Dutch Continuity Board

Home About Us How we work Contact

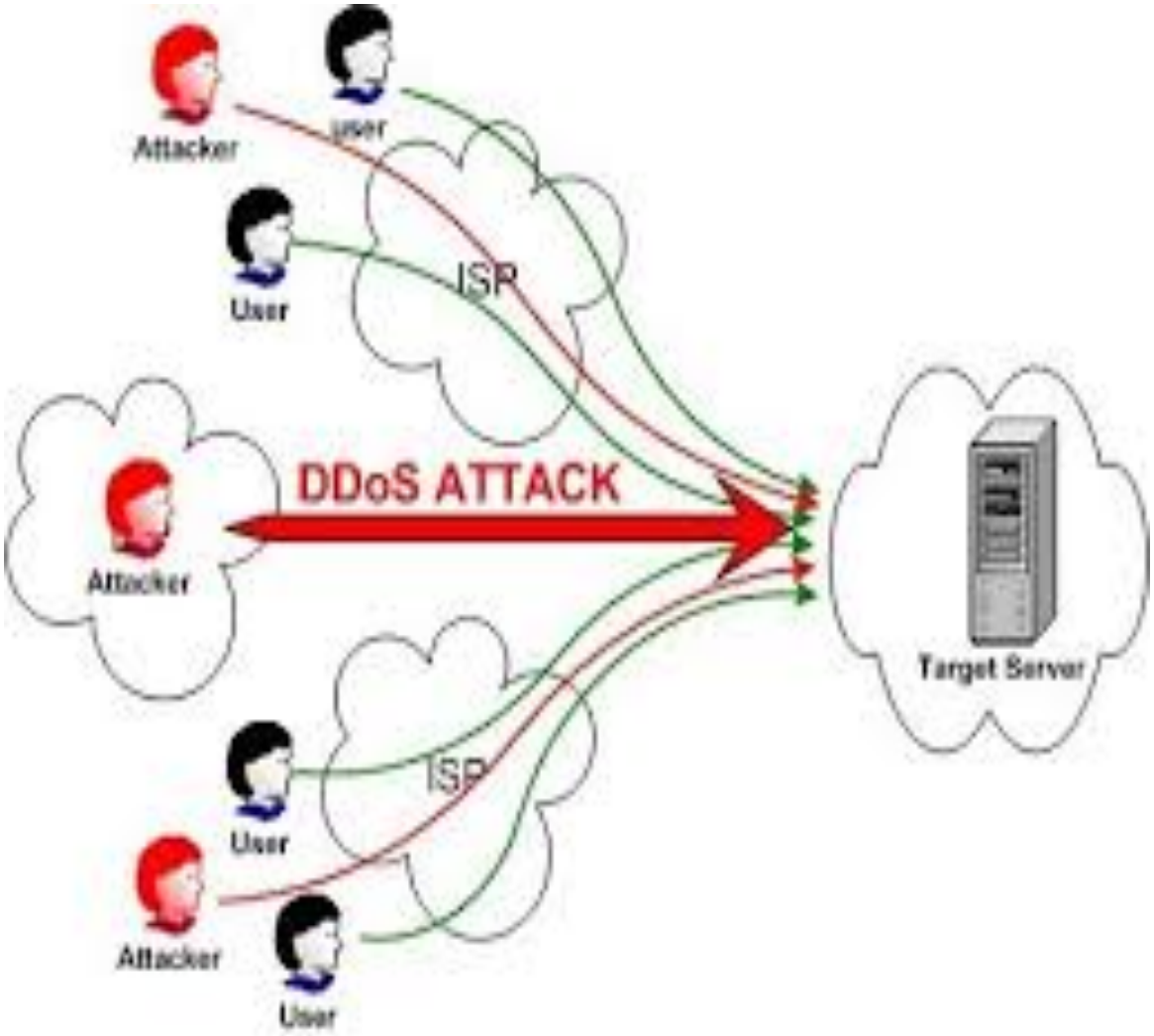
Dutch Continuity Board

Protecting The Netherlands against DDoS attacks.

