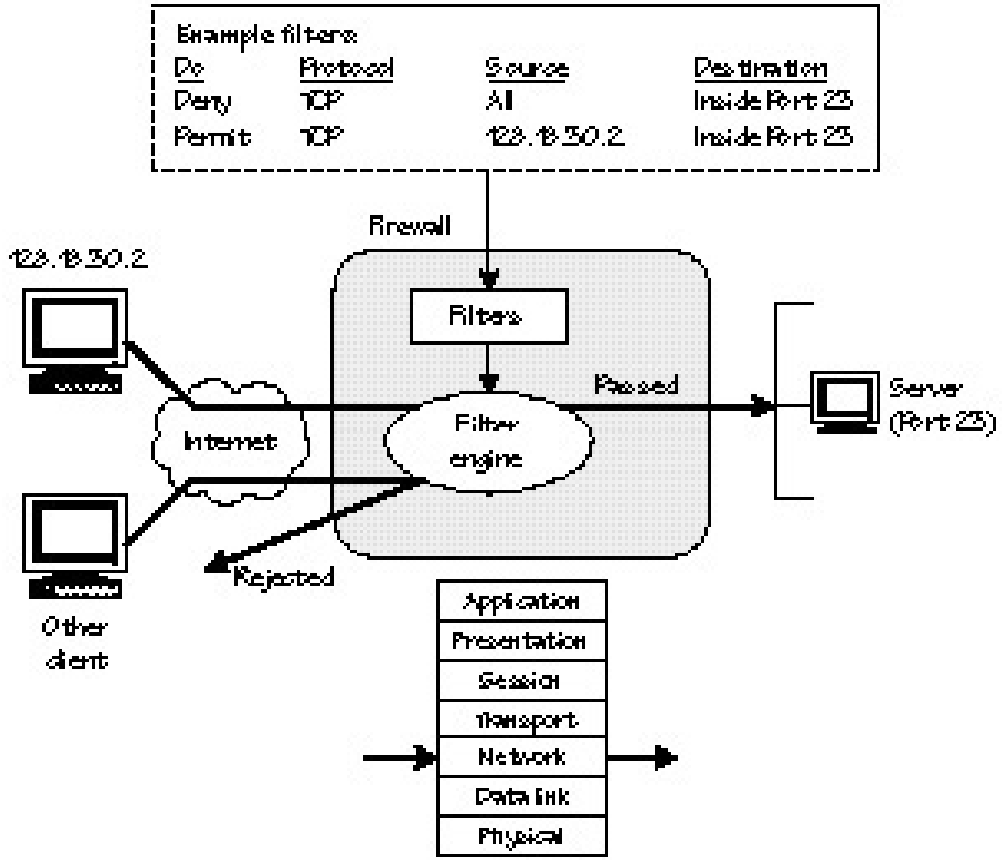
Τοίχοι Ασφαλείας (firewalls)

Γενικά στοιχεία για τους τοίχους ασφαλείας

- Οι τοίχοι ασφαλείας (firewalls) χρησιμοποιούνταν ανέκαθεν για να προστατεύουν τα LANs από εισερχόμενα μη εξουσιοδοτημένα πακέτα. Το φιλτράρισμα αυτό γινόταν με βάση είτε το είδος του πακέτου, είτε το είδος της εφαρμογής είτε της IP διεύθυνσης.
- Υπάρχουν τριών ειδών τοίχοι ασφαλείας:
  - Φίλτρα πακέτων (Packet filters)
  - Πύλες ασφαλείας (security gateways (proxies))
  - Έξυπνα φίλτρα (Smart filters ή stateful inspections firewalls)

Packet filters

- Εξετάζουν στα εισερχόμενα πακέτα τις IP διευθύνσεις πηγής και προορισμού και επιτρέπουν διέλευση, με βάση κάποιους κανόνες που έχει θέσει ο διαχειριστής του δικτύου.



