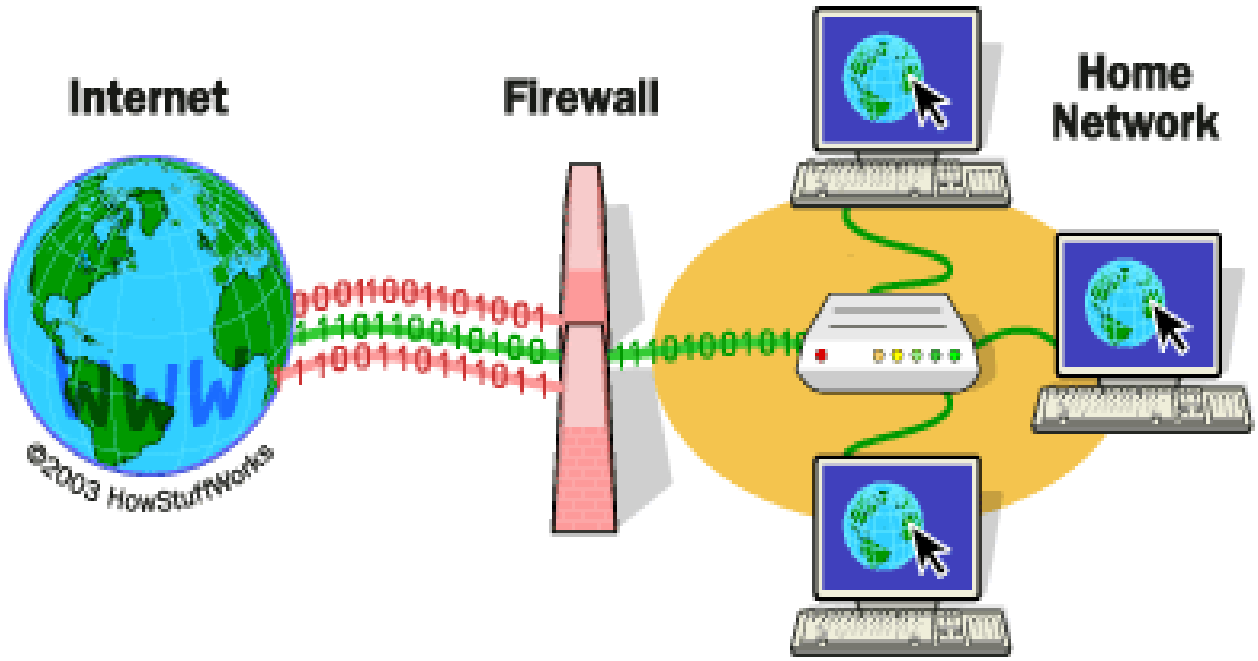
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΣΕΡΡΩΝ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ

ΜΕΛΕΤΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ FIREWALL OTENET SECURITY KIT

ΜΕΛΕΤΗ ΤΩΝ ΤΕΧΝΙΚΩΝ FIREWALL ΜΕ ΒΑΣΗ ΤΟ LINUX-IPTABLES.



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ των ΚΑΡΑΝΙΚΑ ΒΑΣΙΛΙΚΗ & ΑΝΑΣΤΑΣΙΟΥ ΕΥΑΓΓΕΛΙΑ
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΚΥΡΙΟΣ ΕΥΑΓΓΕΛΟΣ ΠΑΠΑΡΓΥΡΗΣ

ΣΕΡΡΕΣ 2008

ΠΕΡΙΛΗΨΗ

Η διαδεδομένη χρήση του Internet στις επιχειρήσεις και γενικά στην καθημερινή ζωή του ανθρώπου έχει καταστήσει αναγκαία τη χρήση ενός εργαλείου για την προστασία του τοπικού μας δικτύου από τους κακόβουλους χρήστες του internet που επιχειρούν να εισβάλουν στο σύστημα μας και να το βλάψουν με διάφορους τρόπους. Τα εργαλεία αυτά ονομάζονται **firewall**. Υπάρχουν διάφοροι τύποι firewall που μπορούμε να χρησιμοποιήσουμε ανάλογα με τις εκάστοτε ανάγκες.

Το πρόβλημα της πρόσβασης μη εξουσιοδοτημένων χρηστών στον προσωπικό μας υπολογιστή ή στο τοπικό επιχειρηματικό μας δίκτυο είναι πολύ σοβαρό και έχει απασχολήσει πολύ τους επιστήμονες της πληροφορικής και γι’ αυτό το λόγο έχουν αναπτυχθεί πολλά εργαλεία – firewall για την αντιμετώπιση του.

Στην παρούσα εργασία θα μελετήσουμε δύο από αυτά, το πρώτο είναι το Otenet Security Kit, ένα σύστημα το οποίο είναι διαθέσιμο στο internet και το δεύτερο είναι ένα εργαλείο που μας παρέχει το Linux (έκδοση 2.4 και νεότερες) και ονομάζεται Netfilter-Iptables.

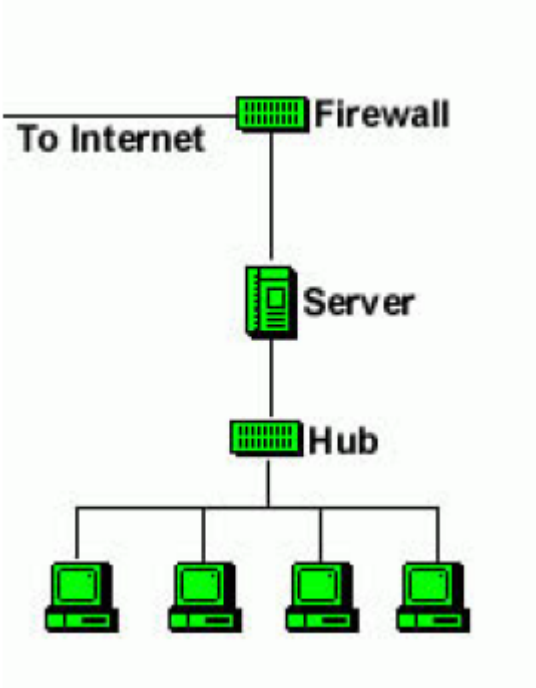
1. ***ΓΕΝΙΚΑ ΓΙΑ ΤΑ FIREWALL***

Τι είναι τα firewalls.

Η χρήση του Internet έχει πλέον διαδοθεί σε τέτοιο βαθμό ώστε είναι απαραίτητη σε κάθε άνθρωπο για την αντιμετώπιση καθημερινών αναγκών. Η αμεσότητα και η ταχύτητα που προσφέρει στις επικοινωνίες είναι μοναδικά πλεονεκτήματα τα οποία κυρίως εκμεταλλεύονται οι επιχειρήσεις για την επικοινωνία τους με τον «έξω κόσμο». **Αποστολή mail, χρήση FTP, on- line τεχνική υποστήριξη, αναζήτηση πληροφοριών, ηλεκτρονικό εμπόριο**, είναι μόνο μερικά από τα πλεονεκτήματα που προσφέρει το διαδίκτυο στις μεγάλες και μικρές επιχειρήσεις.

Όταν όμως μια εταιρεία συνδέει το εσωτερικό επιχειρηματικό της δίκτυο με το Internet αντιμετωπίζει ορισμένους κινδύνους: Εξαιτίας της ανοιχτής δομής του Internet, κάθε επιχειρηματικό δίκτυο που είναι συνδεδεμένο σ' αυτό είναι εκτεθειμένο σε επιθέσεις. Οι κακόβουλοι χρήστες του Internet μπορούν να εισέλθουν στο επιχειρηματικό δίκτυο και να προκαλέσουν ζημιά με διάφορους τρόπους: να κλέψουν ή να καταστρέψουν σημαντικά δεδομένα, να προκαλέσουν ζημιά σε ανεξάρτητους υπολογιστές ή σε ολόκληρο το δίκτυο, όπως π.χ. να χρησιμοποιήσουν τους πόρους των επιχειρηματικών υπολογιστών. Η λύση δεν είναι η αποκοπή του εσωτερικού επιχειρηματικού δικτύου από το Internet, αλλά η χρήση ειδικών προγραμμάτων και συσκευών, των γνωστών σε όλους μας firewall. Η χρήση των firewall εμποδίζει το δίκτυο της εταιρείας να προσεγγίσει το Internet, και το Internet να προσεγγίσει το προστατευόμενο δίκτυο της εταιρείας. Για κάποιον που θέλει να επικοινωνήσει με το Internet μέσα από το προστατευόμενο δίκτυο, πρέπει να κάνει σύνδεση μέσα από το firewall και να χρησιμοποιήσει

το Internet από εκεί. Τα firewalls επιτρέπουν στους υπαλλήλους της επιχείρησης να έχουν πρόσβαση στο Internet και ταυτόχρονα εμποδίζουν τους επίδοξους εισβολείς να αποκτήσουν πρόσβαση στο επιχειρηματικό δίκτυο και να προκαλέσουν ζημιές. Οποιοδήποτε αίτημα προς τα έξω καθώς επίσης και οποιαδήποτε απάντηση προς τα μέσα περνάει πρώτα από το firewall. Αυτό αποφασίζει, με βάση ένα σύνολο κανόνων που έχουν τεθεί από πριν, αν θα προωθήσει τα δεδομένα και αν θα απαντήσει ή όχι.



Εικόνα 1 - FIREWALL

Τι είναι όμως τα firewalls;

Τα **firewalls** αποτελούν συνδυασμούς hardware (υλικό) και software (λογισμικό). Τα firewalls τοποθετούνται στο πιο ευπαθές σημείο μεταξύ του επιχειρηματικού δικτύου και του Internet και μπορεί να είναι από απλά ως εξαιρετικά πολύπλοκα συστήματα.

Εικόνα 2 - FIREWALL: Τείχος προστασίας

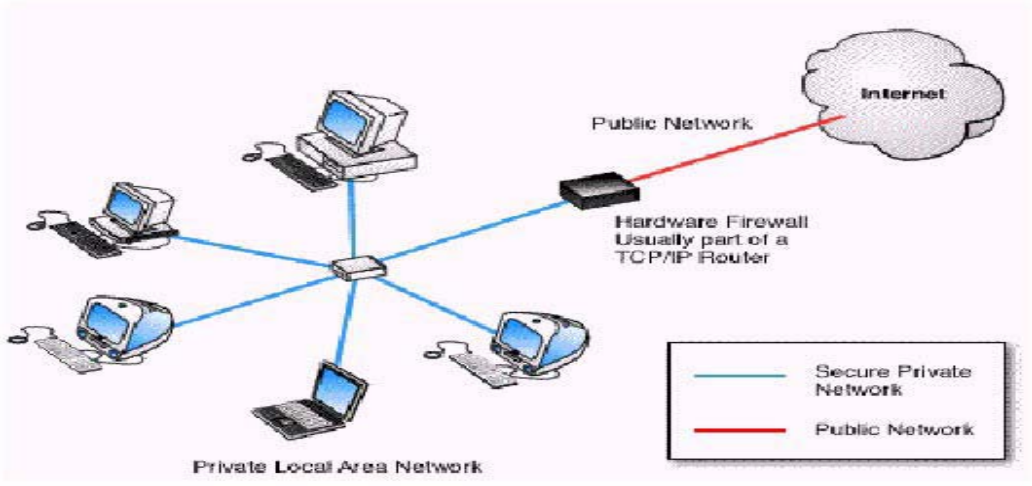
Αν κάποιος χρήστης του Internet ή του δικτύου προσπαθήσει να συνδεθεί στον υπολογιστή σας, το firewall αποκλείει αυτήν τη σύνδεση. Αν εκτελέσετε ένα πρόγραμμα όπως το πρόγραμμα άμεσης ανταλλαγής μηνυμάτων ή ένα παιχνίδι με πολλούς παίκτες και το πρόγραμμα αυτό προσπαθήσει να επιτρέψει μια σύνδεση από το Internet ή από το δίκτυο, το firewall σας ζητά να διατηρήσετε ή να καταργήσετε τον αποκλεισμό της σύνδεσης. Αν επιλέξετε να καταργήσετε τη σύνδεση, το firewall δημιουργεί αυτό που είναι γνωστό ως εξαίρεση έτσι ώστε να μην χρειάζεται να ανησυχείτε κάθε φορά που το πρόγραμμα θέλει να συνδεθεί στο μέλλον.

Αν και μπορείτε να απενεργοποιήσετε το firewall για συγκεκριμένες συνδέσεις δικτύου και Internet, αν το κάνετε αυτό θα αυξήσετε τον κίνδυνο που ενδέχεται να αντιμετωπίσει ο υπολογιστής σας.

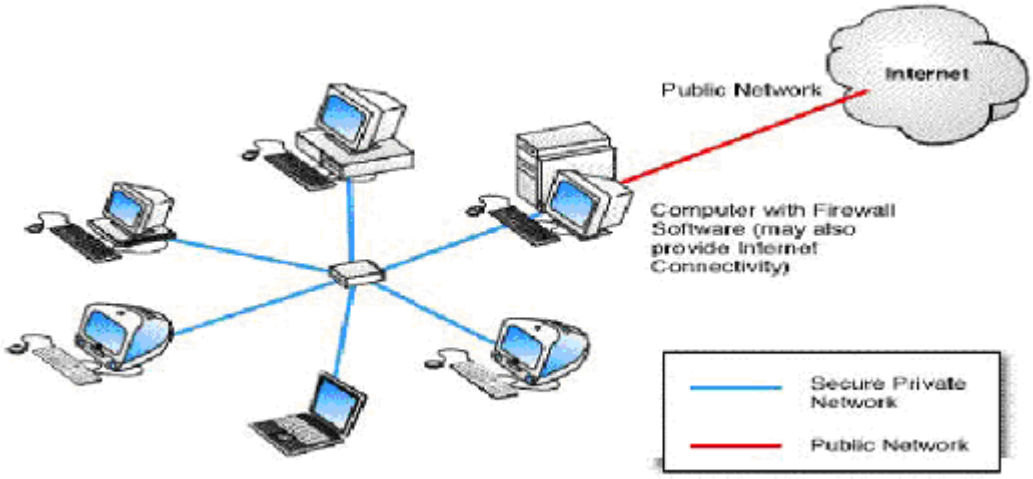
Τι είδους Firewalls υπάρχουν ;

1η κατηγοριοποίηση

Ανάλογα με τη φύση του firewall διακρίνουμε τα **Hardware Firewalls** (Routers) και τα **Software Firewalls** που είναι προγράμματα εγκαταστημένα σε ηλεκτρονικούς υπολογιστές που είναι άμεσα συνδεμένοι στο διαδίκτυο (τα λεγόμενα Gateways) .



Εικόνα 3 - Hardware Firewalls



Εικόνα 4 - Software Firewalls

Και στα δύο είδη των Firewalls παρατηρούμε ότι επιτελούν τις ίδιες λειτουργίες , φιλτράρουν και ελέγχουν τα δεδομένα μόνο που στα software στη θέση του router υπάρχει ένας Η/Υ με εγκατεστημένο πρόγραμμα Firewall.

2η κατηγοριοποίηση

Οι βασικές κατηγορίες των firewall χωρίζονται σε περισσότερες ανάλογα με τον αριθμό των ατόμων που επιθυμούμε να προστατέψουμε από τους κακόβουλους εισβολείς του Internet.

- Enterprise hardware firewall.

- Enterprise software firewall.
- SOHO hardware firewall.
- SOHO software firewall.

Ένας πολύ σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη για την επιλογή ενός firewall είναι: πόσους χρήστες θέλετε να προστατέψετε και πόσα firewall θα χρειαστείτε. Ο αριθμός των χρηστών που θα προστατέψετε θα καθορίσει αν χρειάζεστε ένα firewall για μεγάλη εταιρεία (enterprise) ή ένα για μικρό γραφείο (SOHO). Τα περισσότερα SOHO firewalls μπορούν να ικανοποιήσουν απαιτήσεις σύνδεσης μέχρι 50 χρηστών Αν σκοπεύετε να προστατέψετε πάνω από 50 χρήστες πρέπει να επιλέξετε ένα firewall μεγαλύτερων δυνατοτήτων, δηλαδή τον enterprise firewall. Τυπικά, όσο πιο πολλούς χρήστες θέλουμε να υποστηρίζει το firewall, τόσο περισσότερη RAM και επεξεργαστική δύναμη θα χρειαστεί να έχει το firewall.

Μειονεκτήματα των firewalls.

Τα μειονεκτήματα των προγραμμάτων firewall είναι δύο. Κατ' αρχάς, επειδή, όπως προείπαμε, τα firewall έχουν σχεδιαστεί για ασφάλειες δικτύων, είναι συνήθως αρκετά ακριβά και «βαριά» προγράμματα. Το δεύτερο μειονέκτημα είναι ότι τα firewall στηρίζονται στους δικούς μας κανόνες, οι οποίοι μπορεί να είναι ατελείς (να έχουν «τρύπες», όπως λένε οι διαχειριστές συστημάτων).

Προβλήματα των Firewalls .

Ένα πρόβλημα στα Firewalls είναι τα ίδια τα Firewalls. Σε μερικές περιπτώσεις τα Firewalls είναι τόσο ασφαλή που στο διαδίκτυο δεν μπορείς να κάνεις τίποτα γιατί τα Firewalls δεν επιτρέπουν την πρόσβαση σε αυτό. Επίσης εμφανίζονται συνέχεια μηνύματα όπως << πιθανή επίθεση από …. >> και ειδικά σε Personal Firewalls. Τα Firewalls δεν είναι εύχρηστα επίσης μειώνουν

την απόδοση στην μεταφορά δεδομένων. Δεν μπορούν να ανιχνεύσουν ιούς για αυτό τον λόγο συστήνεται να χρησιμοποιείται και ένα Antivirus πρόγραμμα.

2. ΜΕΛΕΤΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ OTENET SECURITY KIT

Το Security Kit προσφέρει μία ολοκληρωμένη λύση στον τομέα της προστασίας ενάντια στην μη εξουσιοδοτημένη είσοδο χρηστών στον προσωπικό μας υπολογιστή. Κάποιες από τις δυνατότητες του είναι: Γονικός έλεγχος

Προστασία από ιούς

Τείχος προστασίας

Έλεγχος ηλεκτρονικής αλληλογραφίας

Οι λειτουργίες του Security Kit

Εικόνα 5 - Το κεντρικό περιβάλλον του συστήματος

Το κεντρικό παράθυρο του συστήματος αποτελείται από 6 καρτέλες. Οι καρτέλες αυτές είναι οι εξής:

- Καρτέλα **Αρχή**
- Καρτέλα **Προστασία από ιούς και κατασκοπευτικά προγράμματα**
- Καρτέλα **Ασπίδα internet**
- Καρτέλα **Έλεγχος ανεπιθύμητης αλληλογραφίας**
- Καρτέλα **Γονικός έλεγχος**
- Καρτέλα **Αυτόματες ενημερώσεις.**

Αναλυτικά

Η **καρτέλα Αρχή** προσφέρει μια γρήγορη και λεπτομερή προβολή των ρυθμίσεων ασφαλείας του συστήματος.

Η **καρτέλα Προστασία από ιούς και κατασκοπευτικά προγράμματα** λειτουργεί αυτόματα και σε πραγματικό χρόνο στο παρασκήνιο ενώ χρησιμοποιείτε αρχεία στον υπολογιστή σας ή περιηγείσθε σε τοποθεσίες web.

Εικόνα 6 - Καρτέλα Προστασία από ιούς και κατασκοπευτικά προγράμματα

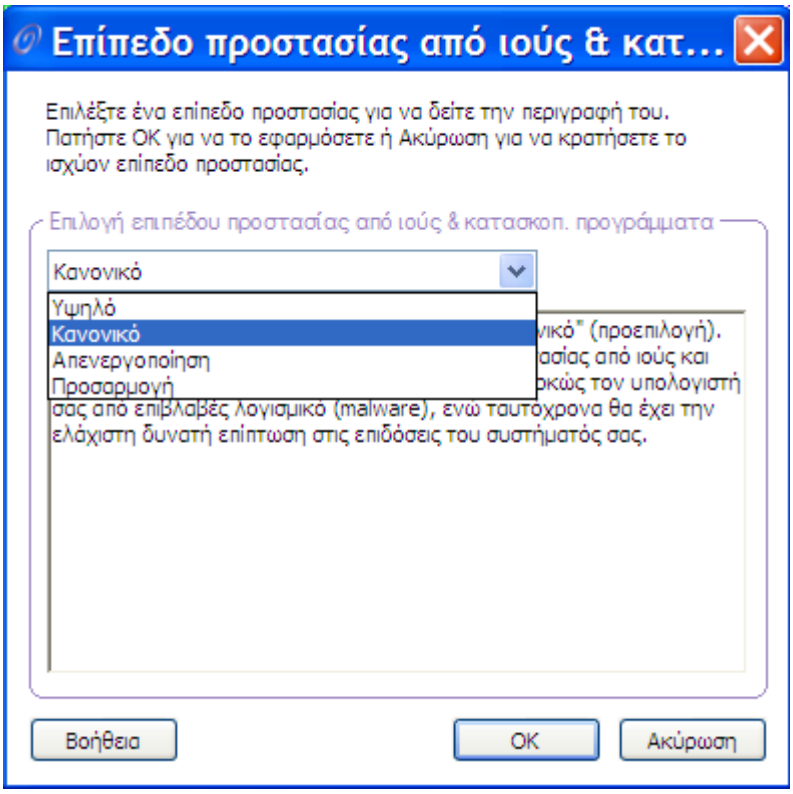
Πως λειτουργεί:

- σταματά επιβλαβές λογισμικό (βλέπε: παράρτημα), ιούς (βλέπε: παράρτημα) και κατασκοπευτικά προγράμματα (βλέπε: παράρτημα), αποτρέποντας την επίθεση στον υπολογιστή σας μέσω e-mail, αφαιρούμενων μέσων ή περιεχομένου λήψης από το Internet.
- τοποθετεί σε καραντίνα (βλέπε: παράρτημα) και καταργεί ιούς, κατασκοπευτικά προγράμματα και άλλο επιβλαβές λογισμικό που είναι εγκατεστημένα στον υπολογιστή σας
- εμποδίζει ενοχλητικά αναδυόμενα παράθυρα και προστατεύει τις ρυθμίσεις του συστήματός σας.

Μπορείτε να αλλάξετε το επίπεδο προστασίας, καθώς και τις ρυθμίσεις σάρωσης πραγματικού χρόνου, σάρωσης e-mail και

προγραμματισμένης σάρωσης από την καρτέλα Προστασία από ιούς και κατασκοπευτικά προγράμματα.

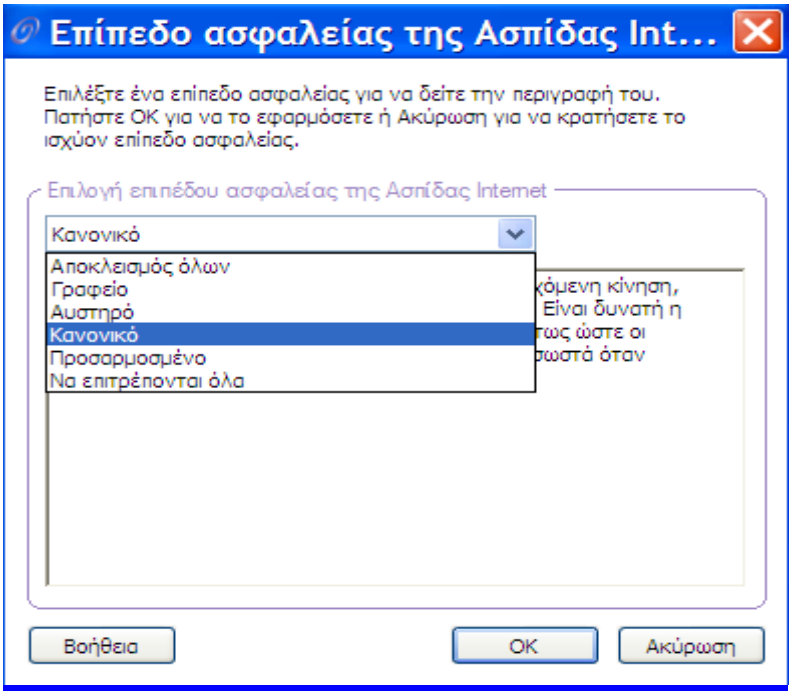
Μπορείτε να προβάλετε τις αναφορές σάρωσης και να εκτελέσετε σάρωση για ιούς και κατασκοπευτικά προγράμματα με μη αυτόματο τρόπο από την καρτέλα Προστασία από ιούς και κατασκοπευτικά προγράμματα.



Η καρτέλα **Ασπίδα internet** παρακολουθεί και φιλτράρει όλη την κυκλοφορία του διαδικτύου. Αποτρέπει με τον τρόπο αυτό την μη εξουσιοδοτημένη πρόσβαση χρηστών στον υπολογιστή μας.

Εικόνα 7 - Καρτέλα Ασπίδα Internet

Στο σημείο αυτό ρυθμίζουμε το βαθμό προστασίας μας.



Εικόνα 8 -Επιλογή επιπέδου ασφαλείας

Στην καρτέλα αυτή μπορούμε να δημιουργήσουμε τους κανόνες που θα ορίζουν τι θα γίνεται με την εισερχόμενη και εξερχόμενη κυκλοφορία. Μπορούμε να ορίσουμε κανόνες που θα επιτρέπουν ή θα αποτρέπουν την κυκλοφορία βάσει κάποιων κριτηρίων όπως θα δούμε στα παραδείγματα παρακάτω.

Στην καρτέλα **Έλεγχος Ανεπιθύμητης Κυκλοφορίας** γίνεται ο έλεγχος της εισερχόμενης αλληλογραφίας.

Εικόνα 9 - Καρτέλα έλεγχος αλληλογραφίας

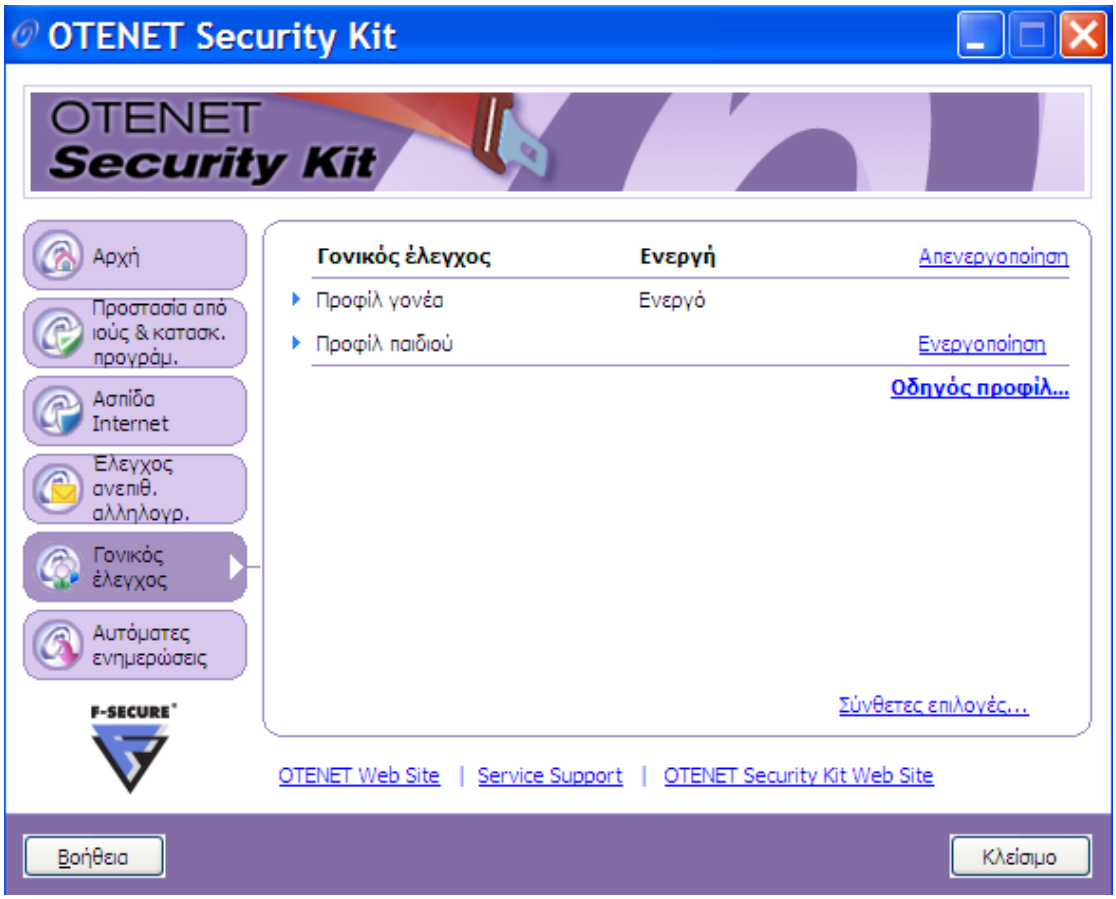
Λειτουργίες του συστήματος που αφορούν την εισερχόμενη και εξερχόμενη αλληλογραφία:

Καταργεί τα μηνύματα ομαδικής αλληλογραφίας και τα τοποθετεί σε ξεχωριστό φάκελο και όχι στα εισερχόμενα.

