ASDM（On-Box Management）を使用したFirePOWER モジュール上での SSL 復号化を設定する

内容

概要

このドキュメントでは、ASDM（オンボックス管理）を使用した FirePOWER モジュールでのセキュア ソケット レイヤ（SSL）復号の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA（適応型セキュリティ アプライアンス）ファイアウォール、ASDM（Adaptive Security Device Manager）。
- FirePOWERアプライアンスに関する知識
- HTTPS/SSLプロトコルに関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン6.0.0以降を実行するASA FirePOWERモジュール(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- ソフトウェア バージョン 6.0.0 以降が稼働する ASA FirePOWER モジュール（ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X）

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。

> **注：**この機能を設定するには、FirePOWERモジュールに**保護ラ**イセンスがあることを確認します。ライセンスを確認するには、[Configuration] > [ASA FirePOWER Configuration] > [License] に移動します。

背景説明

Firepowerモジュールは、それにリダイレクトされる着信および発信SSL接続を復号化して検査します。トラフィックが復号化されると、Facebookチャットなどのトンネルアプリケーションが検出され、制御されます。復号化されたデータは、脅威、URLフィルタリング、ファイルブロッキング、または悪意のあるデータがないか検査されます。

アウトバウンドSSL復号化

firepowerモジュールは、発信SSL要求を傍受し、ユーザがアクセスするサイトの証明書を再生成することによって、発信SSL接続の転送プロキシとして機能します。発行機関(CA)は、Firepower自己署名証明書です。Firepowerの証明書が存在する階層の一部でない場合、またはクライアントのブラウザキャッシュに追加されていない場合、クライアントはセキュアなサイトをブラウズするときに警告を受信します。Decrypt-Resign方式は、発信SSL復号化を実行するために使用されます。

着信SSL復号化

内部Webサーバまたは内部デバイスへの着信トラフィックの場合、管理者は保護されたサーバの証明書とキーのコピーをインポートします。SSLサーバ証明書がFirepowerモジュールにロードされ、着信トラフィックに対してSSL復号化ポリシーが設定されると、デバイスはトラフィックを復号化し、トラフィックの転送時にトラフィックを検査します。このモジュールは、悪意のあるコンテンツ、脅威、このセキュアチャネルを通過するマルウェアを検出します。さらに、着信SSL復号化を実行するためにDecrypt-Known Keyメソッドが使用されます。

SSL復号化の設定

SSLトラフィックの復号化には2つの方法があります。

- 復号化：アウトバウンドSSLトラフィックに対して再署名
- 復号化：着信SSLトラフィックで既知

アウトバウンドSSL復号化（復号化 – 再署名）

Firepowerモジュールは、パブリックSSLサーバのSSLネゴシエーションでMITM(man-in-the-middle)として機能します。Firepowerモジュールに設定されている中間CA証明書を使用して、パブリックサーバの証明書に再サインします。

