

ManageEngine
NetFlow Analyzer

ネットワーク **VS** アプリケーション

NETWORK

APPLICATION

アプリケーションから見る！
トラフィックの監視と制御

目次

従来のネットワークとアプリの監視手法からの脱却.....	2
不適切な帯域幅管理.....	2
ビジネスクリティカルなアプリケーションの優先順位.....	2
動作が遅いホップ.....	3
ネットワークを脅かす攻撃や悪意のあるトラフィック.....	3
アプリケーションから見るトラフィック分析.....	4
より多くの帯域幅を使用しているアプリケーションを特定.....	4
ビジネスに必要なアプリケーションに優先順位を付ける.....	6
WAN 全体の帯域幅のボトルネックを検出.....	7
根本原因を見つけるためのフォレンジック分析.....	8
攻撃や侵入を防ぐ.....	10
NetFlow Analyzer によるアプリケーショントラフィックの制御.....	11

アプリケーションのパフォーマンスを向上させるために、アプリケーションまたはそのホストサーバーを最適化する担当者様は少なくないでしょう。ネットワークは、アプリケーションの提供速度に大きく起因するため、アプリケーション提供に大きな役割を果たします。基盤となるネットワークに問題がある場合やサーバー設定の最適さ、またはアプリケーションの最適さによって、アプリケーションの配信速度は影響されます。

従来のネットワークとアプリの監視手法からの脱却

アプリケーションを最適化するのではなく、ネットワークの観点からアプリケーションのパフォーマンスと配信に関する問題を分析します。ネットワーク管理者は、アプリケーション配信の最適化のため LAN と WAN のトラフィックを可視化し、問題の要因を見つけ改善する必要があります。

不適切な帯域幅管理

アプリケーションやユーザー毎の帯域使用状況の監視と可視化ができないと、ネットワーク管理者は帯域幅が十分であるかどうか、または追加の帯域を契約する必要があるかどうか判断できません。また、追加の帯域を契約したとしても長期的な問題解決にはなりません。最初に帯域を可視化し、ビジネスに必要なアプリケーションとそうではないアプリケーションのどちらがより多くの帯域幅を消費しているかを特定し、それに応じて帯域幅を割り当てる必要があります。

ビジネスクリティカルなアプリケーションの優先順位

ビジネスクリティカルなアプリケーションを優先できている企業は多くありません。その結果、ネットワークはベストエフォート型ですべてのアプリケーションを配信しようとします。このため、ネットワーク輻輳時にすべてのトラフィックがブロックされる可能

■ アプリケーションから見る！トラフィックの監視と制御

性が高くなります。このような問題を回避するには、QoS ポリシーを定義してトラフィックに優先順位を付ける必要があります。

動作が遅いホップ

パケットは複数のホップを通過して利用者に到達します。いずれかのホップに長い待ち時間がかかると、アプリケーションの応答時間が長くなり、利用者から不満があります。このようなクリティカルパスを監視し、待ち時間/パケットロス/ジッタなどを見つける必要があります。

ネットワークを脅かす攻撃や悪意のあるトラフィック

ハッカーはネットワークにジャンクトラフィックを送り、ネットワークとアプリケーションのパフォーマンスを低下させようとします。悪意のあるトラフィックが発生している場合、リアルタイムで識別してブロックできる可能性があるので、ネットワークにアクセスしているトラフィックが正常であるかどうかの監視を実施する必要があります。

アプリケーションから見るトラフィック分析

基本的なネットワーク監視やトラフィック分析は行っているが、それをアプリケーション配信と関連させている企業は多くありません。ネットワークとアプリケーションは異なるレイヤーですが、アプリケーション配信がネットワークに依存していることを再認識する必要があります。ネットワークのパフォーマンス低下やジャンクトラフィックの大量発生は、アプリケーション配信に影響を与えます。そのため、アプリケーションの視点からネットワークトラフィックを分析および制御するのに役立つネットワークトラフィック分析ソフトウェアが必要です。このようなソフトウェアは管理者の課題解決におおいに役立つものと考えられます：

