特定のアプリケーションプロトコルに対するセキュアアクセスポリシーの適用

内容

はじめに

このドキュメントでは、特定のアプリケーションプロトコルを使用する際のセキュアアクセスポリシーの適用について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアなアクセス
- File Transfer Protocol（FTP）
- Transmission Control Protocol（TCP）
- サービスとしてのファイアウォール(FWaaS)
- セキュア シェル（SSH）
- ハイパーテキスト転送プロトコル(HTTP)
- クイックUDPインターネット接続(QUIC)
- セキュアメール転送プロトコル(SMTP)

背景説明

アプリケーションプロトコルベースのポリシー適用を評価する一般的なFWaaSテストは、プロトコル誤用テストです。

このシナリオのテストには通常、非標準ポートでのFTP/SSHなどの特定のアプリケーションプロトコルをブロックするポリシーの作成が含まれます（たとえば、TCPポート21でのFTPのみを許可し、TCPポート80でのFTPをブロックするなど）。

Secure Accessは、OpenAppIDプロトコル検出を使用して、FTP、SSH、QUIC、SMTPなどのアプリケーションプロトコルを検出します。また、HTTP(S)トラフィックを保護するために、セキュリティで保護されたWebゲートウェイを使用します。

問題：TCP 80/443で特定のアプリケーションプロトコルのポリシー適用テストを実行すると、接続タイムアウトが発生し、セキュアアクセスでログが生成されない

TCPポート80/443のFTPなどの特定のプロトコルを許可/ブロックしようとする場合、クライアントとサーバ間の初期接続がプロキシエンジンによってインターセプトされ、TCPハンドシェイクが完了した後、セキュアアクセスのプロキシエンジンがクライアントでトラフィックの送信を待機する状況がありますが、プロトコルはクライアントに到達するためにサーバ側の信号を必要とします。

この状況では、クライアントがサーバ信号で待機し、プロキシが最終的に接続を切断するため、接続がタイムアウトします。Secure Accessでは、このタイプのセッションのログは生成されません。

解決方法

これは、Webトラフィックをセキュアアクセスアーキテクチャで保護する方法が原因で想定される動作であり、このようなテストにはWebポート上の非Webトラフィック（FTP、SSH、Telnet、SMTP、IMAP、および最初はサーバ側の信号に依存するその他のプロトコル）が含まれるため、そのようなセッションのログは生成されません。

関連情報

- セキュアアクセスユーザガイド
- セキュアアクセスコミュニティページ
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。