目次

概要

このドキュメントでは、接続の構築時と切断時の適応型セキュリティ アプライアンス (ASA) デバイスで生成されたトランスミッション コントロール プロトコル (TCP) /User Datagram Protocol (UDP;ユーザ データグラム プロトコル) syslog の解釈方法を説明します。

接続を構築するか、切断するときに、ASA によって生成される syslog を解釈する方法

このドキュメントに記載されているすべての syslog は、次に示すネットワーク トポロジに基づいています。

ネットワーク トポロジ

シナリオ 1： ASA 内部インターフェイス (識別) への管理トラフィックの送信元が内部ホスト

シナリオ 2： ASA を通過するトラフィックの送信元が内部ホストで、宛先が外部ホスト

シナリオ 3： ASA 外部インターフェイス (識別) への管理トラフィックの送信元が外部ホスト

シナリオ 4： ASA を通過するトラフィックの送信元が外部ホストで、宛先が内部ホスト

ネットワーク トポロジ (同じセキュリティのインターフェイス)

シナリオ 1： ASA を通過するトラフィックの送信元が内部ホストで、宛先が外部ホスト

シナリオ 2： ASA を通過するトラフィックの送信元が外部ホストで、宛先が内部ホスト

* ここで、10.1.2.5 は 10.1.1.2 の静的 NAT IP です。

関連情報

- Cisco ASA 5500 シリーズ次世代ファイアウォール レファレンスガイド

- Cisco ASA 5500 シリーズ次世代ファイアウォール設定ガイド
- テクニカルサポートとドキュメント - Cisco Systems