AntiDDoS

Lo scudo 2.0 nell’era della guerra telematica

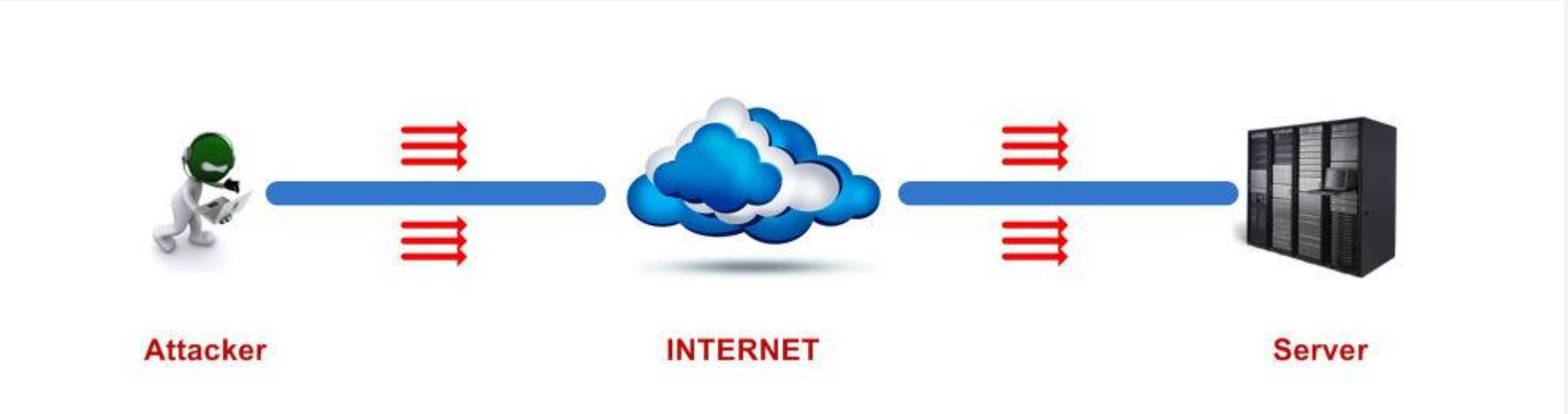
Relatore:

Stefano Giraldo - Sr. Network Engineer

https://www.linkedin.com/in/stefano-giraldo/

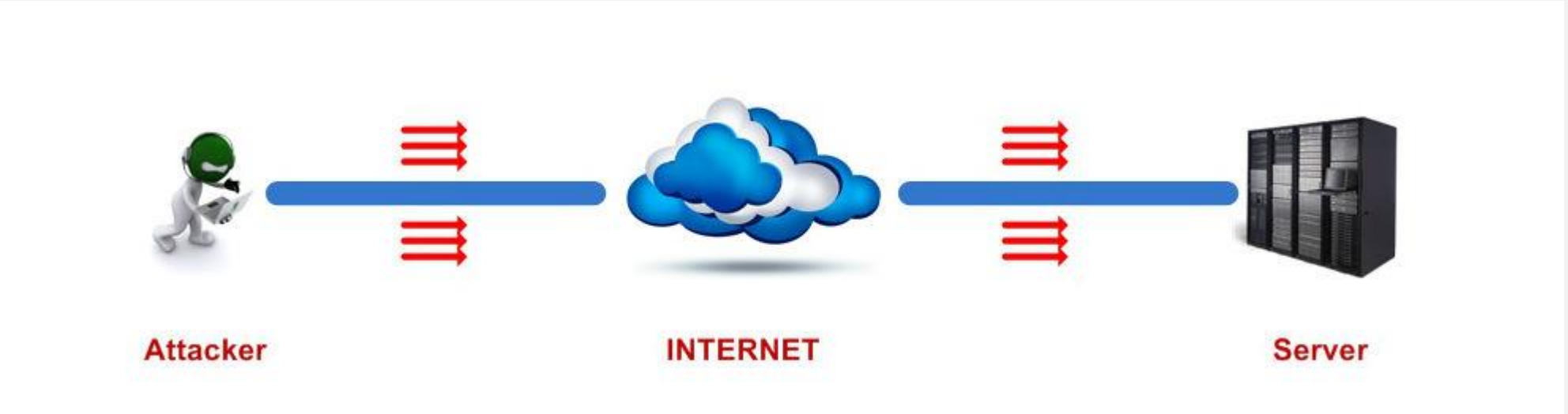
Denial of Service

Denial of Service



- Tramite un DoS, l'attaccante cerca di compromettere un servizio, un sito Internet o un Sistema (nel senso ampio del termine).
- Agisce sfruttando le vulnerabilità dei server che erogano i contenuti oppure falle di sicurezza nel codice del servizio pubblicato.
- Può inoltre sfruttare l'ingenuità o la scarsa propensione alla sicurezza di qualche dipendente per accedere a un Network e lanciare l'attacco.

Denial of Service

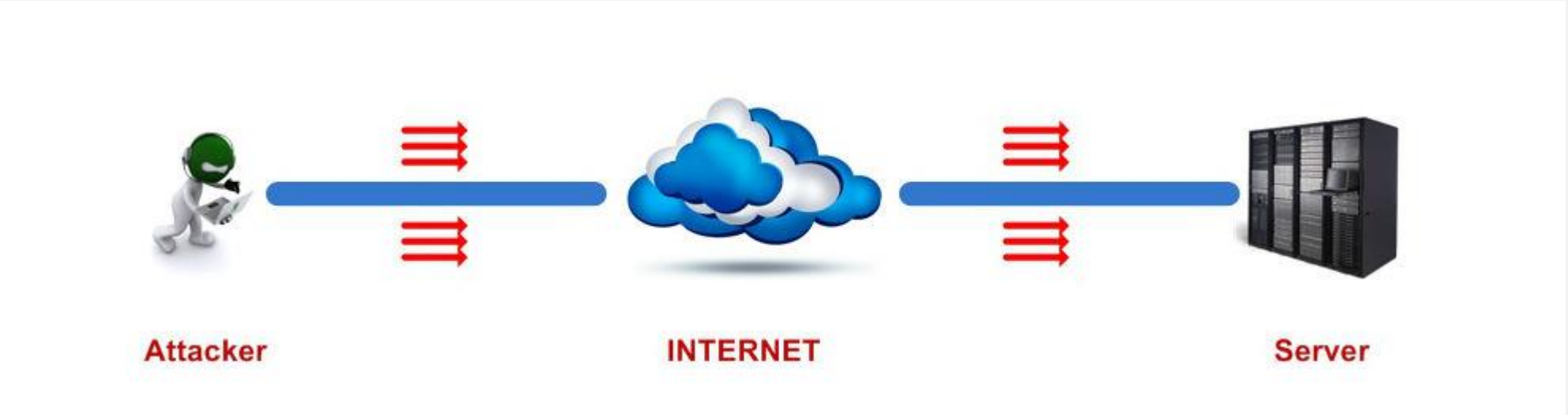


- L'attacco viene portato da una singola sorgente o da un ristretto numero di attaccanti in cooperazione, verso una destinazione.

- Obiettivi: aziende con grossi capitali, enti governativi, organizzazioni in possesso di dati sensibili (dati personali, elenchi di indirizzi, ecc), partiti politici e sostenitori, aziende/governi accusati di non rispettare l'ambiente o i diritti umani o di scatenare guerre.

- Sono necessarie: strategia, pazienza ed eccellenti competenze tecniche.

Denial of Service



Scopi dell'attaccante:

- Causare un disservizio o modificare un contenuto.
- Sottrarre dati per poi cancellarli e rivenderli o cifrarli chiedendo un riscatto.
- Fare sfoggio delle proprie capacità tecniche ridicolizzando sviluppatori e sistemisti del Sistema vittima.
- Lanciare un messaggio politico.
- Trarne un profitto economico.

