Ασφάλεια Δικτύων

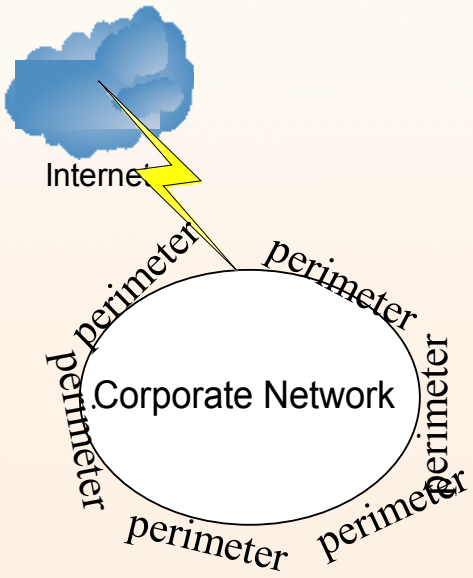
Τι (δεν) είναι Ασφάλεια Δικτύων

Γιάννης Ηλιάδης
Υπεύθυνος Ασφάλειας Δικτύου
ΤΕΙΡΕΣΙΑΣ Α.Ε.

Περίμετρος Δικτύου

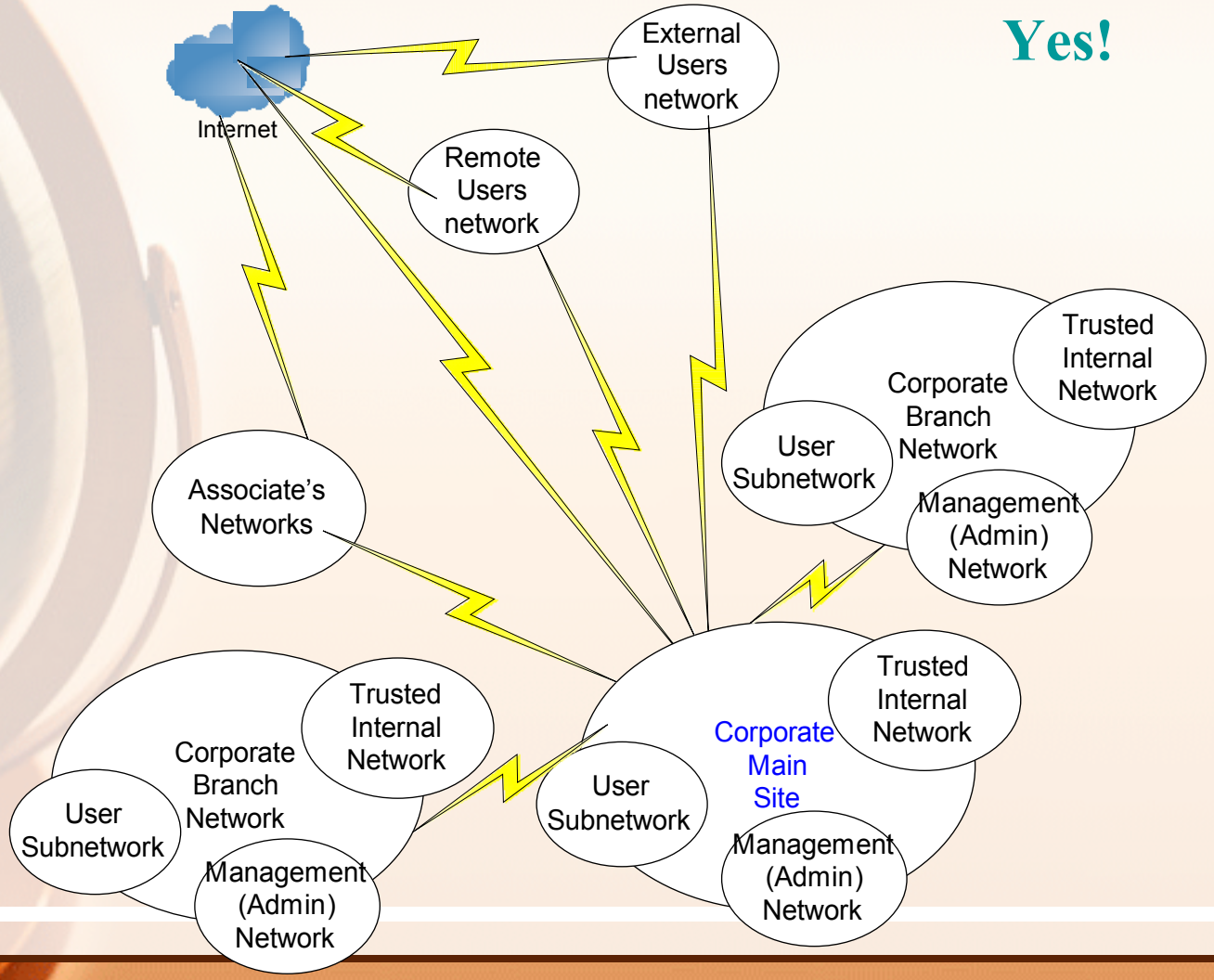
- *Αποτελεί κρίσιμο ζήτημα η περιφρούρηση της περιμέτρου δικτύου…*
  - Έλεγχος Πρόσβασης (εισερχόμενη/εξερχόμενη από τα όρια περιμέτρου)
  - Προστασία εμπιστευτικότητας και ακεραιότητας πληροφοριών που διασχίζουν όρια περιμέτρου
  - κτλ…
- Πού είναι η περίμετρος δικτύου;

