Configurar o Secure Web Appliance para permitir acesso de convidados

Contents

Introdução

Este documento descreve as etapas para permitir que os usuários que não instalaram o certificado de descriptografia acessem a Internet via Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SWA físico ou virtual instalado.
- Licença ativada ou instalada.
- O assistente de instalação foi concluído.

- 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.

Visão geral do cenário

Este artigo aborda um cenário de controle de acesso à rede dentro da sub-rede Wi-Fi 10.10.10.0/24. O ambiente consiste em dois grupos de usuários distintos que exigem políticas de segurança e acesso diferentes:

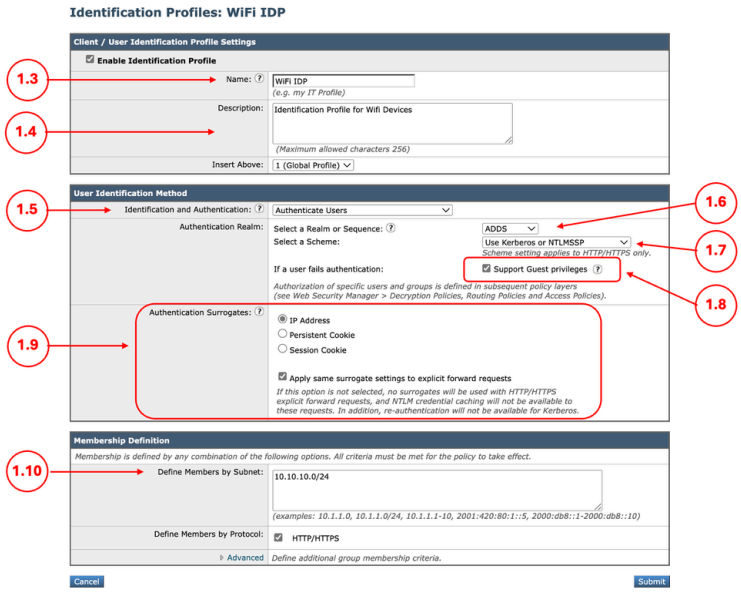
- Dispositivos gerenciados: Laptops fornecidos pela empresa que são totalmente autenticados e têm o certificado de descriptografia SWA instalado. Esses dispositivos são confiáveis e geralmente estão sujeitos às políticas de acesso corporativas padrão.
- Dispositivos não gerenciados/convidados: Laptops pessoais e dispositivos móveis não autenticados e sem o certificado de descriptografia SWA.

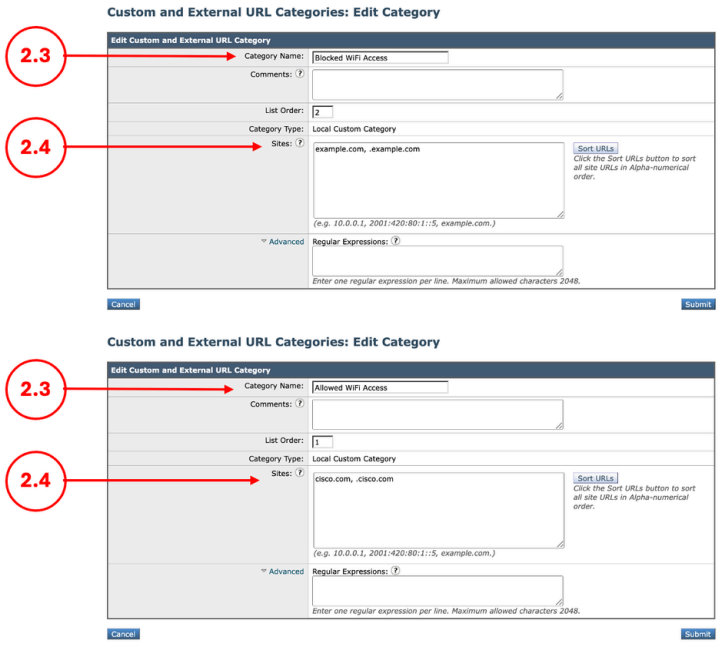
Objetivo:
A empresa tem como objetivo implementar políticas restritivas de acesso à Web para dispositivos não gerenciados, limitando sua conectividade a um subconjunto específico de URLs permitidos, garantindo que os recursos corporativos permaneçam seguros.

