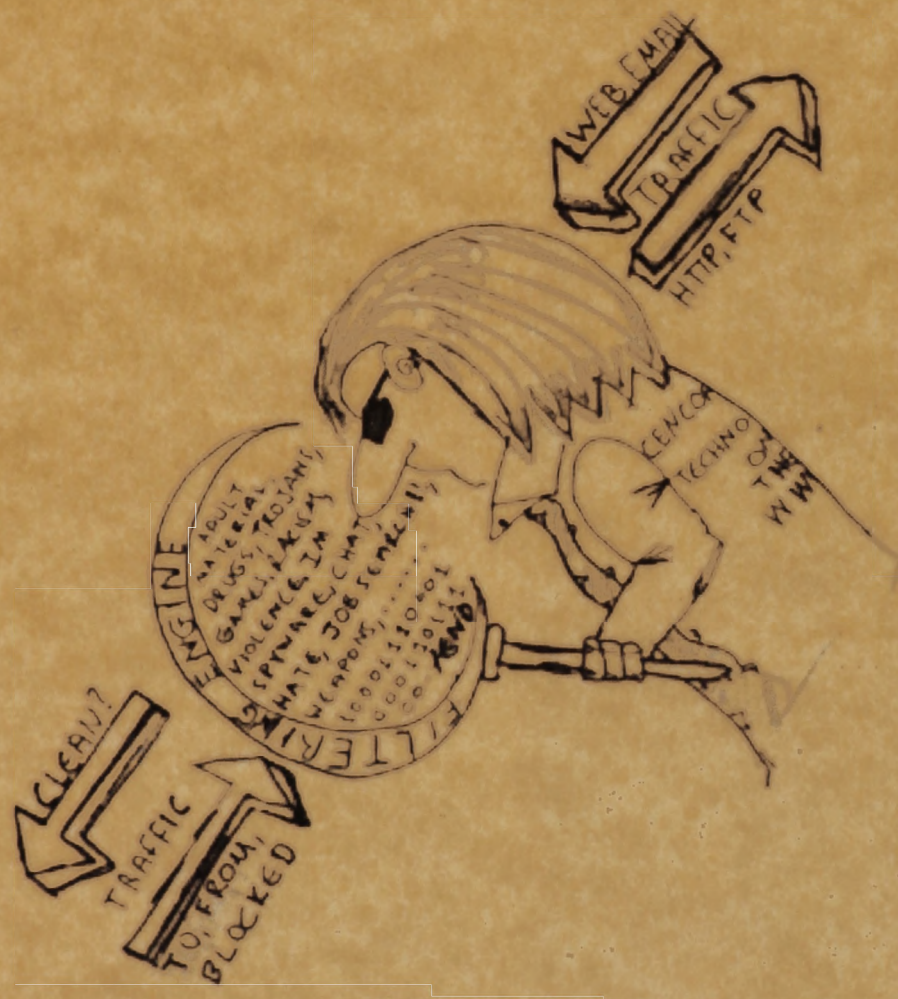
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ : ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ : ΕΦΑΡΜΟΓΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**

# ΛΟΓΟΚΡΙΣΙΑ ΚΑΙ ΕΛΕΓΧΟΣ ΤΟΥ INTERNET

## (Censorship and Inspection on the Internet)




ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ : ΓΕΩΡΓΙΟΣ ΑΛΕΞΑΝΔΡΗΣ

**ΟΜΑΔΑ:**

| | | | |
|---|---|---|---|
| ΛΟΥΛΑΤΗ ΕΒΙΣ | Α.Μ. : | 10897 | Email: evisdolphin@hotmail.com |
| ΚΩΝΣΤΑΝΤΙΝΟΥ ΑΝΝΑ-ΜΑΡΙΑ | Α.Μ. : | 10224 | Email: annamaria_con@yahoo.gr |

*ΜΕΣΟΛΟΓΓΙ ΣΕΠΤΕΜΒΡΙΟΣ 2007*

Τηλ. [illegible] - ΠΑΤΡΑ

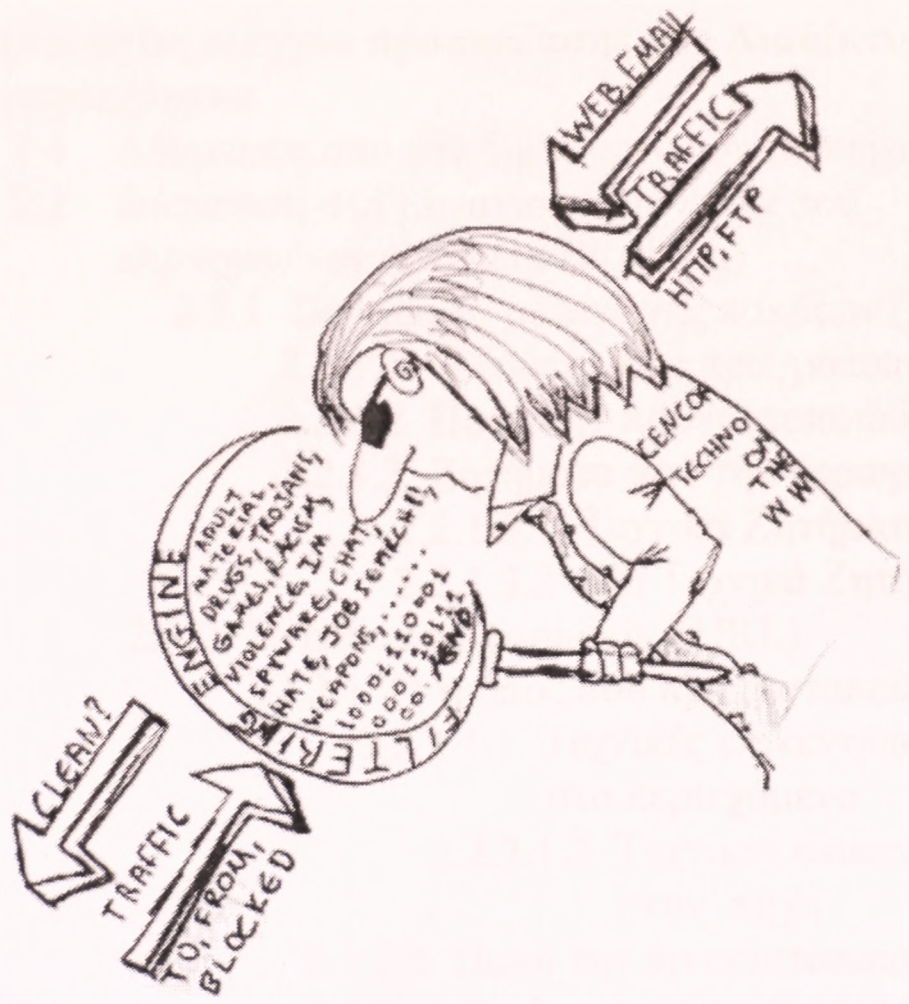
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ : ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ : ΕΦΑΡΜΟΓΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**

# ΛΟΓΟΚΡΙΣΙΑ ΚΑΙ ΕΛΕΓΧΟΣ ΤΟΥ INTERNET

## (Censorship and Inspection on the Internet)





**ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ : ΓΕΩΡΓΙΟΣ ΑΛΕΞΑΝΔΡΗΣ**

**ΟΜΑΔΑ:**

| | | | |
|---|---|---|---|
| **ΛΟΥΛΑΤΗ ΕΒΙΣ** | **Α.Μ. : 10897** | **Email: evisdolphin@hotmail.com** |
| **ΚΩΝΣΤΑΝΤΙΝΟΥ ΑΝΝΑ-ΜΑΡΙΑ** | **Α.Μ. : 10224** | **Email: annamaria_con@yahoo.gr** |


***ΜΕΣΟΛΟΓΓΙ ΣΕΠΤΕΜΒΡΙΟΣ 2007***

**ΠΕΡΙΕΧΟΜΕΝΑ**

# ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο (Internet) αποτελεί το μεγαλύτερο πληροφοριακό σύστημα στον κόσμο. Η δομή του είναι πλήρως ανοικτή σε κάθε χρήστη ηλεκτρονικού υπολογιστή (Η/Υ), είναι απόλυτα αποκεντρωμένο και αυτοδιαχειριζόμενο, καθώς δεν είναι ιδιοκτησία κανενός και δεν ελέγχεται από κανένα.

Οι υπηρεσίες του Διαδικτύου (Internet), όπως ο Παγκόσμιος Ιστός, το Ηλεκτρονικό Ταχυδρομείο, οι Τηλεδιασκέψεις, οι συνομιλίες σε ομάδες συζητήσεων κ.ά., παρέχουν στους χρήστες ηλεκτρονικών υπολογιστών μια πληθώρα ωφελειών, που αν τις αξιοποιήσουν θετικά θα γίνουν κοινωνοί πρωτόγνωρων δυνατοτήτων και εμπειριών σε ότι αφορά στην ανάπτυξη της ελευθερίας, της σκέψης, της έκφρασης, της μάθησης και της επικοινωνίας, στην ενίσχυση της ισοτιμίας τους έναντι των άλλων μελών της ψηφιακής κοινότητας (e-citizen), στην ενίσχυση της ιδιωτικότητας και στην ενίσχυση της ακεραιότητας της προσωπικότητάς τους.

Έτσι λοιπόν, το Διαδίκτυο (Internet), ως εικονικό αντίγραφο του κόσμου στον οποίο ζούμε, παρέχει στο χρήστη τα πάντα, όπως ακριβώς και η πραγματικότητα. Επιπρόσθετα, δημιουργεί υπερβάσεις, καταργώντας αποστάσεις και σύνορα σε έναν κόσμο που δέχεται έναν πρωτόγνωρο τύπο ελευθερίας κινήσεων, ανταλλαγής απόψεων και ιδεών.

Όπως όμως για κάθε τεχνολογικό επίτευγμα, έτσι και για το Διαδίκτυο (Internet) θα ήταν λάθος αν κανείς προσπαθούσε να του προσδώσει το χαρακτηρισμό του «ηθικού» ή του «ανήθικου».

Η δεοντολογική αξιοποίηση των υπηρεσιών του Διαδικτύου (Internet) και η αποφυγή αθέμιτης «e-χρήσης», είναι υπευθυνότητα, καταρχήν κάθε ενήλικου, ώριμου, συνειδητοποιημένου πολίτη και κατά δεύτερο λόγο της Πολιτείας, που πρέπει οπωσδήποτε να εφαρμόσει κατάλληλες πολιτικές εκπαίδευσης και αγωγής των ανηλίκων, των γονέων και των εκπαιδευτικών, όπως και να υλοποιήσει ολοκληρωμένα μέτρα ασφαλείας κατά του διαδικτυακού εγκλήματος.

# ΚΕΦΑΛΑΙΟ 1

# Η ΛΟΓΟΚΡΙΣΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (INTERNET)

## 1.1 Τι είναι λογοκρισία (censorship);

Ως λογοκρισία (censorship), χαρακτηρίζεται η καταστολή δημοσίευσης ιδεών, κειμένων, φωτογραφιών, ταινιών ή άλλου είδους πληροφοριών.

Η αντίστοιχη αγγλική λέξη *censorship* προέρχεται από τη λατινική λέξη *censor* «τιμητής». Ο τιμητής ήταν αξιωματούχος στην αρχαία Ρώμη επιφορτισμένος με την περιφρούρηση των ηθικών αξιών. Η ελληνική λέξη, παράγεται από τα λογο- + -κρισια<κρίνω.

## 1.2 Η ανάγκη της λογοκρισίας (censorship)

### 1.2.1 Ένα πρόβλημα με παγκόσμιες διαστάσεις

Το Διαδίκτυο (Internet), εκτός από τη «φωτεινή» πλευρά του, έχει και μια άλλη «σκοτεινή» πλευρά, η γνωριμία με την οποία εξαρτάται κατά κύριο λόγο από τη στάση ζωής του καθενός.

Το πρόβλημα έχει παγκόσμιες διαστάσεις.

Η «σκοτεινή» (και διόλου αθέατη) πλευρά του «πλανητικού χωριού», περιλαμβάνει κυρίως την ανεξέλεγκτη έκθεση άσεμνου, πορνογραφικού υλικού, πολλές φορές με διαστροφικό περιεχόμενο, σε ένα ανεξάντλητο πλήθος δικτυακών τόπων (web sites) και ιστοσελίδων (web pages).

Εξίσου επικίνδυνη είναι και η πλοήγηση σε sites βίαιης, ρατσιστικής και τρομοκρατικής θεματολογίας, η συμμετοχή σε παράνομο τζόγο, η πρόσβαση σε ιστοσελίδες σατανιστικών και παραθρησκευτικών οργανώσεων. Στο σκοτεινό τοπίο περιλαμβάνεται ακόμη, η λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου με ακατάλληλο περιεχόμενο (χωρίς να είναι τις περισσότερες φορές γνωστά τα στοιχεία του αποστολέα), η διακίνηση αρχείων με προσωπικά-ευαίσθητα δεδομένα, η παραβίαση του ιδιωτικού απορρήτου, το οικονομικό έγκλημα σε on-line συναλλαγές, η αποστολή ιών (computer viruses) και προγραμμάτων με σκοπό την πρόκληση καταστροφών στους ηλεκτρονικούς υπολογιστές των αποδεκτών, η προώθηση προπαγανδιστικού υλικού, η διάδοση μηνυμάτων με σκοπό τον προσηλυτισμό ή ακόμη και την παρότρυνση σε αυτοκαταστροφικές ενέργειες.

Το μακρύ κατάλογο συμπληρώνουν οι τηλε-συνομιλίες με άτομα αμφιβόλου ηθικής και προθέσεων, που εκμεταλλεύονται τις τεχνολογικές τους δεξιότητες για να αντλήσουν δεδομένα προσωπικού χαρακτήρα ή ακόμη να ασκήσουν δράσεις διακίνησης ναρκωτικών και προϊόντων εγκλήματος.

### 1.2.2 Οι «ευπαθείς ομάδες»

Από το σύνολο των κοινωνικών ομάδων, αυτή που πραγματικά χρήζει προστασίας από τις «κακοτοπιές» που αναφέρθηκαν στην προηγούμενη ενότητα (1.2.1), είναι εκείνη των παιδιών.

Σε πρόσφατη έρευνα της METRON ANALYSIS υπολογίστηκε, ότι π.χ. στην Ελλάδα το 35% των Ελλήνων είναι ενεργοί χρήστες ηλεκτρονικών υπολογιστών, 1,4 εκατομμύρια είναι χρήστες του Διαδικτύου (Internet), ενώ οι χρήστες μεταξύ 12-17 ετών είναι περίπου 700.000.

Σε έρευνα του Κέντρου Εκπαιδευτικής Έρευνας, σε 161 σχολεία και 4.317 μαθητές, υπολογίστηκε ότι περίπου το 78% των μαθητών, χρησιμοποιεί συστηματικά τον ηλεκτρονικό υπολογιστή, το 34.3% χρησιμοποιεί e-mail και το 51.2% περιηγείται στον Παγκόσμιο Ιστό.

Τα παραπάνω αποτελέσματα προβάλλουν την αναγκαιότητα και τη σημαντικότητα της ευθύνης των γονέων για τον έλεγχο των sites που επισκέπτονται τα παιδιά τους.

Σε έρευνα του περιοδικού CHIP, 7 στους 10 χρήστες ηλεκτρονικών υπολογιστών, στην Ελλάδα, ηλικίας 7-17 ετών, έχουν επισκεφτεί πορνογραφικά sites, ενώ τα παιδιά σε ποσοστό 98%, δεν έχουν πληροφορηθεί ποτέ σχετικά με τους πιθανούς κινδύνους του Internet. Ο γονιός είναι απαραίτητο, πρώτα απ' όλα, να συνειδητοποιήσει τα οφέλη που παρέχονται στο παιδί από τη χρήση κατάλληλων προγραμμάτων (π.χ. εκπαιδευτικό λογισμικό, ψυχαγωγικά παιχνίδια για κάθε ηλικία), να ενημερωθεί σχετικά με τις ωφέλειες που προκύπτουν από την ορθολογική και με μέτρο χρήση των ηλεκτρονικών υπολογιστών, όπως και για τον εθισμό που είναι δυνατόν να δημιουργηθεί στο παιδί από την αλόγιστη χρήση του ηλεκτρονικού υπολογιστή.

### 1.2.3 Μέτρα που υλοποιούν τη λογοκρισία

Μέτρα για τον περιορισμό ή τον έλεγχο της πρόσβασης στο Internet που μπορούν να χρησιμοποιηθούν είναι πολλά, όπως νόμοι χρήσης, φιλτράρισμα περιεχομένου, παρακολούθηση ή καταγραφή, τιμολογιακές και φορολογικές πολιτικές, χειρισμός αγορών των τηλεπικοινωνιών, χειραγώγηση του hardware και του software και αυτολογοκρισία.

Το πλέον αξιόπιστο όμως μέτρο προστασίας για ανήλικους και ενήλικους χρήστες, είναι η εγκατάσταση στον ηλεκτρονικό υπολογιστή ειδικών προγραμμάτων, που πραγματοποιούν την απαραίτητη «λογοκρισία» στο περιεχόμενο των ιστοσελίδων ή των ηλεκτρονικών μηνυμάτων. Με τα προγράμματα αυτά, μπορεί για παράδειγμα να απαγορευτεί εντελώς η πρόσβαση σε ιστοσελίδες του παγκόσμιου ιστού, ενώ ταυτόχρονα, να επιτραπεί η διακίνηση ηλεκτρονικής αλληλογραφίας. Μπορεί επίσης, να απαγορευτεί η πρόσβαση σε ιστοσελίδες που κάποιος κρίνει ως ακατάλληλες, να καθοριστούν μέτρα ελέγχου του περιεχομένου της ηλεκτρονικής αλληλογραφίας και των συνομιλιών σε ομάδες συζητήσεων (newsgroups) και γενικά να επιλεχτούν ένα σύνολο ρυθμίσεων απαραίτητων για την προστασία των χρηστών των ηλεκτρονικών υπολογιστών.

Είναι αναγκαίο να γίνει μια προσπάθεια από όλους, από τους επίσημους φορείς τους ειδικούς της Πληροφορικής, τους εκπαιδευτικούς, τους γονείς, μέχρι τους απλούς χρήστες του ηλεκτρονικού υπολογιστή, ώστε να διαμορφωθούν κανόνες δεοντολογίας που θα ενισχύσουν πραγματικά την ελεύθερη βούληση και την κριτική θεώρηση του καθενός απέναντι στην τεχνολογία. Αφού πρώτα συνειδητοποιηθεί ότι «κάθε τεχνολογική πρόοδος έχει τριών ειδών επιπτώσεις: τις επιθυμητές, αυτές που μπορούμε να προβλέψουμε και αυτές που δεν μπορούμε» (Jacques Ellul, "The technological Bluff", 1990), απαιτείται προσπάθεια ώστε να αξιοποιηθούν οι πρώτες, να αποκτηθούν περισσότερες γνώσεις για τις δεύτερες και να προφυλαχτούμε, χωρίς ίχνος «τεχνοφοβίας», από τις τρίτες.

## 1.3 Η διεθνής αναφορά στη λογοκρισία και στον έλεγχο του Διαδικτύου (Internet)

Ο «πατέρας του Διαδικτύου (Internet)», Vint Cerf, βάζει μια διαχωριστική γραμμή σε ότι αφορά τη λογοκρισία στο Δίκτυο.

Πιστεύει, ότι η κυβέρνηση δεν πρέπει να αναμιχθεί στα του οίκου των πολιτών, εκτός των περιπτώσεων που υπάρχει παράβαση άλλων νόμων, όπως π.χ. «παιδική πορνογραφία».

Σε ερώτηση δημοσιογράφου του ηλεκτρονικού περιοδικού apcmag.com «Πιστεύετε ότι μπορεί να υπάρξει αρκετή συναίνεση για να εφαρμοστεί μια παγκόσμια λογοκρισία», απαντά πως θα είναι πολύ δύσκολο να υπάρξει κοινή άποψη για λογοκρισία. Κάποιες πράξεις όμως είναι τόσο φρικτές, που θεωρούνται φρικτές σε κάθε κοινωνία.

Όμως, από την άλλη μεριά, κάποιες πρακτικές που είναι αποδεκτές π.χ. στην Ολλανδία, δεν είναι αποδεκτές στις Η.Π.Α.

Μετά από μελέτες έχει προκύψει, ότι η λογοκρισία του Διαδικτύου (Internet), είναι κοινός τόπος για τα περισσότερα μέρη του κόσμου. Είναι ξεκάθαρο, ότι στις περισσότερες χώρες, εδώ και δύο χρόνια, έχει γίνει μια ταχεία προσπάθεια να κλείσει εντελώς ή να αναχαιτισθεί το Διαδίκτυο (Internet).

### 1.3.1 Στην Αφρική

Πρόσφατα, δύο σημαντικές τάσεις έχουν εμφανιστεί στην εξέλιξη των Αφρικανικών επικοινωνιών και στη νομοθεσία που αφορά τα Μ.Μ.Ε.

Από τη μια μεριά, υπάρχει η τάση να απευθύνουν εκδόσεις που αναφέρονται στις καθολικές ψηφιακές γραμμές διαμοιρασμού, οι οποίες έχουν οδηγήσει στην ανάπτυξη της ICT πολιτικής, πολιτική η οποία συχνά αναγνωρίζει τη σπουδαιότητα της ελευθερίας της έκφρασης για την ανάπτυξη της αφρικανικής οικονομίας στα νέα Μ.Μ.Ε.

Αντιθέτως, ένας αριθμός αφρικανικών χωρών, έχει εισάγει ειδική νομοθεσία, που αφορά άμεσα την τρομοκρατία, η οποία χαλιναγωγεί ελευθερίες και εφοδιάζει εξουσίες με αυξανόμενη δύναμη για να παρακολουθεί και να κρίνει επικοινωνίες μεταξύ ατόμων και ομάδων.

### 1.3.2 Στην Ασία

Η Ασία χαρακτηρίζεται από μια πολιτιστική ανομοιομορφία, η οποία επιτρέπει στις κοινωνίες να εφαρμόζουν μοναδικές πρακτικές στα συστήματα αξιών τους.

Το δικαίωμα της ιδιωτικότητας μπορεί επιμελώς να προστατεύεται στη Δύση, αλλά δεν παύει να είναι μια αφηρημένη έννοια σε μέρη της Ασίας, όπου οι παραδοσιακοί συγγενικοί δεσμοί παραμένουν δυνατοί.

Κατά συνέπεια, οι κυβερνήσεις δικαιολογούν κινήσεις που περιορίζουν το περιεχόμενο του Διαδικτύου (Internet), ισχυριζόμενες ότι είναι βλαβερό ή επικίνδυνο για την κοινωνία.

Μια άλλη έκδοση που υπολογίζουν να επεκτείνουν είναι οι πολιτείες να μπορούν να κανονίζουν να οριοθετούν την πρόσβαση στο Διαδίκτυο (Internet) ή στο περιεχόμενο, χωρίς να παραβιάζουν τις στοιχειώδεις ελευθερίες και τα βασικά δικαιώματα που εγγυάται η Παγκόσμια Διακήρυξη των Ανθρωπίνων Δικαιωμάτων.

Η Κίνα π.χ. επιμένει, ότι έχει το δικαίωμα στην απαγόρευση ιστοσελίδων που είναι καθαρά αντικυβερνητικές. Άλλες χώρες στην περιοχή, όλο και περισσότερο επιβάλλουν περιορισμούς στο Διαδίκτυο (Internet) ή στο περιεχόμενο, λέγοντας ότι απλώς προστατεύουν τον «ευπαθή» πληθυσμό, όπως είναι οι γυναίκες και τα παιδιά. Αλλά ο κίνδυνος που υπάρχει είναι ότι όταν οι πολιτείες αρχίσουν να λογοκρίνουν το περιεχόμενο θεωρώντας ότι είναι μη αποδεκτό και επιβλαβές, τότε φροντίζουν να αυξομειώνουν το περιεχόμενο του Διαδικτύου (Internet).

Αυτό που πρακτικά ενοχλεί στον πόλεμο κατά της τρομοκρατίας είναι ότι οι αρχές στην Ασία περιορίζουν τους χρήστες του Διαδικτύου (Internet) στο να δημοσιοποιούν νόμιμα παράπονα ή να ασκούν στοιχειώδεις ελευθερίες έκφρασης.

### 1.3.3 Στην Αυστραλία

Οι νόμοι για τη λογοκρισία στο Διαδίκτυο (Internet) ψηφίστηκαν από το Κοινοβούλιο της Ομοσπονδιακής Αυστραλιανής Κοινοπολιτείας το 1999 και άρχισαν να ισχύουν από την 1η Ιανουαρίου του 2000.

Η Broadcasting Services Act, τροποποιήθηκε έτσι ώστε να δώσει στο ρυθμιστή της τηλεόρασης, δηλαδή στο "ABA", τη δύναμη να διατάξει τους αυστραλιανούς ISP's, να σβήσουν φιλοξενούμενα περιεχόμενα στα δίκτυά τους, συμπεριλαμβανομένων μηνυμάτων χρηστών δικτύου.

Επίσης οι ISP's μπορούν να κατεβάζουν εικόνες και κείμενο από τις ιστοσελίδες και τους newsgroup servers, απειλώντας τους με πρόστιμα.

Το σχήμα κατηγορείται ότι επαληθεύεται από χρήστες που είναι αποδεδειγμένα ενήλικες.

Η πρόσβαση περιορίζεται σε ιστοσελίδες με υλικό σαφώς μη βίαιου σεξουαλικού περιεχομένου, χρήσης ή εθισμού στα ναρκωτικά, στο έγκλημα, στη σκληρότητα, στη βία ή σε απεχθή ή αποτροπιαστικά φαινόμενα, τα οποία προκαλούν τα κατεστημένα της ανθρωπιάς, της καλοσύνης, της ευπρέπειας, που είναι γενικώς αποδεκτά από έλλογους ενήλικες.

Το Νοέμβριο του 2002, το Electronic Frontiers Australia, εξέδωσε μια αναφορά, βρίσκοντας ότι το σχήμα είχε γίνει ευρέως αποτελεσματικό. Η ABA είχε σπαταλήσει πολλές προσπάθειες λογοκρισίας, ερευνώντας παράπονα για περιεχόμενα σε ιστοσελίδες φιλοξενούμενες εκτός χώρας, πάνω στις οποίες δεν είχε κανέναν έλεγχο. Κάποια αυστραλιανά web sites είχαν μετακινηθεί εκτός χώρας προκειμένου να δραπετεύσουν από τον εθνικό έλεγχο.

### 1.3.4 Στην Ευρώπη

Πρόσφατα, κάθε έθνος στην Ευρώπη έχει υπογράψει και θέσει σε ισχύ τη Συνθήκη Προστασίας Δεδομένων. Οι περισσότερες χώρες έχουν υπογράψει τη Συνθήκη του Κυβερνοεγκλήματος με μόνη εξαίρεση την Τουρκία. Εντούτοις καμία ευρωπαϊκή χώρα δεν την έχει καθιερώσει. Πολλές χώρες, συμπεριλαμβανομένων της Ισπανίας και Ρωσίας, έχουν δομές που επιτρέπουν τη λογοκρισία στο Διαδίκτυο (Internet), μόνο αν αυτή καταπολεμά την παιδική πορνογραφία.

Σιγά-σιγά, οι ευρωπαϊκές χώρες φαίνεται να συγκλίνουν σε μια τυποποίηση, κατά την οποία οι ISP's δεν είναι υπεύθυνοι για το περιεχόμενο που φιλοξενούν, εκτός αν αποτύχουν να το ρίξουν, όταν εξακριβωθεί ότι αυτό είναι παράνομο.

Επίσης, δημοφιλείς είναι οι νόμοι που αξιώνουν από τους ISP's, να εγκαταστήσουν (συνήθως με δικά τους έξοδα) εξοπλισμό που να κάνει εφικτή την πολιτική επιτήρησης στους χρήστες τους. Η συγκράτηση των δεδομένων έχει συζητηθεί στην Αγγλία, όπου οι ISP's έχουν διαμαρτυρηθεί για τους κυβερνητικούς κανόνες που αφορούν την αντιτρομοκρατία, το έγκλημα και την ασφάλεια, τόσο για το κόστος, όσο και για την ιδιωτικότητα.

### 1.3.5 Στην Αμερική

#### 1.3.5.1 Στη Λατινική Αμερική

Μια ματιά στη διαφορετική δομή των χωρών της Λατινικής Αμερικής, δείχνει ότι υπάρχουν συνταγματικές προστασίες σε θέματα όπως: ελευθερία λόγου, πρόσβαση στην πληροφόρηση και ιδιωτικότητα των δεδομένων και των επικοινωνιών.

Νόμοι και ρυθμίσεις στη Λατινική Αμερική έχουν ευρέως σχεδιαστεί και ως εκ τούτου εύκολα εφαρμοστεί και ερμηνευτεί, να συμπεριλάβουν νέες τεχνολογίες. Βασικά δεν υπάρχουν συγκεκριμένοι περιορισμοί για τη χρήση του Internet στις χώρες που έχουν ερευνηθεί, εκτός από το Μεξικό που υπάρχει ειδική ανάγκη για συσκευές φιλτραρίσματος πορνογραφικού υλικού.

Στη Βραζιλία, δεν υπάρχει συγκεκριμένη ανάγκη για συσκευές φιλτραρίσματος, αλλά μάλλον είναι απαραίτητο να εγκατασταθούν σημειώσεις στα web sites, τα οποία περιλαμβάνουν πορνογραφικό υλικό.

Και στη Χιλή, το Κογκρέσο έχει ήδη εκφράσει ενδιαφέρον να οριοθετήσει ανήθικο περιεχόμενο και πληροφορίες πορνογραφικού περιεχομένου που μεταφέρονται μέσω του Internet, αλλά το νομοσχέδιο ποτέ δεν έχει δοκιμαστεί.

Τα τελευταία χρόνια, εντούτοις, υπάρχουν ορισμένοι περιορισμοί περιεχομένου για το Internet σε πολλές από τις χώρες που έχουν ερευνηθεί, όπως Αργεντινή, Κολομβία, Περού, που έχουν ψηφίσει συγκεκριμένες νομοθετικές πράξεις που βοηθούν στον περιορισμό πορνογραφικού υλικού με λογισμικό φιλτραρίσματος ή με συσκευές σε περιοχές δημόσιας πρόσβασης ή σε προσωπικούς ηλεκτρονικούς υπολογιστές.

#### 1.3.5.2 Στον Καναδά

Το Σύνταγμα στον Καναδά εγγυάται στον καθένα τη στοιχειώδη ελευθερία «της σκέψης, της πίστης, της γνώμης και έκφρασης, συμπεριλαμβανομένου και της ελευθερίας του τύπου και των άλλων μέσων επικοινωνιών».
Στην πράξη, το Ανώτατο Δικαστήριο έχει επιδείξει σημαντική ανοχή για νόμους που οριοθετούν την ελευθερία της έκφρασης, στο όνομα της προστασίας μεμονωμένων περιπτώσεων, όπως την απαγόρευση εκδικητικών λόγων και της πορνογραφίας.

Δεν είναι γνωστές περιπτώσεις κυβερνητικών προσπαθειών να μπλοκάρουν ή να φιλτράρουν κύριες ιστοσελίδες. Ούτε υπάρχουν δημόσιες πρωτοβουλίες, είτε σε ομοσπονδιακό ή επαρχιακό επίπεδο, να πιέσουν τις δημόσιες βιβλιοθήκες με λογισμικό φιλτραρίσματος. Ο Σύνδεσμος των Καναδικών Βιβλιοθηκών έχει περιγράψει το φιλτράρισμα σαν μια «γλιστερή επιφάνεια» που πρέπει να αντισταθείς δυνατά.

Το 2002, η Ένωση των δημοσίων Καναδών υπαλλήλων, κατάφερε να ακουστούν έξι παράπονα, σε μια δυνατή προσπάθεια ενάντια στη δημόσια βιβλιοθήκη της Οττάβα, να αποτρέψει τους πελάτες της να χρησιμοποιούν τους υπολογιστές για πρόσβαση στο Διαδίκτυο (Internet) σε υλικό σεξουαλικού περιεχομένου, πιθανώς εγκαθιστώντας λογισμικό φιλτραρίσματος.

#### 1.3.5.3 Στις Η.Π.Α

Οι Η.Π.Α έχουν κάποιες από τις σκληρότερες προστασίες για τα δικαιώματα των πολιτών. Έχουν προοδευτικές συνταγματικές προστασίες και νόμους που προάγουν την ελευθερία του λόγου, των πληροφοριών και την ιδιωτικότητα.

