Como definir configurações de passagem adicionais do Web Security Appliance para o aplicativo Webex

Introdução

Este documento descreve como configurar as políticas de desvio do Secure Web Appliance (SWA/WSA) para garantir a funcionalidade adequada do aplicativo Cisco Webex em condições especiais de implantação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Async OS para Secure Web Appliance 14.x ou posterior.
- Administração do acesso do usuário à interface gráfica do usuário (GUI) do Secure Web Appliance.
- Administração de acesso do usuário à interface de linha de comando (CLI) do Secure Web Appliance.

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.

Problema

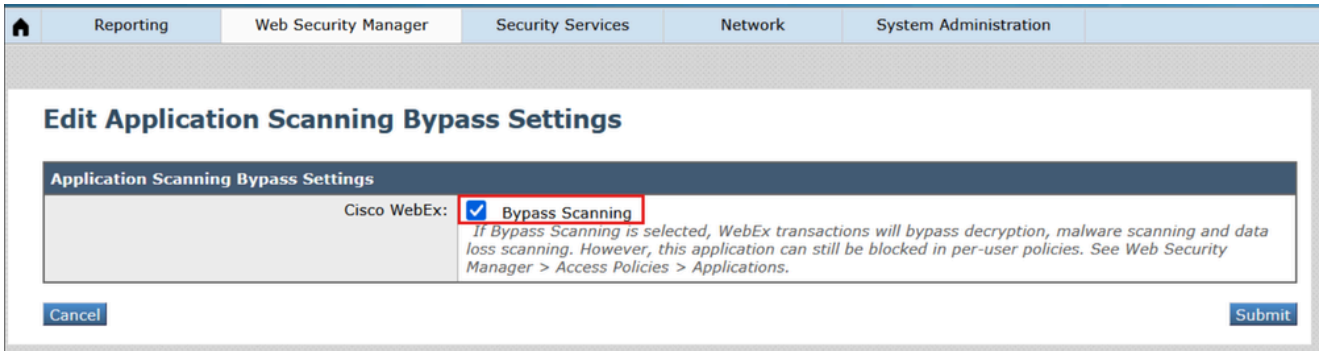
Com base na documentação pública do Webex para Requisitos de rede para serviços Webex, o servidor proxy deve ser configurado para permitir que o tráfego de sinalização do Webex acesse os domínios/URLs listados no documento. O Secure Web Appliance atende aos requisitos da maioria dos ambientes, ativando a caixa de seleção Webex Application Bypass (Ignorar aplicativo Webex) nas configurações de bypass. No entanto, algumas configurações adicionais podem ser necessárias no Secure Web Appliance para evitar a interrupção do serviço no Webex Application. As próximas etapas são recomendadas para tais cenários de caso:

Desvio de verificação de aplicativo Webex

O recurso Cisco Webex: Bypass Scanning é a primeira etapa para permitir que o tráfego do aplicativo Webex passe sem filtragem pelo Secure Web Appliance. Ele deve ser ativado em todos os ambientes e cenários de implantação em que os usuários do desktop Webex ou aplicativos móveis tenham o tráfego da Web intermediado por proxy por meio do Secure Web Appliance.

Etapas para ativar o desvio de verificação de aplicativos Webex:

1. Na GUI do WSA, vá até Web Security Manager > Bypass Settings > Edit Application Bypass Settings.
2. Marque a caixa de seleção "Cisco WebEx".



1_wsa_bypass_scanning_settings

3. Enviar e confirmar alterações

Quando essa configuração é habilitada, ela não ignora o tráfego transparente como seria esperado depois que os FQDNs são adicionados à lista de desvio no Secure Web Appliance. Em vez disso, o tráfego do aplicativo Webex ainda é encaminhado por proxy através do Secure Web Appliance, mas ele será transmitido na descriptografia com a marca de decisão "PASSTHRU_AVC". Veja a seguir um exemplo de como isso pode ser exibido nos logs de acesso:

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

Considerações para ambientes exclusivos

Há algumas situações em que configurações adicionais são necessárias para que o aplicativo Webex funcione quando o tráfego é encaminhado por proxy por meio do Secure Web Appliance.

