Oblivious Relay Feedback

draft-rdb-ohai-feedback-to-proxy-04

IETF 114 · July 2022

T. Reddy (Akamai)
D. Wing (Citrix)
M. Boucadair (Orange)
R.Polli (Team Digitale, Italian Govt)

Agenda

- Updates to address feedback from the WG
- Align with draft-ietf-httpapi-ratelimit-headers

Problem Recap

- Excessive traffic from an oblivious relay to a target will cause target to rate-limit that relay
- Rate-limiting the oblivious proxy harms all clients using that relay

Proposal

- Signal overload from server to oblivious proxy
- Proxy uses the feedback to rate limit transactions from overzealous or misbehaving clients.
- Use draft-ietf-httpapi-ratelimit-headers, it publishes quotas (or service limits) to clients.

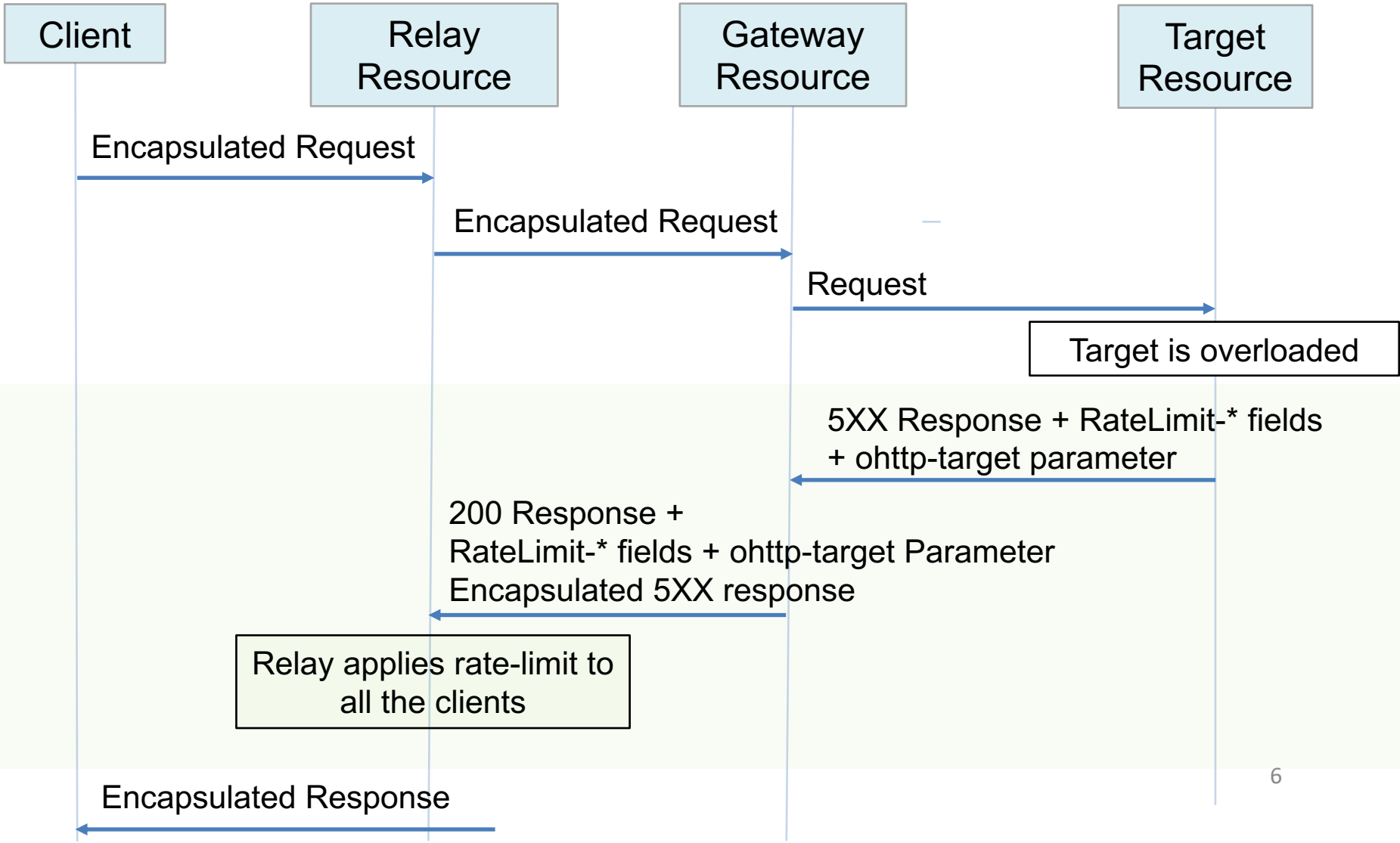
New *ohttp-target* Quota Policy Parameter

- Rate-limit quota policy for the Oblivious Relay

```
HTTP/1.1 200 OK
Date: Wed, 27 March 2022 04:45:07 GMT
Cache-Control: private, no-store
RateLimit-Limit: 10
RateLimit-Policy: 10;ohttp-target=2;attack-severity="high"; \
comment="abnormal header matching a WAF rule"
Content-Type: message/ohttp-res
Content-Length: 38 <content is the encapsulated 400 response>

...encrypted content...
```

Example Message Flow



ohttp-target Parameter values

- 1 => RateLimit fields are applicable to all the clients
- 2 => Ratelimit offending client
  - **The relay does not immediately rate-limit requests from the offending client**
  - **Rate-limits requests only when the ratio of "potential malicious requests" (value=2) to "legitimate requests" is high (no ohttp-target parameter)**
  - Malformed HTTP requests are linkable whereas the valid HTTP requests are not linkable.

The target will not be able to partition the anonymity set of legitimate clients.

Ohttp-Outside-Encap Header

- On forwarding requests, Oblivious gateway indicates HTTP headers that will be moved
- On receiving response, Oblivious gateway moves those headers+values outside encapsulation
  - Allows Oblivious relay to access and act on those headers
- Useful when Oblivious gateway and target are managed by separate entities.

Ohttp-Outside-Encap: RateLimit-Limit|RateLimit-Remaining|RateLimit-Reset|RateLimit-Policy

draft-rdb-ohai-feedback-to-proxy-04

- Comments and suggestions are welcome.