

# Bloquear o tráfego no Secure Web Appliance

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Bloqueio de tráfego](#)

[Motivos para bloquear por fonte](#)

[Motivos para bloquear por destino](#)

[Etapas para bloquear o tráfego](#)

[Bloqueando sites usando expressões regulares na implantação de proxy transparente](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve as etapas para bloquear o tráfego no Secure Web Appliance (SWA).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.

A Cisco recomenda que você:

- SWA físico ou virtual instalado.
- 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.

## Bloqueio de tráfego

Bloquear o tráfego na SWA é uma etapa crucial para garantir a segurança da rede, manter a conformidade com políticas internas e proteger contra atividades mal-intencionadas. Aqui estão alguns motivos comuns para bloquear o tráfego:

## Motivos para bloquear por fonte

- Inundação por um ou vários usuários: quando um ou mais usuários geram tráfego excessivo, ele pode sobrecarregar a rede, levando à degradação do desempenho e a possíveis interrupções do serviço.
- Acesso a Recursos Não Confiáveis por Aplicativos (Agentes de Usuário): Determinados aplicativos podem tentar acessar recursos não confiáveis ou potencialmente prejudiciais. O bloqueio desses agentes de usuário ajuda a evitar violações de segurança e vazamentos de dados.
- Restringindo o acesso à Internet para intervalos de IP específicos: alguns endereços IP ou intervalos possivelmente precisam ser restritos de acessar a Internet devido a políticas de segurança ou para evitar o uso não autorizado.
- Comportamento de tráfego suspeito: o tráfego que exibe padrões ou comportamentos incomuns que podem indicar atividade mal-intencionada ou ameaças à segurança deve ser bloqueado para proteger a rede.

## Motivos para bloquear por destino

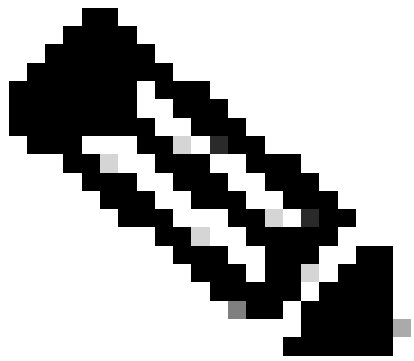
- Conformidade com as políticas internas da empresa: as organizações frequentemente têm políticas que restringem o acesso a determinados sites ou recursos on-line para garantir a produtividade e a conformidade com requisitos legais ou regulatórios.
- Sites não confiáveis: bloquear o acesso a sites considerados não confiáveis ou potencialmente prejudiciais ajuda a proteger os usuários contra phishing, malware e outras ameaças online.
- Comportamento mal-intencionado: sites conhecidos por hospedar conteúdo mal-intencionado ou participar de atividades mal-intencionadas devem ser bloqueados para evitar incidentes de segurança e violações de dados.

## Etapas para bloquear o tráfego

Em geral, há 3 etapas principais para bloquear o tráfego em SWA:

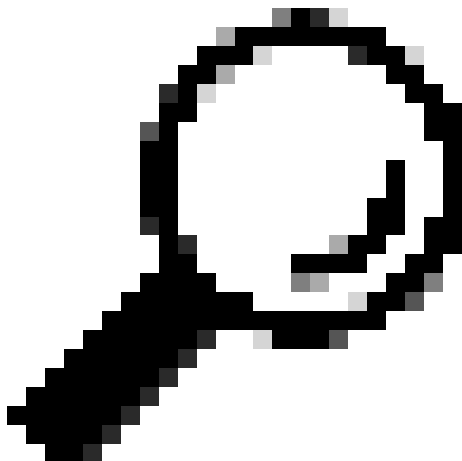
- Crie um perfil de identificação para o(s) usuário(s).
- Bloqueie o tráfego HTTPS na Política decriptografia.
- Bloqueie o tráfego HTTP na política de acesso.

