# Firepower サービスによるプロセス 単一 ストリーム大きいセッション ( 象フロー )

## 目次



## 概要

シングルフローが Cisco Firepower アプライアンスの全体の定格 スループットをなぜ消費する場合がないかこの資料に記述されています。

## 背景説明

Webサイトを、かあらゆる帯域幅測定単位ツールの出力は ( たとえば、iperf ) テストするあらゆる帯域幅速度の結果 Cisco Firepower アプライアンスのアドバタイズされたスループット 定格を表わさないかもしれません。 同様に、あらゆる転送 プロトコル上の非常に大きいファイルの転送は Firepower アプライアンスのアドバタイズされたスループット 定格を示しません。 それは最大スループットを判別するために Firepower サービスが単一のネットワーク フローを使用しないので発生します。

## Snort によるプロセス トラフィック

Firepower サービスの基盤となる検出テクノロジーは Snort です。 Cisco Firepower アプライアンスの Snort の実装はシングル スレッド プロセス トラフィックを処理するためにです。 アプライアンスはアプライアンスを通過するすべてのフローの総スループットに基づいて特定の定格のために評価されます。 アプライアンスが社内ネットワーク ( 通常は境界エッジの近く ) に展開されていること、および何千もの接続を処理することが想定されています。

アプライアンスの各 CPU で動作する 1 Snort プロセスのいくつかの別の Snort プロセスへのトラフィックの Firepower サービス 使用 ロード バランシング。 理想的には、システム 負荷は Snort プロセスすべてを渡ってトラフィックの均等にバランスをとります。 Snort は次世代ファイアウ

ォール（NGFW）、侵入防御システム（IPS）および Advanced Malware Protection （AMP）インスペクション用の適切な文脈上分析を提供できる必要があります。 Snort を確認することは最も有効、シングルフローからのすべてのトラフィックです 1 つの snort 例にバランスをとられるロードです。 シングルフローからすべてのトラフィックが単一 snort 例にバランスをとられなかった場合、システムは避けることができ、Snort ルールが一致するまずないかもしれませんか、またはファイルのピースが AMP インスペクション用の隣接 しないようにトラフィックはこぼされて。 従って、ロード バランシング アルゴリズムはある特定の接続を識別できる接続 情報に基づいています。

### Firepower サービスおよび NGIPS バーチャルの ASA の 2 タプル アルゴリズム

Firepower サービスプラットフォームとので適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）次世代侵入防御システム（NGIPS）（NGIPS）バーチャルは、トラフィック 2 タプル アルゴリズムの使用と鼻を鳴らすためにバランスをとられるロードであり。 このアルゴリズムのデータポイントは次のとおりです。

- 送信元 IP
- 宛先 IP

### ソフトウェア バージョン 5.3 の 3 タプル アルゴリズムか Firepower および FTD アプライアンスの下部の

すべての以前のバージョンで（5.3 または下部の）、トラフィックは鼻を鳴らすためにバランスをとられるロードです 3 タプル アルゴリズムを使用する。 このアルゴリズムのデータポイントは次のとおりです。

- 送信元 IP
- 宛先 IP
- IP プロトコル

送信元、宛先、および IP プロトコルがすべて同じであるトラフィックはすべて、同じ Snort インスタンスにロード バランシングされます。

### Firepower および FTD アプライアンスのソフトウェア バージョン 5.4、6.0、およびより大きいの 5 タプル アルゴリズム

バージョン 5.4、6.0 またはより大きいで、トラフィックは 5 タプル アルゴリズムと鼻を鳴らすために balaned ロードです。 考慮に入れられる datapoints は次のとおりです:

- 送信元 IP
- 送信元ポート
- 宛先 IP
- 宛先ポート
- IP プロトコル

アルゴリズムにポートを追加する目的はトラフィックの大きい部分を占める特定の送信元および宛先ペアがあるときトラフィックのもっと均等にバランスをとることです。 ポートの付加によって、高位はかない送信元ポートはフローごとに異なり異なる snort 例にトラフィックのバランスをとる追加エントロピーをもっと均等に追加する必要があります。

## スループット合計

アプライアンスの総スループットは豊富な可能性にはたらくすべての snort 例の総スループットに基づいていました測定されます。 業界標準推奨事項はさまざまなオブジェクトのサイズの複数の HTTP 接続のためスループットを測定するためにです。 たとえば、NSS NGFW テストの手順は 44k、21k、10k、4.4k および 1.7k オブジェクトが付いているデバイスの総スループットを測定します。 これらは平均パケットサイズからののまわりで 1k 及び HTTP接続に関連する他のパケットが理由でバイトへの 128 バイトの範囲に変換します。

個々の Snort 例のパフォーマンス評価を推定できます。 アプライアンスの定格 スループットを奪取 し、動作する Snort 例の数それを分けて下さい。 たとえばアプライアンスが 1k バイトの平均パケットサイズの IPS のための 10Gbps で評価されれば、およびそのアプライアンス Snort の 20 の例を、シングル インスタンスのためのおおよそ最大スループットです Snort ごとの 500 Mbps 持っています。 トラフィックの異なる型は、ネットワークプロトコル、全面的なセキュリティポリシーの違いと共にパケットのサイズすべての影響デバイスの観察されたスループットできます。

### サード パーティ ツール テスト結果

速度をテストする Web サイトまたは帯域幅測定ツール（*iperf* など）でテストした場合、単一の大規模ストリーム TCP フローが生成されます。 このタイプの大規模 TCP フローは、**エレファント フロー**と呼ばれます。 1 つのエレファント フローは単一のセッションであり、大量の（または不均衡な）帯域幅を消費する、比較的長期間実行されるネットワーク接続です。 このタイプのフローは 1 つの Snort インスタンスに割り当てられるため、アプライアンスの総スループット速度ではなく、単一の Snort インスタンスのスループットがテスト結果に示されます。

## 修正

### インテリジェント アプリケーション バイパス（IAB）

ソフトウェア バージョン 6.0 は IAB と呼ばれる新しい 機能を導入します。 Firepower アプライアンスがあらかじめ定義されたパフォーマンス しきい値に達するとき、IAB 機能はインテリジェントにバイパスするために特定の条件を満たすフローを探します 検出エンジンの負荷を軽減する。

> **ヒント**： IAB の設定に関する詳細はここに見つけることができます。

### 大きいフローを識別し、信頼して下さい

大きいフローは頻繁に高い使用低いインスペクション値トラフィックたとえば、バックアップ、データベース複製、先祖などと関連しています これらのアプリケーションの多数はインスペクションから寄与することができません。 大きいフローにおいての問題を避けるために、大きいフローを識別し、それらのためのアクセスコントロール信頼ルールを作成できます。 これらのルールは大きいフローを識別できましたりそれらのフローが uninspected 渡し、単一 snort 例 動作によって制限されないようにします。

> **注:** 信頼ルールのための大きいフローを識別するために、Cisco Firepower TAC に連絡して下さい。

## 関連情報

- インテリジェント アプリケーション バイパスを使用したアクセス制御
- テクニカル サポートとドキュメント - Cisco Systems