Configurar a cadeia de proxy entre o Secure Web Appliance e o Umbrella SWG

Contents

Introdução

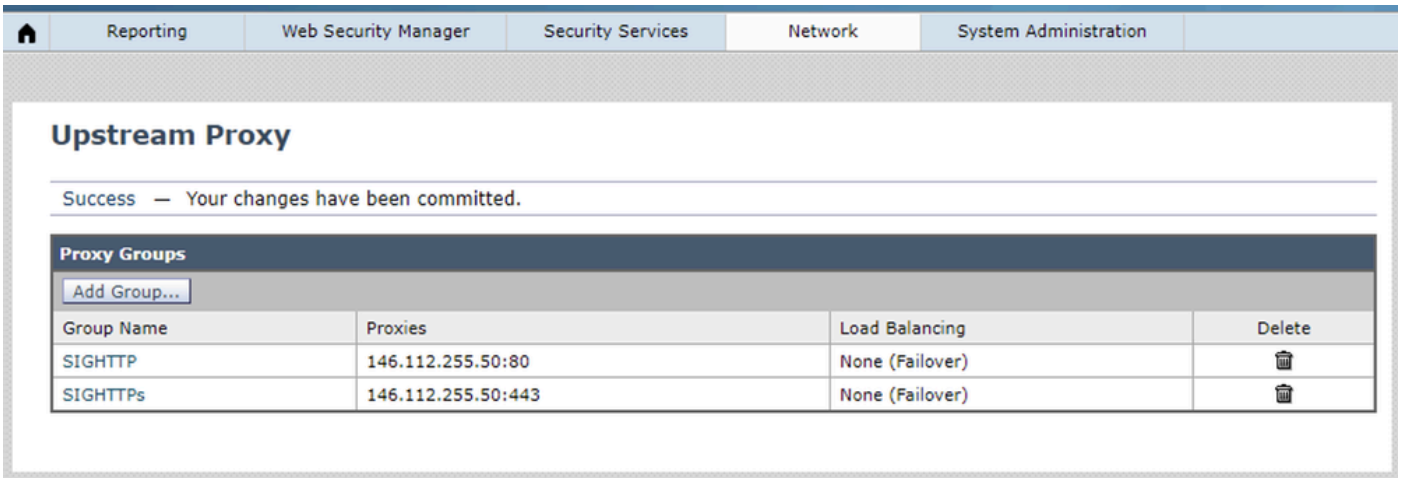
Este documento descreve como configurar a cadeia de proxy entre o Secure Web Appliance e o Umbrella Secure Web Gateway (SWG).

Overview

O Umbrella SIG suporta a cadeia de proxy e pode lidar com todas as solicitações HTTP/HTTPs do servidor proxy downstream. Este é um guia abrangente para implementar a cadeia de proxy entre o Cisco Secure Web Appliance (antigo Cisco WSA) e o Umbrella Secure Web Gateway (SWG), incluindo a configuração para o Secure Web Appliance e o SWG.

