mySites.guru

home.pl Refuses to Unblock mySites.guru, the First Host to Turn Us Down

home.pl drops both of mySites.guru's published IPs across its network and on 2 November 2026 would not lift it, the first host to turn down our direct request.

Phil E. Taylor | 3 November 2026

Since about 04:36 UTC on 14 October 2026, home.pl, one of Poland's largest web hosts, has been dropping every packet from the address mySites.guru runs its uptime checks from. Sometime in the second half of October it began dropping our worker address as well, so audits, backups and updates to home.pl-hosted sites fail too. The drop is network-wide: TCP connections time out and ping gets no reply, on each home.pl webhosting server we have tested, from both of our published addresses. On 2 November we asked home.pl to allow-list those two addresses. At 10:44 UTC its abuse desk said it was working on that. At 14:32 UTC a second reply said no.

In more than a decade of running mySites.guru, home.pl is the first host to turn down our own direct request to unblock our published addresses across its network, and to give our history with it as the reason. Other hosts have insisted on per-customer tickets, or have blocked us by accident and fixed it when asked. None has looked at the full technical picture, including the fact that Cloudflare lists mySites.guru as a verified agent, and said no. home.pl did, and this post is what that looks like from our side, what home.pl claimed, what our logs show, and what it means for home.pl customers.

