IKEv2 Support for Anti-Replay Status Notification

draft-pan-ipsecme-anti-replay-notification

Wei Pan
Qi He
Paul Wouters

IETF 119

March 2024

Background

- RFC 4302 and RFC 4303 specify the details of sequence number generation and verification.
  - When anti-replay is enabled on the receiver, the sender must monitor the sequence number counter, increment the counter with every message sent, and ensure the counter does not cycle.
  - When anti-replay is disabled on the receiver, the sender does not need to monitor or reset the counter.
- RFC 4302 and RFC 4303 also specify that, **during SA establishment, IPsec implementation should notify the peer if it will not provide anti-replay protection**, to avoid having the peer do unnecessary sequence number monitoring and SA setup.

Section 3.4.3 Sequence Number Verification, RFC 4302 & 4303

If the receiver does not enable anti-replay for an SA, no inbound checks are performed on the Sequence Number. However, from the perspective of the sender, the default is to assume that anti-replay is enabled at the receiver. To avoid having the sender do unnecessary sequence number monitoring and SA, if an SA establishment protocol such as IKE is employed, **the receiver SHOULD notify the sender, during SA establishment, if the receiver will not provide anti-replay protection.**

Problems In High-Performance Scenarios

Current Situation

- In high-performance scenarios, high-level QoS packets may arrive earlier than a large number of low-level QoS packets, causing the low-level QoS packets being dropped due to disordered packets exceed the window size of anti-replay.
- **Operators choose to disable the anti-replay function for reasons of QoS, performance, etc.**

Result in Frequent Rekey

- In high-performance scenarios, 32-bit sequence numbers are consumed quickly, resulting in frequent rekeying of Child SAs.
- ESN solves this problem by extending the sequence numbers to 64 bits. But, **ESN relies on the window of anti-replay to guess the high-order 32 bits of the sequence number**.

- **Currently, when the anti-replay is disabled, Child SAs will rekey frequently due to unnecessary sequence number monitoring and the unavailability of ESN**. Solutions could be:
  - To avoid unnecessary sequence number monitoring, i.e., adding anti-replay status notification in IKEv2.
  - To allow the use of ESN when anti-replay is disabled.

Anti-replay status notification

- Peers include the **ANTI_REPLAY_STATUS** notify payload in the IKE_AUTH exchange for creating the initial Child SA or the CREATE_CHILD_SA exchange for creating the subsequent Child SAs.
- When anti-replay is disabled on both peers, neither peer needs to monitor the sequence number counter, thus avoiding frequent rekey of Child SAs.

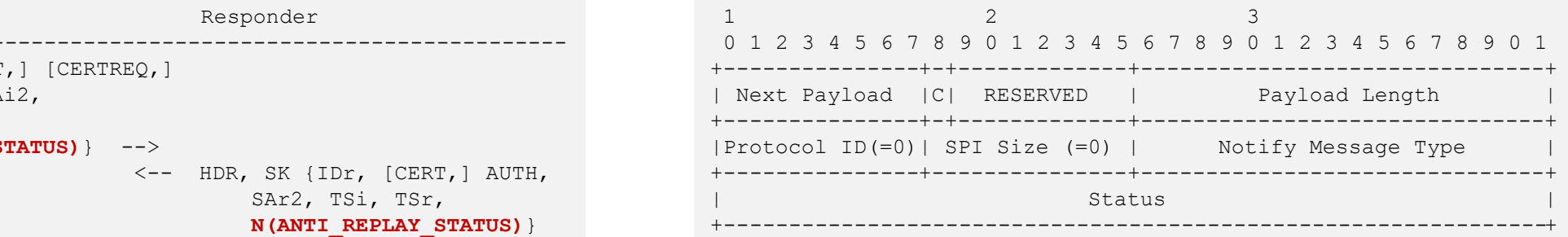
IKE_AUTH Message Exchange Example

```
Initiator                           Responder
-----------------------------------------------------------------
HDR, SK {IDi, [CERT,] [CERTREQ,]
    [IDr,] AUTH, SAi2,
    TSi, TSr,
    N(ANTI_REPLAY_STATUS)}   -->
                              <--   HDR, SK {IDr, [CERT,] AUTH,
                                        SAr2, TSi, TSr,
                                        N(ANTI_REPLAY_STATUS)}
```

CREATE_CHILD_SA Message Exchange Example

```
Initiator                           Responder
-----------------------------------------------------------------
HDR, SK {SA, Ni, [KEi,]
    TSi, TSr,
    N(ANTI_REPLAY_STATUS)}   -->
                              <--   HDR, SK {SA, Nr, [KEr,]
                                        TSi, TSr,
                                        N(ANTI_REPLAY_STATUS)}
```

ANTI_REPLAY_STATUS Notify Payload Format

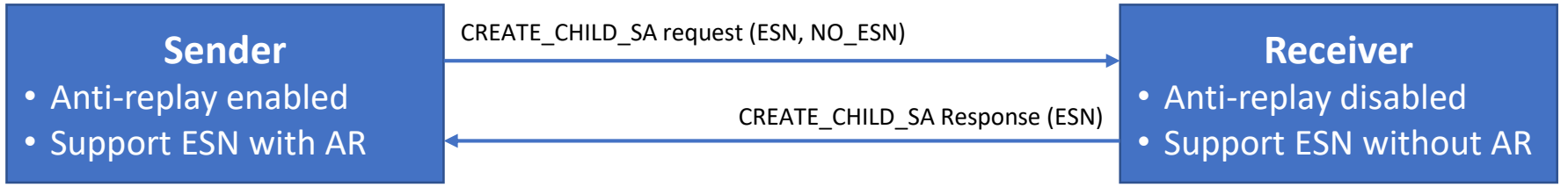


- Status (4 octets) - this field MUST be **0 to indicate the anti-replay is enabled or 1 to indicate the anti-replay is disabled.**

Question: Should this notify be able to convey "I can do ESN without replay protection"?

Unbind ESN From Anti-Replay

- ESN relies on the window of anti-replay to guess the high-order 32 bits of the sequence number.
- **If IPsec implementations can maintain a separate window for ESN, then ESN can be used without anti-replay.**
  - Due to the window size of anti-replay is not negotiable, the window size for ESN may also not need to be negotiable.
- Doing ESN without anti-replay seems to be an unilateral act, is there a need to notify the peer that “I can do ESN without replay-detection”?



Question: Does the receiver also notify the sender that “I’m doing ESN without anti-replay”?

- ESN can be used whichever peer disables the anti-replay, thus avoiding frequent rekey of Child SAs.

Further Considerations

- Is this problem worth solving?
  - Anti-replay status notification is required by RFC 4302 & 4303, and this draft can fulfil this requirement.
  - Unbinding ESN from anti-replay should be covered in this draft or done in a separate draft?
- Suggestions, comments, and reviews are all welcome.