

Manažment a monitoring bezpečnostných incidentov v informačných systémoch (Security incident event management & monitoring)

eFOCUS

 **inveaTECH**

Next-Generation Network, Security & Apps Behavioral Monitoring

Roman Čupka, Invea-Tech

Predstavenie Invea-Tech

- Spoločnosť identifikovaná Gartnerom od roku 2010
- 2x Deloitte CE Technology Fast 50
- Aliancia s medzinárodnými výrobcami ako CISCO, Checkpoint, Radware a ďalšími
- Prvá 100 Gbps NIC na svete
- 600+ klientov po celom svete

Gartner
Research

ID Number: G00208386

Deloitte.

CE Technology Fast 50

Certificate of achievement

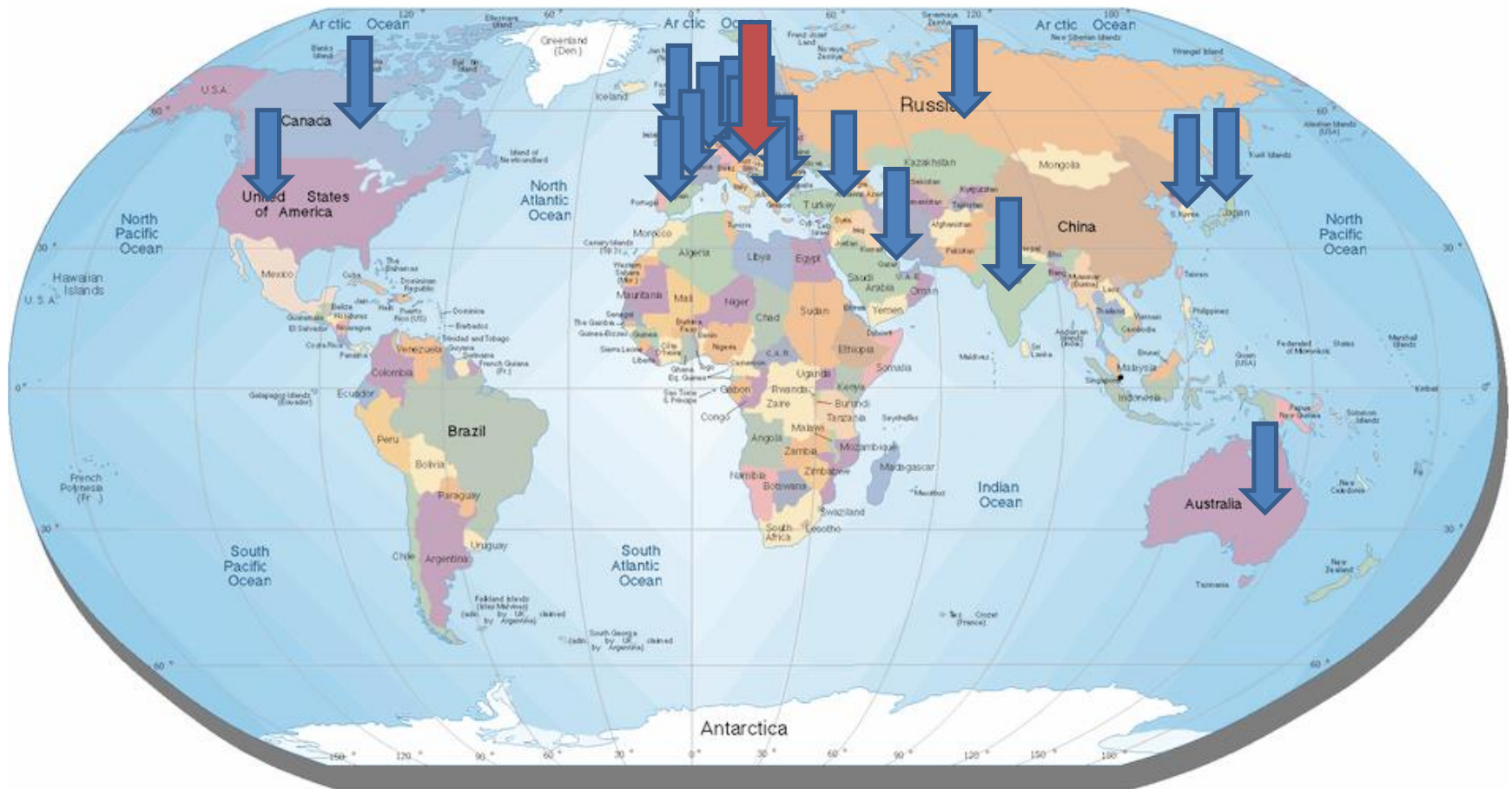
INVEA-TECH a.s.



Check Point
SOFTWARE TECHNOLOGIES LTD.



INVEA-TECH globálna presencia



Gartner a Invea-Tech

Gartner

„Neexistuje bezpečnosť bez monitoringu. Mnoho ľudí bolo dlho presvedčených že bezpečnosť stačí budovať na perimetri a monitoring je zbytočná práca nad rámec povinností. Opak je pravdou.“

Recommendation

After you have successfully deployed firewalls and intrusion prevention systems with appropriate processes for tuning, analysis and remediation, you should consider NBA to identify network events and behavior that are undetectable using other techniques.

Invea-Tech's FlowMon solution analyzes v.5, NetFlow v.9 and IPFIX traffic. It includes the appliance-based FlowMon collector, which processes flow data from routers or from optional FlowMon probes (exporters). A software plug-in can be added to the collectors and exporters to deliver NBA functionality by providing statistical analysis and anomaly detection. For smaller

Research

ID Number: G00208386

Vendor Analysis

The vendors in the following section (see the Introduction and Use Cases section). In addition to packet capture collectors and flow exporters. The exporters export and/or stateful packet inspection and correlation records, NetFlow v.9 or IPFIX records). v.5 records and enable these solutions to be superior to the solutions offered by vendors.

