Approaches to Network Visibility

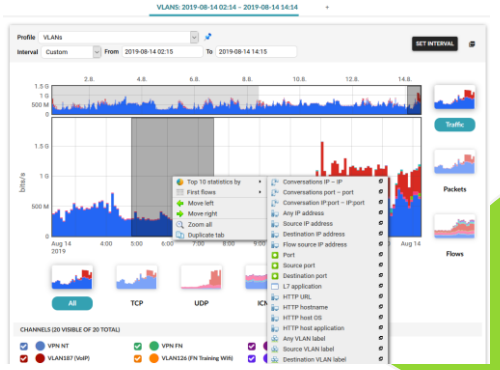
Challenges of visibility in network environment

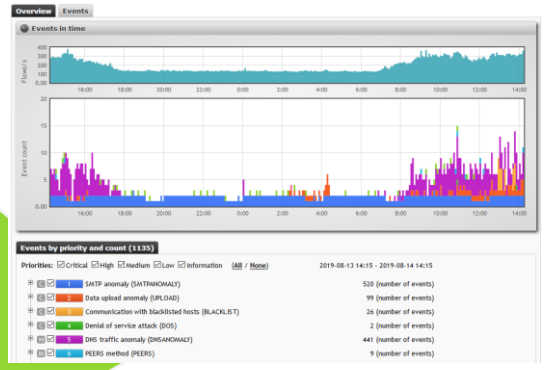
Jiri Knapek, Presales Team Leader

RONOG 6, October 1st, 2019

Flowmon
Driving Network Visibility

Technology Approaches

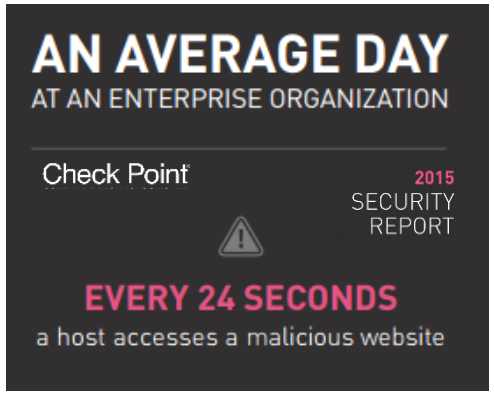




Network Visibility & Security

Perimeter Security

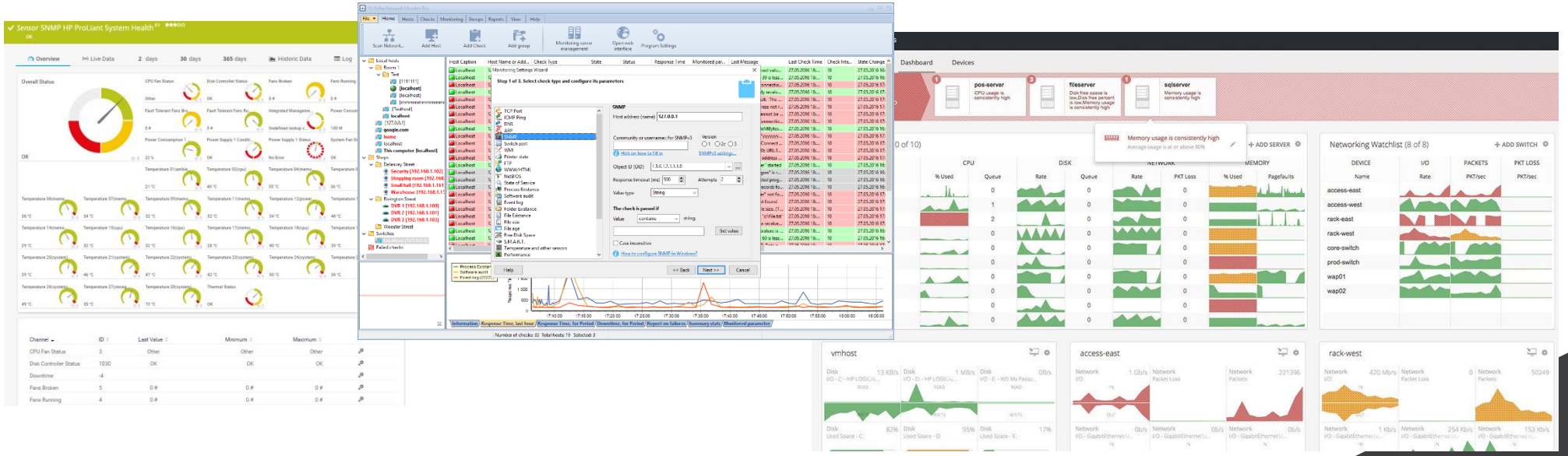
Endpoint Security



Flowmon
Driving Network Visibility

SNMP (Simple Network Management Protocol)

- Allows basic monitoring of equipment generally used to see utilization of different resources.
- You can use also for proactive monitoring utilizing traps
- Helps you quickly to understand that there is a problem
- We can refer to it as infrastructure monitoring



Flowmon
Driving Network Visibility

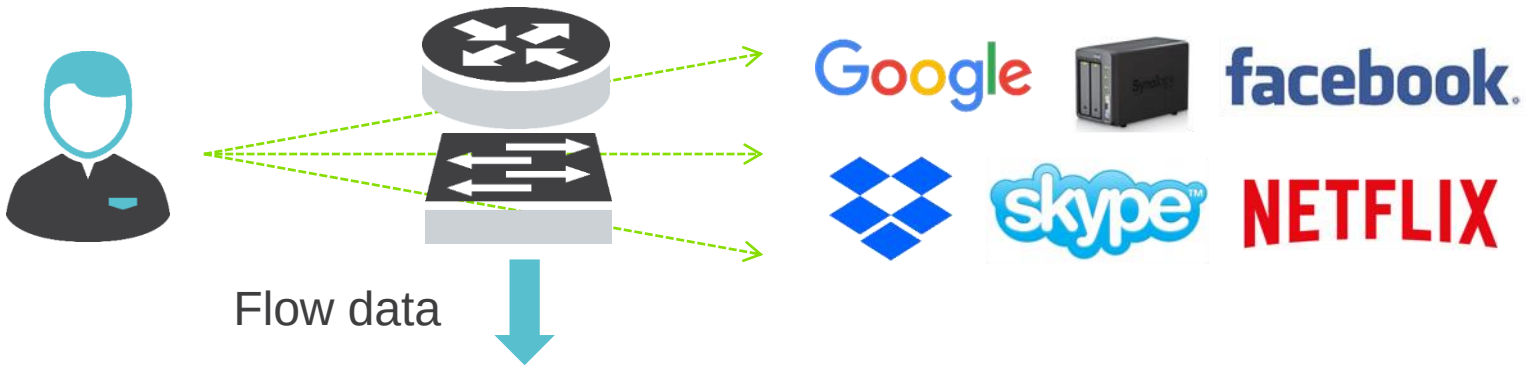
What is Flow Data?

