



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性し、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みます。

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 interface. The top navigation bar includes '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モ', 'NFAナレッジ', 'NFAマニュアル', 'IP SLA', 'WLC', and '攻撃'. Below the navigation is a search bar with 'wan1' and a date range '2019-11-02 15:47 to 2019-12-02 15:47'. The main content area has tabs for '概要', 'トラフィック', 'アプリケーション' (which is selected), '送信元', '宛先', 'QoS', '通信', 'NBAR', 'CBQoS', 'マルチキャスト', 'メディアネット', 'AVC', and '攻撃'. The 'アプリケーション' tab shows a list of applications with their traffic volume and percentage: 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%), cwpserver (904.295 MB, 0%), hptvtrp (847.073 MB, 0%), ms-wbt-server (792.502 MB, 0%), plethora (468.487 MB, 0%), pop3s (171.670 MB, 0%), and smtp (34.389 MB, 0%). A 'ポートの表示' (Port View) link is also present. On the right, there are icons for '受信' (Receive), '送信' (Send), 'メール' (Email), 'PDF', and 'CSV'.

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。

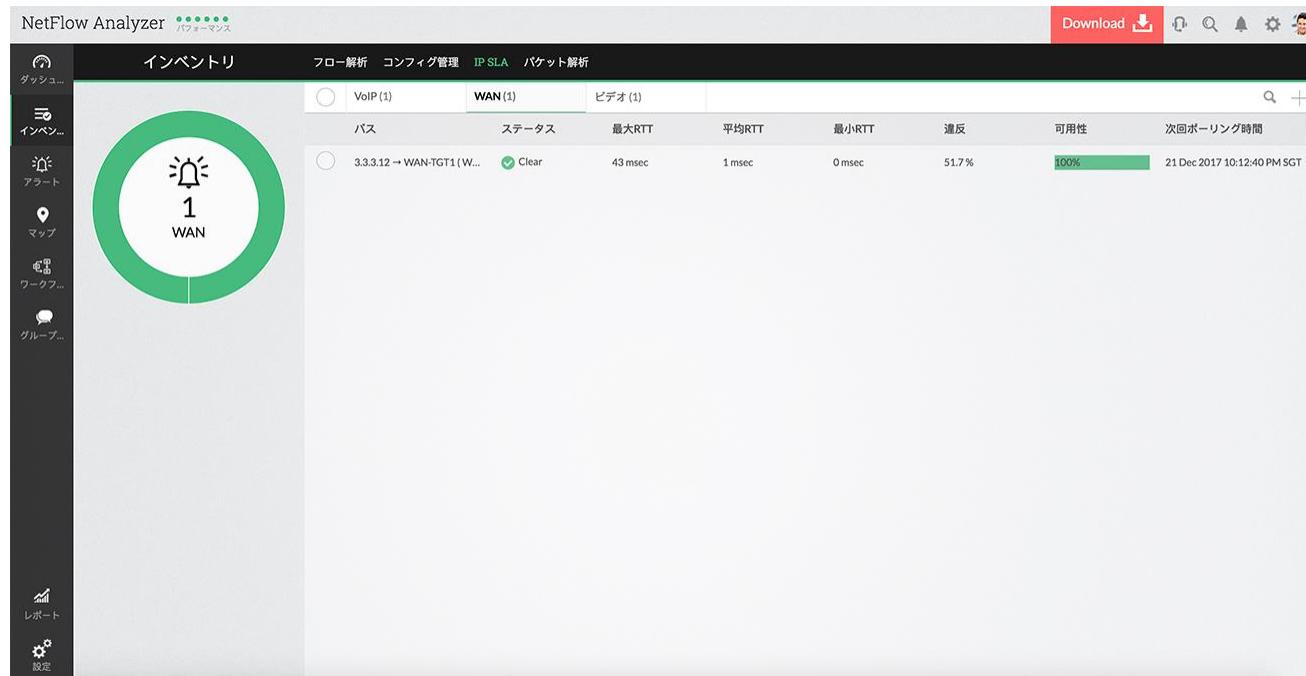


WAN 全体の帯域幅のボトルネックを検出

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。

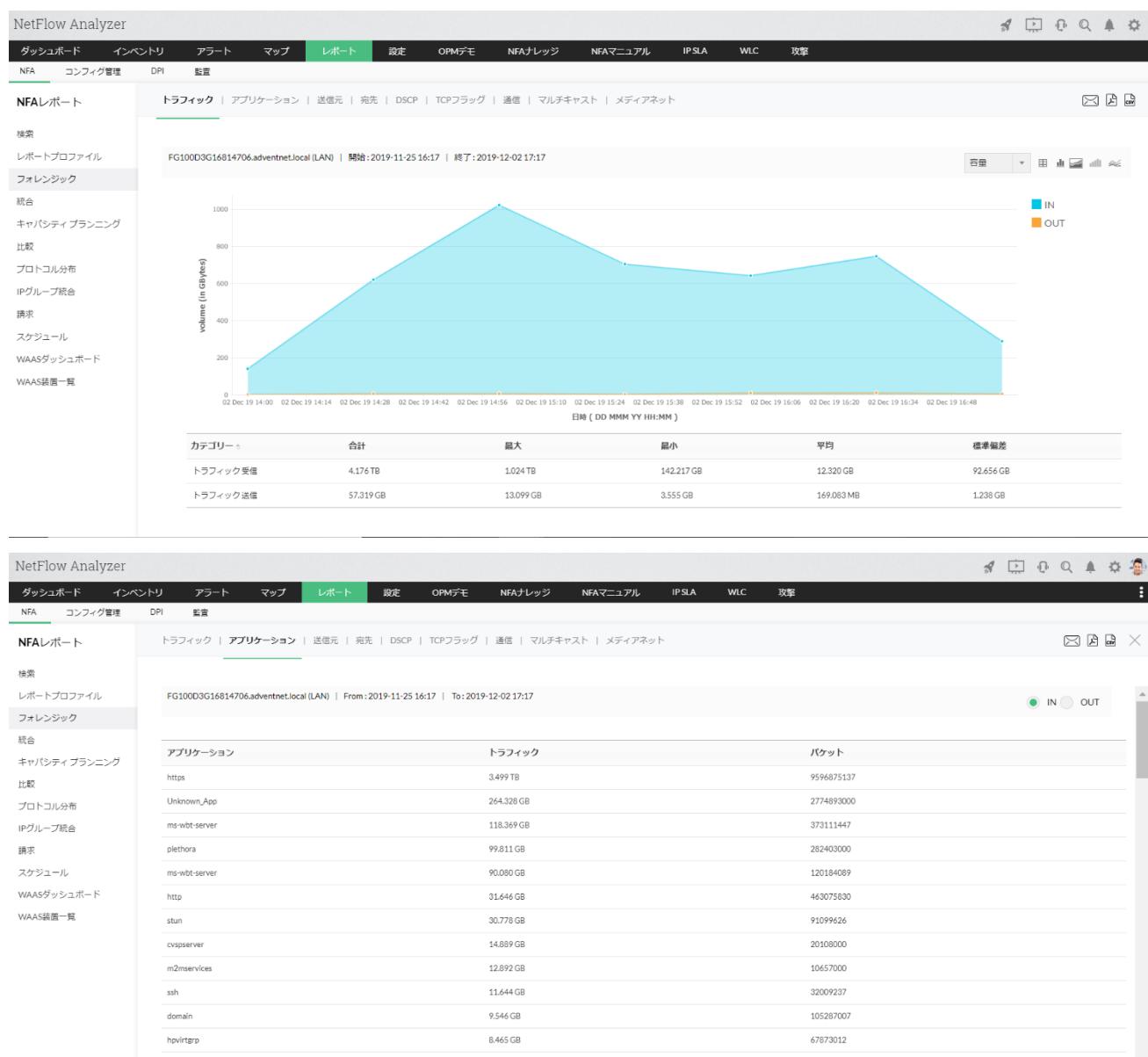


根本原因を見つけるためのフォレンジック分析

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。



■ 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	OPMマップ	OPMモード	NFAナレッジ	NFAマニュアル	IP SLA	WAC	監査						
NFA	コンフュージョン	DPI															
NFAレポート																	
トラフィック アプリケーション 送信元 受信 DSCP TOPフラッグ 溝道 マルチキャスト メディアネット																	
