NAT logging

draft-sivakumar-behave-nat-logging-06
draft-ietf-behave-syslog-nat-logging-00

Senthil Sivakumar (ssenthil@cisco.com)/Reinaldo Penno (repenno@cisco.com)

Cathy Zhou (cathy.zhou@huawei.com) et al

Summary of Drafts 1
draft-sivakumar

- draft-sivakumar uses IPFIX (RFC5101 etc.) as its reporting format
  - Binary, advantage of compactness
- Templates and IEs for reporting the following events:
  - NAT44 Session/BIB create/delete
  - NAT64 Session/BIB create/delete
  - Address exhaustion/Port exhaustion
  - Address binding
  - Quota/Limit exceeded
  - Port block allocation/deallocation

Changes from draft-sivakumar-05

- Comments from Julia
- Incorporated
  - Clarified the draft is not CGN specific
  - Updated the IANA assigned fields & removed inconsistencies
- Outstanding
  - Using a string for address pool name
  - Need an IE for subscriber info.

Summary of Drafts 2
draft-ietf-behave-syslog

- Uses Syslog (RFC5424)
  - ASCII, key-value stucture, header overhead (timestamps, etc.)
- Defines message types and fields for the following:
  - incoming and outgoing source address and port
  - port range allocation (how many, highest value)
  - protocol number
  - subscriber ID
  - NAT identifier
- Conceived with the intent of recording block assignments of resources rather than capturing individual sessions.

Comparison of the two drafts

- IPFIX is binary format – syslog is ASCII
- IPFIX has compactness. Syslog is key-value stucture, header overhead
- Resource exhaustion notifications like address & port exhaustions are present in ipfix.
- Syslog records block assignments of resources rather than capturing individual sessions.

Comparison table

Event	draft-sivakumar	draft-ietf-syslog
NAT44 BIB add/delete	Yes	No
NAT64 BIB add/delete	Yes	No
NAT44 session add/delete	Yes	No
NAT64 session add/delete	Yes	No
Address/port exhaustion	Yes	No
Port block allocation	Yes	Yes
Limits exceeded	Yes	No

Next steps

- Need WG input on if/what events are to be
  - Added to IPFIX draft
  - Added to Syslog draft
  - Removed from IPFIX draft
  - Removed from Syslog draft