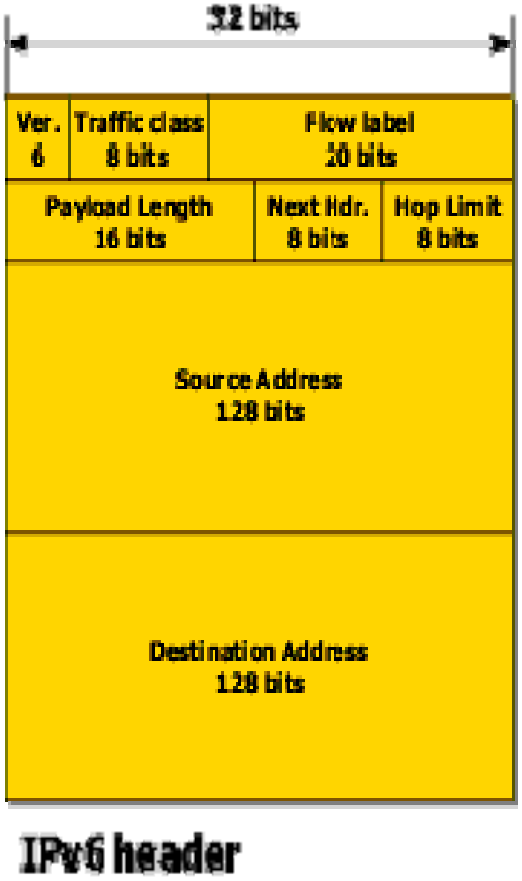
Το πρωτόκολλο IPSec στο VPN

Εισαγωγή – Γενικά χαρακτηριστικά TCP/IP

- Τα TCP/IP πρωτόκολλα δεν έχουν δικούς τους μηχανισμούς κρυπτογράφησης.
- Ένα IP πακέτο περιέχει πληροφορίες τόσο για την πηγή όσο και για τον προορισμό, καθώς και για το είδος των δεδομένων που περιέχει.

Κεφαλίδα IPv6 πακέτων



IPv6 header

Η μεγέθους 40-byte IPv6 κεφαλίδα έχει τα εξής 8 πεδία:

•Version – η έκδοση του Internet πρωτοκόλλου.

•Traffic class – περιέχει πληροφορίες που αφορούν την προτεραιότητα του πακέτου.

•Flow label – Όλα τα πακέτα που ανήκουν στην ίδια ροή δεδομένων ταυτοποιούνται από το πεδίο αυτό. Με βάση αυτό κάνουν και τη δρομολόγηση οι routers.

•Payload length – περιέχει πληροφορία σχετικά με το μέγεθος του IP πακέτου.

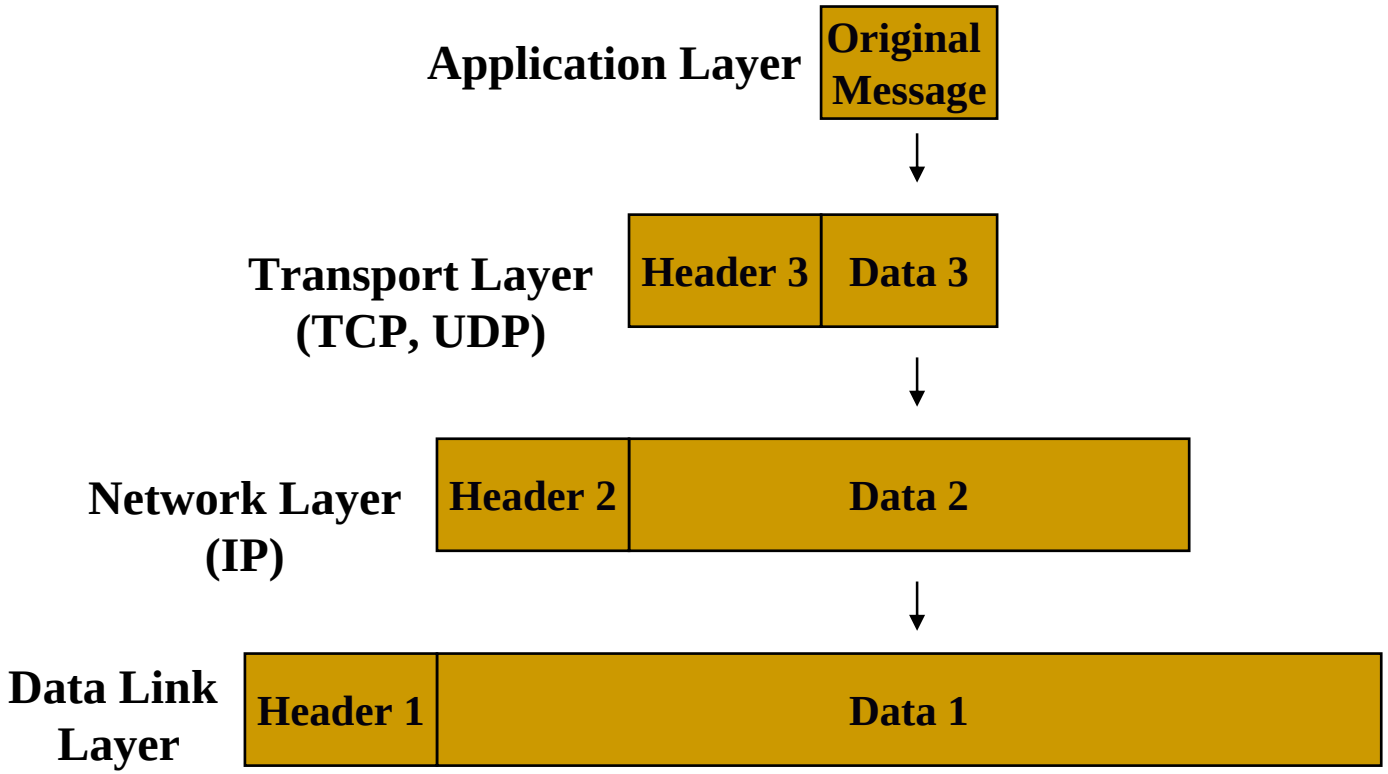
•Next header – Υποδηλώνει το επόμενο, ενθυλακωμένο στο IP, πρωτόκολλο

•Hop limit – Υποδηλώνει το μέγιστο πλήθος hops που επιτρέπονται.

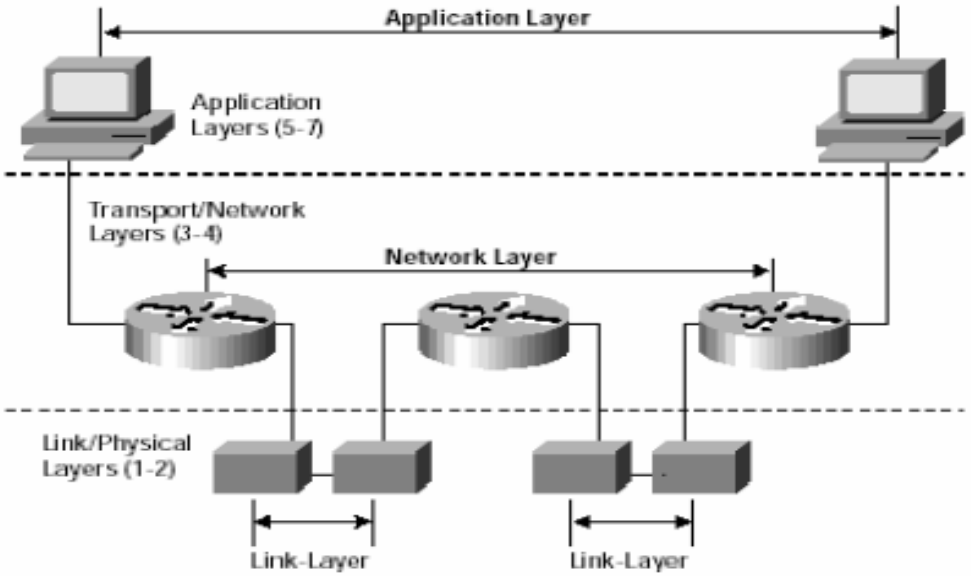
•Source address – Η διεύθυνση του αποστολέα

•Destination address –Η διεύθυνση του παραλήπτη

Ενθυλάκωση πακέτων στο TCP/IP



Ασφάλεια σε διάφορα επίπεδα



Link Layer:	PPTP/L2TP
Network Layer:	IPsec, GRE
Transport Layer:	TLS
Application Layer:	mail: PGP/S-MIME
	web: SSL

