Konfigurieren der SSL-Entschlüsselung auf dem FirePOWER-Modul mithilfe von ASDM (integriertes Management)

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration der SSL-Entschlüsselung (Secure Sockets Layer) auf dem FirePOWER-Modul mithilfe von ASDM (On-Box Management).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis der ASA-Firewall (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Kenntnis der FirePOWER-Appliance
- Kenntnis des HTTPS/SSL-Protokolls

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 6.0.0 und höher
- ASA FirePOWER-Modul (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) mit Softwareversion 6.0.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

> **Hinweis**: Stellen Sie sicher, dass das FirePOWER-Modul über eine **Protect**-Lizenz verfügt, um diese Funktion zu konfigurieren. Um die Lizenz zu überprüfen, wählen Sie **Configuration > ASA FirePOWER Configuration > License aus**.

Hintergrundinformationen

Das FirePOWER-Modul entschlüsselt und prüft ein- und ausgehende SSL-Verbindungen, die an das Modul umgeleitet werden. Sobald der Datenverkehr entschlüsselt ist, werden getunnelte Anwendungen wie Facebook-Chat usw. erkannt und kontrolliert. Die entschlüsselten Daten werden auf Bedrohungen, URL-Filterung, Dateiblockierung oder schädliche Daten geprüft.

Ausgehende SSL-Entschlüsselung

Das Firepower-Modul fungiert als Forward-Proxy für ausgehende SSL-Verbindungen, indem es ausgehende SSL-Anfragen abfängt und ein Zertifikat für die Site wiederherstellt, die der Benutzer besuchen möchte. Die ausstellende Behörde (CA) ist das selbstsignierte FirePOWER-Zertifikat. Wenn das Zertifikat der Firewall nicht Teil einer bestehenden Hierarchie ist oder nicht zum Browser-Cache eines Clients hinzugefügt wird, erhält der Client beim Navigieren zu einer sicheren Website eine Warnung. Die Entschlüsselungsmethode wird zum Durchführen der SSL-Entschlüsselung für ausgehenden Datenverkehr verwendet.

Eingehende SSL-Entschlüsselung

Bei eingehenden Datenverkehr zu einem internen Webserver oder Gerät importiert der Administrator eine Kopie des Zertifikats und des Schlüssels des geschützten Servers. Wenn das SSL-Serverzertifikat auf das Firepower-Modul geladen wird und die SSL-Verschlüsselungsrichtlinie für den eingehenden Datenverkehr konfiguriert wird, entschlüsselt und prüft das Gerät den Datenverkehr beim Weiterleiten. Das Modul erkennt dann schädliche Inhalte, Bedrohungen und Malware, die über diesen sicheren Kanal übertragen werden. Darüber hinaus wird die Entschlüsselungsmethode verwendet, um eine eingehende SSL-Entschlüsselung durchzuführen.

Konfiguration für SSL-Entschlüsselung

Es gibt zwei Methoden zur Entschlüsselung des SSL-Datenverkehrs.

- Entschlüsseln - Für ausgehenden SSL-Datenverkehr kündigen
- Entschlüsseln - Bekannt für eingehenden SSL-Datenverkehr

Entschlüsselung ausgehender SSL-Verbindungen (Entschlüsseln - Zurücksetzen)

Das FirePOWER-Modul fungiert als MITM (Man-in-the-Middle) für alle SSL-Verhandlungen für öffentliche SSL-Server. Das Zertifikat des öffentlichen Servers wird mit einem Zwischenzertifikat der Zertifizierungsstelle zurückgesendet, das auf dem Firepower-Modul konfiguriert ist.

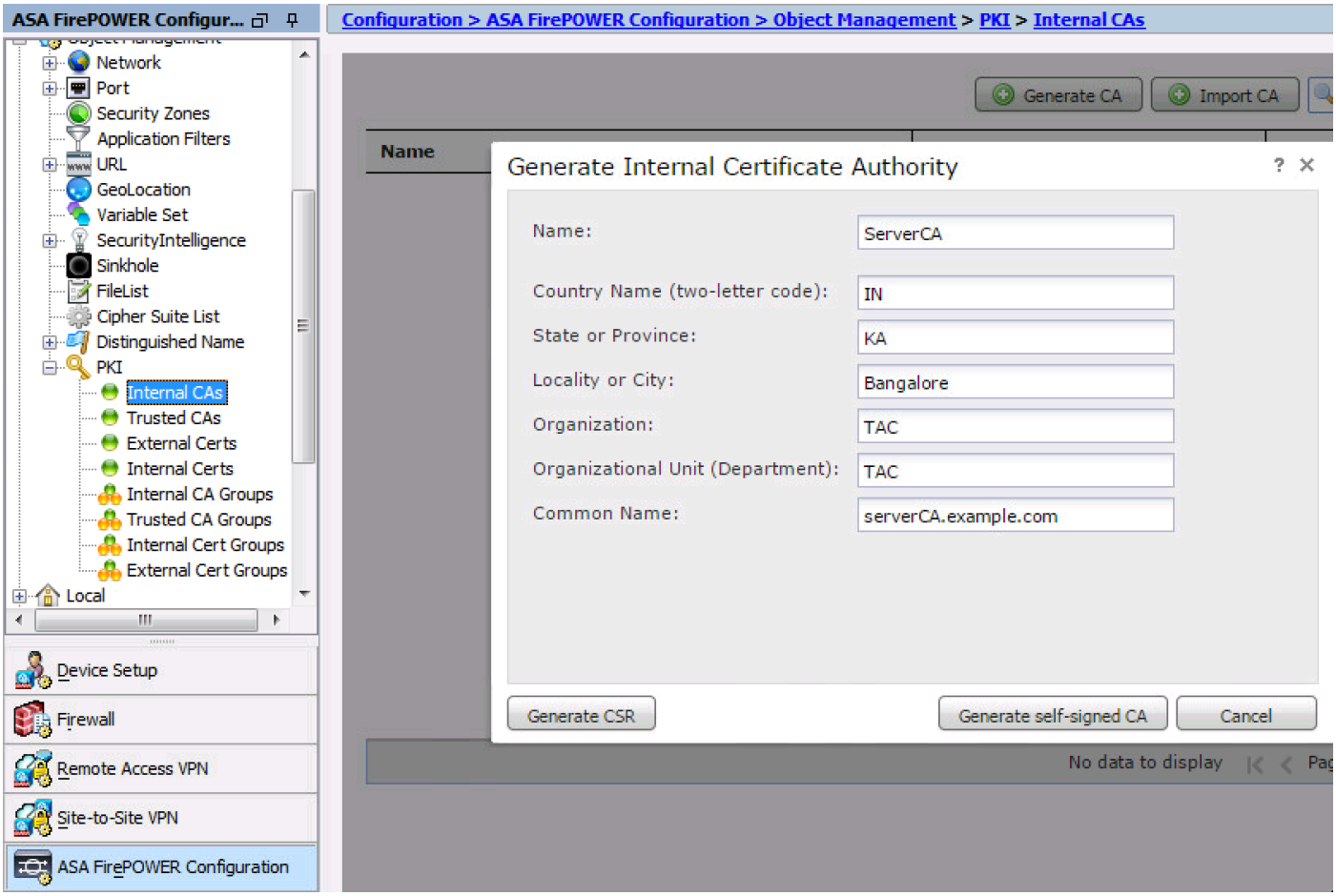
Dies sind die drei Schritte zum Konfigurieren der ausgehenden SSL-Entschlüsselung.

