# تحلیل فنی IRGFW

## شناخت فایروال بزرگ ایران

گزارش یک

دی ۱۴۰۳

IRGFW

irgfw.report

IRGFW
irgfw.report

## واژه‌نامه

| کلمه | معنی | کلمه | معنی | کلمه | معنی | کلمه | معنی |
|---|---|---|---|---|---|---|---|
| TCP | پروتکل انتقال قابل اعتماد و مبتنی بر اتصال | ISP | ارائه‌دهنده خدمات اینترنت | ECH | رمزنگاری ClientHello در TLS برای پنهان‌سازی اطلاعات اولیه | ASIC | مدار مجتمع با کاربرد خاص |
| TIC | شرکت ارتباطات زیرساخت | L2TP | پروتکل تونل‌سازی لایه ۲ برای اتصالات امن | ESNI | رمزنگاری دامنه‌ی SNI | ASN | شناسه منحصربه‌فرد سیستم خودمختار در اینترنت |
| TLS | پروتکل رمزنگاری و اعتبارسنجی در لایه انتقال | MCI | شرکت ارتباطات سیار ایران *(همراه اول)* | GFW | فایروال بزرگ چین | CDN | شبکه توزیع محتوا برای تحویل سریع داده |
| TOR | شبکه‌ی تور | MTN | شرکت ایرانسل | GRPC | چارچوب فراخوانی رویه از راه دور بر پایه HTTP/2 | CIDR | روش تخصیص و مسیریابی آدرس‌های IP بدون کلاس |
| UDP | پروتکل دیتاگرام کاربر بدون تضمین تحویل | NIN | شبکه‌ی ملی اطلاعات | HTTP | پروتکل پایه انتقال مستندات وب | CPU | واحد پردازش مرکزی رایانه |
| UL | ارسال داده به سرور *(آپلود)* | OBFS | مبهم‌سازی | HTTPS | HTTP بر بستر TLS برای امنیت ارتباط | DDOS | حمله گسترده به سرویس از طریق انبوه درخواست‌ها |
| UTLS | نسخه تغییرپذیر TLS برای پنهان‌سازی الگوی ترافیک | P2P | ارتباط همتا به همتا | HU | ارتقای HTTP *(=وبسوکت)* | DL | بارگیری داده از سرور *(دانلود)* |
| VPN | شبکه خصوصی مجازی برای ایجاد اتصال امن از راه دور | PPTP | پروتکل تونل‌سازی نقطه به نقطه *(قدیمی)* | ICMP | پروتکل ارسال پیام‌های کنترل و خطا در شبکه IP | DNS | سامانه تبدیل نام دامنه به آدرس IP |
| VPS | سرور مجازی ابری | QUIC | پروتکل کم‌تأخیر و کارآمد مبتنی بر UDP | IKEV2 | پروتکل مبادله کلید برای ایجاد تونل‌های امن (VPN) | DOH | DNS مبتنی بر HTTPS |
| WS | پروتکل ارتباط دوسویه و بی‌درنگ بین سرویس‌گیرنده و سرور *(وبسوکت)* | SNI | مشخصه نام سرور *(دامنه)* در ابتدای ارتباط TLS | IPM | پژوهشگاه دانش‌های بنیادی ایران | DOQ | DNS مبتنی بر QUIC |
| | | SSH | Secure Shell | IPSEC | چارچوب امنیتی برای بسته‌های IP | DOT | DNS مبتنی بر TLS |
| | | SSTP | تونل‌سازی امن از طریق SSL/TLS | IPV4 | نسخه چهارم پروتکل اینترنت با فضای آدرس محدود | DOU | DNS مبتنی بر UDP |
| | | SYN | بسته اولیه برای همگام‌سازی اتصال TCP | IPV6 | نسخه ششم پروتکل اینترنت با فضای آدرس گسترده‌تر | DPI | بازرسی عمیق بسته‌ها برای تحلیل یا کنترل ترافیک |
| | | TCI | شرکت مخابرات ایران | IRGFW | فایروال بزرگ ایران | DTLS | نسخه دیتاگرام TLS برای ارتباط امن روی UDP |

*(جدول ۱ – واژه‌نامه)*

## تاریخچه مختصری از فایروال بزرگ ایران (IRGFW)

پیش از کشته شدن غم‌انگیز مهسا امینی[۱][۲]، سامانه فیلترینگ اینترنت رژیم اسلامی ایران نسبتاً ساده بود. روش‌های اصلی به‌کارگرفته‌شده، محدود به مسدودسازی از طریق DNS و SNI بود که عملاً ارتباطات غیررمزنگاری‌شده (بدون و با TLS) و آدرس‌های IP خارجی را مختل می‌کرد. فناوری‌های بازرسی عمیق بسته (DPI) و کاوش فعال (Active-Probing) در حداقل ممکن و تقریباً نامحسوس به‌کار می‌رفتند که نشان‌دهنده رویکردی کمتر فراگیر در کنترل ترافیک اینترنت بود.

اما پس از کشته شدن مهسا امینی و اعتراضات سراسری پس از آن، وضعیت به‌شدت تغییر کرد. شرکت ارتباطات زیرساخت (TIC) و سایر نهادها، زیرساخت سانسور اینترنت ملی را به‌طور قابل‌توجهی ارتقا دادند. این امر شامل تهیه و ورود سخت‌افزارهای پیشرفته فایروال و DPI بود و بیانگر گذار به سیستمی سخت‌گیرانه‌تر و پیچیده‌تر در کنترل اینترنت محسوب می‌شود.[۳]

فایروال ایران هر چه بیشتر از مدل سانسور اینترنت چین، که اغلب با عنوان "فایروال بزرگ چین" شناخته می‌شود، الهام گرفته است.[٤] اگرچه مقامات رسمی ادعا می‌کنند که ج.ا. ایران مستقیماً از الگوی چین پیروی نمی‌کند، اما شباهت‌ها و نزدیکی‌های انکارناپذیری در روش‌ها و راهبردهای به‌کاررفته وجود دارد.[٥] ج.ا. ایران زیرساخت اینترنت ملی خود را توسعه داده و تلاش می‌کند حجم ترافیک داخلی اینترنت را به حدود ۷۰ درصد از کل ترافیک کشور برساند، رویکردی مشابه چین در ترویج خدمات اینترنت داخلی برای کاهش وابستگی به پلتفرم‌های جهانی.[٦][۷][۸]

علاوه بر ارتقای سخت‌افزارها، ج.ا. ایران مقررات سخت‌گیرانه‌تری را بر پلتفرم‌های اینترنتی تحمیل کرده و آن‌ها را ملزم می‌کند از قوانین محلی و داخلی تبعیت کنند، در غیر این صورت با سانسور مواجه می‌شوند. این طرح به اسم "صیانت"، رویکردی با هدف ایجاد محیطی کنترل‌شده در فضای اینترنت صورت می‌گیرد تا نفوذ پلتفرم‌های خارجی کاهش یابد و کنترل دولت بر محتوای دیجیتال و ارتباطات افزایش یابد.[۹]

# فایروال ایران: مرزهای دیجیتال

فایروال بزرگ ایران (IRGFW) همچنین از بازرسی عمیق بسته‌ها (DPI) به‌صورت گسترده برای تحلیل و پالایش ترافیک اینترنت در سطحی جزئی استفاده می‌کند. این فناوری به دولت امکان می‌دهد وب‌سایت‌های مشخصی را مسدود، استفاده از اینترنت را نظارت، و دسترسی به محتوای معین را محدود کند. ارائه‌دهندگان اصلی خدمات اینترنت (ISP) در ایران، مانند شرکت ارتباطات سیار ایران-همراه‌اول (MCI)، ایرانسل (MTN) و شرکت مخابرات ایران (TCI)، در سطح بالادستی به شرکت ارتباطات زیرساخت (TIC) با شماره شناسایی AS49666 متصل می‌شوند؛ این نقطه محل استقرار فایروال اصلی است. این تمرکززدایی در نقطه‌ای مشخص، تضمین می‌کند که عملیات مسدودسازی و پالایش ترافیک در میان تمامی ISPs به‌صورت یکنواخت و یکپارچه اعمال شود.[۱۰][۱۱]

اجرای سراسری این فناوری‌های پیشرفته و سیاست‌های سخت‌گیرانه، توانایی ایران در پایش و کنترل استفاده از اینترنت را به‌طرز چشمگیری افزایش داده است. این تحول بازتاب‌دهنده‌ی روندی گسترده‌تر در جهت اقتدارگرایی دیجیتال است که با تکیه بر فناوری‌های پیشرفته، جریان اطلاعات را تحت کنترل درآورده و مخالفت‌ها را سرکوب می‌نماید.

فایروال بزرگ ایران (IRGFW) یک سازوکار سرکوبگر و چندلایه برای سانسور و کنترل اینترنت است که با بهره‌گیری از فنون پیشرفته پالایش شبکه و بازرسی ترافیک، محدودیت‌های فراگیری را بر ارتباطات آنلاین تحمیل می‌کند. هرچند ماهیت سرکوبگرانه‌ی آن آشکار است، این سامانه با ترکیب لایه‌های گوناگون فنی و سیاسی، به شکلی قدرتمند ترافیک اینترنت داخلی را مهار و زیر نظر می‌گیرد. این گزارش با ارائه‌ی تحلیلی فنی از زیرساخت و نحوه‌ی عملکرد IRGFW، به روشن شدن مکانیزم‌های اعمال این کنترل گسترده کمک می‌کند.

در هسته‌ی اصلی، IRGFW از طریق همکاری هماهنگ میان ارائه‌دهندگان اصلی خدمات اینترنت و شرکت ارتباطات زیرساخت (TIC) به‌عنوان ارائه‌دهنده‌ی اصلی سطح بالادستی (Upstream Provider) عمل می‌کند. با بهره‌گیری از روش‌هایی همچون DPI، مسدودسازی آدرس‌های IP و سایر راهکارهای پیشرفته مدیریت شبکه، IRGFW کنترل سخت‌گیرانه‌ای بر جریان داده اعمال می‌نماید. درک معماری و عملکرد این سامانه برای فهم گستره و کارآمدی سانسور اینترنت در ایران ضروری است.

در نخستین گام، نیاز به درکی پایه‌ای از نحوه و محل عملکرد IRGFW داریم. بی‌شک، می‌توان گفت این سامانه مجموعه‌ای منحصربه‌فرد از فایروال‌ها است.

## فایروال‌ها و ASهای اصلی

ارائه‌دهندگان اصلی خدمات اینترنت مصرف‌کنندگان در ایران عبارت‌اند از:

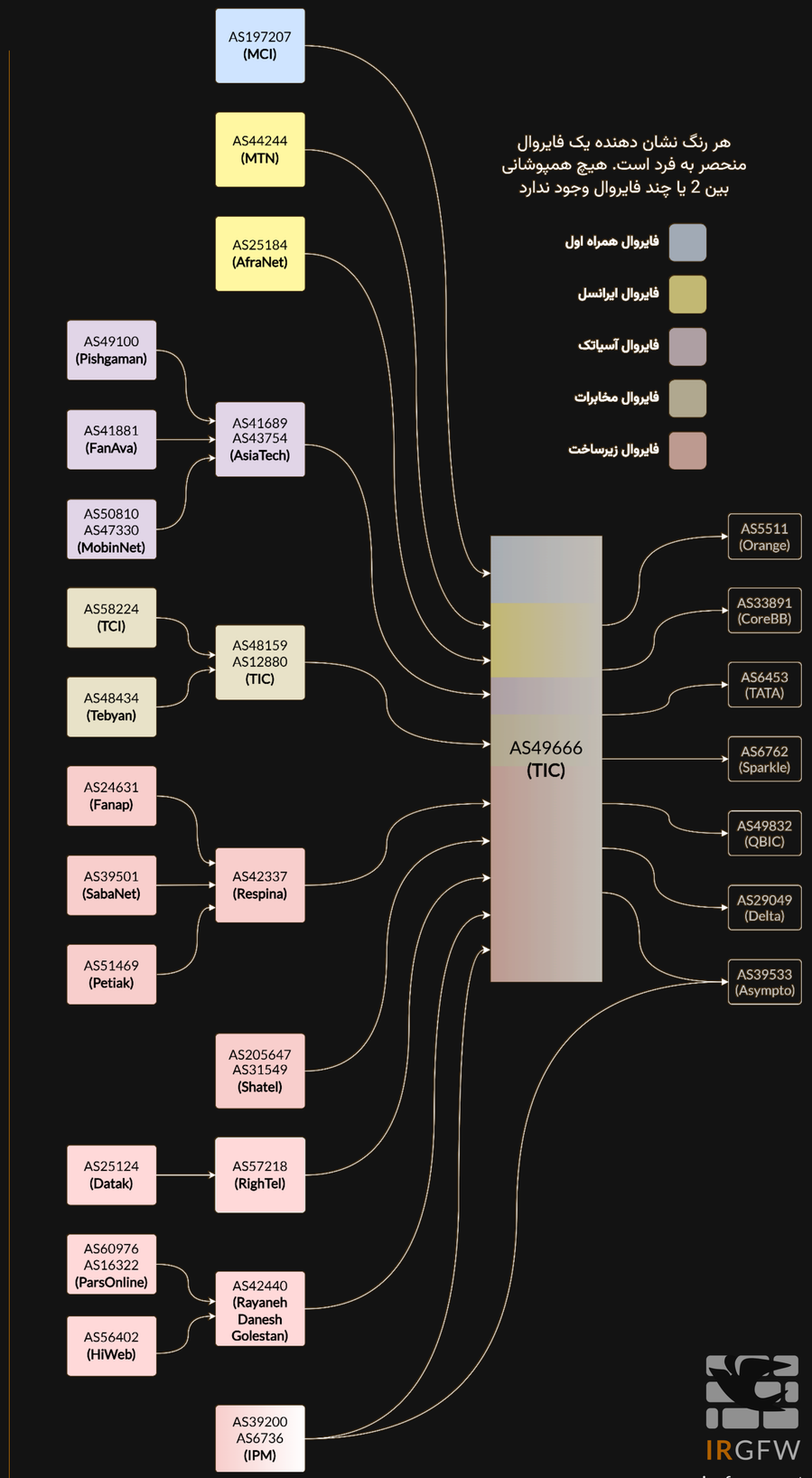
- **شرکت ارتباطات سیار ایران-همراه‌اول** (MCI) با شناسه AS197207 [12]
- **شرکت ایرانسل** (MTN) با شناسه AS44244 [13]
- **شرکت مخابرات ایران** (TCI) با شناسه‌های AS48159 و AS12880 [14][15]

تمامی اپراتورهای اینترنتی در سطح بالادستی به شرکت ارتباطات زیرساخت (TCI) با شناسه AS49666 متصل می‌شوند، جایی که فایروال و گذرگاه (Gateway) اصلی مستقر است.[۱۵]

هر یک از این ارائه‌دهندگان خدمات اینترنت (ISP) از فایروال‌های متفاوتی استفاده می‌کنند و سایر اپراتورها از یکی از این فایروال‌ها پیروی می‌کنند. به‌عنوان مثال، اگر یک آدرس IP بر روی شبکه آسیاتک مسدود شود، این آدرس بر روی شبکه‌های پیشگامان، فناوا و مبین‌نت نیز مسدود خواهد شد. این مسئله در مورد بازرسی عمیق بسته‌ها (DPI) و خود فایروال نیز صادق است. پیشرفته‌ترین فایروال متعلق به بزرگترین تلفن همراه ایران، اپراتور همراه‌اول (MCI) است.

