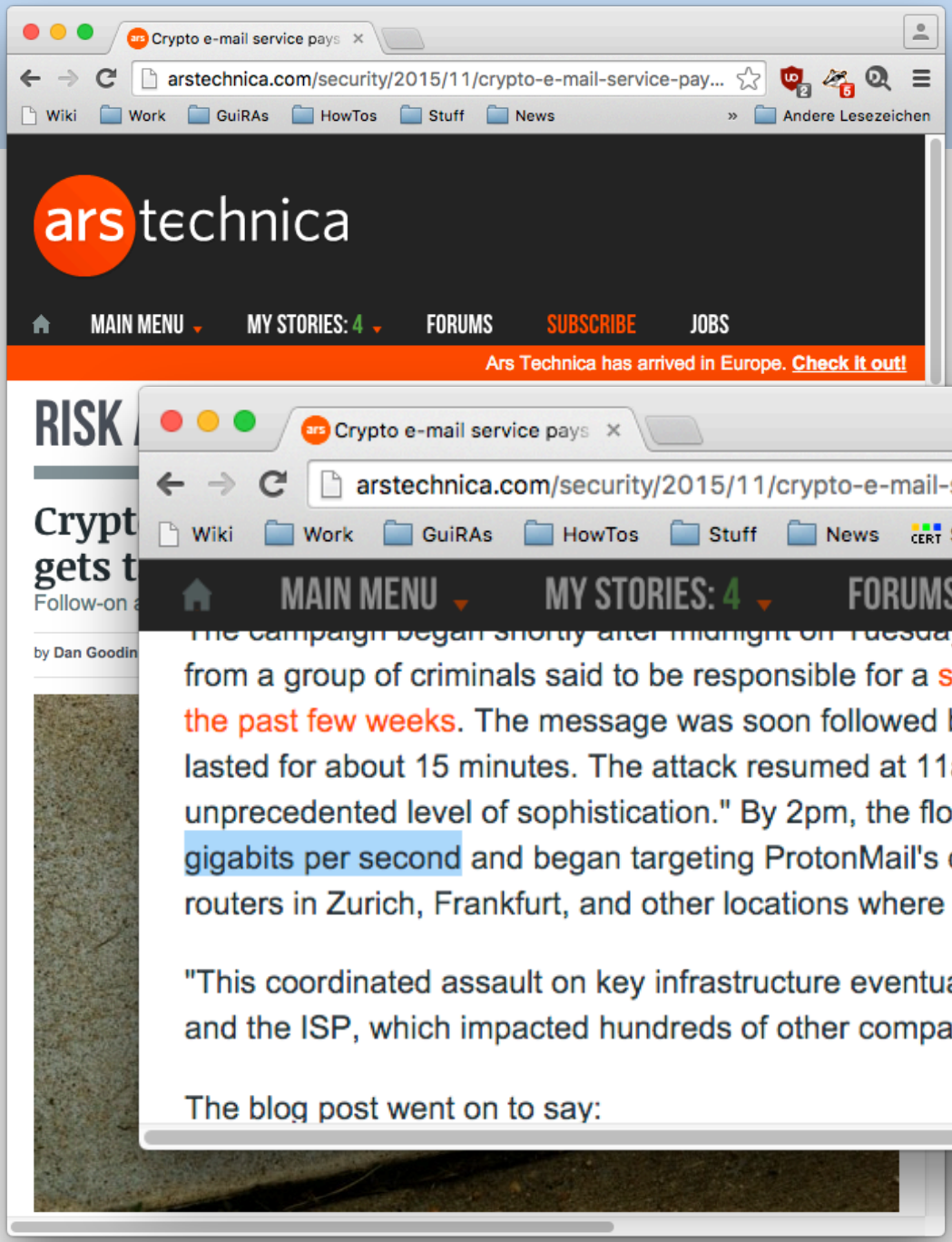
Deutsches Forschungsnetz

DDoS mitigation in DFN's service portfolio

Dr. Ralf Gröper

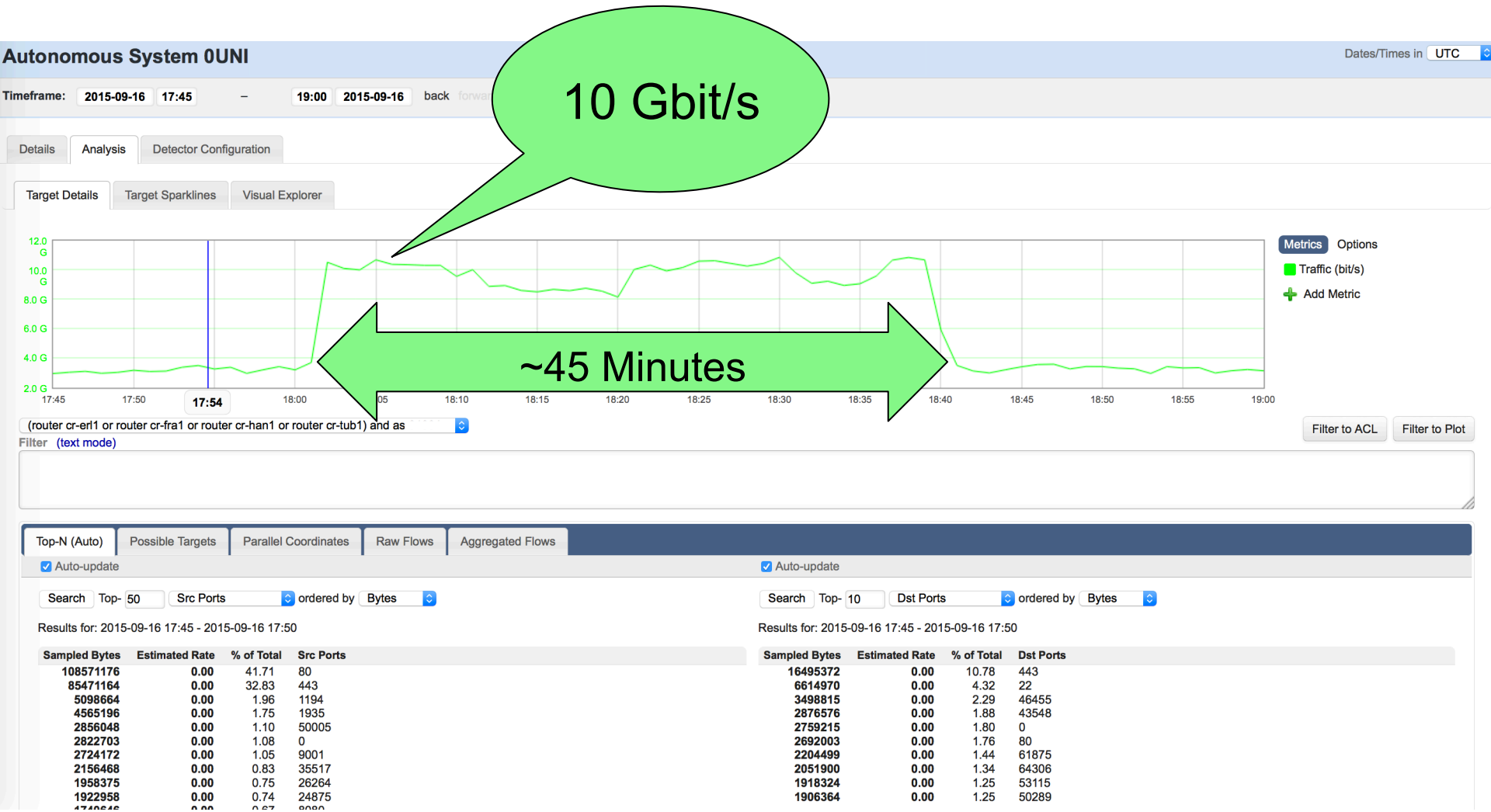
DDoS Mitigation in the NREN Environment Workshop

November 11, 2015


Crypto e-mail service pays
arstechnica.com/security/2015/11/crypto-e-mail-service-pay...
Wiki
Work
GuiRAs
HowTos
Stuff
News
Andere Lesezeichen
ars technica
MAIN MENU
MY STORIES: 4
FORUMS
SUBSCRIBE
JOBS
Ars Technica has arrived in Europe. Check it out!
RISK
Crypt
gets t
Follow-on
by Dan Goodin

Crypto e-mail service pays
arstechnica.com/security/2015/11/crypto-e-mail-service-pays-6000-ransom-ge...
Wiki
Work
GuiRAs
HowTos
Stuff
News
Schwachstellen - DF
Andere Lesezeichen
MAIN MENU
MY STORIES: 4
FORUMS
SUBSCRIBE
JOBS
from a group of criminals said to be responsible for a string of DDoS attacks across Switzerland over the past few weeks. The message was soon followed by a distributed denial-of-service attack that lasted for about 15 minutes. The attack resumed at 11am the same day and was already showing "an unprecedented level of sophistication." By 2pm, the flood of junk traffic reached volumes of 100 gigabits per second and began targeting ProtonMail's datacenter and upstream providers, including routers in Zurich, Frankfurt, and other locations where the ISP has nodes.
"This coordinated assault on key infrastructure eventually managed to bring down both the datacenter and the ISP, which impacted hundreds of other companies, not just ProtonMail."
The blog post went on to say:

Real-World Example in DFN



DDoS-Attacks in DFN

- Small and Medium Attacks all of the time...
  - ...we usually don‘t know who and why and
  - ...attacks are too weak to cause any harm, only visible in monitoring

- G7-Summit 2015 in Bavaria
  - No actual attacks, but Germany‘s Federal Office for Information Security issued a warning to federal organisations
  - 4 organisations that are part of DFN asked in advance for additioal support in case of attacks

- Increasing number of successful attacks that actually cause harm
  - Mitigation by DFN users only possible if access line, local router and/or local firewall not overloaded
  - Otherwise mitigation is only possible within DFN‘s X-WiN network

Current approach to mitigation

- Protection of DFN‘s infrastructure
  - Detect and analyse attack using monitoring tools (especially NeMo)
  - Manual configuration of routers (null-routes, rate-limits)
  - Manual monitoring of attack
  - Manuel re-configuration of routers after attack ended
- Protection of user‘s infrastructure
  - No formalised processes
  - Lots of legal limitations of what we are allowed to do!

