Bloquear o modo Google AI no Secure Web Appliance

Contents

Introdução

Este documento descreve as etapas necessárias para executar o para que o Secure Web Appliance seja configurado para bloquear as solicitações HTTPS para o Modo AI do Google.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- administração de SWA
- Protocolos básicos de rede e proxy
- Processo de descriptografia do SWA
- Expressões regulares

A Cisco recomenda que você tenha estas ferramentas instaladas:

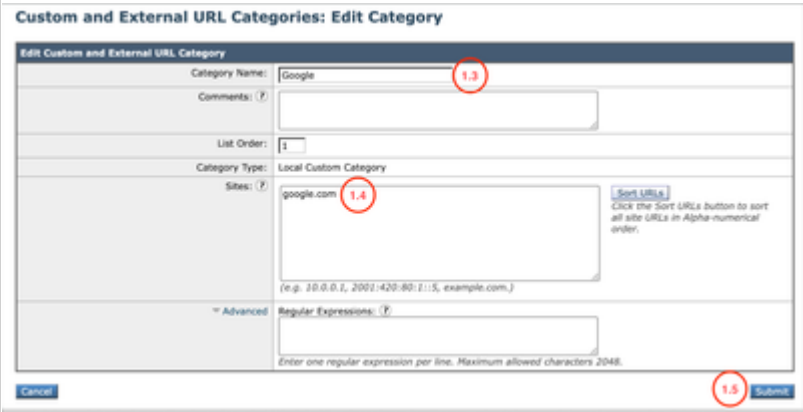
- SWA físico ou virtual
- Acesso administrativo à interface gráfica do usuário (GUI) do SWA

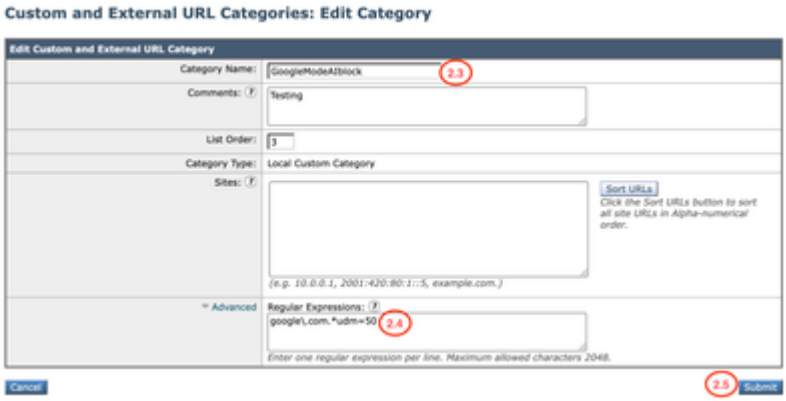
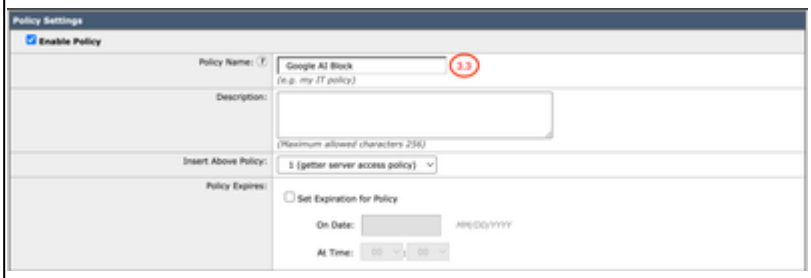
Componentes Utilizados

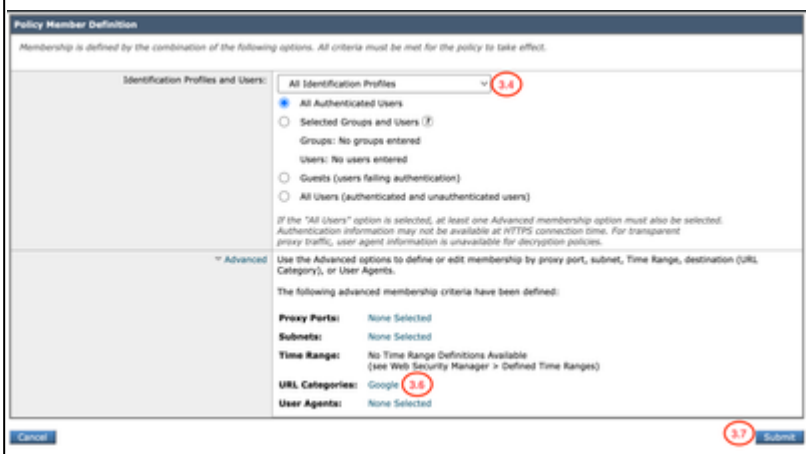
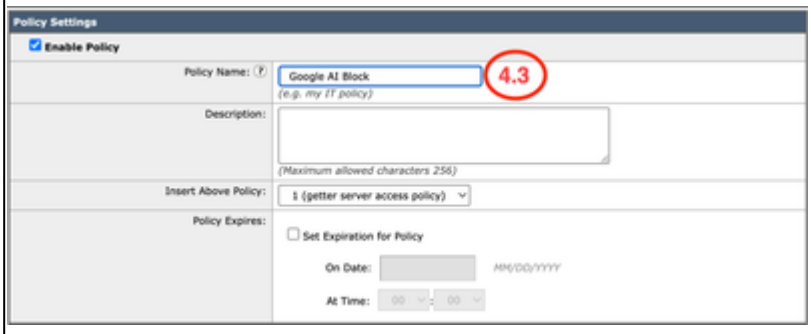
Este documento não se restringe a versões de software e hardware específicas.

