Εργαστήριο Δικτύων Υπολογιστών

6η Διάλεξη:

- Ασφάλεια δικτύων

Ασφάλεια Δικτύων

- Μέθοδοι επίθεσης
  - Denial-of-Service (DoS)
  - Μη εξουσιοδοτημένη πρόσβαση (Unauthorized access attacks)
  - Password attacks, Trojan Horses, Network packet sniffers
- Firewalls
  - Network layer: Router-Access Control List, Bastion Host
  - Application layer: Proxy
- NAT (Network Address Translator)

Denial-of-Service (DoS)

- **DoS attack**: αποστολή περισσοτέρων αιτήσεων σύνδεσης από όσες μπορεί να επεξεργαστεί ένας server
- Το DoS attack πρόγραμμα κάνει μια αίτηση σύνδεσης σε μια port ενός server, αλλάζοντας την πληροφορία της επικεφαλίδας του πακέτου που είναι σχετική με τον αποστολέα του, και μετά τερματίζει την σύνδεση.
- Εάν ο server μπορεί να απαντήσει σε 20 αιτήσεις το δευτερόλεπτο, και ο επιτιθέμενος στέλνει 50 αιτήσεις το δευτερόλεπτο, προφανώς ο server δεν θα μπορέσει να εξυπηρετήσει τον επιτιθέμενο και ούτε τους άλλους «νόμιμους» χρήστες
- Είναι πολύ εύκολο να εξαπολυθούν, δύσκολο να εντοπιστούν, πολύ δύσκολο να αντιμετωπιστούν μιας και είναι δύσκολο να αρνηθείς την αίτηση του attacker χωρίς να απορρίψεις και τους άλλους χρήστες

Μη εξουσιοδοτημένη πρόσβαση (Unauthorized access)

- Διάφοροι τρόποι επίθεσης που εμπεριέχουν την ανάκτηση του δικαιώματος εισόδου, εκτέλεσης εντολών, ή ανάκτησης πληροφορίας σε ένα μηχάνημα που δεν παρέχει τέτοιες υπηρεσίες στον επιτιθέμενο
- Για παράδειγμα: ένας web server πρέπει να απαντάει σε web pages requests και να μην παρέχει την δυνατότητα εκτέλεσης shell εντολών χωρίς να είναι σίγουρος ότι ο χρήστης που τις εκτελεί έχει τέτοια δικαιώματα (local administrator)

Password attacks

- **Brute force attack**: Αποτελεί την μέθοδο εύρεσης ενός password
  - με επαναληπτικό τρόπο δοκιμάζοντας όλους (ή ένα μεγάλο μέρος) τους δυνατούς συνδυασμούς
  - με αποκρυπτογράφηση του password δοκιμάζοντας όλους (η ένα μεγάλο μέρος) τους δυνατούς συνδυασμούς των πιθανών κλειδιών κρυπτογράφησης
- Τρόπος αντιμετώπισης αυτής της απειλής: διαλέγοντας «κάλα» password και ένα «ισχυρό» αλγόριθμο κρυπτογράφησης.
- Ένας αλγόριθμος κρυπτογράφησης σχεδιάζεται έτσι ώστε να είναι υπολογιστικά μη δυνατό να αποκρυπτογραφηθεί η πληροφορία σε χρονικό διάστημα που να είναι ωφέλιμη.

