

Bloquear download de arquivo executável em SWA

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antes de Começar](#)

[Configuration Steps](#)

[Validação do bloqueio de extensão de arquivo](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o processo de configuração do Secure Web Appliance (SWA) para bloquear o download de arquivos executáveis.

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.

Antes de Começar

O Cisco SWA pode efetivamente bloquear o download de arquivos executáveis inspecionando o tipo MIME (Multipurpose Internet Mail Extensions) do conteúdo da Web. Ao identificar tipos de arquivos, como application/x-msdownload, application/x-msi e outros tipos MIME relacionados, o

SWA aplica políticas que impedem que o executável seja entregue aos usuários. Além da detecção de tipo MIME, o SWA pode aproveitar a filtragem de extensão de arquivo, a análise baseada em reputação e as regras de política personalizadas para fortalecer ainda mais a proteção contra downloads indesejados ou arriscados. Esses recursos ajudam as empresas a manter um ambiente de navegação seguro e reduzir o risco de infecções por malware.



Tip: O SWA não pode identificar o tipo MIME do arquivo, a menos que o tráfego seja descriptografado.

application/octet-stream é um tipo MIME genérico usado para indicar que um arquivo contém dados binários. Ele não especifica a natureza do arquivo, portanto, pode ser usado para qualquer arquivo que não se ajuste a um tipo MIME mais específico. Esse tipo é geralmente atribuído a arquivos executáveis, instaladores e outros arquivos não texto quando o servidor Web não pode determinar um tipo mais preciso.

Configuration Steps

Etapa 1. Crie uma categoria de URL personalizada para o site.

Etapa 1.1. Na GUI, navegue até Web Security Manager e escolha Custom and External URL Categories.

Etapa 1.2. Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada.

Etapa 1.3. Digite o nome da nova categoria.

Etapa 1.4. Defina o domínio e/ou subdomínios do site que você está tentando bloquear o tráfego de upload (Neste exemplo, cisco.local e todos os seus subdomínios).

Etapa 1.5. Envie as alterações.

Custom and External URL Categories: Edit Category

The screenshot shows the 'Edit Custom and External URL Category' interface. It includes the following elements:

- Category Name:** A text input field with the value 'Category' and a red circle '1' next to it.
- Comments:** A text area with a help icon (?)
- List Order:** A numeric input field with the value '1'.
- Category Type:** A dropdown menu set to 'Local Custom Category'.
- Sites:** A text area containing 'cisco.local, .cisco.local' and a red circle '2' next to it. A 'Sort URLs' button is located to the right of this field.
- Regular Expressions:** A text area with a help icon (?) and a note: 'Enter one regular expression per line. Maximum allowed characters 2048.'
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom.

Imagem - Criar categoria de URL personalizada

	Tip: Para obter mais informações sobre como configurar categorias de URL personalizadas, acesse: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Etapa 2.Descriptografar o tráfego do URL	Caution: A descriptografia de um grande número de URLs pode prejudicar o desempenho. Etapa 2.1. Na GUI, navegue até Web Security Manager e escolha Políticas de descriptografia Etapa 2.2.Clique em Add Policy. Etapa 2.3.EnterName para a nova política. Etapa 2.4.(Opcional) Selecione oPerfil de identificação ao qual essa política se aplica. Tip: (Opcional) Se quiser aplicar a diretiva a todos os usuários, mesmo que eles não estejam autenticados, escolha Todos os usuários (usuários autenticados e não autenticados). Etapa 2.5.Na seção Definição de membro de política, 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.

Decryption Policy: DecryptingTraffic

Policy Settings

☒ **Enable Policy**

Policy Name: (e.g. my IT policy) 1

Description:

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

☒ All Authenticated Users

☐ Selected Groups and Users (?)

Groups: No groups entered

Users: No users entered

☐ All Users (authenticated and unauthenticated users) 2

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: 2

User Agents: None Selected

Imagem - Criar uma política de descryptografia

Etapla 2.8.Na página Políticas de descryptografia, clique no link daFiltragem de URL para obter a nova política.

Decryption Policies

Policies						
Add Policy...						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DecryptingTraffic Identification Profile: All All identified users URL Categories: Category	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		
Edit Policy Order...						

Imagem - Selecione a filtragem de URL

Etapla 2.9.Escolha Descryptografar como a ação para Categoria de URL Personalizada.

Etapla 2.10.Clique em Enviar.

