(D)DOS DEMYSTIFIED

Tim Wagner – Security Specialist
Wes Stephens - Account Manager

Definitions

- DOS Attack- a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources (e.g., RAM and CPU). The goal is to make the resource unavailable. (Script based usually)
- DDOS Attack- launched from multiple connected devices that are distributed across the Internet. These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved. Unlike single-source DoS attacks, DDoS assaults tend to target the network infrastructure in an attempt to saturate it with huge volumes of traffic. (Botnet based usually)
- Hybrid Protection- The ability to use both on premises and off premises mechanisms to defend against a DOS and/or a DDOS attack

Attack Threats: Pay up or Else!

- April - May of 2015: emails sent to legitimate businesses with the threat of massive DDoS attacks

Hong Kong Banks Hit By Bitcoin Ransom Demands

DD4BC cyber extortion gang targets key European sectors

- DD4BC claims ~400 Gbps
- Extortion demands of 1- 40 Bitcoin
- Initially targeted Bitcoin, Payment providers, banks and now moving to other targets
- UDP Amplification Attacks (NTP, SSDP, DNS); TCP SYN Floods; and Layer 7 attacks

Sample from actual email

> Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother. At least, don't expect cheap services like CloudFlare or Incapsula to help...but you can try. :)

Attack Type Trends

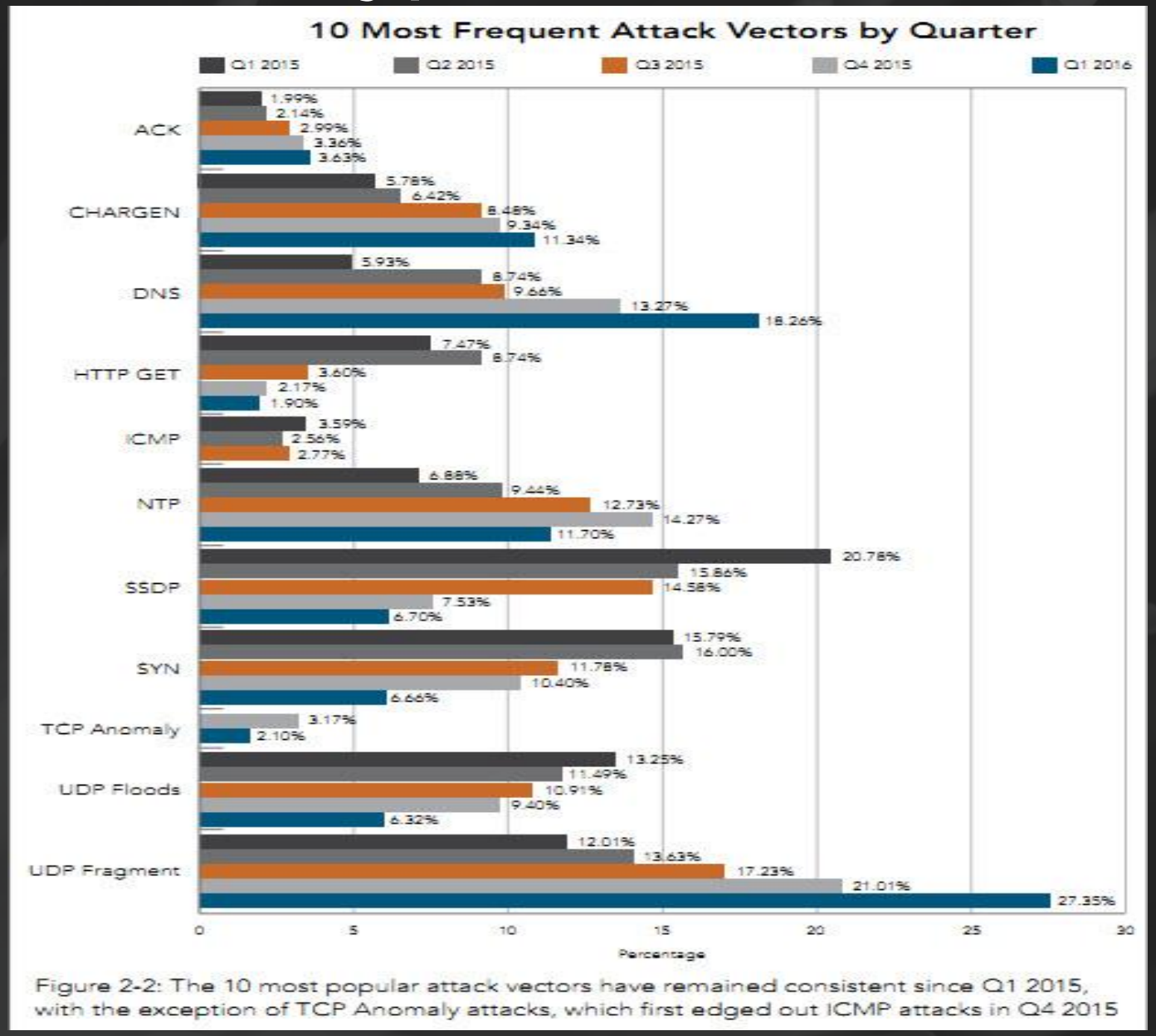


Figure 2-2: The 10 most popular attack vectors have remained consistent since Q1 2015, with the exception of TCP Anomaly attacks, which first edged out ICMP attacks in Q4 2015

