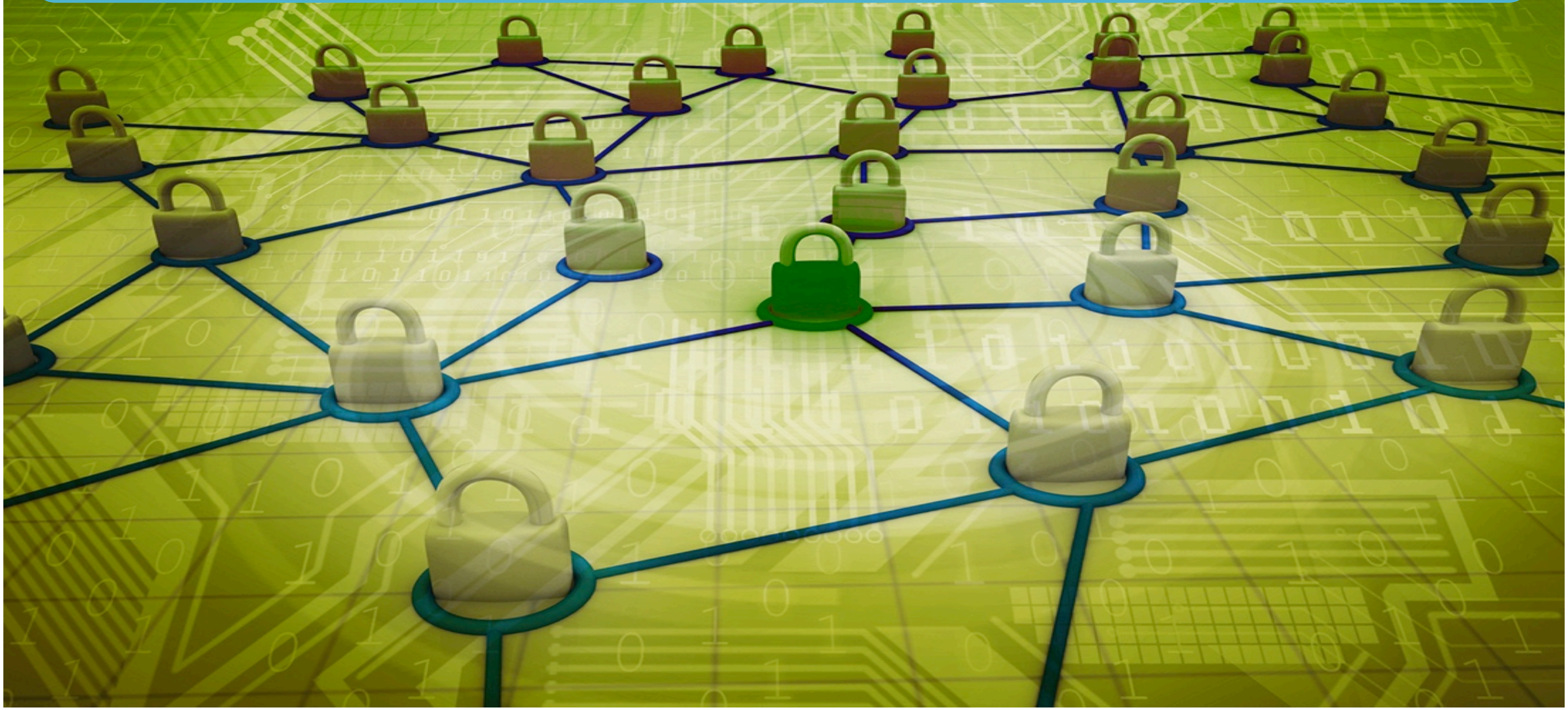
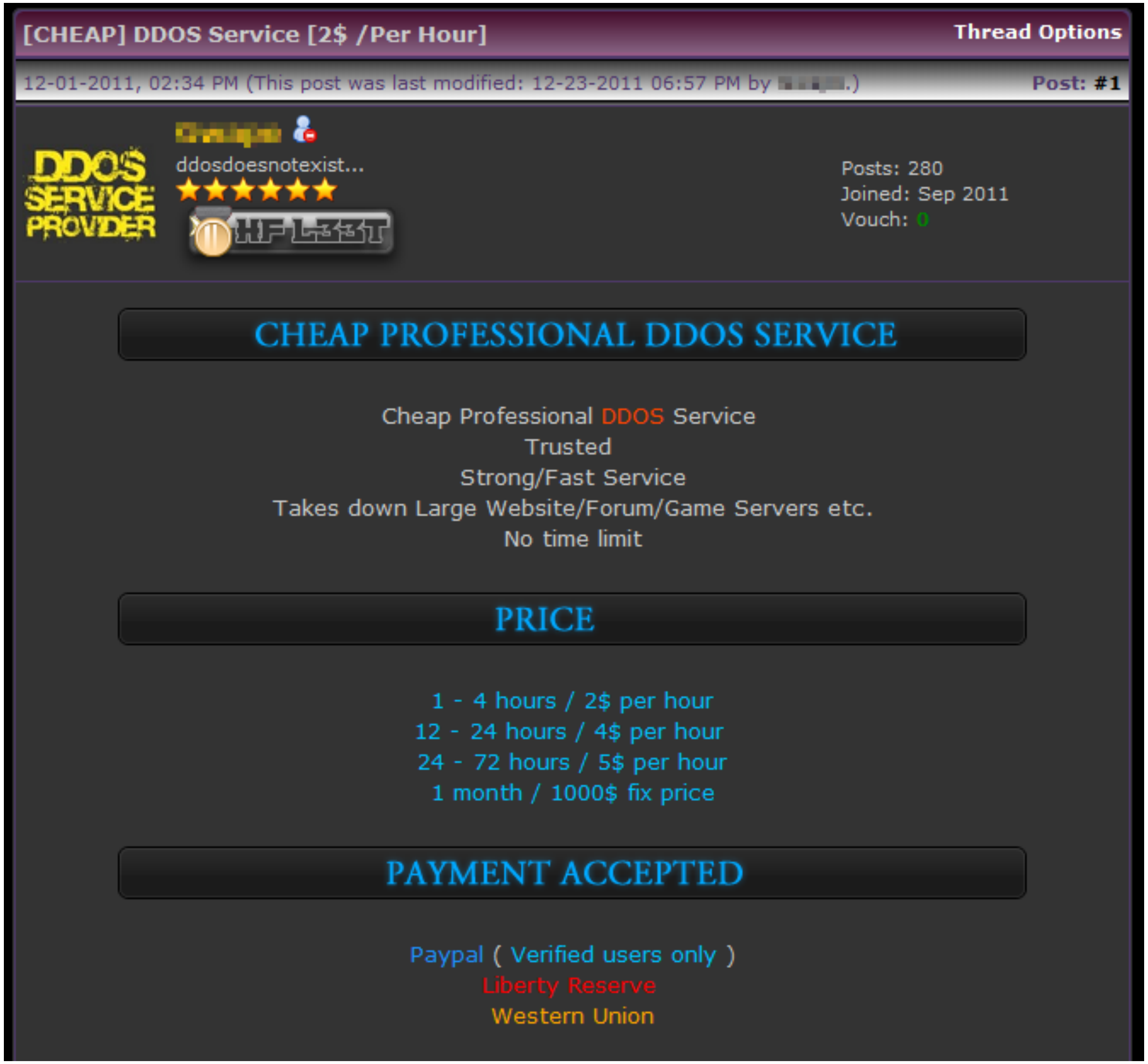
DDoS Mitigation @ SURFnet



Albert Hankel
Productmanager Security Services
Vienna, 10-11-2015

SURF NET

DDoS-as-a-Service



[CHEAP] DDOS Service [2$ /Per Hour] Thread Options

12-01-2011, 02:34 PM (This post was last modified: 12-23-2011 06:57 PM by [redacted].) Post: #1

[redacted]
ddosdoesnotexist...
★★★★★★

Posts: 280
Joined: Sep 2011
Vouch: 0

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional DDOS Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

PRICE

1 - 4 hours / 2$ per hour
12 - 24 hours / 4$ per hour
24 - 72 hours / 5$ per hour
1 month / 1000$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)
Liberty Reserve
Western Union

Why a DDoS attack?