概要																	
FG100030316814705.adventure.local LAN From: 2019-12-06 09:54 To: 2019-12-06 10:56																	
レポート/ログファイル																	
フォレンジック																	
送信元IP	到着IP	アプリケーション	送信元ポート	到着ポート	プロトコル	DSCP	TOPフラッグ	フレーレット	トライフック	パケット	次のホップ	FNF NbarApp	M(送信元IP)	M(到着IP)	M(送信元ポート)	M(到着ポート)	%
送信																	
	https	49903	443	TCP	Default	5.939 Gbps	18.560 GB	13173943	0.000	Sippe	124.155.17.120	0.000	49902	0	Ne		
	https	49903	443	TCP	Default	5.485 Gbps	15.659 GB	11122053	0.000	Sippe	124.155.17.120	0.000	49903	0	Ne		
	https	63556	443	TCP	Default	1.383 Gbps	10.038 GB	6932394	0.000	Dropbox	124.155.17.120	0.000	62555	0	Ne		
	https	49885	443	TCP	Default	10.478 Gbps	7.858 GB	5612000	0.000	Sippe	124.155.17.120	0.000	49885	0	Ne		
	https	64453	443	TCP	Default	8.911 Gbps	7.797 GB	5379200	0.000	Dropbox	124.155.17.120	0.000	64453	0	Ne		
	https	49883	443	TCP	Default	5.191 Gbps	5.948 GB	4812000	0.000	Sippe	124.155.17.120	0.000	49883	0	Ne		
	https	63738	443	TCP	Default	592.403 Mbps	4.368 GB	3033990	0.000	Dropbox	124.155.17.120	0.000	63738	0	Ne		
	https	56992	443	TCP	Default	1.012 Gbps	4.049 GB	2650000	0.000	Dropbox	124.155.17.120	0.000	56992	0	Ne		
	https	49904	443	TCP	Default	1.348 Gbps	3.539 GB	2503664	0.000	Sippe	124.155.17.120	0.000	49904	0	Ne		
	ms-wbt-server	3389	55347	UDP	Default	708.365 Mbps	3.275 GB	3054875	0.000	Sippe	0.000	0	192.168.254.10	0	56347	Ne	
	https	49884	443	TCP	Default	2.867 Gbps	3.225 GB	2420000	0.000	Sippe	124.155.17.120	0.000	49884	0	Ne		
	https	51238	443	TCP	Default	5.019 Gbps	3.114 GB	2228000	0.000	Sippe	124.155.17.120	0.000	51238	0	Ne		
