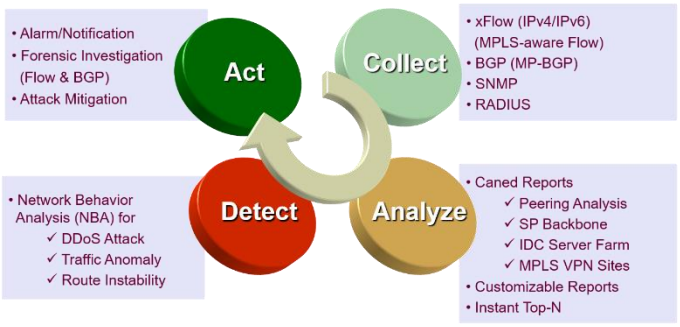
GenieATM™ 6300 シリーズ

An Advanced Traffic Mining System

インテリジェントな機能とハイパフォーマンス性を備えた GenieATM は、ネットワーク全体のトラフィック分析と DDoS 対策のためのトータルソリューションを提供します

急速に拡大する IP ネットワーク環境に対処するために、多くのサービスプロバイダが、ネットワークサービス・オペレーションのための意思決定を効果的にサポートするソリューションを探しています。ピアリングやキャパシティ・プランニングを適切に行うには、SNMP ポーリングだけでなく、フロー情報や BGP ルーティング情報も活用した多角的な分析が必要です。また、猛烈な勢いで増加を続ける悪意のある攻撃によって、サービスやネットワーク・パフォーマンスが深刻な被害を受けていることから、サービスプロバイダの大容量バックボーンを保護するための効果的なセキュリティソリューションも求められていますが、ファイヤウォールや IDS だけでは、大規模なネットワーク環境に十分に対応することはできません。

インテリジェントなネットワーク・モデリング機能と異常トラフィック自動検出エンジンを備えた GenieATM は、サービスプロバイダのネットワーク・セキュリティを強化し、サービスオペレーションにおける意思決定の質的向上を可能にする、最適なトータルソリューションです。



インテリジェント・ネットワーク・トラフィック・モデリング

GenieATM に実装されている「インテリジェント・ネットワーク・トラフィック・モデリング」機能は、多くのプロバイダで採用されている一般的な階層型ネットワーク構造に適用することが可能です。モデリング機能を利用すれば、フロー情報を速く、正確に分類し、受信フローパケットを的確に分析することが可能です。また、事前定義されたいろいろなトラフィック統計レポートを正確に自動生成できます。したがって、ネットワーク管理者はシステムを簡単に運用でき、ネットワーク全体を効率よく、少ない負荷で監視することが可能になります。

異常トラフィック検出と回復

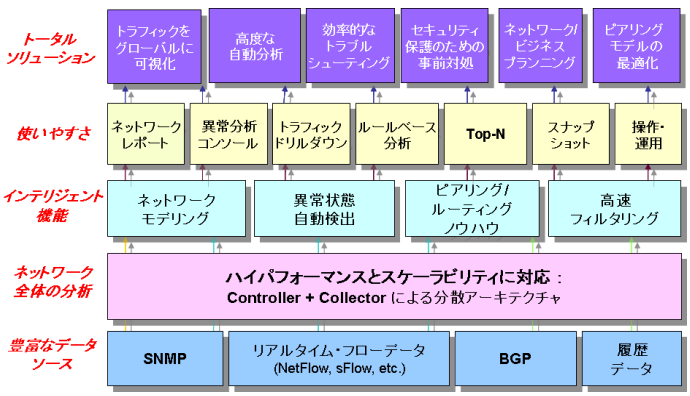
GenieATM の「異常トラフィック検出エンジン」は、ネットワークの内部、外部両方から発生した悪意のあるトラフィックを素早く検出し、疑わしいアタッカーと攻撃された被害者をすぐに特定することができます。そして、これらの異常トラフィックを排除し、状態を回復させるために、適切な「ACL コマンド」をタイムリーに提示します。検出できる異常タイプは、異常トラフィック、プロトコル不正使用、異常アプリケーション、の 3 通りです。「ゼロデイ・アタック」のような異常状態を正しく検出し、アラームとして通知するために、自動トラフィック・ベースラインとダイナミック・スレッシュホールドの設定がサポートされています。

BGP セキュリティ・メカニズム

GenieATM は、隣接 AS の「BGP アップデートメッセージ」を監視することができます。この機能を利用すれば、不正な変更や BGP ハイジャックなどのイベントを検出し、適切なタイミングでアラーム通知を出すことができます。また、監視・収集した統計情報を分析することで、詳細なルーティング管理を行うことも可能です。さらに、GenieATM は、GenieATM システムと BGP ルータ間の通信を不正アタックから保護するために、TCP MD5 シグネチャによる認証機能をサポートしています。

ルールベースのトラフィック分析

GenieATM は、「ネットワーク・トラフィック・モデリング」による自動トラフィック分析のほかに、包括的な「ルールベース」のトラフィック分析メカニズムを提供します。ルールベースのトラフィック分析は、「ファクタ/フィルタ」と呼ばれる項目を自由に設定することで、管理者が特に関心のあるトラフィックに的を絞って詳細に監視、分析することを可能にする機能です。トラフィック分析レポートはユーザが独自に定義できるため、この機能を用いれば複雑なネットワーク環境の変更作業に対するお客さまの多様な要求を完璧に満たすことが可能です。



