Solucionar problemas de DLP em tempo real com o Cisco Secure Access

Contents

Introdução

Este documento descreve as etapas de Troubleshooting para problemas de Prevenção de Perda de Dados (DLP - Data Loss Prevention) em Linha ou em Tempo Real dentro do ambiente Secure Web Gateway (SWG - Secure Web Gateway).

Pré-requisitos e Avisos

- Inspeção HTTPS: Verifique se a inspeção HTTPS está habilitada. O DLP não pode verificar o tráfego criptografado. Verifique se o site está sendo descriptografado com a CA raiz de acesso seguro da Cisco ou a CA personalizada.
- Protocolo QUIC: Desabilite o protocolo QUIC em todos os navegadores. O QUIC usa UDP, que ignora o SWG e impede a verificação DLP.
- IPv6: Desabilite o IPv6 se o tráfego não estiver atingindo o SWG, pois a funcionalidade de pilha dupla deve causar desvios.
- Política de segurança: Certifique-se de que a regra de acesso não tenha "Permitir - Substituir Segurança" ou "Isolamento" ativado.

Overview

O DLP em linha é um recurso de varredura estendida do SWG. Ele monitora ou bloqueia o upload de dados confidenciais, confidenciais ou de identificação pessoal em arquivos carregados através do proxy SWG. Os clientes criam Classificações de Dados usando identificadores definidos pela Cisco (por exemplo, cartões de crédito ou números de previdência social) ou palavras-chave personalizadas. Essas classificações são aplicadas às Políticas DLP atribuídas a identidades e destinos específicos. O mecanismo DLP examina somente os métodos HTTP POST, PUT e PATCH.

Lista de verificação de Troubleshooting Geral

Se a detecção de DLP não estiver ocorrendo, verifique as etapas descritas:

- Conectividade: Confirme se o cliente está usando o SWG acessando http://policy.test.sse.cisco.com. Verifique se o data center SWG correto foi aplicado e se o resultado do teste mostra "protegido pelo acesso seguro".
- Descriptografia: Certifique-se de que a Descriptografia SSL esteja habilitada no Perfil de Segurança. Verifique se não há nenhuma decodificação seletiva ou exclusões da lista "Não descriptografar".
- Direção de tráfego: Verifique se não há desvio de domínio externo configurado nas configurações da Internet.
- Identidade: Se as políticas DLP dependem de grupos do Ative Diretory, confirme se o usuário é membro do grupo correto.
- Configurações do aplicativo: Verifique se as configurações de Ignorar ou Compatibilidade do Office 365 estão desabilitadas se um domínio da Microsoft estiver sendo usado para DLP.
- Pesquisa de atividade: Use Relatórios > Pesquisa de atividade para garantir que o URL completo esteja visível (descriptografado) e que a identidade esperada esteja associada ao tráfego. Marque Relatórios > Prevenção de Perda de Dados para confirmar se a atividade de monitoramento ou bloqueio é registrada.
- Configuração da política: Verifique se a política DLP está configurada para o aplicativo de identidade e destino correto.
- Testando: Use um destino em boas condições (por exemplo, pastebin.com ou dlptest.com) e uma string de teste de amostra em boas condições da documentação da Cisco.
- Dados de suporte: Reúna um arquivo HAR do usuário para verificar se o tráfego é roteado pelo SWG e verifique os cabeçalhos SWG.

Solucionar Falsos Negativos

Se o DLP estiver ativo, mas um classificador específico não for acionado, investigue as seguintes áreas:

Classificadores, arquivos e strings

- Status do arquivo: Verifique se o arquivo não está criptografado ou não é verificável. Teste com um arquivo de texto simples.
- Limiares: Verifique as configurações de Limite e Proximidade em Política > Classificação de dados. O classificador pode exigir um número maior de ocorrências ou proximidade de uma cadeia de caracteres personalizada.
- Padrões Regex: Use uma ferramenta online (por exemplo, regexr.com) para visualizar padrões. Simplifique o padrão para capturar uma parte menor da sequência e expandi-la gradualmente.

Rótulos de arquivo

- Compatibilidade: A detecção de rótulo de arquivo não funciona para Confluence ou JIRA.
- Metadados: Abra Propriedades do Documento em um aplicativo Microsoft. O valor deve corresponder exatamente ao rótulo do arquivo de guarda-chuva; isso diferencia maiúsculas de minúsculas.
- Criptografia: A detecção de rótulo não funciona para arquivos protegidos por senha ou criptografados.

Sites e destinos

- Aplicativos suportados: Revise a lista de aplicativos suportados. Para aplicativos sem suporte ou "Todos os destinos", somente tipos MIME específicos são verificados.
- Aplicativos verificados: Os aplicativos testados (por exemplo, dlptest.com) são examinados de forma mais abrangente. Sites aleatórios só podem ser verificados quanto a violações de arquivos.
- Nomes de arquivo: O sistema pesquisa nomes de arquivo somente para determinados aplicativos verificados.

Solucionar Falsos Positivos

Se o DLP corresponder ao conteúdo inesperadamente, verifique o nome do classificador e a regra DLP em Relatórios > Prevenção de Perda de Dados. Se a detecção for legítima, mas indesejável, ajuste as configurações de Limites ou Proximidade para refinar a política.

Suporte a aplicativos de desktop

O suporte para aplicativos baseados em desktop (por exemplo, Outlook, Teams ou Google Workspace) é fornecido na base do melhor esforço. A eficácia depende do formato de mensagem usado durante o upload de arquivos, que pode diferir entre as versões baseadas na Web e na área de trabalho. Para aplicativos não verificados, não há garantia de que os carregamentos de arquivos serão suportados.

Recursos do classificador DLP

- Números de cartão de crédito: O algoritmo Luhn é usado para validação. Teste somente com números de cartão de crédito válidos.
- Nomes de Pessoas: Requer de 2 a 3 palavras, e cada palavra deve estar em maiúsculas.
- Combinações de Nomes: Uma string separadora é necessária entre o nome e outros dados (por exemplo, "Viagra - John Smith" corresponde, mas "Viagra John Smith" não).
- Data de nascimento: Deve estar próximo a uma palavra-chave ou cabeçalho, como "dob" ou "data de nascimento".
- Conteúdo censurável: Determinadas cadeias de caracteres de exceção impedem que esse classificador seja acionado se o texto se parecer com um livro ou relatório.
- CEP: Deve estar próximo a palavras-chave específicas relacionadas à localização.

Correspondência de dados exata (EDM)

Antes de investigar o EDM, confirme se a varredura geral do DLP está funcionando. Para problemas específicos do EDM, verifique se o campo "Última edição" está atual no painel e verifique a saída da ferramenta de indexação.

Uso do comando:

Execute a ferramenta de indexação com a opção `-d` para gerar um arquivo de filtro de bloom (.blm). Esse comando é usado para validar o índice EDM e solucionar o problema de como os registros devem ser ignorados. O sinalizador `-d` instrui a ferramenta a gerar a saída do arquivo de filtro bloom de diagnóstico, que deve ser compartilhado com o suporte junto com um arquivo de exemplo ou dados da ferramenta de desenvolvedor HAR/Web.

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.