INVEA-TECH & AdvaICT: FlowMon + ADS

ネットワークモニタリングとセキュリティの完全なソリューション

インベアテック
日本代表　中西　陽一
yoichi@invea-tech.com

INVEA-TECH & AdvaICT

- 大学からのスピンアウト企業
  - １０年以上、EU 投資のプロジェクトに開発メンバーとして参加
  - ルーターやプログラム可能なハードウエアの開発などで１０００万ユーロの投資をし、ワールドクラスの独自性の高い技術を創出
- 会社情報

  強いアカデミックなバックグランド：CESNET, MU, VUT

  2007年設立、最初の1年で５０顧客獲得

  チェコ共和国国内でリーディングカンパニー

  強固な国内基盤をもとに、海外進出

- 主な製品:

  FlowMon: ネットワークトラフィックの監視

  ADS: ふるまい検知、運用、セキュリティ問題への対応

  FlowMon + ADS = 監視、セキュリティの完成されたソリューション

事例

- GEÁNT2, Federica – **7つのヨーロッパバックボーンを監視**
- Czech Ministry of Defense
- Korea Telecom
- Uniqa, AVG
- CESNET
- T-Mobile
- University of Madrid

大事なポイント – IT Director

- IP Flowに基づくネットワーク監視

  ネットワークで実際に何がおきているかわかってますか？
  インターネットだけではなくLANやWANで、リアルタイムにあるいは時系列で？

- セキュリティ – NBA (ファイアウォールだけでは不十分)

  サービスに対するDOS, DDOSアタックを簡単に検知できますか?

  アンチウイルスソフトで検知できないウイルスやマルウエアを見つけ出せますか?

  疑わしいふるまいの兆候を検知するツールを持っていますか?

- ネットワークインフラの最適化

  インターネットやWAN接続のために過剰投資していませんか?

  ネットワークは遅くありませんか? アプリケーションのレスポンスが悪くないですか？

- 従業員の効率性

  P2Pサービスやインスタントメッセージが使われていませんか?

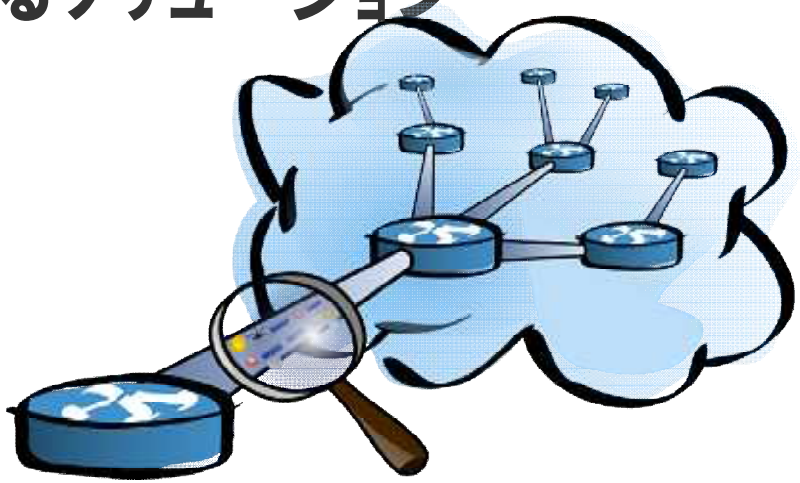
  疑わしいWebページにアクセスしていませんか?

大事なポイント – IT 管理者

- ネットワークで何がおこっているかを正確に把握していますか?
- 本当にネットワークが安全だと確信もてますか?
- ネットワークの問題を迅速に簡単に検知できますか?
- ネットワークは社内及び社外の攻撃から守られていますか?
- リアルタイムにネットワークトラフィックを把握していますか?
- どのユーザ、サービスがネットワークの帯域をどれだけ占有しているか、実際のインターネット帯域使用量を把握していますか?
- ネットワーク問題、トラブルの検知を簡単にできますか?
- SLAを確認できていますか?
- アカント、ビリング、FUP コントロールがシンプルで使いやすいシステムを持っていますか?
- データ保持規定を遵守していますか?

FlowMon

- IP Flowを使った革新的なネットワーク監視ソリューション
- NetFlow v5/v9及びIPFIX技術に準拠
- 誰が誰とどれぐらい通信したか、プロトコルやトラフィック量その他の情報を提供
- 前のページのすべての質問に対する答えを用意
- 業界で最もコストパフォーマンスに優れた製品
- すべての種類のネットワークに対するソリューション
- お客様にとって数多くのベネフィット
- ネットワークを管理者の支配下に!



