Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: March 10, 2013

Z. Chen
China Telecom
C. Zhou
Huawei Technologies
T. Tsou
Huawei Technologies (USA)
T. Taylor
Huawei Technologies

September 6, 2012

Syslog Format for NAT Logging
draft-zhou-behave-syslog-nat-logging-01

Abstract

Under some circumstances operators will need to maintain a dynamic record of external address and port assignments made by a Carrier Grade NAT (CGN), and will find it feasible and convenient to create such records using SYSLOG (RFC 5424). The present document standardizes a SYSLOG format to meet that recording requirement. It specifies a number of fields that could be a part of the log report, leaving it up to operators to select the fields needed for their specific circumstances.

[*** Subject to discussion*** The log format presented here may also be used by PCP server implementations to log the mappings they implement.]

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Operators already need to record the addresses assigned to subscribers at any point in time, for operational and regulatory reasons. When operators introduce Carrier Grade NATs (CGNs) into their network, both addresses and ports on the external side of the CGN are shared amongst subscribers. To trace back from an external address and port observed at a given point in time to a specific subscriber requires additional information: a record of which subscriber was assigned that address and port by the NAT.

Address-port assignment strategies present a tradeoff between the efficiency with which available external addresses are used, the cost of maintaining a trace back capability, and the need to make port assignments unpredictable to counter the threat of session hijacking. At one extreme, the operator could make a one-time assignment of an external address and a set of ports to each subscriber. Traceback would then be a matter of retrieving configuration information from the NAT. Even in this situation, it is possible that a request for legal interception is placed against a specific subscriber, such that each session involving that subscriber is recorded.

At the opposite extreme, a carrier could assign external addresses and ports to subscribers on demand, in totally random fashion. Such a strategy is not really practical, both because of the volume of records that would be required to support a traceback capability, and because the apparent gain in efficiency with which address-port combinations would be utilized would be attenuated by the need to leave address-port assignments idle for some minimum amount of time after last observed use to make sure they weren’t still being used.

Between these extremes, operators may choose to assign specific addresses and specific blocks of ports to subscribers when they log on to the network, releasing the assignments when they drop off. Such a strategy could be desirable in networks with mobile subscribers, in particular. Compared with the fully dynamic strategy, this strategy reduces the number of times that assignments have to be recorded by orders of magnitude.

The point just made is that under some circumstances operators need to record allocations of external address-port combinations in the NAT dynamically, and the volume of information contained in those records is manageable. Various means are available to create such records. This document assumes that for some operators, the most convenient mechanism to do so will be event logging using SYSLOG [RFC5424], where the SYSLOG records are generated either by the NAT itself or by an off-line device.

The next section specifies a SYSLOG record format for logging of NAT address and port assignments and the format of fields that could be used within such a record. It is up to individual operators to choose the fields that match their specific operating procedures.

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 "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

2. SYSLOG Record Format For NAT Logging

This section describes the SYSLOG record format for NAT logging in terms of the field names used in [RFC5424] and specified in Section 6 of that document. In particular, this section specifies values for the APP-NAME and MSGID fields in the record header, the SD-ID identifying the STRUCTURED-DATA section, and the PARAM-NAMEs and PARAM-VALUE types for the individual possible parameters within that section.

2.1. SYSLOG HEADER Fields

Within the HEADER portion of the SYSLOG record, the priority (PRI) level is subject to local policy, but a default value of 86 is suggested, representing a Facility value of 10 (security/authorization) and a Severity level of 6 (informational). Depending on where the SYSLOG record is generated, the HOSTNAME field may identify the NAT or an offline logging device. In the latter case, it may be desirable to identify the NAT using the NID field in the STRUCTURED-DATA section (see below). The value of the HOSTNAME field is subject to the preferences given in Section 6.2.4 of [RFC5424].

The values of the APP-NAME and MSGID fields in the record header determine the semantics of the record. The RECOMMENDED APP-NAME value "NAT" indicates that the record relates to an assignment made autonomously by the NAT itself. [*** Subject to discussion*** The RECOMMENDED APP-NAME "PCP" indicates that the assignment to which the record refers was the result of a Port Control Protocol (PCP) [I-D.PCP-Base] command.] The RECOMMENDED MSGID value "ADD" indicates that the assignment took effect at the time indicated by the record timestamp. The RECOMMENDED MSGID value "DEL" indicates that the assignment was deleted at the time indicated by the record timestamp.

2.2. STRUCTURED-DATA Fields

This document specifies a value of "asgn" (short for "assignment") for the SD-ID field identifying the STRUCTURED-DATA section of the record. In addition it specifies the following parameters for use within that section. All of these parameters are OPTIONAL. All values that are IP addresses are written as a text string in dotted-decimal form (IPv4) or as recommended by [RFC5952] (IPv6).

2.2.1. Incoming IP Source Address Parameter

PARAM-NAME: iSA. PARAM-VALUE: the incoming IP source address of the packet(s) to which the assignment described by this record applies.

2.2.2. Outgoing IP Source Address Parameter

PARAM-NAME: oSA. PARAM-VALUE: the outgoing IP source address of the packet(s) to the assignment described by which this record applies.

2.2.3. Incoming Source Port Parameter

PARAM-NAME: iSP. PARAM-VALUE: the incoming IP source port of the packet(s) to the assignment described by which this record applies.

2.2.4. Outgoing Source Port Parameter

PARAM-NAME: oSP. PARAM-VALUE: the outgoing IP source port of the packet(s) to which the assignment described by this record applies. If the record pertains to the assignment of a range of ports, this parameter gives the lowest port number in the range. In the case of a range, either parameter oSPct or parameter oSPmx SHOULD also be present in the log record.

2.2.5. Number of Port Numbers Parameter

PARAM-NAME: oSPct. PARAM-VALUE: used when the record pertains to the assignment of a range of ports (either consecutive or generated by a known algorithm). This parameter gives the number of port numbers in the range.

2.2.6. Highest Outgoing Port Number Parameter

PARAM-NAME: oSPmx. PARAM-VALUE: used when the record pertains to the assignment of a range of ports (either consecutive or generated by a known algorithm). This parameter gives the highest port number in the range.

2.2.7. Protocol Parameter

PARAM-NAME: Pr. PARAM-VALUE: an integer indicating the value of the Protocol header field (IPv4) or Next Header field (IPv6) in the incoming packet(s) to which the assignment described by this record applies.

2.2.8. Subscriber Identifier Parameter

PARAM-NAME: SID. PARAM-VALUE: an arbitrary UTF-8 string identifying the subscriber to which this assignment applies. This is intended to provide flexibility when the incoming source address will not be unique. The value could be a tunnel identifier, layer 2 address, or any other value that is convenient to the operator and associated with incoming packets.

2.2.9. NAT Identifier Parameter

PARAM-NAME: NID. PARAM-VALUE: an arbitrary UTF-8 string identifying the NAT making the assignment to which this record applies. Needed only if the necessary identification is not provided by the HOSTNAME parameter in the log record header.

3. IANA Considerations

This document requests IANA to make the following assignments to the SYSLOG Structured Data ID Values registry. RFCxxxx refers to the present document when approved.

Structured Data ID	Structured Data Parameter	Required or Optional	Reference
asgn		OPTIONAL	RFCxxxx
	iSA	OPTIONAL	RFCxxxx
	oSA	OPTIONAL	RFCxxxx
	iSP	OPTIONAL	RFCxxxx
	oSP	OPTIONAL	RFCxxxx
	oSPct	OPTIONAL	RFCxxxx
	oSPmx	OPTIONAL	RFCxxxx
	Pr	OPTIONAL	RFCxxxx
	SID	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx

Table 1

4. Security Considerations

When logs are being recorded for regulatory reasons, preservation of their integrity and authentication of their origin is essential. To achieve this result, it is RECOMMENDED that the operator deploy [RFC5848].

Access to the logs defined here while the reported assignments are in force could improve an attacker's chance of hijacking a session through port-guessing. Even after an assignment has expired, the information in the logs SHOULD be treated as confidential, since, if revealed, it could help an attacker trace sessions back to a particular subscriber or subscriber location. It is therefore RECOMMENDED that these logs be transported securely, using [RFC5425], for example, and that they be stored securely at the collector.

5. Normative References

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

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

[RFC5425] Miao, F., Ma, Y., and J. Salowey, "Transport Layer Security (TLS) Transport Mapping for Syslog", RFC 5425, March 2009.

[RFC5848] Kelsey, J., Callas, J., and A. Clemm, "Signed Syslog Messages", RFC 5848, May 2010.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

Authors' Addresses

Zhonghua Chen
China Telecom
P.R. China

Phone:
Email: 18918588897@189.cn

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

Phone:
Email: cathy.zhou@huawei.com

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
Email: tina.tsou.zouting@huawei.com

T. Taylor
Huawei Technologies
Ottawa,
Canada

Phone:
Email: tom.taylor.stds@gmail.com