draft-ietf-radext-radius-fragmentation-01

IETF 88
Status

• draft-perez-radext-radius-fragmentation-06 accepted as a WG document on August 26th
  – draft-ietf-radext-radius-fragmentation-00
• Solution focused on:
  – Transport of large amounts of authorization information between RADIUS client and server
  – Work through unmodified infrastructures
• Version 01 submitted
  – Addresses some issues raised on the mailing list
  – Fixes some minor errors
Issues

• Added text clarifying that proxies are assumed to base their routing decisions on the value of the *User-Name* attribute
  – And the MUST on User-Name in fragments

• New text regarding how proxies implementing RFC6929, but not this draft, will handle with truncated attributes
  – RFC states that packages SHOULD be forwarded even if invalid attributes are found

• Included a practical example of how many roundtrips would the transmission of a SAML assertion of 15,000 octets require
  – Expected overload is low: around 120 bytes (3%)
Issues

• Proxy-State-Len attribute
  – The server MAY artificially increase the quantity to be included in this attribute, in order to handle with situations where proxies behave inconsistently
  – The client MAY apply a value higher than the one suggested by this attribute in environments known to be problematic

• Detailed description of CoA handling
  – CoA packet fragmentation is not allowed
  – CoA clients are required to send a minimal CoA-Request packet, containing Service-Type=Authorize-Only
  – The NAS then performs fragmentation using this draft (Access-Request) through the RADIUS server it is configured to use
  – This server acts as proxy to forward authorization data to the RADIUS system which is co-located with the CoA client
  – Session identification and authorization are kept separated
  – The authorization process remains the same for initial authentication and for CoA
Other (Minor) Updates

• All references to radius-extensions draft now point to RFC6929
• Replaced User-Password attribute with NAS-Identifier for the pre-authorization example