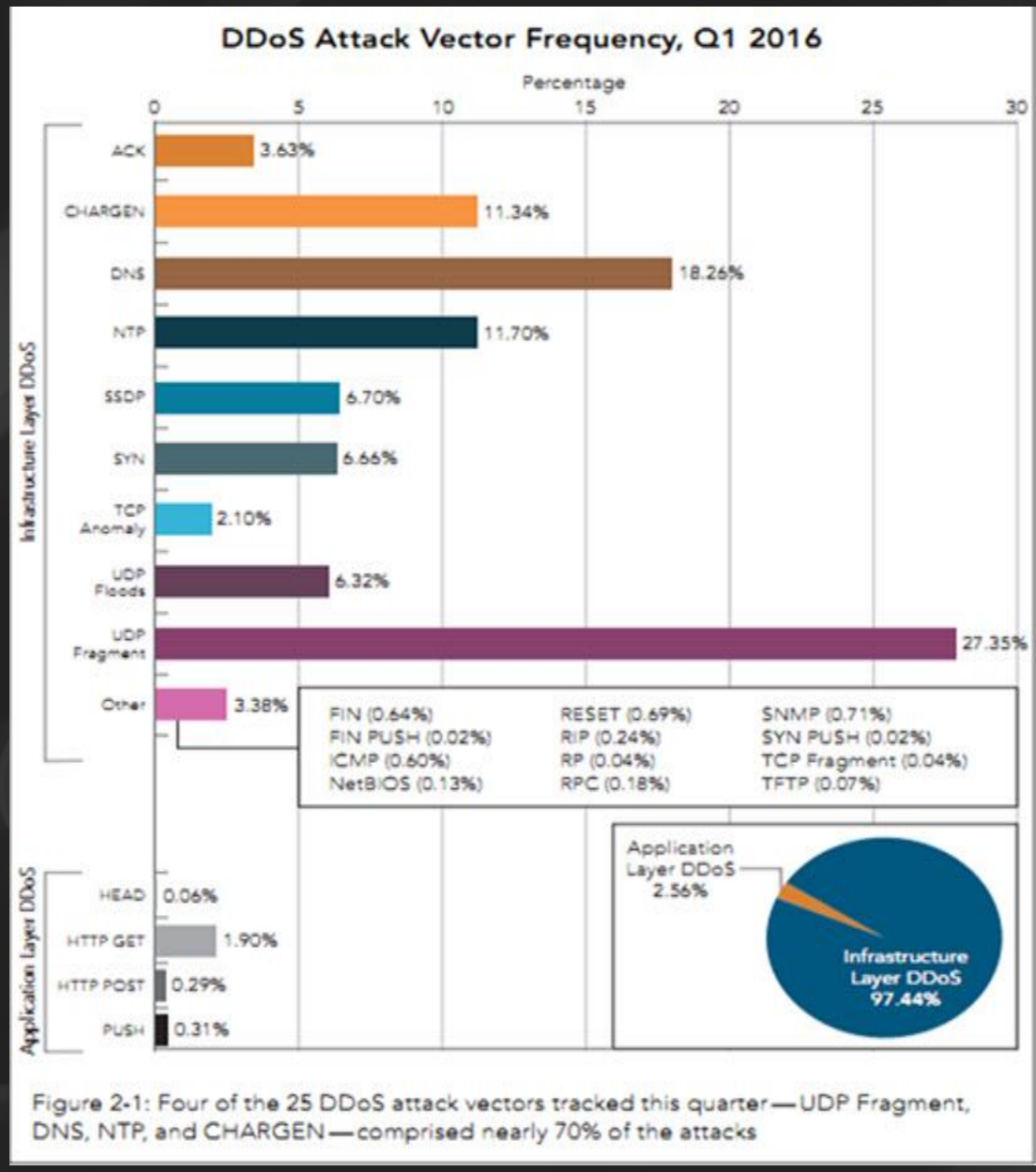


Figure 2-1: Four of the 25 DDoS attack vectors tracked this quarter—UDP Fragment, DNS, NTP, and CHARGEN—comprised nearly 70% of the attacks

The Hybrid Threat

Carphone Warehouse Breach with a DDOS Smoke Screen- http://www.theregister.co.uk/2015/08/11/carphone_warehouse_ddos_before_giant_data_breach/

CyberCriminals Use DDOS to hide attacks: http://www.crn.com/news/security/300071742/cybercriminals-using-ddos-as-smokescreen-experts-warn.htm

