Rekeying SAs

This chapter describes StarOS features for rekeying security Associations (SAs).

The following topics are discussed:

- Rekey Traffic Overlap, on page 1
- Sequence Number-based Rekeying, on page 4

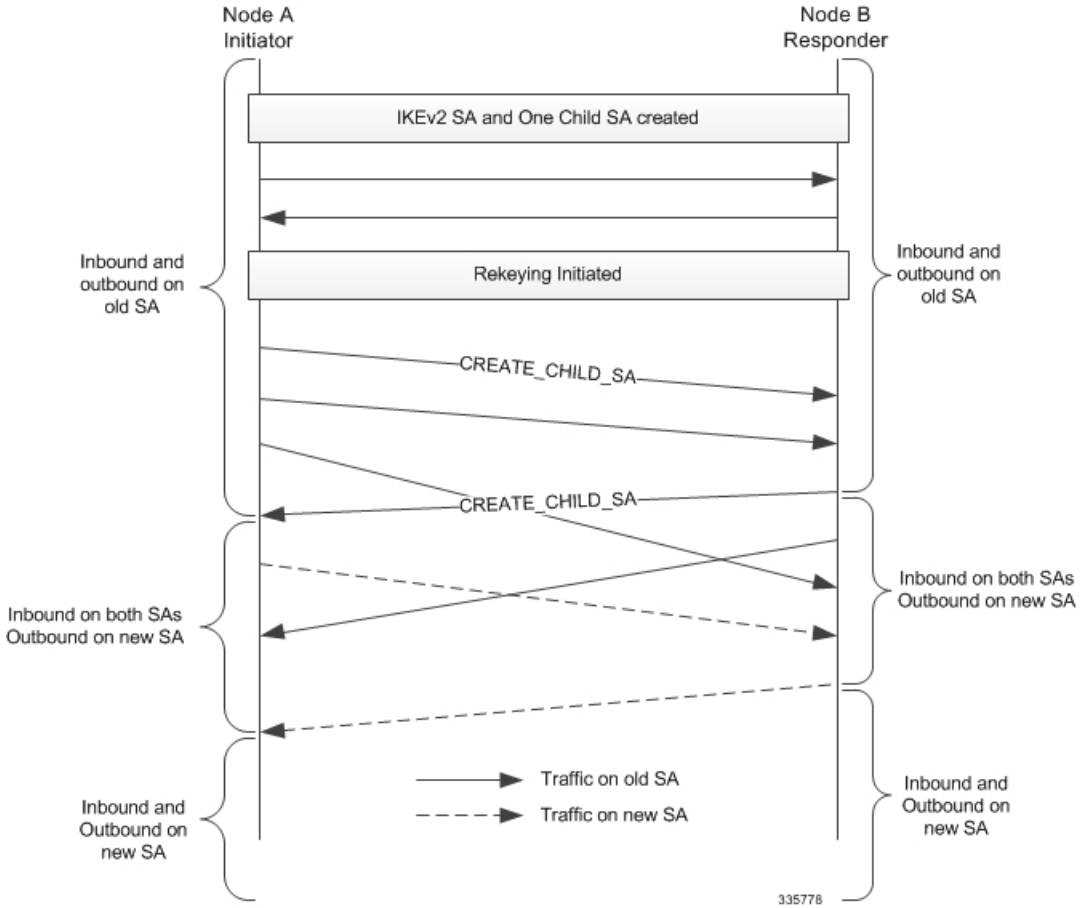
Rekey Traffic Overlap

Overview

An SA may be created with a finite lifetime, in terms of time or traffic volume. To assure interrupt-free traffic IKE SA and IPSec SAs have to be "rekeyed". By definition, rekeying is the creation of new SA to take the place of expiring SA well before the SA expires. RFC 5996 describes the procedure for IKEv2 rekeying with minimal traffic loss.

During the rekeying, both initiator and responder maintain both SAs for some duration during which they can receive (inbound) on both SAs. The inbound traffic on the old SA stops only after each node unambiguously knows that the peer is ready to start sending on the new SA (switch outbound to new SA). Switching the outbound traffic to new SA happens at the initiator and responder as depicted in following diagram.

Figure 1: Call Flow: Maintaining Old and New SAs during Child SA Rekeying



Note the following key points:

- Initiator is the first to switch outbound traffic to the new SA
- Switching outbound traffic on the responder is consequential
- Each node is ready to receive on both SAs for some duration.

If the traffic does not start flowing immediately on the new SAs, the nodes can use another mechanism to switch traffic to the new SA.

- To rekey a child SA (IPSec SA):
  - The node receives an explicit delete for the old child SA on IKE.
  - A predefined time elapses (neither of the above two events happen).

