# Configure a descriptografia SSL no módulo FirePOWER usando ASDM (On-Box Management, gerenciamento integrado)

## Contents



## Introduction

Este documento descreve a configuração da descriptografia SSL (Secure Sockets Layer) no módulo FirePOWER usando ASDM (On-Box Management, gerenciamento integrado).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conhecimento do dispositivo FirePOWER
- Conhecimento do protocolo HTTPS/SSL

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X ) executando a versão de software 6.0.0 e superior
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) executando a versão de software 6.0.0 e superior

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.

> **Note**: Verifique se o FirePOWER Module tem uma licença **Protect** para configurar essa funcionalidade. Para verificar a licença, navegue para **Configuration > ASA FirePOWER Configuration > License**.

## Informações de Apoio

O módulo Firepower descriptografa e inspeciona as conexões SSL de entrada e saída que são redirecionadas para ele. Depois que o tráfego é descriptografado, aplicativos em túnel, como bate-papo no facebook etc., são detectados e controlados. Os dados descriptografados são inspecionados para verificar se há ameaças, filtragem de URL, bloqueio de arquivos ou dados mal-intencionados.

### Descriptografia SSL de saída

O módulo firepower atua como o proxy de encaminhamento para conexões SSL de saída interceptando solicitações SSL de saída e regerando um certificado para o site que o usuário deseja visitar. A autoridade emissora (AC) é o certificado com assinatura automática do Firepower. Se o certificado do firepower não fizer parte de uma hierarquia existente ou se não for adicionado ao cache do navegador de um cliente, o cliente receberá um aviso enquanto navega para um site seguro. O método Decrypt-Resignmethod é usado para executar a descriptografia de SSL de saída.

### Descriptografia SSL de entrada

No caso de tráfego de entrada para um servidor Web interno ou dispositivo, o administrador importa uma cópia do certificado do servidor protegido e a chave. Quando o certificado do servidor SSL é carregado no módulo firepower e a política de descriptografia SSL é configurada para o tráfego de entrada, o dispositivo então descriptografa e inspeciona o tráfego à medida que ele encaminha o tráfego. O módulo, então, detecta conteúdo mal-intencionado, ameaças e malware fluindo por esse canal seguro. Além disso, o método Disrypt-Known Keymethod é usado para executar a descriptografia SSL de entrada.

## Configuração para descriptografia de SSL

Há dois métodos de descriptografia de tráfego SSL.

- Descriptografar - Reiniciar para tráfego SSL de saída
- Descriptografar - conhecido para tráfego SSL de entrada

## Descriptografia SSL de saída (Descriptografia - Reassinatura)

O módulo Firepower atua como MITM (man-in-the-middle) em qualquer negociação SSL para servidores SSL públicos. Ele rende o certificado do servidor público por um certificado CA intermediário que está configurado no módulo firepower.

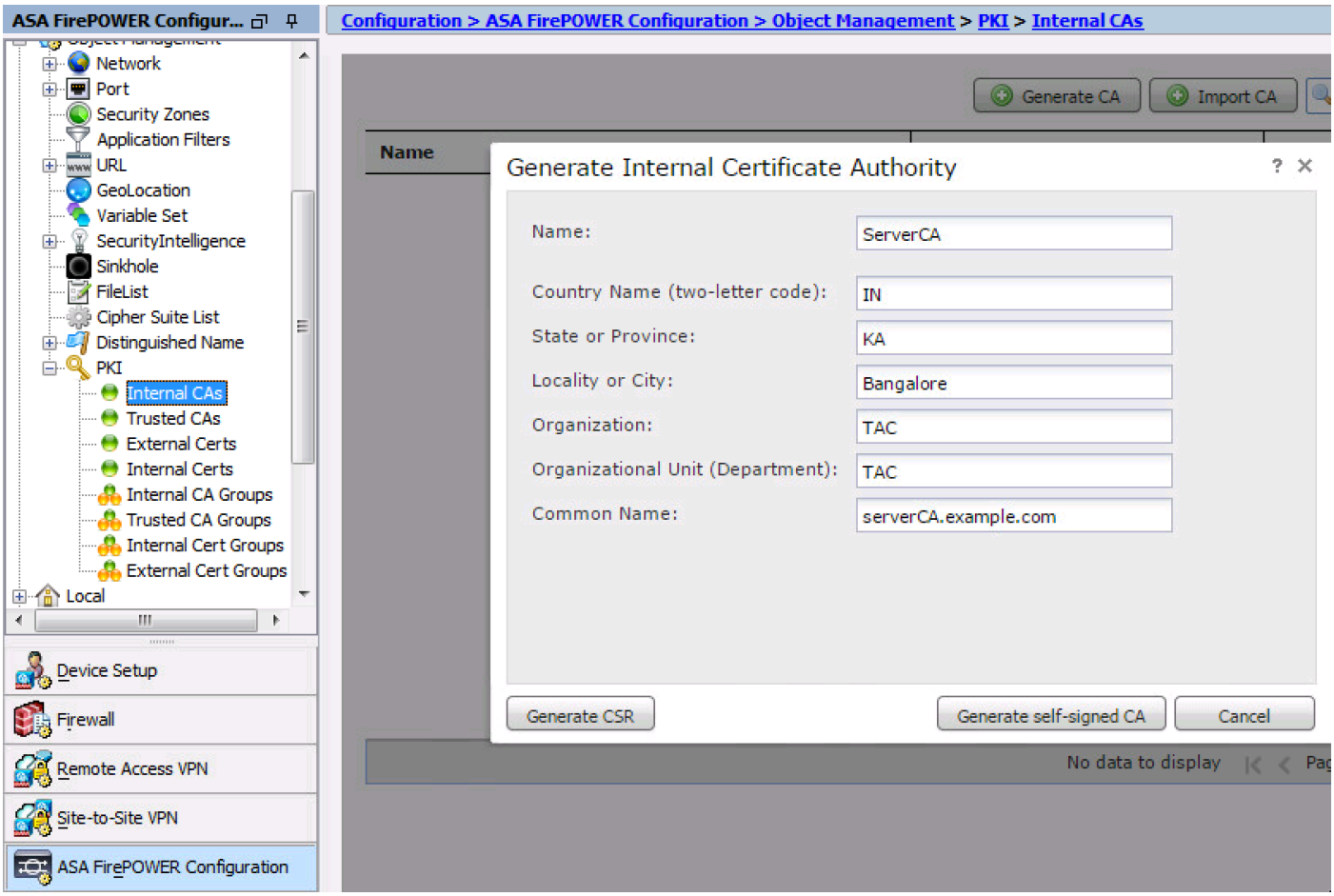
Estas são as três etapas para configurar a Descriptografia SSL de saída.