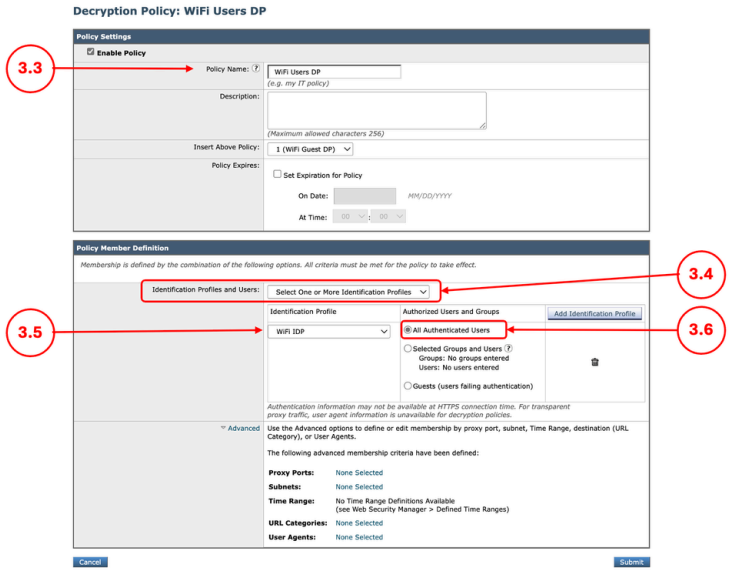
Note: Como o Certificado de descriptografia não é confiável nos dispositivos não gerenciados, você não pode descriptografar o tráfego HTTPS e a ação deve ser definida para passar.

Configuration Steps

Etapa 1. Criar Perfil de Identificação.	Etapa 1.1. Na GUI do SWA, navegue até o Web Security Manager e selecione Identification Profile. Etapa 1.2. Clique em Add Identification Profile. Etapa 1.3. Defina um Nome para o Perfil. Etapa 1.4. (Opcional) Defina a Descrição. Etapa 1.5. Selecione Authenticate Users em Identification and Authentication. Etapa 1.6. Escolha o realm do Ative Diretory em Selecionar um Realm ou Sequência. Etapa 1.7. Em Select a Scheme, selecione os

	protocolos de autenticação desejados. Tip: Não escolha Basic Authentication na lista Select a Scheme. Etapa 1.8. Marque a caixa de seleção Suporte a privilégios de convidado. Etapa 1.9. (Opcional) Dependendo do seu design, você pode habilitar o Substituto, habilitando Aplicar as mesmas configurações de substituto para solicitações de encaminhamento explícitas. Caution: Como não é possível descriptografar o tráfego, na implantação transparente, não selecione Cookie persistente ou Cookie de sessão. Etapa 1.10. Defina a sub-rede do endereço IP em, Definir membros por sub-rede. Etapa 1.11. Enviar e confirmar as alterações.  Imagem - Definir o perfil de identificação
Etapa 2. (Opcional) Criar as categorias de URL personalizadas para URLs permitidas e bloqueadas	Etapa 2.1.Na GUI, navegue até Web Security Manager e escolhaCategorias de URL personalizadas e externas. Etapa 2.2.Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada.

	Etapa 2.3.Digite o nome da nova categoria. Etapa 2.4.Defina o domínio e/ou subdomínios dos sites que você deseja bloquear o acesso. Etapa 2.5.Envie as alterações. Etapa 2.6. Use as mesmas etapas para criar uma categoria de URL para o site ao qual você está permitindo o acesso.  Imagem - Definir categoria de URL personalizada
Etapa 3. Criar política de descriptografia para dispositivos gerenciados	Etapa 3.1. Na GUI, navegue até Web Security Manager e escolhaPolíticas de descriptografia Etapa 3.2.Clique em Add Policy. Etapa 3.3.EnterName para a nova política. Etapa 3.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários. Etapa 3.5.Selecione oPerfil de identificação que foi criado na Etapa 1. Etapa 3.6. Selecione All Authenticated Users. Etapa 3.7.Clique em Enviar.



Criar política de descriptografia para dispositivos gerenciados

Etapa 3.8. Na página Políticas de descriptografia, clique no link de Filtragem de URL para a nova política.

