Ignorar tráfego no Secure Web Appliance

Contents

Introdução

Este documento descreve as etapas para ignorar o tráfego 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

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.

Diferentes tipos de desvio

No SWA, há três conceitos diferentes de ignorar um tráfego para acessar o SWA, que depende da implantação do Proxy (Implantação Explícita ou Transparente) ou de ser analisado e examinado pelo SWA. Aqui está uma breve visão geral desses três conceitos:

- Ignorar: Uma configuração que impede que o tráfego acesse o SWA, o que reduz a utilização da placa de interface de rede (NIC) e elimina a necessidade de uma sessão entre o usuário e o dispositivo.
- Passagem: Essa configuração impede que o SWA descriptografe o tráfego HTTPS. Apesar disso, o SWA continua a facilitar duas sessões distintas: um entre o cliente e o SWA e um segundo entre o SWA e o servidor Web.
- Permissão: Uma configuração na política de acesso em que o tráfego HTTP ou descriptografado ignora a inspeção por mecanismos SWA internos, como AMP, Sophos, WebRoot e o filtro de aplicativos. Nesse caso, ainda há duas sessões em uso no SWA.

Type	Applies to	Transparent Deployment	Explicit Deployment	Configuration Path	Logging	Number of Sessions	Description
Bypass from SWA	HTTPS & HTTP	✓	✗	GUI > Web Security Manager > Bypass Settings	Bypasslogs	1	SWA routes the traffic to configured gateway (Layer 3 redirection)
Bypass from WCCP Router	HTTPS & HTTP	✓	✗	WCCP Router	No Logs on SWA	0	Traffic Redirects to the Gateway from Router
Bypass from PAC	HTTPS & HTTP	✗	✓	From the PAC file	No Logs on SWA	0	Requests are not sent to the proxy.
Bypass from Browser	HTTPS & HTTP	✗	✓	From the Browser or Group Policy	No Logs on SWA	0	Requests are not sent to the proxy.
Pass Through	HTTPS & HTTP	✓	✓	GUI > Web Security Manager > Decryption Policy	Accesslogs	2	SWA does not decrypt the traffic and sends the same ClientHello to the web server.
Allow	Decrypted Traffic & HTTP	✓	✓	GUI > Web Security Manager > Access Policy	Accesslogs	2	SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ...

Imagem - Gráfico de comparação

Procedimentos de desvio de SWA por tipo de implantação

Os procedimentos para ignorar variam de acordo com o modelo de implantação de proxy. Aqui está uma breve visão geral de cada tipo:

- Implantação Explícita: Os clientes são configurados manualmente para direcionar o tráfego para o proxy.
- Implantação transparente: A infraestrutura de rede redireciona o tráfego para o proxy automaticamente, não exigindo configuração no lado do cliente.

Ignorar Tráfego em Implantação Explícita

Para ignorar o tráfego na implantação explícita, você deve configurar o cliente para não encaminhar a solicitação da Web para os URLs desejados ao SWA. Como mostrado neste diagrama de rede, parte do tráfego vai diretamente para o Firewall ou para o Gateway Padrão para ignorar o SWA (Caminho número 2).

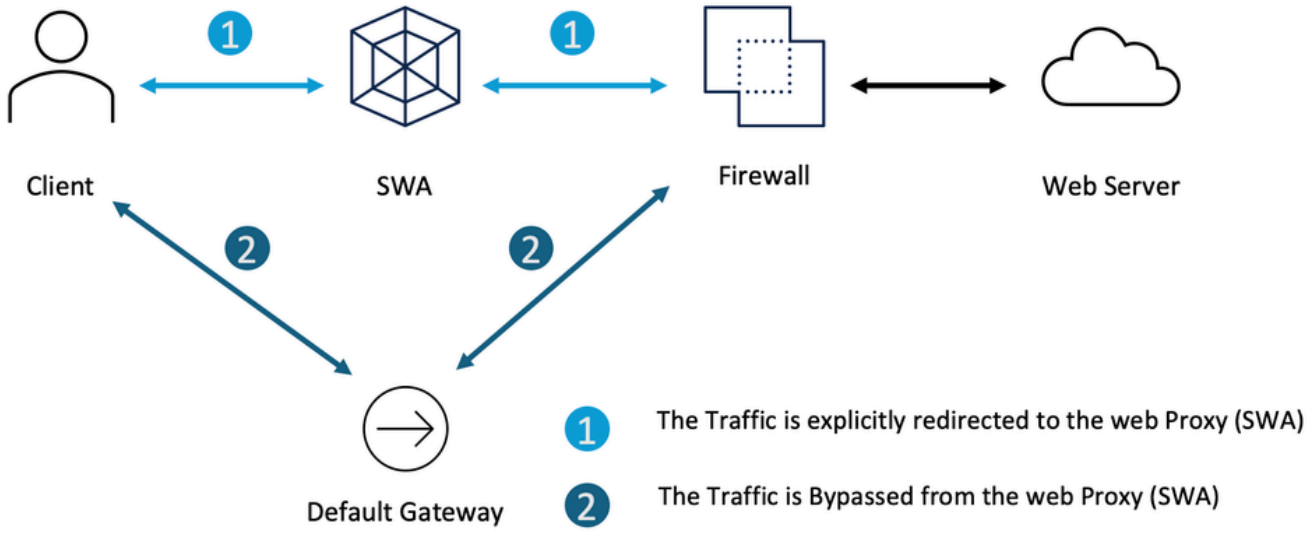


Imagem - Ignorar o Tráfego na Implantação Explícita

Dependendo da sua implantação de proxy explícito, você pode isentar alguns URLs para serem redirecionados para o SWA.