Τι δεν είναι ένα δίκτυο και η περίμετρός του



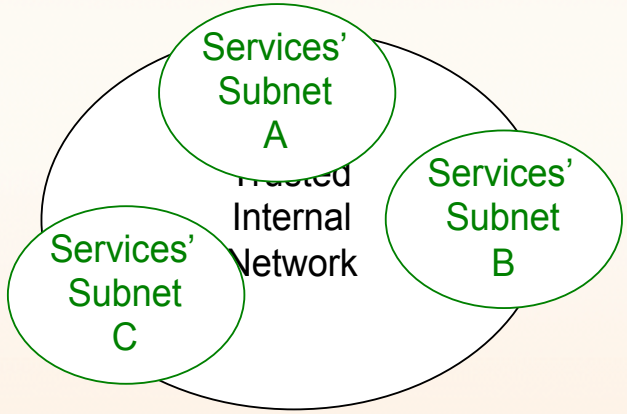
No!

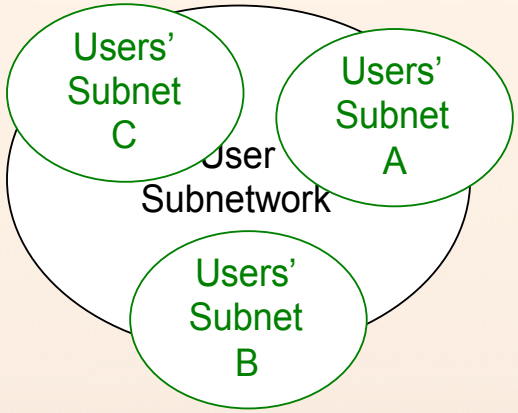
Τι είναι ένα δίκτυο και η περίμετρός του (1)



Yes!

Τι είναι ένα δίκτυο και η περίμετρός του (2)





Ορισμένες Απειλές

- **Απώλεια διαθεσιμότητας**
- **Παραβίαση εμπιστευτικότητας**
- **Μη εξουσιοδοτημένη πρόσβαση**

Απώλεια/μείωση διαθεσιμότητας – 10 Αντίμετρα

- Καλός σχεδιασμός δικτύου
- Καλός σχεδιασμός δικτύου
- Καλός σχεδιασμός δικτύου
- Καλός σχεδιασμός δικτύου
- Καλός σχεδιασμός δικτύου

- Ποιότητα Υπηρεσιών
- Ποιότητα Υπηρεσιών
- Ποιότητα Υπηρεσιών
- Ποιότητα Υπηρεσιών
- Ποιότητα Υπηρεσιών

Καλός σχεδιασμός δικτύου (1)

- Τεκμηρίωση της περιμέτρου δικτύου
- Προσεκτική δημιουργία υποδικτύων
  - Υποδίκτυα μόνο όταν υπάρχει λόγος
  - Συνόψεις διαδρομών (routes)
  - Τεκμηρίωση
  - Διαθεσιμότητα ικανοποιητικού πεδίου διευθύνσεων ανά υποδίκτυο
- Αξιολόγηση της κρισιμότητας δικτυακών ζεύξεων, με βάση τις επιχειρηματικές ανάγκες
  - Απώλεια διαθεσιμότητας συγκεκριμένων υπηρεσιών
  - Μειωμένη ικανοποίηση χρηστών
  - Μείωση εσόδων
  - Ασφάλεια δικτύου (π.χ. απώλεια διαθεσιμότητας των ενημερωμένων εκδόσεων ασφαλείας)