Configuração de política do Secure Web Appliance

1. Configure os links SWG HTTP e HTTPs como o Proxy de Upstream via Rede>Proxy de Upstream.

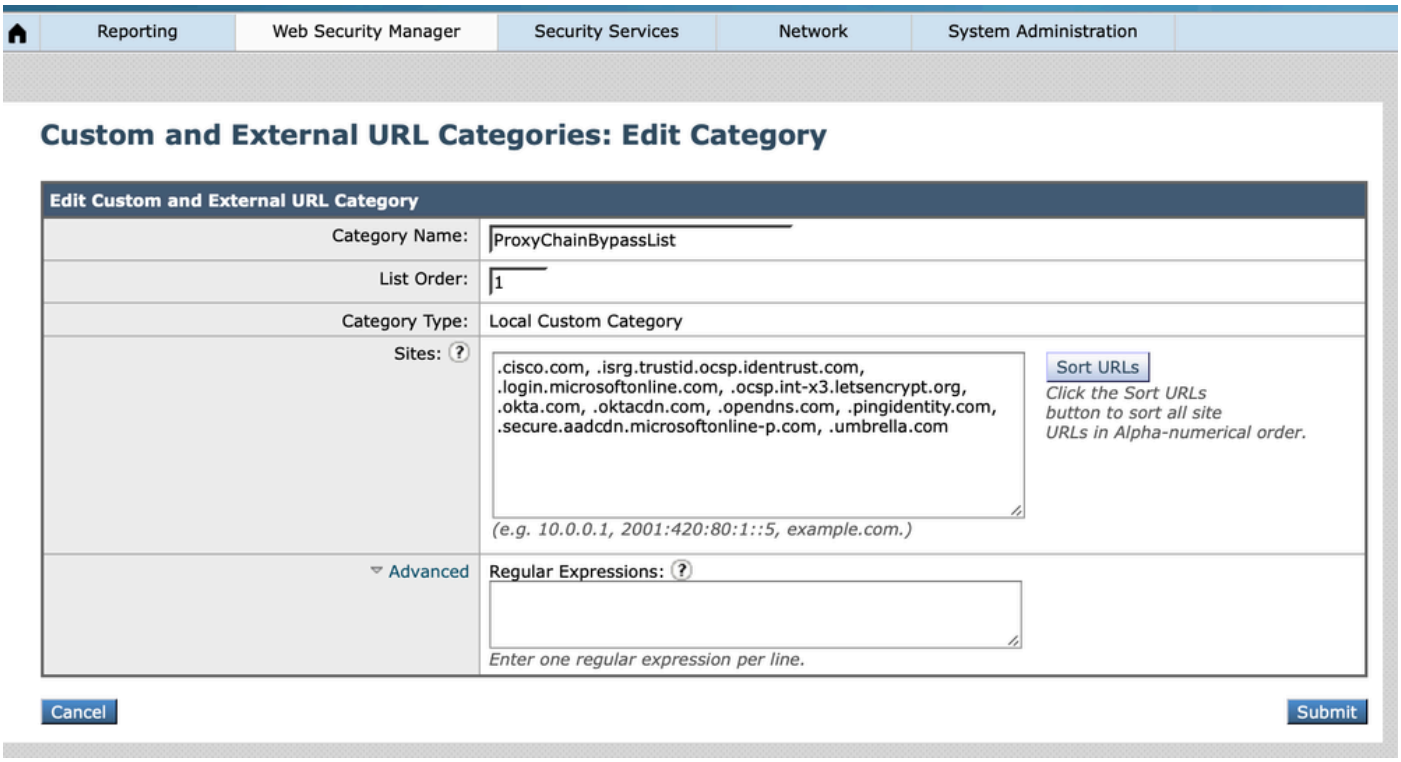


360079596451

2. Crie uma política de desvio através do Web Security Manager>Routing Policy para rotear todos

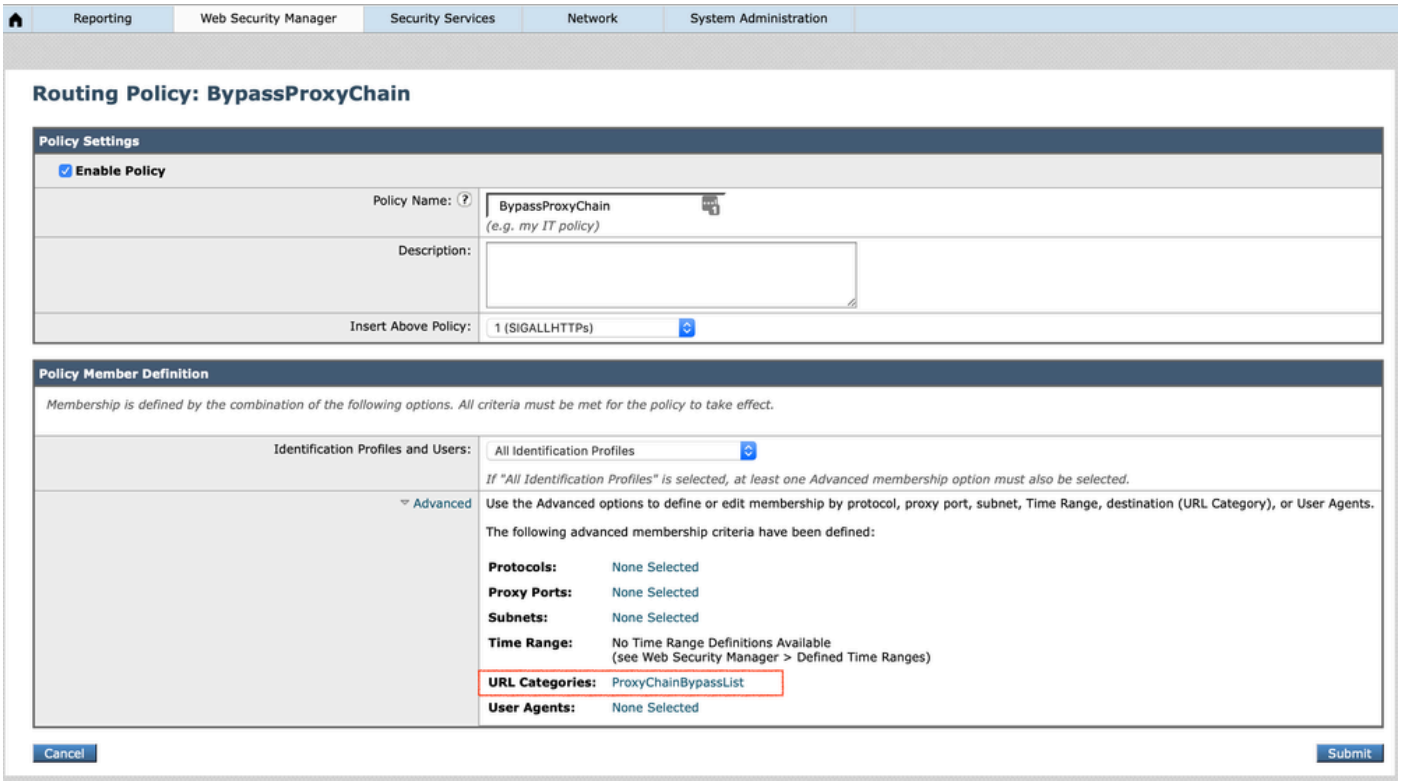
os URLs sugeridos diretamente para a Internet. Todos os URLs ignorados podem ser encontrados em nossa documentação: [Guia do usuário do Cisco Umbrella SIG: Gerenciar Encadeamento de Proxy]

- Comece criando uma nova "Categoria Personalizada" navegando até Web Security Manager>Categorias de URL Personalizadas e Externas, conforme mostrado aqui. A política de desvio é baseada na "Categoria Personalizada".



360050592552

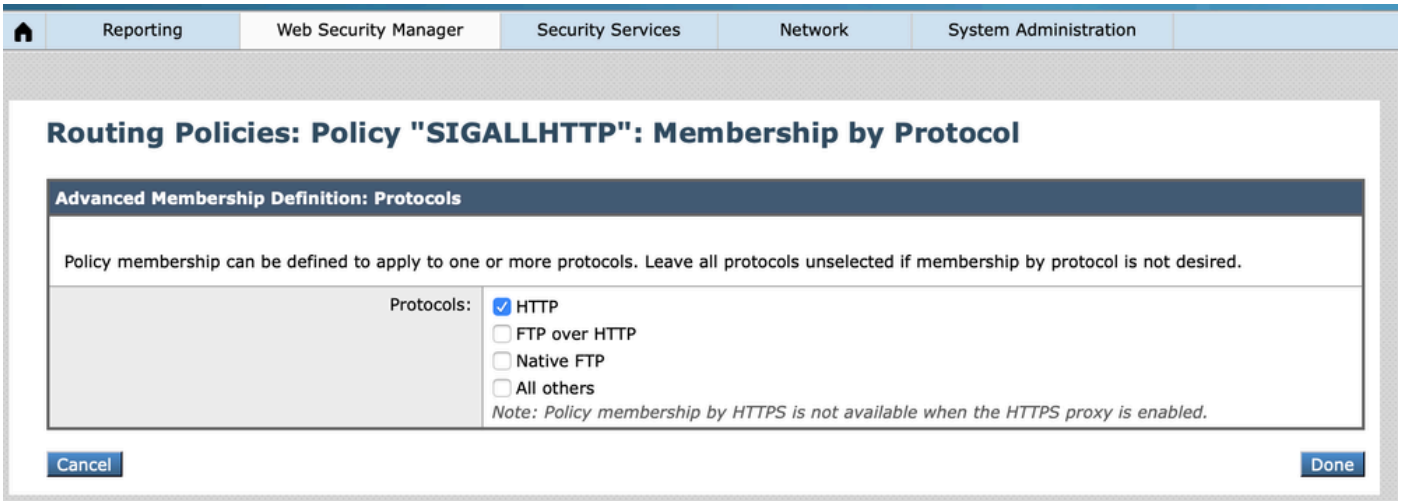
- Em seguida, crie uma nova política de desvio de roteamento navegando até Web Security Manager>Routing Policy. Certifique-se de que esta política seja a primeira, pois o Secure Web Appliance corresponde à política com base na ordem da política.