Etapas	Bloquear o acesso de usuários específicos a qualquer site	Bloquear o acesso de usuários específicos a determinados sites da
--------	---	---

		Web
Categoria de URL Personalizada	Não aplicável.	<p>Crie uma Categoria de URL Personalizada para os sites que você planeja bloquear o acesso a eles.</p> <p>Para obter mais informações, visite:</p> <p><a href="#">Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco</a></p>
Perfil de identificação	<p>Etapa 1. Na GUI, escolha Web Security Manager e clique em Identification Profiles.</p> <p>Etapa 2. Clique em Add Profile para adicionar um perfil.</p> <p>Etapa 3. Use a caixa de seleção Enable Identification Profile para ativar esse perfil ou para desativá-lo rapidamente sem excluí-lo.</p> <p>Etapa 4. Atribua um Nome de perfil exclusivo.</p> <p>Etapa 5. (Opcional) Adicione Descrição.</p> <p>Etapa 6. Na lista suspensa Inserir acima, escolha onde esse perfil deve aparecer na tabela.</p> <p>Passo 7. Na seção Método de identificação do usuário, escolha Isento de autenticação/identificação.</p> <p>Etapa 8. Em Definir membros por sub-rede, insira os endereços IP ou sub-redes que este perfil de identificação deve aplicar. Você pode usar endereços IP, blocos de roteamento entre domínios sem classe (CIDR) e sub-redes.</p>	 <p>Observação: para bloquear o acesso de todos os usuários a determinados sites, não é necessário criar um perfil de ID separado. Isso pode ser gerenciado com eficiência por meio da Política global decriptografia/acesso.</p> <p>Etapa 1. Na GUI, escolha Web Security Manager e clique em Identification Profiles.</p> <p>Etapa 2. Clique em Add Profile para adicionar um perfil.</p> <p>Etapa 3. Use a caixa de seleção Enable Identification Profile para ativar esse perfil ou para desativá-lo rapidamente sem excluí-lo.</p> <p>Etapa 4. Atribua um Nome de perfil exclusivo.</p> <p>Etapa 5. (Opcional) Adicione</p>

		<p>Descrição.</p> <p>Etapa 6. Na lista suspensa Inserir acima, escolha onde esse perfil deve aparecer na tabela.</p> <p>Passo 7. Na seção Método de identificação do usuário, escolha Isento de autenticação/identificação.</p> <p>Etapa 8. Em Definir membros por sub-rede, insira os endereços IP ou sub-redes que este perfil de identificação deve aplicar. Você pode usar endereços IP, blocos de roteamento entre domínios sem classe (CIDR) e sub-redes.</p> <p>Etapa 9. Clique em Avançado e adicione a Categoria de URL que você gostaria de bloquear o acesso a ela.</p>
Política decriptografia	<p>Etapa 1. Em GUI, escolha Web Security Manager e clique em Política de criptografia.</p> <p>Etapa 2. Clique em Add Policy para adicionar uma política de criptografia.</p> <p>Etapa 3. Use a caixa de seleção Enable Policy para habilitar essa política.</p> <p>Etapa 4. Atribua um nome de política exclusivo.</p> <p>Etapa 5. (Opcional) Adicione Descrição.</p> <p>Etapa 6. Na lista suspensa Inserir política acima, escolha a primeira política.</p> <p>Passo 7. Em Perfis de identificação e usuários, escolha o Perfil de identificação que você criou nas etapas anteriores.</p> <p>Etapa 8. Enviar.</p>	<p>Etapa 1. Em GUI, escolha Web Security Manager e clique em Política de criptografia.</p> <p>Etapa 2. Clique em Add Policy para adicionar uma política de criptografia.</p> <p>Etapa 3. Use a caixa de seleção Enable Policy para habilitar essa política.</p> <p>Etapa 4. Atribua um nome de política exclusivo.</p> <p>Etapa 5. (Opcional) Adicione Descrição.</p> <p>Etapa 6. Na lista suspensa Inserir política acima, escolha a primeira política.</p> <p>Passo 7. Em Perfis de identificação e usuários, escolha o Perfil de identificação que você criou nas etapas anteriores.</p> <p>Etapa 8. Enviar.</p>

Etapa 9. Na página Políticas de descryptografia, em Filtragem de URL, clique no link associado a esta nova política de descryptografia.



