Cleaning and Scrubbing at the Internet's Dry Cleaners

restena

network · security · .lu

Agenda

- What?
- Why?
- Where?
- How?

What?

Is DDoS? Clean/Dirty Traffic?

What is DDoS?

Victim Perspectiv

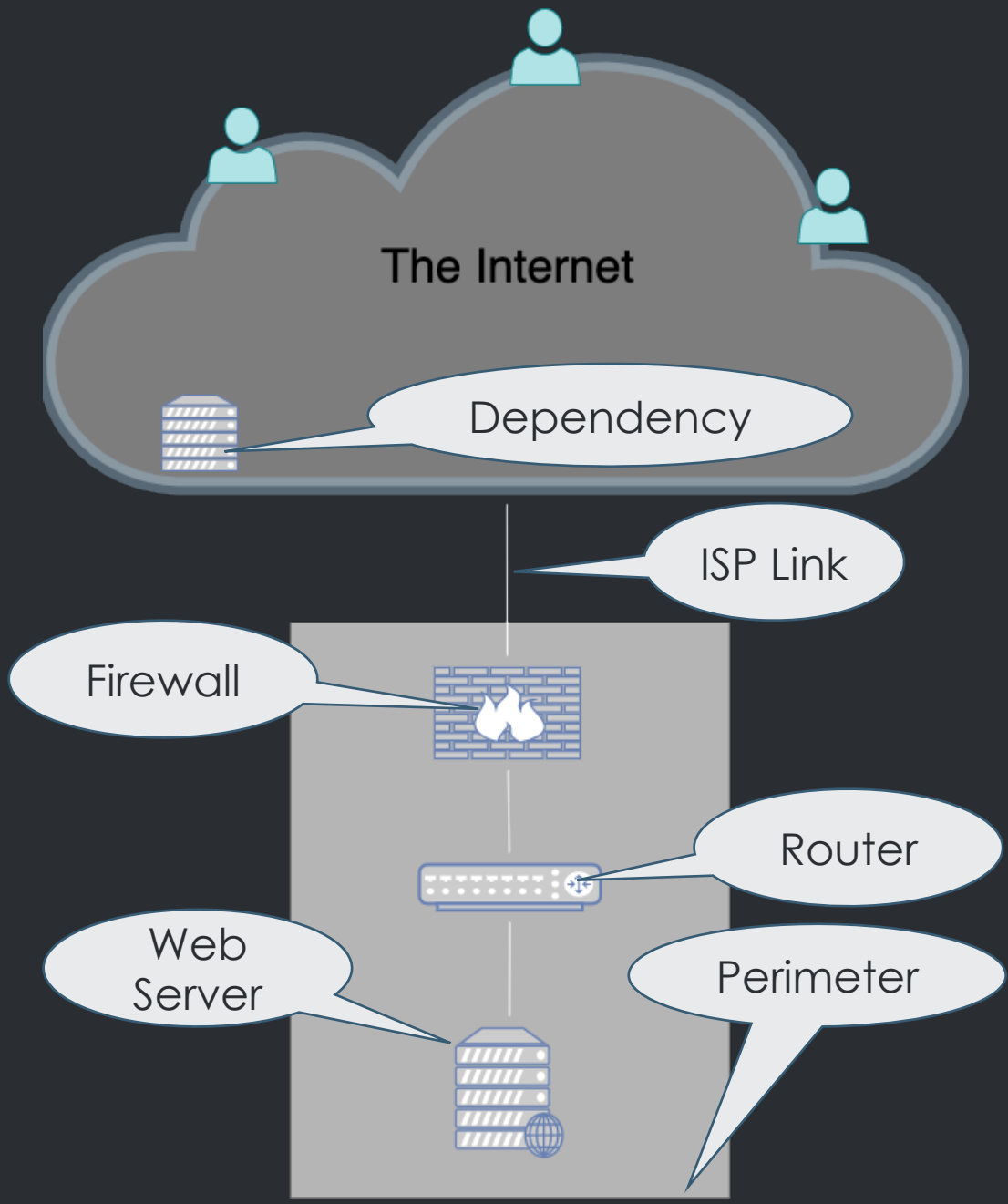
Impact Service Availability!

What Service?