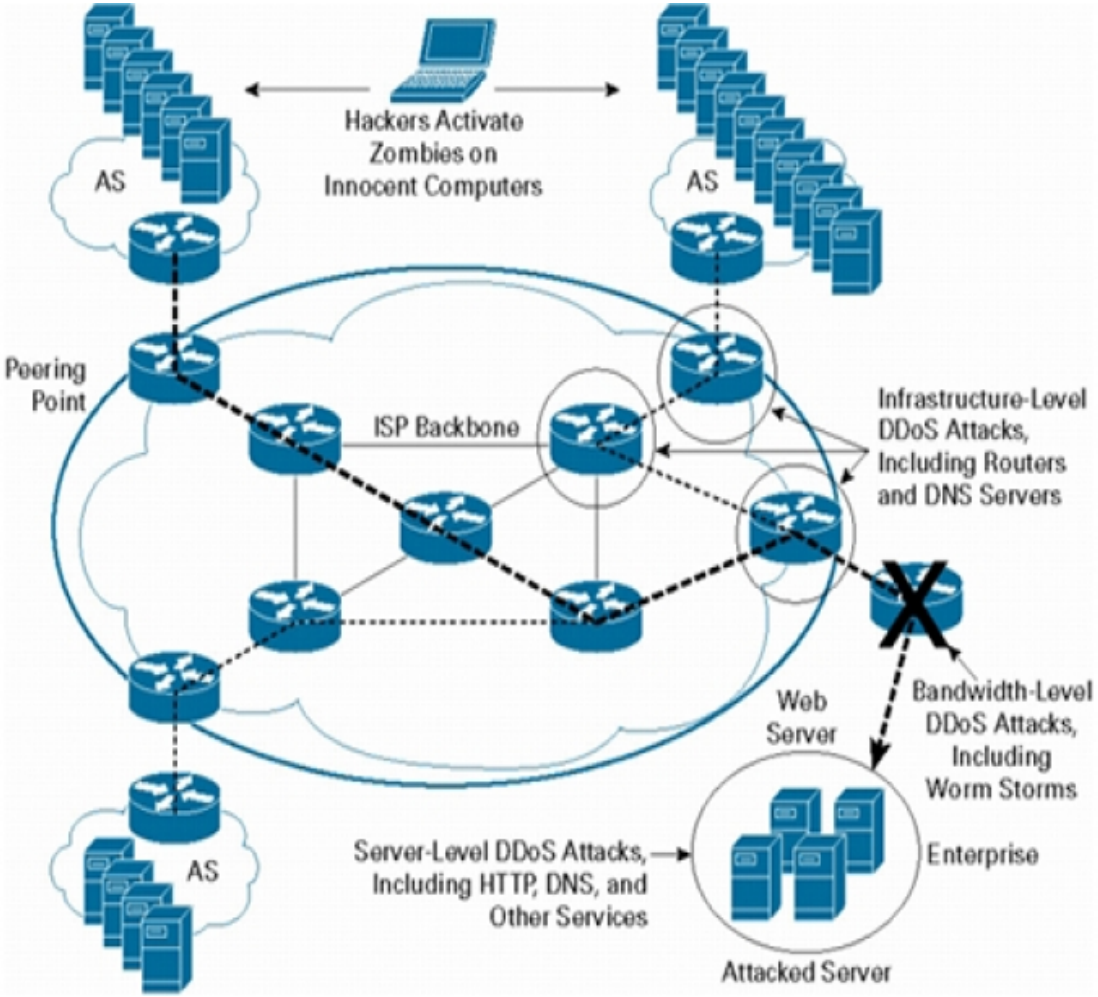
About us How we work

kpn

What does DDOS look like?

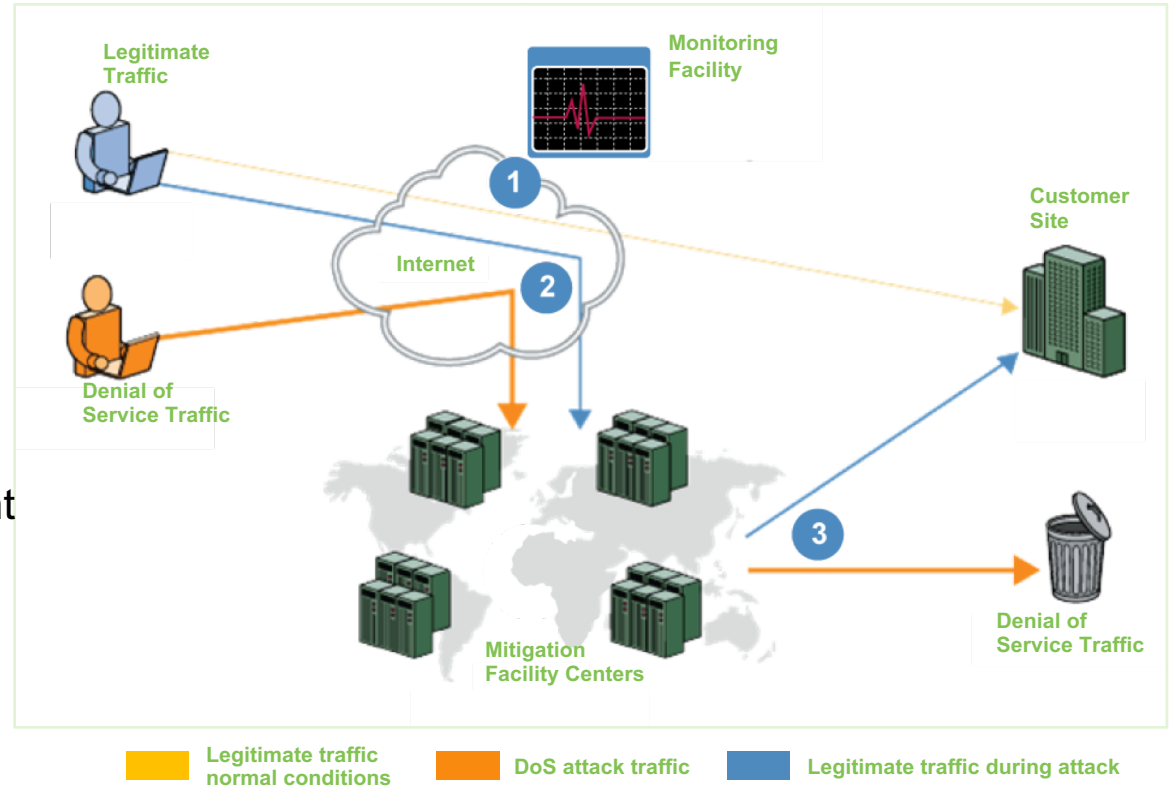


How do DDOS attacks work?



