DOTS
Internet-Draft
Intended status: Informational
Expires: September 10, 2020

M. Chen
Li. Su
China Mobile

March 9, 2020

A method for dots server deployment
draft-chen-dots-server-hierarchical-deployment-02

Abstract

As DOTS is used for DDoS Mitigation signaling, in practice, there are different deployment scenarios for DOTS agents deployment depending on the network deployment mode. This document made an recommandation for DOTS Server deployment, include ISP and enterprise deployment scenarios. The goal is to provide some guidance for DOTS agents deployment.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 10, 2020.

Table of Contents

1. Introduction 2
2. Terminology 3
3. DOTS server Considerations 3
4. DOTS server deployment inside an ISP 4
4.1. DOTS Agents Deployment 4
4.2. DOTS Agents interfaces 6
4.2.1. Bandwidth consuming attack 7
4.2.2. Host resource consuming attack 7
5. DOTS server deployment between ISPs 8
6. DOTS server deployment for Enterprise 9
7. Security Considerations 9
8. IANA Considerations 9
9. Acknowledgement 10
10. References 10
10.1. Normative References 10
10.2. Informative References 10
Authors' Addresses 11

1. Introduction

DDoS Open Threat Signaling (DOTS) is a protocol to standardize real-time signaling, threat-handling requests[I-D.ietf-dots-signal-channel], when attack target is under attack, dots client send mitigation request to dots server for help, If the mitigation request contains enough messages of the attack, then the mitigator can respond very effectively.

In the architecture draft[I-D.ietf-dots-architecture], when comes to the deployment topic, it says this does not necessarily imply that the attack target and the DOTS client have to be co-located in the same administrative domain, but it is expected to be a common scenario. Although co-location of DOTS server and mitigator within the same domain is expected to be a common deployment model, it is assumed that operators may require alternative models.

In the DOTS server discovery draft[I-D.ietf-dots-server-discovery], it is says that a key point in the deployment of DOTS is the ability of network operators to be able to configure DOTS clients with the correct DOTS server(s) information consistently.

In the DOTS multihoming draft[I-D.ietf-dots-multihoming], it provides deployment recommendations for DOTS client and DOTS gateway, it is says when conveying a mitigation request to protect the attack

target, the DOTS client among the DOTS servers available Must select a DOTS server whose network has assigned the prefixes from which target prefixes and target IP addresses are derived. This implies that id no appropriate DOTS server is found, the DOTS client must not send the mitigation request to any DOTS server. So in this document, we give some dots server deployment consideration as the title suggests we prefer hierarchical deployment.

This is DOTS server deployment guidance for operators, We've written about our experience as an ISP, and we hope that other scenarios will contribute as well.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

The readers should be familiar with the terms defined in [I-D.ietf-dots-requirements] [I-D.ietf-dots-use-cases]

The terminology related to YANG data modules is defined in [RFC7950]

In addition, this document uses the terms defined below:

dots svr: abbreviation of dots server.

ISP: Internet service provider.

Orchestrator: With the function of DOTS server that can receive messages from clients and made decisions for mitigators selection.

netflow/ipfix collector: Flow collector used for DDoS attack detection.

3. DOTS server Considerations

When take dots server deployment into consideration, one thing must be involved is mitigator. So far, how many network devices can play the role of mitigator, we make a summerized list as follows:

- Router.
- Special cleaning equipment, such as flow clean device and clean center.
- Network security equipment, such as firewall, IPS and WAF.

- Servers that websites can hidden behind them.

Whether DOTS server can be deployed, the following conditions need to be met:

- DOTS server and mitigator are in the same administrative domain.
- DOTS server can go directly to the mitigator which had best go through without any other DOTS agents.
- DOTS server has the permissions for scheduling on mitigators.
- DOTS server has the ability to know the address of attack target belong to which mitigator, if DOTS server hasn't matched attack target to mitigators, DOTS server need to configure default mitigators.

4. DOTS server deployment inside an ISP

4.1. DOTS Agents Deployment

From the internal structure of ISP, the whole network can divide into backbone and metropolitan area networks logically. There are two most important routers: backbone router, man(metropolitan area network) router. It's worth noting that there are usually Internet Data Centers(IDC), high bandwidth demand customers(such as online game companies) and VIP customer centers(such as financial clients) distributed in metropolitan area networks. When a ddos attack occurs, it must be one of the three cases as follows, and the corresponding mitigator will responsible for mitigation.

- DDoS attacks occur inside the LAN or the attack source inside metropolitan area network launched an attack against the target in local area network, the lan network detected the attack, dots server3 will receive mitigation request, and mitigator3 will act as the first responsible mitigator.
- DDoS attacks occur inside the MAN or the attack source inside backbone network launched an attack against the target in metropolitan area network, the man network detected the attack, dots server2 will receive mitigation request, then mitigator2 will act as the first responsible mitigator.
- DDoS attacks from other ISPs, the backbone network detected the attack, dots server1 will receive mitigation request, then mitigator1 will act as the first responsible mitigator.

If attacks on the same attack target are found both in adjacent areas, there are two strategies for the mitigators' selection, then found the best mitigation node for different scenes.

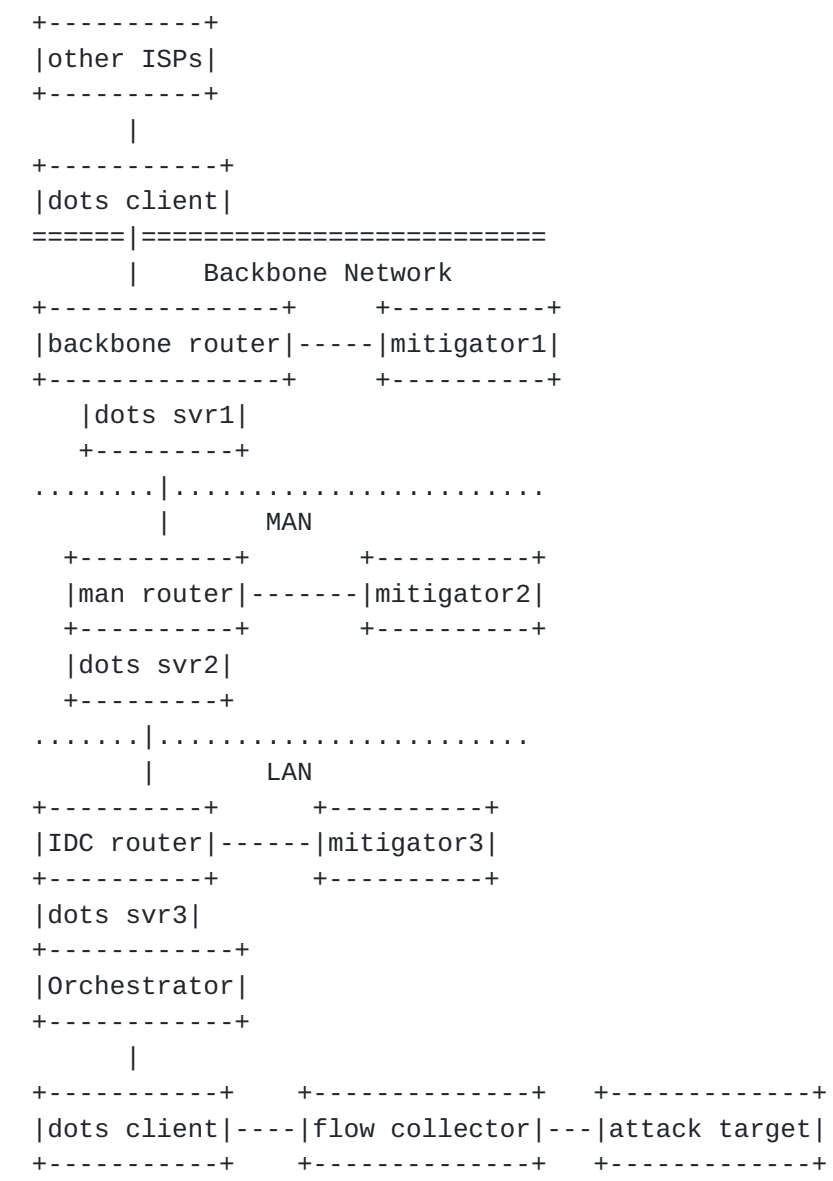
- Near Attack Source Mitigation(NASM), NASM means that the mitigation is performed closest to the source of the attack, this usually happens at the entrance to the edge of the network. This approach can block attack flow at the source and protect network bandwidth maximumly, but requires the ability to operate the entire network. This principle is more suitable for large-traffic attack mitigation.

- Near Attack Target Mitigation(NATM), NATM means that the mitigation is performed closest to the attack target, This is the easiest and most direct way, but it will cause the attack flow long-distance transmission, occupy the bandwidth along the link, more likely to cause link congestion. This principle is more suitable for low-traffic attack mitigation.

According to the NATM, the lower network mitigator will act as the first responsible mitigator. for example, dots server1 and dots server2 both received the mitigation request from attack target by dots client, mitigator2 will responsible for ddos disposition(priority ranking: mitigator3, mitigator2, mitigator1), but according to the NASM the priority will be reverse.

Normally, The lower network the target in, the easier it is to alert. Because the higher network the attack target in, the greater the bandwidth of the pipeline. As shown in the following figure, Orchestrator take on the role for scheduling. Because the importance of the orchestrator, it is suggested to consider bakeup mechanisms or heartbeat technology to ensure continuity and security.

How does DOTS client can find DOTS servers, we can reference the DOTS server discovery draft[I-D.ietf-dots-server-discovery], Static configuration or dynamic discovery depends on the actual scenario and the size of the network.



*MAN is for metropolitan area network
*LAN is for local area network
*flow collector is for netflow/ipfix collector

Figure 1: hierarchical deployment for DOTS servers

4.2. DOTS Agents interfaces

In the dots use case draft[I-D.ietf-dots-use-cases], it is says the orchestrator analyses the various information it receives from DDoS telemetry system, and initiates one or multiple DDoS mitigation strategies. In the telemetry draft, all the telemetry informations are contained and some parameters can be used to make decisions.

This section made a discussion on which attributes could be used in orchestrator for scheduling.

We suggest orchestrator has three capabilities and reuse the method of registration and notification in signal channel to know all the related mitigators capability and residue capability:

1.Can get the neflow/ipfix collector's telemetry informations.

2.Can get the capabilities of each mitigator, it means the initial capacity, this means that with each addition of mitigator there needs to be a protocol that can push this information to orchestrator, we recommend using DOTS signal channel to transfer initial capacity.

3.When mitigation finished, mitigator can inform orchestrator that mitigation is finished and capacity has been released, also we recommend using DOTS signal channel to transfer.

4.2.1. Bandwidth consuming attack

The following parameters will be required by orchestrator:

- top-talker
- source-prefix
- total-traffic
- total-attack-traffic
- total-pipe-capability

The recommended approach here is to redirect traffic and flow cleaning.

4.2.2. Host resource consuming attack

The following parameters will be required by orchestrator:

- top-talker
- source-prefix

The recommended approach here is to use router for disposition.

5. DOTS server deployment between ISPs

Because of global connectivity, the coexistence of different operators is very common, coordination between operators across networks is very important. Interdomain attacks occur frequently, We recommend deploying the DOTS server at the access point.

- DDoS attack from one of other ISPs, for example, ISP A received DDoS attack from ISP B or ISP C, then dots server C or dots server B will receive the mitigation request.

- DDoS attacks from two or more of other ISPs,for example, ISP A and ISP B both start ddos attack to ISP C, then dots server A and dots server B will both receive mitigation request from dots client C.

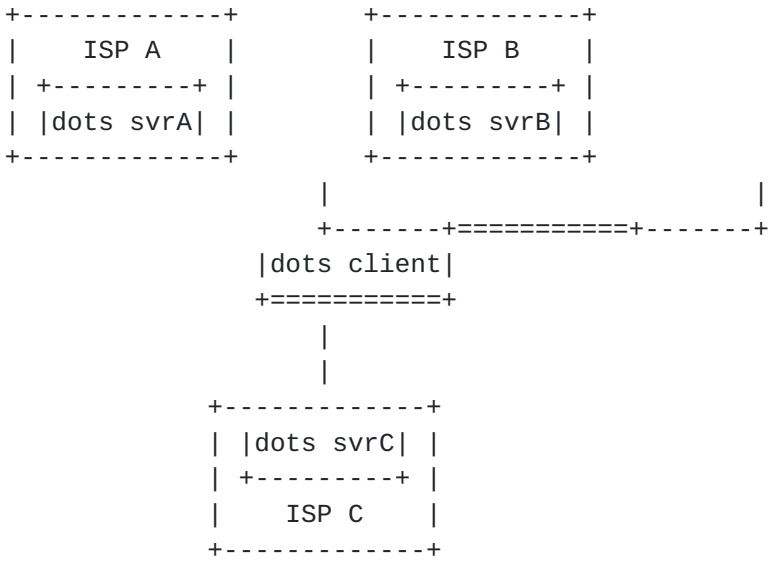
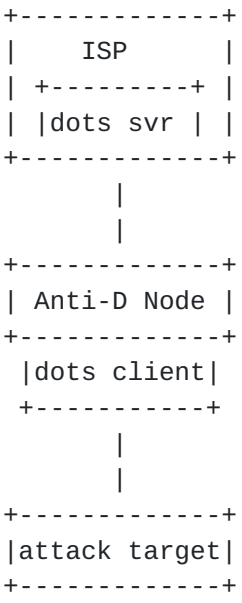


Figure 2: DOTS Server Deployment between different ISPs

It is obvious from the figure 2 that there is a super DOTS client in the middle, this also means that there will be corresponding netflow/ipfix collector on the link between different ISPs, the final location of the DOTS client according to the actual network topology. When an DDoS attack occurs, depending on the direction of the attack, the corresponding server is required for mitigation, DOTS server can use call home to find the source of the DDoS attacks[I-D.ietf-dots-signal-call-home]

6. DOTS server deployment for Enterprise

In addition to operators taking advantage of the pipeline to make a contribution to DDoS attack mitigation, there are also enterprise-level DDoS attack mitigation solutions. It's usually a cloud service and a large number of distributed nodes are deployed to protect their customers from DDoS attack, customers' websites can be hidden behind the nodes, usually the internet game companies and the live streaming company will choose this way.



*Anti-D is for Anti-DDoS

Figure 3: DOTS Server Deployment for Enterprise and ISP

When enterprise-level anti-DDos nodes are unable to mitigate the DDoS attack, they can trigger DOTS client which integrated in the Anti-D Node to send mitigation request to ISP's DOTS server.

7. Security Considerations

TBD

8. IANA Considerations

TBD

9. Acknowledgement

TBD

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

10.2. Informative References

[I-D.ietf-dots-architecture]
Mortensen, A., Reddy.K, T., Andreasen, F., Teague, N., and R. Compton, "Distributed-Denial-of-Service Open Threat Signaling (DOTS) Architecture", draft-ietf-dots-architecture-15 (work in progress), March 2020.

[I-D.ietf-dots-multihoming]
Boucadair, M., Reddy.K, T., and W. Pan, "Multi-homing Deployment Considerations for Distributed-Denial-of-Service Open Threat Signaling (DOTS)", draft-ietf-dots-multihoming-03 (work in progress), January 2020.

[I-D.ietf-dots-requirements]
Mortensen, A., K, R., and R. Moskowitz, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-22 (work in progress), March 2019.

[I-D.ietf-dots-server-discovery]
Boucadair, M. and T. Reddy.K, "Distributed-Denial-of-Service Open Threat Signaling (DOTS) Agent Discovery", draft-ietf-dots-server-discovery-10 (work in progress), February 2020.

[I-D.ietf-dots-signal-call-home]
Reddy.K, T., Boucadair, M., and J. Shallow, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home", draft-ietf-dots-signal-call-home-07 (work in progress), November 2019.

[I-D.ietf-dots-signal-channel]
Reddy.K, T., Boucadair, M., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", draft-ietf-dots-signal-channel-41 (work in progress), January 2020.

[I-D.ietf-dots-use-cases]
Dobbins, R., Migault, D., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", draft-ietf-dots-use-cases-20 (work in progress), September 2019.

Authors' Addresses

Meiling Chen
China Mobile

32, Xuanwumen West

BeiJing
,
BeiJing

100053

China

Email:
chenmeiling@chinamobile.com

Li Su
China Mobile

32, Xuanwumen West

BeiJing

100053

China

Email:
suli@chinamobile.com