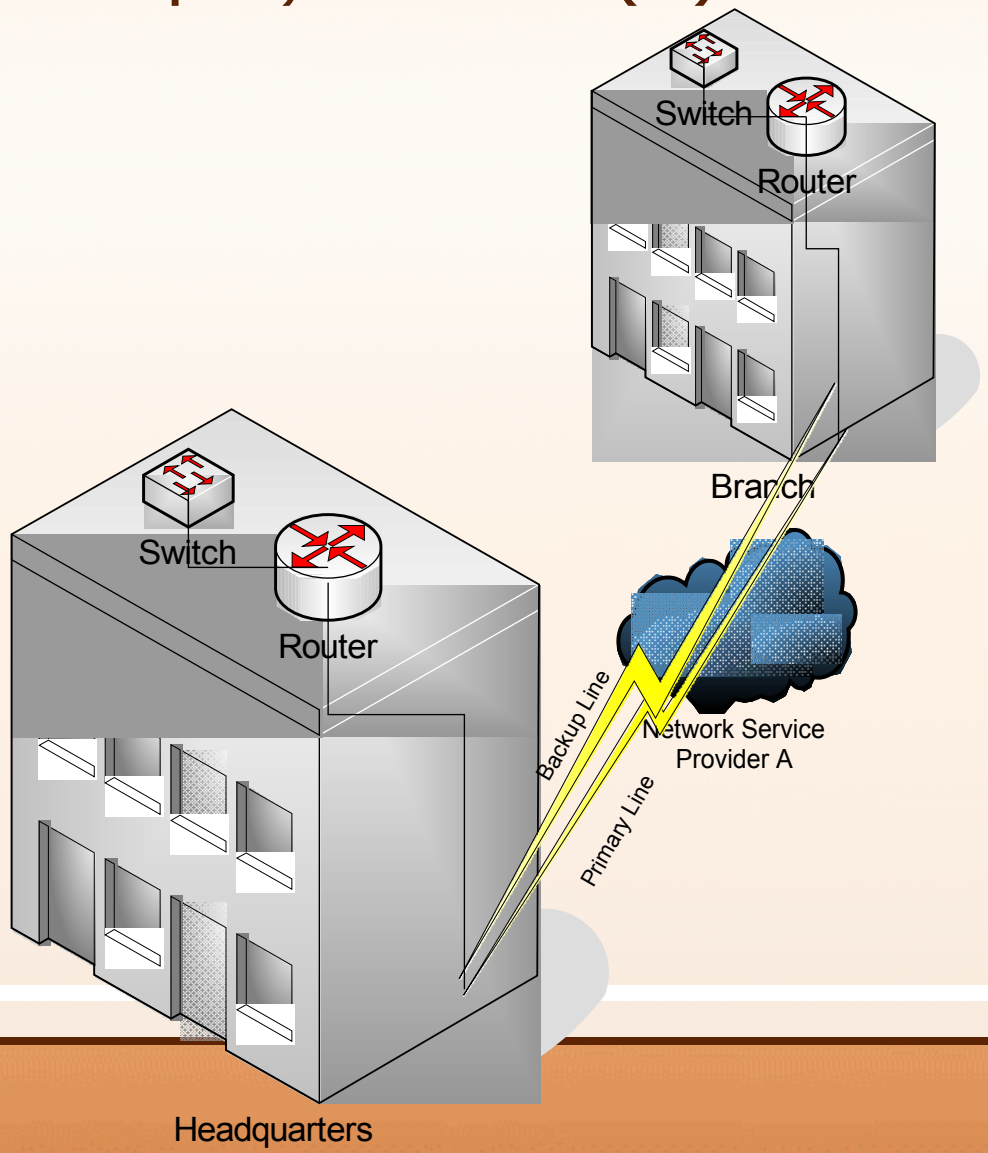
Καλός σχεδιασμός δικτύου(2)

- Πλεονάζουσες ζεύξεις
  - Αυτόματη/μη αυτόματη μετάπτωση
  - Εύρος ζώνης πλεονάζουσας γραμμής ανάλογα τα SLA, εκτιμώμενο χρόνο μη διαθεσιμότητας κύριας γραμμής, κόστους
  - Αποφυγή Μοναδικών Σημείων Αποτυχίας (και οι κύριες και οι πλεονάζουσες ζεύξεις δεν είναι διαθέσιμες)

