Configurar o proxy de upstream no aplicativo da Web seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Configurando o proxy de upstream](#)

- [Etapa 2. (Opcional) Criar um Perfil de Identificação para Usar o Proxy de Upstream](#)
- [Etapa 3. Criar o proxy de upstream](#)
- [Etapa 4. (Opcional) Fazer upload do certificado de descriptografia](#)
- [Etapa 5. Configurar a Política de Roteamento](#)
- [Etapa 6. (Opcional) Definindo as configurações de tempo limite de não resposta do proxy de upstream](#)

[Registro](#)

- [Logs de acesso](#)
- [Logs proxy](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para configurar o proxy de upstream no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.
- Protocolos básicos de rede e proxy.

A Cisco recomenda que você tenha estas ferramentas instaladas:

- SWA físico ou virtual

- Acesso administrativo à interface gráfica do usuário (GUI) do SWA
- Acesso administrativo à interface de linha de comando (CLI) 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.

Configurando o proxy de upstream

Use estas etapas para configurar um proxy de upstream no SWA.

Etapas	Etapas
Etapa 1. (Opcional) Criar uma Categoria de URL Personalizada para os URLs Note: Se quiser definir o proxy de upstream para todo o tráfego, você pode pular esta etapa.	Etapa 1.1.FromGUI, ChooseWeb Security Manager e clique em Categorias de URL personalizadas e externas. Etapa 1.2.Clique em Adicionar categoria para adicionar uma categoria de URL personalizada. Etapa 1.3.Atribua um CategoryName exclusivo. Etapa 1.4. (Opcional) Adicione Descrição. Etapa 1.5. Em Ordem da lista, escolha a primeira categoria a ser posicionada na parte superior. Etapa 1.6. Na lista suspensa Tipo de categoria, selecione Categoria personalizada local. Etapa 1.7. Adicione os URLs desejados na seção Sites. Etapa 1.8. Enviar.

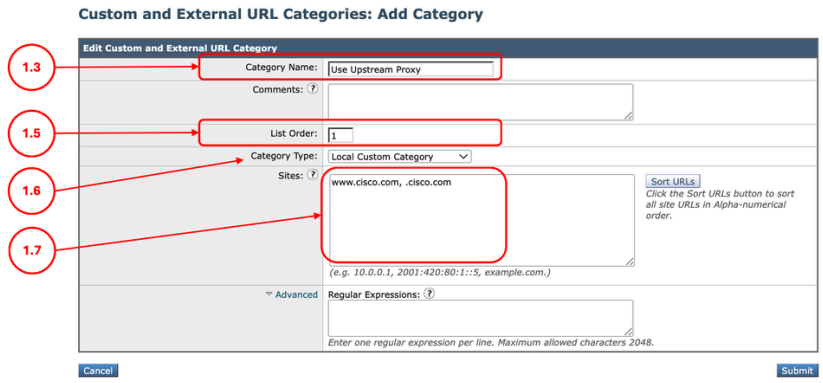


Imagem - Criar uma Categoria de URL Personalizada

Etapa 2. (Opcional) Criar um Perfil de Identificação para Usar o Proxy de Upstream

Note: Se quiser definir o proxy de upstream para todo o tráfego, você pode pular esta etapa.

Etapa 2.1.FromGUI, ChooseWeb Security Manager e clique em Identification Profiles.
Etapa 2.2.Clique emAdd Profile para adicionar um perfil.
Etapa 2.3.Use a caixa de seleçãoAtivar Perfil de Identificação para ativar esse perfil ou para desativá-lo rapidamente sem excluí-lo.
Etapa 2.4.Atribua um profileName exclusivo.
Etapa 2.5. (Opcional) Adicione Descrição.
Etapa 2.6.Na lista suspensa InserirAcima, escolha onde esse perfil deve aparecer na tabela.

Etapa 2.7. Se você quiser não autenticar os usuários que estão acessando essa política, na seção Identificação de usuário Metodsection, escolhaIsentar de autenticação/identificação, senão configure os parâmetros de autenticação.

Etapa 2.8.No campo Definir membros por sub-rede, deixe este campo em branco para incluir todos os endereços IP do cliente, a menos que você queira Passar através do tráfego para determinados endereços IP.

Etapa 2.9. (Opcional: Se você precisar usar um proxy de upstream para usuários específicos que acessam determinados sites, conclua esta etapa.) Na seção Avançado, escolha Categorias de URL personalizadas e Adicionar a Categoria de URL personalizada criada na Etapa 1

Etapa 2.10. Enviar.

