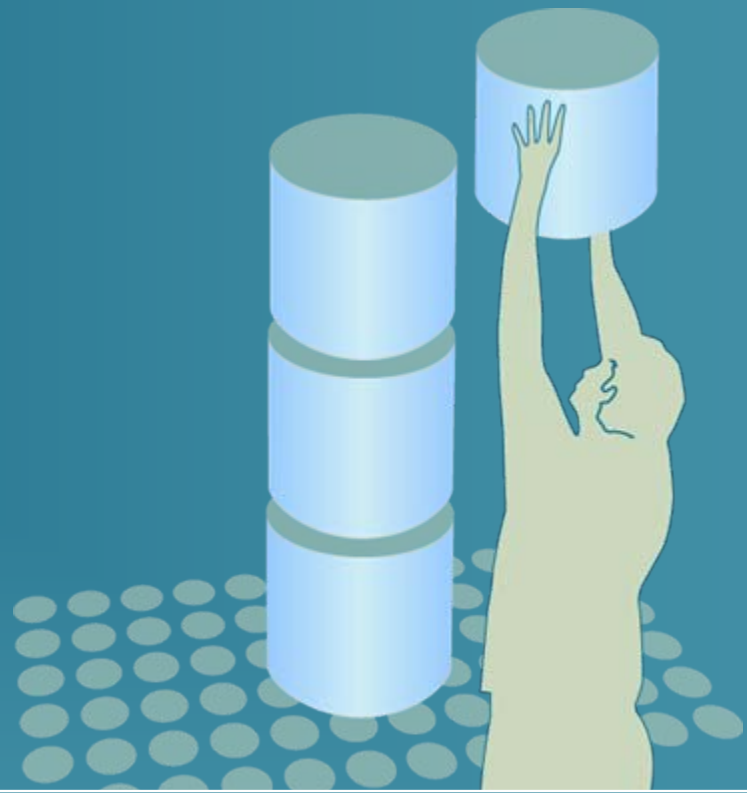
TeliaSonera



Hunting down a DDOS attack

By Lars Axeland +46 70 5291530
lars.axeland@teliasonera.com

TeliaSonera

2006-10-23

What we have seen so far

What can an operator do to achieve core security

What solution can an ISP provide as DDOS protection

What we have seen so far

- So far we have seen a few massive DDOS-attacks in aggregated size of 5-7Gbps. There has been larger attacks out on the internet.
- In the same rate as bandwidth utilization increases for private customers the attackers supervising a large among of BOT clients become extremely powerful and can cause massive damage.
- Also small intelligent attacks can tear down business critical service (typical banking, betting, …).
- ISP’s has reason to believe all kind of DDOS attacks can appear to its customers and their business critical services. Therefore your ISP has to provide these customer a fair solution of protection.

Protection of ISP core network!

Starting with the core:
How does an ISP achieve core security?

- Using specific scooped address structure for core links and loopbacks.
- Global protection shields to protect core infrastructure (Infra ACL)
- Node local protection shields of core infrastructure (rACL, Firewall, CoPP, DCoPP)
- BGP dampening, MD5 (bgp/igp), max-prefix, GTSM (Generic TTL Security Mechanism), prefix-filtering
- Spoofing mechanisms and filters on all ingress edge (Strict/Loose mode).
- Several overlapping layers of protection

Continue…..
How does an ISP achieve core security?

- Be sure you know your HW/SW characteristics
- Replace old HW with new ‘more to architecture’ security prepared
- Close communication with router vendors to secure SW
- It’s important to have a strict test/validation process (HW, SW, features ….)
- Protect our own critical services with a DDOS-protection mechanism (SIP-servers, DNS resolvers, Ext web, NOC …….)
- Train your NOC crew how to react on DDOS alarm

