Βασική αρχιτεκτονική ενός Εικονικού Δικτύου

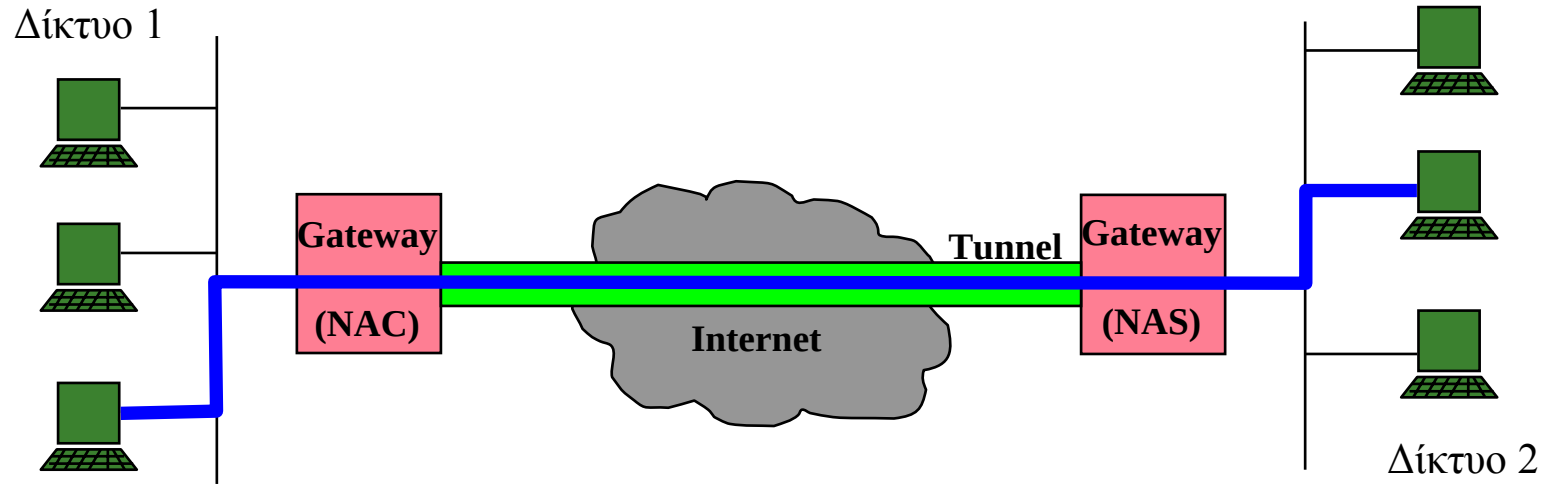
Εικονικό Ιδιωτικό Δίκτυο

- Λέγονται εικονικά γιατί δεν υπάρχει μόνιμα συνδεδεμένη γραμμή – μία λογική σύνδεση αποκαθίσταται όταν ζητείται, και απελευθερώνεται με το πέρας της συνδιαλλαγής. Επιπλέον, όλα τα υπόλοιπα στοιχεία του δικτύου (δρομολογητές κτλ) είναι διαφανή προς το χρήστη. Αυτό επιτυγχάνεται με το *tunneling*.
- Ένα tunnel δημιουργείται με την ενθυλάκωση ενός πακέτου μηνύματος σε πακέτο άλλου πρωτοκόλλου. Ειδικά για τα VPN, κατά την ενθυλάκωση γίνεται κρυπτογράφηση. Η πύλη (gateway) του δέκτη, αφού αποβάλλει την IP επικεφαλίδα, αποκρυπτογραφεί και το προωθεί στον κατάλληλο προορισμό-αποδέκτη.