Ήταν η περιοχή που γεννήθηκε και πρωτοστατούσε στο Διαδίκτυο (Internet), για πολλά χρόνια. Ως εκ τούτου, πρωτοστατούσε και στο να βάλει ελέγχους στο Διαδίκτυο (Internet), εξ ονόματος της προστασίας των παιδιών και των εταιρειών.

Η επίθεση της 11ης Σεπτεμβρίου, έδωσε στην Κυβέρνηση των Η.Π.Α την ευκαιρία να υιοθετήσει νόμους, που ενδυναμώνουν τις πολιτικές που είχαν αποτύχει, να κερδίσουν δημόσια υποστήριξη στη δεκαετία του '90, όπως επίσης να ενεργοποιήσει νόμο που να μπορεί να παρακολουθεί την κίνηση του Διαδικτύου (Internet) λεπτομερώς και να περιορίζει την πρόσβαση σε συγκεκριμένους τύπους δημοσίων πληροφοριών.

Τον Ιούνιο του 2003, η CIPA (Children's Internet Protection Act)- που είχε ιδρυθεί τον Απρίλιο του 2001- απαίτησε από τα δημόσια σχολεία και βιβλιοθήκες να χρησιμοποιήσουν λογισμικό φιλτραρίσματος σε όλους τους υπολογιστές που έχουν πρόσβαση στο Internet. Η CIPA έχει την πρόθεση να προστατέψει τα παιδιά από την πρόσβαση σε υλικό, όπως πορνογραφικό, συνταγών κατασκευής βομβών, σε on-line λόγους εκδίκησης και μίσους.

Η απαίτηση χρήσης λογισμικού φιλτραρίσματος σε τέτοιες τοποθεσίες σαν βασικό όρο είναι ένα ιδιαίτερο θέμα στις Η.Π.Α. Η λογοκρισία που επιβάλλεται από ένα τέτοιο λογισμικό προκαλεί δυσανάλογα μειονεκτήματα σε άλλους τομείς της κοινωνίας.

# ΚΕΦΑΛΑΙΟ 2

# ΤΕΧΝΟΛΟΓΙΕΣ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (INTERNET) ΜΕ ΒΑΣΗ ΤΟ ΠΕΡΙΕΧΟΜΕΝΟ

Οι τεχνικές λύσεις που έχουν μέχρι σήμερα προταθεί για την υλοποίηση της λογοκρισίας – έλεγχο με βάση το περιεχόμενο – μπορούν να ταξινομηθούν σε τρεις (3) κατηγορίες. Η ταξινόμηση προκύπτει αν λάβουμε υπόψη μας τα στάδια δημιουργίας, διακίνησης και ανάγνωσης του περιεχομένου.
Έτσι έχουμε:

- Δέσμευση από το δημιουργό του περιεχομένου
- Δέσμευση στο μηχανισμό διανομής του περιεχομένου (Content Blocking)
- που πραγματοποιείται σε επίπεδο μεταγωγής πακέτου (IP) και σε επίπεδο εφαρμογής (URL )
- Δέσμευση από τον συνδρομητή που πραγματοποιείται με τη βαθμονόμηση περιεχομένου (Content Rating) και την αυτο-οριοθέτηση (Self Determination)

## 2.1 Δέσμευση από το Δημιουργό του περιεχομένου

Δεδομένου ότι κάθε χρήστης του Διαδικτύου (Internet) έχει τη δυνατότητα να είναι και δημιουργός περιεχομένου, η δέσμευση από τον ίδιο το δημιουργό δεν είναι εφικτή για τους παρακάτω λόγους:

1. Η επόπτευση των δημιουργών περιεχομένου δεν είναι εύκολη υπόθεση λόγω του μεγάλου πλήθους τους.
2. Οι δημιουργοί περιεχομένου δε μπορούν εύκολα να ομαδοποιηθούν σε κατηγορίες, στις οποίες να εφαρμοστεί μια συγκεκριμένη πολιτική.
3. Υπάρχει η ανάγκη ύπαρξης κατάλληλου φορέα για τον έλεγχο του περιεχομένου που δημοσιεύεται στο Διαδίκτυο (Internet). Ακόμη και αν υπάρξει τέτοιος φορέας, θα υπήρχαν πολλά νομικά ζητήματα που θα είχαν να κάνουν κυρίως με την παγκόσμια εξάπλωση του Διαδικτύου (Internet).

## 2.2 Δέσμευση στο μηχανισμό διανομής του περιεχομένου (Content Blocking)

Αρκετές λύσεις έχουν προταθεί για τη δέσμευση περιεχομένου (Content Blocking), που θεωρούνται από κάποιους παράνομες ή προσβλητικές. Σύμφωνα με έκθεση που υποβλήθηκε προς την Κυβέρνηση της Αυστραλίας, το περιεχόμενο μιας ιστοσελίδας, μπορεί να δεσμευτεί είτε σε επίπεδο μεταγωγής πακέτου (packet level), είτε σε επίπεδο εφαρμογής (application level).

### 2.2.1 Σε επίπεδο μεταγωγής πακέτου (IP)

#### 2.2.1.1 Ο τρόπος που πραγματοποιείται

Η δέσμευση περιεχομένου στο επίπεδο μεταγωγής πακέτου, απαιτεί δρομολογητές φιλτραρίσματος (screening routers), οι οποίοι εξετάζουν την IP διεύθυνση της προέλευσης

του εισερχόμενου πακέτου, τη συγκρίνουν με μια *μαύρη λίστα* (black list) και είτε προωθούν το πακέτο αν η IP διεύθυνση δεν ανήκει στη μαύρη λίστα, είτε το απορρίπτουν αν ανήκει.

Πιο συγκεκριμένα, η δέσμευση πραγματοποιείται με χρήση της **Λίστας Ελέγχου Πρόσβασης (ACL, Access Control List)** και με κριτήρια που καθορίζονται από την πληροφορία τρίτου επιπέδου (επίπεδο network του μοντέλου OSI) που υπάρχει στο πακέτο, όπως είναι οι διευθύνσεις προέλευσης και προορισμού ή ακόμα και θύρες που προσδιορίζουν εφαρμογές και υπηρεσίες. Για να γίνει αυτό, απαιτείται η δημιουργία μιας λίστας με IP διευθύνσεις. Στη συνέχεια, κάθε πακέτο που φτάνει στο δρομολογητή του δικτύου, συγκρίνεται με τα περιεχόμενα της λίστας γραμμή προς γραμμή και ανάλογα με το αποτέλεσμα της σύγκρισης, ο δρομολογητής μπορεί να απαγορεύσει την πρόσβαση με βάση την IP διεύθυνση του αποστολέα ή του παραλήπτη, το πρωτόκολλο επικοινωνίας (TCP, UDP), το δίκτυο αποστολής ή λήψης και τέλος την πόρτα εφαρμογής.

Η λογική μιας **ACL** μπορεί να είναι:

- Επιτρέπονται όλες οι IP διευθύνσεις, εκτός από αυτές που αναφέρονται στη λίστα (default permit, black list)
- Επιτρέπονται μόνο οι διευθύνσεις, που αναφέρονται στη λίστα και όλες οι άλλες απορρίπτονται (default deny, white list)

Στο παράδειγμα που ακολουθεί φαίνεται η μορφή μιας **Λίστας Ελέγχου Πρόσβασης (ACL, Access Control List):**

```
access-list 101 permit ip 10.1.2.0.0.0.0.255 172.16.2.0.0.0.0.255
access-list 102 deny ip any any
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 ep telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 ep ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 ep syslog
```

#### 2.2.1.2 Ποιοι την πραγματοποιούν

Οι Λίστες Ελέγχου Πρόσβασης (ACL, Access Control List), εφαρμόζονται στους δρομολογητές που ελέγχουν την εισερχόμενη και εξερχόμενη κίνηση του δικτύου. Επομένως, η δέσμευση των IP διευθύνσεων μπορεί να πραγματοποιηθεί:

- Από οποιονδήποτε Πάροχο Υπηρεσιών Διαδικτύου (ISP, Internet Service Provider)
- Από τους Παρόχους Υπηρεσιών Κορμού (BSP, Backbone Service Providers). Λαμβάνοντας υπόψη, ότι οι BSP είναι πιο ψηλά στην ιεραρχία της αρχιτεκτονικής του Διαδικτύου (Internet) η εφαρμογή των ACL στους BSP είναι πιο αποδοτική. Επίσης, για τη βελτίωση των προβλημάτων απόδοσης, μπορούν να χρησιμοποιηθούν και οι συναρτήσεις σύνοψης (hash functions).
- Από το δρομολογητή μιας επιχείρησης ή οργανισμού, που διαθέτει μόνιμη σύνδεση με το Διαδίκτυο (Internet). Αν η επιχείρηση ή ο οργανισμός διαθέτει συσκευή Firewall (Αναχώματα ασφαλείας), οι λίστες θα μπορούσαν να εφαρμοστούν σε αυτή.

#### 2.2.1.3 Ζητήματα που την περιορίζουν

Σε κάθε περίπτωση, η αποτελεσματικότητα της δέσμευσης IP διευθύνσεων είναι ζήτημα αμφιλεγόμενο. Οι υποστηρικτές της τεχνολογίας αυτής ισχυρίζονται ότι πράγματι είναι ένας εφικτός τρόπος για αποτελεσματική δέσμευση παράνομου ή προσβλητικού περιεχομένου στο Διαδίκτυο (Internet) και τον Παγκόσμιο Ιστό. Αντίθετα, οι πολέμιοι της τεχνολογίας αυτής, αναφέρονται στα ακόλουθα τεχνικά ή μη ζητήματα τα οποία σωρευτικά μπορούν να περιορίσουν την αποτελεσματικότητά της.

#### 2.2.1.3.1 Τεχνικά Ζητήματα

- **Η δέσμευση μπορεί να είναι μεγαλύτερης έκτασης από την επιθυμητή**

Η δέσμευση των IP διευθύνσεων δεν κάνει διακρίσεις, με την έννοια ότι η απόφαση να δεσμευτεί ένας δικτυακός τόπος ή μια ιστοσελίδα πρακτικά σημαίνει, ότι ολόκληρη η ιστοθέση θα δεσμευτεί και δε θα είναι προσπελάσιμη από τους χρήστες του Διαδικτύου (Internet), δηλαδή τους συνδρομητές των ISP's. Κατά συνέπεια, αν ένας δικτυακός τόπος φιλοξενείται από μια μεγάλη εταιρεία, όπως έναν ISP ή BSP, τότε οι υπόλοιπες ιστοσελίδες που φιλοξενούνται από αυτή την εταιρεία, επίσης θα δεσμευτούν και θα γίνουν μη προσπελάσιμες στους χρήστες του Διαδικτύου (Internet), και συνδρομητές των ISP's. Το γεγονός αυτό μπορεί να προκαλέσει πολλαπλά πρακτικά και νομικά προβλήματα στις εταιρείες που φιλοξενούν πολλές ιστοσελίδες.

- **Περιορίζονται και άλλες υπηρεσίες που πιθανόν να υποστηρίζονται από διακομιστή με την IP διεύθυνση που απορρίπτεται**

Η δέσμευση IP διευθύνσεων μπορεί να επηρεάσει και άλλες υπηρεσίες TCP/IP, εκτός από το HTTP. Η απόφαση να δεσμευτούν συγκεκριμένες ιστοσελίδες εξαιτίας παράνομου ή προσβλητικού περιεχομένου, ουσιαστικά σημαίνει ότι όλες οι άλλες υπηρεσίες, όπως FTP, SMTP, NNTP, επίσης θα δεσμευτούν. Αυτό θα συμβεί, επειδή οι αποφάσεις δέσμευσης IP διευθύνσεων βασίζονται κυρίως στις ίδιες τις IP διευθύνσεις. Οι παραπάνω κανόνες μπορούν να συμπεριλάβουν αριθμούς θύρας που προσδιορίζουν συγκεκριμένες υπηρεσίες, αλλά αυτό αποφεύγεται γιατί επιβαρύνει σημαντικά την απόδοση του δρομολογητή. Άλλωστε και αν γινόταν, οι αριθμοί θυρών μπορούν να αλλάξουν πολύ εύκολα, επομένως παρακάμπτεται ο έλεγχος με βάση την ACL.

- **Παράκαμψη ή Εξαπάτηση μέσω tunneling ή συχνή αλλαγή της IP διεύθυνσης**

Οι συσκευές δέσμευσης IP διευθύνσεων μπορούν εύκολα να παρακαμφθούν ή να «εξαπατηθούν». Αυτό μπορεί να συμβεί, είτε με συχνή αλλαγή της διεύθυνσης ή της θύρας που χρησιμοποιείται, είτε με χρήση της τεχνολογίας tunneling (IP διέλευσης).

- **Απόδοση- Υπολογιστική ισχύς- Κόστος**

Η δέσμευση των IP διευθύνσεων απαιτεί κάποια υπολογιστική ισχύ από τις συσκευές δρομολόγησης και φιλτραρίσματος. Κατά συνέπεια, οι BSP δρομολογητές, μπορεί να χρειαστεί να αναβαθμιστούν για να κατορθώσουν να υλοποιήσουν δέσμευση των IP διευθύνσεων. Ας σημειωθεί, ότι ένας κατάλληλα ρυθμισμένος αξιόλογος εμπορικός δρομολογητής, μπορεί να πραγματοποιήσει τη δέσμευση στο επίπεδο μεταγωγής πακέτου, σχεδόν σε ταχύτητα γραμμής, ενώ άλλοι φθηνότεροι θα πρέπει να αντικατασταθούν ή τουλάχιστον να αναβαθμιστούν, ώστε να μπορέσουν να ανταποκριθούν στις απαιτήσεις για ικανοποιητική απόδοση των σημερινών εργασιών στο Διαδίκτυο (Internet).

#### 2.2.1.3.2 Μη Τεχνικά Ζητήματα

- **Προβλήματα με εταιρείες που έχουν πολλαπλούς BSP' s**

Ένα μεγάλο ποσοστό της κίνησης δεν περνάει από τον BSP, όπως συμβαίνει για παράδειγμα για την επικοινωνία δύο χρηστών που ανήκουν στον ίδιο ISP ή μιας εταιρείας που διαθέτει μόνιμες συνδέσεις για την επικοινωνία μεταξύ των γεωγραφικά απομακρυσμένων παραρτημάτων της.

- **Λειτουργικό κόστος δημιουργίας και διανομής λιστών**

Υπάρχει αυξημένο λειτουργικό κόστος για τη δημιουργία, διατήρηση, διανομή και ρύθμιση των αντίστοιχων ACL's των συσκευών δρομολόγησης.

- **Ρύθμιση των ACL's δρομολογητών**

Για τη ρύθμιση των ACL's δρομολογητών, απαιτείται ειδικευμένο τεχνικό προσωπικό για τη δημιουργία, διαχείριση και ενημέρωση των ACL's

### 2.2.2 Σε επίπεδο εφαρμογής (URL)

Η περίπτωση της δέσμευσης περιεχομένου σε επίπεδο εφαρμογής αναφέρεται στις εξής περιπτώσεις:

- Αποκλεισμός σελίδων που βρίσκονται σε συγκεκριμένη τοποθεσία.
- Απαγόρευση της πρόσβασης σε αρχεία που βρίσκονται σε μια συγκεκριμένη τοποθεσία εξετάζοντας τον τύπο τους.

#### 2.2.2.1 Ο τρόπος που πραγματοποιείται

Ο αποκλεισμός του χρήστη από ορισμένες σελίδες στον ιστό μπορεί να επιτευχθεί με τη χρήση συγκεκριμένων τεχνικών. Σε επίπεδο εφαρμογής, οι τεχνικές εξέτασης του περιεχομένου επικεντρώνονται, είτε στο ίδιο το περιεχόμενο, είτε στην πηγή προέλευσης του περιεχομένου.

##### 2.2.2.1.1 Τεχνικές επικεντρωμένες στο περιεχόμενο

Πρόκειται για τεχνικές δυναμικού φιλτραρίσματος του περιεχομένου, κατά τις οποίες μια ιστοσελίδα «διαβάζεται» από το πρόγραμμα φίλτρο, το οποίο χρησιμοποιεί κάποιον αλγόριθμο για να την κατηγοριοποιήσει σε πραγματικό χρόνο.

Τα μειονεκτήματα αυτών των τεχνικών είναι οι επιπλέον υπολογιστικοί πόροι που χρειάζονται για να αναλύσουν την κάθε σελίδα, οι μεγάλοι χρόνοι που χρειάζεται μια σελίδα για να προβληθεί στο χρήστη και ο μεγάλος αριθμός ιστοσελίδων που αποκλείονται εσφαλμένα.

Οι τεχνικές αυτές υλοποιούνται σε προϊόντα για χρήση στο σπίτι ή σε εκπαιδευτικά ιδρύματα.

- **Εξέταση των λέξεων-κλειδιών του περιεχομένου**

Τα προϊόντα που πραγματοποιούν εξέταση λέξεων–κλειδιών του περιεχομένου, «σαρώνουν» το περιεχόμενο καθώς διαβιβάζεται από το Διαδίκτυο (Internet) στο χρήστη και αναζητούν λέξεις που περιέχονται στη μαύρη λίστα τους. Αν βρεθούν, η πρόσβαση στη σελίδα αποκόπτεται. Επίσης, ελέγχουν και τις εξερχόμενες αιτήσεις προς το Διαδίκτυο (Internet), προκειμένου να εμποδίσουν τους χρήστες να αναζητούν απρεπές περιεχόμενο μέσω μηχανών αναζήτησης στον Παγκόσμιο Ιστό.

Η εξέταση λέξεων-κλειδιών του περιεχομένου είναι πολύ αποδοτική και γι' αυτό είναι κατάλληλη και για παλαιότερους υπολογιστές μειωμένης ισχύος.

Τα προβλήματα της συγκεκριμένης τεχνικής είναι τα εξής:

- Δεν είναι ικανή να ελέγχει το περιεχόμενο μιας σελίδας που εκτός από κείμενο, περιέχει και άλλου είδους υλικό, όπως εικόνες.
- Προκειμένου να εφαρμοστεί ορθή εξέταση του κειμένου μιας ιστοσελίδας, θα πρέπει το προϊόν που υλοποιεί την τεχνική αυτή να μπορεί να εξετάζει το νόημα από τα συμφραζόμενα.

- Μια λέξη, που είναι παράγωγο μιας λέξης που το πρόγραμμα κρίνει ότι είναι απρεπής, θα θεωρηθεί και αυτή απρεπής.
- Τα περισσότερα θέματα που θεωρούνται απρεπή, περιγράφονται με λέξεις της καθομιλουμένης. Είναι συνεπώς δύσκολο να διαχωριστεί το πρέπον ή το μη πρέπον μόνο από το κείμενο που το περιγράφει.

- **Εξέταση φράσεων**

Πρόκειται για μια εξέλιξη της προηγούμενης τεχνικής. Ο μηχανισμός εξετάζει το κείμενο λαμβάνοντας υπόψη τα συμφραζόμενα, προκειμένου να κρίνει το περιεχόμενα. Είναι μια δύσκολη τεχνική, αν ληφθεί υπόψη το εύρος μιας γλώσσας και συνεπώς απαιτεί επιπλέον υπολογιστικούς πόρους.

- **Εξέταση της μορφολογίας του κειμένου**

Τα προϊόντα της τεχνικής αυτής εξετάζουν ορισμένα χαρακτηριστικά του υλικού που λαμβάνεται, όπως την αναλογία του κειμένου και των εικόνων μέσα σε μια ιστοσελίδα. Και αυτή η τεχνική απαιτεί επιπλέον πόρους και μειώνει το χρόνο απόκρισης του δικτύου. Γι' αυτό συνήθως χρησιμοποιείται επικουρικά σε άλλες πιο απλές μεθόδους, όπως το φιλτράρισμα των URL διευθύνσεων.

- **Ανάλυση εικόνας**

Η τεχνική αυτή αναλύει τα χαρακτηριστικά μιας εικόνας, όπως είναι οι χρωματικές εναλλαγές, προσπαθώντας να ανακαλύψει υλικό με απρεπές περιεχόμενο.

#### 2.2.2.1.2 Τεχνικές επικεντρωμένες στην πηγή-URL filtering

Η πιο κοινή και αποδοτική μορφή αποκλεισμού περιεχομένου, βασίζεται στην εξέταση των διευθύνσεων ενιαίου εντοπισμού (URL, Uniform Resource locator). Οι διευθύνσεις URL παρέχουν έλεγχο σε μεγαλύτερο βαθμό από τον αποκλεισμό περιεχομένου σε επίπεδο πακέτου, καθώς ονοματίζουν μεμονωμένες σελίδες στον Παγκόσμιο Ιστό και όχι ολόκληρα υπολογιστικά συστήματα.

Η τεχνική αυτή, κάνει χρήση βάσεων δεδομένων οι οποίες κατηγοριοποιούν και αποθηκεύουν τις διάφορες τοποθεσίες. Όταν ο χρήστης αιτείται μια τοποθεσία, ο μηχανισμός-φίλτρο, εξετάζει την URL και την αντιπαραβάλλει με τη βάση, για να εντοπίσει αν είναι καταχωρημένη σε κάποια κατηγορία. Στην περίπτωση αυτή, το περιεχόμενό της αποκλείεται ή διατίθεται στο χρήστη, αναλόγως, αν η βάση περιέχει επιτρεπόμενες ή αποκλειόμενες διευθύνσεις αντίστοιχα. Στην πρώτη περίπτωση η βάση καλείται «μαύρη λίστα», ενώ στη δεύτερη «λευκή λίστα».

Η τεχνική βασίζεται στην ιεραρχική δομή ονοματολογίας των σελίδων στο ιστό. Ανάλογα με τη μορφή της URL διεύθυνσης, η τεχνική μπορεί να αποκλείσει μεμονωμένες σελίδες, τμήματα μιας τοποθεσίας ή ακόμα και μια ολόκληρη τοποθεσία.

Τα φίλτρα που βασίζονται σε βάσεις δεδομένων, προτιμούνται κυρίως σε προϊόντα που απευθύνονται σε εταιρείες που ζητάνε υψηλή ταχύτητα απόκρισης του Διαδικτύου (Internet), ακρίβεια και ένα μηχανισμό που καθρεπτίζει τις συνήθειες των υπαλλήλων τους στο Διαδίκτυο (Internet).

Το μειονέκτημα αυτής της τεχνικής είναι ότι δε μπορεί να υπάρχει κατηγοριοποιημένος ολόκληρος ο ιστός σε μια βάση δεδομένων. Οι «ύποπτες» τοποθεσίες στον ιστό μπορούν να ξεγελάσουν τα φίλτρα, αλλάζοντας συχνά URL διευθύνσεις, αναγκάζοντας τους κατασκευαστές τέτοιων μηχανισμών να ανανεώνουν συνεχώς τις λίστες τους με πολλές νέες URL διευθύνσεις.

### 2.2.2.2 Ποιοι την πραγματοποιούν

Η δέσμευση URL,απαιτεί την ύπαρξη πληρεξούσιων εξυπηρετητών (proxy servers) ή αναχωμάτων ασφαλείας (Firewall) επιπέδου εφαρμογής, που εξετάζουν τους πόρους ή τις πληροφορίες, προκειμένου να αποφασίσουν αν η συγκεκριμένη αίτηση πρέπει να εξυπηρετηθεί ή όχι. Έτσι η δέσμευση URL, πραγματοποιείται από:

- **Τον πληρεξούσιο εξυπηρετητή (proxy server)**

Αποτελεί την πύλη ανάμεσα στο χρήστη και το Διαδίκτυο (Internet) και έχει τον απόλυτο έλεγχο στις πληροφορίες που μεταδίδονται από και προς το Διαδίκτυο (Internet). Χρησιμοποιείται συνήθως για να βελτιώσει την απόδοση του δικτύου με το να αποθηκεύουν περιεχόμενο που ζητείται συχνά, όπως επίσης και να παρέχει υπηρεσίες ασφάλειας και μετάφρασης διευθύνσεων στα ιδιωτικά δίκτυα.

Όλοι οι πελάτες του ISP δρομολογούνται μέσα από αυτόν το εξυπηρετητή και θα πρέπει να ρυθμίσουν κατάλληλα τον πλοηγό (browser) που χρησιμοποιούν, ώστε να απευθύνει τις αιτήσεις του για περιεχόμενο στον proxy. Αν δε γίνει η ρύθμιση αυτή, ο χρήστης δε μπορεί να αποκτήσει πρόσβαση στο Διαδίκτυο (Internet) μέσω αυτού του παρόχου.

Κάθε φορά που ο χρήστης αιτείται πρόσβαση σε μια συγκεκριμένη σελίδα στον Παγκόσμιο Ιστό ή σε ένα αρχείο από μια υπηρεσία ftp, συμβαίνουν τα ακόλουθα:

- Ελέγχεται αν το περιεχόμενο της αίτησης βρίσκεται αποθηκευμένο στον proxy. Στην περίπτωση αυτή διαβιβάζεται η σελίδα ή το αρχείο από τον proxy στο χρήστη.
- Αν το περιεχόμενο που ζητήθηκε δε βρίσκεται αποθηκευμένο στον proxy, διαβιβάζεται στο χρήστη από την τοποθεσία που το φιλοξενεί.

Ο proxy μπορεί να διαμορφωθεί κατάλληλα, ώστε να αναλάβει και το αποκλεισμό περιεχομένου των αιτήσεων που παραλαμβάνει. Αρκετοί πάροχοι υπηρεσιών Διαδικτύου (Internet) έχουν εγκαταστήσει στους proxy servers του δικτύου τους, λογισμικό διαφόρων κατασκευαστών, με διαφορετικά επίπεδα υποστήριξης για έλεγχο περιεχομένου. Αυτά τα προϊόντα, συνήθως επιτρέπουν ή απαγορεύουν την πρόσβαση σε ορισμένες τοποθεσίες του Διαδικτύου (Internet), βασισμένα σε λίστες IP ή URL διευθύνσεων επιτρεπόμενων ή απαγορευμένων τοποθεσιών.

Η μέθοδος μέσω proxy server είναι η πιο ασφαλής, διότι ο χρήστης έρχεται σε επαφή μόνο με την επιτρεπόμενη πληροφορία του Διαδικτύου (Internet), ενώ ο μηχανισμός ελέγχου και αποκλεισμού εκτελείται σε ένα ασφαλές περιβάλλον.

- **Τεχνική που είναι προσαρμοσμένη πάνω σε ανάχωμα ασφαλείας (Firewall).**

Ένα ανάχωμα ασφαλείας αναλαμβάνει να περιορίσει την πρόσβαση μεταξύ ενός ιδιωτικού δικτύου και του Διαδικτύου (Internet) ή άλλων δικτύων. Παρόλο που προορίζονται κυρίως για τον αποκλεισμό θυρών υπηρεσιών ενός εξυπηρετητή που είναι συνδεδεμένος στο Διαδίκτυο (Internet), έχουν εμφανιστεί κατασκευαστές αναχωμάτων, οι οποίοι στην προσπάθειά τους να δημιουργήσουν πιο ολοκληρωμένες λύσεις, παράγουν προϊόντα που έχουν τη δυνατότητα να ενσωματώνουν τεχνολογίες τρίτων κατασκευαστών. Ένα χαρακτηριστικό παράδειγμα ασφαλείας είναι της Checkpoint με την ονομασία FireWall-1, που διαθέτει ενσωματωμένη υποστήριξη εφαρμογών αποκλεισμού περιεχομένου.

### 2.2.2.3 Ζητήματα που την περιορίζουν

Και στην περίπτωση αυτή, οι γνώμες για την αποτελεσματικότητα της δέσμευσης URL διίστανται. Οι υποστηρικτές της τεχνολογίας αυτής ισχυρίζονται ότι είναι ένας εφικτός τρόπος για αποτελεσματική δέσμευση παράνομου ή προσβλητικού περιεχομένου. Αντίθετα,

οι πολέμιοι της τεχνολογίας αυτής, αναφέρονται στα ακόλουθα τεχνικά ή μη ζητήματα τα οποία σωρευτικά μπορούν να περιορίσουν την αποτελεσματικότητά της.

#### 2.2.2.3.1 Τεχνικά Ζητήματα

- **Παράκαμψη ή Εξαπάτηση μέσω συχνής αλλαγής της IP διεύθυνσης ή του ονόματος DNS**

Ένας χρήστης μπορεί να προσπελάσει μια ιστοσελίδα, καθορίζοντας το χαρακτηριστικό της DNS όνομα ή την ισοδύναμη IP διεύθυνση. Μια *μαύρη λίστα* που ελέγχει μόνο DNS ονόματα μπορεί να παρακαμφθεί, εκτός αν περιλαμβάνει και την ισοδύναμη IP διεύθυνση διπλασιάζοντας όμως με τον τρόπο αυτό το μέγεθος της μαύρης λίστας. Ομοίως, είναι δυνατό να αλλάζει τακτικά η IP διεύθυνση ή το DNS όνομα του υπολογιστικού συστήματος που φιλοξενεί τον HTTP server ή να τρέχουν περισσότεροι HTTP servers στο ίδιο υπολογιστικό σύστημα και να αλλάζει περιοδικά ο αριθμός της θύρας. Όλα αυτά θα μπορούσαν να οδηγήσουν τη δέσμευση σε αποτυχία, αφού αλλάζουν τα URL. Οι αλλαγές μπορούν να γίνουν γνωστές στους χρήστες επικοινωνώντας μαζί τους ή μπορεί να διαθέτουν υπηρεσίες μετάφρασης URL που να τρέχουν σε νόμιμους εξυπηρετητές.

- **Έλλειψη ρητής αίτησης για δέσμευση του περιεχομένου**

Υπάρχει η τάση στις τεχνολογικές λύσεις να παρακάμπτουν εντελώς τη δέσμευση URL, αφού το περιεχόμενο μπορεί να παραδοθεί στους χρήστες αν δεν έχει ζητηθεί από αυτούς **ρητά**. Ένας πληρεξούσιος εξυπηρετητής που εφαρμόζει δέσμευση URL, γενικά, φιλτράρει αιτήσεις για ανεύρεση συγκεκριμένου περιεχομένου. Αν το περιεχόμενο παραδοθεί χωρίς αντίστοιχη ρητή αίτηση, δε θα δεσμευτεί από τον πληρεξούσιο εξυπηρετητή.

- **Ο αποκλεισμός χρήσιμου περιεχομένου**

Το κύριο πρόβλημα που αντιμετωπίζουν οι κατασκευαστές ως προς τη σύνταξη των λιστών αποκλεισμένων τοποθεσιών, είναι το μέγεθος του Διαδικτύου (Internet). Παρόλο που οι τεχνικές που εφαρμόζει κάθε κατασκευαστής κρατούνται μυστικές, φαίνεται ότι οι περισσότεροι από αυτούς κατασκευάζουν τις μαύρες λίστες τους ερευνώντας στο Διαδίκτυο (Internet) και προσθέτοντας σελίδες που περιέχουν ύποπτο υλικό σε ενδιάμεσες μαύρες λίστες. Αυτές οι ενδιάμεσες μαύρες λίστες υποτίθεται ότι ελέγχονται από ανθρώπους πριν αναβαθμίσουν τις υπάρχουσες. Ομάδες αντιλογοκρισίας, όπως η Peacefire, έχουν εκφράσει ισχυρές αμφιβολίες σχετικά με την αποτελεσματικότητα αυτής της χειροκίνητης επιθεώρησης, δεδομένου του αριθμού των «ακίνδυνων» τοποθεσιών που έχουν αποκλειστεί από προγράμματα μεγάλων κατασκευαστών.

- **Η παράκαμψη λογισμικού δέσμευσης περιεχομένου**

Οι εταιρείες λογοκρισίας, μπορούν να δεσμεύουν σελίδες για λόγους διαφορετικούς από αυτούς που επίσημα έχουν δηλώσει. Για παράδειγμα, υπάρχουν καταγεγραμμένες περιπτώσεις στις οποίες εταιρείες που πουλούσαν λογισμικό δέσμευσης, είχαν αποκλείσει ISP's, επειδή αυτοί οι ISP's είχαν φιλοξενήσει σελίδες που ήταν επικριτικές όσο αφορά το συγκεκριμένο λογισμικό δέσμευσης. Οι εταιρείες πώλησης λογισμικού δέσμευσης θεωρούν ότι έχουν το αποκλειστικό προνόμιο της σύνταξης και εκμετάλλευσης των δικών τους καταλόγων με αποκλεισμένες σελίδες και γι' αυτό οι πελάτες δε μπορούν να έχουν πληροφόρηση ποιες ακριβώς σελίδες ανήκουν στη μαύρη λίστα.