Modern method for network monitoring – flow measurement

Cisco standard NetFlow v5/v9, IETF standard IPFIX

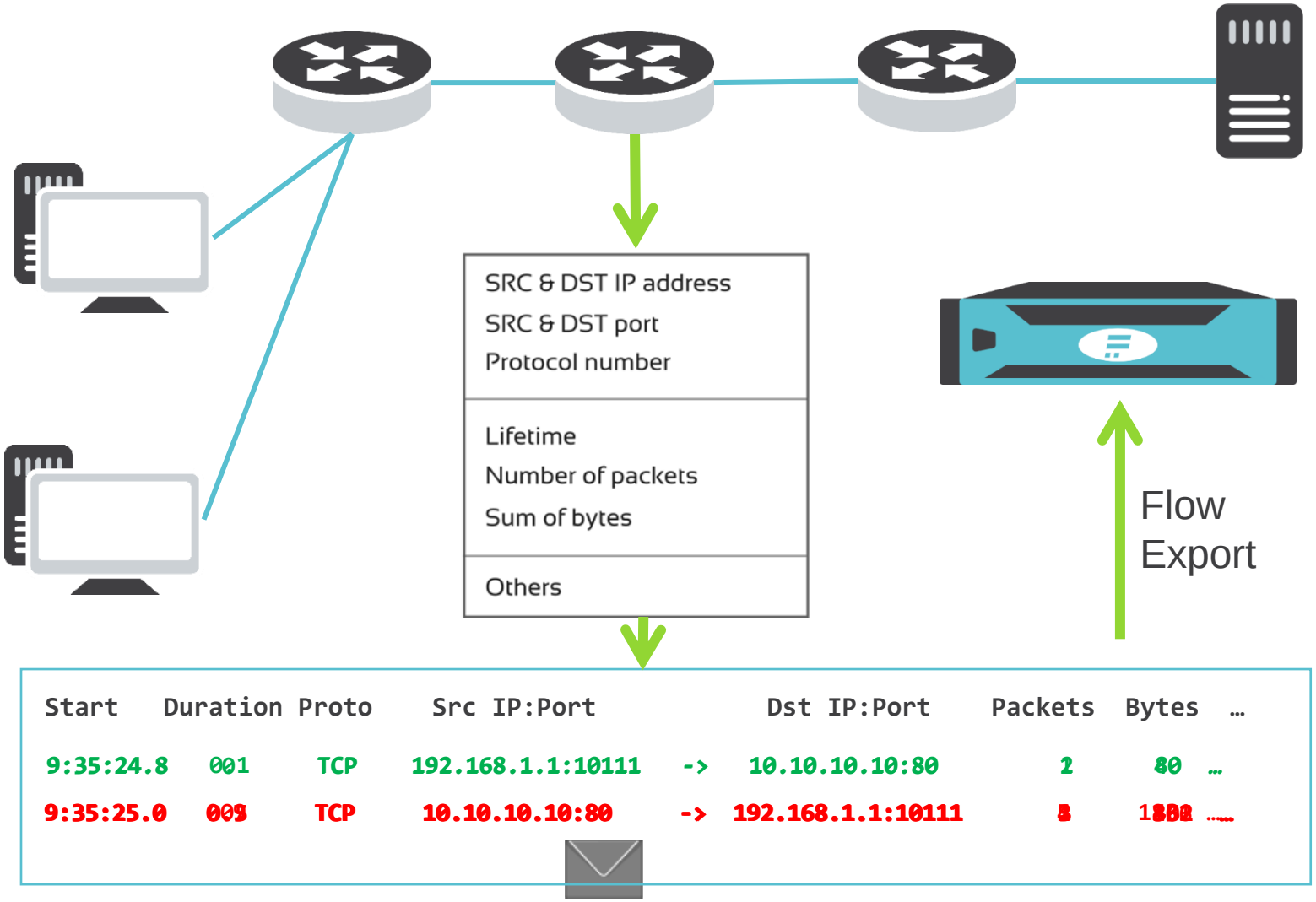
Focused on L3/L4 information and volumetric parameters

