

SHADOWSOCKS ---- SOCKS5 PROXY SOLUTION

-

Team : Ni Luo ,Yousong Zhang

THE GREAT (FIRE)WALL OF CHINA

- Across the Great Wall we can reach every corner of the world.
---- first email sent from China (1987)

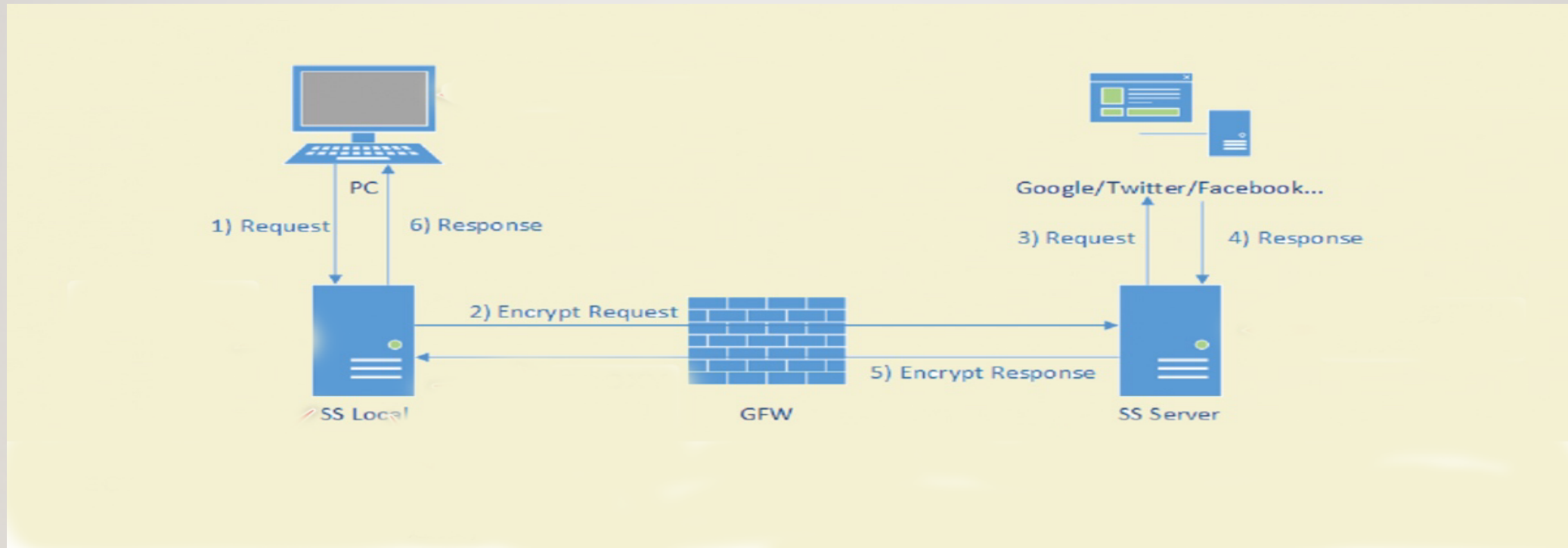
PROXY SOLUTIONS

- HTTP PROXY
- SSH Tunnel
- VPN
- Go App host
- Tor FreeGate
- Shadowsocks

SSH SERVER ← SSH TUNNEL → SSH CLIENT



SS SERVER = SHADOWSOCKS SERVER



GENERATING THE POLY1305 KEY USING CHACHA20

- ChaCha20 create a 512-bit state
- Poly1305 uses first 256 bits as key
- key size: 256bit 8 eight 32-bit little- endian integers.
- blockcount 3 * 32
- nonce 1 * 32

$$12 * 8 = 96 = 32 * 3$$

```
ss-server -m chacha20-ietf-poly1305 -u --fast-open -p 25924 -k toexofFr8YTY --manager-address  
127.0.0.1:4717 -d 183.60.83.19 -d 183.60.82.98
```

CHACHA20 AND POLY1305 FOR IETF PROTOCOL 32-BIT UNSIGNED INTEGERS

After generating Poly1305 one-time key:

| | | | |
|----------|-----------|----------|----------|
| 252bac7b | af47b42d | 557ab609 | 8455e9a4 |
| 73d6e10a | ebd97510 | 7875932a | ff53d53e |
| decc7ea2 | b44ddbada | e49c17d1 | d8430bc9 |
| 8c94b7bc | 8b7d4b4b | 3927f67d | 1669a432 |

Poly1305 Key:

| | | | | | | | | | | | | | | | | | |
|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------|
| 000 | 7b | ac | 2b | 25 | 2d | b4 | 47 | af | 09 | b6 | 7a | 55 | a4 | e9 | 55 | 84 | {.+%- .G.. |
| 016 | 0a | e1 | d6 | 73 | 10 | 75 | d9 | eb | 2a | 93 | 75 | 78 | 3e | d5 | 53 | ff | ...s.u...* |

Poly1305 r = 455e9a4057ab6080f47b42c052bac7b

Poly1305 s = ff53d53e7875932aebd9751073d6e10a

keystream bytes:

HOW TO INSTALL OUTLINE

- https://github.com/yousongzhang/Shadowsocks_VPN/blob/master/README.md

WIRESHARK PACKAGE

| | | | | | | | | |
|---|---|--------------------|----------------|-----|------|---------------|------------|---------------|
| 1063 | 5.718916 | 193.112.159.88 | 192.168.1.153 | TCP | 1478 | 26759 → 63751 | [ACK] | Seq=221685 |
| 1064 | 5.718955 | 193.112.159.88 | 192.168.1.153 | TCP | 1478 | 26759 → 63751 | [ACK] | Seq=223097 |
| 1065 | 5.719016 | 192.168.1.153 | 193.112.159.88 | TCP | 66 | 63859 → 26759 | [ACK] | Seq=304 Ack=2 |
| 1066 | 5.719016 | 192.168.1.153 | 193.112.159.88 | TCP | 66 | 63751 → 26759 | [ACK] | Seq=1 Ack=2 |
| 1067 | 5.719135 | 193.112.159.88 | 192.168.1.153 | TCP | 1478 | 26759 → 63751 | [ACK] | Seq=224509 |
| 1068 | 5.719277 | 192.168.1.153 | 193.112.159.88 | TCP | 66 | 63859 → 26759 | [FIN, ACK] | Seq=304 Ack=2 |
| 1069 | 5.719475 | 192.168.1.153 | 193.112.159.88 | TCP | 66 | 63751 → 26759 | [ACK] | Seq=1 Ack=2 |
| 1070 | 5.731569 | 193.112.159.88 | 192.168.1.153 | TCP | 1478 | 26759 → 63751 | [ACK] | Seq=225921 |
| 1071 | 5.734547 | 193.112.159.88 | 192.168.1.153 | TCP | 1478 | 26759 → 63751 | [ACK] | Seq=227333 |
| 1072 | 5.734599 | 193.112.159.88 | 192.168.1.153 | TCP | 1478 | 26759 → 63751 | [ACK] | Seq=228745 |
| 1073 | 5.734628 | 192.168.1.153 | 193.112.159.88 | TCP | 66 | 63751 → 26759 | [ACK] | Seq=1 Ack=2 |
| ▶ Frame 1063: 1478 bytes on wire (11824 bits), 1478 bytes captured (11824 bits) on interface 0 | | | | | | | | |
| ▶ Ethernet II, Src: Tp-LinkT_6c:d5:fa (50:c7:bf:6c:d5:fa), Dst: 02:42:87:41:d7:a5 (02:42:87:41:d7:a5) | | | | | | | | |
| ▶ Internet Protocol Version 4, Src: 193.112.159.88, Dst: 192.168.1.153 | | | | | | | | |
| ▶ Transmission Control Protocol, Src Port: 26759, Dst Port: 63751, Seq: 221685, Ack: 1, Len: 1412 | | | | | | | | |
| ▼ Data (1412 bytes) | | | | | | | | |
| Data: 4400b881a08bf45af01fd6aa42cfd0d26252e641eae46d95... | | | | | | | | |
| [Length: 1412] | | | | | | | | |
| 0040 | 43 cd 44 00 b8 81 a0 8b f4 5a f0 1f d6 aa 42 cf | C.D.....Z....B. | | | | | | |
| 0050 | d0 d2 62 52 e6 41 ea e4 6d 95 16 c5 6b 14 43 fc | ..bR.A..m...k.C. | | | | | | |
| 0060 | 77 10 dd 87 2e 04 f9 bf ac ef 29 e4 5d 18 69 2e | w.....).l.i. | | | | | | |
| 0070 | f5 bd 29 d7 35 27 a6 a2 0c 62 58 56 7b 9a 30 06 | ..).5'...bXV{.0. | | | | | | |
| 0080 | 02 97 80 87 20 e4 a9 b3 89 53 92 d2 65 ff 98 ac |S...e... | | | | | | |
| 0090 | 6b 2b f7 45 55 53 c2 d6 f3 9f 39 e1 42 42 53 11 | k+.EUS...9.BBS. | | | | | | |
| 00a0 | 13 75 7d 1a 62 ff f1 61 9f 53 2d 25 52 82 b6 e0 | .u}.b..a.S-%R... | | | | | | |
| 00b0 | 3f 8f 03 47 7d 06 88 d4 1c d3 40 b6 85 a7 1d ac | ?..G}...@..... | | | | | | |
| 00c0 | 91 04 bc 49 4d 36 c3 74 97 18 f7 fd db 70 82 d3 | ...IM6.t.....p... | | | | | | |
| 00d0 | 3f 69 66 b9 7c 77 e7 e8 6d 02 b1 e7 c5 23 0e fe | ?if.. w..m....#... | | | | | | |
| 00e0 | 2f 0e c0 54 0a 5e 57 3f ab 6b e3 dc d9 29 38 88 | /...T.^W?.k....)8. | | | | | | |
| 00f0 | 61 99 0d 8f b6 79 9e c2 a8 e6 3b cf 16 aa a3 e2 | a....y...;..... | | | | | | |
| 0100 | 38 44 4f a2 8d 74 a0 ef 06 8e e4 dd d4 c1 ad cd | 8D0..t..... | | | | | | |
| 0110 | 88 6b 58 26 d7 08 52 a5 24 4d 31 11 ea 88 4a ca | ..kX&..R.\$M1...J. | | | | | | |
| 0120 | 8f db 80 2a f7 c0 98 89 42 9c aa 4b a7 74 a3 32 | ...*....B...K.t.2 | | | | | | |
| 0130 | 6c e2 8d b9 7d 2f 67 c3 04 40 0c 4a 52 51 5b 1d | l....}/g..@.JRQ[. | | | | | | |
| 0140 | 0b e5 e0 cd 78 da fd bf 17 d6 5c b5 8c af cf b5 |x...\. | | | | | | |
| 0150 | d1 27 e0 9b 2d 47 56 c2 f0 9e 26 e3 40 d6 62 e4 | ..'...-GV..&.@.b. | | | | | | |

PROXY SEVER LOCAL IN CHINA

My IP Information:


ISP: Tencent cloud computing
City: Beijing
Region: Beijing
Country: China

Hide My IP Address
Click Here

+

-

Click for more details
about **193.112.159.88**



Leaflet | © OpenStreetMap Terms

Location not accurate? [Update your IP location](#)

Click Here to Hide My IP