Extended Sequence Number

This chapter describes support of 64-bit Extended Sequence Numbers (ESNs) for Encapsulating Security Payload (ESP) and Authentication Header (AH) packets. ESN is defined in RFC 4304.

This chapter includes the following sections:

Overview

ESN for ikev2

Every IKE message contains a Message ID (sequence number) as part of its fixed header. This sequence number is a monotonically increasing integer (incremented by 1 for every packet sent) used to match up requests and responses, and to identify retransmissions of messages. The sequence is a 32-bit integer which is zero for the first IKE request in each direction.

Sequence numbers are cryptographically protected to protect against message replays. In the unlikely event that Message IDs grow too large to fit in 32 bits (0xFFFFFFFF = 4294967295 packets), the IKE_SA must be closed. Rekeying an IKE_SA resets the sequence numbers.

RFC 4304 outlines support for a 64-bit ESN implemented for ikev2. The ESN transform is included in an ikev2 proposal used in the negotiation of IKE SAs as part of the IKE_SA_INIT exchange.

The ESN transform has the following meaning:

- A proposal containing one ESN transform with value 0 means "do not use extended sequence numbers".
- A proposal containing one ESN transform with value 1 means "use extended sequence numbers".
- A proposal containing two ESN transforms with values 0 and 1 means "I support both normal and extended sequence numbers, you choose". This case is only allowed in requests; the response will contain only one ESN transform.

In most cases, the exchange initiator will include either the first or third alternative in its SA payload. The second alternative is rarely useful for the initiator: it means that using normal sequence numbers is not acceptable (so if the responder does not support ESNs, the exchange will fail with NO_PROPOSAL_CHOSEN.

Including the ESN transform is mandatory when creating ESP/AH SAs.

StarOS Support for ESN

StarOS supports ESN for ESP packets using ikev2 negotiation; ESN is not supported for ikev1. The configuration and processing sequence is as follows:

- Enable ESN in an IPSec transform set via a StarOS CLI command.
- Negotiate ESN (IPSec Domain of Interpretation (DOI) for Ikev2.
  - Send ESN in the proposal based on configuration.
  - Accept and process ESN in the proposal based on configuration.
- Configure data-path to use ESN.
- Read and checkpoint ESN.

Important ESN is only supported on ASR 5500 and ASR 9000 Virtualized Services Modules (VSMs). It is not supported on the VPC-SI.

Configuring ESN Support

The IPSec Transform Set Configuration mode includes an **esn** command that enables ESN support.

```
configure
   context ipsec_ctx_name
      ipsec transform-set tset_name
         esn
         end
```

Notes:

- *ipsec_ctx_name* is the StarOS context associated with IPSec.
- *tset_name* is the name of the transform set in the current context that you want to configure for ESN.
- For more information on parameters, see the *IPSec Transform Set Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- By default ESN support is disabled.
- Enabling the **esn** command is the equivalent of sending ESN Transform = 0 and 1; supports both 32-bit and 64-bit sequence numbers. If the **esn** command is not enabled, support is only 32-bit sequence numbers (default behavior).

Verifying ESN Configuration

The following Exec mode **show** commands display ESN configuration parameters.

show crypto ipsec transform-set

This command displays the IPSec transform set parameters as configured in a specific context and includes ESN status. A sample output appears below:

```
show crypto ipsec transform-set tsela
IKEv2 IPSec Transform-Set tselsa :
    Cipher      : aes-cbc-128
    HMAC        : sha1-96
    DH Group    : none
    Encaps Mode : TUNNEL
    ESN         : Enabled/Disabled
```

show crypto template

This command displays ESN status under IPSec SA Payload. A sample output appears below.

```
show crypto template tag foo-sa0
  IPSec SA Payload 1/2 (SIP Address - Static Pool)
    Name : foo-sa0
    IPSec SA Transform 1/1
      Transform Set: tselsa
        Protocol: esp
        Encryption Cipher: aes-cbc-128
        Hashed Message Authentication Code: sha1-96
        Diffie-Hellman Group: none
        ESN : Enabled
```