DDoS information session

Lisa Van Loo
Nicolas Kharkevitch
January 2024

Belnet
dedicated connectivity

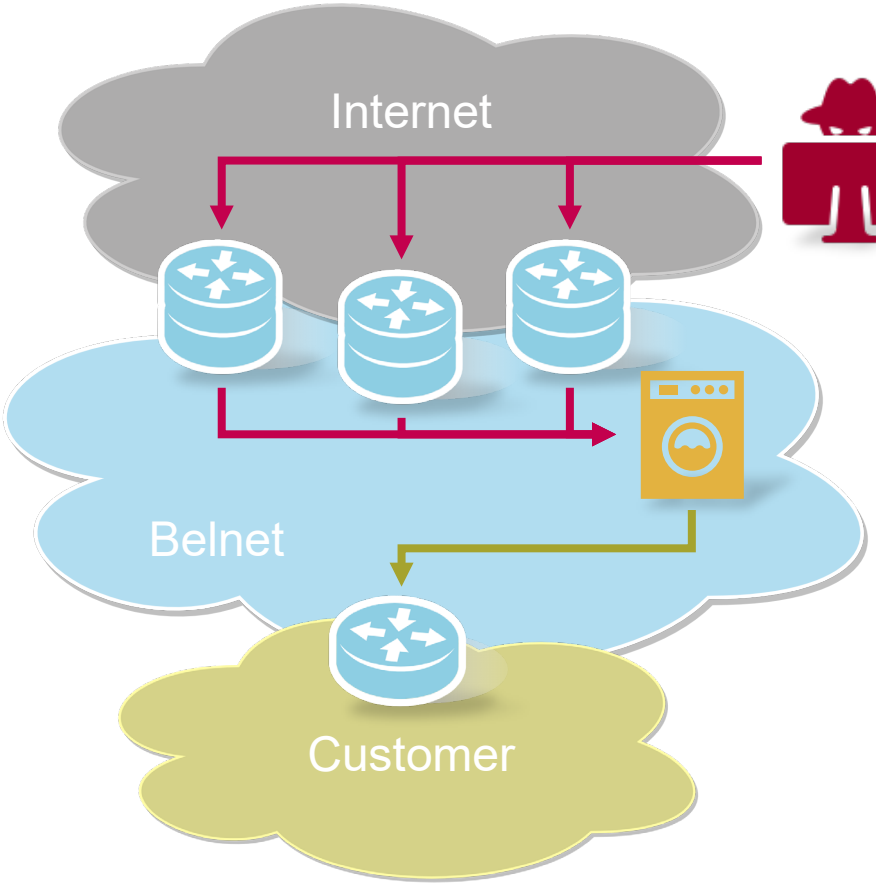
.be

Before we get started...

- Please keep your microphone muted unless speaking
- Any questions can be posted in chat and will be answered at the end of the presentation
- Let people know who you are by putting your title and organization in your display name and/or turning your camera on

Agenda

1. Belnet Adv. DDoS Security:
   - How does it work?
   - Attack mitigation
2. In detail:
   - Mitigated attacks
   - Attacks not detected
3. Best practices to ease mitigation
   Protecting against Applicative DDoS

