ShowNet 2013

活動レポート – Vol.3 -

2013年11月
ShowNet 2013 NOC Team

2. ShowNet 2013 Summary

ShowNet 2013 Summary

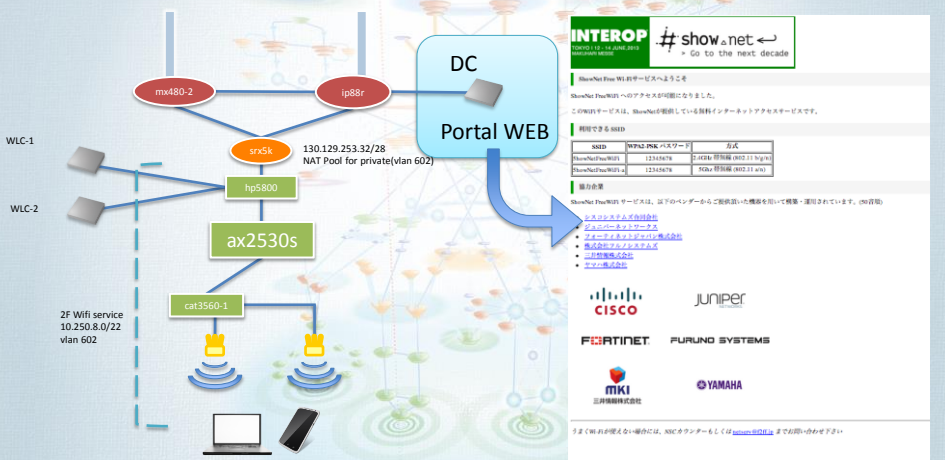
無線

ShowNet2013　WiFiサービス

- コントリビュータの皆様
  - Cisco(ホール4/5/6, 位置情報サービス)
  - YAMAHA(ホール7, 会議棟)
  - フルノシステムズ(会議棟)
  - Juniper(2F通路)
  - Fortinet(Life, バックヤード)
  - AlaxalA(キャプティブポータルスイッチ)
  - 東陽テクニカ(電磁シールド)

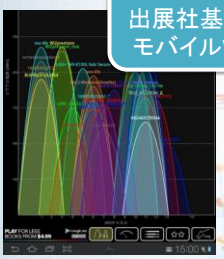
キャプティブポータル

- 2012年に引き続き実装(ホール、2F通路)



きれいな無線をもとめて

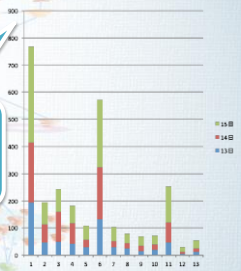
- 2012年　ShowNet無線に苦情
  - アソシエイトできない、アソシエイトできても通信できない
  - 調べてみると…基地局の乱立・電波干渉の多発



ShowNet基地局の他、
出展社基地局・来場者持ち込み
モバイルWiFiルータなどで混雑

特に2.4GHz 1chでは3日間で述べ760もの基地局を検出

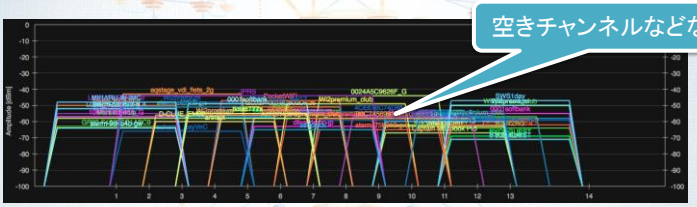
Challenge!!



このような中でWiFiサービスを使えるようにするには
どうすればよいのか？

対策1．基地局使用chの絞り込み

【問題点】他基地局の使用chと重複し電波干渉が発生している
【仮説】他基地局が使っていない空きchを使えばよい？



空きチャンネルなどない

ならば、ホール内に多く観測された1,6,11chの隣接chを使う？
⇒隣接chは干渉によりスループットが安定しない傾向がある
⇒同じchの方がスループットの安定は見込める

2.4GHz帯では1,6,11chを採用し基地局で1つを選択・使用

対策2. 基地局のマイクロセル化

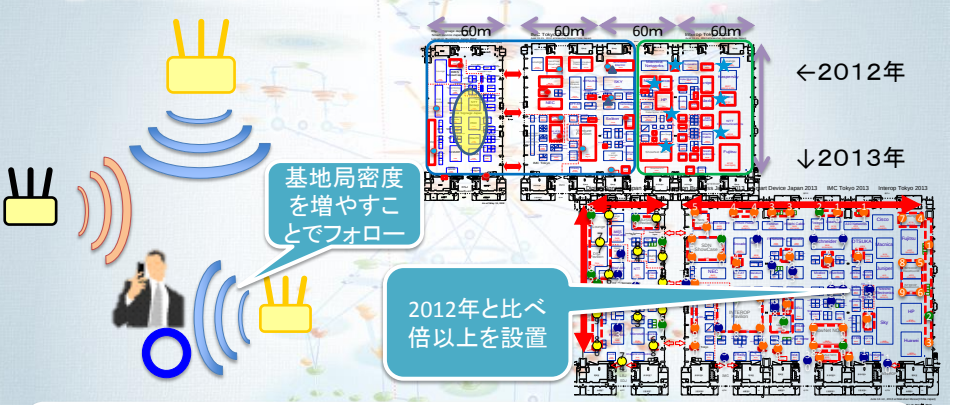
【問題点】電波が必要以上に遠くに届いており、干渉を起こしやすくしている

【仮説】電波出力を弱めることが有効か？

さらに・・・

対策2. 基地局のマイクロセル化

電波出力を抑えた分は基地局密度を上げる



2.4GHz帯では電波出力を抑え基地局数を昨年より増やして運用
各社様コントリビューションのお陰で実現した運用です！

show net > Go to the next decade

INTEROP TOKYO | 11-14 JUNE, 2013

2.4GHz帯に利用したサポート機能

- Radio Resource Management – Cisco
  - WLCと連動し、ShowNet基地局間の無線環境に合わせて1,6,11chのうち最適なchを自動で選ぶ
- 低レートクライアントの遮断
  - 閾値以下の低レートクライアントを遮断し、周波帯域を空ける(11Mbpsを閾値で運用)

show net > Go to the next decade

INTEROP TOKYO | 11-14 JUNE, 2013

対策3. 5GHzでのサービス提供

【仮説】5GHzでのサービス提供を促進してみてはどうだろうか？

周波帯ごとの差異	2.4GHz	5GHz
ch割り当て	5MHzごとに14ch,隣接chとの帯域重複あり	20MHzごとに4ch,隣接chとの帯域重複なし
基地局検出数	1chに3日で述べ760	2.4GHzより少ない

2.4GHzと5GHzでSSIDを明示的に分割
さらに5GHzの電波出力は強めにして運用

また、各社製品の機能を利用し5GHzオフロードを促進

5GHzオフロードのサポート機能

- Frequency Hand Off – Fortinet
  - 2.4GHzのアソシエイトを一旦Reject
  - 5GHzでアソシエイトし直させる
- Band Steering – Juniper
  - クライアントが2.4/5GHz両方対応していたら2.4GHzでの応答を停止する(本番では未使用)

