Aplicação da política de acesso seguro para determinados protocolos de aplicação

Contents

Introdução

Este documento descreve a aplicação da política de Acesso Seguro ao usar determinados protocolos de aplicação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro
- File Transfer Protocol (FTP)
- Transmission Control Protocol (TCP)
- Firewall como serviço (FWaaS)
- Secure Shell (SSH)
- Protocolo HTTP
- Conexão de Internet Quick UDP (QUIC)
- Protocolo SMTP

Informações de Apoio

Um teste FWaaS típico para avaliar a aplicação de políticas baseadas em protocolos de aplicativos é um teste de mau uso de protocolos.

O teste para esse cenário geralmente envolve a criação de uma política que bloqueie um protocolo de aplicação específico, como FTP/SSH em uma porta não padrão . por exemplo, permitir o FTP somente na porta 21 do TCP e bloquear o FTP na porta 80 do TCP.

O Secure Access usa a detecção de protocolo OpenAppID para detectar protocolos de aplicativos como FTP, SSH, QUIC, SMTP e outros. Além disso, utiliza um Secure Web Gateway para proteger o tráfego HTTP(S).

Problema: O teste de aplicação de política para determinados protocolos de aplicação no TCP 80/443 resulta em timeout de conexão e nenhum registro é gerado no Secure Access

Sob certas circunstâncias, como a tentativa de permitir/bloquear certos protocolos como o FTP na porta TCP 80/443, encontramos uma situação em que a conexão inicial entre o cliente e o servidor é interceptada pelo mecanismo de proxy, o handshake TCP é concluído e, em seguida, o mecanismo de proxy no Secure Access espera que o cliente envie tráfego, mas o protocolo requer um sinal do lado do servidor para alcançar o cliente.

Essa situação leva ao tempo limite da conexão, pois o cliente está aguardando o sinal do servidor e o proxy desfaz a conexão eventualmente. E o Secure Access não gera logs para esse tipo de sessão.

Solução

Esse é um comportamento esperado devido à maneira como o tráfego da Web é protegido pela arquitetura de Acesso Seguro e como esse teste envolve tráfego não Web (FTP, SSH, Telnet, SMTP, IMAP e outros protocolos que dependem inicialmente de um sinal do lado do servidor) em portas da Web, nenhum registro é gerado para essa sessão.

Informações Relacionadas

- Guia do usuário do Secure Access
- Página da comunidade de acesso seguro
- Suporte Técnico e Documentação - Cisco Systems

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.