Configuração de proxy explícita	Etapas para impedir que URLs acessem o SWA

Configuração do arquivo PAC	Dependendo de como você configurou seu arquivo PAC, você pode definir a lista de exceções e definir a ação como DIRECT.
	
	Aqui estão alguns exemplos para desviar o endereço IP privado de acessar o SWA
	
	`var resolved_ip = dnsResolve(host);`
	`if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||`
	`isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") ||`
	`isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||`
	`isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`
	`return "DIRECT";`
	
	Este é um exemplo para desviar o tráfego para www.cisco.com do redirecionamento do SWA
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	Este exemplo é para ignorar todos os subdomínios de cisco.com do

	redirecionamento do SWA `if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";` Note: Como o arquivo PAC não é um produto da Cisco, as informações são fornecidas como cortesia para sua conveniência. Para obter mais assistência, entre em contato com o fornecedor do software.
Configuração do navegador (Microsoft Edge, Internet Explorer, Google Chrome)	Etapa 1. No menu Iniciar, digite "Opções da Internet" e pressione Enter Etapa 2. Navegue até a guia Conexões e clique em Configurações da LAN Etapa 3. Clique no botão Avançado Etapa 4. Defina os URLs desejados na seção Exceções.

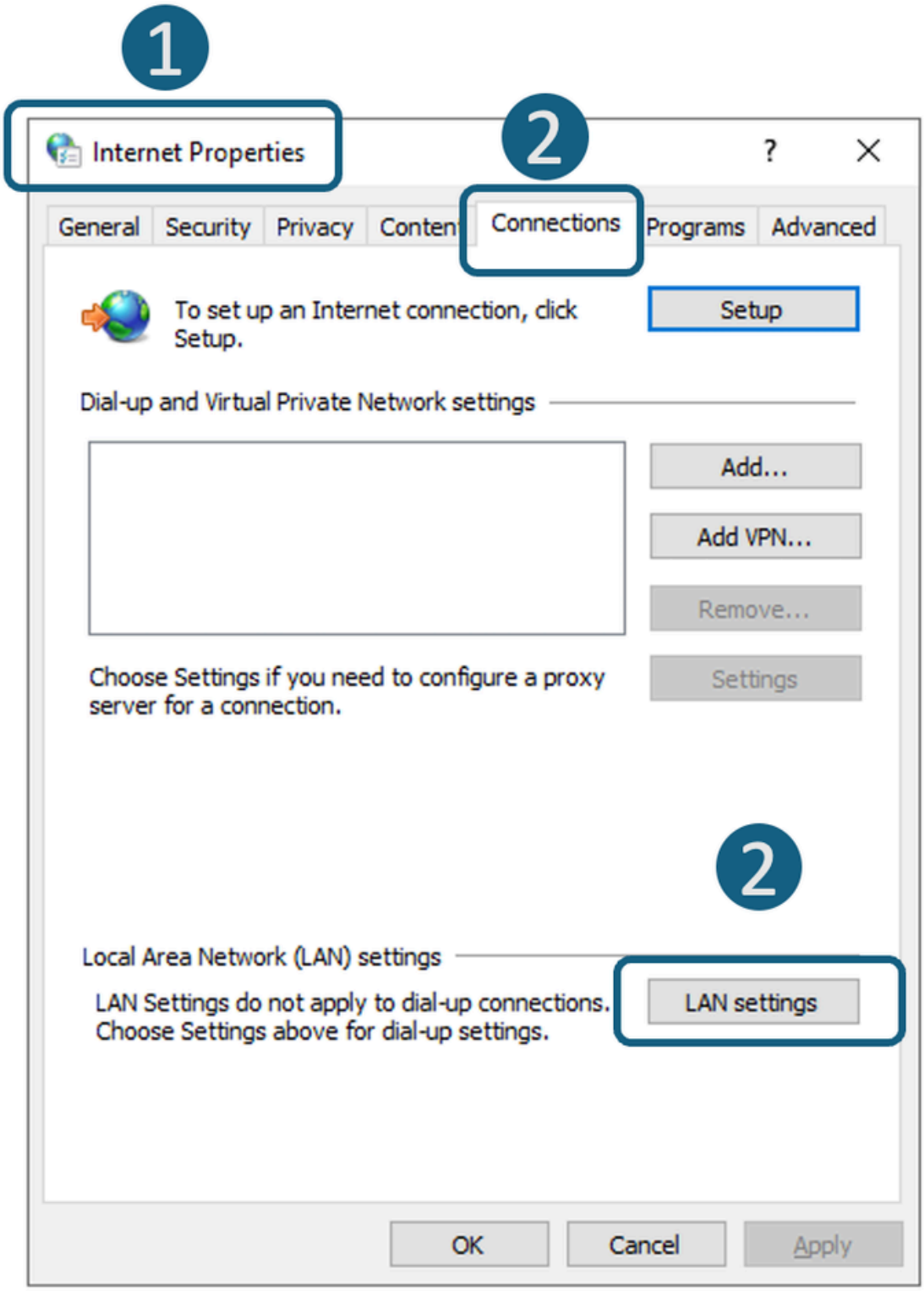


Imagem - Navegue até Configurações de LAN

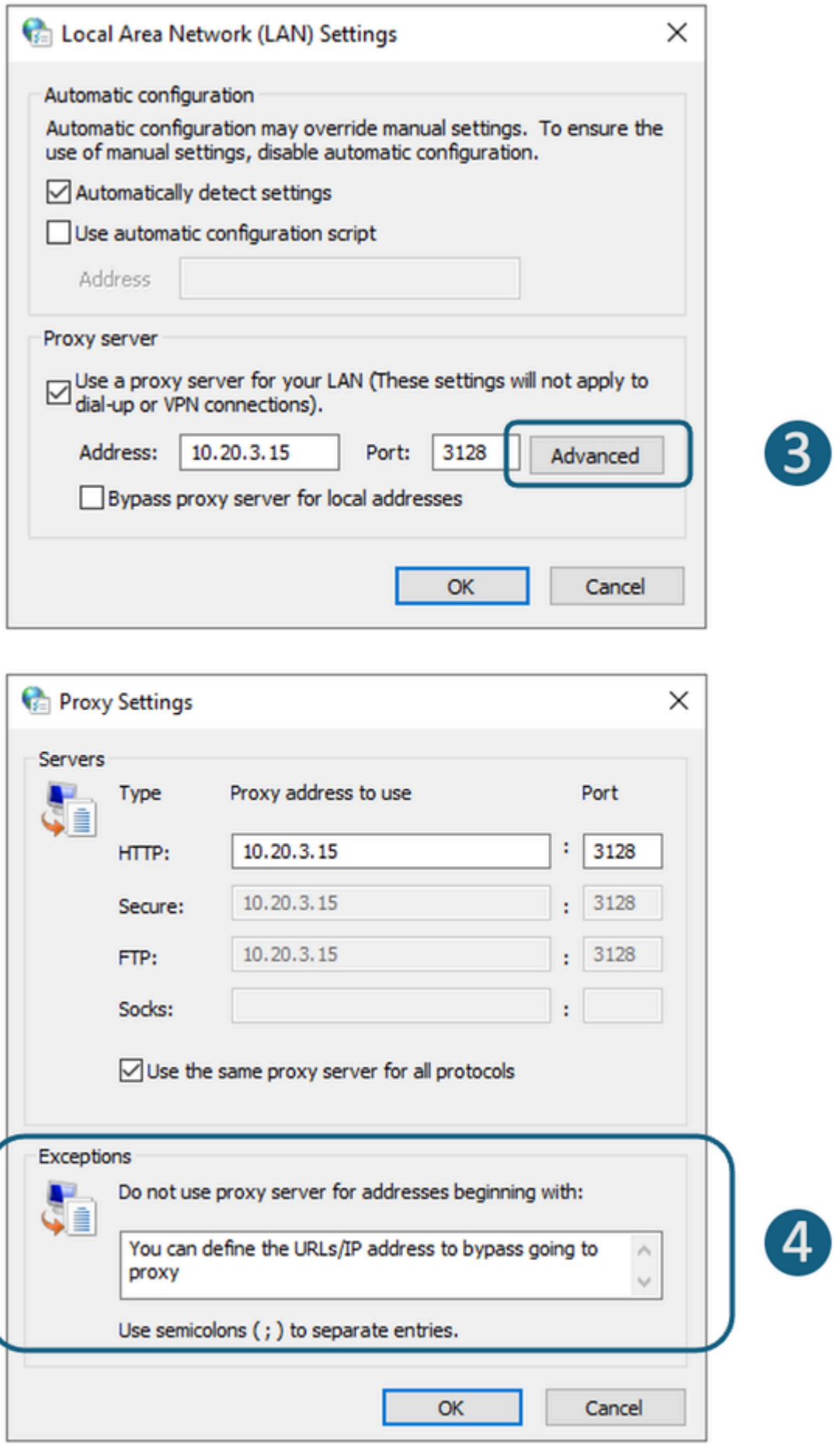
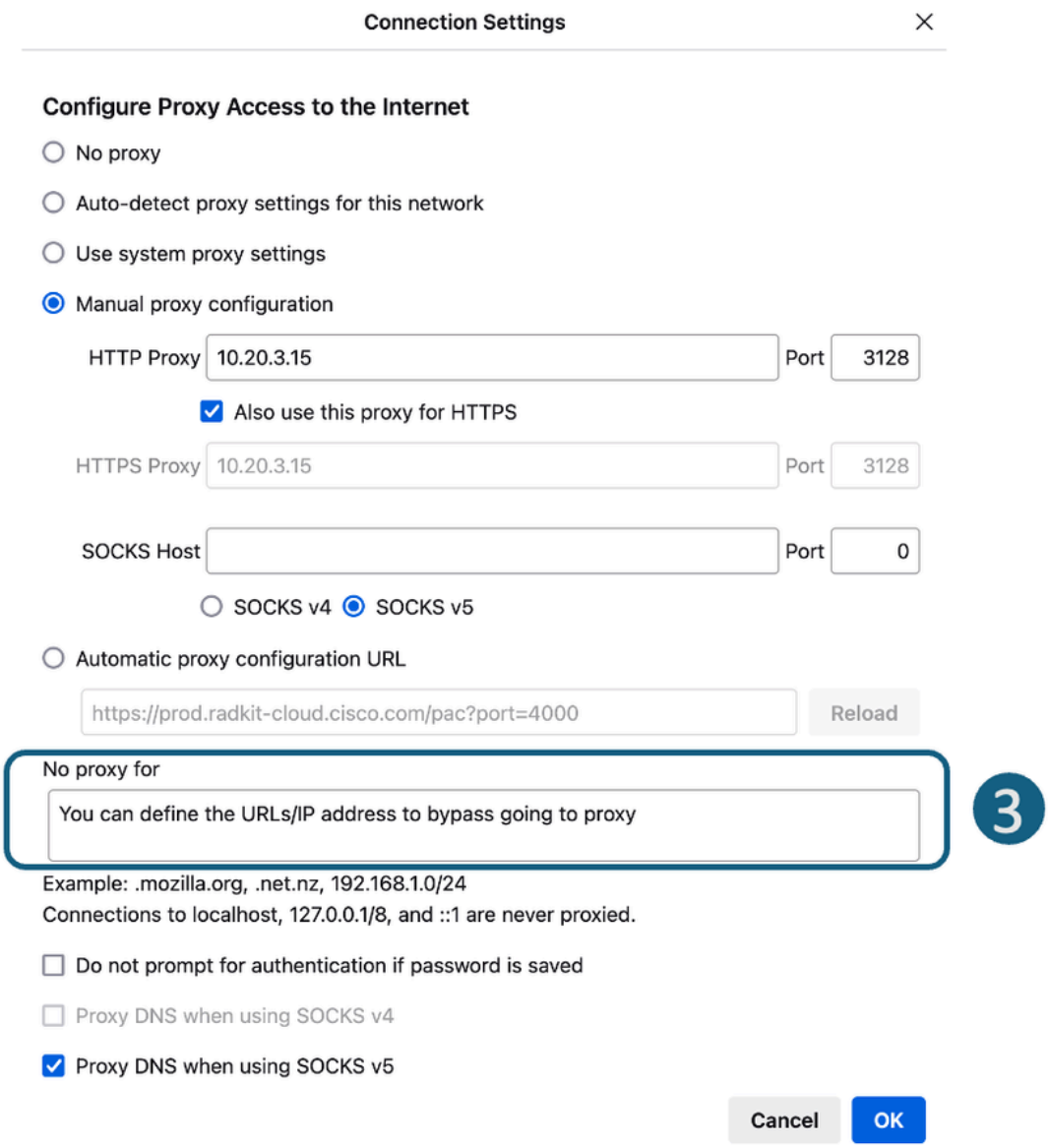
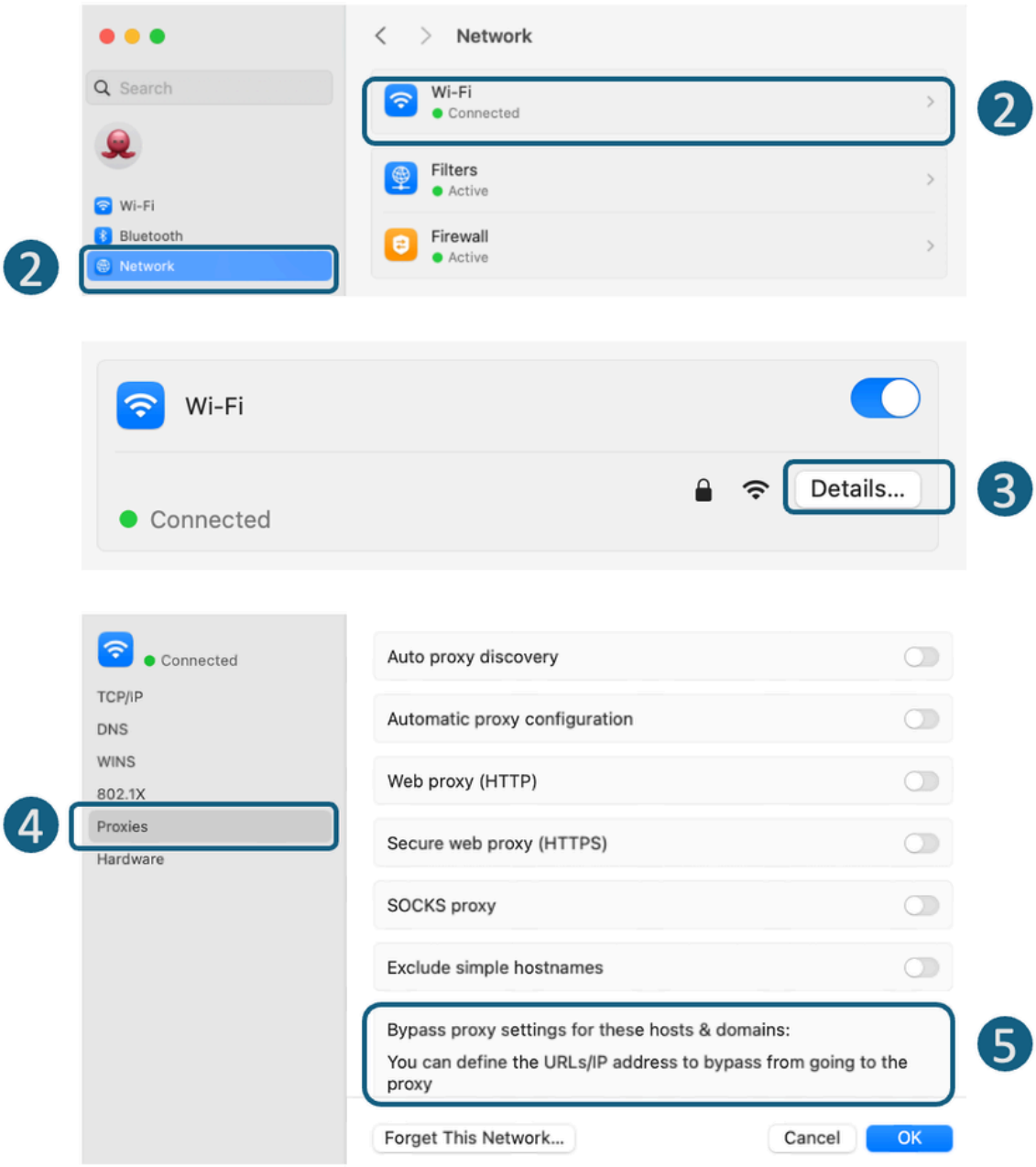