新たな発見

- 電磁シールドテント
  - 電波遮断ソリューションの一つとして提案
  - シールドテント内はホール基地局の電波を完全遮断
- クライアントを高い位置で使う
  - 基地局とクライアント間に人体・造作等の電波伝搬障害物がより少ない状態＝電波受信状態が良くなる

show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

評価

- 5GHzオフロードは有効と考えられる
  - 近年スマートフォン・タブレットともに5GHz対応が進んでおり(右表参照)その部分を救えていたとみられる

【参考】docomo夏モデルの5GHz対応状況	機種数	5GHz 対応機種数
2011年　夏秋モデル	10	1
2012年　夏モデル	16	6
2013年　夏モデル	10	9

- 他方2.4GHzのみ対応デバイスを救うのは難しい
  - 今回の対策が全く無意味とはいえないが「使える」状態にするには今後も試行錯誤が必要

show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

2. ShowNet 2013 Summary

ShowNet 2013 Summary

IPv6移行技術

show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

IPv6移行技術

- IPv6 onlyバックボーンの登場を想定した各種技術を hall7出展者/会議棟来場者向けに提供し、実運用に挑戦

hall7出展者向けに提供した技術
- ✓ DS-Lite
- ✓ 464XLAT
- ✓ MAP-E

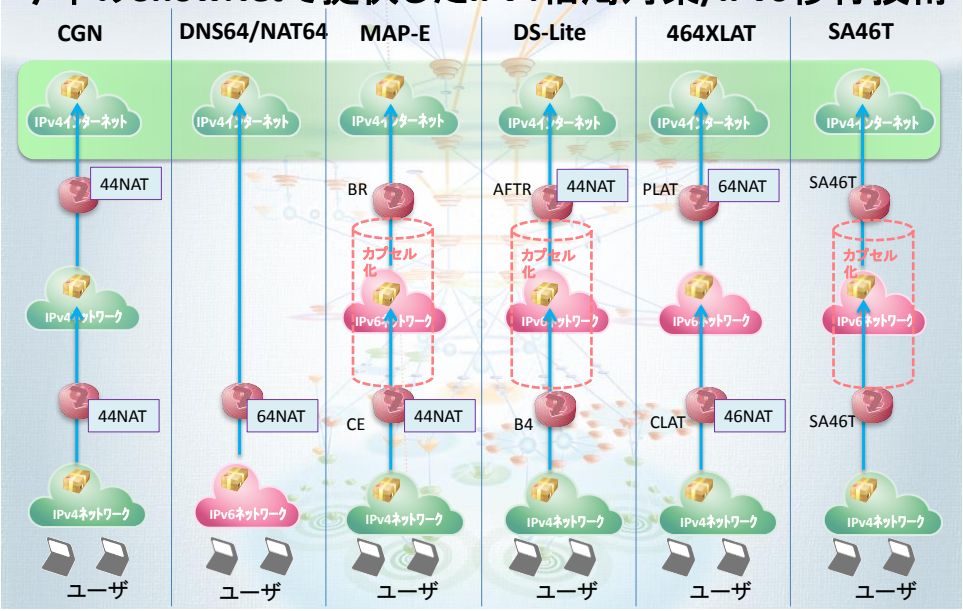
会議棟来場者向けに提供した技術
- ✓ SA46T
- ✓ NAT64/DNS64

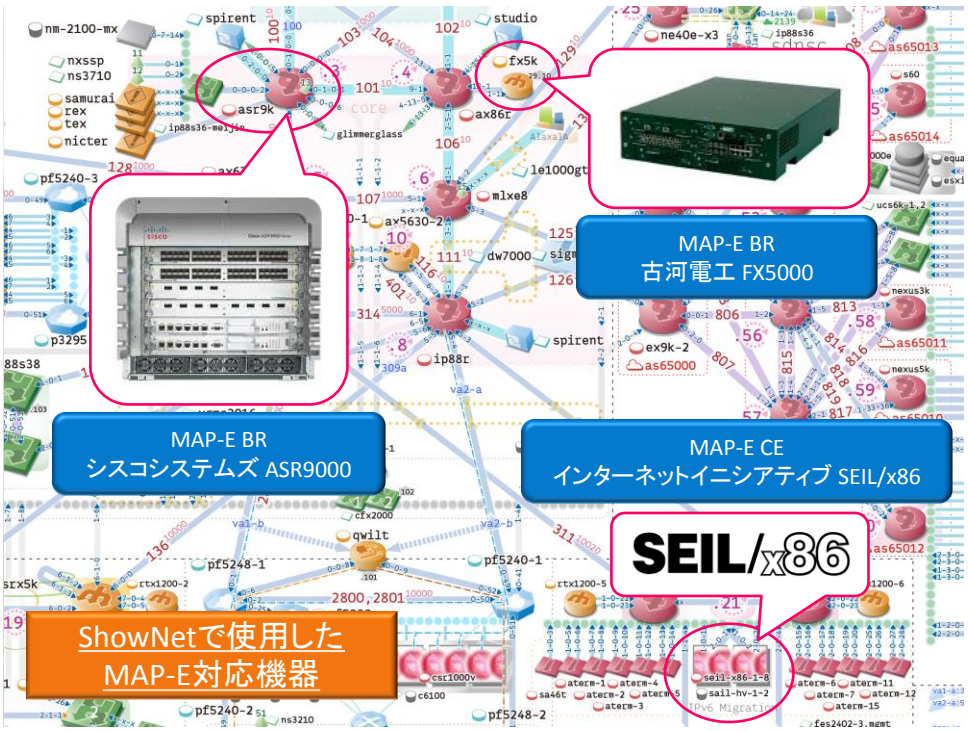
A10 Networks　NEC　CISCO　SEIKO セイコーソリューションズ株式会社　FUJITSU　JUNIPER NETWORKS　Infoblox

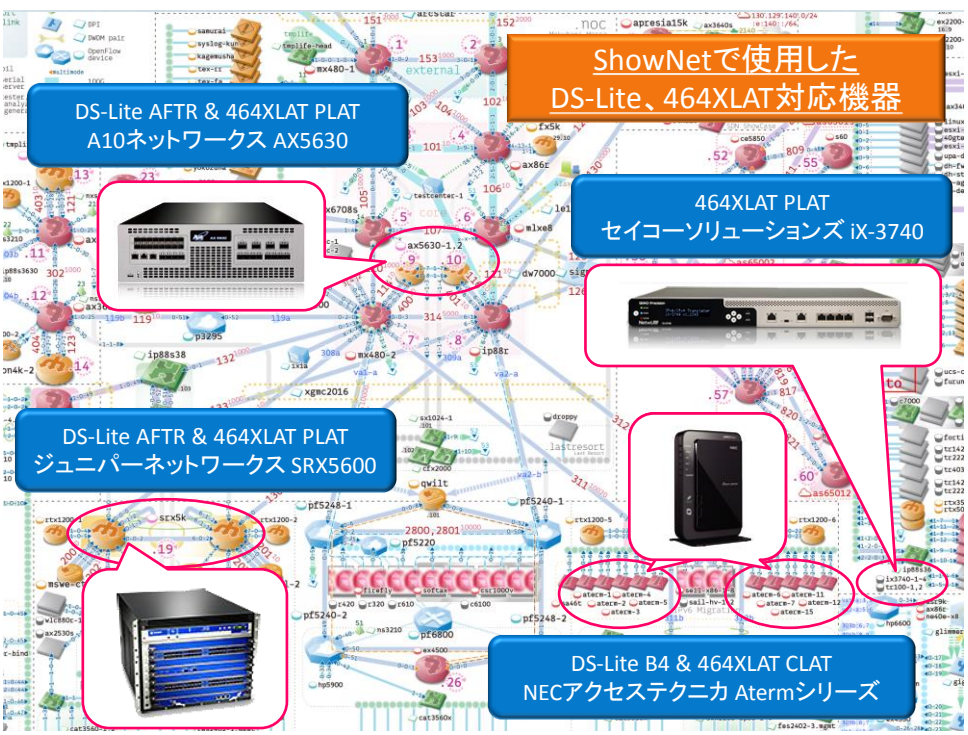
show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

