K ČEMU JE DOBRÝ MONITORING, ZÁZNAM A ANALÝZA SÍŤOVÝCH PARAMETRŮ A PŘENOSU

Peter Potrok

AKADEMIE VLÁKNOVÉ OPTIKY A OPTICKÝCH KOMUNIKACÍ ®

the art of optical communication

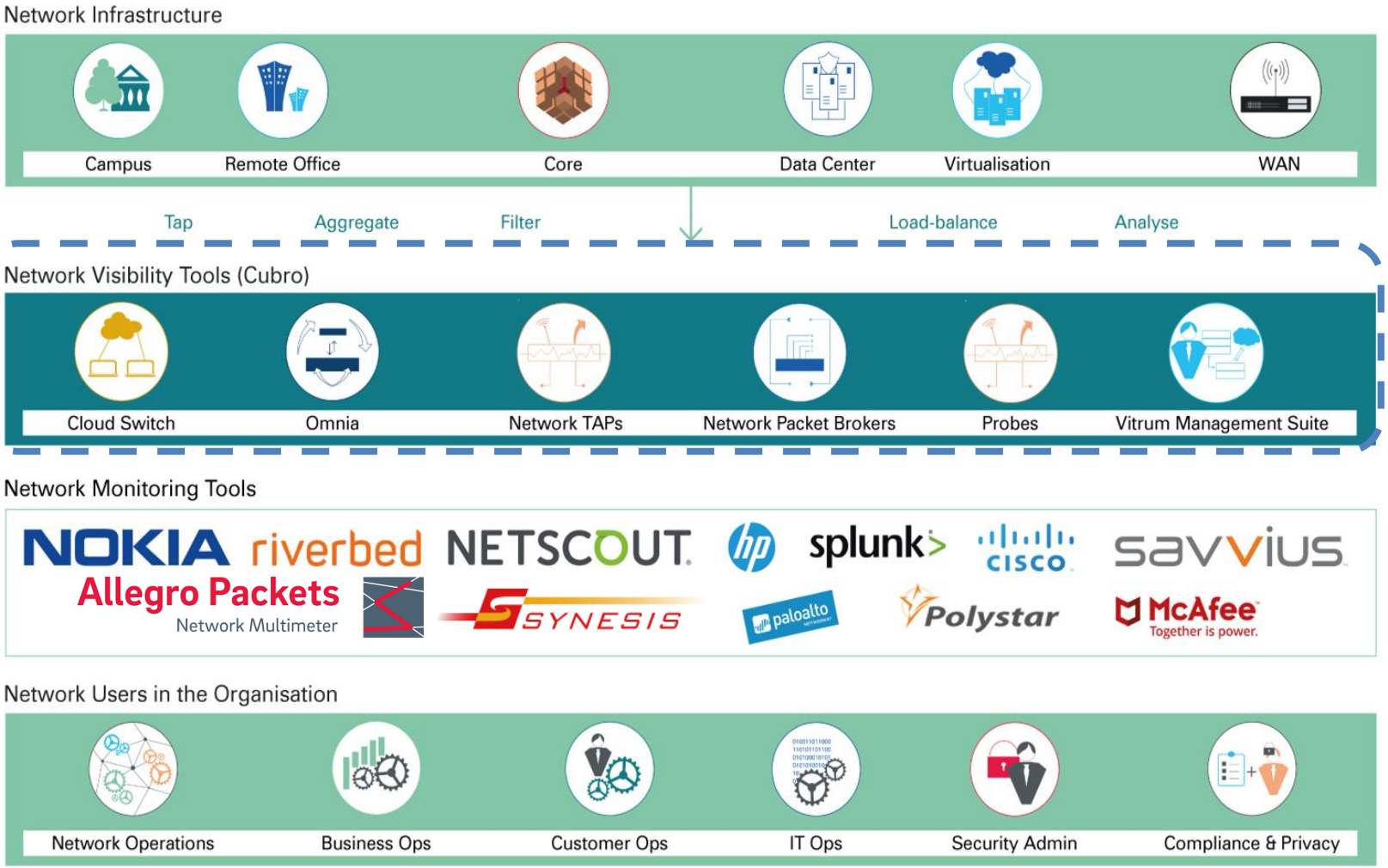
PROFiber® NETWORKING

Čo je Network Visibility

Network visibility alebo sieťová vizibilita znamená vidieť všetko čo je v sieti alebo sa cez ňu pohybuje. Prvky sieťovej vizibility poskytujú prístup k sieťovej prevádzke, monitorovacím aplikáciám, network performance nástrojom, manažmentu siete a nástrojom pre big data analýzu, čo vyžaduje efektívnu, škálovateľný zber dát, agregáciu, distribúciu a doručenie.