Real network traffic to flow statistics reduction ratio 500:1



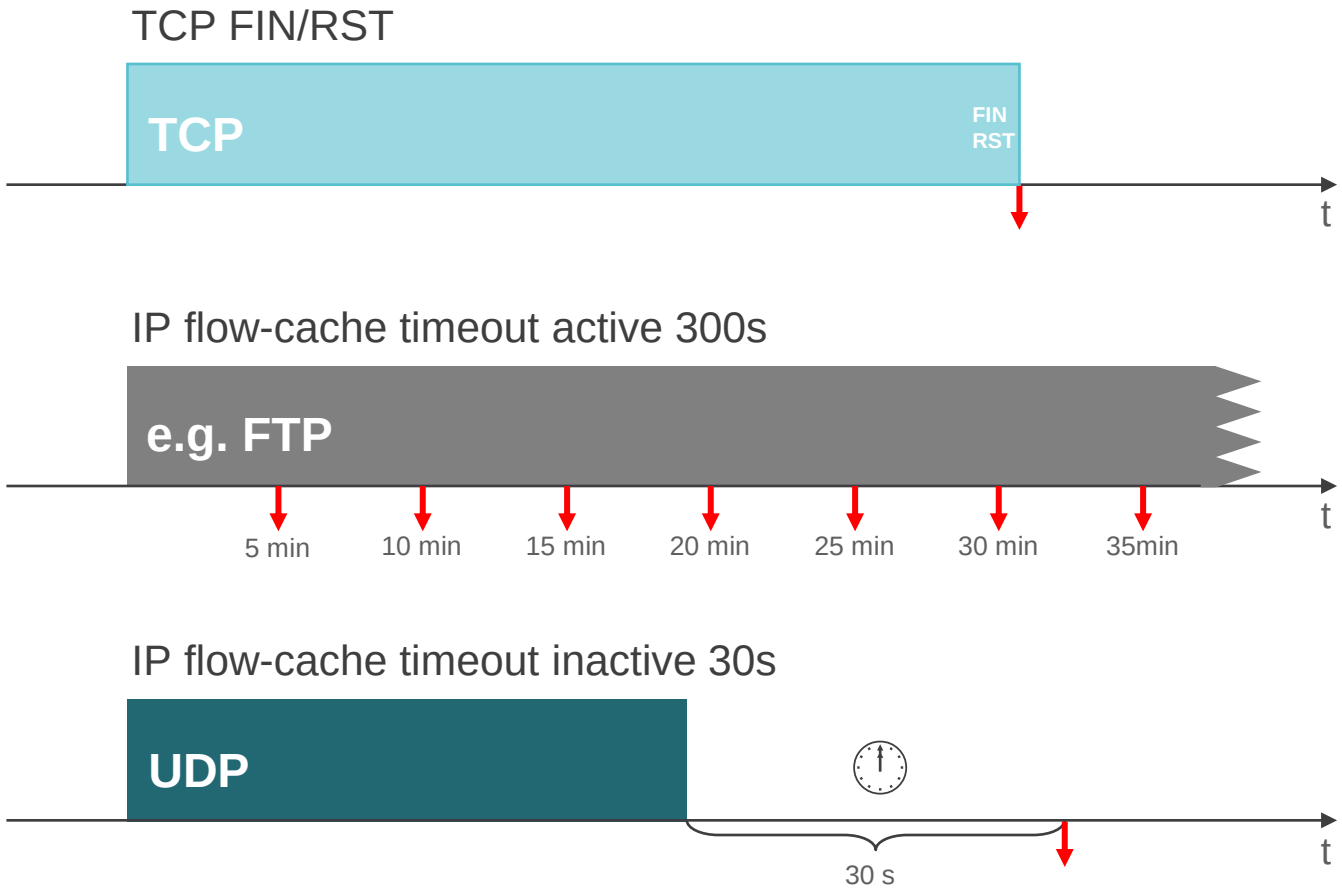
Flowmon
Driving Network Visibility

Flow Monitoring Principle



Flowmon
Driving Network Visibility

Flow Export Principle



Flowmon
Driving Network Visibility

Standard	Vendor	Details
NetFlow v5	Cisco	Original standard for flow monitoring supported by many routers and switches. Fixed format and set of attributes focusing on L3/L4 network information. Considered as obsolete now due to many limitations like missing IPv6 traffic information or no extensibility. Supported by many monitoring tools and applications.
NetFlow v9	Cisco	Extended flow monitoring standard dealing with limitations of version 5. Provides IPv6 traffic monitoring, information from L2 like MAC addresses or VLAN tags. Details are covered in RFC 3954.
Flexible NetFlow	Cisco	Similar standard to NetFlow version 9 with more flexibility on flow export configuration and customization on key fields and what information is being exported. Flexible NetFlow extends monitoring to L7 by technology NBAR2 (Network Based Application Recognition).

Flow Standards – Cisco

Standard	Vendor	Details
jFlow	Juniper	Juniper standard for flow monitoring available in both version v5 and v9. The main difference compared to NetFlow is that timestamps of exported flow data are preserved for whole network session which needs handling on colector side. In general this standard is compatible with NetFlow.
NetStream	Huawei	Huawei standard for flow monitoring available in both version 5 and 9. This standard is compatible with NetFlow.
cflowd	Alcatel-Lucent	Alcatel-Lucent standard for flow monitoring available in both version 5 and 9. This standard is compatible with NetFlow however usually available only as sampled flow data.

Flow Standards – Other Vendors

Standard	Vendor	Details
IPFIX	Independent	Independent international standard that enables vendors of flow based monitoring tools like Flowmon to define own protocol extensions to export literary any information from L2 to L7. Flowmon is a pioneer of this technology providing visibility into many application protocols since 2012 with continuous grow of supported protocol scope. This is crucial technology that enables to deliver unique network visibility without the need of continuous packet capture, integrate NetOps & SecOps into single platform and scale in multi 100G environment. Specifications for IPFIX are covered by RFC 7011 through RFC 7015, and RFC 5103. In Cisco environment IPFIX is usually referred to as NetFlow v10.

Flow Standards – Independent

Standard	Vendor	Details
NEL/NSEL over NetFlow	Cisco	NEL stands for Network Event Logging which refers to logs from network address translation. NSEL stands for Network Security Event Logging which refers to firewall logs produced by Cisco ASA. NetFlow is just transport protocol. This data cannot be considered as flow, information provided does not enable to reconstruct a real network traffic chart.
sFlow	Independent	sFlow is an industry standard technology for monitoring high speed switched networks. Sampled packet headers are encoded to NetFlow like format and exported to collector. Due to heavy sampling rates (usually 1:1000) this data is not accurate enough to handle troubleshooting uses case or network based anomaly detection.
NetFlow Lite	Cisco	NetFlow Lite is Cisco version of sFlow with all pros and cons related to this technology.

Flow Standards – Related

Flow vs. Packet Analysis on 10G Backbone

	Strong aspects	Weak aspects
Packet Analysis	+ Full network traffic + Enough details for troubleshooting + Supports forensic analysis + Signature based detection	- Useless for encrypted traffic - Usually too much details - Very resource consuming

Storage required	1 min	1 hour	1 day
	75 GB	4.5 TB	108 TB

	Strong aspects	Weak aspects
Flow Data	+ Works in high-speed networks + Resistant to encrypted traffic + Visibility and reporting + Network behavior analysis	- No application layer data - Sometimes not enough details - Sampling (routers, switches)

Storage required	1 min	1 hour	1 day
	150 MB	9 GB	216 GB

Flowmon
Driving Network Visibility

Myth:

Flow data do not provide sufficient level of detail when it comes to network troubleshooting or forensics. Full packet traces are absolute must to investigate on network issues and fight cyber crime.

Reality:

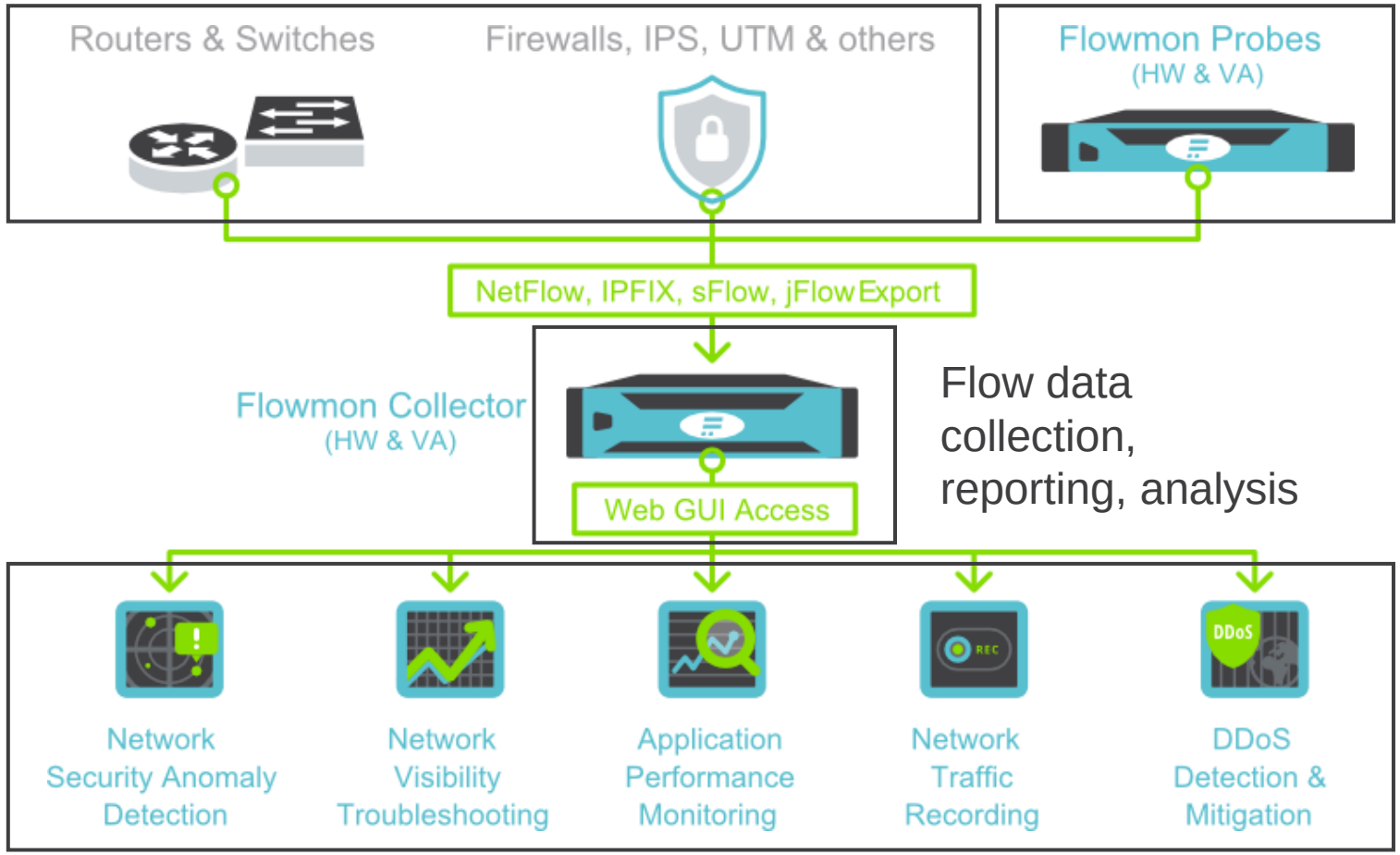
Continuous full packet capture tools cannot scale with bandwidth explosion in corporate networks and companies are switching to flow technologies.

