Durchsetzung von Zugriffsrichtlinien für bestimmte Anwendungsprotokolle

Inhalt

Einleitung

Voraussetzungen

- Anforderungen

Hintergrundinformationen

Problem: Der Richtliniendurchsetzungstest für bestimmte Anwendungsprotokolle unter TCP 80/443 führt zu einem Verbindungs-Timeout, und in Secure Access werden keine Protokolle generiert.

Lösung

Zugehörige Informationen

Einleitung

In diesem Dokument wird die Durchsetzung von Richtlinien für sicheren Zugriff bei der Verwendung bestimmter Anwendungsprotokolle beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff
- File Transfer Protocol (FTP)
- Transmission Control Protocol (TCP)
- Firewall as a Service (FWaaS)
- Secure Shell (SSH)
- Hyper Text Transfer Protocol (HTTP)
- Schnelle UDP-Internetverbindung (QUIC)
- Secure Mail Transfer Protocol (SMTP)

Hintergrundinformationen

Ein typischer FWaaS-Test zur Evaluierung der protokollbasierten Richtliniendurchsetzung ist ein Test auf Missbrauch des Protokolls.

Der Test für dieses Szenario beinhaltet in der Regel das Erstellen einer Richtlinie, die ein bestimmtes Anwendungsprotokoll wie FTP/SSH auf einem nicht standardmäßigen Port blockiert, z. B. FTP nur auf TCP-Port 21 zulässt und FTP auf TCP-Port 80 blockiert.

Secure Access verwendet die OpenAppID-Protokollerkennung, um Anwendungsprotokolle wie FTP, SSH, QUIC, SMTP usw. zu erkennen, und verwendet ein sicheres Web-Gateway, um HTTP(S)-Datenverkehr zu schützen.

Problem: Der Richtliniendurchsetzungstest für bestimmte Anwendungsprotokolle unter TCP 80/443 führt zu einem Verbindungs-Timeout, und in Secure Access werden keine Protokolle generiert.

Unter bestimmten Umständen, z. B. beim Versuch, bestimmte Protokolle wie FTP auf dem TCP-Port 80/443 zuzulassen/zu blockieren, tritt eine Situation auf, in der die ursprüngliche Verbindung zwischen dem Client und dem Server von der Proxy-Engine abgefangen wird, der TCP-Handshake abgeschlossen ist und dann die Proxy-Engine in Secure Access auf den Client wartet, um Datenverkehr zu senden. Das Protokoll erfordert jedoch ein serverseitiges Signal, um den Client zu erreichen.

Diese Situation führt dazu, dass die Verbindung aufgrund des auf das Serversignal wartenden Clients zu einem Timeout führt und der Proxy die Verbindung schließlich abbricht. Secure Access generiert für diese Art von Sitzungen keine Protokolle.

Lösung

Dies ist ein erwartetes Verhalten aufgrund der Art und Weise, wie der Web-Datenverkehr durch die Secure Access-Architektur gesichert wird. Da ein solcher Test nicht-Web-Datenverkehr (FTP, SSH, Telnet, SMTP, IMAP und andere Protokolle, die anfangs auf ein serverseitiges Signal angewiesen sind) an Web-Ports umfasst, werden für eine solche Sitzung keine Protokolle generiert.

Zugehörige Informationen

- Benutzerhandbuch zu Secure Access
- Seite "Sicherer Zugriff auf Community"
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.