Πρωτόκολλο IPSec

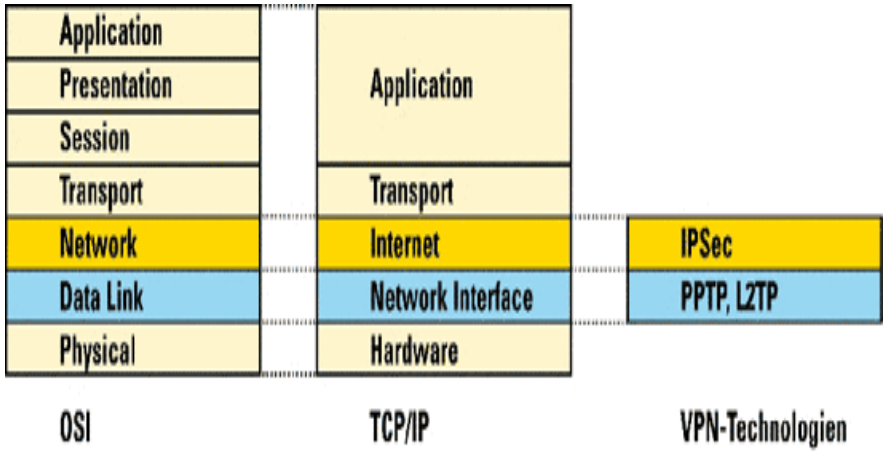
- IP Security (IPSec): **Σύνολο πρωτοκόλλων ανεπτυγμένων από το**

Internet Engineering Task Force (IETF) με στόχο την ασφαλή μετάδοση και ανταλλαγή δεδομένων (packets) μέσω του στρώματος IP

- Αιτία ανάπτυξης IPSec: **Αντιμετώπιση των ακόλουθων απειλών :**
- ✓ **Απώλεια της Ιδιωτικότητας των Δεδομένων (Loss of Privacy)**
- ✓ **Απώλεια Ακεραιότητας Δεδομένων (Loss of Data Integrity)**
- ✓ **Προσποίηση Ταυτότητας (Identity Spoofing)**
- ✓ **Πρόσβαση μη εξουσιοδοτημένων χρηστών**

Τι κάνει το IPSec??

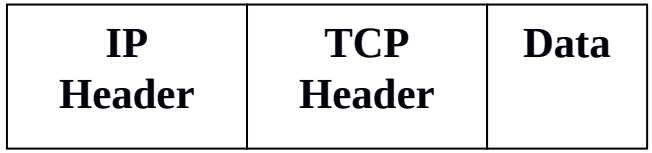
- Προσθέτει δύο κεφαλίδες – Κεφαλίδα πιστοποίησης (IP Authentication Header - AH) για πιστοποίηση ταυτότητας και Ενθυλακωμένη Ασφάλεια (Encapsulating Security Payload - ESP) για κρυπτογράφηση.
- Μπορεί να χρησιμοποιηθεί και σε IPv4 (εκτός από τα IPv6) πακέτα.
- Χρησιμοποιεί τα ακόλουθα:
  - Diffie-Hellman αλγορίθμους για την ανταλλαγή συμμετρικού κλειδιού
  - DES ή AES ή άλλους μπλοκ αλγορίθμους για την κρυπτογράφηση
  - Συναρτήσεις κατακερματισμού για την πιστοποίηση της ακεραιότητας δεδομένων
  - Ψηφιακούς πιστοποιητές (digital certificates) για την επικύρωση των δημοσίων κλειδιών



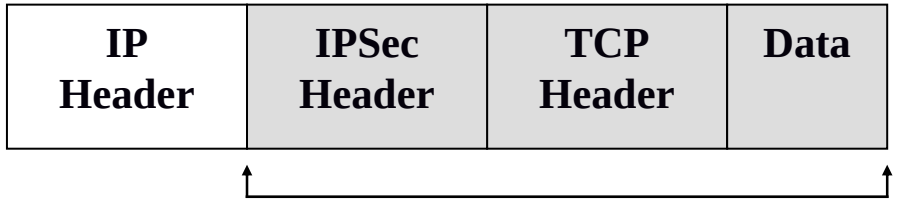
Τρόποι ή καταστάσεις λειτουργίας IPSec

- Τρόπος μεταφοράς (Transport Mode) (κυρίως σε LAN):

Αρχικό IP πακέτο

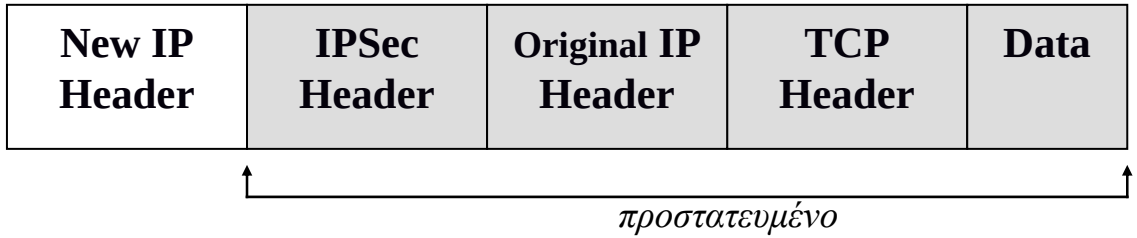


Transport Mode προστατευμένο πακέτο



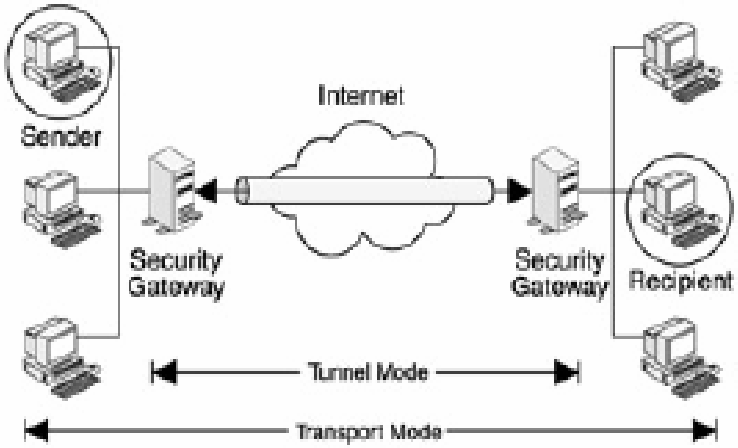
- Τρόπος διόδου (Tunnel Mode) (κυρίως σε VPN):

Tunnel Mode Προστατευμένο πακέτο



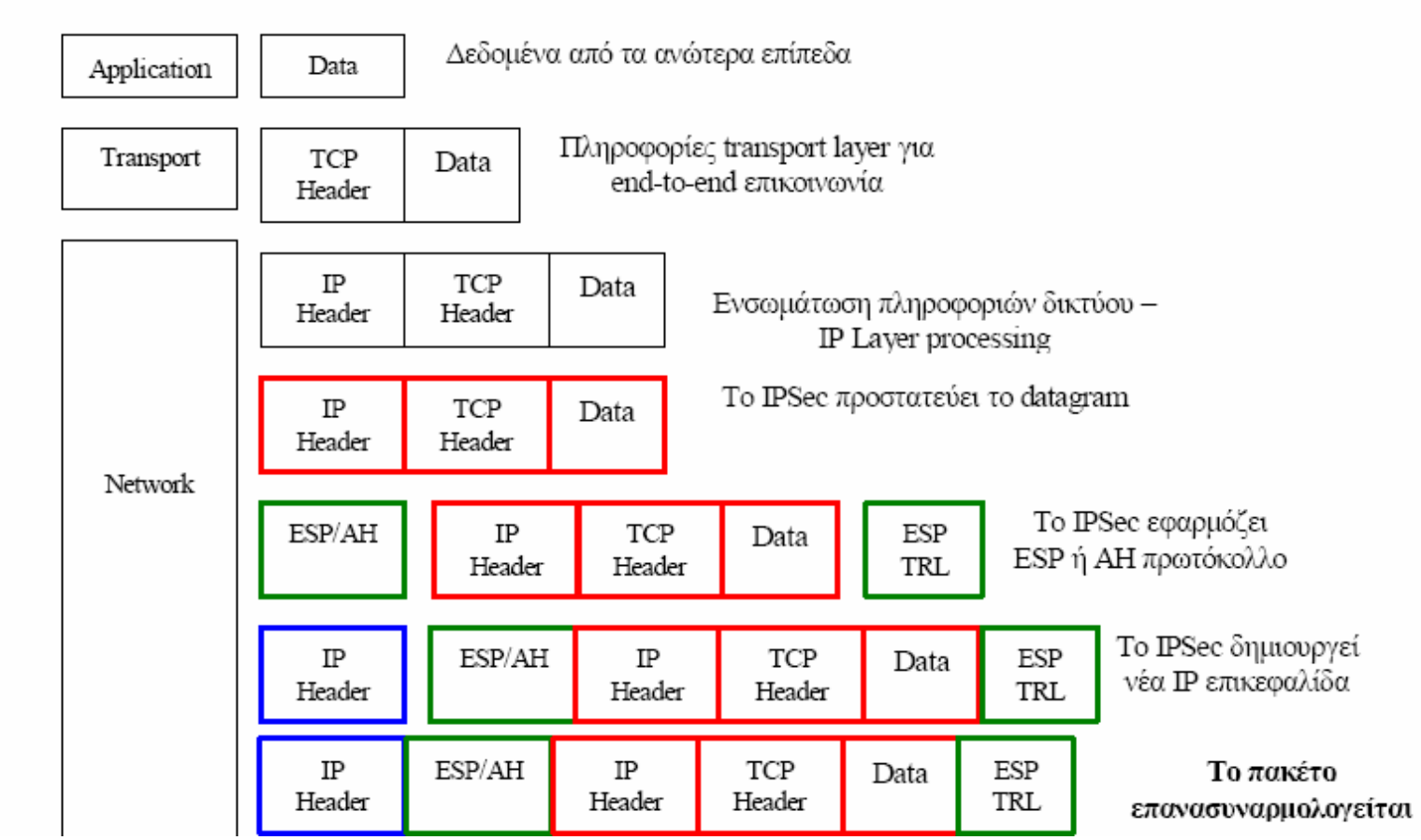
Περιγραφή τρόπων λειτουργίας IPSec

- Tunnel mode:
  - Το νέο IP πακέτο «ταξιδεύει» από τον έναν δρομολογητή στον άλλο χωρίς να μπορούν να διαβάσουν το αρχικό πακέτο που βρίσκεται ενθυλακωμένο.
  - Με ESP κρυπτογραφείται όλο το αρχικό IP πακέτο
  - Με AH αυθεντικοποιείται όλο το αρχικό IP πακέτο, καθώς και κάποια πεδία της νέας IP κεφαλίδας

