Progress® Flowmon®

強化されたフローデータでネットワーク運用を変革

ホワイトペーパー

はじめに

世界中の企業でデジタル変革が進んで、接続性と高速データ交換が全面的に普及し、生産性が大幅に向上しました。ネットワークインフラストラクチャはすべての基盤として非常に重要な役割を果たしており、その信頼性とセキュリティを確保することは今日のすべての組織が最優先で取り組むべき課題です。

ネットワークの状況について言えることは、次第に実体が見えにくくなり、「パブリッククラウド」などを利用することで抽象的に理解されるようになってきて、スイッチやルーターの観点から考えたり、ネットワークデバイスを手動で設定したりすることがなくなりつつあるという点です。ネットワーク機器のベンダーはネットワークのシームレス化を進めており、その結果、エンジニアに必要な専門知識は、ドライバーの使い方といったようなことから、数万台の IoT デバイスが接続されたネットワークを保護する方法へと徐々に移行してきています。SDN、NFV、および仮想化はこの傾向と密接に関係しており、企業は、そのリソースを、ネットワークの管理ではなく、コアビジネスに集中させることにシフトしています。こうした状況は、企業ネットワークの帯域幅使用を爆発的に増加させ、ネットワーク監視の従来のアプローチではプリミティブ過ぎて限界に達しているように思われます。プログレスでは、古いアプローチに再考を加えてそこから脱却し、進歩を制限する壁を取り壊すための努力を続けています。

このホワイトペーパーは、将来のパフォーマンスと容量のニーズに合わせて拡張するのに役立つテクノロジーはフローとパケットレベルの可視性を1つの汎用性の高いソリューションに統合することであるという、当社の信念に沿って記述されています。提案するソリューションは、ネットワークトラフィックに関する詳細情報を保持し、分析の結果を直感的にわかりやすい方法で表示することもできます。請求書と最上位統計情報ツールとして認識されることの多いフローデータが、しっかり習得すればフルパケットキャプチャと分析の完全な置き換えとして機能することができ、これまでになかった、将来に備えたスケーラビリティを提供できることをご理解いただけると思います。

従来のアプローチ：パケット解析

従来のアプローチであるパケット解析は、通信の内部を調べてその内容を分析します。集約、圧縮、トリミングは行われず、データは元のサイズで保存されます。したがって、この方法のパフォーマンス要件は非常に厳しく、極めて大量のディスク容量を必要とします。

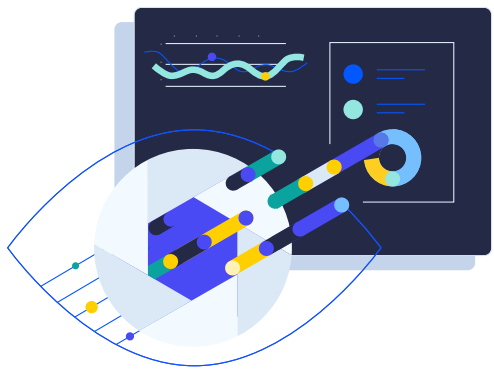
平均 250 Mbps のトラフィックを持つネットワークをキャプチャすることを想像してみてください。これは、1秒あたり 31 MB、1分あたり 1.8 GB、1時間あたり 108 GB、1日あたり 2.6 TB を超えるデータ負荷に相当します。10 Gbps のネットワークであれば、信じられないような数字に達します。単純計算で1日あたり 100 TB 以上のデータが保存されることになります。

パケット解析の問題は、大量のデータを保存する必要があることだけではありません。パケット解析にある主要な制限として、暗号化されたトラフィックの問題があります。暗号化キーがなければ、転送されたデータの内容を理解することはできません。暗号化されたトラフィックは、多くの場合、転送プロトコルやアプリケーションを明らかにしません。にもかかわらず、暗号化されたトラフィックの量は増え続けています。

