DDoS mitigation @ CIX

Mario Klobučar, SRCE

CEE Peering Days

Ljubljana, 22nd – 23rd March 2017

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

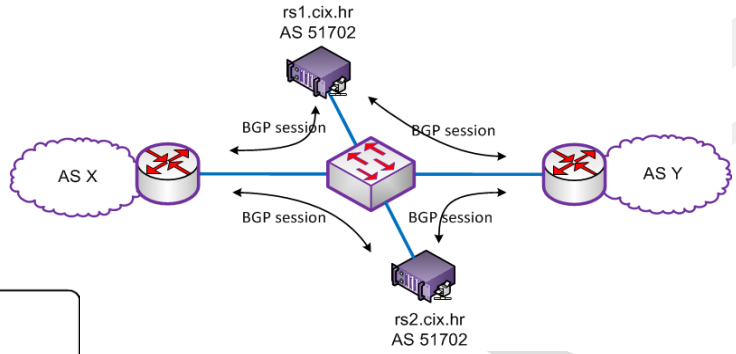
Content

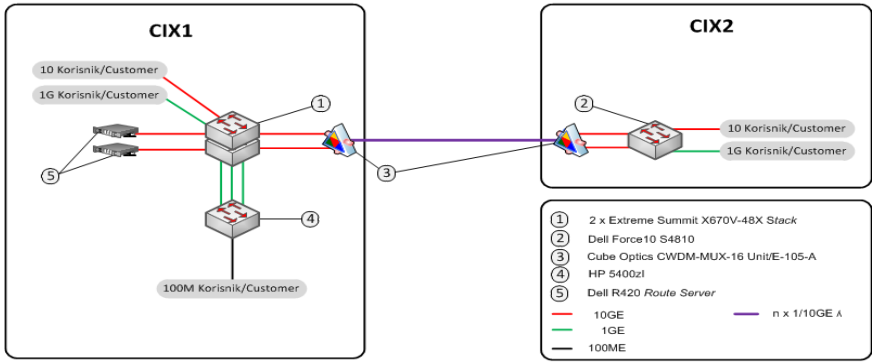
- About CIX
- Blackholing@CIX
- Future (possible) mechanism for mitigating DDoS

About CIX – Croatian Internet eXchange

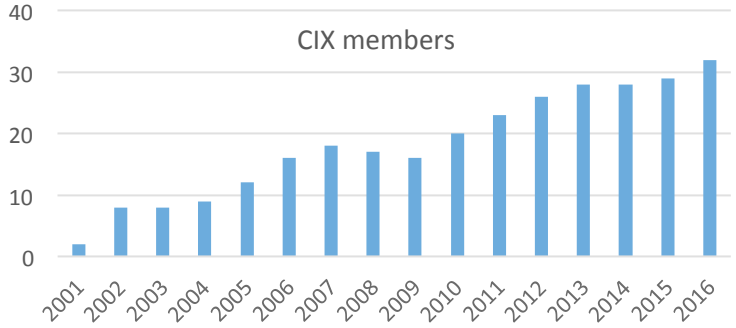
- Founded in 2000
- Neutral, not-for-profit
- Located in Zagreb (distributed on two locations)
- Run by SRCE – University computing centre, University of Zagreb
- 35 members (Status on: 1 Feb 2017)

