ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΔΙΚΤΥΩΝ

ΔΙΑΛΕΞΗ 8

ΔΙΔΑΣΚΩΝ: ΑΝΑΡΓΥΡΟΣ ΣΙΔΕΡΗΣ

<sideris@epp.teiher.gr>

<https://eclass2.teicrete.gr/courses/TP182/>

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΠΟΛΥΜΕΣΩΝ

ΤΕΙ ΚΡΗΤΗΣ

T.E.I. of Crete

ΑΣΦΑΛΕΙΑ ΣΤΑ ΔΙΚΤΥΑ
(Network Security)

Γενικά (1)

- Τι είναι ένα ασφαλές δίκτυο;
  - Ένα δίκτυο το οποίο δεν επιτρέπει την χρήση των πόρων του σε τρίτους και επιπλέον προσφέρει κρυπτογράφηση των προς μεταφορά δεδομένων.
- Πως το επιτυγχάνουμε;
  - Χρήση τεχνολογιών ασφαλείας όπως:
    - 802.11i, RADIUS+802.11i
    - IPsec
    - Firewalls
    - antivirus?

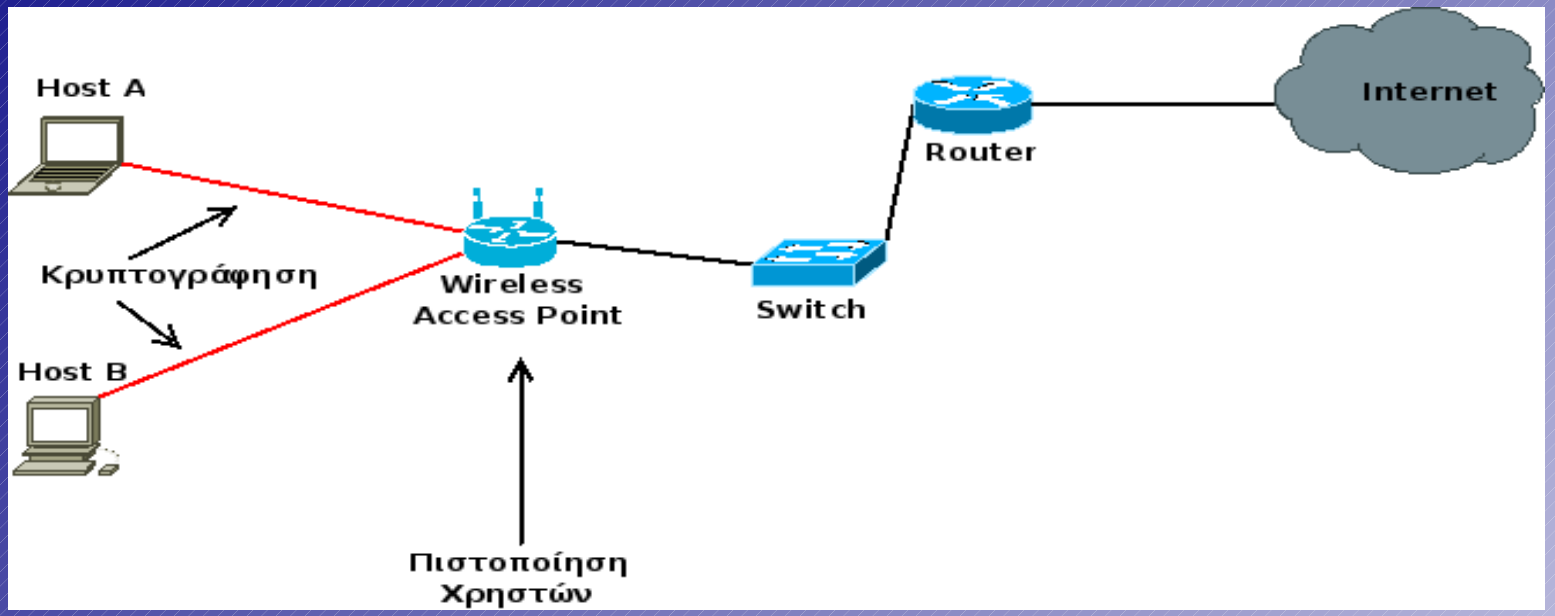
802.11i

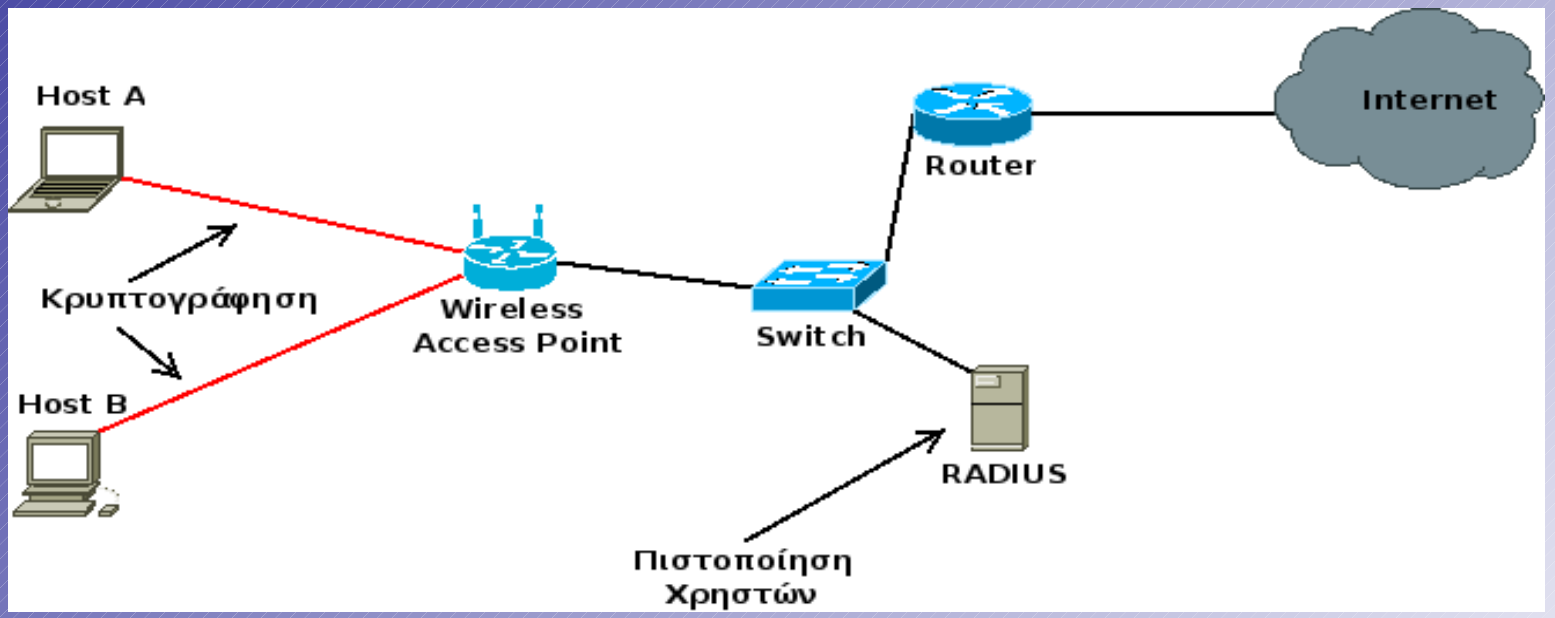
- Αναπτύχθηκε για να λύσει τα προβλήματα του WEP (Wired Equivalent Privacy)
- Αποτελείται από τα:
  - TKIP: πρωτόκολλο για ακεραιότητα και εμπιστευτικότητα.
  - CCMP: πρωτόκολλο για ακεραιότητα και εμπιστευτικότητα (AES encryption).
  - 802.1x: Πρωτόκολλο για πιστοποίηση.
- TSN:802.1x+TKIP (WPA)
- RSN: 802.1x+CCMP (WPA2)

Χρήσεις του 802.11i (1)

- WPA(1/2)-PSK
  - Ο πιο συνηθισμένος και απλός τρόπος για να ασφαλίζουμε τα ασύρματα δίκτυα του σπιτιού μας.
  - Το wirelles point και όλοι οι χρήστες μοιράζονται την ίδια μυστική φράση.
  - Φροντίστε η φράση να περιέχει και ειδικούς χαρακτήρες και να είναι πάνω από 8 χαρακτήρες.
- WPA(1/2)+RADIUS:
  - Χρησιμοποιείται σε εταιρικά ασύρματα περιβάλλοντα για τη:
    - πιστοποίηση χρηστών
    - κρυπτογράφηση των δεδομένων τους.
  - Ο Radius είναι ένας εξυπηρετητής ο οποίος κρατάει τα password/certificates των χρηστών.
  - Το wirelles point και ο RADIUS μοιράζονται την ίδια μυστική φράση.