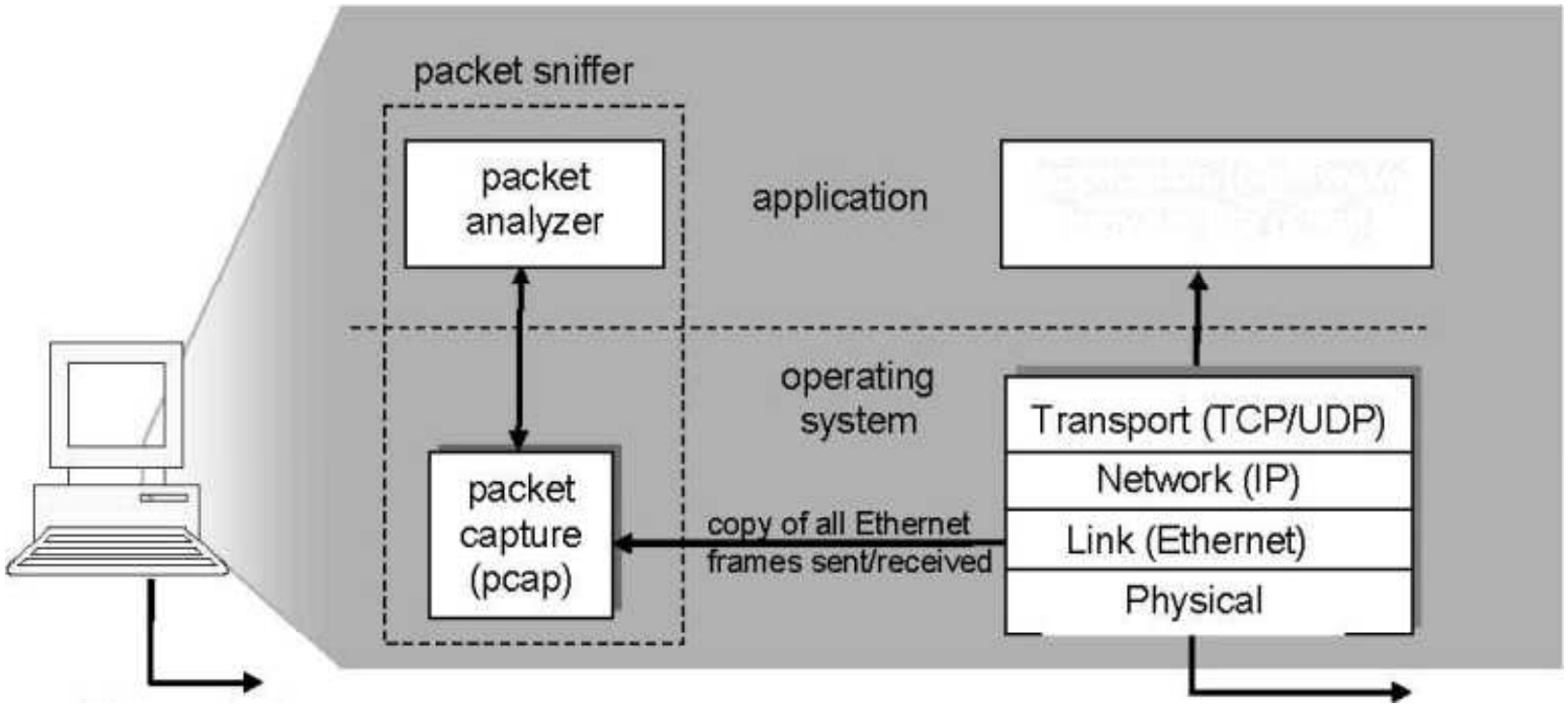
Trojan Horses

- **Trojan horse**: είναι ένα πρόγραμμα που περιέχει η εγκαθιστά μία «κακόβουλη» (malicious) εφαρμογή
- Ένα παράδειγμα ενός trojan horse: ένα πρόγραμμα που ονομάζονταν "waterfalls.scr" το οποίο διαφημιζόταν ως ένας screensaver με καταρράκτες, και όταν εκτελείται δίνει την δυνατότητα απομακρυσμένης πρόσβασης στον υπολογιστή (remote access)
- Μπορούν να χρησιμοποιηθούν για: Remote Access, Email Sending, Data destruction, Downloading, DoS attacks

Network packet sniffers (1)

- Packet sniffer (network analyzer ή protocol analyzer → ethernet sniffer ή wireless sniffer) είναι ένα πρόγραμμα ή μηχάνημα το οποίο μπορεί να υποκλέψει κίνηση που μεταφέρεται από ένα δίκτυο.
- Ο packet sniffer «ακούει» όλα τα πακέτα και τελικά αποκρυπτογραφεί και αναλύει το περιεχόμενο τους
  - Πολλά από τα δεδομένα μεταφέρονται μη κρυπτογραφημένα
  - Το username/password συχνά είναι κοινό για διάφορες εφαρμογές
- Οι Network packet sniffers μπορούν να χρησιμοποιηθούν και καλόβουλα
  - Εντοπισμός προβλημάτων στο δίκτυο
  - Παρακολούθηση κίνησης δικτύου
  - Συλλογή και αναφορά δικτυακών στατιστικών, κ.α.

Network packet sniffers (2)



Δομή ενός packet sniffer

Μη εξουσιοδοτημένη πρόσβαση – Εκτέλεση εντολών

- Υπάρχουν 2 τύποι πρόσβασης σε ένα μηχάνημα: normal user και administrator
  - Ένας normal user μπορεί να κάνει κάποιες εργασίες (όπως ανάγνωση αρχείων, αποστολή των αρχείων με e-mail, κτλ.)
  - Ο administrator μπορεί να αλλάξει το configuration του μηχανήματος (αλλαγή IP διεύθυνσης, αλλαγή δικαιωμάτων των χρηστών του μηχανήματος, κτλ).
- Θέλουμε να προστατεύσουμε ένα μηχάνημα και στις δύο περιπτώσεις

Μη εξουσιοδοτημένη πρόσβαση – Ανάκτηση πληροφορίας και καταστροφή

- Ανάκτηση πληροφορίας:
  - Βασικό ερώτημα: «τι θέλουμε να προστατεύσουμε».
  - Υπάρχει συγκεκριμένη πληροφορία που θέλουμε να προστατεύσουμε γιατί θα ήταν επιβλαβές αν έπεφτε στα χέρια των «ανταγωνιστών». Η είσοδος του επιτιθέμενου ακόμα και σαν απλού χρήστη στο μηχάνημα θα δημιουργούσε πρόβλημα
- Καταστροφική συμπεριφορά
  - Data Diddling: Ο attacker αλλάζει κάποιο αρχείο (π.χ. Εγγραφές σε ένα spreadsheets ή τα account numbers για ένα σύστημα αυτόματης κατάθεσης). Δύσκολο να εντοπιστεί, και αν εντοπιστεί πως ξέρουμε ποια αρχεία, τι έχει αλλάξει σε αυτά, και αν έχουν πάρει και άλλοι αυτή την πληροφορία (έχουν γίνει πληρωμές σε λάθος λογαριασμούς !!!)
  - Data Destruction: Ο attacker διαγράφει αρχεία. Συνήθως αντιμετωπίζεται με επαναφορά των αρχείων από backup