CIX infrastructure

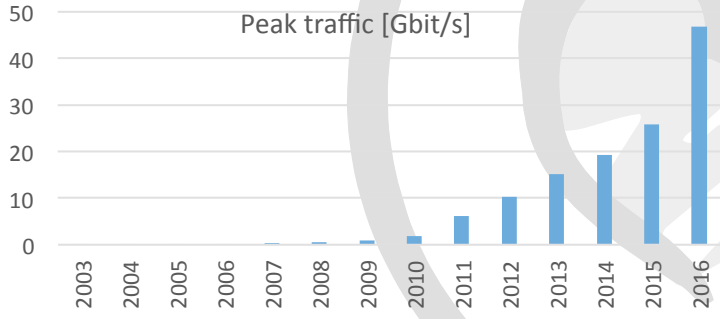




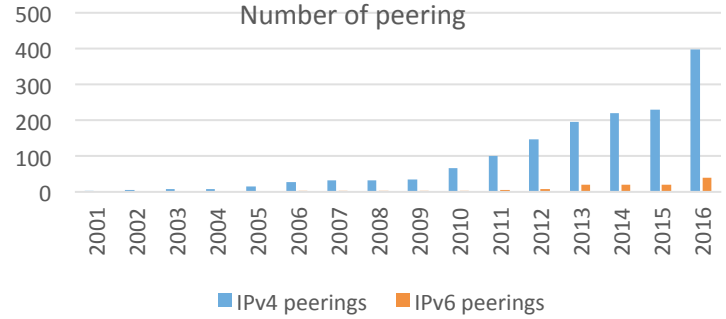
CIX through numbers

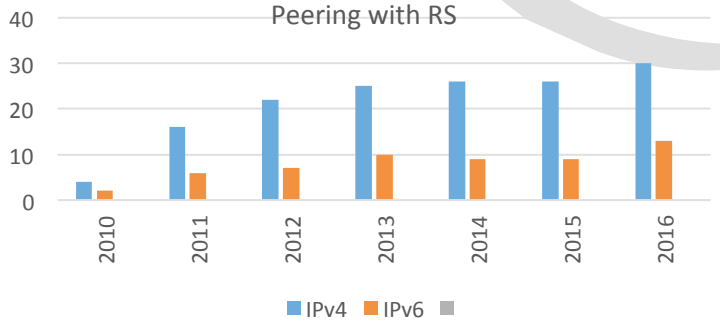


https://www.cix.hr/en/members/members



http://www.cix.hr/en/about-cix/traffic-statistics/historyka





http://www.cix.hr/en/services/peering-matrix

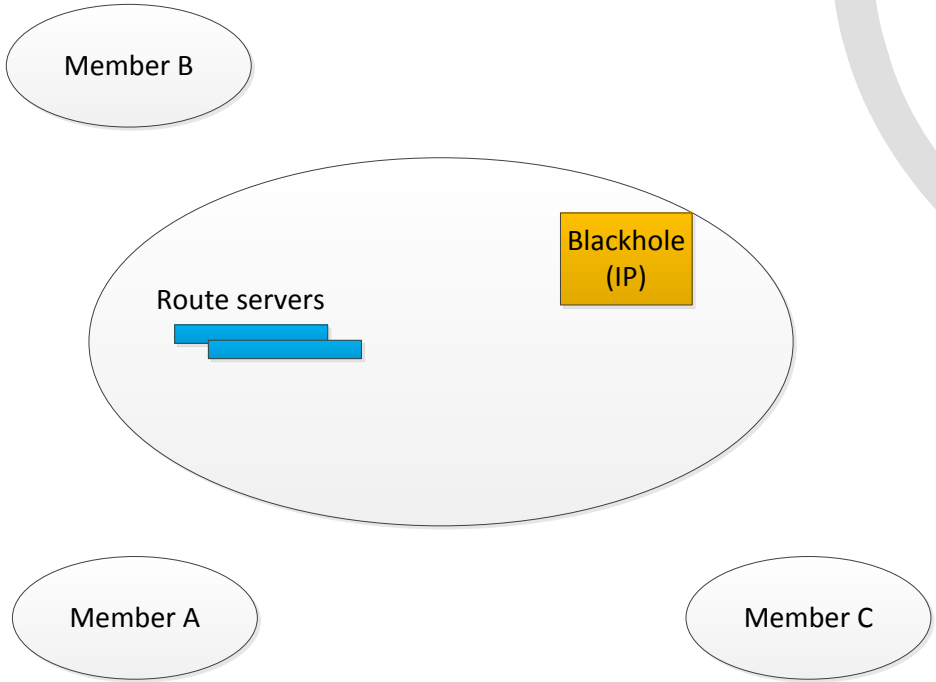
Members demand

- In general - no huge spikes in traffic
- One member constantly asked for a Blackholing service. „We are using them on our upstream, and we would like to have similar mechanism in CIX”
- We have heard that once there was some spoofing attack. We offered to look at problem but we did not recieve any details about problem (time, networks ..)
- Members discussed on this problem at the CIX Council, and most of them told us that they will like to see some DDoS mitigation (blackholing) @CIX

