TelekomSlovenije

TelekomSlovenije

Mitja Jenček

Postopki in metode odbijanja DDoS-napadov

Zakaj potrebujemo sistem za DDoS-zaščito?

DDoS-napadi

Gre za napade na ponudnikovo kritično infrastrukturo ter usmerjene napade na posamezne uporabnike z namenom, da onemogoči storitev za krajše ali daljše obdobje.

Vsak DDoS-napad ima vsaj tri vključene deležnike:

- napadalec (oseba, ki izvaja napad),
- žrtev (računalnik, ki je napaden z namenom, da je onemogočena uporaba storitev),
- uporabniki (osebe, ki trpijo posledice napadov na ponudnikovo infrastrukturo za čas DDoS-napada).

Pogostost napadov se veča. Neodvisne študije ugotavljajo, da se vsako uro zgodi 28 napadov.

Zakaj potrebujemo sistem za DDoS-zaščito?

Kdo izvaja DDoS-napade in zakaj?

Heaktivisti (Hacktivists) – Gre predvsem za napadalce, ki so izrazito politično motivirani. DDoS-napade uporabljajo kot orodje nasprotovanja političnim gospodarskim odločitvam (Anonymous – ACTA, feb. 2012).

Izsiljevalci (Extortionists) – Namen je izsiljevanje uporabnika oz. ponudnika storitev.

Konkurenti – DDoS-napadi so lahko orodje za oteževanje poslovanja konkurence (Cyber Monday).

Vandali (Black hat) – napadalci iščejo osebno zadovoljstvo v tovrstnih napadih.

Požarne pregrade, sistemi za preprečevanje vdorov (IPS)

- Požarne pregrade omejujejo dostop samo do določenih IP naslovov in portov
- IPS naprave blokirajo znane ranljivosti sistemov (s pomočjo podpisov napadov)
- DDoS napad je lahko sestavljen iz regularnega prometa, ki ga požarne pregrade in IPS naprave spustijo skozi. Lahko pa tudi DDoS napad onemogoči delovanje teh naprav

Zakaj potrebujemo sistem za DDoS-zaščito?

	Country/Region	Q4 '14 Traffic %	Q3 '14 %
1	China	41%	49%
2	United States	13%	17%
3	Taiwan	4.4%	3.8%
4	Russia	3.2%	2.1%
5	Turkey	2.9%	1.3%
6	South Korea	2.8%	1.4%
7	India	2.4%	2.9%
8	Brazil	2.3%	1.9%
9	Germany	1.8%	0.6%
10	Hong Kong	1.3%	0.8%
–	Other	25%	18%

Figure 1: Attack Traffic, Top Originating Countries/Regions (by source IP address, not attribution)

Port	Port Use	Q4 '14 Traffic %	Q3 '14 %
23	Telnet	32%	12%
445	Microsoft-DS	15%	8.1%
8080	HTTP Alternate	6.6%	2.5%
80	HTTP (WWW)	6.4%	4.6%
3389	Microsoft Terminal Services	5.9%	2.6%
22	SSH	4.7%	1.8%
1433	Microsoft SQL Server	4.2%	2.9%
3306	MySQL	1.8%	1.1%
443	HTTPS (SSL)	1.7%	1.3%
9064	(Unassigned)	1.6%	0.1%
Various	Other	21%	–

Figure 2: Attack Traffic, Top Ports

Različne metode DDoS-napadov

Področja oziroma tipi napadov:

- Omrežni napadi (OSI-model 3&4) – napadi, kjer z veliko količino prometa onemogočimo delovanje sistema (na primer Syn flood napadi). Poznani so primeri z več kot 200 G prometa.
- Protokolni napadi – napadi, ki se odvijajo predvsem na komunikacijski opremi in onesposobijo delovanje, npr. požarne pregrade oz. „load-balacerje“.
- Aplikacijski napadi (OSI layer 7) – napadi na vire, ki jih uporablja posamezna aplikacija. Namen je onemogočiti delovanje posamezne aplikacije.

Vloga ISP pri preprečevanju DDoS-napadov

Kaj lahko ponudniki storijo za uporabnike pri DDoS-napadih?

DDoS-napadi na infrastrukturo ISP lahko povzročijo degradacijo storitev za uporabnike.

Ponudniki ščitijo lastno infrastrukturo in povezave uporabnikov.

