draft-ietf-behave-nat-icmp-03

Summary of changes from -01

Pyda Srisuresh
Bryan Ford
Senthil Sivakumar
Saikat Guha

Presented by Dan Wing

Summary of changes from -01

- Comments from last WG folded into -03
- Changes due to draft-bonica-internet-icmp
  - REQ-3, REQ-4, and REQ-5
- Requirements for ICMP Error packets traversing NAT vs Generated by NAT.
- ICMP draft specifies only the translation of ICMP messages
  - Reaction to those messages left to protocol-specific documnets. REQ-6 changed accordingly.
- Requirements necessary for current applications to work vs. future applications use

Changes due to draft-bonica-internet-icmp

- Changes Ensure NATs don't break ICMP extensions
- Changes currently have the NAT translate ICMP payloads containing realm-specific IP addresses within ICMP extensions
  - Do we want to do that?
    - No current extensions include IP addresses
    - An extension that does might induce address leakage to public side.
  - Can we accomplish this without the NAT knowing each ICMP extension?

ICMP Errors Traversing NAT vs Generated by NAT

- Requirements for ICMP Error packets traversing a NAT device
  - Sections 4, 5
  - REQ-3, REQ-4, REQ-5, REQ-6, REQ-7
- Requirements for ICMP Error packets generated by a NAT device
  - Sections 6, 7
  - REQ-8, REQ-9

Reaction to ICMP left to Protocol Documents

- REQ-6 changed to be specific to ICMP queries.

> "While processing an ICMP error packet pertaining to an ICMP Query or Query response message, a NAT device MUST NOT refresh or delete the NAT Session that pertains to the embedded payload within the ICMP error packet."

Split between Current Applications and Future Applications

- Requirements for current applications to work:
  - Req-1, Req-2, Req-4, Req-5, Req-6, Req-7, Req-9
- Requirements for future applications:
  - Req-1a, Req-3, Req-4c, Req-5c, Req-8

Miscellaneous

- Folded in individual comments from Philip Matthews, Fernando Gont and Dan Wing.
- Security Considerations section updated for REQ-8.
  - Some NATs may not be able or willing to send an ICMP error message when out of resources
    - Confirms successful DoS to attacker
    - Consumes now-scarce resources to send ICMP errors
- [NAT-TERM], [NAT-TRAD] references moved from Normative to informative

Next Steps

- Any questions/comments?
- Will integrate Cullen's comments and today's comments
- Expect to WGLC next version of document