

Configuração de download de arquivo ZIP protegido por senha para acesso seguro

Contents

Problema

Após a migração para o Cisco Secure Access, os usuários não podem fazer download de arquivos ZIP protegidos por senha (criptografados). Os downloads falham consistentemente ao tentar acessar conteúdo de arquivo criptografado por meio do serviço Secure Access. Esse problema ocorre apesar de ter configurado políticas de tráfego vinculadas à Internet em um dispositivo C8200 com várias regras de segurança, incluindo bloqueio baseado em categoria, controles de inspeção SSL e funcionalidade de sandbox.

Os usuários experimentam falhas de download completo ao tentar acessar arquivos ZIP protegidos por senha que eram anteriormente acessíveis antes da migração do Secure Access. O problema persiste em vários grupos de túnel e afeta todos os 15 locais configurados.

Ambiente

- Cisco Secure Access (ID da empresa de acesso seguro: 8320925)
- Dispositivo C8200 que gerencia políticas de tráfego ligadas à Internet
- Vários grupos de túneis em 15 locais (TK-TG e outros)
- Políticas de inspeção SSL com configurações ativadas e desativadas
- Perfis de segurança de área restrita habilitados em determinadas políticas
- Perfis IPS configurados em regras de acesso específicas

Resolução

A resolução para permitir downloads de arquivos ZIP protegidos por senha no Cisco Secure Access envolve a configuração Permitir acesso a arquivos criptografados e a implementação de soluções apropriadas quando necessário.

Método de configuração principal

Passo 1: Acesse a configuração da política de acesso seguro da Cisco

Navegue até a política de acesso específica que controla o tráfego afetado no painel do Cisco Secure Access.

Passo 2: Habilitar Acesso a Arquivos Criptografados

Na política Advanced Settings, localize e habilite a opção Allow access to encrypted files. Essa configuração é definida por regra e controla se o conteúdo criptografado pode ser acessado por meio dessa política específica.

Passo 3: Aplicar a configuração

Salve e aplique as alterações de política para torná-las ativas para o tráfego do usuário.

Método alternativo

Se o método principal não resolver o problema, implemente a solução descrita nas próximas seções.

Passo 1: Identificar URLs Afetadas

Determine os URLs ou domínios específicos onde os arquivos ZIP protegidos por senha estão hospedados e causando falhas de download.

Passo 2: Configurar Lista Não Descriptografar

Adicione os URLs identificados à lista Do Not Decrypt em sua configuração do Cisco Secure Access. Isso impede a inspeção de SSL nesses URLs específicos.

Passo 3: Criar Política de Desvio de Inspeção SSL

Verifique se uma política de acesso com inspeção SSL desabilitada está configurada para tratar o tráfego para essas URLs.

Essa política deve ter:

- Inspeção SSL desabilitada
- Todos os perfis de segurança desabilitados
- Prioridade mais alta do que as políticas habilitadas para inspeção SSL

Referência de Configuração de Política

A ordem de política descrita nas próximas subseções e suas respectivas configurações podem ser usadas como referência para o tratamento adequado do tráfego.

Política 1: Regra de bloqueio baseada em categoria

- Nome da política: Bloco de conteúdo IA para Internet
- Perfil de IPS: Nenhum

- Propósito: Bloquear categorias de conteúdo específicas
- Destino: Todos os grupos de túnel

Política 2: Regra de Inspeção SSL Desabilitada

- Nome da política: IA-SSL-Inspection-MUKOU
- Perfil de IPS: Desabilitado
- Perfis de segurança: Todos desabilitados
- Destino: Todos os grupos de túnel

Política 3: Regra habilitada para Inspeção SSL

- Nome da política: Inspeção IA-SSL
- Perfil de IPS: Habilitado
- Perfis de segurança: Funcionalidade de área restrita habilitada
- Destino: Todos os grupos de túnel

Notas importantes sobre configuração

Não há configurações globais equivalentes para a funcionalidade Permitir acesso a arquivos criptografados. Essa configuração deve ser definida em políticas de acesso individuais conforme necessário. Cada política que exige acesso a arquivos criptografados deve ter essa configuração explicitamente habilitada na configuração de Configurações avançadas.

Ao testar alterações de configuração, dê tempo suficiente para a propagação da política na infraestrutura do Cisco Secure Access antes de validar a funcionalidade. Os incidentes de serviço ou as janelas de manutenção podem afetar os resultados dos testes e devem ser considerados durante a solução de problemas.

Causa

O problema ocorre porque o Cisco Secure Access, por padrão, bloqueia o acesso a arquivos criptografados como medida de segurança. Quando a inspeção SSL é ativada e encontra conteúdo protegido por senha ou criptografado, o serviço impede o download, a menos que seja explicitamente configurado para permitir esse acesso. A configuração Permitir acesso a arquivos criptografados nas Configurações avançadas de políticas de acesso controla esse comportamento e, sem essa configuração habilitada, os arquivos ZIP criptografados e conteúdo semelhante são bloqueados durante o processo de download.

Além disso, as políticas de inspeção de SSL podem interferir nos downloads de arquivos criptografados quando o processo de inspeção não consegue lidar adequadamente com o conteúdo criptografado, exigindo a configuração de acesso a arquivos criptografados ou o desvio de inspeção de SSL para os URLs afetados.

Conteúdo relacionado

- [Controles de segurança avançados](#)
- [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.