Sieťová vizibilita avšak nie je pasívna funkcia, povoľuje väčšiu kontrolu cez tieto aspekty. Čím viacej máte informácií do hĺbky, proaktívny prístup a rozšírenú sieťov vizibilitú, máte viacej kontroly nad dátami v sieti a tým sa viete lepšie rozhodovať vzhľadom na toky a ochranu dát.

Čo je Network Visibility



Riešenia a funkcie

Service Providers

- DPI in Packet Switched Networks
- GTP load balancing in Hardware
- Metadata extraction
- Subscriber-aware visibility
- Data enrichment for Geolocation applications
- Massive VoIP Correlation

Enterprises

- DNS Traffic analysis
- VoIP Correlation
- Metadata extraction
- Application based filtering
- Time stamping
- Inline Telemetry- Measurement

Core capabilities

- L1 to L7 Visibility
- Tapping
- Aggregation
- Filtering
- Load balancing
- Decapsulation / Encapsulation
- Metadata extraction

Riešenia a funkcie

Data Centers

- Security related two-tier load balancing
- VoIP Correlation
- Metadata extraction
- Application based filtering
- Inline Telemetry- Measurement

Govt. Organisations

- Lawful Interception
- Security related two-tier load balancing
- Keyword and regular expression search
- Deep Packet Inspection (DPI)
- In-line GTP tunnel de-encapsulate & tunnel encapsulate

SPAN port vs. Tapovanie

Použitie TAPov:

+ **Completná vizibilita**
+ **Žiadny dosah na výkonnosť**
+ **Zjednodušuje väčšie inštalácie**

- Väčšie náklady pre malé inštalácie
- Nepoužiteľné pre virtuálne aplikácie

Použite SPAN portov:

+ **Veľmi výhodné pre rýchle testy**

- Duplikácia paketov
- Nesprávne časové značky
- Pakety môžu byť mimo poradia
- Znížená výkonnosť
- Strata visibility
  - CRC / Bit errors
  - L2 Protocols

Metalické TAPy

- 10/100/1000 Ethernet
- Fail Safe
- Nízka spotreba

Optické TAPy

- SM & MM
- LC a/alebo MTP konektory
- Až do 800G
- Rôzne pomer splitovania
- Plne pasívne a transparetné

Klasické aplikácie pre NPB

Agregácia:
Spojenie dát z viacerých vstupov na jeden výstup (n:1) alebo viacej výstupov (m:n) pre paralelné monitorovacie systémy.

Filtrovanie:
Analýza iba tých dát, ktoré majú byť analyzované a odstrániť všetko čo je nie je potrebné.

Load-balancing:
Zdieľanie prevádzky na viacero analyzátorov / nástrojov.

Ochrana vášho monitorovacieho vybavenia pred preťažením nepotrebnými dátami.