1. より多くの帯域幅を使用しているアプリケーションを特定
2. ビジネスに必要なアプリケーションに優先順位を付ける
3. WAN 全体に広がる帯域のボトルネックを調査
4. 根本原因を見つけるためのフォレンジック分析
5. 攻撃や侵入を防ぐ

より多くの帯域幅を使用しているアプリケーションを特定

SNMP によるトラフィック監視では、インターフェース/ポートを流れるトラフィックの総量を監視することができます。アプリケーションの一覧とその帯域消費率を特定するには、より詳細な監視が必要です。

■ アプリケーションから見る！トラフィックの監視と制御

ルーターやスイッチで機能する NetFlow や sFlow などのプロトコルにより生成されるデータを「フローデータ」と呼びます。

フローデータにはトラフィックに関する情報だけでなく、アプリケーションの一覧や各アプリケーションの帯域消費率に関する情報も含まれます。

このフローデータを活用するソフトウェアを「フローコレクター」と呼びますが、

ManageEngine では「NetFlow Analyzer」というフローコレクターを提供しています。

NetFlow Analyzer は、NetFlow や sFlow 等によって生成されるフローデータを受信し見やすい形に整えることで、手軽な帯域分析を支援します。Cisco NBAR などの技術も活用し、ネットワーク経由でアクセスするアプリケーションを識別し、アプリケーションとそれらが消費する帯域幅に関する詳細な情報を提供します。これにより、ビジネスクリティカルなアプリケーションと非ビジネスクリティカルなアプリケーションが帯域の何パーセントを使用しているかを正確に把握できます。また、最も帯域を消費しているデバイスやユーザーを見つけるのにも役立ちます。



■ アプリケーションから見る！トラフィックの監視と制御



The screenshot shows the NetFlow Analyzer web interface. The top navigation bar includes tabs for Dashboard, Inventory, Alerts, Maps, Reports, Settings, OPM, NFA, NFA Manual, IP SLA, WLC, and Attacks. The main content area is titled 'wan1' and shows a table of application traffic. The table has columns for Application, Traffic, and Percentage. The applications listed include https, http, Unknown_App, ssh, microsoft-ds, stun, domain, imaps, syslog, mysql, cvspserv, hpvrtg, ms-wbt-server, plethora, pop3s, and smtp. The traffic values range from 1.297 TB for https down to 34.389 MB for smtp. The percentage values range from 75% for https down to 0% for most other applications.

アプリケーション	トラフィック	割合
https	1.297 TB	75 %
http	403.322 GB	23 %
Unknown_App	8.289 GB	0 %
ssh	7.442 GB	0 %
microsoft-ds	4.518 GB	0 %
stun	3.283 GB	0 %
domain	1.874 GB	0 %
imaps	1.336 GB	0 %
syslog	1.128 GB	0 %
mysql	972.787 MB	0 %
cvspserv	904.295 MB	0 %
hpvrtg	847.073 MB	0 %
ms-wbt-server	792.502 MB	0 %
plethora	488.487 MB	0 %
pop3s	171.670 MB	0 %
smtp	34.389 MB	0 %

ビジネスに必要なアプリケーションに優先順位を付ける

QoS ポリシーは、アプリケーションがどのように帯域幅（高優先度、ベストエフォート、スカベンジャークラス）を優先するかを定義します。組織で使用されているビジネスクリティカルなアプリケーション、または利用者に提供されるアプリケーションやリアルタイム性を求められる音声/ビデオ通信のほとんどは、「最優先」に該当します。それほど重要ではないその他のアプリケーションは、ベストエフォートとして定義されます。例えば、Facebook、Twitter などのソーシャルアプリケーションはスカベンジャークラス（くず拾い）に定義されるべきです。優先順位が設定されていない場合、ネットワークはすべてのアプリケーションを配信するためにベストエフォート型のアプローチを取ります。その結果、ビジネスクリティカルなアプリケーションと非ビジネスクリティカルなアプリケーションの両方が同じ優先順位で提供されます。