Gartner notes that 80% of network troubleshooting can be solved with NetFlow.

Flowmon combines best of breed: flow data enriched with L7 and performance metrics. This helps to solve 95% of all troubleshooting cases. In addition, Flowmon provides on-demand packet capture when flow visibility is not enough.

Flowmon Architecture

Flow export from already deployed devices



Flow data export + L7 monitoring

Flow data collection, reporting, analysis

Flowmon modules for advanced flow data analysis

Flowmon
Driving Network Visibility

Flowmon Architecture and Components

Flowmon Probes

- Passive source of NetFlow/IPFIX data

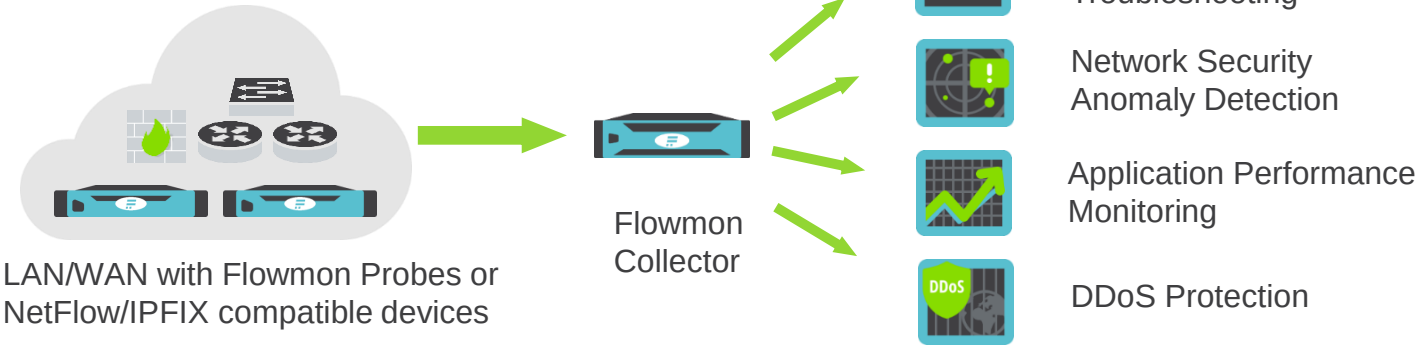
Flowmon Collectors

- Flow collection, reporting, analysis

vmware® Microsoft Hyper-V KVM

amazon web services Microsoft Azure

Flowmon modules



Flowmon
Driving Network Visibility

Flowmon Probe

The most powerful NetFlow / IPFIX Exporter for Network Monitoring

Flowmon
Driving Network Visibility

Challenges

Network troubleshooting using packet capture is very resource consuming

Only feasible alternative is to **use flow data** with information about network communications

Flow data exported from **active device may not be available, accurate or detailed enough**

Use **dedicated high-performance and accurate** flow data exporters

Flowmon Probe - dedicated flow data exporter providing **visibility** into the **application protocols**

Gartner

Gartner last year stated that flow analysis should be done 80% of the time and that packet capture with probes should be done 20% of the time.

Monitoring Recommendations

- Implement the use of advanced flow-based data sources to allow better measurement of the user experience.
- Implement flow-based monitoring technologies extensively, and leverage probes where detail is needed. Using a single platform for both makes management easier.

Flowmon
Driving Network Visibility

Flowmon Probe

High-performance standalone probe – source of unsampled flow records in NetFlow v5, v9 and IPFIX

L2/L3 invisible – transparent for monitored network

Rack mountable hardware and virtual appliances

Remote configuration via a user-friendly web GUI

Maintenance-free appliance with simple configuration

Flowmon
Driving Network Visibility

Flowmon Probe Visibility Options

Versatile and flexible network appliances

- Monitoring ports convert packets to flows
- Un-sampled export in NetFlow v5/v9 or IPFIX
- Wire-speed, L2-L7 visibility, tunnel decapsulation, PCAPs when needed

L2	L3/L4	L7	
• MAC • VLAN • MPLS • GRE tunnel • OTV • ESP	• Standard items • NPM metrics • RTT, SRT, … • TTL, SYN size, … • ASN (BGP) • Geolocation • VxLAN	• NBAR2 • HTTP • SNI • DNS • DHCP • IEC104	• SMB/CIFS • VoIP (SIP) • Email • SQL • SSL/TLS • CoAP