### Etapa 1. Configure o certificado CA.

Configure um certificado autoassinado ou um certificado CA confiável intermediário para a renúncia do certificado.

### Configurar o certificado CA com assinatura automática

Para configurar o certificado CA com assinatura automática, navegue para **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** e clique em **Generate CA**. O sistema solicita os detalhes do certificado CA. Como mostrado na imagem, preencha os detalhes conforme o seu requisito.




Clique em **Gerar CA autoassinado** para gerar o certificado CA interno. Em seguida, clique em **Gerar CSR** para gerar a solicitação de assinatura de certificado que é compartilhada com o

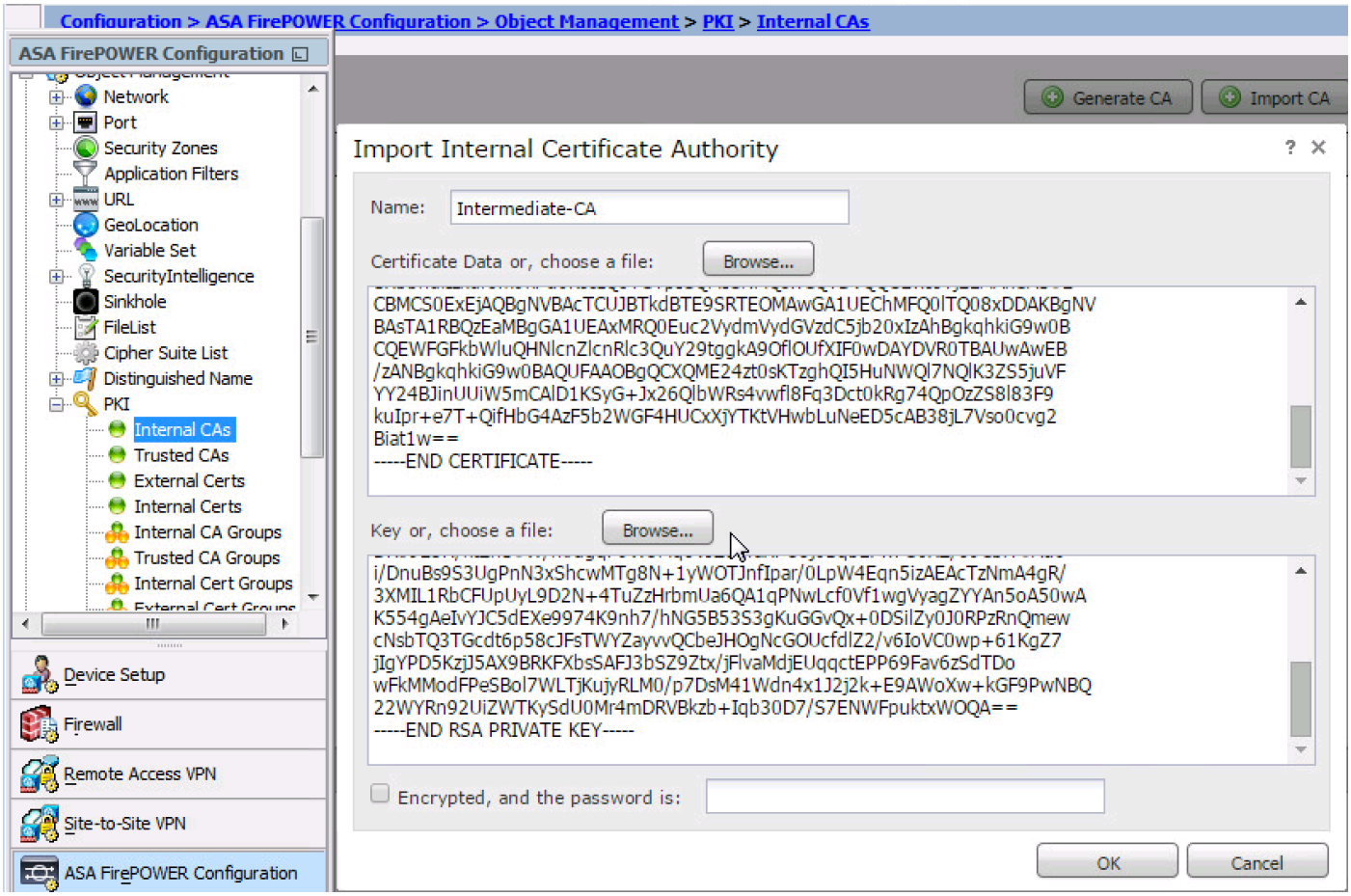
servidor CA para assinar.