- **Η χρήση μοναδικού πληρεξούσιου εξυπηρετητή από το χρήστη**

Η πολιτική που εξαναγκάζει το χρήστη να προσπελαύνει το Διαδίκτυο (Internet) μέσω ενός μοναδικού πληρεξούσιου εξυπηρετητή, μειώνει την αξιοπιστία και την απόδοση της σύνδεσης, αφού εισάγει ένα μοναδικό σημείο δυνητικής αποτυχίας (single point of failure). Επίσης, δημιουργούνται προβλήματα για κάποια πρωτόκολλα εφαρμογών όταν αυτά χρησιμοποιούν πληρεξούσιους εξυπηρετητές. Τέτοιο παράδειγμα εμφανίζεται σε πρωτόκολλα εφαρμογών των οποίων η λειτουργία στηρίζεται στο UDP.

#### 2.2.2.3.2 Μη Τεχνικά Ζητήματα

- **Πολιτική σχεδιασμού**

Οι ISP's θα βρεθούν σε σημαντικά διλήμματα ενώπιον των συνδρομητών τους κατά τη σχεδίαση πολιτικών προσπέλασης, είτε αυτές είναι αυστηρές, είτε υπερβολικά ανεκτικές.

- **Η διαφύλαξη της «*μαύρης λίστας*»**

Οι μαύρες λίστες είναι πολύτιμα αγαθά και για το λόγο αυτό πρέπει να διατηρούνται σε ασφαλή περιβάλλοντα. Μια μαύρη λίστα αποτελεί έναν ενδιαφέροντα στόχο για έναν επίδοξο εισβολέα και για το λόγο αυτό απαιτείται ασφαλής διαχείρισή τους.

## 2.3 Δέσμευση από τον συνδρομητή

### 2.3.1 Με εφαρμογή βαθμονόμησης περιεχομένου (Content Rating) και αυτο-οριοθέτησης (Self Determination)

Σύμφωνα με την τεχνική αυτή, παρέχεται η δυνατότητα στους ίδιους τους χρήστες να κρίνουν το περιεχόμενο μιας ιστοσελίδας με βάση κάποια συγκεκριμένα κριτήρια. Επιπλέον, στην πραγματικότητα συμβαδίζει με το γενικό επιχείρημα ότι οι χρήστες είναι τελικά υπεύθυνοι για τη δική τους στάση και δραστηριότητα. Βεβαίως, η πραγματικότητα είναι διαφορετική, αφού αναφερόμενοι στα σύγχρονα μέσα, όπως, εφημερίδες και τηλεοπτικά προγράμματα, μπορεί κανείς να ισχυριστεί ότι μόνο αυστηροί νομικοί περιορισμοί θα μπορούσαν να ελέγξουν την προσβλητικότητα κάποιου περιεχομένου. Αυτό χρησιμοποιείται συχνά σαν επιχείρημα εναντίον της αξιοποίησης της βαθμονόμησης περιεχομένου (Content Rating) και αυτο-οριοθέτησης (Self Determination).

#### 2.3.1.1 PICS

Το PICS (Platform for Internet Selection), αποτελεί έναν τρόπο βαθμονόμησης του περιεχομένου μιας ιστοσελίδας με τη χρήση ετικετών (labels). Οι ετικέτες PICS περιέχουν μια ή περισσότερες βαθμονομήσεις (ratings), οι οποίες εκδίδονται από μια υπηρεσία βαθμονόμησης (rating service) και όταν λαμβάνονται από τον χρήστη, συγκρίνονται με ένα σύνολο ετικετών, που έχει ορίσει εκείνος ότι είναι αποδεκτές. Είναι κάτι αντίστοιχο με τη σήμανση των τηλεοπτικών εκπομπών. Με τον τρόπο αυτό, παρέχεται η δυνατότητα στους ίδιους τους χρήστες να κρίνουν το περιεχόμενο μιας ιστοσελίδας. Ο τελικός χρήστης, είναι πλέον υπεύθυνος να επιλέξει την πολιτική ελέγχου που θα υιοθετήσει, όπως π.χ. επιλέγοντας να μην αγνοήσει τις ετικέτες ή ακόμη και να του επιτραπεί πλήρης πρόσβαση.

Το PICS έχει «ουδέτερη συμπεριφορά». Δηλαδή δεν καθορίζει το περιεχόμενο των ετικετών, αλλά μόνο τη μορφή τους και περιγράφει τον τρόπο μετάδοσής τους. Οι ετικέτες περιγράφουν απλά το περιεχόμενο μιας ιστοσελίδας και είναι στη δικαιοδοσία της εφαρμογής φιλτραρίσματος να αποφασίσει αν θα επιτρέψει την πρόσβαση στη συγκεκριμένη

ιστοσελίδα. Επομένως, οι ετικέτες PICS είναι χρήσιμες μόνο σε συνδυασμό με μια εφαρμογή δέσμευσης περιεχομένου.

Η τεχνική της βαθμονόμησης περιεχομένου και της αυτο-οριοθέτησης προϋποθέτει τα ακόλουθα στάδια:

- Τον ορισμό του λεξιλογίου των ετικετών
- Τα κριτήρια βάση των οποίων ανατίθενται οι ετικέτες
- Την ανάθεση των ετικετών
- Τη διανομή των ετικετών
- Τη δημιουργία λογισμικού που πραγματοποιεί τη δέσμευση περιεχομένου
- Τον καθορισμό των κριτηρίων βάση των οποίων ενεργοποιούνται τα φίλτρα δέσμευσης περιεχομένου
- Την εγκατάσταση και λειτουργία της εφαρμογής δέσμευσης περιεχομένου

Το PICS δεν υλοποιεί κανένα από τα παραπάνω στάδια. Το PICS είναι μια πρωτοβουλία της W3C (World Wide Web Consortium) και αποτελείται από ένα σύνολο τεχνικών προδιαγραφών, προκειμένου οι παραπάνω λειτουργίες να υλοποιούνται από ανεξάρτητες οντότητες.

Σύμφωνα με την έκδοση 1.1 (ver 1.1), τα επιμέρους συστατικά του PICS είναι:

- Ένα συντακτικό (syntax) που περιγράφει μια υπηρεσία βαθμονόμησης περιεχομένου, ώστε τα προγράμματα να μπορούν να παρουσιάσουν στους χρήστες τους, την υπηρεσία και τις ετικέτες της.
- Ένα συντακτικό για ετικέτες, ώστε να μπορούν τα προγράμματα να τις επεξεργαστούν. Μια ετικέτα μπορεί να περιγράψει είτε ένα μεμονωμένο έγγραφο, είτε μια ομάδα εγγράφων που υπάρχουν σε μια ιστοσελίδα. Επίσης, μπορεί να είναι κρυπτογραφημένη ή ψηφιακά υπογεγραμμένη.
- Μια διαδικασία ενσωμάτωσης ετικετών ή λιστών ετικετών στη μετάδοση, σύμφωνα με το RFC-822, καθώς και στη μορφή των εγγράφων HTML.
- Μια επέκταση του πρωτοκόλλου HTTP, ώστε οι εφαρμογές από την πλευρά του χρήστη (πελάτες), να μπορούν να ζητούν τη μετάδοση των ετικετών μαζί με ένα έγγραφο.
- Ένα συντακτικό αναζήτησης, για την επικοινωνία με ένα γραφείο ετικετών (label bureau).

#### 2.3.1.1.1 Υπηρεσίες βαθμονόμησης

Η RSACi που αναπτύχθηκε από την RSAC (Recreational Software Advisory Council) και η SafeSurf προσφέρουν λεξιλόγια ετικετών μέσω εξυπηρετητών που είναι συνδεδεμένοι στο Διαδίκτυο (Internet) και παράγουν ετικέτες σύμφωνα με τη μορφή που ορίζει το PICS.

Η RSAC δημιουργήθηκε στα μέσα της δεκαετίας του 1990 σαν απάντηση στις αρχικές ενέργειες του Κογκρέσου των Η.Π.Α για τη ρύθμιση του περιεχομένου των παιδικών παιχνιδιών video. Το Κογκρέσο αναγκάστηκε να δράσει μετά από την παραγωγή πολλών τέτοιων παιχνιδιών, στα οποία συμπεριλαμβάνονταν σκηνές βίας, και βάναυσες δολοφονίες. Η βιομηχανία ψυχαγωγίας, υποστήριξε ότι μπορεί να ελέγξει την κατάσταση χωρίς κρατική παρέμβαση και προσφέρθηκε να υιοθετήσει ένα εθελοντικό σύστημα διαβάθμισης, το οποίο θα επέτρεπε στους ανθρώπους, που αναζητούν ένα βιντεοπαιχνίδι να καθορίσουν τα επίπεδα βίας και των σκηνών σεξ που θα περιείχε το πρόγραμμα.

Ειδικότερα, το σύστημα RSACi παρέχει στους καταναλωτές πληροφορίες για το επίπεδο ανάρμοστου περιεχομένου σε παιχνίδια και ιστοσελίδες.

Το επίπεδο ανάρμοστου περιεχομένου ορίζεται από 0 έως 4 για βαθμονόμηση βίας, γυμνού, σεξ και προσβλητικής γλώσσας (Πίνακας 2.1)

| Επίπεδο | Περιγραφέας Βαθμονόμησης Βίας | Περιγραφέας Βαθμονόμησης Γυμνού | Περιγραφέας Βαθμονόμησης Σεξ | Περιγραφέας Βαθμονόμησης Γλώσσας |
|---|---|---|---|---|
| 4 | βιασμός, έντονη βία | εμπρόσθιο γυμνό, χαρακτηρισμένο ως προκλητική περιβολή | σαφείς σεξουαλικές πράξεις ή σεξουαλικά εγκλήματα | ωμή, χυδαία γλώσσα, ακραίος λόγος μίσους |
| 3 | επιθετική βία, δολοφονία | εμπρόσθιο γυμνό | μη Σαφείς σεξουαλικές πράξεις | υβριστική γλώσσα, λόγος μίσους |
| 2 | καταστροφή αντικειμένων | μερικό γυμνό | σεξουαλικό άγγιγμα πάνω από τα ρούχα | μέτρια βλασφημία, αισχρολογία |
| 1 | τραυματισμός ανθρώπων | αποκαλυπτική περιβολή | φλογερό φιλί | ήπια βλασφημία |
| 0 | κανένα από τα παραπάνω ή σχετιζόμενα με το αθλητισμό | κανένα από τα παραπάνω | κανένα από τα παραπάνω, αθώο φιλί, ειδύλλιο | κανένα από τα παραπάνω |

Το σύστημα RSACi υποστηρίζεται από τον Microsoft Internet Explorer, το λογισμικό Cyber Patrol και τον Netscape Navigator.

#### 2.3.1.1.2 Εφαρμογές του **PICS**

Το PICS καθορίζει μόνο τα τεχνικά ζητήματα της διαλειτουργικότητας και δεν ασχολείται με τον τρόπο λειτουργίας των υπηρεσιών βαθμονόμησης ή των εφαρμογών φιλτραρίσματος, αλλά μόνο με το πώς αυτά συνεργάζονται μεταξύ τους. Οι εφαρμογές που είναι συμβατές με το PICS μπορούν να υλοποιήσουν δέσμευση περιεχομένου ως εξής:

- Να υλοποιηθεί η εφαρμογή δέσμευσης περιεχομένου στον browser. Οι δύο πιο διαδεδομένοι browsers, Microsoft Internet Explorer και Netscape Navigator παρέχουν υποστήριξη για το PICS.
- Η δέσμευση περιεχομένου στο network protocol Stack, όπως γίνεται στο CyberPatrol και στο Surfwatch.
- Η δέσμευση περιεχομένου σε κάποιο σημείο του δικτύου, όπως π.χ. στον Proxy Server σε συνδυασμό με κάποιο Firewall.

#### 2.3.1.1.3 Ποιος χρησιμοποιεί το **PICS**

Το PICS μπορεί να χρησιμοποιηθεί από:

- **Τον δημιουργό του περιεχομένου ή κάποιον εκδότη** για να χαρακτηρίσει το περιεχόμενό του. Για να γίνει αυτό θα πρέπει να επιλέξει ή να ορίσει το λεξιλόγιο βαθμονόμησης που θα χρησιμοποιήσει με δική του πρωτοβουλία και να συνδεθεί σε μια ιστοσελίδα για να χαρακτηρίσει το προς δημοσίευση κείμενο συμπληρώνοντας ένα ερωτηματολόγιο. Στη συνέχεια η υπηρεσία του δίνει μια ετικέτα κειμένου σε

ειδική μορφή η οποία θα προσκολληθεί στην επικεφαλίδα HTML της σελίδας που θα δημιουργήσει.

- **Ένα γραφείο ανεξάρτητης βαθμονόμησης** το οποίο δεν είναι απαραίτητο να συνεργάζεται με το δημιουργό του κειμένου. Τα γραφεία αυτά οφείλουν να διανείμουν τις ετικέτες που θα δημιουργήσουν μέσω ενός ξεχωριστού εξυπηρετητή, το γραφείο ετικετών (label bureau). Το λογισμικό φιλτραρίσματος θα αναζητήσει τις ετικέτες στο γραφείο ετικετών.

#### 2.3.1.1.4 Ανάκτηση ετικετών **PICS**

Η ανάκτηση των ετικετών PICS μπορεί να γίνει, είτε μέσω ενός HTTP server, είτε μέσω μιας υπηρεσίας βαθμονόμησης.

##### 2.3.1.1.4.1 Μέσω HTTP server

Το PICS ορίζει μια επέκταση στο πρωτόκολλο HTTP, που επιτρέπει να ζητηθεί μια επικεφαλίδα PICS μαζί με το έγγραφο. Η επέκταση προϋποθέτει την αποστολή μιας εντολής αίτησης πρωτοκόλλου μετά την εντολή GET του HTTP.

Για παράδειγμα ο πελάτης (client) ζητά από τον HTTP server να του στείλει τις ετικέτες μαζί με τα έγγραφα που θέλει. Για να ζητηθεί ένα έγγραφο χρησιμοποιώντας HTTP με ετικέτες RSAC, ο πελάτης (client) μπορεί να στείλει μια αίτηση ως εξής:

```
GET / HTTP/1.0
Protocol-Request: {PICS-1.1 {params minimal{services
http://www.rsac.org/1.0}}}
```

Η λέξη-κλειδί «minimal» στο πεδίο «params", καθορίζει την ποσότητα της πληροφορίας που ζητείται. Υπάρχουν επίσης οι επιλογές: short, full και complete-label.

Η απάντηση του HTTP server είναι:

```
Date: Fri, 30 April 2002 20:30:00 GMT
Server: Stronghold+PICS/1.3.2 Ben-SSL/1.3 Apache/1.1.1
Content-type:text/html
PICS-Label: PICS-1.1 http://www.rsac.org/1.0/'' v 0 v 0 n 2 1 0)

<HTML>
<HEAD>
<TITLE>Welcome to Deus machine Software, Inc</TITLE>
...
```

##### 2.3.1.1.4.2 Μέσω μιας υπηρεσίας βαθμονόμησης

Το πρότυπο PICS ορίζει έναν τρόπο να ζητηθεί μια ετικέτα συγκεκριμένου URL από μια υπηρεσία βαθμονόμησης.

Οι υπηρεσίες βαθμονόμησης με τη σειρά τους, οφείλουν να ανταποκρίνονται σε αιτήσεις GET του HTTP, που κωδικοποιούν αναζητήσεις βάσεων δεδομένων μέσω URL.

Μια αίτηση μπορεί να είναι ως εξής:

```
GET /Ratings?opt=generic&
u="http%3A%2F%2Fwww.questionable.org%2Fimages"&
```

s="http%3A%2F%2Fwww.gcf.org%2Fv2.5"
HTTP/1.0

### 2.3.1.1.5 Χαρακτηρισμένα έγγραφα

Το πρότυπο PICS επιτρέπει στις ετικέτες να μεταδίδονται αυτομάτως μαζί με κάθε μήνυμα που χρησιμοποιεί επικεφαλίδες RFC 822. Αυτές οι επικεφαλίδες χρησιμοποιούνται από το ηλεκτρονικό ταχυδρομείο, το HTTP, και τα πρωτόκολλα Usenet news. Αυτό επιτρέπει την εύκολη προσθήκη ετικετών στην πληροφορία που μεταδίδεται από αυτά τα συστήματα.

Η επικεφαλίδα PICS RFC 822 είναι ετικέτα PICS . Η μορφή είναι:
PICS-Label: <labellist>

Για παράδειγμα, το παρακάτω μήνυμα, μπορεί να περιέχει προσβλητικό περιεχόμενο, μπορεί να πρόκειται για αστεία μεταξύ φίλων κ.λ.π. Ότι και να είναι το μήνυμα, μπορούμε να χρησιμοποιήσουμε μια ετικέτα PICS για να βγάλουμε ένα συμπέρασμα για το περιεχόμενό του και για το αν θα πρέπει να το διαβάσουμε.

To: hpgr@ex.com
From: sgr@ex.com
Date: Tue, 14 July 2003 14:06:14 -0500
Subject: Last Night
PICS –Label: (PICS -1.1.http://www.ssac.org/1.0/ v 0 s 4 n 4 1 4)

### 2.3.1.1.6 Πλεονεκτήματα του **PICS**

- Χαρακτηρίζεται ως ένα προϊόν με ουδέτερη συμπεριφορά, γιατί δεν καθορίζει το περιεχόμενο των ετικετών, αλλά τη μορφή τους και τον τρόπο μετάδοσής τους.
- Χρησιμοποιείται για τη δέσμευση του περιεχομένου για διαφορετικές ανάγκες, όπως, π.χ. ένας γονέας θέλει να προστατέψει τα παιδιά του από ακατάλληλο περιεχόμενο, ένας επιχειρηματίας μπορεί να θέλει να περιορίσει την κίνηση του δικτύου στις ώρες αιχμής ή να περιορίσει την αλόγιστη πρόσβαση των εργαζομένων του σε ιστοσελίδες που δε σχετίζονται με το αντικείμενο εργασίας τους, ενώ κυβερνητικοί οργανισμοί μπορεί να θέλουν να ελέγξουν τη διακίνηση περιεχομένου που δεν είναι νόμιμο σε κάποιες χώρες.
- Με τη χρήση του PICS αντιμετωπίζονται τα προβλήματα καθολικού αποκλεισμού που υπάρχουν στις τεχνικές δέσμευσης IP διευθύνσεων και URL.
- Οι ετικέτες PICS χρησιμοποιούνται από κάποιες μηχανές αναζήτησης και φιλτραρίσματος.

### 2.3.1.1.7 Προβλήματα

- Η μέθοδος αυτή προϋποθέτει τη βαθμονόμηση ενός μεγάλου όγκου περιεχομένου που είναι διαθέσιμο στο Διαδίκτυο (Internet), που δεν υποστήριζε αρχικά ετικέτες. Αυτό συμβαίνει, επειδή η βαθμονόμηση δεν αποτελεί standard και επομένως οι δημιουργοί περιεχομένου δεν είναι υποχρεωμένοι να την ενσωματώνουν.
- Σε περίπτωση που η βαθμονόμηση περιεχομένου γινόταν υποχρεωτική, οι υπηρεσίες βαθμονόμησης δε θα έκαναν πια εθελοντικά τη δουλειά τους, αλλά θα υπήρχε σημαντικό κόστος.

- Υπάρχει διαφορά στις ηθικές αξίες των κοινωνικών ομάδων, γεγονός που δυσκολεύει τη βαθμονόμηση ορισμένων ιστοσελίδων.
- Προβλήματα αξιοπιστίας που προκύπτουν από τη χρήση παραπλανητικών ετικετών. Μια λύση θα μπορούσε να είναι η κρυπτογράφηση της ετικέτας, προκειμένου να διασφαλιστεί η ακεραιότητά της ή ακόμα και η ψηφιακή υπογραφή του δημιουργού, προκειμένου να διασφαλιστεί η αυθεντικότητά του.

### 2.3.2 Με χρήση εφαρμογής που ελέγχει την προσπέλαση στον Παγκόσμιο Ιστό

Η εφαρμογή φιλτραρίσματος εγκαθίσταται στον προσωπικό υπολογιστή του χρήστη και τη διαχειρίζεται ο ίδιος.

Αυτή η τεχνική λύση παρουσιάζει δύο βασικά προβλήματα:

1. Οι μηχανισμοί δέσμευσης κειμένου δεν μπορούν να ελέγξουν και γραφικό περιεχόμενο.
2. Όταν μια ιστοσελίδα περιέχει μια λέξη – κλειδί, δεν σημαίνει απαραίτητα ότι το περιεχόμενο της είναι ακατάλληλο, οπότε δεσμεύεται ολόκληρη η ιστοσελίδα χωρίς λόγο.

# ΚΕΦΑΛΑΙΟ 3

# ΕΡΓΑΛΕΙΑ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

## 3.1 Websense Enterprise v5.0

Το Websense είναι μια ολοκληρωμένη πλατφόρμα Enterprise Internet Management (EIM). Απευθύνεται κυρίως σε επαγγελματικά περιβάλλοντα, όπου γίνεται εκτενής χρήση του διαδικτύου και όπου ο αριθμός των υπαλλήλων καθιστά αδύνατο το έργο ελέγχου των ενεργειών τους στο διαδίκτυο με οποιοδήποτε άλλο μέσο. Προσφέρει πολλούς διαφορετικούς τρόπους ενσωμάτωσής του με το υπάρχον δίκτυο της εκάστοτε εταιρίας και συνεργάζεται άψογα με μια πληθώρα από κατασκευαστές δικτυακού εξοπλισμού.

### 3.1.1 Γενικά Χαρακτηριστικά

- Προσφέρει ολοκληρωμένο και ακριβές φιλτράρισμα του διαδικτύου με την υποστήριξη μιας βάσης δεδομένων από URL, η οποία χτίστηκε δυναμικά με τη χρήση του WebCatcher(βλέπε ενότητα 2), ενώ παράλληλα χρησιμοποιεί ένα συνδυασμό από αυτοματοποιημένη και ανθρώπινη κατηγοριοποίηση.
- Μπορεί να διατηρήσει την ισορροπία της χρήσης του διαδικτύου, του δικτύου και των εφαρμογών μεταξύ αυτών που σχετίζονται με την εργασία και αυτών που αποσκοπούν αλλού, δίνοντας στους διαχειριστές τη δυνατότητα να ορίσουν προσωπικές πολιτικές για τη διαχείριση των παραπάνω.
- Ελαχιστοποιεί το επιπλέον έργο της διαχείρισης του δικτύου με τη χρήση του Websense Enterprise Manager, την κεντρική κονσόλα διαχείρισης.
- Δίνει τη δυνατότητα εφαρμογής του από χρήστες που δεν μιλάνε Αγγλικά με αναφορές, μπλοκαρισμένες σελίδες και ονόματα κατηγοριών σελίδων διαθέσιμες σε εννέα γλώσσες: Κινέζικα (απλοποιημένα και παραδοσιακά), Γαλλικά, Γερμανικά, Ιταλικά, Γιαπωνέζικα, Κορεάτικα, Πορτογαλικά και Ισπανικά.
- Διαθέτει μια πληθώρα από εργαλεία και επεκτάσεις που προσφέρουν άριστες δυνατότητες κατασκευής αναφορών, ενισχυμένη ικανότητα φιλτραρίσματος, εύκολη διαχείριση και βελτιστοποίηση της απόδοσης του δικτύου.

### 3.1.2 Απαιτήσεις / Δυνατότητες

Δύο είναι τα βασικότερα χαρακτηριστικά που προσδιορίζουν τις δυνατότητες μιας τέτοιας πλατφόρμας όπως είναι το Websense: η αρχιτεκτονική της, δηλαδή πώς αυτή αποτελεσματικά επικοινωνεί με το δίκτυό μας και το διασφαλίζει από την εσφαλμένη χρήση των πόρων του, κάτι που θα εξετάσουμε παρακάτω, και η βάση δεδομένων που διαθέτει.

#### 3.1.2.1 Websense Master Database

Η βάση δεδομένων του Websense, ή αλλιώς Master Database, όπως επίσημα ονομάζεται, αποτελείται από τις κατηγορίες των URL, των πρωτοκόλλων και των εφαρμογών, οι οποίες ουσιαστικά οδηγούν το μηχανισμό φιλτραρίσματος της πλατφόρμας. Συνολικά περιέχει 6 εκατομμύρια δικτυακούς τόπους που αντιστοιχούν σε 1.1 δισεκατομμύρια ιστοσελίδες. Αυτοί οι δικτυακοί χώροι είναι ταξινομημένοι σε παραπάνω από 80 κατηγορίες δίνοντας έτσι τη δυνατότητα για λεπτομερέστερη παραμετροποίηση των πολιτικών που υιοθετεί κάθε εταιρία. Η Master Database περιλαμβάνει δικτυακούς τόπους σε 52 διαφορετικές γλώσσες και προστίθενται σε αυτή κατά μέσο όρο 25.000 δικτυακοί τόποι ανά εβδομάδα.

Η βάση ενημερώνεται καθημερινά, καθώς ειδικό λογισμικό ψάχνει και κατηγοριοποιεί σελίδες και εφαρμογές. Όποιες από αυτές δεν κατηγοριοποιούνται με αυτό τον τρόπο εξετάζονται από ειδικό προσωπικό, το οποίο και τις αξιολογεί. Το Websense καθημερινά ενημερώνεται μέσω του διαδικτύου για όλες τις αλλαγές στη βάση του και έτσι πάντα διαθέτει την πιο πρόσφατη λίστα.

Οι κατηγορίες στις οποίες διαχωρίζονται τα URL στη βάση είναι ονομαστικά: εκτρώσεις, υλικό για ενήλικες, πολιτικές ομάδες, επιχειρήσεις και οικονομία, ναρκωτικά, μόρφωση, διασκέδαση, τζόγος, παιχνίδια, κυβερνητικά, υγεία, παράνομα ή αμφιλεγόμενα, πληροφορική, επικοινωνία μέσω διαδικτύου, αναζήτηση εργασίας, στρατιωτικά και εξτρεμιστικά, διάφορα, νέα και μέσα, ρατσισμός και μίσος, θρησκεία, ψώνια, κοινωνικές οργανώσεις, κοινωνίες και τρόποι ζωής, ειδικά γεγονότα, αθλητικά, άγουστα, ταξίδια, καθορισμένα από τον χρήστη, οχήματα, βία, όπλα. Αναλυτικά μπορούμε να δούμε τις κατηγορίες στο http://www.websense.com/products/about/database/categories.php.

Οι κατηγορίες που διαχωρίζονται οι εφαρμογές είναι επίσης εκτενείς και είναι διαθέσιμες στο http://www.websense.com/products/about/cpm/database.php.

Για την καλύτερη και πιο ολοκληρωμένη κατηγοριοποίηση των ιστοσελίδων το Websense παρέχει ένα add-on το οποίο είναι διαθέσιμο σε όλους τους κατόχους του Websense Enterprise για ανάλογο χρηματικό ποσό. Το Add-on αυτό ονομάζεται **Premium Groups** και προσφέρει τις εξής δυνατότητες:

- **Productivity PG**: Προσπαθεί να αυξήσει την παραγωγικότητα δίνοντας τη δυνατότητα διαχείρισης ιστοσελίδων που δεν έχουν σχέση με τη δουλειά και θεωρούνται εξαιρετικά χρονοβόρες, όπως: Διαφημίσεις, Freeware και Software Download, Instant Messaging, Message Boards και Clubs, διαδικτυακές επιχειρήσεις – μετοχές, Pay-to-Surf.
- **Bandwidth PG**: Κατηγοριοποιεί δικτυακές τοποθεσίες που επηρεάζουν σημαντικά την απόδοση και το εύρος του δικτύου επιβαρύνοντας έτσι σημαντικά τη λειτουργία του, όπως: τηλεόραση και ραδιόφωνο μέσω του διαδικτύου, τηλεφωνία μέσω διαδικτύου, Peer-to-Peer ανταλλαγή αρχείων, Personal Network Storage και Backup, Streaming Media.
- **Security PG**: Προσθέτει ένα ακόμα επίπεδο προστασίας στο δίκτυο εμποδίζοντας τους υπαλλήλους να προσπελάσουν, άθελά τους ή εσκεμμένα, ιστοσελίδες οι οποίες μπορούν να είναι επιβλαβείς σε αυτούς και το δίκτυο, όπως: Κακόβουλες ιστοσελίδες δηλαδή ιστοσελίδες που περιέχουν Spyware, MMC (Malicious Mobile Code), Phising και γενικότερα περιπτώσεις απάτης. Μια υπηρεσία του Security PG είναι ο Site Watcher ο οποίος σε ενημερώνει πότε η ιστοσελίδα της εταιρίας έχει προσβληθεί από MMC και τι μέτρα πρέπει να λάβεις ώστε να ελαχιστοποιήσεις τη ζημιά.

Παραπάνω αναφέραμε ότι η Master Database ενημερώνεται με κάποιους μηχανισμούς. Ο σημαντικότερος από αυτούς ονομάζεται WebCatcher. Ο πελάτης μπορεί να επιλέξει την ενεργοποίηση του, εάν αυτός το επιθυμεί. Ο WebCatcher με τη σειρά του καθημερινά ετοιμάζει μια κωδικοποιημένη λίστα σε XML η οποία περιέχει όλες τις ιστοσελίδες, τις οποίες έχουν επισκεφτεί οι χρήστες του δικτύου της εταιρίας και οι οποίες δεν έχουν κατηγοριοποιηθεί από το Websense. Όλες οι λίστες που συλλέγονται με αυτόν τον τρόπο ενώνονται σε μια και με τη βοήθεια του KILO(Knowledge, Indexing, Learning, Organization), ένα εργαλείο που χρησιμοποιεί έξυπνους αλγόριθμους για να διευκρινίσει το περιεχόμενο των σελίδων, οι σελίδες κατηγοριοποιούνται αφού περάσουν πρώτα μια διαδικασία η οποία αποτρέπει την πιθανότητα λάθους κατά το διαχωρισμό τους. Μετά τη διαδικασία όλες οι σελίδες έχουν αποκτήσει αυτό που το Websense αποκαλεί Fingerprint. Ουσιαστικά, πρόκειται για μια ετικέτα η οποία περιέχει βαθμολογίες ανάλογα με το περιεχόμενο της ιστοσελίδας. Εκτός από την προφανή χρήση της ετικέτας, που είναι η κατηγοριοποίηση ανάλογα με τις βαθμολογίες ή η αναζήτηση ανθρώπινης παρεμβολής σε

περίπτωση που οι βαθμολογίες δεν είναι σαφείς, επιπλέον δίνει τη δυνατότητα για να διενεργείται έλεγχος συνέπειας. Παλιά Fingerprints ιστοσελίδων συγκρίνονται με νέα και αν εντοπιστεί μεγάλη διαφορά μεταξύ τους τότε η σελίδα στέλνεται προς επανεξέταση από ανθρώπινο δυναμικό.

Το σύνολο των παραπάνω τεχνικών που αναφέρθηκαν σίγουρα δημιουργεί μια από τις πιο ολοκληρωμένες και πάντα ενημερωμένες βάσεις δεδομένων, ενώ η συμμετοχή του ανθρώπινου παράγοντα σίγουρα εξασφαλίζει, σε σημαντικό βαθμό, τη σωστή κατηγοριοποίηση και την αποφυγή ευτράπελων.

### 3.1.2.2 Websense Reporting Tools

Τα εργαλεία αναφορών του Websense είναι όλα ενσωματωμένα στη βασική συνδρομή για το Websense Enterprise. Προσφέρουν δυνατότητες αναφορών που αποτελούνται είτε από ιστορικά στοιχεία του δικτύου, είτε από στοιχεία σε πραγματικό χρόνο τα οποία συλλέγονται εκείνη ακριβώς την στιγμή. Συνολικά υπάρχουν τρία διαφορετικά εργαλεία.