با این حال، گاهی اوقات این فایروال‌ها به‌ویژه فایروال همراه‌اول به‌دلیل رویدادهای سراسری در کشور غیرفعال می‌شوند. در چنین شرایطی، از فایروال اصلی شرکت زیرساخت (AS49666) استفاده می‌شود. برای نمونه، زمانی که فایروال همراه‌اول فعال است، فایروال زیرساخت تحت‌الشعاع آن قرار می‌گیرد؛ ازاین‌رو اگر یک آدرس IP در شبکه ی همراه‌اول مسدود شود، ممکن است به‌طور هم‌زمان در زیرساخت مسدود نباشد. پس از گذشت مدتی (بر اساس یک "الگوی زمانی" که در این گزارش توضیح داده می‌شود)، پایگاه داده فهرست سیاه با شرکت زیرساخت همگام‌سازی شده و آدرس مذکور در تمامی ISPها مسدود می‌شود.

اینترنت پژوهشگاه دانش‌های بنیادی ایران (AS6736) دسترسی به اینترنت بدون محدودیت‌های فایروال اصلی (AS49666) را دارد. این سازمان یکی از قدیمی‌ترین نهادهاست و در ابتدا برای افراد برگزیده، مقامات دولتی و پژوهشگران تأییدشده تأسیس شده بود. علاوه بر این، IPM محدودیت‌های شدیدی بر پهنای باند اعمال می‌کند که معمولاً در حد ۱۰/۱۰۰ مگابیت بر ثانیه است.[۱۶][۱۷]




(دیاگرام ۱ – فایروال‌ها و ASهای اصلی) - [لینک]

# وضعیت DNS

IRGFW
irgfw.report

## وضعیت DNS

در ایران، درخواست‌های DNS زیر نظر بازرسی عمیق بسته (DPI) قرار دارند و در نتیجه، Poisoning و اختلال در کوئری‌های DNS به دفعات رخ می‌دهد. درخواست‌هایی که به ارائه‌دهندگان مشهور DNS ارسال می‌شوند، بدون توجه به روش رمزگذاری (شامل DNS بر بستر UDP یا DoU، DNS بر بستر TLS یا DoT، DNS بر بستر HTTPS یا DoH، و DNS بر بستر QUIC یا DoQ) همواره در فهرست خاکستری قرار می‌گیرند. این مشکل چنان گسترده است که در بسیاری موارد، برای ارتباطات داخلی (محلی) به‌ویژه آن‌هایی که از مسیر IRGFW عبور می‌کنند، ناچار به اتکا بر سرورهای DNS ارائه‌شده توسط ISP هستیم.[۲۵]

با این حال، کاربران می‌توانند با راه‌اندازی سرورهای DNS شخصی خود که از پروتکل‌های رمزگذاری‌شده (DoT، DoH یا DoQ) استفاده می‌کنند، این اختلالات را تا حدی کاهش دهند. اما این راهکار دو چالش اساسی به‌همراه دارد:

- **خاکستری شدن نشانی IP مقصد:** اگر نشانی IP مقصد در فهرست خاکستری قرار گیرد، فرایند هندشیک TLS ممکن است شکست بخورد و امکان برقراری اتصال DoT و DoH از بین برود.
- **استفاده از DoQ:** اگر ترافیک UDP به نشانی IP مقصد مجاز باشد، می‌توان از DoQ برای غلبه بر محدودیت‌های مربوط به هندشیک TLS بهره گرفت و علیرغم مداخله DPI، همچنان از یک سازوکار امن برای دریافت پاسخ‌های DNS استفاده کرد.

این چالش‌ها بر نیاز به تکنیک‌های پیشرفته مدیریت DNS تأکید می‌کنند؛ تکنیک‌هایی که هم بهره‌گیری از پروتکل‌های رمزگذاری‌شده DNS را پوشش داده و هم پیچیدگی‌های ناشی از DPI و خاکستری‌سازی (Graylisting) را در نظر بگیرند.

# وضعیت DNS

## DNS مبتنی بر HTTPS (DoH)

در این نمونه، یک سرور DoH با نشانی IP سفید و یک دامنه SNI پیکربندی شده است. سرور برای دریافت درخواست‌های DoH روی هر دو پورت ۴۴۳ و ۸۴۴۳ گوش می‌دهد. Nginx نقش وب‌سرور را برای ترافیک عمومی HTTP/HTTPS ایفا می‌کند. هر دو پورت از طریق مرورگر معمولی قابل دسترسی هستند و وب‌سایت مرتبط بدون مشکل بارگذاری می‌شود. با این حال، هنگام استفاده از یک DNS Client (مثل YogaDNS)، درخواست‌های DoH مسدود می‌شوند. به طور مشخص، پیام‌های ClientHello با موفقیت به سرور ارسال می‌شوند، اما هیچ ServerHello دریافت نمی‌شود. این امر باعث می‌گردد اتصال DoH با گذشت زمان بی‌پاسخ بماند. چنین رفتاری نشان می‌دهد یک سازوکار فیلترینگ، هندشیک DoH را مختل کرده و مانع از حل صحیح کوئری‌های DNS بر بستر HTTPS می‌شود.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 6305 | 50.35 | .55 | 10.10.2.205 | TLSv1.3 | 489 | Application Data, Application Data, Application Data |
| 6308 | 50.35 | 10.10.2.205 | .55 | TLSv1.3 | 118 | Change Cipher Spec, Application Data |
| 6312 | 50.52 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6315 | 50.59 | .55 | 10.10.2.205 | TLSv1.3 | 212 | Application Data, Application Data |
| 6316 | 50.59 | .55 | 10.10.2.205 | TLSv1.3 | 626 | Application Data, Application Data |
| 6317 | 50.59 | .55 | 10.10.2.205 | TLSv1.3 | 212 | Application Data, Application Data |
| 6325 | 50.83 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6327 | 50.85 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6329 | 50.86 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6330 | 50.86 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6333 | 50.87 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6335 | 50.87 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6351 | 51.02 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 341 | Client Hello (SNI=d o) |
| 6366 | 51.49 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6371 | 51.59 | .55 | 10.10.2.205 | TLSv1.3 | 78 | Application Data |
| 6378 | 51.66 | 10.10.2.205 | .55 | TLSv1.3 | 286 | Application Data |
| 6379 | 51.66 | 10.10.2.205 | .55 | TLSv1.3 | 93 | Application Data |
| 6384 | 51.75 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6386 | 51.76 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6402 | 51.90 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6403 | 51.90 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6406 | 51.90 | .55 | 10.10.2.205 | TLSv1.3 | 110 | Application Data |
| 6412 | 51.91 | .55 | 10.10.2.205 | TLSv1.3 | 763 | Application Data, Application Data |
| 6417 | 51.98 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6423 | 52.00 | 10.10.2.205 | .55 | TLSv1.3 | 431 | Client Hello (SNI=browserleaks.com) |
| 6430 | 52.00 | 10.10.2.205 | 138.197.54.100 | TLSv1.3 | 324 | Client Hello (SNI=tls.browserleaks.com) |
| 6434 | 52.00 | 10.10.2.205 | 199.5.26.160 | TLSv1.3 | 413 | Client Hello (SNI=rdap.arin.net) |
| 6437 | 52.00 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6439 | 52.02 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6444 | 52.03 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6446 | 52.04 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6449 | 52.07 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6454 | 52.10 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6456 | 52.11 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6459 | 52.13 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6462 | 52.14 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |
| 6464 | 52.16 | 193.149.129.145 | 10.10.2.205 | TLSv1.2 | 85 | Encrypted Alert |

```
▸ Frame 6351: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface \Device\NPF_{D1983690-D354-4E6A-A86D-D41216983DB2}, id 0
▸ Ethernet II, Src: Intel :88), Dst: 2c)
▸ Internet Protocol Version 4, Src: 10.10.2.205, Dst: 193.149.129.145
▸ Transmission Control Protocol, Src Port: 60203, Dst Port: 8443, Seq: 1, Ack: 1, Len: 287
▾ Transport Layer Security
  ▾ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 282
    ▸ Handshake Protocol: Client Hello
```

(عکس ۱ – DOH)
[اینک]

# وضعیت DNS

## DNS مبتنی بر TLS (DoT)

در این سناریو، یک سرور DoT را پیکربندی می‌کنیم تا روی پورت ۸۵۳ به درخواست‌ها گوش دهد. این سرور همچنین از DoQ پشتیبانی می‌کند. یک درخواست DoT به سرور فرستاده می‌شود؛ اما همانند سناریوی DoH پیشین، هندشیک TLS شکست می‌خورد. درحالی‌که پیام‌های ClientHello با موفقیت به سرور ارسال می‌شوند، هیچ ServerHelloای دریافت نمی‌شود و در نتیجه اتصال با گذشت زمان بی‌پاسخ می‌ماند. این وضعیت نشان می‌دهد که گفت‌وگوی TLS مسدود یا مختل شده و برقراری اتصال امن برای حل پرسش‌های DNS بر بستر TLS انجام نمی‌گیرد.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1124 | 22.01 | 10.10.2.205 | 138.197.54.100 | TLSv1.3 | 118 | Change Cipher Spec, Application Data |
| 1125 | 22.01 | 10.10.2.205 | 138.197.54.100 | TLSv1.3 | 146 | Application Data |
| 1126 | 22.01 | 10.10.2.205 | 138.197.54.100 | TLSv1.3 | 474 | Application Data |
| 1130 | 22.09 | 199.5.26.160 | 10.10.2.205 | TLSv1.3 | 1514 | Server Hello, Change Cipher Spec, Application Data |
| 1133 | 22.09 | 199.5.26.160 | 10.10.2.205 | TLSv1.3 | 1514 | Application Data, Application Data |
| 1134 | 22.09 | 199.5.26.160 | 10.10.2.205 | TLSv1.3 | 104 | Application Data |
| 1136 | 22.09 | 10.10.2.205 | 199.5.26.160 | TLSv1.3 | 118 | Change Cipher Spec, Application Data |
| 1137 | 22.09 | 10.10.2.205 | 199.5.26.160 | TLSv1.3 | 672 | Application Data |
| 1142 | 22.25 | 104.236.69.55 | 10.10.2.205 | TLSv1.3 | 195 | Application Data, Application Data |
| 1143 | 22.25 | 10.10.2.205 | 104.236.69.55 | TLSv1.3 | 85 | Application Data |
| 1149 | 22.25 | 138.197.54.100 | 10.10.2.205 | TLSv1.3 | 576 | Application Data, Application Data, Application Data, Application Data |
| 1150 | 22.25 | 10.10.2.205 | 138.197.54.100 | TLSv1.3 | 85 | Application Data |
| 1170 | 22.27 | 104.236.69.55 | 10.10.2.205 | TLSv1.3 | 78 | Application Data |
| 1208 | 22.31 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1210 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1213 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1218 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1222 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1229 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1230 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1247 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1248 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1249 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1250 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1251 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1258 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1259 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1260 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1261 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1262 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1264 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1273 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1274 | 22.32 | 10.10.2.205 | 193.149.129.145 | TLSv1.2 | 240 | Client Hello (SNI=d[redacted]o) |
| 1282 | 22.34 | 104.236.69.55 | 10.10.2.205 | TLSv1.3 | 85 | Application Data |
| 1283 | 22.37 | 104.236.69.55 | 10.10.2.205 | TLSv1.3 | 341 | Application Data |
| 1314 | 22.52 | 199.5.26.160 | 10.10.2.205 | TLSv1.3 | 1356 | Application Data |
| 1351 | 22.73 | 199.5.26.160 | 10.10.2.205 | TLSv1.3 | 938 | Application Data |

```
▸ Frame 1208: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface \Device\NPF_{D1983690-D354-4E6A-A86D-D41216983DB2}, id 0
▸ Ethernet II, Src: Intel[redacted]88), Dst: [redacted]2c)
▸ Internet Protocol Version 4, Src: 10.10.2.205, Dst: 193.149.129.145
▸ Transmission Control Protocol, Src Port: 59915, Dst Port: 853, Seq: 1, Ack: 1, Len: 186
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 181
    ▸ Handshake Protocol: Client Hello
```

(عکس ۲ – DoT)
[لینک]

# وضعیت DNS

### DNS مبتنی بر QUIC (DoQ)

در این حالت، درخواست‌های DoQ با بهره‌گیری از پروتکل DTLS ارسال می‌شوند، پروتکلی که بر بستر UDP کار می‌کند اما رمزگذاری مشابه TLS را فراهم می‌نماید. از آنجاکه این درخواست‌های DoQ در درون DTLS نهفته‌اند، از سد پالایش‌های معمول IRGFW می‌گذرند، زیرا فایروال هنوز این اثرانگشت DTLS را از این فرستنده نشناخته است. بدین‌ترتیب، ارتباط بدون هیچ اخلالی برقرار شده و کوئری‌های DNS از طریق QUIC بدون مزاحمت پاسخ داده می‌شوند.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 18 | 1.22 | 10.10.2.205 | 193.149.129.145 | DTLS | 103 | Continuation Data |
| 19 | 1.22 | 10.10.2.205 | 193.149.129.145 | DTLS | 103 | Continuation Data |
| 24 | 1.39 | 193.149.129.145 | 10.10.2.205 | DTLS | 84 | Continuation Data |
| 25 | 1.40 | 193.149.129.145 | 10.10.2.205 | DTLS | 132 | Continuation Data |
| 26 | 1.40 | 10.10.2.205 | 193.149.129.145 | DTLS | 73 | Continuation Data |
| 27 | 1.40 | 193.149.129.145 | 10.10.2.205 | DTLS | 173 | Continuation Data |
| 28 | 1.40 | 10.10.2.205 | 193.149.129.145 | DTLS | 79 | Continuation Data |
| 35 | 1.57 | 193.149.129.145 | 10.10.2.205 | DTLS | 94 | Continuation Data |
| 36 | 1.60 | 10.10.2.205 | 193.149.129.145 | DTLS | 71 | Continuation Data |
| 746 | 10.55 | 193.149.129.145 | 10.10.2.205 | DTLS | 139 | Continuation Data |
| 747 | 10.55 | 10.10.2.205 | 193.149.129.145 | DTLS | 73 | Continuation Data |

```
▸ Frame 18: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{D1983690-D354-4E6A-A8
▸ Ethernet II, Src: Intel                                  88), Dst:                                  2c)
▸ Internet Protocol Version 4, Src: 10.10.2.205, Dst: 193.149.129.145
▾ User Datagram Protocol, Src Port: 54929, Dst Port: 853
    Source Port: 54929
    Destination Port: 853
    Length: 69
    Checksum: 0x5054 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (61 bytes)
▾ Datagram Transport Layer Security
    DTLS Record Layer: unrecognized content type 0x53
```

(عکس ۳ – DoQ)
[لینک]

# وضعیت UDP

## وضعیت UDP

در ابتدا باید میان UDP عادی و UDP ناشناس (ناشناخته) تمایز قائل شویم. UDP عادی یا کلی، دارای شناسه‌ها و الگوهای قابل تشخیص (Fingerprint) است؛ برای مثال تماس‌های تصویری در اسکایپ، زوم و فیس‌تایم بر پایه UDP شناخته‌شده صورت می‌گیرند. همچنین، فرآیند هندشیک در وایرگارد به‌صورت عادی بر مبنای UDP شناخته‌شده است، ازاین‌رو به‌راحتی قابل شناسایی و اثرانگشت‌برداری (Fingerprinting) است.[۱۸][۱۹]

از سوی دیگر، UDP ناشناس به UDPهایی گفته می‌شود که در فرآیند هندشیک یا ترافیک، فوراً قابل تشخیص نبوده و توسط ابزارهای پایش و امنیت شبکه به یک برنامه یا ترافیک شناخته‌شده منتسب نمی‌شوند. چنین ترافیکی عموماً فاقد امضاهای مشخص جهت شناسایی است و بنابراین تشخیص هدف یا منبع آن دشوار می‌شود.

