DDoS Open Threat Signaling (DOTS) Working Group

https://datatracker.ietf.org/wg/dots/about/

Roman Danyliw <rdd@cert.org>

IETF DOTS WG Co-Chair

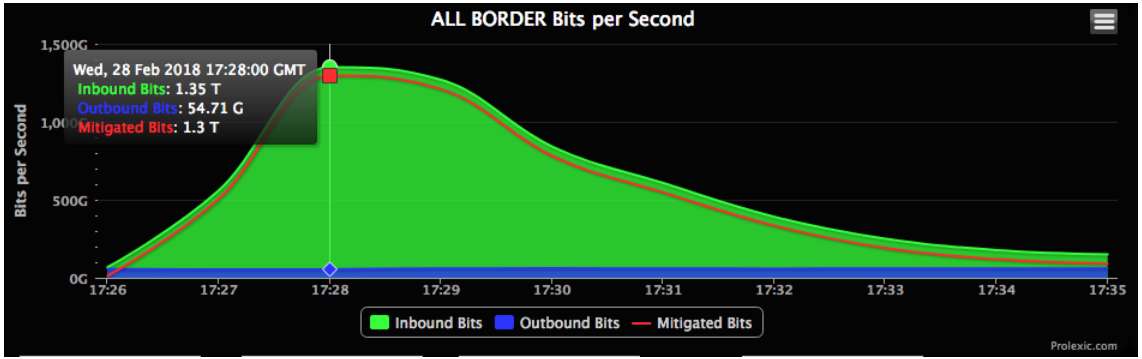
MAMI Management and Measurement Summit (M3S)

March 16, 2018

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0364

February 2018 [GITHUB-DDOS]



GitHub

Target

MEMCACHED

Technique

Akamai

Mitigation

All logos are copyright of their respective owners

Per Vendor APIs

[API-AKAMAI] [API-ARBOR] [API-CLOUDFLARE]

Using the Arbor Networks SP REST API: SP v8.3 API v3

This repository contains the source material for a document that is intended to be a gentle, user-facing introduction to the Arbor Networks SP REST API.

Formatting

The file `sp-rest-api-tutorial.` Orgmode formatting rules. You file; the examples in the file sho and the link to the Orgmode Gu

Contributing

All contributions are greatly ap emailed edits, printed and writt you.

Rendering

If you want to render this you c command to produce HTML, PD

Exporting from Emacs Orgmod then, assuming you have the La the commands:

pdflatex -shell-escape sp-rest-a tutorial makeindex sp-rest-api-t tutorial

Blog Support Log in

Cloudflare API documentation v4

Last modified: March 8th, 2018

Getting started

Cloudflare's API exposes the entire Cloudflare infrastructure via a standardized programmatic interface. Using Cloudflare's API, you can do just about anything you can do on cloudflare.com via the customer dashboard.

The Cloudflare API is a RESTful API based on HTTPS requests and JSON responses. If you are registered with Cloudflare, you can obtain your API key from the bottom of the "My Account" page, found here: Go to My account.

What is Cloudflare?

Cloudflare makes sites lightning fast, protects them from attacks, ensures they are always online, and makes it simple to add web apps with a single click. More than 5 percent of global Web requests flow through Cloudflare's network; every month more than 1.8 billion people experience a faster, safer, better Internet thanks to Cloudflare.

Audience for APIs

Cloudflare offers public APIs with three audiences in mind.

Akamai DEVELOPER GET STARTED APIS TOOLS LEARN CODE COMMUNITY BLOG REGISTER

Prolexic Analytics API BETA

OVERVIEW RESOURCES

The Prolexic Analytics API
Headers
Design Considerations
Errors
Rate Limiting-429 Status
Response Codes

The Prolexic Analytics API

The Prolexic Analytics API exposes analytics data from Prolexic DDoS protection and monitoring services such as alerts and network bandwidth timeseries data.

Headers

```
Authorization: EG1-HMAC-SHA256 client_token=[value];access_token=[value];timestamp=[value];nonce=[value];signature=[value]
```

- This is RFC2616-standard, with proprietary specifics.
- SDKs will be available for some languages.

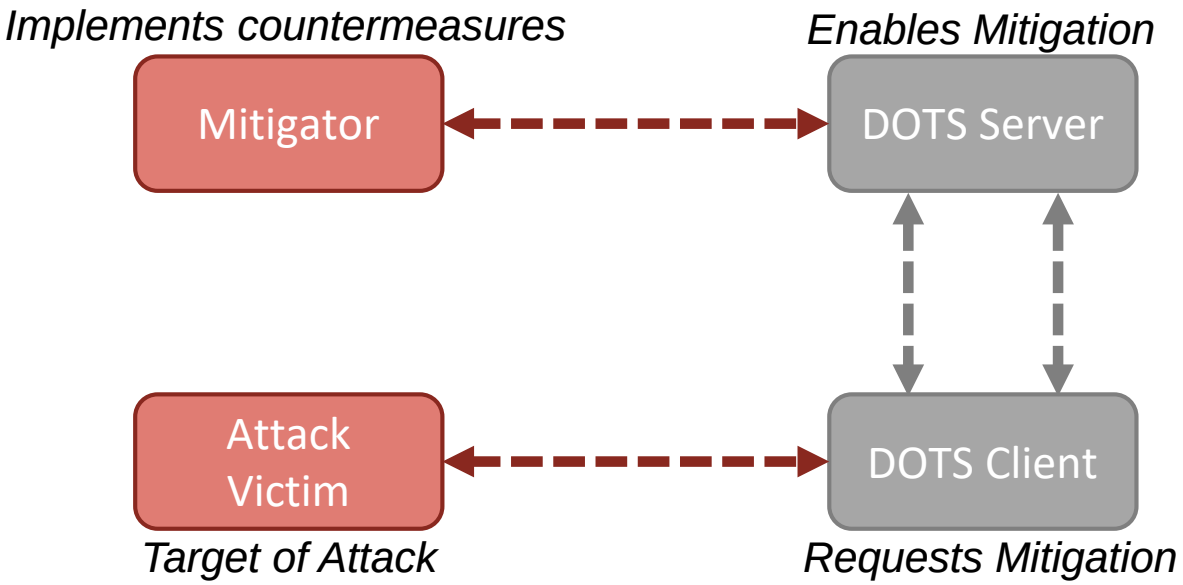
Example:

```
Authorization: EG1-HMAC-SHA256 client_token=akaa-275ca6de04b11b91-cf46074bf3b52950;access_token=akaa-d6cfbdb2d0594ae4-ad000cf3a5473a08;timestamp=20130817T02:49:13+0000;nonce=dd9957e2-4fe5-48ca-8d32-16a772ac6d8f;signature=Q3uWyssCz9qsNxekOX+PXP0WrtGT+J5qd6ssN1UmUmw=
```

Design Considerations

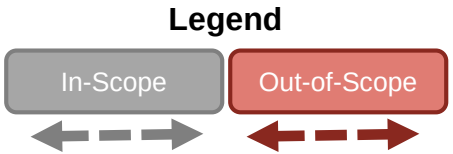
The API design is adapted from the data providers that power the dashboard and other analytics views on the Prolexic Portal.

Basic DOTS Architecture [DOTS-REQUIREMENTS] [DOTS-ARCHITECTURE]

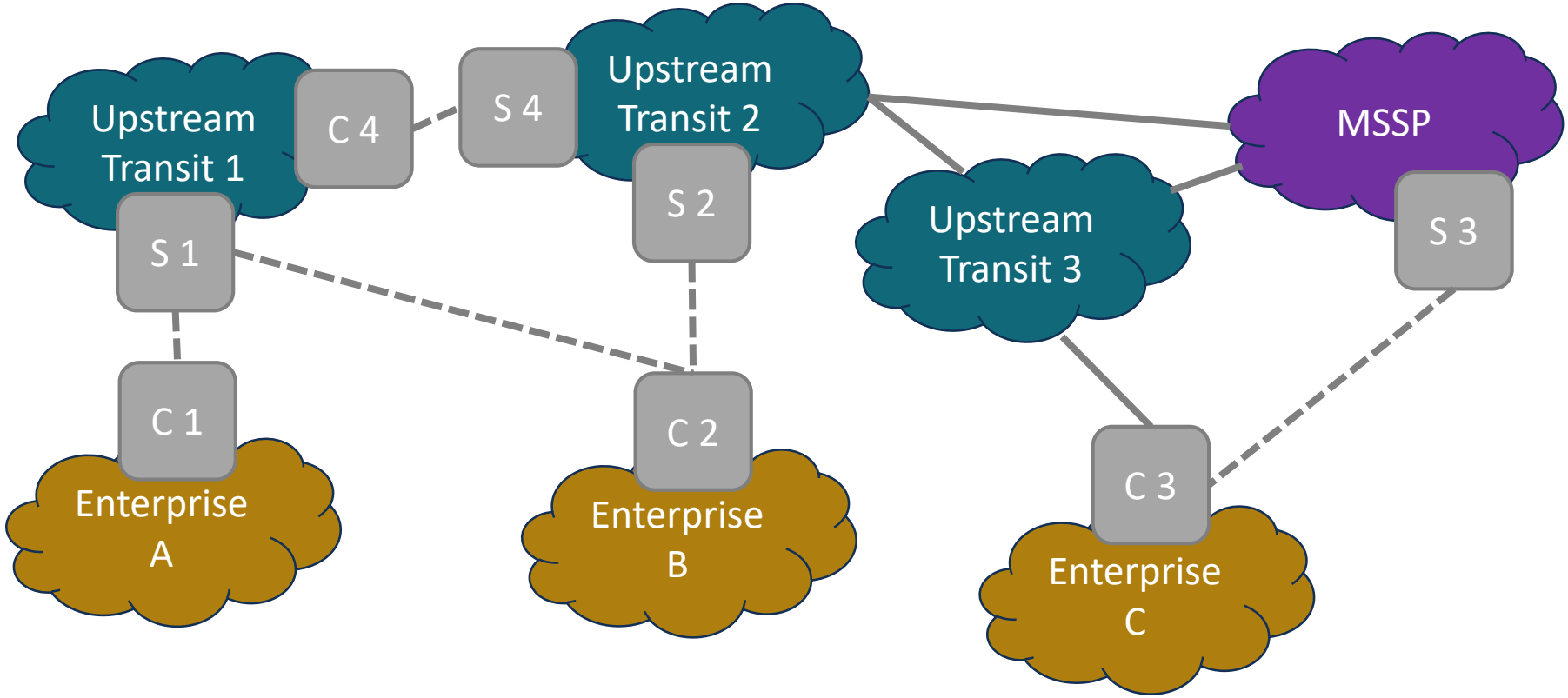


DOTS Gateways chain a Server + Client

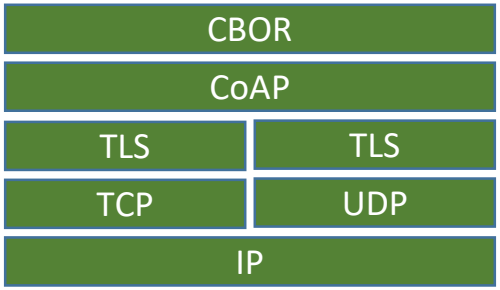
Clients could be a router, layer-3 switch, firewall, IDS/IPS, next-gen firewall, load-balancer, etc.



Select DOTS Use Cases [DOTS-USE-CASES]

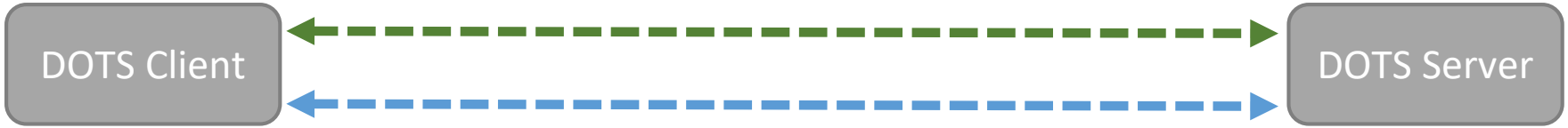


DOTS Protocols



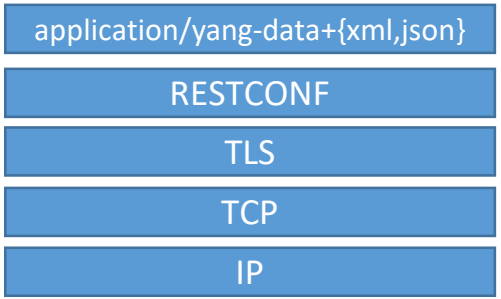
Signal Channel
[DOTS-SIGNAL-CHANNEL]

- Used during attack
- Request mitigation
- Send mitigation status



Data Channel
[DOTS-SIGNAL-CHANNEL]

- Used during “peace-time”
- Sets configurations



References

[API-AKAMAI] Prolexic Analytics API. https://developer.akamai.com/api/luna/prolexic-analytics/overview.html

[API-ARBOR] Arbor SP REST API Cookbook v8.3
https://arbor.github.io/sp-rest-api-cookbook/sp-rest-api-tutorial.html#org307939b

[API-CLOUDFLARE] Cloudflare API documentation v4. https://api.cloudflare.com/

[DOTS-ARCHITECTURE] Distributed-Denial-of-Service Open Threat Signaling (DOTS) Architecture.
https://datatracker.ietf.org/doc/draft-ietf-dots-architecture/

[DOTS-DATA-CHANNEL] Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification.
https://datatracker.ietf.org/doc/draft-ietf-dots-data-channel/

[DOTS-REQUIREMENTS] Distributed Denial of Service (DDoS) Open Threat Signaling Requirements.
https://datatracker.ietf.org/doc/draft-ietf-dots-requirements/

[DOTS-SIGNAL-CHANNEL] Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification.
https://datatracker.ietf.org/doc/draft-ietf-dots-signal-channel/

[DOTS-USE-CASES] Use cases for DDoS Open Threat Signaling.
https://datatracker.ietf.org/doc/draft-ietf-dots-use-cases/

[GITHUB-DDOS] Memcached-fueled 1.3 Tbps attacks.
https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html