Permitir reCAPTCHA do Google quando o acesso aos portais do mecanismo de pesquisa for bloqueado

Contents

Introdução

Este documento descreve as etapas para permitir que o Google reCAPTCHA no Secure Web Appliance (SWA), quando você tiver bloqueado o acesso aos portais do mecanismo de pesquisa.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Web Access e descriptografia HTTPS.

A Cisco recomenda que você também tenha:

- SWA físico ou virtual instalado.
- Licença ativada ou instalada.
- O assistente de instalação foi concluído.
- Acesso administrativo à interface gráfica do usuário (GUI) do SWA.

Componentes Utilizados

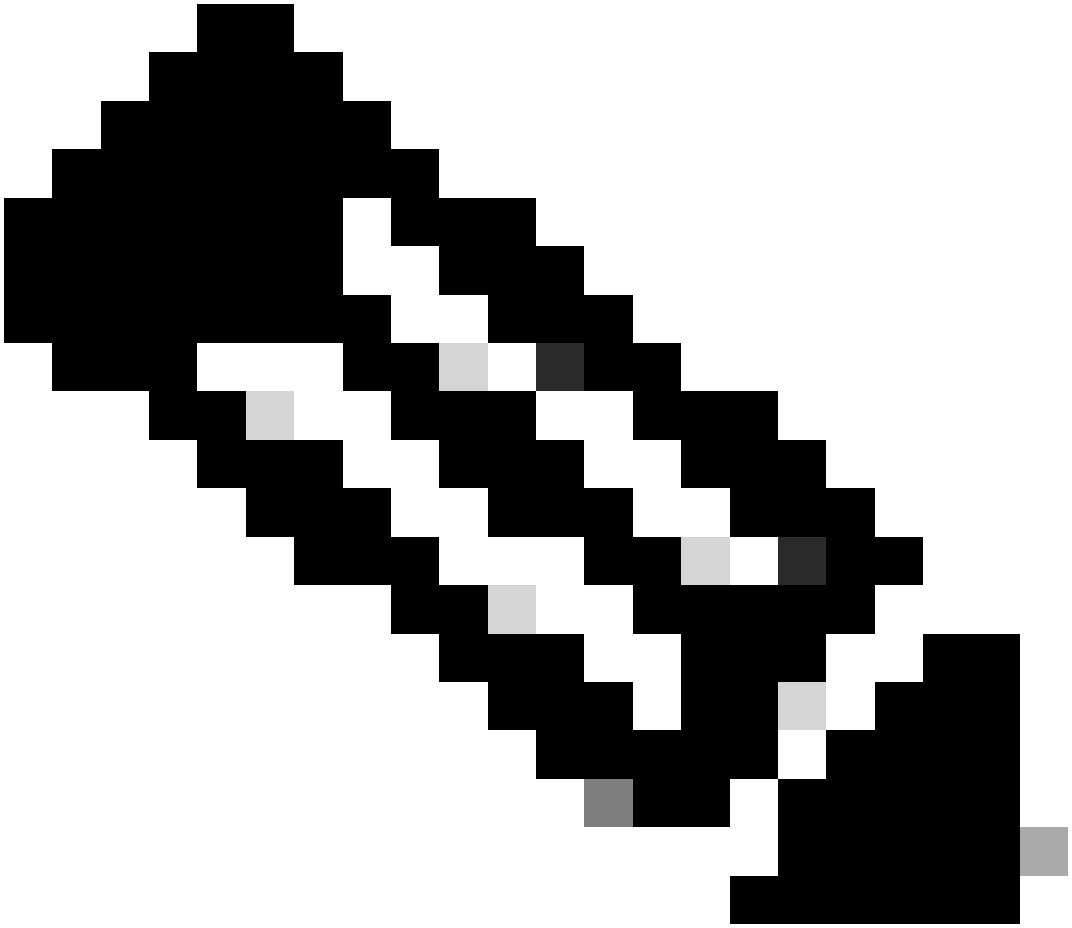
Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

