ストリーム IP インスペクタ

ストリーム IP 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`

Internet Protocol（IP）は、インターネットの基礎を形成するコネクションレス型のネットワーク層プロトコルです。IP はホストアドレスを使用して、IP ネットワークを介し、送信元ホストから接続先ホストにメッセージをルーティングします。IPは、他のトランスポートプロトコルに加えて、TCP データパケットと UDP データパケットの両方をルーティングできます。

IP メッセージには、ヘッダーセクションとデータセクションが含まれています。IP ヘッダーには、メッセージを接続先にルーティングするために使用される IP アドレスが含まれています。IPデータセクションでは、メッセージペイロードがカプセル化されます。IPは、メッセージのリアセンブルとフラグメント化を処理します。

`stream_ip` インスペクタは、IP ネットワークフローを検出し、フロー内のパケットを確認します。`stream_ip` インスペクタは、IP セッションとフロートラッキング、オペレーティングシステム ポリシー、およびデータグラムのオーバーラップ設定パラメータを定義します。モードに応じて、`stream_ip` インスペクタまたは Snort データプレーンが最適化を処理します。

ストリームIPインスペクタを設定するためのベストプラクティス

stream_ip 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、エンドポイント、またはネットワークに適用する IP 設定ごとに stream_ip インスペクタを作成します。ストリーム IP インスペクタは、IP 設定を binder インスペクタで定義された IP ホスト、エンドポイント、またはネットワークに関連付けます。

  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_ip インスペクタを含めることができます。

ストリーム IP インスペクタのパラメータ

max_overlaps

データグラムごとの最大許容オーバーラップを指定します。オーバーラップを無制限に許可するには、0 を指定します。

ルール 123:12 を有効にして、フラグメントのオーバーラップが過剰な場合にアラートをトリガーできます。

型：整数

有効な範囲：0 ～ 4,294,967,295 (max32)

デフォルト値：0

min_frag_length

IP フラグメントで予想される最小バイト数を指定します。IP フラグメントのバイト数を無制限に許可するには、0 を指定します。

ルール 123:13 を有効にして、min_frag_length よりも短いフラグメントのアラートをトリガーできます。

型：整数

有効な範囲：0 ～ 65535

デフォルト値：0

min_ttl

ホップの最小数または存続時間（TTL）を指定します。指定した最小TTLを下回るフラグメントを破棄します。

ルール 123:11 を有効にして、TTL でこの値を下回るフラグメントのアラートをトリガーできます。

型：整数

有効な範囲：1 ～ 255

デフォルト値：1

policy

ターゲットホスト（複数可）のオペレーティングシステムを指定します。オペレーティングシステムは、適切な IP フラグメントのリアセンブルポリシーとオペレーティングシステムの特性を決定します。ストリーム IP インスペクタごとに policy パラメータを 1 つだけ定義できます。

（注） policy パラメータを first に設定すると、Snort はある程度の保護を提供できますが、攻撃は見逃します。IP ストリームインスペクタの policy パラメータを編集して、正しいオペレーティングシステムを指定する必要があります。

型：列挙体

有効な値： policy パラメータのオペレーティングシステムのタイプを設定します。

表 *1*：ポリシーの有効な値

ポリシー	オペレーティング システム
first	不明な OS（Unknown OS）
linux	Linux
bsd	AIX FreeBSD OpenBSD
bsd_right	HP JetDirect（プリンタ）
last	Cisco IOS
windows	Windows 98 Windows NT Windows 2000 Windows XP
solaris	Solaris OS SunOS

デフォルト値：`linux`

session_timeout

`stream_ip` インスペクタが状態テーブルの非アクティブな IP ストリームを保持する秒数を指定します。Snort が同じフローキーを持つ IP 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：`60`

ストリーム IP インスペクタのルール

`stream_ip` インスペクタのルールを有効にし、イベントを生成し、インライン展開では、違反パケットをドロップします。。

表 *2:* ストリーム *IP* インスペクタのルール

GID:SID	ルール メッセージ
123:1	フラグメント化されたパケットの IP オプションに一貫性がない（inconsistent IP options on fragmented packets）
123:2	ティアドロップ攻撃（teardrop attack）
123:3	短いフラグメント、DOS 試行の可能性がある（short fragment, possible DOS attempt）
123:4	フラグメントパケットが最適化済みのパケットの後で終了している（fragment packet ends after defragmented packet）
123:5	ゼロバイトのフラグメントパケット（zero-byte fragment packet）
123:6	フラグメントサイズが誤っているかパケットサイズが負になっている（bad fragment size, packet size is negative）
123:7	フラグメントサイズが誤っているか、パケットサイズが 65536 を超えている（bad fragment size, packet size is greater than 65536）
123:8	フラグメント化が重複している（fragmentation overlap）
123:11	TTL 値が設定された最小値よりも小さい、リアセンブルには使用しない（TTL value less than configured minimum, not using for reassembly）
123:12	フラグメントの重複が多すぎる（excessive fragment overlap）

GID:SID	ルール メッセージ
123:13	フラグメントが小さい（tiny fragment）

ストリーム IP インスペクタの侵入ルールのオプション

stream_ip 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。