



sflow



sFlow / NetFlow InMon TrafficSentinelのご紹介

フローマネージメントを活用した
ネットワークの可視化と管理

株式会社フローネットセキュア

出野 真也

IDENO@flownetsecure.com

フローマネージメントとは

- ソースとデスティネーション間のフレームの流れを以下のような内容などを認識し分析すること
 - ・ Source / Destination Address
 - ・ Source / Destination Port 番号
 - ・ Protocol
 - ・ Interface
 - ・ TOS (IP type of service) / Priority (802.1p)
 - ・ VLAN (802.1Q)
 - ・ AS番号



ネットワークの
可視化

次のような分析が可能

- なぜ、ネットワークが遅いのか？
- 誰がネットワークを使っているか？誰が何をしているか？
- セキュリティ対策は出来ているか？
- SPAM・DoS攻撃・ウイルス・ワームは？
- ネットワークの使用内容は？マルチキャスト通信は、どの程度？

フローマネージメントを実現するために策定された新たなテクノロジー - ハイスピードネットワークにおいて低コストで効果的なモニタリングを実現 -

- ・ SNMPやRMON2に代わる新しい管理技術
- ・ 米国InMon社によって開発され規格化し公開：
 Open Standard - IETF RFC3176(sFlow V4)
- ・ 多くのスイッチ・ルータ機器ベンダーで実装されているネットワーク・トラフィック・モニタリング技術(Industry standard)
- ・ ネットワーク全体を可視化: 全てのスイッチ・ルータで全てのインターフェースを測定
- ・ サンプルベースのテクノロジー
 - スイッチやネットワークのパフォーマンスへの影響が少ない
 - ハイスピードネットワーク内のトラフィックのモニタリングに効果的
 - NetFlow/J-Flow/IPFIXは、キャッシュベース(デバイス側でフローを生成)
- ・ ネットワーク機器埋め込み型として設計されたモニタリング・テクノロジー
 - ルータスイッチ内に実装されスイッチのASICにて処理
- ・ スイッチのsFlowエージェントがsFlowを生成し、sFlowマネージャーへ即座に送信
 - MIBやキャッシュ上で保持・カウントしない
- ・ 特別な機器を増設することなくsFlow対応デバイスであれば即座に使用可能

sFlow Datagram

Packet Header	Src/Dst i/f	Sampling Perms	Forwarding	user ID	URL	i/f counters
---------------	-------------	----------------	------------	---------	-----	--------------

- Flow sample (フローデータ)
 - Packet Header : サンプルパケットのパケットヘッダー情報(一部ペイロード含む)
 - Src/Dst i/f : 入出インターフェースのifIndex
 - Sampling Perms : sFlowパラメータ-(Sampling Rate,Sampling Pool etc)
 - Forwarding
 - Priority (Src/Dst 802.1p/TOS)
 - VLAN (Src/Dst 802.1q)
 - Next hop address
 - Source AS, Source Peer AS
 - Destination AS Path
 - Communities, local preference
 - MPLS
 - User ID : Src/Dst RADIUS/TACACS
 - URL
- SNMP Counter Sample (SNMP カウンタ- 値)
 - i/f counters : インターフェース・カウンター・統計値

sFlow実装ベンダー；

A10 Networks , ADARA Networks , Aerohive , Alaxala Networks,
Alcatel-Lucent Enterprise , Allied Telesis , Arista Networks , AT&T , Aruba
Big Switch Networks , Black Box Network Services , Brocade,
Cameo Communications , Cisco , Comtec Systems , Cumulus Networks
Dax Networks , Digital China Networks (DCN) , Dell , D-Link , DrayTek Corp.
Edge-Core Networks , Enterasys , Extreme Networks , F5 , Fortinet
Gambit Communications , Hewlett-Packard , Hitachi , Huawei , IBM , IP Infusion
ITS Express , Juniper Networks , LANCOM Systems , LevelOne ,
LG-ERICSSON , Maipu , Mellanox , MRV , NEC , NETGEAR , Nevion ,
Open vSwitch , Overture Networks , Pica8 , Plexxi , Pluribus Networks ,
Proxim Wireless , Quanta Computer , Radisys Corporation , Silicom Ltd. ,
SMC Networks , Themis Computer , Vyatta , Xenya ,
XRoads Networks , ZTE , ZyXEL , and InMon Corp.

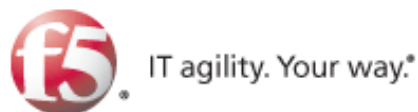
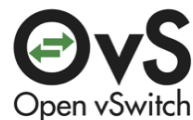
詳しくは、

<http://www.sflow.org/products/network.php>

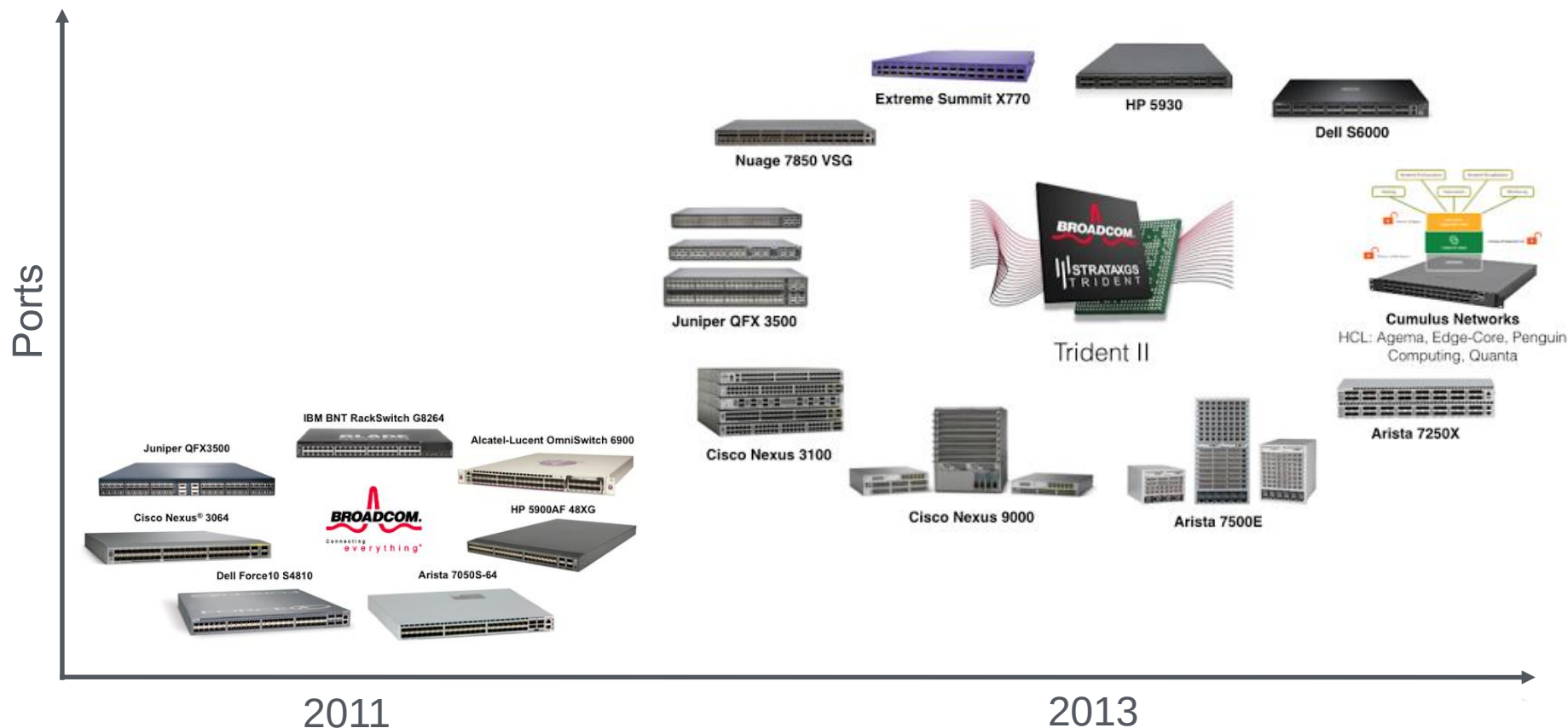
を参照いただき。

詳細は、各ベンダーにご確認ください。

<http://www.sflow.org>



物理的レベル(チップ・ポート・基盤)での実装



共通で使用するチップベースでsFlowが提供されるので、
多くのデバイスベンダーでの実装が進んでいる

NetFlow系(NetFlow/J-Flow/IPFIX)実装メーカー



※ 各機器での対応状況の詳細は、ハードベンダー様へご確認下さい

- ・ サンプルングされた情報から実際のフレーム数やバイト数を導き出す
- ・ プロトコル別トラフィック量の計算

入力したフレームの総数 = N

総サンプル数 = n

そのクラス(プロトコル)でのサンプル数 = c

そのクラス別のフレーム数は次式により計算 :

$$N_c = \frac{c}{n} \cdot N$$

例:

入力したフレームの総数 = 1,000,000

サンプリングレート = 0.25%

総サンプル数 = 2,500

Voicetラフィックのサンプル数 = 1,000

表示されるVoicetラフィックのフレーム数は:

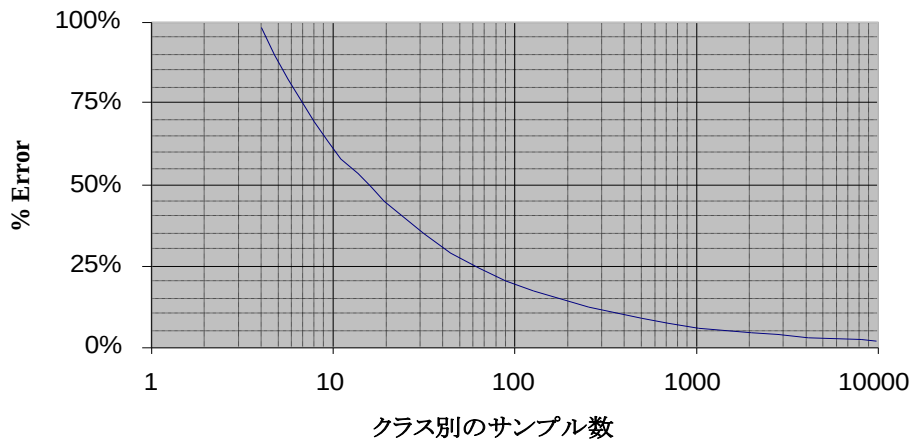
$$\frac{1,000}{2,500} \times 1,000,000 = 400,000 \quad \text{フレーム}$$

サンプリングの誤差が発生 → 統計的手法(95%信頼区間分析)により把握

sFlow: サンプルングの誤差(解析精度)

サンプルングの誤差 → 95%信頼区間によって分析

サンプルングの誤差(95%信頼区間)



95%信頼区間計算式: $\%error \leq 196 \cdot \sqrt{\frac{1}{c}}$

例: 95%の信頼区間でのエラー率を前ページの例で計算すると、
Voicetラフィックのサンプル数 = 1,000
なので、

$$\%Error \leq 196 \times \sqrt{\frac{1}{1,000}} \div \pm 6.2\%$$

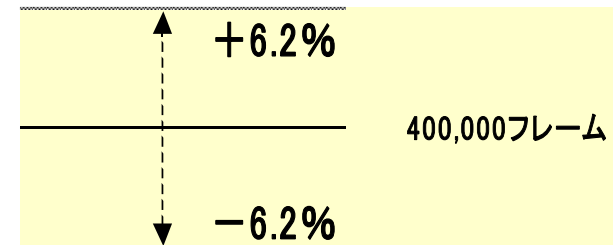
表示された“400,000 フレーム”に対し
95%信頼区間では、±6.2%が誤差になる
ので、区間は、

375,200フレーム(Lower)

～

424,800フレーム(Upper)

となる。



- ・ 誤差とトラフィックはトレードオフの関係（トラフィック=分析対象トラフィック）
 - トラフィックが多い → 誤差は少ない / トラフィックが少ない → 誤差は大きい
- ・ 誤差を少なくするには？
 - 対象となるフローを増加（サンプリングレートを上げる？分析対象期間を延ばす？）
- ・ 誤差を少なくする分析
 - トラフィックが多い場合：通常のサーバーアクセス(HTTP通信など)、DoS攻撃
→ トラフィックが多いので、リアルタイムでも誤差は少ない
 - トラフィックが少ない場合：使用頻度・通信量の少ない通信(チャット通信など)
→ トラフィックが少ないので、リアルタイムでは誤差が大きい
→ 対象期間を延ばす(“分”から”時間“, ”日“, ”週“, ”月“へ)と
対象トラフィックが多くなるので、誤差が少なくなる
 - サンプルング分析のコンセプト
 - ・ メジャーなトラフィックは、誤差が少なく、リアルタイム性も保たれる
 - ・ マイナーなトラフィックは、対象期間を延ばし、誤差を低減
 - ・ スイッチ・パフォーマンス、ネットワーク・パフォーマンスの悪化を防ぐ
- ・ サンプルングベースのテクノロジーの為、1G/10Gネットワークから
更なるハイスピードネットワークへの対応が可能



- Cisco NetFlow → Ciscoが開発した技術
 - ネットワーク上のIPフローについてネットワーク管理者が情報収集する手段を提供
 - エクスポートされたNetFlow データは、ネットワークの管理やプランニング、課金、攻撃対策、データマイニングなど、様々な用途に利用可能
 - NetFlow が出力する基本データは、「フロー レコード」と呼ばれる
 - バージョン1,5,7,8,9が存在
 - バージョン9は、RFC3954として公開(ただ、オープンな規格ではなくCISCOの規格として浸透)
 - 一般的には、全てのポートをモニターするのではなく、特定のポートをモニター
- キャッシュ・ベースのテクノロジー(キャッシュ上でフローをカウント)
- L3以上のトラフィックの分析が可能(L2の分析(MACアドレス分析など)は不可)
- NetFlowは、フローとして集計された情報として送られる
 - マネジャー側でフロー情報化する必要がない
- JuniperのJ-FlowはNetFlowと同等の規格、ただし、サンプリング必須
- パフォーマンス上に問題がある場合は、サンプリング・テクノロジーを使用した“Sampled NetFlow”も用意されている
 - Sampled NetFlow 機能を使用すれば、ルータに転送される「x」個の IP パケットごとに 1 個のパケットをサンプリングできます。サンプリング パケットは、ルータの NetFlow フロー キャッシュに取り込まれます。このサンプリング パケットにより、大多数のパケットに対して NetFlow 用の追加処理が不要となるので、スイッチング処理がより高速に行えるようになり、NetFlow パケットの処理に要する CPU 使用率を大幅に低減できます。
(「Ciscoマニュアルより」抜粋)

- ・ フロー

- 以下の図の内容を、フローとして、統計値(フレーム数・バイト数)をNetFlowキャッシュ内でカウント
- NetFlowキャッシュ内で保持・カウントしている情報を、特定のタイミング(条件)でエクスポート

フロー (7つのキー)						
Source IP Address	Source Port	Destination IP Address	Destination Port	Layer 3 プロトコル・タイ プ	TOS byte	インターフェー ス (ifIndex)

- ・ フローをエクスポートするタイミング

- インアクティブ・タイマー(デフォルト:15秒)
 - ・ 該当のフローセットのセッションが15秒間インアクティブ(無音)の時、エクスポート
 - ・ コマンド ” ip flow-cache timeout inactive 15 “で設定
- アクティブ・タイマー(デフォルト:30分)
 - ・ 該当のフローセットのセッションが継続している場合、30分経過時点で、エクスポート
 - ・ コマンド ” ip flow-cache timeout active 30 “で設定
- TCPコネクションのRSTやFINフラグの検出
- NetFlowキャッシュがフル

- ・ sFlow
 - RFC3176として公開(機器ベンダ非依存のオープンな規格)
 - サンプリングベース
 - 対象レイヤー:L2-L7+Payload
 - 高速スイッチングネットワークの測定を目的に開発
 - WANのモニタリング(BGP AS path 分析)
 - 全インターフェースをモニター
 - AS分析(OriginAS/SourcePeerAS/DestPeerAS/DestinationAS Path)
- ・ NetFlow
 - RFC3954として公開(Cisco色が強い)
 - キャッシュベース
 - 対象レイヤー:L3-L4
 - WANリンクの測定が主たる目的としてリリース
 - LANのモニタリング(CatalystへのNetFlowの実装)
 - 特定のインターフォース(VLAN)をモニター
 - AS分析(SourcePeerAS/DestPeerAS)

Complete Network Visibility and Control - InMonTrafficSentinelによる完全なるネットワークの可視化と管理 -

sFlow / NetFlow / J-Flow / IPFIX etc によるフローマネージメントシステム
- ネットワーク全体を常時監視 -

InMonTrafficSentinelはsFlow/NetFlow/J-Flow/IPFIXを解釈し、フローマネージメントを通してあらゆる企業に有益な情報を提供します。今までのSNMPベースのネットワーク管理では実現し得なかったネットワーク全体に対するネットワーク・トラフィックの常時監視と分析が可能となります。