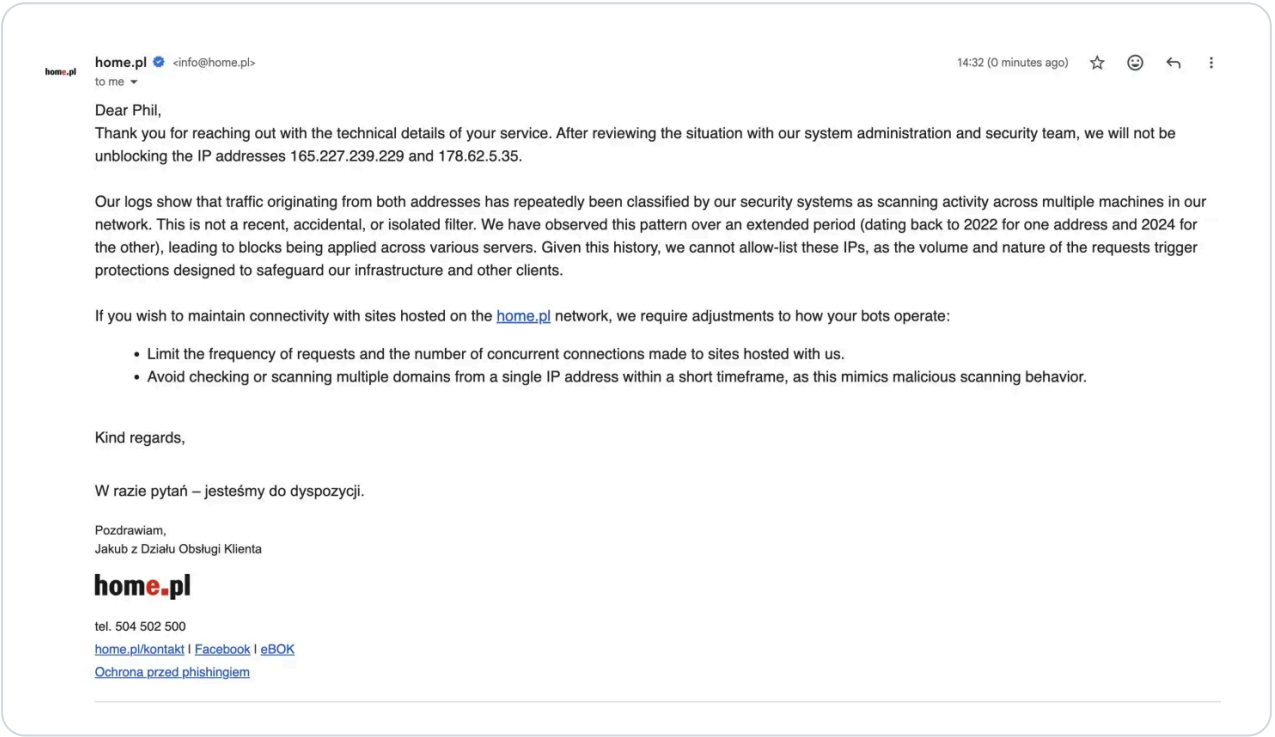
What home.pl Told Us

My email to abuse@home.pl, the abuse mailbox home.pl publishes in RIPE for its webhosting ranges, went out at 09:22 UTC on 2 November. It explained what mySites.guru is, gave both addresses and what each one does, the User-Agent `mySites/6.0 (+https://mysites.guru/bot/)`, the Ed25519 Web Bot Auth signing on connector requests, when each address stopped getting through, and five home.pl server IPs we had tested against, such as 89.161.251.66 (hd898.home.net.pl). It linked our page for web hosts and our service traffic page. It ended with an offer: "If something in our traffic triggered the block, please tell me what was seen and when, and I will fix it on our side."

The first reply, at 10:44 UTC, was encouraging. The abuse desk wrote: "I have already escalated your ticket … directly to our network administration team. They are currently investigating the root cause of the block and working on allow-listing the specified IP

addresses." It added: "I will also let you know if any specific traffic patterns triggered this automated block." So at 10:44 it was an automated block, under investigation, with allow-listing in progress.

The second reply came from info@home.pl at 14:32 UTC, under four hours later, with the subject "Odp: Request to allow-list 178.62.5.35 and 165.227.239.229 (mySites.guru) on the home.pl network". Here it is in full.



home.pl <info@home.pl> 14:32 (0 minutes ago)
to me

Dear Phil,
Thank you for reaching out with the technical details of your service. After reviewing the situation with our system administration and security team, we will not be unblocking the IP addresses 165.227.239.229 and 178.62.5.35.

Our logs show that traffic originating from both addresses has repeatedly been classified by our security systems as scanning activity across multiple machines in our network. This is not a recent, accidental, or isolated filter. We have observed this pattern over an extended period (dating back to 2022 for one address and 2024 for the other), leading to blocks being applied across various servers. Given this history, we cannot allow-list these IPs, as the volume and nature of the requests trigger protections designed to safeguard our infrastructure and other clients.

If you wish to maintain connectivity with sites hosted on the home.pl network, we require adjustments to how your bots operate:

- Limit the frequency of requests and the number of concurrent connections made to sites hosted with us.
- Avoid checking or scanning multiple domains from a single IP address within a short timeframe, as this mimics malicious scanning behavior.

Kind regards,

W razie pytań – jesteśmy do dyspozycji.

Pozdrawiam,
Jakub z Działu Obsługi Klienta

home.pl

tel. 504 502 500
home.pl/kontakt | Facebook | eBOK
Ochrona przed phishingiem

home.pl's reply, 2 November 2026, 14:32 UTC, signed Jakub z Działu Obsługi Klienta (Jakub from Customer Service).

home.pl's reply, word for word

Dear Phil,
Thank you for reaching out with the technical details of your service. After reviewing the situation with our system administration and security team, we will not be unblocking the IP addresses 165.227.239.229 and 178.62.5.35.
Our logs show that traffic originating from both addresses has repeatedly been classified by our security systems as scanning activity across multiple machines in our network. This is not a recent, accidental, or isolated filter. We have observed this pattern over an extended period (dating back to 2022 for one address and 2024 for the other), leading to blocks being applied across various servers. Given this history, we cannot allow-list these

IPs, as the volume and nature of the requests trigger protections designed to safeguard our infrastructure and other clients.
If you wish to maintain connectivity with sites hosted on the home.pl network, we require adjustments to how your bots operate:
Limit the frequency of requests and the number of concurrent connections made to sites hosted with us.
Avoid checking or scanning multiple domains from a single IP address within a short timeframe, as this mimics malicious scanning behavior.
Kind regards,
W razie pytań - jesteśmy do dyspozycji.
Pozdrawiam,
Jakub z Działu Obsługi Klienta

The Polish line means “If you have questions, we are at your disposal.” The reply gives no log lines, no timestamps, no request counts and no example requests. The 10:44 email had promised to share “any specific traffic patterns”, and the 14:32 email, from a different mailbox, shares none. We are told that something was seen, going back years, and that it was serious enough to say no, without being shown a single request. A monitoring service cannot act on that even if it wants to.

