Διαχείριση ενός Εικονικού Ιδιωτικού Δικτύου – Διαχείριση διευθύνσεων

Λίγα λόγια για τις IP διευθύνσεις

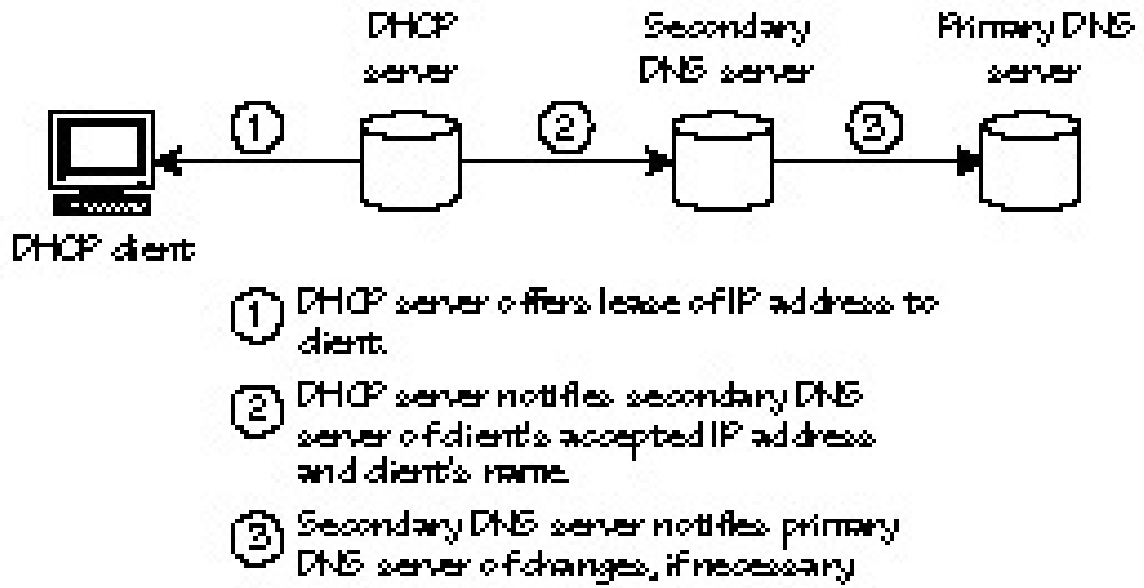
- Για να είναι κάποιος στο Internet, πρέπει να έχει μια **μοναδική** IP διεύθυνση – ένας 32-bit αριθμός.
- Το πλήθος όλων των πιθανών IP διευθύνσεων είναι 4,294,967,296 (2^{32}). Ο πραγματικός αριθμός όμως είναι σημαντικά μικρότερος (μεταξύ 3.2 και 3.3 δισεκατομμύρια) λόγω αφενός του ότι κάποιες διευθύνσεις είναι ειδικά δεσμευμένες, αφετέρου λόγω του ότι δομούνται σε διάφορες κλάσεις (κλάσεις A,B,C).

Διαχείριση των διευθύνσεων

- Dynamic Host Control Protocol (DHCP): πρωτόκολλο για δυναμική απόδοση των IP διευθύνσεων (καθιστώντας έτσι πιο ευέλικτο ένα δίκτυο).
  - Όταν κάποιος συνδέεται, στέλνει μία DHCP αίτηση (request) στον DHCP server για να του αποδώσει μία IP διεύθυνση. Ο server θα στείλει μία απάντηση (reply). Ο πελάτης (client) μπορεί είτε να αποδεχτεί είτε να περιμένει απάντηση από άλλον server. Στη συνέχεια ενημερώνει τον server που προτίμησε ότι τον αποδέχεται, και τέλος ο server στέλνει ένα ACK που περιέχει την IP διεύθυνση συν κάποιες παράμέτρους.
  - Ένας DHCP server μπορεί να κάνει και στατική απόδοση διευθύνσεων (π.χ. σε mail servers)