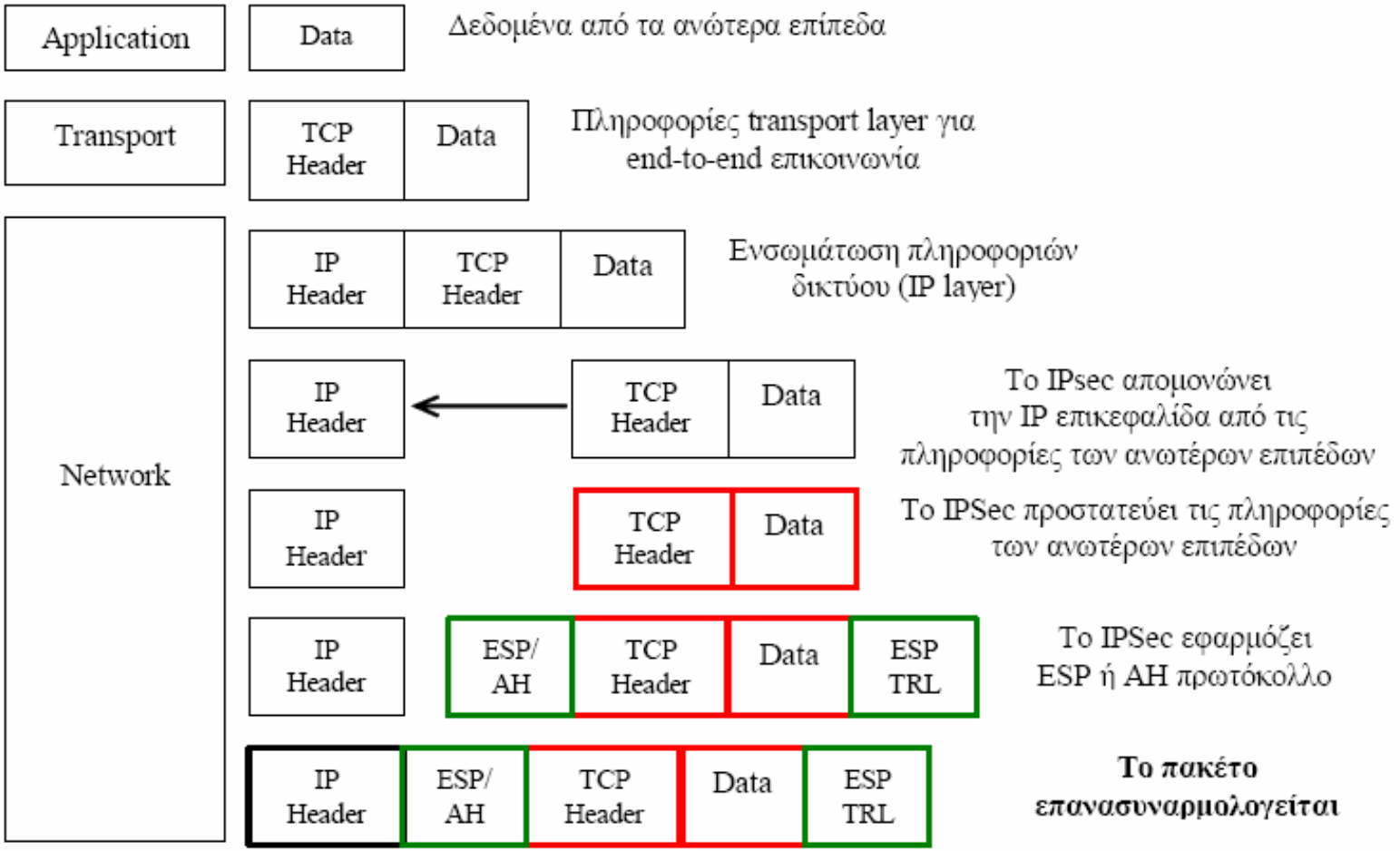


- Transport mode:
  - Χρησιμοποιείται για προστασία της επικοινωνίας από άκρο-σε-άκρο (π.χ. Client-server εφαρμογές).
  - Με ESP κρυπτογραφείται το αρχικό IP payload (όχι η κεφαλίδα)
  - Με AH αυθεντικοποιείται το IP payload, καθώς και κάποια πεδία της IP κεφαλίδας

IPSec σε κατάσταση διόδου (tunnel mode)



IPSec σε κατάσταση μεταφοράς (transport mode)



Πλεονεκτήματα/Μειονεκτήματα των δύο τρόπων

- Tunnel mode: επιτρέπει στους δρομολογητές να λειτουργούν ως IPSec proxies, με άλλα λόγια το λειτουργικό σύστημα του χρήστη δεν χρειάζεται τροποποίηση. Επιπρόσθετα, προστατεύει από τον κίνδυνο ανάλυσης της κίνησης (αφού είναι κρυπτογραφημένα τα πάντα, ακόμα και οι διευθύνσεις αποστολέα και παραλήπτη). Από την άλλη μεριά όμως, απαιτείται επιπρόσθετη επεξεργασία στα πακέτα, από ό,τι στο transport mode.
- Transport mode: Σε κάθε πακέτο προστίθενται μόνο μερικά bytes (η νέα κεφαλίδα). Επίσης, οι δρομολογητές βλέπουν τις διευθύνσεις πηγής/προορισμού και συνεπώς μπορούν να δρομολογήσουν κατά συγκεκριμένη QoS. Μειονέκτημα είναι ότι ανάλυση κίνησης μπορεί πια να γίνει.

IPSec Security Associations

- Δύο οντότητες (τελικοί χρήστες) που επιθυμούν να επικοινωνήσουν πρέπει να συμφωνήσουν εκ των προτέρων στις παραμέτρους επικοινωνίας, όσον αφορά την ασφάλεια

- Η **Συσχέτιση Ασφάλειας (Security Association - SA)** είναι μία συμφωνία των δύο άκρων για μεθόδους και αλγορίθμους ασφαλείας που επιθυμούν να χρησιμοποιήσουν κατά τη σύνοδο:
- αλγόριθμοι κρυπτογράφησης
- αλγόριθμοι αυθεντικοποίησης
- κλειδιά, διάρκεια ισχύος κλειδιών κτλ

Βασικές παράμετροι μιας SA

- IP διεύθυνση πηγής και προορισμού
- Ένα ID χρήστη
- Πρωτόκολλο μεταφοράς (TCP ή UDP)
- Τον αλγόριθμο για έλεγχο πιστοποίησης ταυτότητας, καθώς και τα αντίστοιχα κλειδιά
- Τον αλγόριθμο που χρησιμοποιείται για κρυπτογράφηση, καθώς και τα κλειδιά
- Τρόπος λειτουργίας του IPSec (transfer ή tunnel mode)
- Διάρκεια ζωής μιας SA

IPSec Security Associations (περιγραφή)

- **Κάθε SA είναι <u>μονόδρομη:</u>** μία για τα εισερχόμενα και μία για τα εξερχόμενα μηνύματα