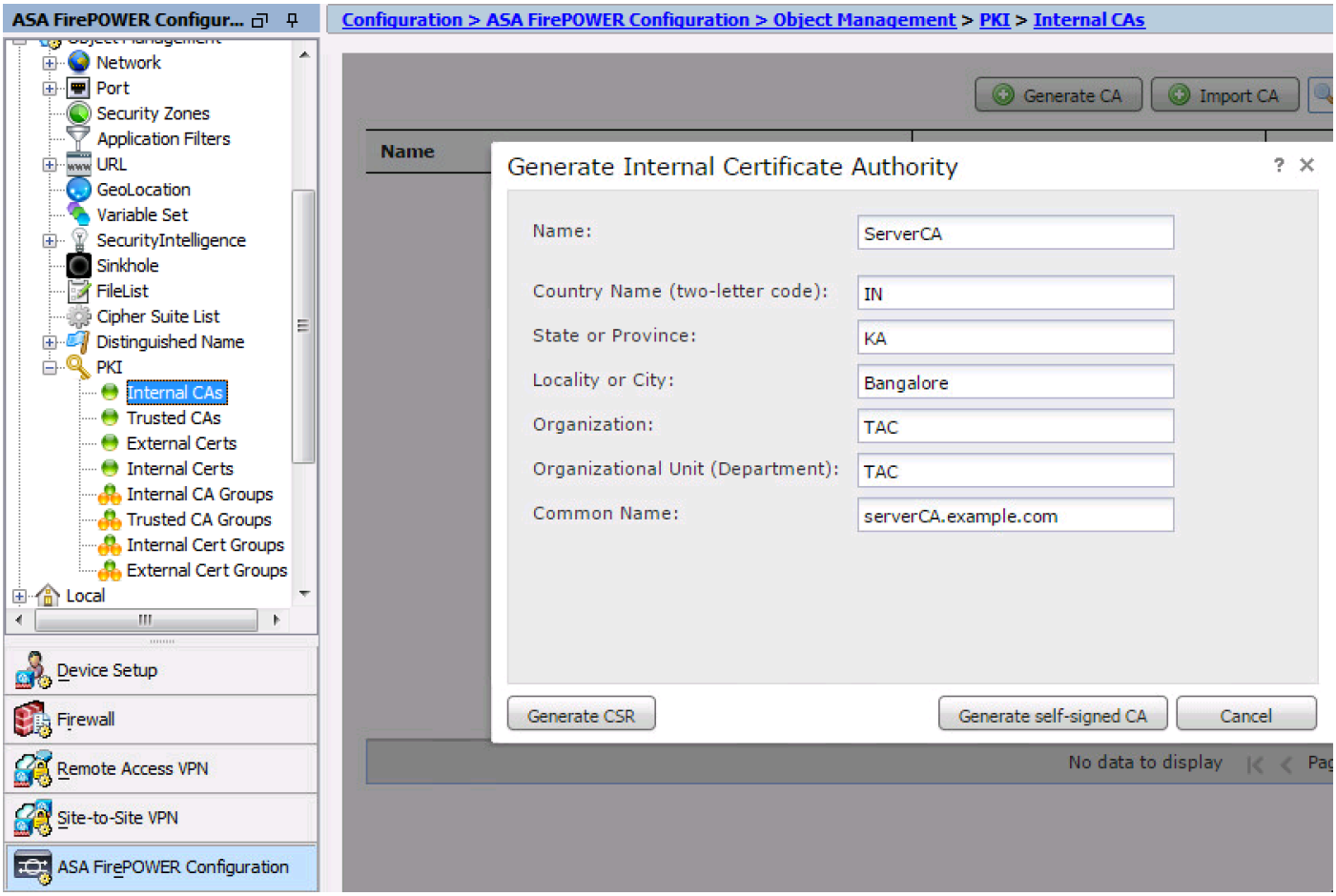
アウトバウンドSSL復号化を設定する3つの手順を次に示します。

ステップ1:CA証明書を設定します。

自己署名証明書または中間の信頼できるCA証明書を証明書署名用に設定します。

自己署名CA証明書の設定

自己署名CA証明書を設定するには、**[Configuration] > [ASA Firepower Configuration] > [Object Management] > [PKI] > [Internal CAs]に移動し、[Generate CA]をクリックします。**CA証明書の詳細を求めるプロンプトが表示されます。図に示すように、要件に従って詳細を入力します。



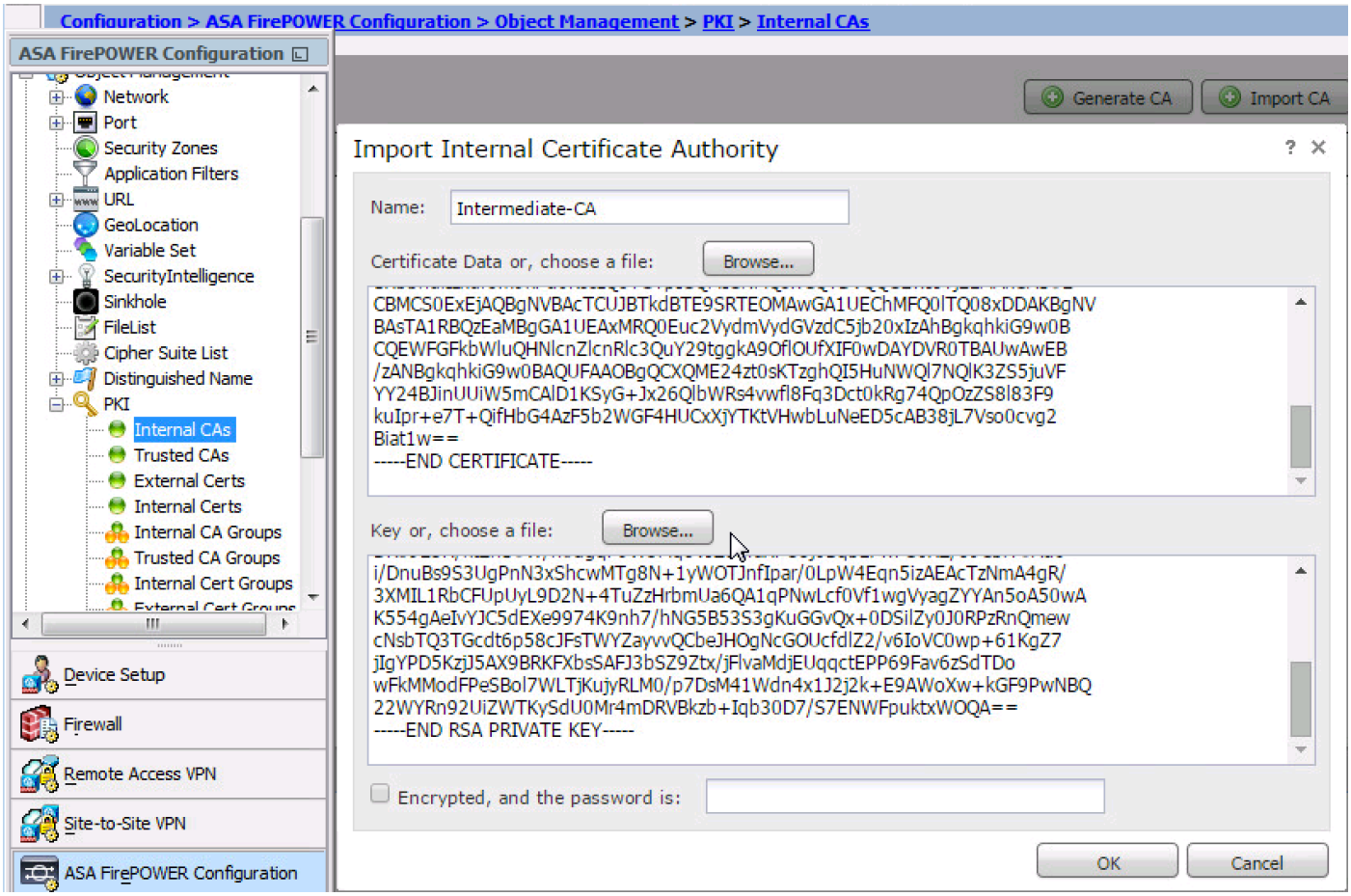
[Generate self-signed CA]をクリックして、内部CA証明書を生成します。次に、**[Generate CSR]**をクリックして、証明書署名要求を生成します。これにより、署名するCAサーバと共有されます。