- Disrupt entire ICT infrastructure
- Disrupt security measures (e.g. fi
- Disrupt a ser
- g)
- the outside world
- “Because we can” (vandalism)

Threat is usually from the inside – very little organized crime in HE&R

Two types of attack

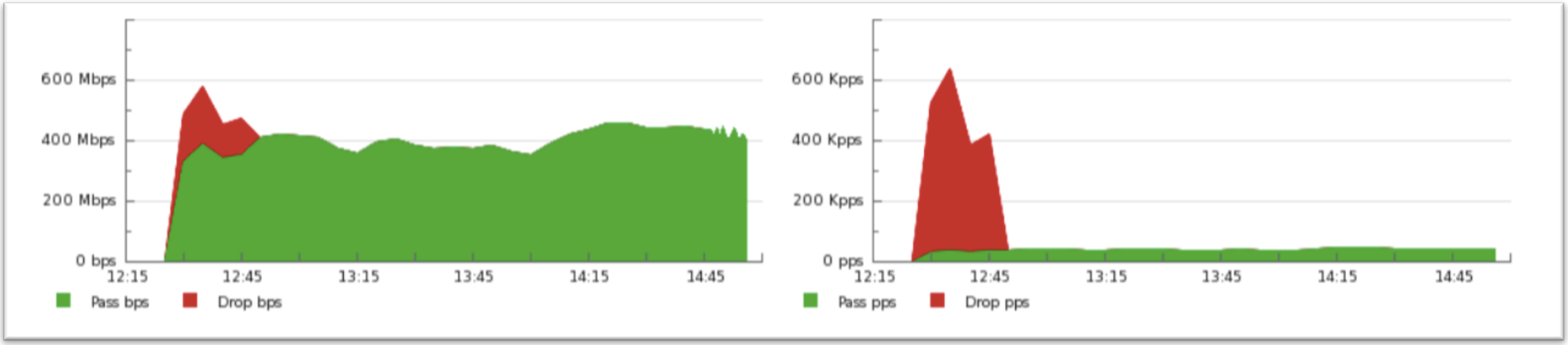
Volumetric attacks (either in bits/s or packets/s)

- Target infrastructure or access
- Can be detected by NRENs (mostly)
- Often brute force

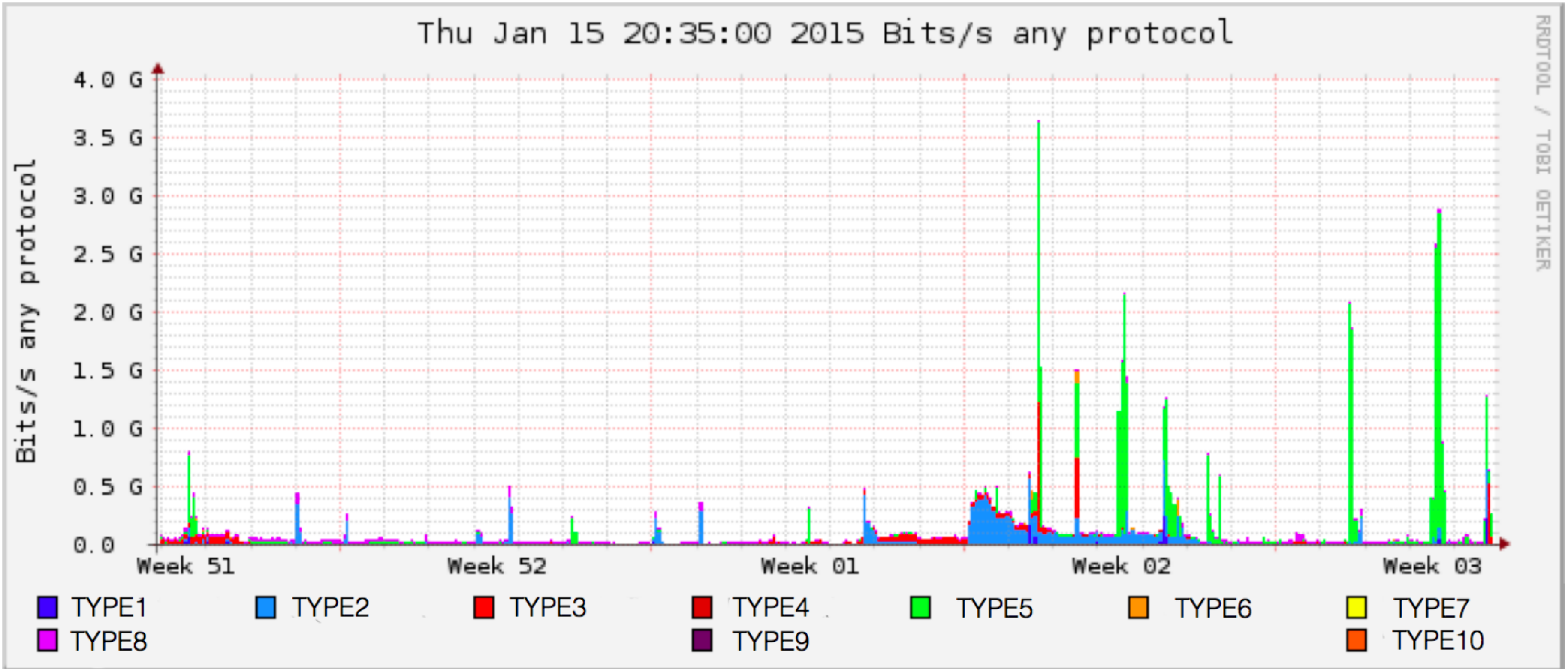
Application layer attacks

- Target specific services
- Seem/are legitimate traffic to NRENs
- More sophisticated; makes use of vulnerabilities in application