Vprašanja, ki jih lahko zastavimo ponudniku:

- Kakšno vrsto zaščite DDoS ponuja?
- Kakšne vrste napadov lahko preprečuje (network layer, application layer)?
- Katere storitve lahko ščitijo DNS-strežnike, infrastrukturo in spletne strani?
- Koliko zaščite lahko nudi?
- Kakšen SLA se uporablja pri „mitigaciji“ napadov?
- Ali lahko terminira storitve ob DDoS-napadu?

Izbira sistema za preprečevanje DDoS-ov

Ključni faktorji pri izbiri DDoS-sistema

Detekcija napada: Uporabljamo lahko avtomatsko ali manualno detekcijo. Trenutno je večina zaznav ročnih v ponudnikovih nadzornih centrih (24/7 monitoring, človeški faktor). Avtomatska detekcija je v tem pogledu boljša.

Čas mitigacije: Zaznava DDoS-ov ni dovolj, potrebno je čimprej ukrepati. Obstajajo različni načini, vendar mora biti čas do mitigacije čim krajši.

Prepoznavanje vsebine napadov: Sistem mora razlikovati med primerno in škodljivo vsebino – Human Traffic 38,5 %, Non-Human Traffic 61,5 % (Search engine-boots, Spammers, Site scrappers).

Izbira sistema za preprečevanje DDoS-ov

Modeli implementacije sistemov za preprečevanje DDoS

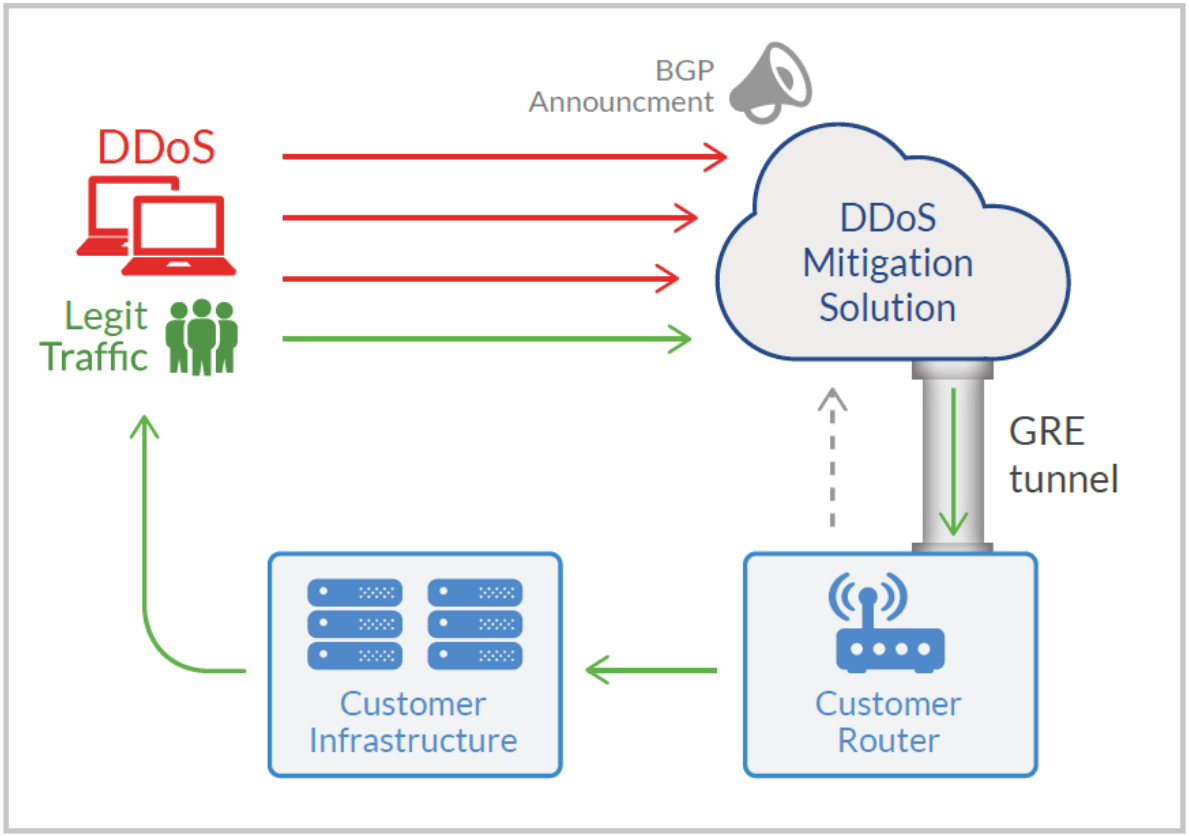
DNS-preusmeritev:

DNS-preusmeritev, kjer preusmerimo ves internetni promet (HTTP/HTTPS) prek sistema DDoS.