I want to be clear about what this exchange was. It was not a form or an automated report. I wrote to home.pl myself, as the founder of mySites.guru, to the abuse mailbox its network publishes, with everything a network team could need to check our traffic, and an open offer to change anything they could show us. That personal, direct approach is the one that has always worked with hosts, and it is the last thing we can do from our side. home.pl flatly said no. We have reached the end of the road with home.pl, and there is nothing more we can do from our side.

When Our Checks Stopped Reaching home.pl

On 14 October at about 04:36 UTC, traffic from our uptime address, 165.227.239.229, to home.pl’s webhosting network stopped getting through. Connections time out at the TCP level and ping gets no reply, which is a network-level drop rather than a web server or firewall answering with an error. Of the 132 sites we monitored on home.pl’s

`*.home.net.pl` servers at the time, 130 went down for us with `ETIMEDOUT`, 113 of them in that same hour. A timeout with no refusal and no HTTP error is the signature of a drop on the network, not of anything on an individual hosting account, and nothing a customer can see or change in their panel.

We diagnosed it on 19 October, from a report by a customer, a Polish Joomla agency, who was getting a daily “site down” reminder for a site that loaded fine. On that date our worker address, 178.62.5.35, still reached home.pl sites; only the uptime checks were blocked. The customer wrote to home.pl, and summed up the host in a sentence: “They are very strict. With limits etc.” Between then and 2 November, on a date we cannot pin down, home.pl began dropping 178.62.5.35 as well. On the morning of 2 November another customer, a Polish public institution, forwarded one of our “Audit Errored” emails and asked which ports the plugin uses, suspecting their own firewall. There are no special ports: everything we do is HTTPS on port 443, and the block was never theirs.

At about 14:40 UTC on 2 November, a few minutes after home.pl’s reply arrived, we re-measured. From 178.62.5.35, TCP connections to port 443 on five home.pl webhosting IPs (89.161.251.66, 89.161.252.48, 89.161.169.160, 89.161.178.61 and 89.161.180.254) all timed out. At 14:42 UTC we ran a control test on a random sample of 12 home.pl-hosted sites from our database. Every site that answered from an ordinary connection (my Mac, on UK broadband) and is still on home.pl’s network (RIPE netname HOMEPL) timed out from both 178.62.5.35 and 165.227.239.229. The only two sites in the sample that did answer our addresses had moved to other Polish hosts, nazwa.pl and Zenbox. The site is up, the host is reachable, and the only variable is which address is asking.

Here are the exact numbers, from the mySites.guru database at 14:55 UTC on 2 November. 256 sites connected to mySites.guru are hosted on home.pl, spread over 159 home.pl servers: 206 Joomla, 49 WordPress and one plain PHP site. 137 of them fail every connection attempt with `CONNECT tunnel failed`, the error our outbound proxy returns when it cannot open a connection to the site at all. Those 137 sit on 75 different home.pl servers: 90 Joomla, 46 WordPress and one plain PHP site. Of the 131 uptime monitors we run on home.pl-hosted sites, 127 currently read DOWN. The failing

sites belong to around twenty mySites.guru customers, mostly Polish agencies and the organisations they look after, including schools and public bodies. Each of those customers chose mySites.guru, installed our connector on their own sites, and is now paying for monitoring and backups their host will not let through.

home.pl's Claims Against Our Logs

home.pl made five claims in its reply. Here is each one, set against what our systems record and where anyone, home.pl included, can check it.

What the home.pl said

> "Traffic originating from both addresses has repeatedly been classified by our security systems as scanning activity across multiple machines in our network."

The facts (on 2 November 2026)

mySites.guru does not scan sites. It calls its own connector plugin, which the site owner installed, and only the endpoints pre-coded into that plugin; the plugin validates each request with a single-use request ID before acting. We do not crawl, follow links or probe a site from the outside. mySites.guru is an audit tool, and it audits from within. A security system that sees requests to many home.pl machines is seeing many home.pl customers who chose the same service.

The source

Every request we send, listed on our service traffic page

What the home.pl said

> "We have observed this pattern over an extended period (dating back to 2022

The facts (on 2 November 2026)

Both addresses are published in plain text, with a contact email in the headers of every request. Whatever home.pl recorded in 2022 and 2024, our uptime checks reached home.pl sites until 04:36 UTC on 14 October 2026, when 113 monitored sites went down in one hour. The

for one address and 2024 for the other).”

reply shows no log line, timestamp or request count from any year.