### Configurar o certificado CA intermediário

Para configurar o Certificado CA intermediário assinado por outra CA de terceiros, navegue para **Configuração > Configuração do ASA Firepower > Gerenciamento de objetos > PKI > CAs internas** e clique em **Importar CA**.

Especifique o nome do certificado. Selecione **Procurar** e carregar o certificado da máquina local ou copie-cole o conteúdo do certificado na opção **Dados do certificado**. Para especificar a chave privada do certificado, navegue no arquivo de chave ou copie-cole a chave na opção **Key**.

Se a chave estiver criptografada, ative a caixa de seleção **Criptografada** e especifique a senha. Clique em **OK** para salvar o conteúdo do certificado, como mostrado na imagem:




### Etapa 2. Configure a política SSL.

A política SSL define a ação de descriptografia e identifica o tráfego no qual o método de descriptografia é aplicado. Configure as várias regras SSL com base nos requisitos de negócios e na política de segurança da empresa.

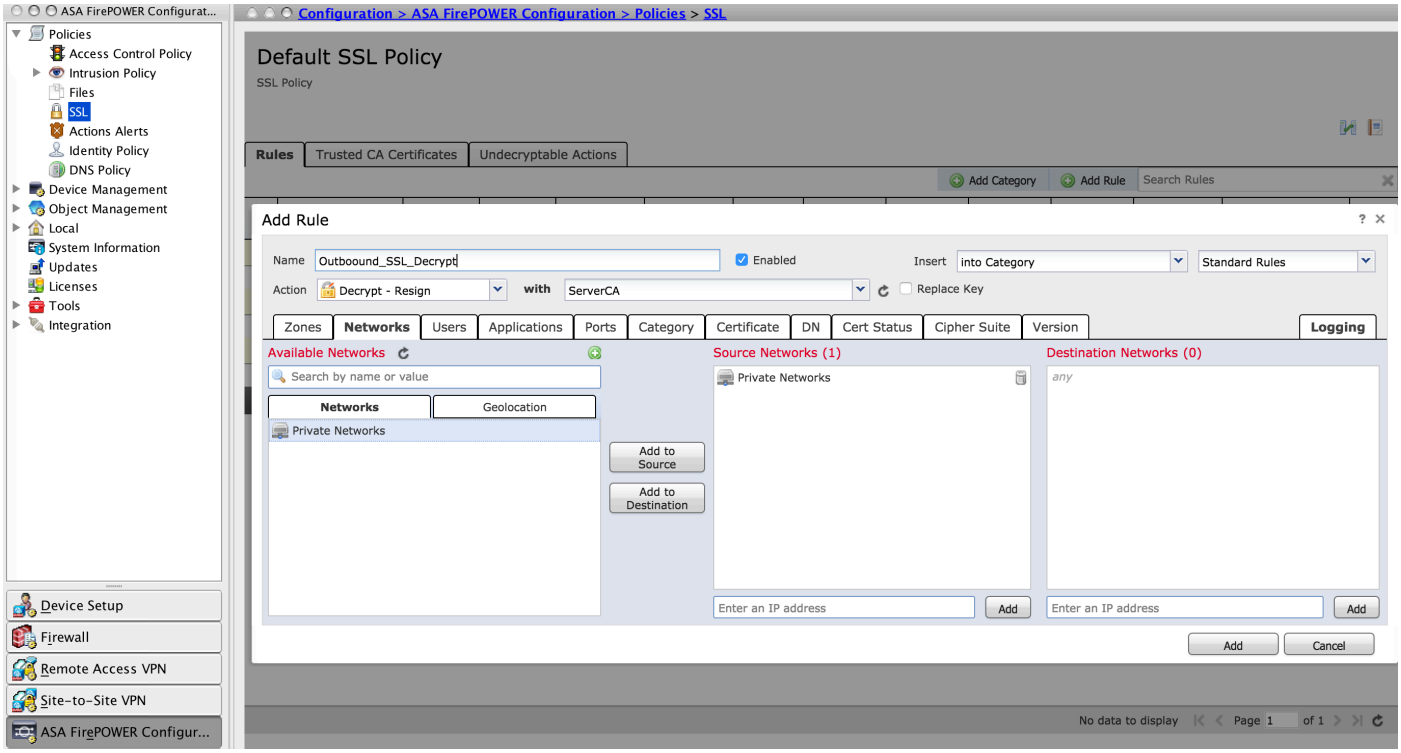
Para configurar a política SSL, navegue para **Configurar > Configuração do ASA FirePOWER > Políticas > SSL** e clique em **Adicionar regra**.