Invea-Tech

Gartner a Slovensko

IT SUMMIT 2014:

Rok 2015 podľa CIOs SR z pohľadu investícií – 1. miesto - **Infraštruktúra a Datové centrá**

Rok 2015 podľa CIOs SR z pohľadu poznatkov – 1. miesto – **Zabezpečenie informácií a ich monitoring**

Kyber hrozby dnes a zajtra

- **Viac sofistikovaný malware**

- POS, Ransomware (cloud, inteligentné zariadenia), Targeted malware a pod.
- Nezabezpečené OS (Windows, Android, iOS) - zraniteľnosti
- Kyber špionáž

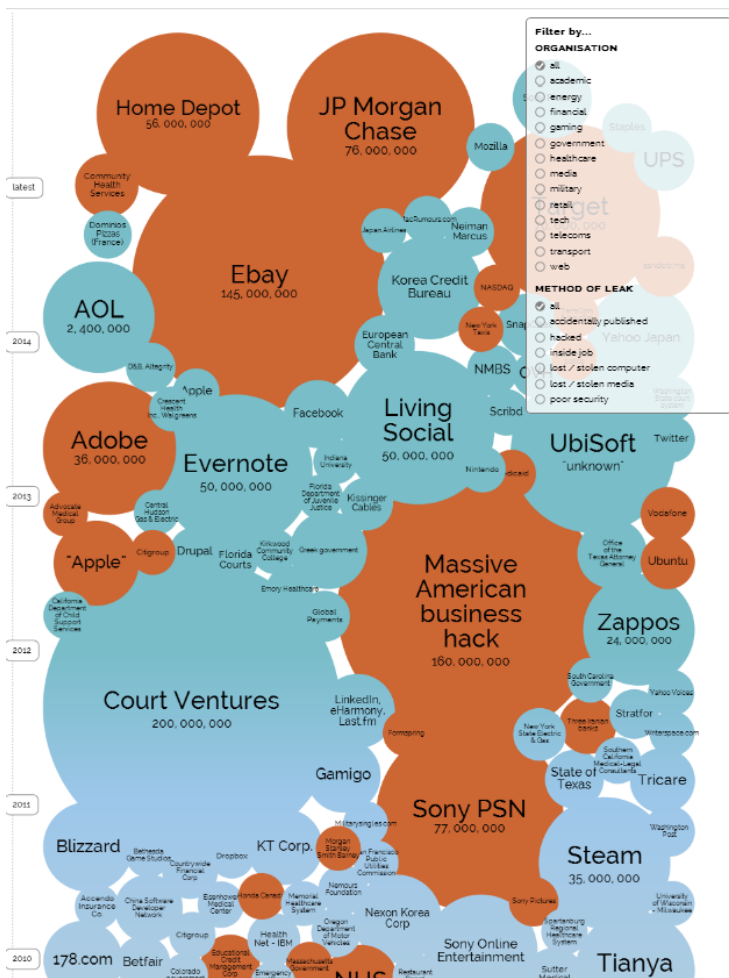
- **Výpadky kritickej informačnej infraštruktúry a služieb**

- DoS a DDoS
- kyber vojna

- **Attacks as a Service (AaaS)**

- Zjednodušenie útokov
- Využívanie grey marketu

Najväčšie svetové kybernetické útoky

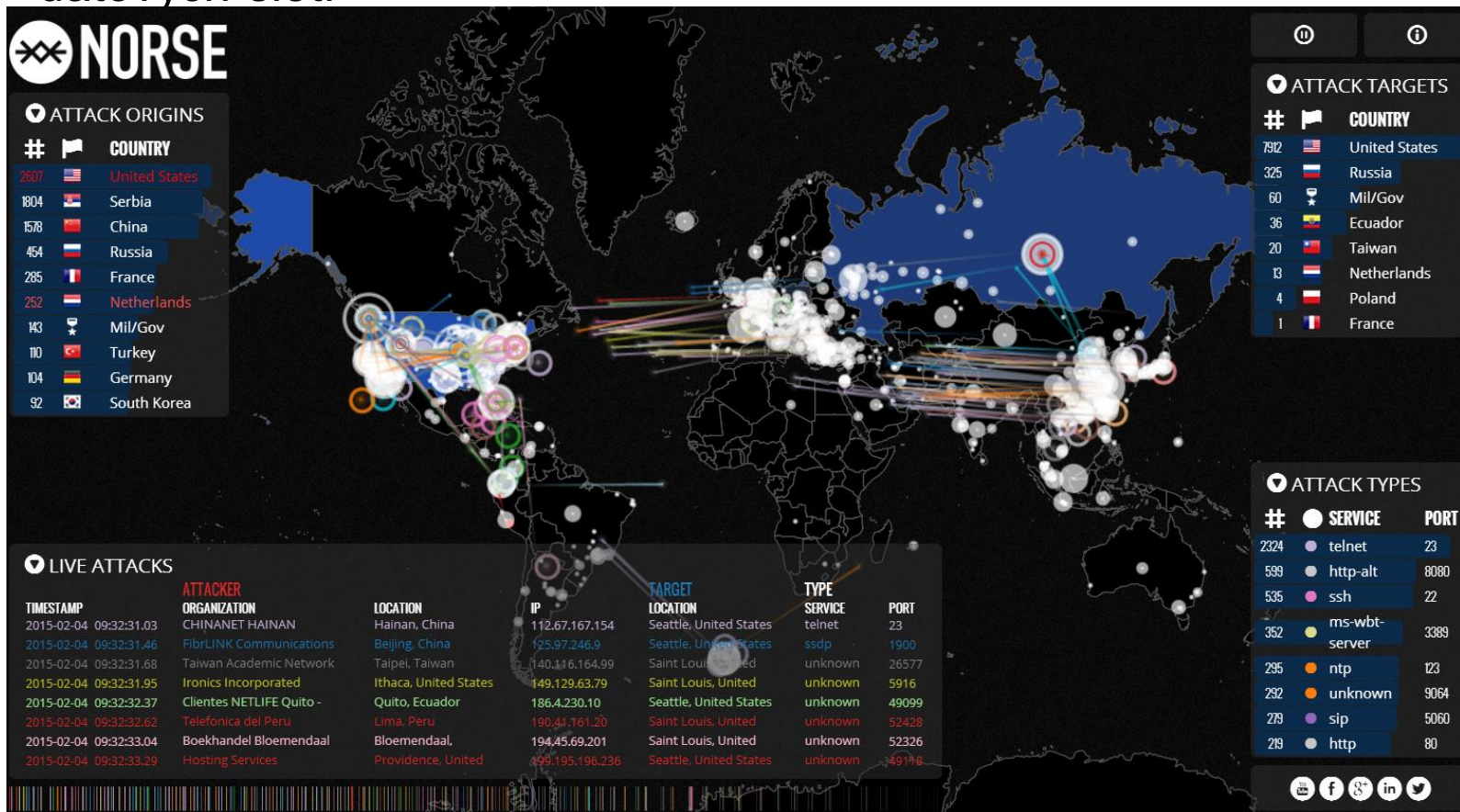


- Detailný pohľad na jednotlivé útoky
- Drill-Down mediálne zdroje informácií

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Kyber útoky po dátových sieťach