- Website
- E-Bank
- E-Shop
- Video Conferencing
- Voice Call
- Instant Messaging
- Streaming

What is DDoS?

Simplified System Architecture

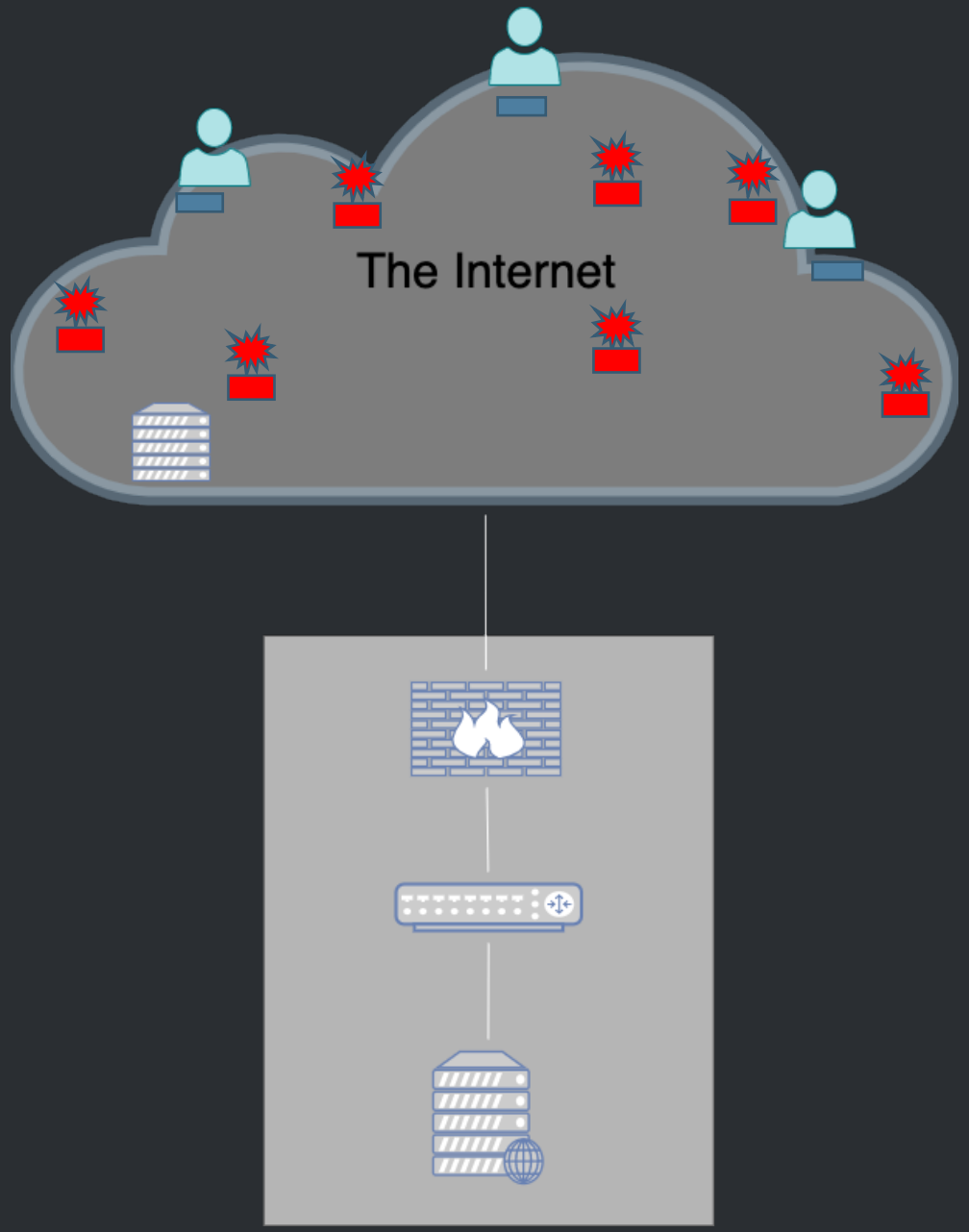


What is DDoS?

Resource Exhaustion

Service in Action

DDoS in Action



What is DDoS?

Resource Exhaustion

What resource?