中間CA証明書の設定

別のサードパーティCAによって署名された中間CA証明書を設定するには、**[Configuration] > [ASA Firepower Configuration] > [Object Management] > [PKI] > [Internal CAs]に移動し、[Import CA]をクリックします。**

証明書の名前を指定します。**[参照]を選択**し、ローカルマシンから証明書をアップロードするか、[証明書データ]オプションに証明書の内容をコピー**アップ**します。証明書の秘密キーを指定するには、キーファイルを参照するか、[キー]オプションにキーをコピーペースト**します。**

キーが暗号化されている場合は、[暗号化]チェックボックスをオン**にし**、パスワードを指定します。[OK]をクリックして、証明書の内容を保存します（図を参照）。



ステップ2:SSLポリシーを設定します。

SSLポリシーは、復号化アクションを定義し、復号化のDecrypt-Resign方式が適用されるトラフィックを識別します。ビジネス要件と組織のセキュリティポリシーに基づいて、複数のSSLルールを設定します。

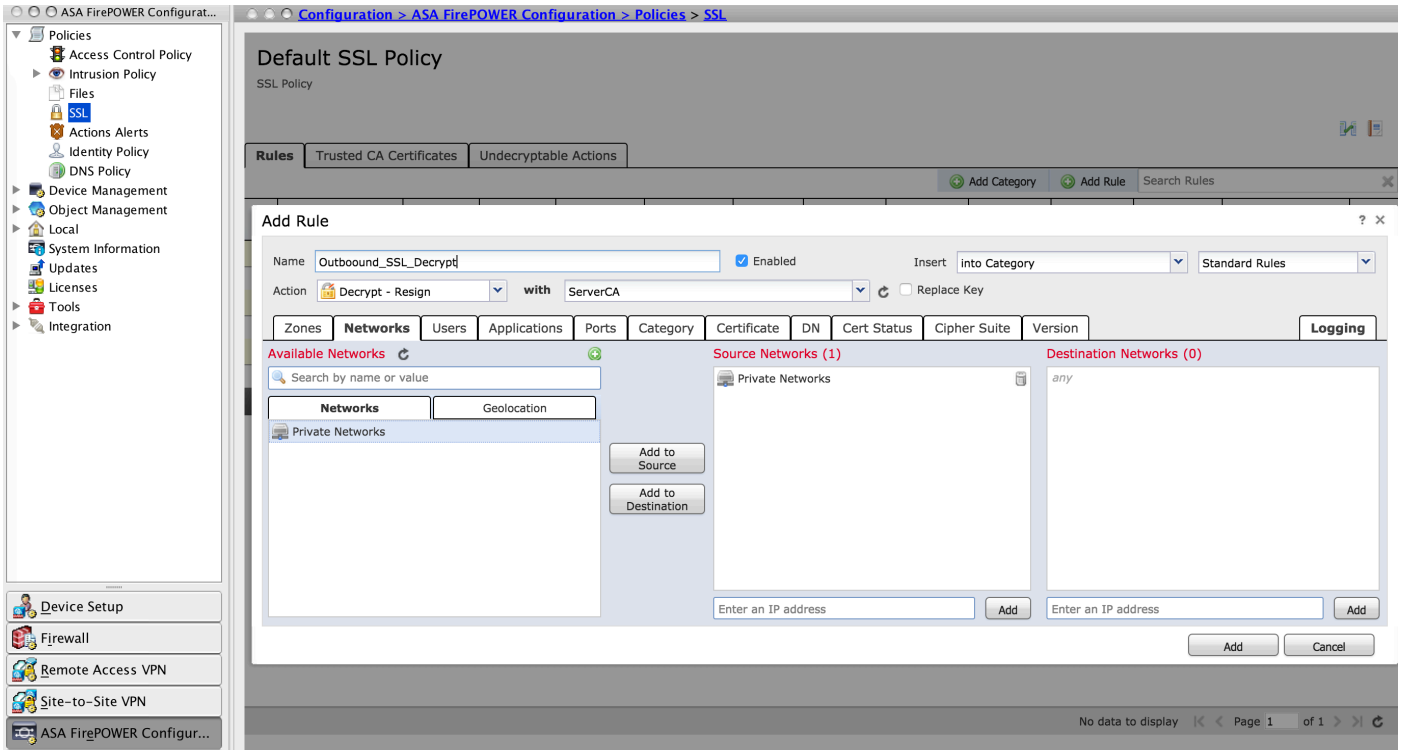
SSLポリシーを設定するには、**[Configure] > [ASA FirePOWER Configuration] > [Policies] > [SSL]に移動し、[Add Rule]をクリックします。**

