Γενικές Αρχές των Εικονικών Δικτύων

Εισαγωγή

- Η ραγδαία ανάπτυξη του Internet έχει αλλάξει πλήρως το γενικότερο τηλεπικοινωνιακό πλαίσιο στις τελευταίες δεκαετίες.
- Προσφέρει πληθώρα υπηρεσιών, πολλές σε χαμηλό κόστος (από χρήση απλών τηλεφωνικών γραμμών για μετάδοση δεδομένων, μέχρι ζεύξεις πολύ υψηλής ταχύτητας για μετάδοση εφαρμογών multimedia)
- Προβλήματα (που ανέκυψαν λόγω της, πέρα από κάθε προσδοκία, εξέλιξής του):
  - Η αύξηση των χρηστών δημιουργεί προβλήματα διαθέσιμου εύρους ζώνης, το οποίο με τη σειρά του θέτει ζητήματα αξιοπιστίας της μετάδοσης – π.χ. δεν πρέπει να χάνονται πακέτα, δεν πρέπει οι καθυστερήσεις πακέτων να είναι μεγάλες κ.ο.κ.)
  - Προβλήματα ασφάλειας

Επίπεδα υπηρεσιών Internet

- Δημόσιο επίπεδο
  - Έχει να κάνει με την ανάπτυξη της Internet τεχνολογίας για υπηρεσίες που όλοι έχουν πρόσβαση (π.χ. ηλεκτρονικό εμπόριο)
  - Ιδιωτικό επίπεδο
    - Έχει να κάνει με υπηρεσίες που χρησιμοποιούν την υπάρχουσα δομή του Internet, αλλά απευθύνονται σε λίγους – μόνο σε εξουσιοδοτημένα άτομα (π.χ. ένα **ιδιωτικό δίκτυο** μιας εταιρίας με στόχο την ενδο-επικοινωνία των στελεχών της ή την επικοινωνία τους με τους απομακρυσμένους πελάτες της).

Προϊστορία ιδιωτικών δικτύων

- Δεκαετία 1960: Μισθωμένη γραμμή για σύνδεση δύο σημείων (endpoints) – χρήση modems 2400 bps
  - Η ζεύξη δεν ανήκε στο δημόσιο τηλεφωνικό δίκτυο (PSTN)
  - Το εύρος ζώνης της ζεύξης ήταν διαθέσιμο μόνο στον πελάτη που την έχει εκμισθώσει
    - Πλεονεκτήματα: εξασφάλιση της μυστικότητας της μετάδοσης, καθώς και εγγυημένη ύπαρξη εύρους ζώνης ανά πάσα στιγμή
    - Μειονεκτήματα: όχι «ευέλικτα» δίκτυα, καθώς και υψηλού κόστους (η εταιρία πλήρωνε τη ζεύξη ακόμα κι αν δεν τη χρησιμοποιούσε)

Προϊστορία ιδιωτικών δικτύων (ΙΙ)

- Δεκαετία 1970: Υπηρεσίες ψηφιακών δεδομένων (Digital Data Service – DDS)
  - Συνδέσεις 56 kbps για ιδιωτικά δίκτυα εταιριών
  - T1 υπηρεσίες: ταχύτητες μετάδοσης 1,544 Mbps
- Αρχές 1990: Ανάγκη για μετάδοση φωνής και όχι δεδομένων -> T1 υπηρεσίες σε εταιρίες για φτηνές φωνητικές κλήσεις. Όμως:
  - η μείωση του κόστους των τηλεφωνικών κλήσεων που ακολούθησε κατέστησε την εκμίσθωση T1 γραμμών για τηλεφωνία οικονομικά ασύμφορη.
  - Ραγδαία αύξηση του αιτούμενου εύρους ζώνης για μετάδοση δεδομένων

Προϊστορία ιδιωτικών δικτύων (ΙΙΙ)

- Προβλήματα όλων των παραπάνω ιδιωτικών δικτύων
  - Η εγκαθίδρυση ενός τέτοιου εικονικού δικτύου είναι χρονοβόρα
  - Υψηλό κόστος συντήρησης και επεκτασιμότητας
  - Ανάγκη ύπαρξης modem banks για τους «κινητούς» πελάτες

Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPNs)

- Ορισμός
  - Δίκτυο εικονικών ζεύξεων, για τη μετάδοση ιδιωτικής πληροφορίας
  - Είναι δομημένο πάνω σε κάποιο δημόσιο υπάρχον δίκτυο (κύρια στο Internet)