The source

Our published addresses

What the home.pl said

“ The volume and nature of the requests trigger protections designed to safeguard our infrastructure and other clients.”

The facts (on 2 November 2026)

An uptime check is one HEAD request per site every five minutes with a 0-byte response body. A full day of monitoring one site moves about 598 KB of response headers, spread over 24 hours; one ordinary page view of our own site moves 653 KB across 27 requests. Audits run one at a time per server, and audits, backups and updates only run when the site owner starts or schedules them.

The source

The load comparison on our page for web hosts

What the home.pl said

“ Limit the frequency of requests and the number of concurrent connections made to sites hosted with us.”

The facts (on 2 November 2026)

The frequency is one request per site every five minutes, and a failed check is retried only twice, 10 seconds apart, before a site is reported down. Concurrency is already one audit per server at a time. Our page for web hosts says what happens when a host throttles us instead: rate-limiting the address causes false downtime alerts, so allow-list it rather than throttle it.

The source

Uptime check anatomy on our page for web hosts

What the home.pl said

The facts (on 2 November 2026)

Checking many customer sites from a small, published set of addresses is how monitoring

> “Avoid checking or scanning multiple domains from a single IP address within a short timeframe, as this mimics malicious scanning behavior.”

services work, and it is the only thing that makes an allow-list possible. Spreading our checks across many rotating addresses is what malicious scanners do to avoid being identified. Cloudflare lists mySites.guru as a verified agent under Monitoring & Operations.

The source

Cloudflare's public listing for mySites.guru

The word “scanning” is the heart of home.pl’s case, and it describes something mySites.guru does not do. A scanner works from the outside: it requests URLs it has guessed or discovered, looking for what answers. mySites.guru works from the inside. Each site owner installs our connector plugin, and our audits, backups and updates call that plugin’s own pre-coded endpoints and nothing else, so the checking of files, extensions and settings happens on the server, inside the site, with the owner’s permission. Beyond the plugin, the only requests we send are the uptime check and the handful of fixed URLs a snapshot reads (robots.txt, sitemaps, one header check and the admin URL), every one of them listed on our service traffic page. We do not crawl a site or “scan” it from outside. We are an audit tool, auditing from within.

One more thing sits oddly with home.pl’s answer. home.pl’s own network terms, the Regulamin Sieci home.pl in force since 3 March 2026, say in section 37 that home.pl may impose a temporary block on access to a service (“może dokonać czasowej blokady dostępu do Usługi”) when that is necessary for the customer’s safe use, giving a DDoS or an attack on the customer’s application as examples. That is our reading of a Polish document, not legal advice. But a written answer that it will not unblock two published addresses used by the customers’ own chosen monitoring service does not read like “temporary”, and it is the customers’ access to their own service that is being blocked.

Why We Won’t Change How We Connect for home.pl

home.pl's two demands are, in effect, that mySites.guru stop being a monitoring service. We will not be doing that, for the same reasons that make us easy to allow-list in the first place.

Monitoring services check many customer sites from a small, fixed, published set of addresses. That is the whole design: a host can read the list once, allow it, and never think about it again. Our two addresses have not changed in over a decade, which our page for web hosts says: "These addresses have not changed in over a decade, so they are safe to hard-code." The alternative home.pl asks for, checking different domains from different addresses so that no single IP touches many machines in a short time, is the behaviour of something trying not to be identified. It would make us harder to recognise and harder to allow-list, for every host, to satisfy one. We are not going to make mySites.guru look more like a scanner because one host's filter cannot tell the difference.

There is also nothing left to throttle, starting with the uptime checks. One HEAD request per site every five minutes, 288 a day, with a 0-byte body and a 45 second timeout, is as light as a check can be while still telling the owner their site is down inside five minutes. On failure, and only on failure, we send a second HEAD 10 seconds later and one GET 10 seconds after that; only if all three fail do we report the site down. A day of our monitoring moves about 598 KB of headers; one visitor loading one page moves more. A single visitor costs the server more than we do all day.