Κατηγορίες VPNs με βάση τα άκρα των tunnels

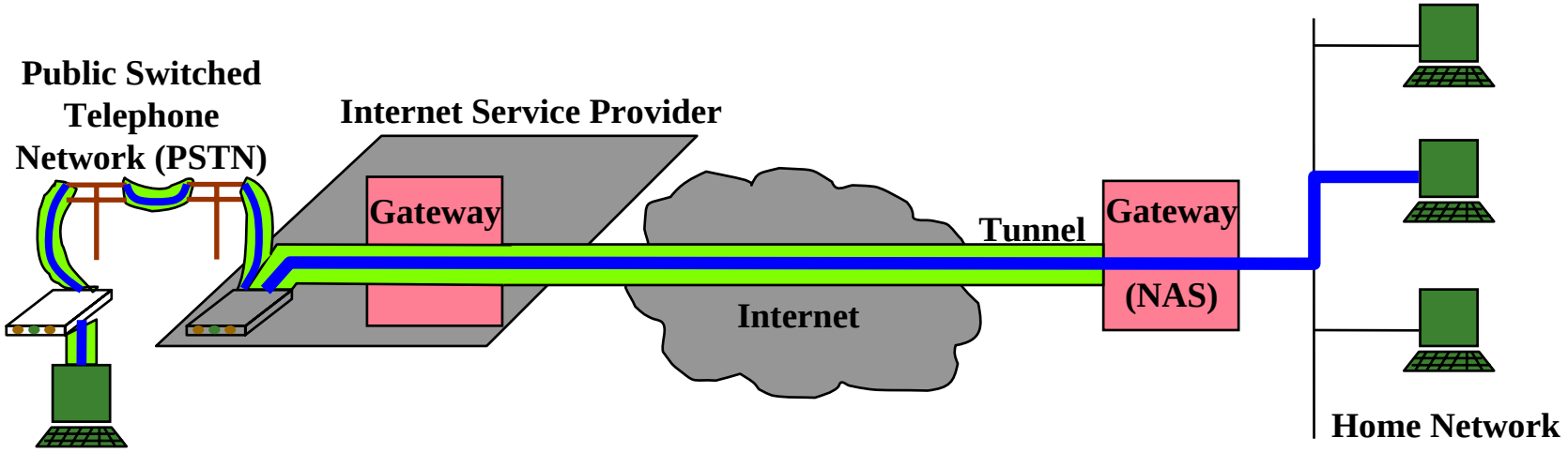
- Το άκρο ενός tunnel μπορεί να είναι είτε ένας απλός χρήστης (ένα ανεξάρτητο computer δηλαδή) είτε ένα LAN.
  - LAN-to-LAN tunneling. Μία πύλη ασφαλείας (security gateway) είναι το Interface ανάμεσα στο LAN και το tunnel
  - Client-to-LAN tunneling. Πραγματοποιείται όταν ένας κινητός χρήστης θέλει να συνδεθεί σε ένα LAN. Ο χρήστης εκτελεί κατάλληλο πρόγραμμα στον υπολογιστή του για να συνδεθεί στην πύλη του LAN