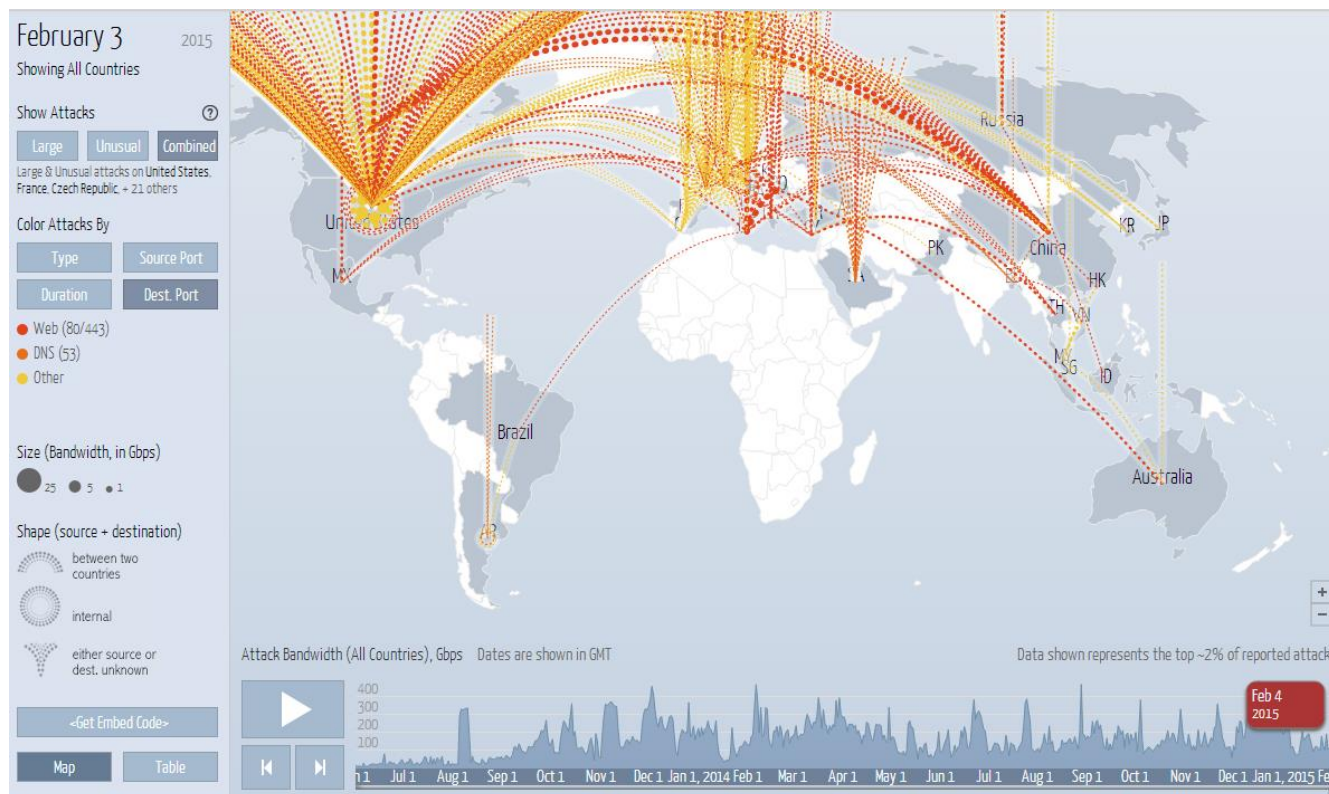
- Útoky realizované prostredníctvom dátových sietí
- Útoky je možné identifikovať pomocou kvalitného monitoringu dátových sietí



<http://map.ipviking.com/>

TOP DDoS útoky – živá mapa

- DDoS útoky podľa typu, zdroja, cieľa a doby
- Denná aktualizácia s možnosťou historického pohľadu
- Štúdia KASPERSKI – DDoS stojí Enterprise segment v priemere 440.000 \$ a SMB 52.000 \$



<http://www.digitalattackmap.com/#anim=1&color=1&country=ALL&list=2&time=16469&view=map>