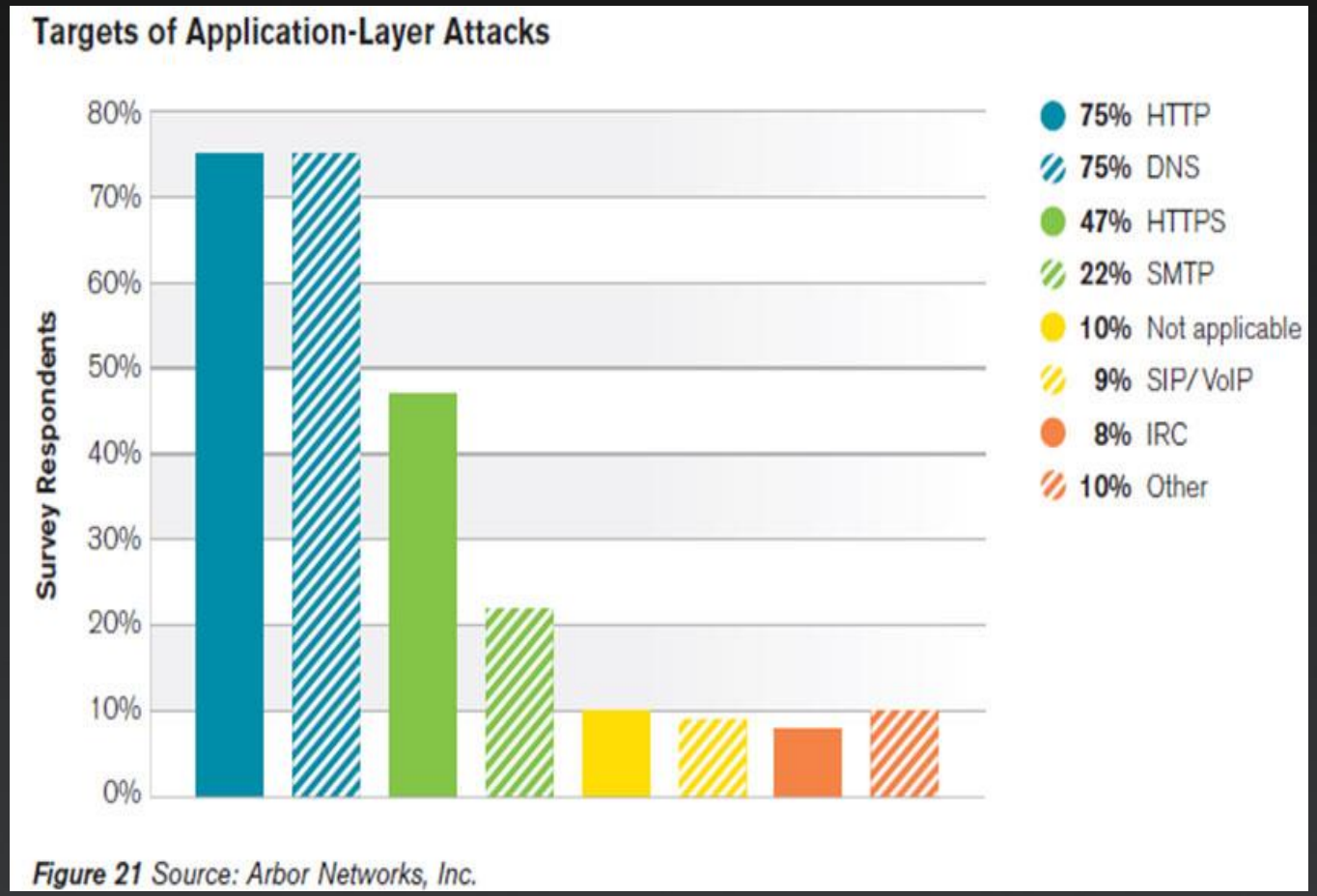
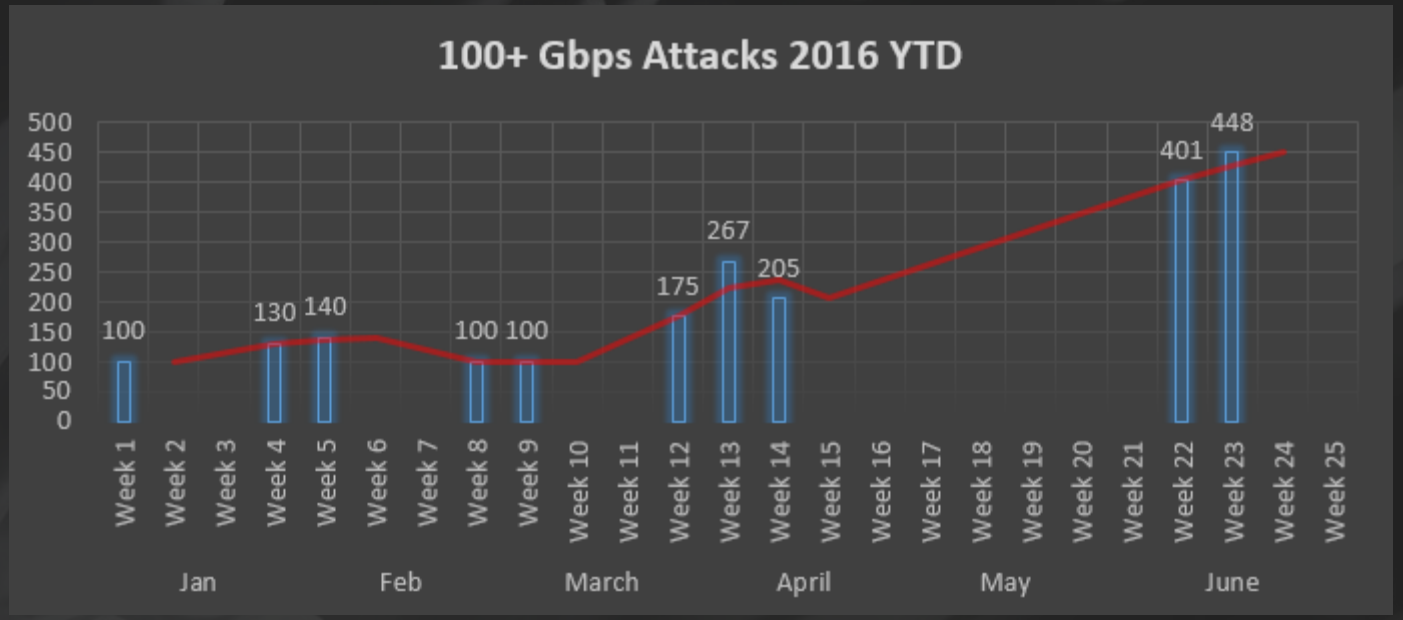
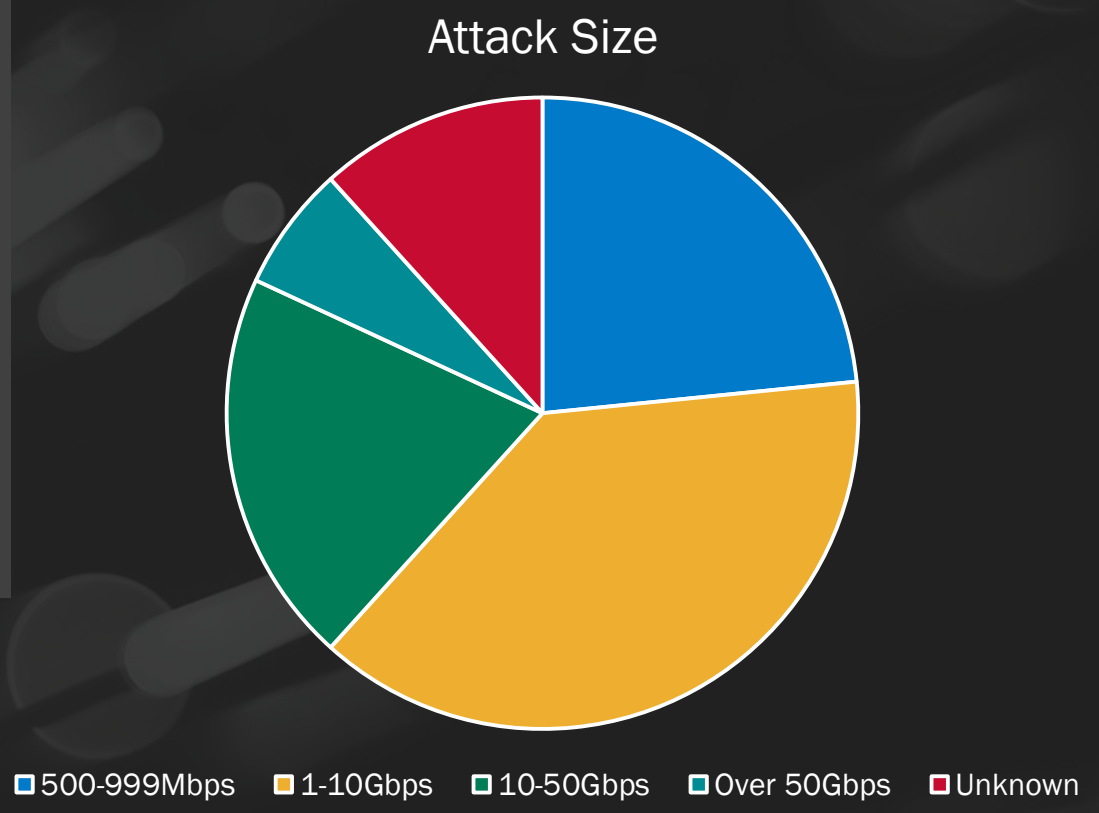


Figure 21 Source: Arbor Networks, Inc.