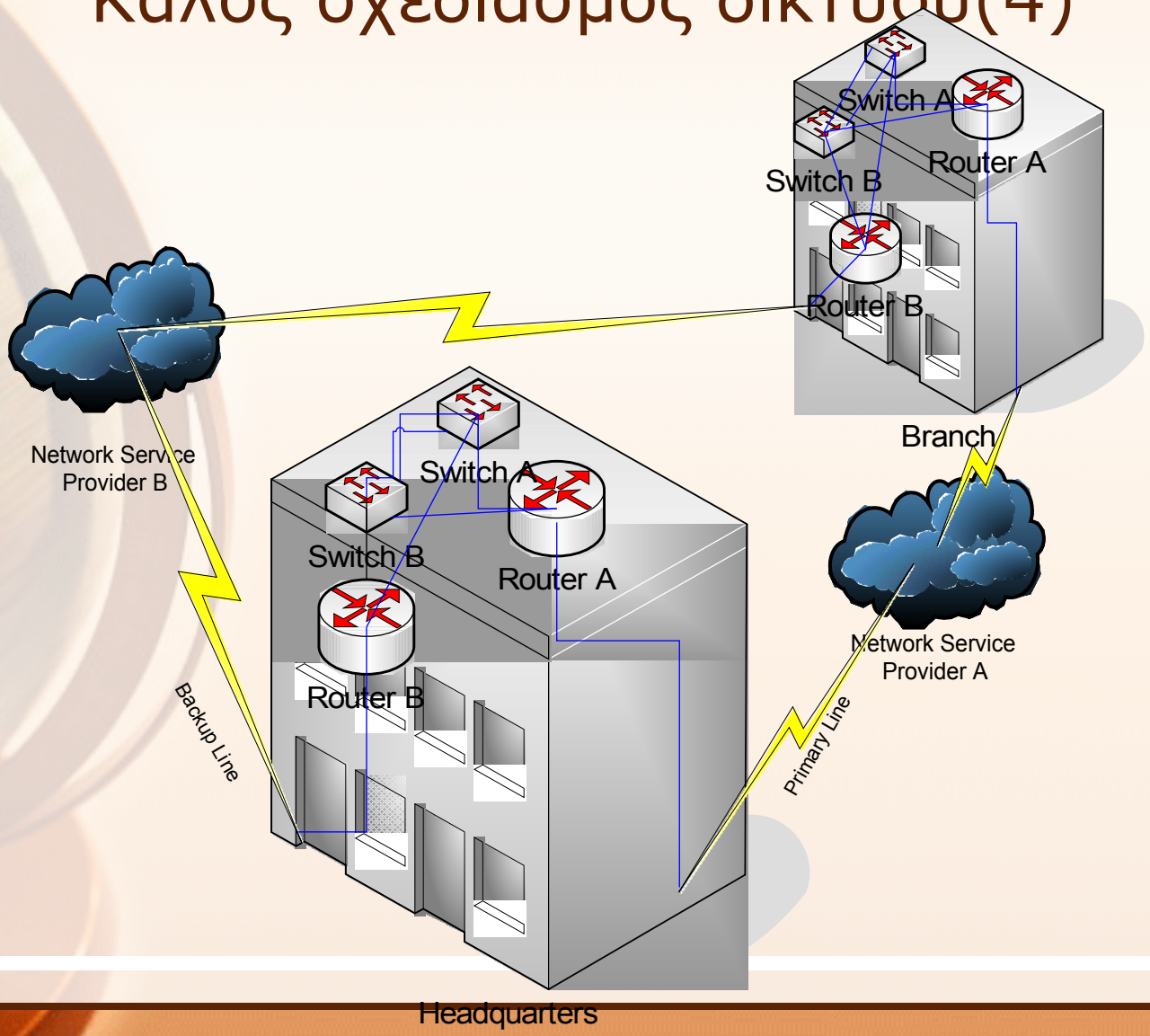
Καλός σχεδιασμός δικτύου(3)

Μοναδικά Σημεία Αποτυχίας:

3. Switches
4. Routers
5. Εσωτερική καλωδίωση κτιρίου
6. Εξωτερική καλωδίωση κτιρίου
7. Δίκτυο Παρόχου Υπηρεσίας Δικτύωσης



Καλός σχεδιασμός δικτύου(4)



Ποιότητα Υπηρεσιών (1)

Όλες οι υπηρεσίες γεννήθηκαν ίσες.
Ορισμένες είναι περισσότερο ίσες από άλλες.

- Η ανάγκη για Ποιότητα Υπηρεσιών
  - Αναμενόμενη εμπειρία χρήστη (SLA ή όχι)
  - Δικτυακή κίνηση σχετική με επιχειρηματικές ανάγκες ή δικτυακή κίνηση για προσωπικούς λόγους
  - Ορισμένες υπηρεσίες απλά χρειάζονται εξασφαλισμένη Ποιότητα (π.χ. VoIP, κίνηση διαχείρισης δικτύου)
  - Προστασία από επιθέσεις Άρνησης Υπηρεσίας και Κατανεμημένης Άρνησης Υπηρεσίας

Ποιότητα Υπηρεσιών (2)