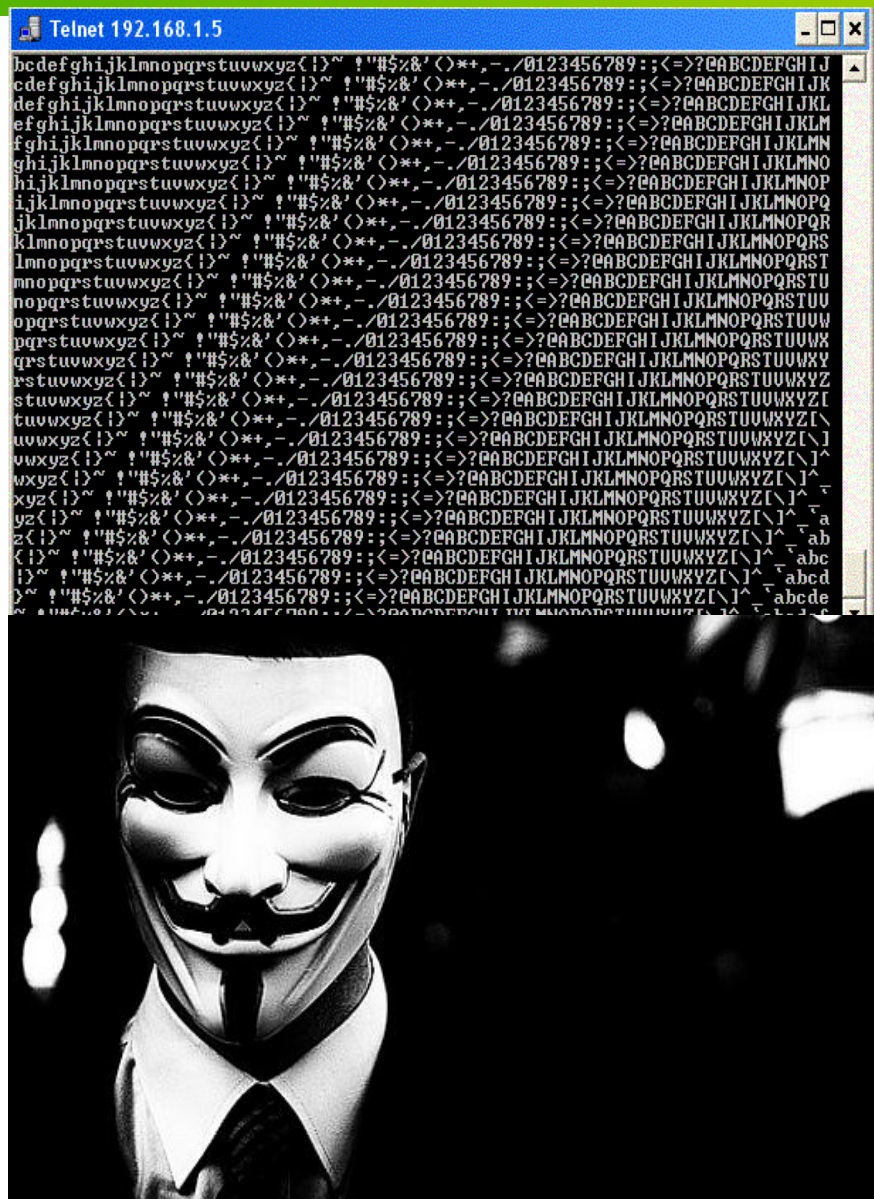
How does Anti –DDOS work?

1. Traffic is actively monitored.
2. During and attack the traffic gets redirected to a mitigation center to get ‘’scrubbed’.
3. Legitimate traffic gets sent back to the customer site as the DDOS traffic gets removed.



Observations

- Anonymous and hactivism on the rise
- Rise in multi-vector, volumetric attacks, longer duration
- UDP Fragment, NTP, DNS amplication, and Chargen still most popular
- Application level attacks on the rise
- Cloudflare and Spamhaus = 300 GB
- Latest American Observed DDOS =1.7 TB



Dutch Continuity Board

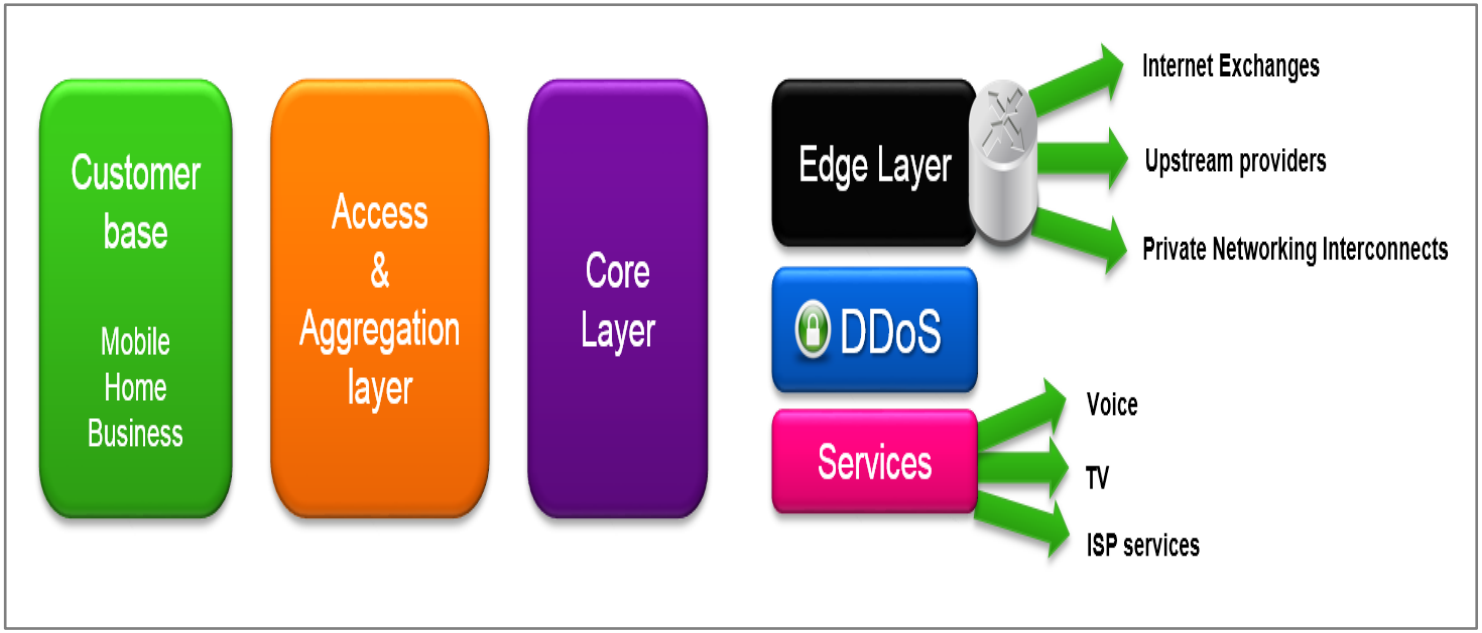
Dutch Continuity Board is similar to Abuse-IX can share information and shut down traffic during incidents as well as regular process on malicious traffic, open resolvers, and other sources of attacks. This currently is supported by all Telco's as well as NCSC; VNO NCW; NED ICT and is regarded favorably by EZ.