- **Real-Time Analyzer** – Μια διεπαφή που παρέχει στους διαχειριστές του δικτύου μια άποψη της κίνησης σε πραγματικό χρόνο μέσα στο τελευταίο εικοσιτετράωρο. Κυρίως χρησιμοποιείται για να δίνει άμεσες απαντήσεις στα ερωτήματα που αφορούν το ποιος επιβαρύνει αυτή την στιγμή το δίκτυο και ποια ήταν η κίνηση προς το διαδίκτυο το τελευταίο x χρονικό διάστημα. Σημαντικό πλεονέκτημά του είναι ότι είναι απλό στην χρήση και έχει μια φιλική Web διεπαφή στην οποία μπορεί ο διαχειριστής να έχει πρόσβαση από οποιοδήποτε σημείο του δικτύου επιθυμεί. Για να λάβει τα στατιστικά ο Analyzer αρκεί να του δώσουμε τη διεύθυνση του Websense Enterprise Server στο δίκτυο του οποίου θέλουμε να παρακολουθήσουμε την κίνηση.
- **Explorer** – Μια διεπαφή που προορίζεται για τους υπεύθυνους του ανθρώπινου δυναμικού, τους διευθυντές της εταιρίας και τους διαχειριστές του δικτύου. Μας δίνει πληροφορίες σχετικά με το ιστορικό της πρόσβασης στο διαδίκτυο και καταδεικνύει πιθανά ζητήματα που έχουν σχέση με το προσωπικό. Δίνει απαντήσεις σε ερωτήματα του τύπου αν κάποιος υπάλληλος έχει επισκεφτεί σελίδες που σχετίζονται με hacking ή αν έχει χρησιμοποιήσει εφαρμογές για hacking. Επίσης, απαντά στο πόσο bandwidth χρησιμοποιείται σε streaming media ή αν κάποιος επισκέφτηκε κάποια σελίδα με Spyware ή MMC. Είναι απλός στη χρήση και χρησιμοποιεί μια Web based διεπαφή. Οι πληροφορίες αντλούνται από την Log Database.
- **Reporter** – Μια ολοκληρωμένη μηχανή αναφορών που αποτελείται από προκατασκευασμένες ή παραμετροποιημένες, από τον χρήστη, μακέτες οι οποίες ξεπερνούν τις 80 σε αριθμό. Μπορεί να προγραμματιστεί η εκτέλεση τους και να διαμοιραστούν μέσω e-mail. Ο μηχανισμός αναφορών μπορεί να είναι εγκατεστημένος στον ίδιο server με το Websense ή σε διαφορετικό, αν υπάρχει αυξημένη δραστηριότητα.

***Επιπλέον απαιτήσεις:***

**Real Time Analyzer**

- Καμία επιπλέον απαίτηση

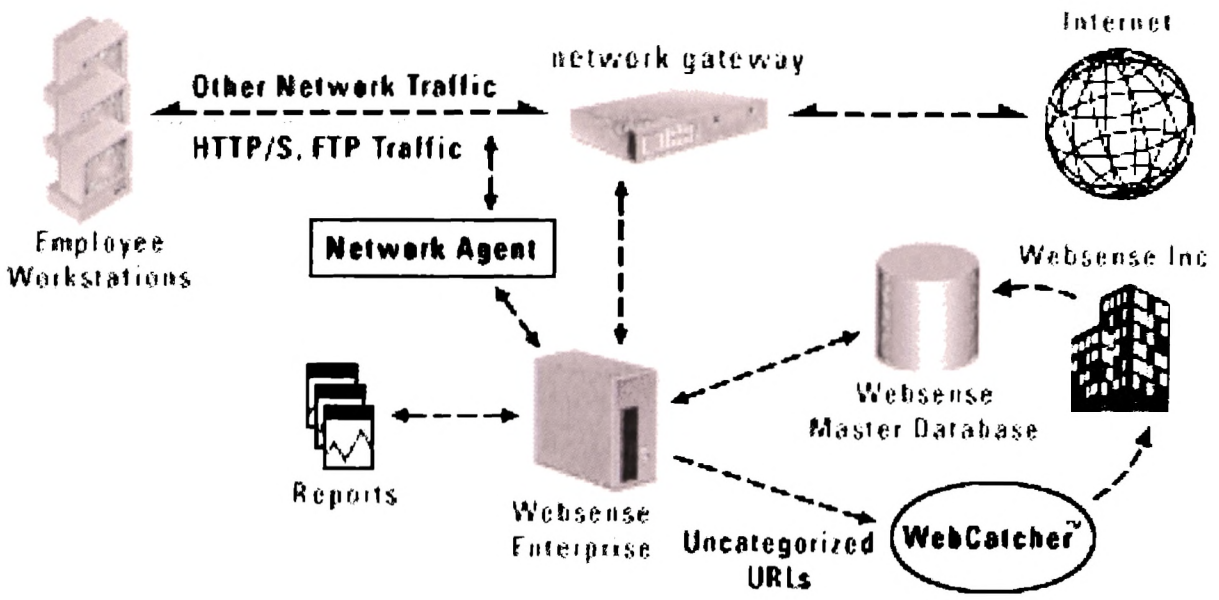
**Explorer**

- Web Server: MS IIS 4.0 ή καλύτερο, ή Apache v2.0.36 ή καλύτερο
- Browser: Internet Explorer v5.5 ή καλύτερο

- Log Server: Windows® 2003 Server (SP3 or higher), Windows® 2000 Server, Windows® NT Server 4.0 (SP6a ή καλύτερο), Solaris 8.9, Red Hat Linux 8.9
- Log Database Microsoft®: MSDE ή Microsoft® SQL Server, MySQL v4.0x

**Reporter**

- Log Server: Windows® 2003 Server (SP3 ή καλύτερο), Windows® 2000 Server, Windows® NT Server 4.0 (SP6a ή καλύτερο)
- Log Database Microsoft®: MSDE ή Microsoft® SQL Server
- Client: Most Windows® Platforms




εικ. 1 Βασική δομή της πλατφόρμας Websense

### 3.1.2.3 Websense Bandwidth Optimizer

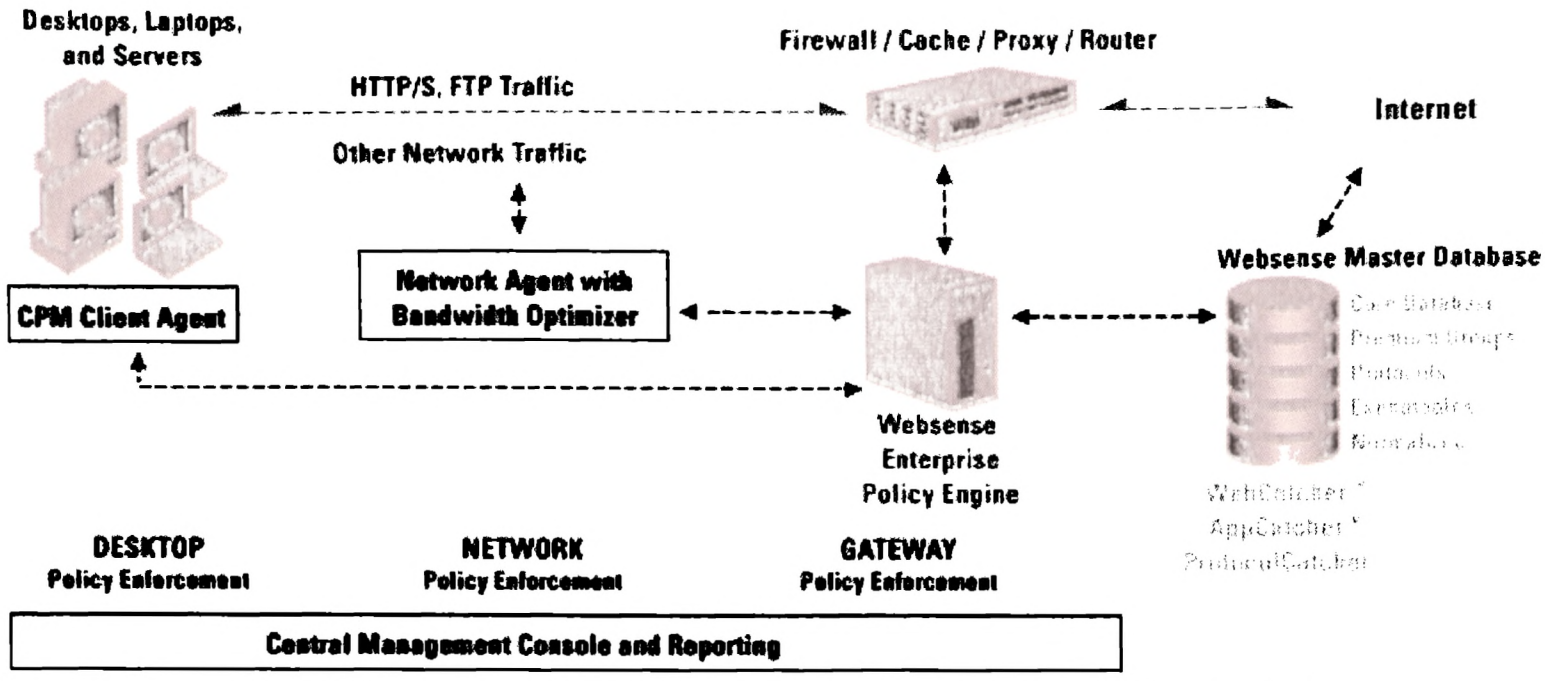
Για την ομαλή λειτουργία ενός δικτύου είναι απαραίτητο να γίνεται σωστή κατανομή του bandwidth που είναι διαθέσιμο. Ο Bandwidth Optimizer είναι ένα επιπρόσθετο εργαλείο το οποίο δεν είναι μέρος της βασικής συνδρομής του Websense Enterprise και έχει σαν σκοπό την παρακολούθηση της κατανάλωσης του Bandwidth και της αποδοτικότερης διαχείρισης του. Δίνει τις εξής δυνατότητες στους διαχειριστές του δικτύου:

- Τον ορισμό ορίων κατανάλωσης Bandwidth ανά κατηγορίες ιστοσελίδων.
- Τη διαχείριση του Bandwidth για υπηρεσίες Instant Messaging και Chatting και τη δυνατότητα χρήσης τους μόνο όταν υπάρχει πολύ διαθέσιμο.
- Το μπλοκάρισμα εφαρμογών streaming media όταν το δίκτυο έχει πλησιάσει την πλήρη χωρητικότητα του.

Διαθέτει πολλές δυνατότητες όπως τη ρύθμιση παραμέτρων βασισμένες σε πρωτόκολλα, κατηγορίες ιστοσελίδων ή ομάδες χρηστών. Μπορεί να επιβάλει περιορισμούς στη χρήση του bandwidth είτε βάση της συνολικής κατανάλωσης του, είτε βάση της κατανάλωσής του ανά εφαρμογή. Τέλος, όλα γίνονται αυτόματα και δυναμικά χωρίς την παρέμβαση του διαχειριστή του δικτύου.

***Επιπλέον απαιτήσεις:***

Ο Bandwidth Optimizer είναι ένα add-on εργαλείο και απαιτεί την ύπαρξη του Websense Enterprise Network Agent.




εικ. 2 Η δομή της πλατφόρμας Websense με τον Bandwidth Optimizer

### 3.1.2.4 Websense IM Attachment Manager

Το Instant Messaging έχει γίνει πολύ δημοφιλές στη εποχή μας λόγω της αμεσότητας παραλαβής του μηνύματος από τον δέκτη, αλλά και της ανωνυμίας που προσφέρει. Επίσης, αποτελεί ένα εύκολο και οικονομικό τρόπο συντονισμού και επικοινωνίας μεταξύ ομάδων μέσα στον εργασιακό χώρο. Η χρήση του αποφεύγεται από τους υπεύθυνους στον εργασιακό χώρο κυρίως για τρεις λόγους:

1. Με τη ανταλλαγή αρχείων το δίκτυο γίνεται ευάλωτο σε κακόβουλο λογισμικό.
2. Επιβάρυνση του Bandwidth.
3. Πιθανή ακούσια αποκάλυψη εμπιστευτικών στοιχείων της εταιρίας σε τρίτους.

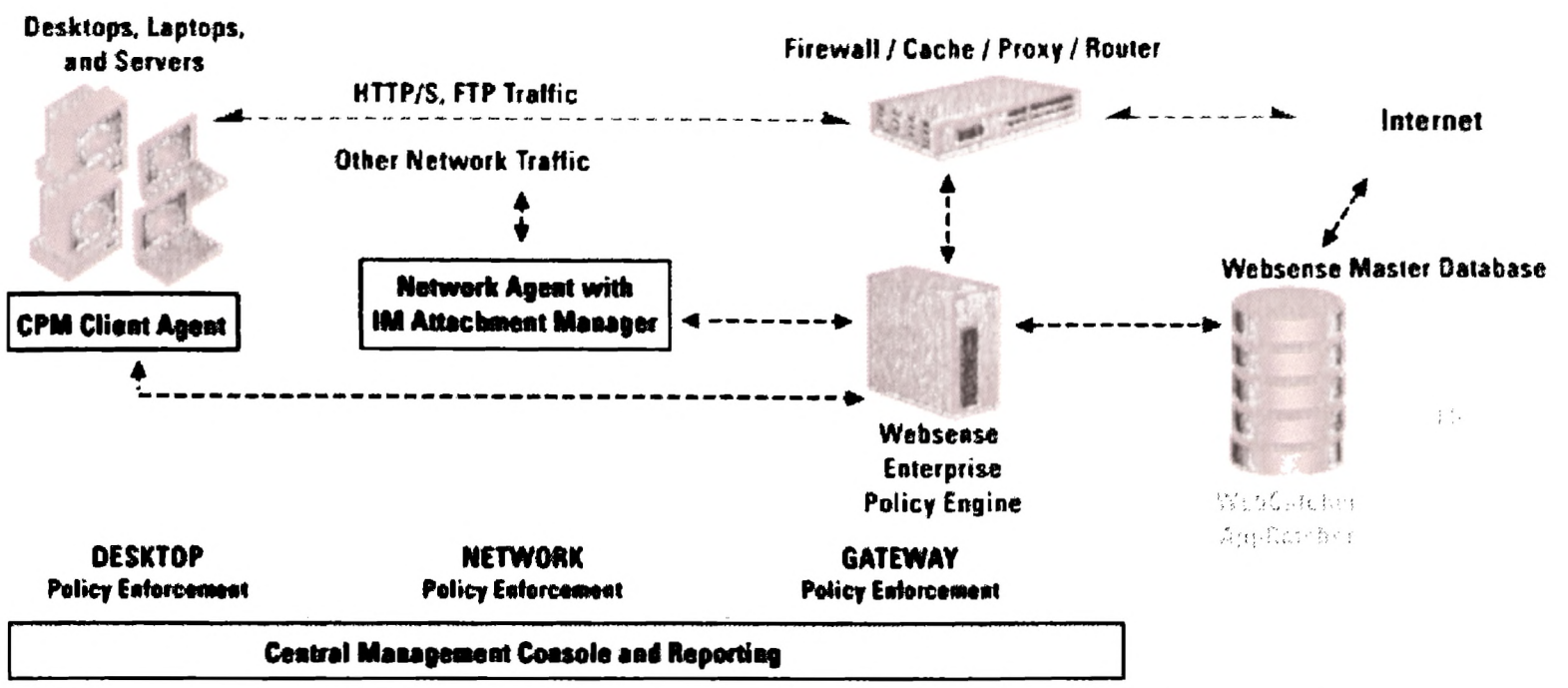
Ο IM Attachment Manager δίνει τη δυνατότητα διαχείρισης της χρήσης του IM από clients του δικτύου απαγορεύοντας την πρόσβαση σε ιστοσελίδες όπου έχουν προγράμματα IM για download και ελέγχοντας τα πρωτόκολλα του IM. Προσφέρει επίσης επιλογές για τη δημιουργία πολιτικής που αφορά το IM. Παρέχει τις εξής δυνατότητες στους διαχειριστές του δικτύου:

- Μπλοκάρει ή επιτρέπει την ανταλλαγή επισυνημμένων αρχείων των πιο δημοφιλών IM εφαρμογών
- Τον ορισμό συγκεκριμένων πολιτικών για επισυνημμένα αρχεία σε IM.
- Παρέχει αναφορές είτε σε πραγματικό χρόνο, είτε ιστορικές για κινδύνους που είχε αντιμετωπίσει η εταιρία σχετικά με επισυνάψεις αρχείων σε IM.
- Δυναμική διαχείριση των επισυνημμένων αρχείων βάση του Bandwidth σε συνεργασία με τον Bandwidth Optimizer.

Διαθέτει μια πληθώρα από επιλογές για τη δημιουργία διαφορετικών πολιτικών ελέγχου, ανάλογα με τις απαιτήσεις του δικτύου. Η επιβολή της πολιτικής αυτής γίνεται αυτόματα με την ελάχιστη δυνατή παρεμβολή του διαχειριστή και όλη η διαχείριση γίνεται κεντρικά χωρίς οι αλλαγές να είναι απαραίτητες και στους clients.

***Επιπλέον απαιτήσεις:***

Ο IM Attachment Manager είναι ένα add-on εργαλείο και απαιτεί την ύπαρξη του Websense Enterprise Network Agent.




εικ. 3 Η δομή της πλατφόρμας Websense με τον Attachment Manager

### 3.1.2.5 Websense Client Policy Manager

Οι απειλές που καλείται να αντιμετωπίσει ένα δίκτυο είναι πολλές και προέρχονται από επίσης πολλές πηγές. Σήμερα με την χρήση των φορητών υπολογιστών τείνουμε να μεταφέρουμε την εργασία μας στο σπίτι ή και στο ταξίδι. Όταν συνδέσουμε τον υπολογιστή μας στο εταιρικό δίκτυο αμέσως το καθιστούμε ευάλωτο σε άγνωστες μορφές απειλών τις οποίες άθελα μας τις μεταφέραμε μαζί μας επειδή πχ ενωθήκαμε στο διαδίκτυο από το σπίτι μας με μια απλή dial-up σύνδεση για να ελέγξουμε το e-mail μας, και όχι από το ασφαλές περιβάλλον της εταιρίας πίσω από τα firewalls και τις πολιτικές ασφαλείας.

Ο Client Policy Manager(CPM) μεταφέρει τις δυνατότητες του Websense στους υπολογιστές της εταιρίας είτε πρόκειται για desktops, laptops ή servers. Τα σημαντικότερα πλεονεκτήματά του είναι:

- Προσφέρει προστασία σε άγνωστες, έως εκείνη τη στιγμή, απειλές.
- Εντοπίζει και αναλύει απειλές ασφαλείας και δραστηριότητες εφαρμογών σε επιτραπέζιους υπολογιστές.
- Επιβάλλει πολιτικές για τη χρήση εφαρμογών σε χρήστες ή ομάδες χρηστών.

Η προστασία από άγνωστες ως εκείνη τη στιγμή απειλές επιτυγχάνεται με το μπλοκάρισμα συγκεκριμένων θυρών και πρωτοκόλλων, την απαγόρευση εκτέλεσης εφαρμογών πέρα από κάποιων συγκεκριμένων που έχουν δηλωθεί ως ασφαλείς και δίνοντας την δυνατότητα στους διαχειριστές να επιβάλουν άμεσα και γρήγορα αλλαγές στην πολιτική ασφαλείας που είναι απαραίτητες κατά το ξέσπασμα κρίσεων με ιούς.

Ο Explorer και Reporter για το CPM φροντίζουν για τον εντοπισμό πιθανών μελλοντικών απειλών και ύποπτων εφαρμογών και για την παραγωγή αναφορών γύρω από αυτά. Ο Inventory Manager δημιουργεί λίστες με το υλικό και το λογισμικό παρέχοντας κατηγοριοποιημένες καταστάσεις προγραμμάτων και εφαρμογών δίνοντας έτσι την δυνατότητα για τον γρήγορο εντοπισμό απειλών και την αναγνώριση μη εξουσιοδοτημένων εφαρμογών.

Οι πολιτικές είναι εύκολο να εφαρμοστούν γιατί οι εφαρμογές είναι χωρισμένες στην Master Database σε κατηγορίες. Επίσης, η βάση ενημερώνεται με τη χρήση των AppCatcher και ProtocolCatcher, τις αντίστοιχες εκδόσεις του WebCatcher, για εφαρμογές και πρωτόκολλα αντίστοιχα.

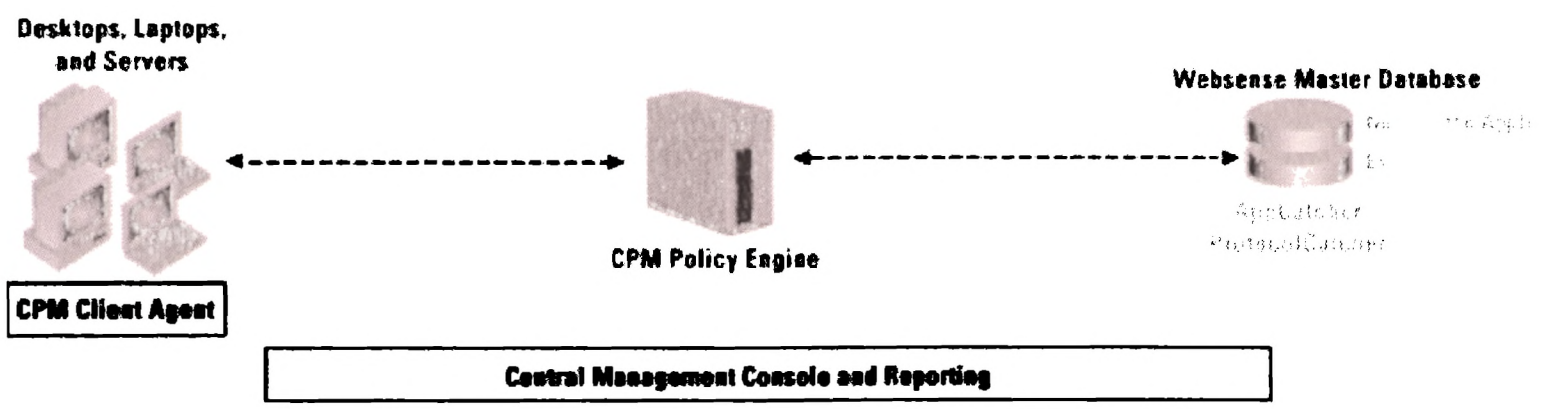
*Επιπλέον απαιτήσεις:*

**CPM Server**

- **Hardware:** Pentium III ή καλύτερος με τουλάχιστον 512 MB RAM. Οι απαιτήσεις σε υλικό διαφέρουν ανάλογα με το δίκτυο.
- **Software:** Microsoft® Windows® 2003 Server, Windows® 2000 Server (SP3 ή καλύτερο) ή Windows® NT 4 Server (SP6a ή καλύτερο).

**CPM Client**

- **Hardware:** Ο CPM client υποστηρίζει τους περισσότερους συνδυασμούς υλικού για επιτραπέζιους υπολογιστές.
- **Software:** Microsoft® Windows® XP, Windows® 2000, Windows® NT, ή Windows® 98 SE.




εικ. 4 Δομή του μηχανισμού CPM

### 3.1.2.6 Βασικές Απαιτήσεις

**Websense Enterprise v5.0**

**Hardware**

- Pentium III ή Sun Ultra 10 ή καλύτερος με τουλάχιστον 512 MB RAM. Οι απαιτήσεις σε υλικό διαφέρουν σημαντικά, ανάλογα με τη δομή του δικτύου, τα επιπρόσθετα εργαλεία που χρησιμοποιούνται και τον αριθμό τον χρηστών που υποστηρίζονται.

**Software**

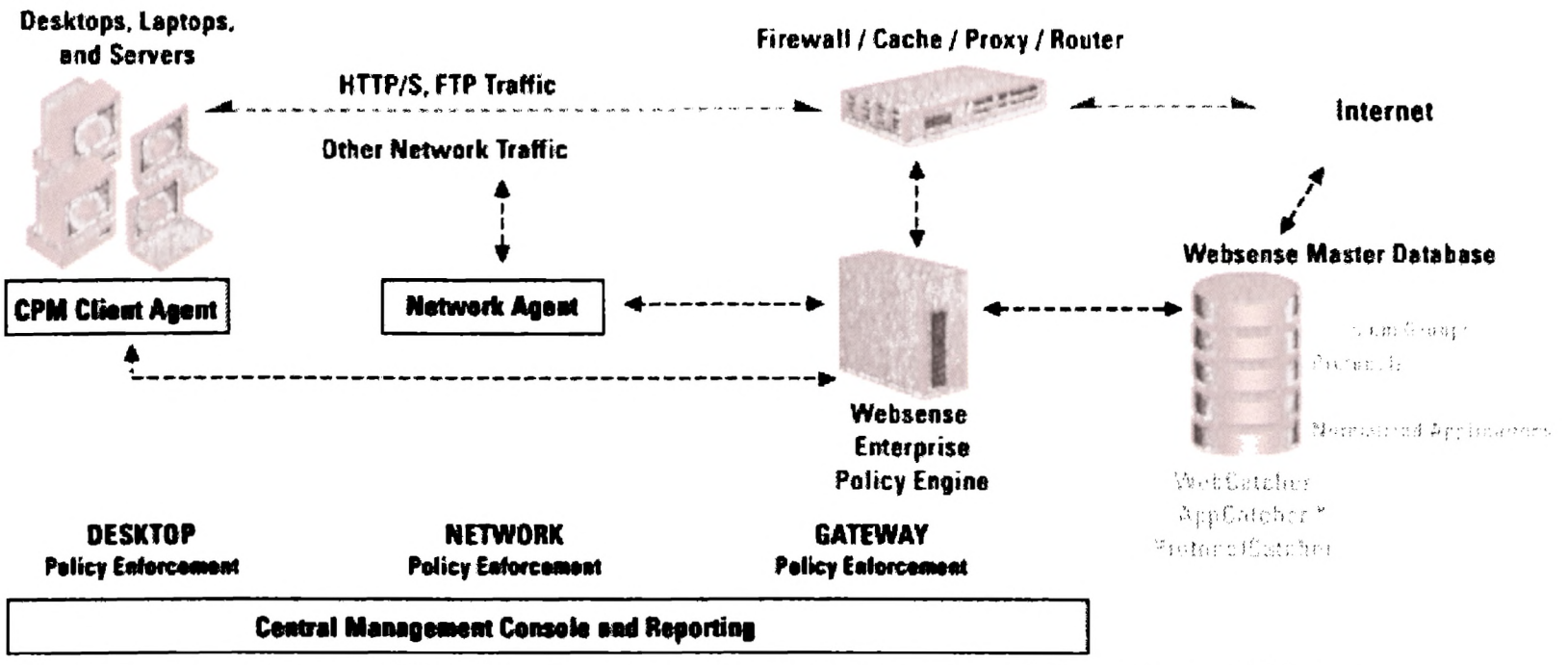
- Microsoft® Windows® 2003 Server, Windows® 2000 Server (SP3 ή καλύτερο) ή Windows® NT 4 Server (SP6a ή καλύτερο) ή Red Hat Linux™ 9 ή Red Hat Enterprise Linux™ 3 ή Sun Solaris™ 8-9.

Πλήρης λίστα απαιτήσεων μπορεί να βρεθεί στο http://www.websense.com/products/about/SysReqs/.

## 3.1.3 Αρχιτεκτονική και τρόπος λειτουργίας

Μια πλατφόρμα σαν το Websense για να λειτουργήσει σωστά και αποτελεσματικά πρέπει να ενσωματωθεί με επιτυχία στην ήδη υπάρχουσα δομή του δικτύου. Το Websense είναι βασισμένο στην τεχνολογία φιλτραρίσματος pass-through. Ουσιαστικά, όλες οι αιτήσεις για ιστοσελίδες περνάνε από ένα συγκεκριμένο σημείο ελέγχου του δικτύου, όπως firewall, proxy server ή μια συσκευή caching. Έτσι, ενσωματώνοντάς το σε αυτά τα σημεία

το Websense έχει πλήρη έλεγχο όλων των αιτήσεων και με βάση την πολιτική που έχει οριστεί καθορίζεται αν η αίτηση απορρίπτεται ή γίνεται δεκτή. Όλες οι αποκρίσεις του συστήματος καταγράφονται στο ημερολόγιό του για τη δημιουργία αναφορών.



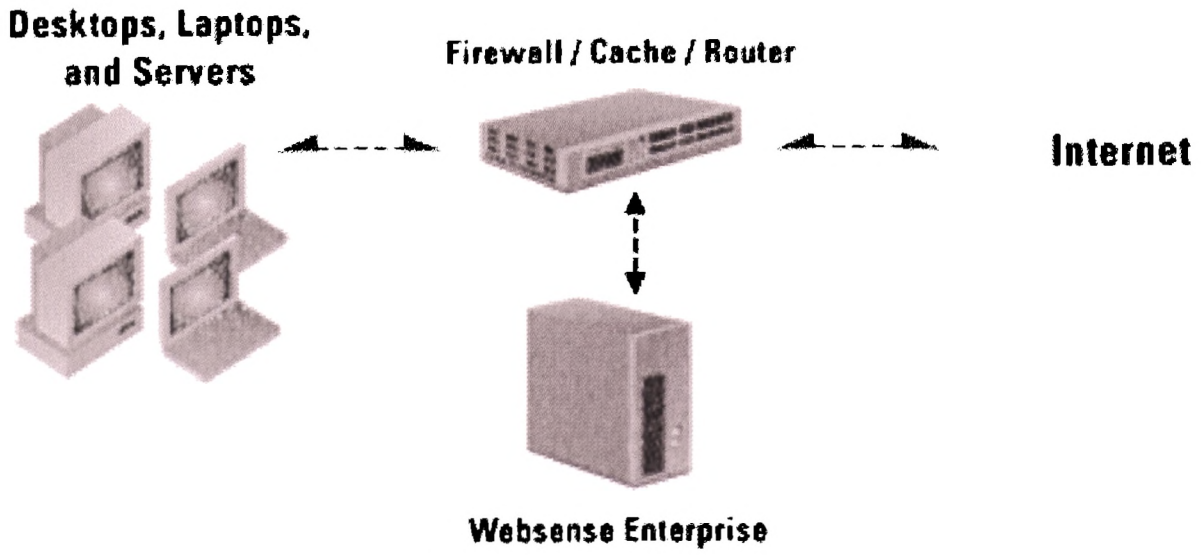

εικ. 5 Γενική αρχιτεκτονική ενσωμάτωσης της Πλατφόρμας Websense

### 3.1.3.1 Ενσωμάτωση και Συμβατότητα

Για να πετύχει την αποτελεσματική λειτουργία του στο δίκτυο το Websense μπορεί και ενσωματώνεται με μια σειρά από δικτυακά προϊόντα ασφαλείας, όπως firewalls, proxy servers, caches, switches και routers. Επίσης, πιστοποιεί τη λειτουργία του με προϊόντα από τις Blue Coat Systems, Check Point, Crossbeam, Cisco, CyberGuard, Dell, F5, Hewlett-Packard, iMimic, Immunix, infoLibria, Inktomi, LightSpeed, Microsoft, Network Appliances, NetScreen, Novell, Nokia, ServGate, SLMsoft, SonicWALL, Squid, Stratacache, Sun Microsystems και 3Com.

Το Websense μπορεί και ενσωματώνεται με τρεις διαφορετικούς τρόπους, ανάλογα με τις απαιτήσεις του δικτύου.

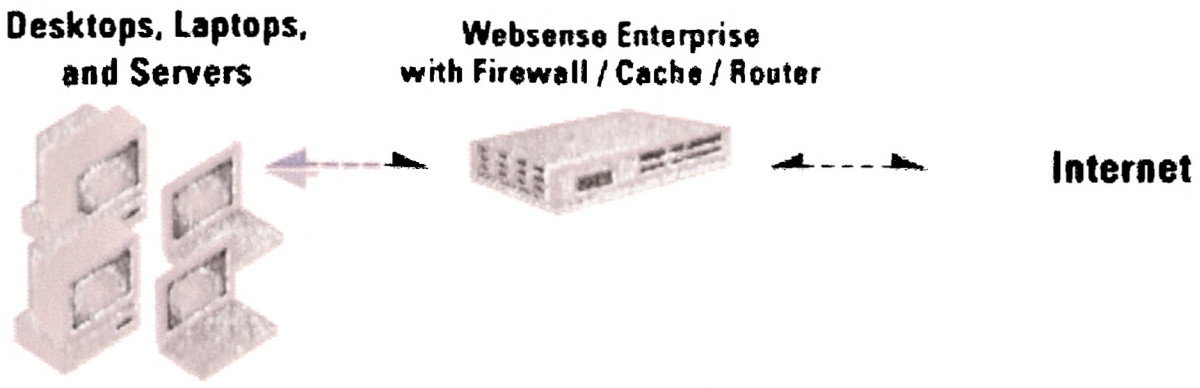
- **Integrated Deployment**: Ενσωματώνεται με τους firewall, proxy server, cache, switch και router προσφέροντας φιλτράρισμα pass-through χρησιμοποιώντας τις δυνατότητες του packet capturing του gateway του δικτύου. Με αυτό τον τρόπο επιτυγχάνεται το πιο αποτελεσματικό φιλτράρισμα ανεξάρτητα από τον όγκο της πληροφορίας και αποφεύγεται κάποια δομή δικτύου με μοναδικό σημείο δυνητικής αποτυχίας.




