Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance

Contents

[Introdução](#)

[Pré-requisitos](#)

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

[Atualizações da Microsoft](#)

[Ignorar Atualizações da Microsoft](#)

- [Ignorando o tráfego no SWA](#)

[Etapas para Passagem de Atualizações da Microsoft](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para ignorar o tráfego de atualizações da Microsoft 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.

Atualizações da Microsoft

As atualizações da Microsoft são patches essenciais, atualizações de segurança e aprimoramentos de recursos lançados pela Microsoft para seus sistemas operacionais e aplicativos de software. Essas atualizações são cruciais para manter a segurança, a estabilidade e o desempenho de computadores e dispositivos de rede. Eles garantem que os sistemas estejam protegidos contra vulnerabilidades, que bugs sejam corrigidos e que novos recursos ou melhorias sejam integrados ao software.

O impacto das atualizações da Microsoft em servidores proxy, como o Cisco SWA, pode ser significativo. Essas atualizações geralmente envolvem o download de arquivos grandes ou de vários arquivos menores, que podem consumir uma largura de banda considerável e recursos de processamento no proxy. Isso pode levar a congestionamento, desempenho de rede mais lento e maior carga na infraestrutura de proxy, afetando potencialmente a experiência geral do usuário e outras operações de rede críticas.

Ignorar o tráfego do Microsoft Update do proxy pode ser uma maneira segura e eficaz de gerenciar esses desafios. Como as Atualizações da Microsoft são fornecidas de servidores confiáveis da Microsoft, permitir que esse tráfego ignore o proxy pode ajudar a reduzir a carga no servidor proxy sem comprometer a segurança da rede. Isso garante que as atualizações essenciais sejam fornecidas de forma eficiente, preservando recursos de proxy para outras tarefas de segurança e filtragem de conteúdo. É importante, no entanto, implementar essas configurações de desvio com cuidado para manter a segurança geral da rede e a conformidade com as políticas organizacionais.

Ignorar Atualizações da Microsoft

Se você estiver considerando evitar usar proxy no tráfego de atualizações da Microsoft, há duas abordagens principais

1. Bypass: Isso envolve a configuração da rede para redirecionar o tráfego para que ele nunca chegue ao SWA.
2. Passagem: Isso envolve a configuração do SWA para não descriptografar nem verificar o tráfego das atualizações da Microsoft, permitindo que ele passe pelo proxy sem inspeção.

Ignorando o tráfego no SWA

Para ignorar o tráfego de Atualizações da Microsoft em redes equipadas com SWA, a abordagem varia de acordo com a configuração de implantação de proxy:

Tipo de implantação	Ignorando o tráfego
Implantação transparente	Você pode redirecionar o tráfego de Atualizações da

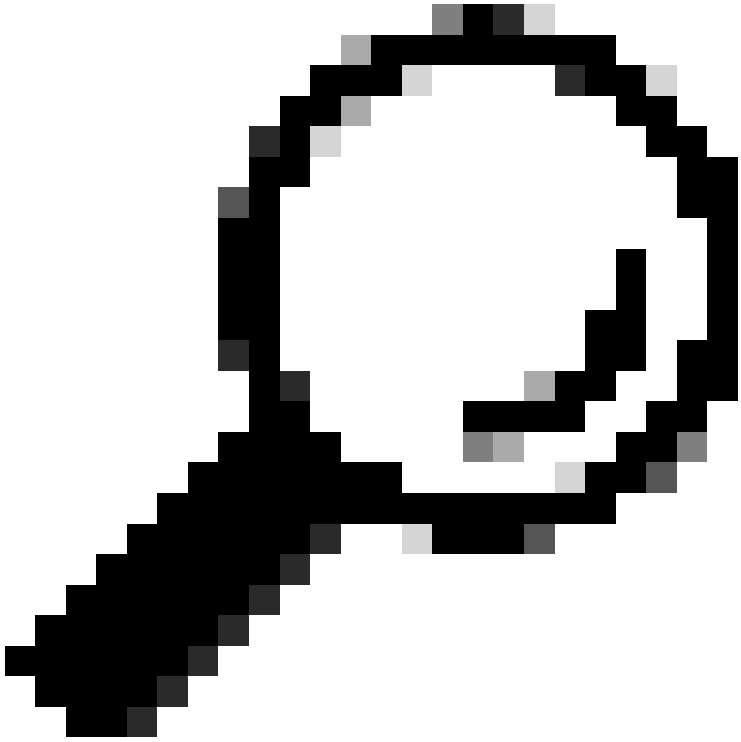
	Microsoft no roteador ou nos switches de Camada 4 que são responsáveis por encaminhar o tráfego para o servidor proxy.
	Você pode definir as configurações de desvio diretamente na interface gráfica do usuário (GUI) do SWA.
Implantação Explícita	Para evitar que o tráfego das atualizações da Microsoft acesse o SWA, você deve configurar o desvio na origem. Isso significa isentar os URLs relevantes nas máquinas clientes para garantir que o tráfego não seja redirecionado para o SWA.