Etapa 3.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 3.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

Etapa 3.11. Clique em Submit

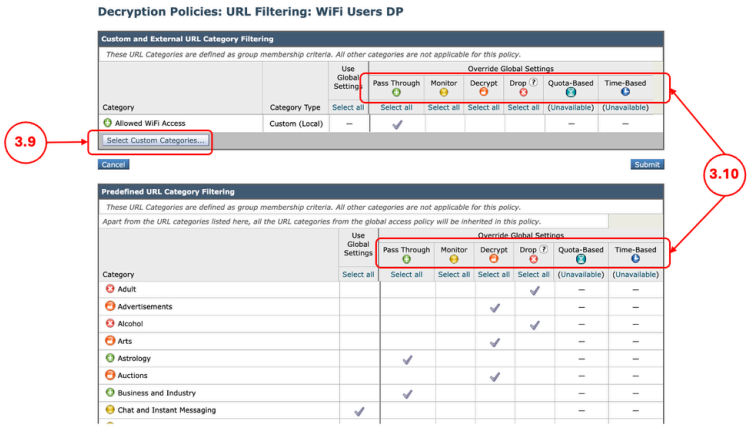
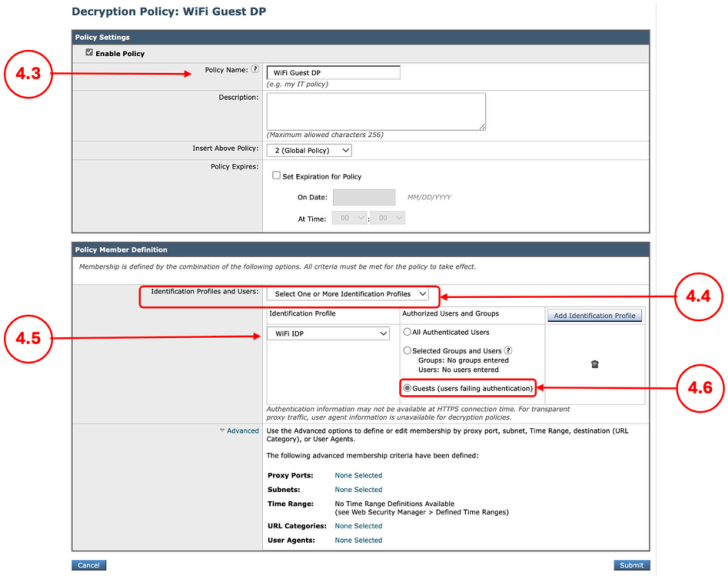
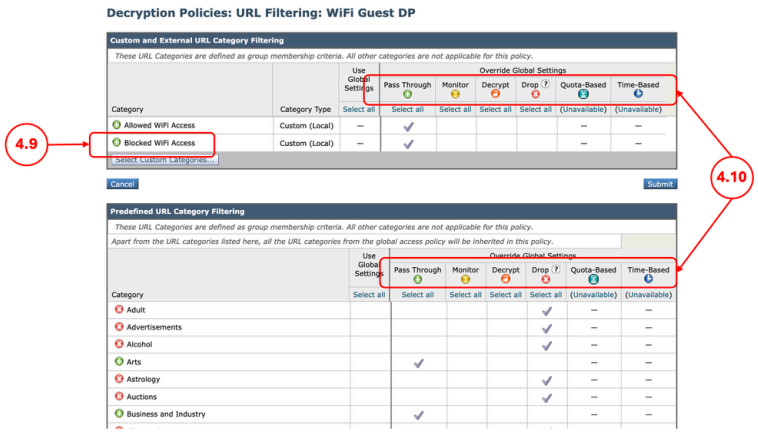


Imagem - Configurar Ação para Política de Descriptografia

Etapa 4. Criar política de	Etapa 4.1. Na GUI, navegue até Web Security Manager e escolhaPolíticas de descriptografia

descriptografia para dispositivos não gerenciados	Etapa 4.2.Clique em Add Policy. Etapa 4.3.EnterName para a nova política. Etapa 4.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários. Etapa 4.5.Selecione oPerfil de identificação que foi criado na Etapa 1. Etapa 4.6. Selecione Convidados (usuários com falha na autenticação). Etapa 4.7.Clique em Submit.  Criar política de descriptografia para dispositivos não gerenciados Etapa 4.8. Na página Políticas de descriptografia, clique no link de Filtragem de URL para a nova política. Etapa 4.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria Etapa 4.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida. Note: Não use Descriptografar como a ação, já que o certificado de descriptografia SWA não é

	confiável nos dispositivos não gerenciados.  Imagem - Ação de descriptografia para dispositivos não gerenciados Etapa 4.11. Role para baixo na seção URLs sem categoria e escolha a ação apropriada.  Imagem - URLs sem categoria Tip: Para a perspectiva de segurança, é melhor definir a ação como Eliminar, caso qualquer URL precise de acesso, você pode adicioná-los na Categoria de URL personalizada atribuída à Política. Etapa 4.12. Clique em Submit
Etapa 5. Criar política de acesso para dispositivos gerenciados	Etapa 5.1. Na GUI, navegue até Web Security Manager e escolhaAccess Policies Etapa 5.2.Clique em Add Policy. Etapa 5.3.EnterName para a nova política. Etapa 5.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários. Etapa 5.5.Selecione oPerfil de identificação que foi criado na Etapa 1.