トラフィックのフルスケールの継続的な記録 (フルパケットキャプチャ) には、適切な技術機器、特に適切な容量の高速ストレージアレイが必要です。ネットワーク監視のためのこのようなアプローチは非常に高価であり、重要なインフラストラクチャと特別な目的を持つネットワークでない限り適切な手法とは言えません。さらに強調すべき点は、データ保存に大容量のストレージが必要だという問題だけには留まらないということです。データはその後の分析と問題解決のために保存されるわけですが、トラブルシューティングのためには大量に保存されたデータから適切な情報を取り出す必要があり、これはかなりの経験とスキルを要します。

ネットワークインシデントの大部分について、高価な継続的なフルパケットキャプチャではない、別のアプローチが採用されることもあります。これはオンデマンドパケットキャプチャと呼ばれるもので、必要な場合にのみオンデマンドでパケットをキャプチャするアプローチです。典型的には、システムの互換性の問題に対処する必要が生じたときであり、また例えば、欠落または破損したパケットが発見されたときなどです。オンデマンドパケットキャプチャは、フルパケットキャプチャに比べて負荷が少なくてすみますが、大きな問題があります。このアプローチの制限は、管理者がどのトラフィックを保存するかを事前に決定する必要があることです。それが何を意味するかというと、インシデントが発生したときに分析のための正しい情報を取得しようとしてもトラフィックアーカイブに到達するオプションがないということです。ネットワーク管理者は、ノートブックを携帯して物理的な場所 (サーバールームなど) に移動し、ノートブックをミラーポートまたはタップに接続して、ネットワークトラフィックの記録を実行するといったことをする必要があります。遠く離れた場所でインシデントが発生する場合も、光ネットワークインタフェースと 10 Gbps インフラストラクチャで問題が発生する可能性もあります。そうなると、これはノートブックではほとんど克服できない制限だと言えます。

パケットをキャプチャする必要性がなくなるわけではありませんが、需要は確実に減少しています。特に、ネットワークに接続されるデバイスの数が増え続けていること、また、より高い帯域幅を必要とするクラウドから配信されるアプリケーションやサービスの数が増加していることにより、明らかなスケーラビリティの問題が存在します。フルパケットキャプチャを行って分析するパケット解析ソリューションはリソースを極めて大量に消費するため、高価になります。また、高速ネットワーク環境にはテクノロジー上の制約があり、トラフィックが暗号化されている場合には使用の可能性が制限されます。



ネットワーク監視の新しいアプローチ：強化されたフローデータ

ネットワークトラフィックの監視、トラブルシューティング、脅威の検出などを行いたい場合、利用できる2つのオプションがあることに思い至るネットワークエンジニアは、あまり多くないようです。1つ目はフルパケットキャプチャと分析で、ネットワークを完全に可視化します。2つ目として、フローデータを使用するオプションがあります。

フローデータは、ネットワークトラフィック自体を抽象化したものと言えます。フロー統計は、ネットワークトラフィックの集約として作成されるものです。個々のフローレコードを識別する属性として、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル番号を使用します。通信内容は保存されず、実現可能な集約率は約 500:1 です。これらの属性情報を使用して、トラフィック構造を分析したり、大量のデータを転送するエンドステーションを特定したり、ネットワーク問題や間違った設定のトラブルシューティングを行ったりすることができます。フローデータでネットワークインシデントの 80% に対応できると、Gartner は 2013 年以来報告しています。

ある種のタスクに対してはフローデータに含まれる情報だけでは十分ではないことは明らかです。対照的に、パケット解析では管理しきれないほどの量の詳細データが結果として得られ、IT 部門は過負荷問題に悩まされることになります。両方の視点を組み合わせ、従来のフローデータをアプリケーション層からの情報で拡張すれば、適切な詳細情報が得られ、データ通信に関する洞察、柔軟なレポート、運用上の問題の効果的なトラブルシューティング、セキュリティインシデントの自動検出などを提供することができます。このアプローチは、IPFIX プロトコルの柔軟性を活用した、強化されたフローデータと呼ばれます。当社の経験した数値として、フローデータに基づいた最もスケーラブルでコスト効率が高く使いやすいソリューション、Progress® Flowmon®、を使用して、ネットワークインシデントの 95% を処理できるようになりました。