パワフルなトラフィック・スナップショット

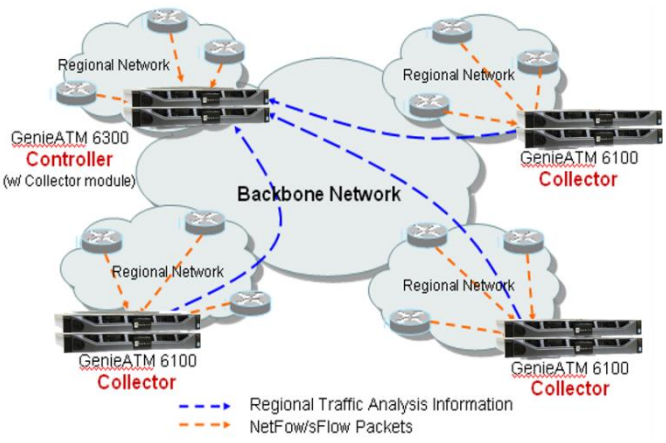
トラフィックの継続的な分析と監視に加えて、キャッシュに保存

Genie Networks Limited

されたデータやディスクに蓄積された履歴生データを用いてトラフィックの短期的特性をリアルタイムに分析する「スナップショット」もユニークな機能です。スナップショット機能は、柔軟なトラブルシューティング・ソリューションとしても有効で、ユーザ定義による豊富な分析基準と、いろいろな分析レポートの重ね合わせ、組み合わせが可能です。さらに、スナップショットを用いれば、異常トラフィックに対して、ステップバイステップで少しずつ対象の範囲を絞り込んでいき、攻撃元を詳細に割り出す、などの運用が可能です。また、異常トラフィック状態を回復させるために、ネットワークオペレータに対して推奨 ACL コマンドを提供します。

分散配置と集中管理

GenieATM は、「分散配置と集中管理」システム・アーキテクチャを通して、大規模なネットワーク全体のトラフィックをハイパフォーマンスで収集し、トータルの運用コスト(TCO)を削減するための一元的なシステム管理、構成管理を可能にしています。GenieATM のコレクタは、拠点ネットワークごとに分散配置され、多様なトラフィック情報(フロー、SNMP ポーリング、BGP メッセージ)をルータ/スイッチから収集し、トラフィックの分類と分析を実行します。分析データは定期的に GenieATM コントローラに転送され、コレクタで分析データの統合と各種表示が行われます。中央に配置されたコントローラは、リモートで稼動するコレクタの構成管理を行い、ネットワーク全体のトラフィックのグローバル表示、不正トラフィックの通知、統合分析レポートの生成などを実行します。



次世代ネットワークへの対応

IPv6 プロトコルがサポートされ、NetFlow / sFlow から出力されるフロー情報に含まれる IPv6 アドレスに関する分析を行うことができるので、次世代 IPv6 ネットワークにおいてもフローベースの高度な運用管理を実現可能にします。

ハイパフォーマンスと容易な運用

GenieATM は、独自 OS を内蔵し、高パフォーマンスと容易な運用・展開を実現しています。日本語対応の GUI により、ユーザは簡単な操作でシステムを運用できます。また、システムへの Web アクセスをサポートしているので、ユーザは Web アクセスが可能な環境であればいつでも、どこからでもネットワーク・トラフィックの状況を監視、分析できます。レポートは、「ネットワーク・モデリング」により事前定義されたトラフィックレポートと、「ルールベース・トラフィック分析」」によるオンデマンドのレポートの両方が利用可能です。また、オフライン・レポート機能により、最新の状況を HTML メールとして定期的に通知することができるので、管理者は装置にログインしていなくてもオフラインで最新レポートを閲覧できます。

内蔵ストレージだけではなく外付けのストレージ接続にも対応し、大容量のデータ保存を可能にします。さらに、豊富なシステム管理ツール、リモート・アップグレード、HA（ハイアベイラビリティ）などにより、システムの運用管理コストをさらに削減させることが可能です。

RADIUS 連携により運用効率がさらにアップ

GenieATM は、RADIUS サーバから出力されるパケットを受け取り、そこに含まれているユーザ名と割当て IP アドレスに関する情報を利用して、装置内部でユーザ名と IP アドレスとのマッピングを自動的に行う機能をサポートしています。この機能を利用することで、通信キャリアや ISP などのネットワーク運用管理者は、ユーザ名をキーにさまざまなトラフィック分析を行うことができ、問題の分析や把握をすばやく行う事ができるようになります。また、ユーザからの問い合わせに迅速かつ的確に答えるのにも大いに役立ちます。

MPLS VPN にも対応 (専用ソフトウェアによる)

GenieATM は、MPLS ルータからのフローを収集し、VPN 拠点ごと、VPN 拠点間、PE ルータ内、PE ルータ間などの通信状況を可視化・分析できるので、MPLS ベースの VPN サービスを提供しているサービスプロバイダにとっては、帯域やパフォーマンス監視によるサービス品質管理、トラブル時の的確な対応、設備計画の最適化など、運用の効率化、コスト削減などの効果が得られます。なお、本機能は v5.6.2 以降は MPLS 専用イメージにてご提供しております。

Genie Networks Limited

製品の特長と利点

アーキテクチャ、運用

■ **独自 OS・アーキテクチャ**: 構成設定やシステム運用、展開が容易です。独自 OS、独自アーキテクチャにて高パフォーマンスを実現します。

■ **運用を止めないで導入、展開が可能**: システムは、データ収集と管理のための IP 接続が可能であれば、どんな環境でも簡単に動作させることが可能です。既存ネットワークの運用を止めたり、変更を加えたりする必要はありません。

■ **高い拡張性**: 2 階層アーキテクチャにおいて、データ収集用のコレクタを追加するだけで簡単に規模の拡大に対応できます。各地に分散配置されたコレクタは、中央に配置された 1 台のコントローラから簡単な操作で管理可能です。