今年のShowNetで提供したIPv4枯渇対策/IPv6移行技術




MAP-E BR
古河電工 FX5000
MAP-E BR
シスコシステムズ ASR9000
MAP-E CE
インターネットイニシアティブ SEIL/x86
SEIL/x86
ShowNetで使用した
MAP-E対応機器


ShowNetで使用した
DS-Lite、464XLAT対応機器
DS-Lite AFTR & 464XLAT PLAT
A10ネットワークス AX5630
464XLAT PLAT
セイコーソリューションズ iX-3740
DS-Lite AFTR & 464XLAT PLAT
ジュニパーネットワークス SRX5600
DS-Lite B4 & 464XLAT CLAT
NECアクセステクニカ Atermシリーズ

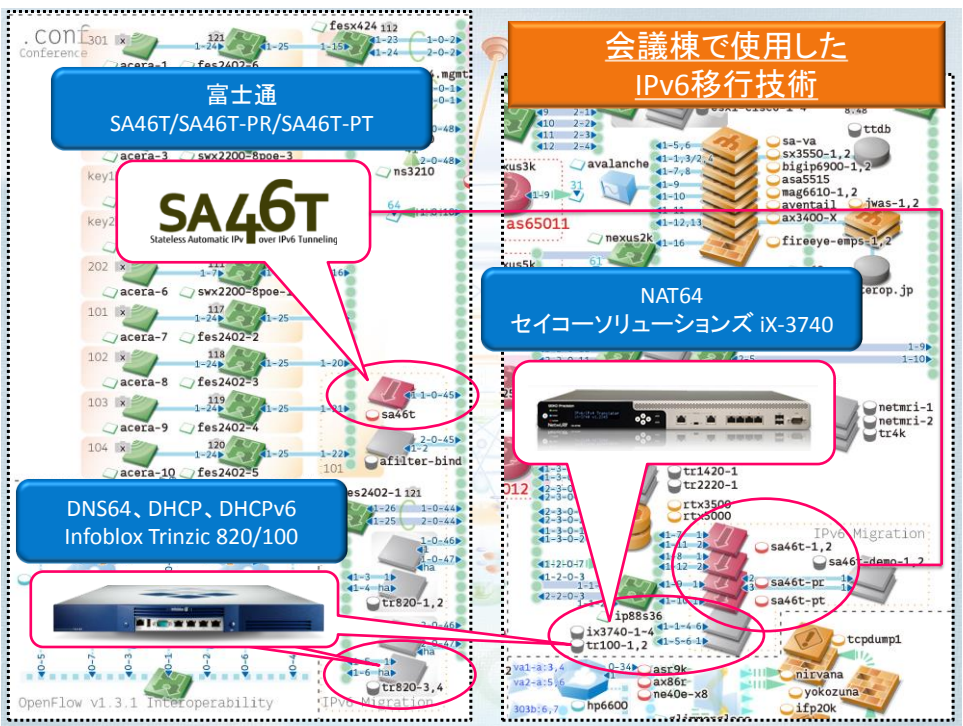
show net
> Go to the next decade

INTEROP
TOKYO | 11 – 14 JUNE, 2013

MAP-E最新ドラフトでの相互接続試験

- SEIL/x86とASRにて、MAP-Eの最新ドラフト(draft-ietf-softwire-map-07)に準拠した相互接続試験を実施。
- ASRがICMPv4パケットのencapsulationに未対応だったが、TCP/UDPパケットの疎通には問題ないことが確認できた。

19:12:49.571434 2001:3e8:6000:c0:0:8281:ff5f:0 > 2001:3e8:0:2900::1:
IP 130.129.255.95.45089 > 133.242.53.30.80: S 1937843878:1937843878(0)
win 14600 <mss 1420,sackOK,timestamp 344073592 0,nop,wscale 6>




show net
> Go to the next decade
INTEROP
TOKYO | 11－14 JUNE, 2013
2. ShowNet 2013 Summary
ShowNet 2013
Summary
SDN

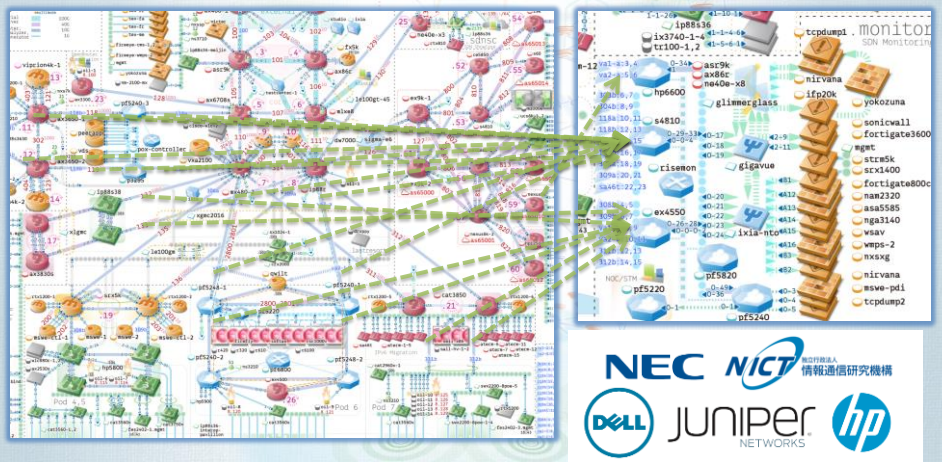

show net
> Go to the next decade
INTEROP
TOKYO | 11－14 JUNE, 2013
ShowNet 2013におけるSDNの取り組み
SDN Security
ShowNetのバックボーントラフィック解析・セキュリティ監視
任意のバックボーントラフィックの抽出
セキュリティ機器との連携によるリアルタイム監視
SDN 出展社収容
サービス
出展者向けネットワークの提供と管理
OpenFlowとクラウドサービスアプライアンスによる
ShowNetアクセスサービスの仮想化
SDN Cache 連携
SDNによる柔軟なコンテンツトラフィック制御
Cacheアプライアンスと連携した
効率的なネットワークサービスの実現
OpenFlow spec 1.3.1
Test & Service
相互接続検証と世界初のサービス提供！！
OpenFlow Spec 1.3.1でインターネットへのアクセスを体験
※詳細は「相互接続」の章で報告

show net
> Go to the next decade

INTEROP
TOKYO | 11－14 JUNE, 2013

SDN Security

ShowNetの10Gbpsリンク17箇所に割り入れた光タップからのキャプチャーパケットを
OpenFlowスイッチ7台のネットワークでコントロールし解析装置などへ供給