Volumetric attacks: bits vs packets



We see daily attacks, 5 on average…

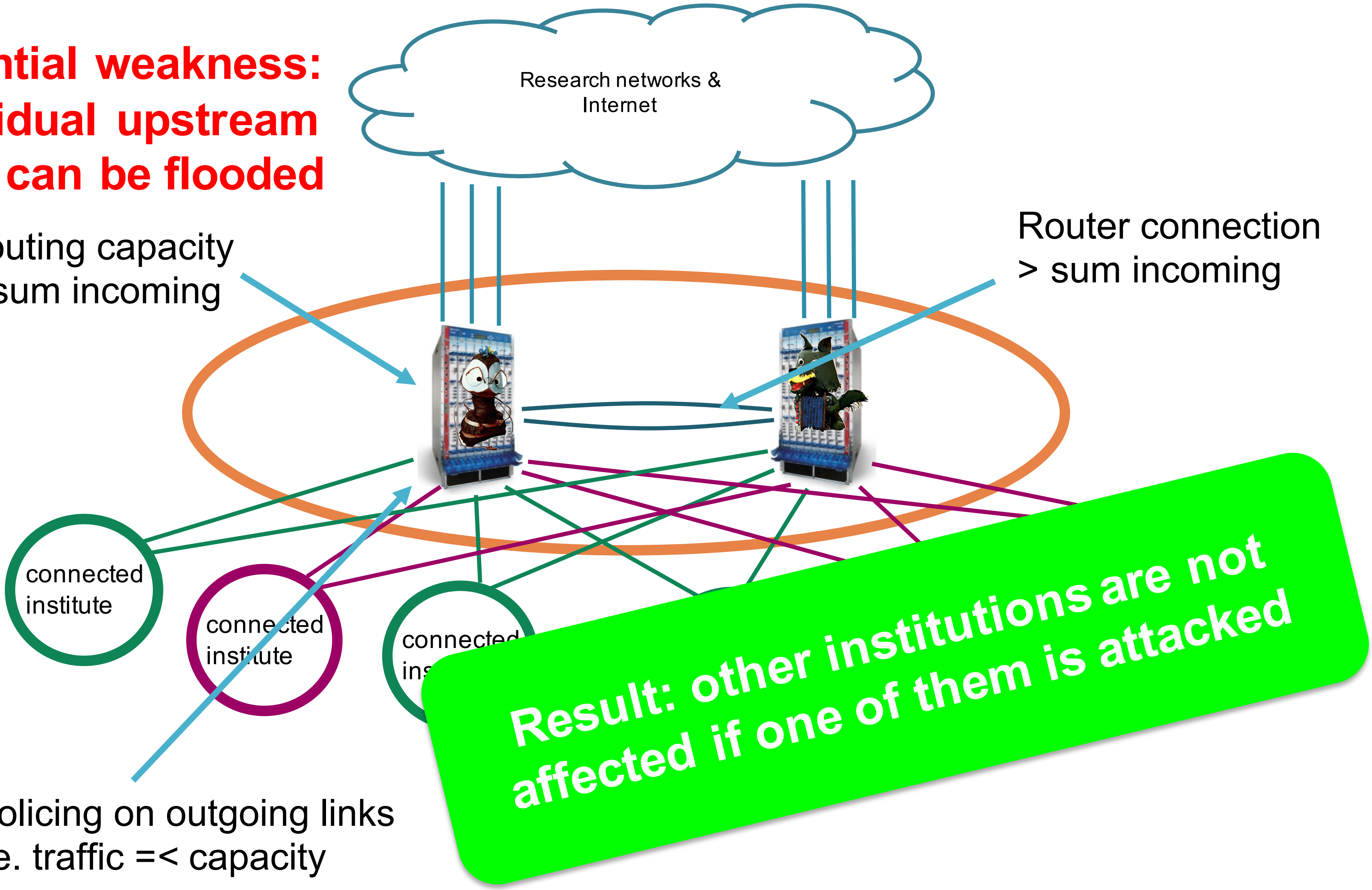


DDoS prevention and mitigation

1) Architecture principles

Our network simplified

Potential weakness: individual upstream links can be flooded



Routing capacity
> sum incoming

Router connection
> sum incoming

Policing on outgoing links
i.e. traffic =< capacity

Result: other institutions are not affected if one of them is attacked

2) Monitoring

SURFcert

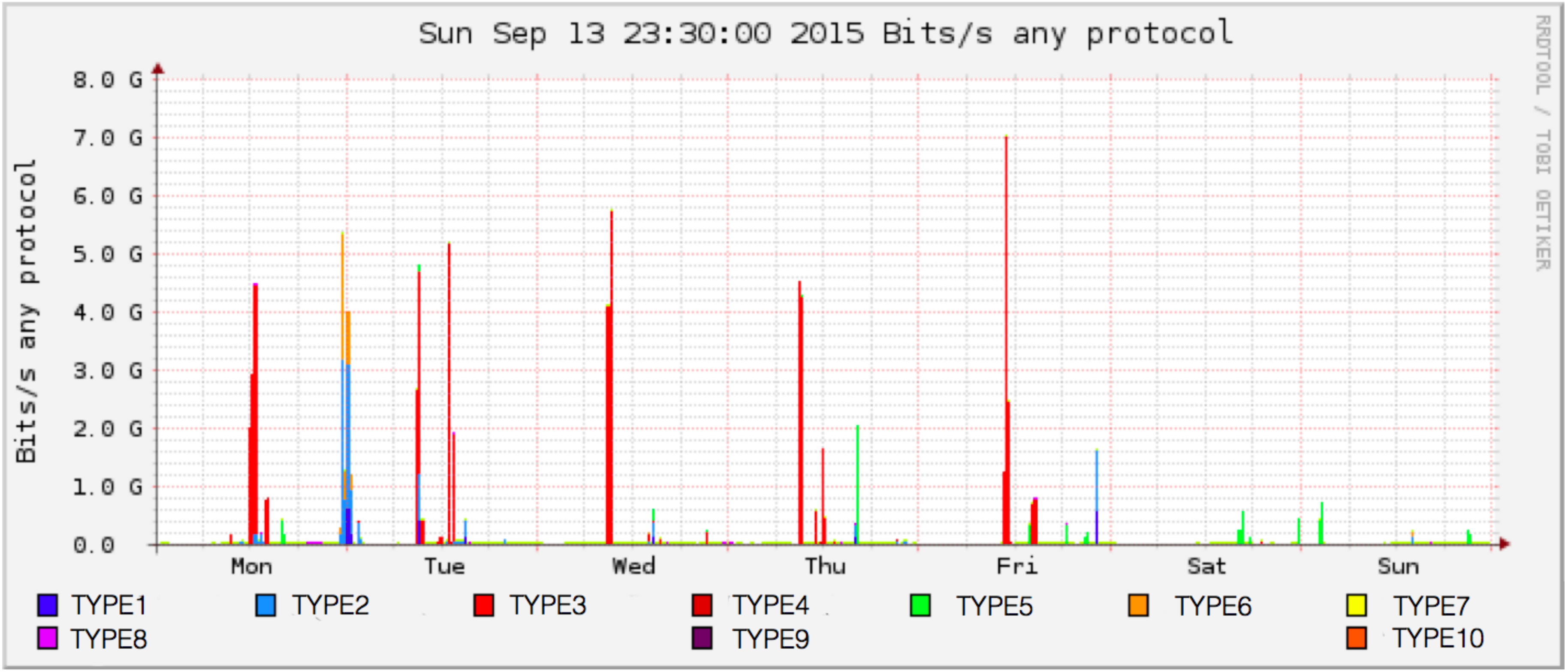
Organization of Team

- Operational security for the SURFnet constituency
- 24x7 service in close coop with local security teams
- Members from connected institutions and SURFnet
- Oldest *emergency response team* in the Netherlands