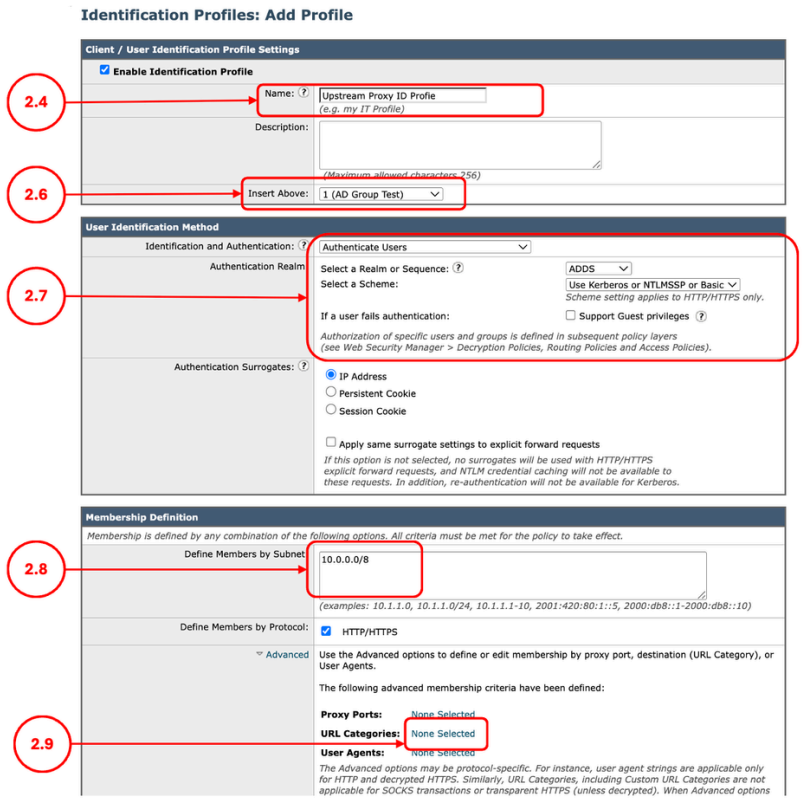
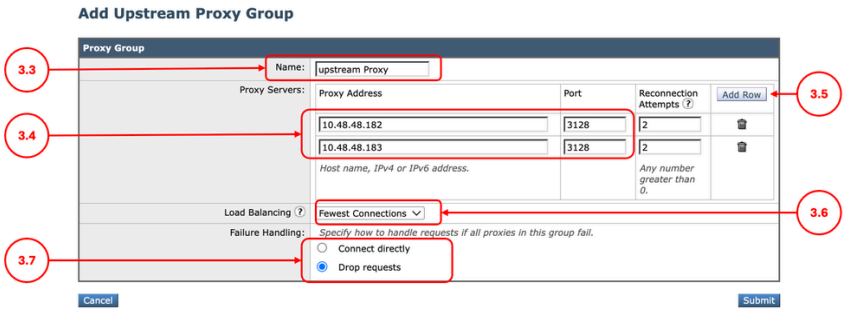


Imagem - Criar um perfil de identificação

Etapa 3. Criar o proxy de upstream	Etapa 3.1.FromGUI, ChooseNetwork e clique em Upstream Proxy. Etapa 3.2. Clique em Adicionar grupo. Etapa 3.3.Atribua um uniqueName. Etapa 3.4. Defina o endereço do proxy e o número da porta. Etapa 3.5. (Opcional) Se você tiver mais de um Proxy de upstream, clique em Adicionar linha para definir o próximo Proxy. Etapa 3.6. (Opcional) Se você inseriu mais de um Proxy de upstream na seção Balanceamento de carga, defina o método de Balanceamento de carga desejado, • Nenhum (failover): O Web Proxy direciona as transações para um proxy externo no grupo. Tenta conectar-se aos proxies na ordem em que estão listados. Se um proxy não puder ser acessado, o Web Proxy tentará se conectar ao próximo da lista. • Menos conexões: O Web Proxy controla quantas solicitações ativas estão com os diferentes proxies no grupo e direciona uma transação para o proxy que está atendendo o menor número de conexões. • Baseado em hash:Menos usado recentemente. O Web