ガートナー 調査と現実

- ガートナー

  監視なしのセキュリティはあり得ない。ファイアーウォール、IPSを導入してチューニングや修復をしても、監視やNBAをさらに検討すべきである。

  安全な組織=ファイアーウォール+IPS+NBA/NBAD/ADS

  ネットワーク通信の監視やネットワークのふるまい検知は2010年の最も重要な10の技術のうちの1つ

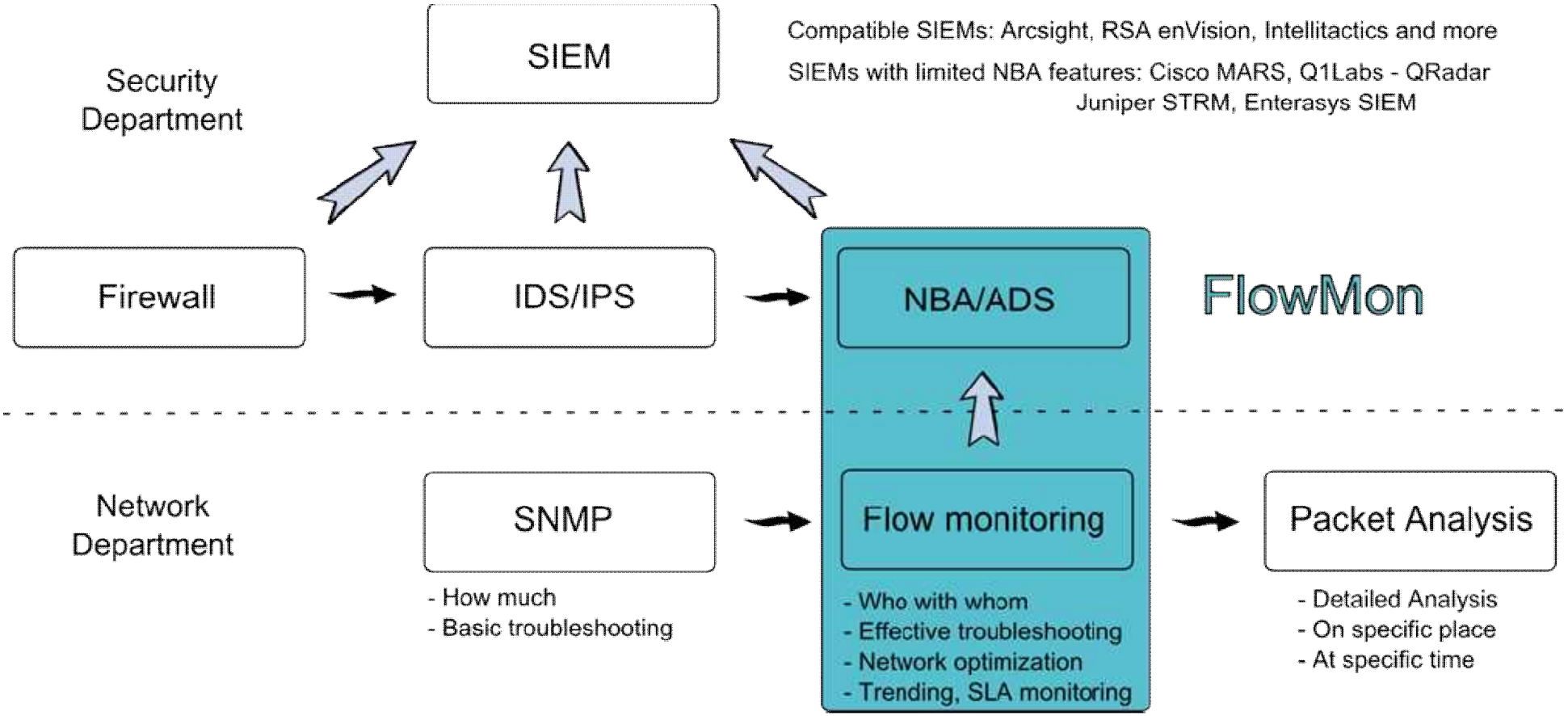
- 現実

  多くの組織はネットワーク監視やIP Flowのモニタリングシステムを持っていない

  FlowMon + ADS 他のモニタリングシステムとも完全な連携ができる

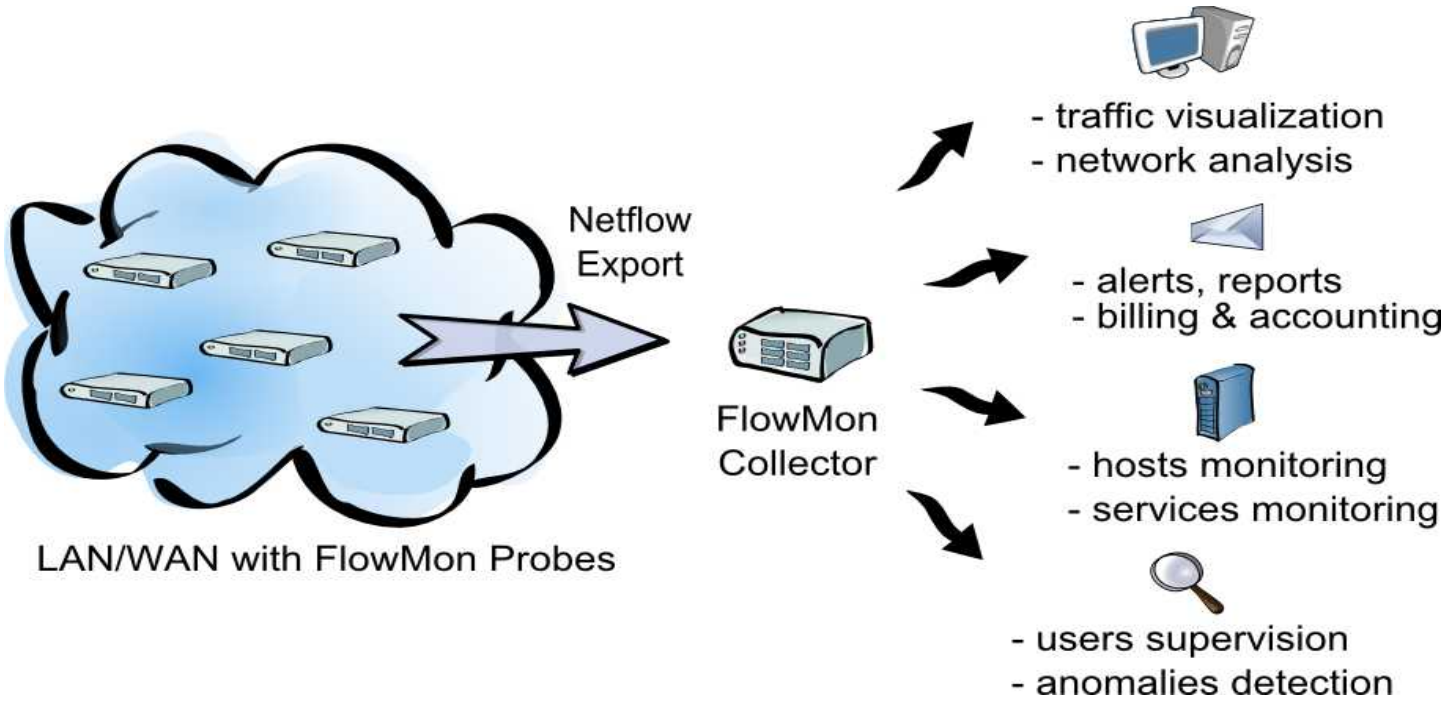
  今でも監視、セキュリティについての増え続ける課題が金融業界、CISRTチームからつきつけられている

技術概要

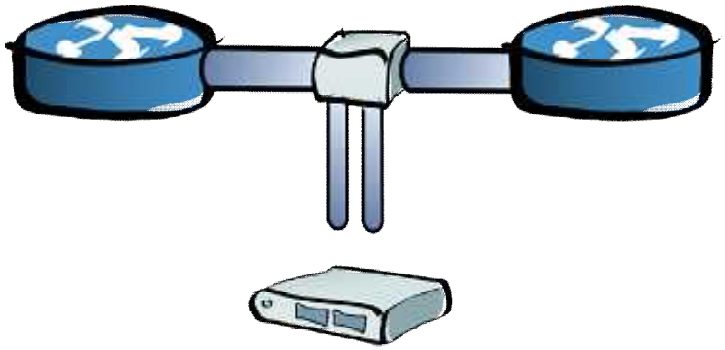

SIEM
Compatible SIEMs: Arcsight, RSA enVision, Intellitactics and more
SIEMs with limited NBA features: Cisco MARS, Q1Labs - QRadar
Juniper STRM, Enterasys SIEM
Security Department
Firewall
IDS/IPS
NBA/ADS
FlowMon
Network Department
SNMP
- How much
- Basic troubleshooting
Flow monitoring
- Who with whom
- Effective troubleshooting
- Network optimization
- Trending, SLA monitoring
Packet Analysis
- Detailed Analysis
- On specific place
- At specific time

FlowMon アーキテクチャー

- スタンドアロンの FlowMon プローブ – ネットワーク統計情報の収集
  - NetFlow / IPFIX data
- 仮想化やネットワーク統計情報評価のためのフローデータの収集



