Ignorar autenticação no Secure Web Appliance

Contents

Introdução

Este documento descreve as etapas para isentar a autenticação no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.

A Cisco recomenda que você tenha estas ferramentas instaladas:

- SWA físico ou virtual
- Acesso administrativo à interface gráfica do usuário (GUI) 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.

Autenticação Isenta

Isentar a autenticação para determinados usuários ou sistemas no Cisco SWA pode ser crucial

para manter a eficiência operacional e atender a requisitos específicos. Primeiro, alguns usuários ou sistemas exigem acesso ininterrupto a recursos ou serviços críticos que podem ser prejudicados por processos de autenticação. Por exemplo, os sistemas automatizados ou as contas de serviço que executam atualizações ou backups regulares precisam de acesso perfeito sem atrasos ou falhas potenciais introduzidas pelos mecanismos de autenticação.

Além disso, há situações em que o provedor de serviços da Web recomenda não usar um proxy para acessar seu serviço. Nesses casos, a isenção da autenticação garante a conformidade com as diretrizes do provedor e mantém a confiabilidade do serviço. Além disso, para bloquear efetivamente o tráfego para determinados usuários, muitas vezes é necessário primeiro isentá-los da autenticação e, em seguida, aplicar as políticas de bloqueio apropriadas. Essa abordagem permite um controle preciso sobre as permissões de acesso.

Em alguns casos, o serviço da Web que está sendo acessado é confiável e universalmente aceitável, como as atualizações da Microsoft. Isentar a autenticação para esses serviços simplifica o acesso de todos os usuários. Além disso, há situações em que o sistema operacional ou aplicativo do usuário não suporta o mecanismo de autenticação configurado no SWA, necessitando de um desvio para garantir a conectividade.

Por fim, os servidores com endereços IP fixos que não têm logins de usuário e têm acesso limitado e confiável à Internet não exigem autenticação, pois seus padrões de acesso são previsíveis e seguros.

Ao isentar estrategicamente a autenticação para esses casos, as empresas podem equilibrar as necessidades de segurança com a eficiência operacional.

Métodos para isenção de autenticação no Cisco SWA

A isenção de autenticação em SWA pode ser obtida por meio de vários métodos, cada um adaptado a cenários e requisitos específicos. Aqui estão algumas maneiras comuns de configurar isenções de autenticação:

- Endereço IP ou Máscara de sub-rede: um dos métodos mais diretos é isentar da autenticação endereços IP específicos ou sub-redes inteiras. Isso é particularmente útil para servidores com endereços IP fixos ou segmentos de rede confiáveis que exigem acesso ininterrupto à Internet ou a recursos internos. Especificando esses endereços IP ou máscaras de sub-rede na configuração SWA, você pode garantir que esses sistemas ignorem o processo de autenticação.
- Portas proxy: você pode configurar o SWA para isentar o tráfego com base em portas proxy específicas. Isso é útil quando determinados aplicativos ou serviços usam portas designadas para comunicação. Ao identificar essas portas, você pode configurar o SWA para ignorar a autenticação do tráfego nessas portas, garantindo acesso contínuo para os aplicativos ou serviços relevantes.
- Categorias de URL: outro método é isentar a autenticação com base nas categorias de URL. Isso pode incluir categorias predefinidas da Cisco e categorias de URL personalizadas

