Cryptography and Network Security Chapter 22

Fifth Edition

by William Stallings

Chapter 20 – Firewalls

The function of a strong position is to make the forces holding it practically unassailable

***—On War,* Carl Von Clausewitz**

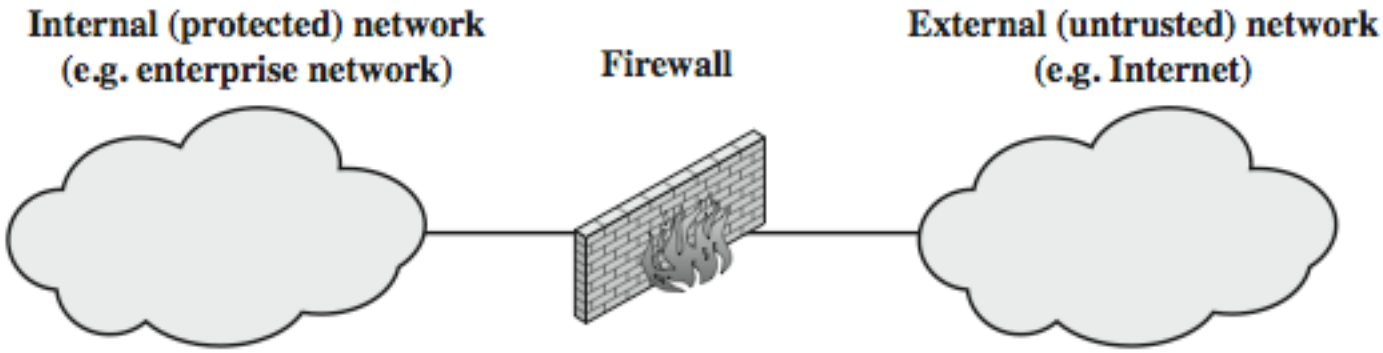
Εισαγωγη

- Σημερα, ο καθενας θελει να ειναι συνδεδεμενος στο Internet
- Αυτο εγειρει σημαντικα θεματα ασφαλειας καθως δεν ειναι ευκολο να ασφαλισει κανεις καθε συστημα σε εναν οργανισμο
- Για την **αμυνα περιμετρου** (perimeter defence) συνηθως χρησιμοποιειται ενα **Firewall**.
- Ως μέρος μιας ευρυτερης στρατηγικης αμυνας

Τι ειναι ενα Firewall?

- Είναι ενα σημειο «στραγγαλισμου» (choke point) για ελεγχο και παρακολουθηση
- Διασυνδεει δικτυα με διαφορετικα επιπεδα εμπιστοσυνης
- Βαζει περιορισμους στης υπηρεσιες του δικτυου
  - Επιτρεπεται η διελευση μονο σε εξουσιοδοτημενο traffic
- Ελεγχει την προσβαση
- Μπορει να υλοποιει και προειδοποιησεις για ανωμαλη συμπεριφορα
- Παρεχει NAT (network address translation) & Παρακολουθηση της χρησης
- Υλοποιει VPNs χρησιμοποιωντας IPSec
- Πρεπει να ειναι ατρωτο σε εισβολες

What is a Firewall?