DCB Charter

- Structural cooperation among operators to mitigate severe DDoS attacks
- DCB resides under the Telecom ISAC and closely cooperates with other entities
  - o-IRT-o
  - ICT response board
  - OPS-Trust DDoS working group
- Share information and best practices between operators
- BCP 38, 84, MANRS

Graduated levels of Readiness

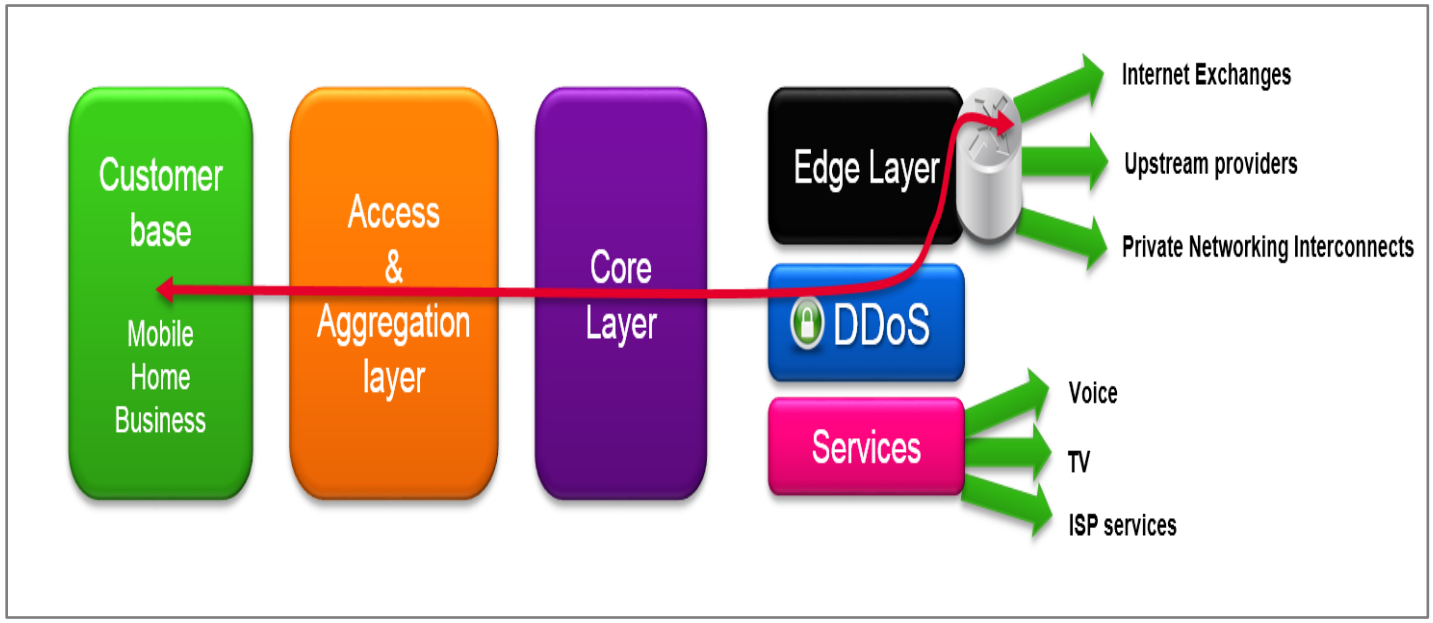
DEFCON 5 FADE OUT



Situation: Normal readiness..

Graduated levels of Readiness

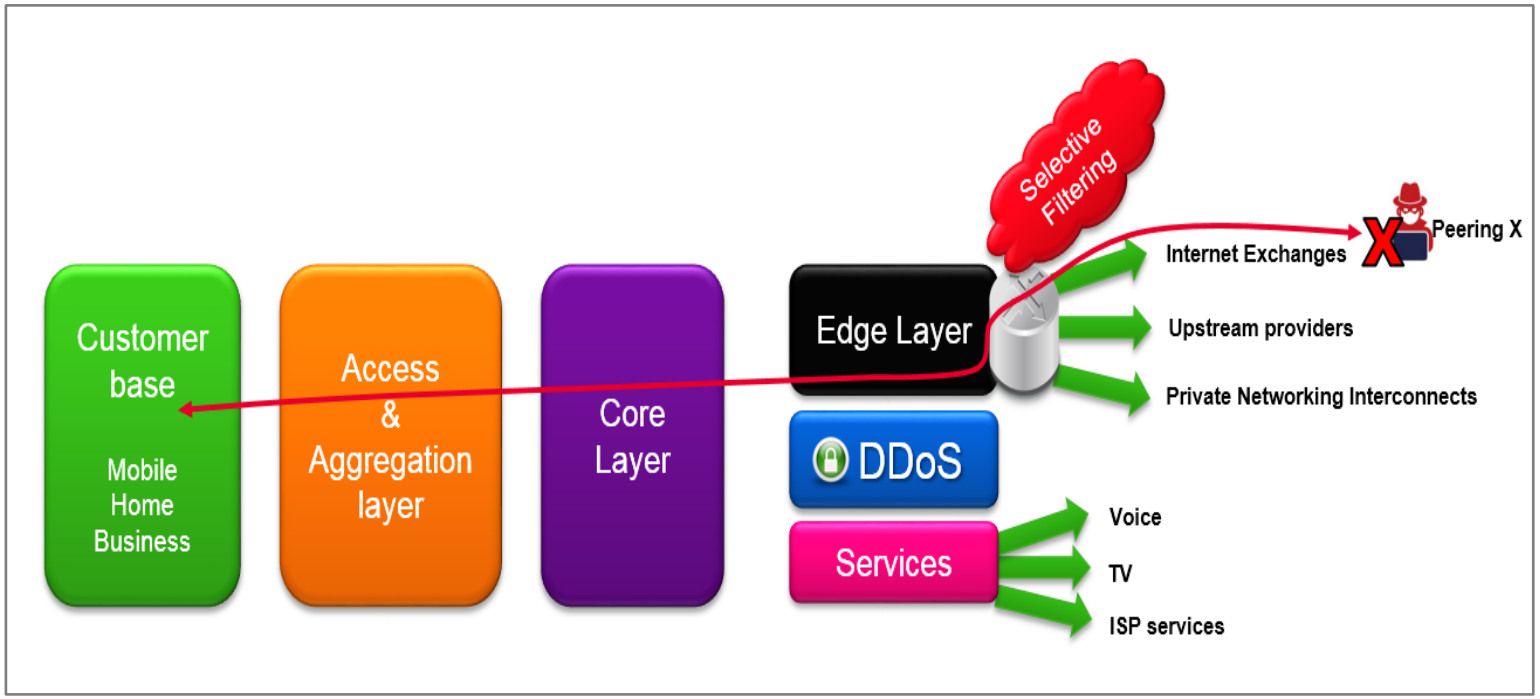
DEFCON 4 DOUBLE TAKE



Situation: Anti-DDOS.nl traffic washing in effect.