Διαλειτουργικότητα DHCP και DNS

- Για κάθε απόδοση διευθύνσεων που κάνει ο DHCP, ενημερώνει τον DNS Server



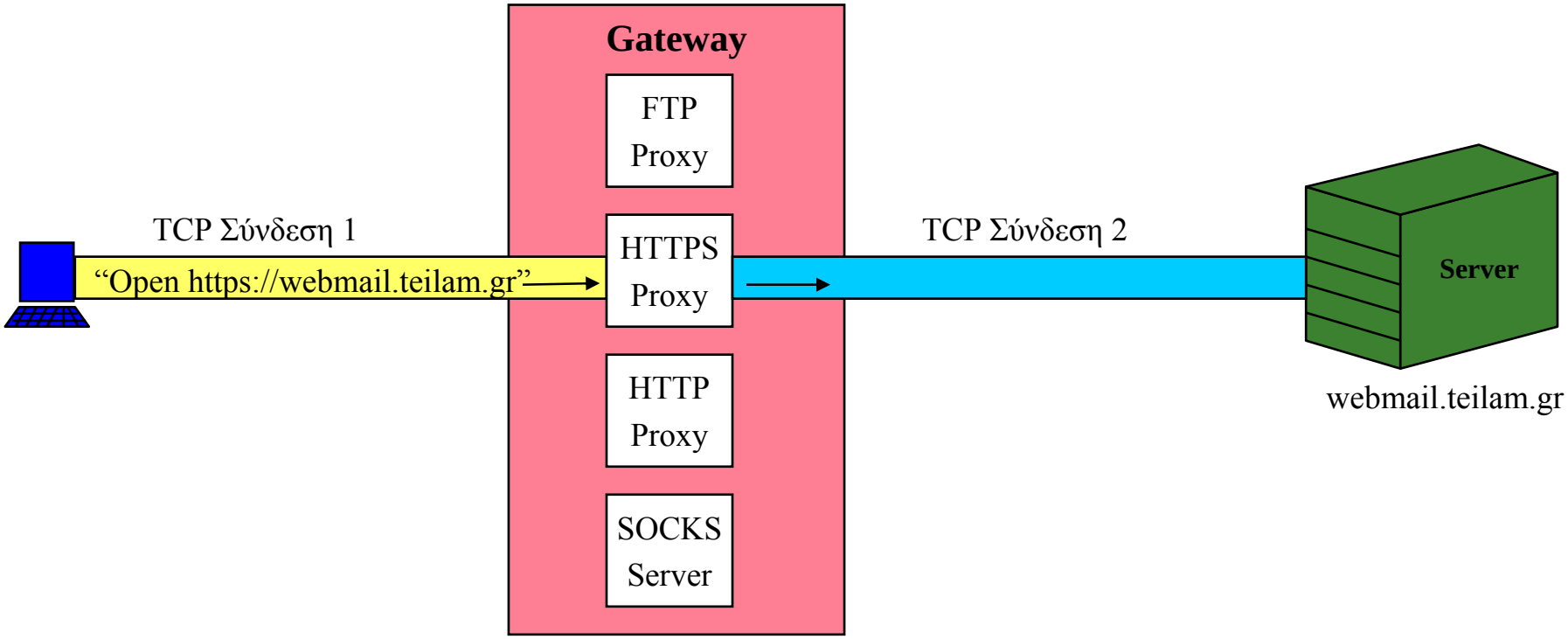
Τι πρόβλημα υπάρχει στα VPN?

- Ειδικά για εσωτερικά δίκτυα (intranets), οι πιθανές IP διευθύνσεις είναι:
  - 10.0.0.0 - 10.255.255.255 (Class A)
  - 172.16.0.0 - 172.31.255.255 (Class B)
  - 192.168.0.0 - 192.168.255.255 (Class C)
- Οι διευθύνσεις αυτές χρησιμοποιούνται από πολλούς οργανισμούς – δεν μπορούν να χρησιμοποιηθούν για πρόσβαση στο internet, γιατί θα βρεθούν δύο διαφορετικοί υπολογιστές με την ίδια IP διεύθυνση.

