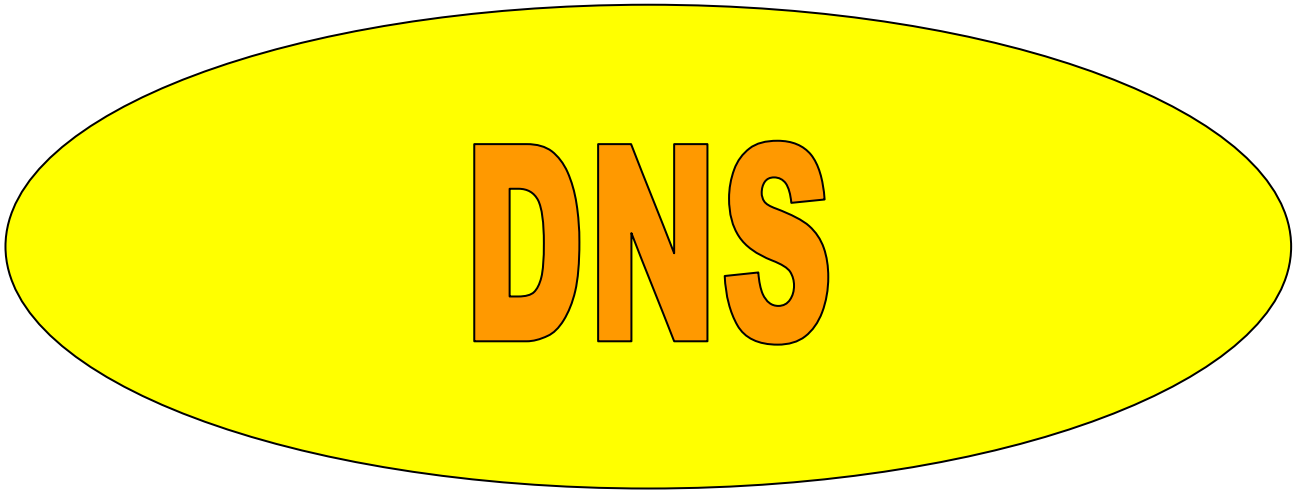
Mikrotik OS

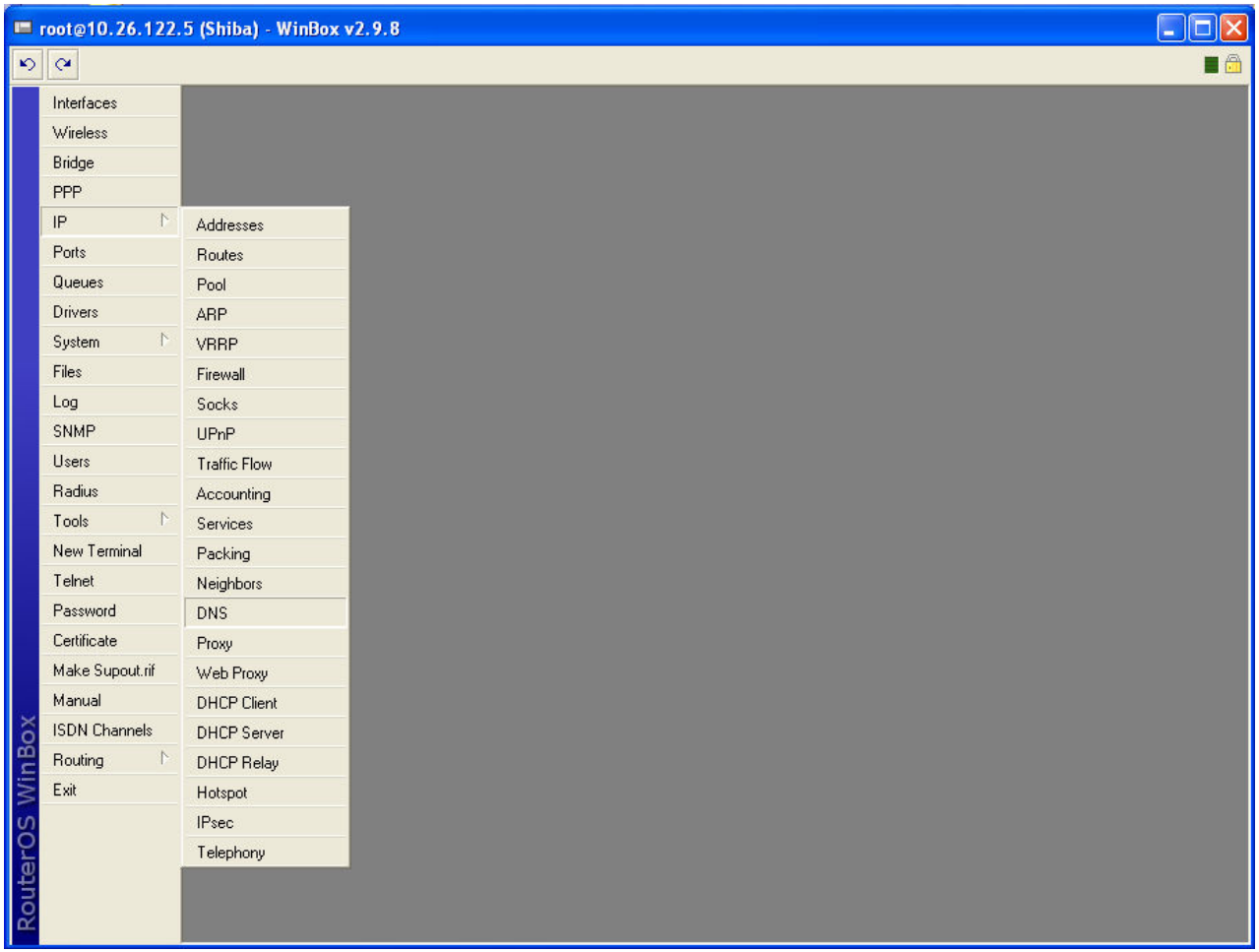
- Το Mikrotik δίνει ένα μεγάλο εύρος δυνατοτήτων στον χρήστη του.
- Σε αρκετούς από μας που θέλουμε να σηκώσουμε γρήγορα και εύκολα μία λειτουργία το Mikrotik μπορεί να μας λύσει τα χέρια
- Το παρακάτω κείμενο αναφέρεται σε κάποιες από της λειτουργίες αυτές


DNS

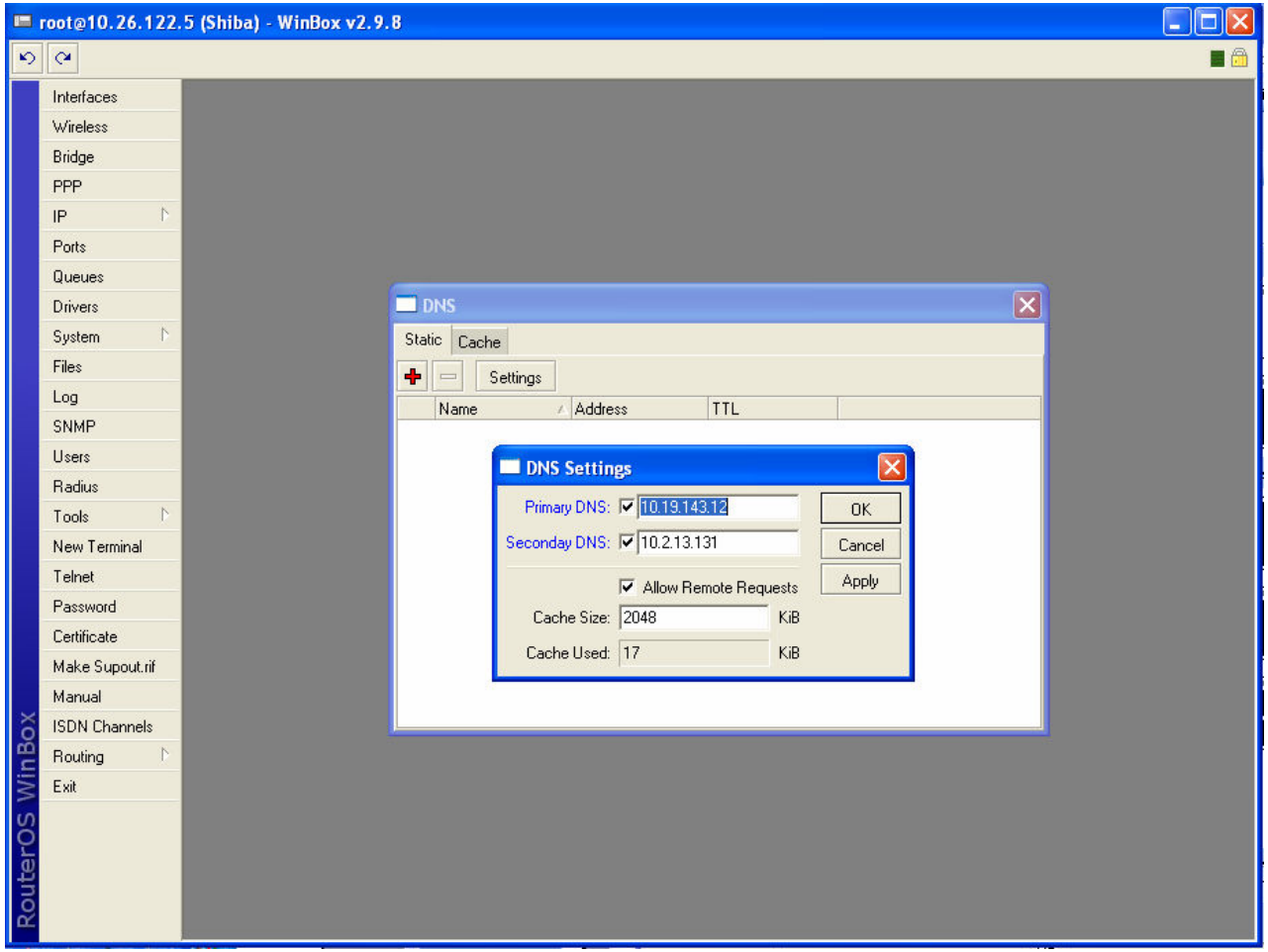
DNS

- Το Mikrotik μπορει να λειτουργήσει ως ένας μικρός DNS Server.

