マネージャブルな仮想化

Interop Tokyo 2010

ShowNet NOC Team

INTEROP
TOKYO | 7-11 JUNE, 2010

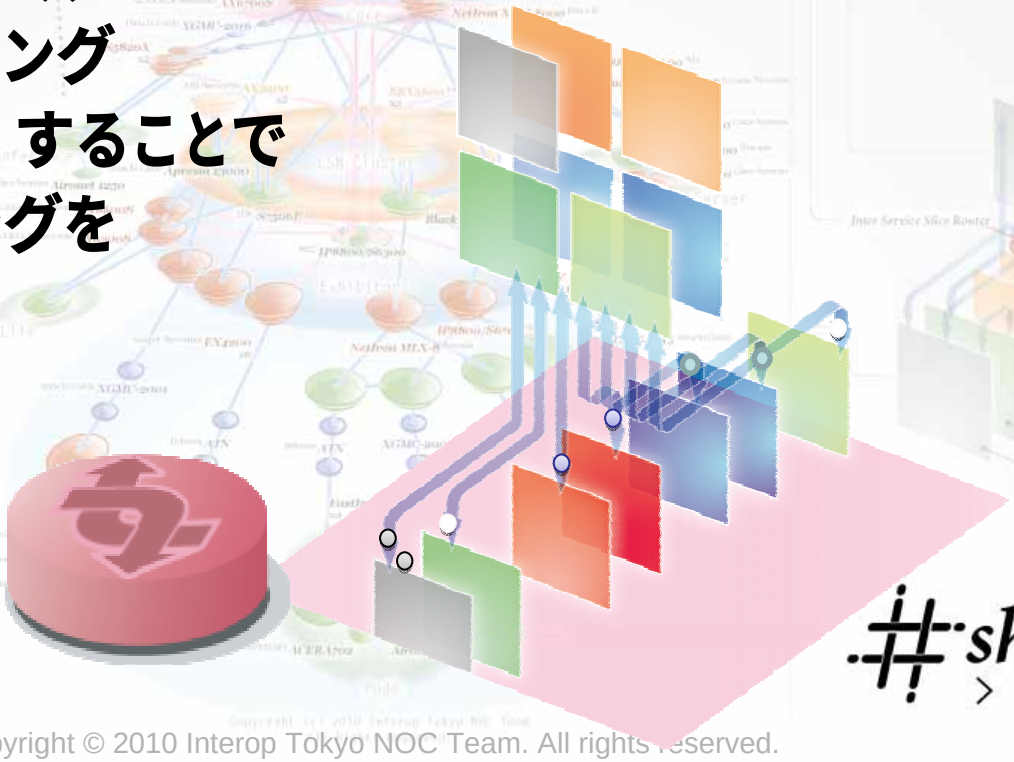
#sh△net
> count zero

L2,L3機器による仮想化

– 1つのデバイスを複数に仮想化

- ISSR(Inter Slice Service Router)で使用

- VRF Import Base ISSR
  - Internet gateway Sliceの**ルーティングテーブルへ各VRFのルーティングテーブルをImport することでSlice間ルーティングを実現**



INTEROP TOKYO | 7-11 JUNE, 2010

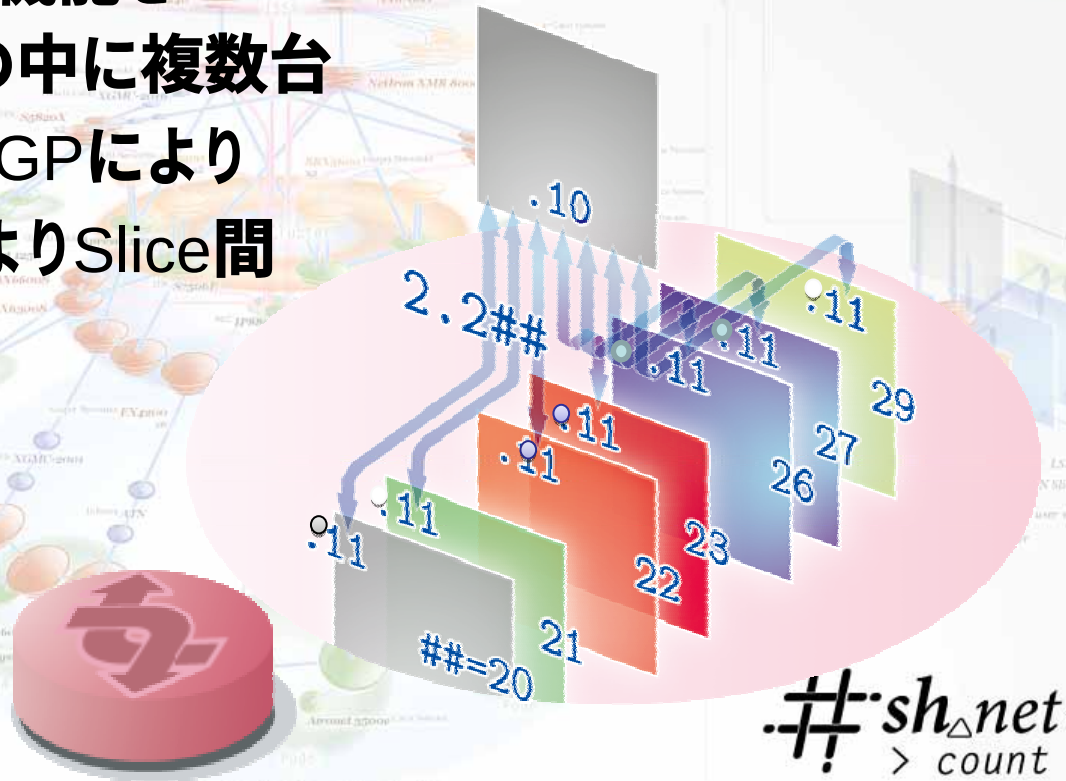
#sh△net > count zero

L2,L3機器による仮想化

– 1つのデバイスを複数に仮想化

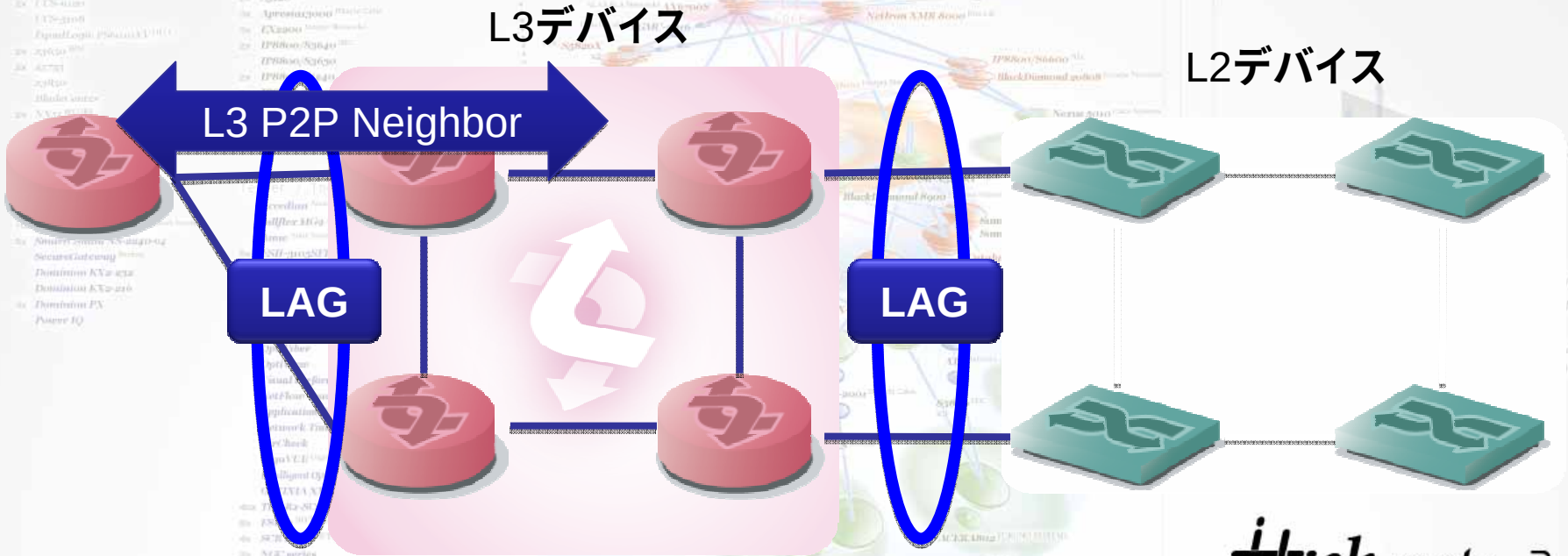
- ISSR(Inter Slice Service Router)で使用

- BGP over Logical tunnel
  - ロジカル･システム機能を使用し1台のルータの中に複数台のルータを作成し、BGPにより経路交換することによりSlice間ルーティングを実現

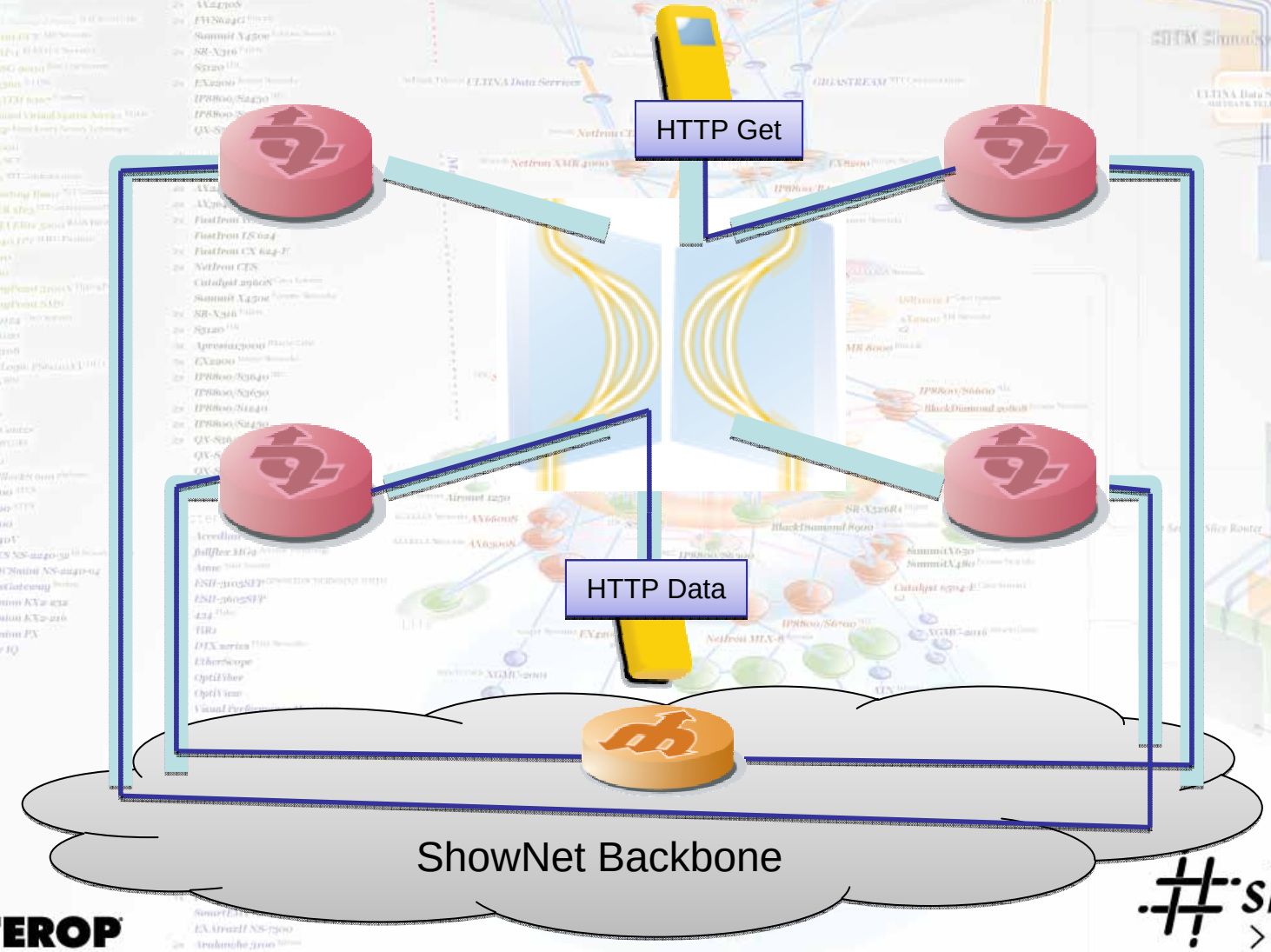


L2,L3機器による仮想化

- **複数**のデバイスを1つに仮想化
  - 1つの管理インタフェース
  - 1つのネットワークデバイス
  - 1つのコントロールプレーン



L1光スイッチを使ったオンデマンドな計測パス構築とNAT負荷試験

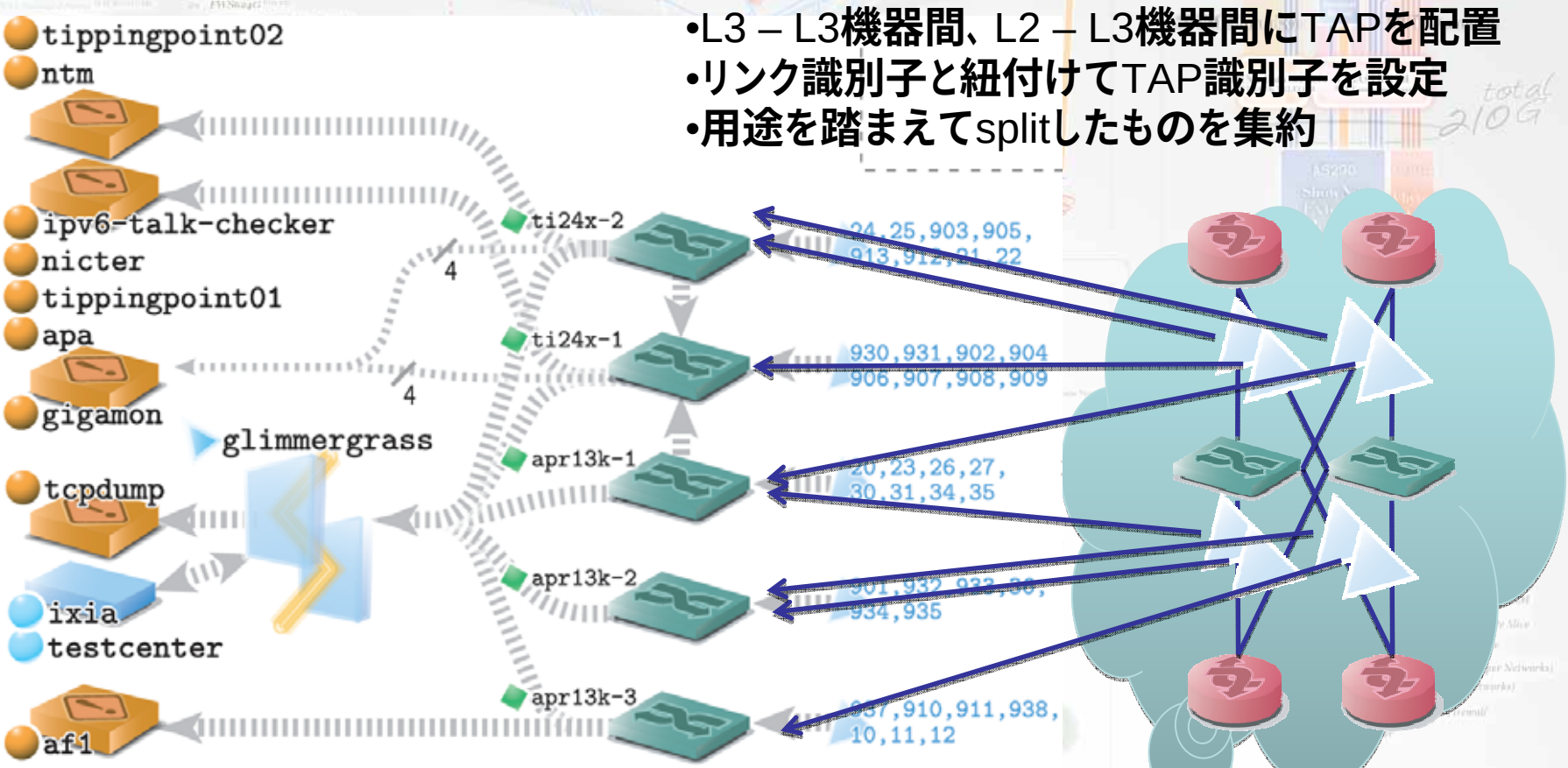


INTEROP
TOKYO | 7-11 JUNE, 2010

#shownet count zero

束ねたり分配したり・・・

- L3 – L3機器間、L2 – L3機器間にTAPを配置
- リンク識別子と紐付けてTAP識別子を設定
- 用途を踏まえてsplitしたものを集約