Flowmon
Driving Network Visibility

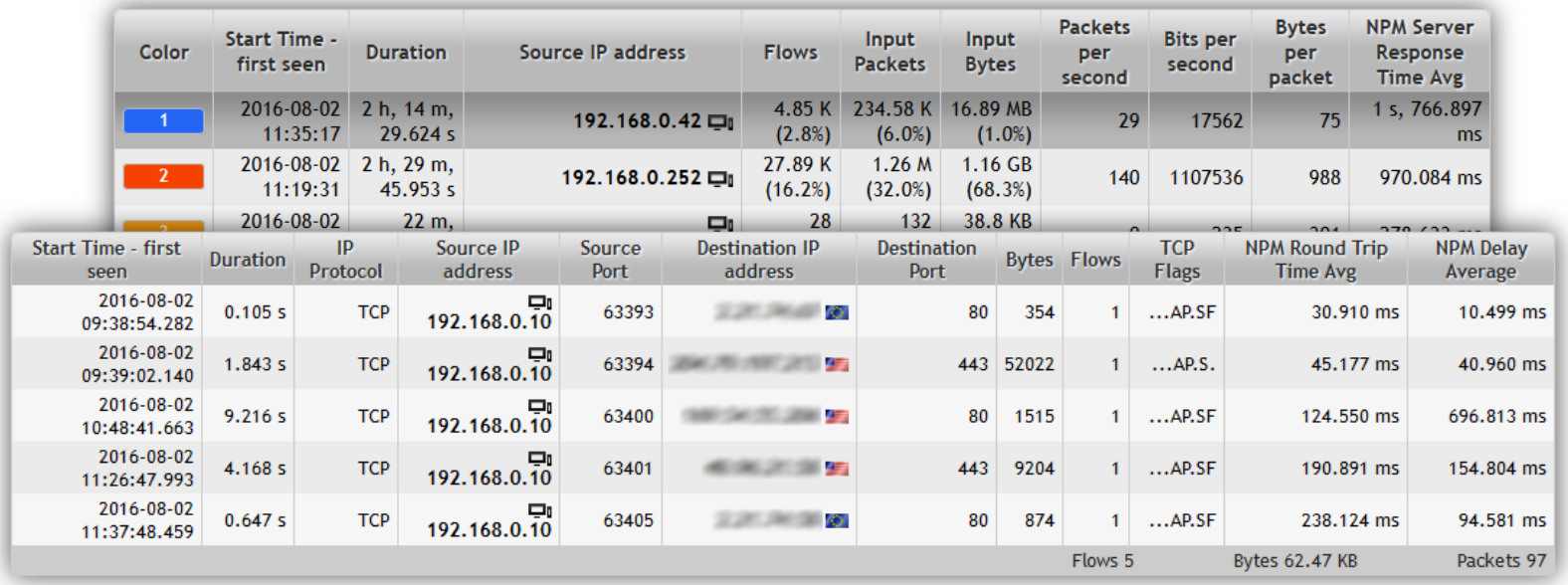
Network Performance Monitoring

Provides insight to performance of your network

SRT (Server Response Time) – server delay

RTT (Round Trip Time) – network delay

Delay, Jitter, TCP Retransmissions

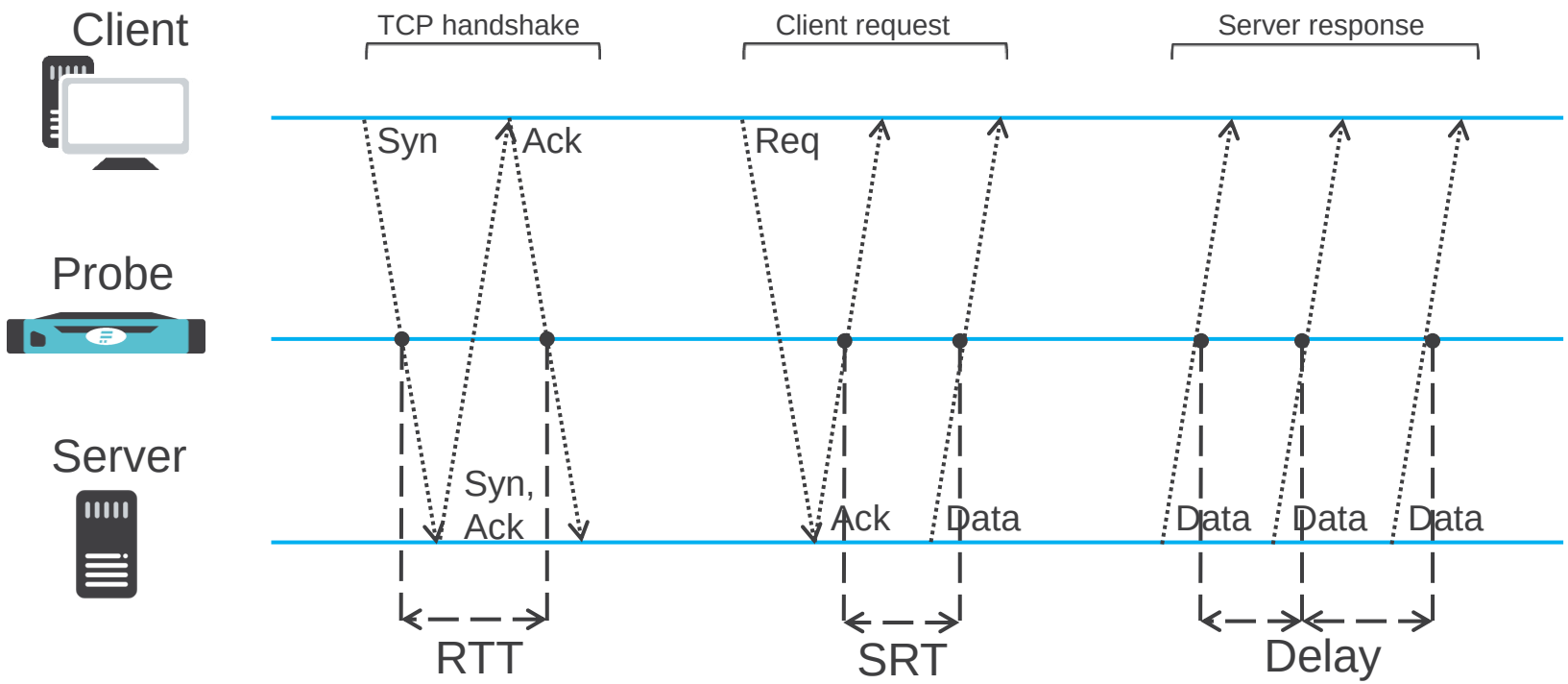


Color	Start Time - first seen	Duration	Source IP address	Flows	Input Packets	Input Bytes	Packets per second	Bits per second	Bytes per packet	NPM Server Response Time Avg
1	2016-08-02 11:35:17	2 h, 14 m, 29.624 s	192.168.0.42	4.85 K (2.8%)	234.58 K (6.0%)	16.89 MB (1.0%)	29	17562	75	1 s, 766.897 ms
2	2016-08-02 11:19:31	2 h, 29 m, 45.953 s	192.168.0.252	27.89 K (16.2%)	1.26 M (32.0%)	1.16 GB (68.3%)	140	1107536	988	970.084 ms
3	2016-08-02	22 m,		28	132	38.8 KB				

Start Time - first seen	Duration	IP Protocol	Source IP address	Source Port	Destination IP address	Destination Port	Bytes	Flows	TCP Flags	NPM Round Trip Time Avg	NPM Delay Average
2016-08-02 09:38:54.282	0.105 s	TCP	192.168.0.10	63393	[redacted]	80	354	1	...AP.SF	30.910 ms	10.499 ms
2016-08-02 09:39:02.140	1.843 s	TCP	192.168.0.10	63394	[redacted]	443	52022	1	...AP.S.	45.177 ms	40.960 ms
2016-08-02 10:48:41.663	9.216 s	TCP	192.168.0.10	63400	[redacted]	80	1515	1	...AP.SF	124.550 ms	696.813 ms
2016-08-02 11:26:47.993	4.168 s	TCP	192.168.0.10	63401	[redacted]	443	9204	1	...AP.SF	190.891 ms	154.804 ms
2016-08-02 11:37:48.459	0.647 s	TCP	192.168.0.10	63405	[redacted]	80	874	1	...AP.SF	238.124 ms	94.581 ms
								Flows 5		Bytes 62.47 KB	Packets 97