■ アプリケーションから見る！トラフィックの監視と制御

ここで QoS ポリシーが役立ちます。ビジネスクリティカルなアプリケーションの帯域利用を優先し、帯域を効率的に利用します。NetFlow Analyzer を使用すると、QoS ポリシーの監視および検証ができ、QoS ポリシー設定の前後を比較するのにも役立ちます。

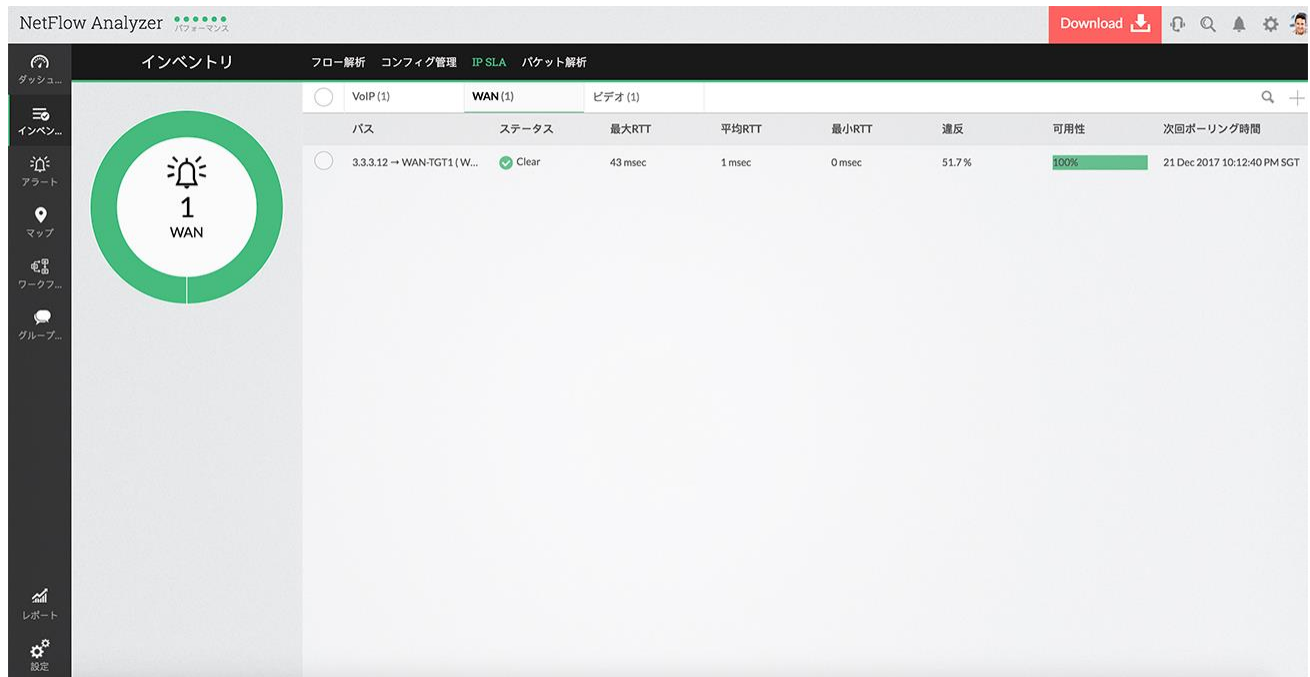
最新1時間		装置 (12)	インターフェース (15)	グループ (10)	アプリ (148)	QoS (32)		
11 装置	15 インターフェイス	名前		トラフィック		パーセント		
		Default		2,430 MB		60%		
		000011		1,069 MB		26%		
		010001		19,785 KB		0%		
		AF31		19,636 KB		0%		
		CS1		19,554 KB		0%		
		001101		19,409 KB		0%		
		AF11		19,288 KB		0%		
		AF13		19,240 KB		0%		
		011011		19,056 KB		0%		
		AF33		19,056 KB		0%		
		000100		18,819 KB		0%		
		AF12		18,372 KB		0%		