Denial of Service

Denial of Service

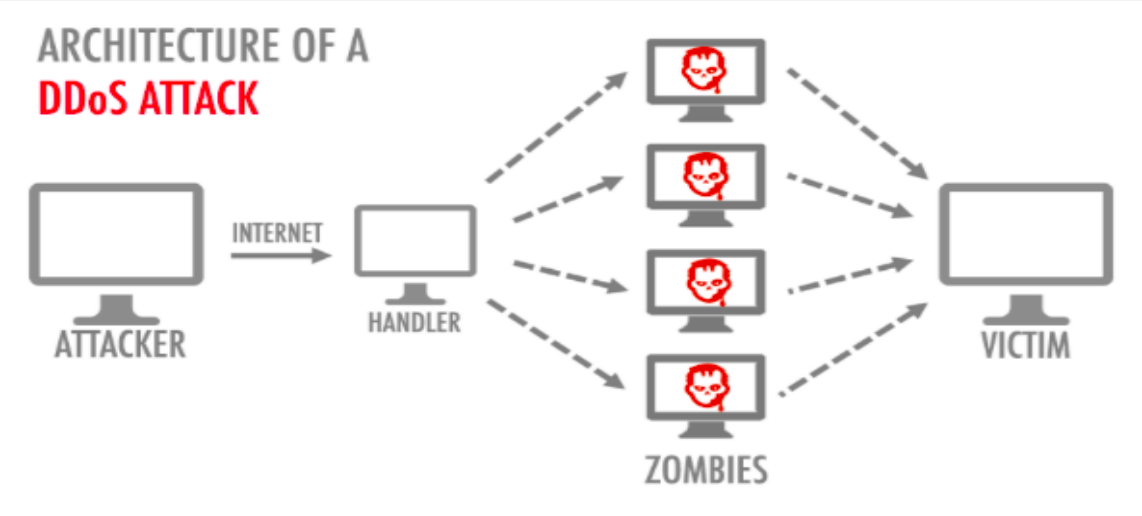
Denial of Service

Denial of Service

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Distributed Denial of Service

Distributed Denial of Service

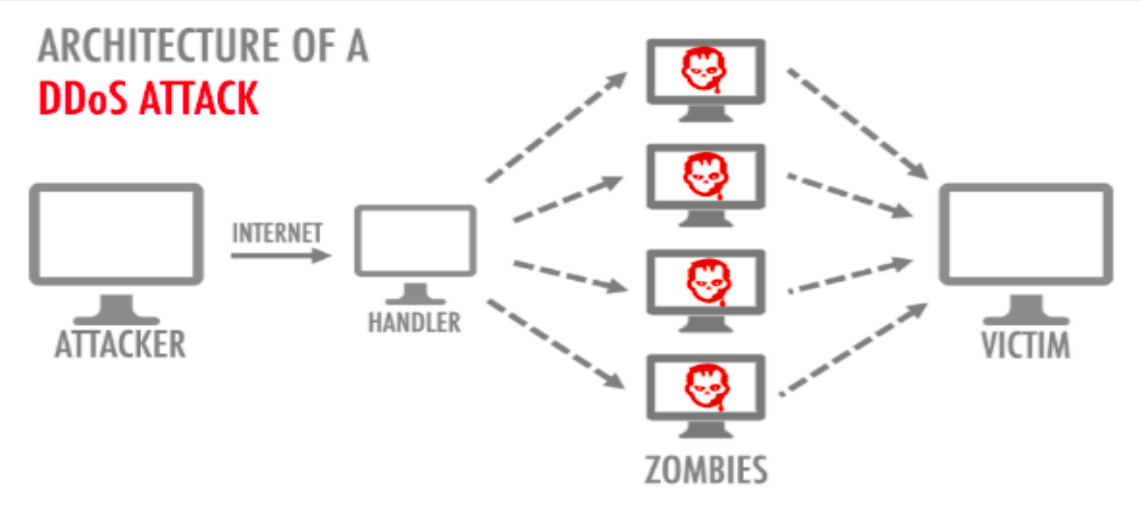


- Tramite un DDoS, l'attaccante sfrutta una "rete di computer zombie" o un bug di un servizio pubblico (DNS, NTP, ecc…).

- Viene generata un'amplificazione di "traffico sporco" verso la vittima (server, rete o Sistema) saturandone la banda o il numero di connessioni che può accettare, allo scopo di inibirne la raggiungibilità tramite Internet, il disservizio è legato alla durata dell'attacco.

- La sorgente viene solitamente ulteriormente mascherata tramite IP spoofing, così da non ricevere nemmeno l'eventuale traffico di ritorno.

Distributed Denial of Service



- La destinazione dell'attacco non viene quindi compromessa, non ci sono accessi illeciti ai Sistemi e non c'è furto di dati.

- Le competenze tecniche richieste possono anche essere basse.

- Sono anche disponibili su Internet delle "botnet" o delle VM da affittare per alcune ore allo scopo di lanciare attacchi volumetrici.
  https://wccftech.com/ddos-for-hire-services-offered-for-just-five-dollars/

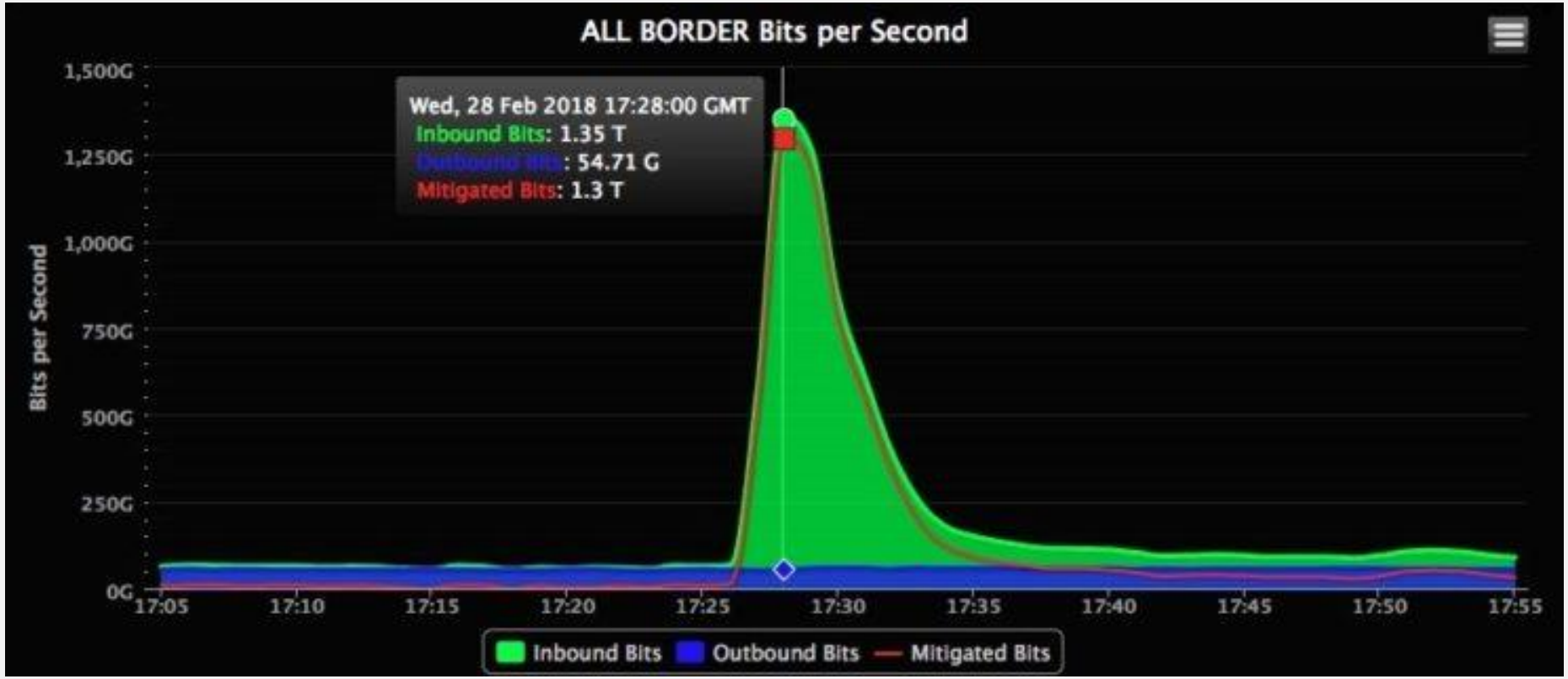
- Spesso sono preannunciati da mail minatorie e piccoli attacchi dimostrativi.

Distributed Denial of Service

I destinatari di un attacco:

- Un singolo Server o gruppi di Server
- Tutti gli indirizzi di un prefisso IP annunciato su Internet
- Il gateway/firewall di una Rete
- Un singolo utente con una connettività residenziale (gaming)

Distributed Denial of Service



- GitHub Memcached Servers attack

https://wccftech.com/github-biggest-ddos-assault-recorded/

Distributed Denial of Service

Distributed Denial of Service

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Cottigli pe gli acquitti

Search...