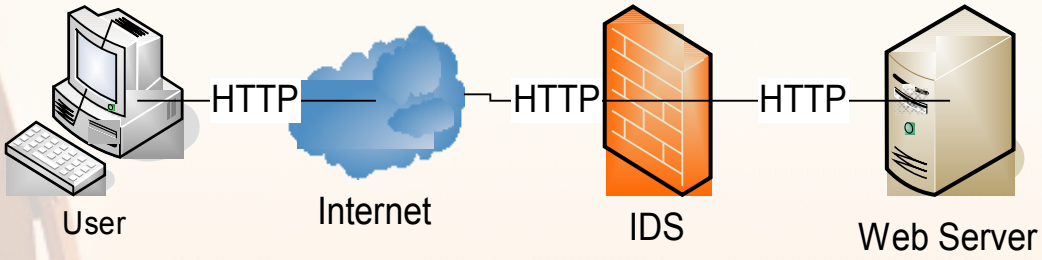
- Ποιότητα Υπηρεσιών – Τι και πως
  - Περιορισμός εύρους ζώνης
  - Περιορισμός ρυθμού πακέτων
  - Εγγύηση εύρους ζώνης
  - Εγγύηση ρυθμού πακέτων
  - Ποσοστά στιγμιαίων υψηλών αναγκών σε εύρος ζώνης (burst)
  - Απόλυτες τιμές, ποσοστά επί της συνολικής χωρητικότητας, ποσοστά επί της διαθέσιμης χωρητικότητας
  - Best Effort: το παιδί ενός κατώτερου Θεού
  - Περιορισμοί Ποιότητας επιβαλλόμενοι σε πρωτόκολλα/διευθύνσεις κατόπιν ενημέρωσης από IDS/IPS (αποφυγή επιθέσεων DoS, DDoS)

Παραβίαση εμπιστευτικότητας (ιδιωτικότητα;) - Αντίμετρα

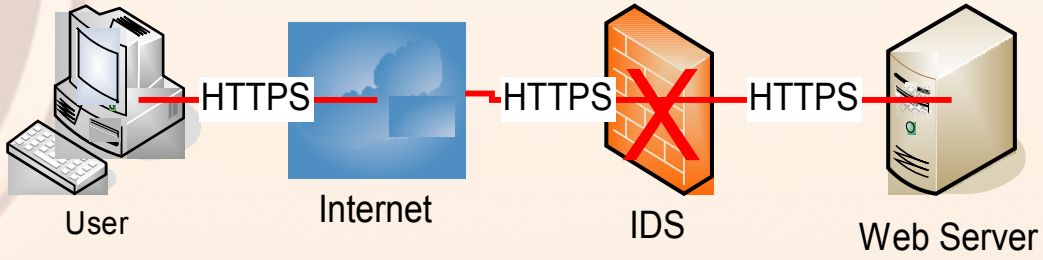
- Κρυπτογράφηση
  - SSL
  - IPsec
  - SSH tunnels
  - WEP?
  - Άλλα

SSL – λανθασμένες υλοποιήσεις

Πριν

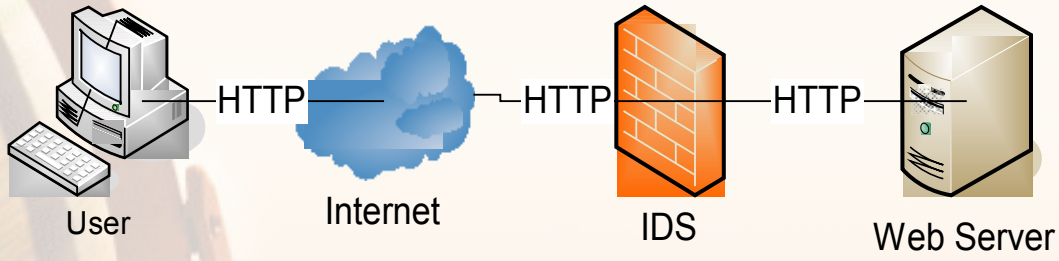


Μετά

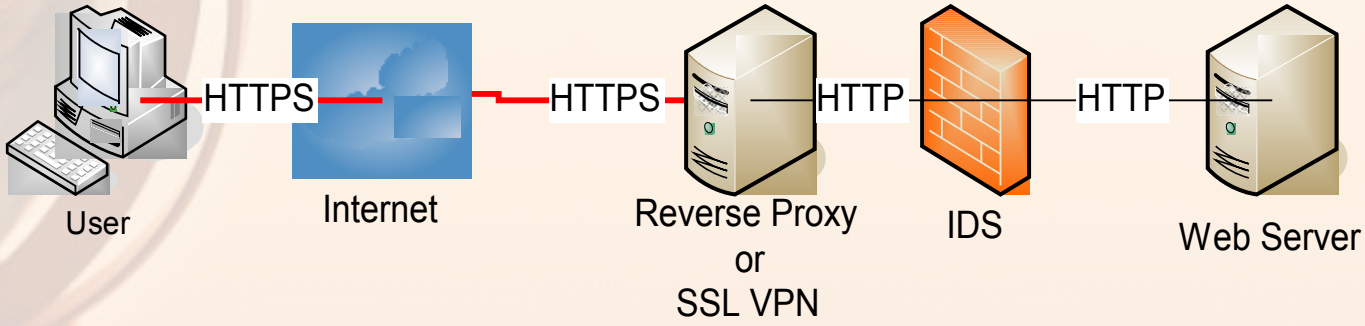


SSL – ο σωστός τρόπος*

Πριν



Μετά



*μειωμένα επίπεδα ιδιωτικότητας…

IPsec – δεν πρόκειται περί…

- Προστασία εμπιστευτικότητας
- Αποτροπή μη εξουσιοδοτημένης πρόσβασης

…τότε περί τίνος πρόκειται ;