■ **ハイアベイラビリティ (HA)**: GenieATM コントローラは VRRP (Virtual Router Redundancy Protocol) をサポート、2 台のコントローラまたはコレクタで冗長構成をとることにより高信頼性を確保します。

■ **リモートバックアップ**: 各種レポートをリモート・マシン（GenieATM コントローラ）にバックアップすることが可能です。メインのコントローラに障害が発生した場合でも、バックアップ側でレポートが保存されているので、運用の継続性が維持されます。

■ **容易なシステム・アップグレード**: システム・ソフトウェアのアップグレードは、装置にリモートアクセスするか、DOM カードをオンサイトで交換することで簡単に実施可能です。

ユーザ・インタフェース

■ **Web ベース GUI**: システム GUI は、Web ブラウザからネットワーク経由でアクセスし、利用可能です。セキュアなアクセスを確保するため、HTTPS にも対応しています。

■ **多言語サポート**: 言語（画面表示）は日本語、英語、中国語のなかから選択して使用できます。

■ **コマンドライン・インタフェース(CLI)**: 構成変更やアップグレードなどのメインテナンス作業をリモートから実施するため Telnet と SSH をサポートしています。

システム・オペレーション

■ **複数レベルのユーザアカウント管理**: システム操作とレポートへのアクセス管理のために、ページごとに表示・非表示を設定したテンプレートをユーザ毎に適用し、複数レベルのユーザアカウント権限を設定可能とします。また、マルチテナント機能において、サブネット・ユーザレベルでは、自分のトラフィックに関するレポートとコンソールしか見ることができません。

■ **RADIUS、TACACS+サポート**: システムのユーザ名/パスワードによる認証に加えて、リモートの RADIUS サーバまたは TACACS+サーバとの連携による認証にも対応しています。

■ **データベース容量管理**: データベースのストレージ使用量が設定されたしきい値に達した時点で、過去のデータベースは古い順に自動的に削除され、新規データ保存用のスペースが確保されます。

■ **拡張データストレージのサポート**: GenieATM には、出荷時に 1.2TB の SAS HDD が 4 台搭載されています（RAID5 構成）。この内蔵ディスクのほかに、外付けの SAS ディスクアレイ、NFS サーバを追加で接続することも可能です。ただし、拡張ストレージの使用は、お客さまの責任で実施していただく必要があります。（拡張ストレージはサポート対象外です）

■ **システムモニター**: システム稼動状態をチェックするために、CPU 使用率、メモリ使用率、データベース使用率、受信フローレコード統計量を常時モニタすることが可能です。

データソース

■ **フローデータ**: NetFlow™ (v1, v5, v7, v9), sFlow® (v2, v4, v5) がサポートされています。また、NetStream™(v5, v9) にも対応しています。

■ **フロー・フォワーディング**: 受信フローデータを他のフローコレクタに対して中継転送することが可能です。

■ **SNMP ベースのトラフィック監視、分析**: フローベースのトラフィック監視、分析のほかに、SNMP ポーリングによるネットワーク・デバイスのトラフィック監視、分析も可能です。

■ **BGP クライアント・サポート**: 内蔵 BGP モジュールは BGP クライアントをサポートしているので、BGP ルーティング情報を収集することが可能です。また、セキュアな BGP 通信の安全性を確保するため、MD5 シグネチャにも対応しています。

トラフィック分析

■ **ネットワーク全体を可視化**: ネットワーク・デバイスとリンクを監視、分析する従来の手法とは異なり、GenieATM はネットワーク全体を可視化、容易に把握するために「トップダウン」管理方式を採用しています。

■ **ネットワーク・トラフィック・モデリング**: 「ネットワーク・トラフィック・モデリング」モジュールを内蔵し、定義済みレポートを自動的に生成することが可能です。簡単なネットワーク・モデルを設定するだけで、すべてのトラフィックが自動的に分類、結合され、必要な関連づけが行われます。

■ **定義済み分析レポート**: システムは、ネットワーク・モデリングによる分析結果として、包括的なトラフィック分析レポートを自動生成します。レポートは、インターネット、隣接ネットワーク、バックボーン、ルータ、インタフェース、サブネットワーク、サーバなど、さまざまな視点の分析結果を表示します。

■ **ルールベース分析レポート**: トラフィック分析に対するあらゆるニーズに対応できる、ファクタ/フィルタを用いたルールベースの分析を通して、より詳細な分析レポートを得ることが可能です。

■ **豊富なレポート形式**: レポートは、ラインチャート、重ね合わせラインチャート、パイチャート形式で、日、週、月、四半期、年

ごとに表示させることができます。また、サマリ、比較、詳細、ブレークダウン、属性タイプなどを指定して表示させることも可能です。

■ **キャパシティ・プランニングとトラフィック・エンジニアリング**: ネットワーク全体のトラフィックやアプリケーションの増減傾向、ユーザの利用状況などを詳細に可視化することで、ユーザはキャパシティ・プランニングやトラフィック・エンジニアリングのための重要で正確な情報を得ることができます。

■ **ピアリングとトランジット管理**: Top-N Origin/Peer AS レポート, AS Path Length 分析、BGP モニタリングなどの可視化機能を利用して AS 間、隣接 AS とのトラフィックの関係を見ることができます。これらの情報から、ピアリングやトランジットの最適な管理を行うことが可能になります。

■ **ルーティング管理**: AS Path Length, Peer/Origin ASN, BGP メッセージ統計量など、BGP ルーティングに関する情報を分析することにより、ルーティングの最適化（計画）を実施することができます。

■ **ルータ監視**: 重要なルータを SNMP ベースで監視し、CPU やメモリ使用率などデバイスの動作状況に関するレポートや、SNMP と Flow の比較、インタフェースごとのトラフィック、廃棄パケット数、CRC エラーなどの統計情報も収集できます。