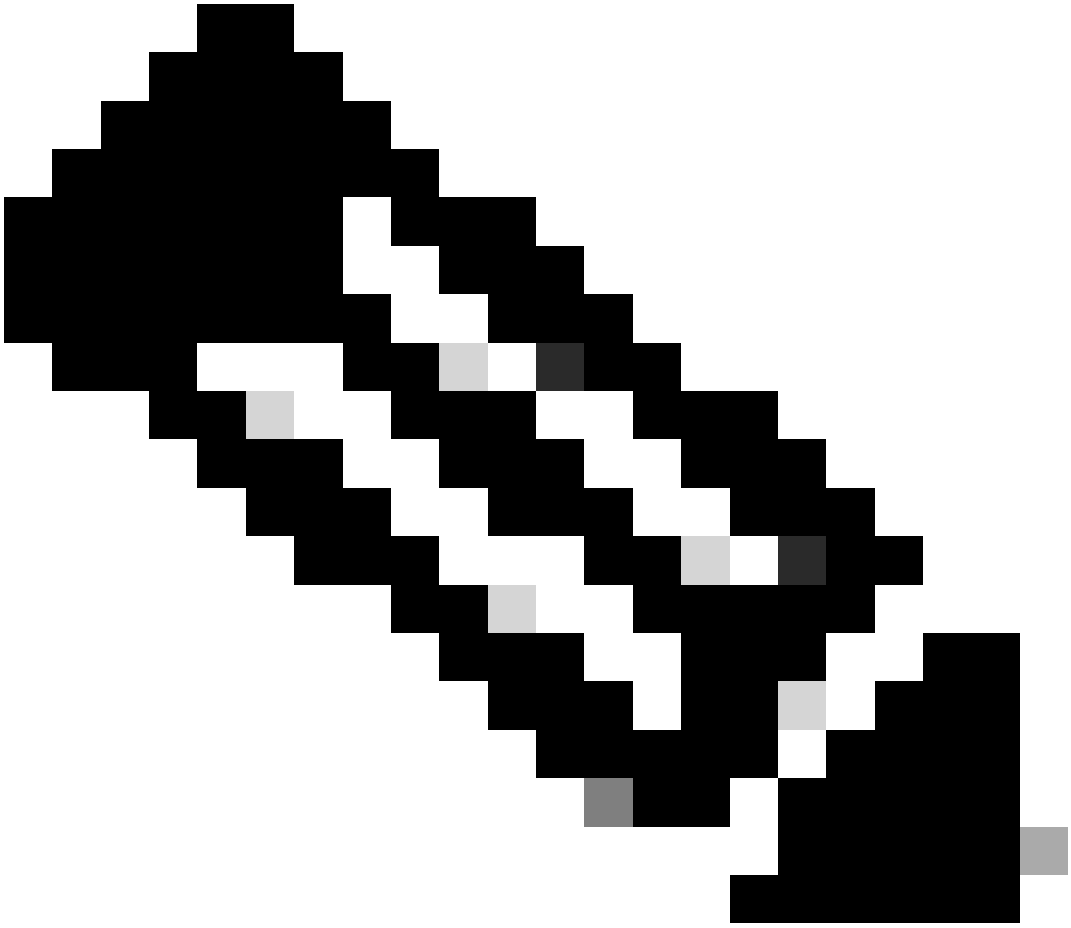
que você define com base nas necessidades específicas da sua organização. Por exemplo, se determinados serviços da Web, como atualizações da Microsoft, forem considerados confiáveis e universalmente aceitáveis, você poderá configurar o SWA para ignorar a autenticação para essas categorias de URL específicas. Isso garante que todos os usuários possam acessar esses serviços sem a necessidade de autenticação.
- Agentes de usuário: isentar a autenticação com base nos agentes de usuário é útil ao lidar com aplicativos ou dispositivos específicos que não suportam os mecanismos de autenticação configurados. Ao identificar as sequências de caracteres do agente do usuário desses aplicativos ou dispositivos, você pode configurar o SWA para ignorar a autenticação para o tráfego originário deles, garantindo conectividade contínua.

.

Etapas para ignorar a autenticação

Estas são as etapas para criar um perfil de identificação para isentar da autenticação:

Etapa 1. Na GUI, escolha Web Security Manager e clique em Identification Profiles.
Etapa 2. Clique em Add Profile para adicionar um perfil.
Etapa 3. Use a caixa de seleção Enable Identification Profile para ativar esse perfil ou para desativá-lo rapidamente sem excluí-lo.
Etapa 4. Atribua um Nome de perfil exclusivo.
Etapa 5. (Opcional) Adicione Descrição.
Etapa 6. Na lista suspensa Inserir o, escolha onde esse perfil deve aparecer na tabela.