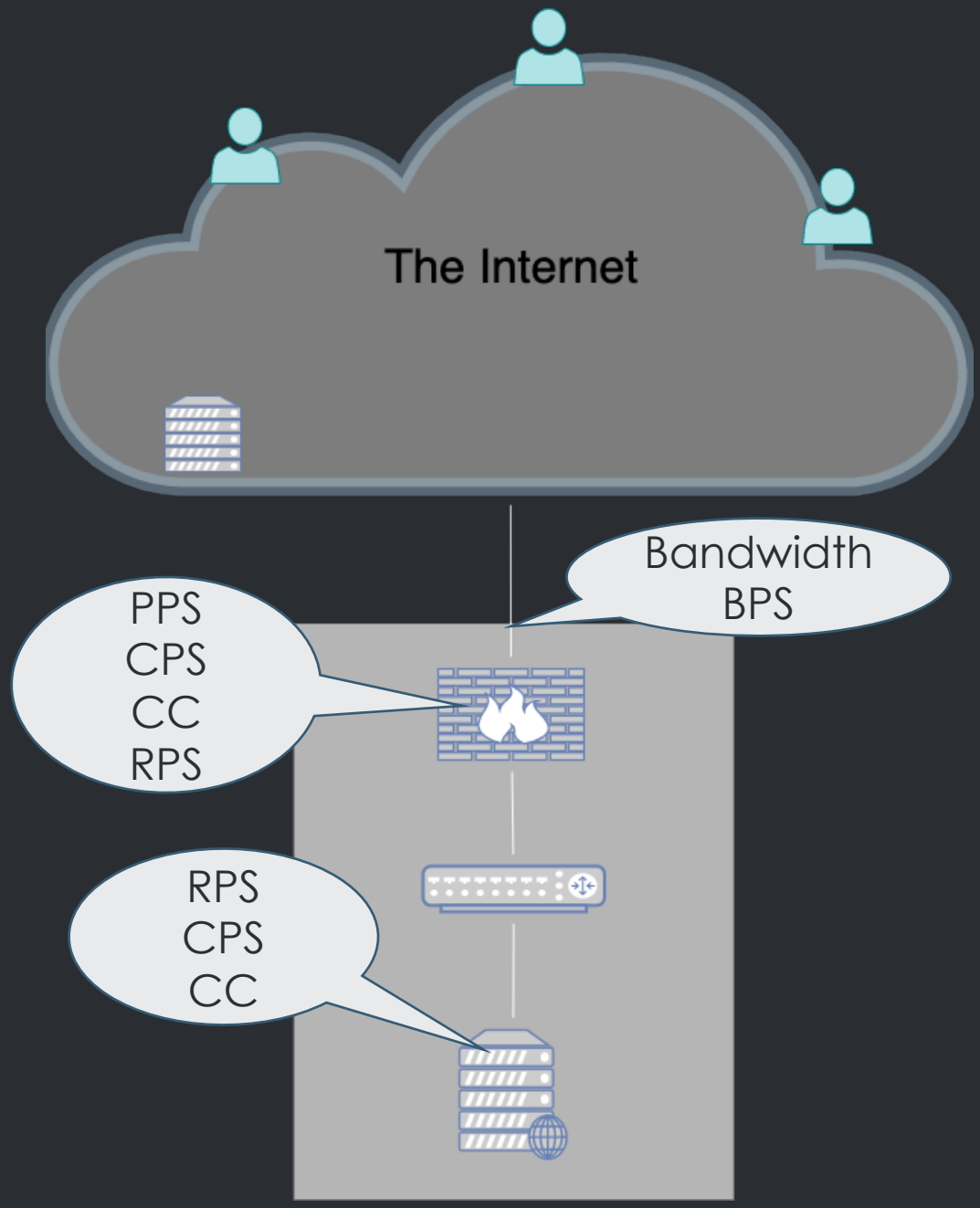
BPS – Bits per Second

PPS – Packet per Second

CPS – Connections per Second

CC – Concurrent Connections

RPS – Requests per Second



Why?