■ **トラフィック・スナップショット**:「トラフィック・スナップショット」はトラブルシューティングのための有効なツールです。スナップショットを利用すれば、システムキャッシュに保存された情報や、履歴生データをリアルタイムに細かく分析することが可能になります。インテリジェントな「ドリルダウン」分析により、問題の原因箇所をピンポイントで特定することができます。また、異常状態から回復させるための推奨「ACL コマンド」を自動的に提供します。

■ **生フローデータの分析**: 収集したフローの生データを蓄積し、蓄積された過去の生データを基にスナップショット分析を行うなど、ルールベース分析レポートにより様々な観点からのトラフィックレポートの再構成が可能になります。

■ **マルチテナント機能**:複数の管理者が 1 台の GenieATM にアクセスして、それぞれ個別のサブネットワークを監視、分析するための機能です。これを利用すれば、複数顧客（企業）向けのマネージド・サービスの提供、運用を簡単に実現できます。

■ **RADIUS 連携**: RADIUS サーバとの連携により、ユーザ名と割り当て IP アドレスとのマッピングが自動的に行われるので、ユーザ名をキーにさまざまなトラフィック分析、スナップショット分析が可能です。

■ **MPLS 対応（専用ソフトウェアによる）**: MPLS-aware なフロー(v9)をサポートし、MP-BGP プロトコルに対応しているので、MPLS ルータからのフローを収集し、VPN 拠点ごと、VPN 拠点間、PE ルータ内、PE ルータ間などの通信状況を可視化・分析できます（VPN トラフィック分布, PE トラフィック分布, PE/VPN サイト間トラフィック (From/To), PE 間トラフィック・マトリックス, VPN サイト間トラフィック・マトリックス, など）。

■ **サーバファームや国別の分析**: サーバファームを定義して、特定のファームにおけるトラフィック量の推移やファームの比較、サーバ単位の通信状況の詳細なども、ワンクリックで見ることが可能です。また、IP アドレスと国のマッピングテーブルが標準でサポートされているので、トラフィックを国別に分析することも簡単に行えます。

■ **オフライン・レポート**: 最新の状況を HTML メールとして定期的に通知することができるので、管理者は、装置にログインしていなくてもオフラインで最新レポートを閲覧できます。

異常検出

■ **トラフィックベースの検出**: 定常トラフィックを示すベースラインはダイナミックに設定され、異常状態を検出するためにリアルタイムトラフィックと比較されます。ベースラインをダイナミックに設定し、ネットワーク・トラフィックの挙動をより正確に把握することで、シグネチャのアップデートを待つことなく「ゼロデイ・アタック」の検出を可能にします。「フローベース」のベースラインはネットワーク全体における異常トラフィック検出に、「SNMP ベース」のベースラインはインタフェースごとの異常トラフィック検出に用いられます。

■ **シグネチャベースの検出**: MS Blaster, Sasser, Code Red, SQL Slammer, ダーク IP など、アプリケーションレベルの異常検出のために、フローベースのシグネチャがデフォルトで設定されています。シグネチャはユーザが追加定義することも可能です。

■ **プロトコル不正使用の検出**: 標準のプロトコル使用方法との差異を検出することで、ICMP-Misuse, IP Protocol Null, TCP Flag Null, TCP/UDP fragmentation, TCP SYN Flood, Land Attack などの攻撃を早期検出することができます。

■ **BGP ベースの検出**: 「BGP アップデートメッセージ異常」と「BGP ハイジャック」がシステムにより監視され、ルーティングに異常な挙動が検出されると、タイムリーにアラート通知を行います。

■ **異常トレースバック**: 異常が検出されると、詳細情報を含む「異常レポート」が自動的に生成され、タイムリーなトレースバックに用いられます。したがって、ユーザは非常に効率のよい方法で異常問題を検知することができます。

■ **異常からの回復**: 異常状態から回復させるアクションをタイムリーにとるために、適切な推奨「ALC コマンド」が自動的に生成されます。

■ **アラーム通知**: 「リソース重要度」と「2 段階しきい値」を連動させることで、フレキシブルなアラーム通知をあげることが可能です。通知方法は、管理コンソール(GUI)に表示、特定のユーザグループに Email を送信、ネットワーク管理システムに SNMP トラップを送信、Syslog に通知、などが利用できます。

主要機能

インターネット・トラフィック分析

ネットワーク・トポロジに従ってインターネット境界を定義すれば、インターネット・トラフィック・モデリング機能により入出力インターネット・トラフィックが自動的に分類され、サマリ、ブレークダウン、属性レポートなど多様な分析レポートが自動的に生成されます。サマリ・レポートはホームネットワークの入力、出力などインターネット・トラフィックの流量を収集・計測し、レポートを生成します。ブレークダウン・レポートは、各サブネットワークから出力される、または各サブネットワークへ入力されるインターネット・トラフィックや、他の AS から受信したインターネット・トラフィックなど、特定のトラフィックに関する分析レポートを生成します。属性レポートは、アプリケーション、プロトコル、ポート番号など特定の属性のみに着目した分析レポートを生成します。

隣接 AS トラフィック分析

ネットワーク・トポロジにしたがって隣接 AS 境界を定義すれば、隣接 AS トラフィック・モデリング機能により隣接 AS とホームネットワークとの間でやりとりされる入出力トラフィックが自動的に分類され、サマリ、ブレークダウン、属性レポートなど多様な分析レポートが自動的に生成されます。サマリ・レポートはホームネットワークと各隣接 AS 間のトラフィックの比較など詳細分析を行います。ブレークダウン・レポートは、着目する隣接 AS において、各サブネットワークや隣接 AS との間でやりとりされる入出力トラフィックや BGP メッセージ・トラフィックなど特定のトラフィックに関する詳細分析を行い、レポートを生成します。属性レポートは、アプリケーション、プロトコル、ポート番号など特定の属性のみに着目した分析レポートを生成します。

