Configure el descifrado SSL en el módulo FirePOWER mediante ASDM (administración integrada)

Contenido

Introducción

Este documento describe la configuración del descifrado de Secure Sockets Layer (SSL) en el módulo FirePOWER mediante ASDM (administración integrada).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conocimiento del appliance FirePOWER
- Conocimiento del protocolo HTTPS/SSL

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecutan la versión de software 6.0.0 y superiores
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) que ejecuta la versión de software 6.0.0 y posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Nota:** Asegúrese de que FirePOWER Module tenga una licencia **Protect** para configurar esta funcionalidad. Para verificar la licencia, navegue hasta **Configuration > ASA FirePOWER Configuration > License**.

Antecedentes

Firepower Module descifra e inspecciona las conexiones SSL entrantes y salientes que se le redirigen. Una vez que se descifra el tráfico, se detectan y controlan las aplicaciones tunelizadas como el chat de facebook, etc. Los datos descifrados se inspeccionan en busca de amenazas, filtrado de URL, bloqueo de archivos o datos maliciosos.

Descifrado SSL saliente

El módulo firepower actúa como proxy de reenvío para las conexiones SSL salientes interceptando las solicitudes SSL salientes y regenerando un certificado para el sitio que el usuario desea visitar. La autoridad emisora (CA) es el certificado firmado automáticamente por Firepower. Si el certificado de firepower no forma parte de una jerarquía que existe o si no se agrega a la memoria caché del navegador de un cliente, el cliente recibe una advertencia mientras navega a un sitio seguro. El método Decrypt-Resignmethod se utiliza para realizar el descifrado SSL saliente.

Descifrado SSL entrante

En el caso del tráfico entrante a un servidor Web o dispositivo interno, el administrador importa una copia del certificado del servidor protegido y la clave. Cuando el certificado del servidor SSL se carga en el módulo firepower y la política de descifrado SSL se configura para el tráfico entrante, el dispositivo descifra e inspecciona el tráfico a medida que reenvía el tráfico. A continuación, el módulo detecta contenido malicioso, amenazas y malware que fluyen a través de este canal seguro. Además, el método de clave conocido por descifrado se utiliza para realizar el descifrado SSL entrante.

Configuración para el Descifrado SSL

Hay dos métodos de descifrado de tráfico SSL.

- Descifrar: renuncia para tráfico SSL saliente
- Descifrado: conocido para tráfico SSL entrante

Descifrado SSL saliente (descifrado - renuncia)

El módulo Firepower actúa como MITM (man-in-the-middle) para cualquier negociación SSL para servidores SSL públicos. Renuncia al certificado del servidor público con un certificado CA intermedio que se configura en el módulo firepower.

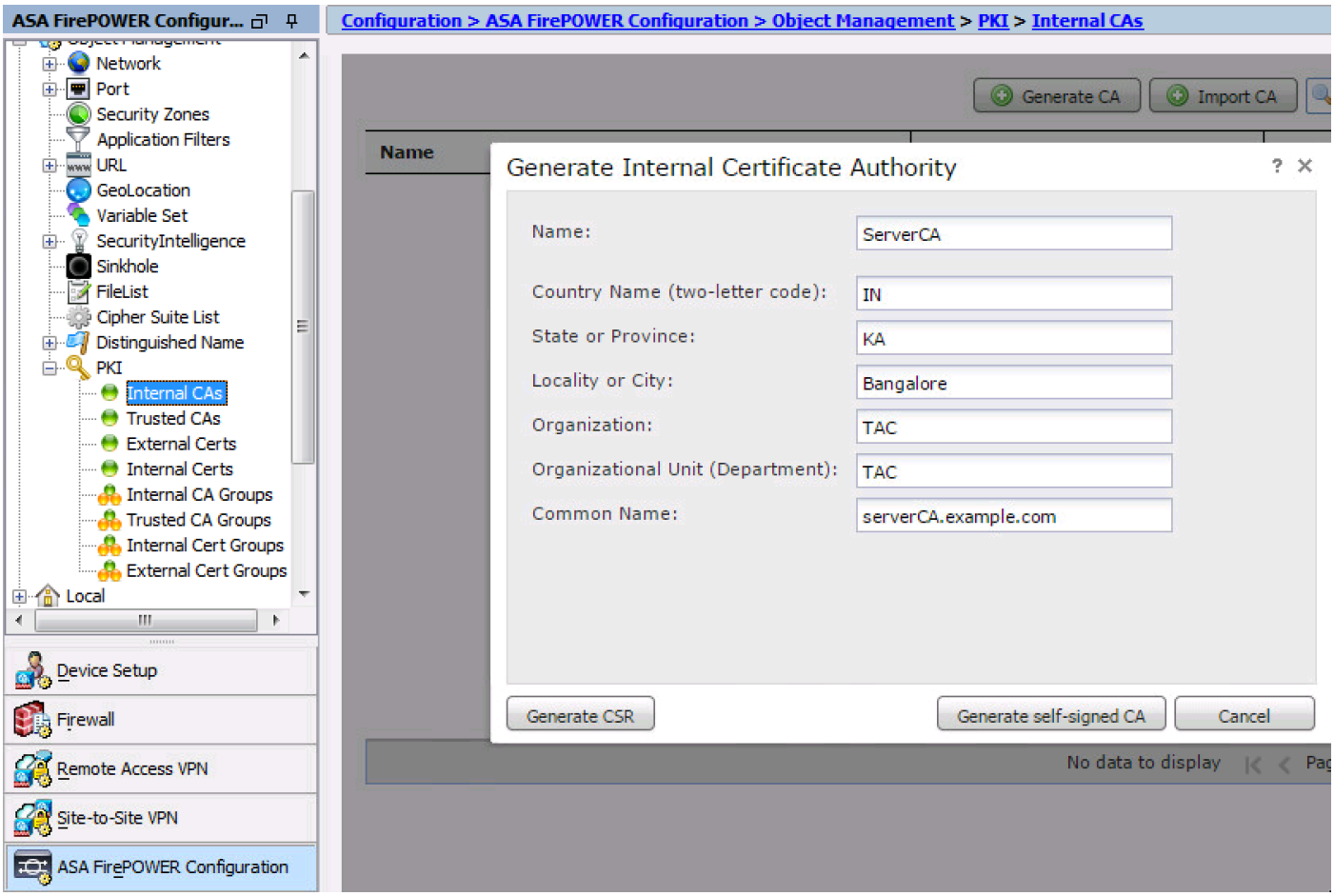
Estos son los tres pasos para configurar el Descifrado SSL saliente.

