Bi-Lateral Security Management Framework (a.k.a. DDoS peering)

CenturyLink & AT&T

Nimrod Levy, Don Smith, John Schiel

nl7942@att.com, donald.smith@Centurylink.com , John.Schiel@Centurylink.com

LEXICON

Inter-ISP Flowspec

- Flowspec announcements initiated by a DDoS peer to drop attack traffic towards a victim ip

Unwanted traffic

- Traffic to be filtered by one ISP for another ISP

DDoS peering

- An ISP is dropping “unwanted traffic” for another

Peer

- Settlement-free peer

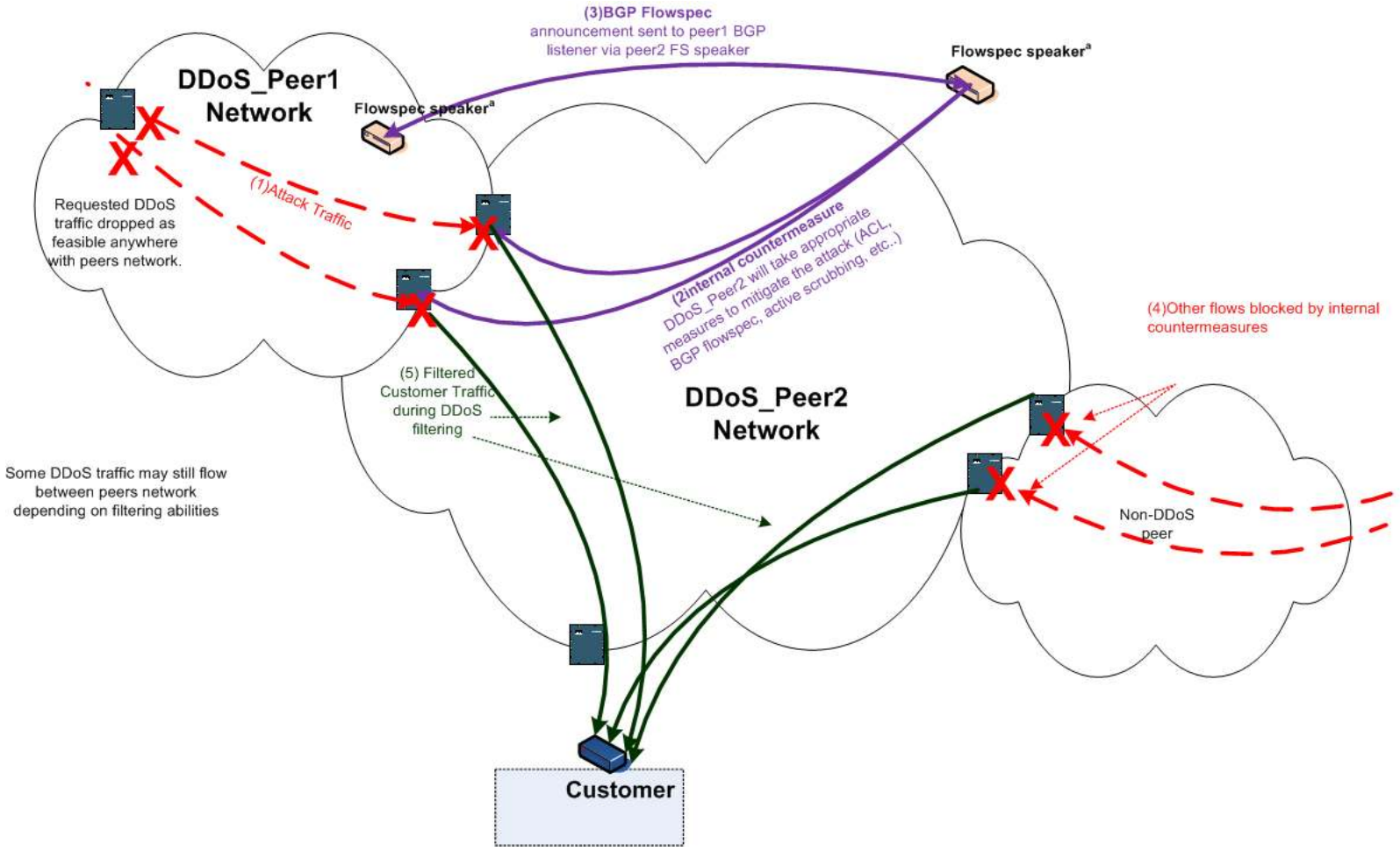
Background, Assumptions and Context

- Provides a process for peer networks to exchange filtering requests
- Between peering networks
- A relationship/environment for reciprocal benefits
- Institutional, not personal -> consistent approach

Reasons to Initiate Outreach to Peer

- Significant impact on customer/victim or infrastructure of the requesting network
- Significant benefit to the notified network
- Convey Network hygiene recommendations
- Management of vulnerabilities
- Pre-Requisite: Requesting network has implemented reasonable mitigations on its own network

DDoS Peering Diagram



Requests : Initiating, Authenticating, Verifying

- Must have AAA and CIA basic concepts.
- Not just Authenticated, Authorized and Accounting required
  - Confidentiality
  - Integrity
  - Availability
- Methods of secure filtering requests
  - BGP route announcements / inter-ISP Flowspec
  - Call using pre-established points of contact
  - EMAIL to a NOC/SOC common alias
  - Ticketing system
  - Other (TBD in individual frameworks)

TYPES/ACTION SUPPORTED (PER PEER)

- "standard 5-tuple" + ICMP
- Available TYPES
  - 1: Dest Prefix
  - 2: Src Prefix
  - 3: IP Protocol
  - 4: Port Type
  - 5: Dest port
  - 6: Src port
  - 7: ICMP type
  - 8: ICMP code
  - 9: TCP flags
  - 10: Packet LEN
  - 11: DSCP
  - 12: Fragment
- Initial types 1,3,5,6,7,8.
- Actions allowed -> drop
- Justification?

Rules for Route Advertisements

- Max-prefix N, alert for % of N, tear down at N+1
- Consistency with redundant announcements
- Duration is indefinite -> max-prefix withdraw then add
- Initial action drop packets
- Use BGPv4 for IPv4 and IPv6 flow routes
- NO_EXPORT, limit length /25 …/32
- Consistent community for this purpose

Response from Notified Network

- Implement block at any reasonable point between peers.
- Consider implementation of network hygiene practice
- Acknowledgement
  - We got your request
  - We did something/somewhere
  - Feed back loop

Other Considerations

- Requests withdrawn/cancelled by requesting peer
- Limited to significant events
- Peer has no obligation, may terminate action any time at their discretion
- Both networks must assess collateral impacts
- Implement with peers on a bi-lateral basis

Benefits of the Pilot/Proof of Concept

- Expands ISPs ability to withstand large DDoS attacks
- DDoS response more efficient:
  - Institutional not personal relationship
  - A pre-established/authenticated trust relationship
  - Pre-negotiated and pre-defined processes
  - Documented requests, specific data elements
- Additional benefit of not carrying unwanted traffic

Issues/Concerns

- Legal/Public Policy/Regulatory
- Confidentiality concerns
- Reporting

REFERENCE MATERIAL

- BCP 38 http://www.bcp38.info/index.php/Main_Page
- BCP 84 https://tools.ietf.org/html/bcp84
- UTRS http://www.team-cymru.org/UTRS/index.html
- DBHF community https://tools.ietf.org/html/rfc7999
- Flowspec
  - https://tools.ietf.org/html/rfc5575
  - https://www.nanog.org/sites/default/files/tuesday_general_ddos_ryburn_63.16.pdf