DOTS
Internet-Draft
Intended status: Standards Track
Expires: December 31, 2015

T. Reddy
P. Patil
M. Geller
D. Wing
S. Rao
Cisco
M. Boucadair
France Telecom
June 29, 2015

Information Model for DDoS Open Threat Signaling (DOTS)
draft-reddy-dots-info-model-00

Abstract

This document discusses the need and the mechanisms to dynamically update configuration of network monitoring devices to help identify distributed denial-of-service (DDoS) attacks in a network. Once an attack is signalled by a client or detected locally, provisioning cycles are triggered to program a set of network elements to undertake appropriate actions (including, blackhole, drop, rate-limit, or add to watch list) on the suspect traffic.

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 http://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 December 31, 2015.

Copyright Notice

Table of Contents

1. Introduction 2
2. Notational Conventions 3
3. Terminology 3
4. Solution Overview 4
5. Security Considerations 9
6. Acknowledgements 9
7. References 9
7.1. Normative References 9
7.2. Informative References 10
Authors' Addresses 10

1. Introduction

A distributed denial-of-service (DDoS) attack is an attempt to make machines or network resources unavailable to their intended users. In most cases, sufficient scale can be achieved by compromising enough end-hosts and using those infected hosts to perpetrate and amplify the attack. The victim in this attack can be an application server, a client or router, a firewall, or an entire network, etc. Typically, enterprises configure Network Elements and Monitoring Devices (appliances) to export traffic flow information for further processing by applications hosted on other devices, such as DDoS monitoring applications.

DDoS monitoring applications analyze and correlate flow records to baseline proper behaviour and measure deviation from that expected norm ("Observed" vs. "Expected"). Analytics is applied to deliver a baseline of the network in normal operation conditions and then to highlight when an anomalous event occurs. As DDoS attacks get more complex and more sophisticated, DDoS monitoring applications may need more or different fields in the flow records, change the frequency of flow record collection, increase the granularity of flow record collection for traffic to a network resource, tweak the sampling logic, enable or disable packet sampling, modify the packet selection technique for sampling, etc., to adjust their decision-making process for a better detection efficiency.

This document explains mechanisms to dynamically change the configuration of IPFIX-compliant Monitoring Devices ([RFC7011]) and PSAMP-compliant Monitoring Devices ([RFC5476]) using the Network Configuration Protocol (NETCONF) [RFC6241] to identify attacks on the network and once an attack is detected, use NETCONF to carry instructions meant to dynamically enforce appropriate filtering rules on a set of network devices. In addition to the required intelligence to decide which actions are needed, a decision-making process to decide "where" (i.e., which network elements) these filtering actions are to be performed.

2. Notational Conventions

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 [RFC2119].

3. Terminology

This document makes use of the following terms:

- Network Element: refers to a node that is involved in the delivery of connectivity services. A Network Element can be a router, a switch, a service function (e.g., firewall), etc.

- DOTS Client: Refers to the entity that is responsible for signalling an attack. The entity could be a network resource (e.g. Network application) subjected to attack or flow collector, firewall, CPE etc. detecting attack on the network.

- DOTS Controller: Refers to the entity that is responsible for undertaking appropriate actions to satisfy the requests from a DOTS Client.

- Flow Collector: Refers to the functional entity that is responsible for instructing the Network Elements about the monitoring strategy. It is also responsible for collecting monitoring information from the network. One or multiple Flow Collectors may be enabled. Considerations about internal communications between multiple Flow Collectors are out of scope. A Flow Collector may be collocated with a DOTS Client.

- Configuration Manager: Refers to an entity that is responsible for the provisioning of a set of Network Elements.

- Monitoring Devices: These are devices in the network that are provisioned to monitor network flows, collect information and export them to a "Flow Collector".

4. Solution Overview

Flow collector (or DDoS monitoring application) needs to program IPFIX- and PSAMP-compliant Monitoring Devices using vendor-independent configuration data model. A vendor-independent configuration data models helps to store and manage the configuration data of Monitoring Devices in a consistent format. The data model could be specified using YANG [RFC6020] to dynamically configure Monitoring Devices. The configuration data models for IPFIX and PSAMP are discussed in [RFC6728].

In order to offer more automation and dynamicity in changing the configuration of network monitoring, this document proposes an architecture that is composed of two parts:

1. Flow Collector communicates the configuration of network monitoring to the DOTS Controller. This assumes the Flow Controller has been provisioned with the locator(s) of DOTS Controller(s) to contact. For multi-homed networks, the Flow Controller should contact the DOTS Controller attached to the network from which the suspect traffic is received from.

2. The DOTS Controller is responsible for configuring the Monitoring Devices. This assumes the DOTS Controller has access to the underlying network topology (including the interconnection map and the set of advanced service functions).

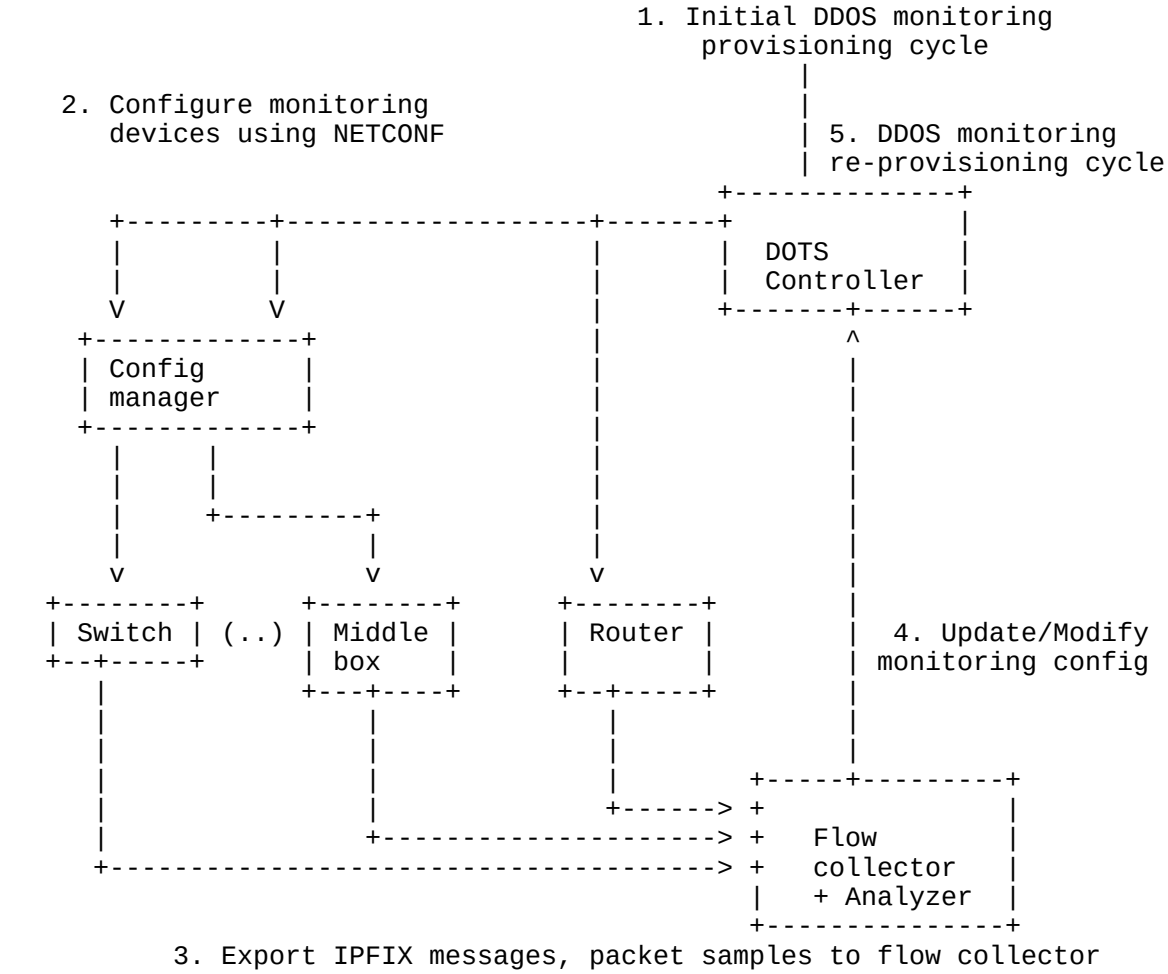

Figure 1: Configuration Cycle for IPFIX

Figure 1 provides a high level overview of the solution. The proposed solution is to build a dynamic configuration model in DDoS Monitoring using a feedback system where a Flow Collector can influence monitoring configurations on the devices to gather information about a potential DDoS event.

The sequences marked (1)-(5) in Figure 1 refer to the work flow of the proposed solution, these flows can be broadly categorized into three phases:

1. Initial Provisioning Cycle: Represents the initial state of the monitoring configuration where an administrator updates the Controller with a default or preliminary monitoring configuration delivered to Monitoring Devices. For example, the initial configuration on the Monitoring Devices is to collect information elements such as IP addresses/prefixes, application type, transport ports, flow timestamps, interfaces and so on.

2. Flow Monitoring: Refers to the activity of Monitoring Devices to inspect and watch network flows. Based on the monitoring configuration, the Monitoring Device is instructed to collect specific flow information and export them to a "Flow Collector".

3. Flow Collection and Analysis: A "Flow Collector" device collects and (possibly) aggregates flow information from one or more Monitoring Devices. As the Collector continues to gather more and more data, it can potentially correlate and analyze flow information to "guess" or determine if a DDoS event is in progress. If so, the Flow Collector may consider gathering additional data from the Monitoring Devices and signals this intent to a "Controller".

4. Re-provisioning Cycle: The Controller receives from the "Flow Collector", the intent to re-provision Monitoring Devices to produce additional flow information elements. The Controller, then delivers the new or updated configuration to the appropriate Monitoring Devices.

The other provisioning interface is the one between the DOTS Controller and Network Elements. Concretely, when the Flow Collector identifies an active attack, it signals to the DOTS Controller the set of traffic identification information (including all suspect IP addresses) together with a suggested action (e.g., rate-limit, drop, monitor). Then, the DOTS Controller propagates the filtering rules to the Network Elements (including routers, middleboxes). The Flow Collector, after certain duration, requests the rules to block traffic from these IP addresses be removed once the attack has stopped. Means to detect an attack is not valid anymore may be static (an administrative decision) or dynamic (based on an analysis of the traffic).

Note, [RFC6088] provides typical information that can be included in the traffic identification information set.

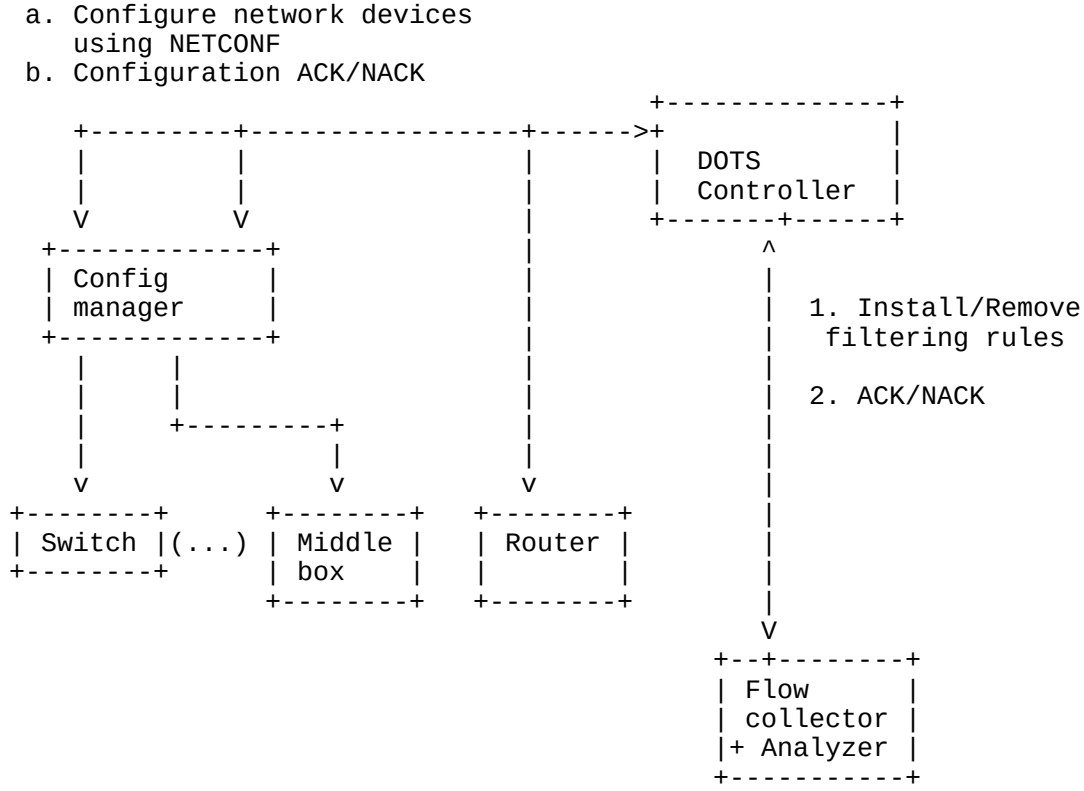

Figure 2: Configuration Cycle for Attack Mitigation

As shown in Figure 3, two distinct interfaces are defined: the one used by a Flow collector to signal appropriate filtering rules to a DOTS Controller (for example, [I-D.reddy-dots-transport] can be used for this interface) and the one to enforce polices in the appropriate nodes (for example, NETCONF can be used).

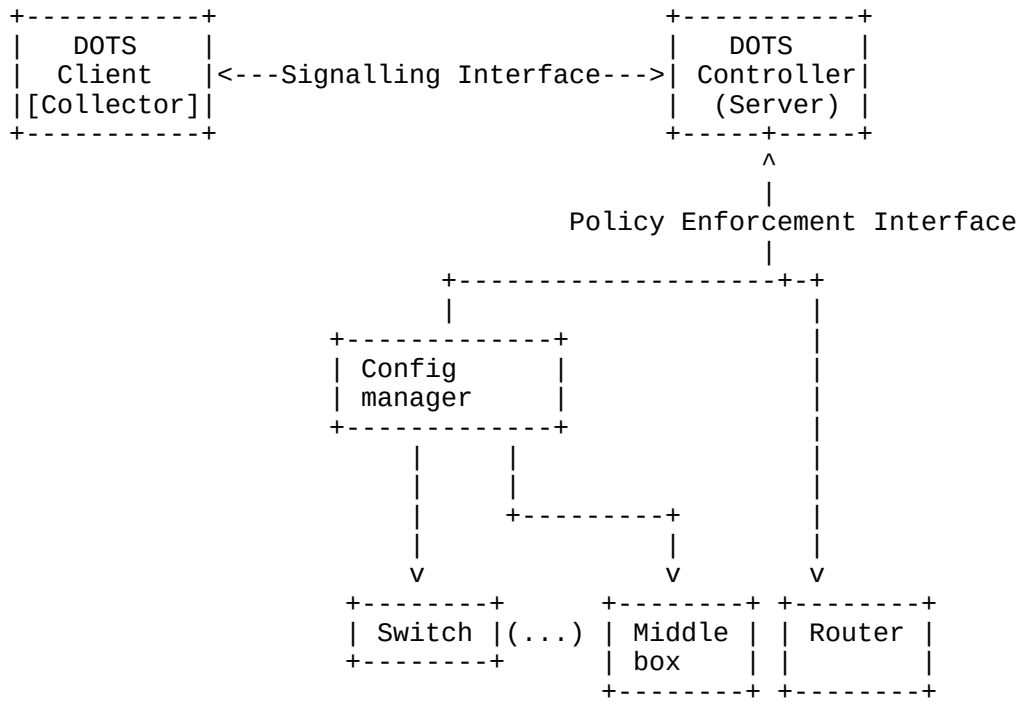

Figure 3: Signalling Interface & Policy Enforcement Interface

DOTS Client and DOTS controller could be located in different administrative domains. Local decisions (e.g., install filters) can be made locally be the DOTS Controller. A notification is then sent to the DOTS Clients using the signaling interface. Concretely, the decision-making process of the DOTS Controller can be based on events that are reported by other DOTS Clients, local monitoring tools, etc. Appropriate notifications and feedback objects should be carried over the signaling interface.

The signaling interface can also be used by a DOTS Controller to request a confirmation from a DOTS Client about the enforcement of a filter. For example, this can occur when the DOTS Controller detects that some traffic is likely to be a DoS, before undertaking actions on Network Elements, the DOTS Controller contacts first the DOTS Client to double check whether that traffic is really a DoS. Upon confirmation from the DOTS Client, the DOTS Controller initiates a configuration cycle accordingly.

5. Security Considerations

The authentication mechanism between the Flow Collector and DOTS Controller should be immune to pervasive monitoring [RFC7258]. An attacker can intercept traffic by installing rules that would lead to redirect all or part of the traffic to an illegitimate Flow Collector. Means to protect against attacks that would lead to install, remove, or modify rules must be supported.

In order to protect against denial of service that would be caused by a misbehaving trusted Flow Collector, DOTS Controller should rate limit the configuration changes received from a Flow Collector.

6. Acknowledgements

Thanks to C. Jacquenet for the review.

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.

[RFC5476] Claise, B., Johnson, A., and J. Quittek, "Packet Sampling (PSAMP) Protocol Specifications", RFC 5476, March 2009.

[RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6728] Muenz, G., Claise, B., and P. Aitken, "Configuration Data Model for the IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) Protocols", RFC 6728, October 2012.

[RFC7011] Claise, B., Trammell, B., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, September 2013.

7.2. Informative References

[RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, May 2014.

Authors' Addresses

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tireddy@cisco.com

Prashanth Patil
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore
India

Email: praspati@cisco.com

Mike Geller
Cisco Systems, Inc.
3250
Florida 33309
USA

Email: mgeller@cisco.com

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: dwing@cisco.com

Sandeep Rao
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: rsandeep@cisco.com

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com