FlowMonプローブ接続

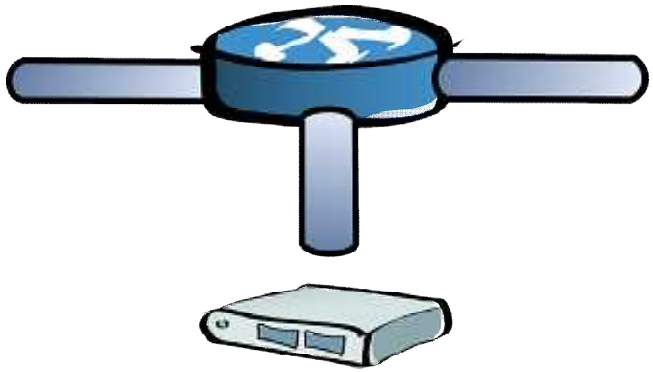


銅線/ファイバー TAP

TAP モード

バックボーン

インターネットアップリンク



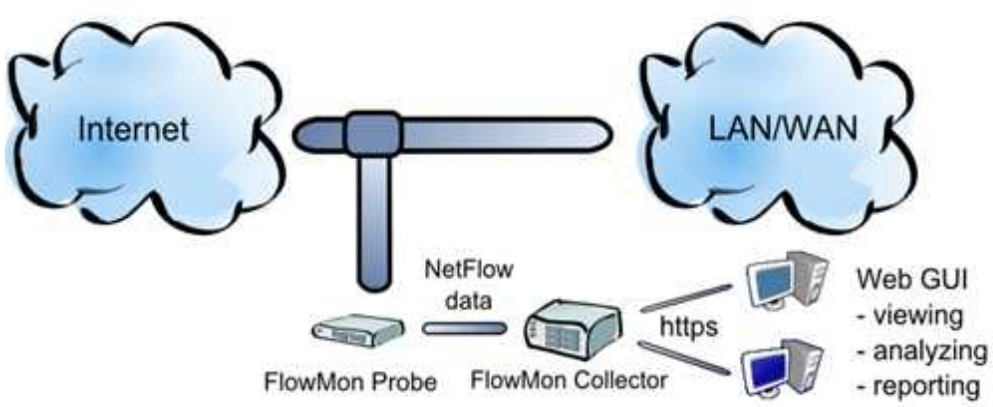
ルーター/スイッチミラーポート

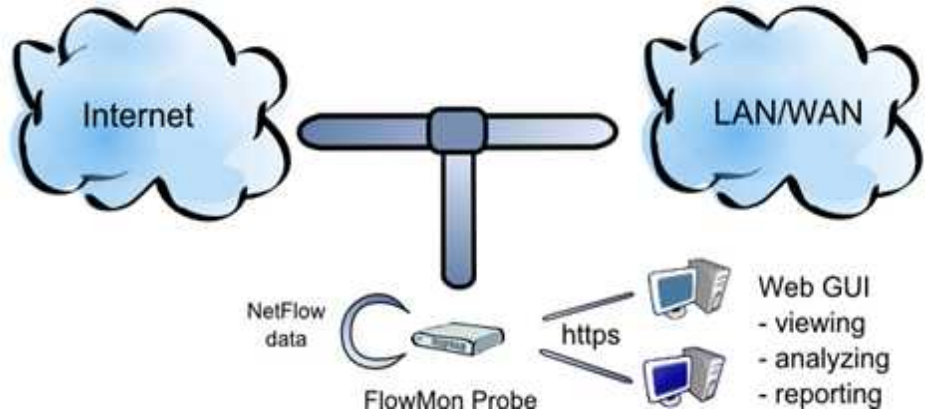
SPAN モード

LAN モニタリング

FlowMon プローブ

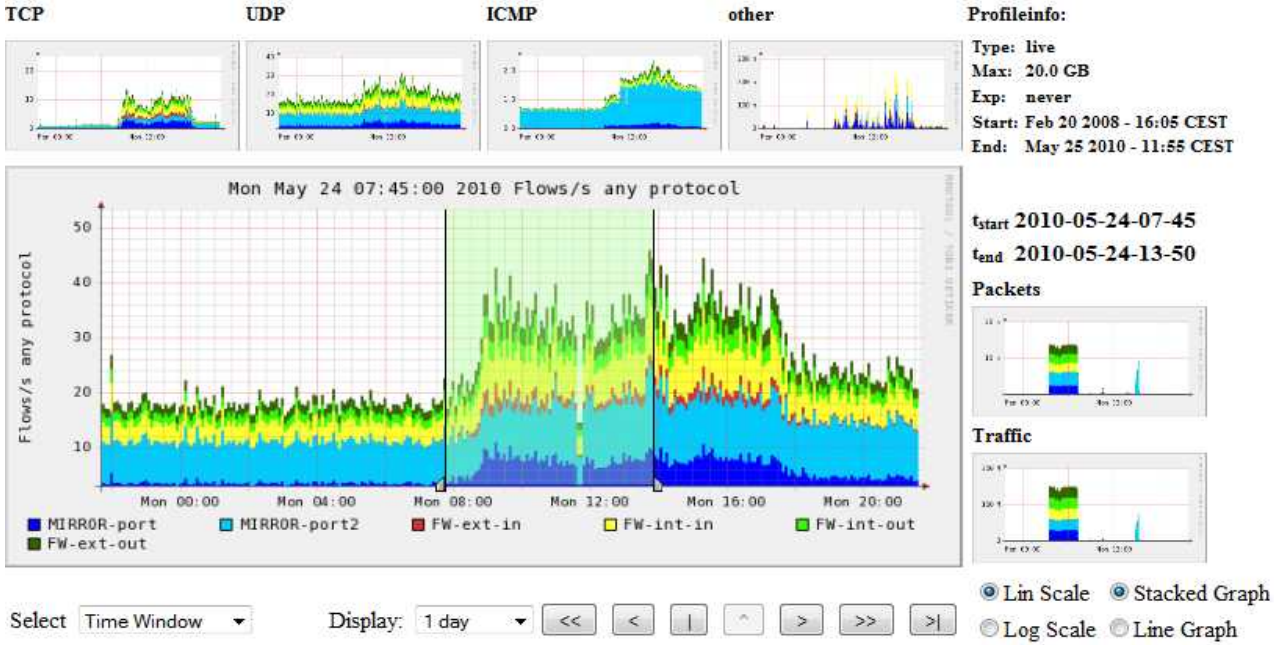
- 高速なスタンドアロンプローブ - NetFlow v5/v9と IPFIX に対応したIP フローレコードのソース
- L2/L3 の見えないデバイス – 監視されたネットワークの可視化
- 標準化及びハードウェアアクセラレートモデル
- Web GUIでの遠隔地からの設定
- 10/100/1000 Ethernet, 10 GE, IPv4, IPv6, MPLS, VLAN





FlowMon 監視センター

- グラフ、テーブル、さらなるデータプロセスのためのフォーム
- 上位統計情報 (ユーザー、サイト、サービス)
- 標準プロトコルに対応したあらかじめ定義されたプロファイル
- 定義されたユーザープロファイル (IP アドレスやポート情報)
- プロファイルサポート及びアラート (電子メールなど)



FlowMon – プラグイン

FlowMon
Configuration Center

FlowMon
Monitoring Center

Caligare
Flow Inspector

FLUKE networks

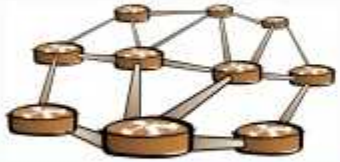
NetFlow Tracker

FlowMon Reporter

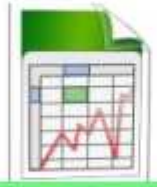
FlowMon
Firewall Auditor

FlowMon HTTP Logger

FlowMon Data Retention
485/2005



Nagios



Zabbix

Temperature and
Environmental Monitoring

NAT Detective

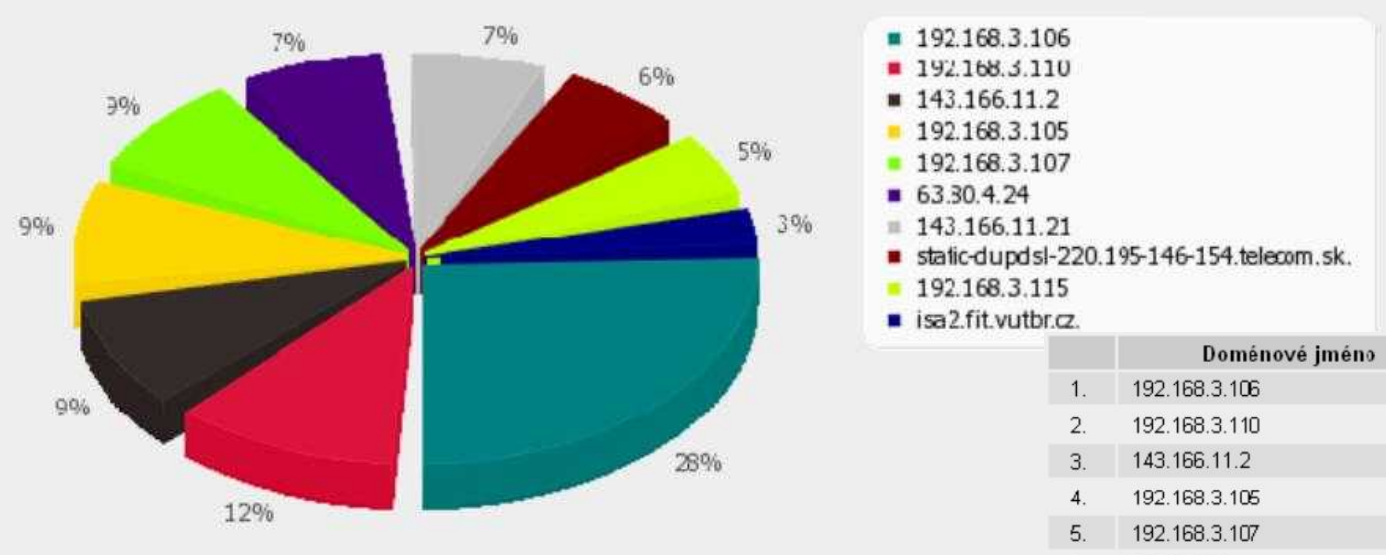
Will be available soon.