Invea-Tech – nový pohľad na monitoring



Riešenie FlowMon

Flow
Monitoring

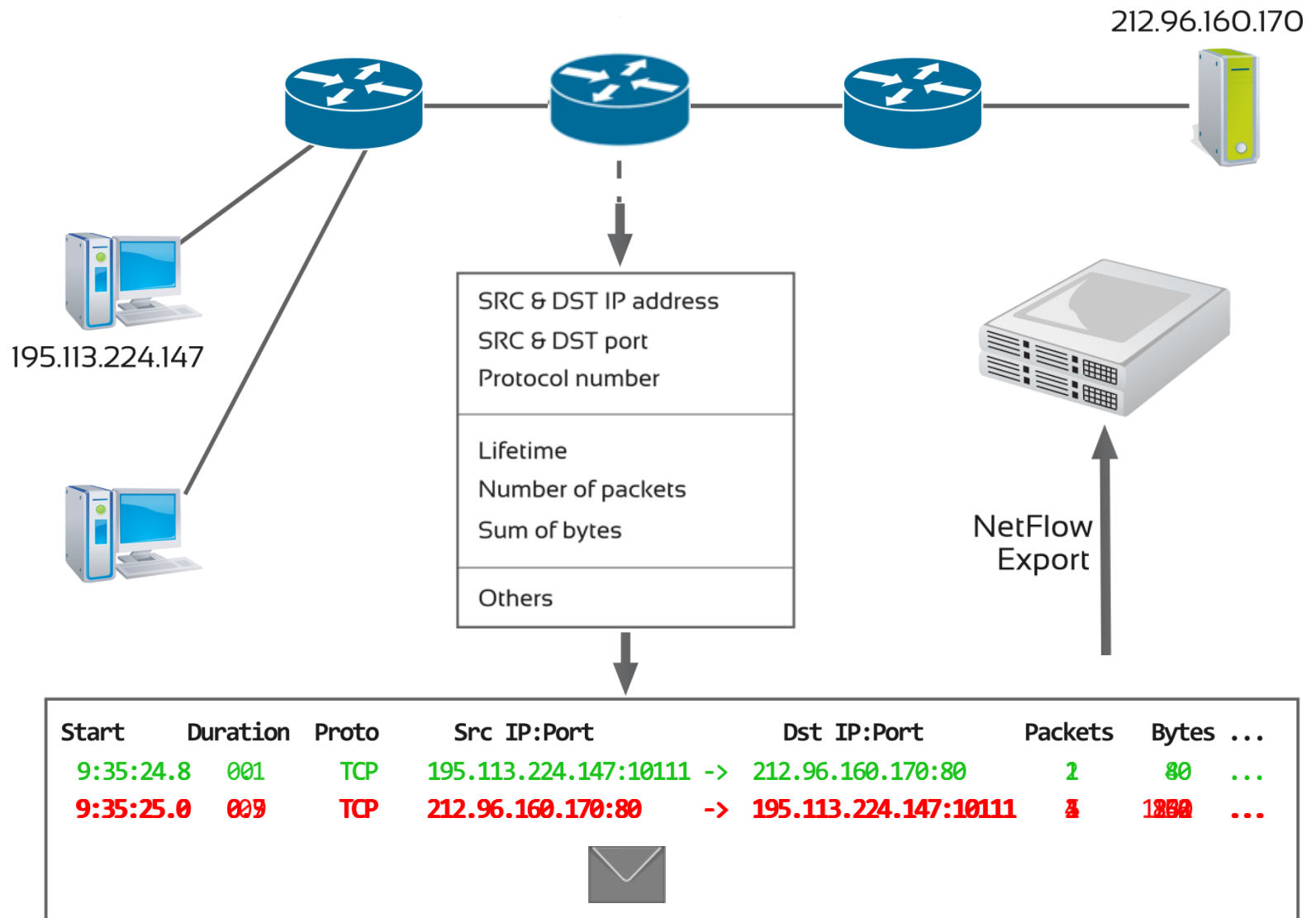
Network
Security
Monitoring

On Demand
Packet
Capture

Network/
Application
Performance

DDoS
Protection

NetFlow – princíp technologie



NetFlow využitie pre FlowMon

- **Monitorovanie prevádzky a výkonu** prostredníctvom moderných aktívnych prvkov a výkonných sond, ktoré garantujú spracovanie všetkých paketov a analýzu naprieč sieťovými vrstvami
- **Dlhodobé ukladanie štatistík** o prevádzke dátovej siete, ich vizualizácia a reporting. Sledovanie aktívnych zariadení na sieti.
- **Automatická detekcia** prevádzkových a bezpečnostných incidentov a anomálií v dátovej sieti založená na priebežnom vyhodnocovaní štatistík o prevádzke dátovej siete a následný automatizovaný alerting



Architektúra

FlowMon Sondy

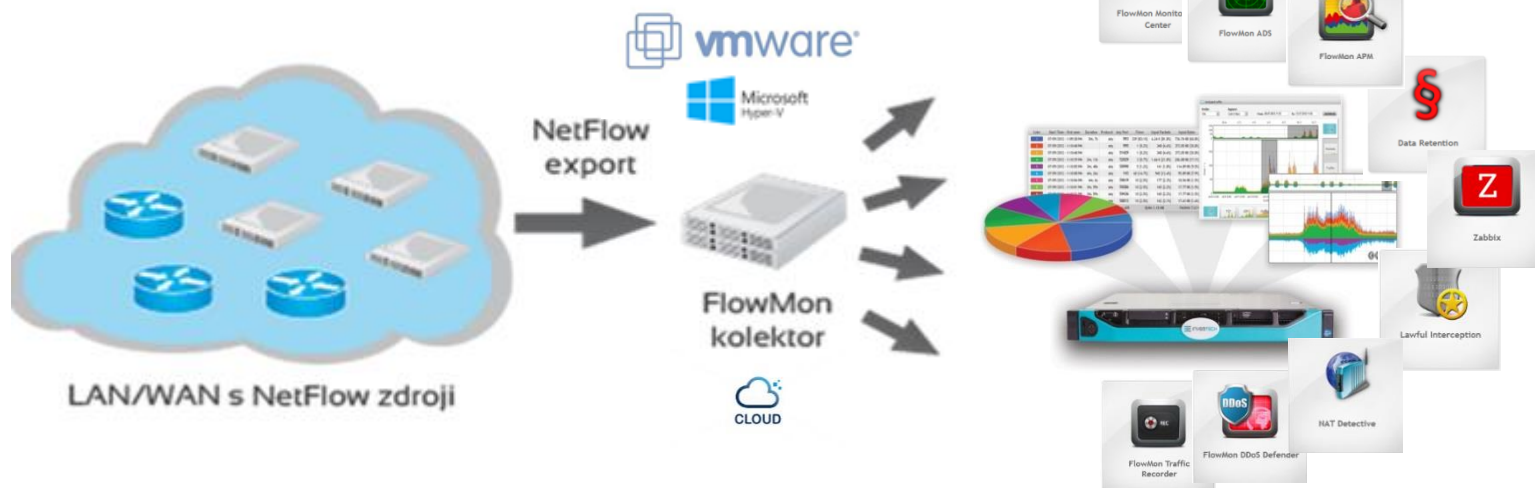
- Výkonné autonómne NetFlow sondy - zdroj záznamov o IP tokoch vo formáte NetFlow v5/v9/IPFIX
- Mobilné, L2/L3 neviditeľné zariadenia – transparentné pre monitorovanú sieť, použiteľná v ľubovoľnom bode siete
- Podpora 10/100/1000 Ethernetu, 10 GE, 40 GE, 100 GE, IPv4, IPv6, VLAN, MPLS

FlowMon Kolektor

- Zber a vizualizácia sieťových štatistík
- Dlhodobé uloženie, alerting a reporting

FlowMon Pluginy (SW vybavenie)

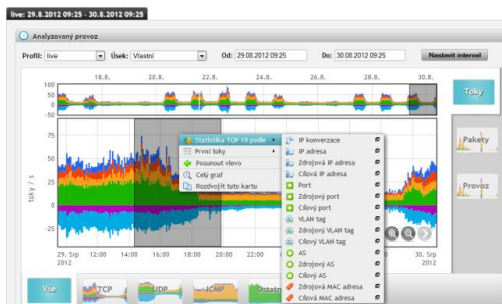
- Detekcia bezpečnostných a prevádzkových udalostí a anomálií
- Packet Capture, Monitoring výkonnosti aplikácií a ďalšie.



