



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



# Najczęstsze wykorzystywanie Netflow przez klientów



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





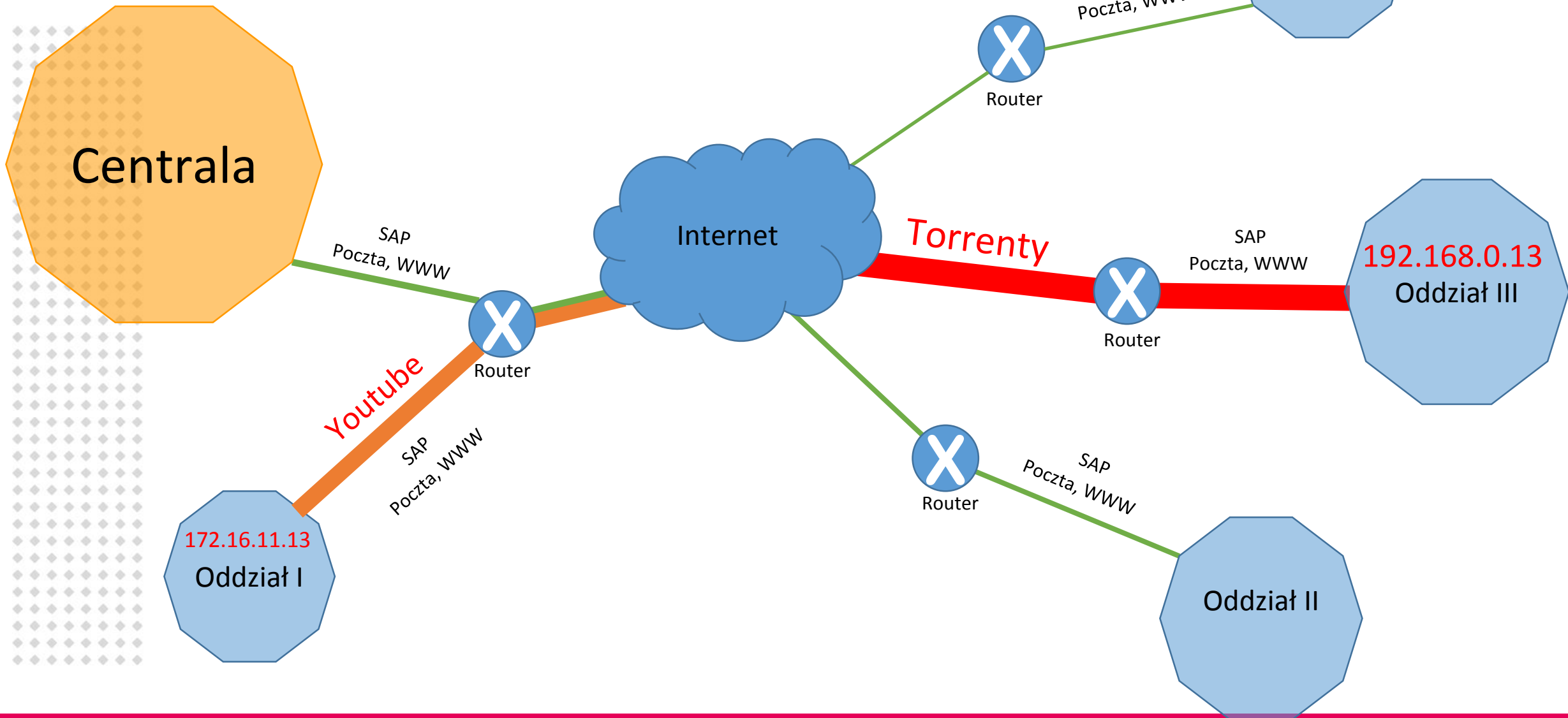
01

---

# Identyfikacja zatoru w ruchu sieciowym



# Identyfikacja