DDOS Mitigation in RedIRIS

SIG-ISM . Vienna

GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMIA
Y COMPETITIVIDAD

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es

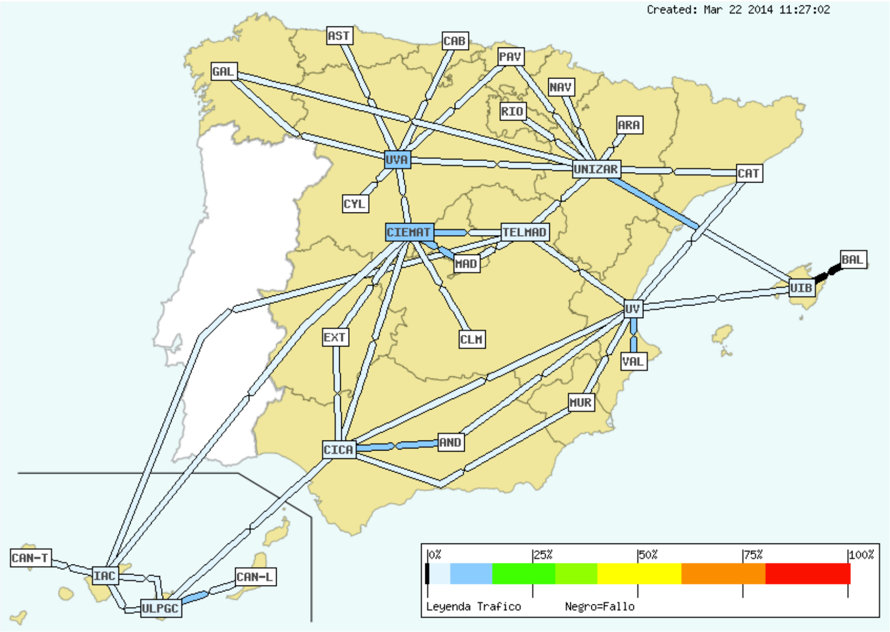
RedIRIS

Index

- Evolution of DDOS attacks in RedIRIS
- Mitigation Tools
- Current DDOS strategy

About RedIRIS

- Spanish Academic & research network ….
- Universities, research centers, ….
- Not schools for now
- But also a lot of government organizations



GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
RedIRIS

Evolution of DDOS attacks in RedIRIS

Reported DDOS attacks against RedIRIS organization were rare some years ago.

- Some IRC wars in in 2000-2001
- Political protest in 2003
- Another political protest in 2010

Usually organizations were used in DDOS more than been victims

Evolution DDOS attacks in RedIRIS

DDOS countermeasures:

- Filtering of compromised machines
- NFSend & reporting to CSIRT as detection system
- CSIRT contacts for mitigations attacks against RedIRIS organizations

Evolution of DDOS attacks in RedIRIS

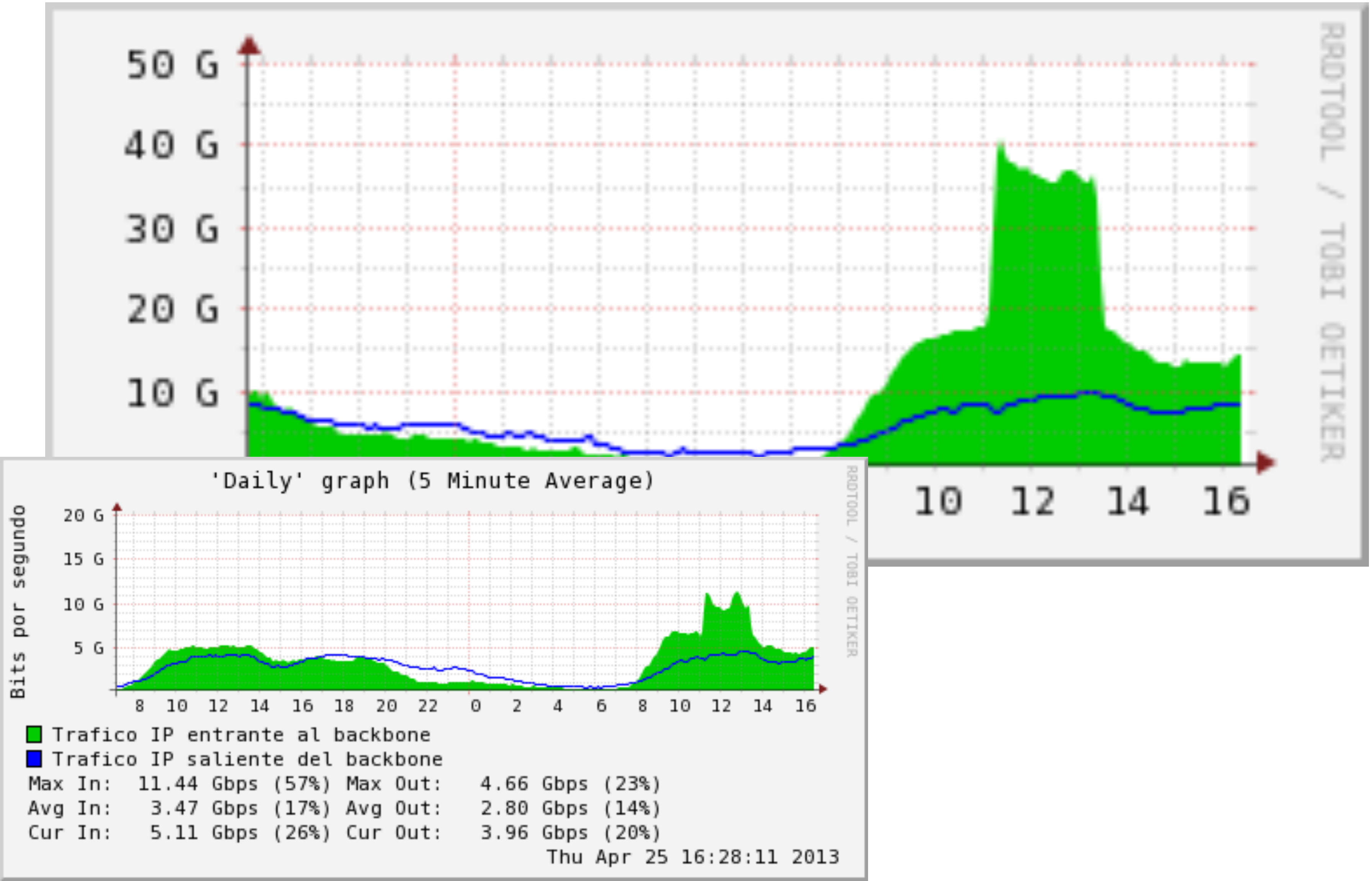
Since 2010 DDOS were more frequent:

- Organizations used RedIRIS connection for their administrative traffic , tuitions, taxes…
- DDOS tools were easily available due to the anonymous movement.
- Some government organizations with political impact were also connected to RedIRIS

