

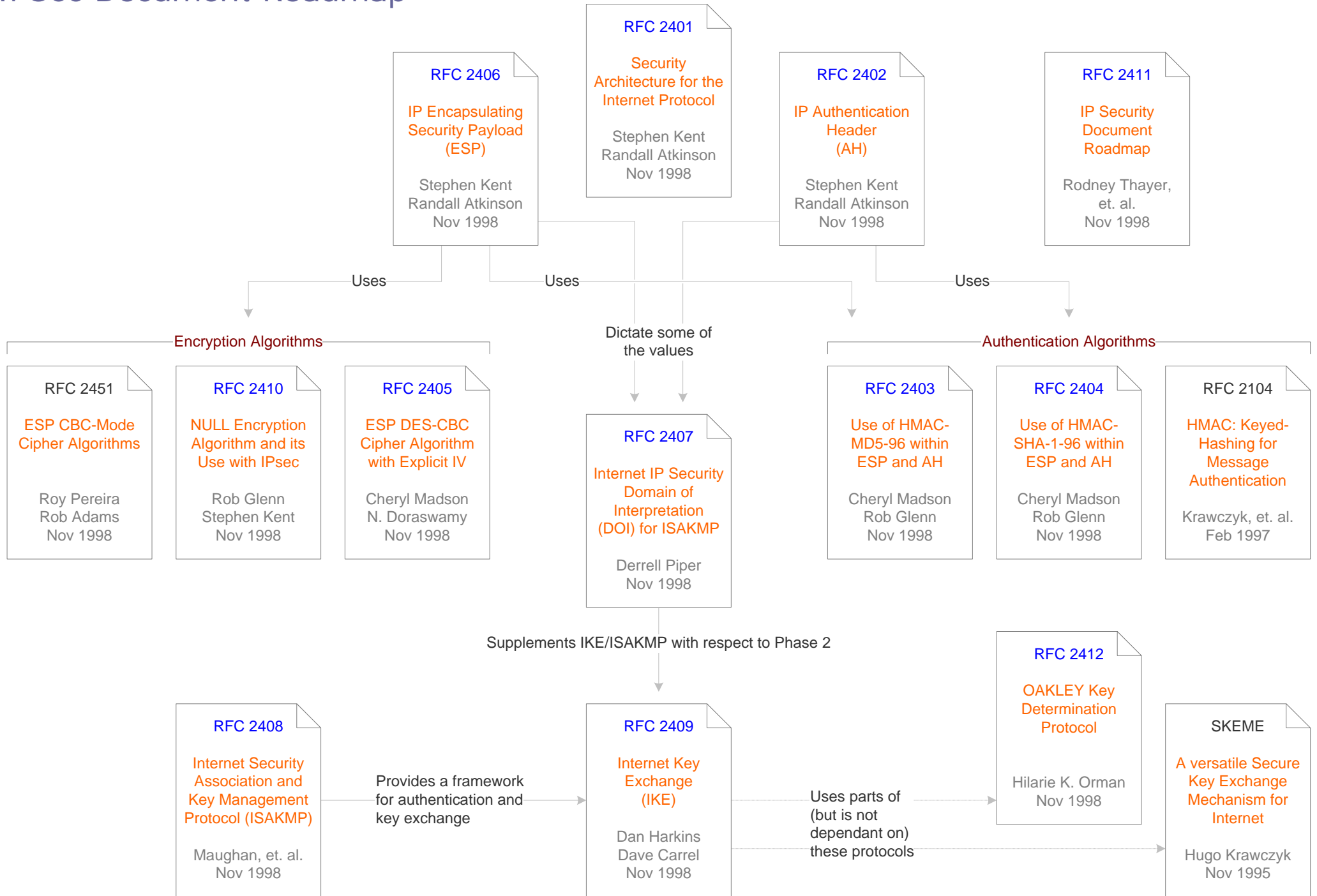
## IPSec Guide

### Architecture & Traffic Processing

