TATA COMMUNICATIONS

TATA

DDOS ATTACKS & COLLATERAL DAMAGE WHAT CAN WE DO TO AVOID IT?

AKSHAY AGARWAL
HEAD OF PRODUCTS – MANAGED SECURITY SERVICES
TATA COMMUNICATIONS LTD

OCTOBER 2016

AGENDA

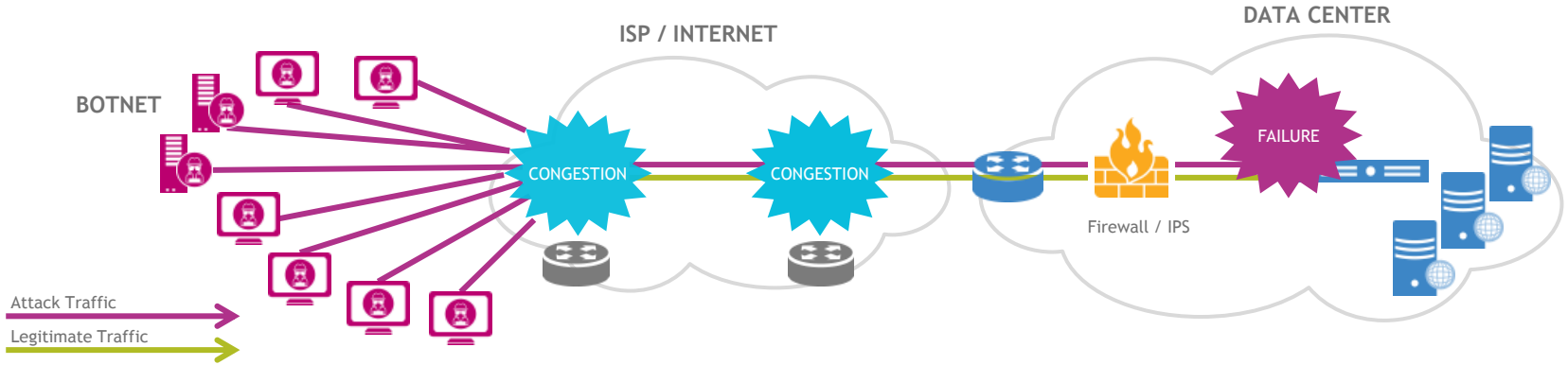
- DDOS ATTACKS – WHAT ? HOW ? WHO ?
- THE IMPACT (SIZE AND TYPES)
- THE COLLATERAL DAMAGE PROBLEM
- GLOBAL INDUSTRY BEST PRACTICES
- HOW CAN TATA COMMUNICATIONS HELP

DDOS ATTACKS - WHAT? HOW? WHO?

Sourced from DISTRIBUTED BOTNETs but triggered by C&C Servers.

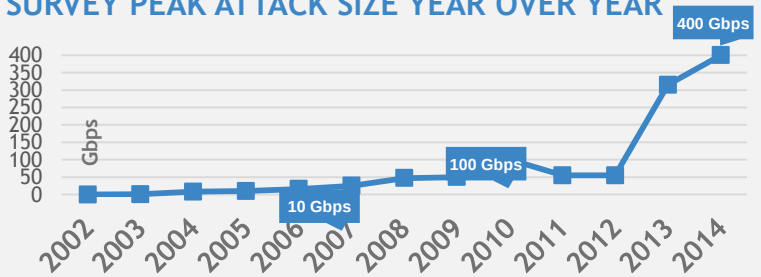
Attempt to consume FINITE resources, exploit design WEAKNESS, saturate infrastructure CAPACITY

Affects service AVAILABILITY, thereby Denial of Service to legitimate user traffic

