ΕΠΛ 674: Εργαστήριο 4

Ασκήσεις από τα Κεφάλαια 14, 19 (5th Edition)

University of Cyprus
Department of Computer Science

Παύλος Αντωνίου

NETworks Research Laboratory

Question 14.1

University of Cyprus

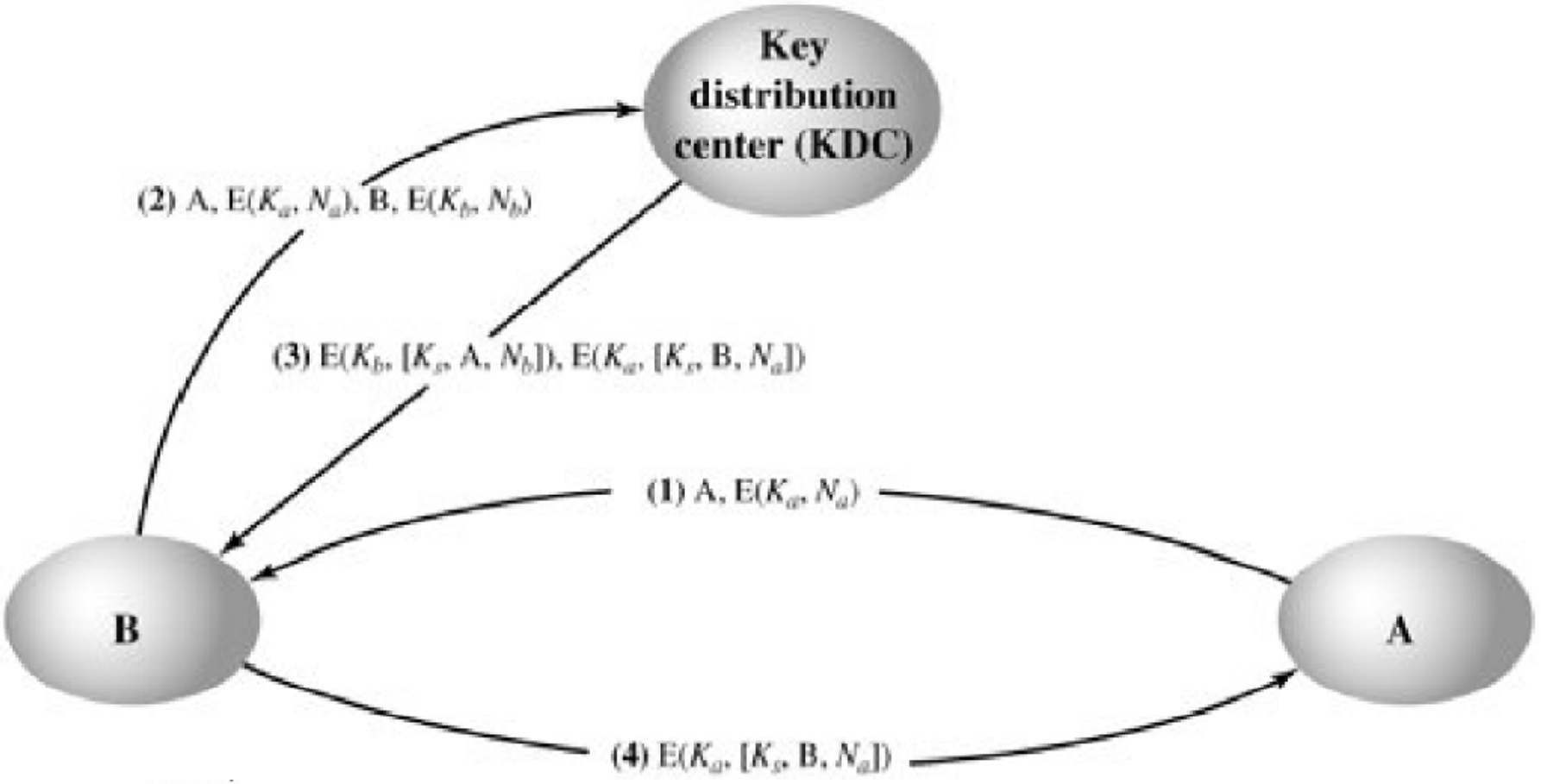
- Q: List ways in which secret keys can be distributed to two communicating parties.
- A: For two parties A and B, key distribution can be achieved in a number of ways, as follows:
  - A can select a key and physically deliver it to B.
  - A third party can select the key and physically deliver it to A and B.
  - If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
  - If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