Χρήσεις του 802.11i (2)



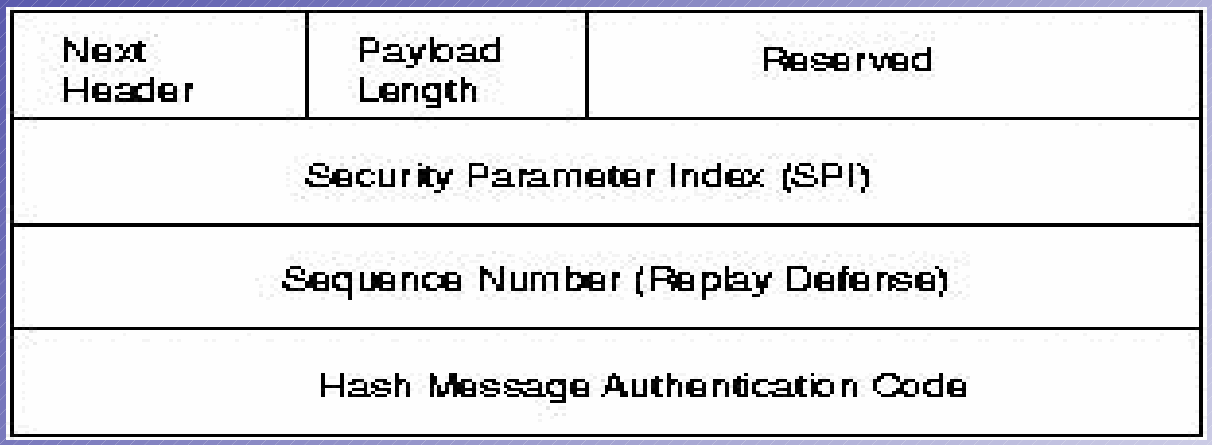


IPSec

- Είναι μια τεχνολογία που προσφέρει ασφάλεια από το στρώμα δικτύου και άνω.
- Χρησιμοποίεται σε IPv6/4 δίκτυα.
- Αξιοποιεί δύο πρωτόκολλα:
  - AH (Authentication Header)
  - ESP (Encapsulated Security Payload)
- Δύο τρόποι χρήσης:
  - Transport mode
  - Tunnel mode

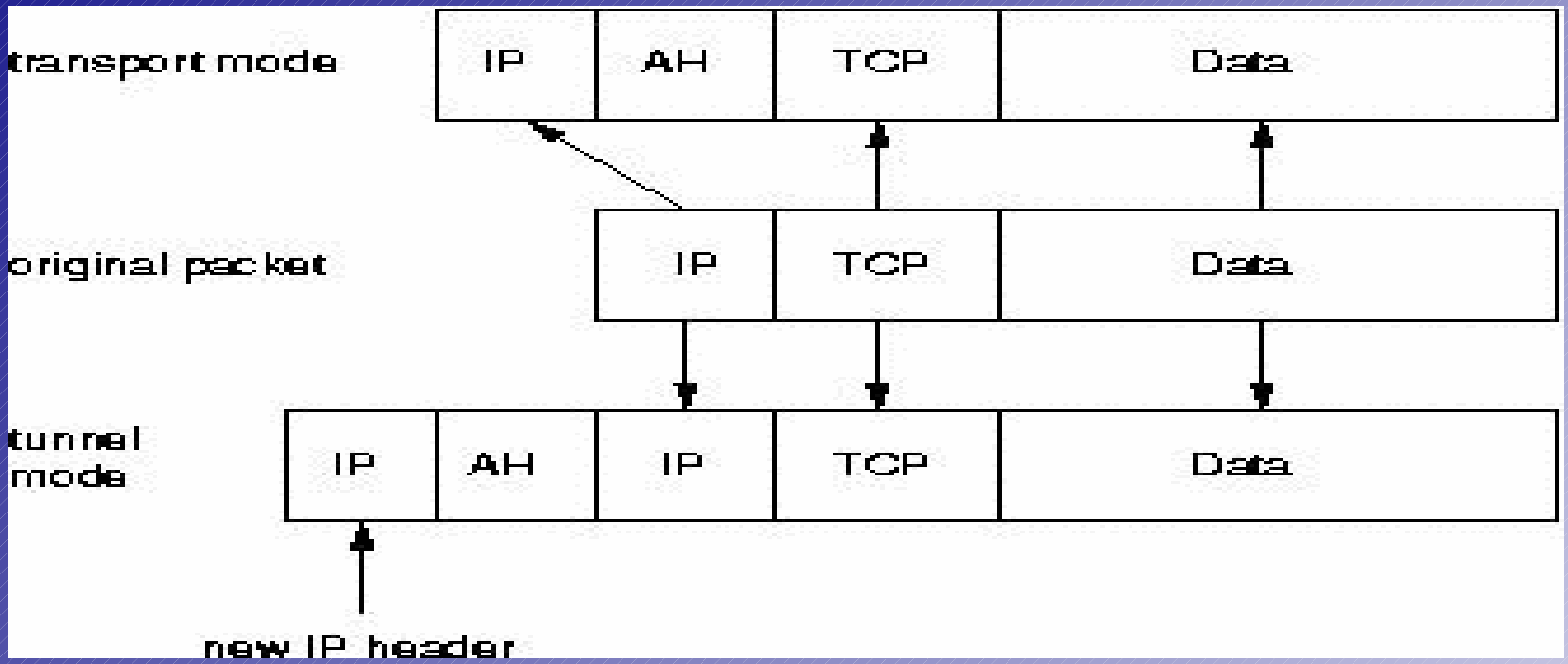
AH (1)