	ms-wbt-server	3389	59075	TCP	Default	429.657 Mbps	3.115 GB	313900	0.000	Sippe	0.000	0	192.168.254.10	0	59075	Ne	
	https	63190	443	TCP	Default	4242028 Mbps	3.021 GB	43964348	0.000	Dropbox	124.155.17.120	0.000	63190	0	Ne		
	https	49890	443	TCP	Default	991.420 Mbps	2.944 GB	2218372	0.000	Sippe	124.155.17.120	0.000	49890	0	Ne		
	ms-wbt-server	3389	59196	TCP	Default	4352322 Mbps	2.619 GB	3045707	0.000	Sippe	0.000	0	192.168.254.10	0	59196	Ne	
	ms-wbt-server	3389	59075	TCP	Default	353.277 Mbps	2.561 GB	2544977	0.000	Sippe	0.000	0	192.168.254.10	0	59075	Ne	
	https	52794	443	TCP	Default	1.201 Gbps	2.552 GB	1804000	0.000	Dropbox	124.155.17.120	0.000	52794	0	Ne		
	https	49904	443	TCP	Default	1.471 Gbps	2.393 GB	1693338	0.000	Sippe	124.155.17.120	0.000	49904	0	Ne		
	ms-wbt-server	3389	59517	TCP	Default	433.411 Mbps	2.330 GB	2490900	0.000	Sippe	0.000	0	192.168.254.10	0	59517	Ne	
	ms-wbt-server	3389	55347	UDP	Default	5184884 Mbps	2.317 GB	2414755	0.000	Sippe	0.000	0	192.168.254.10	0	56347	Ne	
	ms-wbt-server	3389	59517	TCP	Default	402.403 Mbps	2.218 GB	2082183	0.000	Sippe	0.000	0	192.168.254.10	0	59517	Ne	
	ms-wbt-server	3389	59517	TCP	Default	4103534 Mbps	2.207 GB	2413551	0.000	Sippe	0.000	0	192.168.254.10	0	59517	Ne	
	ms-wbt-server	3389	59517	TCP	Default	4053415 Mbps	2.180 GB	2584578	0.000	Sippe	0.000	0	192.168.254.10	0	59517	Ne	
	ms-wbt-server	3389	55347	UDP	Default	755.338 Mbps	2.175 GB	2426325	0.000	Sippe	0.000	0	192.168.254.10	0	56347	Ne	
	ms-wbt-server	3389	59517	TCP	Default	4043149 Mbps	2.174 GB	2304062	0.000	Sippe	0.000	0	192.168.254.10	0	59517	Ne	