名前：ルールの名前を指定します。

アクション：アクションを**Decrypt - Resignと指定**し、前の手順で設定したドロップダウンリストからCA証明書を選択します。

復号化が必要なトラフィックを定義するために指定された複数のオプション（ゾーン、ネットワーク、ユーザなど）があるため、トラフィックを照合するルールの条件を定義します。

SSL復号化のイベントを生成するには、次の図に示すように、ログ**記録オ**プションを有効にします。



[Add]をクリックし、SSLルールを追加します。

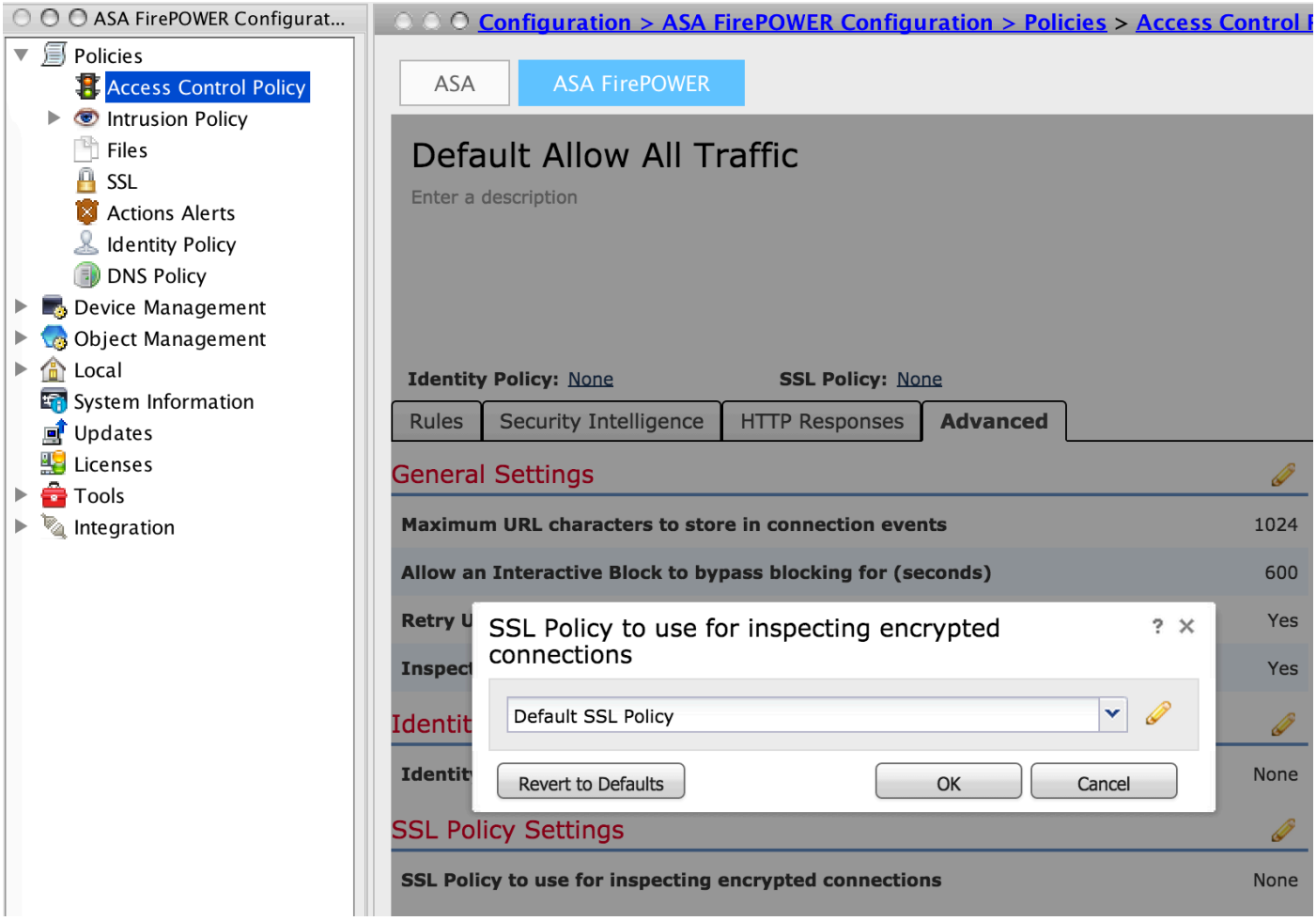
[Store ASA Firepower Changes]をクリックして、SSLポリシーの設定を保存します。

ステップ 3：

適切なルールを使用してSSLポリシーを設定したら、変更を実装するためにアクセスコントロールでSSLポリシーを指定する必要があります。

アクセスコントロールポリシーを設定するには、**[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control]に移動します。**

