Flowmon

V.8.01 ガイド

平成 28 年 8 月 1 日

Ver.8.01 対応

オリゾンシステムズ株式会社

目次

1. Ver7.02.05 以前の Flowmon をお使いの場合

Flowmon Ver7.02.05 以前のバージョンからアップデートをご検討の場合、Ver7.05.09 にアップデートする際、データベースのアップデート及びファイルチェックが行われる為、500GB/1 時間(弊社環境下実績時間)ほどかかります。その間データの収集は出来ませんのであらかじめご了承ください。

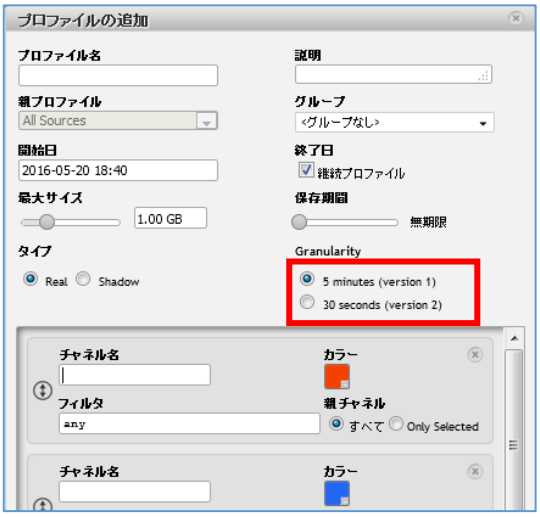
2. Flowmon 8.01 及び DDoS Defender V.3.0 情報

Flowmon 8.01 では Flowmon バージョン 8 で導入した新たなフローデータストレージのためのアーキテクチャを実装しました。Flowmon 8.01 で 30 秒間隔でのフロー収集を実現することで、より詳細な粒度での解析が可能になりました。これは内部アーキテクチャの進化によるものですが、加えて、いくつかの GUI の改善やその他便利な機能も追加されています。
また今回、Flowmon 8.01 では Flowmon DDoS Defender 3.0 を同時にリリースしました。収集粒度の詳細化および BGP Flowspec を活用したミティゲーション機能を提供しています。

3. 30 秒粒度プロファイルと、フローデータのストリーム処理

Flowmon 8.01 では 30 秒粒度でフローデータをプロファイルすることで、フローデータのストリーム処理を実現しています。新しいプロファイルでは、トラフィックグラフ上のトラフィック統計を、30 秒ごとのスライスで表示したまま、詳細分析を実行することが可能です。8.01 のプロファイルでは、驚くべき粒度の細かさによる解析を実現しました。もちろん、ユーザはこれまで通りの 5 分プロファイルと同じ手順で 30 秒プロファイルの作成が可能です。ただし、30 秒プロファイルは以前のデータからは作成できません。プロファイル作成後から有効となります。
粒度の詳細化にともない、即時対応が望まれる以下のケースにおいて、さまざまな効果が期待されます。

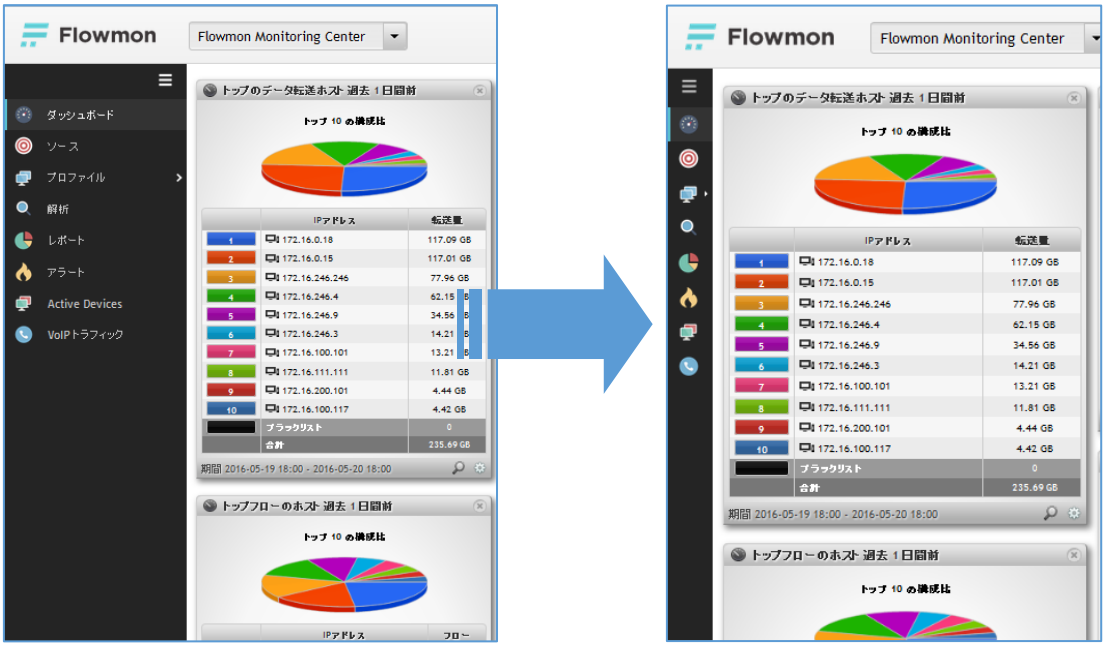
・ネットワークの振る舞い分析や異常検出
・DDoS 検出
・オペレーションの警告やセキュリティの問題の検出