DDOS example

- Bad timing
  - If something could fail it will fails.
    - RedIRIS NOVA backbone migration
    - Training session day for staff
    - Other people attending meetings & workgroups
  - No Previous feedback from the organization
  - Some time trying to contact the right person inside RedIRIS

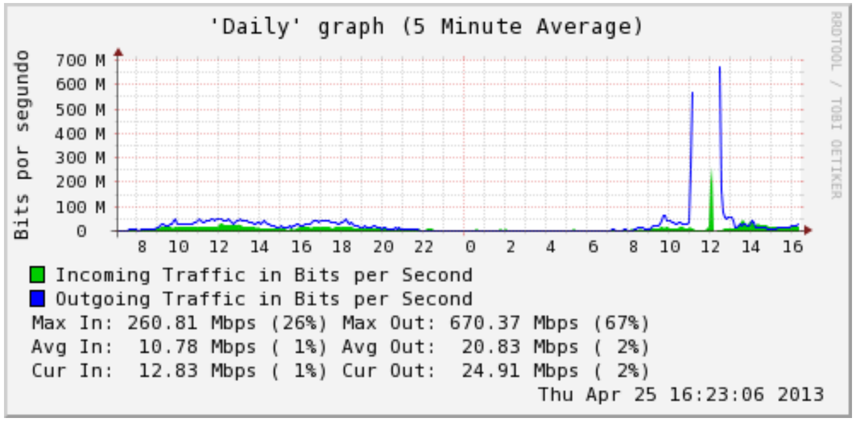
DDOS example



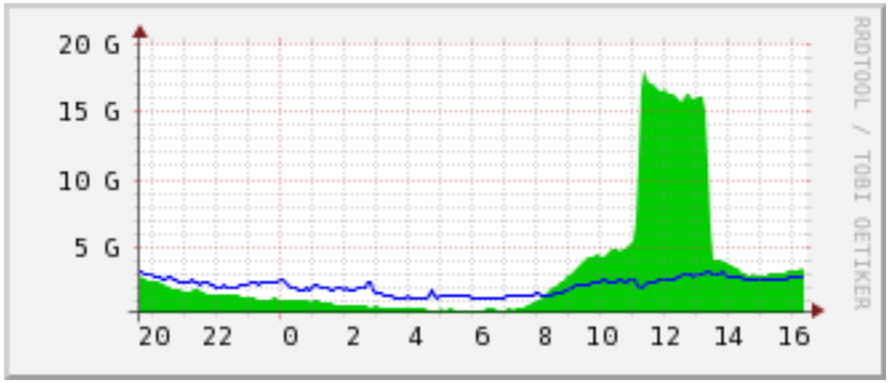
```
Max In:  11.44 Gbps (57%) Max Out:   4.66 Gbps (23%)
Avg In:   3.47 Gbps (17%) Avg Out:   2.80 Gbps (14%)
Cur In:   5.11 Gbps (26%) Cur Out:   3.96 Gbps (20%)
                                 Thu Apr 25 16:28:11 2013
```

DDOS example

- This traffic impact also in our backbone infrastructure
- Customer links completely saturated
- Traffic analysis show port 80/UDP traffic against web server.
- 400 sources outside RedIRIS network → Applied filtering in outside peering connections.
- Contact international ISP security contacts to block & filters the bots



```
Max In: 260.81 Mbps (26%) Max Out: 670.37 Mbps (67%)
Avg In:  10.78 Mbps ( 1%) Avg Out:  20.83 Mbps ( 2%)
Cur In:  12.83 Mbps ( 1%) Cur Out:  24.91 Mbps ( 2%)
                                Thu Apr 25 16:23:06 2013
```



GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO red.es RedIRIS

DDOS.

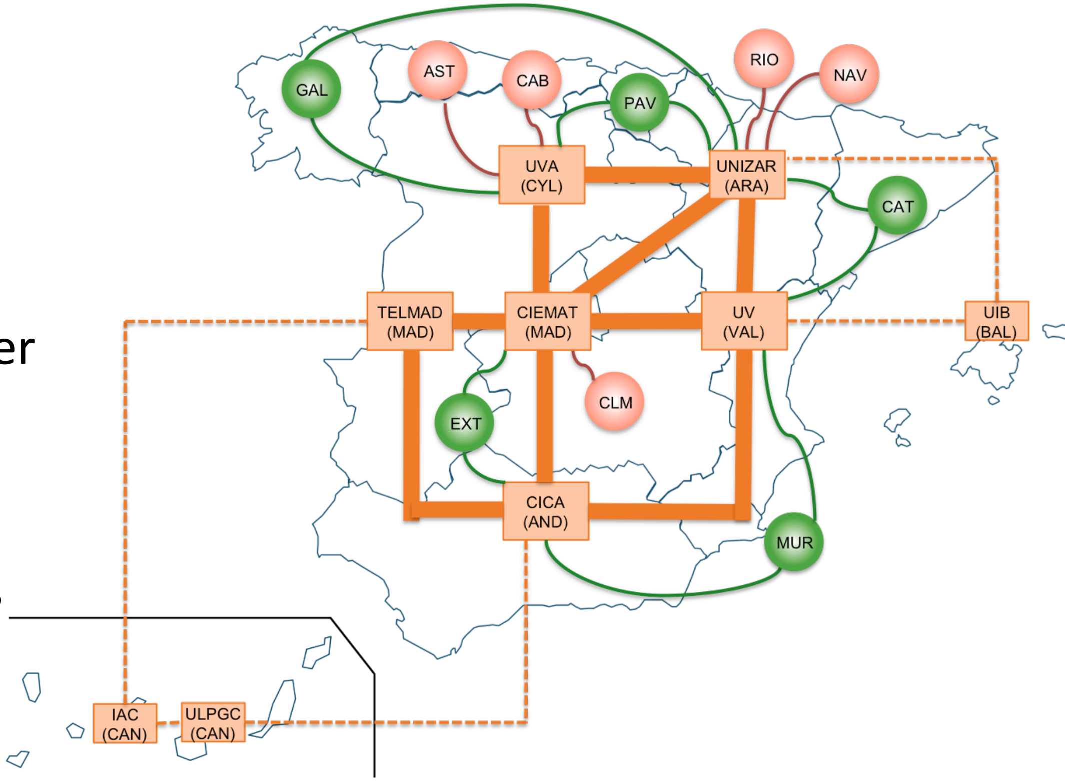
- What we learn..
  - To prepare in advance for the DDOS.
    - Traffic monitoring, what is the “normal” traffic.
    - Prepare (In advance) filtering rules.
    - Define the contact point
      - Internally
      - Externally
  - Prepare mitigation &contention strategy.

