

DOTS

Internet Draft

Intended status: Informational

Expires: December 2015

L. Xia

H. Song

Huawei

June 27, 2015

The Extended DDoS Open Threat Signaling Use Cases
draft-xia-dots-extended-use-cases-00.txt

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), 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/ietf/lid-abstracts.txt>

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

This Internet-Draft will expire on December 27, 2015.

Copyright Notice

Copyright (c) 2015 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 (<http://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.

Abstract

This draft proposes two extended use cases which illustrate more scenarios and multiple ways of implementation within the existing DOTS work scope. One is the data mining and SDN based centralized Anti-DDoS use case, the other is the NFV based distributed DDoS mitigation use case.

Table of Contents

1.	Introduction	2
1.1.	Background	2
2.	Conventions used in this document	4
3.	Data Mining and SDN Based Centralized DDoS Protection	5
4.	NFV Based Distributed DDoS Mitigation Use Case	7
5.	Security Considerations	9
6.	IANA Considerations	9
7.	References	9
7.1.	Normative References	9
7.2.	Informative References	9
8.	Acknowledgments	9

[1.](#) Introduction

DDoS attacks are one of the largest threats to the Internet, and are evolving very quickly whatever its volume size or complexity. The DDoS attack victims include ISPs, enterprises, and websites. To defend their network resource or services against DDoS attack, Anti-DDoS solutions are needed. According to specific scenarios or requirements, as well as the emerging new technologies such as cloud, NFV and big data, various Anti-DDoS solutions exist in current industry.

This document will present two use cases for a distributed Anti-DDoS solution based on standard inter-system communications between the components. These standards will permit a mix of "best of breed" deployment.

[1.1.](#) Background

Current Anti-DDoS solution is to deploy a proprietary Anti-DDoS system close to the protected site, or in the network, close to the protected site. Anti-DDoS systems can be either one physical box or a distributed system. The former application means that the

detection and mitigation modules are all located in the same box. In comparison, the latter is a distributed system which includes distributed devices responsible for detection (i.e., DPI), mitigation (i.e., scrubbing) and central control respectively. The

latter application is better in overall performance and deployment flexibility. To meet the various requirements, the Anti-DDoS system is deployed in various locations in a network. For example, it is deployed near the protected sites for easily detecting application-layer attacks, or near to the attack source to mitigate attacking traffic as soon as possible and prevent them flooding into the network.

Due to the challenges of high volume and complexity brought by today's DDoS attacks, the cloud-based Anti-DDoS service is becoming attractive and adopted by more and more customers. By this way, all of the customer's traffic is monitored and scrubbed by the Anti-DDoS service provider in real time, and the customer can manage its own Anti-DDoS service and get the related information through the web-based customer portal. This type of service has the benefits of high performance and scalability.

On the other hand, Network Function Virtualization (NFV) is considered as a promising technology used by network operators for its great benefits such as saving cost and speeding up new service's provision. Specifically, for the Anti-DDoS service provided by network operators, they can dynamically create the Anti-DDoS Virtual Network Functions (VNFs) and deploy them to the appropriate locations in the network (i.e., near to the attack source or destination, or both) as needed, because they have the information and control of the whole network. The network operators have the inherent advantage comparing with the third-party Anti-DDoS service providers in this aspect.

Furthermore, in addition to the detection by specific devices (e.g., Deep Packet Inspection (DPI)), normal network forwarding devices (e.g., router or switch) can also be involved in the DDoS attack detection by collecting the L3/L4 flow information and sending them to the centralized platform for analysis or data mining. It can be a complimentary way to current DDoS detection mechanism, or an independent detection method by itself.

During the last few years, the above technologies are in the process

of integration, aiming to develop a comprehensive distributed and collaborative Anti-DDoS solution. One example is the hybrid solution by combining the specified on-premise Anti-DDoS devices with cloud-based Anti-DDoS service. The on-premise devices monitor all the traffic of customer and effectively mitigate the application-layer attacks. When attack size reaches customer-established thresholds, mitigation can be moved to the cloud platform. The ultimate goal of the integration is forming a full spectrum of Layer 3-7 defenses both on-premise and in the cloud. For all the distributed and

Xia, et al.

Expires December 27, 2015

[Page 3]

Internet-Draft

Extended DOTS Use Cases

June 2015

collaborative Anti-DDoS solutions, the coordination among all the member elements is necessary for managing them, as well as collecting and correlating various information from them so as to form a holistic network security view.

[I-D.[draft-mglt-dots-use-cases](#)] describes several DDoS Open Threat Signaling (DOTS) use cases for communication across distributed Anti-DDoS devices or between on-premise device and cloud platform. Additionally, it also illustrates the benefits the DOTS work can bring.

This draft proposes two new use cases which illustrate more scenarios and multiple ways of implementation within the existing DOTS work scope:

- o Collect and correlate security related flow information from network forwarding devices and proactively detect the DDoS attack by centralized analysis or data mining;
- o Dynamic and distributed Anti-DDoS solution by creating VNFs and deploying them to the edge network on demand.

[2.](#) Conventions used in this document

DDoS - Distributed Denial of Service

DOTS - DDoS Open Threat Signaling

SDN - Software Defined Network

NFV - Network Function Virtualization

DPI - Deep Packet Inspection

CAPEX - Capital Expenditure

IPFIX - IP Flow Information Export

ACL - Access Control List

PoP - Point of Presence

[3.](#) Data Mining and SDN Based Centralized DDoS Protection

With the development of big data and SDN/NFV technologies, new ways of thinking of DDoS protection come along as well. A centralized data mining and SDN-like control platform plays a key role for DDoS protection in this use case.

The centralized platform collects L3/L4 flow information from normal network forwarding devices (e.g., router or switch) in the whole network, and then analyzes them with data mining technology to get the holistic view of network DDoS threats leading to an easy DDoS attack detection. Compared with traditional signature based solution, data mining analysis focuses more on the behaviors and patterns of the data flows other than the content of the packets. Multi-dimension to ultra-high dimension models can be built to accurately profile the data flows on-line, which allows detecting and even predicting DDoS attacks in real-time. By this way, operators can greatly reduce the Capital Expenditure (CAPEX), as complicated and expensive detecting devices with Deep Packet Inspection (DPI) functions will be no longer essential. Furthermore, in contrast to dedicated Anti-DDoS devices, the data mining platform is highly scalable without obvious performance limit (the data mining functions can be executed on the elastic computing environment). And it has self-adapting capability to proactively detect new mutations of DDoS attacks.

This Anti-DDoS solution involves a large number of elements, i.e., routers, switches, data mining platform, dedicated Anti-DDoS devices,

and etc, as well as frequent information exchange between them to fulfill its essential functions, i.e., packet/flow sampling, traffic diversion, sending security policies, and etc. All these elements and related control processes can be integrated into the SDN-like control architecture to improve the automation level so as to reduce operational involvement in DDoS attack management.

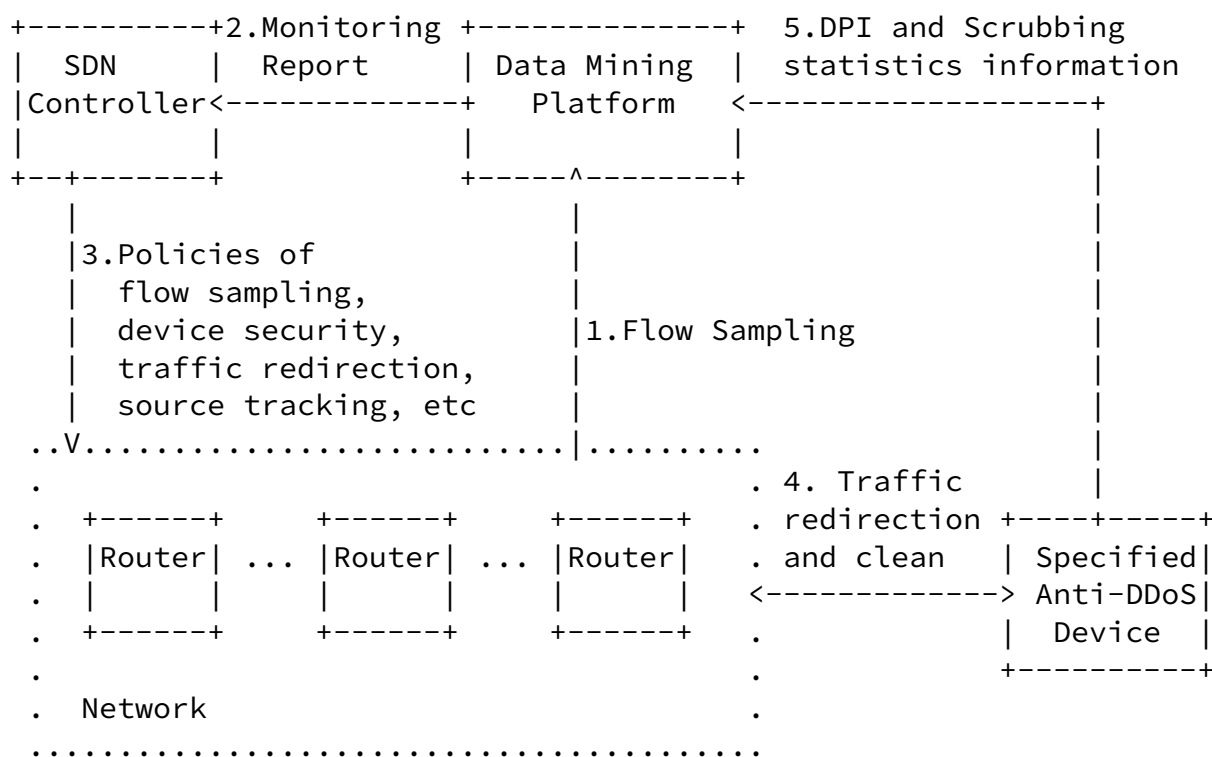


Figure 1. Data Mining and SDN Based Centralized Anti-DDoS Use Case

As illustrated in Figure 1, a data mining and SDN based centralized Anti-DDoS solution forms a closed-loop control system which includes the following steps:

1. Data mining platform monitors network traffics by big data analysis algorithms based on received IP Flow Information Export (IPFIX) packet sampling records, and it probably needs some extensions to current IPFIX specification for security requirements [I-D.[draft-fu-ipfix-network-security](#)].
2. Data mining platform sends the monitoring report to the SDN controller, which provides the inputs for SDN controller to take next step actions. The report contains the information about the detected DDoS attacks based on the data mining models taken by the platform, the information could be the abnormal flows, the suspicious DDoS attack sources or destinations.
3. Based on the monitoring reports input, the SDN controller can control the network forwarding devices to perform various operations, e.g., adjusting the IPFIX flow sampling policies, or configuring device security policies such as rate-limiting or Access Control List (ACL), or traffic redirection to specified mitigation devices or tracking the attack sources and etc.

4. The suspicious traffic is identified and redirected to specified Anti-DDoS devices for further inspection and cleaning, and then clean traffic is transmit back to the network;
5. At last, the DPI and scrubbing statistics information created by the specified Anti-DDoS devices are reported to the data mining platform, which are used to help it to improve and derive further security intelligence by self-learning mechanism.

[4.](#) NFV Based Distributed DDoS Mitigation Use Case

Previously, due to the deployment limit of physical DDoS mitigation devices and the third-party Anti-DDoS service provider does not have the control of the network infrastructure, the centralized deployment of DDoS mitigation devices is more suitable than the distributed deployment. The centralized way is not optimized in saving network bandwidth, and is possible to make DDoS mitigation

Now, the distributed deployment of DDoS mitigation appliances to the network edge is becoming feasible as NFV technologies grows quickly and are widely adopted by network operators for managing network infrastructure. By the way of dynamic deployment, the virtual DDoS mitigation appliances (i.e., virtual FW, scrubbing center, etc) are distributed at the network edges to relieve the performance and network bandwidth consuming problems.

Xia, et al.

[Page 7]

June 2015

```

.....
. Virtual DDoS.
. Mitigation .
. Appliance .
.....
3.Network | //-- --\\
Edge | // +-----+ \\
Deployment | // |Anti-DDoS <--+ \\
| | /Controller| |1.Monitoring
| | /+---+-----+ | Report
| | 2 | | | |
| | / | | | |
| | +V-V+ | | +-----+
| | | | | | DDoS | | Service |
| +---+-----+PoP| 2.Source 2|Monitoring+---+ |
| | | | | Tracking | | appliance | | +-----+

```


There is no IANA consideration for this specification.

[7. References](#)

[7.1. Normative References](#)

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), Internet Mail Consortium and Demon Internet Ltd., November 1997.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), Internet Mail Consortium and Demon Internet Ltd., November 1997.

[7.2. Informative References](#)

- [I-D.[draft-mglt-dots-use-cases](#)] Migault, D., "DDos Open Threat Signaling use cases", work in progress, April 2015.
- [I-D.[draft-fu-ipfix-network-security](#)] Fu, T., Zhang, D., He, D., and Xia, L., "IPFIX Information Elements for inspecting network security issues", work in progress, April 2015.

[8. Acknowledgments](#)

This document was prepared using 2-Word-v2.0.template.dot.

Huawei
101 Software Avenue, Yuhuatai District
Nanjing, Jiangsu 210012
China

Email: Frank.xialiang@huawei.com

Haibin Song
Huawei
101 Software Avenue, Yuhuatai District
Nanjing, Jiangsu 210012
China

Email: haibin.song@huawei.com