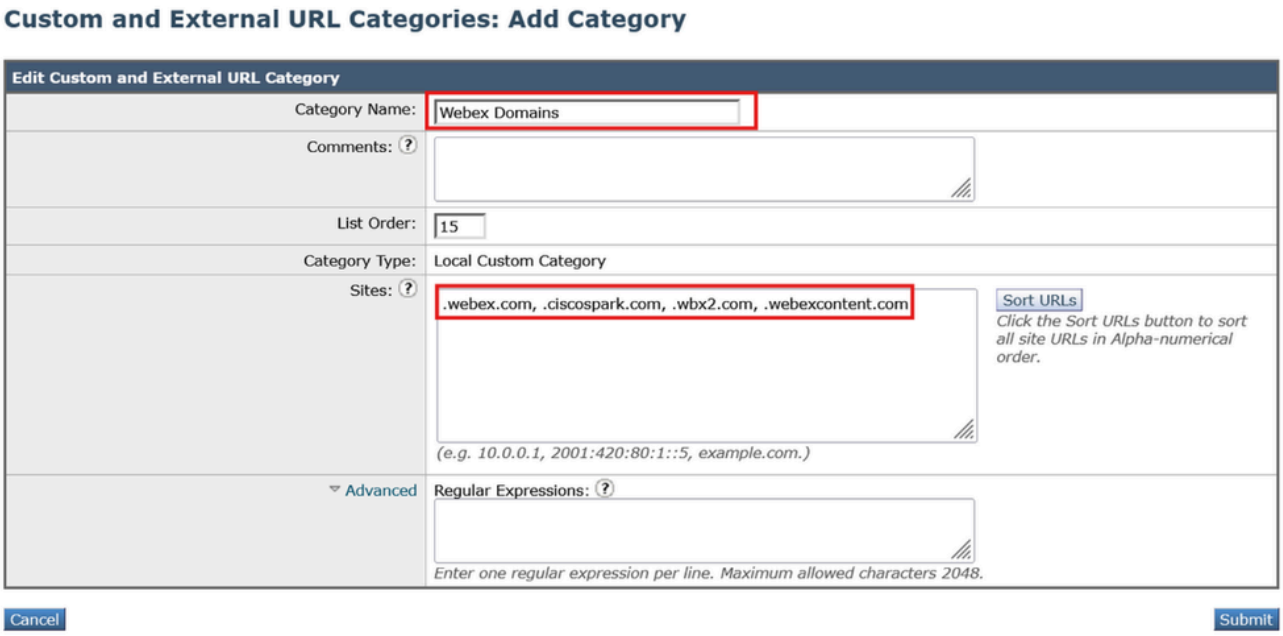
Cenário 1: Os domínios do Webex precisam ser isentos de autenticação

Isso é especialmente evidente em ambientes onde os substitutos de IP não estão ativados no Perfil de identificação e o redirecionamento transparente é usado. Com base na documentação existente, o aplicativo Webex é capaz de fazer a autenticação NTLMSSP em estações de trabalho associadas a domínios onde o proxy é explicitamente definido. Caso contrário, é uma

prática recomendada configurar uma categoria personalizada para os domínios do Webex e isentá-los da autenticação.
Etapas para isentar domínios Webex da autenticação:

