Enhanced Port Forwarding functions with CGNAT

draft-chan-tsvwg-eipf-cgnat-02.txt

Louis Chan
Juniper Networks
IETF 116, Mar 2023
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
  - The hole punching method needs a common 3rd party server
    - Synchronizing actions within a time window for successful connection.
      - e.g. due to 120sec for UDP session timeout

• This needs a solution working for TCP (plus UDP) under CGNAT
  • Each party could run asynchronously, and the solution does not mandate a common server for hole punching

• It requires CGNAT to support EIPF (Endpoint Independent Port Forwarding)
  • Compatible with EIM
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 SRC port per private IP
• Allow chain of forwarding of the same DEST port from CGNAT, RG (Residential Gateway) and hence to the end device
  • Note: One TCP/UDP could only be forward to ONE selected private IP behind RG in incoming direction.
    • E.g. public 100.1.1.1:1024 could only point to one private IP, like 10.1.1.20 for incoming session, and then to 192.168.1.10 which is behind the RG.
    • But multiple devices behind the RG, depending on configuration, could potentially be allowed to share 100.1.1.1:1024 as SRC port for outgoing connections. CGNAT needs to check the existing NAT session table first, if any.
      • Devices (192.168.1.10-12) behind RG could share 200.1.1.1:1234.
      • (To be discussed later in this deck)
Demo: incoming TCP session for NAT444

1. Use STUN to discover opening port (1035 in this demo)
2. Use UPNP to enable port forwarding at RG
3. TCP services allowed
PC1@192.168.20.100

1. checking stun
   XorMappedAddress = 50.152.214.89:1035

2. request to RG via upnp
   external 192.168.1.11:1035 TCP is redirected to internal 192.168.20.100:1035 (duration=0)

3. start http server
   Try http://58.152.214.89:1035

   =======
   ssh/sftp service
   using similar procedure
   XorMappedAddress = 50.152.214.89:1035
   Try ssh -p 1037 louis@58.152.214.89

   root@debian8-upnp:/home/louis/upnp#

Public IP w/ external port 1035 detected

Start http server locally with port 1035

Request to RG for port mapping TCP 1035 to local host

Use the same procedure, and redirect port 1037 at RG to local ssh port 22
PC2: Test the Web service

Access the web server via http://58.152.214.89:1035

This is a placeholder page installed by the Debian release of the **Lighttpd server package**.

This computer has installed the Debian GNU/Linux operating system, but it has nothing to do with the Debian Project. Please do not contact the Debian Project.
PC3: Access the ssh service

Access the ssh via 58.152.214.89:1037 from public internet
Port forwarding@RG Request via UPNP for TCP port 1035 and 1037
EIPF and Existing NAT session table

With the mentioned procedure, the source port mapping from CGNAT -> RG -> PC1
100.1.1.1:1024  -> 10.1.1.20:1024  -> 192.168.1.10:1204

But, port 1024 is not only used by PC1.

Behind RG, there are additional PC1a, 192.168.1.11 and PC1b, 192.168.1.12, and all of these can share port 1024 for outgoing at CGNAT. For example, in outgoing direction

<table>
<thead>
<tr>
<th>dest ip:port</th>
<th>src ip:port@PC</th>
<th>src ip:port@RG</th>
<th>src ip:port@CGNAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC1a 2.2.2.2:888</td>
<td>192.168.1.11:1234</td>
<td>10.1.1.20:4444</td>
<td>100.1.1.1:1024</td>
</tr>
<tr>
<td>PC1b 3.3.3.3:999</td>
<td>192.168.1.12:5678</td>
<td>10.1.1.20:5555</td>
<td>100.1.1.1:1024</td>
</tr>
</tbody>
</table>

There are two sessions appeared in internet (src 100.1.1.1:1024, dst 2.2.2.2:888) and (src 100.1.1.1:1024, dst 3.3.3.3:999).

Procedure
1. First, CGNAT should honor the existing NAT session table first as above
2. For unknown ip+port, the EIPF function will enforce the translation to 10.1.1.20:1024
Others

• Demo video on youtube
  • https://is.gd/mn16ju

• We seek comments and usefulness in live situations