

# Configuração de uma política de inspeção SSL no Cisco FireSIGHT System

## Contents

[Introduction](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Configurações](#)

[1. Descriptografar e reassinar](#)

[Opção 1: Usar o FireSIGHT Center como uma autoridade de certificação \(CA\) raiz](#)

[Opção 2: Faça com que uma AC interna assine seu certificado](#)

[Opção 3: Importar um certificado e uma chave CA](#)

[2. Descriptografar com chave conhecida](#)

[Importando certificado conhecido \(alternativa para descriptografar e reassinar\)](#)

[Configurações adicionais](#)

[Verificação](#)

[Descriptografar - Reassinar](#)

[Descriptografar - Certificado conhecido](#)

[Troubleshooting](#)

[Problema 1: Alguns sites podem não ser carregados no navegador do Chrome](#)

[Problema 2: Obtendo um aviso/erro não confiável em alguns navegadores](#)

[Referências](#)

[Discussões relacionadas da comunidade de suporte da Cisco](#)

## Introduction

O recurso de inspeção SSL permite bloquear o tráfego criptografado sem inspecioná-lo ou inspecionar o tráfego criptografado ou descriptografado com controle de acesso. Este documento descreve as etapas de configuração para configurar uma política de inspeção SSL no Cisco FireSIGHT System.

## Prerequisites

### Componentes Utilizados

- Cisco FireSIGHT Management Center
- Dispositivos Cisco Firepower 7000 ou 8000
- Software versão 5.4.1 ou 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.

**aviso:** Se você aplicar uma política de inspeção SSL no dispositivo gerenciado, ela poderá afetar o desempenho da rede.

## Configurações

Você pode configurar uma política de inspeção SSL para descriptografar o tráfego das seguintes maneiras:

### 1. Descriptografar e reinar:

- Opção 1: Usar o FireSIGHT Center como uma autoridade de certificação raiz (CA) ou
- Opção 2: Fazer com que uma AC interna assine seu certificado ou
- Opção 3: Importar um certificado e uma chave CA

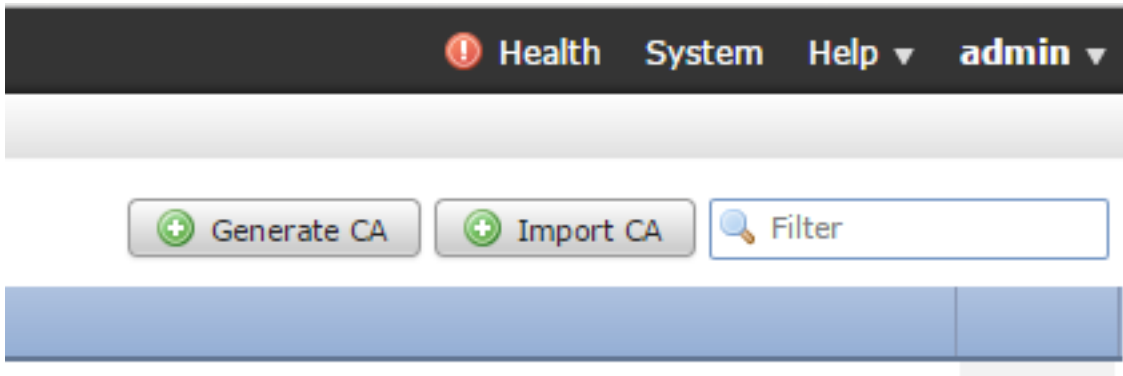
### 2. Descriptografar com certificado conhecido:

- Faça login no FireSIGHT Management Center e, em seguida, navegue até **Objects**.
- Na página **Objetos**, expanda o **PKI** e selecione **CAs internas**.

## 1. Descriptografar e reassinar

Opção 1: Usar o FireSIGHT Center como uma autoridade de certificação (CA) raiz

### I. Clique em **Gerar CA**.



### ii. Preencha as informações relevantes

**Generate Internal Certificate Authority** ? X

Name:

Country Name (two-letter code):

State or Province:

Locality or City:

Organization:

Organizational Unit (Department):

Common Name:

iii. Clique em **Gerar CA autoassinado**.

**Opção 2: Faça com que uma AC interna assine seu certificado**

I. Clique em **Gerar CA**.

! Health System Help admin

ii. Preencha as informações relevantes.

**Generate Internal Certificate Authority** ? X

Name: InternalCA

Country Name (two-letter code): US

State or Province: MD

Locality or City: Columbia

Organization: Sourcefire

Organizational Unit (Department): TAC

Common Name: InternalCA

Generate CSR      Generate self-signed CA      Cancel

**Note:** Talvez seja necessário entrar em contato com o administrador da CA para determinar se ele tem um modelo para a solicitação de assinatura.

iii. Copie o certificado inteiro incluindo —BEGIN CERTIFICATE REQUEST— e —END CERTIFICATE REQUEST— e salve-o em um arquivo de texto com a extensão .req.

**Generate Internal Certificate Authority** ? X

Subject:

