HW-Module8

- Due Mar 3 at 11:59pm
- Points 100
- Questions 6
- Available Jan 7 at 12am - Mar 3 at 11:59pm
- Time Limit None
- Allowed Attempts Unlimited

Instructions

Module 8 (Network Security--IP Security) - Homework Assignment

This quiz was locked Mar 3 at 11:59pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	279 minutes	100 out of 100

Score for this attempt: 100 out of 100

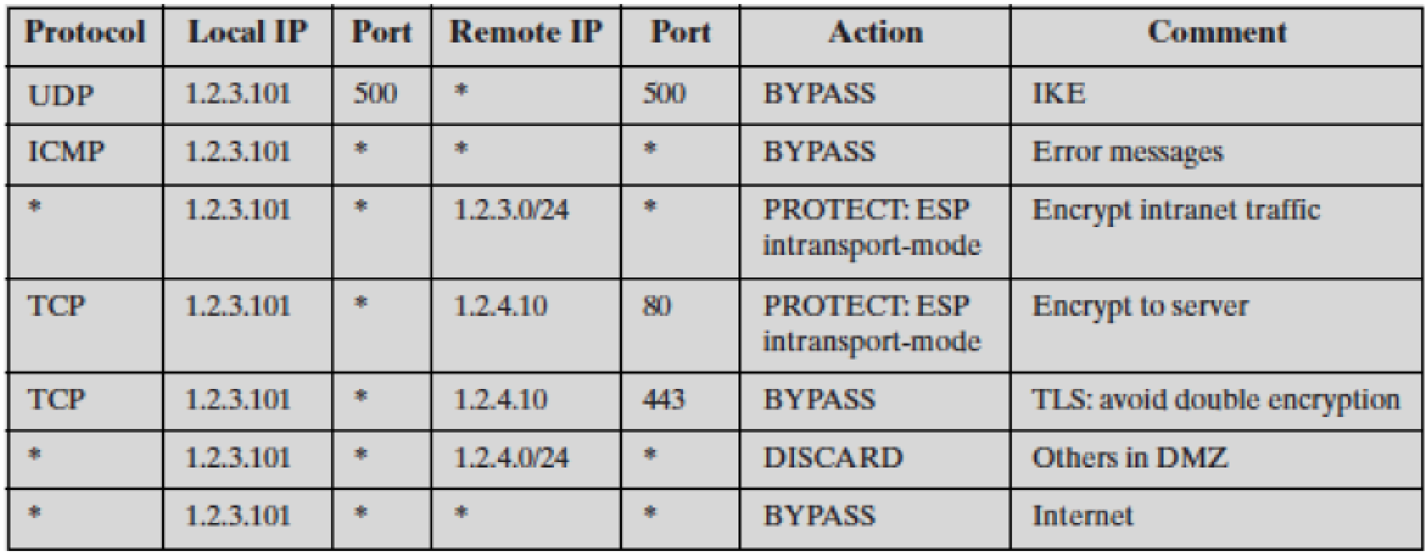
Submitted Mar 3 at 9:35pm

This attempt took 279 minutes.

Question 1

25 / 25 pts

Describe and explain each of the entries in the table below (Table 9.2 in the textbook).



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

Your Answer:

1. UDP traffic flowing through port 500 is used for setting up IKE. This traffic is going to be bypassed because it is necessary to not be interfered with when setting up secure VPN tunnels.

2. ICMP messages are used for network diagnostics. This message originated from the local IP 1.2.3.101 and will bypass filtering so the network diagnostic tool can function properly.

3. This entry applies ESP for encryption between local IP 1.2.3.101 and Remote IP 1.2.4.0/24. The action is "Protect" to encrypt intranet traffic to secure internal traffic using transport mode.

4. TCP traffic from 1.2.4.10 of local IP 1.2.3.101 will be sent through port 80. This port contains HTTP traffic so it will be encrypted using ESP in transport mode to secure communications to the server.

5. TCP traffic from port 1.2.4.10 of local IP 1.2.3.101 to port 443 should bypass encryption to avoid double encryption, for it is likely already secured by TLS

6. Traffic from 1.2.4.0/24 from local IP 1.2.3.101 should be discarded because it was deemed unnecessary because there are others in DMZ.

7. Traffic from local IP 1.2.3.101 will be bypassed to the internet.

UnansweredQuestion 2
25 / 25 pts

Draw a figure similar to Figure 8.8 in the PLE (Figure 9.8 in the textbook) for AH.