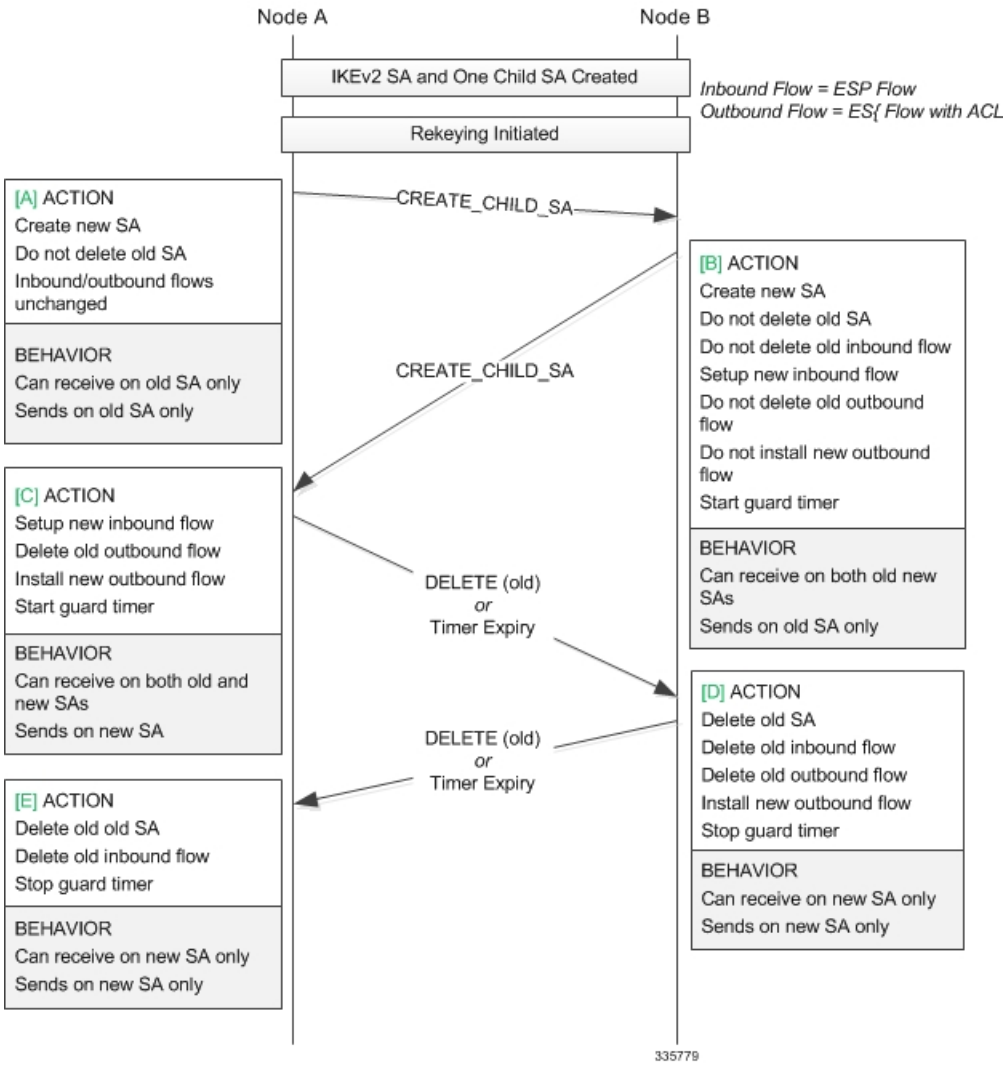
Deployment Scenarios

Network operators prefer using s finite-lifetime SA to minimize the risk of compromising the key when used indefinitely. Rekeying instead of deleting-creating an SA avoids breaks in traffic.

Initiator and Responder Rekeying Behavior

During rekeying, the old SA must not be deleted when the new SA is created. Traffic transmission on the new SA and deletion of the old child SA occurs as depicted in the following diagram.

Figure 2: Initiator and Responder Behavior During Rekeying



Notes:

1. If Node-A does not send DELETE at [C], guard timer expiry in Node-B replaces event [D]; guard timer expiry in Node-A replaces event [E}.
2. If Node-B does not send DELETE at [D], guard timer expiry in Node-A replaces event [E].
3. Guard timer expiry is fixed at 120 seconds.

Sequence Number-based Rekeying

Overview

IKE, ESP, and AH security associations use secret keys to encrypt the data traffic for a limited amount of time and for limited amount of data. This limits the lifetime of the entire security association.

If the life time of a security association expires, new security association needs to be established to replace the expired security association. This reestablishment of security associations to take the place of ones that expire is referred to as "rekeying".

The rekeying can be done for the IKE SA and also for the child (ESP or AH) SA. This feature triggers rekeying only for the Child SA.

This feature supports sequence number based rekeying where the lifetime for the child SA is processed in terms of sequence number of the child SA data flow.

Sequence number-based rekeying is applicable only for the 32-bit based sequence number, so as to protect against the wrapping of sequence number before it reach its maximum limit of 4,293,918,720. The soft limit threshold for sequence number-based rekey trigger is fixed to 90% of the maximum sequence number limit.

Important This feature is not applicable on the configuration that supports Extended Sequence Number (ESN).

This feature can be activated only when the anti-replay functionality is enabled in the configuration. In StarOS the anti-replay is enabled by default.

Deployment Scenarios

This feature can be used to rekey a child SA when the sequence number of the packet passed through the SA exceeds the predefined sequence number threshold.

CLI Commands

Sequence number-based rekeying is enabled when the Context Configuration Mode **ipsec replay** command is enabled along with crypto map and crypto template rekeying configurations.

ipsec rekey

This Context Configuration Mode command configures IKEv2 IPSec specific anti-replay.

```
configure
  context ctxt_name
    ipsec replay [ window-size window_size ]
    end
```

Crypto Map and Crypto Template Rekey Configurations

There are a number of Context Configuration mode commands with rekey keywords.

For crypto maps refer to the following commands:

- **crypto map** *map_name* **ikev2-ikesa replay**
- **crypto map** *map_name* **ikev2-ipv4 rekey**
- **crypto map** *map_name* **ikev2-ipv6 rekey**

For crypto template refer to the following commands:

- **crypto template** *template_name* **ikev2-dynamic payload rekey**
- **crypto template** *template_name* **ikev2-ikesa rekey**

show crypto ipsec security-associations

This Exec mode **show** command displays the childSA lifetime based on sequence number.