Paso 1. Configure el certificado de CA.

Configure un certificado autofirmado o un certificado CA de confianza intermedia para la renuncia del certificado.

Configuración del certificado de CA firmado automáticamente

Para configurar el certificado de CA firmado automáticamente, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** y haga clic en **Generate CA**. El sistema solicita los detalles del certificado de CA. Como se muestra en la imagen, complete los detalles según sus necesidades.



Haga clic en **Generar CA autofirmada** para generar el certificado de CA interno. A continuación, haga clic en **Generar CSR** para generar la solicitud de firma de certificado que, en consecuencia,

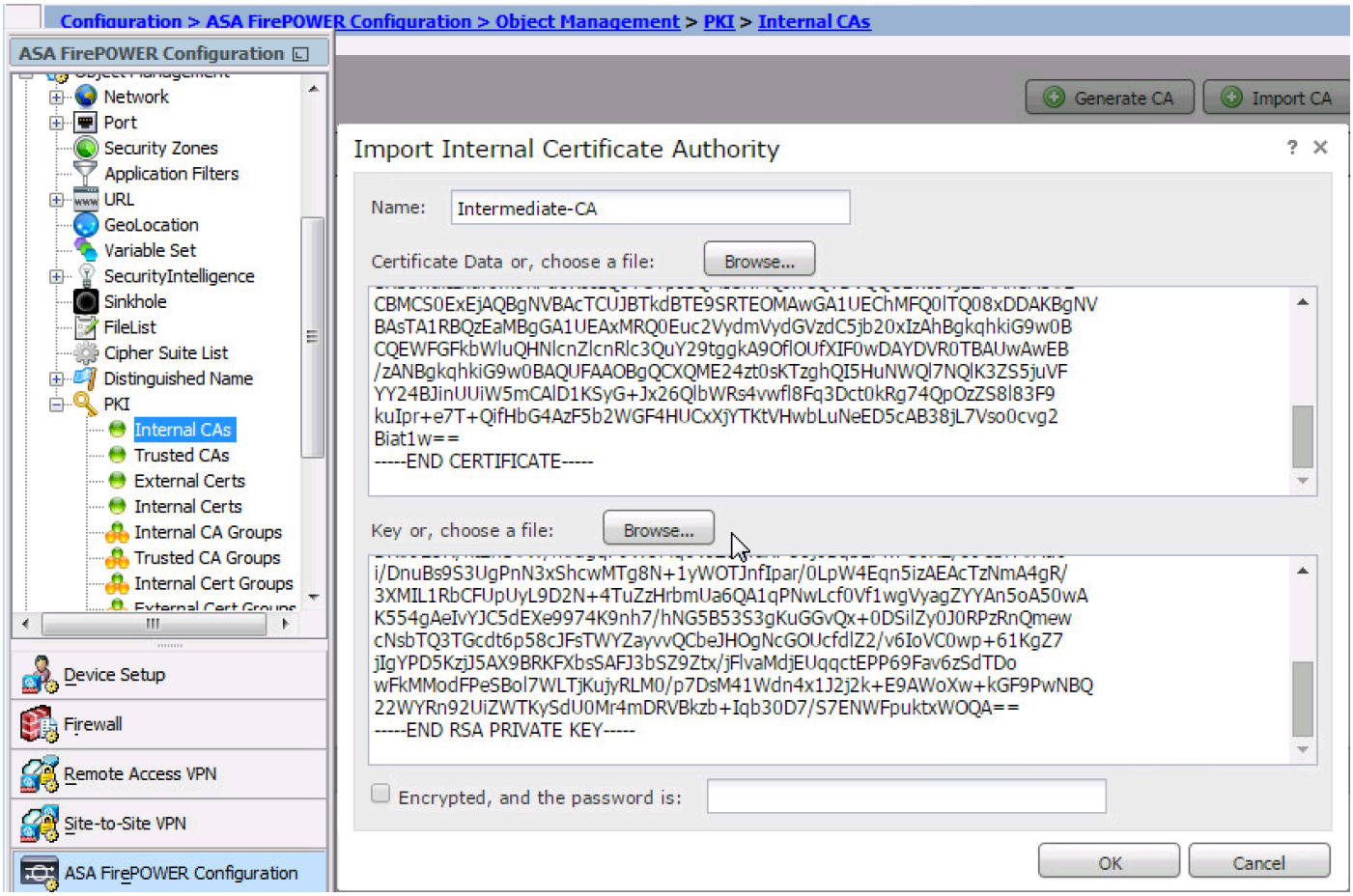
se comparte con el servidor de la CA para firmar.

