NAT

About

About text.

Introduction

NAT, or Network Address Translation, is a necessary evil in the world of network computing. FreeSWITCH tries **very** hard to make your life easier when dealing with NAT scenarios. One problem, however, is that there are differing devices with unpredictable behavior that can make it seem like your FreeSWITCH server is misbehaving. If you're stuck in a NAT situation then be aware that you may face challenges in getting everything on your network all working.

Further Reading

First off, here is a discussion of NAT at Wikipedia for those inclined to dig deeper.

BKW's Audio Presentation

2010-08-18

On August 18, 2010 Brian K West (bkw) gave a brief overview of NAT and FreeSWITCH. You may download the audio here:

- MPEG
- Ogg

2014-01-22

The torrent link no longer works, if you have the audio add it or comment below that you have it and we can obtain it and add it

On Jan 22, 2014 Brian K West (bkw) gave another more indepth overview of NAT and FreeSWITCH. You may download the audio here:

- TORRENT
- You can also view a partial transcript here

Steve Ayre's Excellent Writeup

Steven Ayre wrote up a really nice answer on the mailing list. It is copied verbatim here:

One problem with SIP ALG(Application-Level Gateway)(apart from the varying implementations which mean some work much better than others) is that it absolutely cannot work with SIP TLS - for obvious reasons, it can't see inside or rewrite the encrypted data.

Fair enough if that's the only way you found that worked for you, and if isn't broken don't fix it. :o)

Still, I do suggest people at least try to get their SIP clients handling NAT traversal correctly first.

Unfortunately there's no one true answer to getting NAT traversal working. The reason is that different SIP clients, NAT, firewall settings and implementations mean what works somewhere might not work elsewhere. That of course makes it harder to manage clients at multiple sites, roaming clients, etc.

The first thing to try would be to disable SIP ALG (if your phone is handling NAT correctly some might then rewrite the correct packet breaking it) and enable STUN on your SIP client.

STUN is a useful mechanism where you can talk to the STUN server from your internal address (IP+port) and it will tell you what your external address (IP+port) is. You can then use a trick called UDP hole punching whereby any server online can send to that external address and the NAT mapping will deliver it to your internal address. So your SIP client can learn its external SIP and RTP addresses and fill in the correct Contact header and SDP values. (Assuming SIP ALG is either disabled or intelligent enough not to then rewrite the correct values and break it). FreeSWITCH then has valid addresses it can send SIP responses and RTP media to.

That makes some assumptions though:
1) Your SIP client supports STUN (not all do)
2) Your NAT implementation maps your internal address to the same external port talking to any server. Some don't, mapping to a different port for each server.
3) Your firewall will allow packets to that external port from servers it hasn't spoken to. Personally I have to reduce the security level of my home router's firewall (O2 Broadband) from '' to 'Standard'. I suspect this is why.

This all applies to a number of protocols the same approach to traverse NAT. P2P clients, VoIP, VPNs (tinc), online gaming (eg Call of Duty) etc. If you can get CoD to tell you your NAT type is 'Open' you're probably ok. ;o)

If you can't get the correct IPs in Contact & SDP, you have a few fallback options in FreeSWITCH.
1) NDLB-connectile-dysfunction will change the Contact to the address the INVITE came from. Probably correct in 99% of cases.
2) FreeSWITCH can auto-adjust its RTP address. It tells the client where to send RTP to, and when it receives it it changes the SDP address to send audio back to there. Again probably correct in 99% of cases, but with an unfortunate but unavoidable sideaffect that the caller will hear absolutely no audio until shortly after they send RTP. That probably won't be until the call is actually answered, so they will never hear ringback and the first second of the call might get lost.

NAT devices have a limited number of ports and memory. As such old/unused mappings get removed from the table. You therefore need to make sure you keep the port mapping active. During a call you'll want to enable SIP keepalives to send a SIP request periodically to keep the port open, so that you can receive call state updates. When registering you'll periodically send REGISTER to keep your registration active, so that'll do it for you. In any case though you want to make sure they're sent frequently enough that your particular NAT router doesn't timeout the mapping. Every 30s should be fine.

If absolutely all else fails, your other option is to use a VPN to bypass the NAT entirely. I find OpenVPN over UDP works very well for that, and is very easy to set up. If you want to save load/bandwidth on the VPN server you could also use bypass_media and tinc which is a P2P VPN - sites join any public node and using UDP hole punching can try to talk directly to one another even behind NAT, but if that fails can still route packets via the public nodes.

NAT in FreeSWITCH

In June 2009 the FreeSWITCH developers added code that makes it possible for FreeSWITCH to leverage the utility of UPnP and NAT-PMP devices. A number of home routers support UPnP or NAT-PMP, in some cases both. This includes the ubiquitous WRTG54G. If your NAT device does not support UPnP or NAT-PMP then you will be forced to use some of the less elegant solutions like STUN.

Many people suffer from NAT issues which come from a misunderstanding of how SIP, RTP and FreeSWITCH work. The topic comes up frequently in the IRC chat room. Please see the following links to aid you in your endeavors.

NAT Info

- Auto NAT - This page discusses how to take advantage of FreeSWITCH and the new NAT-busting features.
- External profile - this covers the topic of what makes the external profile so NAT traversal friendly in regards to SIP and RTP protocols. Also, this roughly covers the concept of copying from the external profile and creating a new profile that will enable you to cleanly traverse your NAT /firewall situation.
- NAT Traversal - General information regarding NAT and devices.

NAT just works!

For sip you can set your SIP IP to a STUN server like "stun:stun.fwdnet.net" or to your external non-NAT IP. If you have a dynamic public IP address and use a Dynamic DNS service, you can set your SIP IP to host:your.dns-host.name, and FS will do a DNS lookup to determine your public IP address. For RTP you set the value to "auto".

```
<param name="sip-ip" value="1.2.3.4"/>
<param name="rtp-ip" value="auto"/>
```

If FreeSWITCH discovers that the registered endpoint is behind NAT, it will send SIP OPTIONS packets every 30 seconds to the endpoint to keep NAT alive. It is recommended though, that every endpoint be configured to send NAT keepalives itself.

See Also

For user NAT traversal, see NAT Traversal

Related information, ACL (Modifying NAT behavior when matching a certain access list))