Solution Brief

BGP Flowspec
First Line of Defense Against DDOS Attacks

DATE 11th November 2016 | Managed Security Services

For more information, visit us at www.tatacommunications.com

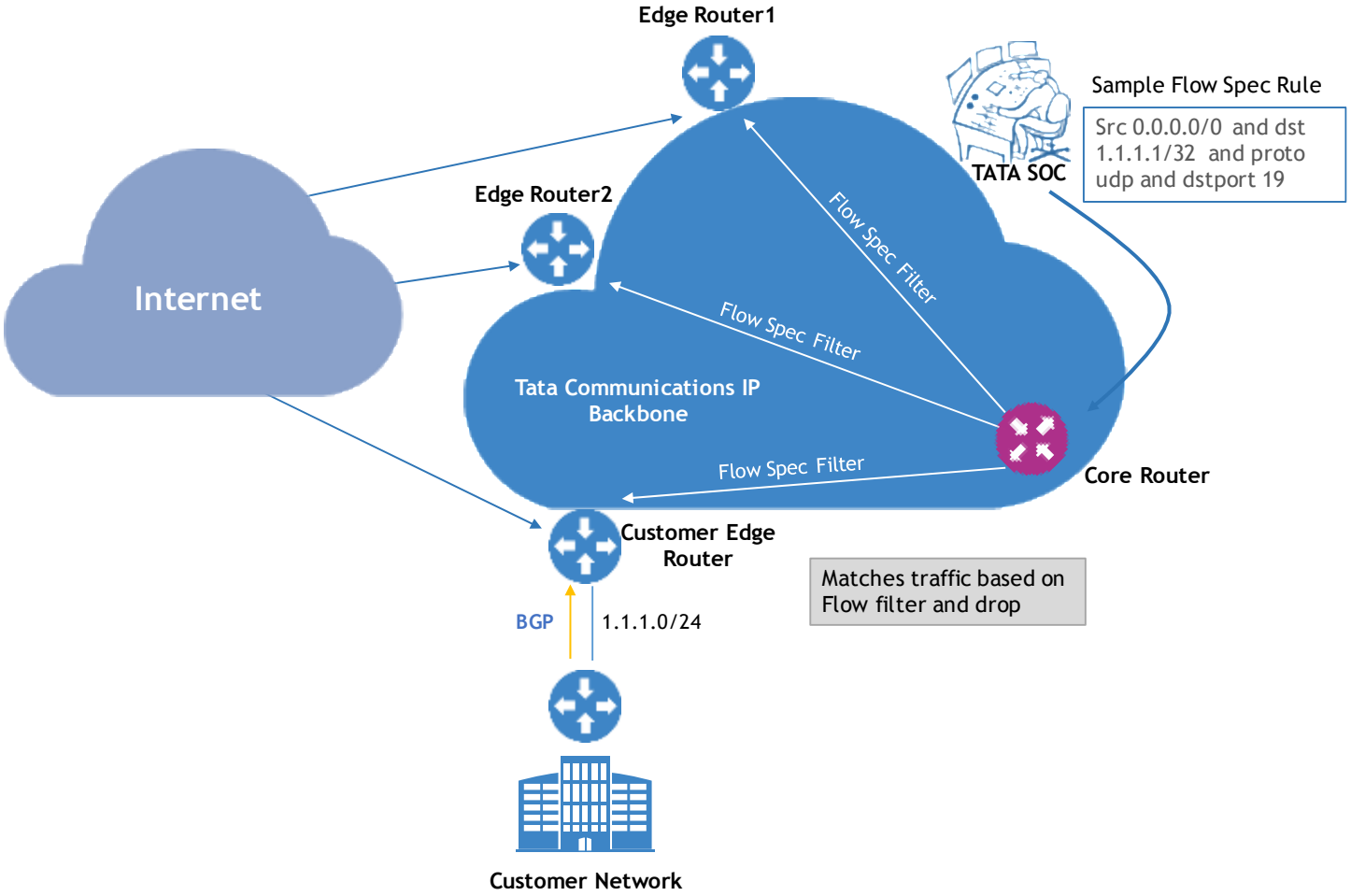
FIRST LINE OF DEFENSE AGAINST DDOS ATTACKS

What is BGP (Border Gateway Protocol)?

BGP (Border Gateway Protocol) is protocol that manages how packets are routed across the Internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) - networks managed by a single enterprise or service provider.

What is BGP Flowspec?

A new feature to assist in DDOS mitigation in a dynamic fashion, leveraging BGP. Flowspec uses the BGP protocol extention to distribute flow specification filters to network routers. By expanding routing information with FlowSpec the routing system can take advantage of filtering capabilities on the forwarding path – if a threat is identified, the Tata Communications Security Operations Center (SOC) inputs a rule to block or deny traffic related to the threat using a number of filter characteristics, incuding Destination Prefix, Source Prefix, IP Protocol, Source or Destination Ports, Packet Length, etc. The malicious traffic is systematically filtered off the network, blocking threats globally before they can fully penetrate the customer network.



For more information, visit us at www.tatacommunications.com

How does it work?

Flowspec defines a way to spread filtering policy using BGP to edge devices for DDoS mitigation.

1) A flowspec rule is defined by the SOC (flow filter) that has both identifier and action information
2) This rule pushed down to the all network edge/border routers

   The routers match the traffic basis the new rule that is deployed; Action – As the match occurs the required actions undertaken on the traffic, these can be dropped, redirect etc.)

Tata Communications initiatives to enable additional layer of defense for our customers

1) Routers on our global capacities have been enabled with this feature, providing a seamless integration between the entire network perimeters
2) In addition to our strong mitigation capabilities, the additional layer allows the network to also provide a first layer of defense against DDoS attacks

DDoS Mitigation capabilities

- 17+ Scrubbing farms deployed globally
- Global Scale: Detect and Mitigate DDoS attacks near source (starting from /32 subnets)
- Sensors deployed in 80+ PoP & 25+ countries
- Handling more than 30 global attack mitigations per day
- 24x7x365 Remote monitoring & management by SOC

Benefits of the Tata Communications BGP Flowspec solution

- Faster responses – The flow spec rule will be built in basis the monitoring of attack patterns. Attacks are stopped at the network perimeter, before they can proliferate across the backbone and reach the customer
- Delivered by by Tata Communications as part of its global backbone capability, enabling an additional defense mechanism for the customer, as against competitors without a native backbone
- Integrated and delivered as part of the DDOS detection and mitigation at no additional cost

For more information, visit us at www.tatacommunications.com