プラグイン- ケーススタディ

あなたは上司に円グラフのチャートを提出する必要がありますか？

FlowMon レポーター

- インテリジェントなレポーティングツール - PDF, CSVでの表示
- 直近の日、週、月でネットワーク上で何が起こっているかの概要表示
- オンラインではWeb表示、オフラインでは電子メールレポート



	Doménové jméno	IP adresa	Bity/s	Bajty
1.	192.168.3.106	192.168.3.106	19.5 k	80.01 M
2.	192.168.3.110	192.168.3.110	3.4 k	34.62 M
3.	143.166.11.2	143.166.11.2	7.0 k	27.75 M
4.	192.168.3.105	192.168.3.105	6.3 k	26.04 M
5.	192.168.3.107	192.168.3.107	7.6 k	25.18 M
6.	63.80.4.24	63.80.4.24	1.1 M	21.27 M
7.	143.166.11.21	143.166.11.21	307.8 k	20.41 M
8.	static-dupdsl-220.195-146-154.telecom.sk.	195.146.154.220	225.4 k	18.79 M
9.	192.168.3.115	192.168.3.115	3.9 k	15.64 M
10	isa2.fit.vutbr.cz	147.229.176.17	2.0 k	9.35 M
	Celkem		16.4 k	164.6 M

FlowMon レポーター

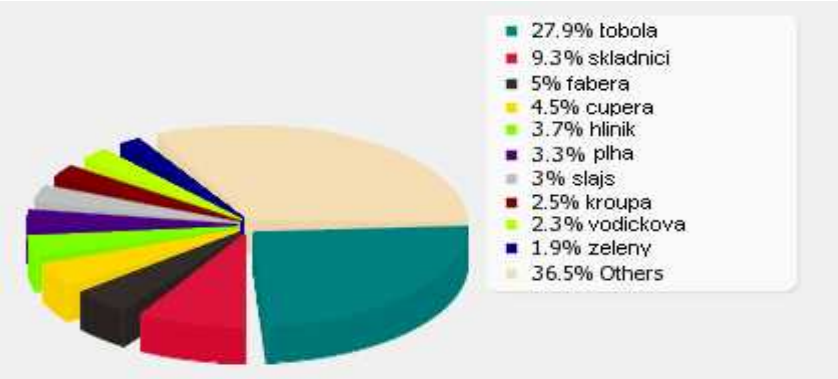
- IT管理者のためのレポート例
  - インターネット接続の負荷は何か？
  - ネットワーク上でどのような異なるサービスが使われているのか？
  - 誰が重要なサーバーの使用率が多いか？
  - 通信上で疑わしいピークが存在しないか？
- 経営陣のためのレポート例
  - Web訪問者のトップランキング
  - 最も人気のWebサイトは何か？
  - 誰が最も多く電子メールを送っているか？
  - 誰がP2Pネットワークのヘビーユーザーか？

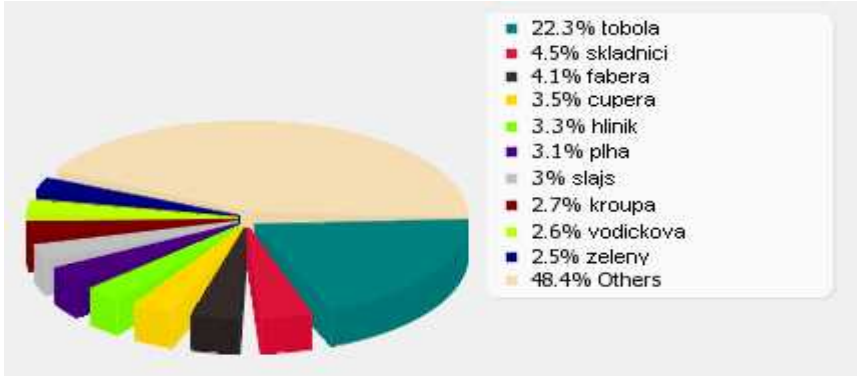
プラグイン – ケーススタディ

あなたはどのWebサイトが従業員によく見られているか知っていますか？

FlowMon HTTP Logger

- 最も頻繁に見られているWebサイト、最もアクティブなユーザーの概要





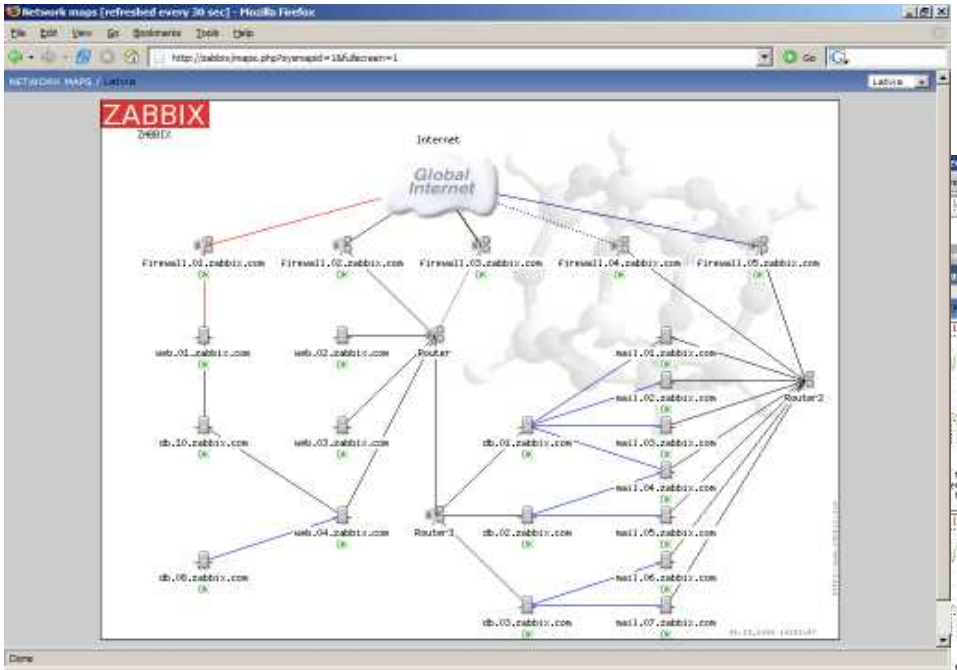
Uživatel	Servery		Domény	
tobola	1131	www.freeefoto.cz	1228	idnes.cz
	147	online.gamesy.cz	264	gamesy.cz
	89	www.idnes.cz	69	freeefoto.cz
	69	www.superstar.cz	42	superstar.com
	48	www.blesk.cz	39	invea-tech.com
	39	www.invea-tech.com	33	google.com
	31	www.lolytky.cz	31	tipsport.com
	31	suggestqueries.google.com	31	lolytky.cz
	31	www.tipsport.cz	29	org.uk
	29	www.agi.org.uk		

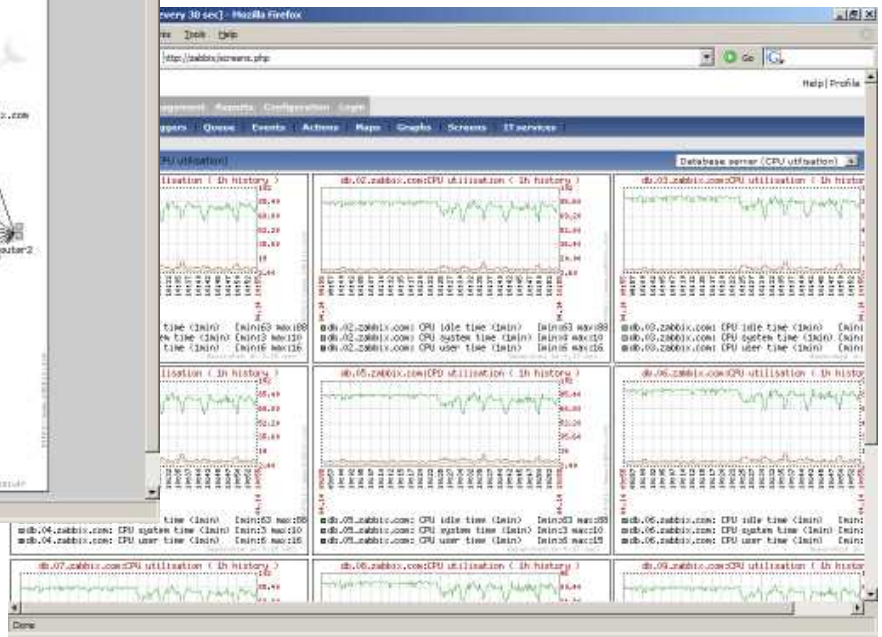
プラグイン – ケーススタディ

あなたは稼動中のネットワーク構成、サーバー、サービスを監視する使いやすいツールを利用したいですか？

Zabbix

- システム上の異変を事前に察知してユーザーからクレームが上がる前に警告
- ネットワーク構成、サーバー、サービスの監視
- ICMP, SNMP, CPU使用率監視エージェント等