Graduated levels of Readiness

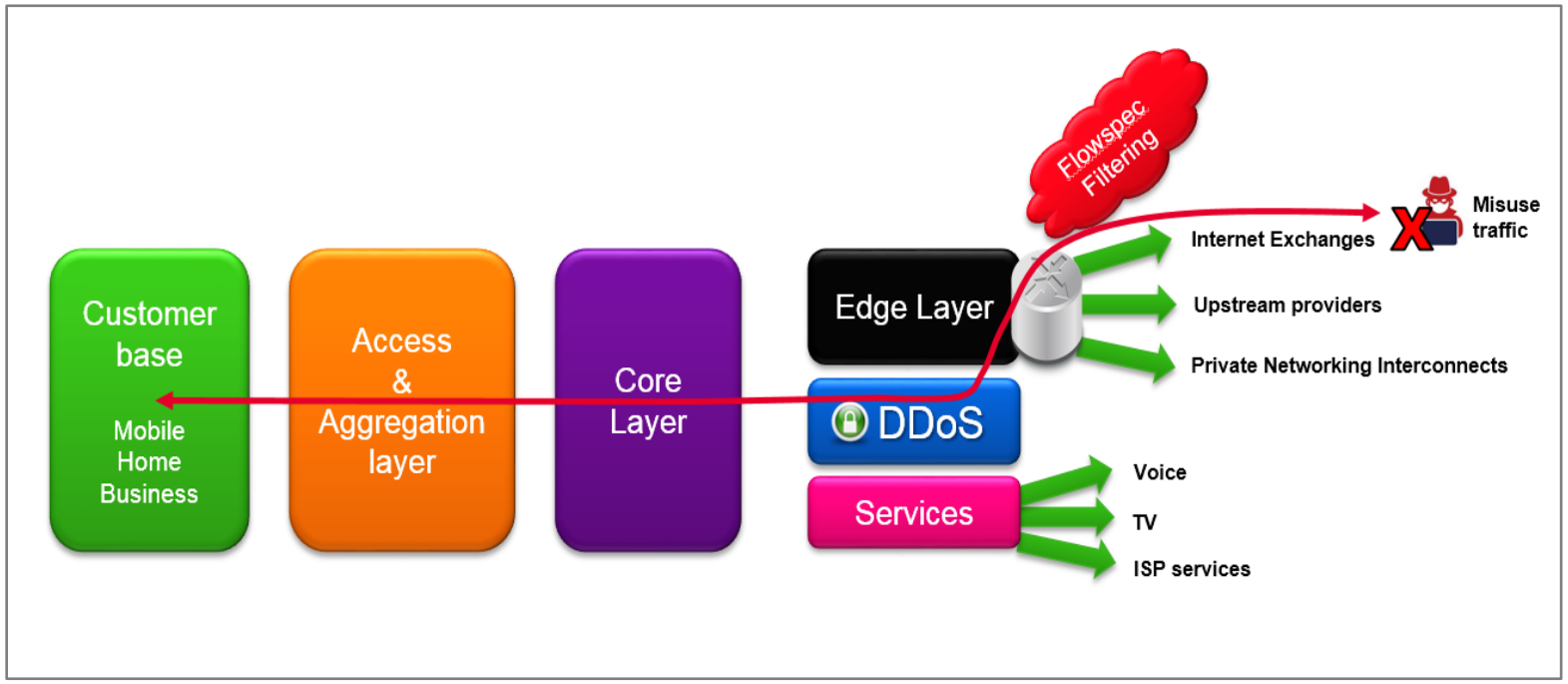
DEFCON 3 ROUND HOUSE



Situation: Anti-DDOS.nl in effect with selective Black holing.

