Configurar SSE Não descriptografar para desvio de descriptografia de IPS e SWG

Contents

Problema

O tráfego HTTPS para destinos da categoria financeira continua a apresentar um certificado Cisco SSE em vez do certificado do site de origem, mesmo depois de adicionar a categoria Finanças ou domínios específicos a uma lista Não descriptografar (DND) e aplicar a regra de acesso relevante. Esse comportamento é observado ao acessar sites pelo Zero Trust Access Client (TIA), impactando especificamente o acesso a sites relacionados a finanças, como https://onlinesbi.sbi.bank.in/, onde é necessária a visibilidade de certificado de ponta a ponta.

O comportamento esperado é que quando um site ou categoria de conteúdo é adicionada à lista DND, o certificado do site de origem pode ser apresentado ao navegador em vez do certificado SSE da Cisco. No entanto, o certificado Cisco SSE continua a ser apresentado, indicando que a descriptografia de tráfego ainda está ocorrendo, apesar da configuração de DND.

Ambiente

- Cisco Secure Service Edge (SSE)
- Conectividade de Zero Trust Access Client (TIA)
- Descriptografia IPS global habilitada
- IPS ativo em políticas de acesso
- Categoria financeira configurada na lista Não descriptografar no perfil de segurança
- Regras de acesso aplicadas com os perfis de segurança correspondentes

Resolução

A resolução envolve entender que o Cisco SSE executa dois tipos distintos de descriptografia e

definir as configurações apropriadas de Não descriptografar para ambos os tipos de descriptografia.

Entendendo os tipos de descriptografia SSE

O Cisco SSE executa dois processos de descriptografia separados:

- Descriptografia SWG (Secure Web Gateway) - Descriptografia do proxy da Web
- Descriptografia IPS - Descriptografia do sistema de prevenção contra invasões

Não descriptografar entradas configuradas dentro de um perfil de segurança aplicam-se somente à descriptografia SWG e não impedem a descriptografia IPS. Quando a descriptografia IPS global está habilitada e o IPS está ativo em qualquer política de acesso, a descriptografia IPS ainda ocorre, resultando na apresentação do certificado Cisco SSE ao navegador.

Configuration Steps

Passo 1: Adicione sites ou categorias de conteúdo à lista Não descriptografar fornecida pelo sistema.

A lista Não descriptografar fornecida pelo sistema é aplicada a todos os perfis IPS. Adicionar um site ou categoria de conteúdo a esta lista Fornecida pelo Sistema resulta na apresentação do certificado do site de origem, efetivamente ignorando a descriptografia de IPS.

Passo 2: Verifique se nenhuma alteração de política adicional é necessária.

Não há necessidade de fazer referência à lista Não descriptografar fornecida pelo sistema dentro das políticas de acesso. A lista é aplicada automaticamente a todos os perfis IPS.

Teste de validação

Estes métodos de validação podem ser usados para confirmar a configuração apropriada:

Método 1: Adicionar Domínio à Lista Não Descriptografar Fornecida pelo Sistema

Adicionar o domínio específico à lista Não descriptografar fornecida pelo sistema pode resultar na apresentação do certificado do site de origem em vez do certificado SSE da Cisco.

Método 2: Desabilitar temporariamente a descriptografia global de IPS (somente para teste)

A desativação temporária da descriptografia global de IPS também faz com que o certificado de origem seja visto para o site testado, confirmando que a descriptografia de IPS foi a causa da apresentação do certificado Cisco SSE.

Resultados esperados

Após a configuração apropriada:

- Sites ou categorias de conteúdo adicionadas à lista Não descriptografar fornecidos pelo sistema apresentam seus certificados de sites originais.
- A descriptografia de SWG e IPS é ignorada para os sites ou categorias especificados.
- O navegador exibe o certificado real do site em vez do certificado SSE da Cisco.

Causa

O problema ocorre porque o Cisco SSE executa dois processos de descriptografia distintos: Descriptografia SWG e descriptografia IPS. Não descriptografar entradas configuradas nos perfis de segurança apenas ignora a descriptografia SWG. Quando a descriptografia IPS global está habilitada e o IPS está ativo nas políticas de acesso, a descriptografia IPS continua a ocorrer de forma independente, fazendo com que o certificado Cisco SSE seja apresentado ao navegador mesmo quando os sites são incluídos nas listas DND do perfil de segurança.

Para ignorar completamente os dois tipos de descriptografia, sites ou categorias de conteúdo devem ser adicionados à lista Não descriptografar fornecida pelo sistema, que se aplica a todos os perfis de IPS e impede que ocorra a descriptografia de SWG e IPS.

Conteúdo relacionado

- Criar lista Não descriptografar efetiva para acesso seguro
- Solucionar problemas e coletar informações básicas para acesso seguro
- 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.