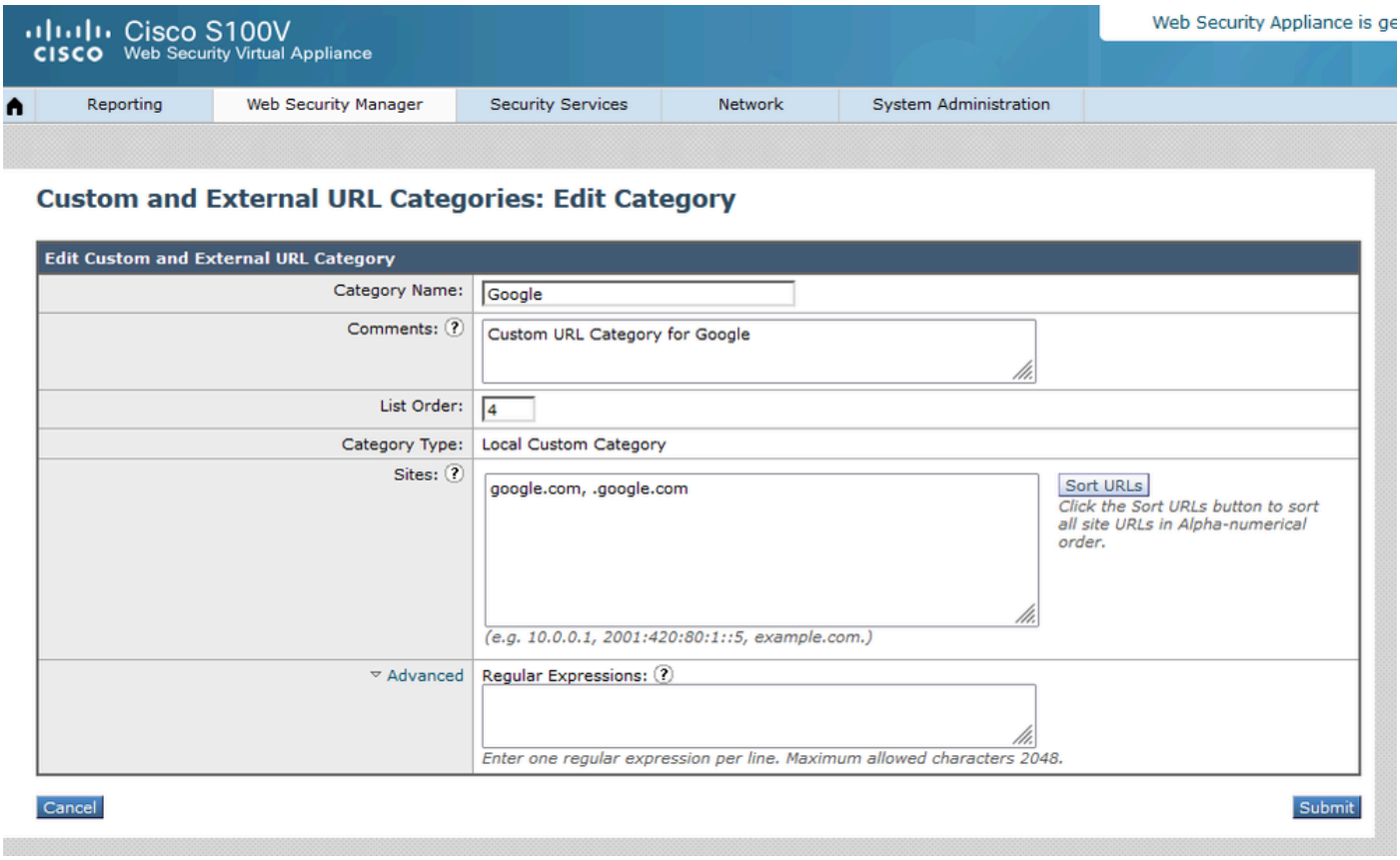
Configuration Steps

Etapa 1. Na GUI, navegue até Security Services e escolha HTTPS Proxy, habilitar descriptografia HTTPS se ainda não estiver habilitada.