MITIGATION TOOLS

Improving DDOS mitigation

With the deployment of RedIRIS-Nova a DDOS

- Configure RedIRIS-Nova backbone for BGP filtering capabilities.
- Provide tools for RedIRIS CSIRT & Organizations to analyze the traffic..
- Implement a cleaning center in case of DDOS attacks.
- Prepare in advance against DDOS against critical resources for organizations
- Provide services for our organizations



BGP filtering capabilities.

Allow CSIRT team to apply filtering and traffic redirection in RedIRIS-Backbone

- Separate route server reflector from NOC team.
- Allow to diverge traffic to other networks nodes using BPG announces.

Successfully applied in security operations.

- Temporally block of compromised sites
- Re-routing DNSchanger traffic
- malware download blocks

BGP filtering capabilities

From this filtering tools we have started to provide a auto filtering tool for the universities.

- Allow Organizations to drop incoming traffic to their IP address space.
- Use a peering session with a separate route server.
- Useful in DDOS against some internal servers or less important services.

Expecting to add flowSpec announces to provide real blocking

Tool for visualization

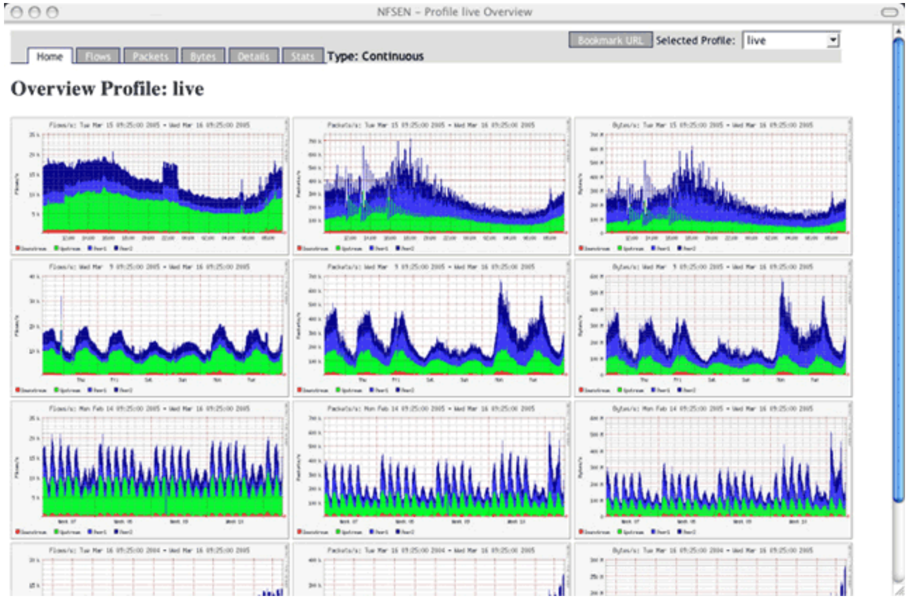
Need tools to monitor and visualize the traffic both for RedIRIS and their organizations

Expertise in the Organizations connected a RedIRIS was not uniform.

- Some organizations has good visibility of their traffics.
- But unfortunately others need rely only in the information provided by us.

Tool for visualization

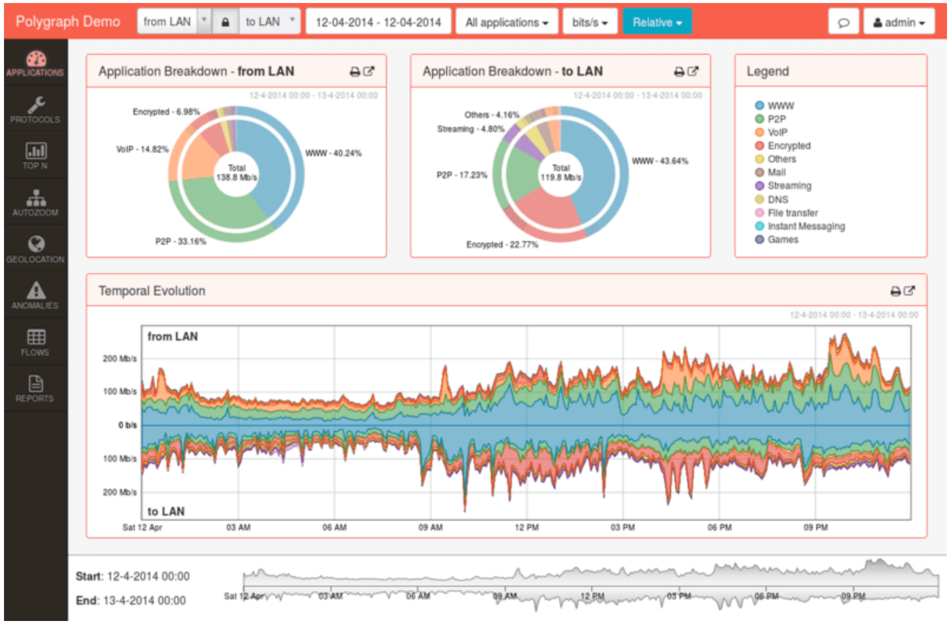
- The old solution based on NFSEN were not practical.
  - Traffic information (flows) is sampled, instead of complete.
  - There was too much organizations to provide a view for each one.
  - Slow queries & processing with the normal incident handling
  - Need to add external authentication



Overview Profile: live

Tool for visualization: Polygraph.io

- Federated access for the organizations.
- Works well with sampled traffic
- Custom database of IP addresses/ports to categorize the Application running
  - Allow to also use a probe to analyze protocols & traffic



Start: 12-4-2014 00:00

End: 13-4-2014 00:00

Tools for visualization

Use FlowSonnar from Team-Cymru for incident handling service.

- No economic cost
- Use their own compromised & botnet feed for CSIRT incident handling
- Enough for daily incident handling
- Nfen based

