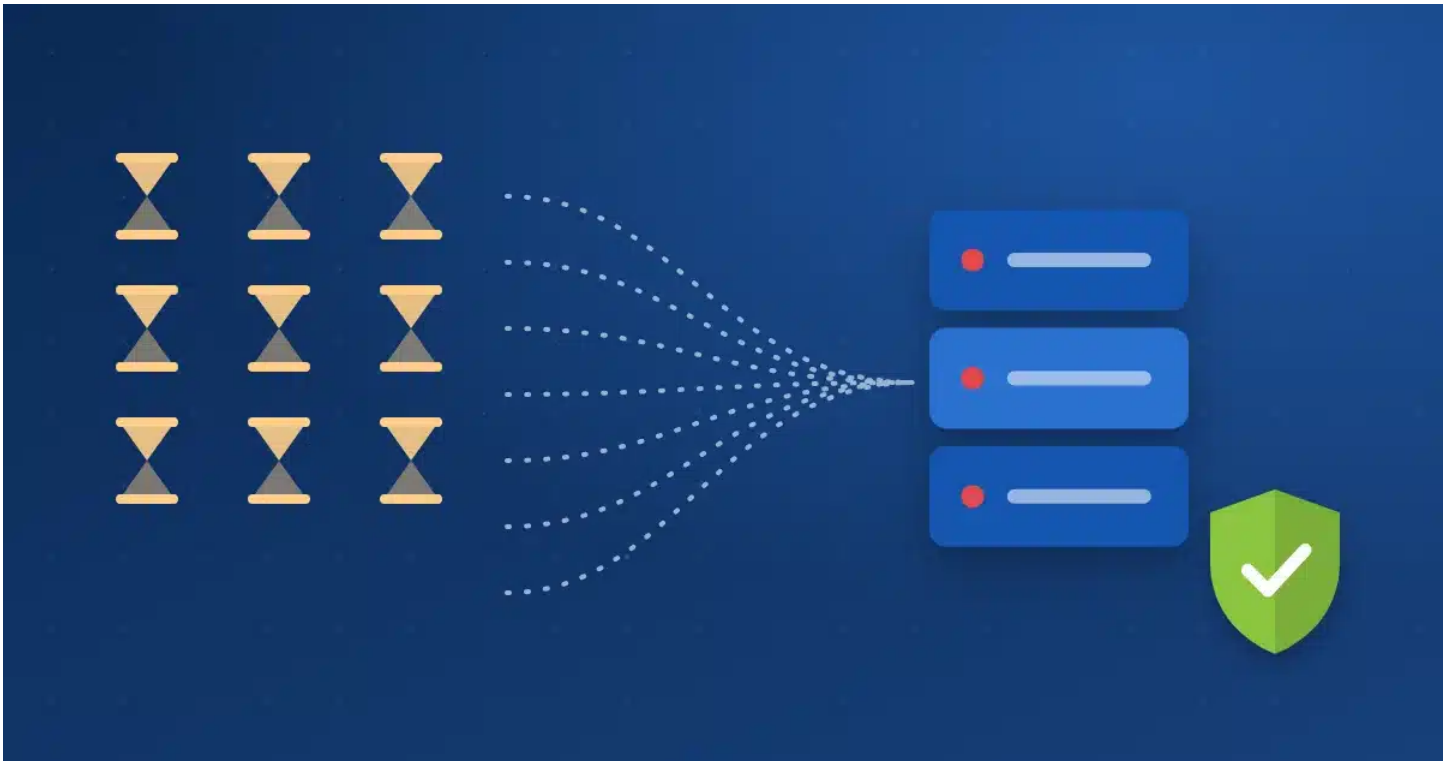
What Is a Slowloris DDoS Attack and How to Protect Your Server

Website Security · https://www.hyyat.com/en/knowledgebase/what-is-a-slowloris-ddos-attack/

In short Slowloris is a “slow” denial of service attack: instead of flooding the server with traffic, the attacker opens hundreds of connections and keeps them alive by sending the request a tiny piece every few seconds, until the server runs out of connections and real visitors cannot get in. Defences: per-address connection limits, a short request timeout, a web server that does not tie up a process per connection, and cloud protection.



How does the attack work?

When someone visits your site, their browser sends a complete HTTP request in a fraction of a second. In Slowloris the attacker sends only the start of the request, then one small extra line every 10 or 15 seconds, so the request never completes. The server assumes a slow visitor and keeps the connection open, waiting.

1. **The attacker opens hundreds of connections:** Sometimes from a single machine, with very little bandwidth.
2. **Keeps them alive slowly:** Each connection sends a small piece just before the server's timeout.
3. **The server runs out of connections:** Web servers that reserve a process per connection hit their limit.
4. **Real visitors are turned away:** The site looks down while CPU and bandwidth stay almost idle.

Signs of the attack

- The site does not respond, yet CPU and memory usage are not high.
- Many open connections from a small number of addresses.
- Web server logs show incomplete or timed-out requests.

How to protect your server

Method	What it does
Per-address connection limit	The firewall (such as CSF) stops one address from opening many connections at the same time.
Short request timeout	In Apache, mod_reqtimeout sets the maximum time for a full request to arrive, closing slow connections.
Event-based web server	LiteSpeed and Nginx do not reserve a full process per connection, so they withstand this attack much better.
Cloud protection in front	Cloudflare accepts connections instead of your server and passes only complete requests. Read Under Attack mode.

How Hyyat Host protects your site

- WordPress hosting servers run **LiteSpeed**, and the **CSF** firewall limits connections per address.
- **Imunify360** watches for suspicious requests and blocks their sources.
- You can connect your site to **Cloudflare** for an extra layer of protection.

For private servers, we configure these protections as part of our server management service. Learn more about Hyyat Host DoS protection.

Frequently asked questions

How is Slowloris different from a regular DDoS attack?
A regular DDoS floods the server with huge volumes of traffic or requests. Slowloris uses few, very slow connections, so it is hard to spot from usage alone.

Is a site on shared hosting affected?
Protection is the server’s job, and it is configured on our servers, so you need no setup in your site.

Is Cloudflare enough on its own?
It protects your site as long as visitors pass through it. If your server’s real IP is known, attackers can bypass it, so server protection is still needed.

Related guides

- The WordPress load-scripts.php Vulnerability (CVE-2018-6389) and How to Protect Your Site
- Brute Force Protection: What It Is and How Hyyat Host Protects Your Site
- How to Keep Your Website Secure: Practical Tips to Prevent Hacking
- What Is an SSL Certificate and How Does It Work?

All website security guides →

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.
Web HostingSaudi Hosting