- Common Name: InternalCA
- Organization: Sourcefire
- Organization Unit: TAC

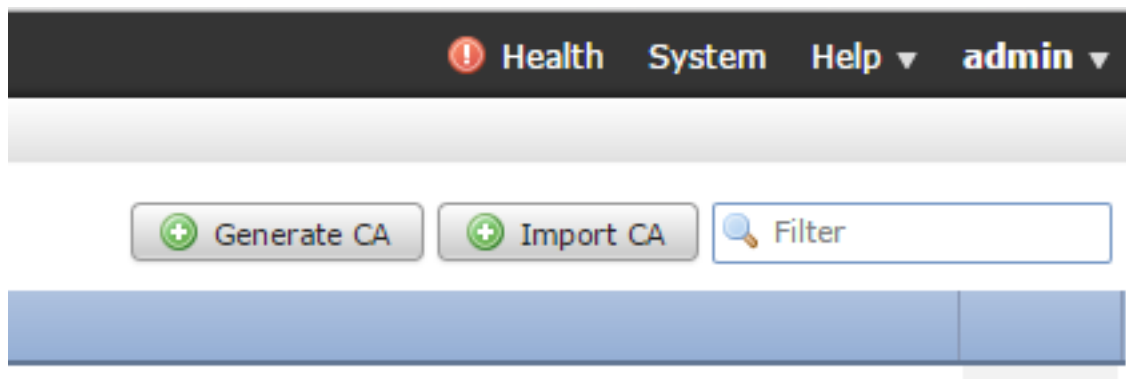
CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB4zCCAQAwCAQAwZTELMakGA1UEBhMCVVMxMzA1BjBjNVBBAgMAK1EMREwDwYDVQQH
DAhDb2x1bWJpYTETMBEGA1UECgwKU291cmNlZmlyZTEMMAAoGA1UECwwDVFEFMRMw
EQYDVQQDDApJbnRlcm5hbENBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5
XTQjxBMnyPNmGTVAXrqG7LhXPXzZ7lgF6MfKxwLh8rVwoejHhwbAUro8ju/R3Ig7
Ty1cwNpr4Bnbk9kDS9jDYqftFJzOu8UJ6wKcmxg2IUx80r9y1SKzSiRprJdSBaRc
LSHey3dI0K5SXNktTb8v8V97RYAfX4VDR7iVDKwxzQIDAQABoD4wPAYJKoZIhvcN
AQkOMs8wLTAdBgNVHQ4EFgQUIh/JeYfJm2itIE3spLdPqzpTXGkwDAYDVR0TBAUw
AwER/zANBnkohkiG9w0BAQUFAAORoORlhzvWEeXilos25vxfv1to/W97u14DeV1.m9
-----END CERTIFICATE REQUEST-----
```

OK      Cancel

**Note:** O administrador da AC solicitou outra extensão de arquivo além do .req.

### Opção 3: Importar um certificado e uma chave CA

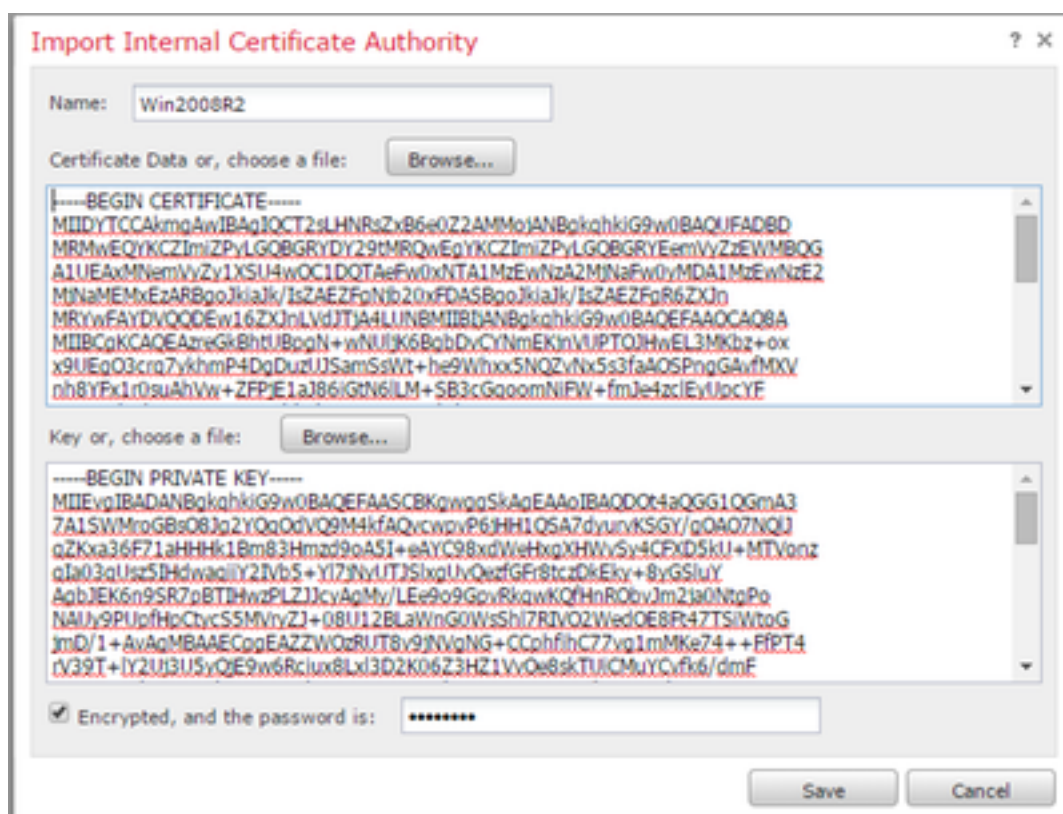


I. Clique em **Importar CA**.

ii. Procure ou cole no certificado.

iii. Navegue até ou cole na chave privada.

iv. Marque a caixa criptografada e digite uma senha.

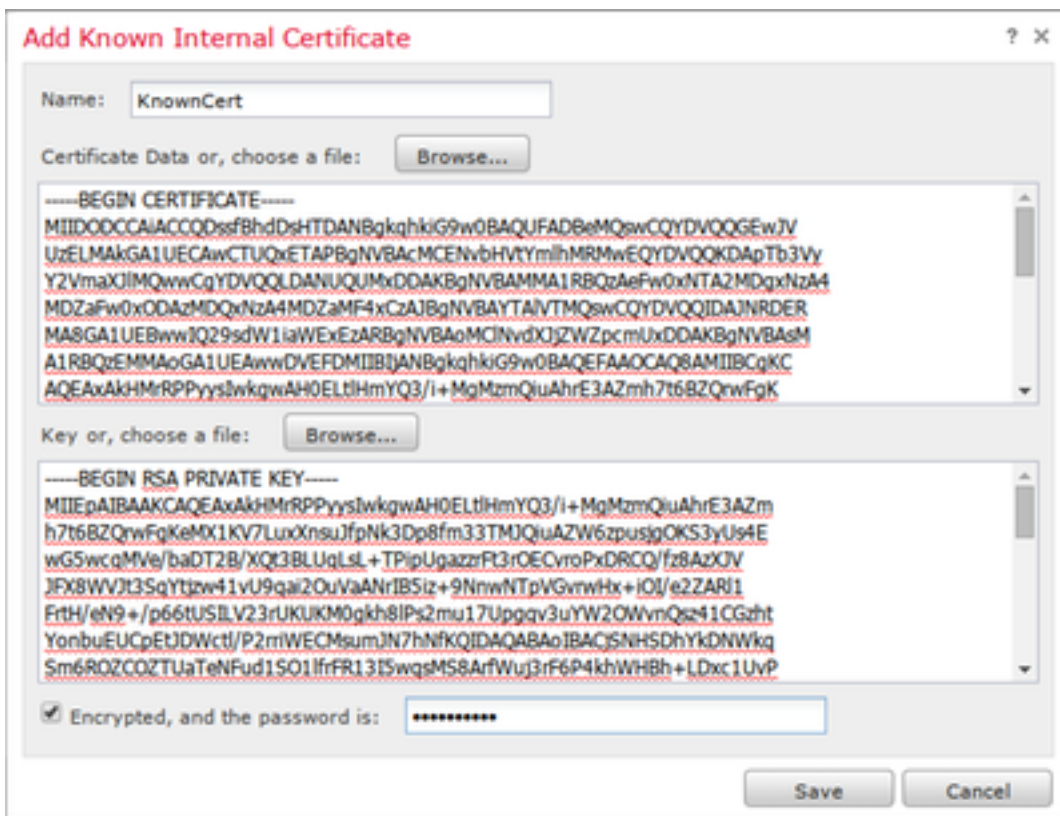


**Note:** Se não houver senha, marque a caixa criptografada e deixe-a em branco.

## 2. Descriptografar com chave conhecida

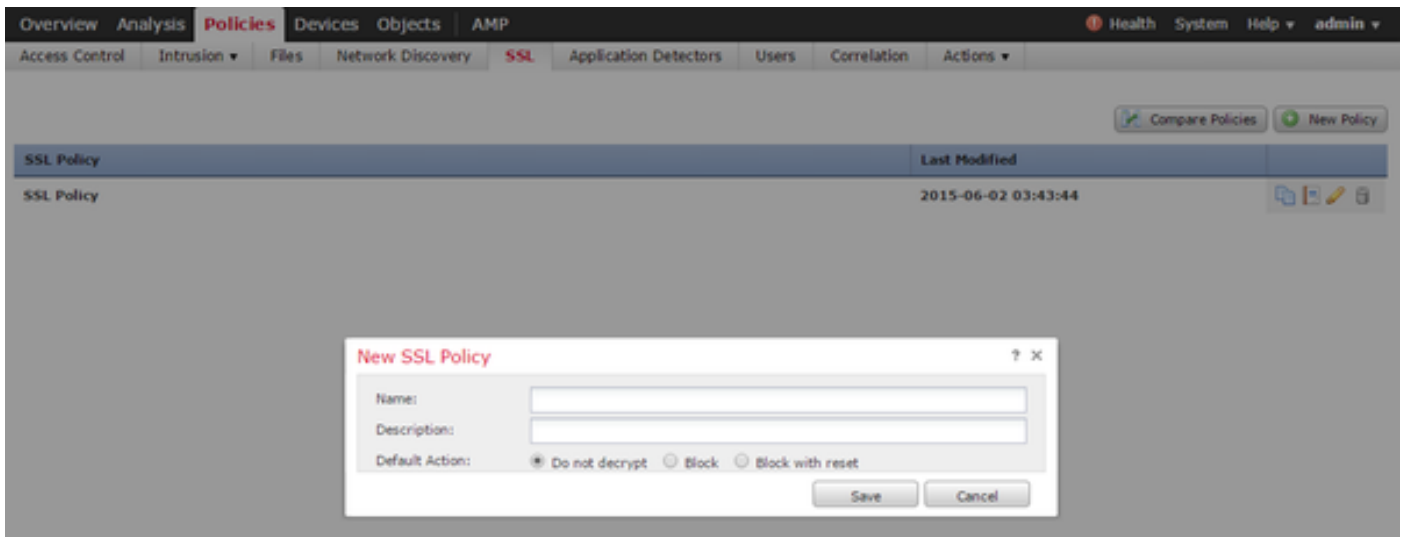
Importando certificado conhecido (alternativa para descriptografar e reassinar)

- I. Na página Objetos à esquerda, expanda PKI e selecione Certificados internos.
- ii. Clique em **Adicionar certificado interno**.
- iii. Procure ou cole no certificado.
- iv. Navegue até ou cole na chave privada.
- v. Marque a caixa **Criptografado** e digite uma senha.



**Note:** Se não houver senha, deixe a caixa **Criptografado** em branco.

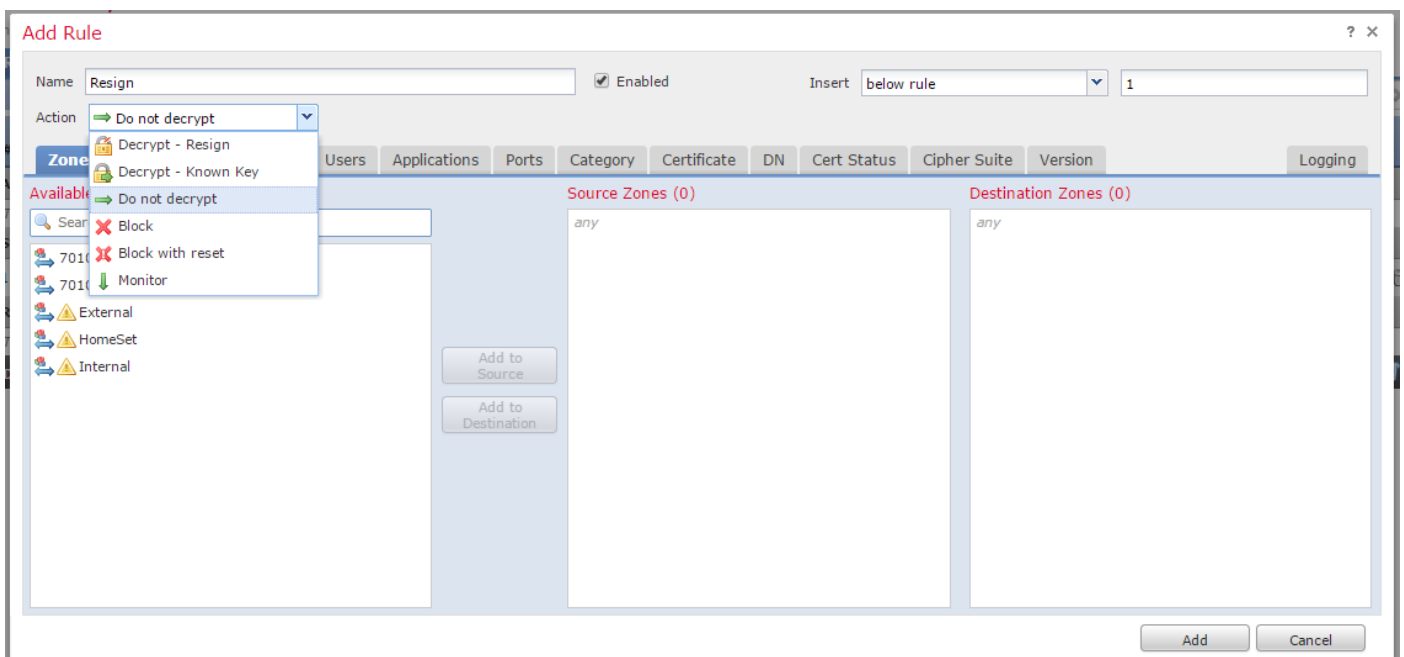
4. Navegue até **Políticas > SSL** e clique em **New Policy**.



5. Forneça um nome e selecione uma **Ação padrão**. A página do editor de política SSL é exibida. A página do editor de política SSL funciona da mesma forma que a página do editor de política de controle de acesso.

**Note:** Se não tiver certeza sobre a **Ação Padrão**, **Não descriptografar** é o ponto inicial recomendado.

6. Na página do editor de política SSL, clique em **Adicionar regra**. Na janela Adicionar regra, forneça um nome para a regra e preencha todas as outras informações relevantes.



A seção a seguir descreve várias opções na janela **Adicionar regra**:

**Ação**

### Descriptografar - Reassinar

- O sensor atua como um homem no meio (MitM) e aceita a conexão com o usuário e, em seguida, estabelece uma nova conexão com o servidor. Por exemplo: O usuário digita em <https://www.facebook.com> em um navegador. O tráfego chega ao sensor, o sensor negocia com o usuário usando o certificado CA selecionado e o túnel SSL A é criado. Ao mesmo tempo, o sensor se conecta a <https://www.facebook.com> e cria o túnel SSL B.

- Resultado final: O usuário vê o certificado na regra, não no facebook.
- Esta ação requer uma CA interna. Selecione Substituir chave se desejar que a chave seja substituída. O usuário receberá o certificado selecionado.

**Note:** Isso não pode ser usado no modo passivo.

## Descriptografar - chave conhecida

- O sensor tem a chave que será usada para descriptografar o tráfego. Por exemplo: O usuário digita em <https://www.facebook.com> em um navegador. O tráfego chega ao sensor, o sensor descriptografa o tráfego e inspeciona o tráfego.
- Resultado final: O usuário vê o certificado do facebook
- Esta ação requer um certificado interno. Isso é adicionado em **Objetos > PKI > Certificados Internos**.

**Note:** Sua organização deve ser a proprietária do domínio e do certificado. Para o exemplo do facebook.com, a única maneira possível de fazer com que o usuário final veja o certificado do facebook seria se você realmente tivesse o domínio facebook.com (ou seja, sua empresa é o Facebook, Inc) e tivesse a propriedade do certificado do facebook.com assinado por uma CA pública. Você só pode descriptografar com chaves conhecidas para sites que sua organização possui.

A principal finalidade da descriptografia de chave conhecida é descriptografar o tráfego que vai para o servidor https para proteger os servidores contra ataques externos. Para inspecionar o tráfego do lado do cliente para sites https externos, você usará o decodificador de resignação, já que não é dono do servidor e está interessado em inspecionar o tráfego do cliente na sua rede, conectando-se a sites criptografados externos.

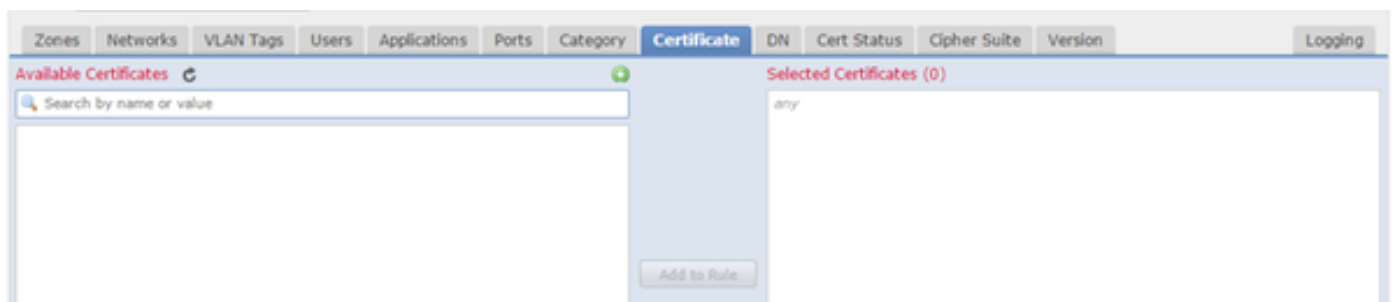
**Note:** Para que DHE e ECDHE descriptografem, devemos estar em linha.

## Não descriptografar

O tráfego ignora a política SSL e continua para a Política de controle de acesso.

### Certificado

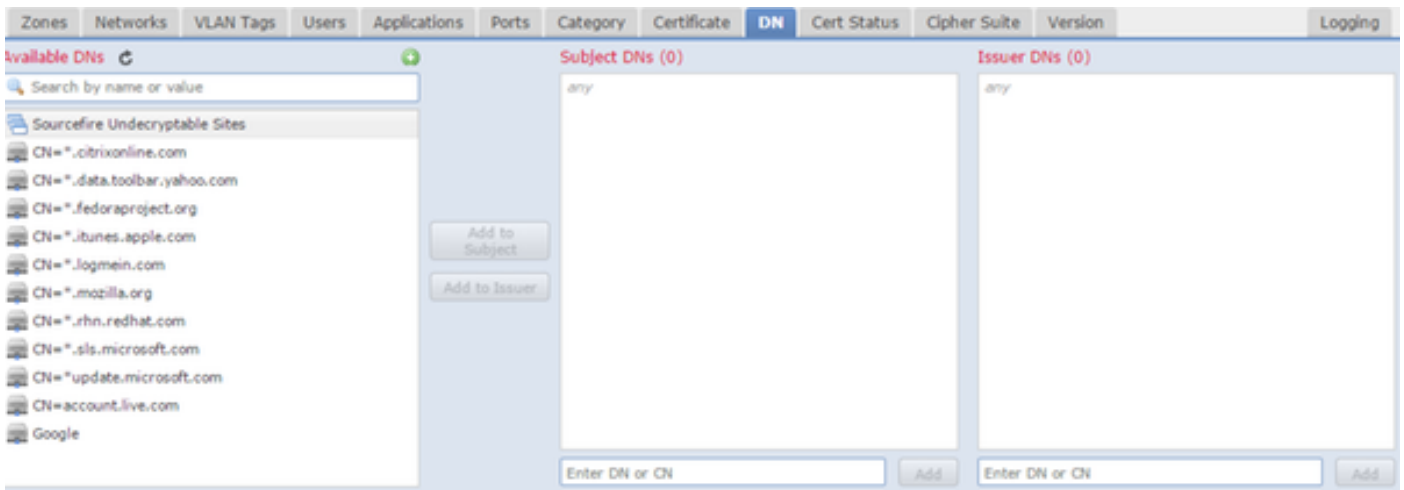
A regra corresponde ao tráfego SSL usando este certificado específico.



### DN

A regra corresponde ao tráfego SSL usando determinados nomes de domínio nos certificados.





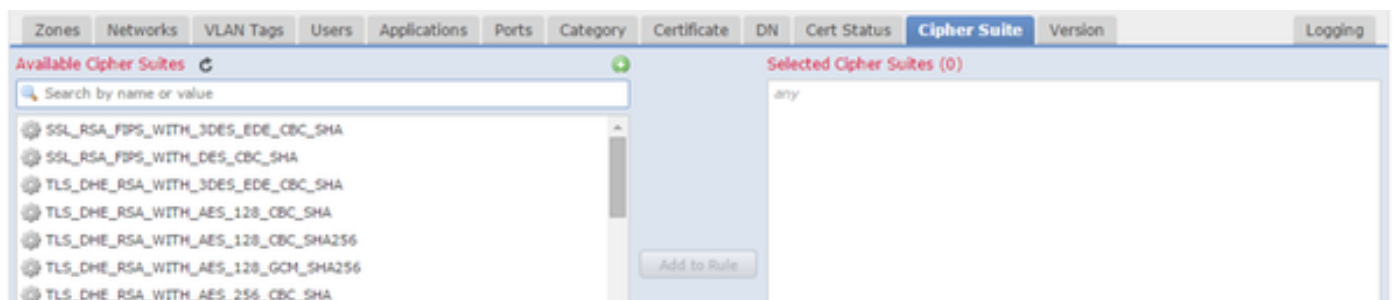
### Status do certificado

A regra corresponde ao tráfego SSL com esses status de certificado.



### Conjunto de Cifras

A regra corresponde ao tráfego SSL usando estes pacotes de cifras.



### Versão

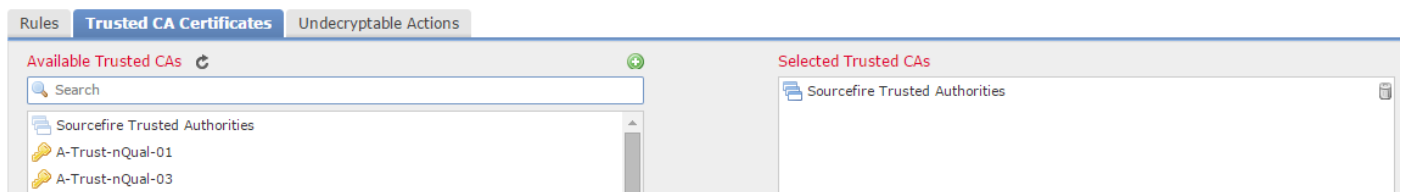
As regras se aplicam somente ao tráfego SSL com as versões selecionadas de SSL.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version
