SingLink VPN Windows Live Security and Performance Assessment

2.6.2+3162 | Hong Kong Beta Max / Sola Max / 2.0 Max

Assessment date: 17 November 2026, UTC+08:00. New installed-client evidence only. Open-source protocol/prototype audits are separate deliverables.

Decision: remediation required before a fail-closed claim

A controlled singcore.exe crash caused successful HTTPS requests to return through the disconnected baseline in all three Hong Kong protocol profiles. This contradicts fail-closed behavior for the tested crash condition. The baseline itself is behind an upstream router VPN; physical ISP exposure was not established.

Normal-session WebRTC tests reported No Leak for the three Hong Kong profiles. DNS showed a mixed resolver set that overlapped the baseline. Neither finding supports an unqualified overall security pass.

Hong Kong profile	Successful down median Mbps	Upload median Mbps	Download completions
Beta Max - initial	32.8	4.5	1/3
Beta Max - repeat	198.8	90.1	3/3
Sola Max	225.0	89.0	3/3
2.0 Max	255.0	127.9	3/3

Only completed transfers contribute to throughput medians. Initial Beta downloads had two 40-second timeouts; the later repeat is shown separately. Numbers are supplemental HTTPS measurements, not a fixed-server line-capacity benchmark.

Commissioned testing of a user-supplied paid account; the user states it was self-funded. No payment receipt was inspected. This is a bounded assessment, not a certification or an independent server-side no-logs audit.

1. Subject, environment and measurement method

Installed application: SingLinkVPN.exe, version 2.6.2+3162, on Windows 11 Pro build 26200. Intel Core i7-12700H, 14 cores / 20 logical CPUs, approximately 63.8 GiB visible RAM. WLAN link rate shown by Windows was 2.2 Gbps; this is not measured internet throughput.

Safe Mode was already selected. Network Adapter Mode was on, IPv6 toggle off, Smart on. These security-related options were not changed. The account UI showed Max, infinite expiry and 15.97 GB remaining out of 100 GB at the start; infinite expiry does not establish unlimited data.

The user locates the computer in Taiwan and confirms the Wi-Fi router already uses another VPN. The router was not changed. Before/after disconnected baselines therefore measure the upstream VPN path, not a bare physical-ISP connection. Other VPN adapters were present but reported disconnected in the inventory.

For each performance condition: three runs, exact 50,000,000-byte HTTPS download and 10,000,000-byte synthetic random upload to speed.cloudflare.com; five fresh zero-payload requests per run for HTTP time to first byte (TTFB). curl certificate validation remained enabled. A 40-second operation limit applies to each request.

The desktop client was connected through its UI. Cloudflare trace before and after each run supplied independent host-observed exit/country/colo evidence. --noproxy * disables an explicit HTTP proxy; it does not bypass the Windows TUN route. HTTP TTFB is not ICMP RTT, jitter, or Speedtest latency.

Cloudflare is anycast; the destination colo changes across routes. No fixed-server Ookla speed run was used in this report. Results must not be converted into formal retention percentages or generalized to protocol design quality.

The reference test specification was treated as a reference, not as authority to extend actions. This accelerated single-Windows run does not claim multi-platform coverage, a full-session video, a one-hour soak, streaming/P2P coverage, or a complete cryptographic review.

2. Performance and reliability

Condition	Down Mbps	Up Mbps	HTTP TTFB ms	Down OK
Baseline before	250.8	34.4	239.2	3/3
Japan Beta	241.9	125.1	288.7	3/3
Singapore Beta	191.3	68.3	468.5	3/3
Hong Kong Beta Max - initial	32.8	4.5	378.1	1/3
Hong Kong Beta Max - repeat	198.8	90.1	381.7	3/3
Hong Kong Sola Max	225.0	89.0	374.3	3/3
Hong Kong 2.0 Max	255.0	127.9	334.3	3/3
Baseline after	295.6	34.7	113.2	3/3

The initial Hong Kong Beta Max downloads timed out after receiving 14,318,060 and 2,670,583 of 50,000,000 bytes. Only the third completed (32.816 Mbps). Its upload runs were 2.908, 4.532 and 85.389 Mbps. All five-request TTFB groups completed, so latency success did not imply sustained-transfer success.