Παρέχει τη δυνατότητα επιλογής μεταξύ 3 επιπέδων φιλτραρίσματος των ομαδικών μηνυμάτων: Επιθετικό, μεσαίο, χαλαρό ανάλογα με το πόσο αυστηρός θέλω να είναι ο έλεγχος.

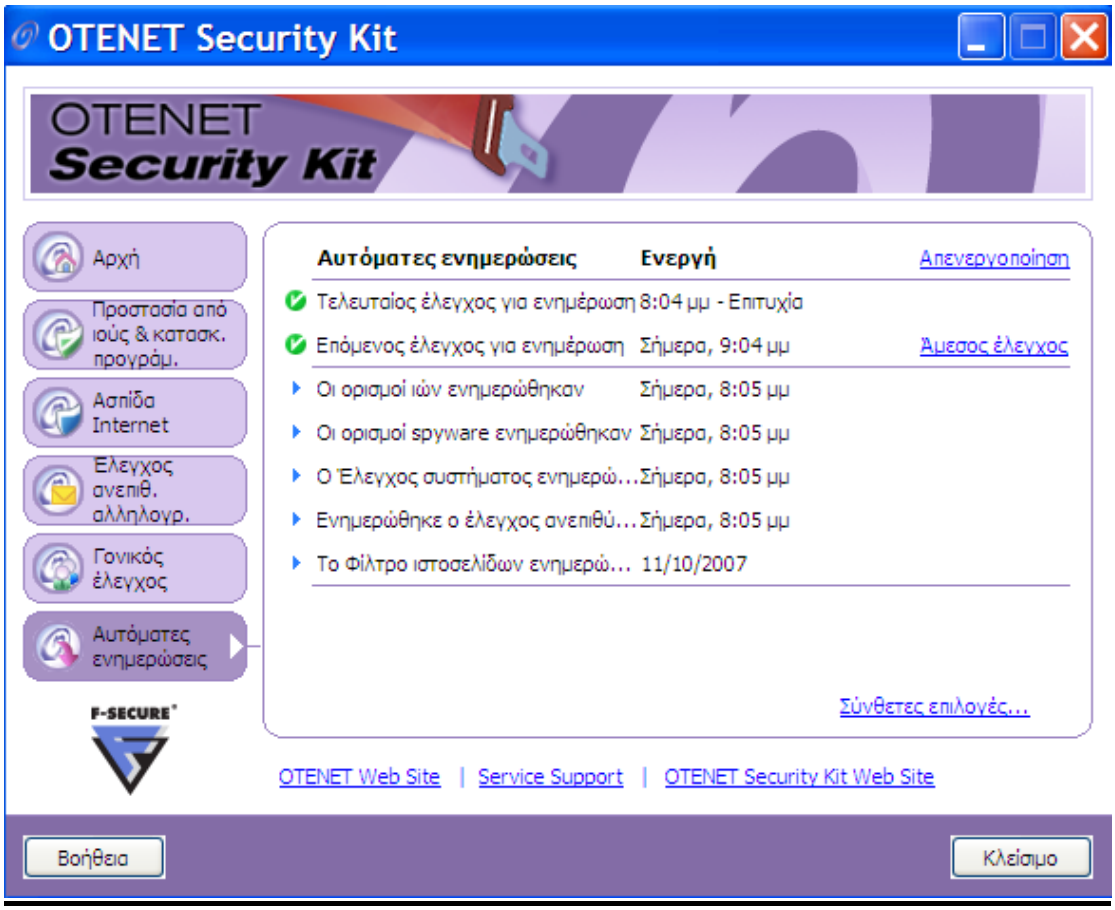
Παρέχει τη δυνατότητα ορισμού διευθύνσεων αποστολέων των οποίων τα μηνύματα πάντα θα κατευθύνονται στον φάκελο της ανεπιθύμητης αλληλογραφίας (φιλτραρισμένοι) και αποστολείς που ποτέ δεν θα κατευθύνονται στον φάκελο της ανεπιθύμητης αλληλογραφίας (επιτρεπόμενοι).

Η καρτέλα **Γονικός Έλεγχος** μας παρέχει τη δυνατότητα να προσδιορίσουμε σε ποιες σελίδες θα έχουμε πρόσβαση. Αυτό γίνεται με την επιλογή προφίλ (Γονέα, Εφήβου και Παιδιού).



Εικόνα 10 - Καρτέλα Γονικός Έλεγχος

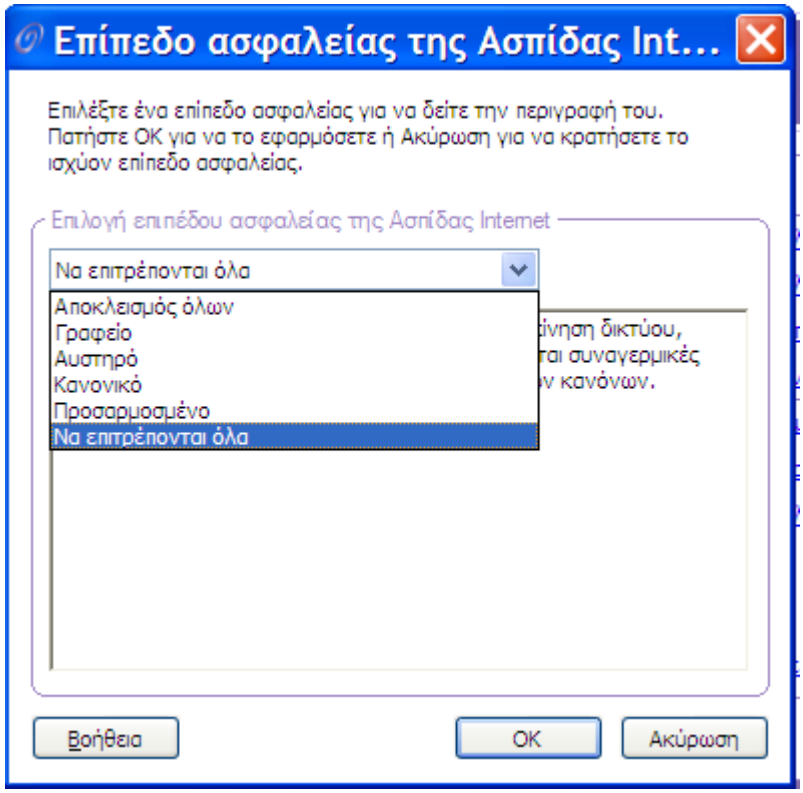
Η καρτέλα Αυτόματες Ενημερώσεις



3. ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ OTENET KIT

1. Διακοπή λειτουργίας του firewall, δηλαδή επιτρέπω κάθε είδους κυκλοφορία.

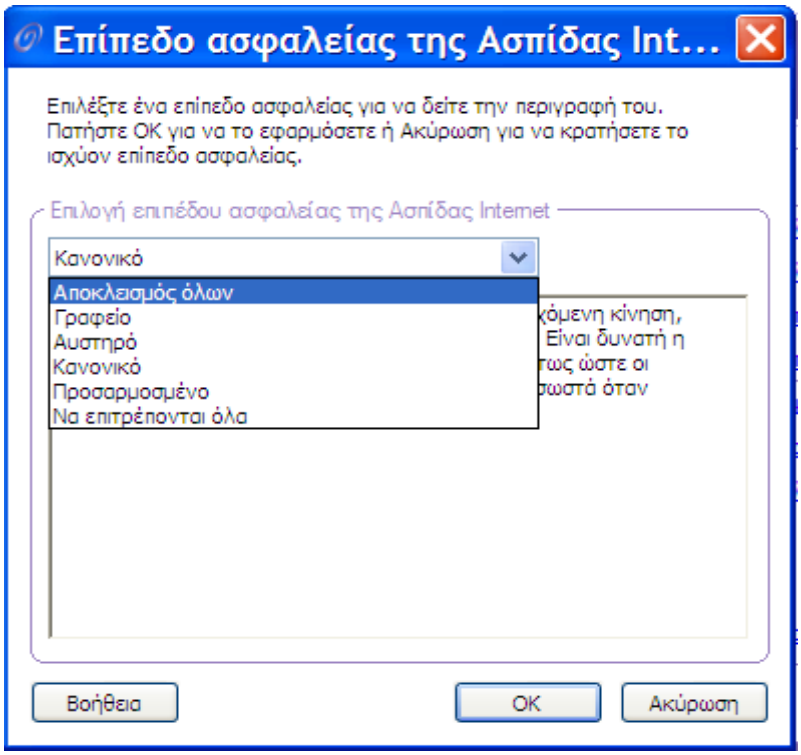
Ανοίγω την καρτέλα **Αρχή→ Ασπίδα internet** και κάνω κλικ στην επιλογή **Αλλαγή→** τέλος επιλέγω **Να Επιτρέπονται Όλα.**



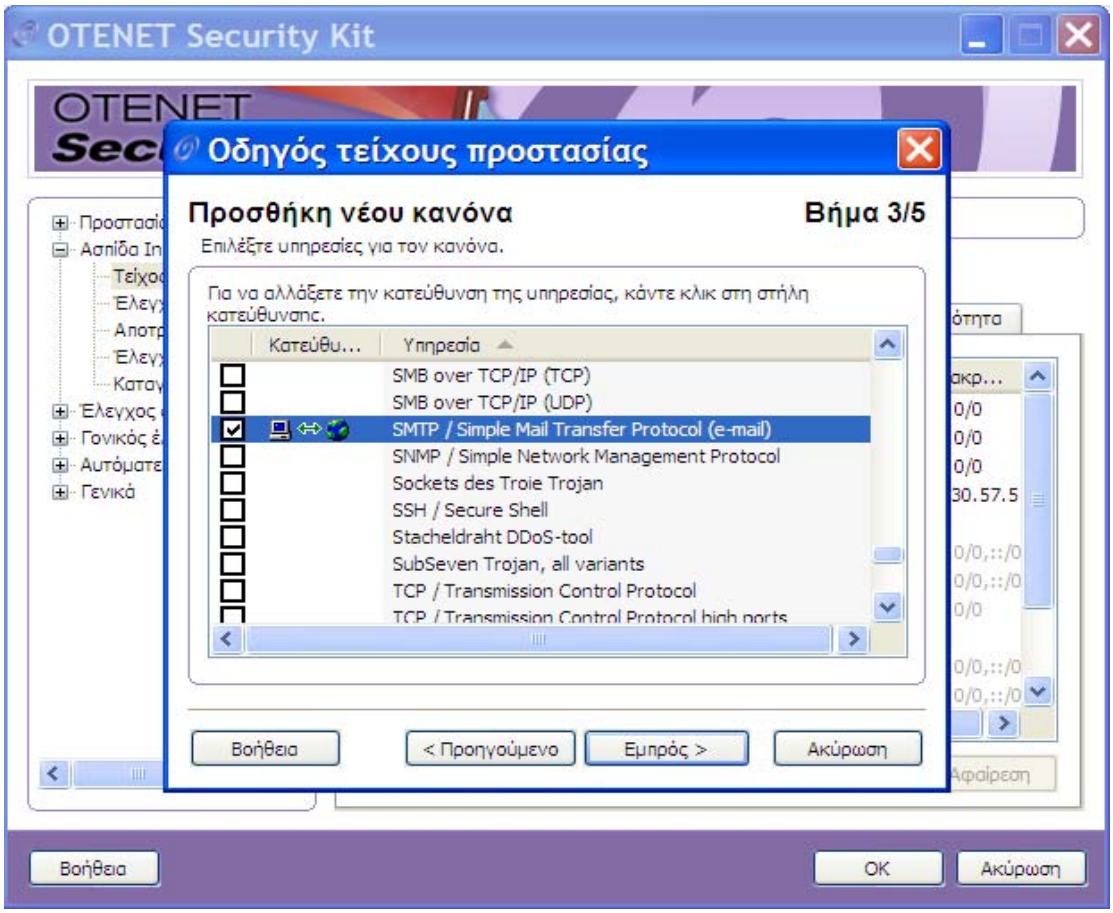
Με τον τρόπο αυτό απενεργοποιώ στην ουσία το firewall και κάθε είδους κυκλοφορία (εισερχ/εξερχ) γίνεται δεκτή.

2. Απαγόρευση κάθε είδους κυκλοφορίας.

Ανοίγω την καρτέλα **Αρχή→ Ασπίδα internet** και κάνω κλικ στην επιλογή **Αλλαγή→** τέλος επιλέγω **Αποκλεισμός Όλων**. Το firewall απαγορεύει την κυκλοφορία. Καμία επικοινωνία δεν γίνεται δεκτή.

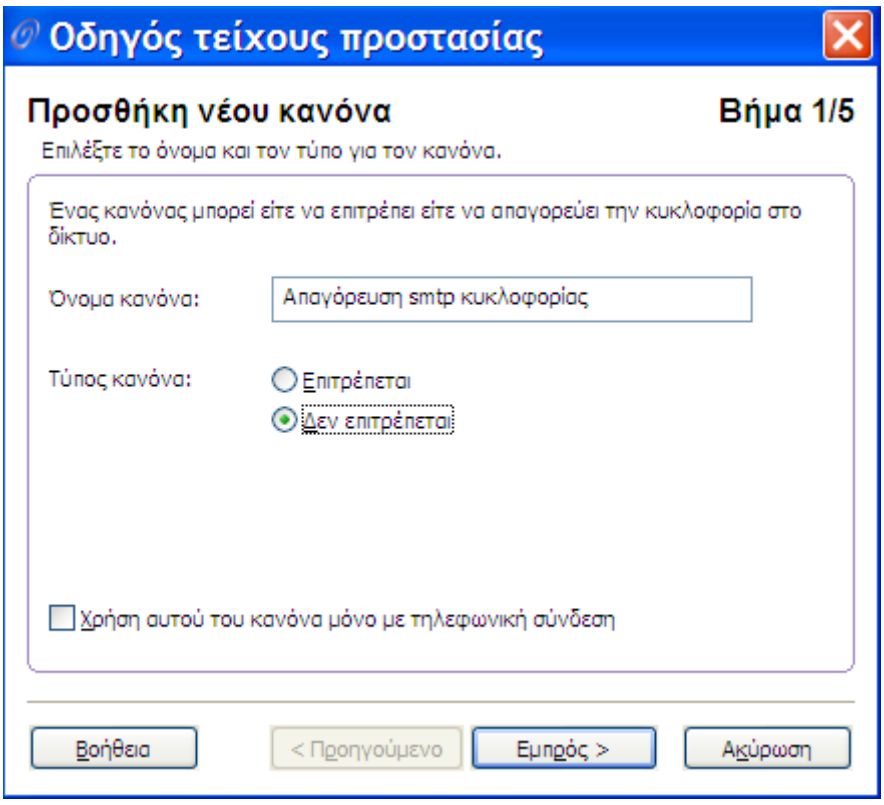


3. <u>Το firewall απαγορεύει οποιαδήποτε εφαρμογή mail.</u>

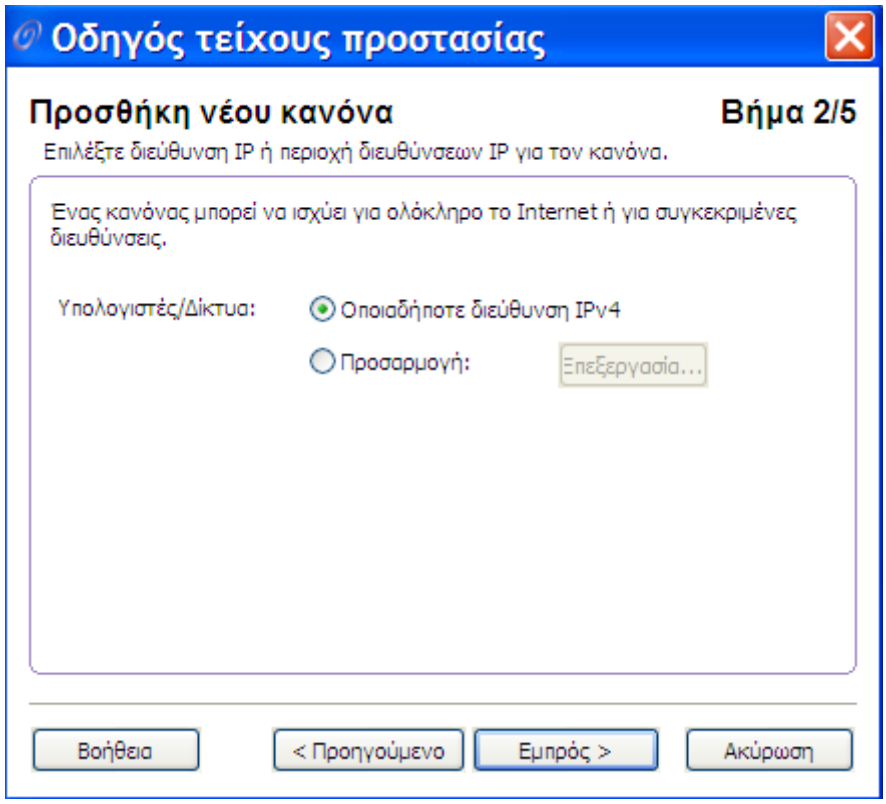


Για να αποκλείσουμε την **smtp** κυκλοφορία πρέπει να ακολουθήσουμε την εξής διαδικασία: Ανοίγουμε την καρτέλα **Ασπίδα internet → Τείχος προστασίας → Ρύθμιση παραμέτρων** → Ανοίγω την καρτέλα **Κανόνες** και κάνω κλικ στο κουμπί **Προσθήκη**. Με τον τρόπο αυτό ξεκινάει ο οδηγός δημιουργίας ενός νέου κανόνα.

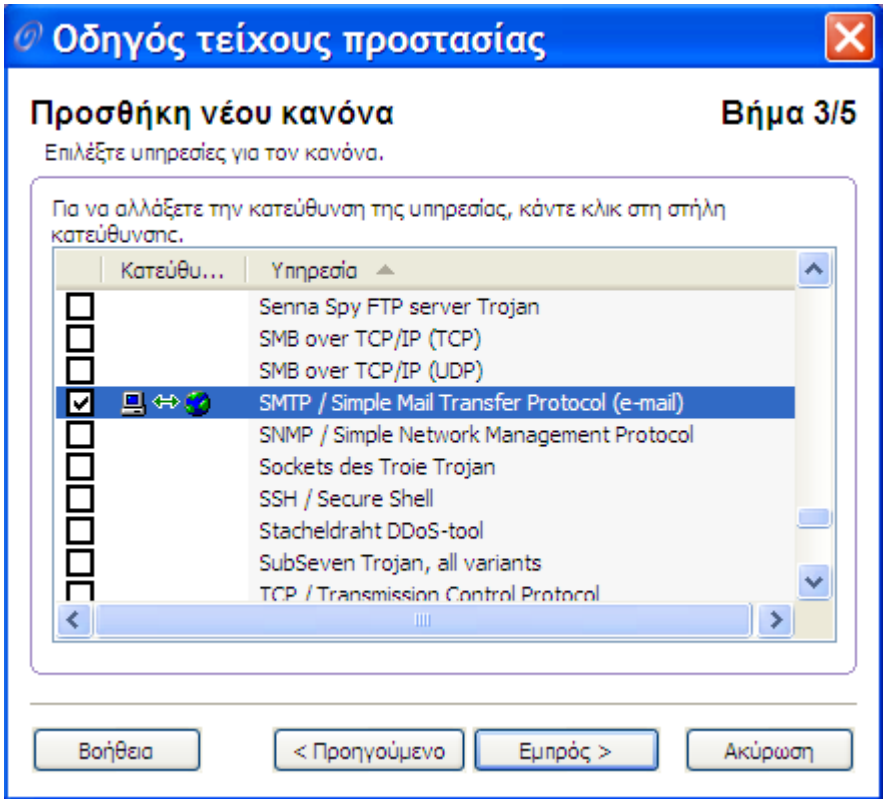
Στο πρώτο βήμα δίνουμε ένα όνομα στον νέο κανόνα και ορίζουμε τι θα κάνει ο κανόνας αυτός, θα επιτρέπει ή θα απαγορεύει την κυκλοφορία.



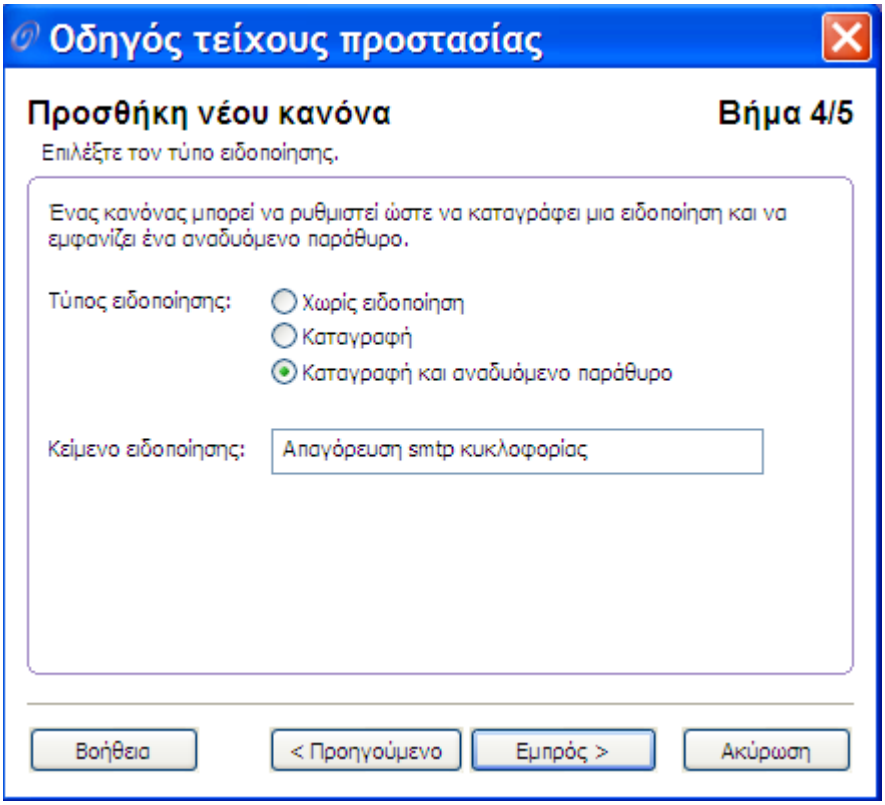
Στο δεύτερο βήμα επιλέγω για ποιες ip διευθύνσεις θα εφαρμόζεται αυτός ο κανόνας. Στην περίπτωση μας για όλες τις διευθύνσεις.



Στο τρίτο βήμα ορίζω ποια υπηρεσία αφορά ο κανόνας, στο παράδειγμα μας η **smtp κυκλοφορία**, και προς ποια κατεύθυνση δηλαδή αν θα απαγορεύσω την εξερχόμενη, την εισερχόμενη κυκλοφορία (ή και προς τις δύο κατευθύνσεις).



Στο τέταρτο βήμα έχω τη δυνατότητα να ορίσω τον τύπο ειδοποίησης. Στο παράδειγμα αυτό ορίζω να καταγράφεται κάθε προσπάθεια σύνδεσης της υπηρεσίας και να εμφανίζεται και το συγκεκριμένο μήνυμα ειδοποίησης.

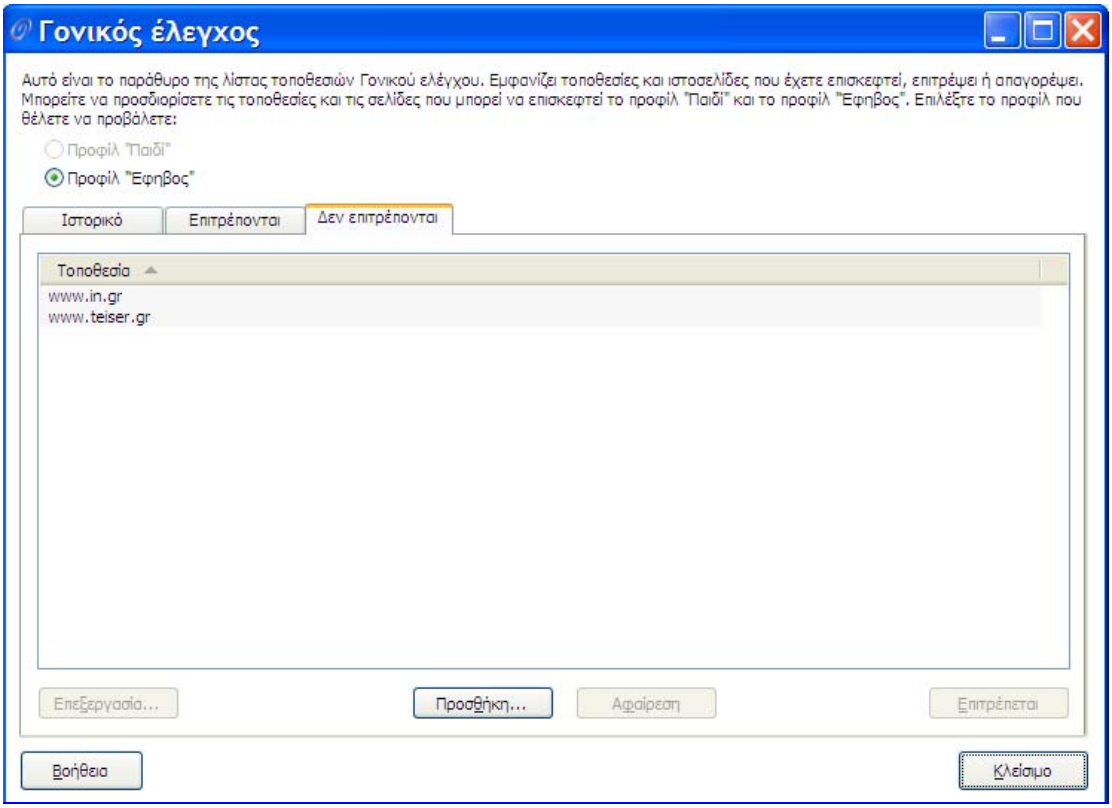


4. <u>Απαγόρευση εμφάνισης συγκεκριμένης web σελίδας (π.χ. www.teiser.gr)</u>.

Υπάρχουν δύο τρόποι για να απαγορεύσω την εμφάνιση συγκεκριμένης ιστοσελίδας (ενώ επιτρέπω την εμφάνιση όλων των άλλων σελίδων):

<u>1ος τρόπος</u>

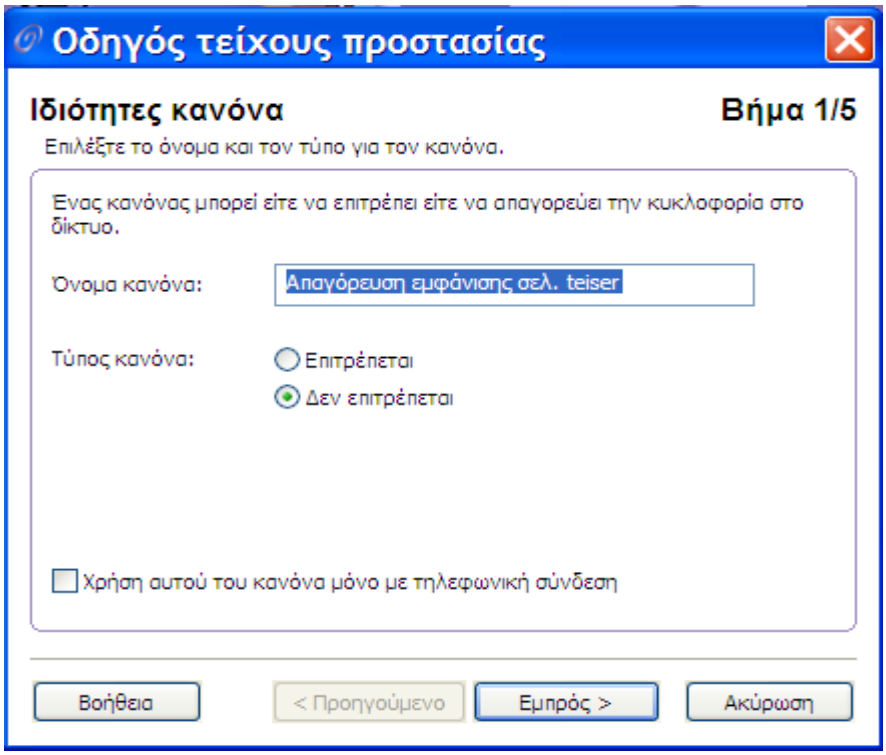
Ανοίγω την καρτέλα **Γονικός Έλεγχος** → Ενεργοποιώ το **Προφίλ Εφήβου** → Στη **Λίστα Τοποθεσιών** → και στην καρτέλα **Δεν Επιτρέπονται** κάνω προσθήκη της ιστοσελίδας www.teiser.gr. Το ίδιο κάνω και στην περίπτωση που θέλω να απαγορεύσω την εμφάνιση ενός σύνολο από σελίδες.



