

An Anomaly Tool Implementation in GEANT

– Part Three of Three

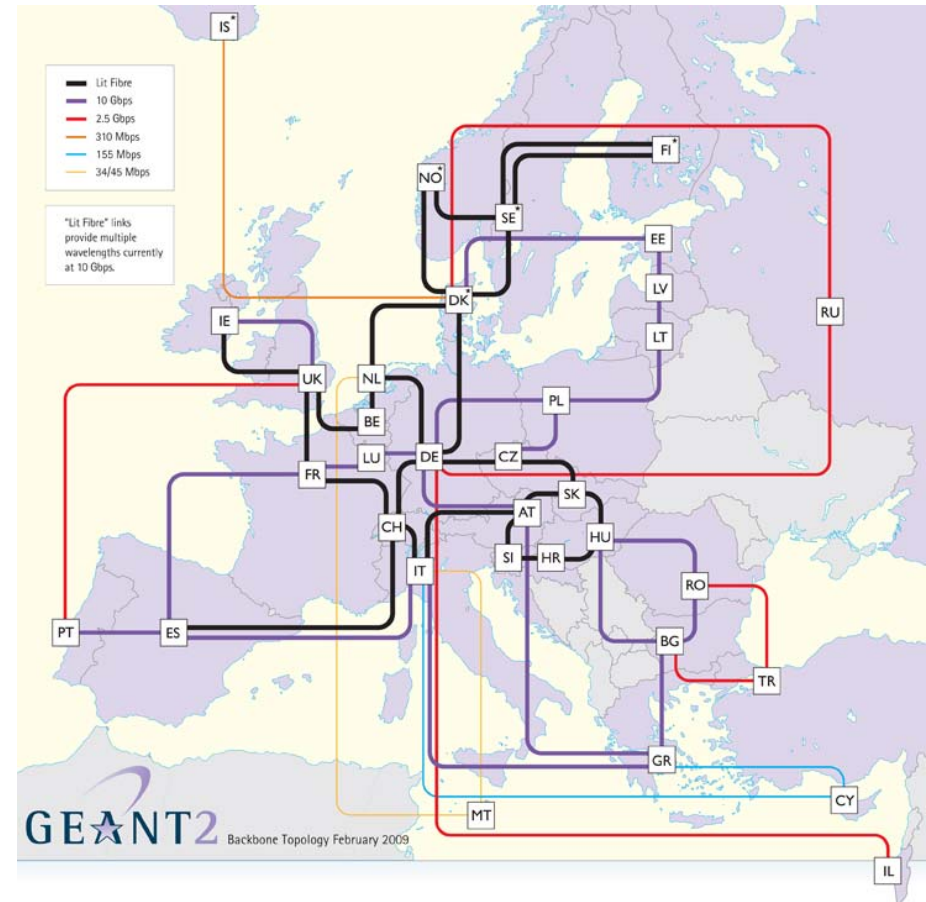
Wayne Routly, DANTE

TF-CSIRT, Leon; Spain, 18 May 2009

Anomaly Tool Testing in GEANT



- A History Of The Process
 - Confirming Anomalies
 - Testing Three Products
 - Analysing Results
- ...And The Winner Is !
- Sneak Peak Of Chosen Solution
- Where We Stand Now



A History Of The Process



- Using Nfsen & Internally Developed Database
- Discussed Collaboration with Various NREN CERTS (Vienna)
- Confirmed Presence of Anomalies in Geant network
- Entered into Trial with Three Industry Anomaly Detection Tools
- Analysed +1000 Unique Events Over Two Week Period
- Presented Results to TF-CSIRT (Riga) & APM Meeting (Cambridge)

...And The Winner Is...