- Χρησιμοποιείται όταν θέλουμε μόνο ακεραιότητα των δεδομένων.
- Η AH επικεφαλίδα:
  - Περιέχει μια hash τιμή (HMAC) η οποία δημιουργείται βασισμένη στο κλειδί του χρήστη, το payload, και τις ip διευθύνσεις.
- Η AH επικεφαλίδα τοποθετείται μέσα στη αρχική IP επικεφαλίδα



Πηγή: http://www.ipsec-howto.org/x202.html

AH (2)

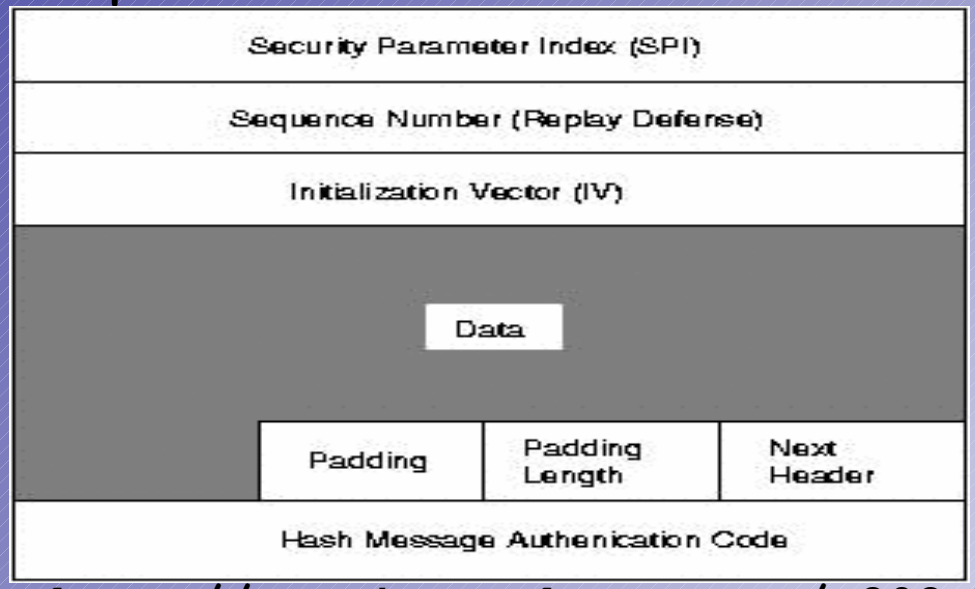


Πηγή: http://www.ipsec-howto.org/x202.html

- **Ερώτηση:**
  - **Το NAT προκαλεί προβλήματα στη χρήση του IPSec με AH;**

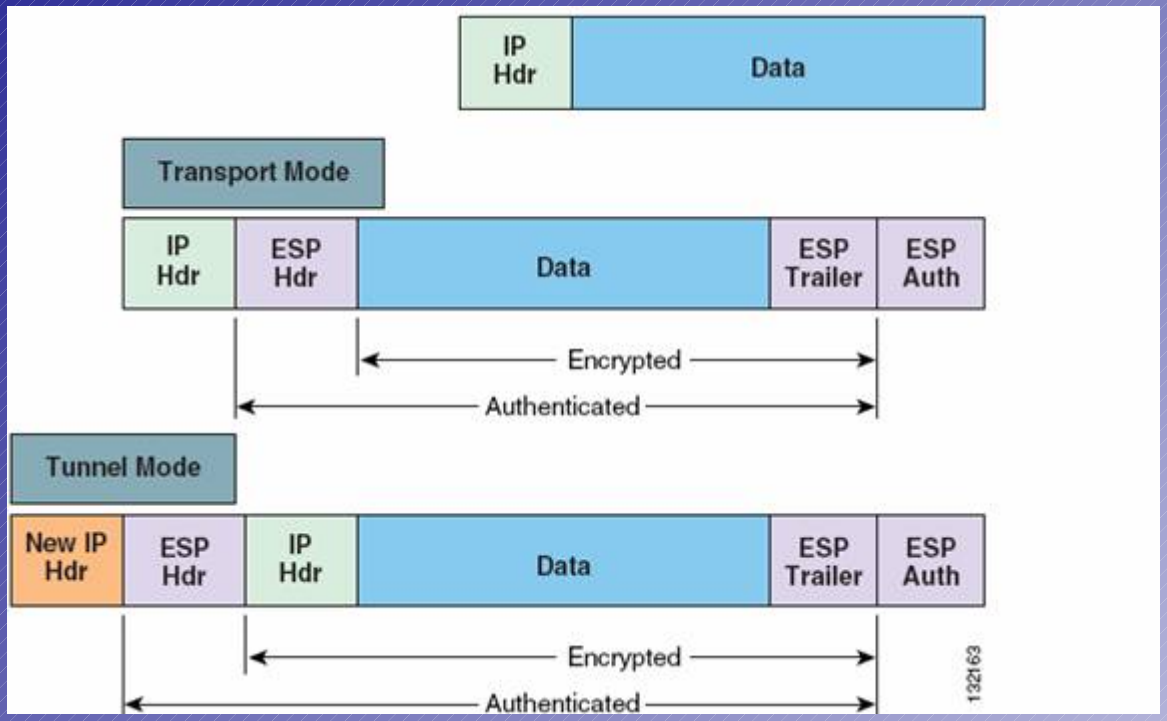
ESP (1)