											<input checked="" type="checkbox"/>
											<input checked="" type="checkbox"/>
											<input checked="" type="checkbox"/>
											<input checked="" type="checkbox"/>

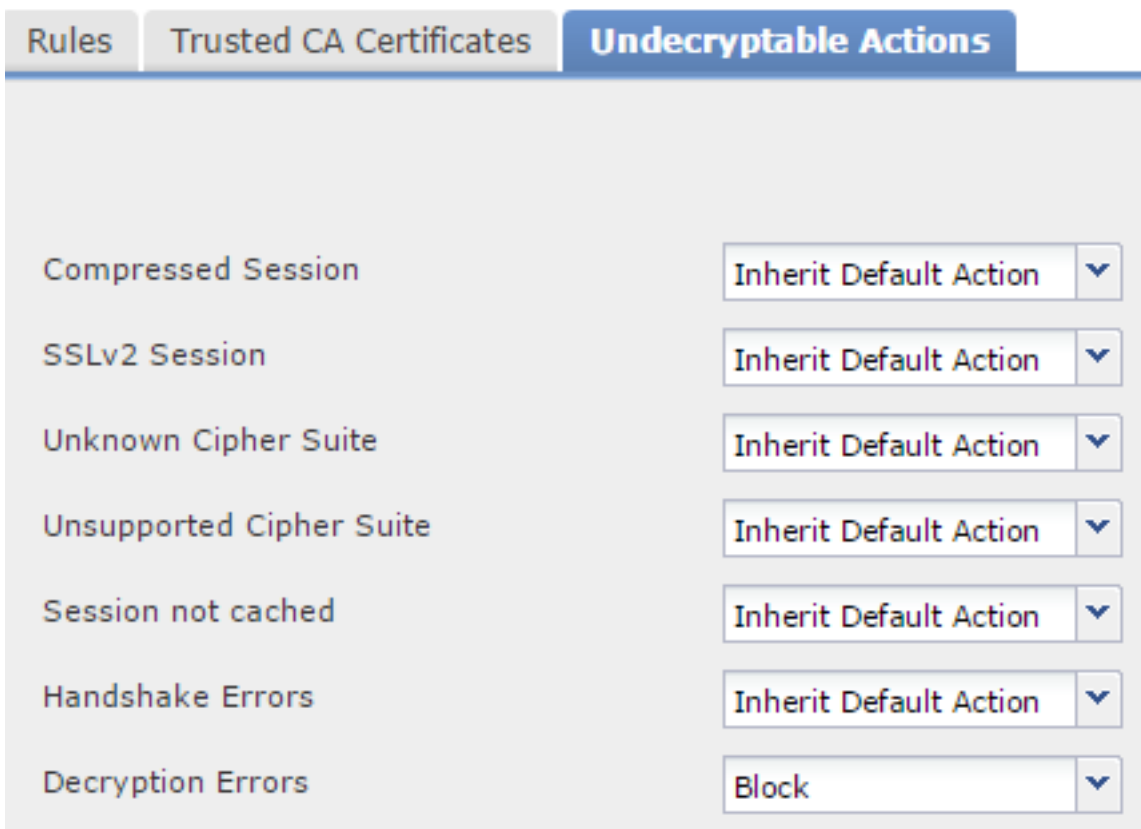
## Registro

Ative o registro para ver eventos de ligação para o tráfego SSL.

7. Clique em **Certificado CA confiável**. É aqui que CA confiável é adicionada à política.



8. Clique em **Ações não descritografáveis**. Aqui estão as ações para as quais o sensor não pode descritografar o tráfego. Você pode encontrar as definições na ajuda on-line (**Ajuda > Online**) do FireSIGHT Management Center.



- **Sessão Compactada:** A sessão SSL aplica um método de compactação de dados.
- **Sessão SSLv2:** A sessão é criptografada com SSL versão 2. Observe que o tráfego é descritografável se a mensagem de saudação do cliente for SSL 2.0 e o restante do tráfego transmitido for SSL 3.0.
- **Conjunto de Cifras Desconhecido:** O sistema não reconhece o conjunto de cifras.

- **Conjunto de Cifras Não Suportado:** O sistema não suporta descryptografia com base no conjunto de cifras detectado.
- **Sessão não armazenada em cache:** A reutilização de sessão SSL está habilitada, o cliente e o servidor restabeleceram a sessão com o identificador de sessão e o sistema não armazenou esse identificador de sessão em cache.
- **Erros de aperto de mão:** Ocorreu um erro durante a negociação do handshake SSL.
- **Erros de descryptografia:** Ocorreu um erro durante a descryptografia do tráfego.

**Note:** Por padrão, elas herdam a Ação padrão. Se a ação padrão for Bloquear, você poderá enfrentar problemas inesperados

9. Salve a diretiva.

10. Navegue para **Políticas > Controle de acesso**. Edite sua política ou crie uma nova Política de Controle de Acesso.

11. Clique em **Avançado** e edite **Configurações gerais**.

The screenshot shows the Palo Alto Networks GUI for configuring an Access Control policy. The 'Policies' tab is active, and the 'Advanced' sub-tab is selected. A 'General Settings' dialog box is open, showing the following configuration:

Setting	Value
Maximum URL characters to store in connection events	1024
Allow an Interactive Block to bypass blocking for (seconds)	600
SSL Policy to use for inspecting encrypted connections	SSL Policy
Inspect traffic during policy apply	<input checked="" type="checkbox"/>

12. No menu suspenso, selecione sua **Política SSL**.

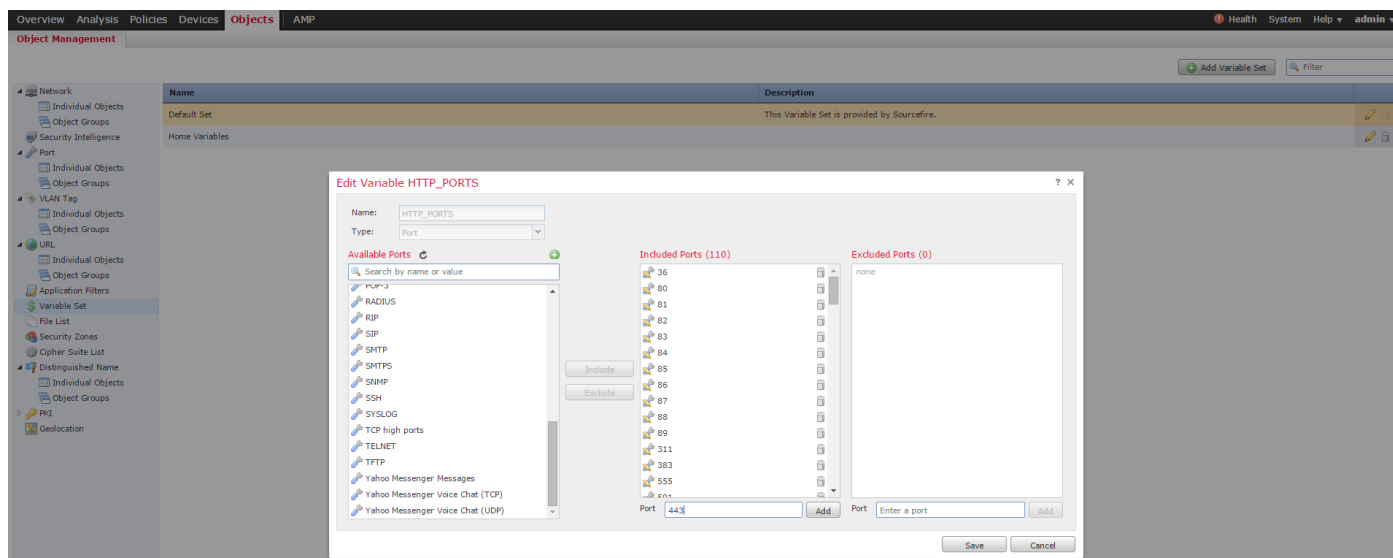
13. Clique em **OK** para salvar.

## Configurações adicionais

As seguintes alterações devem ser feitas nas políticas de intrusão para identificação adequada:

I. A variável \$HTTP\_PORTS deve incluir a porta 443 e quaisquer outras portas com tráfego https que serão descryptografadas pela sua política (**Objetos > Gerenciamento de Objetos > Conjunto**

de Variáveis > Editar o conjunto de variáveis).



ii. A política de análise de rede que está inspecionando o tráfego criptografado deve ter a porta 443 (e quaisquer outras portas com tráfego https que serão descriptografadas pela sua política) incluída no campo de portas das configurações do pré-processador HTTP, caso contrário, nenhuma das regras http com modificadores de conteúdo http (ou seja, http\_uri, http\_header, etc.) será acionada porque isso depende das portas http definidas e os buffers http no snort não serão preenchidos para o tráfego que não passa pelas portas especificadas.

iii. (Opcional, mas recomendado para melhor inspeção) Adicione suas portas https às configurações de configuração de fluxo TCP no campo Executar remontagem de fluxo em ambas as portas.

iv. Reaplique a política revisada de controle de acesso durante uma janela de manutenção programada.

**Aviso:** essa política modificada pode causar problemas significativos de desempenho. Isso deve ser testado fora do horário de produção para reduzir o risco de paralisação ou desempenho da rede.

## Verificação

Descriptografar - Reassinar

1. Abra um navegador da Web.

**Nota:** O navegador Firefox é usado no exemplo abaixo. Este exemplo pode não funcionar em Chrome. Consulte a seção Solução de problemas para obter detalhes.

2. Navegue até um site SSL. No exemplo abaixo, <https://www.google.com> é usado. Os sites da instituição financeira também funcionarão. Você verá uma das seguintes páginas:

The screenshot shows a Firefox browser window with the address bar containing `https://www.google.com/?gws_rd=ssl`. A yellow warning icon is visible on the left. The main heading reads "This Connection is Untrusted". Below it, the text states: "You have asked Firefox to connect securely to **www.google.com**, but we can't confirm that your connection is secure."

An "Add Security Exception" dialog box is open in the foreground. It contains the following information:

- Warning icon and text: "You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this."
- Server section: "Location: `https://www.google.com/?gws_rd=ssl`" with a "Get Certificate" button.
- Certificate Status section: "This site attempts to identify itself with invalid information." with a "View..." button.
- Unknown Identity** section: "The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature."

