Network Admins Hate Him!

Local noob bypasses firewall with ONE WEIRD TRICK

FortiGuard Application Control

Application Blocked!

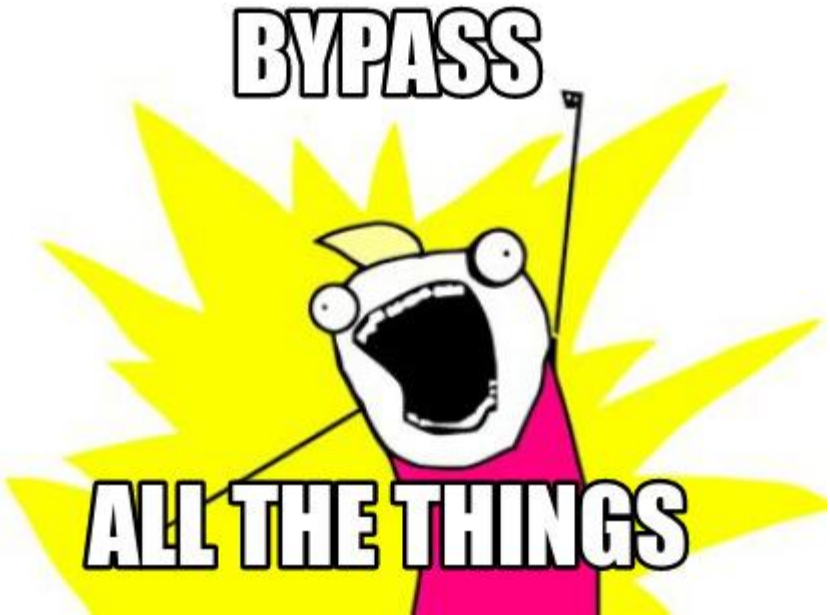
You have attempted to use an application which is in violation of your internet usage policy.

Stream.Media

Category: Video/Audio
URL: http://stream.rib.dataprodigy.my:16731/;stream.mp3
Client IP: 10.0.2.118
Server IP: 50.22.219.97
User name:
Group name:
Policy:
FortiGate Hostname: FG300B3909603181

Agenda

1. Easy bypass tricks
2. Proxies and VPNs
3. SSH Tunnels
4. Alternative protocols
5. DPI Evasion
6. Domain Fronting

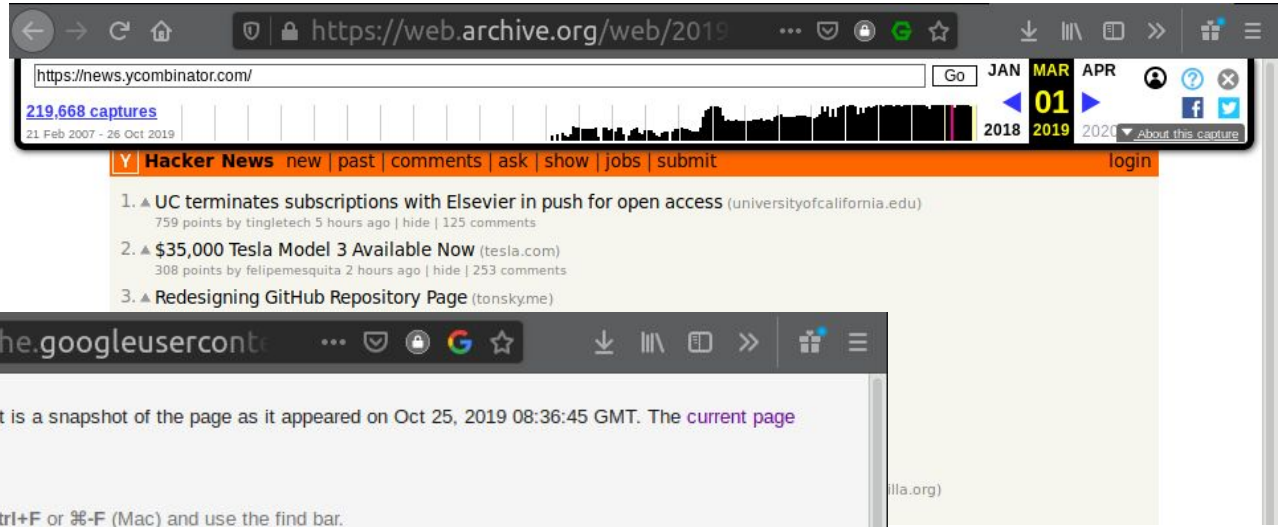


Easy Bypass Tricks

Using Web Caches

https://webcache.googleusercontent.com/search?q=cache:http://news.ycombinator.com

https://web.archive.org/web/20190301001958/https://news.ycombinator.com/

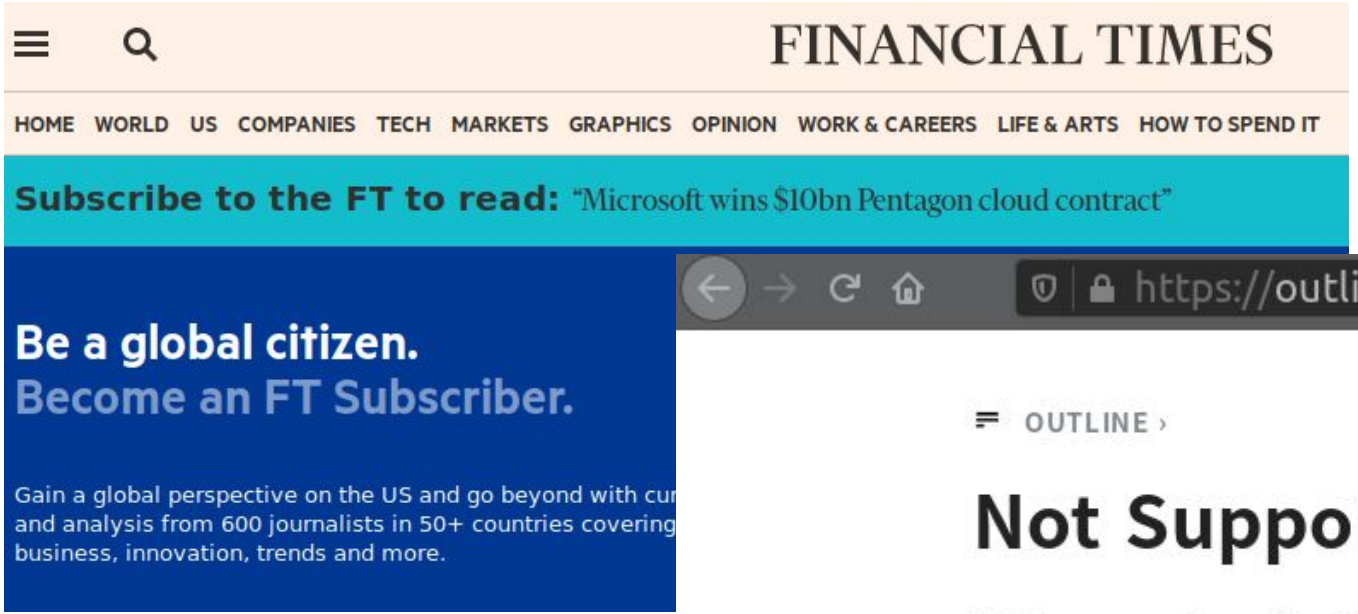


Bypass paywalls for news sites

https://outline.com/https://www.bloomberg.com/news/articles/2019-10-25/pg-e-warns-of-biggest-blackout-ever-as-windstorm-approaches?srnd=premium

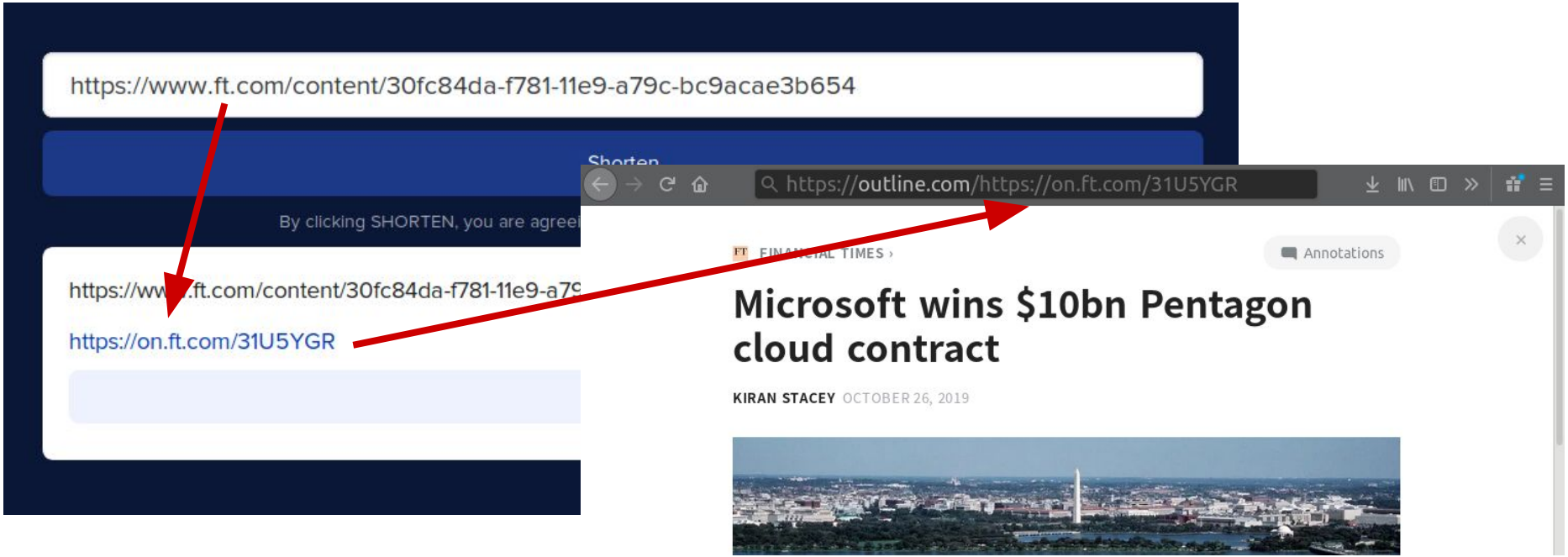
Bypass paywalls for news sites

https://outline.com/https://www.ft.com/content/30fc84da-f781-11e9-a79c-bc9acae3b654



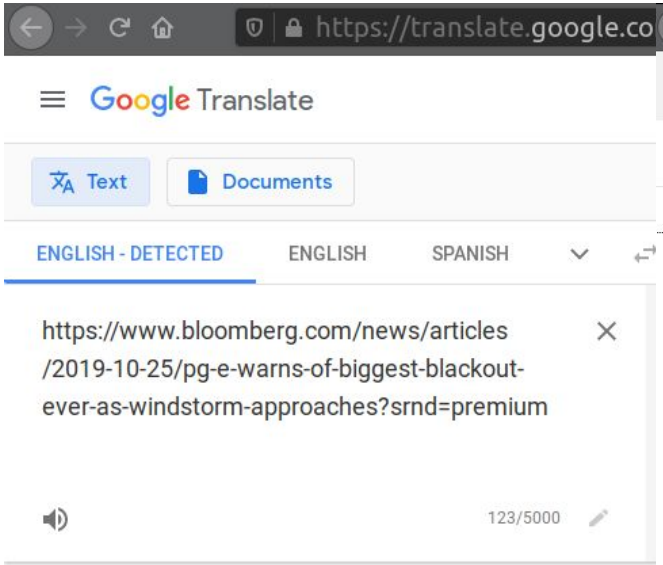
Bypass paywalls for news sites

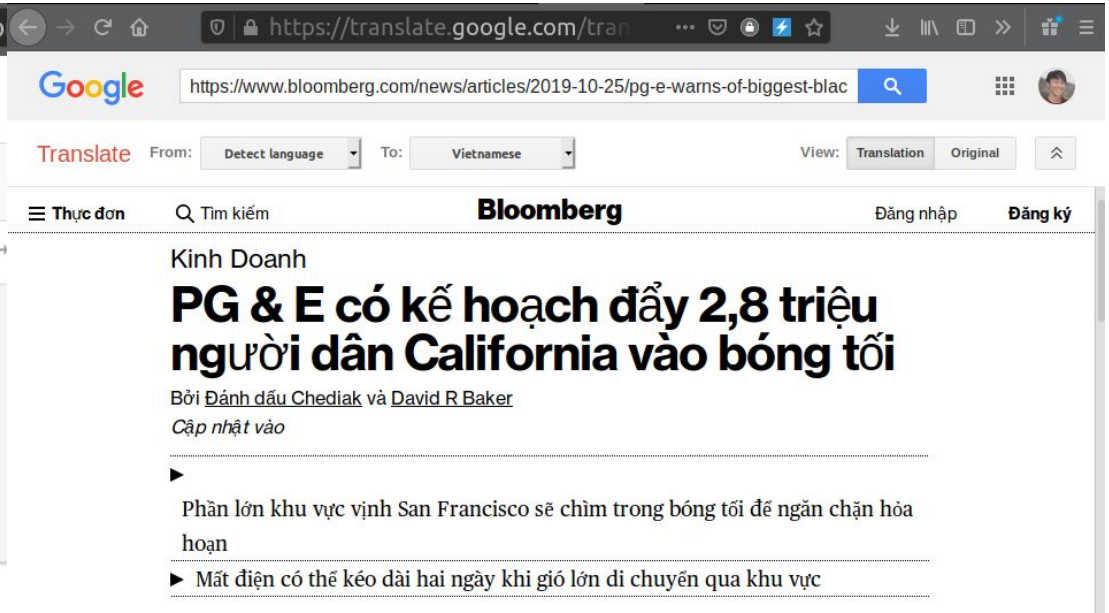
https://outline.com/https://on.ft.com/31U5YGR



Using Google Translate

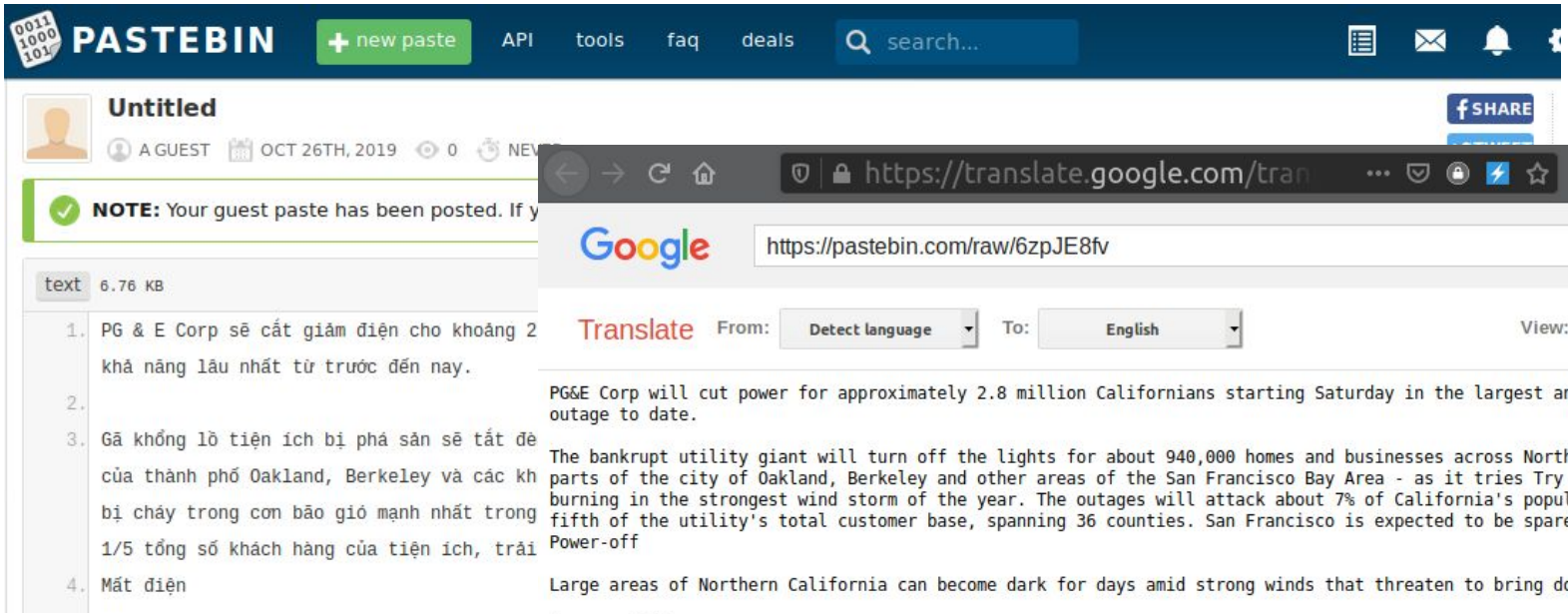
https://translate.google.com/translate?hl=&sl=auto&tl=vi&u=https%3A%2F%2Fwww.bloomberg.com%2Fnews%2Farticles%2F2019-10-25%2Fpg-e-warns-of-biggest-blackout-ever-as-windstorm-approaches%3Fsrnd%3Dpremium





Translate the Translation

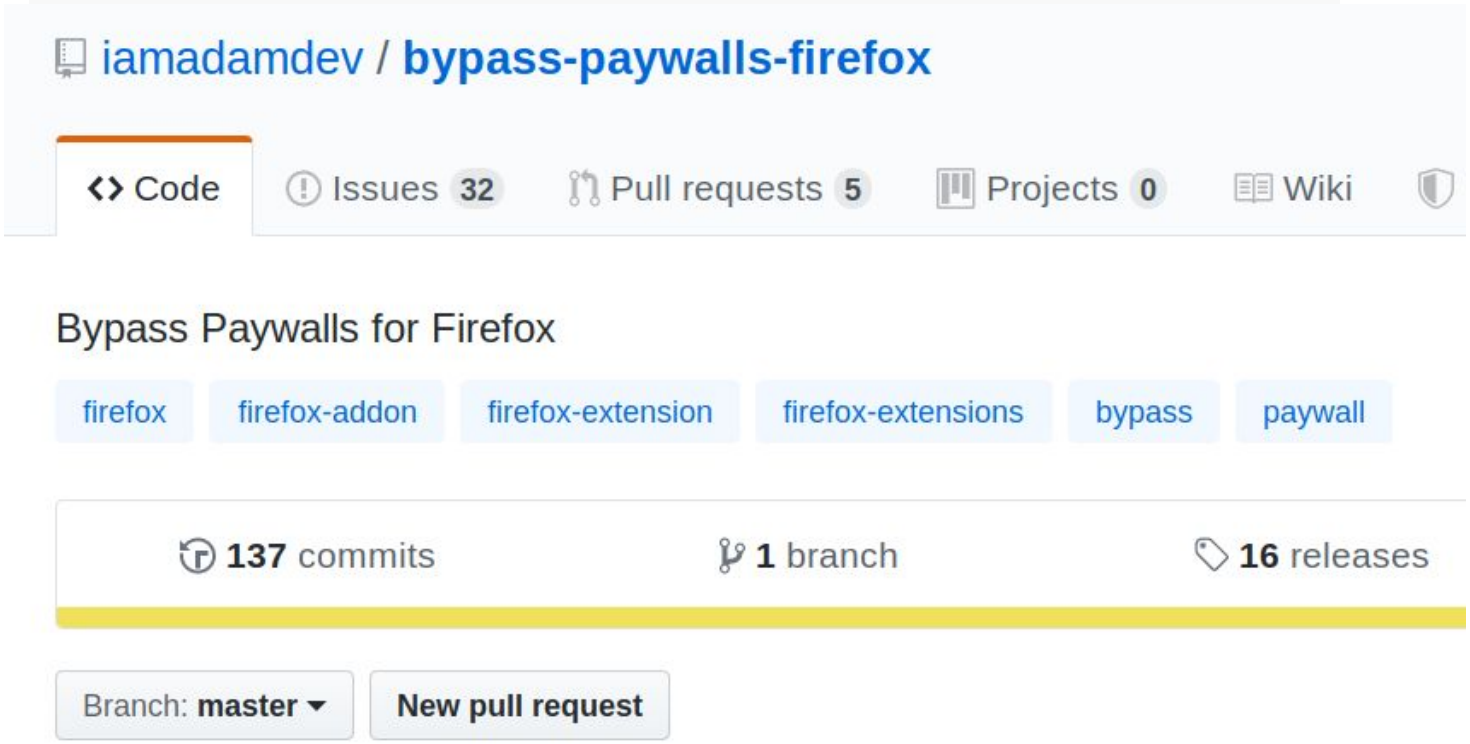
https://translate.google.com/translate?sl=auto&tl=en&u=https%3A%2F%2Fpastebin.com%2Fraw%2F6zpJE8fv



English

German
Dutch
Norwegian
Spanish

Bypass paywalls for news sites



Proxies & VPNs

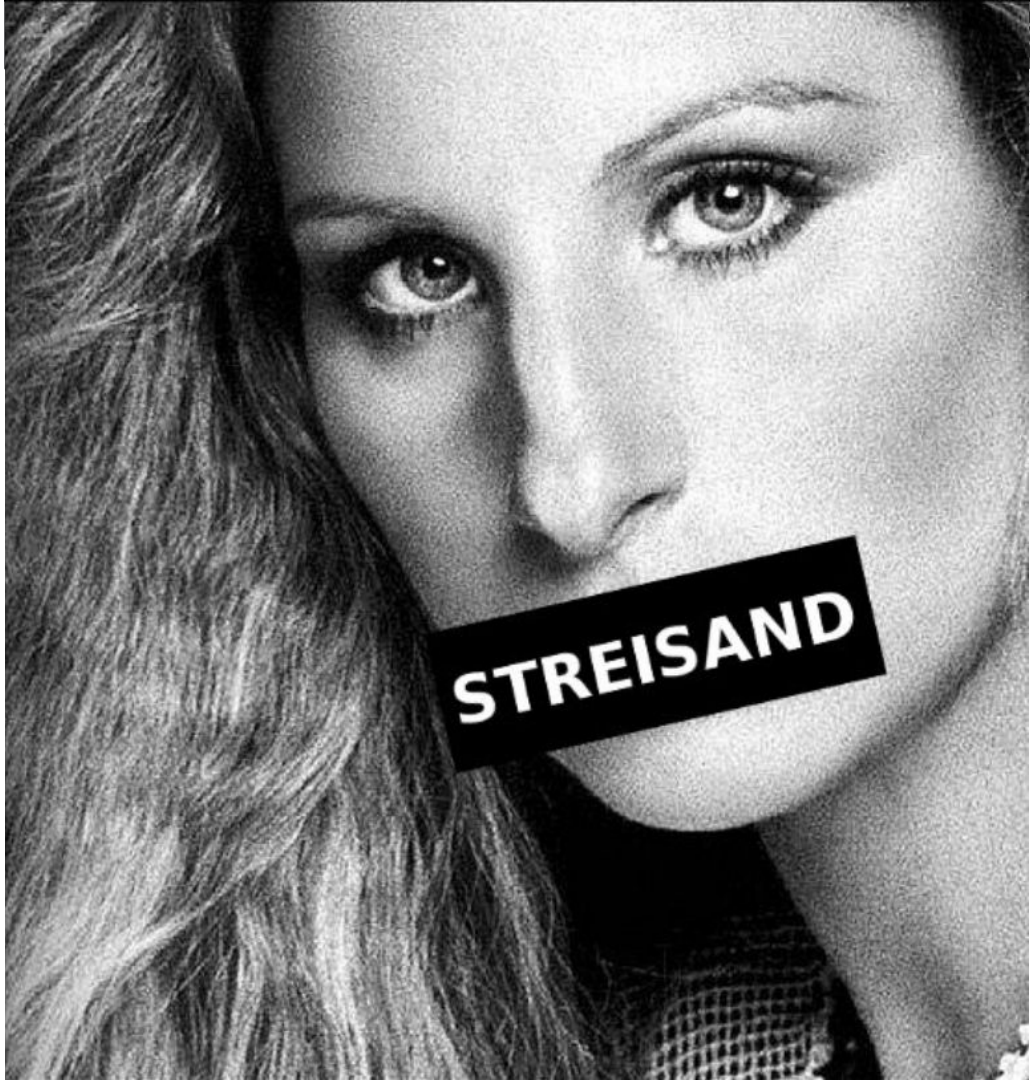
Whoops, something went wrong...

Streaming Error

You seem to be using an unblocker or proxy. Please turn off any of these services and try again. For more help, visit netflix.com/proxy.

Don’t use them*

Roll your own.
It’s easier than you think.



StreisandEffect / **streisand**

Watch 624 | Star 19.7k | Fork 1.7k

Code | Issues 135 | Pull requests 22 | Projects 0 | Wiki | Security | Insights

Streisand sets up a new server running your choice of WireGuard, OpenConnect, OpenSSH, OpenVPN, Shadowsocks, sslh, Stunnel, or a Tor bridge. It also generates custom instructions for all of these services. At the end of the run you are given an HTML file with instructions that can be shared with friends, family members, and fellow activists. https://twitter.com/streisandvpn

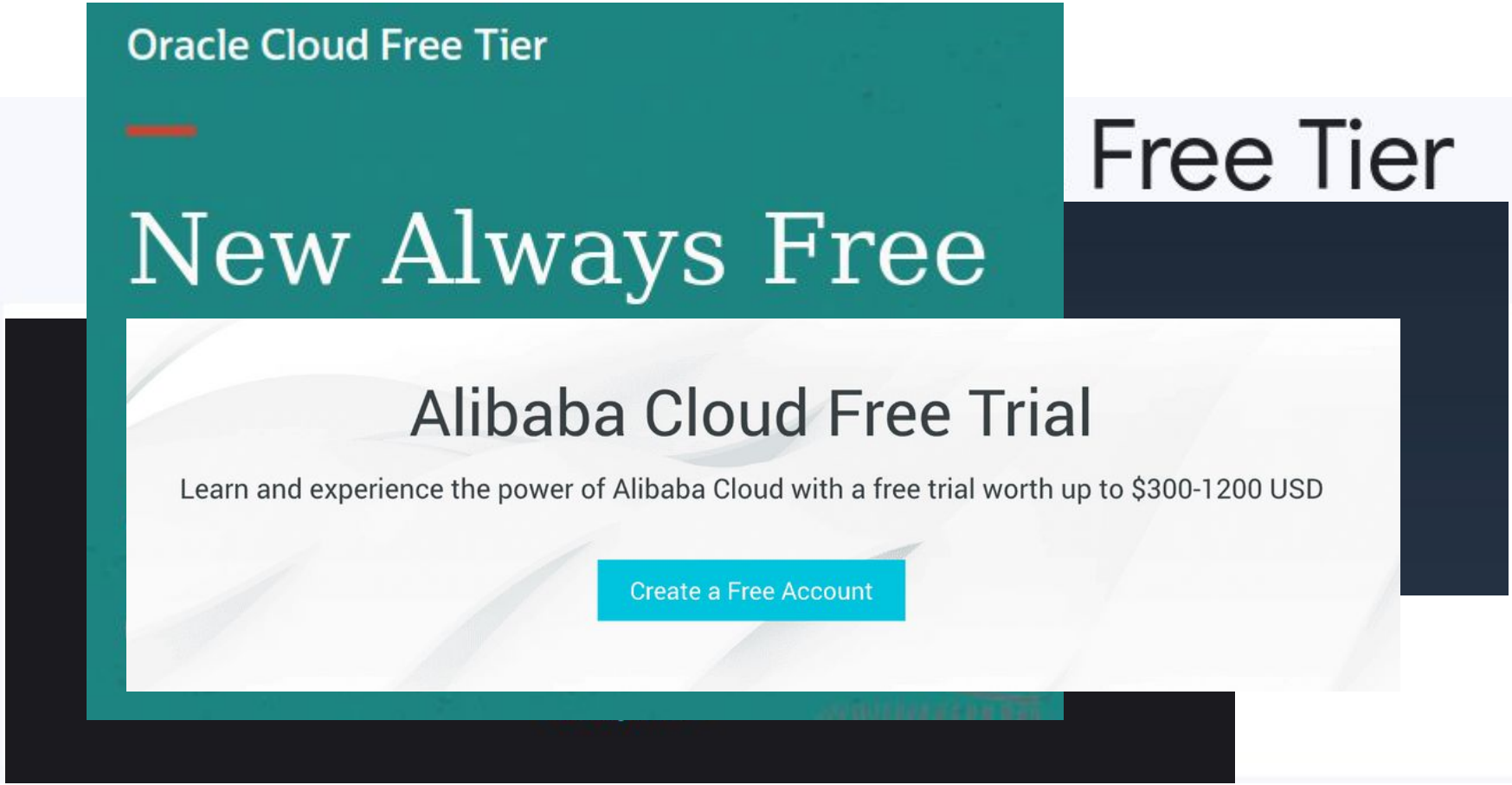
vpn ansible openvpn wireguard openconnect anyconnect shadowsocks stunnel tor ssh streisand censorship

1,402 commits | **7** branches | **0** releases | **127** contributors | View license

Branch: **master** | **New pull request** | **Create new file** | **Upload files** | **Find file** | **Clone or download**

CorbanR and **alimakki** Update corban@raunco.co gpg key (#1654) — Latest commit `be8e7a1` 15 days ago

.github	Update all Github repository links. (#983)	2 years ago
deploy	Rename vars.yml (#1536)	7 months ago
documentation	Add IncludeSec audit report to repo. (#1526)	8 months ago
global_vars	ad-blocking via dnsmasq; disable cloudflared in CI	last month
inventories	Update venv builder for upstream module changes, more compatibility (#…	2 years ago


Oracle Cloud Free Tier
New Always Free
Free Tier
Alibaba Cloud Free Trial
Learn and experience the power of Alibaba Cloud with a free trial worth up to $300-1200 USD
Create a Free Account

STREISAND

Français English

Welcome to the **streisand-iowa** Streisand Gateway server. You are only moments away from an uncensored connection to the Internet.

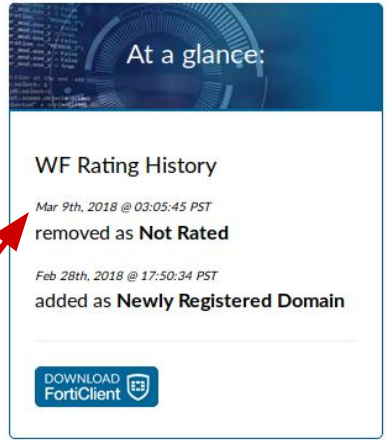
Connection Instructions

There are multiple ways to bypass censorship, and Streisand provides several choices and different protocols in the event that any of them are restricted.

- OpenConnect / Cisco AnyConnect
- OpenVPN (direct)
- OpenVPN (stunnel)
- Shadowsocks
- SSH
- WireGuard

Use High Reputation Domains & IPs

```
k@X1 ~ » curl ip-ranges.amazonaws.com/ip-ranges.json
{
  "syncToken": "1571956989",
  "createDate": "2019-10-24-22-43-09",
  "prefixes": [
     {
     "ip_prefix": "13.248.118.0/24",
     "region": "eu-west-1",
     "service": "AMAZON"
     },
     {
     "ip_prefix": "18.208.0.0/13",
     "region": "us-east-1",
     "service": "AMAZON"
     },
     {
     "ip_prefix": "52.95.245.0/24",
     "region": "us-east-1",
     "service": "AMAZON"
     },
     {
```




```
k@X1 ~ $ curl ipinfo.io/13.248.118.4
{
  "ip": "13.248.118.4",
  "city": "Dublin",
  "region": "Leinster",
  "country": "IE",
  "loc": "53.3331,-6.2489",
  "postal": "D02",
  "timezone": "Europe/Dublin"
}%
```

ExpiredDomains.net

Deleted Domains (172)

Deleted Domains | D

ccTLDs G | ngTLDs | Ca

List: Deleted .org Domai

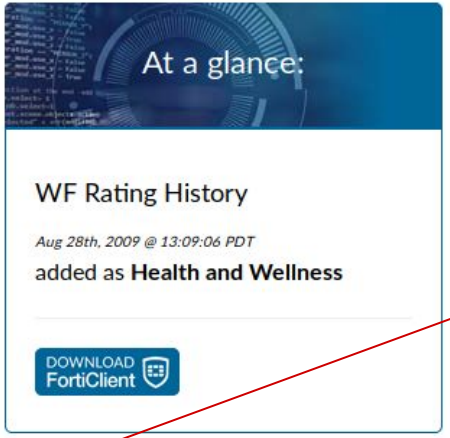
Show Filter (no Filter selec

Domain
ProjectPull.org
People-Forever.org
actstv.org
BaptistHour.org
cmcusa.org
chwo-foundation.org

FortiGuard Labs

News / Research | Services | Threat Lookup | Resou

► Home / Web Filter



Web Filter Lookup

ProjectPull.org

Submit a URL to check its Rating

5.6 +

FortiOS Version

Category: Health and Wellness

Sites that provide information or advice on personal health or medical services procedures, or devices, but not drugs. Includes self-help groups. This category includes cosmetic surgery providers, children's hospitals, but not sites of medic care for pets, which fall in Society and Lifestyle.

Click here to see if this category is currently blocked.

Request a Review

Latest Web Filter Databases 22.30959

https://luminati.io/proxy-netwo

Luminati

Residential Proxy Network

Luminati provides the most advanced Residential Proxy service offering the fastest and largest real-peer IP network in the world.

Start Now

Start Your 7-day Free Trial Today!

oxylabs

Buy Residential IPs

Data center proxies | Residential proxies | Real-Time Crawler

Basic	Pro	Enterprise
50 GB included	100 GB included	1 TB included
$12 per GB	$9 per GB	$5 per GB
$600 min. monthly commitment	$900 min. monthly commitment	$5,000 min. monthly commitment
Get started	Get started	Get started

Why choose residential proxy pool

Luminati residential peers

How do consumers join the Luminati network of peers?

Many applications (such as game applications), require their users to view a video advertisement at certain intervals, so that the game developer can generate revenues. This creates a particularly bad user experience, as it interferes with the experience of the application, wastes around 20MB of cellular data for the ad, and depletes the users' battery.

Luminati offers an attractive alternative.

When these application vendors integrate the Luminati SDK, their users are offered the alternative to not watch these video ads in return for opting in to the Luminati network. Luminati only uses their device as a node on the network when it is not in use (so never interferes with the users' experience), when the device is plugged in to power or charged, and always prefers WiFi over cellular data.

For every user that opts in to the Luminati network, Luminati pays a monthly fee to the application vendor, who passes that value on to the user by not displaying ads (or by not charging a premium for extra features in some cases).

chrome web store

kevin@pham.design

ne > Extensions > Hola Free VPN Proxy Unblocker

Hola Free VPN Proxy Unblocker

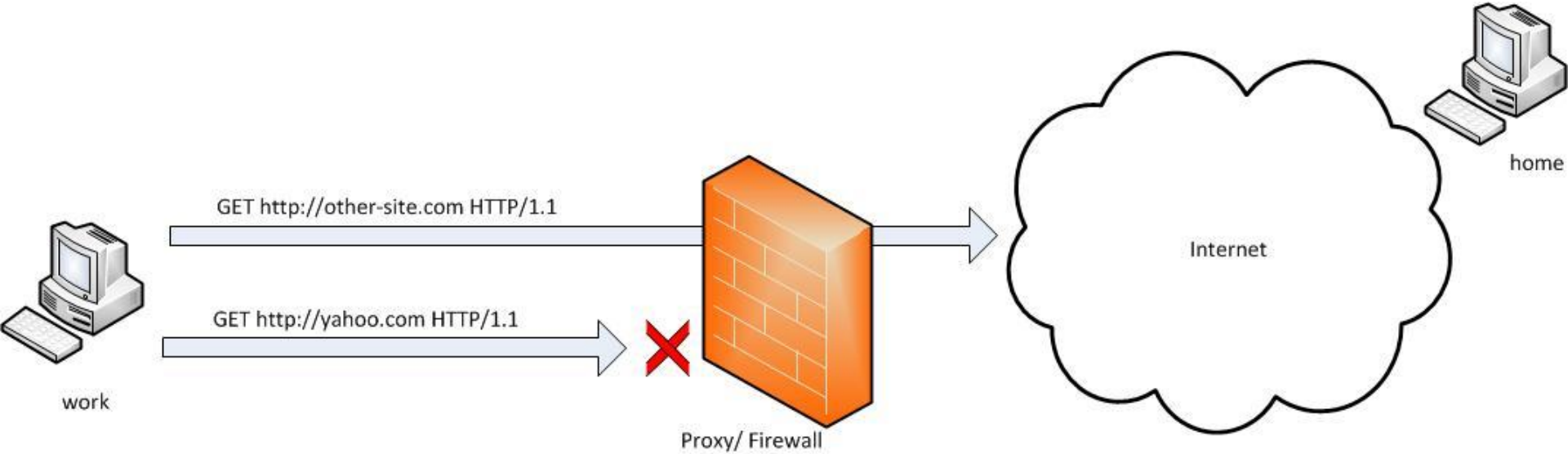
Available on Chrome

Offered by: hola.org

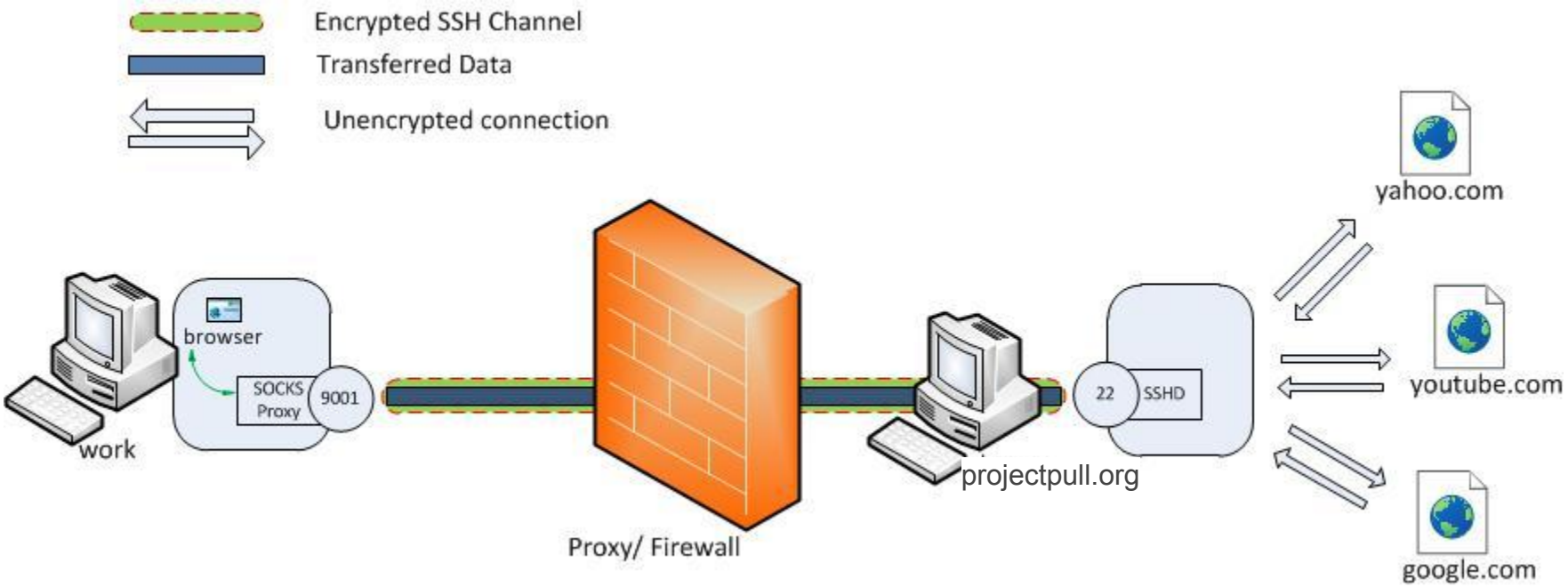
★★★★★ 338,553 | Productivity | 7,981,268 users

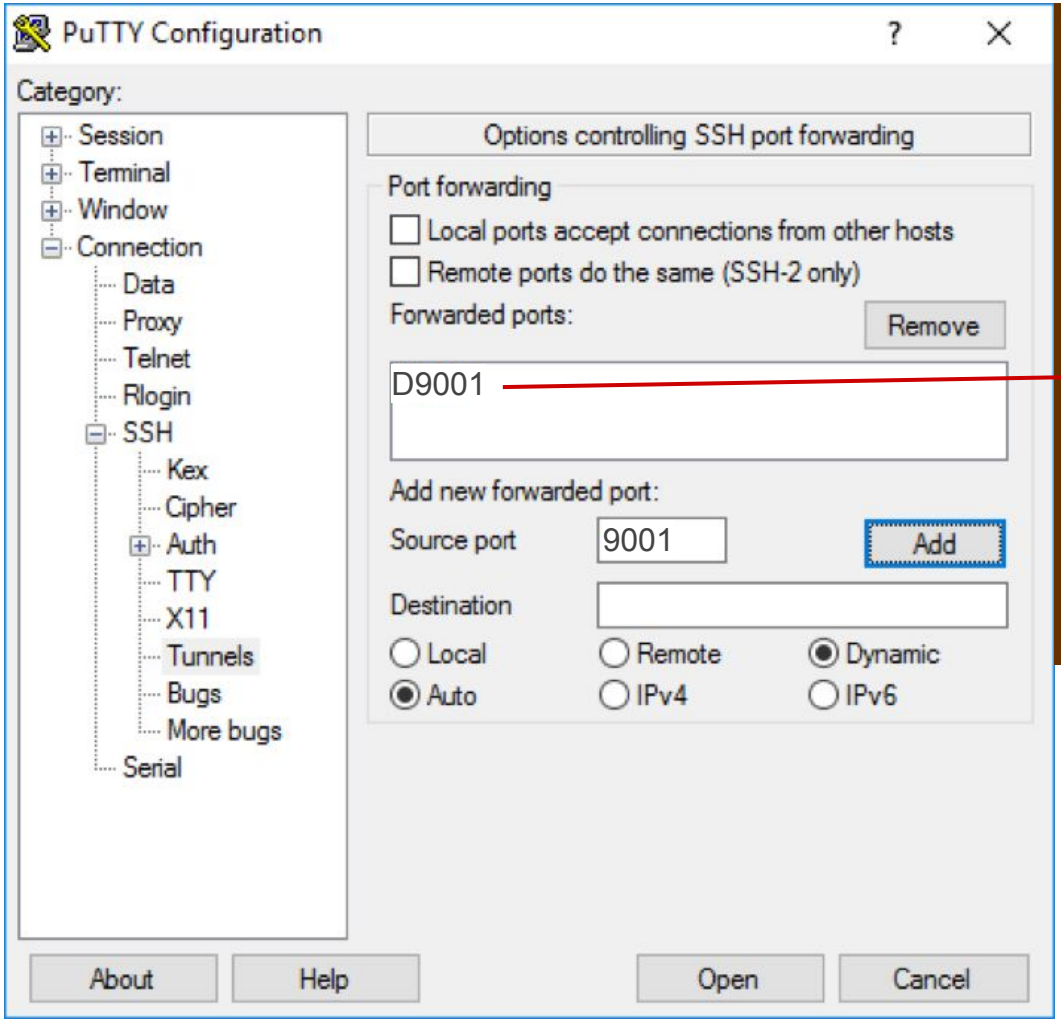
Available for Android Get it.

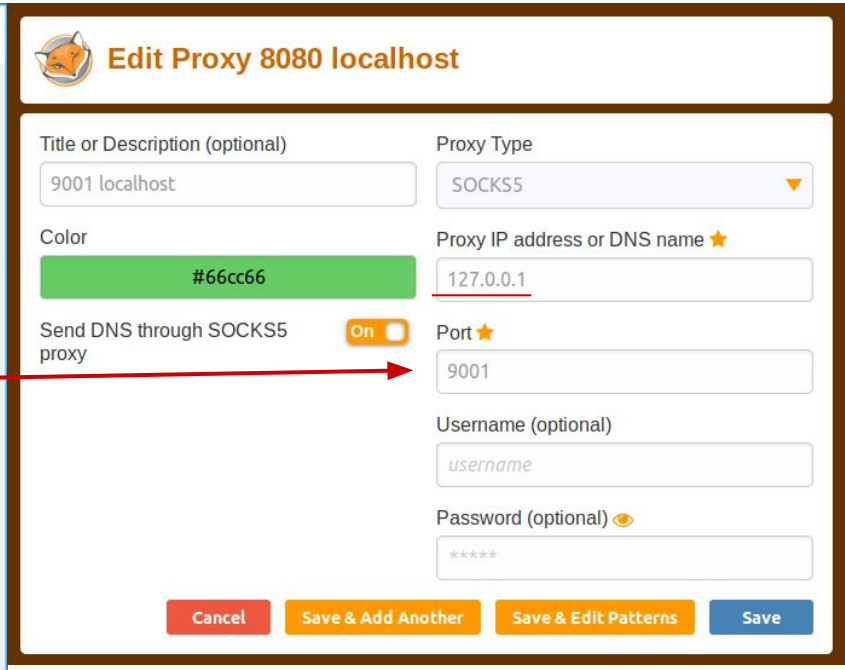
SSH Tunneling


GET http://other-site.com HTTP/1.1
GET http://yahoo.com HTTP/1.1
work
Proxy/ Firewall
Internet
home

ssh -D 9001 projectpull.org







Protip: Use SSH software that's already installed + browser extension

No local admin needed!

Protip: Use SSH config files

```
k@X1 ~ $ cat ~/.ssh/config
  Host streissand
  User          forward
  Port          443
  HostName      projectpull.org
  IdentityFile  ~/.ssh/id_rsa
  DynamicForward 9001

k@X1 ~ $ ssh streissand

OpenSSH_7.6p1 Ubuntu-4ubuntu0.3, OpenSSL 1.0.2n  7 Dec 2017
debug1: Reading configuration data /home/k/.ssh/config
debug1: /home/k/.ssh/config line 18: Applying options for
streisand-iowa-gcp-forward-443
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 104.198.220.37 [104.198.220.37] port 443.
debug1: Connection established.
```

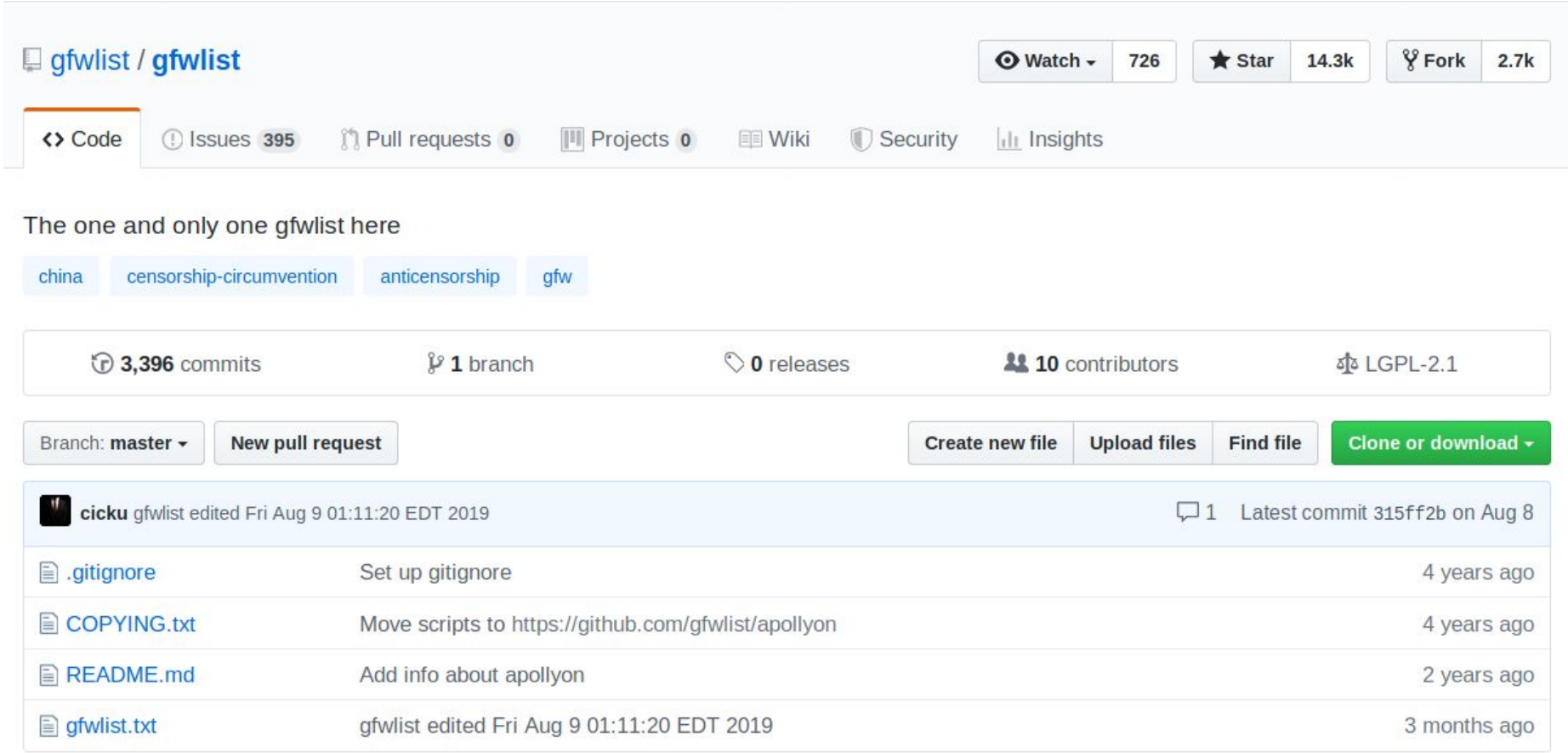
Protip: Use proxychains for specific commands only

```
k@X1 ~ $ proxychains curl ipinfo.io

ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| ipinfo.io
|S-chain|-<>-127.0.0.1:8080-<><>-4.2.2.2:53-<><>-OK
|DNS-response| ipinfo.io is 216.239.34.21
|S-chain|-<>-127.0.0.1:8080-<><>-216.239.34.21:80-<><>-OK
{
  "ip": "104.198.220.37",
  "hostname": "37.220.198.104.bc.googleusercontent.com",
  "city": "New York City",
  "region": "New York",
  "country": "US",
  "loc": "40.7143,-74.0060",
  "org": "AS15169 Google LLC",
  "postal": "10004",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}%
```

Protip: Use sshuttle to tunnel all traffic quickly

```
k@X1 ~ $ sshuttle -vr --listen localhost root@projectpull.org:22

Starting sshuttle proxy.
firewall manager: Starting firewall with Python version 3.6.8
firewall manager: ready method name nat.
IPv6 enabled: False
UDP enabled: False
DNS enabled: False
TCP redirector listening on ('127.0.0.1', 12300).
Starting client with Python version 3.6.8
c : connecting to server...
OpenSSH_7.6p1 Ubuntu-4ubuntu0.3, OpenSSL 1.0.2n  7 Dec 2017
```

Protip: only tunnel blocked traffic



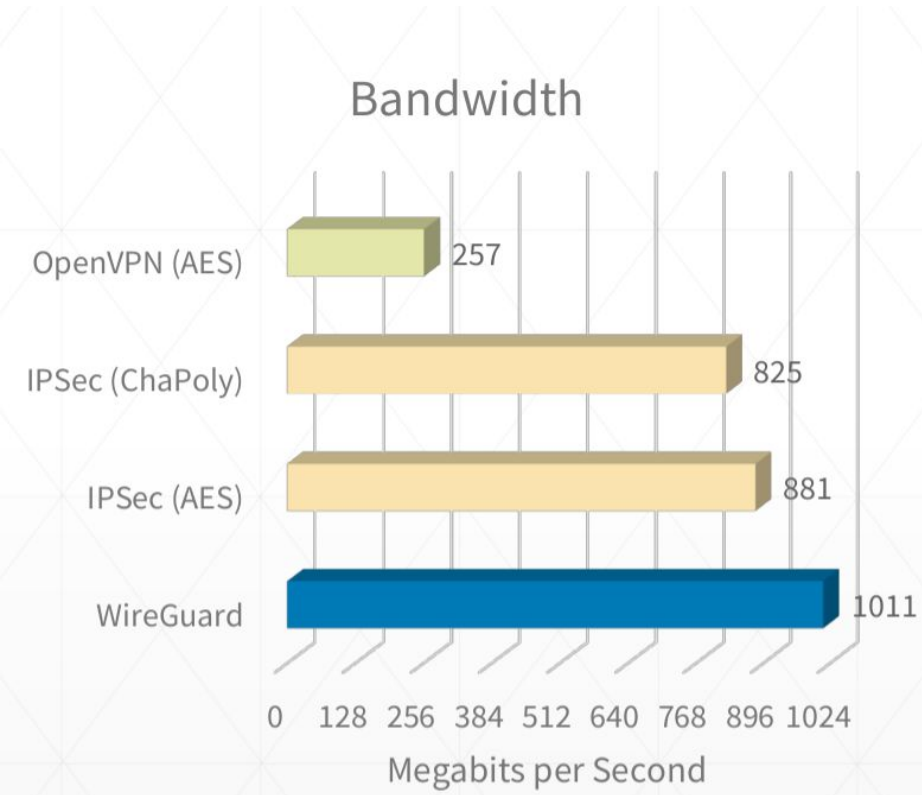
Alternative Protocols

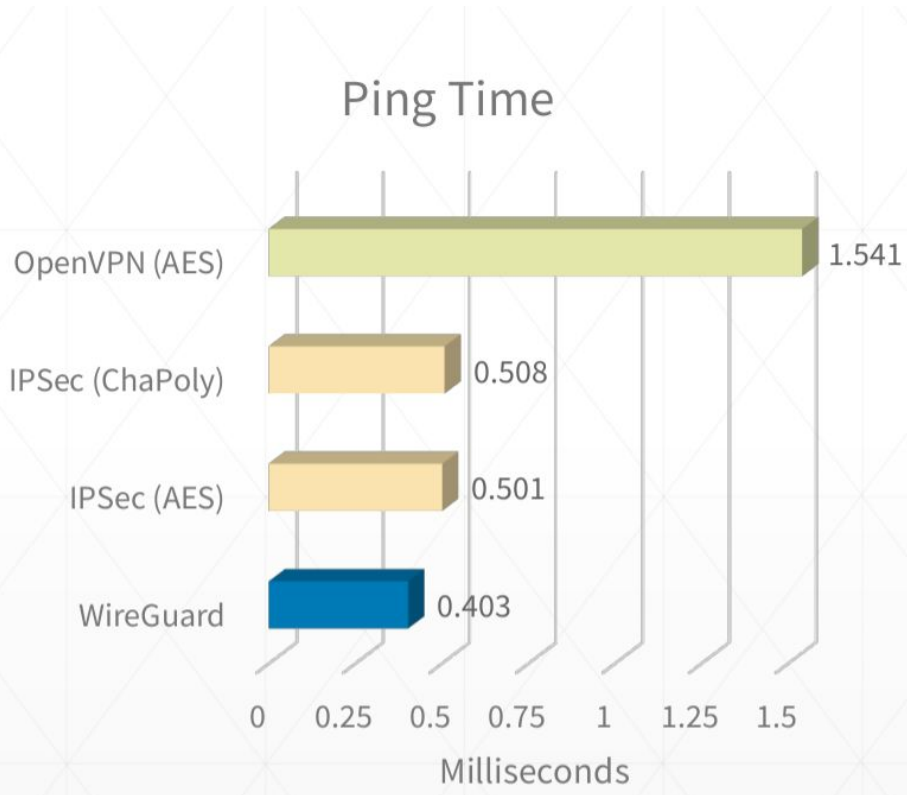

Friendship ended with
OPENVPN
Now
WIREGUARD
FAST, MODERN, SECURE VPN TUNNEL
is my
best friend
OpenVPN Client
OPENVPN
Access
Status
Organization: OpenVPN Technologies, Inc.
11:43
openvpn
Cancel
OpenVPN Connect
Utilities
OPEN

Wireguard Configuration

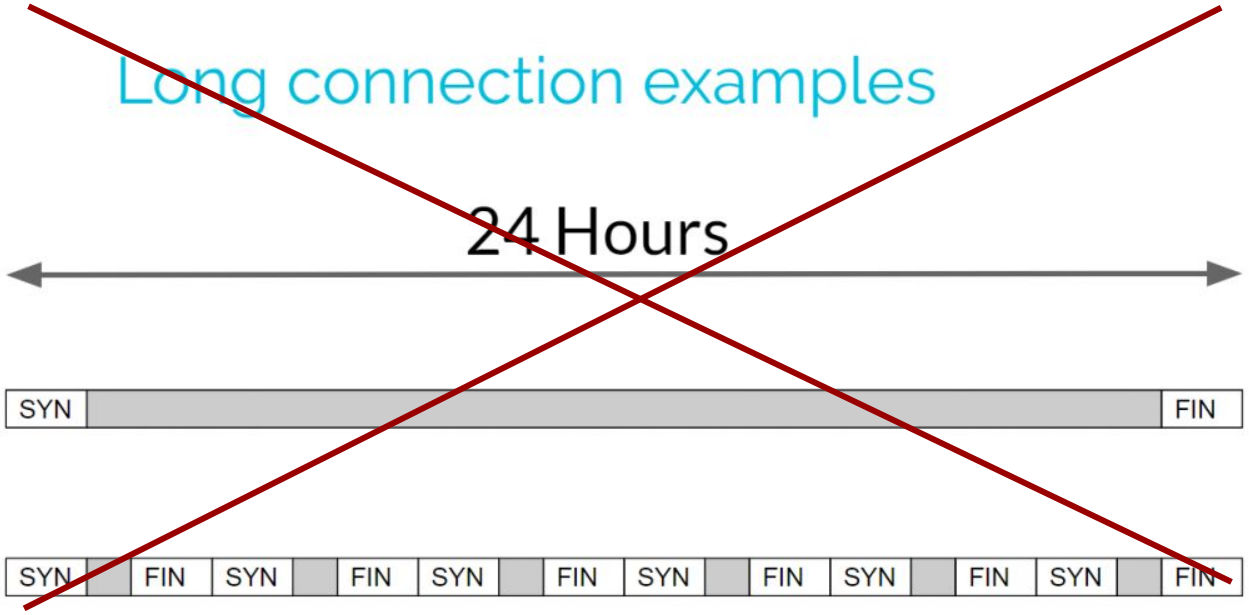
```
k@X1 ~ $ cat /etc/wireguard/projectpull.conf

[Interface]
Address = 10.192.122.2/32
DNS = 10.192.122.1
PrivateKey = UUErDoqPKV5rL7eQlN+kREv2DxIoZF/Ku0zrO7BF838=

[Peer]
PublicKey = Z/yGpYybFwzDVXYz0E3GkGrnPCx8zQXcA4+JQ3eK+3k=
AllowedIPs = 0.0.0.0/0,::/0
Endpoint = 35.230.46.110:51820
```

Wireguard Is Fast





Wireguard Is Quiet



Finding The Longest Connections With Zeek

```
cbrenton@cbrenton-lab-testing:~/lab1$ cat conn.*log | bro-cut id.orig_h id.resp_h du
ration | sort -k 3 -rn | head -10
10.55.100.100   65.52.108.225   86222.365445
10.55.100.107   111.221.29.113  86220.126151
10.55.100.110   40.77.229.82    86160.119664
10.55.100.109   65.52.108.233   72176.131072
10.55.100.105   65.52.108.195   66599.002312
10.55.100.103   131.253.34.243  64698.370547
10.55.100.104   131.253.34.246  57413.278323
10.55.100.111   111.221.29.114  46638.510373
10.55.100.108   65.52.108.220   44615.165823
10.55.100.106   40.77.229.91    41206.913035
cbrenton@cbrenton-lab-testing:~/lab1$ _
```

If You Can’t Beat Them, Join Them

- OpenConnect is built on top of standards like HTTP, TLS, and DTLS, and it's one of the most popular and widely used VPN technologies.

- Common to large multi-national corporations, it often means that at the protocol level, it is seldom blocked.


```
AnyConnect:  UDP 443  || TCP 443
     IKEv2:  UDP 4500 && UDP 500
      PPTP:  TCP 1723
```

Use DNSCAT2 to tunnel traffic (server)

```
root@projectpull.org ~ $ ruby ./dnscat2.rb --dns “host=192.168.0.4”
New window created: 0
New window created: crypto-debug
Welcome to dnscat2! Some documentation may be out of date.

auto_attach => false
history_size (for new windows) => 1000
Security policy changed: All connections must be encrypted
New window created: dns1
Starting Dnscat2 DNS server on 10.168.0.4:53
To talk directly to the server without a domain name, run:

  ./dnscat --dns server=x.x.x.x,port=53 --secret=b042cb96c2717245f26c0b091b33e9af

command (X1) 2> ping
Ping!
command (X1) 2> Pong!
listen 2222 10.69.69.14:22
Listening on 0.0.0.0:2222, sending connections to 10.69.69.14:22
command (X1) 2> Connection from 127.0.0.1:38074; forwarding to 10.69.69.14:22...
[Tunnel 0] connection successful!
```

Use DNSCAT2 to tunnel traffic (client)

```
k@x1 ~ $ ./dnscat --dns server=35.236.29.41,port=53 --secret=7a5517be4d20e2c74e0e0ab597d90c02
Creating DNS driver:
 domain = (null)
 host   = 0.0.0.0
 port   = 53
 type   = TXT,CNAME,MX
 server = 35.236.29.41

** Peer verified with pre-shared secret!

Session established!
Got a command: COMMAND_PING [request] :: request_id: 0x0001 :: data:
AEOTAMWYKBDSSESHJVPGEHQQKGZKIFYNRJXJQUAUXPOHZRGMANFDUBPADGNNKOGMGEVJUESHUWJHUEONYOHWVOYHZKQBWSV
[[ WARNING ]] :: Got a ping request! Responding!
Response: COMMAND_PING [response] :: request_id: 0x0001 :: data:
AEOTAMWYKBDSSESHJVPGEHQQKGZKIFYNRJXJQUAUXPOHZRGMANFDUBPADGNNKOGMGEVJUESHUWJHUEONYOHWVOYHZKQBWSV
Got a command: TUNNEL_CONNECT [request] :: request_id 0x0002 :: host 10.69.69.14 :: port 22
[[ WARNING ]] :: [Tunnel 0] connecting to 10.69.69.14:22...
[[ WARNING ]] :: [Tunnel 0] connected to 10.69.69.14:22!
```

DNSCAT2 Tunneling

```
listen [lhost:]lport rhost:rport

listen 127.0.0.1:4444 google.com:80
```

```
k@x1 ~ $ curl -v --socks5 127.0.0.1:4444 google.com
* Rebuilt URL to: google.com/
*   Trying 127.0.0.1...
* TCP_NODELAY set
* SOCKS5 communication to google.com:80
* SOCKS5 connect to IPv4 172.217.4.174 (locally resolved)
* SOCKS5 request granted.
* Connected to 127.0.0.1 (127.0.0.1) port 4444 (#0)
> HEAD / HTTP/1.1
> Host: google.com
> User-Agent: curl/7.58.0
> Accept: */*
```

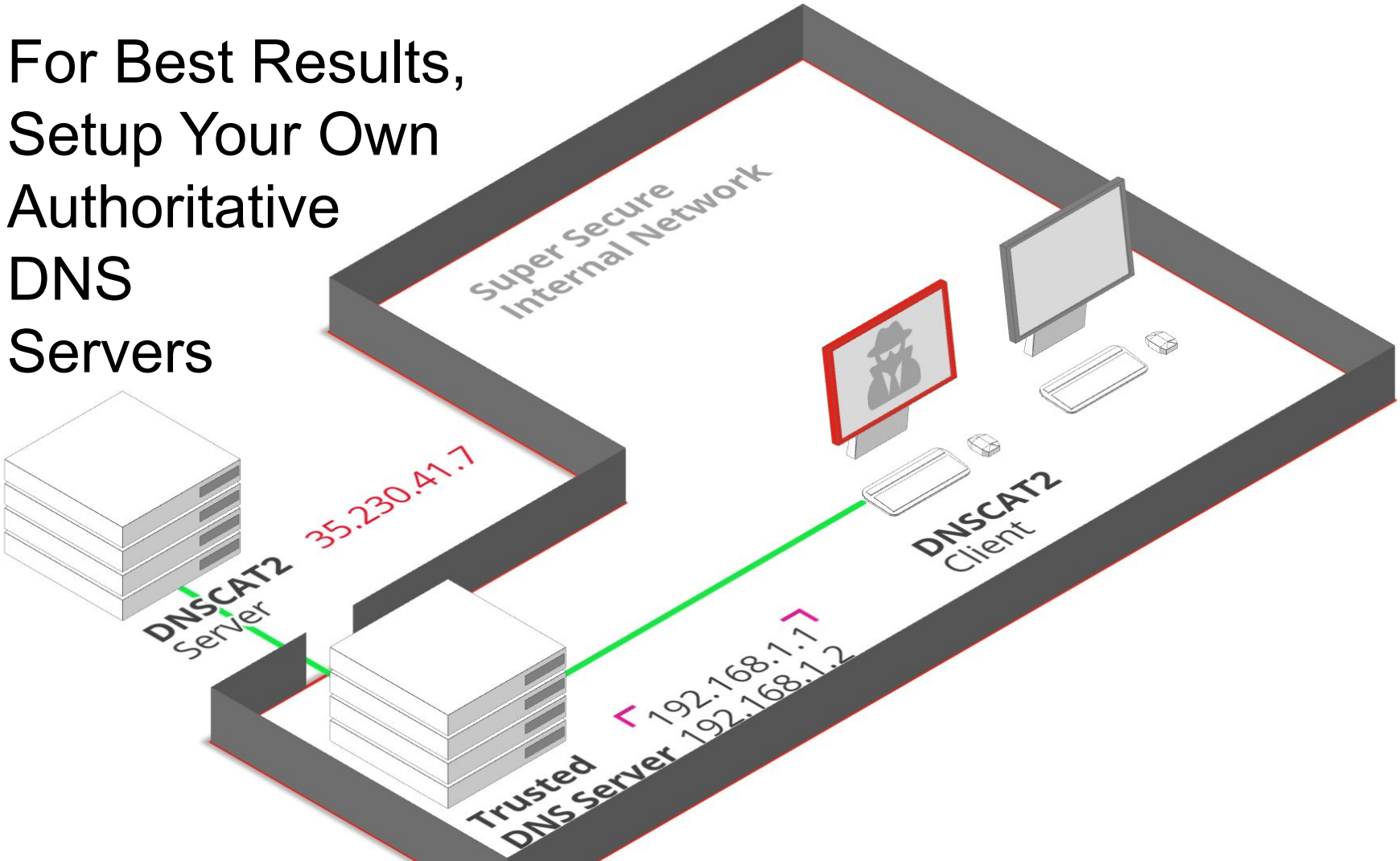
Normal DNS Traffic

```
DNS    114 Standard query 0x4cc8 A webextensions.settings.services.mozilla.com OPT
DNS    191 Standard query response 0x4cc8 A webextensions.settings.services.mozilla.com CNAME prod.webextstoragesync.prod.cloudops.mozgcp.net A 34.95.71.207 …
DNS     90 Standard query 0x0588 A spocs.getpocket.com OPT
DNS    218 Standard query response 0x0588 A spocs.getpocket.com CNAME proxyserverecs-1736642167.us-east-1.elb.amazonaws.com A 52.203.239.202 A 54.243.22.38 A…
DNS     96 Standard query 0x77a2 A getpocket.cdn.mozilla.net OPT
DNS    236 Standard query response 0x77a2 A getpocket.cdn.mozilla.net CNAME getpocket-cdn.prod.mozaws.net CNAME getpocket.cdn.mozilla.net.edgekey.net CNAME e…
DNS     88 Standard query 0xb760 A www3.l.google.com OPT
DNS    104 Standard query response 0xb760 A www3.l.google.com A 172.217.11.78 OPT
DNS     98 Standard query 0x4c65 A safebrowsing.googleapis.com OPT
DNS    114 Standard query response 0x4c65 A safebrowsing.googleapis.com A 172.217.11.170 OPT
DNS     96 Standard query 0x92cb A lh6.googleusercontent.com OPT
DNS    112 Standard query response 0x92cb A lh6.googleusercontent.com A 216.58.217.193 OPT
DNS     96 Standard query 0xf40b A lh4.googleusercontent.com OPT
DNS    112 Standard query response 0xf40b A lh4.googleusercontent.com A 172.217.11.161 OPT
```

DNSCAT2 Traffic

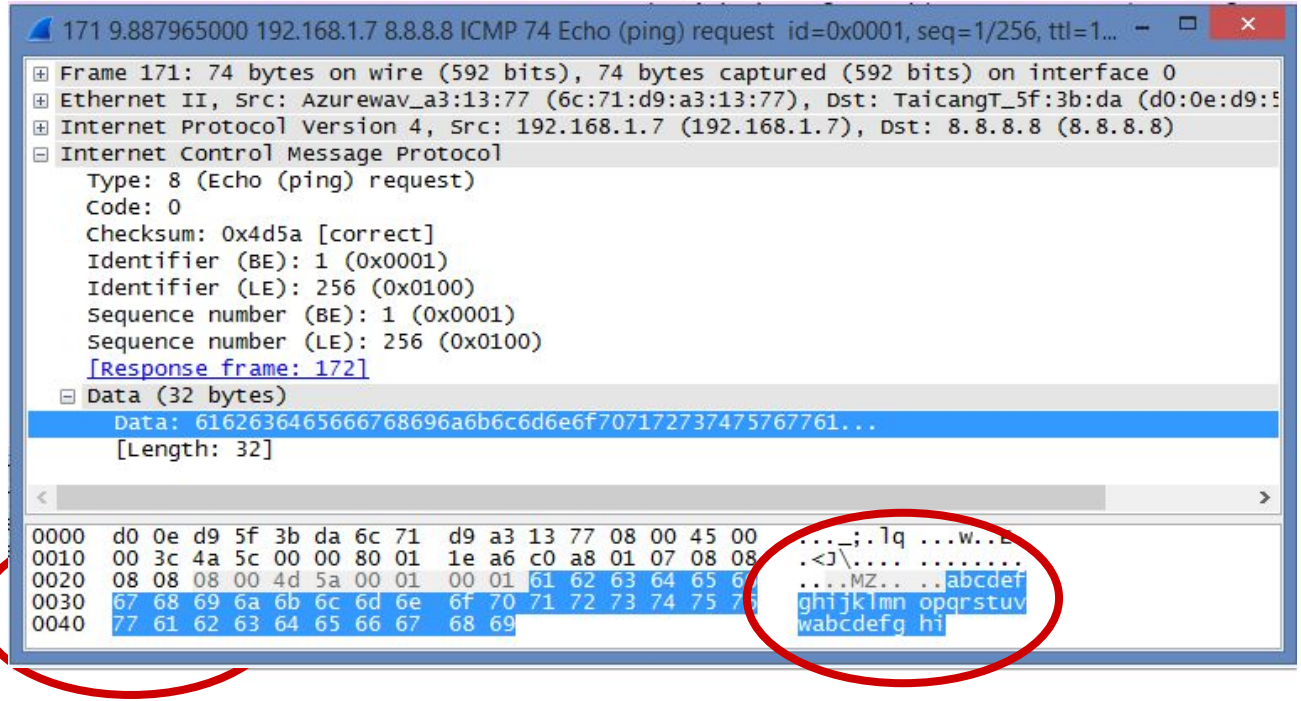
```
DNS    101 Standard query 0x78bb TXT dnscat.32ef01eb2153b4fc4adca700e7ad61635a
DNS    148 Standard query response 0x78bb TXT dnscat.32ef01eb2153b4fc4adca700e7ad61635a TXT
DNS    101 Standard query 0x6e9e CNAME dnscat.cf1001eb2185791440562c00e81fef0884
DNS    156 Standard query response 0x6e9e CNAME dnscat.cf1001eb2185791440562c00e81fef0884 CNAME dnscat.418901eb21f19f24897247ffff630d2ced
DNS    101 Standard query 0xf498 TXT dnscat.458101eb214fa88acfb63100e9ad85d263
DNS    148 Standard query response 0xf498 TXT dnscat.458101eb214fa88acfb63100e9ad85d263 TXT
DNS    101 Standard query 0x414e CNAME dnscat.f4d901eb21d331fff4a85700eaf809f526
DNS    156 Standard query response 0x414e CNAME dnscat.f4d901eb21d331fff4a85700eaf809f526 CNAME dnscat.e60b01eb21d59b326fb0adffff630d2ced
DNS    101 Standard query 0x009a MX dnscat.bd4a01eb213cce7167cea700eb016d33d0
DNS    158 Standard query response 0x009a MX dnscat.bd4a01eb213cce7167cea700eb016d33d0 MX 10 dnscat.9f4e01eb21443b1980d02ceffff630d2ced
DNS    101 Standard query 0x07d2 CNAME dnscat.877c01eb214f52be13bcb100ec0f75f35d
DNS    156 Standard query response 0x07d2 CNAME dnscat.877c01eb214f52be13bcb100ec0f75f35d CNAME dnscat.78f801eb216f7f8b80a510ffff630d2ced
DNS    101 Standard query 0x0838 TXT dnscat.eca401eb217b5cee56f54d00ededbf7e9e
DNS    148 Standard query response 0x0838 TXT dnscat.eca401eb217b5cee56f54d00ededbf7e9e TXT
DNS    101 Standard query 0x30b9 CNAME dnscat.cbdf01eb2131956cf031eb00ee0e6b509a
DNS    156 Standard query response 0x30b9 CNAME dnscat.cbdf01eb2131956cf031eb00ee0e6b509a CNAME dnscat.b02901eb21293447a500ceffff630d2ced
DNS    111 Standard query 0x2f4b MX dnscat.fc7cff4d046f726c67676c6b786e61706a7367646900
DNS    178 Standard query response 0x2f4b MX dnscat.fc7cff4d046f726c67676c6b786e61706a7367646900 MX 10 dnscat.fc7cff4d046f726c67676c6b786e61706a7367646900
```

For Best Results, Setup Your Own Authoritative DNS Servers



Use The Power of Ping

IP Datagram



DhavalKapil / icmptunnel

Watch 99 | Star 2.5k | Fork 272

Code | Issues 10 | Pull requests 2 | Projects 0 | Wiki | Security | Insights

Transparently tunnel your IP traffic through ICMP echo and reply packets. https://dhavalkapil.com/icmptunnel/

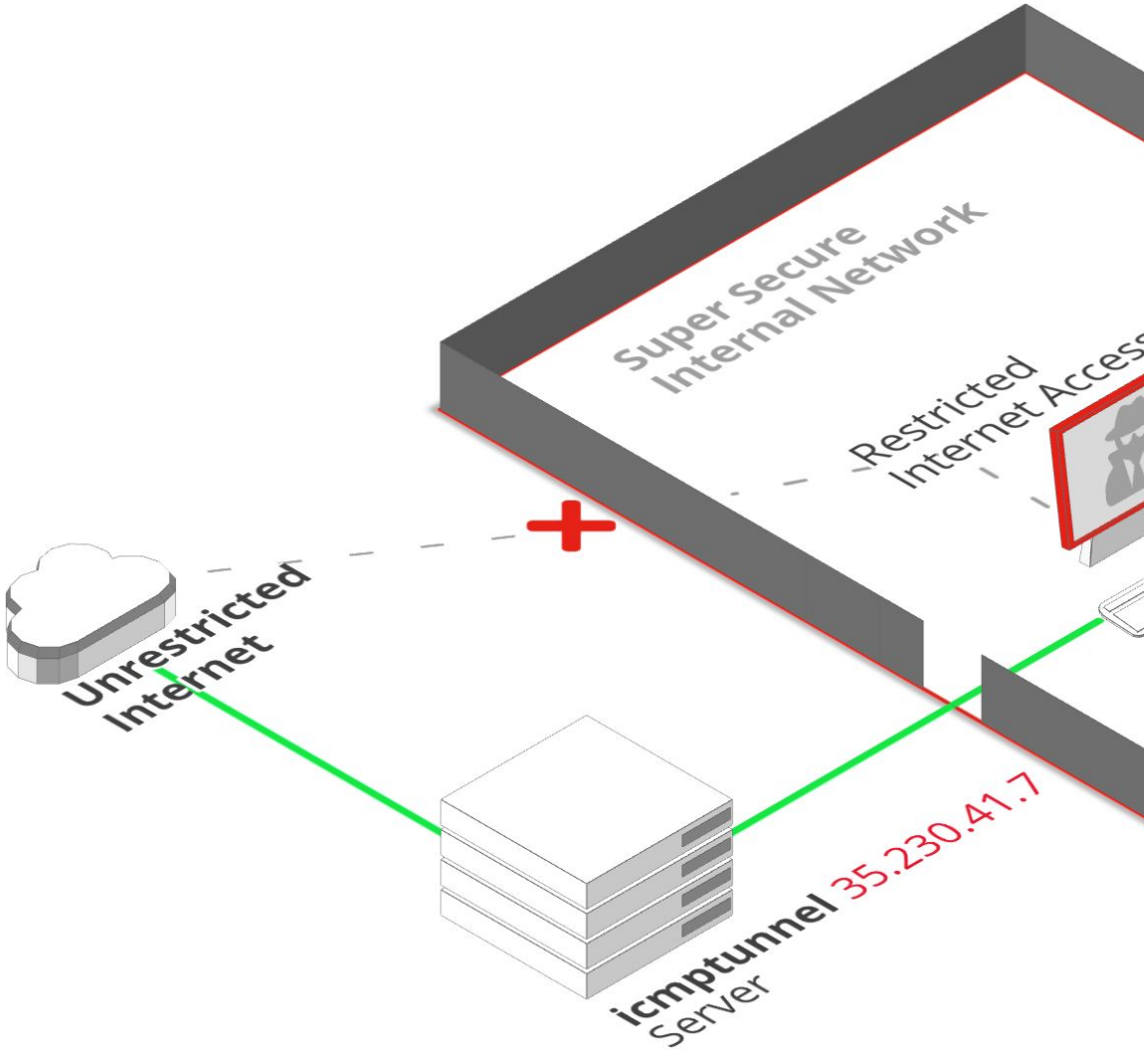
icmp tunnel proxy

62 commits | 4 branches | 0 packages | 1 release | 7 contributors

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

LiYaoYu and DhavalKapil Free the unfree heap — Latest commit 267a9ec on Apr 22, 2017

.gitignore	Renamed icmp_tunnel to icmptunnel	4 years ago
.travis.yml	Added travis	4 years ago
Makefile	Change the MTU size of tunnel (#23)	3 years ago
README.md	Typo fix	4 years ago
client.sh	Change the MTU size of tunnel (#23)	3 years ago
icmp.c	Change the MTU size of tunnel (#23)	3 years ago
icmp.h	Change the MTU size of tunnel (#23)	3 years ago



Internet protocol suite

Application layer

BGP • DHCP • DNS • FTP • HTTP • HTTPS • IMAP • LDAP • MGCP • MQTT • NNTP • NTP • POP • ONC/RPC • RTP • RTSP • RIP • SIP • SMTP • SNMP • SSH • Telnet • TLS/SSL • XMPP • *more...*

Transport layer

TCP • UDP • DCCP • SCTP • RSVP • *more...*

Internet layer

IP (IPv4 • IPv6) • **ICMP** • ICMPv6 • ECN • IGMP • IPsec • *more...*

Link layer

ARP • NDP • OSPF • Tunnels (L2TP) • PPP • MAC (Ethernet • Wi-Fi • DSL • ISDN • FDDI)

more...

V • T • E

icmptunnel (server)

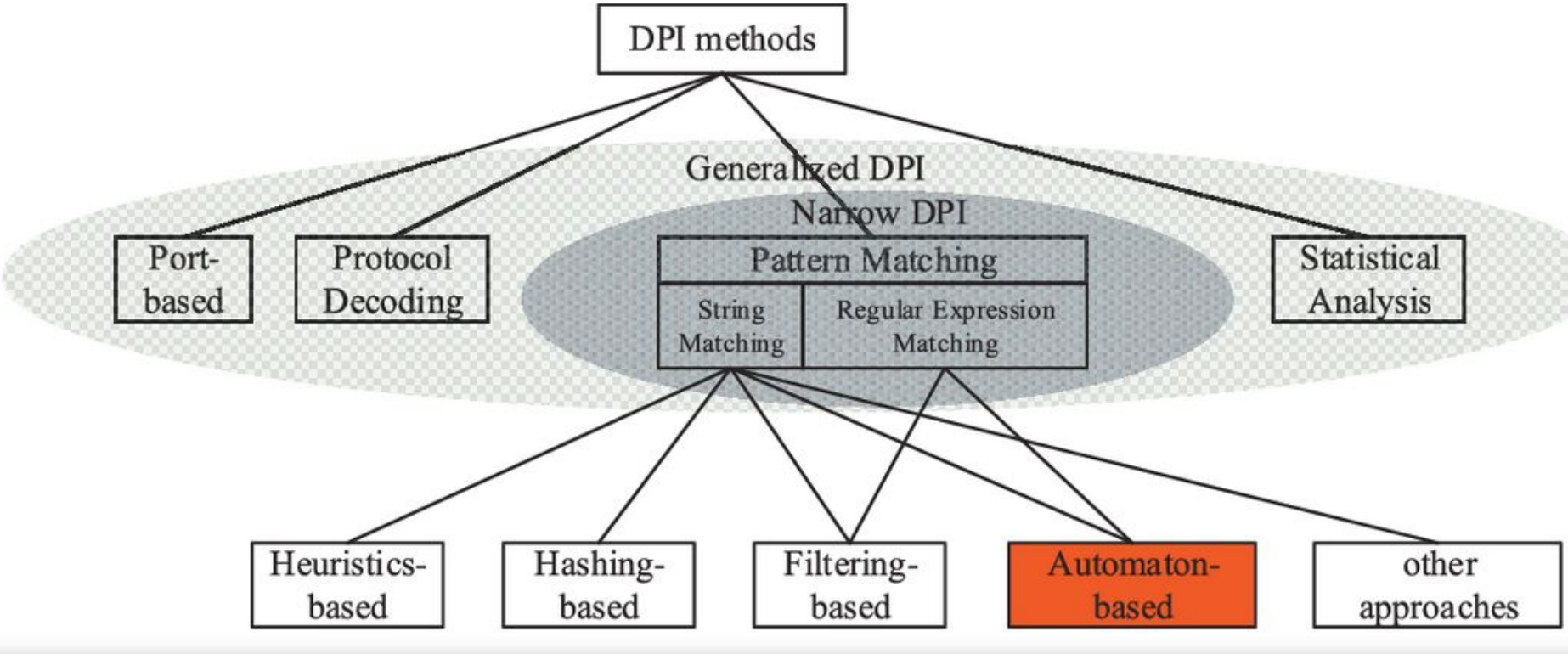
```
root@projectpull.org ~ $ ./icmptunnel -s
opened tunnel device: tun0
(ctrl-z)
# bg
# /sbin/ifconfig tun0 10.0.0.1 netmask 255.255.255.0
```

icmptunnel (client)

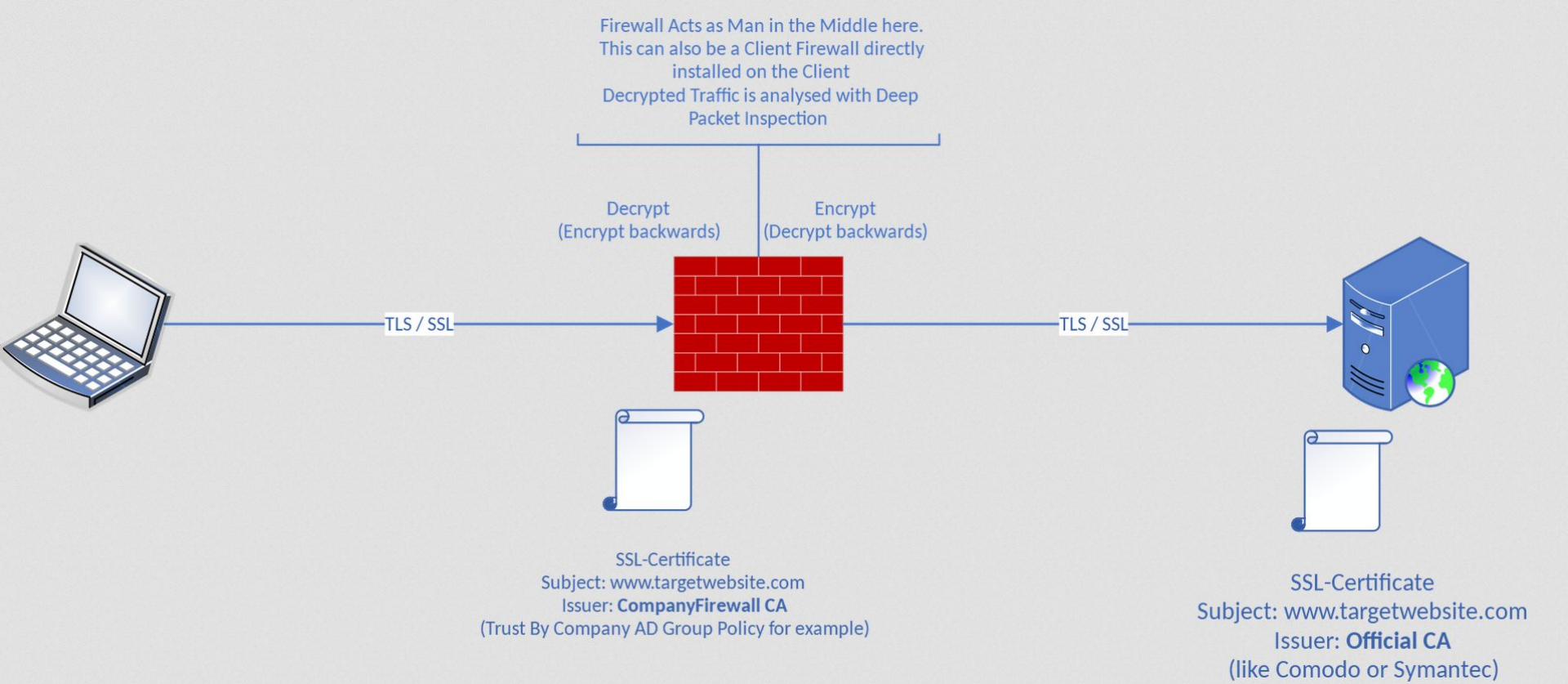
```
k@X1 ~ $ ./icmptunnel projectpull.org
opened tunnel device: tun0
connection established.
(ctrl-z)
# bg
# /sbin/ifconfig tun0 10.0.0.2 netmask 255.255.255.0
```

```
k@X1 ~ $ ssh -v -D 8080 root@10.0.0.1
OpenSSH_7.6p1 Ubuntu-4ubuntu0.3, OpenSSL 1.0.2n  7 Dec 2017
debug1: Connecting to projectpull.org [35.235.29.49] port 22.
debug1: Connection established
```

DPI Evasion


DPI methods
Generalized DPI
Narrow DPI
Port-based
Protocol Decoding
Pattern Matching
String Matching
Regular Expression Matching
Statistical Analysis
Heuristics-based
Hashing-based
Filtering-based
Automaton-based
other approaches

Deep Packet Inspection With SSL Inspection

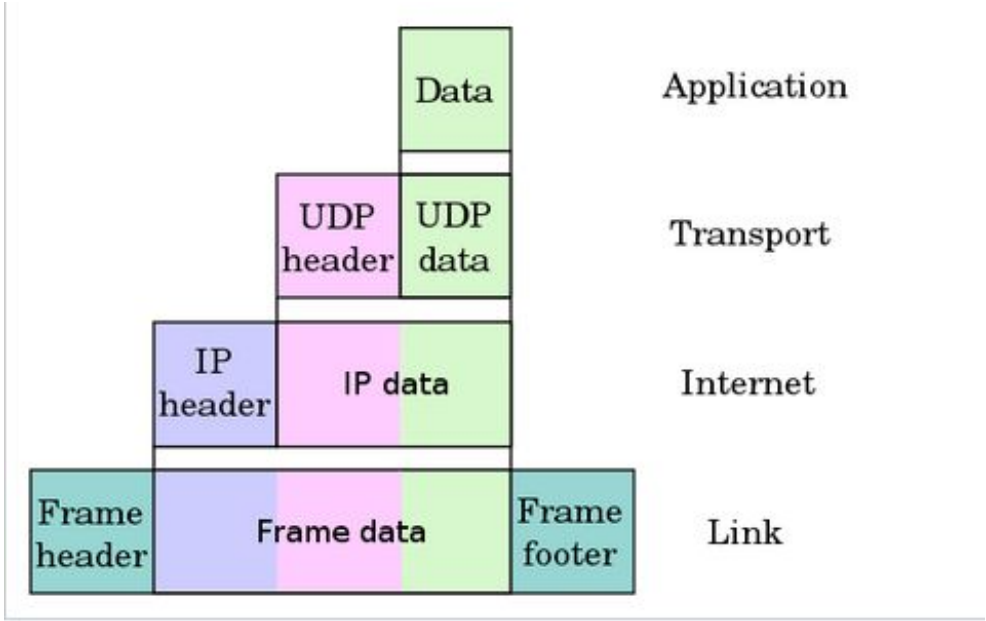


DPI Detection Methods

1. Pattern or Signature Matching

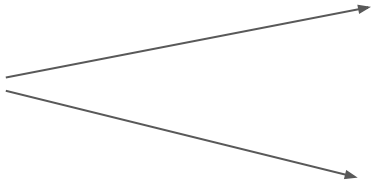
    - Regex on headers
    - Regex on data protocol structures

```
80 46 01 03 01 00 2d 00
00 00 10 00 00 05 00 00
04 00 00 0a 00 00 09 00
00 64 00 00 62 00 00 08
00 00 03 00 00 06 01 00
80 07 00 c0 03 00 80 06
00 40 02 00 80 04 00 80
```



Bypassing
String / Regex Matching

```
GET / HTTP/1.1
Host: www.facebook.com
User-Agent: curl/7.58.0
Accept: */*
```



TCP Packet
Fragmentation

```
GET    /  HTTP/1.1
hoSt:wWw.fAcE

bOoK.cOm.
usEr-AgEnt:cuRl/7.58.0
AccEpt:        */*
```

Simple Obfuscation

https://noxxi.de/research/http-evader.html

ValdikSS / **GoodbyeDPI**

Watch 236 | Unstar 3k | Fork 350

Code | Issues 36 | Pull requests 2 | Projects 0 | Wiki | Security | Insights

GoodbyeDPI—Passive Deep Packet Inspection blocker and Active DPI circumvention utility (for Windows) https://ntc.party/c/community-softwar…

dpi | deep-packet-inspection | censorship-circumvention | anticensorship

ection blocker

t Service Providers which block

It handles DPI connected using optical splitter or port mirroring (**Passive DPI**) which do not block any data but just replying faster than requested destination, and **Active DPI** connected in sequence.

Windows 7, 8, 8.1 and 10 with administrator privileges required.

bol-van / **zapret**

Watch 81 | Star 856 | Fork 129

Code | Issues 1 | Pull requests 0 | Projects 0 | Wiki | Security | Insights

Обход DPI в linux

dpi | censorship-circumvention | linux | russian | wireguard-mod | openwrt

74 commits | **1** branch | **0** releases | **1** contributor

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

bol-van readme.eng : android notice — Latest commit 62e429f 3 days ago

binaries	tpws : --skip-nodelay option	23 days ago
docs	readme.eng : android notice	3 days ago
init.d	history purge	5 months ago

ributors | Apache-2.0

pload files | Find file | Clone or download

Latest commit 2b3e4a4 on Apr 2

8 months ago

10 months ago

2 years ago

3 years ago

7 months ago

Confusing The Great Firewall

Your state is not mine: a closer look at evading stateful internet censorship

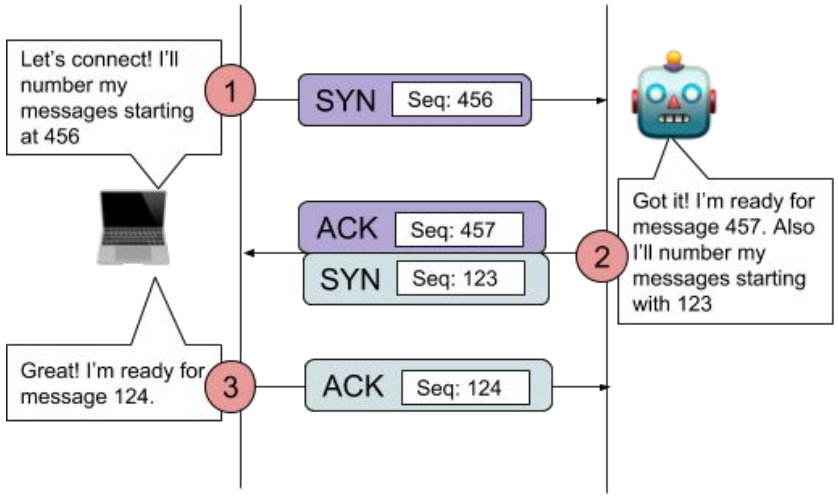
https://dl.acm.org/citation.cfm?doid=3131365.3131374

Desynchronizing the TCP Control Block

1. Send SYN insertion packet with modified sequence number
   - Packet will have wrong checksum or low TTL and be rejected

2. Initiate the connection with the correct sequence number
   - Traffic is ignored due to unexpected sequence number

3. Send invalid RST, RST/ACK or FIN packets at the firewall
   - Packet will have wrong checksum or low TTL and be rejected



No description, website, or topics provided.

20 commits | **2** branches | **0** releases | **3** contributors | GPL-3.0

Branch: **master** | New pull reques

gkso fix typo

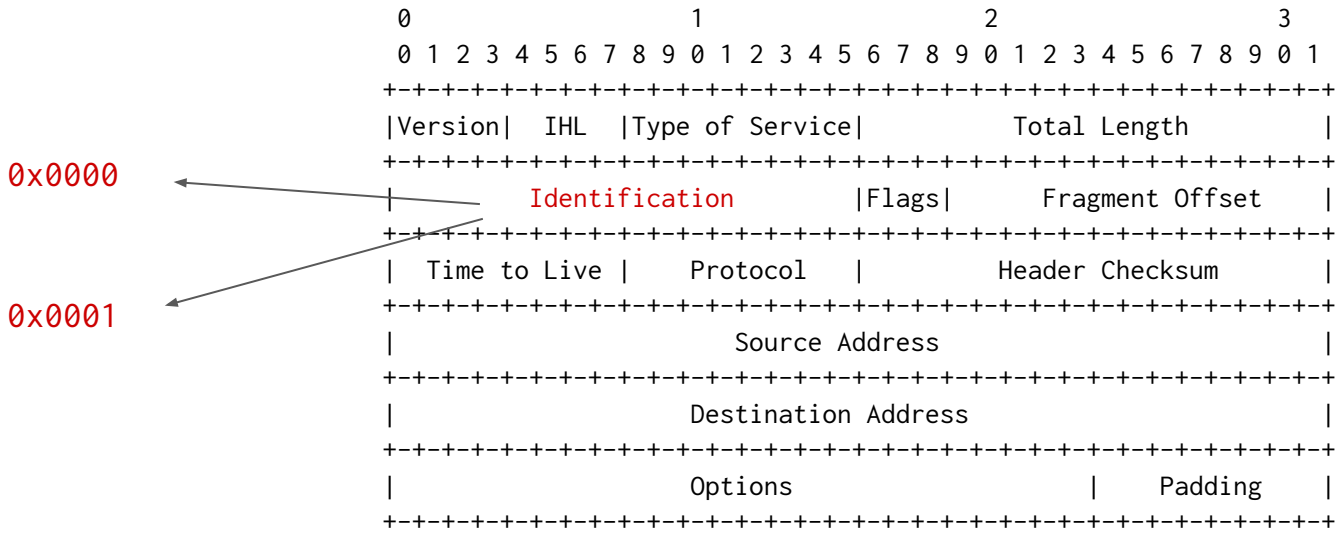
src		
.gitignore		
FAQ.md		
LICENSE	initial commit	2 years ago
Makefile	open source INTANG	2 years ago
README.md	Update README.md	2 years ago
dns_blacklist	open source INTANG	2 years ago
install_deps.sh	open source INTANG	2 years ago

Introduction

INTANG is research project for circumventing the "TCP reset attack" from the Great Firewall of China (GFW) by disrupting/desynchronizing the TCP Control Block (TCB) on the censorship devices. INTANG runs as a client-side only tool in background to protect the TCP connections from being interfered (or even monitored) by the GFW. It works on TCP/IP layers instead of application layer, thus considered more general and can help all application layer protocols, e.g. HTTP, DNS over TCP, OpenVPN, Tor, evading censorship. It can also be run on a proxy to make the deployment easier for those who are incapable of running INTANG (using OSes other than Linux or doesn't have root privillige).

Ignoring RST

IP-Header - RFC 791



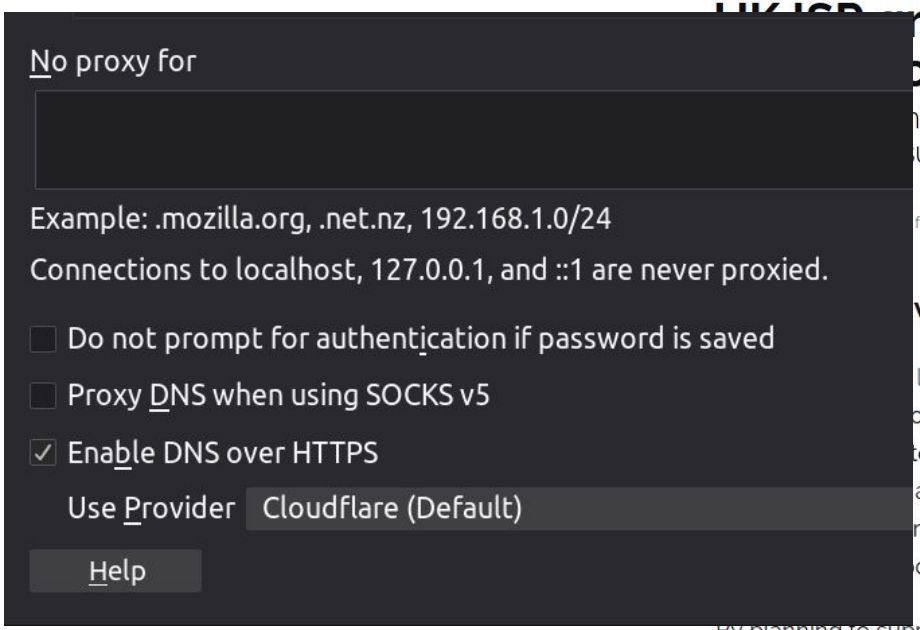
Identification Field: A value assigned by the sender to aid in assembling the fragments of a datagram.

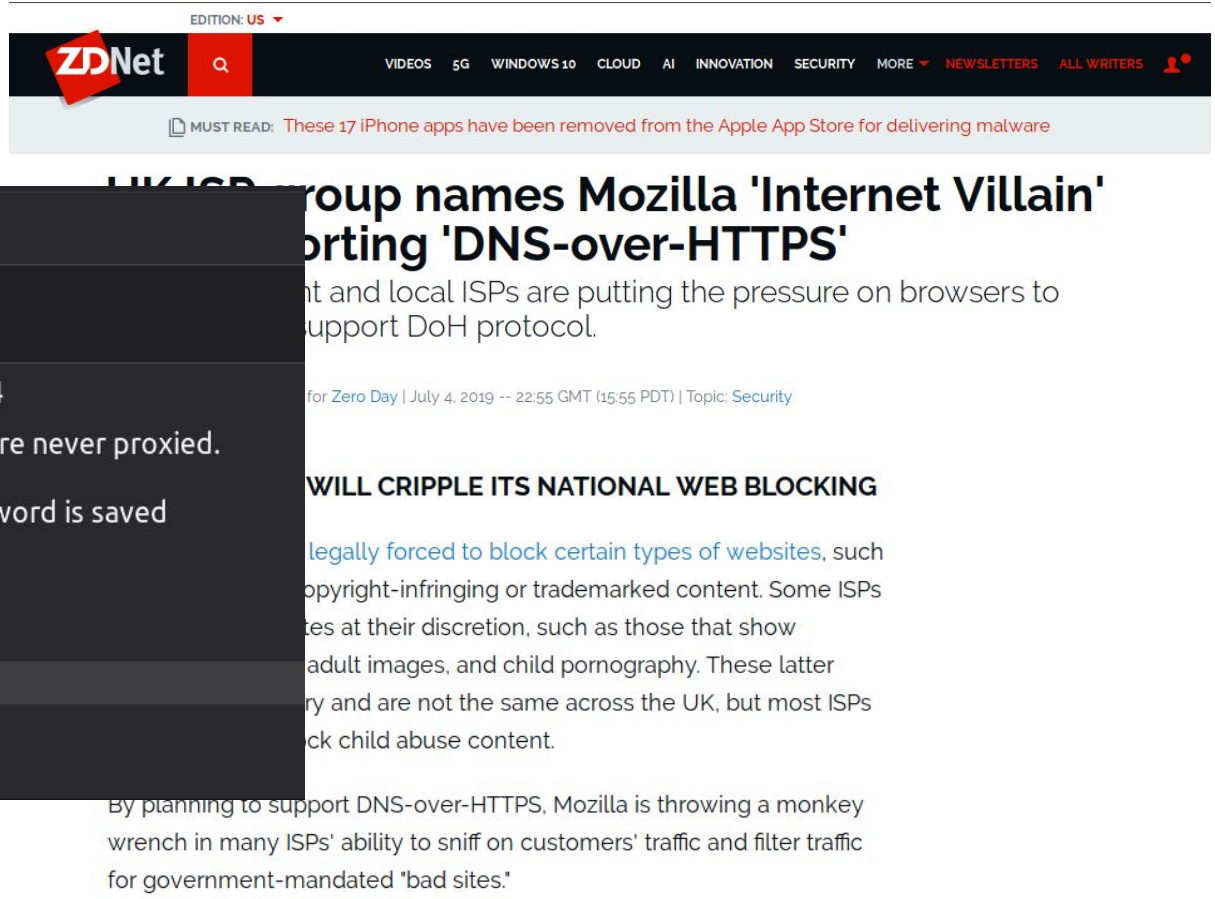

WIREGUARD®
FAST, MODERN, SECURE VPN TUNNEL

Wireguard (UDP) -> UDPTUNNEL (TCP)

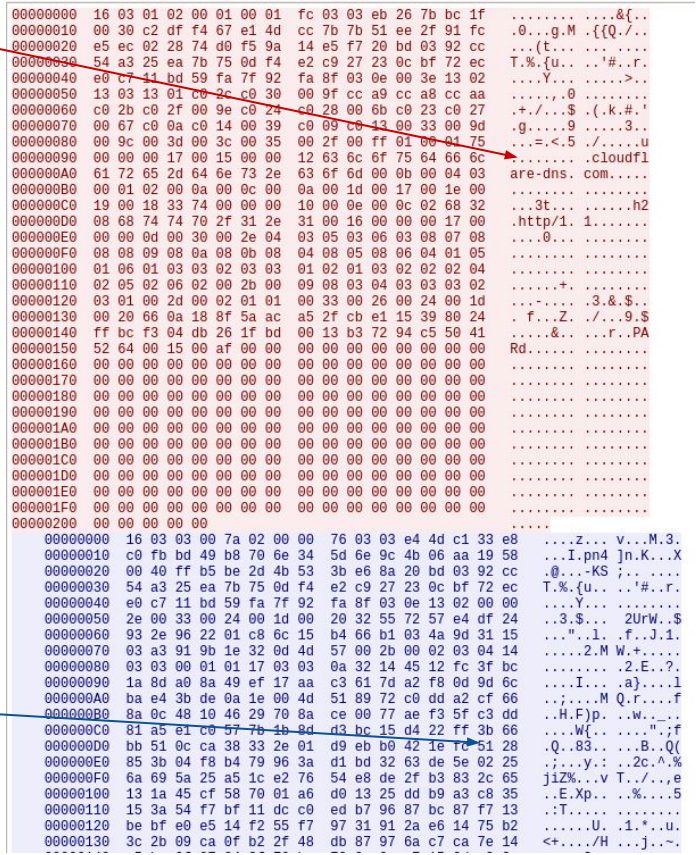
```
root@projectpull.org ~ $ udptunnel -s 443 127.0.0.1/51820

k@X1 ~ $ udptunnel -c 35.230.46.110/443 127.0.0.1 51818
k@X1 ~ $ cat /etc/wireguard/projectpull.conf

[Interface]
Address = 10.192.122.2/32
DNS = 10.192.122.1
PrivateKey = UUErDoqPKV5rL7eQlN+kREv2DxIoZF/Ku0zrO7BF838=

[Peer]
PublicKey = Z/yGpYybFwzDVXYz0E3GkGrnPCx8zQXcA4+JQ3eK+3k=
AllowedIPs = 0.0.0.0/0,::/0
Endpoint = 127.0.0.1:51820
```

DNS Over HTTPS



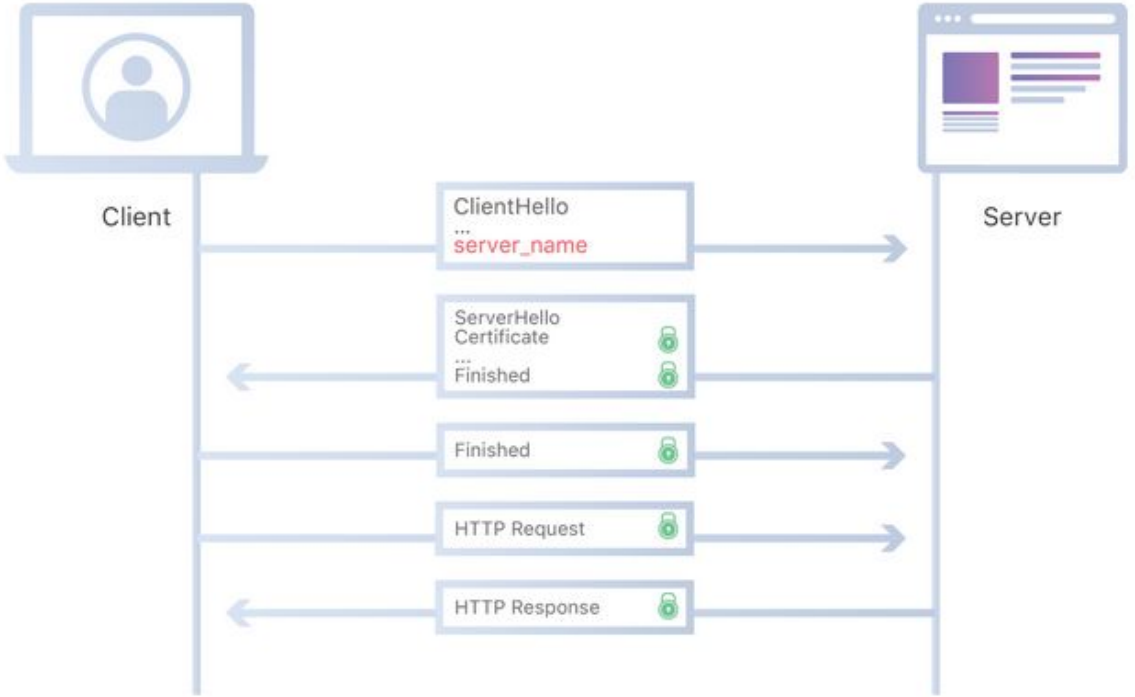


```
k@X1 ~ $ curl -s -H 'accept: application/dns-json' \
'https://cloudflare-dns.com/dns-query?name=facebook.com&type=A' | jq
{
  "Status": 0,
  "TC": false,
  "RD": true,
  "RA": true,
  "AD": false,
  "CD": false,
  "Question": [
    {
      "name": "facebook.com.",
      "type": 1
    }
  ],
  "Answer": [
    {
      "name": "facebook.com.",
      "type": 1,
      "TTL": 77,
      "data": "31.13.70.36"
    }
  ]
```



SNI

The TLS Server Name Indication (SNI) extension, originally standardized back in 2003, lets servers host multiple TLS-enabled websites on the same set of IP addresses, by requiring clients to specify which site they want to connect to during the initial TLS handshake.



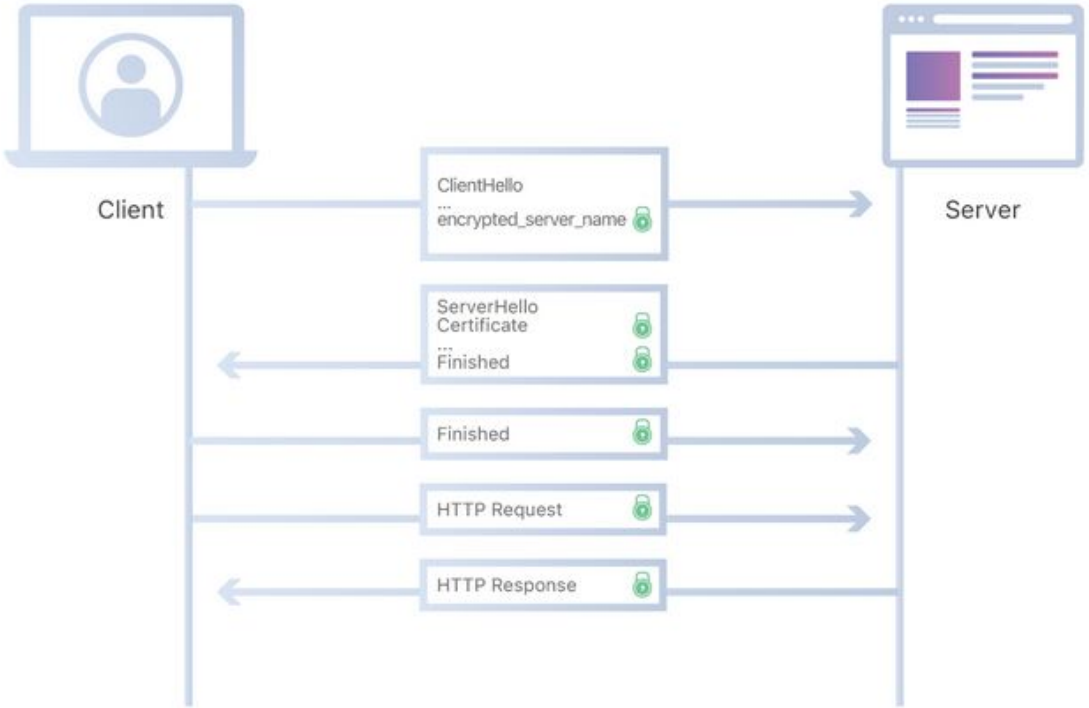
ESNI

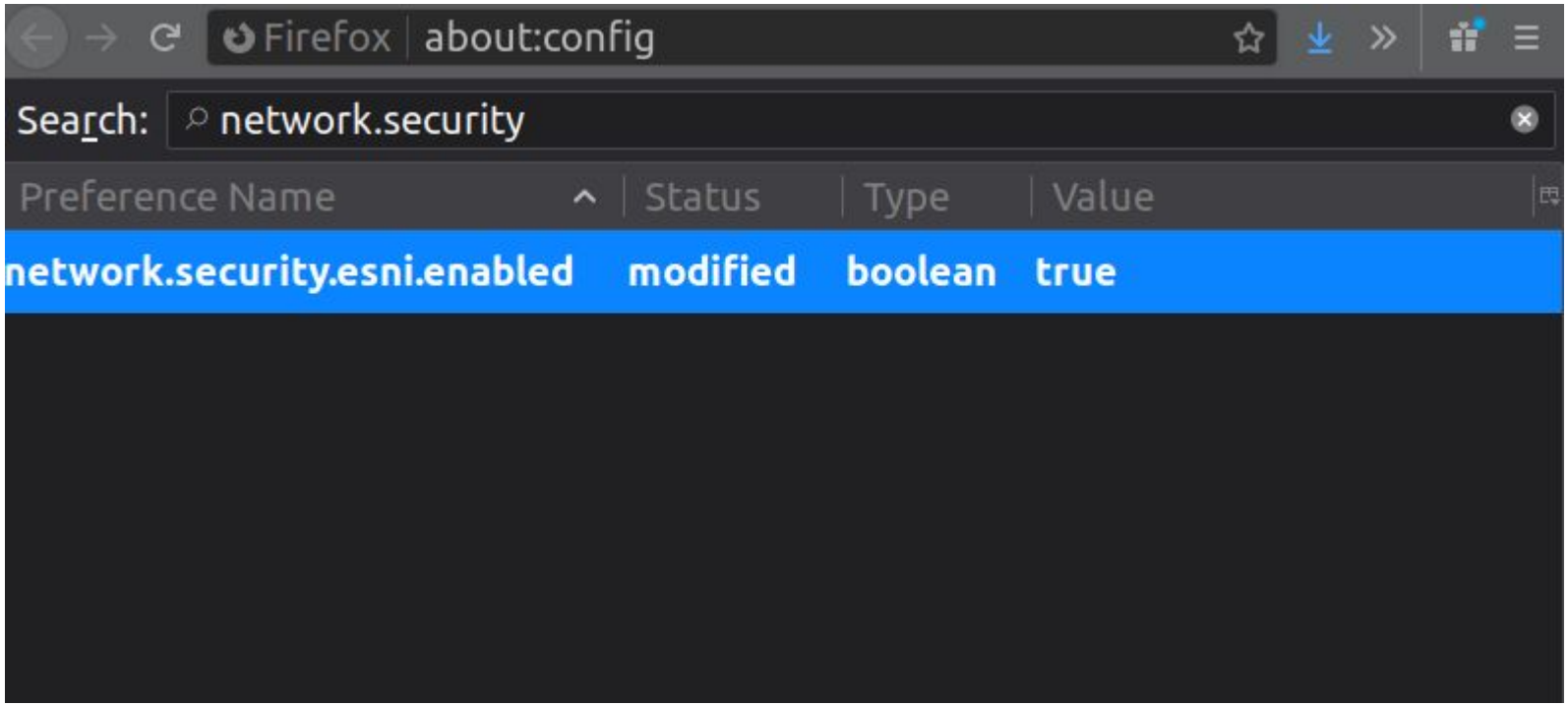
The TLS Encrypted Server Name Indication (ESNI) extension, is currently an experimental protocol proposed on July 08, 2019.

Public key is published on a DNS Record

Server holds private key

Client sends SNI encrypted with public key




Firefox
about:config
Search:
network.security
Preference Name
Status
Type
Value
network.security.esni.enabled
modified
boolean
true

```
▸ Cipher Suites (31 suites)
  Compression Methods Length: 1
▸ Compression Methods (1 method)
  Extensions Length: 373
▾ Extension: server_name (len=23)
    Type: server_name (0)
    Length: 23
  ▾ Server Name Indication extension
      Server Name list length: 21
      Server Name Type: host_name (0)
      Server Name length: 18
      Server Name: cloudflare-dns.com
▸ Extension: ec_point_formats (len=4)
▸ Extension: supported_groups (len=12)
▸ Extension: next_protocol_negotiation (len=0)
▸ Extension: application_layer_protocol_negotiation (len=14)
▸ Extension: encrypt_then_mac (len=0)
▸ Extension: extended_master_secret (len=0)
▾ Extension: signature_algorithms (len=48)
    Type: signature_algorithms (13)
    Length: 48
```

```
00c0  00 ff 01 00 01 75 00 00  00 17 00 15 00 00 12 63   ·····u·· ·· ·····c
00d0  6c 6f 75 64 66 6c 61 72  65 2d 64 6e 73 2e 63 6f   loudflar e-dns.co
00e0  6d 00 0b 00 04 03 00 01  02 00 0a 00 0c 00 0a 00   m·····  ·· ·· ····
00f0  1d 00 17 00 1e 00 19 00  18 33 74 00 00 00 10 00   ·· ·· ·· ·3t· ····
0100  0e 00 0c 02 68 32 08 68  74 74 70 2f 31 2e 31 00   ····h2·h ttp/1.1·
0110  16 00 00 00 17 00 00 00  0d 00 30 00 2e 04 03 05   ·· ·· ·· ·· 0· ····
0120  03 06 03 08 07 08 08 08  09 08 0a 08 0b 08 04 08   ·· ·· ·· ·· ·· ····
0130  05 08 06 04 01 05 01 06  01 03 03 02 03 03 01 02   ·· ·· ·· ·· ·· ····
0140  01 03 02 02 02 04 02 05  02 06 02 00 2b 00 09 08   ·· ·· ·· ·· ···+ ···
0150  03 04 03 03 03 02 03 01  00 2d 00 02 01 01 00 33   ·· ·· ·· ·· -· ··· 3
0160  00 26 00 24 00 1d 00 20  66 0a 18 8f 5a ac a5 2f   ·&·$·· ·  f···Z··/
0170  cb e1 15 39 80 24 ff bc  f3 04 db 26 1f bd 00 13   ···9·$·· ···&····
0180  b3 72 94 c5 50 41 52 64  00 15 00 af 00 00 00 00   ·r··PARd ·· ·· ····
0190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·· ·· ·· ·· ·· ····
01a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·· ·· ·· ·· ·· ····
01b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·· ·· ·· ·· ·· ····
01c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·· ·· ·· ·· ·· ····
01d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·· ·· ·· ·· ·· ····
```

Plaintext SNI

Encrypted SNI

```
▾ Extension: Unknown type 65486 (len=366)
    Type: Unknown (65486)
    Length: 366
    Data: 1301001d00202e9357998b44e383281496a9ea8148ecaeae...
```

```
00b0  00 01 02 00 0a 00 0c 00  0a 00 1d 00 17 00 1e 00   ·· ·· ·· ·· ·· ····
00c0  19 00 18 00 23 00 00 00  16 00 00 00 17 00 00 00   ···· #··· ·· ·· ····
00d0  0d 00 1e 00 1c 04 03 05  03 06 03 08 07 08 08 08   ·· ·· ·· ·· ·· ····
00e0  09 08 0a 08 0b 08 04 08  05 08 06 04 01 05 01 06   ·· ·· ·· ·· ·· ····
00f0  01 00 2b 00 03 02 03 04  00 2d 00 02 01 01 00 33   ··+· ·· ·· -· ··· 3
0100  00 26 00 24 00 1d 00 20  68 9b 99 32 87 1f c6 22   ·&·$·· ·  h··2···"
0110  0c fe 53 86 20 2d e7 4c  eb 06 b3 75 87 ce 0a 10   ··S· -·L ···u ····
0120  fa a1 8e c6 3c 41 7b 41  ff ce 01 6e 13 01 00 1d   ····<A{A ···n ····
0130  00 20 2e 93 57 99 8b 44  e3 83 28 14 96 a9 ea 81   · .·W··D ··(· ····
0140  48 ec ae ae b2 c6 f5 db  ad a1 c3 9d a9 48 ad 94   H··· ···· ···· ·H··
0150  44 6c 00 20 71 ee 04 ea  0a 1a 18 36 fa 02 a9 9d   Dl· q··· ···6 ····
0160  ce 40 5e de e9 f6 06 92  3e 1a 6d f3 ad c2 b7 a1   ·@^· ···· >·m· ····
0170  d7 dd 9d b2 01 24 09 32  59 98 f3 ff e1 06 78 bd   ···· ·$·2 Y··· ··x·
0180  32 1e 94 47 ab 3d 38 64  fc ef b7 fc 3b 44 77 2d   2··G ·=8d ···· ;Dw-
0190  82 f7 1e eb 3a 86 74 11  97 0f 4d 58 d1 8a ec e4   ···· :·t· ··MX ····
01a0  a1 16 e4 73 b5 b8 b5 82  8f b7 53 eb 5a 0a 22 01   ··· s··· ·· S·Z·"·
01b0  3d 6e 91 01 2e 14 de 10  92 17 0a f0 e1 5b 5f 93   =n·· ···· ···· [_··
01c0  41 fd 76 71 81 09 ee f5  61 74 ba 3d 6e 5a 57 19   A·vq ···· at·=nZW·
01d0  3b 90 85 b3 ea ab 8f ff  93 d0 bc 00 48 55 13 c1   ;··· ···· ···· HU··
01e0  ff dc c4 d0 46 ea 55 17  8a 65 3e 18 b0 03 2f 26   ···· F·U· ·e>· ··/&
01f0  23 b8 c8 cf 51 f3 e4 22  0a a4 b7 61 cf a6 f6 fb   #··· Q·" ··· a···
0200  be 61 cd 17 7b 35 e5 09  77 28 c4 ae d5 7b f6 73   ·a·· {5·· w(·· ·{·s
0210  9b f8 94 2a 30 10 e1 fa  a7 96 af 3c 6c df 42 60   ···* 0··· ··· <l·B`
0220  e7 fb e1 ab a8 bf d6 33  10 84 7b bf 60 26 d9 57   ···· ···3 ··{· `&·W
0230  93 1e 0e 83 e1 01 ae 87  5d 34 ff 72 86 e6 38 5b   ···· ···· ]4·r ··8[
0240  aa 45 39 9a 6e 91 db 02  68 1a 24 15 d1 40 05 8e   ·E9· n··· h·$· ·@··
0250  a4 f0 ca 28 0a 95 e7 a1  e9 fa a8 62 26 b3 f4 f8   ···( ···· ···b &···
0260  11 53 e3 df e3 00 31 c1  30 f4 d8 91 4d d8 d8 10   ·S·· ··1· 0··· M···
0270  fd a4 f2 0f 15 b1 7d 74  a2 8b 2f 69 63 38 c3 aa   ···· ··}t ··/i c8··
0280  d6 48 32 7f f8 fd 4d 1e  8b 60 19 c1 18 57 7a 89   ·H2· ··M· ·`·· ·Wz·
0290  17 9d c6 f5 1c 81 55 cc  6f 4a                    ···· ··U· oJ
```

Content Blocking Blocking Methods

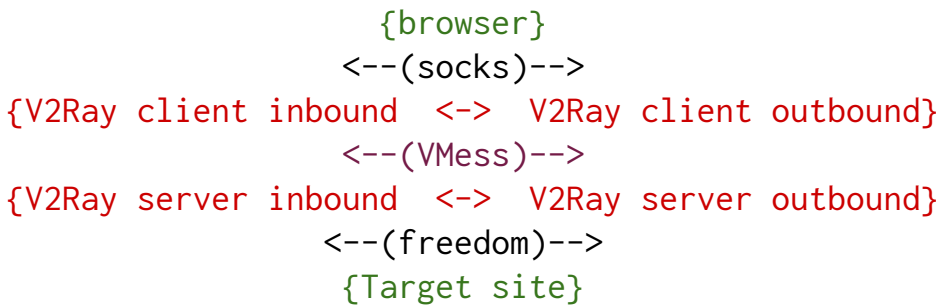
1. Send RST Packet (TCP reset attack)
   - `iptables-A INPUT -p tcp --tcp-flags RST RST -j DROP`

2. Poison DNS (redirect elsewhere)
   - Mitigate with ESNI + DNS Over HTTPS

3. Drop Packet Completely
   - Try to avoid detection with other techniques

Obfuscate Traffic

obfsproxy, ShadowVPN, SoftEther, goho, shadowsocks, SIP003, stunnel, V2Ray

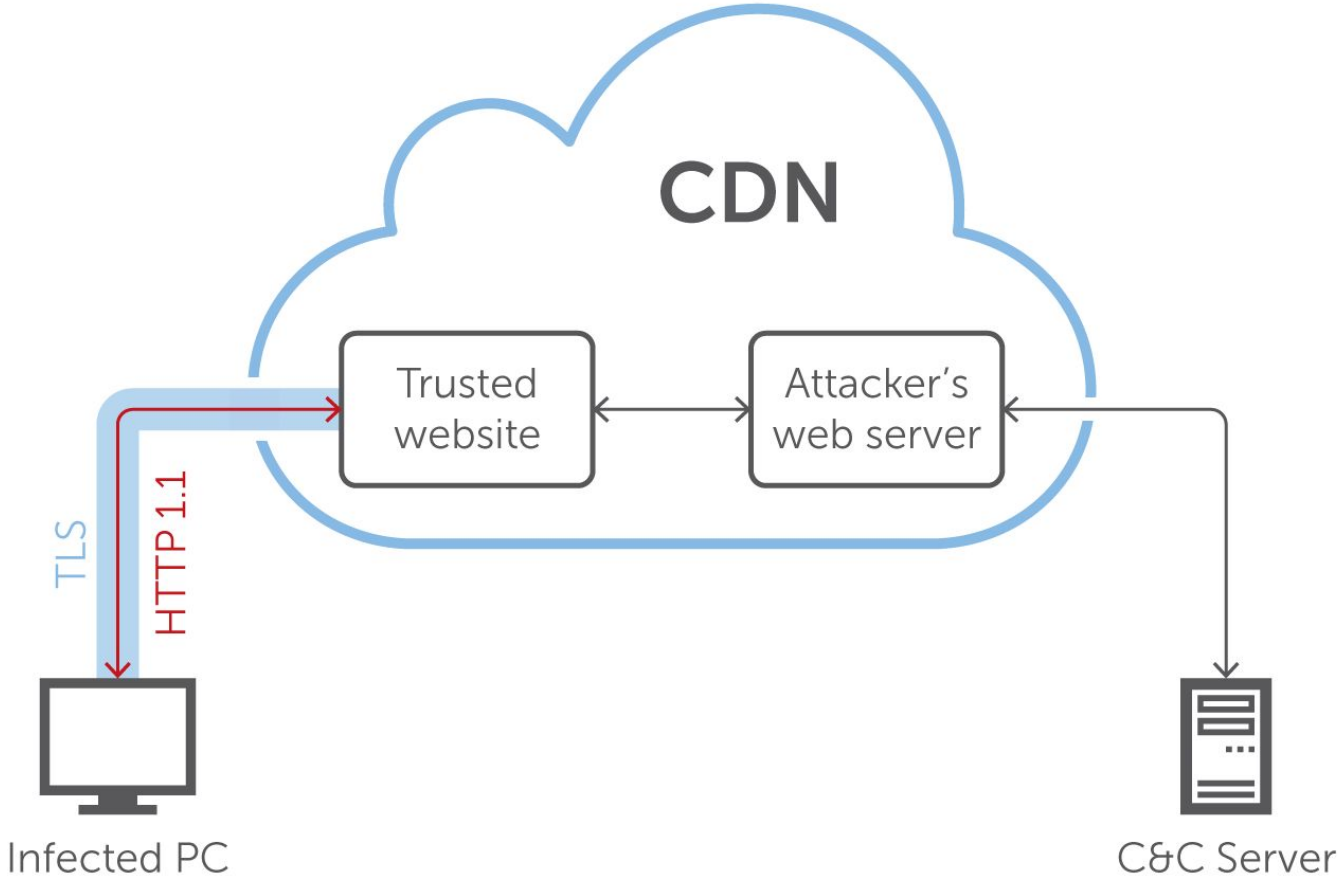


VMESS Protocol

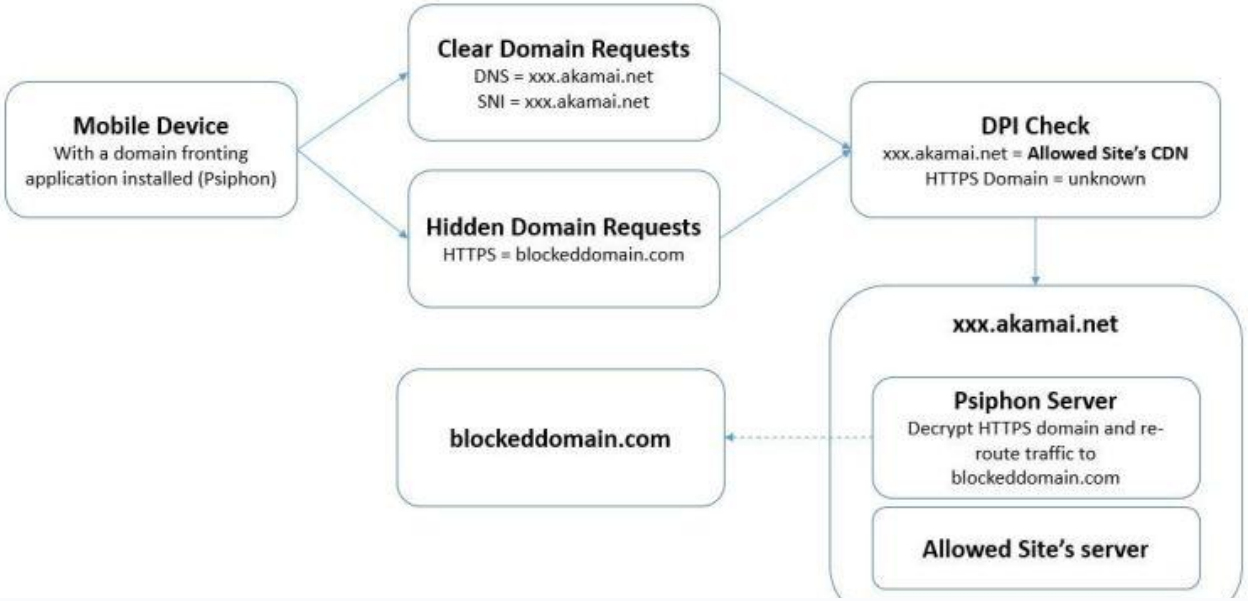
其中：

- 版本号 Ver：始终为 1；
- 数据加密 IV：随机值；
- 数据加密 Key：随机值；
- 响应认证 V：随机值；
- 选项 Opt：
  - S (0x01)：标准格式的数据流（建议开启）；
  - R (0x02)：客户端期待重用 TCP 连接（V2Ray 2.23+ 弃用）；
    - 只有当 S 开启时，这一项才有效；
  - M (0x04)：开启元数据混淆（建议开启）；
    - 只有当 S 开启时，这一项才有效；
    - 当其项开启时，客户端和服务器端需要分别构造两个 Shake 实例，分别为 RequestMask = Shake(请求数据 IV), ResponseMask = Shake(响应数据 IV)。
  - X：保留
- 余量 P：在校验值之前加入 P 字节的随机值；
- 加密方式：指定数据部分的加密方式，可选的值有：
  - 0x00：AES-128-CFB；
  - 0x01：不加密；
  - 0x02：AES-128-GCM；
  - 0x03：ChaCha20-Poly1305；
- 指令 Cmd：
  - 0x01：TCP 数据；
  - 0x02：UDP 数据；
- 端口 Port：Big Endian 格式的整型端口号；

Domain Fronting


CDN
Trusted website
Attacker's web server
TLS
HTTP 1.1
Infected PC
C&C Server

```
k@X1 ~ $ curl -v -H "Host: projectpull.org" https://bing.com
* Rebuilt URL to: https://bing.com/
*   Trying 13.107.21.200...
* TCP_NODELAY set
* Connected to bing.com (13.107.21.200) port 443 (#0)
-<SNIP>-
  * SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
  * ALPN, server accepted to use h2
  * Server certificate:
  *  subject: CN=www.bing.com
  *  start date: Jul 20 17:47:08 2017 GMT
  *  expire date: Jul 10 17:47:08 2019 GMT
  *  subjectAltName: host "bing.com" matched cert's "bing.com"
  *  issuer: C=US; ST=Washington; L=Redmond; O=Microsoft Corporation;
-<SNIP>-
  > GET / HTTP/2
  > Host: projectpull.org
  > User-Agent: curl/7.58.0
  > Accept: */*
-<SNIP>-
  * Connection #0 to host bing.com left intact
  <h2>Our services aren't available right now</h2><p>We're working to restore
all services as soon as possible. Please check back
soon.</p>0OPdbXAAAAACPvltTXmg8T6Ynwb1og0T8TE9OMDRFREdFMDQyMABFZGdl
```



Psiphon-Labs / **psiphon-tunnel-core**

Watch 83 | Star 480 | Fork 158

Code | Pull requests 0 | Actions | Wiki | Security | Insights

Psiphon client and server components implemented in Go. These components provides core tunnel functionality, handling all aspects of evading blocking and relaying traffic through Psiphon.

psiphon | censorship-circumvention | golang

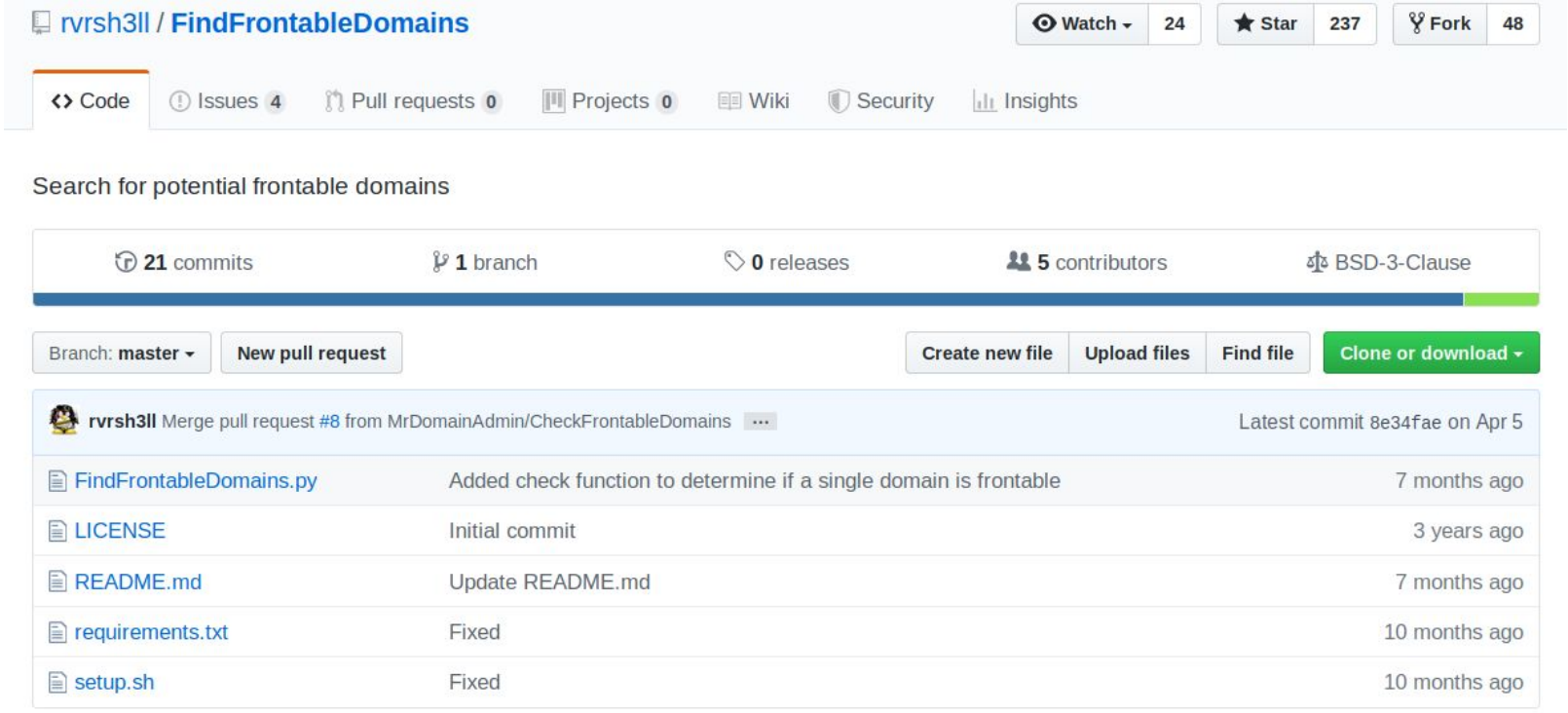
2,900 commits | **3** branches | **34** releases | **15** contributors | GPL-3.0

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

Amazon Web Services starts blocking domain-fronting, following Google's lead

By Russell Brandom | Apr 30, 2018, 6:08pm EDT

SHARE



More Resources on Domain Fronting

https://digi.ninja/blog/domain_fronting.php

https://vincentyiu.com/red-team/domain-fronting/domain-fronting-who-am-i

https://www.peew.pw/blog/2018/2/22/how-i-identified-93k-domain-frontable-cloudfront-domains

kevin@deoxy.net