### ویژگی‌های UDP ناشناس:

- **ابهام‌سازی:** برای پنهان‌سازی ماهیت واقعی ترافیک استفاده می‌شود، و در خدمات VPN نظیر وایرگارد مبهم‌شده (Obfuscated Wireguard) متداول است.
- **پروتکل‌های اختصاصی:** برنامه‌های سفارشی که از روش‌های ارتباطی خاص و غیرعمومی استفاده می‌کنند.
- **رمزنگاری:** ترافیک رمزگذاری‌شده ممکن است با الگوهای شناخته‌شده هم‌خوانی نداشته باشد. این حالت معمولاً در برنامه‌های P2P و ابزارهای امنیتی مشاهده می‌شود.

## وضعیت UDP

در فایروال ایران، هندشیک وایرگارد به نشانی‌های IP خارجی غالباً توسط فایروال ایران با دراپ کردن بسته‌های UDP مسدود می‌شود، زیرا زمانی که این فایروال هندشیک استاندارد وایرگارد را تشخیص می‌دهد، اقدام به مسدودسازی می‌نماید.[۲۰] در برخی موارد نیز محدودسازی نرخ (Rate Limiting) به‌کار گرفته می‌شود تا کارایی چنین اتصالاتی کاهش یابد. این سازوکار مسدودسازی را می‌توان با افزودن نویز یا شبیه‌سازی هندشیک‌های دیگر (یا ارسال بایت‌های شناخته‌شده‌ی سایر پروتکل‌ها) پیش از هندشیک اصلی وایرگارد دور زد. به نظر می‌رسد IRGFW بیشتر بر شناسایی الگوهای بایت خاص در دست‌دهی متکی است تا بهره‌گیری از عبارات منظم پیچیده (Regex) یا روش‌های عمیق بازرسی، و این امر ممکن است با ابهام‌سازی (Obfuscation) برای اجتناب از تشخیص، قابل بهره‌برداری باشد.

به نظر می‌رسد IRGFW تا سقف حدود ۱۷ کیلوبایت از ترافیک (UDP و TCP) را برای هر ترکیب IP:Port بافر کرده و مورد بازرسی عمیق بسته (DPI) قرار می‌دهد تا الگوهای مربوط به وایرگارد را شناسایی کند. پس از این حجم، ترافیک بیشتر تحت بازرسی قرار نمی‌گیرد. مکانیسم مسدودسازی ظاهراً بیشتر بر پورت‌های بالای ۱۰۲۴ متمرکز است، در حالی که پورت‌های پرکاربرد نظیر ۴۴۳ عموماً تأثیری نمی‌پذیرند. این تمرکز بر پورت‌های بالا، پیکربندی‌های معمول وایرگارد را در برابر بازرسی آسیب‌پذیرتر می‌سازد.

اگرچه UDP ذاتاً بدون حالت (Stateless) است، اما فایروال‌ها اغلب برای ترافیک UDP حالتی موقتی شبیه اتصال ایجاد می‌کنند. برای نمونه، آن‌ها بسته‌ها را با یک جفت IP:Port مرتبط کرده و برای مدت محدودی (معمولاً حدود پنج ثانیه) آن را به‌عنوان یک شبه-سشن (Pseudo-Session) در نظر می‌گیرند. این حالت موقت به فایروال امکان می‌دهد چندین بسته در یک جریان را پایش کرده و الگوهایی نظیر هندشیک‌های وایرگارد را شناسایی کند.

یکی از راهکارهای احتمالی برای کاهش احتمال شناسایی، استفاده از جابه‌جایی پورت در بازه‌های زمانی متغیر (Variable-Interval Port Hopping) [۲۱] است که در آن پورت اتصال در فواصل زمانی تصادفی تغییر می‌کند. این روش با ایجاد پیش‌بینی‌ناپذیری در الگوهای ترافیک، امکان اثرانگشت‌برداری را کاهش می‌دهد. علاوه بر این، تغییر پویا در الگوهای هندشیک و ابهام‌سازی Payloadها می‌تواند توانایی فایروال در شناسایی و مسدودسازی ترافیک وایرگارد را بیش از پیش مختل کند.

به مرور زمان، فایروال ایران ظاهراً با شناسایی و مسدودسازی الگوهای خاص هندشیک، به‌ویژه در مواردی که ترافیک تکراری بین محدوده‌های IP یا مراکز داده مشخص دیده می‌شود، سازگار می‌گردد. این رفتار نشان می‌دهد فایروال می‌تواند الگوهای تکراری را بیاموزد و به آن‌ها پاسخ دهد. این مشاهدات بر لزوم آزمایش مداوم روش‌های ابهام‌سازی و رفتارهای تصادفی در ترافیک برای حفظ اتصال قابل اعتماد و پیشی گرفتن از قابلیت‌های در حال تحول فایروال دلالت دارد.

## وضعیت UDP

در این شرایط می‌بینیم که یک WireGuard handshake استاندارد، به‌صورت پیوسته توسط IRGFW در سطح بسته (Packet level) مسدود می‌شود، و این رخداد در بازه‌های زمانی پنج ثانیه‌ای تکرار می‌گردد. گفتنی است این فاصله پنج ثانیه‌ای بخشی از سازوکار KeepAlive نیست، چرا که در این پیکربندی غیرفعال شده است.

با وجود بسته شدن هدفمند WireGuard handshake، هیچ پیام خطای ICMP دیده نمی‌شود و IP مقصد همچنان به درخواست‌های Ping پاسخ مناسب می‌دهد. این رفتار نشان می‌دهد، هرچند فایروال ایران بسته‌های WireGuard handshake را جدا کرده و پالایش می‌کند، اما در کارکرد کلی ترافیک عمومی شبکه مانند ICMP دخالت نکرده است.

| No. | Time | Source | Destination | Protocol | Length | Info | Dest Port |
|---|---|---|---|---|---|---|---|
| 7657 | 9.33 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xAB8758DE | 54571 |
| 8523 | 14.33 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xF55CBEA3 | 54571 |
| 9241 | 19.33 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xD2F7CD1F | 54571 |
| 12590 | 24.34 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xB11AB00C | 54571 |
| 13709 | 29.34 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xB40F9646 | 54571 |
| 17883 | 34.34 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xE3F156D5 | 54571 |
| 21228 | 39.34 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0x352C1132 | 54571 |
| 22784 | 44.34 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0x410EF8D6 | 54571 |
| 26031 | 49.34 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xD8D20074 | 54571 |
| 28588 | 54.34 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0xBF418730 | 54571 |
| 30795 | 59.35 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0x1A46B998 | 54571 |
| 32225 | 64.35 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0x35928FC8 | 54571 |
| 35004 | 69.35 | 62. | 45.138 | WireGuard | 190 | Handshake Initiation, sender=0x9E962A9A | 54571 |

(عکس ۴ – وایرگارد ساده)
[لینک]

## وضعیت UDP

در این بررسی موردی، مشاهده می‌کنیم که یک فایروال به‌طور فعال هم WireGuard handshake و هم ارتباط ICMP به نشانی IP مقصد را مسدود می‌کند.

در ابتدای کار، شمار اندکی junk و noise packets ارسال می‌کنیم تا پیش از آغاز WireGuard handshake، جریان ترافیک را تغییر دهیم. این پکت‌ها تا حدود شماره ۹۴۷۲ در بافر فایروال انباشته می‌شوند، بی‌آن‌که پاسخی برانگیزند. پس از آن، یک QUIC handshake را آغاز می‌کنیم که با ارسال همانند noise و junk پیش ازهندشیک اصلی، توانسته از بافر فایروال عبور کند. این رفتار نشان می‌دهد که فایروال، ترافیک WireGuard را به شکلی متفاوت از QUIC بررسی و پردازش می‌کند.

نکته مهم این است که زمانی که فایروال، هندشیک وایرگارد را مسدود می‌کند، همزمان ICMP (ping) به نشانی IP مقصد نیز بسته می‌شود. این اقدام هم‌زمان نمایانگر سیاست سخت‌گیرانه فایروال است که هم VPN handshake و هم ترافیک ICMP را مختل می‌کند.

نکته دیگر اینکه تست ICMP connectivity در اینجا از پروتکل وایرگارد و مکانیزم KeepAlive مستقل است. در عوض، یک برنامه جداگانه برای آزمون ارتباط ICMP به کار گرفته می‌شود (گرچه در Wireshark پیام Port unreachable دیده می‌شود، اما در دستور ping معمولی منجر به timeout می‌گردد). این جداسازی، رفتار فایروال را در قبال ترافیک ICMP در کنار هندشیک VPN به‌روشنی نمایان می‌کند.

| No. | Time | Source | Destination | Protocol | Length | Info | Dest Port |
|---|---|---|---|---|---|---|---|
| 4163 | 3.33 | 45. | 6 | WireGuard | 190 | Handshake Initiation, sender=0xF787EFB4 | 58040 |
| 4164 | 3.33 | 6 | 45 | ICMP | 218 | Destination unreachable (Port unreachable) | |
| 6152 | 8.44 | | 6 | WireGuard | 190 | Handshake Initiation, sender=0xD1BB7F12 | 58040 |
| 6153 | 8.44 | 6 | 45 | ICMP | 218 | Destination unreachable (Port unreachable) | |
| 6875 | 13.68 | | 6 | WireGuard | 190 | Handshake Initiation, sender=0xD373E425 | 58040 |
| 6876 | 13.68 | 6 | 45 | ICMP | 218 | Destination unreachable (Port unreachable) | |
| 7630 | 18.90 | | 6 | WireGuard | 190 | Handshake Initiation, sender=0x585838EB | 58040 |
| 7631 | 18.90 | 6 | 45 | ICMP | 218 | Destination unreachable (Port unreachable) | |
| 8653 | 24.22 | | 6 | WireGuard | 190 | Handshake Initiation, sender=0xF8CBB029 | 58040 |
| 8654 | 24.22 | 6 | 45 | ICMP | 218 | Destination unreachable (Port unreachable) | |
| 9472 | 27.40 | 6 | 45 | QUIC | 65 | Handshake, DCID=c55c844ce8700531[Malformed Packet] | 35197 |
| 9474 | 27.41 | 6 | 45 | QUIC | 65 | Handshake, DCID=c55c844ce8700531[Malformed Packet] | 35197 |
| 9476 | 27.41 | 6 | 45 | QUIC | 67 | Protected Payload (KP0) | 35197 |
| 9478 | 27.42 | 6 | 45 | QUIC | 67 | Protected Payload (KP0) | 35197 |
| 9479 | 27.43 | 6 | 45 | QUIC | 69 | Protected Payload (KP0) | 35197 |
| 9481 | 27.44 | 6 | 45 | QUIC | 70 | Protected Payload (KP0) | 35197 |
| 9482 | 27.44 | 6 | 45 | QUIC | 65 | Handshake, DCID=b6d42c6c7177df70[Malformed Packet] | 35197 |
| 9484 | 27.44 | 6 | 45 | QUIC | 68 | Protected Payload (KP0) | 35197 |
| 9485 | 27.44 | 6 | 45 | QUIC | 65 | Handshake, DCID=c55c844ce8700531[Malformed Packet] | 35197 |
| 9486 | 27.44 | 6 | 45 | QUIC | 65 | Handshake, DCID=c55c844ce8700531[Malformed Packet] | 35197 |
| 9487 | 27.44 | 6 | 45 | QUIC | 69 | Protected Payload (KP0) | 35197 |

(عکس ۵ – وایرگارد ویرایش شده)
[لینک]

## وضعیت QUIC

در فایروال ایران، پیاده‌سازی و بهره‌گیری از پروتکل‌های QUIC و HTTP/3 با دشواری‌های چشمگیری مواجه است که عمدتاً ناشی از سیاست‌های سخت‌گیرانه فیلترینگ حکومتی است. هرچند HTTP/3 تا حدی مورد استفاده قرار گرفته، عملکرد آن به‌طور چشمگیری کاهش یافته و در نتیجه، سرعت آن حتی از HTTP/2 هم کمتر می‌شود. هندشیک و ترافیک QUIC به بسیاری از مراکز داده خارجی اغلب مسدود می‌شود، و این موضوع بر اساس محدوده‌های گوناگون IP خارجی، تأثیرات ناپایدار و متفاوتی بر کارایی دارد.