**Note:** Você verá a página acima se o certificado em si não for confiável e o certificado CA de assinatura não for confiável pelo navegador. Para descobrir como o navegador determina certificados de CA confiáveis, consulte a seção Autoridades de certificado confiáveis abaixo.



Google Search I'm Feeling Lucky

Page Info - https://www.google.com/?gws\_rd=ssl

General Media Permissions Security

Website Identity

Website: **www.google.com**

Owner: **This website does not supply ownership information.**

Verified by: **Sourcefire**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today?	<b>Yes, 277 times</b>
Is this website storing information (cookies) on my computer?	<b>Yes</b> <a href="#">View Cookies</a>
Have I saved any passwords for this website?	<b>No</b> <a href="#">View Saved Passwords</a>

Technical Details

**Note:** Se esta página for vista, você regravou o tráfego com êxito. Observe a seção **Verificado por: Sourcefire.**

Could not verify this certificate because the issuer is unknown.

---

**Issued To**

Common Name (CN) www.google.com  
Organization (O) Google Inc  
Organizational Unit (OU) <Not Part Of Certificate>  
Serial Number 13:E3:D5:7D:4E:5F:8F:E7

**Issued By**

Common Name (CN) Sourcefire TAC  
Organization (O) Sourcefire  
Organizational Unit (OU) Tac

**Period of Validity**

Begins On 5/6/2015  
Expires On 8/3/2015

**Fingerprints**

SHA-256 Fingerprint 20:00:CB:25:13:8B:1F:89:4D:4A:CF:C5:E2:21:38:92:06:66:00:2E:B7:83:27:72:98:EA:B1:6A:10:B3:67:A1  
SHA1 Fingerprint 1B:C2:30:D9:66:84:DB:97:CF:A9:5E:5F:29:DA:4C:3F:13:E9:DE:5D

**Note:** Esta é uma análise detalhada do mesmo certificado.

- 3. No Management Center, vá para **Analysis > Connections > Events**.
- 4. Dependendo do fluxo de trabalho, você pode ou não ver a opção de descryptografia SSL. Clique em **Table View of Connection Events**.

[Connections with Application Details](#) > [Table View of Connection Events](#)

No Search Constraints ([Edit Search](#))

Jump to... ▼	<input type="checkbox"/>	▼ <a href="#">First Packet</a>	<a href="#">Last Packet</a>	<a href="#">Action</a>	<a href="#">Reason</a>
--------------	--------------------------	--------------------------------	-----------------------------	------------------------	------------------------

- 5. Role para a direita e procure o Status do SSL. Você deve ver opções semelhantes às abaixo:

<a href="#">443 (https) / tcp</a>	<a href="#">Decrypt (Resign)</a>	<input type="checkbox"/> <a href="#">HTTPS</a>	<input type="checkbox"/> <a href="#">Secure Web browser</a>	<input type="checkbox"/> <a href="#">Skype Tunneling</a>
<a href="#">443 (https) / tcp</a>	<a href="#">Decrypt (Resign)</a>	<input type="checkbox"/> <a href="#">HTTPS</a>	<input type="checkbox"/> <a href="#">Secure Web browser</a>	<input type="checkbox"/> <a href="#">Google</a>