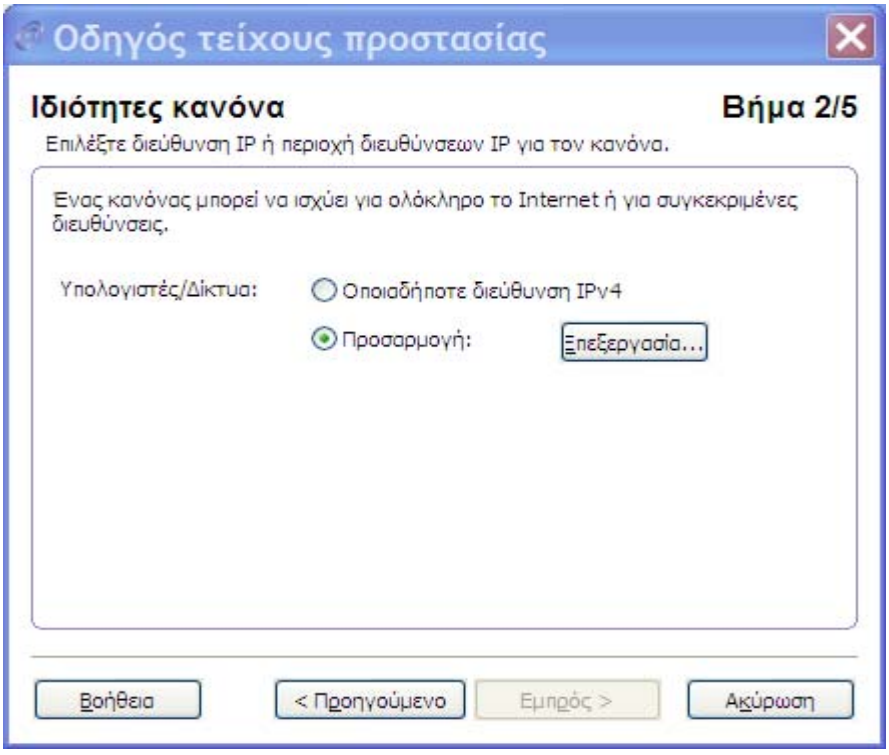
2ος τρόπος

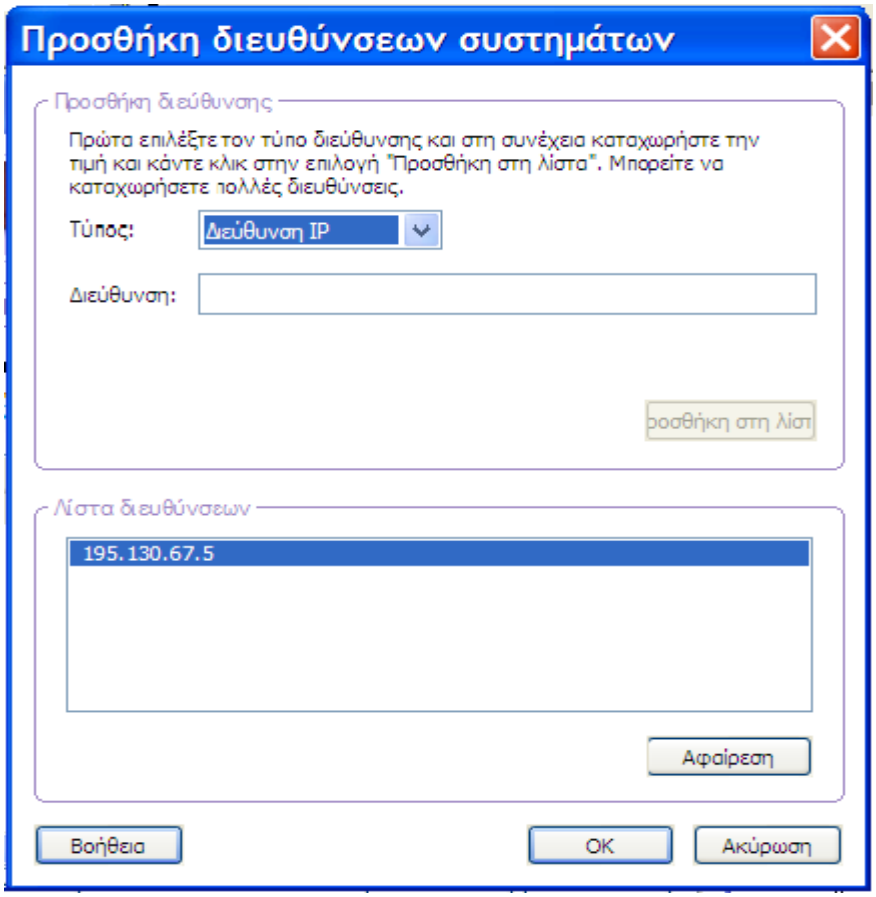
Ανοίγω την καρτέλα **Ασπίδα internet** → Στο τείχος προστασίας κάνω κλικ στη **Ρύθμιση Παραμέτρων** → Στην καρτέλα **Κανόνες** κάνω **Προσθήκη** ενός νέου κανόνα ο οποίος θα απαγορεύει την εμφάνιση της σελίδας.

Μόλις κάνω κλικ στην **Προσθήκη** ξεκινάει ο οδηγός δημιουργίας κανόνων: Στο πρώτο βήμα εισάγω το όνομα του κανόνα και τον τύπο του, δηλαδή τη συμπεριφορά του. Στο παράδειγμα αυτό ο κανόνας **Δεν επιτρέπει**.

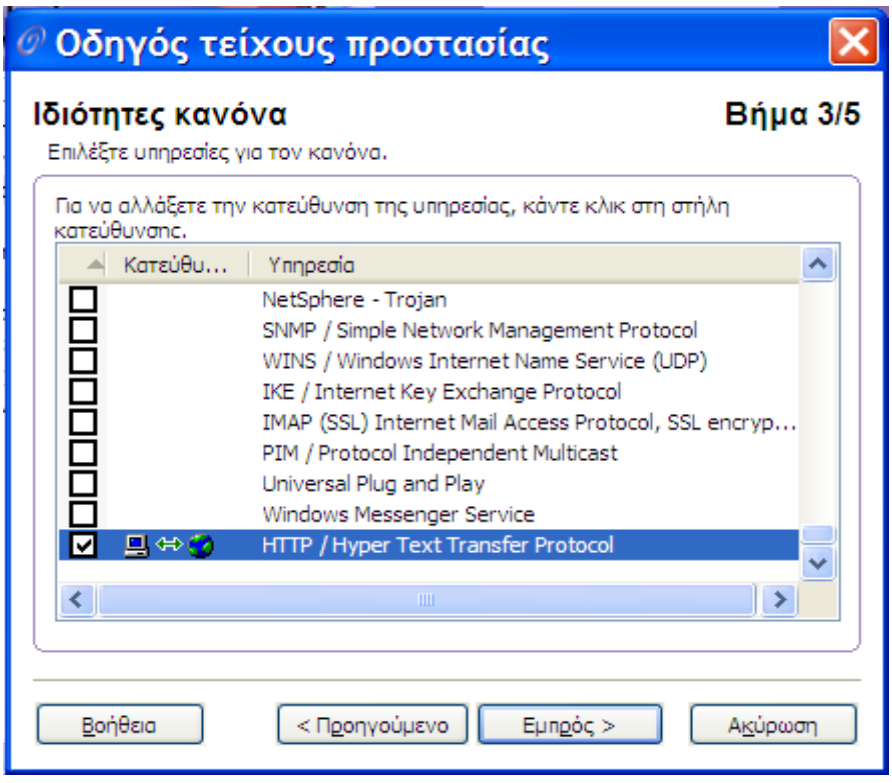


Στο δεύτερο βήμα ορίζω ποιες διευθύνσεις ip θα αφορά αυτός ο κανόνας. Μπορώ να επιλέξω οποιαδήποτε διεύθυνση ή να δώσω συγκεκριμένες ip διευθύνσεις όπως στο παράδειγμά την 195.130.67.5.

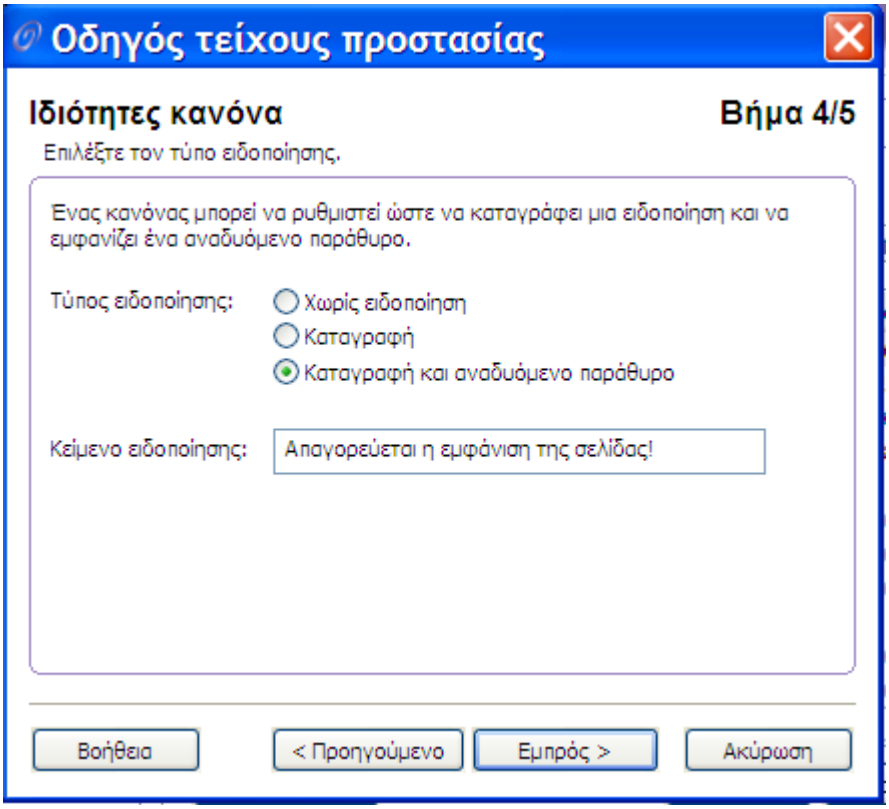




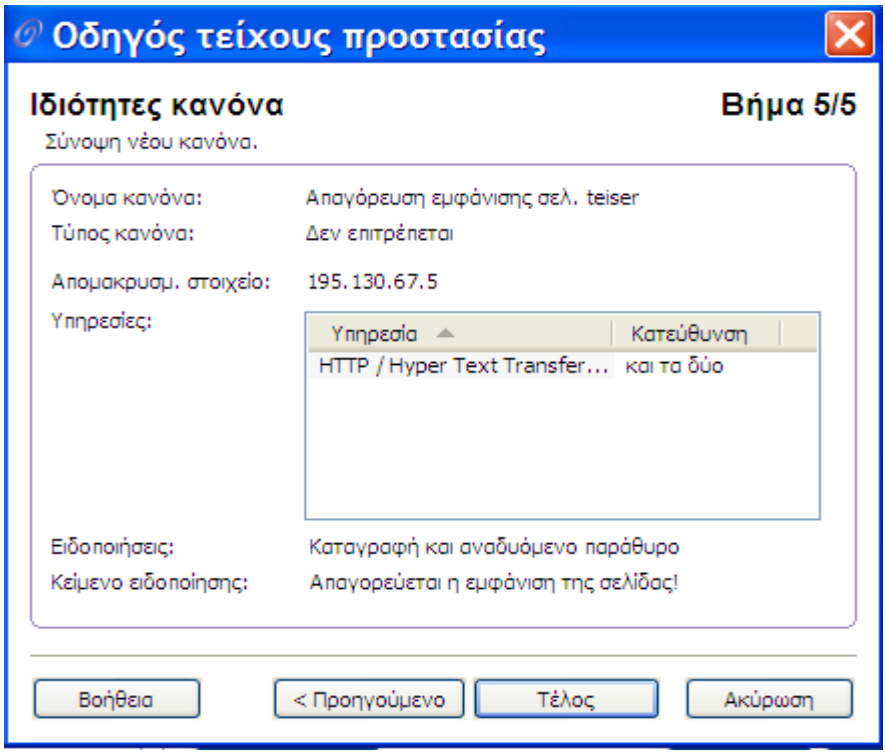
Στο τρίτο βήμα επιλέγω την υπηρεσία που αφορά ο κανόνας και την κατεύθυνση της κυκλοφορίας.



Στο τέταρτο βήμα επιλέγω τον τύπο της ειδοποίησης που θα εμφανίζεται κάθε φορά που κάποιος επιχειρεί να ανοίξει την σελίδα αυτή.



Και στο τελευταίο βήμα βλέπω μία σύνοψη των ρυθμίσεων που έχω ορίσει για τον κανόνα.



Με τον ίδιο τρόπο μπορώ να ρυθμίσω να μην είναι δυνατή η εμφάνιση πολλών ιστοσελίδων.

5. <u>Επιτρέπω την εμφάνιση μόνο μίας ιστοσελίδας.</u>

Η δυνατότητα να εμφανίζεται μία μόνο ιστοσελίδα (και καμία άλλη) γίνεται πάλι με δύο τρόπους. Είτε χρησιμοποιώντας τον **Γονικό Έλεγχο** είτε τις ρυθμίσεις της **Ασπίδας internet.**

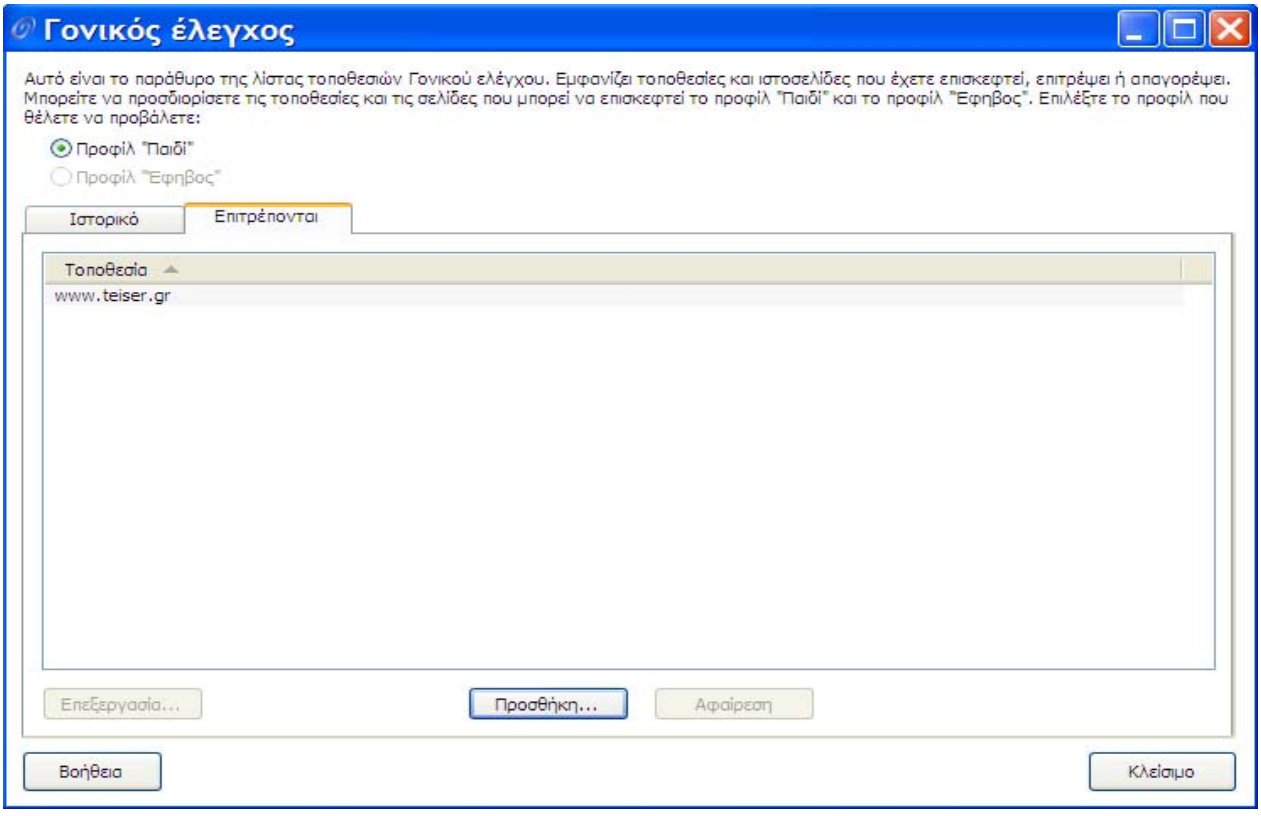
Στην πρώτη περίπτωση καμία σελίδα δεν θα είναι διαθέσιμη για το προφίλ Παιδί παρά μόνο η σελίδα που θα ορίσουμε εμείς, ενώ για τον Γονέα θα είναι όλες οι σελίδες διαθέσιμες. Με τον δεύτερο τρόπο δηλαδή χρησιμοποιώντας την ασπίδα internet όλοι οι χρήστες θα έχουν τη δυνατότητα να βλέπουν μόνο τη σελίδα αυτή και καμία άλλη.

<u>1ος τρόπος</u>

Ανοίγω την καρτέλα **Γονικός Έλεγχος** → Ενεργοποιώ το **Προφίλ Παιδί** (Οδηγός Προφίλ) → έπειτα κάνω κλικ στις **Σύνθετες Επιλογές** και επιλέγω την καρτέλα **Επιτρέπονται** για να κάνω **Προσθήκη** της ιστοσελίδας. Το ίδιο κάνω και στην περίπτωση που θέλω να βλέπω ένα σύνολο από σελίδες και όχι όλες τις σελίδες.

Βλέπουμε ότι το σύστημα otenet kit μας δίνει τη δυνατότητα να απαγορεύουμε την εμφάνιση κάποιων σελίδων ή όλων των σελίδων μόνο για κάποια συγκεκριμένα προφίλ, γεγονός που είναι πολύ χρήσιμο σε περίπτωση που ο υπολογιστής χρησιμοποιείται από εφήβους ή παιδιά και δεν θέλουμε να έχουν πρόσβαση σε κάθε σελίδα του διαδικτύου ενώ το Προφίλ Γονέας έχει πρόσβαση σε όλο το διαδίκτυο.

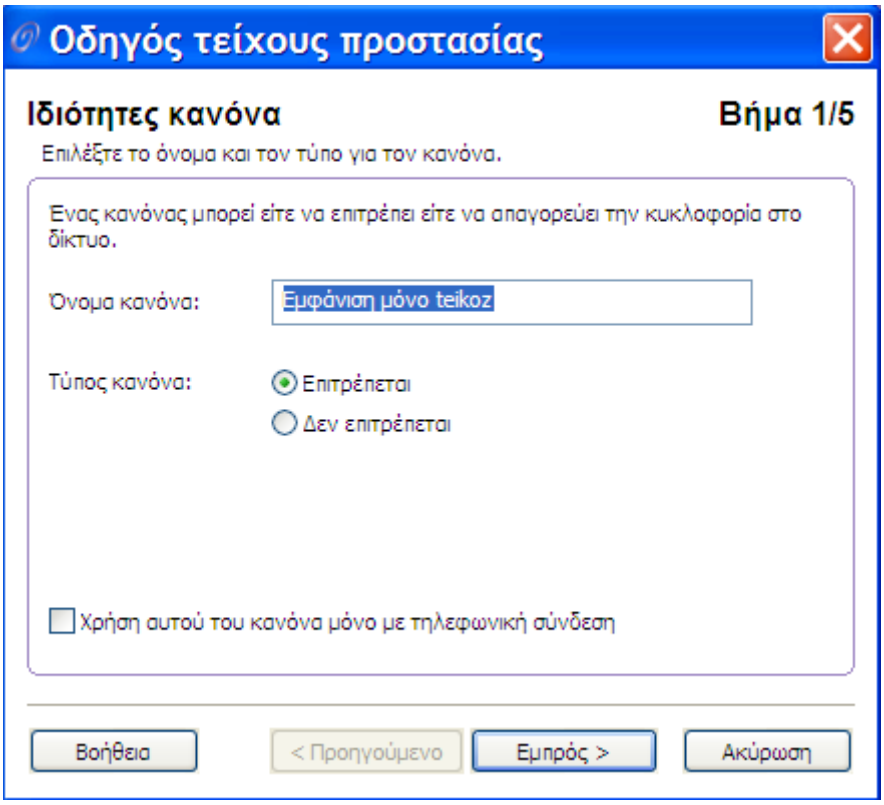

OTENET Security Kit
OTENET
Security Kit
Αρχή
Προστασία από ιούς & κατασκ. προγράμ.
Ασπίδα Internet
Έλεγχος ανεπιθ. αλληλογρ.
Γονικός έλεγχος
Αυτόματες ενημερώσεις
F-SECURE
Γονικός έλεγχος
Ενεργή
Απενεργοποίηση
Προφίλ γονέα
Ενεργοποίηση
Προφίλ παιδιού
Ενεργό
Οδηγός προφίλ...
Σύνθετες επιλογές...
OTENET Web Site | Service Support | OTENET Security Kit Web Site
Βοήθεια
Κλείσιμο


Γονικός έλεγχος
Αυτό είναι το παράθυρο της λίστας τοποθεσιών Γονικού ελέγχου. Εμφανίζει τοποθεσίες και ιστοσελίδες που έχετε επισκεφτεί, επιτρέψει ή απαγορέψει. Μπορείτε να προσδιορίσετε τις τοποθεσίες και τις σελίδες που μπορεί να επισκεφτεί το προφίλ "Παιδί" και το προφίλ "Έφηβος". Επιλέξτε το προφίλ που θέλετε να προβάλετε:
Προφίλ "Παιδί"
Προφίλ "Έφηβος"
Ιστορικό
Επιτρέπονται
Τοποθεσία
www.teiser.gr
Επεξεργασία...
Προσθήκη...
Αφαίρεση
Βοήθεια
Κλείσιμο

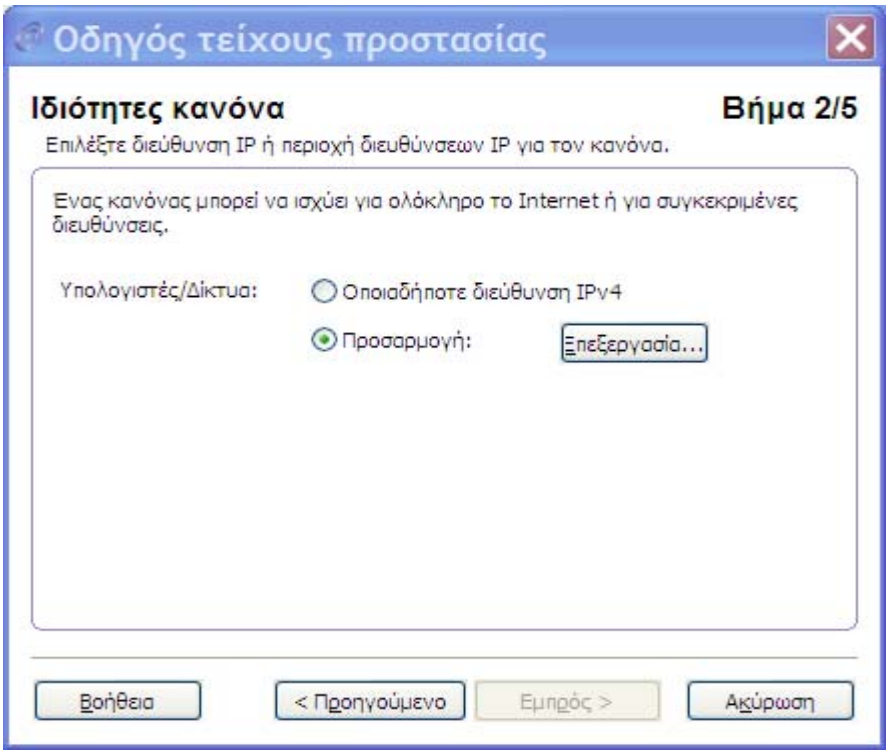
2ος τρόπος

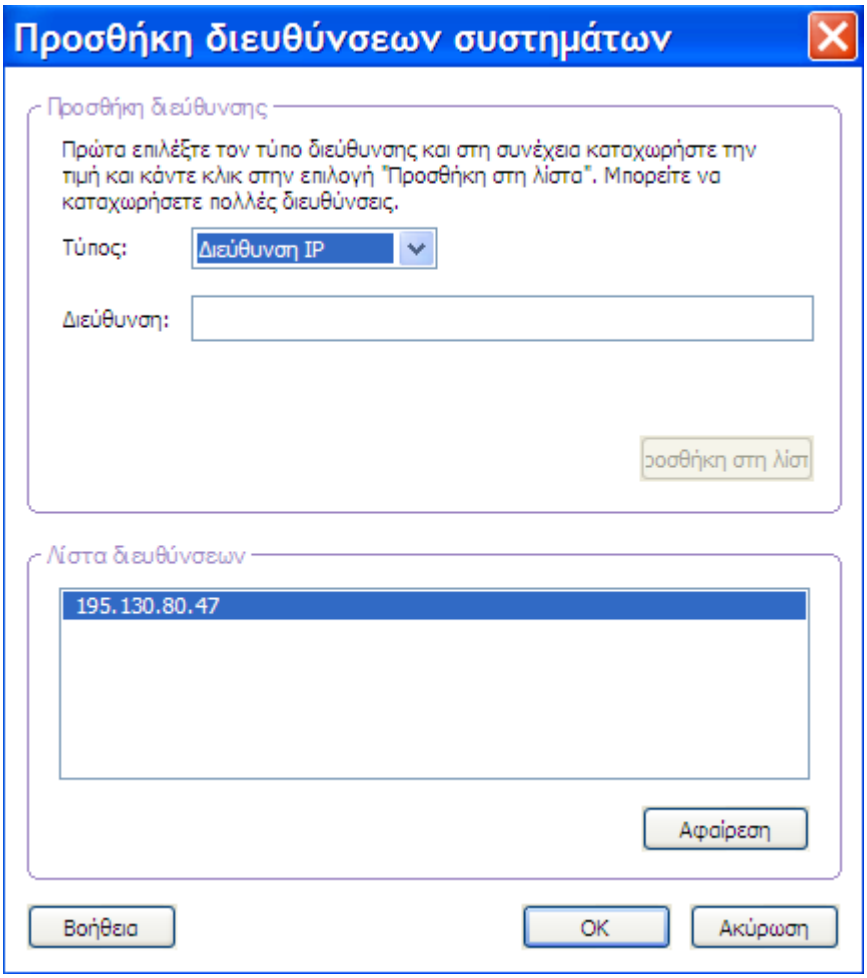
Ανοίγω την καρτέλα **Ασπίδα internet** → Στο τείχος προστασίας κάνω κλικ στη **Ρύθμιση Παραμέτρων** → Στην καρτέλα **Κανόνες** κάνω **Προσθήκη** ενός νέου κανόνα ο οποίος θα επιτρέπει την εμφάνιση της σελίδας (ακολουθώ την ίδια διαδικασία με το παράδειγμα 4).

Στο πρώτο βήμα δίνω όνομα στον κανόνα και ορίζω τι θα κάνει με την κυκλοφορία, θα απαγορεύει ή θα επιτρέπει.