Se ignorar um tráfego específico exigir um novo projeto de rede extenso e não for viável, uma abordagem alternativa será configurar o SWA para passar por determinados tipos de tráfego. Isso pode ser obtido configurando o SWA para não descriptografar nem examinar o tráfego designado, permitindo que ele passe pelo proxy sem inspeção. Esse método garante que o tráfego essencial seja entregue de forma eficiente, minimizando o impacto no desempenho da rede e nos recursos de proxy.

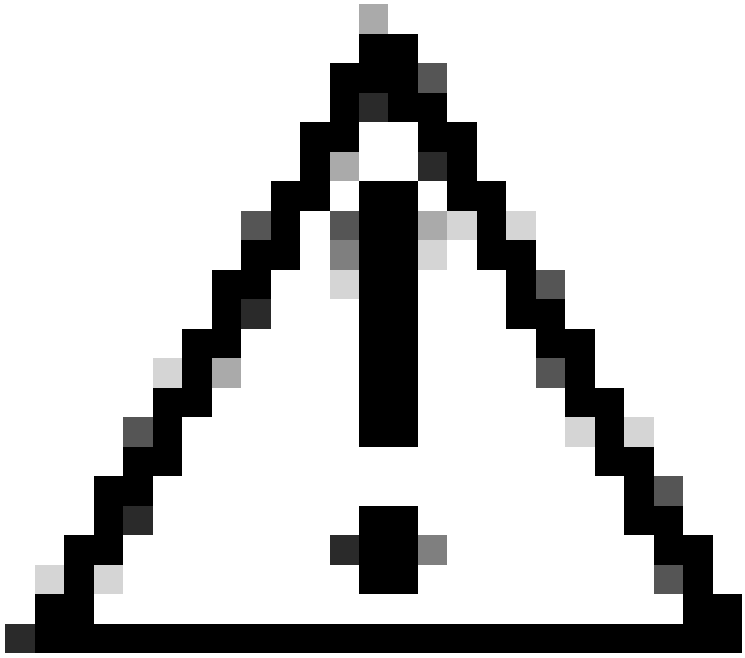
Etapas para Passagem de Atualizações da Microsoft

Há quatro estágios principais para o tráfego de Passagem de Atualizações da Microsoft:

Estágio	Etapas
1. Criar uma Categoria de URL Personalizada para URLs de Atualizações da Microsoft	Etapa 1.FromGUI, ChooseWeb Security Manager e clique em Categorias de URL Personalizadas e Externas. Etapa 2.Clique em Adicionar categoria para adicionar uma categoria de URL personalizada. Etapa 4.Atribua um CategoryName exclusivo. Etapa 5. (Opcional) Adicione Descrição. Etapa 6. Em Ordem da Lista, escolha a primeira categoria para posicionar na parte superior. Passo 7. Na lista suspensa Categoria Tipo, escolha Categoria personalizada local. Etapa 8. Adicione URLs de Atualizações da Microsoft na seção Sites.