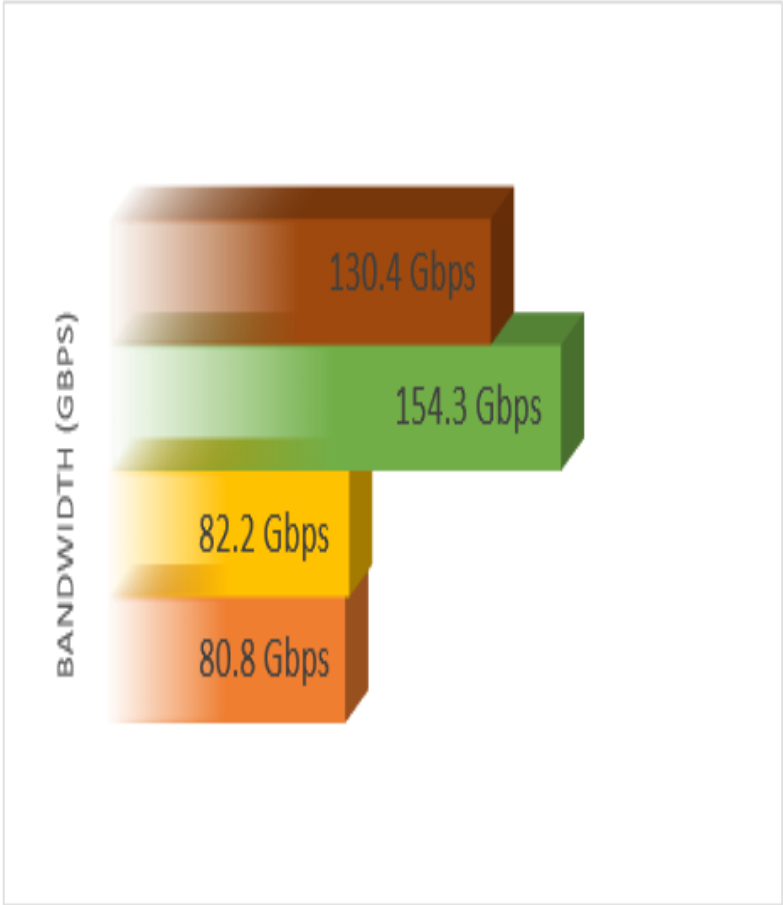
Attack Size Realities

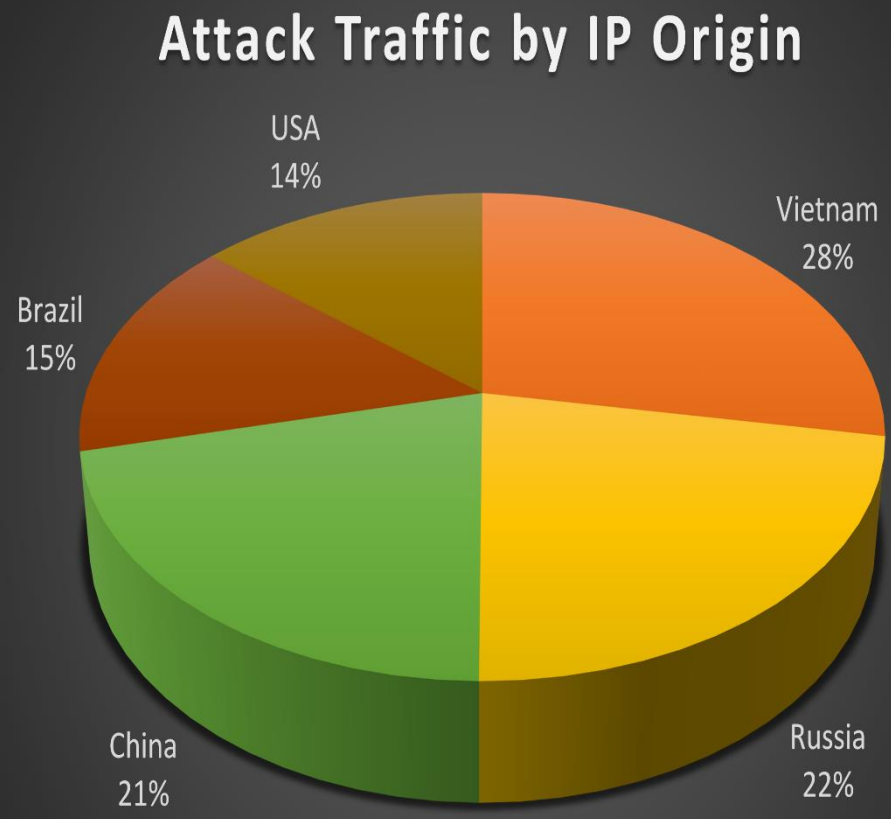




448 Gbps Attack Breakdown

	Bandwidth (Gbps)
Data Center 1	130.4
Data Center 2	154.3
Data Center 3	82.2
Data Center 4	80.8
TOTAL	447.7





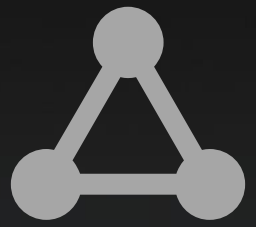
Denial of Service Solution Options

Current Volumetric DDoS Solution Market

Carriers Based

Generally they leverage thresholds and only work on the link that you purchase from the carrier

Example: Verizon/ATT



CDN Based

CDN technology is about absorbing and masking the effects of a DDOS attack, not removing it

Example: Akamai/Cloudflare

Enterprise Cloud Service

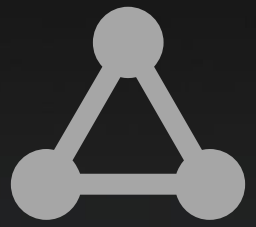
Generally based on 4-7 Scrubbing facilities, geo graphically dispersed, removes bad traffic and is priced on clean bandwidth

Example: F5 Silverline/Prolexic

Current Hybrid Options

Carriers Based

Generally they do not offer any on premises option to customers.



CDN Based

Generally no on premises option is offered to customers

Enterprise Cloud Service

Certain solutions in this group do offer hybrid offerings. While not common, 3 vendors in this space offer something, implementation is the differentiator

Important Decision Criteria

Scale per Customer:

Hybrid Option

Solution Side Effects

Limited Toolsets/Only DOS

False Positives

Visibility into Attacks

24/7 SUPPORT

Ask your vendors where they have SOC locations, what layers of engineering support? Separate provisioning? Response time matters, make sure you understand this level of support. Is there more then one location?

GLOBAL COVERAGE

Where do you scrub traffic?