CART / $0 0

ACCOUNTS ATTACKS EXPLOITS HACKING RANSOMWARE SMS AND CALL INTERCEPT SPAM TOOLS PROOF

HOME / ATTACKS

Take Site Down (DDOS Attack)

$250 – $850

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

CLEAR

Hours Choose an option

Choose an option
6
12
18
24

Website U

- 1

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Cottigli pe gli acquitti

extract data from its database. They are different tasks for different charge. I can hack almost any websites. The website is the object of checking before hacking. The price depends on the website you want me to hack. Please note that the administration of a website requires some knowledge. Depending of the web and what do you want do on it, you will need to access the control panel, or maybe the entire server. It's your responsibility to know what you order and how to manage it.

Cost starts from: **$800**

I can get access to university or college databases in order to change the data (grades or anything else).
To order, give me this info:
- Entry point (link) to your personal area and your credentials (login + pass)
- What grades you want me to change
- The price depends on your university

Cost: **$600-1 200** per student

phone number and even ID.
And, surely, I need some info about the target person, to finish the task. It could be:
- email address
- Social media account
- phone number

Price depends on the info you have about the target person.

Cost starts from: **$400**

Life Crushing

Some people deserve to be crushed. If you want to revenge someone - I could help. I have some cases of life crushing. Most often the victim goes to a jail with public shame. There are several ways to achieve this goal. I will explain the strategy by request.

Cost starts from: **$2 000**

DDoS Attacks

We are able to get down almost any website, you just have to choose how long the attack should last and when to do it
To order, give me this info:
- Target website
- Attack intensivity
- If you can't choose intensivity - I will offer it by myself after website checking.

350 Gbps cost: **$35/hour** or **$450/day**
650 Gbps cost: **$45/hour** or **$650/day**

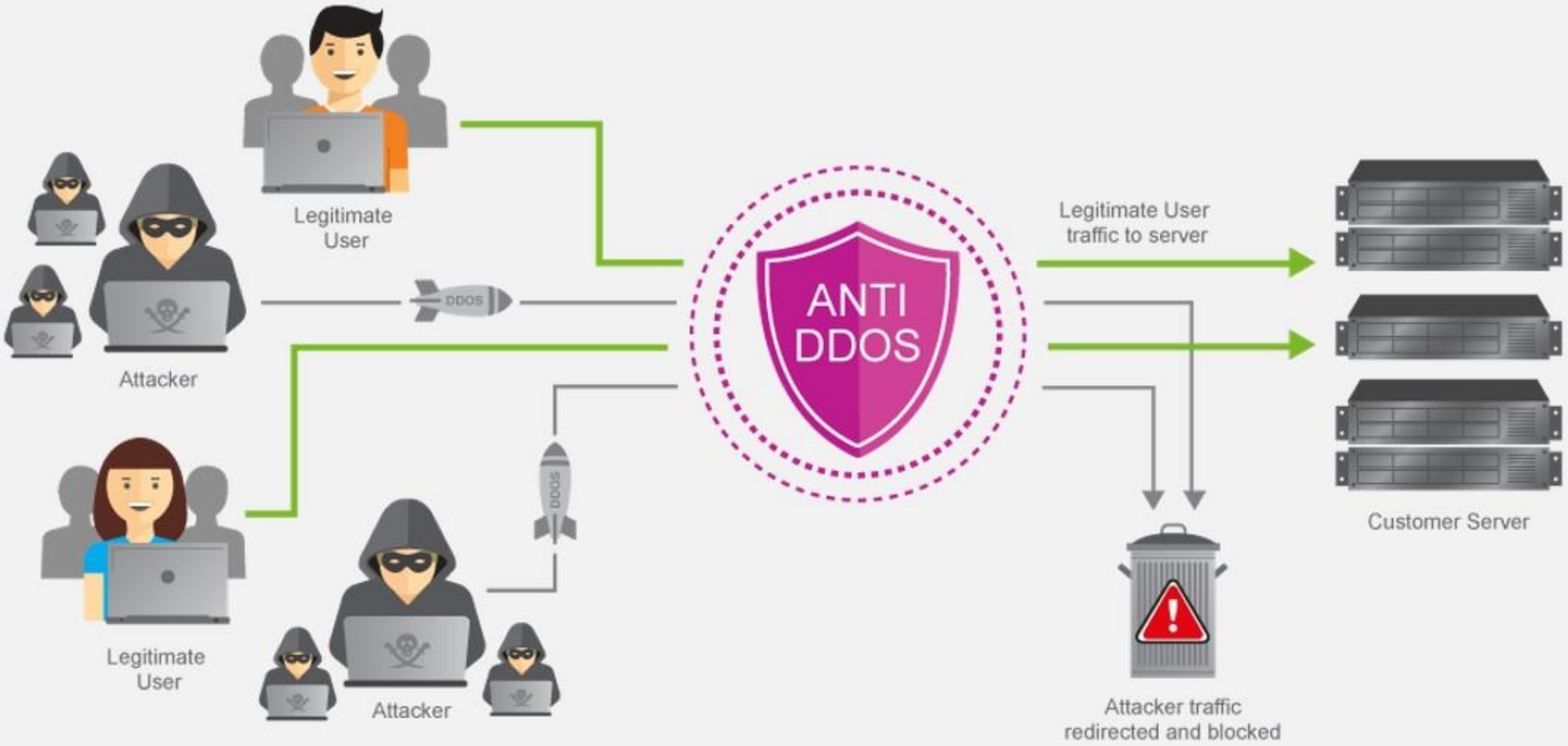
Special Services

I can do many more tasks which are not represented here. And actually I appreciate big interesting unusual tasks. Just contact me and explain what you want me to do.
Note that the price is not related to working hours.
Please describe all the task extremely detailed. It is very important for the job. I have to understand it very clearly.

Cost: **by request**

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Come proteggersi da un attacco DDoS?



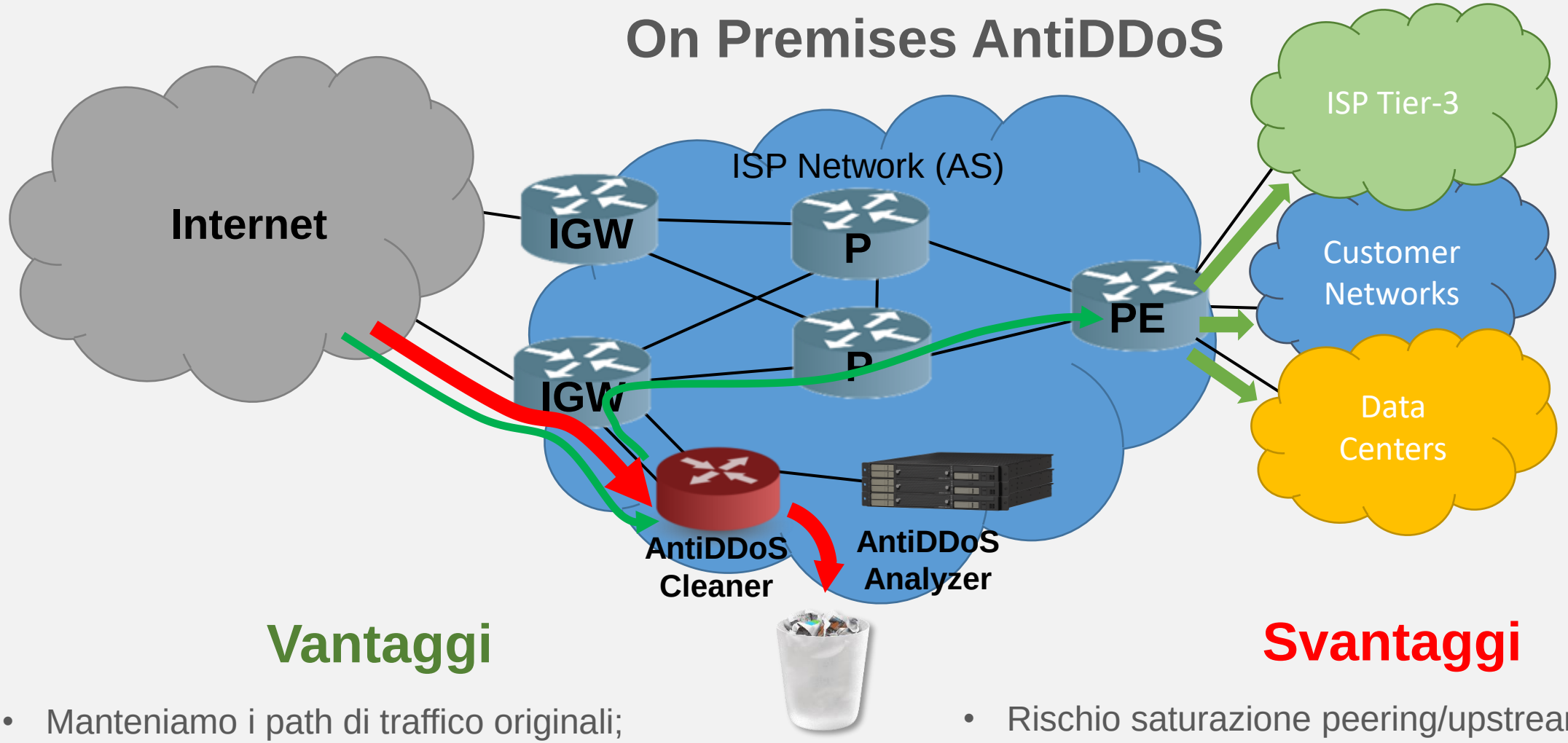
Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Come si proteggono gli ISP: AS Tier-1, Tier-2, i Datacenter e gli OTT?

