Configurar categorias de URL personalizadas no Secure Web Appliance

Contents

Introdução

Este documento descreve a estrutura de categorias de URL (Uniform Resource Locator) personalizadas, no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como o proxy funciona.
- Administração do Secure Web Appliance (SWA).

A Cisco recomenda que você:

- Dispositivo da Web seguro (SWA) físico ou virtual instalado.
- Licença ativada ou instalada.
- O assistente de instalação foi concluído.

- 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.

Categorias de URL personalizadas

O mecanismo de filtro de URL permite filtrar transações em Políticas de acesso, descriptografia e segurança de dados. Ao configurar categorias de URL para grupos de política, você pode configurar ações para categorias de URL personalizadas, se houver, e categorias de URL predefinidas.

Você pode criar categorias de URL de feed ao vivo personalizadas e externas que descrevem Nomes de host e Endereços IP específicos. Além disso, você pode editar e excluir categorias de URL.

Quando você inclui essas categorias de URL personalizadas no mesmo grupo Access, Decryption ou Cisco Data Security Policy e atribui ações diferentes a cada categoria, a ação da categoria de URL personalizada mais alta incluída tem precedência.

Observação: se o Sistema de Nome de Domínio (DNS) resolver vários IPs em um site e se um desses IPs for uma lista personalizada de bloqueados, o Web Security Appliance bloqueará o site para todos os IPs, independentemente de eles não estarem listados na lista personalizada de bloqueados.

Categorias de URL do Live-feed

As categorias de feeds ao vivo externos são usadas para extrair a lista de URLs de um site específico, por exemplo, para buscar URLs do Office 365 da Microsoft.

Se você selecionar Categoria de feed ao vivo externo para o Tipo de categoria ao criar e editar categorias de URL personalizadas e externas, deverá selecionar o formato de feed (Formato de feed da Cisco ou Formato de feed do Office 365) e, em seguida, fornecer uma URL para o servidor de arquivos de feed apropriado.

Aqui estão os formatos esperados para cada arquivo de feed:

- Formato de feed da Cisco - Deve ser um arquivo de valores separados por vírgula (.csv); isto é, um arquivo de texto com uma extensão .csv. Cada entrada no arquivo .csv deve estar em uma linha separada, formatada como tipo de endereço/vírgula/endereço (por exemplo: www.cisco.com,site ou ad2.*\.com,regex). Os tipos de endereço válidos são site e regex.

Aqui está um trecho de um arquivo .csv do formato de feed da Cisco:

```
www.cisco.com,site
\.xyz,regex
ad2.*\.com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Formato de Feed do Office 365 - Este é um arquivo XML localizado em um servidor do Microsoft Office 365 ou em um servidor local no qual você salvou o arquivo. Ele é fornecido pelo serviço do Office 365 e não pode ser modificado.

Os endereços de rede no arquivo estão delimitados por tags XML, esta estrutura: produtos > produto > lista de endereços > endereço. Na implementação atual, um "tipo de lista de endereços" pode ser IPv6, IPv4 ou URL [que pode incluir domínios e padrões de expressões regulares (regex)].

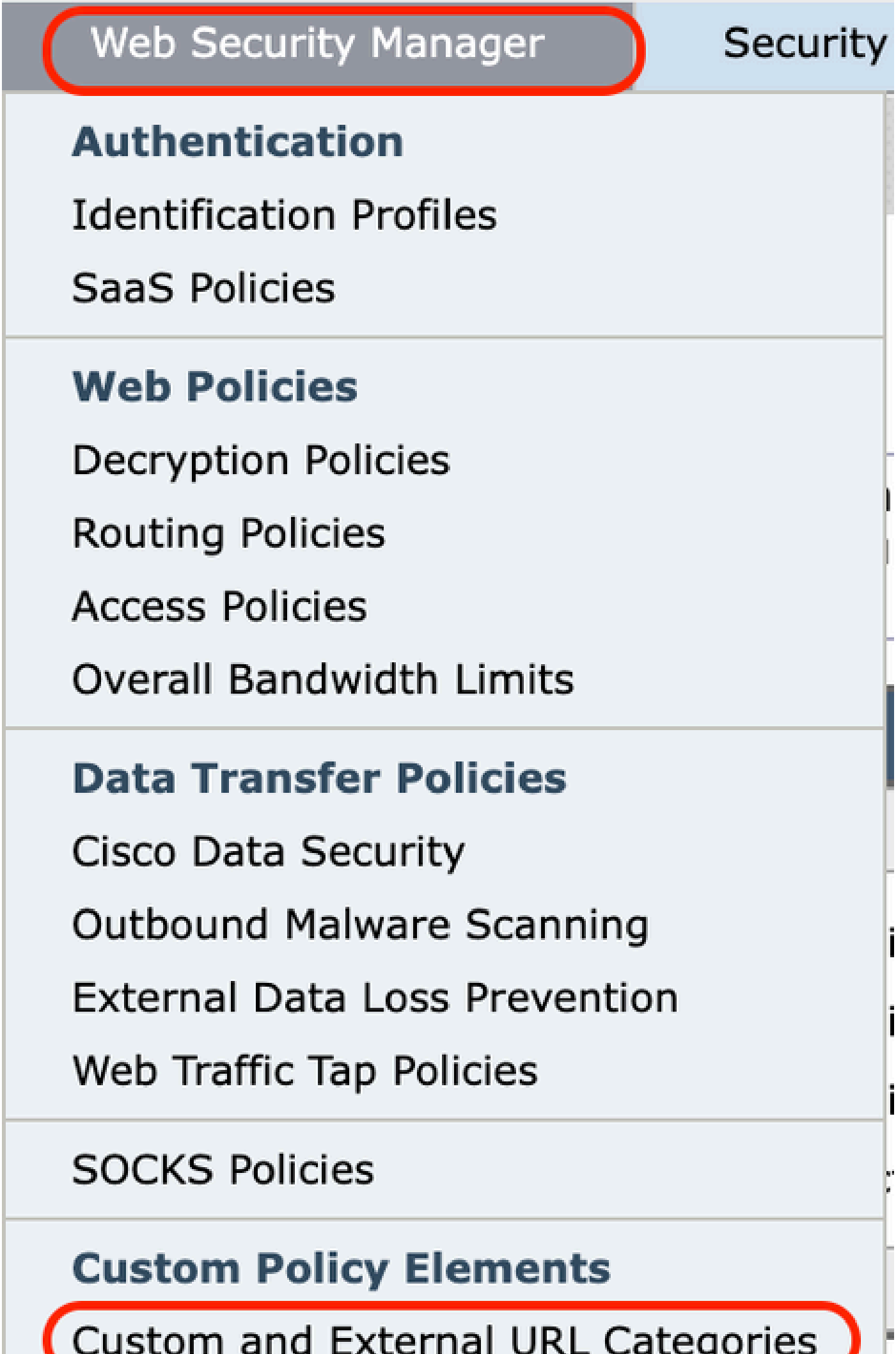
Aqui está um trecho de um arquivo de feed do Office 365:

```
<products updated="4/15/2016">
<product name="o365">
<addresslist type="IPv6">
<address>fc00:1040:401::d:80</address>
<address>fc00:1040:401::a</address>
<address>fc00:1040:401::9</address>
</addresslist>
<addresslist type="IPv4">
<address>10.71.145.72</address>
<address>10.71.148.74</address>
<address>10.71.145.114</address>
</addresslist>
<addresslist type="URL">
<address>*.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
<product name="LYO">
<addresslist type="URL">
<address>*.subdomain.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
</products>
```

Observação: não inclua http:// ou https:// como parte de qualquer entrada de site no arquivo, caso contrário ocorrerá um erro. Em outras palavras, www.cisco.com é analisado corretamente, enquanto http://www.cisco.com produz um erro

Etapas para criar categorias de URL personalizadas

Etapa 1. Escolha Web Security Manager > Categorias de URL personalizadas e externas.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

: Informe um identificador para esta categoria de URL. Esse nome aparece quando você configura o filtro de URL para grupos de política.

- Ordem da Lista: Especifique a ordem desta categoria na lista de categorias de URL personalizadas. Digite "1" para a primeira categoria de URL na lista.
  O mecanismo de filtro de URL avalia uma solicitação de cliente em relação às categorias de URL personalizadas na ordem especificada.

Observação: Quando o mecanismo de filtro de URL corresponde uma categoria de URL ao URL em uma solicitação de cliente, ele primeiro avalia o URL em relação às categorias de URL personalizadas incluídas no grupo de políticas. Se a URL na solicitação não corresponder a uma categoria personalizada incluída, o mecanismo de filtro de URL a comparará com as categorias de URL predefinidas. Se a URL não corresponder a nenhuma categoria de URL personalizada ou predefinida incluída, a solicitação não será categorizada.

- Tipo de categoria: selecione Categoria personalizada local ou Categoria externa de alimentação em tempo real.
- Tabela de Roteamento: Escolha Gerenciamento ou Dados. Essa opção estará disponível apenas se o "roteamento dividido" estiver ativado; isto é, não estará disponível com categorias personalizadas locais.

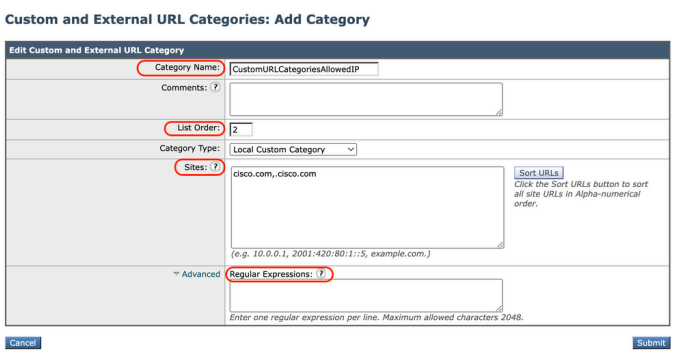
<table>
<tr>
<td> 

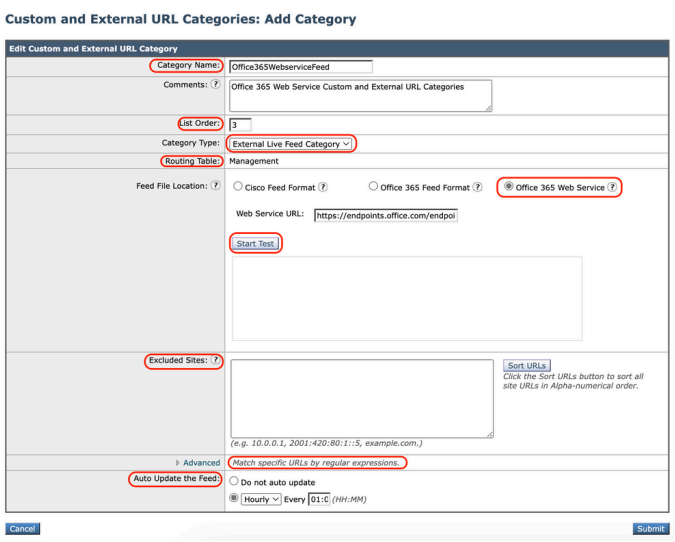
image- Categoria de URL personalizada local</td>
<td> 

Imagem - categoria de URL personalizada para configurar feeds</td>
</tr>
<tr>
<td>Categoria Personalizada Local</td>
<td>Categoria de Live Feed Externo</td>
</tr>
</table>

Definir Usar Expressões Regulares

O Secure Web Appliance usa uma sintaxe de expressão regular que difere um pouco da sintaxe de expressão regular usada por outras implementações do mecanismo de correspondência de padrão Velocity.

Além disso, o equipamento não suporta uma barra invertida para escapar de uma barra. Se você precisar usar uma barra em uma expressão regular, basta digitar a barra sem uma barra invertida.

Observação: Tecnicamente, o AsyncOS para Web usa o analisador de expressões regulares do Flex

Para testar suas expressões regulares, você pode usar este link: flex lint - Testador Regex/Depurador

Cuidado: expressões regulares que retornam mais de 63 caracteres falham e produzem um erro de entrada inválida. Certifique-se de formar expressões regulares que não tenham o potencial de retornar mais de 63 caracteres

Cuidado: expressões regulares que executam correspondência extensa de caracteres consomem recursos e podem afetar o desempenho do sistema. Por esse motivo, as expressões regulares podem ser aplicadas com cautela.

Você pode usar expressões regulares nestes locais:
· Personalizar categorias de URL para políticas de acesso. Ao criar uma categoria de URL personalizada para usar com grupos de política de acesso, você pode usar expressões regulares para especificar vários servidores Web que correspondam ao padrão inserido.
· Personalizar agentes de usuário para bloquear. Ao editar os aplicativos a serem bloqueados para um grupo de política de acesso, você pode usar expressões regulares para inserir agentes de usuário específicos a serem bloqueados.

Dica: não é possível definir o desvio de proxy da Web para expressões regulares.

Esta é a lista de classes de caracteres na expressão regular do Flex

Classes de caracteres	
.	qualquer caractere, exceto nova linha
\w \d \s	palavra, dígito, espaço em branco
\W \D \S	não palavra, dígito, espaço em branco
[abc]	qualquer um de a, b ou c
[^abc]	não a, b ou c
[a-g]	caractere entre a & g
Âncoras	
^abc$	início / fim da string
\b	limite de palavra
Caracteres de escape	
\. * \\	caracteres especiais de escape

\t \n \r	tabulação, avanço de linha, retorno de carro
\u00A9	© de escape unicode
Grupos e Consulta	
abc)	grupo de captura
\1	referência reversa para #1 de grupo
(?:abc)	grupo de não captura
?=abc)	visão positiva
?!abc)	visão antecipada negativa
Quantificadores e alteração	
a + a?	0 ou mais, 1 ou mais, 0 ou 1
a{5} a{2,}	exatamente cinco, dois ou mais
a {1,3}	entre um e três
a+? a{2,}?	corresponder o menor número possível
ab|cd	combinar ab ou cd

⚠ Cuidado: Tenha cuidado com pontos sem escape em padrões longos e, especialmente, no meio de padrões mais longos e tenha cuidado com esse metacaractere (Estrela *), especialmente em conjunto com o caractere de ponto. Qualquer padrão contém um ponto sem escape que retorna mais de 63 caracteres após o ponto ser desativado.