IPsec – πρόκειται περί…

- Πρόκειται περί κρυπτογράφησης, περί της αντικατάστασης ενός πεδίου προβλημάτων με ένα άλλο, δηλαδή
  - Πρόβλημα: “Προστασία της εμπιστευτικότητας της μεταδιδόμενης πληροφορίας”
  - Λύση: “Αντικατάσταση του αρχικού προβλήματος με το πρόβλημα της διαχείρισης κλειδιών”

Διαχείριση Κλειδιών – Συμμετρική Κρυπτογράφηση

- Το πεδίο προβλήματος παραμένει η *προστασία της εμπιστευτικότητας της μεταδιδόμενης πληροφορίας, αλλά:*

2. Η πληροφορία που πρέπει να προστατευθεί (κλειδιά) είναι πολύ μικρότερη σε όγκο
3. Η συχνότητα μετάδοσης της προς προστασία πληροφορίας είναι χαμηλή
4. Η προς προστασία πληροφορία μπορεί να μεταδοθεί με (ασφαλή) τρόπο εκτός του κανονικού καναλιού επικοινωνίας

Διαχείριση Κλειδιών – Ασύμμετρη Κρυπτογράφηση

- Το πεδίο προβλήματος μετατρέπεται σε προστασία ακεραιότητας των κλειδιών
- Η προς προστασία πληροφορία μπορεί να μεταδοθεί με (ασφαλή) τρόπο εκτός του κανονικού καναλιού επικοινωνίας
- Υπάρχουν υποδομές (π.χ. ιεραρχίες PKI, PGP web of trust) που διευκολύνουν την προστασία ακεραιότητας κλειδιών, εφόσον οι υποδομές έχουν ξεκινήσει να λειτουργούν

WEP: Wireless Encryption Protocol (Where Everything is Permitted;)

-"Χαίρετε. Έχουμε μία εξαιρετικά καλή προσφορά για γραμμή ADSL για εσάς. Είναι φθηνή και θα εγκατασταθεί αμέσως, αν την επιλέξετε"

-"Όχι, ευχαριστώ. Μία εταιρεία που βρίσκεται κοντά στην οικία μου χρησιμοποιεί WEP για την κρυπτογράφηση της κίνησης του ασύρματου δικτύου της και τον έλεγχο πρόσβασης, και έχουν μισθωμένη γραμμή 20Mbps με το Διαδίκτυο"

σημείωση1: αν έχει σπάσει, έχει σπάσει

σημείωση 2: Για ασύρματα δίκτυα, προτείνεται VPN πάνω από το WEP/WPA

Μη εξουσιοδοτημένη πρόσβαση - Αντίμετρα

- Πριν το γεγονός
  - Ισχυρή επαλήθευση ταυτότητας (π.χ. δύο παραγόντων)
  - Απομόνωση υπηρεσιών
  - Διαχωρισμός καθηκόντων
  - Αποκλεισμός συγκεκαλυμμένων καναλιών
- Μετά το γεγονός
  - Έλεγχος (Audit)
  - Περισσότερος έλεγχος
  - Έλεγχος: ο σωστός τρόπος και γιατί δεν μπορείτε να το κάνετε

Ισχυρή επαλήθευση ταυτότητας

- Τι γνωρίζω
  - Συνθηματικό
  - Συνθηματική φράση
- Τι κατέχω
  - Πιστοποιητικό στον υπολογιστή
  - Πιστοποιητικό σε συσκευή (usb token, έξυπνη κάρτα)
  - Γεννήτρια ψευδοτυχαίων αριθμών (ζητήματα συγχρονισμού ώρας)

Απομόνωση Υπηρεσιών

- IPsec: Ξεχωριστά κλειδιά ανά ομάδες χρηστών και αντίστοιχες υπηρεσίες στις οποίες έχουν δικαίωμα πρόσβασης
- Υποδίκτυα και φίλτρα πακέτων (firewalling)
- Εικονικά Τοπικά Δίκτυα (VLANs)
- Λίγες (μία) υπηρεσία ανά Εξυπηρετητή
- Τερματισμός μη χρησιμοποιούμενων υπηρεσιών στους Εξυπηρετητές

