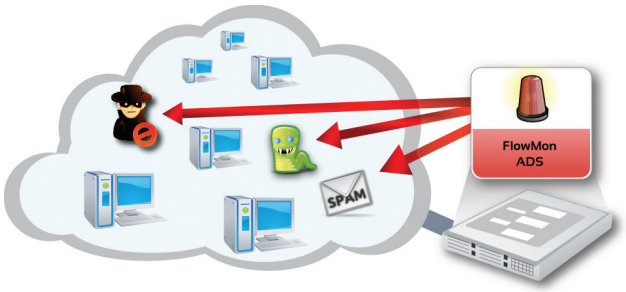
FlowMon ADS

外部と内部の
ネットワークセキュリティ

製品概要

イントロダクション

FlowMon ADS はデータネットワークの異常や好ましくないふるまいについて、継続的なネットワークトラフィックの統計情報（NetFlow データ）に基づいて検出する最新のシステムです。また、FlowMon プローブや FlowMon コレクターの追加プラグインとしても利用可能です。このソリューションの目的は運用上及びセキュリティ上の問題を明らかにし、データネットワークの外部と内部のセキュリティを強化することにあります。ネットワーク機器の一般的なふるまいにしか対処できない標準的なIDSやSNMPモニタリングシステムよりも優れている特徴として、まだ知られていない、あるいはまだシグネチャーができていない特別な脅威に対してもレスポンスが可能という点があげられます。



主な特徴と検出方法

FlowMon ADS のプラグインは効果的な異常検出とネットワーク上での好ましくないふるまいに対して2つの主要なアプローチを提供しています。
まず1つはネットワーク通信のふるまいについてパターン分析をします。
FlowMon ADS は他のシステムとは異なり、パケットペイロードは分析しませんが、送信元及び宛先IPアドレス、ユーザーポート、TCP フラグ、通信時間、その他もろもろのことを分析します。例えばポートスキャニング、辞書攻撃などの攻撃、P2P、匿名サービスなどの好ましくないアプリケーション、ウイルスやスパイウェアに感染したコンピュータその他もろもろの検出が簡単に可能となります。

2つめのアプローチは、継続して取得したプロファイルと照合しながらネットワークホストのふるまいを評価する手法です。これはネットワークふるまい解析（NBA）、ネットワークふるまい異常検知（NBAD）と呼ばれる手法となります。

特徴

- FlowMon プローブとFlowMonコレクターのプラグイン
- 好ましくないふるまいパターン検出のためのルールを事前定義
- 一般的なネットワークの異常検知のためのルールを事前定義
- ネットワークデバイスのサービス、トラフィック量、通信パターンなどのふるまいに関するプロファイルを継続的に取得
- 問題や重要な統計情報を迅速に示す便利で使いやすいダッシュボード
- イベントの早期発見と可視化
- DNS、WHOIS、Geolocationサービスからの情報の統合
- さまざまなレポートやアラートに紐づく多様なフィルタリングオプションやイベントの優先付けが可能
- NetFlow v5/v9 対応、IPv4, IPv6 対応

異常で好ましくないふるまい検知

あらかじめ事前定義されたふるまいパターンやふるまい解析手法に基づいてFlowMon ADS プラグインはコンピュータネットワークにおける下記の異常や好ましくないふるまいを検知します。