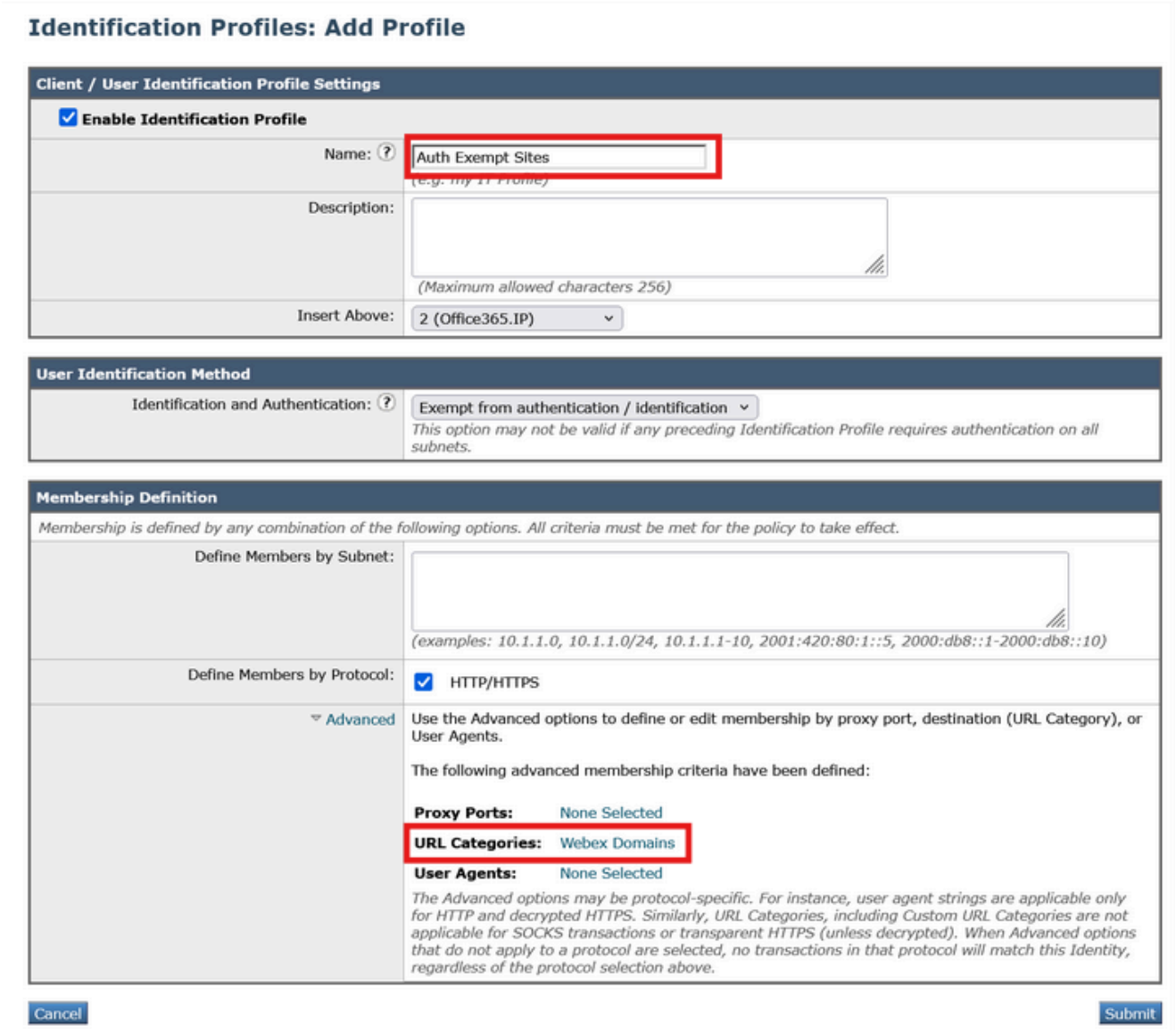
1. Na GUI do WSA, navegue para Web Security Manager > Categorias de URL personalizadas e externas > Adicionar categoria.
2. Dê um nome à nova categoria e coloque os seguintes domínios na seção Sites:

```
.webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
```



2_wsa_custom_url_category

3. Clique em Submit. Em seguida, navegue até Web Security Manager > Identification Profiles > Add Identification Profile
4. Dê um nome ao novo perfil e, na seção Avançado para Categorias de URL, selecione a nova categoria que foi criada na etapa #2



3_wsa_id_profile

5. Certifique-se de que a Identificação e a Autenticação no novo perfil esteja definida como Isenta de autenticação/identificação
6. Enviar e confirmar alterações.

Cenário 2: Os domínios de conteúdo do Webex não são totalmente honrados pelo desvio de descriptografia.