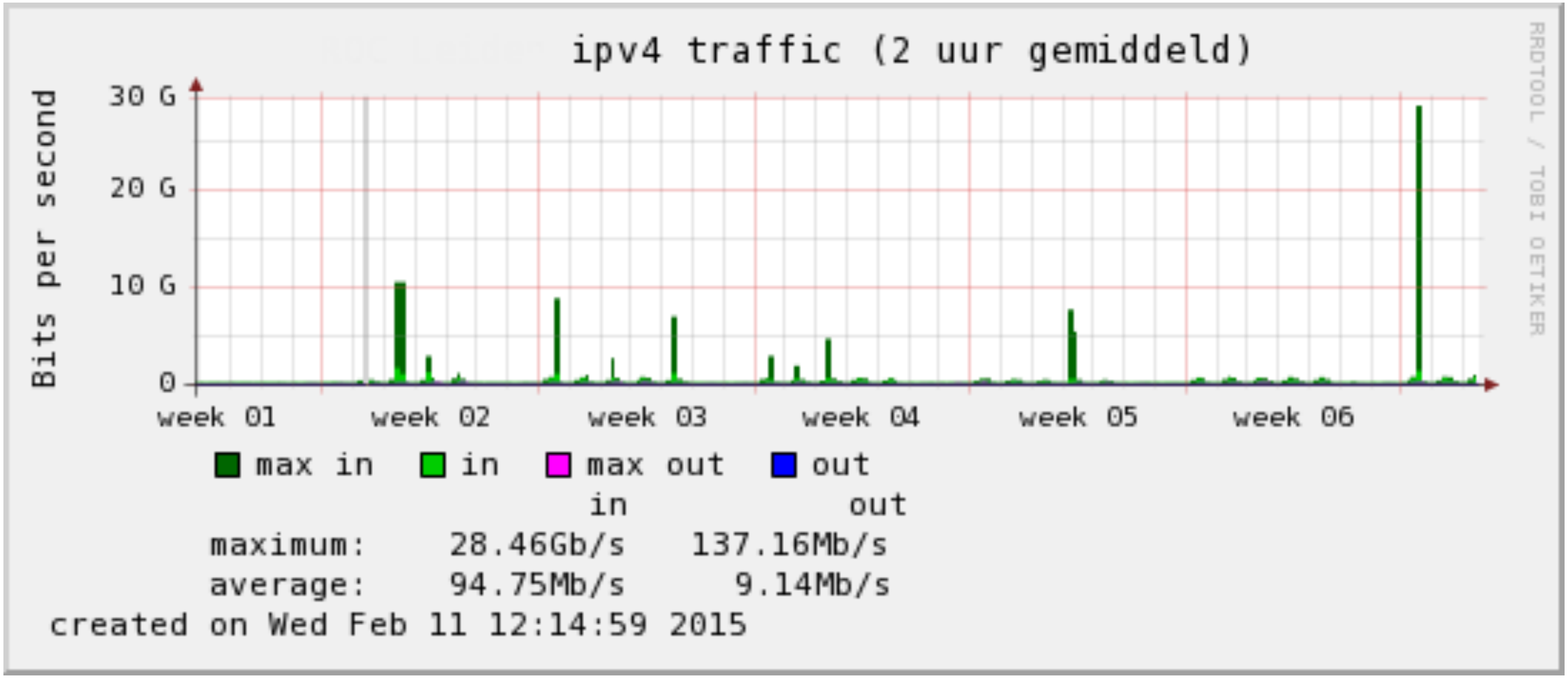
Monitoring

- General and fine-grained traffic flows (nfsen and peakflow)
- Outside intelligence reports (e.g. shadowserver – open resolvers)
- Incident analysis
- Sharing intelligence (national, international)