Izbira sistema za preprečevanje DDoS-ov

Modeli implementacije sistemov za preprečevanje DDoS:

BGP Routing :



Blackhole:

Aktivacija Blackhole storitve:

Na podlagi sistema za detekcijo zaznavamo anomalije:

Flow (sampling).

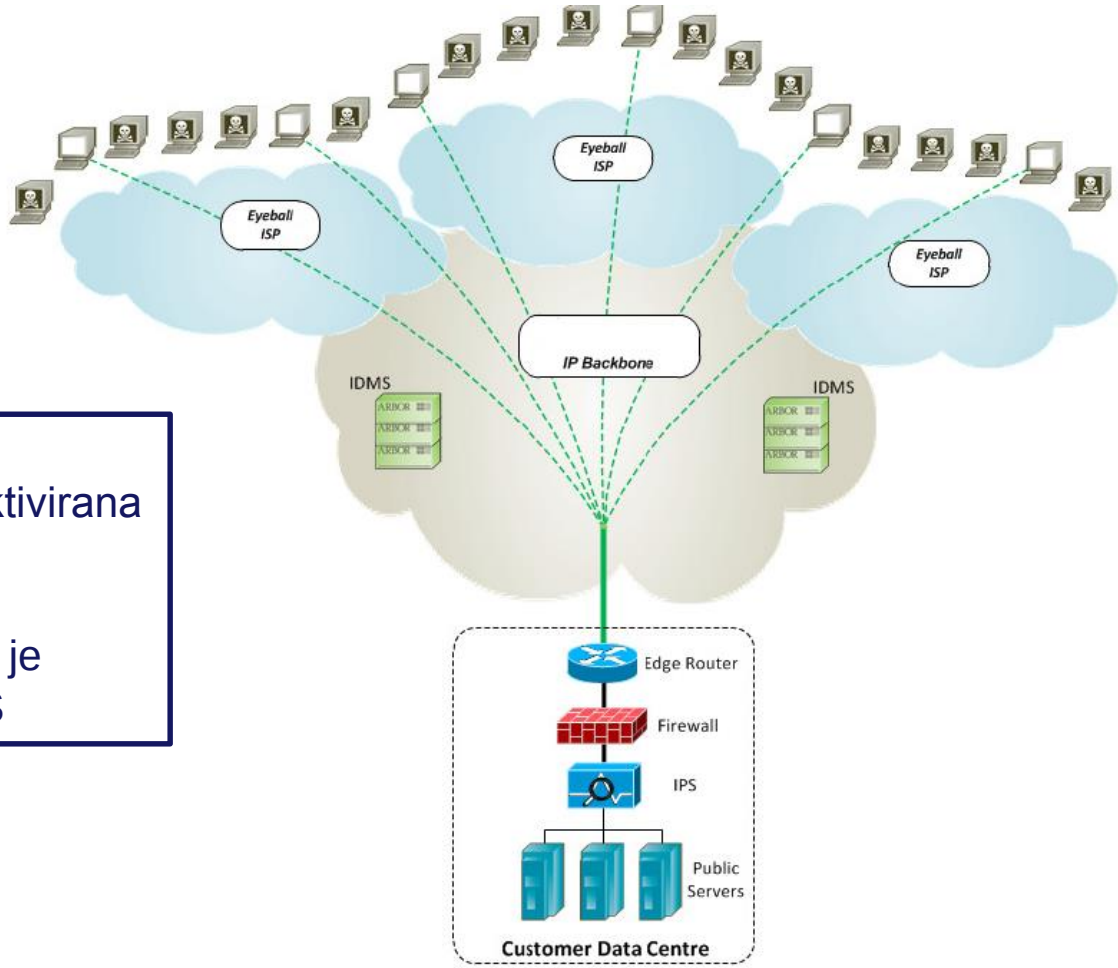
Aktivacija Bhole z oglaševanjem usmerjevalne poti proti nadrejenemu omrežju z uporabo dogovorjenega BGP community.

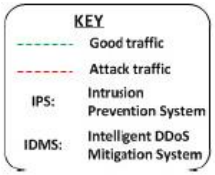
- Ponudnik mora podpirati BGP Blackhole servise.
- Tipično je dovoljen Blackhole samo za poti, definirane v IRR-bazi (Internet Routing Registry).