Etapa 5.6. Selecione All Authenticated Users.

Etapa 5.7.Clique em Submit.

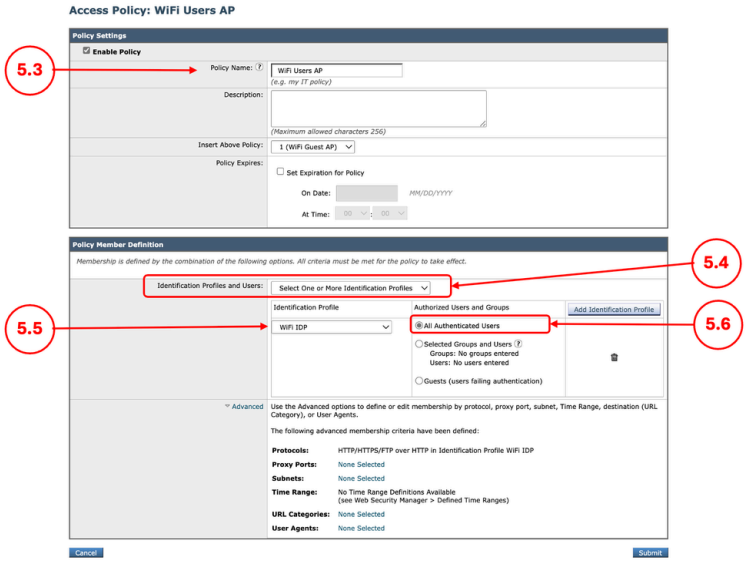


Imagem - Política de acesso para dispositivos gerenciados

Etapa 5.8. Na página Access Policies, clique no link de URL Filtering para a nova política.

Etapa 5.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 5.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

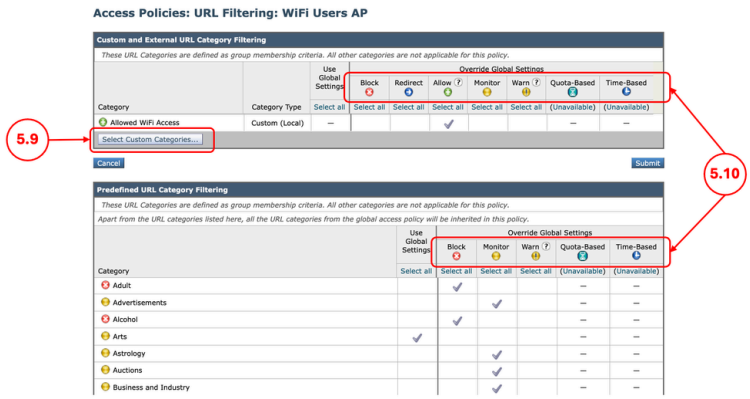
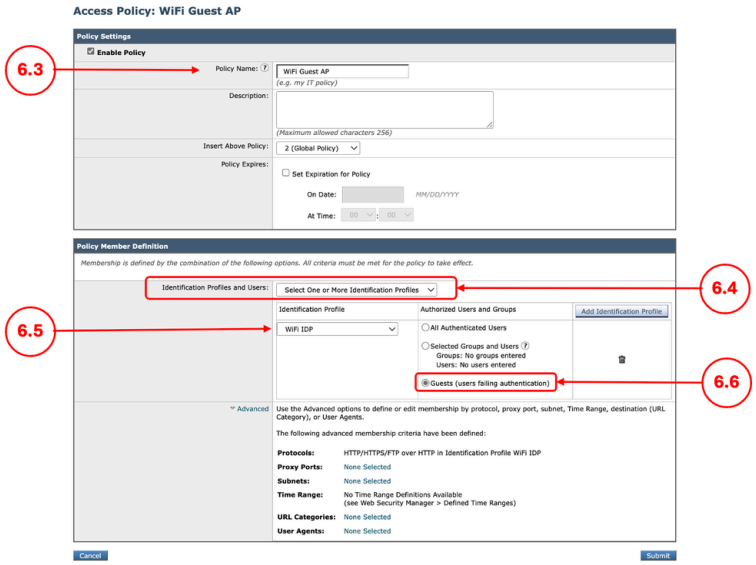


Imagem - Filtragem de URL de política de acesso para dispositivos gerenciados

Etapa 5.11. Clique em Submit.

