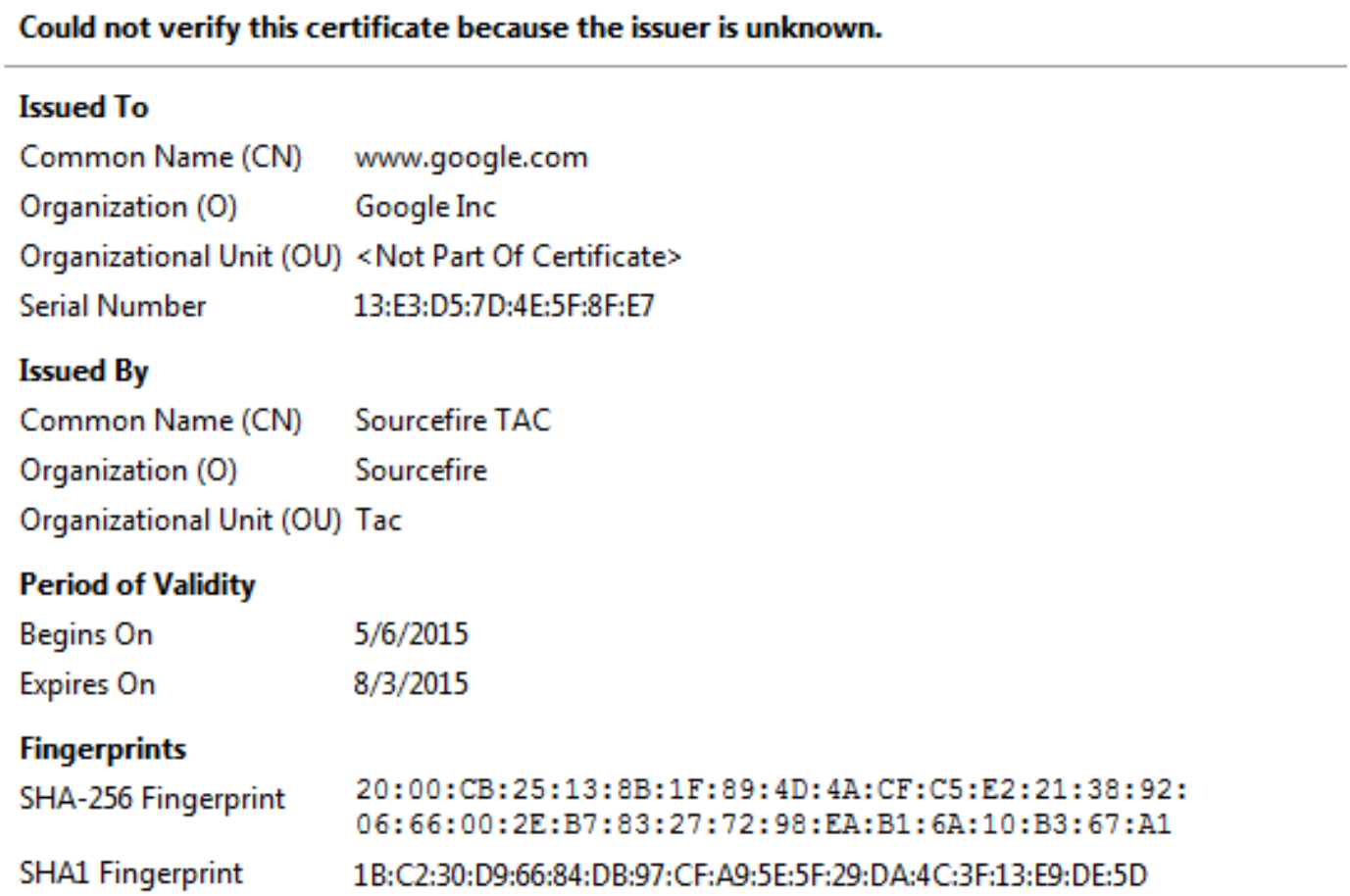
2. SSL Webサイトに移動します。以下の例では、https://www.google.com を使用していますが、金融機関の Web サイトを使用することもできます。次のようなページが表示されます。



注：証明書自体が信頼されていない場合、署名付き CA 証明書がブラウザで信頼されていなければ、上記のページが表示されます。特定のブラウザが、信頼された CA 証明書を判断する方法については、以下の「信頼された認証局」セクションを参照してください。