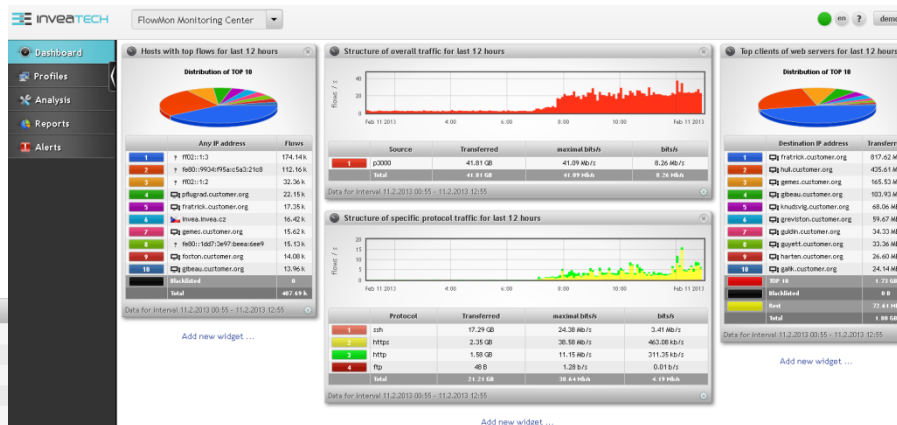
FMC (FlowMon Monitoring Center)

Monitorovacie centrum výkonu a prevádzky

- Vstavaná súčasť FlowMon sondy a kolektoru – základ
- Network Performance Monitoring, Monitoring VoIP prevádzky, Monitoring aktívnych zariadení, serverov používateľov, aplikácií, lokalít atď.
- Grafy a tabuľky a následné nástroje pre detailné analýzy
- Top N štatistiky (užívatelia, služby, navštevované servery, web stránky a pod.)
- Nástroj uľahčujúci optimalizáciu infraštruktúry, dohľad a správu sietí prostredníctvom alertov, dynamických tresholdov a ďalších nástrojov
- Detailný a flexibilný reporting



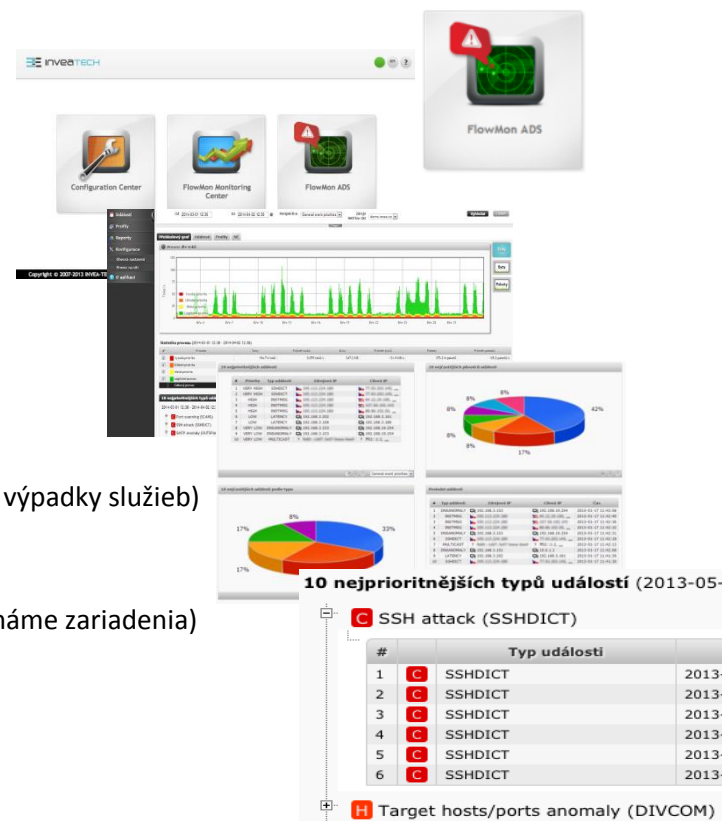
Počátečný čas	Protokol	Zdrojová IP adresa	Cíľový port	HTTP hostname
2013-05-29 08:58:47.009	TCP	192.168.3.179	80	api.play.cz
2013-05-29 08:58:52.668	TCP	192.168.3.179	80	www.gstatic.com
2013-05-29 08:58:52.164	TCP	192.168.3.179	80	0-act.channel.facebook.com
2013-05-29 08:58:46.955	TCP	192.168.3.179	80	clients2.google.com
2013-05-29 08:58:47.009	TCP	192.168.3.179	80	api.play.cz
2013-05-29 08:59:28.061	TCP	192.168.3.179	80	cr1.microsoft.com
2013-05-29 08:59:02.483	TCP	192.168.3.179	80	tools.google.com
2013-05-29 08:58:54.258	TCP	192.168.3.179	80	ocsp.startssl.com
2013-05-29 08:59:02.488	TCP	192.168.3.179	80	tools.google.com



ADS (Anomaly Detection System)

Network behaviorálna analýza

- Útoky (scan portov, slovníkové útoky, DoS, Telnet, APT, Zero Day)
- Anomálie prevádzky (DNS, multicast, vysoká variabilita komunikácie, VoIP)
- Anomálie chovania IP adries (zmena profilu chovania)
- Nežiaduca aplikácia (P2P siete, on-line komunikátory, TOR, TeamViewer)
- Malware (viry, spyware, botnety, komunikácie s adresami na blacklistech)
- Pošta (odchádzajúci SPAM, nelegitímne poštovné servery)
- Prevádzkové problémy (oneskorenie, preťaženie, reverzné DNS záznamy, výpadky služieb)
- Potenciálne úniky dát (upload na verejné servery, webové úložiská)
- Porušenie bezpečnostných politík (obchádzanie proxy serverov, neznáme zariadenia)
- Špecifické metódy (sledovanie senzorovej siete)