- Χρησιμοποιείται όταν θέλουμε ακεραιότητα και εμπιστευτικότητα των δεδομένων.
- Η ESP επικεφαλίδα:
  - Περιέχει μια hash τιμή (HMAC) η οποία δημιουργείται βασισμένη στο κλειδί του χρήστη, και το payload.
  - Το payload κρυπτογραφείται.
  - Η ESP επικεφαλίδα τοποθετείται μέσα στη αρχική IP επικεφαλίδα



Πηγή: http://www.ipsec-howto.org/x202.html

ESP (2)



Πηγή: http://www.gtsllcus.com/images/clip_image004.jpg

- Ερωτήσεις:
  - Το NAT προκαλεί προβλήματα στη χρήση του IPSec με ESP;
  - Πότε χρησιμοποιώ ESP και πότε AH;

IPSec tunnel/transport modes

- Στο tunnel:
  - όλο το IP πακέτο ενθυλακώνεται σε ένα νέο IP πακέτο.
  - Στο νέο πακέτο εφαρμόζεται το IPSec.
  - Χρησιμοποιείται για τη ασφαλή αποστολή κίνησης μεταξύ δρομολογητών.
- Στο transport:
  - Στο IP πακέτο εφαρμόζεται το IPSec.
  - Χρησιμοποιείται για τη ασφαλή αποστολή κίνησης μεταξύ τελικών χρηστών (host2host).

Διαχείριση κλειδιών στο IPSec

- Τα κλειδιά στο IPSec χρησιμοποιούνται για τη ακεραιότητα και εμπιστευτικότητα.
- Μπορούμε να τα εισάγουμε:
  - Με στατικό τρόπο.
  - Με αυτόματο τρόπο.
- Στον αυτόματο τρόπο χρησιμοποιείται ευρέως η τεχνολογία Internet Key exchange.
- Δημιουργεί αυτόματα τα τελικά κλειδιά χρησιμοποιώντας
  - preshared-keys
  - πιστοποιητικά
  - Πιστοποίηση kerberos.