「誰が、いつ、どの様な、通信をしているのか？」

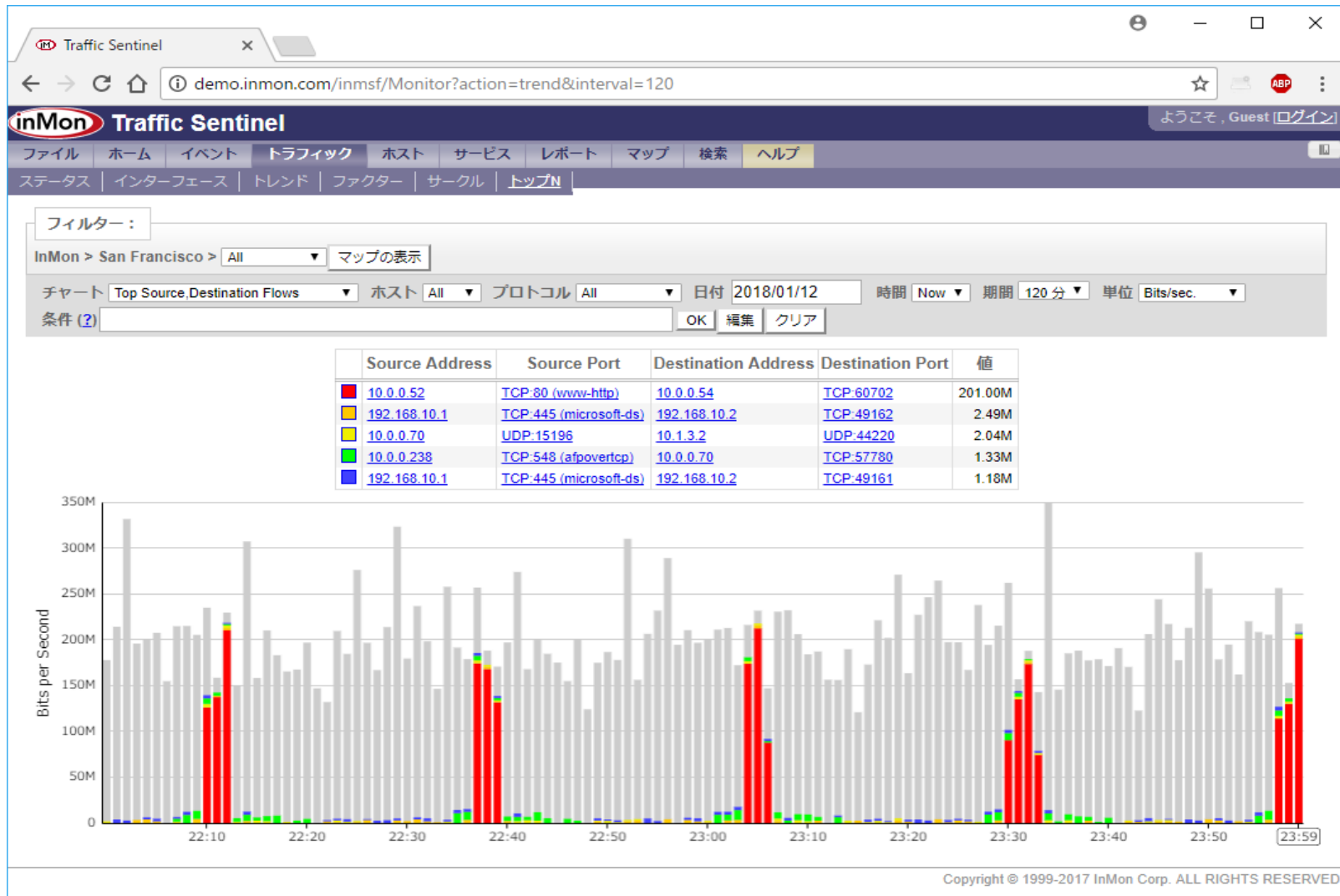
「全社に渡るネットワーク使用状況を把握したいが、コストが・・・」

InMonTrafficSentinelの主要機能；

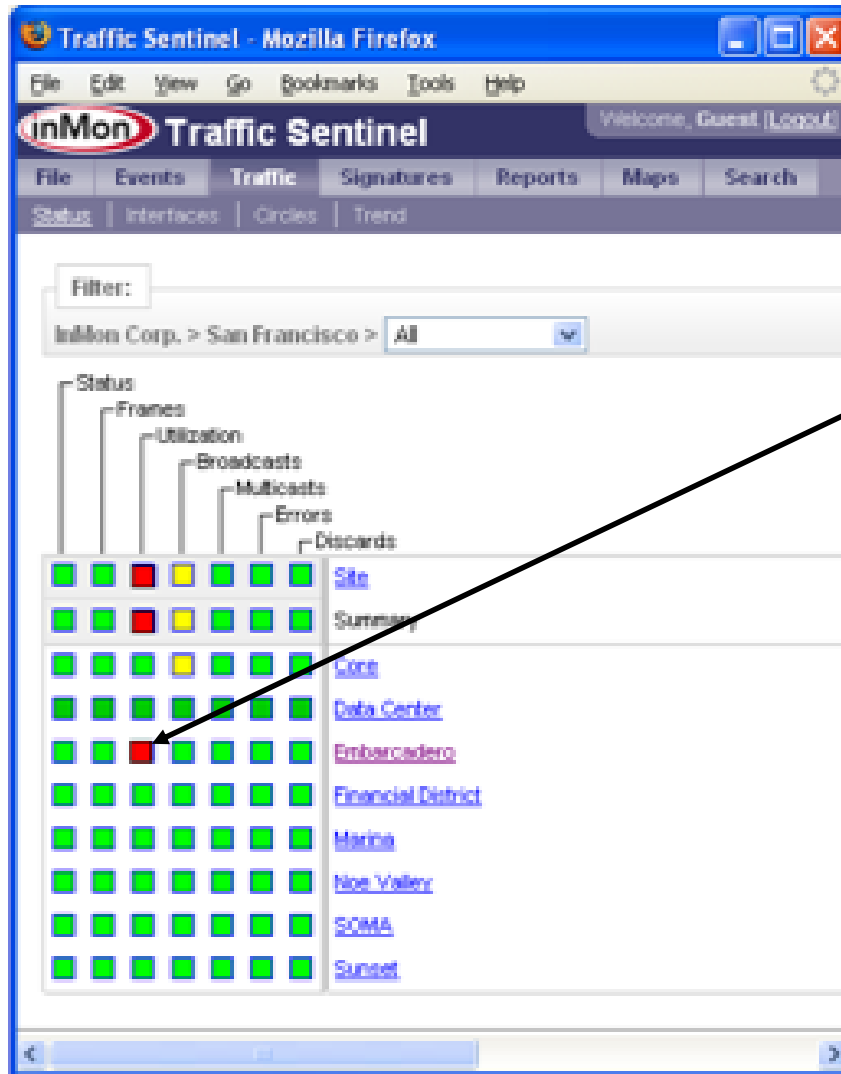
- ・トラブルシューティング
- ・セキュリティ対策
- ・キャパシティープランニング
- ・システムのあらゆる側面（アプリケーション、サーバー、ネットワークなど）を一元的・総合的に管理

InMonTrafficSentinelは、sFlowをIETFでRFC3176として公開したInMon社が開発したフローマネージメントシステムで、世界で唯一、すべてのsFlow統計値を管理できるマネージャーです。

InMon Traffic Sentinelは、日本語版アプリケーションとして提供します



全てのグループ(拠点、組織 etc)の中で問題のあるグループをアラート



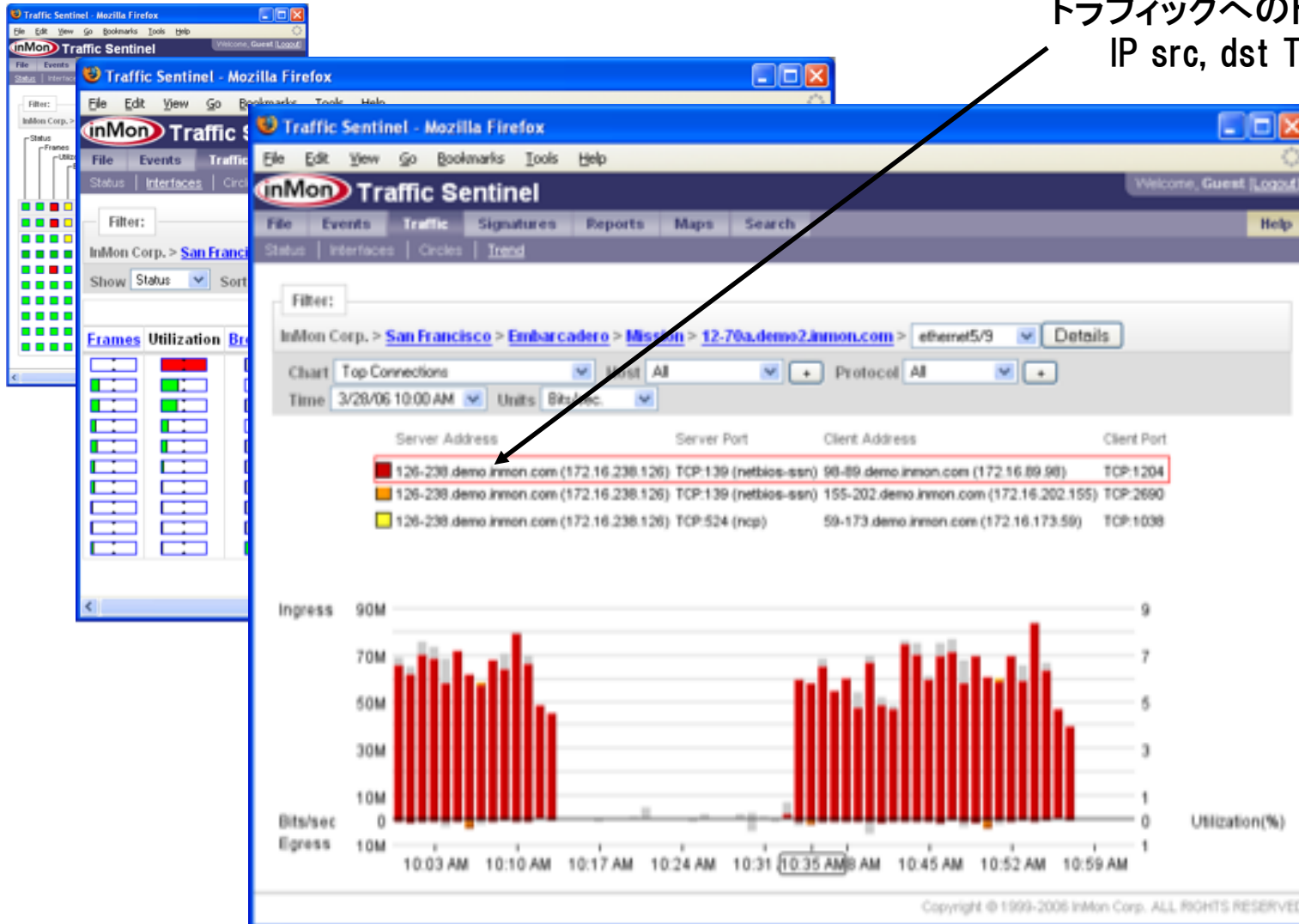
しきい値超過

問題のあるグループでのアラートの内容とロケーションの把握

ロケーションの把握

Status						Interface		
Frames	Utilization	Broadcasts	Multicasts	Errors	Discards	Agent	Interface	ifSpeed
						12-70a.demo2.inmon.com	ethernet5/9	1Gb/sec
						38-70a.demo2.inmon.com	ethernet48	10Mb/sec
						38-70a.demo2.inmon.com	ethernet47	10Mb/sec
						45-70a.demo2.inmon.com	ethernet15	100Mb/sec
						29-70a.demo2.inmon.com	ethernet8	100Mb/sec
						22-70a.demo2.inmon.com	ethernet43	100Mb/sec
						33-70a.demo2.inmon.com	ethernet47	100Mb/sec
						28-70a.demo2.inmon.com	ethernet31	100Mb/sec
						35-70a.demo2.inmon.com	ethernet20	100Mb/sec
						41-70a.demo2.inmon.com	ethernet9/1	1Gb/sec

アラートに対するトラフィック・フローへのドリルダウン



発生アラートのロケーションの把握

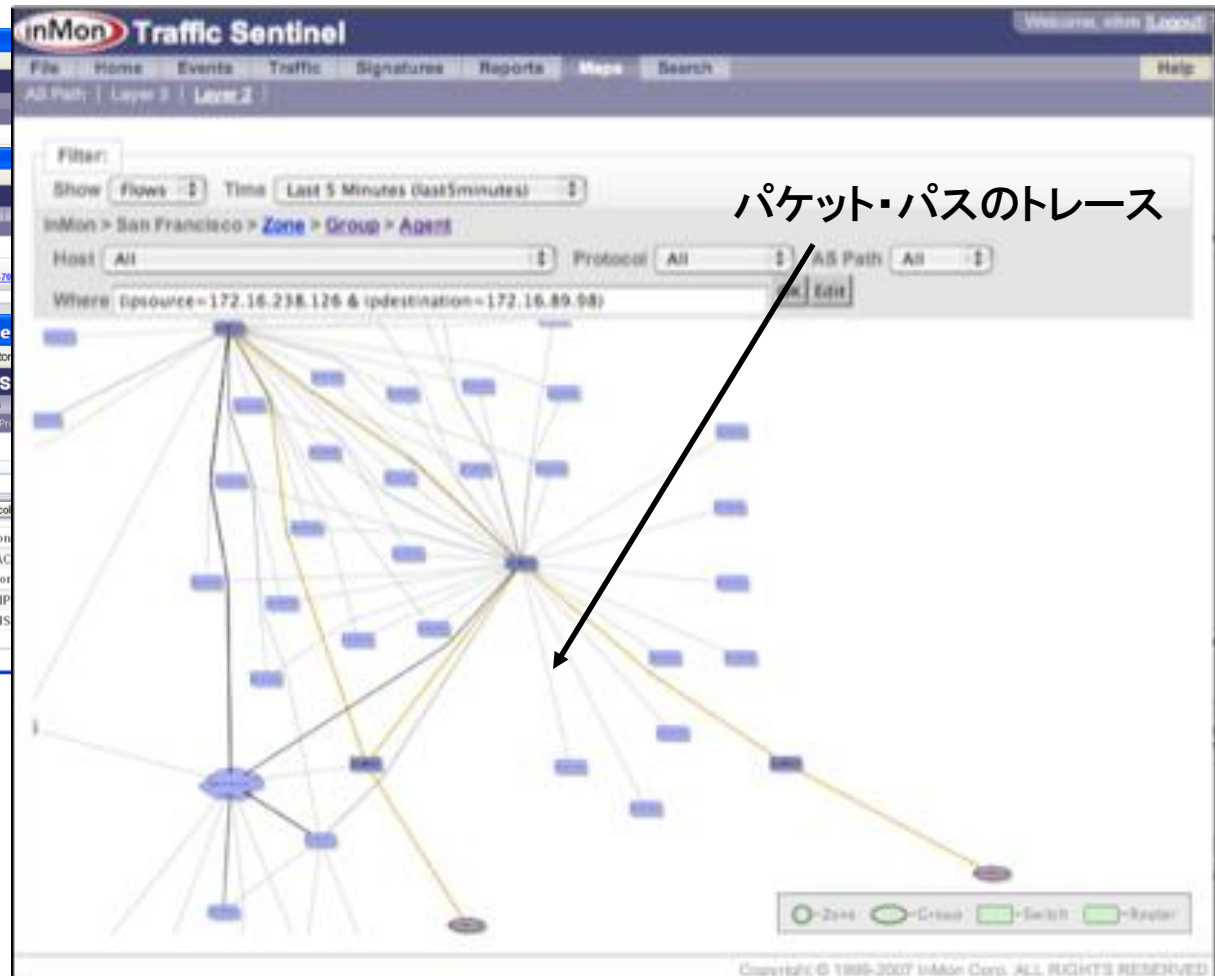
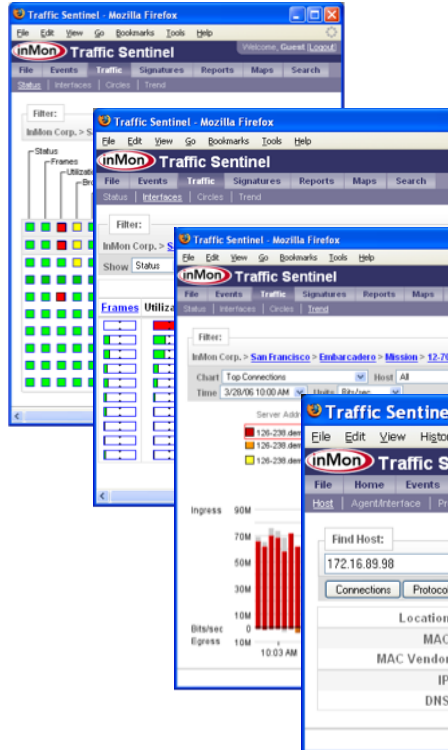
スイッチ・ポートでの
ホストのロケーション

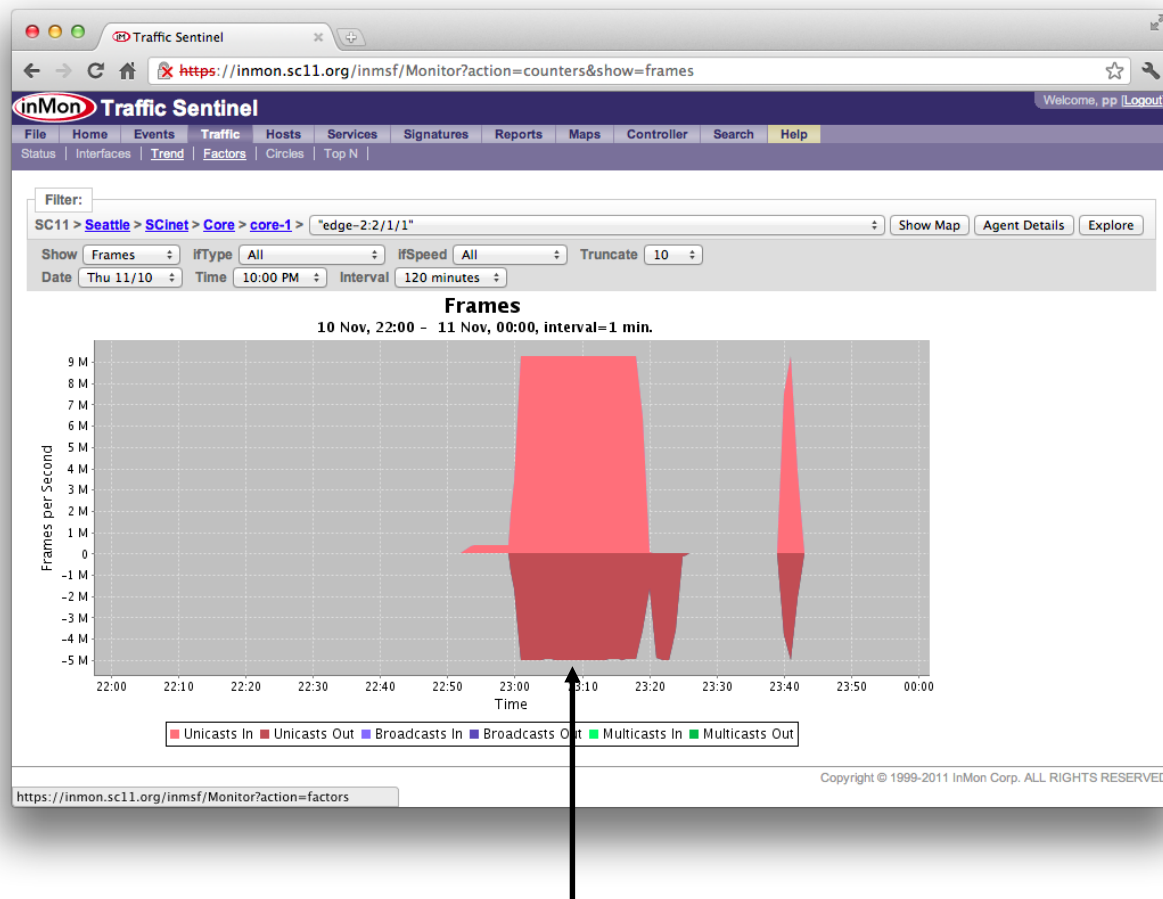
The screenshot shows the Traffic Sentinel interface with the 'Find Host' search bar containing '172.16.89.98'. Below the search bar, the 'Location' field is circled in red and pointed to by an arrow from the text 'スイッチ・ポートでのホストのロケーション'. The location details are as follows:

Location	InMon>San Francisco>SOMA>Beale>21-66.demo.inmon.com>C7
MAC	001279C2DA39
MAC Vendor	Hewlett Packard
IP	172.16.89.98
DNS	98-89.demo.inmon.com

Copyright © 1999-2008 InMon Corp. ALL RIGHTS RESERVED

パケット(トラフィック)パスのトレース





なぜ、トラフィックがここでスパイクしたのか？
(100Gbリンクで 14,000,000 packets/second)

➤ カウンター情報は、障害があることを知らせるが、原因はわからない

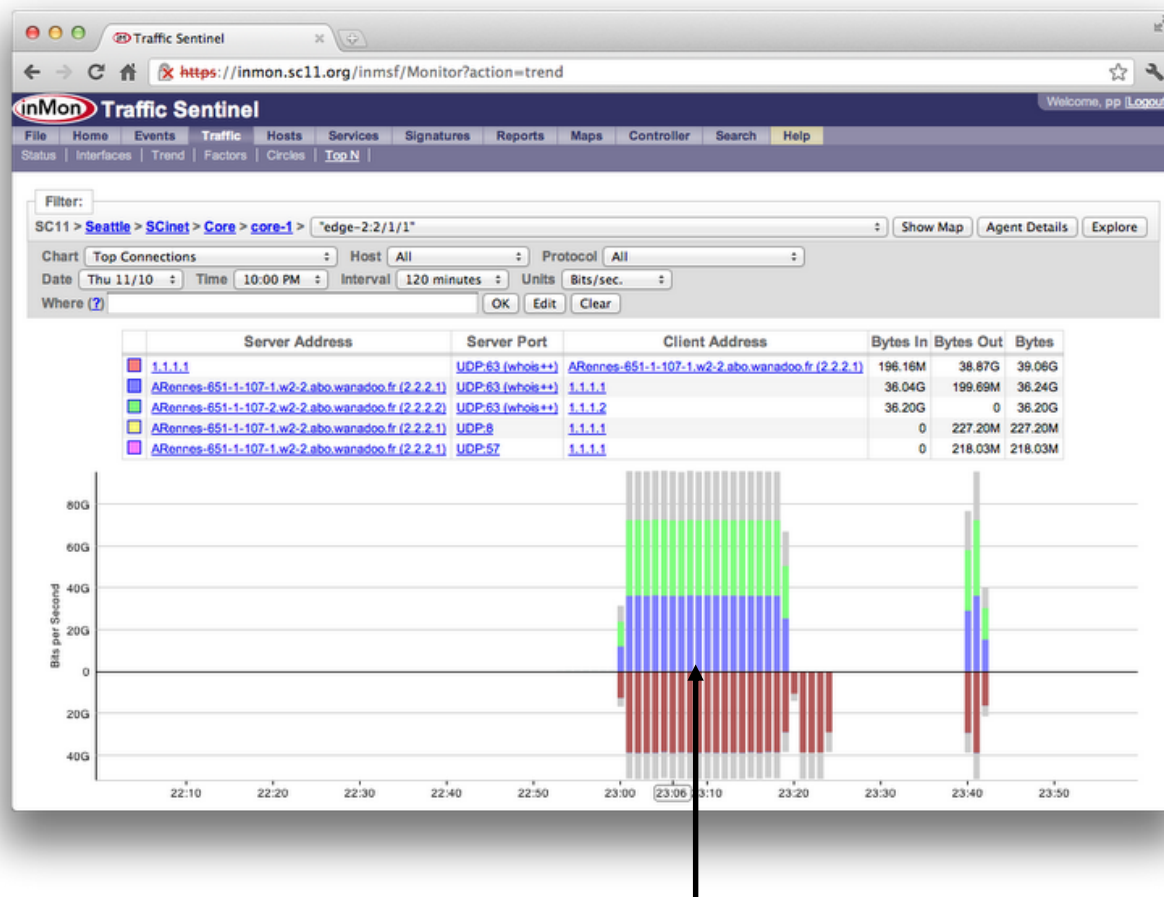
➤ カウンター情報は、パフォーマンスを集約できるが、下記の様な重要な情報は含まれていない：