zatoru w ruchu sieciowym





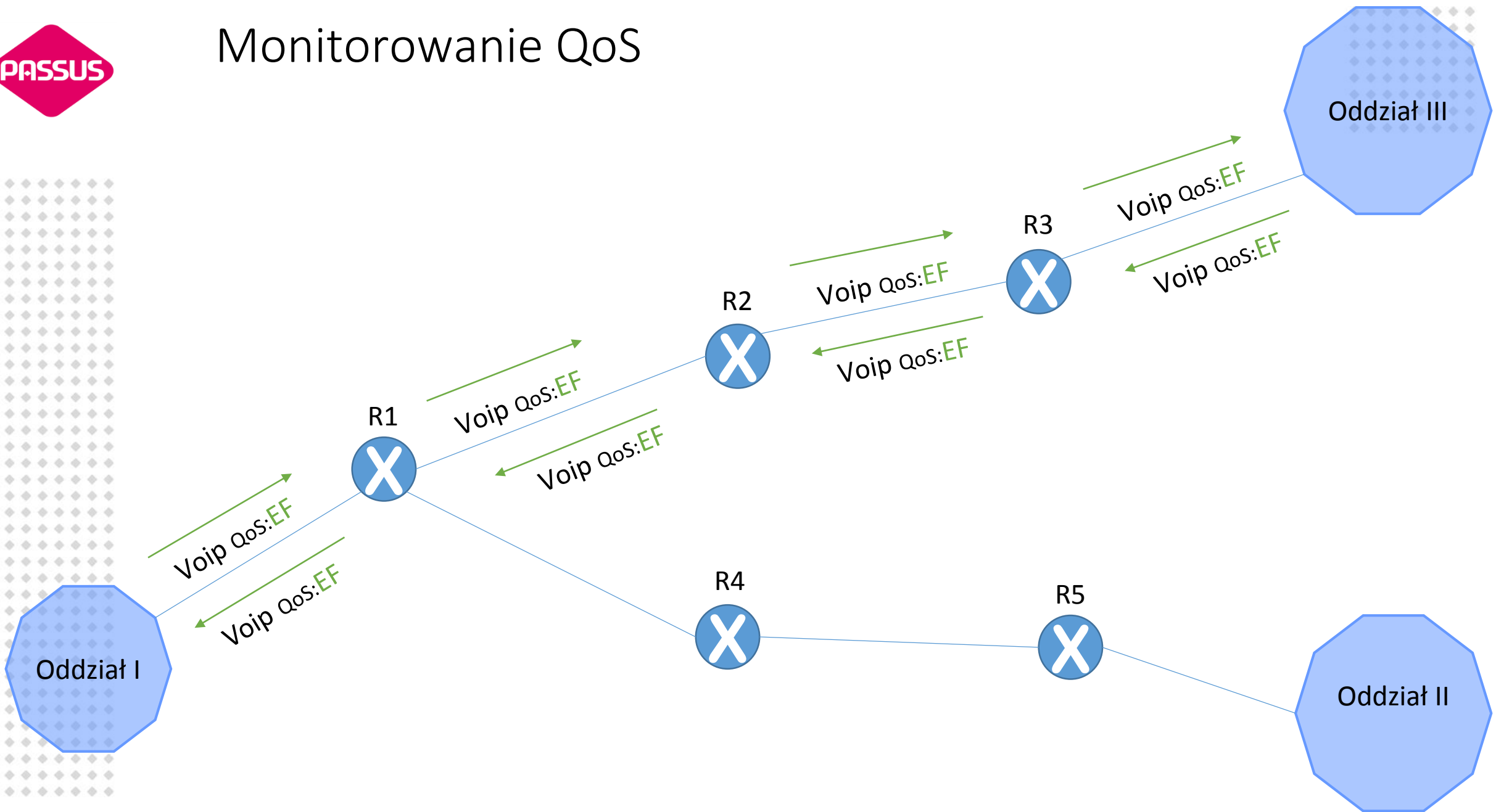
02

---

# Monitoring QoS

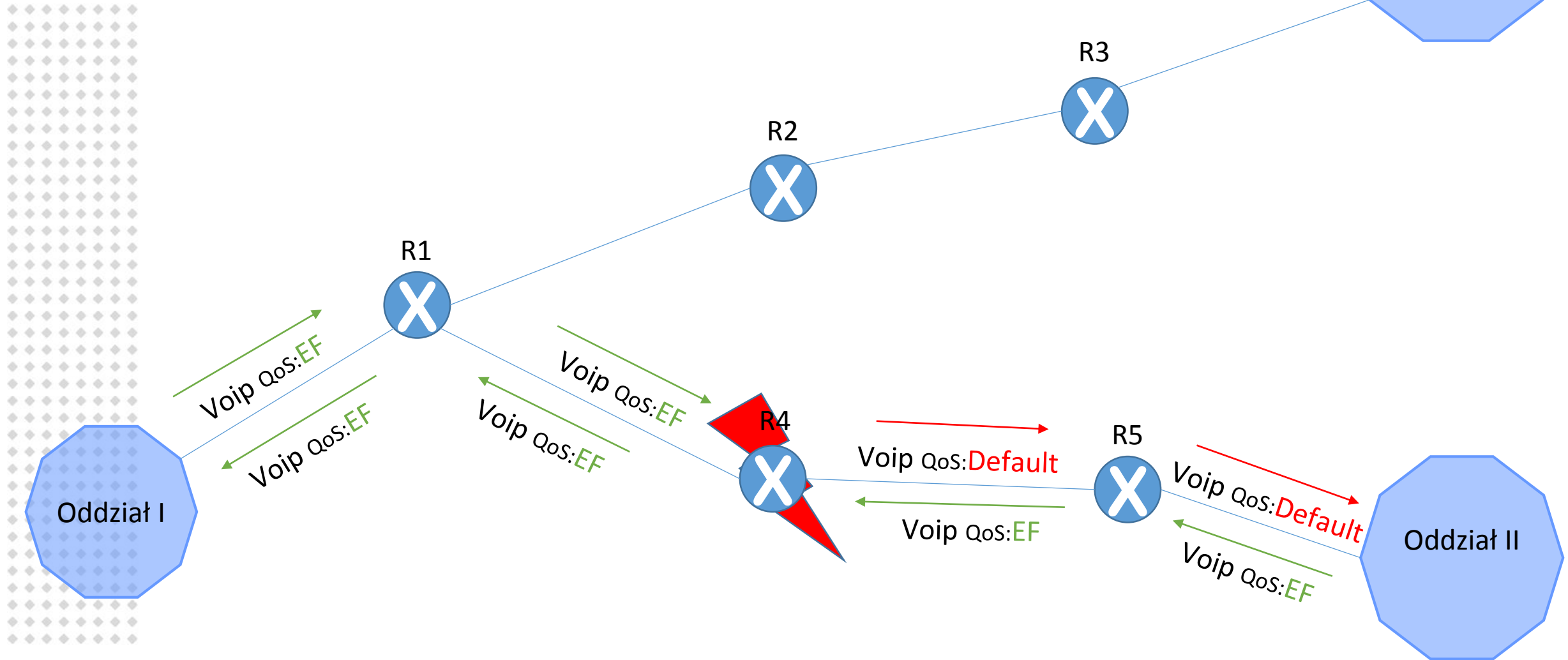