Configuración del certificado de CA intermedio

Para configurar el Certificado CA intermedio firmado por otra CA de terceros, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** y haga clic en **Import CA.**

Especifique el nombre del certificado. Seleccione **examinar** y cargar el certificado desde la máquina local o copie y pegue el contenido del certificado en la opción **Datos de certificado**. Para especificar la clave privada del certificado, navegue por el archivo de claves o copie y pegue la clave en la opción **Key**.

Si la clave está cifrada, active la casilla de verificación **Encrypted** y especifique la contraseña. Haga clic en **Aceptar** para guardar el contenido del certificado, como se muestra en la imagen:



Paso 2. Configure la política SSL.

La política SSL define la acción de descifrado e identifica el tráfico en el que se aplica el método de descifrado de renuncia. Configure las distintas reglas SSL en función de los requisitos empresariales y la política de seguridad de la organización.

Para configurar la política SSL, navegue hasta **Configurar > ASA FirePOWER Configuration > Políticas > SSL** y haga clic en **Agregar regla**.

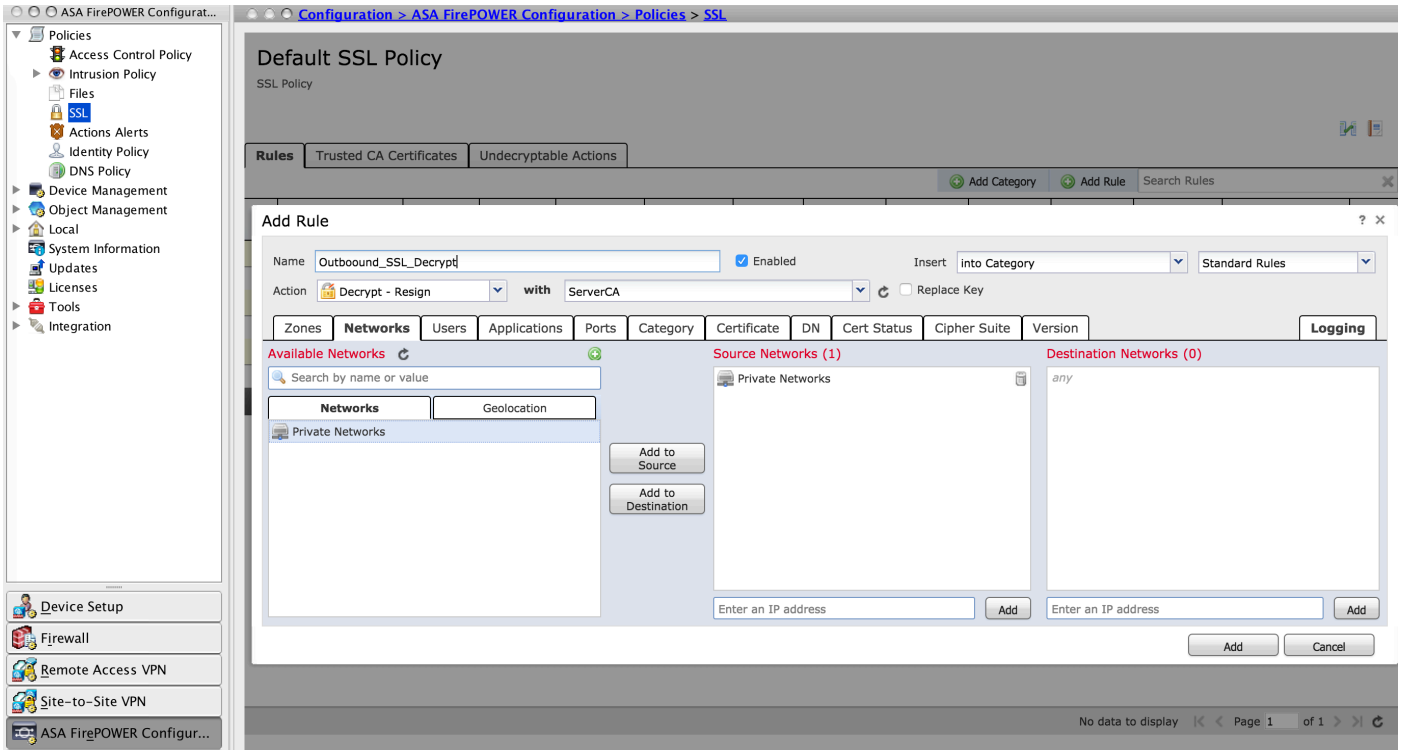
Nombre: Especifique el nombre de la regla.