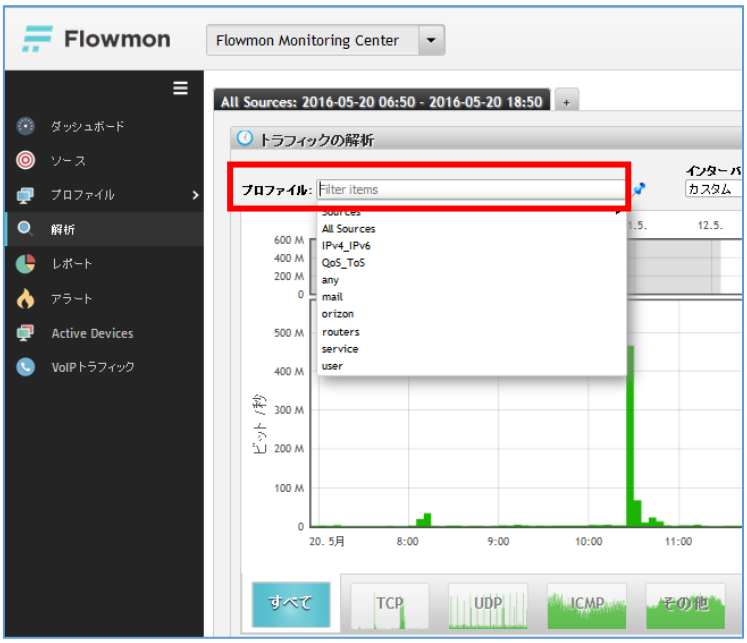
留意点：既存の 5 分間粒度プロファイルはそのままに残り、自動的に 30 秒粒度へ変更されることはありません。