プラグイン – ケーススタディ　ISP

データ保持規定の基準を満たしていますか？（EUの場合）

FlowMon Data Retention

- EC域内での指令– 2006年
  - すべてのISPはIP通信の統計情報をすべて保持しなければならない
  - 最低でも6ヶ月の履歴保持
- FlowMon Data Retentionはチェコ共和国政府の指針に従い、履歴保持の基準値をクリア

INV_070801_1001.txt - KWrite

Soubor Úpravy Pohled Záložky Nástroje Nastavení Nápověda

INV_070801_1001.txt, chat, 212.96.164.9, 2007-08-01 07:00, 2007-08-10 07:00, UTF8, GMT +01:00

ID	SRC_IP:PORT	DST_IP:PORT	PROTOKOL	START	STOP	SLUZBY	KBYTES
0	212.96.164.9:1663	64.12.24.142:5190	TCP	2007-08-01 07:00:12.933	2007-08-01 07:00:32.120	chat	2539
0	212.96.164.9:2340	64.12.31.136:5190	TCP	2007-08-01 07:14:02.203	2007-08-01 07:25:55.200	chat	10258
0	212.96.164.9:1500	64.12.24.142:5190	TCP	2007-08-01 08:05:33.000	2007-08-01 08:45:10.030	chat	34258
0	212.96.164.9:1700	64.12.24.142:5190	TCP	2007-08-01 09:00:04.300	2007-08-01 09:15:10.230	chat	7865
0	212.96.164.9:1700	64.12.24.142:5190	TCP	2007-08-01 09:16:00.000	2007-08-01 09:25:00.050	chat	2987
0	212.96.164.9:1700	64.12.24.142:5190	TCP	2007-08-01 09:26:09.000	2007-08-01 09:45:20.600	chat	67890

プラグイン – ケーススタディ

あなたは社内、社外のネットワークセキュリティが万全だといえますか?

社内のネットワークに設定や運用上の問題はありませんか？

従業員教育は施されていますか?

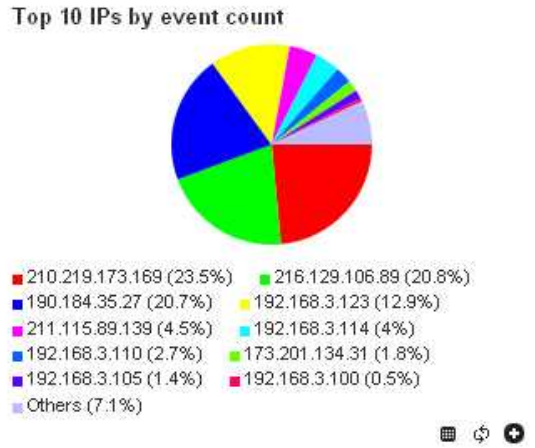
従業員は望ましくないサービスやアプリケーションを使ったりしていませんか?

FlowMon ADS

- 好ましくないふるまいの検知
  - 攻撃
  - 好ましくないサービス
  - 設定や運用上の諸問題
- ふるまい
  - 誰と誰の通信？
  - 異常検知
  - 通信量と構造
- 直感的なユーザーインターフェース
  - 迅速なネットワークにおける問題点の指摘
  - イベントの見える化
  - DNS, WHOIS, 位置情報サービスから取得した情報を統合
- 複雑なフィルタリング設定、アラート、レポート取得

Latest 10 events

#	Event type	Source IP	Target IP	Timestamp
1	INSTMSG	192.168.3.105	64.12.24.192	09:00:53
2	INSTMSG	192.168.3.123	205.188.0.206	09:00:30
3	MULTICAST	192.168.3.114	192.168.3.255	09:00:19
4	MULTICAST	192.168.3.105	192.168.3.255	08:59:50
5	DIVCOM	192.168.3.105		08:59:18
6	MULTICAST	192.168.3.123	192.168.3.255	08:58:49
7	MULTICAST	192.168.3.100	192.168.3.255	08:58:18
8	DIVCOM	192.168.3.123		08:56:35
9	MULTICAST	192.168.3.123	192.168.3.255	08:53:44
10	MULTICAST	192.168.3.123	192.168.3.255	08:53:44



FlowMon ADS

- **通信の好ましくないパターンを検出**
  - 攻撃 (ポートスキャニング、辞書攻撃、サービス拒絶、Telnet通信)
  - データ通信の異常 (DNS、マルチキャスト、標準化されていない通信)
  - デバイスふるまいの異常 (長期間保持されていたプロファイルの変更)
  - 好ましくないアプリケーション (P2Pネットワーク、インスタントメッセージ)
  - 社内のセキュリティ問題 (ウイルス、スパイウエア、ボットネッツ)
  - 電子メールトラフィック (スパムメール)

Events

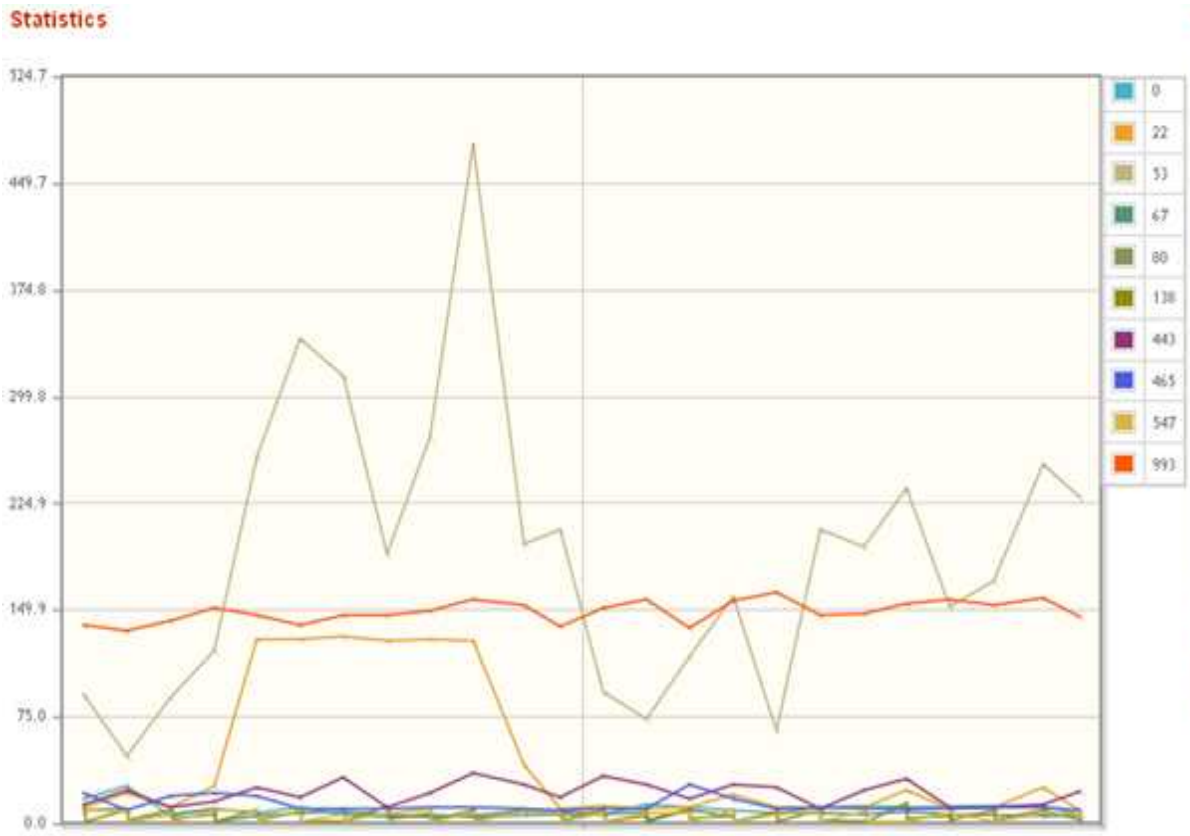
#	Event source	Type	Details	Timestamp	Data source	Event targets
1	[redacted]67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 7)	2009-09-24 19:23:00	PiF	62.3.131.181, 69.7.167.23, 146.201.3.234, 194.109.24.132, 209.145.5.10, 210.101.199.231, 213.232.0.195
2	[redacted]67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 65)	2009-09-24 19:17:45	PiF	62.3.131.181, 63.101.151.1, 64.18.4.11, 64.18.5.10, 64.18.6.10, 64.18.6.14, 64.18.7.13, 64.191.223.42, 65.55.88.22, 65.172.13.10, ...
3	[redacted]67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 75)	2009-09-24 19:16:00	PiF	62.12.136.97, 63.166.155.140, 64.18.6.10, 64.18.6.11, 64.18.7.11, 64.26.60.153, 64.88.167.155, 64.118.228.132, 65.55.88.22, 65.61.115.199, ...