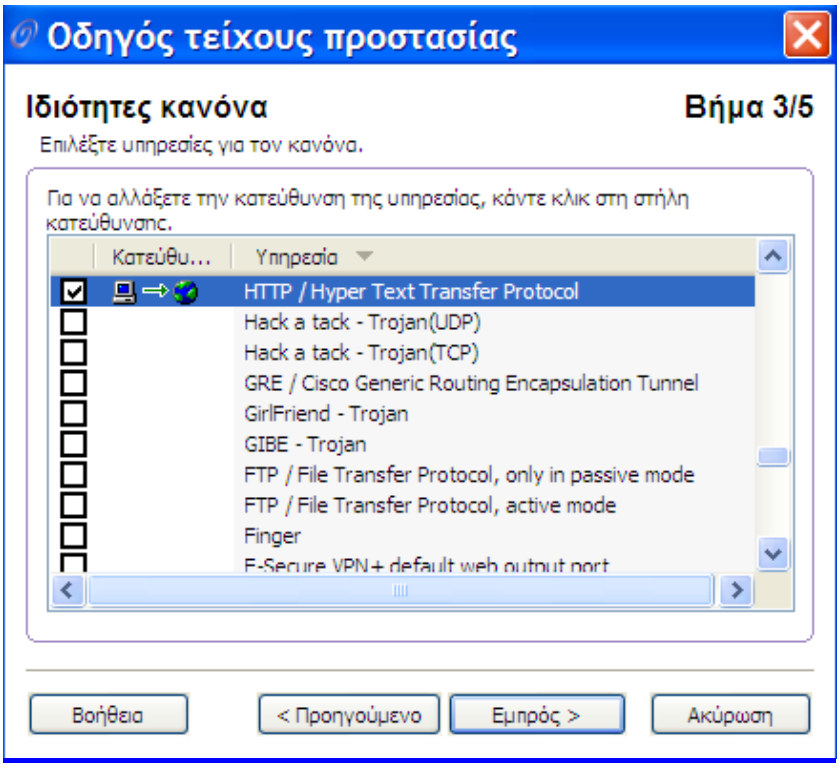


Στο δεύτερο βήμα επιλέγω τις ip διευθύνσεις για τις οποίες ισχύει ο κανόνας. Στο παράδειγμά μας είναι: 195.130.80.47

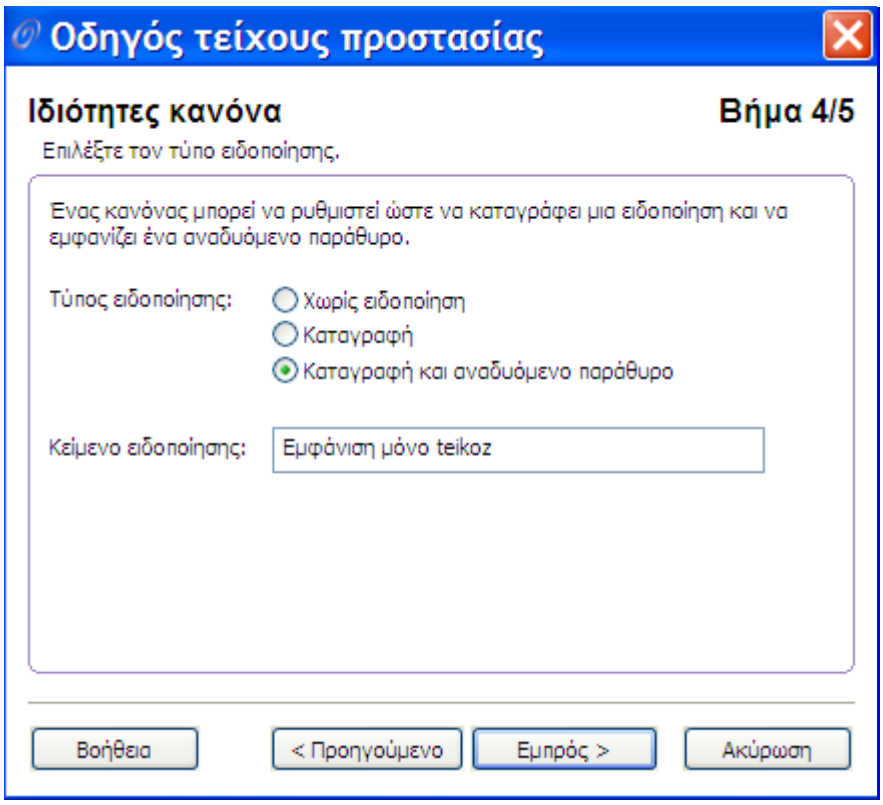




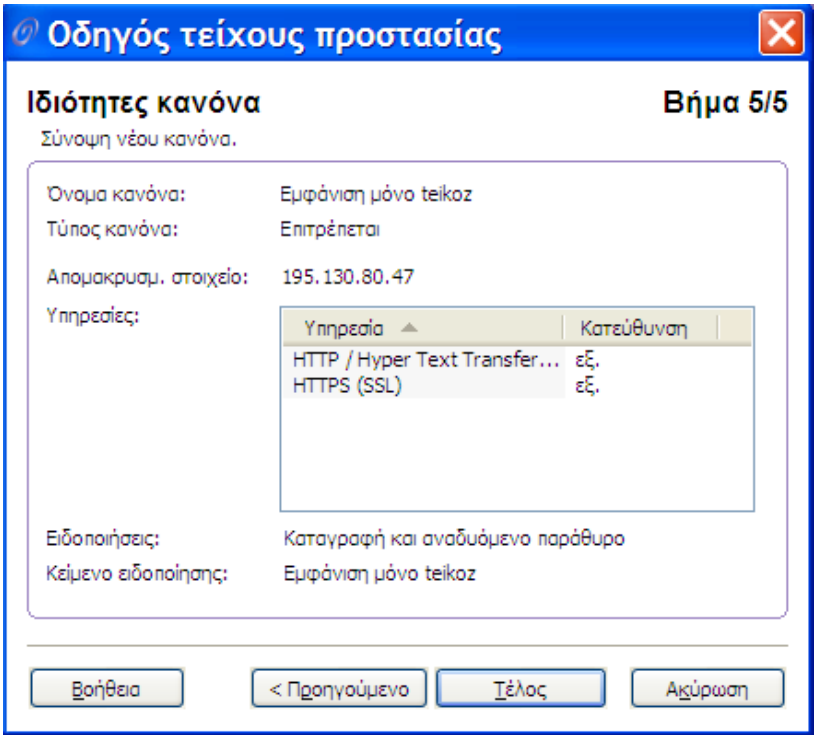
Στο τρίτο βήμα επιλέγω την υπηρεσία: http



Στο τέταρτο βήμα επιλέγουμε ο τύπος προειδοποίησης να είναι καταγραφή και μήνυμα.



Στο πέμπτο βήμα βλέπουμε τη σύνοψη του κανόνα

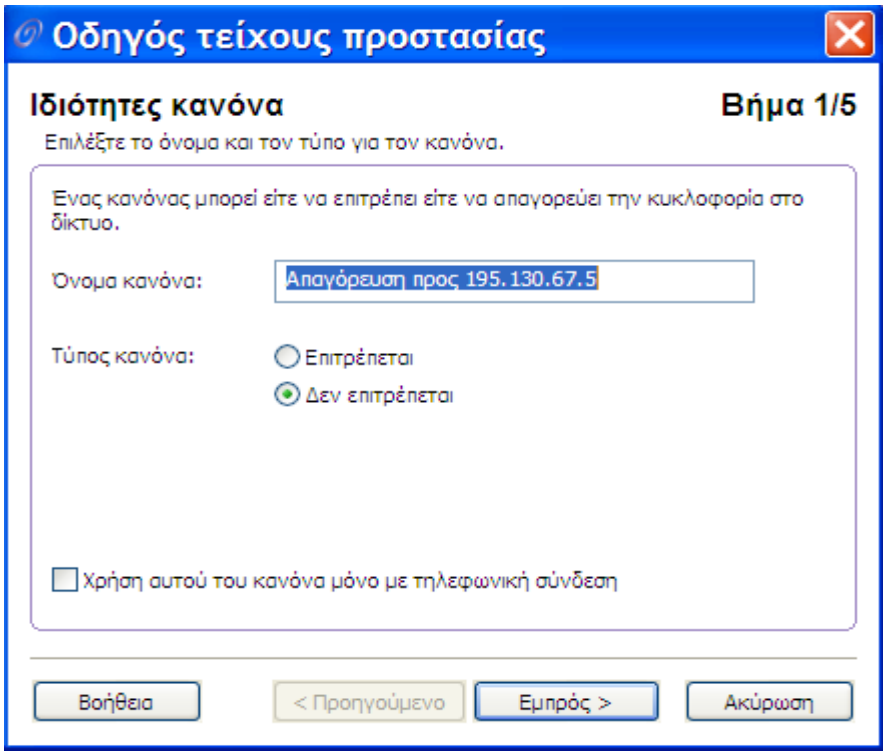


Αυτό που πρέπει να προσέξω είναι το εξής: Από προεπιλογή το firewall επιτρέπει την εμφάνιση όλων των ιστοσελίδων, άρα για να «δουλέψει» ο κανόνας πρέπει να δημιουργήσω και ένα δεύτερο ο οποίος θα απαγορεύει την εμφάνιση οποιαδήποτε http σελίδας και θα τοποθετηθεί πάνω από τον κανόνα που θα επιτρέπει την εμφάνιση της σελίδας.

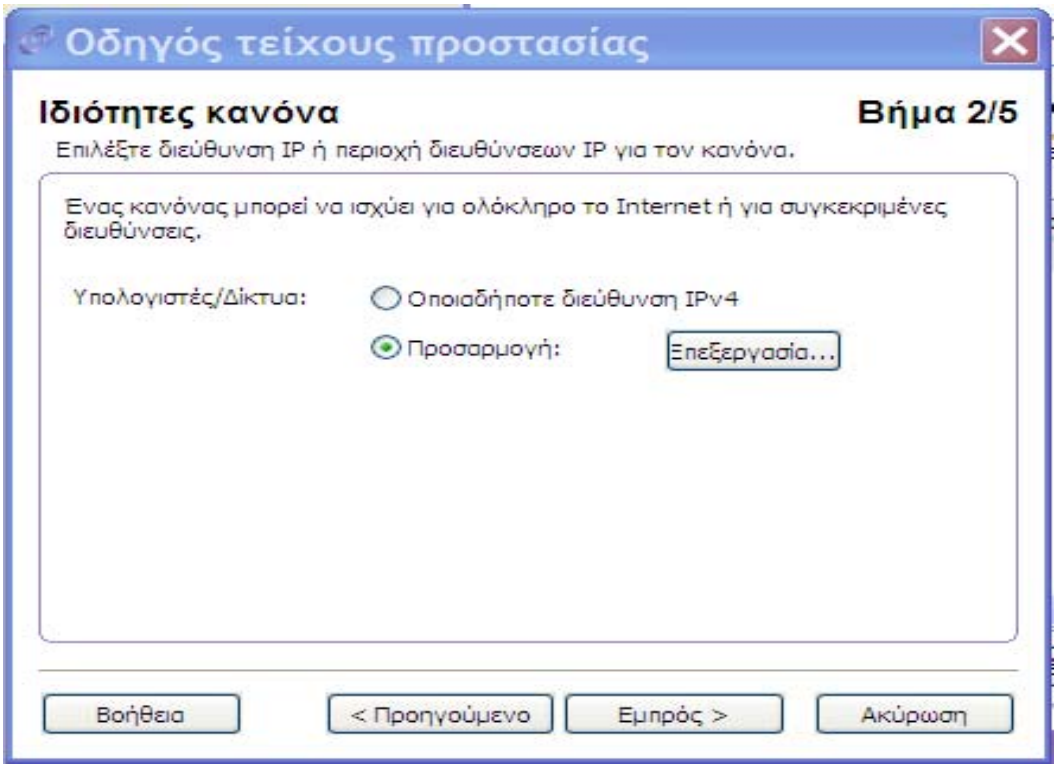
6. Απαγόρευση της εξερχόμενης κυκλοφορίας μόνο προς μία διεύθυνση ip.

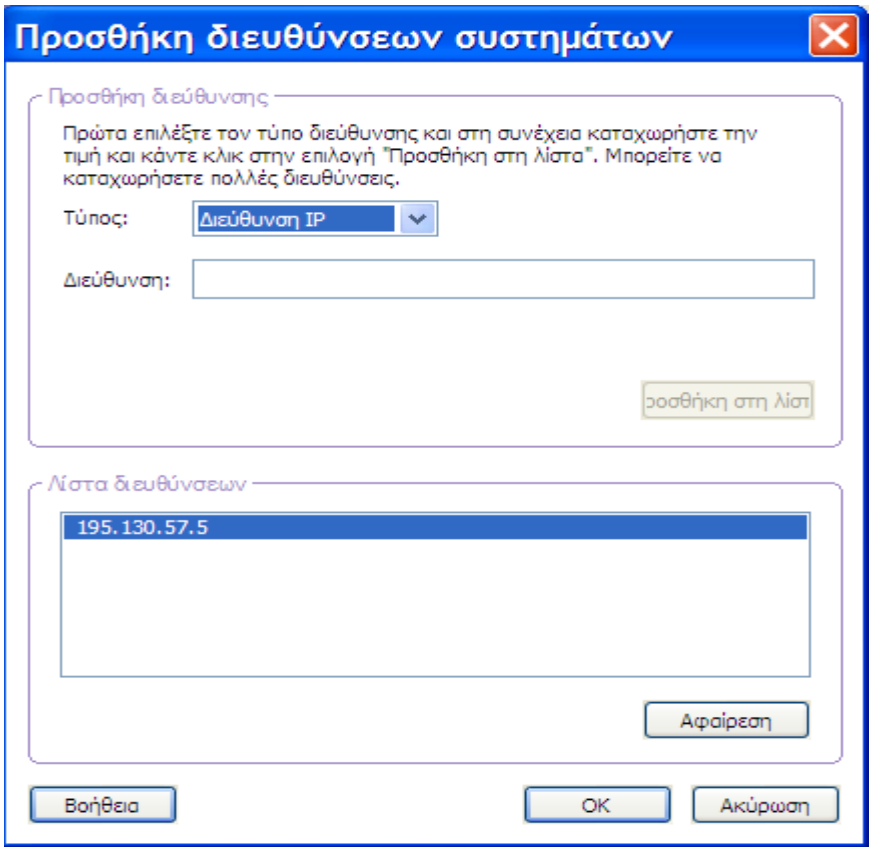
Ανοίγω την καρτέλα **Ασπίδα Προστασίας** → **Ρύθμιση Παραμέτρων** του **Τείχους Προστασίας**. Στην καρτέλα **Κανόνες** κάνω προσθήκη ενός νέου κανόνα ο οποίος θα απαγορεύει οποιαδήποτε εξερχόμενη κυκλοφορία προς την ip 195.130.67.5.

Στο πρώτο βήμα δίνω όνομα στον κανόνα «Απαγόρευση προς 195.130.67.5» και δηλώνω τη συμπεριφορά του κανόνα δηλαδή θα απαγορεύει ή θα επιτρέπει την κυκλοφορία.

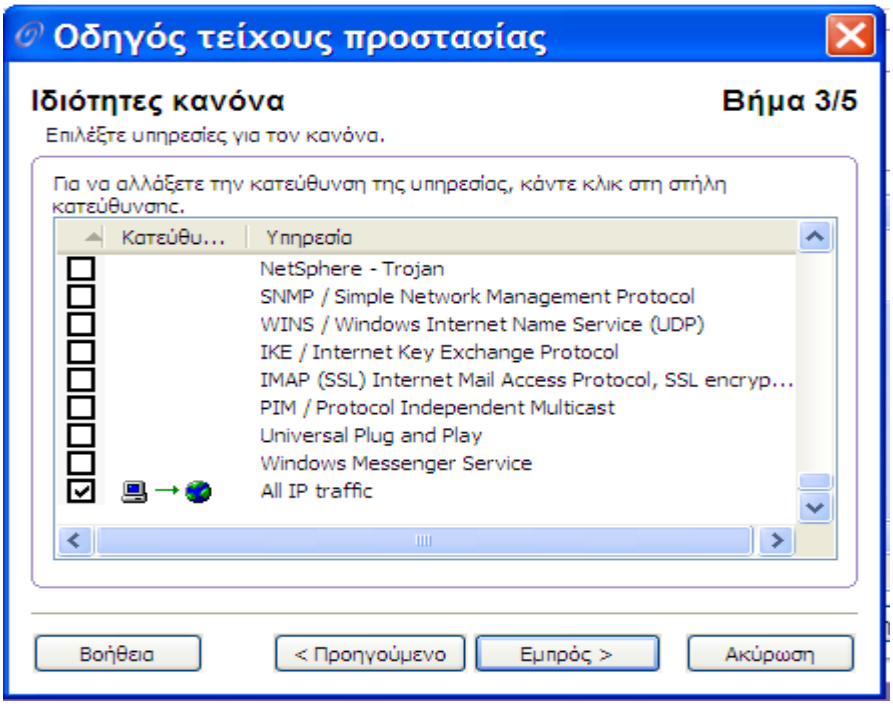


Στο δεύτερο βήμα ορίζω ποια διεύθυνση θα αφορά ο κανόνας. Στο παράδειγμα είναι 195.130.57.5

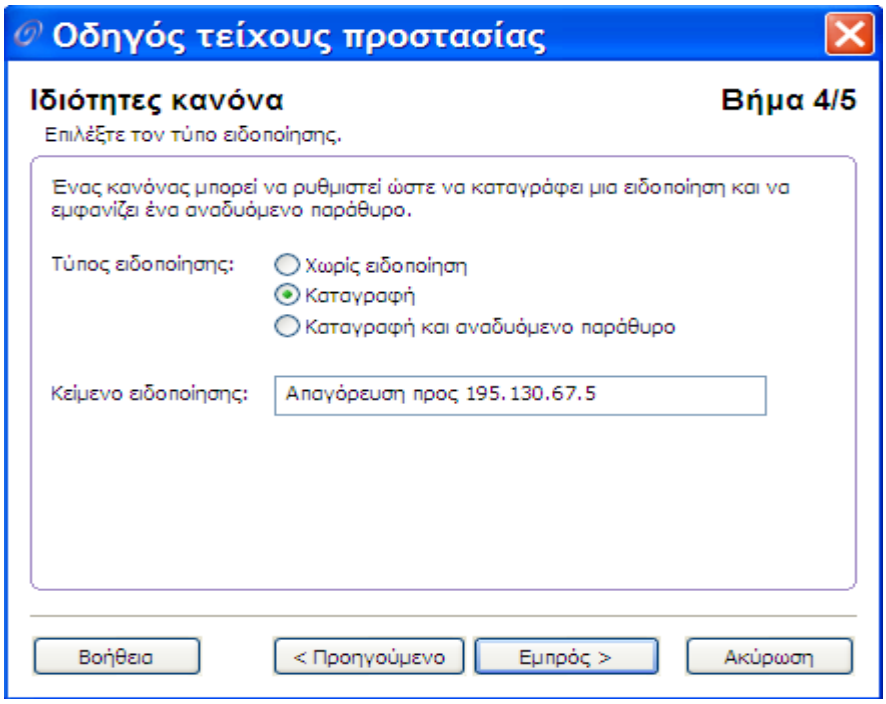




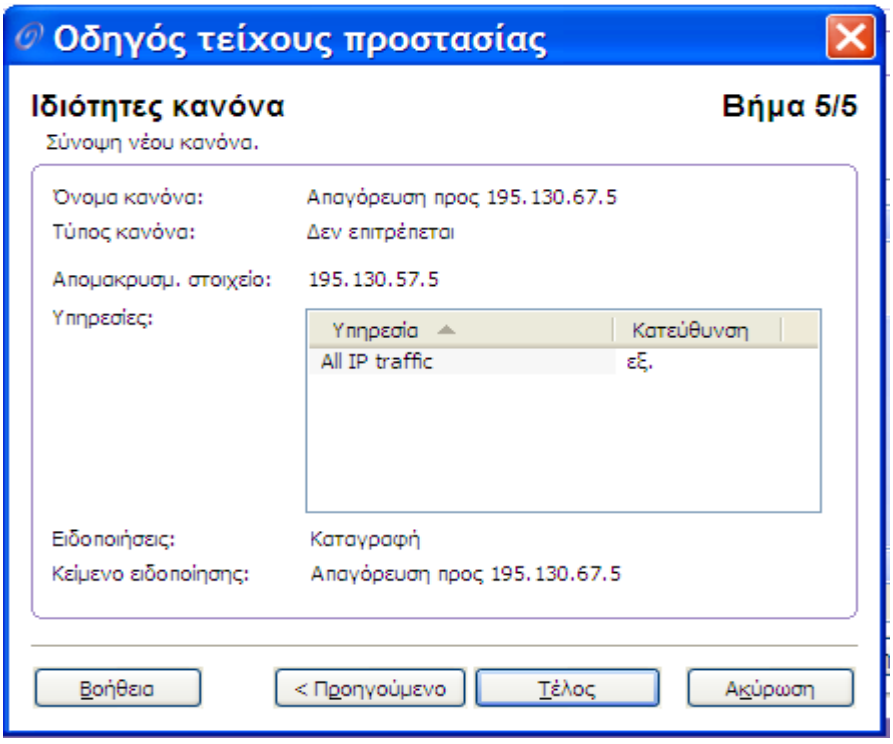
Στο τρίτο βήμα ορίζω ποια υπηρεσία αφορά ο κανόνας, και στην περίπτωσή μας είναι η ip κυκλοφορία, και ποια κατεύθυνση θα έχει η κυκλοφορία (εδώ εξερχόμενη).



Στο τέταρτο βήμα ορίζω αν θα καταγράφεται κάθε προσπάθεια εξερχόμενης κυκλοφορίας προς την ip που έχω ορίσει και το κείμενο που θα εμφανίζεται σαν προειδοποίηση.



Τέλος στο τελευταίο βήμα βλέπω συγκεντρωμένες τις ιδιότητες του κανόνα που έχω ορίσει.

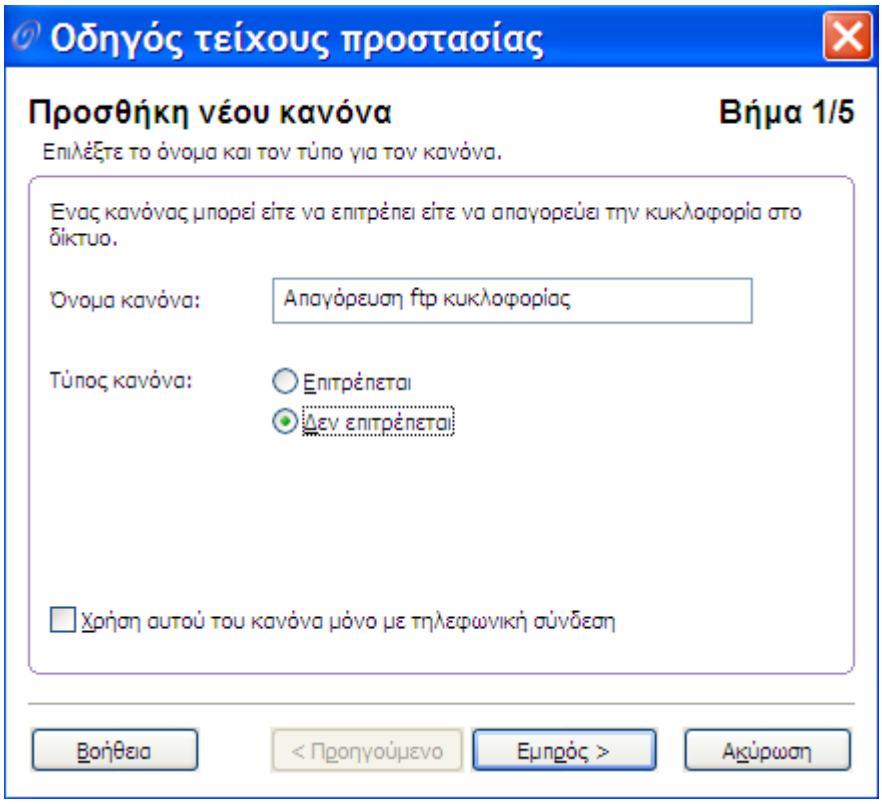


Επίσης μπορώ να προσθέσω έναν κανόνα ο οποίος θα επιτρέπει την εξερχόμενη κυκλοφορία μόνο προς μία ip ή ένα σύνολο ip διευθύνσεων.

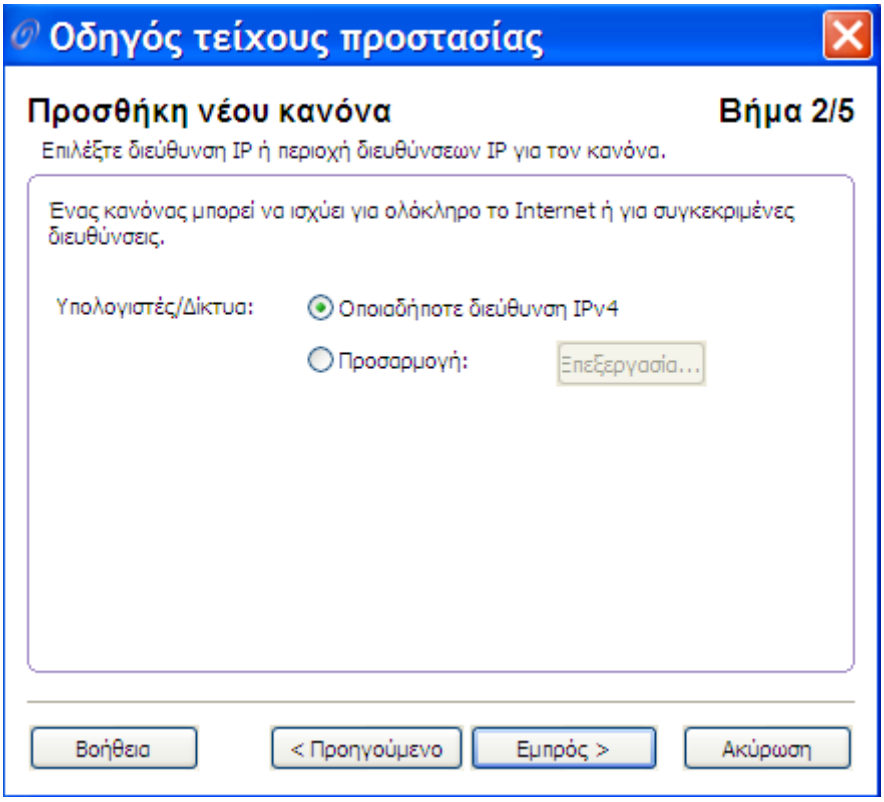
7. Απαγόρευση οποιαδήποτε ftp κυκλοφορίας.

Επιλέγω την καρτέλα **Ασπίδα Προστασίας** → **Ρύθμιση Παραμέτρων** του **Τείχους Προστασίας**. Στην καρτέλα **Κανόνες** κάνω προσθήκη ενός νέου κανόνα ο οποίος θα απαγορεύει οποιαδήποτε ftp κυκλοφορία.

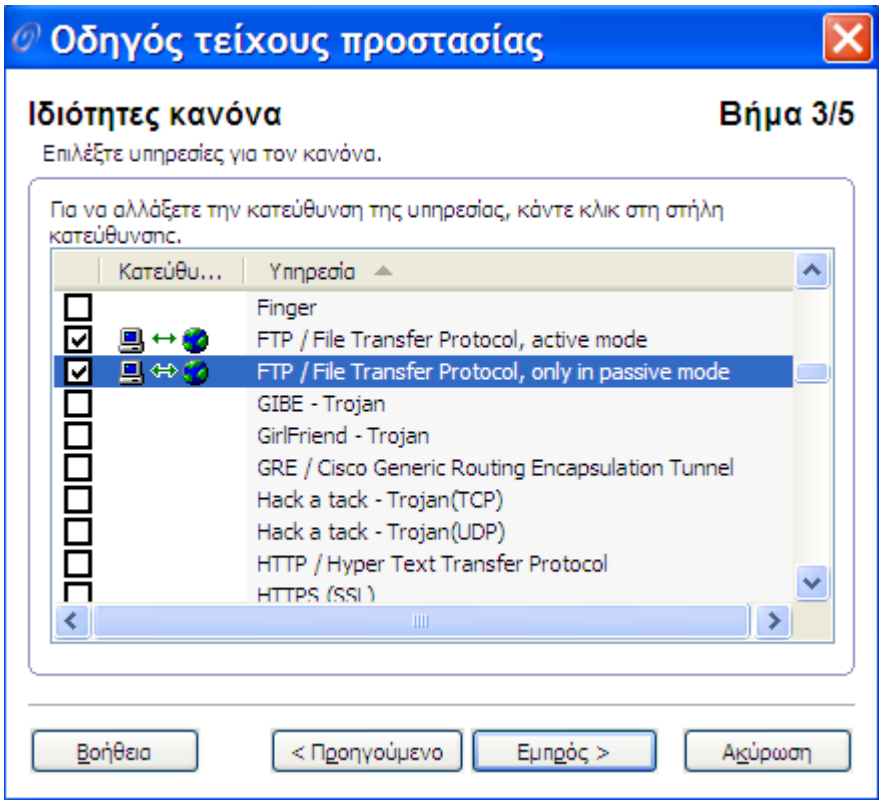
Στο πρώτο βήμα δίνω όνομα στον κανόνα «Απαγόρευση ftp κυκλοφορίας» και δηλώνω τη συμπεριφορά ότι ο κανόνας θα απαγορεύει την κυκλοφορία.