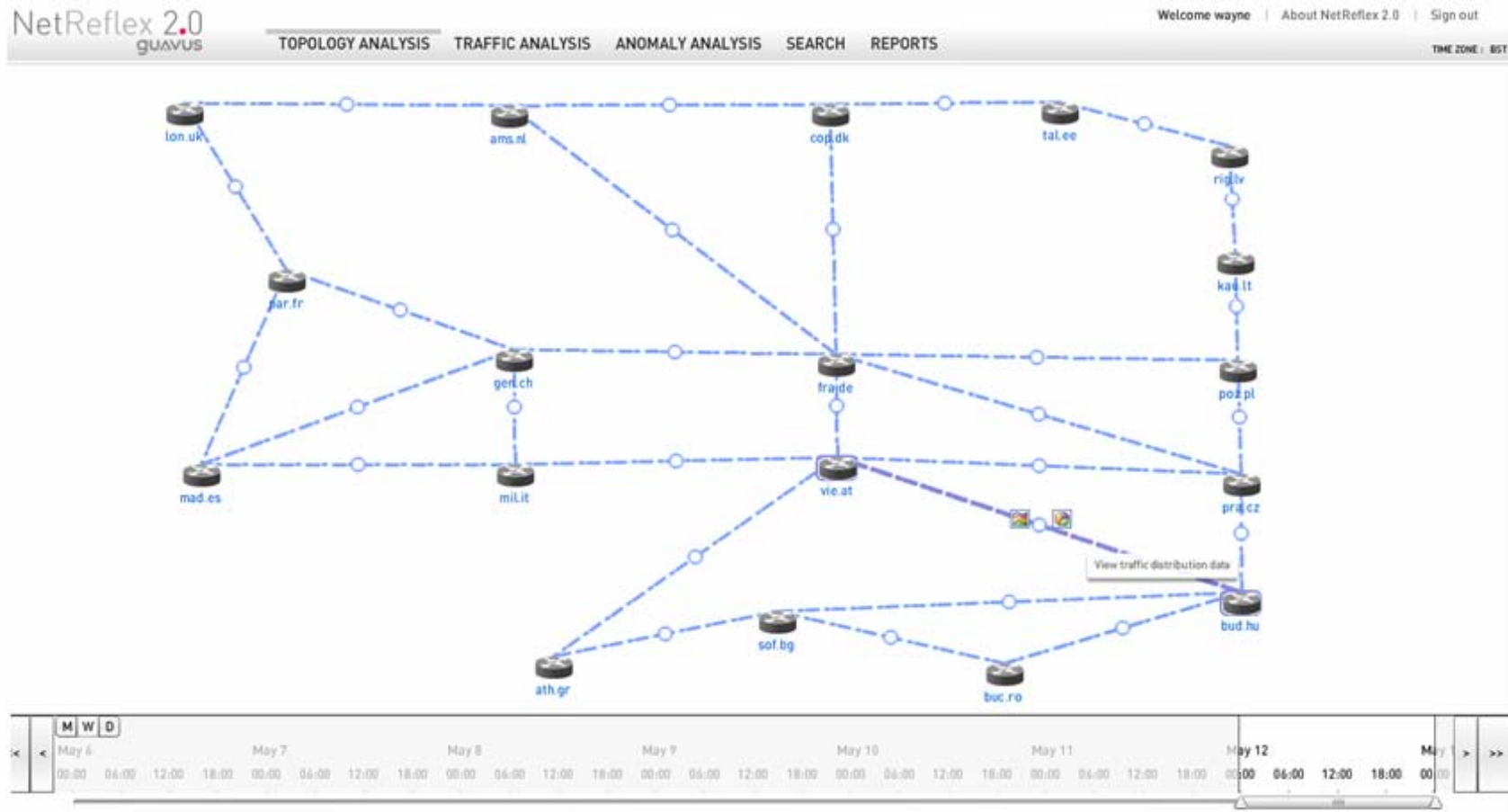
- Netreflex – Guavus
 - Fuses BGP & ISIS Data
 - Creates an 18 x 18 Router Matrix
 - 21.7 Anomalies per Day (True), 4.6 (False)
 - True False Ratio – 21%
 - Strengths Cover Scans & (D)Dos
 - Origin of Anomalies – Well Balanced NREN vs Non
- Tests Used 1/1000 Sampling
- Detected Anomalies In All Peers
- Higher Cross Section Of Detected Anomalies
- Changed to 1/100 Sampling