Acción: Especifique la acción como **Descifrar - Renunciar** y elija el certificado de CA de la lista

desplegable que se configuró en el paso anterior.

Defina las condiciones en la regla para que coincidan con el tráfico, ya que hay varias opciones (zona, red, usuarios, etc.), especificadas para definir el tráfico que se debe descifrar.

Para generar los eventos de descifrado SSL, habilite la opción **registro** de registro, como se muestra en la imagen:



Haga clic en **Agregar** para agregar la regla SSL.

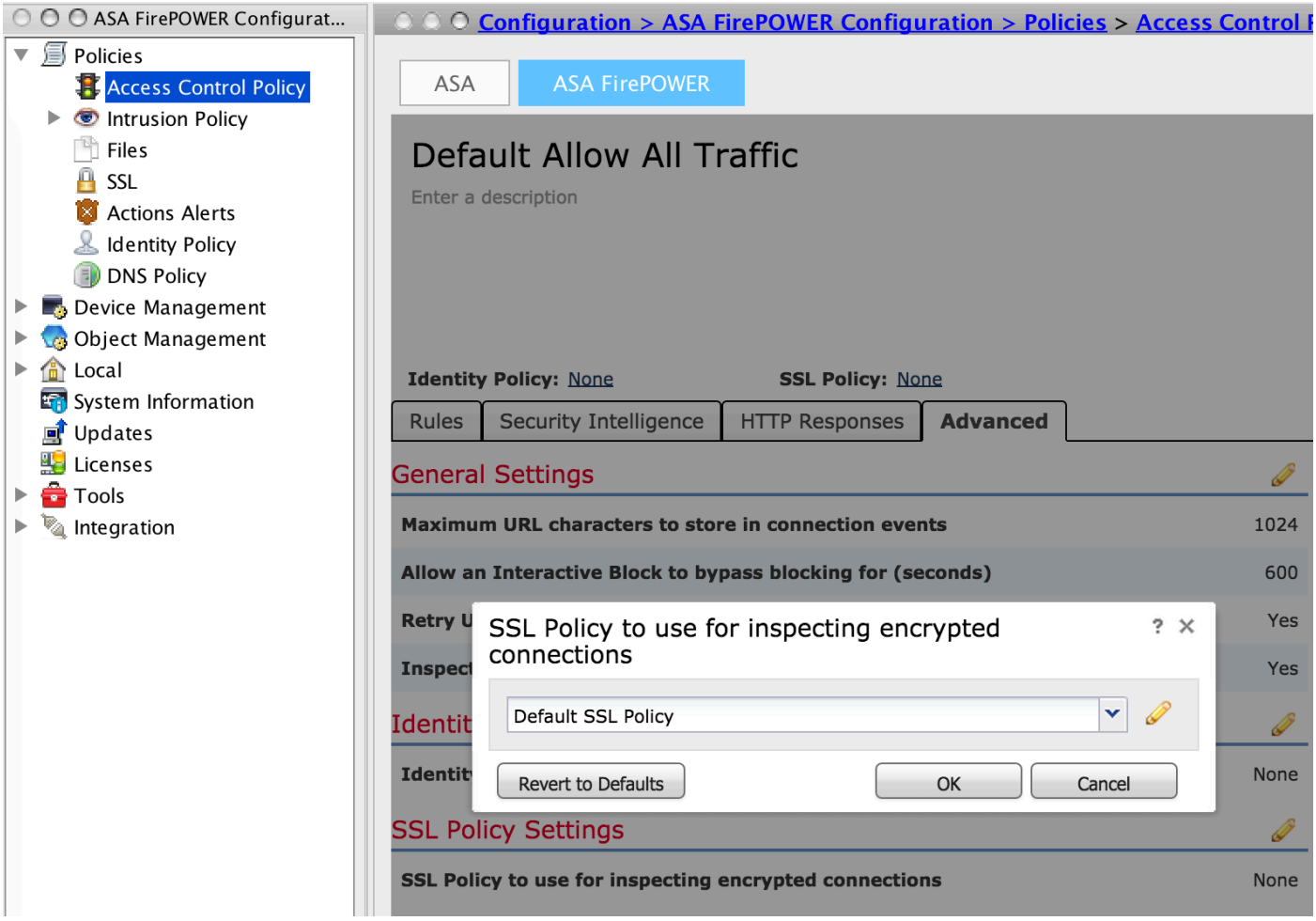
Haga clic en **Store ASA Firepower Changes** para guardar la configuración de la política SSL.

Paso 3. Configuración de la política de control de acceso

Una vez que configure la política SSL con las reglas adecuadas, debe especificar la política SSL en el Control de acceso para implementar los cambios.