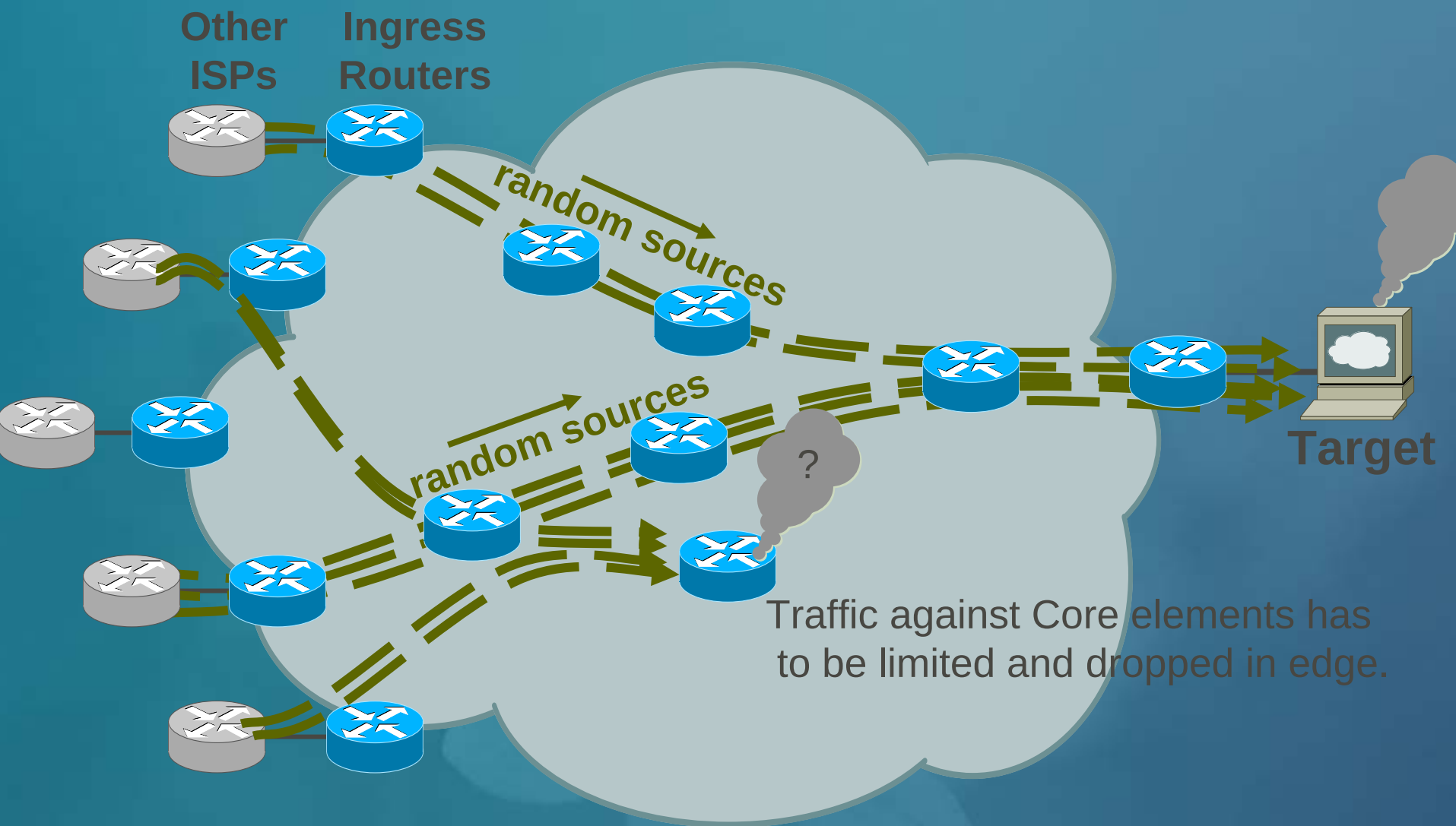
Tools/Techniques to use to prevent DDOS attacks

- Remotely Triggered Blackhole Routing
  - Based on destination address
  - Based on source address (in combination with uRPF loose)
  - Community based RTBH
  - RTBH of own CIDR block and Martians
  - RTBH in different AS

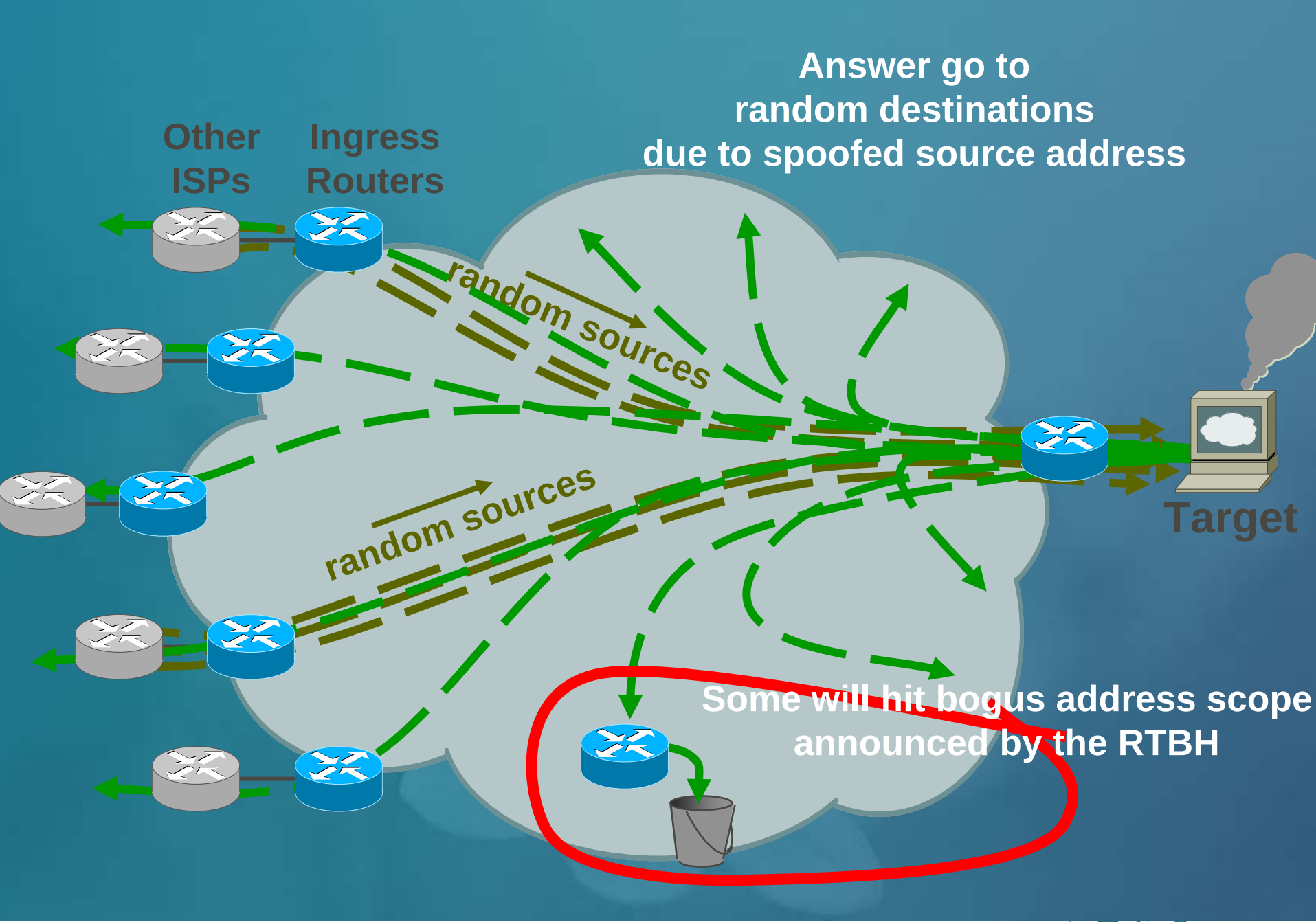
Tools/Techniques to use to prevent DDOS attacks