Problémy so záznamom prevádzky

Sofistikované a komplexné siete

Zvýšené nebezpečenstvo falošnej pozitivity a falošnej negativity

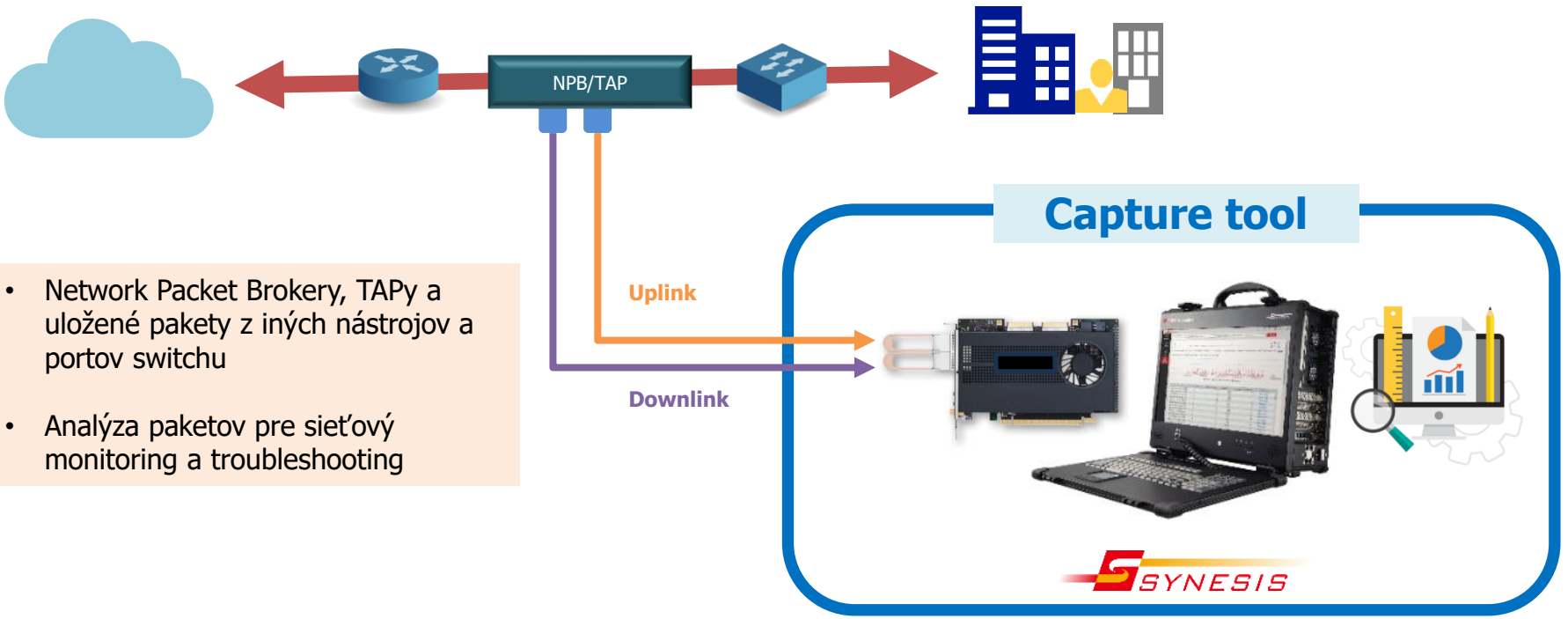
Odkiaľ prichádzajú chyby?
Je nutné spraviť záznam na niektorých miestach v sieti

Obmedzená analýza veľkého množstva paketov

Kde nájdem problém?
Dáta musia byť skontrolované jeden za druhým

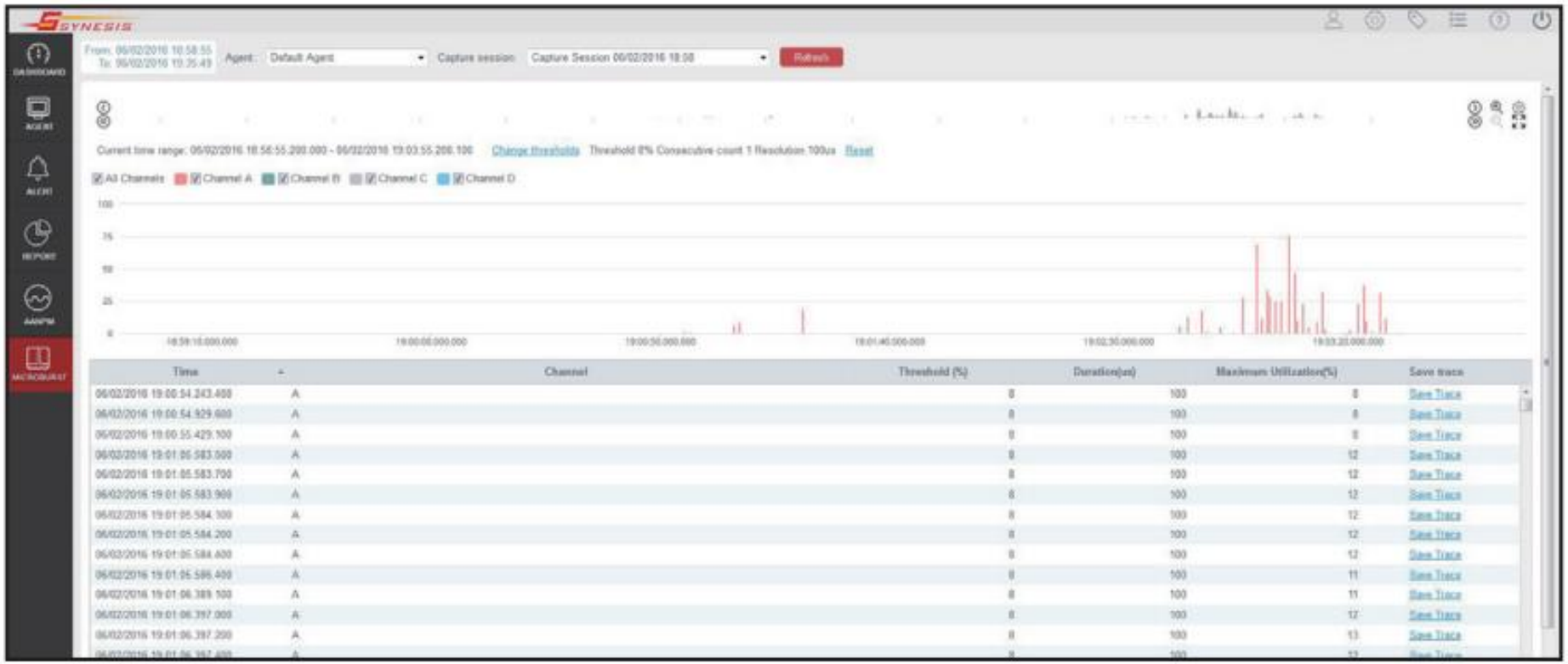
Nedostatočný počet ľudí a skúseností

Čo je nástroj pre záznam prevádzky

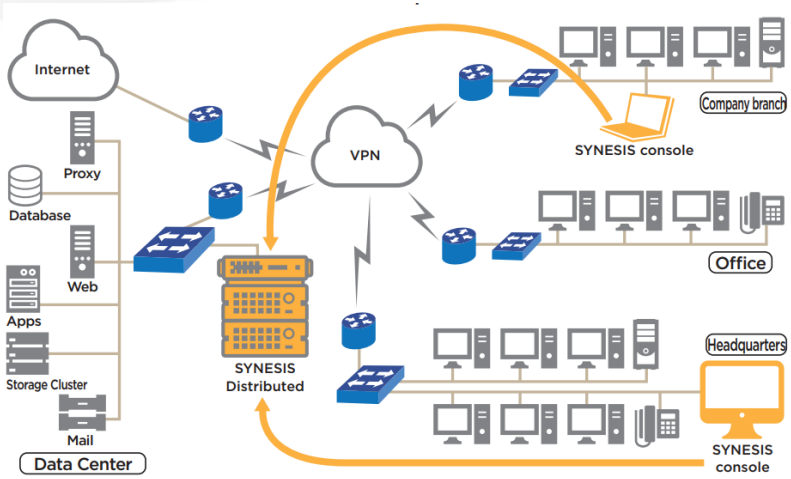


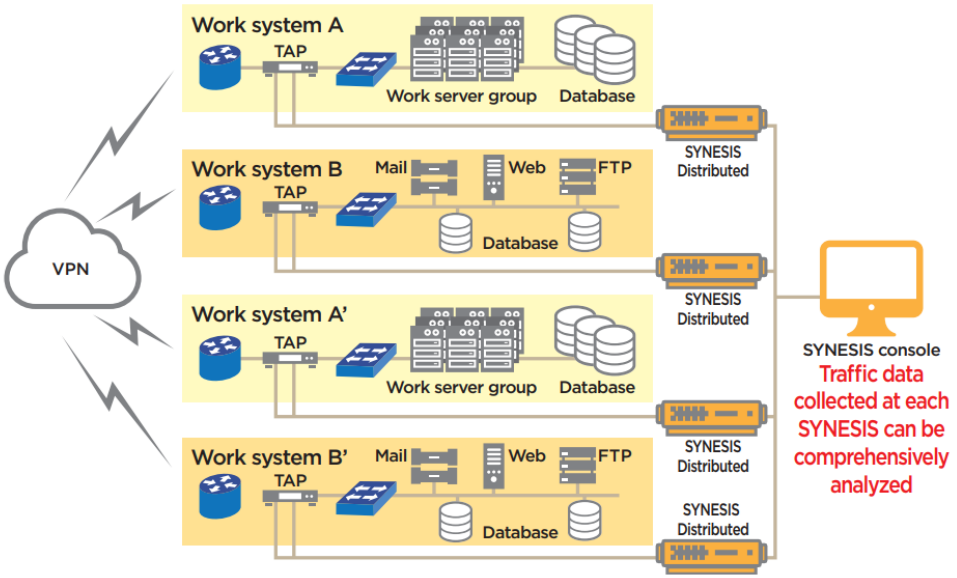
- Network Packet Brokery, TAPy a uložené pakety z iných nástrojov a portov switchu
- Analýza paketov pre sieťový monitoring a troubleshooting

uBurst-y

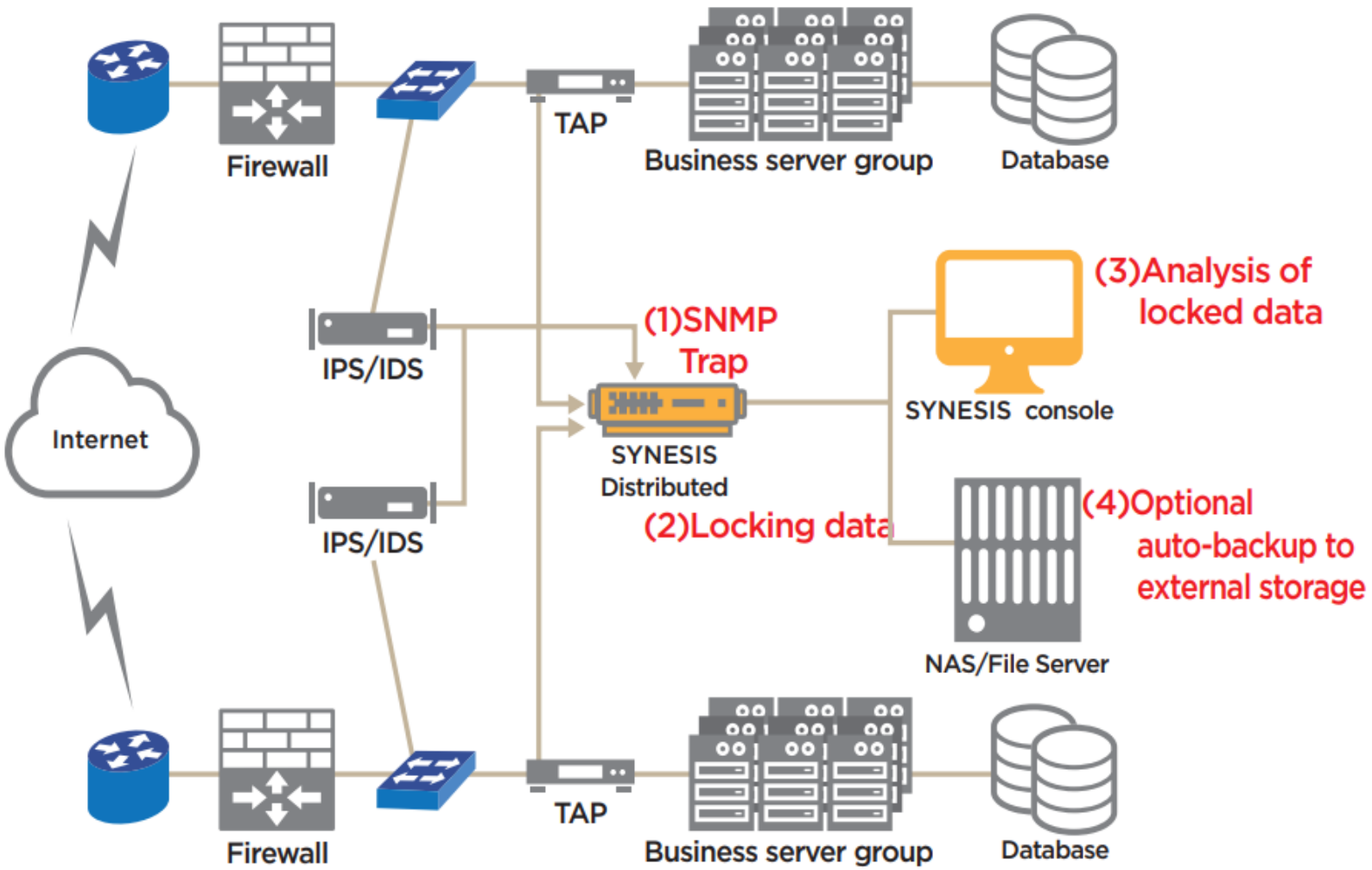

SYNESIS
Agent: Default Agent
Capture session: Capture Session 06/02/2016 18:58
Refresh
Change thresholds
Threshold 8% Consecutive count 1 Resolution 100us
Reset
All Channels
Channel A
Channel B
Channel C
Channel D
Time
Channel
Threshold (%)
Duration(us)
Maximum Utilization(%)
Save trace

Distribuovaná analýza



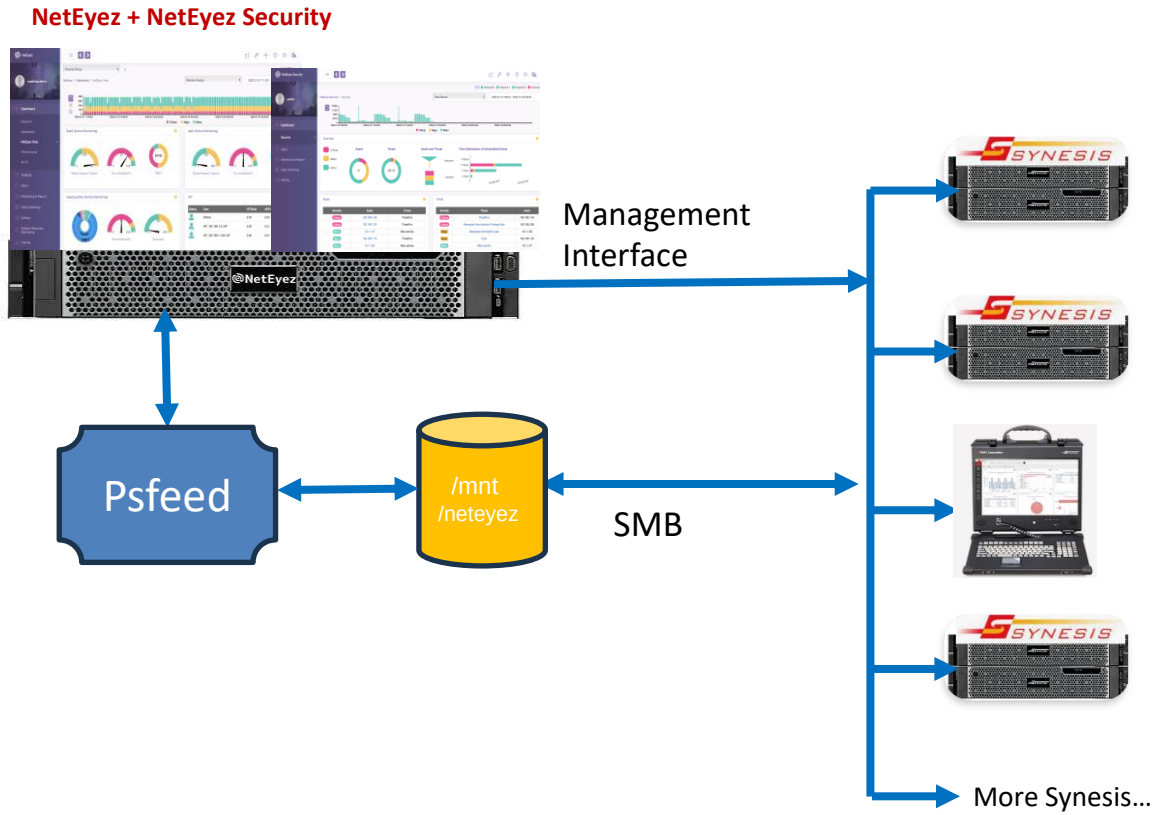


Distribuovaná analýza + SNMP



Synesis + NetEyez

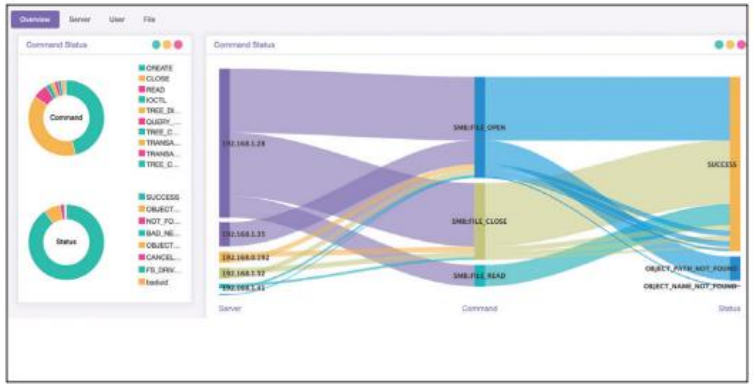
- SYNESIS systém je jednoducho integrovateľný do NetEyez GUI.
- SYNESIS zaznamenáva dáta a analyzuje ich cez SMB disk v NetEyez.
- Dátová analýza pomocou NetEyez zo SYNESIS záznamu sa ukladajú v NetEyez databáze



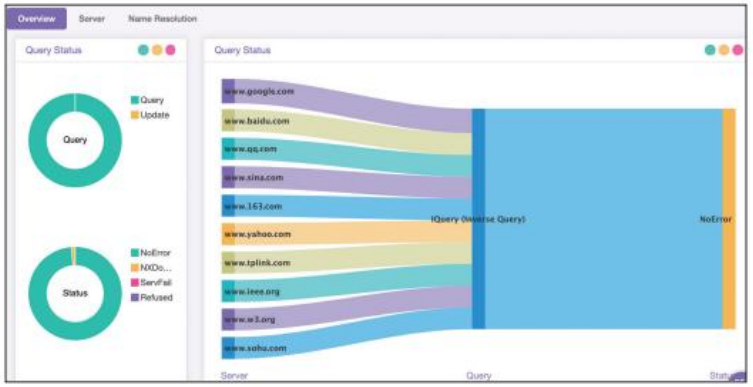
NetEyez

Identification of communication bottlenecks
ART: Application Response time / CRT: Client Response time
NRT: Network Response Time / Retry : Number of retransmitted packets.

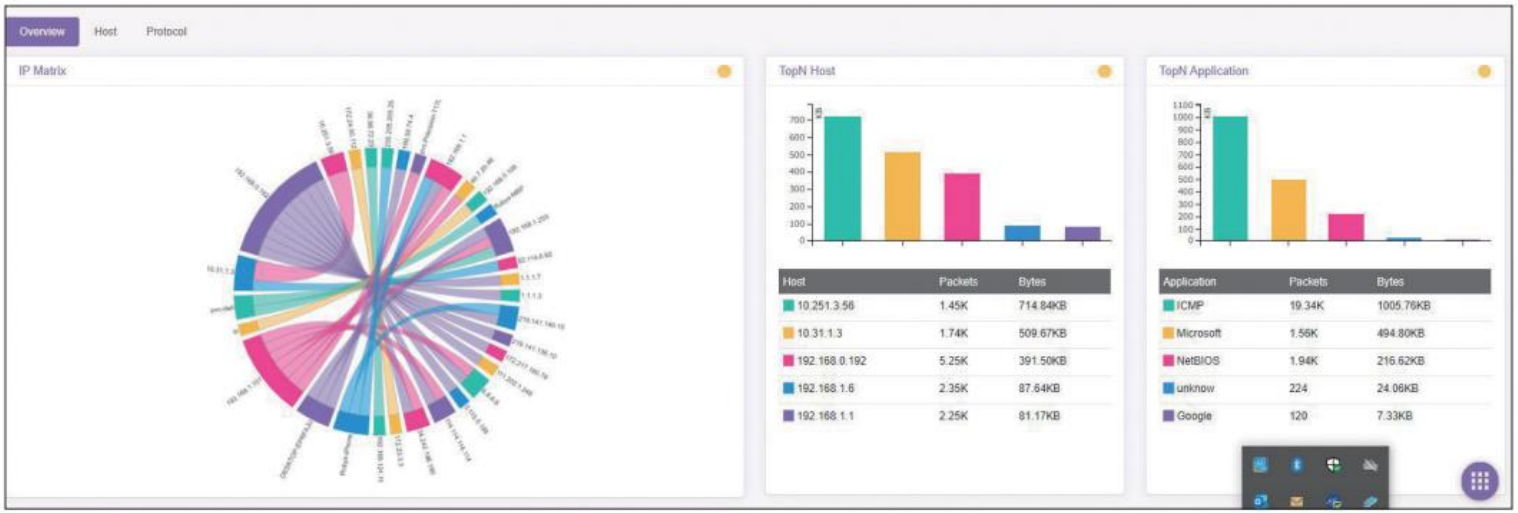
Access status of web



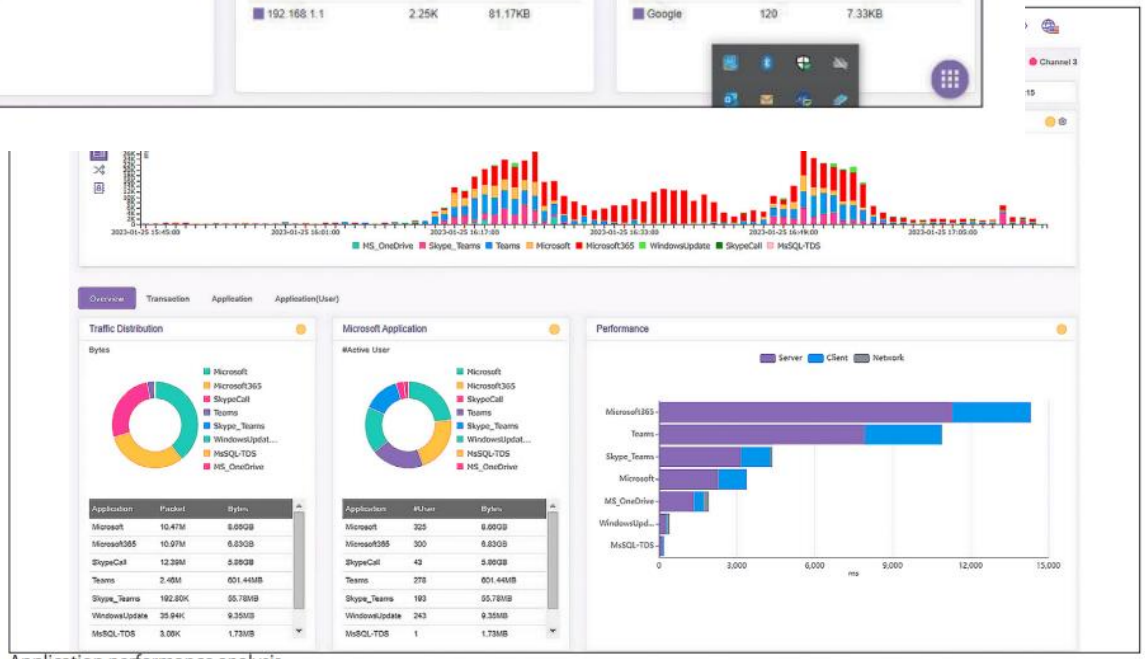
Access status of SMB



Access status of DNS



TOPN application/host



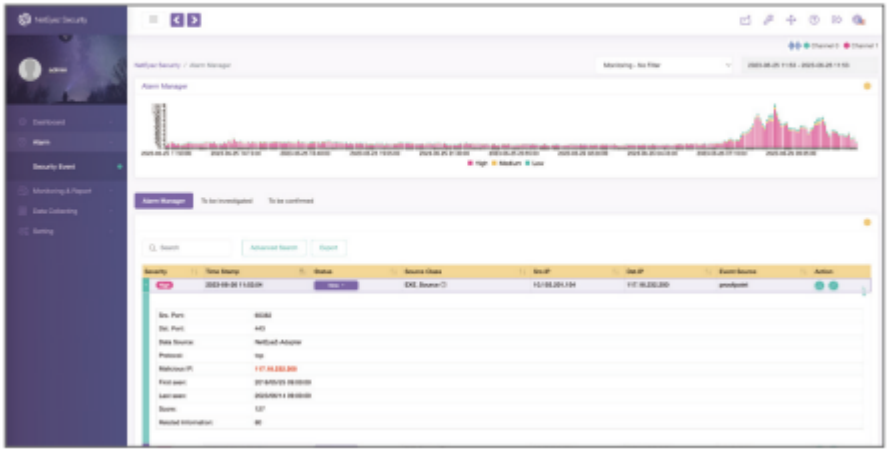
Application performance analysis

NetEyez Security

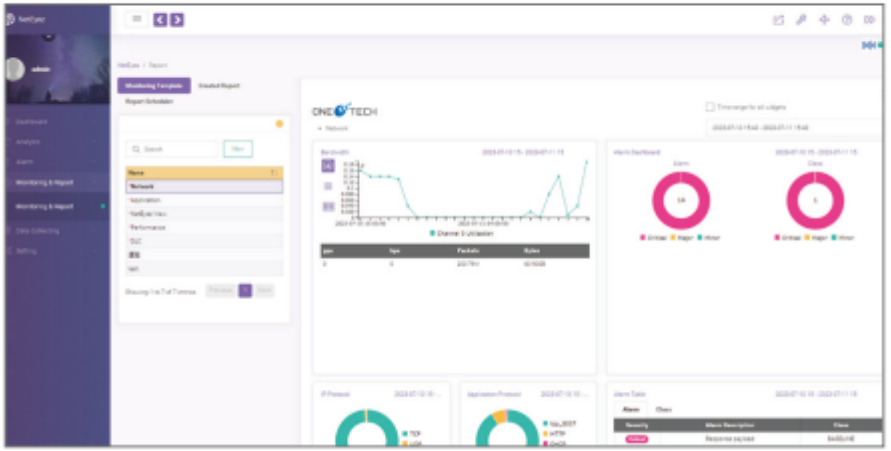
Security Monitoring and Analysis

Detect Threat with Advanced Security

Network Security Visualization



Report



Konferencia

Stretnutie profesionálov 2024

23.05.2024 – 24.5.2024 – Trnava

30.05.2024 – 31.5.2024 - Praha

Ďakujem za pozornosť,

peter.potrok@profiber.eu

AKADEMIE VLÁKNOVÉ OPTIKY A OPTICKÝCH KOMUNIKACÍ ®

PROFiber Networking CZ s.r.o.
Mezi Vodami 205/29
143 00 Praha 4

PROFiber Networking s.r.o.
Bernolákova 2
917 01 Trnava

the art of optical communication

PROFiber® NETWORKING