εικ. 6 Websense Integrated Deployment

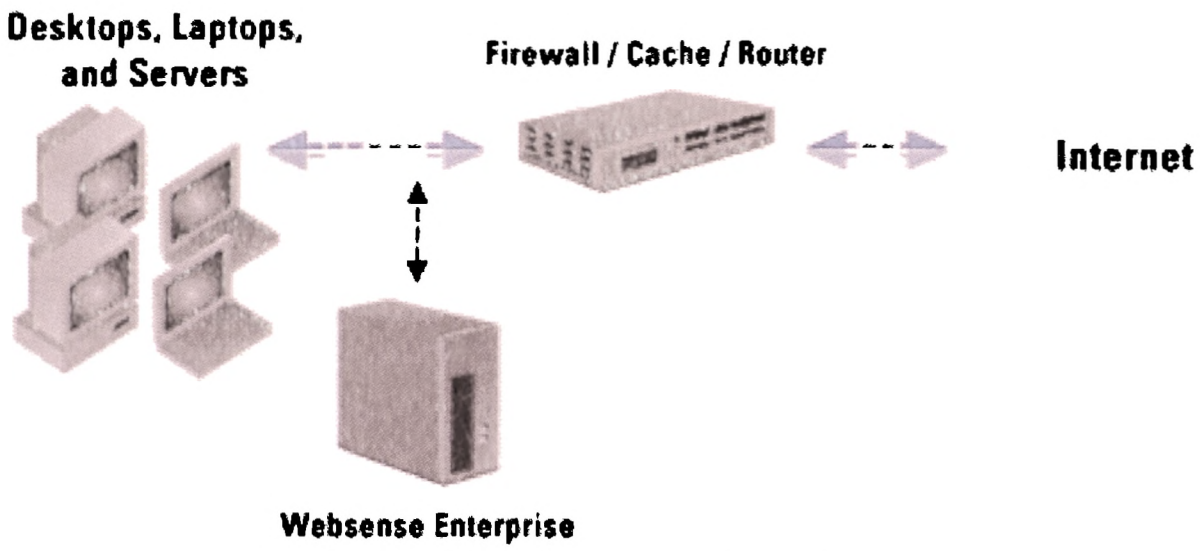
- **Embedded Deployment**: Ενσωματώνεται με μια συσκευή gateway, ουσιαστικά συνδυάζοντας πολλαπλές λειτουργίες σε μια πλατφόρμα. Αν και βέβαια οι

δυνατότητες διαφέρουν ανάλογα με την λύση που επιλέγεται, σημαντικό πλεονέκτημα αποτελεί το γεγονός ότι οι απαιτήσεις σε υλικό μειώνονται δραστικά και φυσικά βοηθάει στην αύξηση του εύρου ζώνης του δικτύου(network latency).




εικ. 7 Websense Embedded Deployment

- **Stand Alone Deployment**: Σε αυτή την περίπτωση το Websense δεν ενσωματώνεται ουσιαστικά αλλά στήνεται μόνο του, ξεχωριστά από την gateway. Ο Network Agent είναι αυτός που αναλαμβάνει το φιλτράρισμα με "pass-by" και συνεργάζεται με το gateway προσφέροντας παράλληλα και όλες τις δυνατότητες φιλτραρίσματος. Τα βασικότερα πλεονεκτήματά του είναι ότι: πρώτον είναι πολύ απλό στην εγκατάσταση και δεύτερον εξασφαλίζει τη μέγιστη δυνατή απόδοση του δικτύου, αφού ο Network Agent λειτουργεί σαν άμεση σύνδεση με την κίνηση του δικτύου φιλτράροντας τα πακέτα, καθώς διασχίζουν το φυσικό μέσο χωρίς να επηρεάζει άμεσα την απόδοση.




εικ. 8 Websense Stand Alone Deployment

### 3.1.3.2 Τα συστατικά του Websense Enterprise

Το Websense Enterprise αποτελείται από μια ομάδα συστατικών τα οποία συνεργάζονται για να παρακολουθούν την κίνηση προς και από το διαδίκτυο, να καταγράφουν τις δραστηριότητες που έχουν σχέση με αυτό και να φιλτράρουν ανάλογα με τις απαιτήσεις της πολιτικής. Η παραμετροποίηση των συστημάτων στα οποία τα συστατικά αυτά θα εγκατασταθούν εξαρτάται από το μέγεθος του δικτύου και την ποσότητα των αιτήσεων για το διαδίκτυο. Ακολουθεί μια σύντομη περιγραφή των συστατικών χωρισμένα στα γενικά και σε αυτά για αναφορές.

Πίνακας 1 Συστατικά του Websense

| Συστατικό | Περιγραφή |
|---|---|
| **DC Agent** | Ένα προαιρετικό συστατικό που χρησιμοποιεί τον Windows Domain Controller για τη διάφανη αναγνώριση των χρηστών προς φιλτράρισμα. |
| **Filtering Service** | Δέχεται τις αιτήσεις για το διαδίκτυο, εντοπίζει την ισχύουσα πολιτική φιλτραρίσματος, και είτε επιτρέπει ή |

| | |
|---|---|
| | απορρίπτει την αίτηση. |
| **Network Agent** | Εντοπίζει την κίνηση του δικτύου και υποστηρίζει τον Bandwidth Optimizer, τη διαχείριση πρωτοκόλλων και την αναφορά πάνω σε byte που μεταφέρθηκαν και τη διάρκεια μια συνόδου. |
| **Policy Server** | Αποθηκεύει τις ρυθμίσεις του Websense και επικοινωνεί αυτά τα δεδομένα με τα υπόλοιπα συστατικά. Επίσης, καταγράφει όλα τα μηνύματα γεγονότων των συστατικών άσχετα με την θέση τους στο δίκτυο. |
| **RADIUS Agent** | Ένα προαιρετικό συστατικό που δίνει τη δυνατότητα για διάφανη αναγνώριση των χρηστών που έχουν πρόσβαση στο δίκτυο μέσο dial-up, VPN, DSL, ή άλλες απομακρυσμένες συνδέσεις. |
| **User Service** | Επικοινωνεί με την υπηρεσία καταλόγου του περιβάλλοντος δικτύου και δίνει τη δυνατότητα να επιβληθούν πολιτικές φιλτραρίσματος βασισμένες σε χρήστες, ομάδες, domains και οργανωτικές μονάδες. Η υπηρεσία καταλόγου δεν είναι συστατικό του Websense αλλά μπορεί να είναι μια από τις Windows Directory Service, Windows Active Directory (μέσω LDAP), SunONE Directory Service(μέσω LDAP) ή Novell eDirectory(μέσω LDAP). |
| **Websense Enterprise Manager** | Η διεπαφή διαχείρισης η οποία επικοινωνεί με τον Policy Server για την παραμετροποίηση και τον έλεγχο της λειτουργικότητας του Websense. |
| **Websense Enterprise Real-Time analyzer** | Δείχνει σε πραγματικό χρόνο την κίνηση που φιλτράρεται από το Websense. Ο RTA παρουσιάζει με γραφικές παραστάσεις πληροφορίες που αφορούν το Bandwidth και δείχνει τις αιτήσεις ανά κατηγορία ή πρωτόκολλο. |
| **Websense Master Database** | Η Master Database όπως την περιγράψαμε παραπάνω. Περιέχει ιστοσελίδες, εφαρμογές και πρωτόκολλα. |

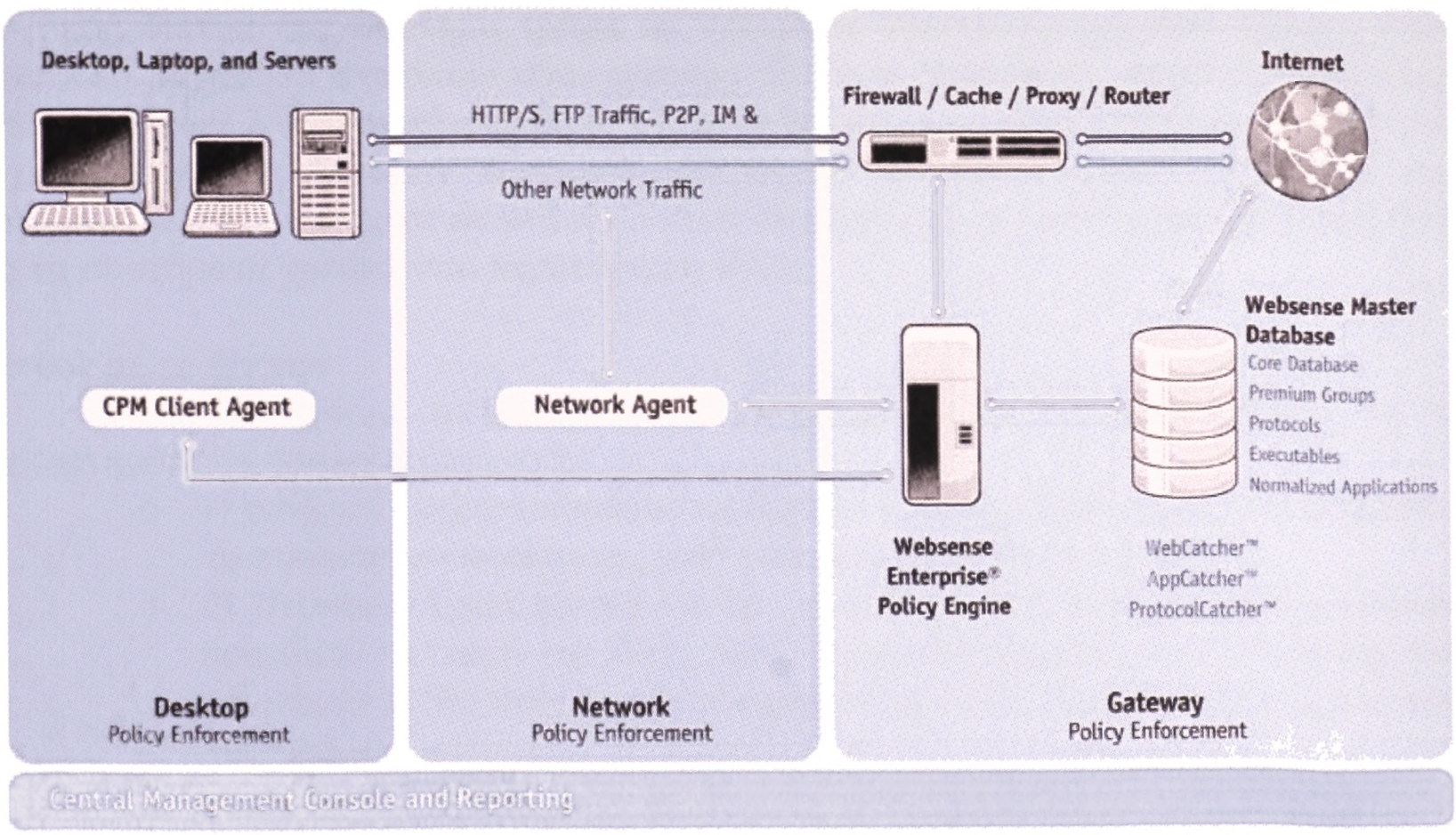
Πίνακας 2 Συστατικά αναφορών του Websense

| Συστατικό | Περιγραφή |
|---|---|
| **Απαραίτητα Συστατικά Αναφορών** | Τα Log Server, Log Database και Database Engine είναι απαραίτητα για την εκτέλεση των Websense Enterprise Reporter, Websense Enterprise Explorer και Log Database Manager. |
| **Database Engine** | Απαραίτητη για την εγκατάσταση των Microsoft SQL server ή MSDE. |
| **Log Database** | Απαραίτητος αποθηκευτικός χώρος για δεδομένα που έχουν σχέση με τη δραστηριότητα του διαδικτύου. Περιέχει εγγραφές από την υπηρεσία φιλτραρίσματος, όπως αυτές συγκεντρώνονται από τον Log Server, και χρησιμοποιούνται από τα Websense Enterprise Reporter και Websense Enterprise Explorer για την δημιουργία αναφορών. |
| **Log Server** | Καταγράφει και αποθηκεύει στην Log Database τη δραστηριότητα του διαδικτύου στο δίκτυο. |
| **Log Database Manager** | Μια εφαρμογή τύπου Web που βοηθάει στη διαχείριση του μεγέθους της Log Database, με δυνατότητες εκκαθάρισης και αρχειοθέτησης. |
| **Websense Enterprise Reporter** | Μια εφαρμογή τύπου Client που επικοινωνεί με το Websense και διαχειρίζεται πληροφορίες σχετικά με τη |

| | |
|---|---|
| | δραστηριότητα του διαδικτύου. |
| **Reporter** | Μια εφαρμογή διεπαφής χρήστη, η οποία κατασκευάζει τις αναφορές, που κατασκευάζονται αυτόματα, στέλνονται μέσω e-mail ή τυπώνονται. |
| **Websense Enterprise Explorer** | Μια εφαρμογή τύπου Web που κατασκευάζει μια πληθώρα από ευνόητες ολοκληρωμένες αναφορές από δεδομένα που βρίσκονται αποθηκευμένα στην Log Database, καθώς και από αρχειοθετημένα δεδομένα. Χρησιμοποιεί:<br>• Web Server: είτε Apache είτε Microsoft IIS<br>• Web Browser: Microsoft Internet Explorer |

### 3.1.3.3 Σχηματικές αναπαραστάσεις


εικ. 9 Οι αλληλεπιδράσεις των συστατικών του Websense Enterprise




εικ. 10 Δομή Websense: Φιλτράρισμα σε επίπεδο gateway, δικτύου και desktop.

### 3.1.3.4 Μελέτη Δικτύων

Οι απαιτήσεις και οι τρόποι εγκατάστασης των συστατικών του Websense διαφέρουν σημαντικά ανάλογα με τον αριθμό των χρηστών που ένα δίκτυο υποστηρίζει. Σε αυτή την ενότητα θα αναφερθούμε στις σημαντικότερες διαφορές χωρίζοντας τα δίκτυα σε τέσσερις κατηγορίες: μικρά (1 έως 500 χρήστες), μεσαία (500 έως 2500 χρήστες), μεγάλα (2500 έως 10000 χρήστες), και επιχειρησιακά (10000+ χρήστες).

- **Μικρά Δίκτυα: 1 έως 500 χρήστες**

Όλα τα συστατικά φιλτραρίσματος μπορούν να εγκατασταθούν σε ένα σύστημα το οποίο χρησιμοποιεί Windows. Εάν χρησιμοποιείται Linux ή Solaris τότε χρειάζονται ξεχωριστά συστήματα με Windows για να εγκατασταθούν τα συστατικά που τρέχουν μόνο σε Windows. Τα συστατικά του Websense Reporter επίσης απαιτούν ξεχωριστό σύστημα.

**Σχετικά με το δίκτυο**

Για να πετύχουμε αποτελεσματικό φιλτράρισμα το Websense πρέπει να είναι εγκατεστημένο με τέτοιο τρόπο ώστε:

- Η υπηρεσία φιλτραρίσματος να δέχεται αιτήσεις διαδικτύου από το gateway ή τη συσκευή ενσωμάτωσης (εάν υπάρχει) ή τον Network Agent.
- Ο Network Agent πρέπει να έχει ορατότητα της κίνησης που χρησιμοποιεί πρωτόκολλα τύπου όχι Web, όπως Instant Messaging, chat, streaming media, peer-to-peer file sharing, file transfer(όπως FTP), mail κα και προς και από το διαδίκτυο.
- Ο Network Agent πρέπει να είναι τοποθετημένος στο δίκτυο σε ένα συγκεκριμένο σημείο τέτοιο, ώστε να μπορεί να παρακολουθεί όλη την κίνηση του διαδικτύου στο εσωτερικό δίκτυο.
- ΣΗΜΑΝΤΙΚΟ: για να εξασφαλίσετε την ακεραιότητα του firewall σας μην εγκαταστήσετε συστατικά του Websense στο σύστημα αυτό.

- **Μεσαία Δίκτυα: 500 έως 2500 χρήστες**

Σε μεσαία δίκτυα τα συστατικά του Websense πρέπει να διαμοιραστούν σε δυο ή περισσότερα αφιερωμένα συστήματα, ανάλογα με το περιβάλλον λειτουργία σας. Όπως και στα μικρά δίκτυα ένα σύστημα τρέχει το Websense Enterprise και είτε Apache, είτε IIS server. Το μηχάνημα στο οποίο είναι εγκατεστημένο το Websense μπορεί να τρέχει κάποιο Windows Server λειτουργικό σύστημα, Linux ή Solaris, αν και το Linux και Solaris μπορεί να χρειαστούν ένα επιπλέον Windows αφιερωμένο μηχάνημα. Προτείνονται πιο ισχυρά συστήματα για τα συστατικά σε μεσαία δίκτυα σε σχέση με τα συστήματα στα μικρά δίκτυα. Όλα τα συστήματα χρειάζονται περισσότερη RAM.

**Σχετικά με το δίκτυο**

Για να πετύχουμε αποτελεσματικό φιλτράρισμα το Websense πρέπει να είναι εγκατεστημένο με τέτοιο τρόπο ώστε:

- Η υπηρεσία φιλτραρίσματος να δέχεται αιτήσεις διαδικτύου από το gateway ή τη συσκευή ενσωμάτωσης (εάν υπάρχει) ή τον Network Agent.
- Ο Network Agent πρέπει να έχει ορατότητα της κίνησης που χρησιμοποιεί πρωτόκολλα τύπου όχι Web, όπως Instant Messaging, chat, streaming media, peer-to-peer file sharing, file transfer(όπως FTP), mail κα και προς και από το διαδίκτυο.
- Ο Network Agent πρέπει να είναι τοποθετημένος στο δίκτυο σε ένα συγκεκριμένο σημείο τέτοιο ώστε να μπορεί να παρακολουθεί όλη την κίνηση του διαδικτύου στο εσωτερικό δίκτυο.
- ΣΗΜΑΝΤΙΚΟ: για να εξασφαλίσετε την ακεραιότητα του firewall σας μην εγκαταστήσετε συστατικά του Websense στο σύστημα αυτό.

- **Μεγάλα Δίκτυα: 2500 έως 10000 χρήστες**

Σε μεγάλα δίκτυα τα συστατικά του Websense πρέπει να διαμοιραστούν σε δυο ή περισσότερα αφιερωμένα συστήματα, ανάλογα με το περιβάλλον λειτουργία σας. Η ανάπτυξη στα αφιερωμένα μηχανήματα είναι η ίδια όπως και στα μεσαία δίκτυα. Εξαιτίας της αυξημένης κίνησης λόγω μεγαλύτερου δικτύου, διπλοί επεξεργαστές και περισσότερη RAM προτείνονται για κάθε αφιερωμένο μηχάνημα.

**Σχετικά με το δίκτυο**

Για να πετύχουμε αποτελεσματικό φιλτράρισμα το Websense πρέπει να είναι εγκατεστημένο με τέτοιο τρόπο ώστε:

- Σε ένα δίκτυο πολλαπλών τμημάτων η υπηρεσία φιλτραρίσματος πρέπει να είναι εγκατεστημένη σε μια τοποθεσία τέτοια ώστε να μπορεί να δεχθεί και να ελέγξει αιτήσεις για το διαδίκτυο από τον συνέταιρο ενσωμάτωσης και να επικοινωνήσει με τον Network Agent.
- Ο Network Agent πρέπει να έχει ορατότητα της κίνησης που χρησιμοποιεί πρωτόκολλα τύπου όχι Web, όπως Instant Messaging, chat, streaming media, peer-to-peer file sharing, file transfer(όπως FTP), mail κα και προς και από το διαδίκτυο.
- Ο Network Agent πρέπει να είναι τοποθετημένος στο δίκτυο σε ένα συγκεκριμένο σημείο τέτοιο ώστε να μπορεί να παρακολουθεί όλη την κίνηση του διαδικτύου στο εσωτερικό δίκτυο.
- Για μεγαλύτερα δίκτυα πρέπει να εγκατασταθούν πολλαπλοί Network Agents όπου ο καθένας θα παρακολουθεί μια συγκεκριμένη έκταση IP διευθύνσεων ή κάποιο συγκεκριμένο τμήμα του δικτύου. Ανάλογα με το μέγεθος και την κίνηση του δικτύου μπορεί να χρειαστούν πολλαπλοί Network Agents για να συλλάβουν όλη την κυκλοφορία και να πετύχουν κατανεμημένη παρακολούθηση και διαχείριση όλης της κίνησης. Μπορείτε να τοποθετήσετε Network Agents σε αφιερωμένους server για να αυξήσετε τη συνολική απόδοσή τους.
- ΣΗΜΑΝΤΙΚΟ: για να εξασφαλίσετε την ακεραιότητα του firewall σας μην εγκαταστήσετε συστατικά του Websense στο σύστημα αυτό.

- **Επιχειρησιακά Δίκτυα: 10000+ χρήστες**

Σε ένα επιχειρησιακό δίκτυο τα συστατικά του Websense θα πρέπει να διαμοιραστούν σε τρία αφιερωμένα συστήματα. Οι απαιτήσεις σε επεξεργαστές και RAM των αντίστοιχων αφιερωμένων συστημάτων είναι ίδιες όπως και στα μεγάλα δίκτυα για κάθε λειτουργικό σύστημα. Σε αντίθεση με τα μικρότερα δίκτυα ο Network Agent, ο Real-Time Analyzer και ο Web Server είναι εγκατεστημένα σε ξεχωριστά μηχανήματα.

**Σχετικά με το δίκτυο**

Για να πετύχουμε αποτελεσματικό φιλτράρισμα το Websense πρέπει να είναι εγκατεστημένο με τέτοιο τρόπο ώστε:

- Σε ένα δίκτυο πολλαπλών τμημάτων η υπηρεσία φιλτραρίσματος πρέπει να είναι εγκατεστημένη σε μια τοποθεσία τέτοια ώστε να μπορεί να δεχθεί και να ελέγξει αιτήσεις για το διαδίκτυο από τον συνέταιρο ενσωμάτωσης και να επικοινωνήσει με τον Network Agent.
- Ο Network Agent πρέπει να έχει ορατότητα της κίνησης που χρησιμοποιεί πρωτόκολλα τύπου όχι Web, όπως Instant Messaging, chat, streaming media, peer-to-peer file sharing, file transfer(όπως FTP), mail κα και προς και από το διαδίκτυο.

- Ο Network Agent πρέπει να είναι τοποθετημένος στο δίκτυο σε ένα συγκεκριμένο σημείο τέτοιο ώστε να μπορεί να παρακολουθεί όλη την κίνηση του διαδικτύου στο εσωτερικό δίκτυο.
- Για μεγαλύτερα δίκτυα πρέπει να εγκατασταθούν πολλαπλοί Network Agents όπου ο καθένας θα παρακολουθεί μια συγκεκριμένη έκταση IP διευθύνσεων ή κάποιο συγκεκριμένο τμήμα του δικτύου. Ανάλογα με το μέγεθος και την κίνηση του δικτύου μπορεί να χρειαστούν πολλαπλοί Network Agents για να συλλάβουν όλη την κυκλοφορία και να πετύχουν κατανεμημένη παρακολούθηση και διαχείριση όλης της κίνησης. Μπορείτε να τοποθετήσετε Network Agents σε αφιερωμένους server για να αυξήσετε την συνολική απόδοσή τους.
- ΣΗΜΑΝΤΙΚΟ: για να εξασφαλίσετε την ακεραιότητα του firewall σας μην εγκαταστήσετε συστατικά του Websense στο σύστημα αυτό.

### 3.1.4 Αξιολόγηση / Συμπεράσματα

Το Websense πιθανότατα αυτή τη στιγμή αποτελεί την πιο ολοκληρωμένη πρόταση στον χώρο του Enterprise Internet Management (EIM). Με την πιο πλήρη και συνεπή βάση δεδομένων και με ένα μηχανισμό φιλτραρίσματος που ενσωματώνεται σε όλους τους τύπους δικτύου μπορεί και εφαρμόζει τις πιο πολύπλοκες πολιτικές φιλτραρίσματος με απόλυτη επιτυχία. Οι πολλαπλές του δυνατότητες σε συνδυασμό με τα επιπρόσθετα εργαλεία αναβαθμίζουν το Websense σε ένα επίπεδο παραπάνω από αυτό ενός λογισμικού λογοκρισίας. Μπορεί, αφενός να βελτιώνει την απόδοσή του δικτύου μας, και αφετέρου να το προστατεύει από απειλές άγνωστες ως εκείνη τη στιγμή. Δίνει λύσεις σε δυναμικά προβλήματα, όπως η έλλειψη bandwidth σε κάποια χρονική στιγμή ή η ραγδαία εξάπλωση κάποιου νέου ιού και προσπαθεί να περιορίσει την πιθανή ζημιά που αυτά μπορούνε να επιφέρουν. Τέλος, η άριστη συνεργασία του με τους μεγαλύτερους κατασκευαστές δικτυακών προϊόντων το καθιστά μια από τις καλύτερες επιλογές, καθώς οι ασυμβατότητες σε δίκτυα υψηλής σημασίας σε ένα οργανισμό ή μια επιχείρηση είναι απαγορευτικές.

## 3.2 MIMEsweeper for Web 5.0

Το MIMEsweeper for Web είναι η πρόταση της Clearswift για αποτελεσματικό φιλτράρισμα της κίνησης από και προς το διαδίκτυο. Όπως και το Websense, απευθύνεται κυρίως σε επαγγελματικά περιβάλλοντα που κάνουν χρήση του διαδικτύου και έχουν ένα σεβαστό αριθμό χρηστών που πρέπει να ελέγχουν. Διαθέτει μια πληθώρα από διαφορετικούς τρόπους ελέγχου του περιεχομένου που μεταφέρεται, αλλά και την προαιρετική δυνατότητα φιλτραρίσματος με βάση τα URL. Μέσα στο δίκτυο παίζει τον ρόλο ενός HTTP πληρεξούσιου εξυπηρετητή (proxy server).

### 3.2.1 Γενικά Χαρακτηριστικά

- Πλήρως συμβατός HTTP caching proxy με δυνατότητες: ανάλυσης περιεχομένου σε βάθος, φιλτράρισμα με βάση URL, ενσωμάτωσης με το υπάρχον λογισμικό αντιβιοτικού, διαχείρισης της πολιτικής και αναφορών.
- Μηχανή ελέγχου του περιεχομένου προς και από το διαδίκτυο με δυνατότητα ανάλυσης του περιεχομένου των σελίδων και των downloads, αλλά και ανάλυση με βάση το μέγεθος και τον τύπο των αρχείων.

- Ελέγχει αρχεία, scripts, και html με βάση το πραγματικό τους περιεχόμενο, αναλύοντάς τα στα συστατικά τους και όχι απλά με βάση τον τύπο τους, το όνομα και το μέγεθος τους.
- Συνεργάζεται πλήρως με ήδη εγκατεστημένο φίλτρο URL ή με το προαιρετικό MIMEsweeper URL filter.

## 3.2.2 Απαιτήσεις / Δυνατότητες

Η Clearswift δηλώνει ξεκάθαρα ότι το πρόγραμμά της δεν περιορίζεται μόνο στο φιλτράρισμα των URL, αλλά ότι προσπαθεί να δώσει μια ολοκληρωμένη λύση στα προβλήματα που παρουσιάζονται από την ανεξέλεγκτη χρήση του διαδικτύου. Βέβαια, αν το MIMEsweeper θέλει να θεωρείται σαν μια ολοκληρωμένη λύση είναι λογικό να καλύπτει και άλλους τομείς πέρα από το απλό φιλτράρισμα. Παρακάτω θα αναφερθούμε στις δυνατότητες που προσφέρει, καθώς επίσης και στην εκτενή βάση δεδομένων του, η οποία όμως είναι επιπρόσθετη στο βασικό πακέτο.

### 3.2.2.1 Βασικές Δυνατότητες

Ο MIMEsweeper for Web είναι ένας full caching security web proxy server.

- Εύκολος τρόπος αναβάθμισής του μέσα στο δίκτυο. Μέχρι και τέσσερις servers μπορούν να λειτουργήσουν σε παράταξη με τέτοιο τρόπο ώστε να υπάρχει ισορροπημένη κατανομή του φόρτου εργασίας, αυξάνοντας γρήγορα και χωρίς μεγάλο κόστος τον αριθμό των χρηστών που μπορούν να εξυπηρετηθούν.
- Αυξημένη επίδοση ανά server έτσι ώστε καθένας τους να μπορεί να υποστηρίξει περίπου 2000 χρήστες επιβάλλοντας τους μια ολοκληρωμένη πολιτική ελέγχου, η οποία περιλαμβάνει προστασία από κακόβουλο λογισμικό, λεξική ανάλυση, μπλοκάρισμα αρχείων και φιλτράρισμα με βάση URL.
- Μεγάλο μέγεθος της cache που φτάνει τα 4Gb, αφαιρώντας έτσι την ανάγκη χρήσης προϊόντων caching από τρίτους κατασκευαστές. Επίσης, αυξάνει την επίδοση του δικτύου παρέχοντας άμεσες αποκρίσεις από την cache.
- Η διαχείριση της πολιτικής για όλους τους servers στην παράταξη μπορεί να γίνει κεντρικά, καθώς όλο το σύστημα θεωρείται ένα, όσον αφορά τον ορισμό των πολιτικών. Η διεπαφή διαχείρισης είναι απλή και παρόμοια με αυτή άλλων προϊόντων της Clearswift, βοηθώντας στη κατανόηση και την εκπαίδευση, αν έχουν χρησιμοποιηθεί και άλλα προϊόντα του ίδιου κατασκευαστή.
- Εντοπισμός και μπλοκάρισμα ύποπτων και πιθανών κακόβουλων scripts επιτρέποντας με αυτό τον τρόπο την χρήση σελίδων με script το οποίο κρίνεται ασφαλές.
- Επιτρέπει τον ορισμό πολιτικής ελέγχου με βάση την ήδη υπάρχουσα δομή κατηγοριοποίησης χρηστών είτε χρησιμοποιούνται LDAP, NT, αρχεία κειμένου ή IP διευθύνσεις. Έτσι, αυτή μπορεί να οριστεί είτε ανά χρήστη, είτε ανά ομάδες χρηστών.
- Εντοπισμός των streaming media και περιορισμός τους, έτσι ώστε κανένα να μην περνάει χωρίς έλεγχο. Επίσης, επιτυγχάνεται αποδοτικότερη κατανομή του bandwidth, έλεγχός τους ανάλογα με το format τους και έλεγχος ως προς το ποιος είναι ο παραλήπτης τους.
- Έλεγχος του περιεχομένου είτε έχει φορά από το διαδίκτυο προς το δίκτυό μας, είτε από το δίκτυό μας προς τα διαδίκτυο. Με αυτό τον τρόπο αποφεύγεται το download άχρηστων ή επιβλαβών πληροφοριών / αρχείων και το upload πληροφοριών / αρχείων που δεν θα έπρεπε να φύγουν από το δίκτυό μας, γιατί μπορεί να περιέχουν ευαίσθητες πληροφορίες.

- Όλοι οι τύποι συμπιεσμένων αρχείων, όπως zip, πρώτα αποσυμπιέζονται, έτσι ώστε ο τύπος των αρχικών / πηγαίων αρχείων να είναι ξεκάθαρος. και μετά ελέγχονται.
- Ο έλεγχος της πληροφορίας που κινείται από και προς το διαδίκτυο επεκτείνεται και στα e-mail τύπου web όπως hotmail, yahoo κ.α., αποκλείοντας με αυτό τον τρόπο πιθανές απειλές που προέρχονται από τη χρήση τους.
- Ο MIMEsweeper αναγνωρίζει τα δεδομένα που γίνονται download και στη συνέχεια καλεί το αντιβιοτικό, με το οποίο είναι ενσωματωμένο για να γίνει έλεγχος για κακόβουλο λογισμικό.
- Ο MIMEsweeper είναι εντελώς αφοσιωμένος στον έλεγχο της κίνησης από HTTP και browser FTP.
- Ο έλεγχος του τύπου του αρχείου δεν γίνεται με βάση την επέκτασή του, αλλά με βάση δυαδικών «αποτυπωμάτων». Με αυτό τον τρόπο δεν μπορεί να ξεγελαστεί απλά με την αλλαγή της επέκτασης. Το πρόγραμμα έχει μια λίστα με τύπους αρχείων, αλλά δίνει τη δυνατότητα στους διαχειριστές να ορίσουν και άλλους τύπους με βάση αυτό το μηχανισμό.

