

Anomaly Detection in Backbone Networks: Building A Security Service Upon An Innovative Tool

Wayne Routly, Maurizio Molina - (DANTE)

Ignasi Paredes-Oliva - Universitat Politècnica de Catalunya (UPC)

Ashish Jain - (Guavus)

TNC, Vilnius, 2nd June 2010

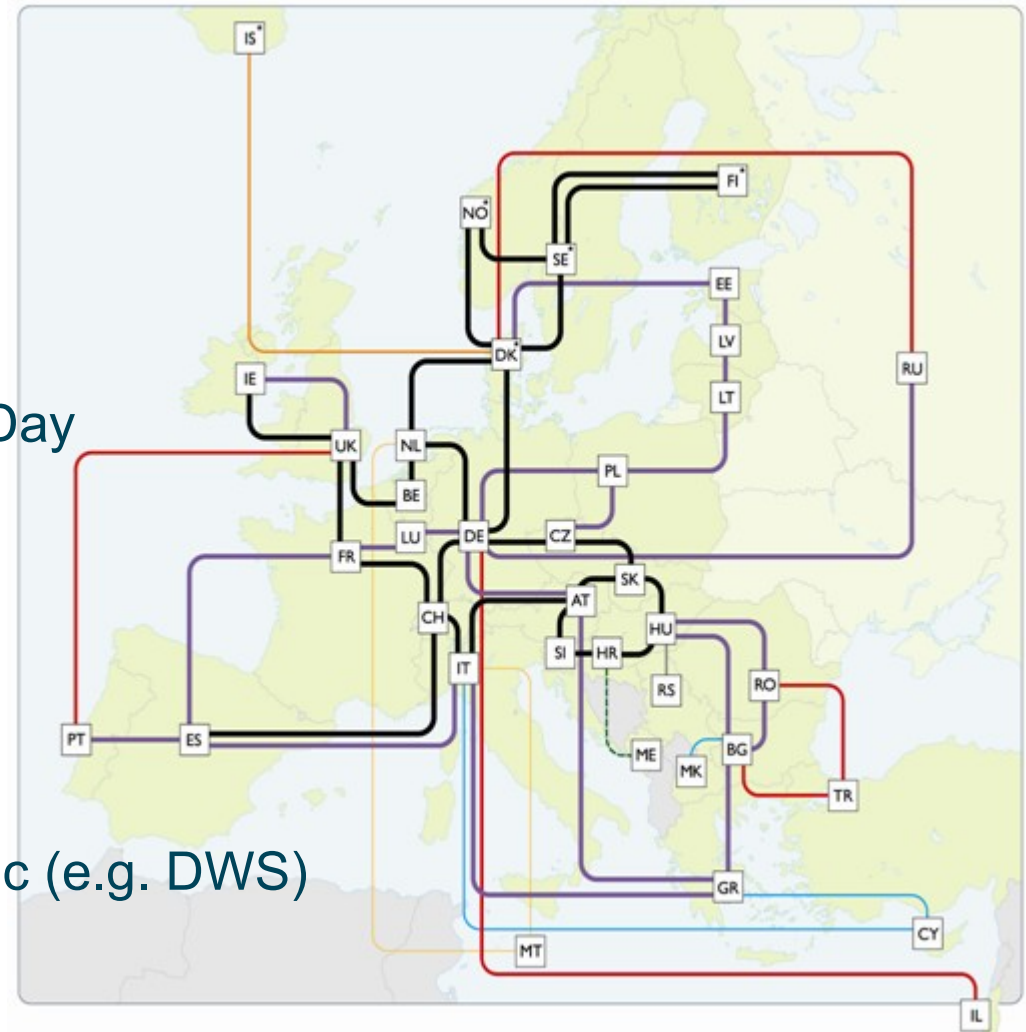
Content

- Introduction: The network and the service scenario
- The Tools
 - The benchmarking process
 - Deployment and initial usage of the selected tool
 - Some recent enhancements (Apriori)
- Network Security Service
 - The Objectives
 - The Service Details
 - Current Status
 - Event Workflow
- Conclusion

The Network Scenario



- A Transit Network with Global Visibility
- Up to 60 Gbit/s in peak times
- +/- 10 Million Speaking Hosts Per Day
- Unusual “research” Traffic
 - Large FTP Transfers
 - SSH Traffic
 - Grid Traffic
 - Bandwidth Testing Traffic
- Mixed with “ordinary” Internet Traffic (e.g. DWS)



1- Periodic Summary Reporting

- Observe global security anomalies trends at the GÉANT “boundary”
 - What are the most common attack types?
 - What the potentially more harmful?
 - Are some Networks heavy security anomalies sources or targets?
 - Why? Can something be done about it?

