

# Τείχη ασφαλείας και αρχιτεκτονικές

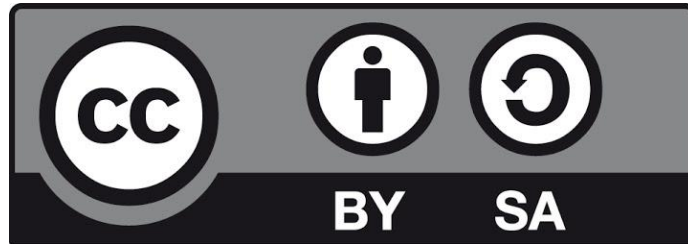
---

Εισηγητής: Χρήστος Δαλαμάγκας

[cdalamagkas@gmail.com](mailto:cdalamagkas@gmail.com)

# Άδεια χρήσης

Το παρόν εκπαιδευτικό υλικό υπόκειται στη διεθνή άδεια χρήσης Creative Commons Attribution-ShareAlike 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).



# Ορισμός

- **Τείχος ασφαλείας** (firewall): Λογισμικό που υλοποιεί κανόνες πολιτικής ασφαλείας μεταξύ δυο δικτύων – μπλοκάρει πακέτα με βάση κάποια κριτήρια
- Βασικό μέτρο ασφαλείας, αλλά όχι το μοναδικό!
- Θεμελιώδους λειτουργίας: αποδοχή ή απόρριψη ενός πακέτου με βάση τα χαρακτηριστικά του
- Καταγραφή επιτρεπόμενων ή μη συμβάντων
- Προστασία συστημάτων από ανεπιθύμητη πρόσβαση

# Περιορισμοί τειχών ασφαλείας

- Δεν ελέγχουν την κίνηση που συμβαίνει «πίσω» από το τείχος.
- Δεν προστατεύουν από κακόβουλο λογισμικό.
- Δεν προστατεύουν από επιθέσεις εκ των έσω.
- Δεν προστατεύουν από άγνωστες απειλές
- Προβλήματα λόγω αυστηρών ρυθμίσεων - Άρνηση παροχής υπηρεσιών
- Εισαγωγή πρόσθετης καθυστέρησης
- Αναστάτωση χρηστών

# Ζητήματα σχεδίασης

- **Χρηστικότητα:** συμβιβασμός μεταξύ ασφάλειας και χρηστικότητας
- **Εκτίμηση κινδύνου:** Υλοποίηση ζωνών διαφορετικού κινδύνου
- **Εκτίμηση απειλών:** Καθορισμός ή εκτίμηση των απειλών που μπορεί να δεχθεί μια δικτυακή οντότητα
- **Εκτίμηση κόστους:** σχετικά με την υλοποίηση και υποστήριξη του συστήματος
- **Τύπος:** επιλογή του πιο κατάλληλου τύπου τείχους ασφαλείας