Flowmon
Driving Network Visibility

NPM Principles



Round Trip Time – **delay introduced by network**

Server Response Time – **delay introduced by server/application**

Delay (min, max, avg, deviation) – **delays between packets**

Jitter (min, max, avg, deviation) – **variance of delays between packets**

Flowmon
Driving Network Visibility

Other Export Capabilities

Network Based Application Recognition (NBAR2)

- Flowmon Probe analyse packet on L7 and export information about used application

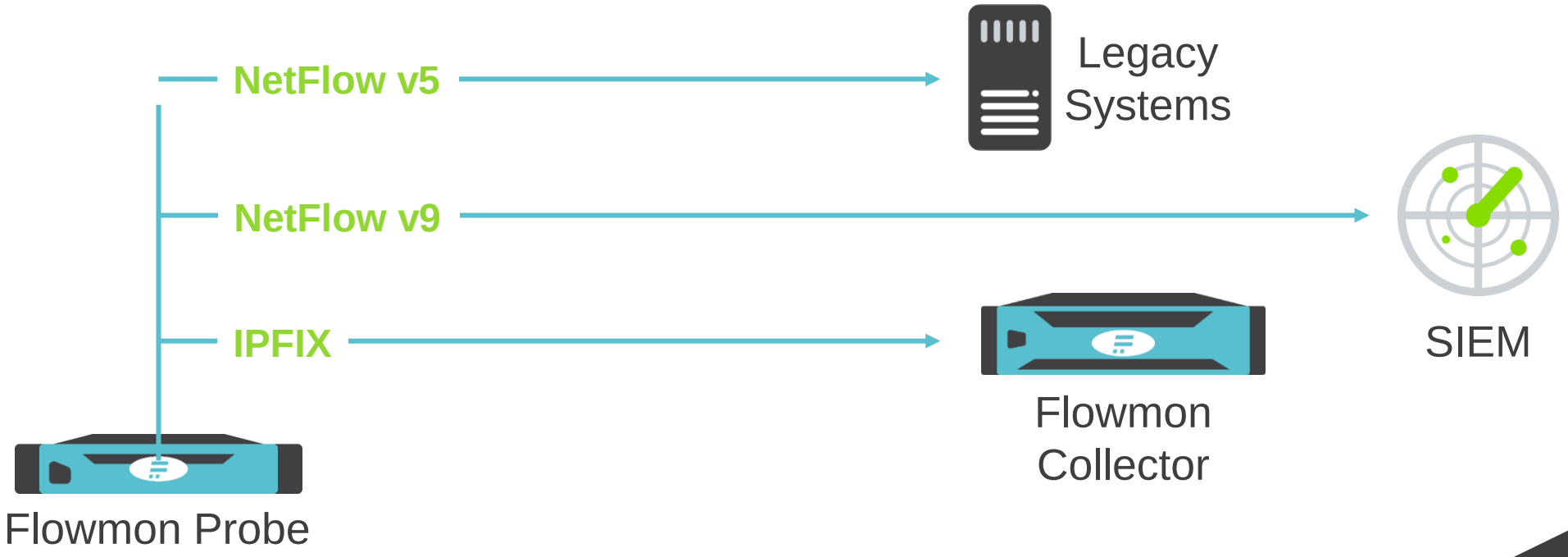
Color	Start Time - first seen	Duration	NBAR2 App Tag	Flows	Input Packets	Input Bytes	Packets per second	Bits per second	Bytes per packet
1	2016-07-01 05:40:46	3 h, 46 m, 30.935 s	ipsec	81 (0.1%)	238.98 K (27.7%)	148.99 MB (41.7%)	17	91961	653
2	2016-07-01 05:44:48	4 h, 4 m, 12.655 s	pop3	312 (0.3%)	102.21 K (11.8%)	92.83 MB (26.0%)	6	53143	952
3	2016-07-01 05:44:18	4 h, 4 m, 54.969 s	http	4.51 K (4.4%)	53.22 K (6.2%)	29.87 MB (8.4%)	3	17051	588
4	2016-07-01 05:41:46	4 h, 7 m, 37.390 s	syslog	1.58 K (1.5%)	68.71 K (8.0%)	17.76 MB (5.0%)	4	10026	271
5	2016-07-01 06:16:16	3 h, 32 m, 56.326 s	secure-http	915 (0.9%)	24.55 K (2.8%)	15.55 MB (4.4%)	1	10206	664
6	2016-07-01 05:44:27	4 h, 4 m, 56 s	snmp	39.4 K (38.0%)	114.78 K (13.3%)	13.6 MB (3.8%)	7	7761	124
7	2016-07-01 05:58:28	3 h, 50 m, 46.857 s	cifs	1.09 K (1.0%)	61.54 K (7.1%)	9.65 MB (2.7%)	4	5847	164
8	2016-07-01 05:44:44	4 h, 4 m, 19.754 s	icmp	2.93 K (2.8%)	83.42 K (9.7%)	8.41 MB (2.4%)	5	4810	105
9	2016-07-01 05:44:45	4 h, 4 m, 42.041 s	dns	44.71 K (43.1%)	46.33 K (5.4%)	7.73 MB (2.2%)	3	4415	174
10	2016-07-01 05:44:17	4 h, 4 m, 44.207 s	sip	1.76 K (1.7%)	7.56 K (0.9%)	4.27 MB (1.2%)	0	2436	591
Other	2016-07-01 05:40:37	4 h, 8 m, 43.774 s	other	6.46 K (6.2%)	61.76 K (7.2%)	8.34 MB (2.3%)	4	4690	141
						Flows 103.74 K	Bytes 356.99 MB		Packets 863.05 K

Autonomous System information

- Probe exports information about source and destination AS based on default or custom AS list

Other Export Capabilities

- Optional sampling on packet and flow level
- Export to more devices in various flow formats at the same time