攻撃（ポートスキャニング、辞書攻撃、DoS攻撃）

データトラフィックの異常（DNS、マルチキャスト、標準ではない通信）

機器ふるまい異常（継続的に保持されてきた機器ふるまいプロファイルの変更）

好ましくないアプリケーション（P2P、インスタントメッセージ、匿名サービス）

内部のセキュリティ問題（ウイルス、スパイウェア、ボットネット）

メールトラフィック（発信スパム）

運用上の問題（遅延、過重な負荷、DNSの逆引き）

inveaTECH

〒160-0023
新宿区西新宿3−1−5新宿嘉泉ビル8階
ヴイエムネット株式会社

担当：中西　陽一
Tel: 090-9838-5081
info@vmnet.co.jp

FlowMon ADS

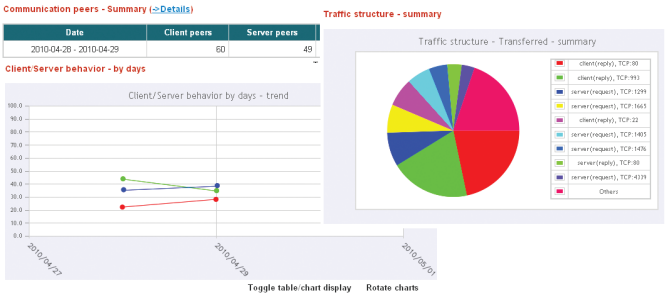
外部と内部の
ネットワークセキュリティ

製品概要

ふるまいプロファイル

ネットワーク上にあるそれぞれのホストのネットワークや通信に関する継続的な統計情報を取得することによって、FlowMon ADS はネットワークやホストのふるまいのどのような変化も見逃さずに監視し、検知することが可能となります。FlowMon ADS によるネットワーク、ホストのふるまいプロファイルは以下のものを含みます。

データトラフィック量（送信データ、接続数）
サービス構造（使用され提供されているサービス）
通信相手
トラフィック構造の全容
ネットワークサーバやクライアントの検索
それぞれの IP アドレスについての詳細なプロファイルとふるまい傾向
ネットワーク上でサービスを提供、使用している機器の検索

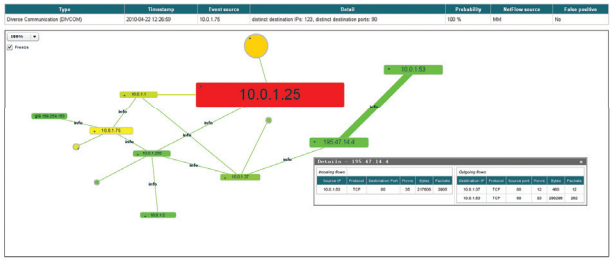


主な利点

- **ネットワークトラフィックの詳細情報と利用上位ユーザの履歴取得**
- **セキュリティガイドラインと規制に対応したコンプライアンス評価**
- **内部や外部からの攻撃の検出**
- **QoSの監視**
- **好ましくないアプリケーションの削除**
- **感染されたネットワーク機器の検出**
- **好ましくないソフトウェア使用や違法なコンテンツ共有の防止**
- **ネットワークトラフィックの制御**
- **ネットワーク、サービス、アプリケーション遅延の迅速な診断**
- **ネットワークやネットワーク機器の誤った設定の検知**

イベントの早期発見と可視化

管理者は好ましくないふるまいのイベントについて詳しい情報を取得することによって、即座に対応することができるようになります。より簡単に早く対応できるようにイベントはグラフで可視化され、ユーザはマウスをクリックするだけでドリルダウンによる原因分析が可能となります。



レポートされたイベントの調査と評価

イベントの原因となったネットワークトラフィックにもとづいてコンパイルされた有向グラフの形式で表示されます。

イベントのチュートリアル

イベントの関連する場所を表示し、ドリルダウンすることで個人のデータ送信レベルまで掘り下げることが可能です。

ネットワークトラフィックの統計情報のエクスポート

原因となったイベントを適切なフォームで抽出･表示します。

展開と拡張性の容易さ

FlowMon ADSは異なった環境でもすぐに展開でき使えるように設計されてます。このシステムは以下のものを含むためとても操作性に優れています。

ネットワークのさまざまなタイプに対応した**代表的なコンフィグレーションのテンプレート**

オンデマンドアプリケーションから生成された**包括的なグラフィックレポート**

E-Mailによる**好ましくないネットワークの状態、状況についての通知**

お問い合わせ先

価格、製品情報などにつきましてはヴイエムネットまでお問い合わせ下さい。

http://www.vmnet.co.jp

inveaTECH

〒160-0023
新宿区西新宿3−1−5新宿嘉泉ビル8階
ヴイエムネット株式会社

担当：中西　陽一
Tel: 090-9838-5081
info@vmnet.co.jp