- Sinkhole Routing
- Using Remote SPAN to analyze traffic on ingress ports/vlan in edge
- Efficient Traffic Monitor System to measure abnormalities
- Centralized IP traffic DDOS Protection Mechanism (Scrubbing machine)
- If necessary redirect private customers to a zone where they only can reach patches for detected infected clients

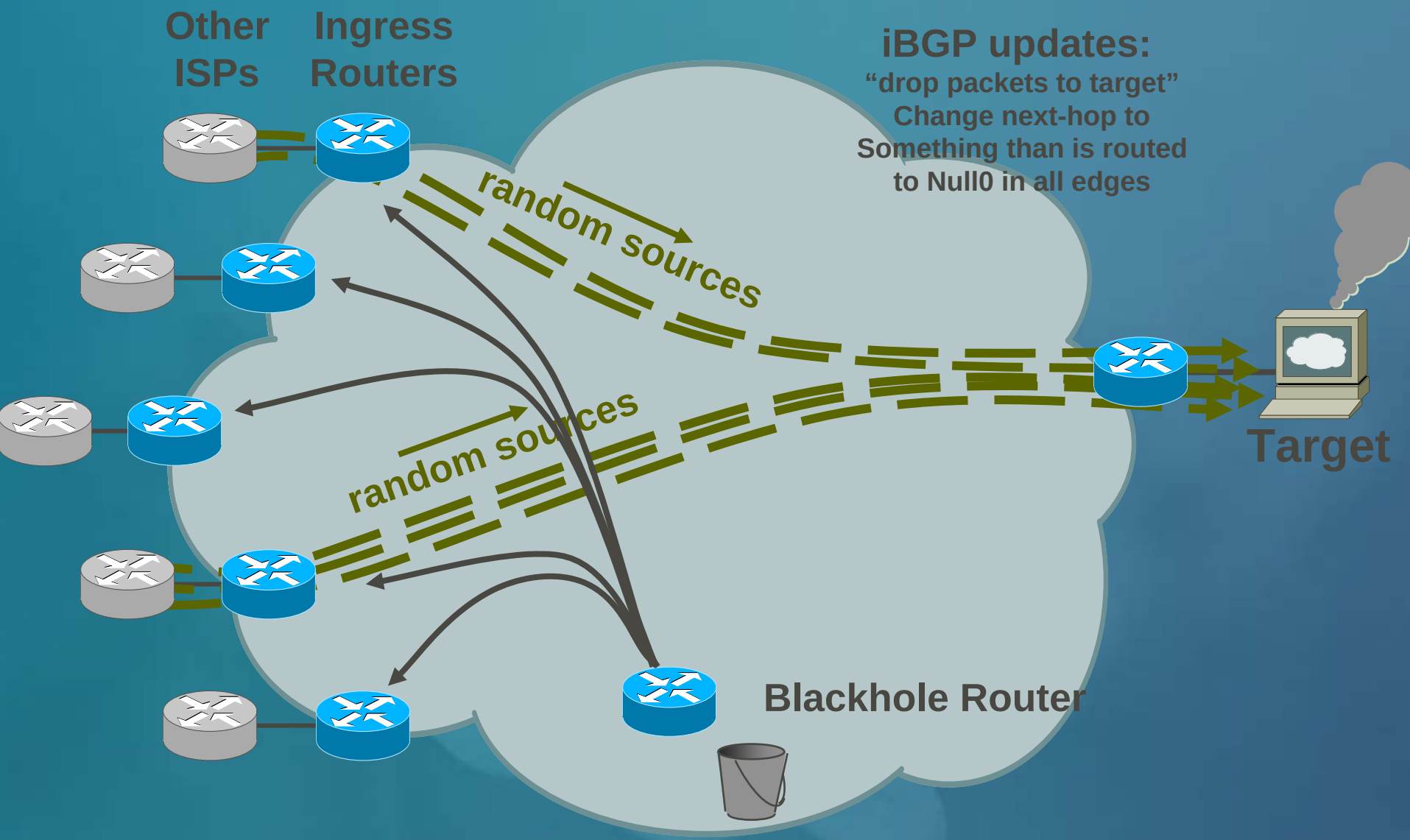
Typical Spoofed DDOS attack



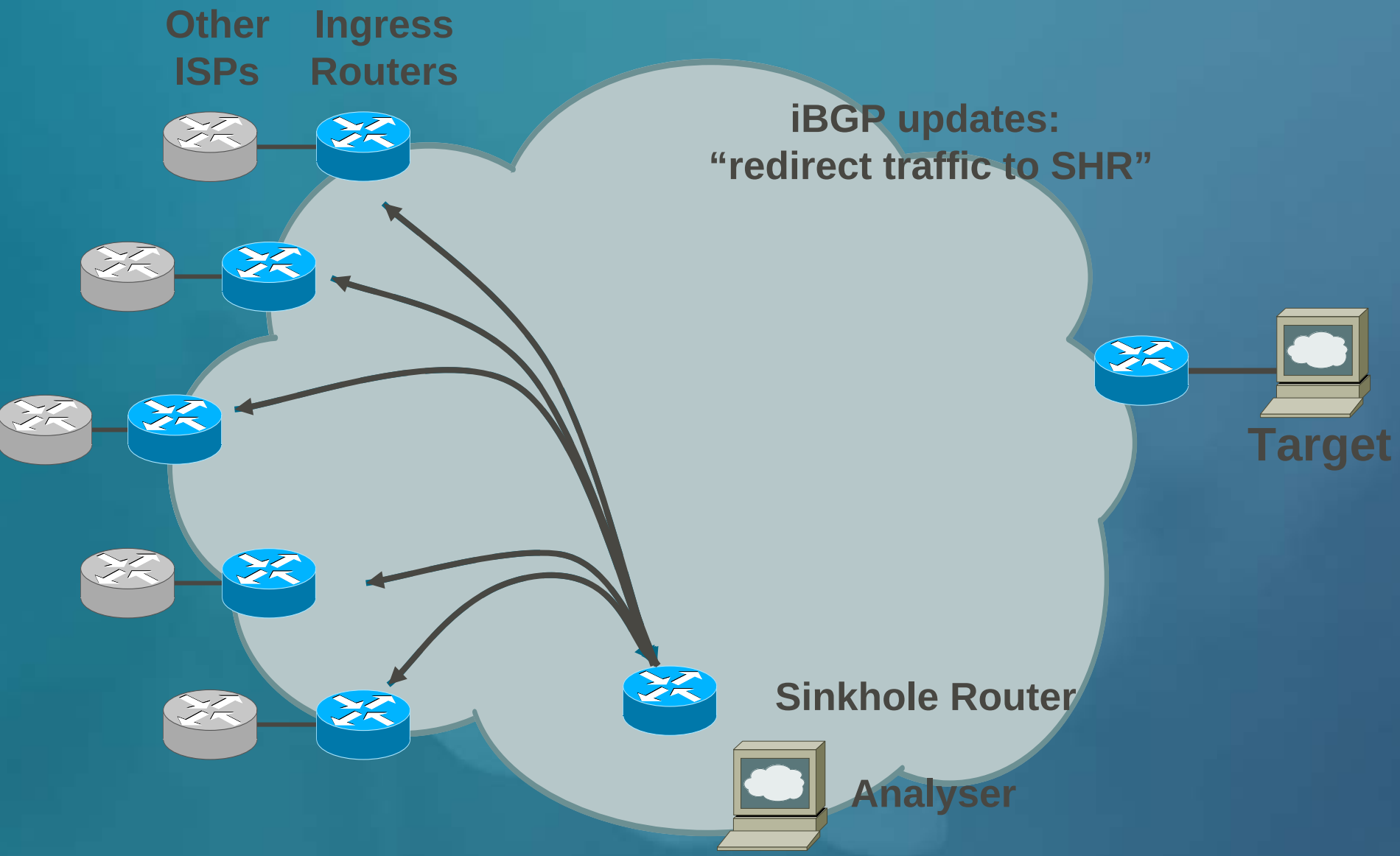
Traffic against Core elements has to be limited and dropped in edge.


Answer go to
random destinations
due to spoofed source address
Other
ISPs
Ingress
Routers
random sources
random sources
Target
Some will hit bogus address scope
announced by the RTBH

Use BGP to stop the attack in all edges:



Redirect traffic to Sinkhole Router:



Drawback of using RTBH

- Using RTBH based on the destination address (the victims source address) will definitely be an effective DDOS attack ☹.
- Using RTBH based on source-address is very manual and will effect the real owner of the spoofed source-addresses.
- Sophisticated attackers uses BOT's with if it's possible random spoofed source addresses.

