What I know:

-> It's a Cisco's Intrusion Detection System.

-> Combining Active detection & Passive detection

* Status: { We know it's work on IPV4 -> Can be bypass using VPN
  We do not know if this works on IPV6 -> You can ask. Long Procedure to go through.
  └ Why? -> ISP in China don't like [give people access IPV6] & no Website in China supports that.

-> GFW now are still a blackbox, Gov doesn't admit it exist
  └ Also no "official" document.
  └ Research all based on "Poke around & see"

Basic Principle. <All based on IPV4>.

-> For http Connection request.
  ① Look into the data flow.
  ② Find Prohibit Key Word. <- A black list.
  ③ send Connection reset request to both side.

-> For https Connection request.
  ① Since it's encrypted. the black list won't work.
    └ IP block <- destination blacklist.
    └ Just hang & not establish Connection <- Ends up timeout.
  ② DNS poison. <- Most Common.
    └ Many DNS server in China gets poisoned.
      └ Redirect you to an non-exist page or Ads.
      └ Workaround: change hosts file can fix this
        └ Experiment: { Access to github.com.
                        Access to community.steampowered.com.

Network Situation:
  ① Yes, most of Chinese Website do use https
  ② Most of blocky is accomplish by drop package & DNS poison.

Runned tests:
  └ All foreign social media is blocked. -> time out / 404 Redirect.
  └ foreign Search engine gets Connection reset
  └ VPN & Connection to offshore server is allowed. (tested send.truman.edu)
  └ Discover GFW is a one-way wall
    * outside can access inside.
    * inside partially access outside.

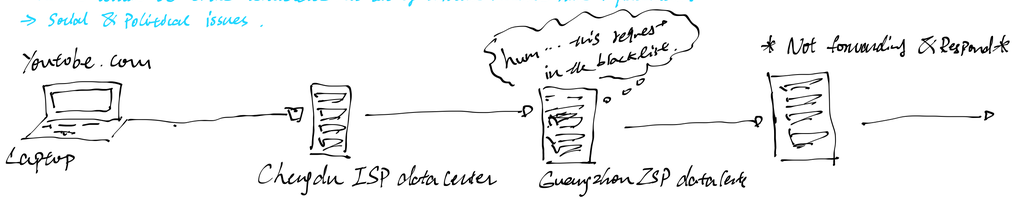
Blacklist & Whitelist.

-> Currently the GFW using blacklist.

-> For some part of china like Fujian, Xinjiang has start trying to use Whitelist on some city.

-> Future would be entire Whitelist. as all of software/website have replacement.

-> Social & Political issues.



Experiment.

nslookup twitter.com -> 104.244.42.1

openssl s_client -connect <:443 -tls1_3

└ Respond to 404.

└ Respond time out <- Server not respond

Side note: There only 3 ISP in China. All of them were national owned. and administrate by government.

* China Telecom
* China Unicom
* China mobile.

} want internet? must use one of those.

-> Go global internet must pass one of these "custom" Server.

* Southern zone go to Guangzhou
* Middle part go to Shanghai
* Northern part go to Beijing.

} Internet backbone
Going foreign or coming back

-> Internet access control also happened in those three datacenters.

In China, we don't have public IP. Everything were in a big intranet.

Routers everywhere, ISP is a huge Router. -> Carrier grade NAT

The process connection would be.

Laptop -> Community NAT -> City ISP -> Provincial ISP -> Global Custom server.

The site being blocked were mostly the social media / Wiki / Search engine.

Some of site like Github can access by modifying hosts file.

└ Not support https download. but ssh works perfectly.

Solution to GFW blocking.

-> Most Common is using a VPN <But it's illegal>

-> For company can spend a lot of money to purchase a line that

Could Connect to the global internet <legal. most foreign company done that.

But it's SUPER EXPENSIVE>

-> Relay Server in HK. it's like a jumper <Grey area> -> VPS is most people using

-> Change DNS <It worked before 2019. But not so much after 2019>

Problem I have:

① What I should looking at?

② The structure of GFW was simpler than I thought.

But it's so effective. should I looking for a way to break it or to enforce it? -> Sounds mostly is the political issue.

③ No one use. few people know IPV6 in China. Is it worth it to investigate?

④ Not much paper supports GFW & Government deny it exist.

⑤ I don't know what I should do research on.

Source from gfw.report. and online forums.

Not much paper talk about this.

-> Also. a lot of repository on Github being deleted / no longer updated.

J. Crandle.

Giovanni Vigna -> UCSB

① Generalize to other firewall. (Campus-firewall).