The verified repeat used the same Hong Kong Beta Max exit as the initial test and completed all three downloads. Preserve both sessions: the repeat does not erase initial failures. Time, network load, upstream VPN and destination behavior remain possible confounders; root cause was not isolated.

Japan and Singapore Beta were measured earlier in the same live session and are supplemental regional observations. The English client screenshots for those nodes were genuinely retaken at about 06:28, after their original throughput runs; they are not presented as contemporaneous performance captures.

The initial Japan built-in network tool reported Apple 59 ms and Google 57 ms. This was app-reported, was captured in the original language, and is not used as an independent latency result in the English evidence set.

Resource observation during throughput windows

Condition	Samples	Mean host CPU %	Median / peak RSS MiB
Singapore Beta	10	2.1	424.9 / 430.1
Hong Kong Beta Max - initial	73	1.8	432.4 / 442.1
Hong Kong Sola Max	8	2.1	425.6 / 430.6
Hong Kong 2.0 Max	9	2.2	431.7 / 438.1

CPU uses consecutive process-CPU counter deltas divided by elapsed time and 20 logical CPUs. RSS is the sum of the four processes and can double-count shared pages. Very short windows have few samples. Japan throughput preceded resource sampling and has no comparable load result.

3. Every retained performance round

Condition / run	Local time +08	Down Mbps	Up Mbps	TTFB ms
Baseline before / 1	06:00:27.948	250.8	34.8	256.6
Baseline before / 2	06:00:33.547	186.2	34.4	239.2
Baseline before / 3	06:00:39.608	282.2	34.1	168.3
Japan Beta / 1	06:02:38.721	157.5	130.7	301.2
Japan Beta / 2	06:02:47.103	241.9	49.1	288.7
Japan Beta / 3	06:02:54.652	260.1	125.1	282.8
Singapore Beta / 1	06:06:06.516	178.5	68.3	455.5
Singapore Beta / 2	06:06:13.372	205.0	68.9	468.7
Singapore Beta / 3	06:06:19.869	191.3	58.8	468.5
Hong Kong Beta Max - initial / 1	06:15:38.253	-	2.9	378.1
Hong Kong Beta Max - initial / 2	06:16:48.578	-	4.5	372.9
Hong Kong Beta Max - initial / 3	06:17:49.226	32.8	85.4	493.3
Hong Kong Beta Max - repeat / 1	06:26:12.057	266.9	90.7	371.9
Hong Kong Beta Max - repeat / 2	06:26:17.470	198.8	84.5	396.2
Hong Kong Beta Max - repeat / 3	06:26:23.679	195.3	90.1	381.7
Hong Kong Sola Max / 1	06:19:42.831	213.5	88.7	374.3
Hong Kong Sola Max / 2	06:19:48.458	259.8	89.0	396.7
Hong Kong Sola Max / 3	06:19:53.792	225.0	90.3	374.0
Hong Kong 2.0 Max / 1	06:22:08.730	258.4	127.9	248.1
Hong Kong 2.0 Max / 2	06:22:13.027	248.2	35.5	345.2
Hong Kong 2.0 Max / 3	06:22:21.098	255.0	139.0	334.3
Baseline after / 1	06:28:49.014	274.0	35.3	113.2
Baseline after / 2	06:28:53.827	304.9	34.5	109.7
Baseline after / 3	06:28:58.386	295.6	34.7	121.7

A dash is an incomplete transfer, not zero speed. Source: data/rounds.csv and per-condition JSON. Byte counts, return codes and HTTP status are retained.

4. DNS, WebRTC and IPv6

Condition	Resolvers	Provider counts	Exact baseline overlap	WebRTC
Baseline after	10	PacketHub: 10	10	No Leak*
Singapore Beta	24	Cloudflare: 21; PacketHub: 3	3	No Leak*
Hong Kong Beta Max	10	Eons Data Communications: 1; PacketHub: 9	9	No Leak*
Hong Kong Sola Max	9	Eons Data Communications: 1; PacketHub: 8	8	No Leak*
Hong Kong 2.0 Max	14	Google: 4; PacketHub: 10	10	No Leak*

DNS used the browser Extended test (six rounds). The new disconnected baseline is collected after the connected tests. Exact resolver overlap is calculated from the original addresses before redaction. Provider/city strings are the test site database labels, not independently proved operator ownership or physical location.

