HTTP/2 Header Memory Exhaustion

- Limit the Request Header Size
- Limit Concurrent Streams per Connection

Traefik serves HTTP/2 through the Go standard library. With HTTP/2, a single connection can multiplex many concurrent requests, each carrying its own header block.

A client can abuse HPACK header compression together with the HTTP/2 flow-control window to expand a small amount of wire data into a large memory allocation on the proxy, and keep that allocation pinned by stalling the streams. With enough concurrent streams and connections, this can exhaust the available memory and terminate the Traefik process.

Two entry point options bound this exposure. It is recommended to use them together.

Limit the Request Header Size

The `maxHeaderBytes` option caps the size, in bytes, of the request headers Traefik reads for each request. Lowering it from the default (`1048576`, that is 1 MiB) to the smallest value your largest legitimate headers need lets Traefik reject an oversized header block before it can be amplified.

```yaml
entryPoints:
  websecure:
    address: ':443'
    http:
      maxHeaderBytes: 65536
```

```toml
[entryPoints.websecure]
  address = ":443"

  [entryPoints.websecure.http]
```

```
    maxHeaderBytes = 65536
```

```
--entryPoints.websecure.address=:443
--entryPoints.websecure.http.maxHeaderBytes=65536
```

Limit Concurrent Streams per Connection

The `maxConcurrentStreams` option caps the number of concurrent HTTP/2 streams each client is allowed to initiate on a single connection (default `250`). Lowering it reduces the amount of memory a single connection can pin.

```
entryPoints:
  websecure:
    address: ':443'
    http2:
      maxConcurrentStreams: 100
```

```
[entryPoints.websecure]
  address = ":443"

  [entryPoints.websecure.http2]
    maxConcurrentStreams = 100
```

```
--entryPoints.websecure.address=:443
--entryPoints.websecure.http2.maxConcurrentStreams=100
```

!!! note "Defense in Depth"

```
These two limits bound the memory a single connection can consume.
For additional protection, also limit the number of concurrent connections and the request
rate per source IP at a fronting load balancer or firewall, and provision the Traefik instance
with enough memory to handle the expected legitimate load.
```

□□□ #2
□ □□□ □□□ 2026-10-31 14:06:09 UTC
□ □□□ □□□ 2026-10-31 14:06:10 UTC