Tools for visualization

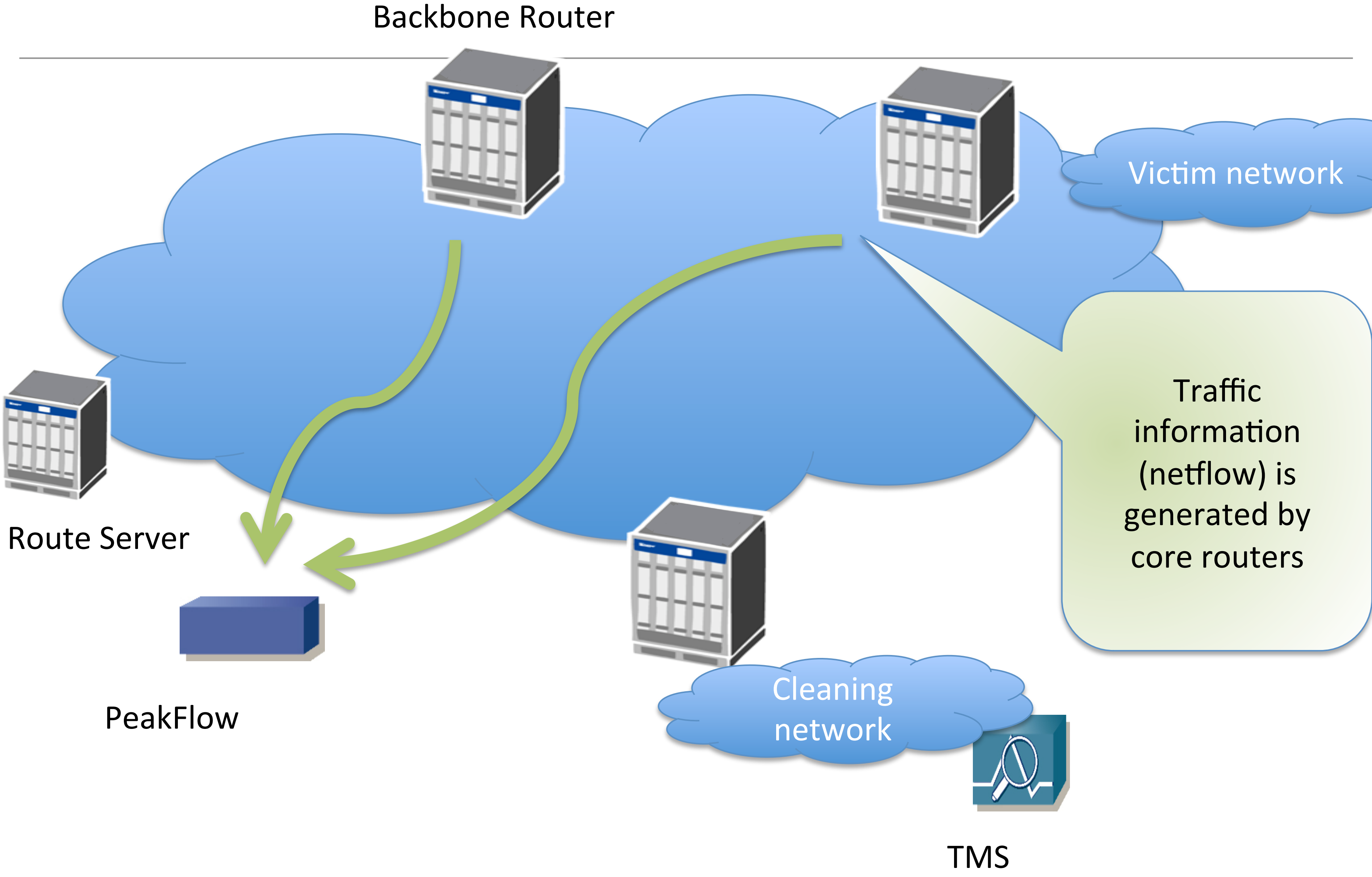
Use Arbor Peakflow for internal monitoring of traffic

- More focused on DDOS
- Combined with TMS to provide a DDOS cleaning facility
- Useful also for NOC people to analyze peering traffic and problems.
- Good API for reporting
- Price is high

Tools for visualization & cleaning center

Using Arbor TMS

- Isolated from the operational RedIRIS infrastructure
    - Different location
    - Router directly connected to our core routers
    - Gre tunnels directly to customers or regional networks
    - Mitigation strategy combined TMS with traditional filtering in the router