DDoS-Attacks in DFN

- Lessons learned:
  - lots of manual actions necessary
  - granularity of filtering is limited
  - complex organisational and legal questions
  - Commercial solutions are somewhat costly...

- Conclusion:
  - Dedicated DDoS-mitigation solution in X-WiN is necessary
  - We‘re almost there already!
    - NeMo can already identify and analyse DDoS-Attacks
    - Mitigation direclty on our core routers possible by newly introduced prduct by Cisco
  - Development of technical platform completed until end of 2015, launch as a service in 2016

Two Scenarios

DFN Deutsches Forschungsnetz

- Scenario 1: DFN protects its own infrastructure
  - Step 1: Implement a DDoS-mitigation platform
  - Step 2: Mitigate Attacks

Easy ☺

- Scenario 2: DFN protects user‘s infrastructure by mitigation before traffic reaches user
  - Step 1: Implement a DDoS-mitigation platform
  - Step 2: ...uh... (to be continued in this talk)

Difficult ☹

Step 1

IMPLEMENTING A DDOS-MITIGATION PLATFORM AT DFN

NeMo – Netzwerk Monitoring

- Objectives of NeMo (currently)
  - Detection of anomalies in data traffic in core network (X-WiN)
  - Notification of detected anomalies
  - Analysis of anomalies
  - Preparation of countermeasures if anomaly is classified as attack

DDoS-Abwehrkomponente

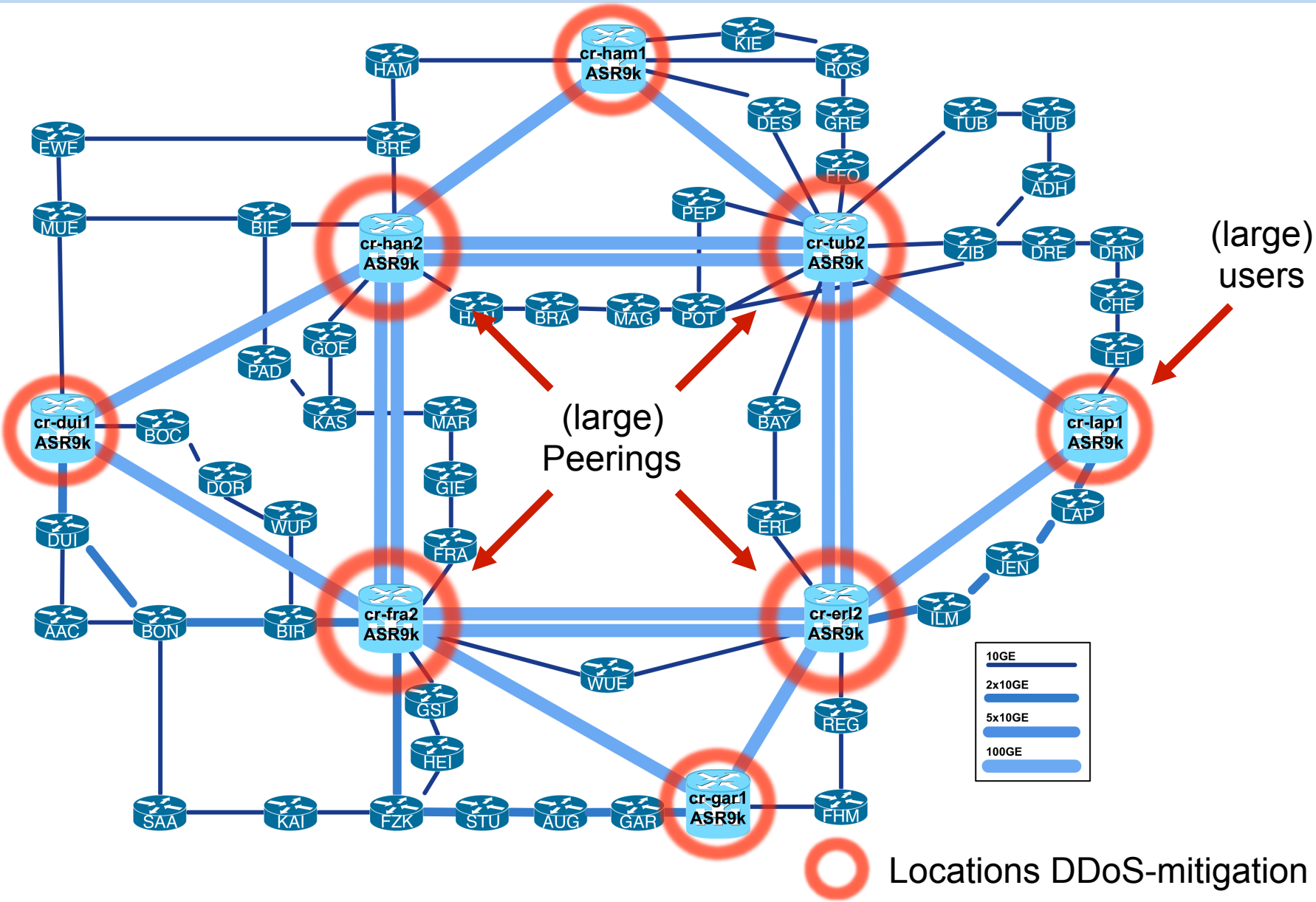
- New Objective of NeMo: Control of mitigation components
- Mitigation components have to be developed (in house):

