IKEv2 Support for Anti-Replay Status Notification

draft-pan-ipsecme-anti-replay-notification

Wei Pan
Qi He
Paul Wouters

IETF 121

November 2024

Problem In High-Traffic-Volume Scenarios

- **Operators often choose to disable the anti-replay function, especially on high speed connections**
  - for the reason of QoS, performance, etc.
  - to avoid the disordered packets being dropped due to exceed the window size of anti-replay (usually 1K)
- **But, high traffic volume means rapid consumption of Sequence Numbers,**
  - 32-bit Sequence Numbers may be exhausted in minutes
  - 64-bit Extended Sequence Numbers (ESN) is better to be chosen and used
- **And, for many IPsec implementations, ESN requires anti-replay**
  - although RFC 4302 & 4303 does not prohibit using ESN when the anti-replay function is not enabled
  - such implementations also comply with RFC 4302 & 4303

> **Section 3.3.3 Sequence Number Generation, RFC 4302 & 4303**
>
> Note: **If a receiver chooses to not enable anti-replay for an SA, then the receiver SHOULD NOT negotiate ESN** in an SA management protocol. Use of ESN creates a need for the receiver to manage the anti-replay window (in order to determine the correct value for the high-order bits of the ESN, which are employed in the ICV computation), which is generally contrary to the notion of disabling anti-replay for an SA.

- **Nobody did wrong, but the outcome was not wanted**
  - ESN can’t be negotiated —> 32-bit SN exhaust rapidly —> Child SAs also rekey frequently

Can ESN be used without anti-replay?

- **Why ESN is bound to anti-replay?**
  - High-order 32 bits of the ESN is not transmitted on the wire
  - Anti-replay window code is the code that is also used for tracking high order bits of ESN
  - RFC 4302 & 4303 both describe the mechanism of using anti-replay window for ESN in the Appendix A

> **Section 3.3.3 Sequence Number Generation, RFC 4302 & 4303**
>
> Note: If a receiver chooses to not enable anti-replay for an SA, then the receiver SHOULD NOT negotiate ESN in an SA management protocol. **Use of ESN creates a need for the receiver to manage the anti-replay window** (in order **to determine the correct value for the high-order bits of the ESN**, which are employed in the ICV computation), which is generally contrary to the notion of disabling anti-replay for an SA.

- **Can ESN be used without anti-replay?**
  - **Yes**, cause RFCs don't prohibit doing so
  - **A separate window is needed** when there is no anti-replay window
  - **This can be a local policy:**
    - Any implementation can choose to do so,
    - Any implementation can choose not to do so as well

One peer’s ESN capability

- **One peer’s ESN capability can be abstracted in the table below**

Peer A		
Current Status		Current ESN Capability
Replay Protection	Using ESN w/o anti-replay	
Y	Y	Y
Y	N	Y
N	Y	Y
N	N	N

- If it enables replay protection, it is able to accept to use ESN.
- If it doesn’t enable replay protection but supports using ESN without anti-replay, it is able to accept to use ESN.
- If it doesn’t enable replay protection and not support using ESN without anti-replay, it is NOT able to accept to use ESN.

ESN Negotiation Results (1/3)

- **The ESN negotiation results of two peers can be abstracted in the table below:**

Peer A			Peer B			Outcome
Current Status		Current ESN Capability	Current Status		Current ESN Capability	ESN negotiation result
Replay Protection	Using ESN w/o AR		Replay Protection	Using ESN w/o AR		
Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	N	Y	Y
Y	N	Y	Y	Y	Y	Y
Y	N	Y	Y	N	Y	Y
Y	Y	Y	N	Y	Y	Y
N	Y	Y	Y	Y	Y	Y
N	Y	Y	N	Y	Y	Y
N	Y	Y	Y	N	Y	Y
Y	N	Y	N	Y	Y	Y
N	Y	Y	N	N	N	N
N	N	N	N	Y	Y	N
N	N	N	N	N	N	N
N	N	N	Y	Y	Y	N
N	N	N	Y	N	Y	N
Y	Y	Y	N	N	N	N
Y	N	Y	N	N	N	N

ESN Negotiation Results (2/3)

- **The ESN negotiation results of two peers can be abstracted in the table below:**