IPアドレス
プロトコル
URL
Memcache keys

➤ パフォーマンスの問題を解明するためには、もっと効果的な情報が必要である

➤ 1秒に数百万ものトランザクションがある場合、どのようにしてデータを収集することができるか？

➡ フルパケットキャプチャ？
➡ 現実的ではない



- ランダム・サンプルは、低負荷
- サンプルされたトランザクションをフロー化するのに要求されるリソースは最小限である
- top keys, connections, clients, servers, URLsなどを識別するのが容易.
- 既知のサンプリング・レートでの分析

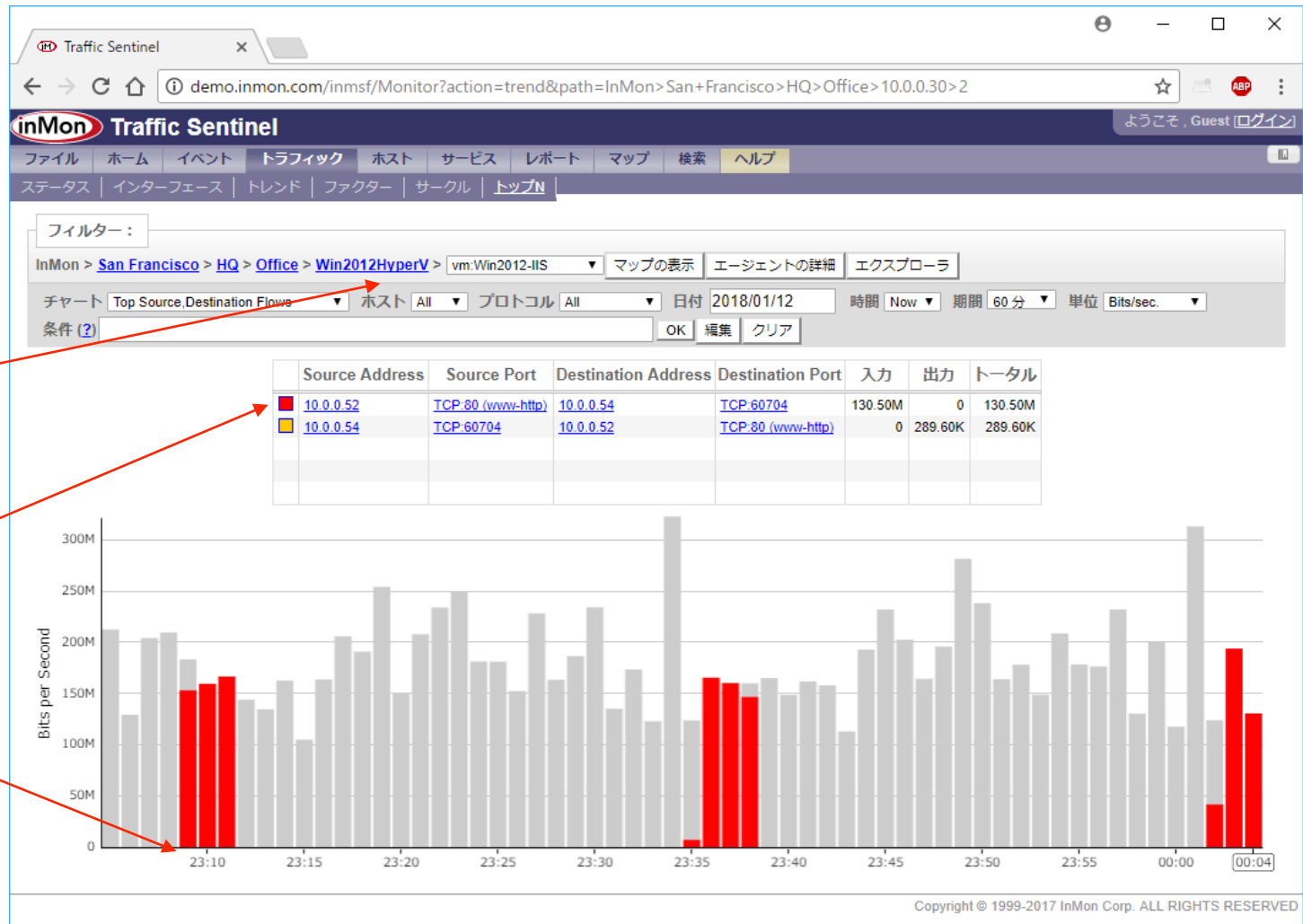
client, server, portで示されたトラフィックの発生
(14,000,000 packets/secondが流れる100Gbリンクでのサンプルをベースとしたグラフ)

「どこで・何が・いつ」問題解決の為の情報入手

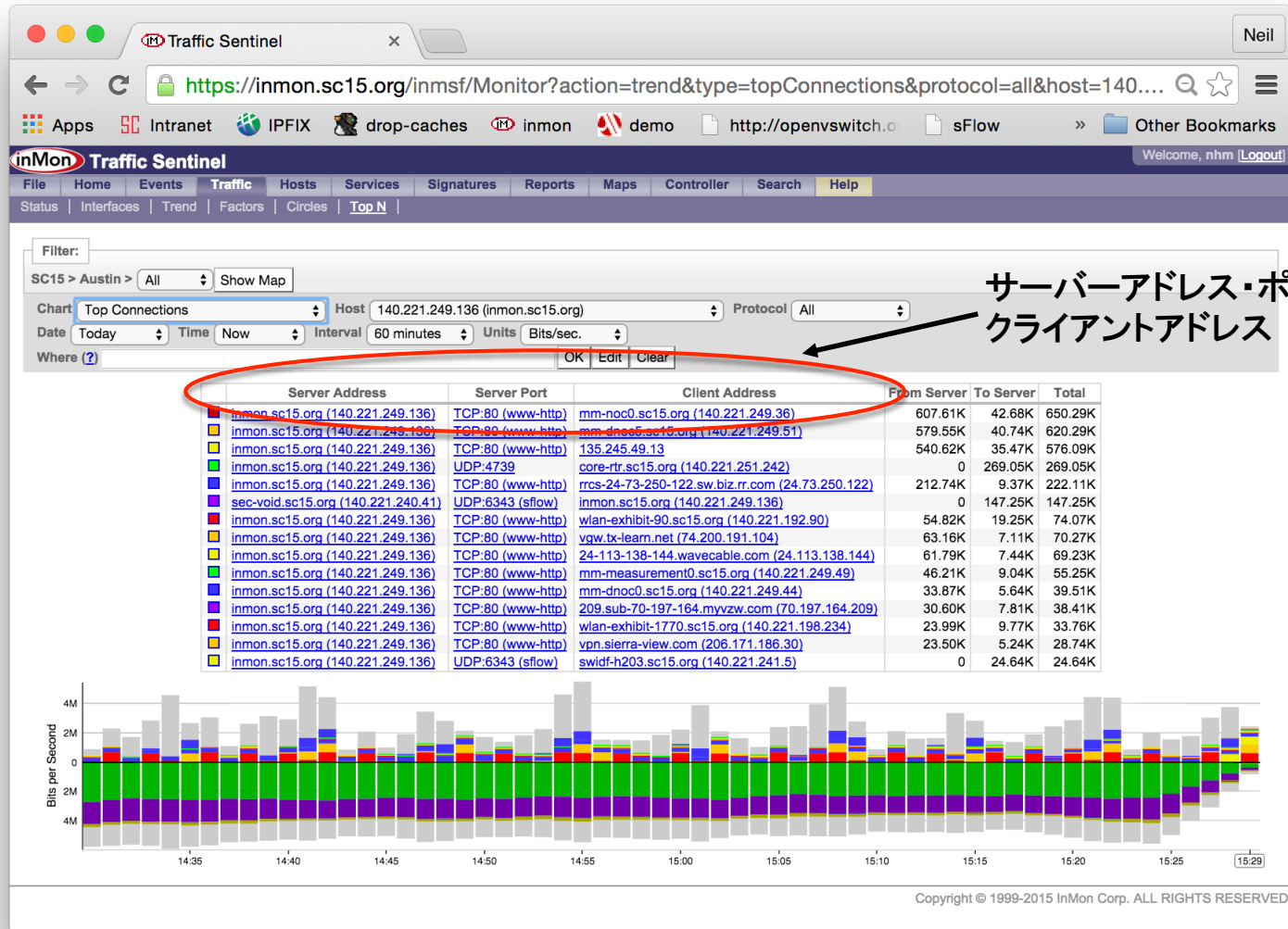
どこで

何が

いつ

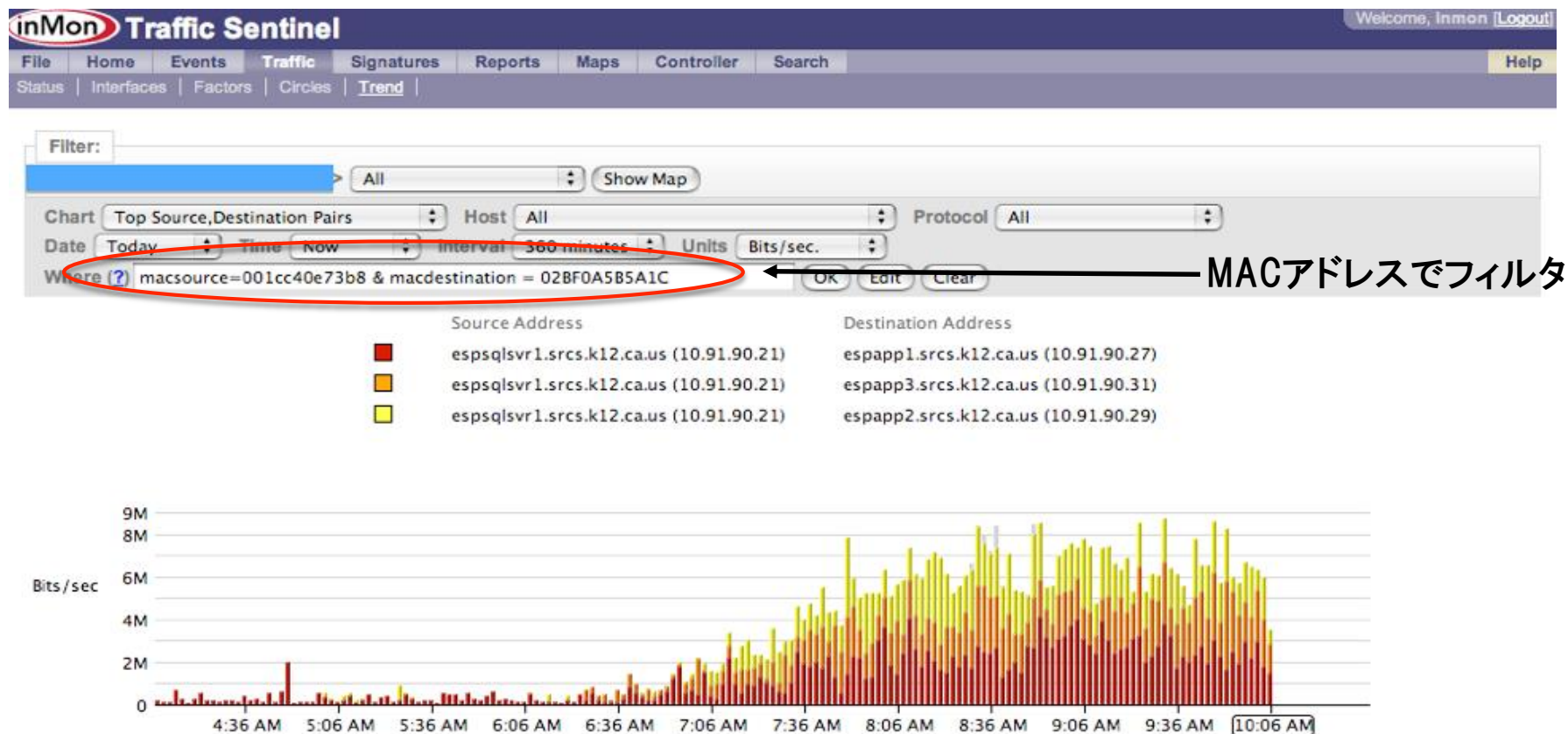


運用管理を受け持っているサーバへの接続状況調査：



サーバーアドレス・ポート、
クライアントアドレス

ユニキャスト・トラフィックをフィルタリング:MACアドレスでフィルタ



Copyright © 1999-2009 InMon Corp. ALL RIGHTS RESERVED

ロケーション:DNS、IP、MAC、Interface、VLAN etc での一覧

DNS Name,Address(IPv4/IPv6),
MAC,Interface,VLAN etc

inMon Traffic Sentinel

Filter: Category Inventory Section List Hosts with VLAN (for selected VLANs / Vendor Code)

List Hosts with VLAN (for selected VLANs / Vendor Code)

List hosts and the switch port connection them to the network (excluding purchased VLAN).

Name	address1	address2	macaddress	manufacturer	interface	vlan	link
1333A-scinet.sc15.org	140.221.138.58		00180A029994	Meraki, Inc.	dnoc1649-sw2.sc15.org~1333 1333-A (Intel Corporation) - PIP VLAN 252 - 100	OM unknown	
1533A-scinet.sc15.org	140.221.138.62		981544C0B07FD		dnoc839-sw2.sc15.org~1533 1533-A (Intel Corporation) - PIP VLAN 271 - VLAN 282 - 100	OM unknown	
A100.322.sc15.org	140.221.167.100	FE80::EEF4.B8FF.FEC8.F3DC	ECF4B8CF30C	Apple, Inc.	dnoc839-sw2.sc15.org~322 322-A (General Atomics) - VLAN 326 - 1000BaseSX	OM unknown	
A100.502.sc15.org	140.221.163.100		406C8F43C088		dnoc839-sw2.sc15.org~502 502-A (Department of Energy) - VLAN 289 - 1000BaseSX	OM unknown	
A105.522.sc15.org	140.221.164.105		70E284140084		dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A106.522.sc15.org	140.221.164.106		70E284140074		dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A107.522.sc15.org	140.221.164.107		F0DEF19BF67B	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A108.211.sc15.org	140.221.171.108	2001:468:1F07:160:3840:77F8:BFC3:B968	F0DEF19BF67B	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~211 211-A (IEEE) - 1000BaseSX	OM unknown	
A108.322.sc15.org	140.221.167.108	2001:468:1F07:146:118D:265C:C22:4DB1	SC260A75D592	Dell Inc.	dnoc839-sw2.sc15.org~322 322-A (General Atomics) - VLAN 326 - 1000BaseSX	OM unknown	
A108.522.sc15.org	140.221.165.108	140.221.165.50	3C970E0CC56F	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A109.211.sc15.org	140.221.171.109	2001:468:1F07:160:6962:81FF:66EE:641D	F0DEF19BF67B	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~211 211-A (IEEE) - 1000BaseSX	OM unknown	
A109.522.sc15.org	140.221.164.109	140.221.165.49	F0DEF19BF67B	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A11.1725.sc15.org	140.221.136.11	FE80::4550:107:2FB3:6AC6	28D244504DE3		dnoc1625-sw1~1725 1725-A (AIST) - 1000BaseSX	OM unknown	
A11.333.sc15.org	140.221.139.11	2001:468:1F07:F2:C8B:F894:113A:18A7	AC87A31C20F5		dnoc839-sw1~333 333-A (NASA) - 1000BaseSX	OM unknown	
A110.522.sc15.org	140.221.166.110	140.221.165.33	3C970E0CC4A9	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A111.522.sc15.org	140.221.164.111	140.221.166.11	F0DEF1E6E7FC	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A112.2906.sc15.org	140.221.166.112	140.221.166.112	00199933C46	Fujitsu Technology Solutions	dnoc1649-sw1~2040 2040-A (Cyviz) - 1000BaseSX	OM unknown	
A112.303.sc15.org	140.221.136.112	169.254.171.12	7428628A2E93		dnoc1649-sw2.sc15.org~2906 2906-A (COMSOL, Inc.) - VLAN 290 - 1000BaseSX	OM unknown	
A113.2040.sc15.org	140.221.136.112	2001:468:1F07:E9:5A5:466F:E3F:1BA3	DBD38595633C	Hewlett-Packard Company	dnoc839-sw1~303 303-A (Purdue University) - 1000BaseSX	OM unknown	
A113.2906.sc15.org	140.221.142.112	2001:468:1F07:110:DDC8:5425:8978:ACB0	AC87A32FC5E8		dnoc839-sw1~933 933-A (CIENA) - 1000BaseSX	OM unknown	
A113.3007.sc15.org	140.221.166.113	140.221.161.113	D867D972B0BA		dnoc1649-sw1~2040 2040-A (Cyviz) - 1000BaseSX	OM unknown	
A113.303.sc15.org	140.221.166.113	2001:468:1F07:15A:60ED:AD7A:6865:E6B6	784598A12F9		dnoc1649-sw2.sc15.org~2906 2906-A (COMSOL, Inc.) - VLAN 290 - 1000BaseSX	OM unknown	
A113.522.sc15.org	140.221.170.113	2001:468:1F07:E9:70CF:1D93:F113:62C7	AC87A327B198		dnoc839-sw1~307 307-A (University of Texas) - VLAN 346 - 1000BaseSX	OM unknown	
A113.933.sc15.org	140.221.136.113	140.221.165.40	3417EBCD72A8		dnoc839-sw1~303 303-A (Purdue University) - 1000BaseSX	OM unknown	
A114.2906.sc15.org	140.221.164.113	140.221.165.40	F0DEF1A8099E	Wistron InfoComm (Kunshan)Co	dnoc839-sw2.sc15.org~522 522-A (IBM) - VLAN 302 - 1000BaseSX	OM unknown	
A114.3007.sc15.org	140.221.142.113	FE80::A87A:3AFF:FE00:DE03	AC87A300DE03		dnoc839-sw1~933 933-A (CIENA) - 1000BaseSX	OM unknown	
A114.303.sc15.org	140.221.161.114	2001:468:1F07:122:34FC:3C82:4DC4:3932	7428628A2E90		dnoc1649-sw2.sc15.org~2906 2906-A (COMSOL, Inc.) - VLAN 290 - 1000BaseSX	OM unknown	
A114.307.sc15.org	140.221.161.114	2001:468:1F07:E9:4CDD:2F23:3D49:CE15	90B11C83051B	Apple Inc	dnoc839-sw1~303 303-A (Purdue University) - 1000BaseSX	OM unknown	
A114.307.sc15.org	140.221.161.114		C82A145521B8	Fujitsu Technology Solutions	dnoc839-sw1~933 933-A (CIENA) - 1000BaseSX	OM unknown	
A114.307.sc15.org	140.221.161.114		C01999F4F05F		dnoc1649-sw1~2040 2040-A (Cyviz) - 1000BaseSX	OM unknown	

https://inmon.sc15.org/inmsf/Go?action=host&go=28D244504DE3

propVirtual	1Gb/sec	203
ethernetCsmacd	10Mb/sec	10107
ethernetCsmacd	1Gb/sec	10120
ethernetCsmacd	1Gb/sec	10124
other	10Gb/sec	14501

Copyright © 1999-2015 InMon Corp. ALL RIGHTS RESERVED

inMon Traffic Sentinel Welcome, Guest [Login]