**Nome:** especifique o nome da regra.

**Ação:** Especifique a ação como **Descriptografar - Resign** e escolha o certificado CA na lista suspensa configurada na etapa anterior.

Defina as condições na regra para corresponder o tráfego, pois há várias opções (zona, rede, usuários, etc.), especificadas para definir o tráfego que precisa ser descriptografado.

Para gerar os eventos de descriptografia SSL, ative a opção de **registro** de log, como mostrado na imagem:




Clique em **Adicionar** para adicionar a regra SSL.

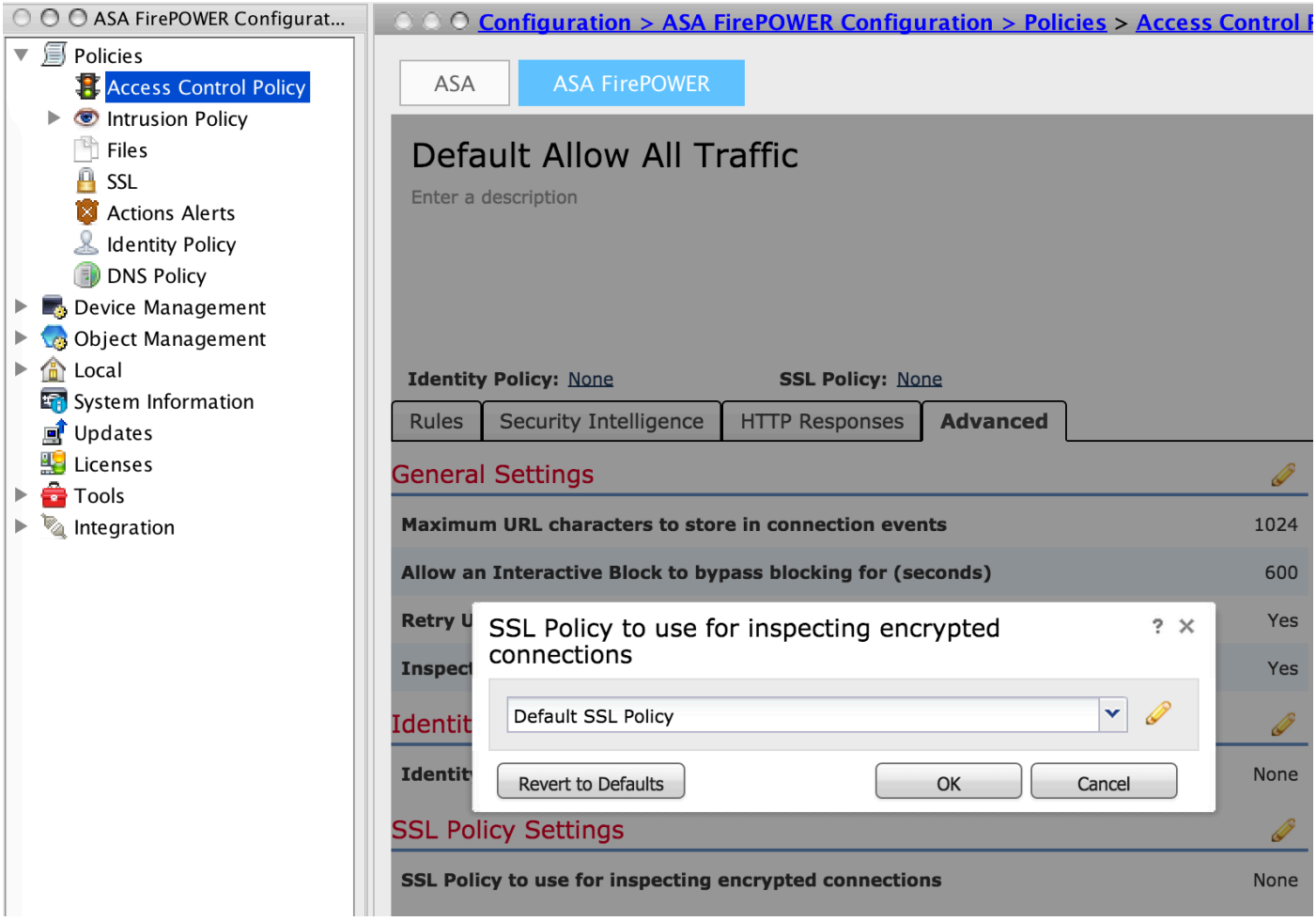
Clique em **Store ASA Firepower Changes** para salvar a configuração da política SSL.

## Etapa 3. Configurar a política de controle de acesso

Depois de configurar a política SSL com regras apropriadas, você deve especificar a política SSL no Controle de Acesso para implementar as alterações.