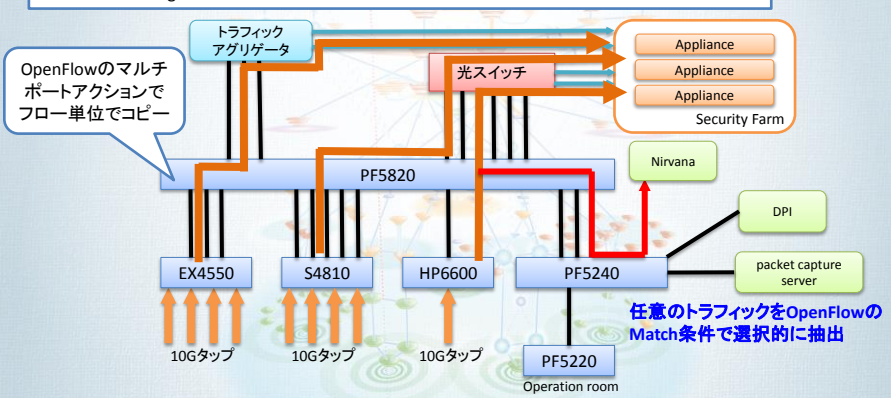
NEC NICT 情報通信研究機構
DELL JUNIPER NETWORKS hp

show net
> Go to the next decade

INTEROP
TOKYO | 11－14 JUNE, 2013

SDN Security

- 従来はポートミラーリングやL1スイッチで行なっていたものをOpenFlowで実現
  - 集中制御と外部との動的連携が可能になった
  - ヘッダ情報を非破壊で複数のスイッチを経由させることが可能
  - モニタリングインフラをネットワーク化することが可能になり拡張性が向上
- NICTコントリビューションのRISEmonコントローラで実現
  - HotStage中に幕張メッセで開発、Tremaベース



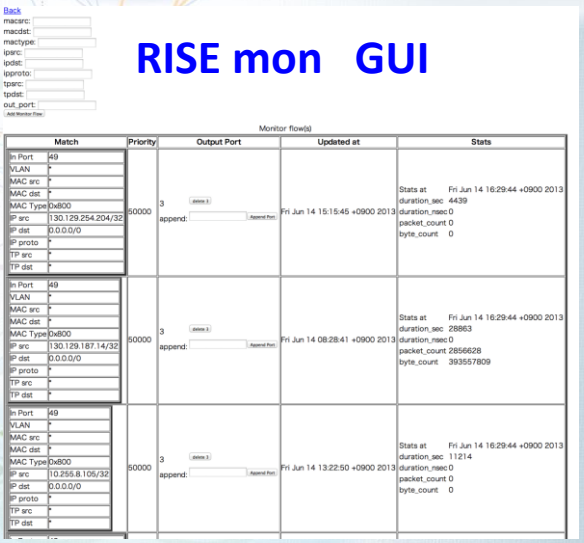
show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

SDN Security

任意のトラフィックを抽出
RISE monから選択

RISE mon GUI

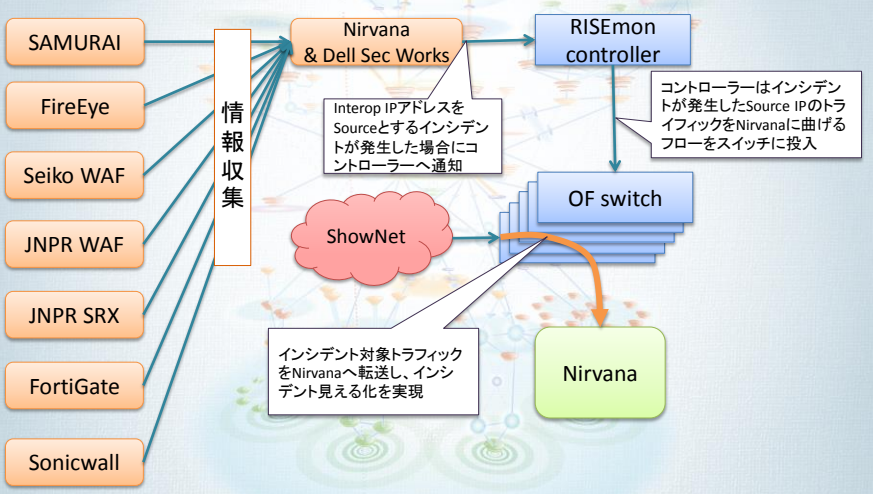


show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

SDN Security

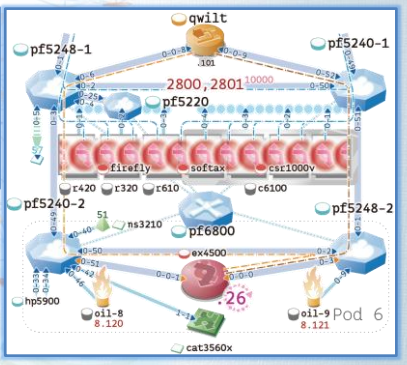
複数の解析装置の結果を収集しインシデント発生を検知。
対象トラフィックのパケットキャプチャーをフロー単位で引き込み詳細解析実施する連携動作



SDN 出展社サービス

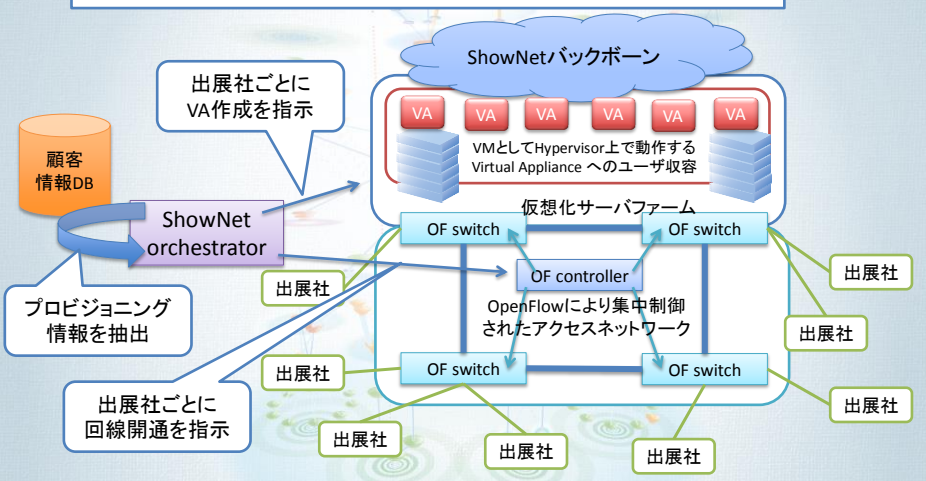
- **SDN**によるネットワークの仮想化とプロビジョニング
  - 仮想ルータ(Virtual Appliance)インスタンスを出展社ごとに1台ずつ生成
  - OpenFlowによってL2ネットワークの動的なテナントの追加や削除を実現

- 全てが**ソフトウェア**で**抽象化**された**ネットワーク**
  - **Software Defined Network**の1つの完成形
  - VAのConfig生成とHVへのデプロイ自動化
  - NEC ProgrammableFlow ControllerのAPIを用いたOpenFlowによる動的なL2ネットワークの自動開通
  - NOCお手製ソフトウェアを用いて出展社収容ネットワークを自動生成



SDN 出展社サービス

6ホール出展社など（計32ユーザ）に対してネットワークサービスを提供。
開通作業無人化と会期中の安定運用を達成。

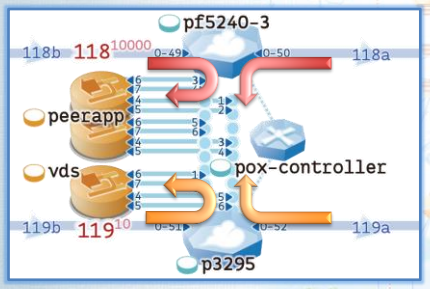


show net
> Go to the next decade

INTEROP
TOKYO | 11 – 14 JUNE, 2013

SDN Cache 連携

- SDN Content Traffic Based Routing
  - ✓ Cache Applianceと連携して自動的にWebコンテンツトラフィックのフローを制御
  - ✓ コンテンツトラフィックのフローを効率的に選択・分散処理することでQoEを向上