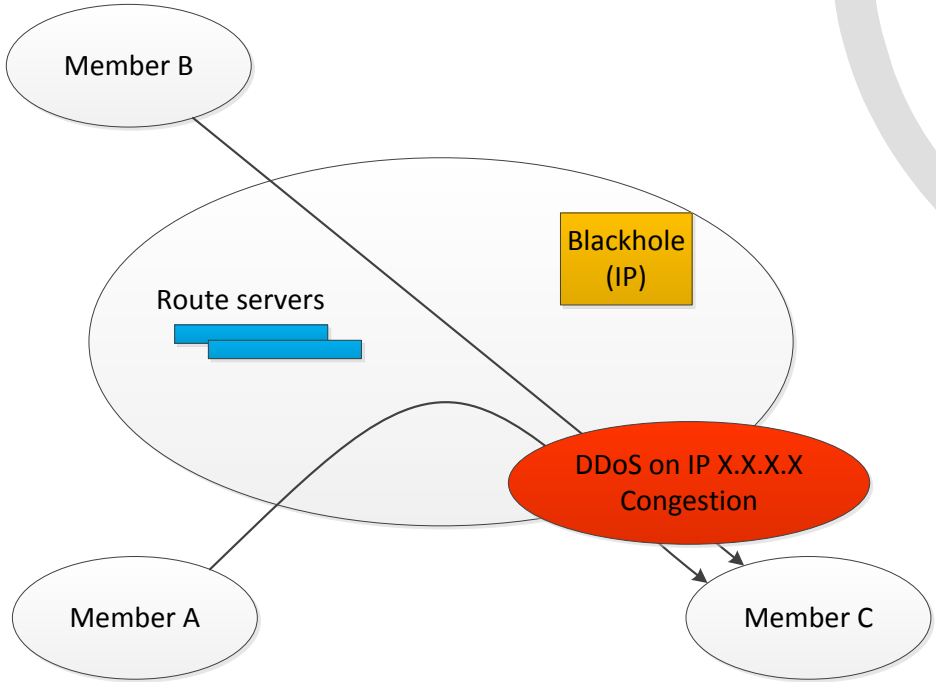
Blackholing@CIX

- We use the IETF draft „BLACKHOLE BGP Community for Blackholing“ https://tools.ietf.org/html/draft-ietf-grow-blackholing-03
- Attacked member is using community 65535:666 and can send prefix up to /32
- Route servers are changing next-hop for this prefix to Backhole IP
- CIX switches dropping the traffic to the Blackhole IP MAC using MAC acl on ingress

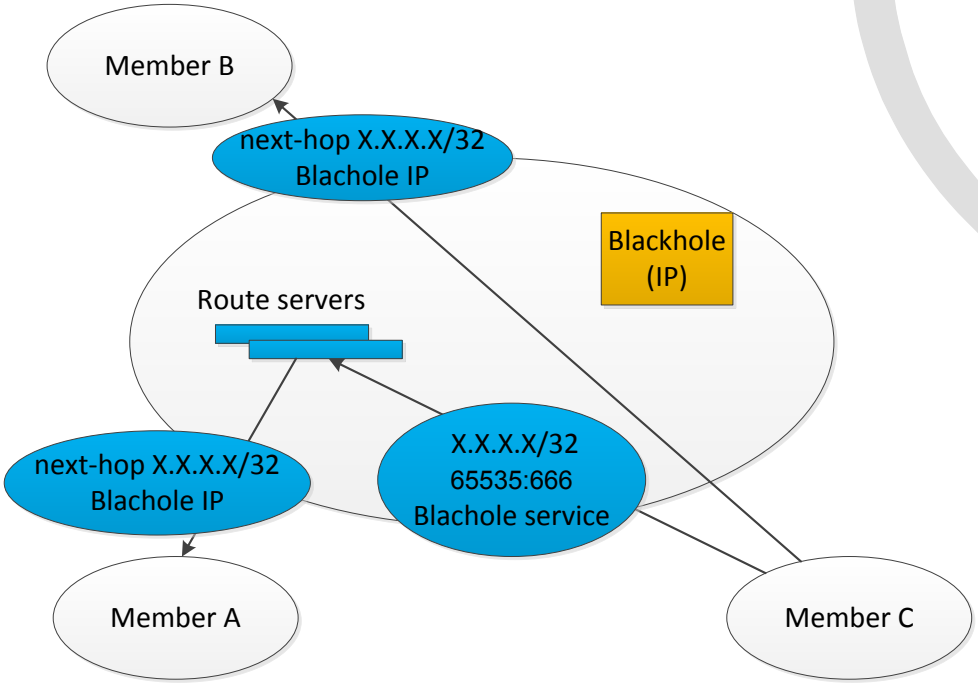
Blackhole flow (1)



