

Definir categorias de URL personalizadas no WSA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Permitir URLs](#)

[Criar uma nova URL personalizada](#)

[Edite a Política de Acesso Global](#)

[Bloquear URLs](#)

[Criar uma nova URL personalizada](#)

[Edite a Política de Acesso Global](#)

Introduction

Este documento descreve como você pode definir categorias de URL personalizadas que funcionam no Web Security Appliance (WSA).

Contribuído por Shikha Grover e editado por Yeraldin Sanchez, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão inicial do Cisco Web Security Appliance

Componentes Utilizados

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

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A categoria em que um URL se enquadra é determinada por um banco de dados de categorias de

filtragem. O Web Security Appliance coleta informações e mantém um banco de dados separado para cada mecanismo de filtragem de URL. Os bancos de dados das categorias de filtragem recebem atualizações periodicamente do servidor de atualização da Cisco e são mantidos pelo Cisco TALOS. Talos, o Security Intelligence and Research Group da Cisco, acompanha constantemente um amplo conjunto de atributos para avaliar conclusões sobre um determinado host.

Pode haver situações em que você queira classificar um endereço de URL/ domínio/IP de forma diferente e tenha classificação personalizada local em sua caixa. Isso pode ser feito com categorias de URL personalizadas.

Quando o mecanismo de filtragem de URL corresponde uma categoria de URL à URL em uma solicitação de cliente, ele avalia primeiro a URL em relação às categorias de URL personalizadas incluídas no grupo de política. Se o URL na solicitação não corresponder a uma categoria personalizada incluída, o mecanismo de filtragem de URL o compara com as categorias de URL predefinidas.

Configurar

Permitir URLs

Se você confiar no site, poderá permitir o processo a seguir.

Criar uma nova URL personalizada

1. Crie uma nova categoria de URL personalizada, navegue para **GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name**: URLs permitidos.
2. Adicione os sites que deseja controlar na seção de sites (company.com..company.com).

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="Allowed URLs"/>
Comments: (?)	<input type="text"/>
List Order:	<input type="text" value="1"/>
Category Type:	Local Custom Category
Sites: (?)	<input type="text" value="company.com, .company.com"/> <small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com,)</small>
Advanced	Regular Expressions: (?) <input type="text"/> <small>Enter one regular expression per line.</small>

- 3.
4. Observe que "domain.com" só corresponderá a "domain.com", não a www.domain.com ou a "host.domain.com". Para permitir um site e todos os subdomínios, serão necessárias duas entradas na seção "sites": ". domain.com, domain.com".
5. Clique em Submit.

Edite a Política de Acesso Global

1. Abra **Web Security Manager > Access Policies > Global Policy > URL Filtering**.
2. Clique em **Selecionar categorias personalizadas**.
3. Clique na seta suspensa **URLs permitidos**, escolha Incluir na política e clique em **Aplicar**.
4. Coloque uma marca de seleção na caixa para Permitir.
5. Clique em **Enviar e Confirmar alterações**.

Access Policies: URL Filtering: Global Policy

Category	Category Type	Block	Redirect	Allow (?)	Monitor	Warn (?)	Quota-Based	Time-based
Allowed URLs	Custom (Local)	Select all	Select all	Select all	Select all	Select all		

Bloquear URLs

Se você não confia no site, pode bloqueá-lo com o seguinte processo.

Criar uma nova URL personalizada

1. Crie uma nova categoria de URL personalizada, navegue para **GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name: URLs bloqueadas**.
2. Adicione os sites que deseja controlar na seção de sites (company.com, .company.com).

Custom and External URL Categories: Edit Category

Category Name:

Comments:

List Order:

Category Type: Local Custom Category

Sites: [Sort URLs](#)
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced: Regular Expressions:
Enter one regular expression per line.

3. Observe que "domain.com" só corresponderá a "domain.com", não a www.domain.com ou a "host.domain.com". Para bloquear um site e todos os subdomínios, serão necessárias duas entradas na seção "sites": ". domain.com, domain.com".
4. Clique em Submit.

Edite a Política de Acesso Global

1. Abra **Web Security Manager > Access Policies > Global Policy > URL Filtering**.

2. Clique em **Selecionar categorias personalizadas...**
3. Clique na seta suspensa **URLs bloqueados**, escolha Incluir na política e clique em **Aplicar**.
4. Coloque uma marca de seleção na caixa para Bloquear.
5. Clique em **Enviar e Confirmar alterações**.

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering								
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.								
Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
<input checked="" type="checkbox"/> Blocked URLs	Custom (LOCK)	Select all	Select all	Select all	Select all	Select all		

[Select Custom Categories...](#)

Observação: as alterações acima podem ser feitas em qualquer política de acesso e não apenas na Política Global. O mesmo procedimento pode ser aplicado às políticas de descryptografia.

Consulte este [guia](#) para obter um caso de uso amplamente implantado.