# Internet Blocking Exposed

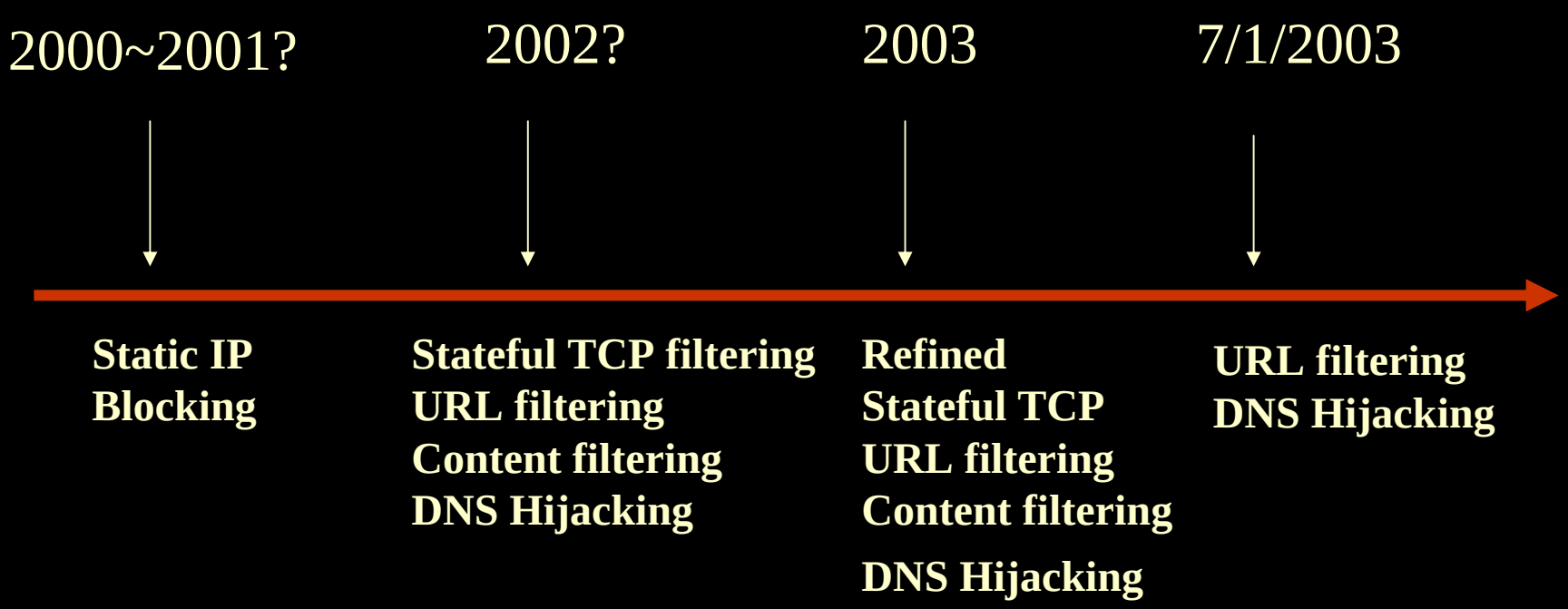
Global Internet Freedom
July 2002

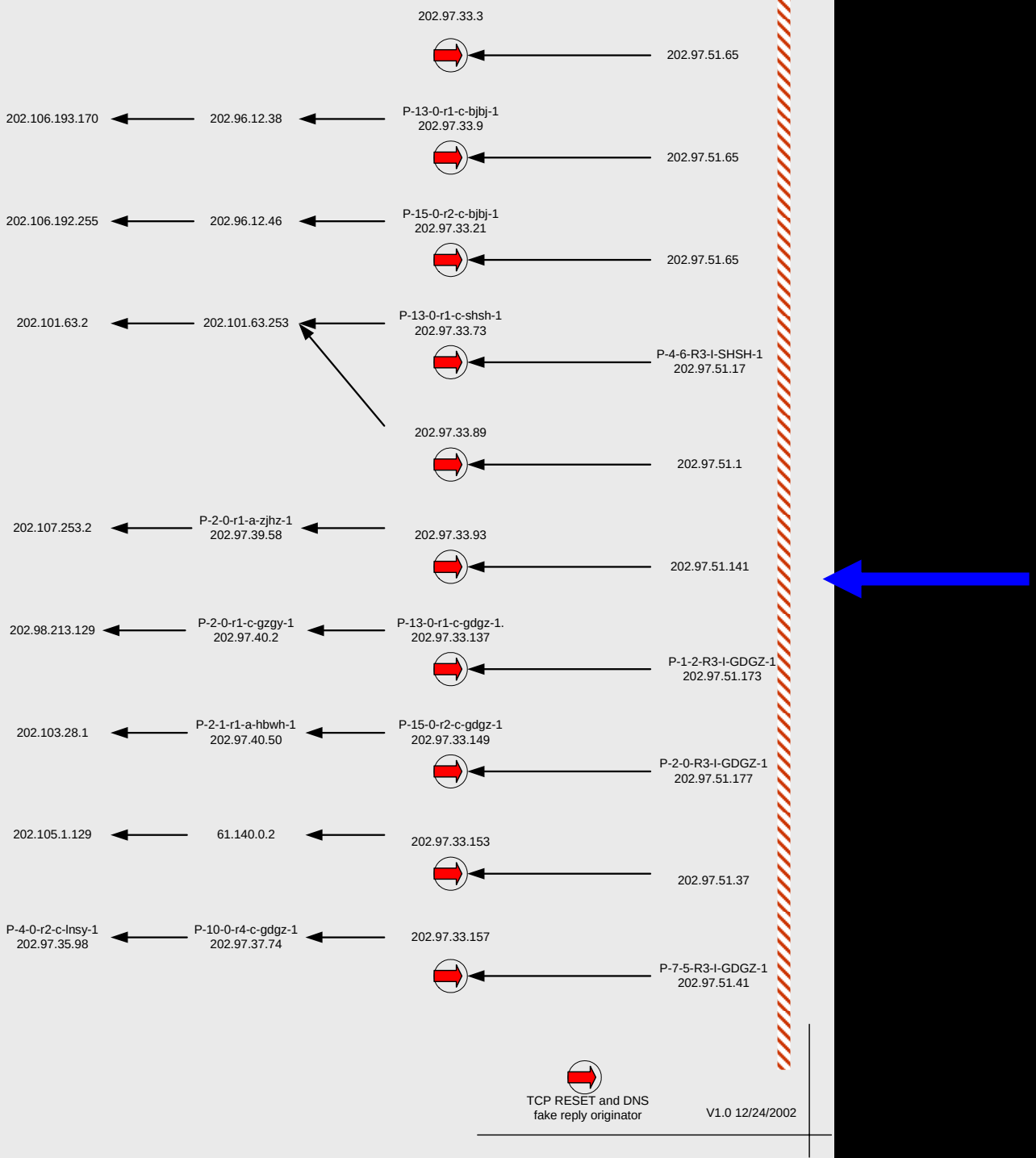
1. Overview
2. DNS Hijacking
3. TCP/IP Filtering
4. Fight Back