4. フローティングメニュー

左側の新しいメニューは折り畳み式で提供され、手動で切り替えられます。



加えて、プロファイルのドロップダウンメニューにプロファイル名を入力することでフィルター機能が使用可能になりました。

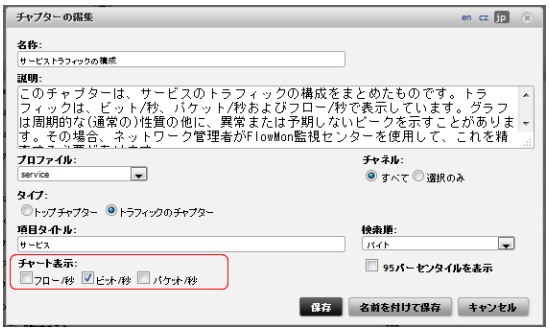


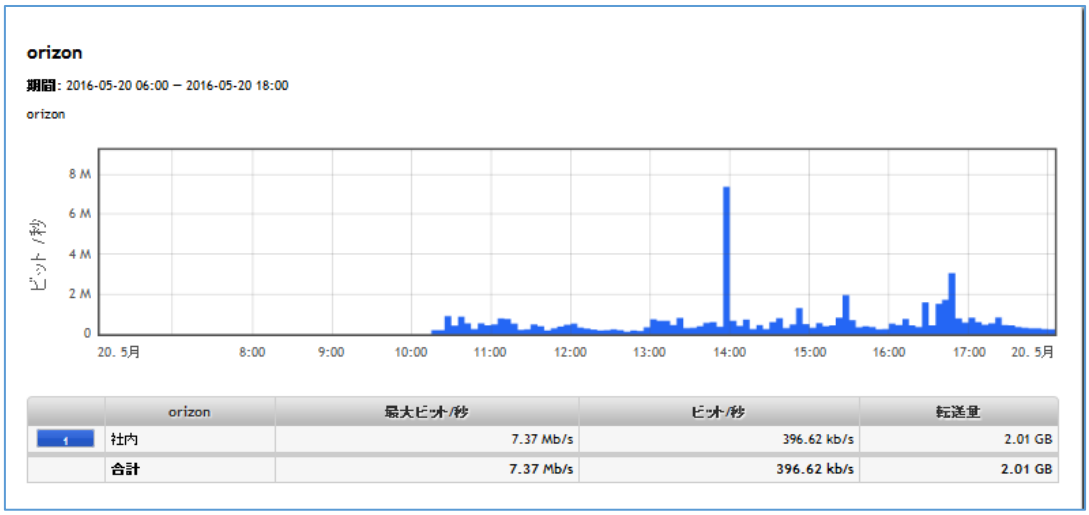
5. その他新機能と特徴

Flowmon　モニタリングセンター

・レポートを複数の E-mail アドレスに送信可能となりました。

・レポートのトラフィックでは選択したグラフのみを表示することが可能です。





・フローソースの可用性を SNMP によって監視します。

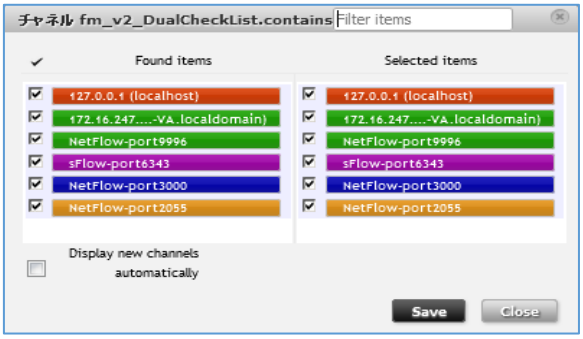
・ユーザログインに TACACS+のディレクトリサービスをサポート

・警告アイコン－設定されている場合、syslog や SNMP トラップでレポートすることが可能です。

・プロファイルと分析のグラフを集約機能(平均、最高)で選択することが出来ます。

・クエリパラメータを高度な解析結果画面に表示することが出来ます。

・分析画面の表示されたチャネルの変更画面の形式が変更されました。

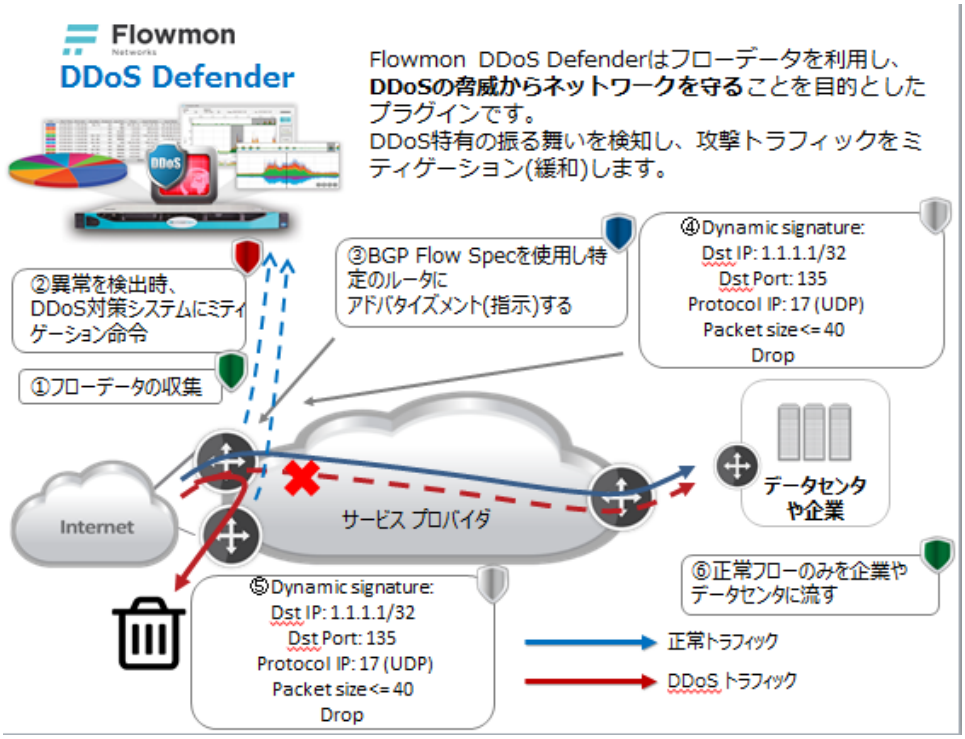


6. Flowmon コンフィグレーションセンター

・LDAP 設定 – グループプレフィックスと名前の間の区切り文字を選択することができます。
・名前解決及び変換オプションは FCC 設定に移動しました。 – システム – ユーザ設定で可能