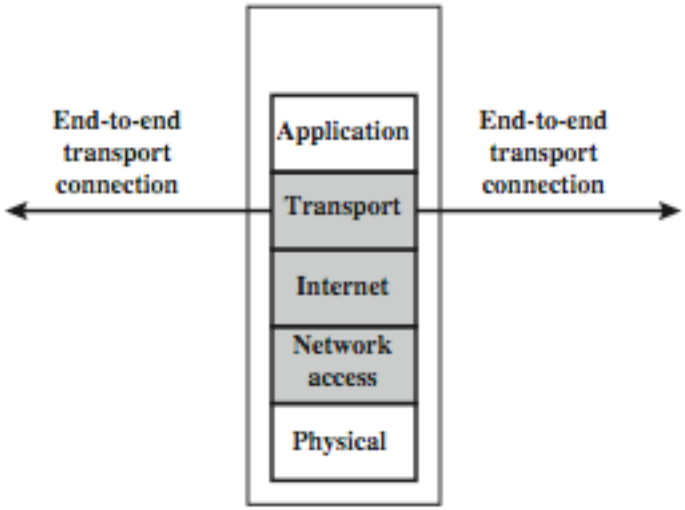
Περιορισμοι των Firewalls

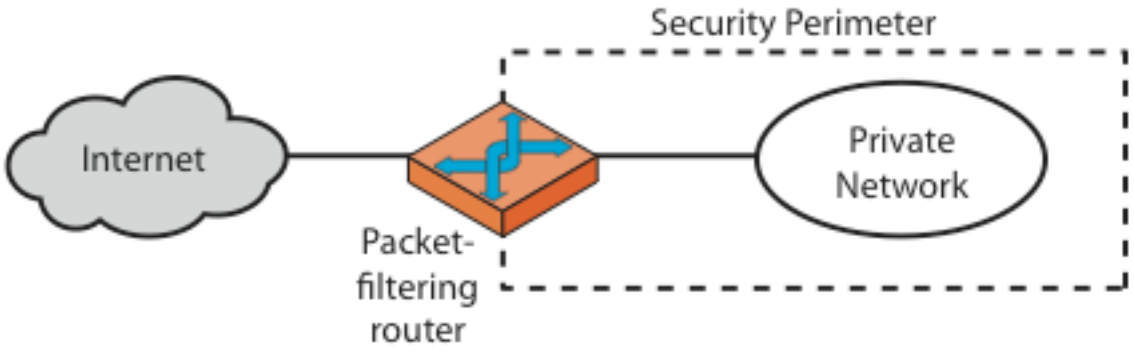
- Δεν προστατευει απο επιθεσεις που το παρακαμπτουν
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- Δεν μπορει να προστατευσει απο εσωτερικες απειλες
  - eg disgruntled or colluding employees
- Δεν προστατευει απο προσβαση μεσω WLAN
  - Αν δεν ειναι σωστα σεταρισμενο για εξωτερικη χρηση
- Δεν προστατει απο κακοβουλο λογισμικο που εχει εισαχθει μεσω laptop, PDA ή αποθηκευτικο μεσο που εχει μολυνθει εξω

Firewalls – Packet Filters

- Το απλουστερο και γρηγοροτερο συστατικο του firewall
- Η βαση καθε συστηματος firewall
- Εξεταζει καθε πακετο IP packet (no context) και επιτρεπει η απαγορευει τη διελευση συμφωνα με κανονες
- Περιοριζει την προσβαση σε υπηρεσιες (σε ports)
- Ειναι δυνατο να τεθουν default πολιτικες
  - Πως οτι δεν επιτρεπεται ρητα, απαγορευεται
  - Πως οτι δεν απαγορευεται ρητα, επιτρεπεται

Firewalls – Packet Filters





(a) Packet-filtering router

Firewalls – Packet Filters

Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Επιθεσεις σε Φιλτρα Πακετων

- IP address spoofing
  - Χρηση ψευτικης εμπιστης διευθυνσης πηγης
  - Για να τις μπλοκαρουμε προσθετουμε φιλτρα στον router
- source routing attacks
  - Ο επιτιθεμενος βαζει ενα δρομολογιο διαφορετικο απο το κανονικο
  - Για να τις αντιμετωπισουμε, μπλοκαρουμε τα source routed πακετα
- tiny fragment attacks
  - Τεμαχιζεται η πληροφορια του TCP header σε μικροσκοπικα πακετα ετσι ωστε να μην μπορει να αναγνωστει απο το φιλτρο
  - Πρεπει ειτε να απορριπτονται, ειτε να επανασυγκροτουνται πριν απο τον ελεγχο

