DDoS: how to detect, prepare and respond

How to detect?

- Regular monitoring tools will indicate at least one of the following **unexpected** metrics:
  - I**ncoming peak bandwidth** from internet (saturation).
  - Routers reaching **100% CPU** usage.
  - **Unresponsive servers** even on the presence of network traffic.
  - Number of **transacions decreasing** even on the presence of network traffic.

What will happen during an attack?

- If you are **not** prepared:
  - Your **routers** will become unresponsive, stopping to send and receive data from/to internet.
  - Your **servers** will become unresponsive, stopping to process queries from your customers and partners.
  - **E-mail** and VPNs will become offline.
  - To sum up: **everything** depending on the internet **will stop working**.

How to prepare?

4

Basic preparation steps

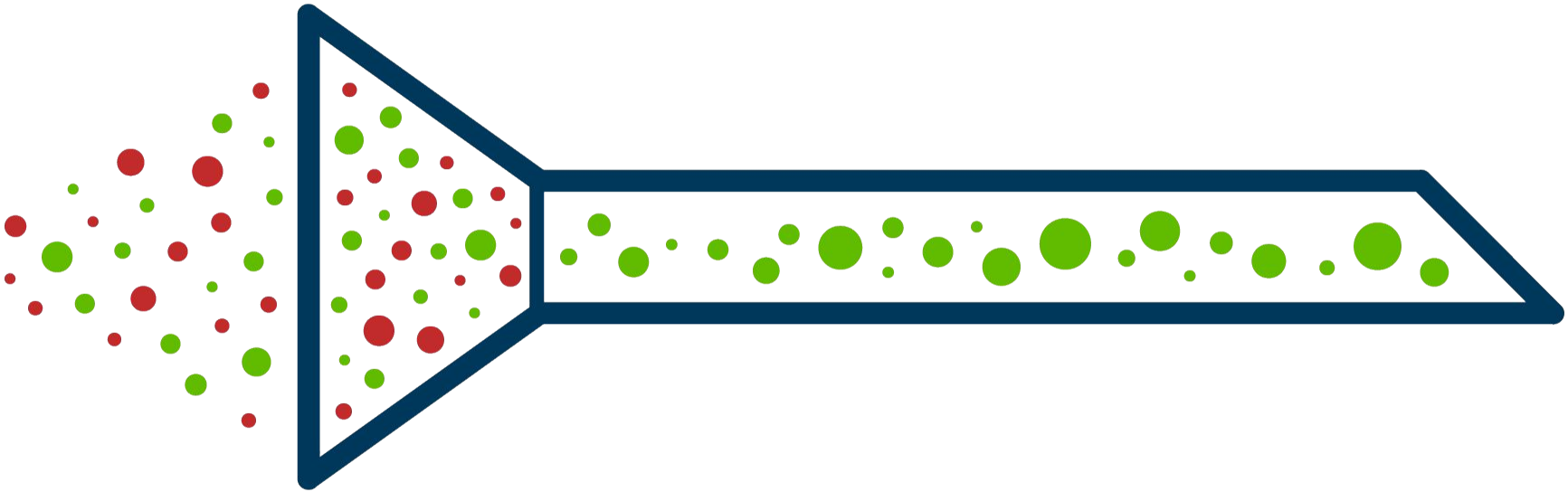
How to prepare?

- Become an Autonomous System (**AS**) and obtain your own IP address space.
- Obtain IP Transit from **multiple providers** and ensure they do not share infrastructure.
- Deploy all regular network protections: **firewall**, Intrusion Detection System (**IDS**), Intrusion Prevention System (**IPS**).
  - Keep in mind **none** of them will protect you from volumetric DDoS, but they are needed for general protection.
- Purchase a specialized **DDoS mitigation service**.

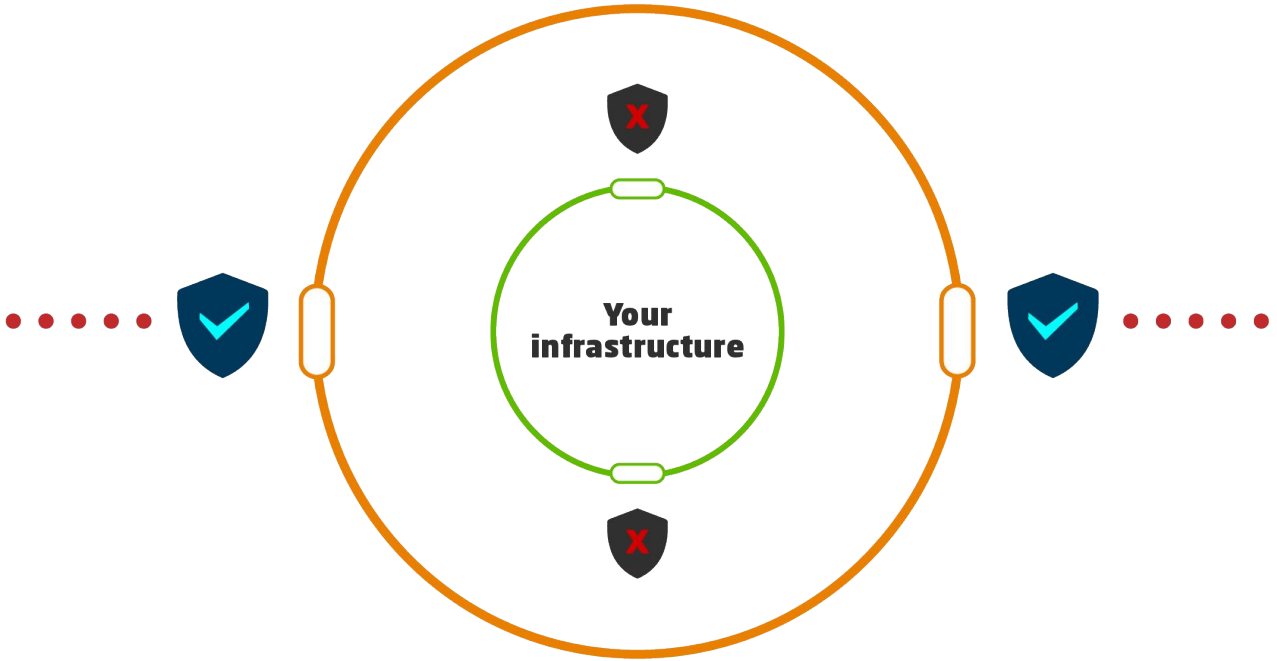
DDoS mitigation in cloud: how does it work?

- It intercepts traffic targeting your infrastructure **before** it reaches your router.
- Multiple algorithms **analyzes the packets** to classify them in abnormal or normal.
- Abnormal packets are **dropped**
- Normal traffic will be **re-routed** to your infrastructure and allowed to reach your servers.

DDoS mitigation in cloud: how does it work?



DDoS mitigation in cloud: how does it work?



DDoS mitigation service: what to look for?

- A **cloud-based solution**. On-premise hardware is very limited.
- An **IP Transit** provider which also provides DDoS mitigation.
- A support team that **understands your business**, knows your topology and internal network.

How to respond?

- Hardly ever **law enforcement** authorities are able to help.
- The **lack of forensic evidence** halts your legal actions.
- You should **report** every IP address detected sending attack to its responsible **Abuse**/CSIRT team.

¡Gracias!

thiago.ayub@upx.com.br