- Επιθυμητά χαρακτηριστικά
  - Ασφάλεια
  - Εγγυημένη ποιότητα υπηρεσιών

Κίνητρα

- Οικονομικά
  - Η χρήση της υπάρχουσας δημόσιας υποδομής μειώνει το κόστος του δικτύου
  - Παύει η ανάγκη ύπαρξης μισθωμένων γραμμών
- Μυστικότητα στις τηλεπικοινωνίες
  - Κρυπτογράφηση της μεταδιδόμενης πληροφορίας
  - Αποκλειστική χρήση του εικονικού δικτύου μόνο από εξουσιοδοτημένους χρήστες
- «Διαφανής» εξοπλισμός
  - Οι ISPs, κι όχι οι ίδιες οι εταιρίες που χρησιμοποιούν τα VPNs, διαχειρίζονται το δίκτυο

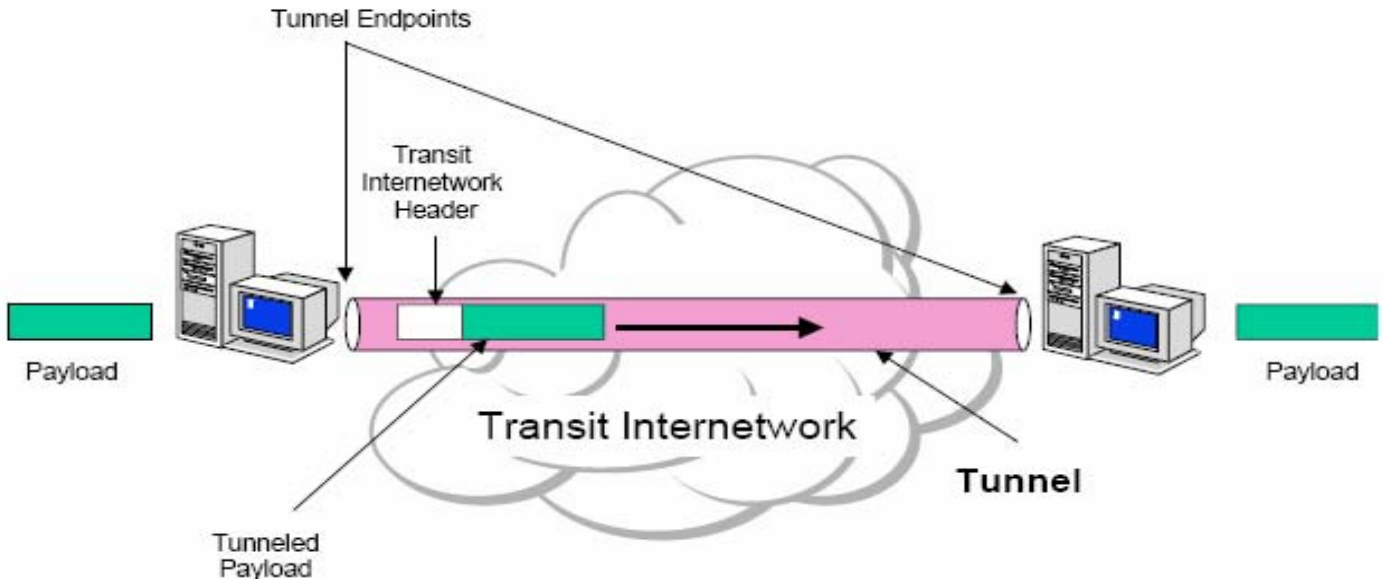
Γενικά χαρακτηριστικά ενός VPN

- Δημιουργεί ένα λογικό («ιδεατό») δίκτυο πάνω σε πολλαπλές φυσικές ζεύξεις.
- Υποστήριξη πολλαπλών πρωτοκόλλων

Βασική λειτουργία ενός VPN

- Μία εταιρία ξεκινά μία ιδιωτική σύνδεση μέσω του ISP (Internet Service Provider), ο οποίος είναι ο αποκλειστικός υπεύθυνος για την περαιτέρω δρομολόγηση της μεταδιδόμενης πληροφορίας (πάνω στην υποδομή του Internet).
- Η ζεύξη για μία συγκεκριμένη επικοινωνία δύο «τελικών χρηστών» γίνεται δυναμικά: όταν ολοκληρωθεί η επικοινωνία, το εύρος ζώνης αποδεσμεύεται.
- Οι εικονικές ζεύξεις πραγματοποιούνται με ενθυλάκωση των πακέτων δεδομένων σε **ειδικά** IP πακέτα, κατάλληλων για μετάδοση σε δίκτυο internet (πρωτοκόλλου IP). Στην ορολογία των VPNs, αυτές οι εικονικές ζεύξεις ονομάζονται **τούνελ** (**tunnels**)