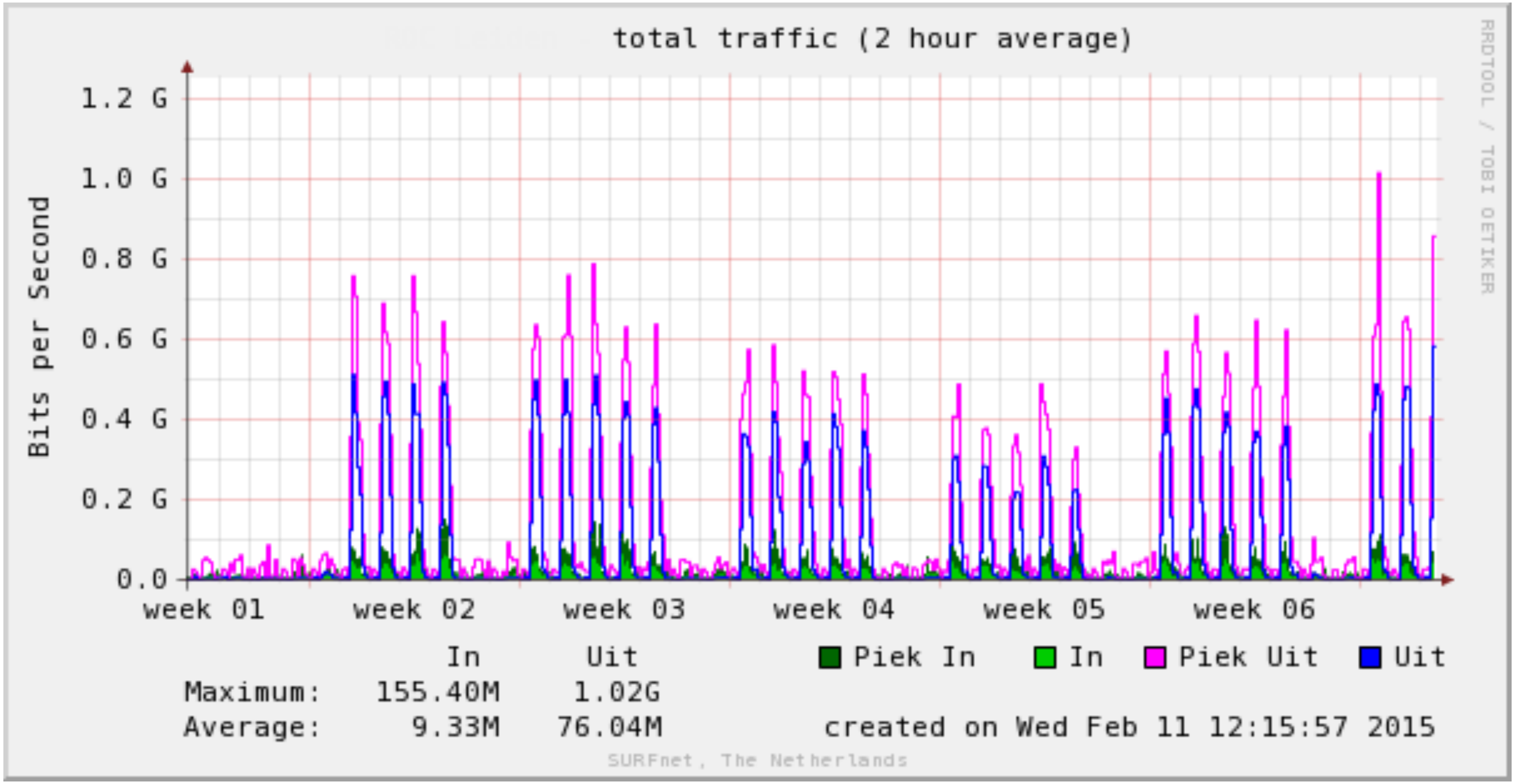
SURFcert monitoring



Monitoring access for institutions: TrafMon

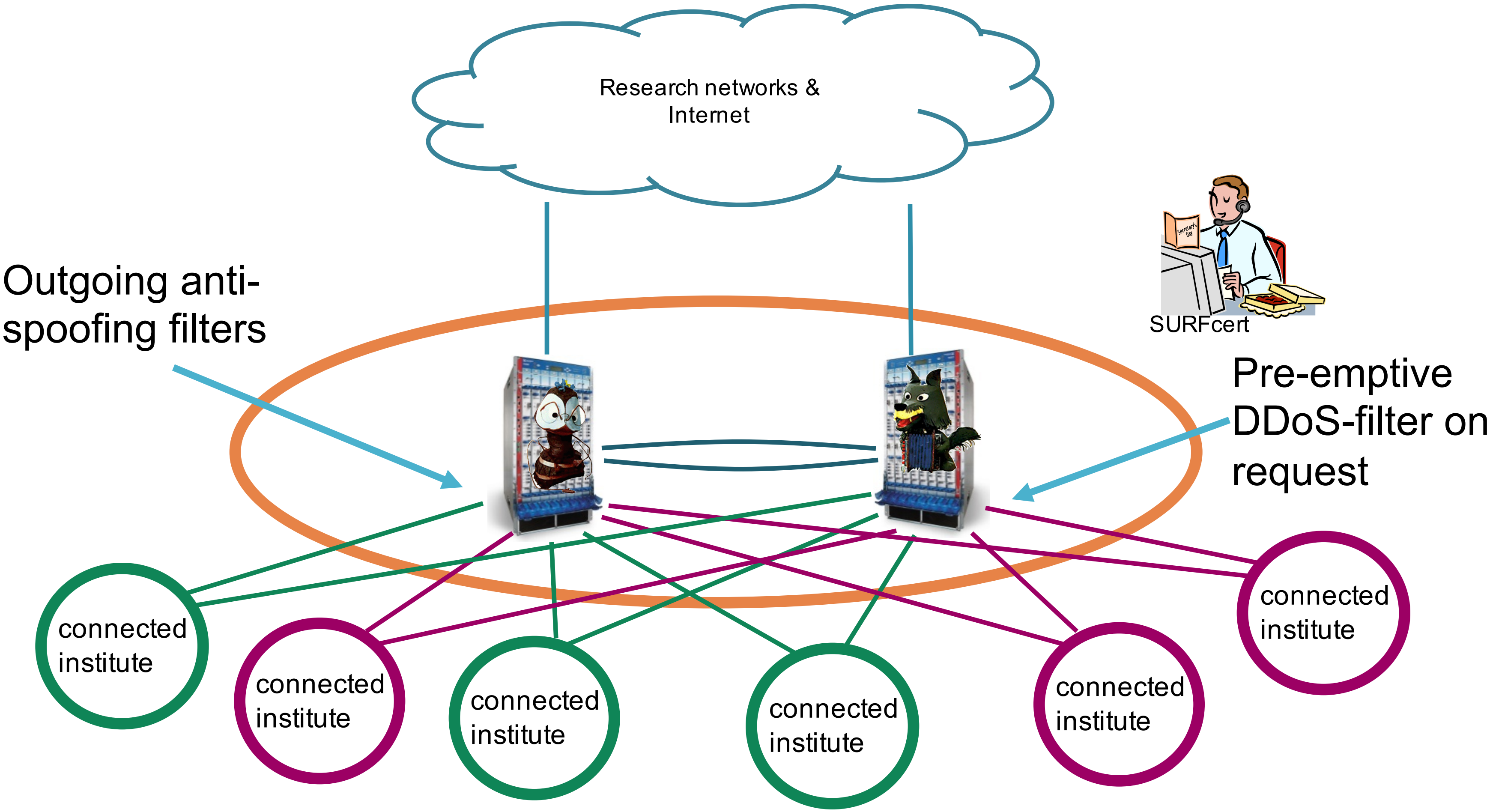


Monitoring access for institutions: SURFstat



3) Mitigation

Network filtering