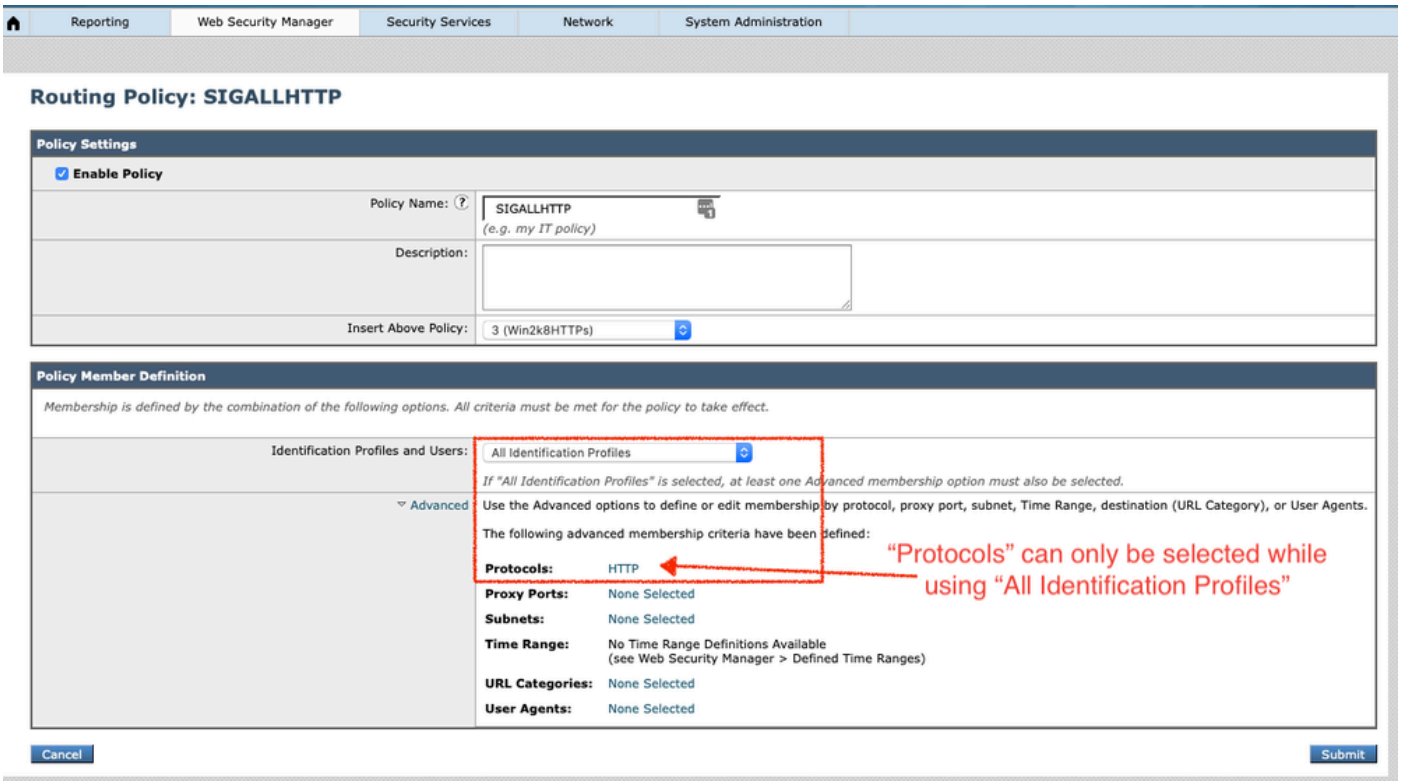
360050703131

3. Crie uma nova política de roteamento para todas as solicitações HTTP.

- Na definição de membro da política de roteamento do Secure Web Appliance, as opções de protocolo são HTTP, FTP sobre HTTP, FTP nativo e "Todos os outros", enquanto "Todos os perfis de identificação" são selecionados. Como não há opção para HTTPs, crie a política de roteamento para solicitações HTTPs individualmente após implementar essa política de roteamento para todas as solicitações HTTP.