Decryption Policies: URL Filtering: DecryptingTraffic

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	Use Global Settings	Override Global Settings				
			Pass Through	Monitor	Decrypt	Drop (?)	Quota-Based
Category	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)
					☒		

Imagem - Definir descritografia como ação

Etapa 3.1. Na GUI, navegue até Web Security Manager e escolha Access Policies.

Etapa 3.2. Clique em Add Policy.

Etapa 3.3. Enter Name para a nova política.

Etapa 3.4. (Opcional) Selecione o Perfil de identificação ao qual você precisa que essa política se aplique.



Tip: (Opcional) Se quiser aplicar a diretiva a todos os usuários, mesmo que eles não estejam autenticados, escolha Todos os usuários (usuários autenticados e não autenticados).

Etapa 3.5. Na seção Definição de membro de 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. Bloquear os arquivos executáveis

Access Policy: Block Exec

Policy Settings

☒ Enable Policy

Policy Name:
(e.g. my IT policy)

Description:
(Maximum allowed characters 256)

Insert Above Policy:

Policy Expires:

☐ Set Expiration for Policy

On Date:
At Time:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

☒ All Authenticated Users
☐ Selected Groups and Users ?
Groups: No groups entered
Users: No users entered

☐ All Users (authenticated and unauthenticated users)

☒ Advanced

If the "All Users" option is selected, at least one Advanced membership option must also be selected.

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols:

Proxy Ports:

Subnets:

Time Range:

URL Categories:

User Agents:

Imagem - Política de acesso



Tip: Para fins de geração de relatórios, é melhor escolher um nome que não seja igual a nenhuma outra política de acesso/descriptografia.

Etapa 3.8. Na página Políticas do InAccess, verifique se a ação de filtragem de URL está definida como Monitorar.

Etapa 3.9. Na página Políticas do InAccess, clique no link de Objetos para a nova política.

Access Policies

Policies									
Add Policy...									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	Block Exec Identification Profile: All All identified users URL Categories: Category	(global policy)	Monitor: 1	Monitor: 325	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 325	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		
Edit Policy Order...									

Imagem - Selecionar os Objetos

Imagem - Selecione a filtragem de URL

Etapa 3.10. No menu suspenso, escolha Definir configurações de bloqueio de objetos personalizados.

Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

☒ Use Global Policy Objects Blocking Settings

☐ Define Custom Objects Blocking Settings

☐ Disable Object Blocking for this Policy

HTTP/HTTPS Max Download Size: No Maximum

FTP Max Download Size: No Maximum

Block Object Type

Not Defined

Custom MIME Types

Block Custom MIME Types: Not Defined

[Cancel](#) [Submit](#)

Imagem - Definir objetos personalizados

Etapa 3.11. Clique em Código Executável para selecionar os tipos de Objetos que deseja bloquear.

Etapa 3.12. Clique em Installers para selecionar os tipos de Objetos que deseja bloquear.

Etapa 3.13. Além disso, você pode inserir os tipos MIME dos

arquivos que deseja bloquear na seção Tipos MIME Personalizados.

Access Policies: Objects: Block Exec

Imagem - Configurando Objetos a Serem Bloqueados



Tip: Para exibir a lista de tipos de MIME, clique em Referência de Tipo de Objeto e MIME.

Etapa 3.14.Envia.

Etapa 3.15.Confirmar alterações.

Validação do bloqueio de extensão de arquivo

Neste exemplo, quando um usuário tenta fazer download de um arquivo executável, esta página de aviso é exibida:

Política de acesso	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup- NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",ns,0,"- ",0,0,0,-,"-,-,-,-,"-,-,-,-,"-,-,-,-,"nc",-,"-,-,-,-,"- ","Desconhecido","Desconhecido",-,"-,-",0.00,0,- ,"Desconhecido",-,"-,-
--------------------	---

Informações Relacionadas

- [Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Guia de instalação do Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco](#)
- [Use as práticas recomendadas de dispositivos da Web seguros](#)
- [Configurar firewall para dispositivo seguro da Web](#)
- [Configurar certificado de descryptografia no aplicativo da Web seguro](#)
- [Configurar e solucionar problemas de SNMP em SWA](#)
- [Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server](#)
- [Habilitar canal/vídeo específico do YouTube e bloquear o restante do YouTube no SWA](#)
- [Entender o formato do registro de acesso HTTPS no Secure Web Appliance](#)
- [Acessar logs do dispositivo da Web seguro](#)
- [Ignorar autenticação no Secure Web Appliance](#)
- [Bloquear o tráfego no Secure Web Appliance](#)
- [Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance](#)

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.