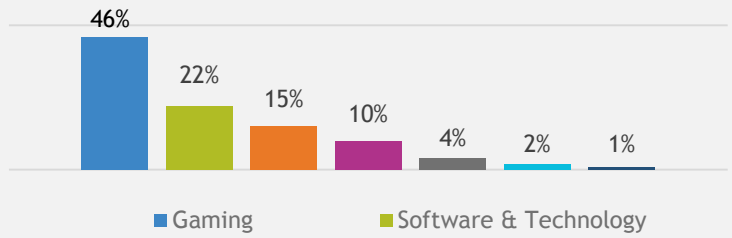


DDoS ATTACK TRENDS

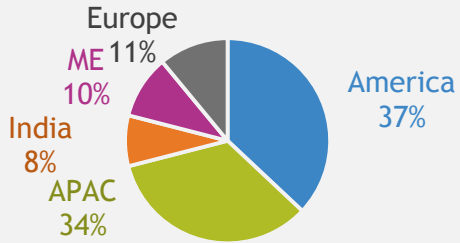
SURVEY PEAK ATTACK SIZE YEAR OVER YEAR



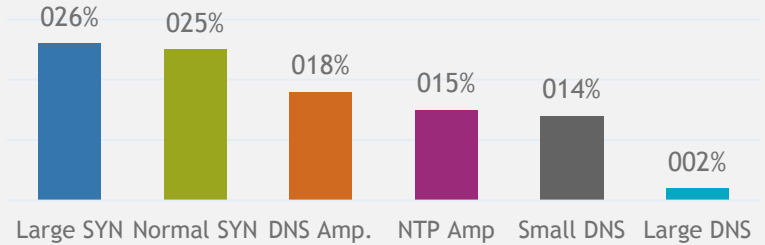
INDUSTRIES AFFECTED



TOP SOURCES OF DDOS ATTACKS



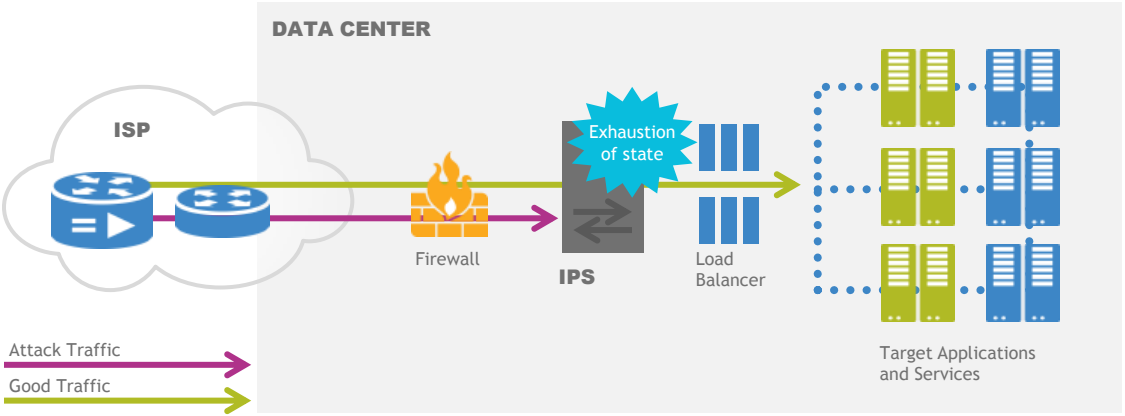
DDOS ATTACKS



DDOS ATTACKS CLASSIFICATIONS

DDOS ATTACK VECTORS ARE MAINLY CLASSIFIED AS VOLUMETRIC ATTACKS, TCP EXHAUSTION ATTACKS, AND APPLICATION LAYER ATTACKS.

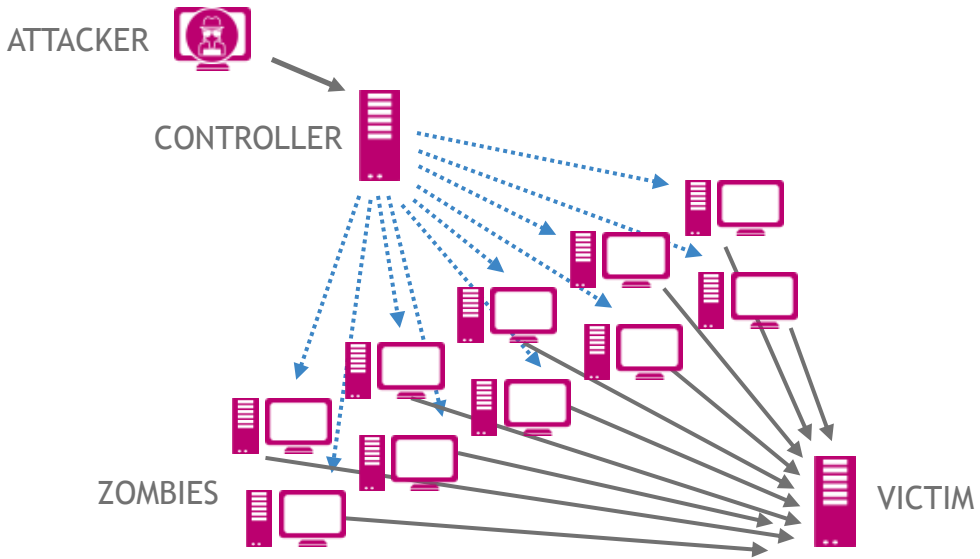
TCP STATE EXHAUSTION ATTACKS



- Consumes the connection state tables in devices like load-balancers, firewalls and application servers.
- High capacity devices capable of maintaining state on millions of connections can be taken down by these attacks
- 'TCP SYN flood' attack is a common example.

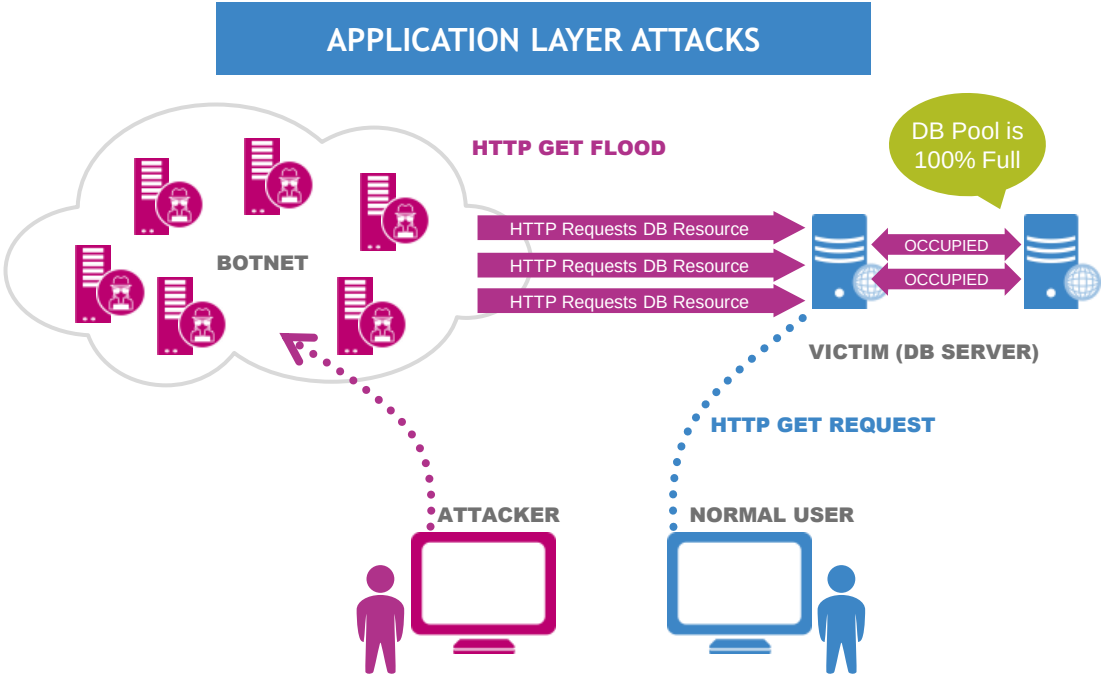
DDOS ATTACKS CLASSIFICATIONS

VOLUMETRIC ATTACKS



- Exploits stateless behavior of UDP protocol
- UDP based floods from spoofed IPs generates heavy bps/pps traffic volume
- Takes out Infra capacity – routers, switches, servers
- 'Ping flood', 'Smurf attack', 'UDP flood' etc. are volumetric in nature

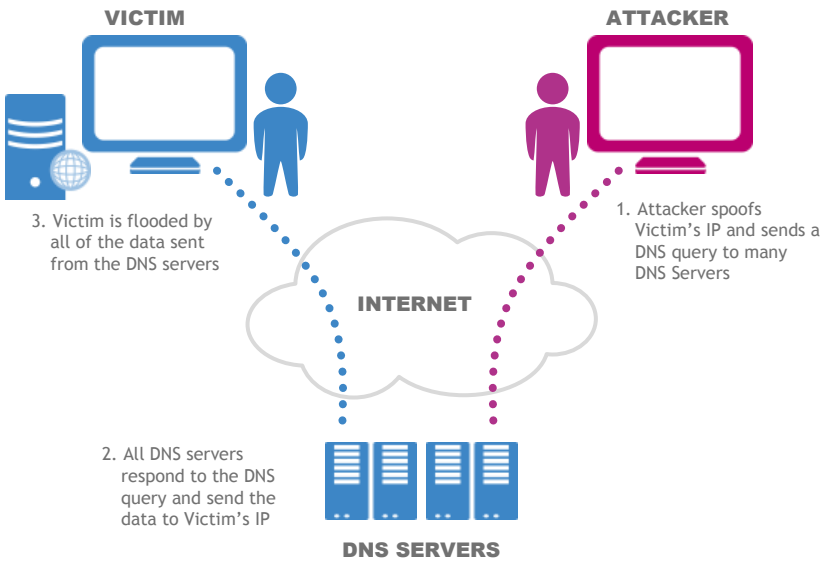
DDOS ATTACKS CLASSIFICATIONS



- Attacks which target an application or service at Layer-7
- Disguised to look like legitimate traffic, except it targets specific applications
- 'Slow Loris' is an attack which takes down a server by keeping open as many connections to the target as possible using http GET/POST floods

DDOS ATTACKS CLASSIFICATIONS

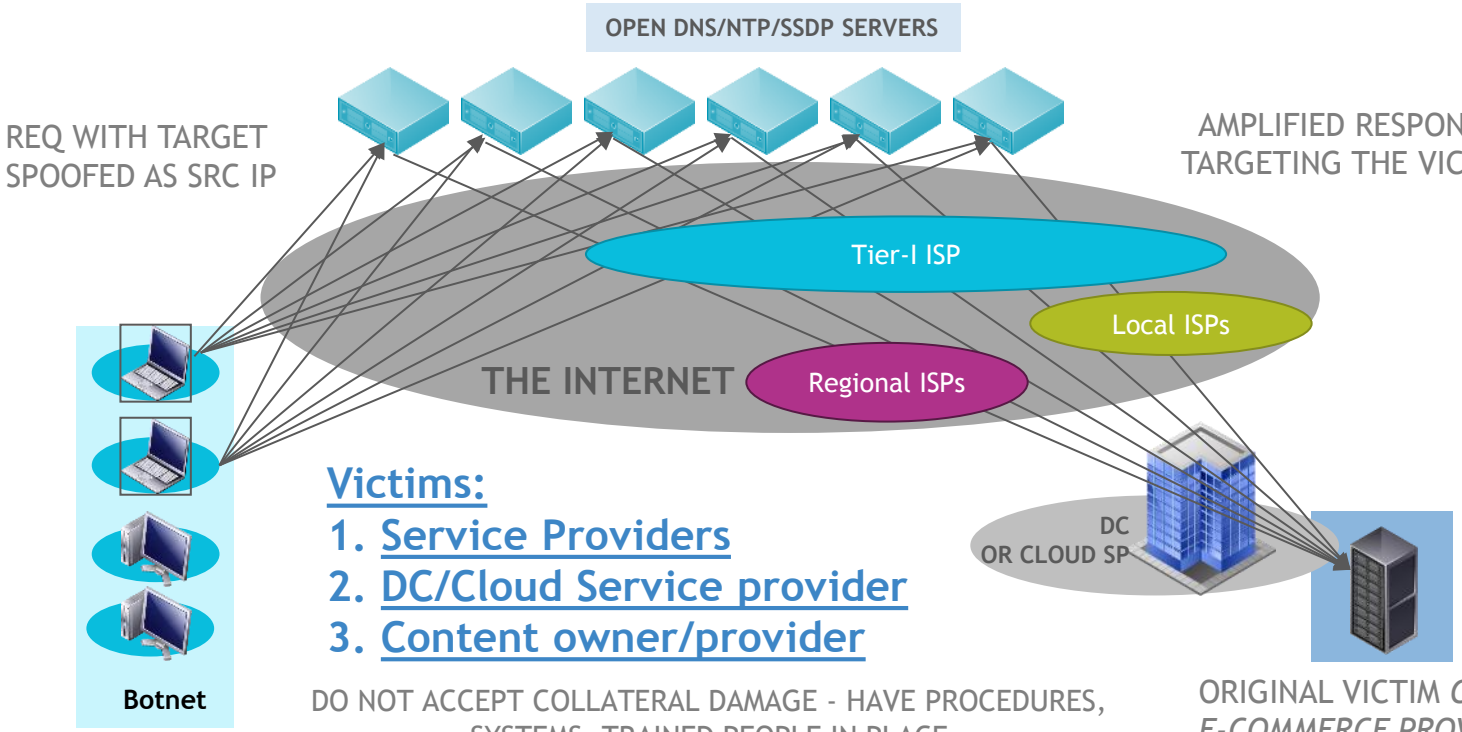
REFLECTION AND AMPLICATION



- Many protocols can be leveraged by attackers
- DNS, NTP, SSDP, CHARGEN, SNMP are commonly observed
- Amplification factors makes it lethal

Protocol	Ports	Amplification factor
NTP	UDP / 123	600x
DNS	UDP / 53	160x
SSDP	UDP / 1900	30x
CHARGEN	UDP / 19	18x
SNMP	UDP / 161	800x

DDOS ATTACKS - COLLATERAL VICTIMS



WHAT MAKES DDOS ATTACKS POSSIBLE?

- Failure to deploy network ingress filtering at the very edge – BCP 38, for anti-spoofing using ACLs or uRPF or IP Source verify
- Abusable services in the open Internet running on servers, home CPE devices, routers, and other IoT devices
- Low difficulty of execution of such attacks; readily available attack tools
- Network operators not utilizing the best practices
- Failure to deploy DDOS attack detection, response and mitigation tools

BEST PRACTICES FOR NETWORK OPERATORS

DON'T BE A PART OF THE PROBLEM

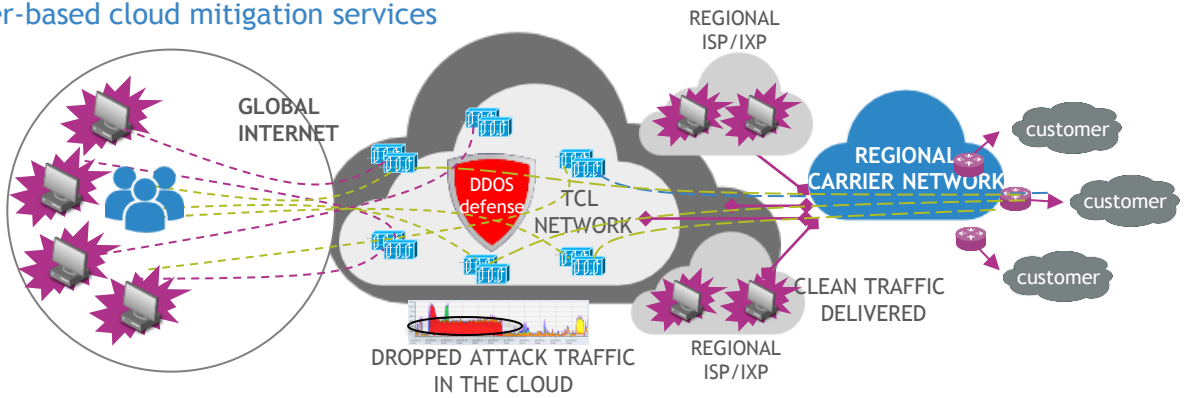
- Deploy anti-spoofing at network edge
- Don't be a spoofing-friendly network - or you will soon be blocked!
- Proactively scan for and fix abusable services
  - Block them if necessary to take them offline
- Check www.openntpproject.org and its equivalents to see if abusable services have been identified on your network and take suitable action
- Do not accept collateral damage - have a process and system in place

BUILD AN EFFECTIVE DDOS DETECTION AND MITIGATION SOLUTION

Regional DDoS defense layer

Deploying a local DDoS attack defense solution helps in mitigating regional attacks without having to direct all local and regional attack traffic to global DDoS defense layer.

- A deployment of DDoS attack detection and mitigation systems within network helps to defend attacks sourced from the region effectively.
- Regional traffic is scrubbed for DDoS attacks with no impact on network latency.
- Ideal Mitigation capacity = Total Ingress network bandwidth
- Minimum mitigation capacity = max attack size in the region, if the network transport has room to carry
- You can only Mitigate what you can carry on your network
- subscribe to Carrier-based cloud mitigation services



WHAT WORKS WELL?