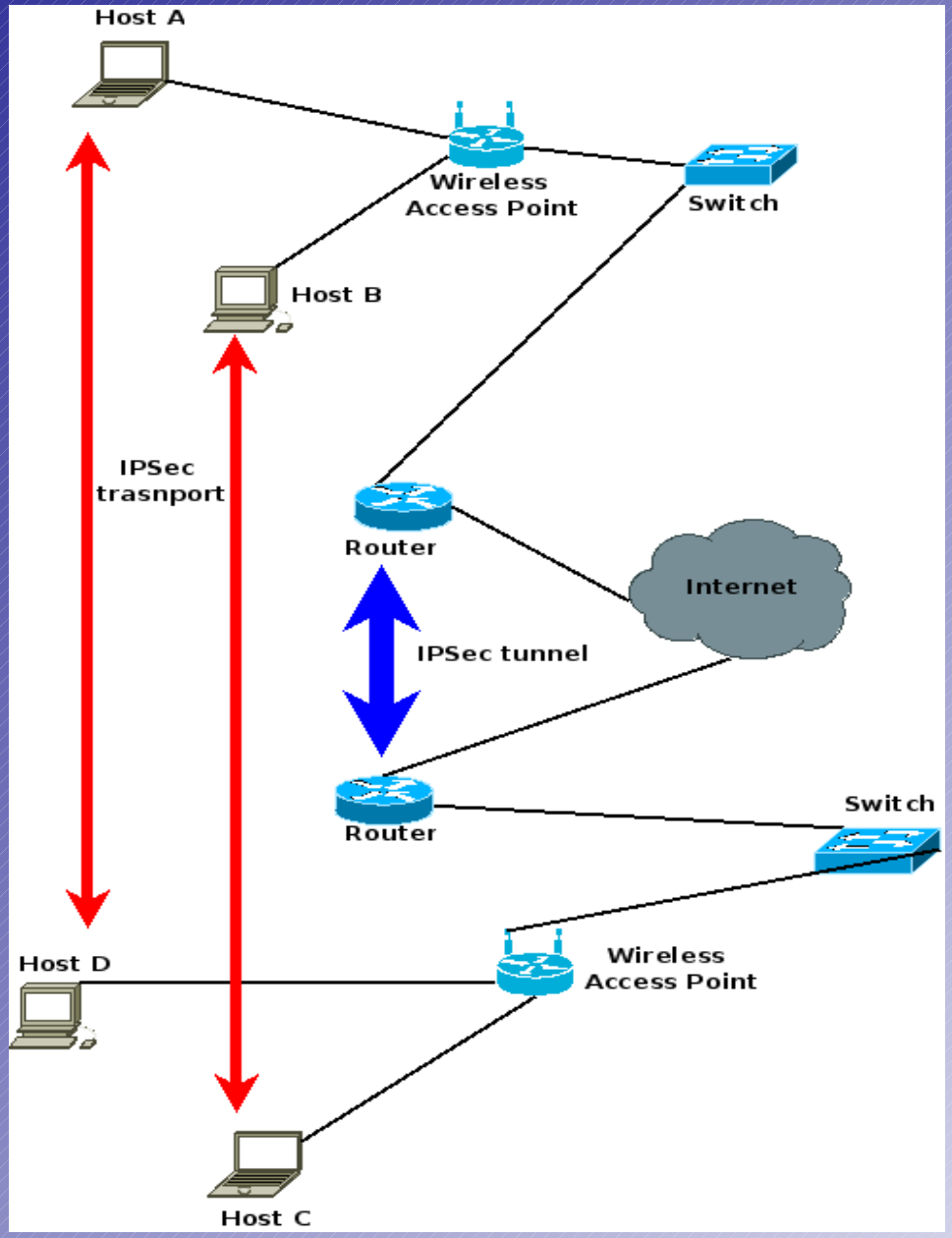
Υλοποίηση του IPSec (1)

- Δημιουργία:
  - Συσχετίσεων ασφάλειας (security associations-sa).
  - Πολιτικών ασφάλειας (security policies-sp).
- Τα sp χρησιμοποιούνται για την επιλογή της IP κίνησης που θέλουμε να εφαρμόσουμε το IPSec.
  - Περιέχει:
    - IP διευθύνσεις πηγής και προορισμού. Στο transport mode είναι οι ίδιες με του sa.
    - Το πρωτόκολλο μεταφοράς και τη θύρα προορισμού-πηγής.
    - Το sa που θα χρησιμοποιηθεί.

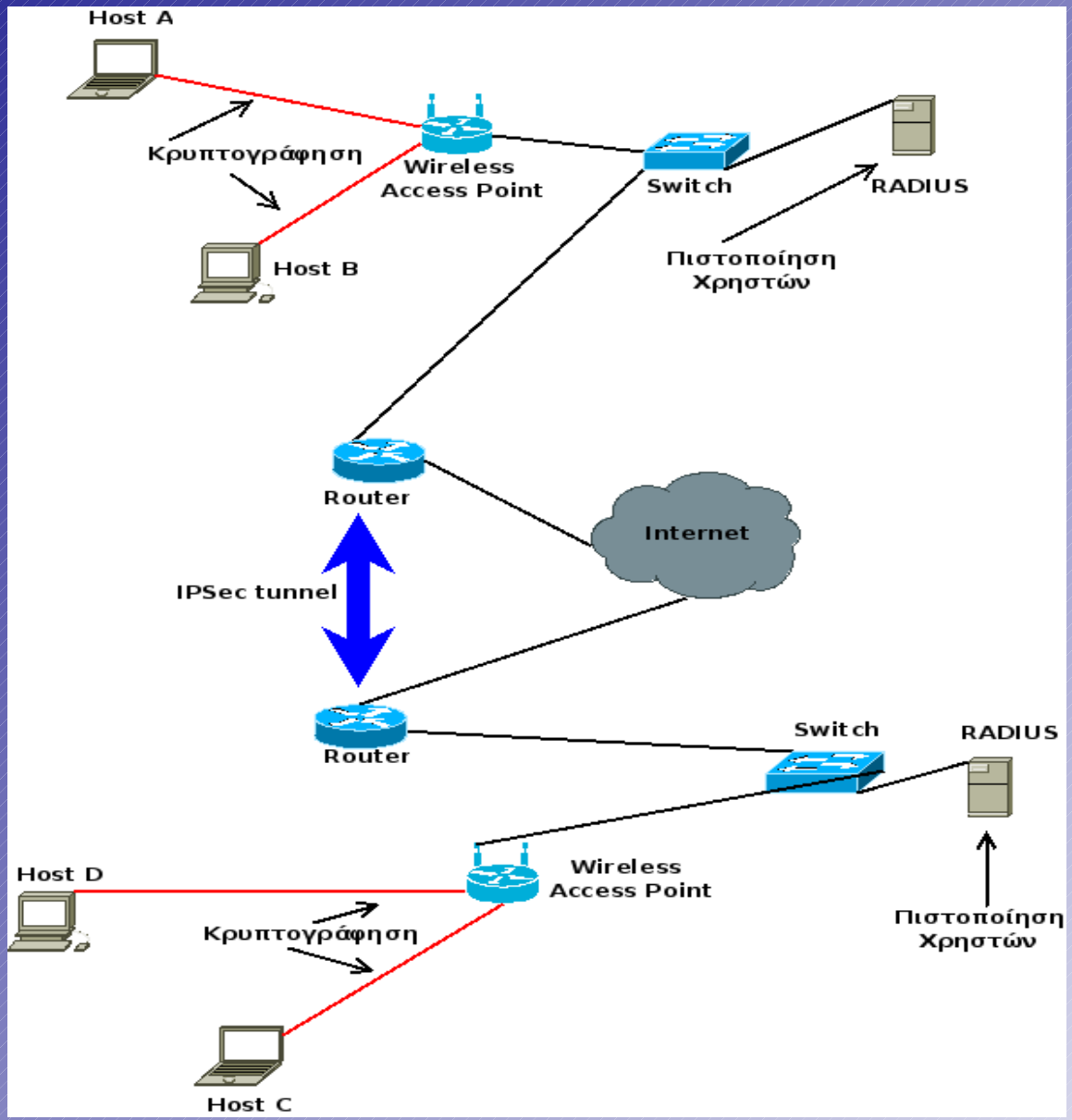
Υλοποίηση του IPSec (2)