このテクノロジーの最もよく知られた実装は、Cisco の NBAR2 (Next Generation Network-Based Application Recognition) です。フローデータの監視は、アプリケーションまたはアプリケーションプロトコルの名前を使用してトラフィック統計を拡張する継続的なパケット解析と組み合わされます。最新のフローコレクターは、この情報に基づいてトラフィックレポートと分析を行います。

最も普及している通信プロトコルの1つは、HTTP、またはその暗号化バージョンの HTTPS です。現在、Web サイトへのアクセスを提供するために使用されていますが、それは唯一の機能ではありません。このプロトコルは、ビジネスシステムのコンポーネント間、または機密データを扱うアプリケーション (電子バンキングなど) 間の通信の基礎でもあります。この転送プロトコル

強化されたフローデータを使用すると、ネットワークインシデントの95%を、最も拡張性が高く、コスト効率が高く、使いやすい方法で処理できます。

を識別することで、基本的な HTTP リクエスト属性 (ホスト名または URL 情報) によってフローデータ統計を拡張できます。HTTPS プロトコルが使用されている場合でも、SNI (Server Name Indication) でホスト名情報を取得できます。同様に、HTTP 通信から他の情報 (例えば、オペレーティングシステムとそのバージョン、ブラウザとそのバージョン、携帯電話の場合はデバイスの種類の識別) を取得できます。これは、手動のデータマイニングを必要とせずに L7 情報を使用できる多くのプロトコルのうちの1つの例にすぎません。

さらに、フローデータは、現代世界でより強力なネットワークパフォーマンス監視 (Network Performance Monitoring、NPM) によって強化することができます。NPM メトリクスは、ネットワークパフォーマンスのトラブルシューティングに非常に役立ちます。サーバー応答時間とラウンドトリップ時間のメトリクスを使用すると、ネットワークインフラストラクチャの遅延 (アクセスポイントの故障など) とサーバーの遅延 (ハードウェアリソースの不足など) を区別できます。ネットワークのトラブルシューティングを迅速に行うためには、この種の情報が非常に重要です。VoIP 通話やビデオ会議を使用している場合は特に、音声とビデオの品質不良が発生していないかを監視するのに、遅延とジッタのメトリクスが有用です。大量のデータ転送が行われているときは、物理層の問題 (干渉、ポートの障害など) を示す可能性がある TCP 再送信の回数に注意を払い、ビットレートの低下や、通信リンクの障害を示す可能性があるパケットの順序の乱れにも着目します。

こうしたレベルの情報ではまだ不十分な場合、Flowmon はフルパケットキャプチャをオンデマンドでトリガーできます。検出されたイベントに対して手動または自動で実行できます。フルパケットキャプチャがトリガーされたら、キャプチャのフィルタは、キャプチャされるデータ量を絶対最小値に絞り込み、トラフィックの関連部分のみを保持するよう、システムによって自律的に決定されます。これは、ネットワークのどの部分であっても、100 Gbps の速度でリモートで実行できますが、Wireshark や WinPCAP では達成できません。

フローデータの監視とアプリケーション層分析の利点は明らかです。データ通信に関するより詳細な情報が得られ、より優れたトラフィック分析機能を提供できます。同時に、元のトラフィック量に対するネットワークトラフィック統計の優れた圧縮率を維持し、複数の100ギガビットネットワークに拡張できます。また、システムは最も重要な情報を集約するので、パケット解析で手動のデータマイニングを行わなくても、一目でわかるよう情報を配信できます。したがって、それほど高いスキルがなくてもソリューションを使用でき、平均解決時間の大幅な短縮が可能になります。Flowmon を使用すると、同じプラットフォームを使用しながら、必要に応じていつでもフルスケールのトラフィックデータの記録を実行できます。