File Home Events Traffic Hosts Services Signatures Reports Maps Controller Search Help

Host Agent/Interface Protocol ASN Path Report

Path Between Hosts:

Source Destination

[10.0.0.151 - 10.0.0.150](#)

Agent	IfIndex In	IfIndex Out	MAC Source	MAC Destination	VLAN In	VLAN Out	Priority In	Priority Out	IP TOS	IP TTL
10.0.0.253	ethernet1	ethernet2	F22901705825	3E5B354B3A72					0	64
xenserver2	switch:ethernet10	21	F22901705825	3E5B354B3A72	0	0	0	0	0	64
xenserver1	vm:xenvm2	switch:ethernet2	F22901705825	3E5B354B3A72	0	0	0	0	0	64

30 Apr, 20:17 - 30 Apr, 21:17

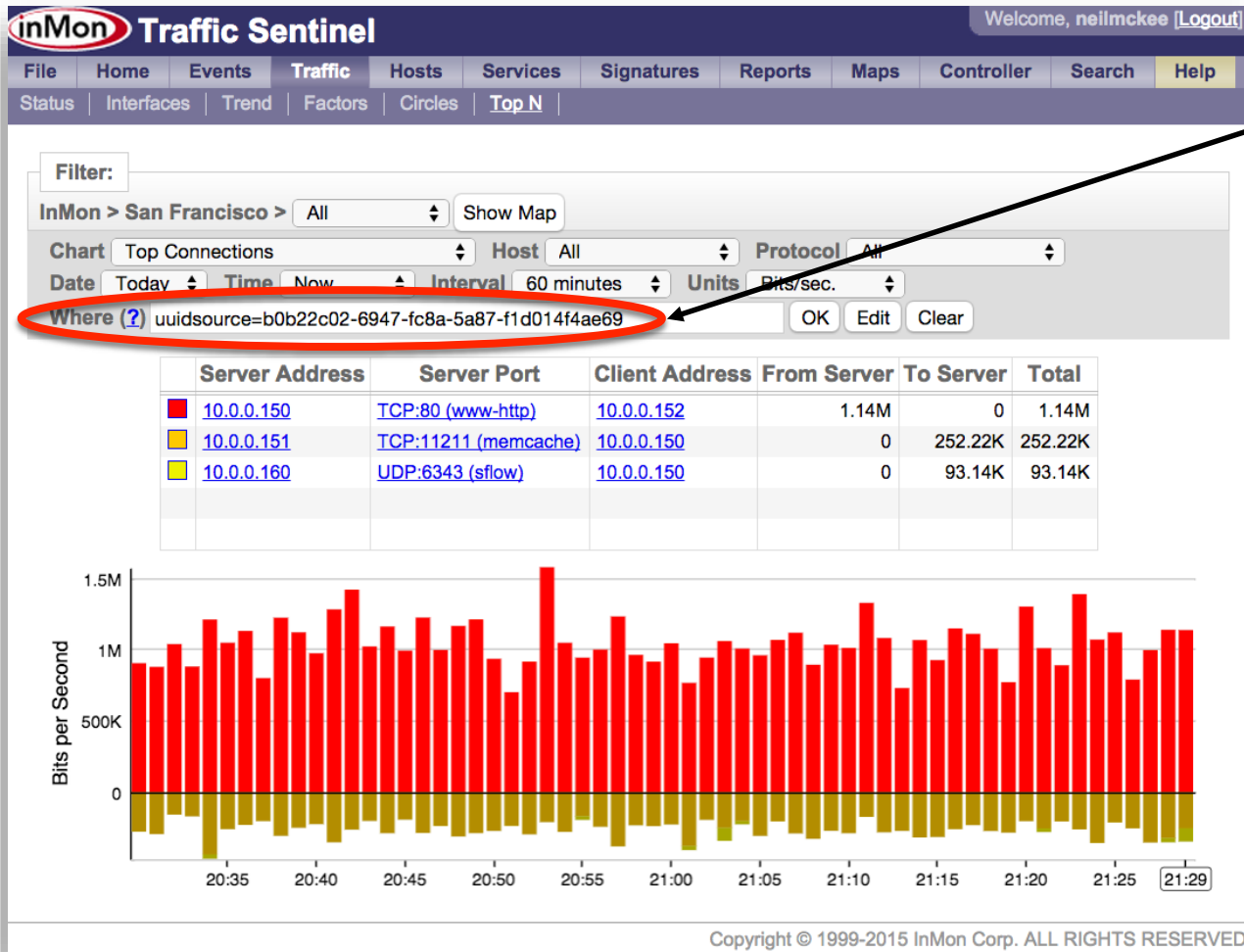
[10.0.0.150 - 10.0.0.151](#)

Agent	IfIndex In	IfIndex Out	MAC Source	MAC Destination	VLAN In	VLAN Out	Priority In	Priority Out	IP TOS	IP TTL
xenserver2	21	switch:ethernet10	3E5B354B3A72	F22901705825	0	0	0	0	0	64
xenserver1	switch:ethernet2	vm:xenvm2	3E5B354B3A72	F22901705825	0	0	0	0	0	64
10.0.0.253	ethernet2	ethernet1	3E5B354B3A72	F22901705825					0	64

30 Apr, 20:17 - 30 Apr, 21:17

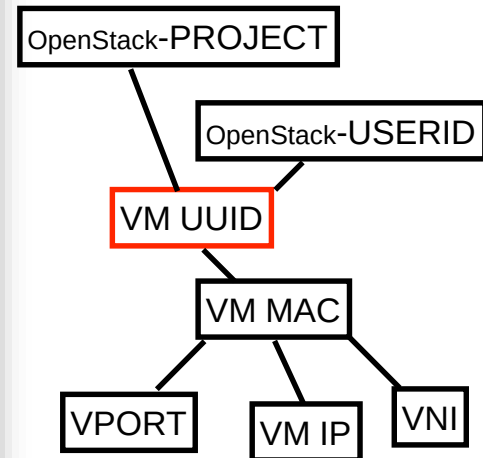
Copyright © 1999-2015 InMon Corp. ALL RIGHTS RESERVED

仮想スイッチの個々の仮想ポート経由でのパケット・パスのトレース

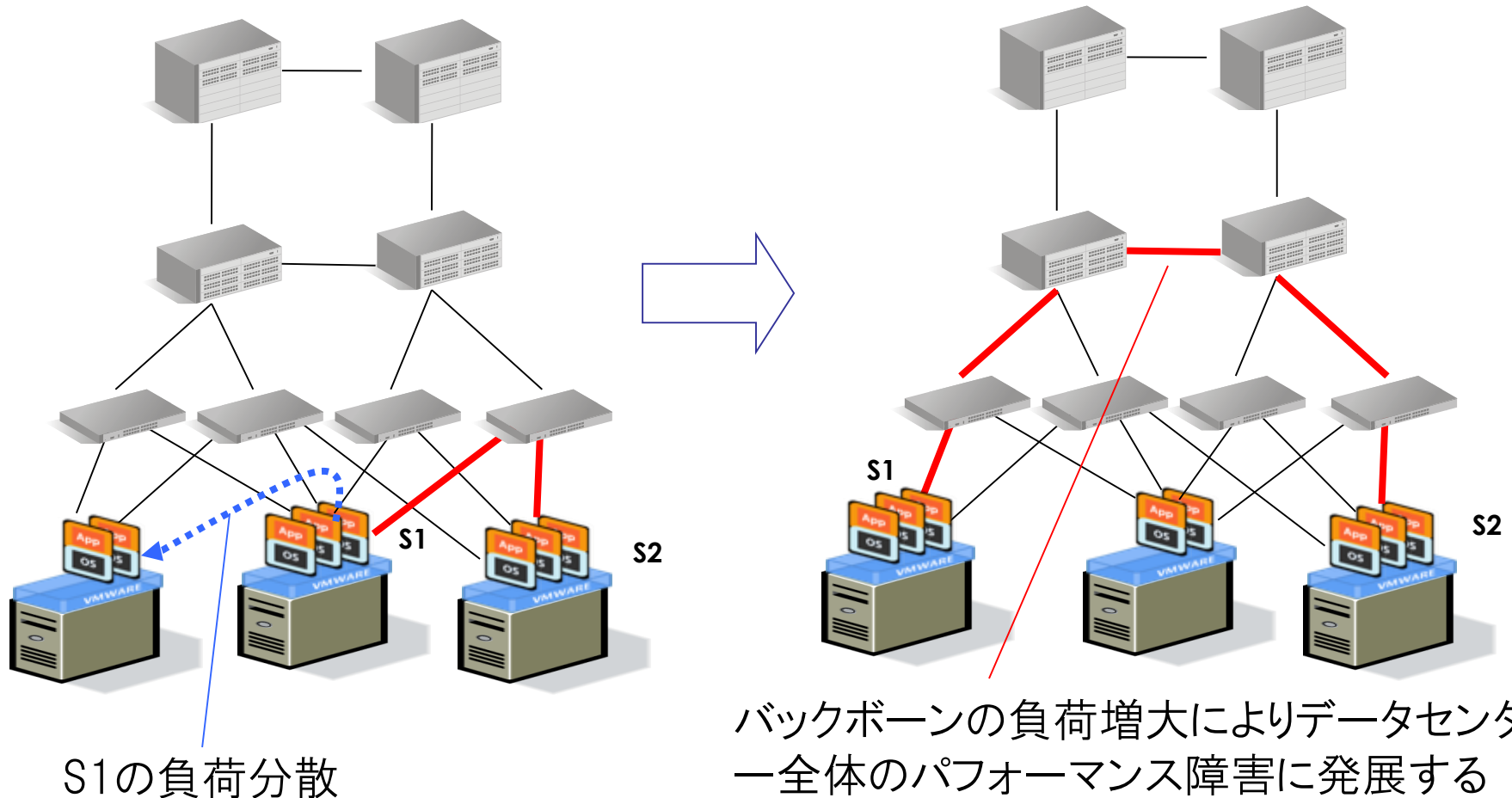


VM UUIDによる
ネットワーク・トラフィックの
フィルタリング

クロス・レイヤーでの
相関関係

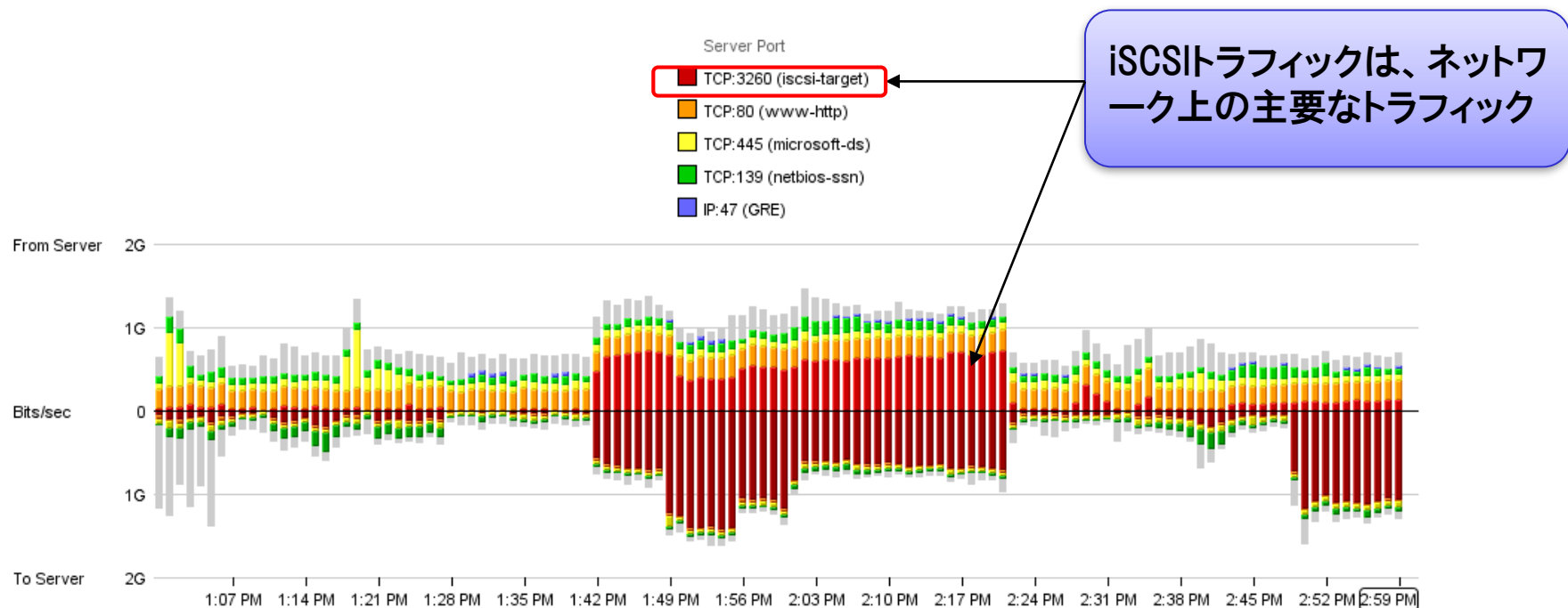


サービスの移動は、データセンター全体のサービス停止につながることもある



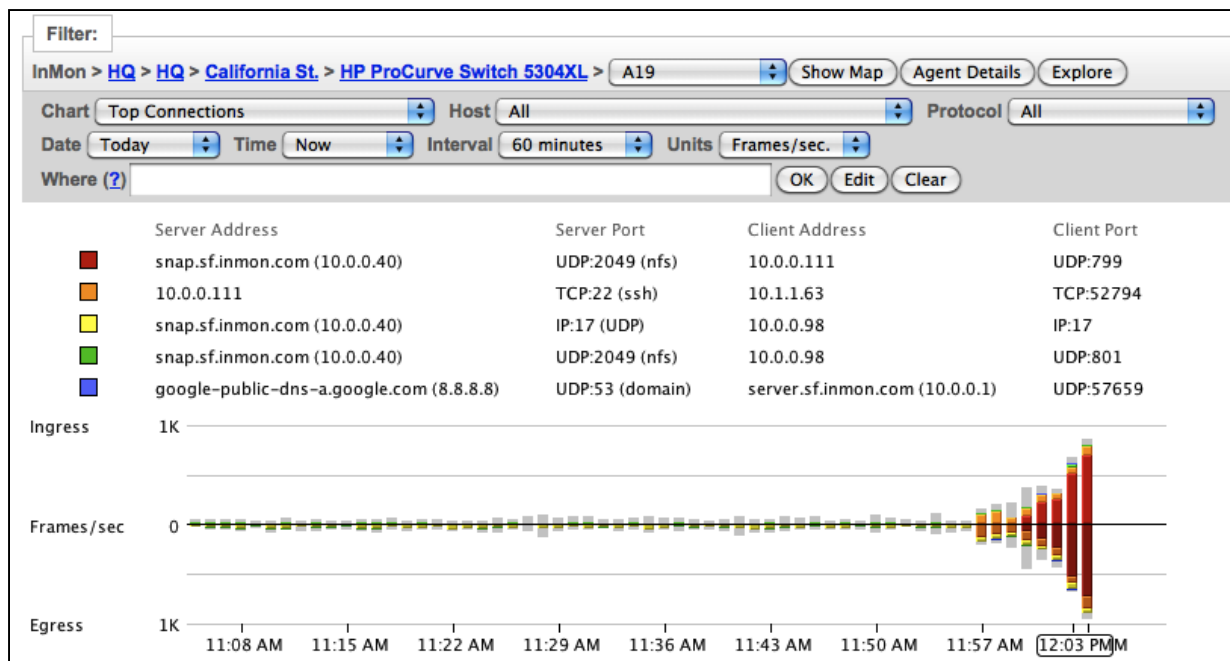
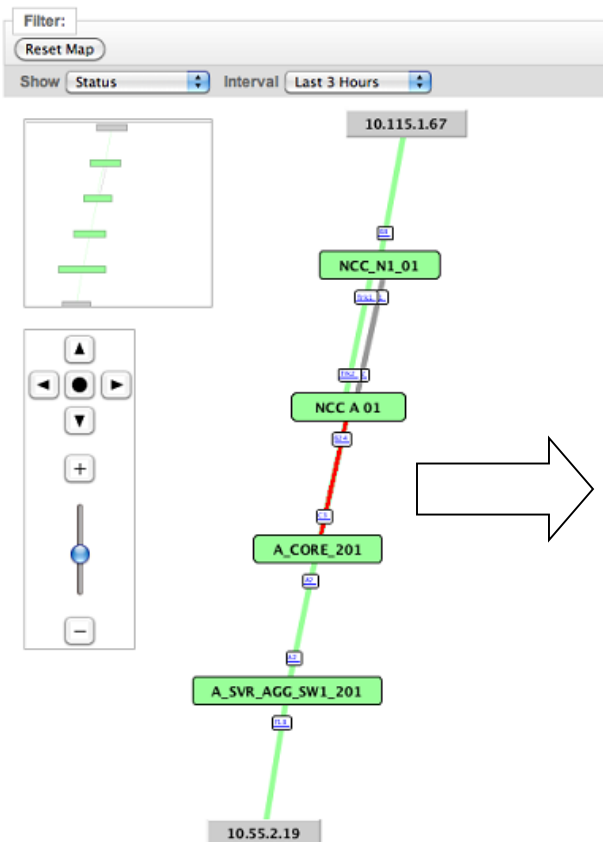
バックボーンの負荷増大によりデータセンター全体のパフォーマンス障害に発展する

ストレージ・トラフィックは、ネットワーク使用率を劇的に増加させ、
SAN や LAN のパフォーマンスに影響を与える。



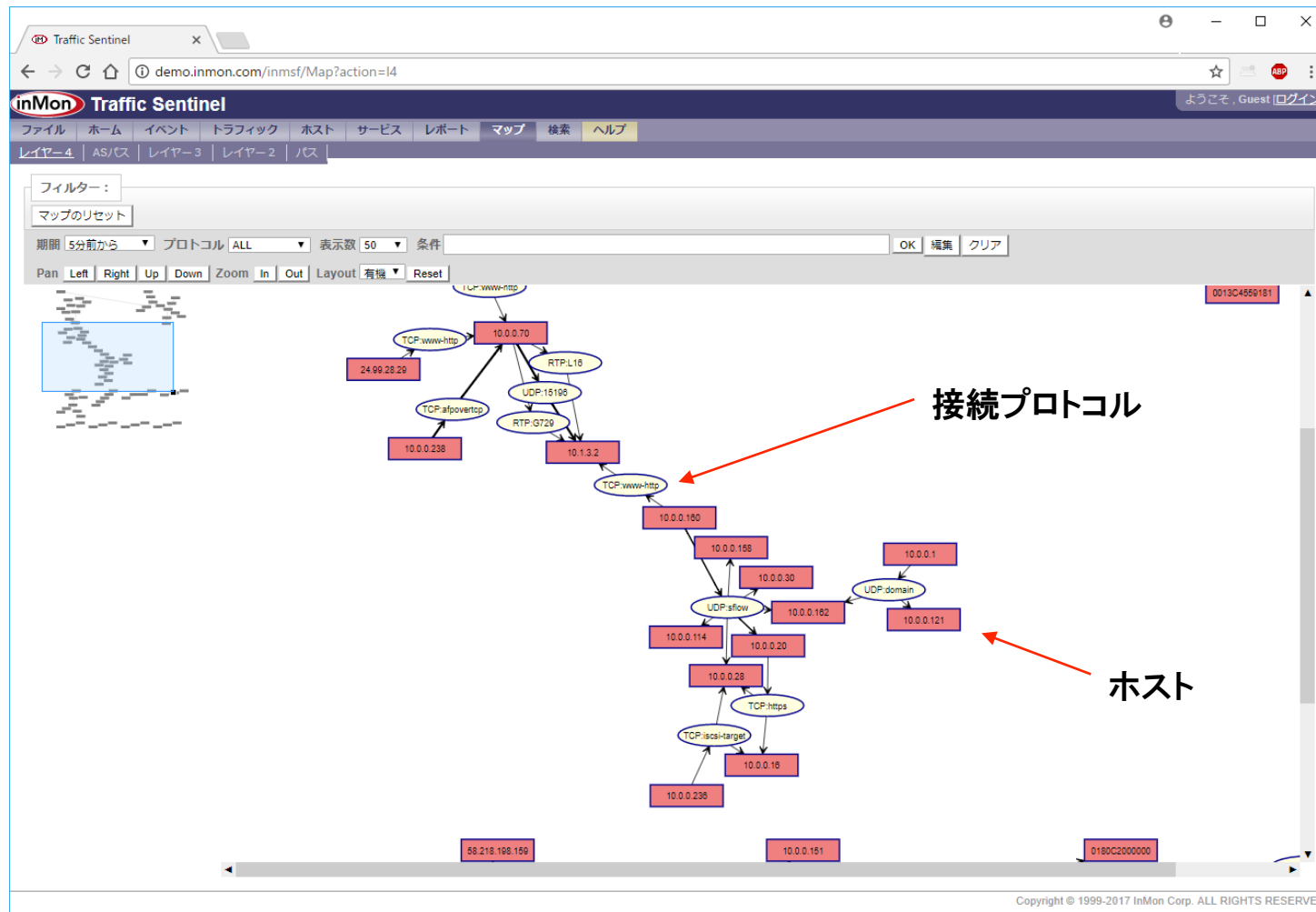
Copyright © 1999-2009 InMon Corp. ALL RIGHTS RESERVED