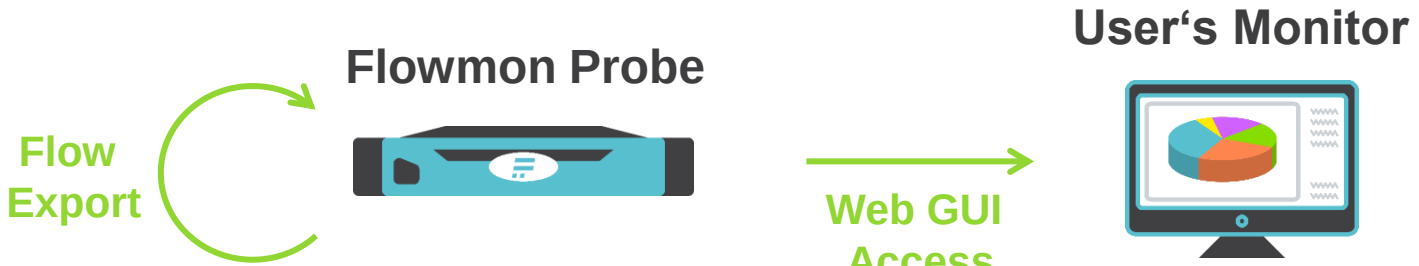


Hardware Appliance

Two modes of operation

- Exporting to collector

- Exporting to built-in collector

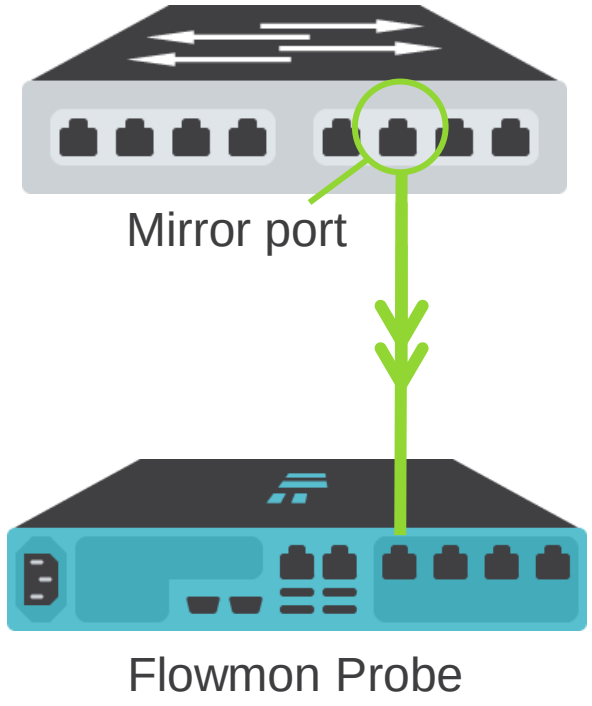


Flowmon
Driving Network Visibility

Flowmon Probe Connection

Using mirror port on switch

- Traffic mirroring from one or more switch ports
- Requires a free port on switch with enough bandwidth
- LAN monitoring

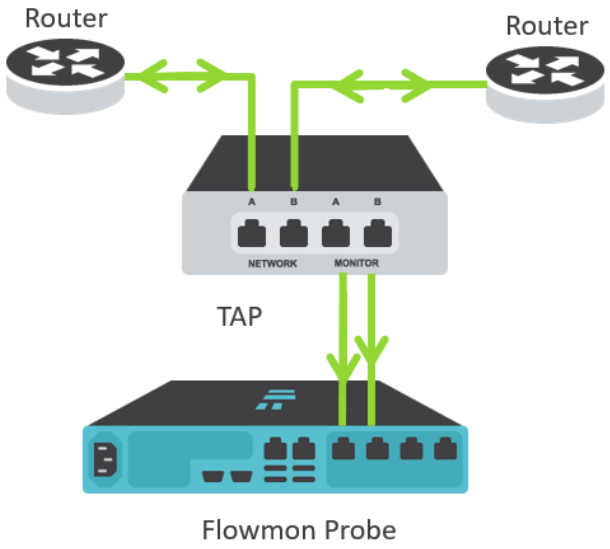


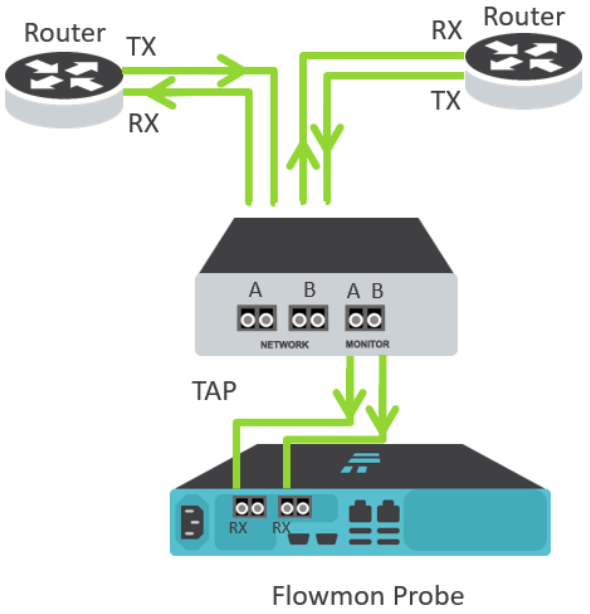
Flowmon
Driving Network Visibility

Flowmon Probe Connection

Using TAP

- Traffic mirroring from one full-duplex link
- Requires two ports on probe
- Backbone links monitoring (ISP), Internet connection





Flowmon
Driving Network Visibility

Monitoring Center (FMC)

Application for flow data storage and visualization

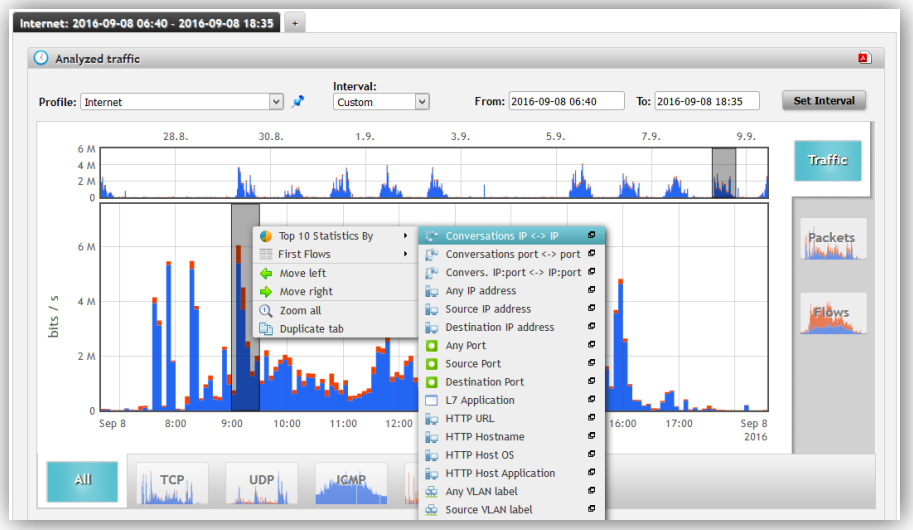
Graphs, tables and form for further data processing

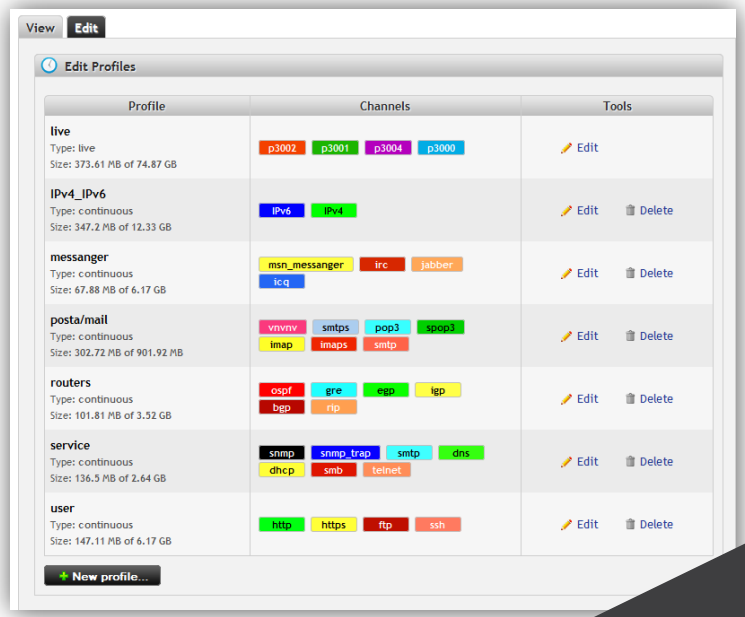
Top N statistics (users, sites, services)