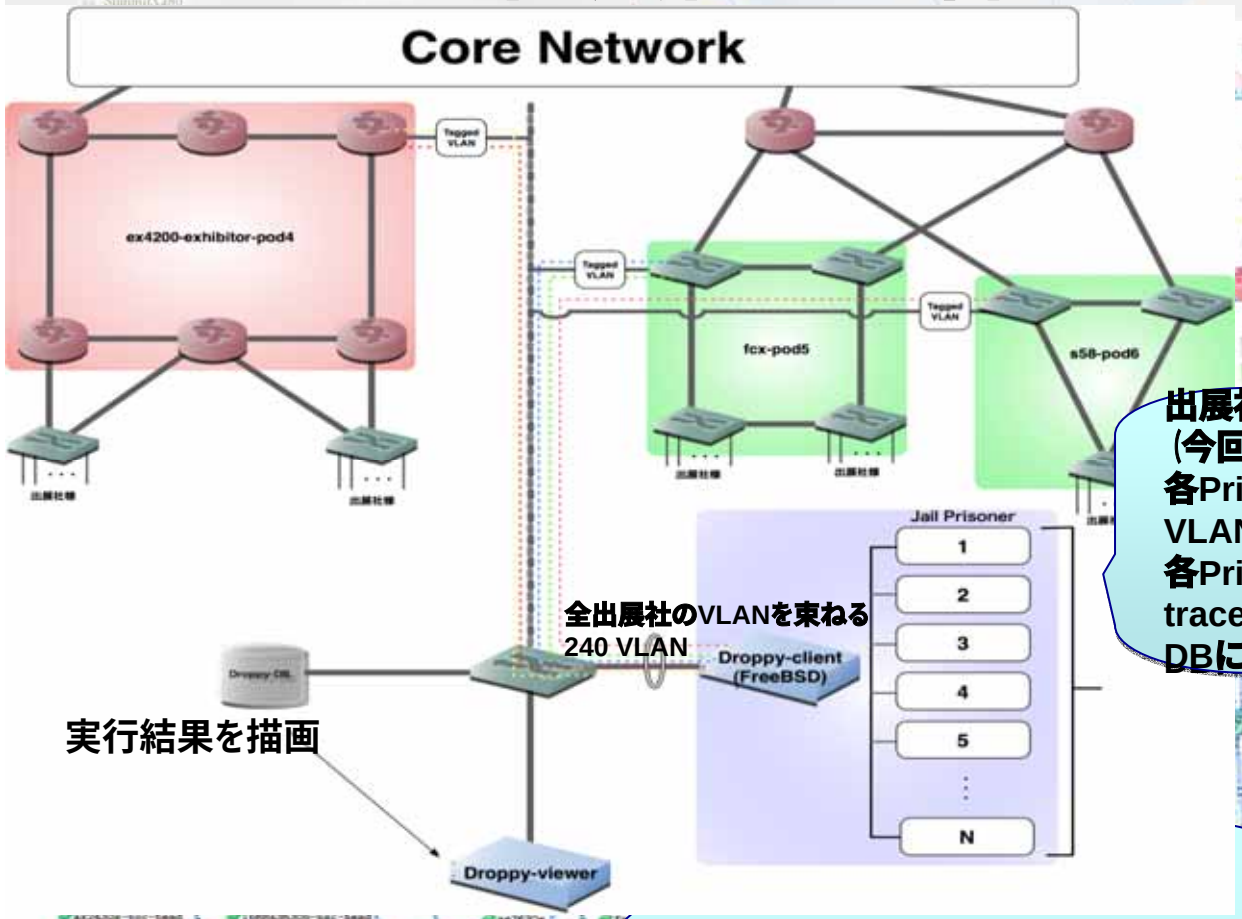
.monitor

- 集約することで一括解析へ
- 分配することで多面的に解析へ
- 解析内容はNOCブースに並ぶディスプレイで

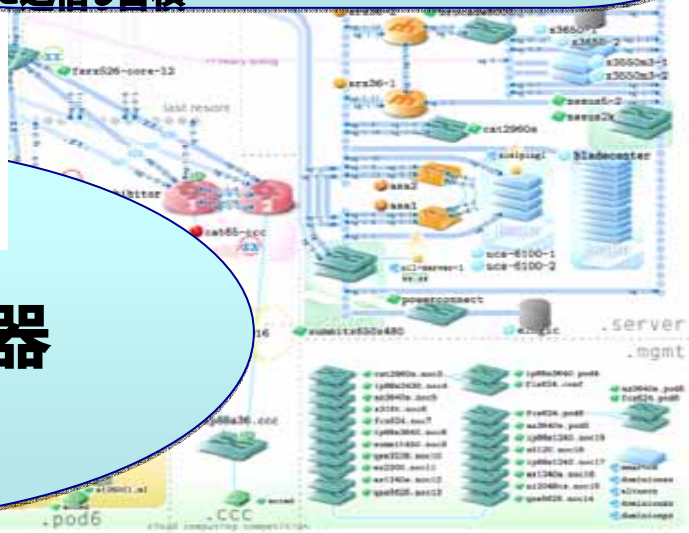
INTEROP TOKYO | 7-11 JUNE, 2010

#sh△net > count zero

出展社死活管理: Droppy



出展社様数分のJail Prisonerを用意
(今回は240個)
各Prisonerで各出展社様に割り当てられた
VLANをTagged-VLANで収容
各PrisonerからDHCP, RA, ping v4,/v6,
traceroute v4/v6を実行実行結果をDroppy-
DBに送信し蓄積

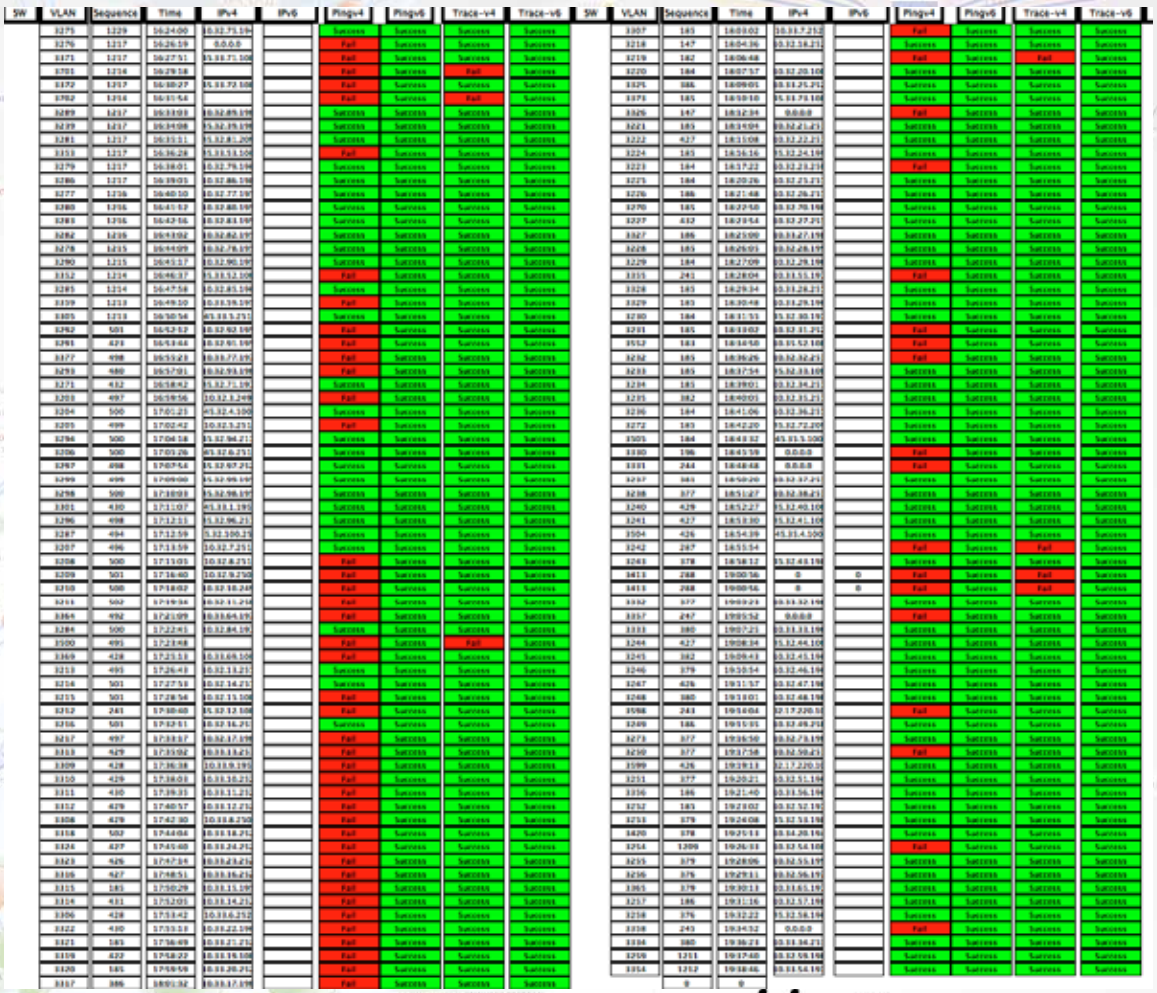


出展社収容機器

Droppy Viewer

240個の簡易仮想マシンからの試験項目結果一覧表

- 収容SW
- VLAN-ID
- IPv4/v6 Address
- Ping結果
- Traceroute結果

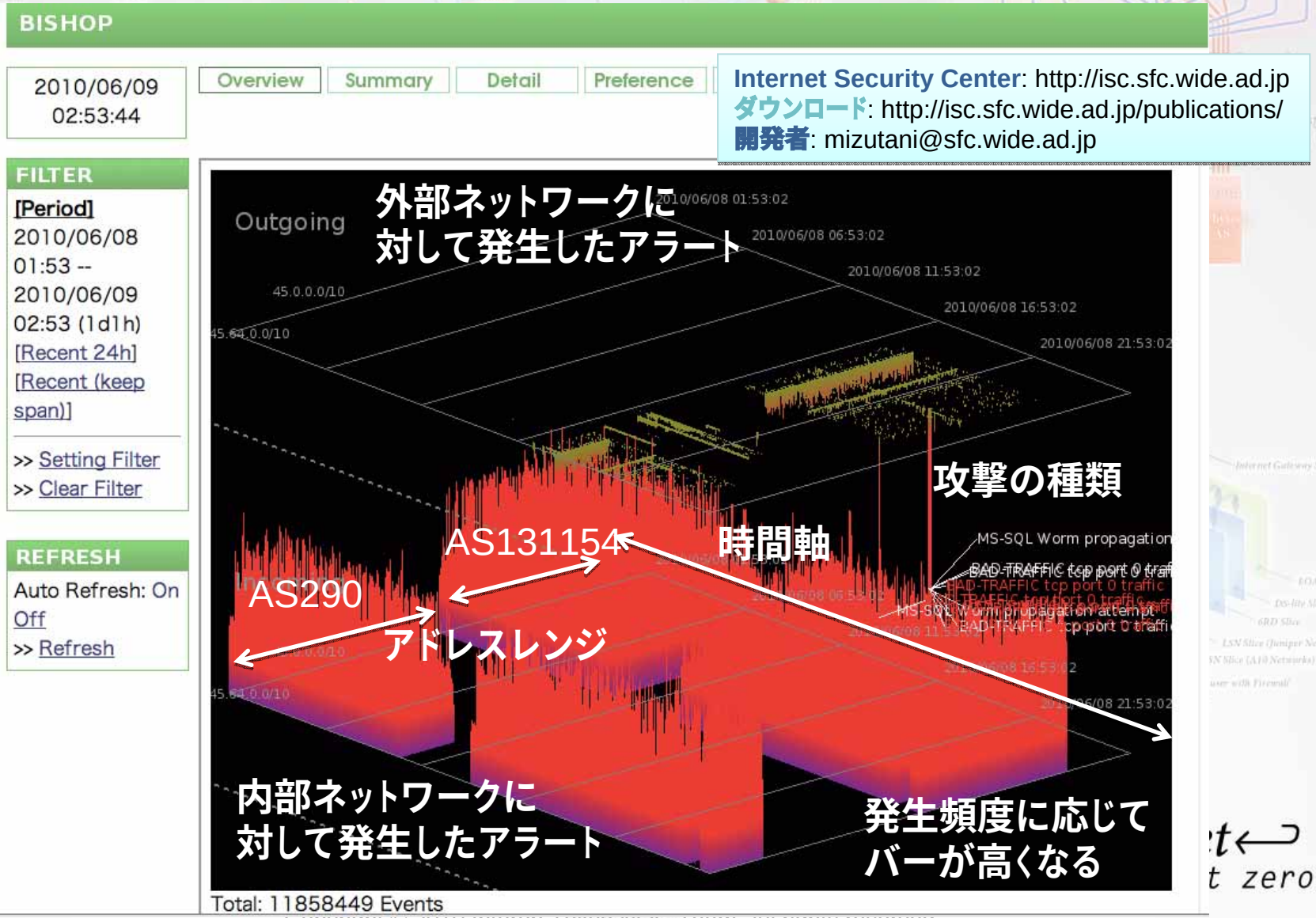


Shownetでのトライアル

- スライスの増加に伴ない、監視アプリインスタンスを作って監視するアプローチ
- スライス利用者・管理者ごとに管理も委譲

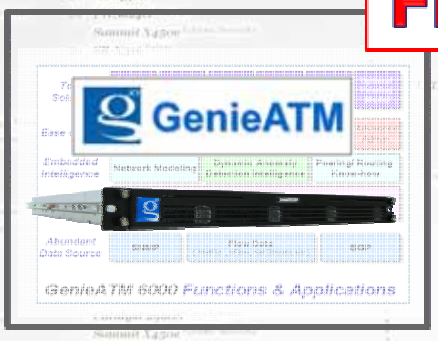
INTEROP
TOKYO | 7-11 JUNE, 2010

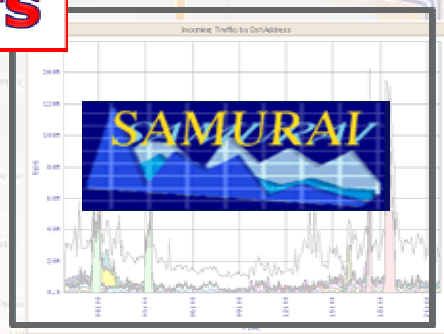
IDSログ視覚化ソフトウェア: Bishop



ShowNetの運用管理を支えるsFlow/NetFlow

Flow Collectors





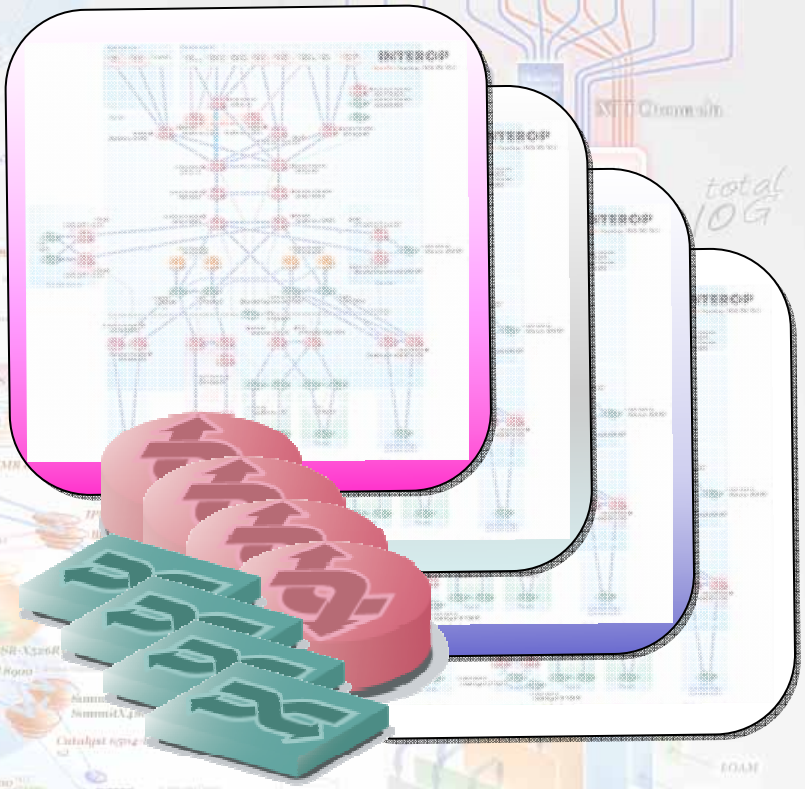
Flow Agents

INTEROP
