Application de politiques d'accès sécurisé pour certains protocoles d'application

Table des matières

Introduction

Ce document décrit l'application de la stratégie d'accès sécurisé lors de l'utilisation de certains protocoles d'application.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé
- File Transfer Protocol FTP
- Protocole de contrôle de transmissions (TCP)
- Pare-feu en tant que service (FWaaS)
- Secure Shell (SSH)
- Protocole HTTP (Hyper Text Transfer Protocol)
- Connexion Internet Quick UDP (QUIC)
- Protocole SMTP (Secure Mail Transfer Protocol)

Informations générales

Un test FWaaS typique pour évaluer l'application des politiques basées sur les protocoles d'application est un test d'utilisation abusive des protocoles.

Le test de ce scénario implique généralement la création d'une stratégie bloquant un protocole d'application spécifique tel que FTP/SSH sur un port non standard . Par exemple, autoriser FTP uniquement sur le port TCP 21 et bloquer FTP sur le port TCP 80.

Secure Access utilise la détection de protocole OpenAppID pour détecter des protocoles d'application tels que FTP, SSH, QUIC, SMTP et autres. et utilise une passerelle Web sécurisée afin de sécuriser le trafic HTTP(S).

Problème : le test d'application de la stratégie pour certains protocoles d'application sur TCP 80/443 entraîne un délai d'expiration de la connexion et aucun journal n'est généré dans Secure Access

Dans certaines circonstances, par exemple en essayant d'autoriser/de bloquer certains protocoles comme FTP sur le port TCP 80/443, nous rencontrons une situation où la connexion initiale entre le client et le serveur est interceptée par le moteur proxy, la connexion TCP est terminée, puis le moteur proxy dans Secure Access attend que le client envoie du trafic, mais le protocole nécessite un signal côté serveur pour atteindre le client.

Cette situation entraîne l'expiration du délai de connexion en raison du fait que le client attend le signal du serveur et que le proxy finit par interrompre la connexion. Et Secure Access ne génère aucun journal pour ce type de session.

Solution

Il s’agit d’un comportement attendu en raison de la manière dont le trafic Web est sécurisé par l’architecture d’accès sécurisé et étant donné qu’un tel test implique un trafic non Web (FTP, SSH, Telnet, SMTP, IMAP et d’autres protocoles qui s’appuient initialement sur un signal côté serveur) sur des ports Web, aucun journal n’est généré pour une telle session.

Informations connexes

- Guide de l'utilisateur Secure Access
- Page Communauté d'accès sécurisé
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.