Επιλέγουμε IP ➔ DNS

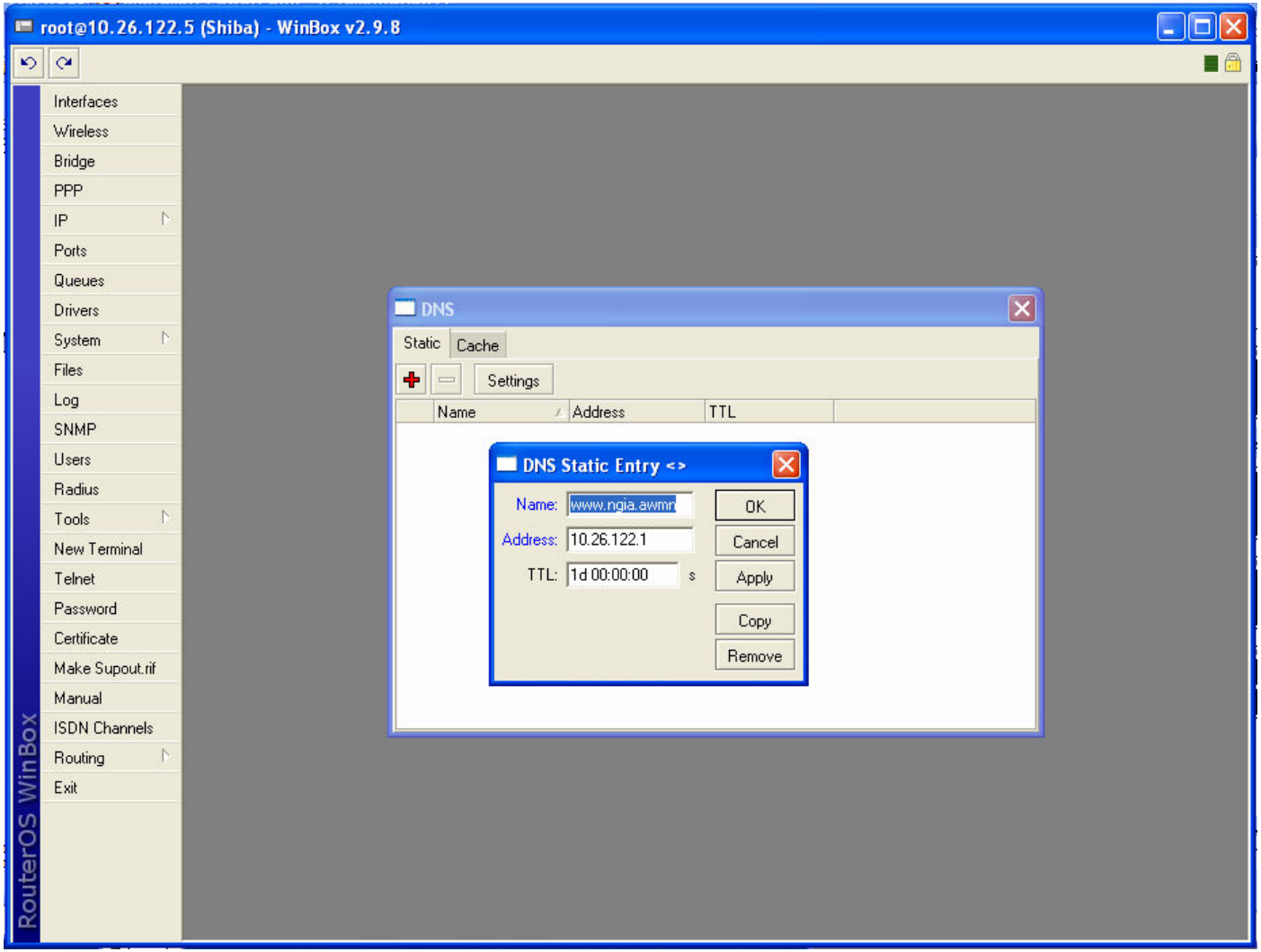


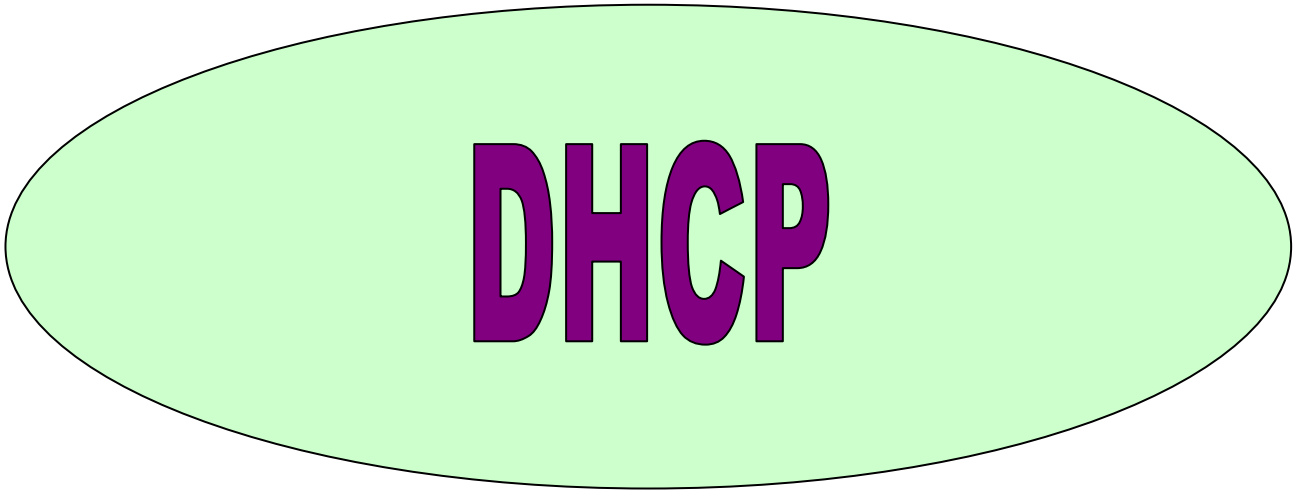
•Στην καρτέλα Static κάνουμε κλικ στο Settings



•Συμπληρώνουμε τα Primary & Secondary DNS και επιλέγουμε το Allow remote Requests και πατάμε OK.

•Για να προσθέσουμε στατικές εγγραφές, πατάμε το + και συμπληρώνουμε το Name με το όνομα του domain μας και το address με την IP διεύθυνση που αντιστοιχεί.

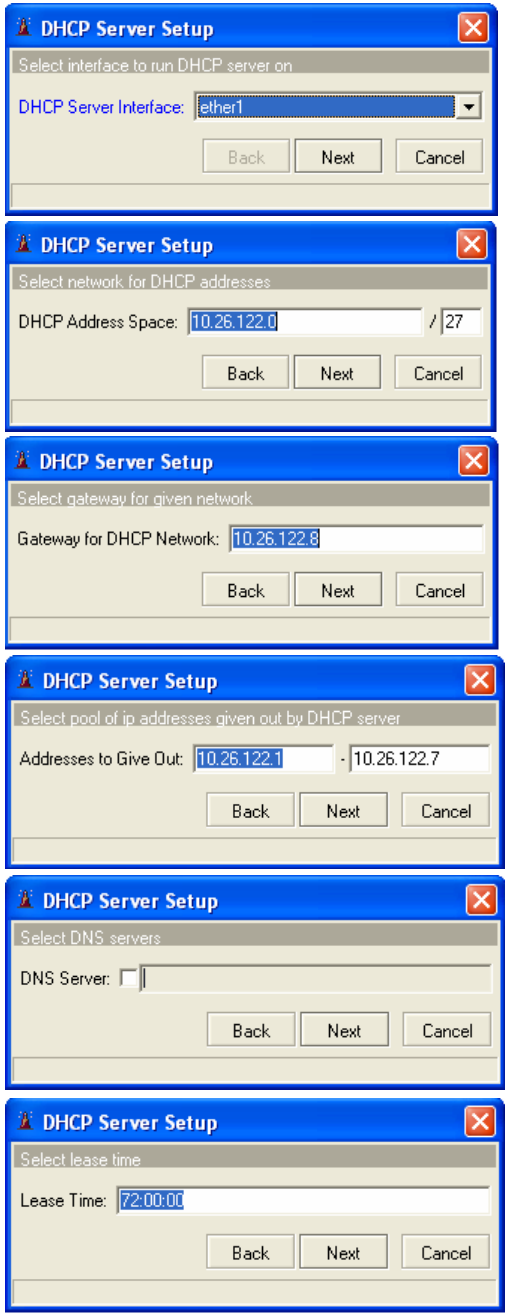



DHCP

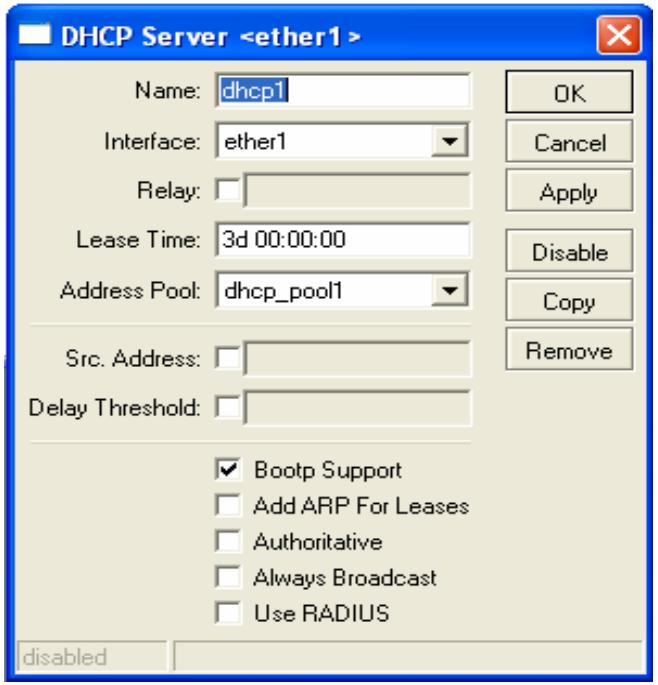
DHCP

Προκειμένου να ενεργοποιήσουμε τον DHCP Server του Mikrotik ακολουθούμε τα επόμενα βήματα:

•Επιλέγουμε IP και κάνουμε κλικ στο DHCP Server
Στην καρτέλα DHCP Πατάμε το Setup
•Επιβεβαιώνουμε ότι έχουμε επιλέξει την σωστή πόρτα (Ethernet / wireless card) που θέλουμε να ενεργοποιηθεί ο DHCP Server.
Πατάμε το Next
•Προσθέτουμε το Subnet που θέλουμε να διαμοιράσουμε διευθύνσεις και πατάμε το Next.
•Προσθέτουμε την IP του gateway που θα έχουν οι IP που θα μοιράσει το DHCP και πατάμε next
•Αν το DHCP χρησιμοποιείται από απομακρυσμένο δίκτυο δίνουμε την DHCP relay IP address και πατάμε next
•Ορίζουμε το εύρος των διαθέσιμων IP για διάθεση από τον DHCP Server (με την μορφή 10.χχχ.χχχ.χχχ – 10.χχχ.χχχ.χχχ) και πατάμε το next
•Επιλέγουμε το default DNS που θα δίνεται με την DHCP IP και πατάμε το next
•Τέλος επιλέγουμε την διάρκεια του lease για την IP



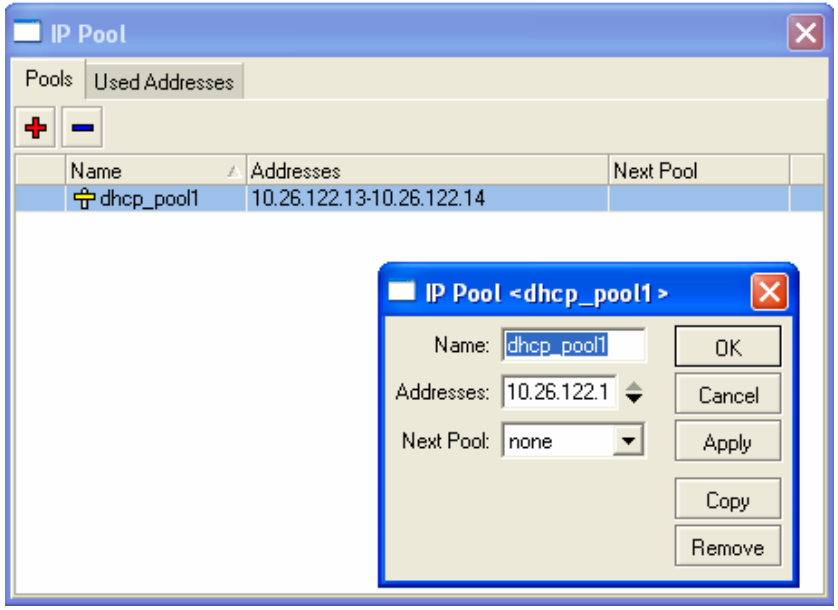
•Με διπλό κλικ στον dhcp server που μόλις σηκώσαμε, μπορούμε να δούμε συγκεντρωτικά τις ρυθμίσεις και να τις αλλάξουμε

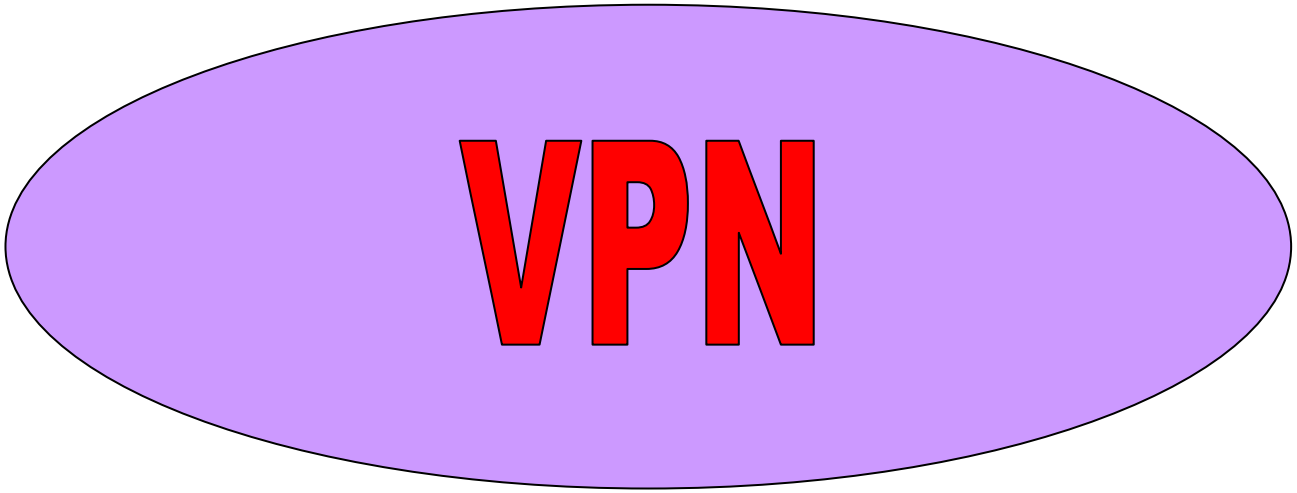


IP→IP Pool

•Παρατηρούμε το pool διευθύνσεων που μόλις δημιούργησε ο wizard

•Μπορούμε και από αυτή την καρτέλα να φτιάξουμε δικά μας pool διευθύνσεων για διάφορες χρήσεις




VPN

Τουνέλια (VPN Router-to-Router tunneling protocols)

Point-to-Point Tunneling Protocol (PPTP)

- VPN tunneling protocol
- Επέκταση του Point-to-Point Protocol (PPP), αξιοποιεί την αυθεντικοποίηση, συμπίεση και κωδικοποίηση του PPP

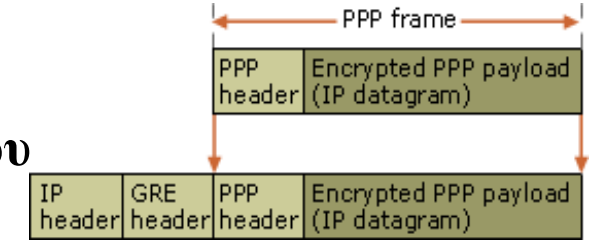
Βασικές υπηρεσίες σε ιδεατό ιδιωτικό δίκτυο (vpn) με PPTP

Ενθυλάκωση (Encapsulation)

•Σε ένα PPP πλαίσιο το οποίο περιλαμβάνει ένα IP datagram προστίθεται κεφαλή Generic Routing Encapsulation (GRE) και IP κεφαλή

•Η IP κεφαλή περιλαμβάνει την πηγή και τον προορισμό που αντιστοιχούν στον VPN client και server

pptp ενθυλάκωση ppp πλαισίου



Κρυπτογράφηση (Encryption)

•Το PPP πλαίσιο κρυπτογραφείται με τον αλγόριθμο Microsoft Point-to-Point Encryption (MPPE) χρησιμοποιώντας κλειδιά κρυπτογράφησης που δημιουργούνται από την διαδικασία αυθεντικοποίησης MS-CHAP ή EAP-TLS

•Οι πελάτες πρέπει να χρησιμοποιούν πρωτόκολλο αυθεντικοποίησης MS-CHAP ή EAP-TLS ώστε να κρυπτογραφούνται τα δεδομένα

•Το PPTP δεν παρέχει κρυπτογράφηση, απλά ενθυλακώνει ένα κρυπτογραφημένο PPP πλαίσιο.

•Επίσης είναι δυνατή μία PPTP σύνδεση χωρίς κρυπτογράφηση αλλά δεν συστήνεται για λόγους ασφαλείας

Layer Two Tunneling Protocol (L2TP)

- Τουνελοπρωτόκολλο που παρέχει **ενθυλάκωση PPP πλαισίων** πάνω σε δίκτυο μεταγωγής πακέτων
- Αξιοποιεί τους μηχανισμούς αυθεντικοποίησης και συμπίεσης του PPP
- Η διαφορά είναι ότι χρησιμοποιείται πρωτόκολλο Internet Protocol security (**IPSec**, RFC 2661) για την κρυπτογράφηση
- Έτσι οι VPN συνδέσεις με L2TP είναι ένας συνδιασμός L2TP και IPSec

Ενθυλάκωση (Encapsulation)

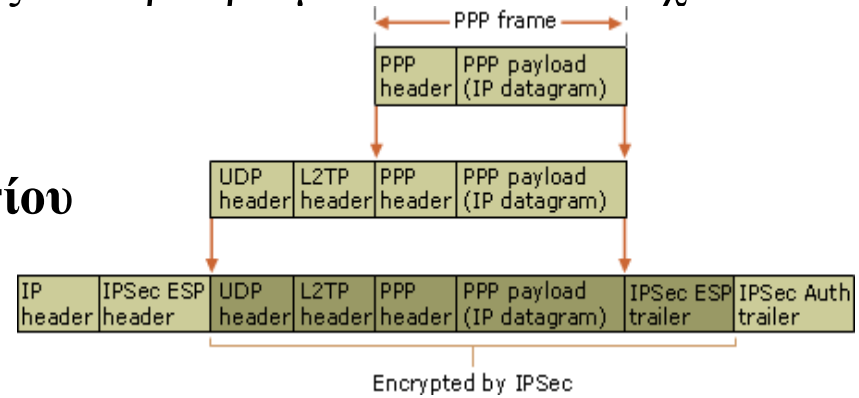
•Η ενθυλάκωση L2TP, IPSec πακέτων αποτελείοται από δύο στάδια ενθυλάκωσης

•L2TP ενθυλάκωση. Ένα PPP πλαίσιο περιέχει ένα IP datagram με μία L2TP κεφαλή και μία UDP κεφαλή

•IPSec ενθυλάκωση. Το L2TP μήνυμα, μαζί με μία IPSec Encapsulating Security Payload (ESP) κεφαλή και ουρά, ένα πεδίο IPSec Authentication που παρέχει έλεγχο της ορθότητας των μηνυμάτων και αυθεντικοποίηση και μία τελική IP κεφαλή

•Την IP κεφαλή υπάρχει η διεύθυνση πηγής και προορισμού που αντιστοιχούν στον VPN client και server

L2TP ενθυλάκωση ppp πλαισίου



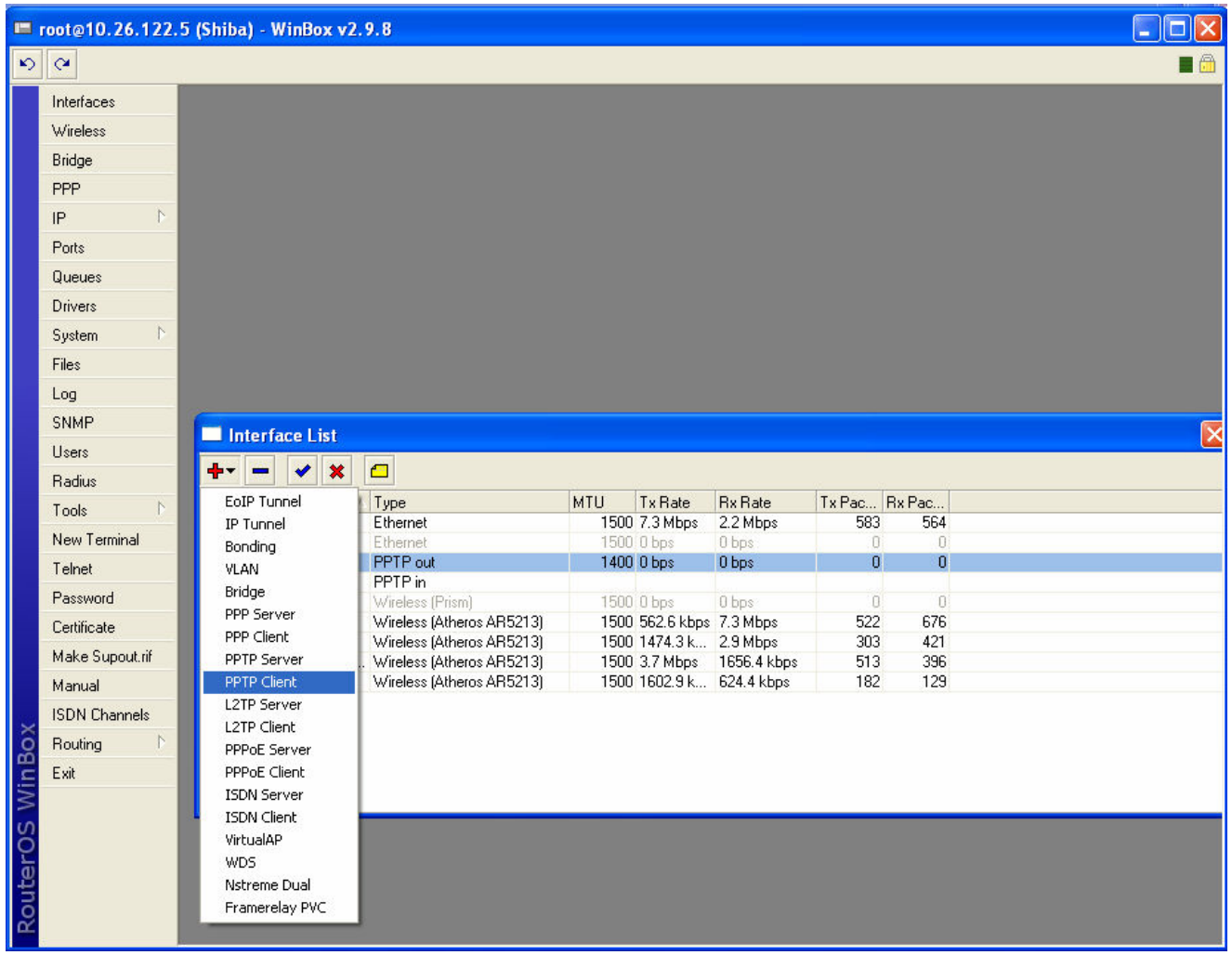
Κρυπτογράφηση (Encryption)

Το L2TP μήνυμα κρυπτογραφείται με αλγόριθμους DES και 3DES χρησιμοποιώντας κλειδιά κρυπτογράφησης τα οποία παράογνται από την διαδικασία αυθεντικοποίησης του IPSec

•Επίσης είναι δυνατή μία PPTP σύνδεση χωρίς κρυπτογράφηση αλλά δεν συστήνεται για λόγους ασφαλείας

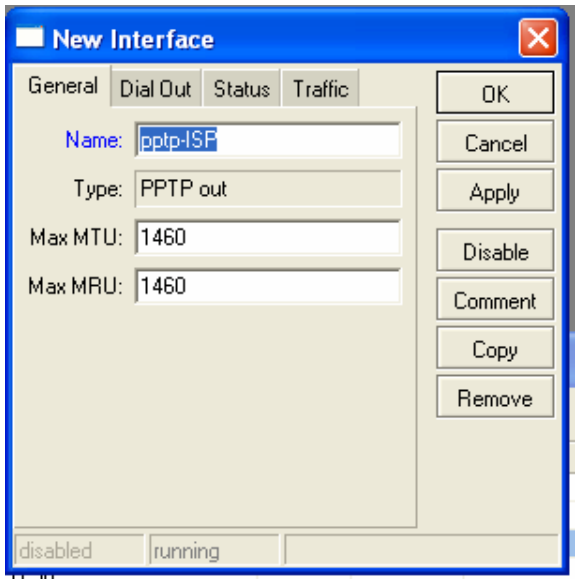
Δημιουργία PPTP σύνδεσης

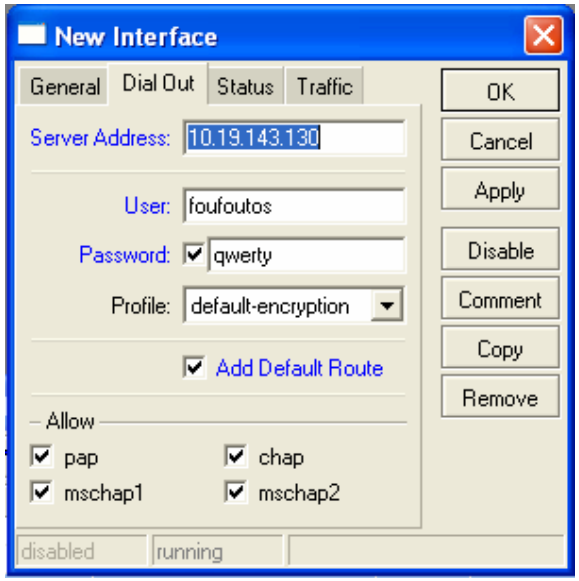
Interfaces → κουμπάκι + → pptp client

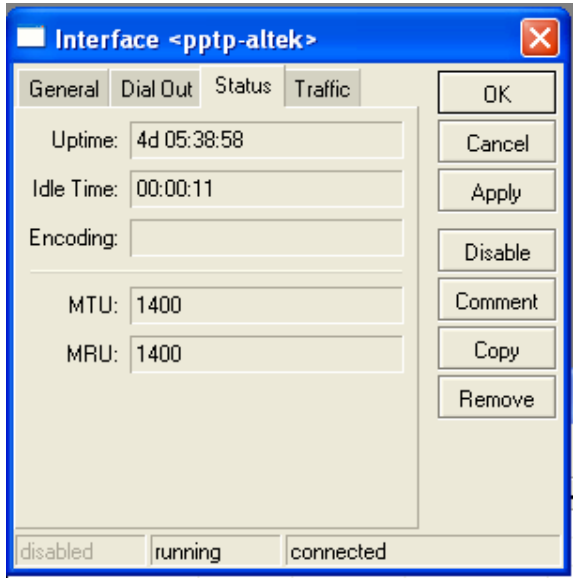


Δημιουργία PPTP σύνδεσης

- **General**: Βάζουμε ένα όνομα για τη σύνδεση
- **Dial Out**: Βάζουμε την ip του VPN server, το user/pass για τη σύνδεση. Τικάρουμε το Add Default Route, ώστε όταν αποκατασταθεί η PPTP σύνδεση να προστεθεί η default διαδρομή
- **Status**: Μας δίνει την κατάσταση της σύνδεσης
- **Traffic**: Κίνηση διαμέσω της σύνδεσης



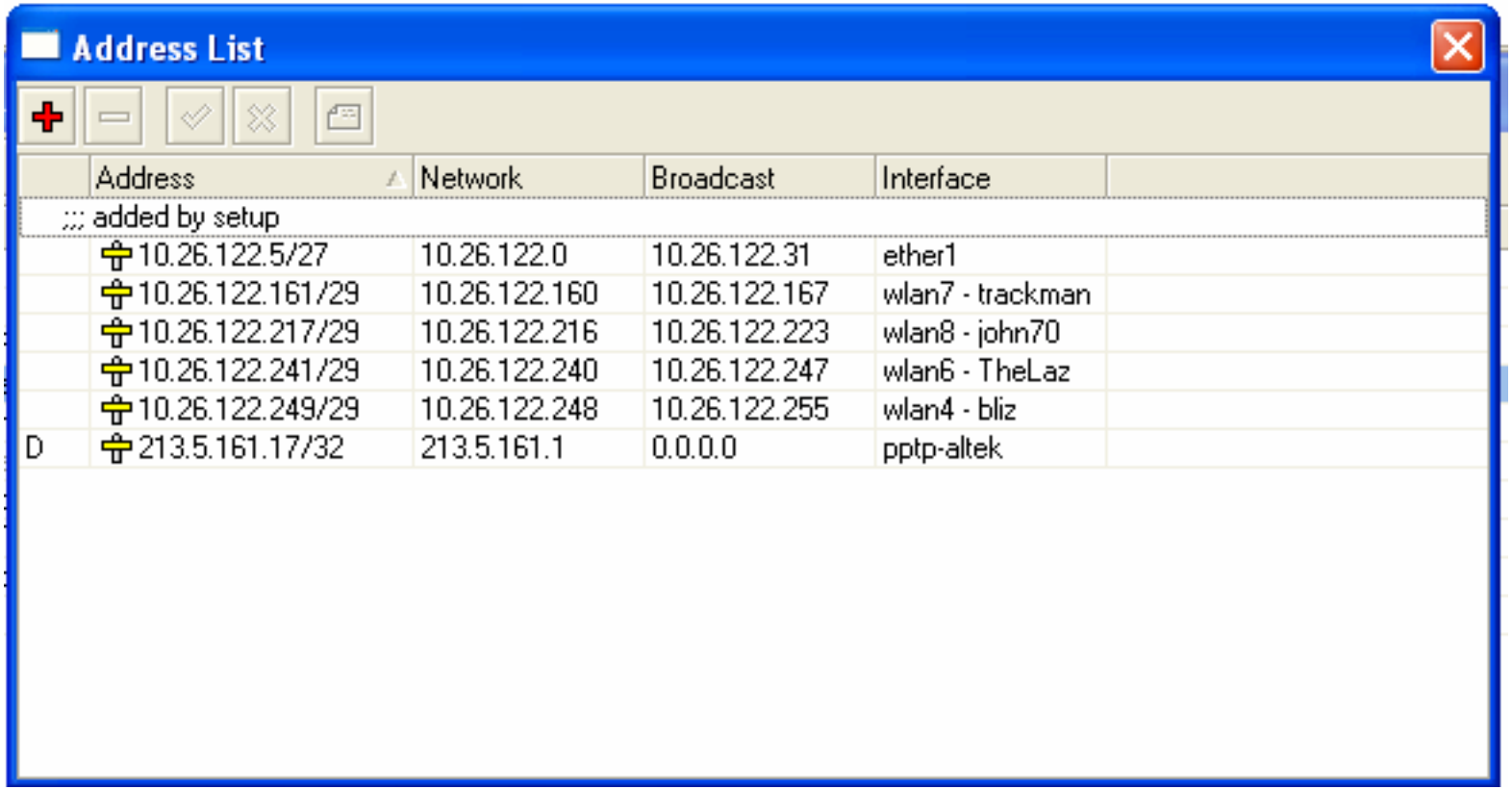




Δημιουργία PPTP σύνδεσης

Ip → addresses

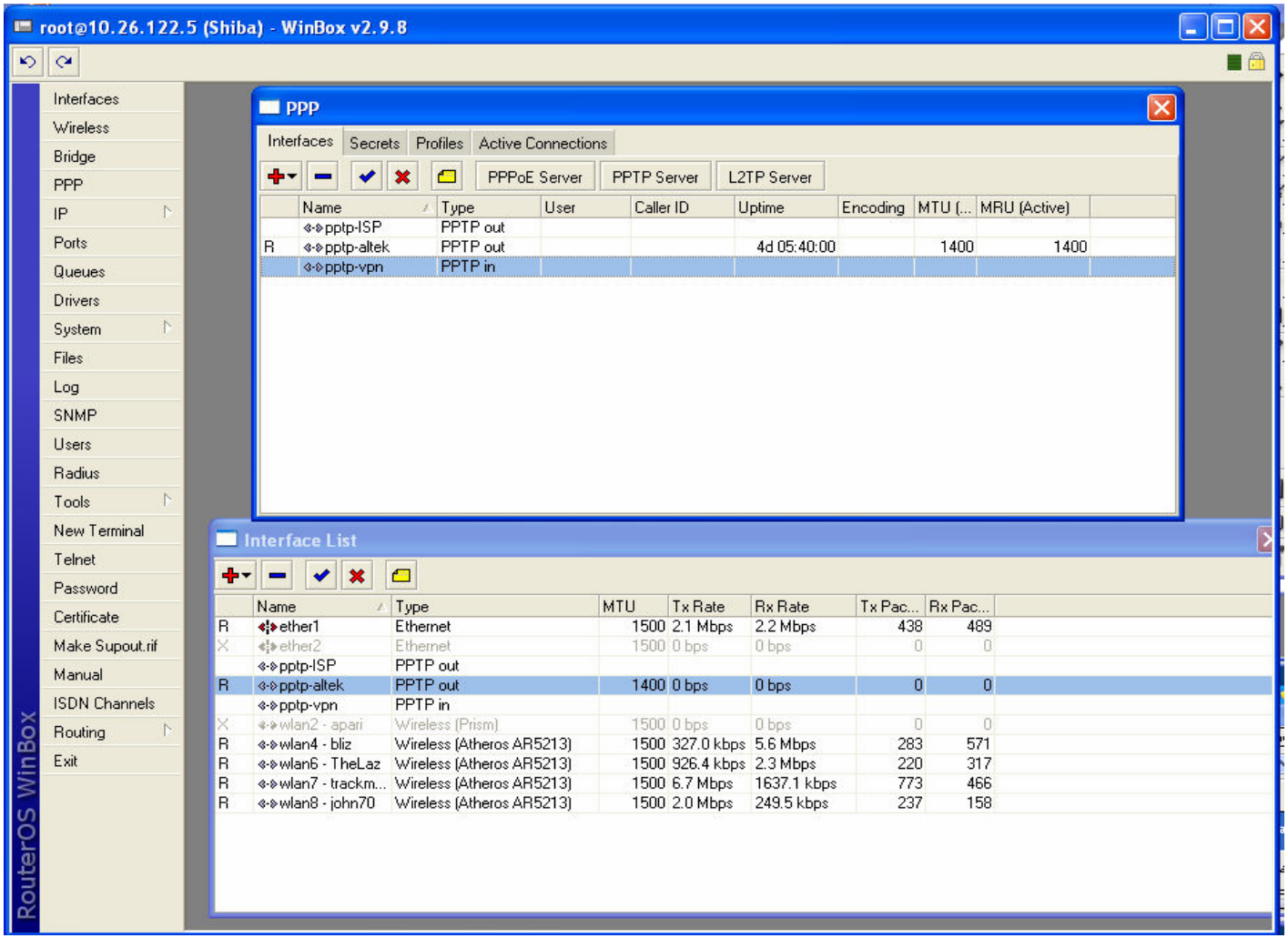
•Παρατηρούμε την νέα ip που μας έχει δώσει ο pptp server



Δημιουργία PPTP σύνδεσης

PPP / Interfaces

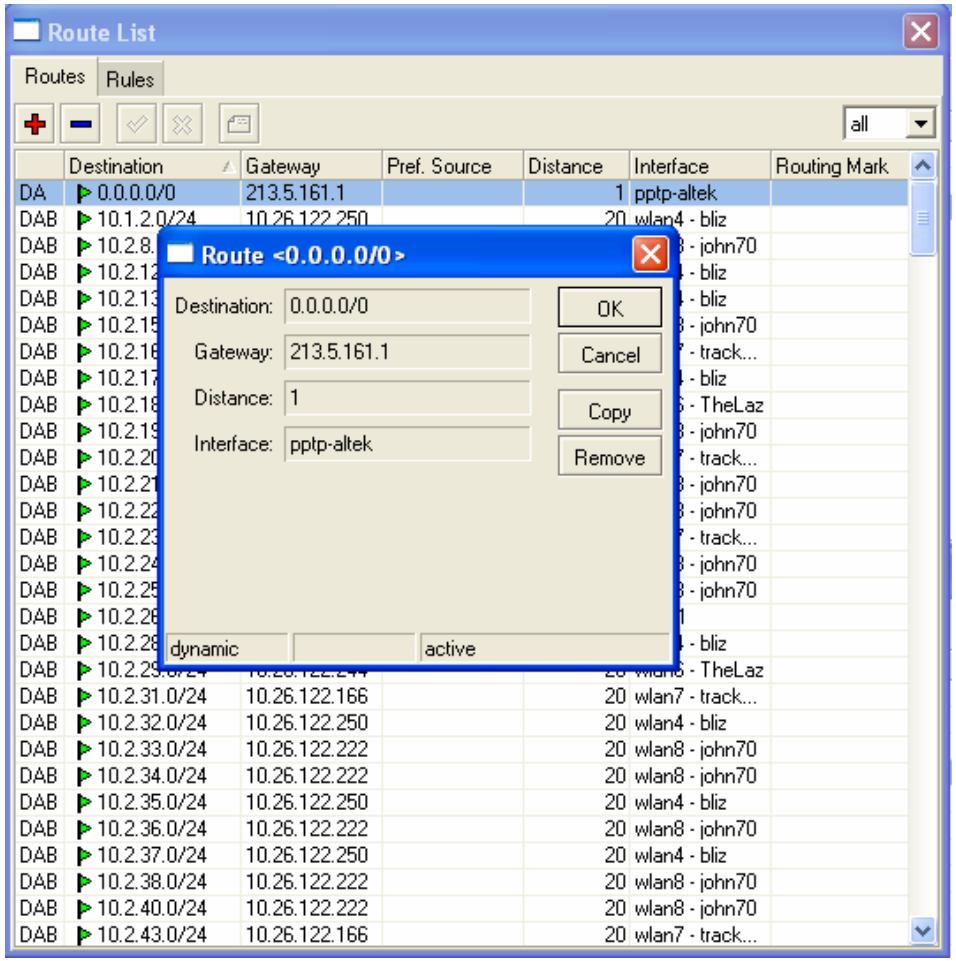
•Παρατηρούμε τα νέα pptp interfaces



Δημιουργία PPTP σύνδεσης

Ip → route

•Παρατηρούμε ότι έχει προστεθεί αυτόματα η default διαδρομή




Firewall

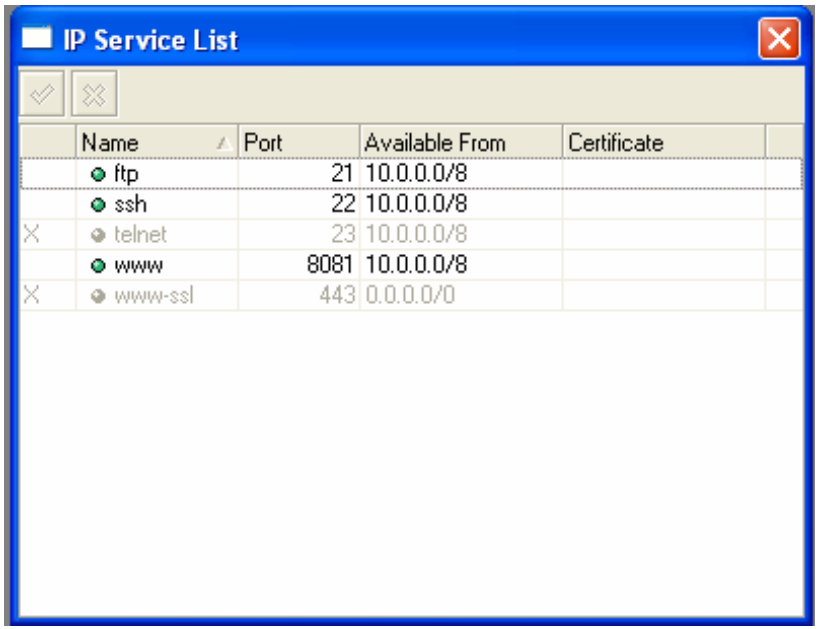
Ασφάλεια

Με το που εκτεθεί η μηχανή στο internet , πρέπει να φροντίσουμε για την ασφάλεια της

Ip → services

•Απενεργοποιούμε το **telnet** καθότι δεν είναι ασφαλές πρωτόκολλο

•Αν δεν τα χρειαζόμαστε απενεργοποιούμε και τα ssh και ftp , αφήνοντας ίσως μόνο το **www** που είναι απαραίτητο για το winbox



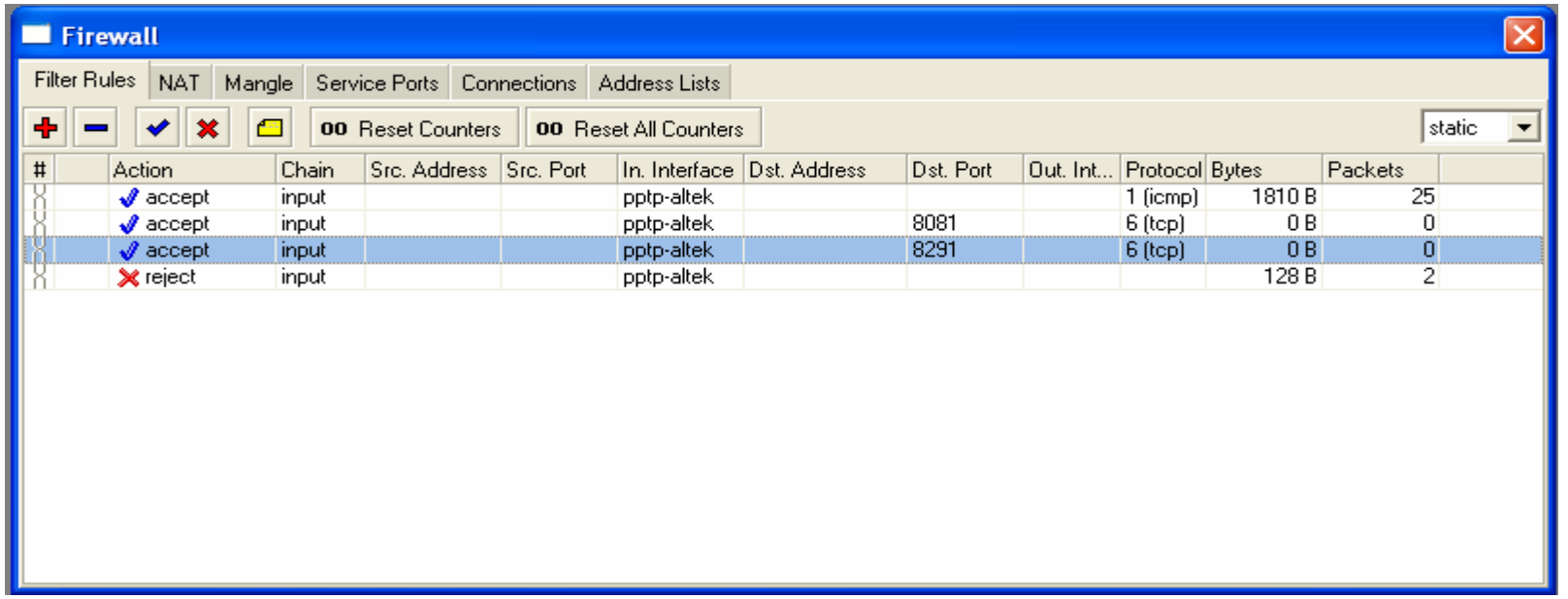
Ασφάλεια

Ip → Firewall → Filter Rules

•Προσθέτουμε κανόνες σχετικά με τη κίνηση επιτρέπουμε

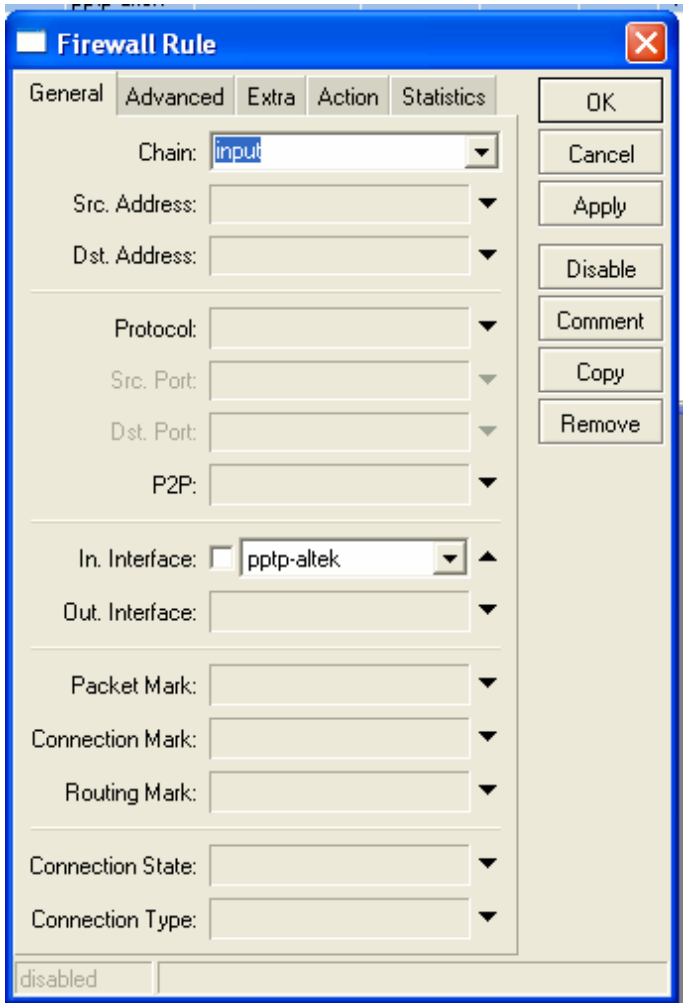
•Οι κανόνες είναι μέρος μιας **αλυσίδας** η οποία ενεργεί από **πάνω προς τα κάτω**

•Τα πακέτα περνάνε **διαδοχικά** τους κανόνες της αλυσίδας, αν ταιριάζουν τα κριτήρια τότε γίνεται μία **ενέργεια** (πχ drop) διαφορετικά εξετάζεται ο **επόμενος** κανόνας



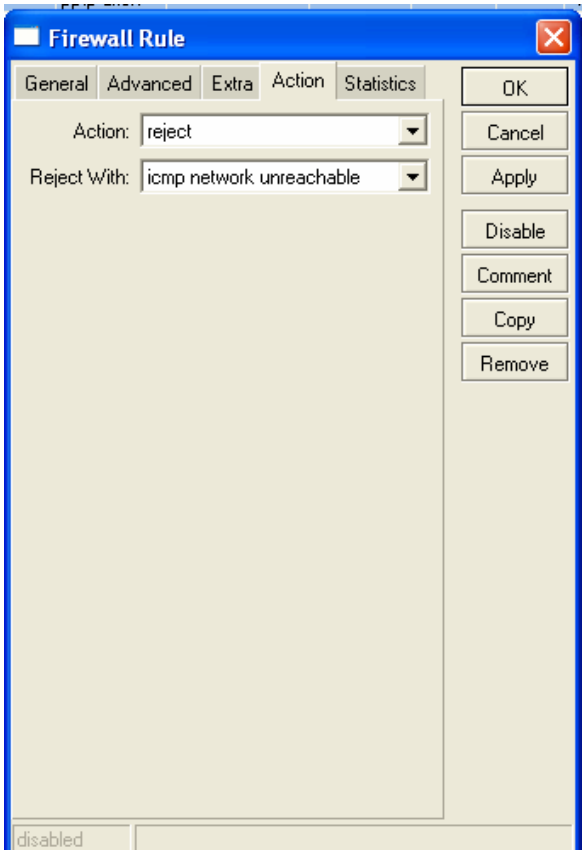
Αλυσίδα (Chain)

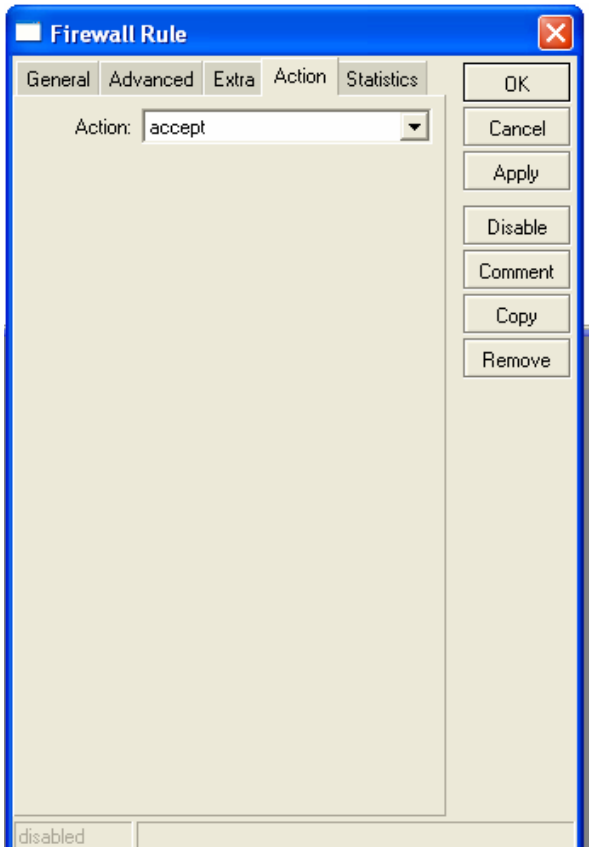
•Η αλυσίδα στην οποία εφαρμόζεται ο κανόνας, η **input** αναφέρεται στην κίνηση που έχει προορισμό την τοπική μηχανή, η **forward** στην κίνηση που προωθείται και η **output** σε αυτή που έχει αφετηρία την τοπική μηχανή.
•Για να προστατέψουμε τη μηχανή μας εφαρμόζουμε κανόνες στην **Input** αλυσίδα
•Για να προστατέψουμε το τοπικό μας δίκτυο αλλά και το υπόλοιπο δίκτυο από το τοπικό μας δίκτυο μπορούμε να εφαρμόσουμε κανόνες στην **forward** αλλά με **in/out interface το τοπικό μας δίκτυο**
•**Τα δεδομένα τα οποία προωθούμε δεν θα πρέπει να τα επηρεάζουμε**, διότι αυτό είναι ενάντια στους κανόνες καλού firewalling (ανούσιο να γίνεται έλεγχος σε όλους τους ενδιάμεσους routers) αλλά και γιατί δημιουργούμε πρόβλημα στην **διάφανη και ανεμπόδιστη προώθηση δεδομένων**



Ενέργεια (Action)

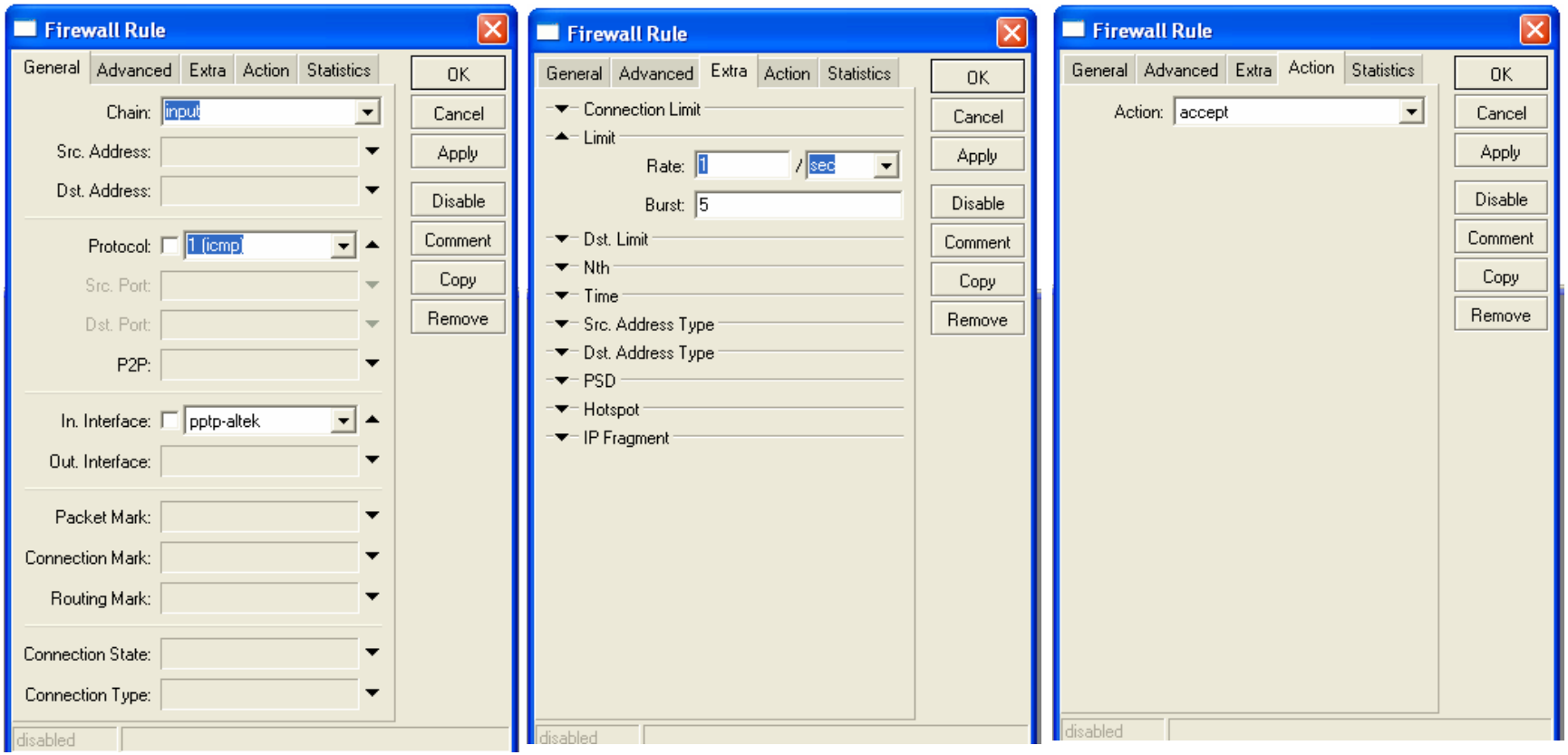
•Η ενέργεια που θα συμβεί όταν **ταιριάξουν** τα κριτήρια
•Μπορεί να είναι **accept**, δηλαδή αποδοχή του πακέτου και έλεγχος του επόμενου κανόνα της αλυσίδας κτλ, **drop** δηλαδή το πακέτο απορρίπτεται ξερά και δεν εξετάζονται επόμενοι κανόνες, ή **reject** όπου απορρίπτεται το πακέτο δεν εξετάζονται επόμενοι κανόνες αλλά στέλνεται αιτιολόγηση





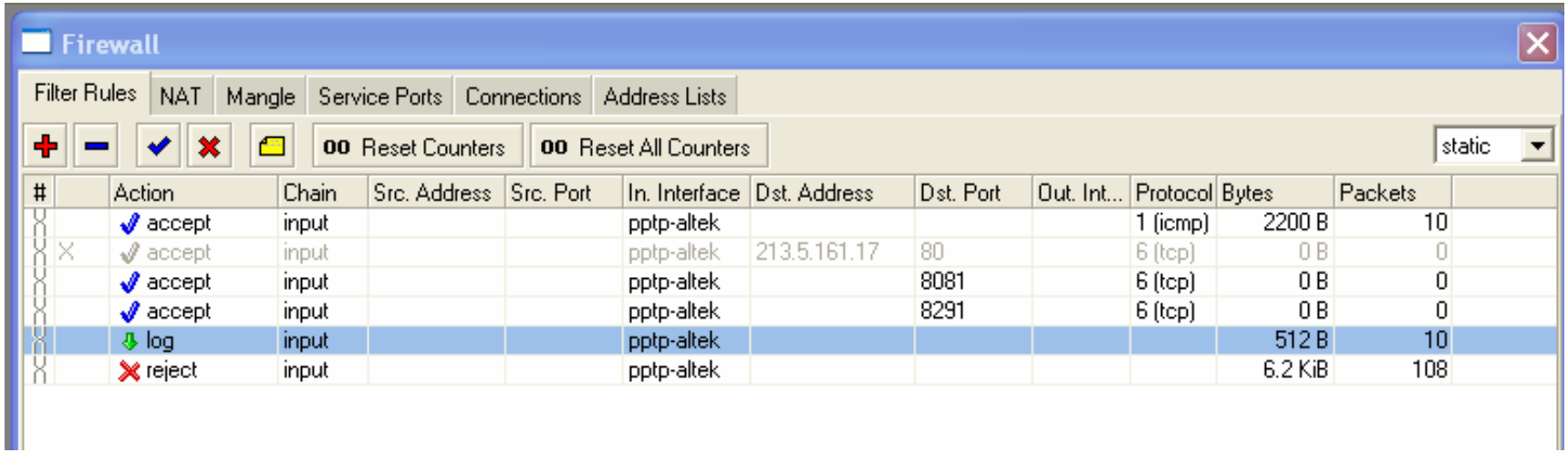
Κανόνας για τα ICMP:

- Τα ICMP πακέτα **δεν τα κόβουμε ποτέ**
- Φτιάχνουμε ένα κανόνα που τα επιτρέπει απλά **περιορίζουμε** τα ρυθμό τους σε ένα το δευτερόλεπτο, αφήνωντας τη δυνατότητα να σταλούν μέχρι 5 σε ριπή
- Με αυτό τον τρόπο δεν θα έχουμε πρόβλημα σε κάποιο **ping flood**



Παράδειγμα

•Στο παράδειγμα έχουμε επιτρέψει τα **icmp**, τις πόρτες **8081** και **8291** ώστε να είναι διαχειρίσιμο το mt μέσω **winbox**
•Παρατηρείστε τον τελευταίο κανόνα που απλά **απορρίπτει** όλα τα υπόλοιπα πακέτα και τον προτελαυταίο ο οπόιο **καταγράφει** όλα τα υπόλοιπα πακέτα
•Το παραπάνω είναι παράδειγμα αυστηρής πολιτικής αφού έχουμε αφήσει **πολύ συγκεκριμένα και λίγα πράγματα τα οποία γνωρίζουμε καλά.**
•Αν αντιμετωπίσουμε πρόβλημα ασφάλειας θα προέρχεται από πρόβλημα στις υπηρεσίες που αφήσαμε ανοικτές
•Στο πεδίο Bytes παρατηρούμε την κίνηση η οποία απορρίφθηκε



Παράδειγμα

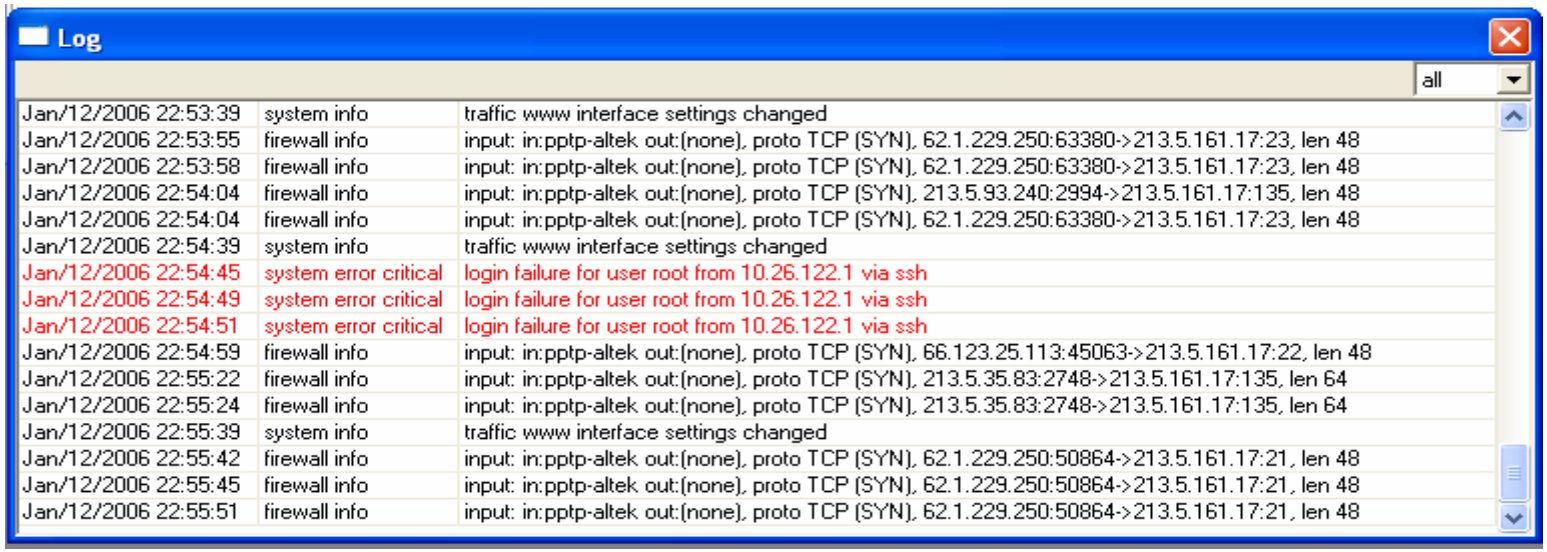
•Παρατηρούμε στο Log ότι καταγράφηκε η κίνηση η οποία απορρίφθηκε από το firewall

•Συγκεκριμένα αφορούσε προσπάθεια telnet, ssh και ftp

•Είναι ιδιαίτερα σημαντικό να προστατέψουμε όποιο μηχάνημα εκτίθεται στο internet, αλλά και να προστατέψουμε το Internet από τα δικά μας μηχανήματα (αν μας πάρουν το μηχάνημα θα το χρησιμοποιήσουν για να πάρουν και άλλα)

•Χαρακτηριστικά σημειώνουμε ότι μόλις μέσα **σε ένα λεπτό** από τη στιγμή που σηκώσαμε το VPN και πήρε η μηχανή πραγματική διεύθυνση παρατηρήσαμε δεκάδες προσπάθειες login

•Ένα **telnet** ανοικτό ή ένα ssh με **εύκολο pass** και θα μας έχουν πάρει το μηχάνημα σε ελάχιστο χρόνο.

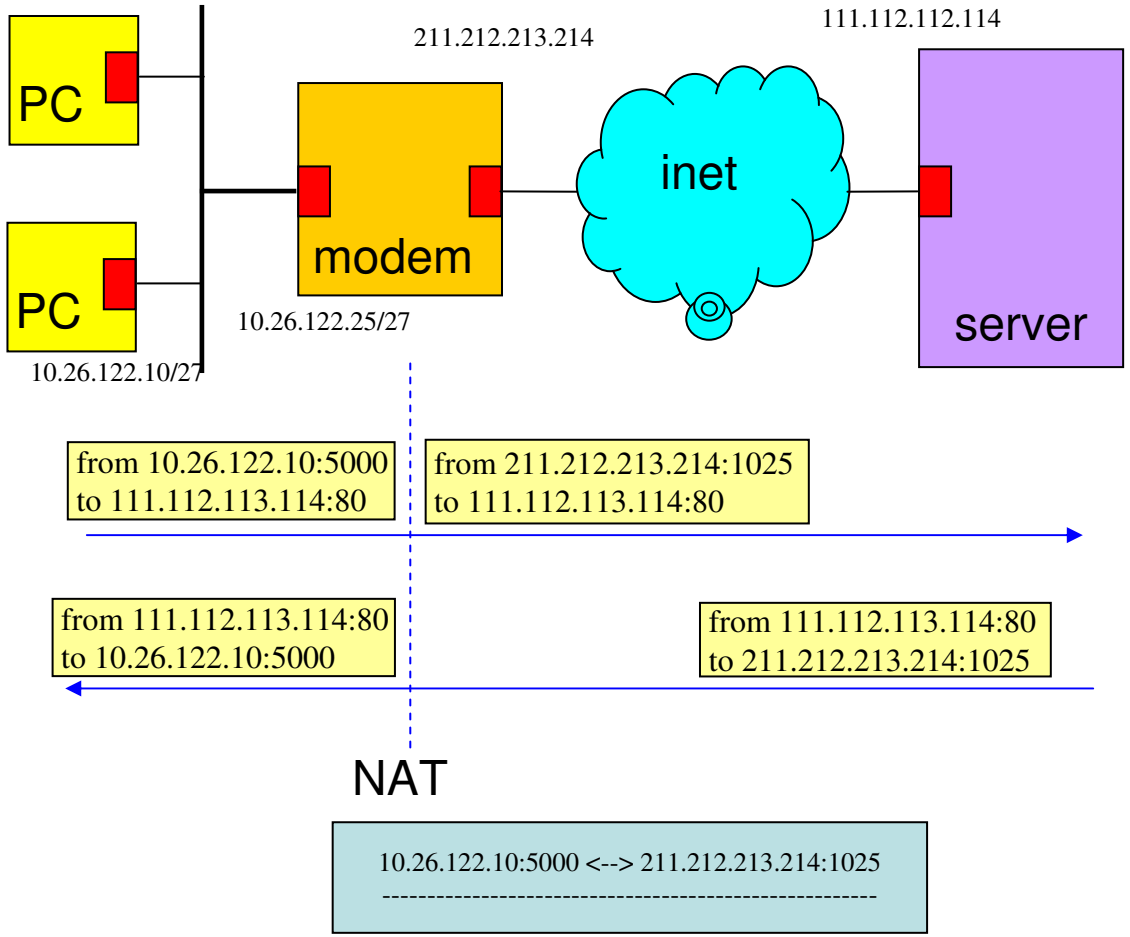



NAT

Source NAT

•Απεικονίζει όλες τις πηγαίες **ιδιωτικές** διευθύνσεις σε μία **δημόσια**, κάνοντας έτσι οικονομία σε IP διευθύνσεις
•Για τα εξερχόμενα πακέτα από το NAT πρωτόκολλο, η πηγαία (ιδιωτική) IP διεύθυνση απεικονίζεται στην διεύθυνση που έχει αποδοθεί από τον ISP (δημόσια) και οι TCP/UDP πόρτες αλλάζουν σε κάποια διαφορετική
•Για τα εισερχόμενα πακέτα στο NAT πρωτόκολλο, η διεύθυνση προορισμού απεικονίζεται στην αρχική ιδιωτική διεύθυνση και οι TCP/UDP πόρτες αλλάζουν πίσω στις αρχικές τους τιμές
•Για την απεικόνιση πολλών διευθύνσεων στην μία χρησιμοποιούνται δυναμικά επιλεγμένες TCP και UPD πόρτες, προκειμένου να **ξεχωρίζουν οι απεικονίσεις**.
•Για τη λειτουργία του το NAT πρωτόκολλο διατηρεί πίνακα μετάφρασης

Source NAT, παράδειγμα



Source NAT, παράδειγμα

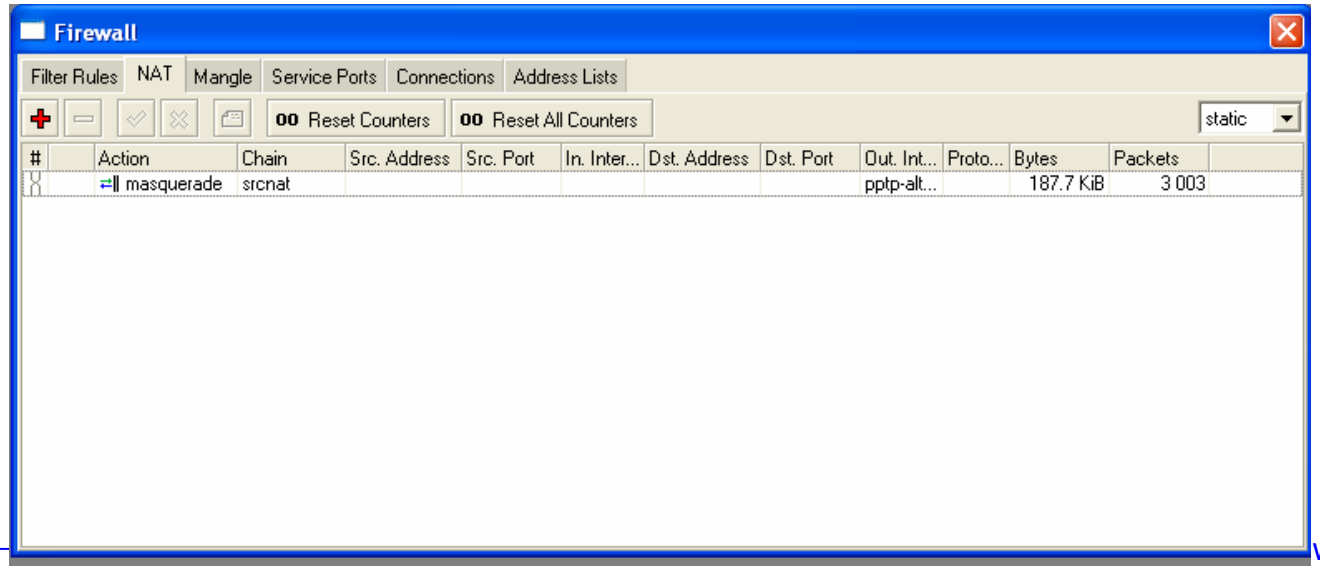
•Έστω το οικιακό τοπικό μας δίκτυο είναι το 10.26.122.0/27
•Στο modem μας έχει αποδοθεί μια δημόσια διεύθυνση 211.212.213.214 από τον ISP μας
•Έστω ότι ο υπολογιστής 10.26.122.10 ζητά να συνδεθεί σε έναν Web server στην 111.112.113.114
•Το modem μεταφράζει την πηγαία διεύθυνση 10.26.122.10 στην δημόσια 211.212.213.214, αλλάζοντας και την πηγαία πόρτα από 5000 σε 1025
•Παράλληλα καταχωρεί σε ένα πίνακα μετάφρασης την αντιστοιχία, προκειμένου να μπορεί να κάνει την αντίστροφη διαδικασία
•Το μεταφρασμένο IP πακέτο στέλνεται στο διαδίκτυο, και ο web server στέλνει πίσω την απάντηση.
•Το NAT πρωτόκολλο κοιτώντας τον πίνακα μετάφρασης, αλλάζει την διεύθυνση προορισμού του ληφθέντος πακέτου από 211.212.213.214 σε 10.26.122.10 και την πόρτα προορισμού από 1025 σε 5000

IP Masquarading

•Το IP masquerading είναι ιδιαίτερα χρήσιμο αν έχουμε 1 σταθερή σύνδεση με το διαδίκτυο που θέλουμε να διαμοιράσουμε στο δίκτυο μας χωρίς περιορισμούς. Για τους σκοπούς αυτού του οδηγού θεωρούμε ότι υπάρχει μία διασύνδεση με το διαδίκτυο και την περάσαμε στα IF του Mikrotik μέσω Ethernet / VPN με τον router μας κτλπ.

•Το masquerading είναι **source NAT** που είδαμε προηγούμενα, με τη διαφορά ότι δεν χρειάζεται να δώσουμε την ιντερνετική ip αλλά απλά το interface και η ip **επιλέγεται δυναμικά**, το οποίο προφανώς μας βολεύει.

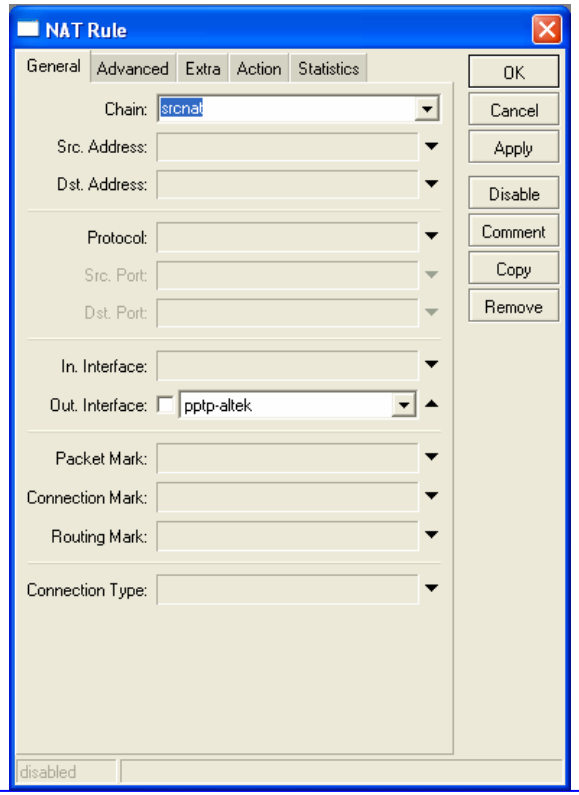
•Επιλέγουμε IP➔ Firewall και κάνουμε κλικ.

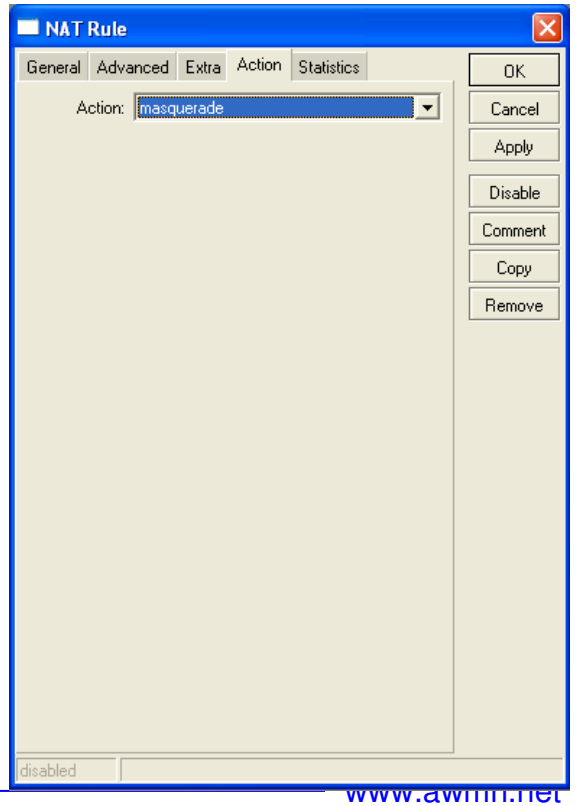


IP Masquarading

•Επιλέγουμε την καρτέλα **NAT** και πατάμε το **+**.
•Στην καρτέλα **General** συμπληρώνουμε τα **chain srcnat** και το **out. Interface** βάζοντας το μέσω σύνδεσης του διαδικτύου π.χ. την IP της Ethernet από DSL modem (ether2)
•Στην καρτέλα Action και επιλέγουμε το **masquerade**. Πατάμε OK και είμαστε έτοιμοι. **Τα Pc του δικτύου μας με τις 10αρες IP βγαίνουν κανονικά στο Internet**.

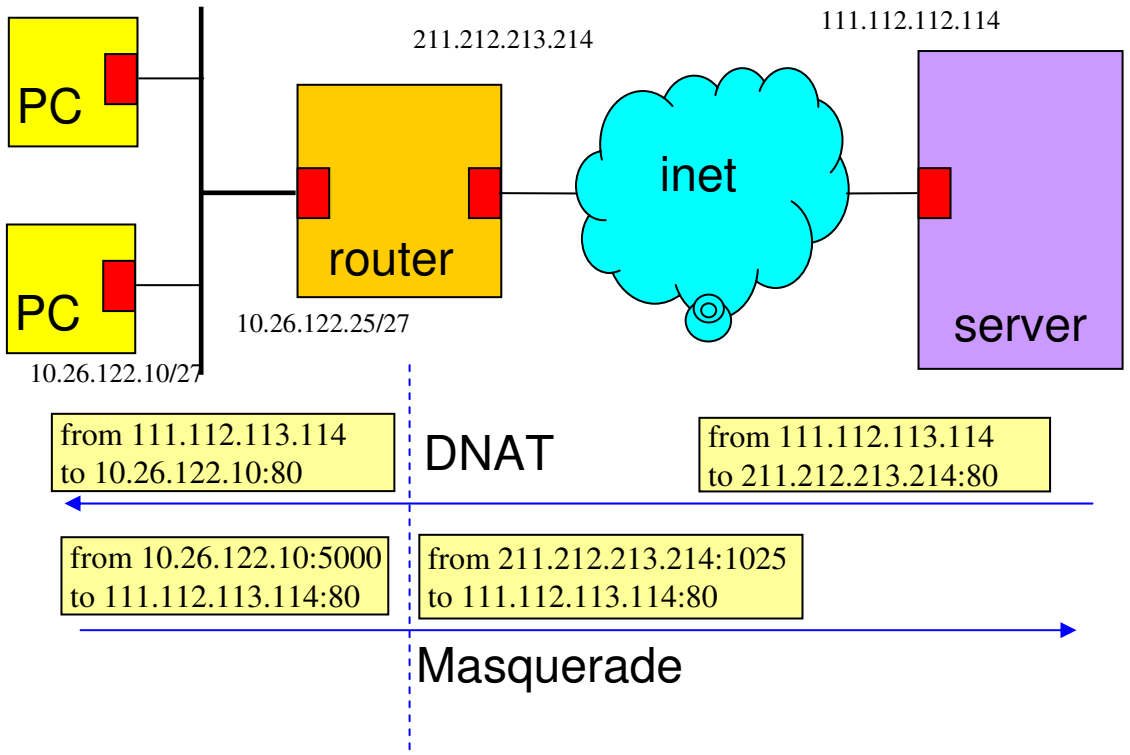
•Εδώ out interface επιλέξαμε το if που έχει πάνω του την πραγματική Ip, στην περίπτωση μας ένα pptp tunel που έχουμε με έναν provider





DNAT (Destination Nat)

•Αναφέραμε πως μπορούμε με το μασκάρεμα να δώσουμε πρόσβαση στο Inet σε πολλές ιδιωτικές διευθύνσεις
•Έστω ότι θέλουμε να δώσουμε πρόσβαση σε συγκεκριμένη υπηρεσία (HTTP, FTP server, SSH κτλ) σε κάποια μηχανή μας που έχει ιδιωτική διεύθυνση , από το internet



DNAT (Destination Nat)

•Παρατηρούμε την αίτηση προς την 111.112.113.114:80 του δρομολογητή μας
•Στη συνέχεια αυτός αλλάζει τον προορισμό του πακέτου προς τον 10.26.122.10:80, κοιτά τον πίνακα δρομολόγησης του και στέλνει το πακέτο στη σωστή διεπαφή
•Ο HTTP server 10.26.122.10 απαντά στην αίτηση στέλνοντας απάντηση προς το αρχικό προορισμό
•Ο δρομολογητής κάνει μασκάρεμα της διεύθυνσης πηγής με την δική του internetική διεύθυνση

DNAT (Destination Nat)

IP➔ Firewall→NAT→ πατάμε το +

General

Chain: dstnat

Dst Address: την ιντερνετική ip του δρομολογητή

Protocol, Dst Port : ανάλογα με την υπηρεσία που θέλουμε να βγάλουμε έξω

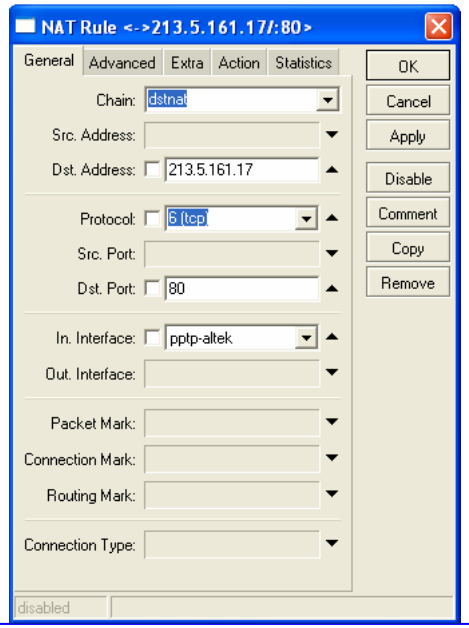
In Interface : Η εισερχόμενη θύρα

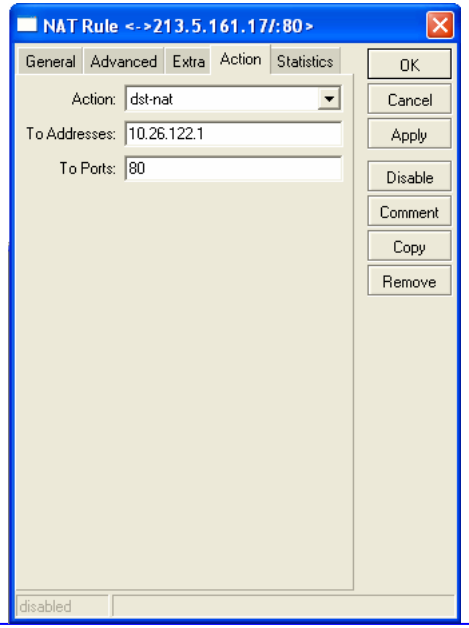
Action

Action: dst-nat

To address: διεθύνση στην οποία θα αλλάξει η αρχική διεύθυνση προορισμού

To Ports: θύρες στις οποίες θα αλλάξει η θύρα προορισμού





DNAT (Destination Nat)

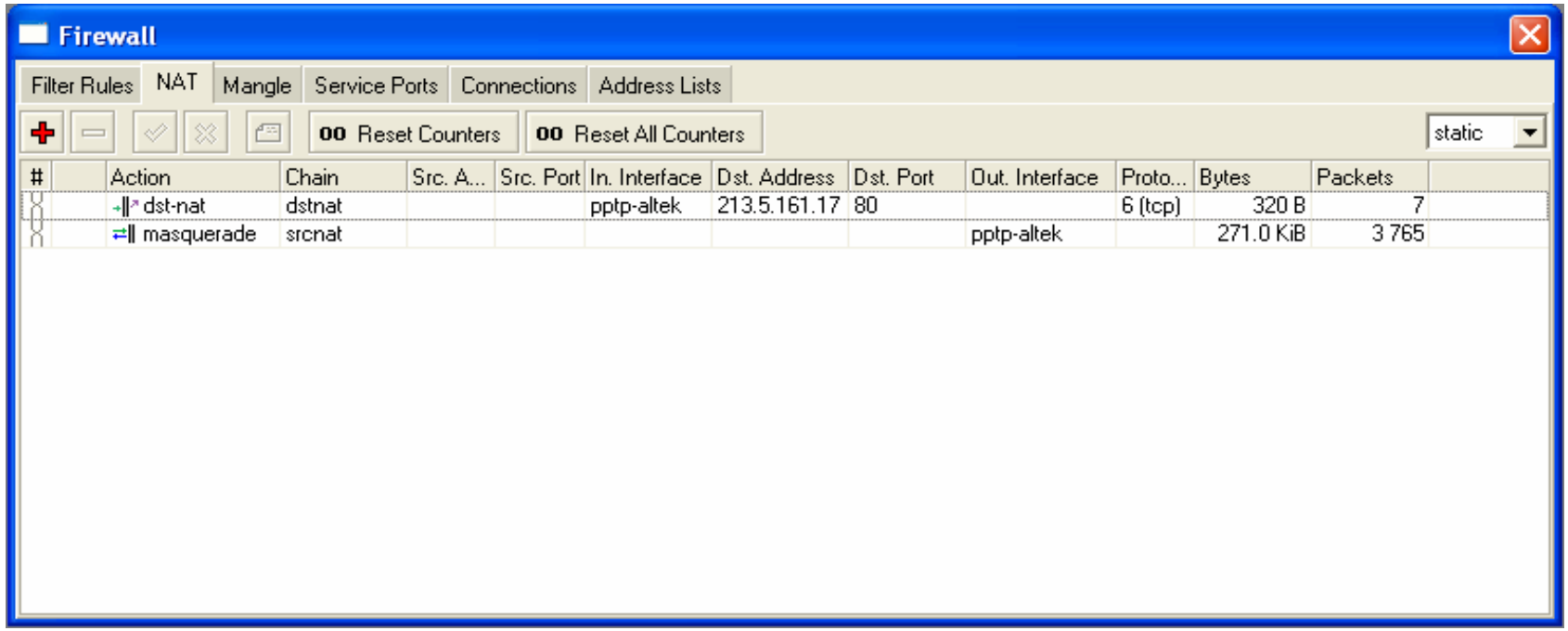
•Προσθέτουμε και τον κανόνα για το masquerade και έχουμε τελειώσει

•Όλες οι αιτήσεις προς την 213.5.161.17:80 κατευθύνονται στην 10.26.122.10:80 και ο WEB server που υπάρχει εκεί είναι προσβάσιμος και στο Internet

•Το μόνο που λείπει είναι να πρστεθεί μία εγγραφή για την internetική μας IP προκειμένου να μπορούμε να χρησιμοποιούμε κάποιο domain

•Παρατηρούμε ότι παρόλο που στο firewall δεν ανοίξαμε την 80 θύρα η κίνηση περνάει.

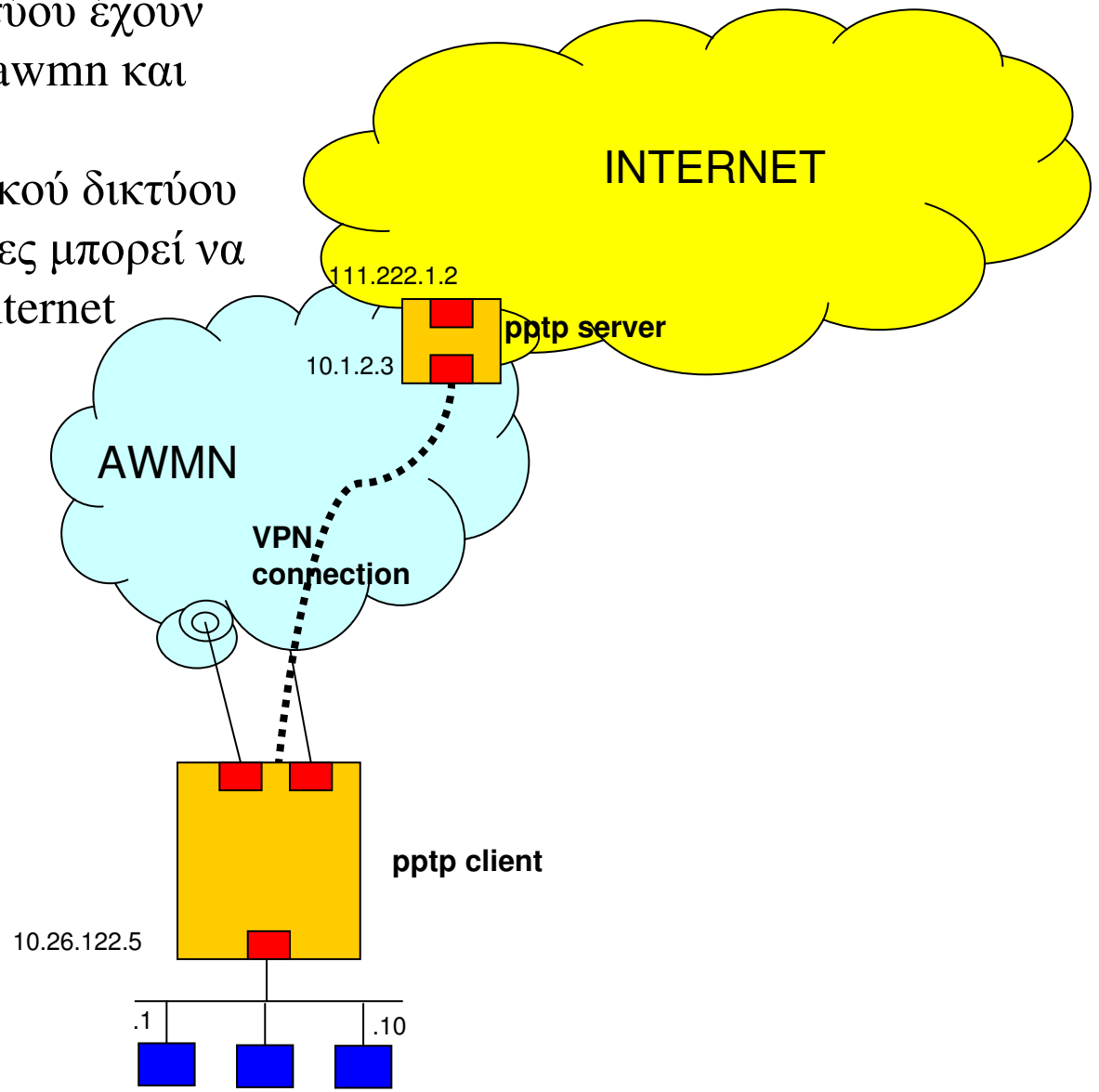
•Τούτο συμβαίνει διότι οι κανόνες firewall που εφαρμόσαμε αναφέρονται σε input αλυσίδα, ενώ αυτή η κίνηση είναι forward



Παράδειγμα

•Όλα τα pc του τοπικού δικτύου έχουν πρόσβαση μέσω του .5 στο awmn και στο internet

•Ο .1 είναι ο server του τοπικού δικτύου του οποίου κάποιες υπηρεσίες μπορεί να είναι προσβάσιμες από το Internet



•Τα παραπάνω είναι τεχνολογίες που απαντάμε και χρησιμοποιούμε στο internet, είναι το internet.
•Σε ένα δίκτυο σαν το awmn, εκμεταλλευόμενοι λειτουργικάκια σαν το mikrotik, μπορούμε εύκολα και γρήγορα να γίνουμε συμμέτοχοι στη γνώση και στις υπηρεσίες και όχι απλά χρήστες του τέρατος που λέγεται internet