# Monitorowanie QoS



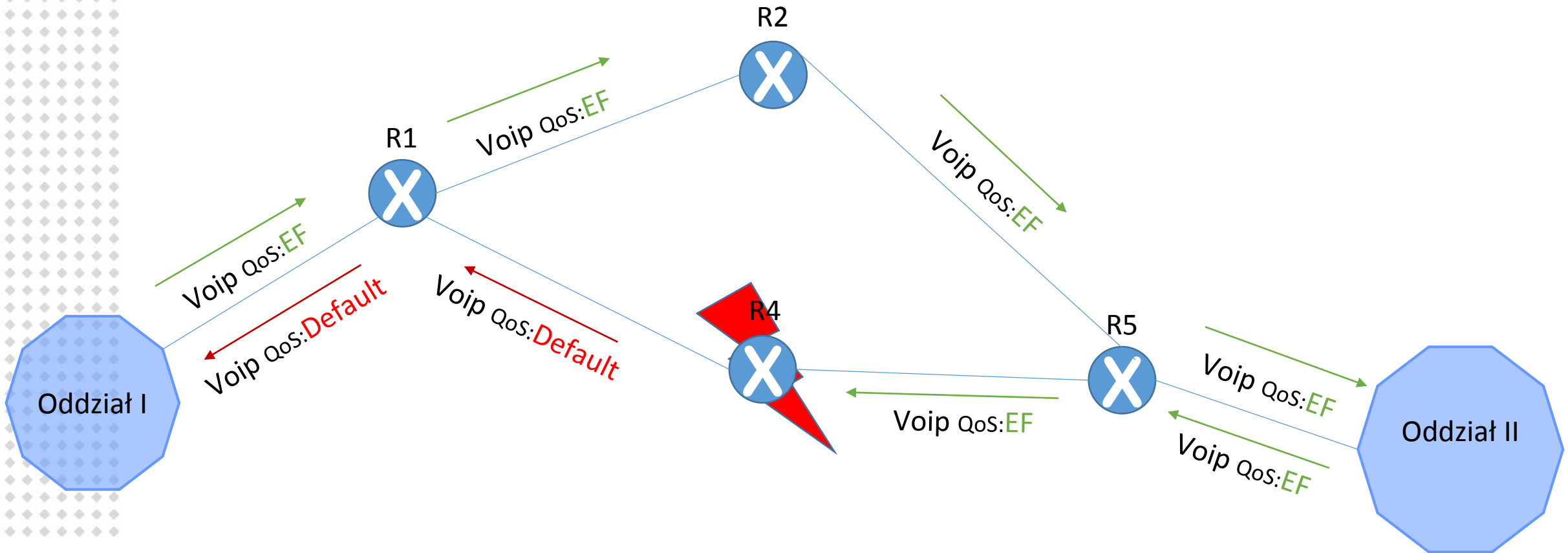


# Monitorowanie QoS – błędna konfiguracja





# Monitorowanie QoS – asynchroniczna