INTERNET-DRAFT
Intended Status: Standards Track
Expires: April 21, 2016

Luyuan Fang
Deepak Bansal
Microsoft

October 19, 2015

Inter-Cloud DDoS Mitigation API
draft-fang-i2nsf-inter-cloud-ddos-mitigation-api-00

Abstract

This document defines an Inter-Cloud DDoS Mitigation Abstract Layer and corresponding standardized APIs to enable the exchange of real time automated information to enable DDoS mitigation across Cloud Service Providers and Network Service Providers.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Terminology 3
2. Problem Statement 4
3. Inter-Cloud DDoS Mitigation Layer 5
4. Inter-Cloud DDoS Mitigation API 6
5. Security Considerations 7
6. IANA Considerations 7
7. References 7
7.1 Normative References 7
7.2 Informative References 7
Authors' Addresses 7

1. Introduction

The recent growth in volume and scale of Distributed Denial of Service (DDoS) attacks, particularly its impact on the large pipes of Inter-Cloud, Inter-Provider connections, calls for mechanisms to enable DDoS mitigation across Cloud Service Providers (CSPs) and Network Service Providers (NSPs). These mechanisms require to define an Inter-Cloud DDoS Mitigation Abstract Layer with corresponding standardized APIs to allow real time, automated information exchange among CSPs and NSPs, and achieve rapid protective response and effective Inter Cloud/Inter Provider DDoS attack mitigation. The need for such standard Inter-Cloud DDoS Mitigation APIs is strong and urgent.

This document defines the Inter-Cloud DDoS Mitigation Abstract Layer and APIs.

This document focuses on Inter-Cloud, Inter-Provider automated exchange of DDoS Mitigation information, although similar APIs could be used within each cloud for handling malicious traffic.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

This document uses the terminology defined in [I-D.draft-hares-i2nsf-use-case-gap-analysis].

In addition, this document uses the following terms.

Term	Definition
BGP	Border Gateway Protocol
CSP	Cloud Service Provider

DC	Data Center
DCI	Data Center Interconnect
DDoS	Distributed Denial of Service
DLC	Disruption Life Cycle
Inter-Cloud	The interconnection between the cloud of different providers
NSP	Network Service Provider
SDN	Software Defined Network
SVR	Server

2. Problem Statement

Along with the rapid growth of cloud services, the large pipes of Inter-Cloud, Inter-Provider connections are increasingly the subject of DDoS attacks. Since these connections are between clouds of different providers, implementing mechanism to achieve rapid protective response in case of attack is challenging. While within its own cloud each provider may be able to protect effectively its network using various DDoS protection techniques, for the Inter-Cloud/Inter-Provider links, each provider does not have full visibility of the attack, and therefore response times may be longer, counter-measures may be less effective, and therefore the severity and impact of the attacks may be very significant.

Large DDoS attacks targeting the Inter-Cloud, Inter-Provider links may consume the available bandwidth or the router/switch/server resources within tens of seconds. While the attack is on, legitimate traffic is prevented from being forwarded over the saturated links. With saturated Inter-Cloud, Inter-Provider links, even if within each cloud the DDoS mitigation may be working effectively, it can quickly be rendered irrelevant.

Today, exchange of DDoS attack information and mitigation strategy among providers is largely manual and typically relies on customized operation processes established ad hoc between each provider. Because of largely manual escalation procedures, providers' reaction times to DDoS attacks to Inter-Cloud, Inter-Provider links tends to be slow (it can easily take tens of minutes if not hours to put effective mitigation measures in place) compared to Intra-Cloud DDoS

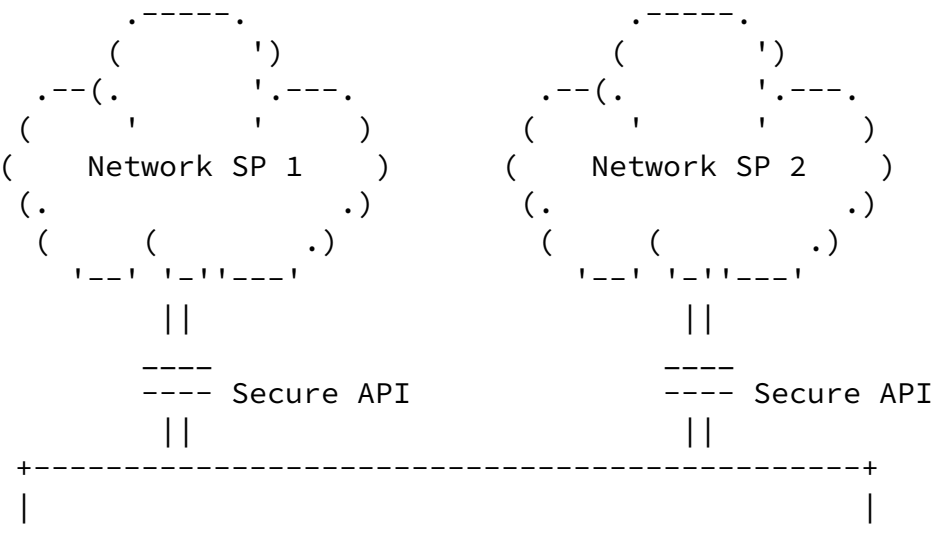
mitigation, and thus the damage caused by such attacks can be substantial. The reaction time may exceed the Disruption Life Cycle (DLC) of the attack.