	Proxy direciona uma transação para o proxy que recebeu recentemente uma transação se todos os proxies estiverem ativos no momento. Essa configuração é semelhante à de rodízio, exceto que o Web Proxy também leva em conta as transações que um proxy recebeu por ser um membro em um grupo de proxy diferente. Ou seja, se um proxy estiver listado em vários grupos de proxy, a opção "menos usada recentemente" tem menor probabilidade de sobrecarregar esse proxy. • Rodízio: O Web Proxy desloca as transações igualmente entre todos os proxies no grupo na ordem listada. Etapa 3.7. Escolha a opção Failure Handling, dependendo da sua política interna. • Conectar diretamente:Envie as solicitações diretamente aos servidores de destino. • Soltar solicitações:Descarte as solicitações sem encaminhá-las. Etapa 3.8. Enviar.  Imagem - Adicionar grupo de proxy de upstream
Etapa 4. (Opcional) Fazer upload do certificado de descriptografia Note: Se o Upstream Proxy não estiver descriptografando o tráfego ou seu servidor de CA já for confiável no SWA, você poderá ignorar esta etapa	Etapa 4.1.FromGUI, ChooseNetwork e clique emCertificate Management. Etapa 4.2. Na seção Gerenciamento de certificados, clique em Gerenciar certificados raiz confiáveis.

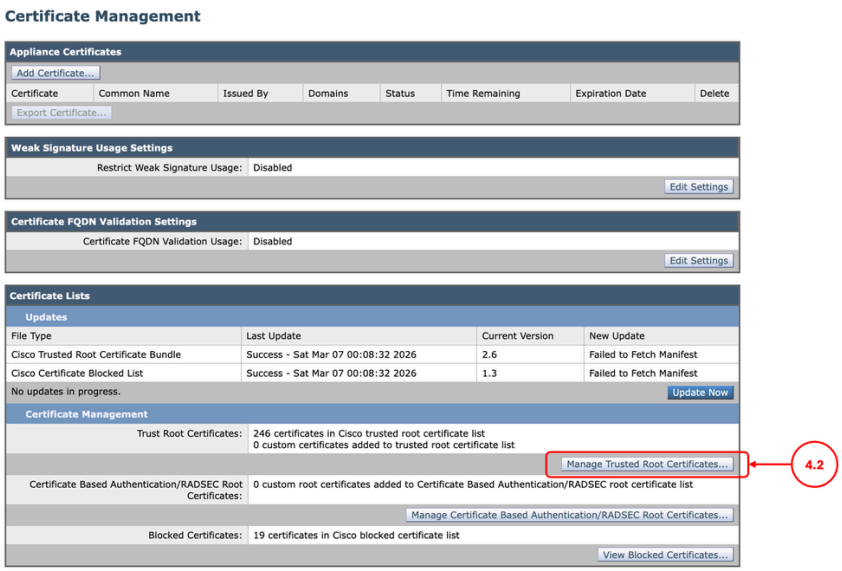


Imagem - Gerenciar certificado raiz confiável

Etapa 4.3. Enviar e confirmar as alterações.

⚠ Cuidado: se os certificados de CA raiz e intermediários forem necessários, carregue primeiro o certificado de CA raiz e clique em Enviar e confirmar. Após a conclusão da confirmação, importe o certificado intermediário da CA e envie e confirme novamente as alterações.

Etapa 5. Configurar a Política de Roteamento

Etapa 5.1. FromGUI, ChooseWeb Security Manager e clique em Routing Policy.

Etapa 5.2. (Opcional) Se você quiser usar o proxy de upstream para usuários ou sites específicos, clique em Adicionar política e selecione o Perfil de identificação que você criou na Etapa 2.