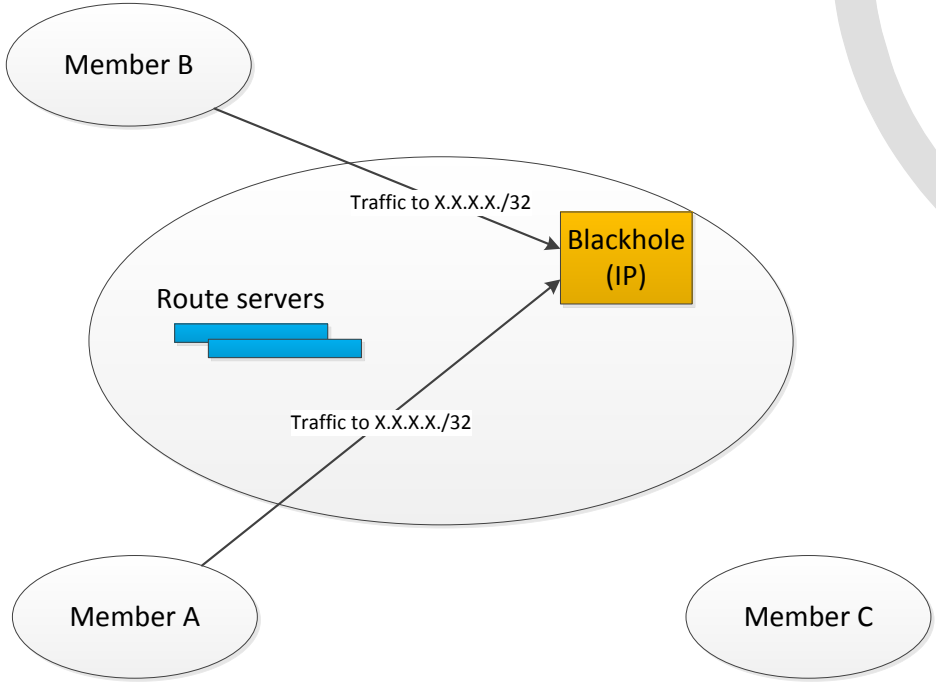
Blackhole flow (2)



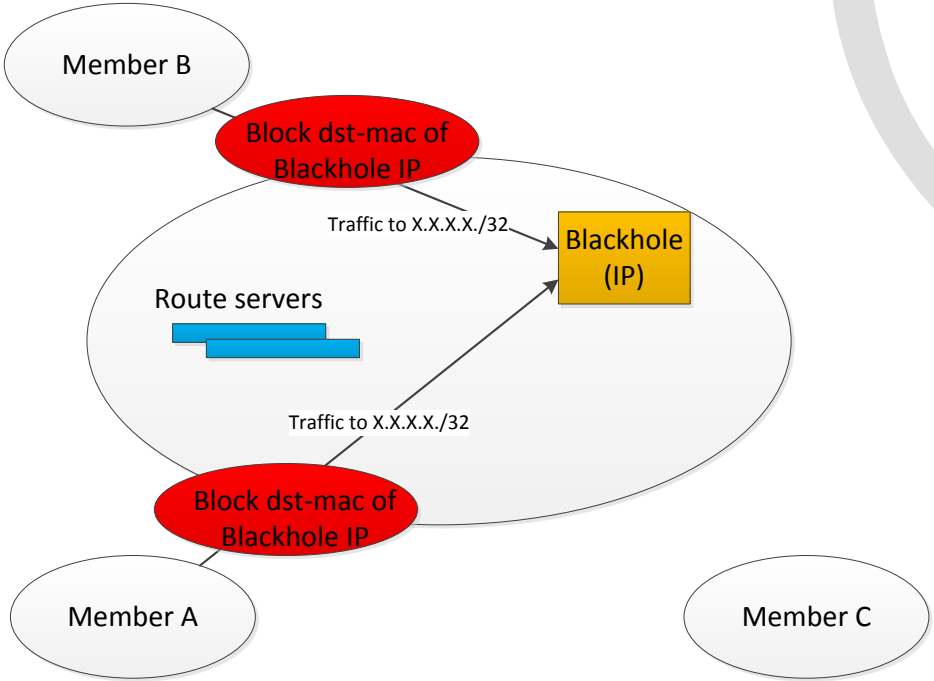
Blackhole flow (3)



Blackhole flow (4)