Graduated levels of Readiness

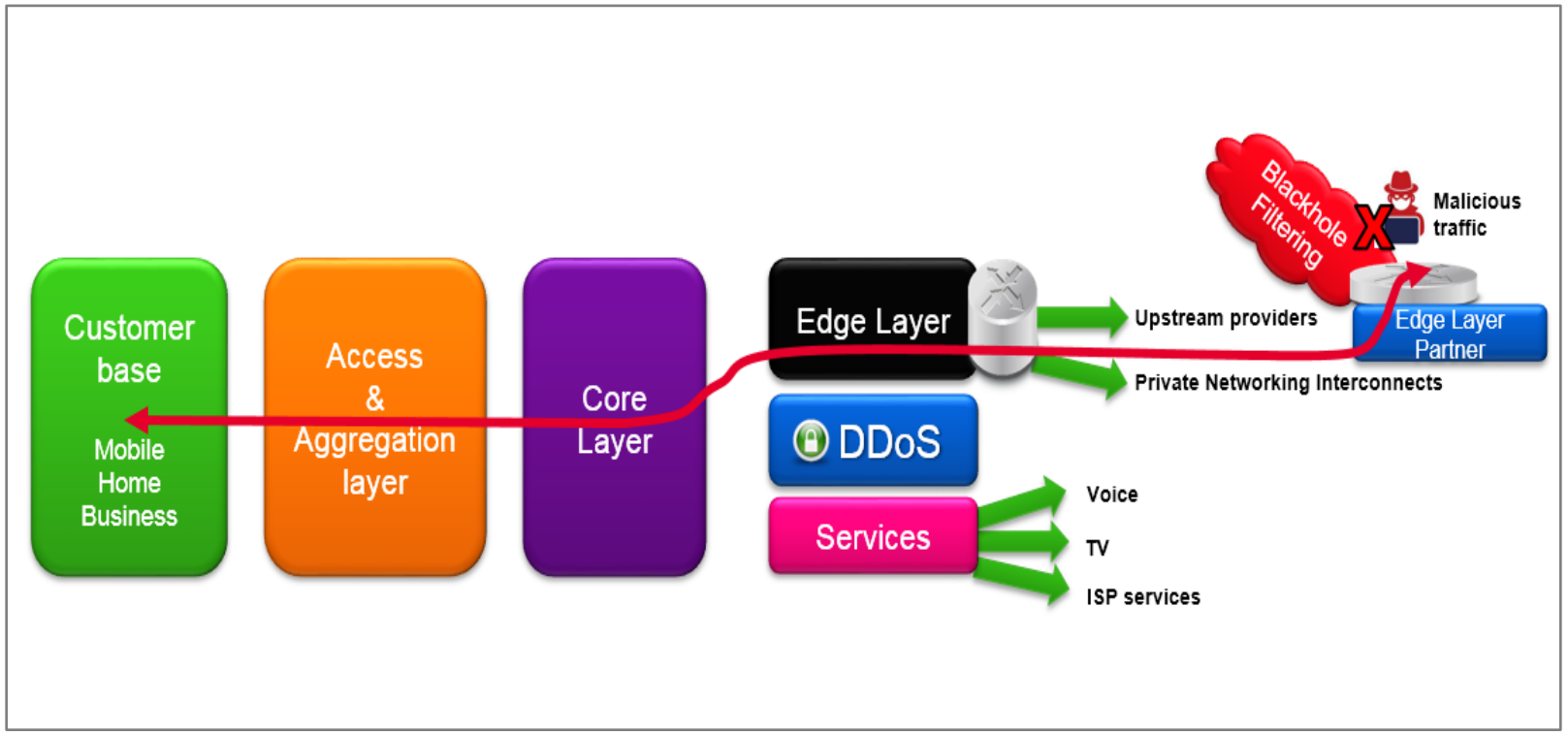
DEFCON 2 FAST PACE



Situation: *Malicious traffic is filtered on provider edge routers through Flowspec. Customer experience on average normal services. Possible some additional latency.*

Graduated levels of Readiness

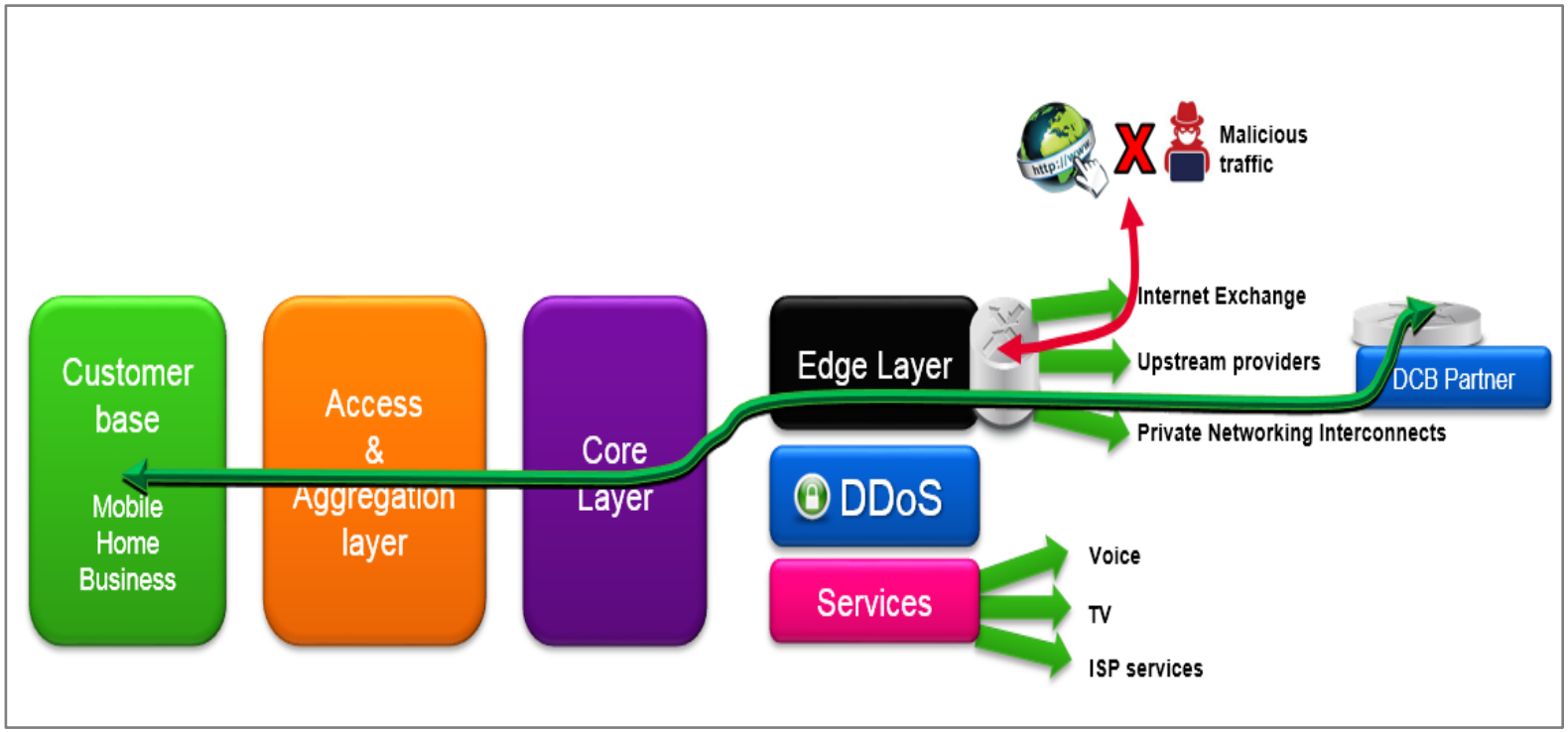
DEFCON 1 COCKED PISTOL



Situation: *Malicious traffic is filtered on upstream(partner) providers edge routers. This solves congestion of links towards upstream/PNI providers. Customer traffic will recover..*

