

Limitações da política DLP com WhatsApp em acesso seguro

Contents

Problema

As políticas DLP no Cisco Secure Access não estão detectando ou bloqueando arquivos confidenciais quando compartilhados via WhatsApp (aplicativo de navegador ou desktop), apesar dacriptografia HTTPS estar habilitada. O mecanismo DLP não consegue disparar ou detectar carregamentos de arquivos por meio dessas plataformas, enquanto as mesmas políticas DLP bloqueiam com êxito arquivos idênticos quando carregados por meio de outras ferramentas de carregamento online. Ao testar o bloqueio de upload básico para o WhatsApp, a funcionalidade funciona corretamente nas versões do navegador e do desktop, mas o problema é especificamente isolado para a aplicação da política DLP.

Ambiente

- Acesso seguro da Cisco
- Políticas DLP configuradas
- Descriptografia HTTPS habilitada
- Aplicativos de WhatsApp Web e WhatsApp Desktop

Resolução

O comportamento observado é uma limitação esperada do WhatsApp e de plataformas semelhantes devido à implementação de criptografia de ponta a ponta (E2EE) e ao tratamento de tráfego fora do padrão. As etapas de solução de problemas descritas nas próximas seções e solução alternativa podem ser implementadas.

Troubleshooting de Etapas de Verificação

Antes de implementar a solução alternativa, verifique estes itens de configuração:

- Verifique se a ID de identidade/origem do SWG correta está configurada.
- Confirme se a inspeção/descriptografia HTTPS está habilitada e não foi ignorada seletivamente para as plataformas de destino.
- Verifique se as configurações de Isolamento/RBI e Allow-Override estão definidas corretamente.
- Confirme a associação a grupos do AD se as políticas DLP forem baseadas em grupos.
- Verifique as listas de desvio de direção de tráfego para obter exclusões.
- Verifique se o protocolo QUIC está desabilitado nos navegadores.
- Verifique os efeitos do tráfego IPv6 que podem ignorar a inspeção.

Solução recomendada

Para habilitar a imposição de DLP para o tráfego da Web do WhatsApp, implemente o Remote Browser Isolation (RBI) para o tráfego destinado à Web do WhatsApp. Essa solução alternativa permite que as políticas DLP sejam aplicadas isolando a sessão do navegador e permitindo a inspeção de conteúdo no ambiente isolado.

Configure a aplicação de RBI especificamente para domínios da Web do WhatsApp para garantir que os carregamentos de arquivos e o compartilhamento de conteúdo através da interface da Web estejam sujeitos à avaliação de política de DLP.

Informações adicionais

Uma solicitação de melhoria de produto foi documentada para essa limitação - CSE-I-1249.

Causa

O WhatsApp (incluindo o WhatsApp Web) e plataformas de colaboração similares implementam criptografia de ponta a ponta (E2EE) que impede a inspeção completa de conteúdo e a varredura de texto de mensagens e uploads de arquivos. Além disso, o tráfego do WhatsApp não utiliza portas HTTP/HTTPS padrão da mesma maneira que os carregamentos da Web típicos, o que significa que o Secure Web Gateway (SWG) não pode interceptar e inspecionar o tráfego através do caminho de inspeção HTTPS normal. Esse método de criptografia e tratamento de tráfego é projetado e representa uma limitação esperada dos recursos atuais de inspeção de DLP para essas plataformas específicas.

Conteúdo relacionado

- [Solicitação de aprimoramento de produto CSE-I-1249](#)
- [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.