Predefined set of profiles (views) for standard protocols

User defined profiles (based on IP address or ports)

Alerts, thresholds

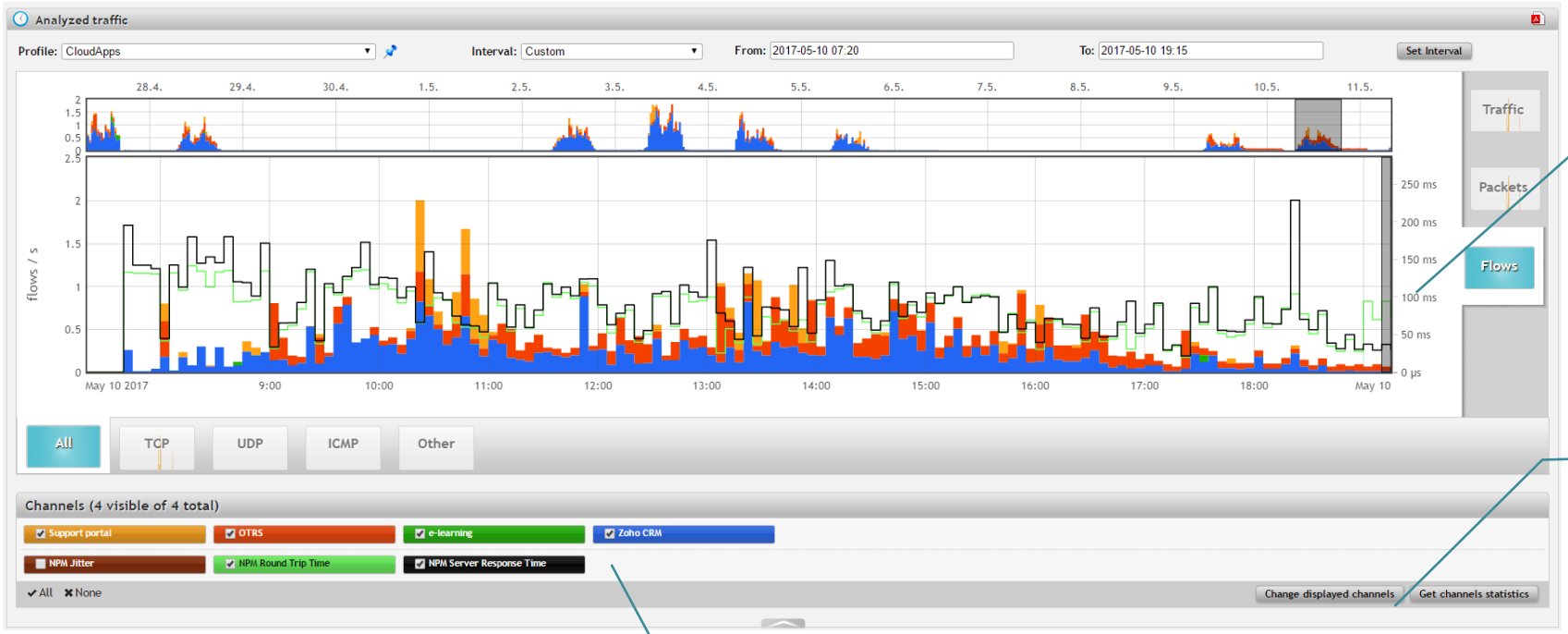




Flowmon
Driving Network Visibility

Network Performance Visualization

- Visualize network performance metrics over time frame
  - RTT, SRT, Jitter per profile/channel



Y axis on the right side of traffic chart

Change of displayed channels

Selection of current view

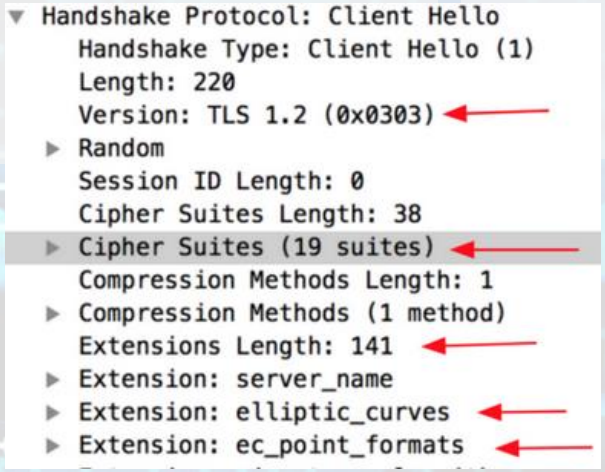
Flowmon
Driving Network Visibility

Encrypted Traffic Analysis

- Analysis of **characteristics and patterns, not decryption**
  - L3/L4: src/dsct IP:port, protocol, timestamp, data volume
- Leveraging unencrypted part of the TLS traffic
  - SSL/TLS handshake

Monitoring and security

- Malicious patterns in encrypted traffic
- JA3 fingerprinting to pinpoint suspicious actors



Cryptographic assessment

- SSL/TLS policy compliance
- Cipher suites (encryption algorithms, key lengths)
- Certificates

User Identity Awareness (Collector)

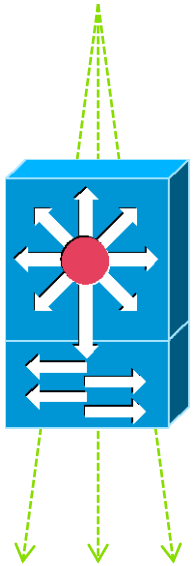
authentication

Identity source – syslog export

ISE

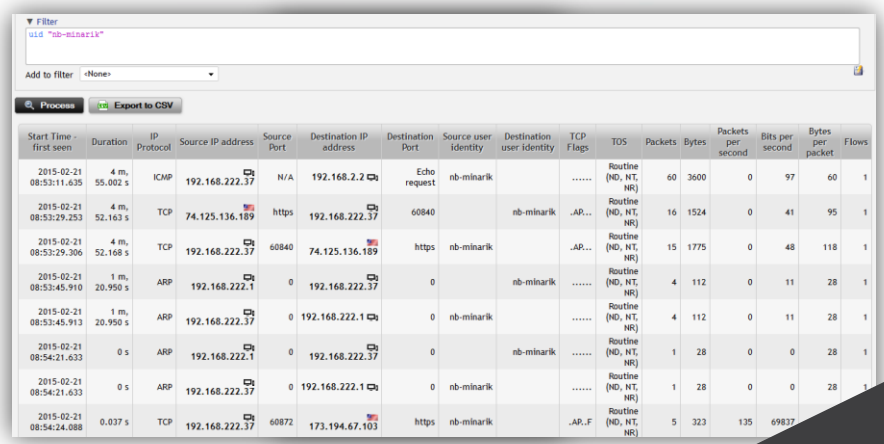
Windows Server Active Directory

Time, login, IP address



Flow (Time, IP, …)

IP	login
...	...



Google facebook

skype NETFLIX

Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security
with a single solution

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility