Jak efektywnie wykorzystać technologię netflow - troubleshooting sieci, monitoring wydajności usług (doświadczenia Klientów)

Warszawa 06.10.2016

Adrian Turowski

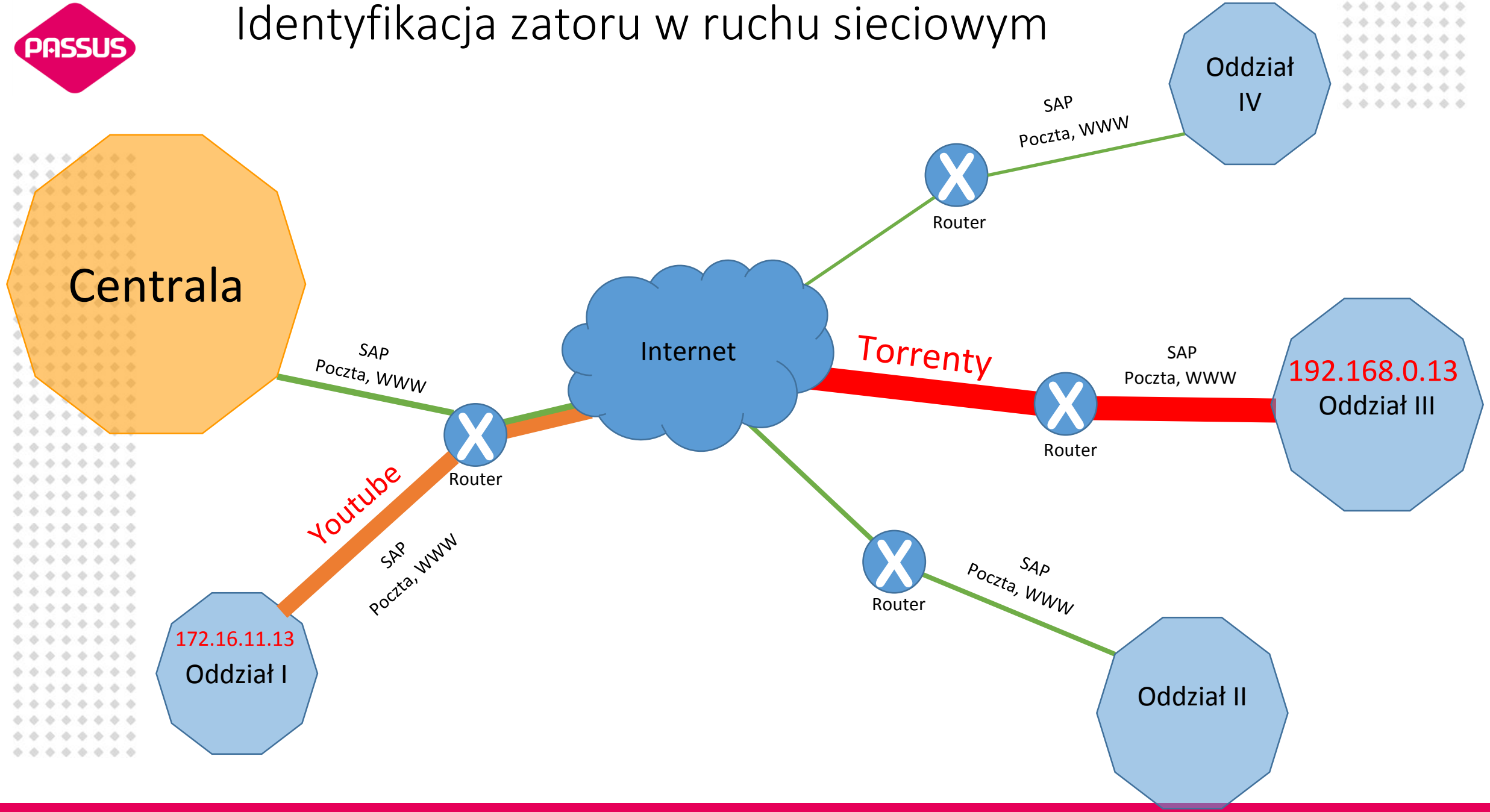
Najczęstsze wykorzystywanie Netflow przez klientów

- Identyfikacja zatoru w ruchu sieciowym
- Monitoring QoS
- Sprawdzanie rozkładania się ruchu po AS
- Wykrywanie anomalii w ruchu sieciowym

01

Identyfikacja zatoru w ruchu sieciowym

Identyfikacja zatoru w ruchu sieciowym

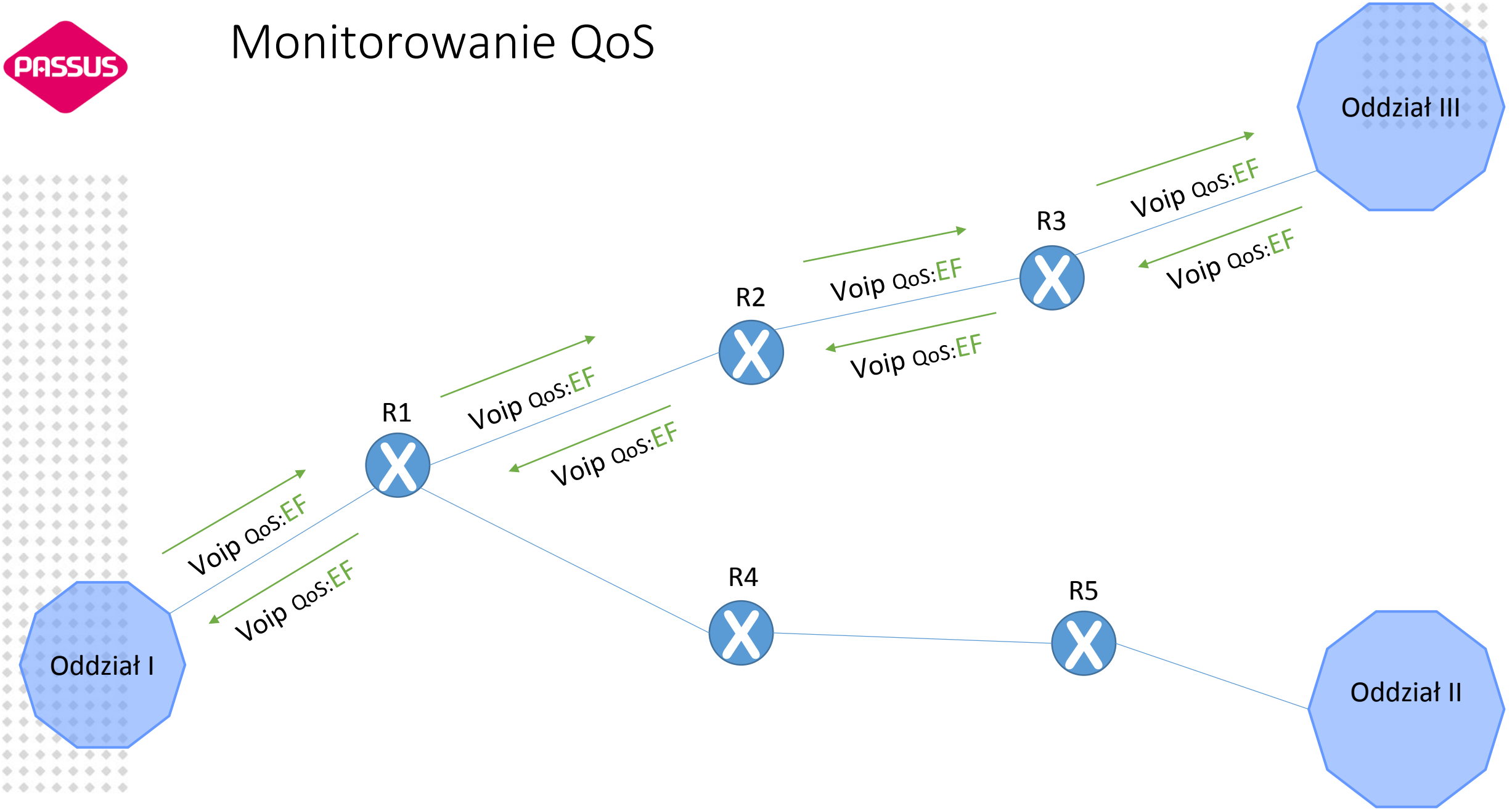


PASSUS

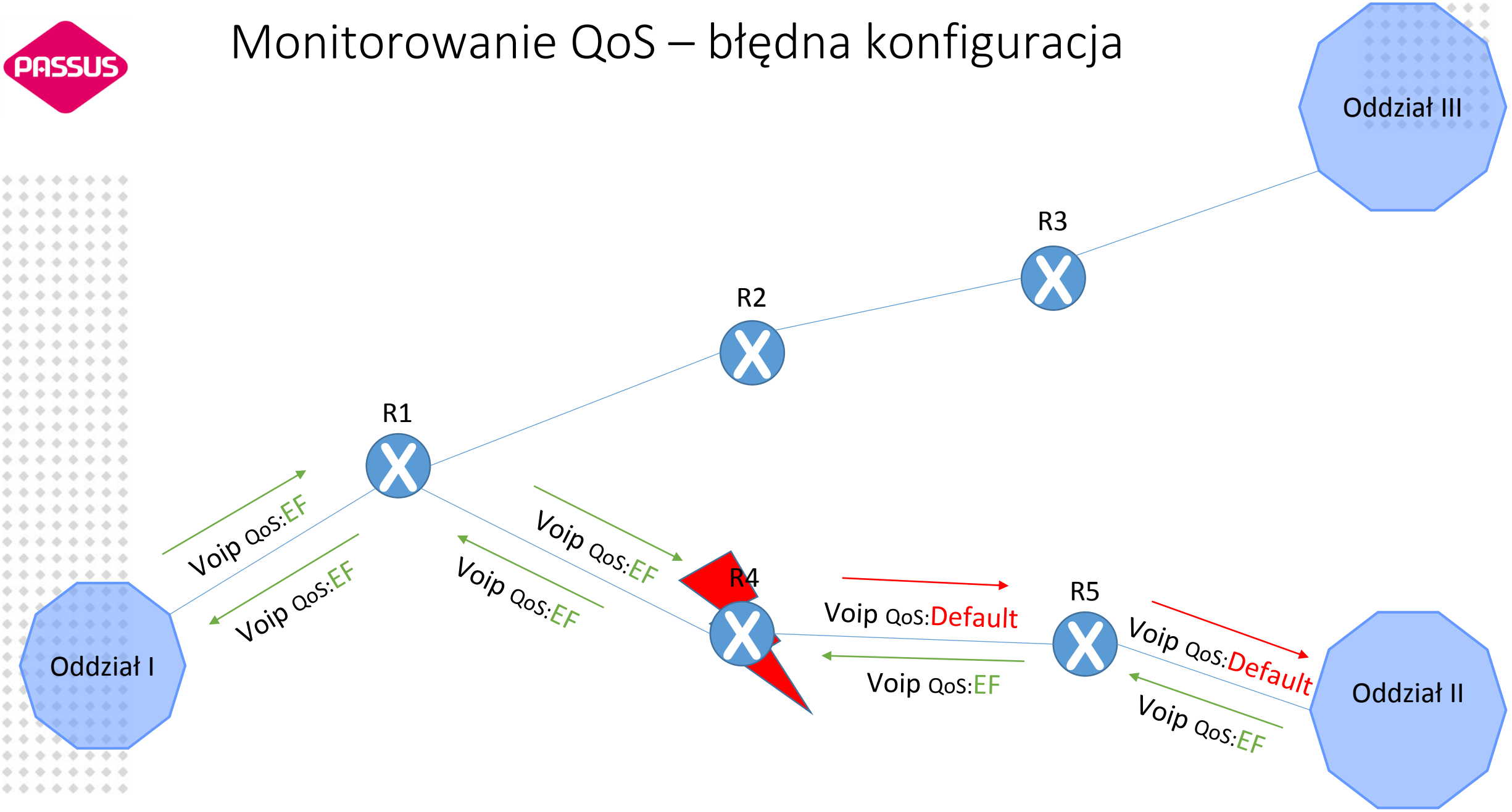
02

Monitoring QoS

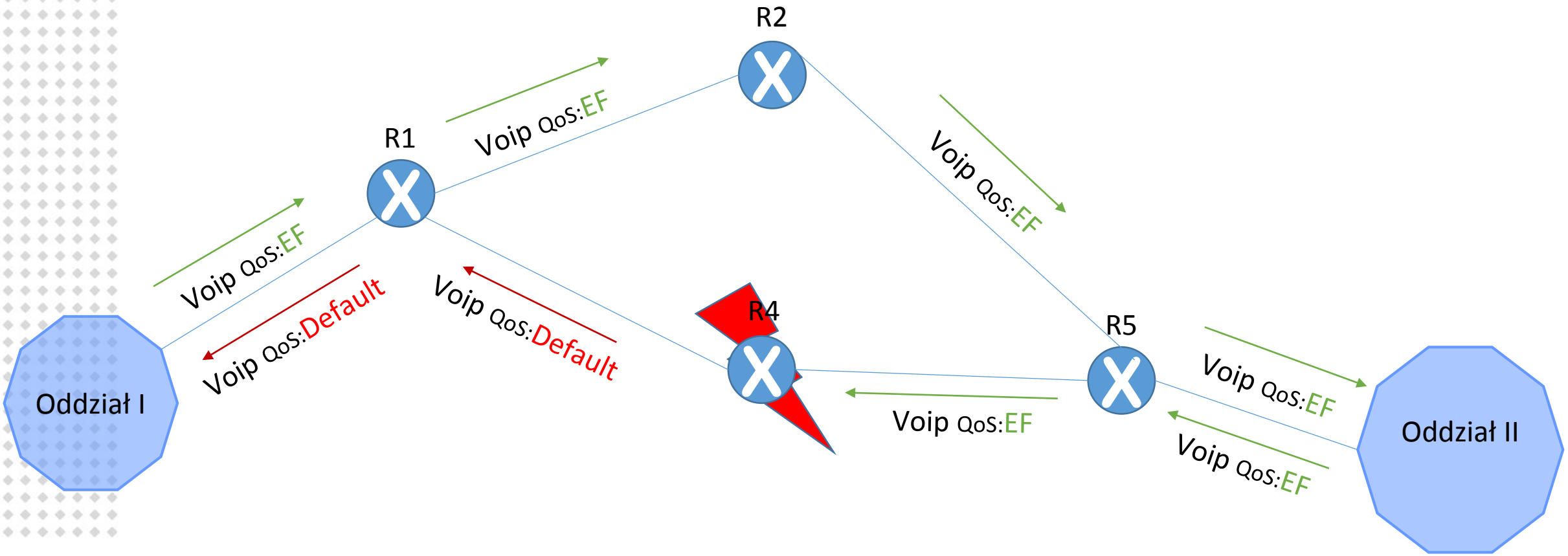
Monitorowanie QoS



