Bloquear o acesso a contas de consumidor do Google no SWA

Contents

Introdução

Este documento descreve o processo de bloqueio do acesso ao Google Workspace ou ao Google Consumer Accounts no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface gráfica do usuário (GUI) do SWA
- Acesso administrativo ao 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.

Configurar

<table>
<tr>
<td>Etapa 1.Crie uma categoria de URL personalizada para os sites do Google.</td>
<td>Etapa 1.1. Na GUI, navegue até Web Security Manager e escolha Custom e External URL Categories.

Etapa 1.2. Clique em Add Category 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:

<code>.google.com</code>

Etapa 1.5. Envie as alterações.

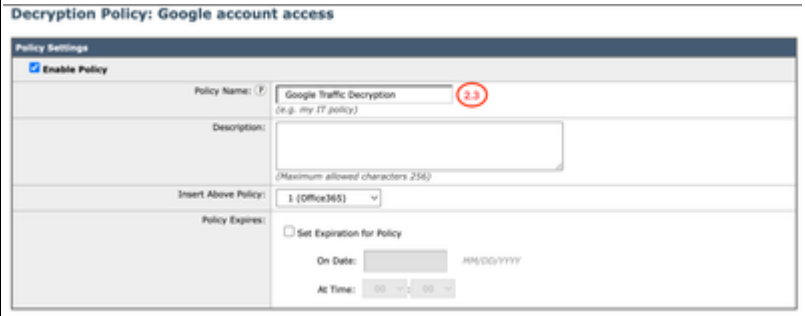
 

Imagem - Categoria de URL personalizada

Tip: Para obter mais informações sobre como configurar categorias de URL personalizadas, visite: Configure categorias de URL personalizadas no Secure Web Appliance.</td>
</tr>
<tr>
<td>Etapa 2.Descriptografar o tráfego.</td>
<td>Etapa 2.1. Na GUI, navegue paraWeb Security Manager e escolhaPolíticas de descriptografia.</td>
</tr>
</table>

Etapa 2.2. Clique em Add Policy.

Etapa 2.3. EnterName para a nova política.



Etapa 2.4. Selecione oPerfil de identificação ao qual você precisa que essa política se aplique.

Tip: Se tiver ignorado as Autenticações para URLs da Microsoft e estiver configurando esta política para Todos os usuários, escolha: Todos os perfis de identificação > Todos os usuários.

Etapa 2.5. Na seção FromPolicy Member Definition, clique nos links URL Categoriespara adicionar a Categoria de URL personalizada.

Etapa 2.6.Selecione a categoria de URL que foi criada na Etapa 1.

Etapa 2.7.Clique em Submit.