Flowmon は、必要に応じてオンデマンドでフルパケットキャプチャをトリガーすることもできます。キャプチャのフィルタは、キャプチャされるデータ量を絶対最小値に絞り込み、トラフィックの関連部分のみを保持するよう、システムによって自律的に決定されます。

パケット解析より、強化されたフローデータ ビジネス上のメリットと技術的なメリット

このホワイトペーパーの前半では、ネットワークトラフィック監視に使用するテクノロジーとしての、継続的なフルパケットキャプチャを行うパケット解析と強化されたフローデータについて説明しました。ここで、強化されたフローデータを使用することのメリットをまとめておきます。

- パケット解析テクノロジーはリソースを消費し過ぎて高価になるため、ネットワークトラフィック全体の監視が可能になることはめったになく、最重要システムを監視するためにのみ導入される傾向があります。一方、フローデータの場合は、データセンターやクラウドを含む企業ネットワークトラフィック全体をカバーすることが標準的です。

- 一般に、トラブルシューティングはリアルタイムで行われることは少なく、報告されたインシデントがネットワーク管理者によって検討されるまでに数日かかることはよくあります。データの保存期間が限られるパケット解析では遡及的に分析することが困難です。フロー監視では、数週間から数か月分のデータを保存でき、作業に優先順位を付けて、より重要なタスクが完了したらいつでも遡及分析に集中できます。

- シームレスな展開、既存のネットワーク機器との統合、幅広いフローソースとの互換性、管理者の迅速なトレーニングなど、フローテクノロジーはネットワークへの導入が簡単で、すぐに効果が得られます。

- パケット解析によって提供される詳細情報は、永続的な問題の深いフォレンジック分析に適していますが、強化されたフローデータを使うことで、コンテキストを認識した表示ができるわかりやすいダッシュボードとドリルダウン機能を使用して、根本原因分析に必要な時間を最小限に抑えて修復にとりかかれます。

- パケット解析の粒度が細かすぎると、コストが高くなり、スケーラビリティが低下し、使用するためには非常に高度なスキルが必要になります。収集されたデータのうち関連するものはほんのわずかです。一方、強化されたフローデータには、関連性が高く意味のある重要な情報が保存されるので、ネットワークインシデントの 95% が解決できます。残りについては、Flowmon は、必要に応じてオンデマンドのフルパケットキャプチャを有効にできます。

- パケット解析は、無制限の可視性を念頭に置いて構築されたもので、時間のかかる永続的な問題のフォレンジックに適しています。通常の業務を迅速に回復する目的では、分析ワークフローと自動化を提供する Flowmon が注目されています。

- 暗号化されたトラフィックが増えると、パケット解析は役に立たなくなります。Flowmon は、暗号化されたトラフィックからフローデータをエクスポートする際、インシデントの 80% の解決に役立つ暗号化されていない IP ヘッダーに焦点を当てます。さらに、様々な技術を使用してアプリケーション層から情報を抽出します。

- パブリッククラウドプロバイダーは、フルパケット解析を可能にするために自社のネットワークを利用することを許可していません。多くのクラウドプロバイダーや仮想ハイパーバイザーは、Flowmon と互換性のある何らかの形式のフローデータをエクスポートするので、高品質のネットワーク監視のシームレスな展開が可能になります。

具体例

パケットキャプチャを使用したトラブルシューティング

筆者の手元には、継続的なキャプチャを備えたパケットアナライザーがあります。ローリングバッファーに必要なデータがまだ保持されているといいのですが。幸いなことに、IP アドレス 193.29.206.1 のトラフィックを含む PCAP をダウンロードし、Wireshark でトラフィックを開くことができました。