σημείωση: οι Εικονικές Μηχανές δεν προσφέρουν απομόνωση υπηρεσιών

Διαχωρισμός Καθηκόντων

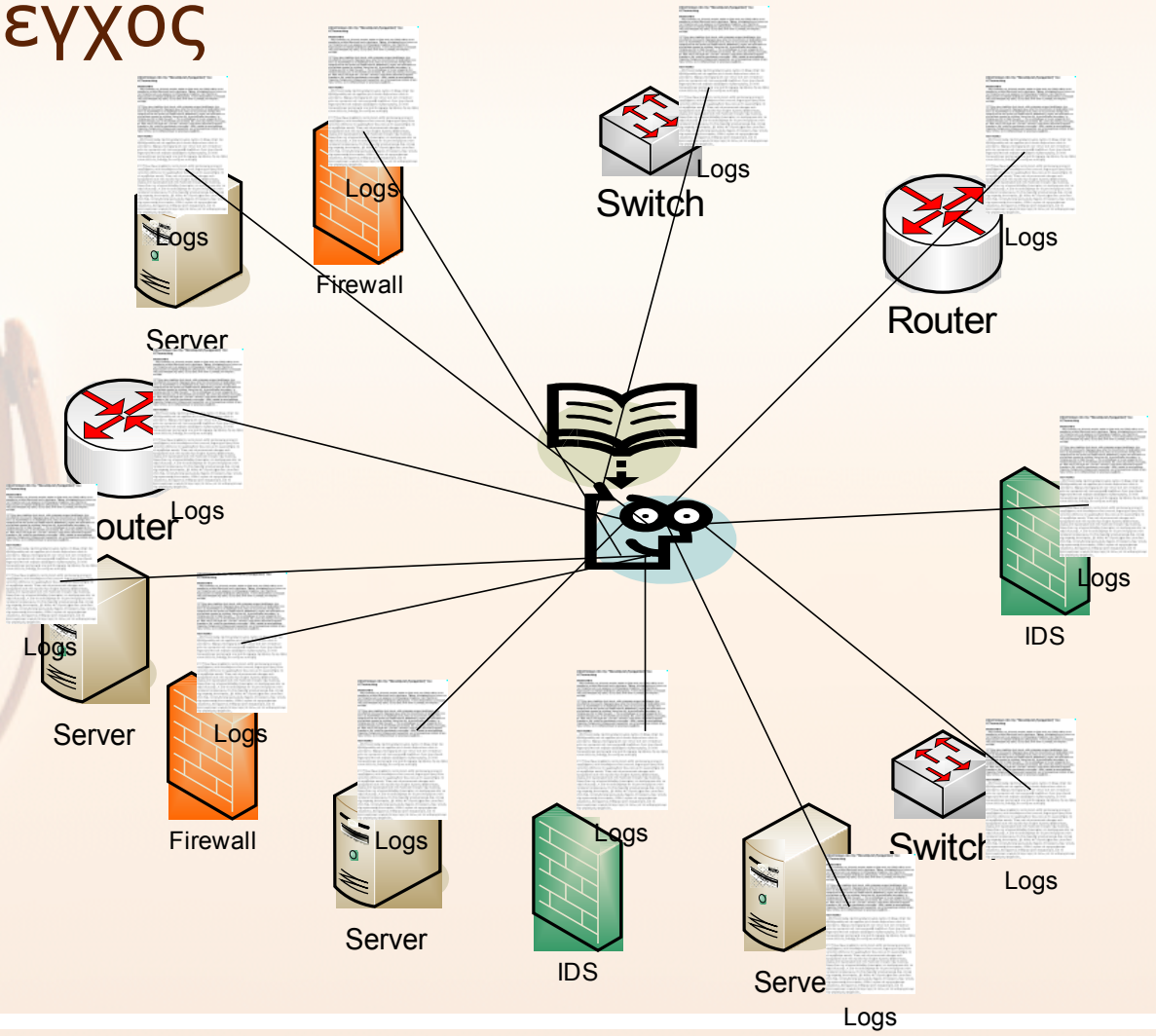
- Διαχειριστές Συστήματος
- Διαχειριστές Δικτύου
- Διαχειριστές Ασφάλειας Συστήματος
- Διαχειριστές Ασφάλειας Δικτύου
- Ελεγκτές
- Αναλυτές Επικινδυνότητας
- Υπεύθυνοι Ασφαλείας (Security Officers)

Αποκλεισμός συγκεκαλυμμένων καναλιών

- Γνωστά συγκεκαλυμμένα κανάλια
  - Port knocking
  - Tunneling (e.g. διοχέτευση ενός επιπέδου IP πάνω από ένα επίπεδο Εφαρμογής)
  - Στεγανογραφικά κανάλια
- Δύσκολα στον εντοπισμό
- Λύσεις:
  - Port knocking: να επιτρέπεται πρόσβαση μόνο στις αναγκαίες θύρες, περιορισμός ρυθμού πακέτων
  - Tunneling: έλεγχος επιπέδου Εφαρμογής για περιεχόμενο που παραβιάζει το συντακτικό/μορφότυπο
  - Στεγανογραφία: στεγανάλυση, στεγανογραφική απολύμανση

