

A proteção da Web do ChromeOS SWG não está funcionando e, consecutivamente, nenhum registro da Web é exibido na pesquisa de atividades

Contents

Problema

Os logs da Web não estavam sendo gerados para usuários do ChromeOS, apesar da proteção do Secure Web Gateway (SWG) parecer estar ativada para a organização. Os endpoints do ChromeOS afetados estavam mostrando apenas proteção no nível de DNS sem atividade de registro SWG/Web visível na interface de pesquisa de atividade. Os usuários estavam observando uma ausência completa de logs de tráfego da Web enquanto o status de proteção do SWG indicava que ele estava habilitado.

Durante a investigação, os logs de diagnóstico revelaram repetidas falhas de sincronização no ponto de extremidade <http://407.checkumbrella.com> com respostas de erro HTTP 407 (autenticação de proxy necessária). O cliente/extensão do ChromeOS não conseguiu se autenticar corretamente com o serviço de proxy, impedindo a ativação da proteção SWG adequada e a geração subsequente do registro da Web.

Ambiente

- Acesso seguro da Cisco
- Endpoints ChromeOS com cliente/extensão Cisco Secure Access
- Console do Google Admin para gerenciamento do ChromeOS

Resolução

O problema foi resolvido com a habilitação do esquema de autenticação Autenticação básica para a Unidade Organizacional (UO) de Administração do Google que contém os usuários do ChromeOS afetados e a execução de uma recarga de política para ativar a proteção SWG.

Passo 1: Coleta e análise de logs

Captura HAR coletada (revise os logs de rede e de console) para identificar a causa raiz da falha de sincronização. Os logs mostraram falhas repetidas de autenticação ao tentar sincronizar com o serviço Cisco Secure Access.

Passo 2: Habilitar Autenticação Básica para a OU de Administração do Google

No console de administração do Google, navegue até a Unidade organizacional que contém os usuários do ChromeOS afetados e ative o esquema de autenticação Autenticação básica. Isso permite que o cliente/extensão do ChromeOS autentique corretamente com o serviço de proxy do Cisco Secure Access.

Passo 3: Recarga e verificação de políticas

Depois de habilitar a Autenticação Básica, execute uma reinicialização de política nos dispositivos ChromeOS afetados. Verifique se a proteção SWG se torna ativa verificando o status da proteção. A proteção SWG agora deve ser mostrada como ativa em vez de apenas proteção no nível DNS.

Passo 4: Validação

Teste a atividade de navegação na Web dos usuários do ChromeOS afetados e confirme se os logs da Web estão sendo gerados e visíveis na interface de pesquisa de atividades. Os registros devem mostrar a inspeção de tráfego da Web adequada e o registro através do serviço SWG.

Causa

O cliente/extensão do ChromeOS tinha o esquema de autenticação Autenticação básica desabilitado para a Unidade Organizacional do Google Admin que contém os usuários afetados. Sem a Autenticação Básica habilitada, os dispositivos do ChromeOS não poderiam ser autenticados corretamente com o serviço de proxy do Cisco Secure Access, resultando em erros HTTP 407 (autenticação de proxy necessária) durante tentativas de sincronização. Isso impediu que a proteção SWG fosse ativada corretamente, fazendo com que os dispositivos voltassem para a proteção somente DNS e impedindo a geração de logs da Web.

Conteúdo relacionado

- [Solucionar problemas e coletar informações básicas do Cisco Secure Access](#)
- [Cisco Secure Access Chromebook Client](#)
- [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.