Backbone Router

Victim network

Traffic information (netflow) is generated by core routers

Route Server

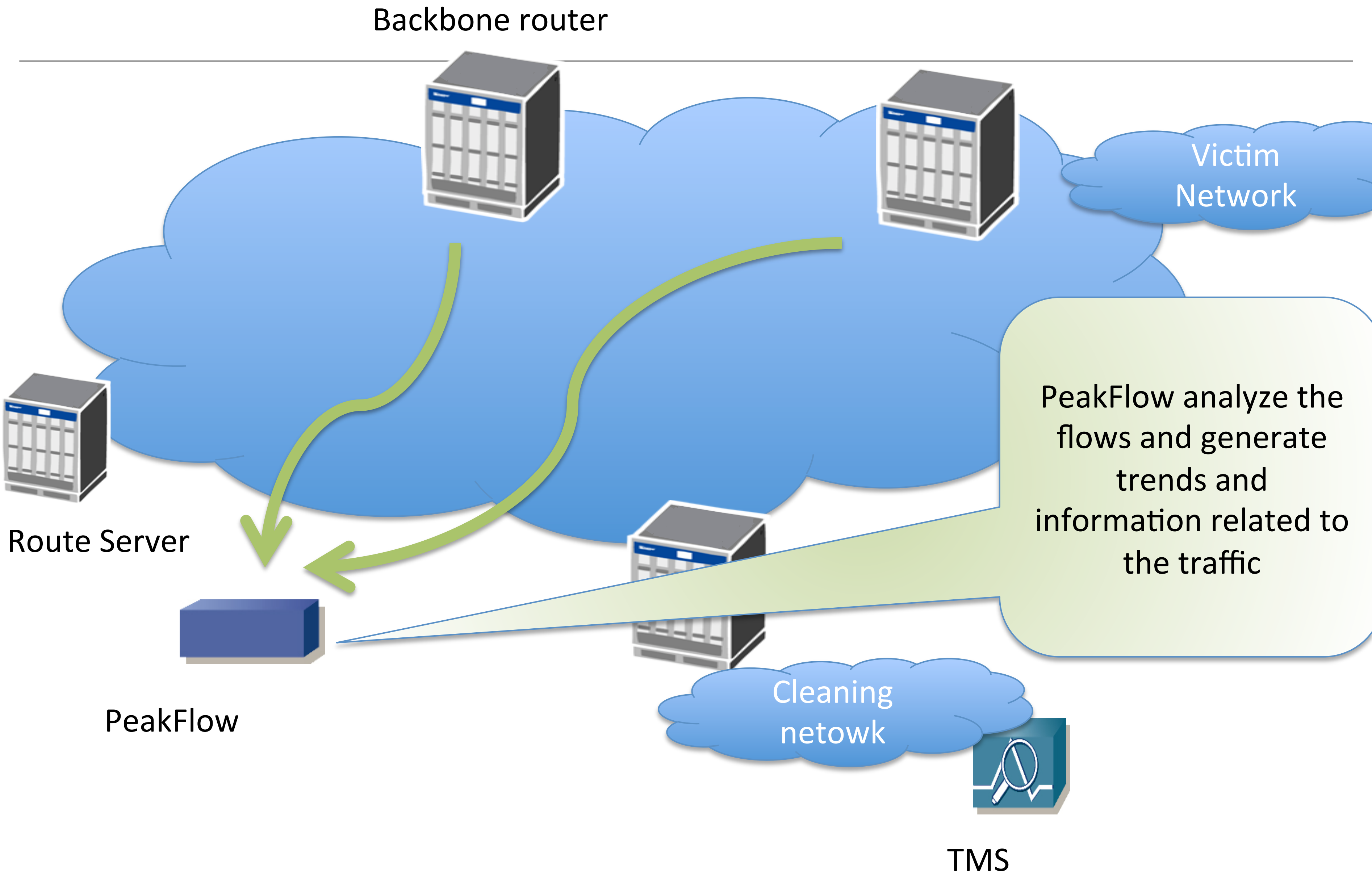
PeakFlow

Cleaning network

TMS

Arbor SP

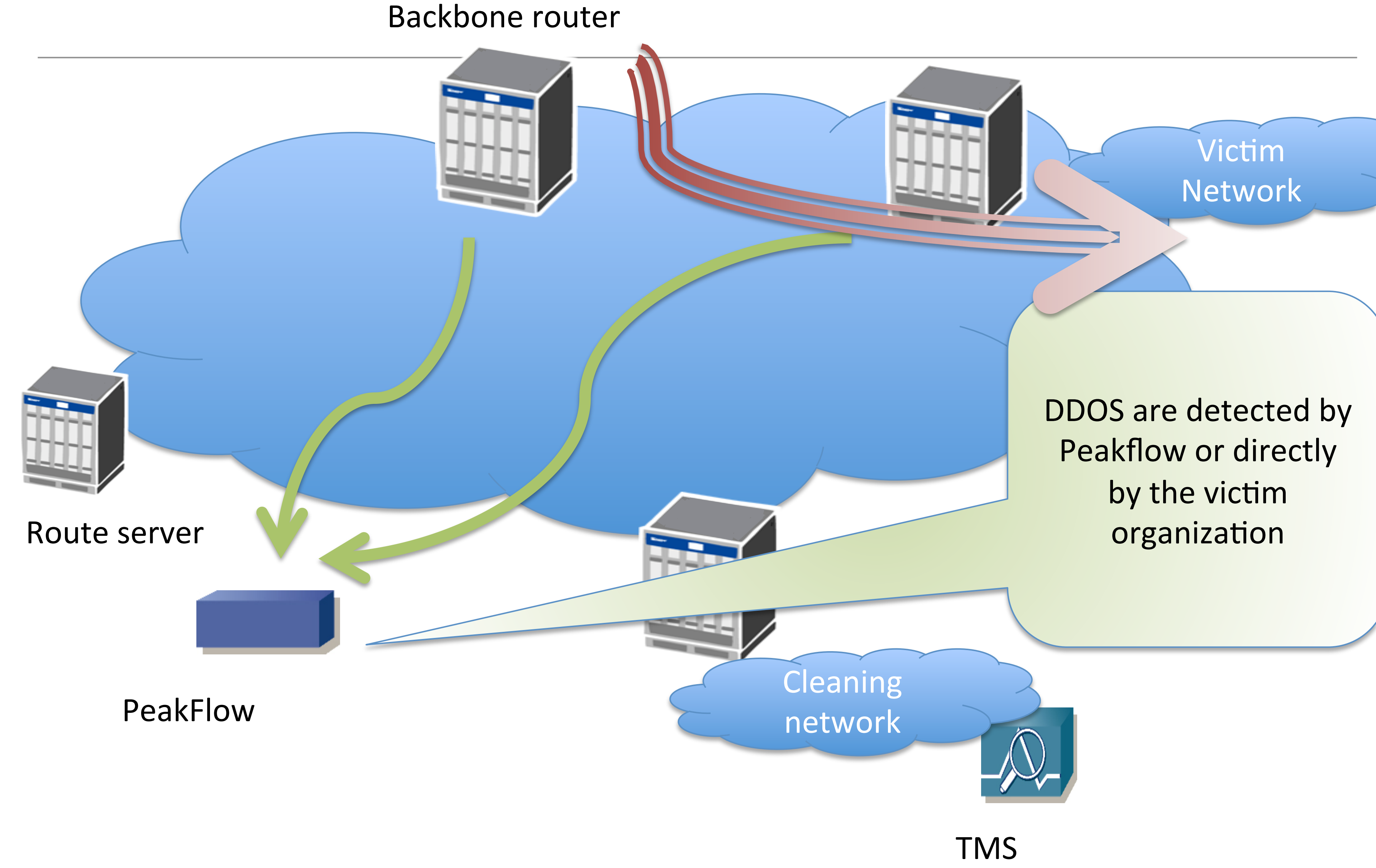
Arbor TMS



PeakFlow analyze the flows and generate trends and information related to the traffic