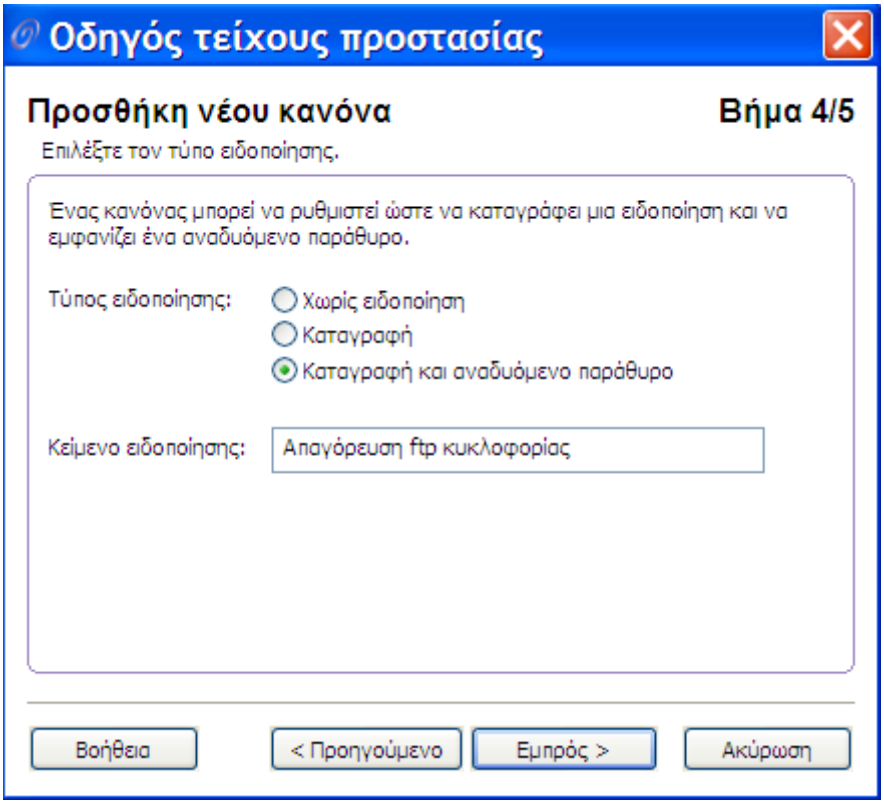
Στο δεύτερο βήμα ορίζω ότι ο κανόνας θα ισχύει για όλες τις Ip διευθύνσεις.



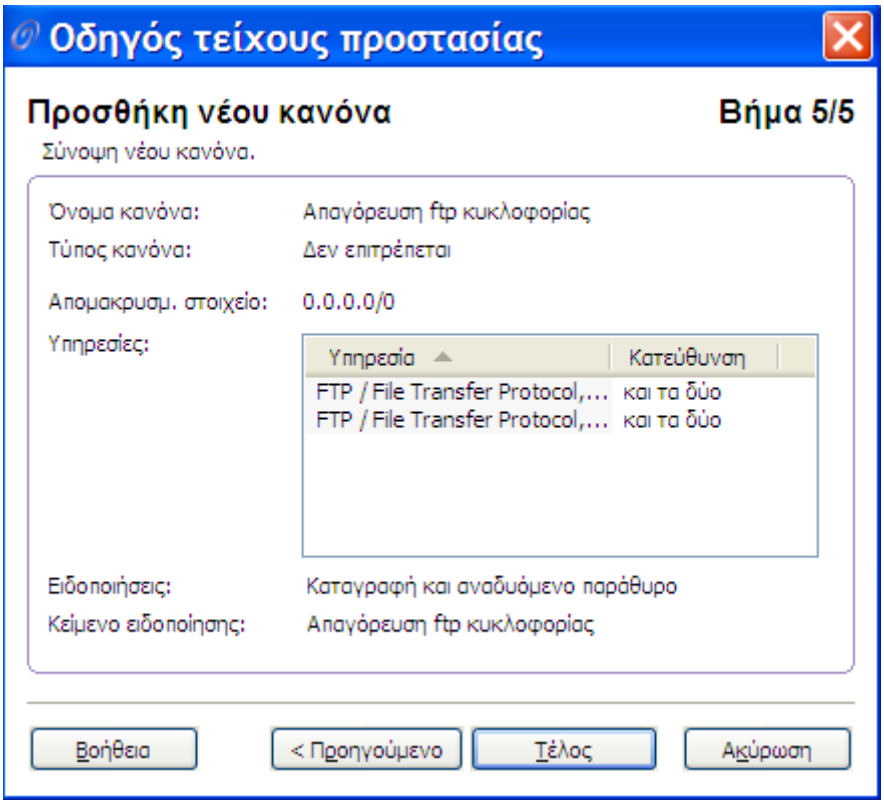
Στο τρίτο βήμα επιλέγω την υπηρεσία ftp και ορίζω ότι ο κανόνας θα ισχύει για κάθε είδους επικοινωνία (εισερχ/εξερχ).



Στο τέταρτο βήμα επιλέγω τον τύπο της ειδοποίησης.



Στο πέμπτο βήμα βλέπω μία σύνοψη των ιδιοτήτων που έχω ορίσει για τον κανόνα.



4. NETFILTER / IPTABLES

Έχοντας πλέον εξετάσει το **firewall** Otenet Security Kit θα μελετήσουμε ένα εργαλείο που μας παρέχει το Linux (έκδοση 2.4 και νεότερες) και ονομάζεται Netfilter-Iptables. Το εργαλείο αυτό θα λέγαμε πως δεν είναι τόσο απλό στη χρήση όσο το Otenet Security Kit, απαιτεί δηλαδή εξειδικευμένες γνώσεις. Είναι όμως πιο σταθερό, πιο ευέλικτο και μας παρέχει περισσότερες επιλογές και δυνατότητες. Πριν όμως εξετάσουμε το σύστημα αυτό ας πούμε κάποια πράγματα για το ίδιο το Linux.

Το **LINUX** είναι ένα open source (ανοικτού κώδικα) λειτουργικό σύστημα το οποίο βασίζεται στο Unix. Αναπτύχθηκε από τον Linus Torvalds υπό την επίβλεψη της GNU General Public License και ο κώδικας του είναι διαθέσιμος στον καθένα. Το Linux είναι ένα ολοκληρωμένο λειτουργικό σύστημα το οποίο περιλαμβάνει γραφικό interface, κειμενογράφο (Emacs) και άλλα εργαλεία.

Σε αντίθεση με τα windows το Linux είναι δημόσια ανοικτό και επεκτάσιμο. Σήμερα υπάρχουν διάφορες εκδόσεις του Linux, κάποιες από αυτές είναι: Red Hat, Mandrake, Debian, SuSE, κ.α. (Για περισσότερες πληροφορίες σχετικά με το λειτουργικό σύστημα Linux συμβουλευτείτε την προτεινόμενη βιβλιογραφία)

Το Linux λοιπόν μας παρέχει ένα πολύ σημαντικό εργαλείο για την ανάπτυξη firewall, το netfilter/iptables, το οποίο αναπτύσσουμε αναλυτικά παρακάτω.

Τι είναι το netfilter/iptables

Το έργο **netfilter/iptables** ξεκίνησε το 1998 από τον Rusty Russell συγγραφέα του προκάτοχου του iptables, του ipchains. Καθώς το έργο μεγάλωσε, το 1999 ίδρυσε την κύρια ομάδα του netfilter (Netfilter Core Team). Το λογισμικό που παρήγαγαν (netfilter) διανέμεται κάτω από τη γενική δημόσια άδεια χρήσης

(GPL) και ενσωματώθηκε στον πυρήνα Linux (2.4 έκδοση) το Μάρτιο του 2000.

Πριν συνεχίσουμε όμως πρέπει να ξεκαθαρίσουμε πως το netfilter και το iptables δεν είναι το ίδιο. Έχουν βέβαια αναπτυχθεί από την ίδια ομάδα προγραμματιστών και αναλυτών, αλλά είναι δύο διαφορετικά κομμάτια ενός συστήματος. Το **netfilter** αποτελεί τον κώδικα επιπέδου πυρήνα (kernel level code) όπου το Linux χρησιμοποιεί για το φιλτράρισμα των πακέτων, τον έλεγχο της κατάστασής τους, την μετάφραση των διευθύνσεων (nat) κ.τ.λ. Το **iptables** από την άλλη είναι το εργαλείο του χρήστη που χειρίζεται αυτά τα συστήματα.

Όταν αναφερόμαστε σε λειτουργίες τείχους προστασίας (firewalling) στο linux σε πυρήνες από 2.4 και μετά, χρησιμοποιούμε τους όρους netfilter και iptables χωρίς να αιτιολογούμε που χρησιμοποιείται ο καθένας.

Netfilter: Σύστημα φιλτραρίσματος πακέτων

Το Netfilter είναι το σύστημα που είναι μεταγλωττισμένο στον πυρήνα και παρέχει διαδικασίες οι οποίες μπορούν να χρησιμοποιήσουν τμήματα πυρήνα (kernel modules) για να εκτελέσουν λειτουργίες πάνω στα πακέτα. Το iptables είναι ένα τέτοιο module. Αφού το netfilter χρησιμοποιεί modules μπορεί κάλλιστα αντί του iptables να χρησιμοποιηθεί κάποιο άλλο module όπως το ipchains.

Το Netfilter είναι ένα πολύ ευέλικτο και δυνατό σύστημα (framework) φιλτραρίσματος πακέτων που προσφέρει ο πυρήνας του Linux. Το Netfilter παρέχει λειτουργίες φιλτραρίσματος πακέτων, NAT (Network Address Translation) και τροποποίησης των εισερχόμενων, εξερχόμενων, ή δρομολογούμενων μέσω του υπολογιστή πακέτων, καθιστώντας το Linux ένα πολύ δυνατό εργαλείο για την ανάπτυξη firewalls, των routers, και των gateways με δυνατότητες αντίστοιχες (ή ίσως και καλύτερες) με εκείνες

ακριβών εμπορικών εφαρμογών ή ακριβών hardware firewalls/ routers.

Network Address Translation (NAT)

Τι είναι;

Ένα πρότυπο που βρίσκει εφαρμογή σε τοπικά δίκτυα των οποίων οι υπολογιστές μοιράζονται μια κοινή σύνδεση Internet. Το NAT ορίζει σε κάθε ηλεκτρονικό υπολογιστή του τοπικού δικτύου μια διαφορετική εσωτερική διεύθυνση IP, της μορφής 192.168.x.x ή 10.1.x.x και μια κοινή εξωτερική IP με την οποία αναγνωρίζονται από άλλα συστήματα συνδεμένα στο Internet.

Το NAT βρίσκει εφαρμογή σε ιδιωτικά και εταιρικά δίκτυα που συνδέονται στο Internet μέσω routers και συνδέσεων ADSL ή μισθωμένων γραμμών. Πολλές φορές ο διαχειριστής των δικτύων αυτών θα πρέπει να ρυθμίσει κατάλληλα τους κανόνες NAT, ώστε να είναι εφικτή η πρόσβαση από το Internet σε υπηρεσίες και εφαρμογές που εκτελούνται σε συγκεκριμένο υπολογιστή του εσωτερικού δικτύου. Η ρύθμιση αυτή ονομάζεται και port forwarding. Επειδή όλοι οι ηλεκτρονικοί υπολογιστές εμφανίζονται στο διαδίκτυο με την ίδια διεύθυνση IP, ένας κανόνας NAT ή port forwarding καθορίζει σε ποιον από όλους θα πρέπει να αναζητηθεί μια συγκεκριμένη υπηρεσία. Αυτό γίνεται με την αντιστοίχιση του port της εν λόγω υπηρεσίας (π.χ. port 80 για HTTP server) στην εσωτερική διεύθυνση του υπολογιστή του τοπικού δικτύου όπου αυτή εκτελείται.

Μια από τις πιο κοινές χρήσεις του NAT είναι η λειτουργία **SNAT (Source Network Address Translation - μετάφραση διευθύνσεων δικτύων προέλευσης)**. Η λειτουργία αυτή χρησιμοποιείται, εάν δεν μπορούμε να έχουμε πραγματική δημόσια IP για κάθε έναν από τους πελάτες. Σε αυτή την περίπτωση χρησιμοποιούμε μια από τις ιδιωτικές διευθύνσεις IP για το τοπικό δίκτυο μας (παραδείγματος χάριν, 192.168.1.0/24) και έπειτα

ανοίγουμε SNAT για το δημόσιο δίκτυό μας. Το **SNAT** κατόπιν θα μετατρέψει όλες τις 192.168.1.0 διευθύνσεις σε δημόσια IP (παραδείγματος χάριν, 217.115.95.34). Με αυτόν τον τρόπο θα υπάρξουν 5-10 πελάτες, ή περισσότεροι που θα χρησιμοποιούν την ίδια διεύθυνση IP. Η ενέργεια αυτή εφαρμόζεται στα πακέτα στην αλυσίδα POSTROUTING.

Υπάρχει επίσης το **DNAT (Destination Network Address Translation - μετάφραση διευθύνσεων δικτύου προορισμού)**, το οποίο μπορεί να είναι εξαιρετικά χρήσιμο όταν πρέπει να παραμετροποιήσουμε τους εξυπηρετητές. Καταρχήν, μπορούμε να χρησιμοποιήσουμε ένα firewall μεταξύ του εξυπηρετητή μας και του πραγματικού εξυπηρετητή ή να μοιραστούμε απλά μια IP για διάφορους εξυπηρετητές που είναι διαμοιρασμένοι σε διάφορους φυσικά ηλεκτρονικούς υπολογιστές. Η ενέργεια αυτή εφαρμόζεται στα πακέτα στην αλυσίδα PREROUTING.

Κλασικές τεχνικές NAT

Καταρχάς η μετάφραση διευθύνσεων μπορεί να γίνει **στατικά** και **δυναμικά**. Στην πρώτη περίπτωση η αντιστοιχία NAT -IPs σε αρχικές IPs είναι σαφής, στη δεύτερη περίπτωση δεν είναι.

Στατικό NAT

Στο στατικό NAT μια ορισμένη αρχική IP είναι πάντα μεταφρασμένη στην ίδια NAT-IP και καμία άλλη IP δεν είναι μεταφρασμένη στην ίδια NAT-IP. Με τη στατική μετάφραση διευθύνσεων μπορούμε να μεταφράσουμε μεταξύ των δικτύων IP που έχουν το ίδιο μέγεθος (περιέχουν δηλαδή τον ίδιο αριθμό IPs).

Παράδειγμα στατικής NAT: Μεταφράστε όλες τις IPs στο δίκτυο 138.201.148 σε IPs στο δίκτυο της 94.64.15. Η μάσκα δικτύου είναι 255.255.255.0 και το 138.201.148.27 μεταφράστηκε σε 94.64.15.27 κλπ.

Δυναμικό NAT

Στο δυναμικό NAT η NAT-IP εξαρτάται από διάφορους παράγοντες και μπορεί να είναι διαφορετική για κάθε σύνδεση. Η δυναμική μετάφραση διευθύνσεων είναι απαραίτητη όταν ο αριθμός των IPs που πρέπει να μεταφραστούν δεν είναι ίσος με τον αριθμό των διαθέσιμων IPs για μετάφραση ή είναι ίσοι αλλά για κάποιους λόγους δεν είναι επιθυμητό να υπάρξει μια στατική χαρτογράφηση.

Παράδειγμα δυναμικής NAT: Μεταφράστε δυναμικά όλες τις IP διευθύνσεις του δικτύου 138.201 κατηγορίας Β σε διευθύνσεις δικτύου 178.201.112 κατηγορίας C. Κάθε νέα σύνδεση από το εσωτερικό παίρνει μια ορισμένη IP από την ομάδα των διευθύνσεων κατηγορίας C, εφ' όσον υπάρχουν αχρησιμοποίητες διευθύνσεις εάν μια χαρτογράφηση υπάρχει ήδη για τον εσωτερικό κόμβο χρησιμοποιείται αυτή.

Masquerade NAT

Μια ειδική περίπτωση δυναμικού NAT είναι η μ:1 μετάφραση ή μεταμφίεση (masquerade) που έγινε διάσημη με αυτό το όνομα. Είναι πιθανώς το είδος NAT που χρησιμοποιείται συχνότερα αυτές τις μέρες. Εδώ πολλές διευθύνσεις IP είναι κρυμμένες πίσω από μια ενιαία. Σε αντίθεση με το αρχικό δυναμικό NAT, αυτό δεν σημαίνει ότι μπορεί να υπάρξει μόνο μια σύνδεση τη φορά. Στη μεταμφίεση χρησιμοποιούνται οι πληροφορίες των TCP θυρών. Ο αριθμός ταυτόχρονων συνδέσεων περιορίζεται μόνο από τον διαθέσιμο αριθμό TCP θυρών.

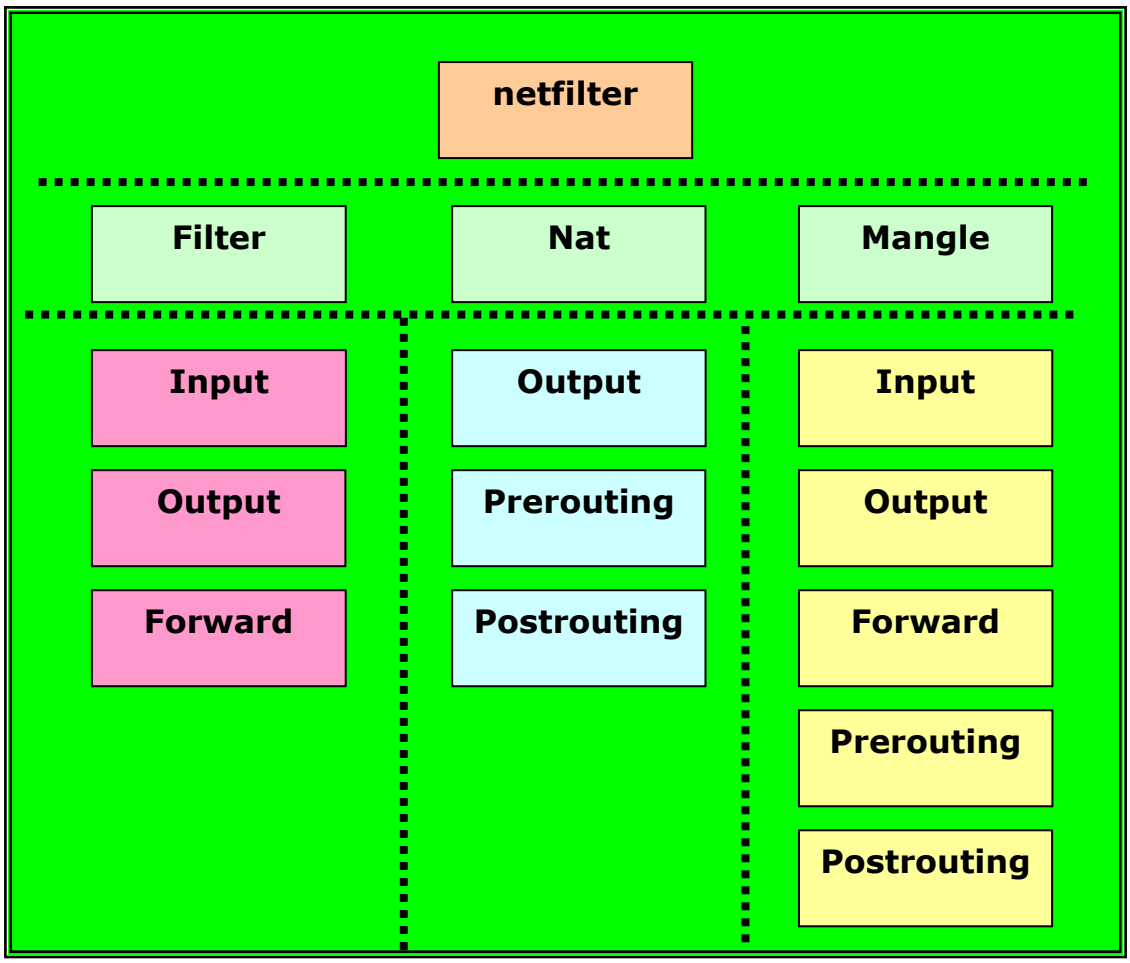
Παράδειγμα masquerade NAT: Μεταμφιέστε το εσωτερικό δίκτυο 138.201 χρησιμοποιώντας τη διεύθυνση του δρομολογητή για κάθε εξερχόμενο πακέτο η IP διεύθυνση προέλευσης αντικαθίσταται από την εξωτερική IP διεύθυνση του δρομολογητή και η θύρα

προέλευσης αλλάζει σε μια αχρησιμοποίητη, από τη σειρά που διατηρείται αποκλειστικά για τη μεταμφίεση στο δρομολογητή. Εάν η IP διεύθυνση προορισμού ενός εισερχόμενου πακέτου είναι ο τοπικός δρομολογητής και η θύρα προορισμού είναι μέσα στο εύρος των θυρών που χρησιμοποιούνται για τη μεταμφίεση στο δρομολογητή, ο NAT δρομολογητής ελέγχει στον πίνακα μεταμφιέσεων του, εάν το πακέτο ανήκει σε μια μεταμφιεσμένη σύνοδο, εάν αυτό συμβαίνει ο η διεύθυνση και η θύρα του εσωτερικού κόμβου παρεμβάλλονται και το πακέτο στέλνεται στον εσωτερικό κόμβο.

5. Αρχιτεκτονική του Netfilter:

Το σύστημα **netfilter** αποτελείται από τρεις **πίνακες (tables)**. Κάθε πίνακας περιέχει μια ομάδα **αλυσίδων (chains)** για συγκεκριμένο τρόπο διαχείρισης των πακέτων. Και κάθε αλυσίδα αποτελείται από κάποιους **κανόνες (rules)** που χειρίζονται τα πακέτα.

Στην εικόνα 8 φαίνεται η αρχιτεκτονική του συστήματος netfilter.



Εικόνα 11 - Η δομή του Netfilter

Πίνακες

Υπάρχουν τρεις προκαθορισμένοι πίνακες:

Πίνακας filter

Ο πίνακας αυτός είναι υπεύθυνος για το φιλτράρισμα (Επιτρέπει ή αποτρέπει σε ένα πακέτο να συνεχίσει την πορεία του). Κάθε πακέτο περνάει από τον πίνακα filter. Περιέχει τις παρακάτω προκαθορισμένες αλυσίδες:

- ***Αλυσίδα INPUT*** – Όλα τα πακέτα τα οποία προορίζονται για αυτό το σύστημα περνάνε από αυτή την αλυσίδα.
- ***Αλυσίδα OUTPUT*** – Όλα τα πακέτα που δημιουργούνται από αυτό το σύστημα περνάνε από αυτή την αλυσίδα.
- ***Αλυσίδα FORWARD*** – Όλα τα πακέτα τα οποία περνάνε από αυτό το σύστημα (δρομολογούνται - δημιουργούνται αλλού και έχουν προορισμό άλλο σύστημα) περνάνε από αυτή την αλυσίδα.

Πίνακας NAT

Ο πίνακας αυτός είναι υπεύθυνος για τους κανόνες τροποποίησης διευθύνσεων των πακέτων. Οι διευθύνσεις μπορεί να είναι τρίτου επιπέδου οπότε μιλάμε για ip διευθύνσεις ή τέταρτου επιπέδου οπότε μιλάμε για θύρες (ports). Το πρώτο πακέτο σε κάθε σύνδεση περνάει από αυτό τον πίνακα. Η απόφαση για το πρώτο πακέτο κάθε σύνδεσης καθορίζει και τις αλλαγές που θα γίνουν στα υπόλοιπα πακέτα της ίδιας σύνδεσης. Περιέχει τις παρακάτω προκαθορισμένες αλυσίδες:

- ***Αλυσίδα PREROUTING*** – Τα εισερχόμενα πακέτα περνάνε από αυτή την αλυσίδα πριν αποφασιστεί για το πού θα δρομολογηθούν. Εκεί γίνεται η μετάφραση της διεύθυνσης πριν την δρομολόγηση.
- ***Αλυσίδα POSTROUTING*** – Τα εξερχόμενα πακέτα περνάνε από αυτή την αλυσίδα αφού έχει αποφασιστεί για το που θα δρομολογηθούν Εκεί γίνεται η μετάφραση της διεύθυνσης μετά την δρομολόγηση.
- ***Αλυσίδα OUTPUT*** – Από αυτή την αλυσίδα περνάνε τα πακέτα που έχουν δημιουργηθεί τοπικά στο ίδιο το σύστημα και πρόκειται να τροποποιηθεί η διεύθυνση προορισμού.

Πίνακας mangle

Ο πίνακας αυτός είναι υπεύθυνος για την τροποποίηση χαρακτηριστικών του πακέτου όπως είναι ο τύπος υπηρεσίας (type of service) στην επικεφαλίδα ενός ip πακέτου. Όλα τα πακέτα περνάνε από αυτόν τον πίνακα. Περιέχει τις παρακάτω προκαθορισμένες αλυσίδες:

- ***Αλυσίδα PREROUTING*** – Όλα τα πακέτα που έρχονται στο σύστημα και πριν να αποφασιστεί αν πρέπει να προωθηθούν ή προορίζονται για το ίδιο το σύστημα περνάνε από αυτή την αλυσίδα.
- ***Αλυσίδα INPUT*** – Όλα τα πακέτα που προορίζονται για το σύστημα περνάνε από αυτή την αλυσίδα.
- ***Αλυσίδα FORWARD*** – Όλα τα πακέτα τα οποία περνάνε από αυτό το σύστημα (δρομολογούνται - δημιουργούνται αλλού και έχουν προορισμό άλλο σύστημα) περνάνε από αυτή την αλυσίδα.
- ***Αλυσίδα OUTPUT*** – Όλα τα πακέτα που δημιουργούνται από το σύστημα περνάνε από αυτή την αλυσίδα
- ***Αλυσίδα POSTROUTING*** – Όλα τα πακέτα που φεύγουν από το σύστημα περνάνε από αυτή την αλυσίδα.

Συγκεντρωτικός Επεξηγηματικός Πίνακας

Πίνακας	Λειτουργία του πίνακα	Αλυσίδα	Λειτουργία της αλυσίδας
Filter	Φιλτράρισμα πακέτων	FORWARD	Φιλτράρει τα πακέτα που πρόκειται να προωθηθούν
		INPUT	Φιλτράρει τα πακέτα που προορίζονται για το firewall
		OUTPUT	Φιλτράρει τα πακέτα που προέρχονται από το firewall
Nat	Μετάφραση διευθύνσεων δικτύου	PREROUTING	Μετάφραση διευθύνσεων δικτύου πριν από τη δρομολόγηση (τροποποίηση της ip διεύθυνσης προορισμού-DNAT)
		POSTROUTING	Μετάφραση διευθύνσεων δικτύου μετά από τη δρομολόγηση (τροποποίηση της ip διεύθυνσης προέλευσης-SNAT)
		OUTPUT	Μετάφραση διευθύνσεων δικτύου για πακέτα που προέρχονται από το firewall
Mangle	Τροποποίηση της ip επικεφαλίδας	PREROUTING POSTROUTING OUTPUT INPUT FORWARD	Τροποποίηση των TOS bits της ip επικεφαλίδας

Πίνακας 1 - Λειτουργία αλυσίδων

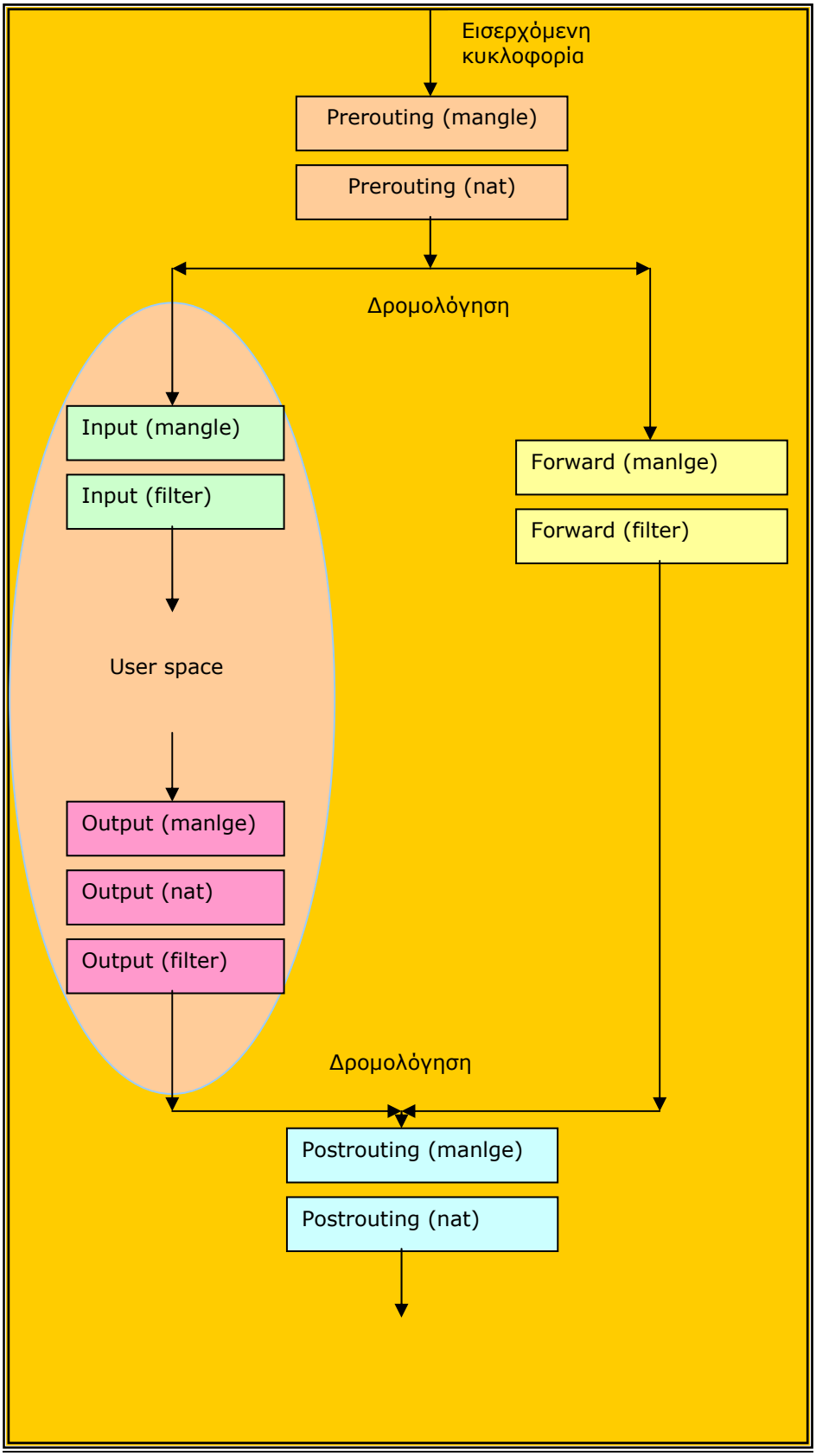
Οι αλυσίδες

Αυτό που πρέπει να τονίσουμε όσον αφορά τις αλυσίδες είναι ότι όλες οι αλυσίδες είναι μοναδικές, δηλαδή η INPUT του FILTER είναι διαφορετική από την INPUT του MANGLE. Μερικά χαρακτηριστικά των πακέτων μπορεί να ελεγχθούν μόνο σε συγκεκριμένες αλυσίδες.