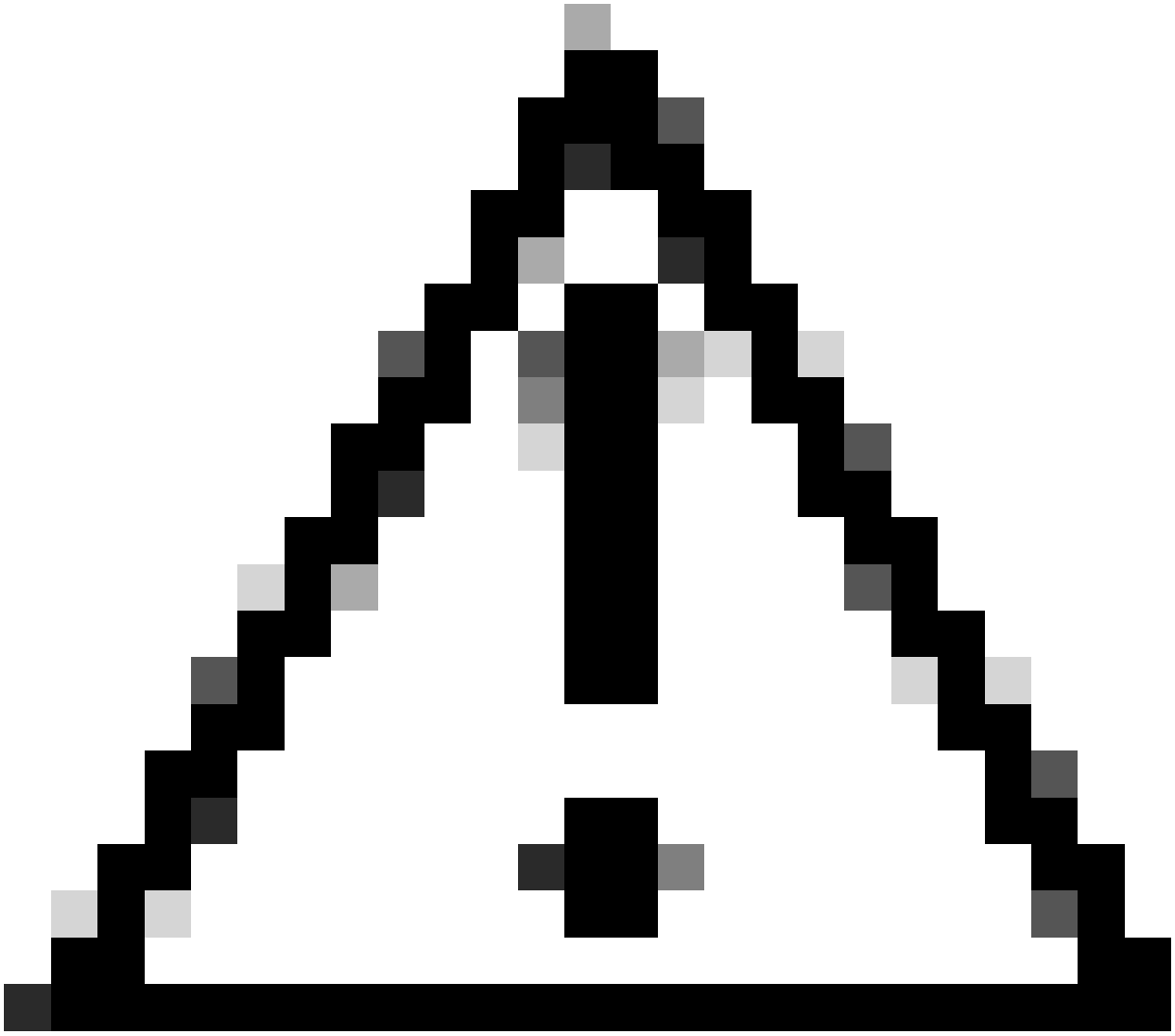


Observação: os perfis de identificação de posição que não exigem autenticação estão no topo da lista. Essa abordagem reduz a carga no SWA, minimiza a fila de autenticação e resulta em autenticação mais rápida para outros usuários.

Passo 7. Na seção Método de identificação do usuário, escolha Isento de autenticação/identificação.

