DOTS
Internet-Draft
Intended status: Informational
Expires: September 9, 2019

Y. Hayashi, Ed.
NTT
K. Nishizuka, Ed.
NTT Communications
M. Boucadair, Ed.
Orange

March 8, 2019

DDoS Mitigation Offload: A DOTS Applicability Use Case
draft-hayashi-dots-dms-offload-usecase-00

Abstract

This document describes the applicability of DOTS to a DDoS mitigation offload use case. This use case assumes that a DMS (DDoS Mitigation System) whose utilization rate is high sends its blocked traffic information to an orchestrator using DOTS protocols, then the orchestrator requests forwarding nodes such as routers to filter the traffic. Doing so enables service providers to mitigate DDoS attack traffic automatically while ensuring interoperability and distributed filter enforcement.

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 9, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Volume-based distributed denial-of-service (DDoS) attacks such as DNS amplification attacks are critical threats to be handled by service providers. When such attacks occur, service providers have to mitigate them immediately to protect or recover their services.

Therefore, for the service providers to immediately protect their network services from DDoS attacks, DDoS mitigation needs to be automated. To automate DDoS attack mitigation, it is desirable that multi-vendor elements involved in DDoS attack detection and mitigation collaborate and support standard interfaces to communicate.

DDoS Open Threat Signaling (DOTS) is a set of protocols for real-time signaling, threat-handling requests, and data between the multi-vendor elements [I-D.ietf-dots-signal-channel] [I-D.ietf-dots-data-channel]. This document describes an automated DDoS Mitigation offload use case inherited from the DDoS orchestration use case [I-D.ietf-dots-use-cases], which ambitions to enable cost-effective DDoS Mitigation.

2. Terminology

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

In addition, this document uses the terms defined below:

Mitigation offload: Getting rid of a DMS's mitigation action and assigning the action to another entity when the utilization rate of the DMS reaches a given threshold. How such threshold is set is deployment-specific.

Utilization rate: A scale to measure load of an entity such as link utilization rate or CPU utilization rate.

3. The Problem

In general, DDoS countermeasures are divided into detection and filtering, and detection is technically difficult. DDoS Mitigation System (DMS) can detect attack traffic based on the technology of their vendors, so service providers can increase DDoS countermeasure level by deploying the DMS in their network.

However, the number/capacity of DMS instances that can be deployed in a service providers network is limited due to equipment cost and dimensioning matters. Thus, DMS's utilization rate can reach its maximum capacity faster when the volume of DDoS attacks is enormous. When the rate reaches maximum capacity, the mitigation strategy needs to offload mitigation actions from the DMS to cost-effective forwarding nodes such as routers.

4. DOTS Applicability to DDoS Mitigation Offload Use Case

This section does not consider deployments where the network orchestrator and DMS are co-located.

4.1. Component and Sequence Diagram

Figures 1 and 2 show a component diagram and a sequence diagram of the use case, respectively.

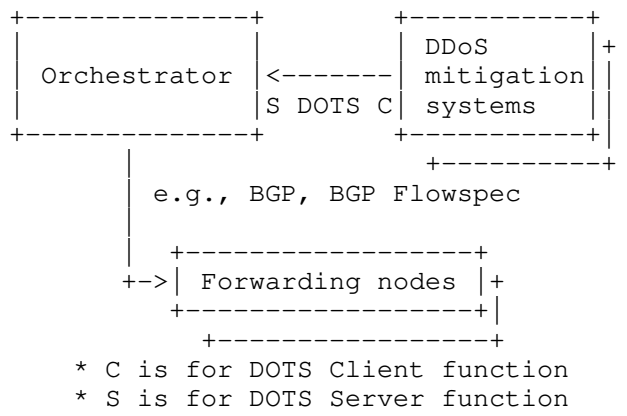

Figure 1: Component Diagram of DDoS Mitigation Offload Use Case

The component diagram shown in Figure 1 differs from that of DDoS Orchestration usecase in [I-D.ietf-dots-use-cases] in some respects. First, the DMS embeds a DOTS client to send DOTS requests to the orchestrator. Second, the orchestrator sends a request to underlying forwarding nodes to filter the attack traffic.

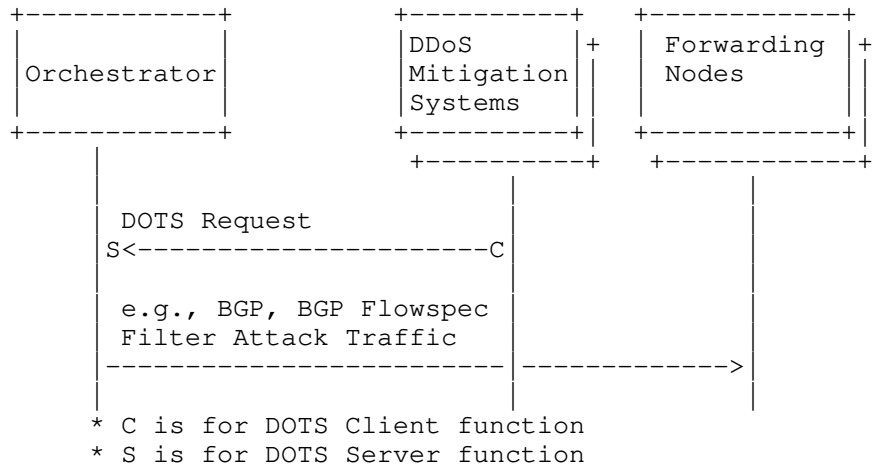

Figure 2: Sequence Diagram of DDoS Mitigation Offload Use Case

In this use case, it is assumed that volume based attack already hits a network and attack traffic is detected and blocked by a DMS in the network. When the volume-based attack becomes intense, DMS's

utilization rate can reach a certain threshold (e.g., maximum capacity). Then, the DMS sends a DOTS request as offload request to the orchestrator with the actions to enforce on the traffic. After that, the orchestrator requests the forwarding nodes to filter attack traffic by dissemination of flow specification rules protocols such as BGP Flowspec [RFC5575] on the basis of the blocked traffic information.

This use case is divided into two cases as discussed below. One is that the DMS sends DOTS requests to the orchestrator via out-of-band link, and the other one is that the DMS sends it via in-band link.

4.2. Case: DOTS Request via Out-of-band Link

In this case, the DMS sends a DOTS request to the orchestrator with information of blocked traffic information by the DMS via out-of-band link. The link is not congested when it is under volume attack-time, so DOTS data channel [I-D.ietf-dots-data-channel] is suitable because DOTS data channel has capability of conveying the drop-listed filtering rules (and other actions such as 'rate-limit'). The applicability of DOTS in such case is as follows:

- The DMS generates a list of flow tuples (e.g., 5-tuples) which the DMS is blocking/rate-limiting and wants to offload.
- The DMS creates ACEs for each elements of the list, setting "matches" as the flow tuple and "forwarding" in "actions" as "drop" (or other actions).
- The DMS aggregates the ACEs under an ACL set, and the DMS sends the ACL to the orchestrator setting "activation-type" as "immediate".

Figure 3 shows a JSON example of ACL conveyed by DOTS data channel.

```
{
  "ietf-dots-data-channel:acls": {
    "acl": [
      {
        "name": "DMS_Offload_Usecase_ACL",
        "type": "ipv4-acl-type",
        "activation-type": "immediate",
        "aces": {
          "ace": [
            {
              "name": "DMS_Offload_Usecase_ACE_00",
              "matches": {
                "ipv4": {
                  "destination-ipv4-network": "192.0.2.2/32",
                  "source-ipv4-network": "203.0.113.2/32",
                  "protocol":17
                },
                "udp": {
                  "source-port": {
                    "operator": "eq",
                    "port": 53
                  }
                }
              },
              "actions": {
                "forwarding": "drop"
              }
            }
          ]
        }
      }
    ]
  }
}
```

Figure 3: JSON Example of ACL conveyed by DOTS data channel

4.3. Case: Mitigation Request via In-band Link

In this case, the DMS sends a mitigation request to the orchestrator with information of blocked traffic by the DMS via in-band channel. The link can be congested when it is under volume attack-time, so DOTS data channel can't be used to convey the drop-listed filtering rules as blocked traffic information [Interop].

The DOTS signal channel and [I-D.ietf-dots-signal-channel] and the source-* clauses defined in [I-D.reddy-dots-home-network] are used to communicate the policies to the orchestrator.

<<<An example will be included>>>>

5. Security Considerations

Security considerations discussed in [I-D.ietf-dots-data-channel] and [I-D.ietf-dots-signal-channel] are to be taken into account.

6. IANA Considerations

This document does not require any action from IANA.

7. Acknowledgement

Thanks to Tirumaleswar Reddy, Shunsuke Homma for the comments.
Thanks to Koichi Sakurada for demonstrating proof of concepts of this use case.

8. References

8.1. Normative References

[I-D.ietf-dots-data-channel]
Boucadair, M. and R. K, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", draft-ietf-dots-data-channel-27 (work in progress), February 2019.

[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-20 (work in progress), February 2019.

[I-D.ietf-dots-signal-channel]
K, R., 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-30 (work in progress), March 2019.

[I-D.ietf-dots-use-cases]
Dobbins, R., Migault, D., Fouant, S., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", draft-ietf-dots-use-cases-17 (work in progress), January 2019.

8.2. Informative References

[I-D.nishizuka-dots-signal-control-filtering]
Nishizuka, K., Boucadair, M., K, R., and T. Nagata, "Controlling Filtering Rules Using DOTS Signal Channel", draft-nishizuka-dots-signal-control-filtering-04 (work in progress), February 2019.

[I-D.reddy-dots-home-network]
K, R., Harsha, J., Boucadair, M., and J. Shallow, "Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home", draft-reddy-dots-home-network-03 (work in progress), December 2018.

[Interop] Nishizuka, K., Shallow, J., and L. Xia , "DOTS Interop test report, IETF 103 Hackathon", November 2018, <https://datatracker.ietf.org/meeting/103/materials/slides-103-dots-interop-report-from-ietf-103-hackathon-00>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <https://www.rfc-editor.org/info/rfc5575>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

Authors' Addresses

Yuhei Hayashi (editor)
NTT
3-9-11, Midori-cho
Musashino-shi, Tokyo 180-8585
Japan

Email: yuuhei.hayashi@gmail.com, yuuhei.hayashi.mr@hco.ntt.co.jp

Kaname Nishizuka (editor)
NTT Communications
GranPark 16F 3-4-1 Shibaura, Minato-ku
Tokyo 108-8118
Japan

Email: kaname@nttv6.jp

Mohamed Boucadair (editor)
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com