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 間接 Hourly レポート			トップN 逆反者 Hourly レポート			
規則	時間	イベント	逆反者IP	Geolocation	イベント	
Invalid ToD Flows	2019-12-02 12:02	2019-12-02 14:01	50	108.1.1.10	Australia(AU)	71
Invalid Src-Dst Flows	2019-12-02 12:00	2019-12-02 13:55	36	108.1.1.11	Australia(AU)	70
TCP Rst Violations	2019-12-02 12:08	2019-12-02 14:00	34	108.1.1.12	Australia(AU)	70
Malformed IP Packets	2019-12-02 12:00	2019-12-02 13:58	32	108.1.1.13	Australia(AU)	70
Non Unicast Source Flows	2019-12-02 12:15	2019-12-02 13:54	18	108.1.1.14	Australia(AU)	70
Malformed TCP Packets	2019-12-02 15:04	2019-12-02 13:42	10	108.1.1.15	Australia(AU)	70
Excess Networkcast Flows	2019-12-02 12:22	2019-12-02 13:54	8	f269.90c.ca8d47cc4d3f4b18c18c48.8f00	Not Available(NA)	6
Malformed ICMP Scan	2019-12-02 13:06	2019-12-02 13:06	1	e79bf9d4cfbcbd93f8a7d694e51ac	Not Available(NA)	4
Malformed UDP Packets	2019-12-02 13:20	2019-12-02 13:20	1	e2d715ff11d4e369b232c4c74a82ad3f	Not Available(NA)	4
				f006.205.612.612cf99.90d235758d77bb6	Not Available(NA)	4
トップN 標的 Hourly レポート			トップN 逆反者ロケーション Hourly レポート			
標的IP	Geolocation	イベント	逆反者位置	イベント		
108.1.1.10	Australia(AU)	71	Not Available(NA)	153		
108.1.1.11	Australia(AU)	70	United States(US)	37		
108.1.1.12	Australia(AU)	70	Cayman Islands(CY)	4		
108.1.1.13	Australia(AU)	70	Canada(CA)	2		
108.1.1.14	Australia(AU)	70				
108.1.1.15	Australia(AU)	70				
f269.90c.ca8d47cc4d3f4b18c18c48.8f00	Not Available(NA)	6				
e79bf9d4cfbcbd93f8a7d694e51ac	Not Available(NA)	4				
e2d715ff11d4e369b232c4c74a82ad3f	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—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:必要充分な機能

ネットワークトラフィックの監視・可視化に必要充分な機能
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