DOTS
Internet-Draft
Intended status: Informational
Expires: September 12, 2019

M. Chen
Li. Su
Jin. Peng
CMCC

March 11, 2019

Using attack bandwidth in signal channel draft-chen-dots-attack-bandwidth-expansion-01

Abstract

This document describes a DDoS Mitigation Request parameter used in the Signal Channel request, as an expansion of the signal channel for mitigating DDoS attack accurately with target-bandwidth. The proposed parameter will help to choose the appropriate mitigator or mitigators for mitigation, When An attack occurs that is greater than the maximum clean capability, this paramter can decide to be blackhole directly or to be drainaged for clean.

Table of Contents

1. Introduction

Distributed Denial of Service (DDoS) is a type of resource-consuming attack, which exploits a large number of attack resources and uses standard protocols to attack target objects. DDoS attacks consume a large amount of target object network resources or server resources (including computing power, storage capacity, etc.) of the target object, so that the target object cannot provide network services normally. At present, DDoS attack is one of the most powerful and indefensible attacks on the Internet, and due to the extensive use of mobile devices and IoT devices in recent years, it is easier for DDoS attackers to attack with real attack sources (broilers).

Volume based distributed denial-of-service attack bring huge amount of attack traffic on the link, and the peaks keep hitting new highs, the economic loss that causes is bigger also. For the service providers to immediately protect their network services from DDoS attacks, DDoS mitigation needs to be automated.

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.

Currently, there are two selections to deal with ddos attacks on the link, one is blackhole, the other is flow clean. Blackhole means that all packets send to the attack target will be discarded by routers on the path, this way can instantly reduce the link load, Other managed services on this link will not be affected, but for the attack target all the normal business messages will be severely damaged, for example, if the attack target provide News and information services and under ddos attack, all users will be inaccessible if the attack target choose blackhole for mitigation. Flow clean means that all the flow will be drainaged by routers to clean center, the clean center will recognize the attack flow from normal business traffic, then reinjects normal business traffic to network link by routers after the operation of attack flow discard, in this way the attack target will not be effected.

Currently, mitigator usually has the ability to cluster cleaning equipment and manage a large number of cleaning equipment. Increasing the attack-bandwidth is also very convenient for the scheduling of cleaning equipment, so it can match to find the most suitable cleaning equipment and improve the usage rate of cleaning equipment. Mitigator can also be companies who provide flow cleaning service, they rent the bandwidth from Upstream Service Provider themselves, so they are very careful with their link bandwidth usage. Another scenario is that the link of attack warning is inconsistent with the link of actual traffic drainage, so increasing the parameter of attack-bandwidth is conducive to selecting the BGP path of drainage.

This document describes attack-bandwidth, as a parameter expansion used in the mitigation request. attack-bandwidth means the amount of traffic under attack, this parameter can effectively reflect the degree of an attack, it will be more convenient for mitigator to dispose attack flow when carry target-bandwidth in the mitigation request.

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:

Attack-bandwidth: the amount of traffic under attack, it is usually expressed numerically.

Flow clean: one selection of Attack traffic deposition, the operation contains recognize, discard and reinage.

3. Mitigation Use Case

3.1. directly discard attack flow

when attack target is under attack, it has to make corresponding disposal, there are two options for disposal, one is blackhole directly, in this way all the attack flow will be discarded by router upper path of attack target, this means that the attack target will not receive any traffic during the attack, all the traffic forwards attack target will be discarded, this has a huge impact on the work environment, especially the host that provide external service.

The other way of the disposition is to drainage all the traffic flow to clean center from router, then the clean center will use pattern matching or any other method to find out the attack traffic flow to discard, finally, clean center reinage the normal business traffic back to attack target by upper router, the whole process above is defined as flow clean(Figure 1).

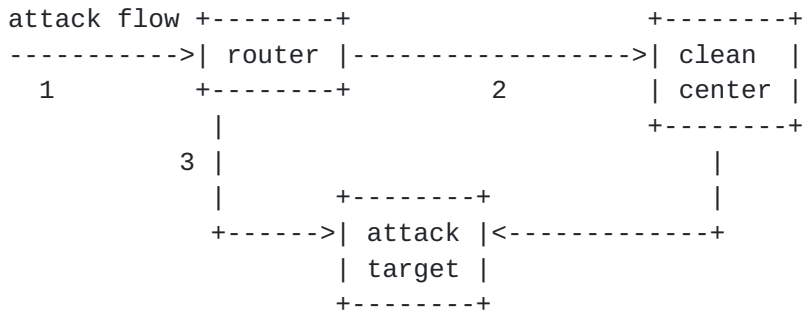

Figure 1: diagram of DDoS Mitigation usecase

Generally, the bandwidth of the link 1 must be larger than link 2 and link 3, and the clean ability of clean center limited to hardware resources. An example of link situation is as below(Figure 2):

figure tag	bandwidth/ capability
link 1	100Gb
link 2	50Gb
link 3	10Gb
clean center	80Gb