バックボーン・トラフィック分析

ネットワーク・トポロジにしたがってバックボーン境界を定義すれば、バックボーン・トラフィック・モデリング機能によりバックボーン・トラフィックが自動的に分類され、サマリ、コアルータ・レポートなどの分析レポートが自動的に生成されます。サマリ・レポートは Home to Home (オンネット・トラフィック)と Internet to Home（バックボーンを通してインターネットからホームへ流れるトラフィック、オフネット・トラフィックとも呼ばれる）を含むバックボーンネットワークの入力、出力トラフィックの分析レポートを生成します。コアルータ・レポートは各コアルータのサマリと特定のコアルータに関するトラフィックの詳細情報レポートを自動的に生成します。

ルータ・トラフィック分析

ルータ・トラフィック分析は、システムが対象とするすべてのルータに関するトラフィックに着目した監視、分析を行います。対象ルータをシステムで定義するだけで、ルータ監視機能が自動的に実行されます。ルータ・トラフィック分析は、ルータの使用率だけでなく、各ルータのインタフェースにおけるデータリンク・レイヤーのトラフィックの比較、分析も行います。

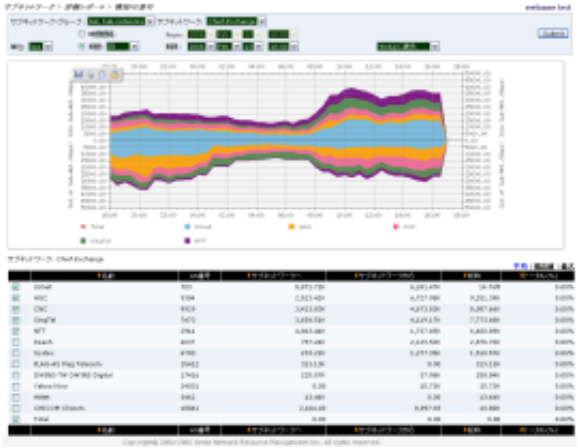
インタフェース・トラフィック分析

インタフェース・トラフィック分析では、登録された各インタフェースのトラフィック比較、特定インタフェースのフローおよび SNMP でのトラフィックレポートなどがレポートされます。また、各インタフェースで、どの IP アドレスが最も多くのトラフィックをやりとりしたかを示す「トップトーカー・レポート」も出力されます。属性レポートとして各インタフェースのアプリケーション、プロトコル、ポート番号、ToS、パケットサイズ毎のトラフィックレポートも出力されます。各インタフェースについて NetFlow / sFlow で見た場合のトラフィックと SNMP で見た場合のトラフィックが同一のグラフ上に描画されるため、NetFlow / sFlow 関係の設定ミスなどを容易に発見することができます。

Genie Networks Limited

サブネットワーク・トラフィック分析

ネットワーク・トポロジにしたがってサブネットワーク境界を定義すれば、サブネットワーク・トラフィック・モデリング機能によりサブネットワークの入出力トラフィックが自動的に分類されサマリ、ブレークダウン、属性レポートなどの分析レポートが自動的に生成されます。サマリ・レポートでは、各サブネットワーク・トラフィックの総量の比較分析、ホームネットワーク、インターネットから特定のサブネットワークへのトラフィックなどの詳細分析を行います。ブレークダウン・レポートは、特定のサブネットワークと各サブネットワーク、すなわち他の隣接 AS との間でやりとりされるトラフィックを詳細に分析します。属性レポートは、アプリケーション、プロトコル、ポート番号など特定の属性のみに着目した分析レポートを生成します。

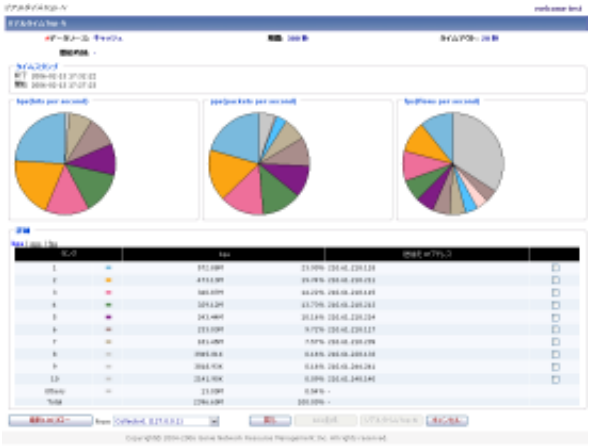


ルールベース・トラフィック分析

上記のような「ネットワーク・トラフィック・モデリング」によって生成される定義済みレポートのほかに、GenieATM は、個別の要求を満たす、ユーザ独自の詳細なトラフィック分析も行うことができます。この分析方法は、「ルールベース」と呼ばれ、フィルタ、ファクタとよばれるパラメータを組み合わせて「ルール」として定義することで実行されます。ルールベース分析を使用すれば、「Permit」「Deny」などの論理演算を組み合わせた細かいルールに基づき、特定のフローデータのみに着目した監視、詳細分析、レポート生成が可能です。