Πλεονεκτήματα-Μειονεκτήματα των φίλτρων πακέτων

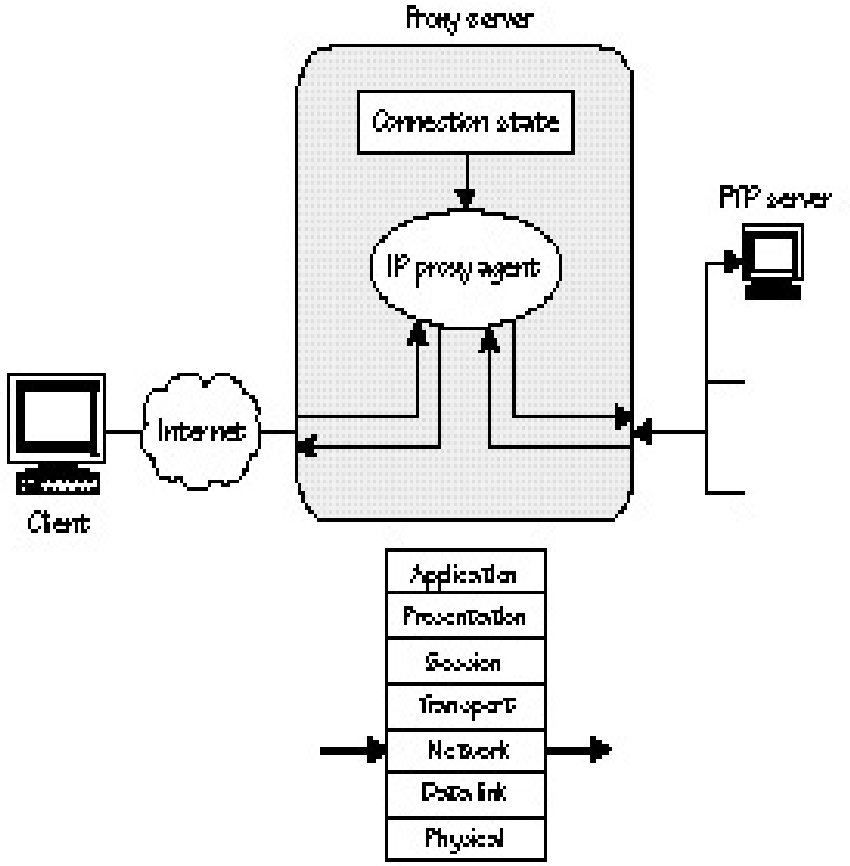
- Εύκολη υλοποίηση
- Είναι «διαφανή» στον χρήστη
- Όμως
  - Γίνονται ολοένα και πιο σύνθετα, όσο οι κανόνες φιλτραρίσματος αυξάνονται
  - Το φιλτράρισμα με βάση την IP διεύθυνση δεν είναι η καλύτερη δυνατή λύση – θα ήταν καλύτερη κάποια πιστοποίηση ταυτότητας του χρήστη που στέλνει τα πακέτα
  - Δεν προστατεύουν από επιθέσεις «man-in-the-middle»
  - Πολλές εφαρμογές δεν έχουν σταθερές IP θύρες στις οποίες στέλνουν πακέτα, έτσι είναι δύσκολο να γίνουν στατικοί κανόνες φιλτραρίσματος

Πύλες ασφαλείας (Application and security gateways (proxies))

- Αυτοί οι τοίχοι ασφαλείας επιτρέπουν στους χρήστες να χρησιμοποιούν έναν proxy για να επικοινωνούν με ασφαλή συστήματα, υποκρύπτοντας τα ασφαλή δεδομένα.
- Ο proxy server δέχεται μία σύνδεση από τη μία πλευρά και, αν η σύνδεση επιτρέπεται, δημιουργεί μια δεύτερη σύνδεση με τον προορισμό από την άλλη πλευρά. Ο χρήστης που ζητά τη σύνδεση δεν συνδέεται ποτέ κατευθείαν με τον προορισμό.
- Ένας Proxy server προκειμένου να εξυπηρετεί διάφορα είδη κίνησης, πρέπει να περιέχει πολλούς *proxy agents.* (όσο πιο πολλά είδη κίνησης πρέπει να εξυπηρετεί, τόσους πιο πολλούς proxy agents χρειάζεται).
- Υπάρχουν οι **circuit proxies** και οι **application proxies**.