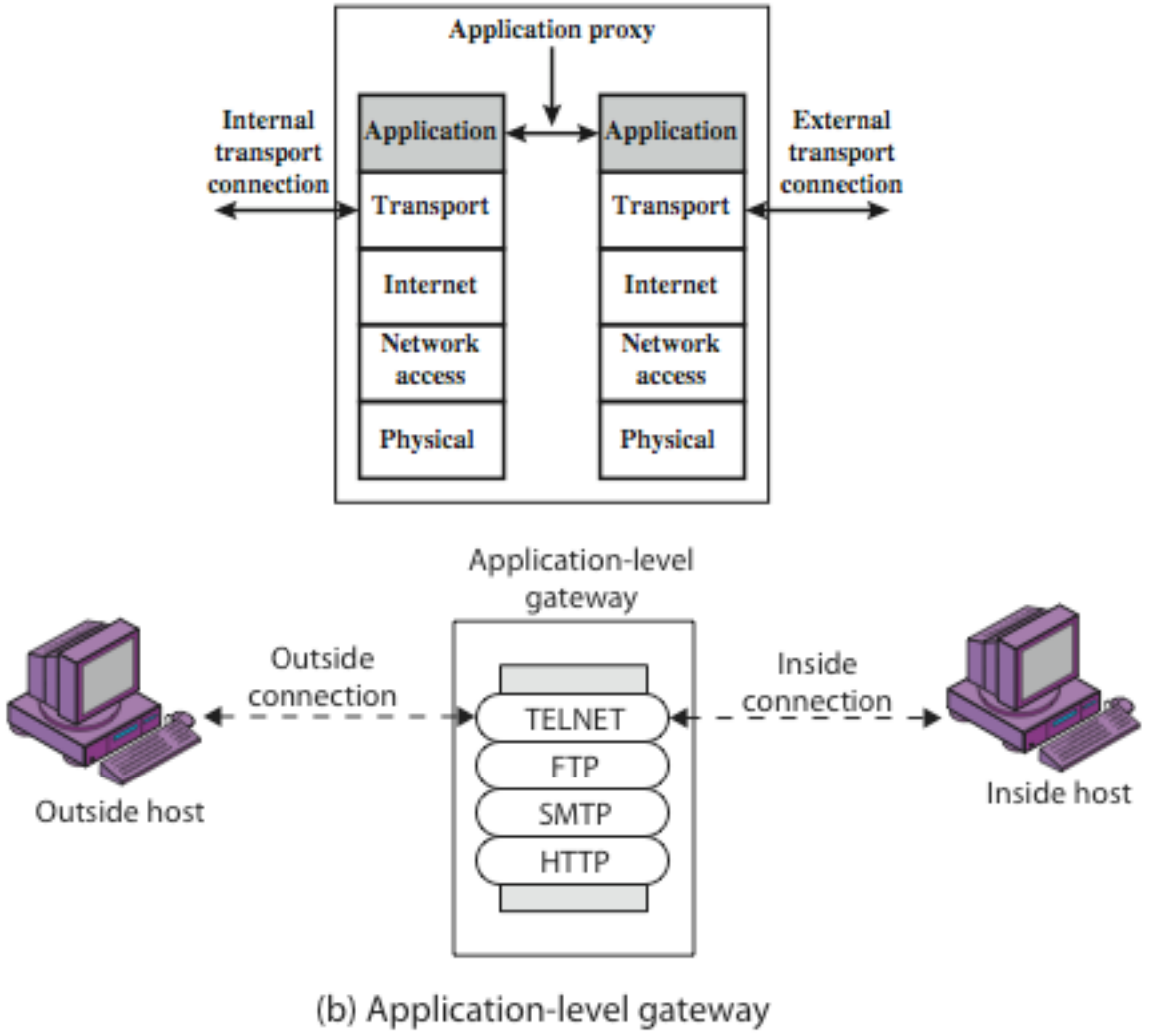
Firewalls – Stateful Packet Filters

- Τα παραδοσιακα φλτρα πακετων δεν εξεταζουν το πακετο στο πλαισιο των ανωτερων επιπεδων.
- Τα stateful packet filters αντιμετωπιζουν αυτην την αναγκη.
- Εξεταζουν καθε πακετο IP packet στο πλαισιο των ανωτερων επιπεδων
  - Καταγραφουν των συνοδων client-server
  - Εξεταζουν τη εγκυροτητα του καθε πακετου να ανηκει σε καποια απο αυτες τις συνοδους
- Ετσι ειναι πιο ευκολο να ανιχνευει κιβδηλα πακετα που δεν ανηκουν στις συνοδους αυτες
- Μπορει ακομη και να ανιχνευει περιορισμενα δεδομενα εφαρμογων

Firewalls - Application Level Gateway (or Proxy)

- Εχει εναν application-specific gateway/proxy
- Εχει πληρη προσβαση στο πρωτοκολλο
  - Ο χρηστης ζητα μια υπηρεσια απο το proxy
  - Το proxy χαρακτηριζει την αιτηση ως νομιμη
  - Στη συνεχεια ενργοποιει την αιτηση και επιστρεφει το αποτελεσμα στο χρηστη
  - Μπορει να καταγραφει ή να ελεγχει το traffic στο επιπεδο εφαρμογης (application level)
- Χρειαζεται ξεχωριστος proxy για καθε υπηρεσια

Firewalls - Application Level Gateway (or Proxy)

