Tech-invite

http://www.tech-invite.com

# IPSec Guide

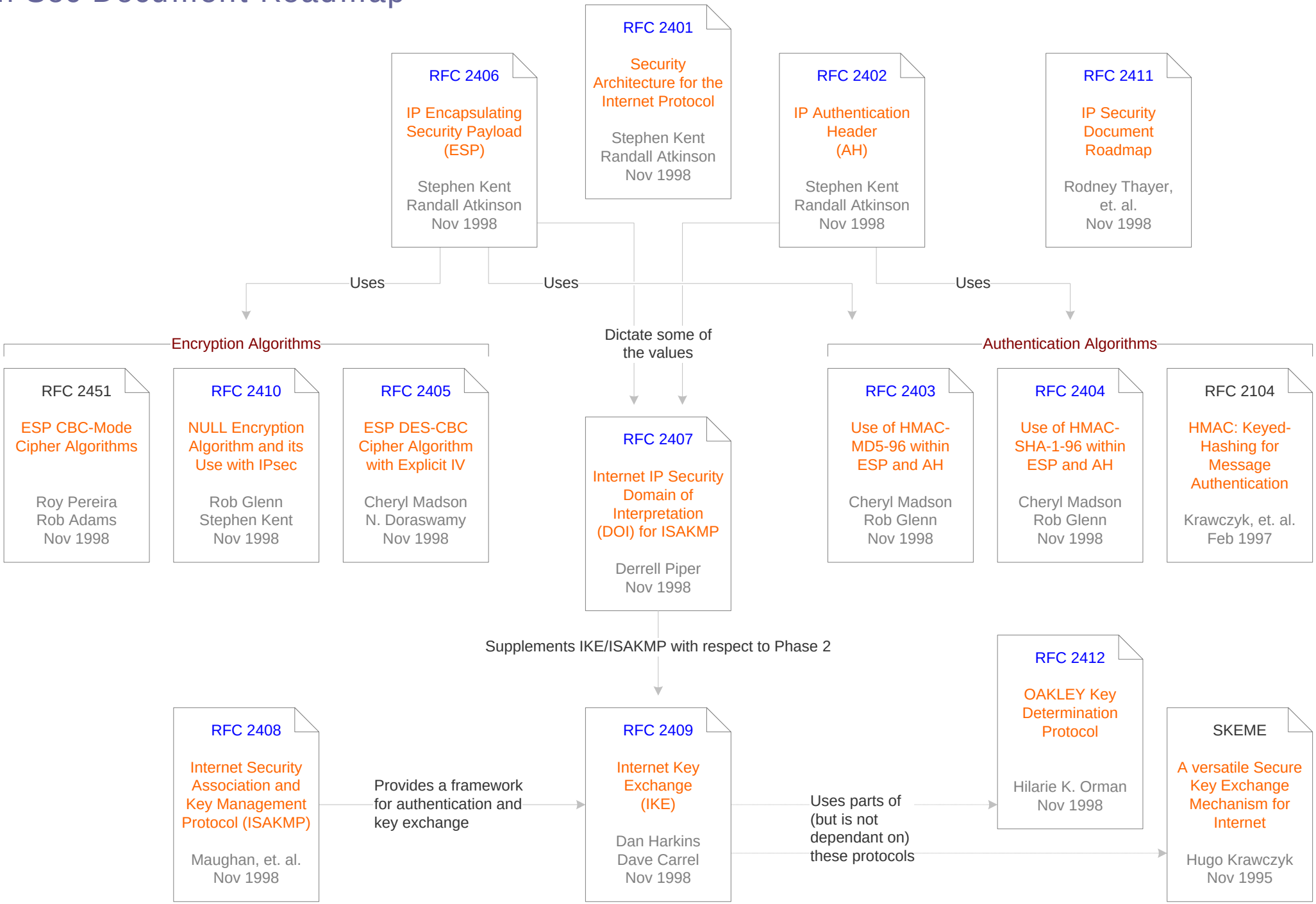
## Architecture & Traffic Processing

V1.0 – March 2, 2005

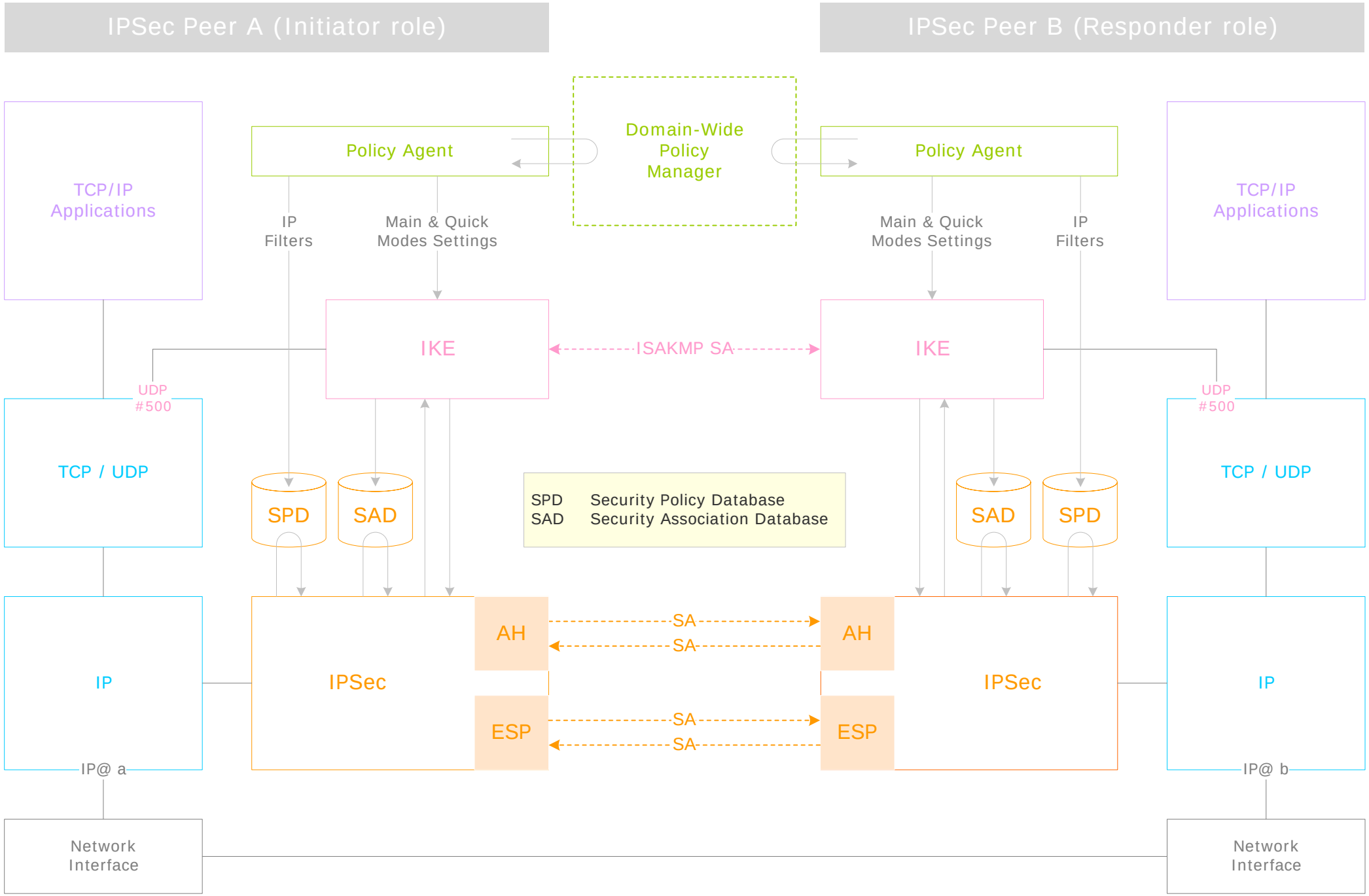
This document presents the document roadmap for IPSec, as well as a host-to-host architectural model, followed by a sequence of slides illustrating IPSec traffic processing related to this model.