Schritt 1: Konfigurieren Sie das CA-Zertifikat.

Konfigurieren Sie entweder ein selbstsigniertes Zertifikat oder ein zwischengeschaltetes vertrauenswürdiges Zertifizierungsstellen-Zertifikat für den Zertifikatsrücktritt.

Konfigurieren des selbstsignierten Zertifizierungsstellenzertifikats

Um das selbst signierte CA-Zertifikat zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal CAs** und klicken Sie auf **Generate CA (CA generieren)**. Das System fordert Sie zur Eingabe der Details des Zertifizierungsstellenzertifikats auf. Wie im Bild gezeigt, füllen Sie die Details entsprechend Ihrer Anforderungen aus.



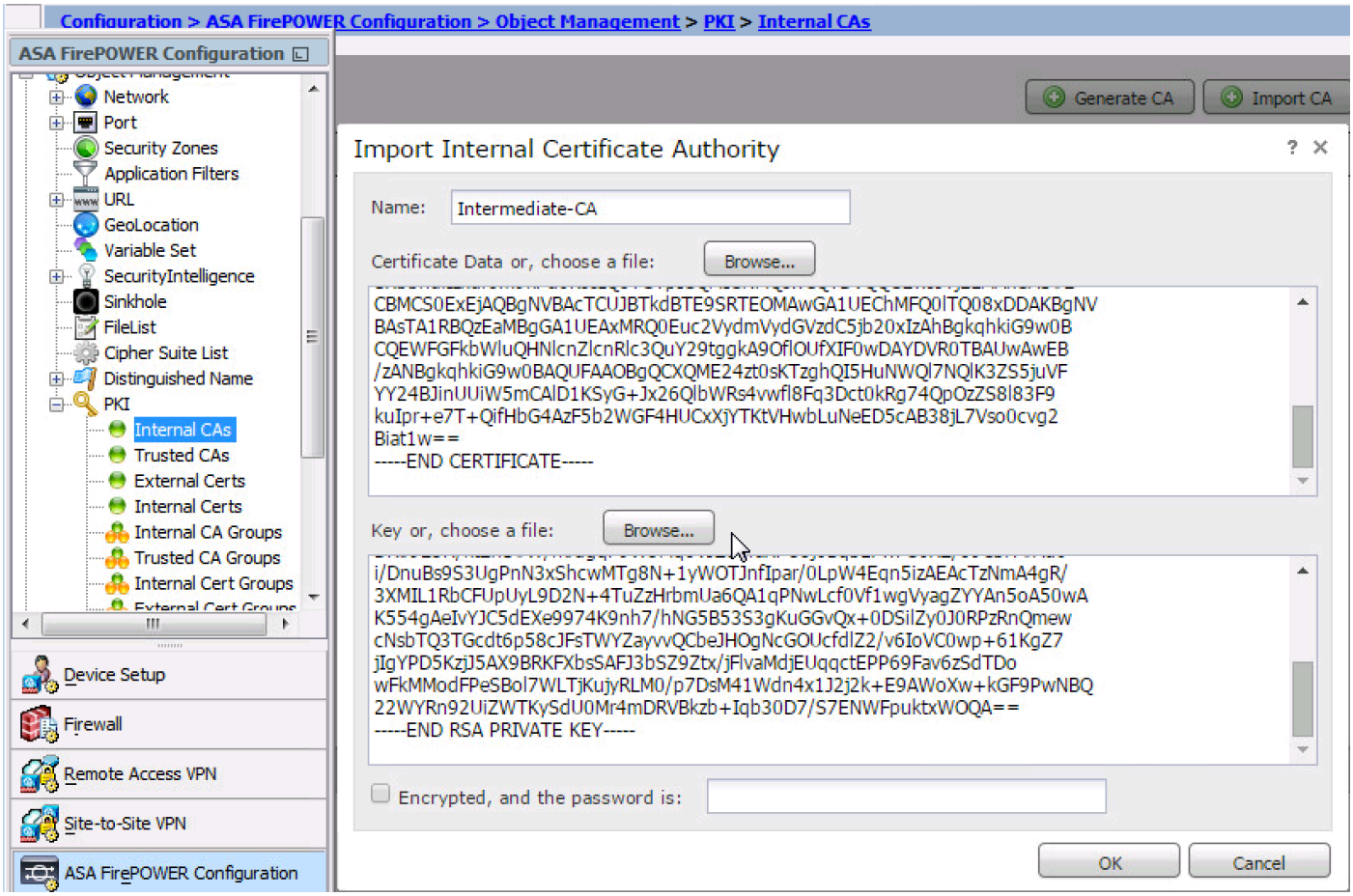
Klicken Sie auf **Eigensignierte CA erstellen**, um das interne Zertifizierungsstellenzertifikat zu generieren. Klicken Sie anschließend auf **CSR erstellen**, um die Zertifikatssignierungsanfrage zu generieren, die dann zur Signierung an den CA-Server weitergegeben wird.