# Είδη τειχών ασφαλείας

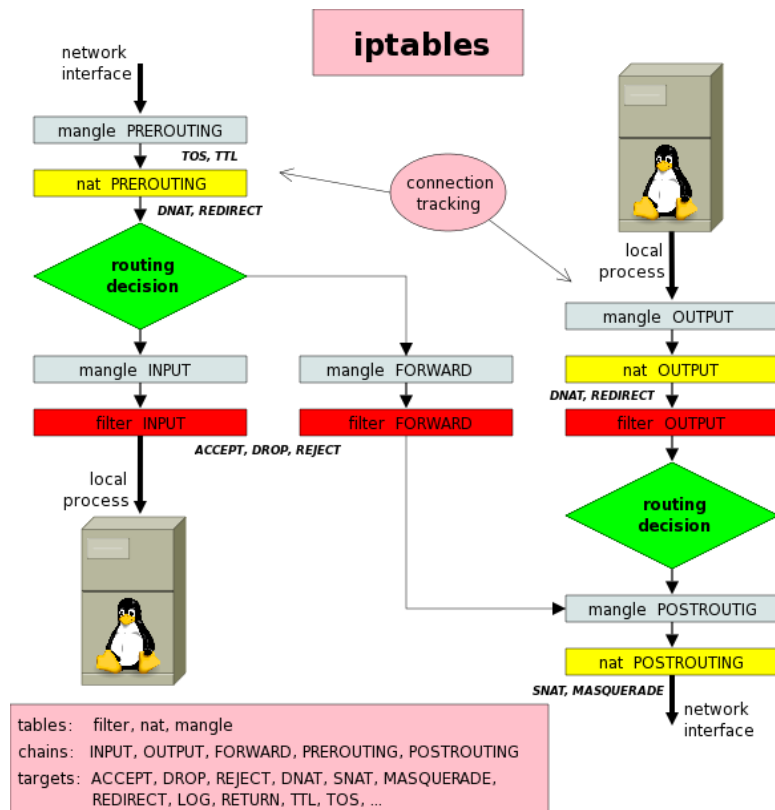
---

# TA με φιλτράρισμα πακέτων

- Φιλτράρει με βάση πληροφορίες του στρώματος δικτύου και του μεταφοράς (διεύθυνση IP, θύρα TCP/UDP)
- Πιο απλή περίπτωση TA δικτύου: δρομολογητής
- Ένα TA δικτύου εφαρμόζει ταυτόχρονα πολλές πολιτικές ασφαλείας
- Δρομολογητής αποκαλείται και ως packet filter
- Παραδείγματα
  - Εμπόδισε πακέτα με διεύθυνση προορισμού 84.32.10.4
  - Απόρριψε τα πακέτα που προέρχονται από το δίκτυο 54.76.12.0/12 και προορίζονται στο 54.21.54.0/24

# ΤΑ κατασταστικής επιθεώρησης (stateful packet inspection)

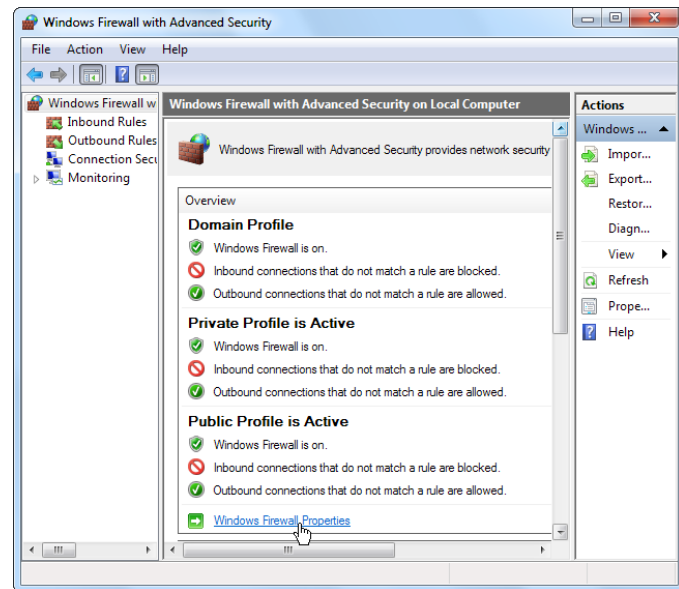
- Εξετάζουν όλες τις πληροφορίες του επιπέδου δικτύου συν την κατάσταση της σύνδεσης TCP
- Κρατούν αρχείο με την κατάσταση των συνεδριών TCP
  - Κανόνες ενδέχεται να εφαρμόζονται με βάση το sequence number ή σε μια συγκεκριμένη συνεδρία TCP
- Παραδείγματα τειχών SPI:
  - iptables
  - pf





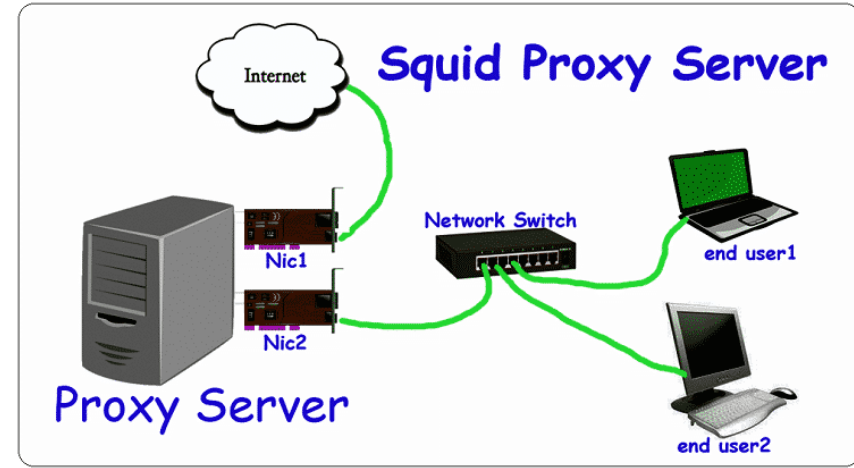
# ΤΑ στρώματος εφαρμογών

- Λογισμικό που ελέγχει τα πακέτα μέχρι και το επίπεδο εφαρμογών
  - Πχ με βάση το URL ή με βάση το περιεχόμενο ενός ερωτήματος DNS
- Υλοποιείται ως εφαρμογή και εκτελείται σε έναν εξυπηρετητή
- Μπορεί να μπλοκάρει πλήρως ή εν μέρει την πρόσβαση σε συγκεκριμένες εφαρμογές ή προγράμματα
- Παραδείγματα
  - Windows Firewall
  - Πληρεξούσιοι - Proxies