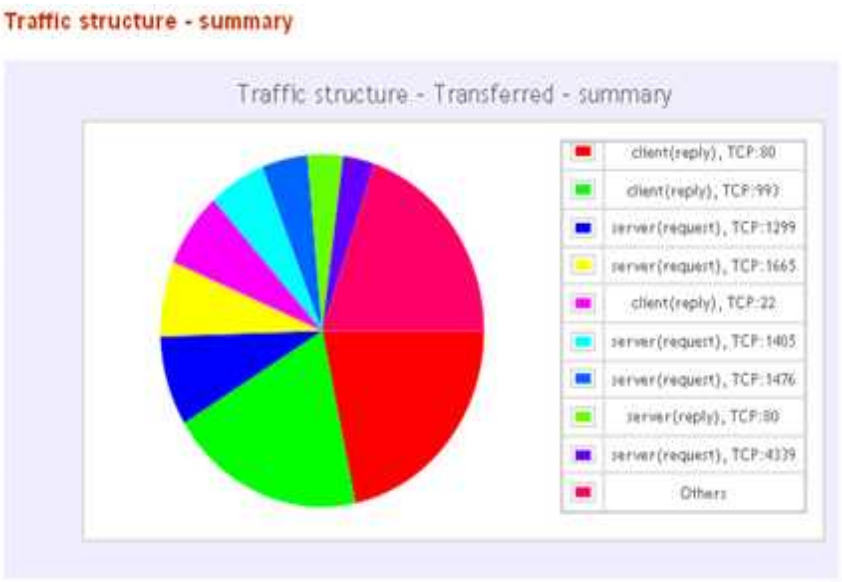
FlowMon ADS

- **ふるまい分析**

  ふるまいプロファイル (クライアント/サーバー、データ通信、パターン、トラフィック構造)

  異常検知 (直近のふるまいと長期間保持されていたプロファイルとの比較)



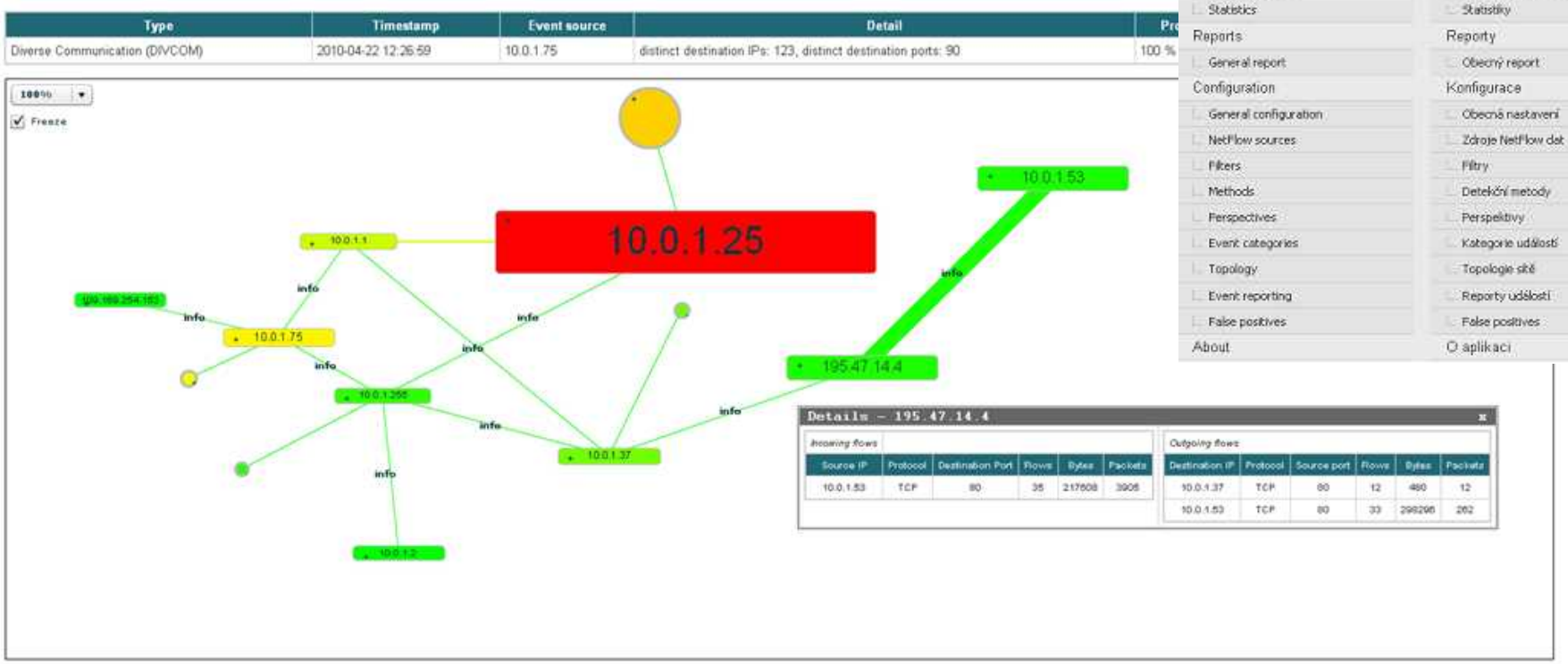


Communication peers - Summary (->Details)

Date	Client peers	Server peers
2010-04-28 - 2010-04-29	60	49

FlowMon ADS

- **ユーザーインターフェース**
  - **馴染み易いWebインターフェース**
  - **イベントに対して多角的な画面の提供**
  - **ふるまいプロファイルのルックアップ**
  - **双方向通信、イベントの見える化**



FlowMon ADS

- **主な顧客の利点**

  ITインフラ問題の処理解決

  - セキュリティ指針や規則に準拠
  - 社内、社外の攻撃、情報漏えい
  - QOS、ネットワークやサービス遅延
  - 好ましくないアプリケーションやデータの共有
  - ネットワーク上で感染したデバイスや誤った設定