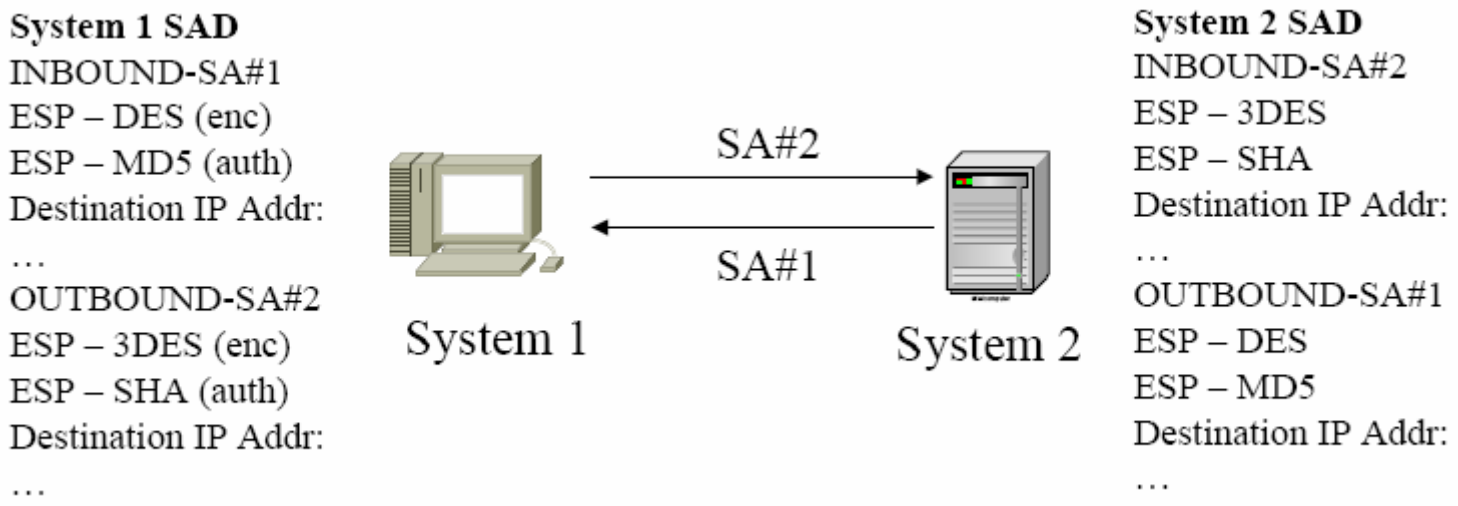
- Αν ο Α θέλει να επικοινωνήσει με τον Β, τότε πρέπει:
  - Ο Α να διαθέτει SAout και SAin
  - Ο Β να δημιουργήσει μία SAout και μία SAin
  - Το SAout του χρήστη Α και το SAin του Β πρέπει να χρησιμοποιούν τους ίδιους αλγορίθμους.

- Πολλαπλές SA μπορούν να υπάρχουν για την ίδια επικοινωνία ταυτόχρονα (π.χ. για διαφορετικές εφαρμογές)
- Μία SA περιγράφεται από την τριπλέτα

  <SPI, διεύθυνση παραλήπτη, κρυπτογραφικές παράμετροι>

  - SPI (Security Parameter Index): ένας 32-bit αριθμός που δημιουργείται από τον αποστολέα
  - Όταν λαμβάνεται ένα πακέτο, μπορεί να αυθεντικοποιείται και να αποκρυπτογραφείται μόνο εάν ο παραλήπτης μπορεί να το συνδέσει με το περιεχόμενο ενός SA
  - Στην ουσία, μία συσχέτιση ασφαλείας προσδιορίζεται πλήρως από το SPI και την IP διεύθυνση του παραλήπτη.

Παράδειγμα SA



- Στην ουσία, μέσω ενός SA έχουμε ένα ασφαλές κανάλι επικοινωνίας (μέσω ενός δημόσιου δικτύου (Internet)) με κάποιον συγκεκριμένο χρήστη.

Κεφαλίδες AH και ESP

- Η κεφαλίδα πιστοποίησης ταυτότητας (Authentication Header (AH)) παρέχει:

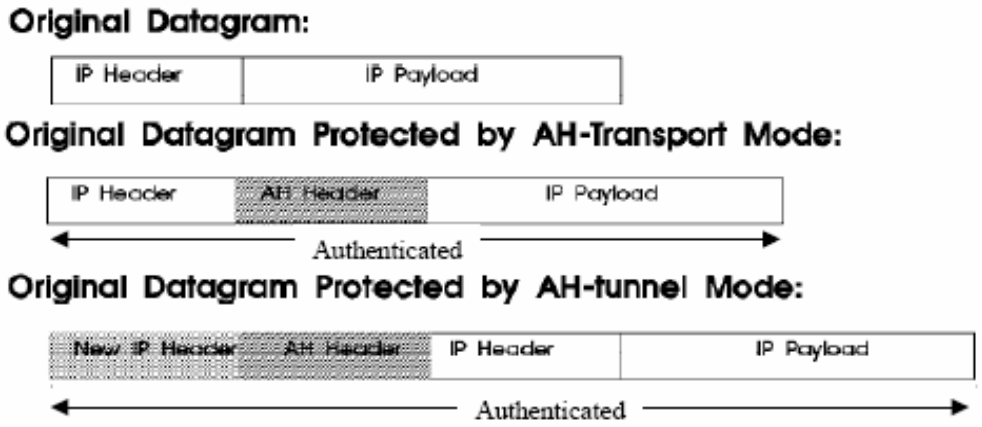
- Υπηρεσία ακεραιότητας δεδομένων. Ο παραλήπτης μπορεί να ανιχνεύσει τυχόν αλλοίωση των δεδομένων κατά τη μετάδοση.
- Πιστοποίηση ταυτότητας αποστολέα
- Προστασία από επανάληψη πακέτων

- Η Ασφαλής Ενθυλάκωση της πληροφορίας (Encapsulating Security Payload (ESP)) παρέχει:

- Εμπιστευτικότητα (κρυπτογράφηση)
- Υπηρεσία ακεραιότητας δεδομένων
- Πιστοποίηση ταυτότητας αποστολέα
- Προστασία από επανάληψη πακέτων

- Οι δύο κεφαλίδες μπορούν να χρησιμοποιηθούν είτε η κάθε μία μόνη της, είτε συνδυασμένες και οι δύο μαζί. Όταν χρησιμοποιούνται ταυτόχρονα, ο AH έπεται του ESP.
- Γιατί υπάρχουν δύο κεφαλίδες??
  - Κάποιες χώρες έχουν αυστηρούς νόμους ως προς την κρυπτογράφηση. Αν δεν υπάρχει η δυνατότητα για κρυπτογράφηση, η κεφαλίδα πιστοποίησης (AH) παρέχει κάποιους μηχανισμούς ασφάλειας και μπορεί να χρησιμοποιηθεί. Με απλά λόγια, η ύπαρξη και των δύο κεφαλίδων είναι αυτή που εξασφαλίζει τη δυνατότητα διάδοσης του IPSec σε όλο το Internet.

AH – Transport και tunnel mode

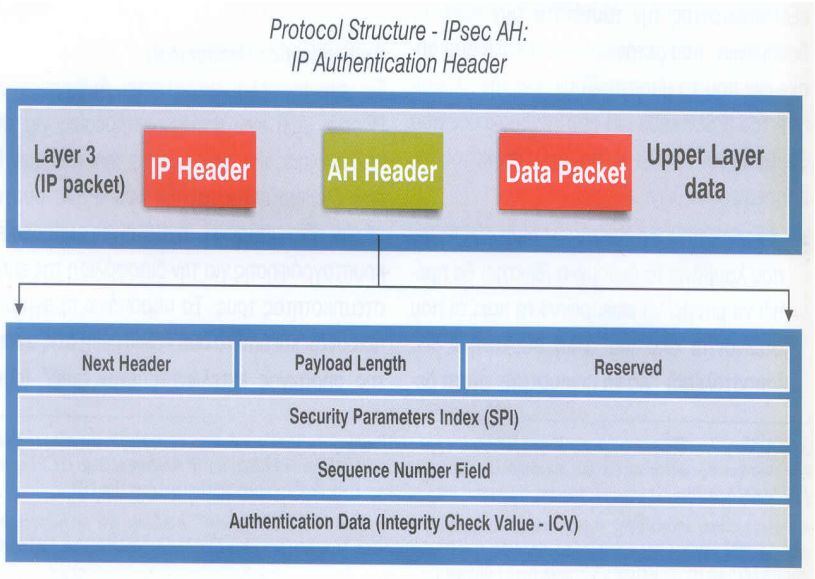


Transport mode: η αρχική header του IP datagram είναι η εξωτερική επικεφαλίδα του νέου πακέτου, ακολουθούμενη από την AH header και στη συνέχεια ακολουθεί το payload του αρχικού IP datagram. Το αρχικό IP datagram μαζί με την επικεφαλίδα AH αυθεντικοποιούνται και προστατεύονται.