Audit, backup and update traffic from 178.62.5.35

The uptime checks are the smaller half of what home.pl blocked. The address it blocked second, 178.62.5.35, is the one that does the real work for the site owner: audits, backups, updates, snapshots and the connection check. All of it goes to one place, the mySites.guru connector the owner installed, at `/plugins/system/bfnetwork/` on Joomla, `/wp-content/plugins/mywpguru/` on WordPress and `/bfnetwork/` on other PHP sites. Nothing else on the site is crawled or followed. Our service traffic page lists every request in a table; here is the part that comes from the worker address:

Request	How often	What it asks for
Connector call (POST, signed)	Snapshots about every 12 hours; audits, backups, updates when the owner runs them	The connector the site owner installed
robots.txt and sitemaps (GET)	With each snapshot	/robots.txt, then up to six sitemap URLs, at most 600 bytes each
Header check (GET)	With each snapshot	One URL that should not exist, to read the security headers
Admin URL (GET)	With each snapshot	/administrator/ on Joomla, /wp-admin/ on WordPress
Certificate check	At most twice a day	A TLS handshake to read the SSL certificate
Favicon (GET)	During an audit only	The home page and its favicon

Most of that is scheduled around the owner, not around us. A snapshot runs about twice a day. An audit, a backup or an update runs when the owner clicks the button or sets a schedule for it, because those are the jobs they pay us for. The scheduling also protects the server: only one audit runs at a time per server, so a home.pl server with many connected sites sees one audit, then the next, never two together, and with the update queue on, only one update runs at a time per account and server. That is the "concurrent connections" limit home.pl asked for, and it was already there.

It is simply not possible to reduce the requests we make any further than we already do. Remember who is making them. home.pl's customers subscribe to mySites.guru and pay for it. They installed the connector, they added their sites, and they are the ones directing our requests at their own websites. Every audit, backup and update home.pl blocks is one its own customer asked for.

Every connector call is signed with Web Bot Auth against our public key, and the connector itself checks each one with a single-use request ID against validate.mysites.guru before it does anything, so a copied or replayed request does nothing. Those signed connector calls are what Cloudflare verified when it listed mySites.guru as a verified agent. An audit is a site owner asking their own site, through software they installed, whether it has been hacked or has known vulnerable extensions. Blocking it does not protect that customer. It leaves them without the security audits and backups they set up.

A monitoring service that hides which address it checks from is not one you can allow-list

home.pl asked us to stop checking many domains from one address. One published address is the only reason an allow-list can exist at all. We will keep connecting the way we always have, and we will keep publishing where from.

What mySites.guru Already Does to Be a Good Neighbour

A host that wants to check whether our traffic is what we say it is has more ways to do that than it has for almost any other automated client on the internet. Each one was in my first email to home.pl.

What we do	How a host
Two fixed addresses, unchanged for over a decade	Read the p manage.m
Forward and reverse DNS match on both addresses	dig the rev (main-worl engine.my then dig it
User-Agent `mySites/6.0 (+https://mysites.guru/bot/)` on every request	grep the a URL explai

What we do	How a host
	request we
`X-Questions: Please email phil@phil-taylor.com` **header on every request**	Email it; a p it
Connector requests signed with Web Bot Auth (RFC 9421, Ed25519)	Verify agai the signatu
Cloudflare verified agent, Monitoring and Operations	Look us up Radar
Only sites whose owner added them; no crawling or indexing	Every requ connector installed
Single-use request IDs validated by the connector before it acts	Check the source on
One audit per server at a time; one uptime HEAD per site per five minutes	Count our the access
A public page written for host support desks	Read info- no login ne

The service traffic page at mysites.guru/bot/ is the URL inside our User-Agent, so anyone who sees our request in a log is one click from it. It says who operates the service (Blue Flame Digital Solutions Limited, in the UK), lists both user agents and both addresses with their reverse DNS names, and sets out in a table every request we send: the method, how often, and what it asks for. It shows how to confirm a request is really from us by checking reverse and forward DNS, how to check the Web Bot Auth signature, and a Cloudflare skip rule for sites behind Cloudflare. It also says how to make us stop: a site owner deletes the monitor or removes the site and the connector, and a server operator who would rather not email the owner can email us and we will contact the owner ourselves. There is a contact section and a dated changelog, because, as the page says, it “is maintained by hand and updated whenever our traffic changes.”

The page for web hosts at manage.mysites.guru/info-for-webhosts is written for a different reader: the person on a host's support or abuse desk who has a ticket open and needs to decide what to do. It describes itself as "the authoritative reference for the exact IP addresses, hostnames and ports involved" and adds: "It is safe to share and contains no customer data." It needs no login. It covers the two inbound addresses, the connector paths that must stay reachable, the anatomy of an uptime check and the load comparison above, the two outbound hostnames a connected site talks to (validate.mysites.guru and cdn.mysites.guru), and how our requests are authenticated. It also anticipates the exact instruction home.pl gave us: "Rate-limiting this IP causes false downtime alerts … Allow-list the address rather than throttling it." A customer can paste that URL into a ticket and the host has everything.

And since 31 October 2026, there is a third party who has already done the checking. Cloudflare lists mySites.guru as a verified agent in its Bots and Agents Directory, classified under Monitoring and Operations and Security Testing, and the listing is public on Cloudflare Radar. Our connector requests are the same signed requests, from the same two addresses, checking many customer sites from one place, that home.pl's security team calls scanning. Cloudflare verified them; home.pl blocked them. A site behind Cloudflare can let us through with a single skip rule from our /bot/ page.

Our uptime checks are not yet signed with Web Bot Auth; the connector requests are, and we said so in the email. Everything else above was in home.pl's hands at 09:22 UTC on 2 November, along with the offer to fix anything they could show us. The answer at 14:32 was still no.

Can You Get Your home.pl Site Monitored Again?

Quite simply, you can't. home.pl has refused flat out. The block is on home.pl's network, in front of every home.pl webhosting server we have tested, and home.pl has told us in writing that it will not allow-list our two addresses. Your site is up and your connector is fine, but nothing you change on your site or in your home.pl panel gets our traffic past that network. home.pl's help pages say security configuration is done by home.pl's

administrators ("Konfiguracja zabezpieczeń realizowana jest przez administratorów home.pl"), and the only customer-facing allow-list we found is inside the paid Ochrona WWW Premium WAF add-on, which configures that add-on's firewall and does nothing about a network-level drop.

While your sites stay on home.pl, mySites.guru cannot audit them, back them up, update them or monitor their uptime. If you want those jobs done, the sites have to move to a host that lets its customers choose their own tools. The two home.pl sites in our sample that answered our addresses today had both moved to other Polish hosts. SiteGround, after a week of blocks, whitelisted both of our addresses across its whole network on 28 October 2026, which is what a host does when it decides its customers' chosen tools should work.

If you do move, tell home.pl why. It told us its blocks protect "other clients". It should hear from those clients what the blocks cost them.

Other Hosts Fixed This; home.pl Chose Not To

Hosts block us from time to time, usually by accident, and the pattern until now has been the same: we explain, they check, they fix it. SiteGround's Anti-Bot AI challenged our worker address for a week in October 2026, and on 28 October SiteGround whitelisted both of our addresses network-wide. OVH once flagged one of our connector files as malware and publicly acknowledged the false positive. Neither host was given anything home.pl was not given, and home.pl was given more: a signed protocol, a page written for its own support desk, a Cloudflare verification that did not exist when the SiteGround blocks began, and an open offer to change anything they could show us.

home.pl is a large company. It has been part of United Internet since 30 December 2015, through 1&1 Internet SE, and today sits inside the IONOS group. By NASK's 2025 annual report it manages 12.47% of .pl domain names, third behind OVH and Aftermarket.pl, and is second by share of .pl domain holders at 14.65%. A host of that size has the staff to read a log and the tools to allow two addresses. What it told us, in writing, after I asked personally, is that it will not.

Think about what that answer means for a home.pl customer. Effectively, home.pl has decided that its customers are no longer allowed to choose the vendors they want to access their own websites. The site owner installed our connector, added the site to mySites.guru and pays for the service, and home.pl has overruled them. What next? The rule home.pl gave us, no checking many domains from one address in a short time, describes Googlebot just as well. Will home.pl block Googlebot from indexing your sites? Or block the services your site talks to while a newsletter goes out, or in the run-up to Christmas, when you are making too many sales? A host decides how its own network is protected. It should not decide which tools its customers may use on their own websites.

Our side of this has not changed and will not. Two published addresses, unchanged for over a decade, with matching reverse DNS. A User-Agent that links to a page listing every request we send. A contact email in every request's headers. Signed connector requests against a public key. A page for hosts that needs no login. And a public verification by Cloudflare that we are what we say we are. If that is not enough for a host to allow-list a monitoring service its own customers chose, the problem is not on our end of the connection.

The bottom line

So the position is this. mySites.guru will not change how it connects for home.pl. home.pl will not allow-list our two addresses, so home.pl customers who want their sites monitored, audited and backed up need a host that will. The ball is in home.pl's hands.

Timeline

30 Dec 2015 — **United Internet completes its purchase of home.pl**
Via 1&1 Internet SE; home.pl is now part of the IONOS group.

14 Oct 2026 — **home.pl starts dropping our uptime IP**

About 04:36 UTC, 165.227.239.229 stops reaching home.pl's webhosting network. 113 monitored home.pl sites go down for us in the same hour.

19 Oct 2026

We diagnose the block from a customer report

Daily down reminders for a site that loads fine. The worker IP still gets through; the customer writes to home.pl.

Late Oct 2026

home.pl drops the worker IP as well

Sometime between 19 October and 2 November, 178.62.5.35 stops getting through too, so audits, backups and updates fail.

2 Nov 2026, 08:40 UTC

A customer asks which ports to open

They suspected their own firewall. There are no special ports; the block is home.pl's.

2 Nov 2026, 09:22 UTC

We ask home.pl to allow-list both addresses

Full technical detail, the info-for-webhosts and /bot/ pages, and an offer to fix anything on our side if they show us what they saw.

2 Nov 2026, 10:44 UTC

home.pl says it is "working on allow-listing"

The abuse team escalates to network administration and promises to share any traffic pattern that triggered the "automated block".

2 Nov 2026, 14:32 UTC

home.pl says no

"we will not be unblocking the IP addresses". No logs, times or examples are given.

Further Reading

- mySites.guru service traffic - every request we send, how to verify it, how to stop it

- Connectivity requirements for web hosts - the page to hand a host's support desk
- mySites.guru on Cloudflare Radar - Cloudflare's verified agent listing
- home.pl: Czym jest WAF - home.pl says its administrators configure the firewall
- Regulamin Sieci home.pl - home.pl's network terms, section 37 on temporary blocks
- NASK annual report 2025 - .pl market shares by registrar

Frequently Asked Questions

Why does mySites.guru show my home.pl site as down when it loads fine in my browser?

home.pl's network drops every packet from mySites.guru's two published addresses, so our uptime checks, audits and backups time out while your browser, which comes from a different address, gets through. Nothing is wrong with your site. The block is on home.pl's side and only home.pl can lift it.

Which IP addresses does mySites.guru connect from?

Two, and they have not changed in over a decade: 178.62.5.35 for audits, backups, updates, snapshots and connection checks, and 165.227.239.229 for uptime checks. Both are published in plain text at manage.mysites.guru/ips, with reverse DNS of main-workers.mysites.guru and monitor-engine.mysites.guru.

Can I allow-list the mySites.guru IPs myself in the home.pl panel?

We could not find a way. home.pl's own help pages say security configuration is done by its administrators, and the only customer-facing allow-list we found sits inside the paid Ochrona WWW Premium WAF add-on. A WAF rule does not undo a network-level drop anyway, and home.pl has refused to lift the block for our addresses, so there is nothing a home.pl customer can switch on to fix it.

Will mySites.guru slow down its checks for home.pl?

No, because there is nothing to slow down. An uptime check is one HEAD request per site every five minutes with a 0-byte response body, audits run one at a time per server, and a full day of monitoring one site moves about 598 KB of headers. A single page view by one visitor costs the server more than we do all day.

What does a mySites.guru audit send to my home.pl site?

Audits, backups, updates and snapshots all come from 178.62.5.35 and go to the connector you installed, as signed POST requests that the connector validates with a single-use request ID before acting. Snapshots run about every 12 hours and also read robots.txt, up to six sitemap URLs, your security headers and whether the admin URL is restricted. Audits, backups and updates run only when you start or schedule them, and only one audit runs at a time per server.

Is mySites.guru traffic verifiable?

Yes, three ways. Both addresses have matching forward and reverse DNS under mysites.guru, connector requests are signed with Web Bot Auth against a public key at manage.mysites.guru/.well-known/http-message-signatures-directory, and Cloudflare lists mySites.guru as a verified agent in its Bots and Agents Directory on Cloudflare Radar.