8 pages

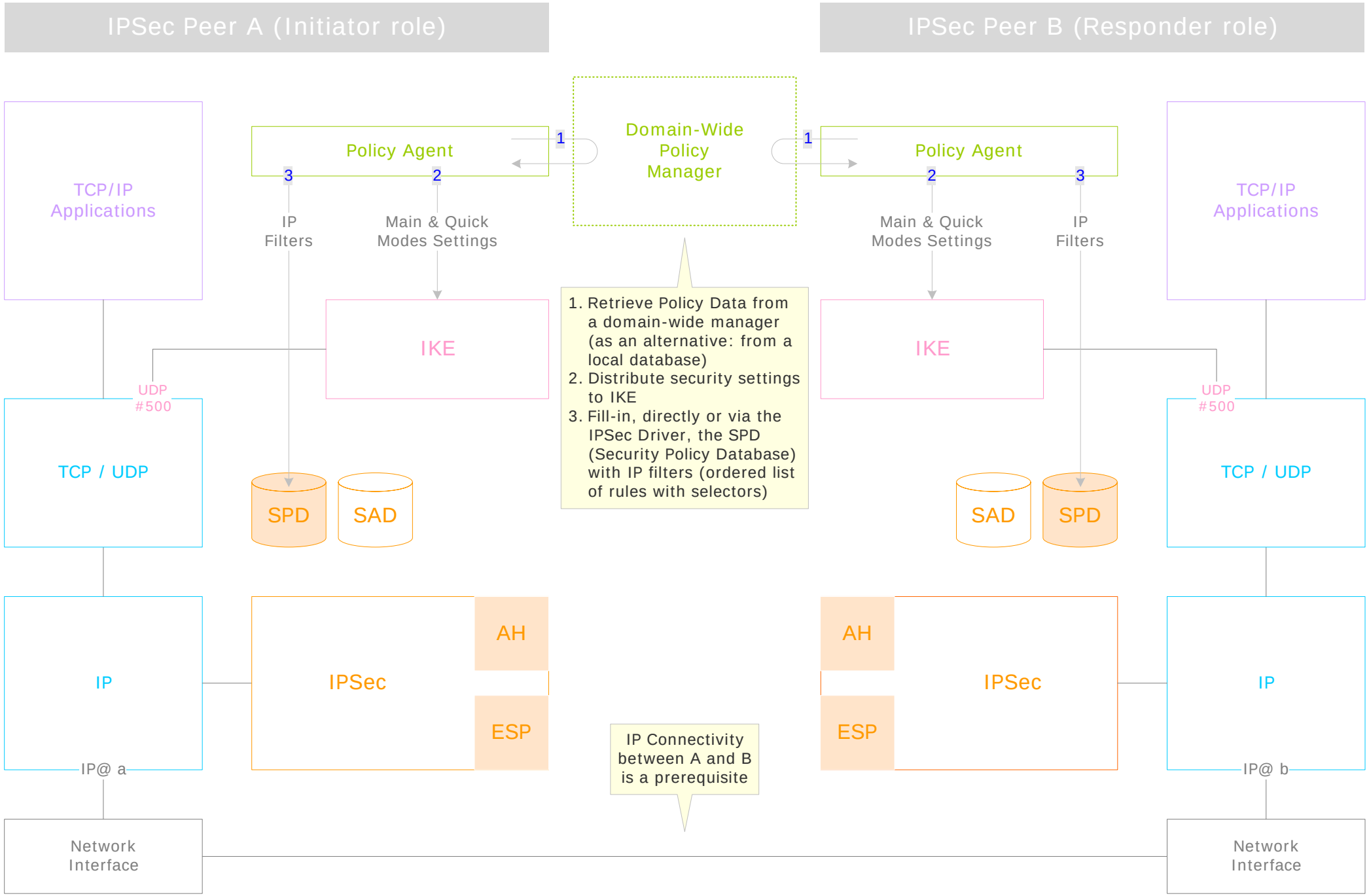
# IPSec Document Roadmap