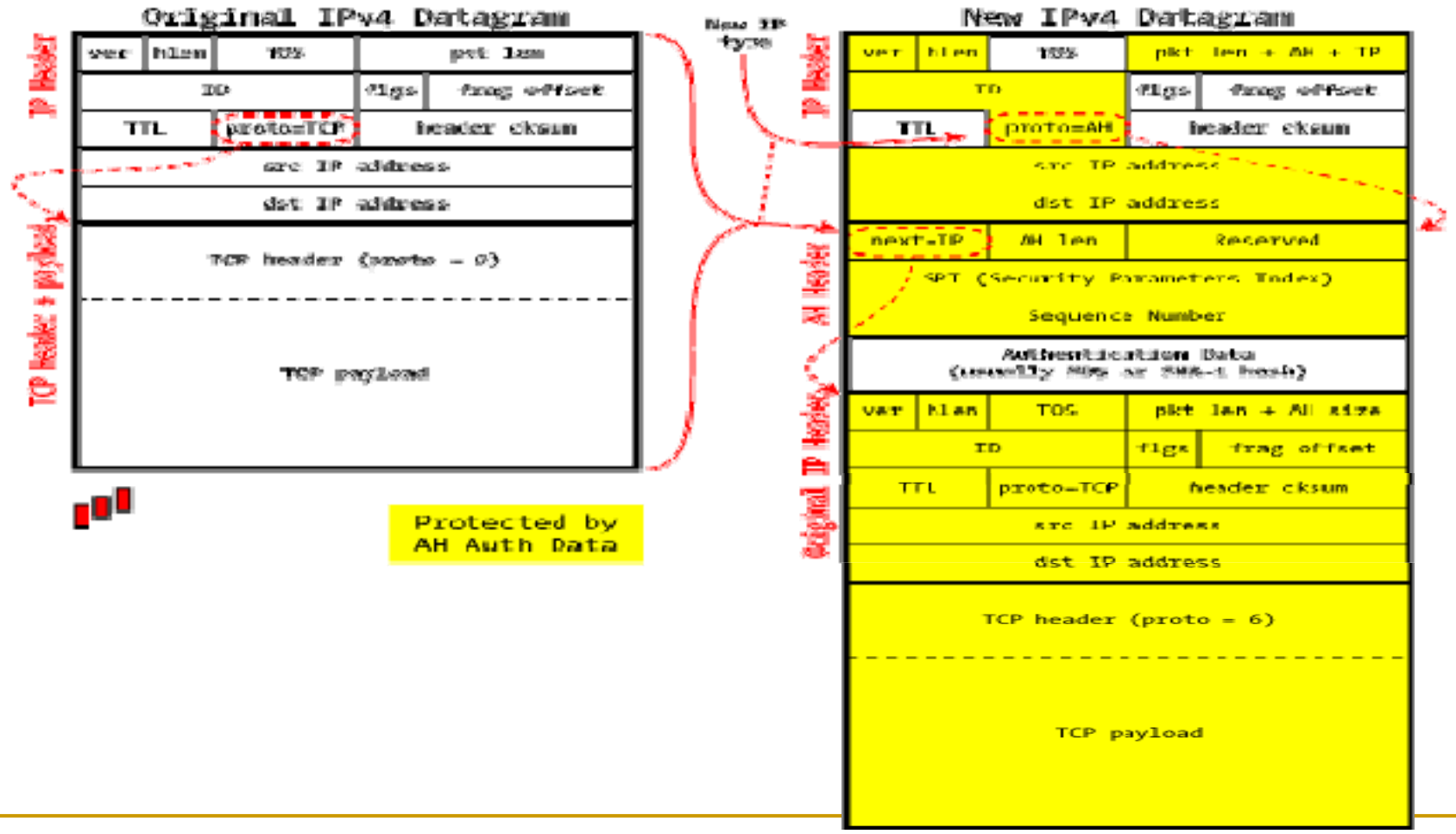
Στην **tunnel mode**, δημιουργείται μία νέα IP header, η οποία είναι η εξωτερική επικεφαλίδα του νέου IP datagram. Οι διευθύνσεις προέλευσης και αποστολής διαφοροποιούνται από αυτές του αρχικού datagram (οι νέες διευθύνσεις είναι αυτές της αρχής και τέλους του tunnel). Η νέα επικεφαλίδα ακολουθείται από την AH header, και τέλος το αρχικό IP datagram (αρχική IP header + payload). Ολόκληρο το νέο datagram (νέα IP Header, AH Header, αρχική IP Header, and αρχικό IP Payload) προστατεύεται από το πρωτόκολλο AH. Οποιαδήποτε αλλαγή σε κάθε πεδίο μπορεί να ανιχνευτεί.

Περιγραφή της κεφαλίδας πιστοποίησης ταυτότητας (AH)

- Περιέχει 5 πεδία:
  - Next Header field (π.χ. TCP, UDP κ.ο.κ.)
  - Payload length
  - Security Parameter Index – προσδιορίζει στον παραλήπτη ποια πρωτόκολλα ασφαλείας χρησιμοποιήθηκαν από τον αποστολέα
  - Sequence number
  - Authentication data – το τμήμα εκείνο που εξασφαλίζει την πιστοποίηση ταυτότητας



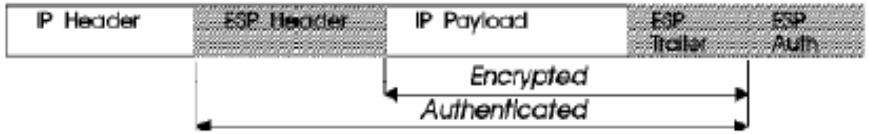
Το νέο IPv4 πακέτο (AH tunnel mode)



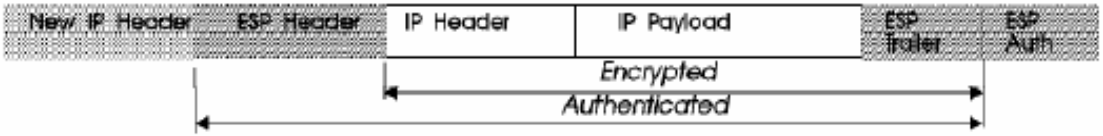
ESP – Transport και tunnel mode

Original Datagram:

Original Datagram Protected by ESP-Transport Mode:



Original Datagram Protected by ESP-tunnel:



Η Transport παρέχει εμπιστευτικότητα στο φορτίο του αρχικού datagram,

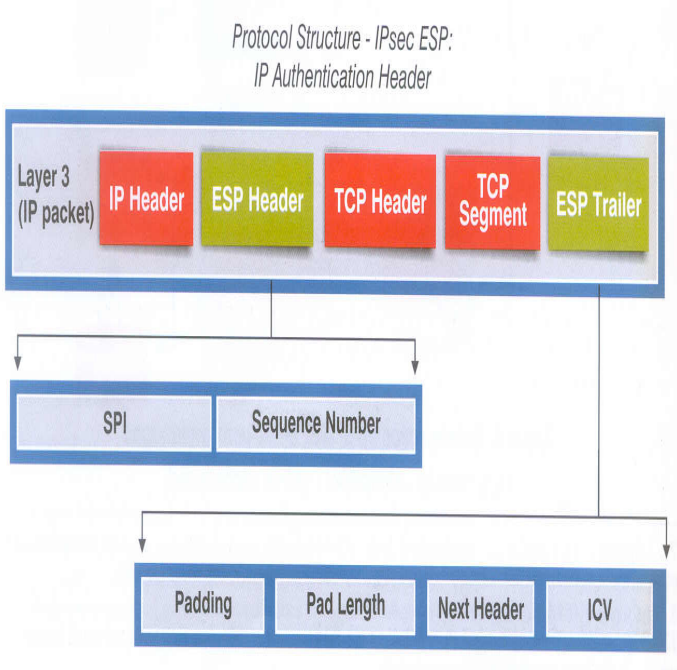
Η Tunnel παρέχει εμπιστευτικότητα και για την επικεφαλίδα και για το φορτίο.

Transport mode: η αρχική IP επικεφαλίδα του IP datagram διατηρείται. Μόνο το φορτίο του αρχικού IP datagram και το ESP Trailer είναι κρυπτογραφημένα. Η επικεφαλίδα δεν είναι ούτε κρυπτογραφημένη ούτε αυθεντικοποιημένη. Άρα οι πληροφορίες για τις διευθύνσεις αποστολέα - παραλήπτη της εξωτερικής επικεφαλίδας είναι ορατές για κάποιον man in the middle attacker

Tunnel mode: νέα IP header προστίθεται. Ολόκληρο το αρχικό IP datagram και το ESP Trailer είναι encrypted. Επειδή η αρχική IP header είναι κρυπτογραφημένη δεν μπορεί να διαβαστεί από κάποιον man in the middle attacker. Προκύπτει λοιπόν η βασική χρήση του ESP σε tunnel mode, που είναι η απόκρυψη των εσωτερικών διευθύνσεων δικτύου μεταξύ δύο firewalls (ή tunnel end points).