guavus

NetReflex 2.0

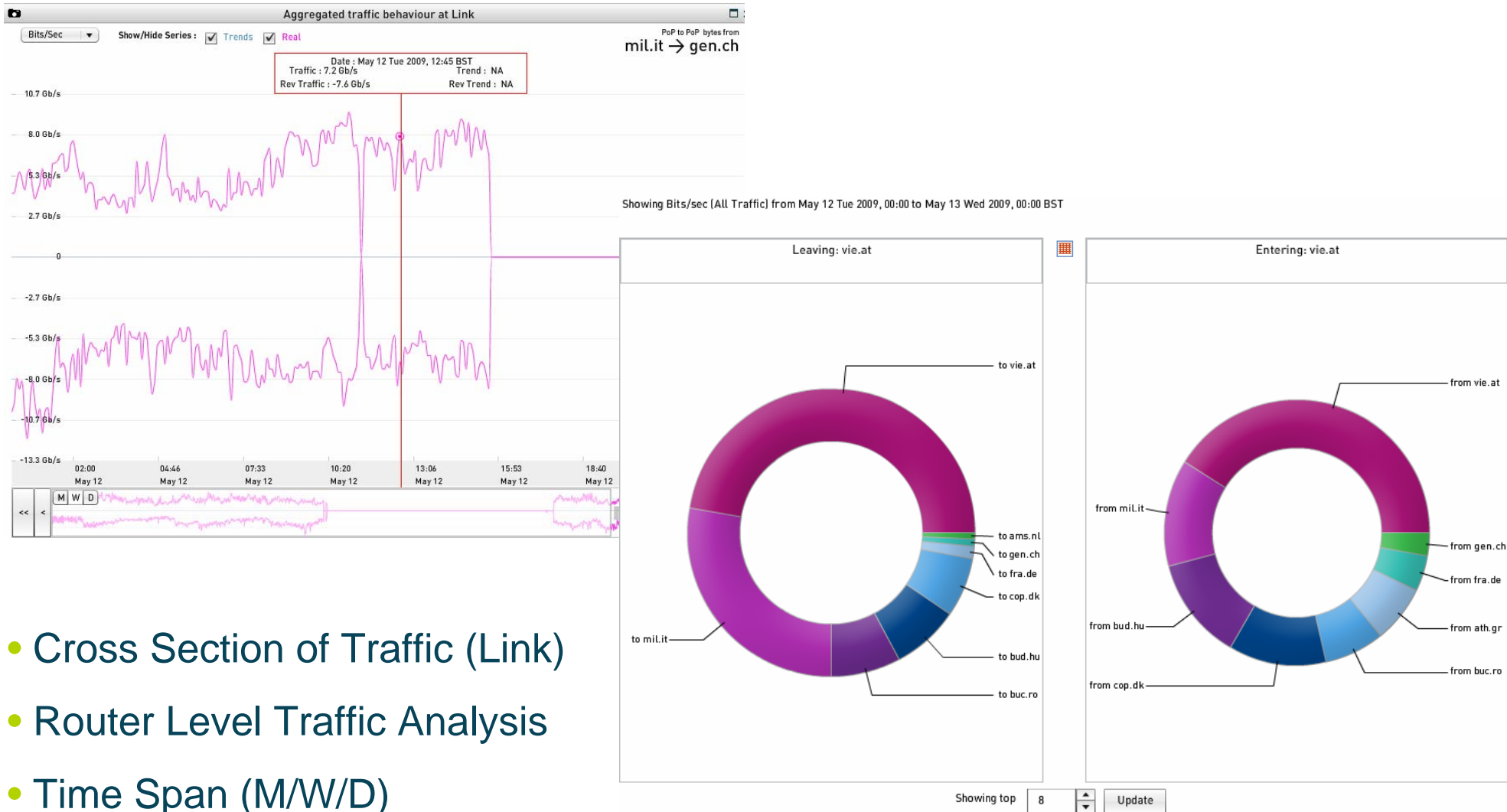


Topology Analysis