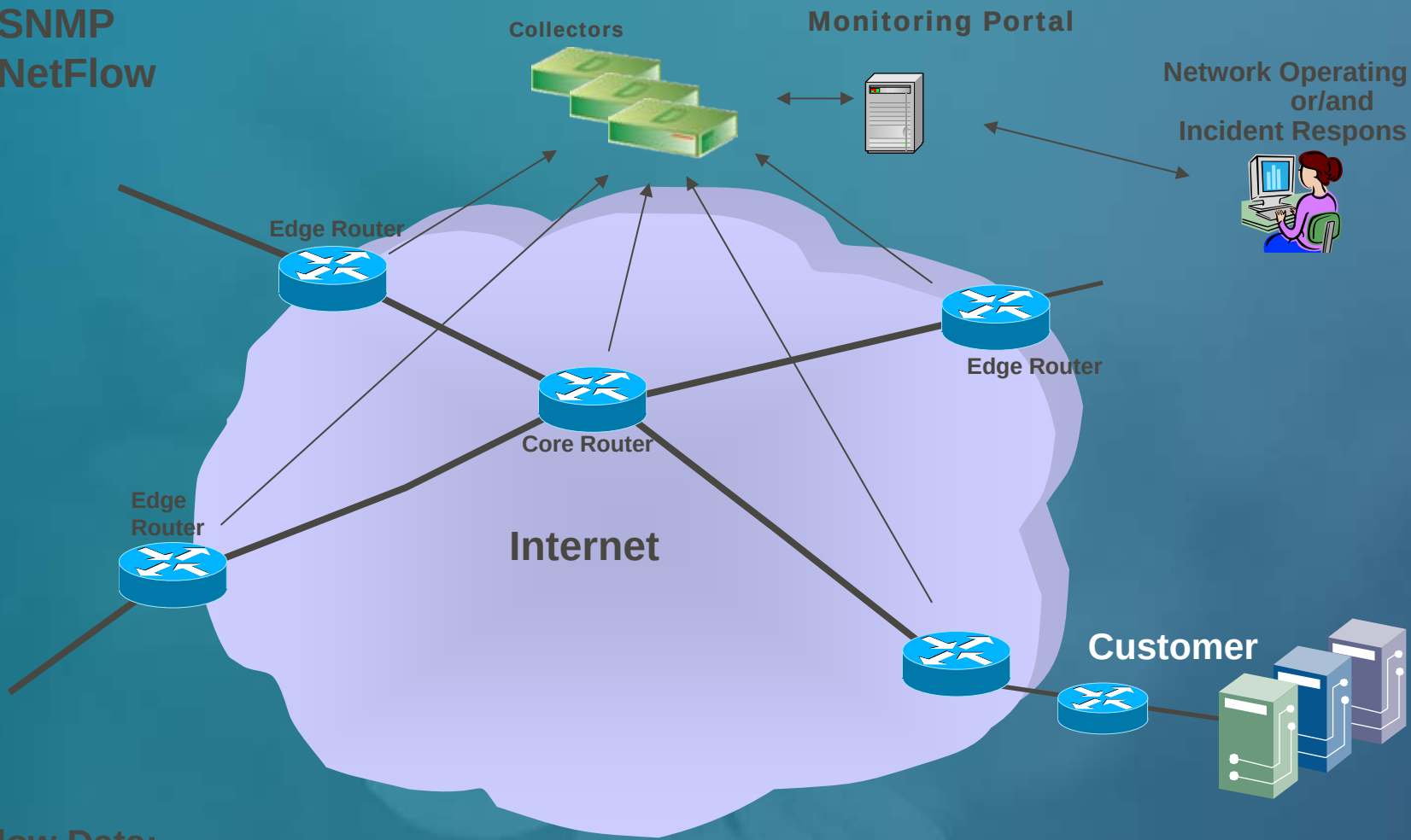
Measure your network!

How to detect abnormal traffic

- Without a traffic measurement tool your blind
- It’s important to monitor network activity in real-time
- You also need a plan how to react on misbehavior
- Learn what abnormal traffic looks like
- Learn what normal traffic looks like is easier ☺
- Share and learn information with others (fingerprints)