#### 3.2.2.2 Βασικές απαιτήσεις

**Ελάχιστο Υλικό**

- Pentium III 1000Mhz (προτείνεται διπλός επεξεργαστής)
- 1Gb RAM
- 1Gb χώρο στον σκληρό δίσκο (μέχρι και 4 Gb για cache)

**Λογισμικό**

- Microsoft Windows 2000 (Server ή advanced Server) με Service Pack 4
- TCP/IP network protocol
- Internet Explorer 6.0 (SP1)

#### 3.2.2.3 Web URL Filter

Το URL filter είναι ένα επιπρόσθετο εργαλείο του MIMEsweeper for Web. Πρόκειται για τη βάση δεδομένων του που αποτελείται από URL, τα οποία είναι ταξινομημένα σε κατηγορίες και τα οποία μπορούμε να χρησιμοποιήσουμε για να δημιουργήσουμε μια πιο ολοκληρωμένη πολιτική πρόσβασης στον παγκόσμιο ιστό για το δίκτυό μας. Η βάση αποτελείται συνολικά από 6.3 εκατομμύρια δικτυακούς τόπους, οι οποίοι αντιστοιχούν σε παραπάνω από 1 δισεκατομμύριο ιστοσελίδες. Η κατηγοριοποίηση των δικτυακών τόπων γίνεται σε 40 κατηγορίες και 130 υποκατηγορίες λαμβάνοντας υπόψη και το domain, αλλά και την σελίδα που ανήκει σε κάποιο domain. Τα sites προέρχονται από παραπάνω από 200 χώρες και καλύπτουν τουλάχιστον 65 διαφορετικές γλώσσες. Η βάση ενημερώνεται καθημερινά από μια ομάδα 40 επαγγελματιών χρησιμοποιώντας αυτοματοποιημένα εργαλεία, καθώς και προτάσεις από τους πελάτες, οι οποίοι μπορούν να καταθέσουν τη σελίδα που επιθυμούν προς εξέταση ή αλλαγή της κατηγορίας της από την ιστοσελίδα του MIMEsweeper (http://www.clearswift.com/products/msw/msw_web/sitecheck.aspx). Υπολογίζεται ότι γύρω στα 35000 URL προσθέτονται σε εβδομαδιαία βάση, ενώ παλιότερα URL επανελέγχονται.

Η ρύθμιση της πολιτικής μπορεί να είναι αρκετά ελαστική δίνοντας τη δυνατότητα ρύθμισής της με βάση τη διάρκεια πρόσβασης στο διαδίκτυο, ή το μέγεθος των αρχείων για download, ή ακόμη με βάση συγκεκριμένες ώρες της ημέρας (π.χ. μετά τις ώρες εργασίας η πρόσβαση να είναι ελεύθερη στα περισσότερα sites).

Οι 40 βασικές κατηγορίες είναι οι ακόλουθες: ενήλικα / σεξουαλικά θέματα, διαφημίσεις, τέχνες και διασκέδαση, chat, υπολογιστές και Internet, εγκληματικές ικανότητες, ναρκωτικά, αλκοόλ και ταμπάκο, μόρφωση, οικονομικά και επενδύσεις, φαγητό και πότο, τζόγος, παιχνίδια, hacking, μίσος, υγεία και φάρμακα, χόμπι, υπηρεσίες hosting, αναζήτηση εργασίας και καριέρα, τρόπος ζωής και κουλτούρα, οχήματα, νέα, προσωπικά και ραντεβού, φωτογραφίες, ακίνητα, απομακρυσμένοι proxies, σεξουαλική επιμόρφωση, μηχανές αναζήτησης, ψώνια, αθλητικά, streaming media, ταξίδια, forums, βία / προσβλητικά, όπλα, web-based e-mail.

Η πλήρης λίστα μπορεί να βρεθεί στο http://www.clearswift.com/products/msw/msw_web/URLfilter.aspx#.

### 3.2.2.4 Δυνατότητες ορισμού πολιτικών ελέγχου

Ανάλογα με τις αρμοδιότητες κάθε υπαλλήλου ή τμήματος ενός οργανισμού καθορίζεται και η ανάγκη του εκάστοτε υπαλλήλου ή τμήματος για πρόσβαση στον παγκόσμιο ιστό. Έτσι, και οι πολιτικές ελέγχου της πρόσβασης πρέπει να είναι ευέλικτες ώστε να μπορούν να προσαρμοστούν στις πολυάριθμες απαιτήσεις που παρουσιάζονται. Παρακάτω παρουσιάζονται οι βασικότεροι τρόποι με τους οποίους το MIMEsweeper for Web το πετυχαίνει αυτό.

- **Φάκελοι σεναρίων**: Οι διαχειριστές του συστήματος μπορούν να δημιουργήσουν αυτούς τους φακέλους και να ορίσουν ρυθμίσεις ασφαλείας για ομάδες χρηστών.
- **Χρόνος πρόσβασης**: Επιτρέπεται ο ορισμός πολιτικών που ισχύουν σε συγκεκριμένες ώρες της ημέρας ή της εβδομάδας. Έτσι, μπορεί μετά τις ώρες του γραφείου κάποιος να έχει πρόσβαση σε περισσότερα από συνηθισμένα URL, ενώ παράλληλα οι υπόλοιπες πολιτικές που διασφαλίζουν την ασφάλεια του δικτύου να ισχύουν χωρίς να περιορίζονται από χρονικά πλαίσια.
- **Ζώνες URL**: Μπορούν να οριστούν ομάδες από URL για να προσπερνάνε την ανάλυση περιεχομένου ή για γρήγορη παράδοση περιεχομένου των ιστοσελίδων που θεωρείται έμπιστο.
- **Κατηγορίες ιστοσελίδων**: Όλες οι ιστοσελίδες είναι χωρισμένες σε κατηγορίες οι οποίες ταξινομούνται βάση κάποιων τεχνικών, όπως ανάλυση κειμένου, PICS και λίστες από URL(βάση δεδομένων).
- **Κληρονομικότητα πολιτικών**: Οι πολιτικές είναι οργανωμένες με ιεραρχική δομή, έτσι ώστε οι υπάλληλοι στα χαμηλότερα επίπεδα μέσα σε ένα οργανισμό να μπορούν να κληρονομήσουν τις πολιτικές που έχουν οριστεί για αυτούς στα υψηλότερα. Εναλλακτικά, όταν μια πολιτική διέπει όλον τον οργανισμό να μπορεί να παρακαμφθεί ανάλογα με τις απαιτήσεις ενός τμήματος ή υπαλλήλου.
- **Λίστες χρηστών**: Ο MIMEsweeper for Web εκμεταλλεύεται την ήδη υπάρχουσα δομή χρηστών, είτε αυτή βασίζεται σε αρχεία κειμένου, LDAP, είτε σε καταλόγους χρηστών Windows NT/2000 για την αυθεντικοποίηση τους, τον καθορισμό πολιτικών για συγκεκριμένο χρήστη, στατιστικά και αναφορές.

### 3.2.2.5 MIMEsweeper for Web Reporting

Η σύνταξη ολοκληρωμένων αναφορών είναι ένας από τους σημαντικότερους τομείς αυτών των προγραμμάτων. Το Websense είδαμε προηγουμένως ότι διαθέτει έναν αρκετά εξελιγμένο μηχανισμό. Τα στατιστικά είναι μια γλώσσα, η οποία ξεπερνάει τα εμπόδια που παρουσιάζονται από την έλλειψη τεχνογνωσίας από κάποια μέλη ενός οργανισμού κάνοντας

έτσι ακόμη πιο σημαντική, όχι απλά την κατασκευή αναφορών, αλλά και την παρουσίασή τους με τέτοιο τρόπο ώστε να είναι φιλικές προς τον χρήστη.

- **Δυνατότητες δημιουργίας γραφικών αναφορών για εξέταση**: Ο MIMEsweeper for Web περιλαμβάνει ολοκληρωμένους μηχανισμούς αναφορών οι οποίοι ενσωματώνονται με SQL server. Διαθέτει μια προκατασκευασμένη ομάδα γραφικών αναφορών οι οποίες βασίζονται σε δεδομένα που έχει συλλέξει ο MIMEsweeper και στις οποίες μπορεί ο διαχειριστής του συστήματος να έχει πρόσβαση από οποιοδήποτε μηχάνημα στο δίκτυο μέσω ενός web browser. Αυτές οι αναφορές μπορούν εύκολα να παραμετροποιηθούν ανάλογα με τις ανάγκες μας. Αναλυτικά, δίνονται δυνατότητες για:
  - Ακριβή ανάλυση της χρήσης του διαδικτύου στον οργανισμό
  - Εντοπισμό των ιστοσελίδων που δέχονται τις περισσότερες επισκέψεις και από ποιον.
  - Πλήρεις αναφορές όλης της κίνησης από και προς το διαδίκτυο
  - Εντοπισμό ωρών αυξημένης χρήσης του διαδικτύου κατά την διάρκεια της ημέρας.
  - Παρακολούθηση του μηχανισμού εντοπισμού πιθανών απειλών με βάση την ιστοσελίδα, τον χρήστη και τη χρονική περίοδο.
- **Παρακολούθηση σε πραγματικό χρόνο**: Δυνατότητα παραγωγής στατιστικών που δίνουν απαντήσεις στον αριθμό των χρηστών που είναι ενωμένοι και στον αριθμό των παράλληλων συνδέσεων προς το διαδίκτυο που έχουν δημιουργηθεί. Τα δεδομένα που συλλέγονται μπορούν στη συνέχεια να περαστούν στο Performance Monitor για τη δημιουργία γραφικών αναφορών π.χ. της χρήσης της cache.

***Επιπλέον απαιτήσεις:***

- Windows 2000 Server με Service Pack 4
- SQL 2000 (ή MSDE 2000 παρέχεται με το CD) με Service Pack 3
- Microsoft IIS v5 (ελάχιστα απαιτούμενα συστατικά: common files, IIS snap-in, www server)
- MDAC 2.6
- Microsoft .Net Framework 1.1
- Microsoft Message Queuing Services (MSMQ)

### 3.2.2.6 Δυνατότητες διαχείρισης

Εδώ παρουσιάζονται δυο βασικές δυνατότητες διαχείρισης του MIMEsweeper for Web.

- Η διεπαφή του MIMEsweeper for Web ενσωματώνεται με την Microsoft Management Console. Με αυτό τον τρόπο είναι εύκολη η διαχείρισή του, καθώς το MMC χρησιμοποιείται από πολλούς οργανισμούς για τη διαχείριση των πληροφοριακών συστημάτων τους.
- Γεγονότα ασφαλείας μπορούν να ρυθμιστούν να ενεργοποιούν alerts μέσω e-mail, Windows NT alerts ή σε μορφή SNMP (Simple Network Management Protocol) όπου δρομολογούνται σε ένα πακέτο διαχείρισης όπως HP Openview.

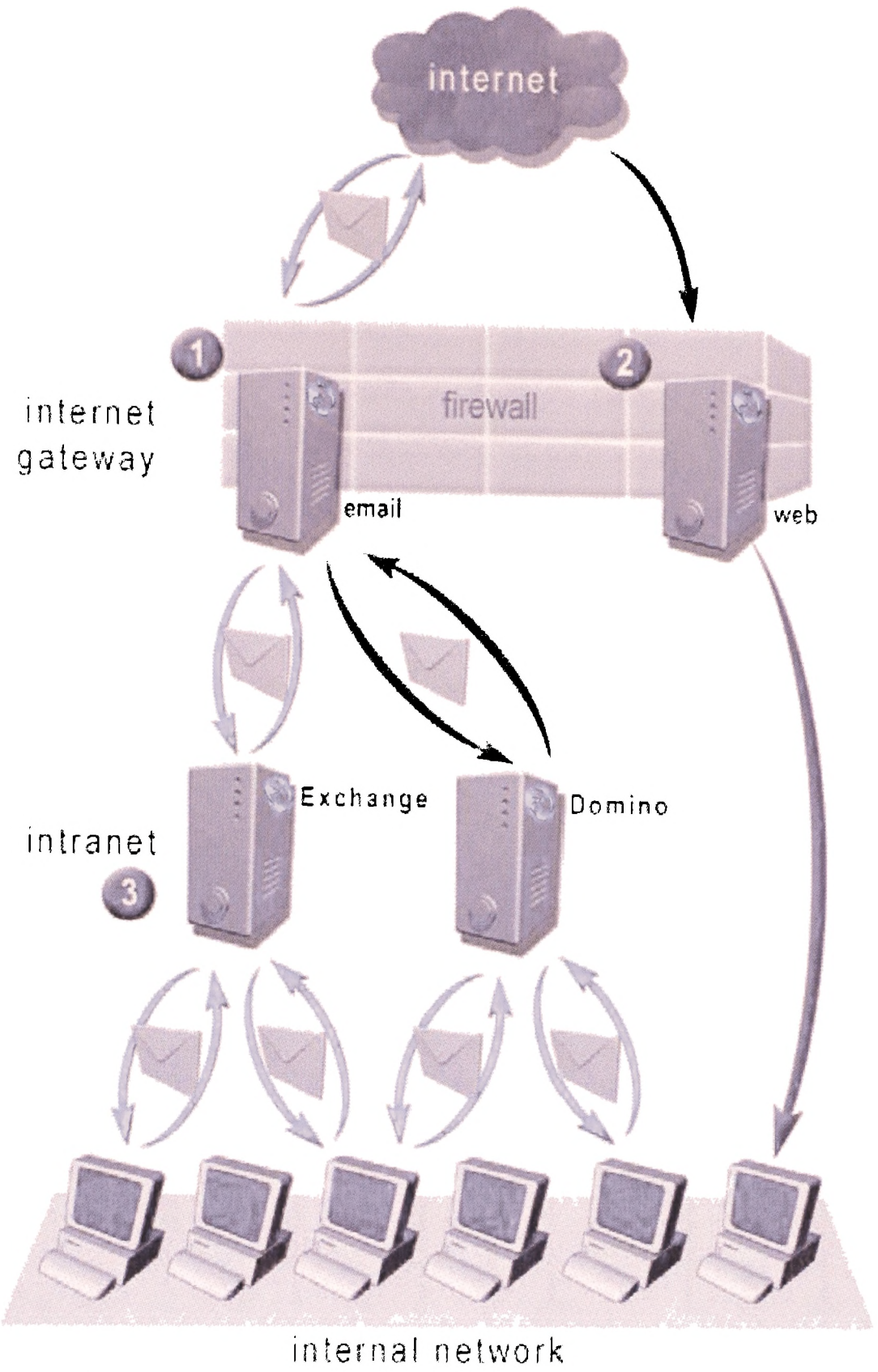
### 3.2.2.7 Η συνολική δομή

Για την ολοκληρωμένη προστασία του δικτύου ενός οργανισμού η Clearswift διαθέτει μια σειρά προϊόντων. Αν και αυτά τα προϊόντα δεν είναι επιπλέον συστατικά του

MIMEsweeper for Web, αλλά ανεξάρτητα πακέτα, η συνολική τους χρήση σε ένα δίκτυο μπορεί να αποτελέσει μια από τις αποτελεσματικότερες λύσεις για όλα τα πιθανά προβλήματα που προκύπτουν από την ένταξη του Internet στον εργατικό τομέα / χώρο. Ακολουθούν ένας πίνακας των προϊόντων και μια σχηματική δομή της ολοκληρωμένης λύσης MIMEsweeper.

Πίνακας 1: Τα υπόλοιπα πακέτα τις Clearswift

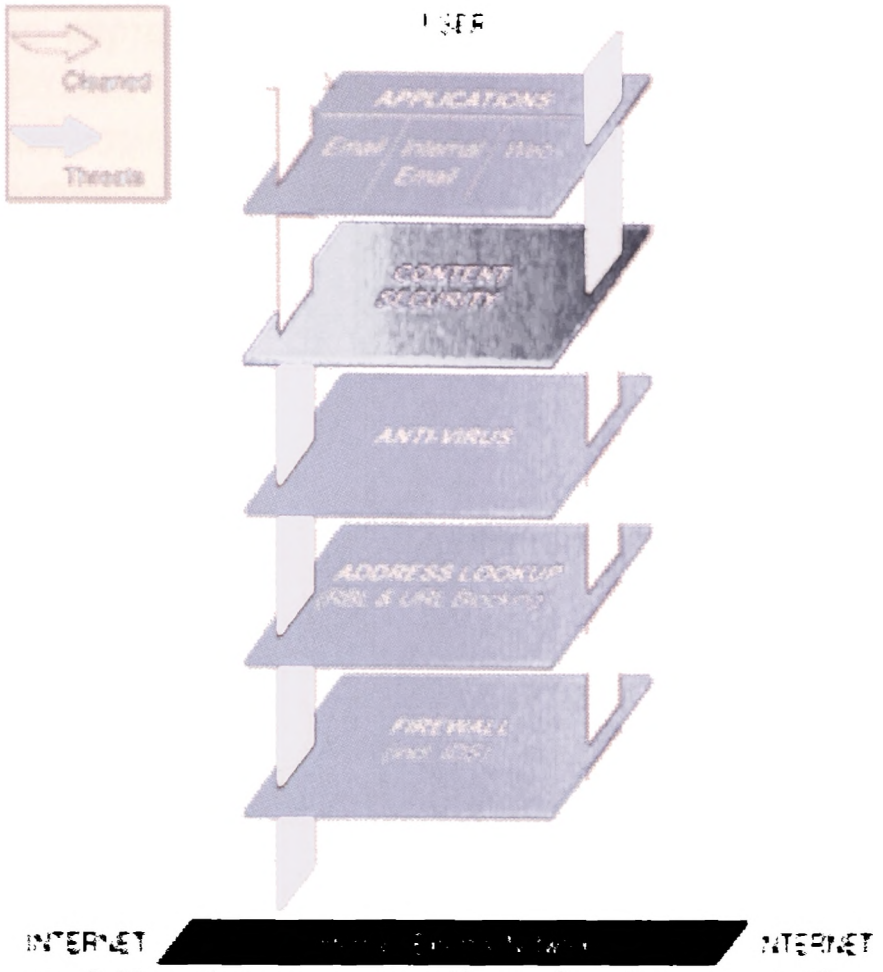
| Εφαρμογή | Περιγραφή |
|---|---|
| MAILsweeper | Παρέχει ασφάλεια μέσω ανάλυσης του περιεχομένου και στα email με κατευθύνσεις από και προς το διαδίκτυο. |
| MAILsweeper for Exchange ή MAILsweeper for Domino | Ότι και ο MAILsweeper αλλά για email που κινούνται στο εσωτερικό δίκτυο και χρησιμοποιούν αντίστοιχα Microsoft Exchange ή Lotus Domino. |
| MIMEsweeper SECRETsweeper | Είναι ένα gateway κρυπτογράφησης / αποκρυπτογράφησης και ψηφιακών υπογραφών. Έτσι αποφεύγεται να προσπερνάνε την πολιτική ασφαλείας δεδομένα που είναι κρυπτογραφημένα. |
| MIMEsweeper IMAGEmanager | Επιτρέπει την επιβολή πολιτικών για εικόνες που μεταφέρονται μέσω email. |
| MIMEsweeper ARCHIVEmanager | Πρόκειται για ένα, βασισμένο σε πολιτικές, λογισμικό αρχειοθέτησης των email με δυνατότητες έξυπνης εύρεσης και ανάκτησής τους για νομικές και ρυθμιστικές συμμορφώσεις. |




εικ. 1 Η πλήρης δομή του MIMEsweeper: (1) MAILsweeper, (2) MIMEsweeper for Web, (3) MAILsweeper for Domino και MAILsweeper for Exchange

### 3.2.3 Αρχιτεκτονική και τρόπος λειτουργίας

Ο MIMEsweeper for Web προσπαθεί να συμπληρώσει τα κενά στην ασφάλεια ενός πληροφοριακού συστήματος προστατεύοντάς το από απειλές μέσω HTTP και FTP. Γι' αυτό το λόγο χρησιμοποιεί μια προσέγγιση με στρώματα «άμυνας» τοποθετώντας τον εαυτό του σαν το πρώτο στάδιο ελέγχου. Με αυτό τον τρόπο συμπληρώνει και ολοκληρώνει την προστασία που παρέχουν οι firewalls, τα συστήματα ανίχνευσης εισβολών και τα αντιβιοτικά. Τέλος, όπως αναφέραμε και παραπάνω ο έλεγχος δεν περιορίζεται μόνο σε δεδομένα από το διαδίκτυο, αλλά και σε δεδομένα προς αυτό, προστατεύοντας έτσι και από απειλές, όπως π.χ. η αποκάλυψη εμπιστευτικών δεδομένων σε τρίτους με την αποστολή τους.



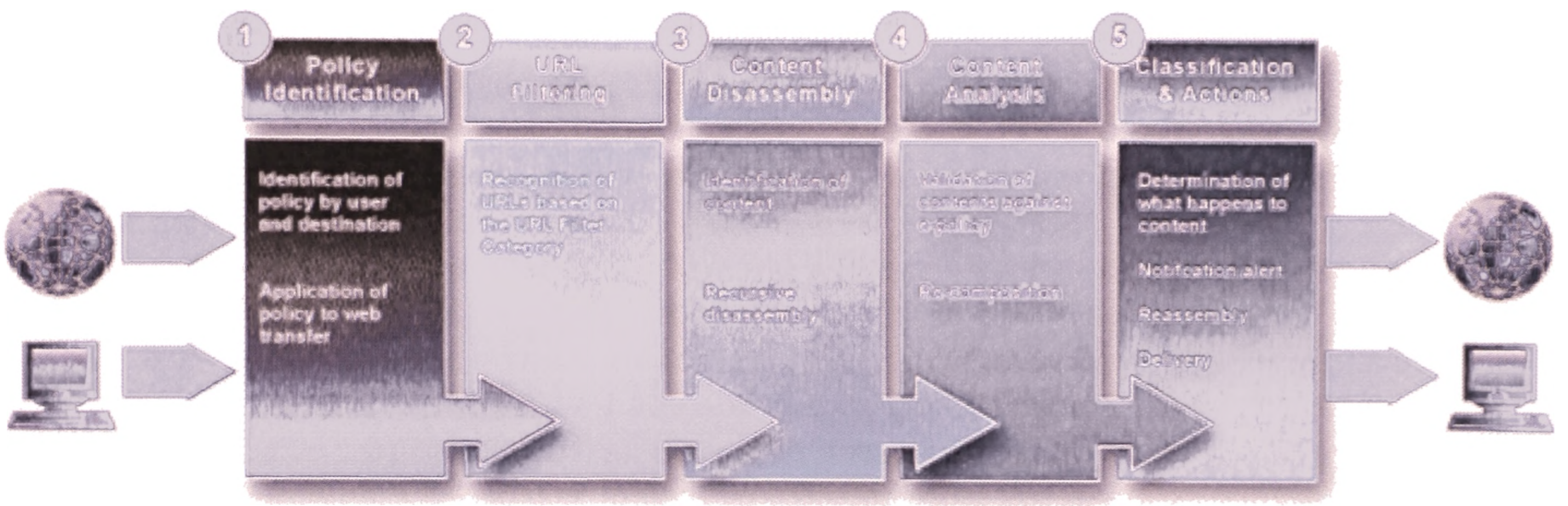
εικ. 2 Προσέγγιση της ασφάλειας δικτύου σε επίπεδα.

### 3.2.3.1 Ο τρόπος λειτουργίας

Ο MIMEsweeper for Web είναι ένας full caching security web proxy server ο οποίος τρέχει σε Windows 2000 server ή Advanced server. Όλα τα δεδομένα τα οποία περνάνε από την gateway με το διαδίκτυο διαχειρίζονται από τον MIMEsweeper σε 5 στάδια.

1. **Αναγνώριση πολιτικής**: Όταν ένας χρήστης ξεκινάει την αναμετάδοση δεδομένων ο MIMEsweeper for Web πρώτα τον αναγνωρίζει και εφαρμόζει την πολική ασφαλείας που του αναλογεί προσδίδοντάς του με αυτό τον τρόπο τα δικαιώματα πρόσβασής που του αντιστοιχούν. Ο MIMEsweeper for Web συνεργάζεται με LDAP, μεθόδους αυθεντικοποίησης των Windows ή μπορεί να εφαρμόσει την πολιτική βασισμένος στην IP διεύθυνση του πελάτη.
2. **Φιλτράρισμα URL**: Γίνεται σύγκριση του URL που ζητήθηκε με τη βάση δεδομένων του MIMEsweeper για να εξακριβωθεί αν ανήκει σε μια από τις κατηγορίες. Αν ναι, τότε ελέγχεται αν επιτρέπεται η πρόσβαση σε αυτή τη σελίδα. Αν δεν επιτρέπεται σε αυτόν το χρήστη η πρόσβαση, τότε η σελίδα μπλοκάρεται. Αν επιτρέπεται, τότε προχωράμε στο επόμενο στάδιο.
3. **Αποσυναρμολόγηση περιεχομένου**: Τα περιεχόμενα της σελίδας χωρίζονται σε βασικά συστατικά, όπως οι ίδιες οι σελίδες, συμπιεσμένα αρχεία, εκτελέσιμα αρχεία, αρχεία κειμένου, εικόνα, ήχος και video και αναλύονται για να αποκαλυφθεί η βασική τους δομή όπως π.χ. ένα ActiveX αντικείμενο. Πρόκειται για μια αναδρομική διαδικασία, η οποία φτάνει σε βάθος μέχρι και 50 επιπέδων. Επίσης, όπως αναφέραμε παραπάνω η αναγνώριση των αρχείων γίνεται με βάση την αρχιτεκτονική τους και όχι απλά από την επέκταση τους, δίνοντας έτσι τη δυνατότητα μπλοκαρίσματος οποιουδήποτε είδους αρχείου.
4. **Ανάλυση περιεχομένου**: Το περιεχόμενο του HTTP ή browser FTP αναλύεται και εκτιμάται ανάλογα με την πολιτική που αντιστοιχεί στον χρήστη που έχει ξεκινήσει την αναμετάδοση των δεδομένων. Ο MIMEsweeper for Web ξεχωρίζει συγκεκριμένους τύπους αρχείων, αναλύει το κείμενο για πιθανές απειλές ασφαλείας και αναγνωρίζει πιθανό επικίνδυνο εκτελέσιμο κώδικα. Επίσης, σε συνεργασία με το αντιβιοτικό που χρησιμοποιείται ελέγχει για ιούς.

5. **Παράδοση**: Αφού το περιεχόμενο έχει πλήρως αναλυθεί ο MIMEsweeper for Web το ανασυνθέτει και επιβάλλει την ανάλογη πολιτική σε αυτό, αφού έχουν πρώτα καθαριστεί πιθανά βλαβερά ή μολυσμένα αρχεία / δεδομένα. Αναλόγως, παραδίδει τη σελίδα στον χρήστη ή μπλοκάρει εντελώς την πρόσβαση σε αυτή. Ένα μήνυμα ή μια HTML σελίδα με δυνατότητες παραμετροποίησης και για τα δυο ενημερώνει τον χρήστη πότε μια σελίδα μπλοκάρεται και αν θέλουμε, τους λόγους για τους οποίους μπλοκάρεται και την ισχύουσα πολιτική. Ενημέρωση για το συμβάν μπορεί να σταλεί με email σε όσους ενδιαφέρονται.

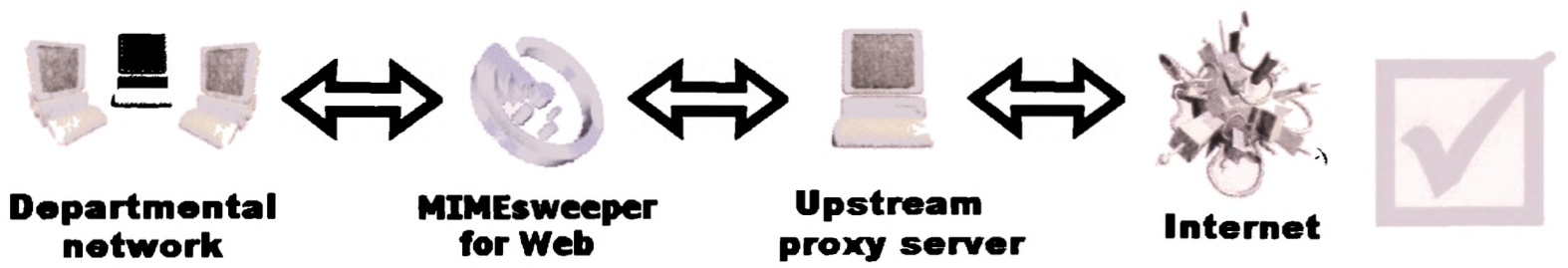



εικ. 3 Τα 5 στάδια της λειτουργίας του MIMEsweeper for Web

### 3.2.3.2 Proxy servers σε αλυσίδα

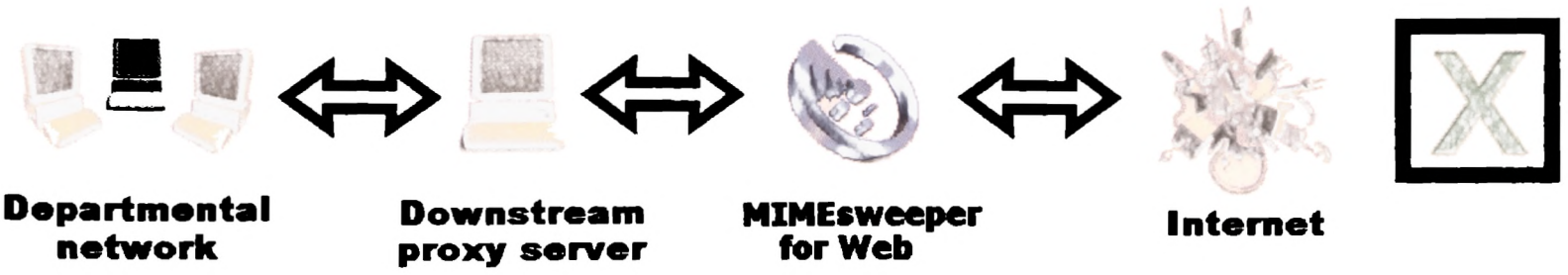
Όπως έχουμε αναφέρει και προηγουμένως το MIMEsweeper for Web είναι ένας proxy server, ο οποίος μπορεί άνετα να παίξει τον ρόλο του βασικού proxy sever του δικτύου. Μπορεί όμως κάποιος οργανισμός να διαθέτει ήδη proxy server για αυθεντικοποίηση χρηστών και για αποθήκευση των ιστοσελίδων που επισκεπτόμαστε συχνά. Έτσι μπορεί να γεννηθεί η ανάγκη να συνδέσουμε σε αλυσίδα τους δυο proxy servers.

Αν πρόκειται για upstream, δηλαδή για κάποιο proxy server που παίζει τον ρόλο του firewall η σύνδεση γίνεται χωρίς πρόβλημα, αρκεί ο MIMEsweeper να είναι εγκατεστημένος μέσα από το firewall.




εικ. 4 Σύνδεση με upstream proxy server

Η σύνδεση με downstream proxy server δεν προτείνεται, γιατί παρουσιάζει προβλήματα. Σε αυτή την περίπτωση οι αιτήσεις μπορούν να εξυπηρετηθούν από την cache του proxy προσπερνώντας την πολιτική ελέγχού για το περιεχομένου. Έτσι, μια σελίδα που έχει περάσει γιατί είναι αποδεκτή λόγω της πολιτικής που ισχύει για ένα χρήστη, αυτομάτως γίνεται προσβάσιμη και σε κάποιον που δεν θα είχε ουσιαστικά το δικαίωμα να την προσπελάσει. Αν πρέπει να χρησιμοποιήσουμε τον downstream proxy server και θέλουμε να επιβάλουμε πολιτική ανά χρήστη, τότε πρέπει να απενεργοποιήσουμε τη δυνατότητα του caching από τον proxy.




εικ. 5 Σύνδεση με downstream proxy server

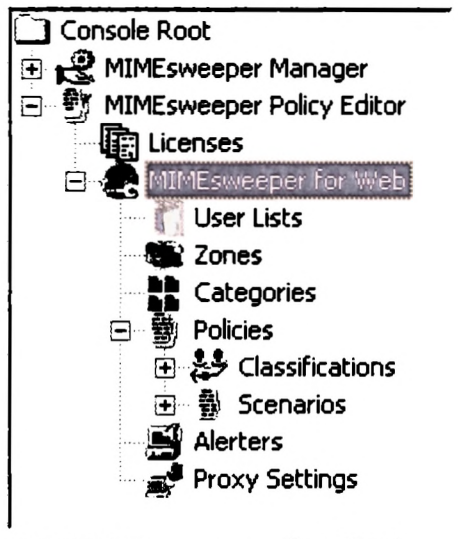
### 3.2.3.3 Βασικά συστατικά

- **MIMEsweeper for Web user interface**

Η διεπαφή χειρισμού βρίσκεται στη μορφή δυο επιπρόσθετων εργαλείων για το MMC (Microsoft Management Console).