Explain how AnyCast works, if that is used

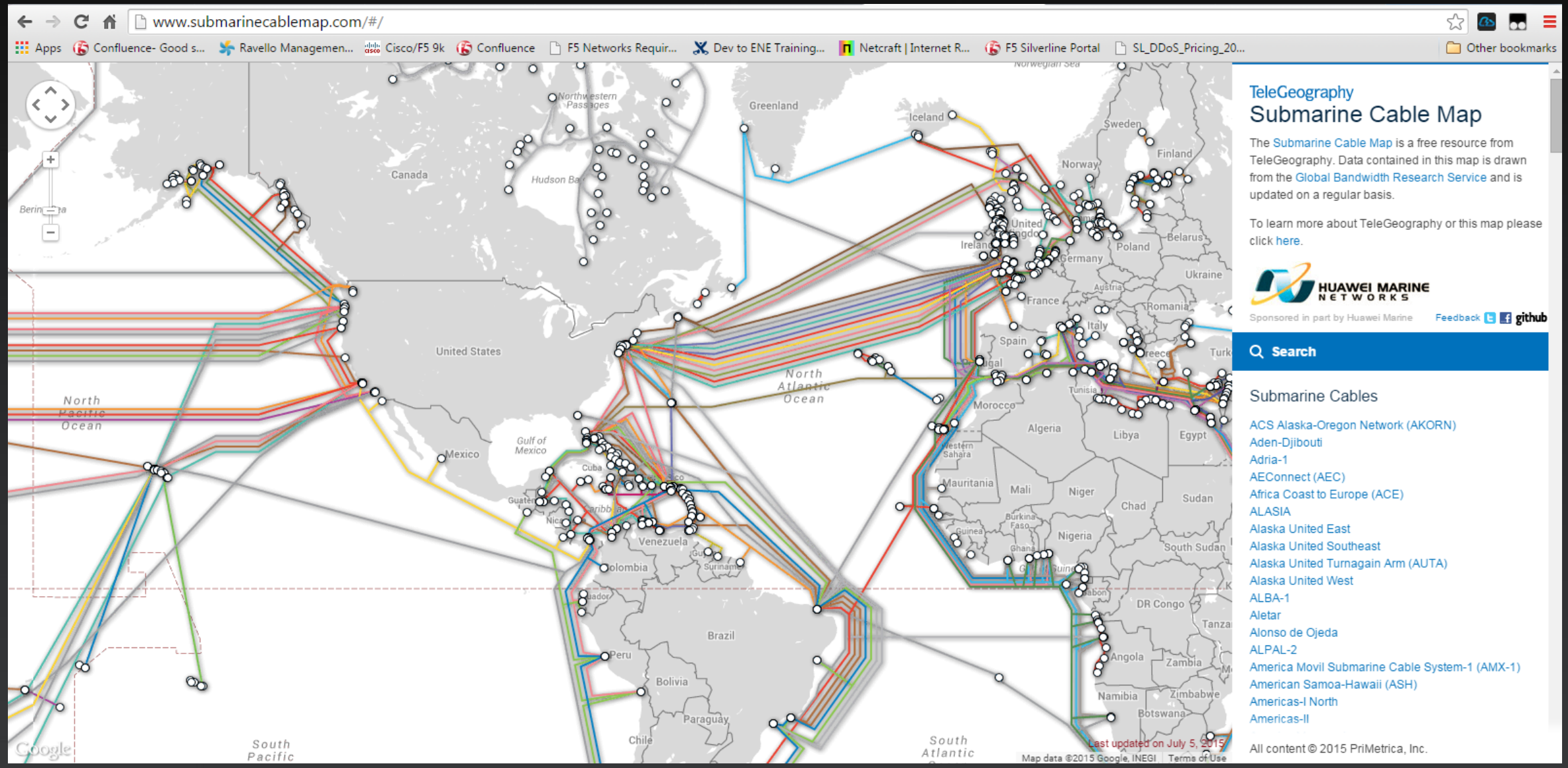
How is backend or private connectivity configured between centers

Replication time?

INDUSTRY-LEADING CAPACITY

- Scrubbing Capacity- Physical gear to clean traffic, this is the key!
- Bandwidth- Today and how does it change when you sign up customers

Physical Internet Cabling

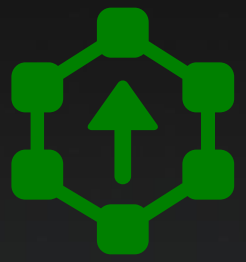


Volumetric DDoS Protection - Service Options

Always on

Primary protection as the first line of defense

The Always On service stops bad traffic from ever reaching your network by continuously processing all traffic through the cloud-scrubbing service and returning only legitimate traffic through your website.