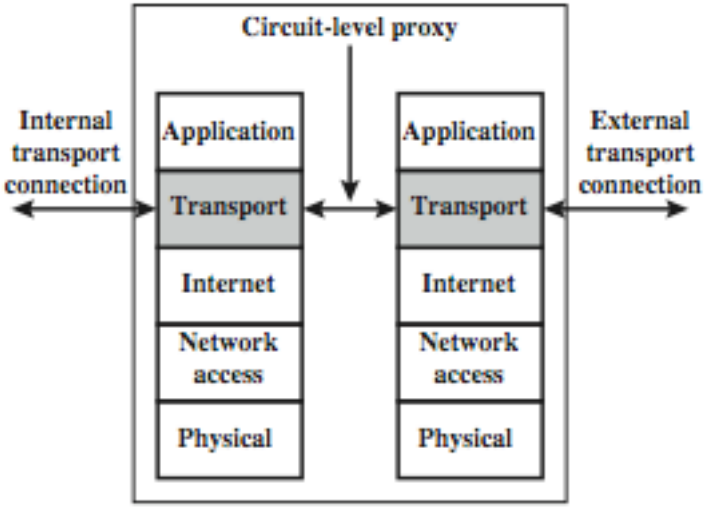


(b) Application-level gateway

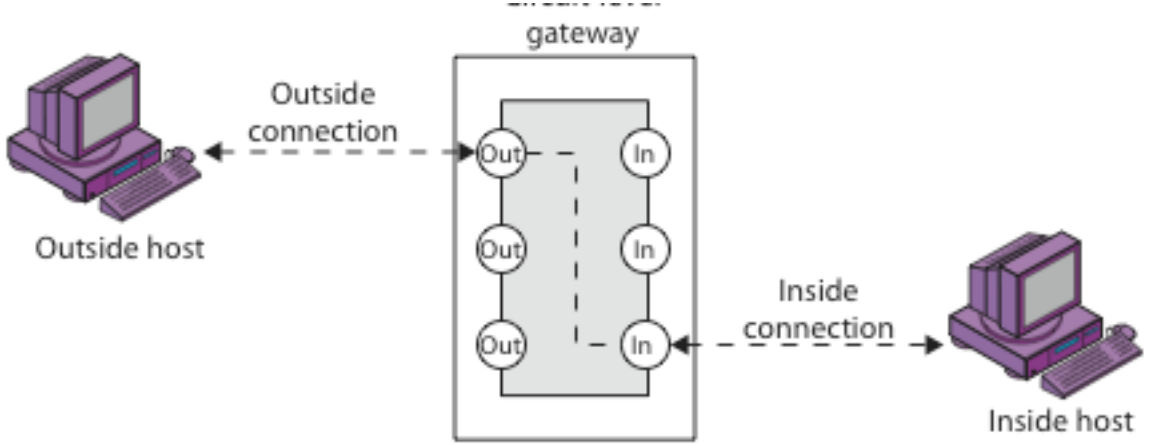
Firewalls - Circuit Level Gateway

- Μεταγει δυο συνδεσεις TCP
- Επιτυγχανει ασφαλεια περιοριζοντας το ποιες συνδεσεις επιτρεπονται
- Αφου δημιουργηθουν, συνηθως μεταγουν την κινηση χωρις να εξεταζουν το περιεχομενο
- Συνηθως χρησιμοποιουνται οταν εμπιστευομαστε τους εσωτερικους χρηστες επιτρεποντας εξερχομενες συνδεσεις
- Συχνα χρησιμοποιειται το πρωτοκολλο SOCKS

Firewalls - Circuit Level Gateway



(e) Circuit-level proxy firewall



(c) Circuit-level gateway

Bastion Host (Υπολογιστης-Οχυρο)

- Ειναι ενα host υψηλης ασφαλειας
- Τρεχει circuit / application level gateways
- ή παρέχει εξωτερικα προσβασιμες υπηρεσιες
- Ειναι εκτεθειμενο σε εχθρικα στοιχεια
- Ειναι συνεπως ασφαλισμενο για να ανταπεξελθει σε αυτο
  - hardened O/S, essential services, extra auth
  - proxies small, secure, independent, non-privileged
- Μπορει να υποστηριζει 2 ή περισσοτερες συνδεσεις δικτυου
- Μπορει να ειναι εμπιστο για να επιβαλει πολιτική εμπιστου διαχωρισμου ματαξυ αυτων των δικτυακων συνδεσεων