Question 14.4

- Q: What is a KDC?
- A: A key distribution center is a system that is authorized to transmit temporary session keys to principals. Each session key is transmitted in encrypted form, using a master key (long-lasting key) that the key distribution center shares with the target principal.

Problem 14.1

- One local area network vendor provides a key distribution facility
  - Describe the scheme.



Problem 14.1

University of Cyprus

- A sends a connection request to B, with an event marker or nonce (Na) encrypted with the key that A shares with the KDC. If B is prepared to accept the connection, it sends a request to the KDC for a session key, including A's encrypted nonce plus a nonce generated by B (Nb) and encrypted with the key that B shares with the KDC. The KDC returns two encrypted blocks to B. One block is intended for B and includes the session key, A's identifier, and B's nonce. A similar block is prepared for A and passed from the KDC to B and then to A. A and B have now securely obtained the session key and, because of the nonces, are assured that the other is authentic.

Problem 14.1

University of Cyprus

– Compare this scheme to that of Figure 14.3. What are the pros and cons?

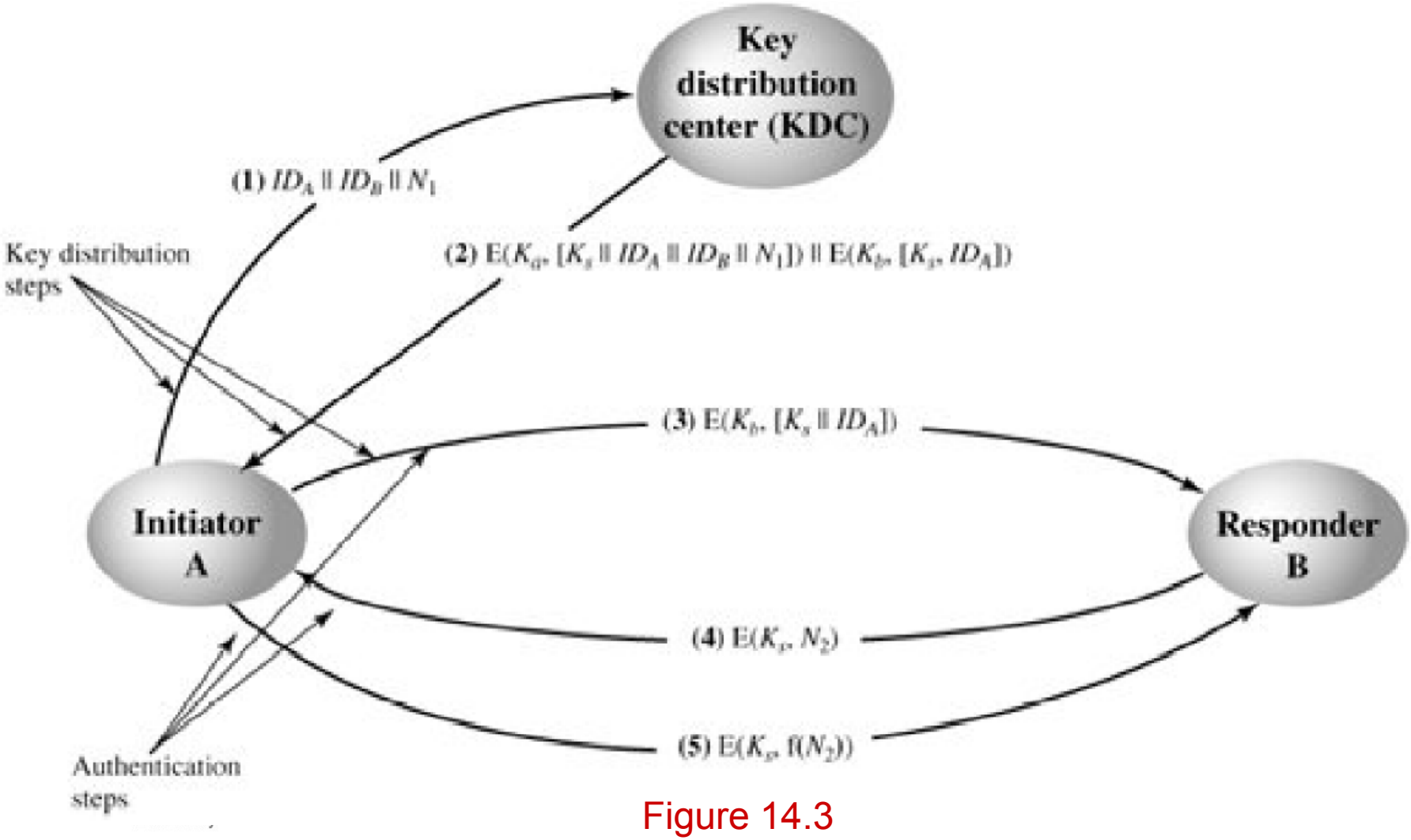


Figure 14.3

Problem 14.1

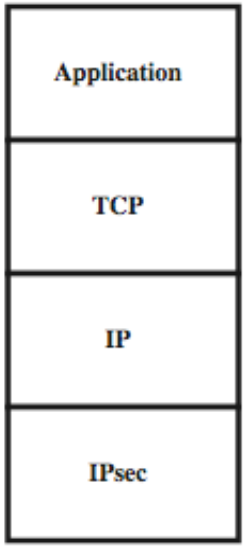
- The proposed scheme appears to provide the same degree of security as that of Figure 14.3. One advantage of the proposed scheme is that the, in the event that B rejects a connection, the overhead of an interaction with the KDC is avoided.

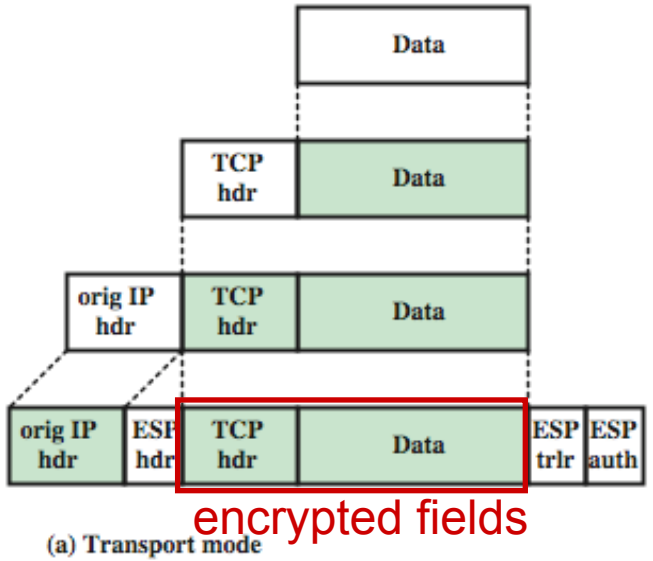
Question 19.4 (IPsec)

University of Cyprus

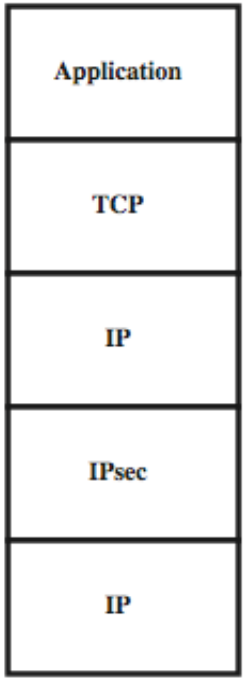
- Q: What is the difference between transport mode (κατάσταση μεταφοράς) and tunnel mode (κατάσταση σήραγγας)?
- A: **Transport mode** provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. **Tunnel mode** provides protection to the entire IP packet.