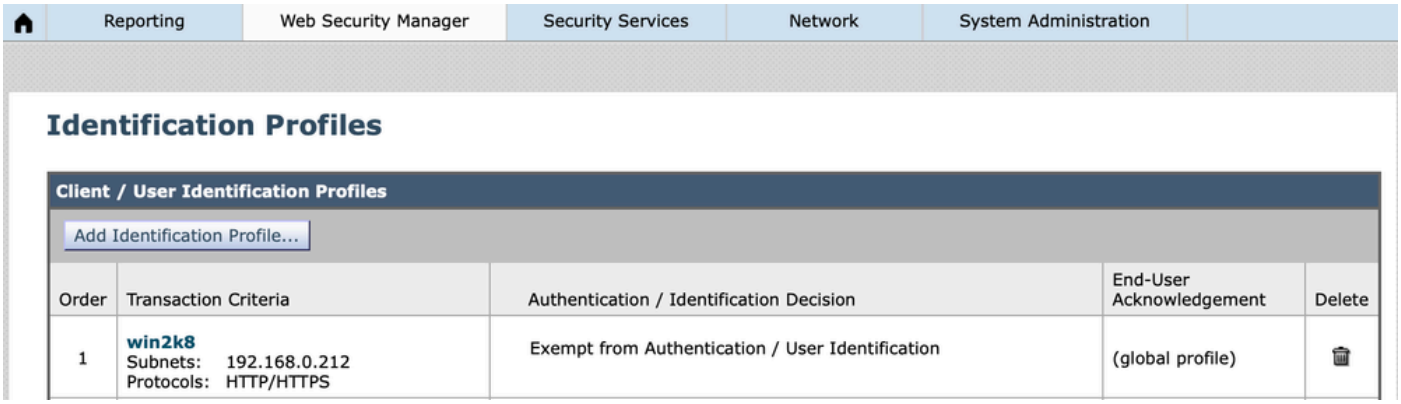


360050592772

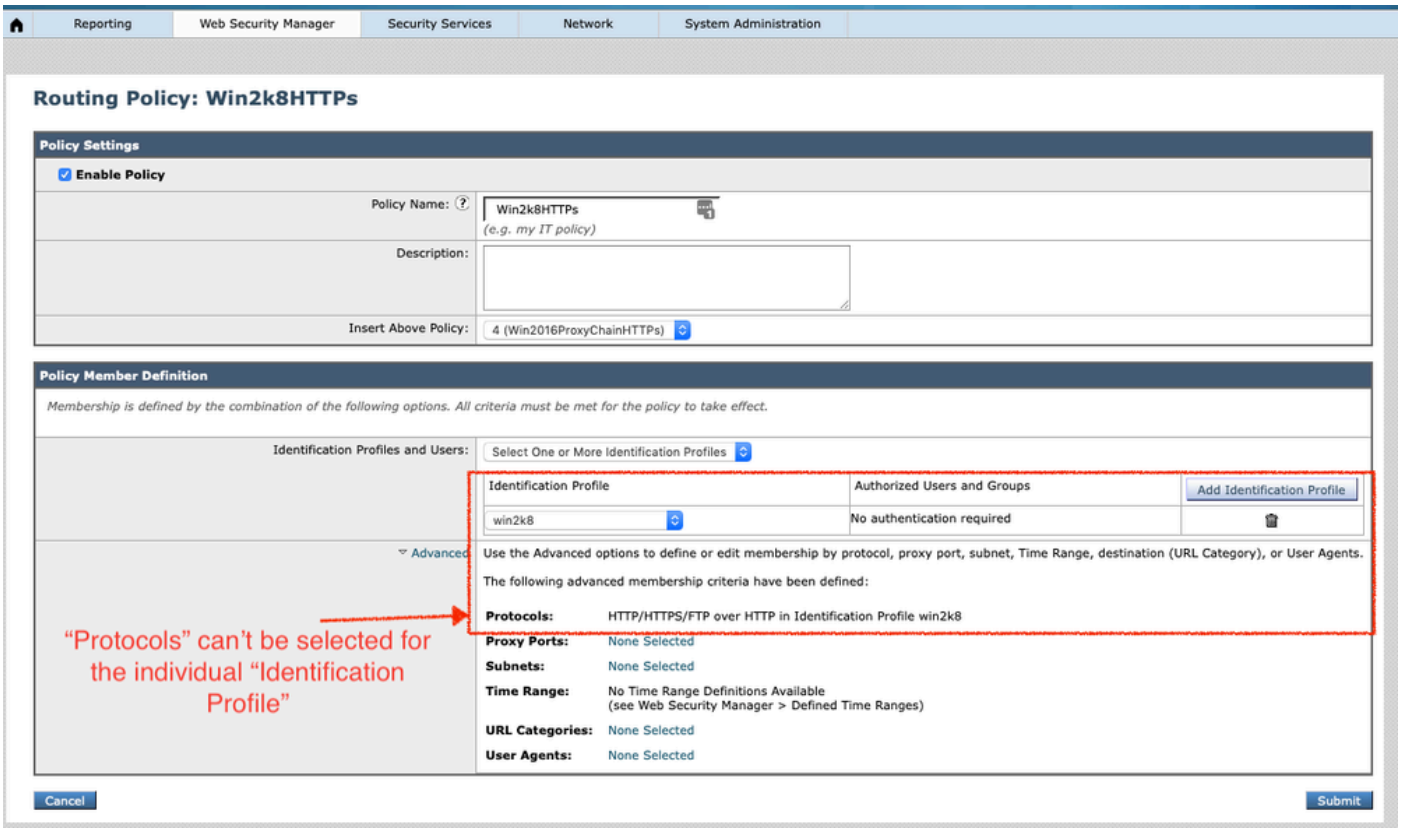


360050589572

4. Crie a política de roteamento para solicitações HTTPs com base no "Perfil de Identificação". Tenha cuidado com a sequência do "Perfil de identificação" definido, pois o Secure Web Appliance corresponde à "Identificação" da primeira correspondência. Neste exemplo, o perfil de identificação "win2k8" é uma identidade baseada em IP interno.



