Network Working Group
INTERNET-DRAFT
Intended status: Standard Track
Expires: Aug 21, 2022

Louis Chan

Juniper Networks
Feb 21, 2022

Enhanced Port Forwarding functions with CGNAT
draft-chan-tsvwg-eipf-cgnat-00.txt

Abstract

There is a need for peer-to-peer (P2P) communication under the use of CGNAT in service providers. With the combination of home gateway, this becomes NAT444.

In RFC5128, methods of using UDP hole punching solves the problem partially when EIM (Endpoint-Independent Mapping) is supported in NAT device in the path, and there exists a common rendezvous server.

The success rate of UDP hole punching is high, but not TCP hole punching in practical world. Also, the P2P solution requires a common server in the public internet to exchange the IP and port information.

In this draft, a method is described to achieve incoming TCP or UDP session without a common rendezvous server in NAT444 situation.

Status of this Memo

This Internet-Draft will expire on Aug 21, 2022.

Copyright Notice

Table of Contents

1. Introduction 2
2. Conventions used in this document.................................... 3
3. Port acquiring procedure in Application.............................. 3
4. Endpoint Independent port forwarding (EIPF) Enhancement 4
   4.1. When this feature enabled in CGNAT with EIM..................... 4
   4.2. When this feature is enabled in CGNAT with both EIM and EIF 4
5. Retrieval of IP and port information via HTTP........................ 5
   5.1. IP and port - URI /ipport/ 5
   5.2. IP and port range - URI /ipportrange/........................... 5
6. Compatibility 6
7. Security Considerations 6
8. References 6
   8.1. Normative References 6
   8.2. Informative References 6
9. Acknowledgments.. 7

1. Introduction

The purpose of this document is to describe to a way to allow incoming TCP or UDP sessions under NAT444 situation.

The success rate of TCP and UDP session would be guaranteed under this proposal.

There would be two sections in the draft.

- The first section describes a procedure for an application in end device to detect and allocate TCP or UDP port for its use for incoming session. The required tools are STUN [RFC5389] and UPNP [RFC6970].

- The second section describes a method for residential gateway RG to discover the usable port range under a CGNAT deployment with port-block-allocation. In turn, the home gateway could allocate TCP or UDP to the end devices via UPNP, NAT-PMP [RFC6886] or PCP [RFC6887].

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in RFC 2119.

3. Port acquiring procedure in Application

```
        PC1-----RG-------CGNAT------Internet------PC2
                                        |
                                        +-----STUN server
```

- Private network: PC1: 192.168.1.10, RG: 192.168.1.1
- WAN: RG: 10.1.1.20, CGNAT: 10.1.1.1
- CGNAT: public IP 100.1.1.1
- PC2: public IP 201.1.1.10

Here is an example of step to acquire a TCP or UDP port

- Application in PC1 sends a STUN request to STUN servers in public internet. The STUN server would reply the XOR-mapped-address. E.g.

```
      100.1.1.1:1024                      ;public ip is 100.1.1.1 with port 1024
```

This detects both public IP address and the UDP port available. This assumes the same TCP port is also available since most CGNAT implementations allocate the same port number for both TCP and UDP with EIM enabled.

The application will then send UPNP request to residential gateway RG, 192.168.1.1, for port forward TCP port 1024 to the local device IP, 192.168.1.10.

- CGNAT, due to PBA allocation and a special setting enabled, TCP traffic sent to 100.1.1.1:1024 as destination would be forwarded to RG 10.1.1.20:1024 without changing port value. Then, RG would pass the TCP traffic to PC1 with 192.168.10.1:1024 as destination due to the registration of UPNP. In this case, PC2 could initiate a direct TCP session to PC1 via 100.1.1.1:1024.

- UDP would work in the same way. Any host in the internet could create TCP or UDP session directly with the application in PC1

The above procedure assumes both RG and CGNAT have EIM capability enabled.

The application in PC1, optionally, could release the UPNP mapping after finishing the session.

4. Endpoint Independent Port Forwarding (EIPF) Enhancement

4.1. When this feature enabled in CGNAT with EIM

- the associated TCP or UDP port is UNCHANGED for the inbound traffic if there is no matching session in the NAT table.
- only the IP address is going through NAT process. That is changing the public IP to a private IP
- It is working like port forward function in a NAT44
- In the example, any IP source address, 202.1.1.1 or 222.1.1.1, sending traffic to 100.1.1.1:1024. CGNAT would translate the traffic as 10.1.1.20:1024 as destination.
- UDP hole punching would be compatible if the UDP session is still in RG and CGNAT session table. Port 1024 would follow the translation.

4.2. When this feature is enabled in CGNAT with both EIM and EIF

- EIF (Endpoint-Independent Filtering), described in RFC5128, will happen only if the external host already has a session through EIM.
- The TCP or UDP port is kept UNCHANGED for any other external hosts sending inbound traffic.
- For example, there is a session originated from PC1 to PC3, 201.1.1.20

```
         PC1-----------RG----------CGNAT-----------Internet---------PC3
                                                       |
                                                       +---------------------
PC4

     Src: 192.168.1.10:3333    10.1.1.20:4444          100.1.1.1:1033

     Dst: 201.1.1.20:5555      201.1.1.20:5555         201.1.1.20:5555
```

When PC3 sends traffic with different source port, 201.1.1.20:6666 and destination 100.1.1.1:1033, CGNAT should honor the EIF behavior. It would be translated back to 10.1.1.20:4444.

When other host without any session established through EIM, and it sends traffic with destination port 1033, the port 1033 should not be changed at CGNAT.

When PC4 send traffic to 100.1.1.1:1033, the port 1033 is kept UNCHANGED. PC4 has no previous established sessions with PC1.

This behavior is an optional implementation with EIF enabled. Another option is to make EIPF and EIF exclusive.

5. Retrieval of IP and port information via HTTP

The internet service provider host a HTTP web server for the enquiry of IP and port information. Two URIs are suggested

5.1. IP and port - URI /ipport/

With the URI /ipport/, the HTTP response is clear text with IP:PORT, where IP is the external public IP address and the PORT is external port as seen.

For example, the response is

```
100.1.1.1:1040
```

The HTTP response should be human readable with a web browser.

Although TCP port 1040 is seen here, it is assumed that UDP port 1040 is also available from CGNAT for incoming mapping.

5.2. IP and port range - URI /ipportrange/

With the URI /ipportrange/, the HTTP response is clear text with

```
IP:PORT_START:PORT_END<LF>

IP:PORT_START:PORT_END<LF>

IP:PORT_START
```

Where <LF> is ASCII character for line feed.

The response is a human readable format in a normal web browser.

For examples, here are valid responses

a) Single line

```
100.1.1.1:1024:1031
```

Port range 1024 to 1031 assigned for both TCP and UDP.

b) Two lines

```
100.1.1.1:1024:1031

100.1.1.1:1064:1071
```

Port ranges 1024 to 1031 and range 1064 and 1071 are assigned for both TCP and UDP.

It is possible to have multiple port block allocated to the same private IP address
from CGNAT perspective.

If the RG device or application could not support multiple entries of IP and port range, it should take one of the lines, preferably the first line.

Human user or RG could use this information to plan for incoming services. For example, when PC1 requests a TCP 8888 port forward from RG via UPNP [RFC6970], NAT-PMP [RFC6886] or PCP [RFC6887], RG would counter offer another TCP port 1031.

6. Compatibility

TBD

7. Security Considerations

TBD

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[RFC5128] Srisuresh, P., Ford, B., and D. Kegel, "State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)", March 2008.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", October 2008.

[RFC6886] S. Cheshire and M. Krochmal. NAT Port Mapping Protocol (NAT-PMP), April 2013.

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P.

Selkirk, "Port Control Protocol (PCP)", April 2013.

[RFC6970] Boucadair, M., Penno, R., and D. Wing, "Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF)", July 2013

9. Acknowledgments

The following people have contributed to this document:

Author Address

Louis Chan (editor)
Juniper Networks
2604, Cityplaza One, 1111 King's Road
Taikoo Shing
Hong Kong

Phone: +852-25876659
Email: louisc@juniper.net