Sempre escape *(estrela) e . (ponto) com \ (barra invertida) como * e \.
Se usarmos .cisco.local na expressão regular, o domínio Xcisco.local também será uma correspondência.
O caractere sem escape afeta o desempenho e cria lentidão durante a navegação na Web. Isso ocorre porque o mecanismo de correspondência de padrões deve passar por milhares ou milhões de possibilidades até encontrar uma correspondência para a entrada correta, além disso, ele pode ter algumas preocupações de segurança em relação aos URLs semelhantes para as Políticas permitidas

Você pode usar a opção de interface de linha de comando (CLI) advancedproxyconfig > miscellaneous > Deseja habilitar a conversão de URL em minúsculas para velocity regex, para habilitar ou desabilitar a conversão de regex padrão em minúsculas para correspondências que não diferenciam maiúsculas de minúsculas. Use se tiver problemas com diferenciação de maiúsculas e minúsculas.

Limitações e preocupações com design

- Você pode usar no máximo 30 arquivos externos de Feed ao vivo nessas definições de categoria de URL, e cada arquivo deve conter no máximo 5000 entradas.
- Se o número de entradas de feed externas aumentar, isso causará degradação do desempenho.
- É possível usar o mesmo endereço em várias categorias de URL personalizadas, mas a ordem na qual as categorias são listadas é relevante.

Se você incluir essas categorias na mesma política e definir ações diferentes para cada uma, a ação definida para a categoria mais alta listada na tabela de categorias de URL personalizadas será aplicada.

- Quando uma solicitação de FTP nativa é redirecionada de forma transparente para o Proxy FTP, ela não contém informações de nome de host para o servidor FTP, apenas seu endereço IP.

Por causa disso, algumas categorias de URL predefinidas e filtros de reputação da Web que têm apenas informações de nome de host não correspondem às solicitações de FTP nativas, mesmo que as solicitações sejam destinadas a esses servidores.

Se desejar bloquear o acesso a esses sites, você deverá criar categorias de URL personalizadas para que eles usem seus endereços IP.

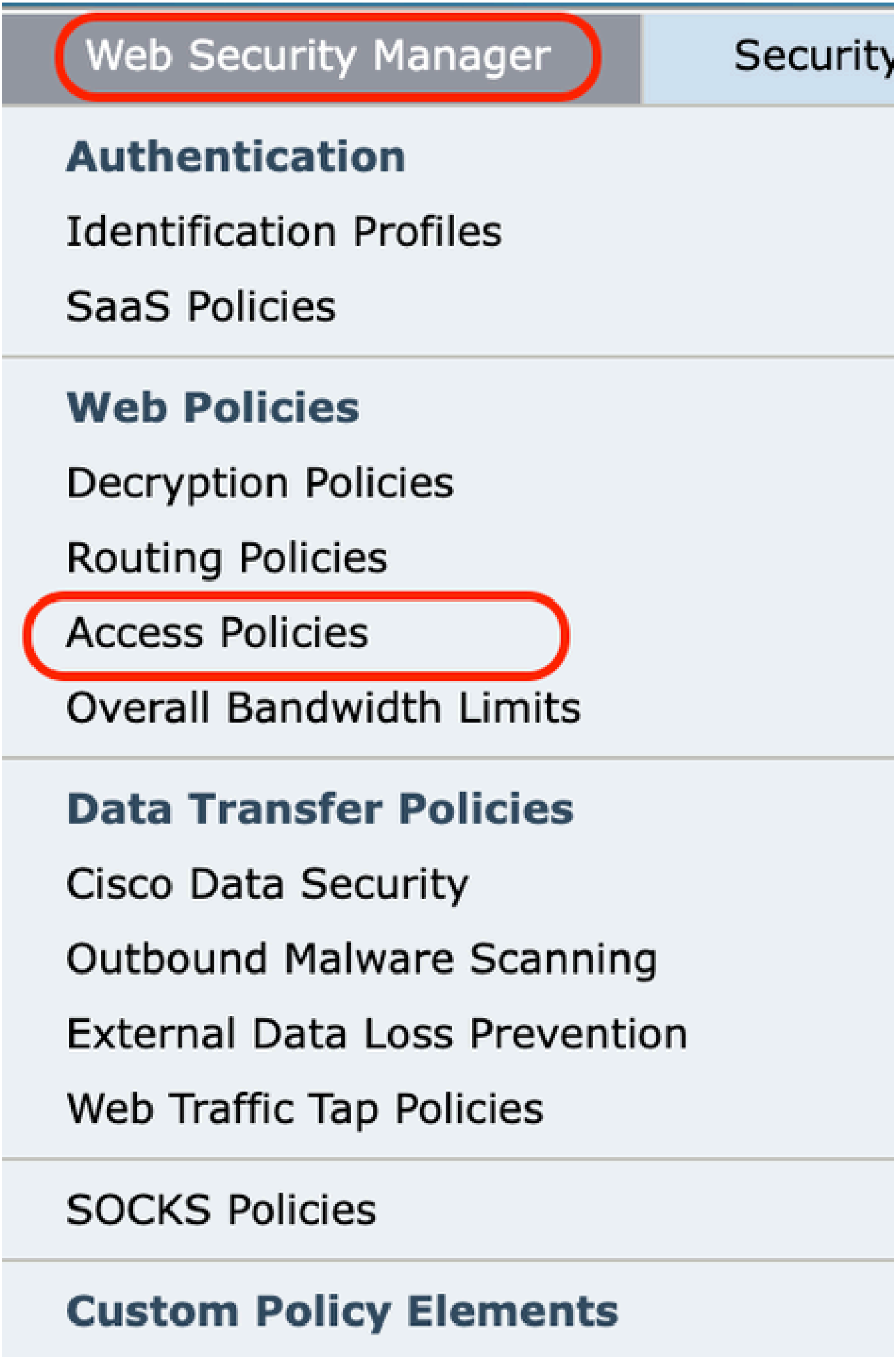
- Uma URL não categorizada é uma URL que não corresponde a nenhuma categoria de URL predefinida ou categoria de URL personalizada incluída

Usar Categorias de URL Personalizadas em Políticas

O mecanismo de filtro de URL permite filtrar transações em Políticas de acesso, descriptografia e segurança de dados. Ao configurar categorias de URL para grupos de política, você pode configurar ações para categorias de URL personalizadas, se houver, e categorias de URL predefinidas.

Etapas para configurar filtros de URL para política de acesso

Etapa 1. Escolha Web Security Manager > Access Policies.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

Clique no link na tabela de políticas na coluna Filtro de URL para o grupo de políticas que deseja editar.

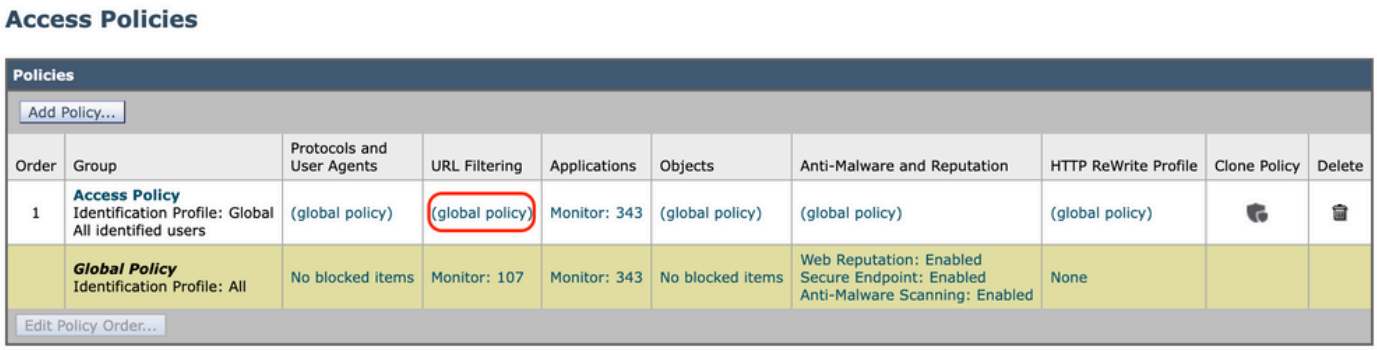
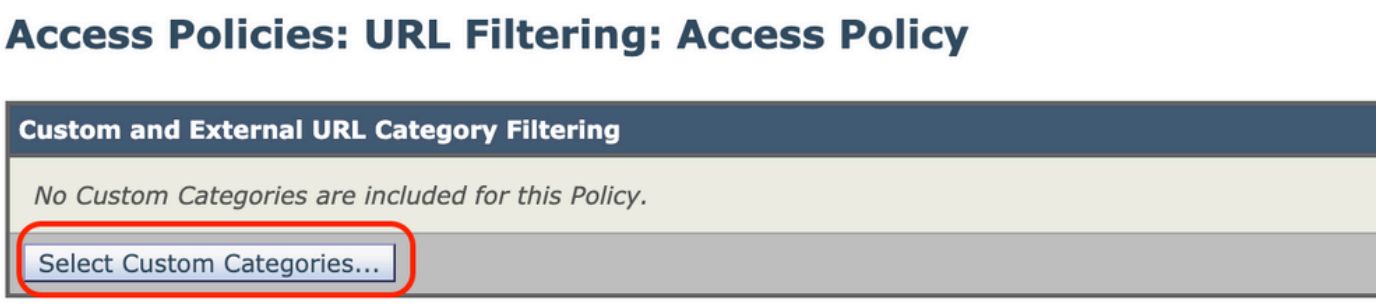


Imagem - Adicionar categoria personalizada à política de acesso

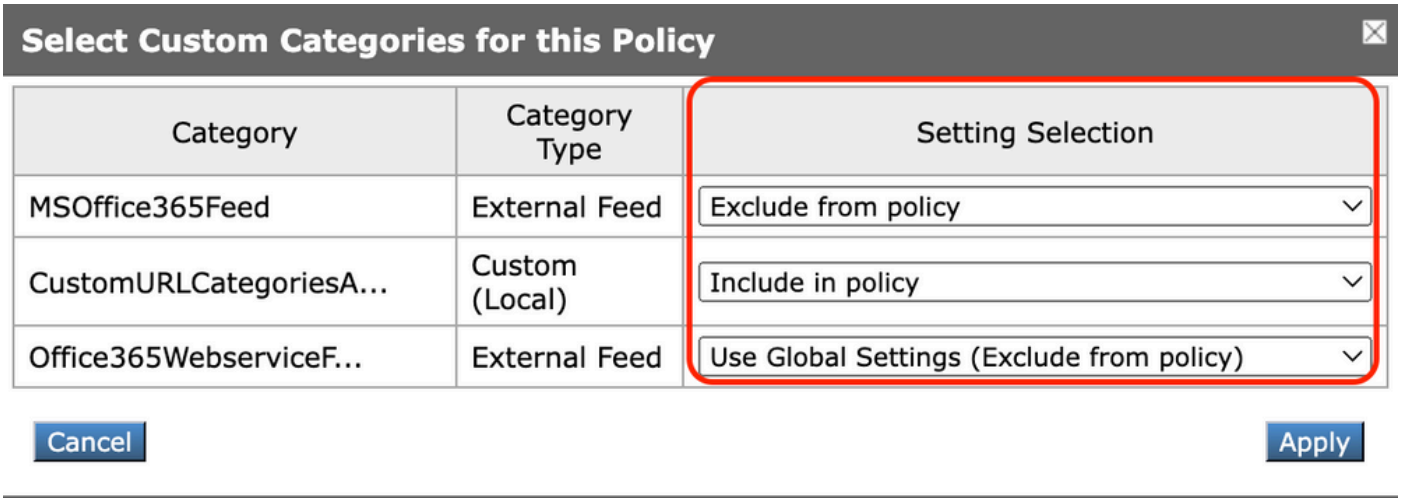
Etapa 3. (Opcional) Na seção Filtragem de categoria de URL personalizada, você pode adicionar categorias de URL personalizadas nas quais executar uma ação nesta política:

a) Clique em Select Custom Categories.



Categoria de URL personalizada de seleção de imagem

b) Escolha quais categorias de URL personalizadas incluir nesta política e clique em Aplicar.



Selecione categorias personalizadas para incluir na política

Escolha em quais categorias de URL personalizadas o mecanismo de filtro de URL deve comparar a solicitação do cliente.

O mecanismo de filtro de URL compara as solicitações do cliente com as categorias de URL personalizadas incluídas e ignora as categorias de URL personalizadas excluídas.

O mecanismo de filtro de URL compara o URL em uma solicitação de cliente com as categorias de URL personalizadas incluídas antes das categorias de URL predefinidas.

As categorias de URL personalizadas incluídas na política são exibidas na seção Personalizar filtragem de categorias de URL.

Etapa 4. Na seção Filtragem de categoria de URL personalizada, escolha uma ação para cada categoria de URL personalizada incluída.

Imagem - Escolher ação para categoria personalizada

Ação	Descrição
Usar configurações globais	Usa a ação para esta categoria no Grupo de Política Global. Esta é a ação padrão para grupos de política definidos pelo usuário. Aplica-se somente a grupos de políticas definidos pelo usuário.
Bloqueio	O Web Proxy nega transações que correspondam a essa configuração.
Redirecionar	Redireciona o tráfego originalmente destinado a um URL nesta categoria para um local que você especificar. Quando você escolhe essa ação, o campo Redirecionar para é exibido. Insira uma URL para a qual redirecionar todo o tráfego.
Permissão	Sempre permite solicitações de clientes para sites desta categoria. As solicitações permitidas ignoram todos os outros filtros e verificações de malware. Use esta configuração apenas para sites confiáveis. Você pode usar essa configuração para sites internos.
Monitor	O Web Proxy não permite nem bloqueia a solicitação. Em vez disso, ele continua a avaliar a solicitação do cliente em relação a outras configurações de controle de grupo de política, como o filtro de reputação da Web.