trasa



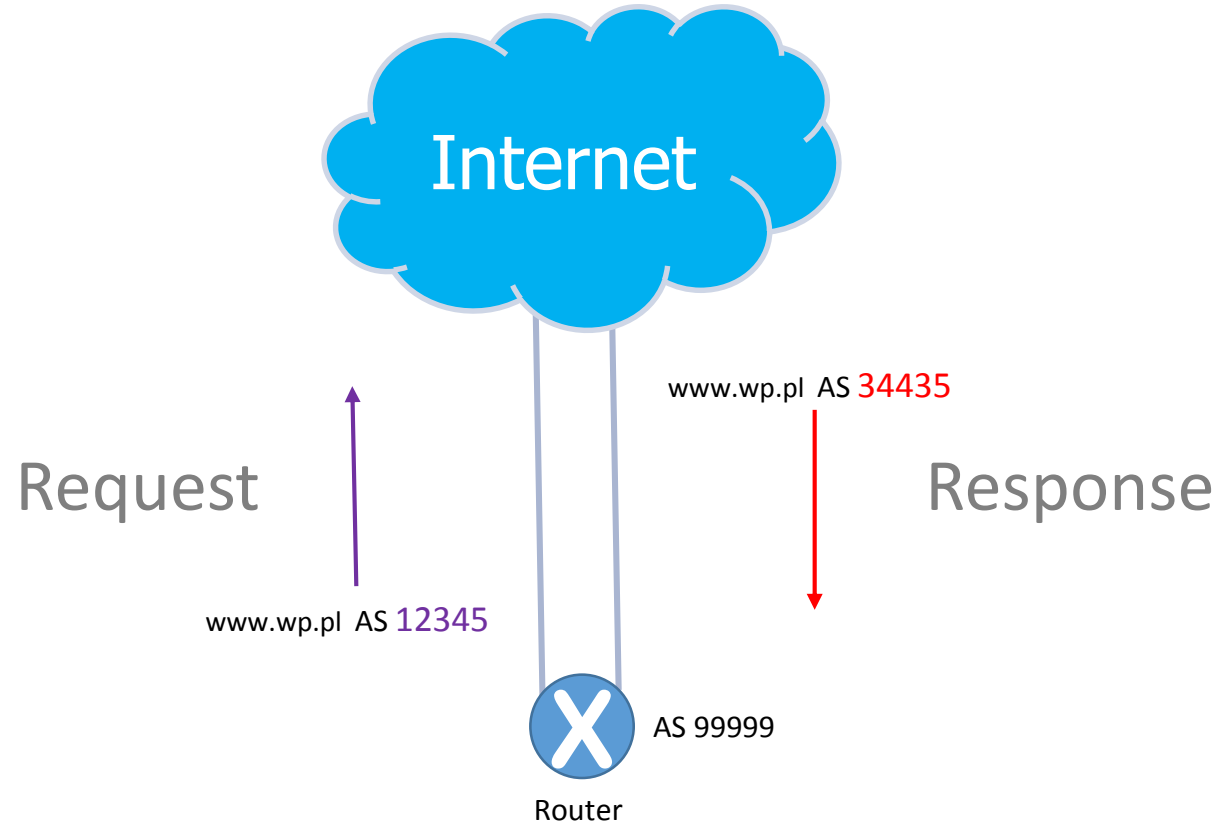


03

---

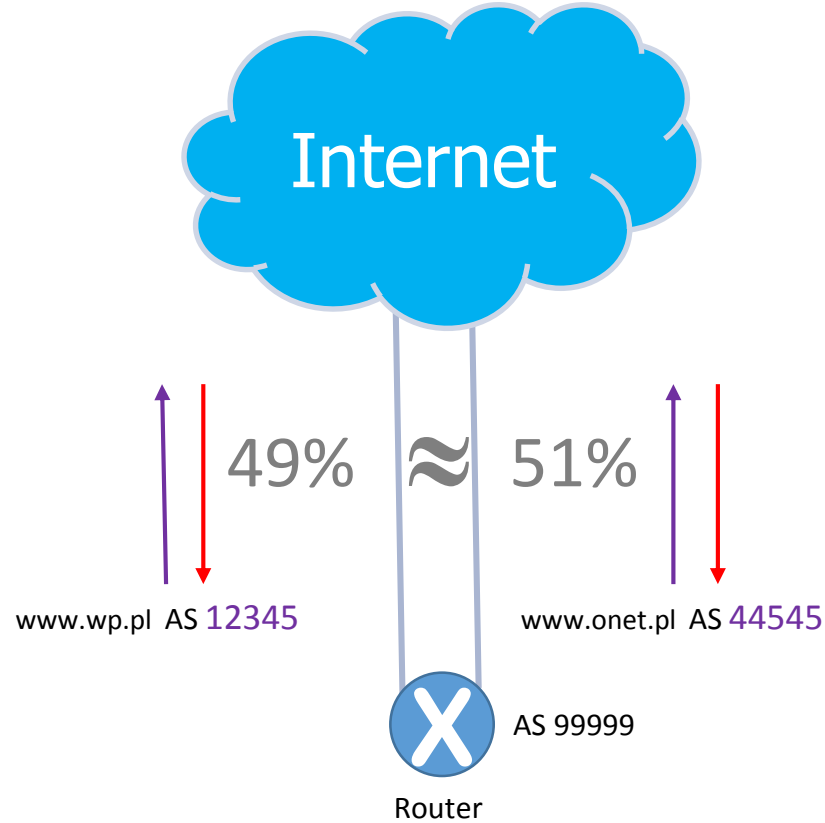
Sprawdzanie rozkładania się ruchu dla AS

# Wykrywanie routingu asynchronicznego



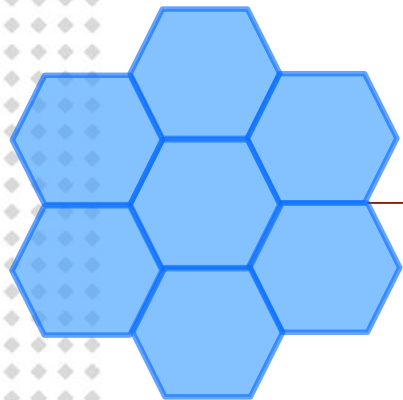


# Sprawdzanie równomiernego rozłożenia ruchu do operatorów





# Sprawdzanie kto dokładnie korzysta z naszych zasobów



Zasoby

- AS 33349 50MB
- AS 12345 10MB
- AS 44545 100MB
- AS 23232 5MB



AS 99999

Router

04

---

# Wykrywanie anomalii w ruchu sieciowym



# Wykrywanie anomalii w ruchu sieciowym

- Skanowanie hostów
- Skanowanie portów
- Podejrzone 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
<b>Total traffic</b>	<b>2.6 M flows</b>	<b>29.853 flows/s</b>	<b>322.7 GiB</b>

**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
<a href="#">32</a>	Med	80	Suspicious Connection	Suspicious Connection	Oct 3, 2016 3:04 PM	1 minute	10.0.10.164	10.0.2.101		udp/20050	
<a href="#">27</a>	Med	70	New Host	New Host	Oct 3, 2016 2:49 PM	1 minute	10.0.10.167				
<a href="#">19</a>	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



## Event Summary

### Event Details

#### Event details

Type: SSH attack (SSHDICT)  
Timestamp: 2016-10-03 14:50:00  
First Flow: 2016-10-03 14:49:50

Event source: 116.31.116.10 (unknown)  
Captured source hostname: N/A  
Flow source: Default  
Detected by instance: Default

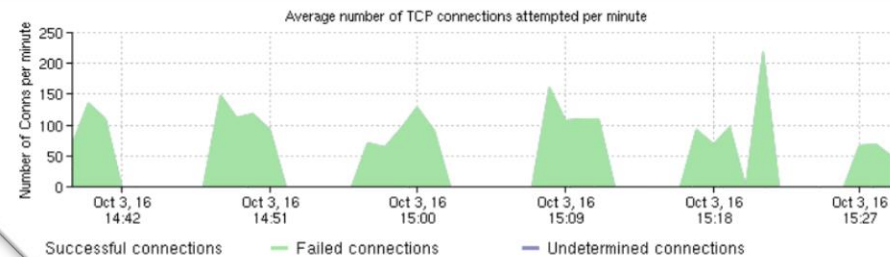
Probability: 71 %  
False positive: No  
User Identity: N/A

Detail: Continuation of attack (unsuccessful) to 3 targets (whole attack). Current statistics: attempts: 8, total upload: 17.75 KiB, maximal upload: 2.76 KiB. Part of distributed attack.

**Targets (3)** Comments (0) Categories (0) Event evidence

**All targets** By country By IP

89.185.224.68 (89-185-224-68...asterinter.net) 89.185.224.81 (89-185-224-81...asterinter.net) 89.185.224.71 (89-185-224-71...asterinter.net)





---

Dziękuję

[adrian.turowski@passus.com.pl](mailto:adrian.turowski@passus.com.pl)