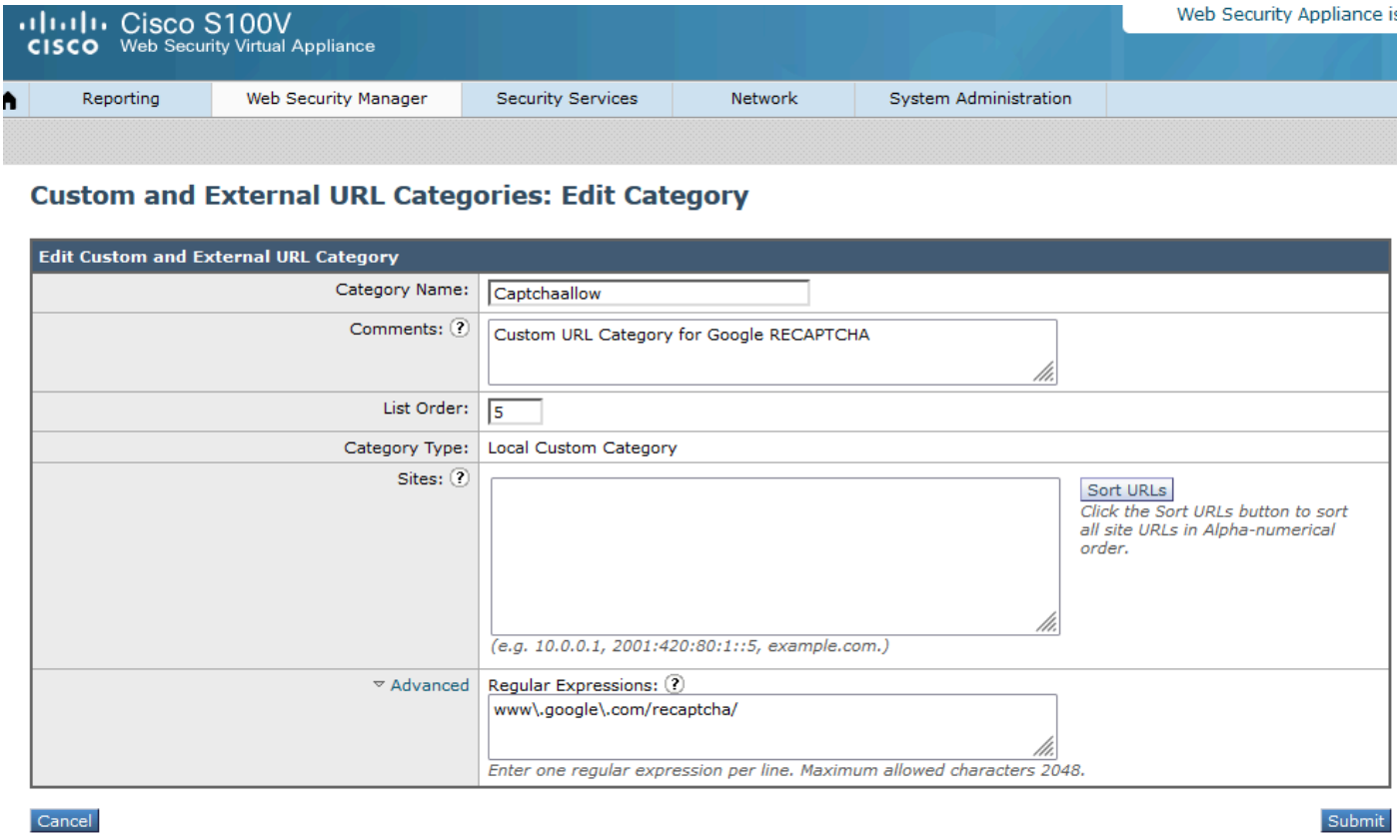


Observação: a descriptografia HTTPS deve ser habilitada para esta configuração. Se não estiver habilitado, consulte o artigo mencionado no final deste documento.

Etapa 2. Na GUI, navegue até Web Security Manager e escolha **Custom and External URL** Categories, crie duas categorias de URL personalizadas, uma para google.com e outra para o Google reCAPTCHA. Clique em Submit.