WAN 全体の帯域幅のボトルネックを検出

アプリケーションの利用者とその管理場所は遠く離れていることが多く、利用時に発生するパケットは複数のホップを通過していきます。そのため、利用者がよりスムーズにアプリケーション利用できるように、各ホップでの待ち時間は最小限に抑える必要があります。ただし、各ホップは複数のトラフィック処理やパケット転送、ルーティングなどに時間がかかることがあるため、常に可能とは限りません。このような状態は遅延を増大させ、アプリケーションの配信に影響を及ぼします。

■ アプリケーションから見る！トラフィックの監視と制御

NetFlow Analyzer では、Cisco IP SLA の監視により、テストパケットをシミュレートして、WAN リンクの待ち時間、ジッタ、およびパケットロスレベルを定期観測します。待ち時間、ジッタ、またはパケットロスを事前把握することができ、パフォーマンスデータの分析や問題が大きくなる前に対策を施すことができます。



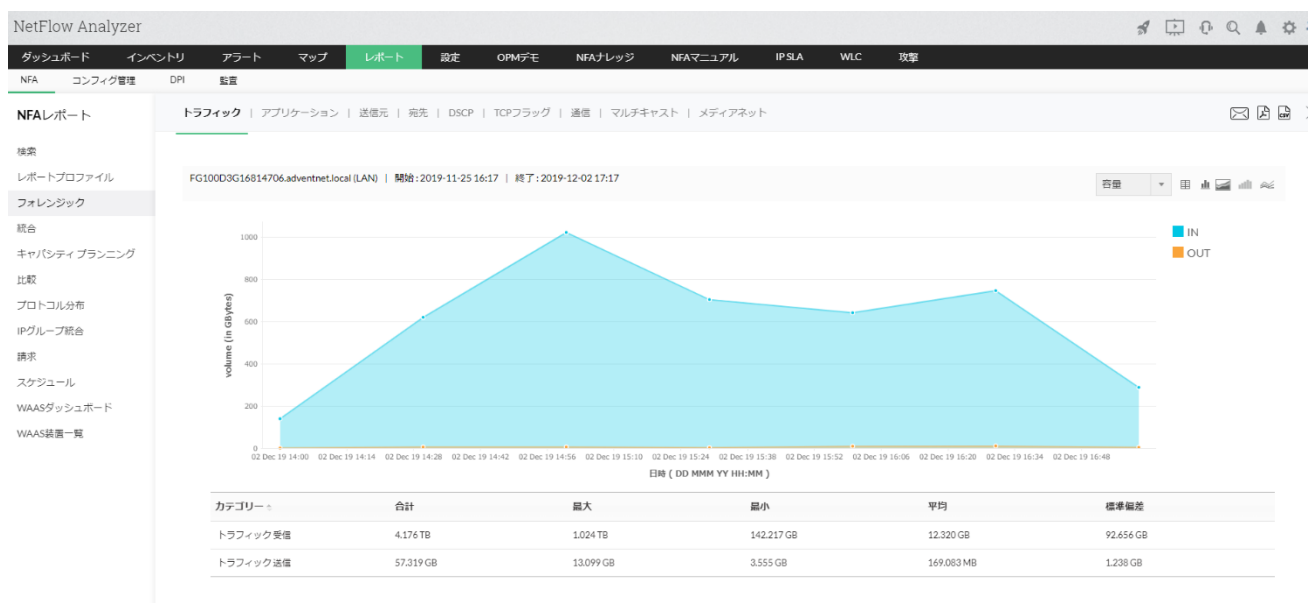
根本原因を見つけるためのフォレンジック分析

問題を迅速に解決することよりも重要なことは、根本的な原因を突き止め再発を防ぐことです。根本原因を見つけるための詳細な分析には膨大な量のデータを分析し、誰が、いつ、何を、そしてなぜ行っていたのかを把握する必要があります。これには広範囲に渡るレポートの生成と入念な分析が必要です。

■ アプリケーションから見る！トラフィックの監視と制御

NetFlow Analyzer は、フォレンジックレポートにより上記のような分析を支援します。この機能では、過去に遡って必要なデータを収集し、レポートを生成します。