  効果的なプロセス及びよりセキュアなインフラ

  - 感染する前に検知し問題からの切り離し

  より少ない支出で生産性の向上

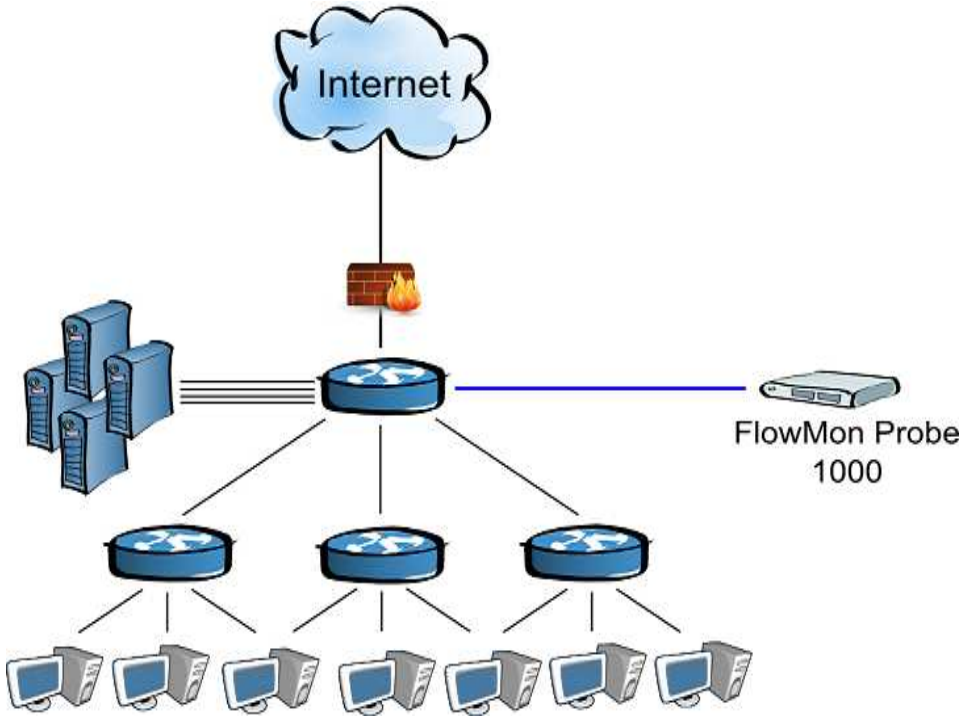
  - 問題が検知されたあと、直ちに分析
  - ユーザーごとのネットワーク使用状況についての把握

- **容易な設定と即時的な効果**

  容易な設定と迅速な導入展開

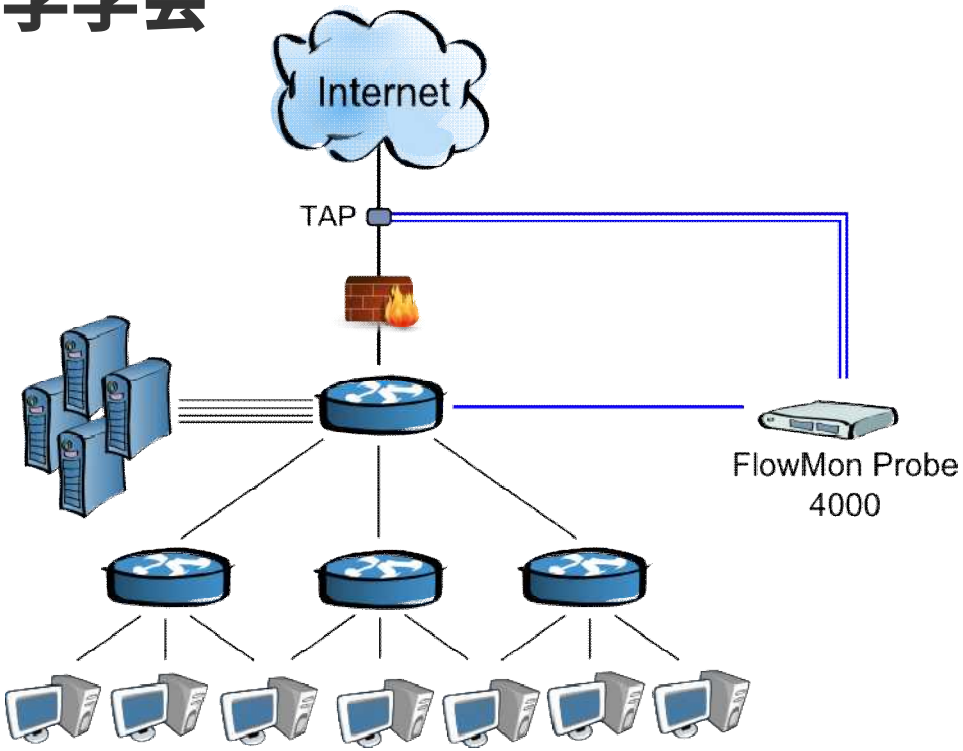
典型的なプロジェクト – 小規模

- 社内ネットワークとインターネット使用状況についての監視
- プラグイン統計ツールも利用
- 事例：Olomouc病院、MVVエナジー等



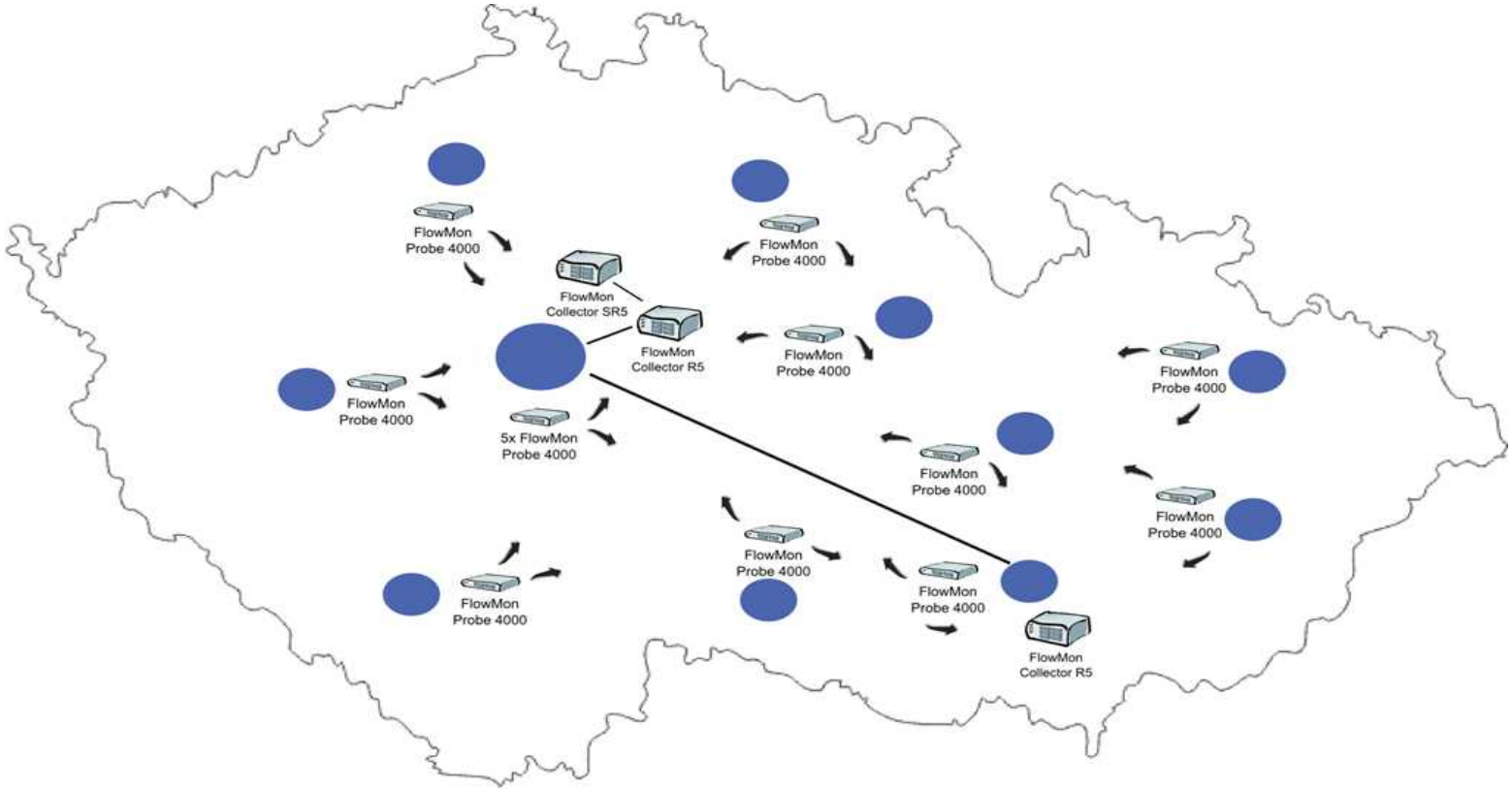
典型的なプロジェクト – 中規模

- アクティブデバイスのSPANミラーポートを使用して社内ネットワークを監視。ファイアーウォール背後の通信はTAPを使って監視。4ポートのギガポートをプローブに実装
- プラグイン統計ツールを実装
- 事例: Aegon, Olomouc科学学会