Imagem - Definir as Exceções

Configuração do navegador (Mozilla FireFox)	Etapa 1. No canto superior direito, clique no menu de três barras e selecione Configurações. Etapa 2. Na barra de pesquisa, digite proxy. Etapa 3. Defina os URLs desejados na seção No Proxy for.  Imagem - Definir as exceções no Fire Fox
Configuração do navegador (Apple Safari)	Etapa 1. No canto superior esquerdo, clique no ícone Apple e escolha Configurações do sistema. Etapa 2. No painel esquerdo, navegue até Network e selecione a Network Interface (Interface de rede) que você está usando para acessar a Internet.

	Etapa 3. Clique em Details. Etapa 4. No painel esquerdo, selecione Proxies. Etapa 5. Defina os URLs desejados na seção Bypass Proxy Settings.  Imagem - Definir as exceções no Fire Fox
Configuração da Política de Grupo	Dependendo de como você configurou a Política de Grupo para enviar as configurações de proxy, você pode definir a lista de exceções.

Ignorar o tráfego na implantação transparente

Você pode desviar o tráfego em uma implantação transparente usando as configurações do roteador WCCP ou do desvio SWA. O desvio de SWA atua na Camada 3, roteando o tráfego para o gateway padrão e ignorando totalmente o dispositivo, o que impede o processamento e a criação de sessões separadas.