顧客は最近、iSCSIストレージクラスタをネットワーク上に展開しました。以前はHTTP / Webトラフィックが支配的でしたが、今やストレージトラフィックは支配的です。

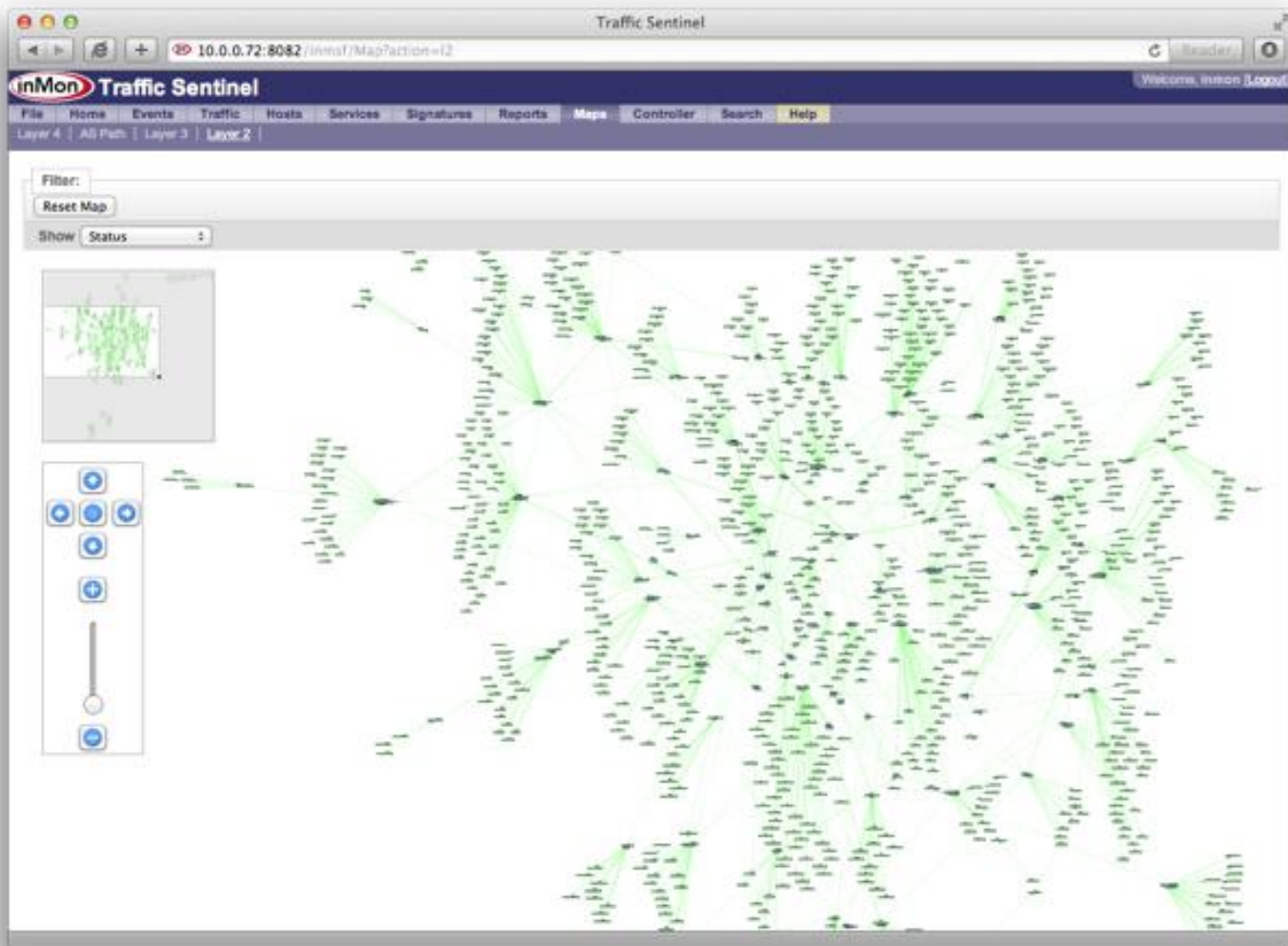


- ・ スイッチ間を経由していくトラフィックの物理的なパスを視覚化
- ・ 輻輳しているリンクを識別
- ・ 混雑しているリンクの輻輳の原因となるコネクション(Top Connections)の識別

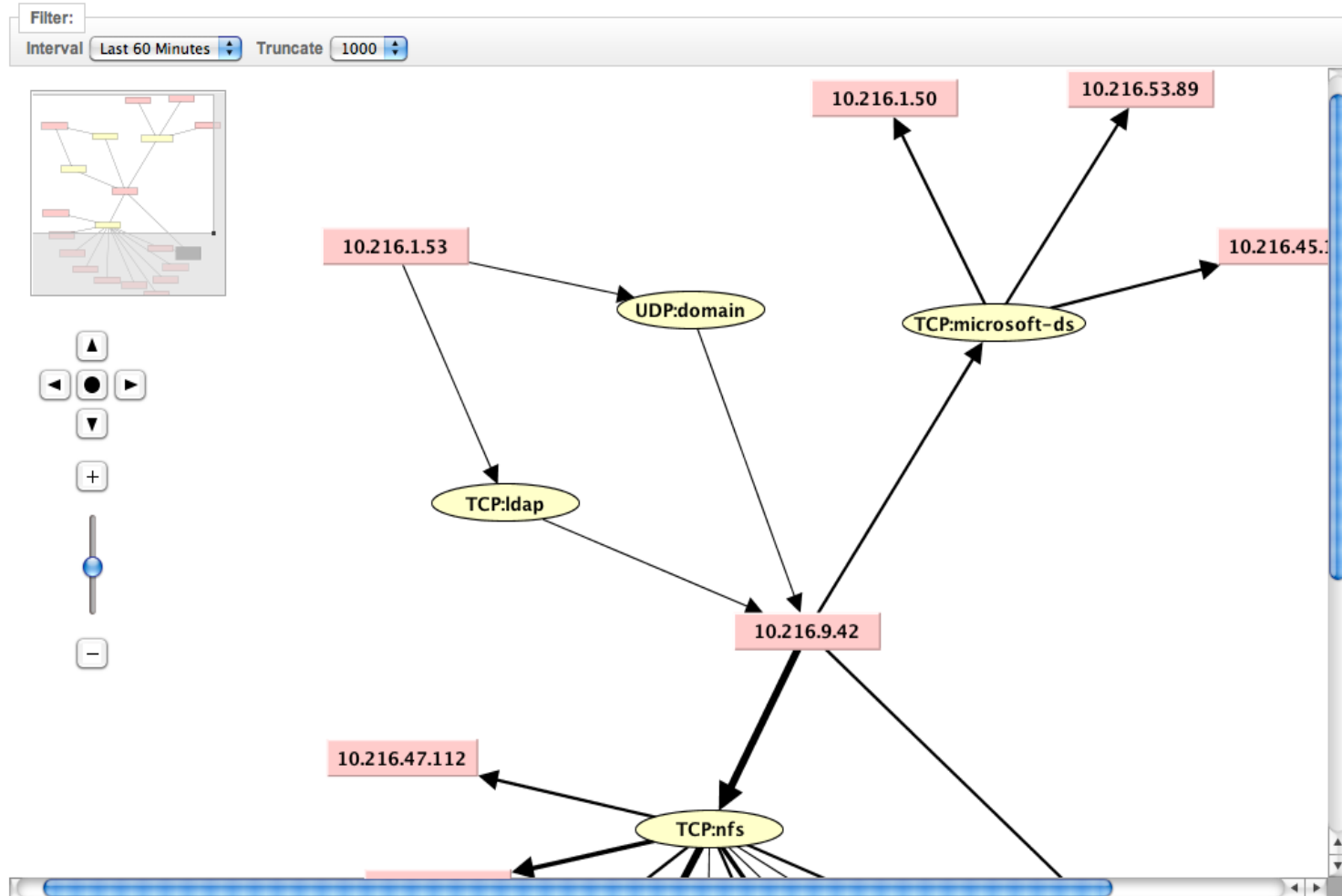
「全体のパスを俯瞰」問題解決の為の情報を入手

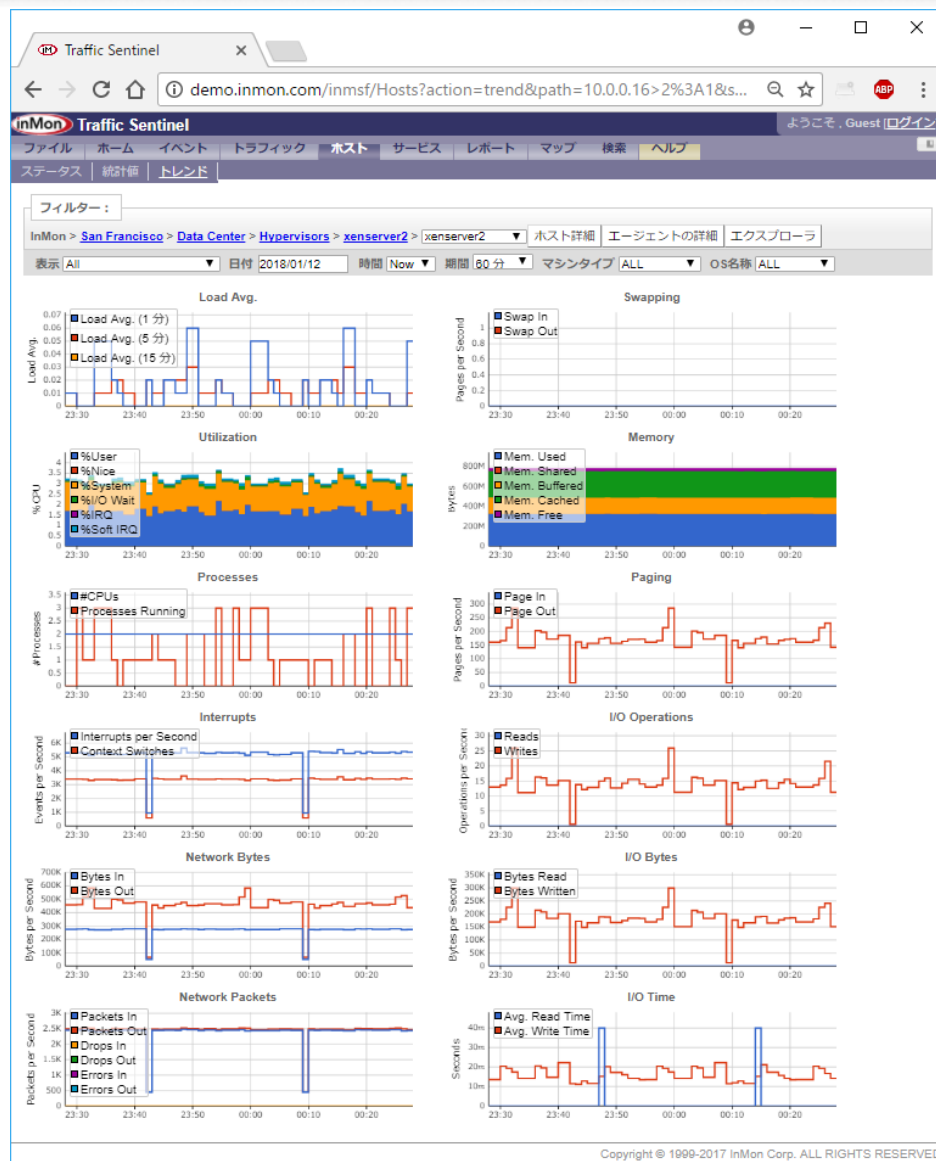


レイヤー2レベルでのコネクション・パス・トレース・マップ:



レイヤー4レベルでの接続プロトコル・マップ:





- ホスト(サーバ)にインストールして統計値を計測
- 計測値は、sFlow(Host sFlow)としてマネージャに送信
- データセンター内の全てのシステムのパフォーマンス計測を集約し表示
 - 計測値を結合
 - 計測値を比較
- このシステムが関連するネットワークリソースや生成されるトラフィックと関連付けることが可能

Host sFlow ダウンロード:

<http://host-sflow.sourceforge.net>

現在、Host sFlow プロジェクト (<http://www.sflow.net>) が、一般的なオペレーティングシステムやアプリケーションにsFlowを実装するのに関連する各種オープンソース・プロジェクトの中心になっている



全てのサーバーのパフォーマンス(Load,CPU,Memory etc)を集約：

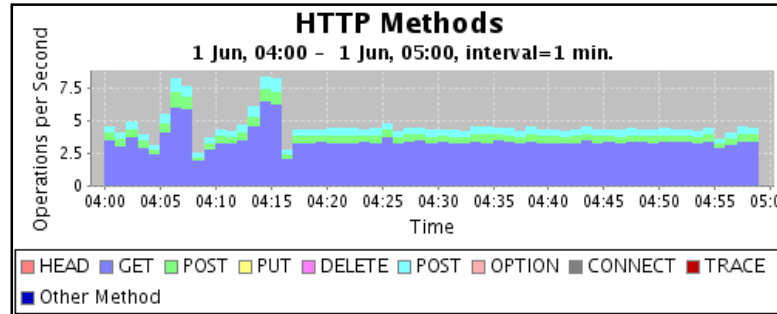
Show Overview 2 Sort Load Avg 1 Truncate 20 Edit Columns											
Counters									Host		
Load Avg 1	%CPU	%Mem.	Swapin/s	Swapout/s	Reads/s	Writes/s	Rx Bytes/s	Tx Bytes/s	Agent	Host Type	Host Name
23.40	100.00	99.44	4.28	0.70	0.78	0.61	25.19	1,274.52	10.219.36.200	Physical	10.219.36.200
7.98	99.53	58.83	0.00	0.00	0.00	0.00	218.30	1,040,385.54	10.219.37.152	Physical	10.219.37.152
7.67	92.86	56.33	0.00	0.00	0.00	0.00	171.86	778,607.24	10.219.37.201	Physical	10.219.37.201
7.52	92.66	55.54	0.00	0.00	0.00	0.00	177.31	817,871.07	10.219.36.72	Physical	10.219.36.72
7.49	94.85	56.33	0.00	0.00	0.00	0.00	170.95	809,419.80	10.219.36.204	Physical	10.219.36.204
7.48	91.73	55.82	0.00	0.00	0.00	0.00	223.14	1,041,724.67	10.219.36.17	Physical	10.219.36.17
7.43	92.02	56.59	0.00	0.00	0.00	0.00	216.85	1,025,722.11	10.219.36.149	Physical	10.219.36.149
7.26	86.14	58.35	0.00	0.00	0.00	0.00	224.49	1,034,503.78	10.219.36.206	Physical	10.219.36.206
7.18	88.49	58.58	0.00	0.00	0.00	0.00	185.79	824,794.10	10.219.36.208	Physical	10.219.36.208
7.17	84.36	56.36	0.00	0.00	0.00	0.00	223.17	1,032,919.56	10.219.36.20	Physical	10.219.36.20
7.15	86.45	62.40	0.00	0.00	0.00	0.00	226.24	1,033,835.55	10.219.36.134	Physical	10.219.36.134
7.10	83.75	60.85	0.00	0.00	0.00	0.00	177.83	833,379.90	10.219.36.136	Physical	10.219.36.136
7.06	85.66	56.11	0.00	0.00	0.00	0.00	168.55	783,295.85	10.219.36.106	Physical	10.219.36.106
7.00	84.72	55.95	0.00	0.00	0.00	0.00	225.33	1,042,690.01	10.219.36.200	Physical	10.219.36.200
7.00	85.90	56.91	0.00	0.00	0.00	0.00	181.16	835,603.10	10.219.36.86	Physical	10.219.36.86
7.00	86.48	60.85	0.00	0.00	0.00	0.00	222.11	1,046,296.23	10.219.36.43	Physical	10.219.36.43
6.96	87.34	56.12	0.00	0.00	0.00	0.00	180.00	826,231.39	10.219.40.112	Physical	10.219.40.112
6.95	82.67	55.58	0.00	0.00	0.00	0.00	215.73	1,020,508.88	10.219.40.36	Physical	10.219.40.36
6.70	81.33	56.61	0.00	0.00	0.00	0.00	173.36	806,747.68	10.219.36.79	Physical	10.219.36.79
6.67	82.72	55.68	0.00	0.00	0.00	0.00	219.71	1,045,871.64	10.219.37.200	Physical	10.219.37.200

20 Mar, 09:22 - 20 Mar, 09:27

sflow counter-push

Per-application counters:

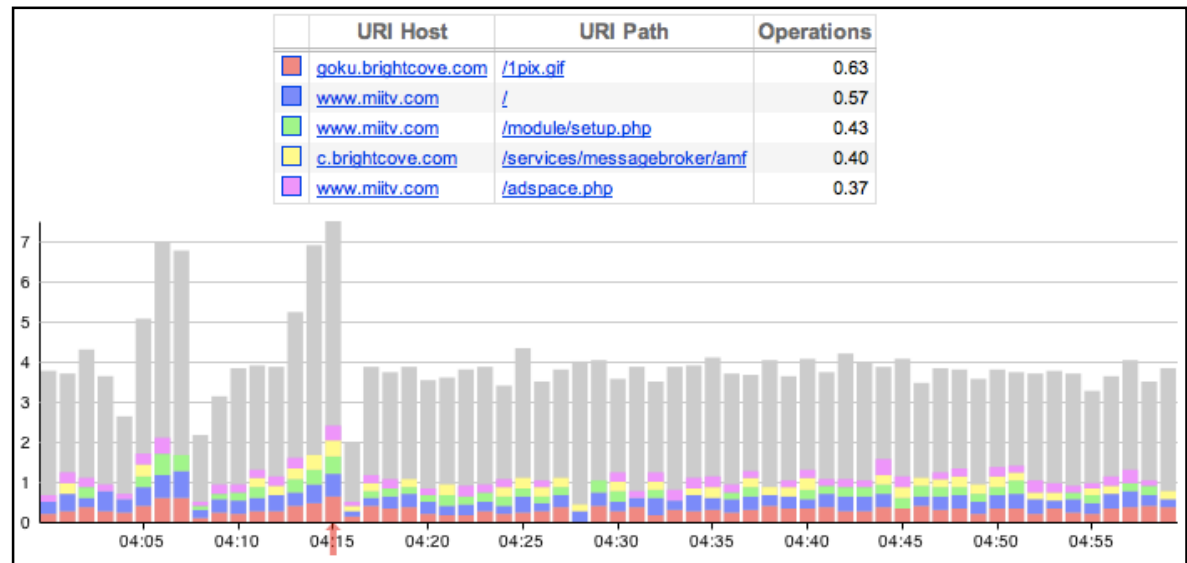
- status codes
- cpu
- memory
- file-descriptors
- connections
- threads
- transactions delayed
- transactions dropped