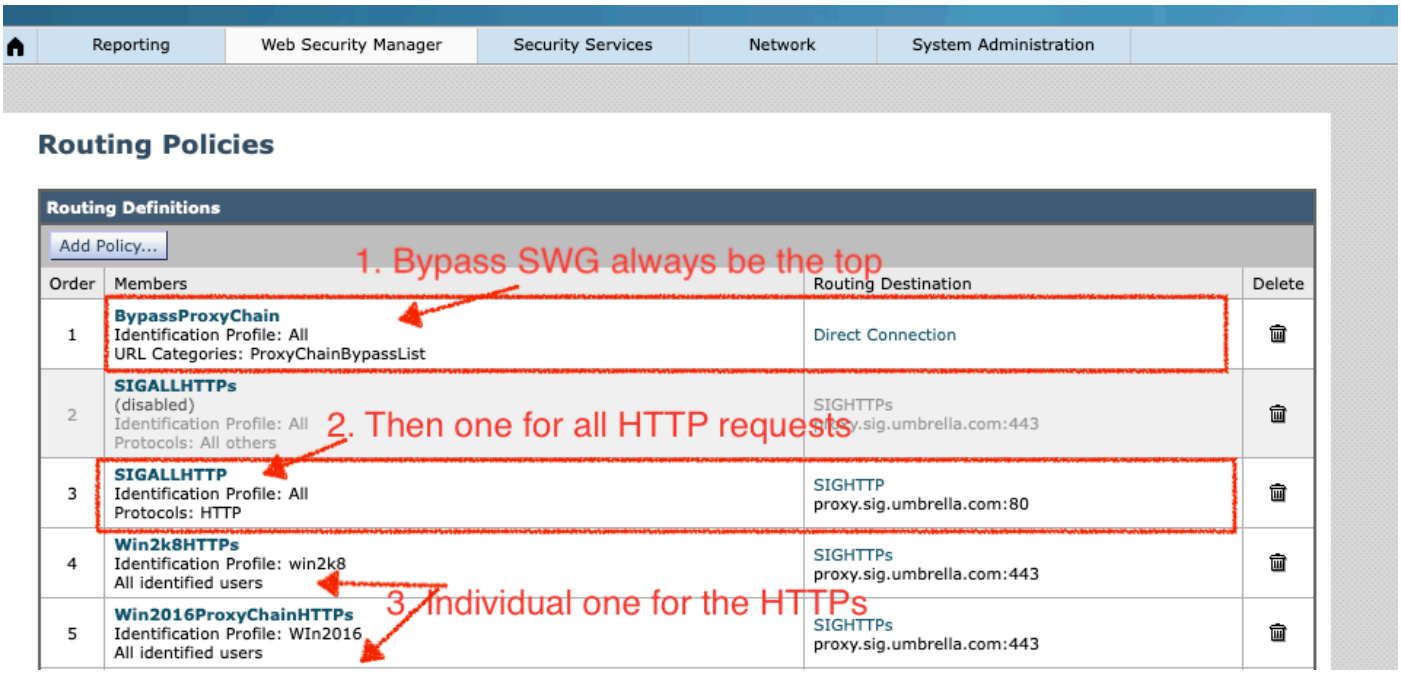
360050703971



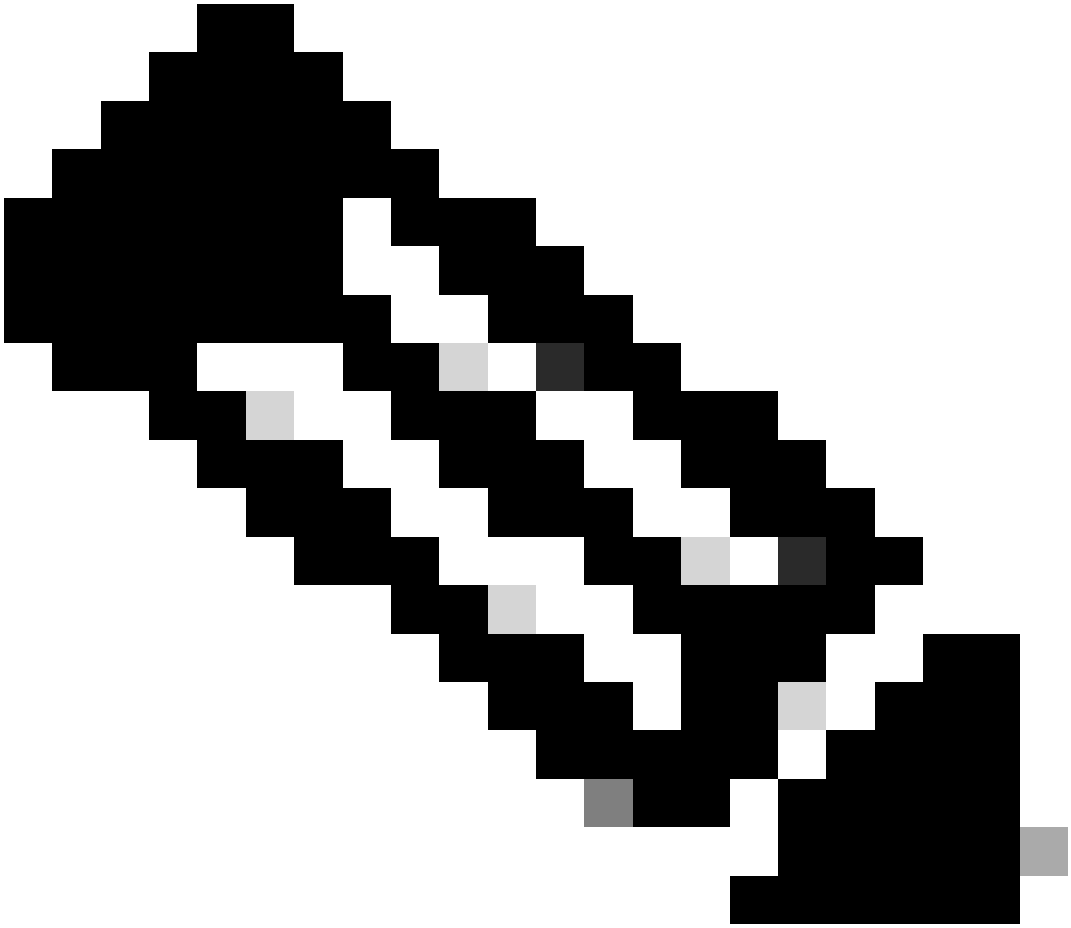
360050700091

5. Configurações finais para as Políticas de Roteamento do Secure Web Appliance:

- Tenha em mente que o Secure Web Appliance avalia as identidades e acessa as políticas usando uma abordagem de processamento de regras "de cima para baixo". Isso significa que a primeira correspondência feita em qualquer ponto no processamento resulta na ação tomada pelo Secure Web Appliance.
- Além disso, as identidades são avaliadas primeiro. Quando o acesso de um cliente corresponde a uma identidade específica, o Secure Web Appliance verifica todas as políticas de acesso configuradas para usar a identidade que corresponde ao acesso do cliente.



360050700131



Note: A configuração de política mencionada é aplicável somente para Implantação de proxy explícito.