Para configurar a política de controle de acesso, navegue para **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Clique em **None** of the **SSL Policy** ou navegue para **Advanced > SSL Policy Setting.** Especifique a política SSL na lista suspensa e clique em **OK** para salvá-la, como mostrado na imagem:




Clique em **Armazene as alterações do ASA Firepower** para salvar a configuração da política SSL.

Você deve implantar a política de controle de acesso no sensor. Antes de aplicar a política, há uma indicação de que a **Política de controle de acesso está desatualizada** no módulo. Para implantar as alterações no sensor, clique em **Implantar** e selecione a **opção Implantar alterações do FirePOWER.** Verifique as alterações feitas e clique em **Implantar.**

> **Note**: Na versão 5.4.x, se precisar aplicar a política de acesso ao sensor, clique em **Aplicar alterações do ASA FirePOWER.**

> **Note**: Navegue até **Monitoring > ASA Firepower Monitoring > Task Status.** Em seguida, você se inscreve para alterações de configuração para garantir que a tarefa seja concluída.

## Descriptografia SSL de entrada (descriptografar - conhecido)

O método Descriptografia SSL de entrada (Descriptografia conhecida) é usado para descriptografar o tráfego SSL de entrada para o qual você configurou o certificado do servidor e a chave privada. Você precisa importar o certificado do servidor e a chave privada para o módulo Firepower. Quando o tráfego SSL atinge o módulo Firepower, ele descriptografa o tráfego e realiza a inspeção no tráfego descriptografado. Após a inspeção, o módulo Firepower criptografa novamente o tráfego e o envia ao servidor.

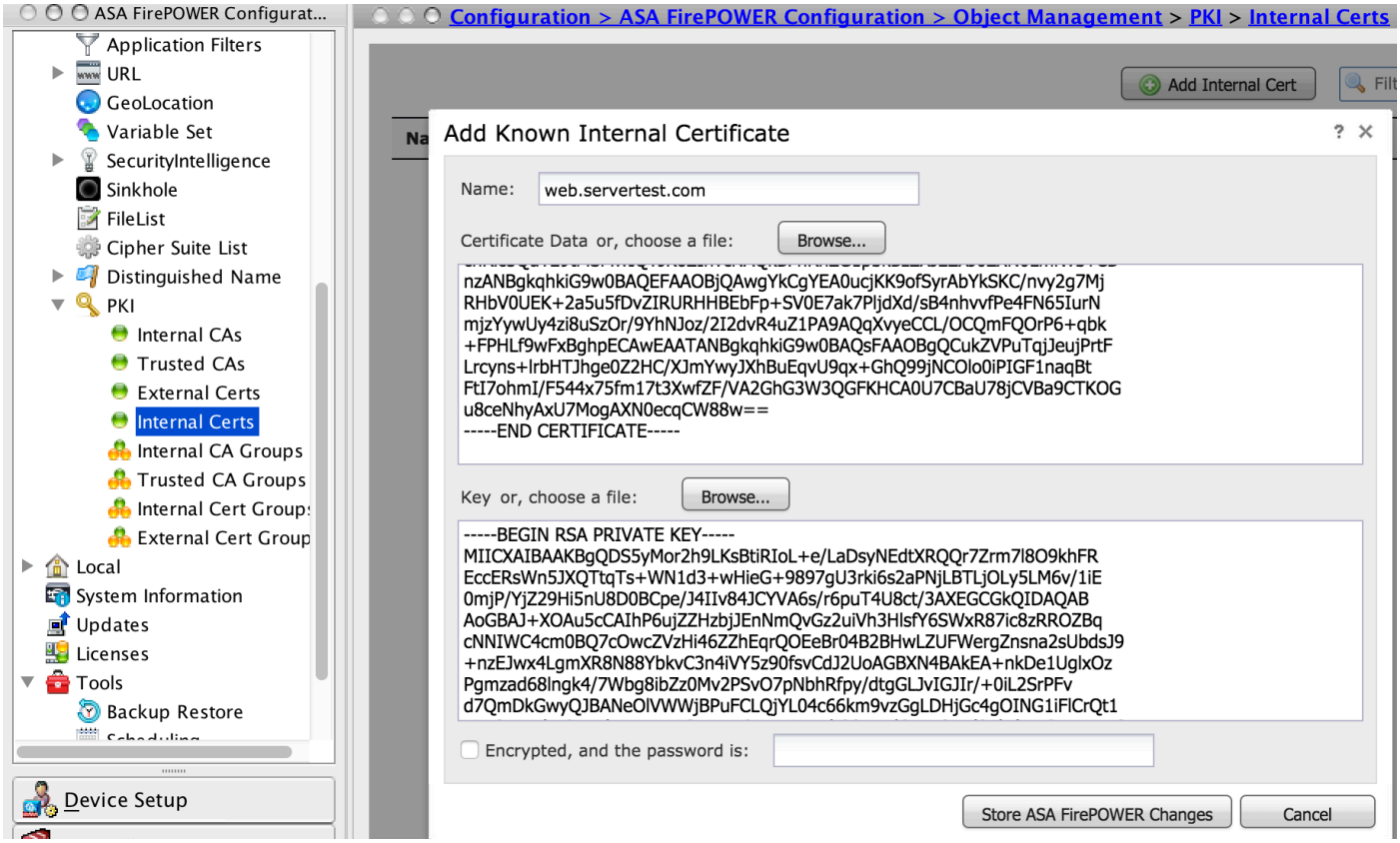
Estas são as quatro etapas para configurar a Descriptografia SSL de saída:

### Etapa 1. Importar o certificado e a chave do servidor.

Para importar o Server Certificate and Key (Certificado e chave do servidor), navegue para **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal Certs (Configuração > Configuração do ASA Firepower > Gerenciamento de objetos > PKI > Certs internos)** e clique em **Add Internal Cert (Adicionar certificado interno)**.