کاربرانی که می‌کوشند با بهره‌گیری از ابزارهای تانلینگ مبتنی بر QUIC از این محدودیت‌ها عبور کنند، با موفقیت‌های متغیری روبه‌رو هستند، چرا که کارآمدی این ابزارها به‌طور چشمگیری به نشانی‌های IP خارجی مورد دسترسی وابسته است. از این رو، اگرچه گاه این ابزارها می‌توانند اتصال سریع‌تر و ایمن‌تری فراهم کنند، میزان اطمینان‌پذیری آن‌ها تا حد زیادی تابع رفتار نامنظم و همه‌جانبه فیلترینگ در ایران است.[۲۲]

افزون بر این محدودیت‌ها، مشاهده شده که ترافیک QUIC به برخی از محدوده‌های IP خارجی در همان مرکز داده ممکن است به‌صورت گزینشی مسدود شود. در حالی که برخی IPها همچنان در دسترس می‌مانند، دسترسی به دیگر IPها کاملاً محدود می‌شود.[۲۳] به‌نظر می‌رسد این فیلترینگ به‌ویژه روی هندشیک‌های QUIC متمرکز است، به‌طوری که الگوی بایت‌های خاص پس از تکرار شناسایی و مسدود می‌شوند. برای نمونه، تکرار مداوم هندشیک QUIC از نشانی‌های IP ایرانی به یک IP خارجی مشخص می‌تواند به مسدودسازی کامل آن اتصال منجر شود. این سازوکار فیلترینگ همچنین قادر است با شناسایی ترافیک QUIC پرتکرار از IPهای مشخص، پس از رسیدن به یک آستانه حجم ترافیک یا تکرار الگوها، آن را مسدود کند. علاوه بر این، اخیراً ترافیک QUIC به Cloudflare به‌طور محسوسی کاهش یافته است، که احتمالاً نشانگر محدودیت‌های هدفمندتر علیه استفاده گسترده از آن است.[۲۴]

برای رویارویی با این چالش‌ها، ابزارهای مبتنی بر QUIC ناچارند سازوکارهایی برای ابهام‌سازی (Obfuscation) پویا در هندشیک و ترافیک خود پیاده کنند تا از شناسایی توسط سیستم‌های DPI ج.ا. ایران بگریزند. تغییر الگوهای هندشیک یا افزودن تصادفی‌سازی به جریان ترافیک QUIC ممکن است کارایی آن‌ها را در مواجهه با این محدودیت‌ها بهبود بخشد.

## وضعیت QUIC

در این سناریو، ما اتصال به یک دامنه با یک نشانی IP مشخص را آزمایش کردیم که در آن ترافیک UDP و QUIC بدون محدودیت است. فرایند هندشیک در Wireshark بررسی شد و توالی زیر تأیید گردید:

1. ClientHello از سوی کاربر فرستاده شد.
2. ServerHello دریافت شد و هندشیک QUIC کامل شد.
3. تبادل Payload در لایه کاربرد بدون هیچگونه وقفه با موفقیت انجام پذیرفت.

سرور هدف از Nginx با پشتیبانی پیش‌فرض از HTTP/3 (QUIC) بهره می‌برد. برای اعتبارسنجی اتصال و ثبات دست‌دهی، از curl با HTTP/3 و Hysteria2 استفاده شد. نتایج نشان دادند که این دامنه و IP برای ترافیک QUIC کاملاً فعال بوده و هیچ نشانه‌ای از فیلترینگ یا کاهش سرعت مشاهده نشد.

| No. | Time | Source | Destination | Protocol | Length | Info | JA4 | JA4S |
|---|---|---|---|---|---|---|---|---|
| 363 | 3.83 | 45. | 172. | QUIC | 1322 | Initial, DCID=54ab8b284029b88aed96, PKN: 0, PADDING, CRYPTO | q13d0312h3_55b375c5d22e_c183556c78e2 | |
| 364 | 3.84 | 172. | 45. | QUIC | 1322 | Handshake, SCID=e5165363 | | q130200_ |
| 365 | 3.84 | 172. | 45. | QUIC | 1322 | Handshake, SCID=e5165363 | | |
| 366 | 3.84 | 172. | 45. | QUIC | 438 | Protected Payload (KP0) | | |
| 367 | 3.84 | 45. | 172. | QUIC | 1322 | Initial, DCID=e5165363, PKN: 1, ACK, PADDING | | |
| 368 | 3.84 | 45. | 172. | QUIC | 78 | Handshake, DCID=e5165363 | | |
| 372 | 3.86 | 45. | 172. | QUIC | 142 | Protected Payload (KP0) | | |
| 373 | 3.86 | 45. | 172. | QUIC | 71 | Protected Payload (KP0) | | |
| 374 | 3.86 | 45. | 172. | QUIC | 70 | Protected Payload (KP0) | | |

```
Frame 364: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits) on interface \Device\NPF_{2CE02A2F-39F1-4BC1-8F27-59A425D4B279}, id 0
Ethernet II, Src: [redacted]08), Dst: [redacted]99)
Internet Protocol Version 4, Src: 172.[redacted], Dst: 45.[redacted]
User Datagram Protocol, Src Port: 20000, Dst Port: 60062
QUIC IETF
  QUIC Connection information
  [Packet Length: 131]
  1... .... = Header Form: Long Header (1)
  .1.. .... = Fixed Bit: True
  ..00 .... = Packet Type: Initial (0)
  [.... 00.. = Reserved: 0]
  [.... ..01 = Packet Number Length: 2 bytes (1)]
  Version: 1 (0x00000001)
  Destination Connection ID Length: 0
  Source Connection ID Length: 4
  Source Connection ID: e5165363
  Token Length: 0
  Length: 117
  [Packet Number: 0]
  Payload: ceae4c6a8a0cdcb2575ec174d78b1af195d7ee4a9cbe3101b7907cd8fe84fdce05a52cc1e425133d2673389b1d57b0cd432121d9c408a7d0a58d5db7f64e3966d3b32e3f0c8ca6173bca32cb26d0999685581b94f6a
  ACK
  CRYPTO
    Frame Type: CRYPTO (0x0000000000000006)
    Offset: 0
    Length: 90
    Crypto Data
    TLSv1.3 Record Layer: Handshake Protocol: Server Hello
QUIC IETF
```

(عکس ۶ – هندشیک QUIC نرمال)
[اینک]

## وضعیت QUIC

در این سناریوی خاص، می‌توان با یک Wireguard مبهم‌شده به نشانی IP مقصد متصل شد، که نشان می‌دهد ترافیک UDP به این IP مسدود نیست. سپس تلاش می‌کنیم یک هندشیک QUIC را با یک دامنه سفید در فایروال ایران آغاز کنیم. با وجود اینکه ترافیک UDP موفقیت‌آمیز به مقصد می‌رسد، هندشیک QUIC به سرانجام نمی‌رسد.

با تحلیل ترافیک در Wireshark، مشاهده می‌کنیم که کلاینت یک ClientHello ارسال می‌کند. اما تمامی ClientHelloهای بعدی در واقع ارسال مجدد هستند، که نشان می‌دهد کلاینت پاسخی از سرور دریافت نمی‌کند. هیچ ServerHello مشاهده یا دریافت نمی‌شود، و این موضوع تأیید می‌کند که هندشیک پس از نخستین ارسال از سمت کلاینت مختل می‌گردد.

این الگو بر وجود یک سازوکار فیلترینگ دلالت دارد که اگرچه اجازه عبور بسته‌های UDP را می‌دهد، اما هندشیک QUIC را در سطح پروتکل مسدود می‌کند. چنین رفتار هدفمندی نشان‌دهنده پیچیدگی سامانه فیلترینگ است و بر نیاز به فنون ابهام‌سازی پیشرفته برای دور زدن این محدودیت‌ها تأکید می‌کند. با این حال، هنگام آزمایش با یک دامنه غیرمسدود، این مسدودسازی همچنان ادامه می‌یابد.

| No. | Time | Source | Destination | Protocol | Length | Info | JA4 |
|---|---|---|---|---|---|---|---|
| 9354 | 4.32 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 0, PADDING, CRYPTO | q13d0312h3_55b375c5d22e_c183556c78e |
| 9381 | 4.52 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 1, PADDING, CRYPTO | |
| 9382 | 4.52 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 2, PADDING, CRYPTO | |
| 10095 | 4.93 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 3, PADDING, CRYPTO | |
| 10096 | 4.93 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 4, PADDING, CRYPTO | |
| 11007 | 5.73 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 5, PADDING, CRYPTO | |
| 11008 | 5.73 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 6, PADDING, CRYPTO | |
| 11544 | 7.33 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 7, PADDING, CRYPTO | |
| 11545 | 7.33 | 6 | 172.232.44.81 | QUIC | 1322 | Initial, DCID=62b0b3c512a1a4601e9b1b0a00575d, PKN: 8, PADDING, CRYPTO | |

```
▸ Frame 9354: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits) on interface ens192, id 0
▸ Ethernet II, Src: VMware_[redacted]f9), Dst: [redacted]3c)
▸ Internet Protocol Version 4, Src: 6[redacted], Dst: 172.232.44.81
▸ User Datagram Protocol, Src Port: 57951, Dst Port: 20000
▾ QUIC IETF
  ▸ QUIC Connection information
    [Packet Length: 1280]
    1... .... = Header Form: Long Header (1)
    .1.. .... = Fixed Bit: True
    ..00 .... = Packet Type: Initial (0)
    [.... 00.. = Reserved: 0]
    [.... ..01 = Packet Number Length: 2 bytes (1)]
    Version: 1 (0x00000001)
    Destination Connection ID Length: 15
    Destination Connection ID: 62b0b3c512a1a4601e9b1b0a00575d
    Source Connection ID Length: 0
    Token Length: 0
    Length: 1255
    [Packet Number: 0]
    Payload [truncated]: 661240ed17a4ae52719087a84dc55ee0f23ebc7a8a2d1a8dbe64014caf5ce5b6bb78fc19503580398100bc952f3ddeb525da2a6c2058fb50083ffb2b22e4ae18632219b3079fefe78b740c8c395ceef
  ▸ PADDING Length: 958
  ▾ CRYPTO
      Frame Type: CRYPTO (0x0000000000000006)
      Offset: 0
      Length: 275
      Crypto Data
    ▸ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
▸ JA4 Fingerprint
```

(عکس ۷ – هندشیک مسدود شده‌ی QUIC)
[لینک]

# وضعیت آدرس‌های IP

## وضعیت آدرس‌های IP

فایروال ایران سه فهرست دارد: لیست **سفید**، لیست **خاکستری**، لیست **سیاه**. پیشینه یک آدرس IP در این موضوع اهمیت زیادی دارد.

**آی‌پی سفید:** آدرس IP باید از یک مرکز داده نسبتاً ناشناخته باشد. در سه ماه گذشته (یا حتی بیشتر) هیچ‌کس نباید از آن برای VPN یا Proxy استفاده کرده باشد. همچنین این آدرس IP باید به‌صورت دستی در پایگاه‌داده‌های ISP تأیید (Whitelisted) شده باشد. به همین دلیل، گاهی یک آدرس IP بسیار ناشناخته ممکن است سریع‌تر مسدود شود، چون در پایگاه‌داده IRGFW ثبت سفید ندارد.

**آی‌پی خاکستری:** فایروال ایران اکثر آدرس‌های IP را Gray در نظر می‌گیرد، زمانی که گمان می‌رود برای VPN یا Proxy به کار رفته‌اند، اما هنوز شواهد کافی برای مسدودسازی فوری وجود ندارد. این آدرس‌ها که اغلب متعلق به مراکز داده مهم هستند، تحت پایش دوره‌ای ترافیک و گردآوری داده قرار می‌گیرند. این رویکرد معمولاً باعث کاهش سرعت بارگذاری (Upload) و افزایش نوسان (Jitter) می‌شود. در حالت پیش‌فرض، IRGFW یک آدرس IP را به‌صورت خاکستری دسته‌بندی کرده و به‌طور مداوم آن را زیر نظر می‌گیرد و از ترافیک آن نمونه‌برداری می‌کند. بر پایه داده‌های گردآوری‌شده و الگوهای مصرف در طول زمان، IRGFW درباره مسدودسازی دائم آدرس IP تصمیم می‌گیرد.

**آی‌پی سیاه:** پس از تحلیل داده‌های کافی از Gray IPها، IRGFW ممکن است یک آدرس IP را به Black IP ارتقا دهد. در این حالت، مسدودسازی کامل یا نسبی با الگوهای مختلف اعمال می‌شود:

- **شرکت‌های زیرساخت و مخابرات:** این الگوها همه انواع ترافیک به IP را مسدود می‌کنند، شامل ICMP، SSH، TLS(v1.0~v1.3)، HTTP و سایر موارد.
- **همراه‌اول:** زمانی که فایروال فعال است، مرحله ServerHello در هندشیک TLS را مسدود می‌کند و بدین‌ترتیب ارتباط امن مختل می‌شود.
- **ایرانسل:** در این الگو، ترافیک به‌طور نامنظم مسدود می‌شود. گاهی SSH و TLS را هدف می‌گیرد و گاه فقط TLS را.

این روش‌ها بخشی از راهکار همه‌جانبه IRGFW برای مهار و محدودسازی VPNها و Proxyها در داخل کشور هستند.

### وضعیت IPv6

IPv6 هنوز در میان اکثر اپراتورها فراگیر نشده است. هرچند برای کاربران موبایل در شبکه‌هایی مانند همراه‌اول و ایرانسل در دسترس است، به شرط آن‌که کاربر آن را به‌صورت دستی فعال کند. در نشانی‌های IPv6 معمولاً DPI به‌طور پیش‌فرض غیرفعال است، در نتیجه زیر نظر کمتری قرار دارند. با این حال، قوانین پایه‌ای IRGFW، مانند دسته‌بندی آدرس‌ها به لیست‌های سفید، خاکستری و سیاه همچنان اعمال می‌شود، هرچند سخت‌گیری کمتری نسبت به IPv4 دارد.

## الگوی زمانی

ما به برخی الگوها درباره زمان‌بندی مسدودسازی دست یافتیم. زمان هماهنگ‌سازی فایروال اصلی شرکت زیرساخت هر روز از ساعت ۵ تا ٦ بامداد (UTC+03:30) است. هنگامی که می‌گوییم آزمون فایروال شرکت زیرساخت، یعنی شرکت زیرساخت سرورها را تنها در این بازه زمانی مسدود خواهد کرد. اما فایروال همراه اول ممکن است بر پایه الگوی زمانی در نیمروز یک نشانی IP یا دامنه را مسدود کند. منظور از ترافیک "متوسط"، ترافیکی در حد ۱۰۰ مگابیت‌برثانیه بصورت متقارن بر سرور است.