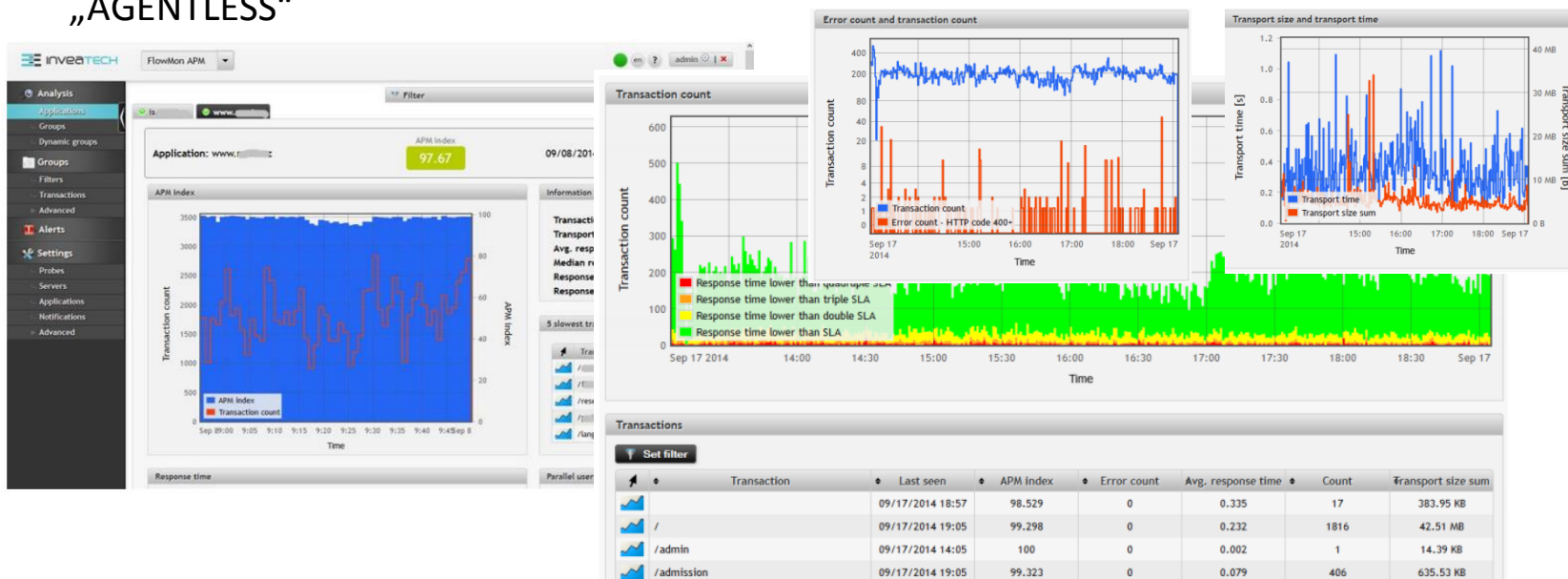


„To, že o tom neviete, neznamená, že to tam nie je“

APM (Application Performance Monitoring)

Monitoring výkonnostných parametrov aplikácií

- Detailný pohľad na výkon HTTP/HTTPS aplikácie
- „Správanie sa“ aplikácií jednotlivým užívateľom
- Identifikácia problémov skôr, než ju ohlási používateľ
- Identifikácia príčin výkonnostných problémov
- Meranie reálnej doby odozvy a chovania sa aplikácie
- Poskytovanie „tvrdých dát“ pre upg. HW
- Monitoring užívateľských transakcií v reálnom čase bez nutnosti inštalácie SW, tzv. „AGENTLESS“



Traffic Recorder

Nahrávanie záznamu dátovej komunikácie

- „Full / OnDemand Packet Capture“ – nahrávanie dátovej komunikácie L2-L7
- Ukladanie do PCAP formátu
- Vhodné pre ďalšie forénzne a iné hlbšie analýzy napr. v nástrojoch Wireshark
- Rozšírenie možností identifikácie prevádzkových problémov



HTTP requests files				
Probe	Interface	File	Created	Tools
192.168.3.174	eth3	20140526152619-20140526152630-192.168.3.174-eth3.pcap	2014/05/26 15:26	Download Remove
192.168.3.174	eth3	20140526152610-20140526152619-192.168.3.174-eth3.pcap	2014/05/26 15:26	Download Remove
192.168.3.174	eth3	20140526152601-20140526152610-192.168.3.174-eth3.pcap	2014/05/26 15:26	Download Remove
192.168.3.174	eth3	20140526152555-20140526152601-192.168.3.174-eth3.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth2	20140526152555-20140526152558-192.168.3.174-eth2.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth2	20140526152551-20140526152555-192.168.3.174-eth2.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth2	20140526152542-20140526152551-192.168.3.174-eth2.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth3	20140526152541-20140526152555-192.168.3.174-eth3.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth2	20140526152538-20140526152542-192.168.3.174-eth2.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth3	20140526152528-20140526152541-192.168.3.174-eth3.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth2	20140526152527-20140526152538-192.168.3.174-eth2.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth3	20140526152519-20140526152528-192.168.3.174-eth3.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth2	20140526152517-20140526152527-192.168.3.174-eth2.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth3	20140526152517-20140526152519-192.168.3.174-eth3.pcap	2014/05/26 15:25	Download Remove
192.168.3.174	eth2	20140526152517-20140526152519-192.168.3.174-eth2.pcap	2014/05/26 15:25	Download Remove

InveaTECH

FlowMon Traffic Recorder

en ? admin | ✕

Tasks

Name	Description	State	Tools
HTTP requests		✓ RUNNING (2)	Start Stop Show Files Edit Delete

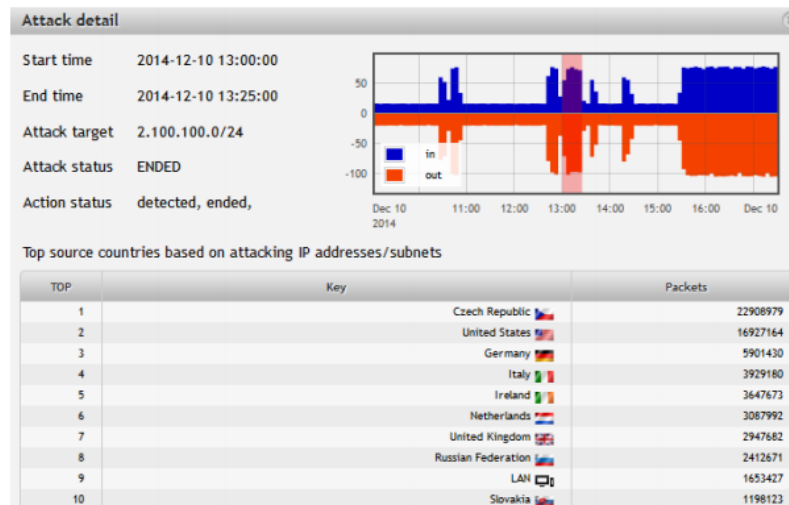
+ Create new task...