Kako deluje: Pred napadom

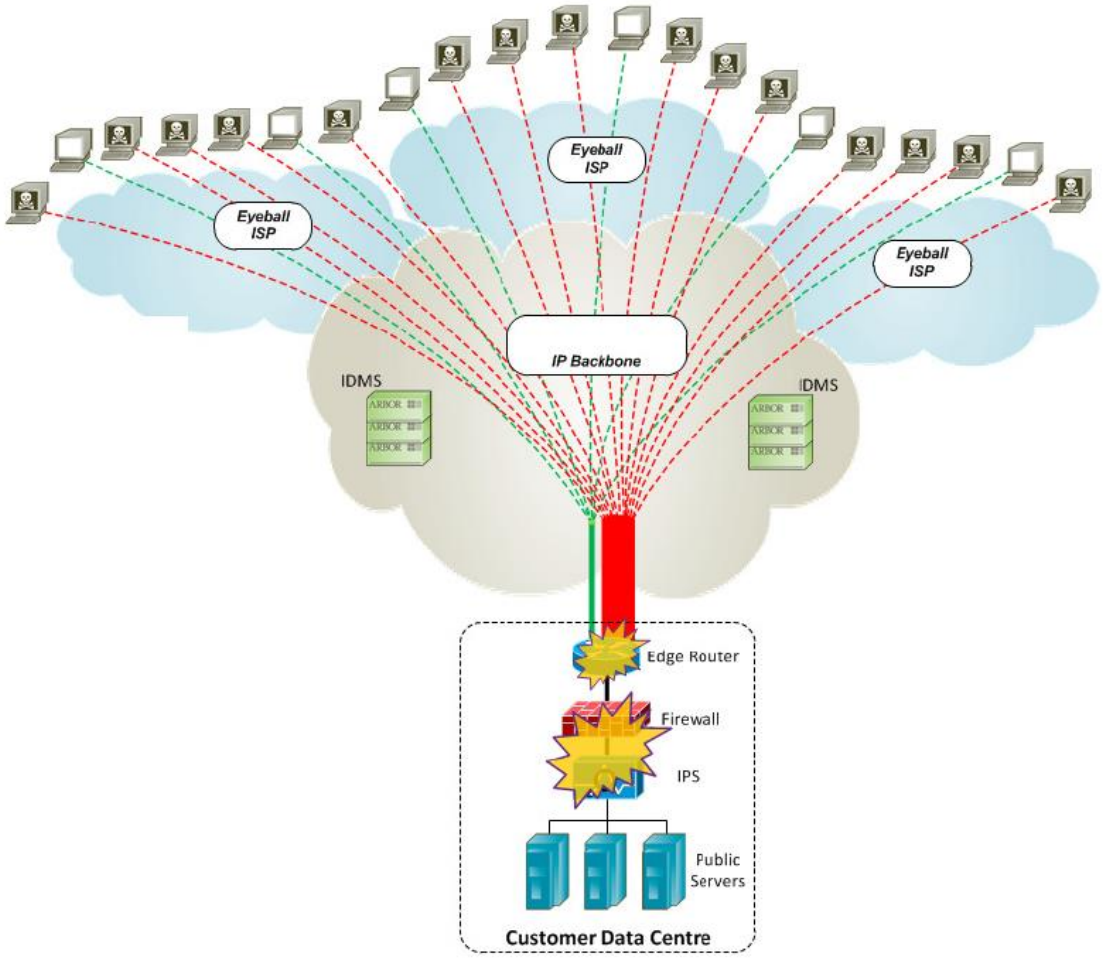
Pred napadom:
DDoS-zaščita ni aktivirana