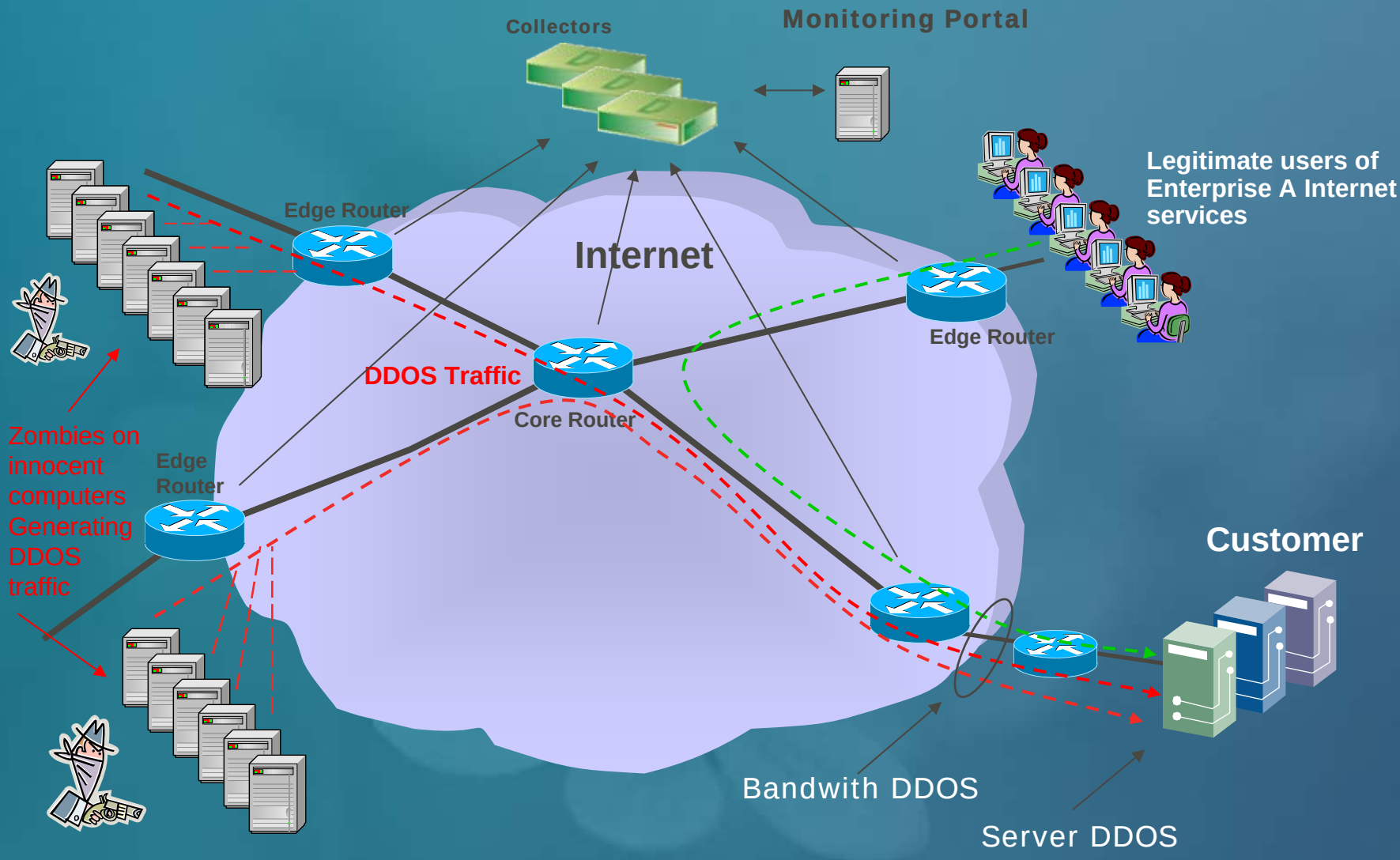
Traffic Monitoring

- BGP
- SNMP
- NetFlow



NetFlow Data:
SourceIf SourceIPaddress DestinationIf DstIPaddress Protocol SrcPort DstPort Pkts

Customer under a DDOS attack



Now what to do?

- We can stop the traffic by using destination based RTBH, but this shunts off the entire service for the customer, and that is an most effective DDOS attack.
- Cannot use source based RTBH if the DDOS attack is well distributed or/and from spoofed sources.
- Hmmmmm……???

Drop illegal traffic and forward legitimate one!

The solution!

- Use a centralized DDOS protection mechanism that can separate legitimate traffic from illegal traffic
- Drop the illegal traffic in bit bucket and forward the legitimate one

TeliaSonera can offer a DDOS Protection service

- TeliaSonera can divert traffic to a centralized scrubber and throw away unwanted traffic that match a known pattern and pass traffic that match a certain pattern.
