Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

Διαχείριση και Ασφάλεια Δικτύων

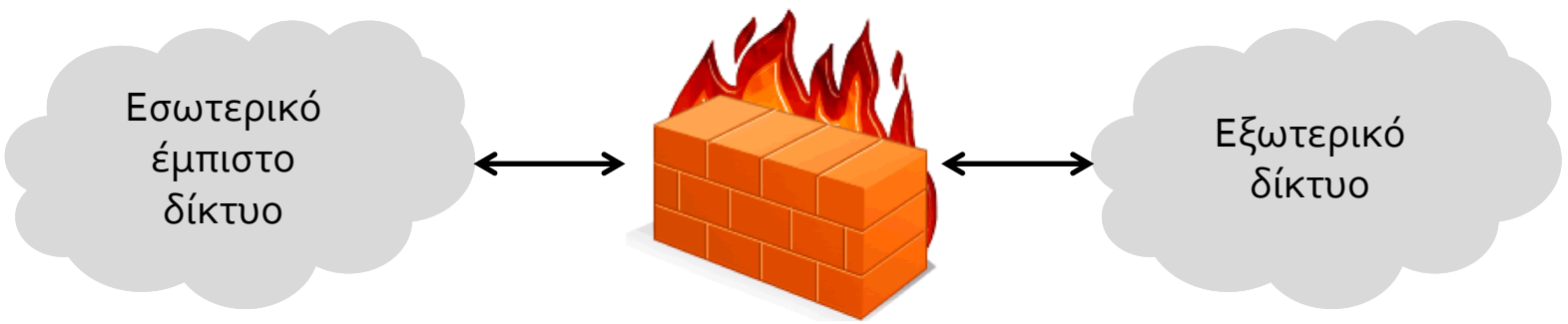
Firewalls

Εισαγωγή

- Firewalls: βασικό συστατικό της "ασφάλειας περιμέτρου" ενός οργανισμού
  - "Οργανισμός": από έναν υπολογιστή μέχρι έναν πάροχο…
- Βασικές σχεδιαστικές αρχές:
  - Όλη η δικτυακή κίνηση, εισερχόμενη και εξερχόμενη, φιλτράρεται από το firewall
  - Το firewall επιτρέπει μόνο σε "εξουσιοδοτημένη" κίνηση να περάσει, βάσει κάποιων κριτηρίων
  - Το firewall αποτελεί "κόκκινο πανί" για επίδοξους εισβολείς
    → απαιτείται ιδιαίτερη προστασία!
- Βασικές τεχνικές:
  - Έλεγχος υπηρεσιών (service control)
  - Έλεγχος κατεύθυνσης (direction control)
  - Έλεγχος χρηστών (user control)
  - Έλεγχος συμπεριφοράς (behavior control)

