Entender a descriptografia de tráfego SWG com descriptografia HTTPS habilitada

Contents

Introdução

Este documento descreve como o Cisco Secure Web Gateway (SWG) trata a descriptografia de tráfego quando a descriptografia HTTPS está habilitada.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure Web Gateway.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

Em um conjunto de regras de política da Web com descriptografia HTTPS habilitada, o tráfego será descriptografado somente se um SNI (Server Name Indicator, indicador de nome de servidor) estiver presente no handshake TLS.

Solução

As Políticas de Segurança e Uso Aceitável ainda podem ser aplicadas com base nos servidores

de destino para os quais a solicitação está sendo enviada. As listas de destino podem ser criadas para esses servidores de destino e as regras podem ser aplicadas de acordo.

Todos os blocos de políticas DNS para túneis e AnyConnect ainda podem ser aplicados.

Causa

Esse comportamento é intencional.

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.