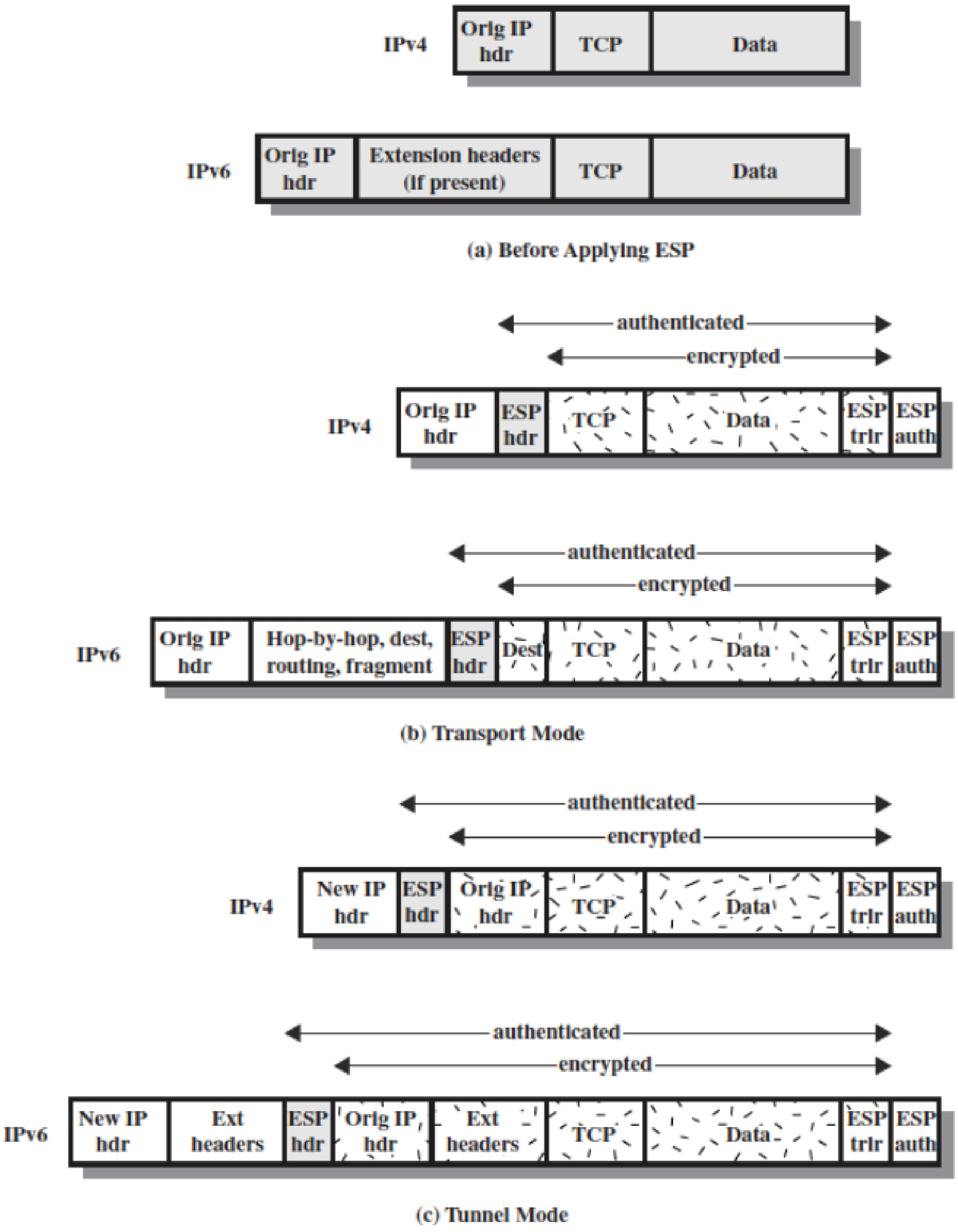


Figure 8.8-Scope of ESP Encryption and Authentication

If you want to attach a document with your solution, use the next question for the attachment.

Your Answer:

Question 3

0 / 0 pts

This is a dummy question so you can attach a document with your solution for the above question (question #2).

[IPv4 IPv6 AH.docx (https://canvas.odu.edu/files/32319290/download)](https://canvas.odu.edu/files/32319290/download)

Question 4

25 / 25 pts

Suppose that the current replay window spans from 120 to 530.

a. If the next incoming authenticated packet has sequence number 105, what will the receiver do with the packet, and what will be the parameters of the window after that?
b. If instead the next incoming authenticated packet has sequence number 440, what will the receiver do with the packet, and what will be the parameters of the window after that?
c. If instead the next incoming authenticated packet has sequence number 540, what will the receiver do with the packet, and what will be the parameters of the window after that?

Your Answer:

a. The next incoming packet 105 does not fall within the window range. This means it will be dropped and the parameters will remain the same.

b. The next incoming packet 440 does fall within the window range. This packet is accepted and if it is new the MAC will authenticate it, but if it is not authenticated it will be dropped.

c. The next incoming packet 540 falls after the window range. This means the packet will be checked, authenticated, and marked causing the parameters to expand to window range 120-540.

UnansweredQuestion 5

25 / 25 pts

End-to-end authentication and encryption are desired between two hosts. Draw figures similar to Figure 8.8 in the PLE (Figure 9.8 in the textbook) that show each of the following.

a. Transport adjacency with encryption applied before authentication.
b. A transport SA bundled inside a tunnel SA with encryption applied before authentication.
c. A transport SA bundled inside a tunnel SA with authentication applied before encryption.

If you want to attach a document with your solution, use the next question for the attachment.

Your Answer:

Question 6

0 / 0 pts

This is a dummy question so you can attach a document with your solution for the above question (question #5).

[SA.docx (https://canvas.odu.edu/files/32319778/download)](https://canvas.odu.edu/files/32319778/download)

Quiz Score: 100 out of 100