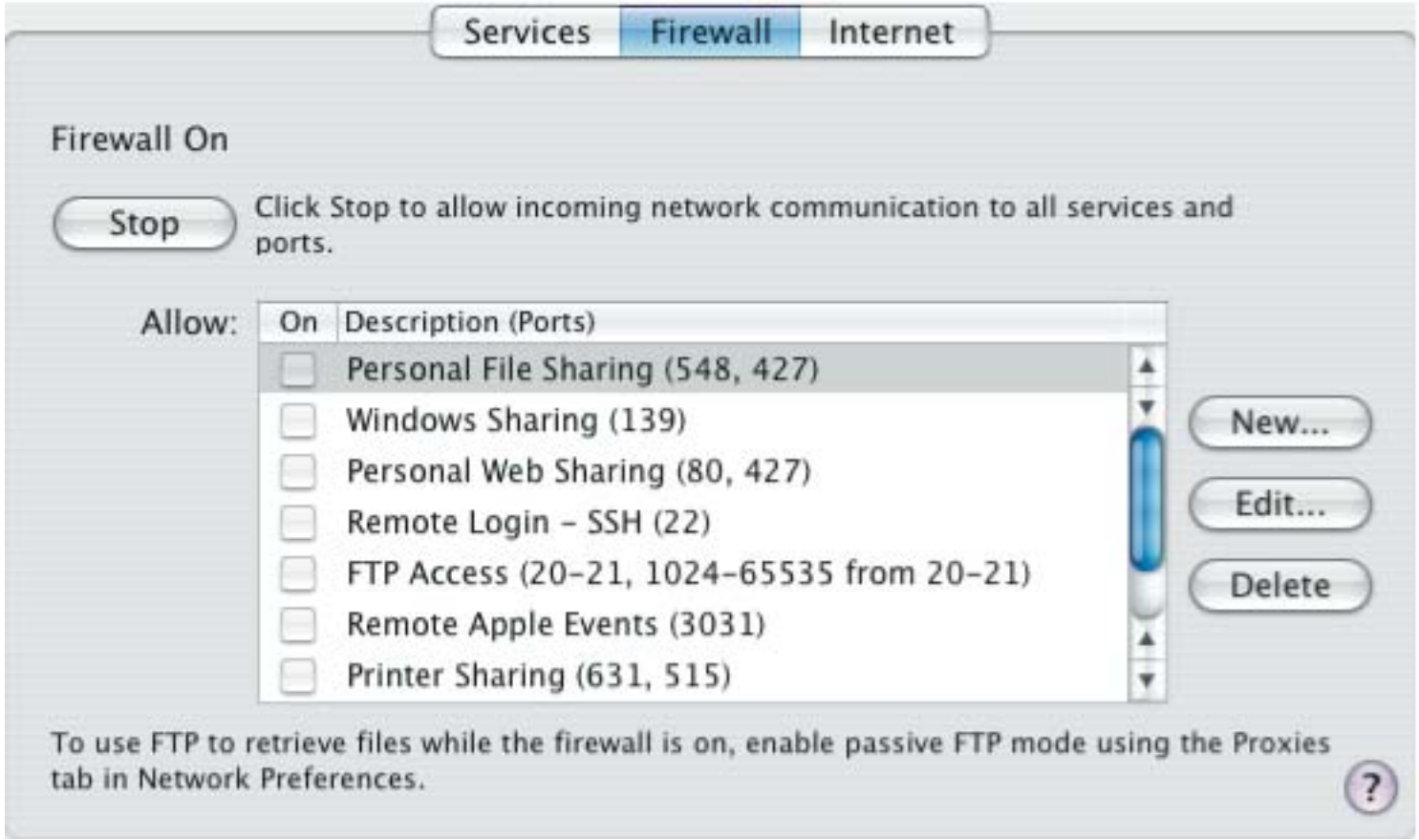
Host-Based Firewalls

- Ειναι ενα s/w module που χρησιμοποιειται για να ασφαλισει συγκεκριμενο host
  - Ειναι διαθεσιμο σε πολλα λειτουργικα συστηματα
  - ή μπορει να παρασχεθει ως add-on
- Χρησιμοποιειται σε servers
- Πλεονεκτηματα:
  - Μπορει να προσαρμοσει τους κανονες φιλτραρισματος στο περιβαλλον του host
  - Η προστασια παρεχεται ανεξαρτητα απο την τοπολογια
  - Παρεχει ενα επιπλεον επιπεδο προστασιας

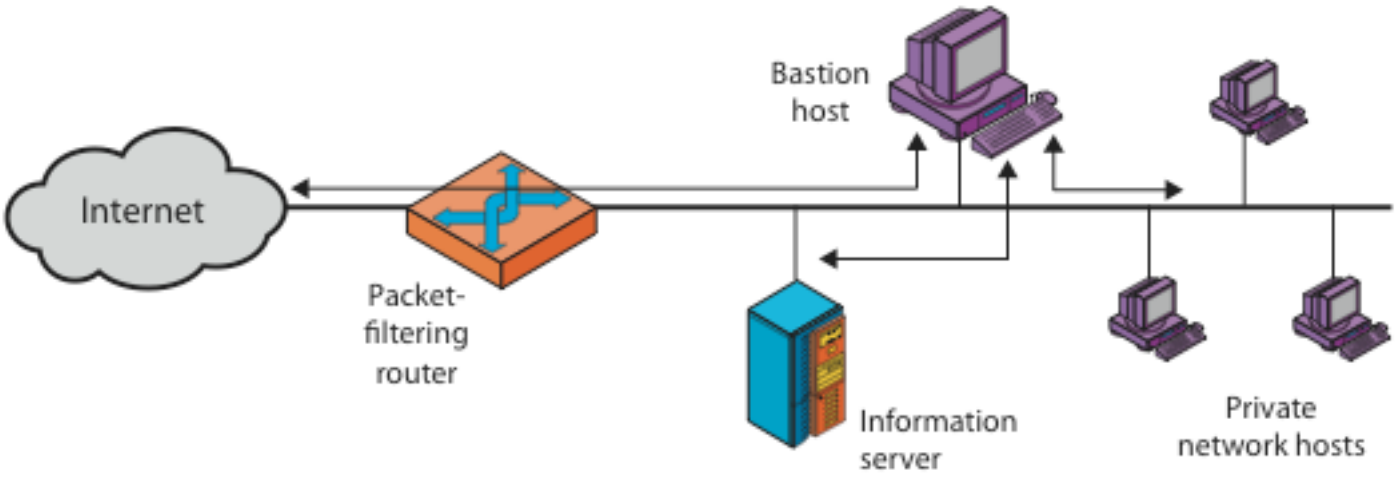
Προσωπικα (Personal) Firewalls

- Ελεγχει το traffic μεταξυ του PC/workstation και του Internet ή του enterprise network
- Ειναι ενα software module στο PC
- ή στο home/office DSL/cable/ISP router
- Συνηθως ειναι πολυ λιγοτερο συνθετο απο αλλους τυπους firewall
- Ο κυριος ρολος τους ειναι να απαγορευουν μη εξουσιοδοτημενη μακρυνη προσβαση στον υπολογιστη
- Και να ελεγχει την εξερχομενη δραστηριοτητα για τυχον κακοβουλο software