Descriptografar - Certificado conhecido

1. No FireSIGHT Management Center, navegue para **Analysis > Connections > Events**.
2. Dependendo do fluxo de trabalho, você pode ou não ver a opção de descriptografia SSL. Clique em **Table View of Connection Events**.

[Connections with Application Details](#) > [Table View of Connection Events](#)

No Search Constraints ([Edit Search](#))

Jump to... ▼	<input type="checkbox"/>	▼ <a href="#">First Packet</a>	<a href="#">Last Packet</a>	<a href="#">Action</a>	<a href="#">Reason</a>
--------------	--------------------------	--------------------------------	-----------------------------	------------------------	------------------------

3. Role para a direita e procure o Status do SSL. Você deve ver opções semelhantes às abaixo:

<a href="#">443 (https) / tcp</a>	<a href="#">Decrypt (Resign)</a>	<input type="checkbox"/> <a href="#">HTTPS</a>	<input type="checkbox"/> <a href="#">Secure Web browser</a>	<input type="checkbox"/> <a href="#">Skype Tunneling</a>
<a href="#">443 (https) / tcp</a>	<a href="#">Decrypt (Resign)</a>	<input type="checkbox"/> <a href="#">HTTPS</a>	<input type="checkbox"/> <a href="#">Secure Web browser</a>	<input type="checkbox"/> <a href="#">Google</a>

## Troubleshooting

### Problema 1: Alguns sites podem não ser carregados no navegador do Chrome

#### Exemplo

www.google.com não pode ser carregado com um descriptografar - reinicia usando o Chrome.

#### Razão

O navegador Google Chrome é capaz de detectar certificados fraudulentos para propriedades do google a fim de evitar ataques de intermediários. Se o navegador Chrome (cliente) tentar se conectar a um domínio google.com (servidor) e um certificado for retornado que não é um certificado válido do google, o navegador negará a conexão.

#### Solução

Se você experimentar isso, adicione uma regra **Não descriptografar** para DN=\*.google.com, \*.gmail.com, \*.youtube.com. Em seguida, limpe o cache e o histórico do navegador.



## Problema 2: Obtendo um aviso/erro não confiável em alguns navegadores

### Exemplo

Quando se conecta a um site usando o Internet Explorer e o Chrome, você não recebe um aviso de segurança, mas quando usa o navegador Firefox, você precisa confiar na conexão toda vez que fechar e reabrir o navegador.

### Razão

A lista de CAs confiáveis depende do navegador. Quando você confia em um certificado, isso não se propaga em navegadores e a entrada confiável geralmente só persiste enquanto o navegador está aberto, então, uma vez fechado, todos os certificados confiáveis serão removidos e, na próxima vez que você abrir o navegador e visitar o site, você deverá adicioná-lo à lista de certificados confiáveis novamente.