Como mostrado na imagem, especifique o nome do certificado. Selecione **Procurar** para selecionar o certificado da máquina local ou copie-cole o conteúdo do certificado nos **Dados do certificado**. Para especificar a chave privada do certificado, navegue no arquivo de chave ou copie-cole a chave na opção **Key**.

Se a chave estiver criptografada, ative a caixa de seleção **Criptografada** e especifique a senha, como mostrado na imagem:




Clique em **Store ASA FirePOWER Changes** para salvar o conteúdo do certificado.

### Etapa 2. Importar o certificado CA (opcional).

Para o certificado do servidor assinado pelo certificado CA interno intermediário ou raiz, é necessário importar a cadeia interna de certificados CA para o módulo firepower. Após a importação ser realizada, o módulo firepower pode validar o certificado do servidor.

Para importar o certificado CA, navegue para **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** e clique em **Add Trusted CA** para adicionar o certificado CA.

### Etapa 3. Configure a política SSL.

A política SSL define a ação e os detalhes do servidor para os quais você deseja configurar o método Descriptografar conhecido para descriptografar o tráfego de entrada. Se você tiver vários servidores internos, configure várias regras SSL com base em diferentes servidores e no tráfego que eles manipulam .

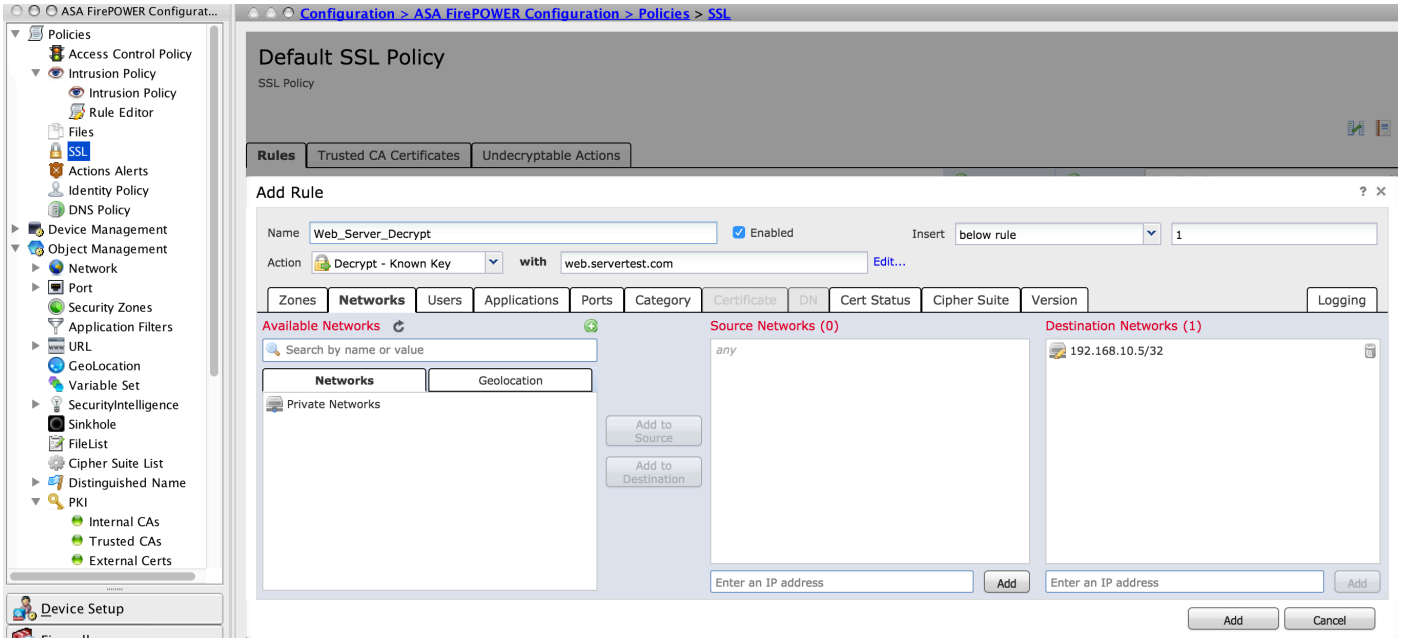
Para configurar a política SSL, navegue para **Configurar > Configuração do ASA FirePOWER > Políticas > SSL** e clique em **Adicionar regra**.

**Nome:** especifique o nome da regra.

**Ação:** Especifique a ação como **Descriptografar - conhecido** e escolha o certificado CA na lista suspensa configurada na etapa anterior.