- **الگوی زمانی ۱:** ٤ ساعت - ۱ روز - ٤ روز - ۱ هفته - ٤٠ روز
- **الگوی زمانی ۲:** ۱ ساعت - ٤ ساعت - ۲ روز - ۲ هفته - ٤٠ روز

**الگوی زمانی ۱:** یک سرور پروکسی با Xray-core مانند VLESS-TCP-Reality(Vision) (نوع و ترکیب مهم نیست) راه‌اندازی کنید و ترافیکی در حد متوسط روی آن برقرار کنید. اگر پس از ٤ ساعت مسدود نشد، احتمالاً ۱ روز کار می‌کند (آزمون فایروال شرکت زیرساخت). اگر هنوز مسدود نشده، احتمال دارد ٤ روز کار کند (آزمون دوباره شرکت زیرساخت). اگر باز هم مسدود نشد، احتمال دارد ۱ هفته کار کند (آزمون فایروال همراه اول). اگر از این مرحله هم بگذرد، احتمالاً ٤٠ روز کار می‌کند، اما پس از آن عوامل تصادفی بسیاری درگیر هستند که الگوی مشخصی نیافتیم.

**الگوی زمانی ۲:** یک سرور پروکسی مانند بالا (هر ترکیبی) راه‌اندازی کنید و ترافیکی در حد متوسط روی آن برقرار کنید. اگر پس از ۱ ساعت مسدود نشد، احتمالاً ٤ ساعت کار می‌کند. اگر همچنان مسدود نشد، احتمالاً ۲ روز کار خواهد کرد (آزمون فایروال شرکت زیرساخت). اگر هنوز مسدود نشد، احتمالاً ۲ هفته کار خواهد کرد (آزمون فایروال همراه اول). اگر از این مرحله هم بگذرد، احتمالاً ٤٠ روز کار می‌کند، ولی پس از آن عوامل تصادفی زیادی وجود دارند که الگوی مشخصی یافت نشد.

اگر یک نشانی IP خاکستری شود، هرگز دوباره سفید نخواهد شد. بنابراین، هنگامی که IRGFW سرعت آدرس IP را کاهش می‌دهد، می‌توان گفت آن آدرس خاکستری است و هنگامی که آدرس IP مسدود می‌شود، در فهرست سیاه قرار می‌گیرد. در بیشتر موارد، پس از ٤٠ روز آدرس IP دوباره آزاد می‌شود، ولی اکنون خاکستری به شمار می‌آید و ممکن است محدودیت‌هایی بر سرعت دریافت/ارسال و نوسان بالا داشته باشد. این الگو برای همه محدوده‌های نشانی IP خارجی رخ می‌دهد، به‌ویژه برای مراکز داده و خدمات میزبانی شناخته‌شده که می‌توانند برای سرورهای VPN/Proxy استفاده شوند، یا برای ASهای خیلی ناشناخته که در فهرست‌های سفید پیش‌فرض فایروال‌ها ثبت نشده‌اند.

این فرایند خاکستری‌سازی می‌تواند برای پروتکل‌ها هم به کار رود. همان‌طور که گفته شد، HTTP3/QUIC و UDP به‌صورت پیش‌فرض خاکستری هستند، مگر اینکه اثرانگشت کلاینت (مانند User-Agent در HTTP یا UTLS در ClientHello) با هیچ یک از پایگاه‌داده‌های فایروال هم‌خوانی نداشته باشد و نشانی IP مقصد نیز تاکنون خاکستری نشده باشد.

# کاوشگرهای فعال
# (Active-Probes)

## کاوشگرهای فعال (Active-Probes)

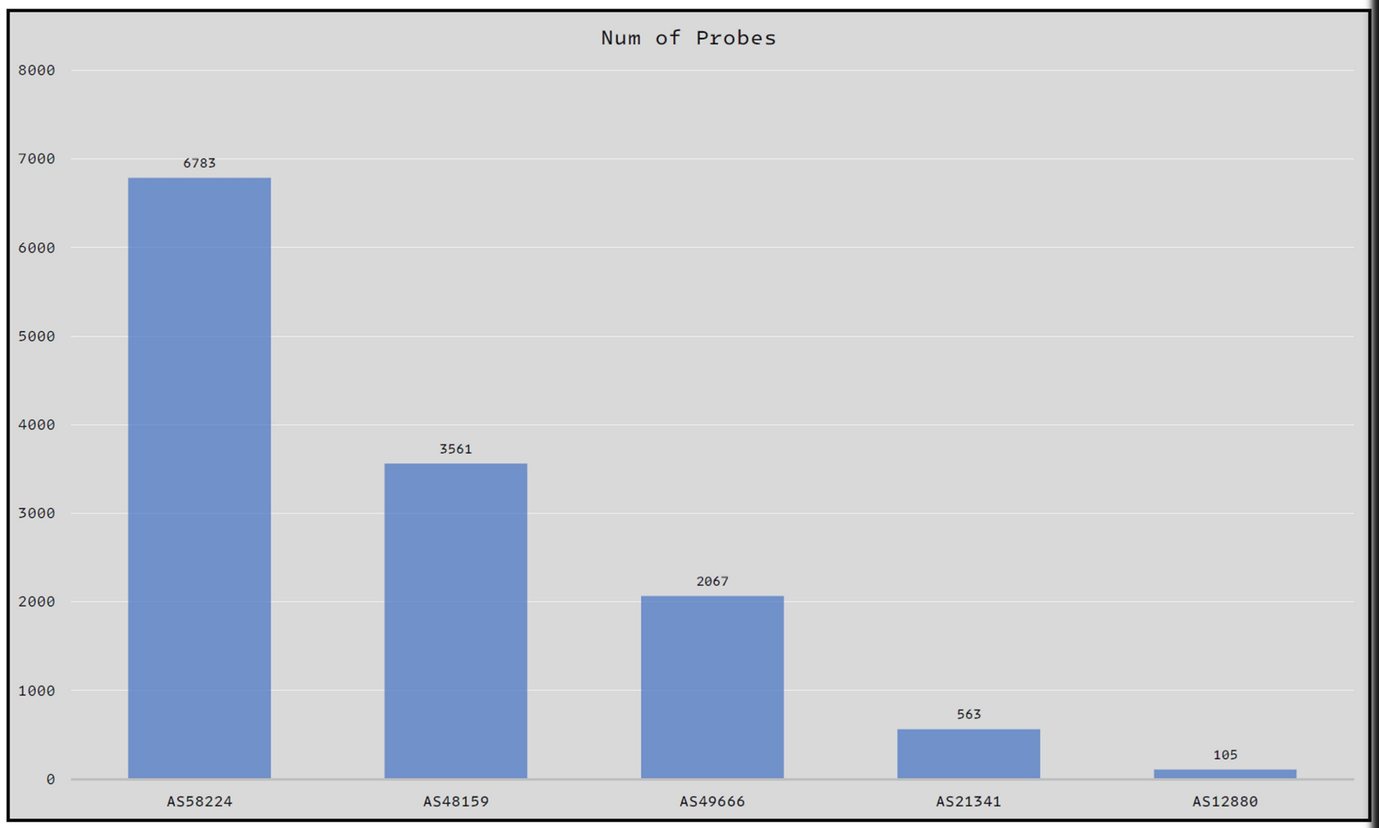
فایروال ایران در شهریورماه ۱۴۰۲ یک سامانه Active-Probing فعال داشت و ما توانستیم تعدادی از آدرس‌های IP مورد استفاده را استخراج کنیم.[۲۶] برخی از سرورهای آزمایشی ما حتی هدف حملات DDoS گوناگون قرار گرفتند که استفاده از CPU سرور را به حداکثر رساند.[۲۷] این آدرس‌های IP در این آزمون‌ها بر روی سرور با بهره‌گیری از Xray-core مدیریت شدند.

اما از اوایل دی‌ماه ۱۴۰۲، فایروال ایران دیگر از Active-Probes استفاده نمی‌کند. هیچ نشانه‌ای از پروب‌ها روی هیچ یک از سرورها وجود ندارد و حدس می‌زنیم IRGFW به سمت رویکرد غیرفعال (Passive) دقیق‌تر و بهینه‌تر رفته باشد که در این گزارش به آن خواهیم پرداخت.

در تصویر زیر، بیشتر محدوده‌های CIDR آدرس IP که به عنوان Prober شناسایی کردیم، ثبت شده‌اند. روش آزمون ما از رویکرد تیم gfw.report الهام گرفته شده است.[۲۸]

در صفحات بعدی، ما تمامی آزمون‌های Active-Probe خود را در **سه تیپ** دسته‌بندی کرده‌ایم. بیشتر این آزمون‌ها با Xray-core و برخی دیگر با هسته‌ها و روش‌های گوناگون در ایران انجام شده‌اند.

| Iran's GFW Active Probing Test | | | |
|---|---|---|---|
| AS Number | Org/Name | Num of Probes | IP Ranges |
| AS58224 | *Iran Telecommunication Company PJS (TCI)* | **6783** | 80.191.0.0/16<br>*(80.191.69.0/24)*<br>*(80.191.64.0/24)*<br>78.38.0.0/16<br>78.39.0.0/16<br>217.218.0.0/16<br>*(217.218.80.0/16)*<br>2.187.0.0/16 |
| AS48159 | *Telecommunication Infrastructure Company (TIC-AS)* | **3561** | 2.189.42.0/24<br>2.184.0.0/16 |
| AS49666 | *Telecommunication Infrastructure Company (TIC-GW-AS)* | **2067** | 2.188.28.0/24 |
| AS21341 | *Soroush Rasanheh Company Ltd (SINET-AS)* | **563** | 62.220.121.0/24 |
| AS12880 | *Information Technology Company (ITC) (DCI-AS)* | **105** | 2.188.170.0/24 |




(عکس ۸ – AP0)
[لینک]

# کاوشگرهای فعال

## تست تیپ ۱

در این سناریو، سرور با بهره‌گیری از پروتکل VLess-TCP-Reality روی پورت ۲۰۵۳، به مدت ۲٤ ساعت فعال بود و حدود ۲ ترابایت داده را پیش از مسدود شدن انتقال داد. درخواست‌های SYN واقعی به‌تدریج افزایش یافتند و در ساعت ۱۹ به ۳۳۲ درخواست رسیدند. اما فعالیت پروب‌ها که احتمالاً از سوی IRGFW صورت می‌گرفت، از ساعت ۵ آغاز شد و در ساعت ۱٦ به‌طور چشمگیری افزایش یافت (٦٤ درخواست SYN از سمت پروب‌ها در کنار ۳۰۱ درخواست SYN واقعی). این الگو نشان‌دهنده هدف‌گیری آگاهانه به عنوان بخشی از سازوکارهای اعمال سانسور است.

**مشاهدات کلیدی:**

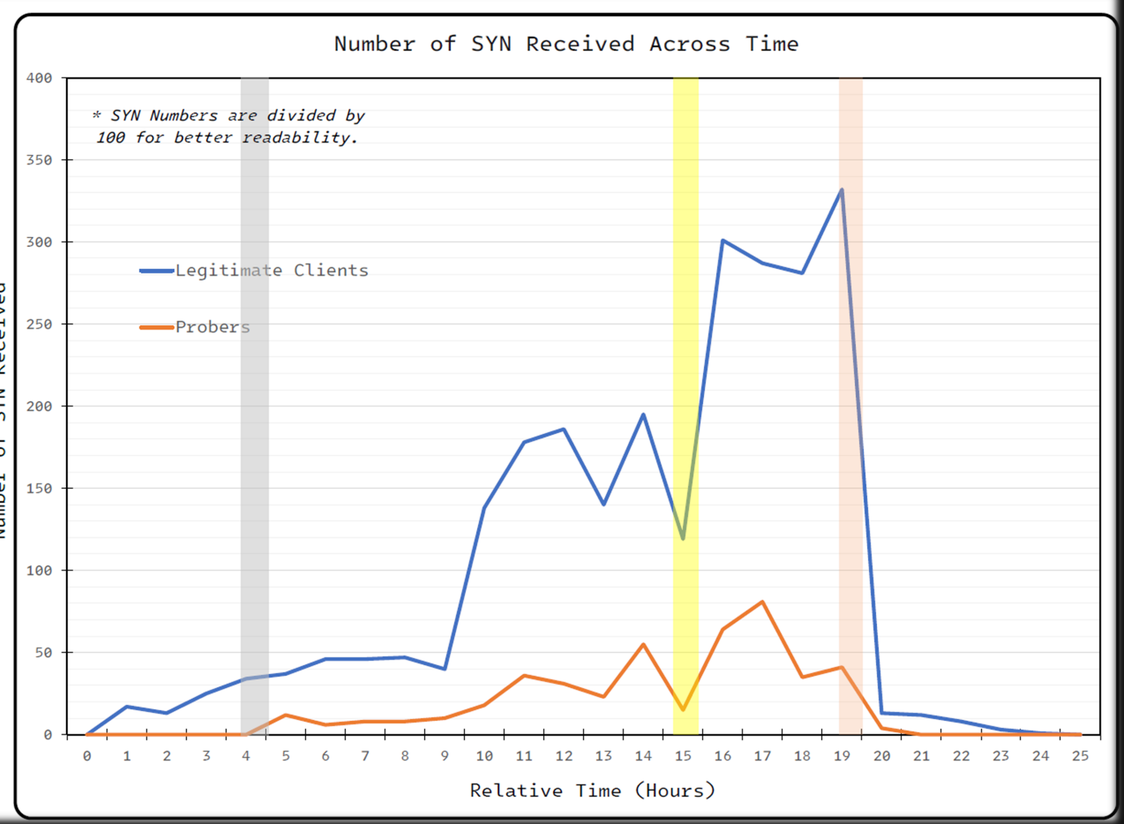
- افزایش پروب‌های فایروال ایران همزمان با رشد ترافیک، حاکی از نظارت فعال و تلاش برای پالایش ابزارهای دور زدن فیلترینگ است.
- با وجود مسدودسازی دامنه‌ها و آدرس‌های IP ایرانی، سرور به‌علت نبود سازوکارهای جایگزین (مانند fallback به Nginx) و عدم استفاده از راهبردهای دفاعی پویا، تحت فشار قرار گرفت.
- افزایش همزمان ترافیک و پروب‌ها در ساعات ۱٦ تا ۱۹ نشان از یک راهبرد پروب‌گذاری هماهنگ داشت که هدفش شناسایی و اختلال در روش‌های ارتباطی رمزگذاری‌شده بود.

| Number of SYN Received Across Time | | | |
|---|---|---|---|
| Relative Time (Hours) | *Legitimate Clients* | *Probers* | |
| 0 | 0 | 0 | |
| 1 | 17 | 0 | |
| 2 | 13 | 0 | |
| 3 | 25 | 0 | |
| 4 | 34 | 0 | |
| 5 | 37 | 12 | |
| 6 | 46 | 6 | ~300Gb Traffic Transferred. Probe Started. |
| 7 | 46 | 8 | |
| 8 | 47 | 8 | |
| 9 | 40 | 10 | |
| 10 | 138 | 18 | |
| 11 | 178 | 36 | |
| 12 | 186 | 31 | |
| 13 | 140 | 23 | |
| 14 | 195 | 55 | |
| 15 | 119 | 15 | |
| 16 | 301 | 64 | Traffic Increased Probes Increased |
| 17 | 287 | 81 | |
| 18 | 281 | 35 | |
| 19 | 332 | 41 | |
| 20 | 13 | 4 | **Server Blocked.** ~1950Gb Traffic Transferred. |
| 21 | 12 | 0 | |
| 22 | 8 | 0 | |
| 23 | 3 | 0 | |
| 24 | 1 | 0 | |
| 25 | 0 | 0 | |

| XRAY CONFIG |
|---|
| VLess-TCP-Reality |
| **Port:** 2053 |
| **Flow:** None |
| **SNI:** ftp.debian.org:443 |

| | |
|---|---|
| **Server Status** | BLOCKED |
| **Runtime** | 24 Hours |
| **Total Traffic** | 2 TB |

| | |
|---|---|
| **Nginx Fallback** | No |
| **IR Domains & IPs** | Blocked on Server |




(عکس ۹ – AP1)
[لینک]

# کاوشگرهای فعال

## تست تیپ ۲

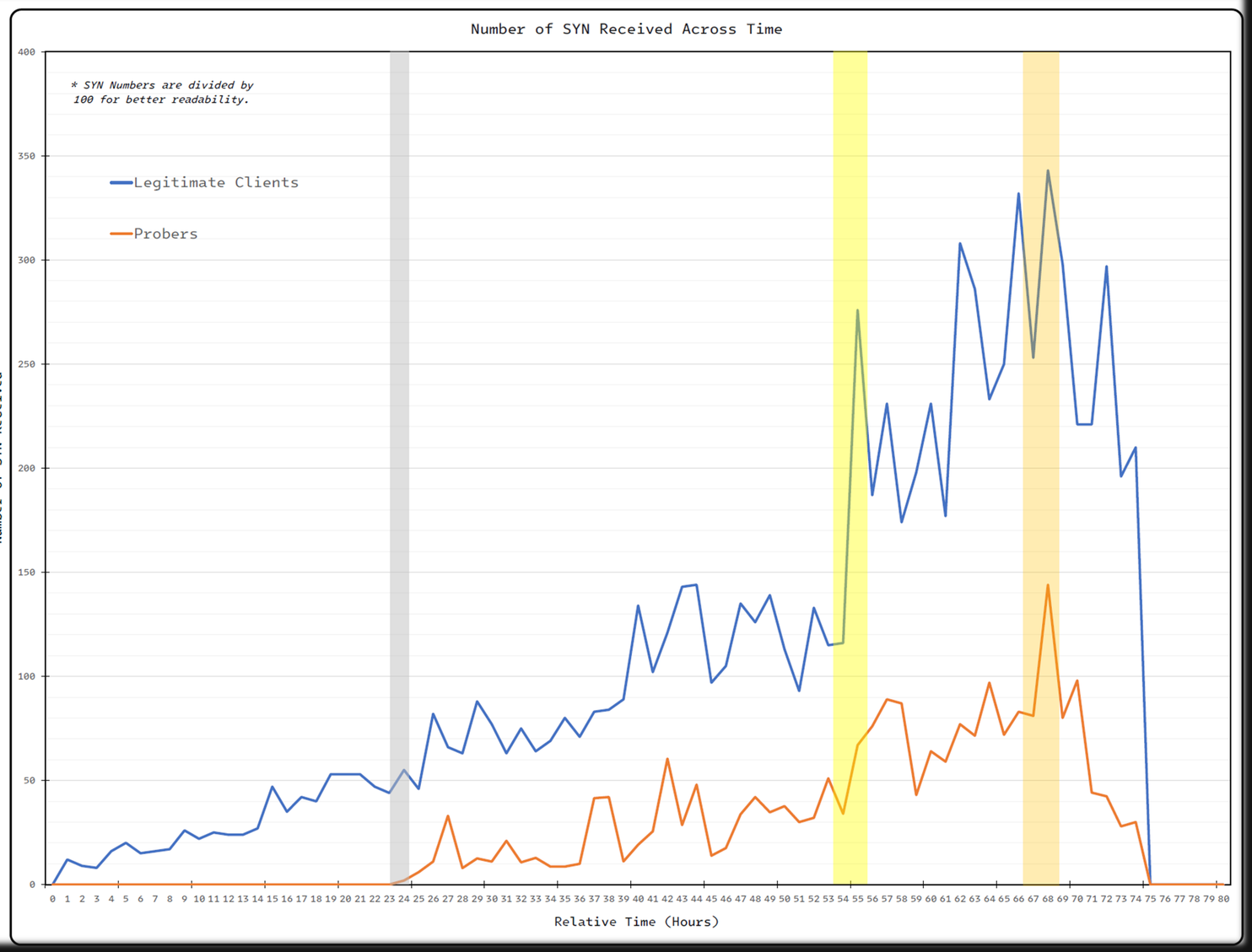
سروری که با VLess-TCP-Reality روی پورت ۸۰۸۰ فعال بود، به‌مدت ۷۵ ساعت کار کرد و حدود ۸ ترابایت داده را بدون مسدود شدن منتقل کرد. ترافیک واقعی به‌تدریج افزایش یافت و در ساعت ۶۸ به اوج ۳۴۳ درخواست SYN رسید. پروب‌ها، که احتمالاً از سوی فایروال ایران صورت می‌گرفت، پس از انتقال ۱.۲ ترابایت داده (ساعت ۲۴) آغاز شدند و در ساعت‌های ۵۵ و ۶۸ شدت گرفتند. این رفتار نشان‌دهنده هدف‌گیری فعال سازوکارهای سانسور است.

**مشاهدات کلیدی:**

- پروب‌ها همزمان با افزایش ترافیک واقعی شدت یافتند و در ساعت ۶۸ به ۳۴۳ درخواست SYN رسیدند. این روند بیانگر تلاش مداوم برای مختل کردن روش‌های رمزگذاری‌شده جهت دور زدن فیلترینگ است.
- با وجود پروب‌های پیوسته و افزایش ترافیک، سرور همچنان فعال ماند و این موضوع نشان می‌دهد که در برابر تلاش‌های فیلترینگ فعال، مقاوم بوده است.

Number of SYN Received Across Time

| Relative Time (Hours) | Legitimate Clients | Probers | XRAY CONFIG |
|---|---|---|---|
| 0 | 0 | 0 | VLess-TCP-Reality |
| 1 | 12 | 0 | **Port:** 8080 |
| 2 | 9 | 0 | **Flow:** xtls-rprx-vision |
| 3 | 8 | 0 | **SNI:** ooklaserver :8080 |
| 4 | 16 | 0 | |
| 5 | 20 | 0 | |
| 6 | 15 | 0 | |
| 7 | 16 | 0 | **Server Status** NOT BLOCKED |
| 8 | 17 | 0 | **Runtime** 75 Hours |
| 9 | 26 | 0 | **Total Traffic** 8 TB |
| 10 | 22 | 0 | |
| 11 | 25 | 0 | |
| 12 | 24 | 0 | |
| 13 | 24 | 0 | **Nginx Fallback** Yes |
| 14 | 27 | 0 | **IR Domains & IPs** Blocked on Server |
| 15 | 47 | 0 | |
| 16 | 35 | 0 | |
| 17 | 42 | 0 | |
| 18 | 40 | 0 | |
| 19 | 53 | 0 | |
| 20 | 53 | 0 | |
| 21 | 53 | 0 | |
| 22 | 47 | 0 | |
| 23 | 44 | 0 | |
| 24 | 55 | 2 | 1.2 TB Traffic Transferred; Probes Started. |
| 25 | 46 | 6 | |
| 26 | 82 | 11 | |
| 27 | 66 | 33 | |
| 28 | 63 | 8 | |
| 29 | 88 | 13 | |
| 30 | 77 | 11 | |
| 51 | 93 | 30 | Redundent Data Hidden. |
| 52 | 133 | 32 | |
| 53 | 115 | 51 | |
| 54 | 116 | 34 | |
| 55 | 276 | 67 | Major Traffic increased; Probes increased. |
| 56 | 187 | 76 | |
| 57 | 231 | 89 | |
| 58 | 174 | 87 | |
| 59 | 198 | 43 | |
| 60 | 231 | 64 | |
| 61 | 177 | 59 | |
| 62 | 308 | 77 | |
| 63 | 286 | 72 | |
| 64 | 233 | 97 | |
| 65 | 250 | 72 | |
| 66 | 332 | 83 | |
| 67 | 253 | 81 | |
| 68 | 343 | 144 | Major Traffic increased; Probes increased. |
| 69 | 298 | 80 | |
| 70 | 221 | 98 | |
| 71 | 221 | 44 | |
| 72 | 297 | 42 | |
| 73 | 196 | 28 | |
| 74 | 210 | 30 | |
| 75 | 0 | 0 | Server Shutdown. |
| 76 | 0 | 0 | |
| 77 | 0 | 0 | |
| 78 | 0 | 0 | |
| 79 | 0 | 0 | |
| 80 | 0 | 0 | |




(عکس ۱۰ – AP2) - [اینک]

# کاوشگرهای فعال

## تست تیپ ۳

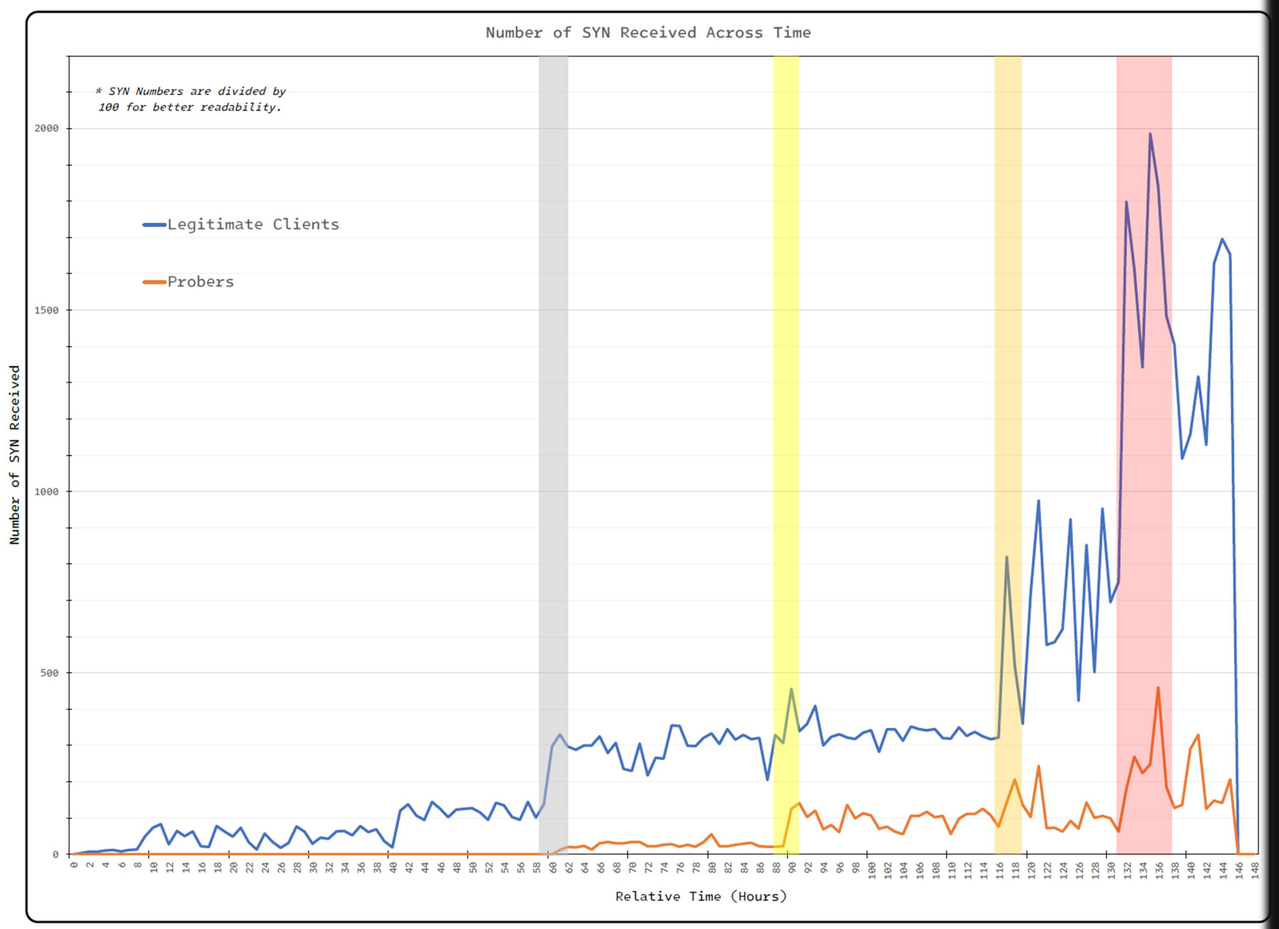
سروری که با VLess-TCP-Reality روی پورت ٤٤٣ کار می‌کرد، به مدت ١٤٥ ساعت فعال بود و حدود ٢١ ترابایت داده را بدون مسدود شدن منتقل کرد. درخواست‌های SYN معتبر به‌تدریج افزایش یافتند و در ساعت ١٣٥ به اوج ١٩٨٦ درخواست رسیدند. فعالیت پروب‌ها که احتمالاً از سوی فایروال ایران انجام می‌شد، پس از انتقال ٤.٢ ترابایت داده (ساعت ٦١) آغاز شد و در سه جهش اصلی در ساعت‌های ٩٠، ١١٧ و ١٣٢ شدت گرفت.

**مشاهدات کلیدی:**

- پروب‌ها از ساعت ٦١ آغاز شده و همزمان با اوج‌گیری شدید ترافیک مشروع به‌شدت افزایش یافتند. در ساعت ١٣٥، پروب‌ها به همراه ترافیک معتبر به اوج ١٩٨٦ درخواست SYN رسیدند.
- هر افزایش چشمگیر در ترافیک واقعی با یک جهش متناظر در پروب‌ها همراه بود که بیانگر اعمال پالایش نظام‌مند در دوره‌های پرترافیک است.
- با وجود ترافیک سنگین و پروب‌های پیوسته، سرور همچنان به کار خود ادامه داد و پایداری در برابر سازوکارهای فیلترینگ فعال را نشان داد.

Number of SYN Received Across Time

| Relative Time (Hours) | Legitimate Clients | Probers | XRAY CONFIG |
|---|---|---|---|
| 0 | 0 | 0 | VLess-TCP-Reality |
| 1 | 3 | 0 | Port: 443 |
| 2 | 7 | 0 | Flow: xtls-rprx-vision |
| 3 | 7 | 0 | SNI: steal personal domain with .com tld |
| 4 | 10 | 0 | |
| 5 | 12 | 0 | |
| 6 | 8 | 0 | |
| 7 | 12 | 0 | Server Status: NOT BLOCKED |
| 8 | 13 | 0 | Runtime: 145 Hours |
| 9 | 49 | 0 | Total Traffic: 21 TB |
| 10 | 73 | 0 | |
| 11 | 83 | 0 | |
| 12 | 27 | 0 | |
| 13 | 64 | 0 | Nginx Fallback: Yes |
| 14 | 50 | 0 | IR Domains & IPs: Blocked on Server |
| 15 | 63 | 0 | |
| 16 | 22 | 0 | |
| 17 | 20 | 0 | |
| 18 | 78 | 0 | |
| 57 | 144 | 0 | Redundent Data Hidden. |
| 58 | 101 | 0 | |
| 59 | 138 | 0 | |
| 60 | 297 | 0 | |
| 61 | 330 | 12 | 4.2 TB Traffic Transferred; Probes Started. |
| 62 | 297 | 20 | |
| 63 | 288 | 19 | |
| 64 | 300 | 23 | |
| 65 | 300 | 13 | |
| 66 | 325 | 30 | |
| 67 | 279 | 34 | |
| 86 | 321 | 22 | Redundent Data Hidden. |
| 87 | 205 | 21 | |
| 88 | 329 | 21 | |
| 89 | 306 | 22 | |
| 90 | 456 | 125 | Major Traffic increased; Probes increased. |
| 91 | 339 | 141 | |
| 92 | 359 | 103 | |
| 93 | 409 | 120 | |
| 94 | 300 | 69 | |
| 95 | 324 | 81 | |
| 96 | 331 | 61 | |
| 113 | 337 | 111 | Redundent Data Hidden. |
| 114 | 325 | 125 | |
| 115 | 317 | 107 | |
| 116 | 322 | 76 | |
| 117 | 820 | 143 | Major Traffic increased; Probes increased. |
| 118 | 520 | 206 | |
| 119 | 359 | 136 | |
| 120 | 720 | 103 | |
| 121 | 975 | 244 | |
| 122 | 577 | 72 | |
| 123 | 585 | 73 | |
| 124 | 620 | 62 | |
| 125 | 923 | 92 | |
| 126 | 423 | 71 | |
| 127 | 853 | 142 | |
| 128 | 502 | 100 | |
| 129 | 953 | 106 | |
| 130 | 695 | 99 | |
| 131 | 751 | 63 | |
| 132 | 1798 | 180 | Major Traffic increased; Probes increased. |
| 133 | 1613 | 269 | |
| 134 | 1342 | 224 | |
| 135 | 1986 | 248 | |
| 136 | 1840 | 460 | |
| 137 | 1483 | 185 | |
| 138 | 1405 | 128 | |
| 139 | 1090 | 136 | |
| 140 | 1158 | 290 | |
| 141 | 1317 | 329 | |
| 142 | 1128 | 125 | |
| 143 | 1628 | 148 | |
| 144 | 1696 | 141 | |
| 145 | 1653 | 207 | |
| 146 | 0 | 0 | Server Shutdown. |
| 147 | 0 | 0 | |
| 148 | 0 | 0 | |




(عکس ١١ – AP3)
[لینک]

# کاوشگرهای فعال

## خلاصه

- **روش آزمون**

تمامی آزمون‌های Active Probe در سه گروه اصلی دسته‌بندی شدند. بیشتر آزمون‌ها با بهره‌گیری از Xray-core انجام شد و شماری دیگر با هسته‌ها و روش‌های گوناگون در ایران آزمایش شدند. نتایج نشان دادند که استفاده از پروتکل‌های گوناگون TLS تأثیر چندانی بر رفتار پروب‌های IRGFW نداشت. نزدیک به ۹۰ درصد از تمام سرورهای ما که روی آن‌ها پراکسی‌های TLS و Non-TLS و تونل‌های VPN بدون توجه به پروتکل، اجرا می‌شد، توسط IRGFW پروب شدند. یک روش برای مدیریت این پروب‌ها استفاده از وب‌سرور Nginx بود. توجه داشته باشید که نباید کاوشگرها (پروب‌ها) مسدود شوند؛ بلکه باید به گونه‌ای مدیریت شوند که یکی از کدهای وضعیت HTTP خنثی دریافت کنند. (مثل 2XX، 3XX، 404 و ...)

- **نسبت پروب‌ها**

میانگین نسبت پروب‌ها به درخواست‌های SYN واقعی بین ۰.۲ تا ۰.۳ بود. به عبارت دیگر، به ازای هر کاربر واقعی، به طور میانگین ۲۰ تا ۳۰ درصد همان میزان پروب ثبت شد که این امر نشان‌دهنده سطح نسبتاً بالای پروب‌های فعال در مقایسه با ترافیک واقعی بود.

- **دوره آزمون و میزان ارتباط**

توجه داشته باشید که این نتایج مربوط به آزمون‌هایی است که تا شهریور ۱۴۰۲ انجام شده‌اند و توانایی پروب فعال IRGFW در آن زمان را نشان می‌دهند. از دی ۱۴۰۲ به بعد، این یافته‌ها دیگر کاربرد ندارند، زیرا IRGFW از آن زمان تاکنون هیچ سازوکار پروب فعالی را به‌کار نبرده است.

# سیستم بازرسی عمیق بسته‌ها
## (The DPI)

## سیستم بازرسی عمیق بسته‌ها (The DPI)

### وضعیت TLS

IRGFW به‌طور پیوسته بازرسی عمیق و اثرانگشت‌برداری از هندشیک‌های TLS ClientHello را انجام می‌دهد تا ترافیک احتمالی VPN یا پراکسی را بر پایه الگوهای متمایز شناسایی کند، بی‌توجه به نسخه TLS. هرچند می‌توان از ابزاری مانند uTLS برای ابهام‌سازی برخی اثرانگشت‌ها بهره گرفت، اما این ابزار به‌طور کامل مانع شناسایی نمی‌شود، زیرا خود uTLS نیز آسیب‌پذیری‌هایی دارد که DPI پیشرفته قادر به تشخیص آن‌هاست.

ما مجموعه‌ای از ابزارها برای سنجش و تحلیل این رفتارها توسعه دادیم. برای نمونه، یک سرور Nginx با یک وب‌سایت استاندارد روی یک آدرس IP عمومی (لیست سفید) راه‌اندازی شد. این سایت از طریق تمامی ISPهای بزرگ ایران، با مرورگرهای Chrome و Firefox، بدون مشکل در دسترس بود. اما هنگامی که یک کوئری DNS با استفاده از DoT یا DoH از طریق یک کلاینت DNS معروف در ویندوز آغاز شد، هندشیک TLS کامل نشد و اتصال با گذشت زمان بی‌پاسخ (Timeout) ماند.

هنگامی که از uTLS (چه در حالت رسمی و چه حالت تکه‌تکه‌سازی) استفاده کردیم، هندشیک کامل شد. این امر نشان می‌دهد که IRGFW، کلاینت DNS را اثرانگشت‌برداری (Fingerprint) کرده است. این مشکل بر کلاینت‌های مهم VPN نیز تأثیر می‌گذارد: با وجود آدرس IP و دامنه SNI در لیست سفید، هندشیک TLS به Timeout منجر می‌شود.[۳۲] با این حال، زمانی که از یک کلاینت کمتر رایج یا غیراستاندارد با ویژگی‌های اثرانگشتی متفاوت استفاده کردیم، هندشیک موفقیت‌آمیز بود و تونل VPN بدون مشکل برقرار شد.

## سیستم بازرسی عمیق بسته‌ها (The DPI)

### سیستم DPI در IRGFW از دو بخش اصلی تشکیل شده است:

- **بخش Active:** این بخش، اولین ۱ تا ۱۷ کیلوبایت از هر اتصال بین‌المللی را بررسی می‌کند. سیستم در نخستین بسته‌های هر جریان به‌دنبال Fingerprintهای از پیش تعیین‌شده مانند 0x3 0x16 می‌گردد که نشان‌دهنده احتمال استفاده از TLS است. سپس به‌دنبال SNI extension در این بسته می‌گردد که با 0x1 شروع می‌شود و شامل طول بسته است. پس از شناسایی SNI، بررسی می‌کند آیا این SNI در Hashtable مسدودسازی قرار دارد یا خیر. اگر بسته از نوع TLS نباشد، سیستم به‌دنبال اثرانگشت‌های دیگر مانند SSH یا HTTP می‌گردد. در مورد HTTP نیز به‌دنبال Host header می‌گردد.

  پیش‌تر سیستم به بزرگی و کوچکی حروف و فاصله‌ها حساس بود، اما اکنون همه فاصله‌ها حذف می‌شوند. این بررسی‌های فعال به‌نظر می‌رسد روی ASICهای تخصصی اجرا می‌شود، چرا که بار پردازشی آن‌ها بالاست، اما حتی با پردازنده‌های قوی هم تأخیر و افزایش Ping رخ می‌دهد. اکثر مردم بعدازظهرها به خانه بازمی‌گردند و VPNهای خود را فعال می‌کنند و این امر سبب شلوغی سیستم DPI می‌شود. شایان ذکر است که اپراتورهای بخش Active متفاوتند و هرکدام باگ‌ها و ضعف‌های خود را دارند، که نشان می‌دهد سیستم چندان یکدست نیست.

- **بخش Passive:** پیش از به‌روزرسانی اخیر (اواخر آذر ۱۴۰۲ / اوایل دی ۱۴۰۲)، سیستم DPI کاملاً Active بود و می‌شد آن را فریب داد بی‌آن‌که مشکلی ایجاد شود. اما پس از به‌روزرسانی، MCI به‌طور تصادفی بخشی از اتصالات هر کاربر را نمونه‌برداری کرده و به‌صورت Passive الگوهای دور زدن را ثبت می‌کند. این الگوها شامل TLS-in-TLS، فرایندهای authentication و packet headerهای استاندارد VPN هستند.

  برای نمونه، هنگام استفاده از VLess (V2ray/Xray)، پیش از ارسال جریان اصلی یک بسته authentication کوچک به هر اتصال می‌فرستد تا از درست بودن کلاینت اطمینان حاصل کند. همچنین هنگامی که یک اتصال VPN جدید با یک اتصال TLS دیگر برقرار می‌شود، سیستم Passive blocking به‌دنبال الگوهای تکراری در بسته‌های کوچک حاوی الگوهای TLS یا V2ray/Xray می‌گردد. اگر IPها و دامنه‌ها شناسایی شوند، هر ٤ ساعت (بر اساس الگوی زمانی) به سیستم مسدودسازی گزارش می‌شوند تا سرعت آن‌ها کاهش یابد یا به‌طور کامل مسدود شوند.

## سیستم بازرسی عمیق بسته‌ها (The DPI)

### راهکار ممکن

برای کاهش خطر مسدود شدن سرور، باید الگوهایی را که باعث شناسایی می‌شوند، مختل کرد. یکی از این روش‌ها، تغییر در الگوهای ترافیکی است که سرورها به‌سادگی شناسایی می‌کنند. با تزریق بسته‌های تصادفی در ابتدای هر جریان می‌توان قصد اصلی ترافیک را پوشاند و تشخیص را دشوارتر کرد. همچنین با چندمسیره کردن (Multiplexing) چندین جریان در تعداد کمتری اتصال، میزان رویت‌پذیری جریان‌های تکی کاهش یافته و احتمال شناسایی کمتر می‌شود.

در مورد ترافیک مربوط به authentication، تزریق بسته‌های تصادفی و خرد کردن (Fragmentation) آن‌ها با طول و Padding متفاوت، مانع از شناسایی الگوهای قابل پیش‌بینی می‌گردد. با کمتر یکنواخت کردن فرایند authentication، احتمال علامت‌گذاری آن کاهش می‌یابد.

میزان اثربخشی مسدودسازی تا حد زیادی به این وابسته است که پروتکل‌ها به‌راحتی قابل تغییر نباشند و نتوان تغییرات را به سادگی به کاربران منتقل کرد. اگر کاربران بتوانند الگوهای ترافیک را پویا تغییر دهند و این تغییرات را به‌طور گسترده اعمال کنند، توانایی فایروال در مسدودسازی بر پایه الگوهای ثابت کاهش می‌یابد. قابلیت تغییر پروتکل‌ها (مثلاً از طریق رمزگذاری، ابهام‌سازی ترافیک یا Fragmentation) به حفظ گمنامی و کاهش خطر شناسایی کمک کرده و اثربخشی تلاش‌های مسدودسازی را کمتر می‌کند.

این استراتژی به سازگاری مداوم برای جلوگیری از رفتار قابل پیش بینی که می تواند برای مسدود کردن یا فیلتر کردن استفاده شود، بستگی دارد.

# بررسی اجمالی پروتکل‌ها

## بررسی اجمالی پروتکل‌ها

این آزمون‌ها به‌طور گسترده با MahsaServer.com (مواقع امکان‌پذیر) انجام شده‌اند. سایر آزمون‌ها به‌طور ناشناس در فضای واقعی و با کاربران ایرانی از طریق پنج ISP برتر صورت گرفته‌اند. تعداد آزمون‌ها برای هر پروتکل یا روش بین ٤ تا ۲۰ سرور متغیر بوده است. نتایج میانگین‌گیری و میانه‌ی آنها در نظر گرفته شده‌اند. همچنین، تمامی آزمون‌ها مستقیماً روی یک سرور خارجی انجام شده‌اند و هیچ سرور واسطه یا تانلی در کار نبوده است.

- **Socks5, SSTP, PPTP, IKEv2/IPSEC:** مسدود بر پایه اثرانگشت برای تمامی آدرس‌های IPخارجی. (لیست سیاه)
- **L2TP:** مسدود. بسیاری از مسئولان دولتی از این پروتکل استفاده می‌کنند، اما آدرس‌های IP ایرانی یا IMEI آنها در فهرست سفید قرار داده شده است. (لیست سیاه)
- **OpenVPN:** کاملاً مسدود از طریق اثرانگشت در تمامی ISP های اصلی. (لیست سیاه)
  - **OpenVPN + Cloak:** تا حدی کارآمد. Cloak به‌تازگی توسط IRGFW شناسایی شده [۲۹] و منجر به سرعت بسیار کم در UL/DL و نوسان بالا می‌شود. (لیست خاکستری)
- **Wireguard:** به‌طور کامل در تمامی ISPهای بزرگ مسدود، اما می‌تواند با یک آدرس IP سفید و ترافیک کم بدون محدودیت در برخی ISPها کار کند. ترافیک بالا سریعاً منجر به مسدودسازی می‌شود.
- **Obfuscated Wireguard:** طبق مطالب بخش UDP، با تغییر هندشیک قابل استفاده است، اما در برابر اثرانگشت‌برداری آسیب‌پذیر است.
- **Shadowsocks** (نسخه‌های قدیمی و جدید رمزگذاری و روش‌ها): عمدتاً مسدود، گاهی خاکستری. برخی تغییرات امکان اتصال را فراهم می‌کنند اما با اتلاف بسته‌ها (Packet Loss) و نوسان بالا همراه است. (لیست خاکستری)
  - **ShadowSocks + Cloak:** تا حدی کارآمد. اما توسط IRGFW شناسایی شده و منجر به سرعت بسیار کم در UL/DL و نوسان بالا می‌شود. (لیست خاکستری)
- **MTProto:** عمدتاً خاکستری. درصورت فعال بودن، از یک الگوی زمانی سخت پیروی می‌کند که منجر به مسدودسازی IP در عرض چهار روز می‌شود، اما می‌تواند تا ۲ هفته یا بیشتر هم ادامه یابد.
- **SoftEther:** مشابه وایرگارد. از طریق اثرانگشت شناسایی و مسدود می‌شود و از الگوی زمانی سخت پیروی می‌کند. (لیست سیاه)
- **SSH:** در برخی ISPها تا حدی کارآمد و در دیگران خاکستری. اغلب از یک الگوی زمانی انعطاف‌پذیر پیروی می‌کند. (لیست خاکستری)
  - **SSH-over-TLS:** تا حدی کارآمد و اغلب از یک الگوی زمانی انعطاف‌پذیر پیروی می‌کند. (لیست خاکستری)

## بررسی اجمالی پروتکل‌ها

- **V2Ray/XRay/SingBox** (v5.22.0/v24.12.18/v1.10.5)**:**
  - **VMess-(TCP/WS/HU/GRPC)-NonTLS:** با یک IP سفید در شبکه همراه اول و مخابرات قابل استفاده است، اما معمولاً طی چهار روز مسدود می‌شود و در برخی موارد تا دو هفته کار می‌کند.
  - **VLess/VMess)-(TCP/WS/HU/GRPC/H2)-TLS):** با یک IP سفید کار می‌کند، اما اغلب ظرف دو هفته مسدود می‌شود (الگوی زمانی).
  - **REALITY/ShadowTLSv3:** معمولاً در عرض چهار روز (گاهی ۲٤ ساعت) مسدود می‌شود، مگر آن‌که با یک SNI در لیست سفید استفاده شود، اما حتی در این صورت معمولاً ظرف دو هفته مسدود می‌گردد. این رفتار نشان می‌دهد که IRGFW احتمالا از یک سیستم Reverse DNS Mapping برای شناسایی و مسدودسازی این نوع پروتکل‌ها و IP های مقصد استفاده می‌کند.
  - **Trojan:** رفتاری مشابه V2Ray/Xray با TLS دارد. خاکستری و دارای الگوی زمانی مسدودسازی.
- **Hysteria2:** نیازمند آپی مقصدی با پشتیبانی از QUIC است. (صفحه ۱۲ - وضعیت UDP)
  - **Hysteria2 + Obfs (Salamander):** ممکن است QUIC روی برخی IPها کاملاً غیرفعال شود، اما اگر UDP بدرستی کار کند، Obfs گاهی می‌تواند از این محدودیت عبور کند.
- **TUIC/JUICITY:** مشابه Hysteria2 ساده. خاکستری با محدودیت پهنای‌باند در دریافت/ارسال (UL/DL) و نوسان بالا.
- **Obfs4** (برای هر پروتکلی مانند OpenVPN/ShadowSocks/Tor): عمدتاً مسدود ولی ممکن است در برخی ISPها کار کند. خاکستری با نوسان بسیار بالا و محدودیت شدید در سرعت آپلود.
- **TOR** (با هر ترکیب Bridge): عمدتاً مسدود، و به ندرت خاکستری با سرعت محدود.

## بررسی اجمالی پروتکل‌ها

- **شبکه توزیع محتوا (CDN):**

برخی CDNها مانند Cloudflare با پروتکل‌های خاصی سازگار هستند که امنیت و حریم خصوصی را بهبود می‌دهند. یک پیکربندی رایج VLess+(WS/gRPC)+TLS است که با عبور ترافیک از CDN، نشانی IP سرور مجازی را پنهان می‌سازد. این رویکرد، شناسایی مستقیم سرور اصلی را برای IRGFW دشوارتر می‌کند.

با این حال، دامنه‌ی SNI/Host در تنظیمات پروتکل به‌عنوان یک نقطه آسیب‌پذیر مطرح است. هنگامی که IRGFW این دامنه را بیابد، می‌تواند آن را مسدود کند و عملاً ترافیک را از کار بیندازد. برای مقابله با این مشکل، از روش تکه‌تکه‌سازی (Fragmentation) استفاده می‌شود. در این روش، دامنه SNI/Host به بخش‌های کوچک‌تر تقسیم می‌شود تا فایروال و DPI نتوانند آن را به درستی بخوانند یا تفسیر کنند.[۳۰]

با وجود این تلاش‌ها، محدودیت‌هایی وجود دارد. ممکن است IRGFW با مسدودسازی همه اتصال‌ها به برخی CDNها که قادر به تفسیر SNI/Host فرگمنت شده نیستند، پاسخ دهد. افزون بر این، از آذر ۱۴۰۳، Cloudflare تدابیر امنیتی سختگیرانه‌تری به کار گرفته که ترافیک ابزارهایی مانند V2ray/Xray را «رفتار رباتی» شناسایی کرده و منجر به اختلال یا قطع اتصال می‌شود.

- **ECH/ESNI:**

ECH که پیش‌تر ESNI نام داشت، هدفی مشابه تکه‌تکه‌سازی را دنبال می‌کند: جلوگیری از خوانده شدن دامنه SNI توسط فایروال‌ها. با رمزگذاری هندشیک، ECH مانع از آن می‌شود که دیواره‌های میانی و سامانه‌های سانسور SNI را مشاهده کنند. این رمزگذاری توانایی IRGFW در بازرسی هندشیک غیررمزگذاری‌شده را مختل کرده و بسیاری از تلاش‌های سانسور را ناکام می‌گذارد.

در گذشته، ECH و ESNI در کشورهایی با سانسور شدید مانند ایران و چین به‌طور کامل مسدود بودند. با این حال، در سال‌های اخیر، ایران اجازه استفاده از ECH را داده است که راهی احتمالی برای دور زدن محدودیت‌ها فراهم می‌کند. این در حالی است که در چین، ECH و ESNI همچنان توسط فایروال بزرگ (GFW) مسدود می‌شوند.[۳۱]

هرچند ECH با رمزگذاری SNI محافظت قدرتمندی ایجاد می‌کند، اما همچنان در برابر مسدودسازی در سطح زیرساخت آسیب‌پذیر است. همان‌طور که در بخش CDN اشاره شد، اگر زیرساخت اصلی شبکه (مانند IRGFW یا Cloudflare) تصمیم به مسدودسازی انواع خاصی از ترافیک رمزگذاری‌شده بگیرد، پیکربندی‌های ECH نیز ممکن است بی‌اثر شوند. این آسیب‌پذیری نشان‌دهنده رقابت پیوسته میان روش‌های دور زدن سانسور و راهکارهای مقابله‌ای حکومت‌های سرکوبگر است.

# بروزرسانی آبان ۱۴۰۳

## به‌روزرسانی آبان ۱۴۰۳ فایروال بزرگ ایران (IRGFW)

از اوایل آبان ۱۴۰۳ (و در زمان نوشتن این گزارش)، IRGFW به طور قابل توجهی عملکرد DPI خود را کاهش داده است. این کاهش منجر به غیرفعال‌سازی یا اجرای حداقل قوانین مسدودسازی سخت‌گیرانه قبلی، الگوهای زمانی (Time-Pattern) و پروتکل‌های کاوش فعال شده است که هسته اصلی کنترل اینترنت فایروال را تشکیل می‌دهند.

در حال حاضر، فایروال‌های اصلی ISPها همچنان فعال هستند، اما با آستانه‌های پایین‌تر کار می‌کنند و تنها به پالایش پایه بسنده می‌کنند، بی‌آن‌که از بازرسی عمیق ترافیک و پایش همه‌جانبه‌ای که DPI عموماً فراهم می‌کند، بهره ببرند. در نتیجه، بسیاری از پروتکل‌ها مانند VPNها، اتصالات رمزگذاری‌شده و خدمات مبتنی بر UDP که پیشتر با محدودسازی‌های شدید، مسدودسازی یا خاکستری‌سازی روبه‌رو بودند، اکنون با محدودیت‌ها و اختلالات کمتری مواجه هستند. وضعیت کنونی بیانگر یک کاهش موقت در شدت سانسور است، چرا که قابلیت‌های پیشرفته‌ی DPI در IRGFW، نظیر شناسایی و اثرانگشت‌برداری الگوهای ترافیک، نمونه‌برداری فعال از بسته‌ها و مسدودسازی با همگام‌سازی لیست سیاه، در حال حاضر به‌کار گرفته نمی‌شوند.

این کاهش شدت کنترل ممکن است فضای بیشتری برای جریان آزاد داده و دسترسی بازتر به خدماتی که پیشتر محدود شده بودند، فراهم کند. با این حال، این تغییر می‌تواند بسته به تصمیمات سیاستی آینده و تنظیمات فنی، برگشت‌پذیر باشد. هرچند احتمال موقتی بودن این تغییر وجود دارد، اما نشان‌دهنده وقفه‌ای قابل توجه در تدابیر فراگیر IRGFW است، وقفه‌ای که فرصتی کوتاه برای افزایش اتصال و کاهش سانسور در گستره اینترنت ایران فراهم کرده است.

## حرف آخر

پیکار پیوسته میان سانسور و روش‌های گریز از آن، همچون یک بازی بی‌پایان موش‌وگربه، پویا و بی‌امان است. شیوه‌های گریز به گونه‌ای مداوم ساخته، به‌کار گرفته و بهبود داده می‌شوند، اما در نهایت به دست فایروال‌های پیچیده‌تر شناسایی، مختل و از کار انداخته می‌شوند. در برابر این فرایند، روش‌های تازه‌ای پدیدار می‌شوند که دسترسی را به شکلی گذرا بازمی‌گردانند و این چرخه بی‌پایان هماوردی و رویارویی را ادامه می‌دهند.

کاستن کنونی از شدت فیلترینگ اینترنتی به دست رژیم اسلامی ایران، نه دگرگونی‌ای پایدار و نه نشانه‌ای از نرمش است. بلکه این کاهش، وقفه‌ای حساب‌شده به نظر می‌رسد که به سامانه‌های وابسته به IRGFW زمان می‌دهد تا برای بهبود توانایی در شناسایی و مقابله با شیوه‌های نوین گریز، آماده شود. این سامانه‌ها به گونه‌ای دقیق‌تر تنظیم می‌شوند تا در دوره‌های حساس سیاسی یا اجتماعی، مهار جریان داده‌ها را برای نگهداشت اقتدار آسان‌تر کنند.

در چنین محیطی، وابستگی به یک روش یکتا برای گریز از فیلترینگ، نه تنها ناکارآمد، بلکه پرخطر است. رویکردی پایدار نیازمند به‌کارگیری مجموعه‌ای گوناگون از شیوه‌ها است که به موازات هم به کار گرفته شوند. بهره‌گیری هم‌زمان از چندین روش گوناگون، از پروتکل‌های تازه و کانال‌های رمزگذاری‌شده گرفته تا روش‌های پنهان‌سازی و تکه‌تکه کردن داده‌ها، به گونه‌ای چشمگیر خطر قطع کامل اتصالات را کاهش می‌دهد. افزونگی در ابزارها تضمین می‌کند که اگر یک شیوه ناکارآمد شود، دیگر شیوه‌ها همچنان کارآمد بمانند و دسترسی پیوسته فراهم باشد.

سرانجام، توانایی سازگاری و گوناگونی راهبردها برای رویارویی با ابزارهای پیشرفته‌تر سانسور ناگزیر است. کامیابی در این پیکار به نوآوری پیوسته، آینده‌نگری و بهره‌گیری از دامنه‌ای گسترده از ابزارها بستگی دارد. نبرد برای آزادی در جهان دیجیتال یک چالش پایدار نیست؛ این نبرد، به پایداری، آفرینندگی و آمادگی برای رویارویی با هر محدودیت تازه، با راه‌حل‌هایی نیرومندتر و انعطاف‌پذیرتر نیازمند است.

# منابع


1. https://www.amnesty.org/en/latest/news/2023/09/what-happened-to-mahsa-zhina-amini/
2. https://www.ohchr.org/en/press-releases/2023/09/iran-one-year-anniversary-jina-mahsa-aminis-death-custody-heightened
3. https://github.com/net4people/bbs/issues/125
4. https://gfw.report
5. https://github.com/net4people/bbs/issues/129
6. https://apps.dtic.mil/sti/citations/AD1107324
7. https://dig.watch/updates/iran-to-implement-national-information-network-to-keep-people-off-the-internet
8. https://www.science.org/content/article/iran-s-researchers-increasingly-isolated-government-prepares-wall-internet
9. https://www.en-hrana.org/tag/tarh-e-sianat/
10. https://bgp.tools/rankings/IR?sort=cone
11. https://internetabad.factnameh.com/fa
12. https://mci.ir/introduction
13. https://irancell.ir/p/4471/
14. https://www.tci.ir/%D8%AA%D8%A7%D8%B1%DB%8C%D8%AE%DA%86%D9%87/
15. https://www.tic.ir/fa/introduce
16. http://www.iranet.ir/
17. https://www.ipm.ir/
18. https://www.paloaltonetworks.com/blog/2014/06/udp-malware-hiding-place-of-choice/
19. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clc6CAC
20. https://github.com/net4people/bbs/issues/140
21. https://ieeexplore.ieee.org/document/1404672
22. https://etchamber.ir/internet-report-2
23. https://github.com/net4people/bbs/issues/113
24. https://irgfw.report/blog/post1/
25. https://github.com/net4people/bbs/issues/224#issuecomment-1462268182
26. https://t.me/irgfw/6
27. https://github.com/XTLS/Xray-core/issues/2778
28. https://gfw.report/blog/gfw_shadowsocks/
29. https://github.com/net4people/bbs/issues/327
30. https://github.com/GFW-knocker/gfw_resist_tls_proxy
31. https://github.com/net4people/bbs/issues/43
32. https://github.com/net4people/bbs/issues/153

# تحلیل فنی IRGFW

## شناخت فایروال بزرگ ایران

گزارش یک

دی ۱۴۰۳

IRGFW

irgfw.report