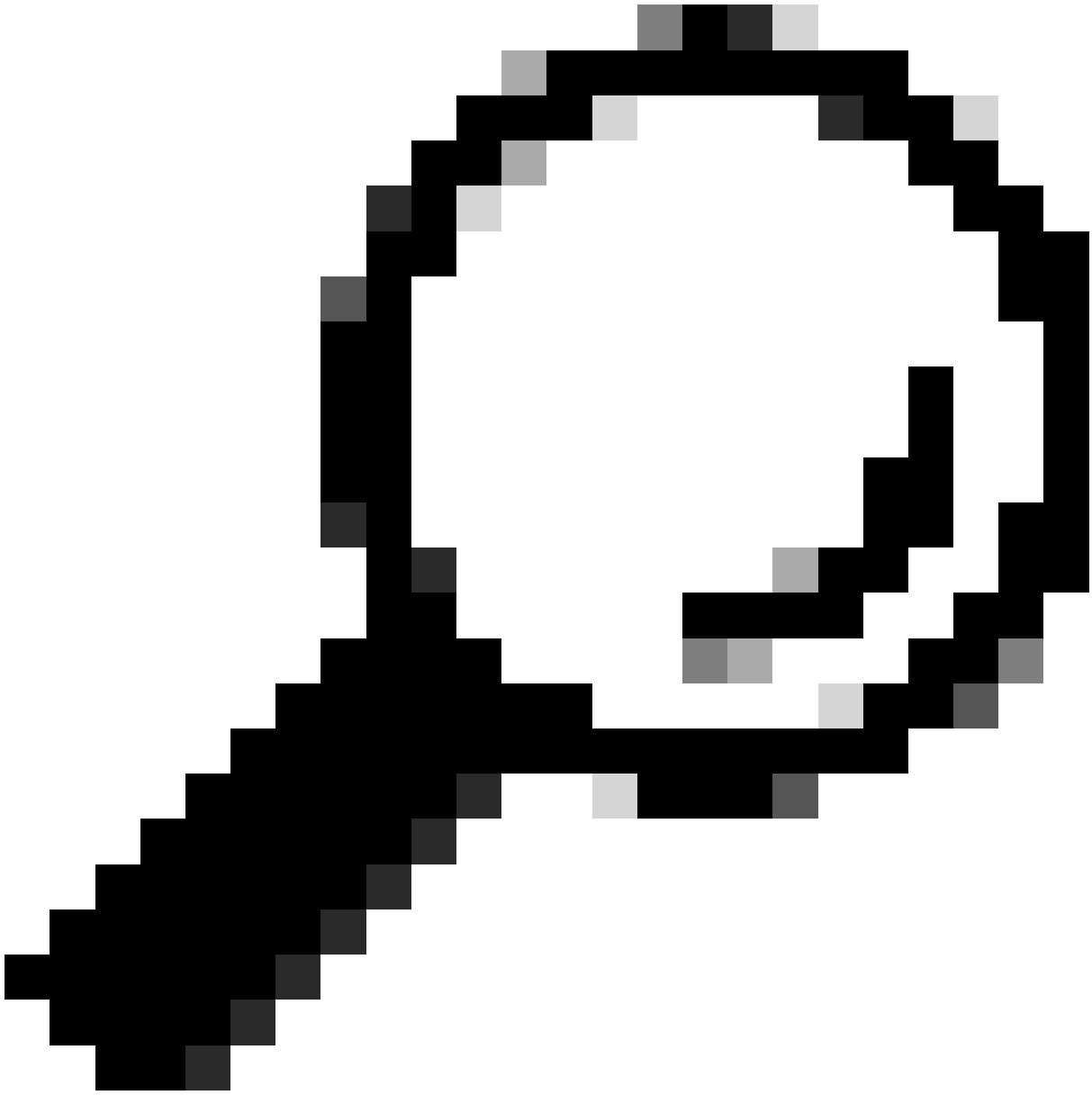
Etapa 8. Em Definir membros por sub-rede, insira os endereços IP ou sub-redes que este perfil de identificação deve aplicar. Você pode usar endereços IP, blocos de roteamento entre domínios sem classe (CIDR) e sub-redes.

Etapa 9. (Opcional) Clique em Avançado para definir critérios de participação adicionais, como Portas de Proxy, Categorias de URL ou Agentes de Usuário.



Cuidado: na implantação de proxy transparente, o SWA não pode ler agentes de usuário ou a URL completa para tráfego HTTPS, a menos que o tráfego seja descriptografado. Como resultado, se você configurar o Perfil de identificação usando Agentes de usuário ou uma Categoria de URL personalizada com expressões regulares, esse tráfego não corresponderá ao Perfil de identificação.

Para obter mais informações sobre como configurar a categoria de URL personalizada, visite: [Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco]



Dica: a política usa uma lógica AND, o que significa que todas as condições devem ser atendidas para que o perfil de ID seja correspondente. Quando as opções Advanced são definidas, cada requisito deve ser atendido para que a política seja aplicada.