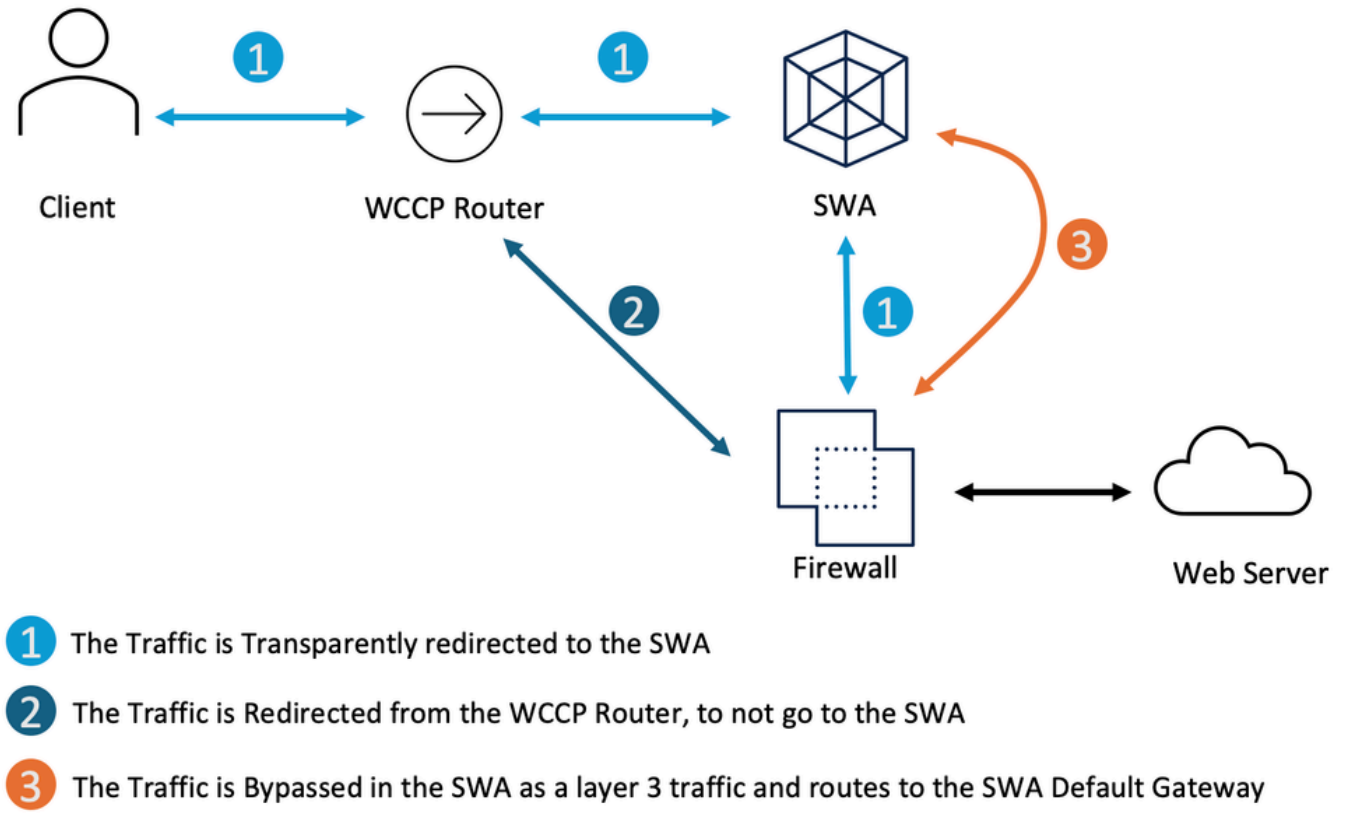
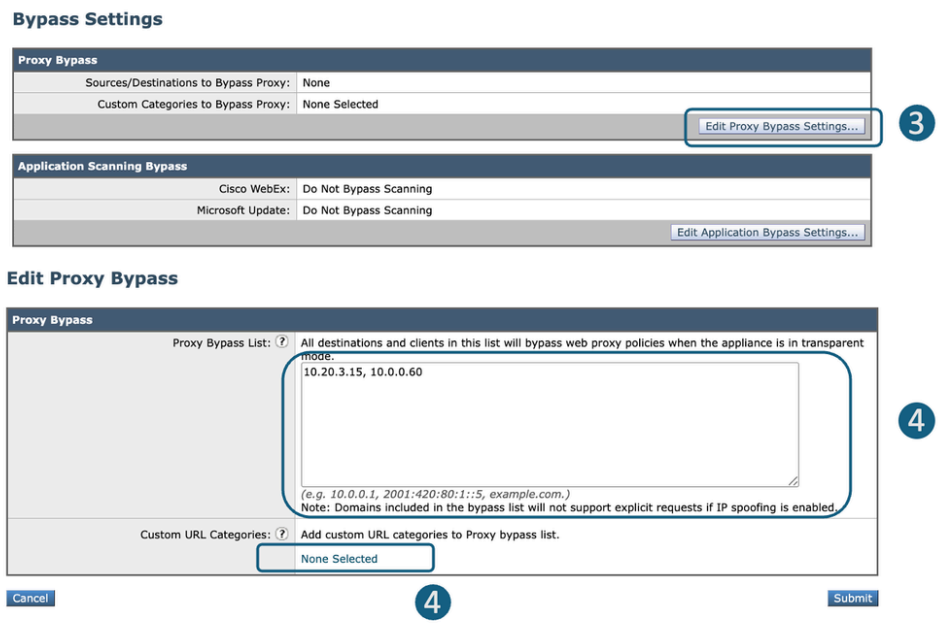


Imagem - Ignorar o tráfego na implantação transparente

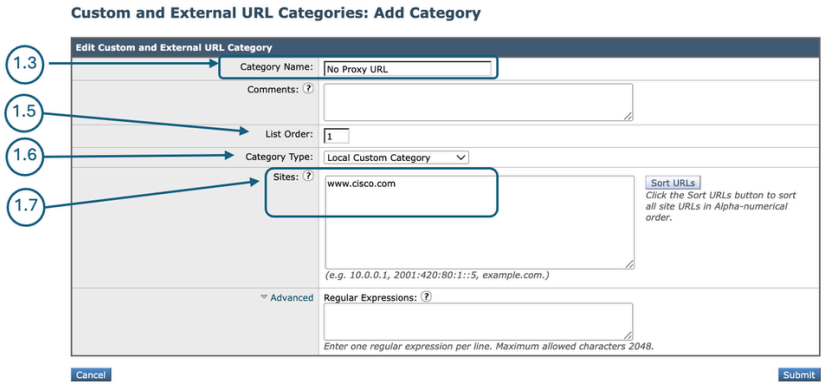
Ignorando a Implantação de Proxy Transparente de tráfego	Etapas para evitar que o tráfego acesse o SWA
Configuração de desvio de SWA	Etapa 1. Em GUI, selecione Web Security Manager. Etapa 2. Selecione Bypass Settings. Etapa 3. Clique em Edit Proxy Bypass Settings. Etapa 4. Você pode inserir o URL, o endereço IP ou adicionar uma Categoria de URL personalizada à lista. Etapa 5. Enviar e confirmar as alterações.

