ストリーム UDP インスペクタ

- ストリーム UDP インスペクタの概要 （1 ページ）
- ストリーム UDP インスペクタを設定するためのベストプラクティス （2 ページ）
- ストリーム UDP インスペクタのパラメータ （2 ページ）
- ストリーム UDP インスペクタのルール （2 ページ）
- ストリーム UDP インスペクタの侵入ルールのオプション （2 ページ）

ストリーム UDP インスペクタの概要

タイプ	インスペクタ（ストリーム）
使用方法	検査
インスタンス タイプ	マルチトン
その他のインスペクタが必要	なし
有効	`true`

User Datagram Protocol（UDP）はコネクションレス型の低遅延トランスポート層プロトコルです。UDP を使用すると、受信側から同意書が提供される前に、2 つのネットワークエンドポイント間のステートレス通信が可能になります。メッセージヘッダーとデータの整合性を評価するには、UDP はチェックサムを使用します。

`stream_udp` は IP データグラムヘッダー内の送信元および接続先の IP アドレスフィールドと、UDP ヘッダー内のポートフィールドを確認して、フローの方向を決定し、セッションを識別します。セッションは、設定可能なタイマーの期限が切れるか、または他のエンドポイントが到達不能という ICMP メッセージをいずれかのエンドポイントが受信したときに終了します。

UDP ストリームインスペクタはイベントを生成しません。パケットデコーダのルール（GID 116）を有効にして、UDP ヘッダーの異常を検出できます。

ストリームUDPインスペクタを設定するためのベストプラクティス

stream_udp インスペクタを設定する場合は、次のベストプラクティスを考慮してください。

- ホストまたはエンドポイントに適用するセッションタイムアウトごとに stream_udp インスペクタを作成します。ストリーム UDP インスペクタは、session_timeout を binder インスペクタで定義されている UDP ホストに関連付けます。

  同じネットワーク分析ポリシーに複数のバージョンの stream_udp インスペクタを含めることができます。

- パケットデコーダのルール（GID 116）を有効にして、UDP ヘッダーの異常を検出します。

ストリーム UDP インスペクタのパラメータ

session_timeout

UDP インスペクタが非アクティブな UDP ストリームを状態テーブルに保持する秒数を指定します。Snort が同じフローキーを持つ UDP データグラムを次に検出すると、以前のフローのセッションタイムアウトが期限切れになっているかどうかが確認されます。タイムアウトの期限が切れると、Snort はフローを閉じて新しいフローを開始します。Snort は、基本のストリーム設定に関連付けられた古いフローを確認します。

型：整数

有効な範囲：0 〜 2,147,483,647 (max31)

デフォルト値：30

ストリーム UDP インスペクタのルール

stream_udp インスペクタには、関連付けられたルールがありません。

ストリームUDPインスペクタの侵入ルールのオプション

stream_udp インスペクタには、侵入ルールのオプションはありません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。