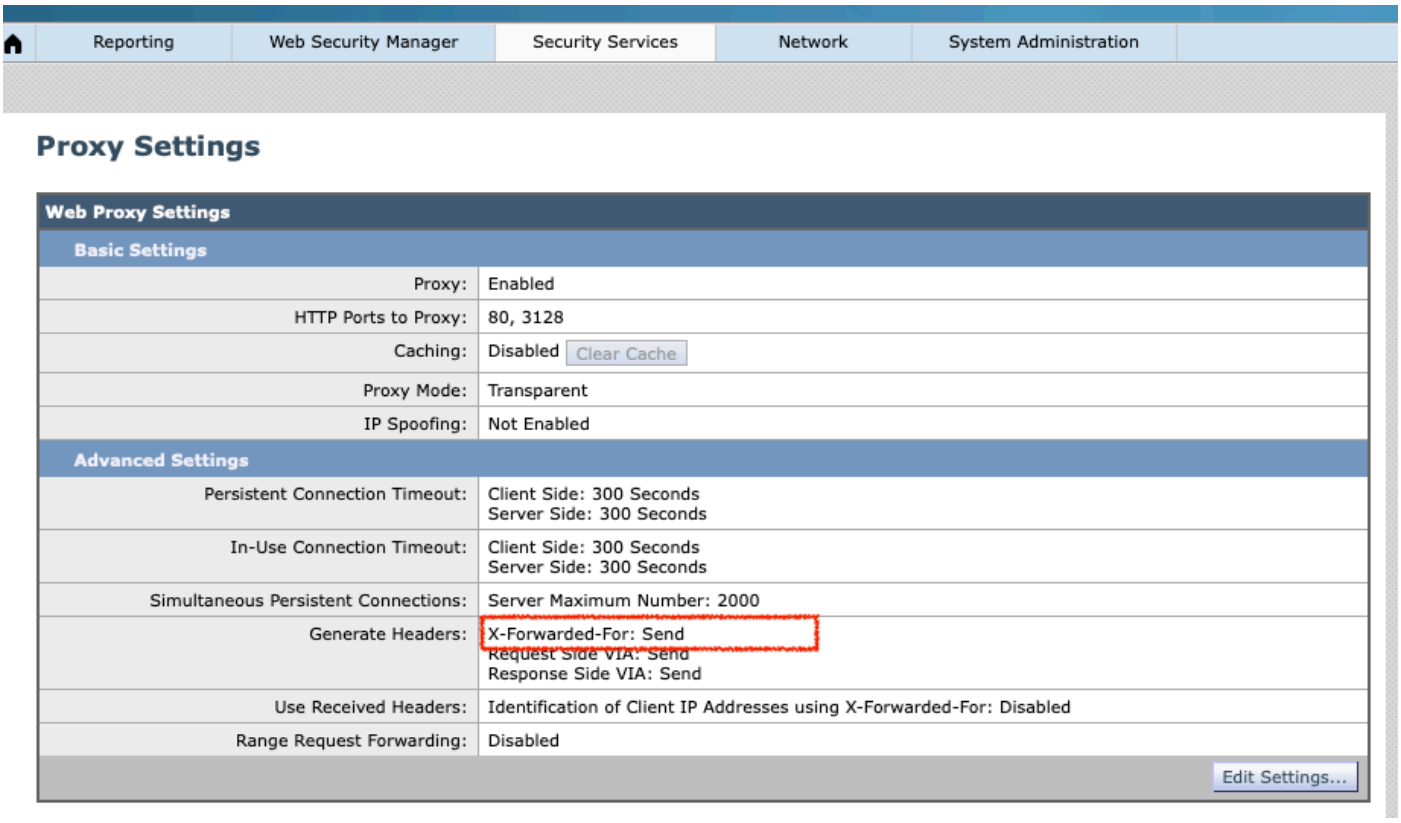
Para implantação transparente de proxy

No caso de HTTPS transparente, o AsyncOS não tem acesso às informações nos cabeçalhos do cliente. Portanto, o AsyncOS não pode aplicar políticas de roteamento se qualquer política de roteamento ou perfil de identificação depender das informações nos cabeçalhos do cliente.

1. Transações HTTPS redirecionadas de forma transparente só correspondem às Políticas de roteamento se:
    - O Grupo de Política de Roteamento não tem um critério de participação de política definido, como categoria de URL, Agente de Usuário etc.
    - O perfil de identificação não tem critérios de participação em políticas, como categoria de URL, agente de usuário etc. definidos.
2. Se qualquer Perfil de identificação ou Política de roteamento tiver uma categoria de URL personalizada definida, todas as transações HTTPS transparentes corresponderão ao Grupo de política de roteamento padrão.
3. Evite configurar a Política de Roteamento com Todos os Perfis de Identificação, pois isso pode fazer com que transações HTTPS transparentes correspondam ao Grupo de Política de Roteamento Padrão.