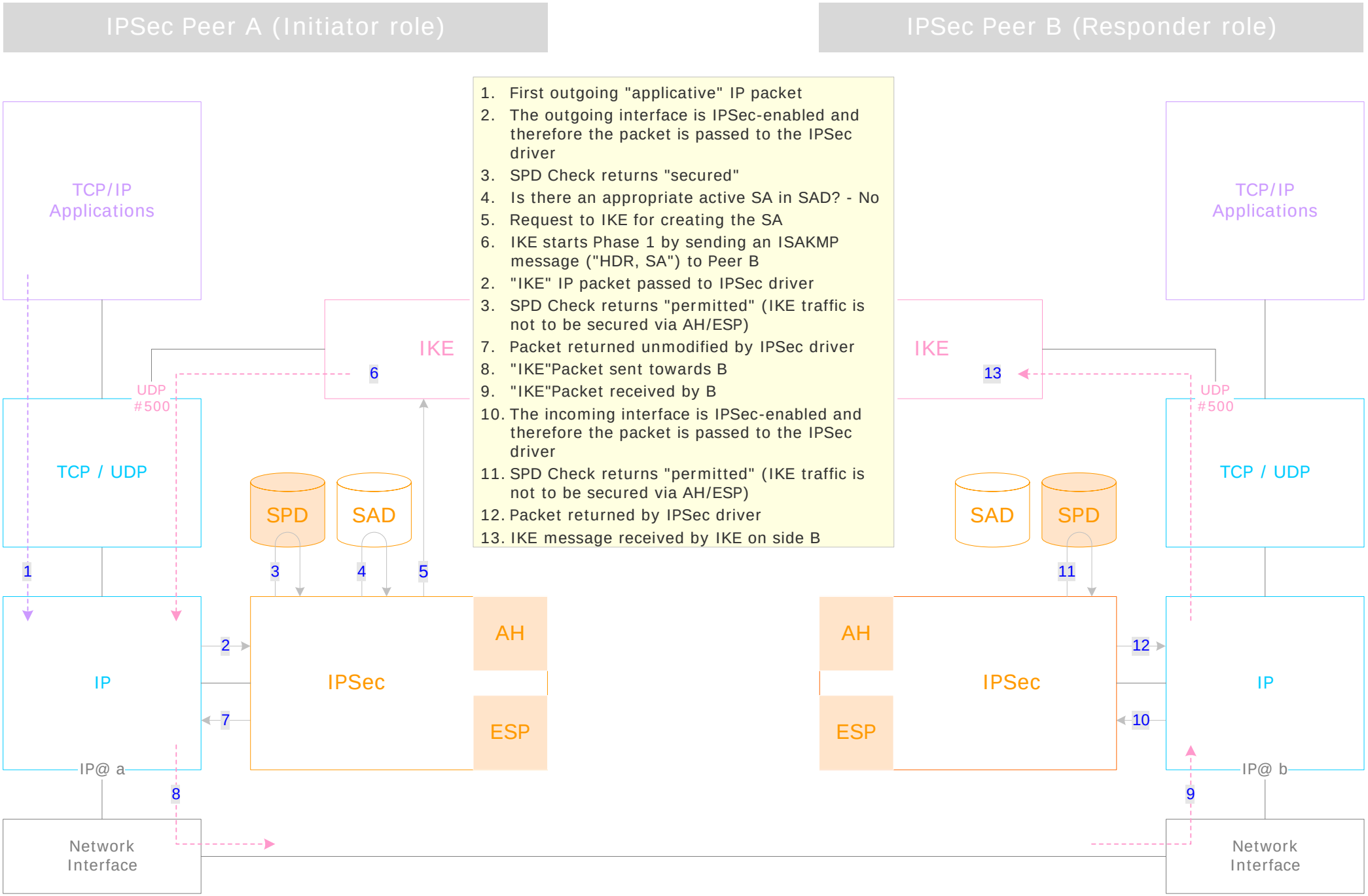
# IPSec Architecture – Host-to-Host Model