Graduated levels of Readiness

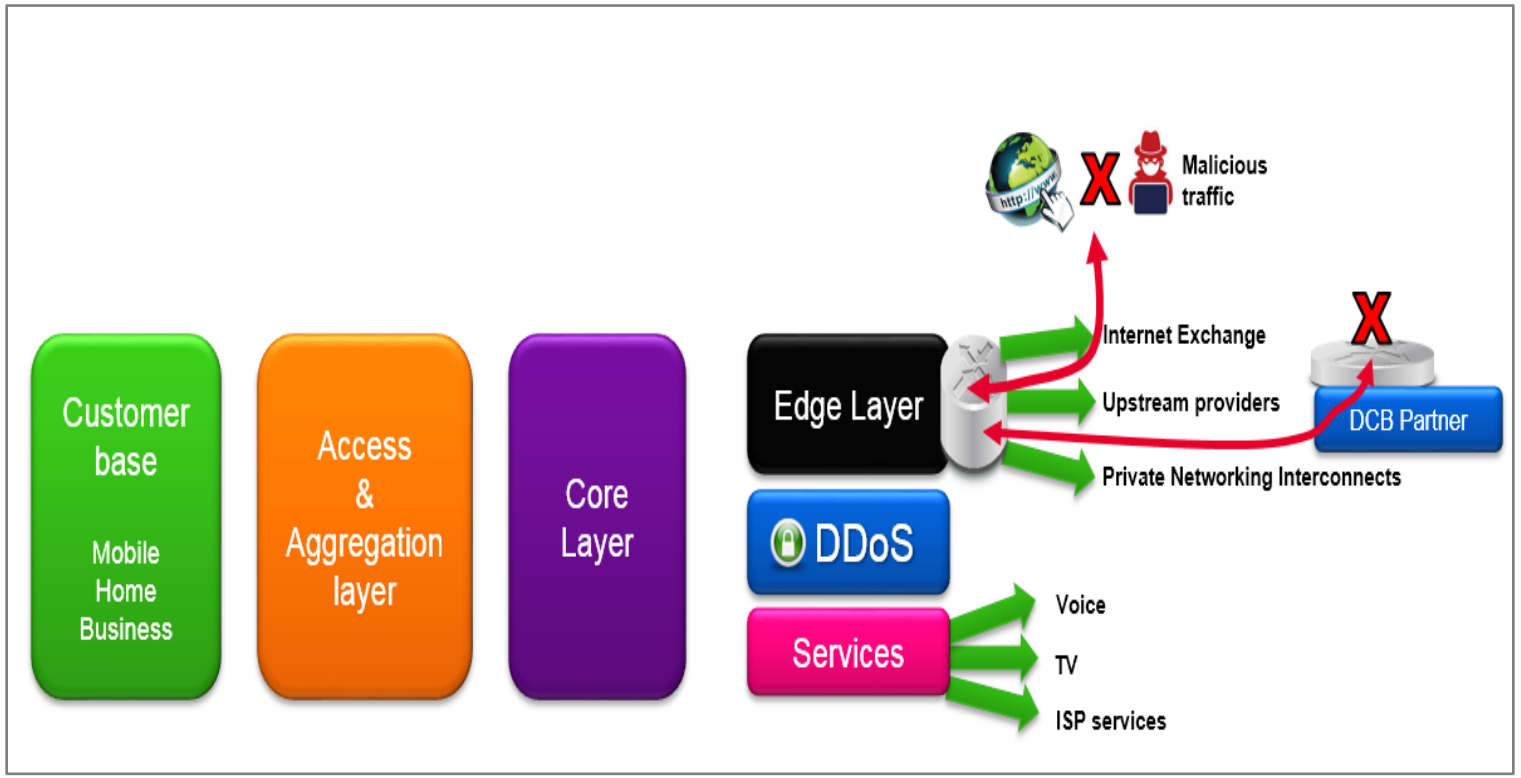
DEFCON .5 DCB Members Only



Situation: *Internet is down. Customers only can reach DCB partner infrastructure*

Graduated levels of Readiness

DEFCON 0 TELCO AUTONOMOUS



Situation: *Internet IS DOWN. Customers only can reach ISP services*

Technical Approach

- Implementing required whitelists / blacklists at single operator.
- Implementing BGP Flow Specification by operators.
- Implementation of BCP38 by all operators would help significantly.
- Customers can acquire anti DDoS scrubbing service.
- Customer can effectively shut himself for DDoS by stopping export of certain routes to the internet.