Dica: você pode verificar a lista de atualizações da Microsoft neste link: Etapa 2 - Configurar o WSUS | Aprender da Microsoft



Cuidado: Não copie/cole os URLs como estão nos documentos da Microsoft; formate-os corretamente como formato SWA. Para obter mais informações, visite: Configurar categorias de URL personalizadas

	no Secure Web Appliance - Cisco Etapa 9. Enviar.
2. Criar um Perfil de Identificação para isentar o tráfego de Atualizações da Microsoft da Autenticação	Etapa 10.FromGUI, ChooseWeb Security Manager e clique em Identification Profiles. Etapa 11.Clique em Add Profile (Adicionar perfil) para adicionar um perfil. Etapa 12.Use a caixa de seleçãoAtivar Perfil de Identificação para ativar esse perfil ou para desativá-lo rapidamente sem excluí-lo. Etapa 13.Atribua um profileName exclusivo. Etapa 14. (Opcional) Adicione Descrição. Etapa 15.Na lista suspensa InserirAcima, escolha onde esse perfil deve aparecer na tabela. Etapa 16. Na seção Método de identificação do usuário, escolha Isento de autenticação/identificação. Etapa 17.No campo Definir membros por sub-rede, se você quiser transmitir o tráfego da Microsoft para alguns usuários específicos, insira os endereços IP ou sub-redes aplicáveis ou deixe este campo em branco para incluir todos os endereços IP. Etapa 18. Na seção Avançado, escolha Categorias de URL personalizadas. Etapa 19. Adicione a categoria de URL personalizada que foi criada para atualizações da Microsoft. Etapa 20. Clique em Concluído. Etapa 21. Enviar.
3. Crie uma Política de Descriptografia para Passar o Tráfego de Atualizações da Microsoft	Etapa 22.FromGUI, ChooseWeb Security Manager e clique emDecryption Policy. Etapa 23. Clique em Adicionar política para adicionar uma política de descriptografia. Etapa 24.Use a caixa de seleçãoEnable Policy para habilitar essa política. Etapa 25.Atribuir um PolicyName exclusivo.

	Etapa 26. (Opcional) Adicione Descrição. Etapa 27.Na lista suspensa Inserir política acima, escolha a primeira política. Etapa 28.Em Perfis de identificação e Usuários, escolha o Perfil de identificação que você criou nas etapas anteriores. Etapa 29. Enviar. Etapa 30.Na página Descriptografia Políticas, emFiltragem de URL, clique no link associado a esta nova Política de Descriptografia. Etapa 32.Selecione Passthrough como a ação para a categoria de URL de Atualizações da Microsoft. Etapa 32. Enviar.
4. Criar uma Política de Acesso para Permitir Tráfego de Atualizações da Microsoft	Etapa 33.FromGUI, ChooseWeb Security Manager e clique em Access Policy. Etapa 34. Clique em Adicionar política para adicionar uma política de acesso. Etapa 35.Use a caixa de seleçãoEnable Policy para habilitar essa diretiva. Etapa 36.Atribuir um PolicyName exclusivo. Etapa 37. (Opcional) Adicione Descrição. Etapa 38.Na lista suspensa Inserir política acima, escolha a primeira política. Etapa 39.Em Perfis de identificação e Usuários, escolha o Perfil de identificação que você criou nas etapas anteriores. Etapa 40. Enviar. Etapa 9. Na página Access Policies, em URL Filtering, clique no link associado a esta nova Access Policy Etapa 10.Selecione Allowas the action for the Custom URL category created for the Microsoft Updates (Permitiu a ação para a categoria de URL personalizada criada para as atualizações da Microsoft). Etapa 11. Enviar. Etapa 12. 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
- Use as práticas recomendadas de dispositivos da Web seguros - Cisco
- 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.