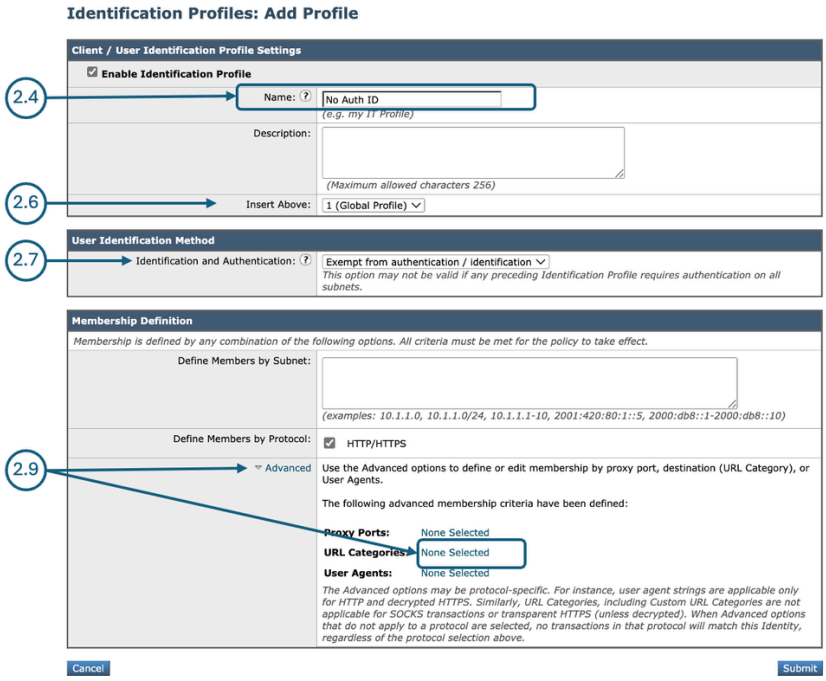
	 Imagem - Definir configurações de desvio Tip: O tráfego que é ignorado com essas configurações não é registrado nos registros de acesso e pode ser exibido nos registros de acesso.
Redirecione o tráfego do roteador WCCP/PBR	Você pode configurar o endereço IP origem ou destino no WCCP ou no Roteador Baseado em Política (PBR) para não redirecionar alguns tráfegos para o SWA.

Configurando a passagem e permitindo o tráfego em SWA

Se o tráfego estiver atingindo o SWA e para reduzir a carga no SWA para devido às preocupações com privacidade, você não deseja que o tráfego para alguns URLs seja inspecionado pelo SWA, use estas etapas.

Etapas	Etapas
Etapa 1. Crie uma Categoria de URL Personalizada para os URLs.	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. Criar um Perfil de identificação para isentar o tráfego da autenticação.	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. Na seção Método de identificação de usuário, escolhaIsentar de autenticação/identificação. 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. Na seção Avançado, escolha Categorias de URL personalizadas.

	 Imagem - Adicionar perfil de identificação Etapa 2.10. Adicione a Categoria de URL personalizada que foi criada na Etapa 1. Etapa 2.11. Clique em Concluído. Etapa 2.12. Enviar.
Etapa 3. Crie uma Política de Descriptografia para passar pelo tráfego.	Etapa 3.1.FromGUI, ChooseWeb Security Manager e clique emDecryption Policy. Etapa 3.2. Clique em Adicionar política para adicionar uma política de descriptografia. Etapa 3.3.Use a caixa de seleçãoEnable Policy para habilitar essa diretiva. Etapa 3.4.Atribua um PolicyName exclusivo. Etapa 3.5. (Opcional) Adicione Descrição. Etapa 3.6.Na lista suspensa Inserir política acima, escolha a primeira política. Etapa 3.7.Em Perfis de identificação e Usuários, escolha o Perfil de identificação que você criou na Etapa 2. Etapa 3.8. Enviar.

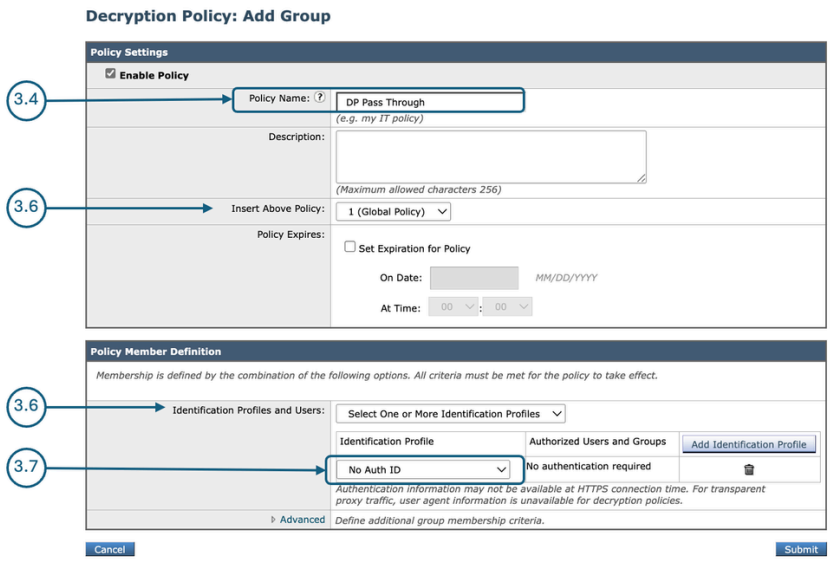


Imagem - Criar uma política de descriptografia

Etapa 3.9.Na página Descriptografia Políticas, emFiltragem de URL, clique no link associado a essa nova Política de Descriptografia.