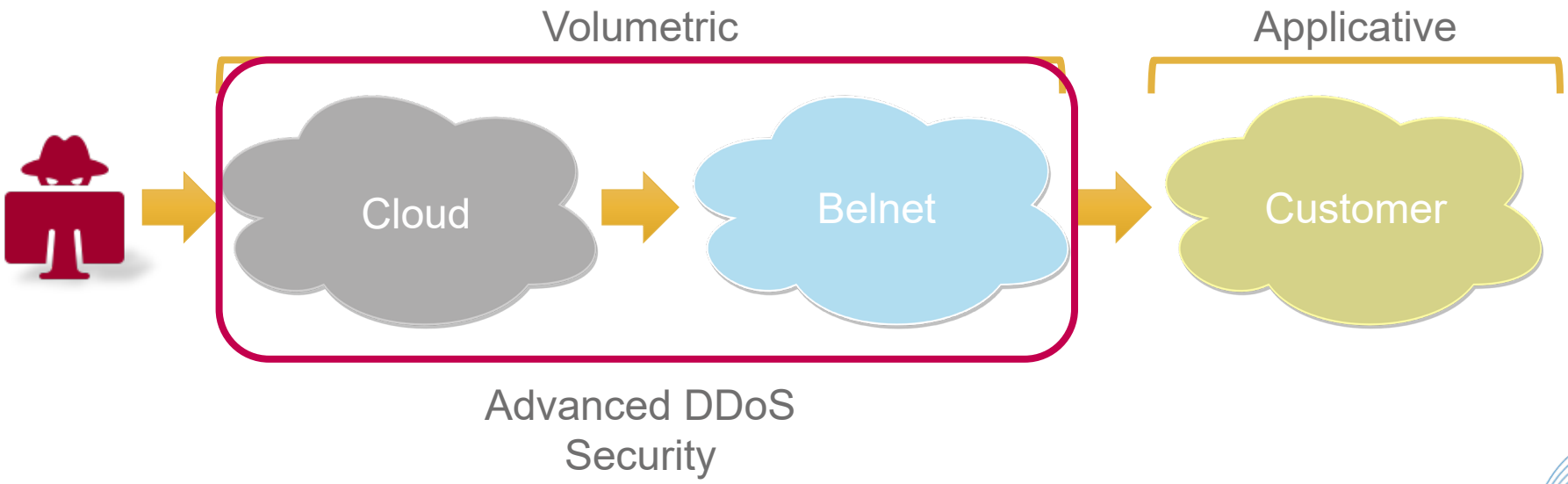


How does it work?

- Out-of-Path DDoS Mitigation
- No extra hops in peacetime
- Time to mitigate: a few seconds
- Mitigation on edge routers as extra layer of protection

Belnet
dedicated connectivity

Attack mitigation



Mitigated attacks

- Mitigation triggered by significant increase of bps or pps
- Anything cleartext in header (transport layer/ L4)
- Anything based on packets/s or bits/s
- UDP amplification attacks, TCP SYN flood,…

Attacks not detected

- Anything encrypted, we are unable to look in the packet
- Any exploits to your applications
- DNS random query attacks
- SQL, HTTP, SSL, … attacks
- We will always help

Best practices to ease mitigation

Spread services across multiple IP’s

Single IP per host / service / type of IP flow

Use NAT Pool for outgoing traffic

Good traffic load repartition between IP’s

Belnet
dedicated connectivity

Protecting against Applicative DDoS

Network firewall + Applicative firewall

Keeping applications up-to-date

Web Application firewall (WAF)

IPS / IDS

Belnet
dedicated connectivity

Protecting against Applicative DDoS

Protect your webservers

- Reverse proxy: keep IP's private
- Content Delivery Network: spreading traffic worldwide

Access Control Lists (ACL)