Μια πρώτη λύση – proxy servers

- Περιπτώσεις όπου υπάρχουν proxy servers (π.χ. SOCKS server) αντιμετωπίζουν αυτό το πρόβλημα – κι αυτό γιατί η δική τους διεύθυνση αποστέλλεται στο δίκτυο και όχι η πραγματική διεύθυνση των κόμβων. Ωστόσο, αυτό δεν αποτελεί γενική λύση.
- Οι Proxy servers εξειδικεύονται για κάποιο συγκεκριμένο πρωτόκολλο (π.χ. HTTP, HTTPS, FTP). Πρωτόκολλα που βασίζονται στο UDP είναι πιο δύσκολα διαχειρίσιμα.

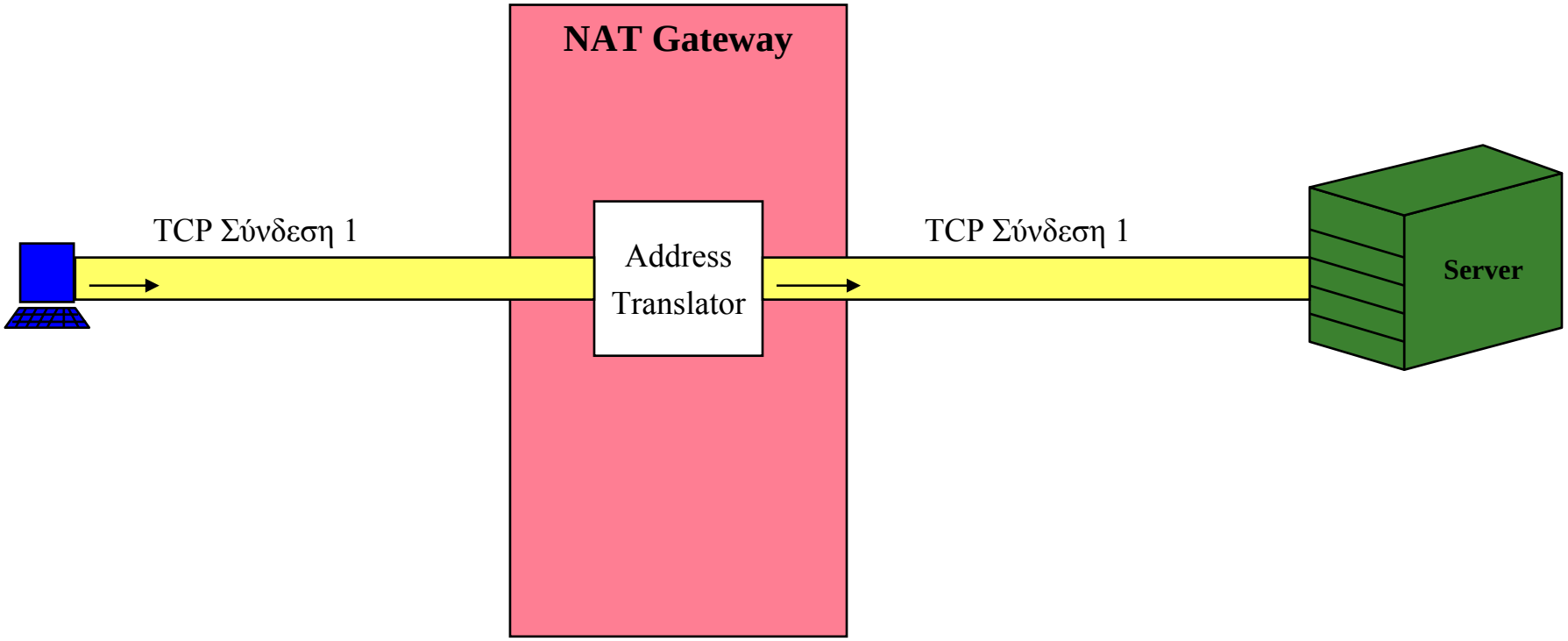
Παράδειγμα Proxy server



Δεύτερη λύση - Network Address Translation(NAT)