スナップショット

「スナップショット」は、特定のネットワークエリアにおける、ある時点のトラフィック状態を分析、表示する機能です。 TOP-N スナップショット・レポートにより、トラフィックの詳細情報が表形式のリストと円グラフで表示されます。分析の基準となる項目として、[IP アドレス（ブロック）], [プロトコル+ポート], [インタフェース], [ピア AS], [Origin AS], [BGP Community], [TCP Flag], [TOS 値] などのパラメータと、対象トラフィックの範囲を指定することができます。Top-N レポートでは、上記で指定した範囲、項目におけるトラフィック量(bps)、パケット(pps)、セッション(fps)の上位ランキングが表示されます。管理者は、ネットワーク・トラフィックの上位ランキングをリアルタイムに分析することで、直近の情報を把握でき、異常トラフィックに関する発信元、宛先、トラフィック特性などをすばやく検出することが可能です。さらに、条件式を組み合わせて分析範囲をより狭い範囲に絞り込み（ドリルダウン）、細部の詳細状況を正確に把握できるので、トラブルシューティング等で非常に役に立ちます。



異常トラフィック検出

GenieATM は、ネットワーク全体のトラフィック分析だけでなく、DoS/DDoS 攻撃や不正ルーティングなどによる異常トラフィックを正確に検出する機能も提供します。これにより、ネットワーク・サービスが実際にインパクトを受け、停止させられる前にオペレータに迅速な通知を行い、被害の拡散を未然に防止することが可能です。GenieATM では、いくつかの検出モデルが提供されています。「特定トラフィック範囲」に関する異常検出としては、トラフィック異常、プロトコル不正使用、アプリケーション異常を検出できます。 「ネットワーク・デバイス（ルータ）」に関する異常検出としては、インタフェース・トラフィック異常、BGP アップデートメッセージ異常、BGP ハイジャックを検出できます。これらの検出機能を利用すれば、既知、未知にかかわらずネットワークへの攻撃を効率的に検出できるようになります。

- **プロトコル不正使用検出**は、システムで定義されたプロトコル使用ルールとのマッチングをとることにより、プロトコル不正使用や DoS/DDos 攻撃を検出する機能です。
- **アプリケーション異常検出**は、システムで事前定義、またはユーザ定義によるフロー・シグネチャとのマッチングをとることにより、ワームや DoS/DDoS など既知のネットワーク攻撃を検出する機能です。
- **トラフィック異常検出**は、定常ネットワーク・トラフィックに対して、ダイナミックに設定されるトラフィック・ベースラインを基準に攻撃などによる異常トラフィックをタイムリーに検出する機能です。
- **インタフェース・トラフィック異常検出**は、L2 ネットワーク分析に対応した SNMP ポーリングをベースとする検出方法です。インタフェースごとに、スループット、パケット、インタフェース使用率、CRC エラー、パケット廃棄、マルチキャスト/ブロードキャスト率などを計測します。
- **BGP アップデートメッセージ異常検出**は、BGP ルータのアップデートメッセージを分析し、基準を超えたアップデートメッ

セージを検出した時点で異常通知を発行する機能です。

■ **BGP ハイジャック分析検出**は、BGP ルータから送出されるルーティング・アナウンスメントを分析することにより BGP ハイジャックが発生しているかどうかを検査する機能です。BGP ハイジャックが検出されたら、システムはすぐに当該通知を発行します。

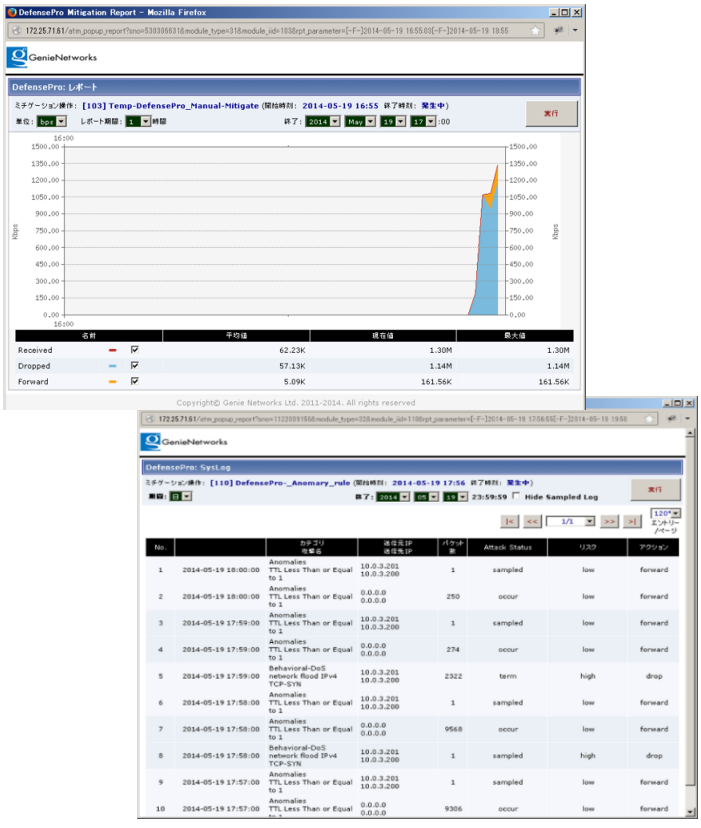
DDoS 攻撃の緩和（Mitigation）

GenieATM は検出した DDoS 攻撃を緩和するための以下の機能をサポートしています。

■ クリーンアップ装置との連携: GenieATM が検出した DDoS に関する情報を、Radware Defense Pro、A10 ThunderTPS といった、いわゆる「トラフィック・クリーンアップ装置」に送ることにより、これらの機器が自動的に攻撃トラフィックのみを廃棄し、正常トラフィックをネットワークに戻してやることができます。
また、上記クリーンアップ装置と連携し、防御対象設定の同期、および Mitigation 結果の GenieATM での表示機能を提供します。