Research networks & Internet

SURFcert

Outgoing anti-spoofing filters

Pre-emptive DDoS-filter on request

connected institute

connected institute

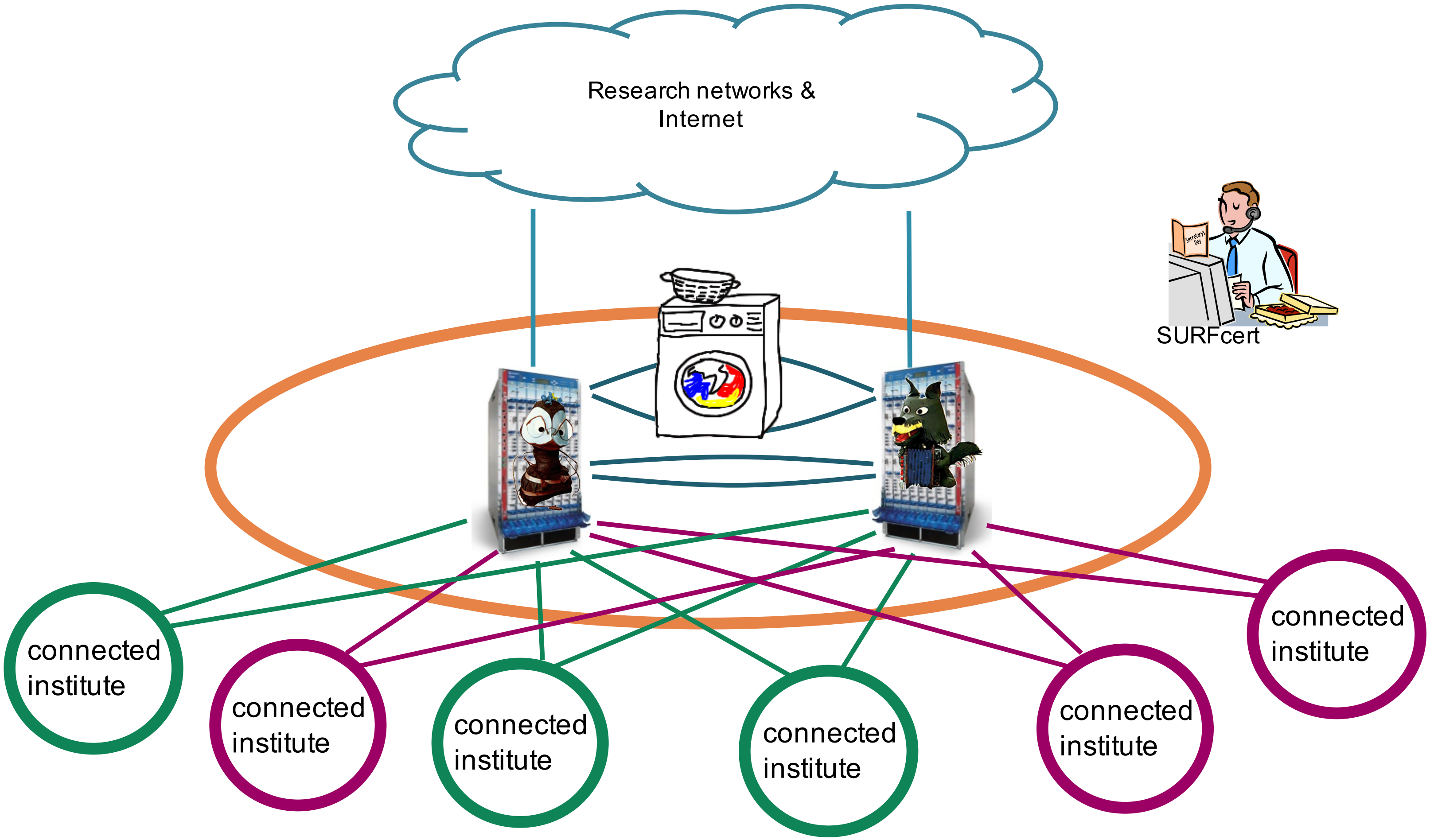
connected institute

connected institute