NetFlow Analyzer は、トラフィック、アプリケーション、送信元/宛先 IP アドレス、DSCP など、さまざまな切り口でのデータ分析に役立ちます。



NetFlow Analyzer

ダッシュボード インベントリ アラート マップ レポート 設定 OPMデモ NFAナレッジ NFAマニュアル IP SLA WLC 攻撃

NFA コンフィグ管理 DPI 監査

NFAレポート

検索
レポートプロファイル
フォレンジック
統合
キャパシティプランニング
比較
プロトコル分布
IPグループ統合
請求
スケジュール
WAASダッシュボード
WAAS設置一覧

トラフィック | アプリケーション | 送信元 | 宛先 | DSCP | TCPフラグ | 通信 | マルチキャスト | メディアネット

FG100D3G16814706.adventnet.local (LAN) | From: 2019-11-25 16:17 | To: 2019-12-02 17:17

IN OUT

アプリケーション	トラフィック	パケット
https	3.499 TB	9596875137
Unknown_App	264.328 GB	2774893000
ms-wbt-server	118.369 GB	373111447
plethora	99.811 GB	282403000
ms-wbt-server	90.080 GB	120184089
http	31.646 GB	463075830
stun	30.778 GB	91099426
cvspserver	14.889 GB	20108000
m2mservices	12.892 GB	10657000
ssh	11.644 GB	32009237
domain	9.546 GB	105287007
hplrtgpr	8.465 GB	67873012
microsoft-ds	6.410 GB	8549301

アプリケーションから見る！トラフィックの監視と制御

NetFlow Analyzer															
ダッシュボード インベントリ アラート レポート 設定 CPUマップ CPU NFAレポート NFAマニュアル IP SLA WAC 管理															
NFA - コンフィグ管理															
NFAレポート															
トラフィック アプリケーション 送信元 宛先 DSCP TCPフラグ 優先度 マルチキャスト メディアポート															
検索															
レポートファイル															
FG1000G168470t.advernet.local (LAN) From: 2019-12-04 09:58 To: 2019-12-04 10:56															
フィルタリング															
送信元IP 宛先IP アプリケーション 送信元ポート 宛先ポート プロトコル DSCP TCPフラグ フローレート トラフィック パケット 次のホップ FNF NbrApp M(送信元IP) M(宛先IP) M(送信元ポート) M(宛先ポート)															
総合															
チャリシティ・プラザエンタ															
出船															
プロトコル分析															
IPグループ分析															
調査															
スケジュール															
WASAダッシュボード															
WASA拡張一覧															
...															
Page no. 1 50															

攻撃や侵入を防ぐ

ファイアウォールや侵入検知システム(IDS)の導入にもかかわらず、ハッカーの標的になっている企業は少なくありません。どちらのシステムもパケットのヘッダーを読み取りシグネチャ・マッチングを実行しますが、DDoS やゼロデイアタックなどの高度なセキュリティ攻撃には対応していません。

このような背景により、高度な攻撃からネットワークやデータセンターを保護するのに役立つ高度なセキュリティ分析と保護を必要とする企業が増えてきています。

NetFlow Analyzer では、フローデータを分析してネットワークを攻撃する悪意のあるトラフィックを検出する、フローベースのネットワーク動作異常検出(NBAD)機能を提供しています。悪意のあるトラフィックにルールとパターンを適用して、それらが

■ アプリケーションから見る！トラフィックの監視と制御

侵入か攻撃かを識別します。攻撃/セキュリティの脅威を識別し、それらを DDoS、Bad SrcDst、Suspect Flow、Scan/Probe などに分類します。