■ FlowSpec によるポリシーベースの Mitigation: BGP FlowSpec (RFC 5575)に基づき、GenieATM がアナウンスした経路情報にしたがって、ルータ（Juniper 等）側でポリシーベースのダイナミックなアクションを実行することで、高度な Mitigation を提供することが可能になります。

■ Blackhole / Sinkhole Routing: GenieATM 単体で BGP の経路情報を操作することにより、不正トラフィックを廃棄（Blackhole Routing）する、または、特定の機器に振り向ける（Sinkhole Routing）などの制御を行うことも可能です。



異常レポート / トレース / 回復

GenieATM は、詳細な異常レポートを生成するだけでなく、攻撃元のトレースバックや検出された異常状態を回復させるためのオペレーションを提示することも可能です。GenieATM は、検出された異常状態を 2 種類のアラーム（異常イベントとアラートイベント）に分類します。異常イベントは、トラフィック・ベースラインにより検出された異常をすべてアラームとしてリストアップします。アラートイベントは、トラフィック・ベースラインにより検出される以外の異常をリストアップします。システムは、ユーザが最新の状況をすぐに把握できるように、検出されたすべての異常情報をステータスサマリとして表形式でコンソールに表示します。

また、スナップショット機能をアラームシステムに組み込むことができるので、異常状態の解析をリアルタイムで行うことが可能です。管理者は、検出された異常に対応するトラフィックを特定し、スナップショット分析を行うことで、異常が起きたときの詳細情報をもれなく見ることができるので、より正確に細かいレベルで異常を把握することができます。
システムは、問題のトラフィックを確認したのち、当該トラフィックを制限するために適切な ACL コマンドを自動的に生成します。これらの機能により、管理者は、必要な情報収集にかかる時間を節約できるとともに、攻撃への対処やダメージからの回復に対するアクションを迅速に行うことが可能になり、セキュリティ監査や障害管理などの観点で、運用性を向上させることができます。

製品の仕様

トラフィック・アグリゲーション
- 積算レポート更新間隔: 5 分
- 異常トラフィック検出測定間隔: 30 秒／1 分

データソース、ネットワーク管理
- 複数コレクタからのトラフィックを収集、集約、分析
- フロー情報: NetFlow(v1,v5,v7,v9), sFlow(v2,v4,v5), IPFIX (over UDP) , NetStream(v5,v9)
- ルーティング: BGP4, BGP(TCP MD5 シグネチャ), MPLS, FlowSpec
- その他プロトコル: IPv4/IPv6, SNMP v1, v2c, v3 GET/TRAP, MIB, 4-byte AS

ユーザ・インタフェース
- 複数言語対応の UI
- 日本語 / 英語 / 中国語（繁体字，簡体字）

トラフィック分析レポート
- タイプ: 標準 / 比較
- 単位: Bits / Packets / Flows (per sec.)
- 期間: 日 / 週 / 月 / 四半期 / 年
- 表示形式: 重畳グラフ / 円グラフ / 表 / Top-N リスト
- エクスポート: HTML / CSV / XML / PDF ファイル / API

ネットワーク・トラフィック・モデリング
- ホームネットワーク、インターネット境界、隣接 AP（SP モデルのみ）、バックボーンリンク、サブネットワーク、サーバファーム、MPLS-VPN に基づくネットワーク・トポロジ・モデルを構成。各モデルにおいて、事前定義されたトラフィックレポートを自動生成（レポートのための特別な設定は必要なし）
- ネットワーク境界の定義: 円形カット / 直線カット
- 事前定義トラフィックレポート: インターネット分析/ 隣接ネットワーク分析/ バックボーン分析/ ルータ分析/ インタフェース分析 / サブネットワーク分析
- 相互分析: 各サブネットワークと隣接ネットワークのトラフィックに関する相互分析が可能
- Top-N 分析: アプリケーション，プトロコル，プロトコル+ポート，TOS 値，パケットサイズごとに Top-N ランキングと比較レポートを生成
- ピアリング分析: 隣接 AS に対するピアリングとトランジット状況を分析
- BGP ルーティング分析: AADIFF / AADUP / TUP / TDOWN / UPDATE メッセージ、AS Path Length 分析に対応。 BGP ルーティングの安定性とパフォーマンスを監視
- ルータ・パフォーマンス分析: CPU / メモリ / インタフェース・トラフィックを監視

マルチテナント設定
- 異常一覧コンソール
- トラフィック分析: 流入 / 流出、サブネットワーク分析 、隣接 AS、Origin AS 分析、トップトーカー分析、属性（アプリケーション、プロトコル、プロトコル/ポート、ToS、パケットサイズ）分析
- スナップショット： 瞬時 Top-N 分析
- プロファイル管理機能

ルールベース・トラフィック分析
- ファクタ: 事前定義またはユーザ定義による設定
- 事前定義: ホーム/ 隣接/ サブネットワーク/ 顧客ネットワーク/ アプリケーション
- ユーザ定義: IP ブロック/ BGP Community/ AS Path/ アプリケーション / RADIUS ユーザ名
- フィルタ: 送信元/宛先 IP, 送信元/宛先 AS Path, 送信元/宛先アプリケーション，ルータ，入出力インタフェース，TOS, TCP Flag, Next Hop, BGP Next Hop，平均パケットサイズ