The connected Hong Kong profiles retained PacketHub resolvers also seen on the baseline, alongside Eons Data Communications (Beta/Sola) or Google (2.0). This establishes baseline-overlapping DNS resolution, not an all-clear result. Because the upstream router VPN remained active, the capture did not isolate host DNS routing, browser DNS behavior, upstream resolver forwarding or the physical ISP.

* BrowserLeaks reported No Leak in each observed normal-session test; public STUN and HTTP addresses matched in the visible result. Hong Kong pages did not expose a literal LAN address. Singapore used an mDNS local candidate. This is a test of this browser/configuration, not proof for every application or all UDP traffic. The disconnected baseline also says No Leak, illustrating why the website label alone is insufficient.

The IPv6 feature was off. Forced curl --ipv6 requests to api6.ipify.org and Cloudflare trace returned code 6 on all three Hong Kong profiles: no usable IPv6 destination was resolved in this configuration. BrowserLeaks showed no public IPv6 address there. A missing native IPv6 path limits leak-test coverage and is not proof that an enabled dual-stack deployment is safe.

Singapore api6 returned an IPv6-formatted reported address over a curl connection whose remote socket address was IPv4. This is not treated as proof of native host IPv6 transport or an IPv6 leak. No microphone, camera or location permissions were granted.

5. High-priority finding: crash-time fallback

Finding LC-01 | High, analyst-assigned; no CVSS score claimed. Preconditions: installed 2.6.2+3162, Safe Mode, Network Adapter Mode on, one selected Hong Kong profile, existing upstream router VPN. Action: terminate only the verified C:\Program Files\SingLinkVPN\singcore.exe process, without manually disconnecting first.

An independent curl Cloudflare trace ran approximately once per second with a 3-second timeout. The baseline address was compared exactly. Successful post-stop requests used that same baseline address in all three profiles. The failure is loss of the local VPN boundary under this specific crash, even though the upstream VPN still masks the physical ISP.

Profile	Stop time +08	First fallback request	Fallback samples	Observed span s
Hong Kong Beta Max	06:26:45.718	06:26:46.488	27	26.1
Hong Kong Sola Max	06:21:14.332	06:21:14.907	18	17.0
Hong Kong 2.0 Max	06:23:49.066	06:23:49.405	16	15.0

These are request start times and finite sampled spans, not packet-level leak latency or a continuous all-traffic duration. In-flight requests, scheduler timing and sampling gaps limit precision. All profiles were recovered via the normal client control and a Hong Kong exit was observed again.

During Sola/2.0 crash observation, screenshots still displayed Connected with Detecting in the top status; Beta eventually showed Not connected. The exact UI transition duration was not continuously recorded. A manual end-of-test disconnect is a separate action and is not counted as a kill-switch failure.

Recommended fix: maintain traffic blocking independently of the core process lifetime; gate user-traffic routes until authenticated tunnel readiness; keep UI protection state aligned with actual route availability. Retest core crash, helper failure, sleep/resume, Wi-Fi changes and node switching using fresh TCP, UDP, DNS and IPv6 canaries on an isolated non-VPN upstream. No firewall or product-code modifications were made in this assessment.

6. Installed binary and local surface checks

Executable	Authenticode	SHA-256
singcore	Valid	626E9E1B97F3E2734578FF33FF534E92F025E3BF5012D7756A8E153BF042CCC7
SingCoreHelperService	Valid	99F9863DA2B02EA72840FF6C6AEE9455C0E34498A3A46AA90259F751A09ABF27
SingLinkProxyGuard	Valid	40A6516460AF96D892F533A53F21C3806D560392B30FAC5F2FF3B6E78CA055B5
SingLinkVPN	Valid	2224703B8D49552708E41C1D373158A115B3ABBE726DB6E99D67D5F5013459DA

Windows Authenticode returned Valid for all four running executables with publisher SingLink LLC. This validates the observed signatures under current Windows trust, not software absence of vulnerabilities, source correspondence, update-signature enforcement or dependency integrity.

The executable-file ACL snapshot showed ReadAndExecute/Synchronize for BUILTIN\Users, without a write ACE on these four files. Parent directories, DLL search order, service IPC authentication, named pipes and privilege escalation were not exhaustively tested.

Protocol	Local binding	Process
TCP	fdfe:dcba:9876::1:15478	20204
TCP	127.0.0.1:36936	23092
TCP	127.0.0.1:23410	5596
TCP	198.18.0.1:15477	20204
TCP	127.0.0.1:7897	20204
UDP	127.0.0.1:7897	20204

No wildcard TCP/UDP listener was observed in the selected process snapshot. Bindings were loopback or tunnel-local addresses. This local snapshot does not prove that another host cannot reach a service; no external reachability scan or authentication exploit was performed. PID values refer to the snapshot and change when a core restarts.

7. Assurance boundaries, evidence and next steps

The UI labels Beta, Sola and 2.0 identify selected product profiles. No deployed outer-tunnel handshake/cipher was independently decoded. End-to-end HTTPS certificate/TLS metadata describes the destination HTTPS connection and cannot establish the VPN outer cipher. The Japan AES-256 upgrade described by the user is recorded as a user statement, not downgraded to AES-128 and not falsely marked independently verified.

No packet capture or decryption was performed in this new live run. No interception certificate was installed. Therefore this run does not establish outer-tunnel plaintext absence, replay resistance, forward secrecy, handshake authentication, server logging behavior or a no-logs policy. A source audit is not substituted for those deployment checks.

Coverage completed: real UI connection and host exit checks, three-run throughput, short HTTP probes, six-round browser DNS for Hong Kong, browser WebRTC, forced-IPv6 checks under IPv6-off configuration, controlled core-crash fallback/recovery, executable signatures/ACLs, local listeners and sampled resources. No clean bill of health is issued.

Still needed for broader assurance: isolated dual-stack upstream; packet-scoped canaries without collecting unrelated applications; binary-to-source provenance; deployed protocol cryptographic audit/fuzzing; update/rollback and IPC attack tests; server-side configuration, access controls and logging review; longer stability and cross-platform tests. These are explicitly untested, not passed.

Evidence: data/rounds.csv; per-condition JSON; dns_webrtc.json; fault_summary.json and timestamped watch samples; installed_security.json; resource_summary.json; English client crops with original-image hashes; raw_source_hashes.csv. Methods are included. Full originals remain local and are not in the share ZIP.

Privacy processing is explicit: account/avatar/IP header cropped from client screenshots; exit and resolver identifiers pseudonymized in shared structured data; original source hashes retained. Screenshots are not machine-translated or synthesized. A mistakenly selected non-target node attempt was quarantined locally and excluded from Hong Kong metrics.

The client was left manually disconnected at the end, matching its initial connection state; Safe Mode and existing security settings were retained. Only synthetic transfer data and ordinary test requests were sent to the named measurement services; no account credentials or collected evidence were uploaded to those services.

English screenshot evidence / genuine UI crops

Account/IP header omitted. Original SHA-256 and capture time: evidence/*.json. English Japan/Singapore images are later retakes.

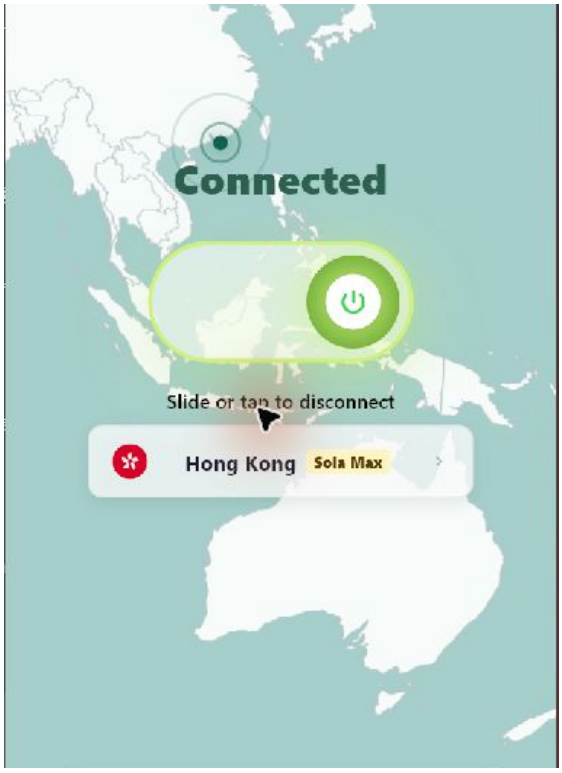
Hong Kong Beta Max / initial connected state

2026-11-16T22:16:38.447Z



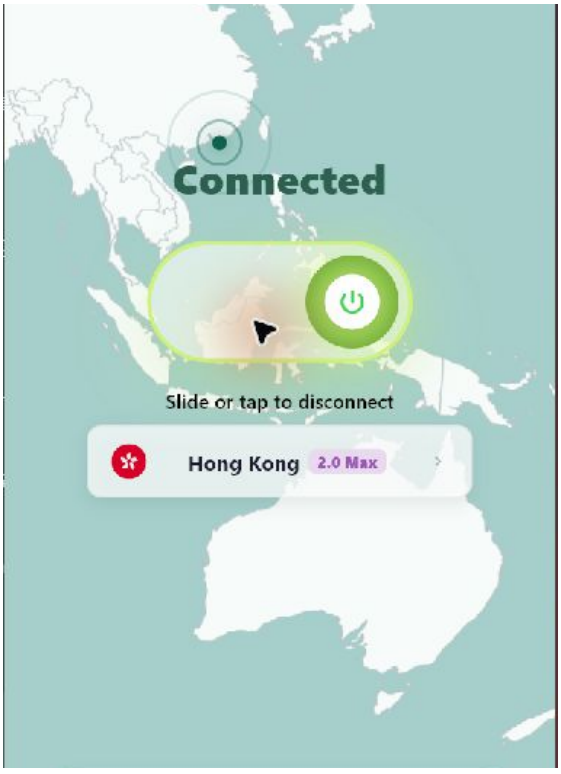
Hong Kong Sola Max / connected state

2026-11-16T22:19:52.788Z



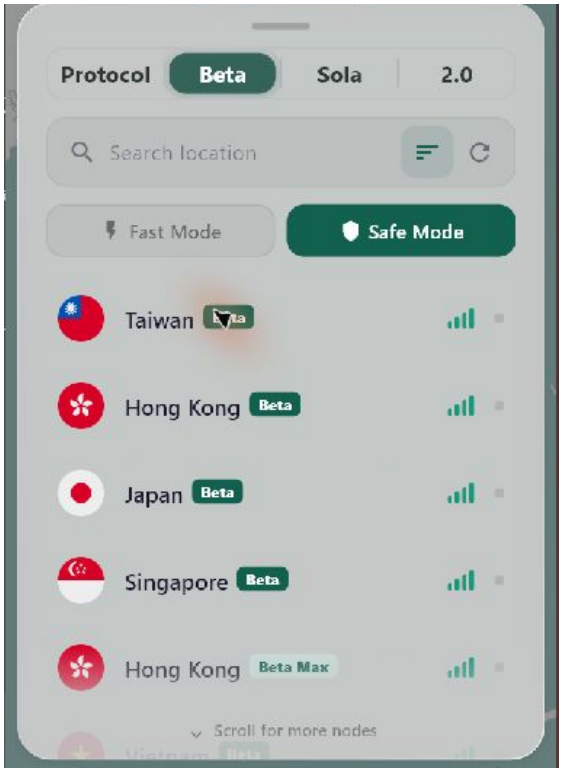
Hong Kong 2.0 Max / connected state

2026-11-16T22:22:18.662Z



Beta protocol filter / Safe Mode selected

2026-11-16T22:24:32.150Z

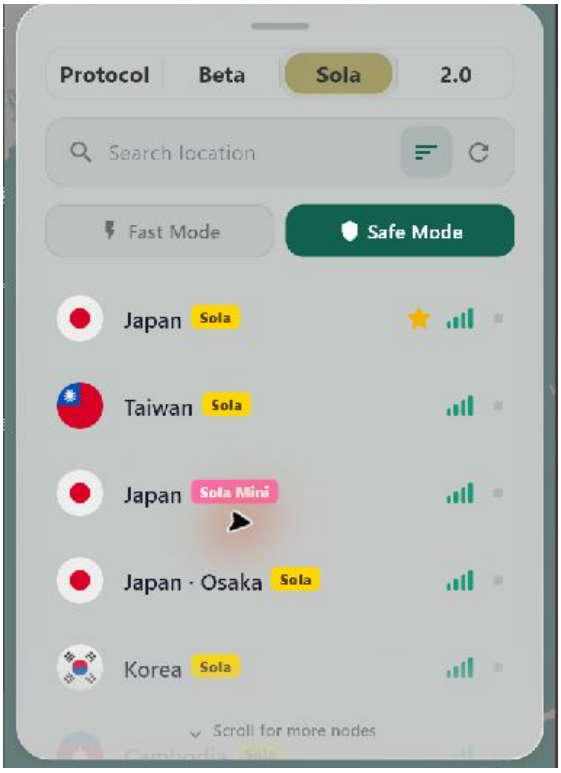


English screenshot evidence / genuine UI crops

Account/IP header omitted. Original SHA-256 and capture time: evidence/*.json. English Japan/Singapore images are later retakes.

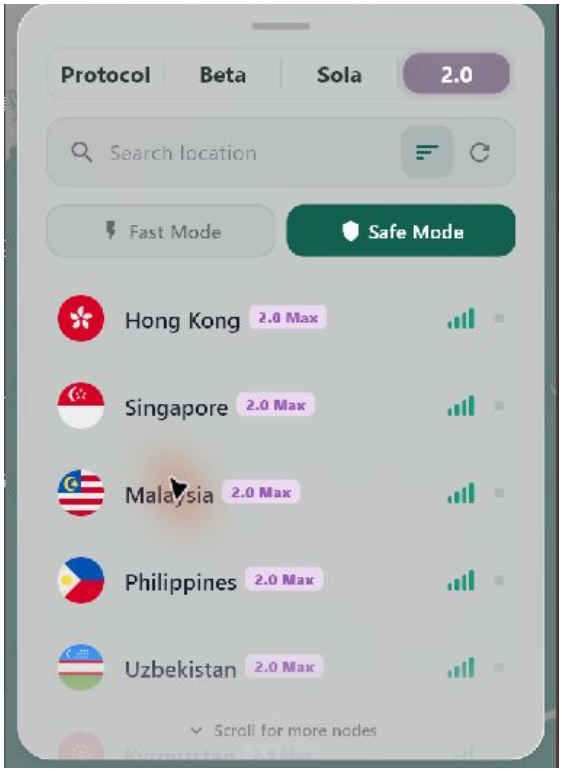
Sola protocol filter / Safe Mode selected

2026-11-16T22:18:28.225Z



2.0 protocol filter / Safe Mode selected

2026-11-16T22:21:52.874Z



Beta after forced core stop / Not connected

2026-11-16T22:26:56.553Z



Sola after forced core stop / Connected, Detecting

2026-11-16T22:21:21.150Z

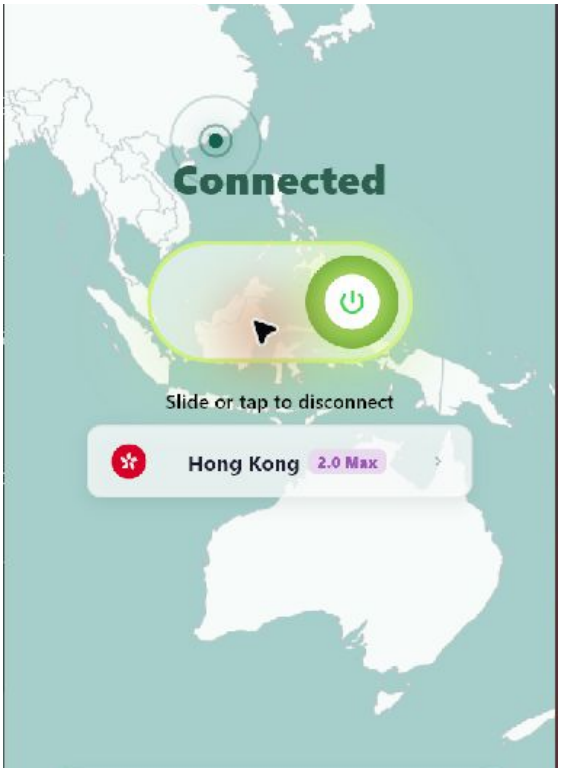


English screenshot evidence / genuine UI crops

Account/IP header omitted. Original SHA-256 and capture time: evidence/*.json. English Japan/Singapore images are later retakes.

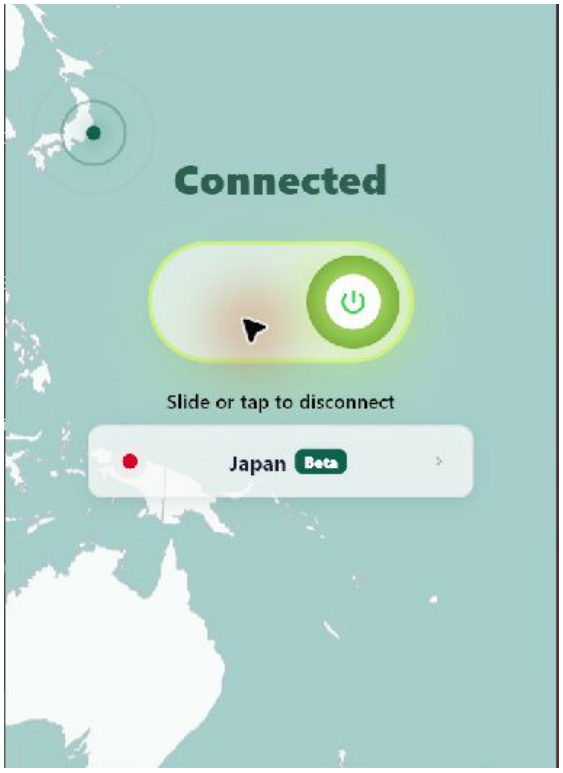
2.0 after forced core stop / Connected, Detecting

2026-11-16T22:23:58.223Z



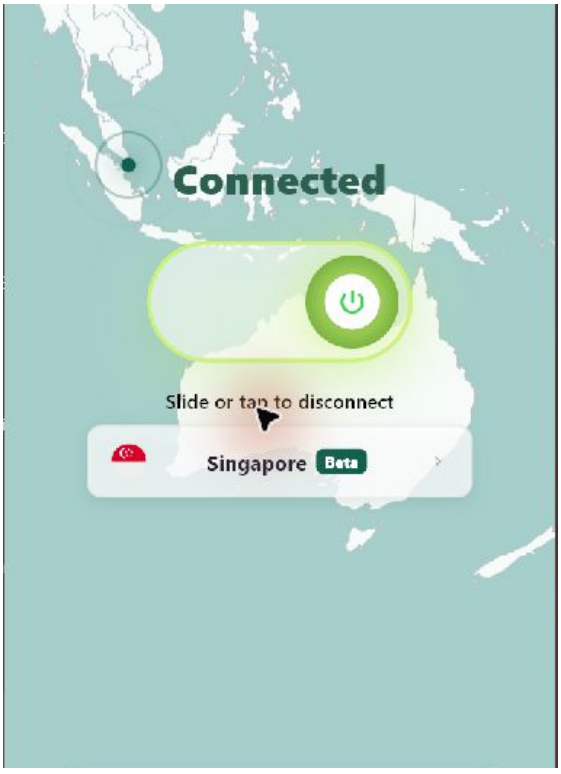
Japan Beta / English retake after original measurement

2026-11-16T22:28:08.964Z



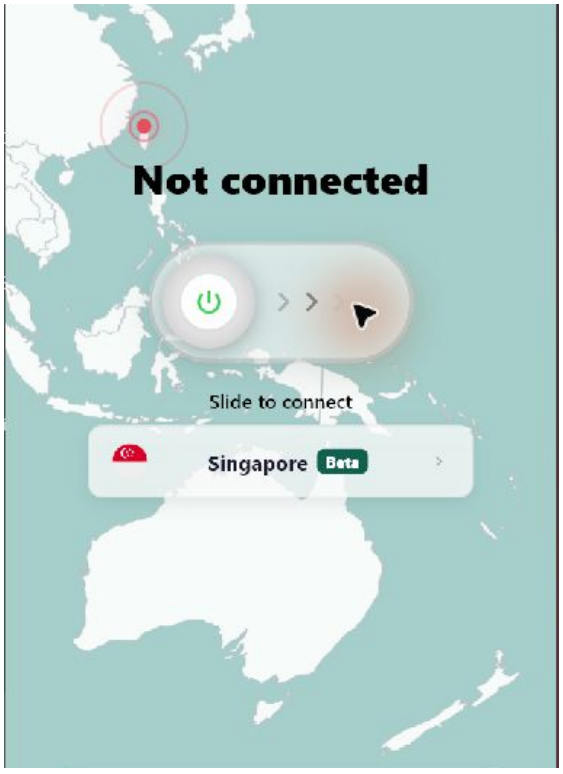
Singapore Beta / English retake after original measurement

2026-11-16T22:28:34.856Z



Final state / manual disconnect for baseline

2026-11-16T22:28:48.558Z



English browser evidence / Hong Kong Beta Max

Original English pages. Gray blocks mask IP fields; metadata records original hashes and crop boxes. DNS address comparison uses the private originals, not the masked image.

DNS Extended / six rounds

Your public IP: [redacted]

Test complete

Query round	Progress...	Servers found
1	.....	4
2	.....	6
3	.....	5
4	.....	6
5	.....	4
6	.....	6

IP	Hostname	ISP	Country
[redacted]	None	Eons Data Communications	Kwai Chung, Hong Kong
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan

WebRTC / normal-session result

WebRTC Leak Test

Your Remote IP :	
IPv4 Address	[redacted]
IPv6 Address	-
WebRTC Support Detection :	
RTCPeerConnection	✓ True
RTCDataChannel	✓ True
Your WebRTC IP :	
WebRTC Leak Test	✓ No Leak
Local IP Address	-
Public IP Address	[redacted]

English browser evidence / Hong Kong Sola Max

Original English pages. Gray blocks mask IP fields; metadata records original hashes and crop boxes. DNS address comparison uses the private originals, not the masked image.

DNS Extended / six rounds

Your public IP: [redacted]

Test complete

Query round	Progress...	Servers found
1	.....	3
2	.....	3
3	.....	4
4	.....	5
5	.....	5
6	.....	4

IP	Hostname	ISP	Country
[redacted]	None	Eons Data Communications	Kwai Chung, Hong Kong
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan

WebRTC / normal-session result

WebRTC Leak Test

Your Remote IP :	
IPv4 Address	[redacted]
IPv6 Address	-
WebRTC Support Detection :	
RTCPeerConnection	✓ True
RTCDataChannel	✓ True
Your WebRTC IP :	
WebRTC Leak Test	✓ No Leak
Local IP Address	-
Public IP Address	[redacted]

English browser evidence / Hong Kong 2.0 Max

Original English pages. Gray blocks mask IP fields; metadata records original hashes and crop boxes. DNS address comparison uses the private originals, not the masked image.

DNS Extended / six rounds

Your public IP: [redacted]

Test complete

Query round	Progress...	Servers found
1	.....	5
2	.....	5
3	.....	5
4	.....	6
5	.....	5
6	.....	5

IP	Hostname	ISP	Country
[redacted]	None	Google	Hong Kong, Hong Kong
	None	Google	Hong Kong, Hong Kong
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	Google	Hong Kong, Hong Kong
	None	Google	Hong Kong, Hong Kong

WebRTC / normal-session result

WebRTC Leak Test

Your Remote IP :	
IPv4 Address	[redacted]
IPv6 Address	-
WebRTC Support Detection :	
RTCPeerConnection	✓ True
RTCDataChannel	✓ True
Your WebRTC IP :	
WebRTC Leak Test	✓ No Leak
Local IP Address	-
Public IP Address	[redacted]

English browser evidence / Disconnected baseline

Original English pages. Gray blocks mask IP fields; metadata records original hashes and crop boxes. DNS address comparison uses the private originals, not the masked image.

DNS Extended / six rounds

Your public IP: [redacted]

Test complete

Query round	Progress...	Servers found
1	.....	4
2	.....	5
3	.....	4
4	.....	5
5	.....	5
6	.....	5

IP	Hostname	ISP	Country
[redacted]	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan
	None	PacketHub	Taipei, Taiwan

WebRTC / normal-session result

WebRTC Leak Test

Your Remote IP :	
IPv4 Address	[redacted]
IPv6 Address	-
WebRTC Support Detection :	
RTCPeerConnection	✓ True
RTCDataChannel	✓ True
Your WebRTC IP :	
WebRTC Leak Test	✓ No Leak
Local IP Address	-
Public IP Address	[redacted]