TOKYO | 7-11 JUNE, 2010

#sh△net
> count zero

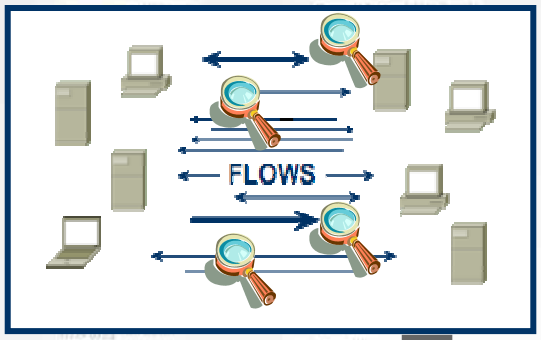
マネージャブルなxFlow管理@ShowNet

- 仮想化されたネットワークは、各仮想面ごとに特性を持ったインフラを提供
- xFlowにより管理も、仮想面ごと、特製ごとのフロー管理を求められる
- ShowNetでは、ネットワーク機器で持つ各仮想面をフローサンプル、コレクタで仮想面ごとの管理を実施

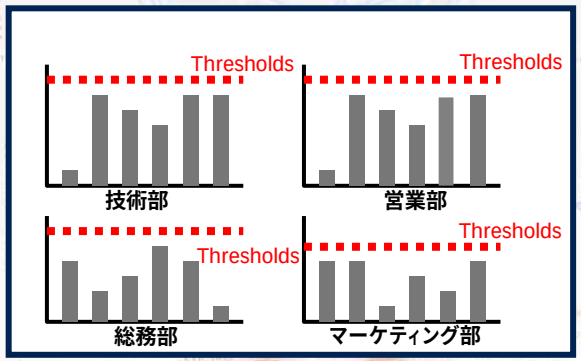


マネージャブルなセキュリティ管理もxFlowで

リアルタイムなxFlow情報から振る舞いを監視し、不正又はその可能性が高いホストや被害者を特定



sFlow/NetFlow/Mirror

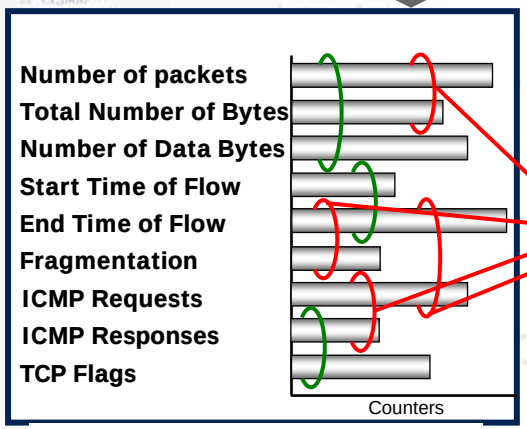


定常状態の把握(閾値を自動設定)
トラフィック/各Indexカウント等

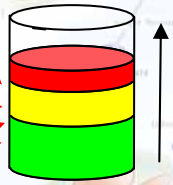
スイッチ/ルータ/ファイアウォール/IPS
などと連携した防御(自動/手動)