Come proteggono i propri Backbone ed i clienti?

On Premise AntiDDoS

On Premises AntiDDoS



Vantaggi

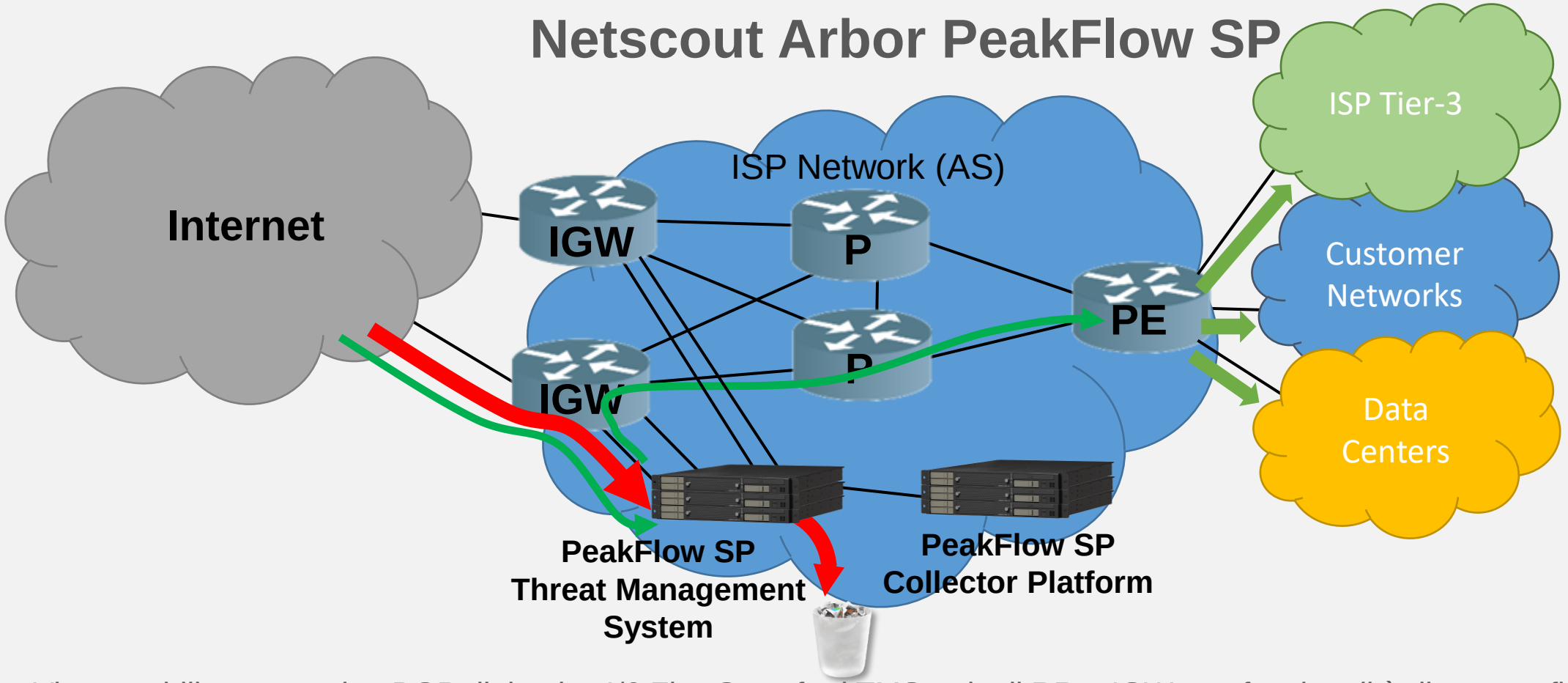
- Manteniamo i path di traffico originali;
- Piattaforma di Mitigazione in nostro controllo;
- Protegge facilmente il nostro backbone ed i clienti, agendo su tutti i prefissi IP;
- Update nuove minacce e protezione aggiuntiva via Cloud.

Svantaggi

- Rischio saturazione peering/upstream;
- Capacità di scrubbing (!?) legata alla connettività ed alle performance degli appliance AntiDDoS;
- Richiesta molta banda e router performanti;
- Costo molto elevato.

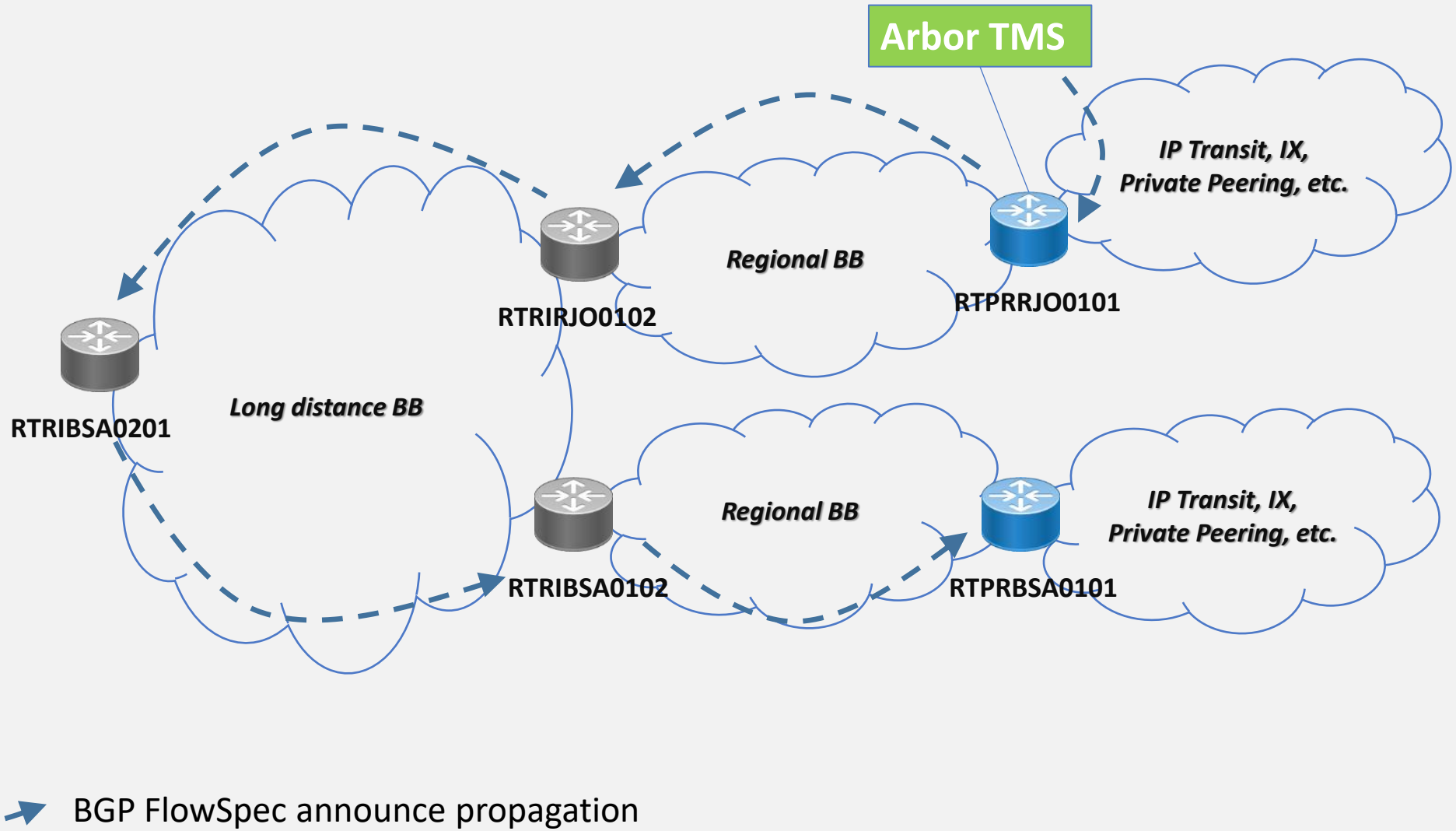
Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Netscout Arbor PeakFlow SP