[Edit Probes](#)

DDoS Defender

Detekcia a mitigácia útokov typu DoS a DDoS real-time

- Zrýchlenie reakčnej doby na útok
- Získanie charakteristických znakov útokov a prezentácia používateľovi
- Notifikácie a alerting – email, syslog, SNMP trap
- Pokročilé funkcie okamžitej reakcie a mitigácie
- Podpora smerovacích protokolov BGP, PBR, RTBH
- Nezávislá konfigurácia ochraňuje rôznych zákazníkov, služby alebo segmenty siete
- Postačuje základná kvalita flow dát z aktívnych prvkov (NetFlow, IPFIX, jFlow, sFlow, NetStream), samplované i nesamplované štatistiky
- Integrácia s 3. stranami tzv. DDoS Protection riešení (cez RESTFul API)



DDoS Protection

FlowMon DDoS Defender



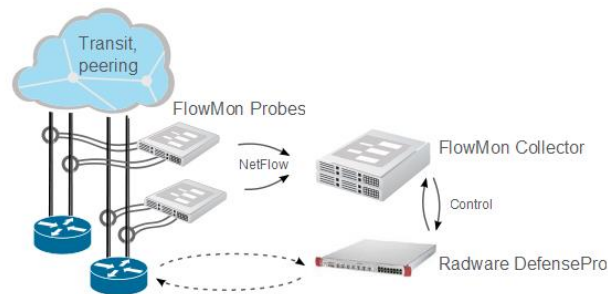
Standalone

- Samostatne jako súčasť FlowMon kolektora
- Schopnosť analyzovať akékoľvek Flow

Out-of-band eliminace DDoS útoku

(PBR, BGP)

- S využitím aktívnych prvkov a ich protokolov
- Súčasť out-of-band riešenia: Radware Defence Pro