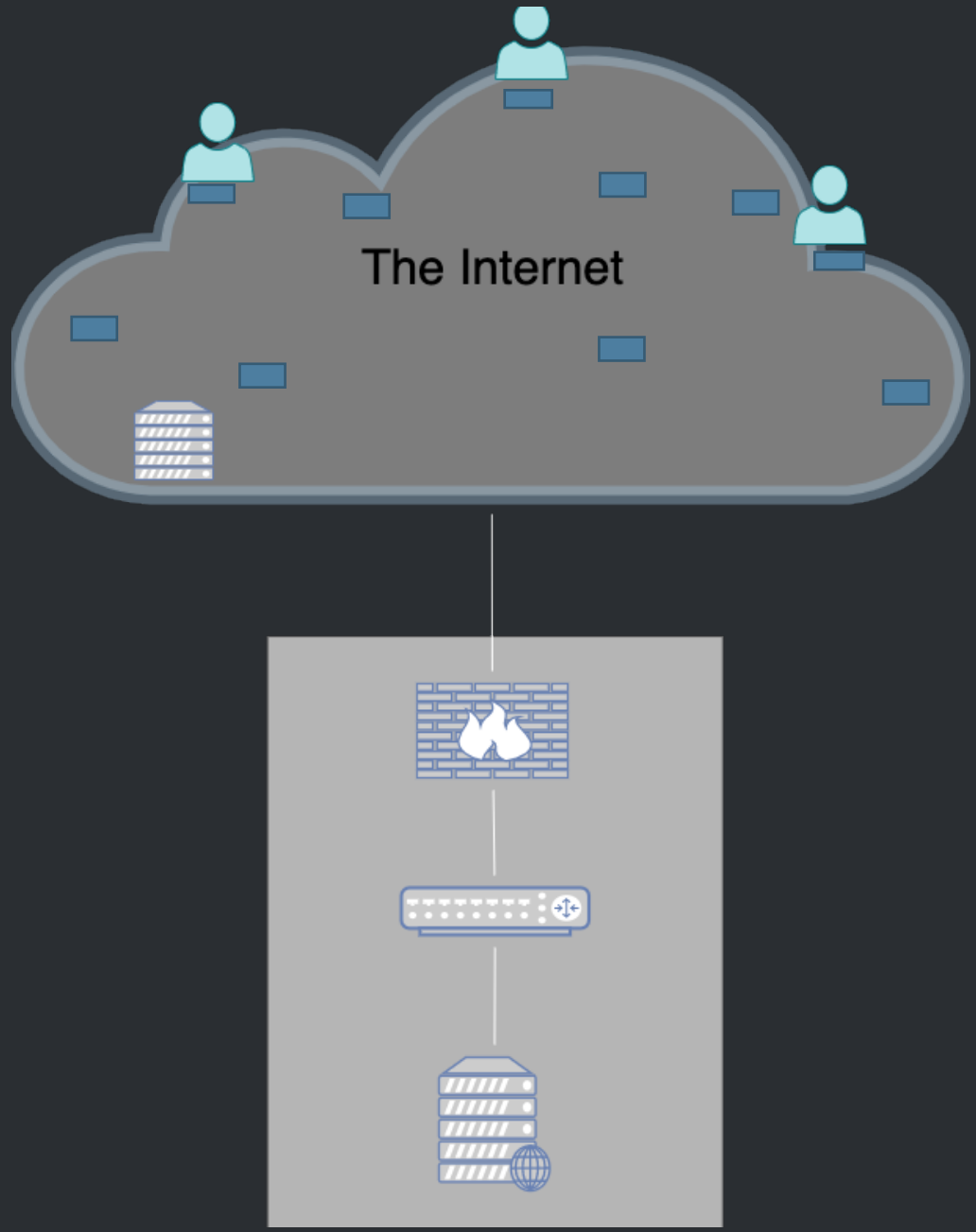
Blocking DDoS; Big deal?

Why?

Is blocking hard?

Perimeter!

Traffic has no colour!



Where?

Should we clean?