1. Cabeçalho X-Encaminhado-Para

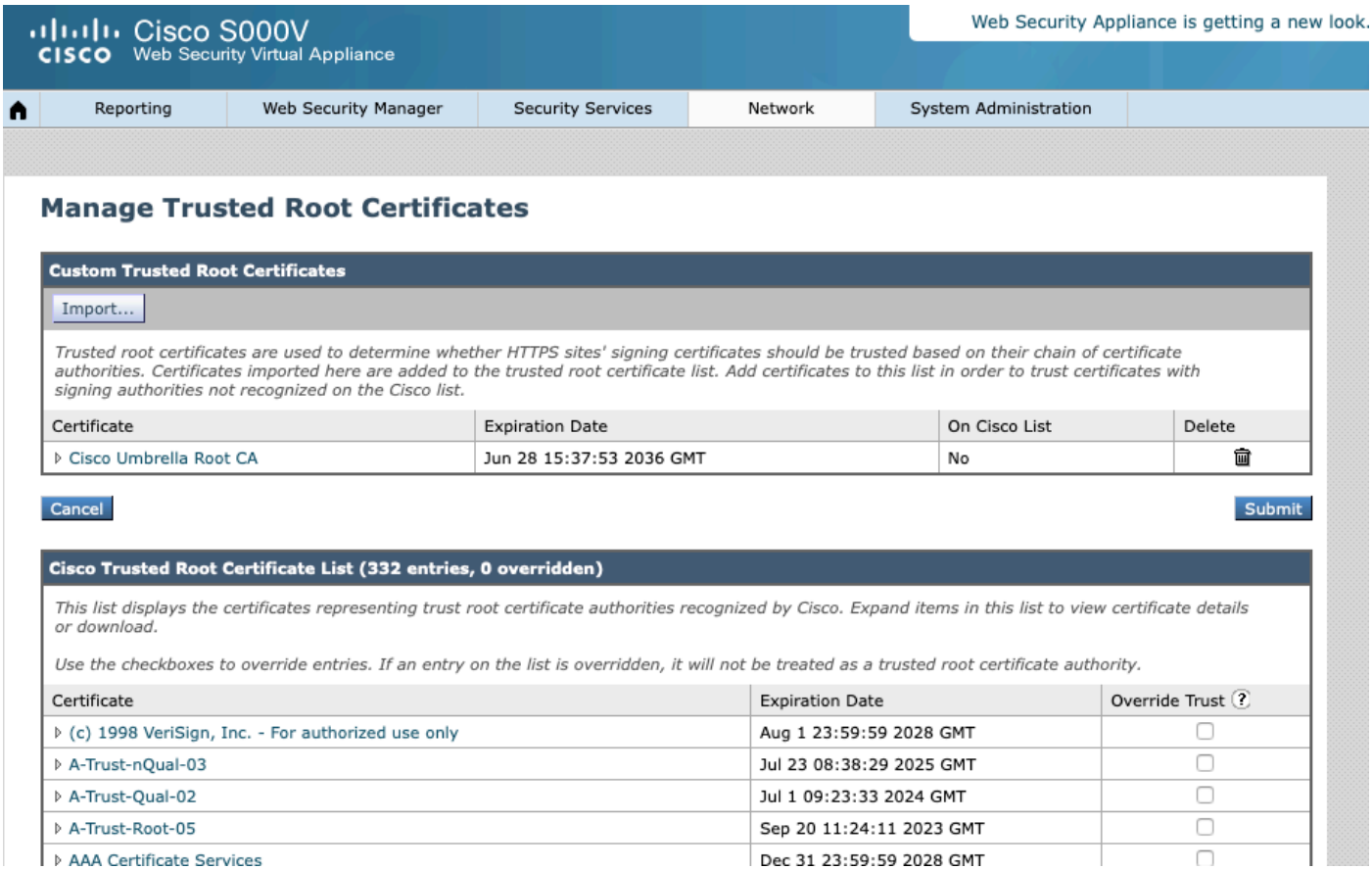
- para implementar a política da Web baseada em IP interna no SWG.Certifique-se de habilitar o cabeçalho "X-Forwarded-For" no Secure Web Appliance via Security Services > Proxy Settings.



360050700111

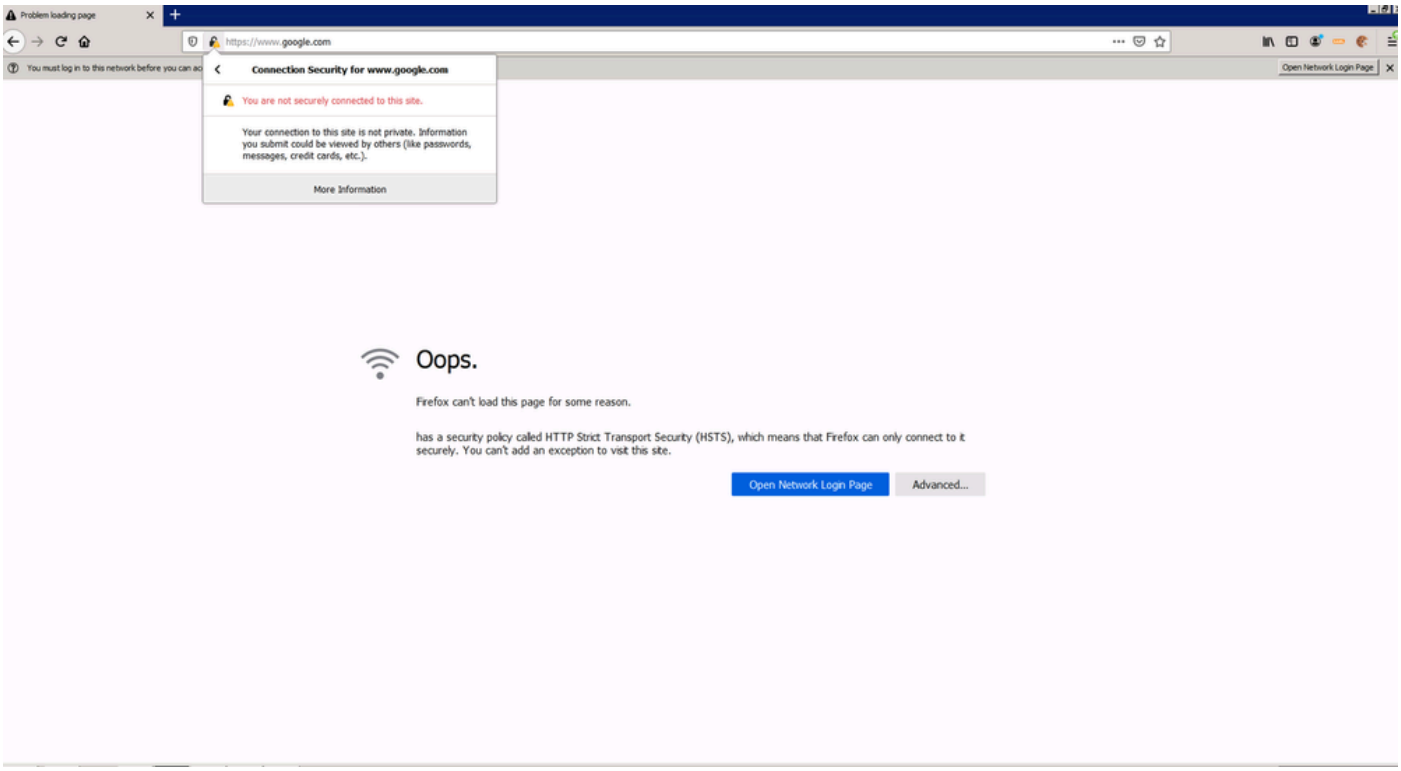
2. Certificado raiz confiável para descriptografia de HTTPs.

