



**I E T F**<sup>®</sup>

# DDoS Open Threat Signaling (DOTS) Working Group

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

Roman Danyliw <[rdd@cert.org](mailto:rdd@cert.org)>

IETF DOTS WG Co-Chair

MAMI Management and Measurement Summit (M3S)

March 16, 2018

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

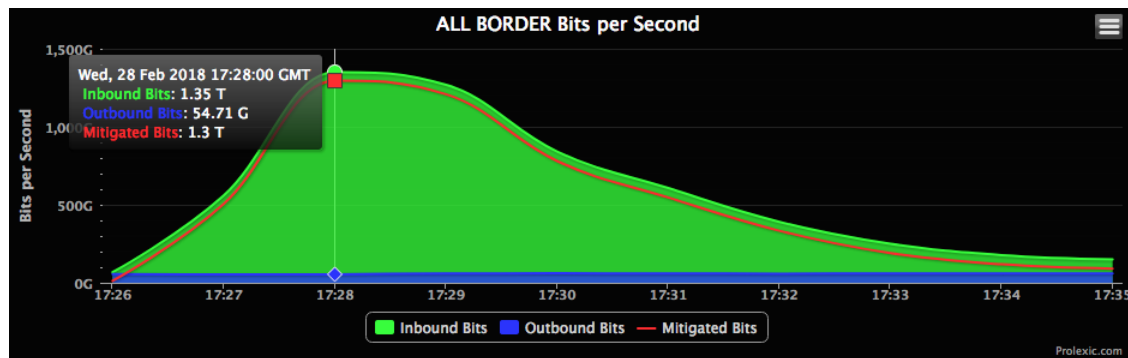
References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

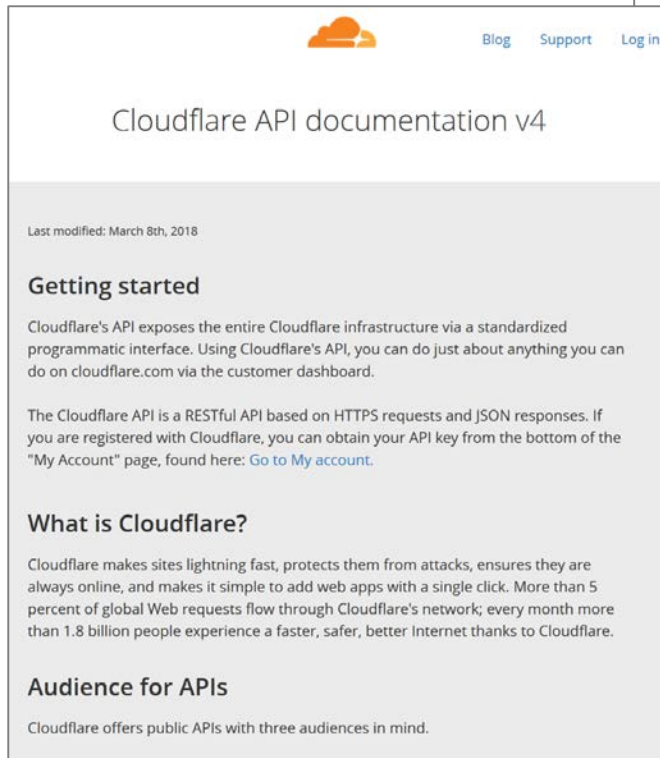
DM18-0364



All logos are copyright of their respective owners

# Per Vendor APIs

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



The screenshot shows the Cloudflare API documentation page for version 4. The page has a white background with a blue header containing the Cloudflare logo and navigation links for 'Blog', 'Support', and 'Log in'. The main heading is 'Cloudflare API documentation v4'. Below this, it says 'Last modified: March 8th, 2018'. The page is divided into sections: 'Getting started', 'What is Cloudflare?', and 'Audience for APIs'. The 'Getting started' section explains that the API exposes the entire Cloudflare infrastructure via a standardized programmatic interface. The 'What is Cloudflare?' section states that Cloudflare makes sites lightning fast, protects them from attacks, and ensures they are always online. The 'Audience for APIs' section mentions that Cloudflare offers public APIs with three audiences in mind.

## 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` contains the source file; the examples in the file show the file's formatting and the link to the Orgmode Guide.

### Contributing

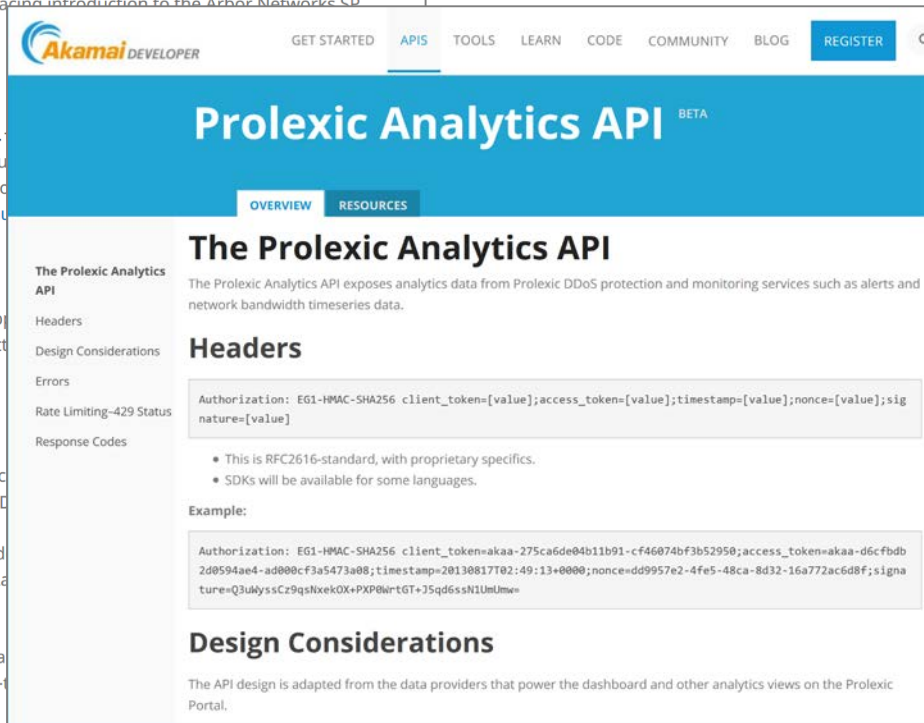
All contributions are greatly appreciated. Please email edits, printed and written comments, or pull requests.

### Rendering

If you want to render this you can use the `orgmode` command to produce HTML, PDF, or other formats.

Exporting from Emacs Orgmode to HTML is simple, then, assuming you have the LaTeX package installed, the commands:

```
pdflatex -shell-escape sp-rest-api-tutorial.orgmode > sp-rest-api-tutorial.html
```



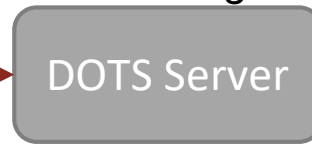
The screenshot shows the Prolexic Analytics API documentation page. The page has a blue header with the Akamai Developer logo and navigation links for 'GET STARTED', 'APIS', 'TOOLS', 'LEARN', 'CODE', 'COMMUNITY', 'BLOG', and a 'REGISTER' button. The main heading is 'Prolexic Analytics API BETA'. Below this, there are tabs for 'OVERVIEW' and 'RESOURCES'. The page is divided into sections: 'The Prolexic Analytics API', 'Headers', and 'Design Considerations'. The 'The Prolexic Analytics API' section explains that the API exposes analytics data from Prolexic DDoS protection and monitoring services. The 'Headers' section shows an example of an authorization header: `Authorization: EG1-HMAC-SHA256 client_token=[value];access_token=[value];timestamp=[value];nonce=[value];signature=[value]`. The 'Design Considerations' section states that 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]

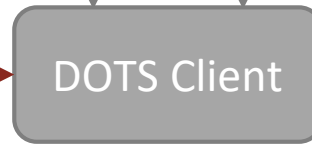
*Implements countermeasures*



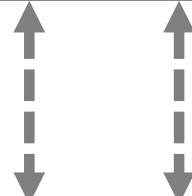
*Enables Mitigation*



*Target of Attack*



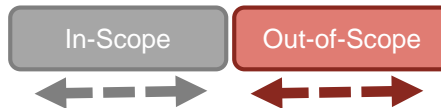
*Requests Mitigation*



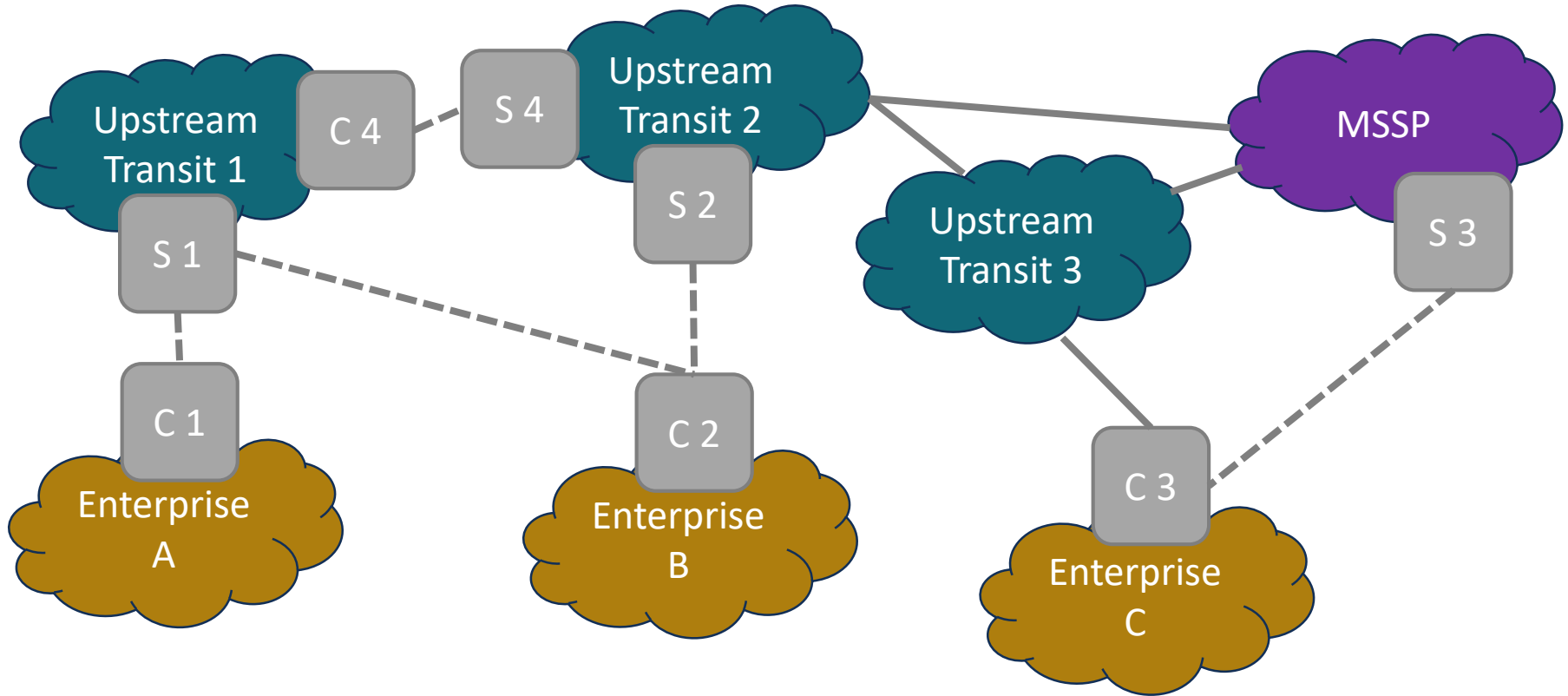
DOTS Gateways chain a Server + Client

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

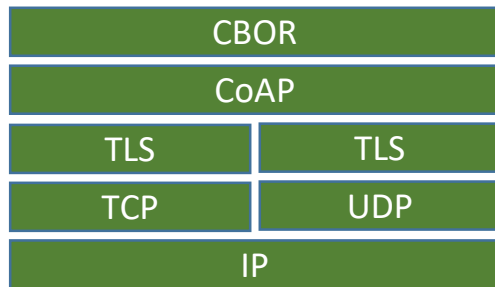
## Legend



# Select DOTS Use Cases [DOTS-USE-CASES]



# DOTS Protocols



## Signal Channel

[DOTS-SIGNAL-CHANNEL]

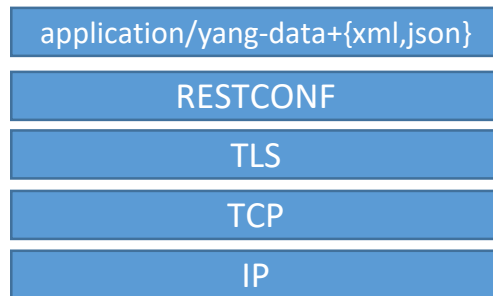
- Used during attack
- Request mitigation
- Send mitigation status



## 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>