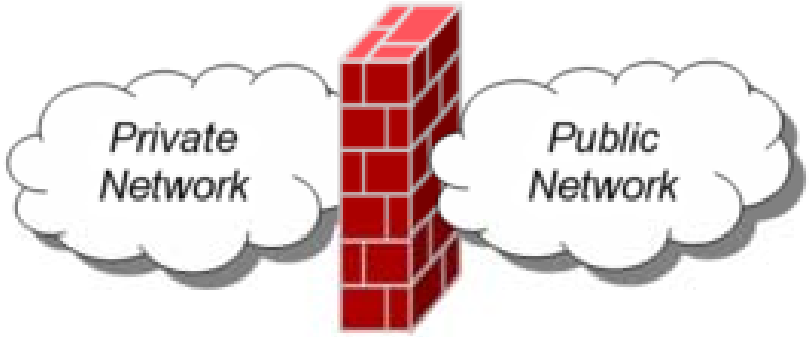
Πως ένας attacker αποκτεί πρόσβαση στο μηχάνημα?

- Από οποιαδήποτε σύνδεση με τον «έξω κόσμο». Αυτό εμπεριέχει Internet connections, dial-up modems, ακόμα και φυσική πρόσβαση!!!!
- Για να προστατέψετε το μηχάνημα, όλοι οι πιθανοί τρόποι εισόδου πρέπει να εντοπιστούν και να εκτιμηθούν (risk levels)

Απλά μαθήματα ασφάλειας

- Backups
- Μην βάζετε δεδομένα εκεί που δεν χρειάζονται
- Αποφύγετε συστήματα με single points of failure
- Μείνετε ενημερωμένοι με τα operating system patches, και κοιτάτε τις σχετικές οδηγίες για ασφάλεια
- Οι επιχειρήσεις πρέπει να έχουν κάποιον εργαζόμενο εξειδικευμένο σε θέματα ασφάλειας

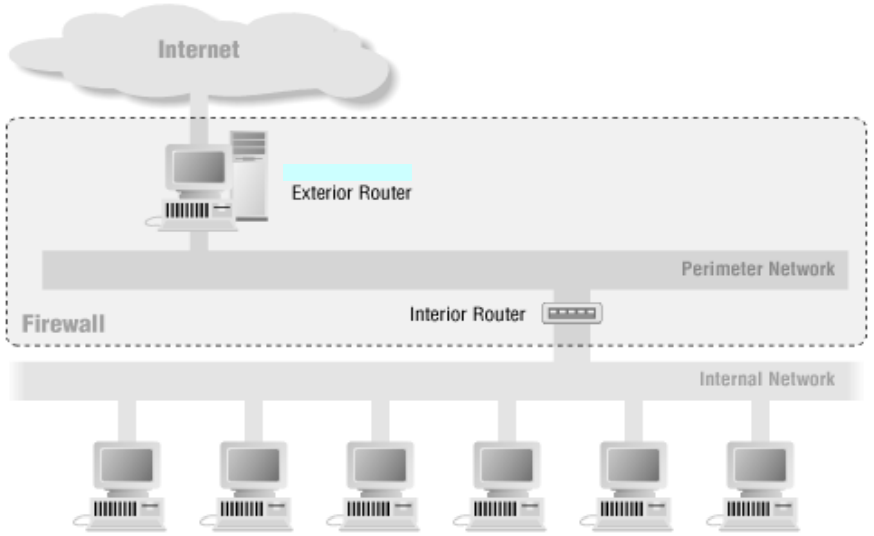
Firewalls



- Έστω ότι έχουμε δύο ξεχωριστά δίκτυα: το Internet και ένα εσωτερικό δίκτυο (intranet) μιας επιχείρησης, τα οποία θέλουμε να επικοινωνούν. Είναι προφανές επιθυμητό η πληροφορία που είναι διαθέσιμη εσωτερικά στο intranet να μην είναι προσπελάσιμη εξωτερικά από άλλους
- Firewall είναι ένα πρόγραμμα ή ένα μηχάνημα που μπορεί να χρησιμοποιηθεί σαν διαχωριστικό μεταξύ των δύο αυτών δικτύων
- Ήδη firewalls
  - Network layer: Router - Access Control List (ACL), Bastion host
  - Application layer: Proxy
  - Software Personal Firewall