Figure 2: an example of link bandwidth

The Figure2 is a scenario of the link bandwidth, when a ddos attack is ongoing, if the link 1 bandwidth is completely jammed, the best way to mitigate the attack is to discard all the attack flow; if the amount of the traffic flow is lower than the remainder cleaning ability, the most suitable deposition is to drainage all the attack flow to clean center.

Therefore, it is an obvious requirement in the current network environment. In the architecture of DOTS, Dots client send mitigation request to dots server, the parameters in the mitigation request contains some message of attack target, but there have not any messages of attack, if add attack-bandwidth to mitigation request as an expansion, it will be more effective and convenient for the disposition of mitigator.

3.2. Optimal device selection

Mitigator may owns a cleaning device cluster and can manage cleaning devices.The capacity of each cleaning equipment is not the same, usually each cleaning equipment utilization rate is not the same, then the remaining cleaning capacity is not consistent.When the attack flow is less than the ability of a cleaning equipment, according to the attack-bandwidth can choose a suitable cleaning equipment,that is conducive to the utilization of equipment;When the attack flow is larger than the cleaning capacity of one cleaning device, several cleaning devices can be optimally scheduled according to the attack-bandwidth.

3.3. Optimum path for disposal

When mitigator is an attack flow cleaning service, they typically deployed the mitigator in a distributed way because of the cost of bandwidth usage with their own leased operator's link bandwidth, and choosing the best traction path was the key to profitability.If the

parameter of attack-bandwidth is carried, then the generation of the best drainage path is very meaningful.

When mitigator is at the upstream service operator level, they might have multiple networks, with the attack alert using one network and the flow drainage using another, and the link load is not the same, then carrying the attack-bandwidth is very beneficial for choosing the drainage path, mainly for link load balancing.

4. Request Mitigation expansion

When a DOTS client requires mitigation for some reason, the DOTS client uses the CoAP PUT method to send a mitigation request to its DOTS server(s). If a DOTS client is entitled to solicit the DOTS service, the DOTS server enables mitigation on behalf of the DOTS client by communicating the DOTS client's request to a mitigator (which may be colocated with the DOTS server) and relaying the feedback of the thus-selected mitigator to the requesting DOTS client.

DOTS clients use the PUT method to request mitigation from a DOTS server. During active mitigation, DOTS clients may use PUT requests to carry mitigation efficacy updates to the DOTS server.

The new parameter in the CBOR body (Figure 3) is described below:

```
 Content-Format: "application/dots+cbor"
                 {
                 "ietf-dots-signal-channel:mitigation-scope": {
                   "scope": [
                     {
                       "target-prefix": [
                          "string"
                        ],
                       "target-port-range": [
                          {
                            "lower-port": number,
                            "upper-port": number
                          }
                        ],
                        "target-protocol": [
                          number
                        ],
                        "target-fqdn": [
                          "string"
                        ],
                        "attack-bandwidth":[
                         "string"
                         ],
                        "target-uri": [
                          "string"
                        ],
                        "alias-name": [
                          "string"
                        ],
                       "lifetime": number,
                       "trigger-mitigation": true|false
                     }
                   ]
                 }
  }
```

Figure 3: PUT to Convey DOTS Mitigation Requests

attack-bandwidth: bandwidth occupied by an attack, The recommended format is numerical form, such as xxGb. Different attack has different attack bandwidth, numerical value directly reflects the urgency of the current attack. Serious attacks are treated with blackhole, Other cases use flow cleaning, attack-bandwidth is conducive to the selection of disposal mode.

This is an optional attribute.

The definition of the rest parameters are the same as the [I-D.ietf-dots-signal-channel]

5. Security Considerations

TBD

6. IANA Considerations

TBD

7. Acknowledgement

TBD

8. References

8.1. 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>.

8.2. Informative References

[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.

Authors' Addresses

Meiling Chen
CMCC
32, Xuanwumen West
BeiJing , BeiJing 100053
China

Email: chenmeiling@chinamobile.com

Li Su
CMCC
32, Xuanwumen West
BeiJing 100053
China

Email: suli@chinamobile.com

Jin Peng
CMCC
32, Xuanwumen West
BeiJing 100053
China

Email: pengjin@chinamobile.com