- MIMEsweeper Manager: Χρησιμοποιείται για τον έλεγχο των υπηρεσιών Web του MIMEsweeper και για την εμφάνιση των αναφορών.
- MIMEsweeper Policy Editor: Παρέχει την δυνατότητα προσδιορισμού της πολιτικής για τον έλεγχο της πρόσβασης και του περιεχομένου στο διαδίκτυο.

Και τα δυο παραπάνω εργαλεία εγκαθίστανται στην κεντρική μηχανή του MIMEsweeper for Web. Ο Manager μπορεί να εγκατασταθεί και απομακρυσμένα σε ένα ή και παραπάνω μηχανήματα του δικτύου (Remote Management).




εικ. 6 MIMEsweeper for Web user interface

- **MIMEsweeper for Web services**

Οι υπηρεσίες του MIMEsweeper τρέχουν ουσιαστικά σαν 3 ξεχωριστές υπηρεσίες Windows.

- Clearswift Web Policy Engine: Ουσιαστικά αυτή η υπηρεσία είναι ο WWW proxy server συμπεριλαμβάνοντας και την μηχανή ασφαλείας του περιεχομένου. Υποστηρίζει τα πρωτόκολλα HTTP 1.0 και 1.1, αλλά και browser FTP. Μπορεί να λειτουργήσει και σε απλά, αλλά και πολύπλοκα περιβάλλοντα που περιλαμβάνουν πολλούς proxy σε αλυσίδα.
- Clearswift Consolidation Service: Συγκεντρώνει όλα τα δεδομένα που έχουν ελεγχθεί από την Policy Engine και αν επιθυμούμε τα μεταφέρει στο Report Center.
- Clearswift Cache Management Service: Εκτελεί καθαρισμό της cache, όποτε χρειάζεται, παρατηρώντας τη χωρητικότητα των σκληρών δίσκων στις περιοχές της cache.Εάν ο διαθέσιμος χώρος δεν είναι αρκετός, ώστε η cache να φτάσει το μέγιστο μέγεθος στο οποίο έχει ρυθμιστεί, τότε ενημερώνει τον διαχειριστή.

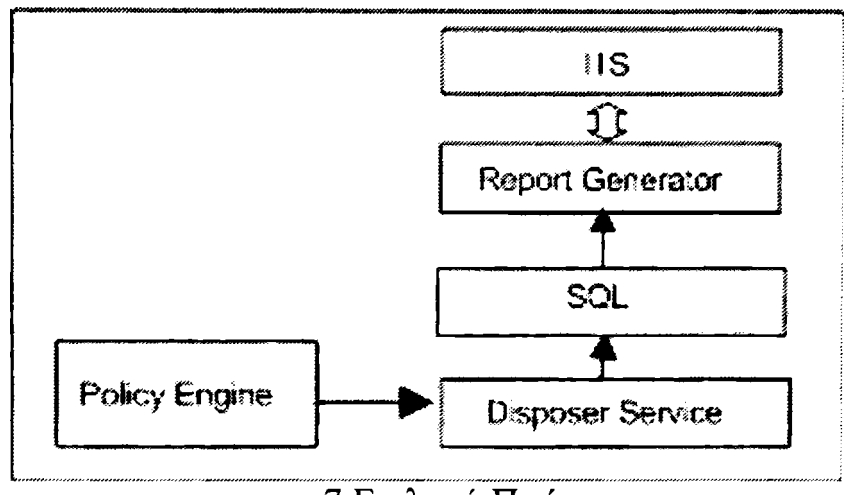
- **MIMEsweeper for Web Report Center**

Το Report Center αποθηκεύει αναφορές για αναζήτηση, εύρεση και εμφάνιση σχετικά με ελεγμένα δεδομένα και τις παρουσιάζει σαν Web τύπου αναφορές διαχείρισης. Αποτελείται από δυο μέρη.

- Clearswift Disposer Service: Αυτή η υπηρεσία δέχεται ελεγμένα δεδομένα από την Consolidation Service και τα αποθηκεύει σε μια βάση δεδομένων σε SQL.
- Report Generator: Χρησιμοποιεί ένα IIS (Internet Information Services) Web Server για να δημιουργεί και να παρέχει αναφορές τύπου Web.

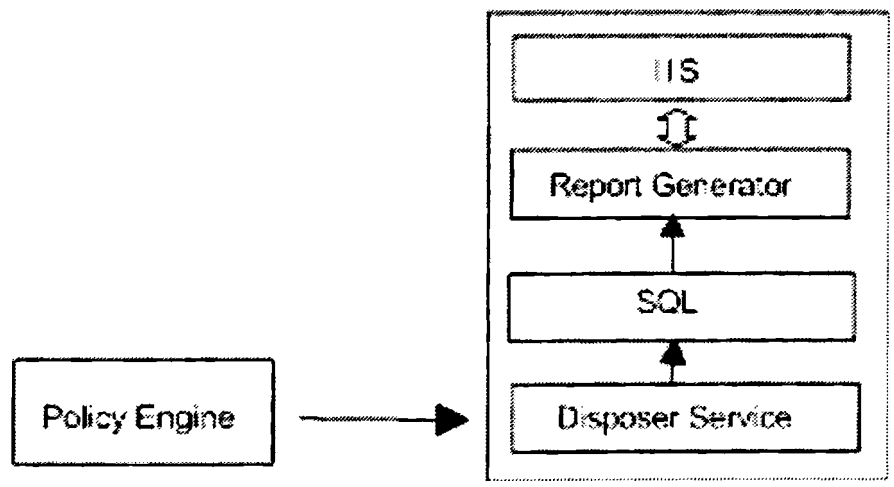
Η εγκατάσταση των υπηρεσιών του Report Center μέσα στο δίκτυο μπορεί να γίνει με ποικίλους τρόπους, ανάλογα με τις απαιτήσεις μας. Ουσιαστικά έχουμε 4 διαφορετικά συστατικά: την Policy Engine, τη βάση δεδομένων σε SQL, την Disposer Service και τον Report Generator σε IIS web server. Ακολουθούν οι 3 βασικοί τρόποι εγκατάστασής τους στο δίκτυο.

- Επιλογή Πρώτη: Όλα τα συστατικά βρίσκονται εγκατεστημένα στο ίδιο μηχάνημα με την Policy Engine.



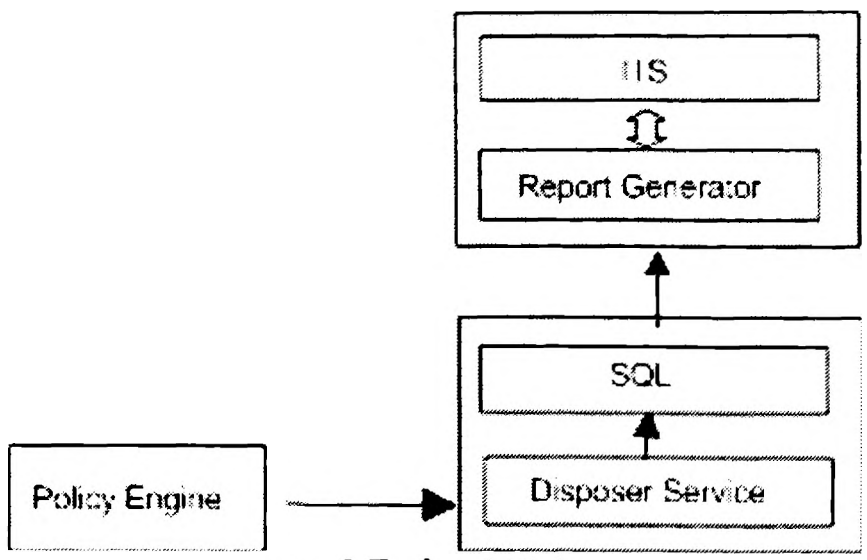
εικ. 7 Επιλογή Πρώτη

- Επιλογή Δεύτερη: Όλα τα συστατικά του Report Center εγκαθίστανται σε μηχάνημα ξεχωριστά από την Policy Engine. Αυτή η λύση είναι η ιδανική τις περισσότερες των περιπτώσεων.



εικ. 8 Επιλογή Δεύτερη

- Επιλογή Τρίτη: Εδώ συναντάμε σε διαφορετικά μηχανήματα εκτός από την Policy Engine, τον Report Generator και το Disposer Service. Συνήθως χρησιμοποιείται σαν λύση όταν ήδη υπάρχουν στο δίκτυο ξεχωριστοί SQL server και IIS server.



εικ. 9 Επιλογή Τρίτη

### 3.2.3.4 Μελέτη κατανεμημένης παράταξης MIMEsweeper for Web proxy servers στο δίκτυο

Αναφέραμε παραπάνω ότι το MIMEsweeper μπορεί να λειτουργήσει τοποθετώντας μέχρι και 4 servers του σε παράταξη, εξυπηρετώντας με αυτό τον τρόπο περισσότερους χρήστες και πετυχαίνοντας, με τη χρήση του πρωτοκόλλου CARP (Cache Array Routing Protocol), τη σωστή κατανομή του φόρτου εργασίας μεταξύ τους. Προτού προχωρήσουμε στον τρόπο παράταξης των servers στο δίκτυο θα αναφερθούμε στις απαιτήσεις σε αριθμό server ανά χρήστες.

Κάθε MIMEsweeper for Web server μπορεί να υποστηρίξει περίπου έως και 200 χρήστες που προσπαθούν συγχρόνως να επισκεφτούν ιστοσελίδες. Έχοντας αυτό σαν κανόνα ακολουθεί ο παρακάτω πίνακας.

Πίνακας 2: Απαιτήσεις # server ανά χρήστες

| Χρήστες που απαιτούν σελίδες συγχρόνως | # Servers |
|---|---|
| Μέχρι 200 | 1 |
| 201-400 | 2 |
| 401-600 | 3 |
| 601-800 | 4 |

Φυσικά, η παραπάνω είναι μια απλουστευμένη προσέγγιση όσον αφορά το ζήτημα των απαιτήσεων. Είναι λογικό να υποθέσουμε ότι μια αυξημένη κίνηση από τους χρήστες, σε συνδυασμό με μια πολύπλοκη πολιτική θα έχει υψηλότερες απαιτήσεις από τις καθορισμένες για συγκεκριμένο αριθμό χρηστών, ενώ για την αντίθετη περίπτωση χαμηλότερες.

Από εδώ και στο εξής την κατανεμημένη παράταξη των MIMEsweeper proxy servers, με τέτοιο τρόπο ώστε να υπάρχει ισορροπημένη κατανομή του φόρτου εργασίας, θα την καλούμε load balancing.

Το load balancing λειτουργεί με τους εξής βασικούς κανόνες:

- Κάθε μέλος της παράταξης είναι ένας ξεχωριστός proxy με τη δική του IP διεύθυνση.
- Ο συνολικός αριθμός των διευθύνσεων του διαδικτύου είναι ομοιόμορφα μοιρασμένος μεταξύ των μελών της παράταξης.
- Αν μια αίτηση από πελάτη φτάσει σε ένα μέλος της παράταξης το οποίο δεν είναι υπεύθυνο για την επεξεργασία των URL αιτήσεων, τότε προωθείται στο κατάλληλο μέλος.
- Το μέλος το οποίο είναι υπεύθυνο για την επεξεργασία της URL αίτησης θα δεχθεί και την απάντησή της από το διαδίκτυο και θα την ελέγξει ενάντια στις πολιτικές ασφαλείας.

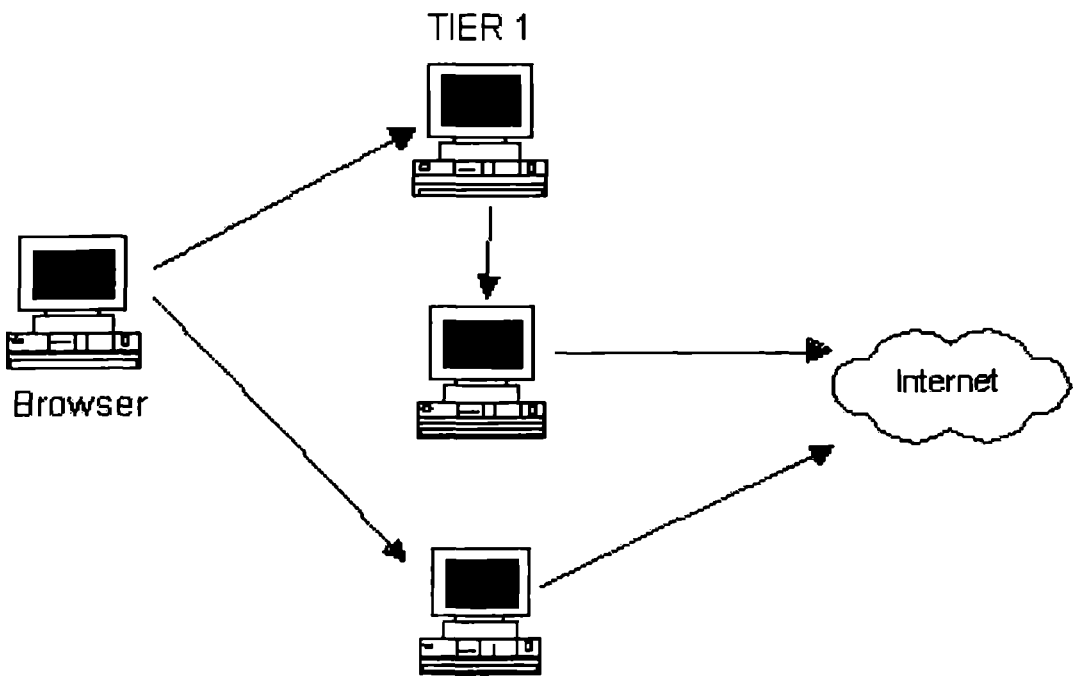
Μπορούν να χρησιμοποιηθούν PAC (Proxy Auto Configuration) scripts για να μειωθεί το πλήθος των μηνυμάτων που ανταλλάσσονται μεταξύ των μελών της παράταξης και την αποφυγή της «κυκλοφοριακής συμφόρησης» που δημιουργείται από τον ισορροπημένο διαμοιρασμό των αιτήσεων.

#### 3.2.3.4.1 Μέθοδοι εγκατάστασης στο δίκτυο

- Κατανεμημένη μέθοδος
- Ιεραρχική μέθοδος
- Εξωτερική / PAC script μέθοδος

**Κατανεμημένη Μέθοδος**

Αυτή η μέθοδος χρησιμοποιεί μια σειρά από μέχρι και τέσσερα μέλη μιας παράταξης που λειτουργούν πανομοιότυπα. Οποιοδήποτε μέλος μπορεί να δεχθεί μια αίτηση από ένα browser και να προχωρήσει σε αυθεντικοποίηση του χρήστη. Στη συνέχεια την προωθεί σε οποιοδήποτε μέλος είναι υπεύθυνο για την εξυπηρέτηση της αίτησης. Αν αυτό το μέλος είναι το ίδιο, τότε θα δεχθεί και την απάντηση της αίτησης από το διαδίκτυο και θα την ελέγξει ενάντια στις πολιτικές ασφαλείας, πριν επιστρέψει την απάντηση στον πελάτη. Για κάθε URL αντιστοιχεί συγκεκριμένο μέλος της παράταξης και μόνο αυτό μπορεί να αποθηκεύει δεδομένα (caching) από τη συγκεκριμένη σελίδα, αποφεύγοντας με αυτό τον τρόπο την δημιουργία διπλών εγγραφών.

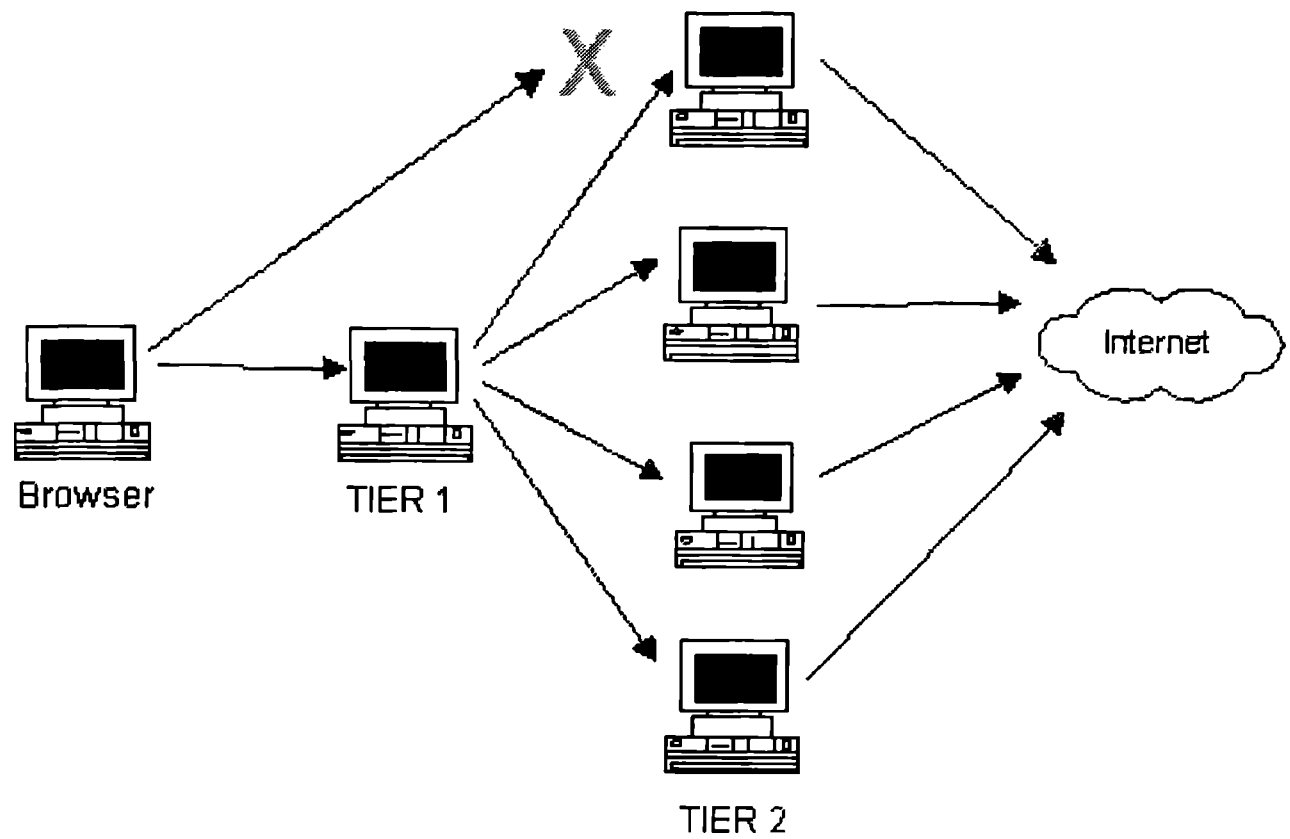



εικ. 10 Κατανεμημένη μέθοδος

**Ιεραρχική μέθοδος**

Αυτή μέθοδος είναι πιο κατάλληλη εάν η χρήση των PAC scripts δεν είναι δυνατή, όπως π.χ. στην περίπτωση που υπάρχει άλλος proxy server μεταξύ του browser και της παράταξης. Σε αυτή την περίπτωση χρησιμοποιούνται δύο σειρές από proxies που αποτελούνται από έως και 4 μέλη η κάθε μια. Τα μέλη μιας σειράς συμπεριφέρονται διαφορετικά από τα μέλη της άλλης. Οι αιτήσεις των πελατών καταλήγουν στην πρώτη σειρά. Τα μέλη της εκτελούν τη διαδικασία αυθεντικοποίησης του χρήστη, στη συνέχεια αποφασίζουν ποιο μέλος από τη δεύτερη σειρά είναι το κατάλληλο για να εξυπηρετήσει την αίτηση και τελικά την προωθούν σε αυτό. Το συγκεκριμένο μέλος της δεύτερης σειράς είναι υπεύθυνο για τον έλεγχο του περιεχομένου βάση της ισχύουσας πολιτικής για τον χρήστη. Με αυτό τον τρόπο, η πρώτη σειρά είναι υπεύθυνη για τη διαδικασία της αυθεντικοποίησης, ενώ η δεύτερη για τον έλεγχο. Έτσι, η πρώτη σειρά μοιράζει τις αιτήσεις στη δεύτερη χωρίς

τη χρήση των PAC scripts. Αν βέβαια η πρώτη σειρά αποτελείται από παραπάνω από ένα μέλος, τότε PAC scripts είναι απαραίτητα για τον διαμοιρασμό των αιτήσεων από τους browsers στην πρώτη σειρά μόνο.




εικ. 11 Ιεραρχική μέθοδος

**Εξωτερική / PAC script μέθοδος**

Αυτή η λύση εφαρμόζεται στην περίπτωση που χρησιμοποιείται λογισμικό load balancing από τρίτο κατασκευαστή όπως π.χ. Windows Load Balancing. Σε αυτήν τη μέθοδο κάθε μέλος της παράταξης έχει πλήρη ευθύνη για κάθε αίτηση που δέχεται και δεν προωθεί ποτέ τις αιτήσεις σε άλλα μέλη. Ουσιαστικά, γίνεται απενεργοποίηση του CARP. Οι πελάτες κάνουν χρήση των PAC script για τον διαμοιρασμό των αιτήσεων στα μέλη.

## 3.2.4 Αξιολόγηση / Συμπεράσματα

Ο MIMEsweeper for Web αποτελεί μια πάρα πολύ καλή λύση για Content Filtering και URL blocking σε οργανισμούς και επιχειρήσεις. Διαθέτει μια από τις πιο ολοκληρωμένες βάσεις δεδομένων URL με μηχανισμούς για να διατηρείται πάντα ενημερωμένη. Είναι πολύ εύκολη η εγκατάσταση του στο δίκτυο με χαμηλές απαιτήσεις σε υλικό και εξοπλισμό, ακόμη και για μεγάλο αριθμό χρηστών, έχοντας τη δυνατότητα να λειτουργήσει σαν φυσιολογικός proxy, αντικαθιστώντας έτσι την ανάγκη χρήσης ενός. Υποστηρίζεται από μια απλή, στη χρήση, διεπαφή και ένα ολοκληρωμένο μηχανισμό αναφορών και ενημέρωσης. Επίσης, διαθέτει μια μηχανή πολιτικής που επιτρέπει τη λεπτομερή παραμετροποίηση της. Από την άλλη μεριά, οι δυνατότητές του περιορίζονται κυρίως στο Content Filtering και URL blocking με ελάχιστα επιπρόσθετα εργαλεία για τη διευκόλυνση της διαχείρισης του δικτύου και την αύξηση της παραγωγικότητάς του. Τέλος, για να προσφέρει ολοκληρωμένη προστασία απαιτεί την ύπαρξη και των λοιπών πακέτων της Clearswift καθώς και τρίτων κατασκευαστών για απειλές που δεν προέρχονται από HTTP και browser FTP.

## 3.3 Net Nanny 5.0

Το Net Nanny είναι ένα προϊόν της BioNet Systems. Απευθύνεται κυρίως σε ενήλικες που θέλουν να παρακολουθήσουν, να ελέγξουν ή να περιορίσουν την πρόσβαση του υπολογιστή τους στο Internet. Αποτελεί μια από τις καλύτερες λύσεις για οικογενειακά περιβάλλοντα. Το προϊόν προσφέρεται, είτε σε μορφή πακέτου, είτε για download από την ιστοσελίδα της εταιρίας και ενεργοποιείται με τη χρήση κλειδιού. Η ίδια εταιρία προσφέρει μια σειρά παρόμοιων προϊόντων για τον έλεγχο των περισσότερων μορφών επικοινωνίας μέσω του Internet (mail, chat, IRC).

### 3.3.1 Γενικά Χαρακτηριστικά

- Είναι το πρώτο προϊόν του είδους του και κυκλοφόρησε τον Ιανουάριο του 1995. Από τότε βελτιώνεται με τη συνεργασία γονέων, συμβούλων παιδιών, δασκάλων / καθηγητών καθώς και του νόμου.
- Απευθύνεται σε κάθε χρήστη, άπειρο ή πεπειραμένο (poweruser) με μια πληθώρα επιλογών και ρυθμίσεων, εύκολες στην κατανόηση και εφαρμογή.
- Προστατεύει την ελευθερία του λόγου επιτρέποντας στους χρήστες του να έχουν πλήρη πρόσβαση στη βάση δεδομένων του από ιστοσελίδες, εφαρμογές και λέξεις κλειδιά (black/white lists).
- Προσφέρεται για χρήση σε περιβάλλοντα όπου πρόσβαση σε ένα υπολογιστικό σύστημα έχουν ενήλικες και ανήλικοι (όπως βιβλιοθήκες). Απενεργοποιείται εύκολα από κάποιον εξουσιοδοτημένο χρήστη και η μαύρη λίστα του είναι διαθέσιμη για ανάγνωση και παραμετροποίηση. Επίσης, αναφέρει ξεκάθαρα τα κριτήρια με τα οποία φιλτράρει τις ιστοσελίδες.
- Βοηθάει στη διατήρηση της ιδιωτικότητας προστατεύοντας ευαίσθητες πληροφορίες (πιστωτικές κάρτες, διευθύνσεις, κ.α.), μπλοκάρει pop διαφημίσεις και cookies.

### 3.3.2 Εγκατάσταση / Αρχική παραμετροποίηση

Η εγκατάσταση του προγράμματος είναι απλή και δεν διαφέρει καθόλου από την τυπική εγκατάσταση ενός προγράμματος για το λειτουργικό σύστημα των Windows. Μετά την αρχική εγκατάσταση γίνεται η αρχική παραμετροποίηση του προγράμματος και δίνεται η δυνατότητα στον διαχειριστή του Net Nanny να δημιουργήσει χρήστες και να ορίσει τον κωδικό του πρόσβασης στις ρυθμίσεις του προγράμματος. Όταν το πρόγραμμα ενεργοποιηθεί αυτό  το εικονίδιο είναι ορατό στο system tray.

### 3.3.3 Απαιτήσεις / Δυνατότητες

| **Απαιτήσεις Συστήματος** |
|---|
| Μνήμη: 32MB |
| Χώρος στον Δίσκο: 50MB |
| Internet Browsers που υποστηρίζονται: Internet Explorer, Netscape |
| Πλατφόρμες που υποστηρίζονται: Win 98/Me/Nt4/2000/XP |
| **Δυνατότητες Ασφαλείας** |
| Δυνατότητες Stealth |
| Παρεμπόδιση απεγκατάστασης |
| Αντίσταση σε αλλοίωση |
| Έλεγχος της πρόσβασης στο Internet ανά εφαρμογή |
| **Προστασία Περιεχομένου και Ιδιωτικότητας** |
| Μπλοκάρισμα Εμπιστευτικών Πληροφοριών |
| Μπλοκάρισμα Cookies |
| Μπλοκάρισμα popup και popunder διαφημίσεων |
| Μπλοκάρισμα διαδικτυακών παιχνιδιών |
| Μπλοκάρισμα προγραμμάτων ανταλλαγής αρχείων |
| Μπλοκάρισμα εφαρμογών συζητήσεων και ανταλλαγής μηνυμάτων |
| Δυνατότητα καθορισμού σε ποιες εφαρμογές να παρέχεται πρόσβαση |
| Φιλτράρισμα νέων, τροποποιημένων ή και δυναμικά παραγόμενων ιστοσελίδων |
| Φιλτράρισμα εισερχόμενων και εξερχόμενων e-mail |
| Μπλοκάρισμα IP διευθύνσεων |
| Μπλοκάρισμα μηχανών αναζήτησης |
| Πάντα ελεύθερη πρόσβαση σε συγκεκριμένες ιστοσελίδες |
| Φιλτράρισμα με βάση URL |
| Αυτόματη Αναβάθμιση των ACL (Access Control Lists) διαδικτυακά |
| Δυνατότητα να δούμε τα περιεχόμενα των ACL και να τα παραμετροποιήσουμε |
| Μπλοκάρισμα την πρόσβασης στο Internet βάση χρονικών περιόδων |
| Περιορισμός του Online χρόνου |
| **Ευκολία στην Χρήση, Αναφορές και Βοηθητικά Εργαλεία** |
| Wizards που καθοδηγούν τον χρήστη για εύκολη εγκατάσταση |
| Οδηγίες και παραδείγματα για να βοηθήσουν τους χρήστες σε βασικά ζητήματα |
| Υποστήριξη μέσω E-mail |
| Εύκολη πρόσβαση στις αναφορές διαδικτυακών ενεργειών |
| Αναφορές μέσω E-mail |
| Ημερολόγιο διαδικτυακών τόπων που έχουμε επισκεφτεί |
| Εύκολη παραμετροποίηση αναφορών |
| **Άλλες Δυνατότητες** |
| Υποστήριξη πολλαπλών χρηστών |
| Προκαθορισμένος αρχικός χρήστης |

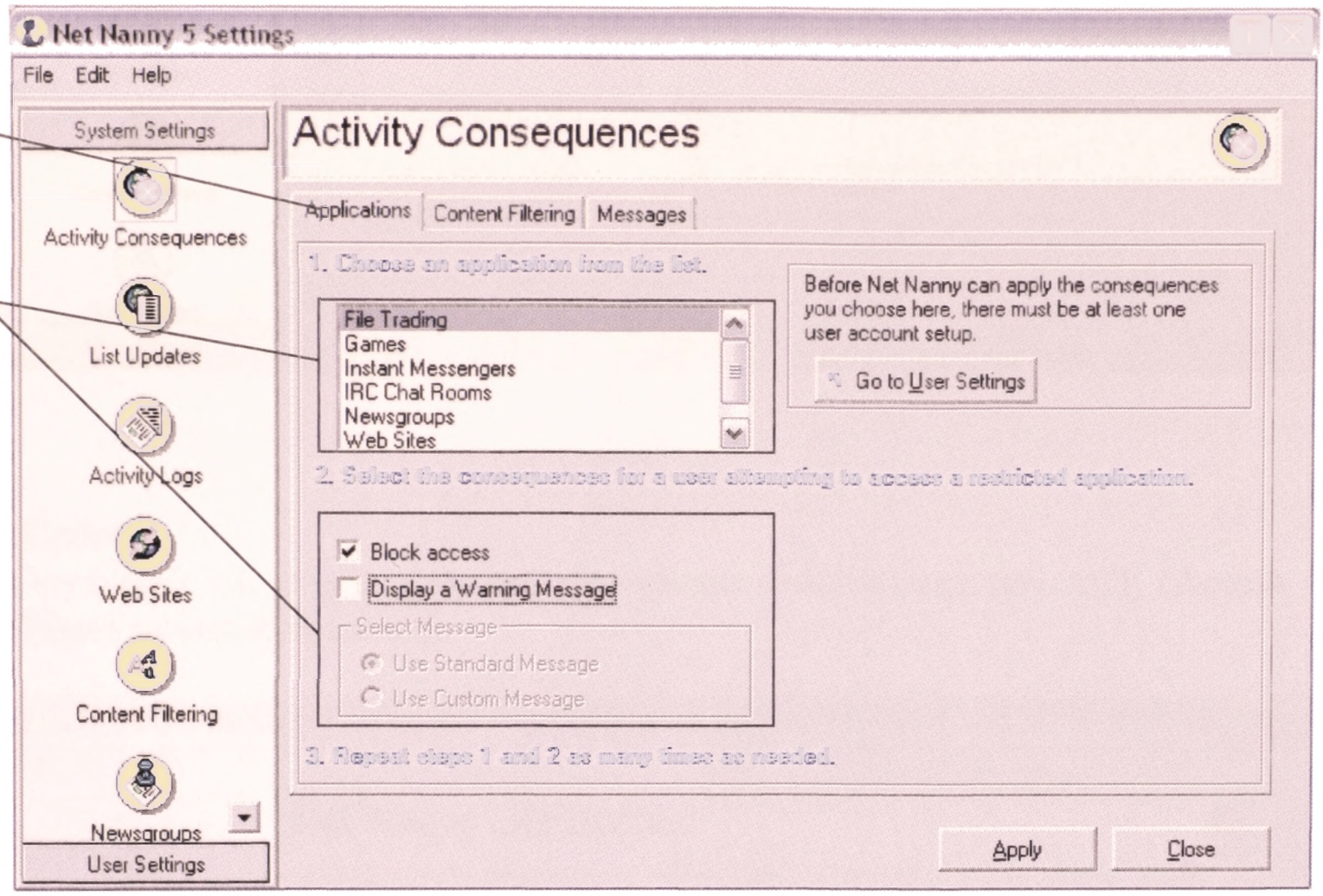
### 3.3.4 Λειτουργία

Παρακάτω θα δούμε τις βασικές λειτουργίες / δυνατότητες του προγράμματος καθώς και τα μενού παραμετροποίησής του.