NADA

Netzwerkbasierte Abwehr von DDoS-Angriffen

(Network-based defence against DDoS-Attacks)

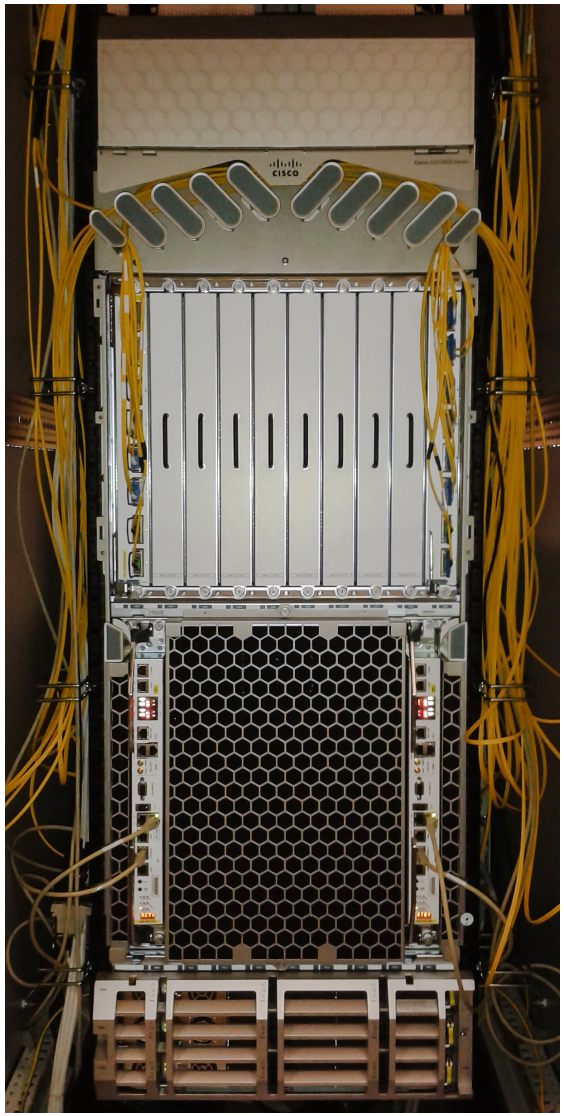
Ort der DDoS-Mitigation



CISCO Virtualized Services Module

CISCO VSM

+



Supercore router (Cisco ASR 9k)

Technische Umsetzung

DFN Deutsches Forschungsnetz

- Cisco Virtualized Services Module (VSM)
  - Blade-Server in SuperCore-Router
    - 4x 10 Core Intel Xeon, 128 GB RAM
  - Connected directly to router backplane
    - in total 120 Gbit/s throughput
  - Integrated hypervisor
    - Allows for deployment of own virtual machines
- DFN-CERT develops virtual machines with firewall features for VSM
- Filtering rules in two steps
  - Coarse filtering: Which traffic to route through VSM?
    - + null routes and/or rate limits
  - Fine filtering: Which traffic to filter in VSM?
- Contol of the whole system through NeMo

Step 2

INTRODUCING A DDOS-MITIGATION SERVICE FOR DFN‘S USERS

Challenges

- Potentially high capacities of attack traffic
- Fast activation
- Controlled and accountable procedure (who does what when?)
- Easy deployment (prevention of misconfiguration)
- Organised removal of mitigation measures (measures are always only temporary)

Organisational Aspects

- Who‘s autorised to authorise mitigation?
  - And how do we authenticate that person?
    - Signed E-Mail?
    - Callback on pre-approved phone numer*?
  - Not possibe in case of DDoS!

- Who‘s authorised to authorise suspension of mitigation?

- What‘s the contractual basis of restricting network access of a whole institution?

*) Lots of users use VoIP...

Legal aspects

- Ciminal law (§206 StGB, secrecy of telecommunications)
  - States not only that we must not look into communications, but also that we must not suppress communications

- Data protection laws/regulation
  - IP addresses are considered „personal data“ by default, may thus not be communicated to third parties without legal basis

Approach (under discussion)

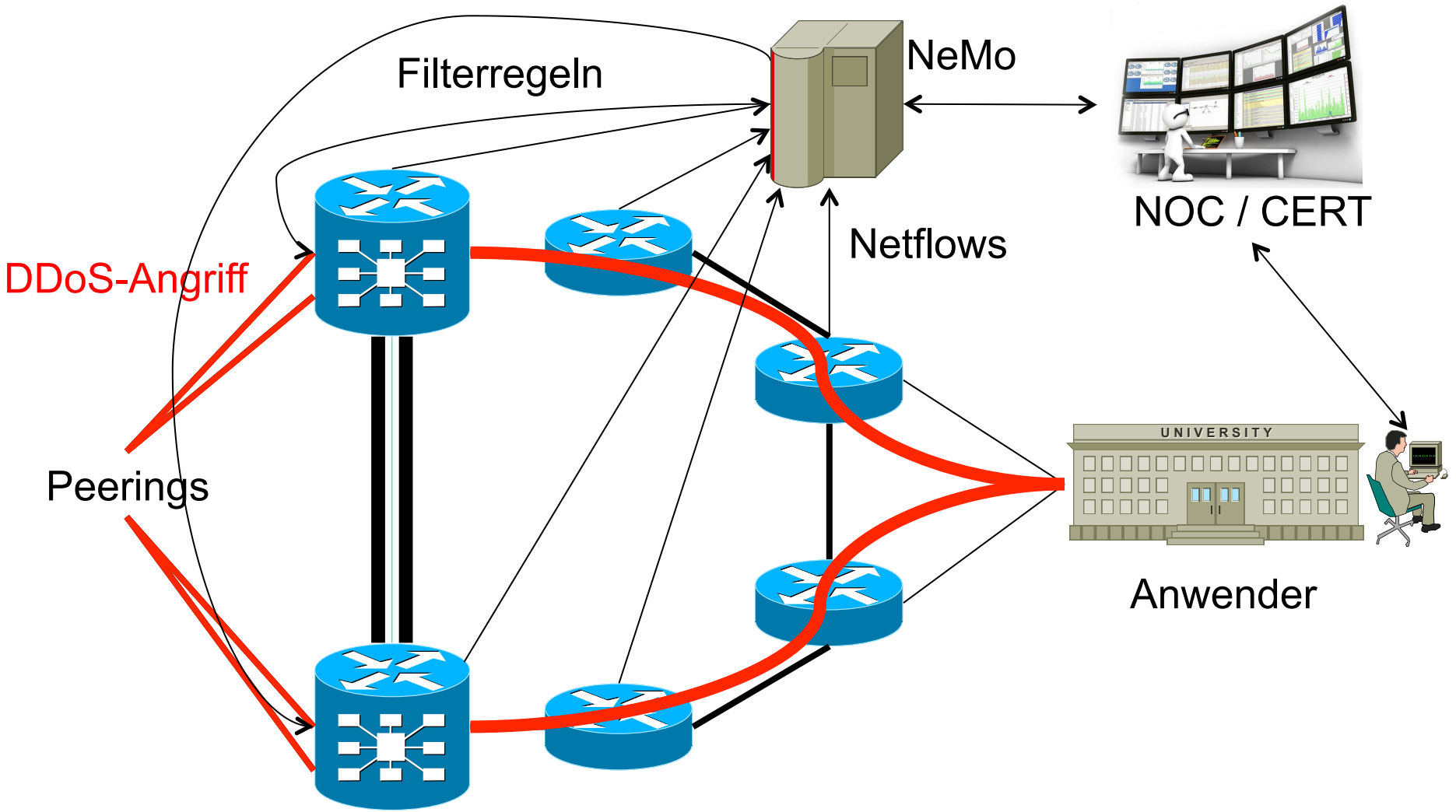
- Implementation of special service agreement bound to DFNInternet service agreement
  - Concise statement of legal framework, roles of involved persons and processes for mitigation
  - Legal certainty for both parties
  - Precise definition of responsibility and liability
  - Templates for communication and documentation

- Currently under investigation by DFN‘s Research Center for Law (University of Münster)

Approach (under discussion)

- Mitigation ensued only with explicit consent of user
  - i.e. DFN does not act if attack on user is alerted but user does not react and DFN‘s infrastructure is not affected
- Consent must be expressed by pre-appointed personnel (no exceptions!)
- Consent must be communicated over authentivcated channels (signed e-mail, Fax, callback on pre-approved mobile phone number)
  - Channel has to be agreed on in advance
  - Channel has to be usable in case of DDoS-attack

Vorgehen bei der DDoS-Mitigation



Offline Demo: Analyse SYN Flood

DFN Deutsches Forschungsnetz

Summary | Alerts | Objects | Topology Map | Visual Explorer | Sparklines | Preferences ▼ | System Information — DFN-NEMO

Summary of Open Alerts

Dates/Times in CEST

Tags ☐ Infrastructure ☐ Manual

All Severities (10) | Critical (5) | Warning (0) | Info (5)

See all alerts opened during the last hour, the last 24 hours, or last 7 days.

10 results

Alert ID	Workflow Status	Severity	Duration	Start Time	Event Count	Tags	Description	Details
389297	Seen	Critical	39 min (ongoing)	16:14, 2014-11-27	42		High UDP packet rate. 72 UDP Packets/s	GE/TEAG0263_JEN_F... UDP Packets
389283	New	Critical	1 h, 28 min (ongoing)	15:25, 2014-11-27	91		High UDP packet rate.	GE/TSI4004_GOE_MH... UDP Packets
389180	Seen	Critical	5 h, 12 min (ongoing)	11:41, 2014-11-27	315		High ICMP packet rate. 8k ICMP Packets/s	GE10/DFNWDM3061_... ICMP Packets
389164	New	Critical	5 h, 45 min (ongoing)	11:08, 2014-11-27	348		High UDP packet rate. 4k UDP Packets/s	GE10/ANWD_KA2750... UDP Packets
389124	Seen	Critical	6 h, 50 min (ongoing)	10:03, 2014-11-27	394		High ratio of SYN packets to ACK packets. 355k ACK Packets/s, 42k SYN Packets/s	GE10/DFNWDM3034_... SYN/ACK Packets
389310	New	Info	3 min (ongoing)	16:51, 2014-11-27	5		High UDP packet rate. 396 UDP Packets/s	GE/TSI4134_KIE_MPI... UDP Packets

Offline Demo: Analyse SYN Flood

DFN Deutsches Forschungsnetz

Summary | **Alerts** | Objects | Topology Map | Visual Explorer | Sparklines | Preferences ▼ | System Information — DFN-NEMO

Critical Alert 389124

Dates/Times in CEST

Alarm Begin/End **today, 08:36** – **ONGOING** **(6 h, 52 min)**
Events First/Last **today, 09:59** / **16:53**

1 affected object , 396 events

Merge... Close Mute

scrolling

Alert Analyses

This alert has not been analyzed. **Analyze Alert >>**

Event Sources

GE10/DFNWDM3034_BIR_FRA SYN/ACK Packets

Alert Details

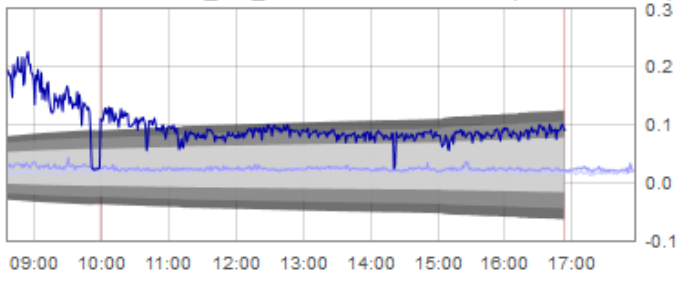
Description High ratio of SYN packets to ACK packets.
Tags -
Event Count 396 View all events...
Trigger High SYN / ACK Ratio (ID 8)

Alert History / Comments

Add Comment

Date	User	Message
today, 10:24	System	Observed critically high values of the ratio of SYN packets to ACK packets with 389k ACK Packets/s, 40k SYN Packets/s on line GE10/DFNWDM3034_BIR_FRA, GE10/DFNWDM3035_BIR_FRA. Upgraded to severity Critical.
today, 10:12	System	Observed more high values of the ratio of SYN packets to ACK packets with 359k ACK Packets/s, 44k SYN Packets/s on line GE10/DFNWDM3034_BIR_FRA, GE10/DFNWDM3035_BIR_FRA. Upgraded to severity Warning.
		Observed high values of the ratio of SYN packets to ACK

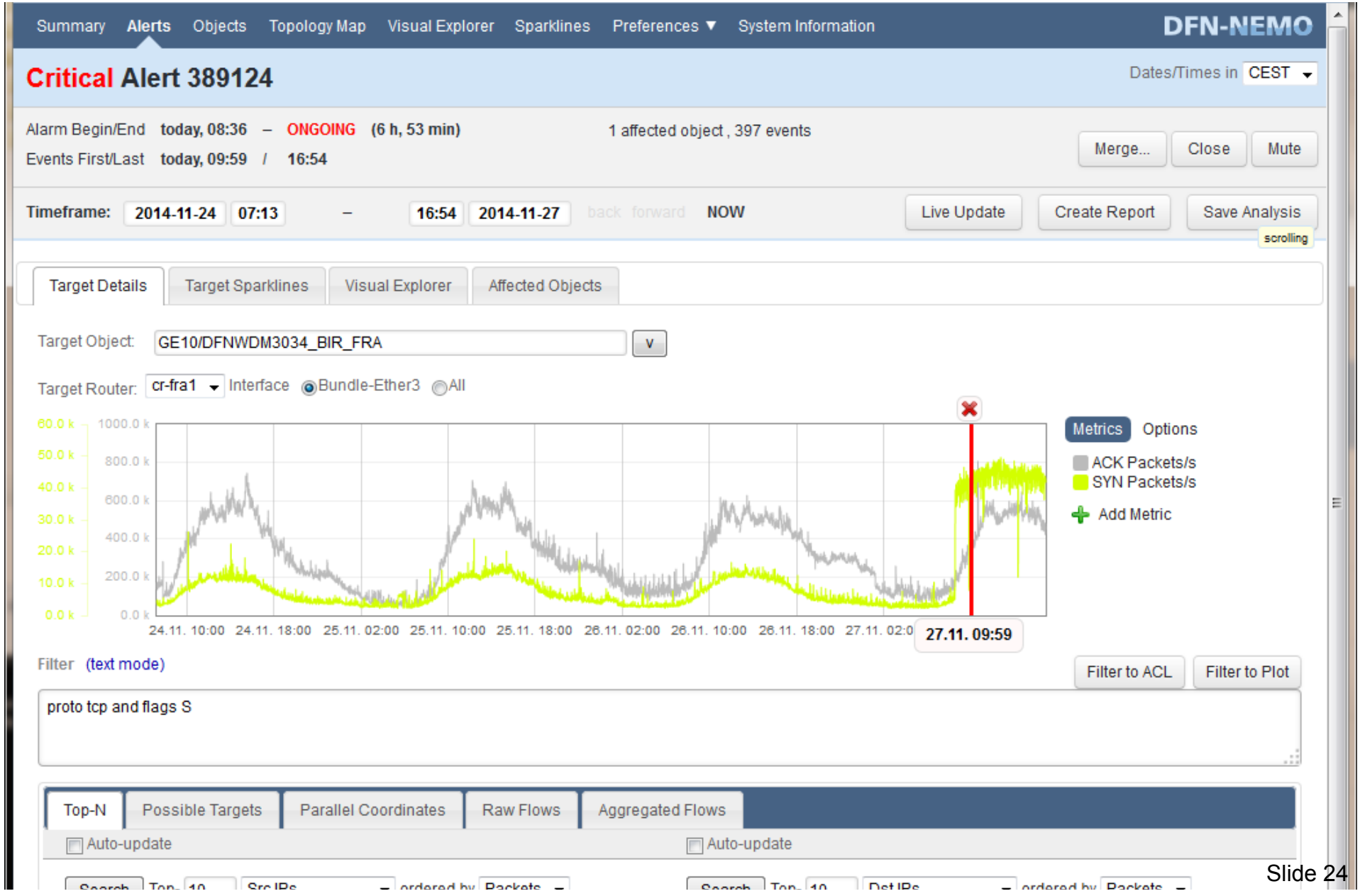
GE10/DFNWDM3034_BIR_FRA - SYN/ACK Packets (SYN ACK Ratio)



Blue: Current value
Light blue: Same timeframe 1 week ago
Lighter blue: Same timeframe 4 weeks ago
Gray shaded area: Model corridor (if applicable)
Pink: Model prediction (if applicable)

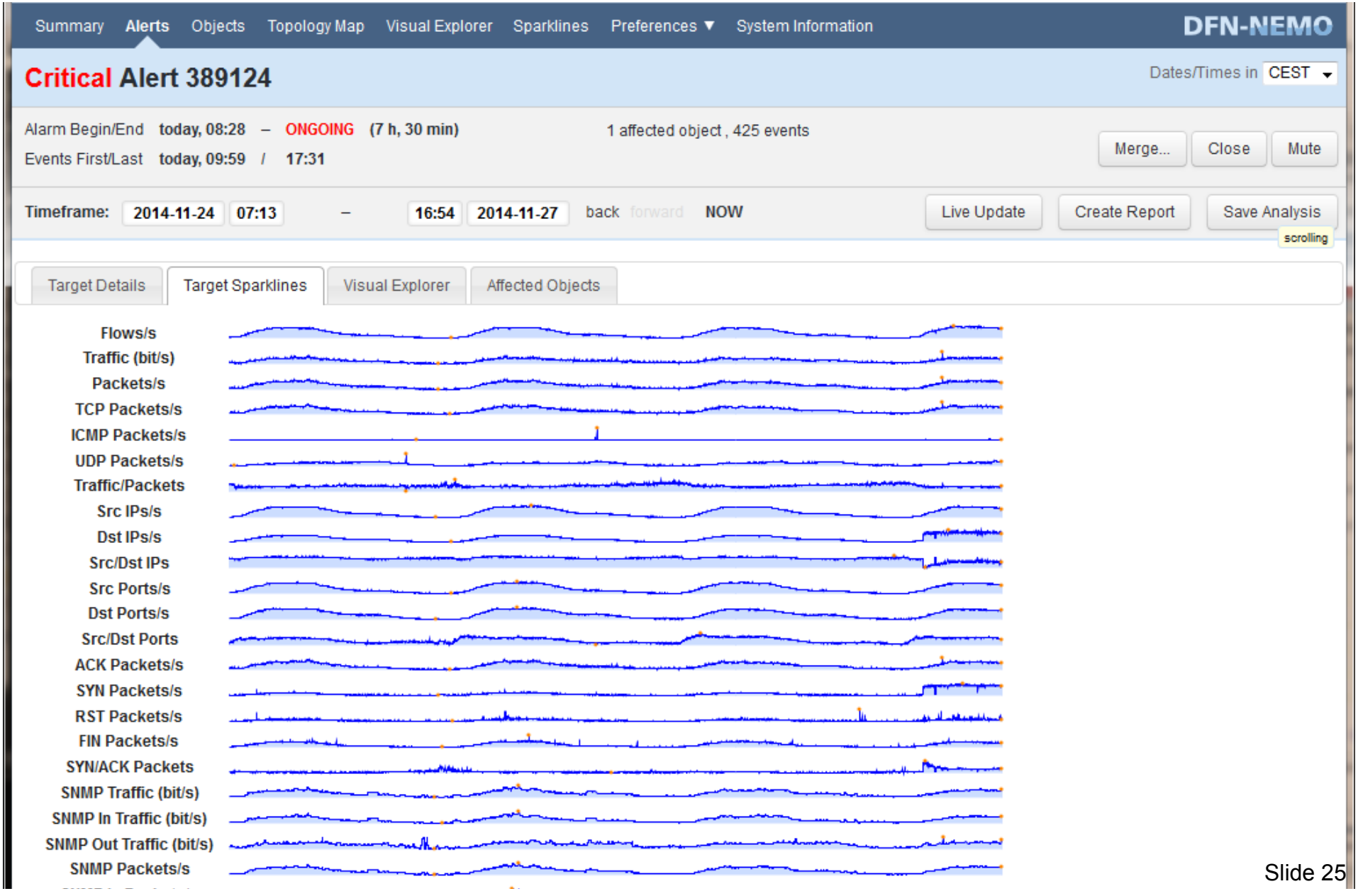
Offline Demo: Analyse SYN Flood

DFN Deutsches Forschungsnetz



Offline Demo: Analyse SYN Flood

DFN Deutsches Forschungsnetz



Offline Demo: Analyse SYN Flood

DFN Deutsches Forschungsnetz

Overview Alarms per Day

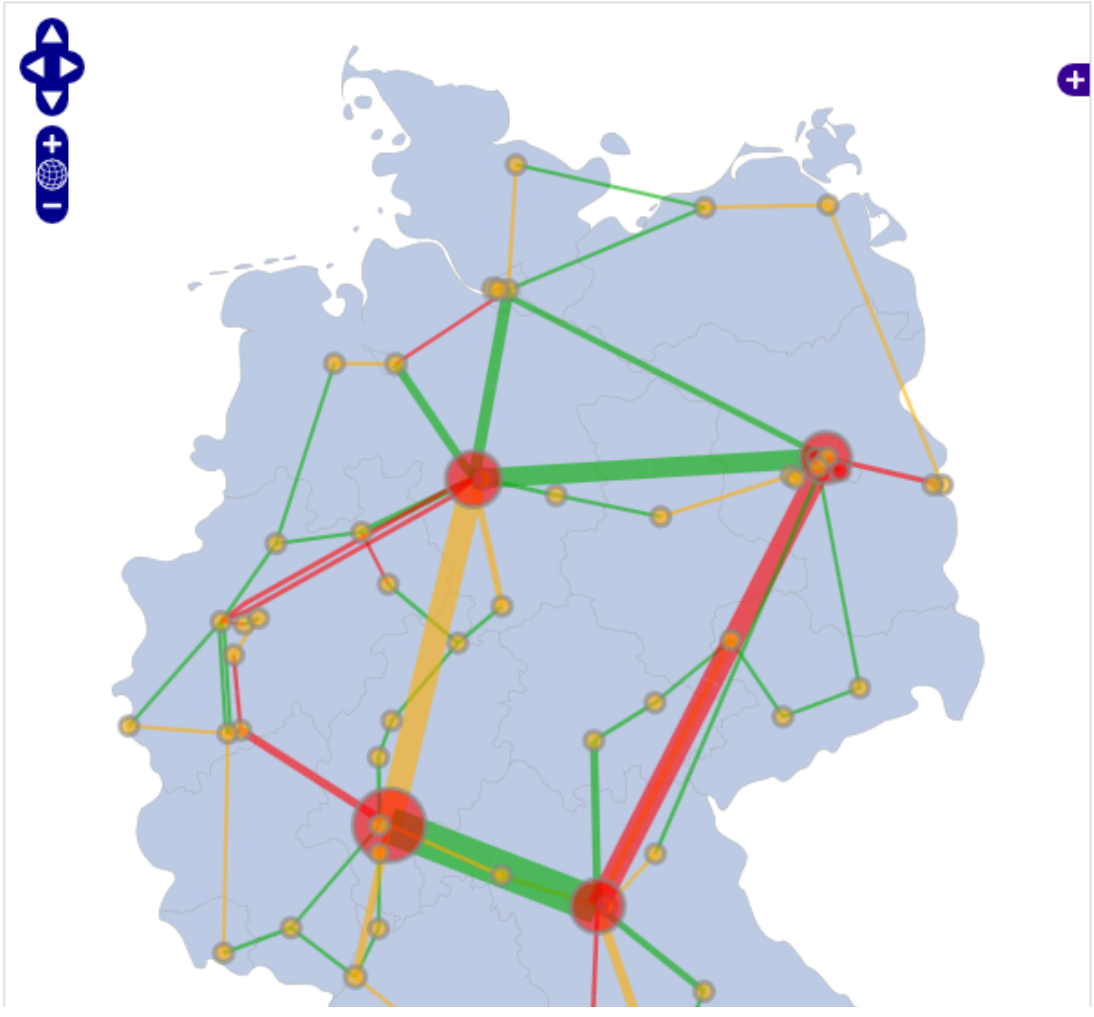
Deutsches Forschungsnetz

Summary | Alerts | Objects | **Topology Map** | Visual Explorer | Sparklines | Preferences ▼ | System Information — DFN-NEMO

Network Topology Map

Dates/Times in CEST

Timeframe: 2014-11-24 00:00 – 00:00 2014-11-25 back forward NOW



Object Size: Traffic averaged over the chosen timeframe.

Object Color: not used | number of events | number of alerts

Color Legend: 0 | 1 - 2 | > 2