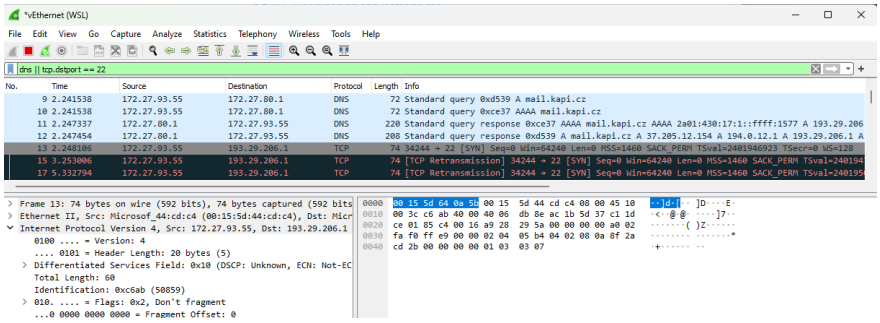


図1: Wireshark でキャプチャされたネットワークトラフィック分析

上の図では、ユーザーと mail.kapi.cz の間の通信がわかります。ドメイン mail.kapi.cz は IP アドレス 193.29.206.1 と正しく解決されましたが、DNS 応答を受信した後、ユーザーが TCP セッションを確立しようとしたところ、外部 IP アドレスからの応答はありませんでした。この通信が許可されているかどうか、ファイアウォールの設定を確認する必要があります。

2番目の問題は、ユーザーマシンによってクエリされた存在しないドメインに関連しています。update.invea.com が存在しないことがわかります。これはおそらく、ネットワーク関連の問題ではなく、ユーザーの設定が間違っていることを意味します。

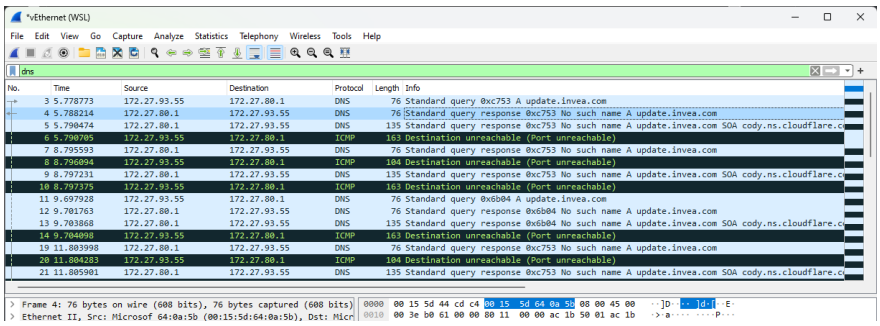


図2: 存在しないドメインを解決するためのホストクエリ

強化されたフローデータを使用したトラブルシューティング

Flowmon Probe が監視ネットワークに導入され、Flowmon Collector に数週間分の非サンプリングおよび非集約トラフィック統計履歴が保存されている場合の例です。ドメイン winatp-gw-weu-microsoft.com について DNS の質問を行います。

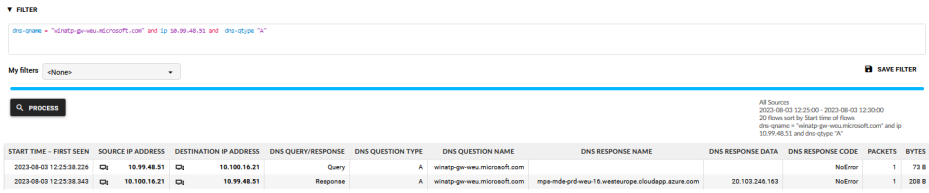


図3: DNS トラフィックのフィルタリング - DNS 情報で強化されたフロー統計

DNS サーバーから応答として提供された IP アドレスを確認し、その IP アドレスに向かうトラフィックを簡単に確認できます。これが可能になるのは、DNS に対応する Flowmon Probe からのフローが、DNS プロトコルからの最も重要な L7 情報で強化されているためです。