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.

Etapas de configuração

Etapa 1. Crie uma categoria de URL personalizada para o site do Google.	Etapa 1.1. Na GUI, navegue para Web Security Manager e escolha Categorias de URL externas e personalizadas. Etapa 1.2. Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada. Etapa 1.3. Digite Name para a nova categoria. Etapa 1.4. Defina esses URLs na seção Sites: `google.com` Etapa 1.5. Envie as alterações. 
Etapa 2.Crie uma categoria de URL personalizada para o Google AI Mode.	Etapa 2.1. Na GUI, navegue para Web Security Manager e escolha Categorias de URL externas e personalizadas. Etapa 2.2. Clique em Adicionar categoria para criar uma nova categoria de URL personalizada. Etapa 2.3. Digite Name para a nova categoria.

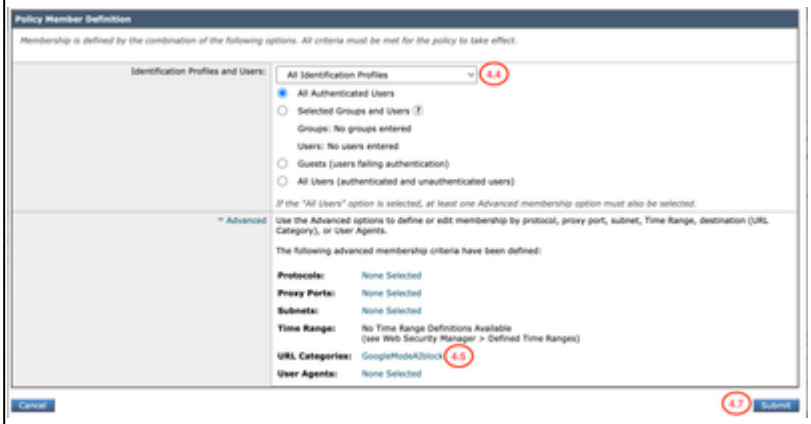
	Etapa 2.4. Defina esses URLs na seção Expressões regulares: `google\.com.*udm=50` Etapa 2.5. Enviar as alterações. Tip: Para obter mais informações sobre como configurar categorias de URL personalizadas, visite: Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco 
Etapa 3. Descriptografar o tráfego do Google.	Etapa 3.1. Na GUI, navegue para Web Security Manager e escolha Políticas de descriptografia Etapa 3.2. Clique em Add Policy. Etapa 3.3. Digite Name para a nova política.  Etapa 3.4. (Opcional) Selecione o Perfil de identificação ao qual você precisa que essa política se aplique. Etapa 3.5. Na seção Definição de membro da política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada.

	Etapa 3.6. Selecione a categoria de URL que foi criada na Etapa 1. Etapa 3.7. Clique em Enviar.  Etapa 3.8. Na página Políticas de descriptografia, clique no link Filtragem de URL para obter a nova política. Etapa 3.9. Escolha Descriptografar como a ação para Categoria de URL Personalizada. Etapa 3.10. Clique em Enviar. 
Etapa 4. Bloquear o tráfego do modo Google AI.	Etapa 4.1. Na GUI, navegue até Web Security Manager e escolha Access Policies. Etapa 4.2. Clique em Add Policy. Etapa 4.3. Digite Name para a nova política.  Etapa 4.4. (Opcional) Selecione o Perfil de identificação ao qual você precisa que essa política se aplique.

Etapa 4.5. Na seção Definição de membro da política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada.

Etapa 4.6. Selecione a categoria de URLque foi criada na Etapa 2.

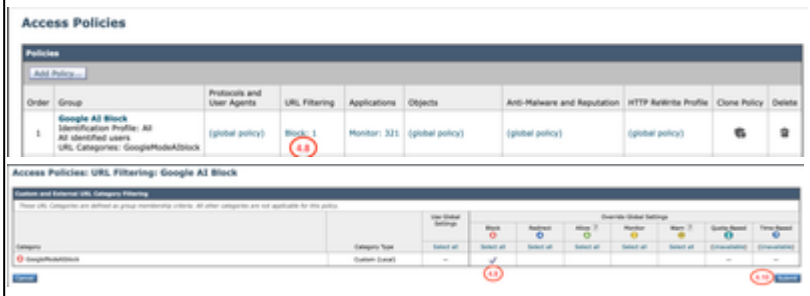
Etapa 4.7. Clique em Enviar.



Etapa 4.8. Na página Access Policies, clique no link de URL Filtering para a nova política.

Etapa 4.9. Escolha Block como a ação para Custom URL Category.

Etapa 4.10. Clique em Enviar.



Etapa 4.11. Confirmar alterações.

Verificar

Quando as definições de configuração são concluídas, o tráfego do Google AI é processado nos logs de acesso como Bloquear, pois é detectado pela Categoria personalizada que criamos para o Bloqueio do Google AI.

<#root>

```
1779219170.427 101 10.184.103.26
```

TCP_DENIED_SSL/403

```
 0 GET https://www.google.com:443/search?q=cisco+live+&sca_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo
```

BLOCK_CUSTOMCAT_12-Google_AI_Block

```
-ciscotest-NONE-NONE-NONE-NONE-NONE <"C_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_srch"
```

Uma solicitação para uma consulta de pesquisa pelo modo Google AI está bloqueada e exibe esta Notificação de usuário final.

Todo o tráfego restante do Google continua a ser permitido.

Informações Relacionadas

Definir categorias de URL personalizadas no WSA

Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance

Configurar certificado de descriptografia no aplicativo da Web seguro

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.