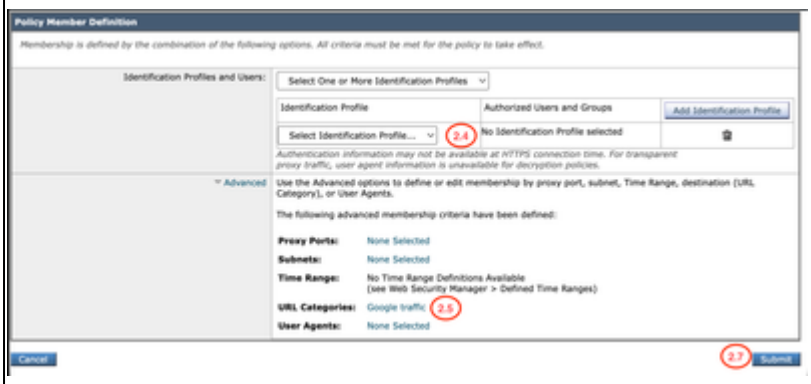
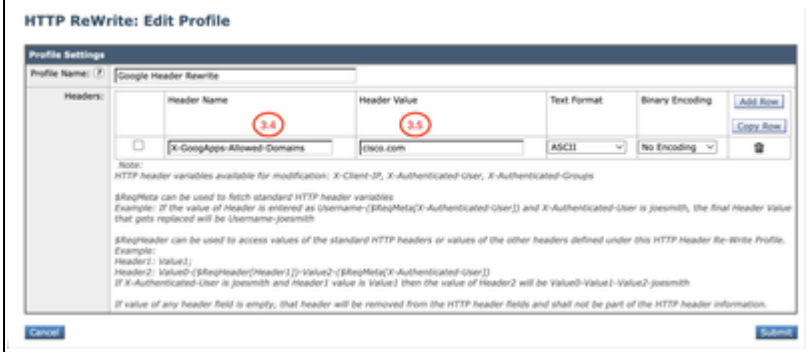
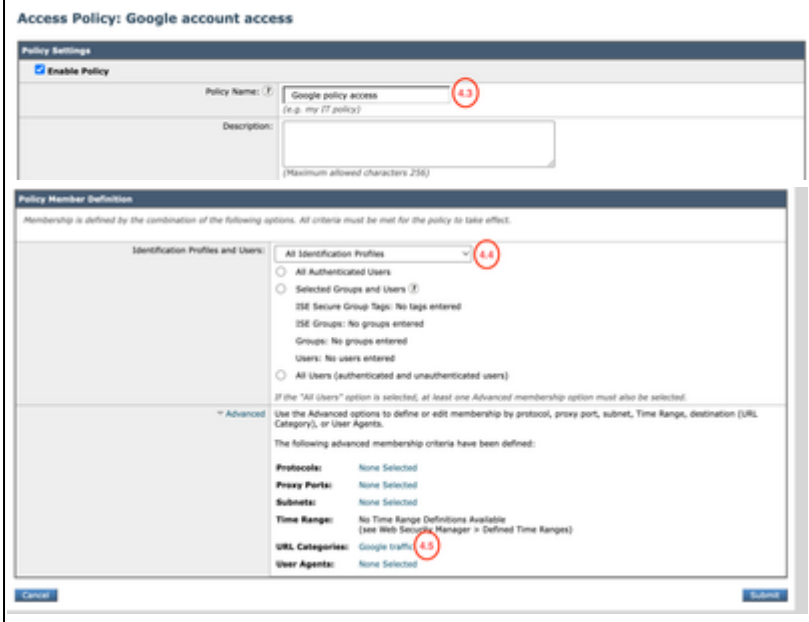
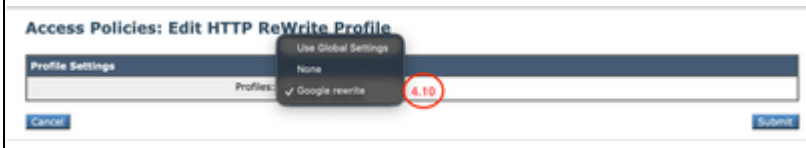


Imagem - Configurar política de descriptografia

Etapa 2.8. Na página InDecryption Policies, clique no link fromURL Filtering para obter a nova política.

	Imagem - Editar ação de filtragem de URL Etapa 2.9. Escolha Descriptografar como a ação para Categoria de URL Personalizada. Etapa 2.10.Clique em Enviar.  Imagem - Descriptografar a categoria de URL personalizada
Etapa 3.Criar perfil de regravação HTTP.	Etapa 3.1.Na GUI, navegue paraWeb Security Manager e escolhaHTTP ReWrite Profiles. Etapa 3.2. Clique em Adicionar perfil. Etapa 3.3. EnterName para o novo perfil. Etapa 3.4. Use X-GoApps-Allowed-Domains para o nome do cabeçalho. Etapa 3.5. Para a configuração Restrict-Access-To-Tenants, use um valor de domínio da lista de espaços permitidos, que deve ser uma lista separada por vírgulas dos espaços que os usuários têm permissão para acessar. Etapa 3.9.Clique em Enviar.  Imagem - Adicionar perfil de regravação HTTP