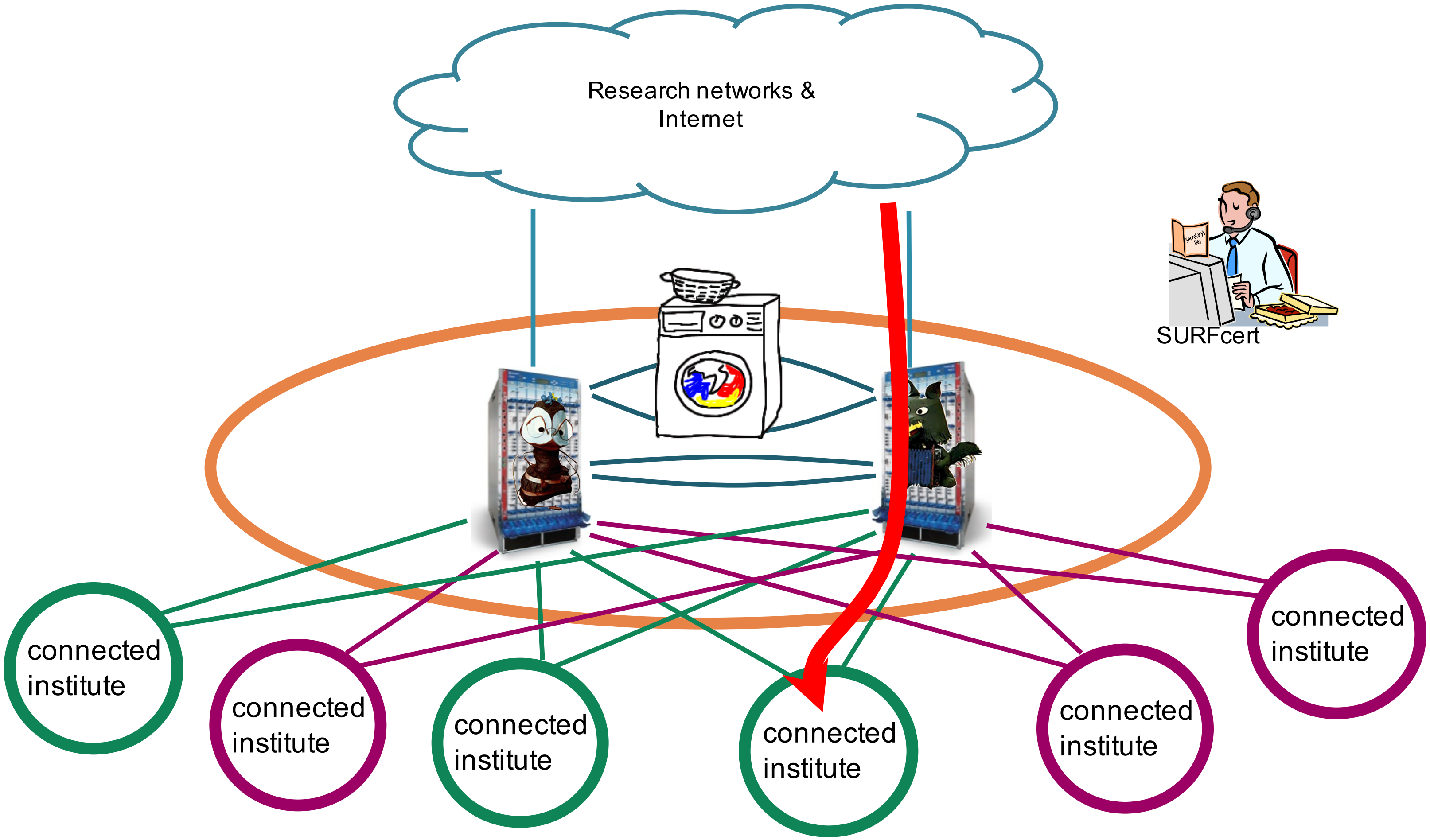
connected institute

connected institute

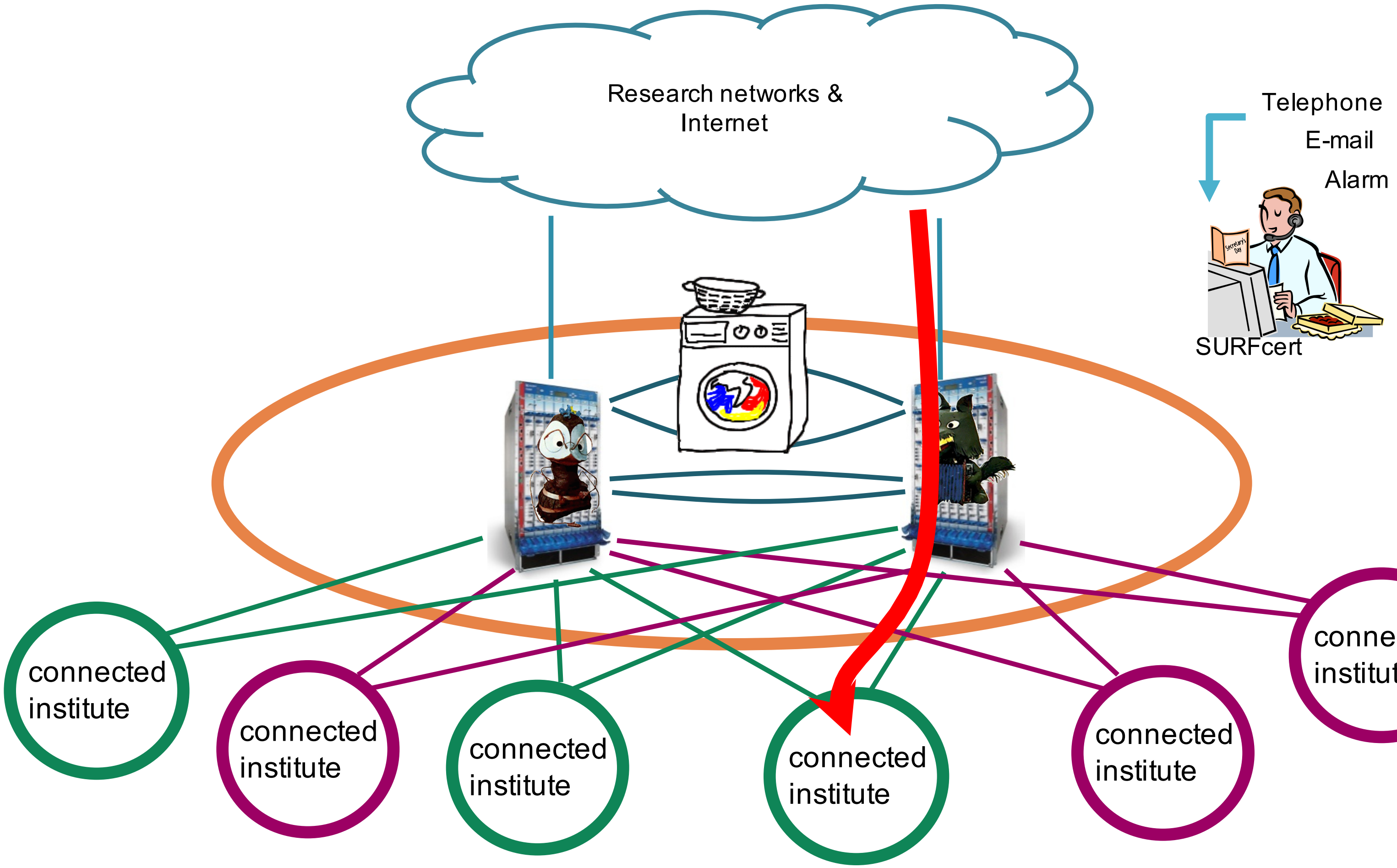
SURFnet washing-machine



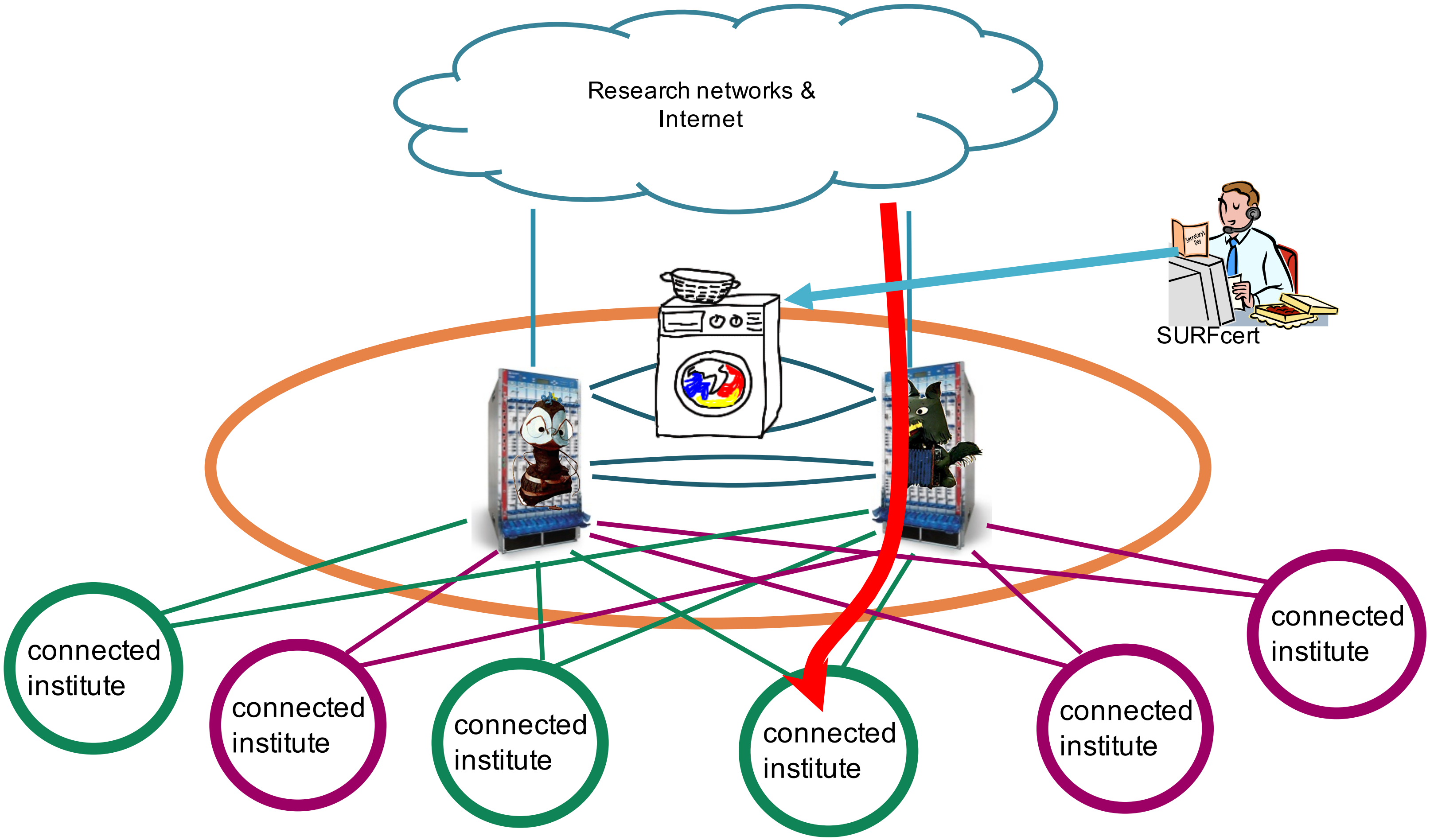
SURFnet washing-machine – Denial-of-Service