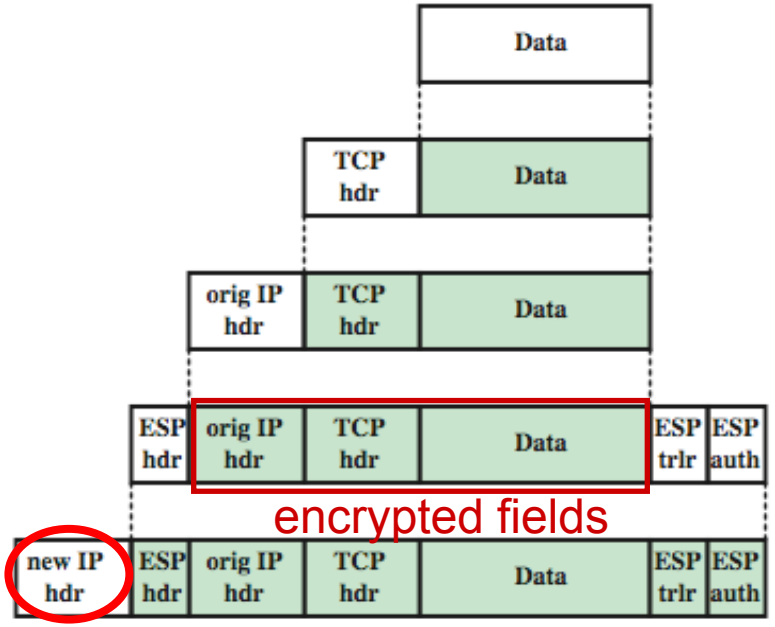
Transport & Tunnel Mode





(a) Transport mode





(b) Tunnel mode

Question 19.5

- Q: What is a replay attack (επίθεση επανάληψης)?
- A: A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.

Anti-replay service

University of Cyprus

- Για να αντιμετωπιστει η επίθεση επανάληψης πρεπει να χρησιμοποιουνται ακολουθιακοι αριθμοι (sequence numbers)
- Οταν εγκαθισταται μια νεα Συσχετιση Ασφαλειας (SA), ο αποστολεας αρχικοποιει τον ακολουθιακο αριθμο σε 0.
  - Αυξανεται κατα 1 για καθε πακετο
  - Δεν πρεπει να υπερβαινει το οριο $2^{32} – 1$
  - Αν φτασει το οριο αυτο, τοτε τερματιζεται η συγκεκριμενη SA και διαπραγματευεται η δημιουργια νεας SA με νεο κλειδι.

Anti-replay service

Αν N ειναι ο μεγαλύτερος ακολουθιακος αριθμος που εχει ληφθει μεχρι στιγμης και W το μεγεθος του παραθυρου, τοτε το δεξι ακρο του παραθυρου τοποθετειται στο N και ο αποδεκτης δεχεται μονο πακετα με ακολουθιακο αριθμο μεσα στο παραθυρο [*N –W+1, N*]