Konfigurieren des Zertifikats der vermittelten Zertifizierungsstelle

Um das von einer anderen CA signierte Zertifikat der Zwischen-Zertifizierungsstelle zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal CAs** und klicken Sie auf **Import CA**.

Geben Sie den Namen des Zertifikats an. Wählen Sie **Durchsuchen** und Hochladen des Zertifikats vom lokalen Computer aus, oder fügen Sie den Inhalt des Zertifikats in die Option **Zertifikatsdaten** ein. Um den privaten Schlüssel des Zertifikats anzugeben, durchsuchen Sie entweder die Schlüsseldatei, oder fügen Sie den Schlüssel in die **Key-**Option ein.

Wenn der Schlüssel verschlüsselt ist, aktivieren Sie das Kontrollkästchen **Verschlüsselt,** und geben Sie das Kennwort an. Klicken Sie auf **OK**, um den Zertifikatsinhalt zu speichern, wie im Bild gezeigt:



Schritt 2: Konfigurieren Sie die SSL-Richtlinie.

Die SSL-Richtlinie definiert die Entschlüsselungsaktion und identifiziert den Datenverkehr, auf den die Entschlüsselungsmethode angewendet wird. Konfigurieren Sie die verschiedenen SSL-Regeln auf Basis Ihrer geschäftlichen Anforderungen und Sicherheitsrichtlinien.

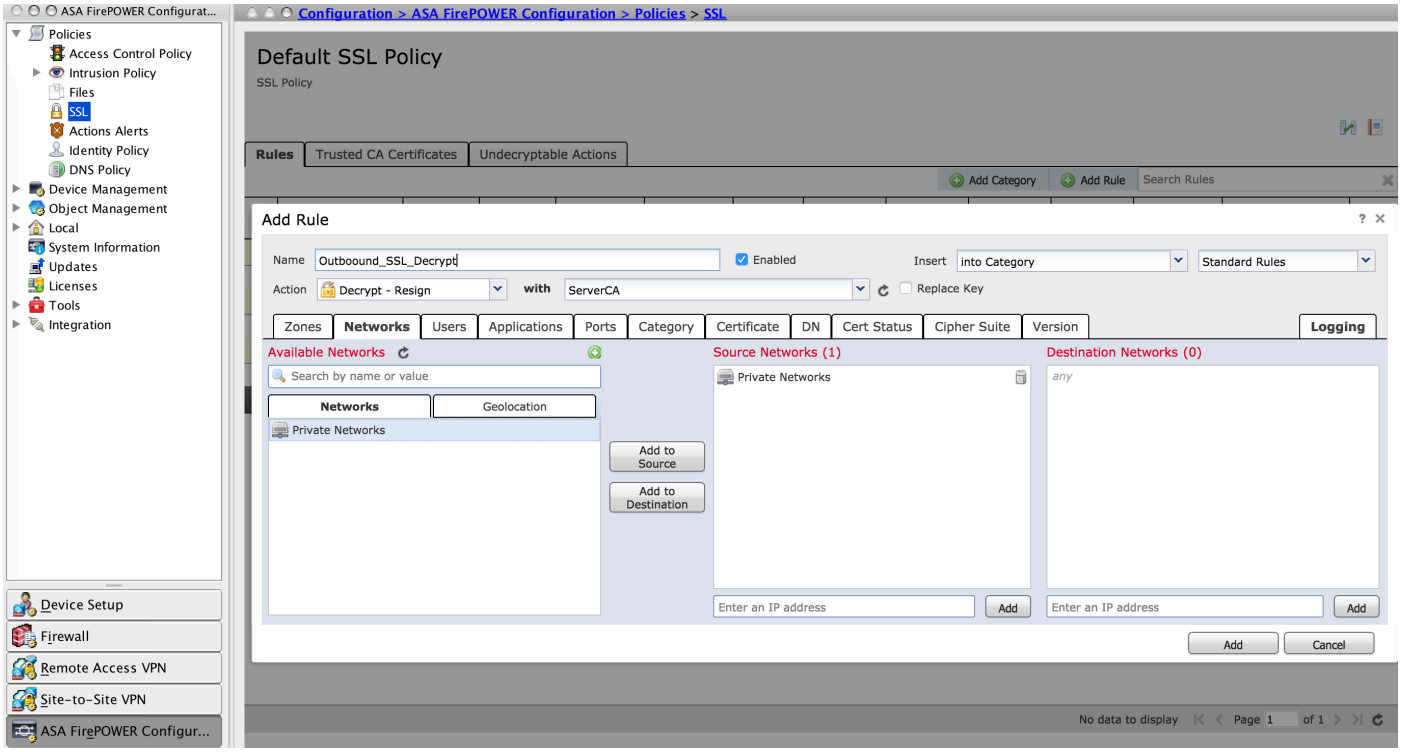
Um die SSL-Richtlinie zu konfigurieren, wählen Sie **Configure > ASA FirePOWER Configuration > Policies > SSL aus,** und klicken Sie auf **Add Rule (Regel hinzufügen)**.