2- Punctual Anomaly Notification

- Specific events can be reported to NREN CERTs...
 - ...that the NREN may not have noted due to lack of monitoring...
 - ...or noted but lacking metadata for root cause analysis

Pre-requisite: anomaly detectability in GÉANT backbone



- Both service elements require anomaly “detectability” in the GÉANT backbone
 - With Sampled NetFlow only => no dedicated probes!
- Already proved with NfSen plugins (Molina: TNC 08)
- Decision to look at commercial tools for:
 - Support
 - Quick evolution to detecting new threats
 - Anomaly origin/destination analysis

The benchmarked tools

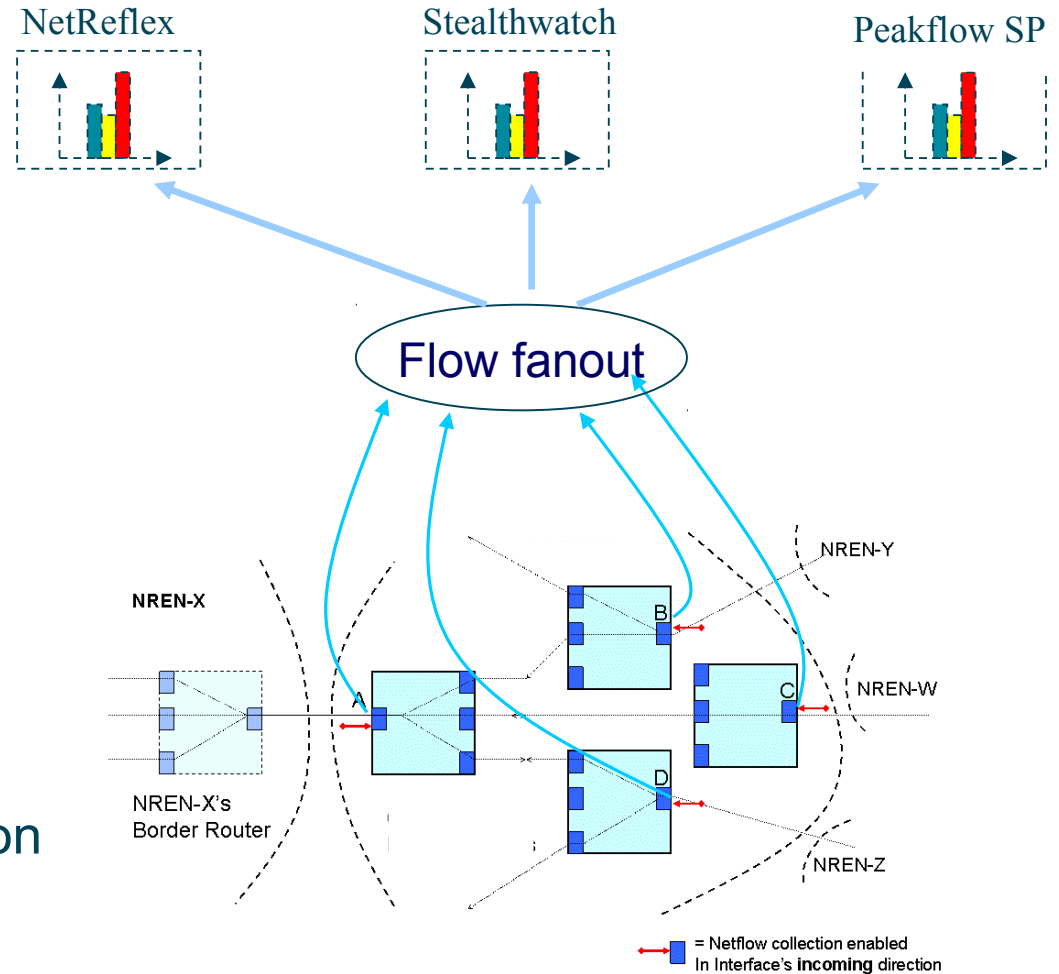


- Three Distinct Tools
 - Netreflex – Guavus
 - Fuses BGP & ISIS Data
 - Creates an 18 x 18 Router Matrix
 - Peakflow SP – Arbor
 - Uses BGP & SNMP Data
 - Originally designed to pick large scale (D)DoS attacks
 - Stealthwatch – Lancope
 - Per Host Behavioural Analysis
 - Requires 1 anomaly end point to be part of prefix list