- Viene stabilito un peering BGP di tipo ipv4/6 FlowSpec fra i TMS e degli RR o IGW con funzionalità di route reflector;
- Gli IGW inviano informazioni sullo del traffico TCP ed UDP ai TMS tramite il protocollo NetFlow. In caso di attacco L7, il TMS rileva le quantità di traffico anomalo destinate ad un IP/Rete ed invia ai RR un annuncio BGP FlowSpec con l'IP/Rete sotto attacco in modo che gli IGW inoltrino il traffico al TMS per la pulizia. Solo il traffico legittimo viene rimandato agli IGW per la consegna. L'annuncio FlowSpec viene propagato a tutti gli IGW e PE dai RR.
- In caso di attacco L3/4 (non è necessario un controllo applicativo), l'IGW può effettuare direttamente il blocco tramite un'ACL dinamica. Il Sistema può inoltre limitare (non bloccare) l'attacco consentendone solo una certa quantità.

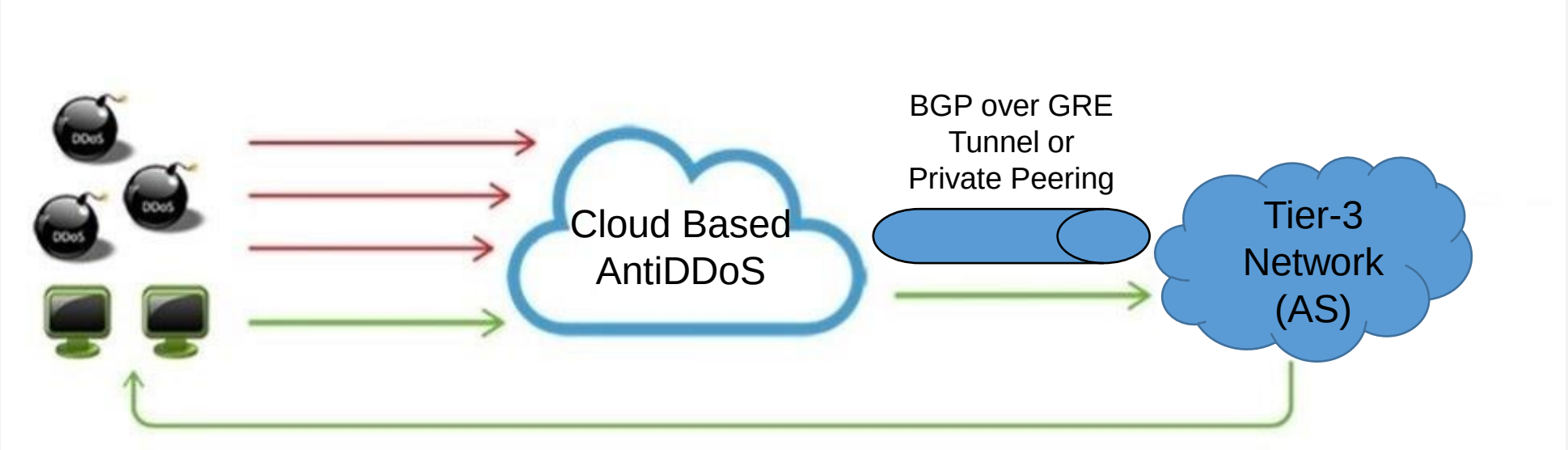
BGP FlowSpec announce in double layer route reflection scenario



Come si proteggono gli AS Tier-3?

Cloud Based AntiDDoS

Cloud Based AntiDDoS



Vantaggi

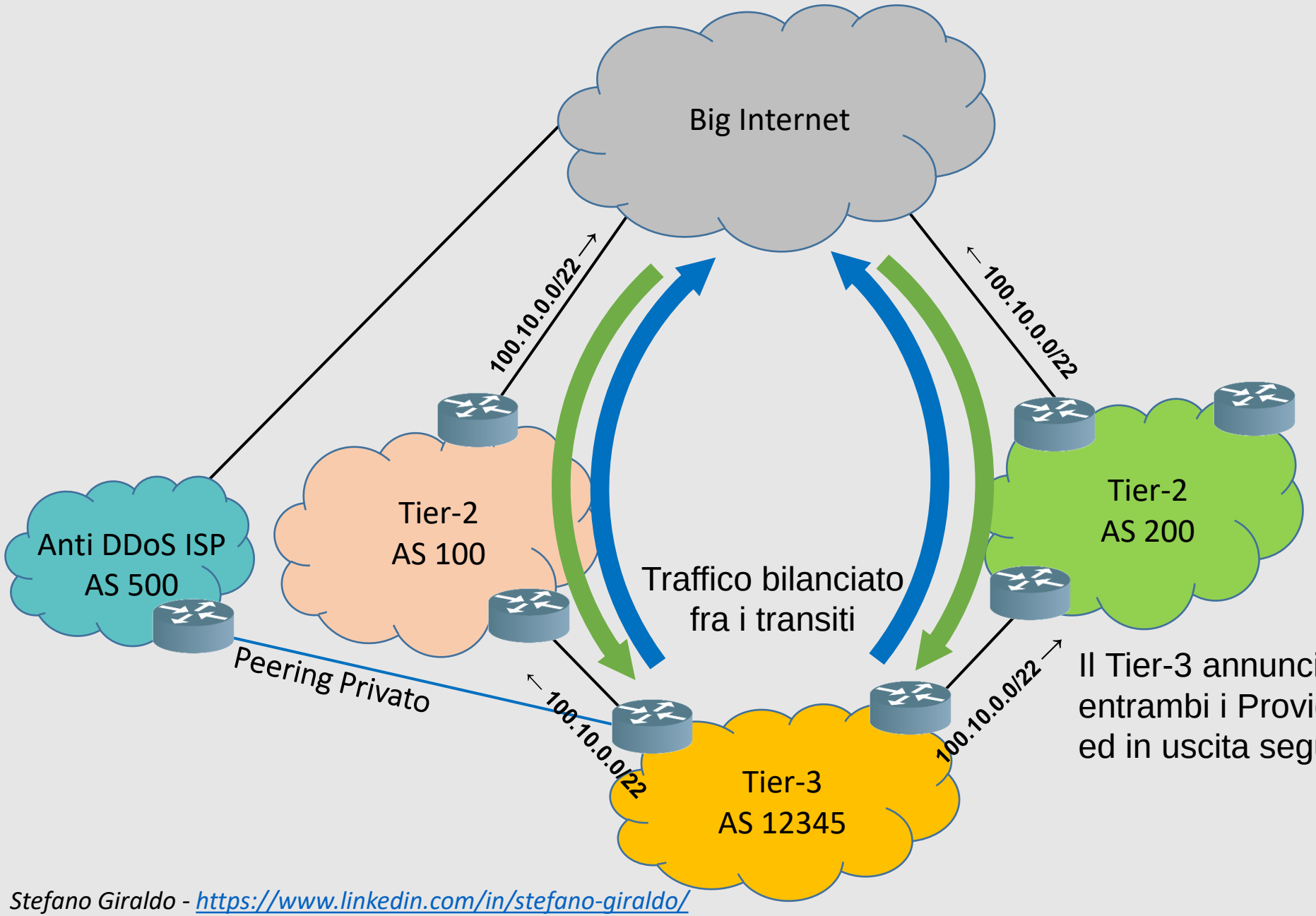
- Poco effort per gestire la piattaforma di mitigazione;
- Scrubbing Center capaci di assorbire attacchi molto forti;
- Basso rischio di saturazione degli Upstream Internet;
- Gestibile in "Always On" oppure "On Demand";
- Protezione da Layer3 a Layer7.