Attack type	Impact on Network / DC Service Provider	Impact on content owner	Effective Mitigation technique
TCP State exhaustion	• Limited or Nil	**High** – Impacts all statefull devices in transit	• Arrested by SP Cloud Mitigation, if detected • On-premise CPE solutions are proactive
Volumetric	• Tier-1 operator – Nil or limited impact on rare occasions • Other DC and Tier-2/3 operators – Causes bandwidth choke-points based on capacity; leading to collateral damage	**High** – Impact at the network edge to server edge - weakest link fails	• SP Cloud mitigation
Application layer	• Tier-1/2/3 operator - Limited or Nil impact • DC Service provider services such as IaaS are impacted; design should adapt protection against noisy-neighbors (tenants)	**High** – weakest node breaks-down	• On-premise CPE solutions are effective • Basic attacks are defended by SP Cloud mitigation techniques
Reflective Amplification	• Tier-1 operator – Nil or limited impact on rare occasions • Other DC and Tier-2/3 operators – Causes bandwidth choke-points based on capacity; leading to collateral damage	**High** – Impact at the network edge to server edge - weakest link fails	• SP Cloud mitigation

TATA COMMUNICATIONS

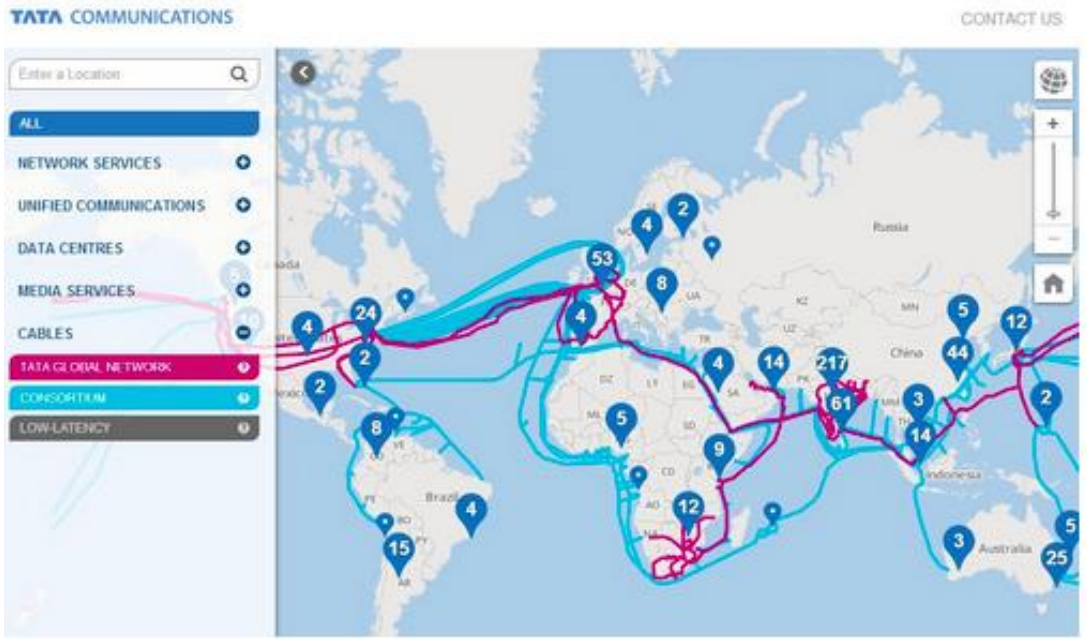
TATA

HOW CAN TATA COMMUNICATIONS HELP?