- Τα sa χρησιμοποιούνται για προσδιορισμό του τρόπου προστασίας της κίνησης που έχει επιλεχθεί με τα sp.
  - Περιέχει:
    - IP διευθύνσεις πηγής και προορισμού. Στο transport mode είναι οι ίδιες με του sp.
    - Εάν το πρωτόκολλο είναι AH ή ESP.
    - Τον αλγόριθμο κρυπτογράφησης και το κλειδί κρυπτογράφησης.
    - Τον αριθμό ταυτοποίησης του sa (SPI index).
    - Το IPSec mode (tunnel ή transport)
    - Τη διάρκεια ζωής του sa.

Υλοποίηση του IPSec (3)



IPSec + RADIUS+802.1x



Firewalls

Firewall (1)

- Εφαρμογές οι οποίες επιτρέπουν τον έλεγχο και διαχείριση της εισερχόμενης, εξερχόμενης και προωθούμενης κίνησης από τους δικτυακούς κόμβους.
- Η λειτουργία τους έγκειται στην αποδοχή ή απόρριψη της δικτυακής κίνησης.
- Η αποδοχή η απόρριψη γίνεται βάση των πολιτικών ασφαλείας.
- Για τη ταυτοποίηση μιας κίνησης χρησιμοποιούνται κατάλληλα φίλτρα.

