Aplicación de políticas de acceso seguro para determinados protocolos de aplicación

Contenido

Introducción

Prerequisites

Requirements

Antecedentes

Problema: la prueba de aplicación de políticas para determinados protocolos de aplicación en TCP 80/443 produce un tiempo de espera de conexión y no se generan registros en Secure Access

Solución

Información Relacionada

Introducción

Este documento describe la aplicación de políticas de Secure Access cuando se utilizan ciertos protocolos de aplicación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro
- Protocolo de transferencia de archivos (FTP)
- Transmission Control Protocol (TCP)
- Firewall como servicio (FWaaS)
- Secure Shell (SSH)
- Protocolo de transferencia de hipertexto (HTTP)
- Conexión rápida a Internet UDP (QUIC)
- Protocolo de transferencia de correo seguro (SMTP)

Antecedentes

Una prueba típica de FWaaS para evaluar la aplicación de políticas basadas en el protocolo de aplicación es una prueba de uso incorrecto del protocolo.

La prueba para este escenario usualmente involucra la creación de una política que bloquea un protocolo de aplicación específico tal como FTP/SSH en un puerto no estándar . por ejemplo permitiendo FTP solamente en el puerto TCP 21 y bloqueando FTP en el puerto TCP 80.

Secure Access utiliza la detección del protocolo OpenAppID para detectar protocolos de aplicación como FTP, SSH, QUIC, SMTP y otros. y utiliza un gateway web seguro para proteger el tráfico HTTP(S).

Problema: la prueba de aplicación de políticas para determinados protocolos de aplicación en TCP 80/443 produce un tiempo de espera de conexión y no se generan registros en Secure Access

En ciertas circunstancias como intentar permitir/bloquear ciertos protocolos como FTP en el puerto TCP 80/443, nos encontramos con una situación en la que la conexión inicial entre el cliente y el servidor es interceptada por el motor proxy, se completa el intercambio de señales TCP y luego el motor proxy en Secure Access espera al cliente para enviar tráfico, pero el protocolo requiere una señal del lado del servidor para alcanzar al cliente.

Esta situación provoca que se agote el tiempo de espera de la conexión debido a que el cliente espera la señal del servidor y el proxy interrumpe la conexión finalmente. Secure Access no genera registros para este tipo de sesiones.

Solución

Se trata de un comportamiento esperado debido a la forma en que la arquitectura Secure Access protege el tráfico web y dado que dicha prueba implica tráfico no web (FTP, SSH, Telnet, SMTP, IMAP y otros protocolos que dependen inicialmente de una señal del lado del servidor) en puertos web, no se generan registros para dicha sesión.

Información Relacionada

- Guía del usuario de Secure Access
- Página Comunidad de Secure Access
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).