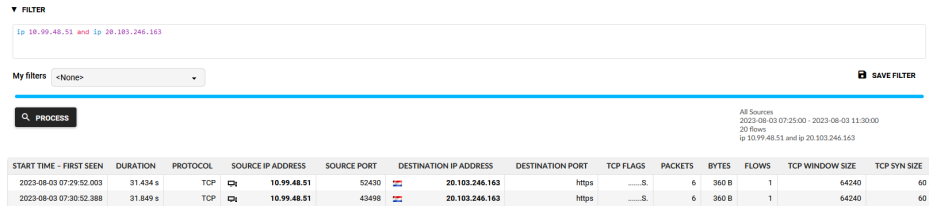


図4: ユーザーと外部サービスとの通信のフィルタリング。ホストは応答を受信していません。

上の図では、SYN パケットのみがネットワークに送信されており、外部 IP アドレスからの応答がありません。これは、ファイアウォールのルールを確認する必要があることを意味します。一般的な L3/L4 情報に加えて、デフォルトの TCP Window size などの TCP 固有の項目も把握できるので、TCP セッションのトラブルシューティングに役立ちます。

存在しないドメインはフローデータでも確認できます。ドメイン flowmonos が存在しないことが、DNS サーバーの「NXDomain」という応答でわかります。

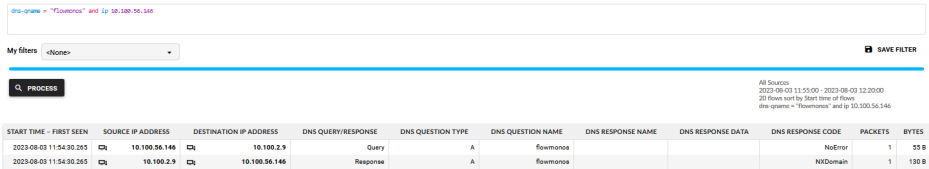


図5: DNS トラフィックのフィルタリング – NXDomain DNS 応答コード

導入事例:
根本原因調査のワークフロー

5万人をかかえる、ある銀行の IT 部門には上級のエンジニアが所属して、他のチームでは解決できないネットワークインシデントの根本原因分析に重点を置いて業務を行っています。例えば、異なる大陸にある顧客と銀行の間の VPN 接続が停止した理由の解明などを行います。IT 部門では、複雑で異種環境の何百もの異なるシステムによって生成されたペタバイト規模のデータを何時間もかけて Wireshark で調査しなければならない、といったことがよく起こります。非常に負荷が大きいため、運用上のインシデントに対処するための、より効果的なソリューションを探すことになりました。

この IT 部門では、実はネットワーク運用タスクを支援するプラットフォーム全体を自社で構築していました。そのプラットフォームは、継続的なパケットキャプチャ用の商用ツール、フロー監視用にカスタマイズされたオープンソースソフトウェア、およびデータ転送ヒートマップをリアルタイムで表示する SNMP ベースのツールに基づいていました。

この自社開発ソリューションを、日常業務に合わせて、維持、サポート、アップグレードするには、費用と時間がかかりすぎることが判明し、自社ソリューションに代わる NetFlow/IPFIX テクノロジーを模索し始めました。現在のソリューションを、NetFlow/IPFIX テクノロジーを使用するソリューションで完全に置き換えることを念頭に置いていました。予算は問題ではなかったものの、その選択は当初思ったほど簡単ではありませんでした。様々なベンダーをテストしてみましたが、データの集約が問題になることもあれば、仮想化ができないこともありました。測定結果の提供に必要な時間の遅さは、どのテストでも問題になりました。