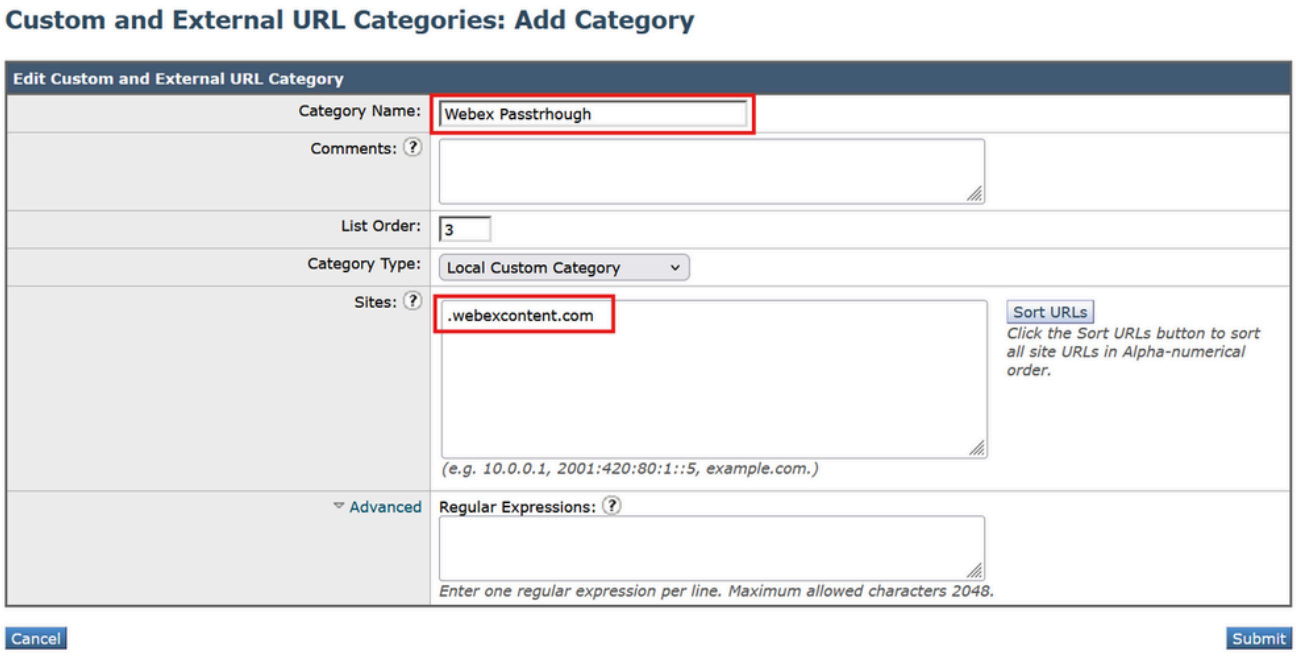
Há alguns subdomínios relacionados ao webexcontent.com que não passam automaticamente na descriptografia quando o desvio de verificação de aplicativos Webex está habilitado. O conteúdo servido desses domínios é confiável para o aplicativo Webex quando é descriptografado, desde que o certificado de descriptografia do Secure Web Appliance já tenha sido adicionado ao repositório de certificados raiz confiáveis do dispositivo ou assinado por uma autoridade de certificação interna que já seja confiável para o dispositivo que executa o aplicativo Webex. No entanto, se o dispositivo não for gerenciado e o certificado de descriptografia do Secure Web Appliance não for confiável, esses domínios deverão ser configurados para passar na descriptografia.

Quando a implantação de redirecionamento transparente está em vigor e há mais de um SWA junto com o spoofing de IP do cliente sendo usado para grupos de redirecionamento, o tráfego pode ser configurado para redirecionar para o Secure Web Appliance com base no IP de destino e, da mesma forma, o tráfego de retorno dos servidores Web é configurado para redirecionar de volta através do Secure Web Appliance com base no endereço de origem. Quando o Secure Web Appliance é configurado para fazer conexões com o servidor da Web usando o IP que ele resolve usando a pesquisa de DNS, o tráfego de retorno pode ser redirecionado inadvertidamente para um Secure Web Appliance diferente e subsequentemente descartado. Esse problema afeta não apenas o Webex, mas também outros aplicativos de transmissão de vídeo, devido ao uso de endereços IP rotativos nos servidores da Web.