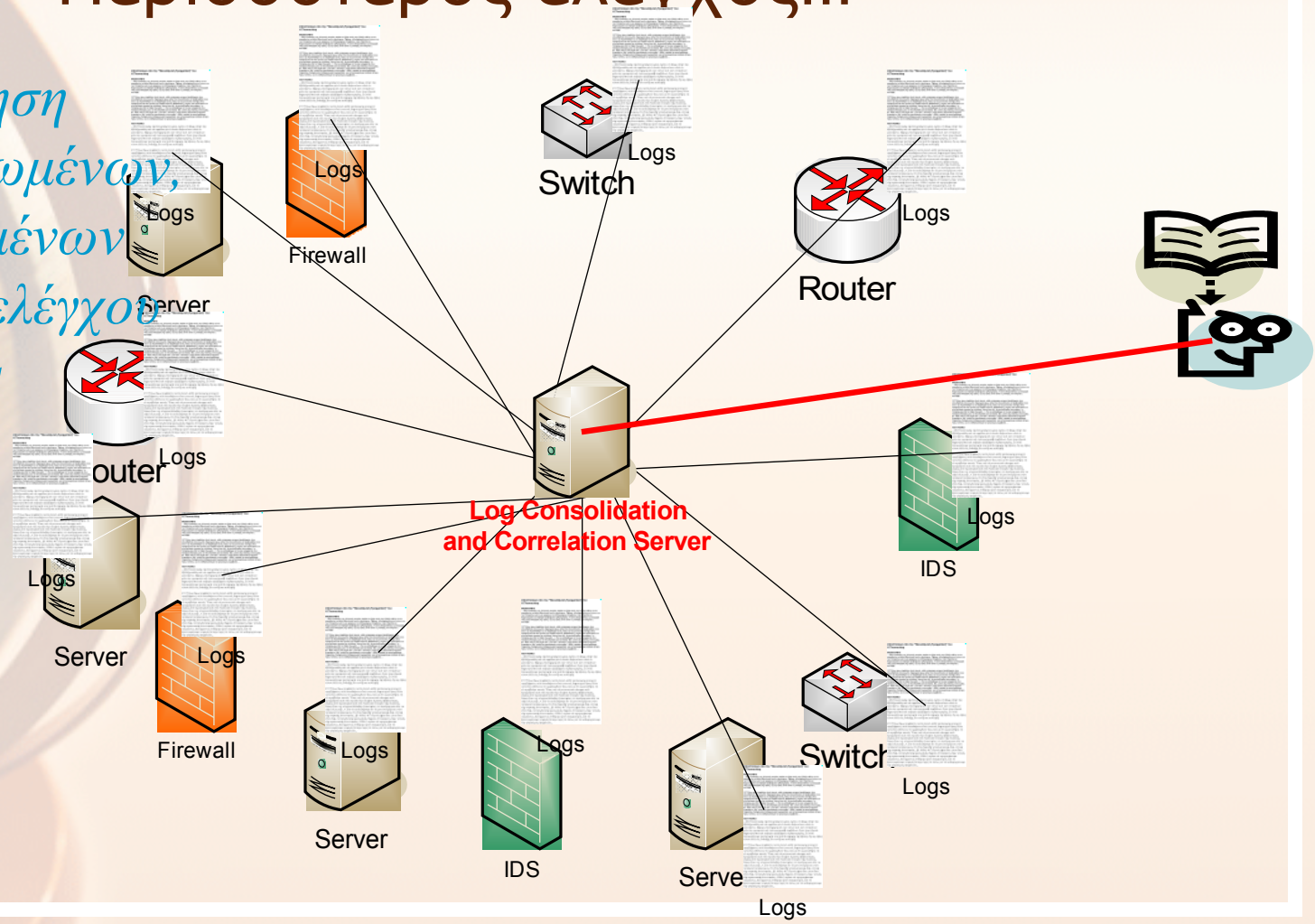
Έλεγχος

Επιθεώρηση αρχείων ελέγχου



Περισσότερος έλεγχος…

Επιθεώρηση συγκεντρωμένων, συσχετισμένων αρχείων ελέγχου και alerts



Έλεγχος: ο σωστός τρόπος (ζητήματα ιδιωτικότητας…)

Επιθεώρηση συγκεντρωμένων, συσχετισμένων αρχείων ελέγχου, alerts και κίνησης δικτύου που πιθανώς σχετίζεται με τα alerts