Ação	Descrição
Avisar	Inicialmente, o Web Proxy bloqueia a solicitação e exibe uma página de aviso, mas permite que o usuário continue clicando em um link de hipertexto na página de aviso.
Com base em cota	À medida que um usuário se aproxima das cotas de volume ou tempo especificadas, um aviso é exibido. Quando uma cota é atingida, uma página de bloqueio é exibida. .
Baseado no tempo	O Web Proxy bloqueia ou monitora a solicitação durante os intervalos de tempo especificados.

Etapa 5. Na seção Filtro de categoria de URL predefinido, escolha uma destas ações para cada categoria:

- Usar configurações globais
- Monitor
- Avisar
- Bloqueio
- Baseado no tempo
- Com base em cota

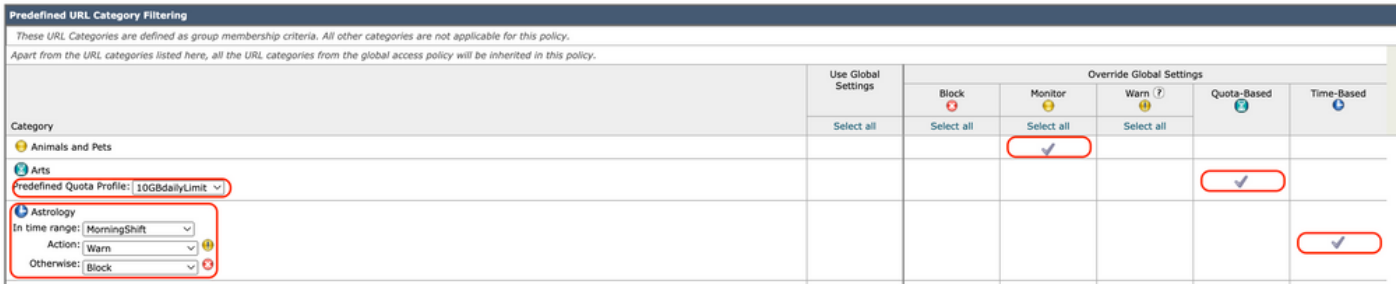


Imagem - Selecionar Ação para Categoria predefinida

Etapa 6. Na seção URLs sem categoria, escolha a ação a ser tomada para solicitações de clientes a sites que não se enquadram em uma categoria de URL predefinida ou personalizada. Essa configuração também determina a ação padrão para resultados de categorias novas e mescladas a partir de atualizações do conjunto de categorias de URL.

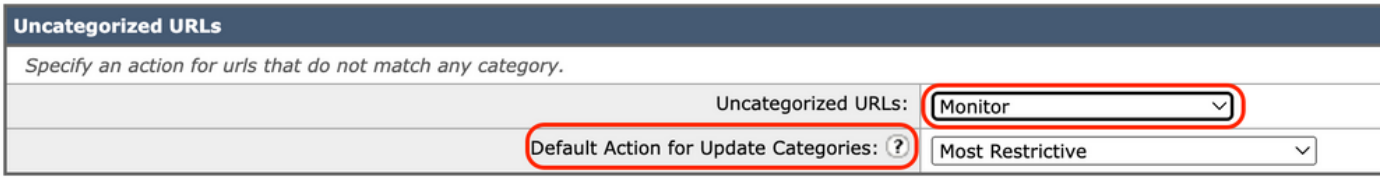
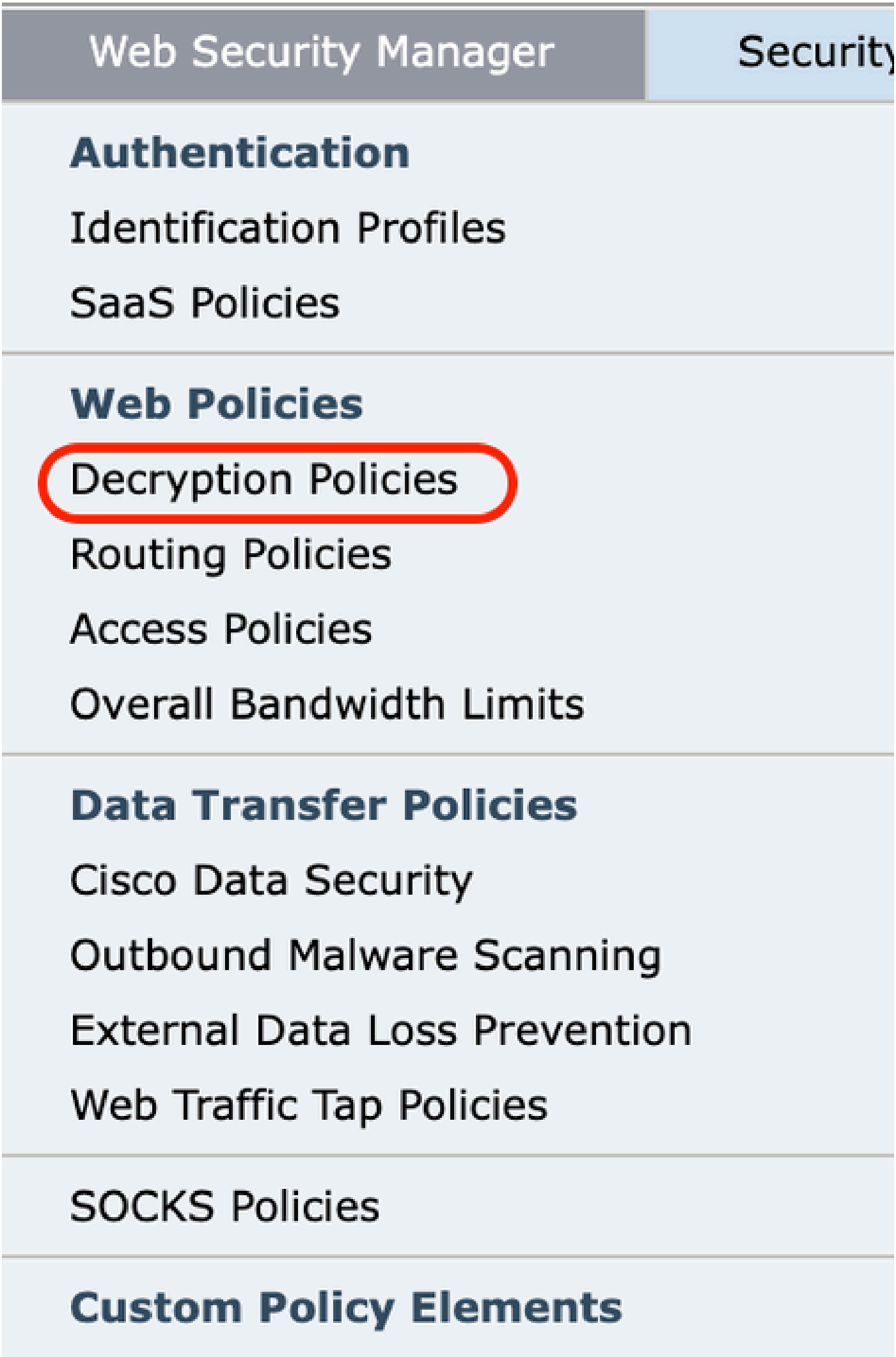


Imagem - Escolher ação para URL sem categoria

Passo 7. Enviar e confirmar alterações.

Etapas para Configurar Filtros de URL para Política de Descriptografia

Etapa 1. Escolha Web Security Manager > Políticas de descriptografia.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

Clique no link da tabela de políticas na coluna Filtragem de URL para o grupo de políticas que deseja editar.

Imagem - Escolher filtro de URL

Etapa 3. (Opcional) Na seção Personalizar filtragem de categoria de URL, você pode adicionar categorias de URL personalizadas nas quais tomar medidas nesta política:

a. Clique em Selecionar categorias personalizadas.

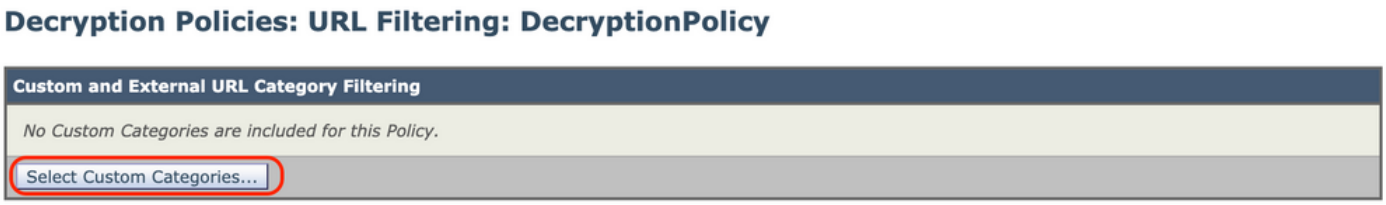
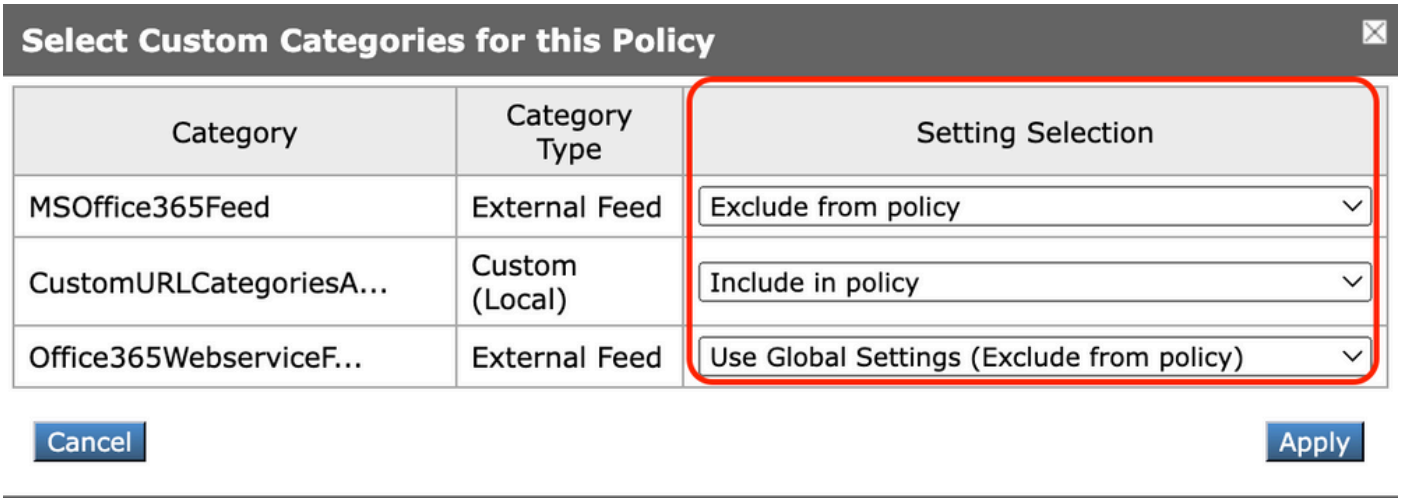


Imagem - Escolher categorias personalizadas

b. Escolha quais categorias de URL personalizadas incluir nesta política e clique em Aplicar.



Selecione categorias personalizadas para incluir na política

Escolha em quais categorias de URL personalizadas o mecanismo de filtro de URL deve comparar a solicitação do cliente.

O mecanismo de filtro de URL compara as solicitações do cliente com as categorias de URL personalizadas incluídas e ignora as categorias de URL personalizadas excluídas.

O mecanismo de filtro de URL compara o URL em uma solicitação de cliente com as categorias de URL personalizadas incluídas antes das categorias de URL predefinidas.

As categorias de URL personalizadas incluídas na política são exibidas na seção Personalizar filtragem de categorias de URL.

Etapa 4. Escolha uma ação para cada categoria de URL personalizada e predefinida.

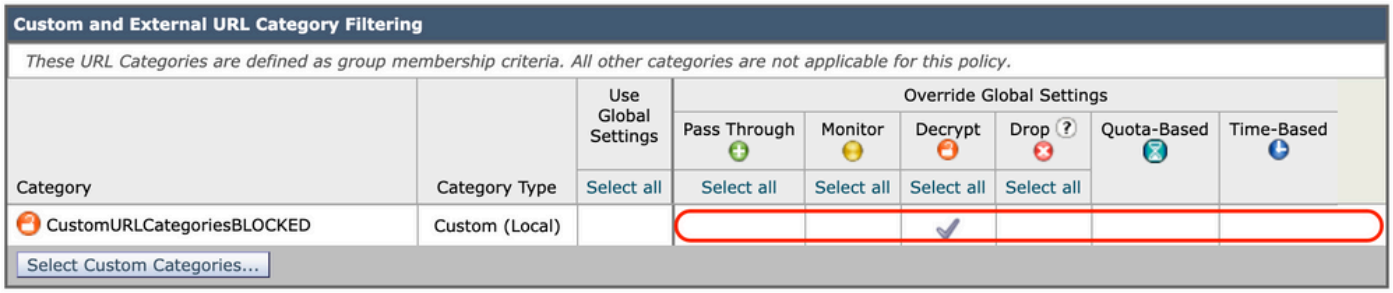


Imagem - Escolher Ação para Política de Descriptografia

Ação	Descrição
Usar configuração global	Usa a ação para esta categoria no grupo Política de descriptografia global. Esta é a ação padrão para grupos de política definidos pelo usuário. Aplica-se somente a grupos de políticas definidos pelo usuário. Quando uma categoria de URL personalizada é excluída da Política de descriptografia global, a ação padrão para categorias de URL personalizadas incluídas nas Políticas de descriptografia definidas pelo usuário é Monitorar em vez de Usar configurações globais. Não é possível escolher Usar configurações globais quando uma categoria de URL personalizada é excluída na Política de descriptografia global.
Passagem	Passa pela conexão entre o cliente e o servidor sem inspeção do conteúdo do tráfego.
Monitor	O Web Proxy não permite nem bloqueia a solicitação. Em vez disso, ele continua a avaliar a solicitação do cliente em relação a outras configurações de controle de grupo de política, como o filtro de reputação da Web.
Descriptografar	Permite a conexão, mas inspeciona o conteúdo do tráfego. O equipamento descriptografa o tráfego e aplica as Políticas de acesso ao tráfego descriptografado como se fosse uma conexão HTTP de texto simples. Quando a conexão é descriptografada e as políticas de acesso são aplicadas, você pode verificar o tráfego em busca de malware.

Ação	Descrição
Soltar	Descarta a conexão e não passa a solicitação de conexão ao servidor. O equipamento não notifica o usuário de que removeu a conexão.

Etapa 5. Na seção URLs sem categoria, escolha a ação a ser tomada para solicitações de clientes a sites que não se enquadram em uma categoria de URL predefinida ou personalizada.

Essa configuração também determina a ação padrão para resultados de categorias novas e mescladas a partir de atualizações do conjunto de categorias de URL.

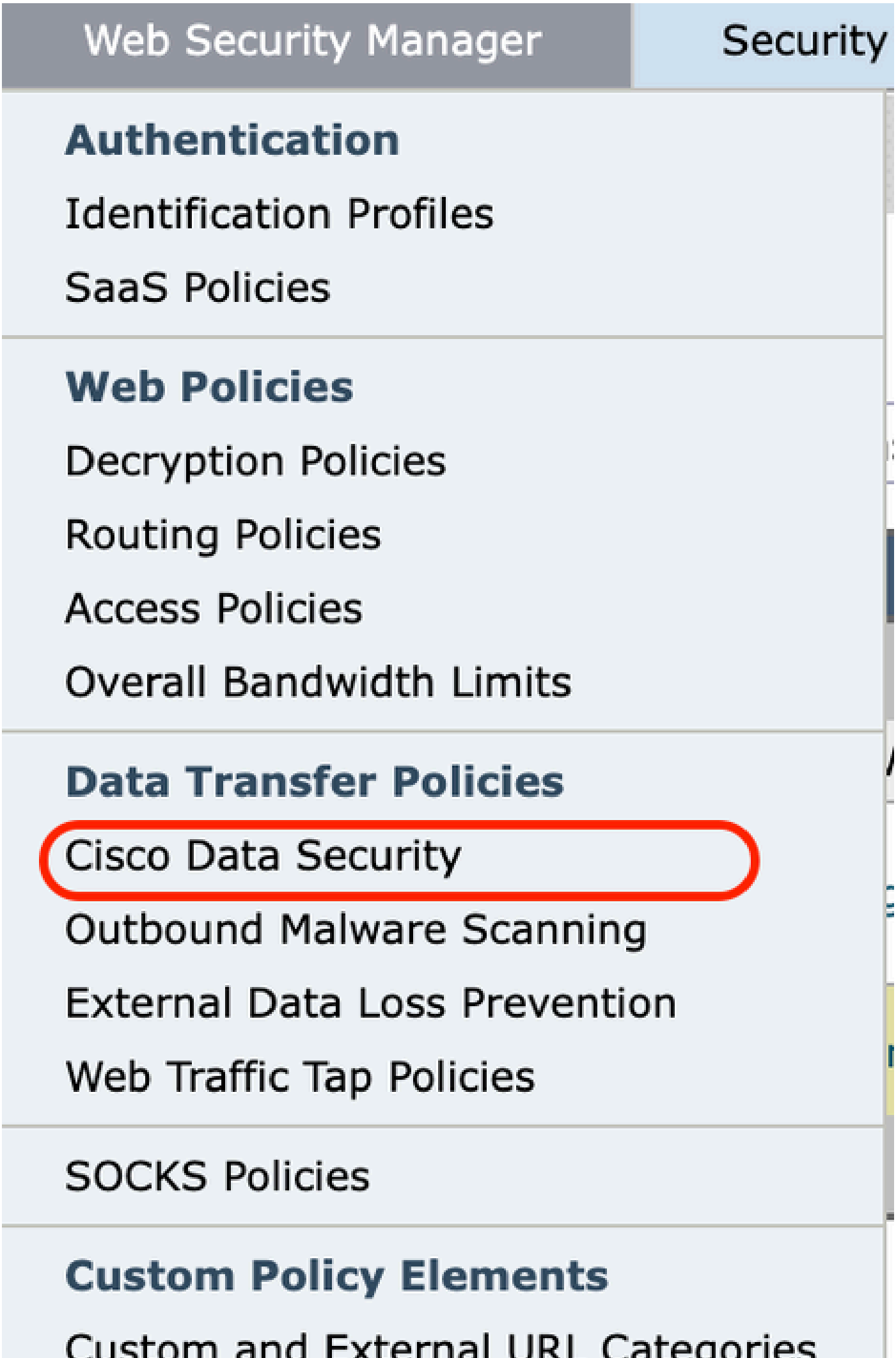
Imagem - Política de descriptografia não categorizada

Etapa 6. Enviar e confirmar alterações.

⚠ Cuidado: se você quiser bloquear uma categoria de URL específica para solicitações de protocolo HTTPS, opte por descriptografar essa categoria de URL no grupo de política de descriptografia e, em seguida, opte por bloquear a mesma categoria de URL no grupo de política de acesso.

Etapas para Configurar Filtros de URL para Grupos de Políticas de Segurança de Dados

Etapa 1. Escolha Web Security Manager > Cisco Data Security.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

