Firepower サービスによる単一ストリーム大規模セッション（エレファント フロー）の処理

目次

概要

帯域幅速度をテストする Web サイトの結果や、帯域幅測定ツール（*iperf* など）の出力は、Cisco Firepower アプライアンスの公称スループット速度を示さないことがあります。 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。 これは、Firepower サービスが最大スループットの判別に単一のネットワーク フローを使用しないことが原因です。 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。

著者：Cisco TAC エンジニア、Nazmul Rajib および Foster Lipkey

Snort によるトラフィックの処理

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 アプライアンスでの Snort の実装は、トラフィック処理用の単一スレッド プロセスです。 アプライアンスでは、アプライアンスを通過するすべてのフローのスループット合計に基づいて、特定の速度が評価されます。 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。

Firepower はアプライアンスの各 CPU の 1 つの Snort プロセスが実行といくつかの別の Snort プロセスにトラフィックの使用ロード バランシングを保守します。 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 NGFW、IPS および 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、システムはトラフィックの分割によって Snort ルールが一致するま

ずないか、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 しないように避けることができます。 したがって、ロード バランシングのアルゴリズムは、特定の接続を固有に識別できる接続情報に基づきます。

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および NGIPS バーチャルの ASA で、トラフィックは 2 タプル アルゴリズムを使用して鼻を鳴らすために balaned ロードです。 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 3 タプル アルゴリズムを使用して鼻を鳴らすために balaned ロードです。 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 アルゴリズムを使用して鼻を鳴らすために balaned ロードです。 考慮されるデータポイントは次のとおりです。

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

ポートをアルゴリズムに追加する目的は、特定の送信元/宛先ペアがトラフィックのかなりの部分を占める場合に、トラフィックをより均等にバラシングすることです。 ポートを追加することにより、上位の一時的な送信元ポートがフローごとに異なり、エントロピーが増して、さまざまな Snort インスタンスにより均等にトラフィックがバランシングされます。

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。 スループットを測定するための業界標準推奨事項はさまざまなオブジェクトのサイズを使用して複数の HTTP 接続のためです。 たとえば、NSS NGFW テスト の 手順は 44k、21k、10k、4.4k および 1.7k オブジェクトを使用してデバイスの総スループットを測定します。 これらは HTTP接続に関連する他のパケットが理由で 1k バイトからののまわ

りでにに範囲の 128 バイト 平均パケットサイズ変換します。

アプライアンスの定格 スループットを奪取 し、動作している Snort 例の数それを分けることによって個々の Snort 例のパフォーマンス評価を推定できます。 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 ツールのテスト結果

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 には、**インテリジェント アプリケーション バイパス**（IAB）と呼ばれる新機能が導入されています。 Firepower アプライアンスが、事前定義されたパフォーマンスしきい値に達すると、IAB 機能は特定の基準を満たすフローを探してインテリジェントにバイパスするため、検出エンジンへの負荷が軽減されます。

> **ヒント**： IAB の設定の詳細については、こちらを参照してください。

大規模フローの特定および信頼

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されないかもしれません。 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:** 信頼ルールの対象となる大規模フローを識別するには、Cisco Firepower TAC にご連絡ください。

関連資料

- 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