PCCW Global | consoleconnect

KHNOG 7 - 30 Nov 2025

Cybersecurity
Anti-DDoS Service and Network Security

Gordon Lee
Assistant Vice President, Security Product

Product Manager

Gordon Lee

Responsibility Product Ownership of all security products (e..g. Anti-DDoS Service, Web Application Firewall, SASE, etc) in PCCWG Global

Experience more than 20 years in cyber security industry.

Cambodia related Introduced PCCW Global's Anti-DDoS Service to Cambodia customers. The Anti-DDoS Service protects over several hundred network from DDoS attack

Our Agenda

DDoS attack trend

Design of DDoS Infrastructure

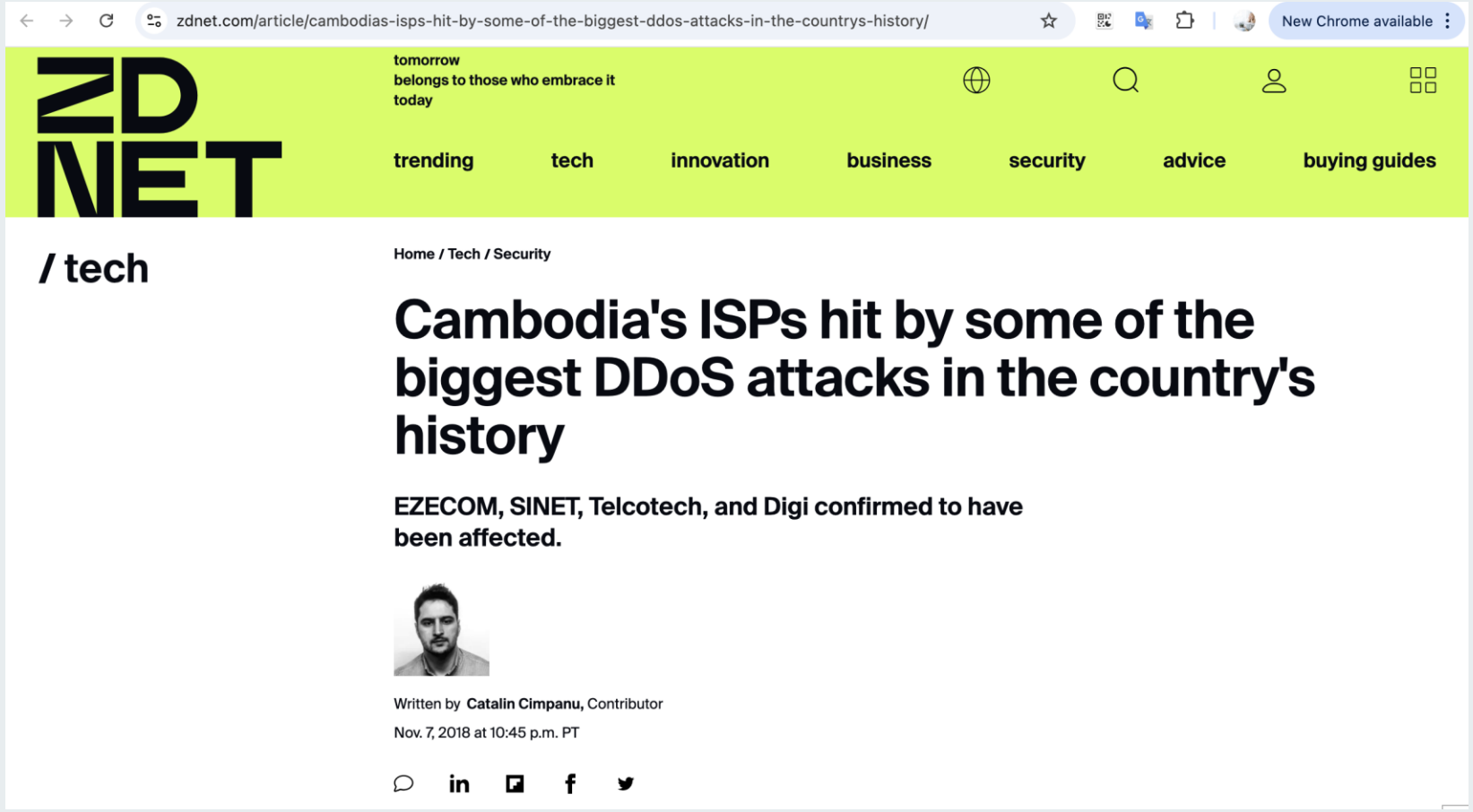
Background

Past Event : Cambodia under DDoS attack in 2018

Time : 2018
Size : 150G

"DDoS attacks totaling nearly 150Gbps have hit Cambodian ISPs on Monday."

URL :
https://www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history/



Background of Anti-DDoS Service

- Long before, more than 15 years ago, we provides Anti-DDoS Service
- Technology includes Arbor, Alibaba, Radware, NS Focus, etc
- We have built multiple SCs already globally so far

Today, we focus on DDoS traffic to ISP network

PCCW Global | consoleconnect

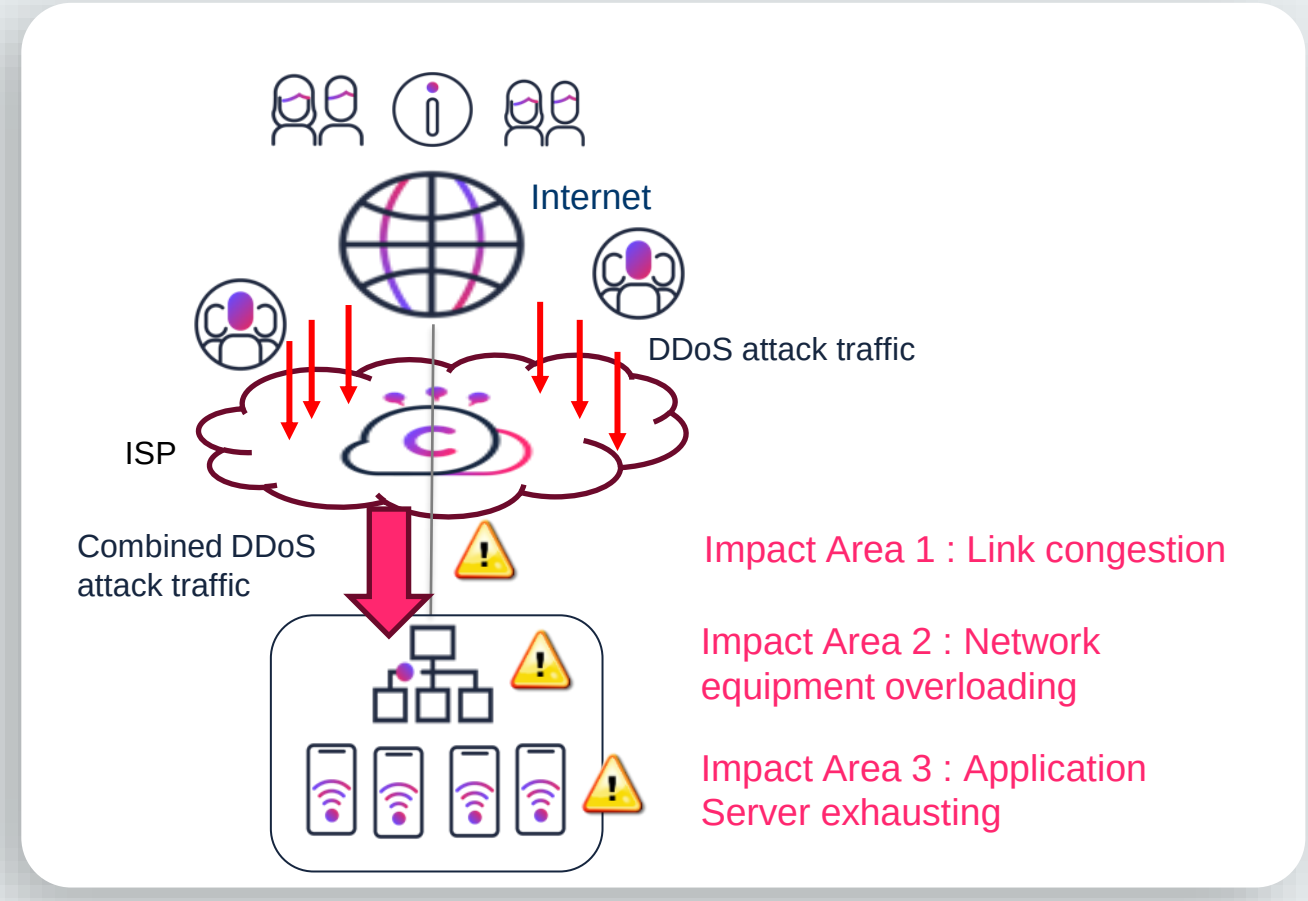
Basic 101

What is DDoS ?

What is DDoS attacks?

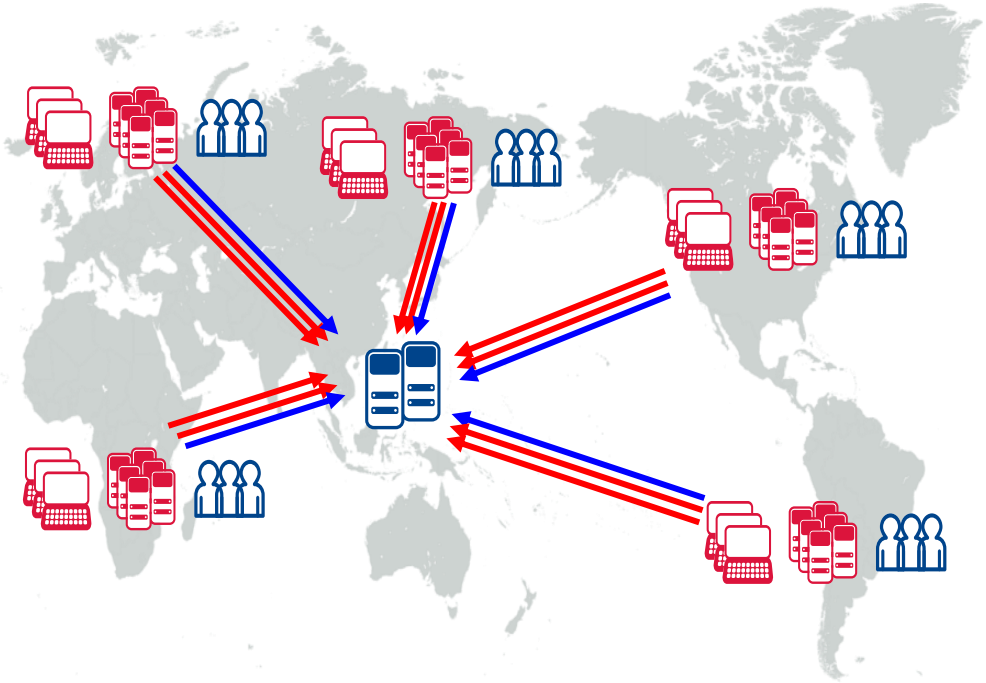
Distributed Denial of Service (DDoS) attack

- Goal
  - To take down a website, application or infrastructure, making it unavailable to legitimate users.
  - Typical victims such as, web sites, e-commerce systems, online gaming, email servers, VoIP systems etc.
- By
  - Overwhelming the victim with a flood of Internet traffic generated by compromised computer systems/devices (aka Zombie Computers or Botnet)
- On-premise standalone cannot defend DDoS completely

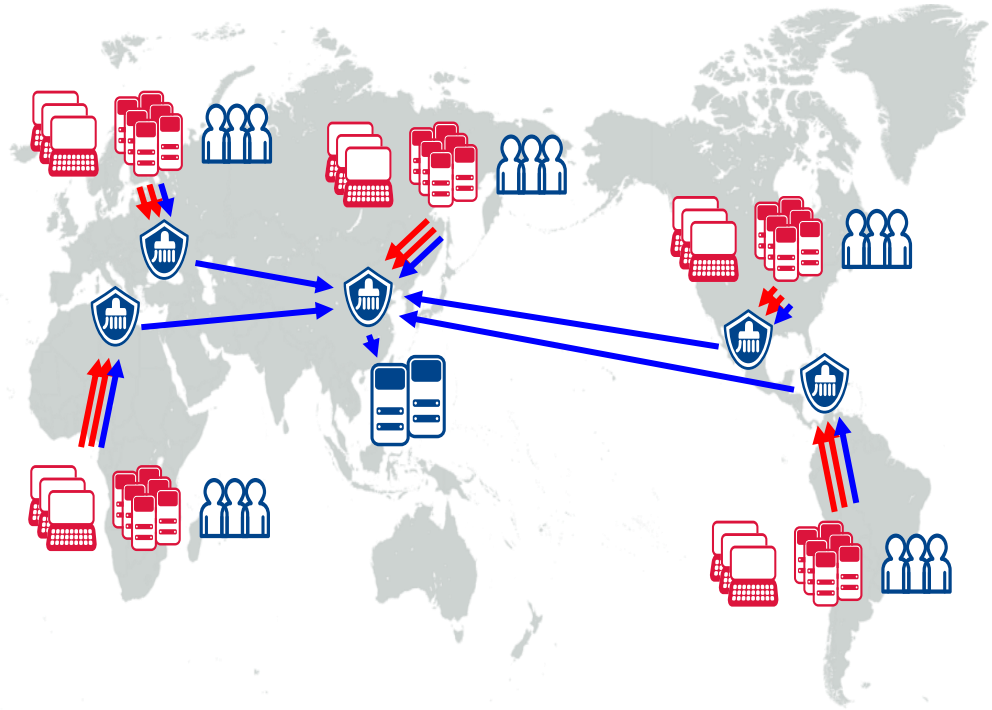


DDoS attacks originated globally and mitigated near the source

Globally-originated attack



Cloud Mitigation near the attack source



Globally Distributed Scrubbing Centers (Example)

So,

DDoS attack comes from multiple distributed source to saturate the victim’s Internet, overload server or routers.

DDoS Trend

Attack Size jumped up substantially

DDoS attack volume is increasing recently

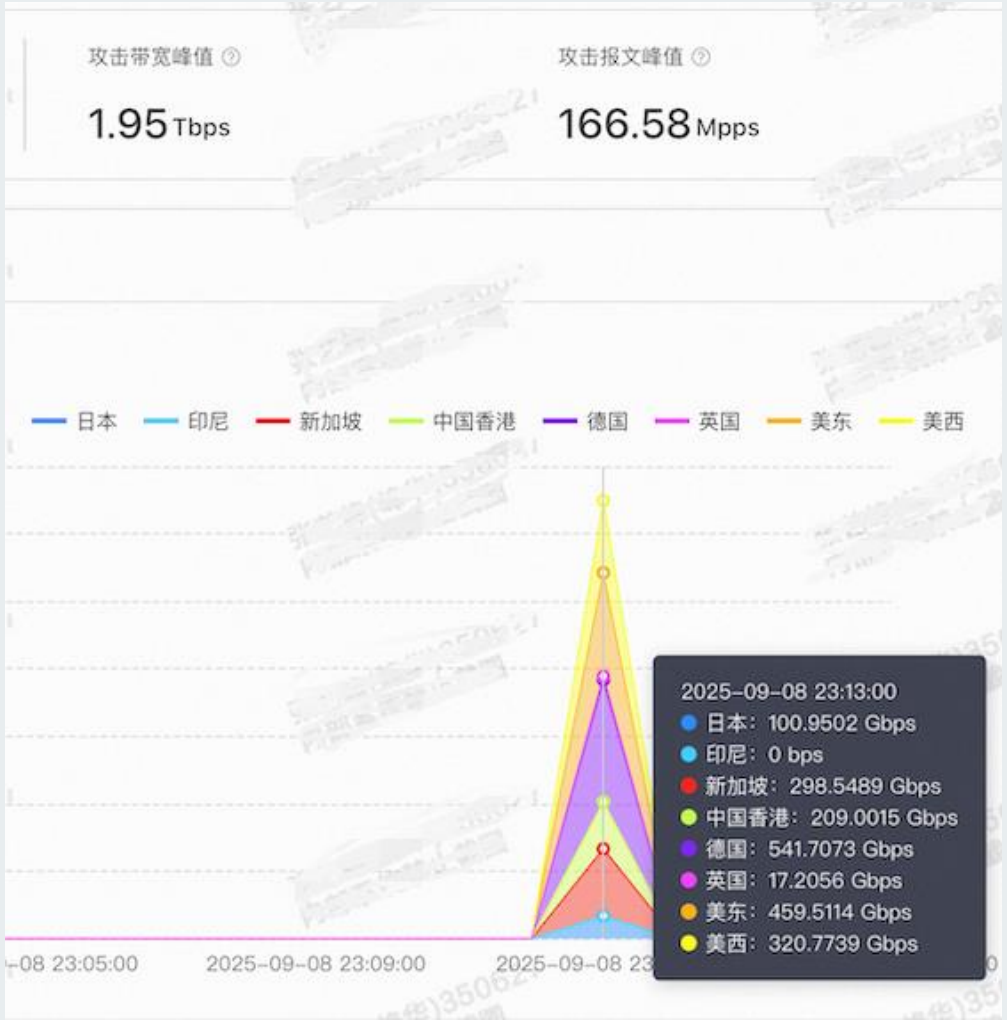
- Market News
  * *“DDoS Botnet Aisuru Blankets US ISPs in Record DDoS” – 10 Oct,2025*
    Due to new IoT device vulnerability - DDoS Botnet Aisuru Blankets
  * https://krebsonsecurity.com/2025/10/ddos-botnet-aisuru-blankets-us-isps-in-record-ddos/
* Message 1 : IoT amplify DDoS attack size
  * **6.35 T bps** reported in May2025
  * **11.5 T bps** reported in Sept,2025
  * **29.6 T bps** reported in Oct,2025
  * Prevalent IoT equipment in the Internet, e.g. Surveillance cameras
  * High bandwidth connection per household-equipment
- Message 2 : DDoS jeopardize ISP Network
  * US ISP suffered network congestion
- Message 3 : Bot-originated DDoS traffic is hard to defend

Example of DDoS mitigation

- DDoS attack - 2T bps in Sept,2025

Traffic distribution of the recent 2T bps attack

- Japan : 100 G bps
- Singapore : 298 G bps
- Hong Kong : 209 G bps
- Germany : 542 G bps
- London : 17 G bps
- US Ashburn : 460 G bps
- US San Jose : 321 G bps



The Trend

It is highly likely that higher and higher volume / size of DDoS attack happens in future.

PCCW Global | consoleconnect

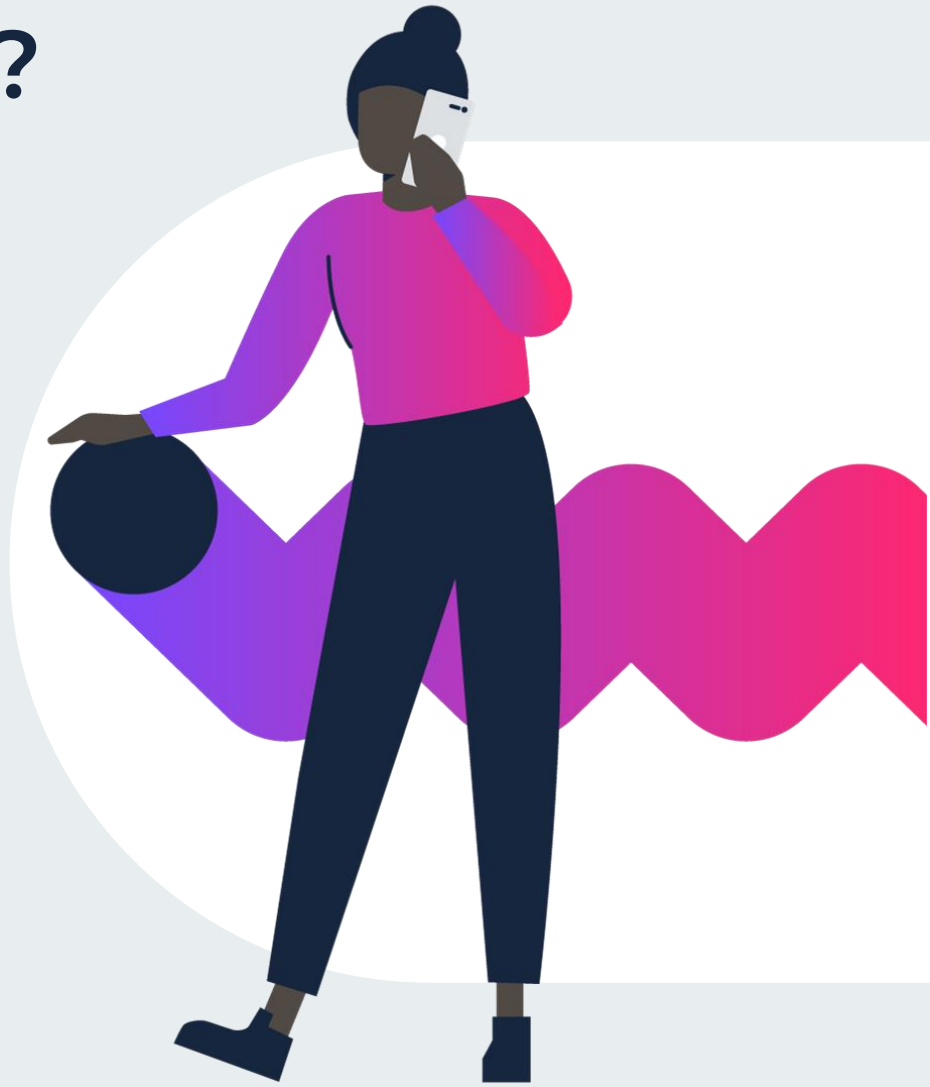
Network Design

Design of Anti-DDoS Infrastructure

Key Consideration

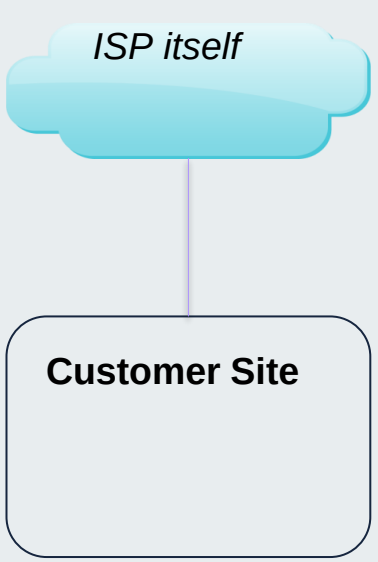
How to Maintain Network Stability during DDoS attack?

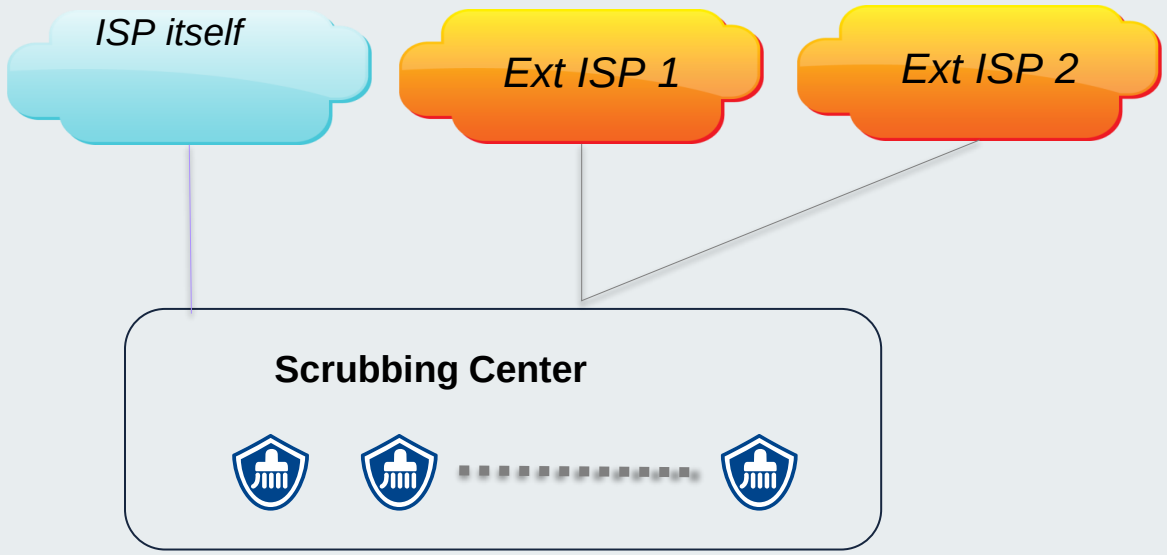
- Concern
  - "We (Network Engineer) cannot offer DDoS business since it will easily congest some links"
  - Anti-DDoS nature is poison to ISP network
    - Link / Backbone congestion risk
    - Direct impact to non-victim customers
- Design for Anti-DDoS Service Network
  - Include more upstream links
  - Dedicated routers for Anti-DDoS business (easy to fine-tune route policy and fine-tuning)
  - Dedicated AS Number



Anti-DDoS Transit: Avoid Congestion

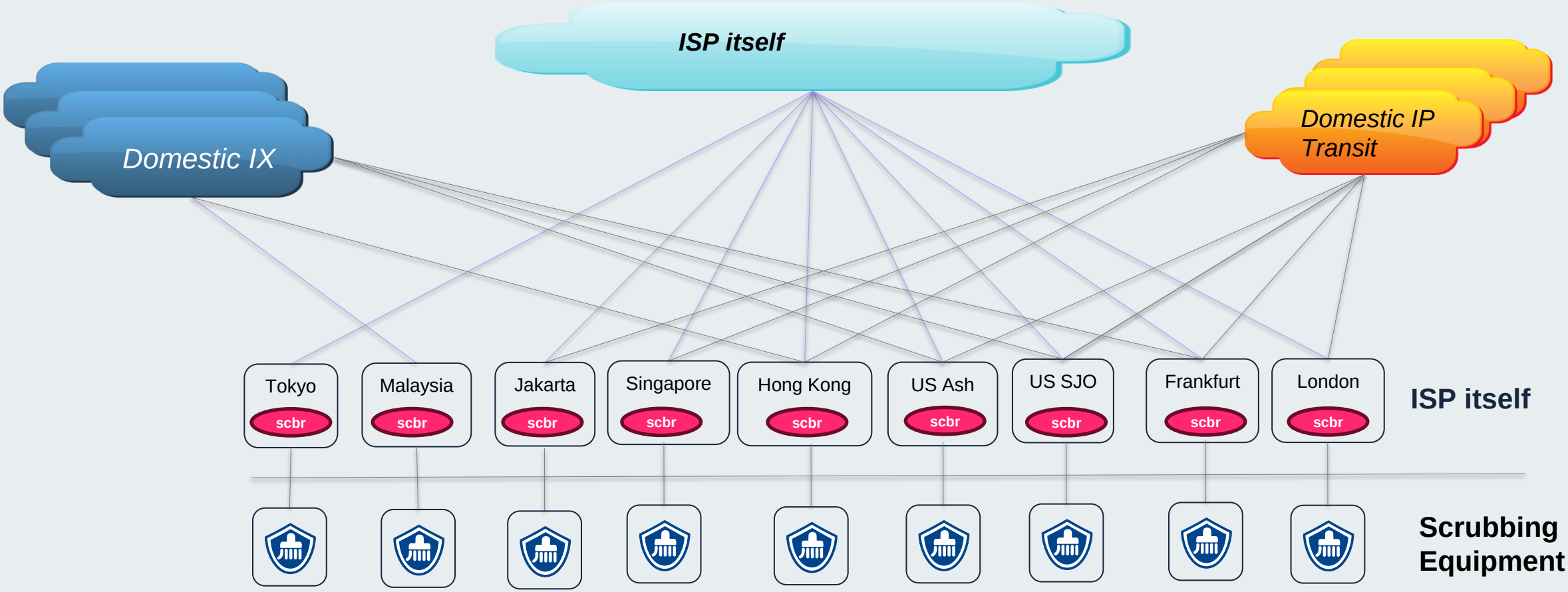
- Normal Transit vs Anti-DDoS Transit
- ISP itself can be the bottleneck for receiving DDoS attacks





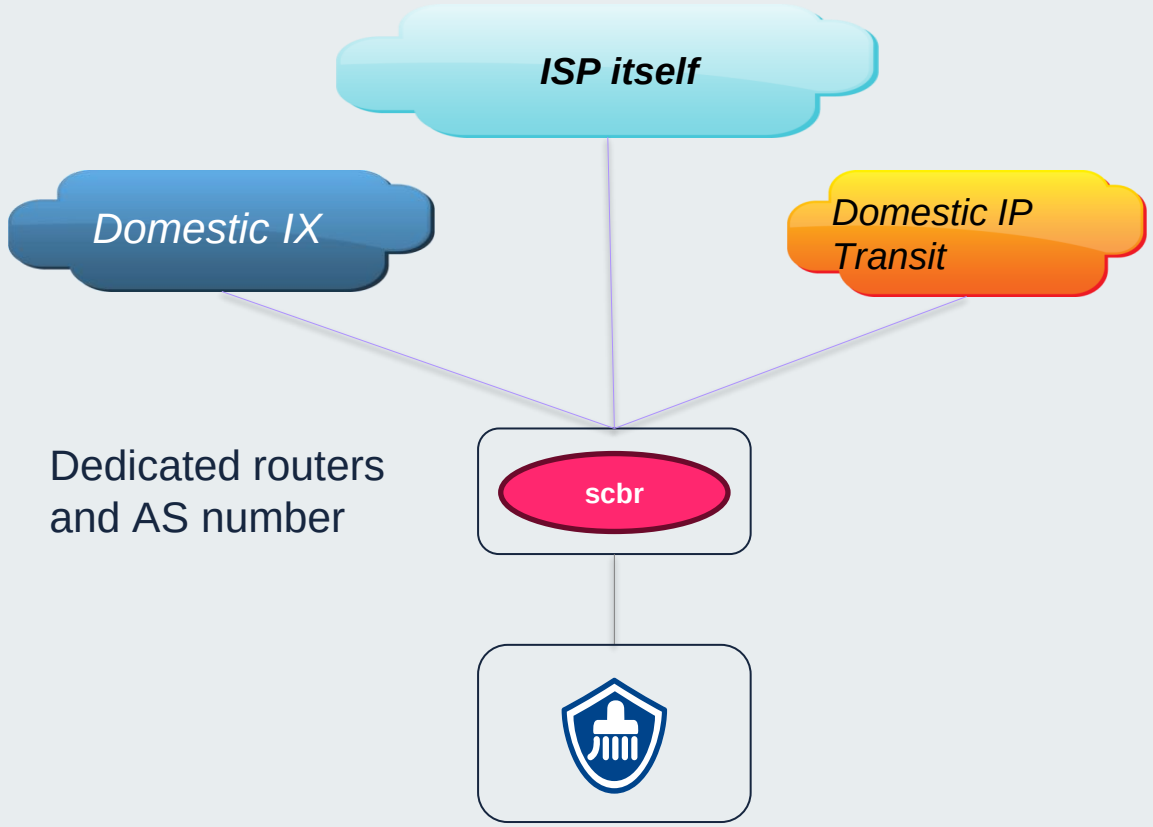
Multi-upstream Design

- multiple Anti-DDoS PoPs



Dedicated Routers and AS number for Anti-DDoS Scrubbing Center

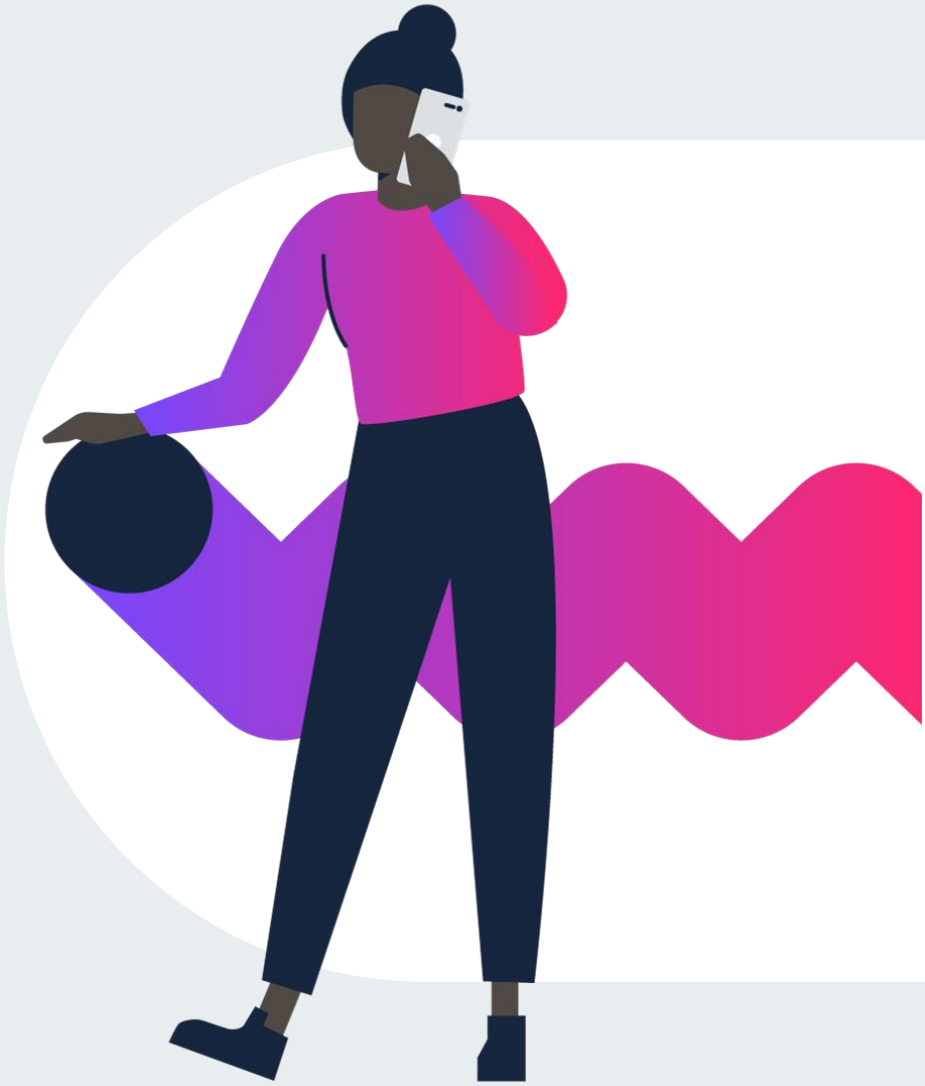
- Dedicated routers
  - for Scrubbing Center's equipment
  - No other customers will be connected to this routers
- Dedicated AS number
- Result : Anti-DDoS network is 'isolated' from normal Transit Network



Our approach - Recap

To isolate DDoS traffic from main connectivity network via

1. More upstream links
2. Dedicated router
3. Dedicated AS number



PCCW Global | consoleconnect

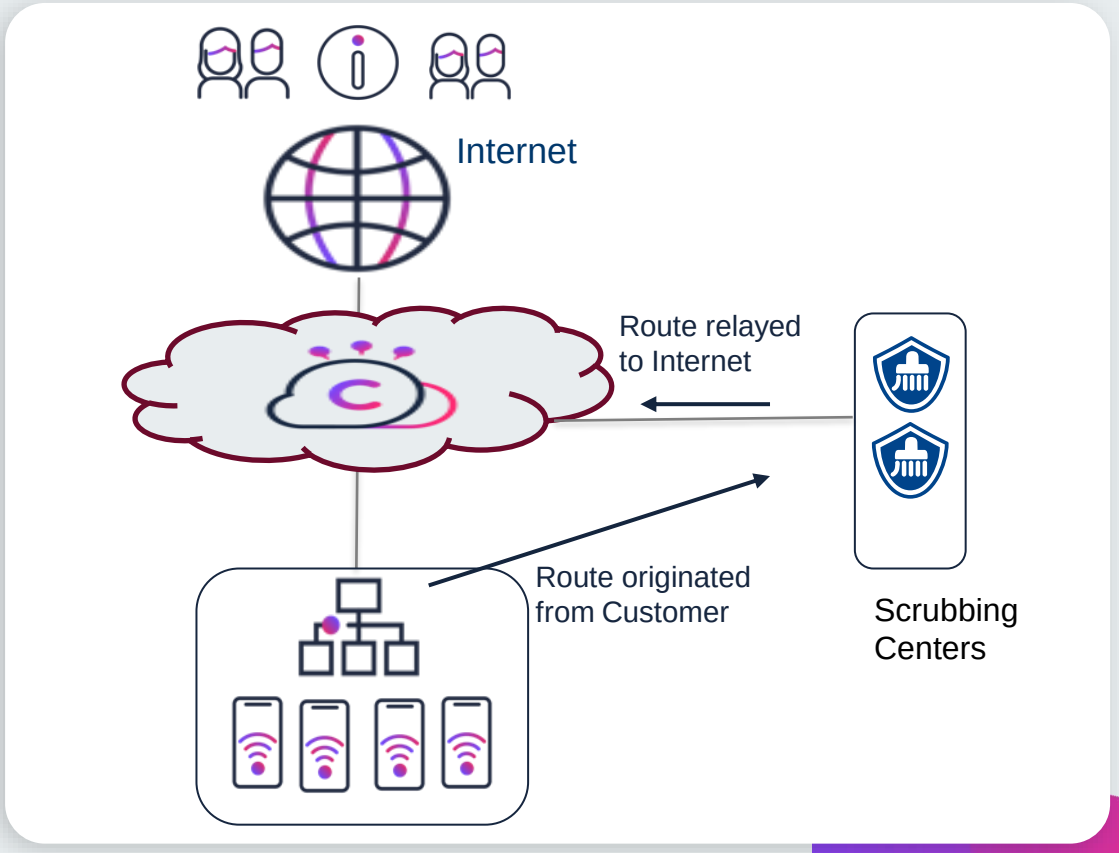
Network Design

Route Hijack triggering

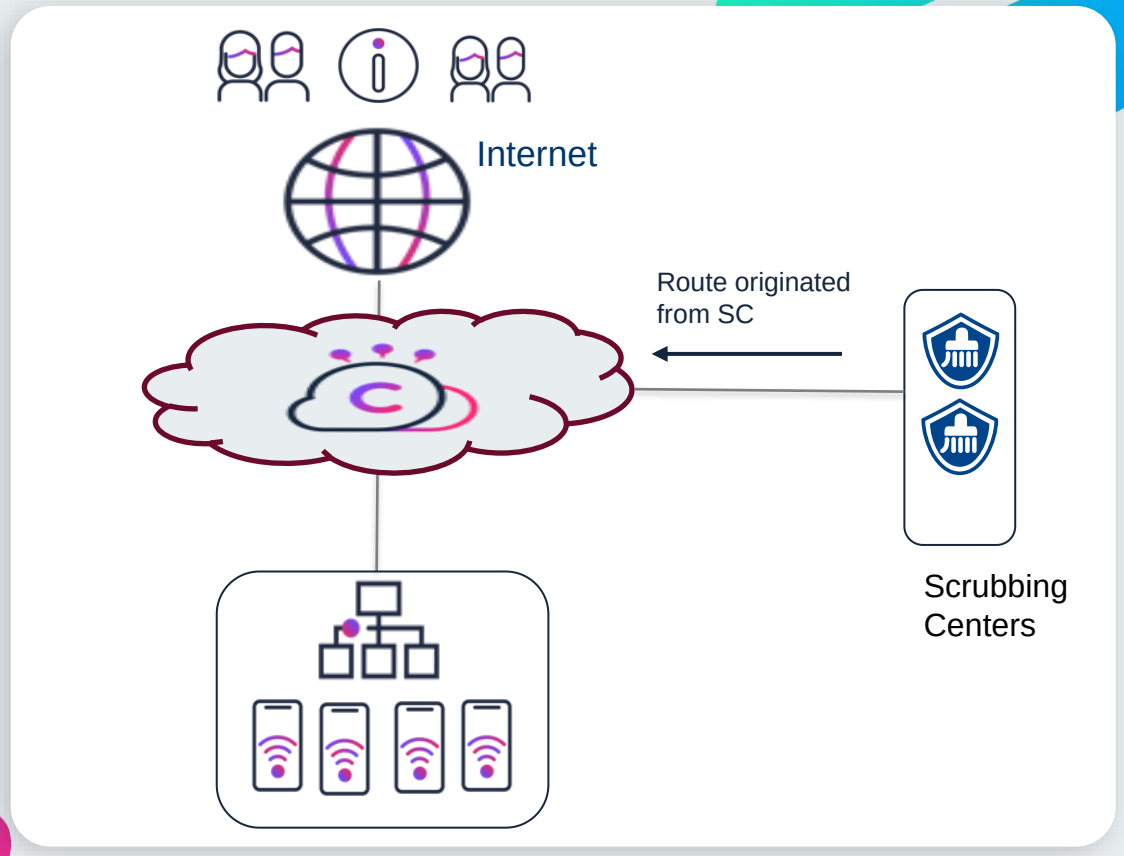
Two ways to trigger traffic hijacking (DDoS mitigation)

PCCW Global | consoleconnect

By Customer



By Scrubbing Center

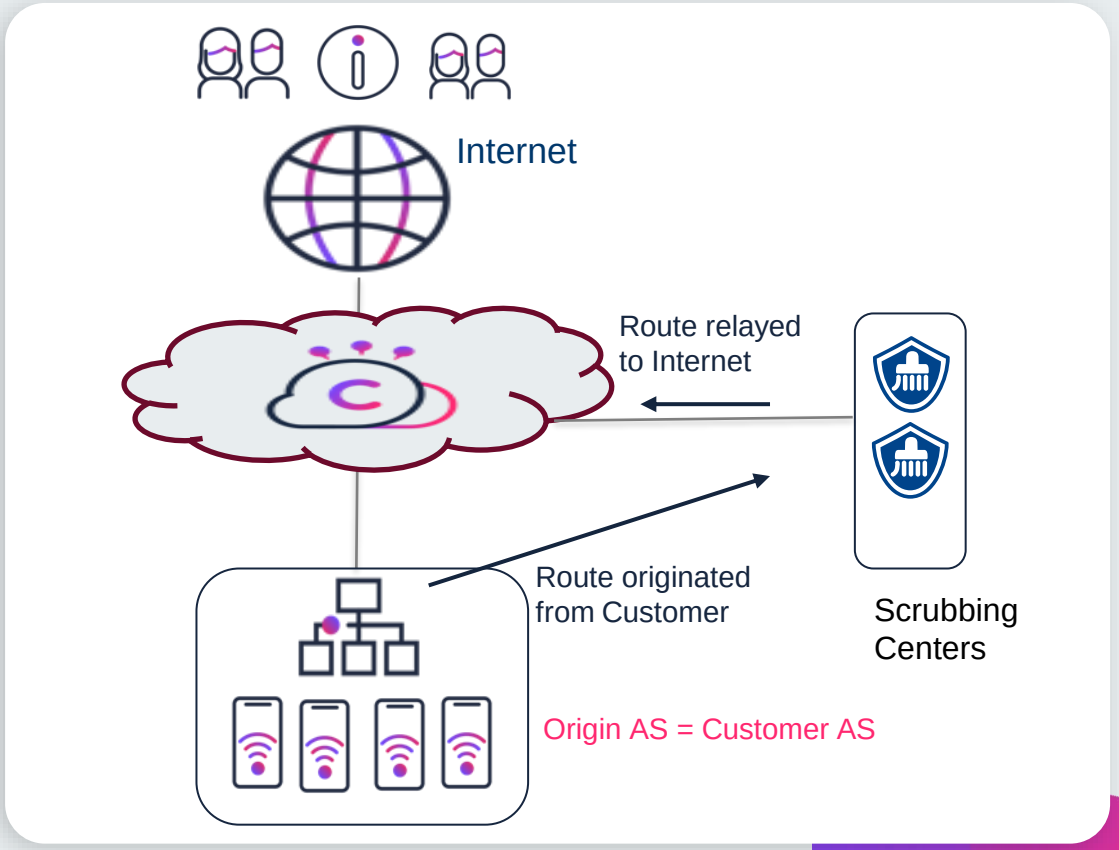


Network consideration for route verification during traffic hijacking

PCCW Global | consoleconnect

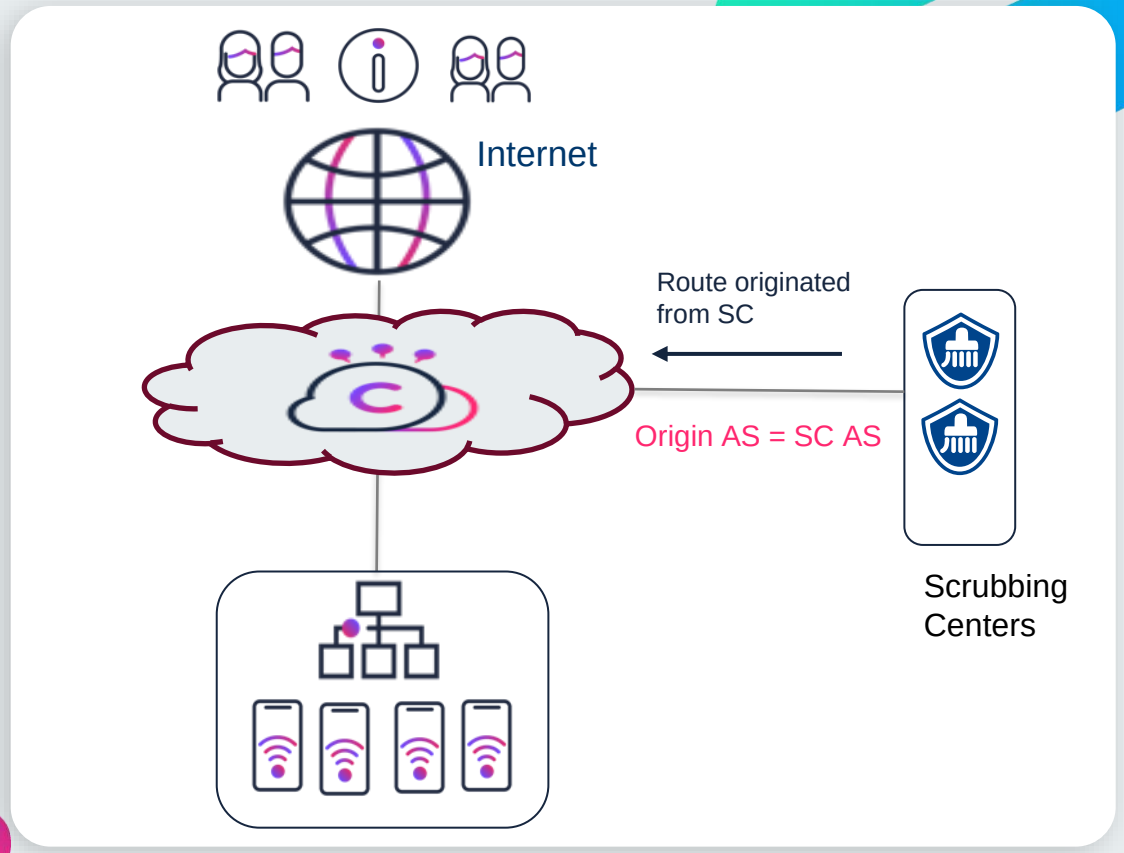
Origin AS # is unchanged → Preferred

By Customer



Origin AS # is changed → Origin AS creation in Router Object

By Scrubbing Center



Best Practice

Maintain the same level of Security Check for Anti-DDoS Service as Internet Service to validate Traffic Origin

PCCW Global | consoleconnect

Thank you

Australia
Level 3 | 200 Mary Street | Brisbane QLD 4000 | Australia

United Kingdom
7/F 63 St. Mary Axe | London EC3A 8AA | UK

France
2/F 16 rue Washington | 75008 Paris | France

Greece
340 Kifisias Avenue/340 Olimpionikon | Neo Psychiko 154 51 | Athens | Greece

Germany
Schillerstr. 31 | 60313 Frankfurt/M. | Germany

United States
475 Springpark Place | Suite 100 | Herndon | VA 20170 | USA

Singapore
6 Temasek Boulevard | #41-04A/05 | Suntec Tower Four | 038986 | Singapore

Hong Kong
20/F, Telecom House | 3 Gloucester Road | Wan Chai | Hong Kong

Japan
3/F Marunouchi Mitsui Building| 2-2, Marunouchi 2-chome | Chiyoda-ku | Tokyo 100-0005 | Japan

South Africa
Building 12 | 1 Woodmead Drive | Woodmead | Johannesburg 2191 | South Africa

UAE, Dubai
Office 504 & 505 | Level 5 | Arjaan Business Tower | Dubai Media City | Dubai

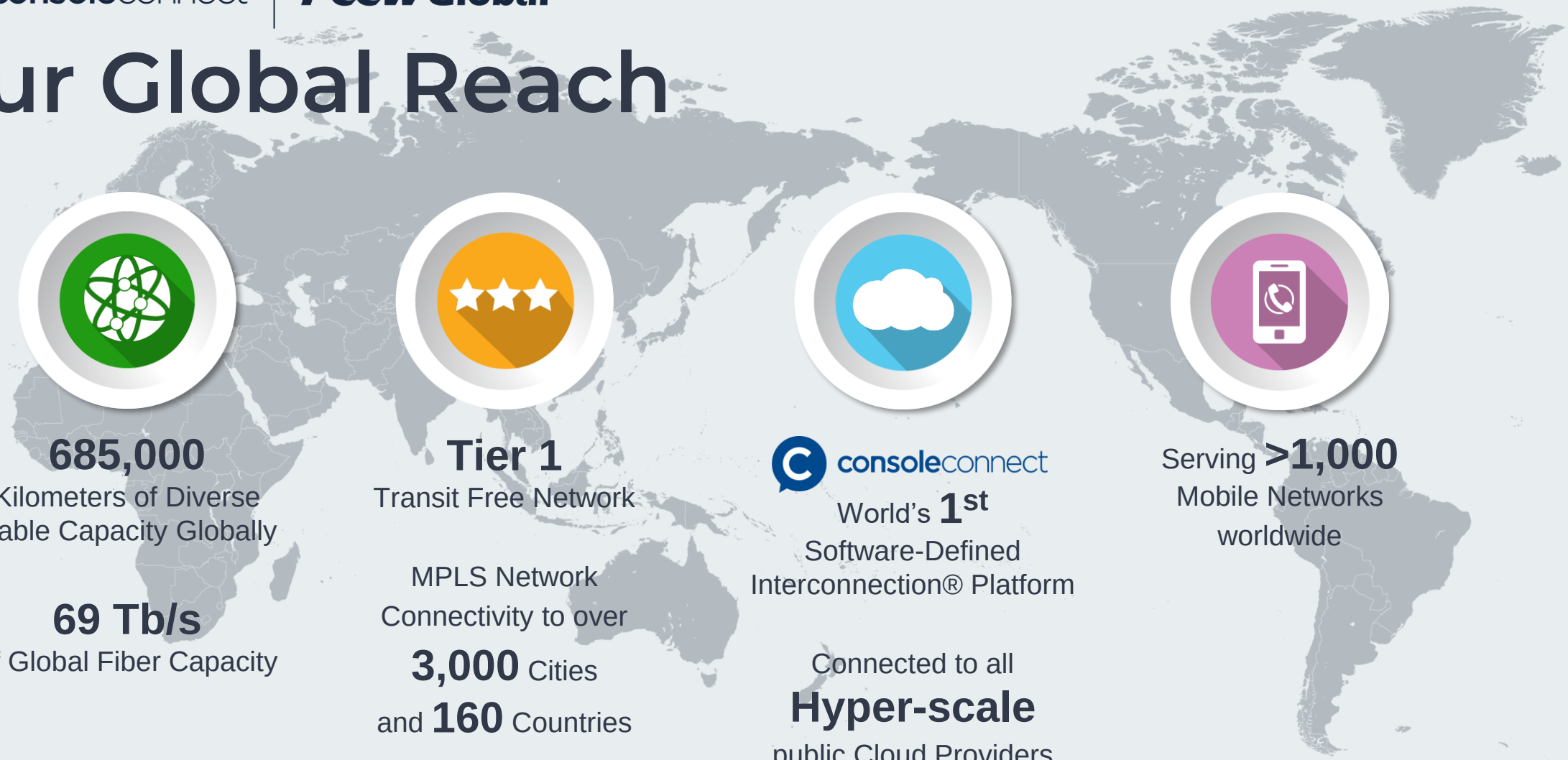
Talk to us: sales@consoleconnect.com

Section 05

Back Up

consoleconnect | PCCW Global

Our Global Reach



685,000
Kilometers of Diverse Cable Capacity Globally

69 Tb/s
of Global Fiber Capacity

Tier 1
Transit Free Network

MPLS Network Connectivity to over **3,000** Cities and **160** Countries

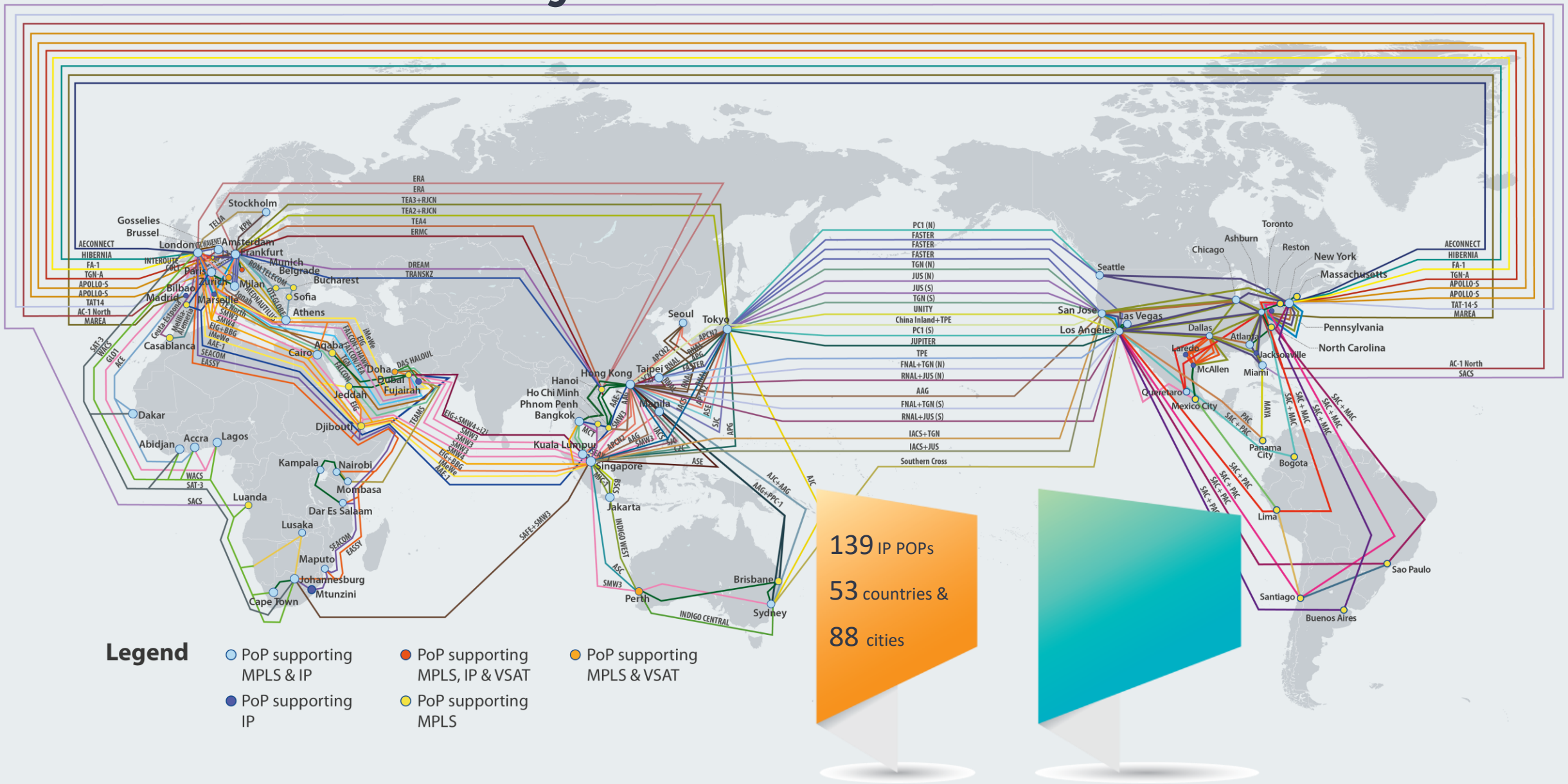
consoleconnect
World's **1st** Software-Defined Interconnection® Platform

Connected to all
Hyper-scale
public Cloud Providers

aws · Alibaba Cloud · Microsoft Azure · Google Cloud

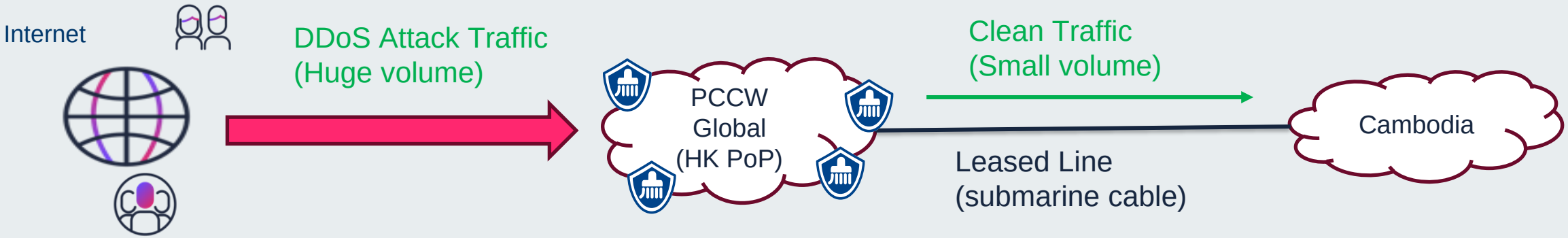
Serving **>1,000** Mobile Networks worldwide

Global Connectivity – IP Network



Advantage : Protecting expensive fiber usage

- Minimize the risk of link congestion



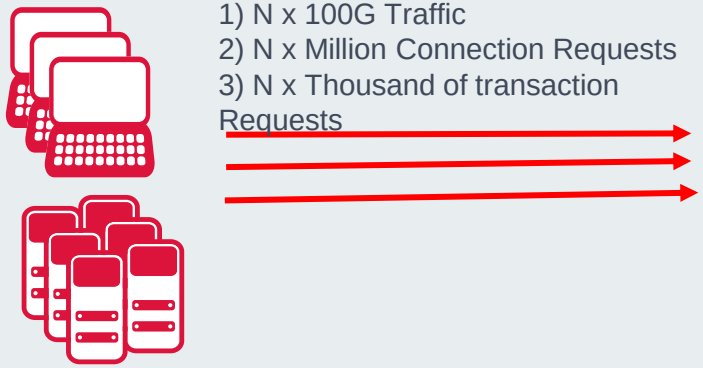
Advantage : Short latency

	Normal Transit (Single upstream provider)	ADD-Transit (Multiple upstream providers)
Scenario	Singapore source to Singapore destination	Singapore source to Singapore destination
Traffic Path	Customer may not enjoy local Singapore route (e.g. Singtel, SG IX) Singtel originated traffic goes to HK, then back to Singapore site	ADD customers can enjoy local Singapore route (e.g. Singtel, SG IX) Singtel originated traffic goes to Singapore site within Singapore
Impact	Long latency	Short latency

- The network quality of Anti-DDoS Transit is much better than pure AS 3491

What are the types DDoS Attack?

1. Volumetric Attacks
2. TCP State-Exhaustion Attacks
3. Application-Layer Attacks



1) N x 100G Traffic
2) N x Million Connection Requests
3) N x Thousand of transaction Requests

Zombie Computers / Botnet

Internet

Firewall

IDS / IPS

Server

2 TCP State-Exhaustion Attack

Attempt to consume the connection state tables in many infrastructure components, such as load balancers, firewalls, IPS and and etc by creating some amount of protocol request (e.g. connection requests).

Goal of attack : malfunction of infrastructure components
Impact due to attack : infrastructure cannot process normal protocol request

1) Volumetric Attack

Attempt to over-consume the Internet bandwidth between the target network / service and the Internet by creating massive traffic (huge data rate).

Goal of attack : link congestion
Impact due to attack : legitimate traffic cannot pass in / out from the target network

3 Application-Layer Attack

Attempt to consume the computing resource of targeted servers by generating a flood of transactions requests.

Goal of attack : malfunction of application servers
Impact due to attack : application servers cannot process normal application requests (e.g. HTTP request)

CyberSecurity

Market Landscape_

Market Competition – Anti-DDoS Service

1. Cloud-based managed security providers

- **Comprehensive security Portfolio**
- **Few or no CPE Solution**

- AWS
- Alibaba Cloud
- Cloudflare
- Google Cloud
- Microsoft Azure

2. Telecom Service Providers

- **Buy off-the-shelf technology box**
- **Integrate the box into its own network**

- BT (British Telecom)
- Lumen
- NTT Ltd.
- Tata Communications
- Verizon

3. Pure-play DDoS mitigation specialists

- **Specialized in developing DDoS technology**
- **Both CPE and Cloud solution**

- Akamai / Prolexic
- Arbor Networks
- F5 Networks
- Imperva
- Radware

As a network Provider
Our Advantage

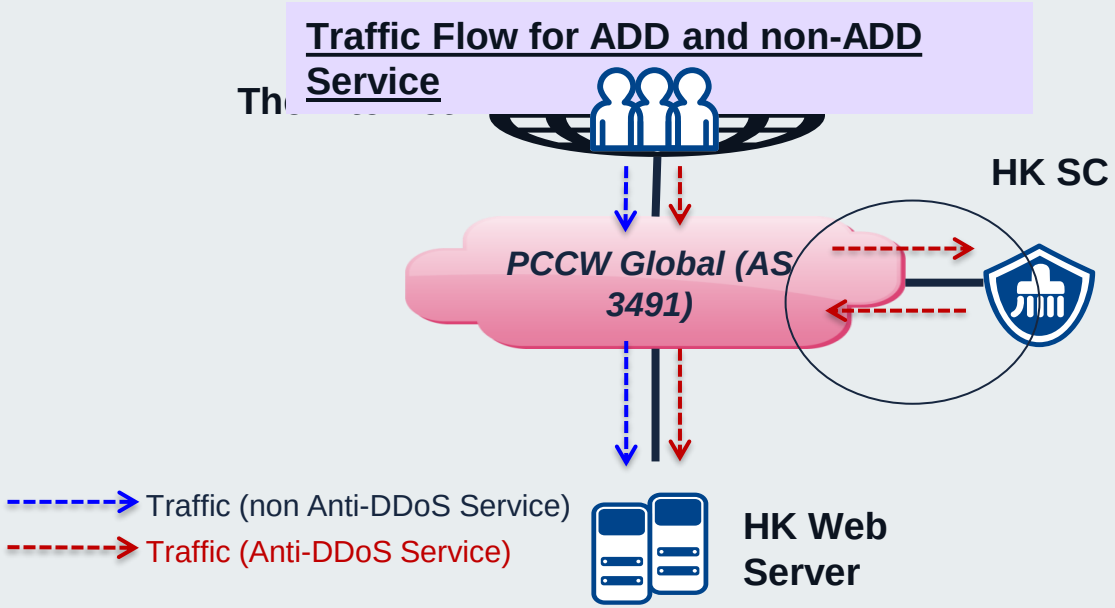
For BGP-based Traffic Diversion – Anti-DDoS Service

Single IP address (/32) diversion we, ISP, can divert only single IP address (/32) to Scrubbing Centres, not affecting the traffic path of other non-attack IP addresses

Short latency SC is only one network equipment, which may introduce additional 2-3 ms latency only due to Anti-DDoS Service..

Example of Predictable Traffic Performance

- Example, Users (Looking glass from US) while Server and SC are located in HK (AS 3491)
  - Without Anti-DDoS service
    - A US user pings a Hong Kong web server
    - 204 - 208 ms
  - With Anti-DDoS service activated
    - A US user pings a HK web server (traffic passes HK SC)
    - 212 - 214 ms
  - Extra 6-8 ms is introduced due to Anti-DDoS Service



Looking Glass

Welcome to Hurricane Electric's Network Looking Glass. The information provided by and the support of this service are on a best effort basis. These are some of our routers at core locations within our network. We also operate a public route server accessible via telnet at route-server.he.net.

Show options

core1.ash1.he.net> ping 209.9.217.6 numeric count 5

Count	5
Size	16 bytes
Target	209.9.217.6
Timeout	5000ms
TTL	64

Type	Source	Bytes	Time	TTL
Reply	209.9.217.6	16	207ms	61
Reply	209.9.217.6	16	208ms	61
Reply	209.9.217.6	16	204ms	61
Reply	209.9.217.6	16	204ms	61
Reply	209.9.217.6	16	223ms	61

Received Percent	Received Count	Received Fastest	Received Average	Received Slowest
100%	5/5	204ms	209ms	223ms

Entry cached for another 60 seconds.

2019-06-19 09:58:00 UTC

Show options

core1.ash1.he.net> ping 209.9.217.6 numeric count 5

Count	5
Size	16 bytes
Target	209.9.217.6
Timeout	5000ms
TTL	64

Type	Source	Bytes	Time	TTL
Reply	209.9.217.6	16	214ms	61
Reply	209.9.217.6	16	212ms	61
Reply	209.9.217.6	16	213ms	61
Reply	209.9.217.6	16	213ms	61
Reply	209.9.217.6	16	213ms	61

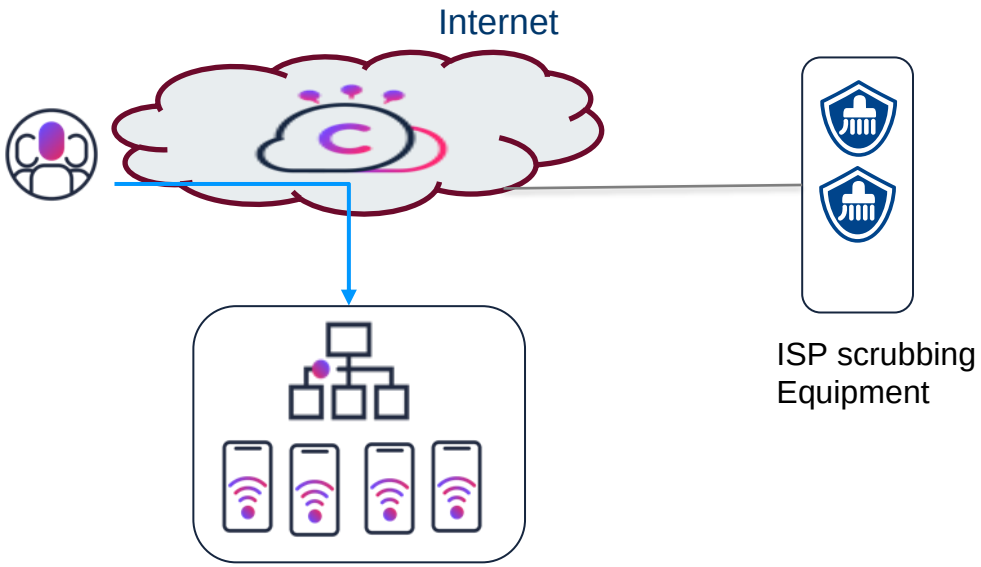
Received Percent	Received Count	Received Fastest	Received Average	Received Slowest
100%	5/5	212ms	213ms	214ms

Entry cached for another 60 seconds.

2019-06-19 09:52:02 UTC

IP Transit Customer

Traffic does not pass through SC

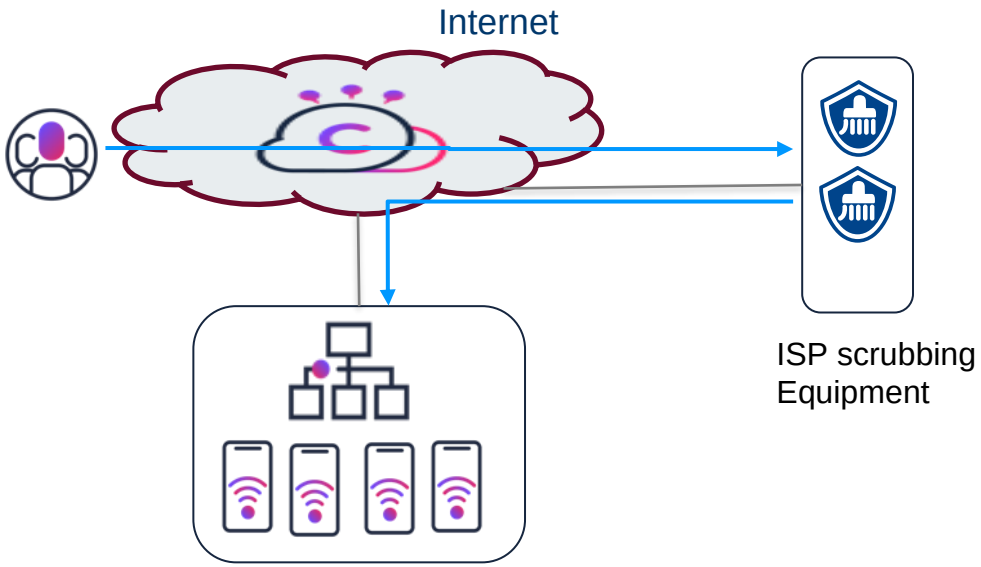


Latency is 3-5 ms

```
C:\Users\01295914>
C:\Users\01295914>
C:\Users\01295914>ping 209.9.217.6

Pinging 209.9.217.6 with 32 bytes of data:
Reply from 209.9.217.6: bytes=32 time=4ms TTL=57
Reply from 209.9.217.6: bytes=32 time=5ms TTL=57
Reply from 209.9.217.6: bytes=32 time=3ms TTL=57
Reply from 209.9.217.6: bytes=32 time=4ms TTL=57

Ping statistics for 209.9.217.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\Users\01295914>tracert 209.9.217.6

Tracing route to testweb1.pccwglobal.com [209.9.217.6]
over a maximum of 30 hops:

  1     3 ms     2 ms     2 ms  172.19.7.253
  2     2 ms     1 ms     2 ms  172.18.13.10
  3     2 ms     3 ms     7 ms  63-217-72-2.static.pccwglobal.net [63.217.72.2]
  4     2 ms     3 ms     4 ms  63-218-43-69.static.pccwglobal.net [63.218.43.69]
  5     3 ms     3 ms     5 ms  TenGE0-0-0-3.br02.hkg39.pccwbtn.net [63.223.20.49]
  6     7 ms     3 ms     6 ms  63-223-29-202.static.pccwglobal.net [63.223.29.202]
  7     3 ms     4 ms     5 ms  testweb1.pccwglobal.com [209.9.217.6]

Trace complete.

C:\Users\01295914>
```

Normal Anti-DDoS – 2ms more

Traffic passes through SC



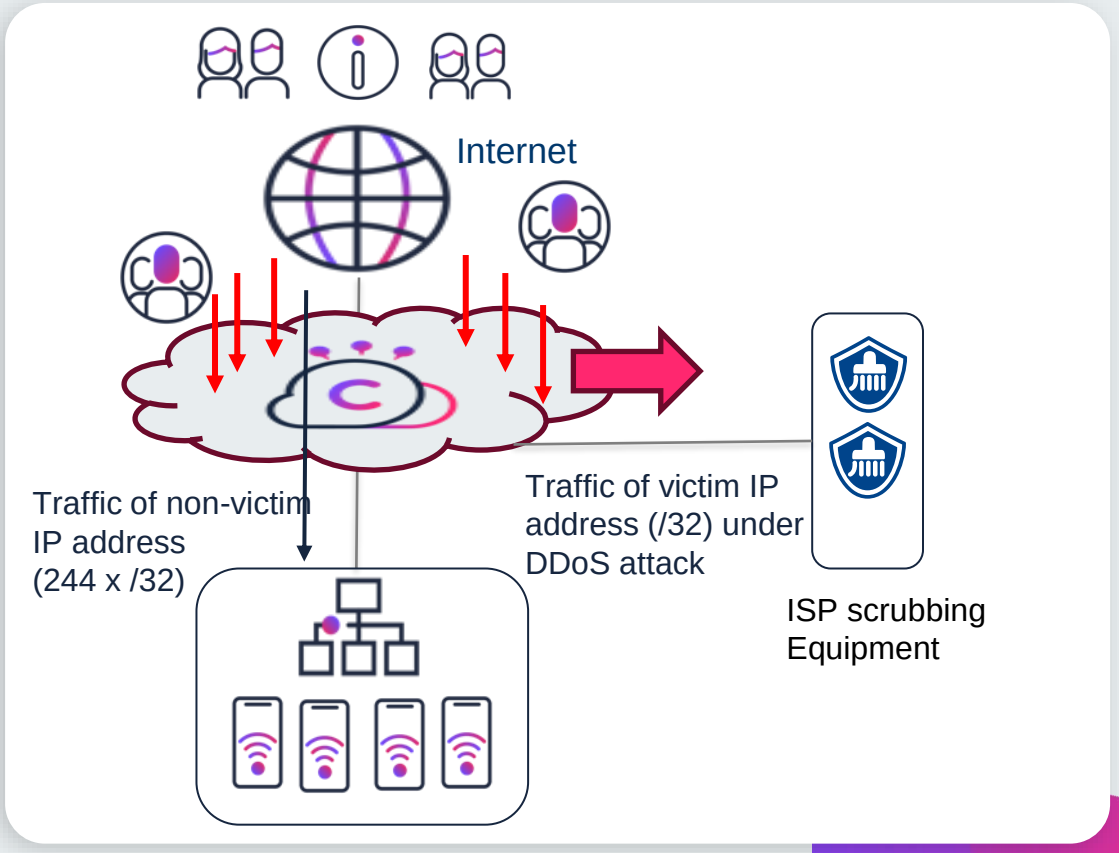
Latency is 4-6 ms

```
C:\Users\01295914>
C:\Users\01295914>
C:\Users\01295914>ping 209.9.217.6

Pinging 209.9.217.6 with 32 bytes of data:
Reply from 209.9.217.6: bytes=32 time=5ms TTL=57
Reply from 209.9.217.6: bytes=32 time=4ms TTL=57
Reply from 209.9.217.6: bytes=32 time=5ms TTL=57
Reply from 209.9.217.6: bytes=32 time=6ms TTL=57

Ping statistics for 209.9.217.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 6ms, Average = 5ms

C:\Users\01295914>tracert 209.9.217.6

Tracing route to testweb1.pccwglobal.com [209.9.217.6]
over a maximum of 30 hops:

  1     4 ms     2 ms     2 ms  172.19.7.253
  2    52 ms     2 ms     2 ms  172.18.13.10
  3     1 ms     2 ms     2 ms  63-217-72-2.static.pccwglobal.net [63.217.72.2]
  4     5 ms     3 ms     3 ms  63-218-43-69.static.pccwglobal.net [63.218.43.69]
  5     4 ms     3 ms     4 ms  HundredGE0-2-0-0.scbr01.hkg33.pccwbtn.net [63.223.44.33]
  6     3 ms     3 ms     3 ms  HundredGE0-2-0-0.scbr01.hkg33.pccwbtn.net [63.223.44.33]
  7     3 ms     3 ms     2 ms  63.222.64.18
  8     5 ms     2 ms     3 ms  10.15.10.3
  9     4 ms     7 ms     5 ms  10.20.30.38
 10     5 ms     4 ms     5 ms  testweb1.pccwglobal.com [209.9.217.6]

Trace complete.

C:\Users\01295914>
```

ISP Advantage for Anti-DDoS Service

Per-IP (/32) address traffic diversion

ISP-based Ant-DDoS Service (BGP Traffic Diversion)



Non-ISP-based Ant-DDoS Service (BGP Traffic Diversion)