# Πληρεξούσιος (proxy)

- Ειδική κατηγορία τειχών ασφαλείας στρώματος εφαρμογών
- Φιλτράρει τα πακέτα των χρηστών ενός τοπικού δικτύου με βάση διάφορα κριτήρια
- Η υπηρεσία λαμβάνει αιτήματα ειπέδου εφαρμογών από τους χρήστες και τα διεκπεραιώνει για λογαριασμό τους
- Σε ένα δίκτυο με πληρεξούσιο, όλοι οι υπολογιστές εξυπηρετούν την κίνησή τους μέσω του πληρεξούσιου
- Ο πληρεξούσιος διεκπεραιώνει τα αιτήματα των χρηστών με τη δική του IP



# Τοπολογίες

---

# Ορολογία

- **Περιμετρικό δίκτυο:** Πρόσθετο δίκτυο που τοποθετείται μεταξύ του εξωτερικού δικτύου και του εσωτερικού (ιδιωτικού, προστατευμένου) δικτύου
  - Τα δίκτυα αυτά αποκαλούνται και Demilitarized Zones (DMZ)
  - Διαθέτουν ελάχιστη ασφάλεια και εκθέτουν τις συσκευές που βρίσκονται σε αυτό απευθείας στο Διαδίκτυο
- **Υπολογιστής – Έπαλξη (bastion host):** Ο υπολογιστής/πληρεξούσιος στον οποίον πηγαίνει η κίνηση των χρηστών, πριν βγει στο Διαδίκτυο
- **Honeypot:** Υπολογιστής που προσομοιώνει μια συσκευή ή υπηρεσία και σκοπεύει στο να προσελκύσει και να καταγράψει στοιχεία επιτιθέμενων

