DOTS

dots@ietf.org

IETF92

DOTS?...

DDoS

Open

Threat

Signaling

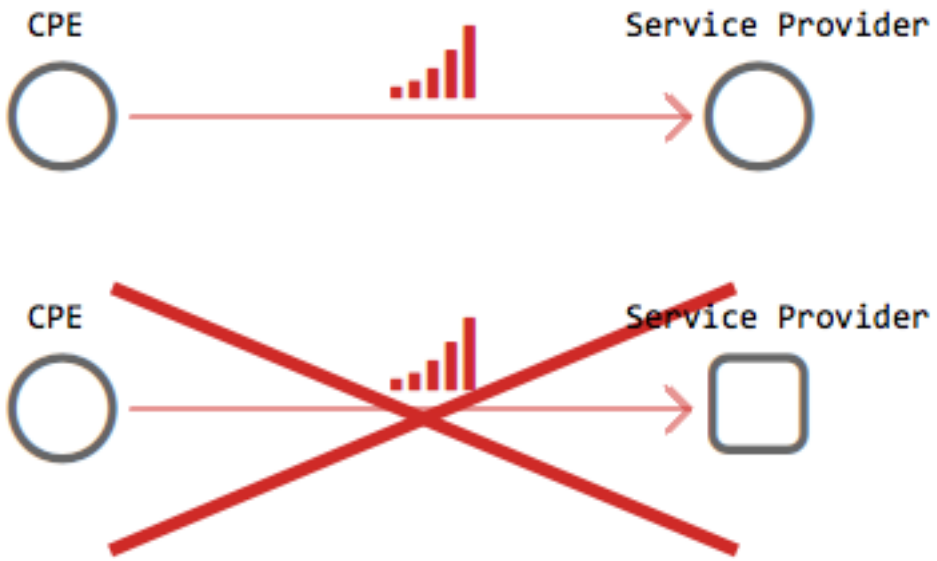
draft-teague-threat-signaling-00

The landscape…

- DDoS mitigation is an arms race
- Organisations deploying sophisticated on-premise mitigation devices
- Look to integrate with service provider offerings for traffic offramp
- This integration has a few challenges…

Communication

- No vendor agnostic communication solutions



Choice

- Which reduces my options
  - I prefer a circle for on-premise mitigation but my favored DDoS mitigation provider only supports squares
  - I want to create my own DDoS protection CPE capability which is a triangle and that doesn't work with anything else out there

Visibility

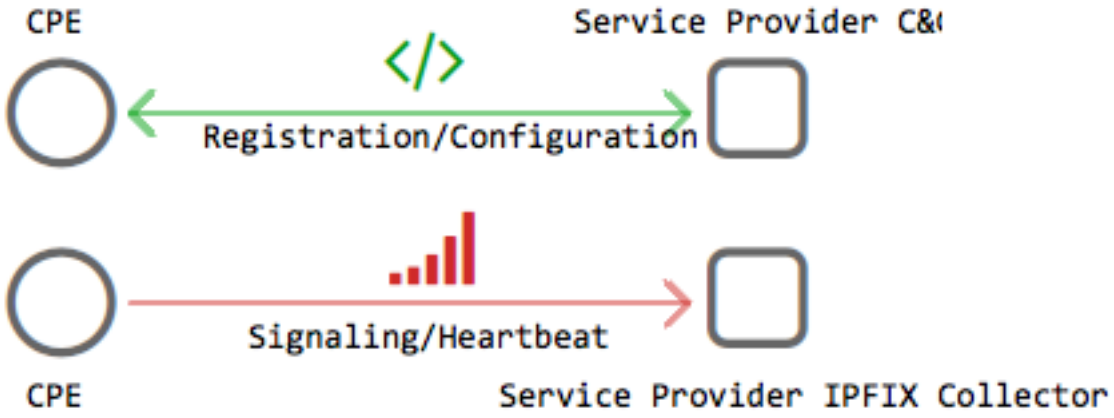
- The CPE dealing with an attack has a unique view of the network both in a steady state and while under attack
- Exposing this information to the service provider is invaluable in order for the provider to then tailor a faster response

What does DOTS offer?

- Vendor agnostic approach
- A greater choice to mix and match implementations - no lock in
- Upstream has the information it requires to initiate an immediate response (no relearning)
- Condense current exports to a single protocol
  - Flow, SNMP, syslog etc.
- An agreed implementation makes it easier to share

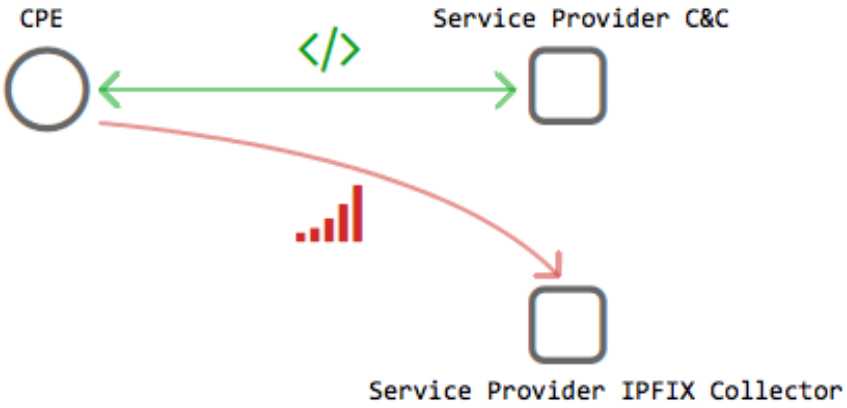
But what is exactly is DOTS?

- DOTS proposes a standard method for registration, configuration and real time communication of threat handling data by a CPE DDoS mitigation node



…

- DOTS 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

CPE -> Provider

- CPE initiates a periodic connection to the service provider using a user/role:password or api-key for initial authentication

```
METHOD:POST
URL:{scheme}://{host}:{port}/ocs/api/cloudinfo
Request Body:
{"device_ip":"<device ip>", "load_factor1": "<alias>",
"load_factor2": "<alias>" }
```

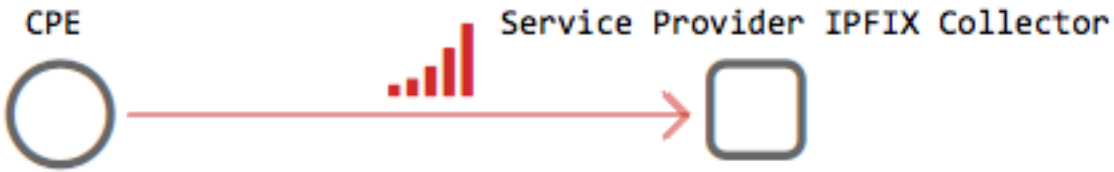
Provider -> CPE

- The provider will respond with configuration information

```
Response Body:
{
"access_token":"<Access-Token>",
"export_host":"<ip>",
"whitelist_ips":["<ip1>","<ip2>"..],
"device_threshold_config": {"load_factor1": "% of max",
"load_factor2": "% of max", "load_factor3":"% of max"}
"mitigation_info":
{"status":"<status(Inactive,Monitoring,Mitigating)>"
,"swing_flag":"<true or false>",
"blacklistaddrs":["<ip1>","<ip2>"..]}
"custom":"arbitrary data"
}
```

IPFIX Channel

- Utilized for heartbeat and actual signaling
  - Initially 3x 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
  - The event export may be used as a heartbeat when exported with null content



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 3

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 CPE 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 00 draft the JSON channel may be potentially expanded to exchange updated dictionaries

What else?

- Encryption?
- Heartbeat from provider -> CPE
- Optimisations
- Field name standardisation
- Interoperability with IODEF?