E-Mail Alart/SNMP Trap/Syslogで
管理者に通知

非定常状態や変則的な振る舞いをするホスト検出
ネットワーク感染型ワームなどの検出

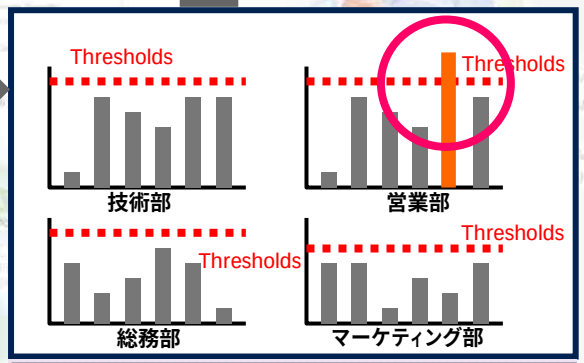


各種DBの作成/フローの解析
ホストの行動分析・解析



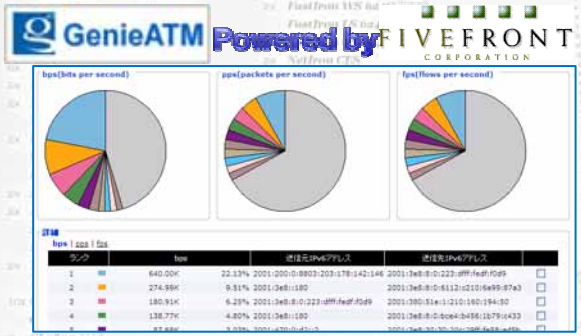
- Concern Index
- File Sharing Index
- Application Verification Index
- Target Index

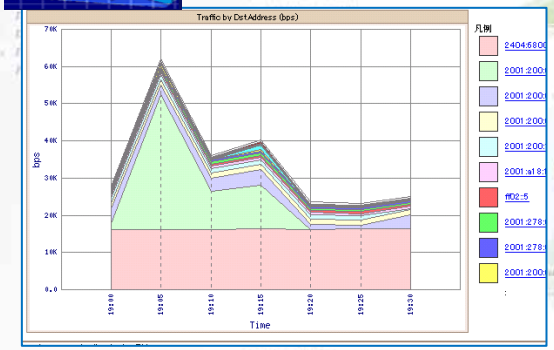
管理/レポートの自動送信



マネージャブル度向上のためのACLs-Based-sFlow

◆ACLs-Based-sFlowとは
- ベンダー独自機能 (コレクタも対応している必要があります)
- access-listを用いて、特定のパケットのみを指定し、該当するパケットはsFlowにてコレクタに送信する技術
- コレクタは、通常のサンプリングにて取得したsFlowのデータとは別に、フローレコードをストアする
- ACLs-Based-sFlowで取得したフローデータは、パケット数やバイト数など、通常のsFlow管理の量的な計算には含めない

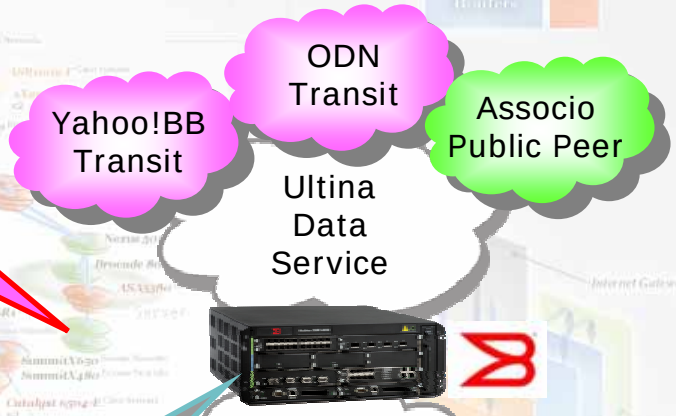




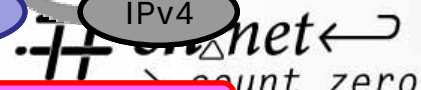
IPv4トラフィックに埋もれるIPv6トラフィックを正確かつ容易に管理

sFlow

```
[ALL IPv6 Traffic]
!
ipv6 access-list ACLs-sFlow
 permit ipv6 any any copy-sflow
 permit ipv6 any any
!
```