Clique no link da tabela de políticas na coluna Filtragem de URL para o grupo de políticas que deseja editar.

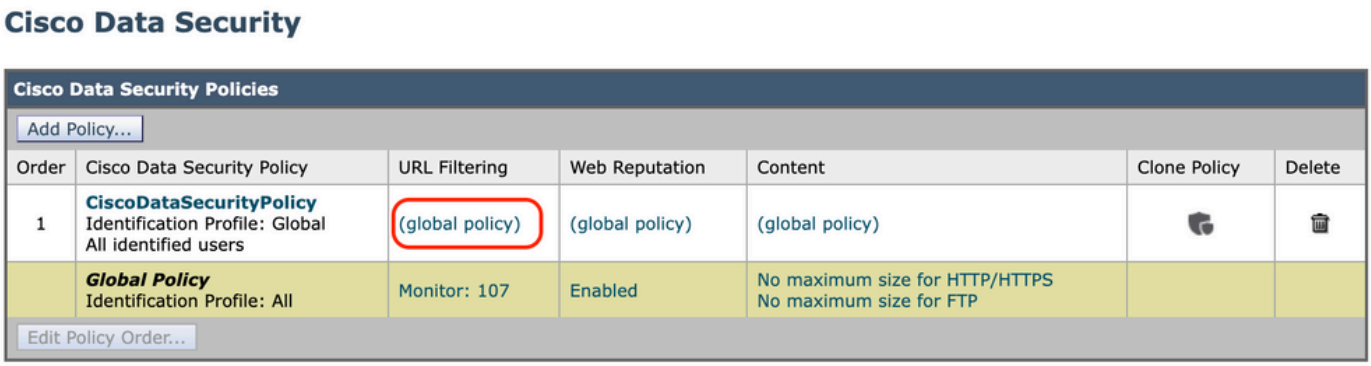


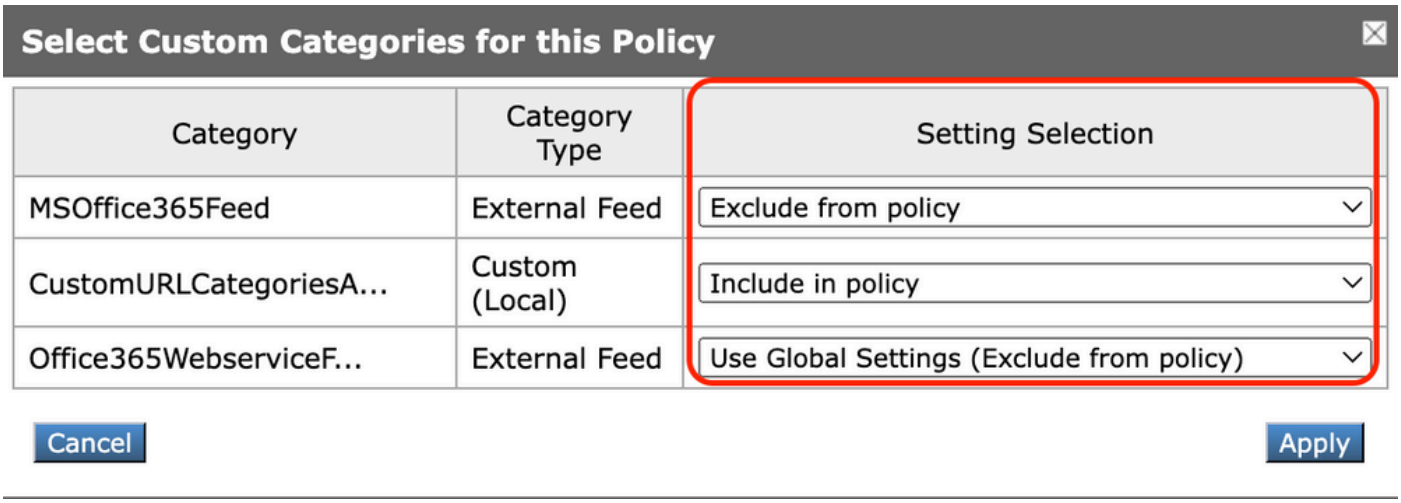
Imagem - Segurança de Dados - escolha o filtro de URL

Etapa 3. (Opcional) Na seção Personalizar filtragem de categoria de URL, você pode adicionar categorias de URL personalizadas nas quais tomar medidas nesta política:

a. Clique em Selecionar categorias personalizadas.

Imagem - Selecionar Campo Personalizado

b. Escolha quais categorias de URL personalizadas incluir nesta política e clique em Aplicar.



Selecione categorias personalizadas para incluir na política

Escolha em quais categorias de URL personalizadas o mecanismo de filtro de URL deve comparar a solicitação do cliente.

O mecanismo de filtro de URL compara as solicitações do cliente com as categorias de URL personalizadas incluídas e ignora as categorias de URL personalizadas excluídas.

O mecanismo de filtro de URL compara o URL em uma solicitação de cliente com as categorias

de URL personalizadas incluídas antes das categorias de URL predefinidas.

As categorias de URL personalizadas incluídas na política são exibidas na seção Personalizar filtragem de categorias de URL.

Etapa 4. Na seção Filtragem de categoria de URL personalizada, escolha uma ação para cada categoria de URL personalizada.

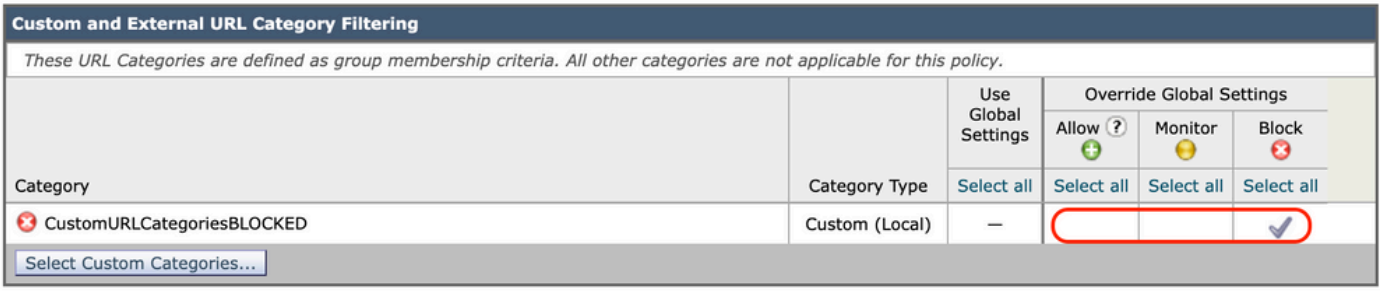


Imagem - Segurança de dados - Escolher ação

Ação	Descrição
Usar configuração global	Usa a ação para esta categoria no Grupo de Política Global. Esta é a ação padrão para grupos de política definidos pelo usuário. Aplica-se somente a grupos de políticas definidos pelo usuário. Quando uma categoria de URL personalizada é excluída na Política de segurança de dados global da Cisco, a ação padrão para categorias de URL personalizadas incluídas nas Políticas de segurança de dados da Cisco definidas pelo usuário é Monitorar em vez de Usar configurações globais. Você não pode escolher Usar configurações globais quando uma categoria de URL personalizada é excluída na Política de segurança de dados global da Cisco.
Permissão	Sempre permite solicitações de carregamento para sites desta categoria. Aplica-se somente a categorias de URL personalizadas. As solicitações permitidas ignoram todas as verificações de segurança de dados adicionais e a solicitação é avaliada em relação às Políticas de Acesso. Use esta configuração apenas para sites confiáveis. Você pode usar essa configuração para sites internos.
Monitor	O Web Proxy não permite nem bloqueia a solicitação. Em vez disso, ele continua a avaliar a solicitação de carregamento em relação a outras configurações de controle do grupo de políticas, como o filtro de reputação da Web.

Ação	Descrição
Bloqueio	O Web Proxy nega transações que correspondam a essa configuração.

Etapa 5. Na seção Filtragem predefinida de categorias de URL, escolha uma destas ações para cada categoria:

- Usar configurações globais
- Monitor
- Bloqueio

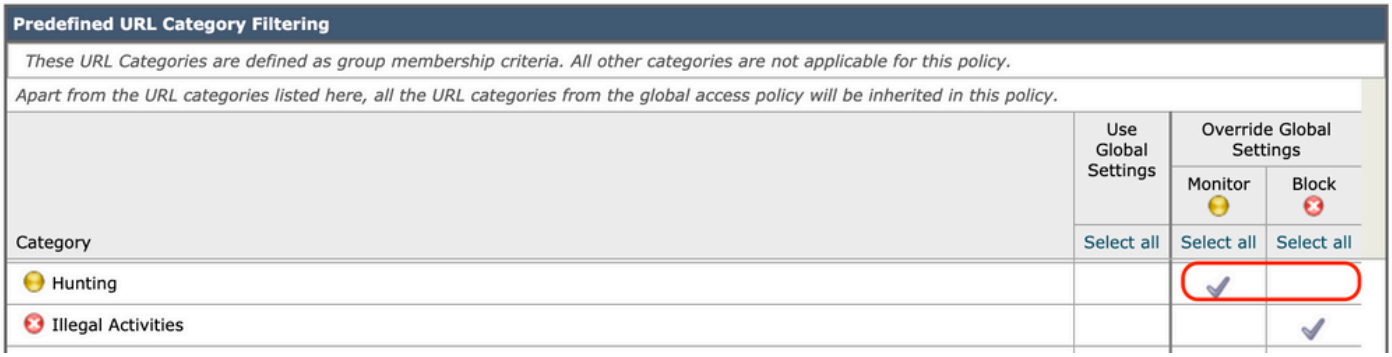


Imagem - Segurança de Dados URL Predefinida Escolher Ação

Etapa 6. Na seção URLs sem categoria, escolha a ação a ser tomada para solicitações de upload para sites que não se enquadram em uma categoria de URL predefinida ou personalizada.

Essa configuração também determina a ação padrão para resultados de categorias novas e mescladas a partir de atualizações do conjunto de categorias de URL.

Imagem - Segurança de dados não categorizada

Passo 7. Enviar e confirmar alterações.

⚠ Cuidado: se você não desativar a limitação de tamanho máximo de arquivo, o Web Security Appliance continuará a validar o tamanho máximo de arquivo quando as opções Permitir ou Monitorar forem selecionadas na filtragem de URL.

Etapas Para Configurar O Controle De Solicitações De Upload Com Categorias De URL Personalizadas

Cada solicitação de carregamento é atribuída a um grupo de políticas "Varredura de malware de saída" e herda as configurações de controle desse grupo de políticas.

Depois que o Web Proxy recebe os cabeçalhos de solicitação de upload, ele tem as informações necessárias para decidir se deve verificar o corpo da solicitação.

O mecanismo DVS verifica a solicitação e retorna um veredito ao Web Proxy. A página de bloqueio é exibida para o usuário final, se aplicável.

<table>
<tr><td>Passo 1</td><td>Escolha Web Security Manager > Varredura de malware de saída.</td></tr>
<tr><td>Passo 2</td><td>Na coluna Destinos, clique no link do grupo de políticas que deseja configurar.</td></tr>
<tr><td>Etapa 3</td><td>Na seção Edit Destination Settings, selecione "Define Destinations Scanning Custom Settings" no menu suspenso.</td></tr>
<tr><td>Passo 4</td><td>Na seção Destinos para varredura, selecione uma destas opções:
<table>
<tr><th>Opção</th><th>Descrição</th></tr>
<tr><td>Não verificar nenhum upload</td><td>O mecanismo DVS não verifica solicitações de upload. Todas as solicitações de upload são avaliadas em relação às Políticas de acesso</td></tr>
<tr><td>Verificar todos os carregamentos</td><td>O mecanismo DVS verifica todas as solicitações de upload. A solicitação de carregamento é bloqueada ou avaliada em relação às Políticas de Acesso, depende do veredito de verificação do mecanismo DVS</td></tr>
<tr><td>Verificar uploads em categorias de URL personalizadas especificadas</td><td>O mecanismo DVS verifica solicitações de upload que pertencem a categorias de URL personalizadas específicas. A solicitação de carregamento está bloqueada ou avaliada em relação às Políticas de acesso, depende do veredito de verificação do mecanismo DVS.