# Ορολογία

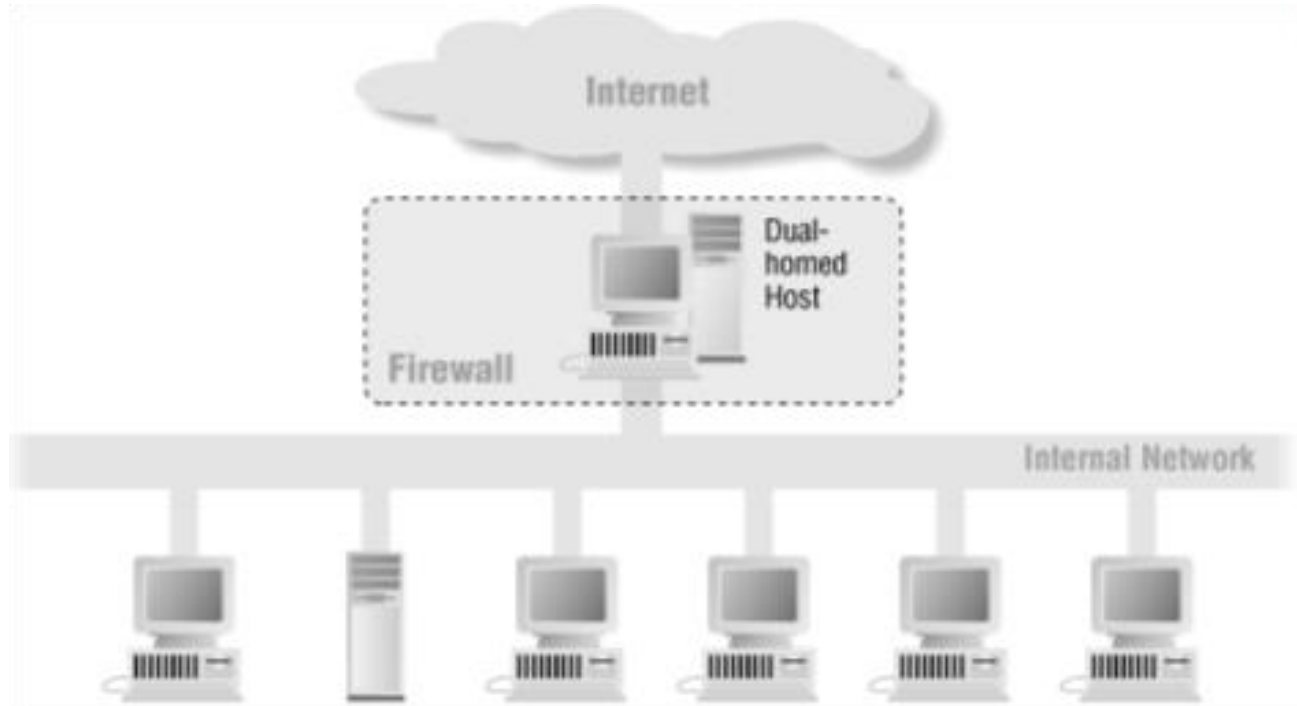
- **Εσωτερικός δρομολογητής**

- Προστατεύει το εσωτερικό δίκτυο από το Διαδίκτυο και το περιμετρικό δίκτυο
- Φιλτράρει πακέτα
- Επιτρέπει μόνο επιλεγμένες υπηρεσίες από το εσωτερικό δίκτυο προς το Διαδίκτυο

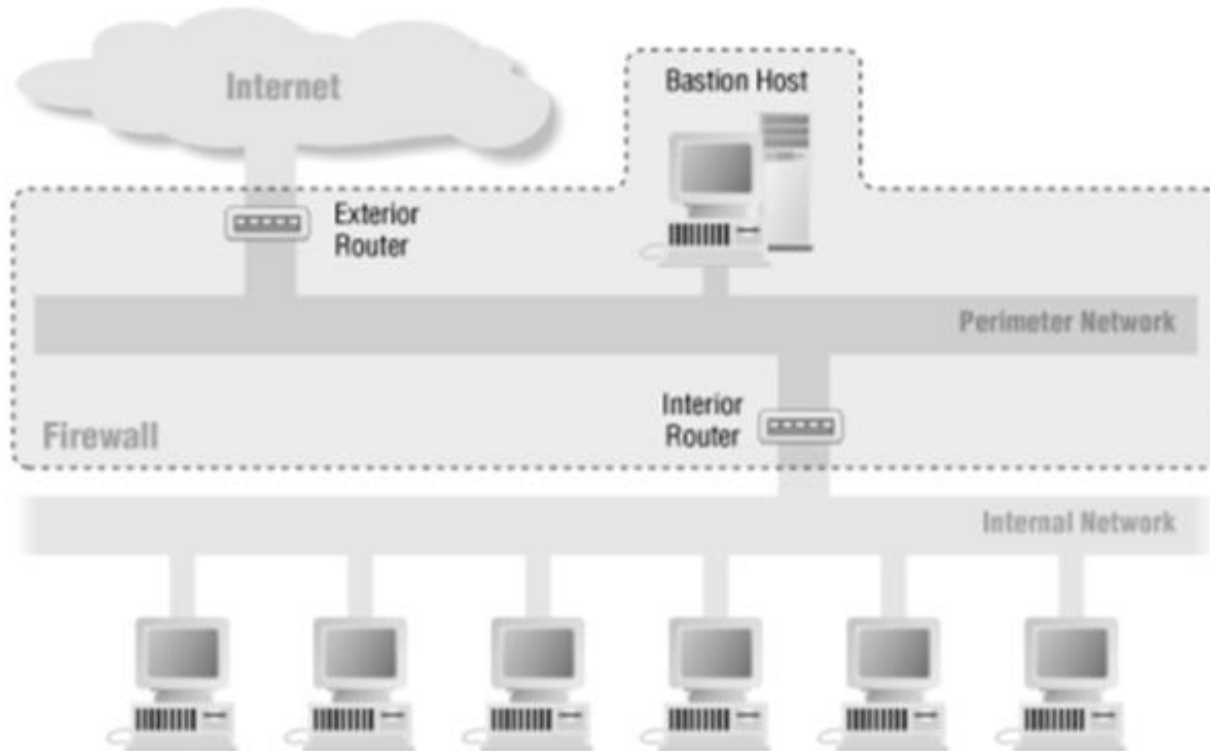
- **Εξωτερικός δρομολογητής**

- Προστατεύει το περιμετρικό δίκτυο από το Διαδίκτυο.
- Διαθέτει αντίγραφα κανόνων από τον εσωτερικό δρομολογητή.
- Δέσμευση εισερχόμενων συνδέσεων.

# 1<sup>η</sup> κατηγορία: Διπλοσυνδεδεμένα δίκτυα



## 2<sup>η</sup> κατηγορία: Υποδίκτυα διαλογής



# Επιλογές σχεδίασης

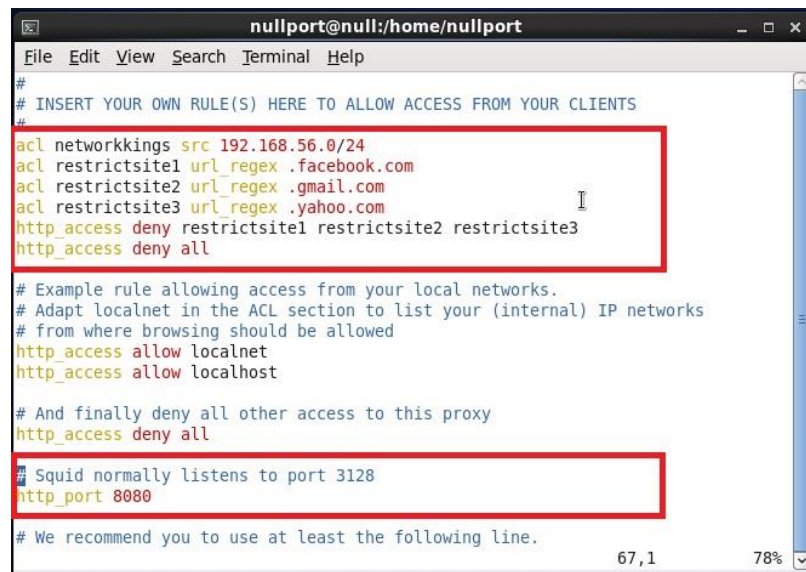
---



# Λίστα Ελέγχου Πρόσβασης

- Ένα τείχος ασφαλείας παρομοιάζεται με μια λίστα ελέγχου πρόσβασης
- Λίστα ελέγχου πρόσβασης (Access Control List – ACL): Μια λίστα με εντολές αποδοχής ή απόρριψης μιας σύνδεσης, με βάση κάποια κριτήρια

```
R1(config)#
R1(config)#ip access-list resequence OutBoundAccess 10 10
R1(config)#do sh access-list OutBoundAccess
Extended IP access list OutBoundAccess
 10 permit ip 192.168.1.0 0.0.0.255 any
 20 deny tcp 192.168.2.0 0.0.0.127 any eq smtp
 30 deny tcp 192.168.2.0 0.0.0.127 any eq sunrpc
 40 deny tcp 192.168.2.0 0.0.0.127 any eq pop2
 50 deny tcp 192.168.2.0 0.0.0.127 any eq nntp
 60 deny tcp 192.168.2.0 0.0.0.127 any eq ftp
 70 deny tcp 192.168.2.0 0.0.0.127 any eq ftp-data
 80 deny tcp 192.168.2.0 0.0.0.127 any eq telnet
 90 deny tcp 192.168.2.0 0.0.0.127 any eq cmd
100 deny tcp 192.168.2.0 0.0.0.127 any eq irc
110 permit ip 192.168.2.0 0.0.0.255 any
120 permit ip 192.168.3.0 0.0.0.255 any
130 permit ip 192.168.4.0 0.0.0.255 any
140 permit ip 192.168.5.0 0.0.0.255 any
R1(config)#
R1(config)#
```



The screenshot shows a terminal window titled 'nullport@null:/home/nullport'. The terminal displays the configuration of an Access Control List (ACL) for a proxy server. The configuration includes rules for allowing access from specific IP ranges and denying access from others. The configuration is as follows:

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl networkkings src 192.168.56.0/24
acl restrictsite1 url_regex .facebook.com
acl restrictsite2 url_regex .gmail.com
acl restrictsite3 url_regex .yahoo.com
http_access deny restrictsite1 restrictsite2 restrictsite3
http_access deny all

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 8080

# We recommend you to use at least the following line.
```

The terminal window also shows the status bar at the bottom with '67,1' and '78%'.

# Πολιτικές στις Λίστα Ελέγχου Πρόσβασης

- Αν κάποιο πακέτο δεν ταυτιστεί με καμία καταχώρηση της ACL, πρέπει να προβλέπεται η προεπιλεγμένη ενέργεια. Αυτή η ενέργεια ονομάζεται πολιτική ασφαλείας
- Διακρίνονται οι εξής κατηγορίες:
  - **Πολιτική προκαθορισμένης απόρριψης:** Απαγορεύεται οτιδήποτε δεν επιτρέπεται ρητά
  - **Πολιτική προκαθορισμένης αποδοχής:** Επιτρέπεται οτιδήποτε δεν απαγορεύεται ρητά
- Οι κανόνες που θα βάλουμε σε μια ACL εξαρτάται από την πολιτική ασφαλείας!
- **Ποια θεωρείτε προτιμότερη πολιτική και γιατί;**