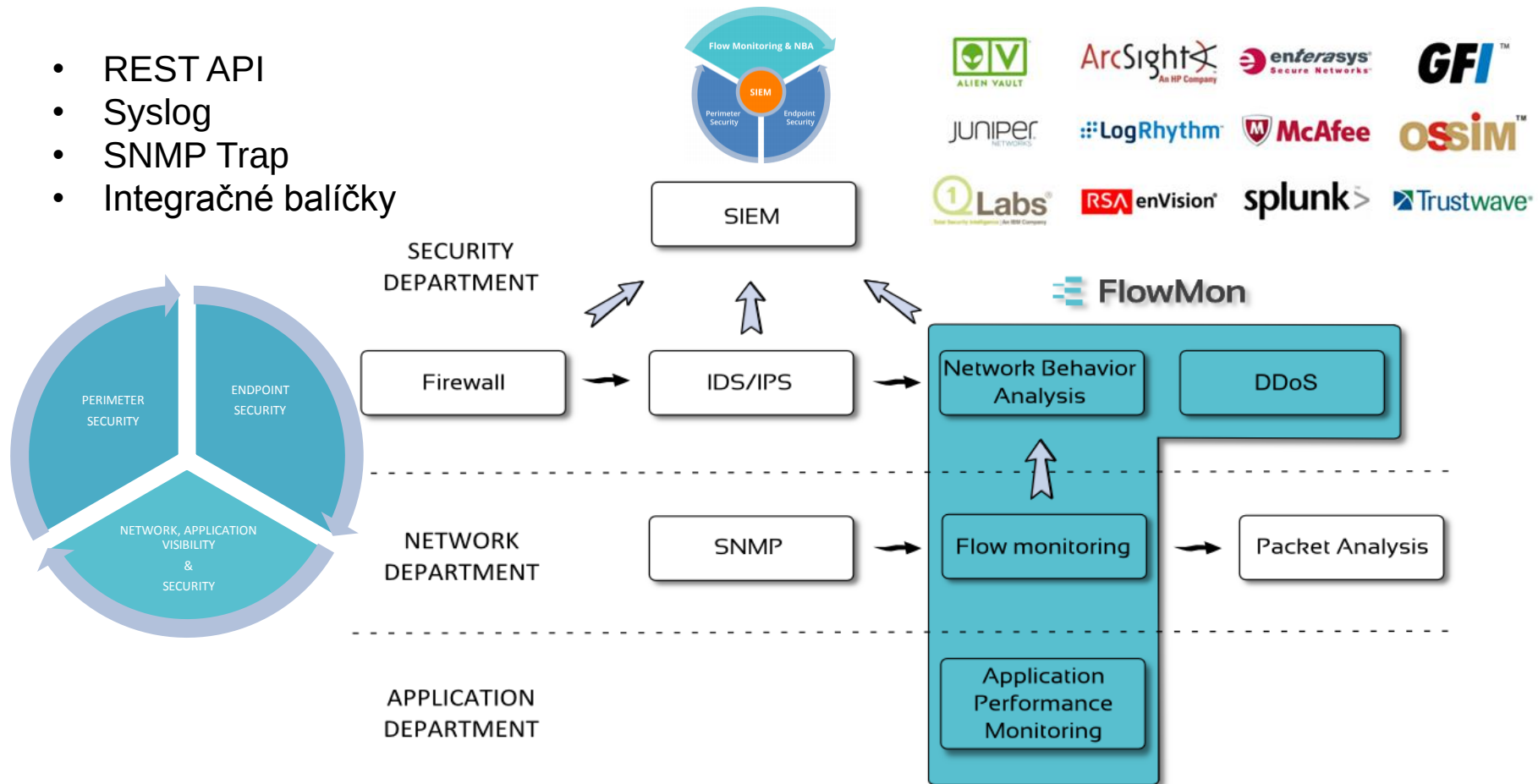


Scrubbing Center

- S využitím súčasného scrubbing centra

Komplexné pokrytie monitoringu dátových sietí, aplikácií a bezpečnosti

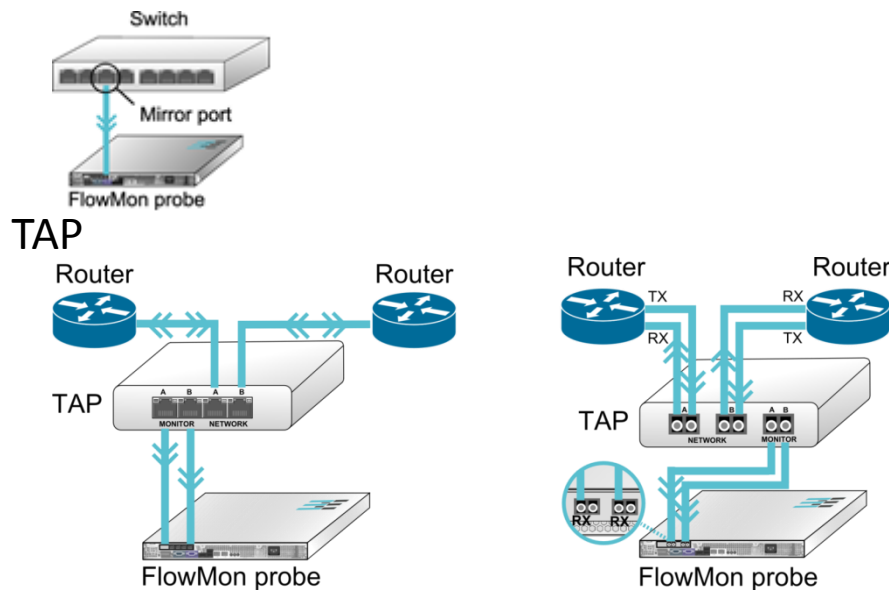
- REST API
- Syslog
- SNMP Trap
- Integrované balíčky



FlowMon – nasadenie riešenia

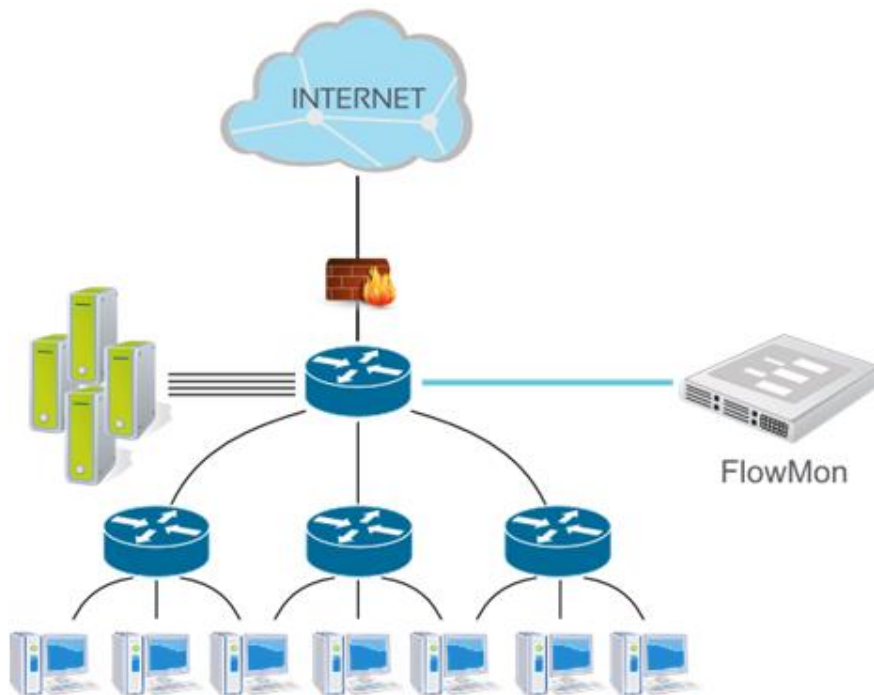
- Riešenie je pasívne a neinvazívne, nezasahuje do funkčnosti siete.
- Riešenie je možné nasadiť centralizovane alebo decentralizovane, poprípade kombináciou obidvoch možností, pričom sa zapojenie uskutočňuje pomocou:

Mirror port / SPAN port

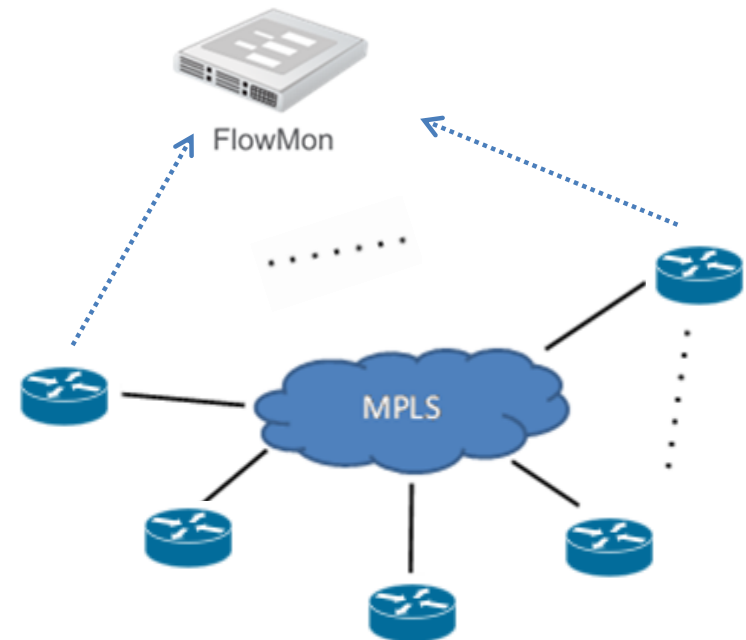


FlowMon – nasadenie riešenia

Centralizované nasadenie



Decentralizované nasadenie



Prínosy

„VIDITEĽNOSŤ“

- detailné a presné real-time, či historické informácie o dianí v dátovej sieti
- uchovávanie všetkých potrebných informácií pre ďalšie analýzy



„ÚSPORY“

- okamžitá identifikácia výkonnostnej, prevádzkovej a bezpečnostnej hrozby
- automatizovaná alebo manuálna real-time / spätná analýza problému



„KOMPLEXNOSŤ“

- troubleshooting, správa sietí, aplikácií, serverovej, či virtuálnej infraštruktúry
- custom reporting
- cross – departments využívanie informácií : support dep. -> TOP management



„INTEGRÁCIA“

- využitie inštalovanej bázy, súčasných investícií a zabehnutých procesov
- škálovateľnosť , solution development a otvorenosť platformy



„COMPLIANCE“

- aplikovateľnosť na legislatívne, audítorské a compliance požiadavky





High-Speed Networking Technology Partner

Roman Čupka

roman.cupka@invea.com

roman.cupka@dvsro.eu

+421 948 464 123

INVEA-TECH a.s.

U Vodárny 2965/2

616 00 Brno

Czech Republic

www.invea.com



Ďakujeme za pozornost