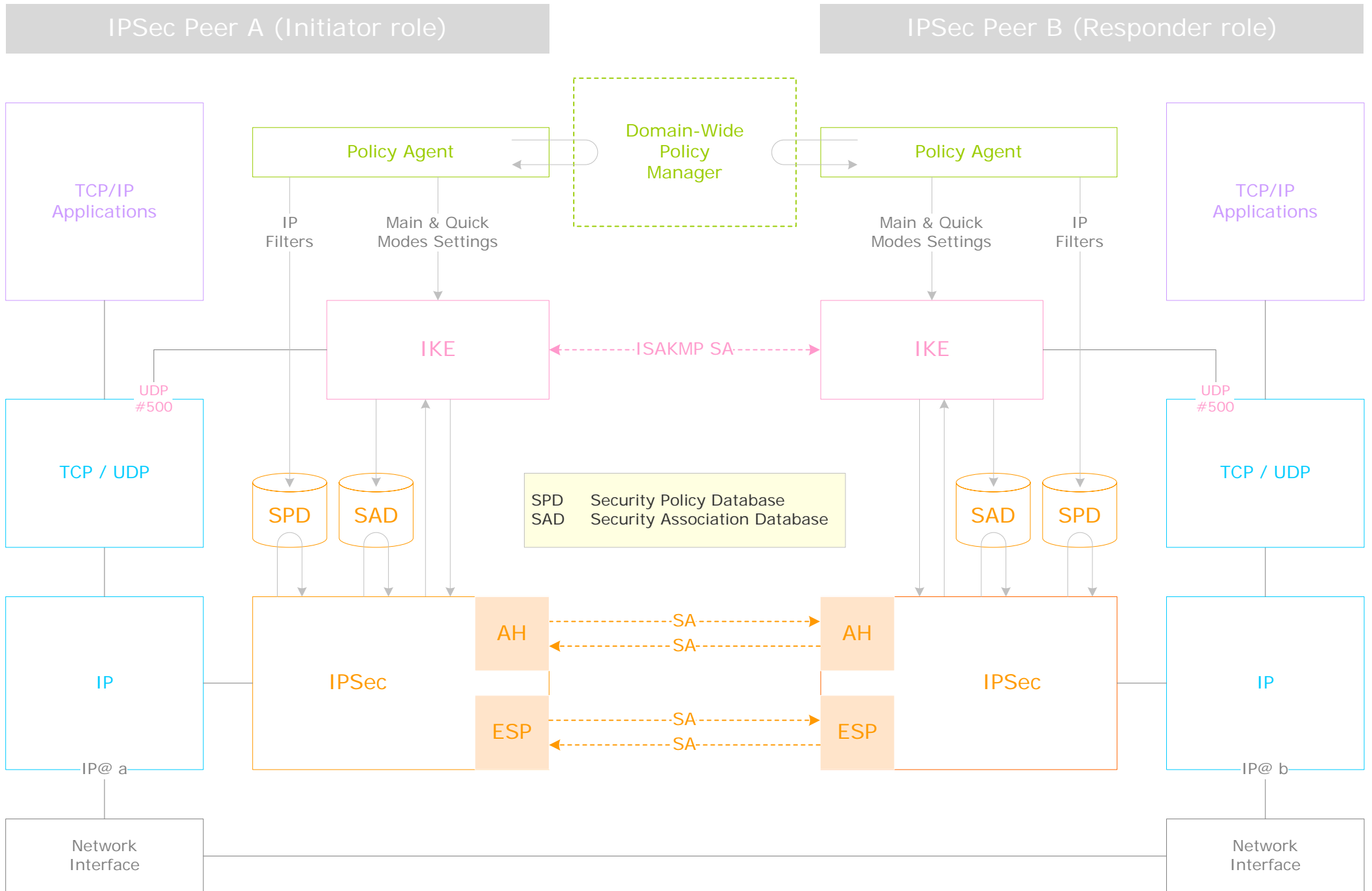
V1.0 – March 2, 2005

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.