Περιγραφή του ESP

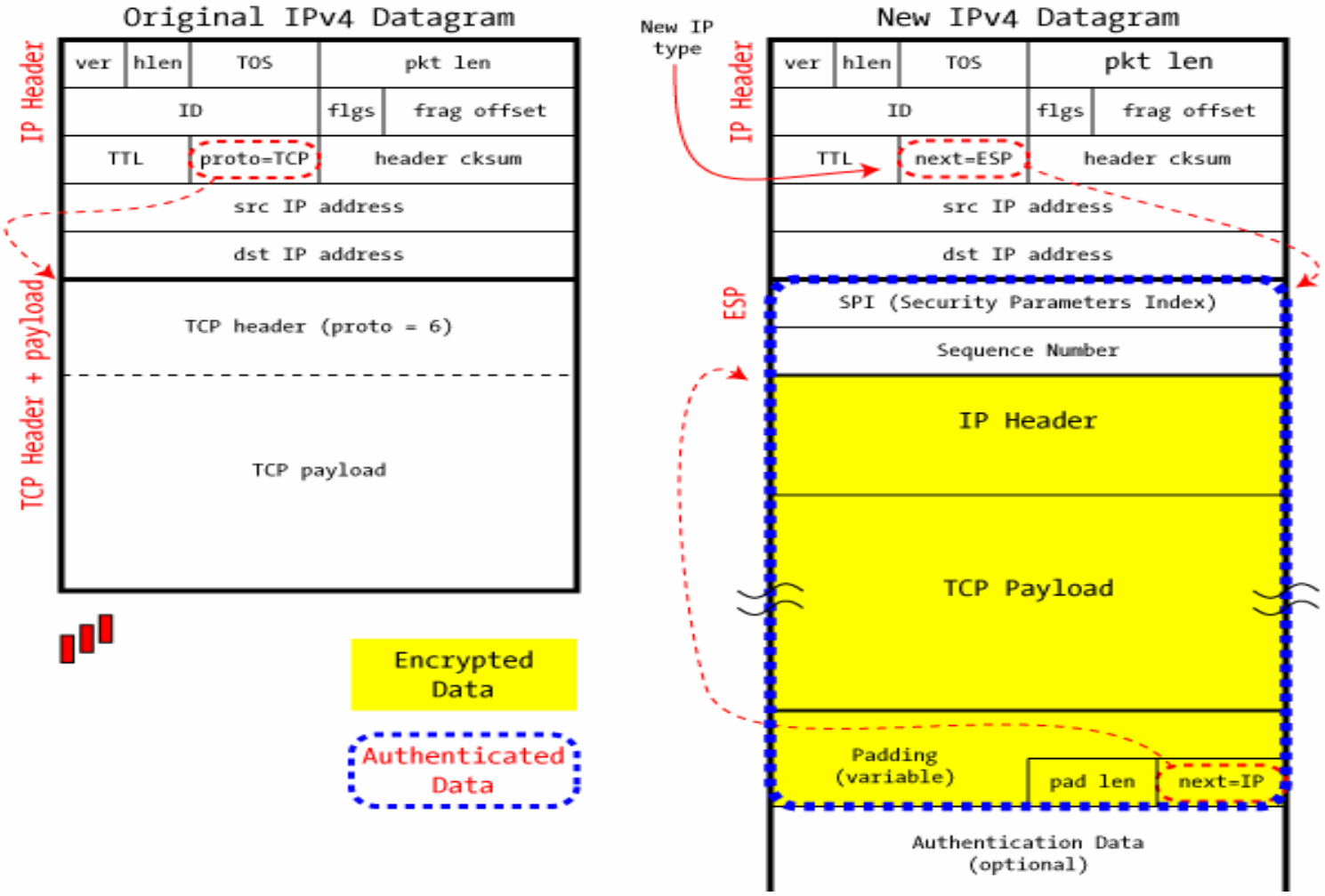
- Περιέχει τα πεδία:
  - Security Parameter Index (SPI)
  - Sequence number (μετρητής που αυξάνεται κάθε φορά που ένα πακέτο στέλνεται στον ίδιο παραλήπτη και υπό το ίδιο SPI) – έτσι αντιμετωπίζεται το πρόβλημα επανάληψης πακέτων από κάποιον «επιτιθέμενο».
  - Padding: το πολύ 255 bytes (λόγω του γεγονότος ότι κάποιοι αλγόριθμοι κρυπτογράφησης απαιτούν τα δεδομένα να είναι μήκους πολλαπλάσιου κάποιου συγκεκριμένου αριθμού bytes).
  - Pad length: προσδιορίζει το μήκος του padding
  - Next Header: προσδιορίζει ποια είναι η επόμενη κεφαλίδα στο πακέτο
  - ICV: πεδίο που χρησιμοποιείται για την πιστοποίηση της ταυτότητας (Προαιρετικό).



Σχόλια πάνω στο ESP

- Υποστηρίζει διάφορες μεθόδους κρυπτογράφησης
- Το ESP μπορεί προαιρετικά να έχει ένα πεδίο για πιστοποίηση ταυτότητας – το μήκος του ποικίλει, ανάλογα τον αλγόριθμο πιστοποίησης που χρησιμοποιείται. Ως προεπιλεγμένο αλγόριθμο έχει τον HMAC με συναρτήσεις κατακερματισμού SHA-1 και MD5. Η πιστοποίηση αυτή διαφέρει σε σχέση με αυτήν που παρέχει ο AH στο ότι δεν προστατεύει την IP κεφαλίδα που είναι μπροστά από το ESP (αν και προστατεύει την ενθυλακωμένη IP κεφαλίδα στον τρόπο λειτουργίας διόδου (tunneling mode)).
- Αν επιθυμούμε και εμπιστευτικότητα και πιστοποίηση ταυτότητας, είναι καλύτερα να χρησιμοποιούμε μόνο ESP παρά ESP και AH ταυτόχρονα (είναι πιο αποδοτικό, μια που απαιτείται μικρότερη επεξεργασία πακέτων). Σε tunnel mode δεν υπάρχουν ποτέ ταυτόχρονα και οι δύο.
- Συνδυασμός AH-ESP με τους διάφορους τρόπους λειτουργίας: πρώτα κρυπτογράφηση και πιστοποίηση σε tunnel mode και κατόπιν εκ νέου εφαρμογή AH ή ESP σε transport mode στο νέο πακέτο.

Το «νέο» IPv4 πακέτο (ESP tunnel mode)



Διαχείριση κλειδιών στο IPSec

- Μέχρι το 1997, η ανταλλαγή κλειδιών που θα χρησιμοποιούνταν στο IPSec γινόταν «με το χέρι» (manual keying) (για παράδειγμα μέσω courier ή δισκετών).
- Η ανάγκη για μια αυτοματοποιημένη διαχείριση κλειδιών οδήγησε στο IKE (Internet Key Exchange), το οποίο προήλθε σαν επέκταση του ISAKMP/Oakley.
- Κάποιες εταιρίες (Sun Microsystems, Novell) ανέπτυξαν ένα δικό τους πρωτόκολλο, το SKIP (Simple Key management for IP), το οποίο όμως δεν υιοθετήθηκε σαν standard από το IPSec.

Στόχοι του IKE

- Να δίνει στους συνομιλούντες τη δυνατότητα να συμφωνούν με ποια πρωτόκολλα θα μιλούν, με ποιους αλγορίθμους και με ποια κλειδιά
- Η εξασφάλιση του να γνωρίζει ο καθένας από την αρχή της επικοινωνίας ότι μιλάει πράγματι με το σωστό άτομο (πιστοποίηση ταυτότητας)
- Εξασφάλιση του ότι η ανταλλαγή κλειδιών γίνεται με ασφάλεια.

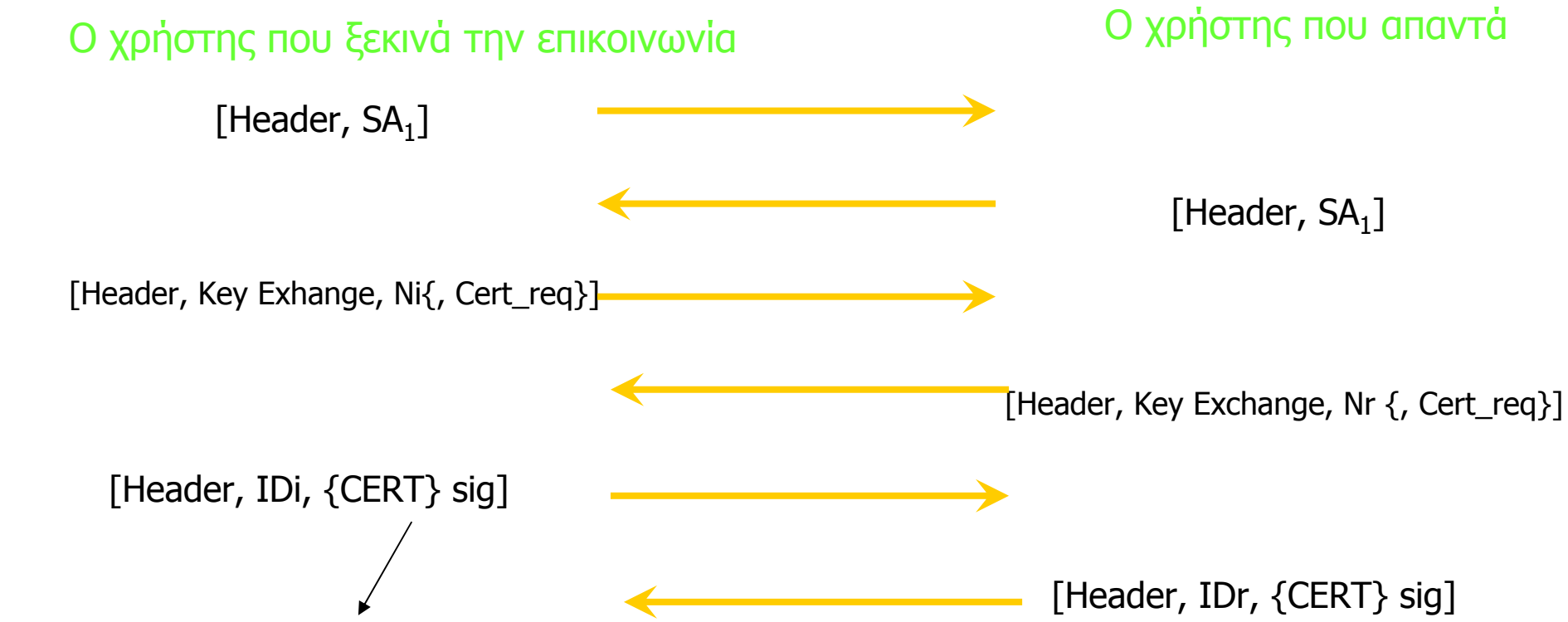
Φάσεις του IKE

- Στην πρώτη φάση, οι δύο συνομιλούντες εγκαθιδρύουν μία ασφαλή σύνδεση μεταξύ τους. Στη δεύτερη φάση, οι συνομιλούντες ανταλλάζουν γενικού σκοπού SAs. (ΠΡΟΣΟΧΗ: ο όρος «συνομιλών» είναι γενικός – μπορεί να είναι είτε ένας υπολογιστής είτε μια πύλη ασφαλείας).
- Η πρώτη φάση έχει δύο πιθανούς τρόπους (modes) λειτουργίας: τον κύριο τρόπο (Main mode) και τον επιθετικό τρόπο (aggressive mode). Η δεύτερη φάση έχει τον γρήγορο τρόπο (quick mode).