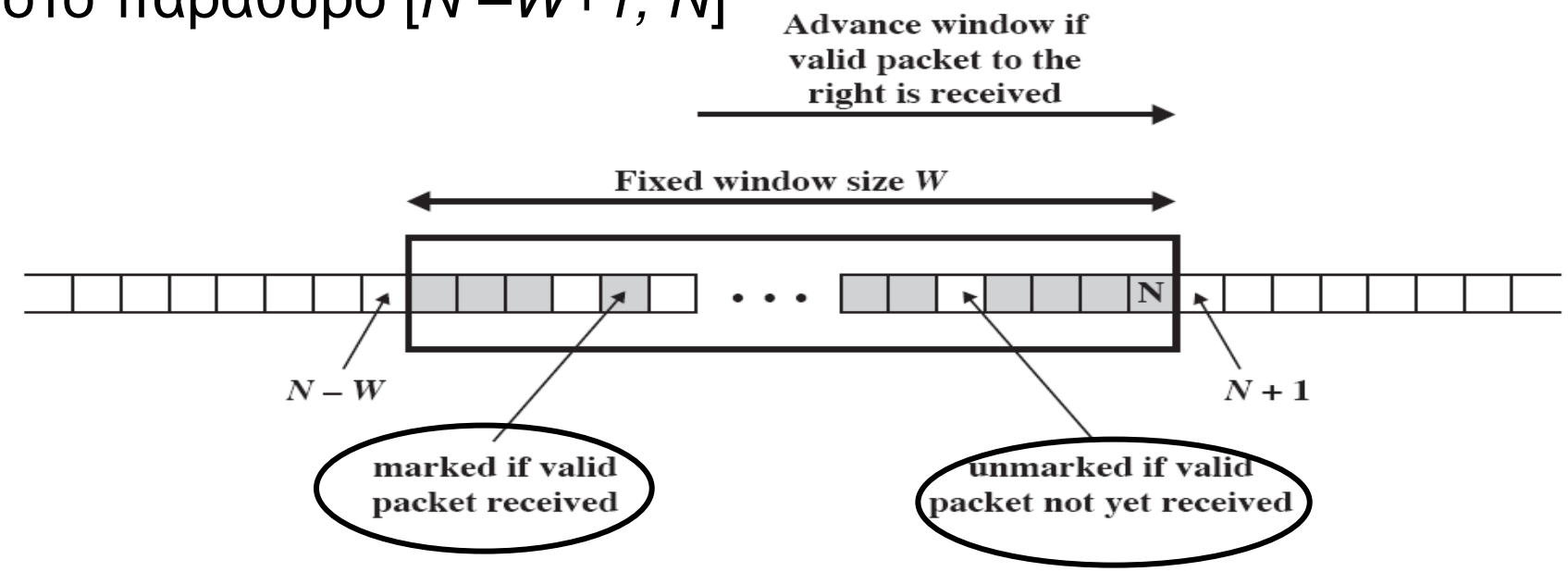


Figure 19.6 Anti-Replay Mechanism

Security Associations (SA)

University of Cyprus

- Συσχετιση Ασφαλειας (SA) ειναι μια μονοδρομη σχεση μεταξυ αποστολεα και παραληπτη που παρεχει υπηρεσιες ασφαλειας στην κυκλοφορια που διεξαγεται πανω σε αυτη.
- Το μεσο με το οποιο η κυκλοφορια IP σε ένα κόμβο συσχετιζεται με μια συγκεκριμενη SA ειναι η βαση δεδομενων πολιτικης ασφαλειας (Security Policy Database, SPD)

Security Policy Database (SPD)

University of Cyprus

- Συσχετιζει την κινηση IP με συγκεκριμενες SAs
  - Ταιριαζει ενα υποσυνολο της κινησης IP με την SA που αυτο αντιστοιχει.
  - Καθε καταχωρηση στη βαση SPD προσδιοριζεται απο ενα συνολο τιμων πεδιων του IP και πρωτοκολλων υψηλοτερου επιπεδου που ονομαζονται επιλογεις (selectors).
  - Οι επιλογεις χρησιμοποιουνται για το φιλτραρισμα της εξερχομενης κινησης, με σκοπο την κετευθυνση της σε συγκεκριμενη SA.
  - Selectors: Διευθυνση IP πηγης και προορισμου, θυρες πηγης και προορισμου, Πρωτοκολλο του Transport Layer.

Problem 19.1

University of Cyprus

- Q: Explain each row of the Security Policy Database shown below.

selectors	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

Problem 19.1

University of Cyprus

- row 1: Traffic between this host and any other host, both using port 500, and using UDP, bypasses IPsec. This is used for IKE traffic.
- row 2: ICMP message to or from any remote address are error messages, and bypass IPsec.
- row 3: Traffic between 1.2.3.101 and 1.2.3.0/24 is intranet traffic and must be protected by ESP, with the exception of traffic defined in earlier rows.
- row 4: TCP traffic between this host (1.2.3.101) and the server (1.2.4.10) on server port 80 is ESP protected.
- row 5: TCP traffic between this host (1.2.3.101) and the server (1.2.4.10) on server port 80 is protected by TLS and so can bypass IPsec.
- row 6: Any other traffic between 1.2.3.101 and 1.2.3.0/24 is prohibited and is discarded.
- row 7: Any other traffic between 1.2.3.101 goes to the Internet and bypasses IPsec.