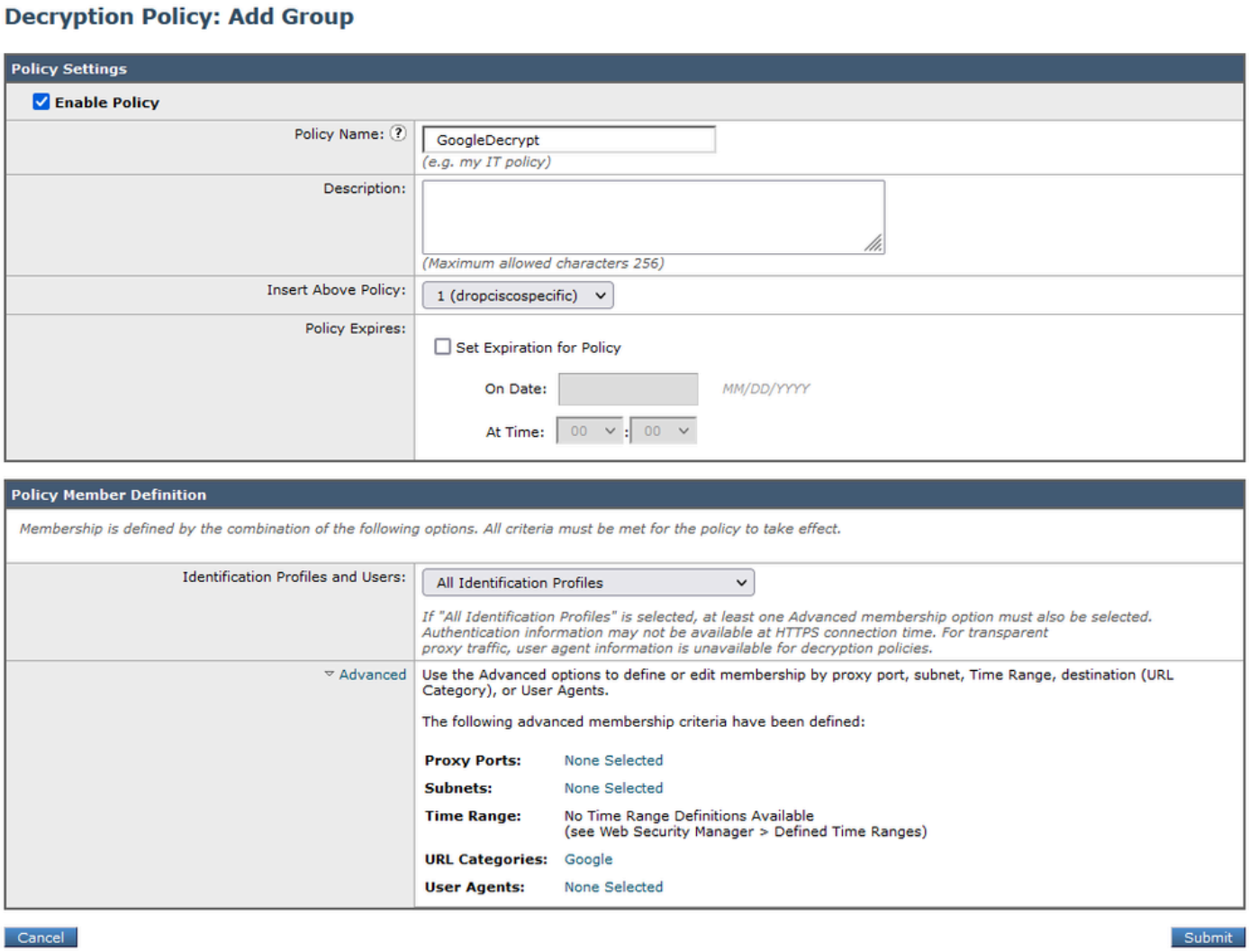
Criar categoria de URL personalizada para o Google



Criar categoria de URL personalizada para o Google

Etapa 3. Na GUI, navegue até **Web Security Manager** e escolha **Decryption Policies**, crie a política de descriptografia para descriptografar google.com. Clique em **Nenhum selecionado** ao lado de **Categorias de URL** e selecione **Google** categoria de URL personalizada. Clique em