1. **Overview**

- **Timeline of Blocking**
- **Network Topology**

# Timeline

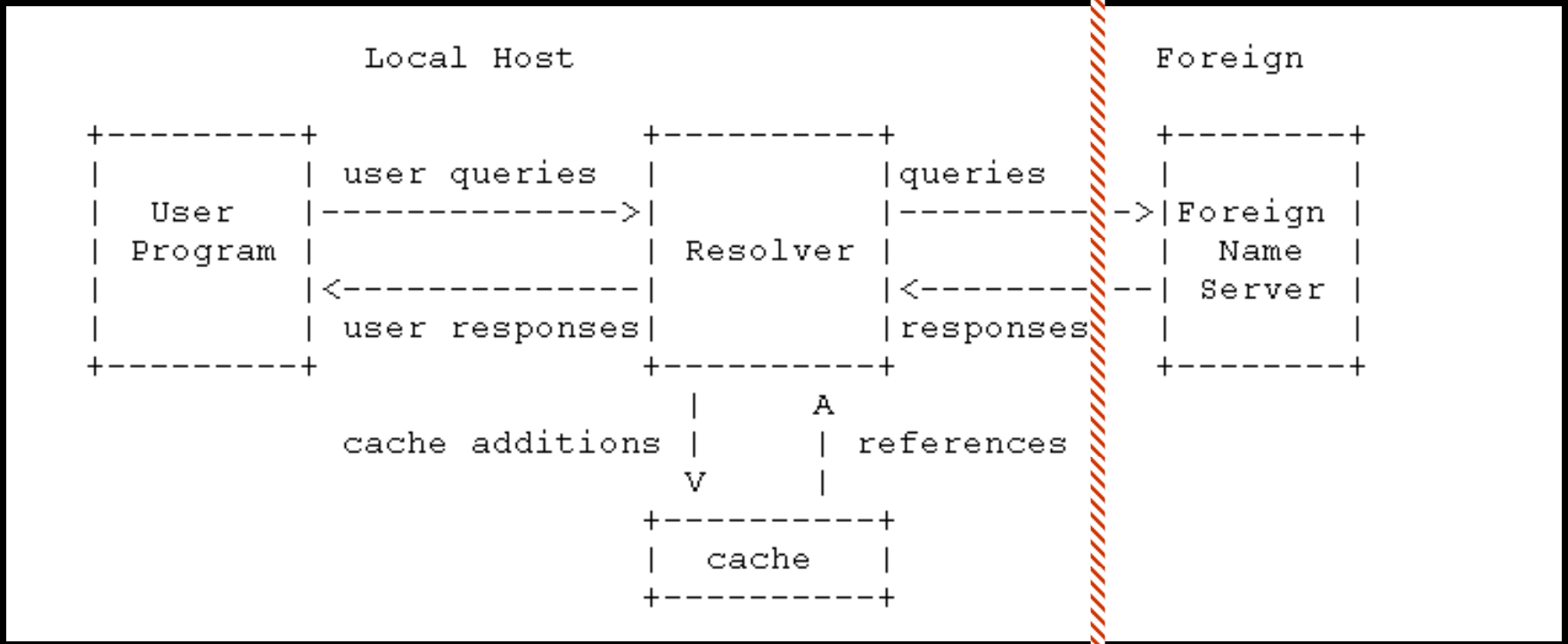

2000~2001?
2002?
2003
7/1/2003
Static IP Blocking
Stateful TCP filtering
URL filtering
Content filtering
DNS Hijacking
Refined Stateful TCP
URL filtering
Content filtering
DNS Hijacking
URL filtering
DNS Hijacking


202.97.33.3
202.97.51.65
202.106.193.170
202.96.12.38
P-13-0-r1-c-bjbj-1
202.97.33.9
202.97.51.65
202.106.192.255
202.96.12.46
P-15-0-r2-c-bjbj-1
202.97.33.21
202.97.51.65
202.101.63.2
202.101.63.253
P-13-0-r1-c-shsh-1
202.97.33.73
P-4-6-R3-I-SHSH-1
202.97.51.17
202.97.33.89
202.97.51.1
202.107.253.2
P-2-0-r1-a-zjhz-1
202.97.39.58
202.97.33.93
202.97.51.141
202.98.213.129
P-2-0-r1-c-gzgy-1
202.97.40.2
P-13-0-r1-c-gdgz-1.
202.97.33.137
P-1-2-R3-I-GDGZ-1
202.97.51.173
202.103.28.1
P-2-1-r1-a-hbwh-1
202.97.40.50
P-15-0-r2-c-gdgz-1
202.97.33.149
P-2-0-R3-I-GDGZ-1
202.97.51.177
202.105.1.129
61.140.0.2
202.97.33.153
202.97.51.37
P-4-0-r2-c-lnsy-1
202.97.35.98
P-10-0-r4-c-gdgz-1
202.97.37.74
202.97.33.157
P-7-5-R3-I-GDGZ-1
202.97.51.41
TCP RESET and DNS
fake reply originator
V1.0 12/24/2002