LAN-to-LAN tunnel



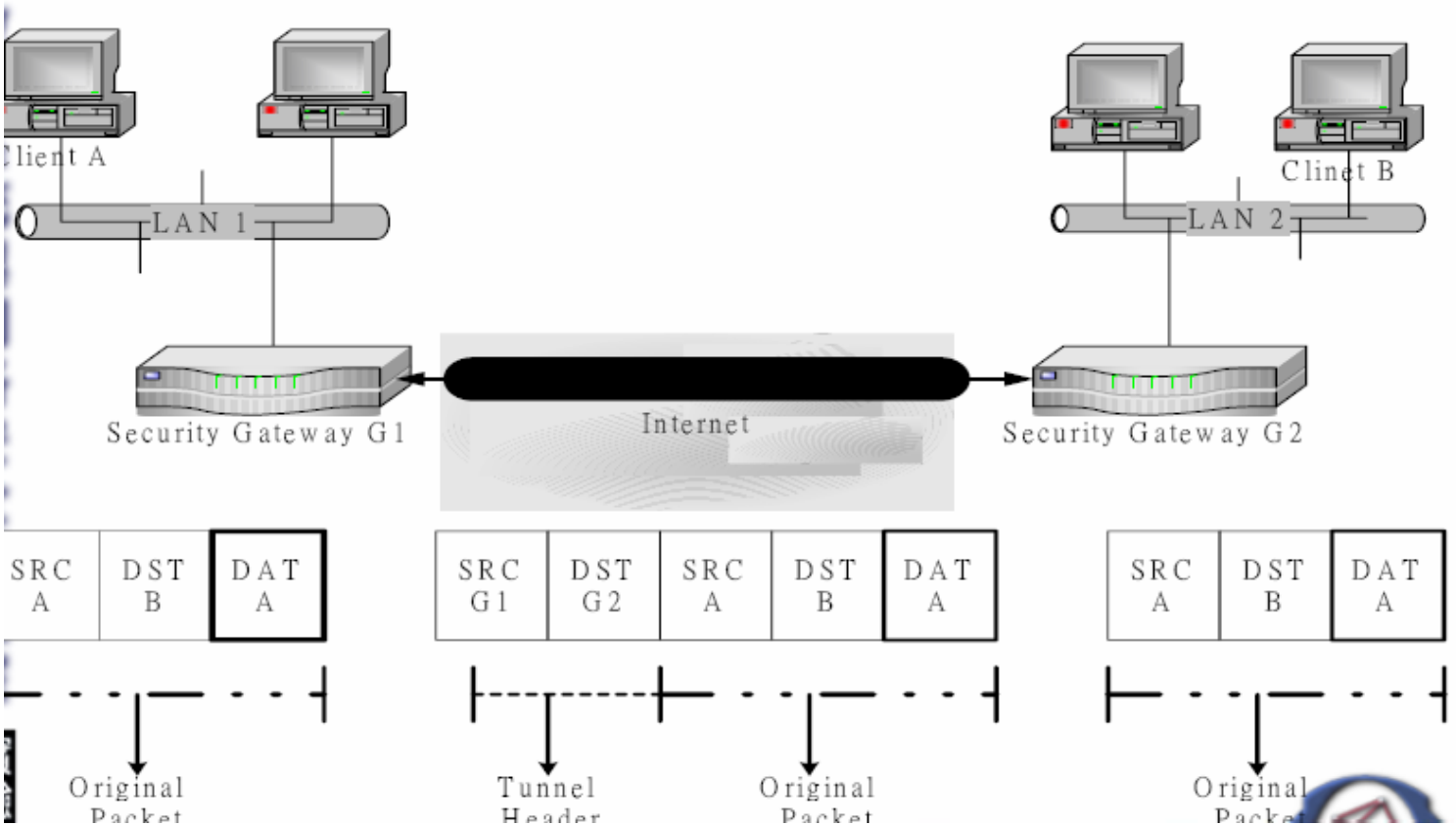
- Δημιουργία λογικών δικτύων μεταξύ των δικτύων 1 και 2

Client-to-LAN tunnel



- Ο χρήστης (ενδεχομένως κινητός) καλεί τον ISP για IP υπηρεσίες. Στη συνέχεια, ο IP αναλαμβάνει τη δημιουργία του tunnel με το δίκτυο

Σχηματική αναπαράσταση ενθυλάκωσης πακέτων για δημιουργία tunnel



Εικονικό **Ιδιωτικό** Δίκτυο

- Λέγονται ιδιωτικά γιατί παρέχουν μυστικότητα (ασφάλεια) στη μετάδοση της πληροφορίας.
- Τέσσερα πράγματα πρέπει να εξασφαλίζονται, όσον αφορά την ασφάλεια:
  - Πιστοποίηση ταυτότητας (authentication)
  - Έλεγχος πρόσβασης (access control)
  - Μυστικότητα στη μετάδοση (confidentiality)
  - Ακεραιότητα των δεδομένων (data integrity)

Πρωτόκολλα VPN

- Τα πρωτόκολλα στα VPN ανήκουν σε δύο κατηγορίες:
  - Σε εκείνα που έχουν να κάνουν με την ενθυλάκωση των πακέτων προκειμένου να σχηματιστεί το tunnel, καθώς επίσης και με την κρυπτογράφησή τους
  - Σε εκείνα που σχετίζονται με τη διαχείριση του κλειδιού, με τεχνικές πιστοποίησης ταυτότητας και γενικότερα με λειτουργίες που συντελούνται από αποστολέα και παραλήπτη σχετικές με κρυπτογραφικά πρωτόκολλα

VPN Πρωτόκολλα στο επίπεδο 2

- Point to Point Tunneling Protocol (PPTP)
  - Microsoft, Ascend κ.ά.
- Layer Two Forwarding (L2F)
  - Cisco
- Layer Two Tunneling Protocol (L2TP)
  - Ενοποίηση PPTP και L2F σε ένα πρότυπο (standard)

- Όλα υποστηρίζουν tunneling.

VPN πρωτόκολλα σε υψηλότερα επίπεδα

- IPSec: παρέχει ασφάλεια στο TCP/IP επίπεδο. Εκτός από το tunneling, παρέχει δηλαδή μηχανισμούς κρυπτογράφησης, πιστοποίησης ταυτότητας, διαχείρισης κλειδιού κτλ.
- SOCKS: επιτρέπει σε δεδομένα να διαπερνάνε έναν τοίχο ασφαλείας (firewall) ανάλογα με την ταυτότητα του αποστολέα (και όχι με βάση π.χ. τη UDP πόρτα που αναγράφεται στο IP πακέτα)

Στρωμάτωση των πρωτοκόλλων στα VPN – συσχέτιση με τα στρώματα OSI

Application	**Application proxy server**	
Presentation		
Session		**HTTPS**
Transport	**SOCKS**	**SSL**
Network	**IPSec**(IP Security)	**L2TP** (Layer 2 Tunneling Protocol)
Data Link	**L2F**(Layer 2 Forwarding) **PPTP**(Point to Point Tunneling Protocol)	
Physical		

Πρωτόκολλα Διαχείρισης

- Για client-to-LAN tunnels: RADIUS
- Για LAN-to-LAN tunnels: ISAKMP/Oakley
- RADIUS:
  - υπεύθυνο για πιστοποίηση ταυτότητας και χρέωση. Διατηρεί μία βάση δεδομένων για κάθε χρήστη, περιέχοντας πληροφορίες όπως passwords (για πιστοποίηση ταυτότητας), δικαιώματα πρόσβασης και ποσοστό χρήσης δικτύου (για χρέωση).
  - Όταν ένας απομακρυσμένος χρήστης θέλει να συνδεθεί στο VPN, το δίκτυο ρωτά το RADIUS σχετικά με το αν ο χρήστης έχει δικαίωμα.

Δομικά στοιχεία VPN – Πύλες ασφαλείας

- Υπάγονται σε 4 κατηγορίες:
  - Δρομολογητές (routers)
    - Κάνουν κρυπτογράφηση των πακέτων που λαμβάνουν και προωθούν. Δύο είδη υπάρχουν στο εμπόριο: με add-on software ή με ξεχωριστό κύκλωμα για την κρυπτογράφηση (το τελευταίο χρησιμοποιείται όταν θέλουμε μεγάλη ταχύτητα). Βέβαια, αν πέσει η απόδοση ενός router, πέφτει η απόδοση όλου του VPN.
  - Τοίχοι προστασίας (firewalls)
    - Φιλτράρουν τα δεδομένα, με βάση τη διεύθυνση που αναγράφει το κάθε πακέτο. Σε μεγάλα δίκτυα με πολύ φόρτο, αν τα firewalls πραγματοποιούν κρυπτογράφηση τότε πέφτει η συνολική απόδοση.
  - Integrated VPN hardware
    - Ειδικός εξοπλισμός για να παρέχει tunneling και κρυπτογράφηση. Τα περισσότερα στο εμπόριο είναι για LAN-to-LAN τοπολογίες.
  - VPN software
    - Κατάλληλα για μικρά δίκτυα, χωρίς μεγάλο φόρτο. Επίσης πιο οικονομική λύση.