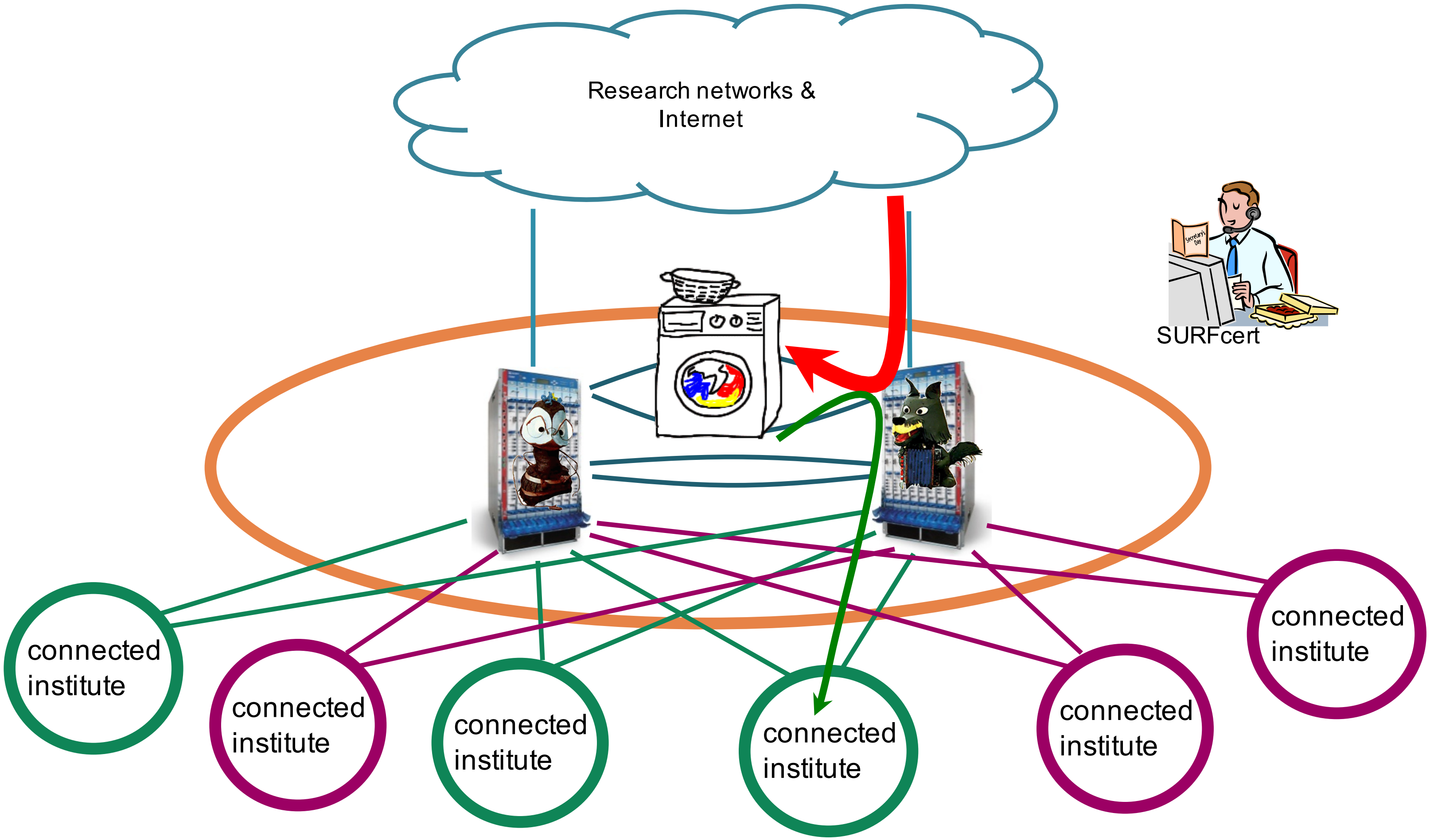
SURFnet washing-machine – Detection



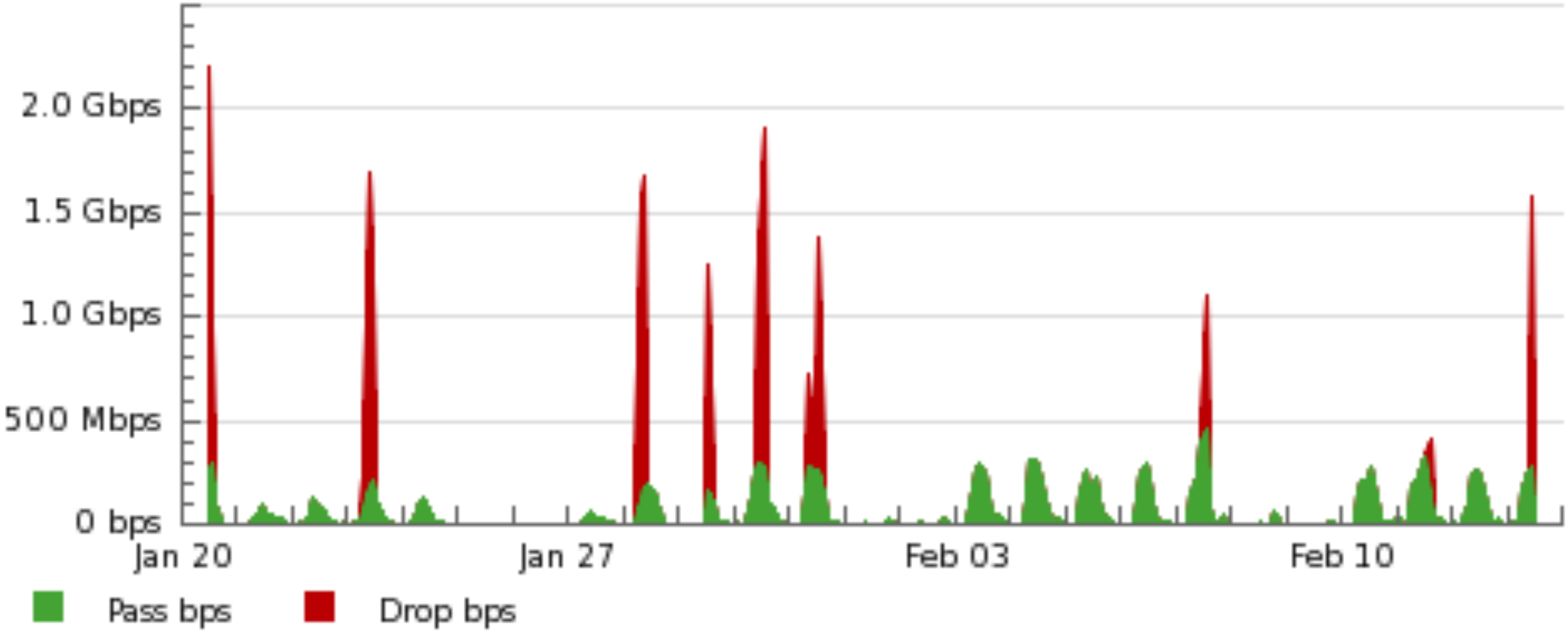
SURFnet washing-machine – Activate washprogram



SURFnet washing-machine – DDoS in the washing-machine

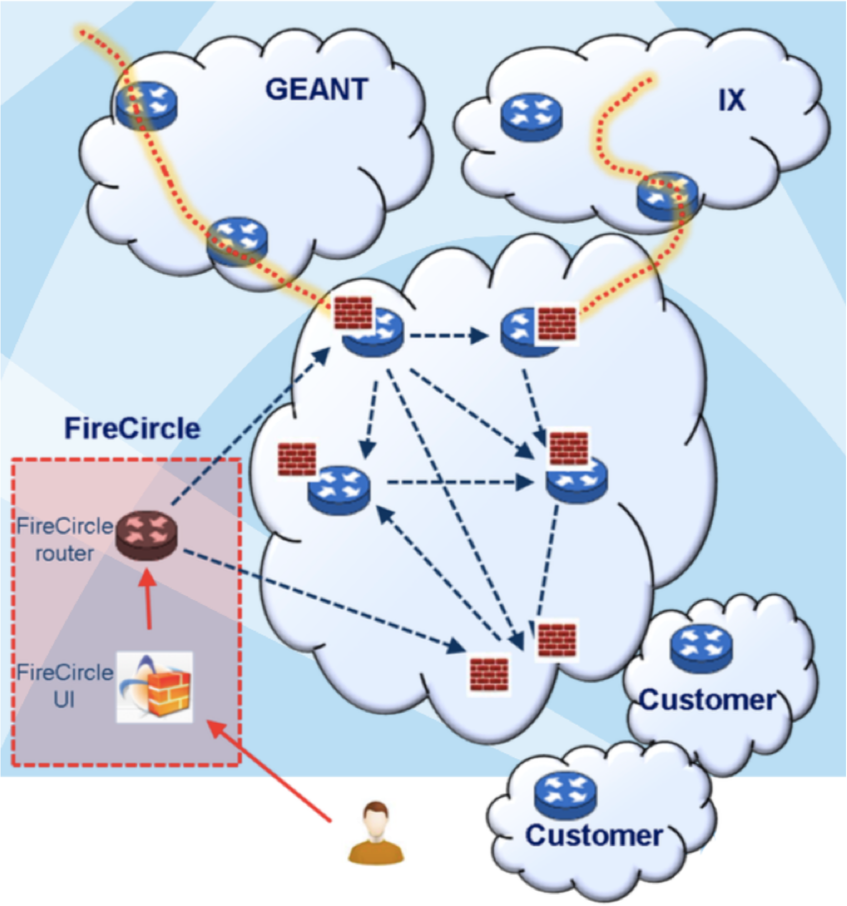


Washing effect



Pilot: self-service network filtering

Firewall-on-Demand



Pilot

- 14 institutions participating
- Two months (until end of year)
- Testing functionality

Finding the best place to mitigate

- **Upstream (us)**
  - Standard security measures on customer connection
  - The “washing-machine” for first aid
  - Pre-emptive filters (rate limiters) on the core routers
  - Self-service filtering

- **Firewall (institutions)**
  - Not always the right solution
  - Not a remedy for flooded connections
  - Can help in case of SYN floodi
    limiting)

We are setting up a project to see if we can help with application layer DDoS-attacks

4) Tracing the culprits

Who is attacking?

- The (D)DoS ‘source’ is often an internal factor (person)
- Match timestamps of attacks with class & exam schedules
- Collaborate with people from education
- Report findings to the police

Advise against NAT

Best practice at one of our institutions (freely translated quote):

- Student attacks his own IP address
- We do not have a NAT, but provide each computer with a public IP address
- All the computer rooms have their own separate VLAN so we know where the culprit is
- ActiveDirectory logging allows us to connect computer to student
- So we can apprehend the student within 2 minutes
- We deliver the student with logging proof to the dean and he confessed immediately

Something related to DDoS but different: legal issues

The BotLeg Project (1/2)

New project (just started):
Aim is to enhance legal certainty in botnet-fighting and anti-botnet operations

Context
Combatting botnets, which facilitate many forms of cyber-attacks, is a key challenge in cybersecurity. The classic crime-fighting approach of prosecuting perpetrators and confiscating crime tools fails here: botnets cannot be simply 'confiscated', and law-enforcement's reactive focus on prosecuting offenders is ill-suited to deal effectively with botnet threats.
A wider set of anti-botnet strategies, including pro-active strategies and public-private co-operation, is needed to detect and dismantle botnets. Public-private anti-botnet operations, however, raise significant legal questions: can data about (possibly) infected computers be shared among private parties and public authorities? How far can private and public actors go in anti-botnet activities? And how legitimate are public-private partnerships in which private actors partly take up the intrinsically public task of crime-fighting?

Objectives

- Investigate legal limits and possibilities for anti-botnet operations
- Raise awareness among stakeholders on such operations
- Develop guidelines / code of conducts

The BotLeg Project (2/2)

The overall research question is: **under which conditions can efficacious public-private anti-botnet operations be lawfully and legitimately undertaken?**

With the following sub-questions:

- Which types of operations are desired by public and private stakeholders to efficaciously combat botnets?
- Under which conditions can botnet-related information be exchanged among private parties and between private and public parties?
- Under which conditions are intrusive anti-botnet operations lawful, i.e., what are the legal limits and possibilities?
- Which requirements can be formulated to enhance the legitimacy of Public-Private Partnerships in anti-botnet operations?
- Which practicable guidelines and codes of conduct for stakeholders can be derived from these findings?

In Summary

To combat DDoS (and other) attacks, we need to:

- Minimize structural weaknesses
- Monitor at multiple layers (institutions, NREN, upstream providers)
- Mitigate at multiple layers (idem)
- Trace (and prosecute) perpetrators

The challenge here is that all these items usually cannot be addressed by one party – technical, organizational, forensic and legal collaboration is needed

Questions?

✉ Albert Hankel
albert.hankel@surfnet.nl

SURF NET