SSLポリシーの**[None]**をクリック**するか、**[Advanced] > **[SSL Policy Setting]に移動します。**次の図に示すように、ドロップダウンリストからSSLポリシーを指定**して**、**[OK]**をクリックして保存します。



クリック **ASA Firepowerの変更の保存** SSLポリシーの設定を保存します。

アクセスコントロールポリシーをセンサーに展開する必要があります。ポリシーを適用する前に、モジュール上のアクセスコントロールポリシーが古いことを示しています。センサーに変更を展開するには、**[Deploy]をクリック**し、**[Deploy FirePOWER Changes]オプションを選択してください。**変更を確認し、[Deploy]をクリック**します。**

> **注：**バージョン5.4.xで、アクセスポリシーをセンサーに適用する必要がある場合は、**[Apply ASA FirePOWER Changes]**をクリックします。

> **注：**[Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動します。次に、設定変更を適用して、タスクが完了したことを確認します。

着信SSL復号化（復号化 – 既知）

着信SSL復号化(Decrypt-Known)方式は、サーバ証明書と秘密キーを設定した着信SSLトラフィックを復号化するために使用されます。サーバ証明書と秘密キーをFirepowerモジュールにインポートする必要があります。SSLトラフィックがFirepowerモジュールにヒットすると、トラフィックが復号化され、復号化されたトラフィックに対する検査が実行されます。インスペクション後、Firepowerモジュールはトラフィックを再暗号化し、サーバに送信します。

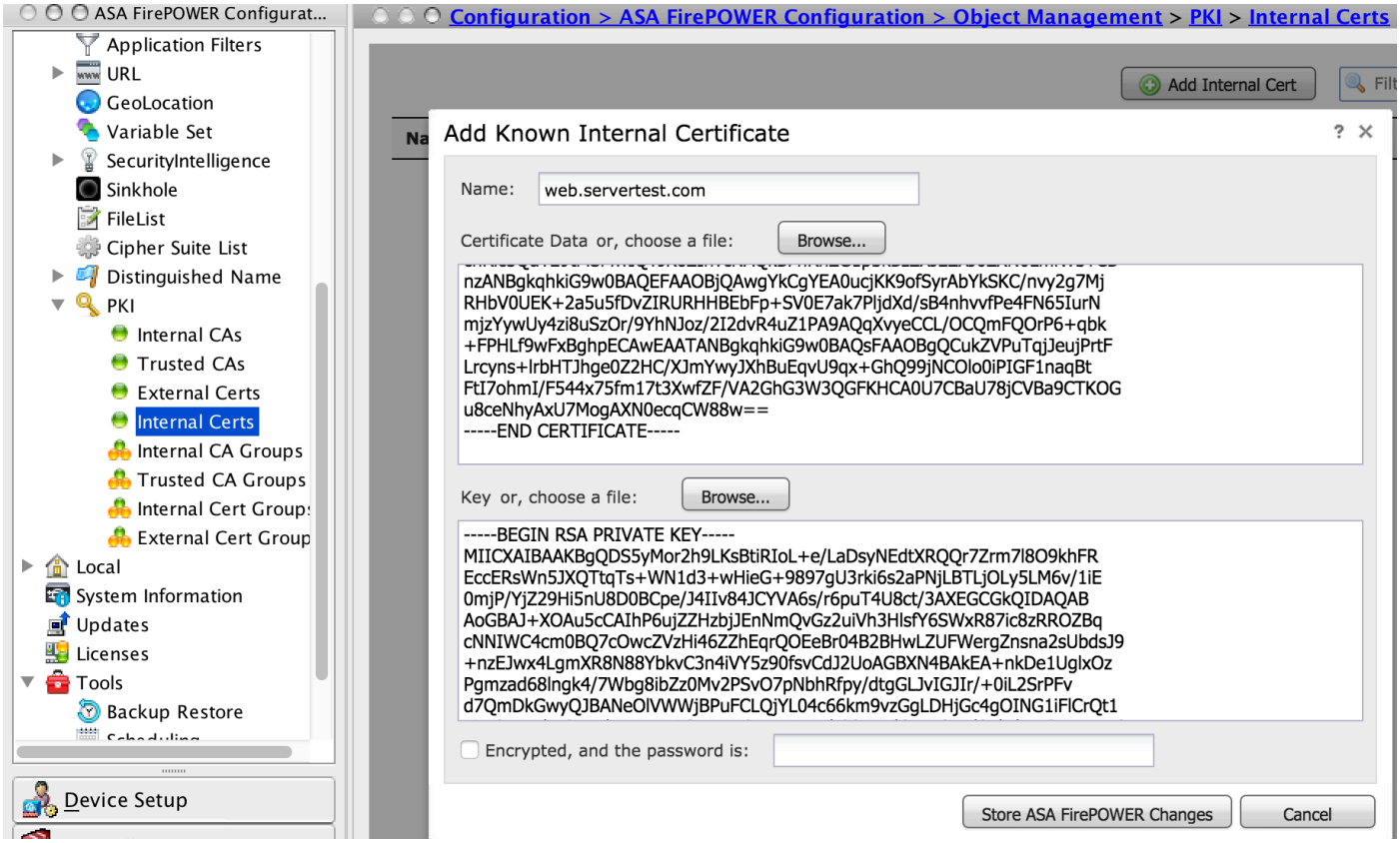
アウトバウンドSSL復号化を設定する4つの手順を次に示します。

ステップ1：サーバ証明書とキーをインポートします。

サーバ証明書とキーをインポートするには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [PKI] > [Internal Certs]に移動し、[Add Internal Cert]をクリックします。