Clique em Editar lista de categorias personalizadas para selecionar as categorias de URL a serem verificadas</td></tr>
</table>
</td></tr>
<tr><td>Etapa 5</td><td>Envie suas alterações.</td></tr>
</table>

Etapa 6	Na coluna Filtragem Anti-Malware, clique no link do grupo de políticas.
Etapa 7	Na seção Configurações Anti-Malware, selecione Definir Configurações Personalizadas Anti-Malware.
Passo 8	Na seção Cisco DVS Anti-Malware Settings, selecione quais mecanismos de verificação antimalware devem ser habilitados para esse grupo de políticas.
Passo 9	Na seção Malware Categories, selecione se deseja monitorar ou bloquear as várias categorias de malware. As categorias listadas nesta seção dependem de quais mecanismos de varredura você ativa.
Passo 10	Enviar e confirmar alterações.

Etapas para Configurar Solicitações de Carregamento de Controle em Políticas de DLP Externo

Quando o Web Proxy recebe os cabeçalhos de solicitação de carregamento, ele tem as informações necessárias para decidir se a solicitação pode ir para o sistema DLP externo para verificação.

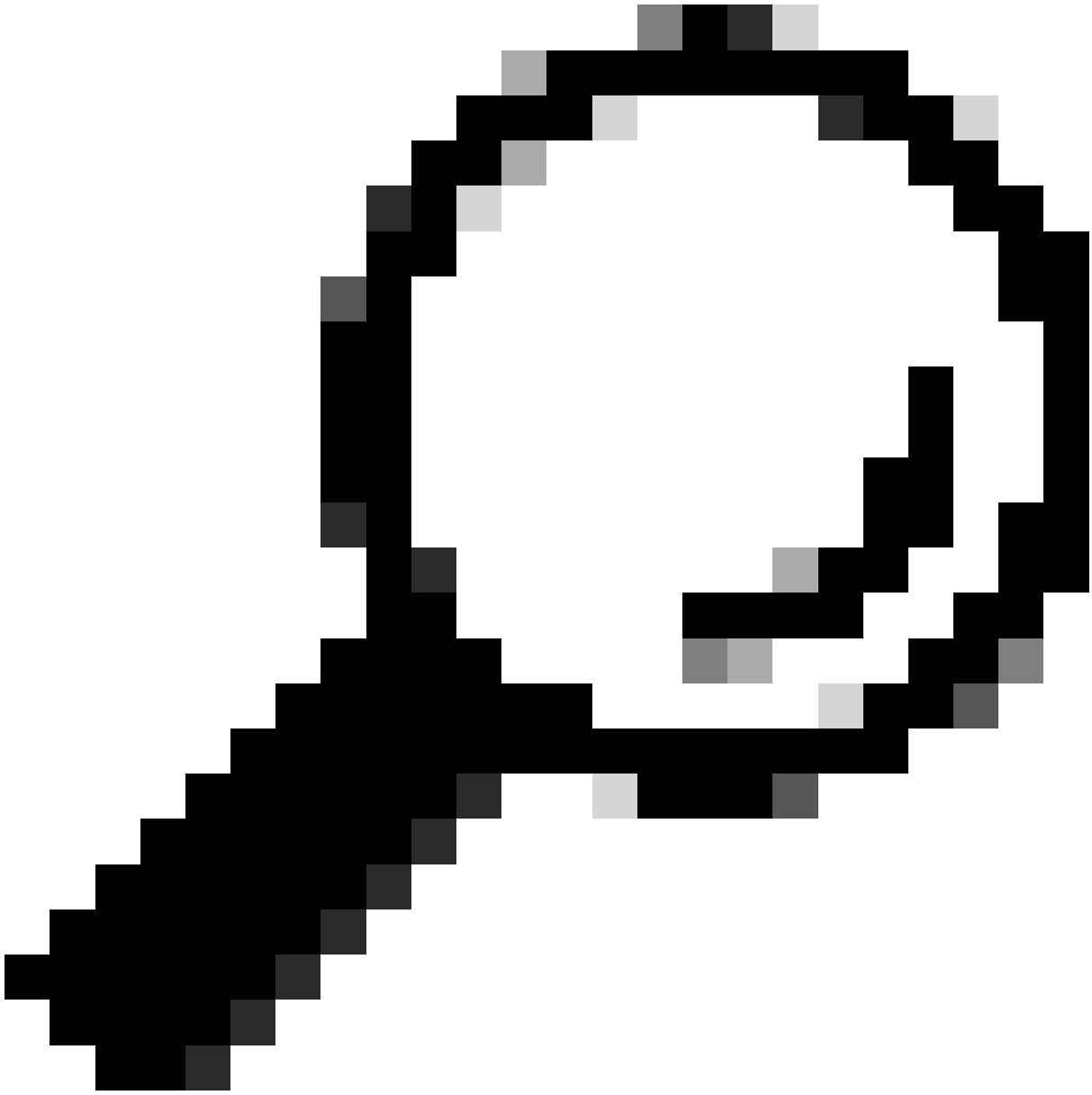
O sistema PPD verifica a solicitação e retorna um veredito ao Web Proxy, seja bloqueando ou monitorando (avalie a solicitação em relação às Políticas de acesso).

Passo 1	Escolha Web Security Manager > Prevenção de Perda de Dados Externos.
Passo 2	Clique no link na coluna Destinos do grupo de políticas que deseja configurar.
Etapa 3	Na seção Edit Destination Settings, selecione "Define Destinations Scanning Custom Settings".
Passo 4	Na seção Destino para varredura, escolha uma destas opções: • Não verificar nenhum upload. Nenhuma solicitação de carregamento foi enviada para o(s) sistema(s) configurado(s) de Prevenção de Perda de Dados (DLP) para verificação. Todas as solicitações de upload são avaliadas em relação às

	Políticas de acesso. • Verificar todos os carregamentos. Todas as solicitações de carregamento são enviadas para o(s) sistema(s) DLP configurado(s) para verificação. A solicitação de carregamento é bloqueada ou avaliada de acordo com as Políticas de Acesso depende do veredito de verificações do sistema PPD. • Verificar uploads, exceto para categorias de URL externas e personalizadas especificadas. As solicitações de carregamento que se enquadram em categorias de URL personalizadas específicas são excluídas das políticas de verificação de DLP. Clique em Editar lista de categorias personalizadas para selecionar as categorias de URL a serem verificadas.
Etapa 5	Enviar e confirmar alterações.

URLs de desvio e passagem

Você pode configurar o Secure Web Appliance na implementação de proxy transparente para ignorar as solicitações HTTP ou HTTPS de clientes específicos ou para destinos específicos.



Dica: você pode usar a passagem para aplicativos que exigem tráfego para passar pelo dispositivo, sem precisar fazer qualquer modificação ou verificações de certificado dos servidores de destino

⚠ Cuidado: o recurso Mapa de Domínio funciona no modo transparente de HTTPS. Este recurso não funciona no modo Explícito e para tráfego HTTP.

- A Categoria Personalizada Local deve ser configurada para permitir que o tráfego use esse recurso.
- Quando esse recurso está habilitado, ele modifica ou atribui o nome do servidor de acordo com o nome de servidor configurado no Mapa de Domínio, mesmo que as informações de Indicação de Nome de Servidor (SNI) estejam disponíveis.

- Esse recurso não bloqueará o tráfego baseado no nome de domínio se esse tráfego corresponder ao Mapa de Domínio e corresponder à categoria personalizada, à política de descriptografia e à ação de passagem forem configurados.
- A autenticação não funciona com esse recurso de passagem. A autenticação requer descriptografia, mas o tráfego não será descriptografado nesse caso.
- o tráfego não é monitorado. Você deve configurar o tráfego UDP para não vir para o Web Security Appliance , em vez disso, ele deve ir diretamente através do firewall para a Internet para aplicativos como WhatsApp, Telegram e assim por diante.
- WhatsApp, Telegram e Skype funcionam no modo Transparente. No entanto, alguns aplicativos como o WhatsApp não funcionam no modo Explícito devido a restrições no aplicativo.

Verifique se você tem uma política de identificação definida para os dispositivos que exigem tráfego de passagem para servidores específicos. Especificamente, você deve:

- Escolha Isento de autenticação/identificação.
- Especifique os endereços aos quais esse perfil de identificação deve ser aplicado. Você pode usar endereços IP, blocos de roteamento entre domínios sem classe (CIDR) e sub-redes.

Passo 1	Habilite o proxy HTTPS.
Passo 2	Escolha Web Security Manager > Mapa de domínio. a. Escolha Add Domain. b. Insira o Domain Name ou o servidor de destino. c. Escolha a ordem de prioridade se houver alguns domínios especificados. d. Insira os endereços IP. e. Clique em Submit.
Etapa 3	Escolha Web Security Manager > Categorias de URL externas e personalizadas. a. Escolha Adicionar categoria. b. Forneça essas informações.

<table>
<tr><td></td><td>
<table>
<tr><th>Configurações</th><th>Descrição</th></tr>
<tr><td>Nome da categoria</td><td>Insira um identificador para esta categoria de URL. Esse nome aparece quando você configura o filtro de URL para grupos de política.</td></tr>