- ネットワークサービスリソースを有効活用
  - ✓ サービスを意識せずに利用可能
  - ✓ 必要な機能をオンデマンドで提供
- 対象コンテンツトラフィックフローを識別
  - ✓ Hashによるロードバランス
  - ✓ Output port指定
  - ✓ Ethernet destinationをset
- POXベースのSDN Controller
  - ✓ NOCメンバお手製
  - ✓ オープンソース　たった250行!

cisco NCLC NEC NTT AT Allot communications PeerApp

show net
> Go to the next decade

INTEROP
TOKYO | 11 – 14 JUNE, 2013

2. ShowNet 2013 Summary

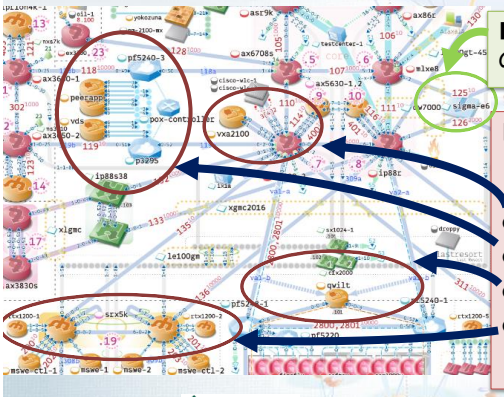
ShowNet 2013 Summary

Cache / DPI

show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

Cache/DPI 概要



■バックボーン<->データセンタトラフィック
のトラフィック傾向をDPI装置で調査

■様々な方法でHTTPトラフィックを
Cache装置へ誘導
(ホール毎に異なるCache装置に誘導)

- L3ポリシベースルーティング
- OpenFlow
- HTTPリダイレクション
- BGPルーティング

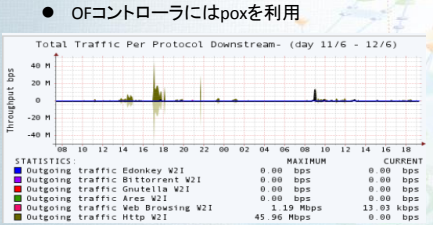
NTT AT　IT Frontier　Allot communications　JUNIPER NETWORKS　PeerApp　CISCO

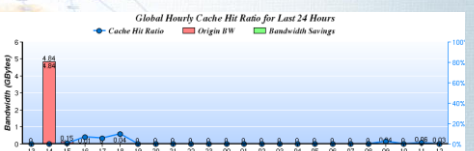
show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

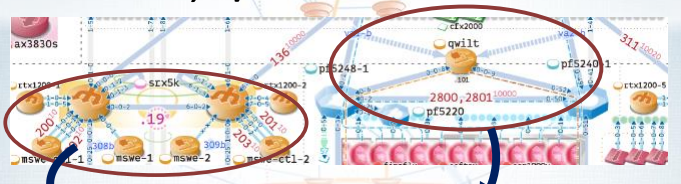
LIFE/Hall7向けCache

- 2種類のCacheと2種類のOpenFlowスイッチを用いて冗長性を持った相互接続
  - 各Cache装置は両スイッチに接続性を持つ
  - OFコントローラにはpoxを利用
- バックボーンスイッチに直結し、Hall7向けの通信のみをポリシベースルーティング
  - LAG接続により回線の冗長性を確保

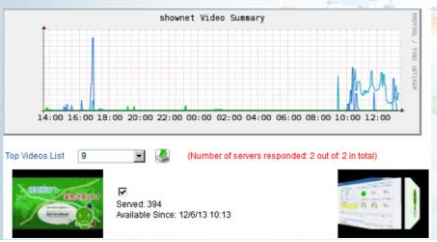


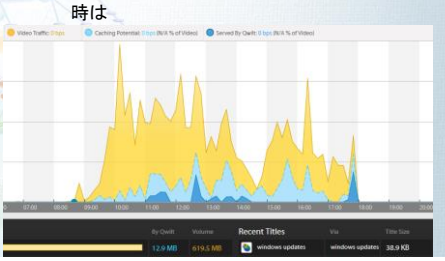


Hall4,5/Hall6向けCache



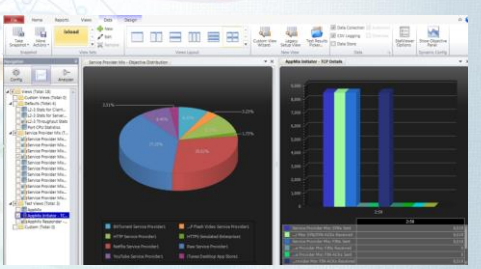
- BGPでコンテンツサイトへの通信をキャッシュ装置にルーティング
  - 2組のシステムを配備し負荷分散/冗長性を実現
- コンテンツサイトへの通信を検知しキャッシュ装置にHTTPリダイレクション
  - メイン系・予備系の両トラフィックを監視し切り替わり時は





Cache装置の試験

- 2種類の試験機を試験内容に応じて使用
  - Ixia IxLoad
  - Ixia BreakingPoint FireStorm
- 試験1: スループット試験
  - 数種類のアプリケーショントラフィックを混在させ、リアルワールドに近いトラフィック分布を再現し、処理能力を試験



show net
> Go to the next decade

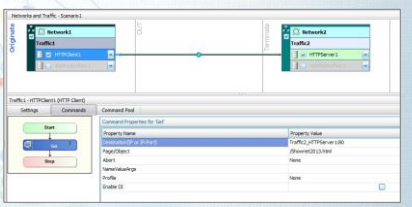
INTEROP
TOKYO | 11 – 14 JUNE, 2013

Cache装置の試験

- 試験2: コンテンツ試験
  - アプリケーショントラフィックを疑似的に生成し、各キャッシュ装置の動作を確認
    - アプリケーショントラフィックとして識別されるか
    - キャッシュ対象のトラフィックとして識別されるか

- ビデオトラフィック
  - 試験機のシミュレーション機能でトラフィックを生成
  - コンテンツサイトにアクセスした実トラフィックを試験機でキャプチャリプレイ
  - コンテンツ内容: YouTube/Dailymotion/XVideos