TATA COMMUNICATIONS' TIER 1 IP NETWORK

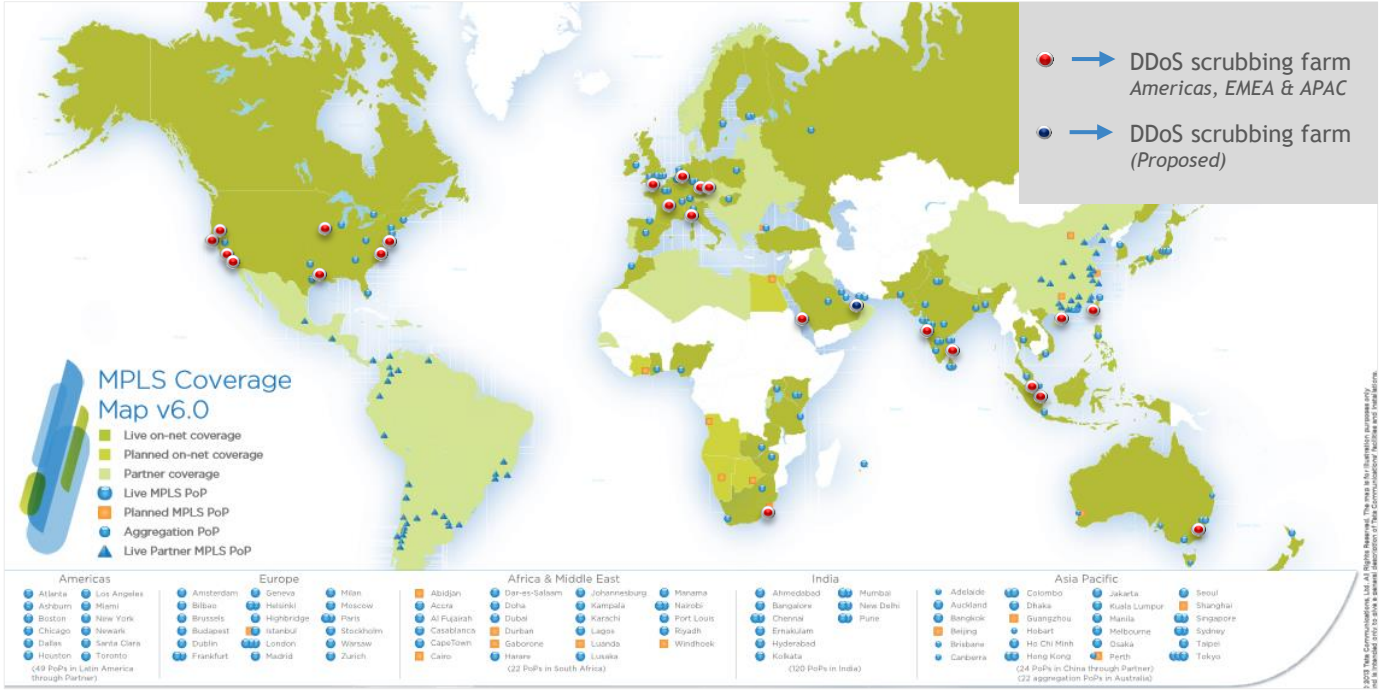
POWERS INTEGRATED DDOS DETECTION AND MITIGATION SERVICES

- 24% of the world's Internet routes are on our network
- Only Tier 1 Provider to feature in the Top 5 in 5 continents
- 99.7% of the world's GDP can be reached using the Tata Communications' Global Network



DDOS SCRUBBING FARM

GLOBAL DEPLOYMENT FOOTPRINT



WHAT MAKES TATA COMMUNICATIONS DIFFERENT

PROTECTING CUSTOMERS FROM DDOS ATTACKS FOR LAST 10 YEARS

EFFECTIVE PROTECTION INGREDIENTS




Tier 1 Service Provider - we peer with EVERYONE	Huge backbone capacity – we can absorb DDoS attacks easily	DDoS mitigation capabilities are already deployed in our network	We can deliver mitigation services to ANYONE, ANYWHERE
Other Service Providers accept new routing info from us automatically	The traffic is minor in comparison to the normal traffic we route	Customers don't have to wait for us to deploy new capacity – it's already there	No need to take connectivity services from Tata

WHY DO TRADITIONAL TOOLKITS FAIL TO PROTECT FROM DDoS ATTACKS?

- Traditional network protection devices like firewall and IPS/ IDS are in-line, stateful devices and are vulnerable to state exhaustion ddos attacks.
- Firewall /ips/ ids are the first to be affected by large flood or connection attacks and are the 'weakest link in the chain'
- These network protection devices use signature – based analysis or URL blacklisting to detect and prevent threats and hence fail to detect the ddos attacks
- Attacks like TCP SYN flood, targets webservers with partial open TCP connections choking the bandwidth and forbid legitimate customers to access the requested service