トラフィック・スナップショット
- 対象トラフィック: ホーム/隣接/サブネットワーク/顧客ネットワーク
- データソース: キャッシュ/ 生データ
- 分析基準: IP, プロトコル+ポート，インタフェース，ピア ASN, Origin ASN, TOS 値, Next Hop, BGP Community, TCP Flag, Time Duration，異常
- アグリゲーション単位: 送信元: IP / プロトコル+ポート / インタフェース / ピア ASN / Origin ASN，宛先: IP / Protocol+Port / Interface / Peer ASN / Origin ASN，方向指定なし: TCP Flag / TOS 値 / Next Hop
- レポート形式: 円グラフ + Top-N リスト（表）
- 異常トラフィックについて段階的にドリルダウン分析できるので、詳細で正確なスナップショット結果を得ることが可能
- 最新 の生フロー（10,000 フローまで） の表示とダウンロード
- Cisco 互換の ACL コマンドを生成

異常トラフィック検出
- トラフィック異常（フロー、SNMP/インタフェース）
- DDoS 攻撃の検知: プロトコル不正使用，アプリケーション異常
- シグネチャ: ユーザによる追加定義も可能
- BGP ベース検出: BGP ハイジャック,スタビリティ,フラッピング
- トラフィック・ベースラインを自動設定
- 過去のトラフィック・ベースライン履歴を確認、リセット可能
- しきい値設定: 固定 & ダイナミック
- 2 段階のアラーム・スレッシュホールド: Red & Yellow
- トラフィック集計単位時間の選択が可能（30 秒, 1 分）

異常、アラート管理用コンソール
- サマリ: 異常サマリをレポート - イベントの統計量，最新（発生中）の異常，最新アラート，システム・ステータス（CPU，メモリ，DB ディスク，フロー，パケット廃棄）
- 異常コンソール: すべての異常をレポート – トラフィック異常，プロトコル不正使用，アプリケーション異常，インタフェース・トラフィック異常
- アラートログ: ログの検索が可能

システム管理
- Web ベース・インタフェース: HTTP と HTTPS に対応
- CLI 管理: Telnet と SSH 暗号化に対応
- 認証: ユーザ名 & パスワード / RADIUS / TACAS+
- ユーザアカウント管理: 複数の権限レベル - 管理者レベル、ユーザレベル（ユーザグループもサポート）
- アラーム通知: Email, SNMP トラップ, Syslog
- ユーザグループ: アラーム通知の配布先をネットワークリソースに応じてユーザグループごとに制御
- 構成管理: Web インタフェースにより変更、バックアップ、リストアを操作。リモートコレクタの操作もひとつのインタフェースで可能。
- ストレージ: 300 GB x 4 内蔵 HDD (RAID 5), 外付け SAS ディスク、NFS も接続可能
- データ管理: レポート/ログの保存期間、ディスクの自動メインテナンスを設定可能
- レポート復元: 期間を指定することにより、過去のトラフィックレポートを復元可能
- リモートバックアップ: 別マシン(GenieATM Controller)にレポートをバックアップ

アプライアンス製品

GenieATM 6300-J (Controller w/Collector)

GenieATM 6100-J (Collector)

フロントパネル

リアパネル

製品ラインアップ/スペック

Model	GenieATM 6371-J 6171-J	GenieATM 6369-J 6169-J	GenieATM 6367-J 6167-J	GenieATM 6365-J 6165-J	GenieATM 6335-J 6135-J	GenieATM 6333-J 6133-J
Flow Capacity (flows/sec)	110,000	90,000	70,000	50,000	30,000	20,000
Routers	100					
Software Version	v5.6.4 or above					
CPU	Intel® Xeon® processor E5-2620v3 x 2 or above					
Memory	32GB (8GB x 4); DDR4-2133					
Hard drives	4x 1.2TB SAS HD 2.5” (10K RPM) as RAID 5 (Optional : Up to 8 as RAID6)					
LAN ports	4x GbE ports, supporting 10/100/1000 BASE - T					
Power supplies	Dual 750W Hot-swap redundant AC power supply; 100-240VAC 50/60 Hz					
Form factor	1U rack, 19”					
Dimensions	H/D/W : 42.8 / 700.5 / 482.3 mm					
Environmental	Operating Temperature : +10° C ~ +35° C (50° F ~ 95° F) Humidity : 10% to 80% Relative Humidity with 26° C (78.8° F) maximum dew point					
Regulatory approvals	cULus Listing Marks (USA/Canada), CE (Europe), CB, FCC Class A (USA) VCCI Class A (Japan), BSMI (Taiwan), CCC (China), KCC (Korea) GOST R (Russia), ICES (Canada), RoHS, BSI					

VA(Virtual Appliance)製品

GenieATM 6300-VM (Controller w/Collector)

GenieATM 6100-VM (Collector)

製品ラインアップ/スペック

Model		GenieATM 6371-VM 6171-VM	GenieATM 6369-VM 6169-VM	GenieATM 6367-VM 6167-VM	GenieATM 6365-VM 6165-VM	GenieATM 6335-VM 6135-VM	GenieATM 6333-VM 6133-VM
Flow Capacity (flows/sec)		110,000	90,000	70,000	50,000	30,000	20,000
Routers		100					
Software Version		v5.6.4 or above					
Requirements	vCPUs	16	16	12	8	4	4
	Memory	16GB	16GB	16GB	16GB	12GB	12GB
	NW Interface	1 to 4					
	Storage	ATM 63xx-VM : per report(DB) and raw data preservation as required					
		ATM 61xx-VM : per raw data preservation as required					

*CPU Recommended : @2.1 GHz or above

*Supported hypervisor : VMWare ESXi 5.x, ESXi 6.0

Genie Networks Limited

Genie Networks 正規代理店

クオリティネット株式会社

東京都新宿区大久保2－1－8 プラザ新大樹4F 〒169-0072
TEL: 03-6380-2980
FAX: 03-6380-2982
Mail: Sales@quality-net.co.jp
https://www.quality-net.co.jp

お問合せ