- HTTPトラフィック
  - キャッシュ対象となるファイルを生成してアクセス
  - コンテンツ内容: 2KBytes/固定データ



show net
> Go to the next decade

INTEROP
TOKYO | 11 – 14 JUNE, 2013

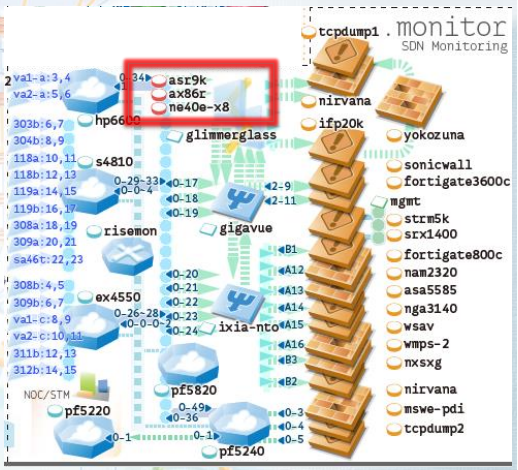
2. ShowNet 2013 Summary

ShowNet 2013 Summary

セキュリティ/モニター/監視

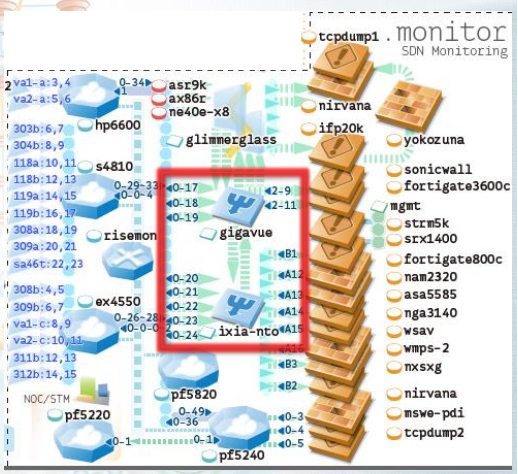
TAP

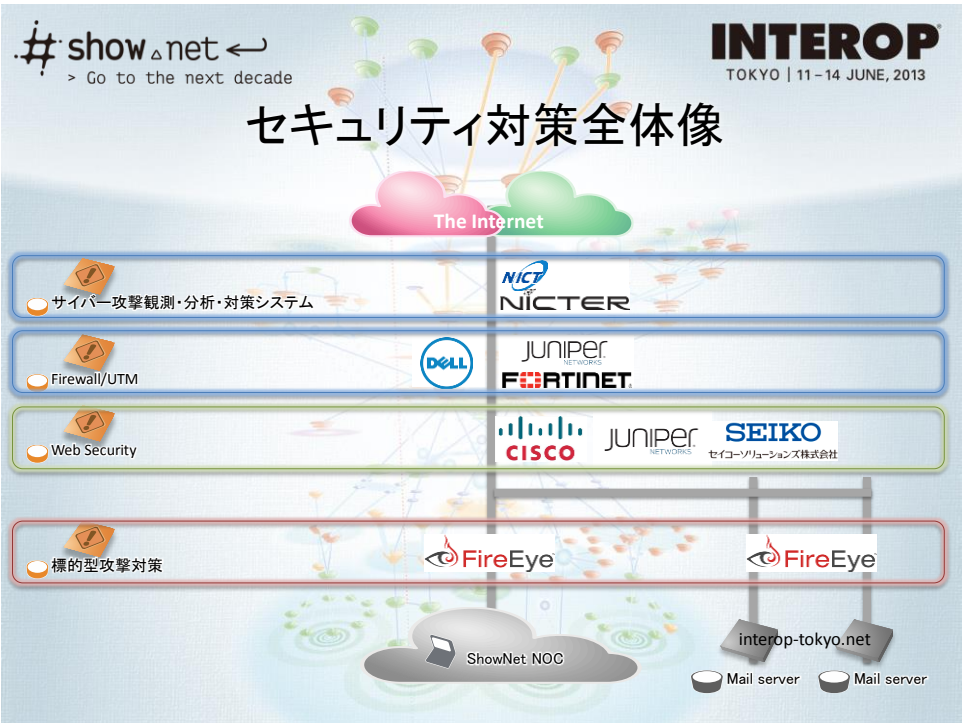
- TAP
  - –ShowNet2013では、これまでのトラブルシューティング目的によるトラフィック収集では無く、セキュリティ製品活用のためのトラフィック収集とし、以下のポイントにTAPを収容。
    - ファイアウォール向けにバックボーンで収集
    - 標的型攻撃向けに出展社収容などのエッジの上位リンク
  - –合計20カ所にて収集
- TAPの導入により、解析に必要なトラフィックを確実に収集可能に。

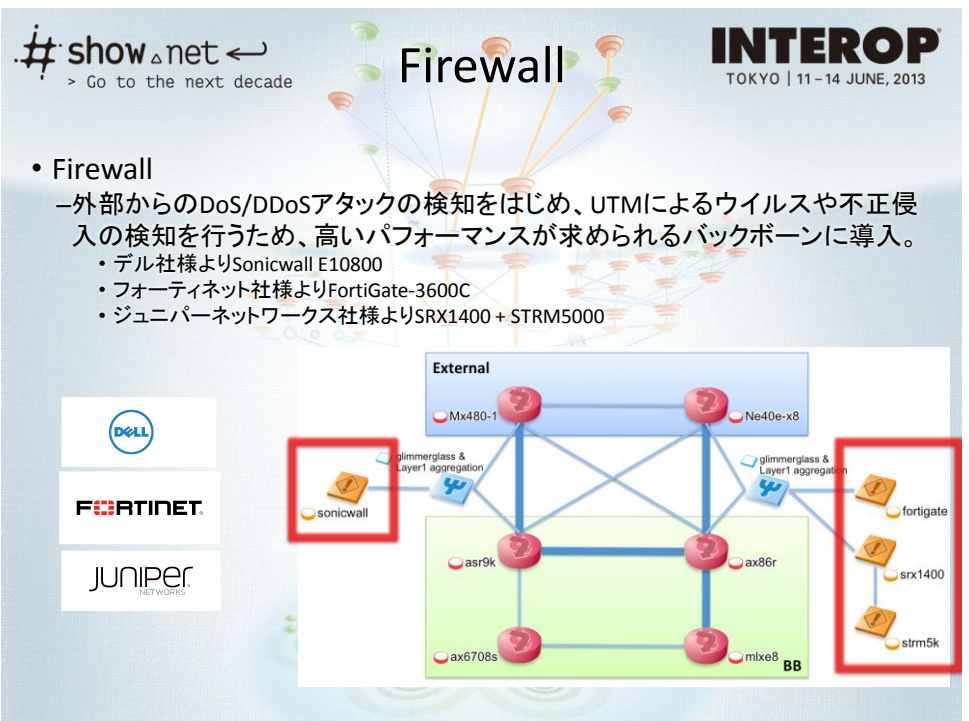


Aggregator

- Aggregator
  - –TAPからセキュリティ製品活用のためのトラフィック収集を行い、集約や分散、重複排除のために以下の2機種を導入。
    - ビットリーブ社様よりGigamon社のGigaVUE
    - IXIA様よりBreakingpoint
  - –各社様のご提供により、無駄の無い、効率的なトラフィック収集を実現




show net
> Go to the next decade
INTEROP
TOKYO | 11 – 14 JUNE, 2013
セキュリティ対策全体像
The Internet
サイバー攻撃観測・分析・対策システム
NICT
NICTER
Firewall/UTM
DELL
JUNIPER NETWORKS
FORTINET
Web Security
CISCO
JUNIPER NETWORKS
SEIKO
セイコーソリューションズ株式会社
標的型攻撃対策
FireEye
FireEye
ShowNet NOC
interop-tokyo.net
Mail server
Mail server