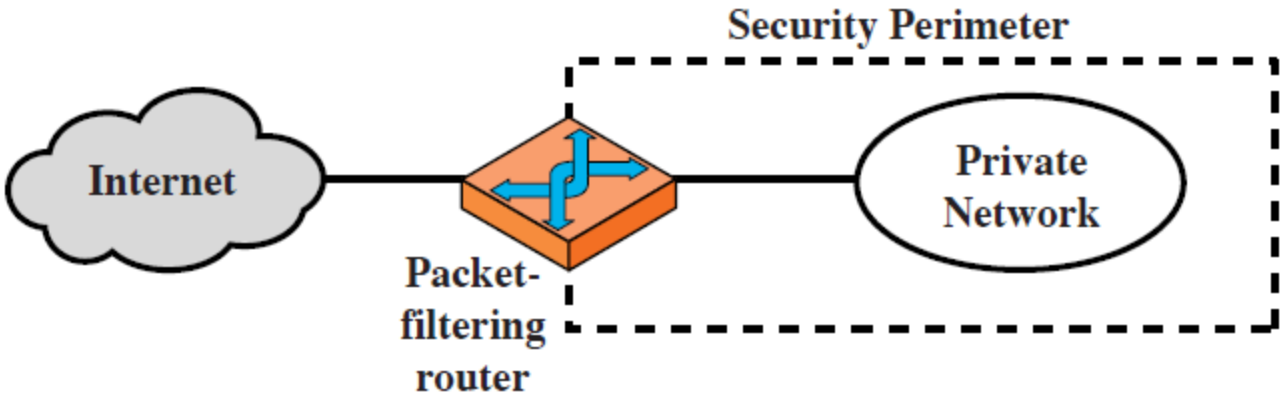
Τυπικές λειτουργίες

- "Σημείο στραγγαλισμού" (choke point), το οποίο παρακολουθεί και ελέγχει τις ροές κίνησης από και προς το υπό προστασία δίκτυο
- Παρακολουθεί συμβάντα σχετικά με την ασφάλεια και σημαίνει συναγερμούς (alarms)
- Ανιχνεύει περίεργες συμπεριφορές και λειτουργεί αποτρεπτικά
- Σημείο τερματισμού για εικονικά ιδιωτικά δίκτυα (VPNs)
- Παρέχει υπηρεσίες όχι άμεσα σχετικές με την ασφάλεια:
  - Μετάφραση δικτυακών διευθύνσεων (NAT)
  - Λειτουργίες διαχείρισης