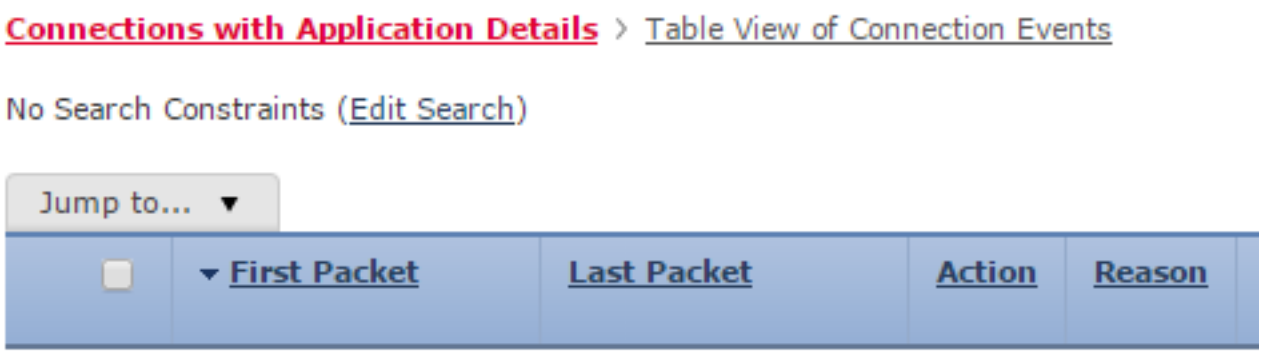
注： このページが表示された場合、トラフィックへの再署名が成功したことを意味します。[Verified by:] セクションに**Sourcefire** と示されていることに注目してください。



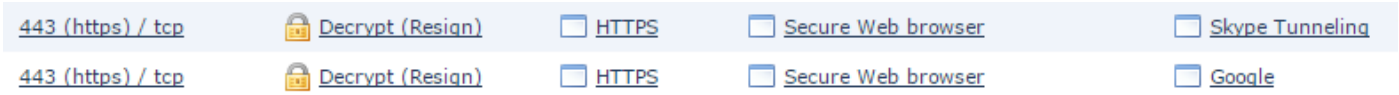
注： 上記は、同じ証明書をクローズアップして表示したものです。

3. Management Centerで、[Analysis] > [Connections] > [Events]に移動します。

4.ワークフローによっては、SSL復号化オプションが表示される場合と表示されない場合があります。[Table View of Connection Events] をクリックします。



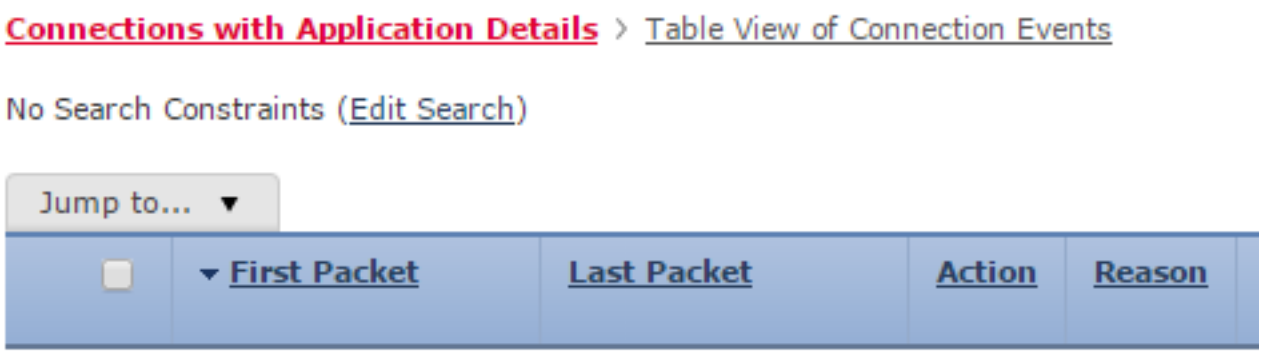
5.右にスクロールし、[SSL Status]を探します。次のようなオプションが表示されます。



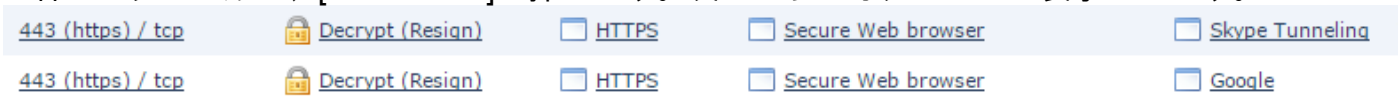
Decrypt - Known Certificate

1. FireSIGHT Management Centerで、[**Analysis**] > [**Connections**] > [**Events**]**に移動します。**

2.ワークフローによっては、SSL復号化オプションが表示される場合と表示されない場合があります。[Table View of Connection Events] をクリックします。