Dica: como você está bloqueando todas as categorias de URL, pode otimizar a política removendo Categorias de URL personalizadas e usando apenas as categorias de URL predefinidas. Isso reduz a carga de processamento no SWA, evitando a etapa adicional de correspondência de URLs com categorias de URL personalizadas.

Etapa 10. Selecione Eliminar como a ação para cada categoria de URL.

Etapa 11. Na mesma página, role para baixo até Uncategorized URLs e escolha Drop na lista suspensa.

Etapa 12. Enviar.

#### Decryption Policies

Policies						
Add Policy						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Block All Decryption Policy Identification Profile: Blocked User All identified users	Drop: 100	(global policy)	(global policy)		

Imagem - Política de Descryptografia para Bloquear Todos os Sites para Determinados Usuários

Etapa 9. Na página Políticas de descryptografia, em Filtragem de URL, clique no link associado a esta nova política de descryptografia.


Etapa 10. Selecione Eliminar como a ação para a categoria de URL personalizada criada para os sites bloqueados.

Etapa 11. Clique em Submit.

#### Decryption Policies

Policies						
Add Policy						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Block Some URLs Decryption Policy Identification Profile: ID profile Block some URL All identified users	Drop: 1	(global policy)	(global policy)		

Imagem - Bloquear alguns URLs na política de descryptografia

<p>Política de acesso</p>	<p>Etapa 1. Em GUI, escolha Web Security Manager e clique em Access Policy.</p> <p>Etapa 2. Clique em Adicionar política para adicionar uma política de acesso.</p> <p>Etapa 3. Use a caixa de seleção Enable Policy para habilitar essa política.</p> <p>Etapa 4. Atribua um nome de política exclusivo.</p> <p>Etapa 5. (Opcional) Adicione Descrição.</p> <p>Etapa 6. Na lista suspensa Inserir política acima, escolha a primeira política.</p> <p>Passo 7. Em Perfis de identificação e usuários, escolha o Perfil de identificação que você criou nas etapas anteriores.</p> <p>Etapa 8. Enviar.</p> <p>Etapa 9. Na página Access Policies, em Protocols and User Agents, clique no link associado a esta nova Access Policy.</p> <p>Etapa 10. Na lista suspensa Edit Protocols and User Agents Settings, escolha Define Custom Settings.</p> <p>Etapa 11. IN Bloquear Protocolos selecione a opção caixa de seleção para ambos FTP sobre HTTP e HTTP.</p> <p>Etapa 12. IN HTTP CONNECT Ports, remova todos os números de porta para bloquear todas as portas.</p>	<p>Etapa 1. Em GUI, escolha Web Security Manager e clique em Access Policy.</p> <p>Etapa 2. Clique em Adicionar política para adicionar uma política de acesso.</p> <p>Etapa 3. Use a caixa de seleção Enable Policy para habilitar essa política.</p> <p>Etapa 4. Atribua um nome de política exclusivo.</p> <p>Etapa 5. (Opcional) Adicione Descrição.</p> <p>Etapa 6. Na lista suspensa Inserir política acima, escolha a primeira política.</p> <p>Passo 7. Em Perfis de identificação e usuários, escolha o Perfil de identificação que você criou nas etapas anteriores.</p> <p>Etapa 8. Enviar.</p> <p>Etapa 9. Na página Access Policies, em URL Filtering, clique no link associado a esta nova Access Policy</p> <p>Etapa 10. Selecione Block como a ação para a categoria de URL personalizada criada para os sites bloqueados.</p> <p>Etapa 11. Enviar.</p> <p>Etapa 12. Confirmar alterações.</p>  <p>Imagem - Bloquear alguns URLs na política de acesso</p>
---------------------------	--	--

**Access Policies: Protocols and User Agents: AP Blocked**

Define Custom Settings

**Protocol Controls**

Block Protocols:  FTP over HTTP  
 HTTP

Note: Blocking of HTTPS is not available in Access policies when the HTTPS proxy is enabled. If the HTTPS proxy is enabled, use Observation policies to control HTTPS access.