Etapa 6. Criar política de acesso para dispositivos não gerenciados	Etapa 6.1. Na GUI, navegue até Web Security Manager e escolhaAccess Policies Etapa 6.2.Clique em Add Policy. Etapa 6.3.EnterName para a nova política. Etapa 6.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários. Etapa 6.5.Selecione oPerfil de identificação que foi criado na Etapa 1. Etapa 6.6. Selecione Convidados (usuários com falha na autenticação). Etapa 6.7.Clique em Submit.  Imagem - Política de acesso para dispositivos não gerenciados Etapa 6.8. Na página Access Policies, clique no link de URL Filtering para a nova política. Etapa 6.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria Etapa 6.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

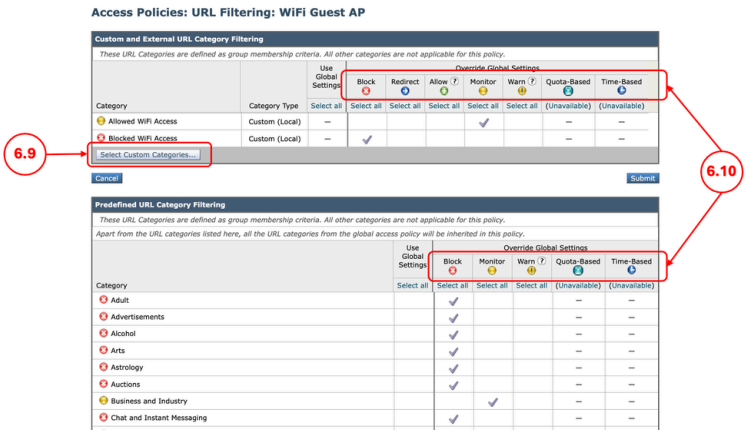
<table>
<tr>
<td></td>
<td>


Imagem - Filtragem de URL de política de acesso para dispositivos não gerenciados

Etapa 6.11. Role para baixo na seção URLs sem categoria e escolha a ação apropriada.

Imagem - URLs sem categoria da política de acesso

Tip: Para a perspectiva de segurança, é melhor definir a ação como Bloquear, caso qualquer URL precise de acesso, você pode adicioná-los na Categoria de URL personalizada atribuída à política.

Etapa 6.12. Clique em Enviar
</td>
</tr>
<tr>
<td>
Etapa 7. (Opcional) Criar a política de segurança de dados da Cisco para dispositivos gerenciados

Note: Se você não quiser filtrar o tráfego de carregamento para dispositivos gerenciados, ignore esta etapa.
</td>
<td>
Etapa 7.1. Na GUI, navegue até Web Security Manager e escolha Cisco Data Security.

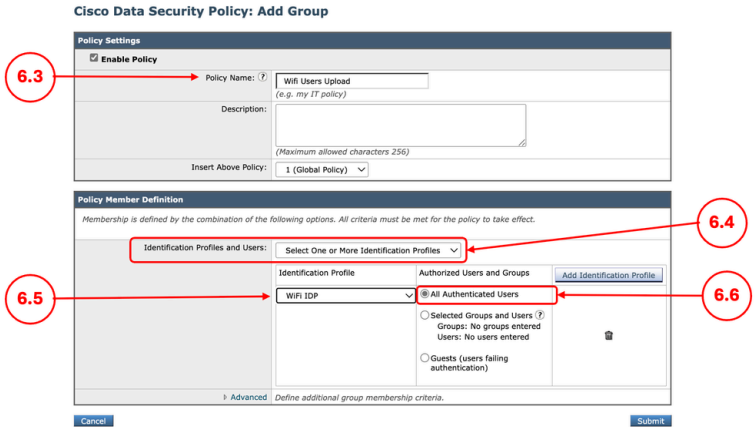
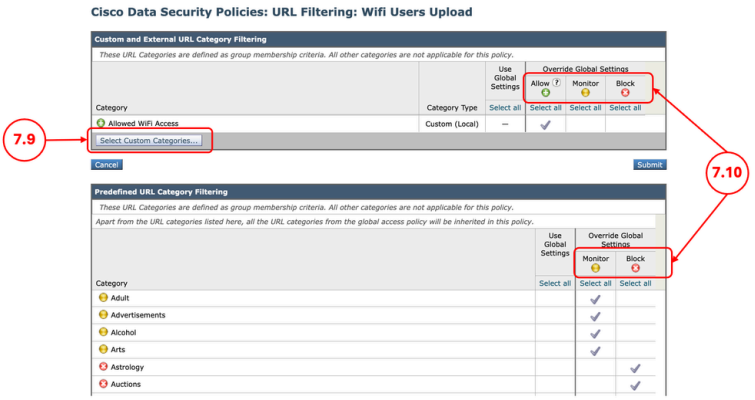
Etapa 7.2.Clique em Add Policy.