Σχηματική αναπαράσταση



Ένα tunnel μεταφέρει δεδομένα από ένα δίκτυο σε άλλο

Πλεονεκτήματα των VPNs

- Λιγότερο κόστος, σε σχέση με τις μισθωμένες γραμμές
- «Ευελιξία» (flexibility)
  - Με τα παλιότερα εικονικά δίκτυα, άλλες τεχνολογίες που ενυπάρχουν στο εσωτερικό της εταιρίας (DSL, ISDN κ.ο.κ.) χρειάζονται πρόσθετο εξοπλισμό προκειμένου να συμμετέχουν στο εικονικό δίκτυο. Στα VPN όλες οι τεχνολογίες είναι συμβατές, αφού όλες μπορεί να τις χειριστεί ο ISP.
- Προσαρμοστικότητα (scalability)
- Μειωμένες απαιτήσεις εξοπλισμού

Πλεονεκτήματα των VPNs

- Προσαρμοστικότητα/Κλιμάκωση (scalability)
  - Γεωγραφική: οποιοσδήποτε χρήστης από οποιοδήποτε μέρος κι αν βρίσκεται μπορεί να συνδεθεί στο VPN, αρκεί ο ISP να διαθέτει POP (*Point of Presence: σημείο πρόσβασης στο internet που βρίσκεται σε κάθε ISP. Το πλήθος τους σε έναν ISP προσδιορίζει το μέγεθός του).*
  - Εύρους ζώνης: Μπορεί ένας υπολογιστής σε γραφείο που ανήκει στο δίκτυο να χρειάζεται T1, ενώ ο υπολογιστής του ίδιου εργαζόμενου που βρίσκεται στο σπίτι του να του αρκεί μία dial-up σύνδεση.
- Μειωμένες απαιτήσεις εξοπλισμού

Θέματα που ανακύπτουν στη σχεδίαση ενός VPN

- Ασφάλεια (Security)
  - Η μετάδοση μέσω των tunnels πρέπει να είναι κρυπτογραφημένη (αν και αυτό είναι μεν αναγκαίο, αλλά όχι αρκετό για τη γενικότερη μυστικότητα που θέλει να διατηρεί μία εταιρία).
- Πιθανή συμφόρηση
  - Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν υπολογιστική ισχύ, συνεπώς μπορούν να ρίξουν την ολική απόδοση. Για ζεύξεις υψηλού εύρους ζώνης είναι προτιμότερη η hardware-based κρυπτογράφηση.
  - Η ενθυλάκωση των πακέτων μπορεί να κάνει το μέγεθός τους μεγαλύτερο από ό,τι οι δρομολογητές μπορούν να χειριστούν. Σε αυτήν την περίπτωση, τα πακέτα διασπώνται (fragmentation). Αυτό επηρεάζει τη συνολική ποιότητα υπηρεσιών (Quality of Service - QoS)

Θέματα που ανακύπτουν στη σχεδίαση ενός VPN (II)

- Διαλειτουργικότητα (Interoperability)
  - Είναι ανοιχτό πρόβλημα. Τα PPTP και L2TP «ταιριάζουν» καλύτερα σε client-initiated tunnels, ενώ το IPSec προσφέρεται για LAN-to-LAN tunnels (θα αναλυθούν παρακάτω).
- Διαχείριση IP Διευθύνσεων (Addressing)
  - Μπορούν δύο ιδιωτικά δίκτυα με τον ίδιο χώρο IP διευθύνσεων να επικοινωνήσουν μεταξύ τους?

Θέματα που ανακύπτουν στη σχεδίαση ενός VPN (III)

- Αξιοπιστία και απόδοση (reliability-performance)
  - Υπόκεινται σε όσα προβλήματα μετάδοσης υπάρχουν στο Internet. Ευαίσθητες είναι οι real-time εφαρμογές.
- Υποστήριξη πολλαπλών πρωτοκόλλων (multiprotocol support)
  - Το IPSec είναι σχεδιασμένο για TCP/IP, κι έτσι η μετάδοση άλλων πακέτων (όχι IP) δεν είναι δυνατή – συνεπώς, οδηγηθήκαμε στην ύπαρξη πολλών πρωτοκόλλων.