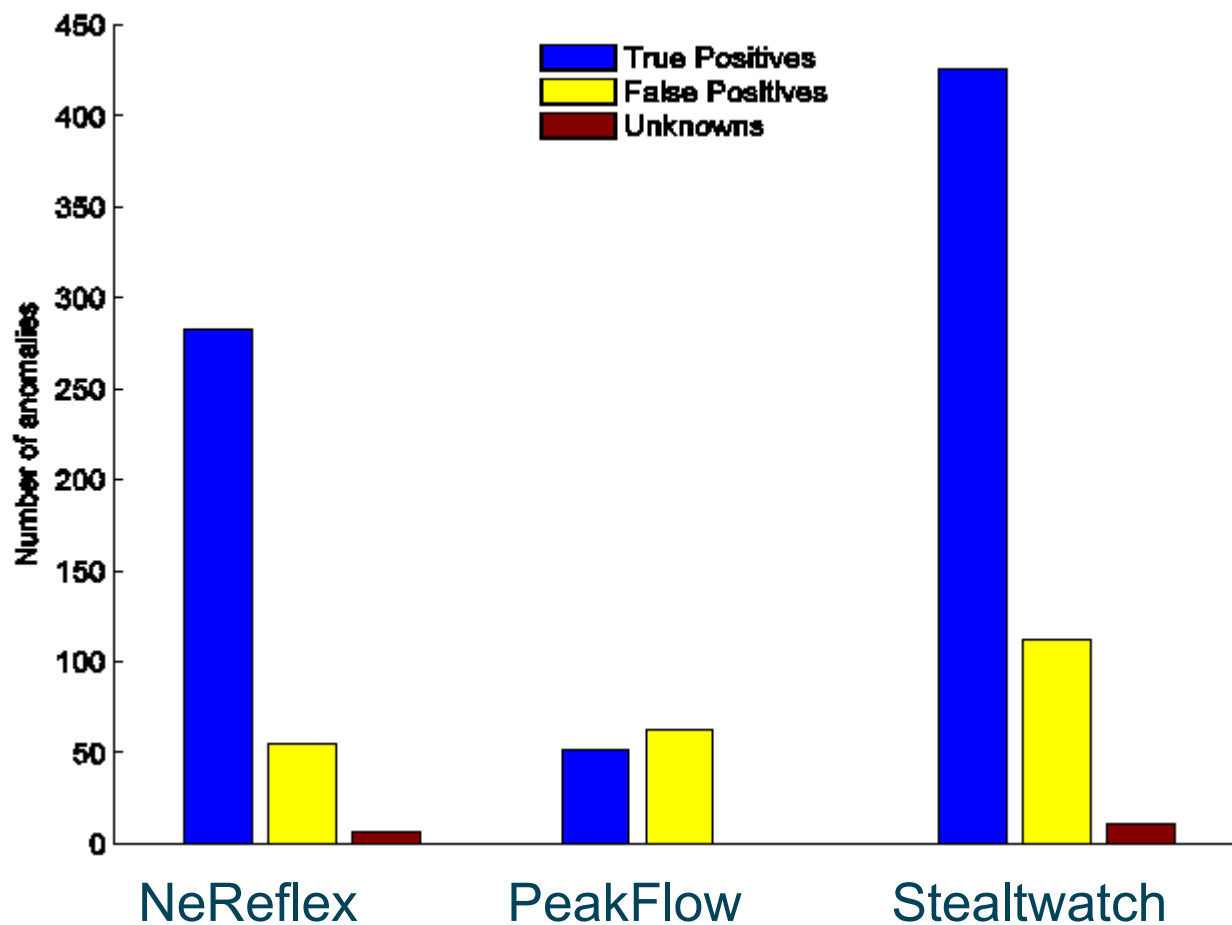
The benchmarking process



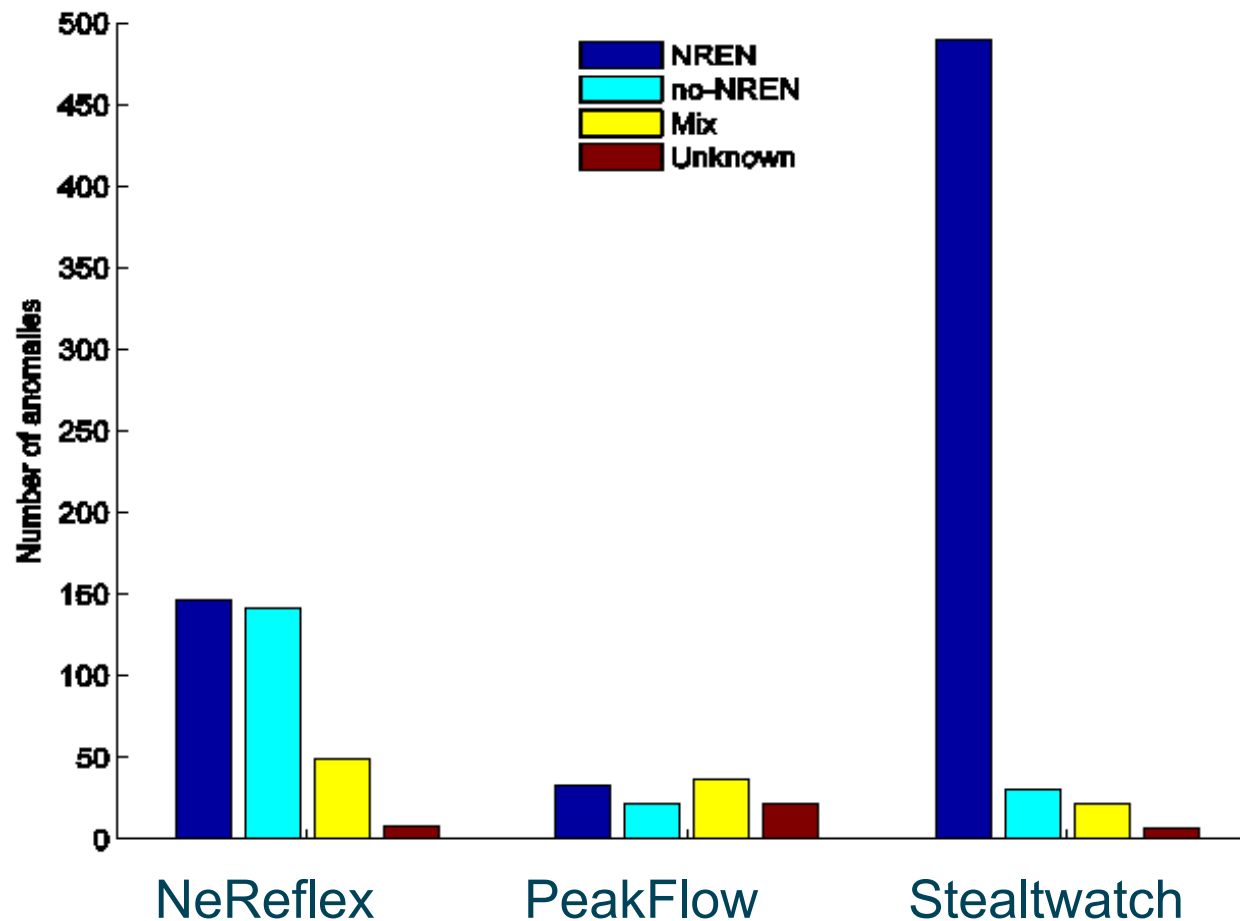
- Same data fed to tools
 - 13 days of cross comparison
 - 1066 anomalies in total
- Each anomaly
 - Cross checked with NfSen and raw NetFlow
 - Classified as True or False positive
- Some events forwarded to CERTs for further Confirmation & Discussion



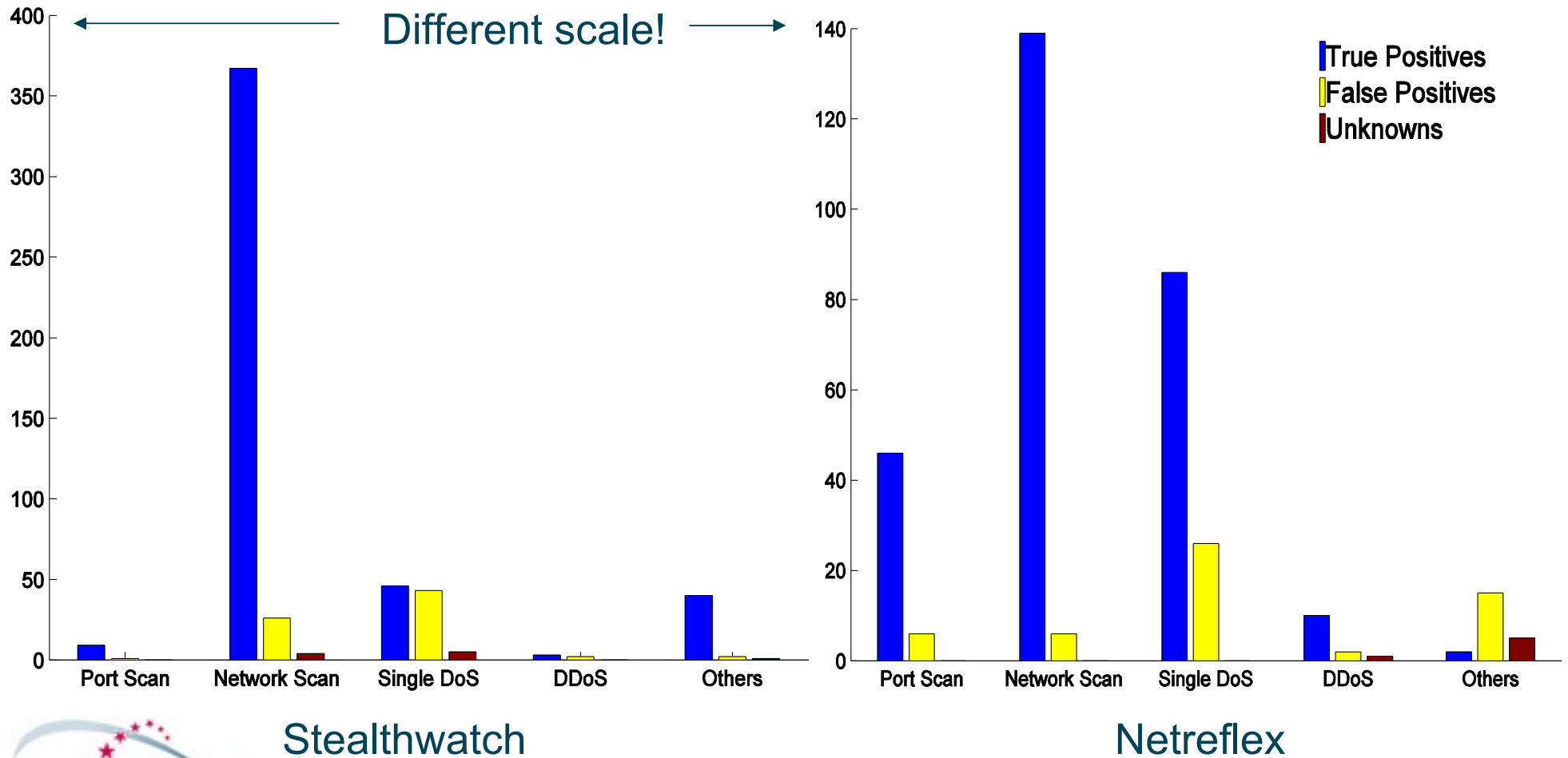
The benchmarking results: True and False Positives



The benchmarking results: source of anomalies



NetReflex vs Stealthwatch: more details



Tool Selection - Netreflex



- Chose Netreflex as the Tool for anomaly detection
- More uniform detection of Anomalies across Types
- More uniform detection across Geant Peers
- Higher Cross Section Of Detected Anomalies
- Strengths Cover Scans & (D)Dos
- Origin of Anomalies – Well Balanced NREN vs Non



Deployment and Initial Usage of NetReflex



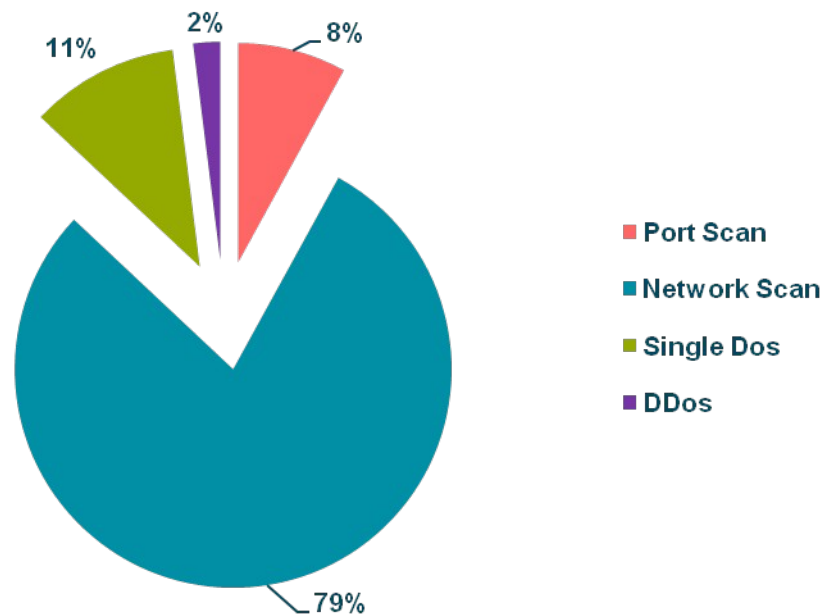
- NetFlow is now 1/100 sampled (was 1/1,000 during trials)
 - Better detection
 - Lower false positives (below 8%)
- Anomalies can be exported via e-mail
 - Anomaly database created
 - Statistics & Reports Generated for Analysis
- Netreflex v2.5 Deployed in Production Environment
 - Advanced Filtering Capabilities in Anomaly Analysis
 - Updated Reporting

Early Results – Anomaly Distribution



- Network Scans 79%
- DDos only 2%
- Network Scans a Precursor
- 40% of Network Scans from Global Connectivity Providers
- Network Scan SRC IP's traced to Port Scans & Dos Events

