

# DOTS



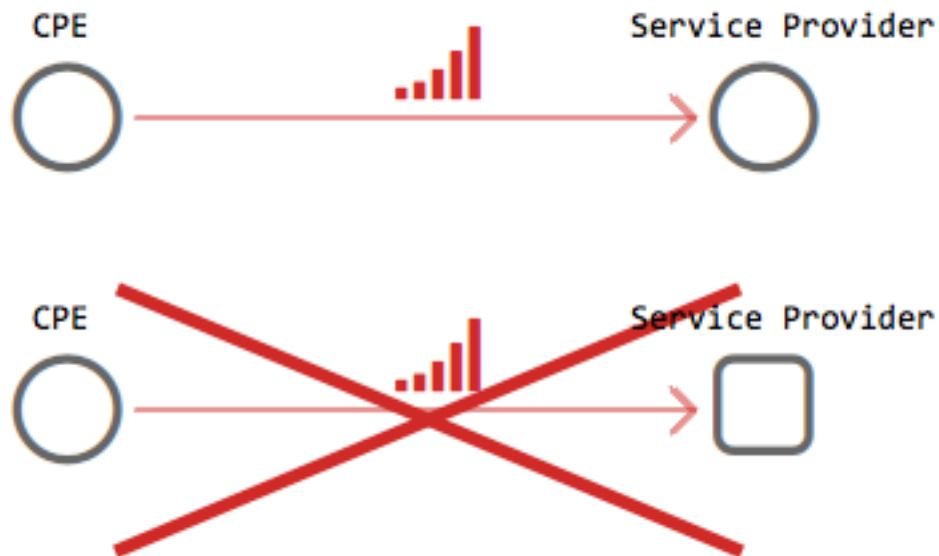
dots@ietf.org

IETF93

draft-teague-threat-signaling-01

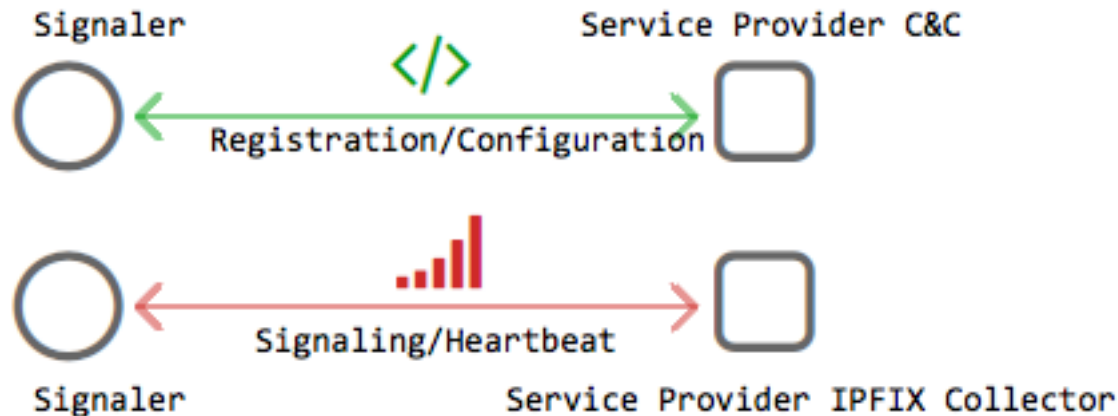
# Remind ourselves why...

- No vendor agnostic solutions.



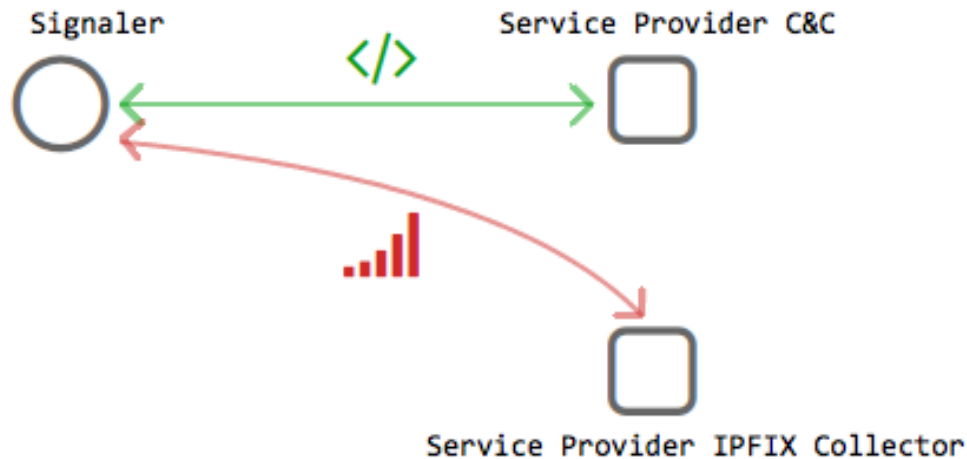
# draft-teague-threat-signaling-01

- I-D proposes a standard method for registration, configuration and real time communication of threat handling data by an on-premise DDoS mitigation node.



# draft-teague-threat-signaling-01

- Comprises 2x channels:
  - JSON RPC API over HTTPS for registration and configuration exchange
  - IPFIX based export using custom templates for heartbeat and data export while under attack



# JSON Channel

- Utilized to exchange command and control which can occur outside of mitigation activities
  - Registration
  - Authentication
  - Whitelist/Blacklist exchange
  - Dynamic allocation of IPFIX collector
  - Communication of load factor thresholds
  - Channel likely to be 12hourly or daily




# IPFIX Channel

- Utilized for heartbeat and actual signaling
  - 4x signaling templates are suggested
    - Events – summarizes attack profile
    - Protected object – details the target host/subnet and associated relevant stats
    - Attack/threat template – details information pertinent to the attack itself
    - Hearbeat response
    - UDP only??



# Template - Event

Event

Access Token
Key
Time
Type
Description
Scope
SOS
Thresholds

# A few words about events...

- Correlates to a device unique incident identifier
- Events are tied to the attack type
  - Multiple attacks will be communicated as multiple events
  - Where multiple attacks are correlated as belonging to a larger event, these may be linked by reusing the same key (a key being an incident identifier unique to the exporting instance).



...


- An SOS field is provided to request a mitigation by additional infrastructure or a service provider
  - This may communicate when a device or resource is constrained but may also be used to arbitrarily request action upstream based upon operator needs.
  - Draft page 4

# Template – Protected Object

Protected Object

Access Token
Key
Label
IP version
Address/Prefix
Protocol
Port
SLA Code Point
Mitigation Status
B/W Threshold
Current Pps
Current Bps
Peak Pps
Peak Bps
Typical Pps
Typical Bps

# Template - Attack

Attack/Threat ID

Access Token
Key
Threat Identifier
Threat Data


...

- The attack/threat export includes a data field which may be used to communicate additional data that may be useful to the upstream mitigation
  - Payload for analysis
  - Regex or signature from working on premise filters

# Attack definitions

- In order for disparate systems to be able to agree on what attack is being dealt to the victim, they must agree on how the attacks are to be identified and how they are represented
  - An attack dictionary is defined in the proposal which may be expanded with custom additions
  - Although not covered in detail in the 01 draft the JSON channel may be potentially expanded to exchange updated dictionaries

# Template – Feedback/Heartbeat

Feedback/Heartbeat

Access Token
Key
CurrentBps
CurrentPps

# Where next?

- You decide...