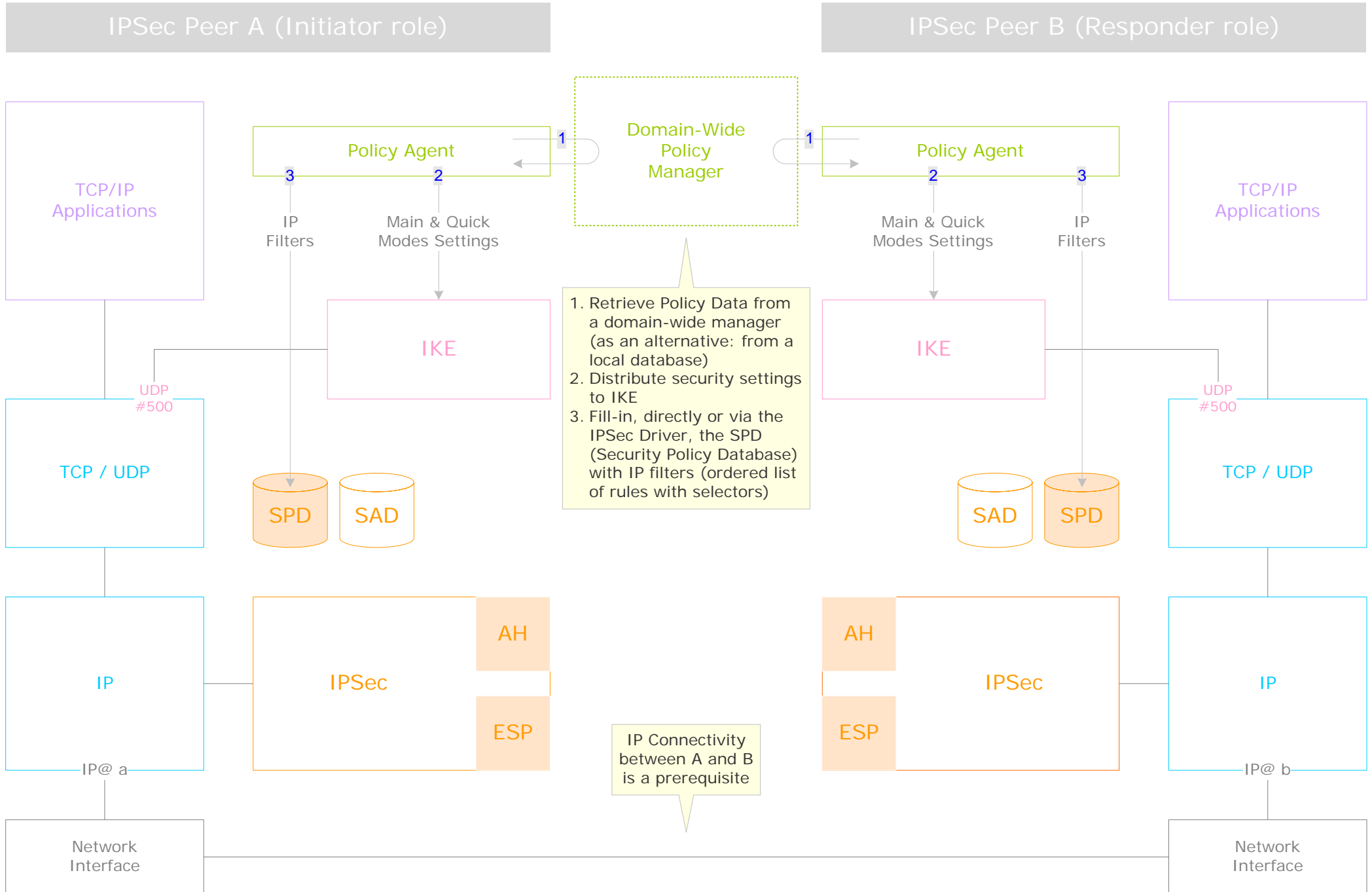
# IPSec Document Roadmap



# IPSec Architecture – Host-to-Host Model



# IPSec Traffic Processing – 1) Initialisation

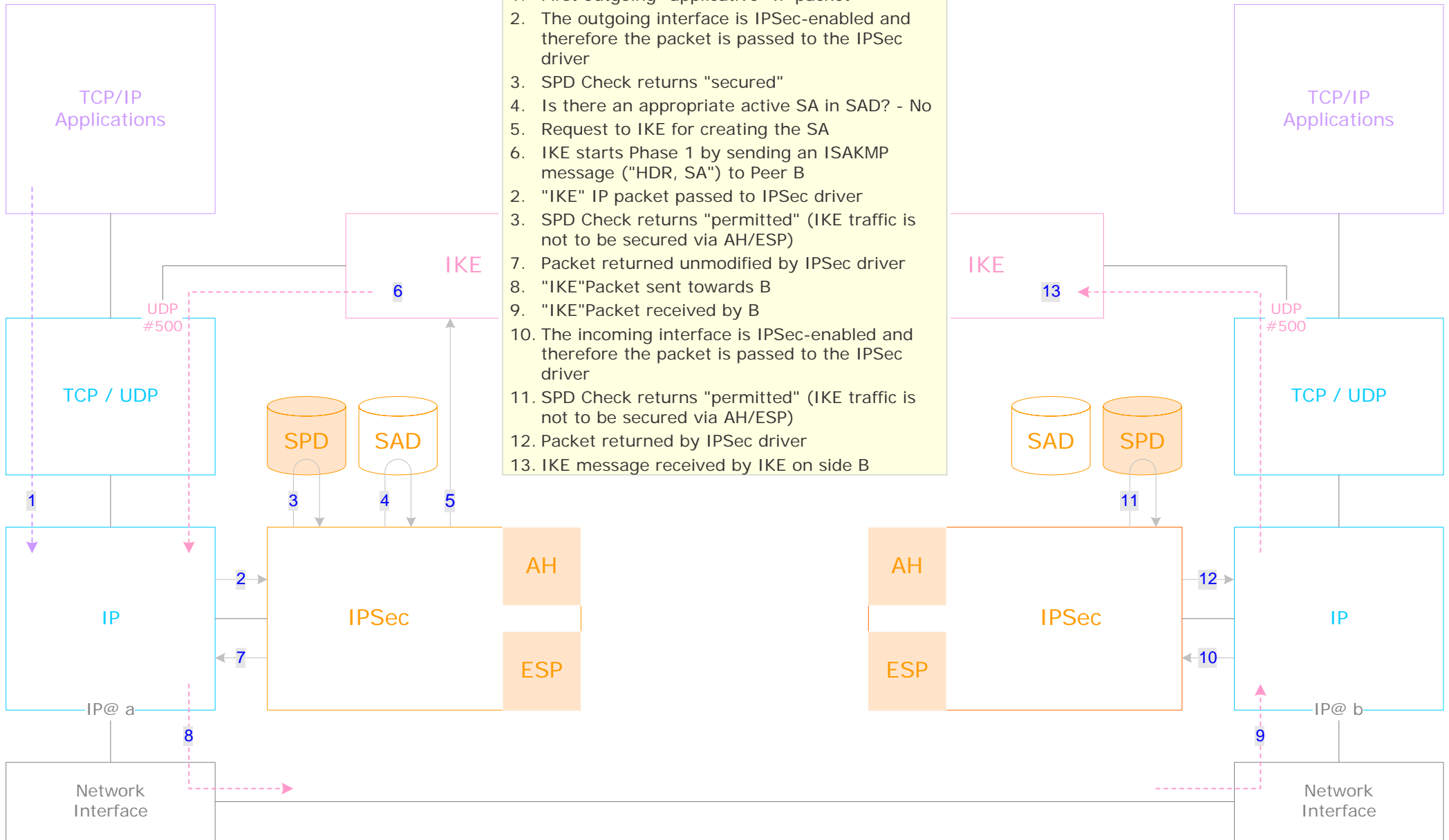


# IPSec Traffic Processing – 2) IKE Phase 1 Triggering

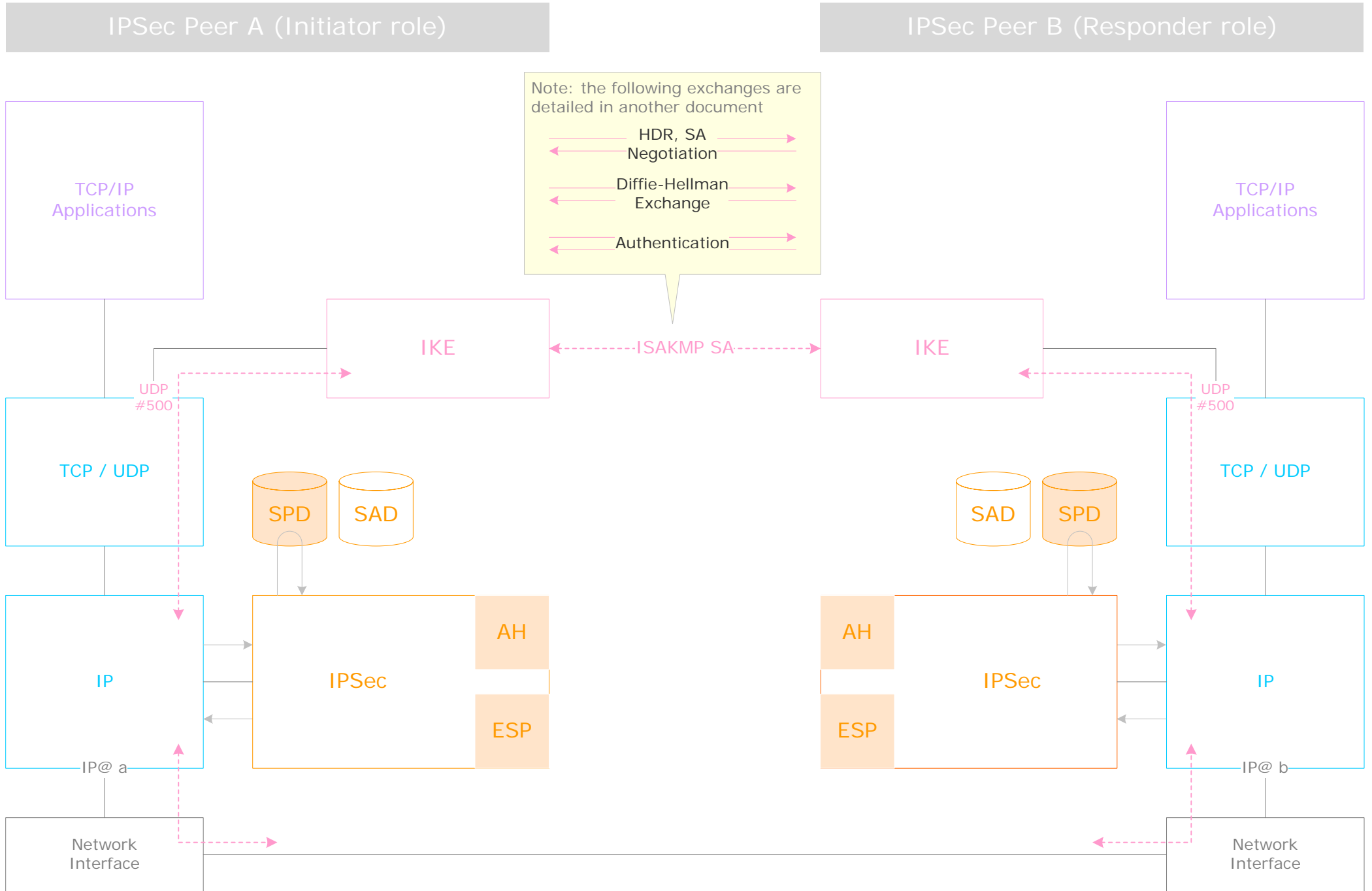
IPSec Peer A (Initiator role)

IPSec Peer B (Responder role)

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
7. "IKE" IP packet passed to IPSec driver
8. SPD Check returns "permitted" (IKE traffic is not to be secured via AH/ESP)
9. Packet returned unmodified by IPSec driver
10. "IKE"Packet sent towards B
11. "IKE"Packet received by B
12. The incoming interface is IPSec-enabled and therefore the packet is passed to the IPSec driver
13. SPD Check returns "permitted" (IKE traffic is not to be secured via AH/ESP)
14. Packet returned by IPSec driver
15. IKE message received by IKE on side B