Defina a condição para corresponder a essas regras, pois há várias opções (rede, aplicação, portas etc.) especificadas para definir o tráfego interessante do servidor para o qual você deseja habilitar a descriptografia SSL. Especifique a AC interna em **CAs confiáveis selecionadas na** guia **de certificado CA confiável.**

Para gerar os eventos de descriptografia de SSL, ative a opção de **registro** de log **de** log.




Clique em **Adicionar** para adicionar a regra SSL.

Em seguida, clique em **Store ASA Firepower Changes** para salvar a configuração da política SSL.

## Etapa 4. Configure a política de controle de acesso.

Depois de configurar a política SSL com regras apropriadas, você deve especificar a política SSL no Controle de Acesso para implementar as alterações.

Para configurar a política de controle de acesso, navegue para **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Clique na opção **Nenhum** ao lado de **Política SSL** ou navegue para **Avançado > Configuração de política SSL**, especifique a política SSL na lista suspensa e clique em **OK** para salvá-la.

Clique em **Armazene as alterações do ASA Firepower** para salvar a configuração da política SSL.

Você deve implantar a política de controle de acesso. Antes de aplicar a política, você pode ver uma indicação Política de controle de acesso desatualizada no módulo. Para implantar as alterações no sensor, clique em **Implantar** e escolha a **opção Implantar alterações do FirePOWER.** Verifique as alterações feitas e clique em **Implantar** na janela pop-up.

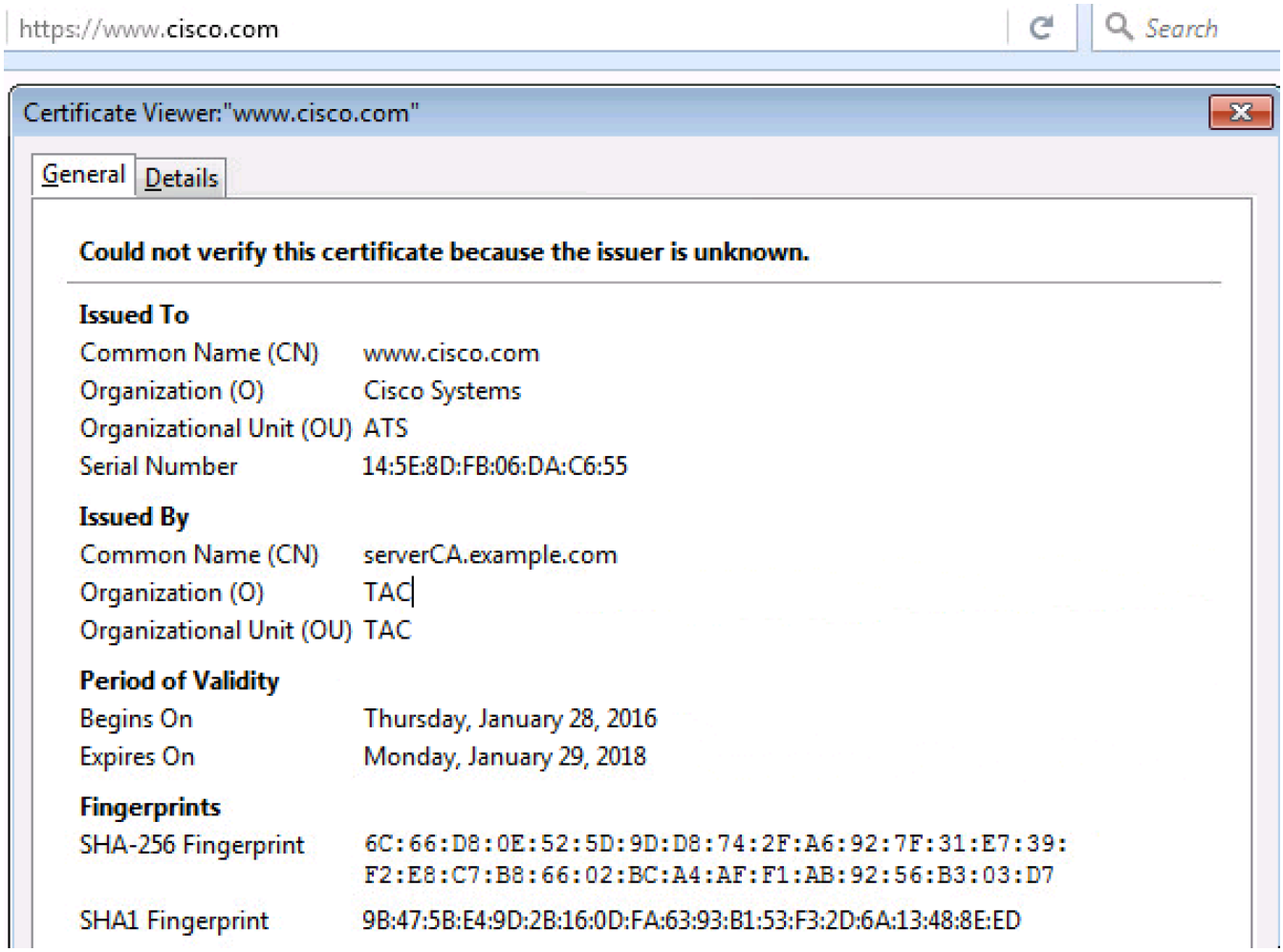
> **Note**: Na versão 5.4.x, se precisar aplicar a política de acesso ao sensor, clique em **Aplicar alterações do ASA FirePOWER**.