Network layer firewalls – Router + ACL

Router

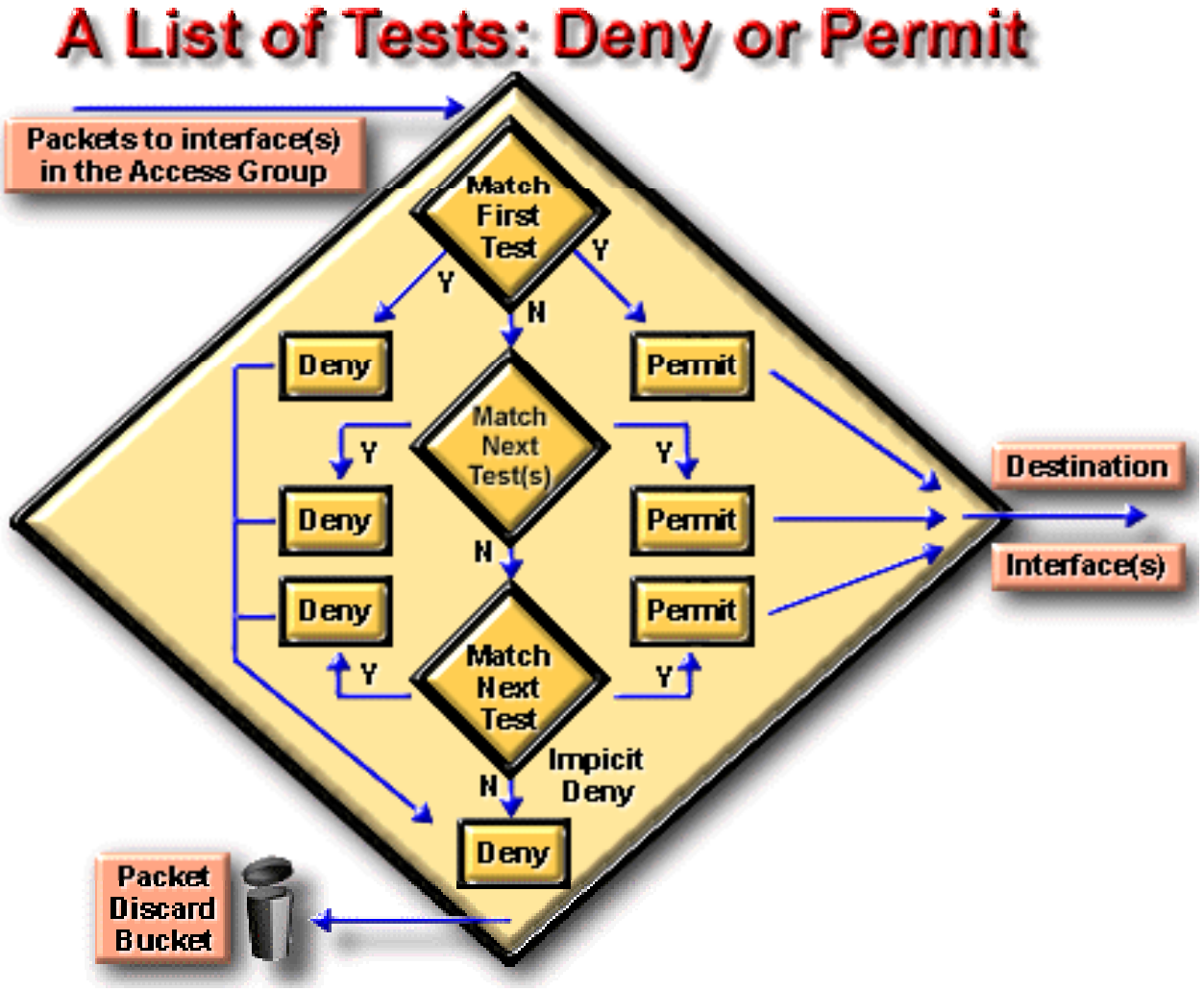


- Ειδικής χρήσης μηχάνημα
- Ο απλός router είναι το «παραδοσιακό» network layer firewall μιας και μπορεί να πάρει πολύπλοκες αποφάσεις για το αν και πως θα προωθήσει τα πακέτα βασιζόμενος στα source, destination addresses και το είδος της κίνησης (βασισμένοι στα protocols και ports)

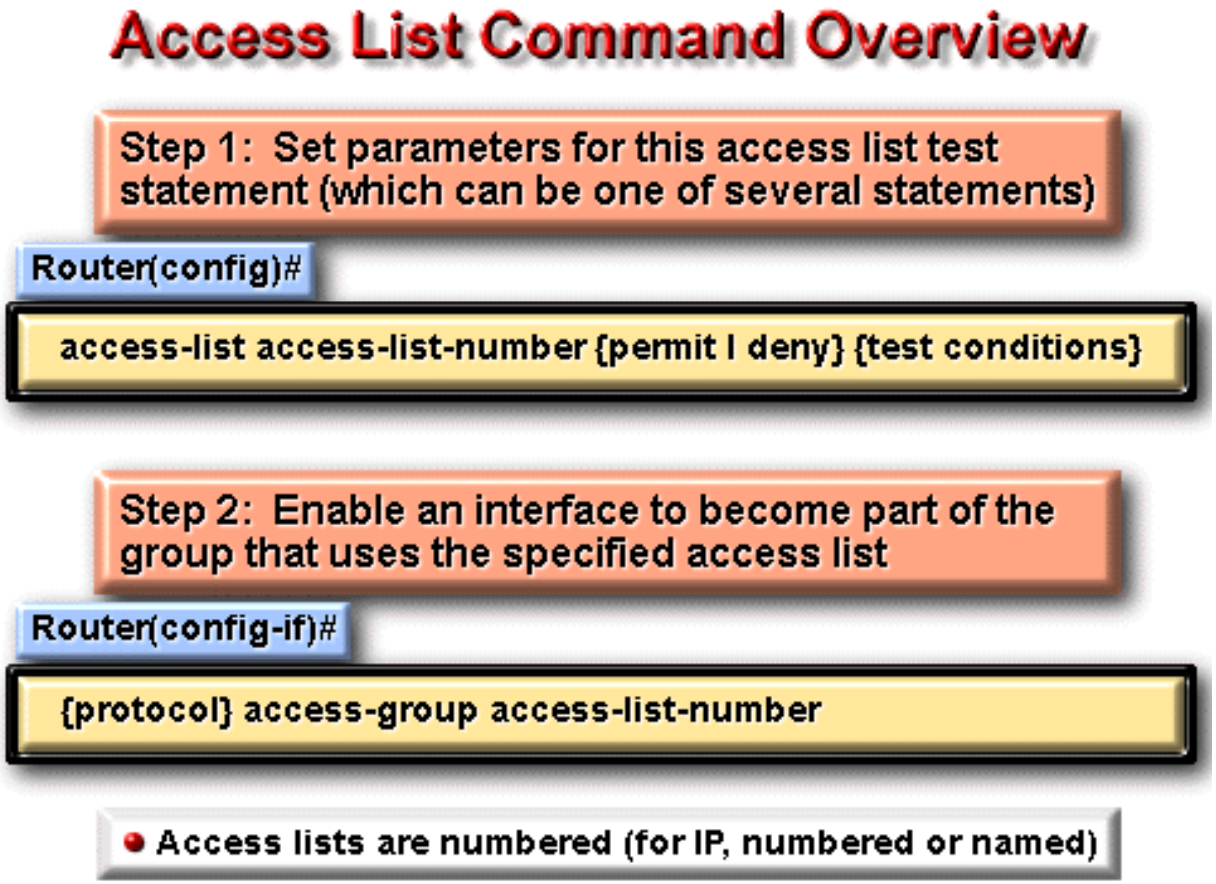
Access Control List (ACL)