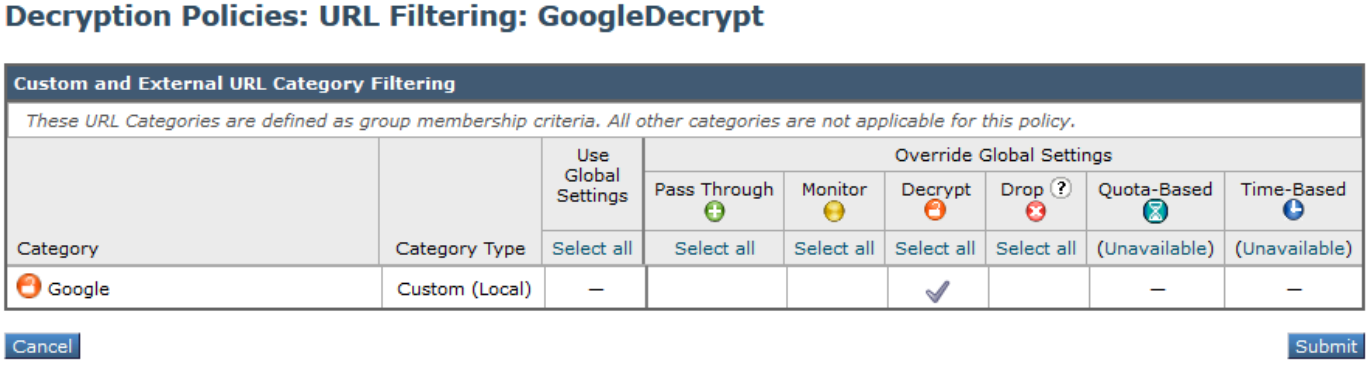
Submit.



Política de descriptografia para descriptografar o Google

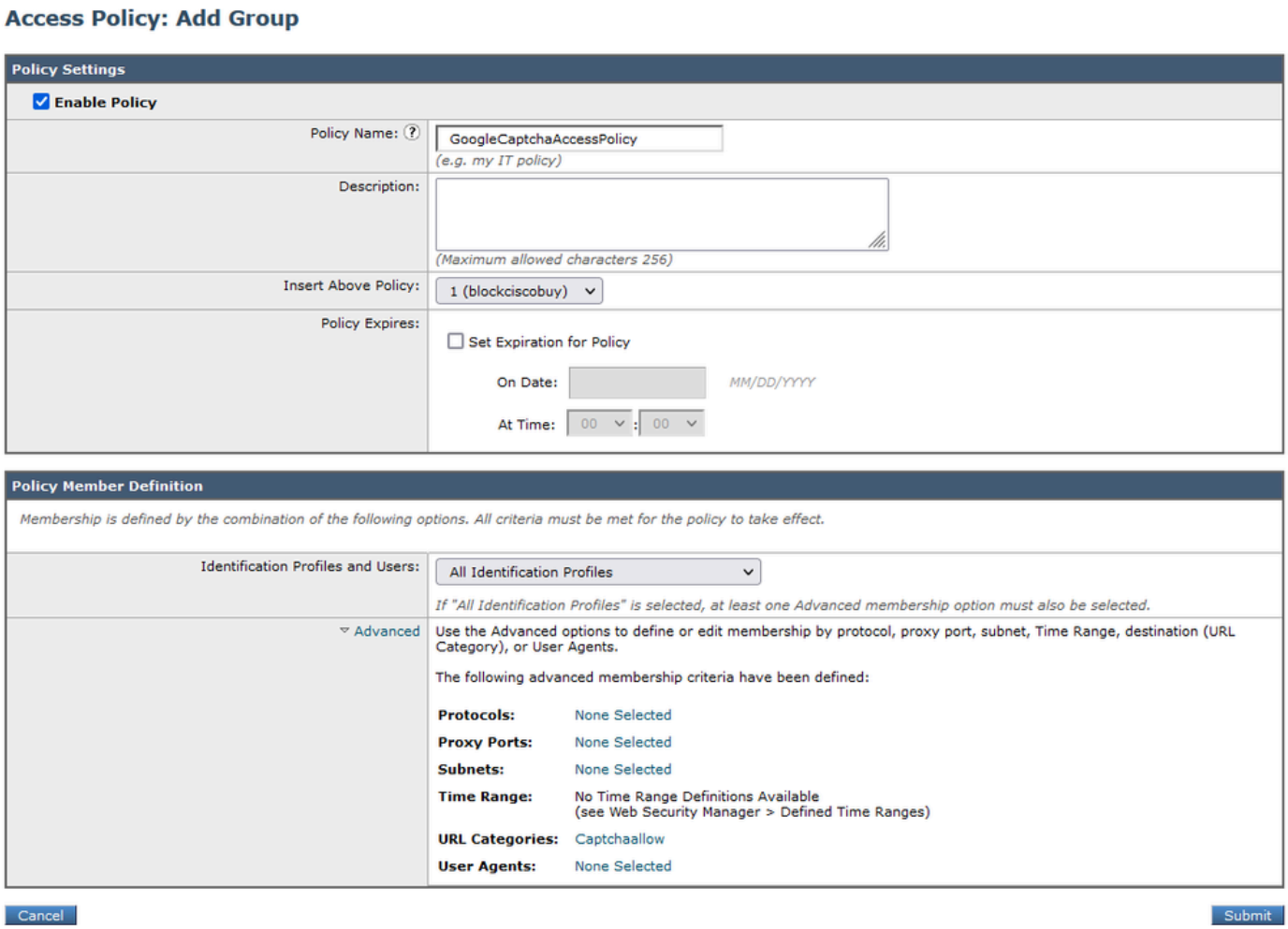
Etapa 3.1. Navegue até **Decryption Policies** e clique em **Monitor** de acordo com a **políticaGoogleDecrypt.**