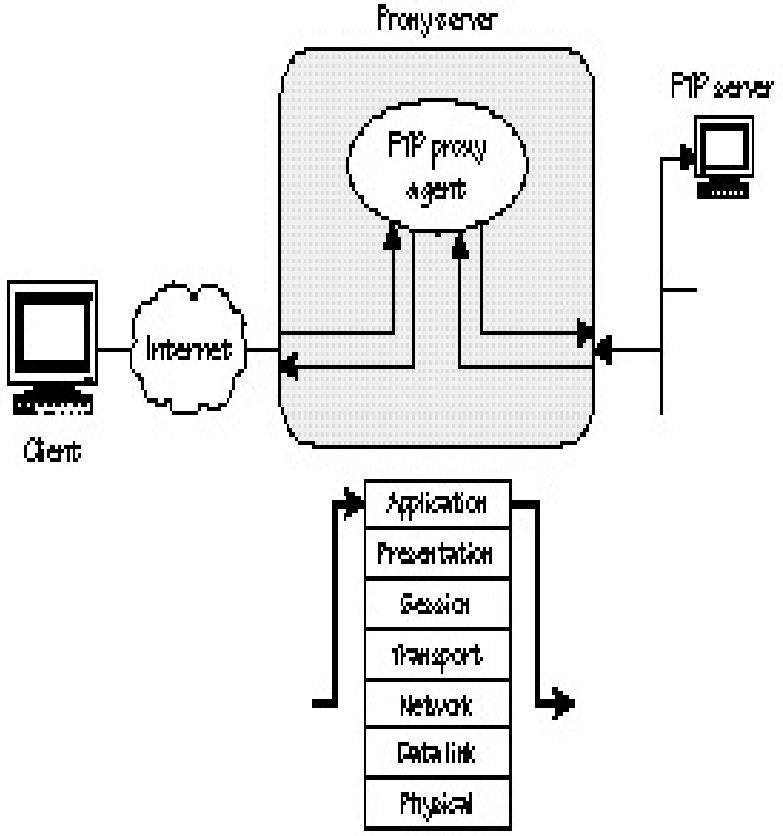
Πού τοποθετείται ένας circuit proxy?

- Ανάμεσα στον δρομολογητή δικτύου (network router) και στο Internet.
- **Οι πραγματικές IP διευθύνσεις δεν μεταδίδονται στο Internet – μόνο η διεύθυνση του proxy.**
- Ένας circuit proxy δεν εξετάζει ποτέ το είδος της εφαρμογής στην οποία υπάγονται τα πακέτα που δέχεται.
- Είναι πιο αργοί από τα φίλτρα πακέτων, γιατί δομούν εκ νέου την IP διεύθυνση κάθε πακέτου. Επίσης δεν είναι διαφανείς προς τον χρήστη (απαιτείται ειδικό λογισμικό στο PC).



Application proxy

- Εξετάζουν όλο το πακέτο (άρα και την εφαρμογή στην οποία ανήκουν). Έτσι αποθαρρύνουν το IP spoofing.
- Χρειάζεται ένας agent για κάθε IP υπηρεσία (π.χ. HTTP, FTP, SMTP κ.α.) για την οποία θέλουμε να ελέγχουμε την πρόσβαση. Άρα για κάθε νέα υπηρεσία υπάρχει πρόβλημα αφού δεν μπορεί να χρησιμοποιηθεί κάποιος υπάρχων agent.
- «Αναγνωρίζουν» χρήστες και εφαρμογές – άρα, η πιστοποίηση ταυτότητας είναι πιο ασφαλής.
- Ωστόσο, είναι πιο αργοί από τους circuit proxies.



