Inter-Cloud DDoS Mitigation API

draft-fang-i2nsf-inter-cloud-ddos-mitigation-api

Luyuan Fang lufang@microsoft.com

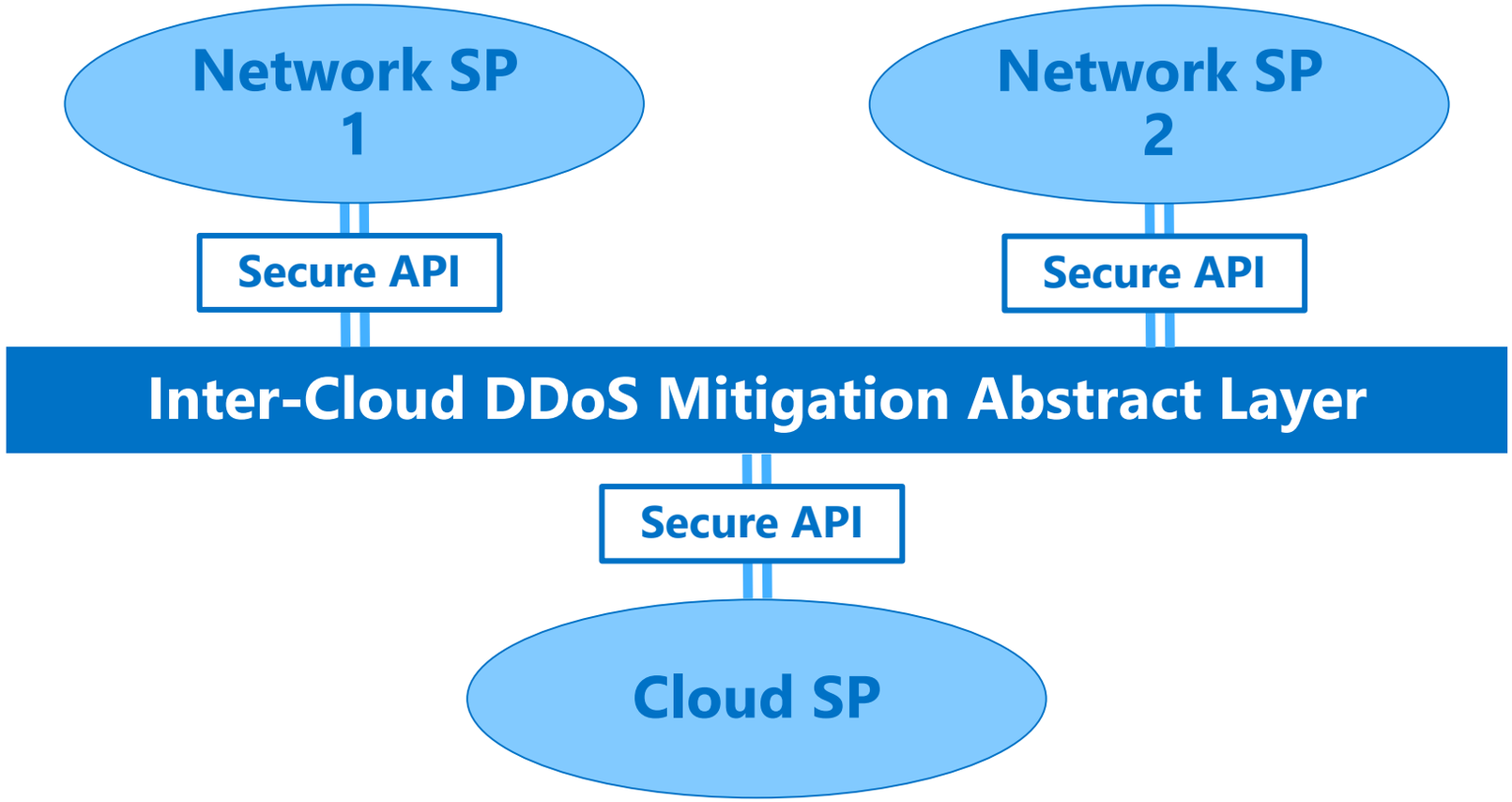
Deepak Bansal dbansal@microsoft.com

IETF 94, I2NSF WG, November 3, 2015

Problem Statement

- The recent growth in volume and scale of DDoS attacks can quickly saturated large inter-connection pipes of Inter-Cloud/Inter-Provider
- This types of attack can quickly render intra-cloud mitigation irrelevant
- Manual, slow, uncoordinated responses resulting in service loss
- Mitigation response time much slower than Intra Cloud DDoS attack response due to:
  - Lack of visibility of the DDoS status of partner Cloud or Network Providers
  - Lack of tools to support coordinated DDoS mitigation among providers
  - No standard API to allow automated real time information exchange

Inter-Cloud DDoS Mitigation Abstract Layer and APIs



- Achieve rapid protective response to Inter-Cloud DDoS attacks
- Provide standardized secure APIs to programmatically initiate real time information exchanges and coordinate DDoS mitigation mechanisms

Inter-Cloud DDoS Mitigation APIs

- DDoS Protection Types
  - TCP flood rate limiting
  - UDP flood rate limiting
  - TCP SYN/ACK/RST flood protection and authentication
  - Max concurrent connections per interval rate limiting
  - Max number of new connections allowed per interval rate limiting
  - Max fragment packets allowed per interval rate limiting
  - Max number of packets allowed per interval rate limiting
  - Black-holing
- BGP Signaling and Mitigation
  - BGP /24 route advertisement with community string option
  - Mitigation support for /32 with type and rate limit thresholds
  - /32 removal from mitigation
  - BGP support for /24 removal
- Attack Lifecycle Monitoring and Reporting
  - Volume and scale of the attack, signatures, forensic
  - Timestamps

Next Steps

- Collect feedback from WG
- Expand Inter-Cloud DDoS mitigation use cases and functionality
- Define API format
- Welcome contribution