Arbor SP

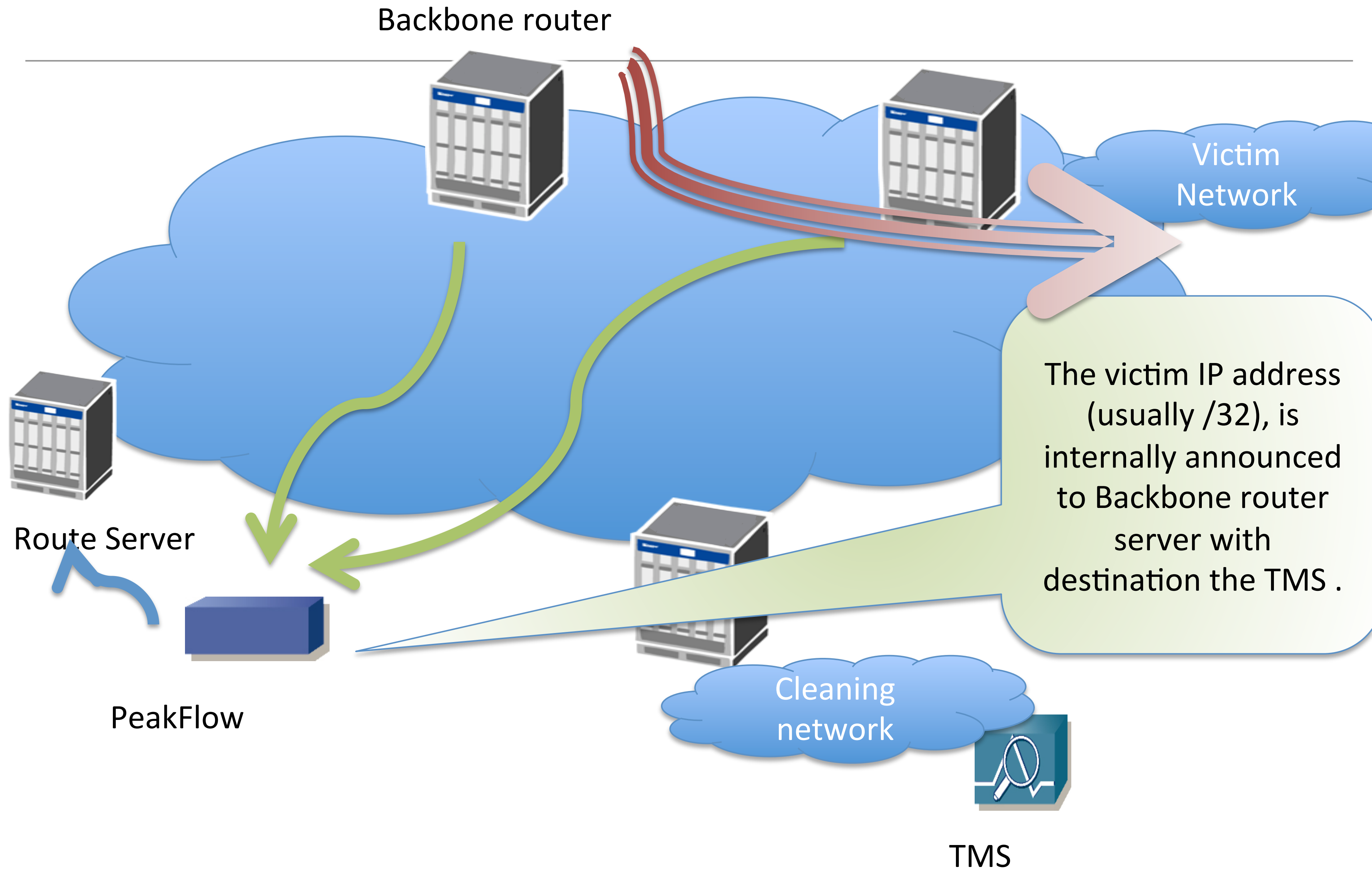
Arbor TMS



DDOS are detected by Peakflow or directly by the victim organization

Arbor SP

Arbor TMS



Backbone router

Victim Network

Route Server

PeakFlow

The victim IP address (usually /32), is internally announced to Backbone router server with destination the TMS .

