draft-janfred-radext-radius-congestion-control

Request-Block and Response-Delay

IETF 123 in Madrid – radext | 21.07.2025

Janfred Rieckers | DFN-Verein

Problem statement (recap from IETF122)

- Some supplicants/NASes send excessive amounts of requests
  - Requests will never result in Access-Accept (based on supplied attributes), but this is only known to the home server
  - Requests have to be sent across the whole proxy chain
  - Supplicants/NASes may re-start the authentication immediately
- Proposed solution: Delay replies or block requests closer to the edge
  - If a Reply gets delayed closer to the edge, the RADIUS ID is freed immediately on the hops to the home server
  - If the request can be blocked based on specific attributes, a proxy on the chain can send the response instead of the home server

Goal of the I-D

- We don't want to solve every problem
  - i.e. we don't care about missing responses and their effect on the proxy fabric. Out-of-scope.
  - We may not be able to mitigate all active attacks, focus on misbehaving clients
- We want to have an (automated) mitigation that makes the RADIUS Proxy Fabric a little bit more robust
  - If a request for delay/reject is not satisfiable, it could be ignored. (It's a **request** to delay/reject, not an **order** to do it)
  - It might be that the reject capability was announced, but the proxy cannot reject based on the requested attributes
    - Ignoring the request ok, still better than current situation if some special use cases are not covered
  - Mitigation can be much more targeted (especially if automated) compared to manual filters

Discussion and questions on the Mailinglist

- Is this an actual problem that needs solving?
  - @Operators: can you share details on observed issues and the current fixes
- Is the proposed solution an actual solution for the problem?
- Does this actually reduce load or add it load by requiring caches on proxies?
- How do we deal with under- or over-blocking?
- How should a home server/proxy determine what should be blocked/delayed?
- Should we do a RADIUS routing protocol? ICMP? RCMP? ABFAB trust router? ....
- Do we need more/less functionality?

Going forward with this document?

- If we actually problem worth solving:
  - Continue with this document?
  - Should this be included in the Proxy BCP document?
  - Something complete different?

Discussion/Questions?

- Contact
  - Jan-Frederik Rieckers

Mail: rieckers@dfn.de
Phone: 0049 30 884299-339
Fax: 0049 30 884299-370

Address:
DFN-Verein, Geschäftsstelle
Alexanderplatz1
10178 Berlin