3.右にスクロールし、[SSL Status]を探します。次のようなオプションが表示されます。



トラブルシューティング

問題 1：一部の Web サイトを Chrome ブラウザでロードできない

例

[Decrypt - Resign] が設定されている状態では、Chrome で www.google.com をロードできない場合があります。

原因

中間者攻撃を防ぐために、Google Chrome ブラウザには、Google の資産に対する不正な証明書を検出する機能が備わっています。Chrome ブラウザ（クライアント）が google.com ドメイン（サーバ）に接続しようとして、有効な Google 証明書ではない証明書が返された場合、ブラウザは接続を拒否します。

解決方法

この問題が発生した場合は、DN=*.google.com、*.gmail.com、*.youtube.comのDo Not Decryptルールを追加してください。その後、ブラウザのキャッシュと履歴を消去します。

問題 2：一部のブラウザでサイトの信頼性に関する警告/エラーが表示される

例

Internet Explorer や Chrome を使用してサイトに接続するときはセキュリティ警告が表示されないのに、Firefox ブラウザを使用すると、ブラウザを閉じて開くたびに接続を信頼することを確認しなければなりません。

原因

信頼済み CA のリストは、ブラウザに依存します。証明書を信頼しても、その設定はすべてのブラウザに伝搬されません。通常、信頼済みエントリは、ブラウザが開いている間だけ存続するため、ブラウザを閉じると、信頼されたすべての証明書がプルーニングされます。それで、次回ブラウザを開いてサイトにアクセスするときには、信頼済み証明書のリストに再度追加する必要があります。

解決方法

このシナリオでは、IE と Chrome はどちらもオペレーティング システムの信頼済み CA のリストを使用しますが、Firefox は独自のリストを維持します。そのため、CA 証明書は OS のストアにインポートされても、Firefox ブラウザにはインポートされません。Firefox でセキュリティ警告が表示されないようにするには、CA 証明書を信頼済み CA としてブラウザにインポートする必要があります。

信頼された認証局

SSL 接続を確立する際に、ブラウザはまず、サイトの証明書が信頼されているかどうか（つまり、このサイトに以前アクセスして、ブラウザがこの証明書を信頼するよう手動で設定したかどうか）を検査します。 証明書が信頼されていなければ、ブラウザはこのサイトの証明書を検証した認証局（CA）証明書を検査します。CA 証明書がブラウザで信頼されている場合、ブラウザはサイトの証明書を信頼できるものとみなし、接続を許可します。CA 証明書が信頼されていない場合、ブラウザはセキュリティ警告を表示して、証明書を信頼済み証明書として手動で追加するよう強制します。

ブラウザ内の信頼済み CA のリストは、そのブラウザの実装に完全に依存し、各ブラウザが取り込む信頼済み CA のリストは他のブラウザとは異なる場合があります。一般に、信頼済み CA のリストに最近のブラウザがエントリを追加する方法には、次の 2 つがあります。

1. オペレーティング システムの信頼済み CA のリストを使用する方法
2. 信頼済み CA のリストをソフトウェアで配布し、ブラウザに組み込む方法

一般によく使用されるブラウザでは、信頼済み CA には次のようにエントリが追加されます。

- **Google Chrome**：オペレーティング システムの信頼済み CA のリスト
- **Firefox**：独自の信頼済み CA のリストを維持
- **Internet Explorer**：オペレーティング システムの信頼済み CA のリスト
- **Safari**：オペレーティング システムの信頼済み CA のリスト

クライアント上で見られる動作の違いはこうしたことが要因となるため、この違いを把握することが重要です。たとえば、Chrome および IE に信頼済み CA を追加するには、その CA 証明書を OS の信頼済み CA ストアにインポートする必要があります。CA 証明書を OS の信頼済み CA ストアにインポートすると、その CA によって署名された証明書を使用するサイトに接続する際に警告が表示されることはなくなります。Firefox ブラウザでは、ブラウザ自体の信頼済み CA ストアに CA 証明書を手動でインポートする必要があります。インポートした後は、その CA によっ

て署名された証明書を使用するサイトに接続する際に警告が表示されることはなくなります。

参考資料

- SSL ルールの概要