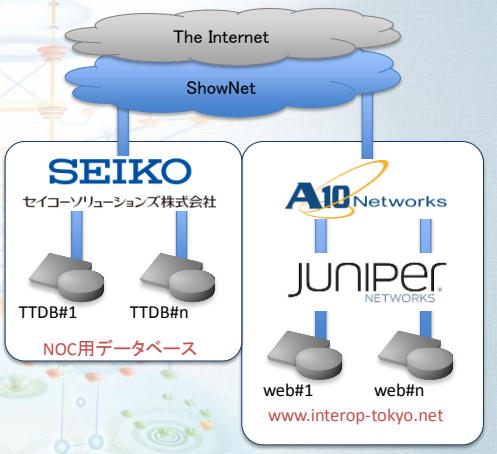

show net
> Go to the next decade
Firewall
INTEROP
TOKYO | 11 – 14 JUNE, 2013
• Firewall
–外部からのDoS/DDoSアタックの検知をはじめ、UTMによるウイルスや不正侵入の検知を行うため、高いパフォーマンスが求められるバックボーンに導入。
• デル社様よりSonicwall E10800
• フォーティネット社様よりFortiGate-3600C
• ジュニパーネットワークス社様よりSRX1400 + STRM5000
DELL
FORTINET
JUNIPER NETWORKS
External
Mx480-1
Ne40e-x8
glimmerglass & Layer1 aggregation
glimmerglass & Layer1 aggregation
sonicwall
fortigate
srx1400
strm5k
asr9k
ax86r
ax6708s
mlxe8
BB

show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

SLB + Web Security

- NOC用データベース
  - –ShowNetで利用している全ての機材を管理するTTDBをロードバランスしながらWAF機能により攻撃を防御
    - セイコーソリューションズ社様ご提供のsx3550
- 公開用Web
  - –高負荷な公開用Webにはロードバランス機能に加え、攻撃者撃退のための心理的防御方法に基づく対策、Web侵入ディセプションで防御
    - A10ネットワークス社様ご提供のax3400
    - ジュニパーネットワークス社様ご提供のJWAS

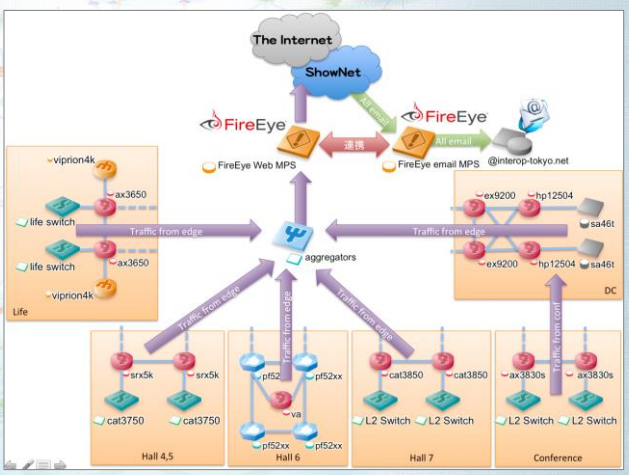


show net > Go to the next decade

INTEROP TOKYO | 11 – 14 JUNE, 2013

標的型攻撃対策

- 標的型攻撃対策
  - –高度な標的型攻撃の入り口・出口双方の対策としてemail及びweb対応の仮想化実行エンジン(サンドボックステクノロジ)を導入することで対策。
  - –全てのhttpなどの通信を分析・解析を行うことで、これまで検知が難しかった、会場内のPCからのコールバックやマルウェアを検知
  - –NOCで利用しているメールも、スピアフィッシングメールや添付されたエクスプロイトを起点とするマルチプローでの解析を実施

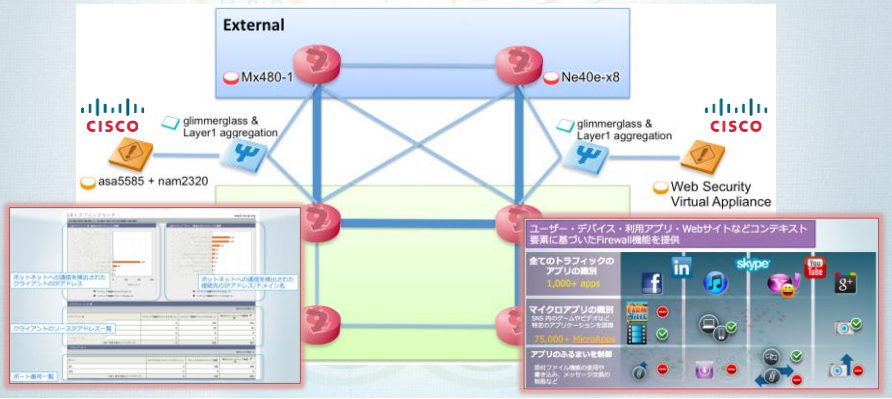


show net
> Go to the next decade

INTEROP
TOKYO | 11 – 14 JUNE, 2013

アプリケーション可視化と Webによるマルウェア検知

- バックボーンの上位にてトラフィックをモニタリングすることで、次世代ファイアウォールにて利用アプリケーションの可視化とマルウェアの検出を実施
  - シスコシステムズ社様ご提供のASA5585 + NAM2320によるマルウェアの検知
  - シスコシステムズ社様ご提供のWeb Security Virtual Applianceによるアプリケーション可視化



show net
> Go to the next decade

xFlow

INTEROP
TOKYO | 11 – 14 JUNE, 2013

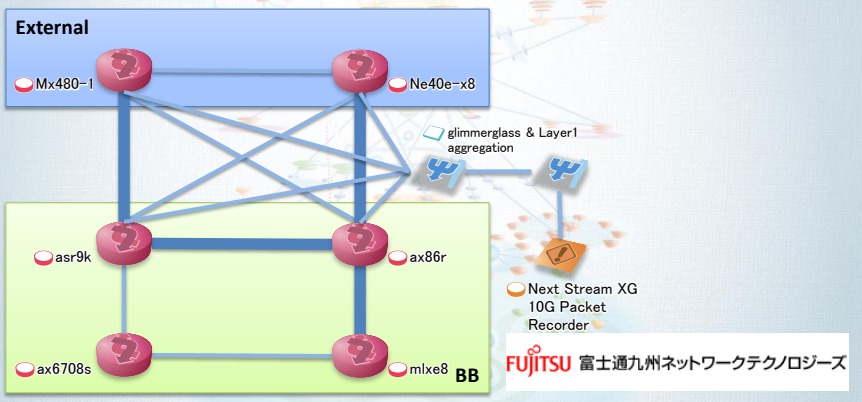
- 全てのxFlowパケットは全てNTTコミュニケーションズ社様yokozunaに集約し、コピーを転送
- sFlow/NetFlow対応ネットワーク製品からは直接yokozunaへFlow情報を送信
- sFlow/NetFlow未対応製品周辺では、TAPからトラフィックを抽出し、以下の2機種の製品で、NetFlowに変換しyokozunaへ送信
  - シスコシステムズ社様ご提供のNGA3140
  - オリゾンシステムズ社様ご提供のInveaTech社 IFP-2000
- ご提供頂いたFlow Collectorは以下の通り
  - NTTコミュニケーションズ社様ご提供のSAMURAI
  - 情報通信研究機構様ご提供のNirvana
  - オリゾンシステムズ社様ご提供のInveaTech社 IFC-1000

show net > Go to the next decade

INTEROP TOKYO | 11-14 JUNE, 2013

ネットワークレコーダー

- バックボーンを流れるトラフィックを、富士通九州ネットワークテクノロジーズ社様よりご提供いただいた「Next Steam XG 10G Packet Recorder」にてレコーディング。トラブルシュート時にトラフィック確認を後から実施する際に有効



show net > Go to the next decade

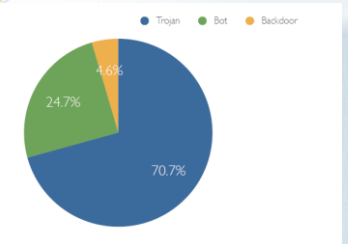
INTEROP TOKYO | 11-14 JUNE, 2013

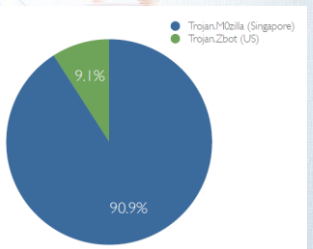
syslog/snmp

- 全てのSyslog及びsnmp-trapをNTTコミュニケーションズ社様ご提供の「yokozuna」へ送信
- 「よこづな」からは、以下のようにコピーを送信
  - NTTコミュニケーションズ社様ご提供の「maiko」へ全てのSyslog及びsnmp-trapを送信
  - 情報通信研究機構様ご提供の「NIRVANA改」へは、セキュリティ製品から送信される全てのsyslog及びsnmp-trapを送信
  - 奈良先端技術大学院大学様へはセキュリティ製品から送信される全てのsyslogを送信

