Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2016

C. Zhou
L. Xia
Huawei Technologies
M. Boucadair
France Telecom
J. Xiong
Huawei Technologies

October 19, 2015

The Capability Interface for Monitoring Network Security Functions (NSF) in I2NSF

draft-zhou-i2nsf-capability-interface-monitoring-00

Abstract

This document focuses on the monitoring aspects of the flow-based Network Security Functions (NSFs). The NSF Capability interface between the Service Provider's management system (or Security Controller) and the NSFs is meant to enforce the required monitoring capability.

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 April 21, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
2. Terminology 3
3. The Capability Interface for Monitoring 3
3.1. Overview 3
3.2. Traffic Report 4
3.3. Policy Enforcement 5
4. Security Considerations 5
5. IANA Considerations 5
6. References 6
6.1. Normative References 6
6.2. Informative References 6
Authors' Addresses 6

1. Introduction

Rising security problems bring challenges for the security enterprises and organizations. There are already some software and hardware devices deployed for these problems, e.g., antivirus, firewall, intrusion detection systems (IDS), Web security gateway, and DPI, which build up many safety lines accordingly. However, one individual safety line only defenses the security threats of only one aspect. And more seriously, these safety defense devices are generating large amount of logs and events in the operating procedure, which makes a lot of "information island". With large quantity and isolated security information, it brings low efficiency for the security managers who operate on their own control platform and warning window of various devices.

The network security mechanism would be more efficient if the Security Controller defined in [I-D.merged-i2nsf-framework] could monitor, analyze and investigate the abnormal events and finally produce security reports to the security administrators. The security controller should also be able to collect the traffic and session information from the NSF, in order to steer the suspected attack source or victim traffic to the cleaning center.

The data mining use case defined in [I-D.xia-dots-extended-use-cases] has provided a good example for distributed denial-of-service (DDoS) attack monitoring report. [I-D.reddy-dots-info-model] also describes the information model of flow monitoring to help identify DDOS

attacks in a network. This document aims to cover more cases and more attack types in the network, e.g., botnets, spam, and spyware.

This document describes how to use the capability interface to collect the security information from the NSFs and which security information will be reported using this interface. The protocol and information model will be described for the monitoring aspects of the Capability Interface.

2. Terminology

3. The Capability Interface for Monitoring

3.1. Overview

The capability interface should be able to provide unified event format for the logs and warning information of the overall network, to facilitate the failure discovery and failure locating timely and accurately. With the unified event format, the security managers could run easily and quickly through various security events which guarantees the availability of service information system and service continuity. To achieve this, the Security Controller needs to collect the detailed information of the network status and traffic information from the NSF to make intelligent security decision and to dynamically adjust the sampling and steering policy.

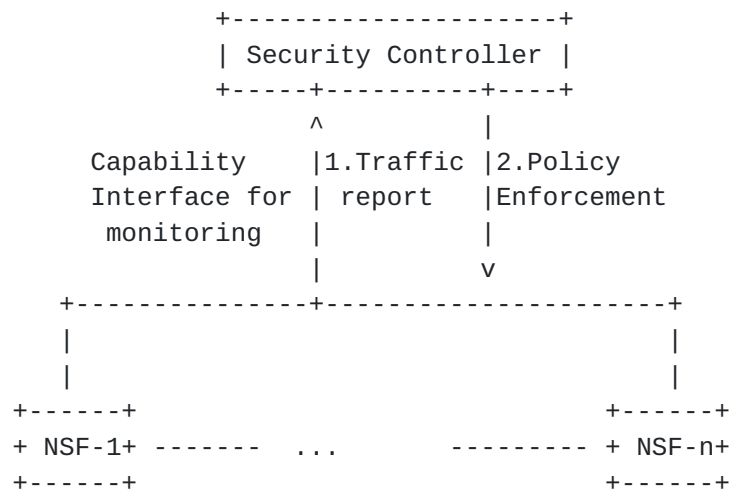

Figure 1: Monitoring Interface

As described in Figure 1, the traffic monitoring procedure involves two network elements: Security Controller (SC) and NSF. The NSF reports the monitoring information to the SC, which provides the specific traffic information, e.g., abnormal flows, security logs, statistics or the suspicious attack sources or destinations. The SC is responsible for monitoring and collecting traffic information from NSFs. Based on the input from the NSF, the SC could make policy enforcement for the specific flows, e.g., traffic steering or adjusting the flow sampling policies.

3.2. Traffic Report

The traffic reported from the NSF may contain the information of IP addresses, security logs, statistics, warnings, and etc. The syslog protocol [RFC5424] could be used to send event notification messages to the SC for traffic collection. The IP Flow Information Export (IPFIX) protocol [RFC5101] may also be adopted for the flow sampling information collection. There are mainly three types of information reported using the capability interface:

- Traffic Statistics:
  - Normal traffic statistics based on the source and destination address, including byte per second (bps) and packet per second (pps).
  - Abnormal traffic statistics based on the source and destination address, including bps and pps.
  - Traffic statistics based on the network address range (including port usage), including bps and pps.
- Session Statistics:
  - Concurrent session statistics based on the source and destination address.
  - New session statistics based on the source and destination address.
  - Abnormal session statistics based on the source and destination address, including null link, retransmission session and slow-start link.
- Abnormal/Attack Event: analysis results of the relevant abnormal/attack event, e.g., time, type, level, detail description, threshold, source IP address and destination IP address.

The NSF could report the accurate source and destination of the attack to the security controller for which to make traffic steering policy, e.g., steering the bad "botnet" traffic to the cleaning center. The type, size and proportion of the abnormal traffic could also be reported to assist the security controller to determine the steering priority, e.g., priority traction, large flow cleaning.

3.3. Policy Enforcement

The Security Controller is responsible for making policy decisions after getting the security information from the NSF (and, typically, other instructions from the operator). It will provide the attack mitigation and defense strategy with the acquired sampling traffic information for attack detection by the way of dynamically adjusting the flow sampling policy, e.g., flow information, sampling ratio, sampling encapsulation method and/or sampling point information. The policies may include: traffic cleaning and sampling adjustment.

- Traffic cleaning: with the suspicious result of the analyzed sampling traffic, the security controller dynamically sends the steering policy to the related NSF or sends the flow blocking policy to the NSF which is nearest to the attack point, to block the attack traffic from the source. The traffic cleaning policy may include the following three ones:

  * Access Control List (ACL), to block the attack traffic.

  * Packet hash digest to block the attack traffic.

  * Traffic steering policy to clean the traffic.

- Flow sampling adjustment: after filtering the abnormal object of the sampling traffic, the security controller could dynamically adjust the sampling policy to improve the sampling rate of the TOPN abnormal object, in order to make more accurate attack detection. The abnormal object may include: Top N network address range of the abnormal session, Top N IP address of the abnormal session and the Top N of abnormal sessions.

4. Security Considerations

5. IANA Considerations

This document has no actions for IANA.

6. References

6.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5101] Claise, B., Ed., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, DOI 10.17487/RFC5101, January 2008, <http://www.rfc-editor.org/info/rfc5101>.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, DOI 10.17487/RFC5424, March 2009, <http://www.rfc-editor.org/info/rfc5424>.

6.2. Informative References

[I-D.merged-i2nsf-framework] Lopez, E., Lopez, D., Zhuang, X., Dunbar, L., Parrott, J., Krishnan, R., and S. Durbha, "Framework for Interface to Network Security Functions", June 2015.

Authors' Addresses

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: cathy.zhou@huawei.com

Liang Xia (Frank)
Huawei Technologies
101 Software Avenue, Yuhuatai District
Nanjing, Jiangsu 210012
P.R. China

Email: Frank.xialiang@huawei.com

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Jie Xiong
Huawei Technologies
101 Software Avenue, Yuhuatai District
Nanjing, Jiangsu 210012
P.R. China

Email: emma.xiong@huawei.com