> **Note**: Navegue até **Monitoring > ASA Firepower Monitoring > Task Status.** Em seguida, você se inscreve para alterações de configuração para garantir que a tarefa seja concluída.

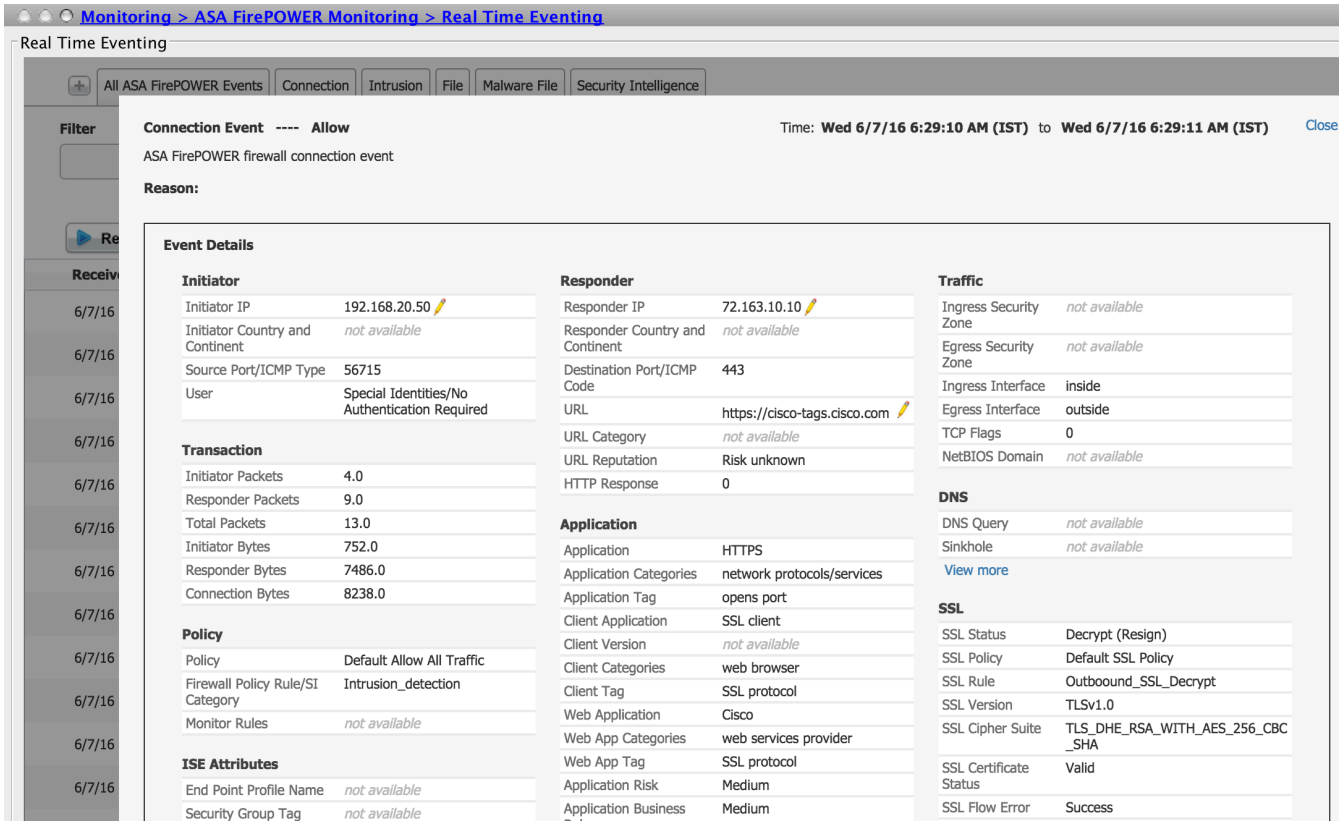
# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Para a conexão SSL de saída, quando você navega em um site SSL público da rede interna, o sistema solicita uma mensagem de erro do certificado. Verifique o conteúdo do certificado e verifique as informações da AC. O certificado CA interno configurado no módulo Firepower é exibido. Aceite a mensagem de erro para navegar no certificado SSL. Para evitar a mensagem de erro, adicione o certificado CA à lista de CAs confiáveis do navegador.




- Verifique os eventos de conexão para verificar qual política SSL e regra SSL são atingidas pelo tráfego. Navegue até **Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing.**Selecione um evento e clique em **View Details**. Verifique as estatísticas de descriptografia de SSL.




- Certifique-se de que a implantação da política de controle de acesso seja concluída com êxito.
- Certifique-se de que a política SSL esteja incluída na política de controle de acesso.
- Assegure-se de que a política SSL contenha regras apropriadas para as direções de Entrada e Saída.
- Certifique-se de que as regras SSL contêm a condição adequada para definir o tráfego interessante.
- Monitorar os eventos de ligação para verificar a política SSL e a regra SSL.
- Verifique o status da descriptografia SSL.

# Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

# Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems