Internet facing server logging recommendation

Alain Durand, Juniper networks

Background

- The IPv4 IANA free pool will soon be exhausted
- ISPs around the world will be deploying NATs
- Draft-ietf-intarea-shared-addressing-issues explains the issues around logging to deal with abuse/LEA
- Logs on the NAT side need to be matched with logs on the server side
  - Need more specific information on the server side logs than we currently have.

Recommendation (BCP candidate)

- It is RECOMMENDED as best current practice that Internet facing servers logging incoming IP addresses also log:
  - The source port number.
  - A timestamp accurate to the second, with associated time zone.
  - The transport protocol (usually TCP or UDP) and destination port number, when the server application is defined to use multiple transports or multiple ports.