Name: Geben Sie den Namen der Regel an.

Aktion: Geben Sie die Aktion als **Entschlüsseln - Zurückweisen an,** und wählen Sie das Zertifizierungsstellenzertifikat aus der Dropdown-Liste aus, die im vorherigen Schritt konfiguriert wurde.

Definieren Sie in der Regel Bedingungen, um den Datenverkehr abzugleichen, da es mehrere Optionen gibt (Zone, Netzwerk, Benutzer usw.), die zum Definieren des Datenverkehrs, der entschlüsselt werden muss, angegeben werden.

Aktivieren Sie zum Generieren der SSL-Entschlüsselungsereignisse die **Protokollierungsoption**, wie im Bild gezeigt:



Klicken Sie auf **Hinzufügen**, um die SSL-Regel hinzuzufügen.

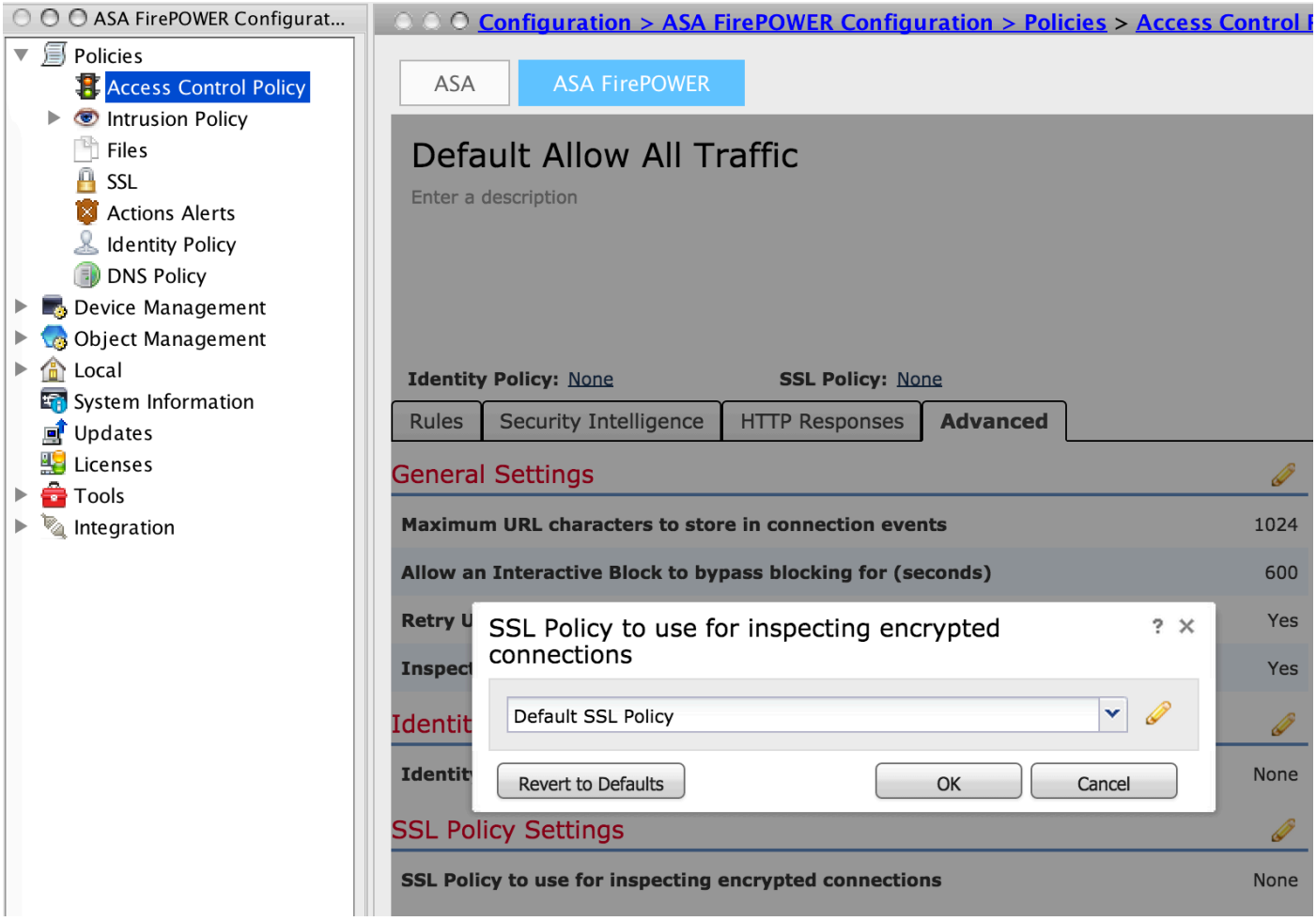
Klicken Sie auf **Store ASA FirePOWER Changes**, um die Konfiguration der SSL-Richtlinie zu speichern.

Schritt 3: Konfigurieren der Zugriffskontrollrichtlinie

Wenn Sie die SSL-Richtlinie mit entsprechenden Regeln konfigurieren, müssen Sie die SSL-Richtlinie in der Zugriffskontrolle angeben, um die Änderungen zu implementieren.

Um die Zugriffskontrollrichtlinie zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control.**

Klicken Sie entweder auf **Keine** der **SSL-Richtlinie** oder navigieren Sie zu **Erweitert > SSL Policy Setting.** Geben Sie die SSL-Richtlinie aus der Dropdown-Liste ein, und klicken Sie auf **OK**, um sie zu speichern, wie im Bild gezeigt:



Klicken **ASA FirePOWER-Änderungen speichern** um die Konfiguration der SSL-Richtlinie zu speichern.