希望する理想的なソリューションは、以下のニーズを満たす必要がありました。

- コンテキストを認識したトップレベルのダッシュボードだけでなく、任意のフローへの手動ドリルダウンを可能にするダッシュボードも提供
- 保存されたデータを集約せず、ストレージが続く限り生のフローを保持
- 単一のテクノロジーに固定できない異種環境に対応できるよう、独自センサーに依存しない
- 管理と移行が柔軟で仮想化が可能
- フロー監視とオンデマンドのフルパケットキャプチャの組み合わせ
- 最も重要な点として、10年前にオープンソースツールから自社で構築したプラットフォームよりも速く、フローデータの測定された統計情報の出力を提供

最終的に、銀行の IT 部門は、ようやくこれらのニーズを完全に満たす Flowmon を見つけました。概念実証プロジェクトを実施し、それ以来、Flowmon は IT 部門で使用するツールセットの基礎となり、根本原因調査のワークフローそのものになっています。エンジニアたちは現在、まずダッシュボードをチェックし、トップレベルの統計を調べ、NetFlow のレベルへとさらに深く分析していきます。フルパケットキャプチャを実行するのはトラフィックのごく一部です。

「Flowmon は、ネットワーク内のデータフローメトリクスを提供し、ネットワークの状況が簡単にチェックできます。問題が発生した場合、問題の原因となっているトラフィックを視覚化できるこのツールを使用して、非常に迅速かつ効率的なトラブルシューティングが可能になります。」

Marc Deamen 氏、
KBC 上級システムエンジニア

おわりに

今日のネットワークのダイナミクスと多様性は、ネットワーク監視アプローチに課題をつきつけ、再考を促しています。ネットワークの高速化、クラウドへの移行によって生じる可視性のギャップ、IoT、ソフトウェアデファインドネットワークといった変化に直面して、パケットキャプチャソリューションでは、期待通りの結果を迅速かつ手頃な価格で提供することが難しくなっています。

パケットキャプチャソリューションは、今日のネットワーク環境のダイナミクスが想定されていない時代に設計されました。現在では、特定の限られた使用例ではうまく機能しますが、ネットワークエンジニアが直面する日常的な使用例のほとんどでは、フローデータの柔軟性、拡張性、使いやすさにはかないません。

このホワイトペーパーでは、強化されたフローデータがフルパケットキャプチャとパケット解析に対して同程度に強力であることを示しました。一方で、フローレベルの可視性が拡張されたとしても、依然として PCAP (Packet CAPture、パケットキャプチャ) の分析が避けられない問題がなくなることはないでしょう。

当社は、将来のパフォーマンスと容量のニーズに合わせて拡張するのに役立つテクノロジーはフローとパケットレベルの可視性を1つの汎用性の高いソリューションに統合することであると信じています。継続的なフロー監視を行い、必要に応じてパケットキャプチャを実行するのが最善策です。最終的には PCAP が必要なケースはそれほど多くないとわかるはずです。Flowmon の導入を是非ご検討ください。

Flowmon の詳細については、以下のページをご参照ください。
www.flowmon.com/jp

プログレスについて

プログレス (Nasdaq：PRGS) は、テクノロジーが牽引する世界において専心的にビジネスを推進し、多くの企業がイノベーションのサイクルを加速し、躍進して業績を向上させていくプロセスを支援します。プログレスは信頼できるプロバイダーとして、インパクトが大きいアプリケーションを開発、展開、管理するための最高の製品を提供し、お客様は必要なアプリケーションとエクスペリエンスを開発し、適切な手法で展開し、すべてを安全かつ確実に管理することが可能になります。1,700のソフトウェア会社と350万の開発者を含め何十万もの企業が目標達成のために確信を持ってプログレス製品を利用しています。詳細については www.progress.com をご覧ください。また、LinkedIn、YouTube、Twitter、Facebook、Instagram へのフォローをお願いいたします。

プログレス・ソフトウェア・ジャパン株式会社
〒106-0047
東京都港区南麻布4-11-22 南麻布T&F ビル
www.flowmon.com/jp
sales_japan@progress.com

Progress