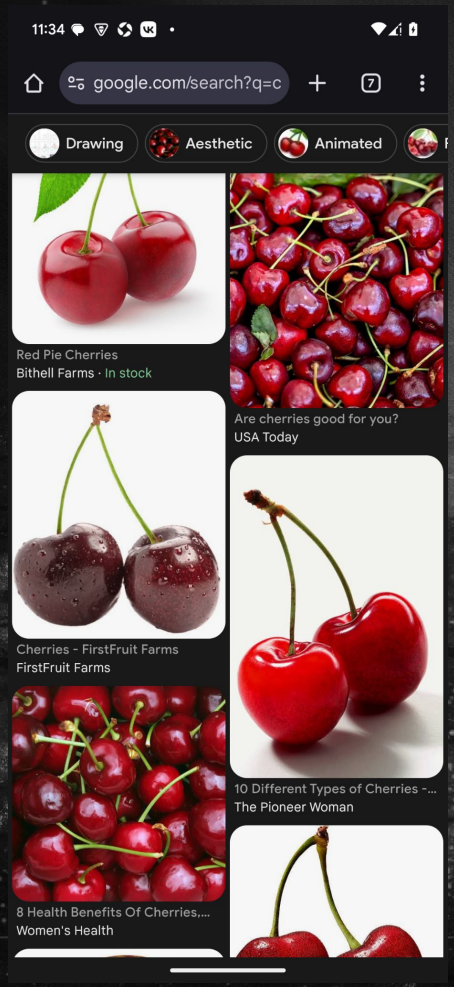
TSPU: Russia's Firewall and Defending Against the Future of Digital Repression

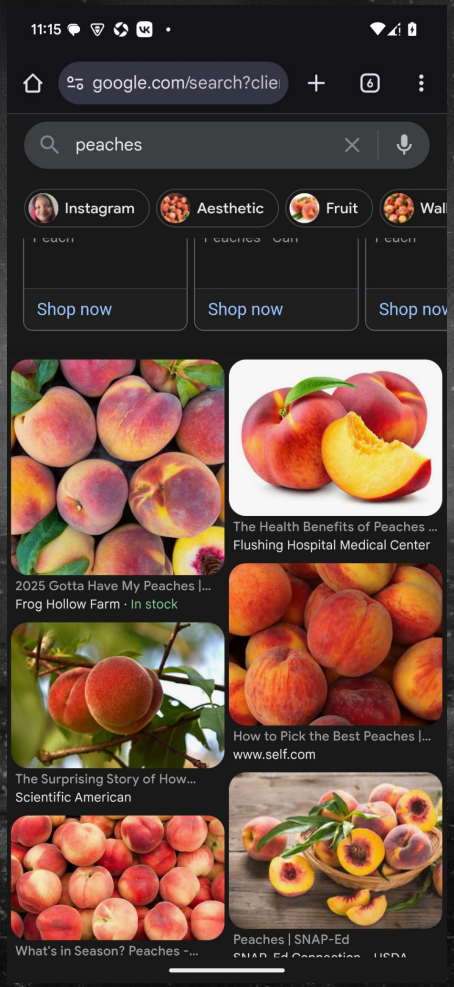




Benjamin Mixon-Baca

- Arizona State University / Breakpointing Bad
- bmixonbaca@gmail.com, Signal: bmixonbaca.22


11:34
google.com/search?q=c
Drawing
Aesthetic
Animated
Red Pie Cherries
Bithell Farms · In stock
Are cherries good for you?
USA Today
Cherries - FirstFruit Farms
FirstFruit Farms
10 Different Types of Cherries -...
The Pioneer Woman
8 Health Benefits Of Cherries,...
Women's Health


11:15
google.com/search?clie
peaches
Instagram
Aesthetic
Fruit
Shop now
Shop now
Shop now
2025 Gotta Have My Peaches |...
Frog Hollow Farm · In stock
The Health Benefits of Peaches ...
Flushing Hospital Medical Center
How to Pick the Best Peaches |...
www.self.com
The Surprising Story of How...
Scientific American
Peaches | SNAP-Ed
What's in Season? Peaches -...


11:32
mbd.baidu.com/newspa
百度一下，你就知道
APP内打开
茄子别名
背后的千年故事
盛夏时节，菜场总是挤满了圆润饱满的紫茄，它不仅是餐桌上的美味，更藏着跨越千年的文化密码。今天带大家扒一扒这颗"紫色精灵"名字背后的传奇——
变清晰
去水印
智能抠图
科技产品喵
云南
关注
🌿茄子别名背后的千年故事🌿
盛夏时节，菜场的紫茄承载着千年文化密码——
✨落苏：谐音避讳的雅称
江浙人称茄子为"落苏"，源于五代吴越王为避"瘸子"谐音，以垂落苏
公子相关，
两版故事皆
百度APP内阅读
发表你的看法

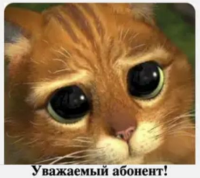
11:40 yandex.com/images/tou

Уважаемый абонент!

Данный ресурс заблокирован

Доступ к сайту ограничен в соответствии с Федеральными законами № 114-ФЗ от 25.07.2002 (О противодействии экстремистской деятельности), №436-ФЗ от 29.12.2010 (О защите детей от информации, причиняющей вред их здоровью и развитию), №149-ФЗ от 27.07.2006 (Об информации, информационных технологиях и о защите информации) и Постановлением Правительства РФ от 26.10.2012 №1101.

По всем возникшим вопросам, касающимся работы ресурса, обращайтесь к уполномоченным представителям Роскомнадзора и МинЮста.

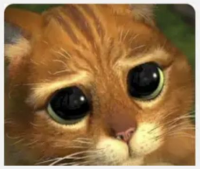


Уважаемый абонент!

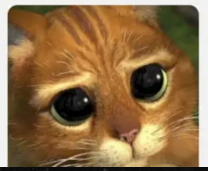
Данный ресурс заблокирован

Доступ к сайту ограничен в соответствии с Федеральными законами № 114-ФЗ от 25.07.2002 (О противодействии экстремистской деятельности), №436-ФЗ от 29.12.2010 (О защите детей от информации, причиняющей вред их здоровью и развитию), №149-ФЗ от 27.07.2006 (Об информации, информационных технологиях и о защите информации) и Постановлением Правительства РФ от 26.10.2012 №1101.

По всем возникшим вопросам, касающимся работы ресурса, обращайтесь к уполномоченным представителям Роскомнадзора и МинЮста.



По всем возникшим вопросам, касающимся работы ресурса, обращайтесь к уполномоченным представителям Роскомнадзора и МинЮста.



7:38 rt.com

THIS DOMAIN HAS BEEN SEIZED

The domains for

OVH Booter WeLeakInfo IPStress.in

have been seized by the Federal Bureau of investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the District of Columbia as part of law enforcement action taken in parallel with the Netherlands National Police Corps and the Belgium Federal Police.

THIS DOMAIN HAS BEEN SEIZED

The domains for

OVH Booter WeLeakInfo IPStress.in

have been seized by the Federal Bureau of investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the District of Columbia as part of law enforcement action taken in parallel with the Netherlands National Police Corps and the Belgium Federal Police.

THIS DOMAIN HAS BEEN SEIZED

The domains for

OVH Booter WeLeakInfo IPStress.in

have been seized by the Federal Bureau of investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the District of Columbia as part of law enforcement action taken in parallel with the Netherlands National Police Corps and the Belgium Federal Police.

11:32 mbd.baidu.com/newspa



“Hacker making a peach, cherry, and eggplant salad arrested by a drone.”



Policies

- Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»
- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон № 139-ФЗ 2012 года — дополнения «о защите детей», приведшие к созданию «Единого реестра запрещённых сайтов»;
- Федеральный закон № 187-ФЗ от 2 июля 2013 года — закон, подразумевающий возможность блокировки сайтов, содержащих нелицензионный контент, по требованию правообладателя;
- Федеральный закон № 398-ФЗ 2013 года — дополнения, связанные с блокировкой экстремистских сайтов;
- Федеральный закон № 97-ФЗ от 5 мая 2014 года — «закон о блогерах», обязывающий владельцев популярных блогов и сайтов регистрироваться в Роскомнадзоре.
- Федеральный закон № 90-ФЗ от 1 мая 2019 года — закон о «суверенном интернете», увеличение

- Federal Law of July 7, 2003 No. 126-FZ "On Communications"
- Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection"
- *Federal Law No. 139-FZ of 2012* — amendments "on the **protection of children**", which led to the creation of the "Unified Register of Prohibited Sites";
- *Federal Law No. 187-FZ of July 2, 2013* — a law implying the possibility of blocking sites containing unlicensed content at the request of the copyright holder;
- *Federal Law No. 398-FZ of 2013* — amendments related to the blocking of extremist sites;
- *Federal Law No. 97-FZ of May 5, 2014* — the "law on bloggers", obliging owners of popular blogs and sites to register with Roskomnadzor.
- Federal Law No. 90-FZ of May 1, 2019 — the law on the "sovereign Internet", increasing the stability of the Runet.

Policies

- Федеральный закон № 90-ФЗ от 1 мая 2019 года — закон о «суверенном интернете», увеличение устойчивости Рунета.

- Federal Law No. 90-FZ of May 1, 2019 — the law on the "sovereign Internet", increasing the stability of the Runet.

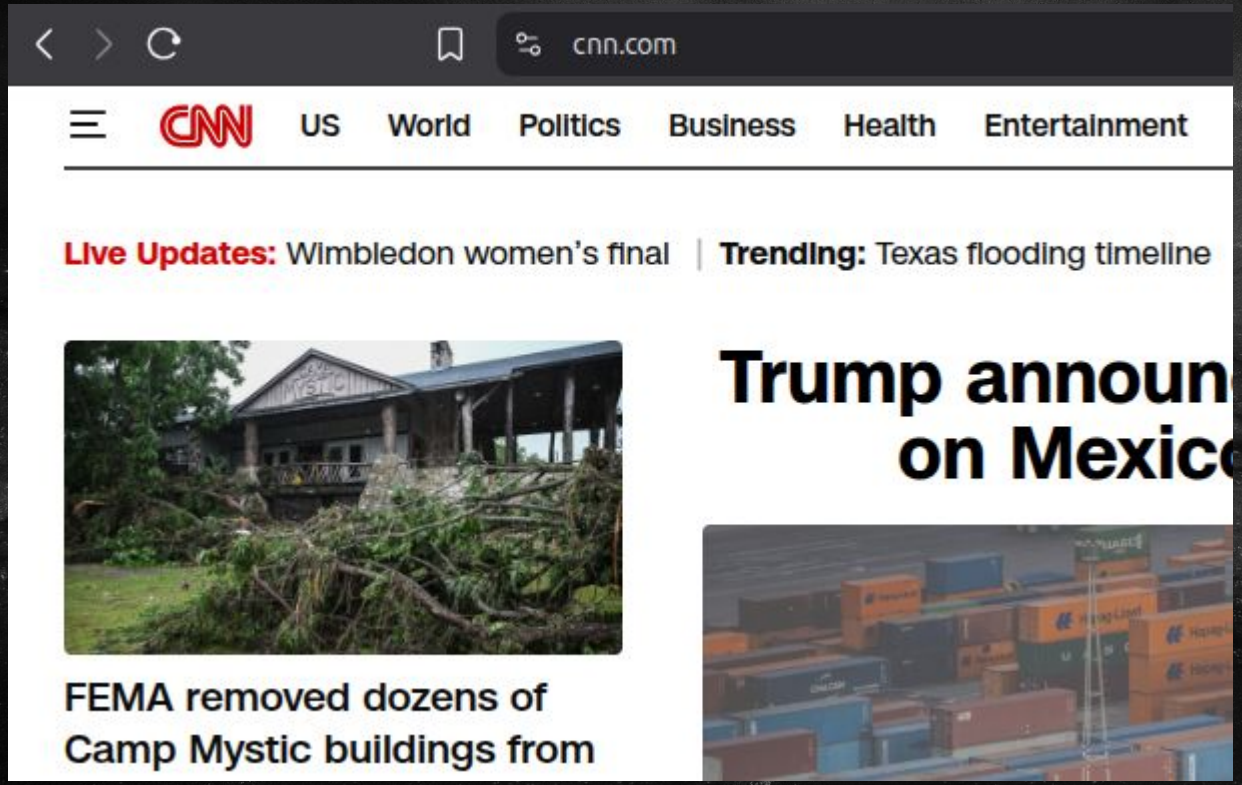
RuNet: Russia's Sovereign Internet

- Роскомнадзор (РКН)
- Rozkomnadzor (RKN)

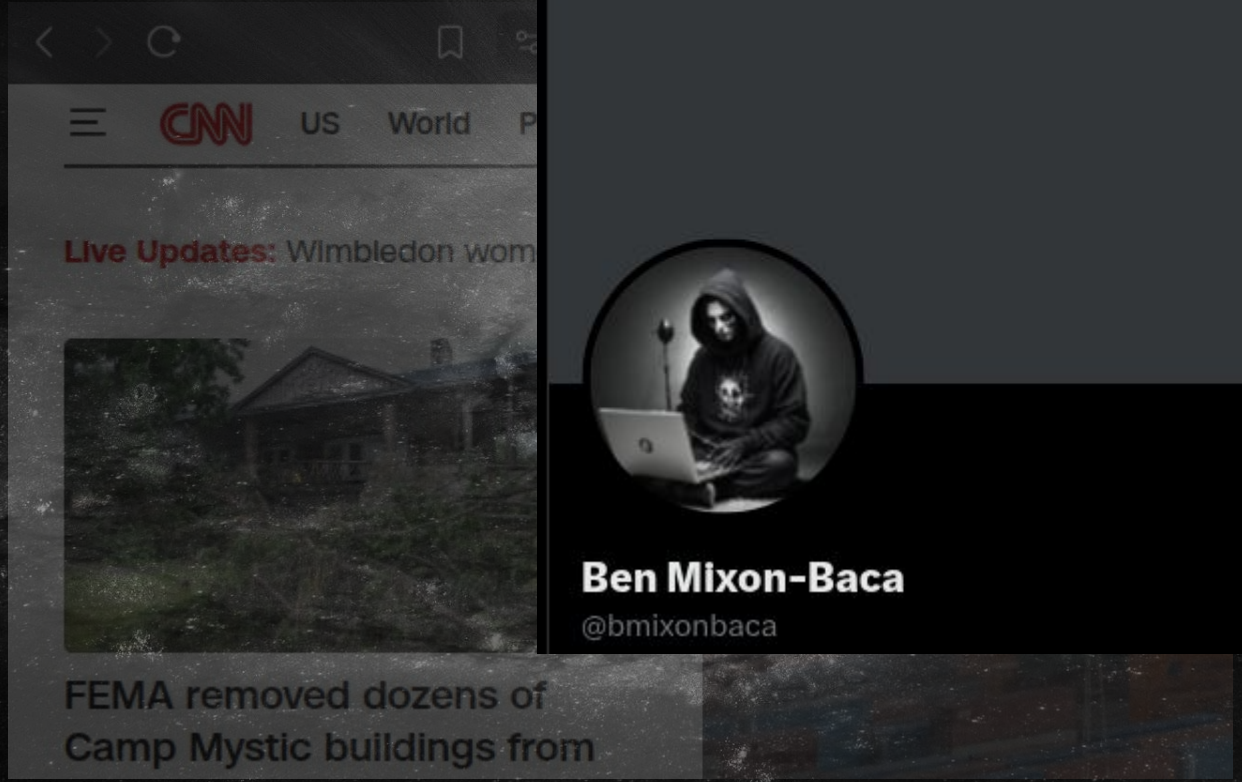


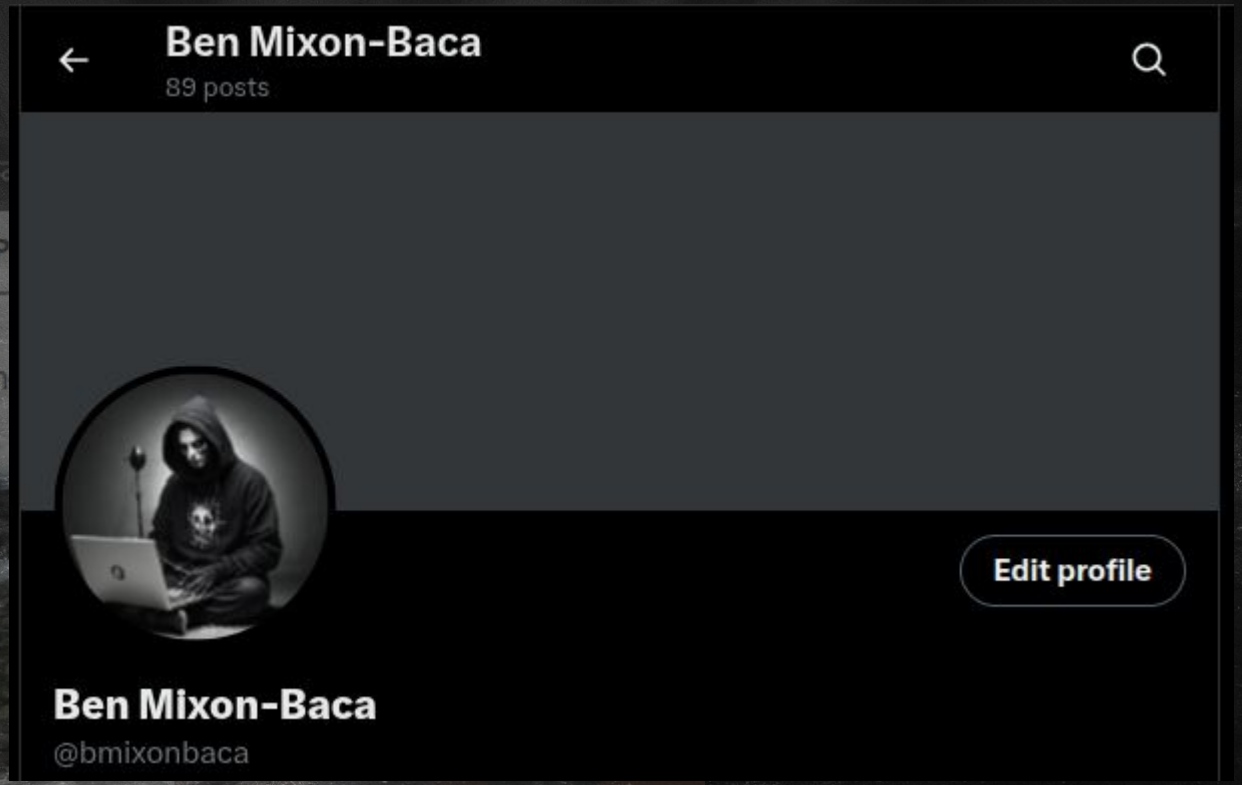
https://en.wikipedia.org/wiki/Roskomnadzor

What's Blocked?

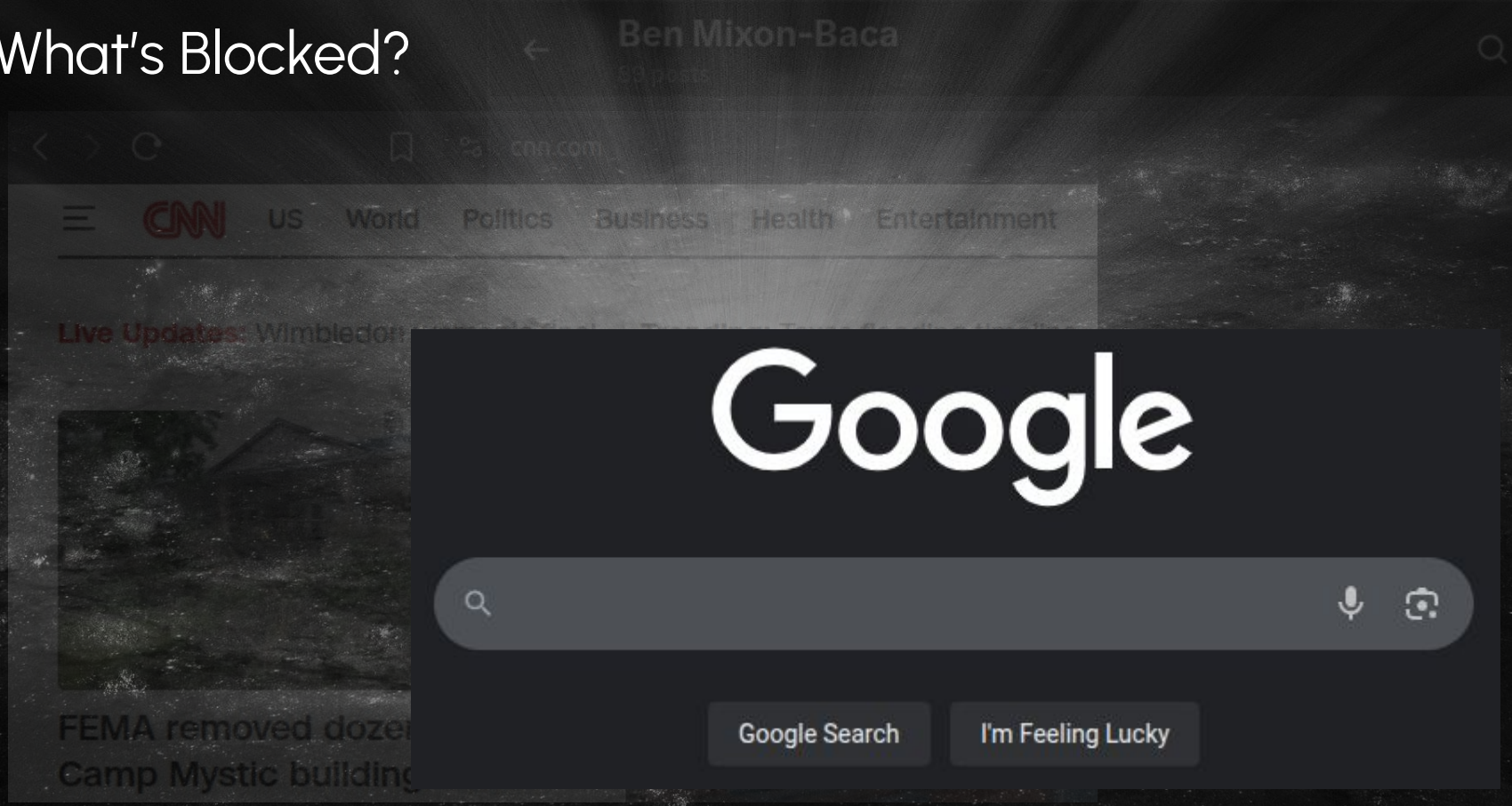


What's Blocked?

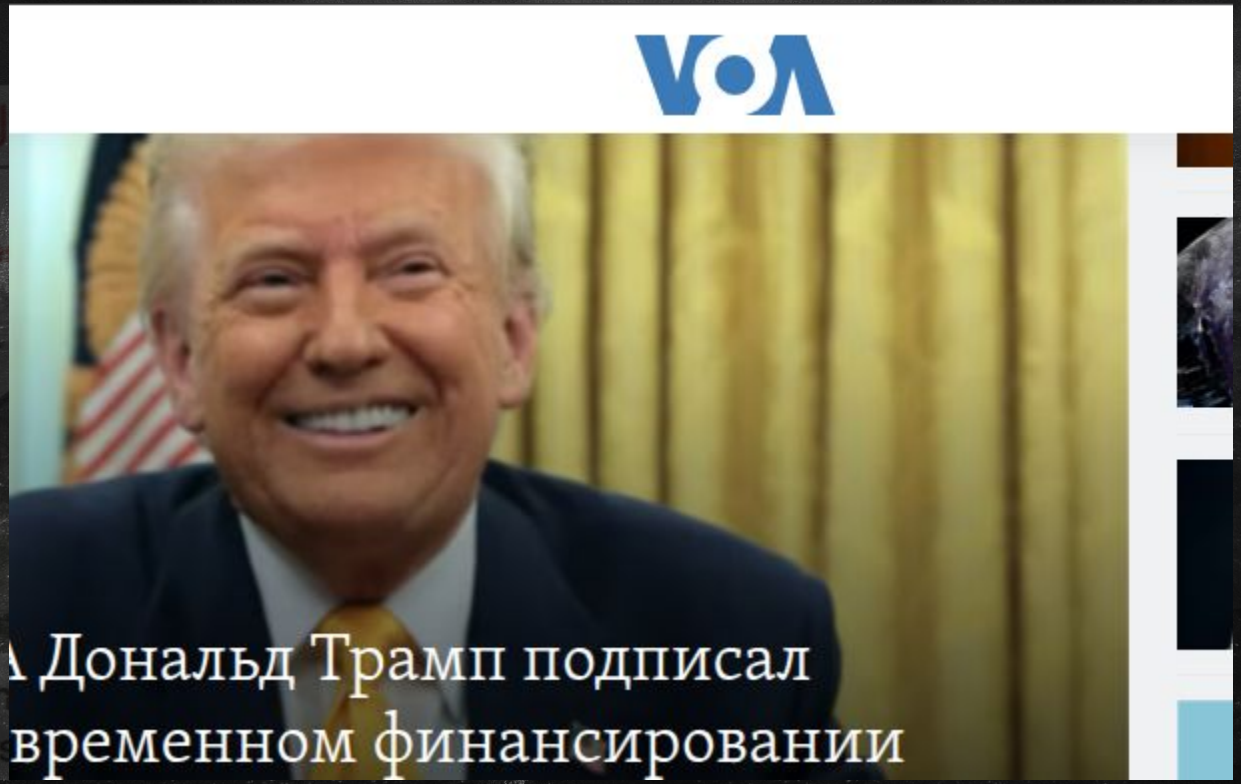




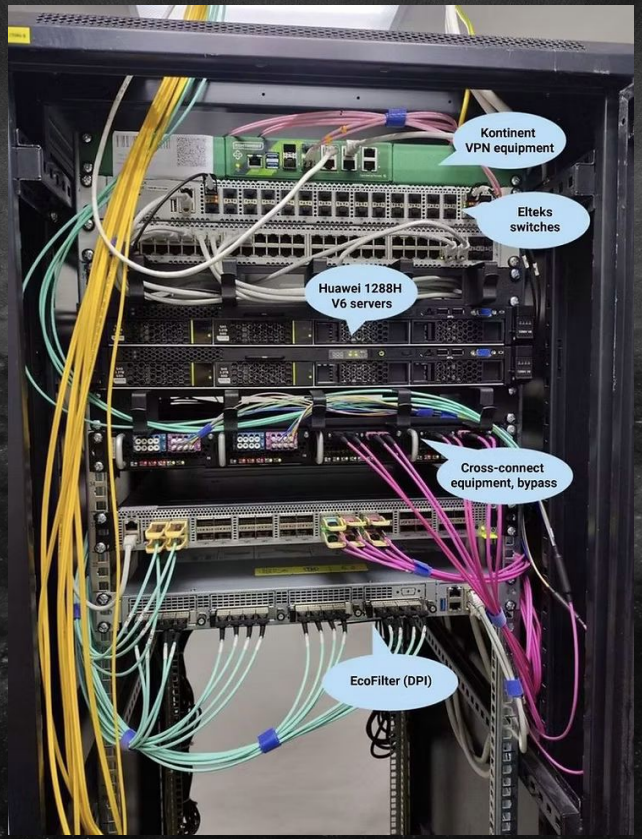
What's Blocked?



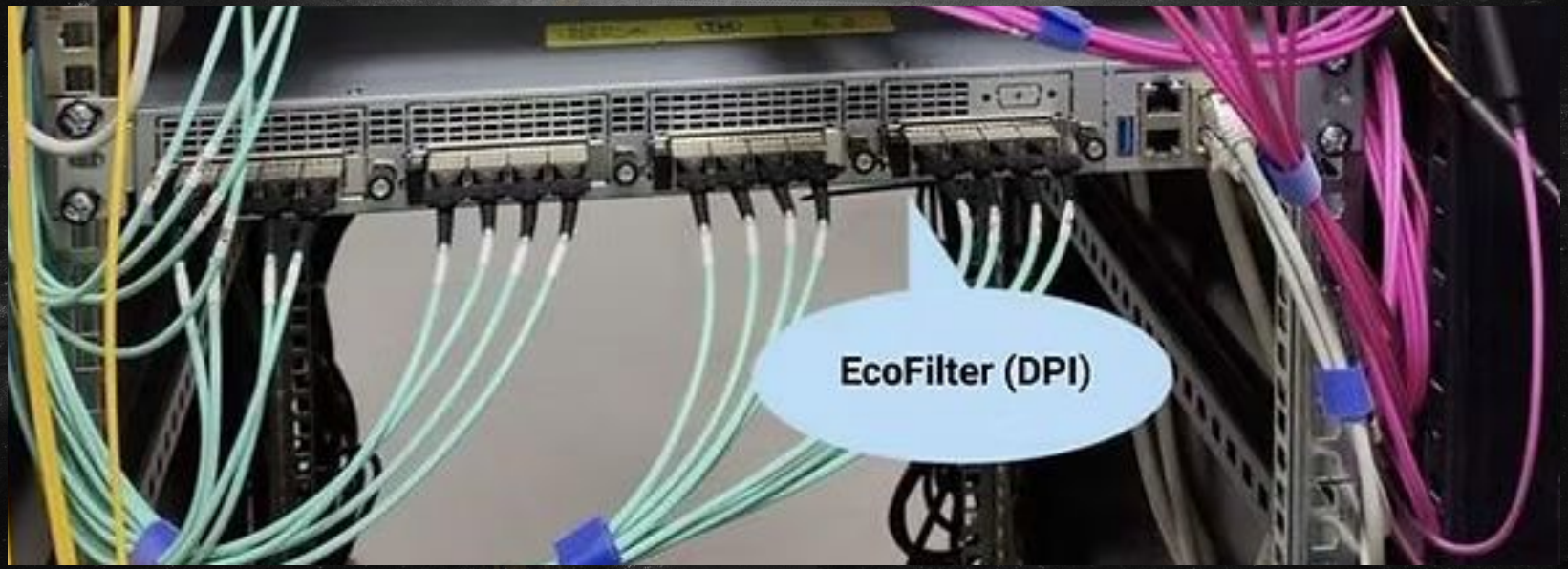
What's Blocked?



ТСПУ: технических средств противодействия угрозам



ТСПУ: технических средств противодействия угрозам



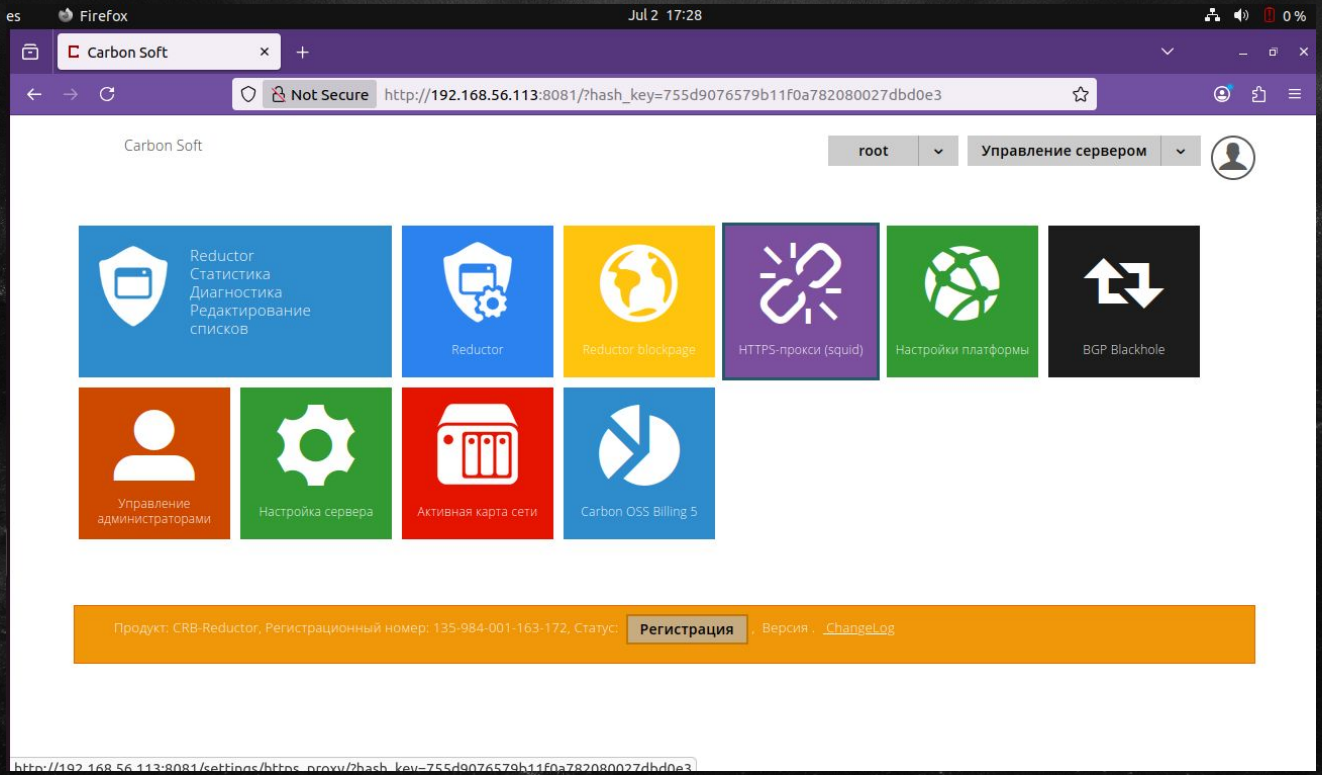
TSPU: Technical Means of Countering Threats



Devices

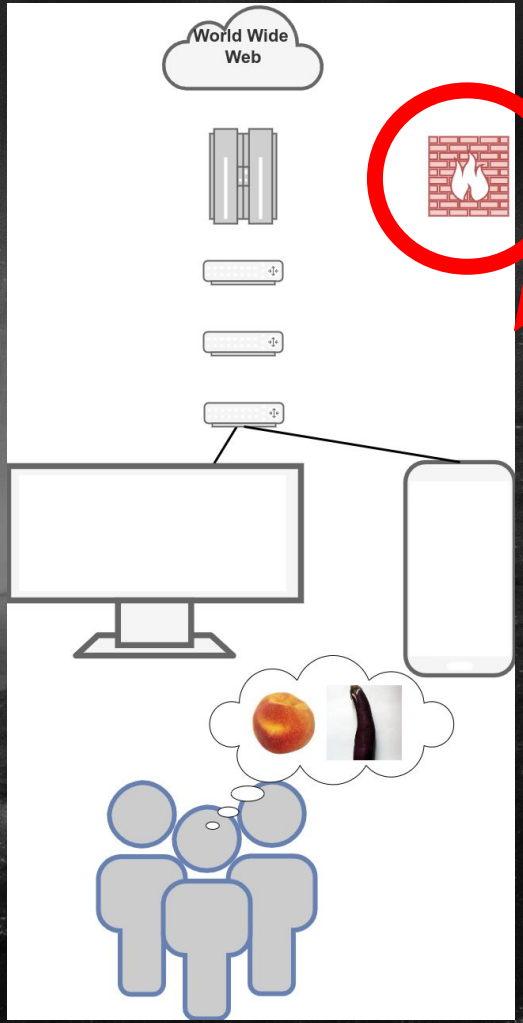
1. EcoFilter, rdp.ru
2. SKAT DPI, https://vasexperts.ru/products/skat/
3. CPAK “Equalia”, https://napalabs.ru/
4. CyberFilter, http://cyberfilter.ru/, Linux
5. Admfilter, http://adm-systems.com/,
6. Zapretservice, zapretservice.ru, Linux
7. Ideco, http://ideco.ru/, Linux
8. Carbonfilter, http://carbonsoft.ru/, Linux
9. SkyDNS Zapret, Linux
10. Tixen-Blocking
11. SKAT, vasexperts.ru
12. UBIC, q

Other Platforms - CarbonFilter



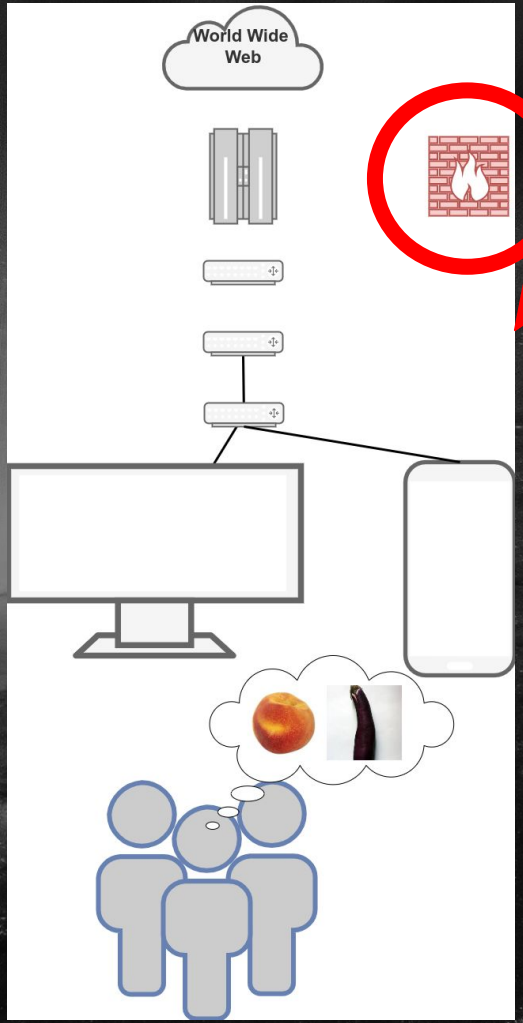
GFW est. 2005





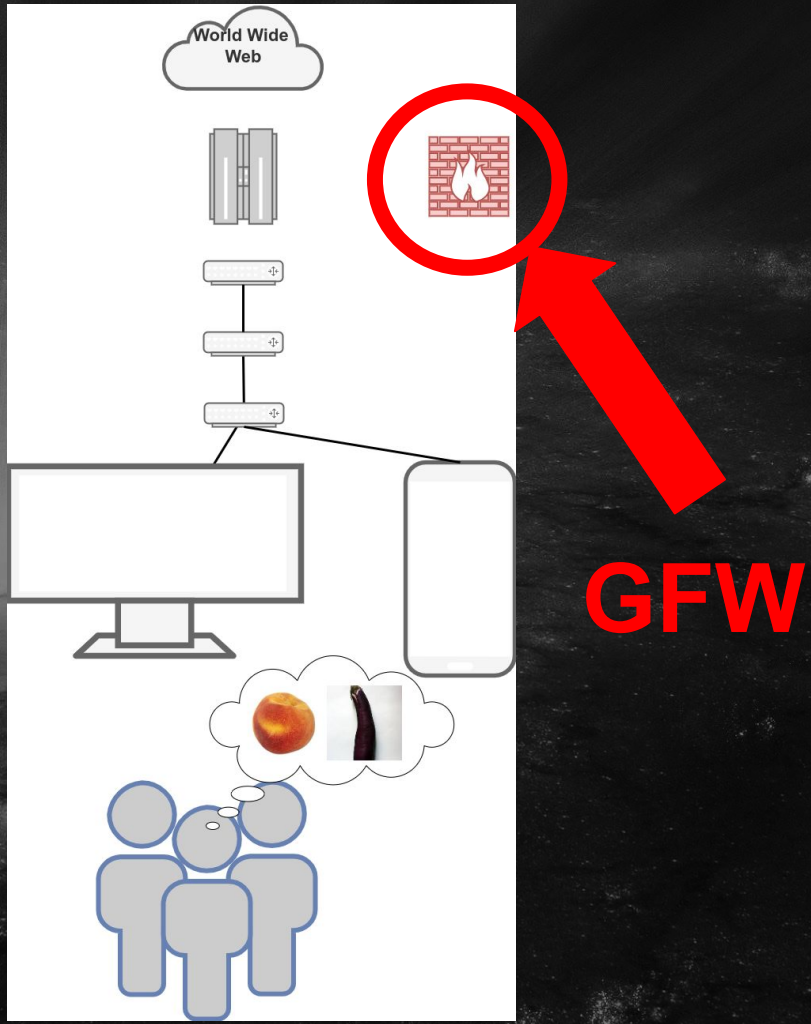
GFW est. 2005





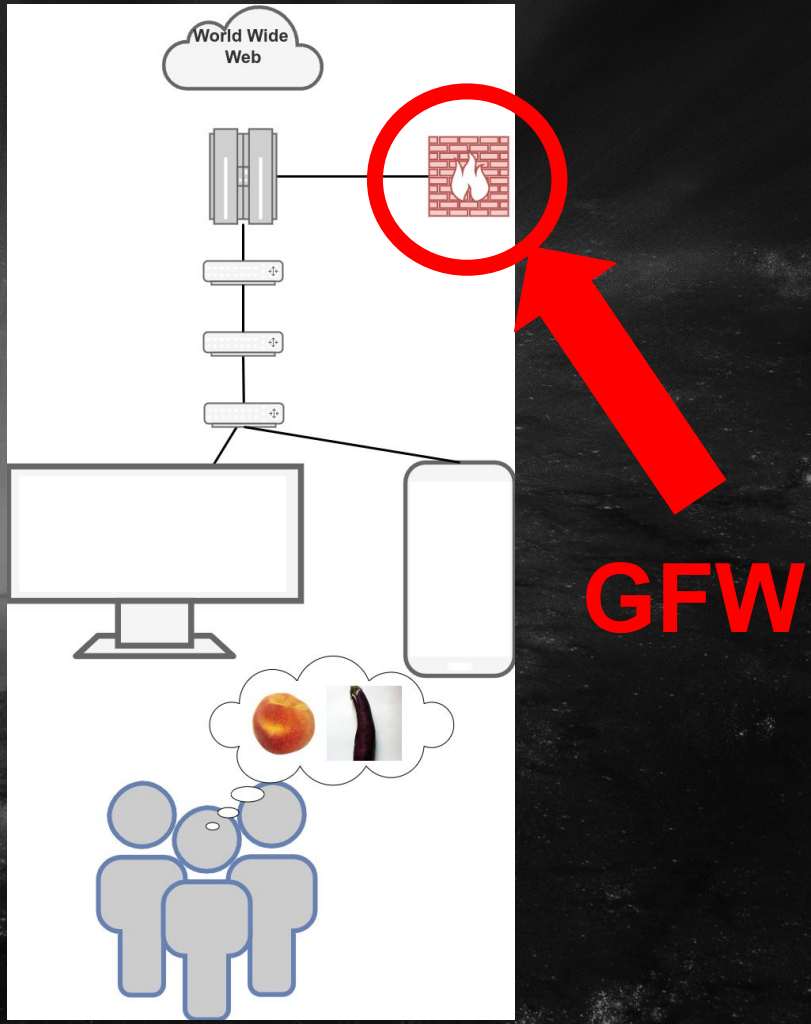
GFW est. 2005





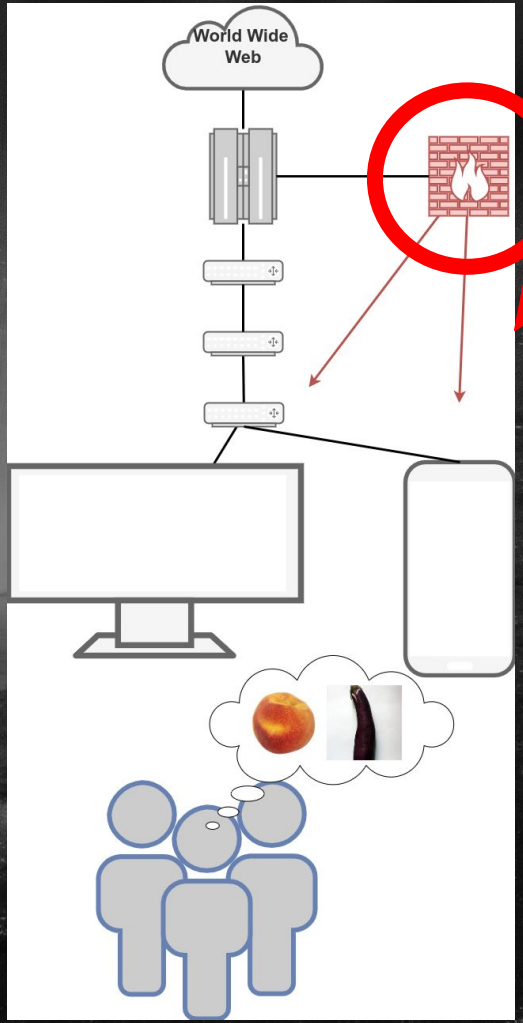
GFW est. 2005





GFW est. 2005

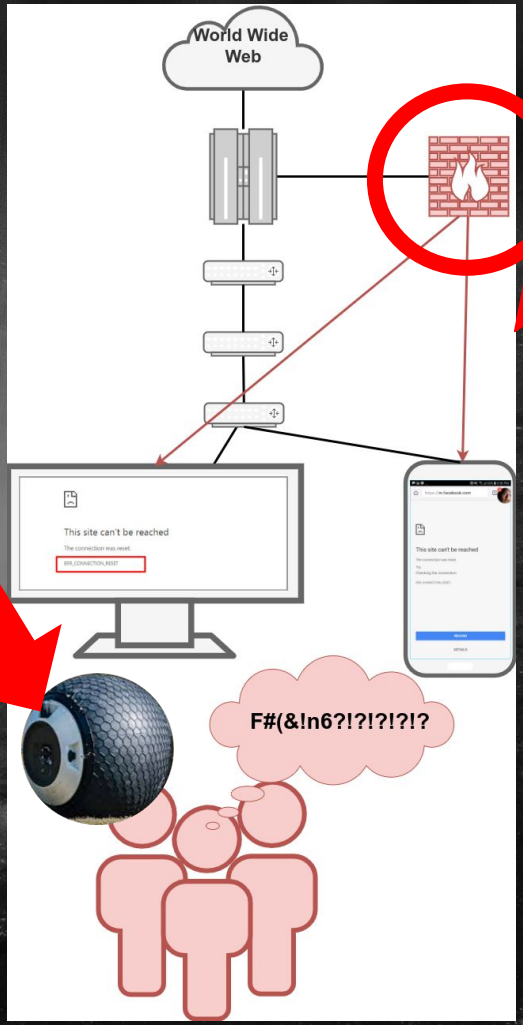




GFW est. 2005: RST Injection



Scary police drone



GFW

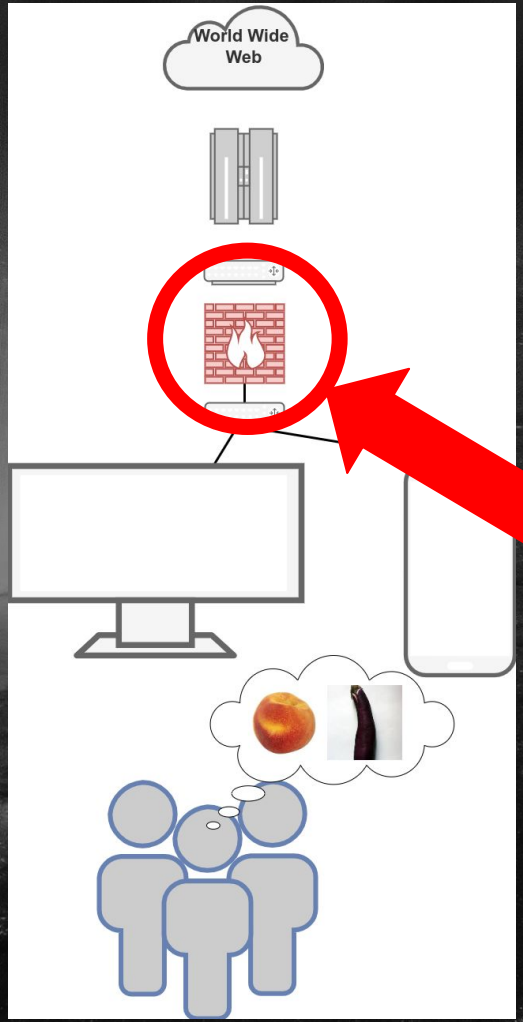
TSPU: est. 2017





TSPU: est. 2017

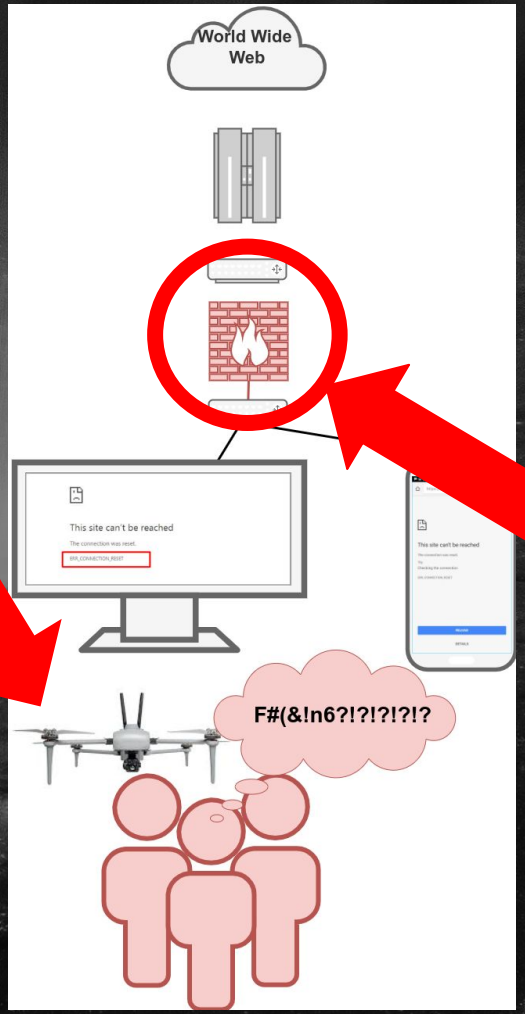




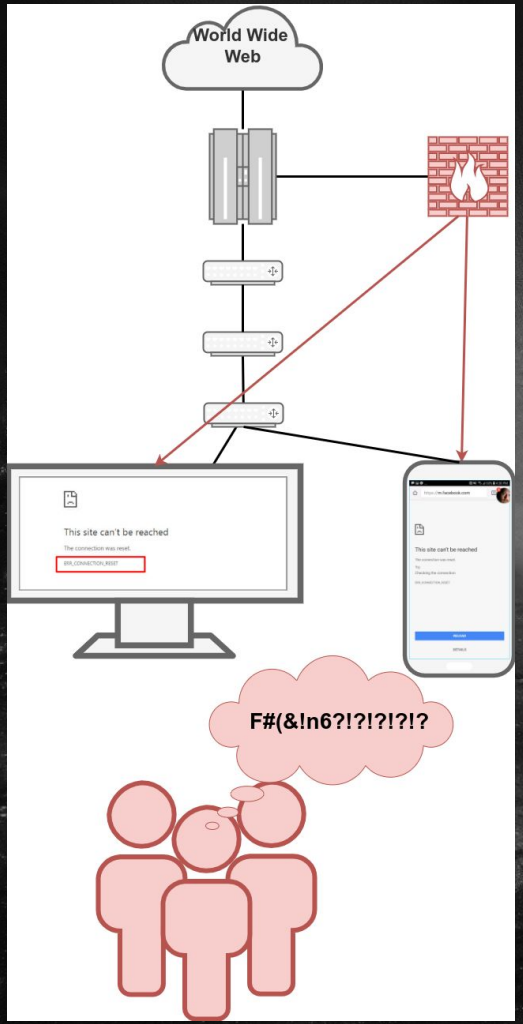
TSPU: est. 2017

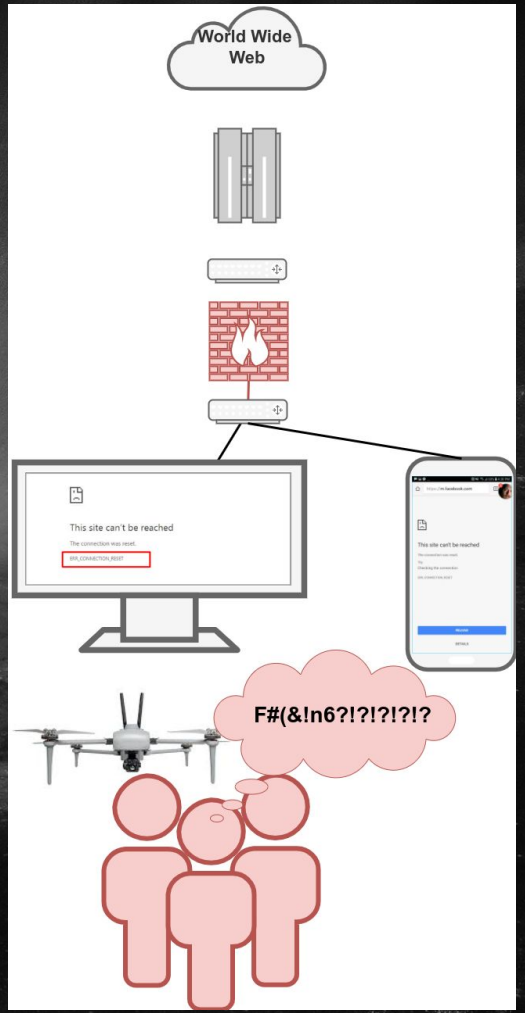


Scary police drone



TSPU


World Wide Web
This site can't be reached
F#(&!n6?!?!?!?!?

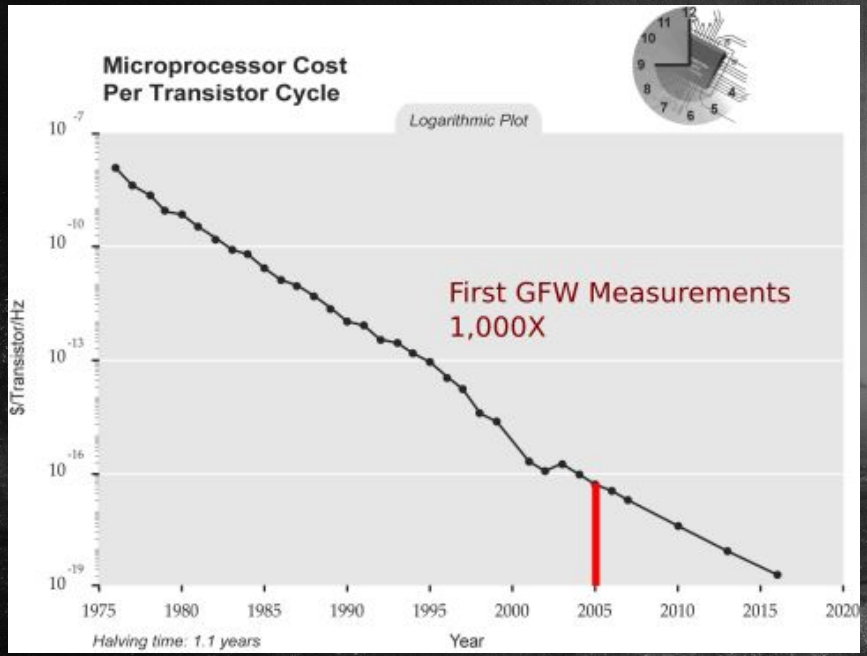

World Wide Web
This site can't be reached
F#(&!n6?!?!?!?!?

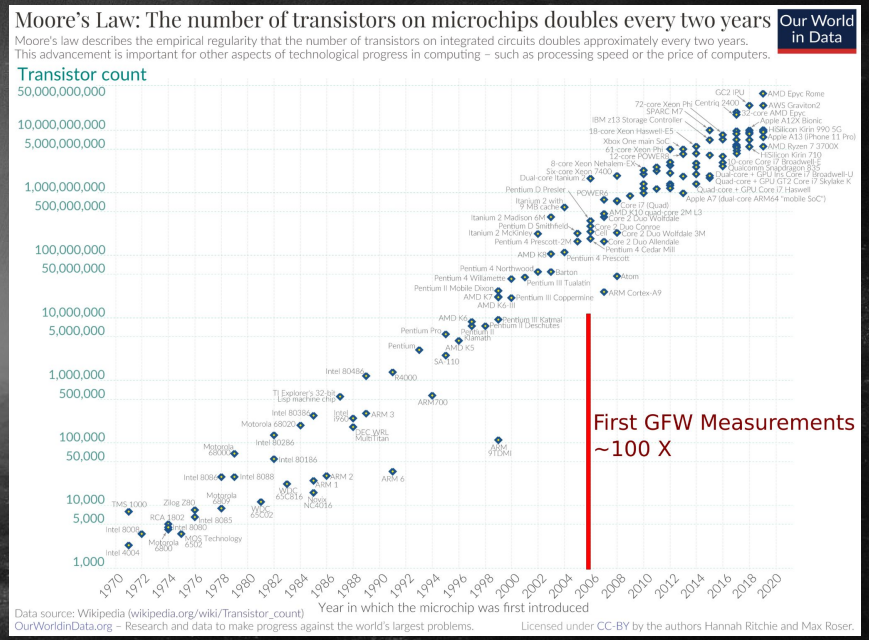

Grok

Why?

- ISP Ecosystem factors:
  - Thousands of ISPs/network operators throughout Russia
  - few in Mainland China
- Economic Factors
  - Transistors in 05-06 were 30000 X more expensive than Today
- Data Scale
  - Number of devices/person increased
  - Amount of data each person generates

Economics



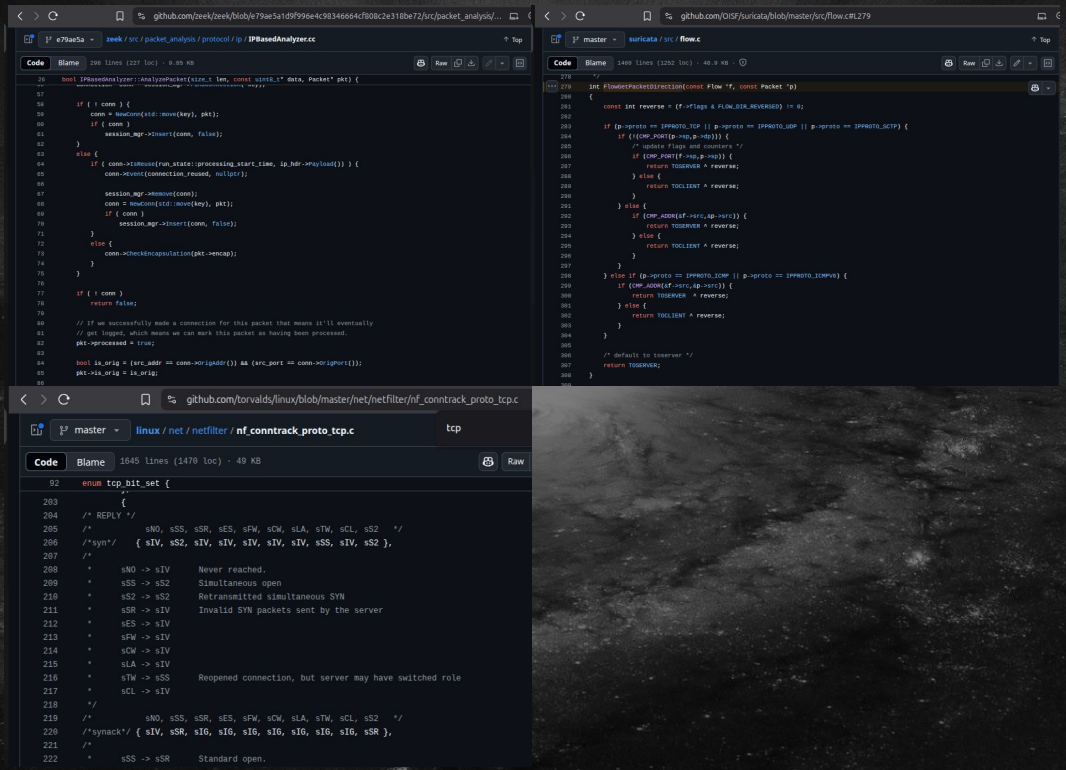


https://www.singularity.com/images/charts/MicroProcessCostPerTrans.jpg, https://en.wikipedia.org/wiki/Moore%27s_law#/media/File:Moore's_Law_Transistor_Count_1970-2020.png

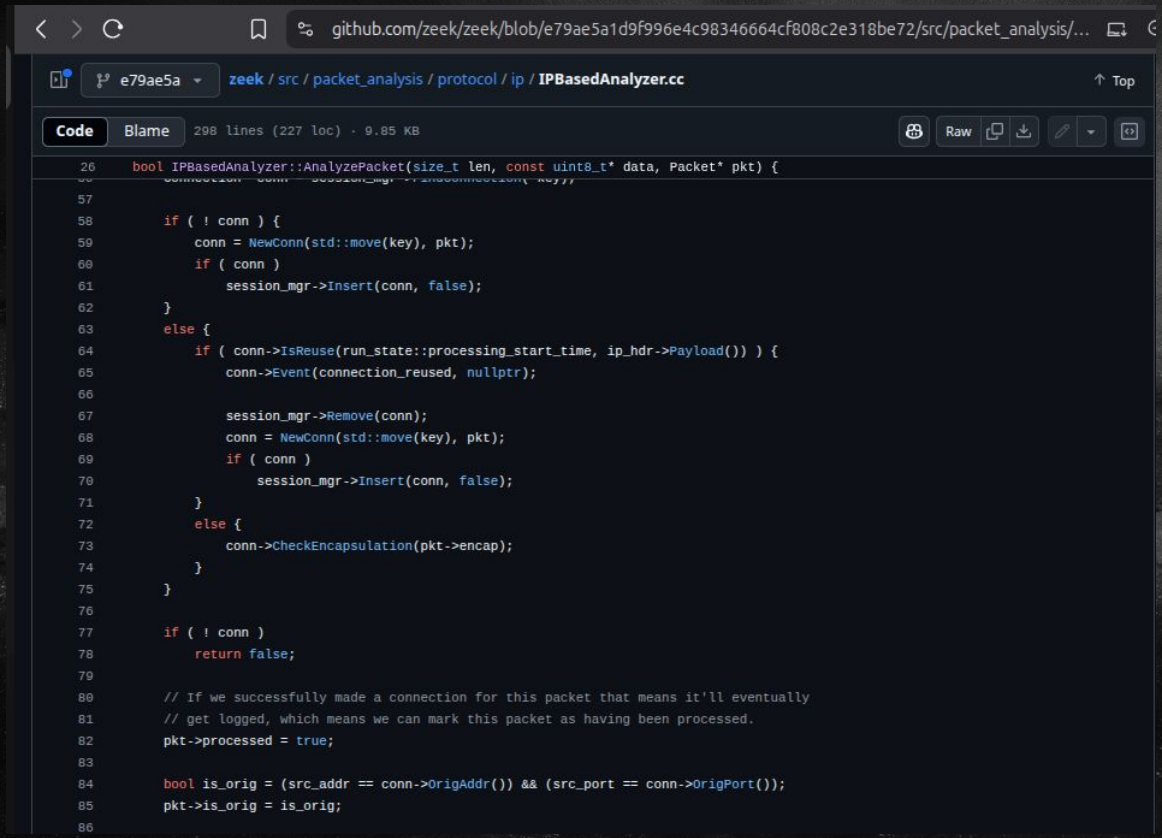
TSPU In-the-Wild

- 2019: RuNet Law Passed
- 2021: Twitter Blocking
- 2022: Ukraine War
  - Russia begins throttling Google, Twitter, and other news sites.
- Provide details on previous studies
  - How it was done
  - Mapped out TSPU architecture
  - Identified new bypass strategies

Connection Tracking



Connection Tracking: Zeek

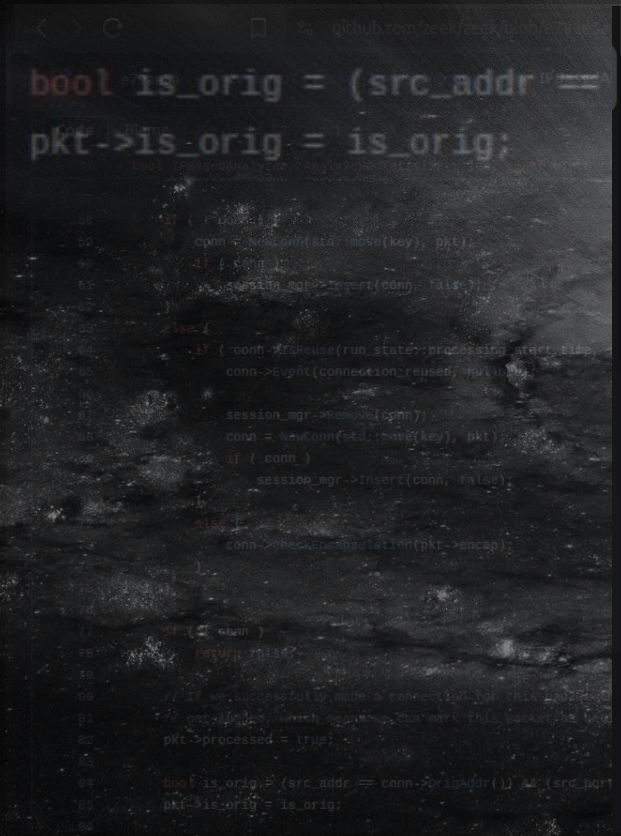



```
26  bool IPBasedAnalyzer::AnalyzePacket(size_t len, const uint8_t* data, Packet* pkt) {
57
58      if ( ! conn ) {
59          conn = NewConn(std::move(key), pkt);
60          if ( conn )
61              session_mgr->Insert(conn, false);
62      }
63      else {
64          if ( conn->IsReuse(run_state::processing_start_time, ip_hdr->Payload()) ) {
65              conn->Event(connection_reused, nullptr);
66
67              session_mgr->Remove(conn);
68              conn = NewConn(std::move(key), pkt);
69              if ( conn )
70                  session_mgr->Insert(conn, false);
71          }
72          else {
73              conn->CheckEncapsulation(pkt->encap);
74          }
75      }
76
77      if ( ! conn )
78          return false;
79
80      // If we successfully made a connection for this packet that means it'll eventually
81      // get logged, which means we can mark this packet as having been processed.
82      pkt->processed = true;
83
84      bool is_orig = (src_addr == conn->OrigAddr()) && (src_port == conn->OrigPort());
85      pkt->is_orig = is_orig;
86
```

Connection Tracking: Zeek

```
bool is_orig = (src_addr == conn->OrigAddr()) && (src_port == conn->OrigPort());
pkt->is_orig = is_orig;
```

Connection Tracking: Suricata



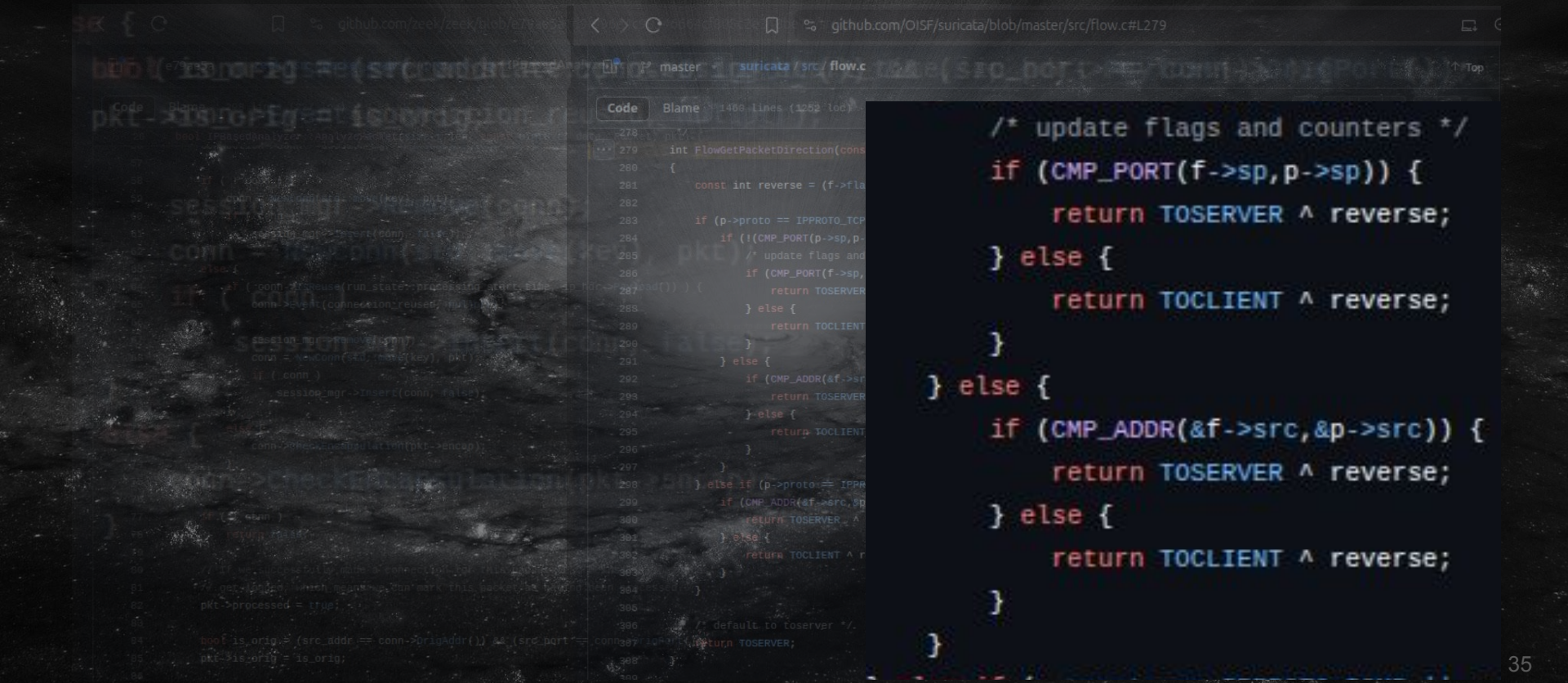
github.com/OISF/suricata/blob/master/src/flow.c#L279

master · suricata / src / flow.c · ↑ Top

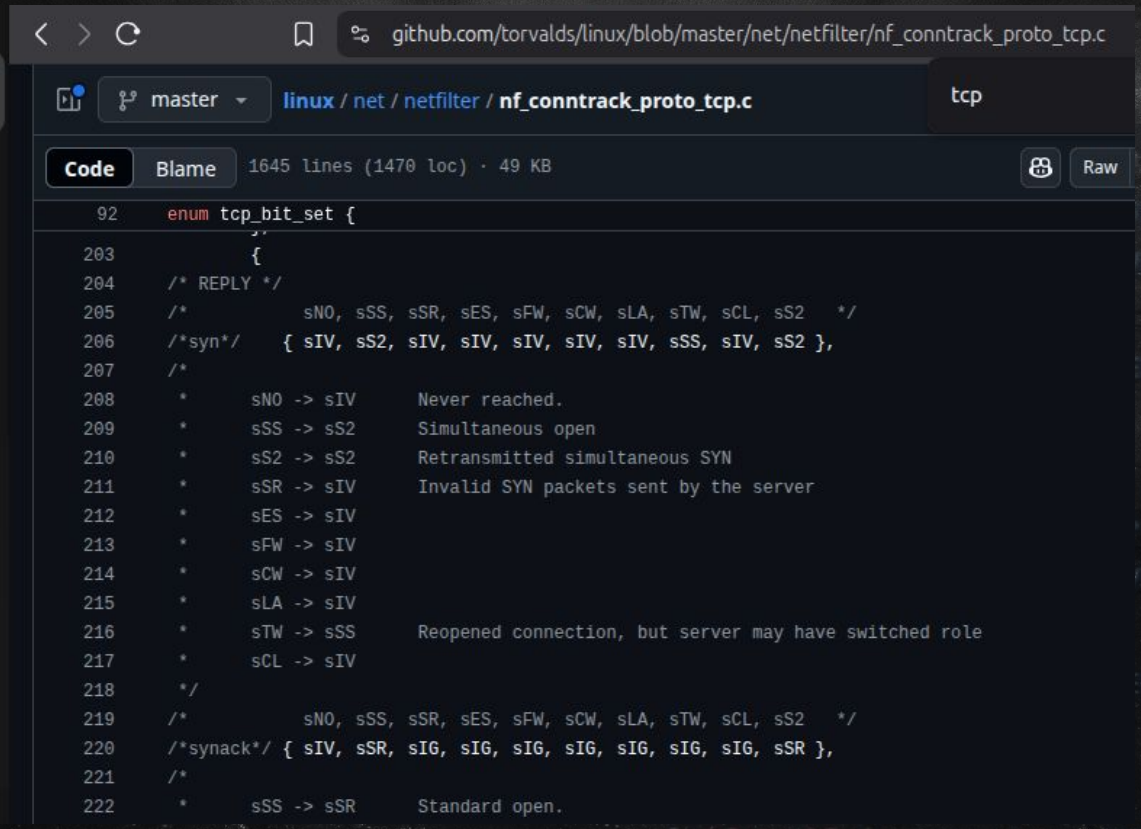
Code · Blame · 1460 lines (1252 loc) · 48.9 KB · Raw

```
278  */
279 int FlowGetPacketDirection(const Flow *f, const Packet *p)
280 {
281     const int reverse = (f->flags & FLOW_DIR_REVERSED) != 0;
282
283     if (p->proto == IPPROTO_TCP || p->proto == IPPROTO_UDP || p->proto == IPPROTO_SCTP) {
284         if (!(CMP_PORT(p->sp,p->dp))) {
285             /* update flags and counters */
286             if (CMP_PORT(f->sp,p->sp)) {
287                 return TOSERVER ^ reverse;
288             } else {
289                 return TOCLIENT ^ reverse;
290             }
291         } else {
292             if (CMP_ADDR(&f->src,&p->src)) {
293                 return TOSERVER ^ reverse;
294             } else {
295                 return TOCLIENT ^ reverse;
296             }
297         }
298     } else if (p->proto == IPPROTO_ICMP || p->proto == IPPROTO_ICMPV6) {
299         if (CMP_ADDR(&f->src,&p->src)) {
300             return TOSERVER  ^ reverse;
301         } else {
302             return TOCLIENT ^ reverse;
303         }
304     }
305
306     /* default to toserver */
307     return TOSERVER;
308 }
309
```

Connection Tracking: Suricata



Connection Tracking: Netfilter in Linux



Connection Tracking: Netfilter in Linux

Reply

Simultaneous Open

```
/* REPLY */
/*            sNO, sSS, sSR, sES, sFW, sCW, sLA, sTW, sC
/*syn*/    { sIV, sS2, sIV, sIV, sIV, sIV, sIV, sSS, sI
/*
 *      sNO -> sIV      Never reached.
 *      sSS -> sS2      Simultaneous open
 *      sS2 -> sS2      Retransmitted simultaneous SYN
```

Connection Tracking: Direction

```
bool is_orig = (src_addr == conn->OrigAddr()) && (src_port == conn->OrigPort());
pkt->is_orig = is_orig;
```

```
/* REPLY */
/*                sNO, sSS, sSR, sES, sFW, sC
/*syn*/     { sIV, sS2, sIV, sIV, sIV, sI
/*
 *      sNO -> sIV      Never reached.
 *      sSS -> sS2      Simultaneous ope
 *      sS2 -> sS2      Retransmitted si
```

```
        /* update flags and counters */
        if (CMP_PORT(f->sp,p->sp)) {
            return TOSERVER ^ reverse;
        } else {
            return TOCLIENT ^ reverse;
        }
    } else {
        if (CMP_ADDR(&f->src,&p->src)) {
            return TOSERVER ^ reverse;
        } else {
            return TOCLIENT ^ reverse;
        }
    }
```

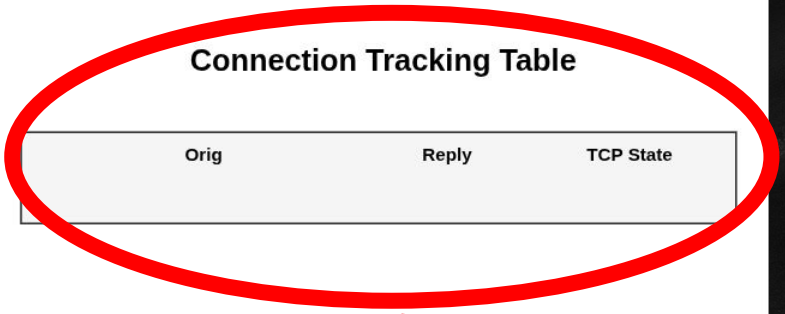


Web Server

TSPU







Connection State Table
(for TSPU)



TSPU



Web Server



“Client”

Conne cking Table

Orig	Reply	TCP State



Web Server



TSPU



“Server”

Connection Tracking Table

Orig	Reply	TCP State



Web Server

TSPU

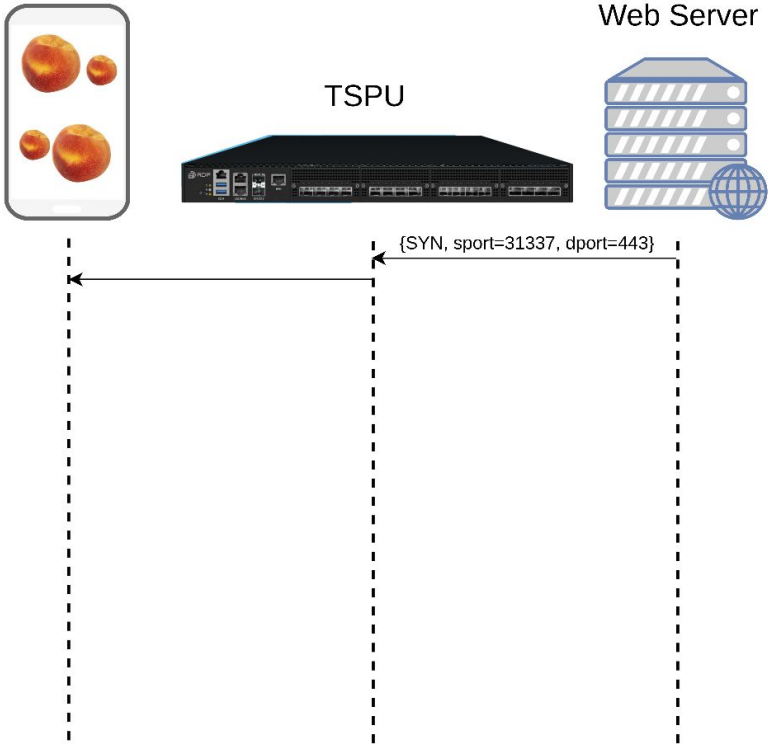




TCP State

Connection Tracking Table

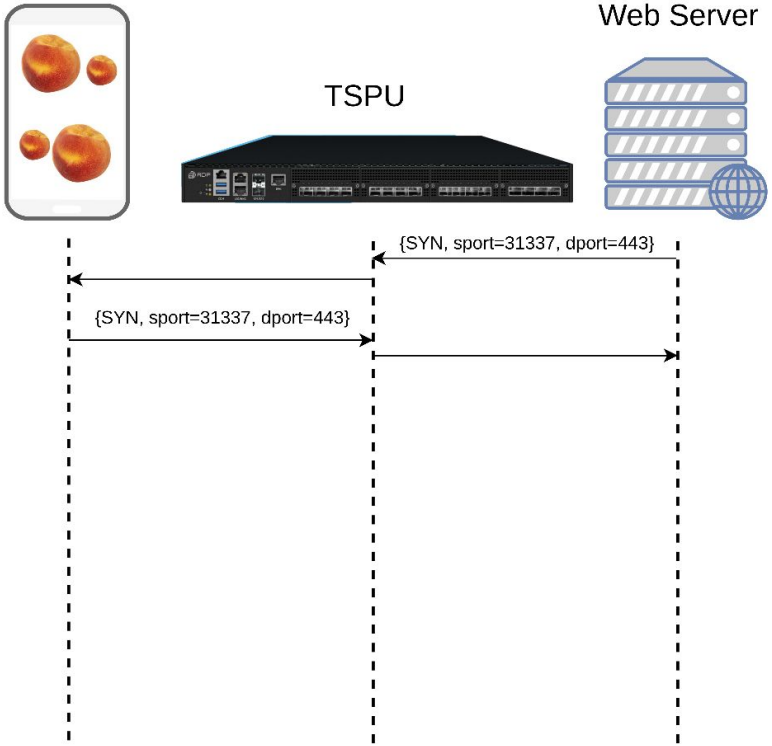
Orig	Reply	TCP State



Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337	SYN_SENT

SYN_SENT

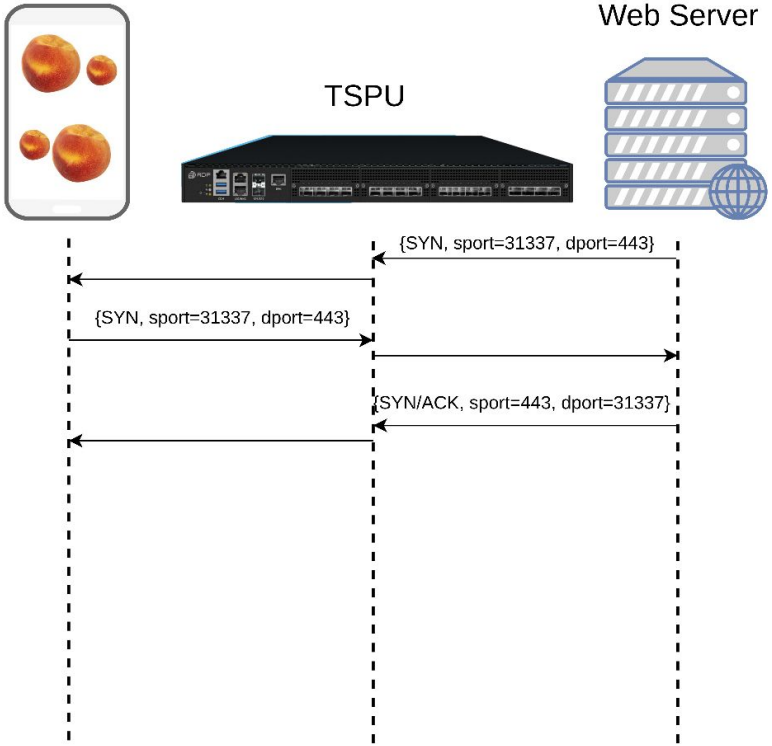


Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337	SYN SENT2

SYN_SENT2



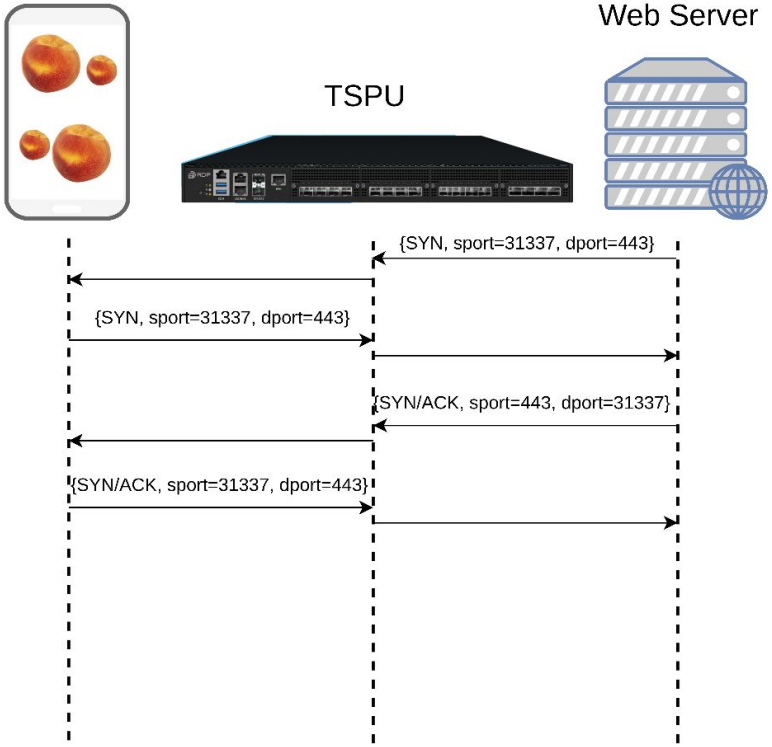
Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337	SYN_RCVD

SYN_RCVD



Connection Tracking Table

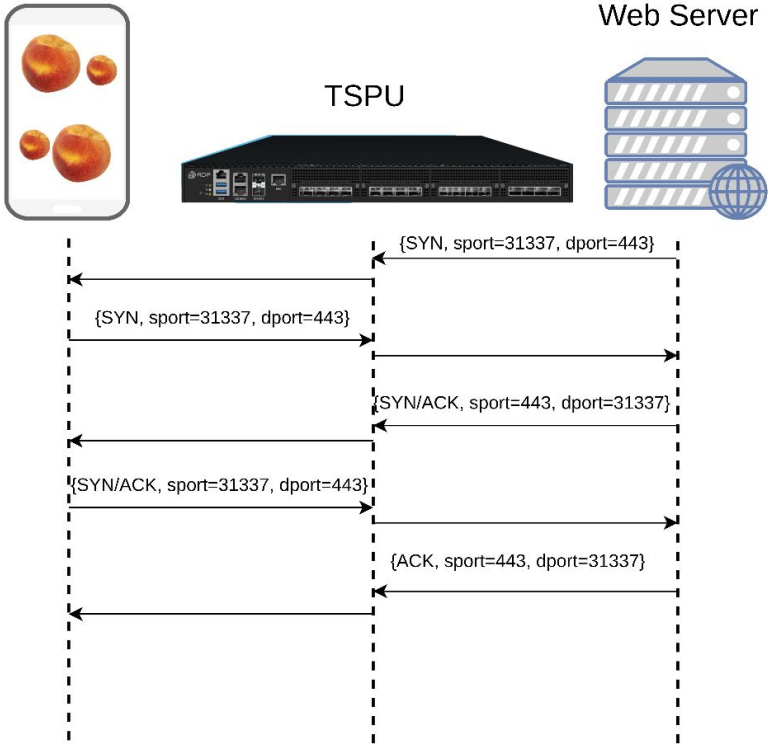
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337	SYN_RCVD

SYN_RCVD



Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

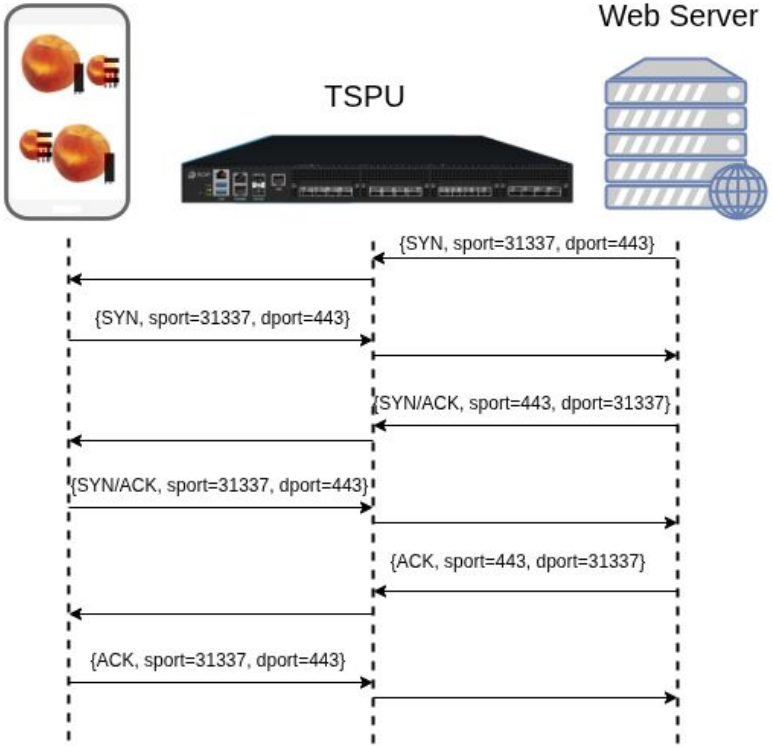
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337	ESTBALISHED

ESTABLISHED



Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	ESTBALISHED

Server-side Bypass: Simultaneous Open

Internal Client



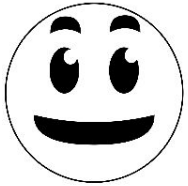
TSPU



Web server

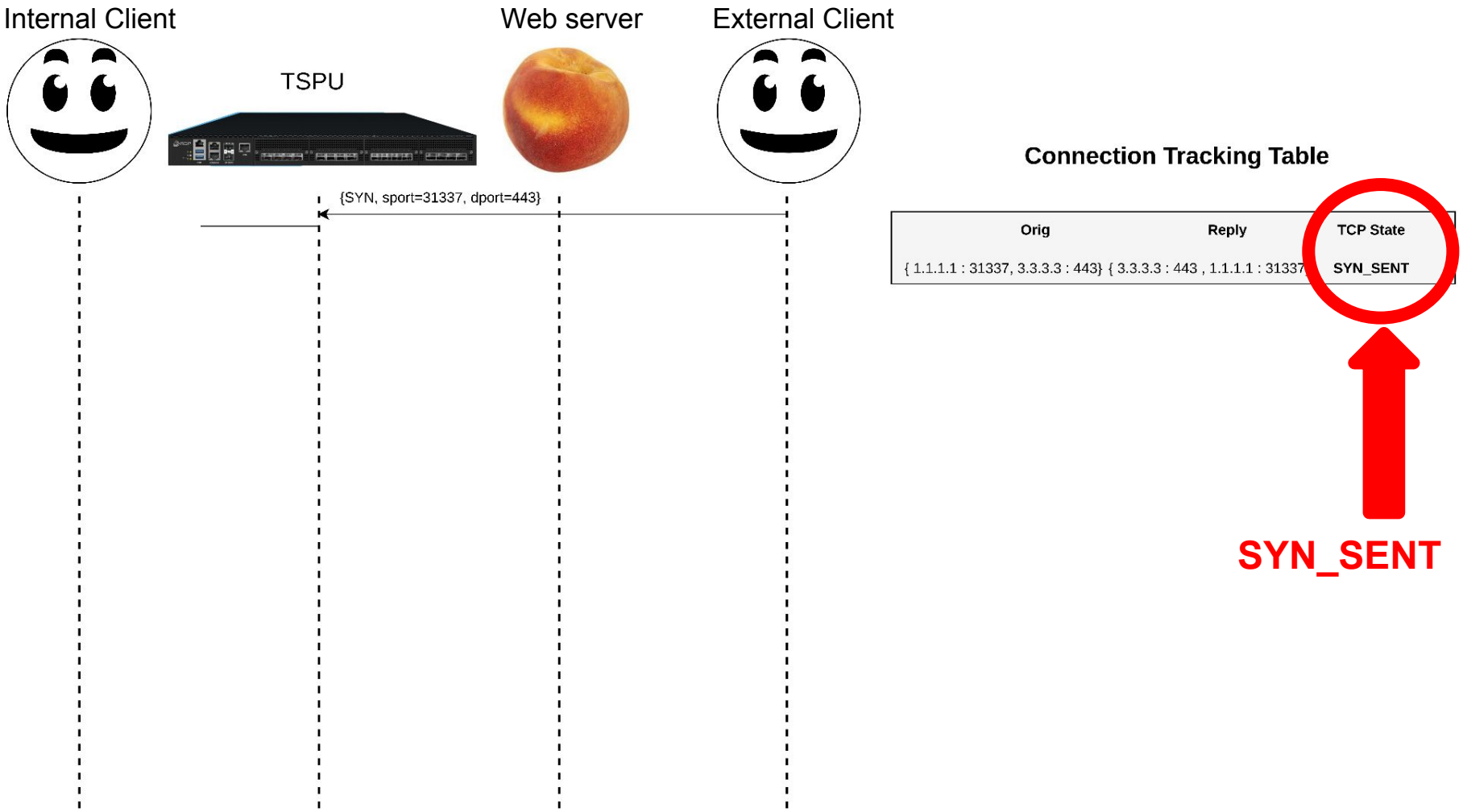


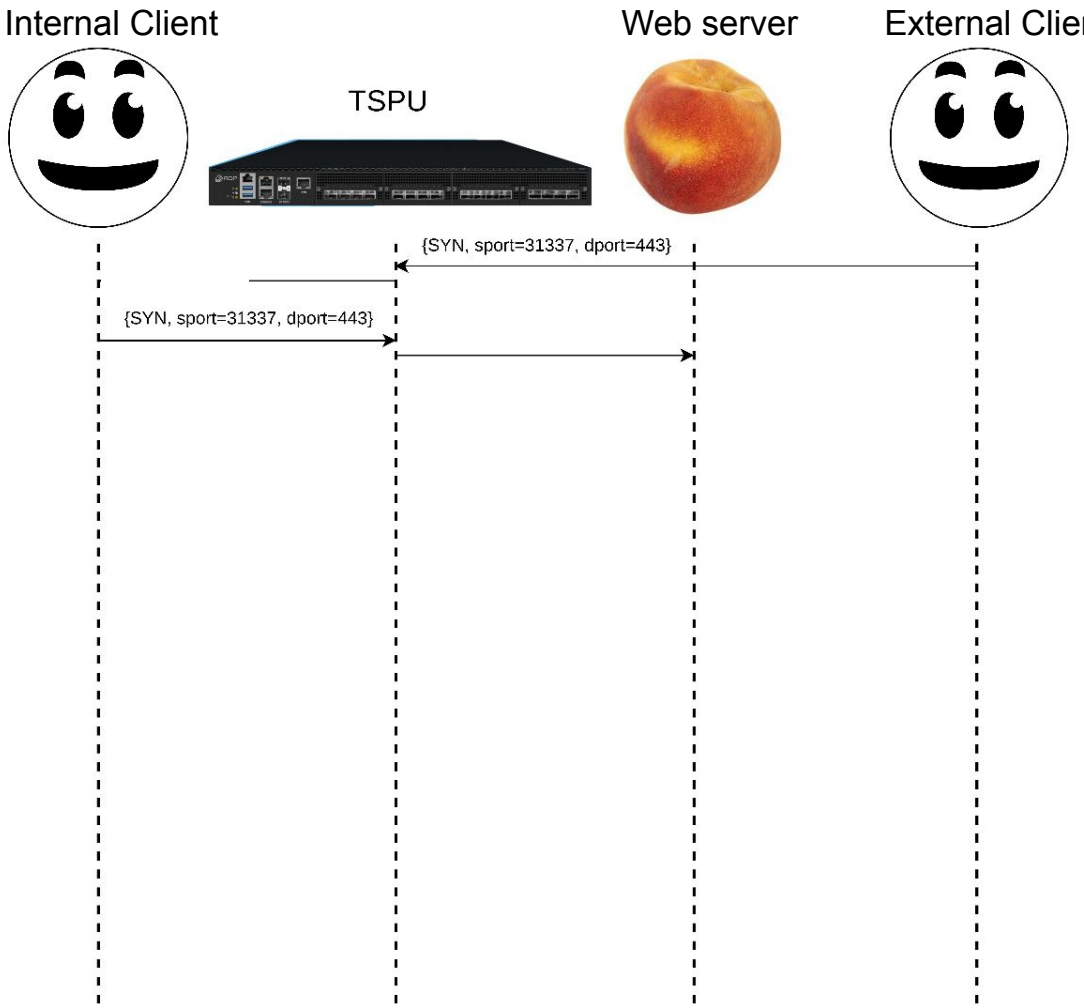
External Client



Connection Tracking Table

Orig	Reply	TCP State
		None


Internal Client
Web server
External Client
TSPU
{SYN, sport=31337, dport=443}
Connection Tracking Table
Orig
Reply
TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}
{ 3.3.3.3 : 443 , 1.1.1.1 : 31337
SYN_SENT
SYN_SENT

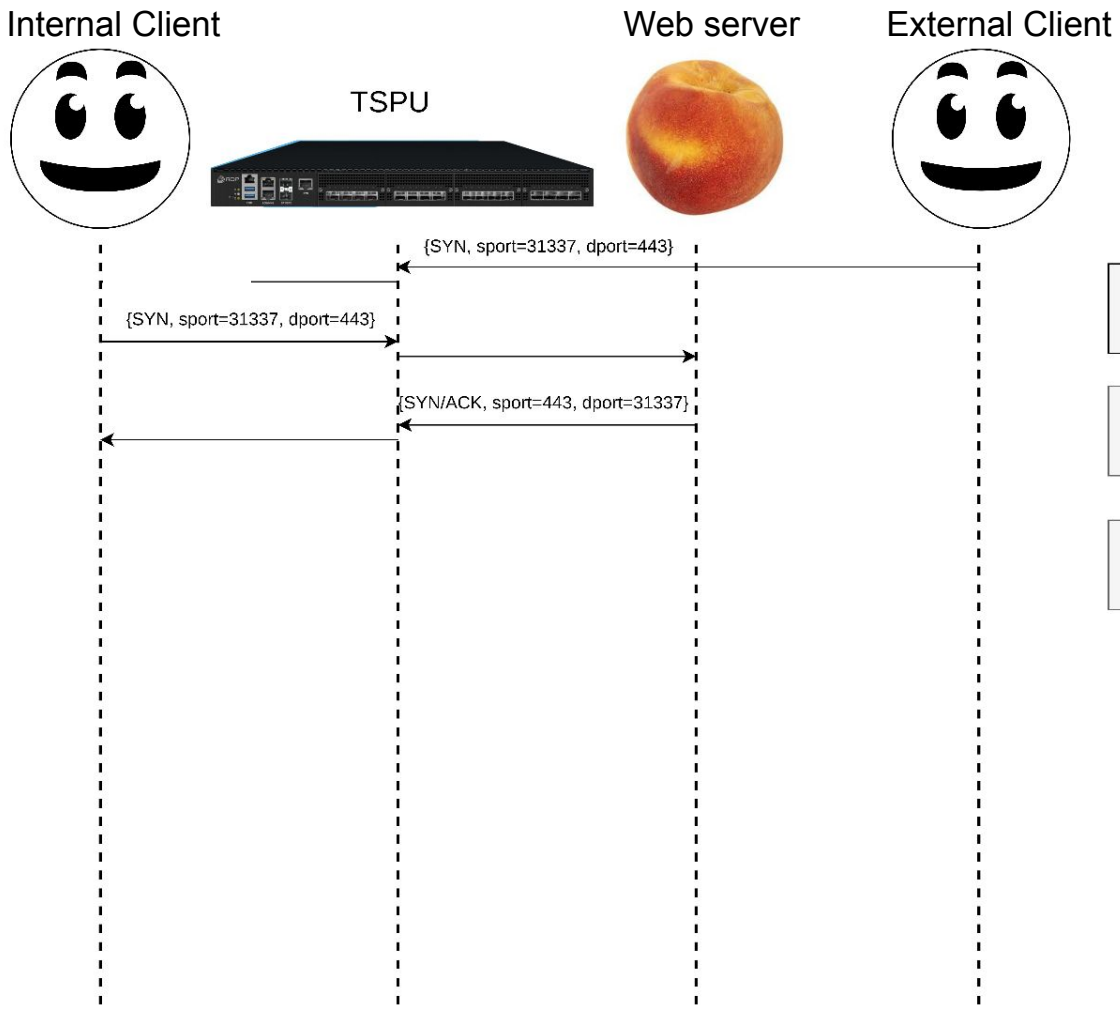


Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337	SYN_SENT2

SYN_SENT2



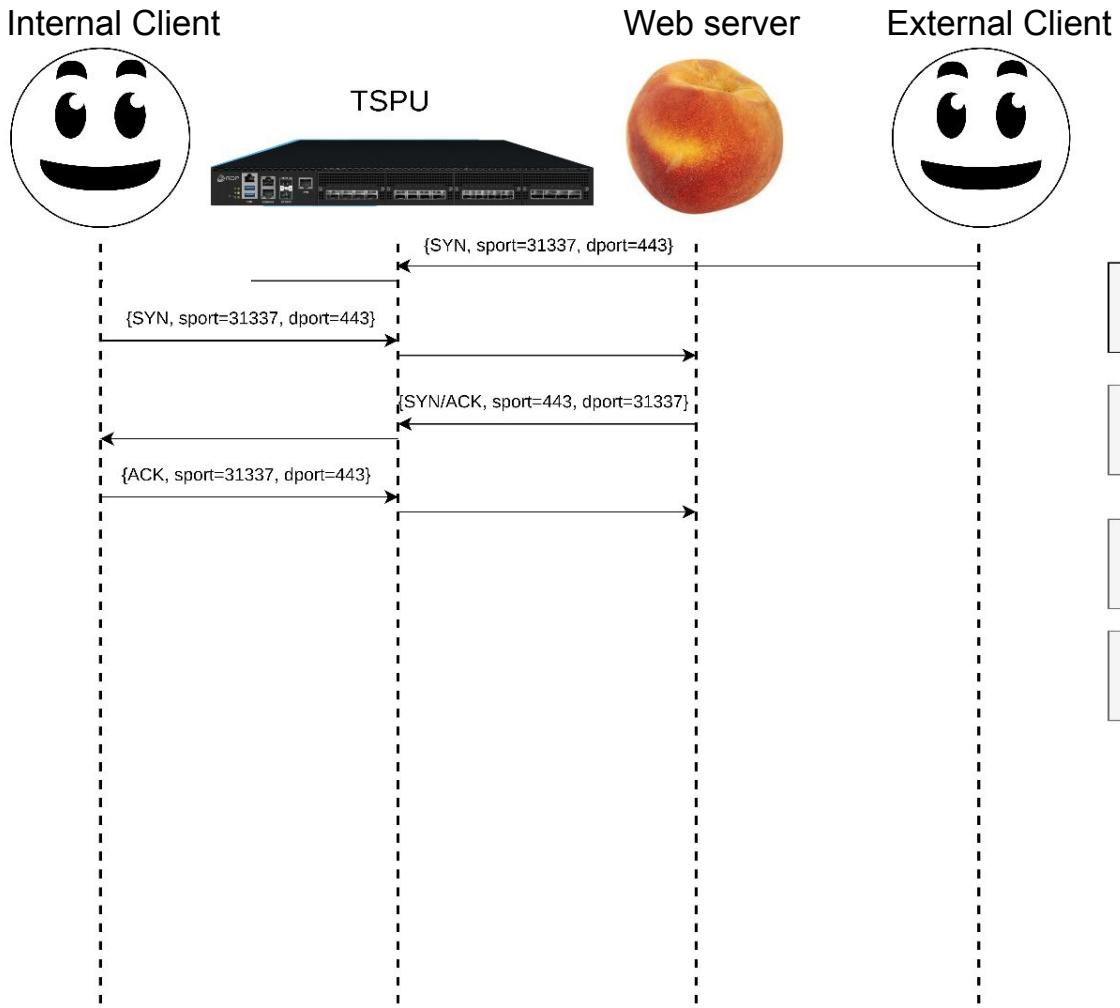
Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

SYN_RCVD



Connection Tracking Table

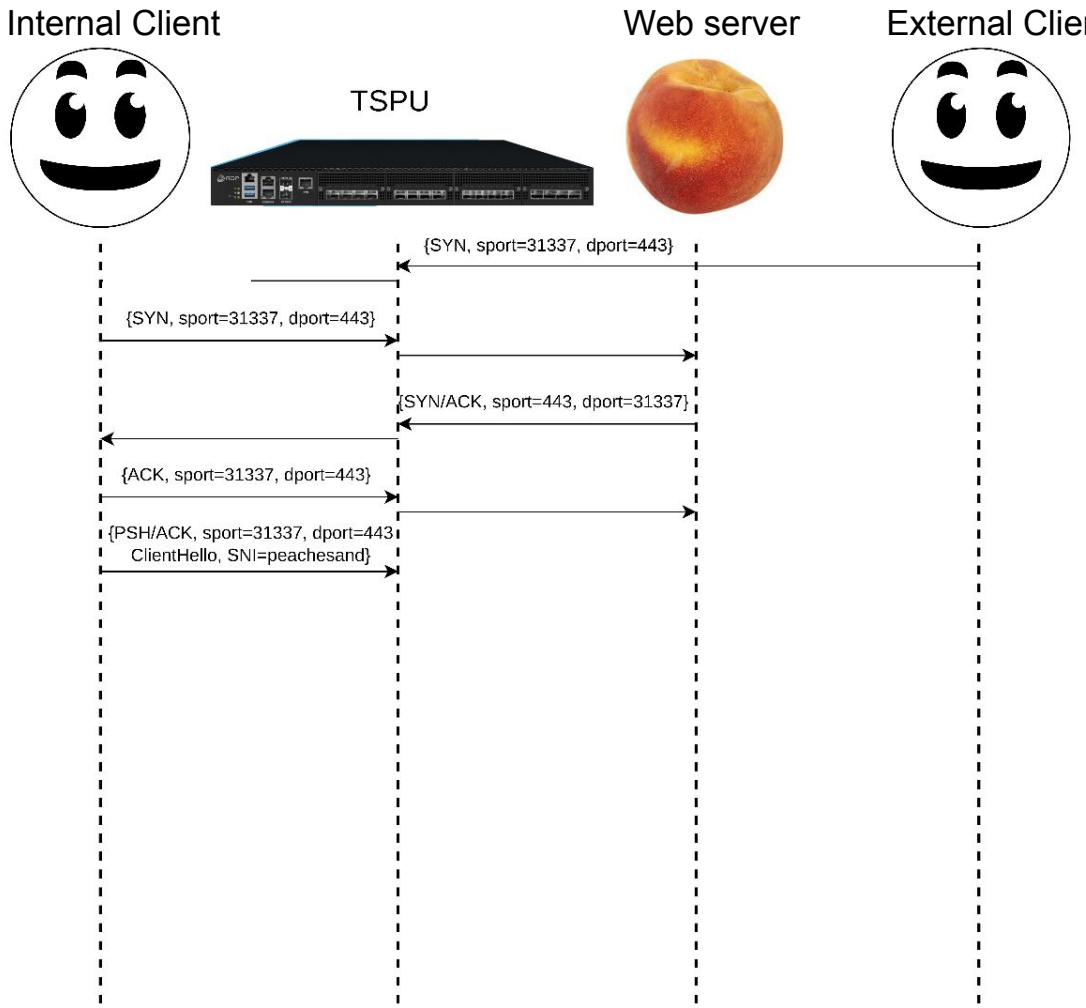
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337	SYN_RCVD

SYN_RCVD



Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

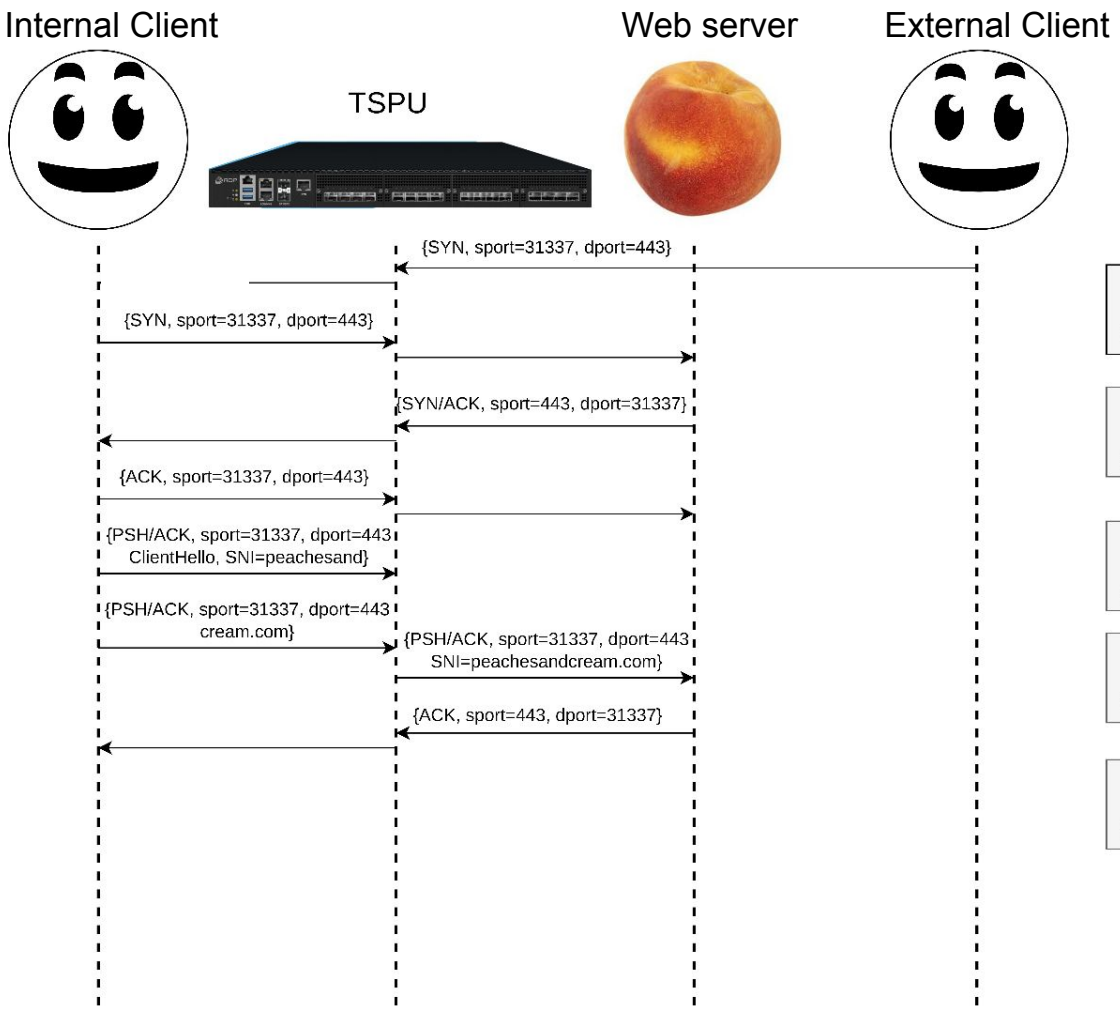
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337	ESTBALISHED

ESTABLISHED



Connection Tracking Table

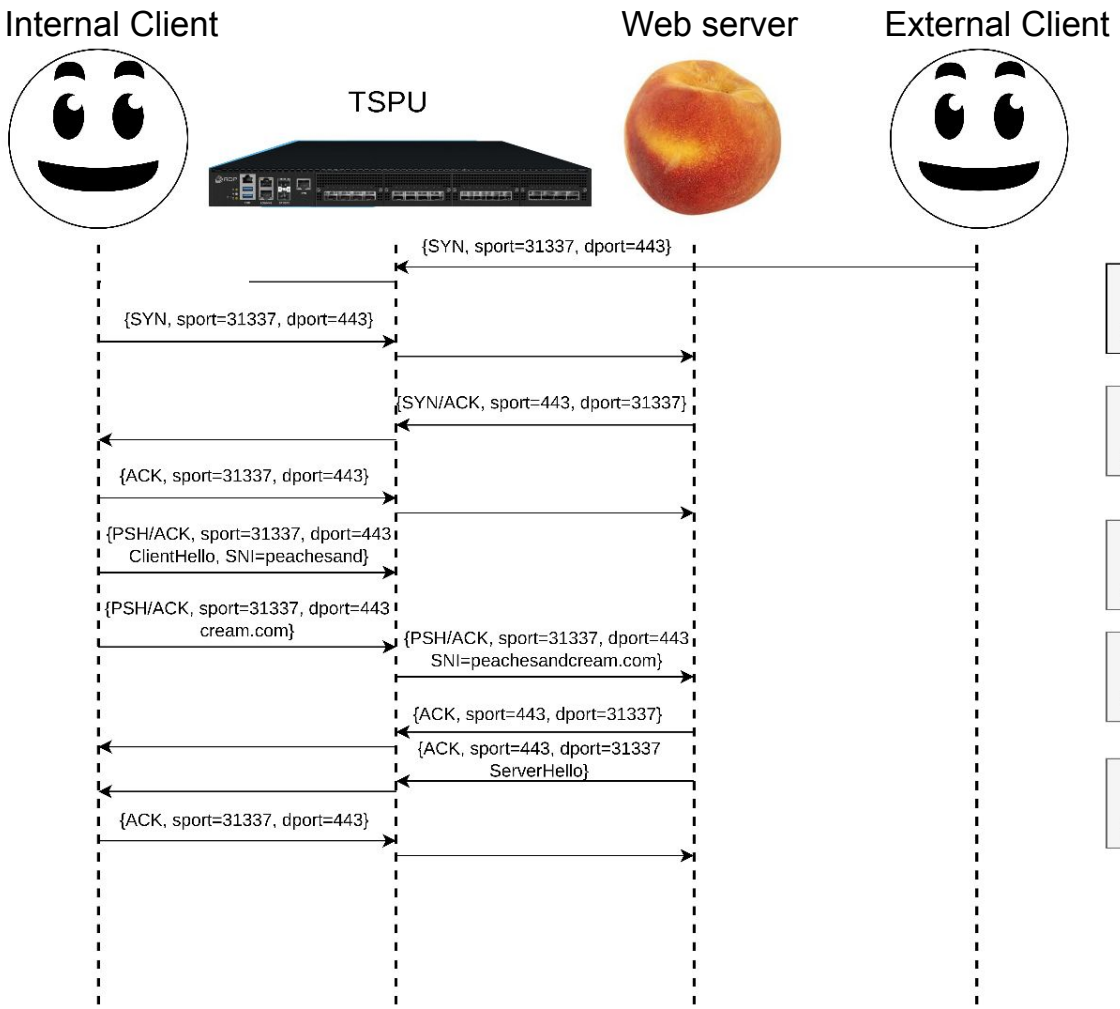
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	**SYN_SENT**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_SENT2**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_RCVD**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_RCVD**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**ESTBALISHED**



Connection Tracking Table

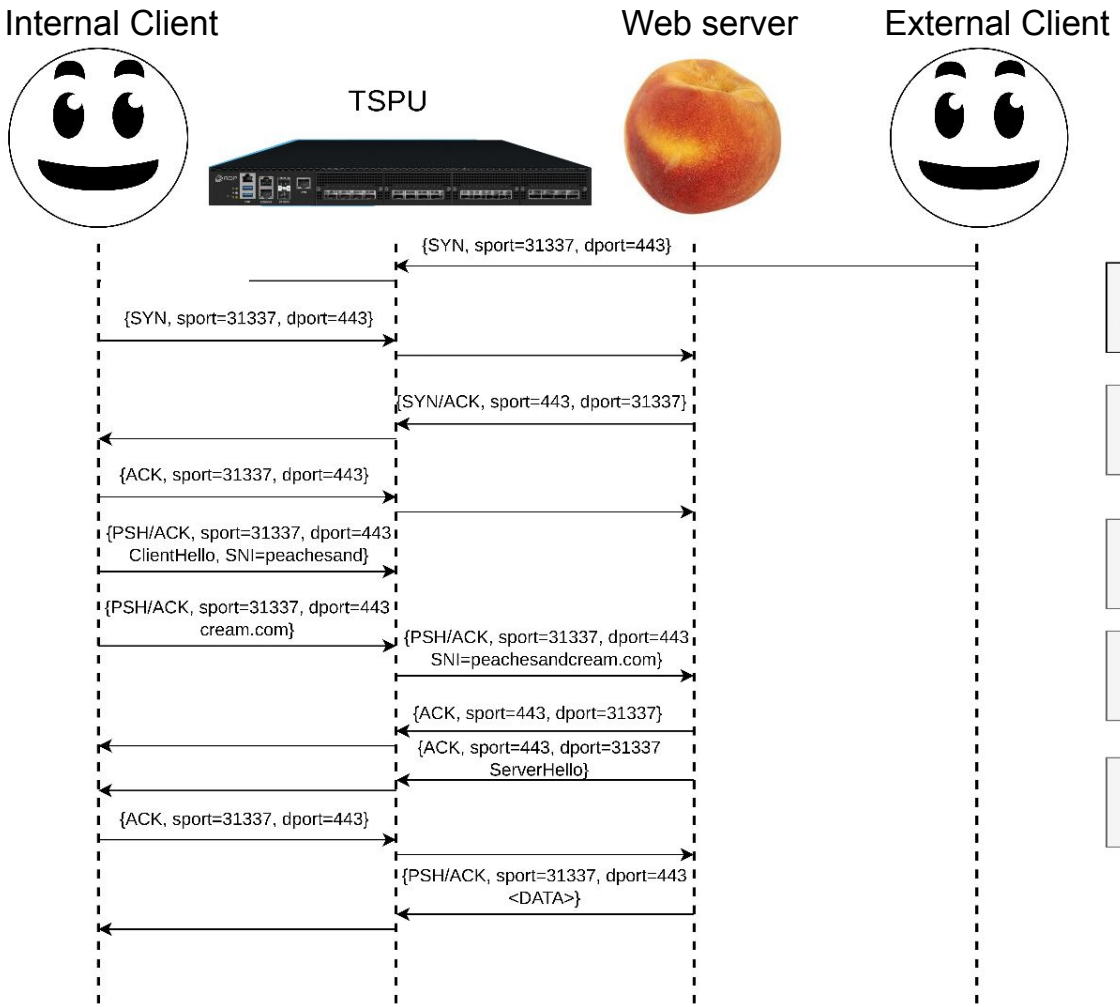
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	**SYN_SENT**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_SENT2**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_RCVD**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_RCVD**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**ESTBALISHED**



Connection Tracking Table

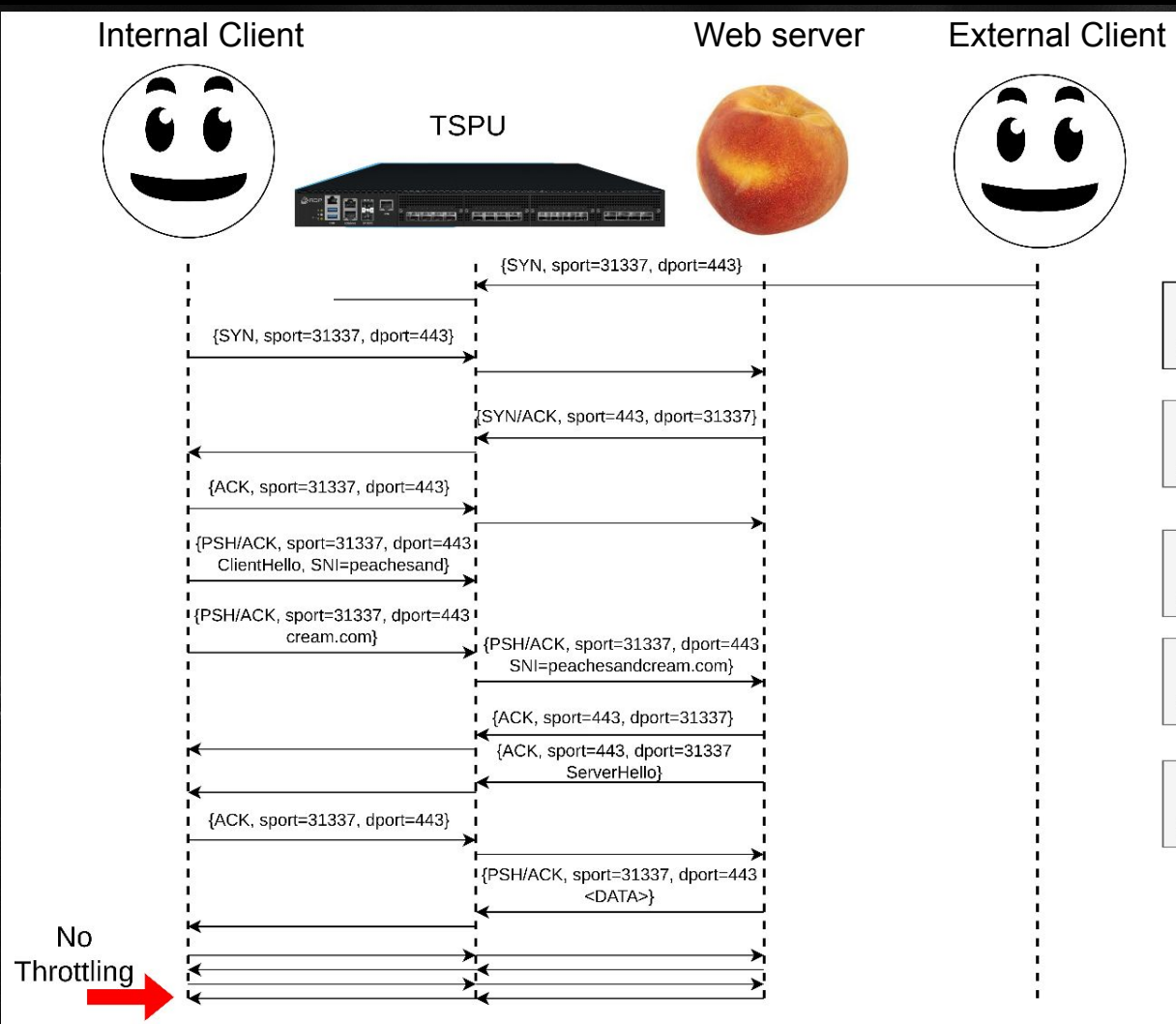
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	**SYN_SENT**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_SENT2**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_RCVD**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**SYN_RCVD**

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	**ESTBALISHED**



Connection Tracking Table

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443}	{ 3.3.3.3 : 443 , 1.1.1.1 : 31337}	SYN_SENT

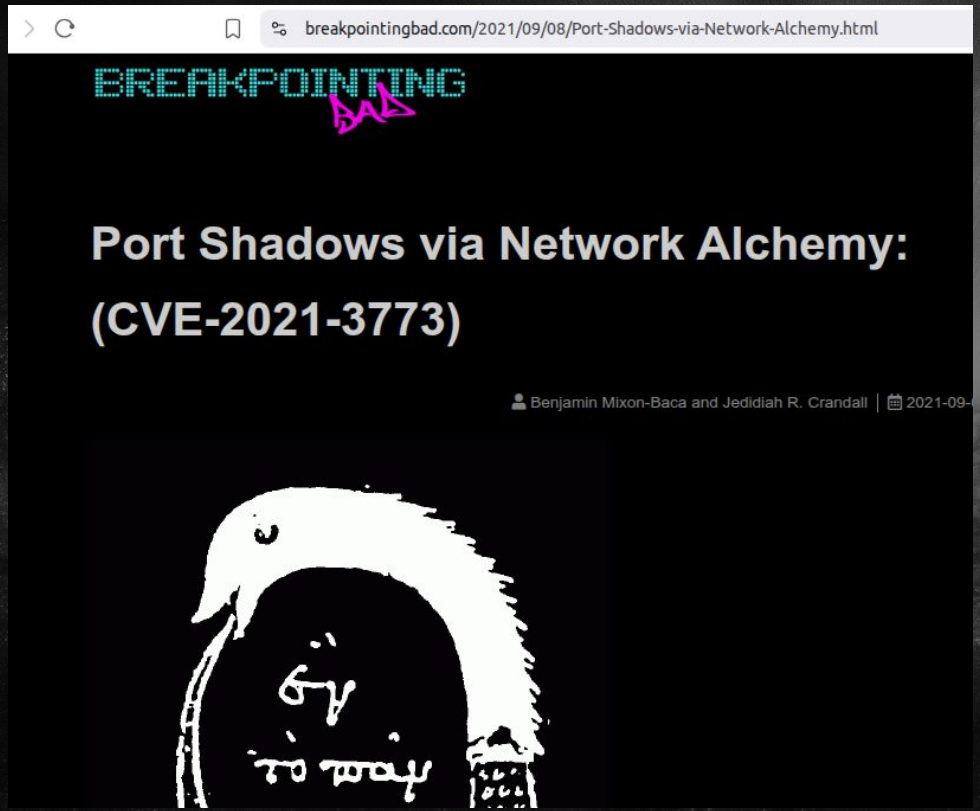
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_SENT2

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

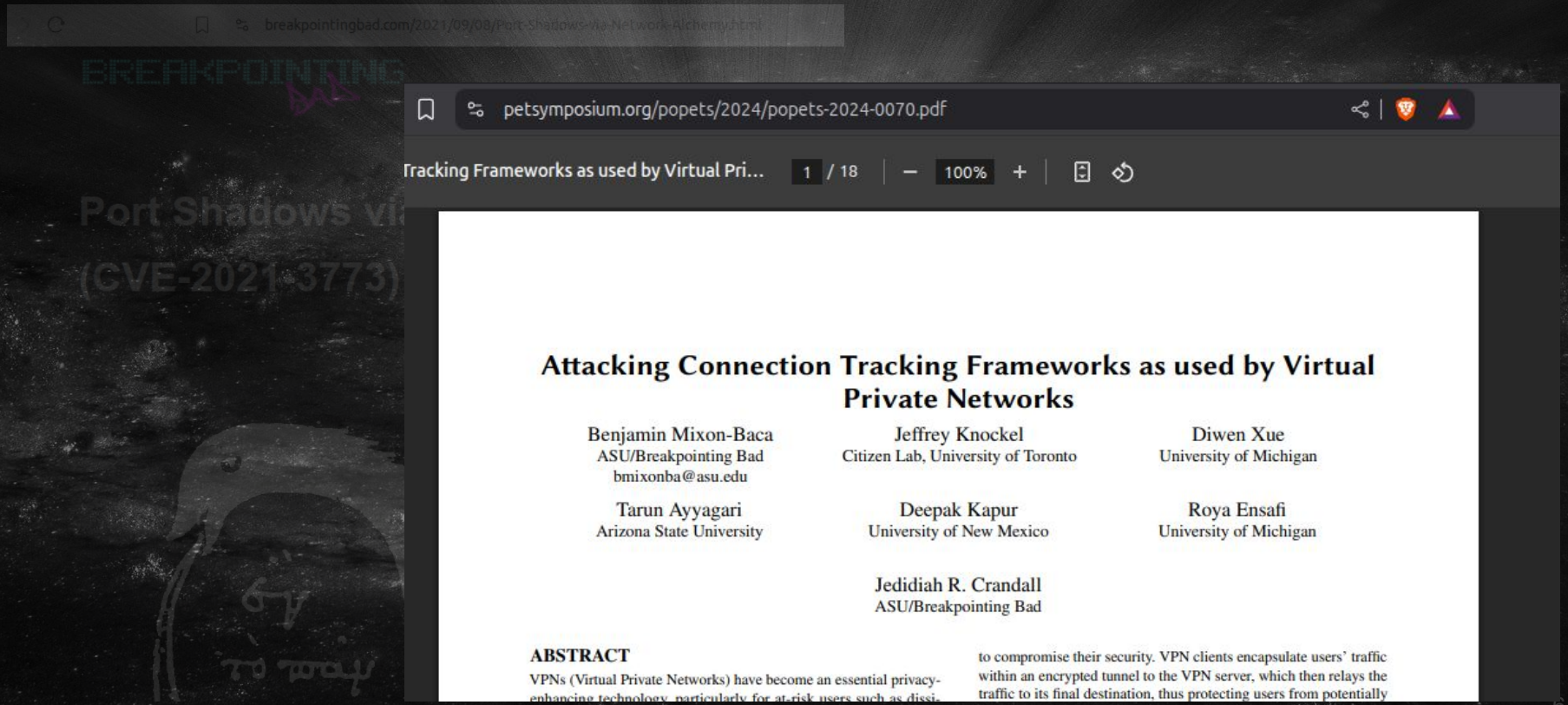
Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	SYN_RCVD

Orig	Reply	TCP State
{ 1.1.1.1 : 31337, 3.3.3.3 : 443 }	{ 3.3.3.3 : 443, 1.1.1.1 : 31337 }	ESTBALISHED

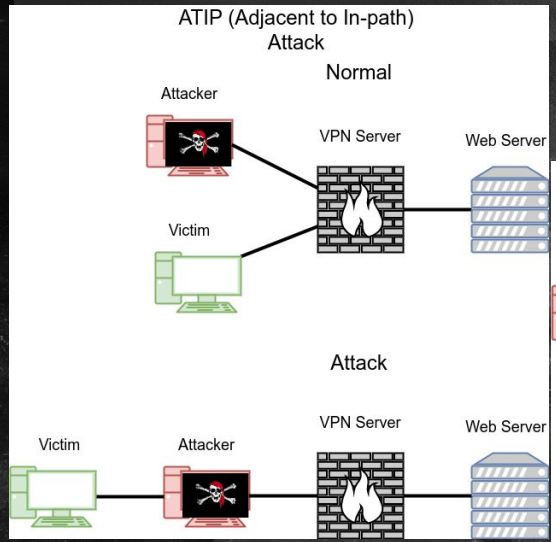
Other Implications: VPN Security

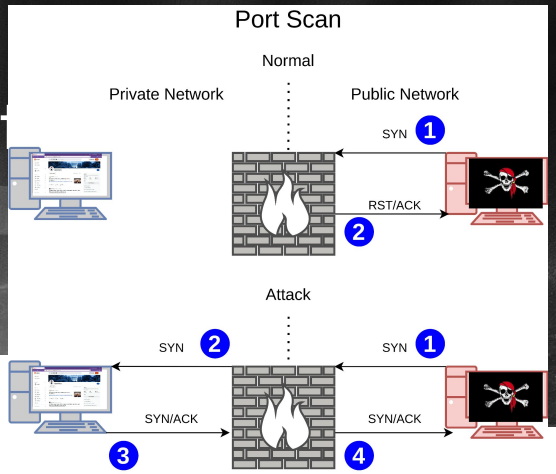


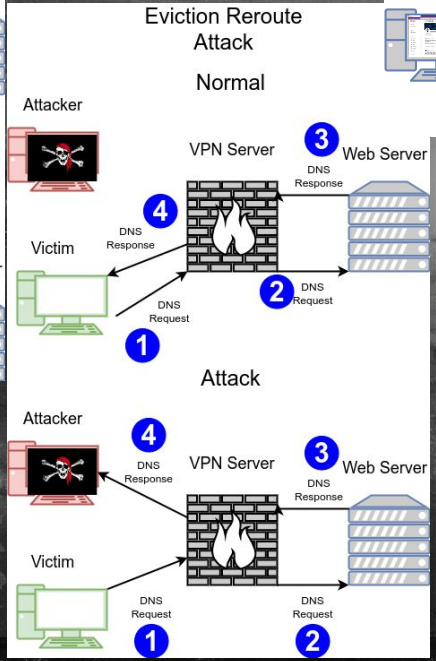
Other Implications: VPN Security

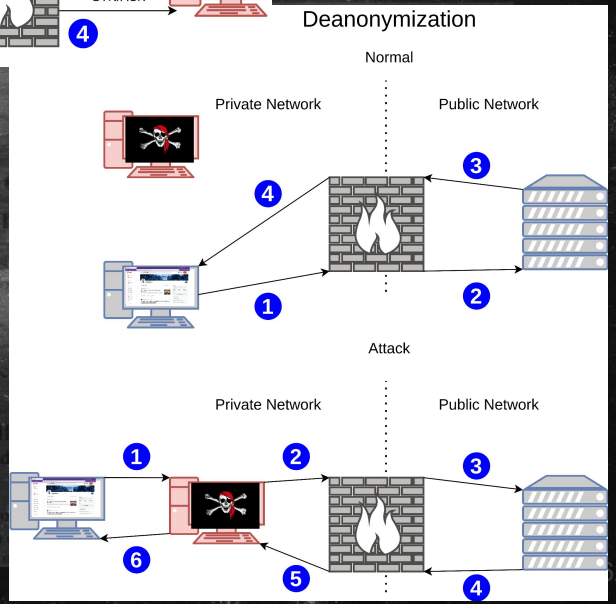


Other Implications: VPN Securit









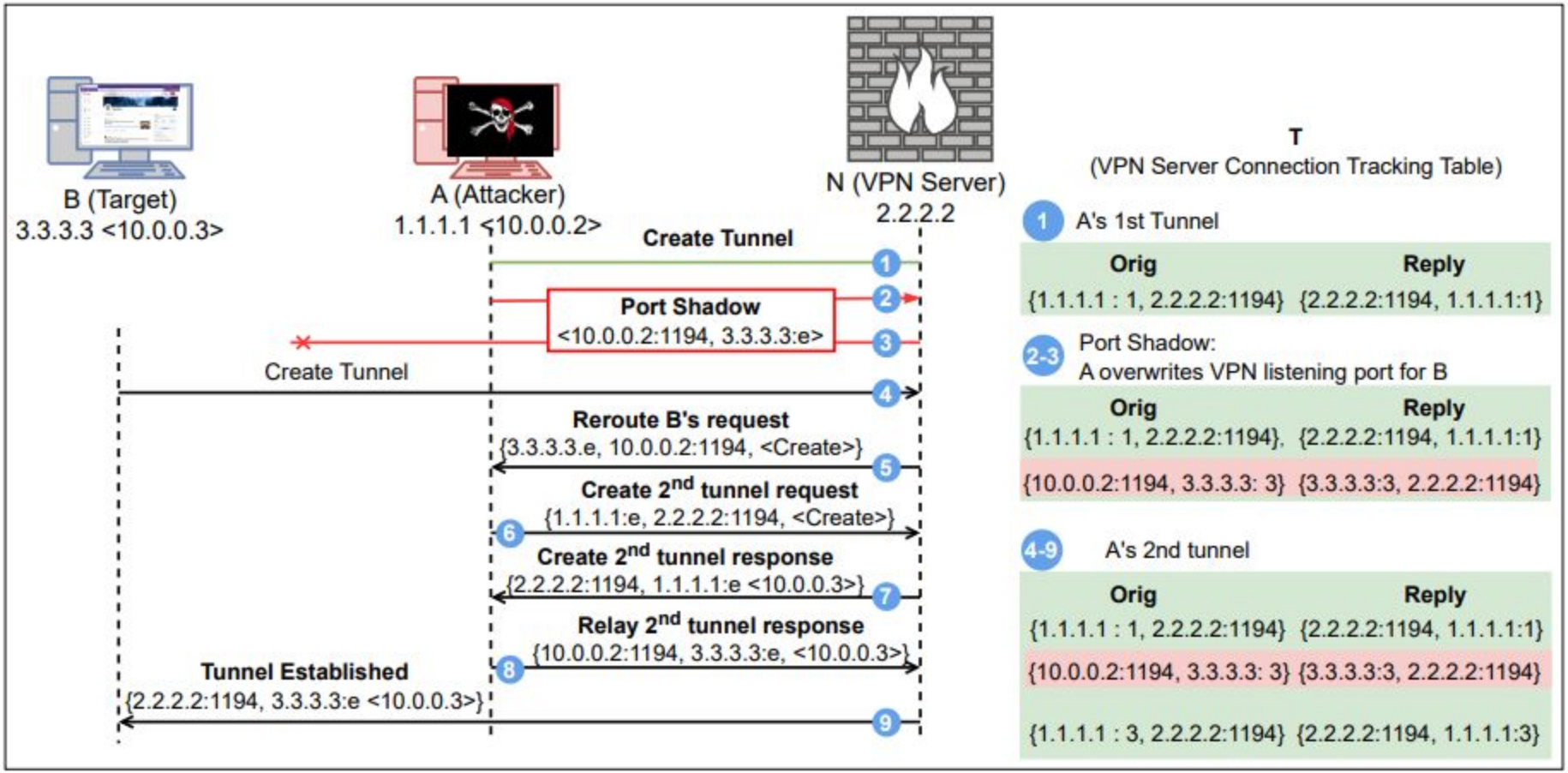


Figure 2: Adjacent-to-in-path attack.

Other Implications: VPN Security

petsymposium.org/popets/2024/popets-2024-0070.php

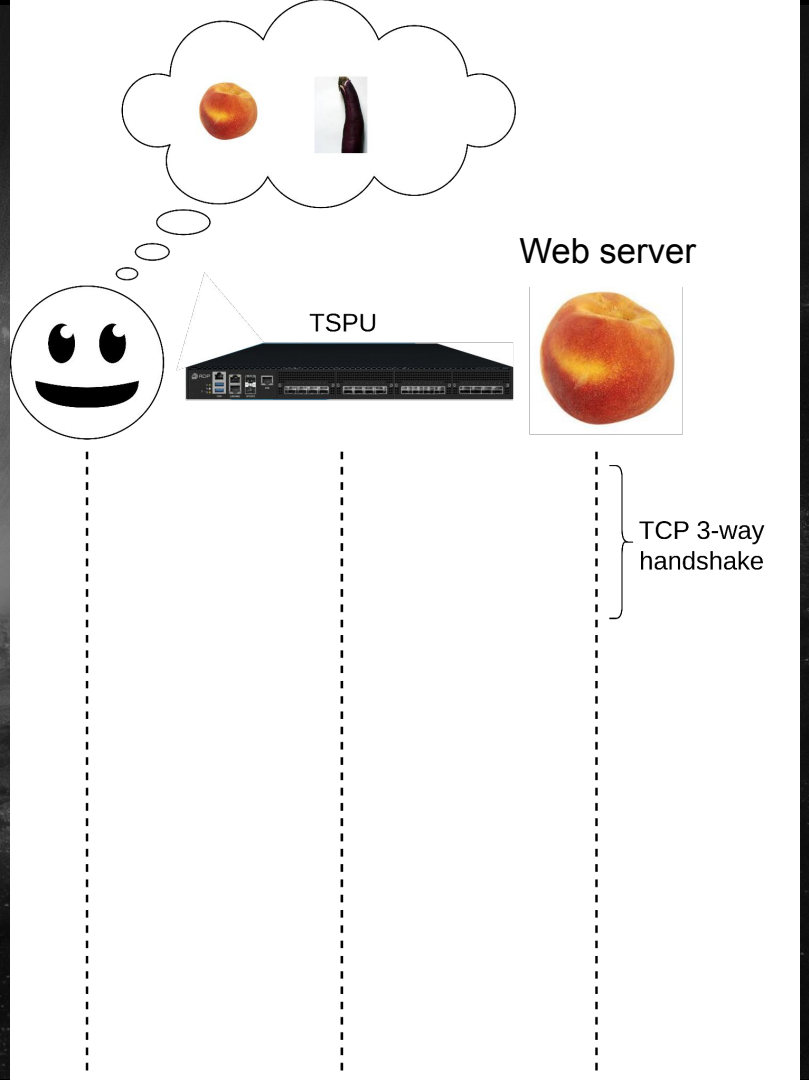
(CVE-2021-3773)

breakpointingbad.com/2021/09/08/Port-Shadows-via-Network-Alchemy.html

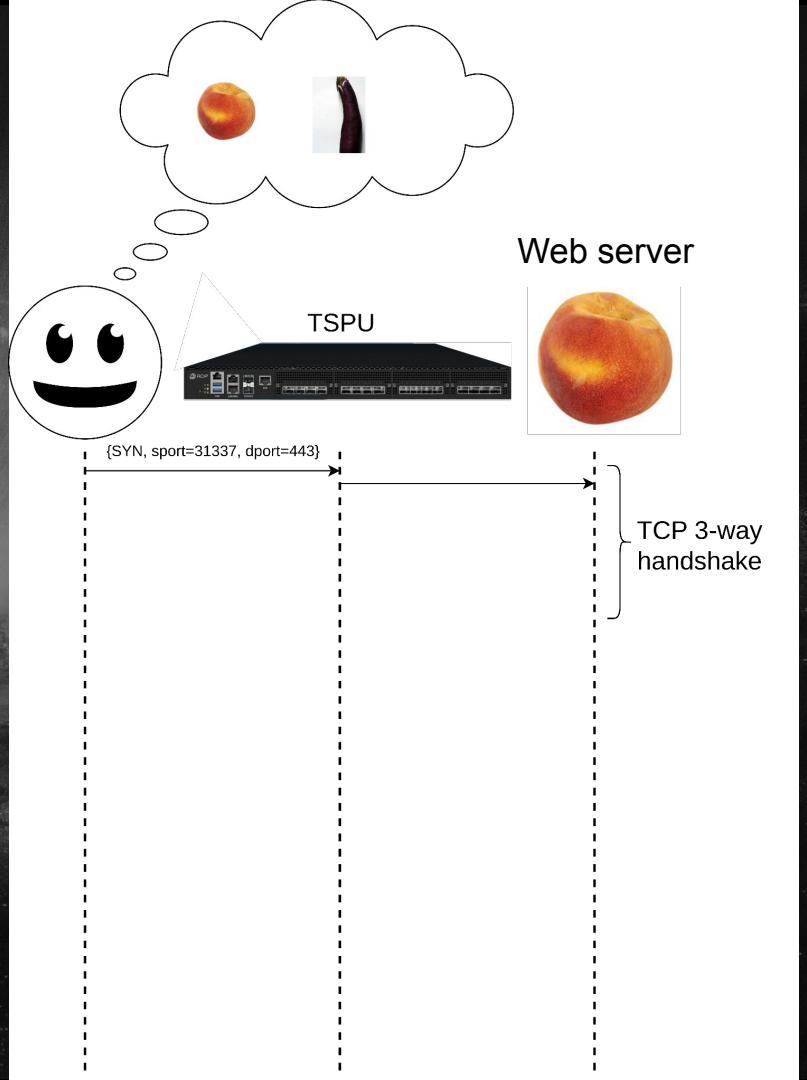
Client-side Bypass:

5 ACKS

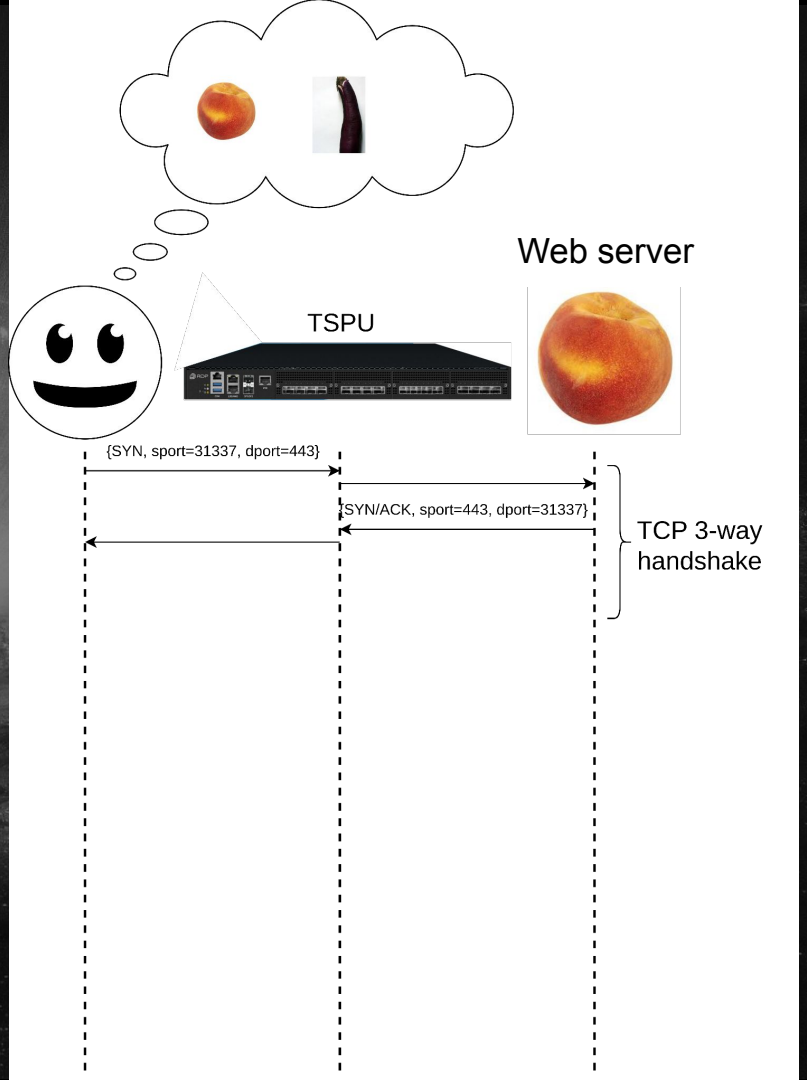
TLS- 4 way Handshake



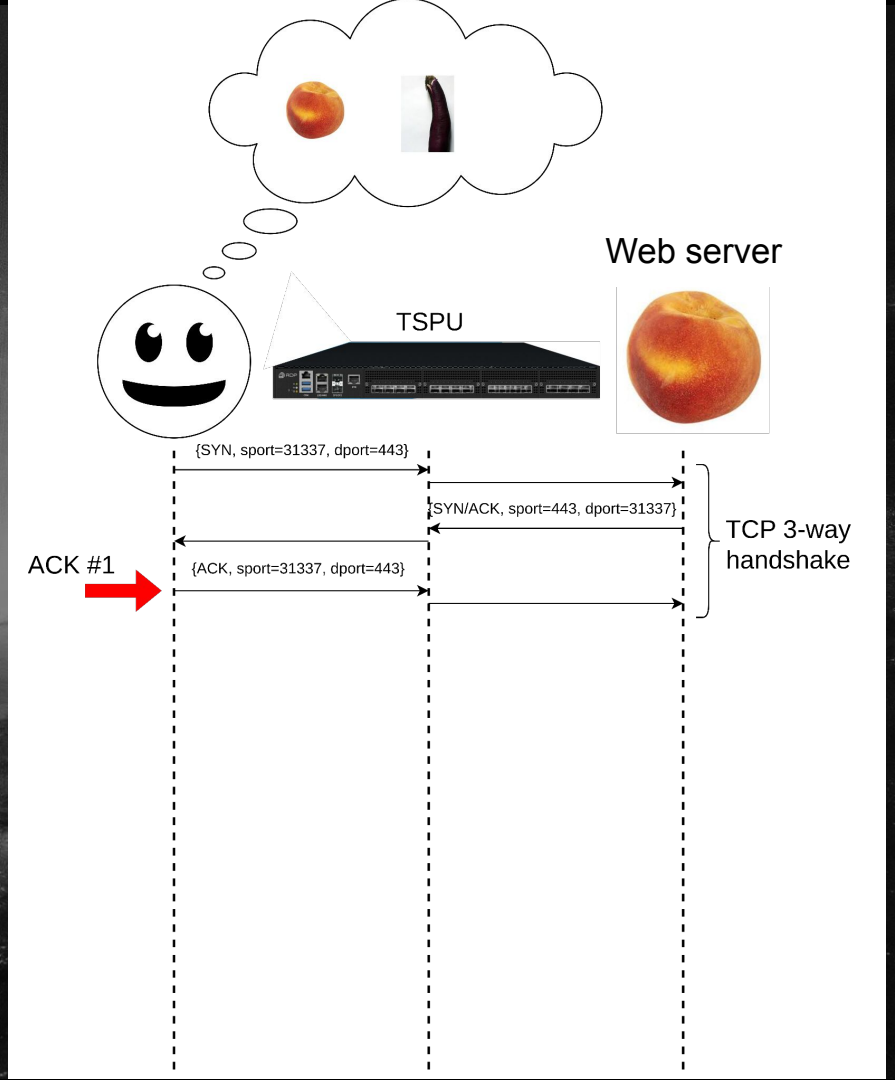
TLS- 4 way Handshake



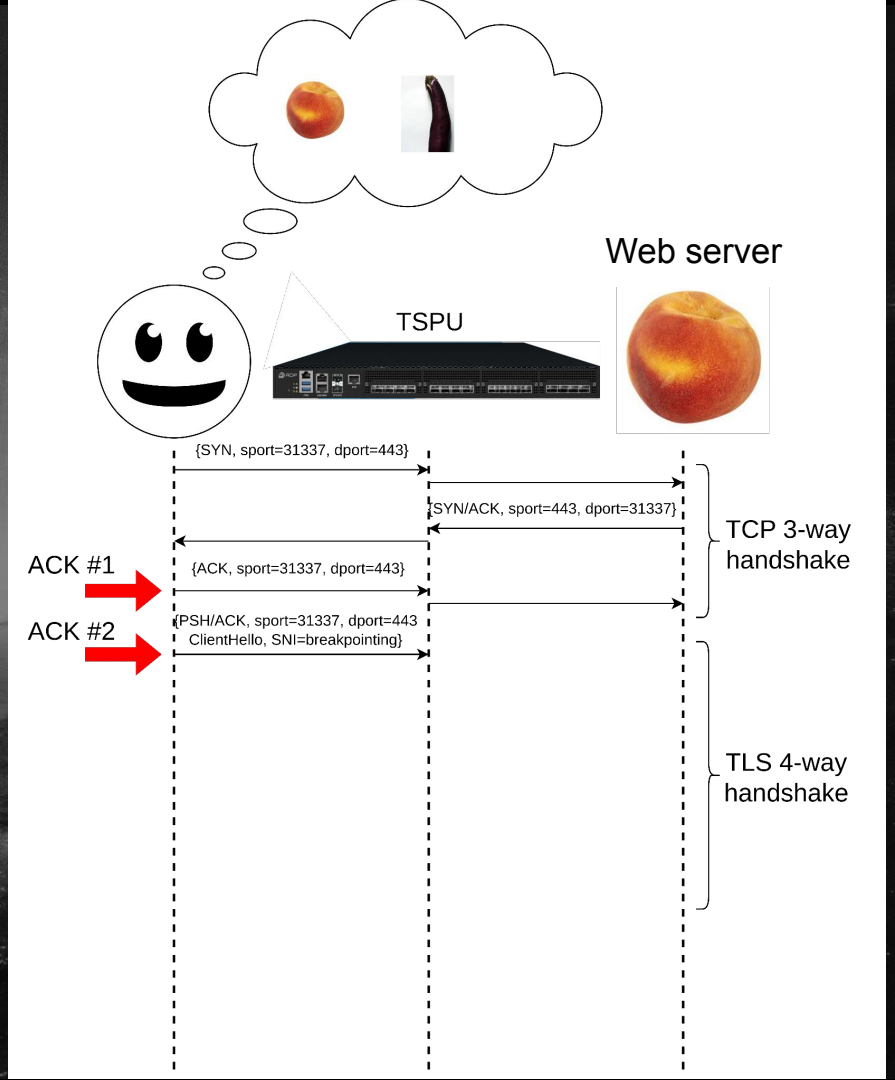
TLS- 4 way Handshake



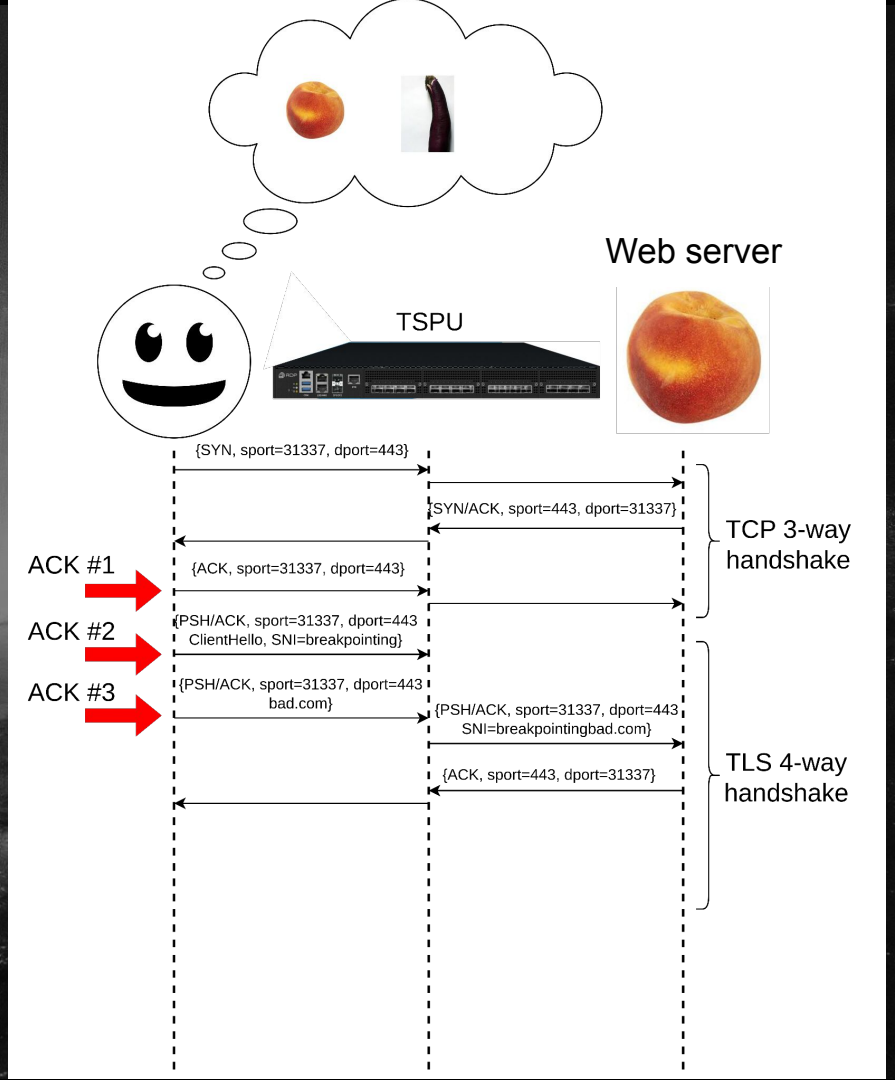
TLS- 4 way Handshake



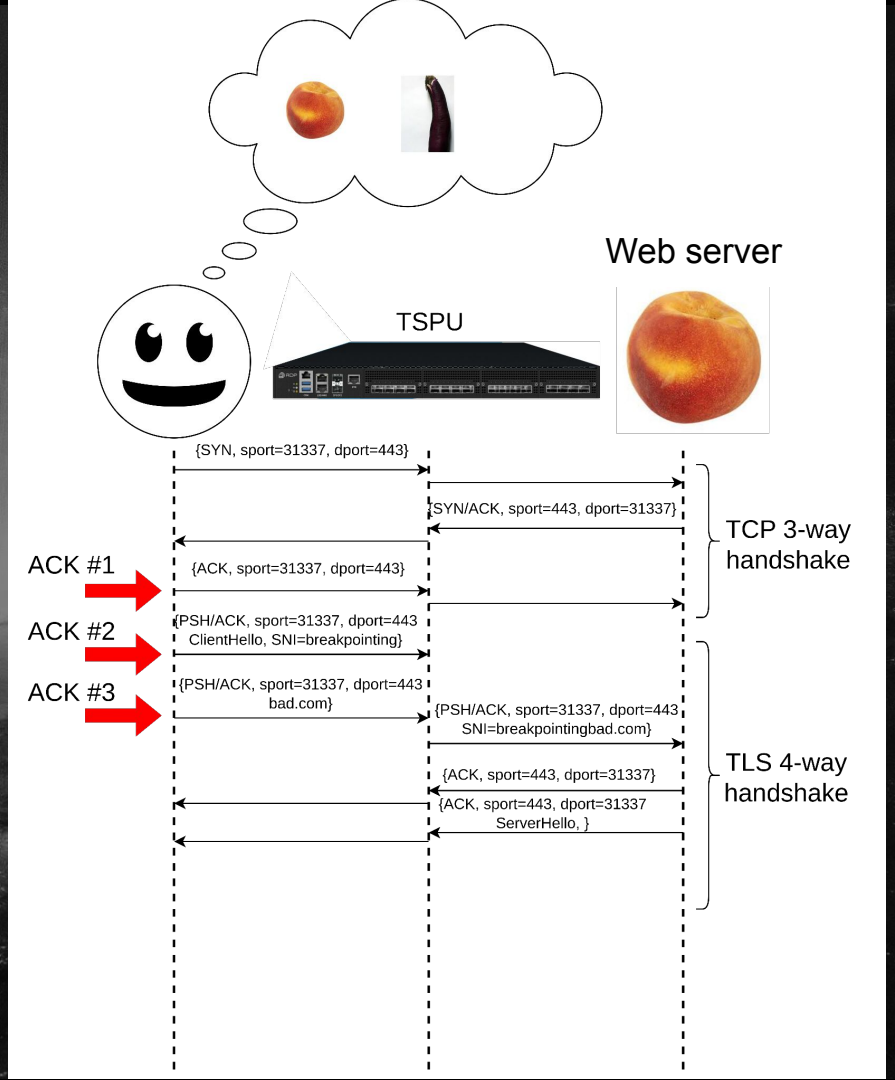
TLS- 4 way Handshake



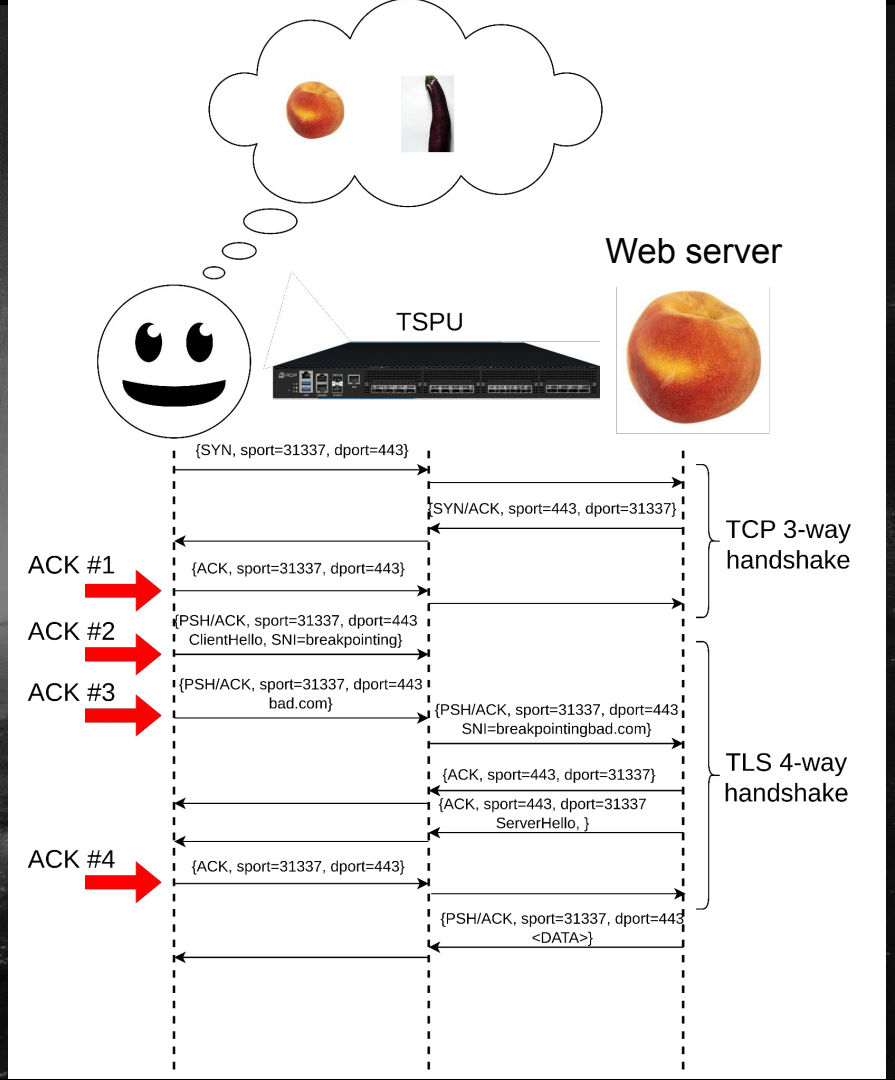
TLS- 4 way Handshake



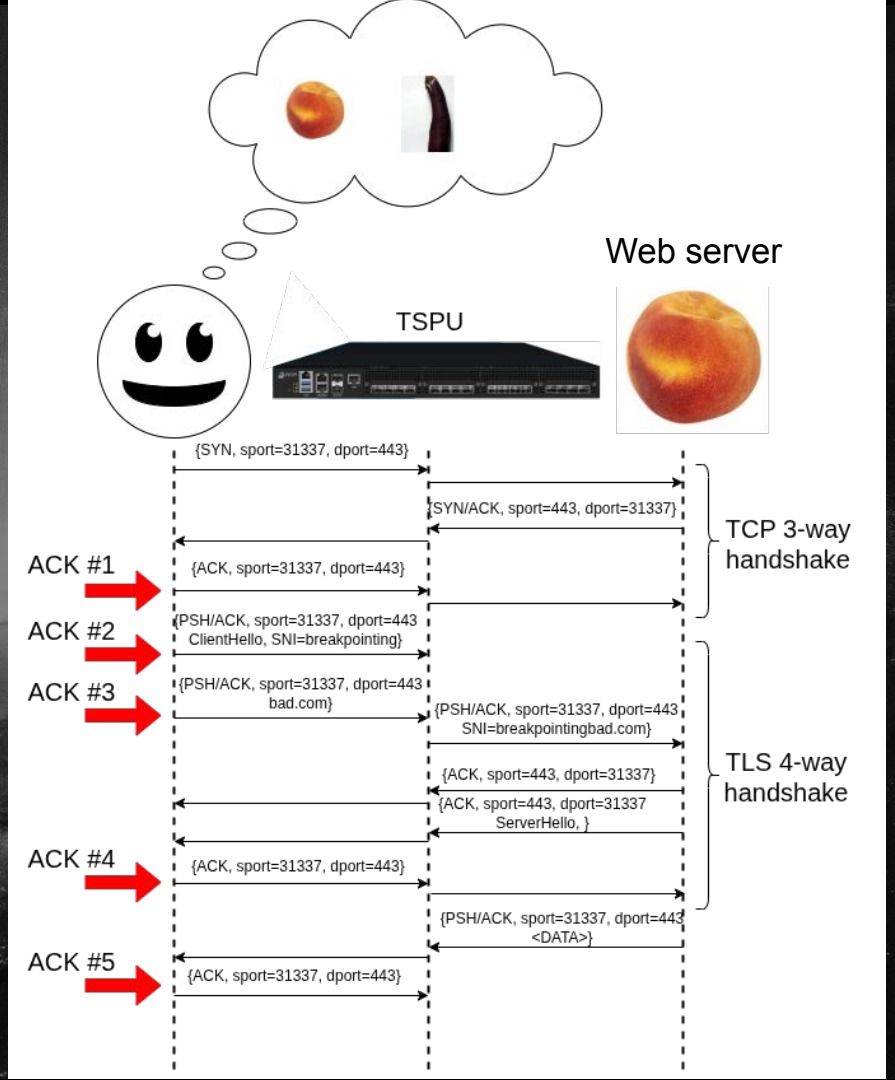
TLS- 4 way Handshake



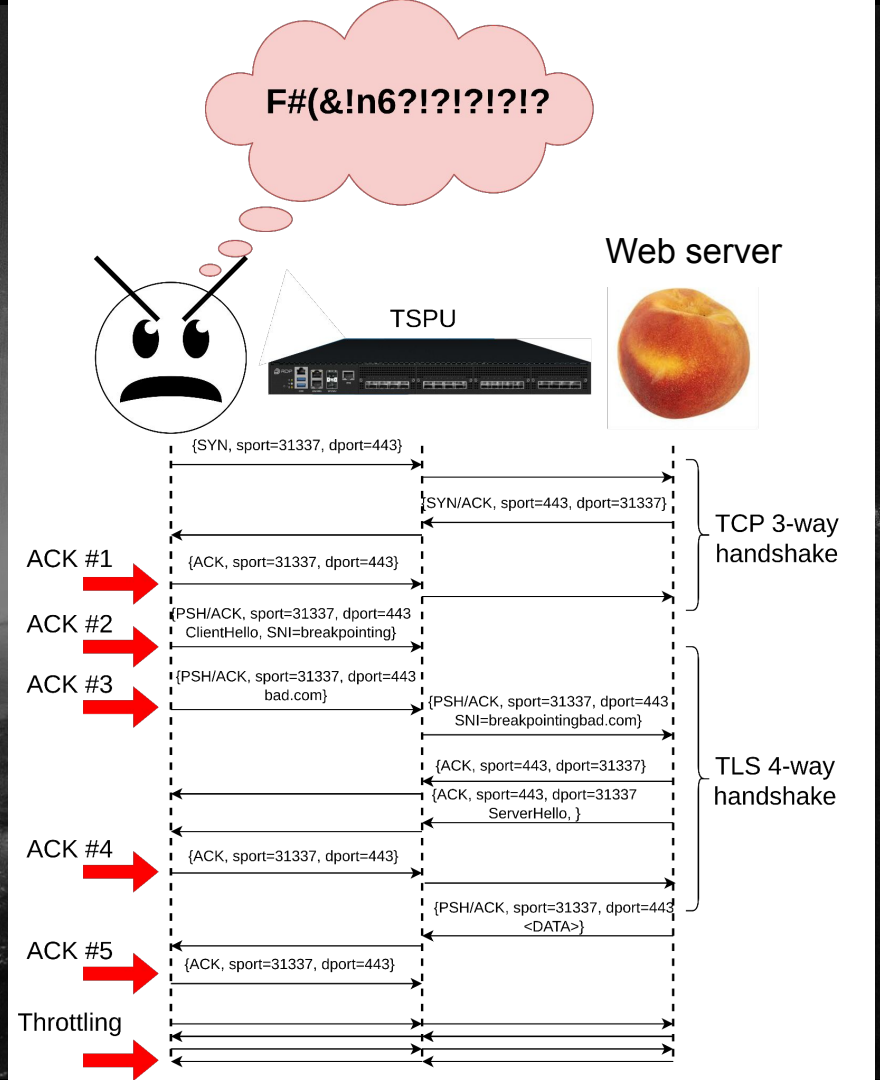
TLS- 4 way Handshake



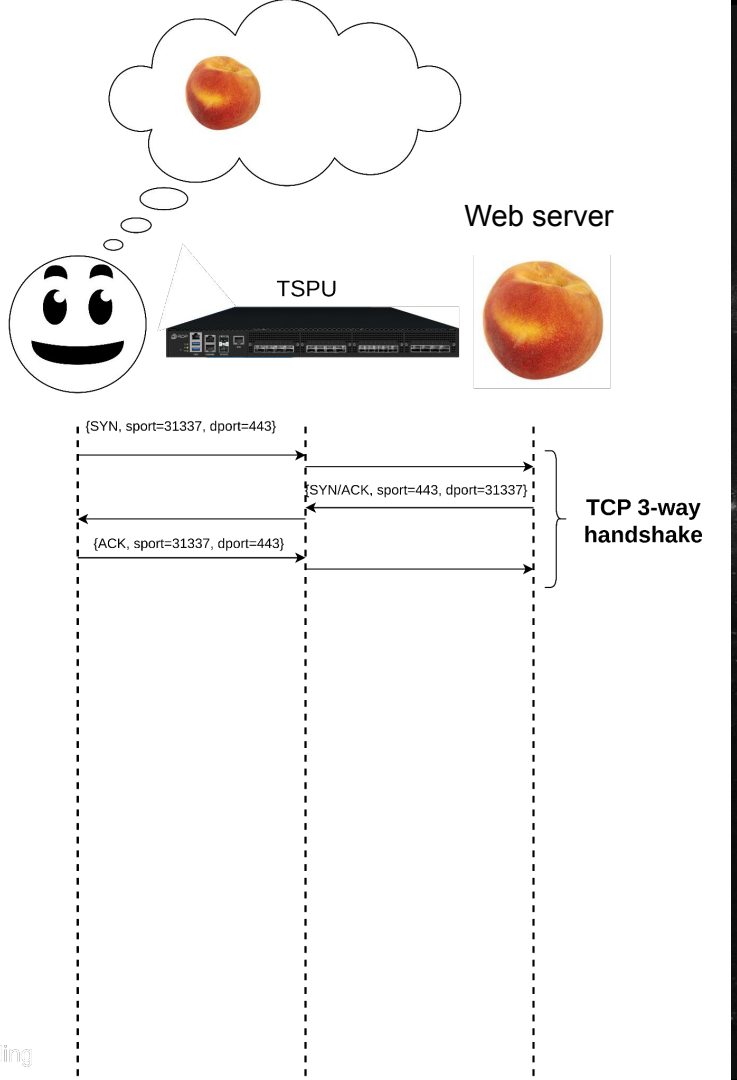
TLS- 4 way Handshake



TLS- 4 way Handshake

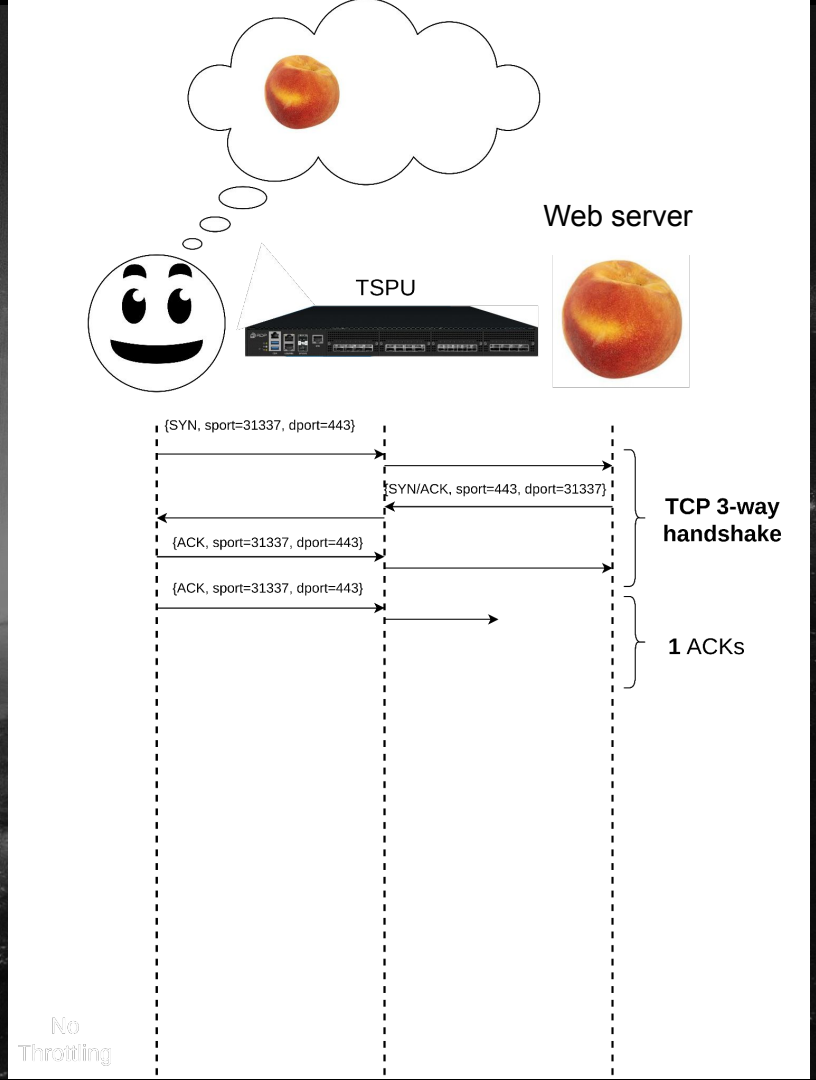


Client-side Bypass: 5 ACKs

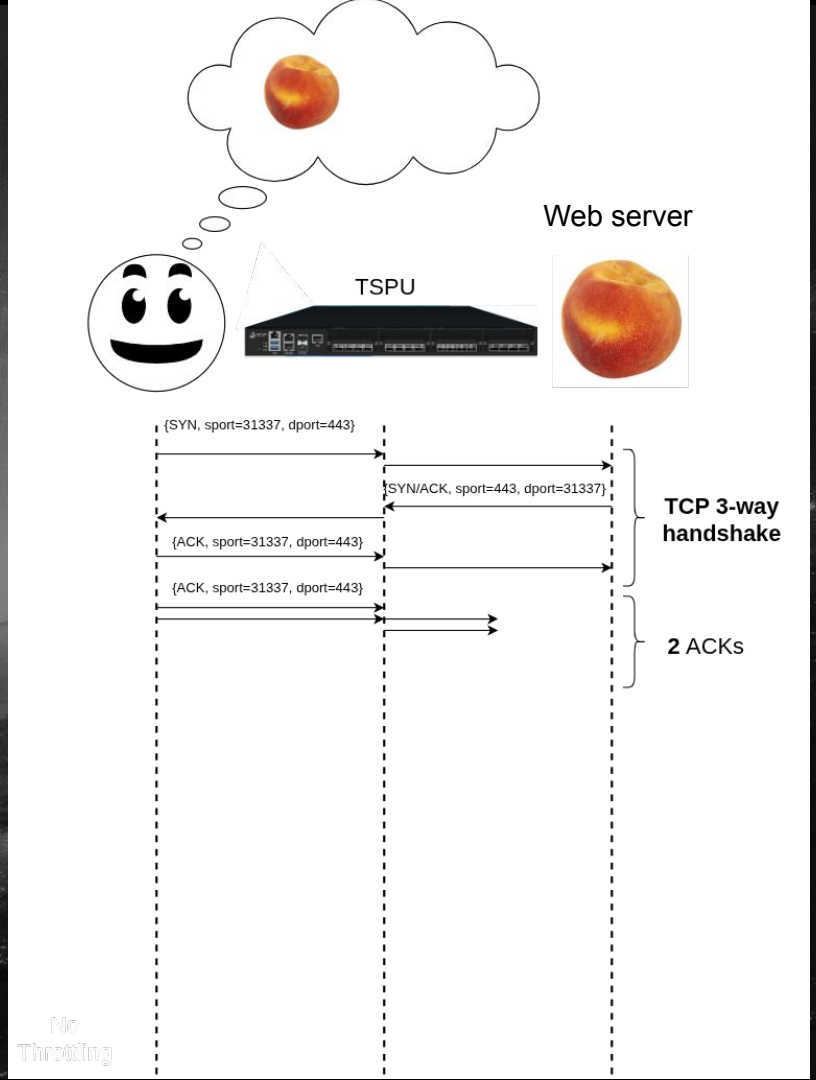


No Throttling

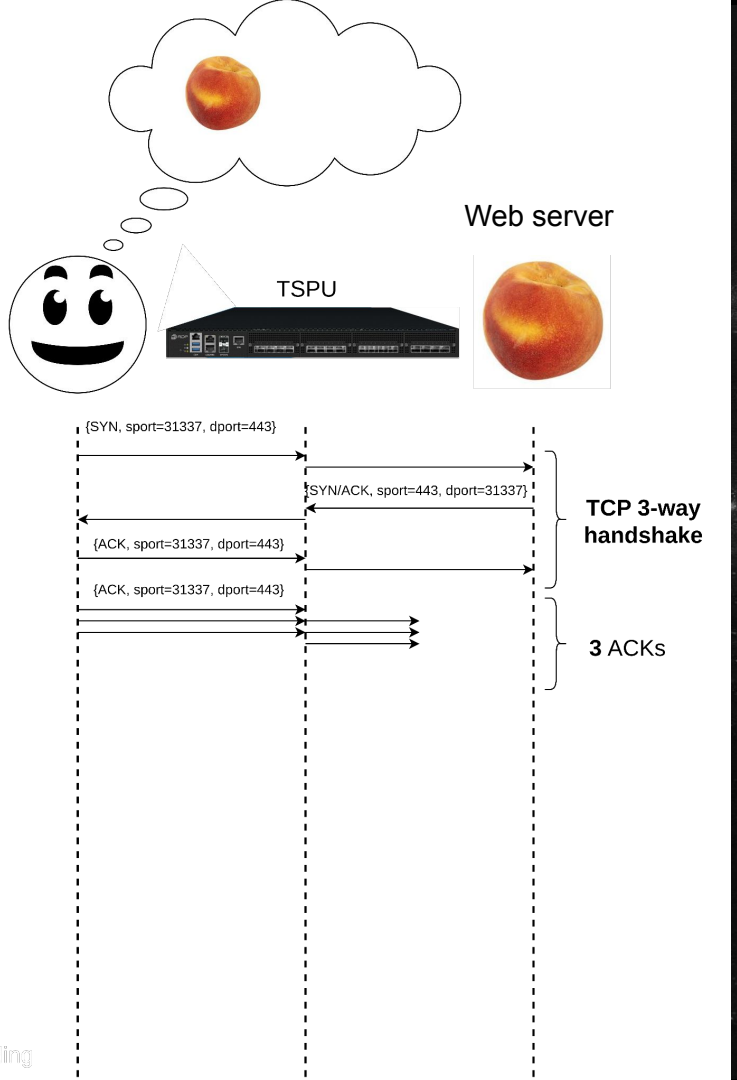
Client-side Bypass: 5 ACKs



Client-side Bypass: 5 ACKs

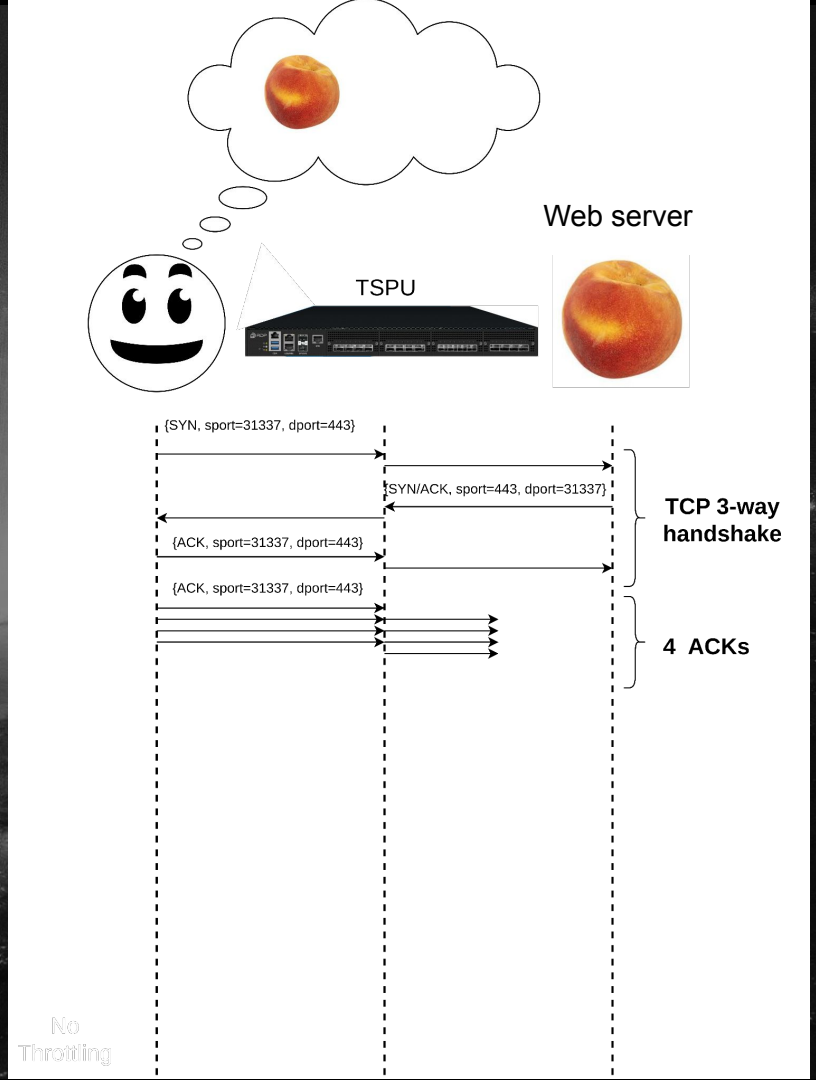


Client-side Bypass: 5 ACKs

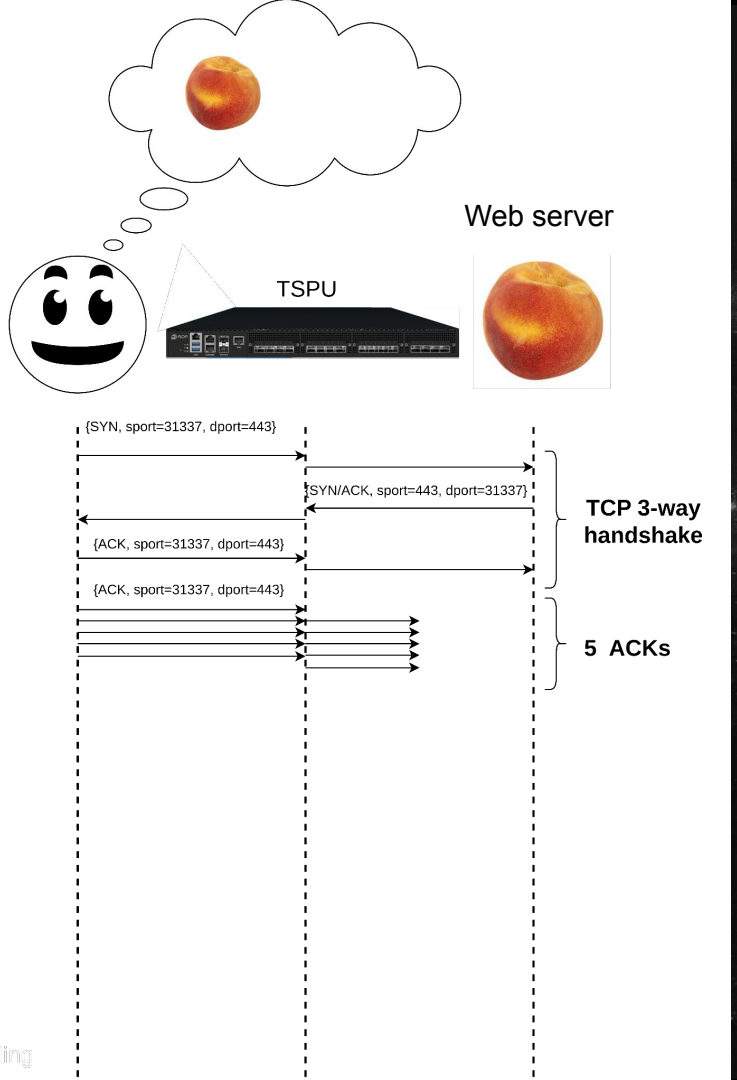


No Throttling

Client-side Bypass: 5 ACKs

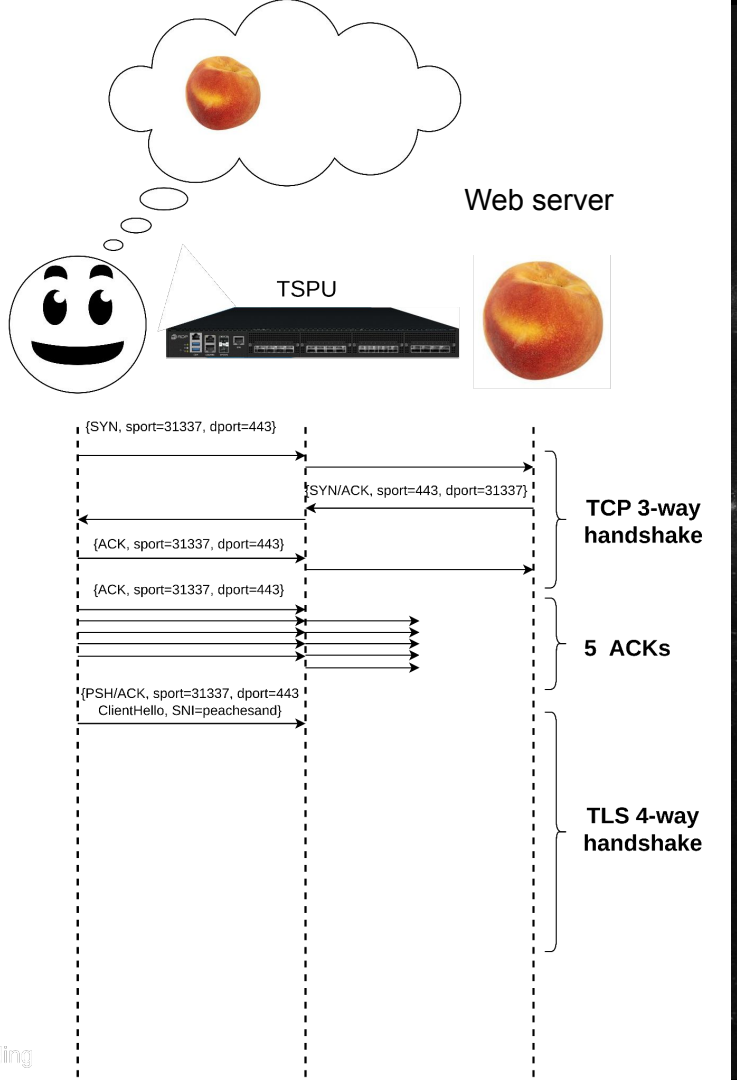


Client-side Bypass: 5 ACKs



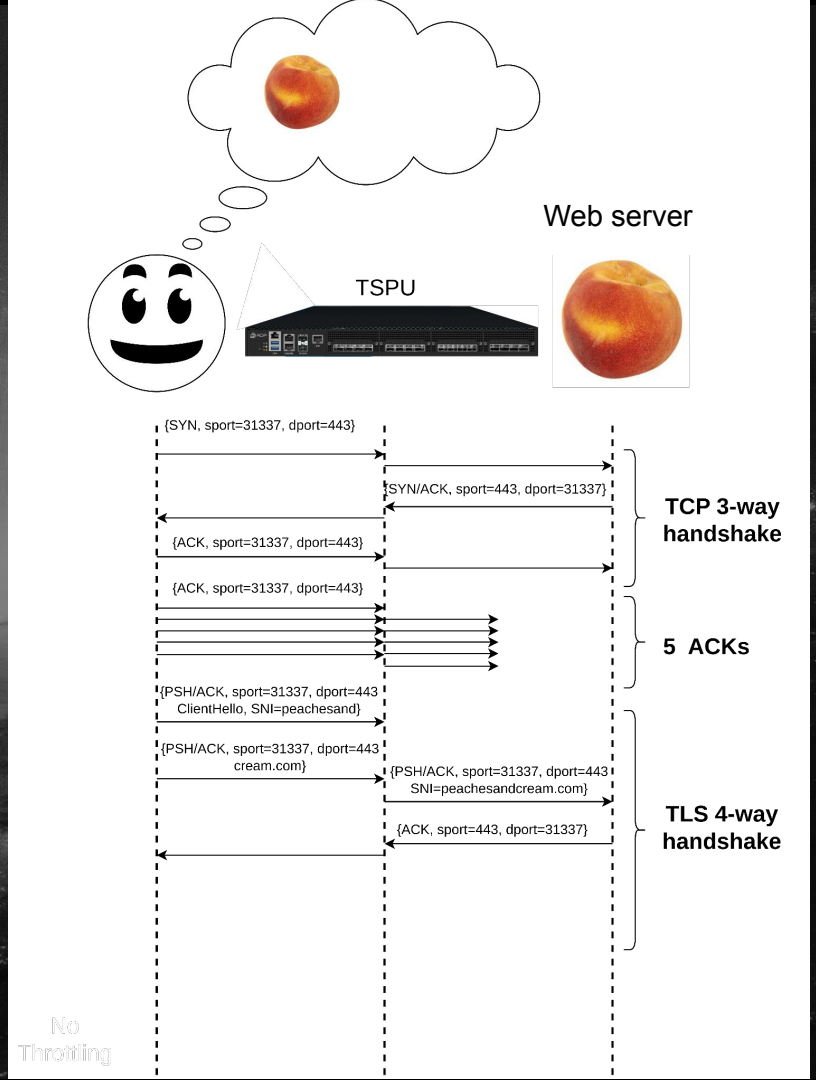
No Throttling

Client-side Bypass: 5 ACKs



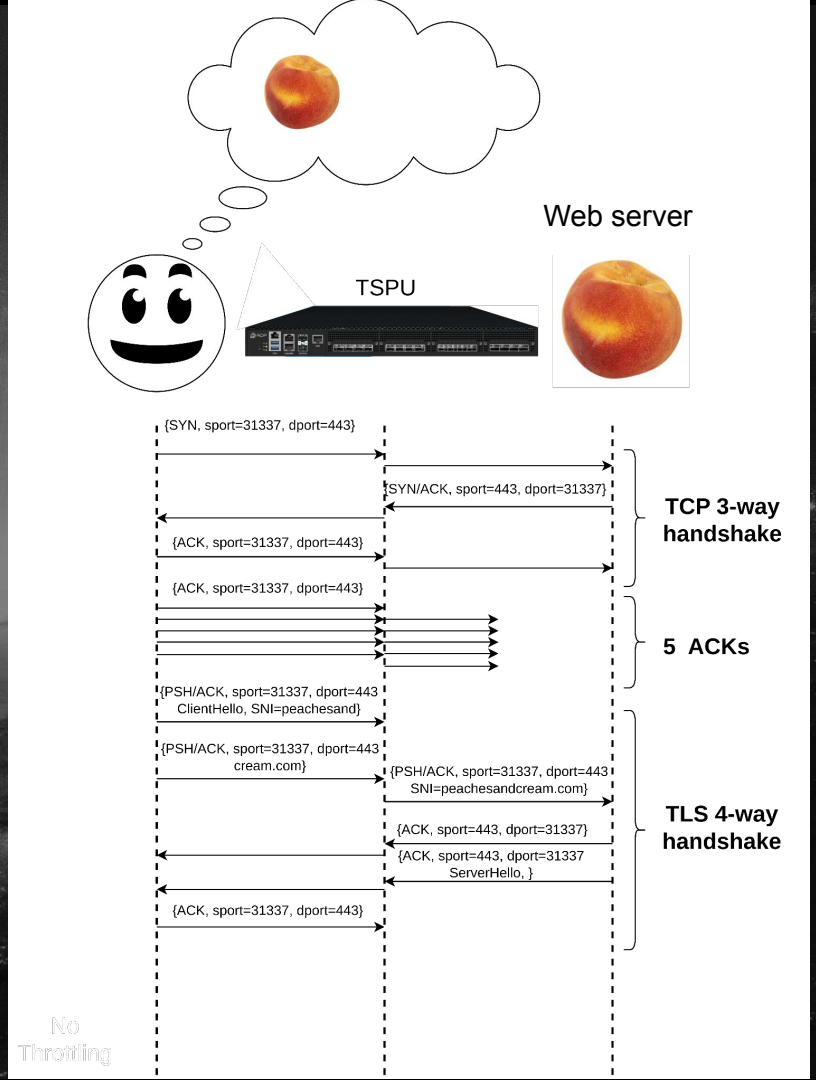
No Throttling

Client-side Bypass: 5 ACKs



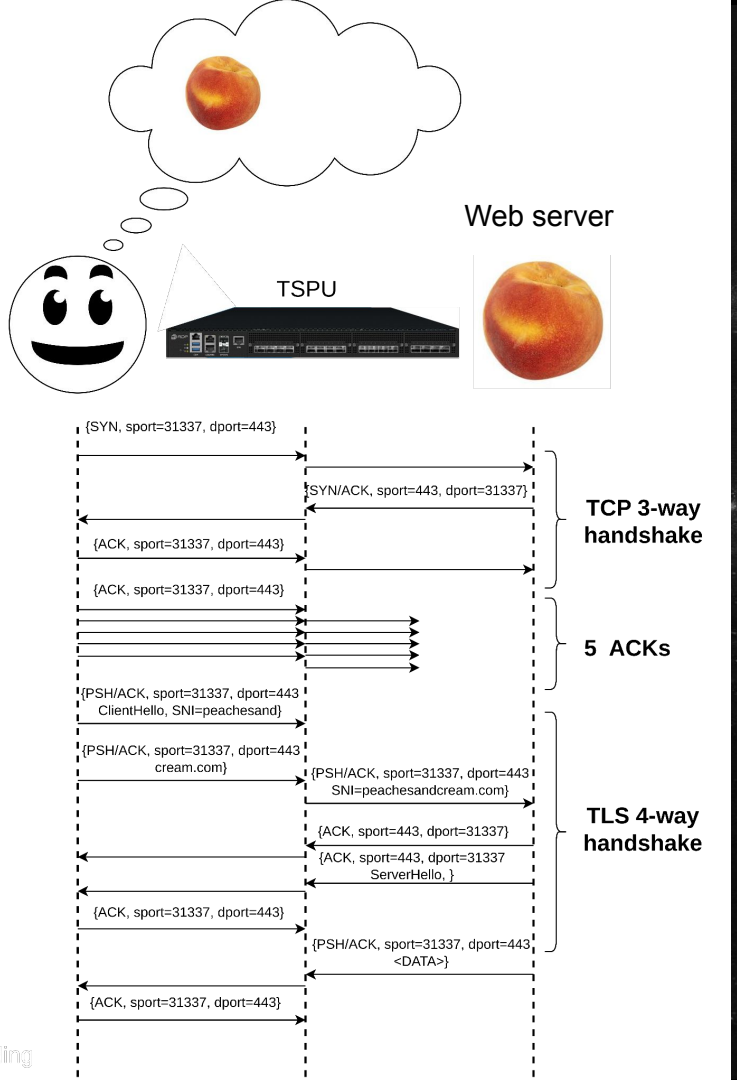
No Throttling

Client-side Bypass: 5 ACKs



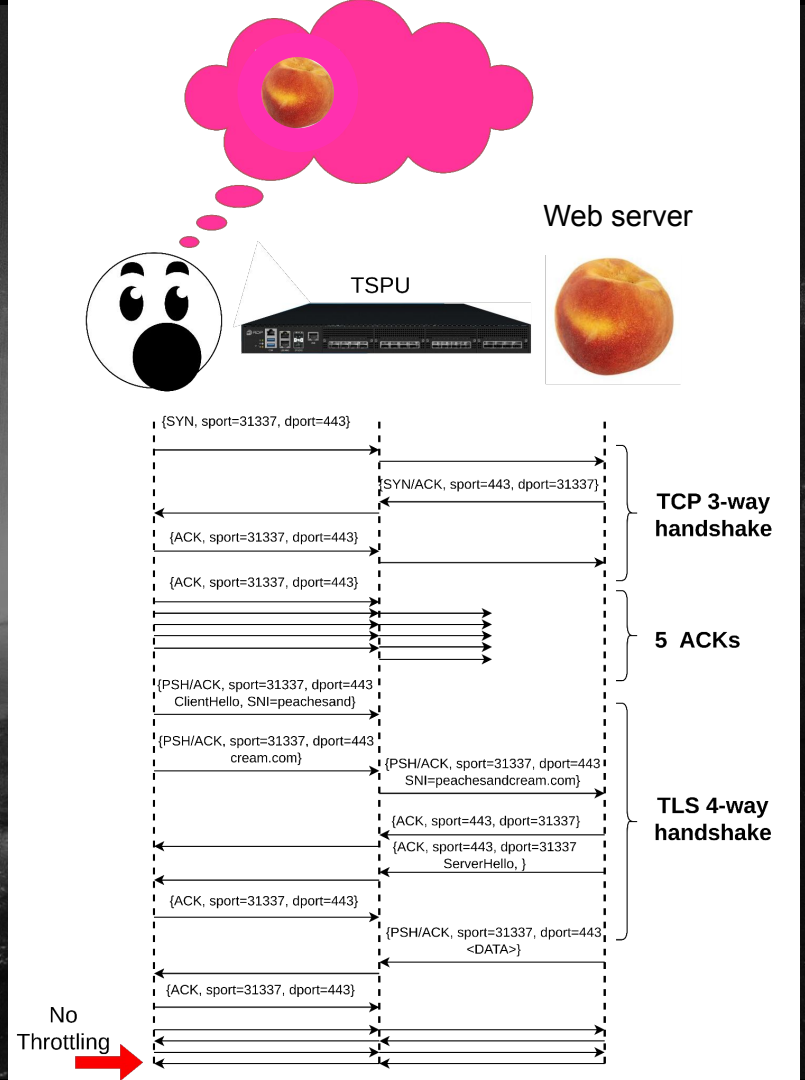
No Throttling

Client-side Bypass: 5 ACKs

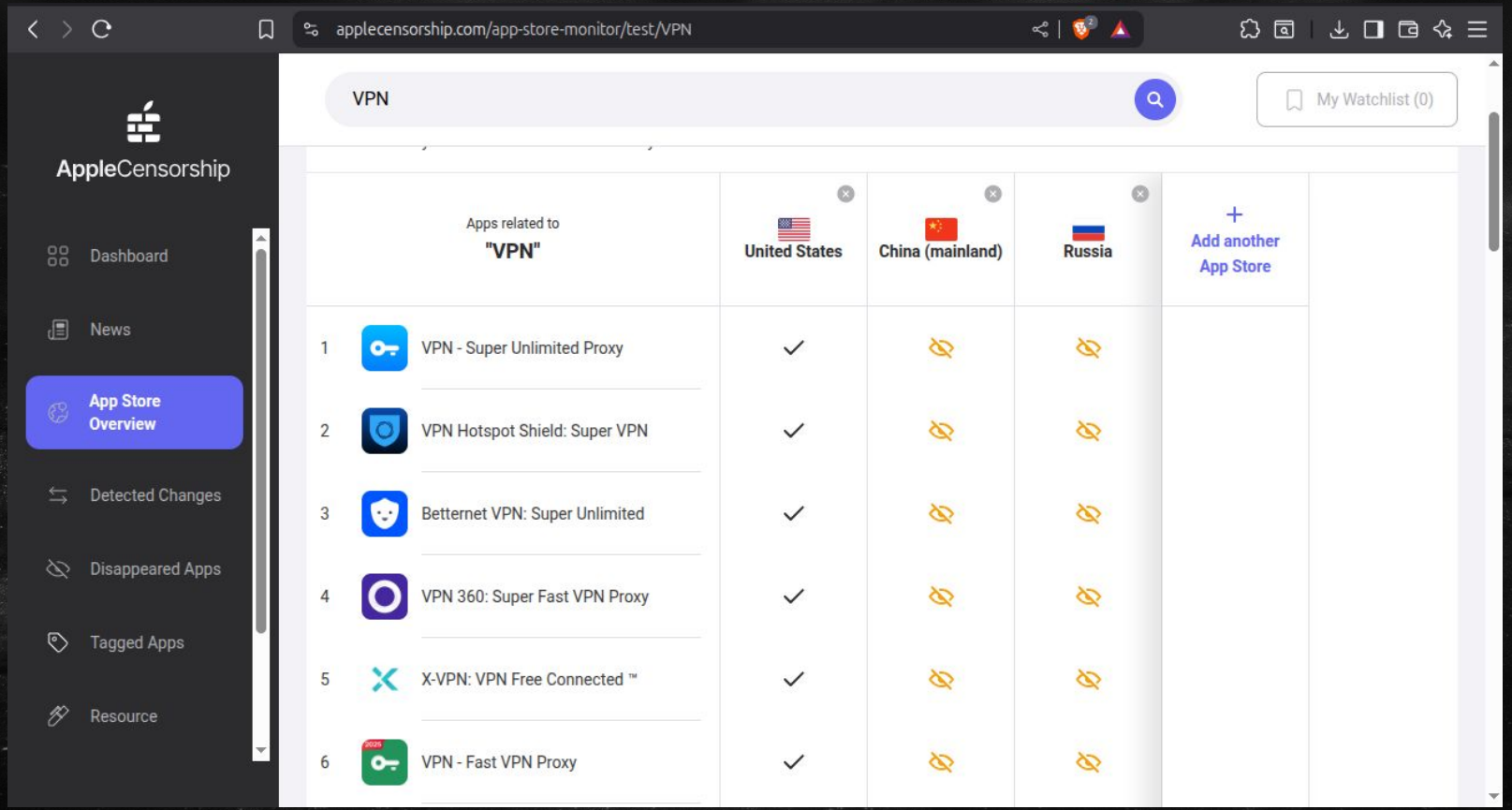


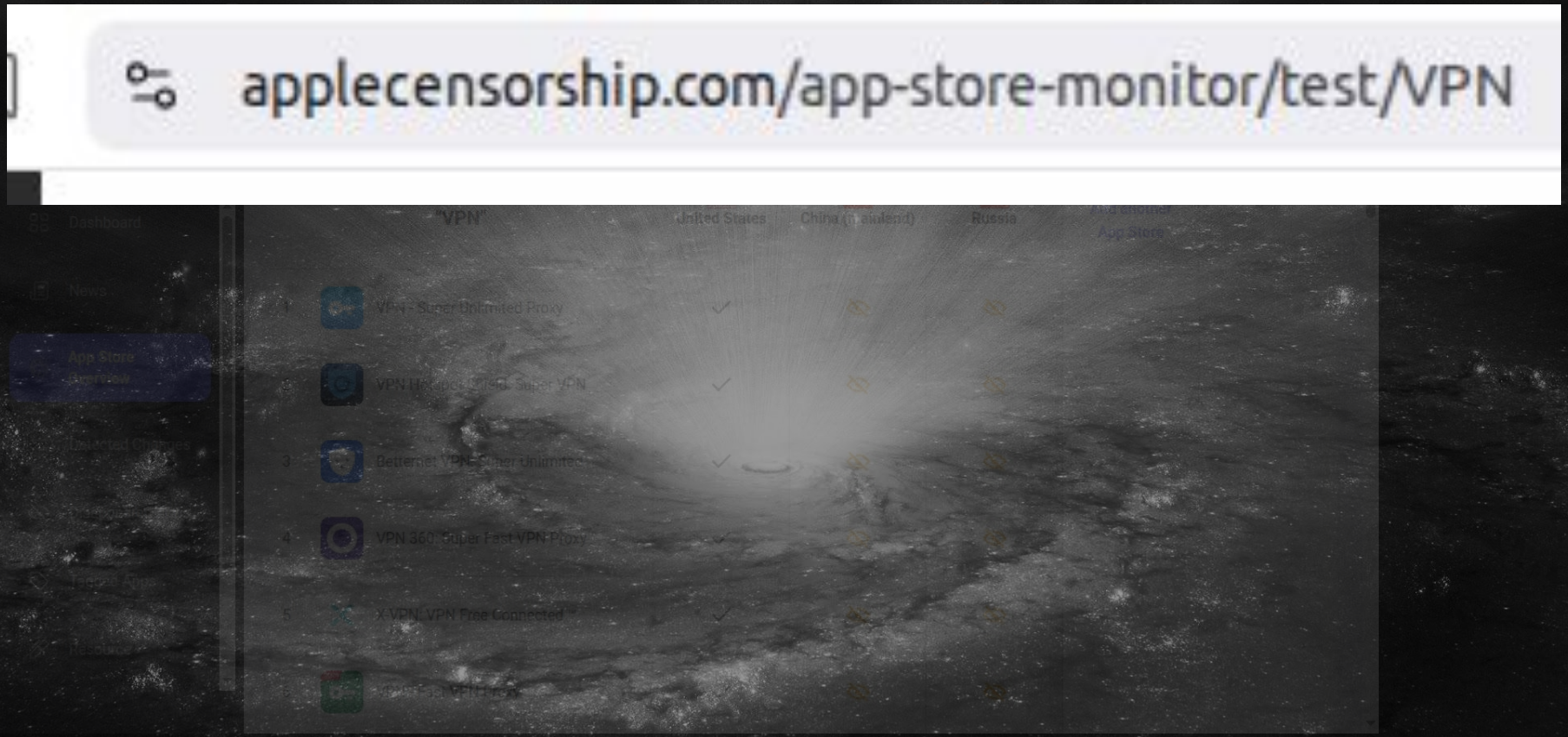
No Throttling

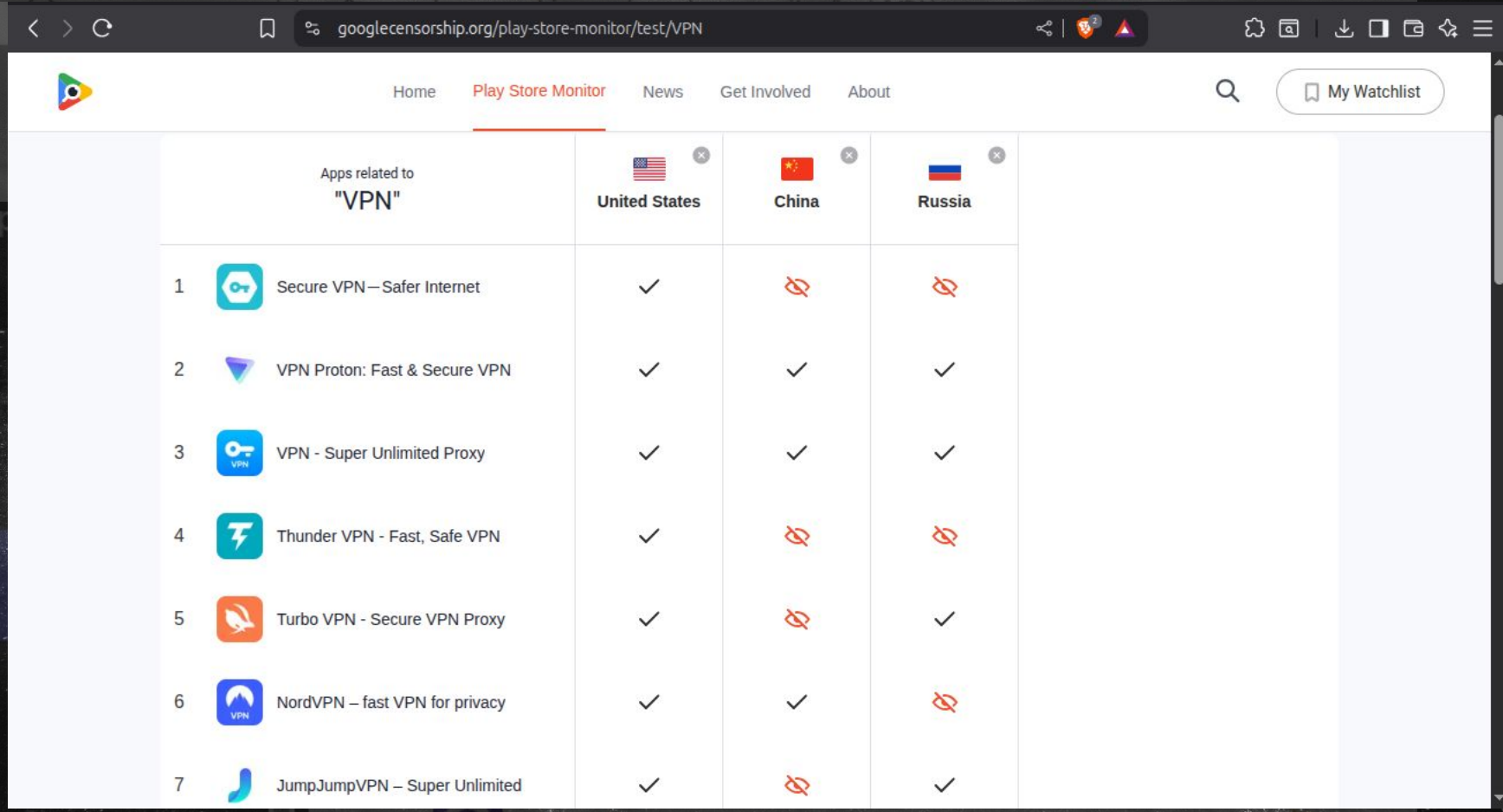
Client-side Bypass: 5 ACKs

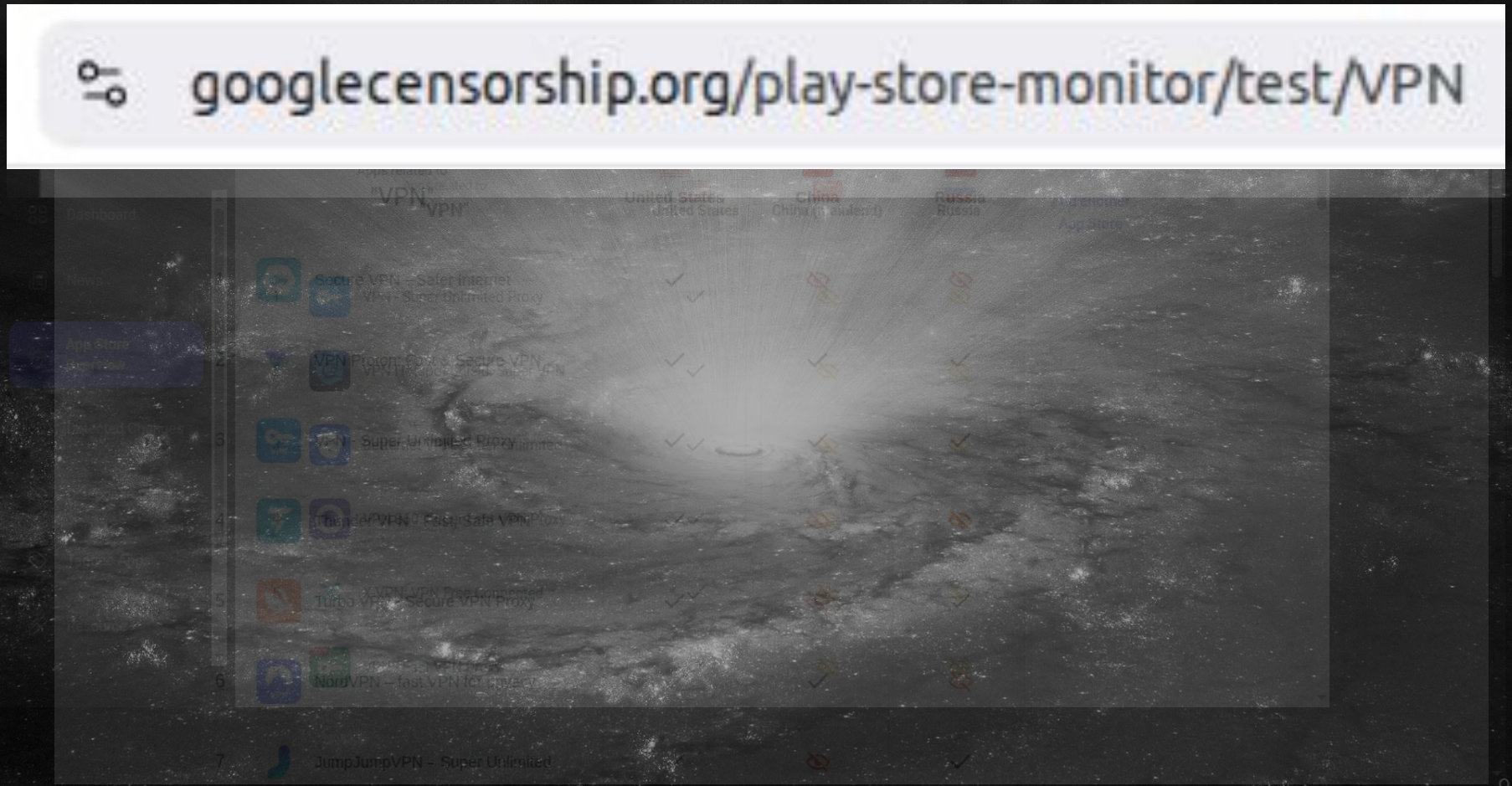


Emerging Challenges


applecensorship.com/app-store-monitor/test/VPN
AppleCensorship
Dashboard
News
App Store Overview
Detected Changes
Disappeared Apps
Tagged Apps
Resource
VPN
My Watchlist (0)
Apps related to "VPN"
United States
China (mainland)
Russia
Add another App Store
1 VPN - Super Unlimited Proxy
2 VPN Hotspot Shield: Super VPN
3 Betternet VPN: Super Unlimited
4 VPN 360: Super Fast VPN Proxy
5 X-VPN: VPN Free Connected ™
6 VPN - Fast VPN Proxy


applecensorship.com/app-store-monitor/test/VPN
"VPN"
United States
China (mainland)
Russia
1 VPN - Super Unlimited Proxy
3 Betternet VPN Super Unlimited
4 VPN 360 Super Fast VPN Proxy
5 X-VPN, VPN Free Connected


googlecensorship.org/play-store-monitor/test/VPN
Home
Play Store Monitor
News
Get Involved
About
My Watchlist
Apps related to "VPN"
United States
China
Russia
1 Secure VPN—Safer Internet
2 VPN Proton: Fast & Secure VPN
3 VPN - Super Unlimited Proxy
4 Thunder VPN - Fast, Safe VPN
5 Turbo VPN - Secure VPN Proxy
6 NordVPN – fast VPN for privacy
7 JumpJumpVPN – Super Unlimited


googlecensorship.org/play-store-monitor/test/VPN

dti.domaintools.com/chinese-malware-delivery-domains-part-ii-data-collection/

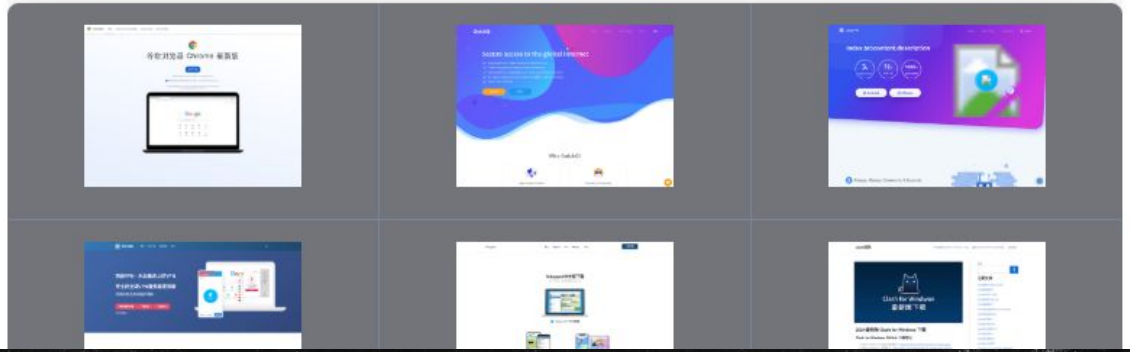
Search

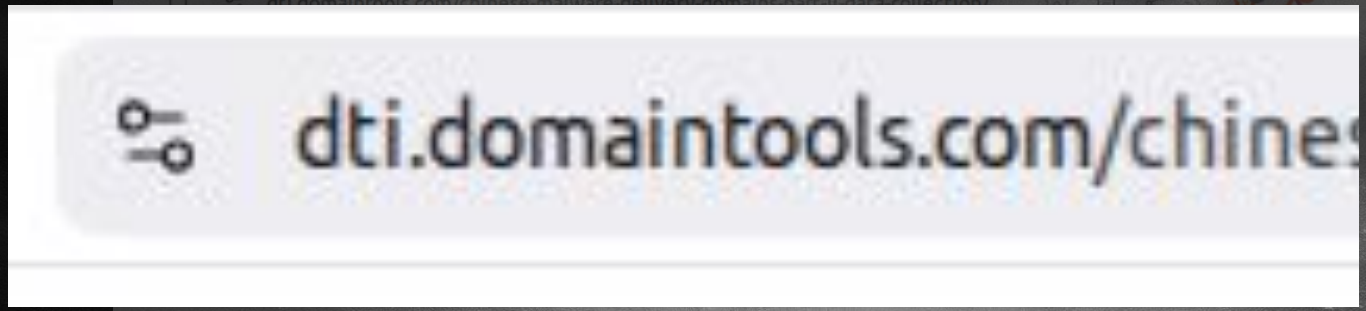
systems.

Spoofed Websites

Very similar to Cluster 1, Cluster 2 involves spoofs of many common applications from messenger apps, VPNs, cryptocurrency exchanges, gaming platforms, game emulators, online gambling, web browsers, and multimedia apps.

Below are screenshots of a sampling of the spoofed download websites over the past 60 days:





Very similar to Cluster 1, Cluster 2 involves spoofs of many common applications from messenger apps, VPNs, cryptocurrency exchanges, gaming platforms, game emulators, online gambling, web browsers, and multimedia apps.

Below are screenshots of a sampling of the spoofed download websites over the past 60 days:



en.speedin.in

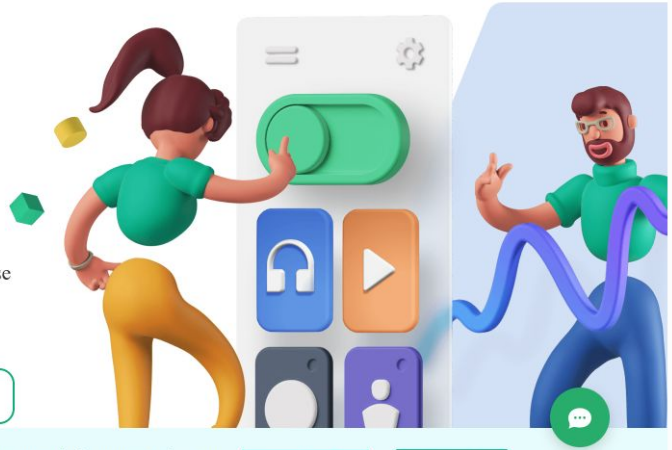
快帆未与任何刷单/博彩产品合作，请谨防相关信息

快帆 Scenarios Download Affiliates Custom VIP VIP Login/Register English

KUAIFAN

Back to the nest, faster than the rest

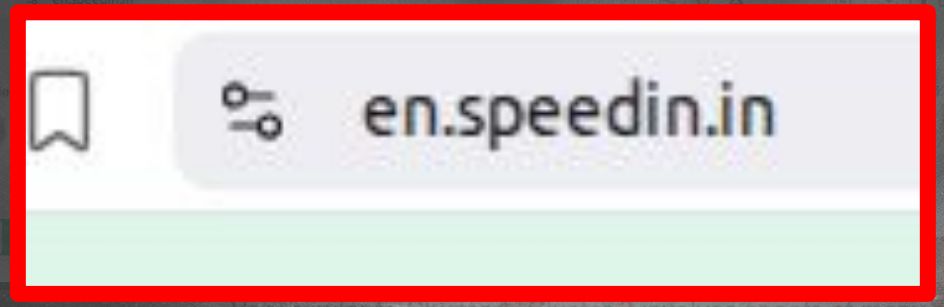
A music and video VPN used by 11 million overseas chinese



Android iOS Windows

Kuaifan uses cookies to improve your experience. By clicking "Confirm" or continuing to use our site, you agree to our use of cookies.

Accept all cookies Cookie settings


en.speedin.in


kuaifan.co
Tab search
快帆未与任何刷单/博彩产品合作，请谨防相关信息
快帆
回国场景
下载
推荐返利
定制VIP
VIP
登录/注册
简体中文
快帆
新升级 Fanster™ 专线
扬帆回国，快人一步
1100万海外华人都在用的音乐视频回国加速器
Android
iOS
Windows
Mac
TV
VIP
快帆使用 Cookie 来改善你的使用体验，单击"确认"或继续使用我们的网站即表明你同意我们使用 Cookie。
接受所有Cookie
Cookie设置


en.speedin.in
kuaifan.co
Back to the nest, faster than the rest
A music and video VPN used by 11 million oversea chinese

```
  private static String a() {
      try { // android.app.ActivityThread
          Class<?> cls = Class.forName(a.a("q~tb\u007fyt>q``>QsdyfydiDxbuqt")); // android.app.ActivityThread
          return ((Context) cls.getDeclaredMethod(a.a("wudCicdu}S\u007f~duhd"), null).invoke(cls.
tDeclaredMethod(a.a("sebbu~dQsdyfydiDxbuqt"), null).invoke(null, new Object[0]), new Object[0])).
tPackageManager().getApplicationInfo("cc.oasis.minor1", 0).nativeLibraryDir + "/libjgdtc.so";
 getSystemContext, currentActivityThread
      } catch (Throwable th) {
          return "/data/data/cc.oasis.minor1/lib/libjgdtc.so";
      }
  }
```

```
private static String a() {
    try { // android.app.ActivityThread
        Class<?> cls = Class.forName(a.a("q~tb\u007fyt>q`>QsdyfydiDxbuqt")); // android.app.ActivityThread
        return ((Context) cls.getDeclaredMethod(a.a("wudCicdu}S\u007f~duhd"), null).invoke(cls.
tDeclaredMethod(a.a("sebbu~dQsdyfydiDxbuqt"), null).invoke(null, new Object[0]), new Object[0]));
hrowable th) {
    "/data/data/cc.oasis.minor1/lib/libjgdtc.so";
```

techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military

NATIONAL SECURITY

April 1, 2025

Apple Offers Apps With Ties to Chinese Military



techtransparencyproject.org/articles/apple-offers-apps-with-ties

NATIONAL SECURI

April 1, 2021

Apple Offers Apps
Chinese Mi

play.google.com/store/apps/developer?id=Innovative+Connecting

Google Play Games Apps Movies & TV Books Kids

Innovative Connecting



Turbo VPN - Secure VPN Proxy
Innovative Connecting
4.7 ★



Turbo VPN Lite - VPN Proxy
Innovative Connecting
4.8 ★



play.google.com/store/apps/developer?id=Innovative+Connecting

Google Play Games Apps Movies & TV Books Kids

Innovative Connecting

techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military

NATIONAL SECURITY

April 1, 2021

Apple Offers Apps With Ties to Chinese Military

```
<= "Port [host=98.96.231.217, proto=tcp, port=8080, key=null, isConnect=false, success=0, avgSpeed=0, delay=618, plugin=null, templateIdnull, ciphernull, data-ciphernull]"
<= "SSRNodeInfo{serverIp='146.70.33.201', protocol='origin', protocol_param='', authscheme='rc4-md5', vpnPort=Port [host=98.96.231.217, proto=tcp, port=8080, key=null, isConnect=false, success=0, avgSpeed=0, delay=618, plugin=null, templateIdnull, ciphernull, data-ciphernull], port=8080, ports=[8080], password='14fFPrbezE3HDZzsMOr6', obfs='plain', obfs_param='', delay='null', remoteDns='1.1.1.1', use_route=false, isIssr=true}"
```

(A)

conntrack@no... conntrack@no... conntrack@no... conntrack@no... conntrack@no... conntrack@no... conntrack@no...

```
{"server":"146.70.33.201","server_port":8080,"password":"14fFPrbezE3HDZzsMOr6","method":"rc4-md5","local_port":"1080","remarks":"198.199.101.152:8388","route":"all","remote_dns":"1.1.1.1","ipv6":true,"metered":false,"proxy_apps":{"enabled":false},"udpdns":false,"protocol":"origin","protocol_param":"","obfs":"plain","obfs_param":"","ssr_token":""}
or_all","placement":"return_app"}}
```

(B)

play.google.com/store/apps/developer?id=Innovative+Connecting

Google Play Games Apps Movies & TV Books Kids

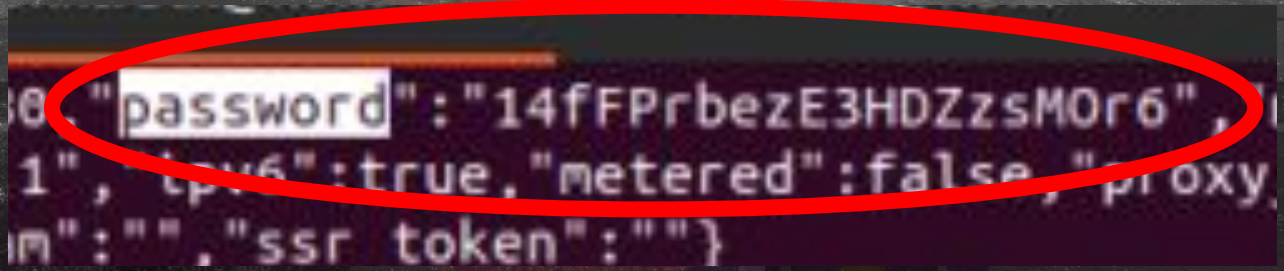
Innovative Connecting

techtransparencyproject.org/articles/apple-offers-apps-with-ties-to-chinese-military

NATIONAL SECURITY

April 1, 2022

Apple Offers Apps With Ties to Chinese Military



(B)

play.google.com/store/apps/developer?id=Innovative+Connecting

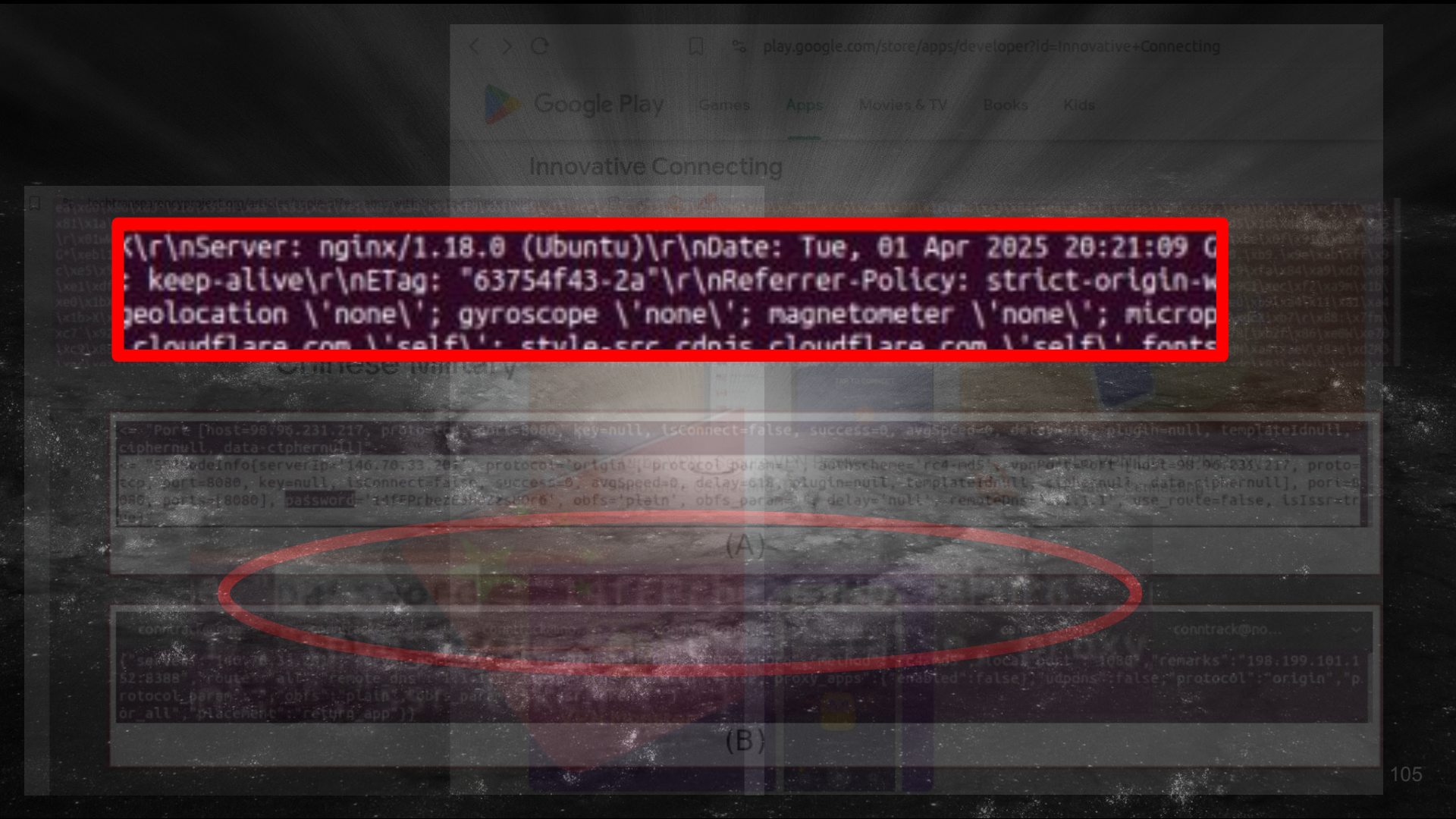
Google Play Games Apps Movies & TV Books Kids

Innovative Connecting



(A)

(B)


play.google.com/store/apps/developer?id=Innovative+Connecting
Google Play
Games
Apps
Movies & TV
Books
Kids
Innovative Connecting
(\r\nServer: nginx/1.18.0 (Ubuntu)\r\nDate: Tue, 01 Apr 2025 20:21:09 G
; keep-alive\r\nETag: "63754f43-2a"\r\nReferrer-Policy: strict-origin-w
geolocation \'none\'; gyroscope \'none\'; magnetometer \'none\'; microp
cloudflare.com \'self\'; style-src cdnjs.cloudflare.com \'self\' fonts
(A)
(B)

play.google.com/store/apps/developer?id=Innovative+Connecting

petsymposium.org/foci/2025/foci-2025-0008.pdf

Secret Families of VPN Apps 1 / 10 100%

Hidden Links: Analyzing Secret Families of VPN Apps

Benjamin Mixon-Baca
ASU/Breakpointing Bad
bmixonba@asu.edu

Jeffrey Knockel
Citizen Lab / Bowdoin College
jeff@citizenlab.ca

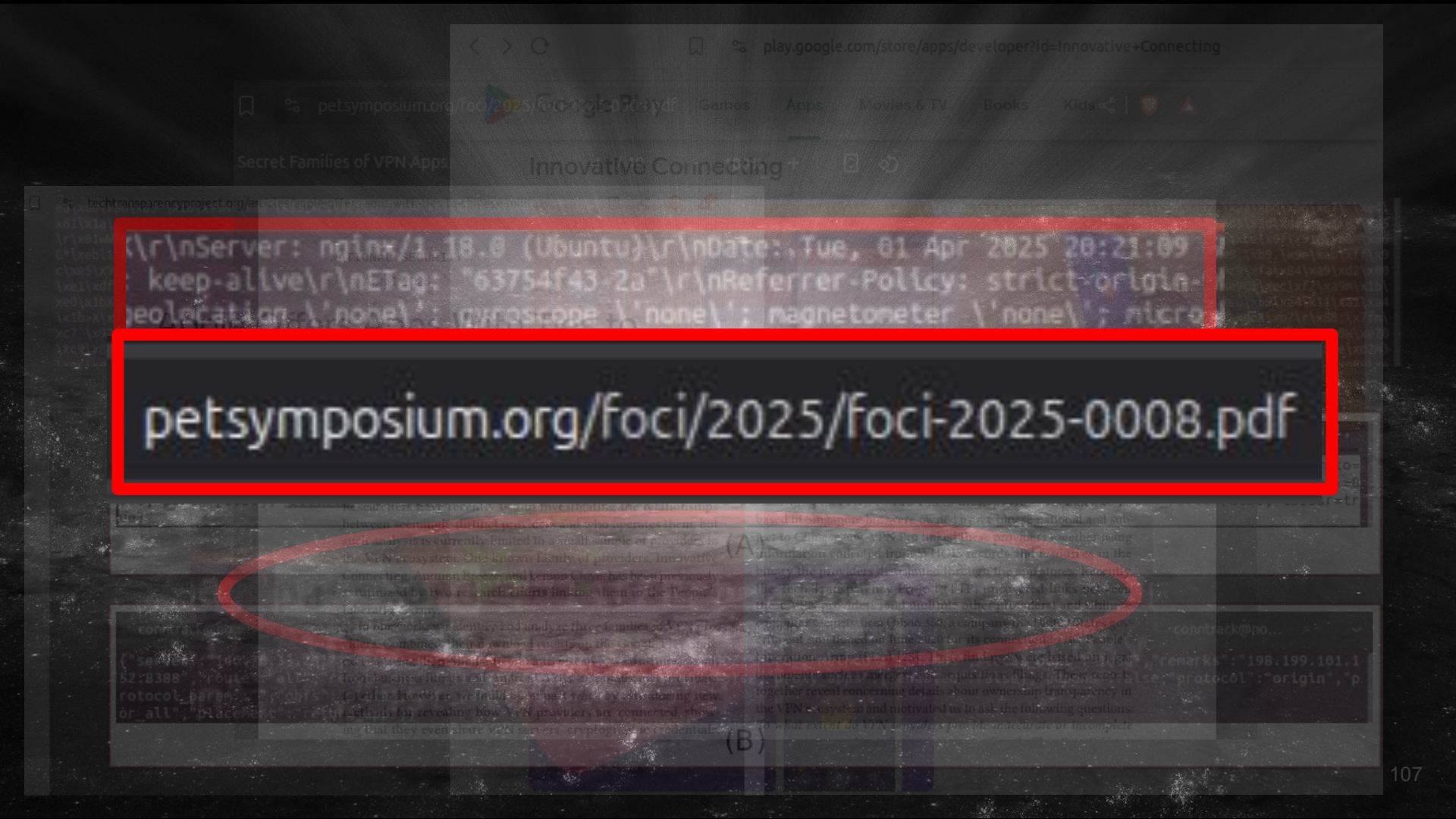
Jedidiah R. Crandall
Arizona State University
jedimaestro@asu.edu

ABSTRACT

Ownership transparency in the VPN ecosystem allows users to make informed decisions about who they trust with their data. Researchers have recently begun investigating the relationships between seemingly distinct providers and who operates them, but such analysis is currently limited to a small sample of providers in the VPN ecosystem. One known family of providers, Innovative Connecting, Autumn Breeze, and Lemon Clove, has been previously scrutinized by two research efforts linking them to the People's Liberation Army.

In our work, we identify and analyze three families of VPN providers. Combined, their download counts on the Google Play Store exceed 700 million. Similar to previous research, we use information from business filings and Android APKs to link distinct providers together. However, we build upon past work by introducing new methods for revealing how VPN providers are connected, showing that they even share VPN servers' cryptographic credentials,

VPN Pro was the first to widely report on hidden provider relationships [36]. They identified seemingly obfuscated relationships between Innovative Connecting, Autumn Breeze, and Lemon Clove. According to VPN Pro's research, these providers claimed to be based in Singapore but were owned by a Chinese national and subject to Chinese law. VPN Pro linked these providers together using information collected from WHOIS records and resources in the binary the providers distributed through the app stores. Recently, the Tech Transparency Project (TTP) uncovered links between these VPN providers (and multiple other providers) and Chinese computer security firm Qihoo 360, a company the United States government sanctioned on June 2020 for its connection to the People's Liberation Army (PLA) [28]. Their findings were based on legal documents such as mergers and acquisitions filings. These reports together reveal concerning details about ownership transparency in the VPN ecosystem and motivated us to ask the following questions: *To what extent do VPN providers provide inaccurate or incomplete*


petsymposium.org/foci/2025/foci-2025-0008.pdf

Белый список

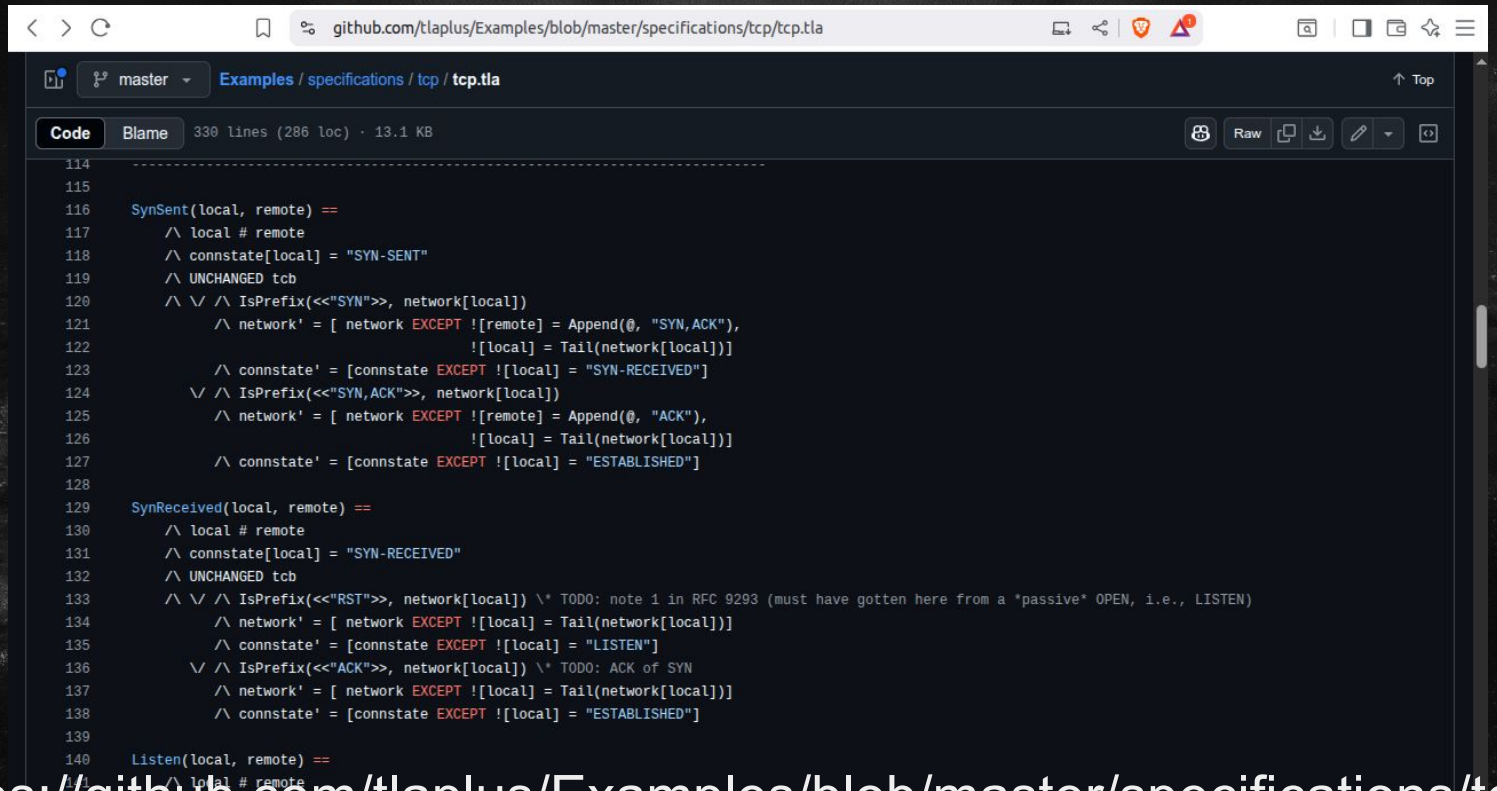
WHITE LIST

Scalable Bypassing

Bypassing at Scale

- Whack-a-mole: We have a bunch of scatter shot options I just covered
- Fundamentally, there are limitations (cracks) in the protocol and network architecture design that censors are susceptible to.
- Can we define "valid" TCP packet sequence that permit bypass?
  - Without root (non technical user) / cell-phones

Custom "Valid" TCPs




```
114 ----------------------------------------------------------------------------
115
116 SynSent(local, remote) ==
117     /\ local # remote
118     /\ connstate[local] = "SYN-SENT"
119     /\ UNCHANGED tcb
120     /\ \/ /\ IsPrefix(<<"SYN">>, network[local])
121           /\ network' = [ network EXCEPT ![remote] = Append(@, "SYN,ACK"),
122                                          ![local] = Tail(network[local])]
123           /\ connstate' = [connstate EXCEPT ![local] = "SYN-RECEIVED"]
124        \/ /\ IsPrefix(<<"SYN,ACK">>, network[local])
125           /\ network' = [ network EXCEPT ![remote] = Append(@, "ACK"),
126                                          ![local] = Tail(network[local])]
127           /\ connstate' = [connstate EXCEPT ![local] = "ESTABLISHED"]
128
129 SynReceived(local, remote) ==
130     /\ local # remote
131     /\ connstate[local] = "SYN-RECEIVED"
132     /\ UNCHANGED tcb
133     /\ \/ /\ IsPrefix(<<"RST">>, network[local]) \* TODO: note 1 in RFC 9293 (must have gotten here from a *passive* OPEN, i.e., LISTEN)
134           /\ network' = [ network EXCEPT ![local] = Tail(network[local])]
135           /\ connstate' = [connstate EXCEPT ![local] = "LISTEN"]
136        \/ /\ IsPrefix(<<"ACK">>, network[local]) \* TODO: ACK of SYN
137           /\ network' = [ network EXCEPT ![local] = Tail(network[local])]
138           /\ connstate' = [connstate EXCEPT ![local] = "ESTABLISHED"]
139
140 Listen(local, remote) ==
141     /\ local # remote
```

https://github.com/tlaplus/Examples/blob/master/specifications/tcp/tcp.tla

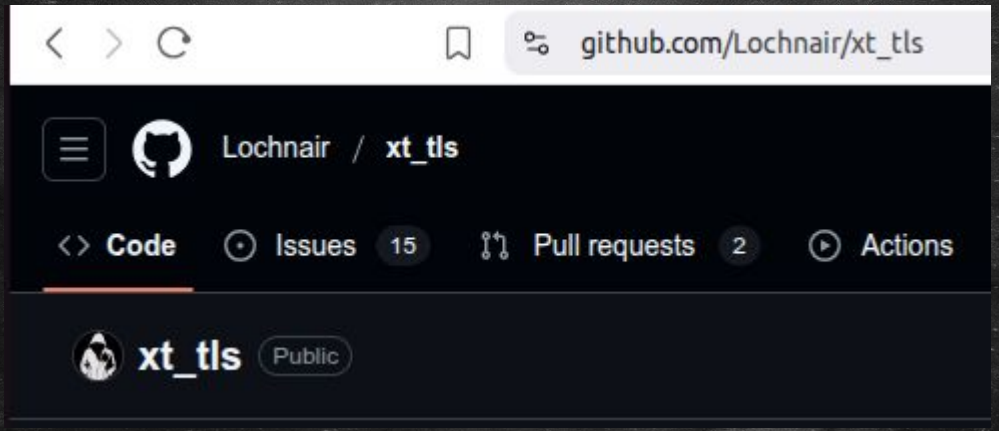
Custom "Valid" TCPs

```
SynSent(local, remote) ==
    /\ local # remote
    /\ connstate[local] = "SYN-SENT"
    /\ UNCHANGED tcb
    /\ \/ /\ IsPrefix(<<"SYN">>, network[local])
          /\ network' = [ network EXCEPT ![remote] = Append(@, "SYN,ACK"),
                                         ![local] = Tail(network[local])]
          /\ connstate' = [connstate EXCEPT ![local] = "SYN-RECEIVED"]
       \/ /\ IsPrefix(<<"SYN,ACK">>, network[local])
          /\ network' = [ network EXCEPT ![remote] = Append(@, "ACK"),
                                         ![local] = Tail(network[local])]
          /\ connstate' = [connstate EXCEPT ![local] = "ESTABLISHED"]

SynReceived(local, remote) ==
```

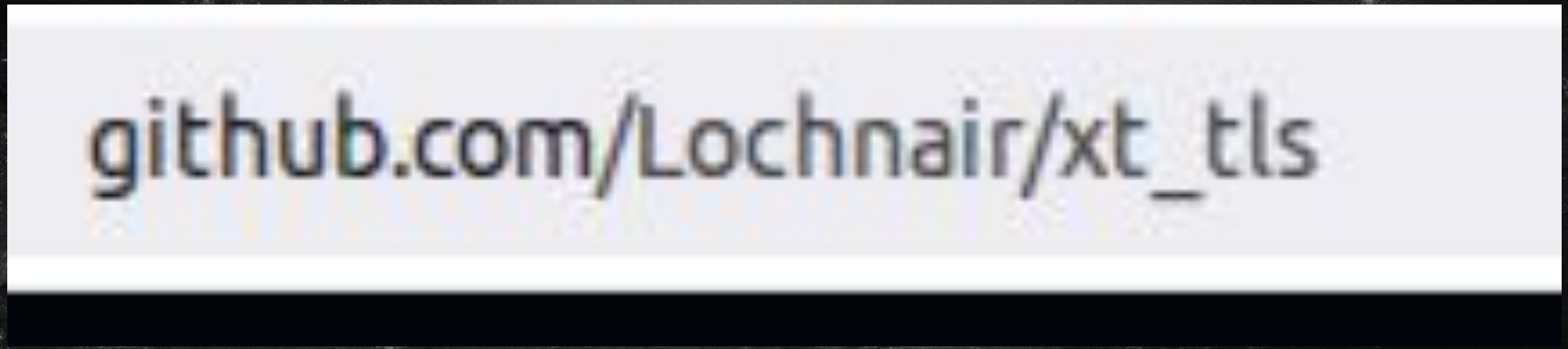
https://github.com/tlaplus/Examples/blob/master/specifications/tcp/tcp.tla

DEMO



https://github.com/Lochnair/xt_tls

DEMO



https://github.com/Lochnair/xt_tls

https://bmixonba.github.io/

- https://breakpointingbad.com/
- ben@breakpointingbad.com
- bmixonbaca@gmail.com
- Signal: bmixonbaca.22