Sie müssen die Zugriffskontrollrichtlinie auf dem Sensor bereitstellen. Bevor Sie die Richtlinie anwenden, gibt es Hinweise darauf, dass die **Zugriffskontrollrichtlinie** auf dem Modul **veraltet ist**. Um die Änderungen am Sensor bereitzustellen, klicken Sie auf **Deploy** und wählen Sie die **Option Deploy FirePOWER Changes (FirePOWER-Änderungen bereitstellen).** Überprüfen Sie die vorgenommenen Änderungen, und klicken Sie auf **Bereitstellen.**

> **Hinweis**: Wenn Sie in Version 5.4.x die Zugriffsrichtlinie auf den Sensor anwenden möchten, klicken Sie auf **ASA FirePOWER-Änderungen anwenden.**

> **Hinweis**: Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Task Status.** Anschließend beantragen Sie Konfigurationsänderungen, um sicherzustellen, dass die Aufgabe abgeschlossen ist.

Eingehende SSL-Entschlüsselung (Entschlüsseln - bekannt)

Die Methode der eingehenden SSL-Entschlüsselung (Entschlüsselung - bekannt) wird verwendet, um den eingehenden SSL-Datenverkehr zu entschlüsseln, für den Sie ein Serverzertifikat und einen privaten Schlüssel konfiguriert haben. Sie müssen das Serverzertifikat und den privaten Schlüssel in das FirePOWER-Modul importieren. Wenn SSL-Datenverkehr auf das FirePOWER-Modul trifft, entschlüsselt er den Datenverkehr und führt die Überprüfung des entschlüsselten

Datenverkehrs durch. Nach der Überprüfung verschlüsselt das FirePOWER-Modul den Datenverkehr neu und sendet ihn an den Server.

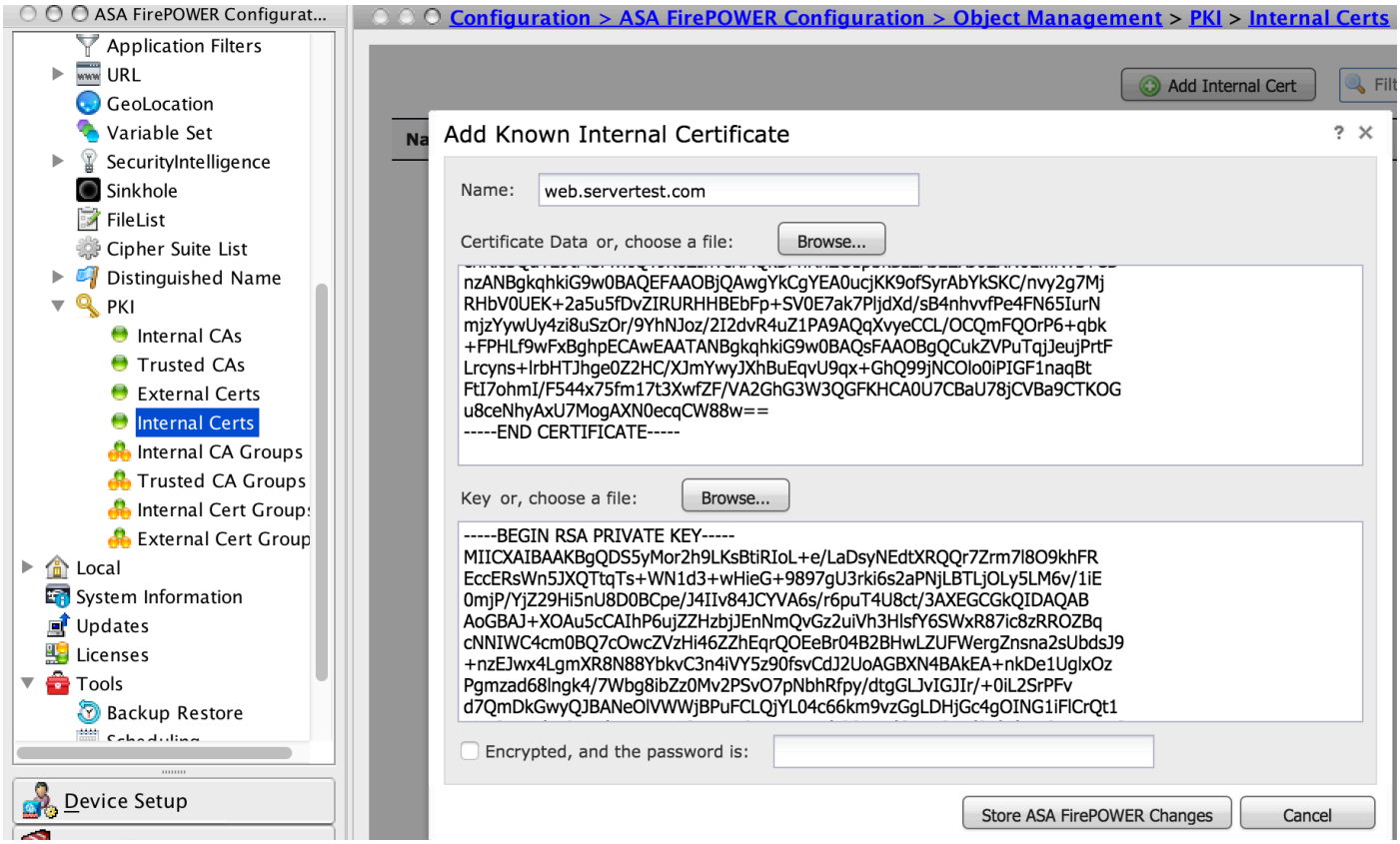
Dies sind die vier Schritte zum Konfigurieren der ausgehenden SSL-Entschlüsselung:

Schritt 1: Importieren Sie das Serverzertifikat und den Serverschlüssel.