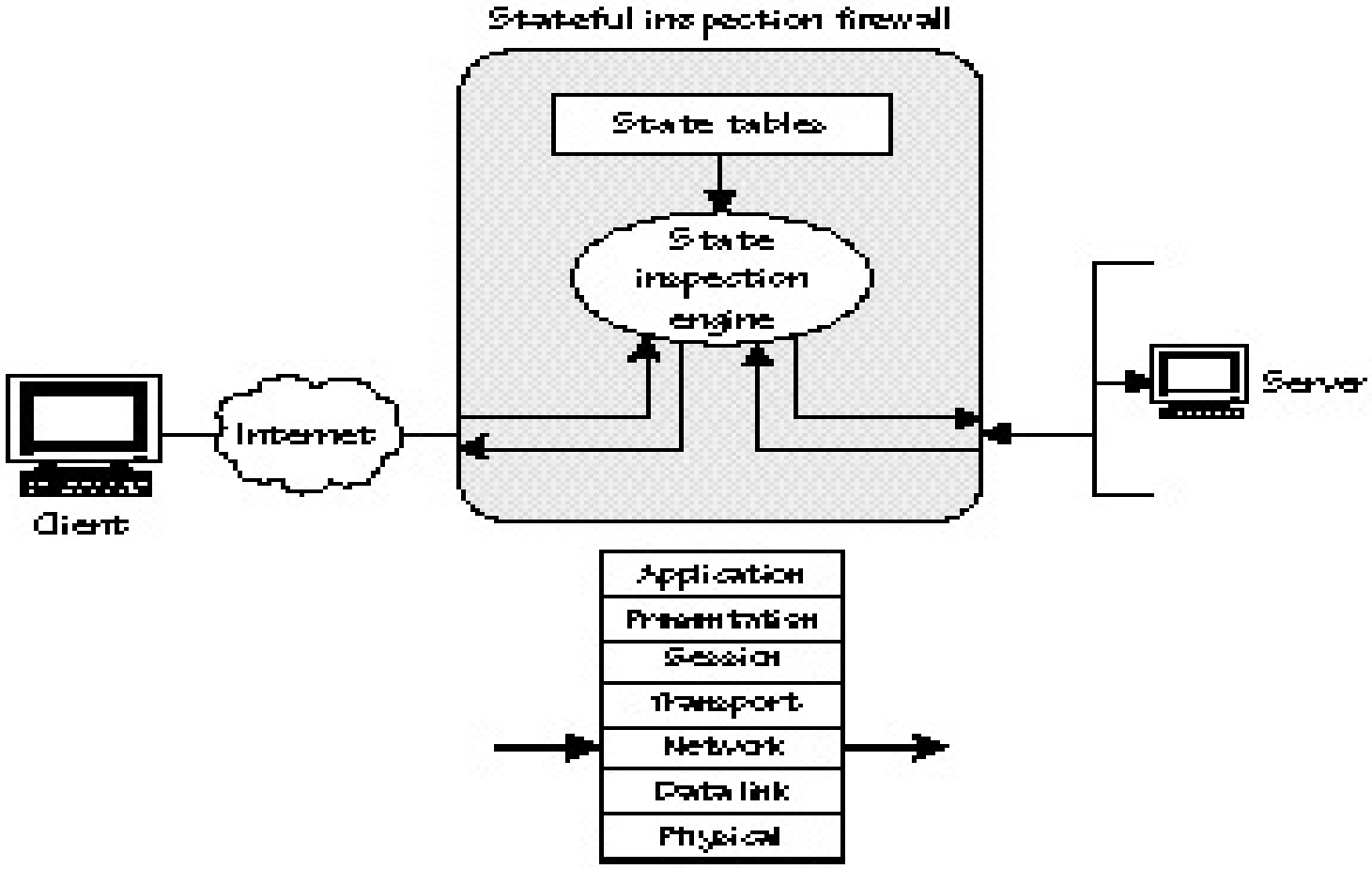
SOCKS

- Πρότυπο για circuit proxies.
- Ένας SOCKS proxy επιτρέπει τη διέλευση μόνο «ειδικών» SOCKS πακέτων, άρα χρειάζεται ειδικό software που να μετατρέπει κάθε πακέτο σε κατάλληλη μορφή.
- Σχεδιασμένο για TCP αλλά και UDP client/server εφαρμογές.

Έξυπνα φίλτρα (Smart filters ή stateful inspections firewalls)

- Stateful Multi-Layer Inspection (SMLI): τεχνική που αναπτύχθηκε για δόμηση τοίχων ασφαλείας μεγίστης δυνατής ασφάλειας και βέλτιστης δυνατής απόδοσης.
- Μοιάζει με τους Application proxies, υπό την έννοια ότι εξετάζει όλο το πακέτο (τις κεφαλίδες όλων των επιπέδων OSI). Χρησιμοποιεί όμως ειδικούς αλγορίθμους (traffic-screening) για να καθορίζει ή μη τη διέλευση των εισερχόμενων πακέτων. Κάθε πακέτο συγκρίνεται με άλλα «φιλικά» πακέτα.

Σχηματική αναπαράσταση του SMLI

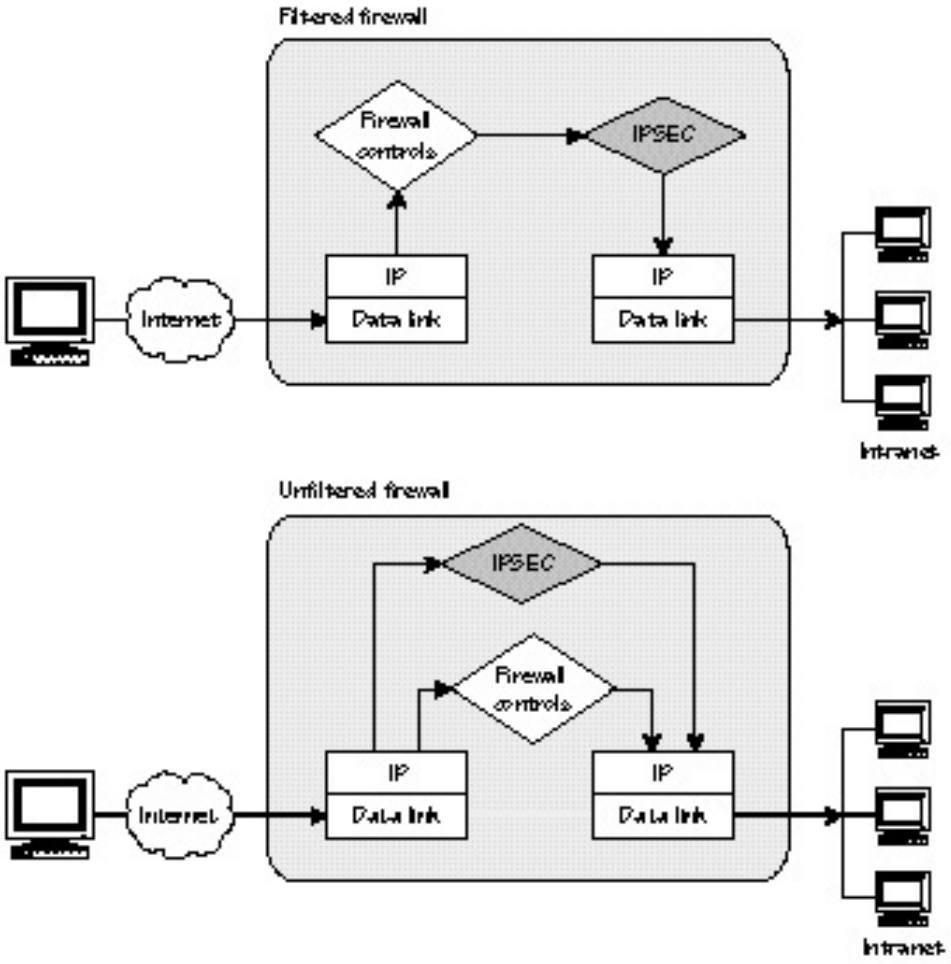


Πλεονεκτήματα του SMLI

- Κλείνει όλες τις TCP θύρες και τις ανοίγει δυναμικά, όταν κάποιες συνδέσεις τις χρειάζονται.
- Επιτρέπει επίσης και UDP φιλτράρισμα.
- Λόγω της μεγάλης ασφάλειας που παρέχουν χρησιμοποιούνται κατά κόρον στα VPN – αν και συνδυάζονται και με proxies, για αυθεντικοποίηση.

Τοίχοι ασφαλείας και Εικονικά Ιδιωτικά Δίκτυα

- Σε IPSec δίκτυα όπου υπάρχει φιλτράρισμα, υπάρχει η δυνατότητα να επιτρέπονται μόνο κάποιες συγκεκριμένες εφαρμογές (π.χ. Email ή ftp).



Κρίσιμα θέματα για την εγκατάσταση firewall σε ένα VPN

- Να μπορεί να υποστηρίζει τους αλγόριθμους κρυπτογράφησης που αναμένεται να χρησιμοποιηθούν από το VPN.
- Ειδικά για IPSec δίκτυα, να υποστηρίζουν όχι μόνο τις κεφαλίδες ESP και AH, αλλά και τον ταυτόχρονο συνδυασμό τους
- Για PPTP δίκτυα, να επιτρέπουν διέλευση από τη θύρα 1723.
- Το λειτουργικό σύστημα έχει κρίσιμο ρόλο – τα firewalls του Unix είναι πιο ασφαλή από των Windows
- Πολλά VPNs έχουν firewalls σαν άκρα της διόδου: αυτό βοηθά πολύ την υλοποίησή τους, αλλά αν «καταρρεύσει» το firewall καταρρέει ολόκληρο το VPN.