Etapa 3.2. Selecione Decrypt na linha para **Google Category** e clique em **Submit.**



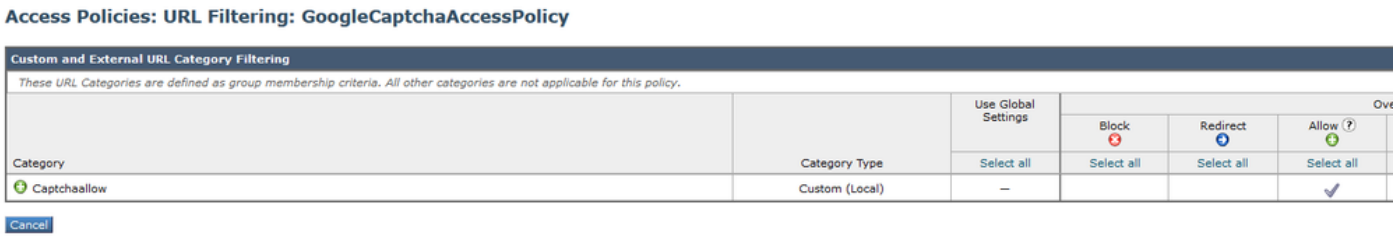
Selecione a categoria de URL personalizada criada para o Google para descriptografá-la na política de descriptografia

Etapa 4. Na GUI, navegue para **Web Security Manager** e escolha **Access Policies**, crie Access policy para permitir que o Google reCAPTCHA e selecione **captchaallow** como **URL Categories**.