Um das Serverzertifikat und den Serverschlüssel zu importieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal Certs** und klicken Sie auf **Add Internal Cert**.

Geben Sie, wie im Bild gezeigt, den Namen des Zertifikats an. Wählen Sie entweder **Durchsuchen**, um das Zertifikat vom lokalen Computer auszuwählen, oder fügen Sie den Inhalt des Zertifikats in die **Zertifikatsdaten ein**. Um den privaten Schlüssel des Zertifikats anzugeben, durchsuchen Sie entweder die Schlüsseldatei, oder fügen Sie den Schlüssel in die Option **Schlüssel** ein.

Wenn der Schlüssel verschlüsselt ist, aktivieren Sie das Kontrollkästchen **Verschlüsselt,** und geben Sie das Kennwort an, wie im Bild gezeigt:



Klicken Sie auf **Store ASA FirePOWER Changes**, um den Zertifikatsinhalt zu speichern.

Schritt 2: Importieren Sie das Zertifizierungsstellenzertifikat (optional).

Für ein Serverzertifikat, das vom internen Zwischenzertifikat oder dem Stammzertifikat der Zertifizierungsstelle signiert wird, müssen Sie die interne Kette von Zertifizierungsstellenzertifikaten in das Firepower-Modul importieren. Nach dem Import kann das Firewall-Modul das Serverzertifikat validieren.

Um das CA-Zertifikat zu importieren, navigieren Sie zu **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** und klicken Sie auf **Add Trusted CA (Vertrauenswürdige CA hinzufügen)**, um das CA-Zertifikat hinzuzufügen.

Schritt 3: Konfigurieren Sie die SSL-Richtlinie.

Die SSL-Richtlinie definiert die Aktion und die Serverdetails, für die Sie die Entschlüsselungsmethode zum Entschlüsseln des eingehenden Datenverkehrs konfigurieren möchten. Wenn Sie über mehrere interne Server verfügen, konfigurieren Sie mehrere SSL-Regeln, die auf unterschiedlichen Servern und dem von ihnen verarbeiteten Datenverkehr basieren.

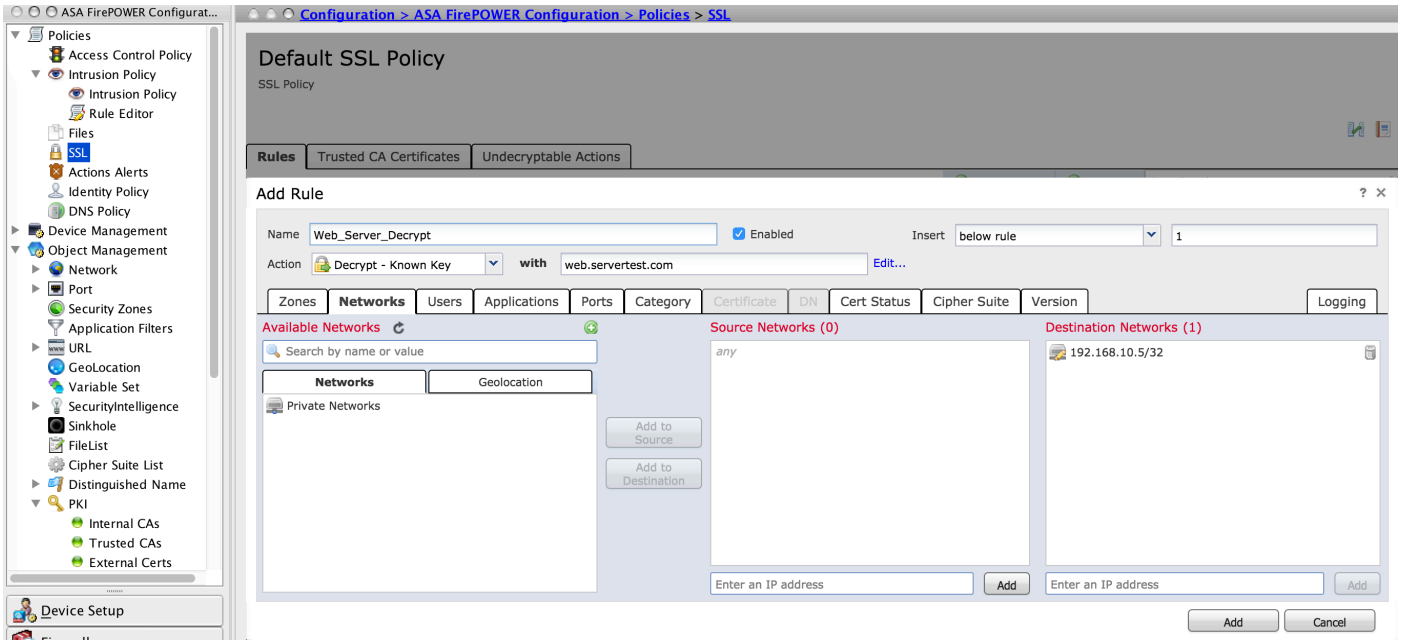
Um die SSL-Richtlinie zu konfigurieren, wählen Sie **Configure > ASA FirePOWER Configuration > Policies > SSL aus,** und klicken Sie auf **Add Rule (Regel hinzufügen)**.

Name: Geben Sie den Namen der Regel an.

Aktion: Geben Sie die Aktion als **Entschlüsseln - bekannt an** und wählen Sie das Zertifizierungsstellenzertifikat aus der Dropdown-Liste aus, die im vorherigen Schritt konfiguriert wurde.

Definieren Sie die Bedingung, um diese Regeln zu erfüllen, da mehrere Optionen (Netzwerk, Anwendung, Ports usw.) angegeben sind, um den interessanten Datenverkehr des Servers zu definieren, für den Sie die SSL-Entschlüsselung aktivieren möchten. Geben Sie die interne CA auf der Registerkarte **Ausgewählte vertrauenswürdige CAs im Zertifikat für vertrauenswürdige CA an.**

Um die SSL-Entschlüsselungsereignisse zu generieren, aktivieren Sie die Option **Loggingat logging**.