トップN 問題 Hourly レポート				トップN 違反者 Hourly レポート		
問題	初回	前回	イベント	違反者IP	Geolocation	イベント
Invalid ToS Flows	2019-12-02 13:02	2019-12-02 14:01	56	168.1.1.10	Australia(AU)	71
Invalid Src-Dst Flows	2019-12-02 13:03	2019-12-02 13:35	36	168.1.1.11	Australia(AU)	70
TCP Reset Violations	2019-12-02 13:08	2019-12-02 14:00	34	168.1.1.12	Australia(AU)	70
Malformed IP Packets	2019-12-02 13:03	2019-12-02 13:38	32	168.1.1.13	Australia(AU)	70
Non Unique Source Flows	2019-12-02 13:15	2019-12-02 13:54	18	168.1.1.14	Australia(AU)	70
Malformed TCP Packets	2019-12-02 13:04	2019-12-02 13:42	10	168.1.1.15	Australia(AU)	70
Excess Networked Flows	2019-12-02 13:22	2019-12-02 13:54	8	f269790c:ea8d47cc:d3ff:ebc1:8c48:8f50	Not Available(NA)	6
Malformed ICMP Host Scan	2019-12-02 13:06	2019-12-02 13:06	1	e779:f9d7:c4ff:c3d9:3ff:8a7d:d94e:51ac	Not Available(NA)	4
Malformed UDP Packets	2019-12-02 13:20	2019-12-02 13:20	1	e2d7:16ff:ed24:fe36:79d3:d04c:94ed:ad3f	Not Available(NA)	4
				f806:2c55:d13c:fa09:90d2:3573:dc07:b0bd	Not Available(NA)	4
トップN 違反者 Hourly レポート				トップN 違反者ロケーション Hourly レポート		
違反者IP	Geolocation	イベント	違反者ロケーション		イベント	
168.1.1.10	Australia(AU)	71	違反者ロケーション			
168.1.1.11	Australia(AU)	70	Not Available(NA)		153	
168.1.1.12	Australia(AU)	70	United States(US)		37	
168.1.1.13	Australia(AU)	70	Cayman Islands(KY)		4	
168.1.1.14	Australia(AU)	70	Canada(CA)		2	
168.1.1.15	Australia(AU)	70	トップN 違反者 Hourly レポート			
f269790c:ea8d47cc:d3ff:ebc1:8c48:8f50	Not Available(NA)	6				
e779:f9d7:c4ff:c3d9:3ff:8a7d:d94e:51ac	Not Available(NA)	4				
e2d7:16ff:ed24:fe36:79d3:d04c:94ed:ad3f	Not Available(NA)	4				

NetFlow Analyzer によるアプリケーショントラフィックの制御

NetFlow Analyzer は企業の LAN と WAN のトラフィックを可視化し、アプリケーションとそれらの帯域消費に関する情報を提供します。この情報を基に、QoS ポリシーを監視し、ミッションクリティカルなアプリケーションを高い優先度で処理するために必要な変更を加えることができます。LAN や WAN の問題や攻撃はプロアクティブに識別され、利用者が影響を受ける前に修正されます。ネットワークに NetFlow Analyzer を導入し、シームレスなアプリケーション配信のためにネットワークパフォーマンスを向上させましょう。

ManageEngine NetFlow Analyzer について

NetFlow や sFlow などのプロトコルを活用し、ネットワーク帯域の「可視化」を支援するフローコレクター製品です。

NetFlow Analyzer の特徴は以下の通りです。

特徴 1: コストを抑制

アプライアンス製品よりも導入しやすい年間 17.8 万円からの低価格帯

特徴 2: 必要十分な機能

ネットワークトラフィックの監視・可視化に必要な十分な機能をデフォルトで実装

特徴 3: 直感的な管理画面

クリックによるドリルダウンで、障害の原因調査も楽々。直感的な操作でトラフィックの調査も迅速化

お問い合わせ先

ゾーホージャパン株式会社

〒 220-0012

神奈川県横浜市西区みなとみらい 3 丁目 6 番 1 号 みなとみらいセンタービル 13 階

Web : <https://www.manageengine.jp/>

E-mail : jp-mesales@zohocorp.com (弊社営業宛)

2019 年 12 月発行 ZJMR20191225130

※当 eBook は Zoho corporation で発行されたものをゾーホージャパンが加筆・修正したものです

