KEEP_OLD_IKE_SA

draft-mglt-ipsecme-keep-old-ike-sa-00.txt

D. Migault

30/07/2013- IETF87- Berlin

Table of Contents

Introduction

Motivations:

- Communications with multiple interfaces
- Take advantage of established communications for a new interfaces
  - Avoid re-authentication

When a new interface appears we consider proceeding as follows:

- Create a new IKE_SA channel on the existing interface
- Optionally set your VPN (CREATE_CHILD_SA)
- Move the new IKE_SA (+ CHILD_SA) on the new interface (MOBIKE)

This draft focuses on creating a new IKE_SA

- Using the CREATE_CHILD_SA Exchange

CREATE_CHILD_SA (IKE_SA)

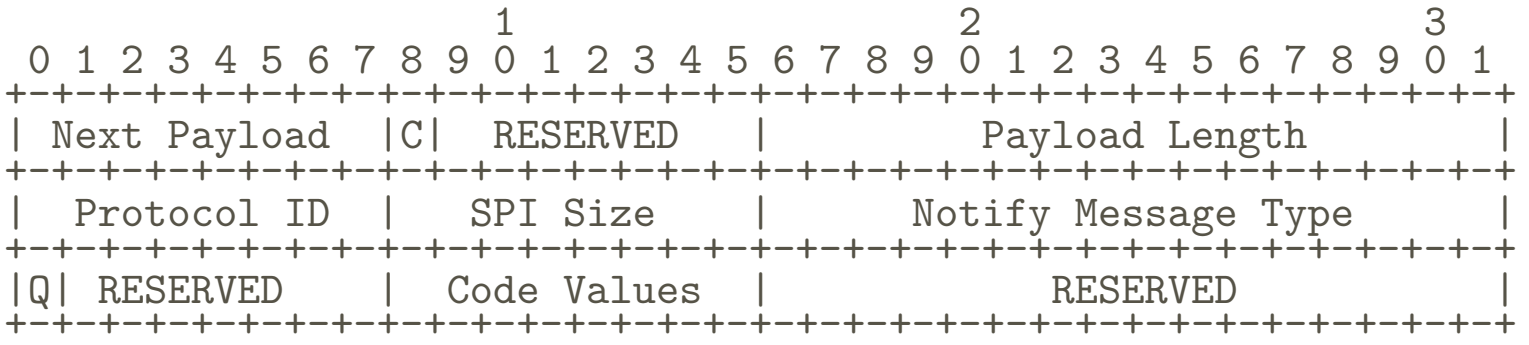
A CREATE_CHILD_SA exchange for a IKE_SA includes:

- 1. Create a new IKE_SA
- 2. Update CHILD_SA to the new IKE_SA
  - References, ...
- 2. Delete the old IKE_SA with a Delete Payload
  - Can be initiated by the two peers
  - Some implementations rekey IKE_SA and CHILD_SA

In our case, we only need to create a new IKE_SA

- Our extension indicates only perform step 1.

CLONE_IKE_SA



Code Values

Keep Old IKE_SA	0
Unused Old IKE_SA	1
Unassigned	2-255

Next Step

- Rename by KEEP_OLD_IKE_SA by CLONE_IKE_SA
- Create CLONE_IKE_SA_SUPPORTED Notify Payload
  - Initiator knows the responder supports the extension
- Specify the Codes Values
  - To make possible supporting the extension without cloning the IKE_SA.
- Syntax Error returned when extension not used with IKE_SA

Thank you for your attention