図に示すように、証明書の名前を指定します。ローカルマシンから証明書を選択するか、証明書データに証明書の内容をコピーアンドペーストする場合は、[参照]を選択します。証明書の秘密キーを指定するには、キーファイルを参照するか、キーをコピー&ペーストしてオプションKeyに貼り付けます。

キーが暗号化されている場合は、図に示すように、[Encrypted]チェックボックスをオンにし、パスワードを指定します。



[Store ASA FirePOWER Changes]をクリックして、証明書の内容を保存します。

ステップ2:CA証明書をインポートします（オプション）。

内部の中間CA証明書またはルートCA証明書によって署名されたサーバ証明書の場合、CA証明書の内部チェーンをFirepowerモジュールにインポートする必要があります。インポートの実行後、firepowerモジュールはサーバ証明書を検証できます。

CA証明書をインポートするには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [Trusted CAs]に移動し、[Add Trusted CA]をクリックしてCA証明書を追加します。

ステップ3:SSLポリシーを設定します。

SSLポリシーは、着信トラフィックを復号化するDecrypt-known方式を設定するアクションとサーバの詳細を定義します。複数の内部サーバがある場合は、異なるサーバと、それらのサーバが処

理するトラフィックに基づいて、複数のSSLルールを設定します（SSLルールはSSLルールに基づいて設定します）。

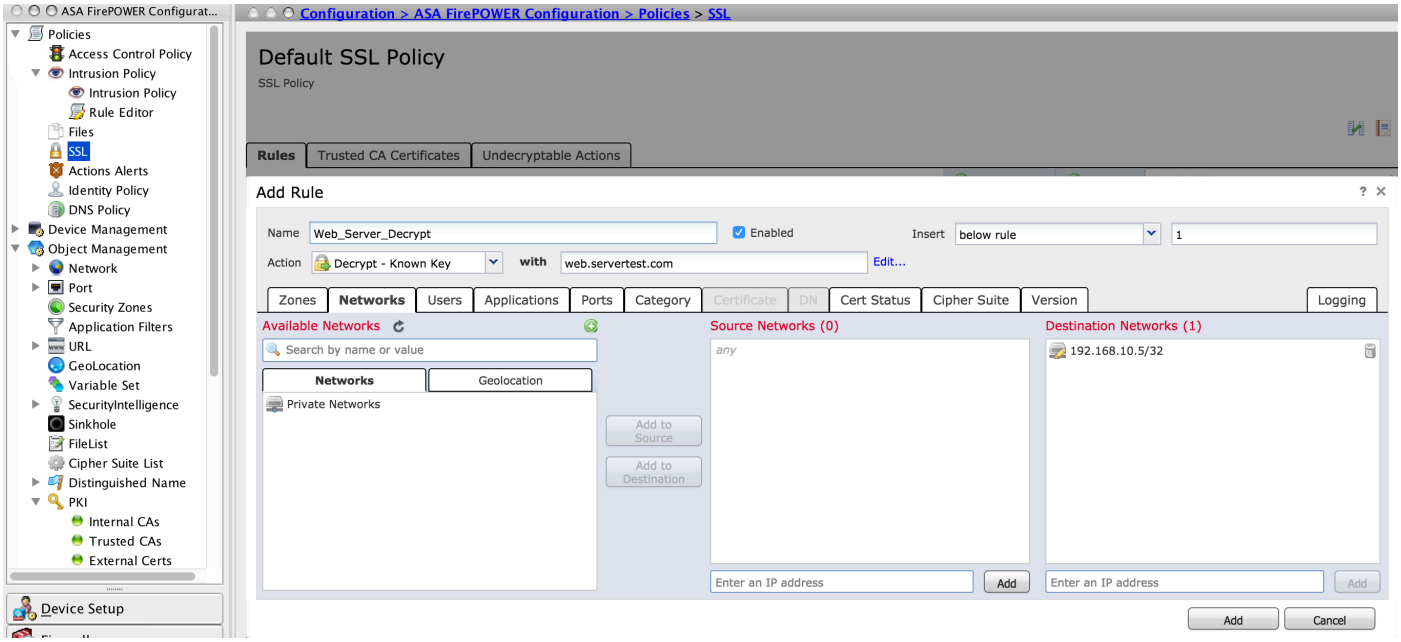
SSLポリシーを設定するには、[Configure] > [ASA FirePOWER Configuration] > [Policies] > [SSL]に移動し、[Add Rule]をクリックします。

名前：ルールの名前を指定します。

アクション：アクションとして**Decrypt - known**を指定し、前の手順で設定したドロップダウンリストからCA証明書を選択します。

SSL復号化を有効にするサーバーの対象トラフィックを定義するために複数のオプション（ネットワーク、アプリケーション、ポートなど）が指定されているため、このルールに一致する条件を定義します。[信頼できるCA証明書]タブの[選択された信頼できるCA]で内部CAをををにします。

