Syslog NAT Logging
draft-zhou-behave-syslog-nat-logging-00

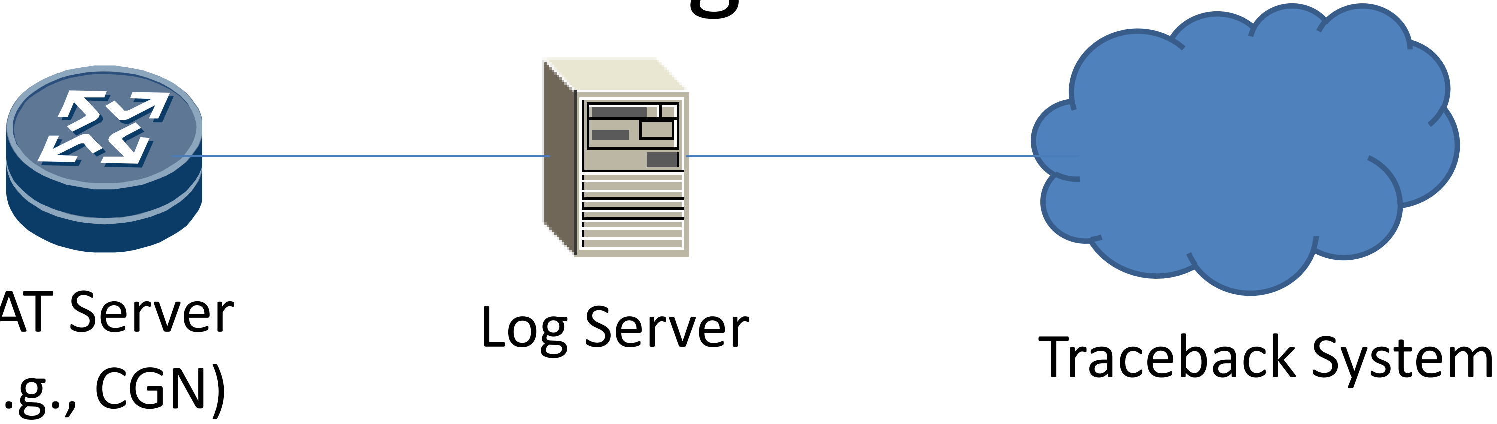
Zhonghua Chen <18918588897@189.cn>
Cathy Zhou <cathy.zhou@huawei.com>
Tina Tsou <tina.tsou.zouting@huawei.com>

IETF 84, Vancouver

Introduction

- This document defines:
  - Requirements of NAT log server
  - Syslog interface for NAT logging.
- Reference:
  - The Syslog Protocol [RFC5424]
  - Transport Layer Security (TLS) Transport Mapping for Syslog [RFC5425].
  - Transmission of Syslog Messages over UDP [RFC5426]. The log server must support sending the syslog log using standard UDP port 514, and support sending syslog log using any one self-configured port of the user.
  - Reliable Delivery for Syslog [RFC3195].

NAT Log Server



Log Server:

- Acquire dynamic address/port mapping information from the NAT device
- Provide the mapping to the traceback system (or AAA)
- The storage information in the log server:
  - Application name
  - Hostname
  - Start time
  - Original source IP
  - Translated source IP
  - Translated source start port
  - Translated source stop port

Syslog Interface

- HEADER
  - PRI: Facility value =16; Severity value=6
  - VERSION: 1
  - TIMESTAMP: <year> <mon> <day> <hh:mm:ss>
  - HOSTNAME: IPv4 address of the originating device
  - APP-NAME: The name of the device that originated the syslog message
  - PROCID: The interrelated logs in one device
  - MSGID: Message type (NAT444 or DS-Lite)
- MSG
  - [<L4> < Original Source IP > < Original Source IPv6> < Translated Source IP > < Original Port > < Translated First Source Port > < Translated Last Source Port >]

Next Steps

- Update data structure elements to specify SD-ID and SD-PARAM in 01 version.
- Add syslog NAT logging in Behave charter?