Ο διαχειριστής συστήματος μπορεί να δημιουργήσει και να διαγράψει αλυσίδες σε κάθε πίνακα. Αρχικά όλες οι αλυσίδες είναι κενές και η προκαθορισμένη πολιτική είναι να αφήνουν τα πακέτα να περνάνε, χωρίς να τα απορρίπτουν ή να τα τροποποιούν.

Όταν ένα πακέτο στέλνεται σε μια αλυσίδα συγκρίνεται με κάθε κανόνα που έχει η αλυσίδα με τη σειρά. Ο κανόνας ορίζει τα χαρακτηριστικά που πρέπει να έχει το πακέτο έτσι ώστε να ταιριάζει με αυτόν, όπως η ip διεύθυνση προέλευσης ή η tcp θύρα προορισμού κτλ. Αν η αλυσίδα περιέχει κριτήρια που δεν ταιριάζουν με το πακέτο ο έλεγχος συνεχίζεται με τον επόμενο κανόνα. Αν όμως τα κριτήρια της αλυσίδας ταιριάζουν στο πακέτο τότε εκτελείται η ενέργεια του κανόνα και ο περαιτέρω έλεγχος με τους υπόλοιπους κανόνες σταματάει.

Σε περίπτωση όμως που το πακέτο δεν ταιριάζει με κανέναν κανόνα, τότε η **προεπιλεγμένη πολιτική της αλυσίδας (chain policy)** καθορίζει την τύχη του πακέτου. Μόνο η ενέργειες ACCEPT και DROP μπορούν να χρησιμοποιηθούν ως προεπιλεγμένη πολιτική. Η προεπιλεγμένη πολιτική των αλυσίδων είναι η ACCEPT. Στην περίπτωση που δεν αρκούν αυτές οι επιλογές μία λύση είναι να εισάγουμε έναν κανόνα για όλα τα πακέτα που δεν ταιριάζουν στους προηγούμενους κανόνες και να εφαρμόσουμε σε αυτά όποια ενέργεια θέλουμε. Για να μη μας «ξεφύγει» όμως κανένα πακέτο μπορούμε να αλλάξουμε και την προεπιλεγμένη πολιτική σε DROP. ***Τονίζεται ότι προεπιλεγμένη πολιτική έχουν μόνο οι build-in αλυσίδες και όχι αυτές που δημιουργήθηκαν από το χρήστη.***



Εικόνα 12 - Η σειρά διέλευσης από τις αλυσίδες

Κανόνες

Κάθε κανόνας καθορίζει τα χαρακτηριστικά που πρέπει να έχει το πακέτο για να ταιριάζει στην αλυσίδα, ορίζει δηλαδή τα κριτήρια, και μία ενέργεια που ορίζει τι θα γίνει με κάποιο πακέτο που ταιριάζει στον κανόνα. Κάθε εισερχόμενο ή εξερχόμενο πακέτο περνάει από μια ή περισσότερες αλυσίδες. Αν δεν ταιριάξει ελέγχεται από τον επόμενο κανόνα μέχρι να φτάσει στο τέλος της αλυσίδας όπου εφαρμόζεται η προεπιλεγμένη πολιτική.

Οι κανόνες ορίζουν κριτήρια που μπορεί να είναι:

- Το πρωτόκολλο του πακέτου (π.χ. TCP, UDP, ICMP, GRE, IGMP κλπ).
- Η θύρα (port) αφετηρίας ή προορισμού (για όσα πρωτόκολλα αυτή ορίζεται).
- Η διεύθυνση αφετηρίας ή προορισμού.
- Η κατάσταση της σύνδεσης (stateful inspection).
- Ο ρυθμός εισροής πακέτων.
- Η φυσική διεύθυνση (MAC address).
- Το ποιος χρήστης εκτελεί το πρόγραμμα που προκαλεί αυτήν την κίνηση κλπ.

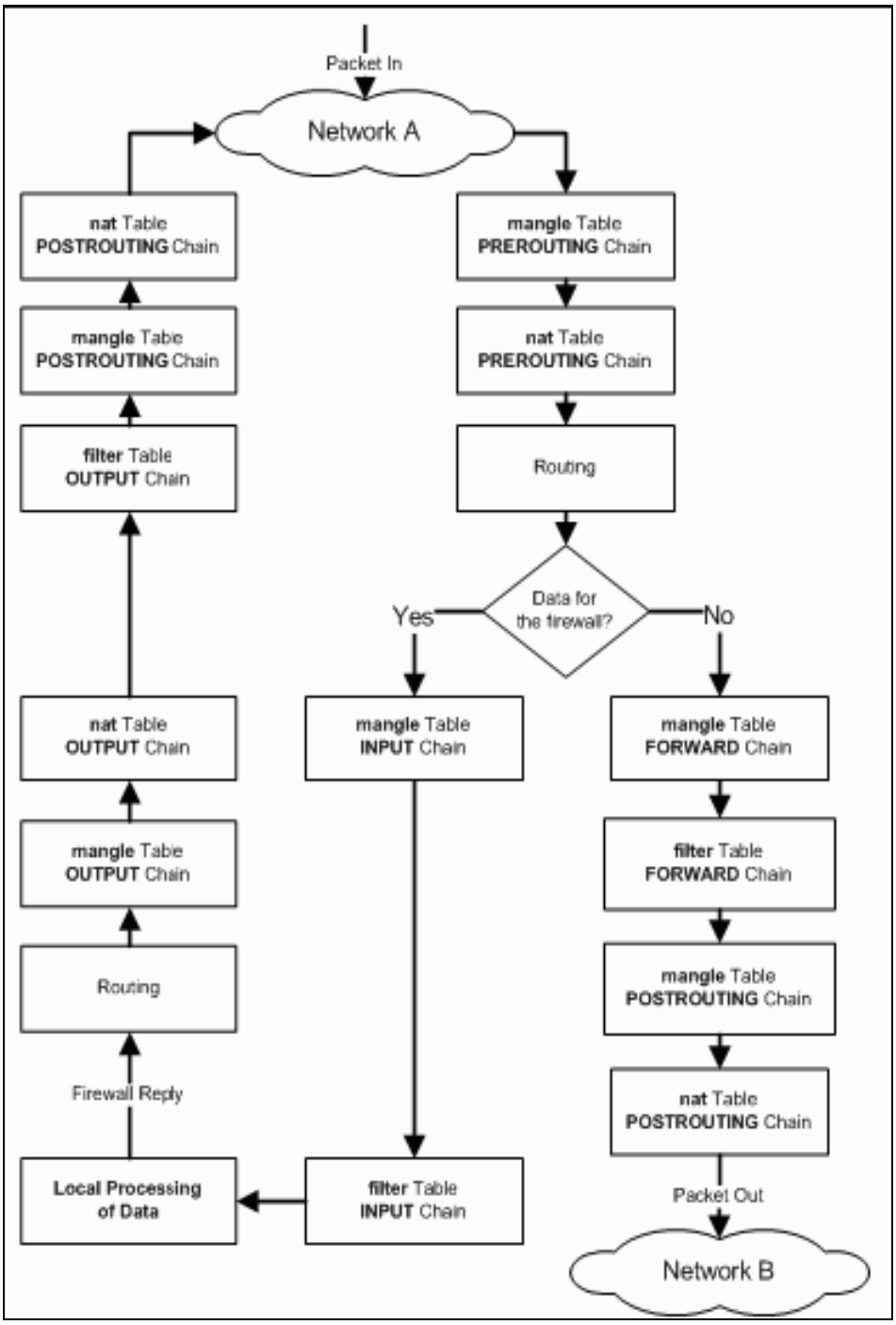
Τρόπος χειρισμού των πακέτων από τα iptables

Στην παρακάτω εικόνα (Εικόνα 10) φαίνεται η πορεία που ακολουθεί ένα tcp πακέτο, φτάνοντας στη διασύνδεση του firewall στο δίκτυο Α, προσπαθώντας να δημιουργήσει μια σύνδεση με έναν υπολογιστή που βρίσκεται στο δίκτυο Β.

Το πακέτο πρώτα ελέγχεται από τους κανόνες που υπάρχουν στην αλυσίδα PREROUTING του πίνακα mangle (για τον καθορισμό του τύπου υπηρεσίας) -αν υπάρχουν-. Ύστερα ελέγχεται από τους κανόνες στην αλυσίδα PREROUTING του πίνακα nat για να αποφασιστεί αν χρειάζεται να γίνει DNAT (να αλλάξει δηλαδή η

διεύθυνση προορισμού του ip πακέτου). Μετά γίνεται η δρομολόγηση.

Αφού το πακέτο προορίζεται για υπολογιστή του δικτύου Β και όχι για το ίδιο το firewall, θα ελεγχθεί με τους κανόνες της αλυσίδας FORWARD του πίνακα mangle και με τους κανόνες της αλυσίδας



Εικόνα 13 - τρόπος χειρισμού των πακέτων

FORWARD του πίνακα filter για να αποφασιστεί αν πρέπει να απορριφθεί ή όχι.

Πριν φύγει για το δίκτυο Β περνάει από την αλυσίδα POSTROUTING του πίνακα mangle και μετά από την αλυσίδα POSTROUTING του nat για να αποφασιστεί αν πρέπει να γίνει SNAT (να αλλάξει η διεύθυνση προέλευσης).

Σε περίπτωση που το πακέτο προοριζονταν για το ίδιο το firewall, το πακέτο θα περνούσε από την αλυσίδα INPUT του mangle, μετά από την αλυσίδα INPUT του filter και αφού από τους κανόνες αποφασιστεί ότι το πακέτο δεν πρέπει να απορριφθεί, τότε θα έφτανε στην εφαρμογή για περαιτέρω επεξεργασία.

Σε κάποιο σημείο το firewall χρειάζεται να απαντήσει. Η απάντηση δρομολογείται και εξετάζεται από τους κανόνες της αλυσίδας OUTPUT του πίνακα mangle. Ύστερα οι κανόνες της αλυσίδας OUTPUT του πίνακα nat καθορίζουν αν χρειάζεται να γίνει μετάφραση της διεύθυνσης δικτύου προορισμού και μετά ελέγχεται από την αλυσίδα OUTPUT του πίνακα filter.

Τελικά το πακέτο περνάει από την αλυσίδα POSTROUTING των mangle και nat και ύστερα αποστέλλεται.

Ενέργειες των Iptables

Κάθε κανόνας που ταιριάζει με ένα πακέτο καθορίζει τι θα γίνει με αυτό. Η λειτουργία πάνω στο πακέτο: αποδοχή, απόρριψη ή τροποποίηση καθορίζεται από την ενέργεια του κανόνα. Παρακάτω ακολουθούν οι συνηθέστερες ενέργειες με τις περιγραφές τους και τις συνηθισμένες επιλογές τους.

- **ACCEPT**: με την ACCEPT το firewall αποδέχεται το πακέτο ως «καλό» και «ακίνδυνο» για το σύστημα, και το στέλνει εκεί που θα έπρεπε να πάει κανονικά, σύμφωνα με τα στοιχεία που φέρει.

- **DROP:** όταν κάνουμε DROP ένα πακέτο, τότε ουσιαστικά το σβήνουμε από τη μνήμη και είναι σα να μην υπήρξε ποτέ. Εννοείται ότι δε φτάνει ποτέ στον τελικό του προορισμό.
- **QUEUE**: Το πακέτο μεταφέρεται για επεξεργασία στον χώρο του χρήστη. Εάν δεν υπάρχει εφαρμογή στο χώρο του χρήστη τότε η ενέργεια αυτή είναι ισοδύναμη με την DROP.
- **RETURN**: Σταματάει ο έλεγχος σε αυτή την αλυσίδα και ο έλεγχος συνεχίζεται με τους κανόνες της καλούσας αλυσίδας.
- **LOG:** το target αυτό είναι non-terminating, δηλαδή - σε αντίθεση με τα ACCEPT, DROP και REJECT - το πακέτο συνεχίζει την πορεία του στην αλυσίδα. Αυτό που κάνει το LOG είναι ότι γράφει μια καταχώρηση στο syslog του συστήματος, με κάποιες πληροφορίες για το πακέτο που έκανε match δηλαδή που ταιριάζει με τα κριτήρια του κανόνα. Η προσεκτική χρήση του κανόνα μπορεί να μας παράσχει πολύτιμες πληροφορίες για διάφορες «ύποπτες» δραστηριότητες πακέτων στο δίκτυό μας. Τέλος ως target μπορεί να χρησιμοποιηθεί οποιαδήποτε user-defined αλυσίδα. Η δυνατότητα αυτή διευκολύνει το φιλτράρισμα κατά ομάδες κίνησης. Έστω π.χ. εάν έχουμε ένα μηχάνημα με πολλές κάρτες δικτύου και θέλουμε να εφαρμόσουμε διαφορετικούς κανόνες σε κάθε κάρτα.
- **REJECT:** όταν απορρίπτουμε ένα πακέτο με REJECT, τότε το σβήνουμε από τη μνήμη και δε φτάνει ποτέ στον τελικό του προορισμό. Σε αντίθεση με τη DROP όμως, στέλνουμε ένα μήνυμα πίσω στον αποστολέα, το οποίο συνήθως τον ενημερώνει για το λόγο της απόρριψης. π.χ.:
  Κώδικας:
  iptables -p tcp --dport 80 -j REJECT --reject-with icmp-host-prohibited. Εάν δεν καθοριστεί η επιλογή «--reject-with» τότε ο προεπιλεγμένος τύπος είναι «icmp-host-unreachable».Είναι

συνετό να χρησιμοποιούμαι την εντολή REJECT για τα πακέτα που δημιουργούνται μέσα στο τοπικό μας δίκτυο έτσι ώστε να είναι ευκολότερη η διόρθωση σφαλμάτων. Η ενέργεια αυτή είναι διαθέσιμη για τις αλυσίδες: INPUT, FORWARD και OUTPUT.

- **DNAT**: Χρησιμοποιείται για τη μετάφραση της διεύθυνσης δικτύου προορισμού.
- **SNAT** : Χρησιμοποιείται για τη μετάφραση της διεύθυνσης δικτύου προέλευσης.
- **MASQUERADE**: Χρησιμοποιείται για τη μετάφραση της διεύθυνσης δικτύου προέλευσης. Εξ' ορισμού ως διεύθυνση προέλευσης επιλέγεται η διεύθυνση της εξερχόμενης διεπαφής του firewall.
- **TOS**: Χρησιμοποιείται για την τροποποίηση του πεδίου Type-Of-Service της ip επικεφαλίδας. Χρησιμοποιείται μόνο από τον πίνακα mangle.

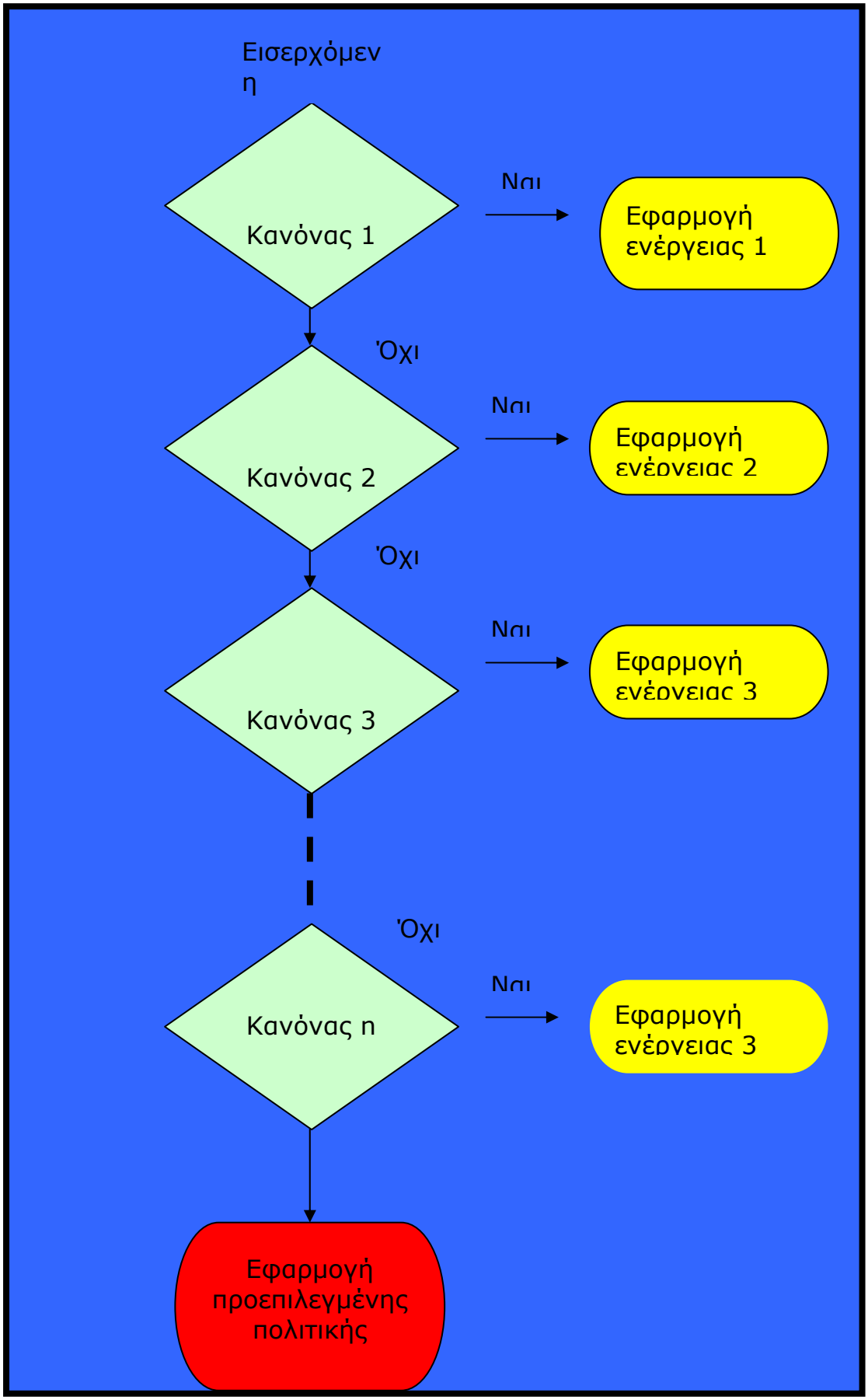
Τι γίνεται όμως όταν τα πακέτα διατρέχουν τις αλυσίδες;

Τα πακέτα διατρέχουν μια αλυσίδα από την κορυφή προς τα κάτω, δηλαδή από τον πρώτο κανόνα προς τον τελευταίο, γι' αυτό και **η σειρά με την οποία βάζουμε τους κανόνες έχει σημασία**. Κάθε κανόνας της αλυσίδας είναι στην πραγματικότητα ένα conditional if, με κάποια κριτήρια σχετικά με το πακέτο.

Αν το πακέτο συμφωνεί με τα κριτήρια του κανόνα, τότε κατευθύνεται προς έναν προορισμό (**target**), όπου εφαρμόζεται πάνω του μια ενέργεια. Οι προορισμοί για το μεν φιλτράρισμα μπορούν να είναι οι «κλασσικοί» **ACCEPT, DROP, REJECT** και **LOG**, για το nat μπορεί να είναι **DNAT** (destination NAT), SNAT (source NAT) ή **MASQUERADE** (dynamic source NAT), ενώ για το mangle διατίθενται διάφοροι «ειδικοί» προορισμοί (π.χ. MARK, CONNMARK, TCPMSS κλπ). Τέλος, σε όλα τα tables μπορούμε να ορίσουμε δικές

μας αλυσίδες, οι οποίες μπορούν να χρησιμεύσουν ως προορισμοί για τα πακέτα. Στο σημείο αυτό αξίζει να τονιστεί ότι κάποιοι προορισμοί είναι «τερματικοί» (terminating), δηλαδή τα πακέτα σταματούν εκεί και δε διασχίζουν την υπόλοιπη αλυσίδα, ενώ κάποιο άλλοι προορισμοί είναι απλά προορισμοί διέλευσης. Για παράδειγμα οι ACCEPT, DROP και REJECT είναι τερματικοί, αφού είτε αποδεχόμαστε το πακέτο (ACCEPT) και το στέλνουμε προς το δίκτυο, είτε το απορρίπτουμε (DROP και REJECT), ενώ οι προορισμοί LOG και MARK για παράδειγμα δεν είναι τερματικοί.

Στην περίπτωση που το πακέτο δεν ταιριάξει με κανένα κριτήριο εφαρμόζεται σε αυτό οι προεπιλεγμένη πολιτική της αλυσίδας (ACCEPT).



Εικόνα 14 - Ροή πακέτων σε μια αλυσίδα του filter table

6. Iptables – Σύνταξη

Σύνταξη των εντολών

Τα **iptables** είναι ένα εργαλείο συστήματος που επιτρέπει στον διαχειριστή να ρυθμίζει κανόνες, αλυσίδες και πίνακες. Επειδή τα **iptables** απαιτούν αρκετά δικαιώματα για να λειτουργήσει πρέπει να εκτελεστεί από το διαχειριστή - root, αλλιώς αποτυχαίνει η εκτέλεση.

Στα περισσότερα συστήματα Linux είναι εγκατεστημένο ως /sbin/iptables. Η λεπτομερής περιγραφή των παραμέτρων της εντολής περιγράφεται στο εγχειρίδιο της (man page). Για να το δει κανείς αρκεί να πληκτρολογήσει man iptables.

Μια εντολή iptables αποτελείται συνήθως από 5 μέρη:

1. τον **πίνακα** τον οποίο θέλουμε να χρησιμοποιήσουμε και παίρνει τις τιμές filter, nat και mangle. Αν παραληφθεί, τότε η iptables υποθέτει ότι μιλάμε για τον πίνακα filter.
2. την **αλυσίδα,** σε αυτόν τον πίνακα που, θέλουμε για να χρησιμοποιήσουμε.
3. μια **λειτουργία** (εισαγωγή, πρόσθεση, διαγραφή, τροποποίηση).
4. μια **περιγραφή ενεργειών** για αυτόν τον κανόνα
5. μια **περιγραφή των πακέτων** που θέλουμε να ταιριάξουμε με αυτόν τον κανόνα.

Η βασική σύνταξη είναι:

iptables -t table [πίνακας] -Operation chain [αλυσίδα του πίνακα] matching rules -j target [ενέργεια αλυσίδας] target options

Κριτήρια που πρέπει να πληρεί το πακέτο.

Η περιγραφή του κανόνα ξεκινά με τα κριτήρια που πρέπει να πληρεί το πακέτο:

- Πρωτόκολλο: **-p** [tcp,icmp,udp,...]
- Διεύθυνση αποστολέα: **-s** 1.2.3.4
- Διεύθυνση παραλήπτη: **-d** 2.3.4.5
- Θύρα αποστολής: **--sport** 123 ή **--source-port** 1234
- Θύρα προορισμού: **--dport** 2345 ή **--destination-port** 2345
- Interface εισόδου (μόνο στις INPUT, PREROUTING, FORWARD): **-i eth0**
- Interface εξόδου (μόνο στις OUTPUT, POSTROUTING, FORWARD): **-o eth1**
- και ολοκληρώνεται με την ενέργεια-προορισμό: **-j** [ACCEPT, DROP, REJECT, LOG, ...].

Βασικές λειτουργίες (iptables switches)

-A Εισαγωγή κανόνα στο τέλος της αλυσίδας

-I Εισαγωγή κανόνα σε συγκεκριμένη θέση

-**D** Διαγραφή κανόνα

-R Αντικατάσταση κανόνα με κάποιον άλλο

-L Λίστα κανόνων

-F Διαγραφή όλων των κανόνων

-N Δημιουργία αλυσίδας

-P Αλλαγή της πολιτικής μιας αλυσίδας

-X Διαγραφή αλυσίδας

-E Μετονομασία αλυσίδας

-h Εμφάνιση πληροφοριών

-t ακολουθεί πίνακας

-m ακολουθεί η κατάσταση του πακέτου

-j ακολουθεί η ενέργεια

Βασικές αντιστοιχίες κοινές για όλες τις αλυσίδες:

-p πρωτόκολλο (tcp /icmp /udp/…)

-s διεύθυνση προέλευσης (διεύθυνση IP /μήκος μάσκας)

-d διεύθυνση προορισμού (διεύθυνση IP/ μήκος μάσκας)

-i εισερχόμενη διεπαφή

-o εξερχόμενη διεπαφή

Κοινά κριτήρια TCP και UDP

Παράμετροι	Περιγραφή
- p tcp --sport <port>	TCP θύρα προέλευσης Μπορεί να είναι μια συγκεκριμένη θύρα ή ένα εύρος θυρών στη μορφή start-port-number: end-port-number
-p tcp --dport <port>	TCP θύρα προορισμού
-p tcp --syn	Χρησιμοποιείται για να προσδιορίσει ένα νέο αίτημα σύνδεσης TCP ! --syn σημαίνει ότι δεν απαιτείται νέο αίτημα σύνδεσης
-p udp --sport <port>	UDP θύρα προέλευσης
-p udp --dport <port>	UDP θύρα προορισμού

Πίνακας 4 - Παράμετροι TCP και UDP

Κριτήρια ICMP

Παράμετροι	Περιγραφή
-p icmp --icmp-type <type>	Όπου type είναι ο τύπος του icmp μηνύματος με το οποίο ταιριάζει το πακέτο. Οι συνηθέστεροι τύποι είναι οι echo-reply και echo-request

Πίνακας 2 - Παράμετροι ICMP

Κριτήρια κατάστασης πακέτου

Το σύστημα **Netfilter** μας δίνει τη δυνατότητα να ελέγξουμε τα πακέτα και ως προς την κατάσταση της σύνδεσής τους, δηλαδή αν ένα πακέτο αποτελεί μέρος κάποιας νόμιμης σύνδεσης ή αν είναι πακέτο κάποιου επίδοξου εισβολέα. Το σύστημα αναγνωρίζει 4 καταστάσεις των πακέτων:

- **NEW**: Το πακέτο ξεκινάει μια νέα σύνδεση. Μόνο το πρώτο πακέτο της σύνδεσης θα έχει αυτή την κατάσταση, οι καταστάσεις των υπόλοιπων πακέτων της σύνδεσης δεν θα θεωρηθούν σαν new.
- **ESTABLISHED**: Αναφερόμαστε σε μία σύνδεση η οποία έχει αποκατασταθεί και έχει αναγνωρισθεί από το firewall (state engine), τα πακέτα που ακολουθούν ένα πακέτο με κατάσταση new έχουν κατάσταση established.
- **RELATED**: Είναι μία ειδική κατάσταση όπου μία ξεχωριστή σύνδεση σχετίζεται με μία υπάρχουσα σύνδεση. Αυτό συμβαίνει όταν μία σύνδεση δημιουργεί μία ακόμη σύνδεση ως τμήμα της διαδικασίας μεταφοράς των δεδομένων της, όπως πχ ένα ICMP μήνυμα λάθους.
- **INVALID**: Αφορά κάποιο πακέτο του οποίου η κατάσταση δεν μπορεί να αναγνωρισθεί. Είναι συνετό τα πακέτα αυτά να απορρίπτονται.