HTTP CONNECT Ports: /

Enter 1-65535 to allow all ports via HTTP CONNECT. Leave field blank to block all ports.

**Custom User Agents**

Block Custom User Agents:

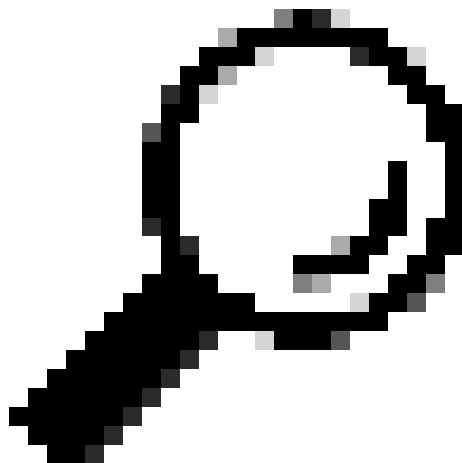
Example User Agent Patterns

(Enter any regular expression, one regular expression per line, to block user agents. Maximum allowed characters 2048.)

Imagem - Protocolos de bloqueio e portas de conexão na política de acesso

Etapa 13. Enviar.

Etapa 14. (Opcional) Na página Access Policies, em URL Filtering, clique no link associado a esta nova Access Policy e selecione Bloquear como a ação para cada categoria de URL e a URLs sem categoria e, em seguida, Enviar.



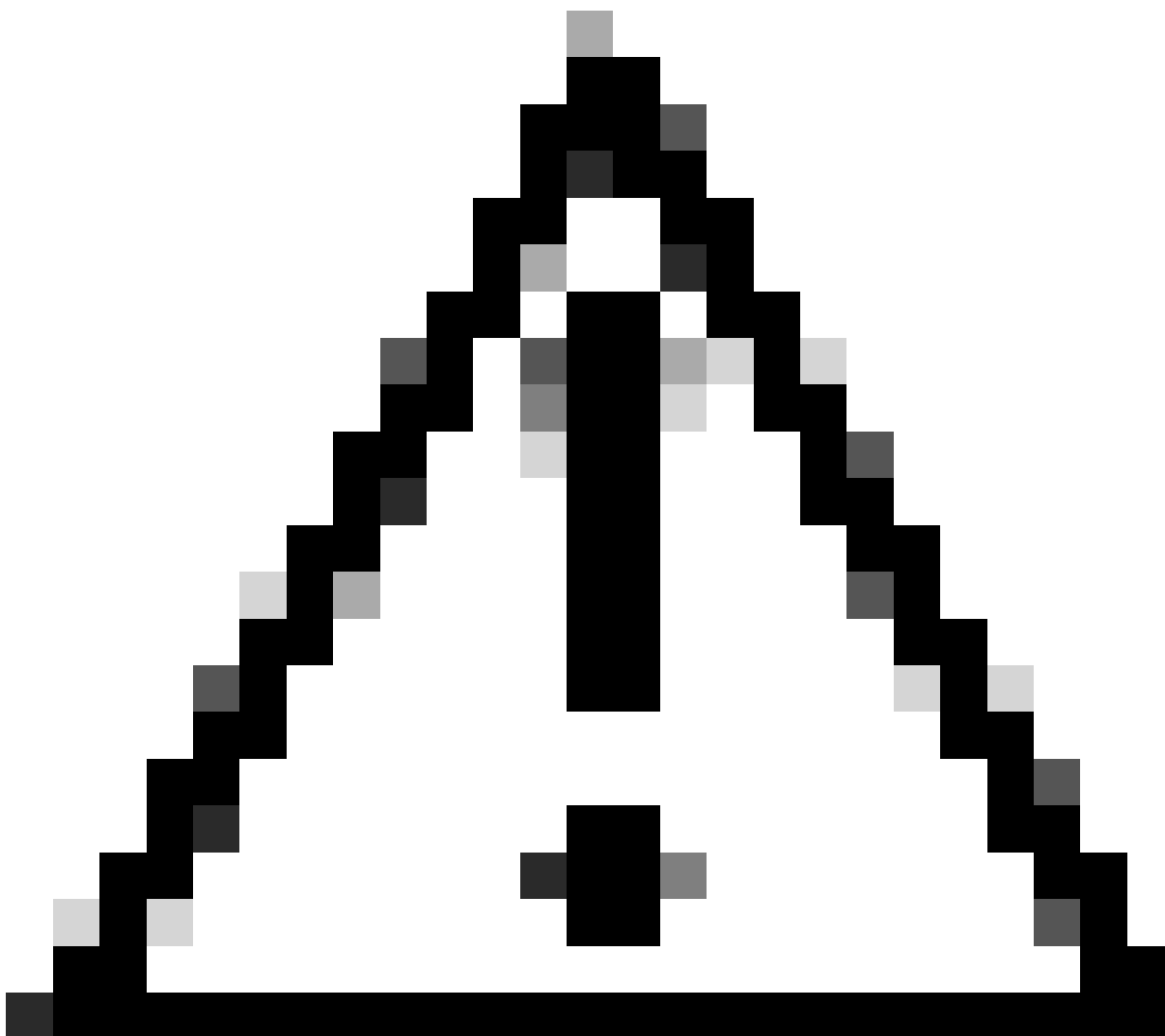
Dica: como você está bloqueando todas as categorias de URL, pode otimizar a política removendo Categorias de URL personalizadas e usando apenas as categorias de URL predefinidas. Isso reduz a carga de processamento no SWA, evitando a etapa adicional de correspondência de URLs com categorias de URL personalizadas.