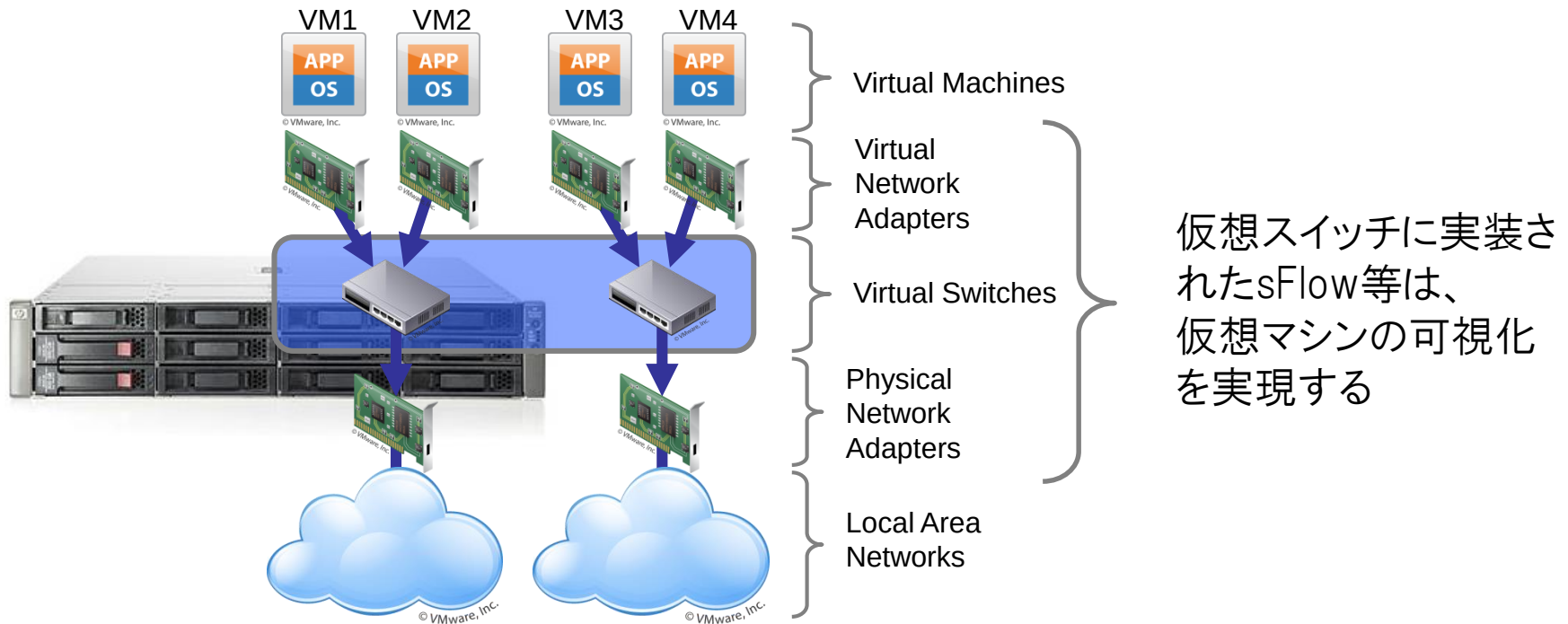
sflow transaction-sampling

Application transactions:

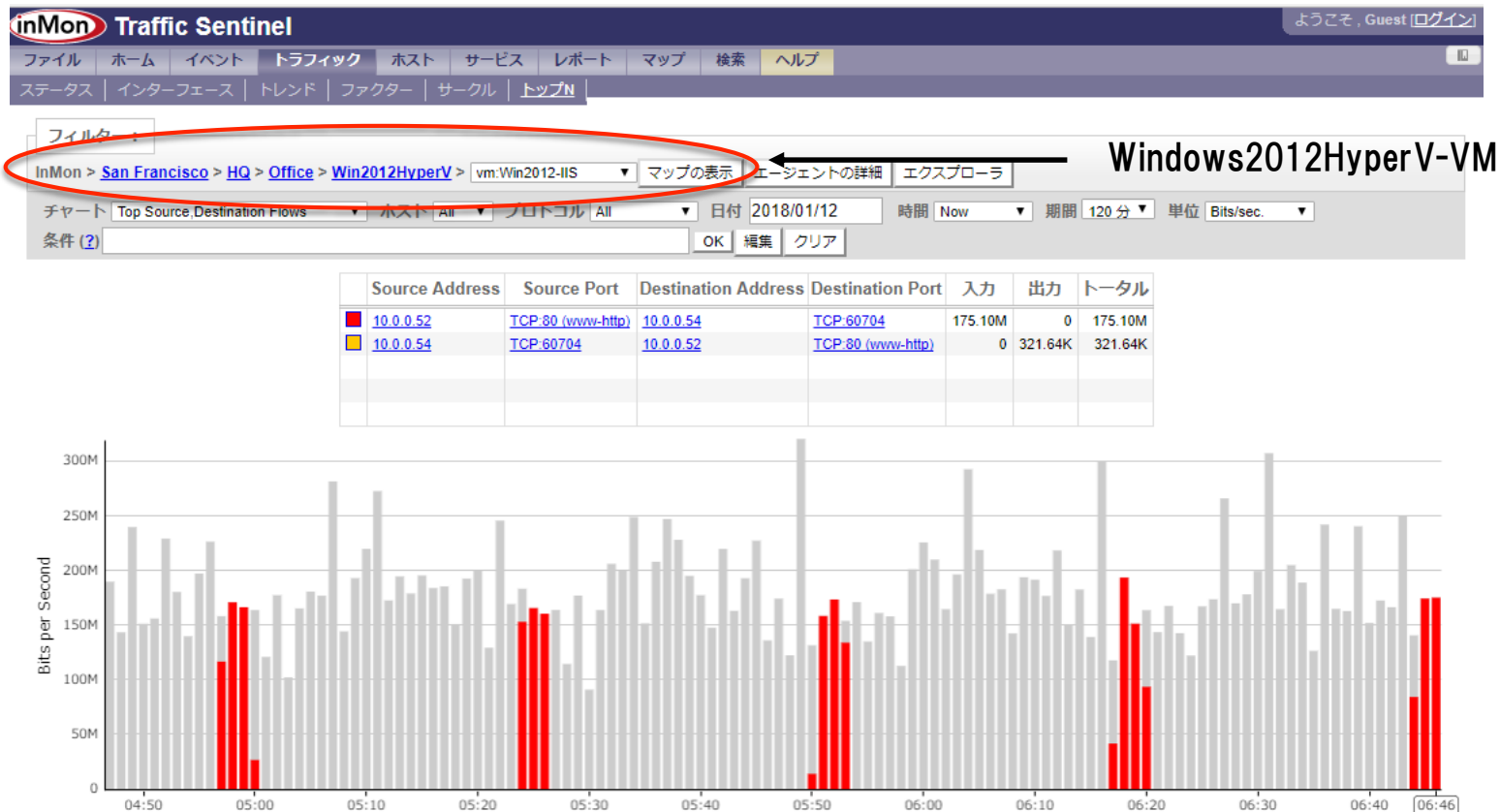
- application
- operation
- client
- server
- initiator
- target
- attributes
- status
- time duration
- bytes sent/received



例: HTTP, memcached, database queries, storage r/w, VoIP calls



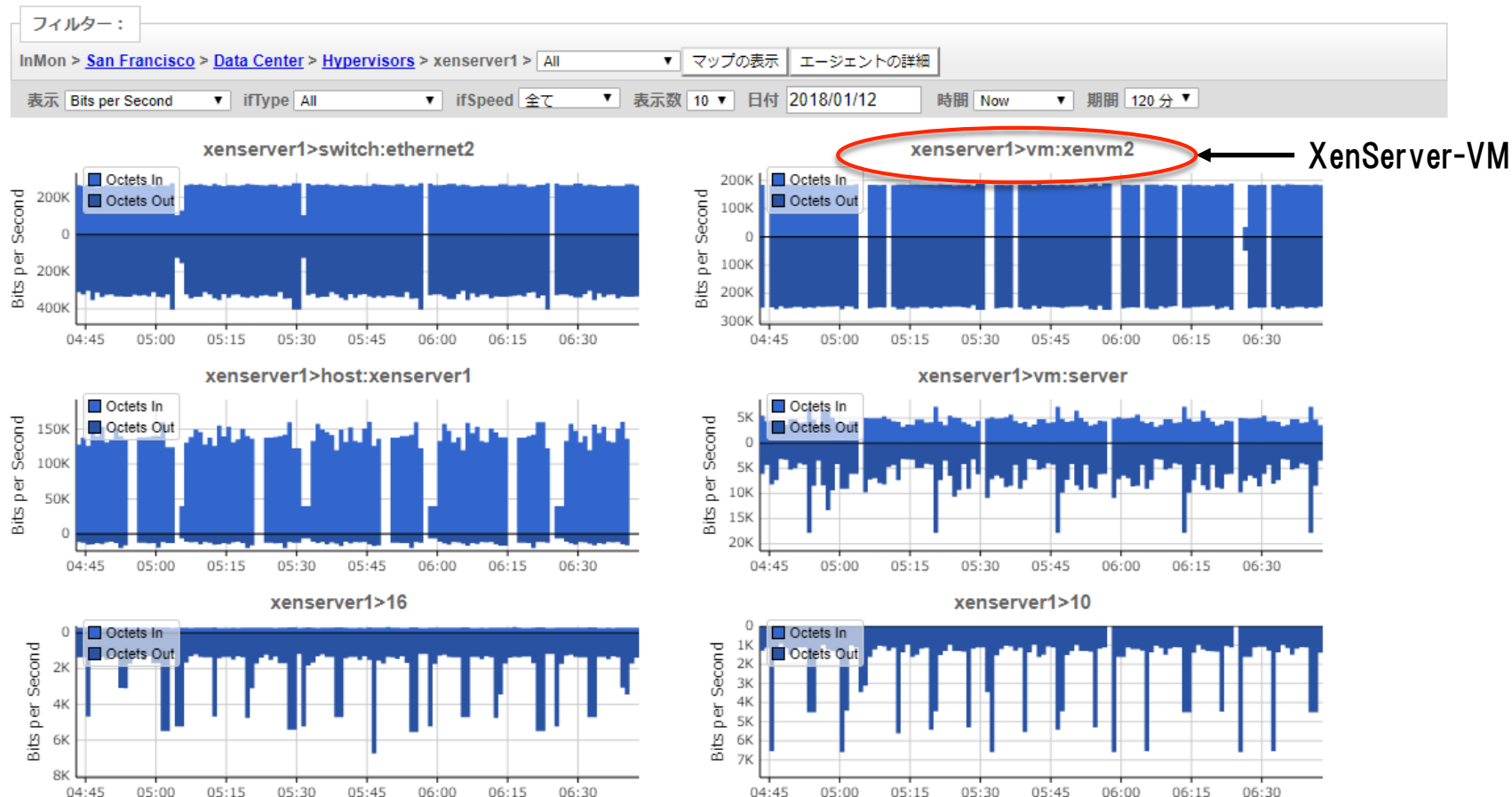
- Open vSwitch (Xen, KVM, Proxmox VE, VirtualBox) : sFlow/NetFlow/IPFIX
- Microsoft Windows 2012 Server Hyper-V : sFlow
- VMWARE vSphere : NetFlow



Windows2012HyperV-VM

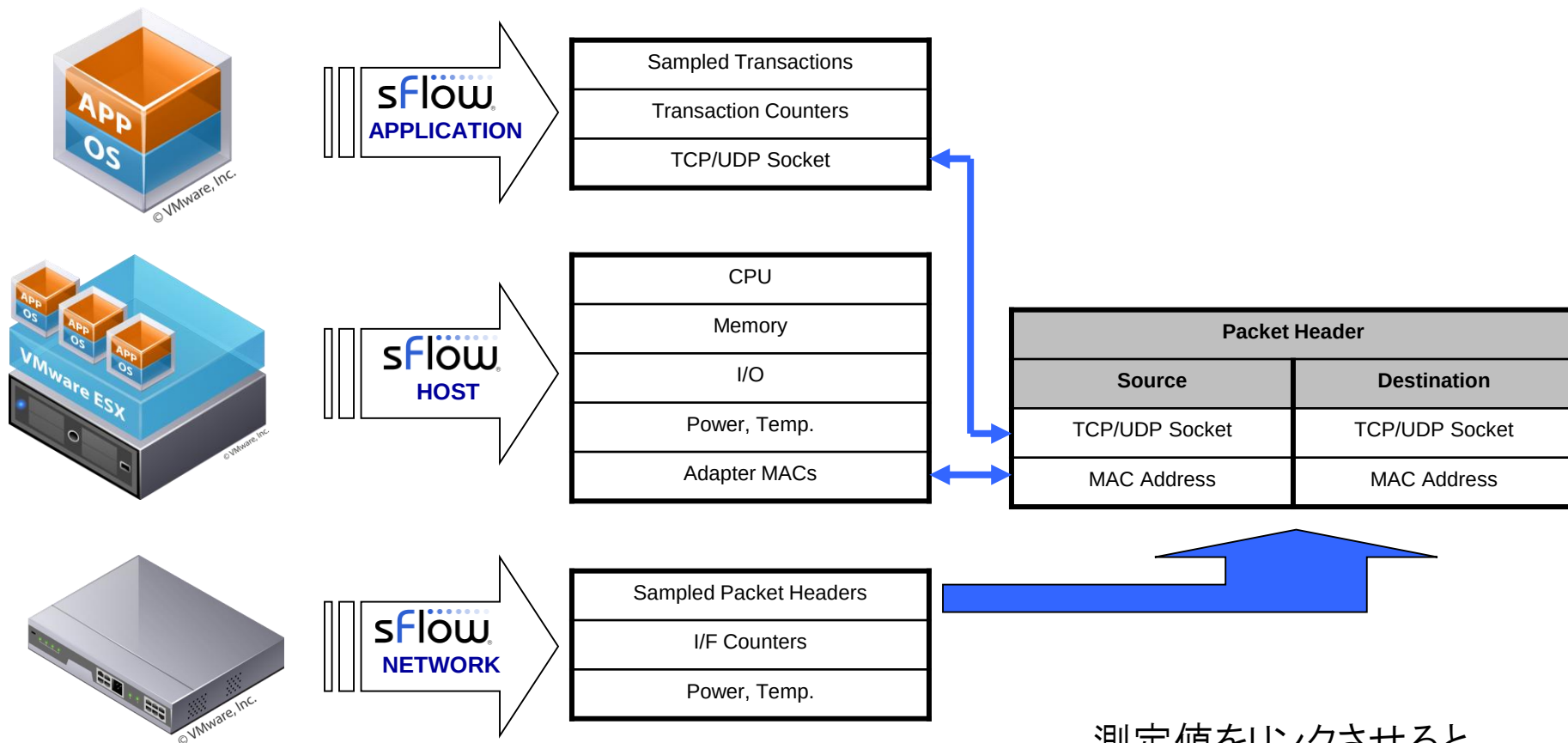
- 全てのトラフィックを可視化
 - VM-VM,
 - VM から 他ホスト
 - Layer 2
 - TCP/UDP
 - IPv6

- 管理されたスイッチトラフィック・データ
 - VLANs
 - Layer 2 priorities (CoS etc)



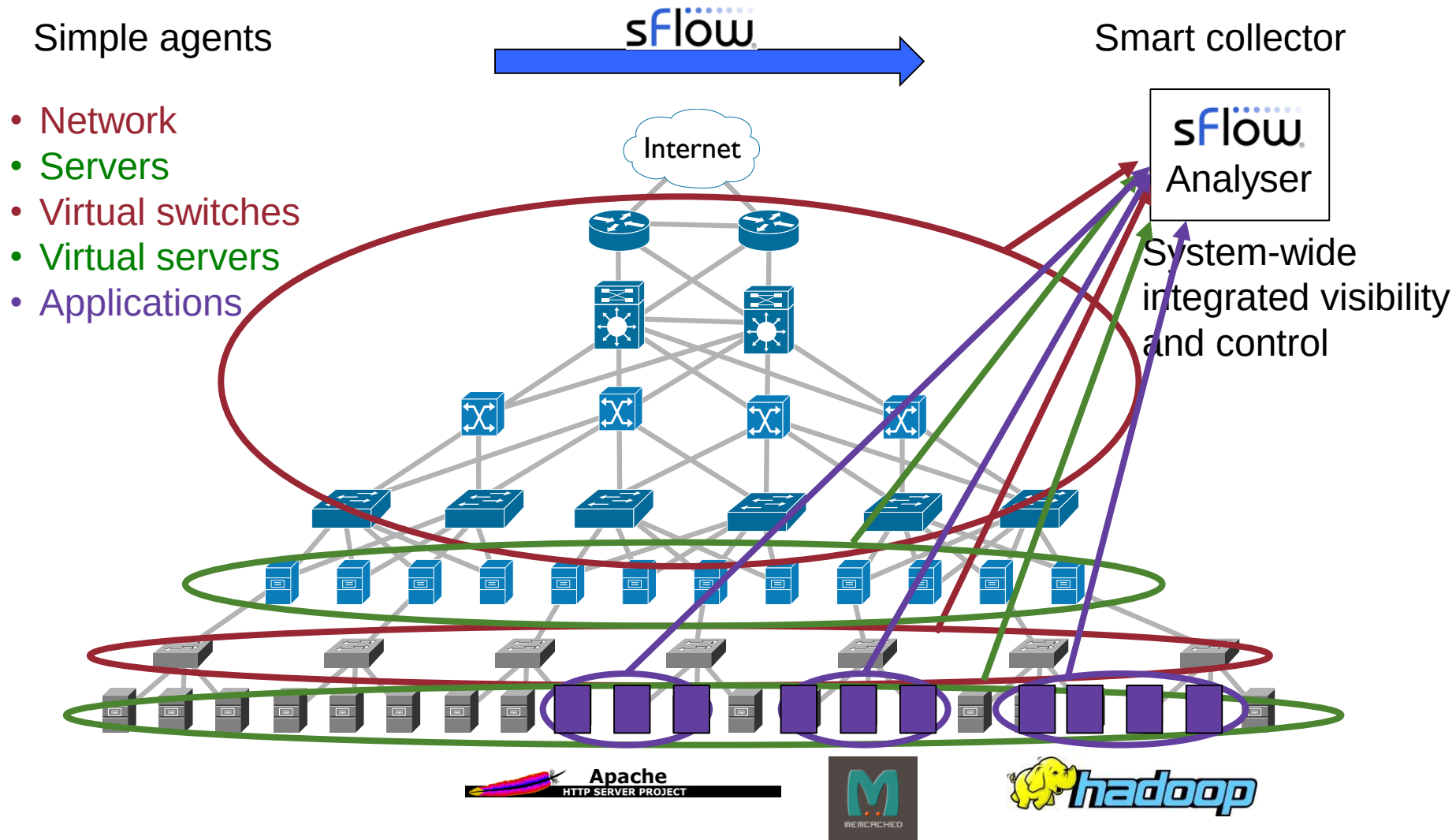
- ネットワーク管理での重要要素であるインターフェース使用率のトレンド
- sFlowは、仮想インターフェースを管理するための現実的な方法
 - sFlowカウンター・エクスポートは、200,000以上の仮想ポートをサポートできるスケーラビリティ