- Η πύλη (gateway) επιτελεί πια ξεχωριστή λειτουργία
  - Οι IP διευθύνσεις αποστολέα και προορισμού αλλάζουν («μεταγλωτίζονται»)
  - Καμία αλλαγή δεν λαμβάνει χώρα στους εσωτερικούς κόμβους του δικτύου
- Καμία αλλαγή δεν χρειάζεται να γίνει στις εφαρμογές
- Τα πρωτόκολλα που βασίζονται σε TCP λειτουργούν πολύ καλά, αλλά δυστυχώς όχι τα υπόλοιπα
- Παροχή ενός είδους ασφάλειας (μια που είναι «κρυμμένοι» οι κόμβοι πίσω από την πύλη (gateway))

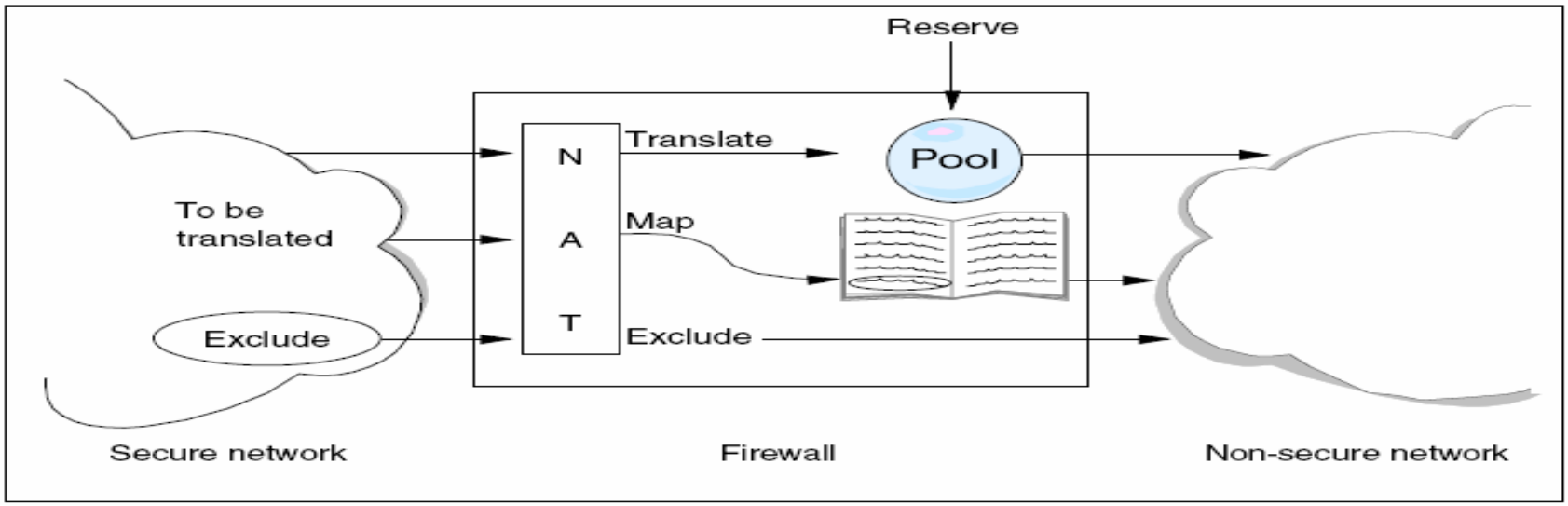
Παράδειγμα NAT



Τεχνικές NAT

- **Στατική μεταγλώττιση διευθύνσεων**
  - Μία συγκεκριμένη IP διεύθυνση μετατρέπεται πάντα σε μία άλλη συγκεκριμένη (NAT-IP). Καμία άλλη IP διεύθυνση δεν μετατρέπεται στην ίδια NAT-IP.
- **Δυναμική μεταγλώττιση διευθύνσεων**
  - Η NAT IP δεν είναι πάντα σταθερή για κάθε συγκεκριμένο κόμβο – αλλάζει κάθε φορά που επιχειρεί νέα σύνδεση (η συνηθέστερη περίπτωση).

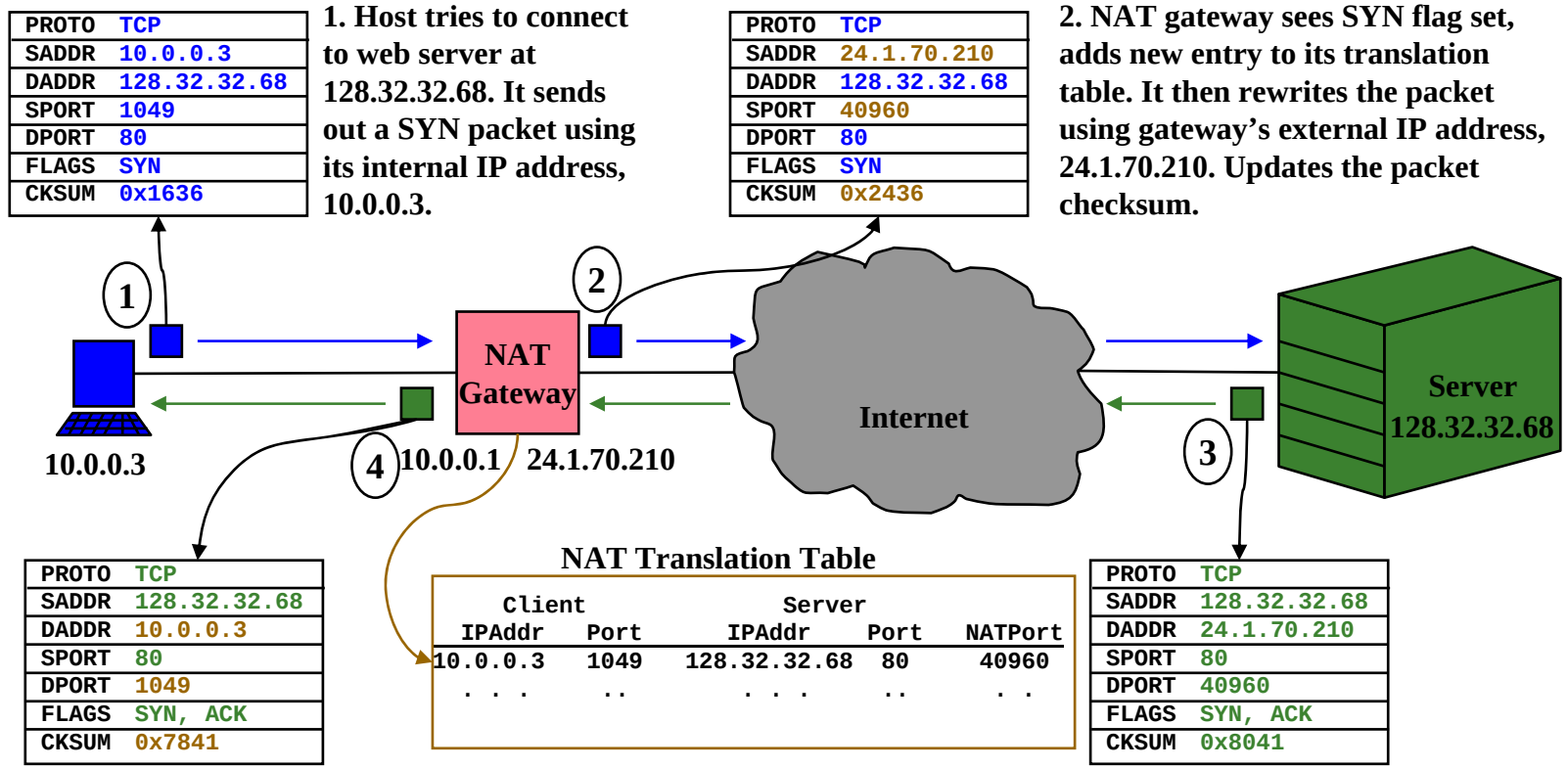
Λειτουργία της μεταγλώττισης των διευθύνσεων



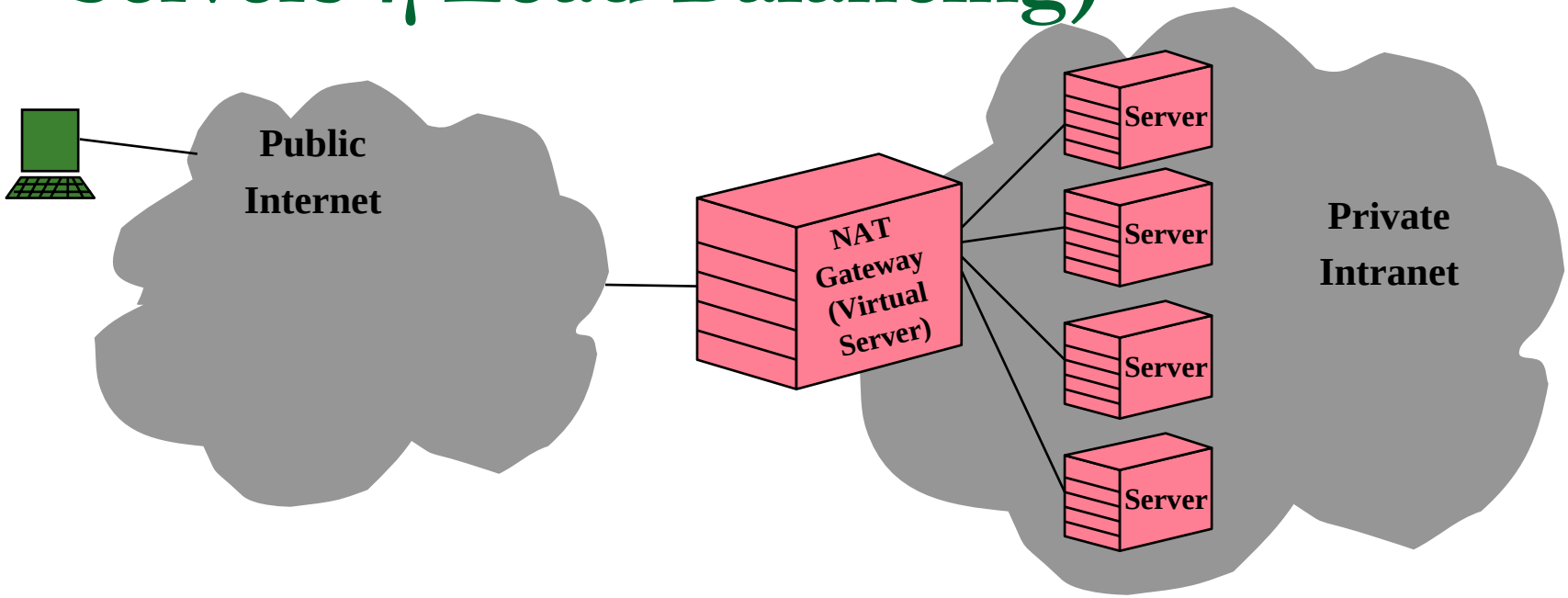
•Η εσωτερική διεύθυνση κάθε εξερχόμενου πακέτου ελέγχεται από τη NAT διαδικασία για το αν πληρεί συγκεκριμένους κανόνες. Αν ναι, τότε του αποδίδεται μια νέα διεύθυνση, από αυτές που διαθέτει ελεύθερες ο NAT μετασχηματισμός (στο σχήμα, οι ελεύθερες διευθύνσεις βρίσκονται στο pool). Καταχωρείται επίσης σε μία βάση δεδομένων (διαδικασία MAP στο σχήμα) η νέα διεύθυνση.

•Για κάθε εισερχόμενο πακέτο, ελέγχεται αυτή η βάση δεδομένων και, ανάλογα με το περιεχόμενό της, γίνεται η δρομολόγηση του εισερχόμενου πακέτου.

Παράδειγμα TCP NAT



Ιδεατοί εξυπηρετητές NAT (Virtual Servers ή Load Balancing)

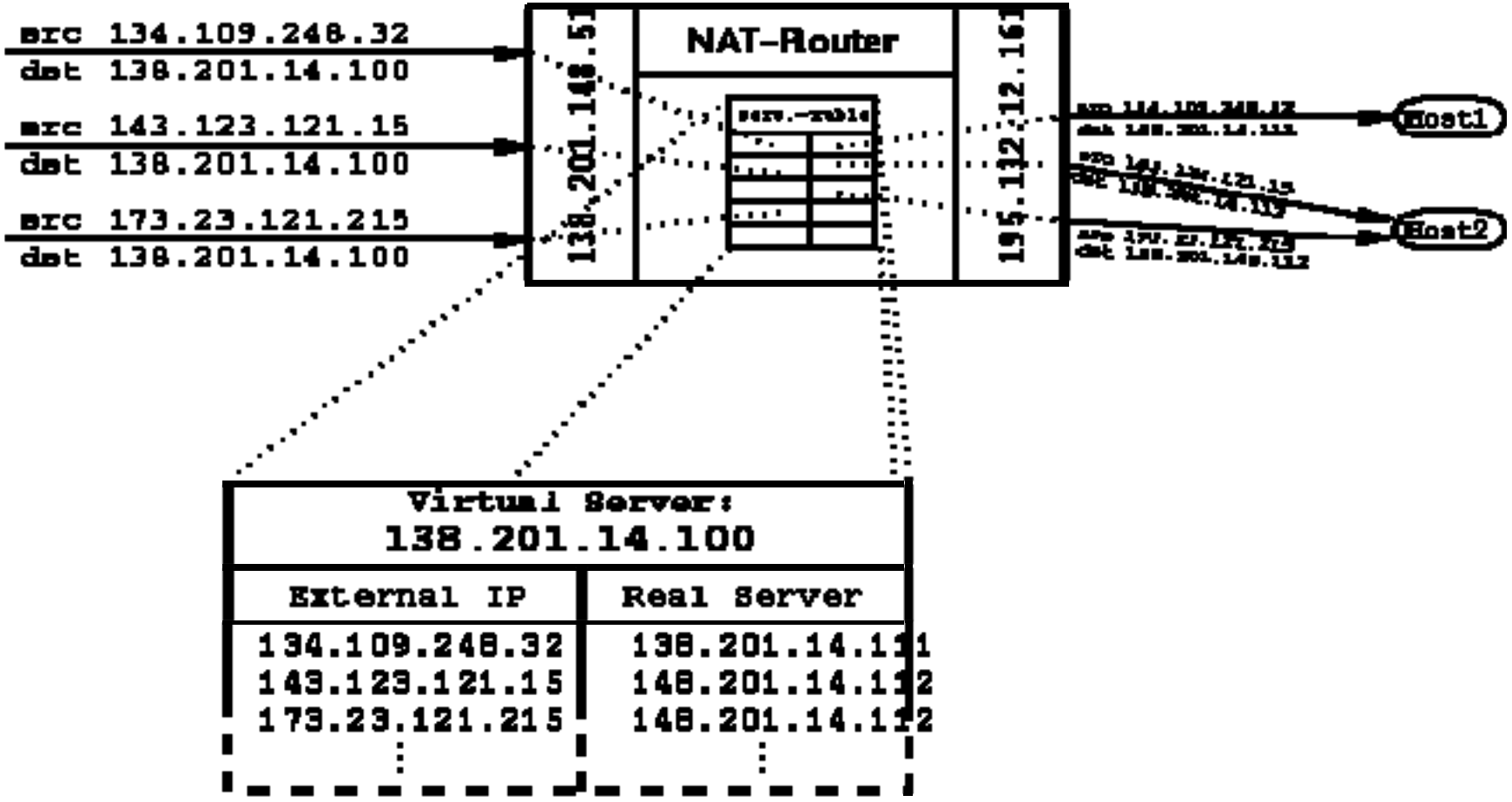


- Μία IP διεύθυνση αποδίδεται σε έναν ιδεατό server, ο οποίος δεν αντιστοιχεί σε καμία πραγματική συσκευή. Υπάρχουν και κάποια «πραγματικά» IPs, που αντιστοιχούν σε υπαρκτές συσκευές του ιδιωτικού δικτύου (του VPN για την περίπτωση που εξετάζουμε). Οι εξωτερικοί χρήστες επιχειρούν σύνδεση στο ιδιωτικό δίκτυο χρησιμοποιώντας ως διεύθυνση προορισμού των πακέτων τους την ιδεατή IP διεύθυνση. Τότε ο NAT μετασχηματισμός εναλλάσσει τις IP διευθύνσεις του ιδεατού server και ενός πραγματικού server (αναλόγως την εφαρμογή που αιτείται ο χρήστης.)

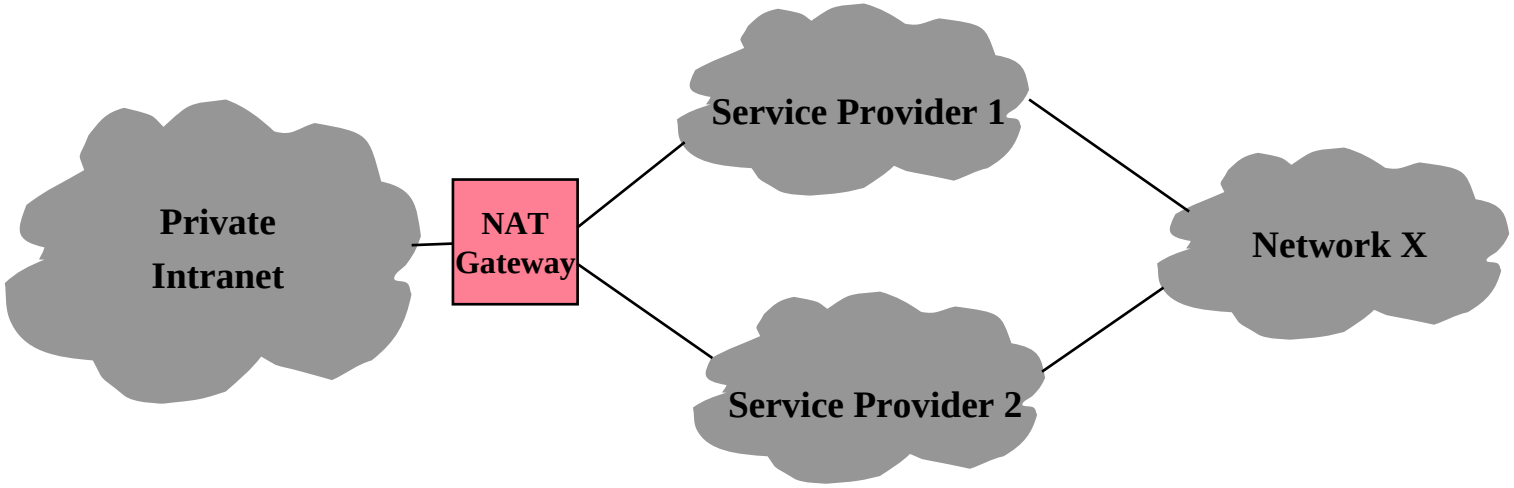
Παράδειγμα NAT με ιδεατό server

- Δημιουργία ιδεατής IP διεύθυνσης 138.201.14.100
- Χρήση 2 servers μέσα στο δίκτυο, με IP διευθύνσεις 138.201.14.111 και 148.201.14.112.
- Κάθε χρήστης που θέλει να συνδεθεί στο VPN στέλνει στην ιδεατή διεύθυνση – υπάρχει αλγόριθμος (ο οποίος ποικίλει από υλοποίηση σε υλοποίηση) που καθορίζει σε ποιον πραγματικό server του VPN θα δρομολογηθεί κάθε εισερχόμενο πακέτο. Διατηρείται μία βάση με τις ενεργές κάθε στιγμή συνδέσεις.

Σχηματική αναπαράσταση του προηγούμενου παραδείγματος



Εξισορρόπηση φορτίου



- Υπάρχουν αλγόριθμοι που καθορίζουν το ποιος server θα χρησιμοποιηθεί για τη σύνδεση, αναλόγως το φορτίο που ήδη έχει επιβαρυνθεί ο καθένας