Promet do uporabnikovega IP je usmerjen skozi AS

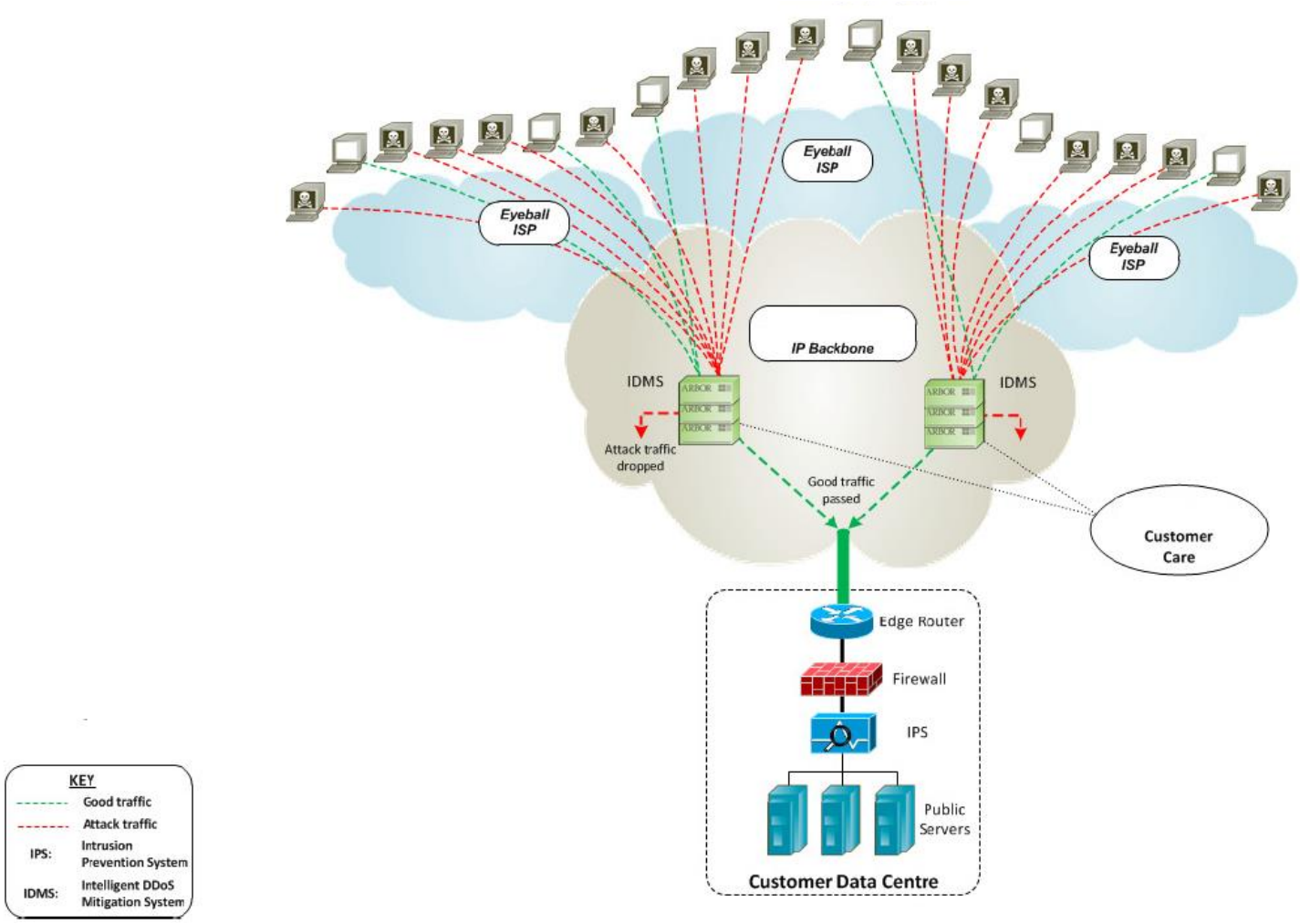




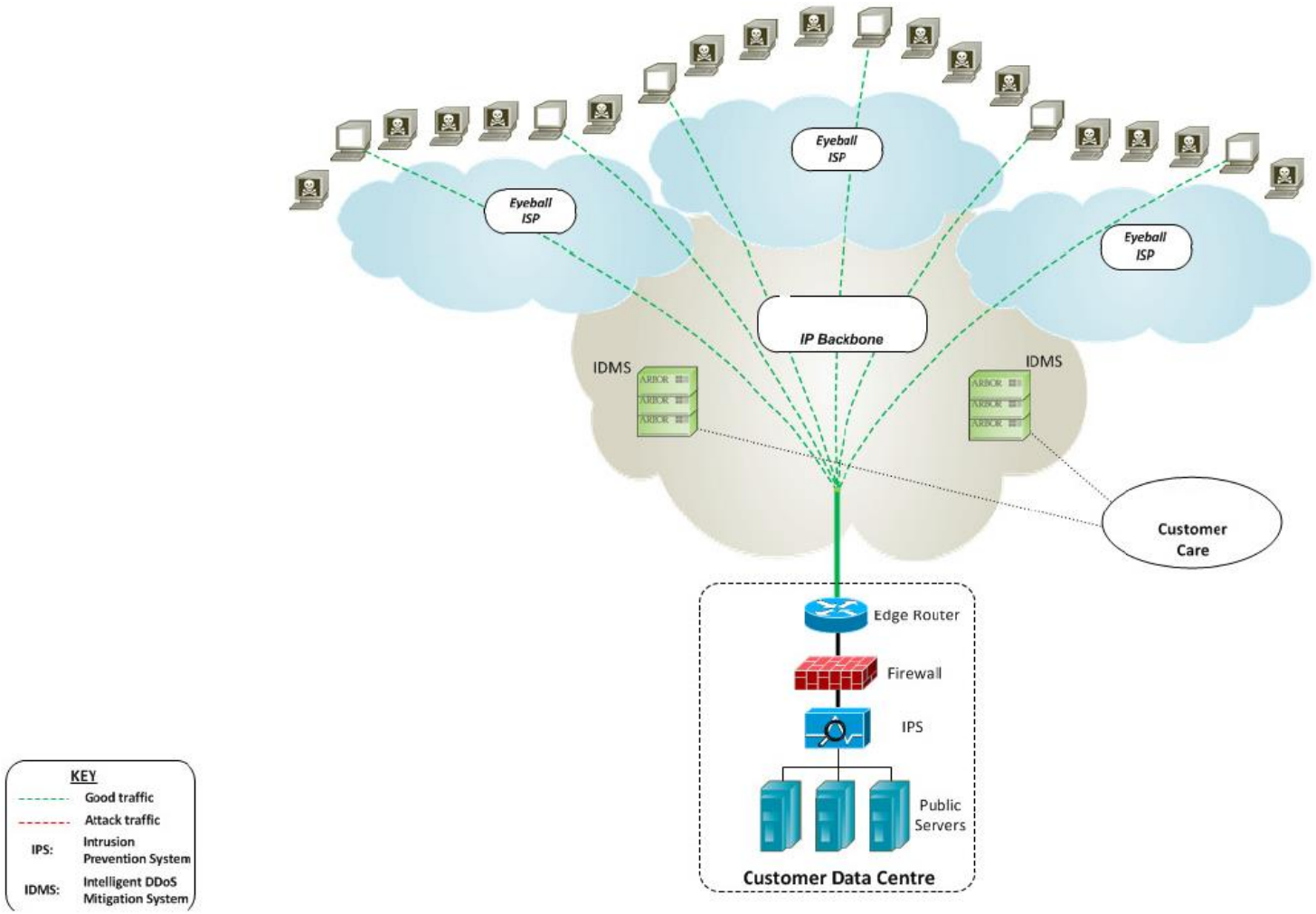
Kako deluje: Med napadom



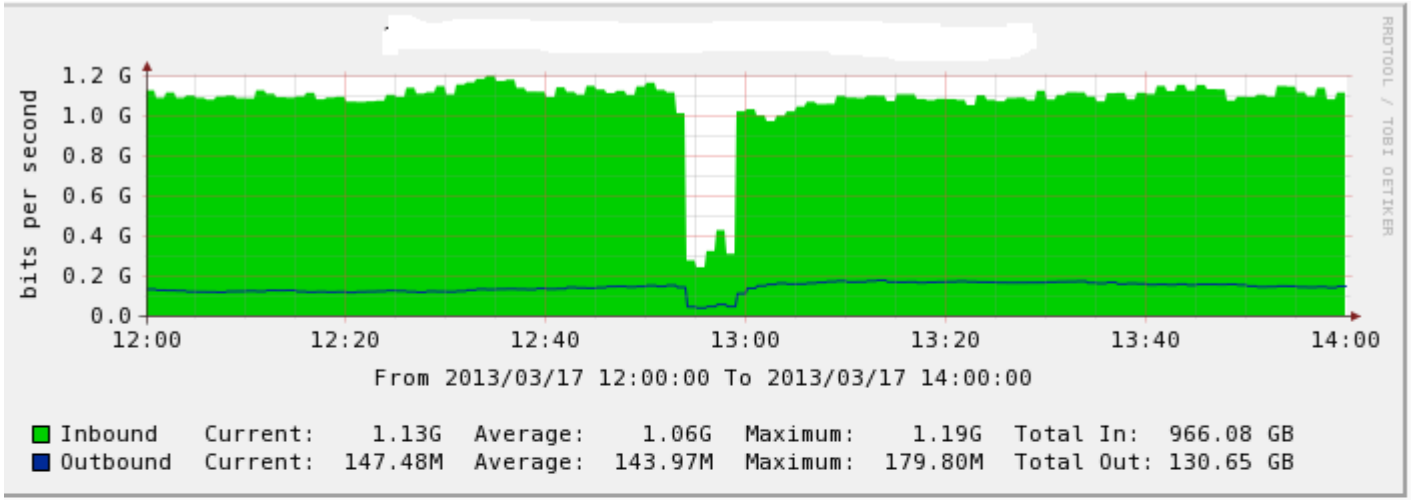
Kako deluje: Vključena zaščita

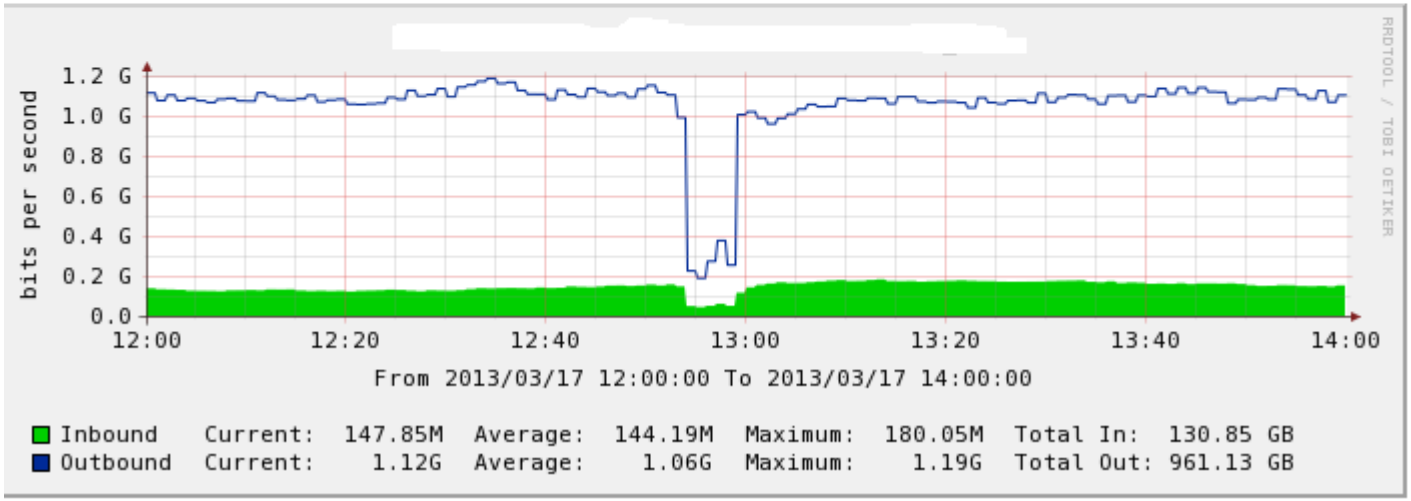