Etapa 7.3.EnterName para a nova política.

Etapa 7.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 7.5.Selecione oPerfil de identificação que foi criado na Etapa 1.

Etapa 7.6. Selecionar Todos os Usuários Autenticados.
</td>
</tr>
</table>

	Etapa 7.7.Clique em Submit.  Imagem - Política de segurança de dados da Cisco para dispositivos gerenciados Etapa 7.8. Na página Cisco Data Security Policies , clique no link de URL Filtering para a nova política. Etapa 7.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria Etapa 7.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.  Imagem - Ação de carregamento para dispositivos gerenciados Etapa 7.11. Clique em Submit.
Etapa 8. (Opcional) Criar a política de segurança de dados da Cisco para dispositivos não gerenciados	Etapa 8.1. Na GUI, navegue até Web Security Manager e escolha Cisco Data Security. Etapa 8.2.Clique em Add Policy.

Note: Se você não quiser filtrar o tráfego de carregamento para dispositivos não gerenciados, ignore esta etapa.

Etapa 8.3.EnterName para a nova política.

Etapa 8.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 8.5.Selecione oPerfil de identificação que foi criado na Etapa 1.

Etapa 8.6. Selecionar Todos os Usuários Autenticados.

Etapa 8.7.Clique em Enviar.

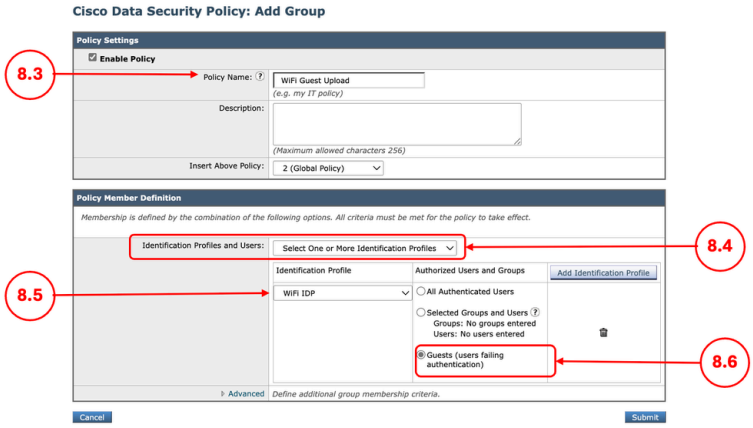
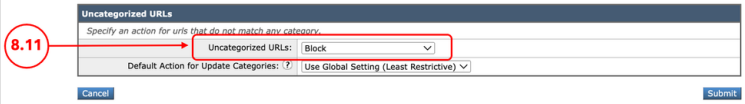


Imagem - Política de segurança de dados da Cisco para dispositivos não gerenciados

Etapa 8.8. Na página Cisco Data Security Policies , clique no link de URL Filtering para a nova política.

Etapa 8.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 8.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

	 Imagem - Ação de carregamento para dispositivos não gerenciados Etapa 8.11. Role para baixo na seção URLs sem categoria e escolha a ação apropriada.  Imagem - Ação de Carregamento para URLs Não Categorizados Tip: Para a perspectiva de segurança, é melhor definir a ação como Bloquear, caso qualquer URL precise de acesso, você pode adicioná-los na Categoria de URL personalizada atribuída à política. Etapa 8.12. Clique em Enviar
Etapa 9. Salvando as Alterações	Etapa 9.1. Confirmar as alterações

Informações Relacionadas

- Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - LD (implantação limitada) - Solução de problemas...
- Bloquear download de arquivo executável em SWA
- Bloquear tráfego de upload no dispositivo da Web seguro
- Bloquear o tráfego no Secure Web Appliance
- Ignorar autenticação no Secure Web Appliance
- Configurar Restrição de Locatário do Microsoft O365 em SWA
- Configurar a configuração inicial do Secure Web Appliance
- Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance

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.