Enhanced Port Forwarding functions with CGNAT

draft-chan-tsvwg-eipf-cgnat-00.txt

Louis Chan
Juniper Networks
Jul 2022
Problem statement:

- RFC5128 provides methods for setting up P2P connection behind NAT44. However,
  - Only works for UDP in live situation
  - For TCP, it has low success rate.
    - e.g. Direct TCP connection for webcam does not work
  - It hole punching method needs a common 3rd party server

- Need a solution working for TCP under CGNAT
  - Each party could run independently
UDP hole punching

UDP – High success rate
  But a common 3rd party server is a must, and all runs software from same entity

TCP – Low success rate. Practically, it is not deployed.
Endpoint Independent port forwarding (EIPF) Enhancement

• Allow TCP/UDP incoming connection through CGNAT WITHOUT changing the DEST port
  • DEST port is actually allocated from CGNAT as outgoing source port per private IP
• Allow chain of forwarding of the same DEST port from CGNAT, RG and hence to the end device
Example: incoming TCP session for NAT444

1. Use STUN server to discover opening port
2. Use UPNP to enable port forwarding at RG
3. UDP/TCP services allowed
TCP/UDP port usable

RG assigned with public IP

0

Usable

65,535

RG assigned with private IP w/ CGNAT

1024

Port Block Allocation

1055

Need to detect
- Public IP
- Usable port
Other

• Use URI to retrieve port mapping from Service provider
  • URI /ipport/
    • E.g. 100.1.1.1:1040

  • URI /ipportrange/
    • E.g. 100.1.1.1:1024:1031