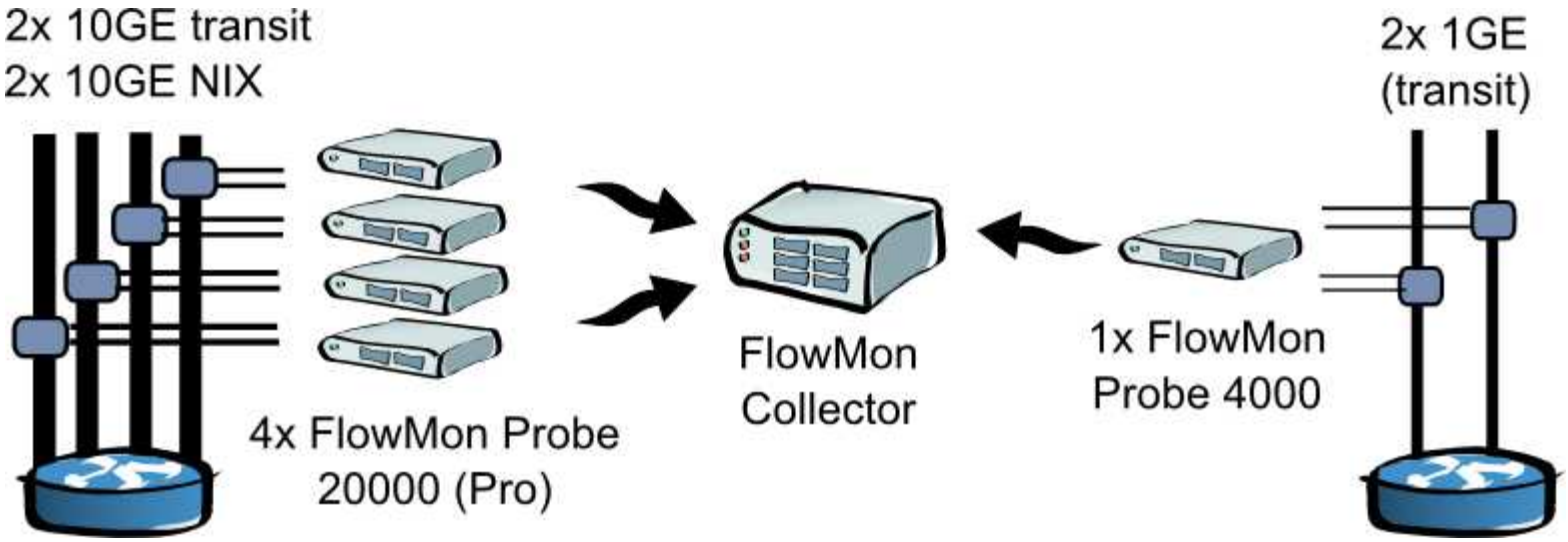
典型的なプロジェクト – 大規模

- 各地のプローブ、コレクター、プラグイン統計ツールからの一括情報収集と監視
- 多種のプラグインツールを活用して、多面的に分析
- 事例: AVG, 防衛省



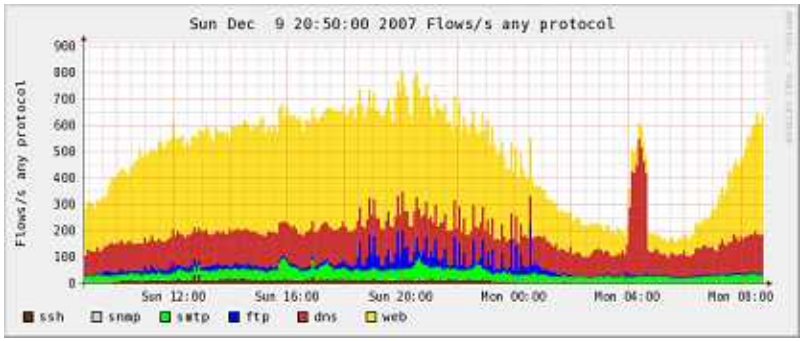
典型的なプロジェクト - ISP

- アップリンク監視
- 標準的なプロジェクト規模
  - 小規模ISP, 1-2 ギガビットリンク
  - 大規模ISP, 10　ギガビットリンク
- 事例: Sloane Park, ČD Telematika, KT Přerov



システム管理者のベネフィット...

- 全体ネットワークの可視化 (LAN, WAN) – リアルタイムと時系列
- ネットワークパフォーマンスの監視
- 素早く、正確で効果的なトラブルシューティング
- インターネット使用状況の監視 (ゲーム、ビデオストリームなど)
- 効果的なキャパシティプランニングとトラフィックエンジニアリング
- 社内及び社外からの攻撃検知
- ユーザー別リソース使用状況及びアプリケーション利用状況のランキング表示



..セキュリティ部門と経営陣..

- セキュリティ部門のベネフィット

  社内、社外攻撃発生前のふるまい変化、兆候の検知

  データベースへのユーザーアクセスのコントロール

  調査及びセキュリティインシデントの証明

  ステータスとセキュリティポリシーの比較

  情報漏えいの事前阻止

- 経営陣のベネフィット

  ネットワークの管理及び運用におけるコスト削減

  視覚的な統計情報 (テーブル、円グラフなど)

  従業員ごとのリソース使用状況の監視 (労働時間中の業務に無関係なアクセス)

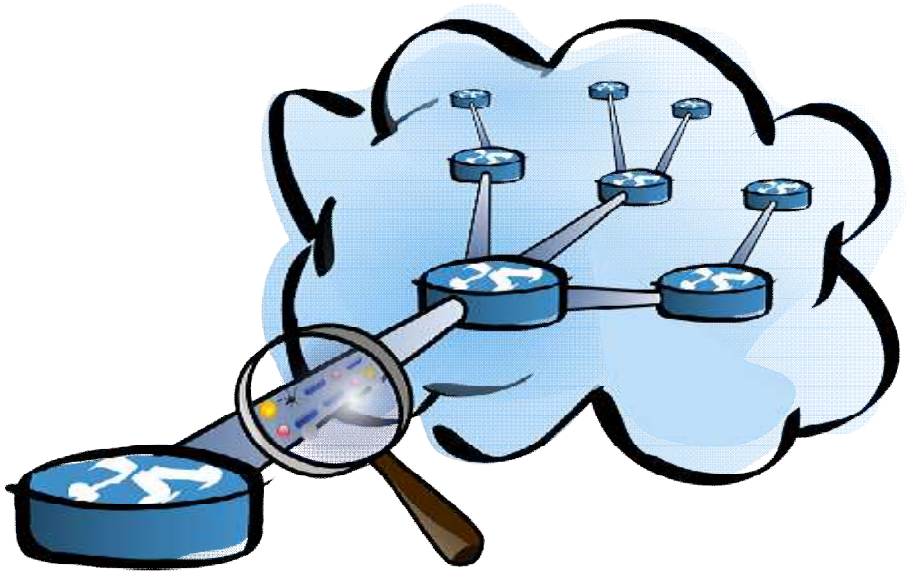
  P2Pアプリケーションの使用状況の把握

…インターネットサービスプロバイダー

- トラフィックについて長期間の統計情報を保持
- ネットワークのキャパシティプランニング
- 最適で効率的な接続
- 高品質なSLAの実現
- データ保持規定に準拠
- トラフィック容量に応じた課金システムの確立
- グラフやテーブルを自社システムに組み込み

FlowMon ソリューションの利点

- あらゆる種類のネットワークに対してサービス対応可能
- スケーラブルで柔軟なソリューション
- 優れたコストパフォーマンス



ネットワークセキュリティ分析

- 顧客へのプロフェッショナルサービス
- セキュリティ、パフォーマンス、リソース最適化についての深い考察と分析情報を提供
- ネットワーク監視とセキュリティについての豊富な経験と実績
- ネットワークセキュリティ分析の利点
  - ネットワークトラフィックの詳細なビュー
  - 素早く正確なトラブルシューティング
  - 予測可能なインシデントの事前防止
    (ネットワークオーバーロードと障害)
  - ユーザーとアプリケーション稼動状況の監視と分析
  - ネットワークセキュリティの改善