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 structure, 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 structure, header overhead
- Resource exhaustion notifications like address & port exhausted are present in IPFIX.
- Syslog records block assignments of resources rather than capturing individual sessions.
### Comparison table

<table>
<thead>
<tr>
<th>Event</th>
<th>draft-sivakumar</th>
<th>draft-ietf-syslog</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT44 BIB add/delete</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NAT64 BIB add/delete</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NAT44 session add/delete</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NAT64 session add/delete</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Address/port exhaustion</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Port block allocation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Limits exceeded</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
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