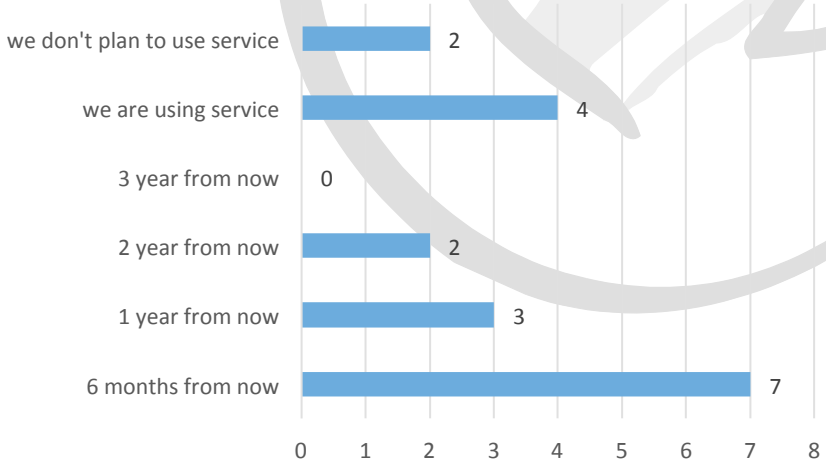


Blackhole flow (5)



Observations and 2016 survey

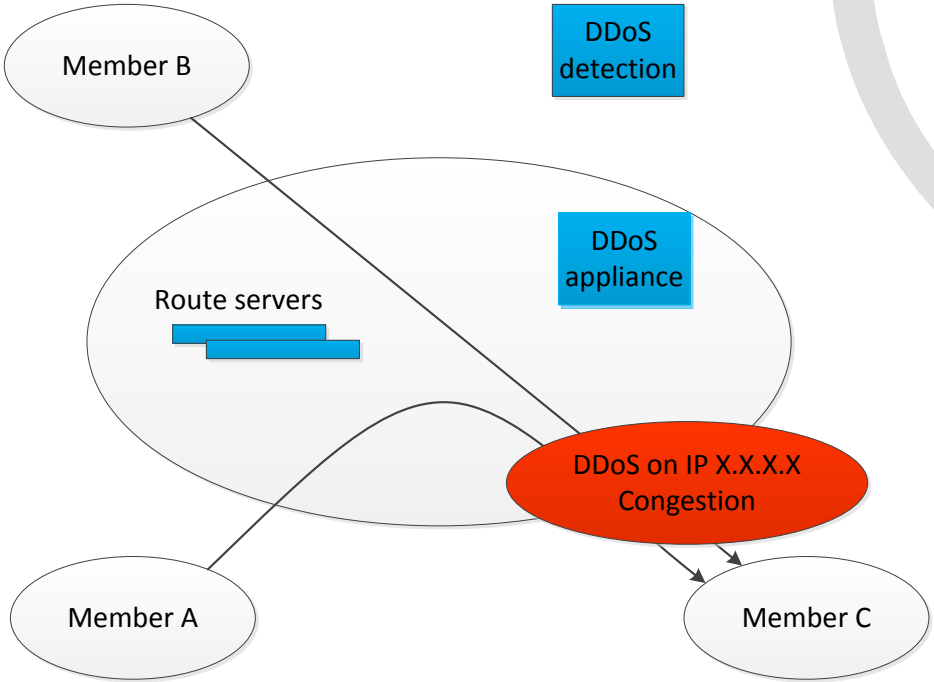
- 2016 member questionnaire
  - (17 members answered),
  - Question was : „When do you plan to use Blackholing@CIX service ?”
- We didn’t observe “huge” activities (in route server logs, or packet counters on switch acl)
- We are still „blind” to see some small volumetric or slow attacks