Παράμετροι	Περιγραφή
-m state --state <state>	Όπου state είναι η κατάσταση του πακέτου και μπορεί να είναι μια από: NEW, ESTABLISHED, RELATED, INVALID

Πίνακας 3 - Παράμετρος -m state

7. Παραδείγματα χρήσης iptables

1. ***Προσθήκη κανόνα στο τέλος της αλυσίδας***.

Όλα τα πακέτα που εισέρχονται στην αλυσίδα **INPUT** καταγράφονται από το σύστημα.

Κώδικας:

iptables -A INPUT -j LOG

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-A** δηλώνει ότι θα γίνει εισαγωγή ενός κανόνα στο τέλος της αλυσίδας **INPUT** (εισερχόμενη κυκλοφορία), το **–j** δηλώνει ότι ακολουθεί η ενέργεια **LOG.**

Παρατηρούμε ότι δεν αναφέρεται ο πίνακας, όταν συμβαίνει αυτό καταλαβαίνουμε ότι αναφερόμαστε στον filter.

2. Προσθήκη κανόνα σε προκαθορισμένη θέση της αλυσίδας.

Θα εισάγουμε έναν κανόνα στη θέση 3 της αλυσίδας ***INPUT*** του πίνακα **FILTER** κατά τον οποίο τα πακέτα θα γίνονται δεκτά από την αλυσίδα.

Κώδικας:

iptables -I INPUT 3 -j ACCEPT

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **–I** δηλώνει τό θα γίνει εισαγωγή κανόνα στην αλυσίδα **INPUT** (εννοείται του filter) στη θέση **3,** το **–j** δηλώνει ότι ακολουθεί η

ενέργεια που θα εφαρμοστεί στα πακέτα και είναι η αποδοχή **ACCEPT.**

3. Αντικατάσταση κανόνα που βρίσκεται σε συγκεκριμένη θέση της αλυσίδας:

Αντικαθιστούμε τον κανόνα που υπάρχει στη θέση 3 της αλυσίδας **INPUT** με έναν νέο.

Κώδικας:

iptables -R INPUT 3 -p tcp --dport http –j ACCEPT

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-R** δηλώνει ότι θα αντικατασταθεί ο κανόνας που υπάρχει στην αλυσίδα **INPUT** (εννοείται του filter) στη θέση **3,** το **-p** πρωτόκολλο που μας ενδιαφέρει είναι το **tcp,** και η θύρα προορισμού **--dport** είναι η **http,** το **–j** μας πληροφορεί ότι ακολουθεί η ενέργεια **ACCEPT.**

4. Διαγραφή όλων των κανόνων της αλυσίδας.

Κώδικας:

iptables -F INPUT

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», ακολουθεί το **–F** όπου δηλώνει ότι θα διαγράψει όλους τους κανόνες της αλυσίδας **INPUT** (του filter)**.**

5. Διαγραφή όλων των κανόνων όλων των αλυσίδων ενός πίνακα.

Κώδικας:

iptables -t nat –F

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», ακολουθεί το **–t** που δηλώνει ότι ακολουθεί ο πίνακας **nat,** το **–F** θα διαγράψει όλους τους κανόνες του πίνακα.

6. **Διαγραφή κανόνα από συγκεκριμένη θέση της αλυσίδας.**

Κώδικας:

iptables –D INPUT 1

Αναλυτική επεξήγηση του κώδικα.

Η εντολή **iptables** τοποθετείται στην αρχή, **–D INPUT 1:** διαγράφεται ο κανόνας που βρίσκεται στην $1^{η}$ θέση στην αλυσίδα **INPUT,** (όταν δεν αναφέρεται πίνακας εννοείται ο filter).

7. ***Εμφάνιση των κανόνων που περιέχει μια αλυσίδα.***

Κώδικας:

iptables -L INPUT

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **–L** θα μας εμφανίσει όλους τους κανόνες που υπάρχουν στην αλυσίδα **INPUT.**

8. ***Εμφάνιση όλων των κανόνων όλων των αλυσίδων ενός πίνακα (π.χ. του πίνακα NAT).***

Κώδικας:

iptables -t nat -L

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί ο πίνακας **nat,** και το **–L** ότι θα μας εμφανίσει όλους τους κανόνες που υπάρχουν στον πίνακα.

9. Δημιουργία αλυσίδας

Κώδικας: iptables –N my_chain

Αναλυτική επεξήγηση του κώδικα.

Η εντολή **iptables** τοποθετείται στην αρχή, **–N:** δημιουργία αλυσίδας με όνομα **my_chain.**

10. Διαγραφή αλυσίδας.

Κώδικας: iptables –X my_chain

Αναλυτική επεξήγηση του κώδικα.

Η εντολή **iptables** τοποθετείται στην αρχή, **–X:** Διαγραφή της αλυσίδας με όνομα **my_chain.**

11. Μετονομασία αλυσίδας.

Κώδικας:

iptables –E my_chain new_name_for_my_chain

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **–E** δηλώνει ότι θα αλλάξει το όνομα της αλυσίδας που ακολουθεί, και από **my_chain** θα μετονομαστεί σε **new_name_for_my_chain.**

12. Απενεργοποίηση του firewall.

Για να απενεργοποιήσουμε το firewall έτσι ώστε να είναι δυνατή κάθε είδους εξερχόμενη και εισερχόμενη κυκλοφορία:

Κώδικας:

iptables -t filter -A INPUT -j ACCEPT

iptables -t filter -A OUTPUT -j ACCEPT

iptables -t filter -A FORWARD -j ACCEPT

13. Απαγόρευση κάθε είδους κυκλοφορίας.

Κώδικας:

iptables -t filter -A INPUT -j DROP

iptables -t filter -A OUTPUT -j DROP

iptables -t filter -A FORWARD -j DROP

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A INPUT:** Στην αλυσίδα **INPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A**, το **-j** δηλώνει ότι ακολουθεί κανόνας. **DROP:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **DROP** τα πακέτα θα απορρίπτονται**.**

Το ίδιο ισχύει και για τις αλυσίδες **OUTPUT, FORWARD.**

14. Για να προσθέσουμε έναν κανόνα που θα απαγορεύει την smtp κυκλοφορία.

Απαγορεύουμε δηλαδή να εξέλθουν από το σύστημα μας όλα τα Mail.

Κώδικας:

iptables -t filter -A OUTPUT -j DROP -p TCP -- dport smtp

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει

επισύναψη ενός κανόνα όπως δηλώνει το **-A**, το **-j** δηλώνει ότι ακολουθεί κανόνας. **DROP:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **DROP** τα πακέτα θα απορρίπτονται**, -p TCP:** το πρωτόκολλο που χρησιμοποιείται είναι το **TCP, -- dport smtp:** η θύρα που μας αφορά είναι η τοπική θύρα SMTP.

15. Απαγόρευση της εμφάνισης μιας ιστοσελίδας ή ενός συνόλου από σελίδες.

Αν θέλω να απαγορεύσω την εμφάνιση μίας ιστοσελίδας π.χ. www.teiser.gr :

Κώδικας:

iptables –t filter -A OUTPUT –sport http –d 195.130.67.5–j drop

Αν θέλω να απαγορεύσω την εμφάνιση ενός συνόλου από ιστοσελίδες π.χ. www.teiser.gr και www.teikoz.gr :

Κώδικας:

iptables –t filter -A OUTPUT –sport http –d 195.130.67.5,195.130.8.5 –j drop

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –sport http:** η θύρα προορισμού είναι η **http, –s 195.130.67.5,195.130.8.5:** και οι διευθύνσεις προέλευσης **–j drop:** , το **-j** δηλώνει ότι ακολουθεί κανόνας. **DROP:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **DROP**

16. Επιτρέπω την εμφάνιση μόνο μιας ιστοσελίδας ή ενός συνόλου από σελίδες ενώ απαγορεύω όλες τις υπόλοιπες.

Αν θέλω να επιτρέψω την εμφάνιση μίας ιστοσελίδας π.χ. www.teiser.gr :

Κώδικας:

iptables –t filter -A OUTPUT --sport http –d 195.130.67.5–j accept

iptables –t filter -A OUTPUT --sport http –j drop

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –sport http:** η θύρα προορισμού είναι η **http, –d 195.130.67.5:** και η διεύθυνση προέλευσης, **–j drop:** , το **-j** δηλώνει ότι ακολουθεί κανόνας. **accept:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **accept**

Από προεπιλογή το firewall επιτρέπει την εμφάνιση όλων των ιστοσελίδων, άρα είναι απαραίτητη η προσθήκη ενός κανόνα ο οποίος θα απαγορεύει την εμφάνιση όλων των υπολοίπων. Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –sport http:** η θύρα προορισμού είναι η **http,** το **-j** δηλώνει ότι ακολουθεί κανόνας. **DROP:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **DROP (απόρριψη)**

Αν θέλω να επιτρέψω την εμφάνιση ενός συνόλου από ιστοσελίδες π.χ. www.teiser.gr και www.teikoz.gr :

Κώδικας:

iptables –t filter -A OUTPUT –sport http –d 195.130.67.5,195.130.8.5 –j accept

iptables –t filter -A OUTPUT --sport http –j drop

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –sport http:** η θύρα προορισμού είναι η **http, –d 195.130.67.5,195.130.8.5:** και οι διευθύνσεις προέλευσης **–j drop:** , το **-j** δηλώνει ότι ακολουθεί κανόνας. **DROP:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **accept**

Από προεπιλογή το firewall επιτρέπει την εμφάνιση όλων των ιστοσελίδων, άρα είναι απαραίτητη η προσθήκη ενός κανόνα ο οποίος θα απαγορεύει την εμφάνιση όλων των υπολοίπων. Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –sport http:** η θύρα προέλευσης είναι η **http,** το **-j** δηλώνει ότι ακολουθεί κανόνας. **DROP:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **DROP (απόρριψη)**

17. Απαγόρευση της εξερχόμενης κυκλοφορίας προς μία ip ή προς ένα σύνολο από ip.

Κώδικας:

iptables –t filter -A OUTPUT –d 195.130.67.5 –j drop

iptables –t filter -A OUTPUT -d 195.130.67.5,195.130.8.5 –j drop

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –d 195.130.67.5:** η διεύθυνση προέλευσης είναι η **195.130.67.5, –j drop:** το **-j** δηλώνει ότι ακολουθεί ο κανόνας **DROP** δηλαδή η απόρριψη των πακέτων.
Από προεπιλογή το **firewall** επιτρέπει την εισερχόμενη κυκλοφορία, άρα είναι απαραίτητη η προσθήκη ενός κανόνα ο οποίος θα απαγορεύει την κυκλοφορία με τις άλλες ip. Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A,** το **-j** δηλώνει ότι ακολουθεί κανόνας. **DROP:** ο κανόνας που επισυνάπτεται είναι ο κανόνας **DROP (απόρριψη)**

18. Επιτρέπω την εισερχόμενη κυκλοφορία μόνο από μία ip ή από ένα σύνολο ip.

Κώδικας:

```
iptables –t filter -A INPUT –s 195.130.67.5 –j ACCEPT
```

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –d 195.130.67.5:** η διεύθυνση προέλευσης είναι η **195.130.67.5, –j drop:** το **-j** δηλώνει ότι ακολουθεί ο κανόνας **ACCEPT** δηλαδή η αποδοχή των πακέτων.

19. Το firewall απαγορεύει την ftp λήψη και αποστολή.

Κώδικας:

```
iptables –t filter -A INPUT –p ftp –s 195.130.67.5 –j drop
iptables –t filter -A OUTPUT –p ftp –d 195.130.67.5 –j drop
```

Αναλυτική επεξήγηση του κώδικα.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A INPUT:** Στην αλυσίδα **INPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –p ftp:** το πρωτόκολλο που εξετάζουμε είναι το **ftp, –s 195.130.67.5:** η διεύθυνση προέλευσης είναι η **195.130.67.5, –j drop:** το **-j** δηλώνει ότι ακολουθεί ο κανόνας **drop** δηλαδή τα πακέτα απορρίπτονται.

Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», το **-t** δηλώνει ότι ακολουθεί πίνακας, και συγκεκριμένα ο πίνακας **filter, -A OUTPUT:** Στην αλυσίδα **OUTPUT** του πίνακα θα γίνει επισύναψη ενός κανόνα όπως δηλώνει το **-A, –p ftp:** το πρωτόκολλο που εξετάζουμε είναι το **ftp, –d 195.130.67.5:** η διεύθυνση προορισμού είναι η **195.130.67.5, –j drop:** το **-j** δηλώνει ότι ακολουθεί ο κανόνας **drop** δηλαδή τα πακέτα απορρίπτονται.

20. *Αποδοχή icmp πακέτων*

Το iptables διαμορφώνεται έτσι ώστε να επιτρέψει στο firewall να στείλει ICMP echo-request (pings) και στη συνέχεια, να δεχτούν τις αναμενόμενες echo-replies ICMP.

Κώδικας:

1. **iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT**
2. **iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT**

Αναλυτική επεξήγηση του κώδικα.

1. Στην αρχή είναι απαραίτητη η χρήση της εντολής **«iptables»**, -A: επισύναψη κανόνα στην αλυσίδα **OUTPUT, OUTPUT:** είναι η αλυσίδα της εξερχόμενης κυκλοφορίας, **-p icmp:** το

πρωτόκολλο **icmp, --icmp-type echo-request:** αποστολή μηνύματος **echo-request, -j ACCEPT:** ο κανόνας που επισυνάπτουμε στην αλυσίδα **OUTPUT** είναι ο **ACCEPT** με τον οποίο αποδεχόμαστε αυτά τα πακέτα.

2. Στην αρχή είναι απαραίτητη η χρήση της εντολής **«iptables»**, -A: επισύναψη κανόνα στην αλυσίδα **INPUT, INPUT:** είναι η αλυσίδα της εισερχόμενης κυκλοφορίας, **-p icmp:** το πρωτόκολλο **icmp, --icmp-type echo- reply:** λήψη μηνύματος **echo- reply, -j ACCEPT:** ο κανόνας που επισυνάπτουμε στην αλυσίδα **INPUT** είναι ο **ACCEPT** με τον οποίο αποδεχόμαστε αυτά τα πακέτα.

21. *Αλλαγή της προεπιλεγμένης πολιτικής των αλυσίδων*

Εδώ αλλάζουμε την πολιτική των αλυσίδων INPUT, OUTPUT και FORWARD σε DROP. Καθορίζουμε δηλαδή το τι θα γίνει με τα πακέτα που δεν ταιριάζουν σε κανέναν κανόνα. Η προεπιλεγμένη πολιτική είναι ACCEPT.

Κώδικας:

1. **iptables -P INPUT DROP**
2. **iptables -P OUTPUT DROP**
3. **iptables -P FORWARD DROP**

Αναλυτική επεξήγηση του κώδικα.

1. Στην αρχή είναι απαραίτητη η χρήση της εντολής «**iptables**», –P : σημαίνει «Αλλαγή της πολιτικής μιας αλυσίδας», INPUT: Αλυσίδα της εισερχόμενης κυκλοφορίας την πολιτική της οποίας επιθυμούμε να αλλάξουμε, DROP: η προεπιλεγμένη πολιτική στο εξής θα είναι η DROP δηλ. απόρριψη των πακέτων.

2. Το ίδιο συμβαίνει και για την προεπιλεγμένη πολιτική της αλυσίδας **OUTPUT.**
3. Το ίδιο συμβαίνει και για την προεπιλεγμένη πολιτική της αλυσίδας **FORWARD.**

22. Το firewall απαγορεύει το rerouting (αλλαγή δρομολόγησης πακέτων)

Για να απαγορεύσουμε την αλλαγή της δρομολόγησης των πακέτων:

Κώδικας:

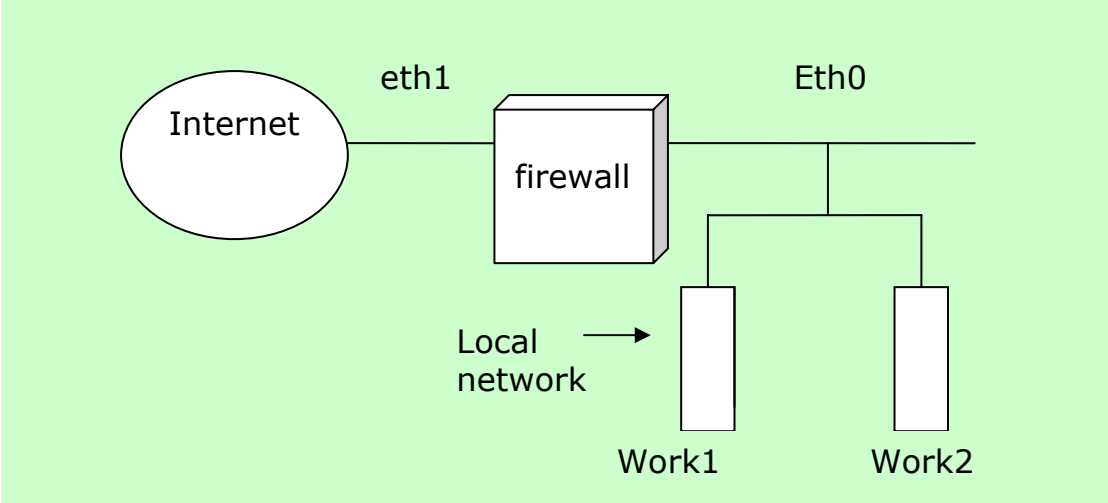
iptables –t filter –A forward –j Drop

Αναλυτική επεξήγηση του κώδικα.

Ο κανόνας ξεκινάει με την εντολή **iptables,** το **–t** δηλώνει ότι ακολουθεί πίνακας και συγκεκριμένα ο **filter (υπεύθυνος για την δρομολόγηση των πακέτων),** το **–A** δηλώνει ότι θα γίνει εισαγωγή ενός νέου κανόνα στην αλυσίδα **forward** και το **–j** δηλώνει ότι ακολουθεί η ενέργεια που θα εφαρμοστεί στα πακέτα, η ενέργεια **Drop(απόρριψη).**

23. ***Μετάφραση διεύθυνσης του δικτύου προέλευσης***

Χρησιμοποιείται όταν δεν θέλουμε να χρησιμοποιήσουμε μια διεύθυνση ip για κάθε υπολογιστή αλλά μία κοινή εξωτερική ip (όταν έχουμε static ip) για την επικοινωνία μας με το internet. Έστω ότι έχουμε το δίκτυο 192.168.1.0/24 που συνδέεται με το firewall στην διεπαφή eth0 που έχει την διεύθυνση 192.168.1.1. Στο Διαδίκτυο το firewall συνδέεται με την διεπαφή eth1 που έχει την διεύθυνση 195.251.239.197. Αν θέλουμε οι υπολογιστές του ιδιωτικού δικτύου 192.168.1.0/24 να συνδέονται με το internet πρέπει να ορίσουμε το εξής:



Εικόνα 15 - Παράδειγμα SNAT

Κώδικας:

iptables -t nat -A POSTROUTING -i eth0 -o eth1-j SNAT--to-source 195.251.239.197

Αναλυτική επεξήγηση του κώδικα.

Η εντολή **iptables** τοποθετείται στην αρχή του κώδικα υποχρεωτικά, το **-t** δηλώνει ότι ακολουθεί πίνακας και συγκεκριμένα ο πίνακας **nat, -A:** επισύναψη κανόνα στην αλυσίδα **POSTROUTING,** το **–ι** δηλώνει την διεπαφή εισόδου η οποία είναι η **eth0,** το **-o** δηλώνει την διεπαφή εξόδου η οποία είναι η **eth1, –j:** ακολουθεί ο κανόνας **SNAT--to-source 195.251.239.197.**

Όποιο πακέτο φτάνει στο firewall από την διεπαφή eth0 και αποφασιστεί να δρομολογηθεί από την eth1 πριν φύγει αλλάζει η διεύθυνση προέλευσης σε 195.251.239.197.

24. *Μετάφραση διεύθυνσης δικτύου προέλευσης δυναμικά.*

Σε περίπτωση που σε κάθε σύνδεσή μας στο internet η ip διεύθυνσή μας αλλάζει και θέλουμε να έχουμε SNAT έχουμε το πρόβλημα ότι κάθε φορά πρέπει να αλλάζουμε τον κανόνα και να

βάζουμε την διεύθυνση που μας έχει δοθεί. Για να λυθεί το πρόβλημα αυτό το iptables παρέχουν τον στόχο MASQUERADE επιτρέποντας έτσι να καθορίσουμε την διεπαφή της οποίας την διεύθυνση θα παίρνουν τα εξερχόμενα πακέτα. Έστω ότι συνδεόμαστε με modem στο internet και θέλουμε να μοιραστούμε την σύνδεση με τους υπολογιστές του δικτύου 192.168.1.0/24 που συνδέονται στο eth0. Η διεύθυνση που παίρνουμε από τον isp (internet service provider) κάθε φορά αλλάζει. Αρκεί να δώσουμε:

Κώδικας:

iptables -t nat -A POSTROUTING -i eth0 -o ppp0 -j MASQUERADE

και η διεύθυνση προέλευσης κάθε πακέτου που φεύγει από το firewall και ήρθε από το eth0 θα είναι η διεύθυνση της διεπαφής ppp0 (Η διεύθυνση που πήραμε από τον isp όταν συνδεθήκαμε με το modem). Η προώθηση πακέτων πρέπει να είναι ενεργοποιημένη.

Αναλυτική επεξήγηση του κώδικα.

Η εντολή **iptables** τοποθετείται στην αρχή του κώδικα υποχρεωτικά, το **-t** δηλώνει ότι ακολουθεί πίνακας και συγκεκριμένα ο πίνακας **nat, -A:** επισύναψη κανόνα στην αλυσίδα **POSTROUTING,** το **–ι** δηλώνει την διεπαφή εισόδου η οποία είναι η **eth0,** το **-o** δηλώνει την διεπαφή εξόδου η οποία είναι η **ppp0** και το **–j ότι** ακολουθεί ο κανόνας **MASQUERADE.**

25. Μετάφραση διεύθυνσης δικτύου προορισμού

Έστω ότι έχουμε έναν υπολογιστή με δύο διεπαφές eth0 και eth1. Η μια έχει ip 195.251.239.142/24 και η άλλη 192.168.0.1/24.Αν θέλουμε να υλοποιήσουμε κάποιες υπηρεσίες σε ξεχωριστούς υπολογιστές χρειάζεται η κατάλληλη μετάφραση των διευθύνσεων των πακέτων και η προώθησή τους. Έτσι αν θέλουμε

να έχουμε έναν ssh εξυπηρετητή στην 192.168.0.9 διεύθυνση και έναν web εξυπηρετητή στην 192.168.0.10 χρειαζόμαστε:

Κώδικας:

1. **iptables -t nat -A PREROUTING -i eth0 -d 195.251.239.142 -p tcp --dport 22 -j DNAT --to-destination 192.168.0.9**
2. **iptables -t nat -A PREROUTING -i eth0 -d 195.251.239.142 -p tcp --dport 80 -j DNAT --to-destination 192.168.0.10**
3. **iptables -t nat -A POSTROUTING -s 192.168.0.9 -p tcp --sport 22 -j SNAT --to-source 195.251.239.142**
4. **iptables -t nat -A POSTROUTING -s 192.168.0.10 -p tcp --sport 80 -j SNAT --to-source 195.251.239.142**

Αναλυτική επεξήγηση του κώδικα.

1. Το **iptables** τοποθετείται πάντα στην αρχή της εντολής, το **–t** δηλώνει ότι ακολουθεί πίνακας, ο πίνακας που μας αφορά είναι ο nat, το **–A** δηλώνει ότι θα γίνει εισαγωγή ενός κανόνα στο τέλος της αλυσίδας **PREROUTING** στην οποία εισέρχονται τα πακέτα πριν την δρομολόγηση για την αλλαγή της διεύθυνσης προορισμού**,** το **-i eth0** δηλώνει την διεπαφή εισόδου, **-d 195.251.239.142:** η διεύθυνση προορισμού είναι η 195.251.239.142, **p tcp:** το πρωτόκολλο tcp, **--dport 22:** θύρα προορισμού 22, **-j:** ακολουθεί ο κανόνας, **DNAT:** ο κανόνας που καθορίζει ποια είναι η διεύθυνση προορισμού, **--to-destination 192.168.0.9:** η διεύθυνση προορισμού είναι η **192.168.0.9.**
2. **Το iptables** τοποθετείται πάντα στην αρχή της εντολής, το **–t** δηλώνει ότι ακολουθεί πίνακας, ο πίνακας που μας αφορά είναι ο nat, το **–A** δηλώνει ότι θα γίνει εισαγωγή ενός κανόνα στο τέλος της αλυσίδας **PREROUTING** στην οποία εισέρχονται τα

πακέτα πριν την δρομολόγηση για την αλλαγή της διεύθυνσης προορισμού**,** το **-i eth0** δηλώνει την διεπαφή εισόδου, **-d 195.251.239.142:** η διεύθυνση προορισμού είναι η 195.251.239.142, **p tcp:** το πρωτόκολλο tcp, **--dport 80:** θύρα προορισμού 80, **-j:** ακολουθεί ο κανόνας, **DNAT:** ο κανόνας που καθορίζει ποια είναι η διεύθυνση προορισμού, **--to-destination 192.168.0.10:** η διεύθυνση προορισμού είναι η **192.168.0.10.**

3. Το **iptables** τοποθετείται στην αρχή, **-t:** ακολουθεί ο πίνακας **nat:** ο πίνακας μας είναι ο nat, **-A POSTROUTING:** εισαγωγή κανόνα στο τέλος της αλυσίδας POSTROUTING στην οποία εισέρχονται τα πακέτα μετά την δρομολόγηση για την μετάφραση της διεύθυνσης προέλευσης, **-s 192.168.0.9:** η διεύθυνση προέλευσης είναι η 192.168.0.9**, -p tcp:** το πρωτόκολλο tcp, **--sport 22:** η θύρα προέλευσης είναι η 22, **-j:** ακολουθεί ο κανόνας, **SNAT:** ο κανόνας που καθορίζει τη διεύθυνση προέλευσης, **--to-source 195.251.239.142:** η διεύθυνση προέλευσης είναι η **195.251.239.142.**
4. Το **iptables** τοποθετείται στην αρχή, **-t:** ακολουθεί ο πίνακας **nat:** ο πίνακας μας είναι ο nat, **-A POSTROUTING:** εισαγωγή κανόνα στο τέλος της αλυσίδας POSTROUTING στην οποία εισέρχονται τα πακέτα μετά την δρομολόγηση για την μετάφραση της διεύθυνσης προέλευσης, **-s 192.168.0.10:** η διεύθυνση προέλευσης είναι η 192.168.0.10**, -p tcp:** το πρωτόκολλο tcp, **--sport 80:** η θύρα προέλευσης είναι η 80, **-j:** ακολουθεί ο κανόνας, **SNAT:** ο κανόνας που καθορίζει τη διεύθυνση προέλευσης, **--to-source 195.251.239.142:** η διεύθυνση προέλευσης είναι η **195.251.239.142.**

26. *Τροποποίηση TOS*

Εδώ τροποποιούμε τον τύπο υπηρεσίας των ssh πακέτων έτσι ώστε να έχουμε την ελάχιστη καθυστέρηση.

Κώδικας:

iptables -t mangle -A PREROUTING -p tcp --dport 22 -j TOS --set-tos Minimize-Delay

Αναλυτική επεξήγηση του κώδικα.

Μετά το **iptables** που τοποθετείται στην αρχή της εντολής ακολουθεί το **–t:** δηλώνει ότι ακολουθεί πίνακας, **mangle:** ακολουθεί ο πίνακας mangle ο οποίος είναι υπεύθυνος για την τροποποίηση της ip επικεφαλίδας των πακέτων, το **-A** δηλώνει ότι ακολουθεί αλυσίδα, η **PREROUTING** είναι η αλυσίδα στην οποία εισέρχονται τα πακέτα μετά την δρομολόγηση για την μετάφραση της διεύθυνσης προέλευσης, **-p tcp --dport 22:** η tcp θύρα προορισμού είναι η 22, το **-j** δηλώνει ότι ακολουθεί κανόνας, **TOS:** κανόνας για την αλλαγή του πεδίου Type Of Service της επικεφαλίδας των πακέτων, **--set-tos Minimize-Delay:** δίνει στο πεδίου την τιμή Minimize-Delay έτσι ώστε το πακέτο να έχει την ελάχιστη καθυστέρηση.