### Solução

Neste cenário, o IE e o Chrome usam a lista de CAs confiáveis no sistema operacional, mas o Firefox mantém sua própria lista. Portanto, o certificado CA foi importado para a loja do SO, mas não foi importado para o navegador Firefox. Para evitar receber o aviso de segurança no Firefox, você deve importar o certificado de CA para o navegador como uma CA confiável.

### Autoridades de certificado confiáveis

Quando uma conexão SSL é estabelecida, o navegador primeiro verifica se esse certificado é confiável (ou seja, você já esteve neste site antes e manualmente instruiu o navegador a confiar nesse certificado). Se o certificado não for fidedigno, o browser verifica o certificado da Autoridade de Certificação (AC) que verificou o certificado para este site. Se o certificado CA for confiável pelo navegador, ele o considerará um certificado confiável e permitirá a conexão. Se o certificado CA não for confiável, o navegador exibirá um aviso de segurança e forçará você a adicionar manualmente o certificado como um certificado confiável.

A lista de CAs confiáveis em um navegador depende completamente da implementação do navegador e cada navegador pode preencher sua lista confiável de forma diferente dos outros navegadores. Em geral, há duas maneiras de os navegadores atuais preencherem uma lista de CAs confiáveis:

1. Eles usam a lista de CAs confiáveis em que o sistema operacional confia
2. Eles enviam uma lista de CAs confiáveis com o software e ele é incorporado ao navegador.

Para os navegadores mais comuns, as CAs confiáveis são preenchidas da seguinte forma:

- **Google Chrome:** Lista de ACs confiáveis do sistema operacional
- **Firefox:** Mantém sua própria lista de CAs confiáveis
- **Internet Explorer:** Lista de ACs confiáveis do sistema operacional
- **Safari:** Lista de ACs confiáveis do sistema operacional

É importante saber a diferença porque o comportamento visto no cliente varia dependendo disso. Por exemplo, para adicionar uma CA confiável para o Chrome e o IE, é necessário importar o certificado de CA para o armazenamento de CA confiável do SO. Se importar o certificado CA para o armazenamento de AC fidedigno do SO, deixará de receber um aviso ao ligar a sites com um certificado assinado por esta AC. No navegador Firefox, você deve importar manualmente o certificado CA para o armazenamento de CA confiável no próprio navegador. Depois de fazer

isso, você não receberá mais um aviso de segurança ao se conectar a sites verificados por essa CA.

## Referências

- [Introdução às regras SSL](#)