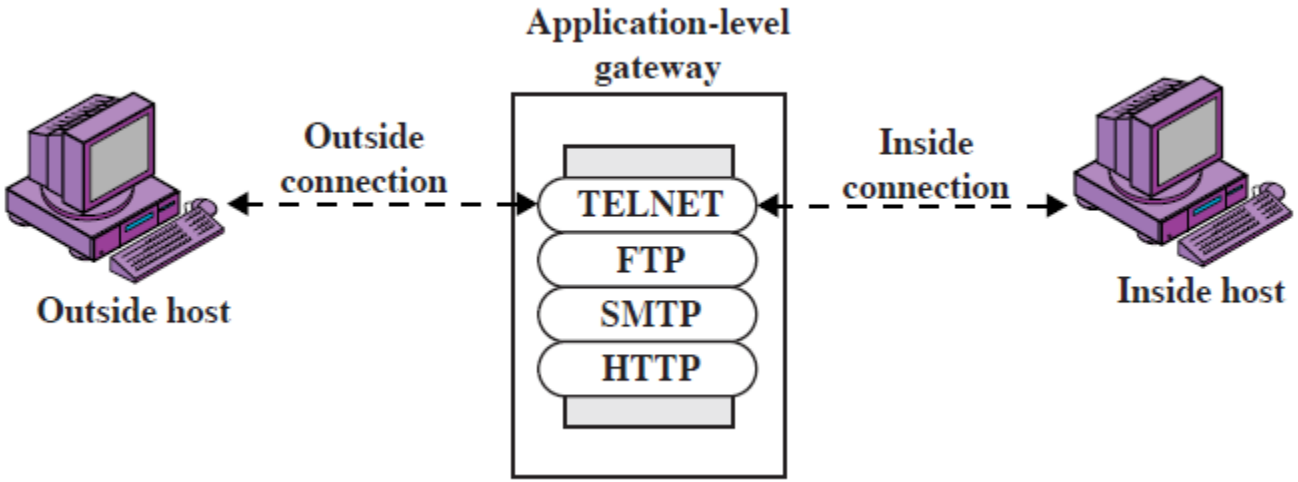
Τύποι Firewalls

Δρομολογητής φιλτραρίσματος πακέτων



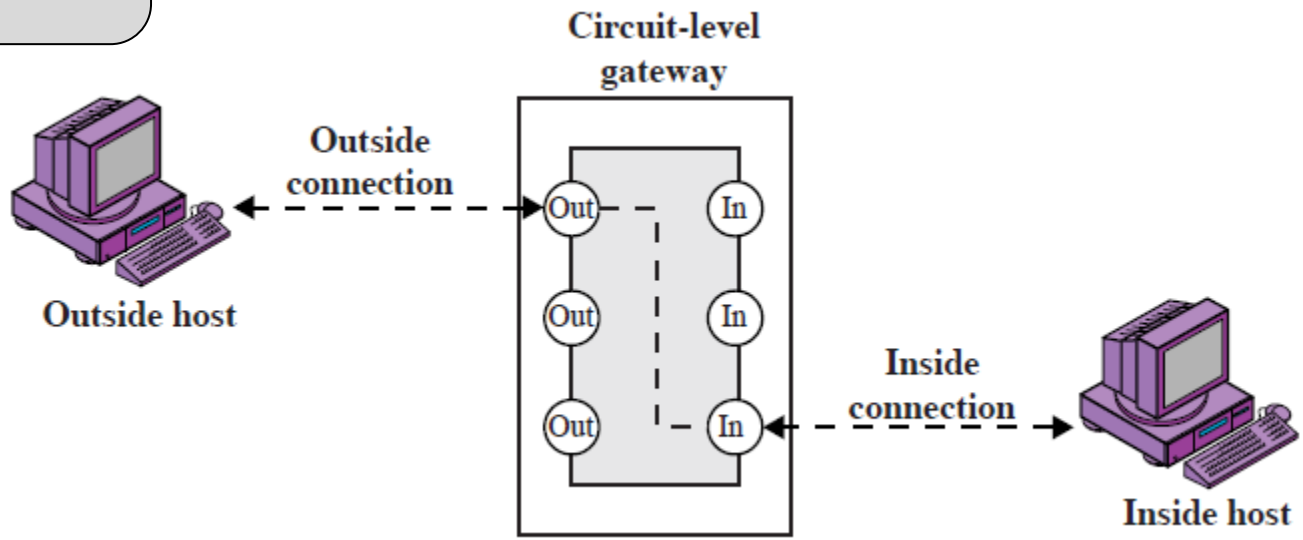
Τύποι Firewalls

Πύλη επιπέδου εφαρμογής



Τύποι Firewalls

Πύλη επιπέδου κυκλώματος



Δρομολογητής φιλτραρίσματος πακέτων

- Η πιο απλή, συνηθισμένη και γρήγορη περίπτωση
- Εφαρμογή κανόνων για εισερχόμενα και εξερχόμενα πακέτα που οδηγούν σε
  - Προώθηση πακέτου
  - Απόρριψη πακέτου
- Οι κανόνες συνήθως βασίζονται σε:
  - IP διεύθυνση αποστολής και προορισμού
  - TCP/UDP πόρτες
  - Πρωτόκολλο
  - Interface
- Default πολιτικές
  - Προεπιλογή προώθησης
  - Προεπιλογή απόρριψης

