Information Model and APIs for Network Security Policy Exchange

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

Luyuan Fang lufang@microsoft.com

Deepak Bansal dbansal@microsoft.com

I2NSF WG, IETF 95, Buenos Aires

April 7, 2016

Problem Statement – 1

- Today, there is no efficient, automated, standard way to exchange security information between providers
- As a result, the inter-provider inter-connection links are particularly vulnerable to attacks that can cause significant service disruptions
- Attacks to large inter-provider pipes:
  - Growing in volume
  - Growing in frequency
  - Growing in sophistication (e.g., leverage vulnerable services to amplify effect)
  - Increasingly using cloud services to launch major attacks

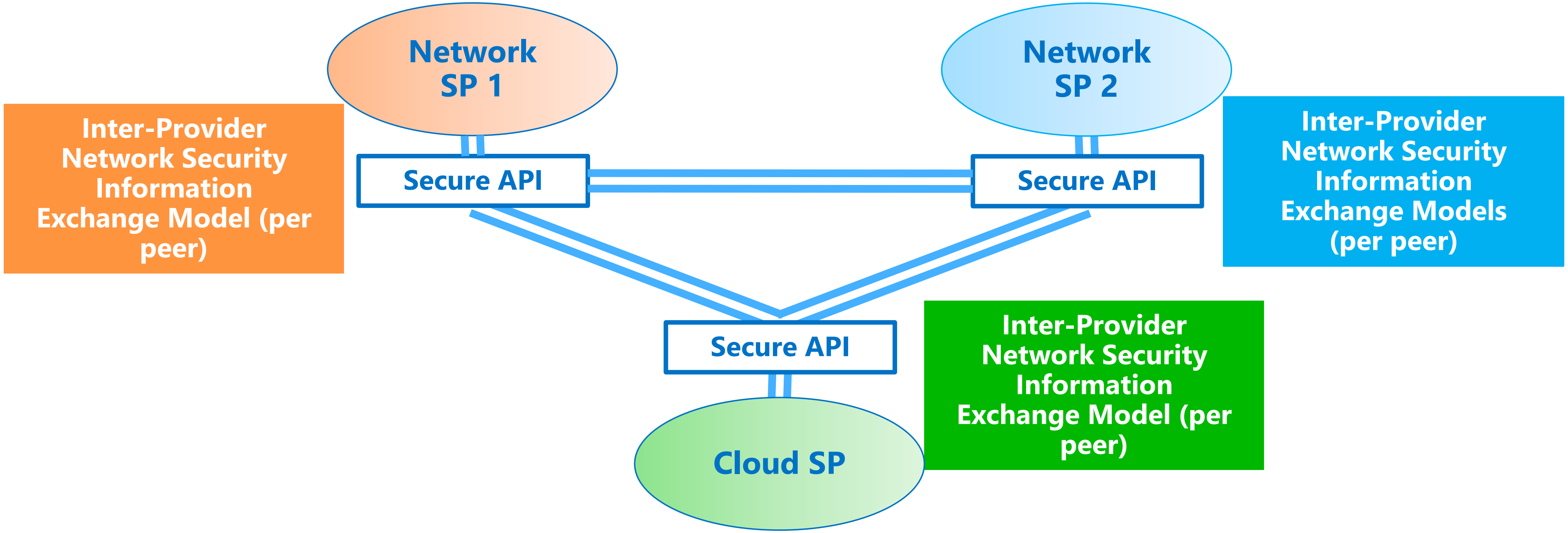
Problem Statement – 2

- The problem is at the demarcation between providers
  - Cloud Provider to Cloud Provider or Cloud Provider to Network Provider
  - Within its own Cloud/Network, each Provider has several automated mitigation mechanisms in place
- This types of attack can quickly render intra-cloud mitigation irrelevant
- Manual, slow, uncoordinated responses
  - Mitigation response time much slower than it is for Intra Cloud
- What makes these attacks more difficult to handle:
  - Lack of visibility of the attack status of partner providers
  - Lack of automated tools to exchange attack-related information and support coordinated mitigation

Requirements

- Standardized inter-provider information model for network security policy exchange
  - Information during attacks
  - Mitigation coordination
  - Forensic
- Standardized inter-provider APIs for network security policy exchange
  - Policy exchange on regular basis
  - Real time mitigation exchanges
  - Forensic exchanges
- Provider-specific tools can be built/deployed on top of this information model and APIs

Inter-Provider Network Security Information Exchange: Information Model and APIs


Inter-Provider Network Security Information Exchange Model (per peer)
Network SP 1
Secure API
Network SP 2
Secure API
Inter-Provider Network Security Information Exchange Models (per peer)
Secure API
Inter-Provider Network Security Information Exchange Model (per peer)
Cloud SP

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

Categories of Inter-Provider Network Security Information Exchange Model

1. Mitigation capabilities
   - Mitigation mechanism supported
2. Mitigation Request and response
   - Mitigation Request: One provider can "Request" for mitigation by partner provider
   - Mitigation Response: acknowledge, execute the required mitigation, report back
3. Monitoring and Reporting
   - Monitoring: Allow partner provider to monitor DDoS status and mitigation processes.
   - Reporting: Provide attack status reports to partner providers.
4. Knowledge sharing
   - Share forensic information
   - Coordinate mitigation strategies

Mitigation Capability Objects

- Rate limiting
  - TCP flood rate limiting
  - UDP flood rate limiting
  - TCP SYN/ACK/RST flood protection & authentication
  - Max concurrent connections per interval
  - Max new connections allowed per interval
  - Max fragment packets allowed per interval
  - Max number of packets allowed per interval
- Surgical mitigation
  - Black-holing
  - BGP flowspec
  - IDMS (Intelligent DDoS Mitigation Systems)

Requests and Response Objects

- Request Rate limiting
  - Rate limiting
    - TCP flood rate limiting
    - UDP flood rate limiting
    - TCP SYN/ACK/RST flood protection & authentication
    - Max concurrent connections per interval
    - Max new connections allowed per interval
    - Max fragment packets allowed per interval
    - Max number of packets allowed per interval
  - Surgical mitigation
    - Black-holing
    - BGP flowspec
    - IDMS (Intelligent DDoS Mitigation Systems)
- Response
  - Ack
  - Action

Monitoring and Reporting Objects

- Real time monitoring and reporting
  - Attack lifecycle: Volume, scale, location, time stamp
  - Black list and white list
  - Honey Pot
- Regular based monitoring and reporting
  - Status
  - Policy update
  - Black list and white list
  - Analytics report
- Forensic reporting
  - Attack analysis: signature, location, time stamp
  - Forensic analytics

Knowledge Sharing Objects

- Forensic reporting
  - Attack analysis: signature, location, time stamp
  - Forensic analytics
- Honeypot
- Black list and white list
- Policies
- Mitigation strategies
- General analytics

Next Steps

- Continue collecting feedback from WG
- Welcome contribution to complete information model objects