Kako deluje: Vključena zaščita

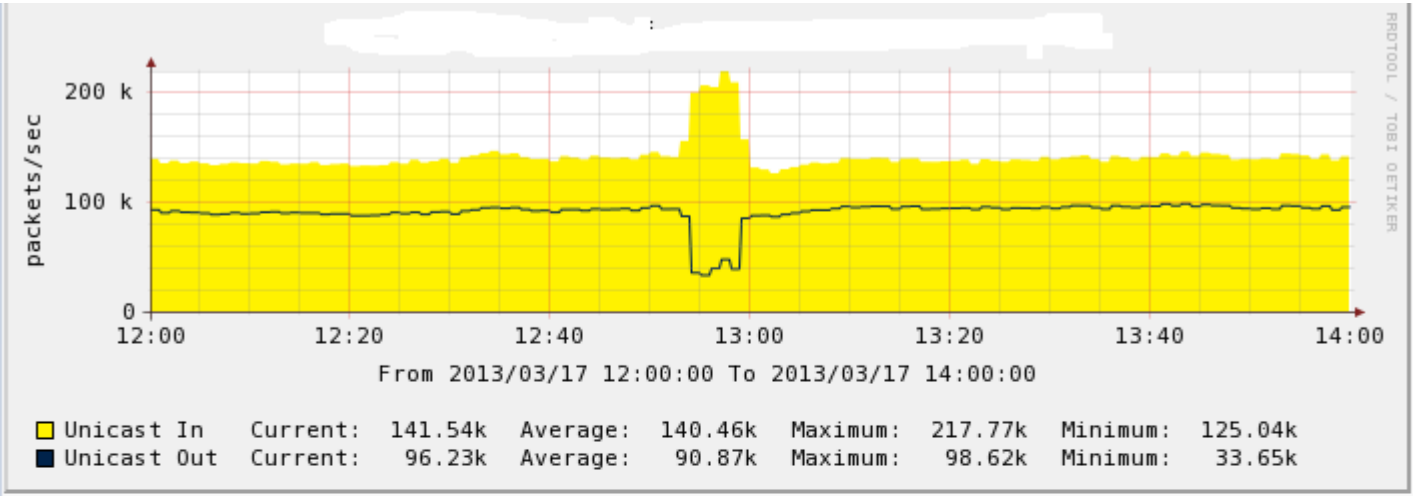


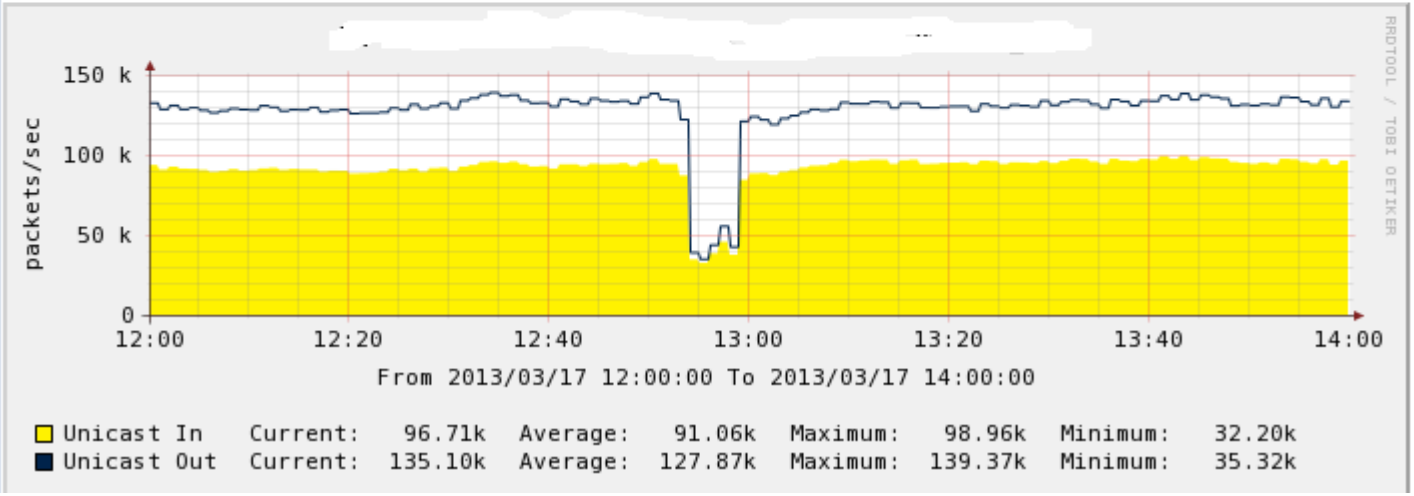
Nenaden padec prometa. Zakaj?





Paketi na sekundo?

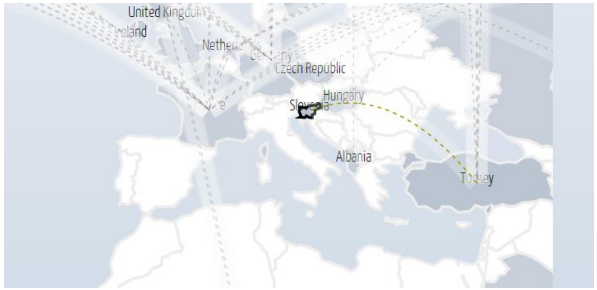




Kaj se je zgodilo?

- Povečano število paketov je povzročilo:
  - IPS sistem je preklopil v Bypass način
  - Na požarni pregradi se je povečala obremenitev procesorja na 100%, zato ni zmogla obdelati vsega legitimnega prometa uporabnikov, posledično je promet padel.

439347		**High** 418.3% of 300 Kpps 19.0 Gbps, 2.3 Mpps	**DoS Alert** Incoming UDP Misuse Attack to	Apr 20 20:19 - 20:32 (0:13)
439346		**High** 4,224.5% of 250 Mbps 19.0 Gbps, 2.3 Mpps	**DoS Alert** Incoming Total Traffic Misuse Attack to	Apr 20 20:19 - 20:33 (0:14)



TelekomSlovenije

Hvala za pozornost

mitja.jencek@telekom.si