<tr><td>Ordem da lista</td><td>Especifique a ordem desta categoria na lista de categorias de URL personalizadas. Digite "1" para a primeira categoria de URL na lista.

O mecanismo de filtro de URL avalia uma solicitação de cliente em relação às categorias de URL personalizadas na ordem especificada.</td></tr>
<tr><td>Tipo de categoria</td><td>Escolha Local Custom Category.</td></tr>
<tr><td>Avançado</td><td>Você pode inserir expressões regulares nesta seção para especificar conjuntos adicionais de endereços.

Você pode usar expressões regulares para especificar vários endereços que correspondam aos padrões inseridos.</td></tr>
</table>
c. Envie e confirme as alterações.
</td></tr>
<tr><td>Passo 4</td><td>Escolha Web Security Manager > Políticas de descriptografia.

a. Crie uma nova política de descriptografia.

b. Escolha o perfil de identificação que você criou para ignorar o tráfego HTTPS para aplicativos específicos.

c. No painel Avançado, clique no link para Categorias de URL.

d. Na coluna Add, clique para adicionar a categoria de URL personalizada criada na etapa 3.

e. Escolha Concluído.

f. Na página Políticas de descriptografia, clique no link para Filtragem de URL.

g. Escolha Passagem.</td></tr>
</table>

	h. Envie e confirme as alterações. (Opcional) Você pode usar o especificador de formato %(para exibir informações do log de acesso.

Configurar desvio de proxy da Web para solicitações da Web

Depois de adicionar as categorias de URL personalizadas à lista de desvio de proxy, todos os endereços IP e os nomes de domínio das categorias de URL personalizadas são ignorados para a origem e o destino.

Passo 1	Escolha Web Security Manager > Bypass Settings.
Passo 2	Clique em Edit Bypass Settings.
Etapa 3	Digite os endereços para os quais você deseja ignorar o proxy da Web. Observação: quando você configura /0 como uma máscara de sub-rede para qualquer IP na lista de desvio, o dispositivo ignora todo o tráfego da Web. Nesse caso, o equipamento interpreta a configuração como 0.0.0.0/0.
Passo 4	Escolha as categorias de URL personalizadas que deseja adicionar à lista de desvio de proxy.
Etapa 5	Envie e confirme suas alterações.

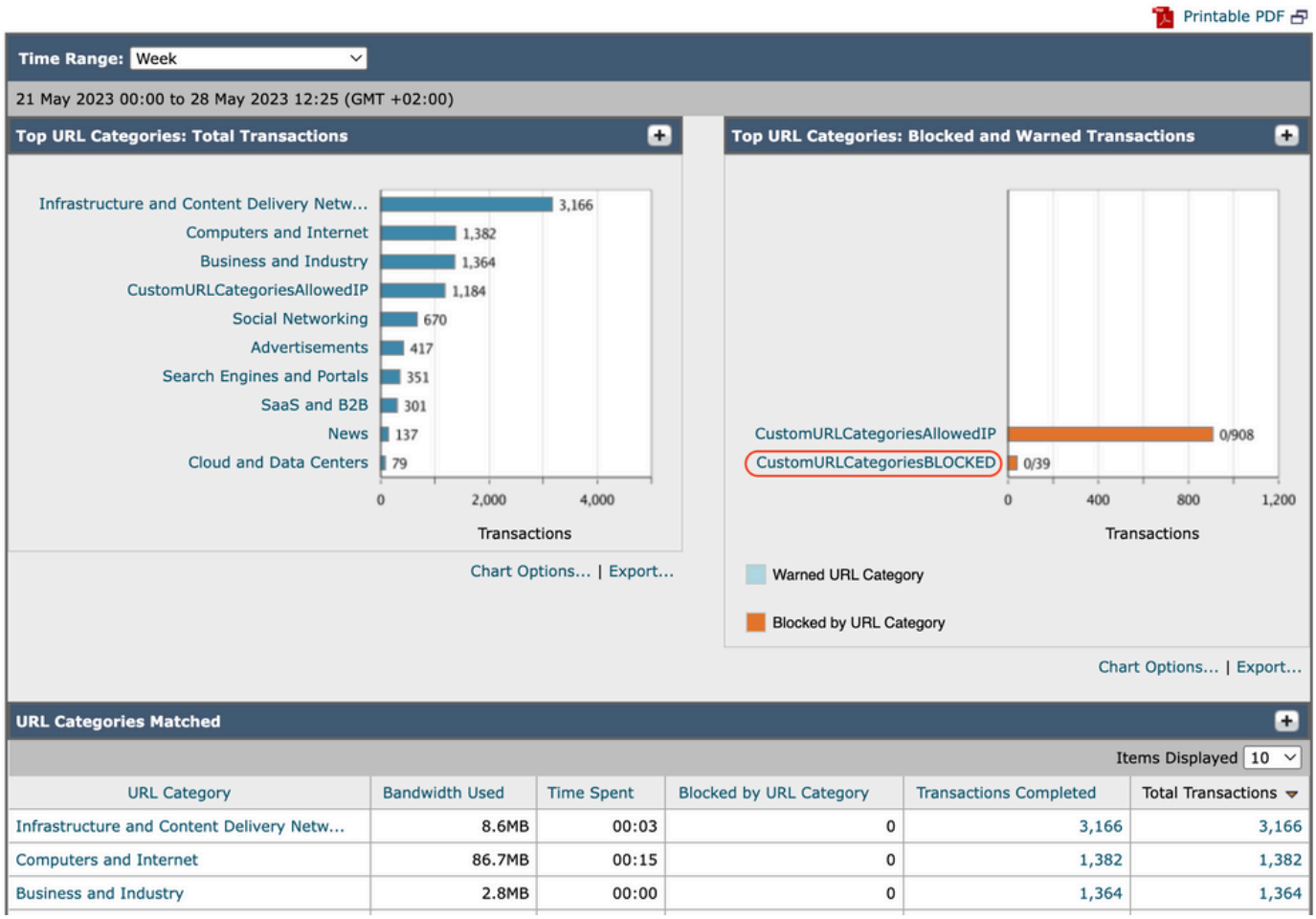
Cuidado: você não pode definir o desvio de proxy da Web para Expressões Regulares.

Relatórios

Na página "Reporting" >> URL Categories', é apresentada uma visualização coletiva das estatísticas dos URL que incluem informações sobre as principais categorias de URL correspondentes e as principais categorias de URL bloqueadas.

Esta página exibe dados específicos da categoria para economia de largura de banda e transações da Web.

Seção	Descrição
Intervalo de tempo (lista suspensa)	Escolha o intervalo de tempo para o relatório.
Principais categorias de URL por total de transações	Esta seção lista as principais categorias de URL visitadas no site em um formato gráfico.
Principais categorias de URL por transações bloqueadas e com aviso	Lista o URL principal que disparou uma ação de bloqueio ou aviso para ocorrer por transação em um formato de gráfico.
Categorias de URL correspondentes	Mostra a disposição das transações por categoria de URL durante o intervalo de tempo especificado, mais a largura de banda usada e o tempo gasto em cada categoria. Se a porcentagem de URLs sem categoria for superior a 15-20%, considere estas opções: • Para URLs localizados específicos, você pode criar categorias de URL personalizadas e aplicá-las a usuários ou políticas de grupo específicos. • Você pode relatar URLs e URLs sem categoria e classificados incorretamente à Cisco para avaliação e atualização do banco de dados. • Verifique se o Filtro do Web Reputation e o Filtro Anti-Malware estão habilitados.



Relatório de categoria de URL de imagem

Você pode clicar em qualquer nome de categoria para exibir mais detalhes relacionados a essa categoria, como Domínios correspondentes ou lista de usuários.

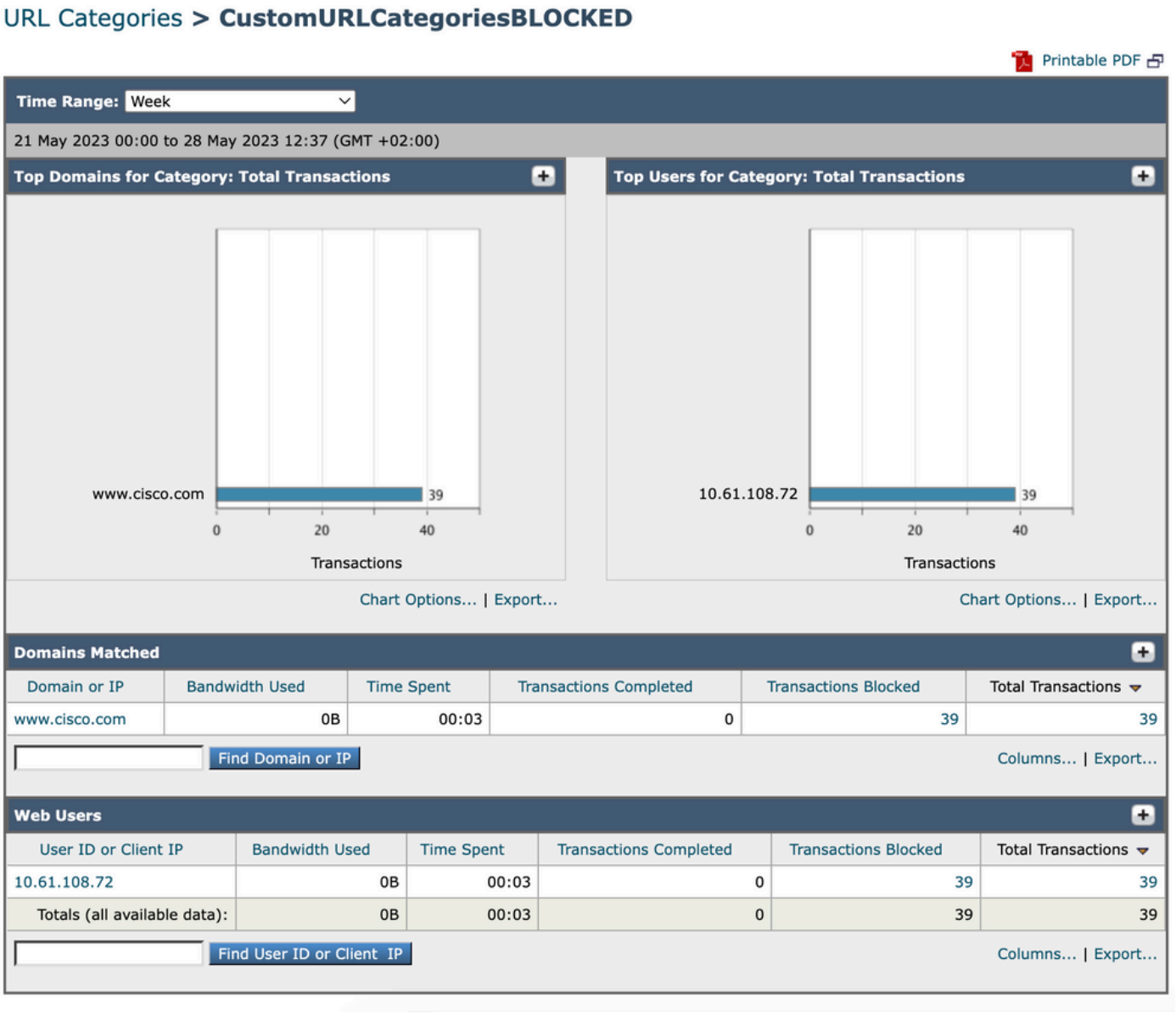


Imagem - Página Relatório detalhado

O conjunto de categorias de URL predefinidas pode ser atualizado periodicamente automaticamente no Web Security Appliance .

Quando essas atualizações ocorrerem, os nomes de categoria antigos continuarão a aparecer nos relatórios até que os dados associados às categorias mais antigas sejam muito antigos para serem incluídos nos relatórios.

Os dados de relatório gerados após a atualização de um conjunto de categorias de URL usam as novas categorias, para que você possa ver as categorias novas e antigas no mesmo relatório.

Nas estatísticas de URL na página Categorias de URL dos relatórios, é importante entender como interpretar esses dados:

Tipo de dados	Descrição
Filtragem de URL Ignorada	Representa a política, a porta e o agente de usuário administrador bloqueado, o que ocorre antes da filtragem de URL.

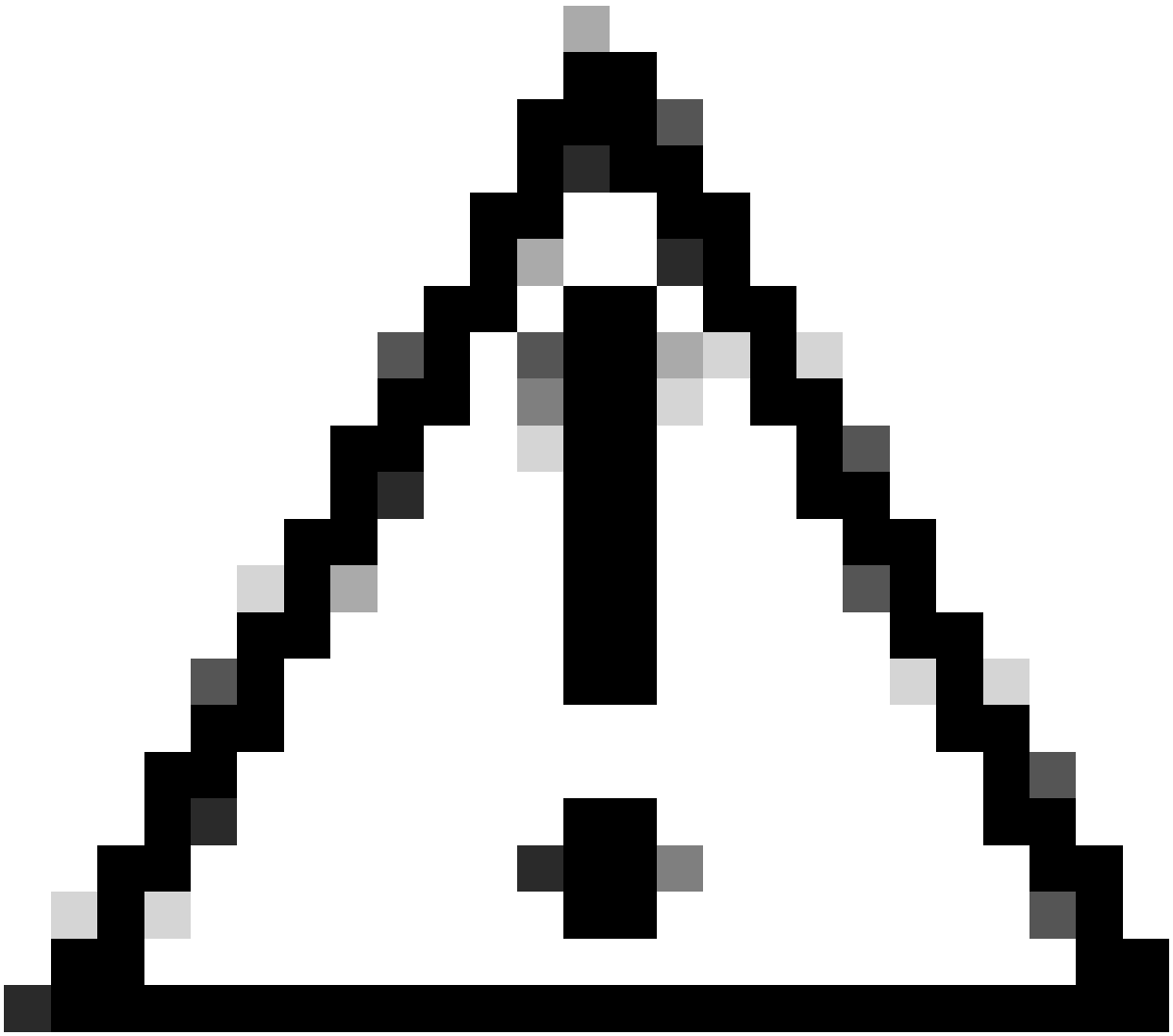
URL sem categoria	Representa todas as transações para as quais o mecanismo de filtragem de URL é consultado, mas nenhuma categoria é correspondida.

Exibir Categorias De URL Personalizadas No Log De Acesso

O Secure Web Appliance usa os quatro primeiros caracteres de nomes de categorias de URL personalizadas precedidos por "c_" nos logs de acesso.

Neste exemplo, o nome da categoria é CustomURLCategoriesBLOCKED e nos registros de acesso você pode ver C_Cust :