Monitorowanie QoS – błędna konfiguracja



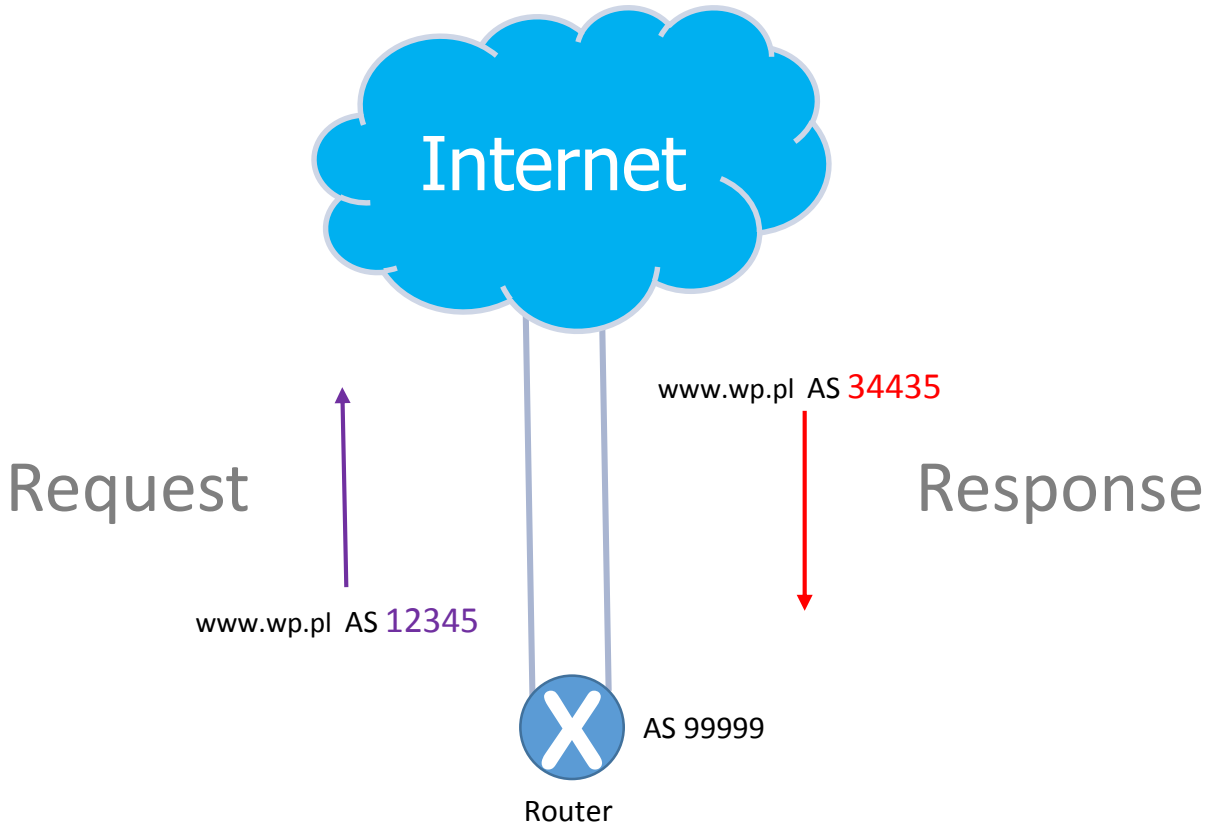
Monitorowanie QoS – asynchroniczna trasa



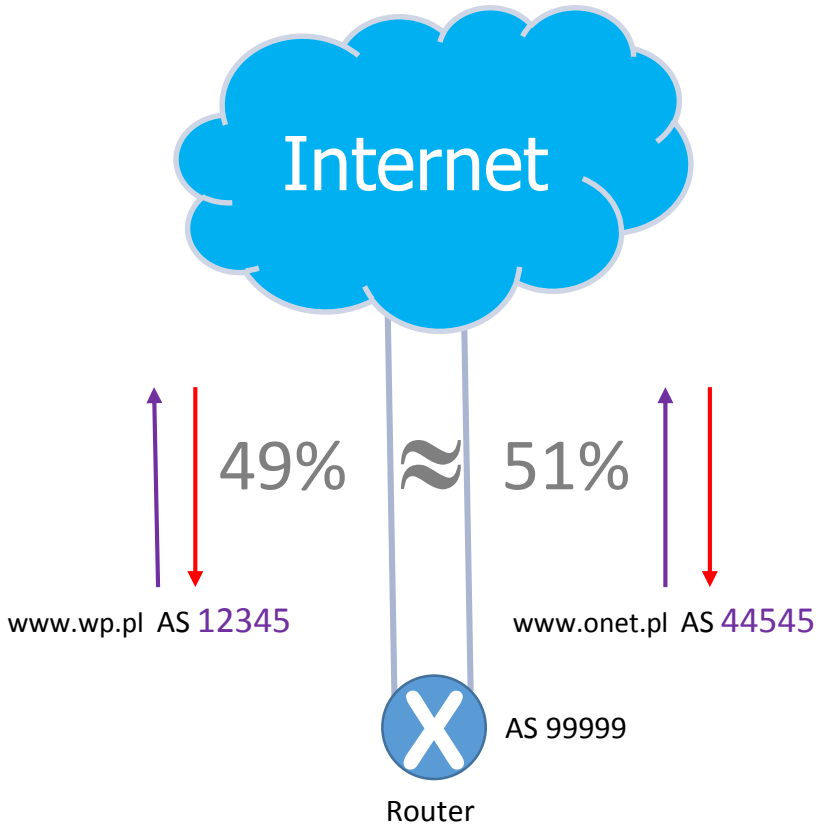
03

Sprawdzanie rozkładania się ruchu dla AS

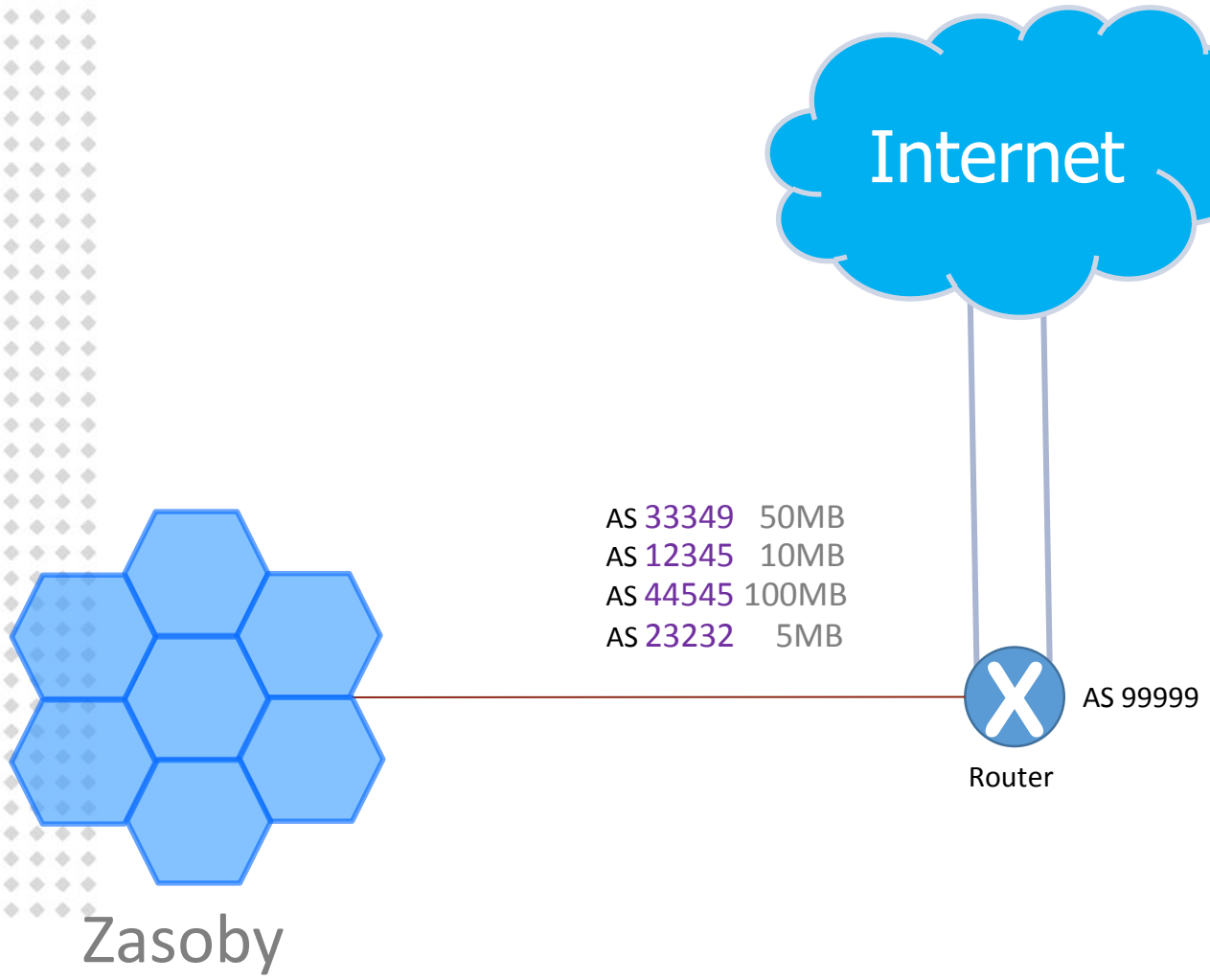
Wykrywanie routingu asynchronicznego



Sprawdzanie równomiernego rozłożenia ruchu do operatorów



Sprawdzanie kto dokładnie korzysta z naszych zasobów

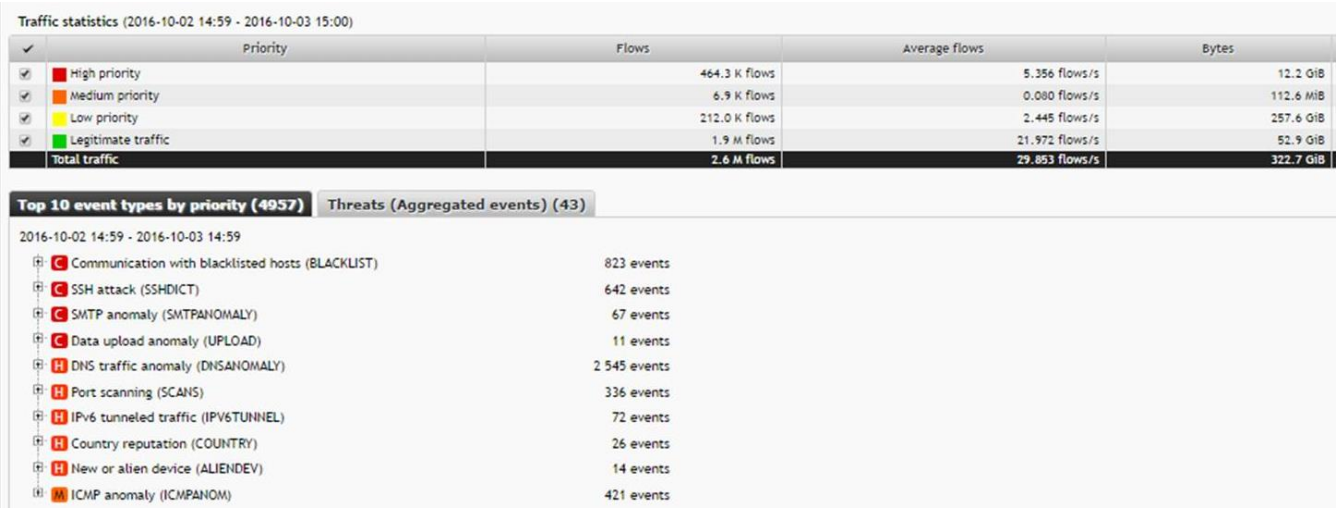


04

Wykrywanie anomalii w ruchu sieciowym

Wykrywanie anomalii w ruchu sieciowym

- Skanowanie hostów
- Skanowanie portów
- Podejrzane połączenia
- Nowe hosty w sieci
- Nowe usługi w sieci
- Nie zaufane DNSy
- Podejrzany ruch DHCP



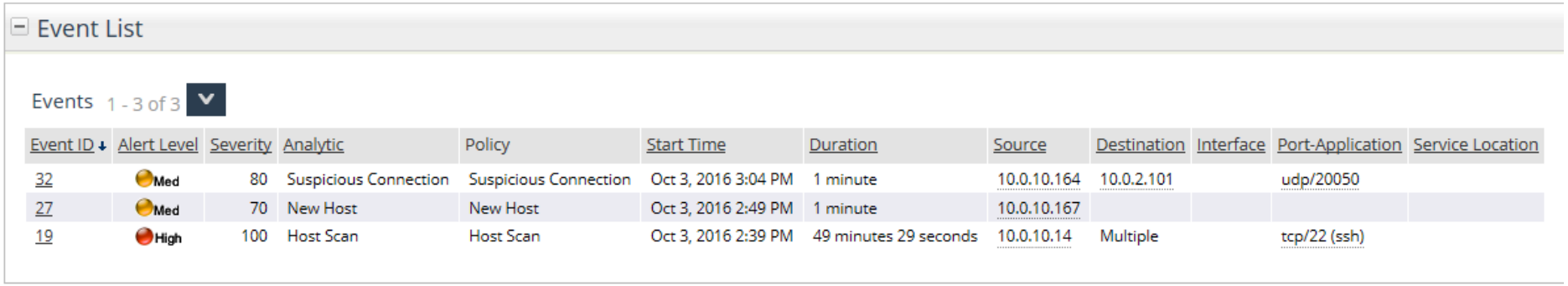
Traffic statistics (2016-10-02 14:59 - 2016-10-03 15:00)

Priority	Flows	Average flows	Bytes
High priority	464.3 K flows	5.356 flows/s	12.2 GiB
Medium priority	6.9 K flows	0.080 flows/s	112.6 MiB
Low priority	212.0 K flows	2.445 flows/s	257.6 GiB
Legitimate traffic	1.9 M flows	21.972 flows/s	52.9 GiB
Total traffic	2.6 M flows	29.853 flows/s	322.7 GiB

Top 10 event types by priority (4957) | Threats (Aggregated events) (43)

2016-10-02 14:59 - 2016-10-03 14:59

Communication with blacklisted hosts (BLACKLIST)	823 events
SSH attack (SSHDICT)	642 events
SMTP anomaly (SMTPANOMALY)	67 events
Data upload anomaly (UPLOAD)	11 events
DNS traffic anomaly (DNSANOMALY)	2 545 events
Port scanning (SCANS)	336 events
IPv6 tunneled traffic (IPV6TUNNEL)	72 events
Country reputation (COUNTRY)	26 events
New or alien device (ALIENDEV)	14 events
ICMP anomaly (ICMPANOM)	421 events



Event List

Events 1 - 3 of 3

Event ID	Alert Level	Severity	Analytic	Policy	Start Time	Duration	Source	Destination	Interface	Port-Application	Service Location
32	Med	80	Suspicious Connection	Suspicious Connection	Oct 3, 2016 3:04 PM	1 minute	10.0.10.164	10.0.2.101		udp/20050	
27	Med	70	New Host	New Host	Oct 3, 2016 2:49 PM	1 minute	10.0.10.167				
19	High	100	Host Scan	Host Scan	Oct 3, 2016 2:39 PM	49 minutes 29 seconds	10.0.10.14	Multiple		tcp/22 (ssh)	

Podsumowania zdarzeń

Dziękuję

adrian.turowski@passus.com.pl