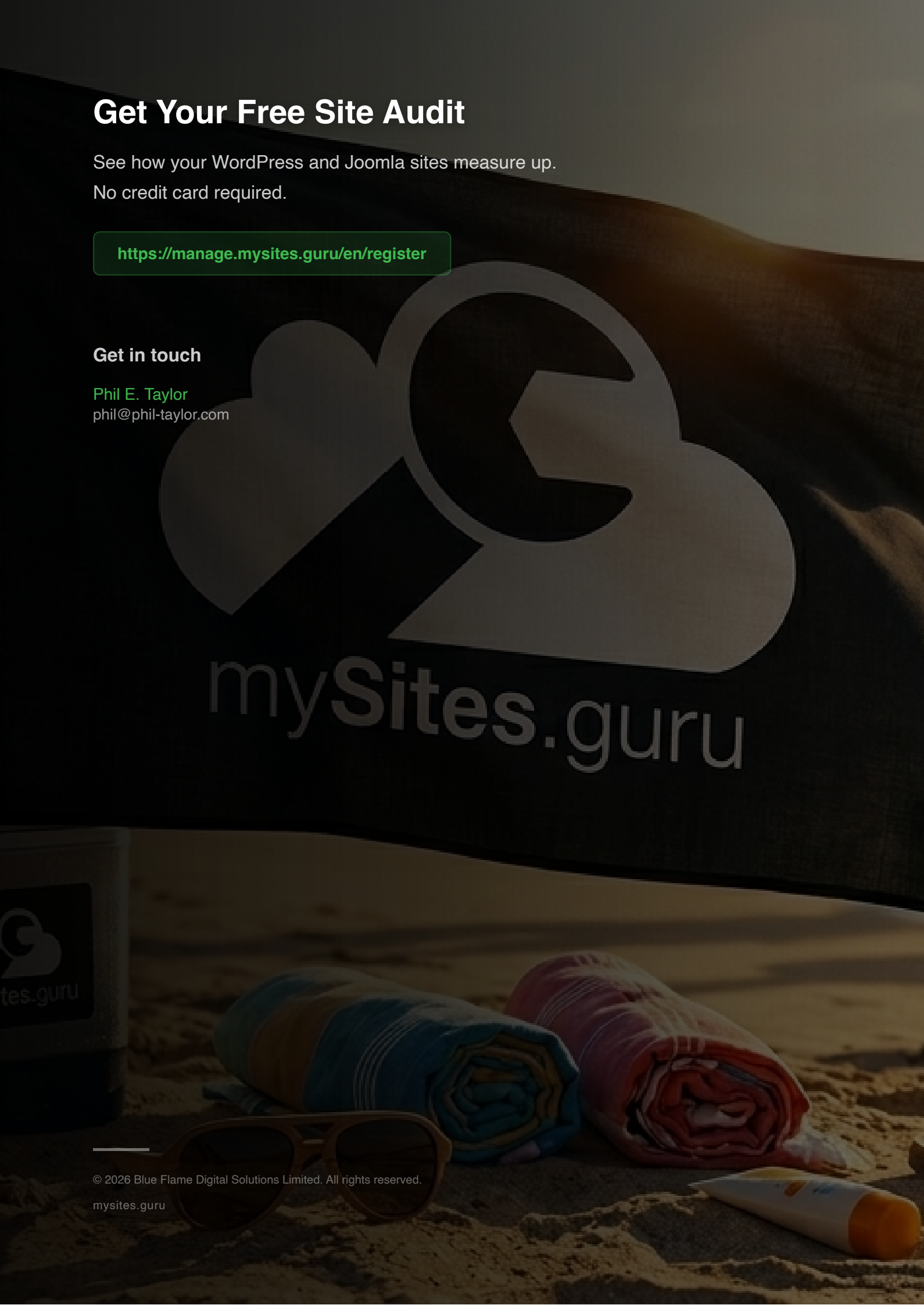
AI MODIFIED Written and edited by a human, with AI assistance. Our approach to AI

Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.

No credit card required.

https://manage.mysites.guru/en/register



Get in touch

Phil E. Taylor
phil@phil-taylor.com

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.