Klicken Sie auf **Hinzufügen**, um die SSL-Regel hinzuzufügen.

Klicken Sie dann auf **"Store ASA FirePOWER Changes"**, um die Konfiguration der SSL-Richtlinie zu speichern.

Schritt 4: Konfigurieren Sie die Zugriffskontrollrichtlinie.

Wenn Sie die SSL-Richtlinie mit entsprechenden Regeln konfigurieren, müssen Sie die SSL-Richtlinie in der Zugriffskontrolle angeben, um die Änderungen zu implementieren.

Um die Zugriffskontrollrichtlinie zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control.**

Klicken Sie entweder auf die Option **Keine** neben **SSL Policy (SSL-Richtlinie),** oder navigieren Sie zu **Advanced > SSL Policy Setting (Erweitert > SSL Policy Setting),** geben Sie die SSL-Richtlinie in der Dropdown-Liste an, und klicken Sie auf **OK**, um die Richtlinie zu speichern.

Klicken **ASA FirePOWER-Änderungen speichern** um die Konfiguration der SSL-Richtlinie zu speichern.

Sie müssen die Zugriffskontrollrichtlinie bereitstellen. Bevor Sie die Richtlinie anwenden, sehen Sie eine veraltete Anzeige "Zugriffskontrollrichtlinie" auf dem Modul. Um die Änderungen am Sensor bereitzustellen, klicken Sie auf **Deploy** und wählen Sie die **Option Deploy FirePOWER Changes (FirePOWER-Änderungen bereitstellen).** Überprüfen Sie die vorgenommenen Änderungen, und klicken Sie im Popup-Fenster auf **Bereitstellen**.

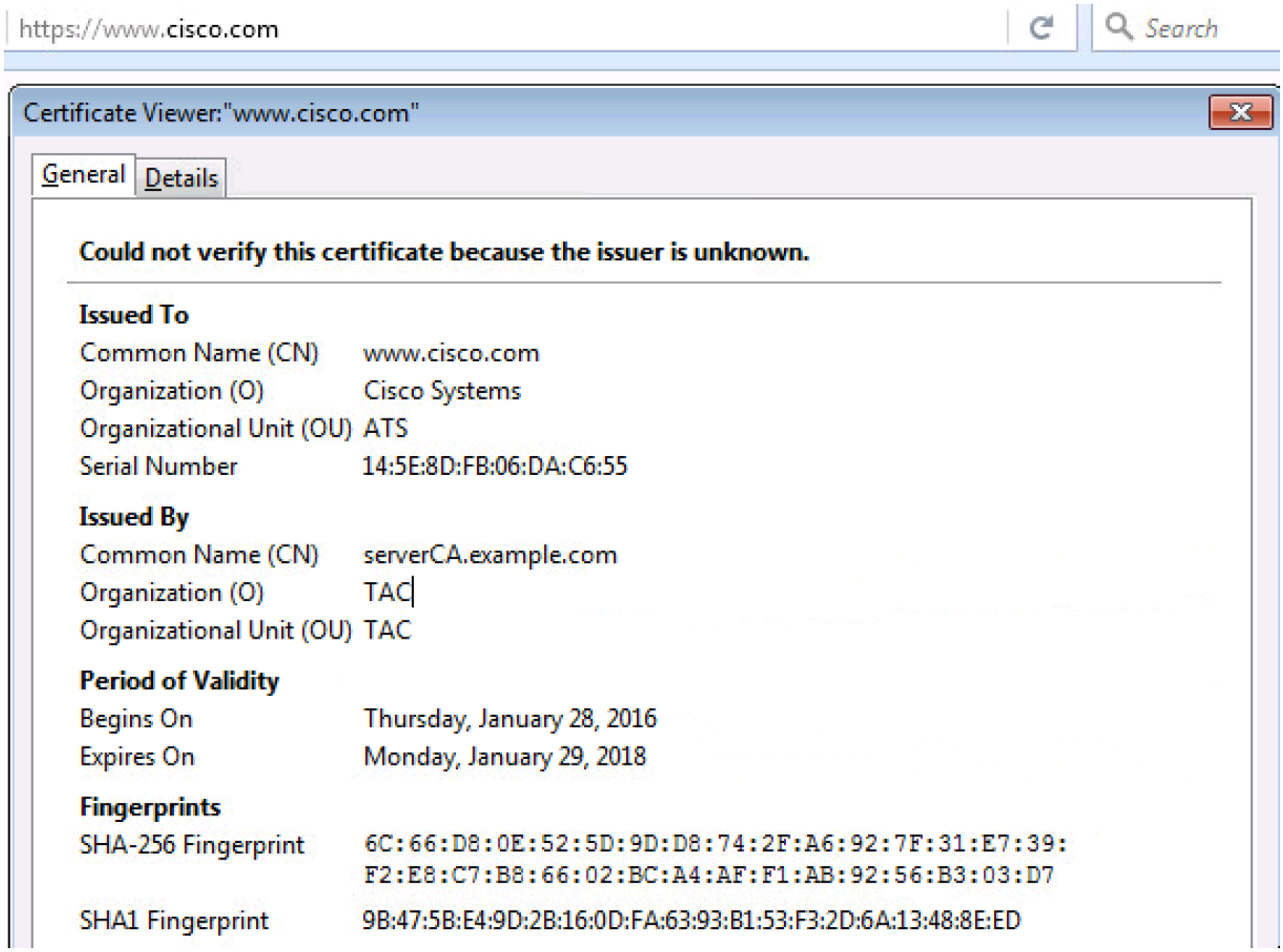
> **Hinweis**: Wenn Sie in Version 5.4.x die Zugriffsrichtlinie auf den Sensor anwenden möchten, klicken Sie auf **Apply ASA FirePOWER Changes**.