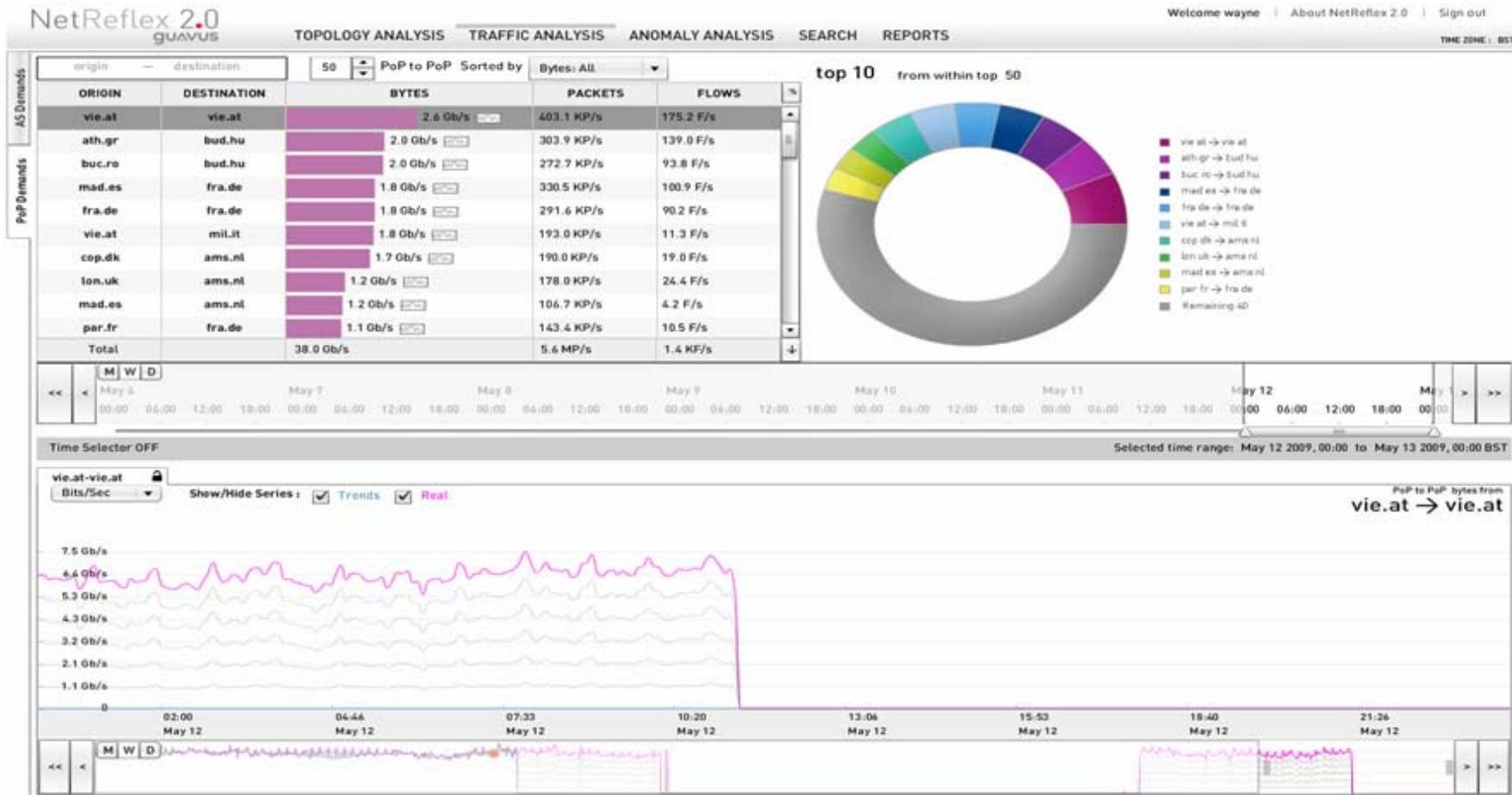
- Landing Page
- Heat Maps (in pipe line)

Topology Analysis...cont



- Cross Section of Traffic (Link)
- Router Level Traffic Analysis
- Time Span (M/W/D)

Traffic Analysis

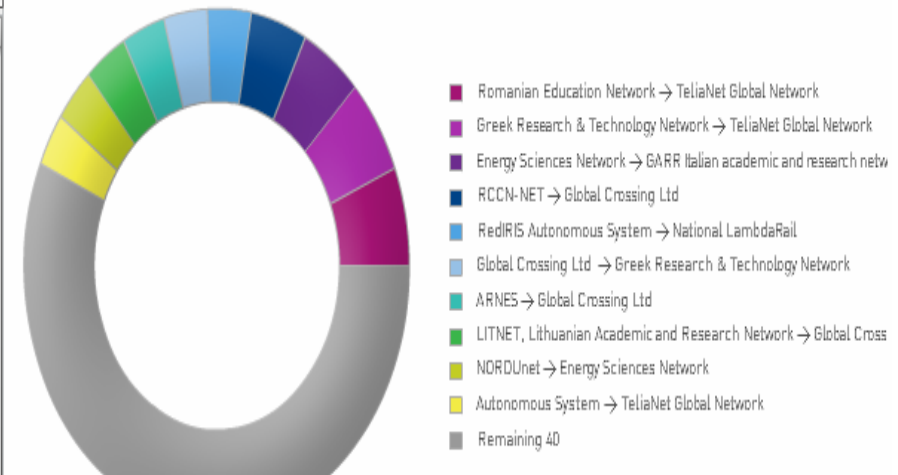


- Multiple Methods to View Data
- Clear Easy to Interpret Interface

Traffic Analysis

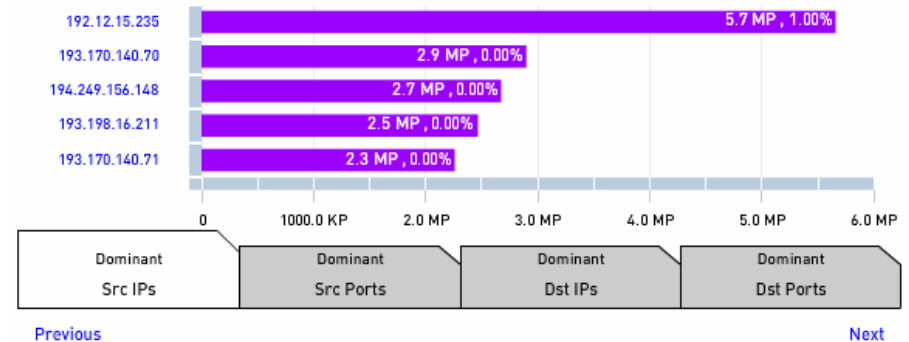
origin - destination		50	AS to AS	Sorted by	Bytes: All
ORIGIN	DESTINATION	BYTES	PACKETS	FLows	%
Romanian Educat...	TeliaNet Global N...	2.7 Gb/s	399.7 KP/s	153.9 F/s	
Greek Research ...	TeliaNet Global N...	2.7 Gb/s	423.0 KP/s	204.3 F/s	
Energy Sciences ...	GARR Italian acad...	2.3 Gb/s	250.1 KP/s	12.6 F/s	
RCCN-NET	Global Crossing L...	2.1 Gb/s	398.5 KP/s	157.0 F/s	
RedIRIS Autonom...	National Lambda...	1.6 Gb/s	141.2 KP/s	1.8 F/s	
Global Crossing L...	Greek Research ...	1.6 Gb/s	256.8 KP/s	132.2 F/s	
ARNES	Global Crossing L...	1.6 Gb/s	200.6 KP/s	90.9 F/s	
LITNET, Lithuania...	Global Crossing L...	1.6 Gb/s	301.7 KP/s	105.4 F/s	
NORDUnet	Energy Sciences ...	1.5 Gb/s	130.0 KP/s	1.6 F/s	
Autonomous Syst...	TeliaNet Global N...	1.5 Gb/s	241.3 KP/s	72.4 F/s	
Total		44.2 Gb/s	6.5 MP/s	2.0 KF/s	

top 10 from within top 50



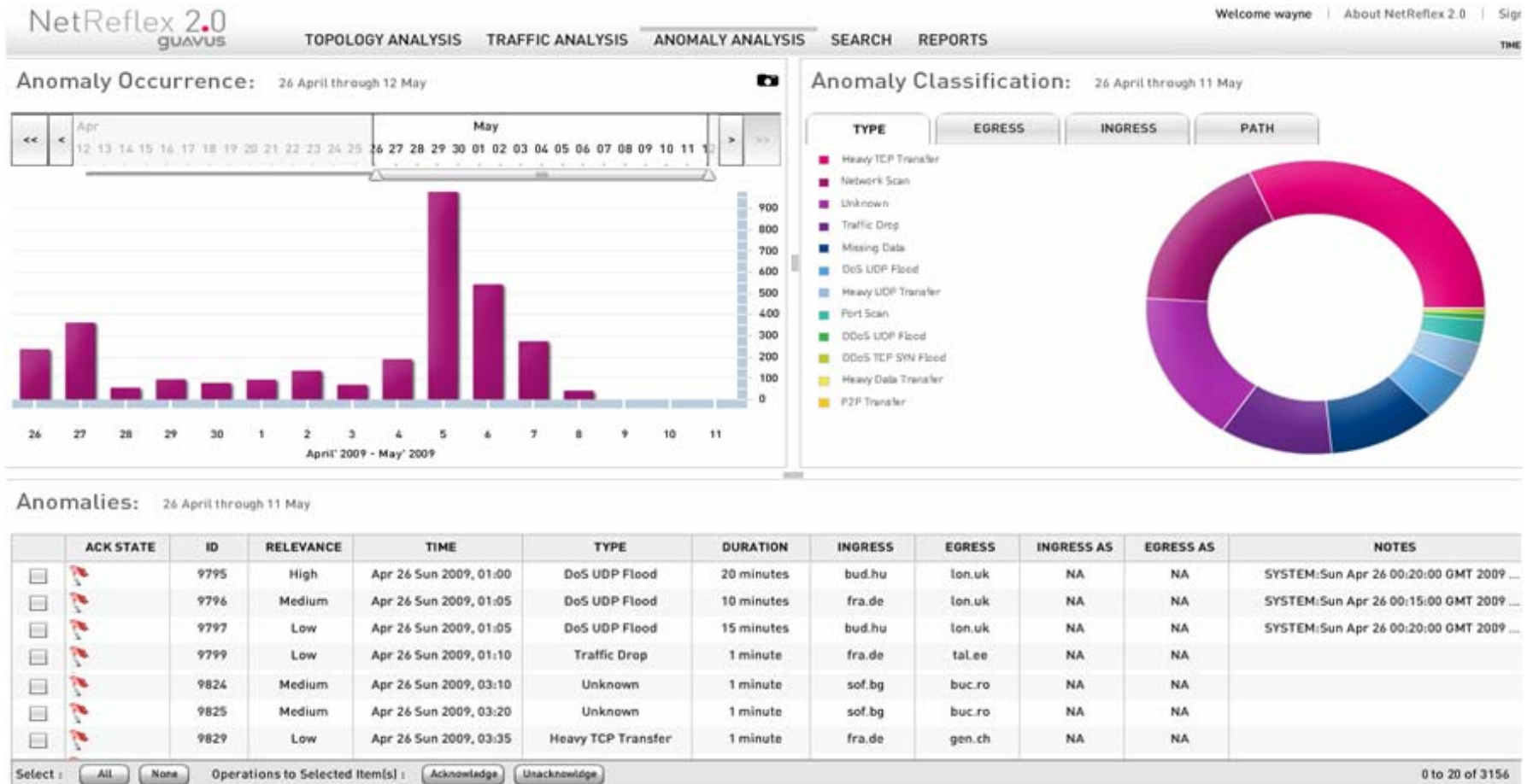
Traffic Details

Traffic details between Vie.at and Vie.at on May 12 Tue 2009, 09:45 BST



- Filter Per POP OD / AS OD
- Drill Down Capability IP / Ports
- Time Span (M/W/D)
- Traffic Planning Possibilities

Anomaly Analysis



- Anomaly Interface / Alerts
- Per Ingress / Egress / Type / Path

Anomaly Analysis

- Highlight Anomaly Per Type / OD
- Acknowledge Event
- Add Notes
- View SRC / DST / Ports
- Associated Points
- Look at Preceding / Post Times

Acknowledge

Time :
May 08 Fri 2009, 00:15

Type :
Network Scan

Duration :
85 minutes.

Note :
SYSTEM:Fri May 08 00:40:00 GMT 2009: Duration changed to 85 minutes.. Fusion-count changed to 7.
SYSTEM:Fri May 08 00:35:00 GMT 2009: Duration changed to 80 minutes.. Fusion-count changed to 6.
Add your note here...

Append to Notes:

PoP Path :
poz.pl → lon.uk

AS Path :
NA → NA

Evidence :

Anomalous in :

- Distribution

Dominants :

- Source IP : 212.33.91.56
- Destination Port : 1433
- Protocol : TCP

Unique Occurrence :

- Destination IP : 744

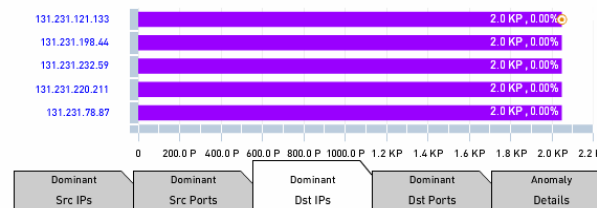
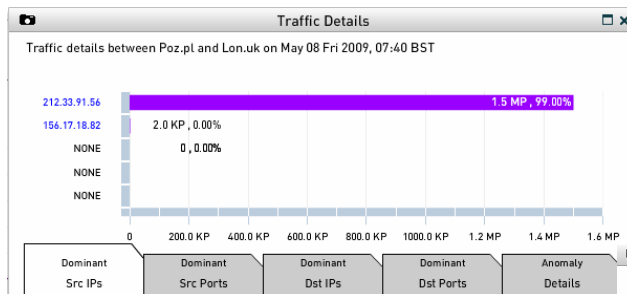
Source AS : NA

PoP to PoP ip-flows from poz.pl → lon.uk

Packets
IP-Flows
Bytes

Flows/Sec
Show/Hide Series: Trends Real





Conclusion (Not a TBC 😊)

- Started Down Long Road Of Tool Testing
- Sifted Through Hundreds of Results (Forest For The Trees)
- Presented Results To Community
- Chose Solution (Easier Than Said)
- Working Towards Final Implementation
- Work With NREN Partners To Facilitate A Secure GEANT

Questions ?



THANK-YOU!

wayne.routly@dante.net