Para configurar la política de control de acceso, navegue hasta **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Haga clic en **Ninguno** de la **política SSL** o navegue hasta **Avanzado > Configuración de la política SSL.** Especifique la política SSL en la lista desplegable y haga clic en **Aceptar** para guardarla, como se muestra en la imagen:



Haga clic **Almacenar cambios en el firewall ASA** para guardar la configuración de la política SSL.

Debe implementar la política de control de acceso en el sensor. Antes de aplicar la política, hay una indicación de que la **Política de control de acceso está desactualizada** en el módulo. Para implementar los cambios en el sensor, haga clic en **Implementar** y seleccione la **opción Implementar cambios de FirePOWER.** Verifique los cambios realizados y haga clic en **Implementar.**

> **Nota:** En la versión 5.4.x, si necesita aplicar la política de acceso al sensor, haga clic en **Aplicar cambios de FirePOWER ASA.**

> **Nota:** Vaya a **Monitoring > ASA Firepower Monitoring > Task Status .** A continuación, se aplican los cambios de configuración para asegurarse de que la tarea se ha completado.

Descifrado SSL entrante (descifrado - conocido)

El método de descifrado SSL entrante (conocido por descifrado) se utiliza para descifrar el tráfico SSL entrante para el que ha configurado el certificado de servidor y la clave privada. Debe importar el certificado de servidor y la clave privada al módulo Firepower. Cuando el tráfico SSL llega al módulo Firepower, descifra el tráfico y realiza la inspección en el tráfico descifrado. Después de la inspección, el módulo Firepower vuelve a cifrar el tráfico y lo envía al servidor.

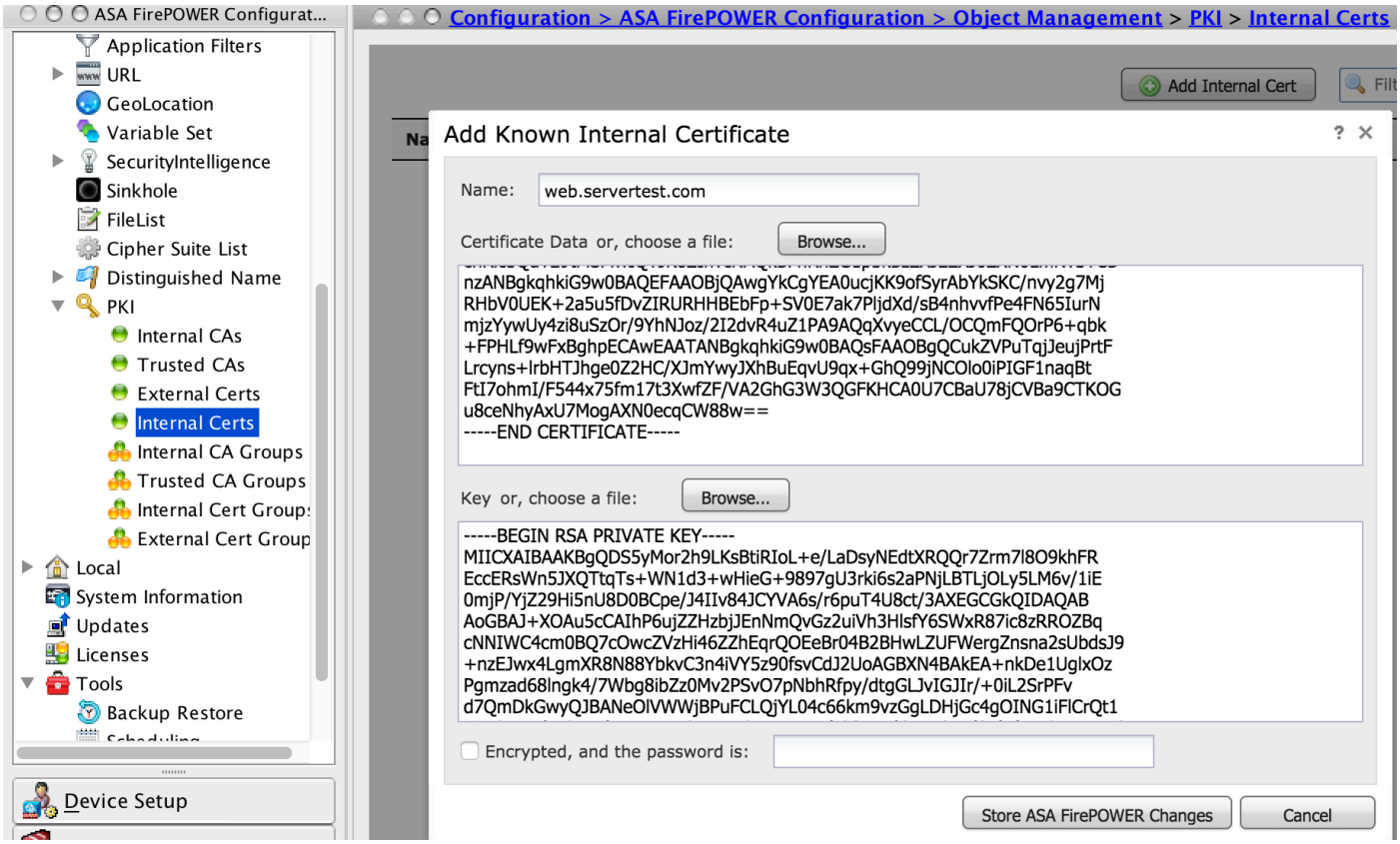
Estos son los cuatro pasos para configurar el Descifrado SSL saliente:

Paso 1. Importe el certificado y la clave del servidor.

Para importar el certificado y la clave del servidor, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal Certs** y haga clic en **Add Internal Cert** .

Como se muestra en la imagen, especifique el nombre del certificado. Seleccione **examinar** para seleccionar el certificado de la máquina local o copiar y pegar el contenido del certificado en los **datos del certificado**. Para especificar la clave privada del certificado, navegue por el archivo de clave o copie y pegue la clave en la **clave** de opción.

Si la clave está cifrada, active la casilla de verificación **Encrypted** y especifique la contraseña, como se muestra en la imagen:



Haga clic en **Store ASA FirePOWER Changes** para guardar el contenido del certificado.

Paso 2. Importe el certificado de CA (opcional).

Para el certificado de servidor firmado por el certificado de CA interna intermedia o raíz, debe importar la cadena interna de certificados de CA al módulo de firepower. Una vez realizada la importación, el módulo firepower puede validar el certificado del servidor.

Para importar el certificado de CA, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** y haga clic en **Add Trusted CA** para agregar el certificado de CA.

Paso 3. Configure la política SSL.

La política SSL define la acción y los detalles del servidor para los cuales desea configurar el método conocido de descifrado para descifrar el tráfico entrante. Si tiene varios servidores internos, configure varias reglas SSL basadas en diferentes servidores y el tráfico que manejan .

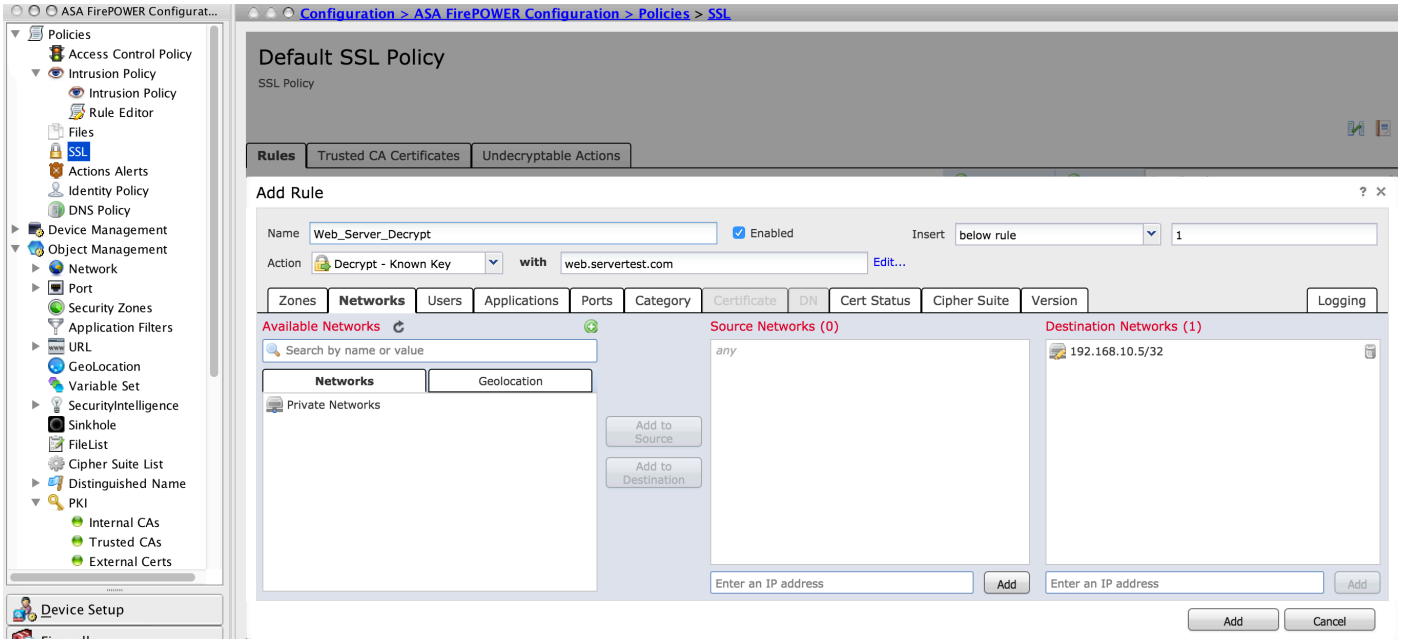
Para configurar la política SSL, navegue hasta **Configurar > Configuración de ASA FirePOWER > Políticas > SSL** y haga clic en **Agregar regla**.

Nombre: Especifique el nombre de la regla.

Acción: Especifique la acción como **Descifrar - conocido** y elija el certificado CA de la lista desplegable que se configura en el paso anterior.

Defina la condición para que coincida con estas reglas, ya que hay varias opciones (red, aplicación, puertos, etc.) especificadas para definir el tráfico interesante del servidor para el que desea habilitar el descifrado SSL. Especifique la CA interna en las **CAs de confianza seleccionadas en la** ficha **de certificado de CA de confianza.**

Para generar los eventos de descifrado SSL, habilite la opción **logging** logingat.