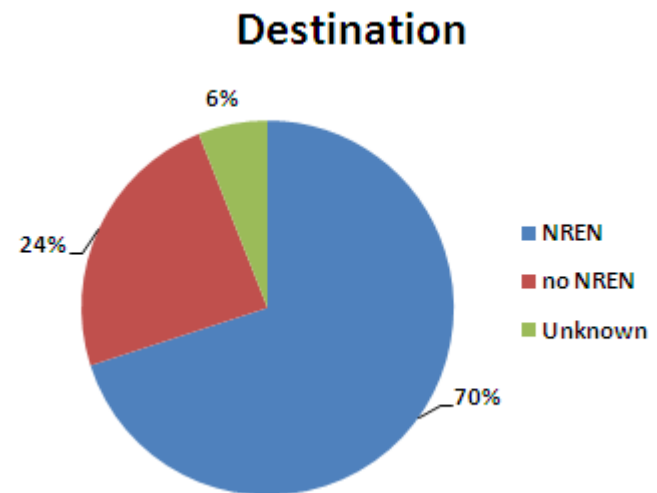
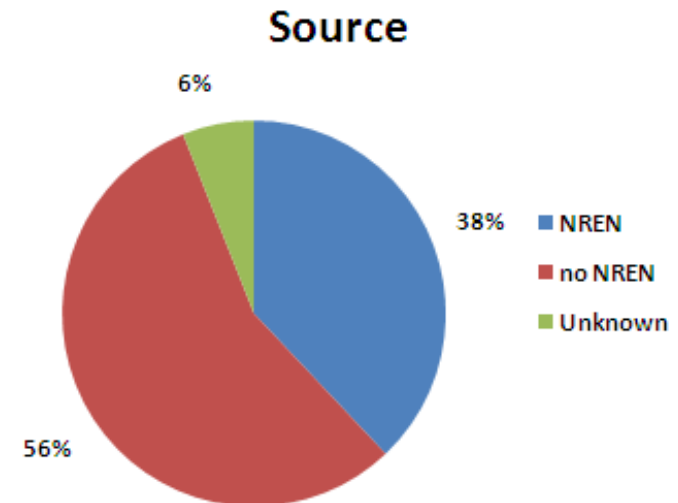
Anomaly Distribution



Early Results – Source & Destination Grouping



- NRENs target of attacks at 70%
- 56% of Events originating outside of GN
- 38% of Events originating from NRENs
 - NREN to no NREN accounts for 21%
 - NREN to NREN 17%
- 25% of Countries & Regions account for 77% of Attacks

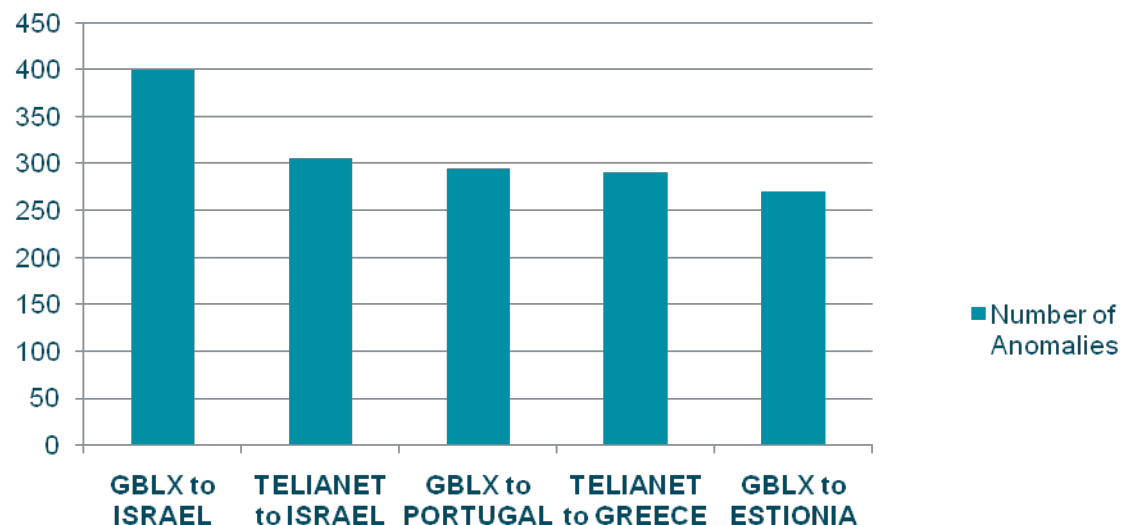


Early Results, AS Pairs for Anomaly Distribution



- Global Connectivity Providers
- Greece & Portugal?
- Israel & Estonia
- Small networks appear high in the list of targets: why?

Number of Anomalies

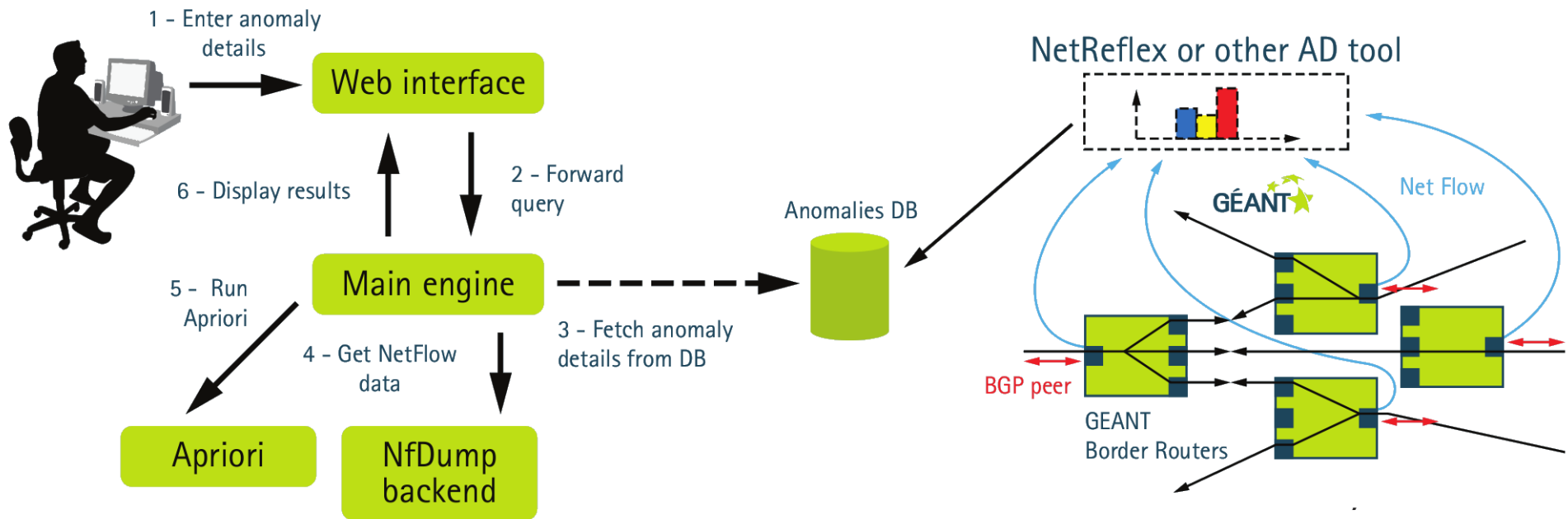


A (research) enhancement: apriori



- The *manual* validation of 1000+ anomalies via NetFlow record inspection stimulated us to explore *automatic* approaches
- “Apriori”: algorithm adapted from market basket analysis to find association rules (*)
 - “If customer buys item X, what is he likely to buy as well?”
- Analogy: if a flow is involved in an anomaly, what other “similar” flows may be involved?
- We refined the original algorithm and implemented a GUI

Apriori for mining anomalies: GUI



Anomaly Investigation

Anomaly detection

Apriori for mining anomalies: one example



The Anomaly detection tool detected this port scan

| | Source IP | Destination IP | Source Port | Destination Port |
|-----------|-------------|----------------|-------------|------------------|
| Portscans | .191.64.165 | .13.137.129 | 55548 | * |
| | .191.26.33 | .13.137.129 | 39573 | * |
| DDoS | * | .13.137.129 | 3072 | 80 |
| | * | .13.137.129 | 1024 | 80 |

Apriori revealed another port scan can on the same target, and a DDoS as well

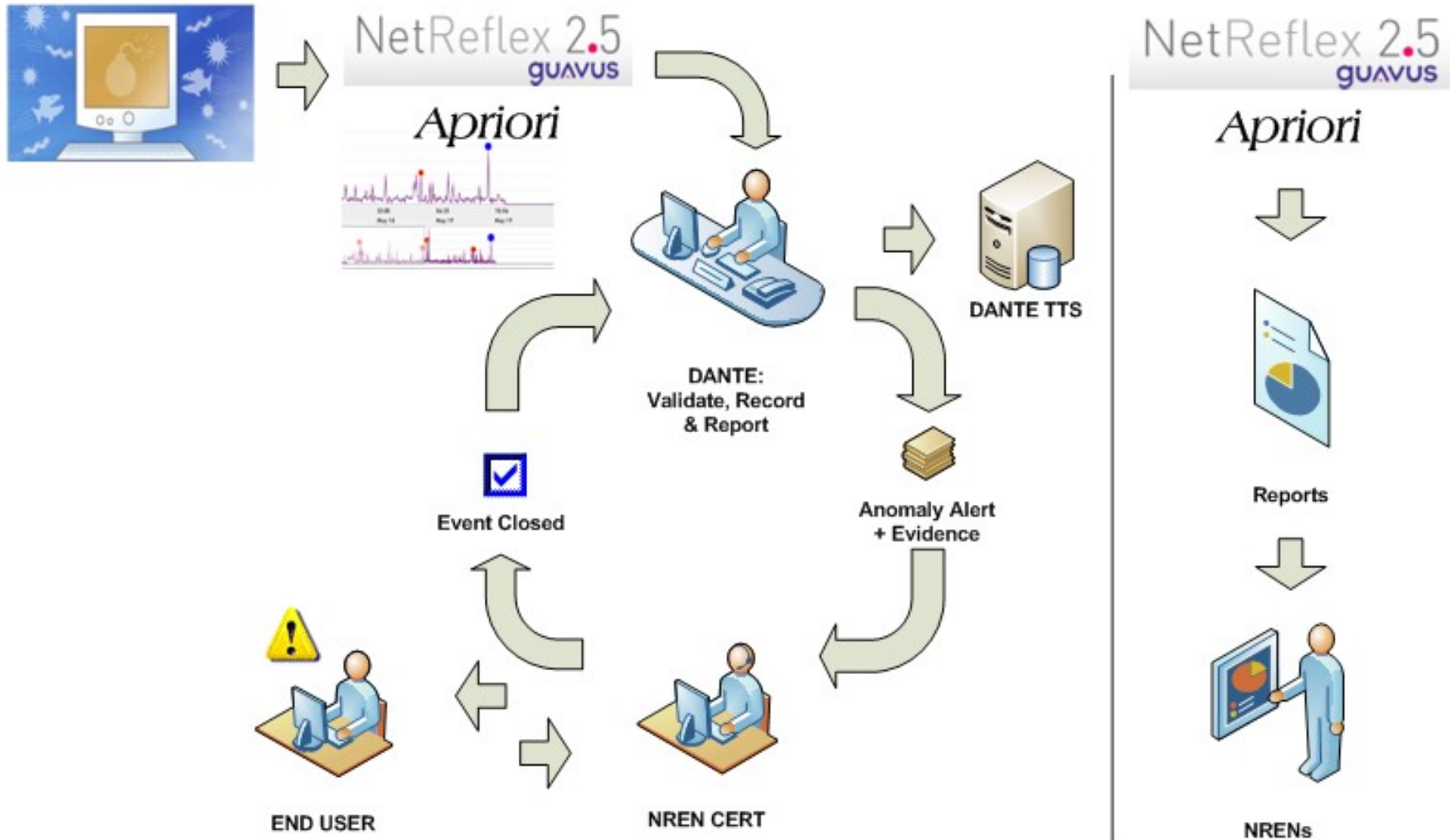
Network Security Service – The Objectives



The NSS is a service that will enhance backbone security and will extend the NRENs ability to protect their infrastructure.

- ... thereby assisting in reducing the network impact of security events on their networks
- ... provide additional security incident response to NRENs to extend to their customers
- ... and prevent attacks against the GN infrastructure thereby providing a safer GN network

Network Security Service – Event Workflow



Network Security Service – The Service Details



● Protect GEANT Infrastructure

- Identify Threats
- Identify Targets & Sources
- Identify Affected Peering's

● Protect NREN Access to the Backbone

- Collaborate with NRENs to mitigate threats affecting them
- Provide NREN's with additional network visibility
- Assist less advanced NREN's with security event notifications
- Provide reports on security events affecting NREN

Network Security Service – Current Status



- **Phase 1 – Anomaly Detection Toolset Deployment,**
 - Selection & Tool Tuning
 - Further Analysis & Reduction of FP rate
 - Findings widely reported to community; TF-CSIRT; FIRST;
- **Phase 2 - NREN Security Event reporting**
 - Reporting Security Events to NRENs
 - Provide event evidence with notifications
 - Collaborate with NREN's on events.
 - Increase level of security monitoring for NREN's

Conclusion



- Proven detectability of Security Events in the Backbone Network
- Extensive Tool Comparison Trial
- Reduction in FP Ratio of Anomalies in Netreflex
- Automatic Anomaly Validation
- Network Security Service
 - Provide NREN's with Additional Visibility
 - Provide Security Event Notification and Reporting
- Phase Two of Deployment
 - Targeted NREN Alerts
 - Closer Security Interaction & Collaboration

Acknowledgements



Daniela Brauckhoff & Xenofontas Dimitropoulos (ETH Zurich) for sharing their implementation of Apriori

Domenico Vicinanza & Mariapaolo Sorrentino (DANTE) for the discussion on bandwidth test tools



Thank-You

wayne.routly@dante.net