> **Hinweis**: Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Task Status.** Anschließend beantragen Sie Konfigurationsänderungen, um sicherzustellen, dass die Aufgabe abgeschlossen ist.

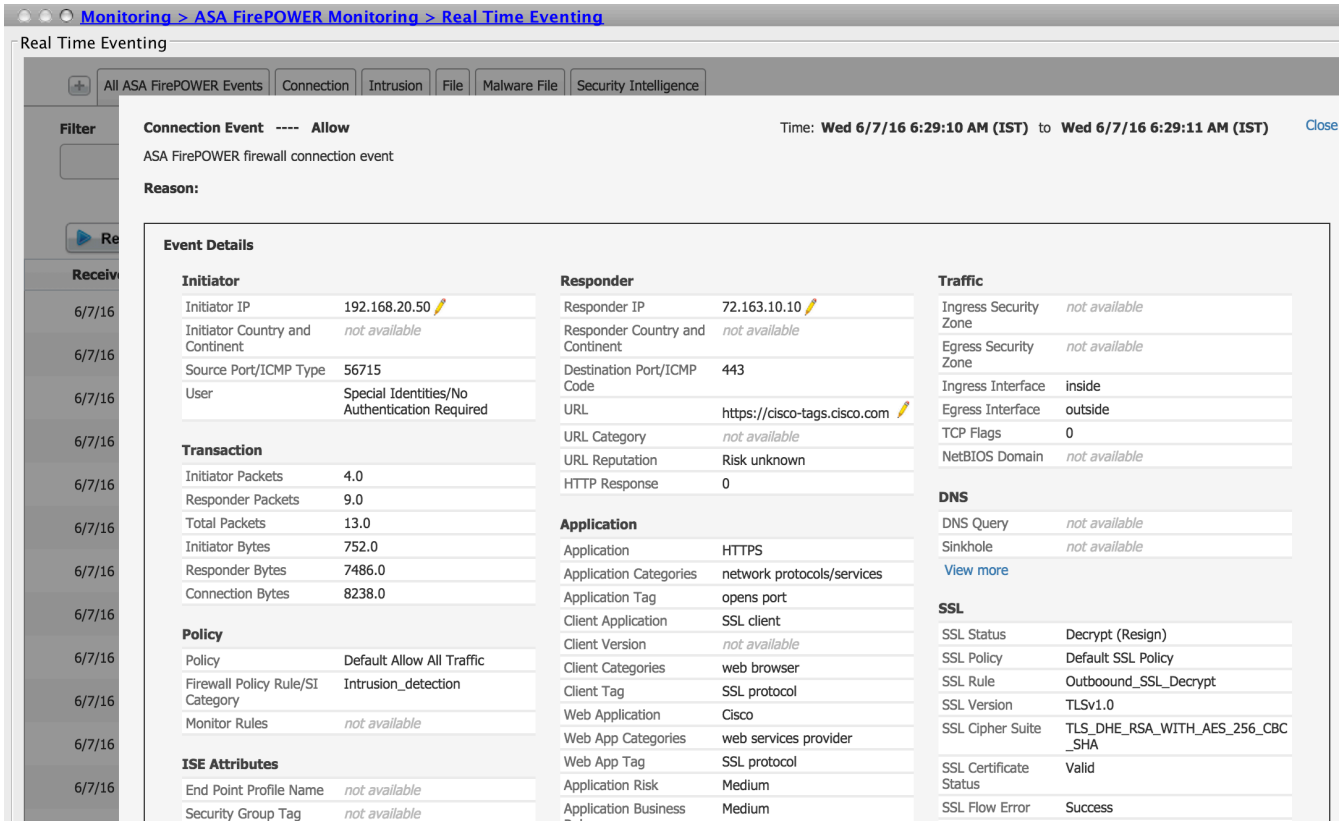
Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- Bei einer ausgehenden SSL-Verbindung fordert das System beim Durchsuchen einer öffentlichen SSL-Website aus dem internen Netzwerk eine Fehlermeldung für das Zertifikat an. Überprüfen Sie den Zertifikatsinhalt, und überprüfen Sie die CA-Informationen. Das interne Zertifizierungsstellenzertifikat, das Sie im FirePOWER-Modul konfiguriert haben, wird angezeigt. Akzeptieren Sie die Fehlermeldung zum Durchsuchen des SSL-Zertifikats. Um die Fehlermeldung zu vermeiden, fügen Sie das CA-Zertifikat in die Liste der vertrauenswürdigen CAs Ihres Browsers hinzu.



- Überprüfen Sie die Verbindungsereignisse, um zu überprüfen, welche SSL-Richtlinie und SSL-Regel vom Datenverkehr betroffen ist. Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing.**Wählen Sie eine Veranstaltung aus, und klicken Sie auf **Details anzeigen**. Überprüfen der SSL-Entschlüsselungsstatistik



- Stellen Sie sicher, dass die Bereitstellung der Zugriffskontrollrichtlinie erfolgreich abgeschlossen ist.
- Stellen Sie sicher, dass die SSL-Richtlinie in die Zugriffskontrollrichtlinie integriert ist.
- Stellen Sie sicher, dass die SSL-Richtlinie die entsprechenden Regeln für die eingehende und die ausgehende Richtung enthält.
- Stellen Sie sicher, dass SSL-Regeln die richtige Bedingung für die Definition des interessanten Datenverkehrs enthalten.
- Überwachen Sie die Verbindungsereignisse, um die SSL-Richtlinie und die SSL-Regel zu überprüfen.
- Überprüfen Sie den SSL-Entschlüsselungsstatus.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems