星連VPN Windows 實機安全與性能測試

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

測試日期：2026 年 11 月 17 日，UTC+08:00。本報告使用新採集的已安裝客戶端證據；開源協議及原型軟體審計另行交付。

結論：宣稱異常斷線保護前須先修復

香港三種協議設定在受控 singcore.exe 核心崩潰測試中，均有 HTTPS 請求成功回退至未連線基準出口。就此次核心崩潰情境，未達流量封鎖預期。基準本身經過上游路由器 VPN，未證實暴露實體寬帶出口。

香港三種設定的正常連線 WebRTC 均顯示 No Leak。DNS 出現與基準重疊的混合解析器。這些結果不能支持不附條件的整體安全通過。

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

僅完整傳輸計入吞吐中位數。Beta 初測有兩次 40 秒逾時；後續複測另列。數值為補充性 HTTPS 測量，並非固定伺服器的線路容量測速。

本次為使用者委託、使用者提供的付費帳號測試；使用者表示自行付費，未查驗付款憑證。這是限定範圍的實測評估，並非認證或獨立伺服器無日誌審計。

1. 對象、環境與測試方法

對象為已安裝 SingLinkVPN.exe，版本 2.6.2+3162；Windows 11 Pro build 26200，i7-12700H，14 核心 / 20 邏輯處理器，可見記憶體約 63.8 GiB。Windows 顯示 Wi-Fi 連線速率 2.2 Gbps，這不是網際網路實測吞吐。

原設定已選 Safe Mode，Network Adapter Mode 開啟、IPv6 選項關閉、Smart 開啟；未變更這些安全設定。開始時帳號顯示 Max、到期日無限、剩餘 15.97 GB / 100 GB；到期日無限不等於流量無限。

使用者確認電腦在台灣，且 Wi-Fi 路由器另有 VPN，測試未修改路由器。前後未連線基準代表上游 VPN 路徑，不能當作無 VPN 的實體 ISP 基準。系統另有 VPN 網卡，盤點時顯示未連線。

每個性能情境測三輪：向 speed.cloudflare.com 下載 50,000,000 bytes、上傳 10,000,000 bytes 自產隨機資料；每輪五次零負載新連線計算 HTTP 首位元組時間 TTFB。保留 curl 憑證驗證，每個請求上限 40 秒。

透過桌面客戶端介面實際連線；每輪前後的 Cloudflare trace 提供本機觀測的出口、國別及機房代碼。--noproxy * 僅停用明確指定的 HTTP 代理，不會繞過 Windows TUN 路由。HTTP TTFB 不能稱為 ICMP RTT、抖動或 Speedtest 延遲。

Cloudflare 使用 anycast，機房可能隨路由改變。本報告未採用固定伺服器的 Ookla 測速，不把結果換算成正式速度保留率，也不由單點性能推論協議設計優劣。

提供的測試規範作為參考文件，不當作擴大操作授權。本次加速單台 Windows 實測不宣稱涵蓋多平台、全程錄影、一小時耐久、串流 / P2P，或完整密碼學審計。

2. 性能與可靠性

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

香港 Beta Max 初測兩次下載分別只收到 14,318,060、2,670,583 / 50,000,000 bytes 就逾時；只有第三次完成（32.816 Mbps）。三次上傳為 2.908、4.532、85.389 Mbps。各組五次 TTFB 請求均成功，顯示小請求成功不代表長傳輸成功。

核對後的 Beta Max 複測使用與初測相同的香港出口，三次下載均完成。兩組資料都保留，複測不能抹去初測失敗；時間、負載、上游 VPN 和目的端行為均可能影響，尚未隔離根因。

日本、新加坡 Beta 為同一實機測試較早的區域補充數據。兩地英文客戶端畫面約於 06:28 真實重連補拍，晚於原性能測試，不冒充原測速當下的畫面。

日本初測的內建網路工具顯示 Apple 59 ms、Google 57 ms。這屬客戶端自報、原語言截圖，不作為英文證據組的獨立延遲結果。

吞吐測試期間資源觀測

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 由相鄰程序累計 CPU 秒數差值除以實際時間，再按 20 邏輯處理器正規化。RSS 為四程序工作集相加，可能重複計入共享頁；短窗口樣本少。日本測速早於資源採樣，沒有可比負載數據。

3. 保留的每一輪性能數據

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 與 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 使用瀏覽器 Extended test 六輪，連線測試後重新建立未連線基準。地址遮蔽前以原始值計算解析器精確重疊；業者 / 城市為測試網站資料庫標籤，未獨立證實實際營運者或物理位置。

香港連線設定仍見到基準中的 PacketHub 解析器，同時有 Eons Data Communications（Beta / Sola）或 Google（2.0）。可確認 DNS 與基準重疊，不能判定完全通過；因上游路由器 VPN 仍開啟，未隔離本機 DNS 路由、瀏覽器 DNS、上游轉送及實體 ISP 的影響。

* BrowserLeaks 正常連線測試均標示 No Leak，當時頁面可見的公網 STUN 與 HTTP 地址相符。香港頁面未顯示明文 LAN 地址，新加坡使用 mDNS 本機候選。這只驗證此瀏覽器及設定，不能代表所有應用或全部 UDP。未連線基準亦標示 No Leak，說明不能只依網站標籤判斷 VPN 是否安全。

IPv6 功能原為關閉。三種香港設定強制 curl --ipv6 請求 api6.ipify.org 及 Cloudflare trace 均回傳代碼 6，該設定無可用 IPv6 目的地址解析，BrowserLeaks 亦未顯示公網 IPv6。缺少原生 IPv6 路徑限制了驗證能力，不能證明開啟雙棧後仍安全。

新加坡 api6 經 curl 遠端 socket 為 IPv4 的連線回傳 IPv6 格式地址，不能據此當作原生本機 IPv6 傳輸或 IPv6 洩漏。未授予麥克風、攝影機或定位權限。

5. 優先問題：核心崩潰時流量回退

問題 LC-01 | 分析者評定高優先級，未宣稱 CVSS 分數。前提：2.6.2+3162、Safe Mode、Network Adapter Mode 開啟、選取香港協議設定、上游路由器 VPN 存在。操作：先不手動斷開，僅結束已核對路徑 C:\Program Files\SingLinkVPN\singcore.exe 的核心程序。

獨立 curl Cloudflare trace 約每秒一次，每請求上限 3 秒；使用原始地址精確比對基準。三種設定均在停止核心後成功經相同基準地址出站。問題是此次核心崩潰時本機 VPN 邊界失效，儘管上游 VPN 仍遮蔽實體 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

表中為請求起始時間及有限採樣跨度，不是封包級洩漏延遲，也不是全部流量連續暴露時長；在途請求、排程及採樣空隙限制精度。三種設定都已透過正常客戶端控制恢復，並再次觀察香港出口。

Sola / 2.0 故障觀察截圖仍顯示 Connected，頂部為 Detecting；Beta 後來顯示 Not connected。未連續錄影取得完整介面轉換時間。測試結尾的手動斷開另行記錄，不算入斷網保護失敗。

建議：讓流量封鎖獨立於核心程序生命週期，經驗證隧道就緒後才放行使用者路由，並同步介面保護狀態與實際路由。修復後在無上游 VPN 的隔離網路，以新 TCP、UDP、DNS、IPv6 測試流量複測核心崩潰、輔助服務故障、睡眠喚醒、Wi-Fi 切換及節點切換。本次未修改防火牆或產品程式。

6. 已安裝程式與本機介面檢查

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

Windows Authenticode 對四個運行程式均回報 Valid，發行者為 SingLink LLC。這驗證目前 Windows 信任下的觀測簽章，不代表無漏洞、與開源碼一致、更新必定驗章或所有依賴完整可信。

四個執行檔的 ACL 快照中，BUILTIN\Users 為 ReadAndExecute / Synchronize，未見寫入 ACE。未全面測試父目錄、DLL 搜尋順序、服務 IPC 認證、命名管道或提權。

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

該程序快照未見 TCP / UDP wildcard 監聽；地址為 loopback 或隧道本機地址。單台快照不能證明其他主機一定不可達，未進行外部可達性掃描或認證漏洞利用。PID 對應快照，核心重啟後會改變。

7. 驗證邊界、證據與後續處理

Beta、Sola、2.0 為實際選取的產品設定標籤。未獨立解析部署中隧道外層握手 / 加密套件；目的站 HTTPS 憑證及 TLS 資料不能證明 VPN 外層演算法。使用者表示日本已升級 AES-256，記為使用者說明，不誤寫為 AES-128，也不冒稱已獨立驗證。

本次新實機測試未抓包或解密，未安裝攔截憑證。因此不能由本次資料證明隧道外層無明文、抗重放、前向保密、握手認證、伺服器記錄內容或無日誌政策；也不以開源碼審計替代部署驗證。

已完成：真實介面連線與本機出口核對、三輪吞吐、短 HTTP 請求、香港六輪瀏覽器 DNS、WebRTC、IPv6 關閉設定下的強制 IPv6 檢查、受控核心崩潰回退與恢復、執行檔簽章 / ACL、本機監聽與資源採樣。不出具整體安全無問題結論。

要擴大安全保證，仍需：隔離雙棧上游、能排除其他程式流量的限定封包測試、二進位與原始碼溯源、部署協議密碼學審計 / 模糊測試、更新回滾與 IPC 攻擊面、伺服器設定 / 權限 / 記錄審查、較長穩定性及跨平台測試。這些明列未測，並非通過。

證據：data/rounds.csv、逐情境 JSON、dns_webrtc.json、fault_summary.json 及逐筆時間戳觀測、installed_security.json、resource_summary.json、附原圖雜湊的英文客戶端裁切圖、raw_source_hashes.csv；另附方法程式。完整原始資料保留本機，不納入分享 ZIP。

隱私處理明確標示：客戶端截圖裁去帳號 / 頭像 / IP 頂欄，分享結構資料使用出口及解析器代號，保留原始來源雜湊。截圖未機器改字或生成。一次誤選非目標節點的資料保留在本機隔離區，不計入香港數據。

結尾客戶端手動保持未連線，與初始連線狀態相符；保留 Safe Mode 和原安全設定。僅向上述測試服務送出自產傳輸資料及一般測試請求，未上傳帳號憑證或採集的證據。

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.

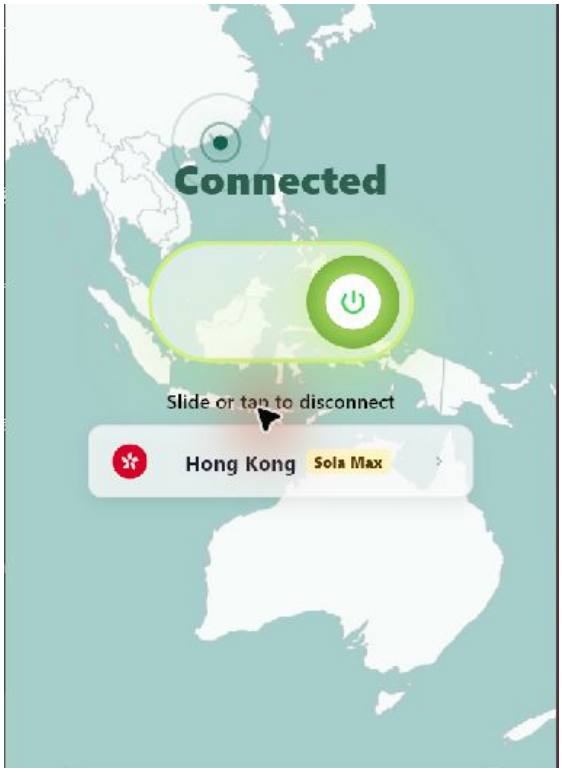
Hong Kong Beta Max / initial connected state

2026-11-16T22:16:38.447Z



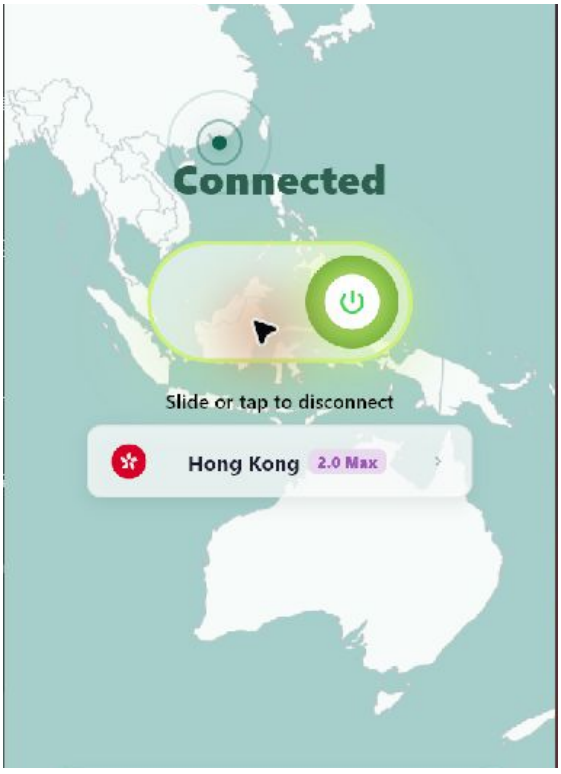
Hong Kong Sola Max / connected state

2026-11-16T22:19:52.788Z



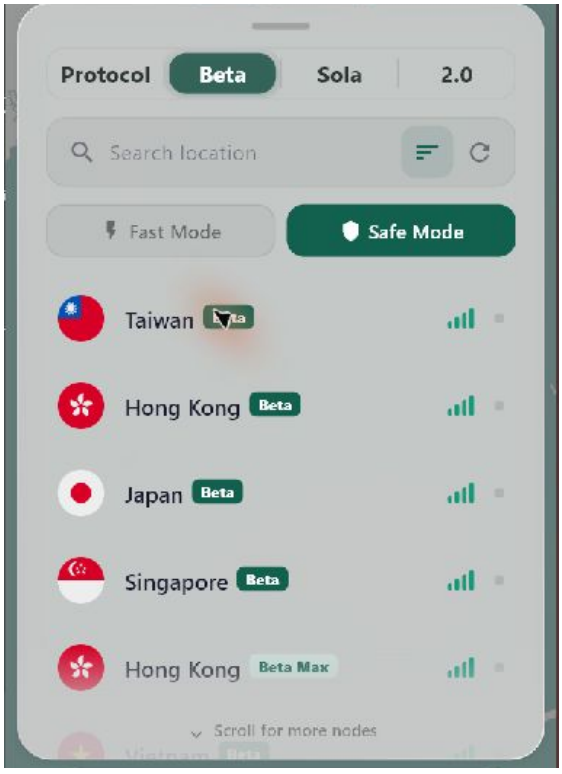
Hong Kong 2.0 Max / connected state

2026-11-16T22:22:18.662Z



Beta protocol filter / Safe Mode selected

2026-11-16T22:24:32.150Z

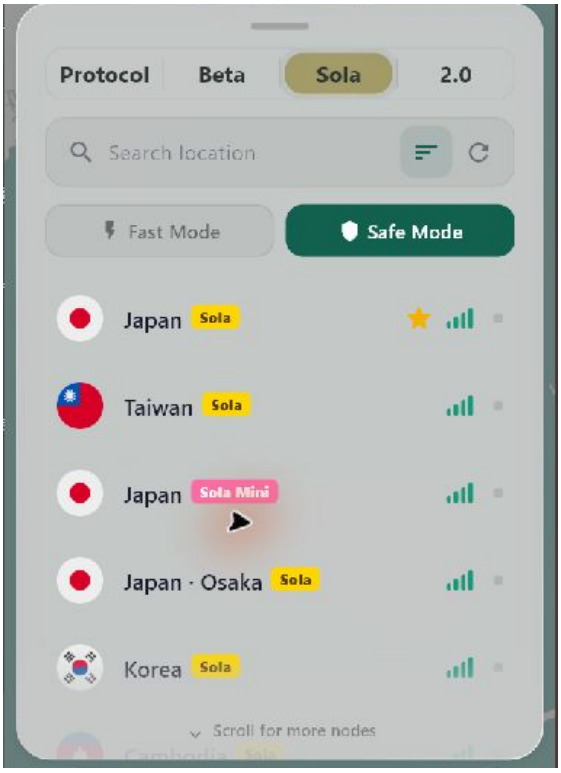


English screenshot evidence / genuine UI crops

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

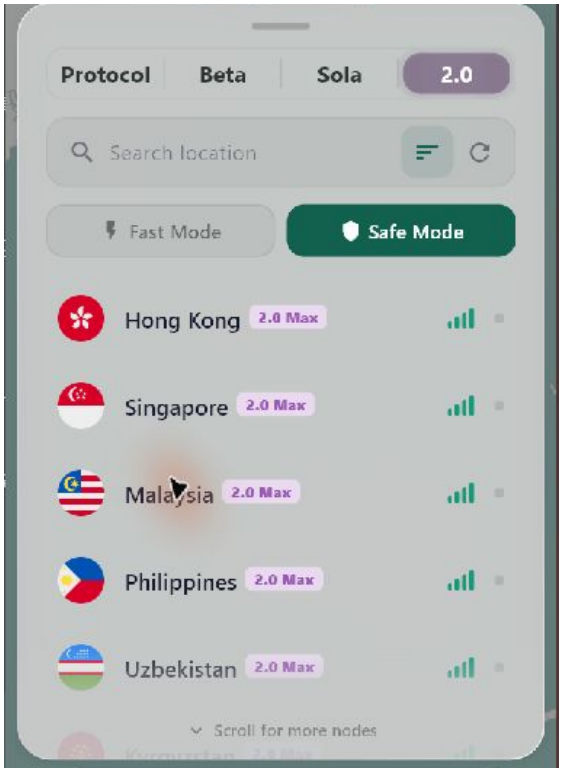
Sola protocol filter / Safe Mode selected

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

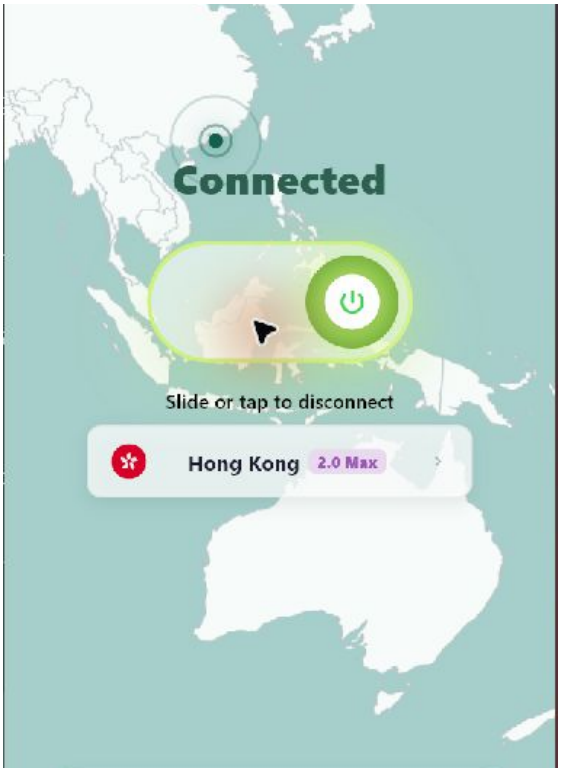


English screenshot evidence / genuine UI crops

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

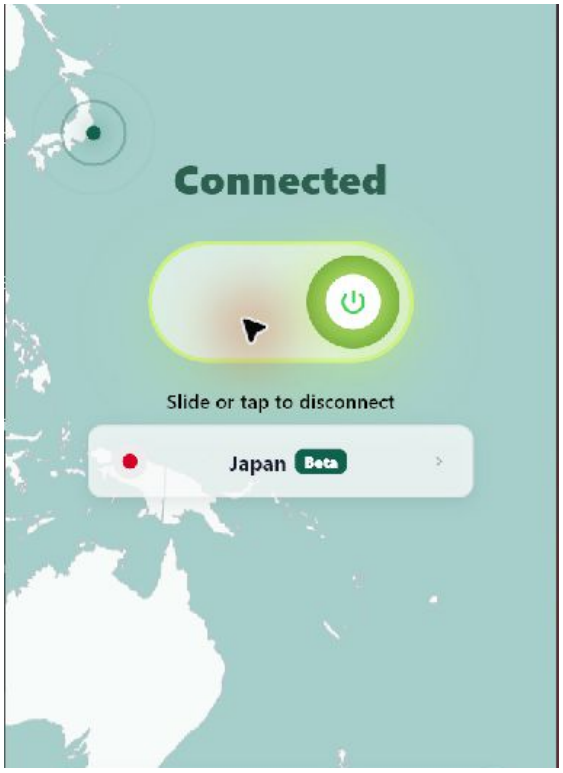
2.0 after forced core stop / Connected, Detecting

2026-11-16T22:23:58.223Z



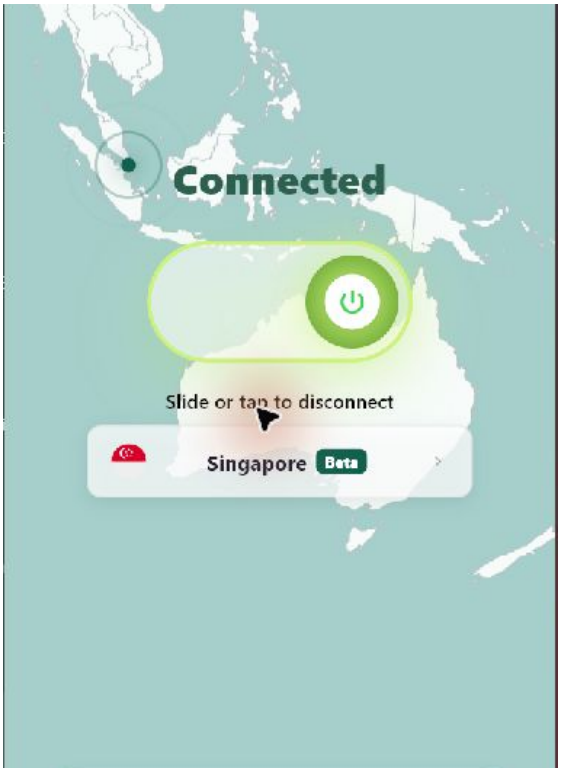
Japan Beta / English retake after original measurement

2026-11-16T22:28:08.964Z



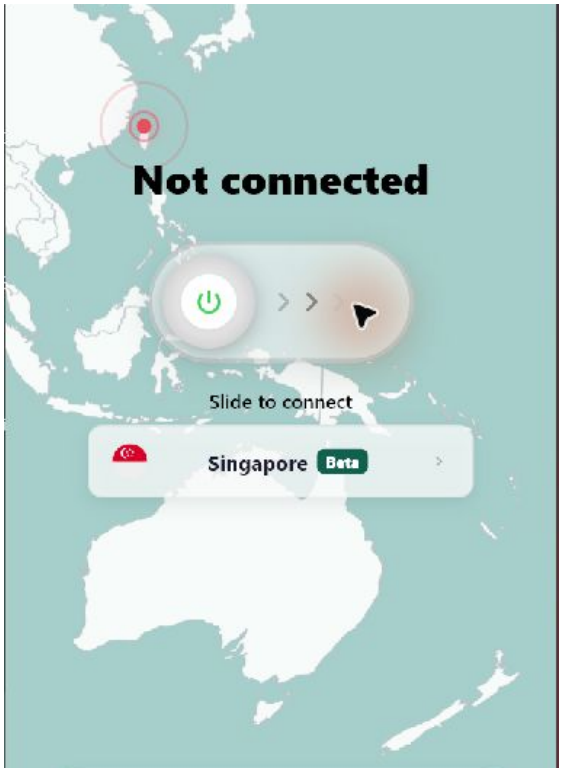
Singapore Beta / English retake after original measurement

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]