

HTTP 429 Limite de taxa e erros de conexão ao acessar aplicativos por meio do SWG de acesso seguro

Contents

Problema

Os usuários encontram erros de limite de taxa HTTP 429 ao tentar acessar o aplicativo, por exemplo, <https://xxx.com> através do Cisco Secure Access SWG (Secure Web Gateway). O problema afeta os notebooks gerenciados pela empresa e começou aproximadamente duas semanas antes da abertura do caso. Os usuários experimentam esses erros durante as tentativas de login ou ao acessar certas funções do aplicativo após a autenticação bem-sucedida.

Além disso, quando o domínio é adicionado à lista de desvio de Acesso Seguro, os usuários encontram erros de servidor HTTP 500 durante a entrada OTP (One-Time Password - Senha ocasional) ou erros gerais de conexão quando o tráfego não sai mais pelos intervalos de IP do SWG (151.186.x.x).

O proprietário do aplicativo confirmou que nenhum limite de taxa foi alterado recentemente no lado do servidor, e o problema parece estar relacionado ao tráfego originário dos endereços IP de saída do Cisco Secure Access SWG.

Ambiente

- Cisco Secure Access (antigo Cisco Umbrella) com SWG habilitado
- Notebooks gerenciados pela empresa com o cliente Cisco SSE (Security Service Edge)
- Intervalos de IP de saída SWG: 151.186.x.x
- Data centers: AWS Cingapura (Ásia-Pacífico 1) e AWS EUA Oeste (Oregon)
- Aplicativo: <https://sbstransit.aereacomercial.com>

Resolução

A resolução envolve a implementação de uma configuração de desvio e a coordenação com o proprietário do aplicativo para permitir a listagem de endereços IP específicos.

Siga as próximas etapas.

Passo 1: Verificar o comportamento atual do SWG

Verifique a política atual e as informações de IP de saída acessando esta URL a partir de um dispositivo afetado:

`https://policy.test.sse.cisco.com/?host=https://sbstransit.aereacommercial.com`

Isso mostra o IP de saída SWG atual sendo usado (geralmente o intervalo 151.186.x.x) e confirma que o tráfego está sendo processado pelo SWG de acesso seguro.

Passo 2: Adicionar domínio à lista de desvio de acesso seguro

Navegue para Internet Settings > Bypass Secure Access no painel Cisco Secure Access e adicione o domínio problemático para ignorar a inspeção de DNS e SWG:

`sbstransit.aereacommercial.com`

Passo 3: Testar o acesso a partir de uma rede não corporativa

Teste o acesso de aplicativos de uma rede onde o tráfego não sai via Secure Access SWG (intervalos 151.186.x.x). Isso pode ser feito a partir de um dispositivo pessoal ou desativando temporariamente o cliente SSE.

Identifique o endereço IP público do ISP visitando:

<https://whatismyip.com>

Passo 4: Coordenar a listagem de permissão de IP com o proprietário do aplicativo

Forneça o endereço IP público do ISP identificado ao proprietário do aplicativo e solicite que esse IP seja permitido listado no lado do aplicativo. Isso ajuda a verificar se o aplicativo está implementando restrições baseadas em IP que afetam os IPs de saída do SWG de acesso seguro.

Passo 5: Verificar resolução

Depois que o proprietário do aplicativo implementar a lista de permissão de IP, teste o comportamento de acesso para confirmar se os usuários podem acessar o aplicativo com êxito sem encontrar HTTP 429 ou erros de conexão.

Causa

O aplicativo parece implementar limitação de taxa ou restrições de acesso com base nos endereços IP de origem. Quando vários usuários acessam o aplicativo por meio do Cisco Secure Access SWG, todo o tráfego parece se originar de intervalos IP de saída SWG compartilhados (151.186.x.x). Isso faz com que o mecanismo de limitação de taxa do aplicativo seja acionado, pois ele percebe solicitações excessivas provenientes de um único endereço IP ou intervalo de IP.

O problema é agravado pelo fato de que os dispositivos gerenciados pela empresa continuam a rotear o tráfego através do cliente SSE, mesmo quando conectados a redes pessoais, mantendo o mesmo comportamento de IP de saída que aciona as restrições do aplicativo.

Conteúdo relacionado

- [Suporte técnico e downloads da 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.