# IPSec Traffic Processing – 3) IKE Phase 1 Completion

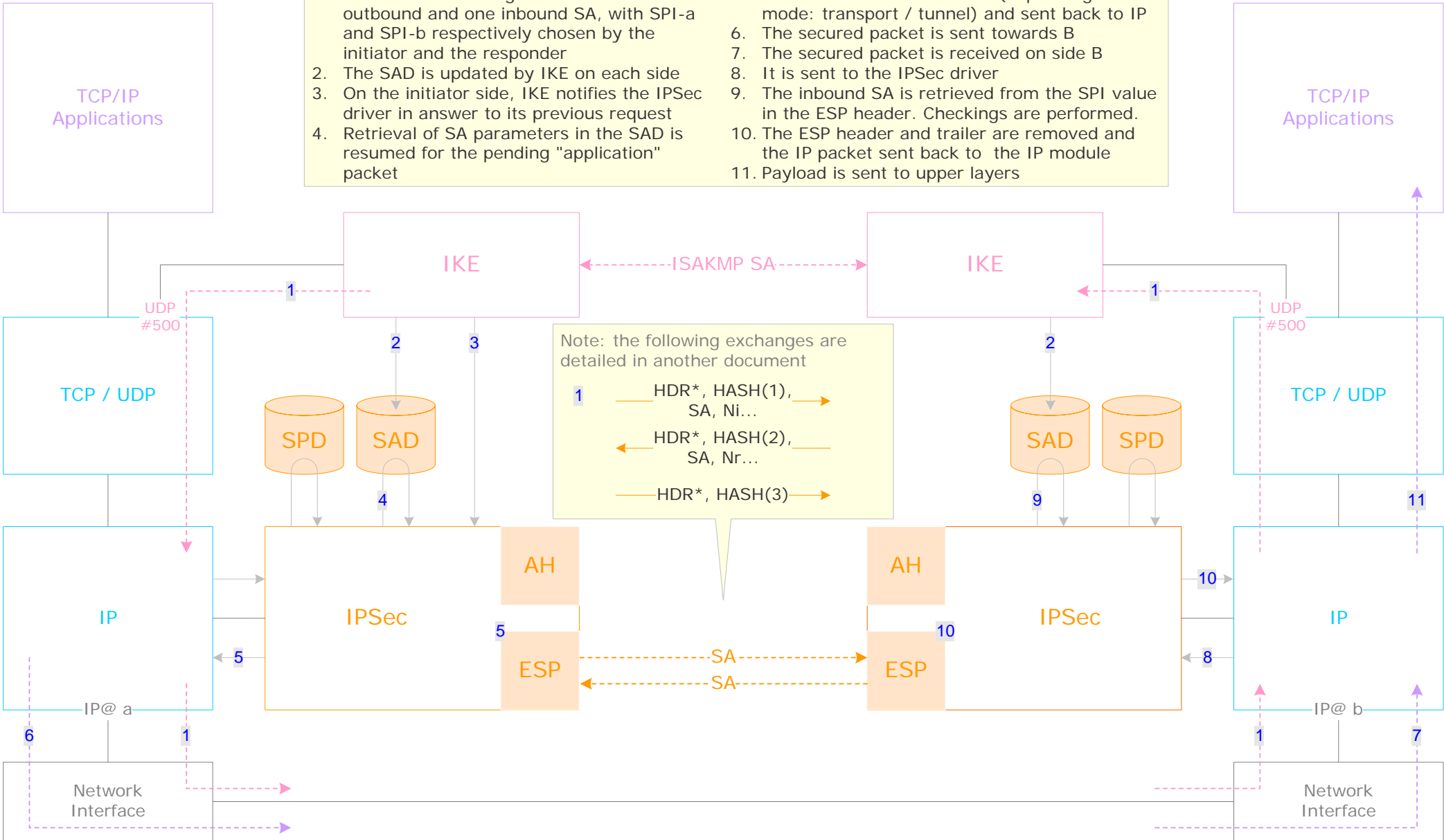


# IPSec Traffic Processing – 4) IKE Phase 2 & Secured Traffic Resumption

IPSec Peer A (Initiator role)

IPSec Peer B (Responder role)

1. The Quick mode negotiation results in one outbound and one inbound SA, with SPI-a and SPI-b respectively chosen by the initiator and the responder
2. The SAD is updated by IKE on each side
3. On the initiator side, IKE notifies the IPsec driver in answer to its previous request
4. Retrieval of SA parameters in the SAD is resumed for the pending "application" packet
5. Packet is modified with ESP (depending on SA mode: transport / tunnel) and sent back to IP
6. The secured packet is sent towards B
7. The secured packet is received on side B
8. It is sent to the IPsec driver
9. The inbound SA is retrieved from the SPI value in the ESP header. Checkings are performed.
10. The ESP header and trailer are removed and the IP packet sent back to the IP module
11. Payload is sent to upper layers



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

IPSec Peer A (Initiator role)

IPSec Peer B (Responder role)