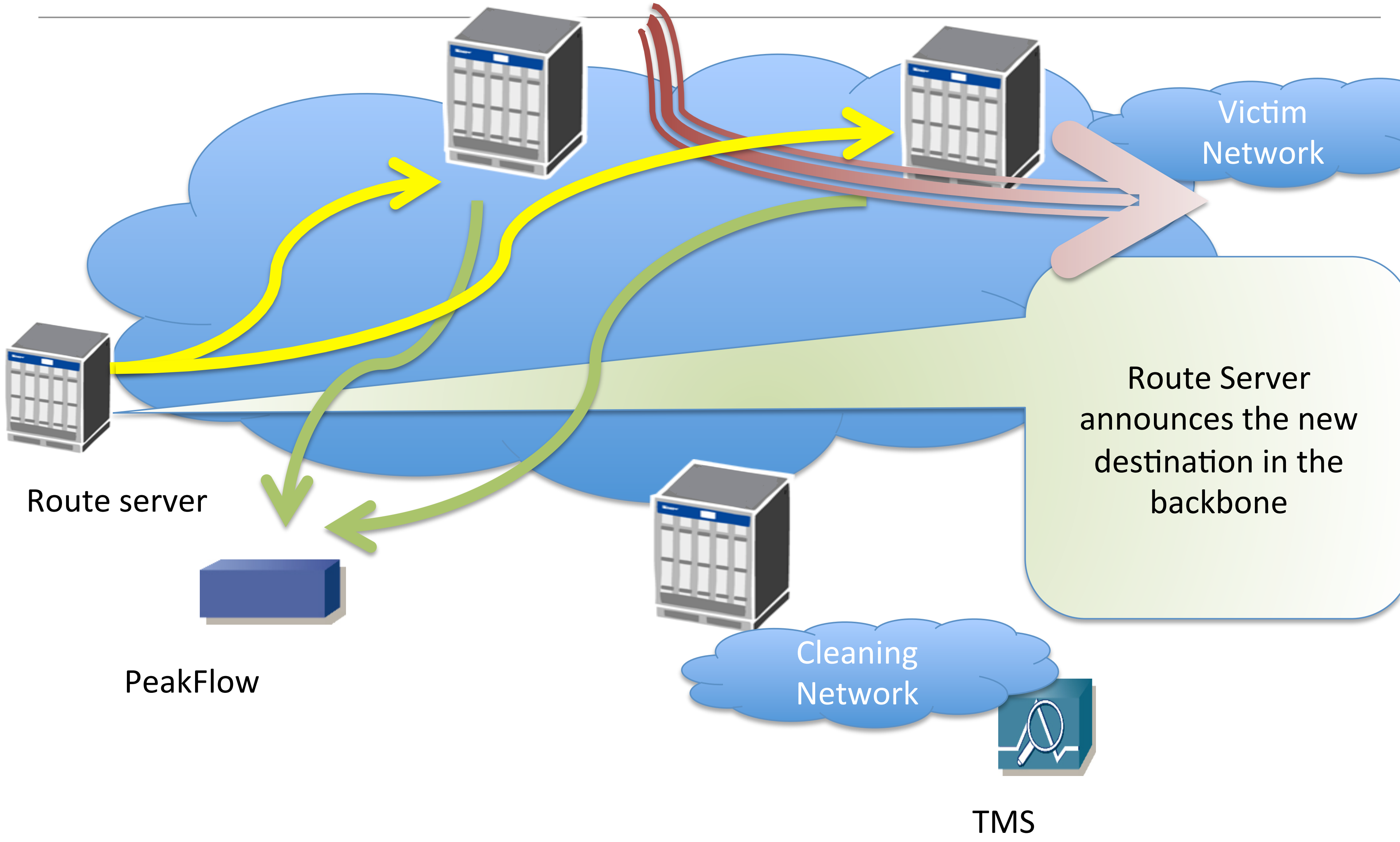
Cleaning network

TMS

Arbor SP

Arbor TMS

Backbone Router



Victim Network

Route Server announces the new destination in the backbone

Route server

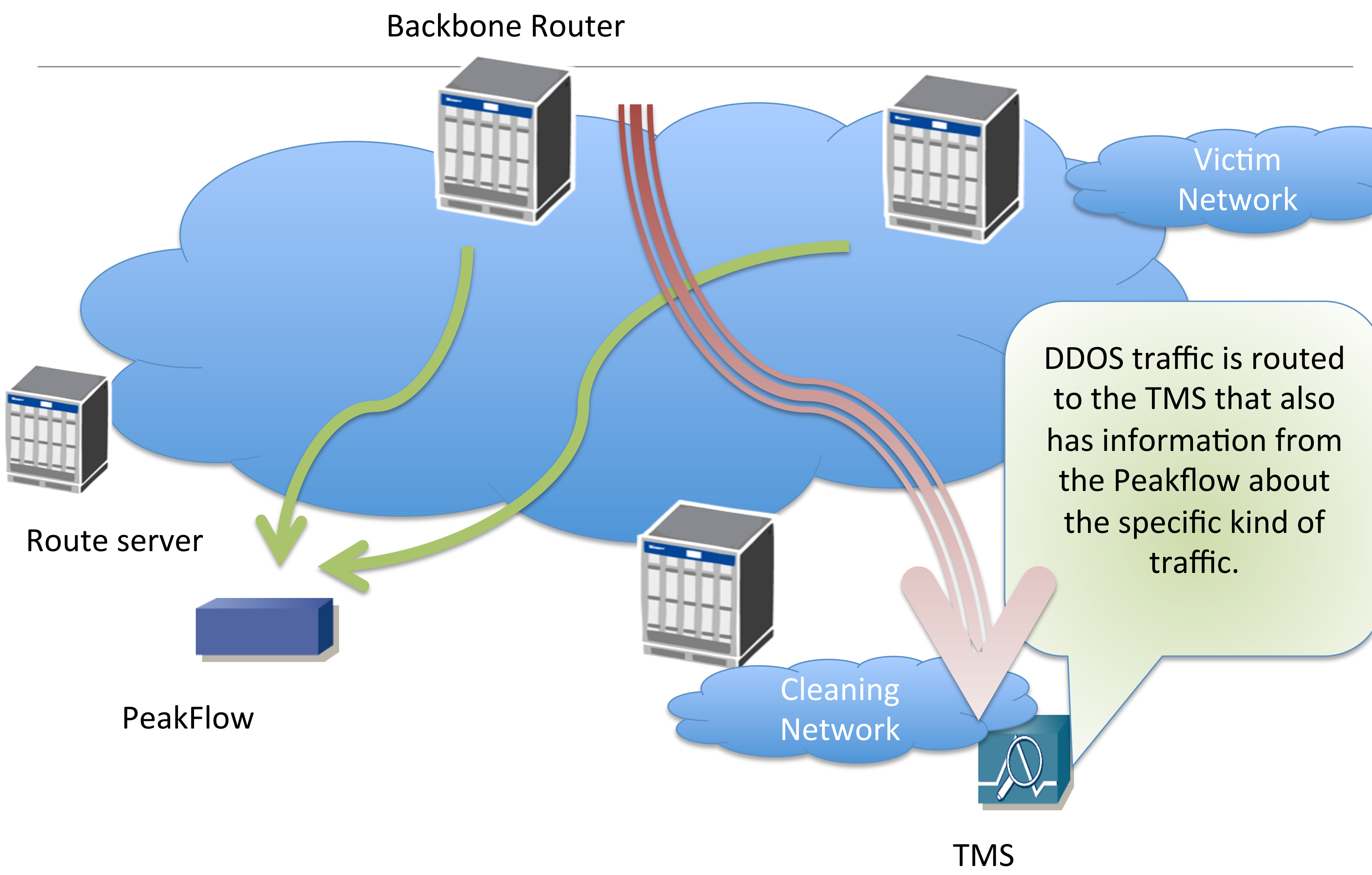
PeakFlow

Cleaning Network

TMS

Arbor SP

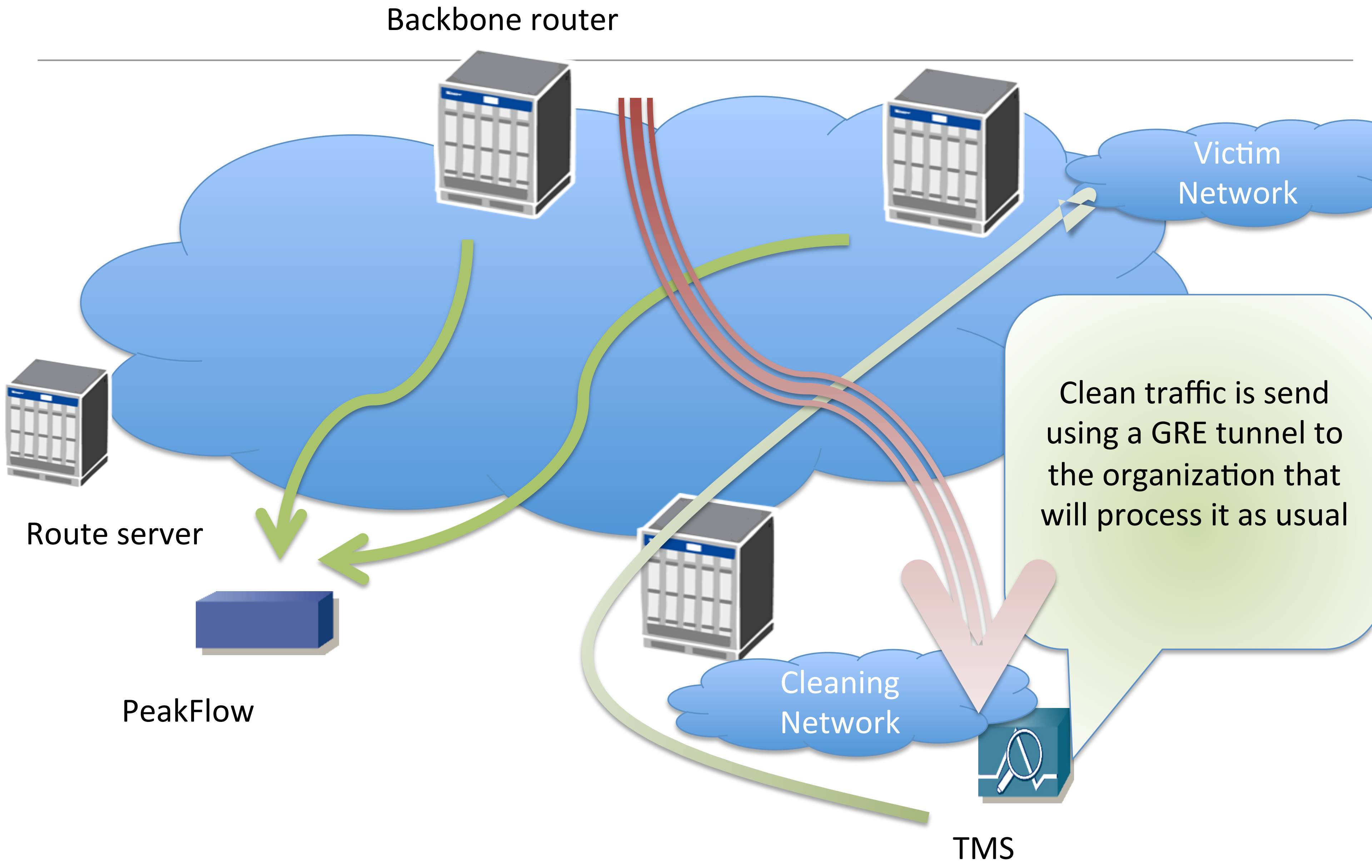
Arbor TMS



DDOS traffic is routed to the TMS that also has information from the Peakflow about the specific kind of traffic.