SSL復号化のイベントを生成するには、ロギング・オプションを**有効に**します。



[Add]をクリックし、SSLルールを追加します。

次に、[Store ASA Firepower Changes]をクリックし、**SSLポリシー**の設定を保存します。

ステップ 4：アクセス コントロール ポリシーを設定する。

適切なルールを使用してSSLポリシーを設定したら、変更を実装するためにアクセスコントロールでSSLポリシーを指定する必要があります。

アクセスコントロールポリシーを設定するには、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control]に移動します。

[SSL Policy]の横にある[None]オプションをクリックするか、[Advanced] > [SSL Policy Setting]に移動し、ドロップダウンリストからSSLポリシーを指定し、[OK]をクリックして保存します。

クリック **ASA Firepowerの変更の保存** SSLポリシーの設定を保存します。

アクセス コントロール ポリシーを展開する必要があります。ポリシーを適用する前に、モジュールにAccess Control Policyの最新の情報が表示されます。センサーに変更を展開するには、[Deploy]をクリックし、[**Deploy FirePOWER Changes]オプションを選択します。**変更を確認し、ポップアップウィ**ンドウ**で[Deploy]をクリックします。

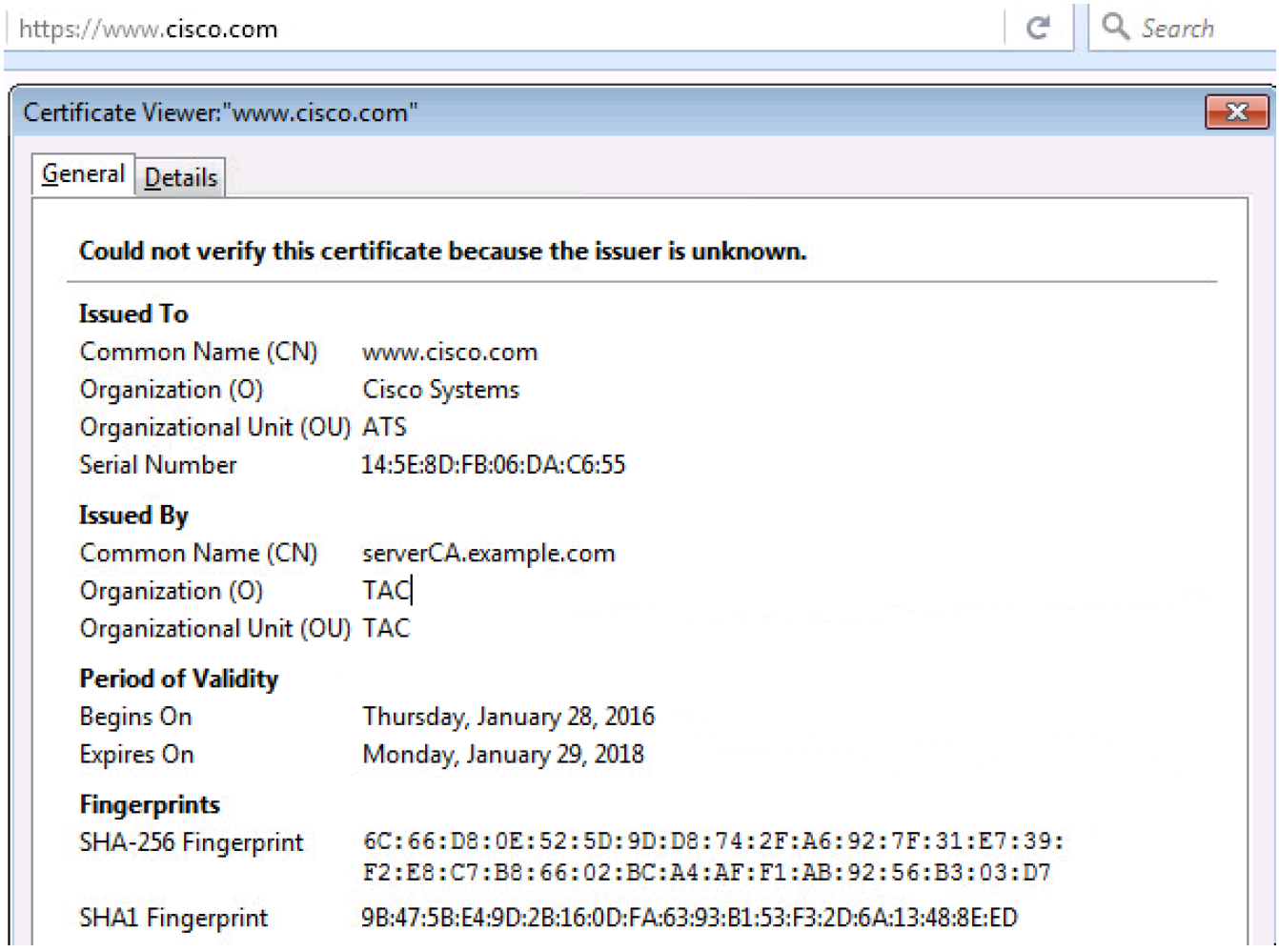
> **注**：バージョン5.4.xでは、アクセスポリシーをセンサーに適用する必要がある場合は、[Apply ASA FirePOWER Changes]をクリックします。

