针对特定应用协议的安全访问策略实施

目录

简介

本文档介绍使用某些应用协议时的安全访问策略实施。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全访问
- 文件传输协议 (FTP)
- 传输控制协议 (TCP)
- 防火墙即服务(FWaaS)
- Secure Shell (SSH)
- 超文本传输协议(HTTP)
- 快速UDP互联网连接(QUIC)
- 安全邮件传输协议(SMTP)

背景信息

用于评估基于应用协议的策略实施的典型FWaaS测试是协议误用测试。

此场景的测试通常涉及创建阻止特定应用协议（例如，非标准端口上的FTP/SSH）的策略。例如，仅允许FTP在TCP端口21上，而阻止FTP在TCP端口80上。

安全访问使用OpenAppID协议检测来检测FTP、SSH、QUIC、SMTP等应用协议，并使用安全Web网关来保护HTTP(S)流量。

问题：TCP 80/443上特定应用协议的策略实施测试导致连接超时

，并且不会在安全访问中生成任何日志

在某些情况下，例如在TCP端口80/443上尝试允许/阻塞FTP等协议时，客户端与服务器之间的初始连接被代理引擎截取，TCP握手完成，然后安全访问中的代理引擎等待客户端发送流量，但是协议需要服务器端信号才能到达客户端。

这种情况会导致连接超时，因为客户端正在等待服务器信号，而代理最终会断开连接。并且，安全访问不会生成此类会话的日志。

解决方案

由于安全访问架构保护Web流量的方式，并且此类测试涉及Web端口上的非Web流量（FTP、SSH、Telnet、SMTP、IMAP以及最初依赖服务器端信号的其他协议），因此这是预期行为，因此不会为此类会话生成日志。

相关信息

- 安全访问用户指南
- “安全访问：社区”页
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。