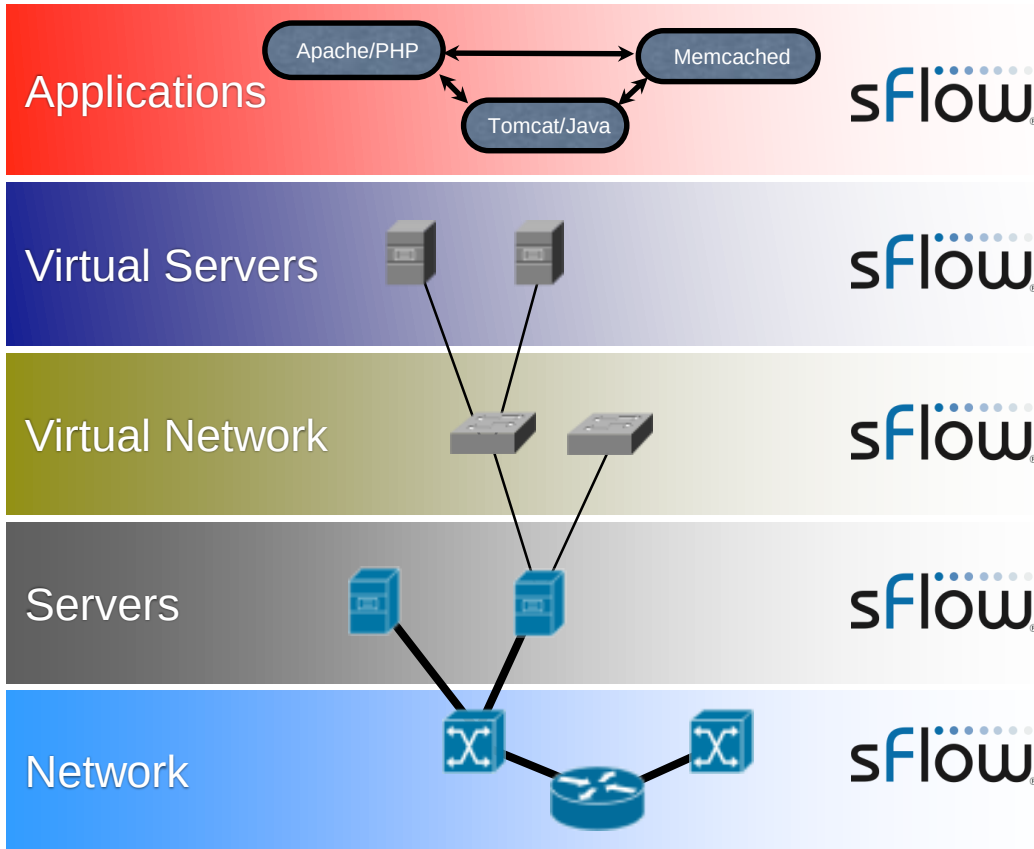
Traffic Sentinelは、各種sFlowデータを統合します



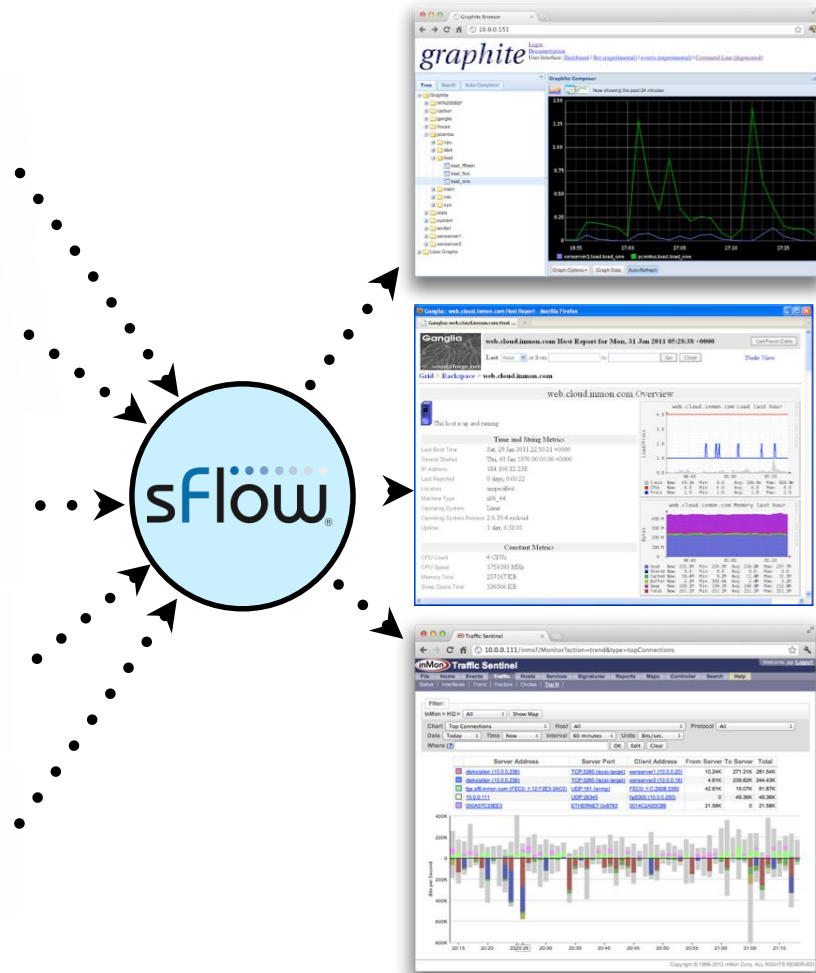
独立したエージェント

測定値をリンクさせると、
データの値が指数関数的に
増加します





Embedded monitoring of all switches, all servers, all applications, all the time



一貫性のある測定が複数の管理ツールで共有される

豊富なレポートテンプレートからのレポート作成・スケジュール化が可能

Recent Traffic Totals by Time

期間別集約されたインターフェース上の最新トップ・トーカーを表示するテーブル

時間	Source Group
07/11/29 15:35	SNMP検証センター
07/11/29 15:35	ネットワークインテグレーション部
07/11/29 15:35	大阪検証センター
07/11/29 15:40	SNMP検証センター
07/11/29 15:40	大阪検証センター
07/11/29 15:40	ネットワークインテグレーション部
07/11/29 15:45	SNMP検証センター

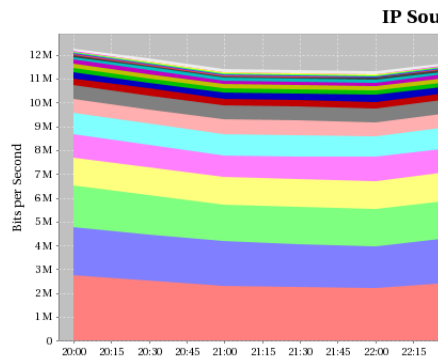
Traffic Totals by Time

期間単位で集約したトップ・トーカーを表示するテーブル

時間	Source Address	Source Port	Destination Address	Destination Port	Layer2 Bytes
18/01/11 20:00	10.0.0.52	TCP:80 (www-http)	10.0.0.54	TCP:60699	52.18 G
18/01/11 20:00	10.0.0.52	TCP:80 (www-http)	10.0.0.54	TCP:60697	51.31 G
18/01/11 20:00	10.0.0.52	TCP:80 (www-http)	10.0.0.54	TCP:60700	51.29 G
18/01/11 20:00	10.0.0.52	TCP:80 (www-http)	10.0.0.54	TCP:60704	50.33 G
18/01/11 20:00	10.0.0.52	TCP:80 (www-http)	10.0.0.54	TCP:60703	50.25 G
18/01/11 20:00	10.0.0.52	TCP:80 (www-http)	10.0.0.54	TCP:60701	47.44 G

Traffic Trend

トップ・カテゴリーによるトラフィックトレンド

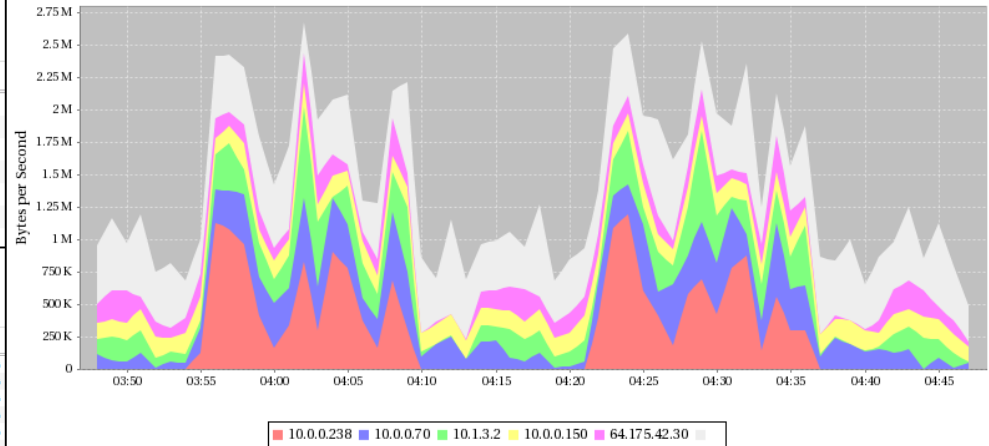


10.0.0.238 10.0.0.70 10.1.3.2 10.0.0.150 64.175.42.30 209.119.35.3
10.0.0.54 10.0.0.151 10.0.0.30 173.194.66.109 10.0.0.239 192.168.

[TXT](#) | [HTML](#) | [イメージ](#)

Source Address

1 12 03:48 - 1 12 04:48, =1

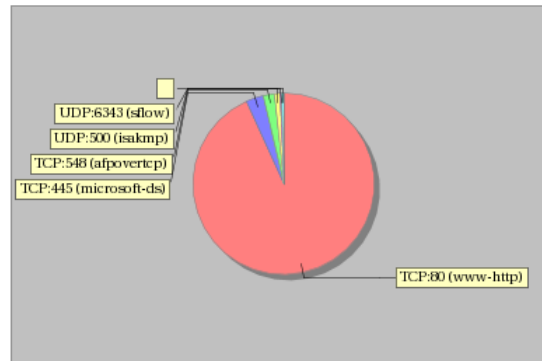


10.0.0.238 10.0.0.70 10.1.3.2 10.0.0.150 64.175.42.30

[TXT](#) | [HTML](#) | [イメージ](#)

Top Protocols

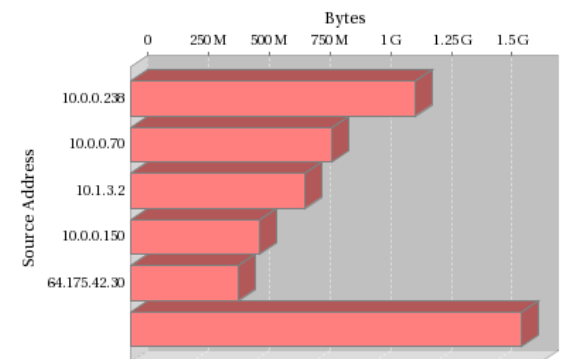
10 14 00:00 - 10 15 00:00



[TXT](#) | [HTML](#) | [イメージ](#)

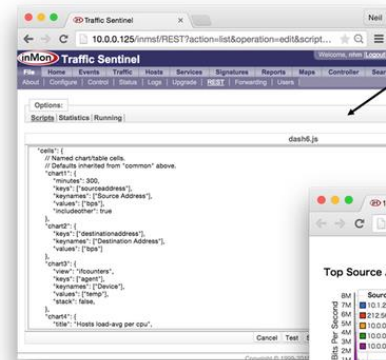
Source Address

1 12 03:52 - 1 12 04:52

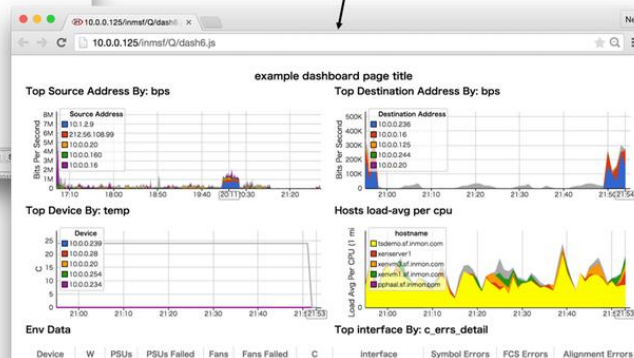


[TXT](#) | [HTML](#) | [イメージ](#)

スクリプト/API連携によるアクセスが可能



スクリプトの開発



URL経由のスクリプトの実行

```
// author: Peter Phaal
// date: 10/12/2012
// version: 1.0
// description: csv Query(view, select, where, interval, sort, n, group, headers)
// ttl: 60
// view: rtraffic
// resultFormat: csv
// authClients: 10.0.0.114

var view = "rtraffic";
var select = typeOf(select) != "undefined" ? select : "sourceaddress.bytes";
var where = typeOf(where) != "undefined" ? where : "";
var interval = typeOf(interval) != "undefined" ? interval : "last50minutes";
var sort = typeOf(sort) != "undefined" ? sort : "bytes";
var n = typeOf(n) != "undefined" ? n : "10";
var group = typeOf(group) != "undefined" ? group : "";
var headers = typeOf(headers) != "undefined" ? headers : false;

var max_n = 100;
var max_range = 180;

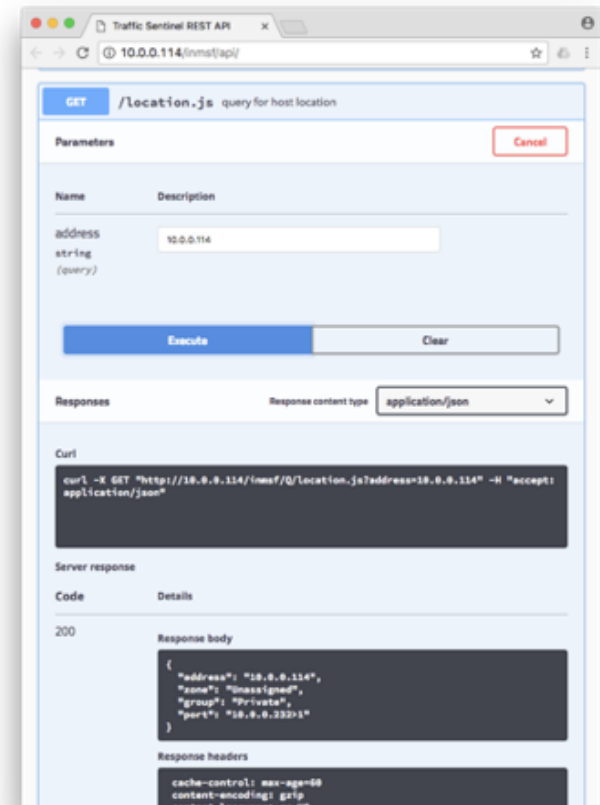
try {
  @select throw "missing select";
  @interval throw "missing interval";
  @sort throw "missing sort";
  @n throw "missing n";
  @n <= 0 throw "error n <= 0";
  @n > max_n throw "error n > max_n";
  var q = QueryTop(view, select, where, interval, sort, n, group);
  var times = q.timeRange();
  var now = (new Date()).getTime();
  @Math.abs(now - times[0].getTime()) / 60000 > max_range throw "interval range";
  @Math.abs(now - times[1].getTime()) / 60000 > max_range throw "interval range";
  var table = q.run();
  table.printCSV(headers);
} catch(err) {
  print(err) + "\n";
}
```

スクリプトの開発

URL経由のスクリプトの実行

```
demo.inmon.com/nmsf/q?select=sourceaddress.bytes&where=10.0.0.114&interval=last50minutes&sort=bytes&n=10&group=&headers=false
```

REST API ブラウザ



- ・ トラフィックの内容に対ししきい値を設定し超過時にイベントを発生させる
 - しきい値: トラフィック(プロトコル・アドレス・グループなど)に対して設定
 - スケジュール化し、超過時にイベントを発生させる

inMon Traffic Sentinel ようこそ, administrator [ログアウト]

ファイル ホーム イベント トラフィック セキュリティ レポート マップ 検索

表示 | クエリ | 編集 | スケジュール | インストール | スクリプト |

フィルター:

カテゴリー Miscellaneous セクション Detect Report - MSYS

Detect Report - MSYS

セクション DoS攻撃検知レポート

説明 ICMP ECHOを10,000フレーム/秒受信する大阪支

キーの選択 time,destinationaddress,ipprotocol

値 fps

期間 last5minutes

グループ 5

名前解決 no

条件 (オプション) ipprotocol=IP:1 & destinationzone = 大阪支店

しきい値 10000

例: 拠点内のサーバーでICMP ECHOを10,000フレーム/秒受信した場合にDoS攻撃と判断しイベントを発生し、レポートを作成する。

Traffic Sentinel

DoS攻撃検知レポート

ICMP ECHOを10,000フレーム/秒受信する大阪支店のサーバーを表示

時間	Destination Address	IP Protocol	fps
07/12/13 13:00	traffic.osk.ps.msol.co.jp	IP:1 (ICMP)	51.587
07/12/13 13:00	pixy.osk.ps.msol.co.jp	IP:1 (ICMP)	10.073

ページが表示されました

マイ コンピュータ 100%

- 豊富なテンプレートを編集して、カスタマイズ・レポートが作成可能
 - 文言・表示情報・表示情報のフィルタリングなどの編集が可能
 - 定型レポートはスケジュール化

The screenshot displays the inMon Traffic Sentinel web interface. The left panel shows the 'Customize Report' configuration for a 'Miscellaneous' category report. The right panel shows the resulting report output for 'Customize Historical Report'.

Configuration (Left Panel):

- セクション: カスタマイズ・ヒストリカル・レポート
- 説明: 昨日の上位使用者を表示(丸紅情報システムズ大阪支店)
- キーの選択: ipsource
- 値: Bits per Second
- 表示数: 10
- 期間: yesterday
- 名前解決: Yes
- 前回のランクの表示: No
- 条件 (オプション): sourcezone = 大阪支店

Report Output (Right Panel):

カスタマイズ・ヒストリカル・レポート

昨日の上位使用者を表示(丸紅情報システムズ大阪支店)

IP Source	Bits per Second
traffic.osk.ps.msol.co.jp	79.210 K
nhosaka.osk.ps.msol.co.jp	11.130 K
192.168.71.90	2.728 K
bs350t.osk.ps.msol.co.jp	1.277 K
192.168.71.75	974.704
justice.osk.ps.msol.co.jp	612.288
192.168.71.98	586.584
192.168.71.54	177.184
pixy.osk.ps.msol.co.jp	137.624
nhserver.osk.ps.msol.co.jp	127.328
	322.064

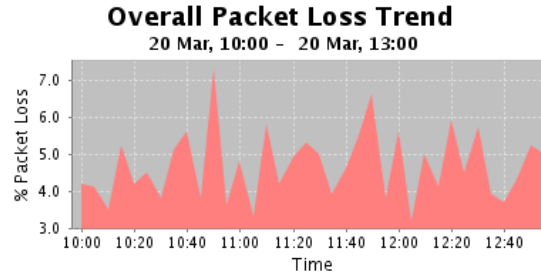
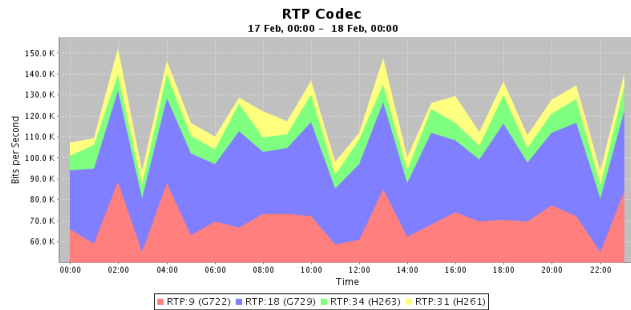
12月12日 00:00 - 12月13日 00:00

Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED

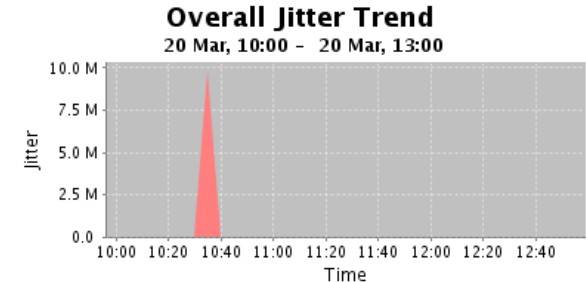
ページが表示されました

インターネット 100%

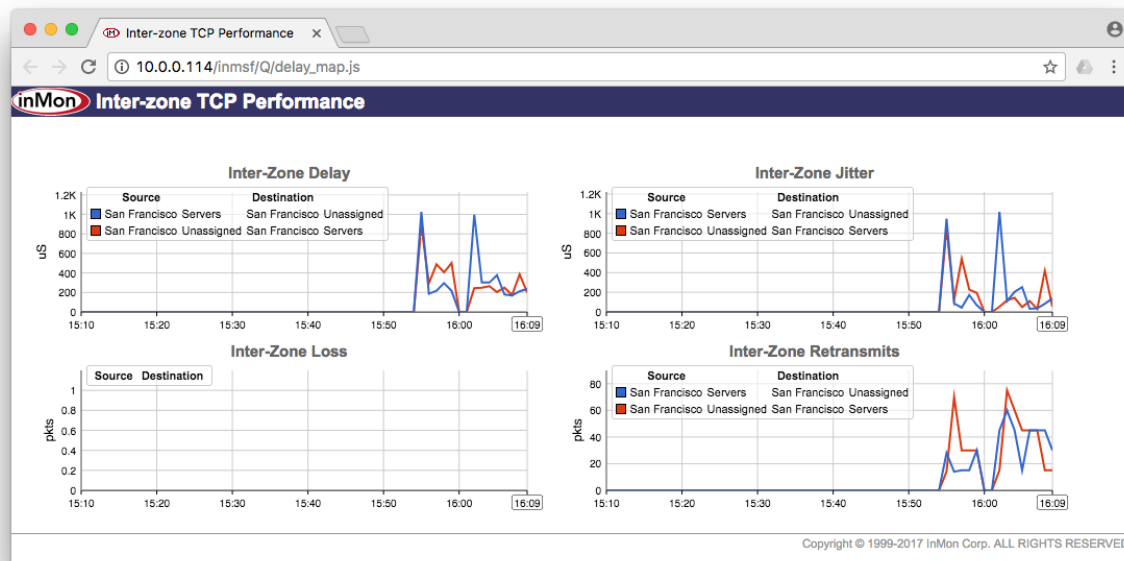
VoIPは、RTPによって提供されます。
sFlowによってRTPのCodec、QoSの把握が可能です。