Svantaggi

- Funziona in base ai prefissi annunciati via BGP;
- Si sostituisce ai nostri Upstream Provider;
- Diventa inutile afferire ad un Internet eXchange;
- Dobbiamo averlo su tutti gli Upstream;
- Routing asimmetrico.

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

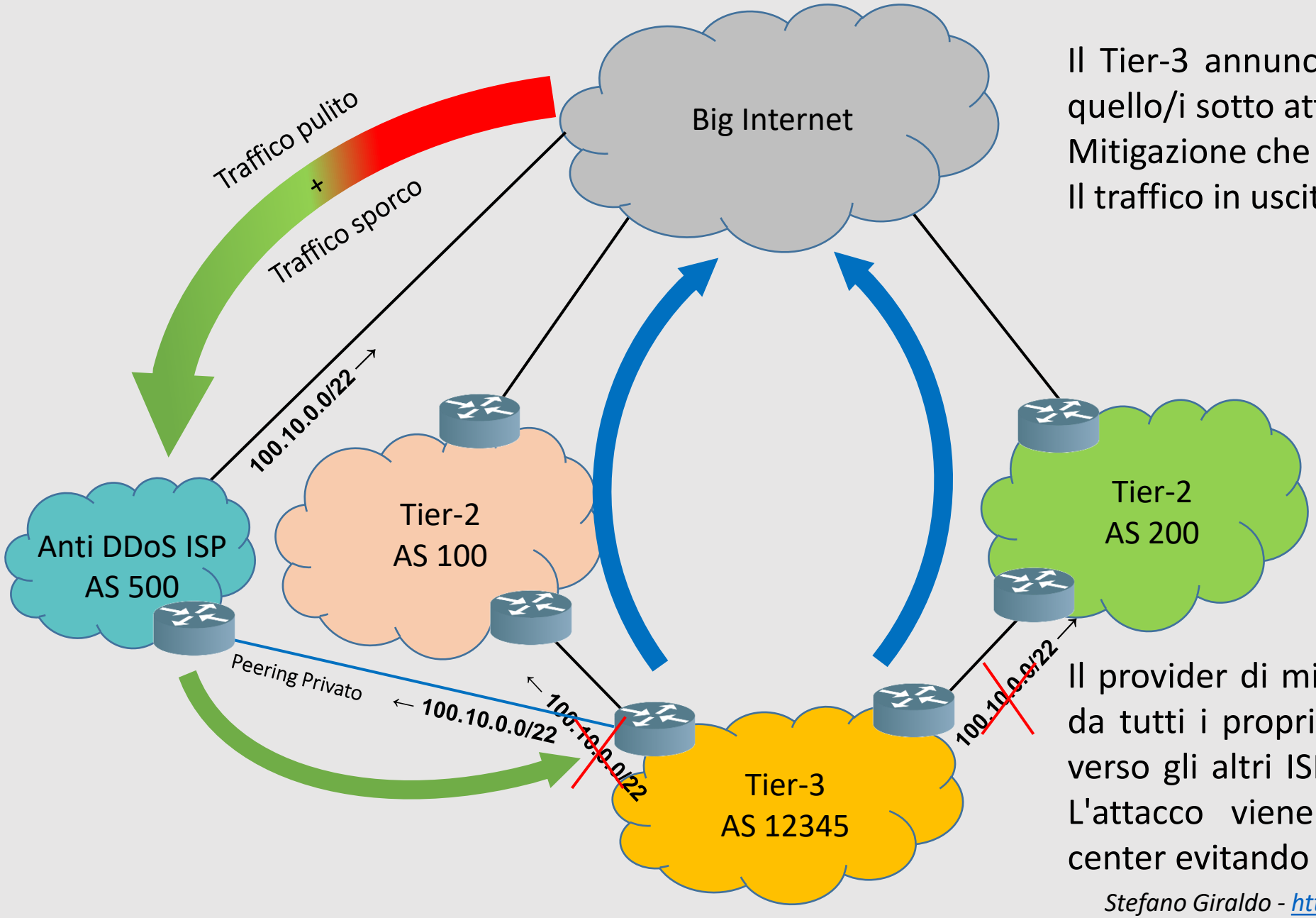
Instradamento traffico AS Tier-3 con AntiDDoS in Cloud



Il Tier-3 annuncia una major Network ad entrambi i Provider. Il traffico in ingresso ed in uscita segue il path naturale.

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Instradamento traffico AS Tier-3 con AntiDDoS in Cloud via Peering

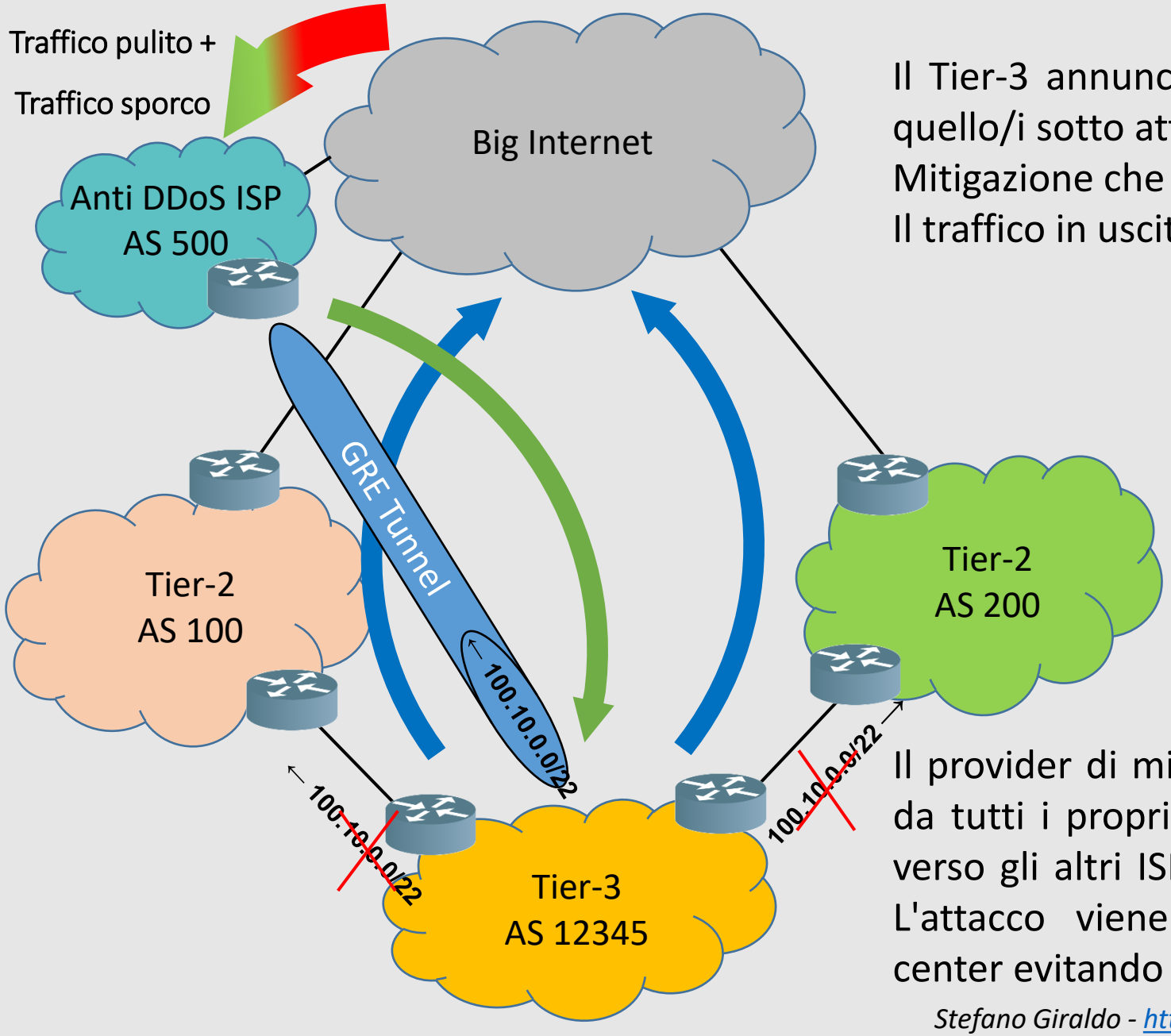


Il Tier-3 annuncia tutti i prefissi oppure solo quello/i sotto attacco (se li identifica) all'ISP di Mitigazione che gli fornirà il traffico pulito.
Il traffico in uscita segue il path naturale.