Περιγραφή του κύριου τρόπου λειτουργίας (main mode)

- Χρησιμοποιείται, σε συνδυασμό με τον γρήγορο τρόπο της φάσης 2, ως εξής:
  - Με τον κύριο τρόπο εγκαθιδρύεται μία προσωρινή SA (Security Association)
  - Με τον γρήγορο τρόπο, μέσα σε αυτήν τη SA δημιουργείται μία νέα SA
  - Η επικοινωνία γίνεται με τη νέα SA μέχρι τέλους
- Κατά τη διάρκεια εγκαθίδρυσης της πρώτης (προσωρινής) SA, λαμβάνουν χώρα 3 ανταλλαγές μηνυμάτων (όπου κάθε ανταλλαγή αντιστοιχεί σε μία αμφίδρομη επικοινωνία πομπού-δέκτη και δέκτη-πομπού), οι οποίες είναι οι εξής :
  1. Καθορίζονται οι αλγόριθμοι κρυπτογράφησης και πιστοποίησης ταυτότητας. Ένα SA δημιουργείται ξεχωριστά για κάθε κατεύθυνση.
  2. Εκτελείται ο αλγόριθμος Diffie-Hellman παραγωγής και ανταλλαγής κοινού μυστικού κλειδιού. Επίσης ανταλλάζονται τυχαίοι αριθμοί (Nonce) με σκοπό ο καθένας να τους «υπογράψει» (με κάποια συνάρτηση κατακερματισμού), ώστε να πιστοποιήσει την ταυτότητά του
  3. Γίνεται πιστοποίηση ταυτότητας

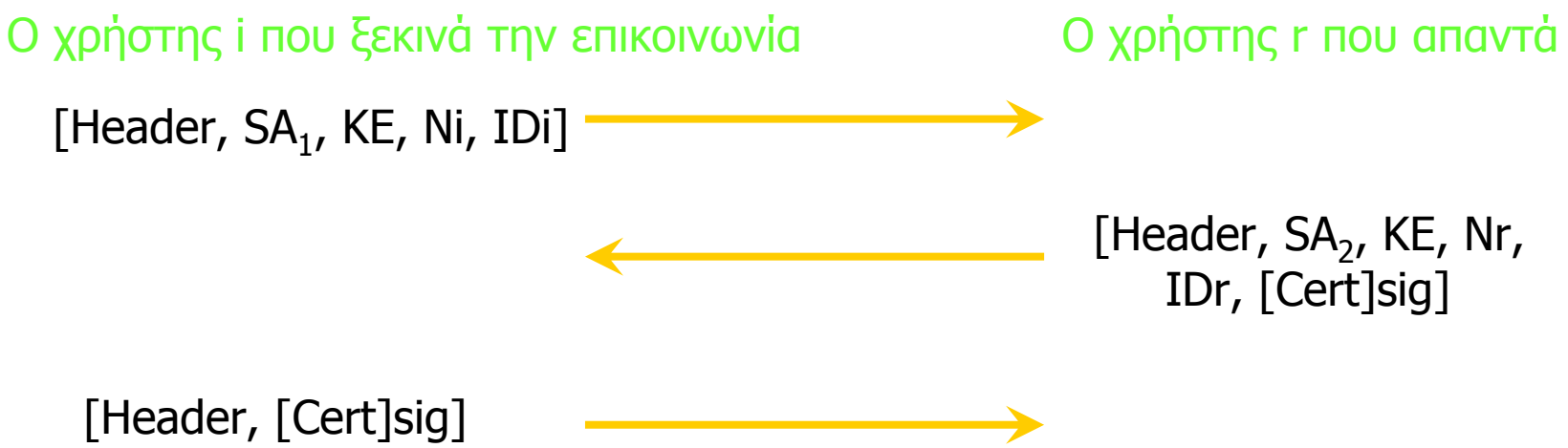
Απλοποιημένη σχηματική αναπαράσταση του κύριου τρόπου (Main Mode)



Περιγραφή του επιθετικού τρόπου λειτουργίας (aggressive mode)

- Λαμβάνει χώρα σε δύο ανταλλαγές μηνυμάτων και όχι σε τρεις.
- Είναι πιο γρήγορος από τον κύριο τρόπο. Ωστόσο, το ID στέλνεται μη κρυπτογραφημένο, οπότε κάποιος εχθρός μπορεί να δει ποιος χρήστης ξεκινά μία SA (επίθεση sniffing).

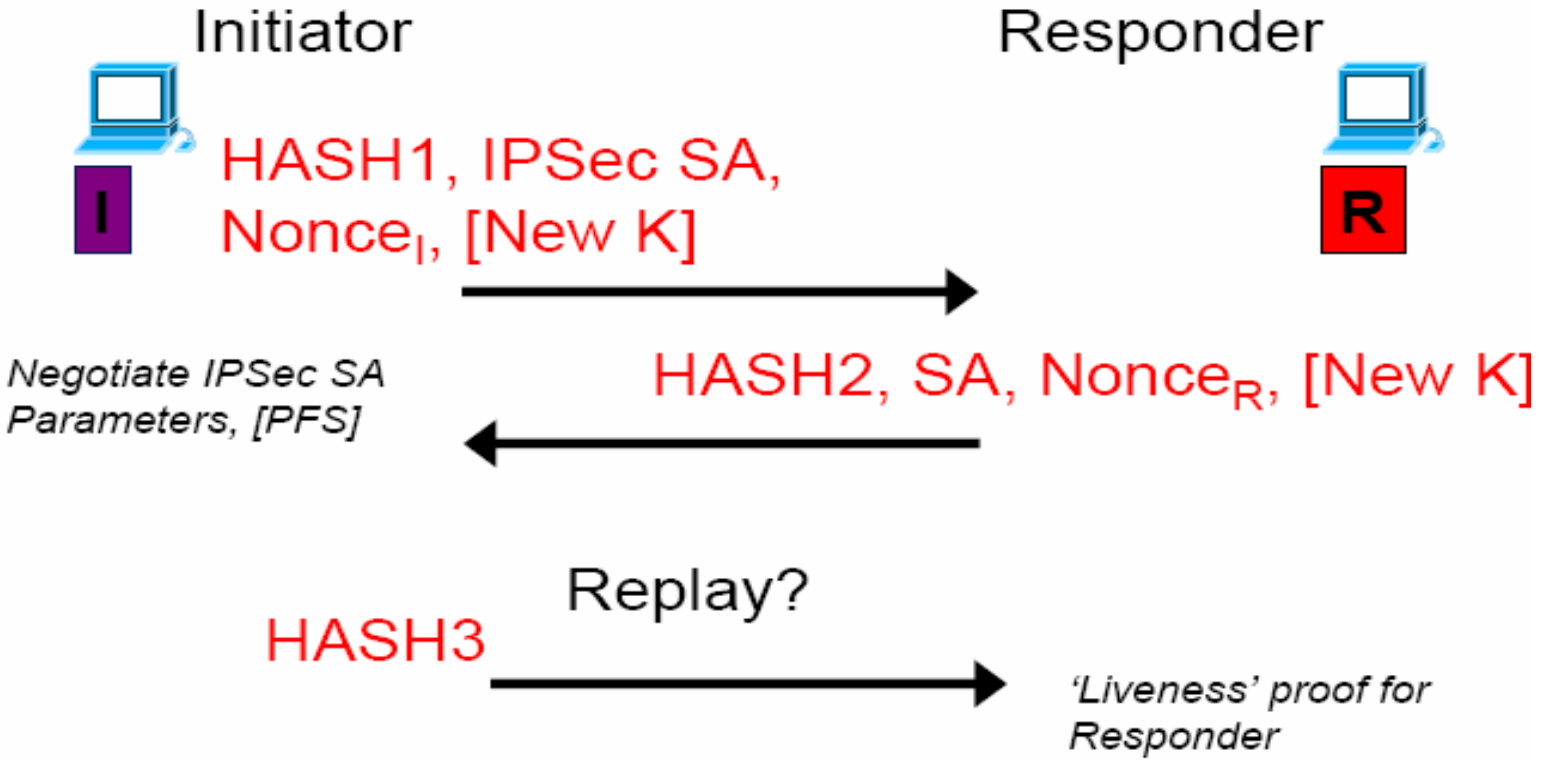
Απλοποιημένη σχηματική αναπαράσταση του επιθετικού τρόπου (Aggressive Mode)



Δεύτερη φάση IKE – Γρήγορος τρόπος (Quick mode)