- Se a descriptografia de HTTPs estiver habilitada em Web Policy no painel Umbrella, baixe "Cisco Root Certificate" do Umbrella dashboard> Deployments> Configuration e importe-o para os certificados raiz confiáveis do Secure Web Appliance.



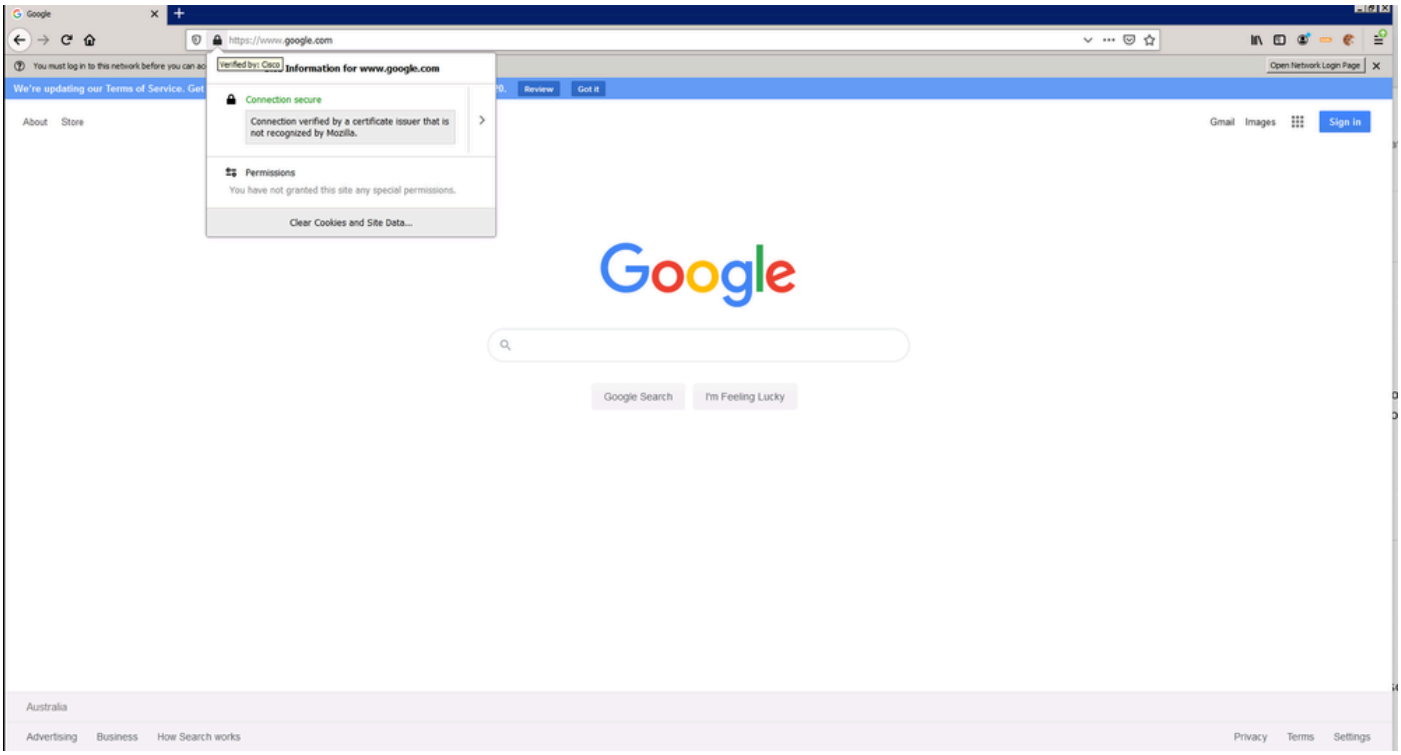
360050589612

- Se o "Certificado raiz da Cisco" não tiver sido importado para o Secure Web Appliance enquanto a descriptografia de HTTPs estiver habilitada na SWG Web Policy, o usuário final receberá um erro semelhante a este exemplo:
  - "Opa. (navegador) não pode carregar esta página por algum motivo. A tem uma política de segurança chamada HTTP Strict Transport Security (HSTS), o que significa que o (navegador) só pode se conectar a ele com segurança. Você não pode adicionar uma exceção para visitar este site."
  - "Você não está conectado com segurança a este site."



360050700171

- Este é um exemplo dos HTTPs descriptografados pelo Umbrella SWG. O certificado é verificado pelo "Certificado raiz da Cisco" chamado "Cisco".



360050700191

Configuração da política da Web do SWG no painel Umbrella

Política da Web do SWG baseada em IP interno:

- Certifique-se de habilitar o cabeçalho "X-Forwarded-For" no Secure Web Appliance, pois o SWG conta com ele para identificar o IP interno.
- Registre o IP de saída do Secure Web Appliance em Deployment > Networks.
- Crie um IP interno da máquina cliente em Deployment > Configuration > Internal Networks. Selecione o IP de saída registrado do Secure Web Appliance (Etapa 1) depois de marcar/selecionar "Mostrar redes".
- Crie uma nova Política da Web com base no IP interno criado na Etapa 2.
- Verifique se a opção "Habilitar SAML" está desabilitada na Política da Web.

Política da Web do SWG baseada em usuário/grupo do AD:

- Verifique se todos os usuários e grupos do AD foram provisionados no painel do Umbrella.
- Crie uma nova política da Web com base no IP de saída registrado do Secure Web Appliance com a opção "Enable SAML" ativada.
- Crie outra nova política da Web com base no usuário/grupo do AD com a opção "Habilitar SAML" desabilitada. Também é necessário posicionar essa política da Web antes da Política da Web criada na Etapa 2.

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.