27. Εισαγωγή κανόνων για κάθε interface σε ξεχωριστή αλυσίδα.

Κώδικας:

1. **iptables -N in_eth0**
2. **iptables -N in_eth1**
3. **iptables -A INPUT -i eth0 -j in_eth0**
4. **iptables -A INPUT -i eth1 -j in_eth1**

Αναλυτική επεξήγηση του κώδικα.

Η εντολή **iptables** τοποθετείται στην αρχή κάθε γραμμής.

1. Δημιουργία αλυσίδας με τη χρήση του: **-N**. Το όνομα της αλυσίδας είναι **in_eth0**.

2. Δημιουργία αλυσίδας με τη χρήση του: **-N**. Το όνομα της αλυσίδας είναι **in_eth1**.
3. **–A**: εισαγωγή κανόνα σε αλυσίδα, **INPUT**: η αλυσίδα στην οποία θα γίνει η εισαγωγή του κανόνα (**INPUT**: Αλυσίδα που φιλτράρει τα πακέτα που προορίζονται για το **firewall**), **-i eth0**: εισερχόμενη διεπαφή, **-j**: ακολουθεί ο κανόνας, **in_eth0**: τα πακέτα εισέρχονται στην αλυσίδα **in_eth0**.
4. **–A**: εισαγωγή κανόνα στο τέλος της αλυσίδας, **INPUT**: η αλυσίδα στην οποία θα γίνει η εισαγωγή του κανόνα (**INPUT**: Αλυσίδα που φιλτράρει τα πακέτα που προορίζονται για το firewall), **-i eth1**: εξερχόμενη διεπαφή, **-j**: ακολουθεί κανόνας, **in_eth1**: τα πακέτα εισέρχονται στην αλυσίδα **in_eth1**.

28. Matches

Σύμφωνα με αυτά που έχουμε δει μέχρι στιγμής, τα κριτήρια επιλογής πακέτων περιορίζονται κυρίως στις IP's, στις θύρες και στα πρωτόκολλα, πράγμα το οποίο δε δίνει και μεγάλη ευελιξία. Ευτυχώς το **netfilter** αλλά και τα **iptables** διαθέτουν **modules** (ή **matches** κατά την ορολογία της **iptables**), τα οποία προσθέτουν επιπλέον λειτουργικότητα. Τα modules αυτά φορτώνονται με την επιλογή **-m module_name**, στο κυρίως σώμα της εντολής. Από τα διάφορα modules που υπάρχουν, το πιο χρήσιμο είναι το **state match** (ταίριασμα κατάστασης), το οποίο επιτρέπει να ξεχωρίζουμε τις παλιές από τις νέες συνδέσεις.

Έλεγχος της κατάστασης των πακέτων

Μια καινοτομία των iptables είναι ο έλεγχος της κατάστασης πακέτων(stateful packet inspection). Με αυτόν τον τρόπο μας δίνεται η δυνατότητα να αναγνωρίσουμε αν ένα πακέτο αποτελεί μέρος των δεδομένων μιας νόμιμης σύνδεσης ή αν προέρχεται από έναν επίδοξο εισβολέα. Στο παράδειγμα που ακολουθεί επιτρέπουμε να περάσουν τα πακέτα που αποτελούν μέρος της σύνδεσης, στην

θύρα 80 (δηλαδή έχουν προορισμό το web) του εξυπηρετητή. Παρατηρούμε οι νέες εξωτερικές συνδέσεις δεν χρειάζονται καθώς η σύνδεση έχει ήδη ξεκινήσει από τον πελάτη.

Κώδικας:

iptables -A INPUT -m state -p tcp --dport 80 --state NEW, ESTABLISHED, RELATED -j ACCEPT

iptables -A OUTPUT -m state -p tcp --sport 80 --state ESTABLISHED, RELATED -j ACCEPT

Αναλυτική επεξήγηση του κώδικα.

Ο κώδικας ξεκινάει με την εντολή **iptables, το -A** δηλώνει ότι θα προστεθεί ένας κανόνας στην αλυσίδα **INPUT** (όπου δεν δηλώνεται ο πίνακας εννοείται ότι αναφερόμαστε στον **filter**), **-m state:** ακολουθεί η κατάσταση του πακέτου**, -p:** ακολουθεί το πρωτόκολλο **tcp** και η θύρα προορισμού η οποία είναι η **--dport 80,** η κατάσταση **–state** των πακέτων είναι η **NEW, ESTABLISHED, RELATED.** Τα πακέτα που ταιριάζουν με αυτά τα κριτήρια γίνονται δεκτά από την αλυσίδα **-j ACCEPT.**

Το ίδιο συμβαίνει και στο δεύτερο τμήμα του κώδικα, αυτή τη φορά όμως για την αλυσίδα **OUTPUT** (του **filter** πάλι).

Το module λοιπόν αυτό μας επιτρέπει να φτιάξουμε το εξής **firewall** για ένα workstation:

Παράδειγμα:

Με μόλις 3 εντολές έχουμε κλείσει τελείως το σύστημά μας προς τα έξω. Εδώ το πιο σημαντικό στοιχείο είναι ότι αφήνουμε επιλεκτικά να περάσουν οι συνδέσεις εκείνες που είναι ήδη **ESTABLISHED**, δηλαδή αυτές που έχουμε ξεκινήσει εμείς. Το **RELATED** μας γλιτώνει από διάφορα άλλα προβλήματα, κυρίως με το **FTP**, το οποίο ανοίγει μια δεύτερη, άσχετη σύνδεση για να φέρει

τα δεδομένα. Με το **state match**, το **netfilter** μπορεί να αναγνωρίσει ότι η σύνδεση αυτή είναι από το **FTP session** που έχουμε και να την αφήσει να περάσει. Θα θυμάστε ίσως ότι από τα τρία βασικά πρωτόκολλα (UDP, TCP, ICMP), μόνο το **TCP** είναι stateful, οπότε Θα περίμενε κανείς το state match να δουλεύει μόνο για **TCP**. Ωστόσο το netfilter είναι αρκετά «έξυπνο» ώστε να καταλαβαίνει ποια UDP πακέτα αποτελούν μια «λογική» σύνδεση και ποιο PONG είναι απάντηση σε ποιο PING, ώστε να δουλεύει και με UDP και ICMP.

Τέλος, αξίζει να δώσουμε προσοχή στη 2η γραμμή, η οποία αφήνει όλα τα πακέτα που έρχονται από το loopback interface. Πάντα είναι το πρώτο πράγμα που κάνουμε σε ένα firewall, να αφήνουμε τα πακέτα από το loopback interface. Αυτά είναι τα πακέτα που στέλνονται στο ίδιο το μηχάνημα από τον εαυτό του και αν τα κόψουμε δε θα δουλεύουν διάφορα πράγματα (π.χ.τα XP Windows).

Κώδικας:

1. **iptables -F**
2. **iptables -A INPUT -i lo -j ACCEPT**
3. **iptables -A INPUT -m state --state RELATED, ESTABLISHED -j ACCEPT**
4. **iptables -P INPUT DROP**

Αναλυτική επεξήγηση του κώδικα.

Η εντολή iptables τοποθετείται πάντα στην αρχή κάθε γραμμής.

1. Διαγραφή όλων των κανόνων
2. **–A**: εισαγωγή κανόνα στο τέλος της αλυσίδας που ακολουθεί, **INPUT**: η αλυσίδα που φιλτράρει την εισερχόμενη προς το firewall κυκλοφορία, **-i lo**: εισερχόμενη κυκλοφορία από το loopback interface, **-j**: ακολουθεί ο κανόνας, **ACCEPT**: ο

κανόνας που αποδέχεται τα πακέτα που πληρούν τις προϋποθέσεις.

3. **–A**: επισύναψη κανόνα στο τέλος της αλυσίδας, **INPUT**: η αλυσίδα που φιλτράρει την εισερχόμενη προς το firewall κυκλοφορία, **-m**: ακολουθεί το module κατάστασης, **state --state RELATED**,**ESTABLISHED**: τα πακέτα που μας ενδιαφέρουν είναι αυτά που η κατάστασή τους είναι **RELATED** ή **ESTABLISHED** δηλαδή τα πακέτα που έχουν ήδη μία σύνδεση ή σχετίζεται με μία ήδη υπάρχουσα, **-j:** ακολουθεί ο κανόνας, **ACCEPT**: ο κανόνας που αποδέχεται τα πακέτα που ταιριάζουν με τα κριτήρια.
4. **–P**: αλλαγή της προεπιλεγμένης πολιτικής της αλυσίδας

Συμπεράσματα

Από την μελέτη των δύο αυτών συστημάτων καταλαβαίνουμε πως το δεύτερο που μελετήσαμε είναι σαφώς αποτελεσματικότερο και προσφέρει μεγαλύτερη ασφάλεια και ευελιξία στο σύστημα είτε αφορά έναν χρήστη είτε ένα δίκτυο.

Το **netfilter** έχει τις δυνατότητες να ελέγχει την κίνηση που προορίζεται για το firewall εξέρχεται από αυτό είτε προωθείται μέσω αυτού. Και επιπλέον προσφέρει δυνατότητες που ξεπερνούν κατά πολύ το βασικό firewalling.

Το σύστημα **netfilter/ iptables** αποτελεί ένα πολύ σημαντικό εργαλείο για την προστασία μας. Δεν πρέπει όμως να ξεχνάμε πως ο κόσμος της τεχνολογίας συνεχώς αλλάζει και πως νέοι κίνδυνοι θα απειλήσουν το σύστημα μας. Για το λόγο αυτό είμαστε υποχρεωμένοι να ελέγχουμε συνεχώς το firewall που χρησιμοποιούμε.

Ευρετήριο

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Βιβλιογραφία

Βιβλία

Άρης Αλεξόπουλος και Παύλος Λαγογιάννης, "Τηλεπικοινωνίες και δίκτυα υπολογιστών", 5η έκδοση, Copyright 1999.

Gregor N. Purdy, "Linux iptables pocket reference", 1st edition, August 2004.

Michael Shinn and Scott Shinn, "Troubleshouting Linux Firewall", 1st printing, December 2004.

Ιστοσελίδες

Η επίσημη σελίδα του netfilter είναι διαθέσιμη στη διεύθυνση: http://www.netfilter.org.

Linux iptables HOWTO, By Rusty Russell, 1999. Διαθέσιμο στη διεύθυνση: http://www.linuxguruz.com/iptables/howto/

Introduction to Linux, Machtelt Carrels. Διαθέσιμο στη διεύθυνση: http://www.faqs.org/docs/linux_intro/index.html

Εισαγωγικός οδηγός iptables. Διαθέσιμο στην διεύθυνση: *http://insomnia.gr/vb3/showthread.php?t=170844*

Unix Introduction, Διαθέσιμο στην διεύθυνση: *http://www.ee.surrey.ac.uk/Teaching/Unix/unixintro.html*

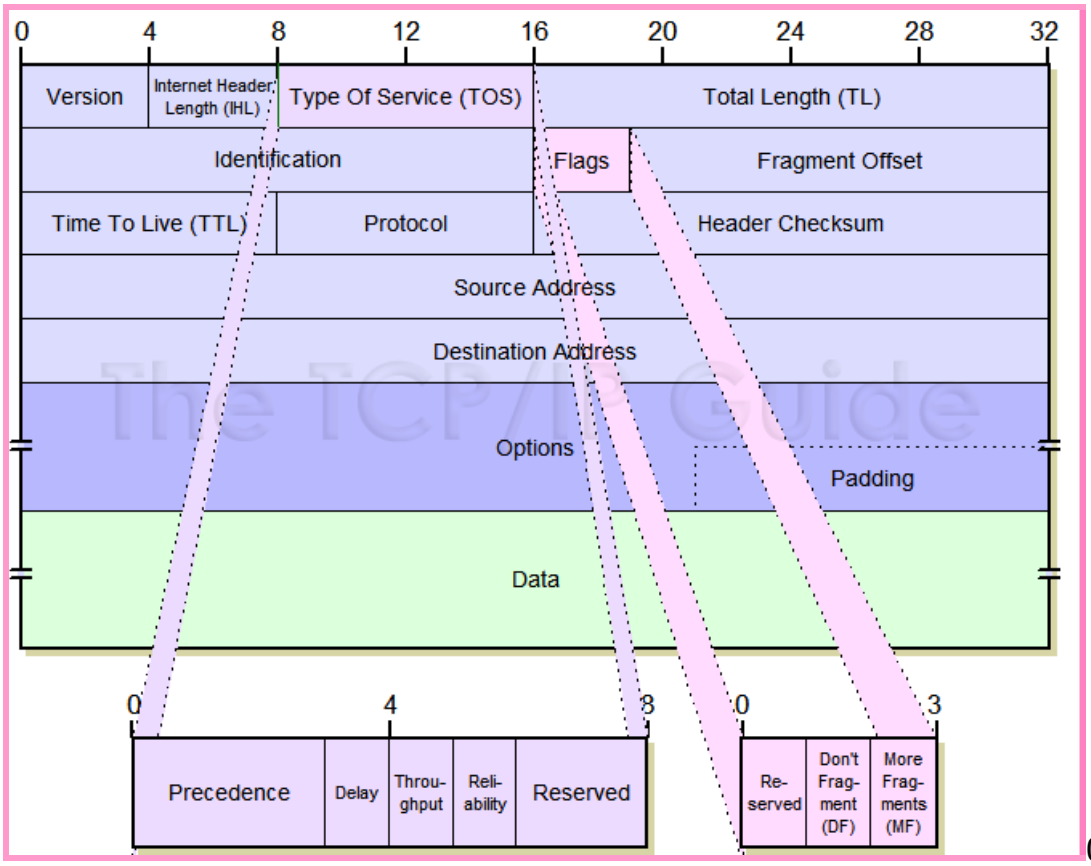
Η επίσημη διεύθυνση του Linux: *http://www.linux.org/*

Δοκιμαστικές εκδόσεις

Για download του συστήματος Otenet Security Kit επισκεφτείτε την ιστοσελίδα.

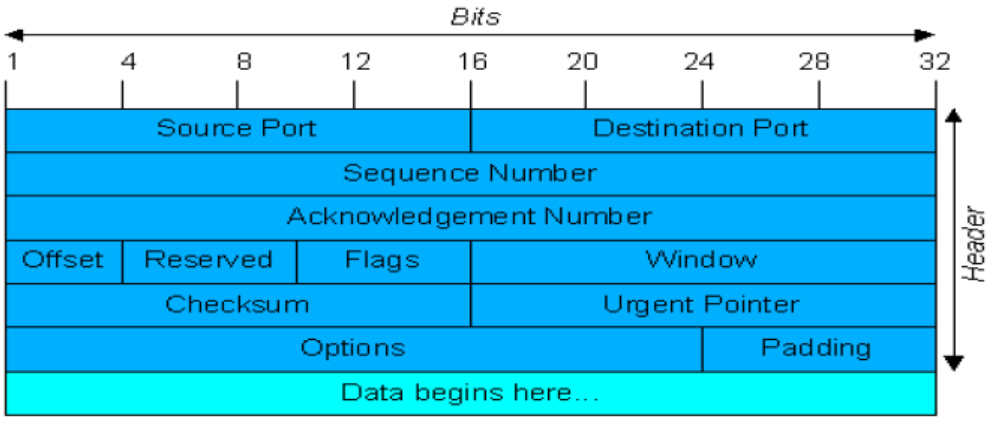
Παράρτημα

1. Δομή της **ip** επικεφαλίδας.



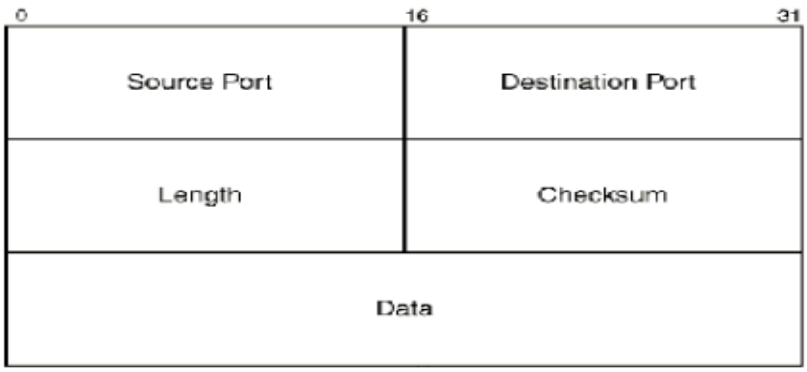
IP (Internet Protocol):Το IP πρωτόκολλο είναι το βασικό πρωτόκολλο (τρίτου επιπέδου) πάνω στο οποίο «κάθονται» όλα τα συνήθη πρωτόκολλα. Ορίζει μόνο διευθύνσεις παραλήπτη και αποστολέα και δεν έχει καμία άλλη πληροφορία. Το IP είναι stateless, δηλαδή δεν υπάρχει η έννοια της «σύνδεσης»· είναι απλά πακέτα που πάνε από έναν κόμβο του δικτύου προς έναν άλλον.

2. Δομή της **tcp** επικεφαλίδας.



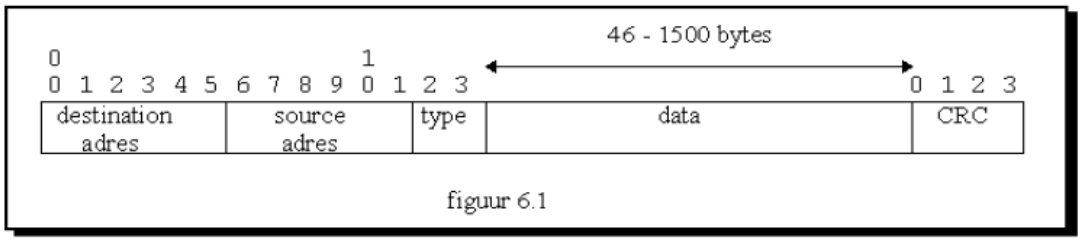
TCP (Transmission Control Protocol): Το TCP πάει ένα βήμα παραπέρα, εισάγοντας - εκτός από τις θύρες - και την έννοια της «σύνδεσης». Πρόκειται για ένα stateful πρωτόκολλο, το οποίο έχει έναν ολόκληρο μηχανισμό συνεννόησης προκειμένου να διατηρεί μια «σύνδεση» ανάμεσα στους δύο κόμβους, προσφέροντας αξιόπιστη επικοινωνία. Ενώ με το UDP δεν μπορούμε να ξέρουμε - σε επίπεδο πρωτοκόλλου - αν το πακέτο παρελήφθη από την άλλη πλευρά, ενώ με το TCP η γνώση αυτή είναι ενσωματωμένη στο πρωτόκολλο. Επιπλέον το TCP παρέχει μηχανισμούς κατακερματισμού μεγάλων ποσοτήτων δεδομένων (fragmentation), ανίχνευσης συμφόρησης (congestion), απόδοσης προτεραιότητας (QoS: Quality of Service) κλπ. Συνολικά είναι ένα πολύ πιο στιβαρό πρωτόκολλο, αλλά γι' αυτό και απαιτεί περισσότερους πόρους για την υλοποίησή του απ' ότι το UDP.

3. Δομή της **udp** επικεφαλίδας.



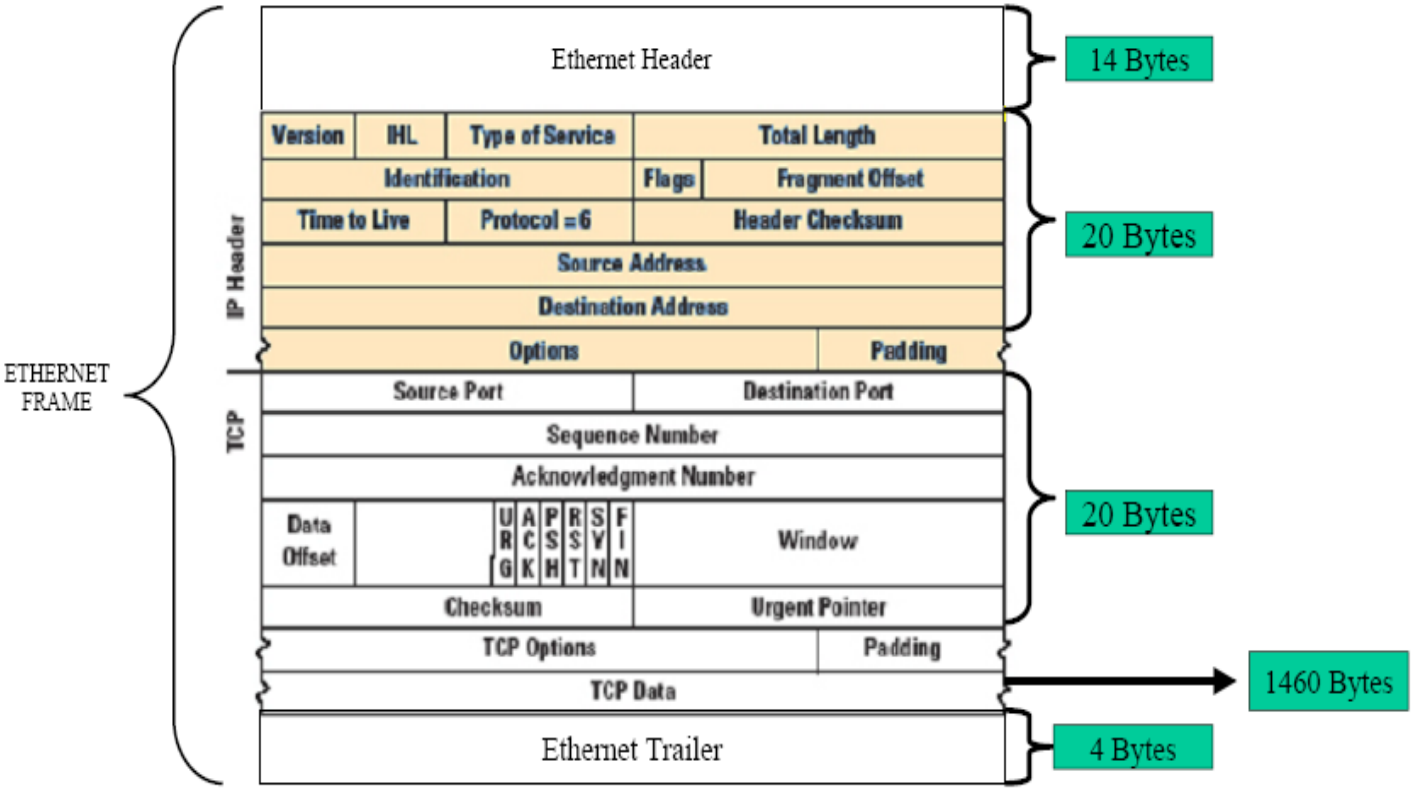
UDP (User Datagram Protocol): Το UDP προσφέρει επιπλέον από το IP την έννοια της «θύρας»: κάθε πακέτο, επιπλέον της IP διεύθυνσης, έχει και θύρα αποστολέα και παραλήπτη. Το UDP όπως και το IP είναι stateless, δεν έχει δηλαδή την έννοια της σύνδεσης και έχει πολύ μικρό overhead, αφού το header του κουβαλάει απλά την πληροφορία για τις θύρες. Για το λόγο αυτό χρησιμοποιείται κυρίως σε εφαρμογές low-latency, οι οποίες όμως δε μας ενδιαφέρει να είναι αξιόπιστες (π.χ. VoIP: δε χάθηκε ο κόσμος αν χαθεί ένα πακέτο, δε θα καταλάβεις τη διαφορά στη φωνή).

4. Δομή της **ethernet** επικεφαλίδας.

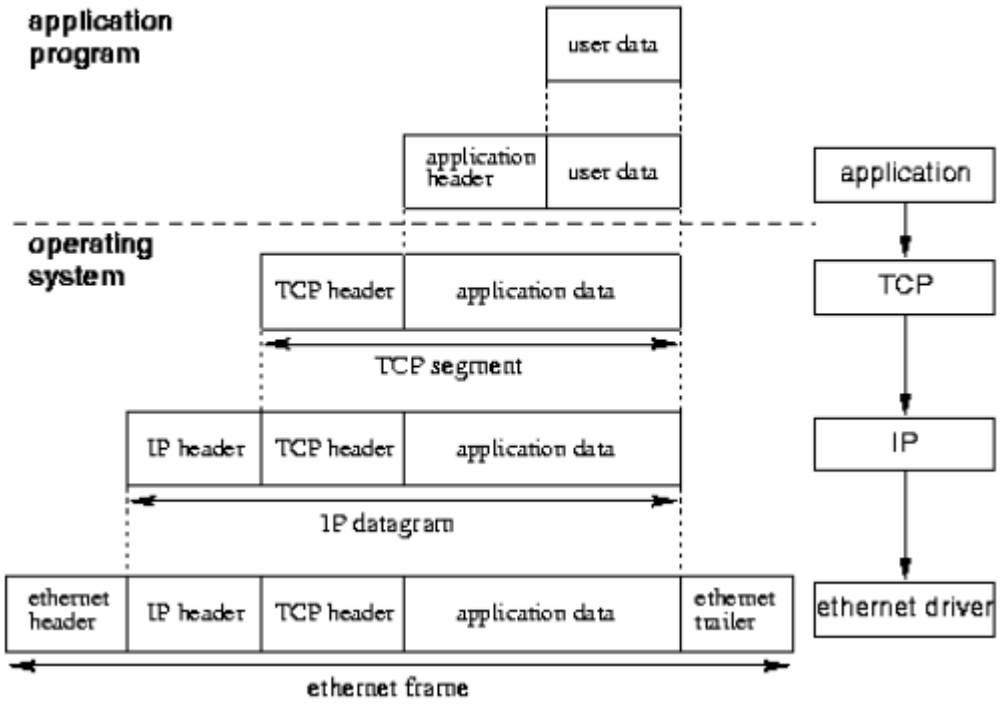


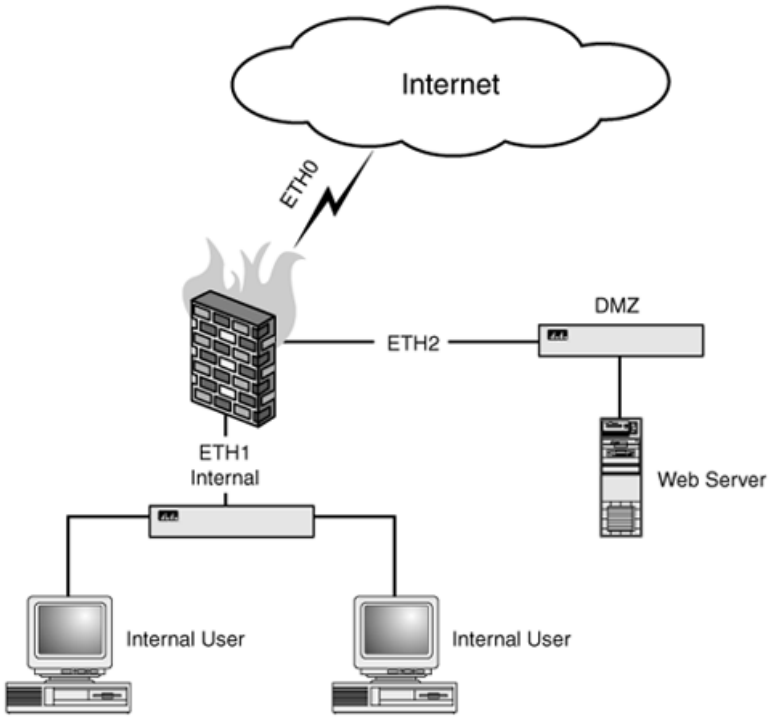
figuur 6.1

5. Δομή του **Ethernet** πλαισίου.



6. **IP** Ενθυλάκωση





Ιός είναι ένα πρόγραμμα το οποίο μπορεί να επισυναφθεί σε αρχεία, να εισχωρήσει στο σύστημά μας μέσω internet, ή μέσω μιας μολυσμένης δισκέτας και να προκαλέσει φθορές όπως καταστροφή αρχείων και φακέλων, κλήσεις internet κ.τ.λ.

Επιβλαβές λογισμικό είναι το λογισμικό το οποίο προορίζεται για να καταστρέψει ή να αποδιοργανώσει τον υπολογιστή. Τέτοιο λογισμικό είναι οι ιοί και προγράμματα που προσπαθούν να αναλάβουν τον έλεγχο του συστήματος, να ανακατευθύνουν τις αναζητήσεις, να εμφανίζουν διαφημίσεις, να ελέγχουν τις τοποθεσίες του internet που επισκεπτόμαστε και να κλέβει προσωπικές πληροφορίες όπως τραπεζικούς κωδικούς κ.τ.λ.

Κατασκοπευτικά προγράμματα είναι προγράμματα που εγκαθίστανται στον υπολογιστή μας και έχουν ως σκοπό να κλέψουν πληροφορίες όπως διευθύνσεις mail, κωδικούς πιστωτικών καρτών κ.τ.λ.