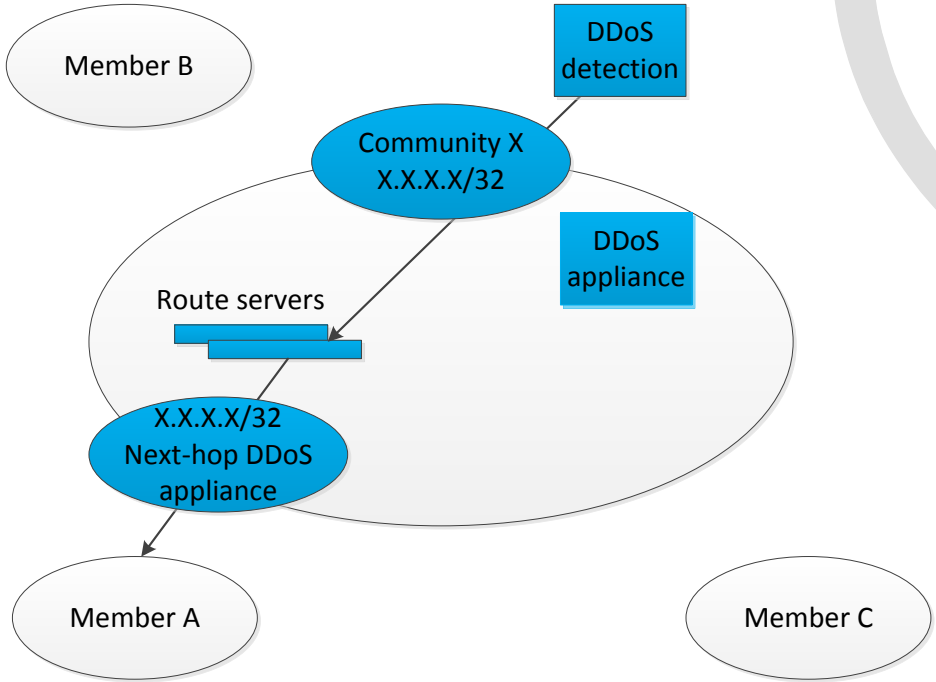
Future plans - wishlist

- Testing sFlow analyzers
  - to see how many attacks we have ?
  - can we spot a small or application attacks ?
  - can those tools have operator/automated mitigation ?
  - are those tools have big pane for CIX (that we can react when CIX services for all members are degraded), and small pane for each members (so they can resolve their problems) ?
- Can we add some DDoS appliance instead of blackhole to *clean* instead of *dropping* the traffic
- Build CIX service catalogue based on members requests/wishes

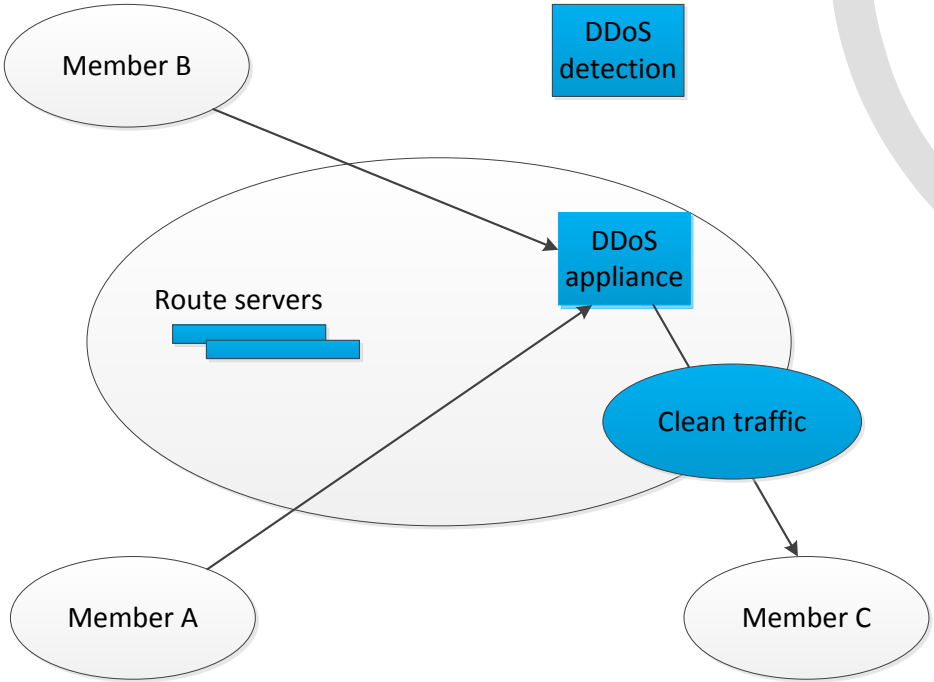
Something like this (1)



Something like this (2)



Something like this (3)



Questions ?

Thanks!

cix@srce.hr

www.cix.hr

www.srce.hr

srce
University of Zagreb
University Computing Centre

www.srce.unizg.hr/en

According to the Open Access Policy, Srce ensures that all research data made by Srce is accessible and free to use by the general public, especially educational and professional information and content derived from the actions and work of Srce.

www.srce.unizg.hr/oa-and-oer

srce
otvoreni pristup