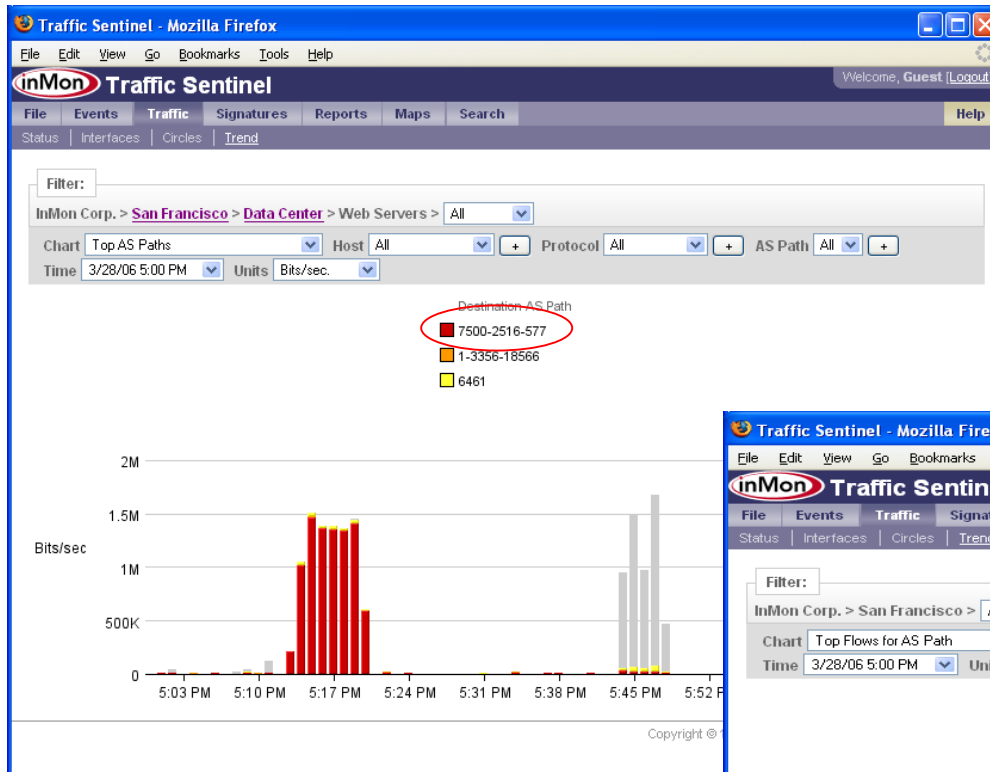


Packet loss は、均一的に継続

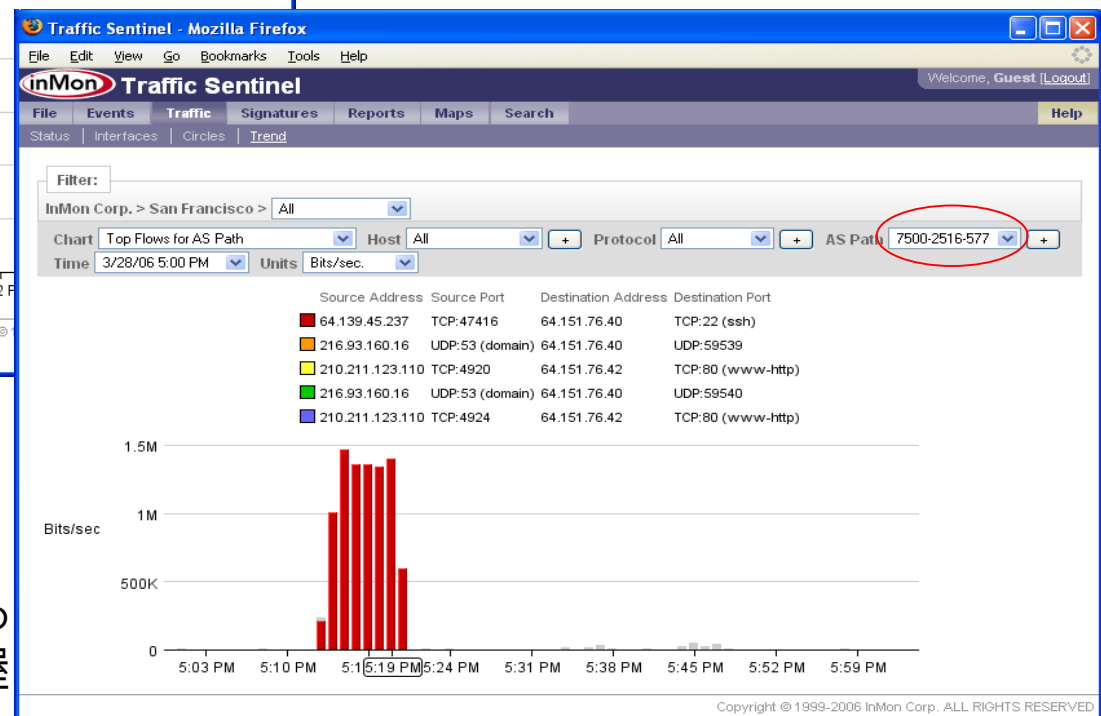


しかし、Jitterは10:35にスパイク





7500-2516-577 は、最も激しく使用されているASパスで、また、パスも長い。



このASパスによって転送されている
フローの把握

ポートスキャンや新種のウイルス・ワームの検知：

Filter:

Category: Security Report: Compromised local hosts Time: Latest

Section: Port Scanning Activity PDF HTML Edit Schedule Edit Report

Port Scanning Activity

Identify port scanning activity associated with worm propagation.

New Hosts

IP Source	Destination Port	# Destinations
-----------	------------------	----------------

Cached Hosts

IP Source	Destination Port	# Destinations	First Seen	Last Seen
172.16.144.52	TCP:445	446	3/13/06 5:30 PM	3/28/06 2:15 PM
172.16.144.52	TCP:139	331	3/13/06 5:30 PM	3/28/06 2:15 PM

172.16.144.52 は、TCPポート445や139を使用して、多くのホストとの接続が測定された。

監査：フローログ – サーバーへのTELNET接続者のログ

Traffic Sentinel – Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

inMon Traffic Sentinel ようこそ, Administrator [ログアウト]

ファイル イベント トラフィック セキュリティ レポート マップ 検索 ヘルプ

表示 | 実行 | 編集 | スケジュール | スクリプト |

フィルター:

カテゴリー Traffic レポート General Queries セクション Historical Traffic 最新の表示

戻る PDF HTML

TELNET監査ログ

TELNETを使用したクライアントの分析

時間	Server Address	Server Port	IP Protocol	Client Address	Frames	Bytes
06/07/01 0:00	192.168.10.33	TCP:23 (telnet)	IP:6 (TCP)	192.168.116.240	2,584	109,990
06/07/01 0:00	192.168.114.18	TCP:23 (telnet)	IP:6 (TCP)	192.168.71.94	408	20,973
06/07/01 0:00	192.168.71.97	TCP:23 (telnet)	IP:6 (TCP)	192.168.71.94	256	10,240
06/07/01 0:00	traffic.osk.ps.msol.co.jp	TCP:23 (telnet)	IP:6 (TCP)	192.168.114.18	52	2,243
06/07/01 0:00	traffic.osk.ps.msol.co.jp	TCP:23 (telnet)	IP:6 (TCP)	192.168.110.53	32	1,833
06/07/01 0:00	203.141.42.73	TCP:23 (telnet)	IP:6 (TCP)	192.168.71.94	31	3,249
06/07/01 0:00	turbo.osk.ps.msol.co.jp	TCP:23 (telnet)	IP:6 (TCP)	192.168.70.21	5	204
06/07/01 0:00	142.240.92.29	TCP:23 (telnet)	IP:6 (TCP)	192.168.71.94	3	144
06/07/01 0:00	192.168.10.33	TCP:23 (telnet)	IP:6 (TCP)	192.168.116.235	0	0
06/07/01 0:00	192.168.71.36	TCP:23 (telnet)	IP:6 (TCP)	kataka.osk.ps.msol.co.jp	0	0
06/07/01 0:00	192.168.10.33	TCP:23 (telnet)	IP:6 (TCP)	192.168.116.233	0	0

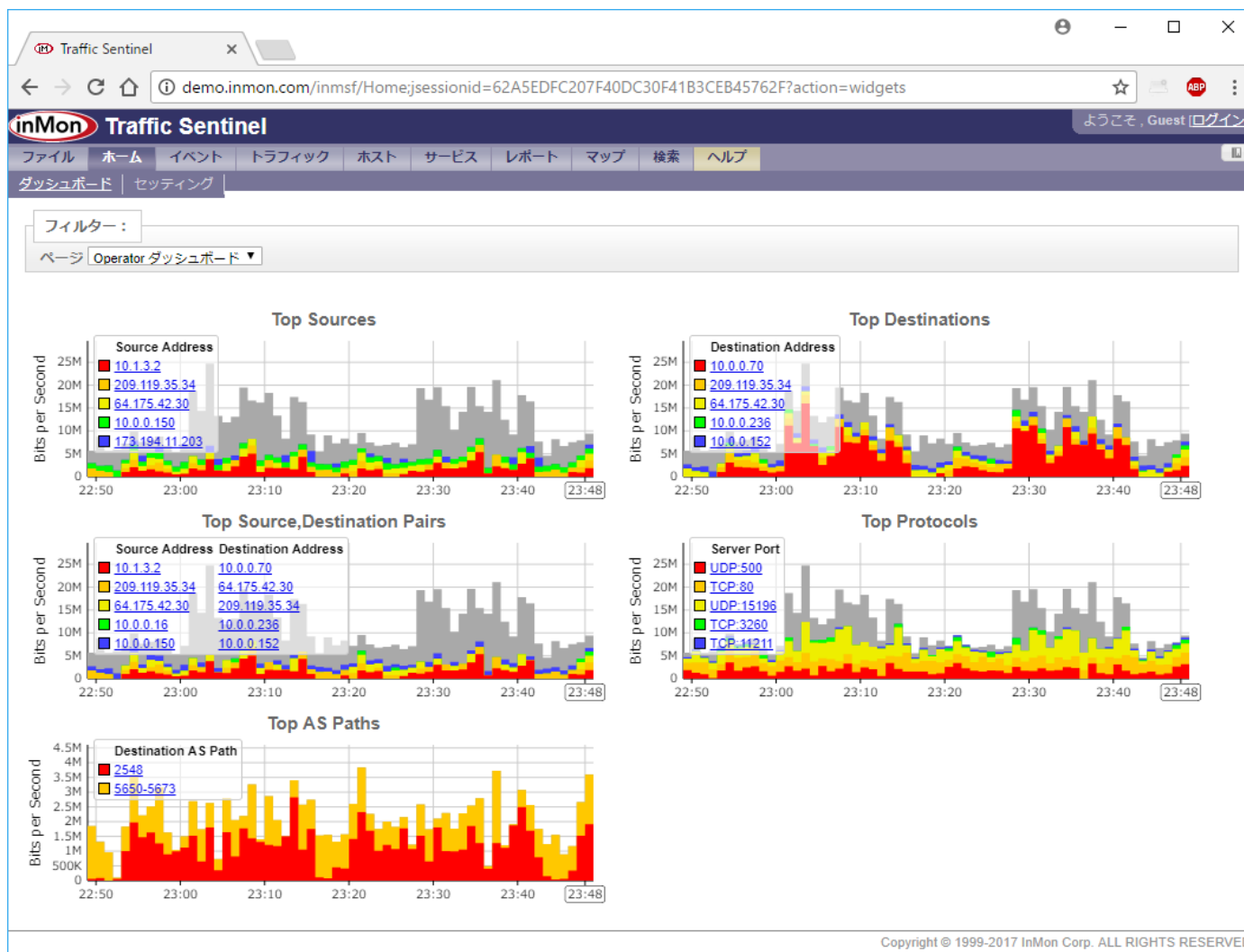
7月1日 00:00 - 8月1日 00:00

Copyright © 1999-2006 InMon Corp. ALL RIGHTS RESERVED

特定のサーバーへのアクセスや特定のクライアントの使用内容の把握

ログインユーザー毎にダッシュボードが作成できます。

使用頻度の高いグラフ等を任意に組み合わせて自分用画面が作成できます。

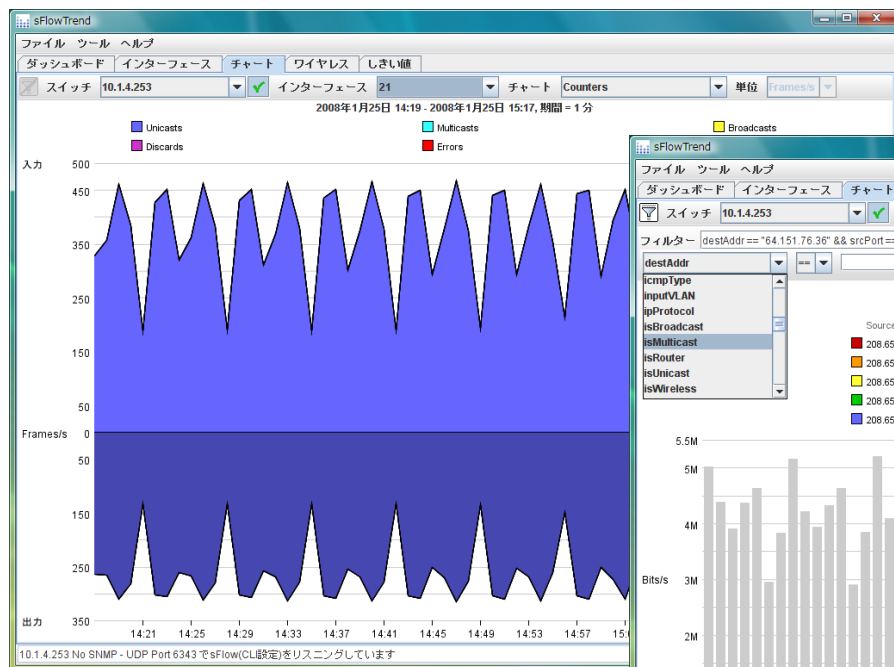


sFlowTrend™ は、フリー（無償）のツールです。

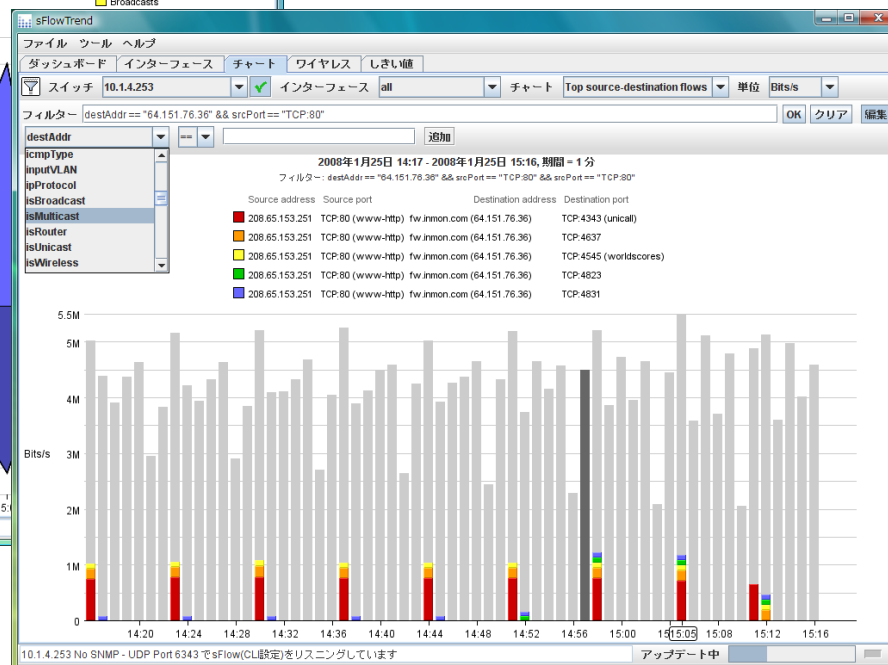
グラフィカルな sFlow® コレクターで、トポトーカーやインターフェースカウンタを経過時間に渡りプロットします。

弊社のsFlowTrendホームページより、ダウンロード・インストールできます。

<http://www.flownetsecure.com/products/sflowtrend/>



sFlowTrend
InMon Corp.



sFlowTrend-Proは、sFlowTrendの機能強化商用版です。

sFlowTrendと比較し、

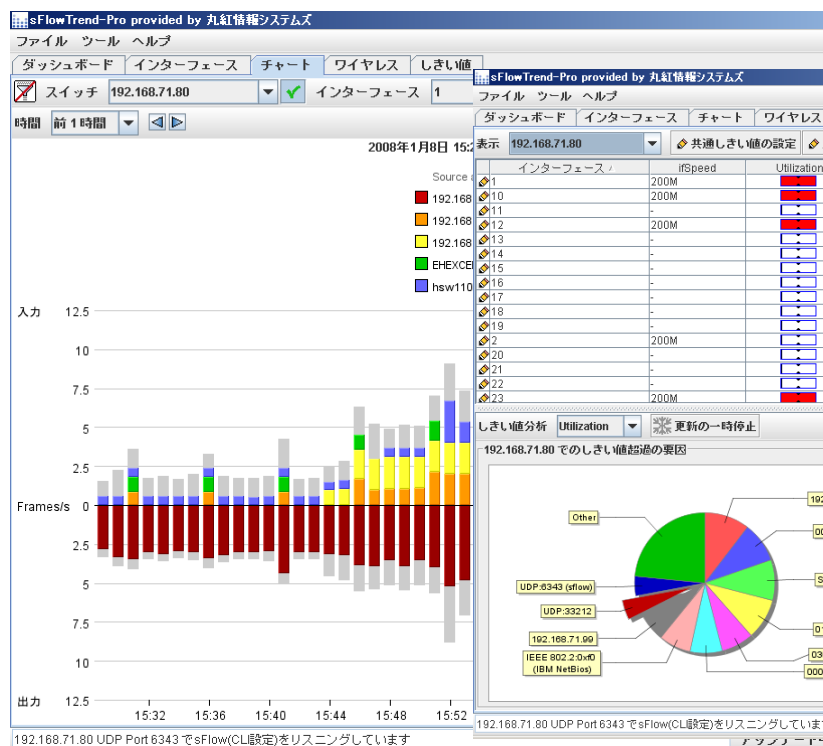
複数台のスイッチのモニタリング(10台程度まで)

データの長期保存(数週間程度)

時間フィルタリング

などの機能が拡張されています。

標準価格は、90万円です。



■ InMonTrafficSentinel評価用ライセンス

必要であれば、InMonTrafficSentinelのソフトウェアと評価用(1か月)ライセンスを提供しますので、自社環境にて評価いただくことが可能です。ご依頼ください。

ハードウェア/OSは、ご用意ください。

評価であれば、パソコンレベルで評価いただくことが可能です。

以下、参考スペックになります。

CPU:Core2Duoクラス以降

Memory:4GB以上 / Disk:100GB以上 / NIC : 1Gbps

OS:Red Hat Enterprise Linux or CentOS or Fedora

※H/Wスペックについては監視対象規模やサンプリングレート、データ保存期間などに依存します。

■ InMonTrafficSentinelデモンストレーションサイト

<http://demo.inmon.com/>

■ InMon製品紹介WEBサイト(弊社サイト)

<http://www.flownetsecure.com/>

■ お問い合わせ先

株式会社フローネットセキュア 出野(いでの)宛

TEL:075-555-3482 Mobile:070-2305-1962

eMail : IDENO@flownetsecure.com