# IPSec Traffic Processing – 1) Initialisation

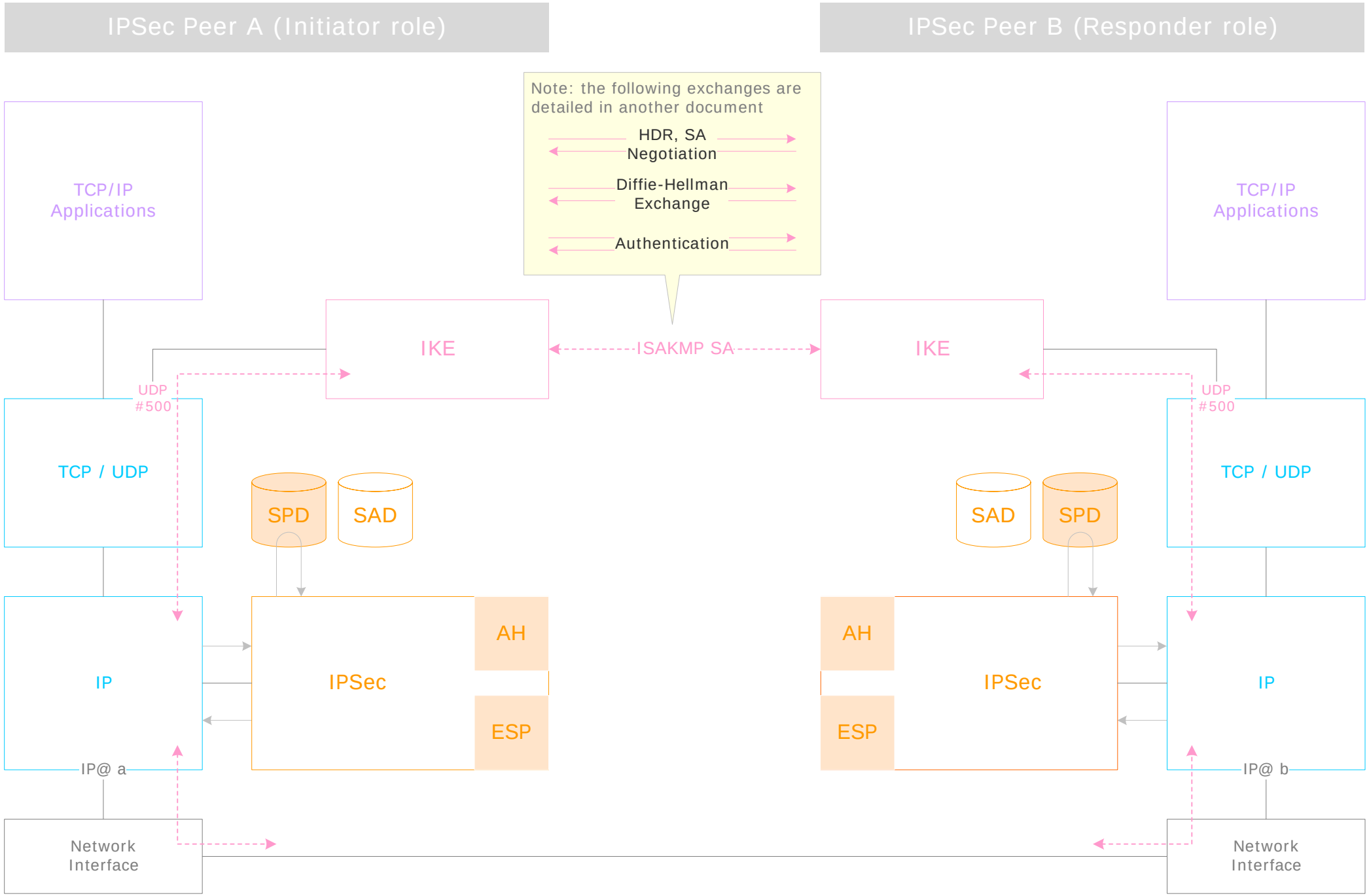


# IPSec Traffic Processing – 2) IKE Phase 1 Triggering

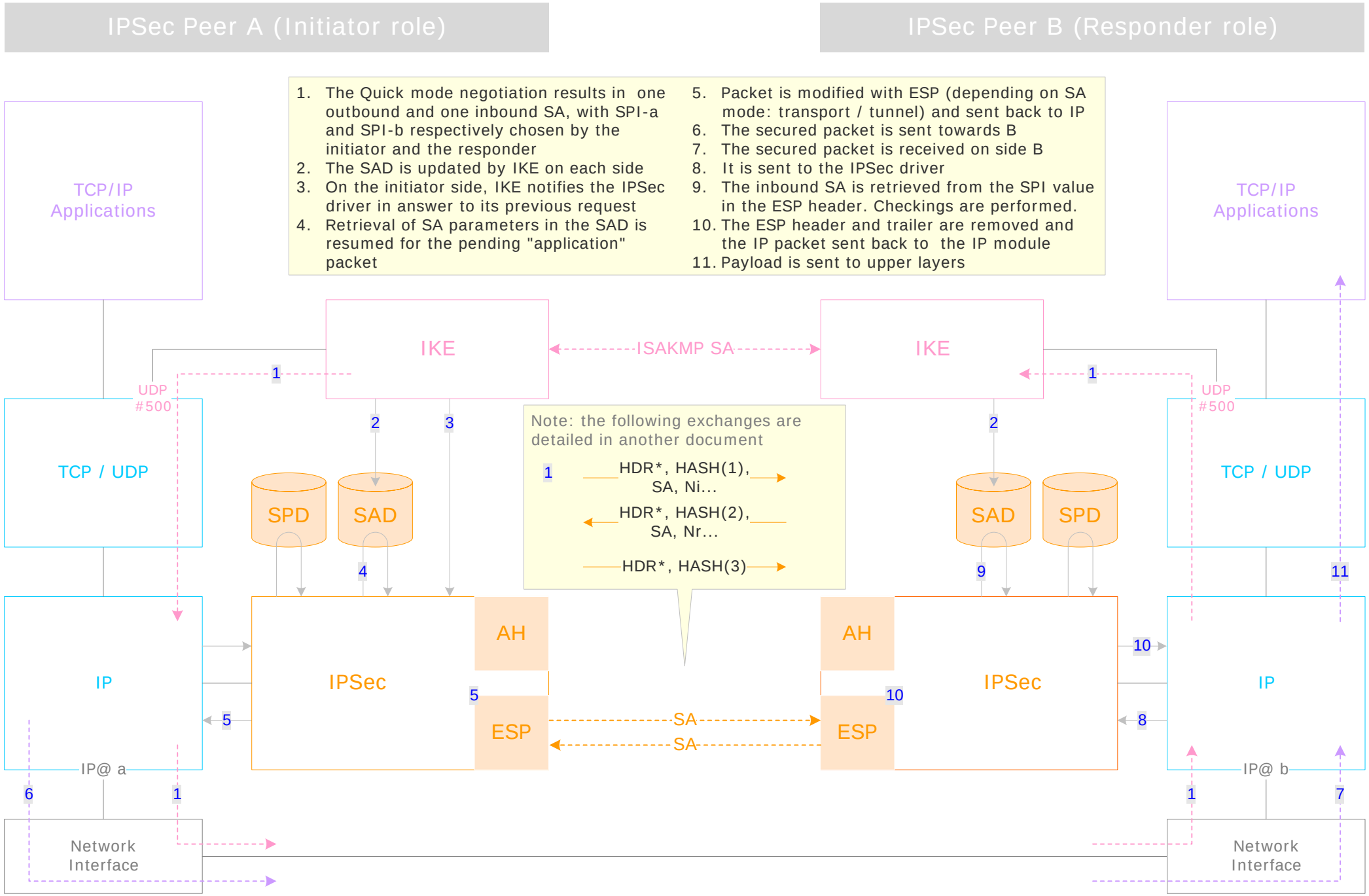



1. First outgoing "applicative" IP packet
2. The outgoing interface is IPSec-enabled and therefore the packet is passed to the IPSec driver
3. SPD Check returns "secured"
4. Is there an appropriate active SA in SAD? - No
5. Request to IKE for creating the SA
6. IKE starts Phase 1 by sending an ISAKMP message ("HDR, SA") to Peer B
2. "IKE" IP packet passed to IPSec driver
3. SPD Check returns "permitted" (IKE traffic is not to be secured via AH/ESP)
7. Packet returned unmodified by IPSec driver
8. "IKE"Packet sent towards B
9. "IKE"Packet received by B
10. The incoming interface is IPSec-enabled and therefore the packet is passed to the IPSec driver
11. SPD Check returns "permitted" (IKE traffic is not to be secured via AH/ESP)
12. Packet returned by IPSec driver
13. IKE message received by IKE on side B

# IPSec Traffic Processing – 3) IKE Phase 1 Completion



# IPSec Traffic Processing – 4) IKE Phase 2 & Secured Traffic Resumption



# IPSec Traffic Processing – 5) Secured (Outgoing) Traffic