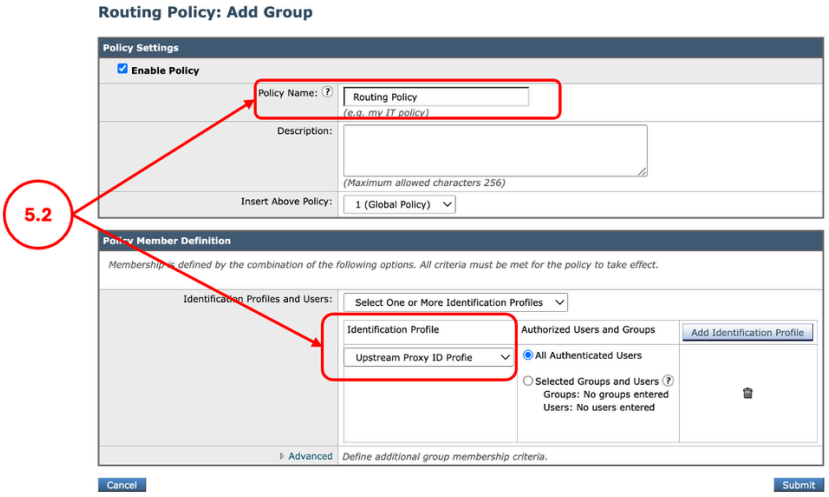


Imagem - Adicionando o perfil de ID à política de roteamento

Etapa 5.3. Para as condições desejadas, que você gostaria de usar o proxy de upstream, clique no link Routing Destination (Destino do Roteamento) e selecione o Upstream Proxy Group que você criou na Etapa 3.

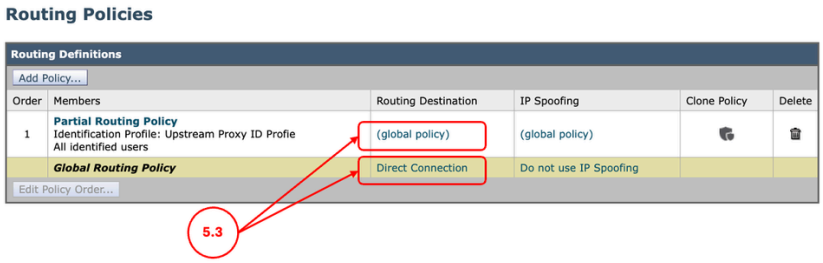


Imagem - Configurando o destino de roteamento

Note: Se desejar todo o tráfego usando o proxy de upstream, na Política de roteamento global, selecione o Proxy de upstream desejado.

Etapa 5.4. Enviar e confirmar as alterações.

Etapa 6. (Opcional) Definindo as configurações de tempo limite de não resposta do proxy de upstream

Dica: Recomenda-se não modificar esses valores, a menos que você compreenda totalmente seu comportamento e impacto potencial.

Etapa 6.1. Efetue login na CLI e execute advancedproxyconfig

Etapa 6.2. Selecionar DIVERSOS

Etapa 6.3. Pressione Enter até ver Enter minimum idle timeout para verificar proxy de upstream sem resposta (em segundos). Você pode configurar a quantidade mínima de tempo que o SWA espera para tentar novamente o proxy de upstream que foi declarado anteriormente como doente. O valor padrão é de 10 segundos.

Etapa 6.4. Pressione Enter para prosseguir para a próxima configuração. Ao definir o timeout ocioso máximo para verificar um proxy de upstream sem resposta, observe que se esse valor de timeout for atingido antes que o número configurado de tentativas de reconexão seja esgotado (Etapa 3), o SWA considerará o proxy de upstream off-line.

Etapa 6.7. Continue pressionando Enter, até sair do assistente, execute commit para salvar as alterações.

Registro

Logs de acesso

Nos registros de acesso, o tráfego que foi roteado para o proxy de upstream é mostrado como DEFAULT_PARENT seguido pelo nome do proxy de upstream. veja um exemplo:

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

Logs proxy

Nos registros de proxy, você pode verificar o status de integridade dos proxies de upstream.

Tip: Você pode filtrar por peer para revisar os logs relacionados ao proxy de upstream.

Aqui estão alguns exemplos, como configuramos as Tentativas de Reconexão na Etapa 3 duas vezes, após duas falhas de conexão com o proxy de upstream, o proxy de upstream é declarado como add e o SWA remove esse proxy de upstream da lista até que o processo de proxy seja reiniciado.

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

Note: Se o proxy de upstream não responder às solicitações TCP SYN, falhar ao retornar um código de resposta HTTP ou retornar uma resposta HTTP 504 (Gateway Timeout), o SWA considerará o proxy de upstream indisponível e alterará seu status de Íntegro para Doente.

Tip: O SWA considera um proxy de upstream saudável se retornar um cabeçalho VIA.

Informações Relacionadas

- Manual do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance
- Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco
- Como isentar o tráfego do Office 365 da autenticação e descriptografia no Cisco Web

Security Appliance (WSA) - Cisco
- Use as práticas recomendadas de dispositivos da Web seguros - Cisco
- Bloquear o tráfego no Secure Web Appliance
- Bloquear tráfego de upload no dispositivo da Web seguro
- Bloquear download de arquivo executável em SWA
- Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance
- Autenticação de desvio no 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.