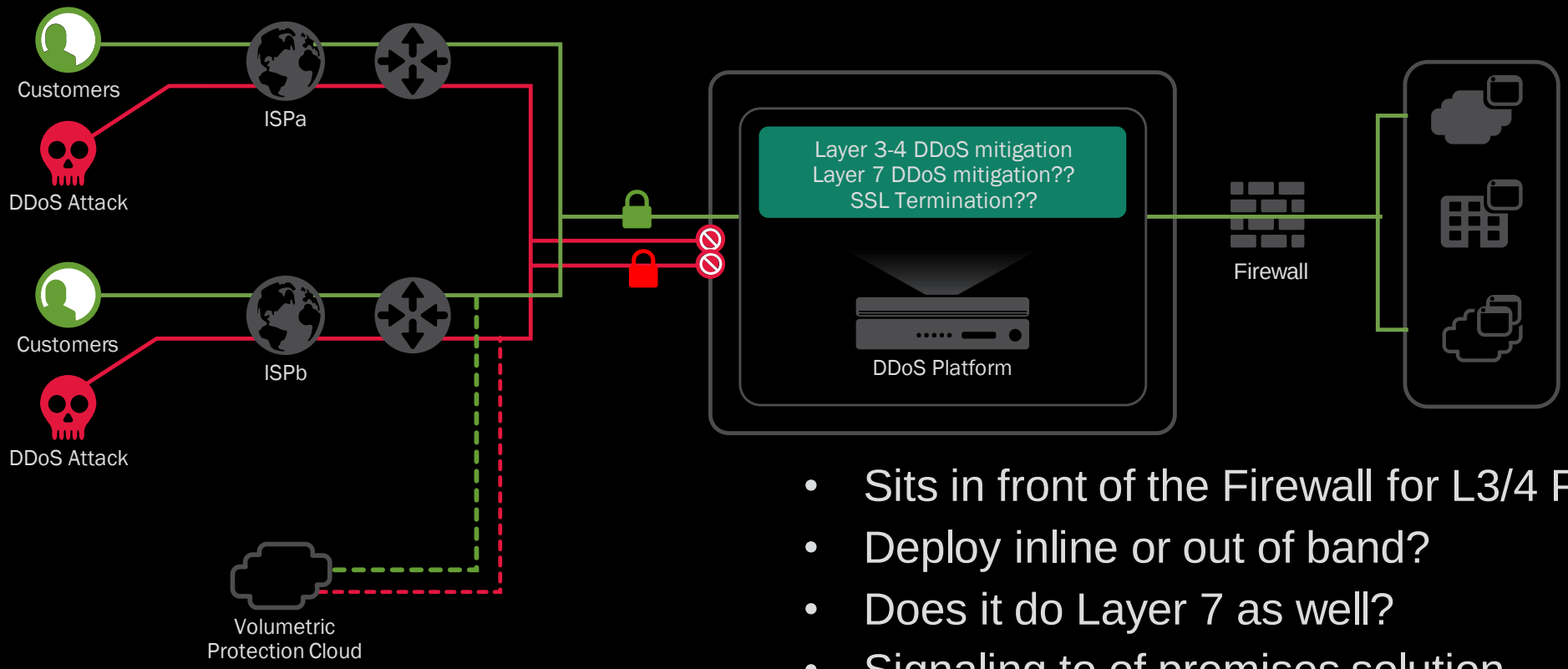


Always available

Primary protection available on-demand

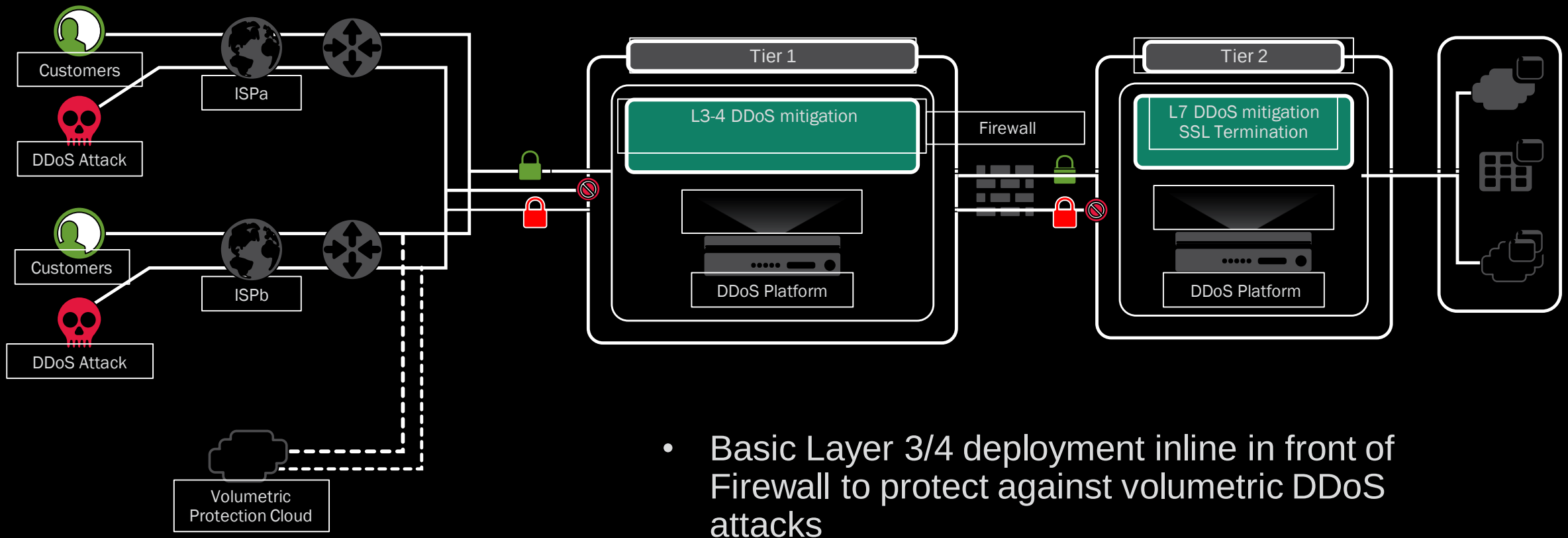
The Always Available service runs on stand-by and can be initiated when under a DDoS attack.

Single Tier DDoS mitigation for all attacks



- Sits in front of the Firewall for L3/4 Protection
- Deploy inline or out of band?
- Does it do Layer 7 as well?
- Signaling to of premises solution

Two tier DDoS Protections



- Basic Layer 3/4 deployment inline in front of Firewall to protect against volumetric DDoS attacks
- Layer 7 DDoS mitigation on the inside tier. Requires SSL termination on the DDoS appliance

Two Ways to Direct Traffic to Silverline Scrubbing Centers

BGP (BORDER GATEWAY PROTOCOL)
ROUTED MODE

DNS
PROXY MODE

Multiple Ways to Return Clean Traffic

GRE TUNNELS

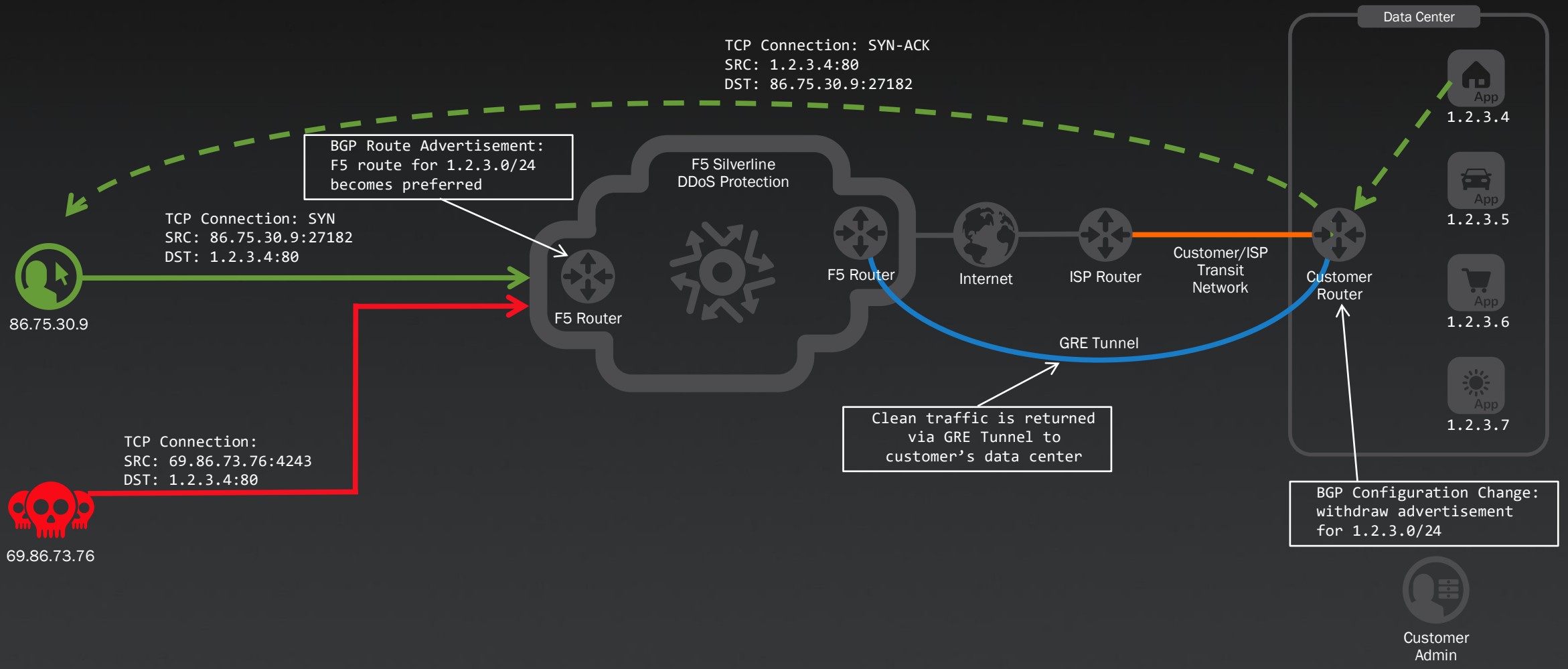
L2VPN / VIRTUAL ETHERNET SERVICE

IP REFLECTION ™

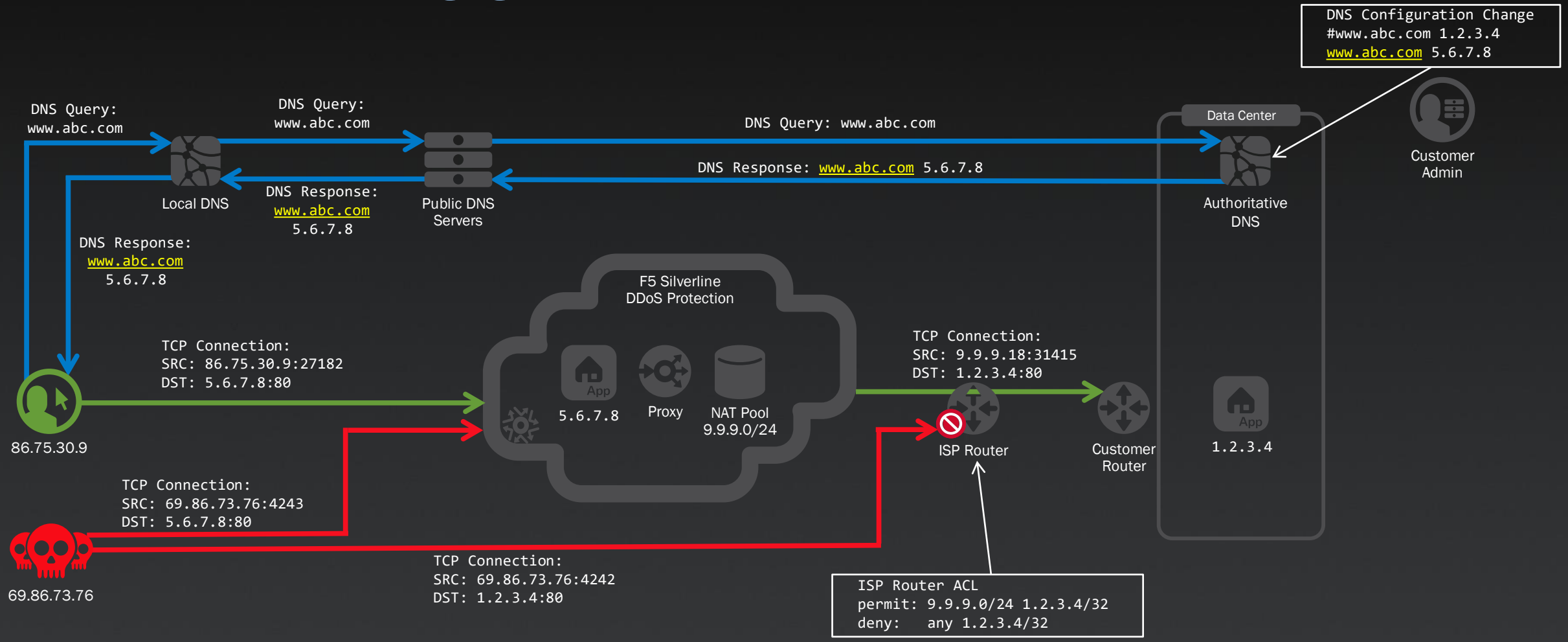
EQUINIX CLOUD EXCHANGE

PROXY

Routed Configuration
DDoS Protection Engaged

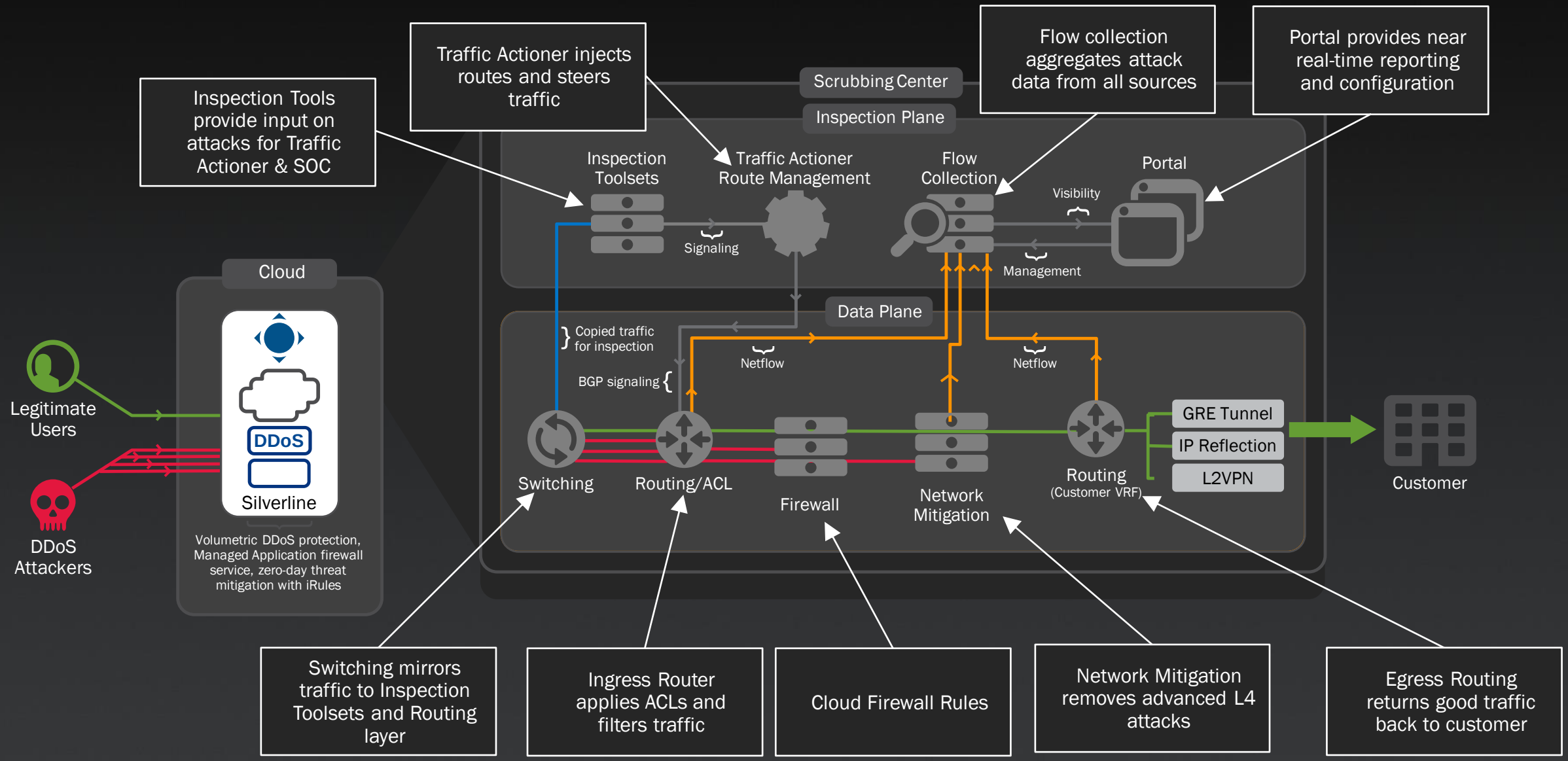


Proxy Configuration
DDoS Protection Engaged

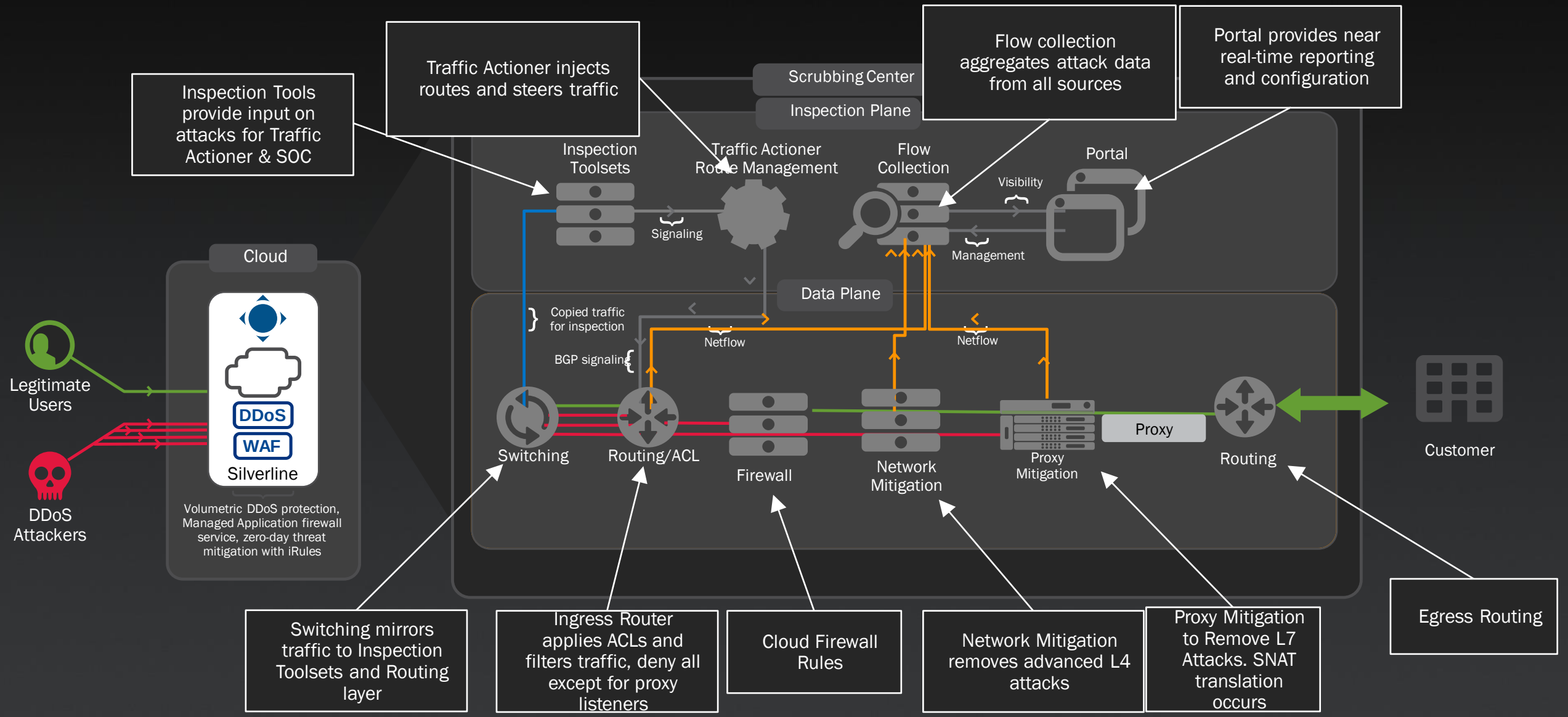


What does traffic flow look like in a Scrubbing Center?

F5 Scrubbing Center Architecture- Routed Traffic



F5 Scrubbing Center Architecture- Routed + Proxy



Key Considerations

- DDOS is about economics, both for the attacker and the victim
- DOS or DDOS is not a hack, but rather an attack
- Is DDOS/DOS protection a market or a feature of broader solutions?
- DDOS protection needs to become “baked in” to bandwidth considerations
- SSL DDOS is not common today, but it is growing
- Protection levels depend on Risk assessment
- Is it as a Service or Managed Service, it does matter
- https://f5.com/Portals/1/Cache/Pdfs/2421/the-f5-ddos-protection-reference-architecture.pdf

Solutions for an application world.