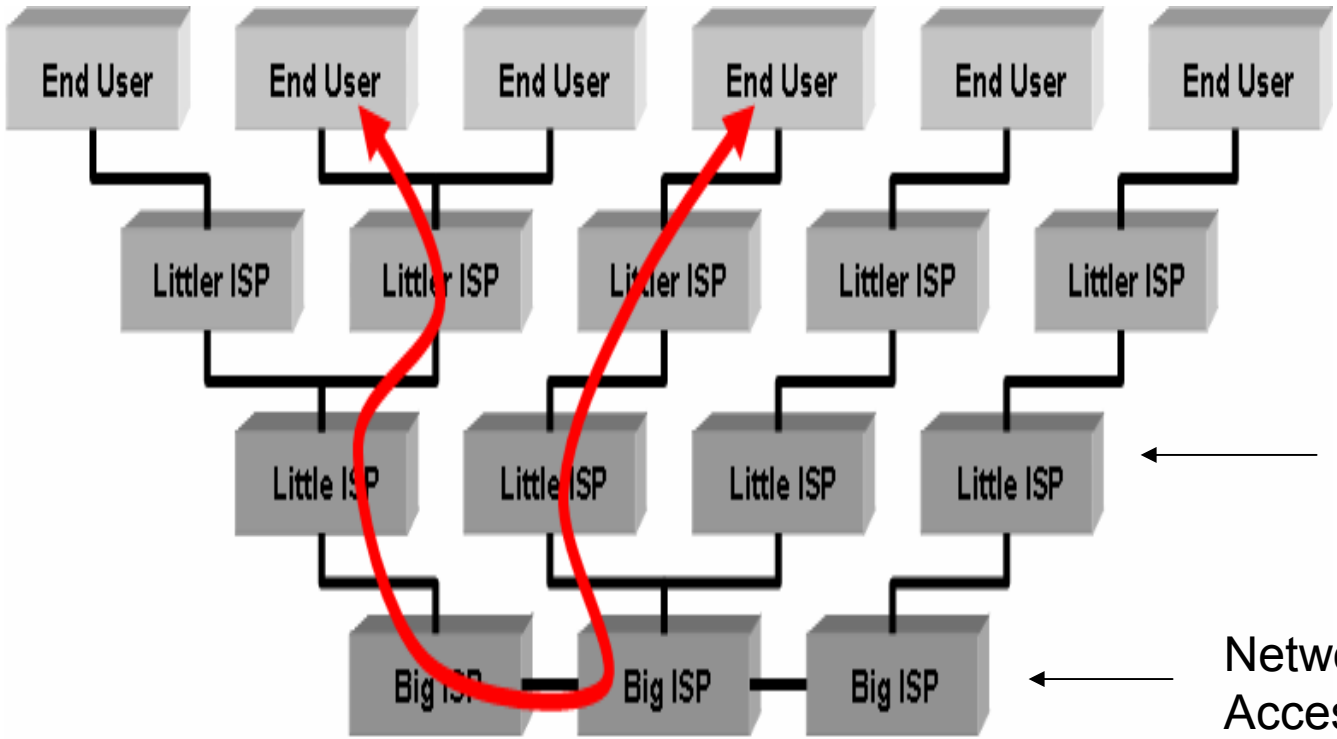
Δομικά στοιχεία ενός Εικονικού Ιδιωτικού Δικτύου
- Παροχείς Υπηρεσιών Internet (Internet Service Providers)

Γενικά

- Τι ερωτήματα πρέπει να έχουν απαντηθεί, προτού επιχειρηθεί η δόμηση ενός VPN?
  - Πόσοι χρήστες υπάρχουν σε κάθε πλευρά?
  - Τι είδους σύνδεση θα υπάρχει στο Internet? Μόνιμη ή κατόπιν αίτησης (π.χ. Dial-up)?
  - Πόση περίπου κίνηση αναμένεται να υπάρξει από την κάθε πλευρά? (καθώς και πώς μεταβάλλεται η κίνηση αναλόγως την ώρα ή τη μέρα)
  - Θα υπάρχει η δυνατότητα σύνδεσης απομακρυσμένων χρηστών? Αν ναι, πόσοι?
  - Τι εφαρμογές θα εξυπηρετούνται? (αυτό θα καθορίσει το κατά πόσον υπάρχοντα WAN μπορούν να χρησιμοποιηθούν σαν βάση ενός VPN).
  - Είναι όλα τα δεδομένα που θα αποστέλλονται της ίδιας βαρύτητας και σημασίας? Δεδομένα που δεν είναι τόσο κρίσιμη η μυστικότητά τους θα ήταν καλό να αντιμετωπίζονται διαφορετικά – αποφεύγοντας έτσι κάποιο κόστος.
  - Προνοητικότητα για το τι αλλαγές αναμένεται να υπάρξουν στο μέλλον, όσον αφορά τις ανάγκες του δικτύου

Η Ιεραρχία των ISPs



Στην ουσία, το Internet στο σύνολό του είναι αποτέλεσμα της διασύνδεσης των NAPs.

Point of Presence (POP)

- Το POP είναι το τμήμα εκείνο του ISP στο οποίο συνδέονται οι χρήστες, χειρίζεται τα διάφορα εισερχόμενα είδη κίνησης και τα προωθεί στο δίκτυο κορμού (από το οποίο μεταβιβάζονται στο Internet).
- Ένα POP περιέχει:
  - Συλλογή modems (modem bank) για dial-in συνδέσεις
  - Δρομολογητές (routers)
  - Servers για mail (σε ορισμένες περιπτώσεις)
  - RADIUS Servers

Κριτήρια επιλογής ISP για τη δόμηση ενός VPN

- Η γεωγραφική κάλυψη που παρέχει. Για παράδειγμα, για ένα VPN διακρατικό πρέπει να χρησιμοποιηθούν αναγκαστικά και NAPs, ενώ για ένα VPN που περιορίζεται σε μία πόλη ενδεχομένως να αρκεί ένας απλός τοπικός ISP.
- Το είδος της πρόσβασης που θα παρέχει το VPN. Αν είναι μόνο απομακρυσμένης πρόσβασης, τότε πρέπει να υπάρχουν POPs στα μέρη από τα οποία οι χρήστες αναμένεται να συνδέονται. (για περιπτώσεις roaming, κάποιες εταιρίες παρέχουν τη δυνατότητα διασυνδεσιμότητας περισσότερων ISPs, δηλαδή ο χρήστης συνδέεται κάθε φορά μέσω POP διαφορετικού ISP).
- Τα χρησιμοποιούμενα πρωτόκολλα. Αν χρησιμοποιείται IPSec, όλοι οι ISPs είναι κατάλληλοι μια που παρέχουν IPSec δυνατότητες. Αντίθετα, δεν είναι εφοδιασμένοι όλοι οι ISPs με PPTP ή L2TP δυνατότητες.
- Τέλος, πρέπει πάντα να έχουμε κατά νου ενδεχόμενη εξάπλωση του VPN στο μέλλον (ποιες περιοχές θα καλύπτει, τι κίνηση θα εξυπηρετεί κτλ) για τη σωστή επιλογή του ISP.

Ποια χαρακτηριστικά του ISP ενδιαφέρουν τον σχεδιαστή ενός VPN?

- **Η ISP υποδομή** (το δίκτυο που σχηματίζουν οι ISPs). Η καλύτερη περίπτωση για ένα VPN είναι μία full-mesh topology (ο κάθε ISP συνδέεται άμεσα με όλους τους άλλους). Σήμερα, οι διαδικτυακές υποδομές των ISPs δεν δημιουργούν πρόβλημα για οποιοδήποτε είδος VPN.
- **Απόδοση**: Πρέπει να ληφθεί υπ' όψιν πόσο εύρος ζώνης έχει ήδη διαθέσει ο ISP σε άλλους πελάτες. Γενικότερα, είναι αναγκαίος ο έλεγχος του κατά πόσον ο ISP μπορεί να εξυπηρετήσει το εύρος ζώνης που χρειάζεται για το VPN. Επίσης, έλεγχος του κατά πόσον μπορεί να παρέχει το QoS που το εκάστοτε VPN απαιτεί.
- **Η ασφάλεια που παρέχει**: πρέπει να παρέχει ένας ISP δικούς του μηχανισμούς για έλεγχο της ασφάλειας των συστημάτων του.

Διαλειτουργικότητα ISP και VPN

- Αν ο ISP χρησιμοποιείται απλά και μόνο για τη σύνδεση στο Internet, τότε δεν χρειάζονται ιδιαίτερες απαιτήσεις διαλειτουργικότητας. Αν όμως είναι αυτός που εγκαθιστά τη δίοδο, τότε ζητήματα όπως το αν π.χ. υποστηρίζει RADIUS είναι κρίσιμα.
- Ζητήματα κρυπτογράφησης
  - Ποιους αλγόριθμους υποστηρίζει
  - Αν μπορεί να «μεταπηδάει» από τον έναν αλγόριθμο στον άλλο

Συμφωνίες για επίπεδο υπηρεσιών (Service Level Agreements (SLA))

- Είναι μία συμφωνία μεταξύ δύο πλευρών, όσον αφορά το πώς θα συνεργαστούν για τη διεκπεραίωση μίας συναλλαγής (επικοινωνίας).
- Κάθε ISP παρέχει μία SLA η οποία περιέχει πληροφορίες για τα εξής:
  - Διαθεσιμότητα δικτύου
  - Απόδοση
  - Καθυστέρηση
  - Μέσος χρόνος επαναφοράς, μετά από βλάβη

Πού θα επιτελούνται οι βασικές λειτουργίες του VPN?

- Έχουμε ήδη δει ότι πολλές λειτουργίες μπορούν να γίνουν από τους χρήστες του δικτύου (In-House VPN) αλλά επίσης και από άλλους παροχείς – ISPs (Outsourced VPNs). Στη δεύτερη περίπτωση γίνεται πιο επιτακτική η ανάγκη ύπαρξης SLA (όπου ο κάθε πάροχος υπηρεσιών καθορίζει την ποιότητα υπηρεσιών που παρέχει).
- Δεν είναι σαφής ο διαχωρισμός In-House με Outsourced VPNs. Συνήθως τόσο οι χρήστες του δικτύου όσο και κάποιος πάροχος επιτελούν ταυτόχρονα λειτουργίες.