## 2. DNS Hijacking

- How DNS Works
- DNS Hijacking Exposed
- Past and Present

# How DNS Works

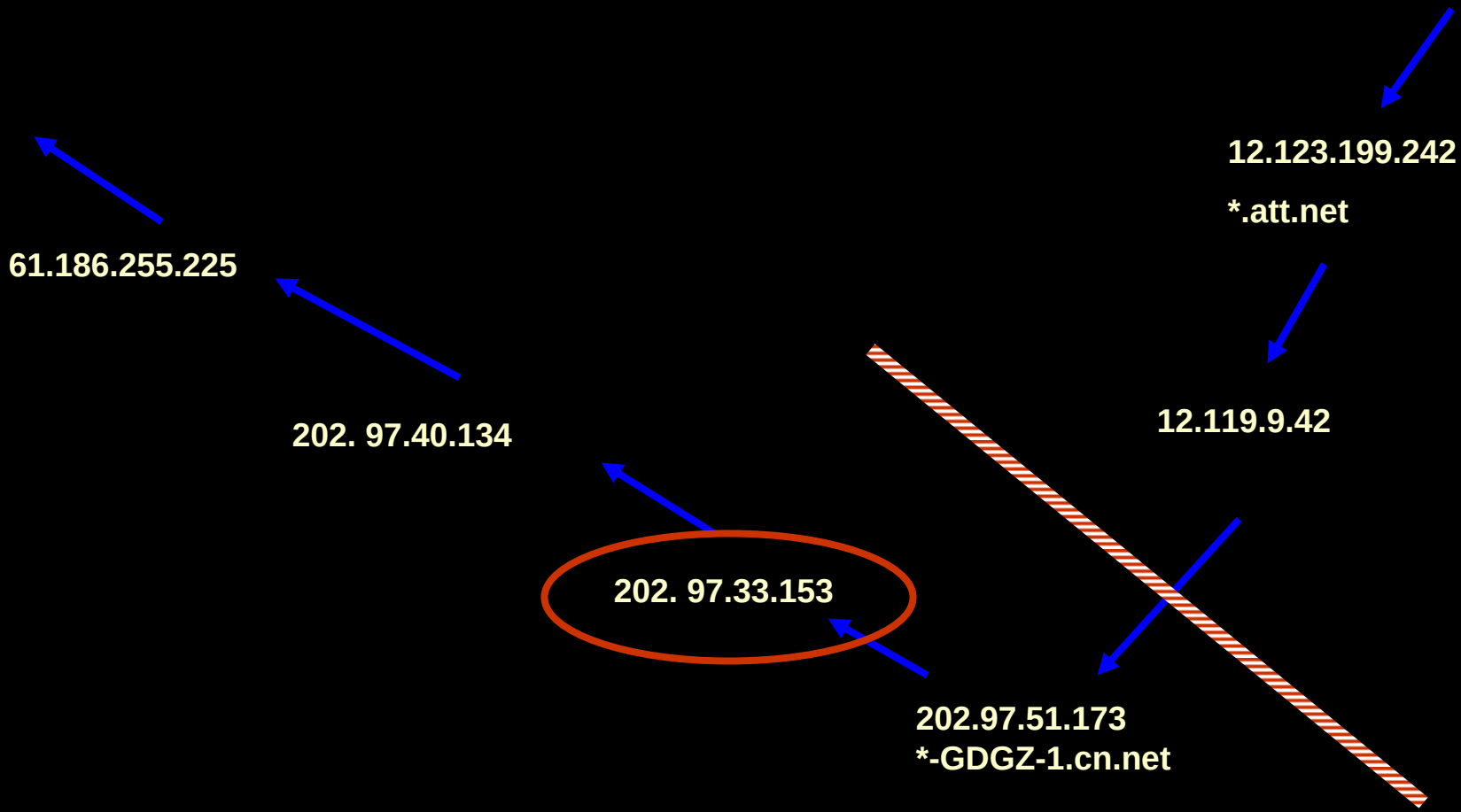


# DNS HJ exposed: look at the surface

```
$ nslookup
> server ns.cta.net.cn
Default server: ns.cta.net.cn
Address: 61.128.192.68#53
> www.google.com
Address: 216.239.33.99
> www.minghui.cc
Address: 216.127.147.245
> www.no-ip.com
Address: 88.88.88.88
> www.no-ip.org
Address: 64.33.88.161
> www.epochtimes.com
Address: 65.80.152.100
```

# DNS HJ exposed: look deeper

```
[lis@X8 lis]$ /usr/sbin/traceroute dns.cta.net.cn
traceroute to dns.cta.net.cn (61.128.128.68), 30 hops max, 38 byte packets
  .. ..snip.. ..
8 gbr2-p53.wswdc.ip.att.net (12.123.8.245)
9 tbr1-p012801.wswdc.ip.att.net (12.122.11.165)
10 tbr1-cl4.sl9mo.ip.att.net (12.122.10.30)
11 tbr2-p012401.sl9mo.ip.att.net (12.122.9.142)
12 tbr2-p013701.la2ca.ip.att.net (12.122.10.14)
13 gar1-p370.lsrca.ip.att.net (12.123.199.242)
14 12.119.9.42 (12.119.9.42)
15 p-1-2-R3-I-GDGZ-1.cn.net (202.97.51.173)
16 202.97.33.153 (202.97.33.153)
17 202.97.40.134 (202.97.40.134)
18 61.186.255.225 (61.186.255.225)
19 61.128.253.101 (61.128.253.101)
20 61.128.128.68 (61.128.128.68)
```


12.123.199.242
*.att.net
61.186.255.225
202. 97.40.134
12.119.9.42
202. 97.33.153
202.97.51.173
*-GDGZ-1.cn.net

# DNS HJ exposed: who is the hijacker?

```
$ nslookup
> server 12.119.9.42
> www.no-ip.org
*** [12.119.9.42] can't find www.no-ip.org: No response from server

> server 202.97.51.173
> www.no-ip.org
*** [202.97.51.173] can't find www.no-ip.org: No response from server

> server 202.97.33.153
> www.no-ip.org
Address:  65.80.152.100

> server 202.97.40.134
> www.no-ip.org
Address:  88.88.88.88
```

# DNS HJ exposed: more details

```
C:\>nslookup
> server dns.cta.net.cn
Default Server:  dns.cta.net.cn
Address:  61.128.128.68
> www.google.com
Address:  216.239.39.99
> www.no-ip.org
Address:  65.80.152.100
> abcde.no-ip.orgXYZ
Address:  88.88.88.88
> nadaily.com
Address:  64.33.88.161
> CCCCno-ip.org
Address:  65.80.152.100
> chinadaily.com
Address:  64.45.41.117
> xyz.nadaily.comXXX
Address:  88.88.88.88
```

# DNS HJ exposed: Summary

1. **Three fake IPs**:

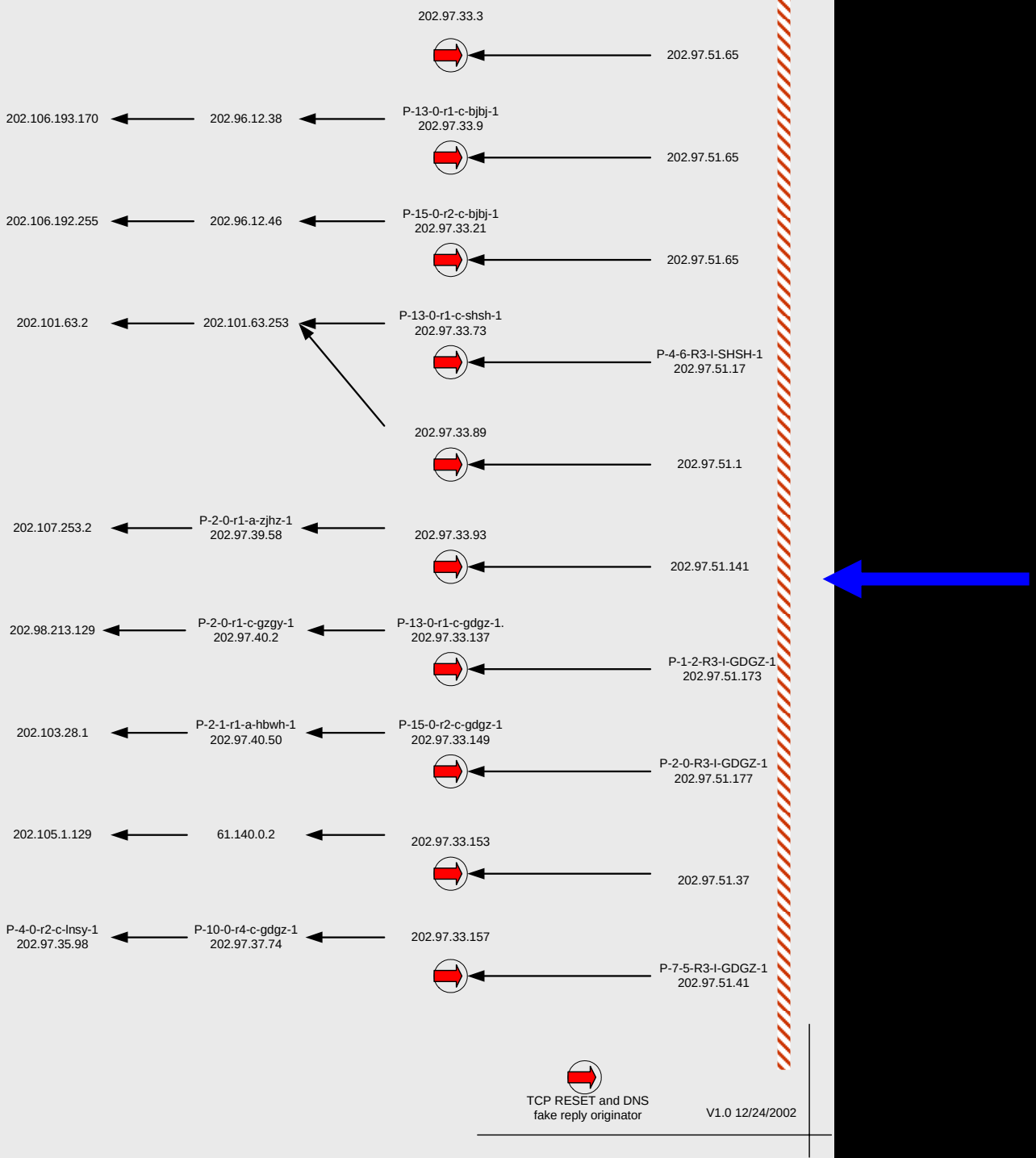
88.88.88.88  64.33.88.161  65.80.152.100

2. **HJ @ national gateway level**

3. **Fake replies have IP TTL < 50**

4. **Pattern matching**

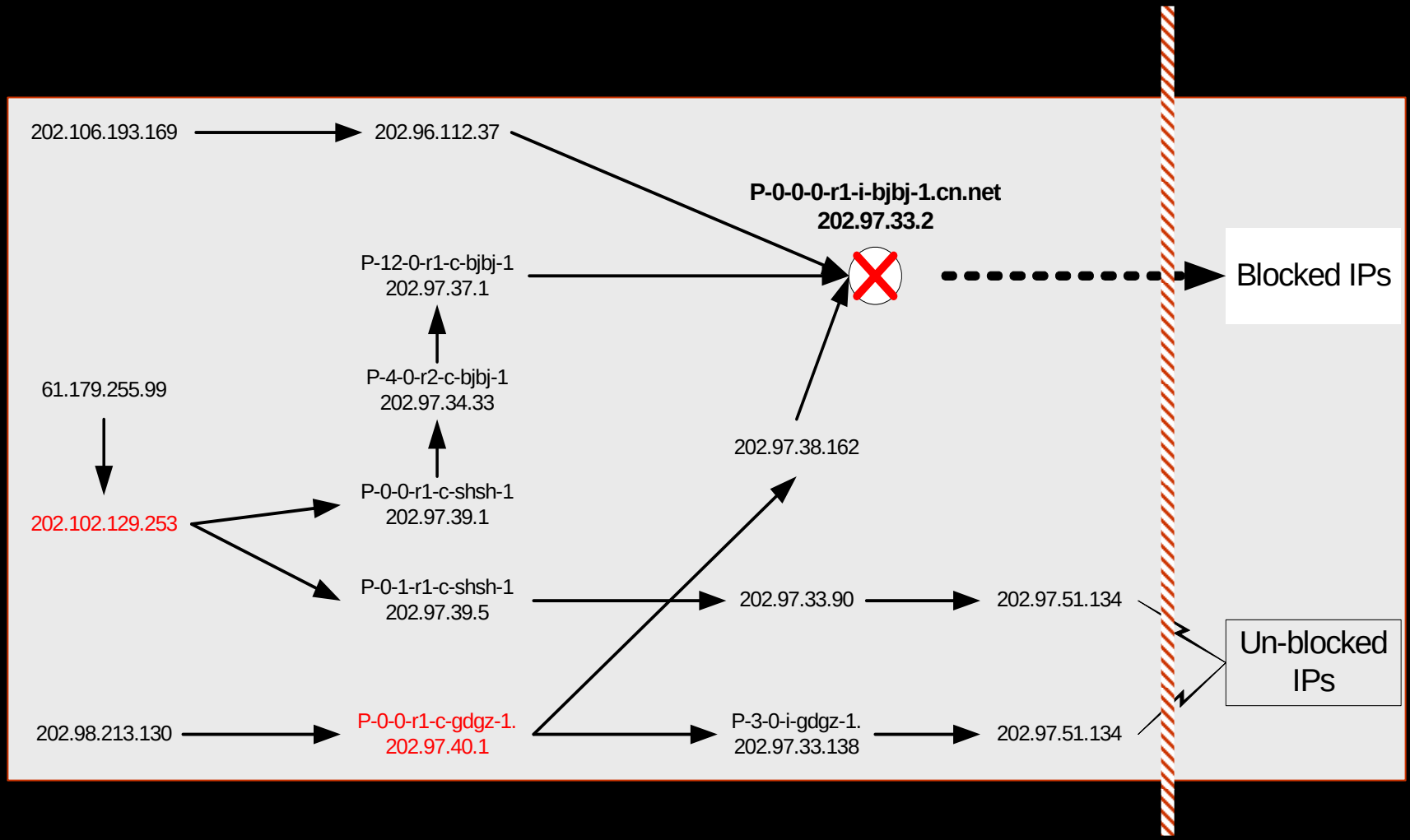
5. **Past and present**


202.97.33.3
202.97.51.65
202.106.193.170
202.96.12.38
P-13-0-r1-c-bjbj-1
202.97.33.9
202.97.51.65
202.106.192.255
202.96.12.46
P-15-0-r2-c-bjbj-1
202.97.33.21
202.97.51.65
202.101.63.2
202.101.63.253
P-13-0-r1-c-shsh-1
202.97.33.73
P-4-6-R3-I-SHSH-1
202.97.51.17
202.97.33.89
202.97.51.1
202.107.253.2
P-2-0-r1-a-zjhz-1
202.97.39.58
202.97.33.93
202.97.51.141
202.98.213.129
P-2-0-r1-c-gzgy-1
202.97.40.2
P-13-0-r1-c-gdgz-1.
202.97.33.137
P-1-2-R3-I-GDGZ-1
202.97.51.173
202.103.28.1
P-2-1-r1-a-hbwh-1
202.97.40.50
P-15-0-r2-c-gdgz-1
202.97.33.149
P-2-0-R3-I-GDGZ-1
202.97.51.177
202.105.1.129
61.140.0.2
202.97.33.153
202.97.51.37
P-4-0-r2-c-lnsy-1
202.97.35.98
P-10-0-r4-c-gdgz-1
202.97.37.74
202.97.33.157
P-7-5-R3-I-GDGZ-1
202.97.51.41
TCP RESET and DNS
fake reply originator
V1.0 12/24/2002

## 3. TCP/IP Filtering

- Static IP blocking
- Instant TCP connection reset
- Stateful TCP connection reset
- Content filtering
- Past and Present

# Static IP blocking



# Instant TCP connection reset

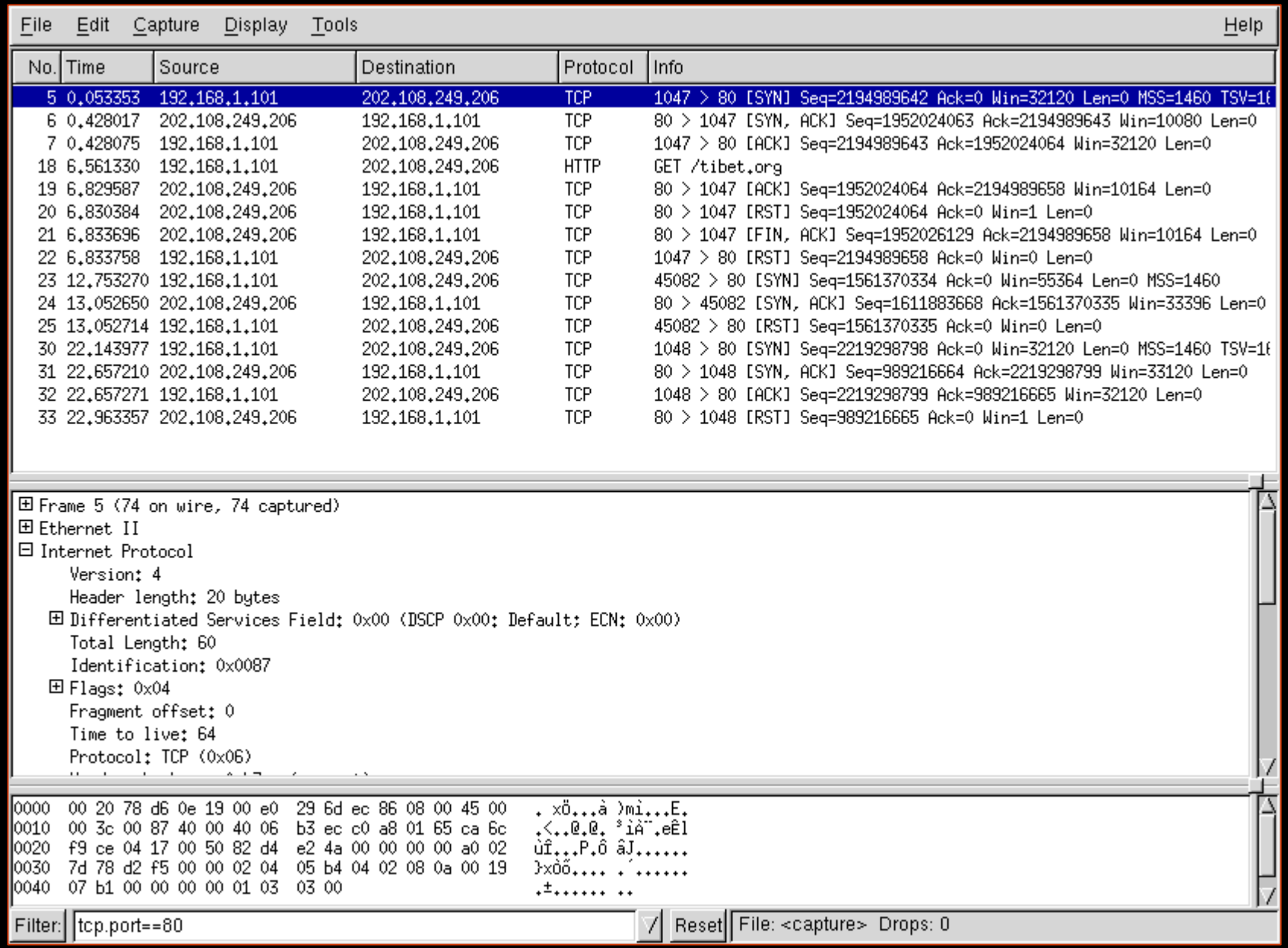
Any TCP segment containing the URL keyword pattern will induce a returning TCP RST packet from the gateway, regardless the TCP connection context

# Stateful TCP connection reset

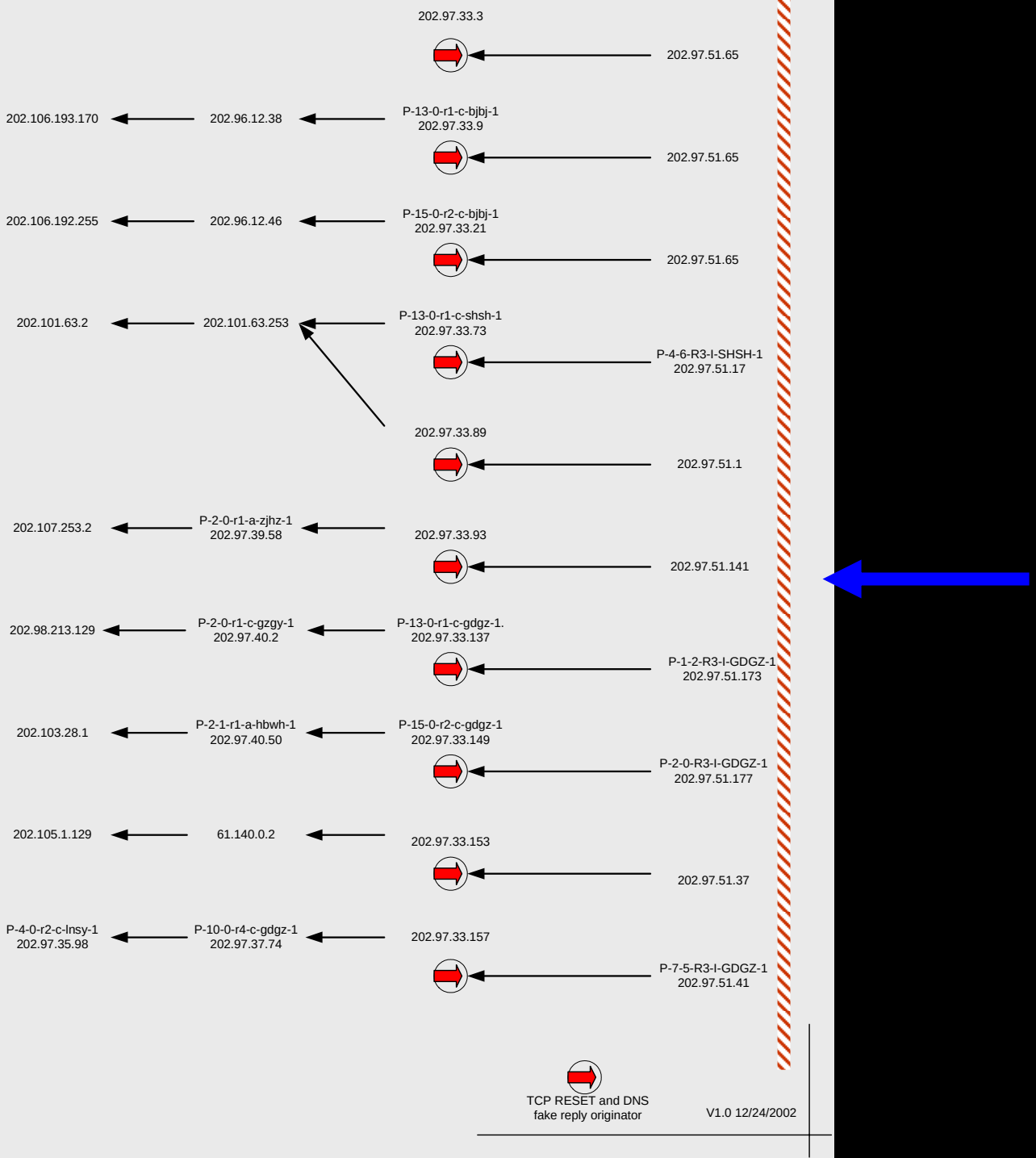
After an RST packet is triggered by URL keywords in a TCP segment, the combination of [clientIP, clientPort, serverIP, serverPort] will be remembered by the gateway for ~10min. Any subsequent TCP connection attempts during this period from the same client will be reset.

```
$ [lis@X8 lis]$ telnet www.cctv.com.cn 80
Trying 202.108.249.206...
Connected to www.cctv.com.cn.                <=== TCP connection OK
Escape character is '^]'.
GET /minghui.html                            <=== Send http request (*)
Connection closed by foreign host.           <=== Connection reset

[lis@X8 lis]$ telnet www.cctv.com.cn 80
Trying 202.108.249.206...
Connected to www.cctv.com.cn.
Escape character is '^]'.
Connection closed by foreign host.           <=== connection is blocked after
```


File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
5 0.053353 192.168.1.101 202.108.249.206 TCP 1047 > 80 [SYN] Seq=2194989642 Ack=0 Win=32120 Len=0 MSS=1460 TSV=1
6 0.428017 202.108.249.206 192.168.1.101 TCP 80 > 1047 [SYN, ACK] Seq=1952024063 Ack=2194989643 Win=10080 Len=0
7 0.428075 192.168.1.101 202.108.249.206 TCP 1047 > 80 [ACK] Seq=2194989643 Ack=1952024064 Win=32120 Len=0
18 6.561330 192.168.1.101 202.108.249.206 HTTP GET /tibet.org
19 6.829587 202.108.249.206 192.168.1.101 TCP 80 > 1047 [ACK] Seq=1952024064 Ack=2194989658 Win=10164 Len=0
20 6.830384 202.108.249.206 192.168.1.101 TCP 80 > 1047 [RST] Seq=1952024064 Ack=0 Win=1 Len=0
21 6.833696 202.108.249.206 192.168.1.101 TCP 80 > 1047 [FIN, ACK] Seq=1952026129 Ack=2194989658 Win=10164 Len=0
22 6.833758 192.168.1.101 202.108.249.206 TCP 1047 > 80 [RST] Seq=2194989658 Ack=0 Win=0 Len=0
23 12.753270 192.168.1.101 202.108.249.206 TCP 45082 > 80 [SYN] Seq=1561370334 Ack=0 Win=55364 Len=0 MSS=1460
24 13.052650 202.108.249.206 192.168.1.101 TCP 80 > 45082 [SYN, ACK] Seq=1611883668 Ack=1561370335 Win=33396 Len=0
25 13.052714 192.168.1.101 202.108.249.206 TCP 45082 > 80 [RST] Seq=1561370335 Ack=0 Win=0 Len=0
30 22.143977 192.168.1.101 202.108.249.206 TCP 1048 > 80 [SYN] Seq=2219298798 Ack=0 Win=32120 Len=0 MSS=1460 TSV=1
31 22.657210 202.108.249.206 192.168.1.101 TCP 80 > 1048 [SYN, ACK] Seq=989216664 Ack=2219298799 Win=33120 Len=0
32 22.657271 192.168.1.101 202.108.249.206 TCP 1048 > 80 [ACK] Seq=2219298799 Ack=989216665 Win=32120 Len=0
33 22.963357 202.108.249.206 192.168.1.101 TCP 80 > 1048 [RST] Seq=989216665 Ack=0 Win=1 Len=0
Frame 5 (74 on wire, 74 captured)
Ethernet II
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 60
Identification: 0x0087
Flags: 0x04
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
0000 00 20 78 d6 0e 19 00 e0 29 6d ec 86 08 00 45 00
0010 00 3c 00 87 40 00 40 06 b3 ec c0 a8 01 65 ca 6c
0020 f9 ce 04 17 00 50 82 d4 e2 4a 00 00 00 00 a0 02
0030 7d 78 d2 f5 00 00 02 04 05 b4 04 02 08 0a 00 19
0040 07 b1 00 00 00 00 01 03 03 00
Filter: tcp.port==80
Reset
File: <capture> Drops: 0

| Destination IP:port | 202.108.249.206:80 | | 202.108.44.208:110 | |
|---|---|---|---|---|
| keywords | Instant reset | Stateful reset | Instant reset | Stateful reset |
| "GET /tibet.org" | **Y** | **Y** | **Y** | **Y** |
| " GET /tibet.org" | N | N | N | N |
| "GET  /tibet.org" | N | N | N | N |
| "get /tibet.org" | **Y** | **Y** | **Y** | **Y** |
| "GET tibet.org" | N | N | N | N |
| "tibet.org" | N | N | N | N |
| "GET /tibet" | N | N | N | N |
| "GET /tibet.orgCCCC" | **Y** | **Y** | **Y** | **Y** |
| "GET /CCCCCtibet.org" | **Y** | **Y** | **Y** | **Y** |
| "GET /CCCCCtibet.orgDD" | **Y** | **Y** | **Y** | **Y** |
| "GET tibet.orgCCCC" | N | N | N | N |
| "HEAD /tibet.org" | N | N | N | N |
| "minghui" | N | N | N | N |
| "GET /minghui" | **Y** | **Y** | **Y** | **Y** |
| "minghui"(Chinese GB) | N | untested | N | untested |
| "Falun Gong"(Chinese GB) | N | untested | N | untested |


202.97.33.3
202.97.51.65
202.106.193.170
202.96.12.38
P-13-0-r1-c-bjbj-1
202.97.33.9
202.97.51.65
202.106.192.255
202.96.12.46
P-15-0-r2-c-bjbj-1
202.97.33.21
202.97.51.65
202.101.63.2
202.101.63.253
P-13-0-r1-c-shsh-1
202.97.33.73
P-4-6-R3-I-SHSH-1
202.97.51.17
202.97.33.89
202.97.51.1
202.107.253.2
P-2-0-r1-a-zjhz-1
202.97.39.58
202.97.33.93
202.97.51.141
202.98.213.129
P-2-0-r1-c-gzgy-1
202.97.40.2
P-13-0-r1-c-gdgz-1.
202.97.33.137
P-1-2-R3-I-GDGZ-1
202.97.51.173
202.103.28.1
P-2-1-r1-a-hbwh-1
202.97.40.50
P-15-0-r2-c-gdgz-1
202.97.33.149
P-2-0-R3-I-GDGZ-1
202.97.51.177
202.105.1.129
61.140.0.2
202.97.33.153
202.97.51.37
P-4-0-r2-c-lnsy-1
202.97.35.98
P-10-0-r4-c-gdgz-1
202.97.37.74
202.97.33.157
P-7-5-R3-I-GDGZ-1
202.97.51.41
TCP RESET and DNS
fake reply originator
V1.0 12/24/2002

# Content filtering

- “freenet” is a keyword
- Groups of RST packets
- Location of the filter has not been determined

# Content filtering

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.1.100 | 202.108.44.210 | TCP | 20000 > 25 [SYN] Seq=1427838225 Ack=0 Win=16384 Len=0 |
| 2 | 0.787388 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [SYN, ACK] Seq=3621691342 Ack=1427838226 Win=65340 Len=0 |
| 3 | 0.787518 | 192.168.1.100 | 202.108.44.210 | TCP | 20000 > 25 [ACK] Seq=1427838226 Ack=3621691343 Win=17520 Len=0 |
| 4 | 1.604619 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [PSH, ACK] Seq=3621691343 Ack=1427838226 Win=65340 Len=68 |
| 5 | 1.712073 | 192.168.1.100 | 202.108.44.210 | TCP | 20000 > 25 [ACK] Seq=1427838226 Ack=3621691411 Win=17452 Len=0 |
| 6 | 6.077520 | 192.168.1.100 | 202.108.44.210 | TCP | 20000 > 25 [PSH, ACK] Seq=1427838226 Ack=3621691411 Win=17452 Len=17 |
| 7 | 6.897580 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [ACK] Seq=3621691411 Ack=1427838243 Win=65340 Len=0 |
| 8 | 6.898894 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [PSH, ACK] Seq=3621691411 Ack=1427838243 Win=65340 Len=19 |
| 9 | 7.019694 | 192.168.1.100 | 202.108.44.210 | TCP | 20000 > 25 [ACK] Seq=1427838243 Ack=3621691430 Win=17433 Len=0 |
| 10 | 17.767742 | 192.168.1.100 | 202.108.44.210 | TCP | 20000 > 25 [PSH, ACK] Seq=1427838243 Ack=3621691430 Win=17433 Len=30 |
| 11 | 18.112669 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [RST] Seq=0 Ack=0 Win=9714 Len=0 |
| 12 | 18.113358 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [RST] Seq=0 Ack=0 Win=9714 Len=0 |
| 13 | 18.114338 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [RST] Seq=0 Ack=0 Win=9714 Len=0 |
| 14 | 18.514567 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [PSH, ACK] Seq=3621691430 Ack=1427838273 Win=65340 Len=8 |
| 15 | 18.636410 | 192.168.1.100 | 202.108.44.210 | TCP | 20000 > 25 [ACK] Seq=1427838273 Ack=3621691438 Win=17425 Len=0 |
| 16 | 19.295183 | 202.108.44.210 | 192.168.1.100 | TCP | 25 > 20000 [RST] Seq=3621691438 Ack=0 Win=0 Len=0 |

# Content filtering: test from cn

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [SYN] Seq=3174250130 Ack=0 Win=8192 Len=0 |
| 2 | 0.000097 | 192.168.1.101 | 202.107.211.186 | TCP | 9090 > 3858 [SYN, ACK] Seq=3444586310 Ack=3174250131 Win=31728 Len=0 |
| 3 | 0.479612 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [ACK] Seq=3174250131 Ack=3444586311 Win=8192 Len=0 |
| 4 | 17.612999 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [PSH, ACK] Seq=3174250131 Ack=3444586311 Win=8192 Len=25 |
| 5 | 17.613061 | 192.168.1.101 | 202.107.211.186 | TCP | 9090 > 3858 [ACK] Seq=3444586311 Ack=3174250156 Win=31728 Len=0 |
| 6 | 29.749046 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [PSH, ACK] Seq=3174250156 Ack=3444586311 Win=8192 Len=28 |
| 7 | 29.759546 | 192.168.1.101 | 202.107.211.186 | TCP | 9090 > 3858 [ACK] Seq=3444586311 Ack=3174250184 Win=31728 Len=0 |
| 8 | 29.759646 | 192.168.1.101 | 202.107.211.186 | TCP | 9090 > 3858 [PSH, ACK] Seq=3444586311 Ack=3174250184 Win=31728 Len=249 |
| 9 | 30.248951 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [RST] Seq=3174250184 Ack=0 Win=1 Len=0 |
| 10 | 30.255488 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [RST] Seq=0 Ack=3174250156 Win=46974 Len=0 |
| 11 | 30.256451 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [RST] Seq=0 Ack=3174250156 Win=46974 Len=0 |
| 12 | 30.257420 | 202.107.211.186 | 192.168.1.101 | TCP | 3858 > 9090 [RST] Seq=0 Ack=3174250156 Win=46974 Len=0 |

# Content filtering: state memory

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.1.100 | 202.108.42.72 | TCP | 4315 > 80 [SYN] Seq=2494182331 Ack=0 Win=16384 Len=0 |
| 2 | 0.250559 | 202.108.42.72 | 192.168.1.100 | TCP | 80 > 4315 [SYN, ACK] Seq=2521184274 Ack=2494182332 Win=33396 Len=0 |
| 3 | 0.250688 | 192.168.1.100 | 202.108.42.72 | TCP | 4315 > 80 [ACK] Seq=2494182332 Ack=2521184275 Win=17424 Len=0 |
| 4 | 0.252469 | 202.108.42.72 | 192.168.1.100 | TCP | 80 > 4315 [RST] Seq=2521184275 Ack=2494182332 Win=7495 Len=0 |
| 5 | 0.253082 | 202.108.42.72 | 192.168.1.100 | TCP | 80 > 4315 [RST] Seq=2521184275 Ack=2494182332 Win=7495 Len=0 |
| 6 | 0.253881 | 202.108.42.72 | 192.168.1.100 | TCP | 80 > 4315 [RST] Seq=2521184275 Ack=2494182332 Win=7495 Len=0 |

Traffic replay: min4rst
Test log review: trans.log

## 4. Fight Back

- **DNS hijacking: “feed the dog”**
- **Stateful TCP reset: flooding**
- **Content filtering: “ping-pong”**

# Ping-pong: an attempt to overflow blocker