Παραδείγματα φιλτραρίσματος πακέτων

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

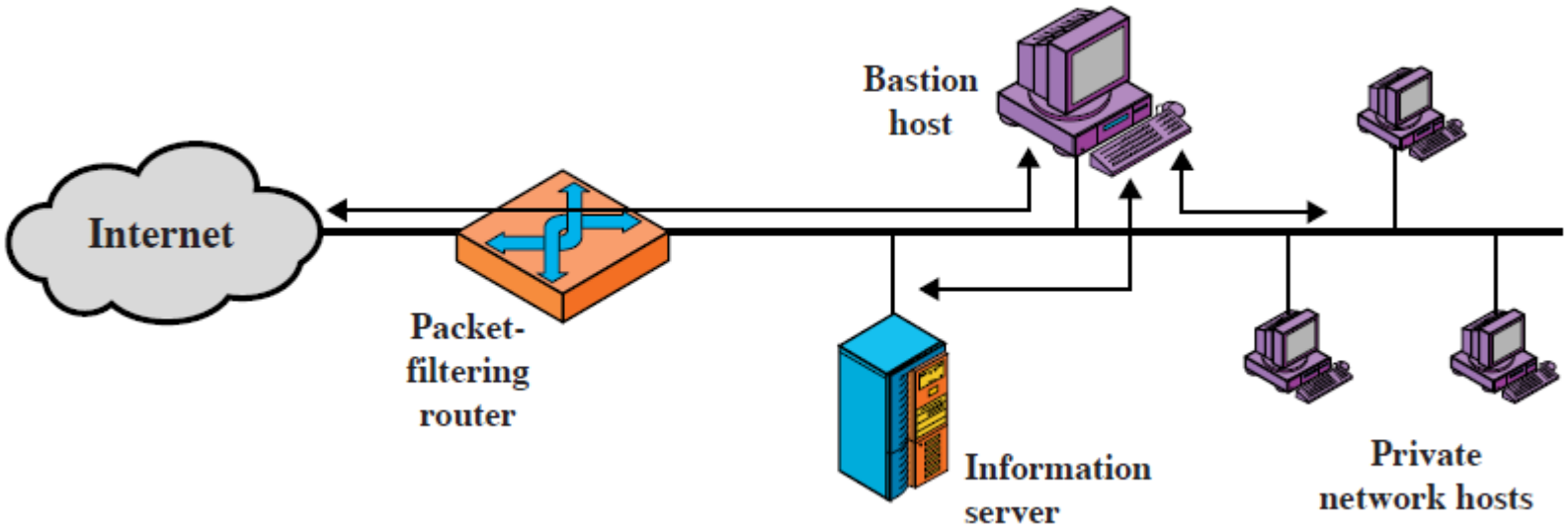
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Επιθέσεις

- Πλαστές IP διευθύνσεις (IP spoofing)
  - Ο επιτιθέμενος πλαστογραφεί την IP διεύθυνση πηγής με στόχο να ξεγελάσει το firewall
  - Αντιμετώπιση: απόρριψη πακέτων που φτάνουν σε εξωτερικό interface αλλά φαίνεται να έχουν εσωτερική διεύθυνση
- Επιθέσεις δρομολόγησης πηγής (source routing)
  - Δρομολόγηση πηγής: τεχνική που επιτρέπει τον καθορισμό των βημάτων δρομολόγησης από τον κόμβο-πηγή
  - Ο επιτιθέμενος ορίζει διαδρομή δρομολόγησης προσπαθώντας να παρακάμψει μέτρα ασφάλειας
  - Αντιμετώπιση: απόρριψη όλων των πακέτων με επιλεγμένη τη δρομολόγηση πηγής

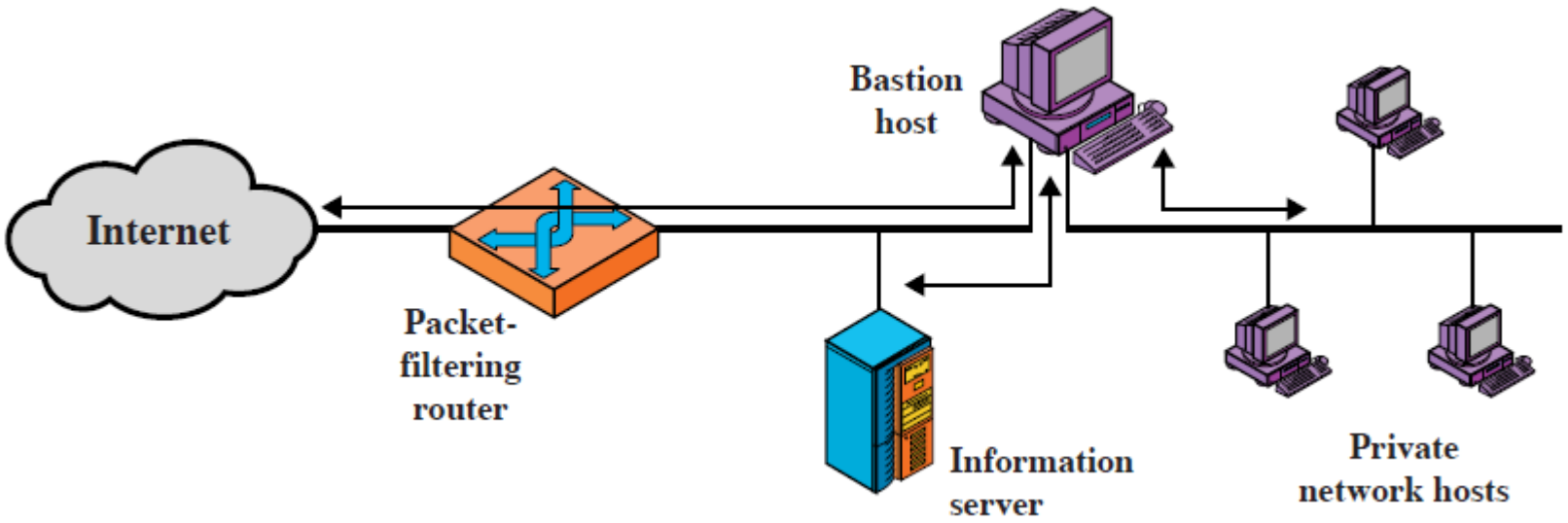
Συνδεσμολογίες

Screened host firewall system (single-homed bastion host)



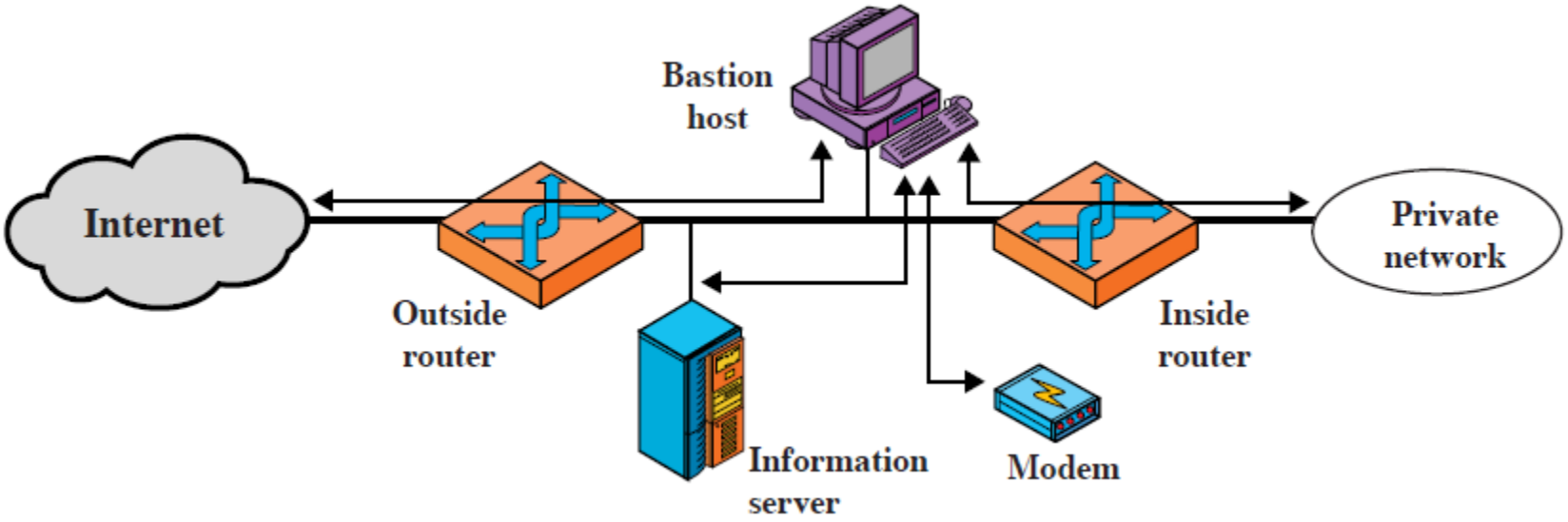
Συνδεσμολογίες

Screened host firewall system (dual-homed bastion host)



Συνδεσμολογίες

Screened-subnet firewall system



Παράδειγμα αρχιτεκτονικής