Haga clic en **Agregar** para agregar la regla SSL.

Y luego haga clic en **Store ASA Firepower Changes** para guardar la configuración de la política SSL.

Paso 4. Configure la política de control de acceso.

Una vez que configure la política SSL con las reglas adecuadas, debe especificar la política SSL en el Control de acceso para implementar los cambios.

Para configurar la política de control de acceso, navegue hasta **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Haga clic en la opción **None** junto a **SSL Policy** o navegue hasta **Advanced > SSL Policy Setting**, especifique la política SSL en la lista desplegable y haga clic en **OK** para guardarla.

Haga clic **Almacenar cambios en el firewall ASA** para guardar la configuración de la política SSL.

Debe implementar la política de control de acceso. Antes de aplicar la política, puede ver una indicación de Directiva de control de acceso desactualizada en el módulo. Para implementar los cambios en el sensor, haga clic en **Implementar** y elija la **opción Implementar cambios de FirePOWER.** Verifique los cambios realizados y haga clic en **Implementar** en la ventana emergente.

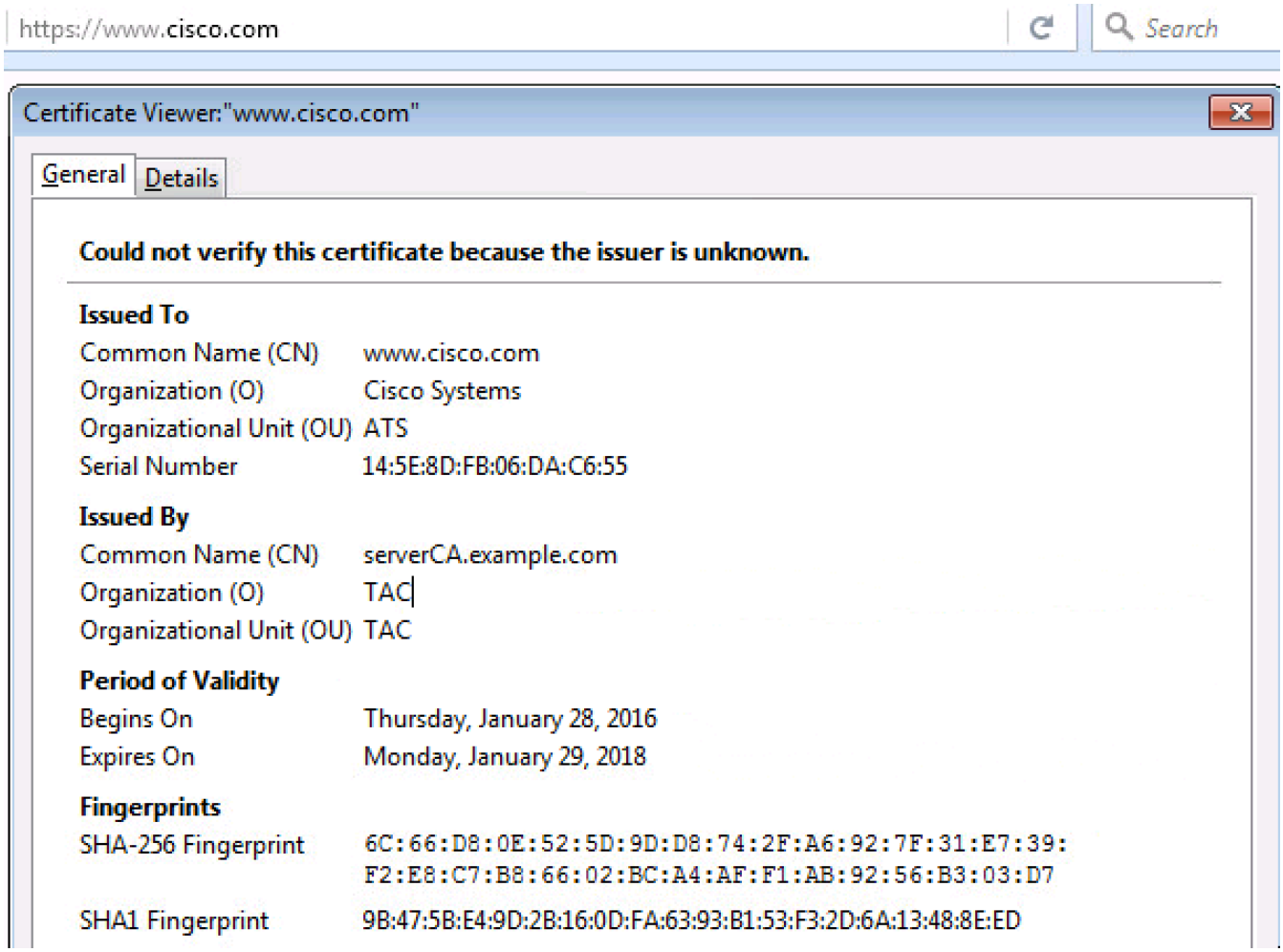
> **Nota:** En la versión 5.4.x, si necesita aplicar la política de acceso al sensor, haga clic en **Aplicar cambios de ASA FirePOWER**.