- Αποτελούν δηλώσεις οι οποίες αποθηκεύονται στο configuration file ενός δρομολογητή
- Επιτρέπουν ή αποκόπτουν την εισερχόμενη/εξερχόμενη από μία διεπαφή κίνηση βασιζόμενες σε ένα ή περισσότερα κριτήρια:
  - IP διεύθυνση του αποστολέα
  - IP διεύθυνση του παραλήπτη
  - IP διεύθυνση του (υπο)-δικτύου προορισμού
  - IP διεύθυνση του (υπο)-δικτύου προέλευσης της κίνησης
  - Πρωτόκολλο
  - Αριθμός θύρας (καθορίζει την εφαρμογή)
- Εφαρμόζονται στην εισερχόμενη ή εξερχόμενη κίνηση μιας διεπαφής ενός δρομολογητή
- Cisco IOS
  - Standard IP ACL
  - Extended IP ACL

Λειτουργία ACL



ACLs εντολές



Cisco IOS Standard IP ACL (1)

- Εξετάζουν την IP διεύθυνση του αποστολέα
- Επιτρέπουν ή απαγορεύουν την κίνηση στηριζόμενη στην network/subnet/host διεύθυνση του αποστολέα
- Παίρνουν αριθμούς από 1-99
- Ορισμός standard IP ACL
  - access-list list# {permit/deny} source IP [wildcard mask]
  - interface [router interface]
  - ip access-group [list#] in|out (out is the default)

Cisco IOS Standard IP ACL (2)

- Δημιουργία ACL η οποία αποκόπτει την κίνηση από το δίκτυο 210.93.105.0/24 να εξέρχεται από το Serial interface s0 ενός δρομολογητή. Όλη η υπόλοιπη κίνηση επιτρέπεται.

```
access-list 4 deny 210.93.105.0 0.0.0.255
access-list 4 permit any
interface s0
ip access-group 4 out
```

Cisco IOS Extended IP ACL (1)

- Παρέχουν περισσότερες δυνατότητες ελέγχου της κίνησης σε σχέση με τις standard IP ACL
- Παίρνουν αριθμούς από 100-199
- Εξετάζουν την IP διεύθυνση του αποστολέα, του παραλήπτη, το πρωτόκολλο και τον αριθμό της θύρας
- Ορισμός extended IP ACL
  - access-list list# {permit/deny} protocol source [source mask] destination [destination mask] operator [port]
  - interface [router port]
  - ip access-group [list#] in|out (out is the default)

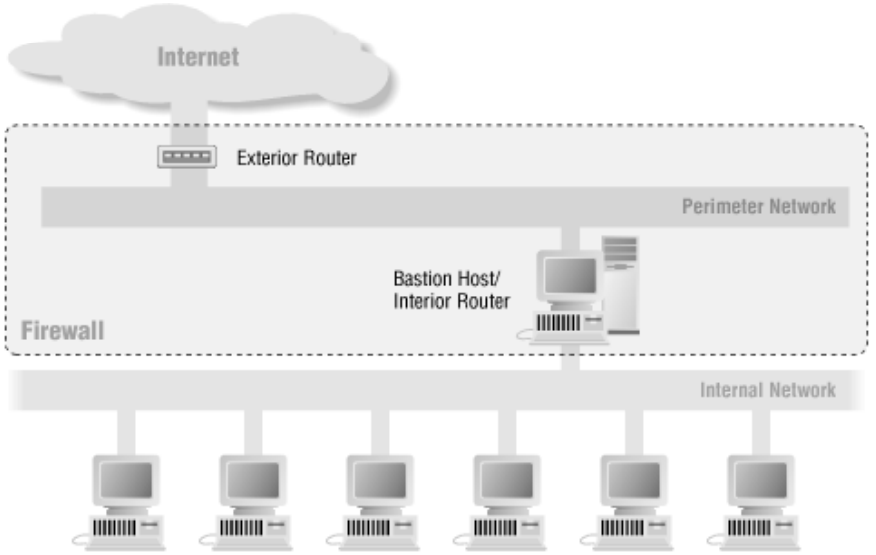
Cisco IOS Extended IP ACL (2)

- Δημιουργία ACL η οποία αποκόπτει την εισερχόμενη μέσω της διεπαφής Serial0 IP κίνηση, προερχόμενη από οποιοδήποτε δίκτυο προς το δίκτυο 10.1.1.0/8. Όλη η υπόλοιπη κίνηση επιτρέπεται.

```
access-list 101 deny ip any 10.1.1.0 0.0.0.255
access-list 101 permit any
interface s0
ip access-group 101 in
```

Network layer firewalls

Bastion Hosts



- Γενικής χρήσης υπολογιστής
- Συνήθως τρέχει μια έκδοση του Unix η οποία έχει τροποποιηθεί για να υποστηρίζει τις απαιτούμενες λειτουργίες (οι γενικές εφαρμογές του Λ.Σ. δεν είναι ενεργοποιημένες ή έχουν σβηστεί έτσι ώστε να υπάρχει αυξημένη ασφάλεια στο Bastion Host)
- Οι routers επιτρέπουν κίνηση μόνο προς/από τον Bastion host

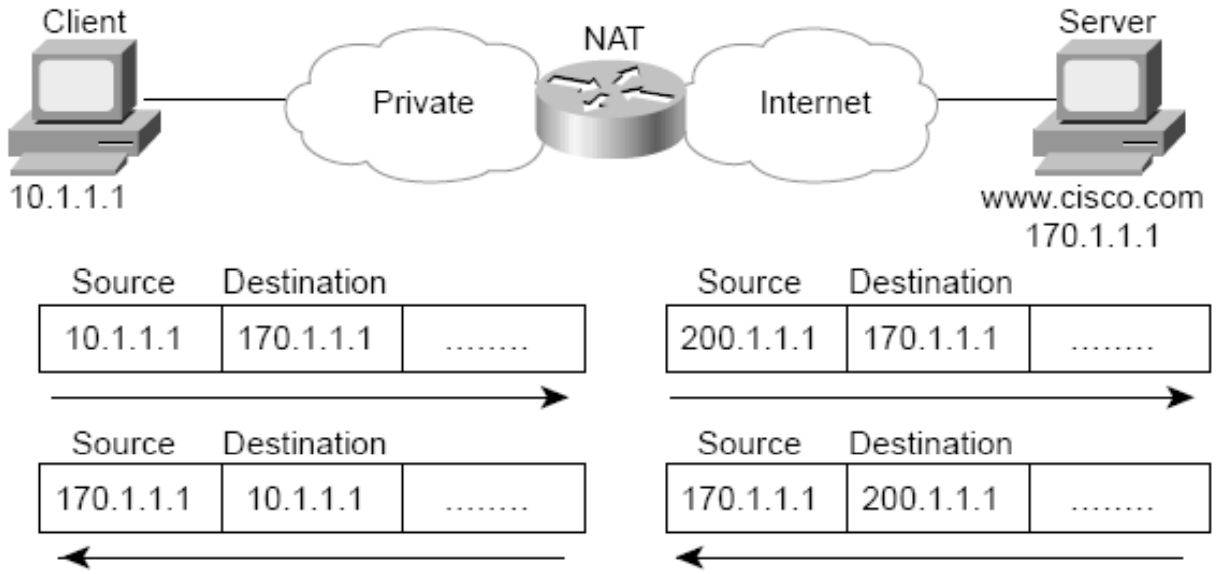
Application layer firewall - Proxy

- Ένα application layer firewall δεν ελέγχει την κίνηση στο επίπεδο δικτύου αλλά στο επίπεδο εφαρμογών
- Ένας Proxy μπορεί να απαγορεύσει την επικοινωνία μεταξύ δικτύων, και να εκτελέσει σύνθετες λειτουργίες καταχώρησης και χρέωσης της κίνησης που περνάει από αυτόν
- Οι αιτήσεις «σταματάνε» στον Proxy ο οποίος αναλαμβάνει να ξεκινήσει μια σύνδεση αν αυτή ικανοποιεί κάποιους κανόνες
- Ο Proxy μπορεί να επιθεωρεί το περιεχόμενο της κίνησης, να μπλοκάρει την επικοινωνία όταν διαπιστώσει «περίεργο» περιεχόμενο, όπως συγκεκριμένα websites, ιούς, απόπειρα εκμετάλλευσης γνωστών προβλημάτων (logical flaws) στο client software, κ.α.

Software Personal Firewalls

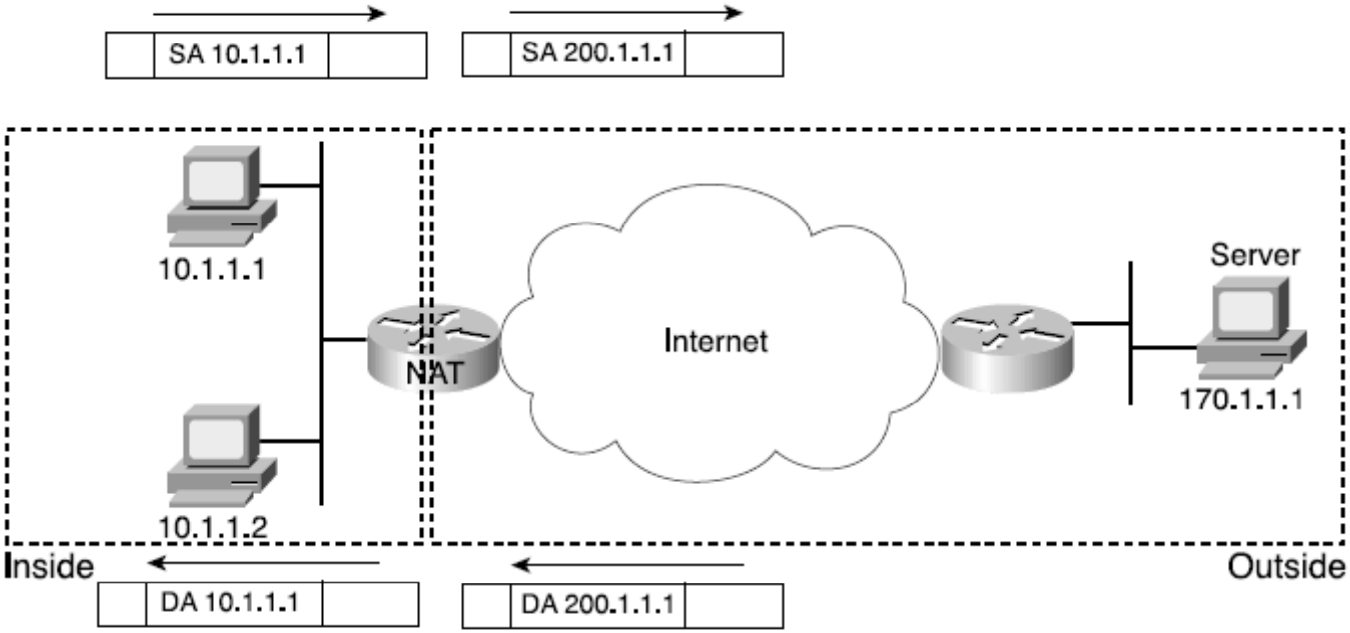
- Μια εφαρμογή (software) που φιλτράρει την κίνηση που εισέρχεται ή εξέρχεται από ένα μηχάνημα
- Ένα προσωπικό (personal) firewall διαφέρει από τα συνηθισμένα firewalls στο μέγεθος και τον τρόπο χρήσης: Τα personal firewalls είναι συνήθως φτιαγμένα για χρήστες (end-users), οπότε συνήθως προστατεύουν έναν υπολογιστή
- Συνήθως ρωτούν τον χρήστη κάθε φορά που ξεκινάει μία σύνδεση και προσαρμόζουν ανάλογα με την απάντηση την πολιτική ασφάλειας του μηχανήματος
- Μπορούν να περιέχουν διαδικασίες intrusion detection

NAT - Network Address Translation



- Η τεχνολογία NAT επιτρέπει σε ένα μηχάνημα που έχει μία ιδιωτική IP διεύθυνση να επικοινωνήσει με άλλα μηχανήματα μέσω του Internet
- Μεταφράζει την ιδιωτική IP διεύθυνση του αποστολέα σε μία δημόσια διεύθυνση
- Δεν είναι δυνατή η άμεση πρόσβαση στο ιδιωτικό δίκτυο από το δημόσιο δίκτυο
- Επιλύει το πρόβλημα των λιγοστών IP διευθύνσεων σε συνδυασμό με την τεχνολογία Port Address Translation

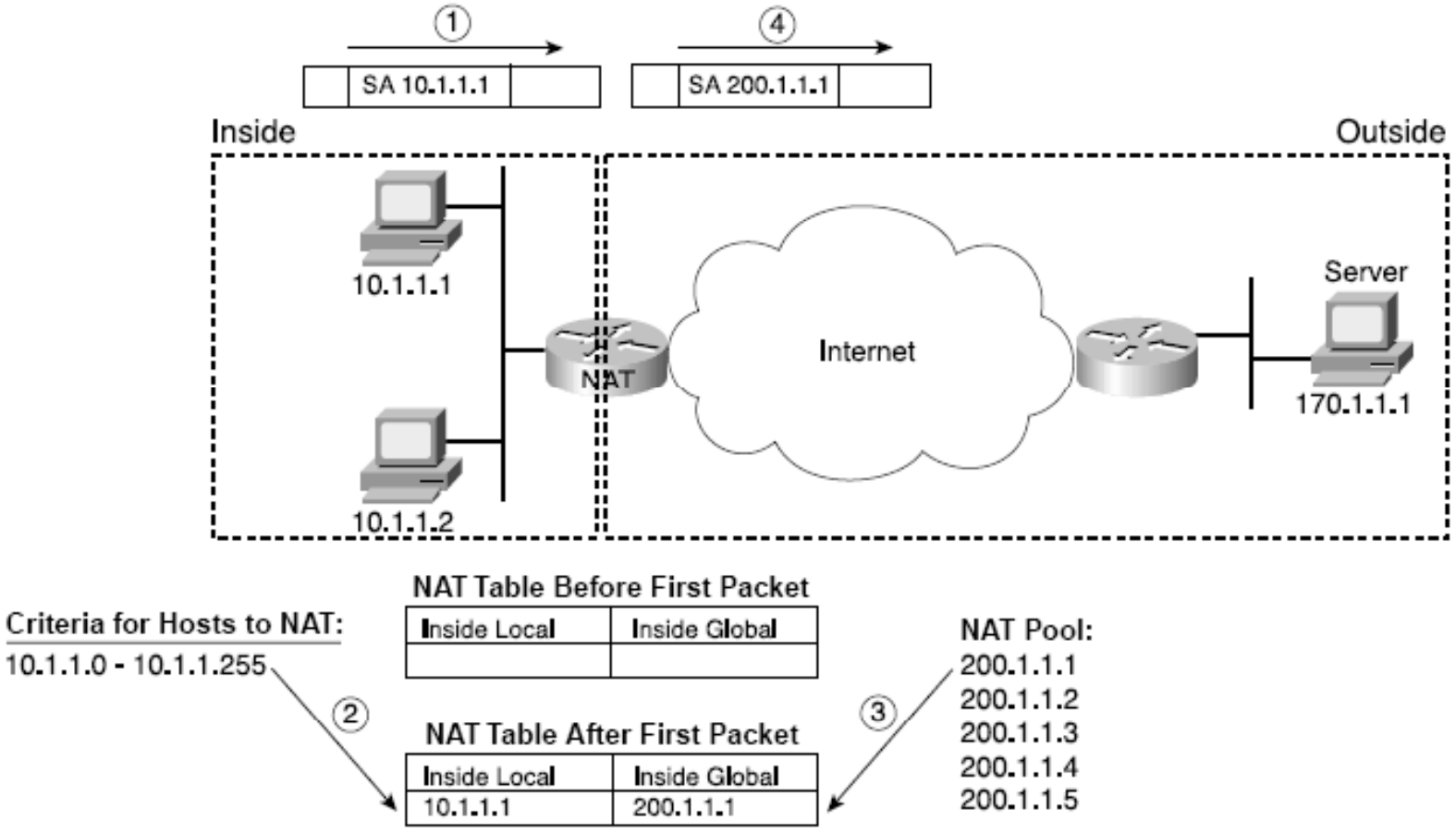
Static NAT



Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

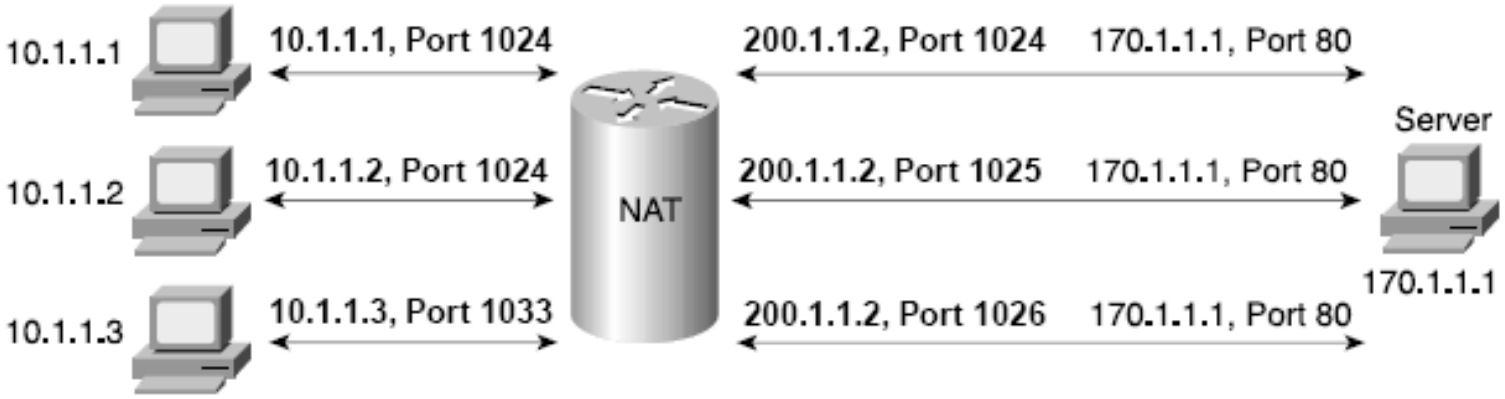
Αντιστοίχηση εξ' αρχής μίας ιδιωτικής IP διεύθυνσης σε μία δημόσια

Dynamic NAT



Η αντιστοίχηση μεταξύ μίας ιδιωτικής IP διεύθυνσης και μίας δημόσιας γίνεται δυναμικά

PAT – Port Address Translation



Dynamic NAT Table, With Overloading

Inside Local	Inside Global
10.1.1.1:1024	200.1.1.2:1024
10.1.1.2:1024	200.1.1.2:1025
10.1.1.3:1033	200.1.1.2:1026

- Με την ένα-προς-ένα αντιστοίχιση των ιδιωτικών και δημοσίων IP διευθύνσεων δεν επιλύεται σημαντικά το πρόβλημα των λιγοστών IP διευθύνσεων
- Τεχνολογία PAT
  - Αντιστοίχηση port numbers
  - Αντιστοίχιση πολλών ιδιωτικών IP διευθύνσεων στην ίδια δημόσια διεύθυνση