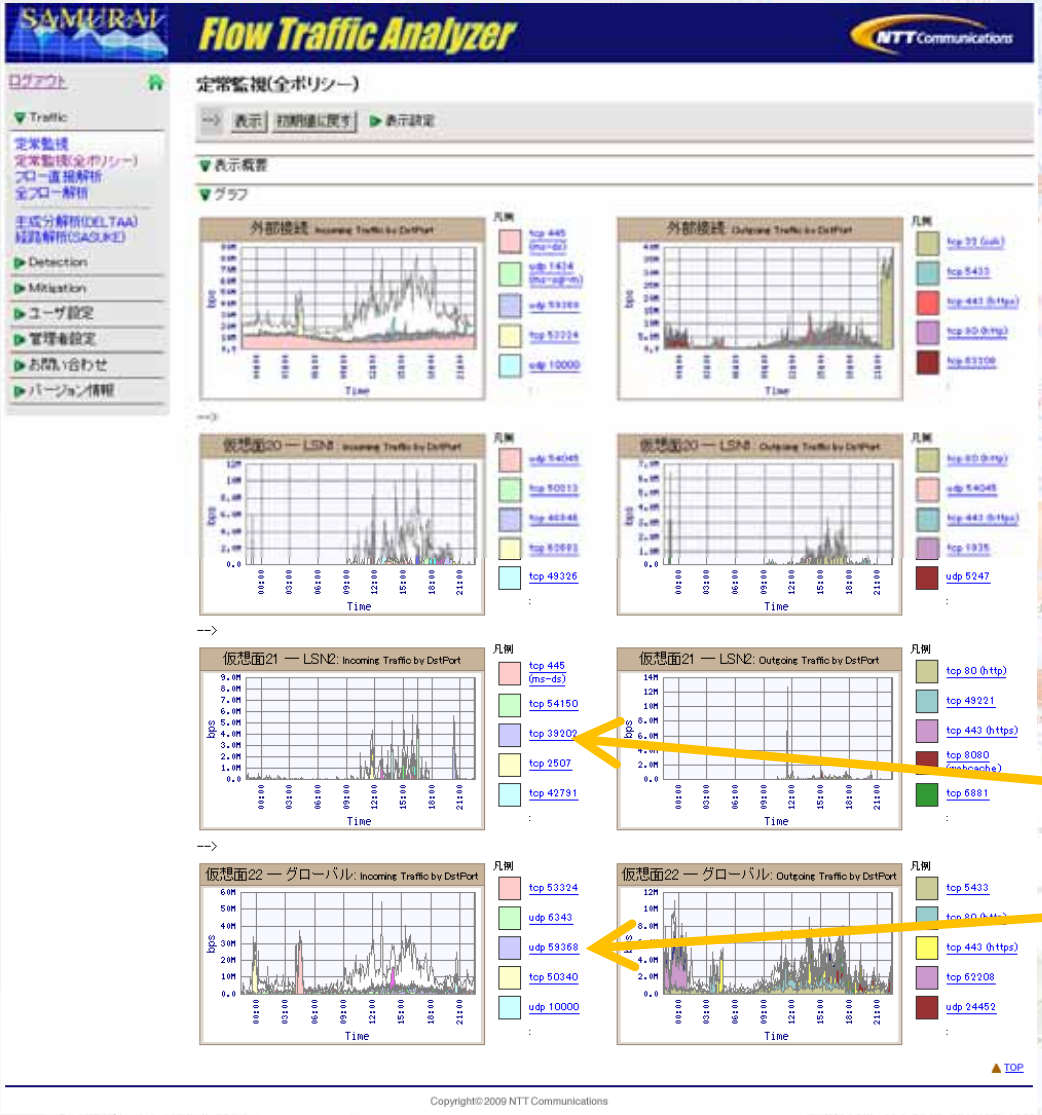


IPv6　IPv4



ACLsルールにて、「TCP syn」パケットのみを全て取得することでアクセス管理にも応用可能

マルチスライス対応フローコレクター



マルチスライス環境にて、
フロートラフィックの収集・
分析したアプライアンス

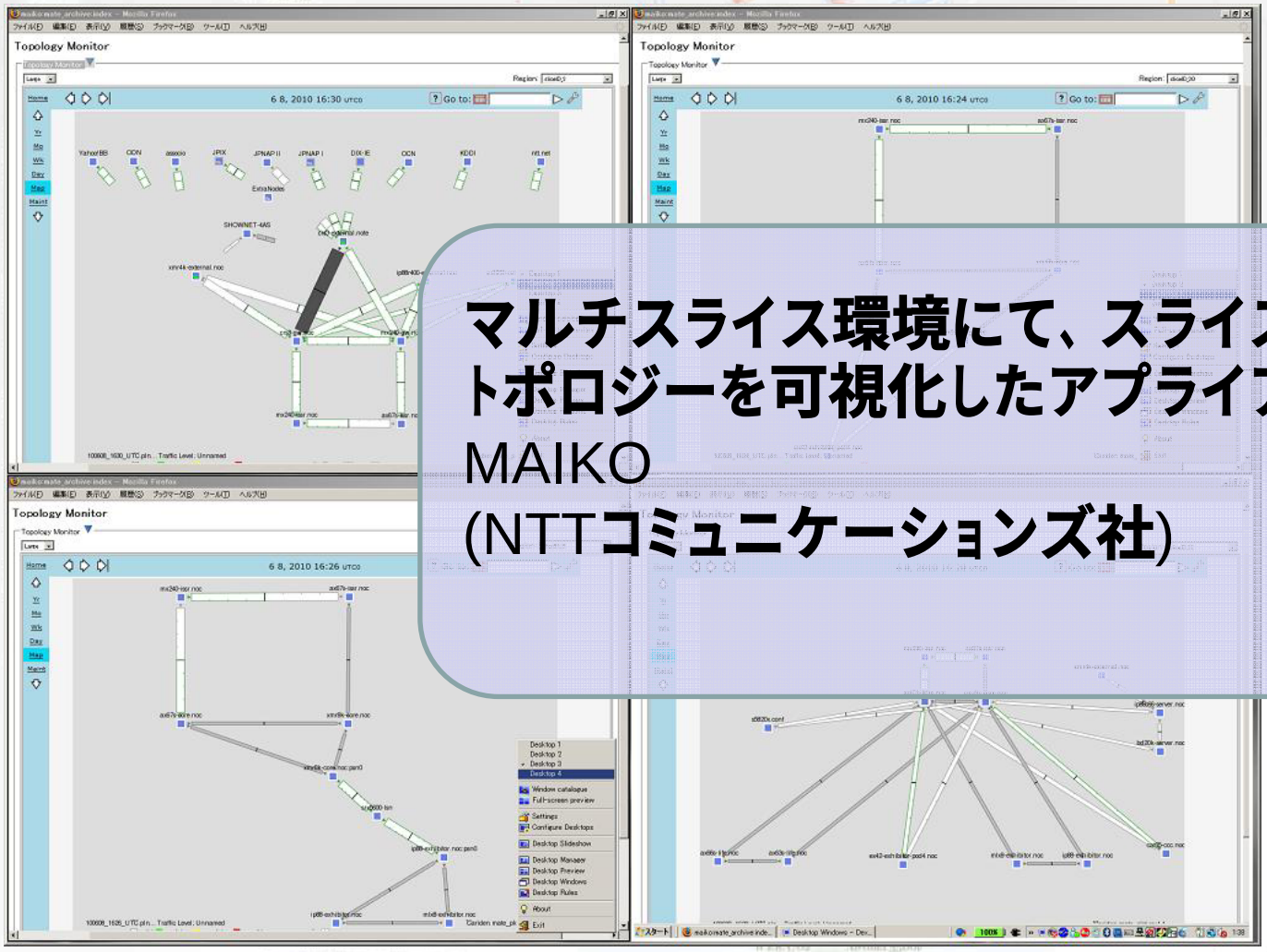
SAMURAI
(NTTコミュニケーションズ社)

スライス Global

スライス LSN

#sh△net
> count zero

マルチスライス対応オペレーションツール



マルチスライス環境にて、スライスごとのトポロジーを可視化したアプライアンス

MAIKO

(NTT**コミュニケーションズ社**)