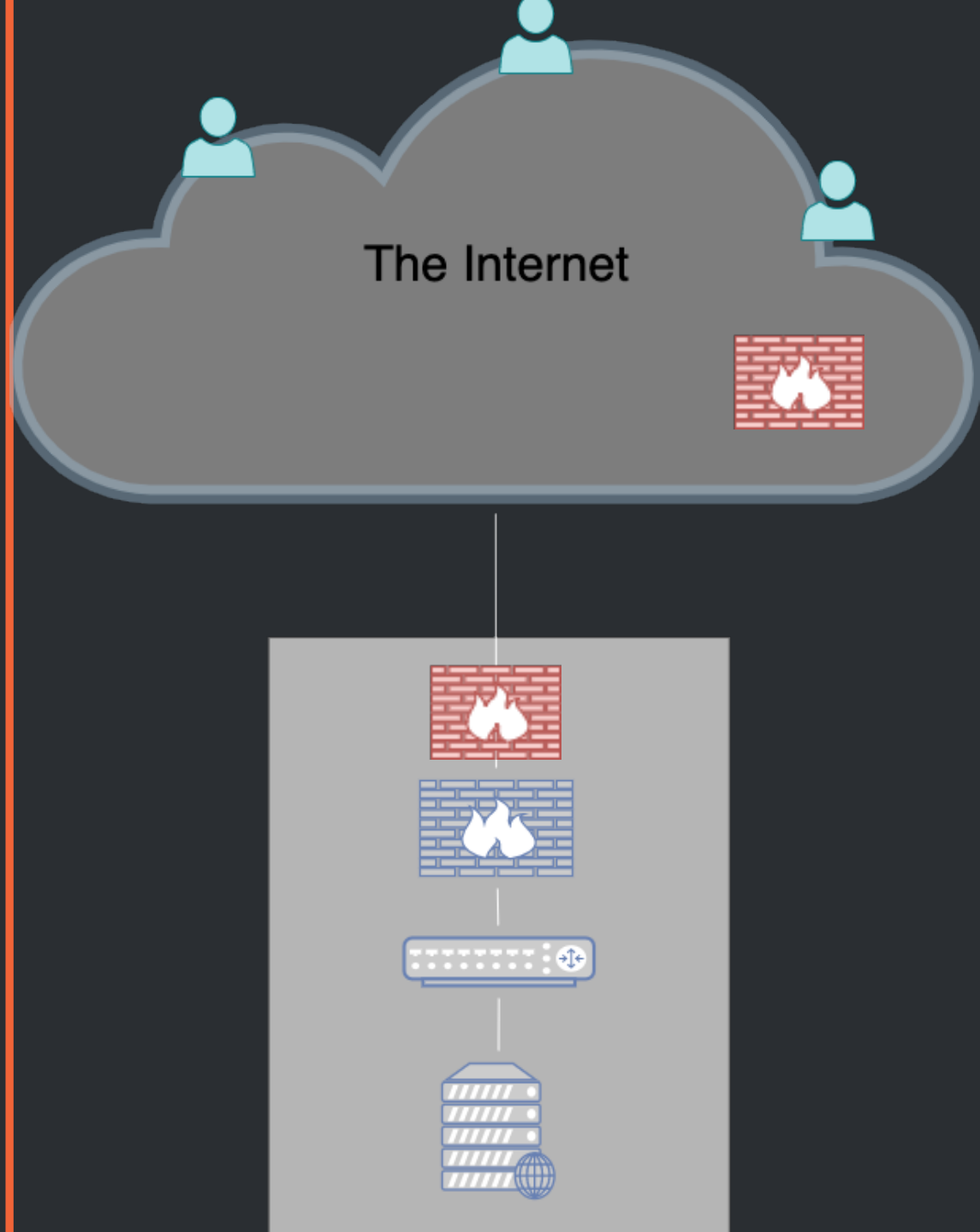
Where?

To clean or scrub?

On-site

Off-site, ISP…

Or both



How?

Every stain has its cleaning potion.

How?

Identify the bot

Are you a legitimate client?

Are you a bot?

- Guilty until proven innocent
- Works with connection oriented protocols
- Checks if client observes protocol

- Innocent until proven guilty
- Mostly with connectionless protocols
- Rate based

How?

Characterise the attack

Protocol Fields

Statistics

- UDP based:
  - Source Port
  - Payload length
  - Destination IP
- HTTP based:
  - Request method
  - URI
  - HTTP version
  - User-Agent
  - Host
  - Forwarded
  - X-Forwarded*

Conclusion

What is DDoS?	Impact Service availability through resource exhaustion
Why is it difficult to block?	Perimeter, not everything is under our control, and difficult to distinguish legitimate from bot
Where do we intervene?	On-site, off-site in a scrubbing centre, or both
How do we block?	Identifying bots, characterizing attack traffic

Time for Questions?

www.restena.lu