Anycast DNS

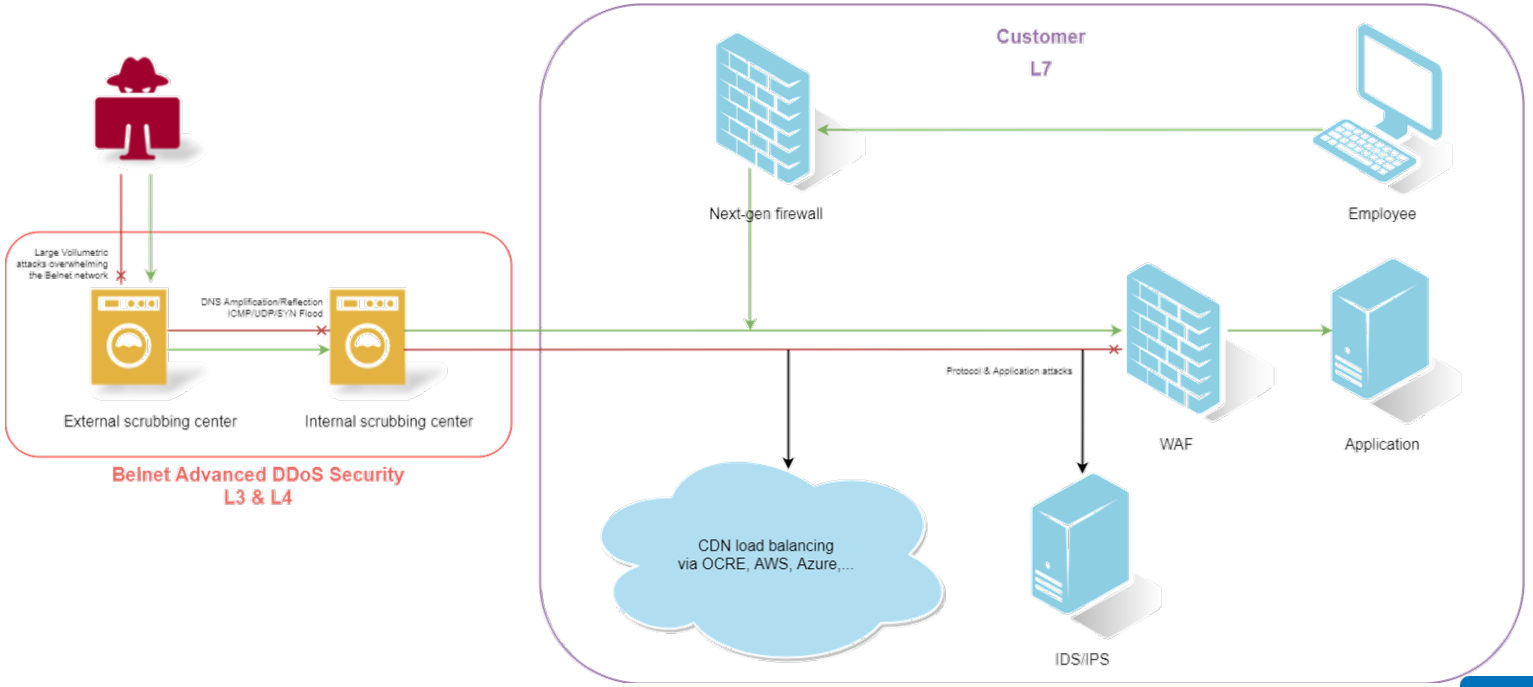
- Spread DNS traffic worldwide

Network Intrusion Detection System (NIDS)

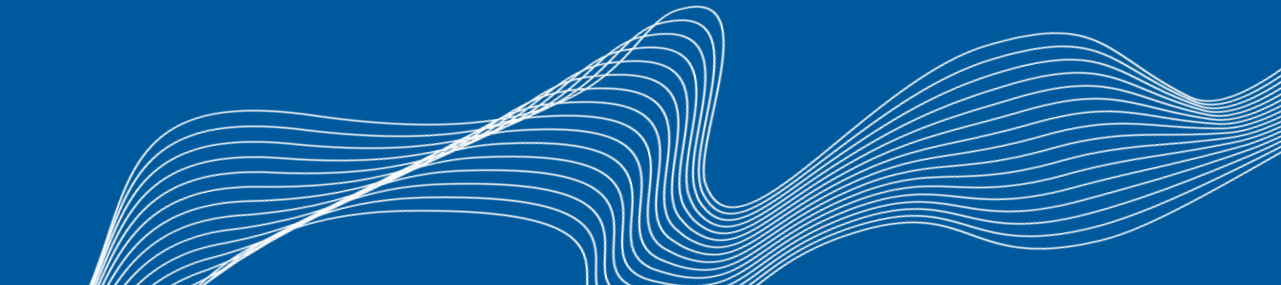
- Advanced, improves visibility

Belnet
dedicated connectivity

Protecting against Applicative DDoS



Q&A




Thank you
for your attention
Belnet
dedicated connectivity


Belnet
dedicated connectivity