Il provider di mitigazione riannuncia i prefissi da tutti i propri scrubbing center nel mondo verso gli altri ISP, peering privati e clienti AS. L'attacco viene quindi distribuito sui vari center evitando il sovraccarico di un singolo.

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Instradamento traffico AS Tier-3 con AntiDDoS in Cloud via GRE

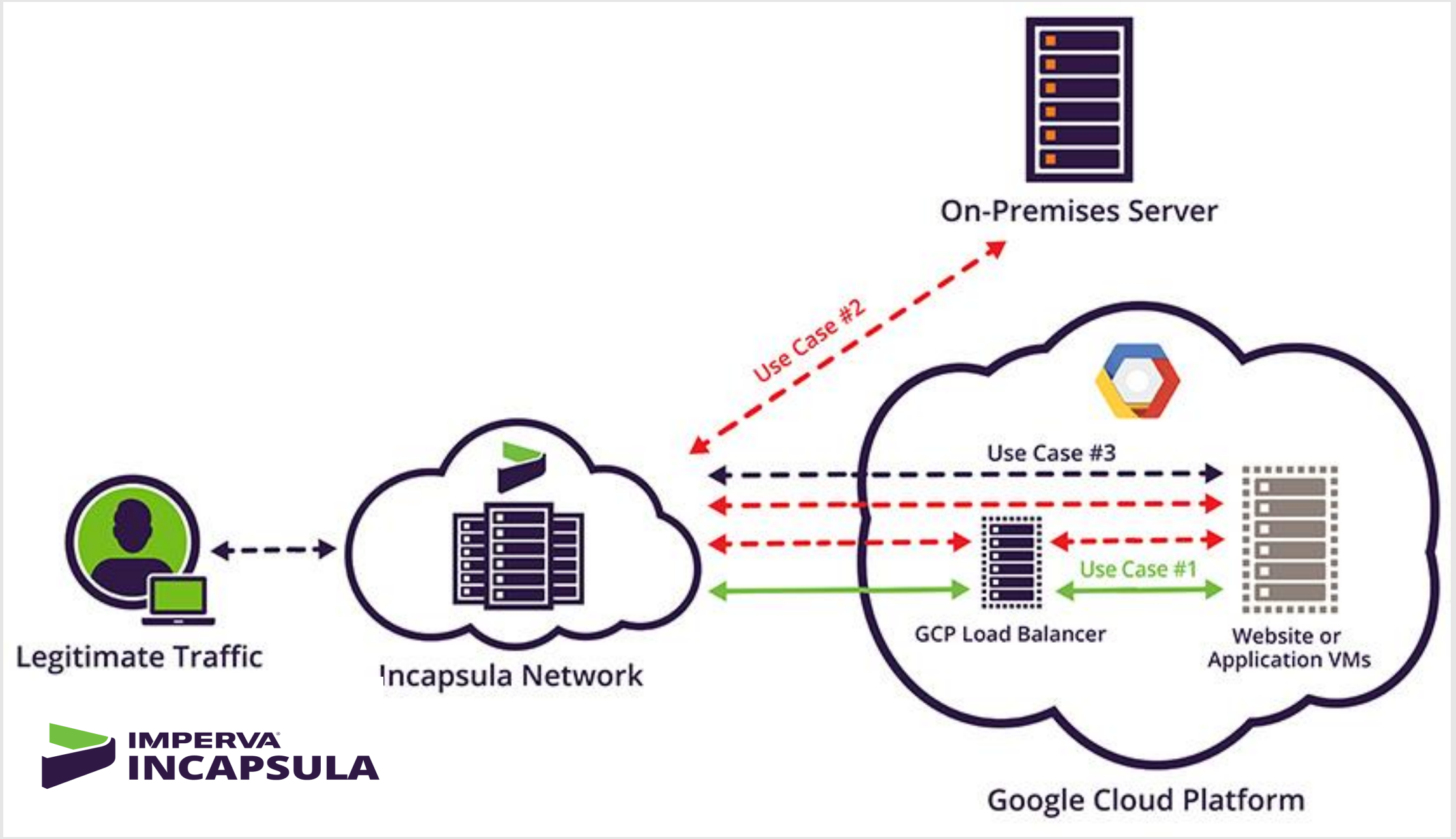


Il Tier-3 annuncia tutti i prefissi oppure solo quello/i sotto attacco (se li identifica) all'ISP di Mitigazione che gli fornirà il traffico pulito.
Il traffico in uscita segue il path naturale.

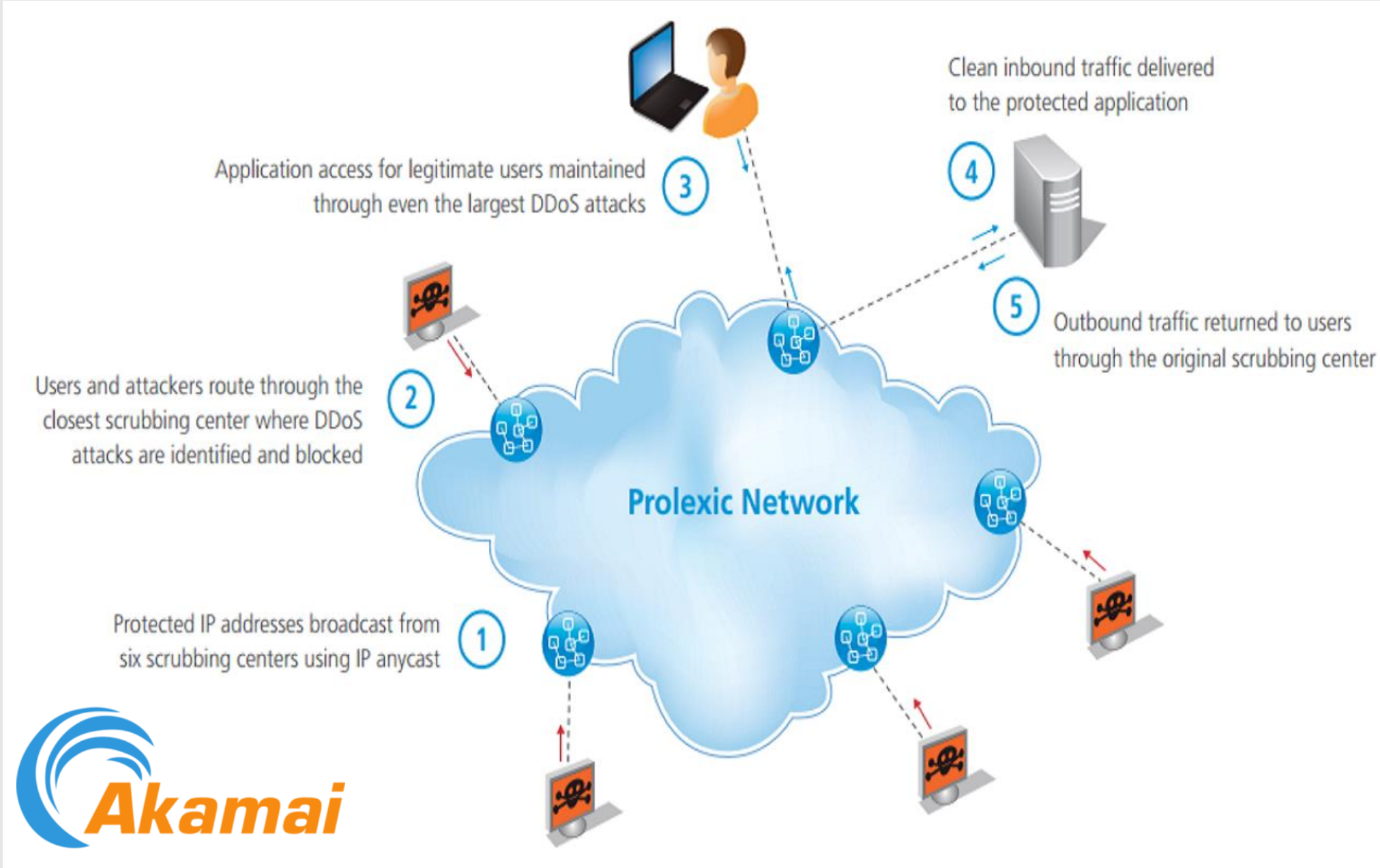
Il provider di mitigazione riannuncia i prefissi da tutti i propri scrubbing center nel mondo verso gli altri ISP, peering privati e clienti AS. L'attacco viene quindi distribuito sui vari center evitando il sovraccarico di un singolo.