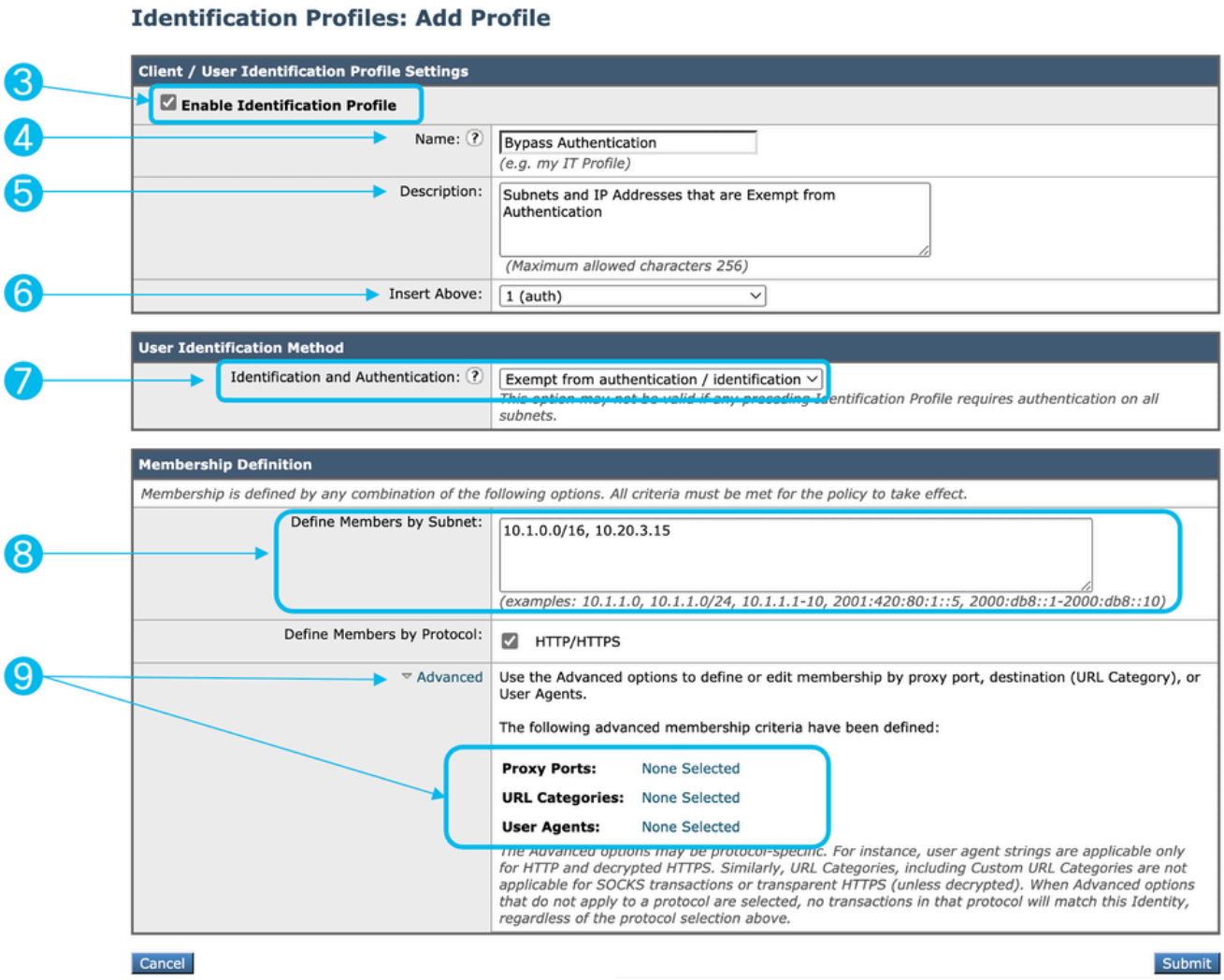


Imagem - Etapas para criar perfil de ID para ignorar autenticação

Etapa 10. Enviar e confirmar alterações.

Informações Relacionadas

- Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - GD (General Deployment) - Classifique os usuários finais para aplicação de política [Cisco Secure Web Appliance] - Cisco
- 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

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.