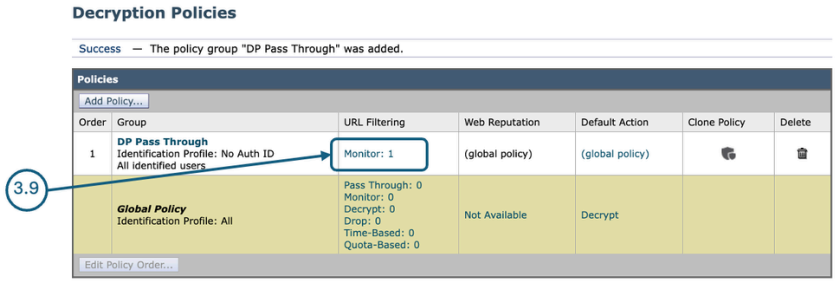


Imagem - Selecionar filtragem de URL

Etapa 3.10.SelectPass Através da ação para a Categoria de URL criada na Etapa 1.

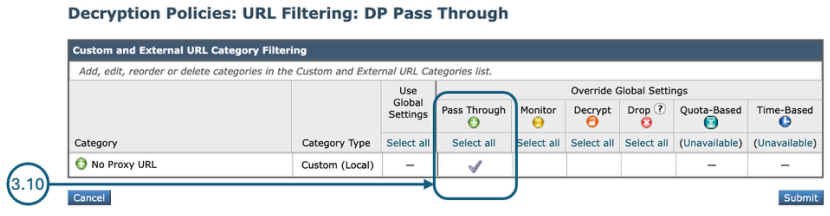


Imagem - Definir a ação para passar

Etapa 3.11. Enviar.

Etapa 4. Criar uma Política de Acesso para permitir o tráfego de Atualizações da Microsoft.

Etapa 4.1.FromGUI, ChooseWeb Security Manager e clique em Access Policy.

Etapa 4.2. Clique em Adicionar política para adicionar uma política de acesso.

Etapa 4.3.Use a caixa de seleçãoEnable Policy para habilitar essa diretiva.
Etapa 4.4.Atribua um PolicyName exclusivo.
Etapa 4.5. (Opcional) Adicione Descrição.
Etapa 4.6.Na lista suspensa Inserir política acima, escolha a primeira política.

Etapa 4.7.Em Perfis de identificação e Usuários, escolha o Perfil de identificação criado na Etapa 2.

Etapa 4.8. Enviar.

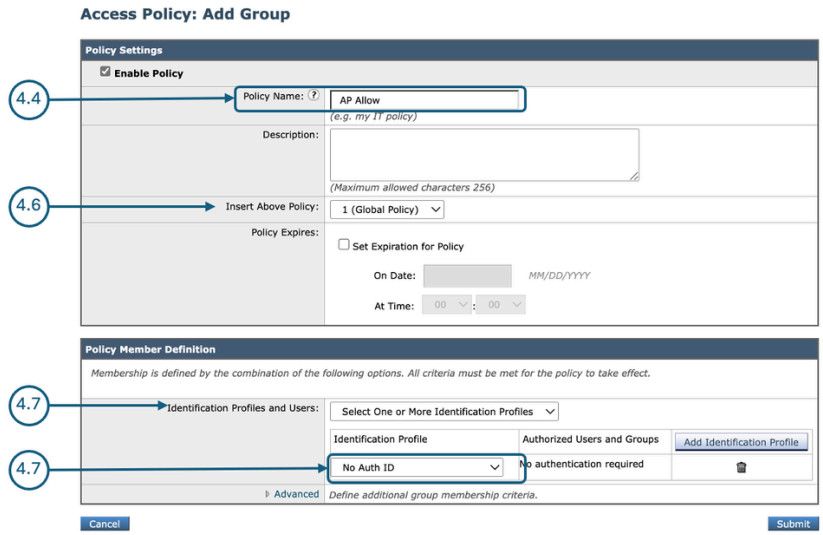


Imagem - Criar política de acesso

Etapa 4.9. Na página Access Policies, em URL Filtering, clique no link associado a esta nova Access Policy.

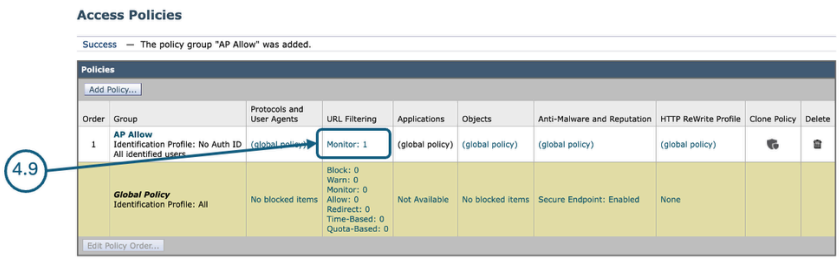
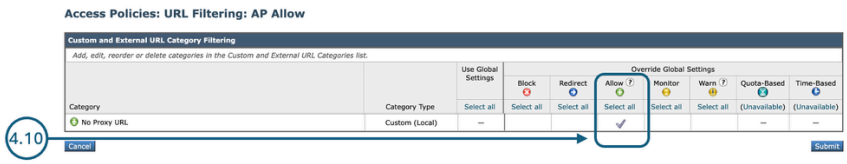


Imagem - Selecionar filtragem de URL

Etapa 4.10.Selecione Allowas the action for the Custom URL category created for the URL Category created on Step 1 (Permitir a ação para a categoria de URL personalizada criada para a categoria de URL criada na Etapa 1).

	 Imagem - Definir a ação como permitir Etapa 4.11. Enviar. Etapa 4.12. Confirmar alterações.

Informações Relacionadas

- Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance
- Autenticação de desvio no Secure Web Appliance - Cisco
- 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
- 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

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.