> **Nota:** Vaya a **Monitoring > ASA Firepower Monitoring > Task Status .** A continuación, se aplican los cambios de configuración para asegurarse de que la tarea se ha completado.

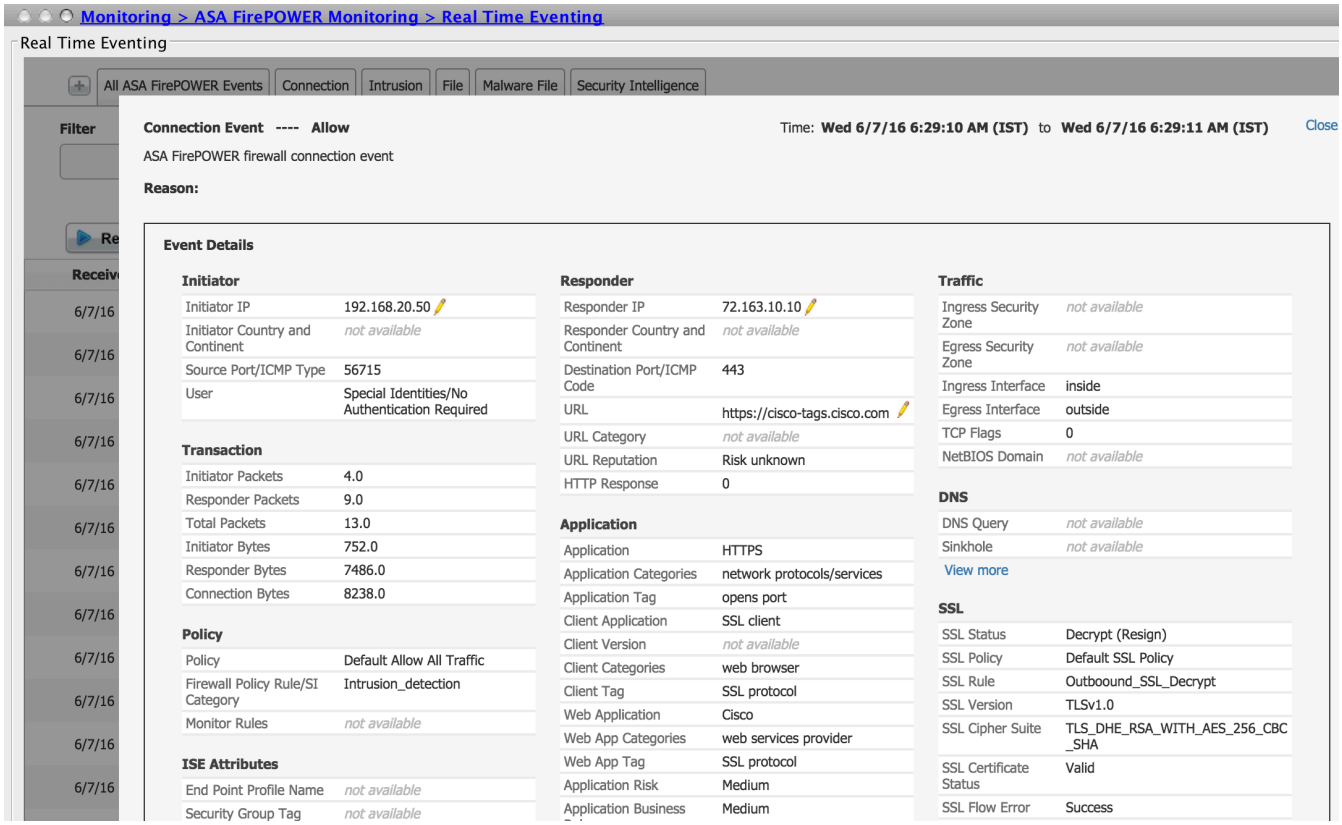
Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

- Para la conexión SSL saliente, una vez que navega por un sitio web público de SSL desde la red interna, el sistema envía un mensaje de error del certificado. Verifique el contenido del certificado y verifique la información de CA. Aparece el certificado de CA interno que configuró en el módulo Firepower. Acepte el mensaje de error para examinar el certificado SSL. Para evitar el mensaje de error, agregue el certificado de CA a la lista de CA de confianza de su navegador.



- Verifique los eventos de conexión para verificar qué política SSL y regla SSL están en el tráfico. Vaya a **Monitoring > ASA FirePOWER Monitoring > Real-Time Event.**Seleccione un evento y haga clic en **Ver detalles**. Verifique las estadísticas de descifrado SSL.



- Asegúrese de que la implementación de la política de control de acceso se complete correctamente.
- Asegúrese de que la política SSL está incluida en la política de control de acceso.
- Asegúrese de que la política SSL contiene las reglas adecuadas para la dirección entrante y saliente.
- Asegúrese de que las reglas SSL contengan la condición adecuada para definir el tráfico interesante.
- Supervise los eventos de conexión para verificar la política SSL y la regla SSL.
- Verifique el estado de descifrado SSL.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems