Secure Access Policy Enforcement for Certain Application Protocols

Contents

Introduction

This document describes Secure Access policy enforcement when using certain application protocols.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Access
- File Transfer Protocol (FTP)
- Transmission Control Protocol (TCP)
- Firewall as a Service (FWaaS)
- Secure Shell (SSH)
- Hyper Text Transfer Protocol (HTTP)
- Quick UDP Internet Connection (QUIC)
- Secure Mail Transfer Protocol (SMTP)

Background Information

A typical FWaaS test to evaluate application protocol-based policy enforcement is a protocol misuse test.

The test for this scenario usually involves creating a policy blocking a specific application protocol such as FTP/SSH on a non-standard port . for example allowing FTP only on TCP port 21 and blocking FTP on TCP port 80.

Secure Access uses OpenAppID protocol detection to detect application protocols such as FTP, SSH, QUIC, SMTP and others. and utilizes a Secure Web Gateway in order to secure HTTP(S) traffic.

Problem: Policy enforcement test for certain application protocols on TCP 80/443 results in connection timeout and no logs are

generated in Secure Access

Under certain circumstances such as attempting to allow/block certain protocols like FTP on TCP port 80/443, we encounter a situation where the initial connection between the client and the server is intercepted by the proxy engine, the TCP handshake is completed and then the proxy engine in Secure Access waits on the client to send traffic, but the protocol requires a server-side signal to reach the client.

This situation leads to the connection timing out because of the client waiting on the server signal and the proxy tears down the connection eventually. And Secure Access generates no logs for this type of sessions.

Solution

This is an expected behavior due to the way web traffic is secured by the Secure Access architecture and since such a test involves non-web traffic (FTP, Telnet, SMTP, IMAP and other protocols that rely on a server-side signal initially) on web ports, no logs are generated for such a session.

Related Information

- **Secure Access User Guide**
- **Secure Access Community Page**
- **Technical Support & Documentation - Cisco Systems**