Arbor SP

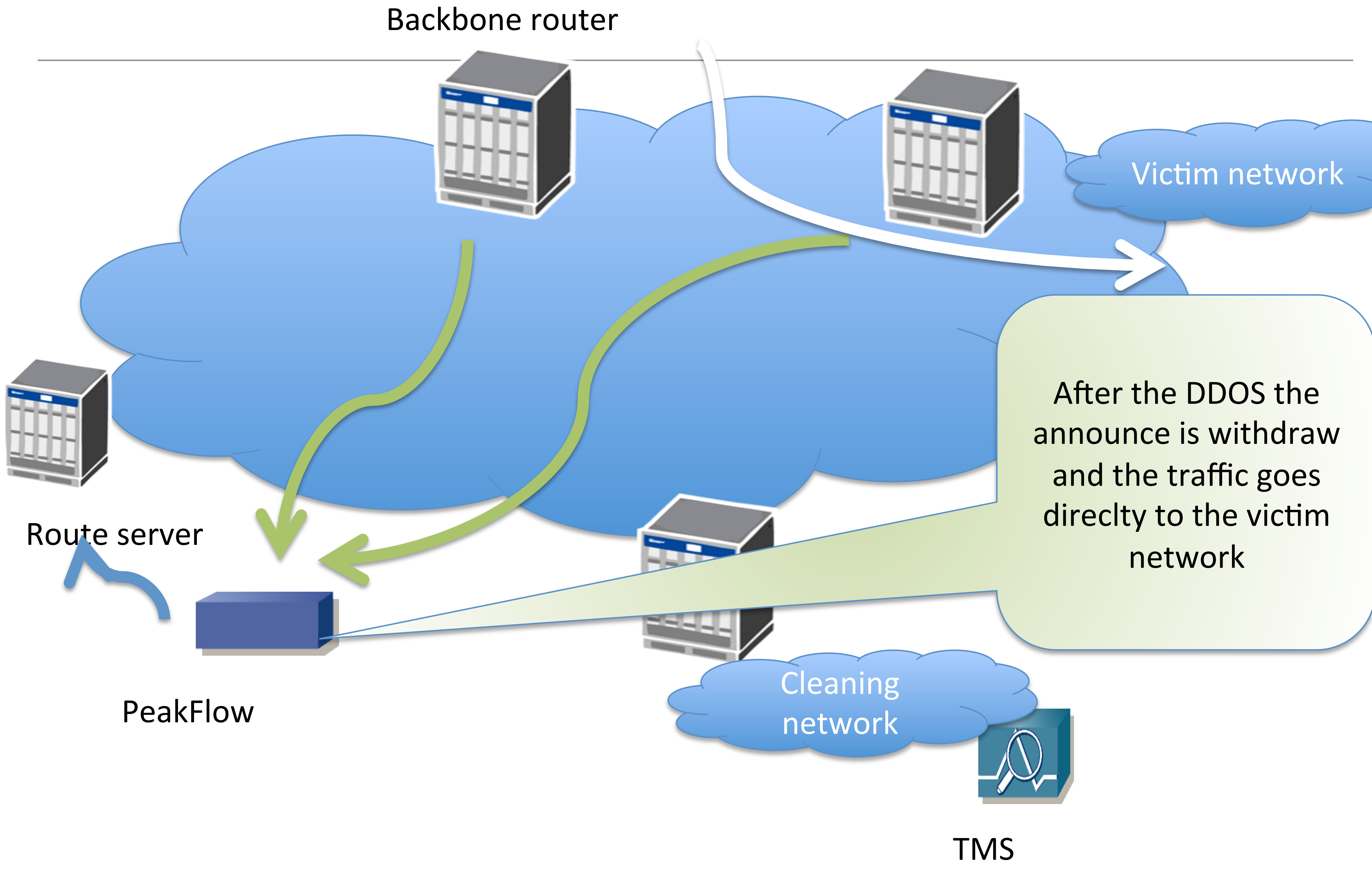
Arbor TMS



Clean traffic is send using a GRE tunnel to the organization that will process it as usual

Arbor SP

Arbor TMS



After the DDOS the announce is withdraw and the traffic goes direclty to the victim network

Arbor SP

Arbor TMS

CURRENT DDOS STRATEGY

Services

We are not still not listing anti-DDOS capabilities in our customer portfolio.

- No 20x7 SOC than could analyze and detect the attacks.
- But we are running a test phase in a best support mode with some organizations
  - Support with the regional NRENs
  - First steps to prepare the service

- Still using traditional ACL

DDOS STRATEGY: information

Organizations need to provide:

- what resources need to be protected ?
- what is the expected traffic ?

With this information:

we can prepare custom filters to mitigate common amplification DDOS attacks.

Create monitoring objects to detect traffic anomalies.

DDOS strategy: cleaning center

We need to stabilish a GRE tunnel outside our backbone for the clean traffic

- Regional Networks can provide the tunnel directly
- In other cases organizations use their equipment for the tunel
- Traffic redirection is verified with test address

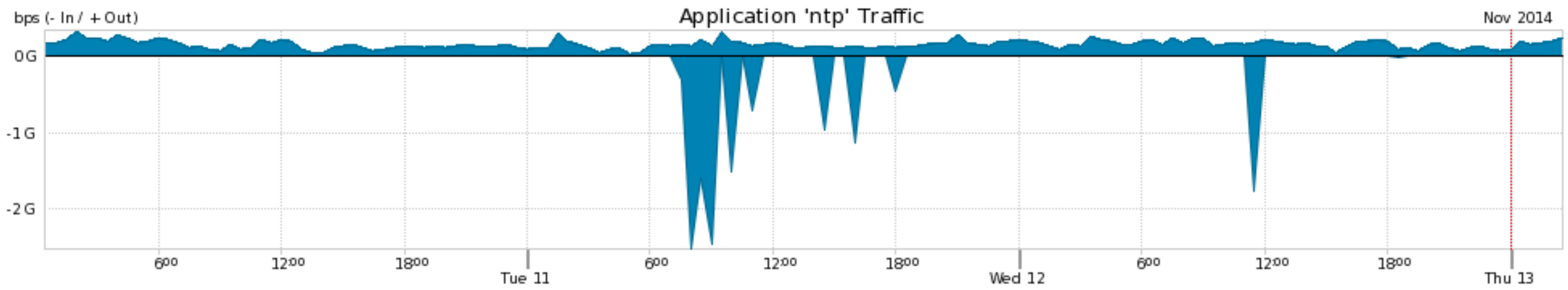
About 10 networks (17 objects) protected

DDOS strategy: upstream carrier

- Improve communications with our upstream carrier.
  - Tested the GEANT FoD tools
- Verify the DDOS procedures with other carriers & IX

Current status

- After a year of Arbor deployment we haven’t suffered a major DDOS attack.
- There was some short time DDOS not reported by organizations
- Mostly amplification attacks



Future works

- Continue working on the deployment of the cleaning center
  - Add more organizations
  - Get more experience on DDOS
  - Train our customers
- Participate in other global projects.
  - Team Cymru UTRS service
  - Geant FoD
- Start testing FlowSpec

¡Muchas gracias!

RedIRIS

Más de 25 años al servicio de la investigación