7. Flowmon DDoS Defender

・検出時間の短縮
DDoS Defender3.0 は Flowmon8.01 で追加された、30 秒収集間隔プロファイルの利点を活用し、DDoS 攻撃を 60 秒間間隔で検出します。これはフローベースの検出間隔としては最先端に位置します。
・BGP Flowspec サポート
検出時間の短縮に加えて、DDoS　Defendere3.0 では BGP Flowspec をサポートしています。この技術は、他のスクラビングツールなどを利用せずに、DDoS 攻撃を緩和出来ます。
DDoS Defender は BGP Flowspec 機能を持っているルータに攻撃に関する動的シグネチャを提供しその情報を基に、ルータは攻撃を緩和します。



上の図は Flowmon DDoS Defender と BGP Flowspec を使って DDoS の緩和を行う際の例です。Flowmon の DDoS Defender はルータから恒常的にフローデータを収集し、トラフィックパターンを評価します。DDoS が発生した際は、BGP Flowspec を利用して、特定のルータにアドバタイズメント(指示)をします。この情報には、攻撃に関する動的なシグネチャが含まれており、その情報に基づきルータは特定トラフィックに対して対処を行います。

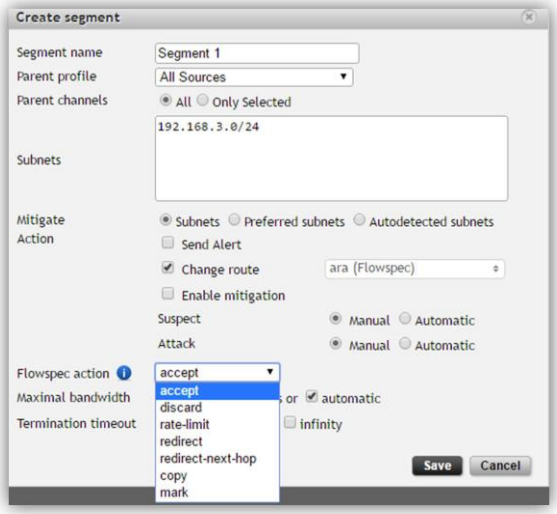
BGP Flowspec では、様々なタイプのフロー項目を指定することが可能なので、攻撃に関連した動的シグネチャとしてそれらを利用できます。詳しくは RFC5575 のドキュメントを参照して下さい。

DDoSDefender3.0 は動的なシグネチャを作成するに当たり、次の属性を参照しています。

・宛先プレフィックス
・送信元プレフィックス
・IP プロトコル
・宛先 port
・ICMP タイプ
・ICMP コード

攻撃を検知した際、ユーザは攻撃の詳細をアラートとして受け取ることが可能です。ユーザは攻撃が発生した際の緩和処理について、ルータの Flowspec ルールで事前に定義可能です。もしくは自動的に緩和処理が行われるように指定することも可能です。その場合、Flowspec ルールに追加する動的シグネチャは、初めの 30 秒の攻撃に基づき決定されます。ルールは、宛先ネットワーク、ソースネットワーク、宛先ポート、送信元ポートと L4 プロトコルにより定義されます。特定のセグメントに応じ

て、様々なタイプの対処が可能です。



Flowspec アクションでは、ルータ設定に応じて、緩和またはその他の行動を選択することが可能です。

8. その他

・より正確な緩和対処を行うために、攻撃を受けた IP/サブネットを自動検出します。
・より正確に緩和を行うために、1.2.3.4./32 のようなサブネットを設定できます。
・特定セグメントベースラインのリセット機能追加
・自動の最大帯域幅の設定に加え、手動で特定セグメントの最大帯域幅を設定する新しいオプションが利用可能です。
・攻撃をベースラインからのトラフィックを誤警報に含めることで、誤検知としてマークすることが可能です。
・ユーザコメントを各攻撃の関連情報に詳細情報として加えることが出来ます。

9. お問い合わせ

バージョンアップにおいて問題が発生した場合や本マニュアルの不明点などにつきましては下記までご連絡ください。

- 連絡先
  オリゾンシステムズ株式会社
  ORIZON Systems Co. LTD.
  東京都新宿区新宿 6-27-56 新宿スクエア 7F
  E-mail：flowmon-sales@orizon.co.jp