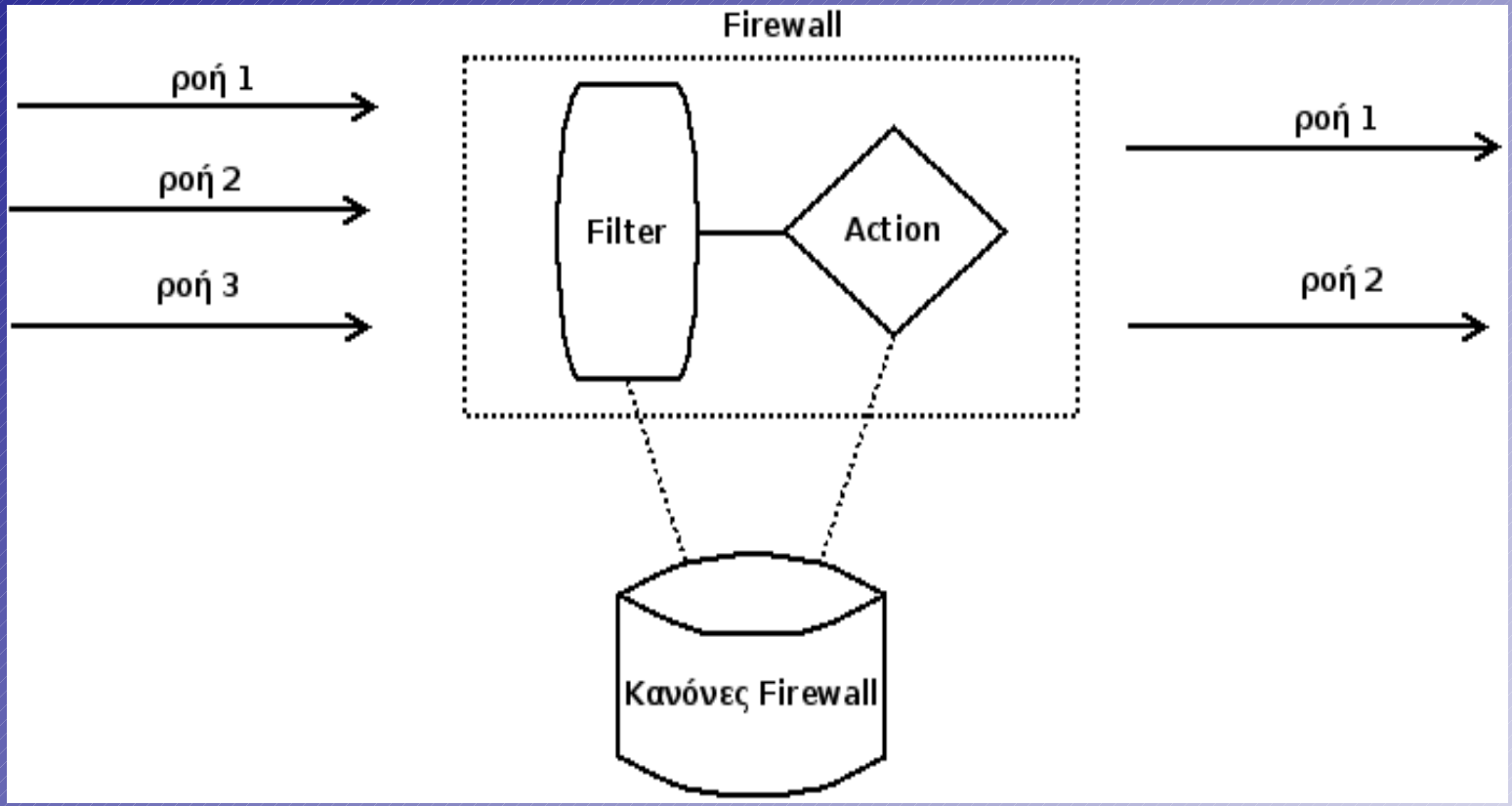
Firewall (2)

- Αναλόγως το επίπεδο εφαρμογής τους χωρίζονται σε:
  - L2 firewalls (Data Link Layer)
  - L3/4 firewalls (Network/Transport Layer)
  - L7 firewalls (Application Layer)
- Αναλόγως με το αν μπορούν να διακρίνουν την κατάσταση μια κίνησης χωρίζονται σε:
  - Statefull
  - Unstatefull

Firewall (3)

- Στο L2 επίπεδο (Ethernet) η διάκριση της κίνησης γίνεται με τις mac διευθύνσεις και/ή τις θύρες εισόδου/εξόδου των switch.
- Στο L3/4 επίπεδο (IP/TCP_UDP) η διάκριση της κίνησης γίνεται με τις IP διευθύνσεις, τα πρωτόκολλα δικτύου και μεταφοράς και/ή τις θύρες αποστολής προορισμού.
- Στο L7 επίπεδο η διάκριση της κίνησης γίνεται με βάση τις εφαρμογές που δημιουργούν την κίνηση.
- Στα statefull firewall λαμβάνεται υπόψιν και η κατάσταση μιας κίνησης για την απόρριψη η αποδοχή της
  - π.χ. Μπορούν να καταλάβουν εάν ένα πακέτο ανήκει σε μία ήδη ελεγμένη κίνηση γλιτώνοντας έτσι τους πόρους για νέο έλεγχο.

Firewall (4)



Υλοποίηση κανόνων firewall

- Δύο προσεγγίσεις:
  - Προκαθορισμένη πολιτική τα δέχομαι όλα.
    - Γράφω κανόνες για τη κίνηση που θα απορρίψουμε.
  - Προκαθορισμένη πολιτική τα απορρίπτω όλα.
    - Γράφω κανόνες για τη κίνηση που θα δεχτούμε.
- Ερώτηση:
  - Ποιά από τις δύο προσεγγίσεις είναι πιο ασφαλής και γιατί;

ΒΙΒΛΙΟΓΡΑΦΙΑ

- "Δίκτυα Υπολογιστών", A.S. Tanenbaum, Εκδόσεις Παπασωτηρίου, 3η έκδοση.
- *"The TCP/IP Guide", Charles M. Kozierok, http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm, τελευταία πρόσβαση 20/05/2010.*
- *"802.1X Port-Based Authentication HOWTO", Lars Strand, http://tldp.org/HOWTO/html_single/8021X-HOWTO/, τελευταία πρόσβαση 20/05/2010.*