Etapas para configurar a passagem na descriptografia para todos os domínios do Webex:

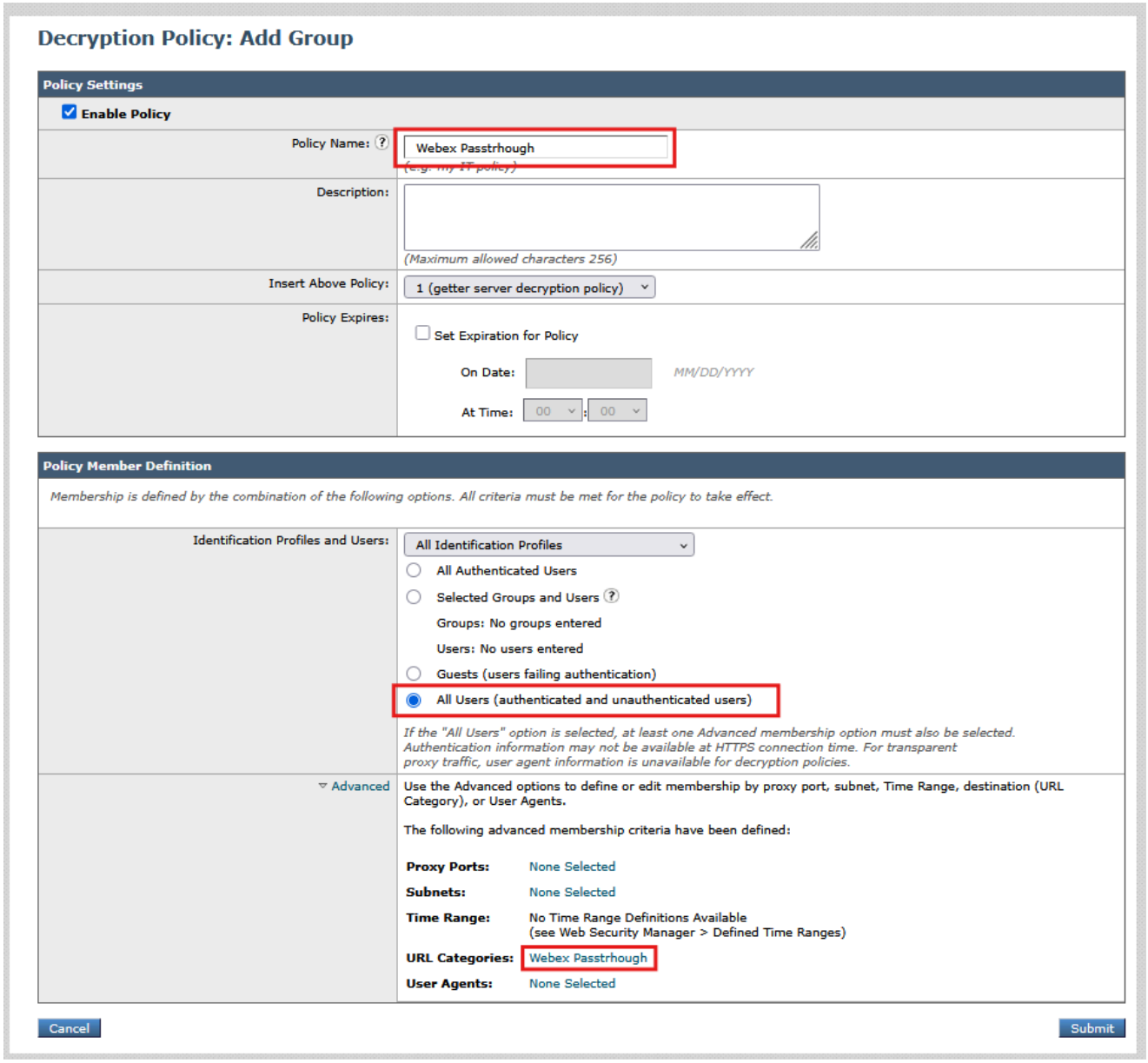
1. Certifique-se de que Webex Application Scanning Bypass esteja habilitado conforme as instruções acima.
2. Na GUI do WSA, navegue para Web Security Manager > Categorias de URL personalizadas e externas > Adicionar categoria.
3. Dê um nome à nova categoria e coloque o próximo domínio na seção Sites:

```
.webexcontent.com
```