- The goal is to be able to set up a protection for an attacked customer on a 5 minute basis.
- To be able to scrub traffic in most efficient way the scrubber has to do at least 48 hours ‘peace time learning’.
- Advanced Spoofing mechanisms is in use.
- User defined policies and profiles per protocol and behavior
- White list and black list

Traffic Diversion

Hijacking part:

To divert the traffic to a centralized scrubber you have to use a more specific match than existing route to destination. This can be done in many ways. For example by announcing a longer matching prefix or with a higher metric than original. For redundancy purposes you can use anycast addressing as nexthop.

Injection Part:

- Using BPR on interface were the scrubbed traffic arrives on and throw that traffic out on a GRE-tunnel to last hop router in origin path.
- Using VRF instead of GRE tunnel.

TeliaSonera Traffic Diversion

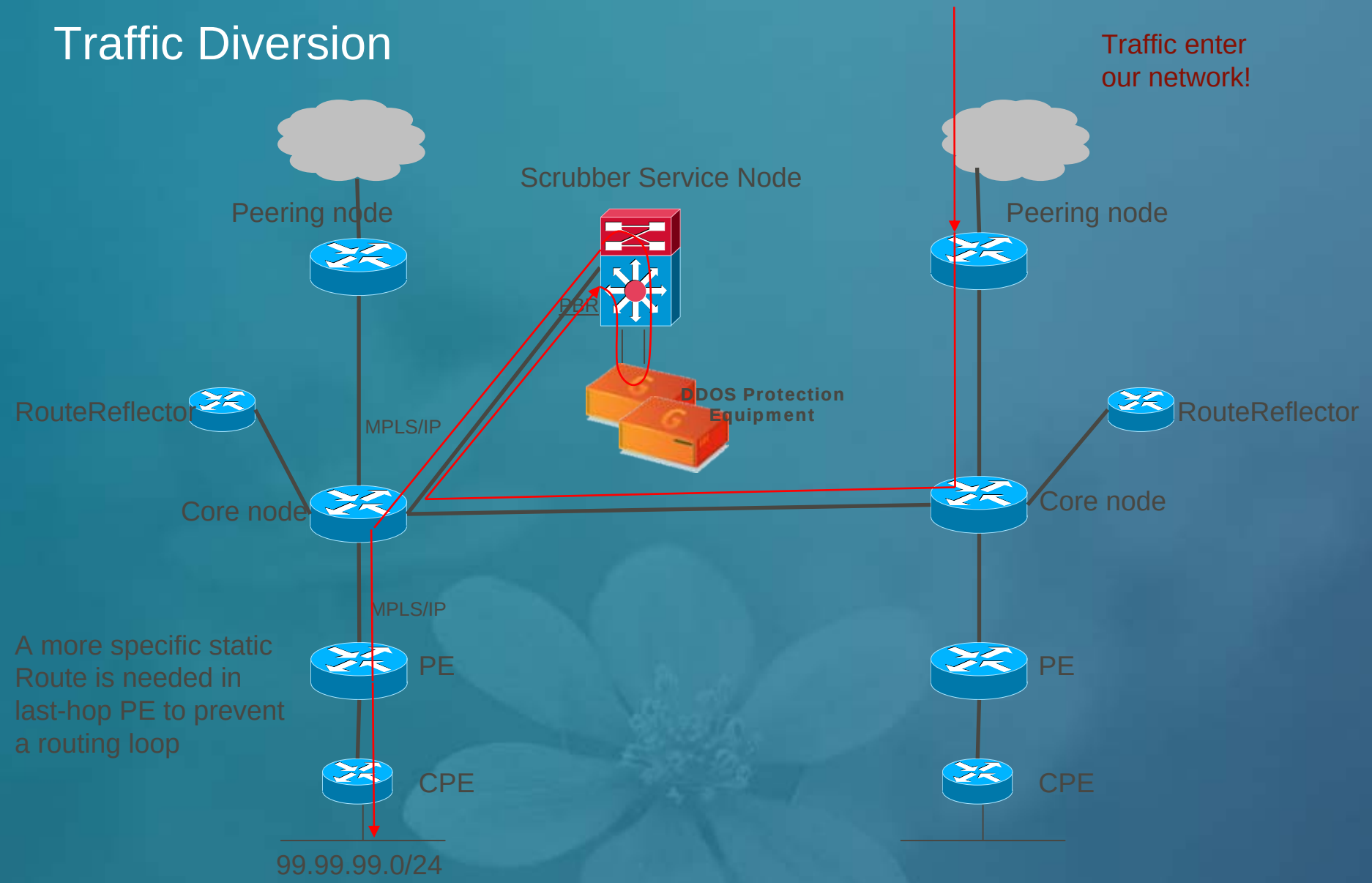
Hijacking part:

TeliaSonera are using Route Health Injection for redirect traffic toward the service nodes. The traffic for a specific destination will in all service edges be MPLS-label switched instead of IP switched. A static route (with a longer match than original , maybe a host-route /32) from the service node will use specific Loopback interface that is MPLS switched as next-hop address and in that way will pass all the core routers that doesn't have this entry in their RIB. This has been filtered out on all core routers.

Injection Part:

Using PBR of the entire VLAN there the scrubbed traffic returns, the service node forwards the traffic to the core-nodes that in their turn using native IP to the customer destination segment. In the last hop iBGP router we use a more specific static route to avoid a routing loop.

Traffic Diversion



TeliaSonera DDOS Protection

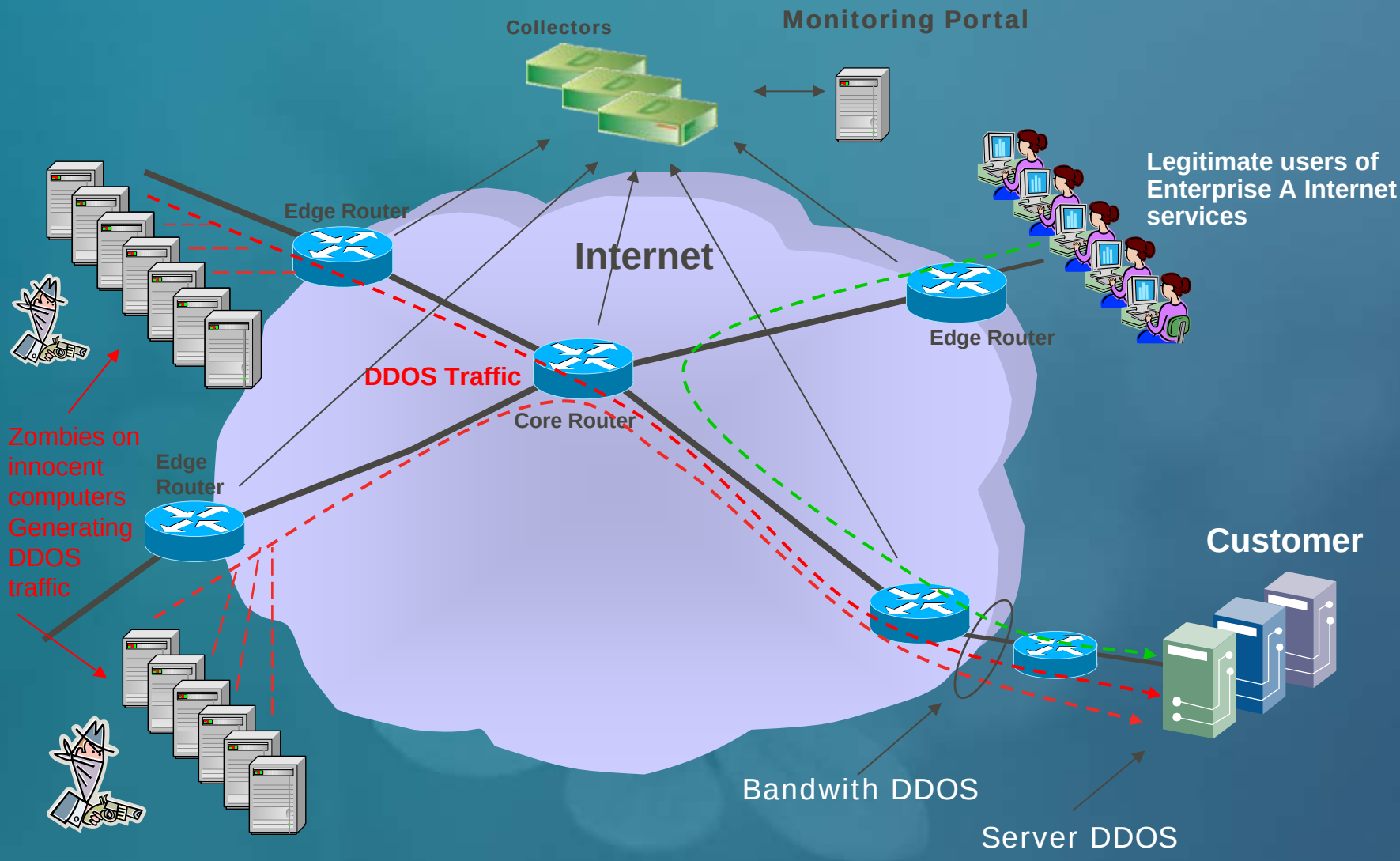
- The threat is to obvious. ISP's has to be able to offer these kind of services today. The customer can not do this for them selves. Has to be done as close to the source due to bandwidth demands.