kpn

Inter-operator cooperation

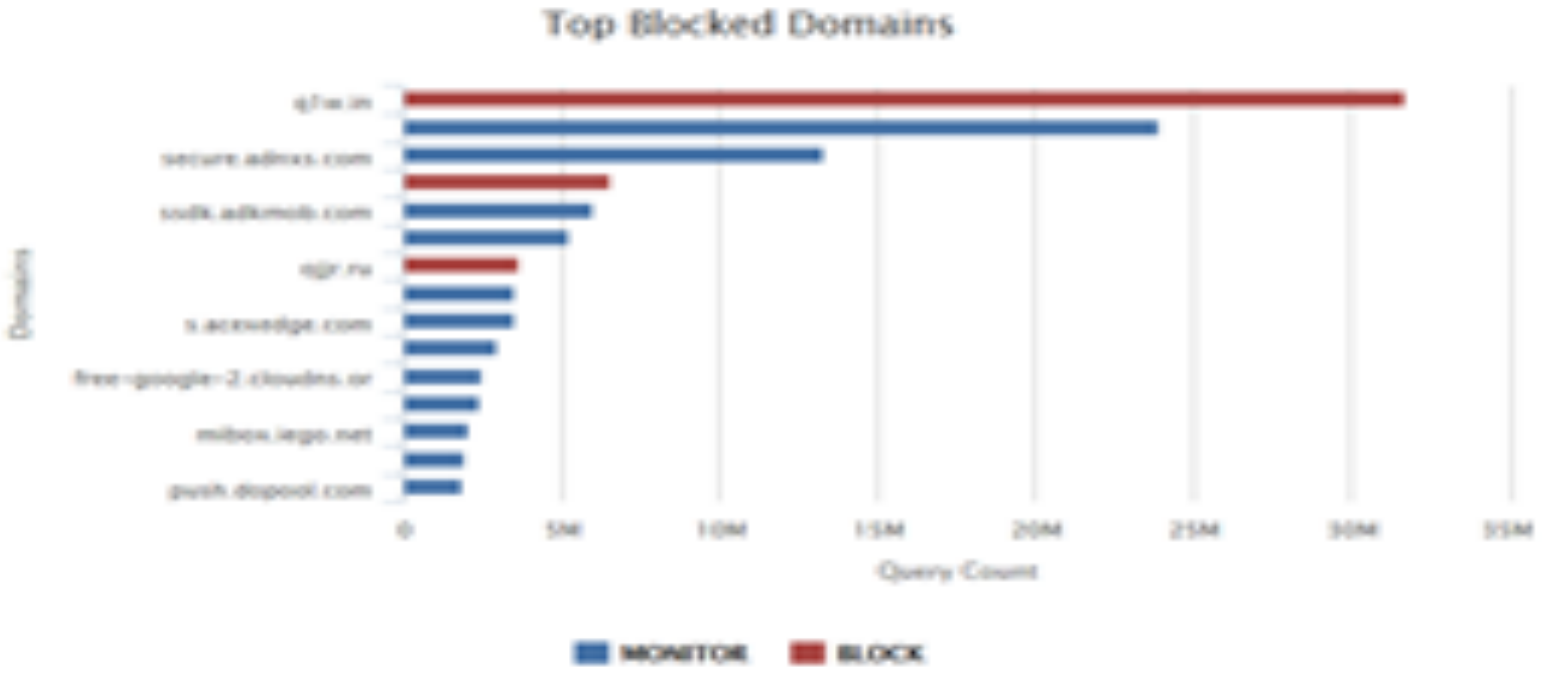
- It is the responsibility of the Telco provider to safeguard its customers from malicious network attacks.
- good due diligence in eliminating the source of the problems results in a good stable end-state.
- A single Telco provider cannot do this on their own, collaboration here between telcos is crucial for success. Each Telco is dependent on network due diligence of the up and downstream partner.
- Prevention and detection best practice is to eliminate problems at the source.

kpn

Inter-operator cooperation Tooling

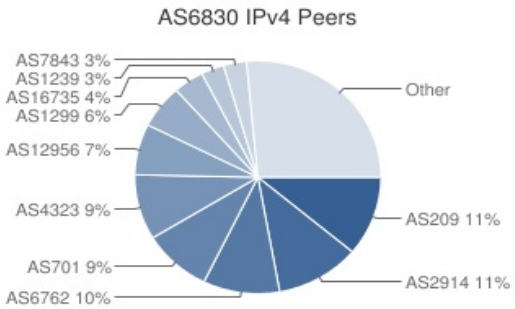
NetFlow to determine the source of the attack

Inter-operator cooperation
Tooling

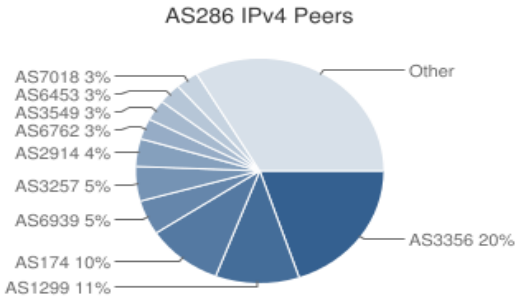


DNS Traffic examination to block the use of malicious domains

Inter-operator cooperation
Routing Diversity as an Asset



ASN	Name
AS209	Qwest Communications Company, LLC
AS2914	NTT America, Inc.
AS6762	TELECOM ITALIA SPARKLE S.p.A.
AS701	Verizon Business/UUnet
AS4323	tw telecom holdings, inc.
AS12956	Telefonica International Wholesale Services, SL
AS1299	TeliaSonera AB
AS16735	ALGAR TELECOM S/A
AS1239	Sprint
AS7843	Time Warner Cable Internet LLC



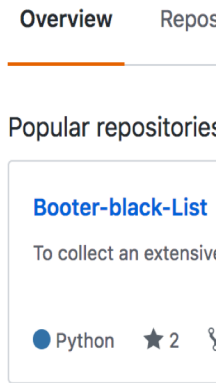
ASN	Name
AS3356	Level 3 Communications, Inc.
AS1299	TeliaSonera AB
AS174	Cogent Communications
AS6939	Hurricane Electric, Inc.
AS3257	Tinet SpA
AS2914	NTT America, Inc.
AS6762	TELECOM ITALIA SPARKLE S.p.A.
AS3549	Level 3 Communications, Inc. (GBLX)
AS6453	TATA COMMUNICATIONS (AMERICA) INC
AS7018	AT&T Services, Inc.

Operator have different upstream providers which broadens their view on the source of the attack

kpn

Issues resolution through Inter-operator cooperation Follow standards and truly work together in ops

- Anti –Spoofing = BCP 38 & 84
  - ingress filtering as a technique to ensure that incoming packets are actually from the networks from which they claim to originate
- Routing Resilience Manifesto (MANRS)
  - Provide a framework for ISPs to better understand and help address issues related to resilience and security of the Internet's global routing system
- Hierarchical Protocols – DNS; NTP ; CAs
- Upstreams embrace RPKI – BGP : DNS SEC for DNS
- NTP & use of Atomic Clocks
- Internet Abuse = Abuse –IX cooperation
- Mobile Abuse and resilance = GSMA WARP
- Fingerprint Booter & Stressors and share knowledge



Q&A

Board Members

kpn

T-Mobile

Ziggo

TELE2

ZEELANDNET

vodafone

amsix

SIDN

UNIVERSITY OF TWENTE.

kpn