strongSwan - Issue #2686

Packet loss during rekey

19.06.2018 19:45 - Saurabh Mohan

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.5.3	**Resolution:**	No feedback

Description

I think i am seeing a sequencing issue during rekey where the dut (device-under-test) sends a Delete notification to the peer prior to installing the new inbound SA in the kernel. Therefore the peer starts using the new rekey'd SA. But on the dut the IPSec SA hasn't yet moved from Acquire to Valid.

Strongswan version: 5.5.3
2018-06-12 23:31:53.441 04[IKE] closing CHILD_SA 172.17.0.10-172.17.0.11{1} with SPIs c6b5a585_i (3660656 bytes) ce83fedb_o (3660890 bytes) and TS 0.0.0.0/0 === 0.0.0.0/0
Delete notification to peer **vvvvvvvvvvvv
2018-06-12 23:31:53.441 04[IKE] sending DELETE for ESP CHILD_SA with SPI c6b5a585
2018-06-12 23:31:53.441 04[ENC] generating INFORMATIONAL request 1 [D]
2018-06-12 23:31:53.441 04[NET] sending packet: from 172.17.0.10[500] to 172.17.0.11[500] (69 bytes)
2018-06-12 23:31:53.441 06[KNL] creating rekey job for CHILD_SA ESP/0xce83fedb/172.17.0.11
2018-06-12 23:31:53.441 06[IKE] establishing CHILD_SA 172.17.0.10-172.17.0.11{2} reqid 50
2018-06-12 23:31:53.441 06[KNL] got SPI c4377183
2018-06-12 23:31:53.441 06[ENC] generating CREATE_CHILD_SA request 0 [N(REKEY_SA) SA No KE TSi TSr]
2018-06-12 23:31:53.441 06[NET] sending packet: from 172.17.0.10[500] to 172.17.0.11[500] (269 bytes)
2018-06-12 23:31:53.441 04[NET] received packet: from 172.17.0.11[500] to 172.17.0.10[500] (257 bytes)
2018-06-12 23:31:53.441 04[ENC] parsed CREATE_CHILD_SA response 0 [SA No KE TSi TSr]
*****New inbound SA installed in kernel** ****vvvvvvvvvvv
2018-06-12 23:31:53.441 04[KNL] adding SAD entry with SPI c4377183 and reqid {50}
2018-06-12 23:31:53.441 04[KNL] using encryption algorithm AES_GCM_16 with key size 160
2018-06-12 23:31:53.441 04[KNL] using replay window of 32 packets
2018-06-12 23:31:53.441 04[KNL] adding SAD entry with SPI cdf90bca and reqid {50}
2018-06-12 23:31:53.441 04[KNL] using encryption algorithm AES_GCM_16 with key size 160
2018-06-12 23:31:53.441 04[KNL] using replay window of 0 packets
2018-06-12 23:31:53.441 04[IKE] inbound CHILD_SA 172.17.0.10-172.17.0.11{2} established with SPIs c4377183_i cdf90bca_o and TS 0.0.0.0/0 === 0.0.0.0/0
2018-06-12 23:31:53.441 04[IKE] outbound CHILD_SA 172.17.0.10-172.17.0.11{2} established with SPIs c4377183_i cdf90bca_o and TS 0.0.0.0/0 === 0.0.0.0/0

$ cat /proc/net/xfrm_stat
XfrmInError 0
XfrmInBufferError 0
XfrmInHdrError 0
XfrmInNoStates 0
XfrmInStateProtoError 0
XfrmInStateModeError 0
XfrmInStateSeqError 0
XfrmInStateExpired 0
XfrmInStateMismatch 0
XfrmInStateInvalid 0
XfrmInTmplMismatch 0
XfrmInNoPols 0
XfrmInPolBlock 0
XfrmInPolError 0
XfrmOutError 0
XfrmOutBundleGenError 0
XfrmOutBundleCheckError 0
XfrmOutNoStates 0
XfrmOutStateProtoError 0
XfrmOutStateModeError 0
XfrmOutStateSeqError 0

XfrmOutStateExpired 0
XfrmOutPolBlock 0
XfrmOutPolDead 0
XfrmOutPolError 0
XfrmFwdHdrError 0
XfrmOutStateInvalid 0
XfrmAcquireError 3 <<<<<<<<<<<

https://github.com/torvalds/linux/blob/4608f064532c28c0ea3c03fe26a3a5909852811a/net/xfrm/xfrm_input.c#L349

History

#1 - 20.06.2018 10:12 - Tobias Brunner

- Status changed from New to Feedback

Try using a more recent version. And if it's still a problem provide more logs.

#2 - 11.01.2019 23:45 - Noel Kuntze

- Status changed from Feedback to Closed

- Resolution set to No feedback