Personal Firewalls

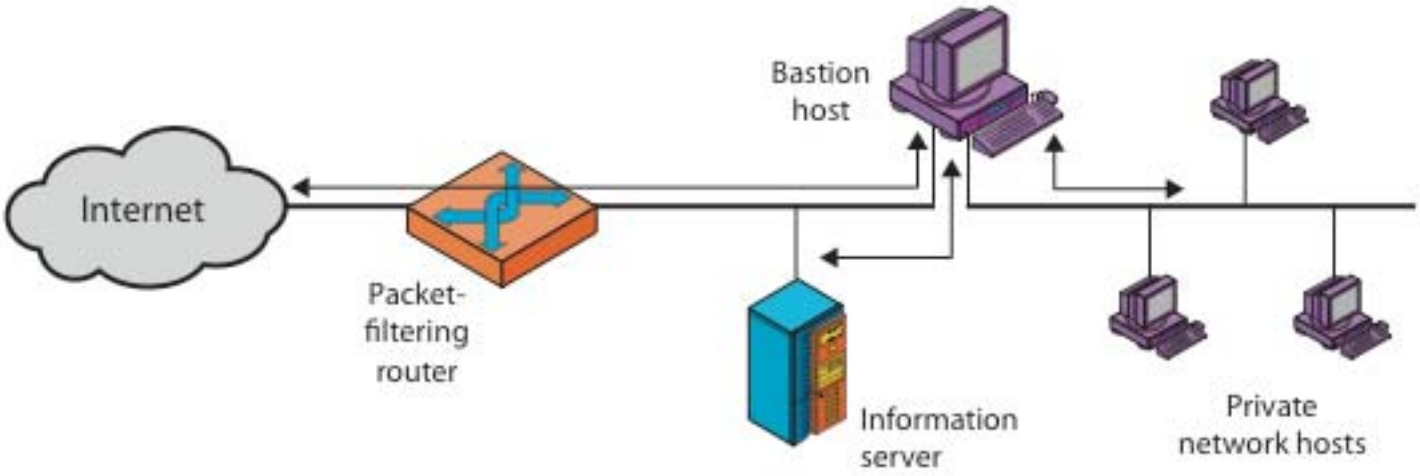


Firewall Configurations



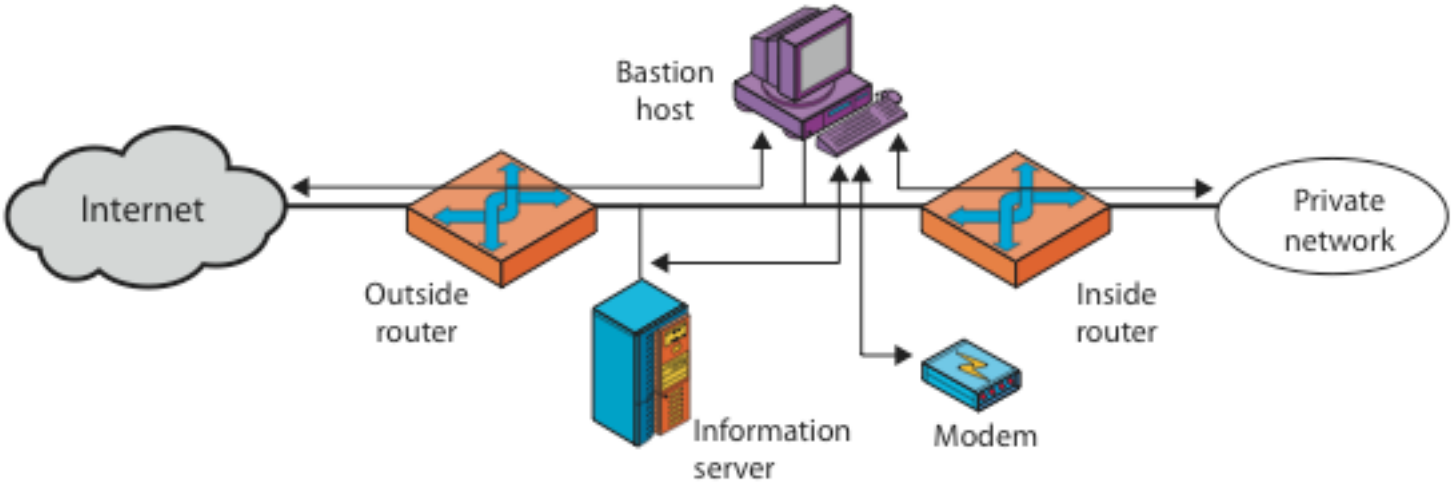
(a) Screened host firewall system (single-homed bastion host)

Firewall Configurations



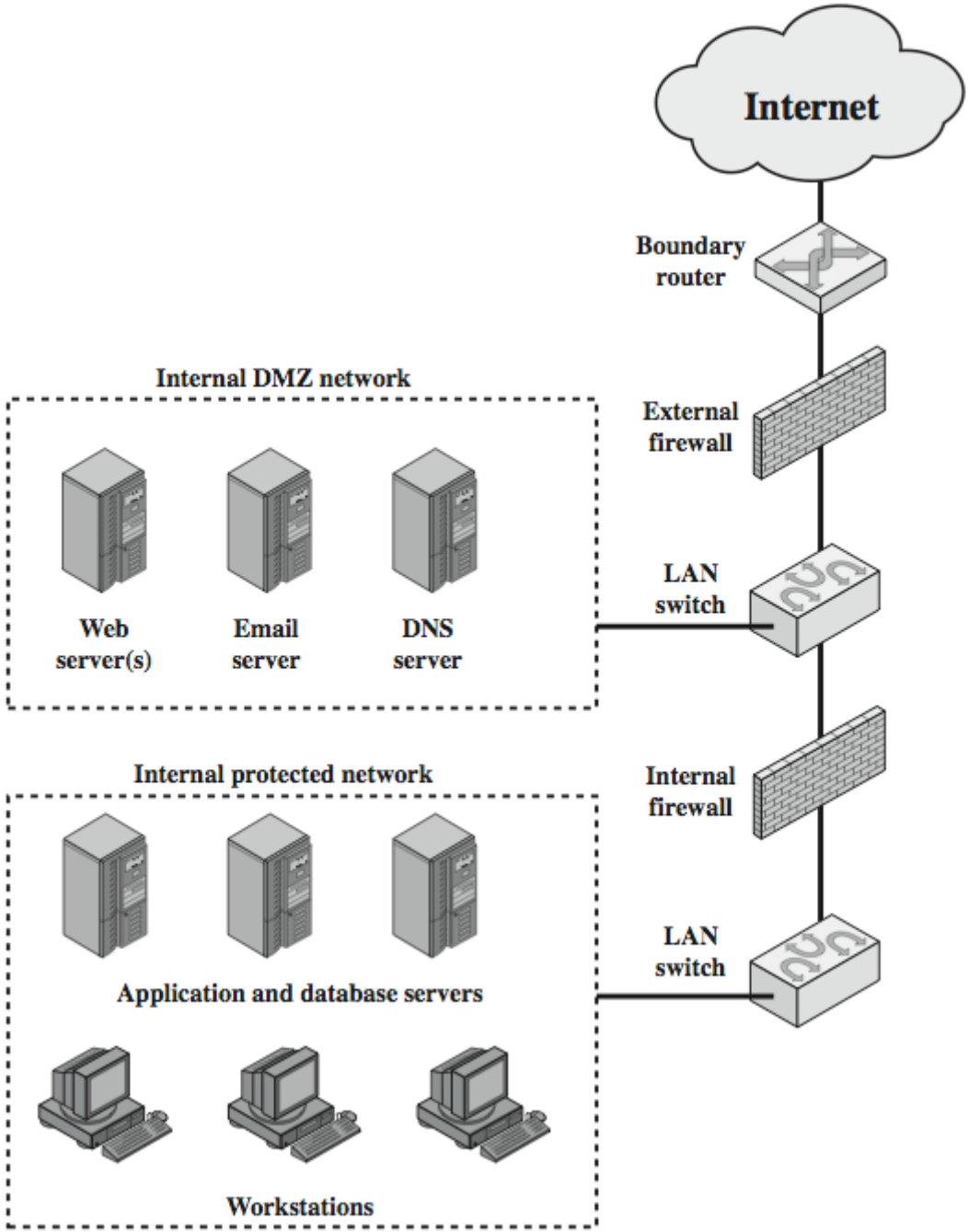
(b) Screened host firewall system (dual-homed bastion host)

Firewall Configurations

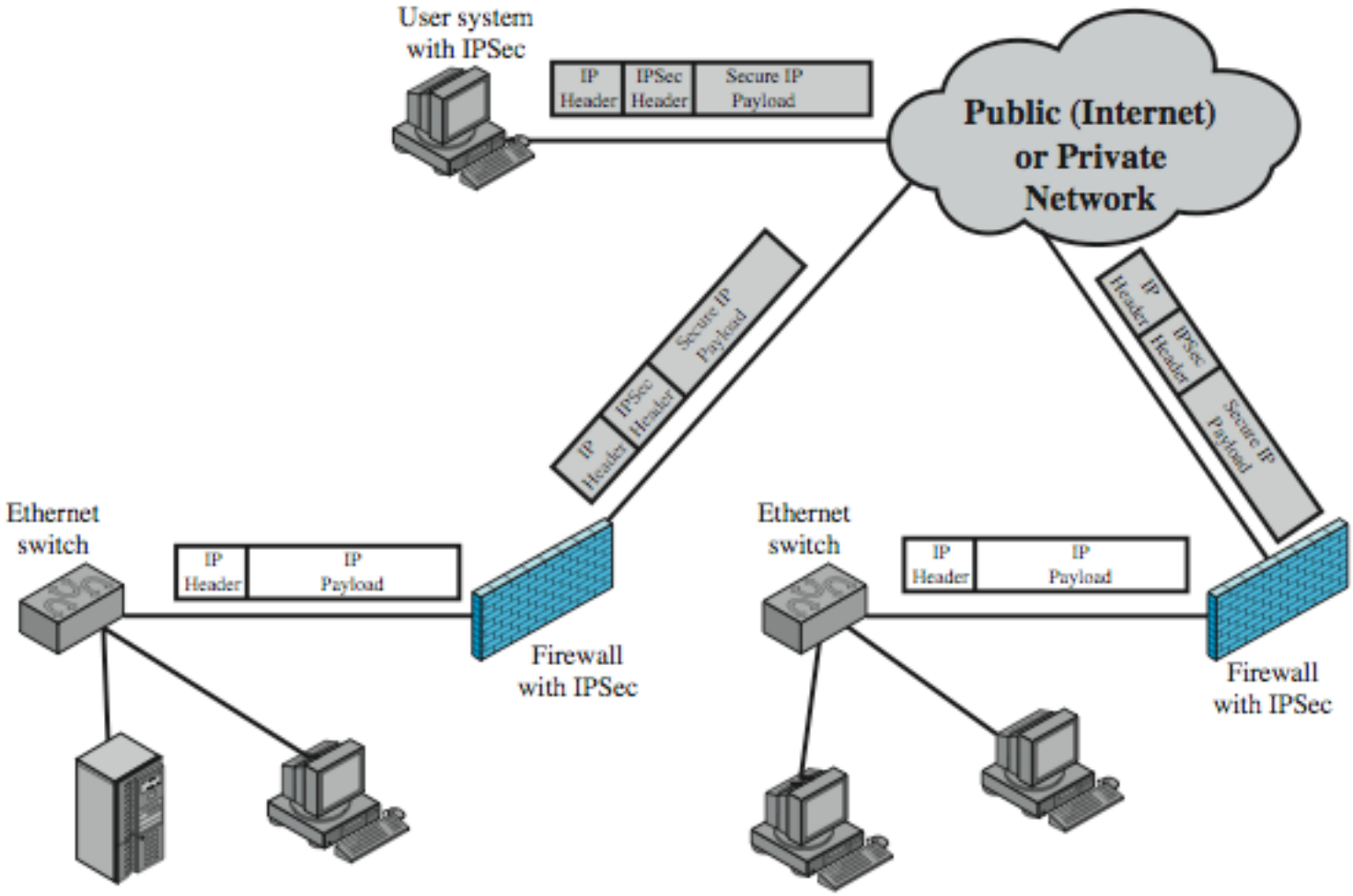


(c) Screened-subnet firewall system

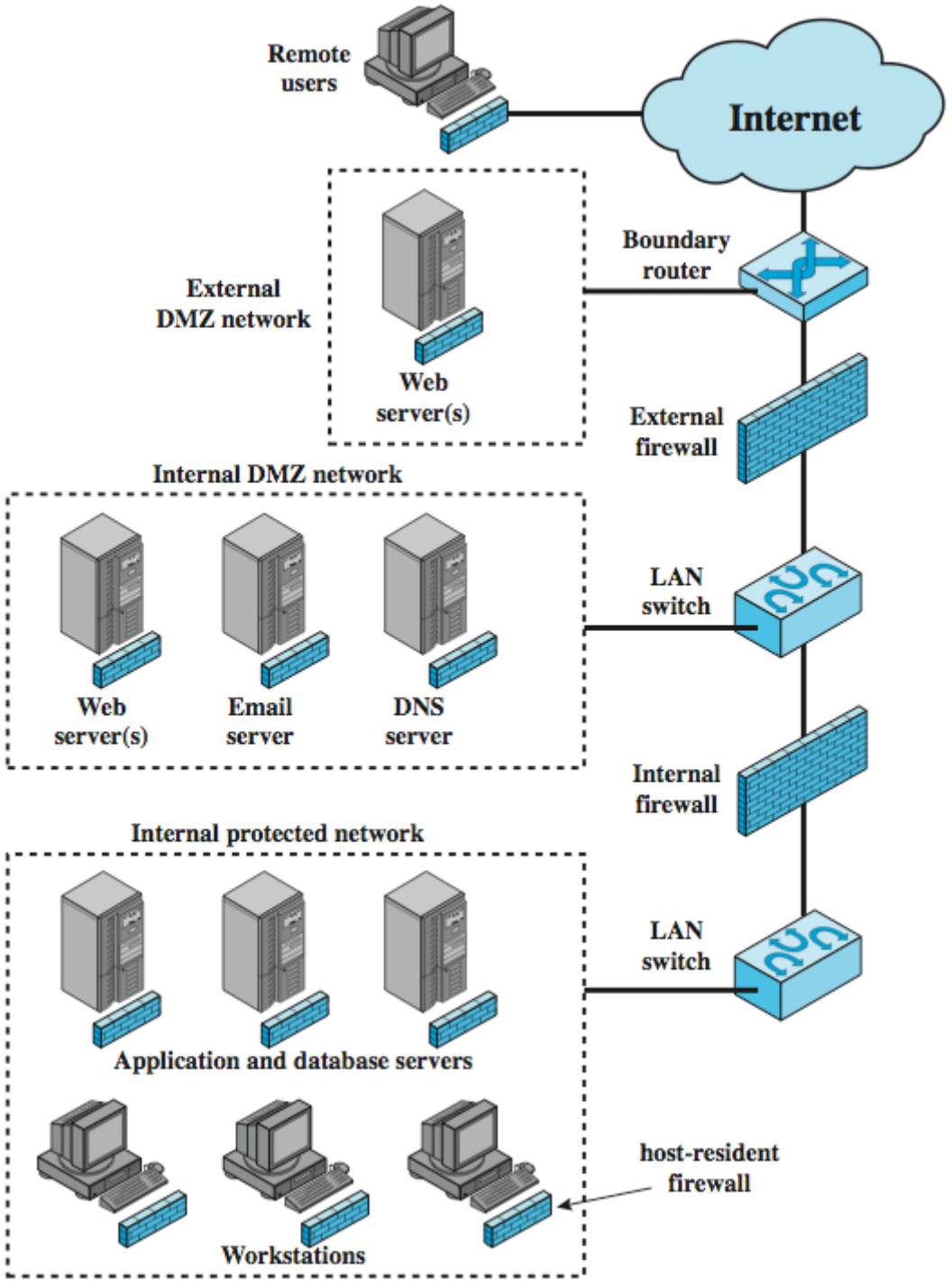
DMZ Networks



Virtual Private Networks



Distributed Firewalls



Περιληψη των Τοποθεσιων και των Τοπολογιων των Firewalls

- host-resident firewall
- screening router
- single bastion inline
- single bastion T
- double bastion inline
- double bastion T
- distributed firewall configuration

Συνοψη

- Εξετασαμε:
  - Τα firewalls
  - Τους τυπους των firewalls
    - packet-filter, stateful inspection, application proxy, circuit-level
  - basing
    - bastion, host, personal
  - Τοποθεσιες και διαμορφωσεις
    - DMZ, VPN, distributed, topologies