NAT Behavioral Requirements Updates

draft-ietf-behave-requirements-update-00

Reinaldo Penno <rpenno@cisco.com>
Simon Perreault <simon.perreault@viagenie.ca>
Sarat Kamiset
Mohamed Boucadair <mohamed.boucadair@orange.com>
Kengo Naito <kengo@lab.ntt.co.jp>

IETF 87, Berlin
BEHAVE meeting

2013-07-29

Status

- Since ieTf 86
  - Adopted by WG
  - Long discussion about ways of achieving external port scalability

External port scalability

- External ports are one resource that a stateful NAT manages
- Big NAT operators need better scalability so as to use fewer external IPv4 addresses
- BEHAVE RFCs mandate Endpoint-Independent Mapping (EIM)
  - 1 internal ports <--> 1 external port
  - Justification: allows NAT traversal using e.g. STUN
- EIM for UDP is widely implemented.
  EIM for TCP is still rare.

Port overloading

- Not to be confused with Endpoint-Dependent Mapping (EDM) !!!
- Port overloading relates to port preservation
  - Preservation: external port = internal port
  - Overloading: external port = internal port, even if the external port is already in use by another mapping
    - A special kind of port preservation
- Port overloading implies EDM for overloaded mappings
  - Says nothing about non-overloaded mappings
  - One of the overloaded mappings could be a catch-all (quasi-EIM)
- EDM does not imply port overloading because EDM does not imply port preservation

Port overlapping

- This term is currently used in the draft
- Undefined
- Needs to be rewritten with IETF terminology

External port scalability

- Both port overloading and EDM increase scalability w.r.t. external ports
- Both are strictly forbidden by RFC 4787:
  - REQ-1: A NAT MUST have an "Endpoint-Independent Mapping" behavior.
  - REQ-3: A NAT MUST NOT have a "Port assignment" behavior of "Port overloading".
- The important question: **Is there a way to relax those requirements so as to increase scalability without sacrificing traversability?**

Proposal A

- MUST do EIM by default
- MAY do EDM when it is known that EDM does not cause the application-layer protocol to break (how to determine this is out of scope)
  - Formulation borrowed from RFC 6888:

    REQ-7: It is RECOMMENDED that a CGN use an "endpoint-independent filtering" behavior (as defined in Section 5 of [RFC4787]). If it is known that "Address-Dependent Filtering" does not cause the application-layer protocol to break (how to determine this is out of scope for this document), then it MAY be used instead.
- Applying EDM to TCP port 80 and UDP port 53
  - Easy
  - Significant scalability improvement
  - Minimal breakage (if any)

Proposal B

(Not sure this is an accurate description.)

- MUST do EIM by default.
- MUST do port preservation and overloading.
- Applications that need NAT traversal can detect overloading and react by using a different internal port.

Proposal C

- Do nothing.

Proposal D

- ???

Next steps

- Rewrite section about port overlapping based on guidance received
- Many smaller fixes throughout the document