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Cloud Based AntiDDoS with Content Delivery Network

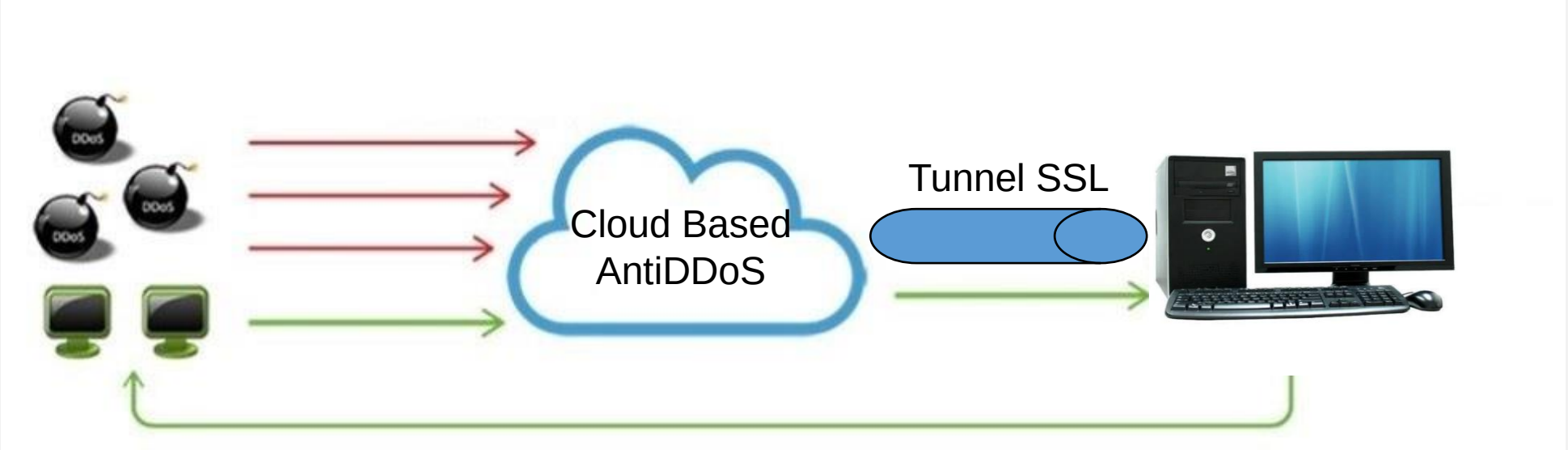


Cloud Based AntiDDoS with Content Delivery Network



Come possono proteggersi gli utenti finali?

Cloud Based AntiDDoS via VPN



Vantaggi

- Costo basso;
- Automaticamente attiva perché protegge tutte le VPN;
- Mascheramento del proprio IP;
- Può essere usato con qualunque ISP e non richiede di essere un AS e di avere un proprio indirizzamento IP;
- Protezione da Layer3 a Layer7.

Svantaggi

- Potenziale aumento della latenza;
- Percorso verso la destinazione più lungo;
- Potenziale calo delle performance;
- Potenziali server di terminazione VPN, fisicamente distanti;
- Rischio tracciamento del traffico.

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Cloud Based AntiDDoS via VPN

Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Most famous DDoS attacks

Largest European DDoS Attack on Record

https://www.akamai.com/blog/security/largest-european-ddos-attack-ever

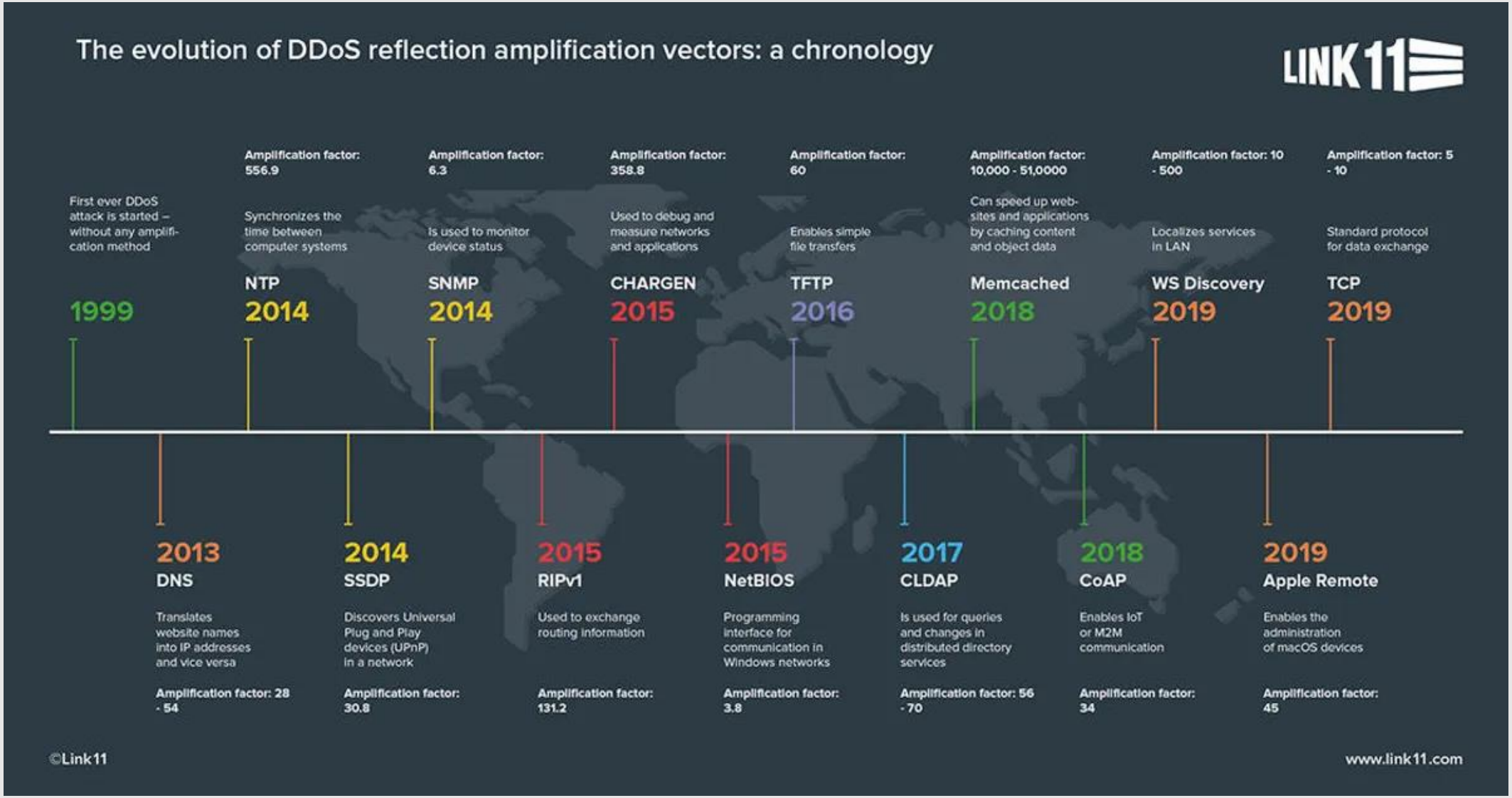
Cloudflare: Famous DDoS Attacks

https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

A10: 5 Most Famous DDoS Attacks

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Amplification Techniques in the years



Stefano Giraldo - https://www.linkedin.com/in/stefano-giraldo/

Realtime DDoS attacks maps

https://horizon.netscout.com/

https://cybermap.kaspersky.com/it

https://www.imperva.com/cyber-threat-attack-map/

Conclusioni

Chi vince e chi perde?

AntiDDoS

Lo scudo 2.0 nell’era della guerra telematica

Grazie per l'attenzione

https://www.linkedin.com/in/stefano-giraldo/