Etapa 4.Criar política de acesso.	Etapa 4.1. Na GUI, navegue paraWeb Security Manager e escolhaAccess Policies. Etapa 4.2. Clique em Add Policy. Etapa 4.3. EnterName para a nova política. Etapa 4.4. (Opcional) Selecione oPerfil de identificação ao qual você precisa que essa política se aplique. Etapa 4.5.Na seção Definição de membro de política, clique nos links URL Categoriespara adicionar a Categoria de URL personalizada. Etapa 4.6.Selecione a URL Category que foi criada na Etapa 1. Etapa 4.7. Clique em Enviar.  Imagem - Criar política de acesso Etapa 4.8.Na página Políticas do InAccess, verifique se a ação da Filtragem de URL está definida como Monitor. Etapa 4.9.Clique no link em HTTP ReWrite Profile para adicionar o Perfil do Cabeçalho HTTP a esta política.  Imagem - Propriedades da política de acesso Etapa 4.10. Escolha os perfis de regravação HTTP, criados

	na Etapa [3].  Imagem - Adicionar perfil de regravação HTTP Etapa 4.11. Clique em Enviar. Etapa 4.12. CommitChanges.

Relatórios e registros

Logs

Você pode adicionar campos personalizados aos logs de acesso ou aos logs W3C para exibir o nome do perfil de regravação do cabeçalho HTTP.

Especificador de Formato em Logs de Acesso	Campo Log nos Logs W3C	Descrição
%]	x-http-rewrite-profile-name	Nome do perfil de regravação do cabeçalho HTTP.

Você pode gerar o relatório de Rastreamento da Web para exibir os relatórios do tráfego pelo nome da Política de acesso.

Siga estas etapas para gerar os relatórios:

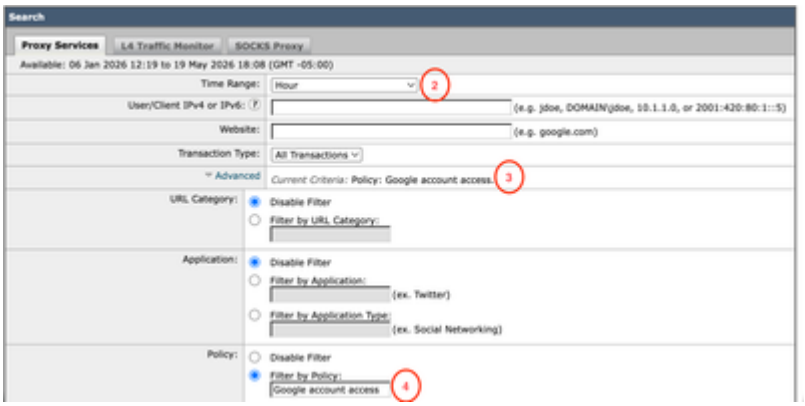
Etapa 1. Na GUI, selecioneReporting e escolhaWeb Tracking.

Etapa 2. Escolha o intervalo de tempo desejado.

Etapa 3. Clique no link Avançado para pesquisar transações usando critérios avançados.

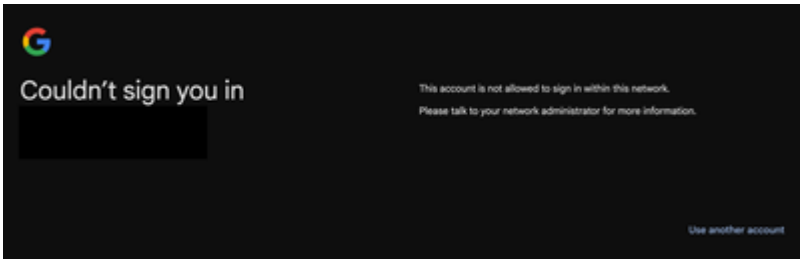
Etapa 4. Na seção Política, selecione Filtrar por política e digite o nome da Política de acesso que foi criada anteriormente.

Etapa 5. Clique em Pesquisar para revisar o relatório.



Verificar

Quando a configuração de restrição de domínio do Google é concluída, o usuário só pode acessar as contas que estão sob o domínio configurado no perfil Header Rewrite na Etapa 3. Se o usuário tentar acessar uma conta em um domínio diferente, ou uma conta diferente, pessoal, do Google, o acesso é restrito com este aviso:



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]

[Regravação de Cabeçalho HTTP WSA]

[Bloquear acesso a contas de consumidor (Documentação do Google)]

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.