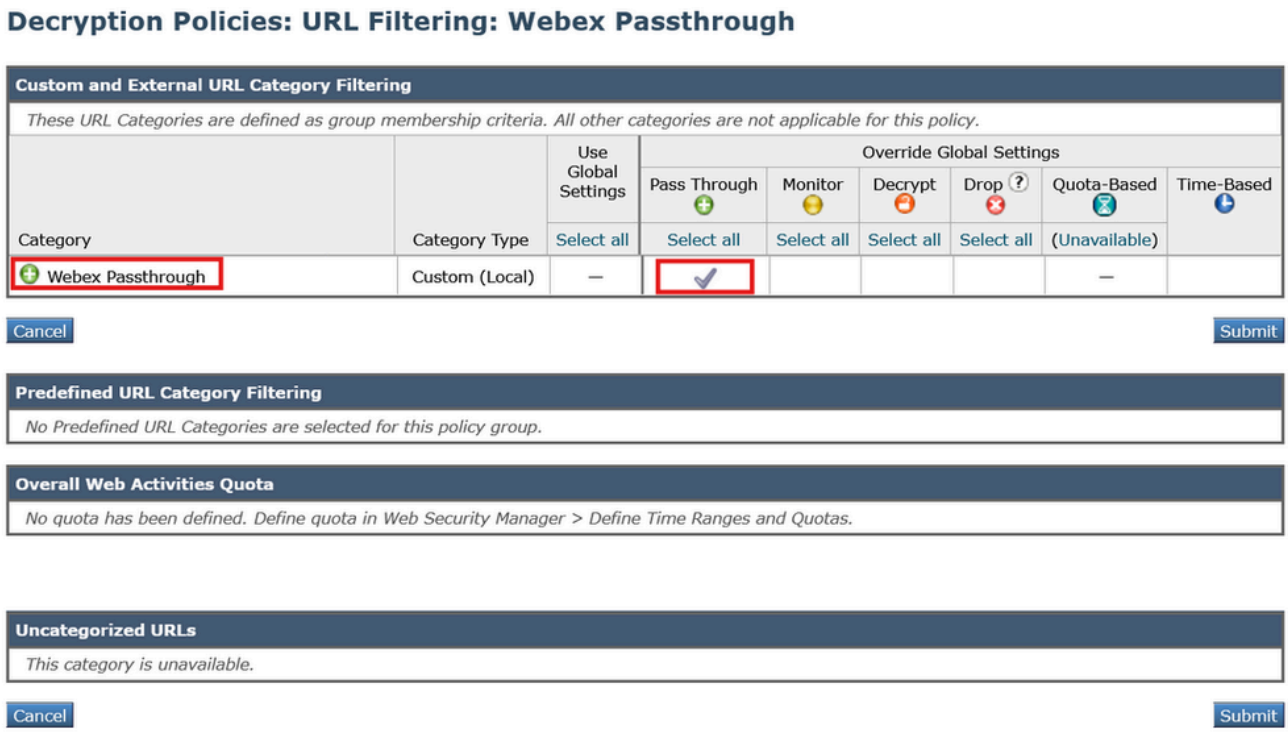
4_wsa_url_category

4. Clique em Submit. Agora, navegue até Web Security Manager > Políticas de descriptografia > Adicionar política
5. Nomeie a nova política, defina Perfis de identificação e usuários como "Todos os usuários" e, na seção Avançado de Categorias de URL, selecione a nova categoria criada na etapa #3



5_wsa_decryption_policy

6. Clique em Submit. Em seguida, clique na seção Filtragem de URL e defina a categoria personalizada criada na etapa #3 como "Passagem".



6_wsa_url_filtering

7. Envie e confirme as alterações.

Se vários dispositivos da Web seguros forem implantados para redirecionamento transparente e o spoofing de IP do cliente estiver habilitado, há duas soluções para isso:

1. Defina os serviços WCCP de saída e de retorno para balancear a carga com base no endereço do cliente em vez do endereço do servidor.
2. Na CLI do WSA, defina advanced proxyconfig > DNS > "Find web server by" para sempre usar o endereço IP fornecido pelo cliente nas conexões com o servidor da Web (opções 2 e 3). Para obter mais informações sobre essa configuração, consulte a seção DNS do guia Use Secure Web Appliance Best Practices.

Verificação

Quando as configurações de passagem forem concluídas, o tráfego do Webex será processado nos logs de acesso como Pass through conforme as políticas:

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

Analise e monitore o aplicativo webex; se for relatada alguma lentidão ou interrupção de serviço, revise os logs de acesso mais uma vez e valide se todo o tráfego do lado do webex foi processado corretamente.

Informações Relacionadas

- Requisitos de rede para serviços Webex
- Use as práticas recomendadas de dispositivos da Web seguros

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.