## Etapa 16. Confirmar alterações.

### Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP Response Profile	Class Policy	Delete	
1	Blocked Access Policy	Blocked user All Identifier users	Block: 2 Protocols	Block: 108	Block: 15 Members: 24	(global policy)	Web Reputation: Enabled Secure Engines: Enabled Network: Enabled Malware: Enabled Sophos: Enabled	(global policy)		

Imagem - Política de acesso para bloquear todos os sites



Cuidado: na implantação de proxy transparente, o SWA não pode ler agentes de usuário ou a URL completa para tráfego HTTPS, a menos que o tráfego seja criptografado. Como resultado, se você configurar o Perfil de identificação usando Agentes de usuário ou uma Categoria de URL personalizada com expressões regulares, esse tráfego não corresponderá ao Perfil de identificação.

## Bloqueando sites usando expressões regulares na implantação



## de proxy transparente

Na implantação de proxy transparente, se você estiver planejando bloquear uma Categoria de URL personalizada que tenha condição de Expressões regulares - por exemplo, você está bloqueando o acesso a alguns canais do YouTube - você pode usar estas etapas:

Etapa 1. Crie uma Categoria de URL Personalizada para o site principal. (Neste exemplo: YouTube.com).

Etapa 2. Crie uma política de descryptografia, atribua esta categoria de URL personalizada e defina a ação como Descryptografar.

Etapa 3. Crie uma política de acesso, atribua a categoria de URL personalizada com as expressões regulares (neste exemplo, a categoria de URL personalizada para os canais do YouTube) e defina a ação como Block (Bloquear).

## Informações Relacionadas

- [Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - GD \(General Deployment\) - Classifique os usuários finais para aplicação de política \[Cisco Secure Web Appliance\] - Cisco](#)
- [Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco](#)
- [Como isentar o tráfego do Office 365 da autenticação e descryptografia no Cisco Web Security Appliance \(WSA\) - Cisco](#)

## 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.