FIT 3031 – Information and Network Security
Tutorial 8

Q1 Give examples of applications of IPSec.

Q2 What are the services provided by IPSec?

Q3 What parameters identify an SA (security association) and what parameters characterize the nature of a particular SA?

Q4 What is the difference between transport mode and tunnel mode?

Q5 What is a replay attack and how can IPSec prevent it?

Q6 Why does ESP include a padding field?

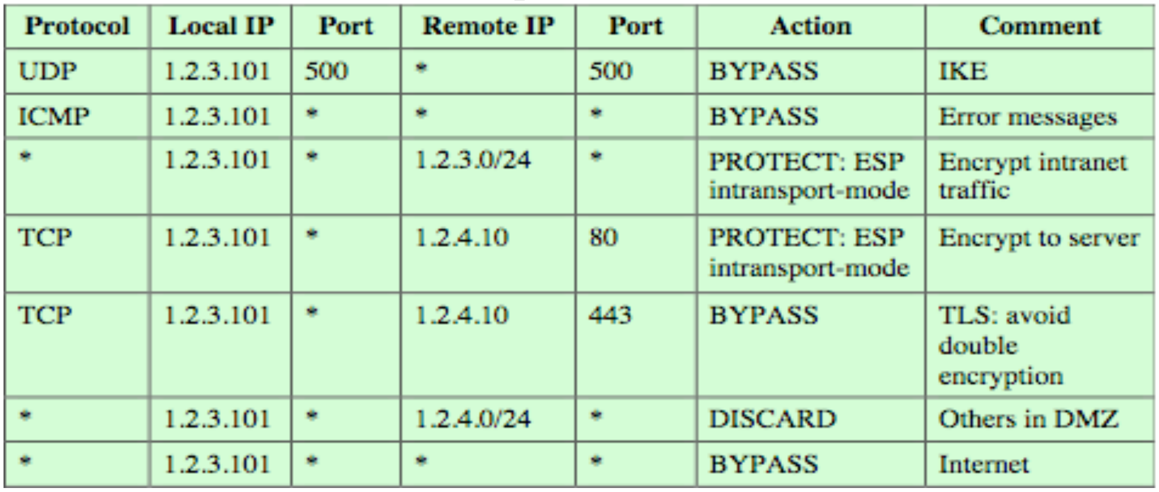
Q7 What are the roles of the Oakley key determination protocol and ISAKMP in IPSec?

Q8 What are the basic approaches to bundling SAs?

<u>PROBLEMS</u>:

1. Describe and explain each of the entries in the Table 8.2.

Table 8.2 Host SPD Example



Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

2. Draw a Figure similar to Figure 8.8 for AH.

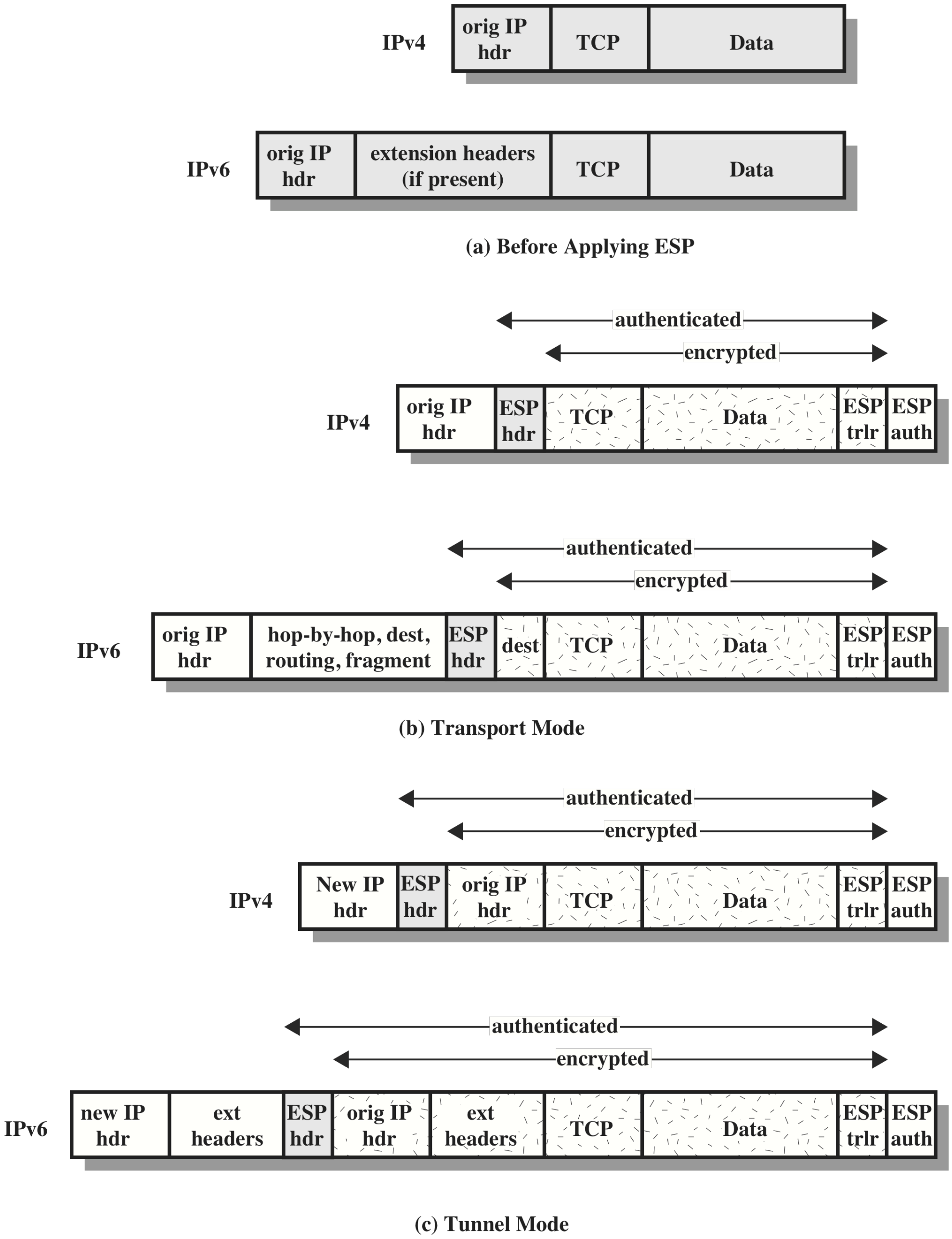


Figure 8.8 Scope of ESP Encryption and Authentication

3. List the major security services provided by AH and ESP respectively.

4. The IPSec architecture document states that when two transport mode SAs are bundled to allow for both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?

5. Where does IPSec reside in a protocol stack?