```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUST
```



Cuidado: Considere o nome da categoria de URL personalizada se você usar o Sawmill para analisar os logs de acesso. Se os primeiros quatro caracteres da categoria de URL personalizada incluírem um espaço, a Sawmill não poderá analisar corretamente a entrada do log de acesso. Em vez disso, use somente caracteres suportados nos primeiros quatro caracteres.

Dica: se quiser incluir o nome completo de uma categoria de URL personalizada nos logs de acesso, adicione o especificador de formato %XF aos logs de acesso.

Quando um grupo de política de acesso à Web tem uma categoria de URL personalizada definida como Monitor e algum outro componente (como os Filtros de reputação da Web ou o mecanismo de verificação de vereditos diferentes (DVS)) toma a decisão final de permitir ou bloquear uma solicitação de um URL na categoria de URL personalizada, a entrada do log de acesso para a solicitação mostra a categoria de URL predefinida em vez da categoria de URL personalizada.

Para obter mais informações sobre como configurar campos personalizados em Logs de Acesso, visite : Configurar Parâmetro de Desempenho em Logs de Acesso - Cisco

Troubleshooting

Categoria Incompatível

Nos logs de acesso, você pode ver que a solicitação pertence a qual Categoria de URL personalizada, se a seleção não for como esperado:

- Se a solicitação for categorizada em outras categorias de URL personalizadas, verifique se há uma URL duplicada ou uma expressão regular correspondente em outras categorias ou mova a categoria de URL personalizada para o topo e teste novamente. é melhor inspecionar cuidadosamente a categoria de URL personalizada correspondente.

- Se a solicitação for categorizada em Categorias predefinidas, verifique as condições na Categoria de URL personalizada existente, se todas corresponderem, tente adicionar o endereço IP e teste ou certifique-se de que o erro de digitação e a expressão regular correta sejam usados, se houver.

As Categorias Predefinidas Não Estão Atualizadas

Se as categorias predefinidas não estiverem atualizadas, ou nos logs de acesso que você vir "err" na seção de categoria de URL, certifique-se de que o TLSv1.2 esteja habilitado para o Atualizador.

Para alterar a configuração de SSL do Atualizador, use estas etapas da GUI:

Etapa 1. Em Administração do Sistema, escolha Configuração SSL

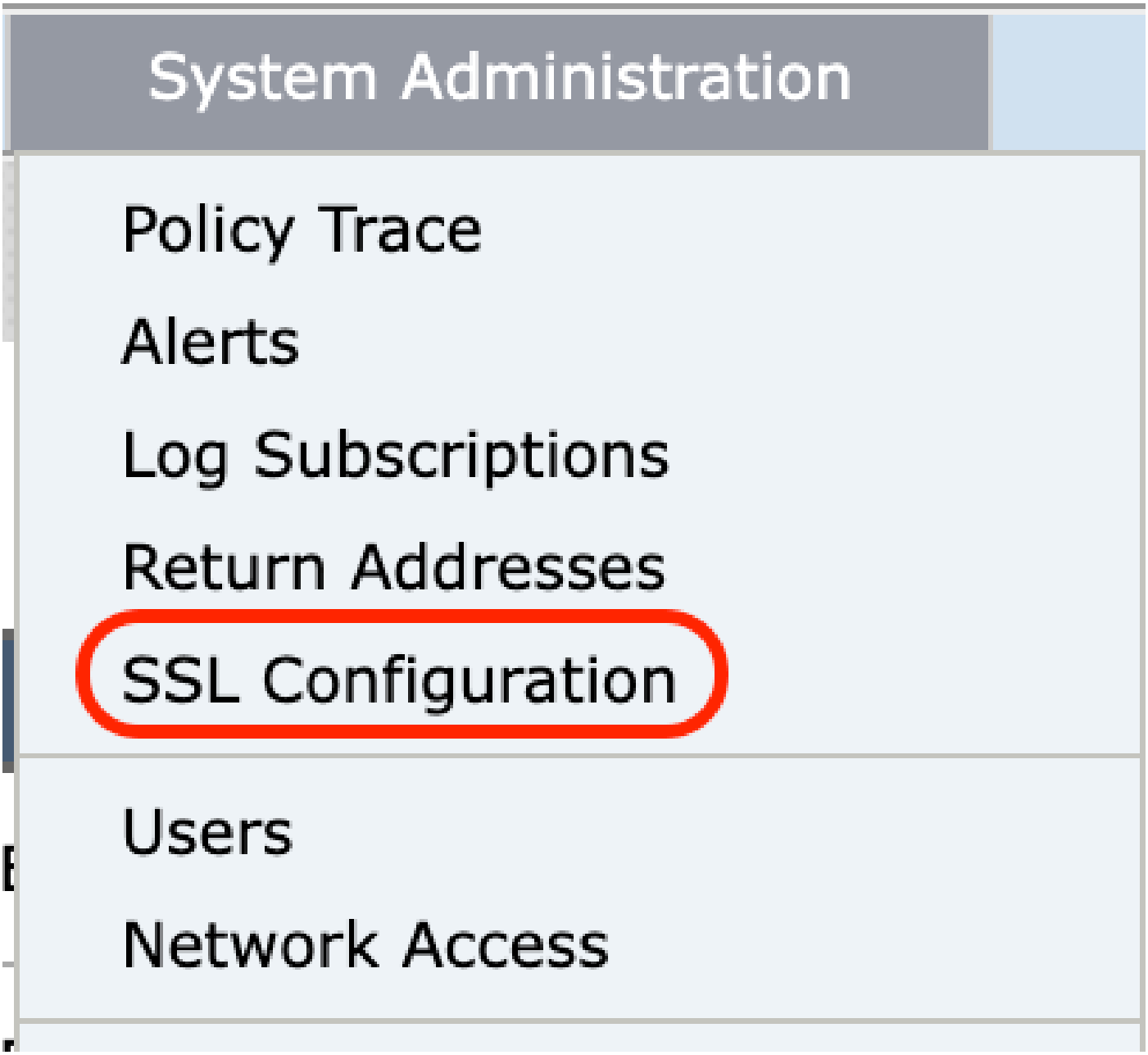


Imagem - configuração ssl

Etapa 2. Escolha Editar configurações.

Etapa 3. Na seção Atualizar serviço, escolha TLSv1.2

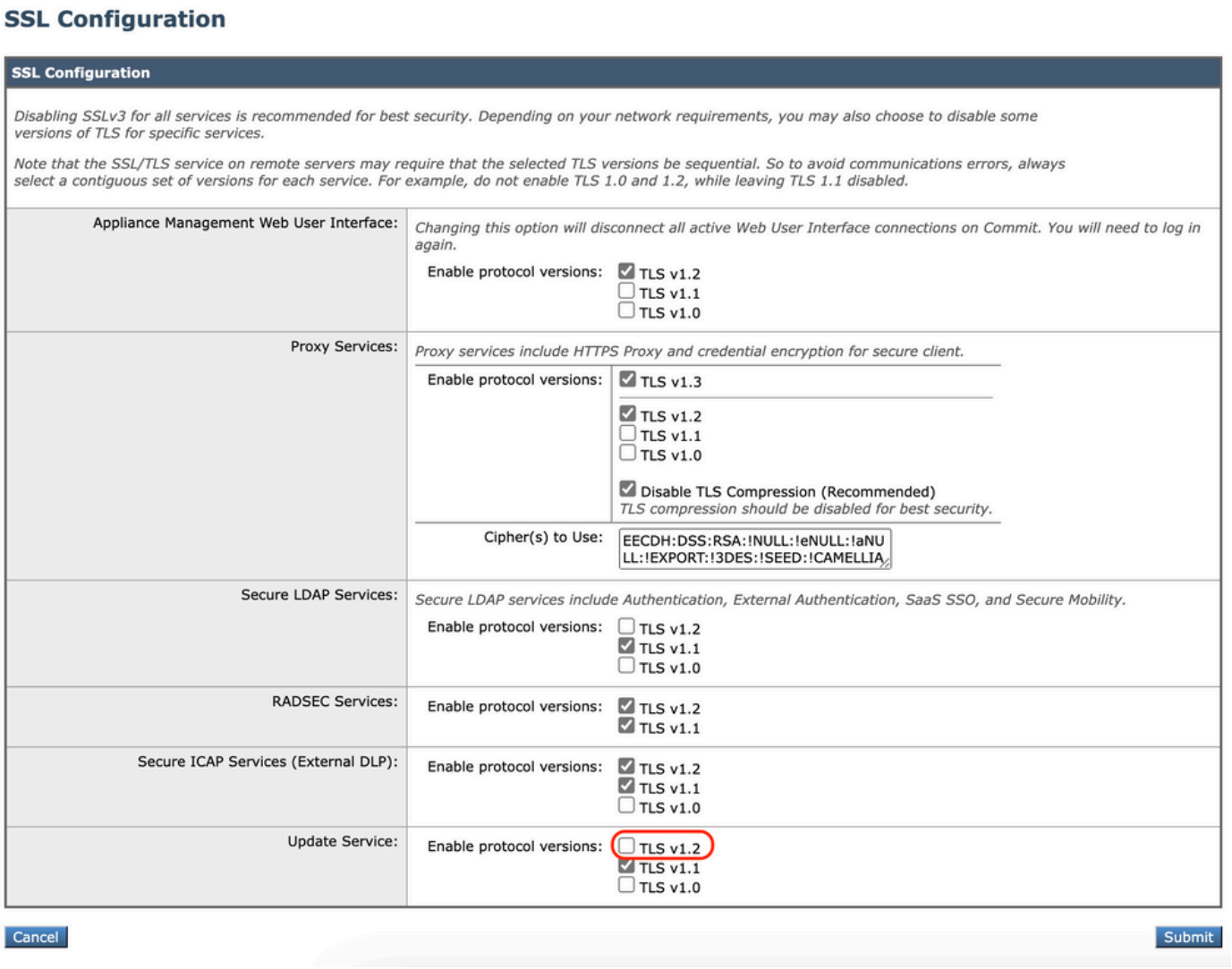


Imagem - Serviço de atualização TLSv1.2

Etapa 4. Enviar e confirmar alterações

Para alterar a configuração SSL do Atualizador, use estes passos da CLI:

Etapa 1. No CLI, execute sslconfig

Etapa 2. Digite version e pressione enter

Etapa 3. Escolher Atualizador

Etapa 4. Escolha TLSv1.2

Etapa 5. Pressione Enter para sair do assistente

Etapa 6. confirme as alterações.

```
SWA_CLI> sslconfig

Disabling SSLv3 is recommended for best security.
```

```
Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequentia
1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.
[]> versions

SSL/TLS versions may be enabled or disabled for the following services:

        LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secu
        Updater - Update Service
        WebUI - Appliance Management Web User Interface
        RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
        SICAP - Secure ICAP Service
        Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

         LDAPS  Updater  WebUI   RADSEC  SICAP   Proxy
TLSv1.0    N       N       N      N/A      N       N
TLSv1.1    Y       Y       N       Y       Y       N
TLSv1.2    N       N       Y       Y       Y       Y
TLSv1.3   N/A     N/A     N/A     N/A     N/A      Y

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services
[]> 2


Currently enabled protocol(s) for Updater are TLSv1.1.


To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
[]> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y


Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.
```

Referência

Diretrizes de práticas recomendadas do Cisco Web Security Appliance - Cisco

BRKSEC-3303 (ciscolive)

Manual do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD (General Deployment) - Conectar, Instalar e Configurar [Cisco Secure Web Appliance] - 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.