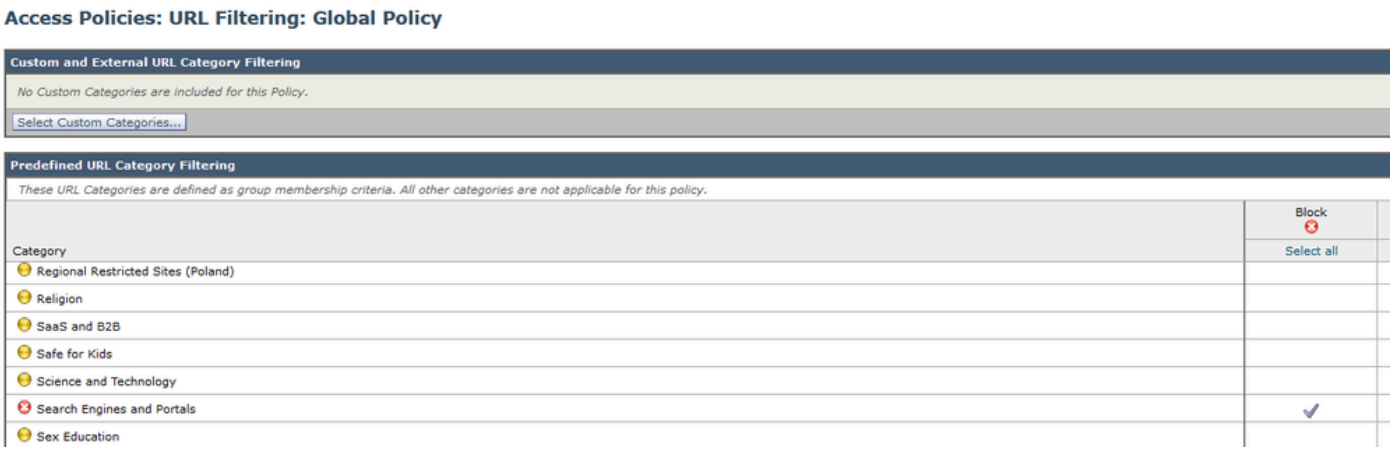
Política de acesso para permitir o Google RECAPTCHA

Etapa 4.1. Navegue para Access Policies e clique em **Monitor** de acordo com a **política do GoogleCaptchAccessPolicy. Selecione Permitir** na linha para **Captchaallow** Categoria**. Enviar** e **confirmar alterações.**



Selecione a categoria de URL personalizada criada para o Google RECAPTCHA para permitir na política de acesso

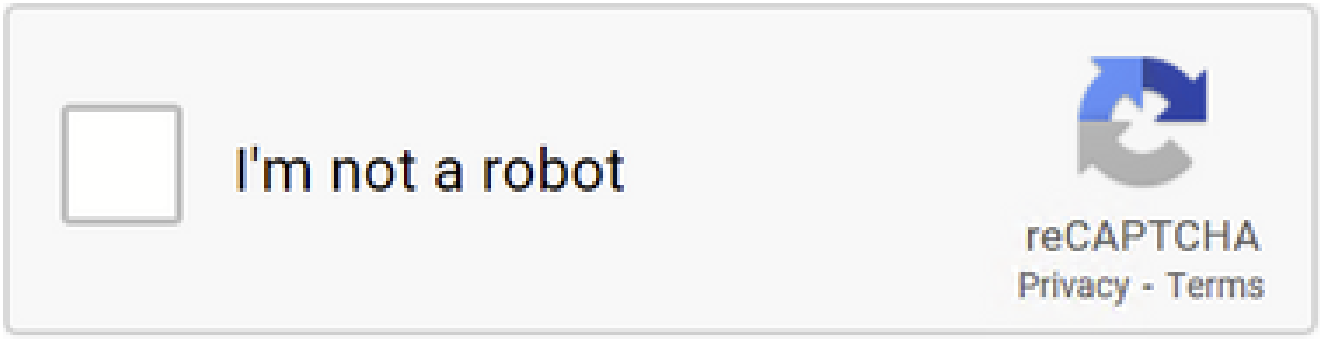
Etapa 5. Certifique-se de que os **mecanismos de pesquisa e portais** em **Filtragem de categoria de URL predefinida** estejam bloqueados na política de acesso global:



Política padrão para bloquear o acesso a mecanismos de pesquisa

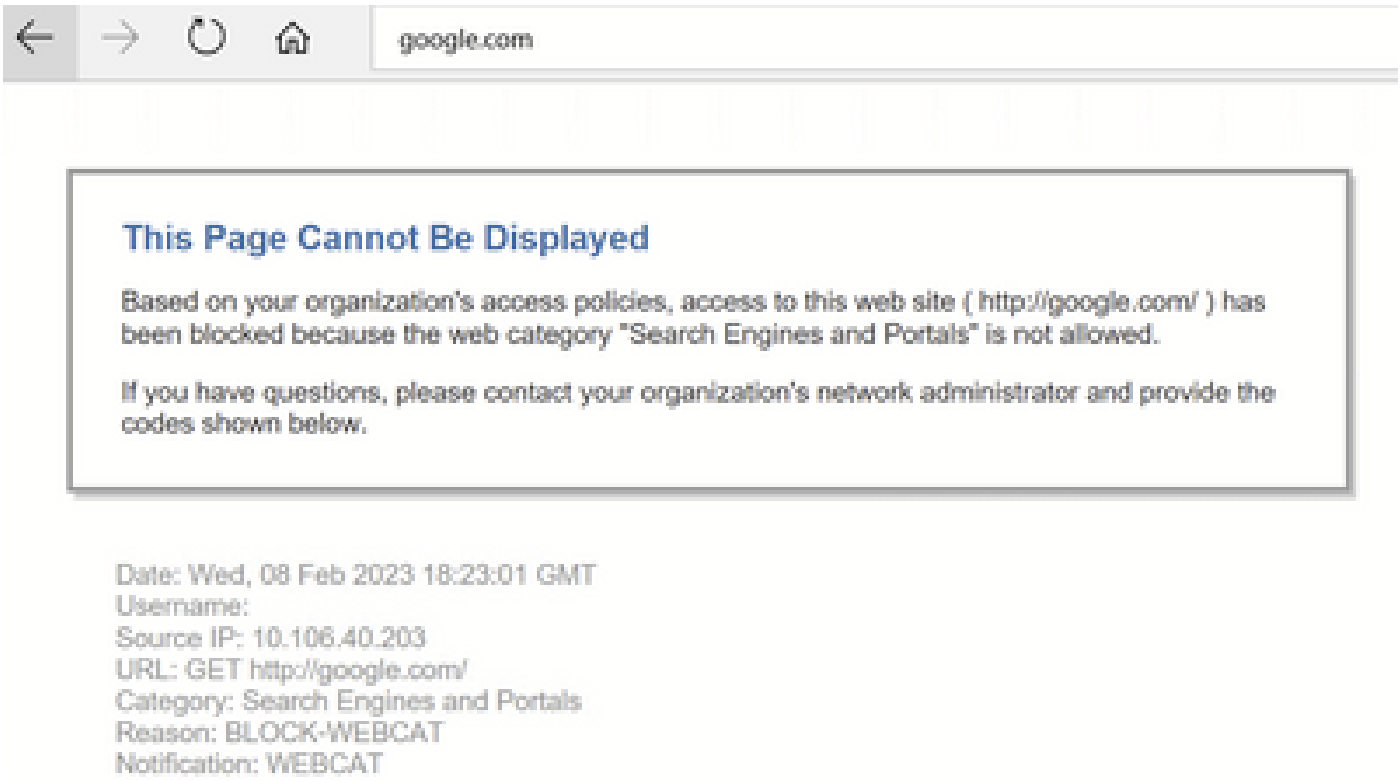
Verificar

Você pode ver o acesso ao Google reCAPTCHA funciona, mas o acesso ao mecanismo de pesquisa (Google) ainda é negado, depois que você habilita a descriptografia HTTPS e permite o acesso ao Google reCAPTCHA na política de acesso:



Google CAPTCHA Works

1675880489.667 279 10.106.40.203 TCP_MISS_SSL/200 23910 GET https://www.google.com:443/recaptcha/api2/anchor?ar=1&k=6LdN4qUZAAAAAF



O site do Google está bloqueado

1675880581.157 0 10.106.40.203 TCP_DENIED/403 0 GET "https://google.com/favicon.ico" - NONE/- - BLOCK_WEBCAT_12-DefaultGroup-DefaultC

Troubleshooting

Se o acesso ao Google reCAPTCHA estiver bloqueado, você poderá verificar os logs de acesso na CLI SWA. Se você vir o URL do Google e não o URL reCAPTCHA do Google, pode ser que a descriptografia não esteja ativada:

1675757652.291 2 192.168.100.79 TCP_DENIED/403 0 CONNECT tunnel://www.google.com:443/ - NONE/- - BLOCK_WEBCAT_12-DefaultGroup-Fi

Referências

- Manual do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD (General Deployment) - Conectar, Instalar e Configurar [Cisco Secure Web Appliance] - Cisco
- Uso do certificado WSA para descriptografia HTTPS

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.