Security Log 解析結果速報

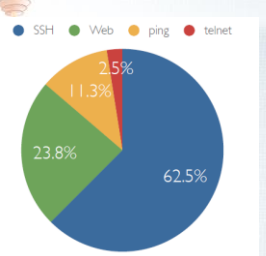
- FireEye
  - 総計 1,867件
  - 出展者割当アドレス以外でのアラートは11件

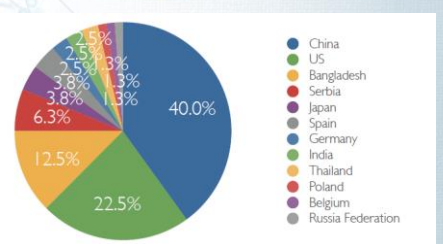




Security Log 解析結果速報

- FortiGate UTM
  - プロトコル別が右上
  - 国別が右下





show net
> Go to the next decade

100Gbps開通

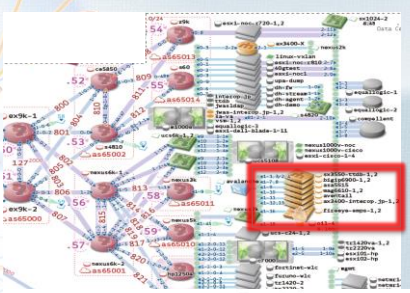
INTEROP
TOKYO | 11 – 14 JUNE, 2013

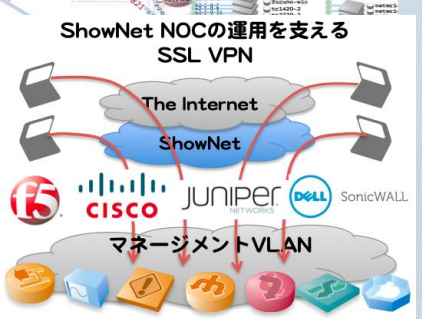
show net
> Go to the next decade

SSL VPN

INTEROP
TOKYO | 11 – 14 JUNE, 2013

- SSL VPN
  - –運用管理目的でマネージメントセグメントへのアクセスで利用
  - –ShowNet連携デモでも利用し、各コントリビュータ様ブースからShowNetのライブで利用されている装置をブースでデモ
    - シスコシステムズ社様よりASA5515
    - ジュニパーネットワークス社様よりMAG6610
    - デル社様よりAventail
    - F5社様よりBigIP-6900
  - –コントリビューター各社様におけるShowNetとブースでの連携デモとNOCの運用管理では必要不可欠なテクノロジー



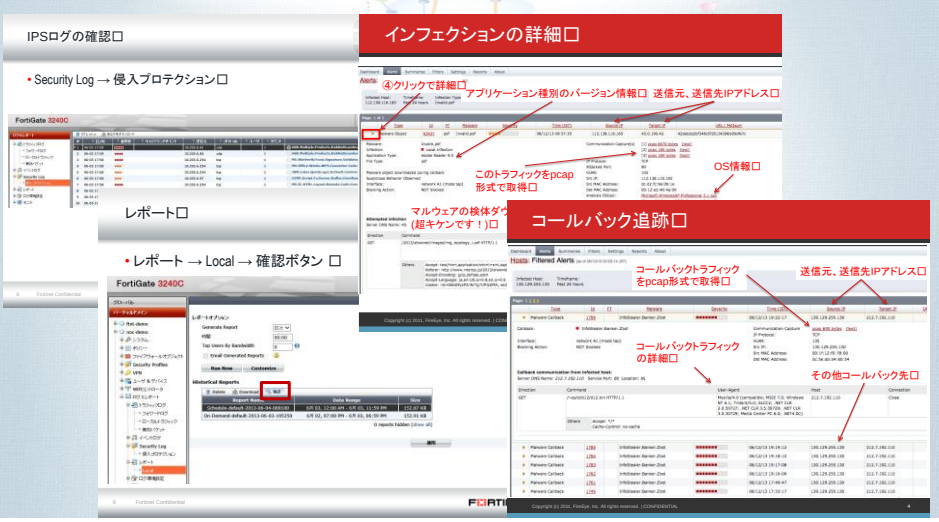


セキュリティ製品体験デモコーナー

- セキュリティ製品群は可視化が困難なため、ShowNet2013では体験デモコーナーを設置
- ShowNetで利用されている各社様の製品群を実際に操作して頂くことで、ビジビリティ向上に貢献

セキュリティ製品体験デモコーナー

- 操作方法例を明確化することで、簡単に体験可能に。



ShowNet完成までの軌跡

- ShowNet構築過程を可視化することで、生のShowNet構築までの軌跡を辿ることで、より親近感のあるShowNetへ

クレジット

show net > Go to the next decade

INTEROP TOKYO | 11-14 JUNE, 2013

本資料について

- 本資料に関するお問い合わせ先
  Interop Tokyo 2013 運営事務局
  株式会社ナノオプト・メディア
  ShowNet担当：大嶋
  Tel: 03-6431-7803 Email: shownet@f2ff.jp

show net > Go to the next decade

INTEROP TOKYO | 11-14 JUNE, 2013

Special Thanks…

Sponsors

AlaxalA NEC NTT Communications CISCO JUNIPER NETWORKS 東陽テクニカ NISSHO ELECTRONICS Network Initiative

Co-Sponsors

ISA IXIA vmware A10 Networks ATEN SII Allot PeerApp FXC Schneider Electric NICT SEIKO DELL IBM HP Hitachi Cable HUAWEI FireEye FORTINET FUJITSU Plat'Home FLUKE networks FURUNO SYSTEMS BROCADE MKI YAMAHA

Supporters

IT Frontier Infoblox Web Service Development NCLC ORIZON クオリティネット株式会社 JUNIPER DYDEN DATAHOTEL 東京大学 NTT西日本 jpix Bitrieve ALAXALA RISO LogicVein

（株）Xenlon/さくらインターネット（株）/国立情報学研究所/ドコモ・システムズ（株）/トランスコスモス（株）/センターピア（株）KDDI（株）/慶應義塾大学/倉敷芸術科学大学/インターネットマルチフィード（株）/（株）インターネットイニシアティブ（株）/アールシーエー/WIDEプロジェクト/北陸先端科学技術大学院大学/古河ネットワークソリューション（株）/日本テレガートナー（株）/奈良先端科学技術大学院大学/（株）ナビタイムジャパン