> **注**：[Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動します。次に、設定変更を適用して、タスクが完了したことを確認します。

確認

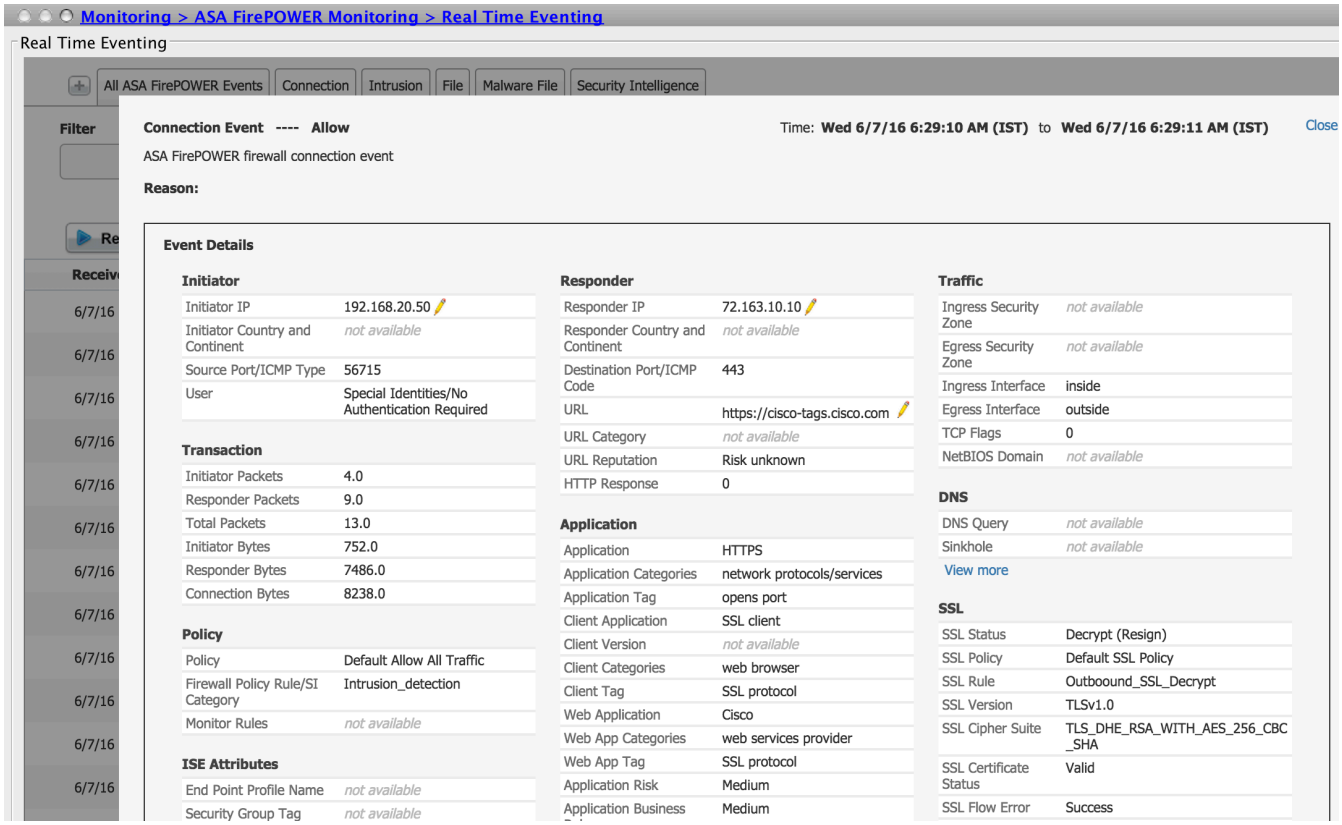
ここでは、設定が正常に機能しているかどうかを確認します。

- アウトバウンドSSL接続では、内部ネットワークからパブリックSSL Webサイトを参照すると、システムから証明書のエラーメッセージが表示されます。証明書の内容を確認し、CA情報を確認します。Firepowerモジュールで設定した内部CA証明書が表示されます。エラーメッセージを受け入れて、SSL証明書を参照します。エラーメッセージが表示されないようにするには、ブラウザの信頼できるCAリストにCA証明書を追加します。



- 接続イベントをチェックして、トラフィックによって中断されているSSLポリシーとSSLル

ールを確認します。[Monitoring] > [ASA FirePOWER Monitoring] > [Real-Time Eventing]に移動します。イベントを選択し、[View Details]をクリックします。SSL復号化の統計情報を確認します。



- アクセス コントロール ポリシーの導入が正常に完了したことを確認します。
- アクセスコントロールポリシーにSSLポリシーが含まれていることを確認します。
- SSLポリシーに、インバウンド方向とアウトバウンド方向の適切なルールが含まれていることを確認します。
- SSLルールに、対象トラフィックを定義する適切な条件が含まれていることを確認します。
- 接続イベントを監視して、SSLポリシーとSSLルールを確認します。
- SSL復号化ステータスを確認します。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems