DOTS Agent Deployment

draft-chen-dots-server-hierarchical-deployment-03

Interim-2020-DOTS

Meiling Chen /China Mobile
Li Su /China Mobile

Back Ground

- - First presented at IETF105.

- Received some comments

  - how to know the scope of management on the other side in addition to manual configuration?

  - Such as how DOTS Client know the Attack Target belong to which DOTS Servers?

  - how DOTS Server know the Attack Target belong to which DOTS client?

Objective & Contents

- **Objective**

 - Made recommandations for DOTS Agents deployment.

- **Contents(**Modified and added**)**

 - DOTS agents deployment inside an ISP
 - DOTS agents deployment between ISPs
 - DOTS agents deployment between Enterprise and ISP

- DOTS agents deployment inside an ISP

(Changed the description and diagram of the network structure)

(New: Detector could be netflow/ipfix collector, firewall or IDS)

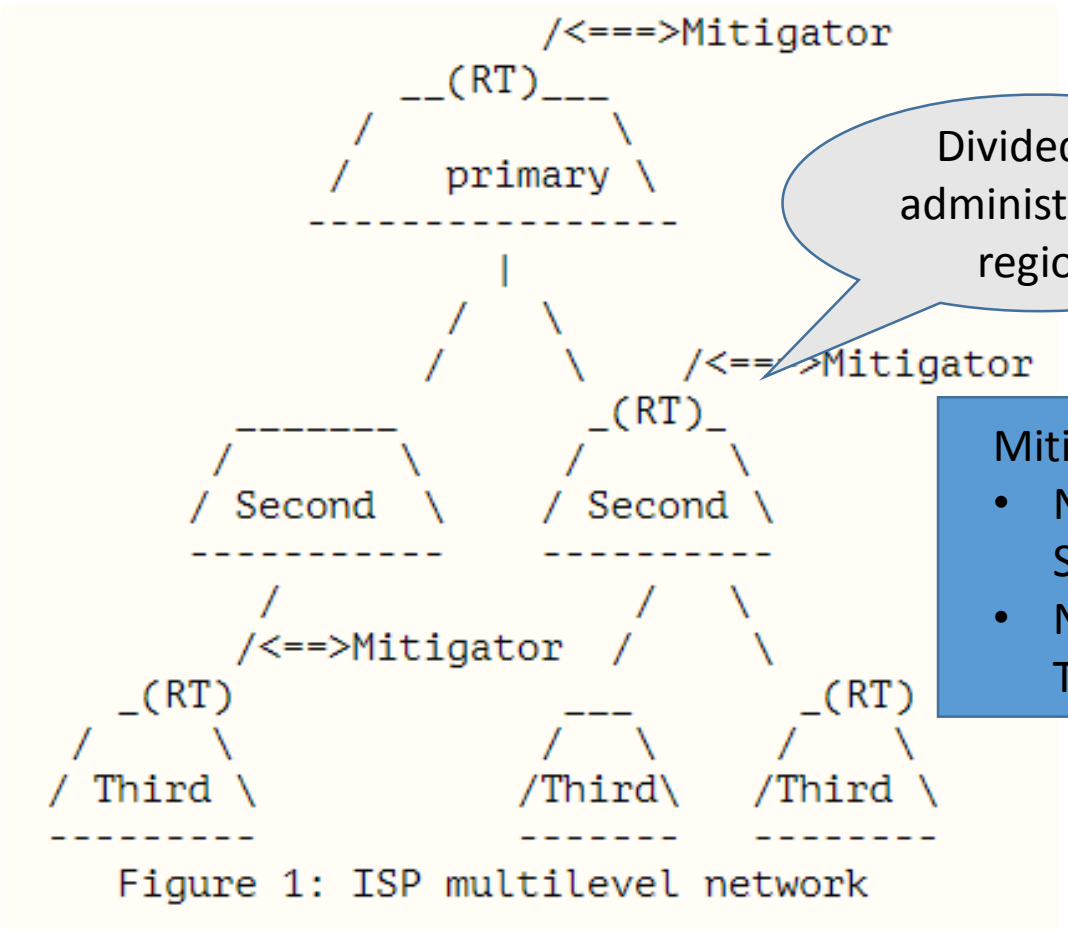

Figure 1: ISP multilevel network

Divided by administrative region

Mitigation Principle:

- Near Attack Source
- Neart Attack Target

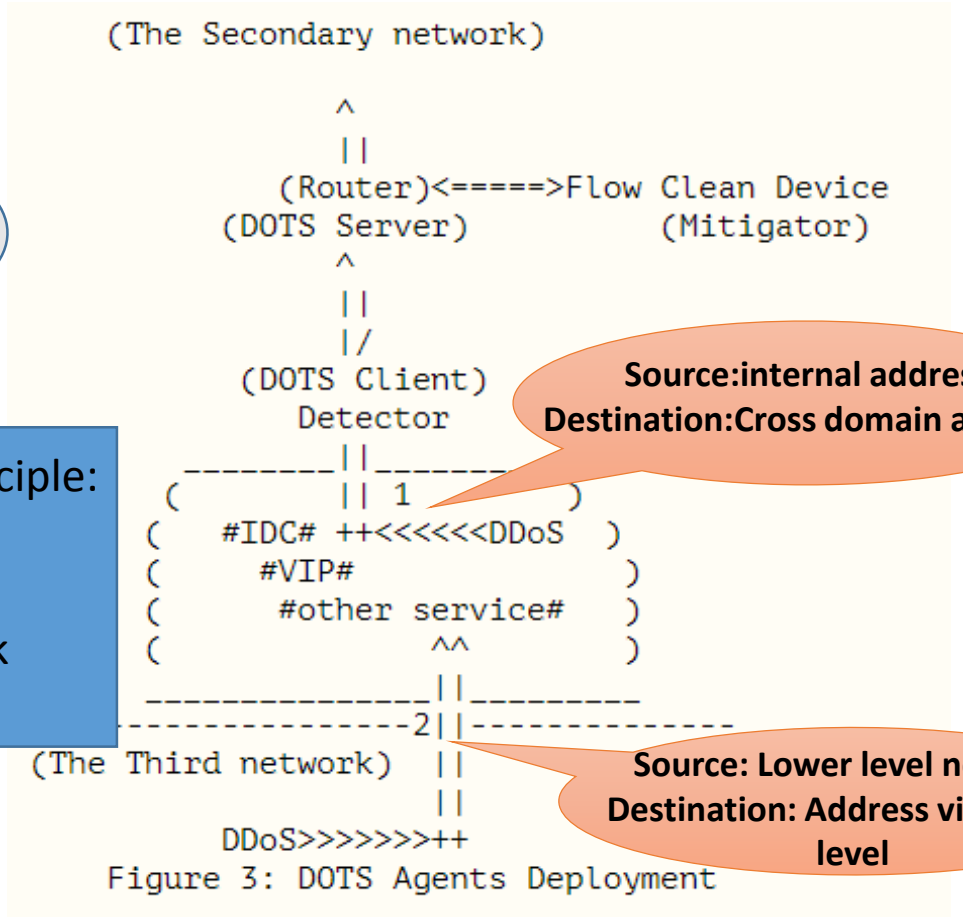

Figure 3: DOTS Agents Deployment

DOTS agents deployment between ISPs (Changes:Decentralize DOTS clients within ISPs)

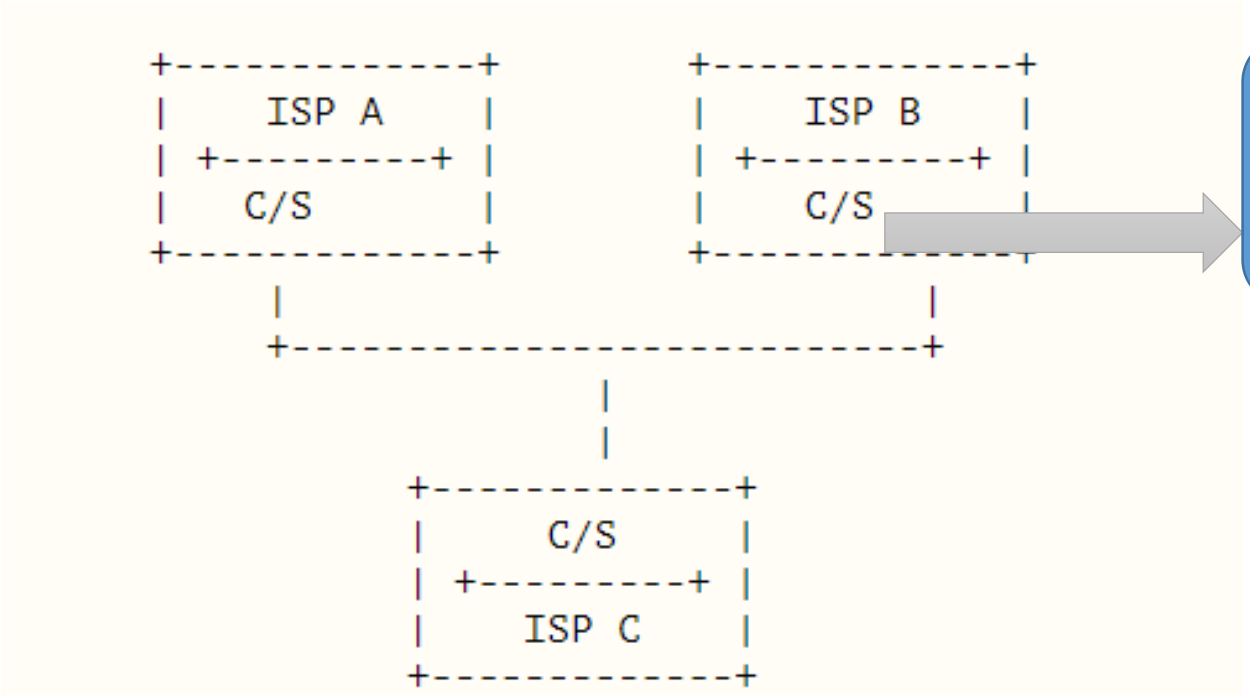

Figure 4: DOTS Agents Deployment between ISPs

C: located with Detector
S:co-located with Key Router

DOTS agents deployment between Enterprise and ISP

(New: Added deployment mode for high defense node)

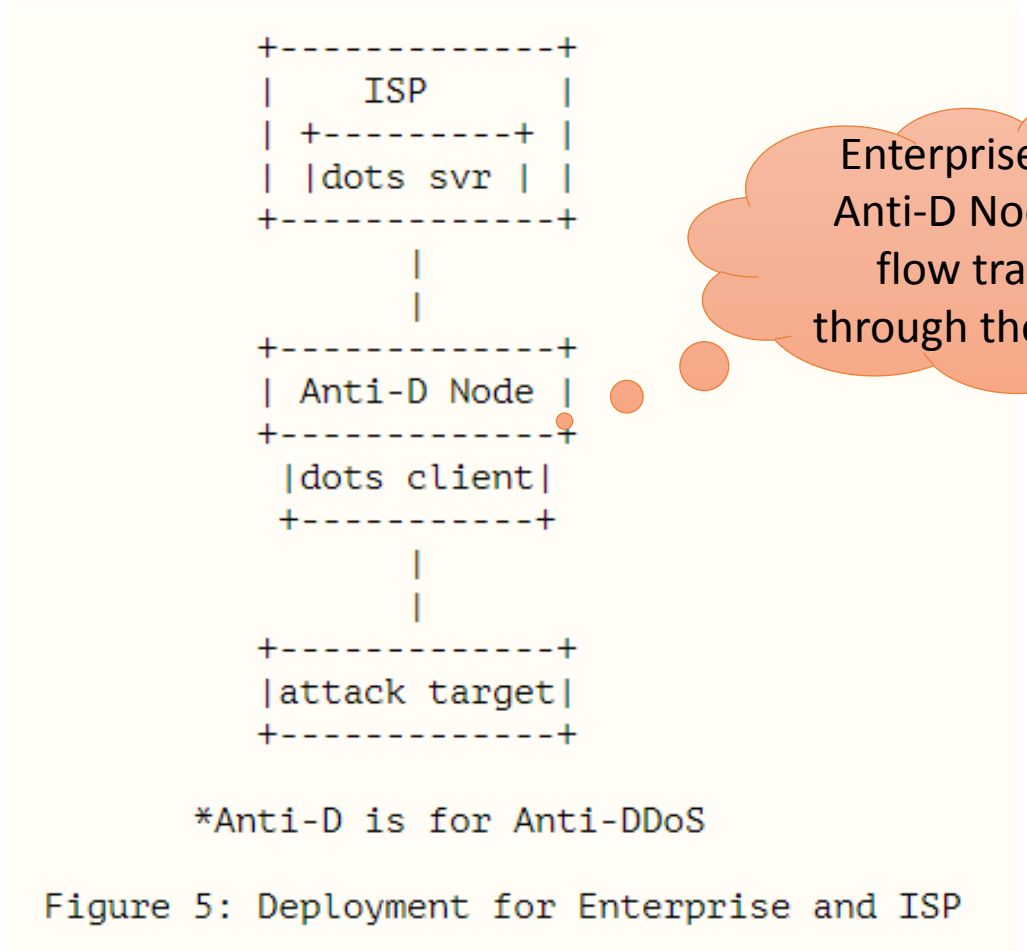

Figure 5: Deployment for Enterprise and ISP

ToDo

- Further describe the deployed nodes in detail
- Solve the problem “know the scope of management on the other side with automatic configuration”

- Addressing comments from WG
  - Comments and co-authors are welcome!

Discussion

Some options on how to move forward with this draft.

Opt 1. Require WG adoption after addressing comments from WG.

Opt 2. ?