- Can be combined with RTBH in TeliaSonera International core for international peers/traffic to limit the DDOS effect.

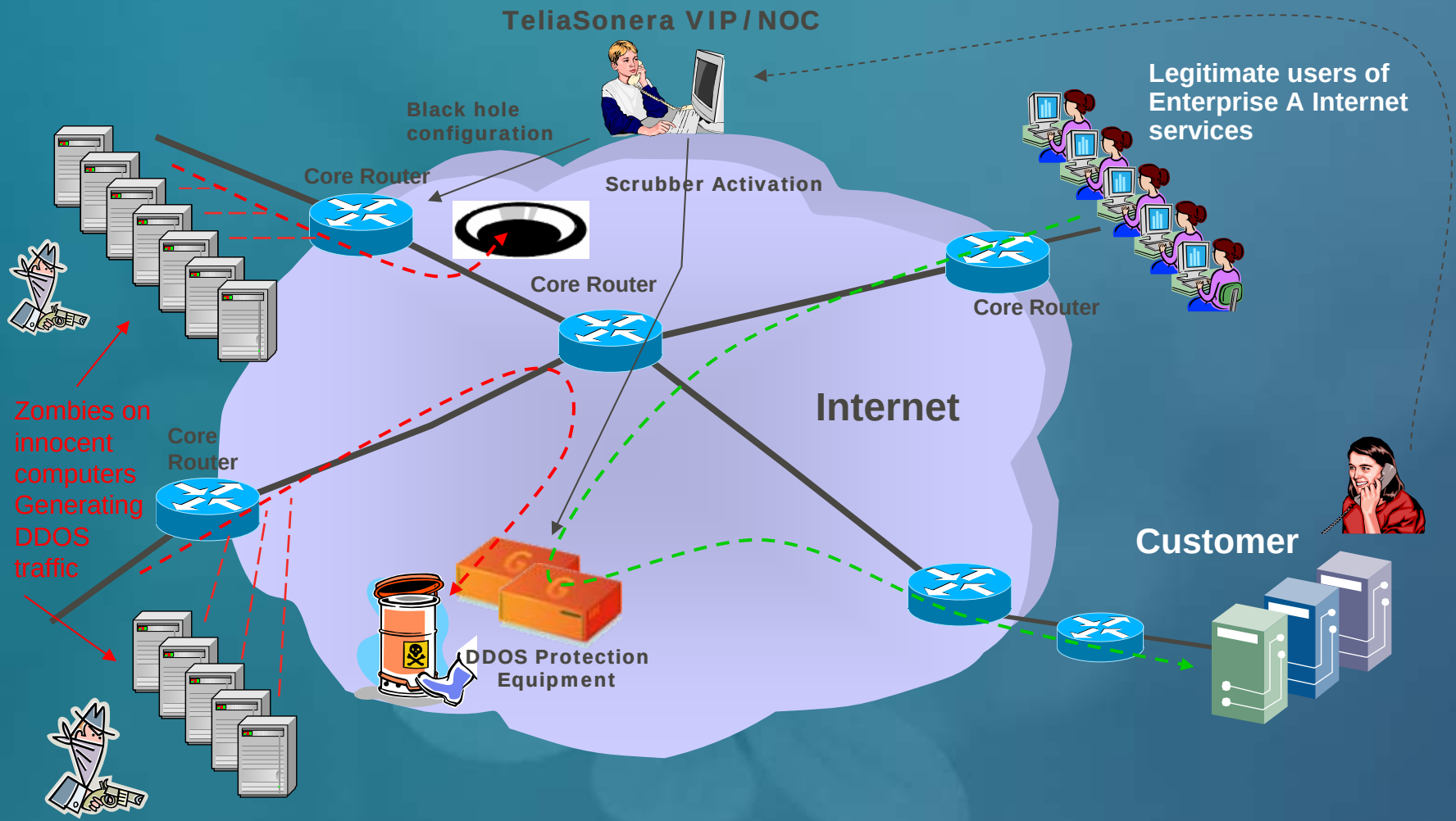
- If the Traffic Monitor System detects a DDOS towards a customer that has bought this DDOS Protection Service, it will send a trap to our NOC. They in their turn will in co-operation with the customer start divert the traffic and prevent this DDOS attack to reach its destination.

- Everything can be traced back through statistics and history will tells about what have happened and when.

DDOS attack


Collectors
Monitoring Portal
Legitimate users of Enterprise A Internet services
Edge Router
Internet
Edge Router
DDOS Traffic
Core Router
Zombies on innocent computers Generating DDOS traffic
Edge Router
Customer
Bandwith DDOS
Server DDOS

THE COMPLETE PICTURE
DDOS Protection using Cleaning and RTBH



The Nordic and Baltic telecommunications leader

TeliaSonera