Sophisticated and determined malicious attackers are able to quickly learn the intended Inter-Cloud Inter-Provider link capabilities and limitations through probing. This includes bandwidth capacity, saturation resistance, and DDoS absorption resilience of the link. The attacker is also able to learn the DDoS countermeasures and their response times, from which the attacker can infer the DLC that can be exacted toward the intended target. The DLC is measured by the assailant from the time the attack is initiated to the time the mitigation response becomes evident. An attacker can then use this information to design the attacks in such a way that the current and subsequent attacks inflict the most harm.

In order to achieve rapid protective response, the exchange of DDoS mitigation information between providers must be enabled in real time and in an automated, standardized fashion.

3. Inter-Cloud DDoS Mitigation Layer

The Inter-Cloud DDoS Mitigation Layer and its corresponding standardized, secure Inter-Cloud DDoS Mitigation APIs is illustrated in Figure 1.



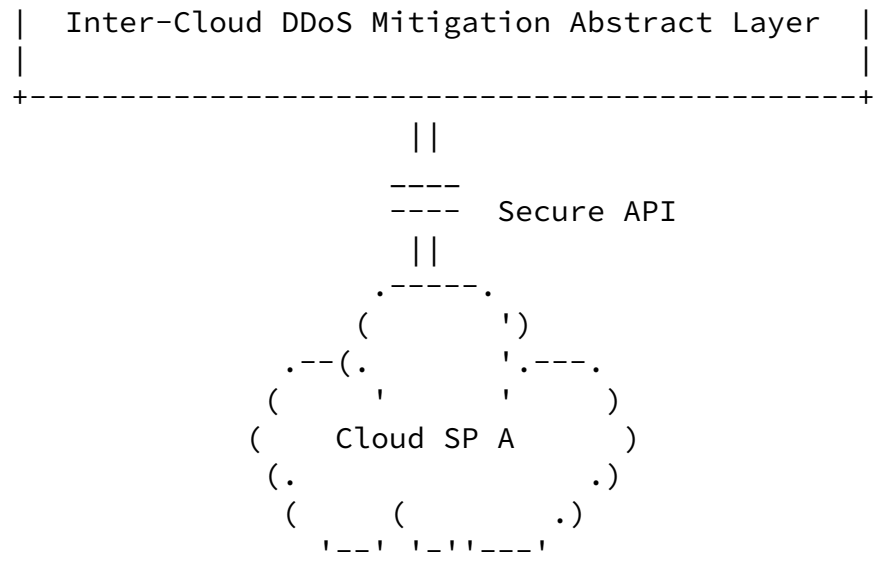


Figure 1. Inter-Cloud DDoS Mitigation Abstract Layer and APIs.

Today there is no accepted industry common DDoS Mitigation Layer that can be used to reduce the reaction time and increase the effectiveness of mitigation in case of attack.

The Inter-Cloud DDoS Mitigation Abstract Layer provides standardized secure APIs that can be used by each provider to programmatically initiate real time information exchanges to other providers to provide visibility of the attack and coordinate DDoS mitigation

mechanisms, Exchanged information may include signatures and forensic of the attack, timestamps, and black-holing countermeasures.

The Inter-Cloud DDoS Mitigation Abstract Layer provides corresponding API calls to exchange mitigation information on the following areas.

DDoS Protection Types:

- TCP flood rate limiting
- UDP flood rate limiting
- TCP SYN.ACK/RST flood protection and authentication
- Maximum concurrent connections per interval rate limiting

- Maximum number of new connections allowed per interval rate limiting
- Maximum fragment packets allowed per interval rate limiting
- Maximum number of packets allowed per interval rate limiting
- Black-holing

BGP Signaling and Mitigation

- BGP /24 route advertisement with community string option
- Mitigation support for /32 with type and rate limit thresholds
- /32 removal from mitigation
- BGP support for /24 removal

Attack Lifecycle Monitoring and Reporting

- Volume and scale of the attack, signatures, forensic
- Timestamps

4. Inter-Cloud DDoS Mitigation API

TBD.

5. Security Considerations

TBD.

6. IANA Considerations

TBD.

7. References

7.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7.2 Informative References

[I-D.draft-hares-i2nsf-use-case-gap-analysis] S. Hares et al., "Analysis of Use Cases and Gaps in Technology for I2NSF ",draft-hares-i2nsf-use-case-gap-analysis-00 (work in progress), October 2015.

Authors' Addresses

Luyuan Fang
Microsoft
15590 NE 31st St
Redmond, WA 98052
Email: lufang@microsoft.com

Deepak Bansal
Microsoft
15590 NE 31st St
Redmond, WA 98052
Email: dbansal@microsoft.com