Peer A			Peer B			Outcome
Current Status		Current ESN Capability	Current Status		Current ESN Capability	ESN negotiation result
Replay Protection	Using ESN w/o AR		Replay Protection	Using ESN w/o AR		
Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	N	Y	Y
Y	N	Y	Y	Y	Y	Y
Y	N	Y	Y	N	Y	Y
Y	Y	Y	N	Y	Y	Y
N	Y	Y	Y	Y	Y	Y
N	Y	Y	N	Y	Y	Y
N	Y	Y	Y	N	Y	Y
Y	N	Y	N	Y	Y	Y
N	Y	Y	N	N	N	N
N	N	N	N	Y	Y	N
N	N	N	N	N	N	N
N	N	N	Y	Y	Y	N
N	N	N	Y	N	Y	N
Y	Y	Y	N	N	N	N
Y	N	Y	N	N	N	N

If both peers enable the anti-replay, ESN can be negotiated successfully.

If both peers support using ESN without anti-replay, the ESN can be negotiated successfully regardless of the anti-replay status.

If one peer disables anti-replay and supports using ESN without anti-replay, and the other peer enables anti-replay and doesn't support using ESN without anti-replay, the ESN can be negotiated successfully.

ESN Negotiation Results (3/3)

- **The ESN negotiation results of two peers can be abstracted in the table below:**

Peer A			Peer B			Outcome
Current Status		Current ESN Capability	Current Status		Current ESN Capability	ESN negotiation result
Replay Protection	Using ESN w/o AR		Replay Protection	Using ESN w/o AR		
Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	N	Y	Y
Y	N	Y	Y	Y	Y	Y
Y	N	Y	Y	N	Y	Y
Y	Y	Y	N	Y	Y	Y
N	Y	Y	Y	Y	Y	Y
N	Y	Y	N	Y	Y	Y
N	Y	Y	Y	N	Y	Y
Y	N	Y	N	Y	Y	Y
N	Y	Y	N	N	N	N
N	N	N	N	Y	Y	N
N	N	N	N	N	N	N
N	N	N	Y	Y	Y	N
N	N	N	Y	N	Y	N
Y	Y	Y	N	N	N	N
Y	N	Y	N	N	N	N

If either peer disables anti-replay and doesn't support using ESN without anti-replay, the ESN won't be negotiated successfully.

ESN Negotiation Results Summary

- **The ESN negotiation results are summarized as the following:**
  - If both peers enable the anti-replay, the ESN can be negotiated successfully.
  - If both peers support using ESN without anti-replay, the ESN can be negotiated successfully regardless of the anti-replay status.
  - If one peer disables anti-replay and supports using ESN without anti-replay, and the other peer enables anti-replay and doesn't support using ESN without anti-replay, the ESN can be negotiated successfully.
  - If either peer disables anti-replay and doesn't support using ESN without anti-replay, the ESN won't be negotiated successfully.

- **Whether supporting using ESN without anti-replay is a local policy, and any implementation can choose to do it or not.**
- **Therefore, it seems the IPsec implementations don't have to notify the peer of this capability.**
  - **Question: Do we need to notify the peer that I support using ESN without anti-replay?**

We can do more (1/3)

- **For the cases that ESN can't be negotiated to use, we can still do something to improve the outcome**

Peer A			Peer B			Outcome
Current Status		Current ESN Capability	Current Status		Current ESN Capability	ESN negotiation result
Replay Protection	Using ESN w/o AR		Replay Protection	Using ESN w/o AR		
Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	N	Y	Y
Y	N	Y	Y	Y	Y	Y
Y	N	Y	Y	N	Y	Y
Y	Y	Y	N	Y	Y	Y
N	Y	Y	Y	Y	Y	Y
N	Y	Y	N	Y	Y	Y
N	Y	Y	Y	N	Y	Y
Y	N	Y	N	Y	Y	Y
N	Y	Y	N	N	N	N
N	N	N	N	Y	Y	N
N	N	N	N	N	N	N
N	N	N	Y	Y	Y	N
N	N	N	Y	N	Y	N
Y	Y	Y	N	N	N	N
Y	N	Y	N	N	N	N

When both peers disable anti-replay:

- ESN isn't successfully negotiated.
- Each peer does not check the sequence number of inbound packets. (RFC 4303 Section 3.4.3)
- Each peer also does not need to monitor or reset the sequence number counter of outbound packets (if it gets the notification of the anti-replay status from the other peer). (RFC 4303 Section 3.3.3)

So, **Child SAs don't need to be rekeyed when 32-bit SNs are exhausted**.
(Other reasons can still trigger rekeying)

We can do more (2/3)

- **For the cases that ESN can't be negotiated to use, we can still do something to improve the outcome**

Peer A			Peer B			Outcome
Current Status		Current ESN Capability	Current Status		Current ESN Capability	ESN negotiation result
Replay Protection	Using ESN w/o AR		Replay Protection	Using ESN w/o AR		
Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	N	Y	Y
Y	N	Y	Y	Y	Y	Y
Y	N	Y	Y	N	Y	Y
Y	Y	Y	N	Y	Y	Y
N	Y	Y	Y	Y	Y	Y
N	Y	Y	N	Y	Y	Y
N	Y	Y	Y	N	Y	Y
Y	N	Y	N	Y	Y	Y
N	Y	Y	N	N	N	N
N	N	N	N	Y	Y	N
N	N	N	N	N	N	N
N	N	N	Y	Y	Y	N
N	N	N	Y	N	Y	N
Y	Y	Y	N	N	N	N
Y	N	Y	N	N	N	N

When one peer disables anti-replay and the other doesn't:

If the traffic from Peer B to Peer A is high-volume, and if Peer A notifies its replay protection status to Peer B, then Peer B doesn't need to monitor the sequence number counter and trigger Child SAs rekey when SN is exhausted.

Similar processing as above

We can do more (3/3)

- **In conclusion, for the cases that ESN can’t be negotiated to use, notifying the status of replay protection to the peer can help improve the outcome.**
  - The sender doesn’t need to do unnecessary sequence number monitoring and SA setup when the receiver disables replay protection.
  - Frequent Child SAs rekey can be avoided.

Anti-replay and ESN status notification

- Peers include the **REPLAY_PROT_AND_ESN_STATUS** notification payload in the IKE_AUTH exchange for creating the initial Child SA or the CREATE_CHILD_SA exchange for creating the subsequent Child SAs.

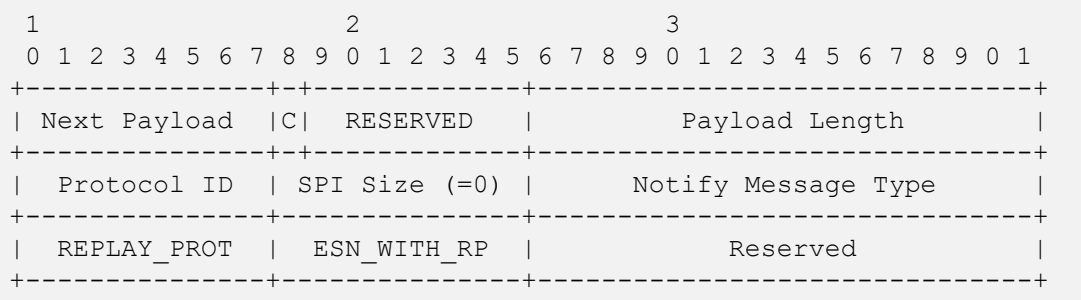
IKE_AUTH Message Exchange Example

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

CREATE_CHILD_SA Message Exchange Example

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

REPLAY_PROT_AND_ESN_STATUS Notify Payload Format



- Protocol ID (1 octet) - this field MUST contain either (2) to indicate AH or (3) to indicate ESP.
- REPLAY_PROT (1 octet) - this field MUST be **0 to indicate the replay protection is enabled or 1 to indicate the replay protection is disabled.**
- ESN_WITH_RP (1 octet) - this field MUST be 0 to indicate that ESN is used with the replay protection enabled or 1 to indicate that ESN can be used without enabling the replay protection.

Further Considerations

- How should the status of supporting using ESN without anti-replay be notified?
  - Exchanged in IKE_SA_INIT? Or in IKE_AUTH & CREATE_CHILD_SA?
  - Or even not exchanged at all?
- If IPsec implementations can maintain a separate window for ESN, should the window size be negotiable?
  - The window size of anti-replay is not negotiable.
- Suggestions, comments, and reviews are all welcome.