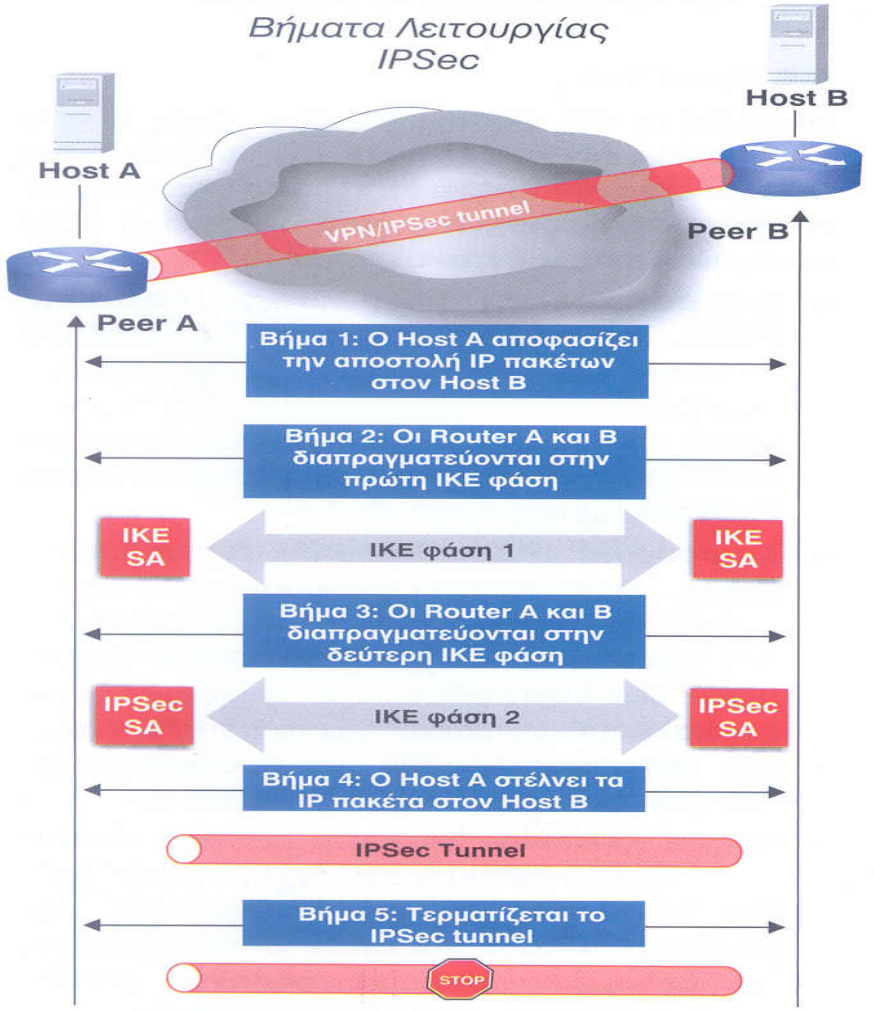
- Χρησιμοποιείται για την εγκαθίδρυση της SA πάνω στην οποία θα στηριχτεί το IPSec για την επικοινωνία.
- Όλα τα πακέτα είναι κρυπτογραφημένα και στην αρχή τους έχουν μία τιμή που προέκυψε από κατακερματισμό (με τη συνάρτηση κατακερματισμού που έχει προσυμφωνηθεί στη φάση 1). Με την τιμή αυτή γίνεται η αυθεντικοποίηση του πακέτου.
- Μπορούν, προαιρετικά, να ανανεωθούν τα κλειδιά επικοινωνίας.

Σχηματική αναπαράσταση της δεύτερης φάσης του IKE (quick mode)



Λειτουργία του IPSec – πώς συνδυάζονται όλα τα παραπάνω??

- **Η υλοποίηση μίας σύνδεσης IPSec VPN πραγματοποιείται μέσω δύο φάσεων:**
- ***♦ Δημιουργία και λειτουργία του IKE/ISAKMP SA (πιστοποίηση & δημιουργία κλειδιών)***
- ***♦ Δημιουργία και λειτουργία του AH/ESP SA (κοινή πολιτική IPSec & χρήση κλειδιών)***



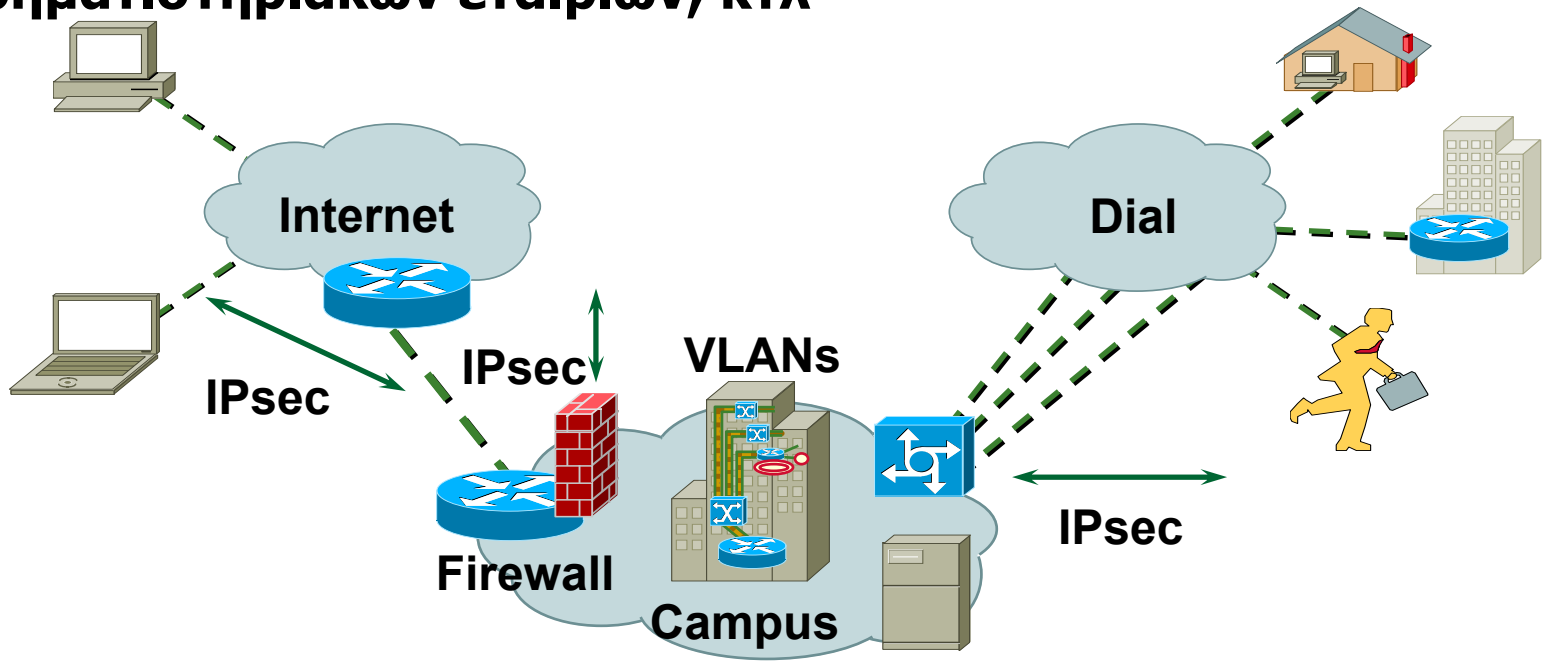
Πού πρέπει να εκτελείται το IPSec software?

- Στις πύλες ασφαλείας
- Στους κινητούς χρήστες
- Στους κόμβους (hosts) των δικτύων

Για LAN-to-LAN VPNs, αρκεί να υπάρχει το software στις πύλες ασφαλείας. Από την άλλη μεριά, όταν κάποιος χρήστης θέλει να συνδεθεί από τον υπολογιστή του σπιτιού του σε ένα VPN, πρέπει ο υπολογιστής του να διαθέτει το κατάλληλο IPSec software.

Εφαρμογές IPSec VPNs

- **Ασφαλής επικοινωνία μεταξύ δύο hosts ή μεταξύ δύο LANs**
- **Απομακρυσμένη πρόσβαση μέσω dial-up σε ιδιωτικά δίκτυα**
- **Μέγιστη δυνατή ασφάλεια σε περιπτώσεις χρηματοπιστωτικών ιδρυμάτων,**
- **χρηματιστηριακών εταιριών, κτλ**



Προβλήματα του IPSec

- Τα μεγέθη των IP πακέτων μεγαλώνουν, συνεπώς μεγαλώνει ο χρόνος επεξεργασίας τους και μειώνεται η συνολική απόδοση. Μία λύση που εξετάζεται είναι η συμπίεση των πακέτων πριν την κρυπτογράφηση.
- Είναι σχεδιασμένο μόνο για IP – σε περιπτώσεις που υπάρχουν ταυτόχρονα πολλά πρωτόκολλα (π.χ. της AppleTalk ή της NETBEUI) δεν μπορεί να χρησιμοποιηθεί άμεσα.
- Υπάρχουν διά νόμου απαγορεύσεις χρήσης συγκεκριμένων κρυπτογραφικών πρωτοκόλλων σε κάποιες χώρες – συνεπώς, δεν υπάρχουν παγκοσμίως κοινά αποδεχτά πρωτόκολλα για να υπάρχουν ως παράμετροι στις SA.