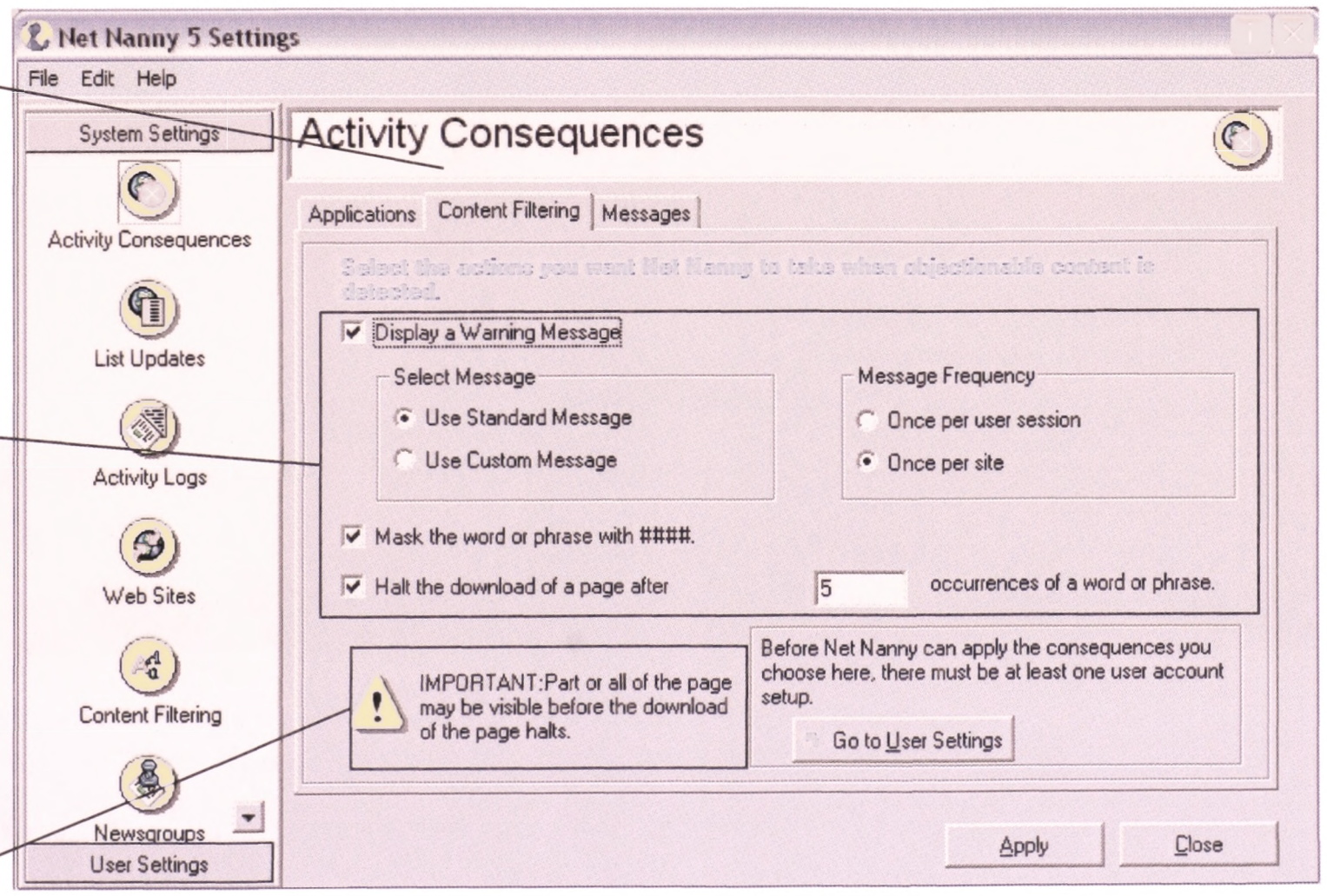
#### 3.3.4.1 Ρυθμίσεις Συστήματος

1. Activity Consequences

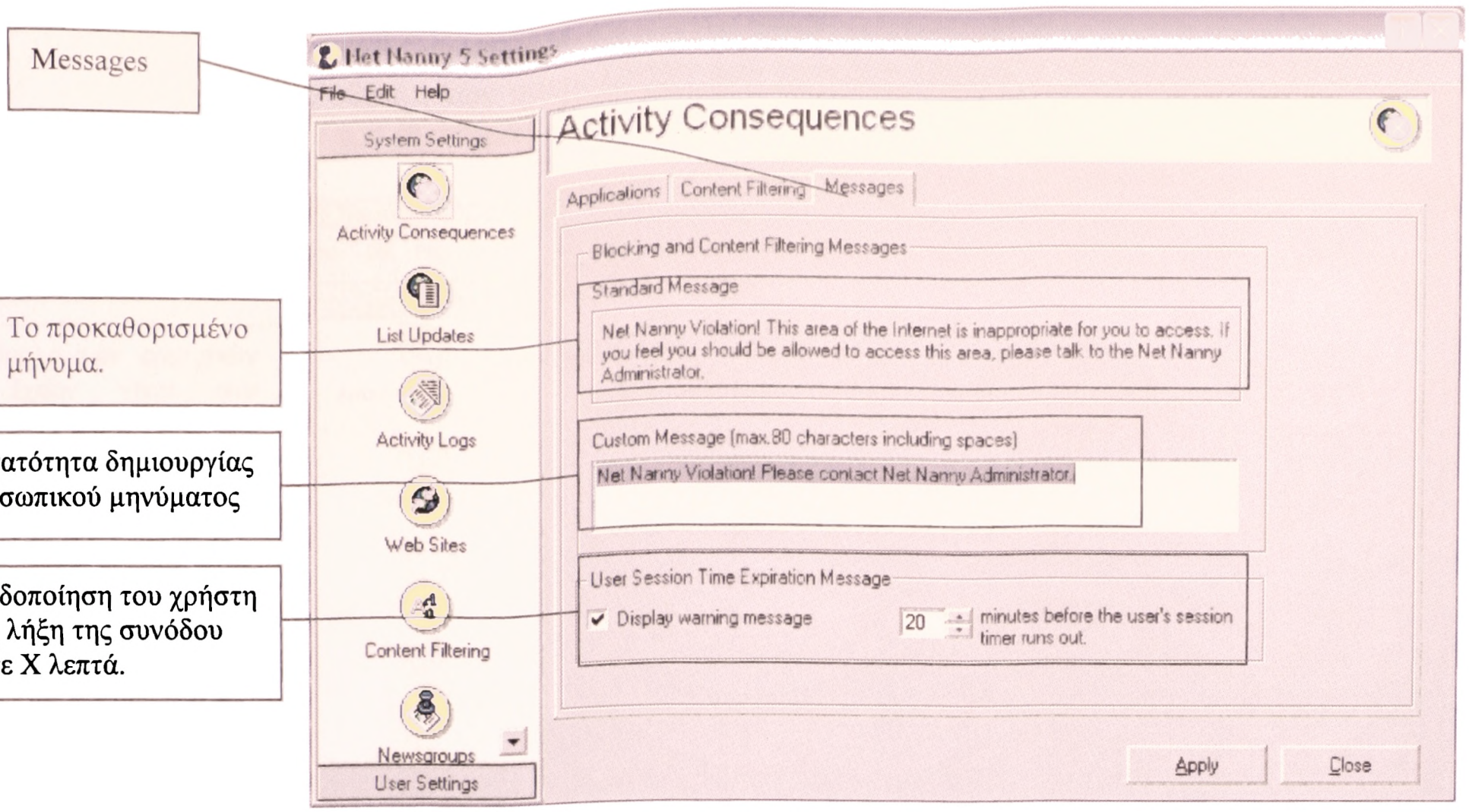
Οι συνέπειες που προκύπτουν όταν ο χρήστης προβεί σε μια απαγορευμένη ενέργεια.




Επιλογή προγράμματος και συνέπειας. Μπορεί να γίνει μπλοκάρισμα της πρόσβασης ή/και εμφάνιση προκαθορισμένου ή δημιουργημένου μηνύματος

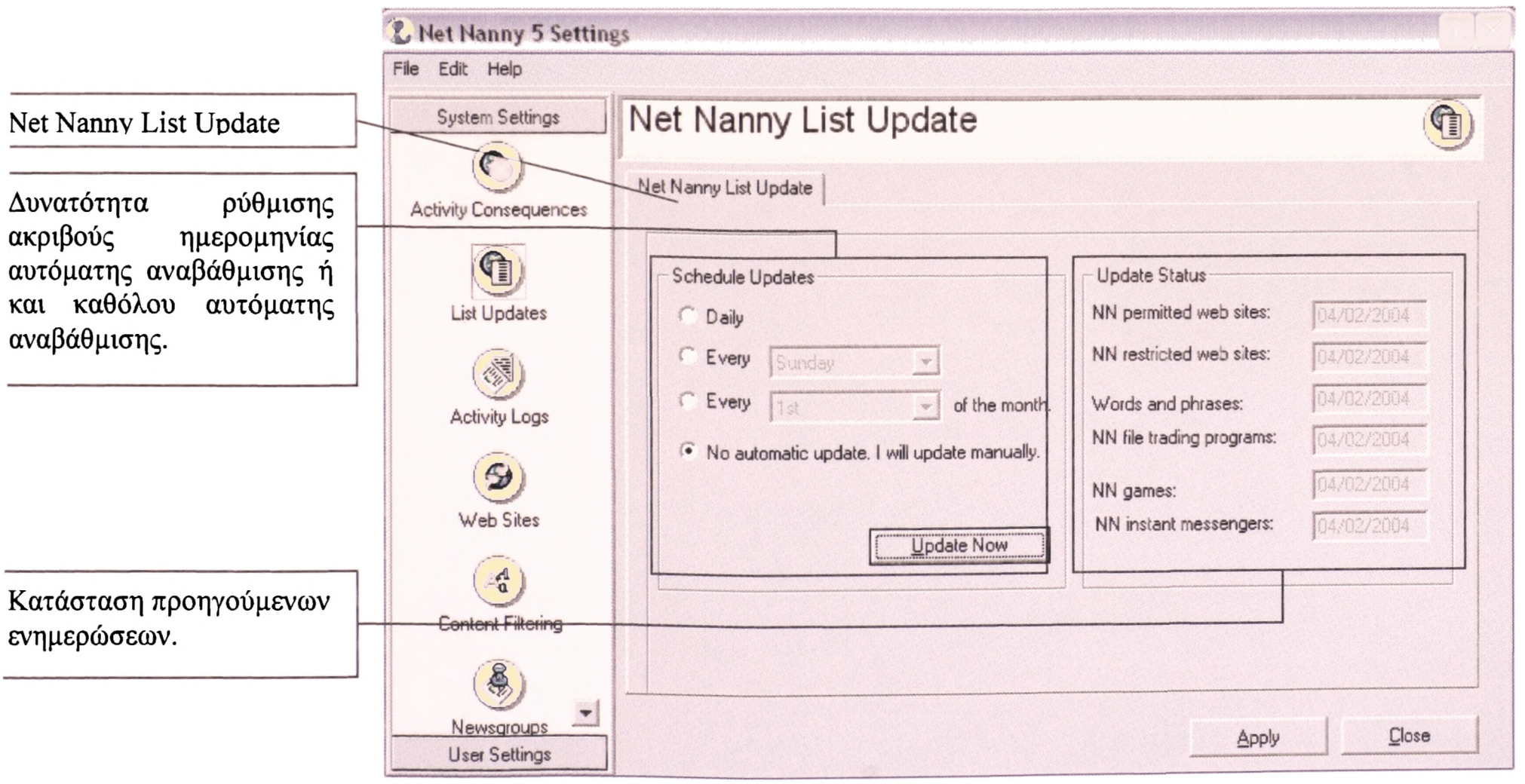



Συνέπειες σε περίπτωση που εντοπίζεται λογοκριμένο περιεχόμενο. Μπορεί να γίνει εμφάνιση προκαθορισμένου ή δημιουργημένου μηνύματος καθώς και να ρυθμιστεί η συχνότητα εμφάνισής του. Το λογοκριμένο περιεχόμενο / λέξεις καλύπτονται από τον χαρακτήρα #. Μπορούμε επίσης να ρυθμίσουμε μετά από πόσες εμφανίσεις της εν λόγω λογοκριμένης λέξης θα μπλοκάρεται η πρόσβαση στη σελίδα. Το πρόγραμμα μας προειδοποιεί ότι το μπλοκάρισμα της σελίδας μπορεί να γίνει αφού ένα κομμάτι της έχει ήδη κατέβει.




2. List Updates

Οργάνωση της συχνότητας και του τρόπου αναβάθμισης των ACL (Access Control Lists) του προγράμματος.



3. Activity Logs

Ρύθμιση των ημερολογίων που κρατάνε εγγραφές για όλες τις ενέργειες των χρηστών του συστήματος που σχετίζονται με το Net Nanny.

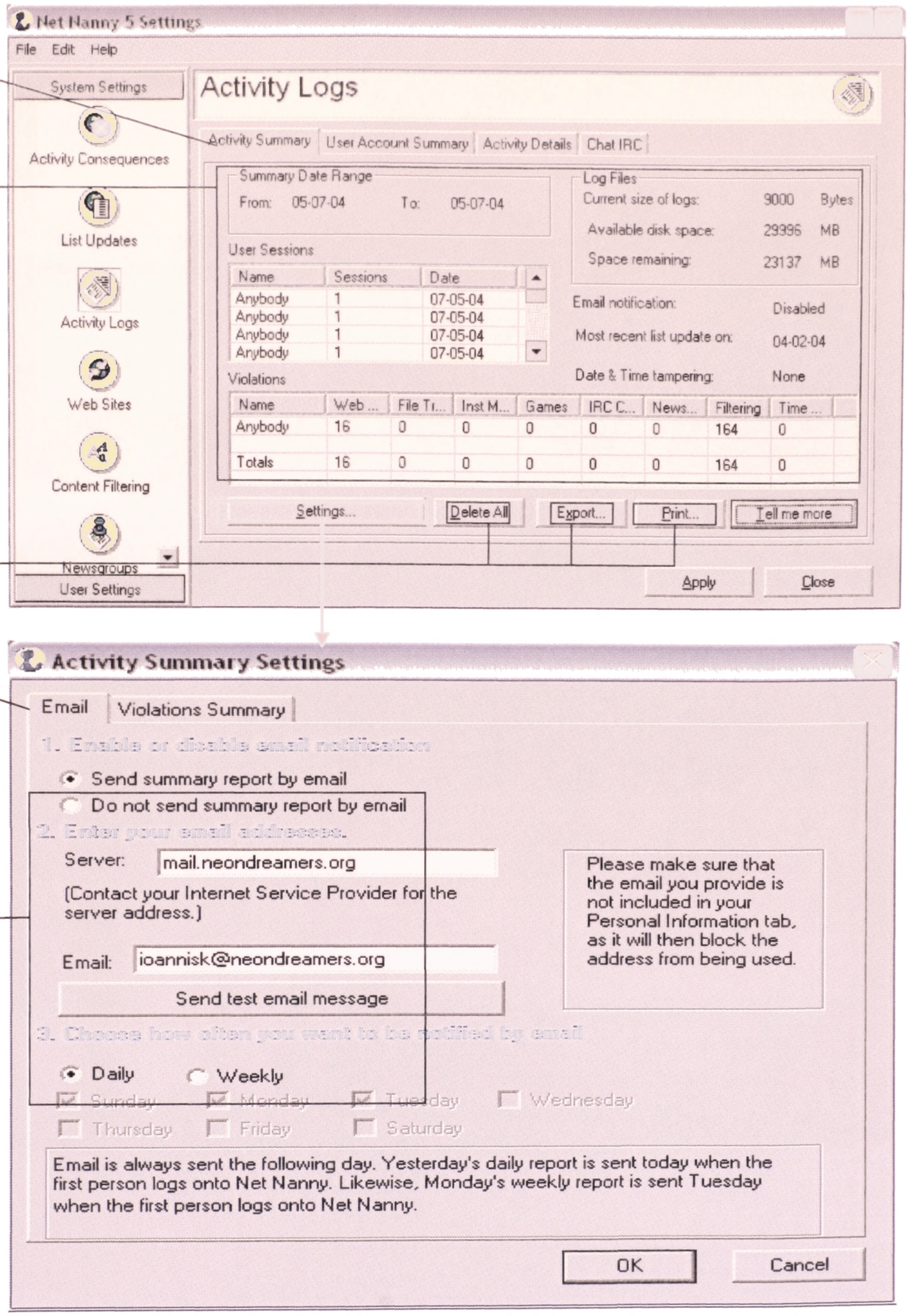
Activity Summary

Το σύνολο των ενεργειών του έχουν γίνει στο σύστημα. Μας δίνονται πληροφορίες για κάθε ένα session και για το σύνολο των παραβάσεων που έχουν γίνει. Επίσης μας ενημερώνει για το συνολικό μέγεθος του log file. Οι παραβάσεις χωρίζονται σε: Web Sites, File Trade, Instant Messages, Games, IRC chat, Newsgroups, Filtering και Time Limit.

Διαγραφή, εξαγωγή σε μορφή αρχείου txt και εκτύπωση των εγγραφών

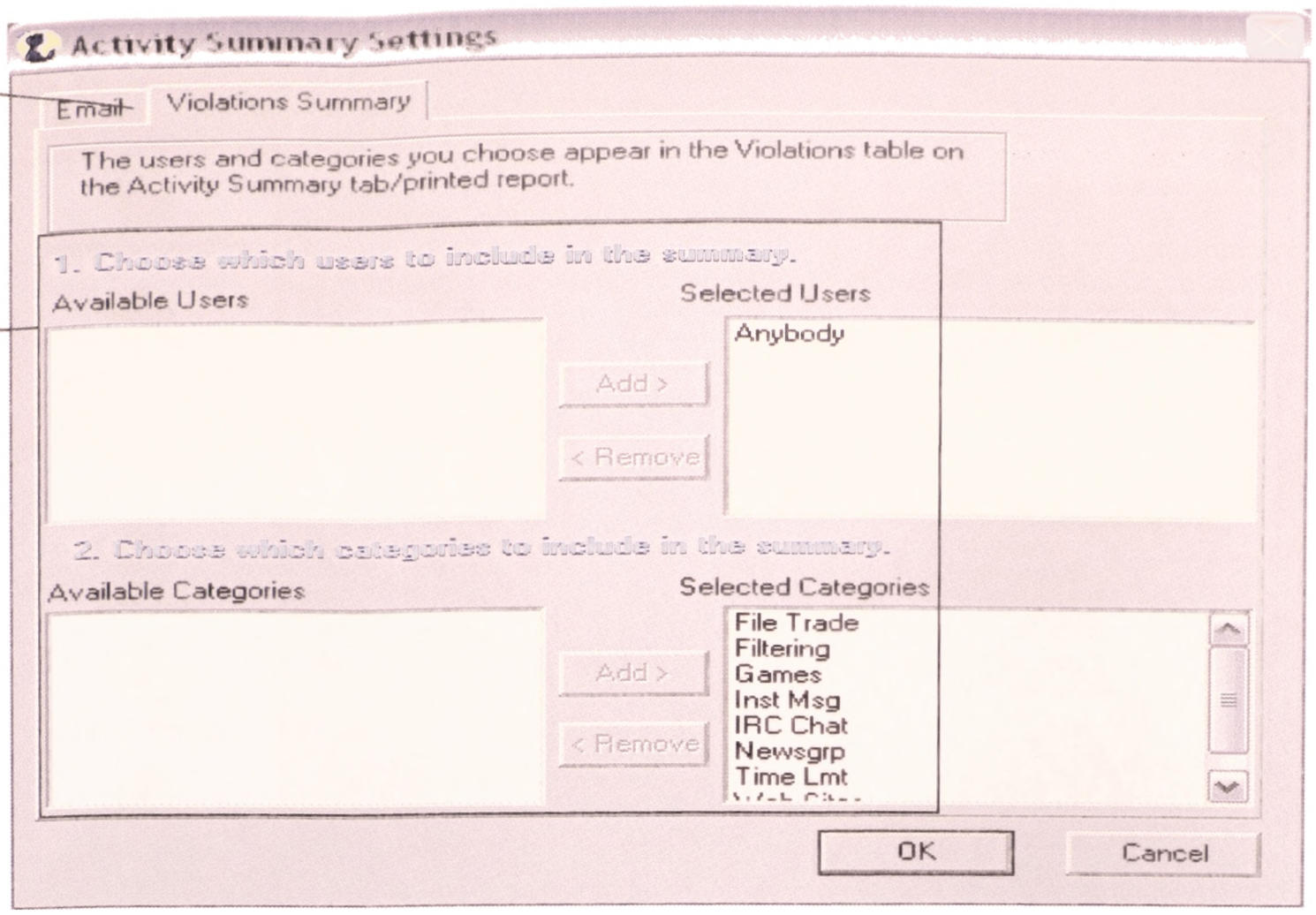
E-mail

Ρυθμίσεις για αποστολή ενημερωτικού e-mail. Το e-mail και ο SMTP server πρέπει να βρίσκονται στο ίδιο domain. Επίσης, αν ο SMTP χρειάζεται αυθεντικοποίηση το πρόγραμμα δεν μπορεί να τον χρησιμοποιήσει. Μπορούμε να ρυθμίσουμε την συχνότητα με την οποία θα μας αποστέλλονται .



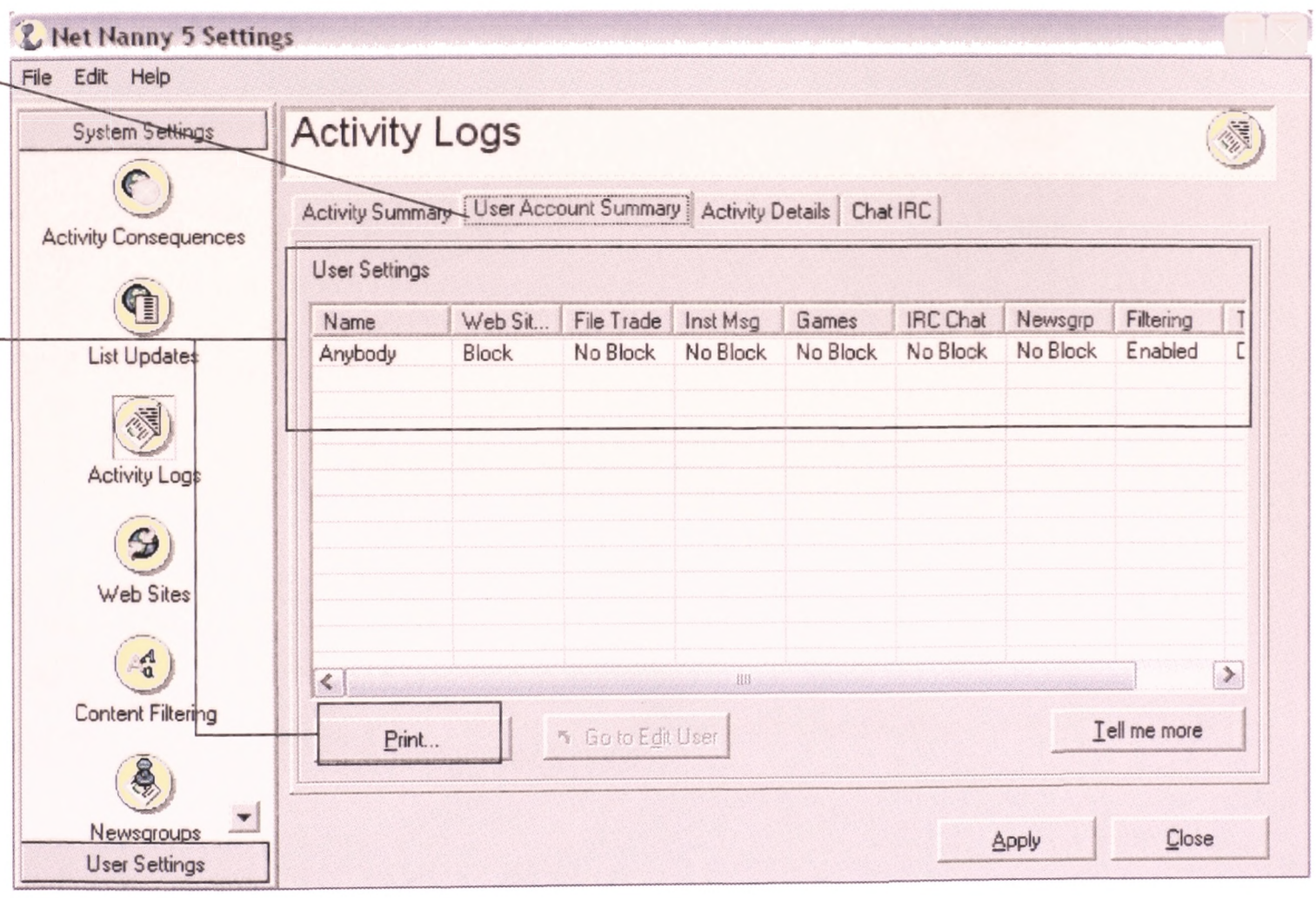
Violations Summary

Ρυθμίζουμε τους χρήστες και τις κατηγορίες παραβάσεων που θέλουμε να εμφανίζονται στην καρτέλα και στην εκτυπωμένη αναφορά ενεργειών.




User Account Summary

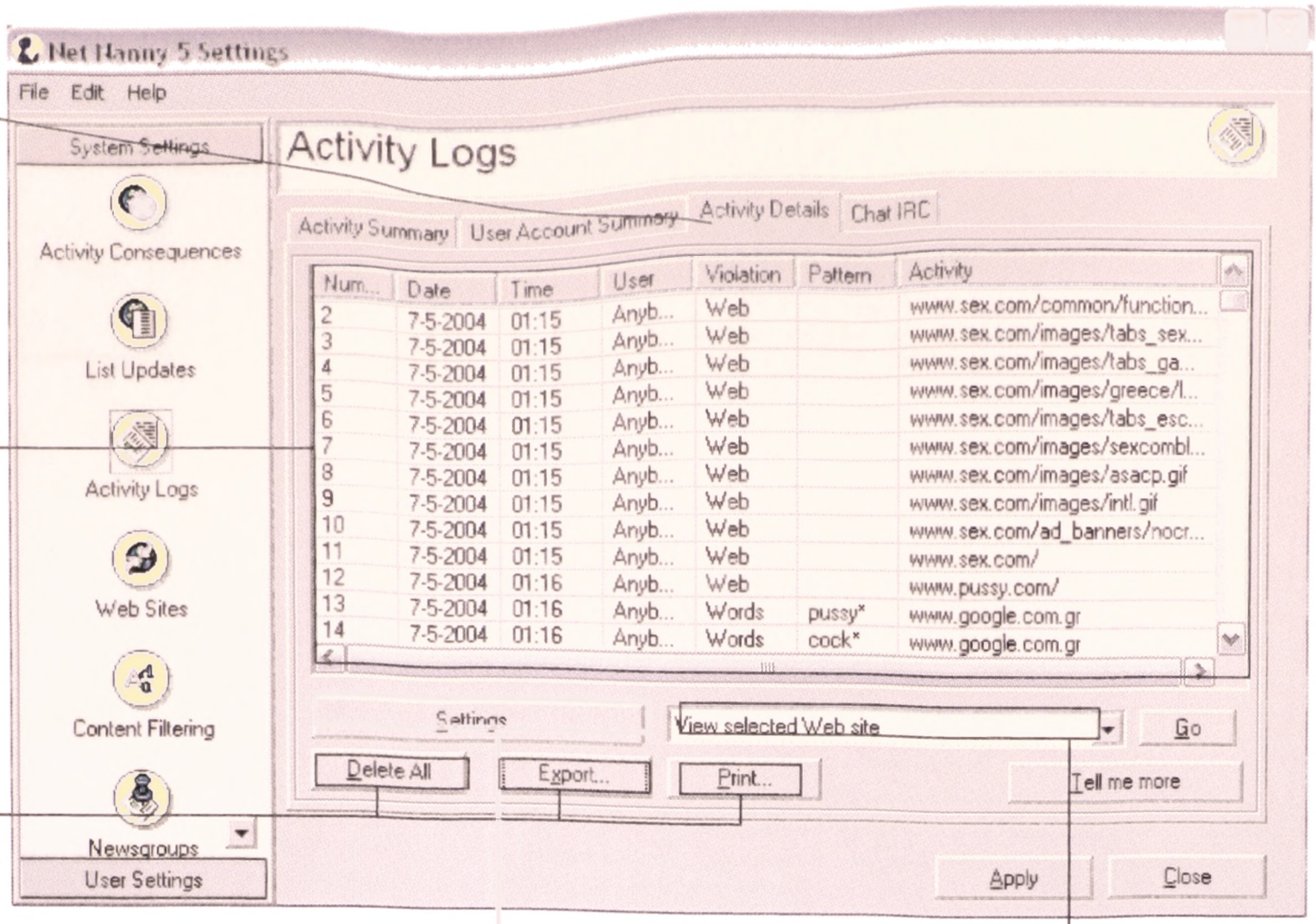
Συνολική αναφορά των κατηγοριών παραβάσεων / εφαρμογών που μπλοκάρονται ανά χρήστη. Μας δίνεται η δυνατότητα εκτύπωσης.



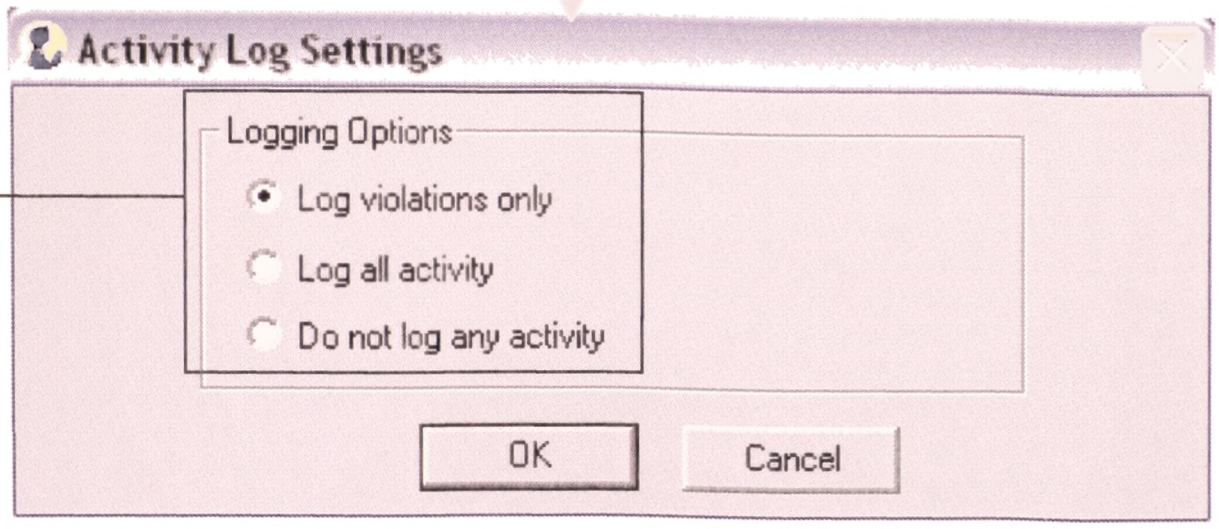
Activity Details

Η λεπτομερής ανάλυση του συνόλου των ενεργειών / παραβάσεων. Μας δίνεται: Ο Α/Α της παράβασης, η ημερομηνία, η ώρα, ο χρήστης, το είδος της παράβασης, το μοτίβο σύμφωνα με το οποίο έγινε το μπλοκάρισμα και η ενέργεια.

Διαγραφή, εξαγωγή σε μορφή αρχείου txt και εκτύπωση των εγγραφών.




Μπορούμε να ρυθμίσουμε αν θα καταγράφονται μόνο οι παραβάσεις, όλες οι ενέργειες ή καμία ενέργεια.



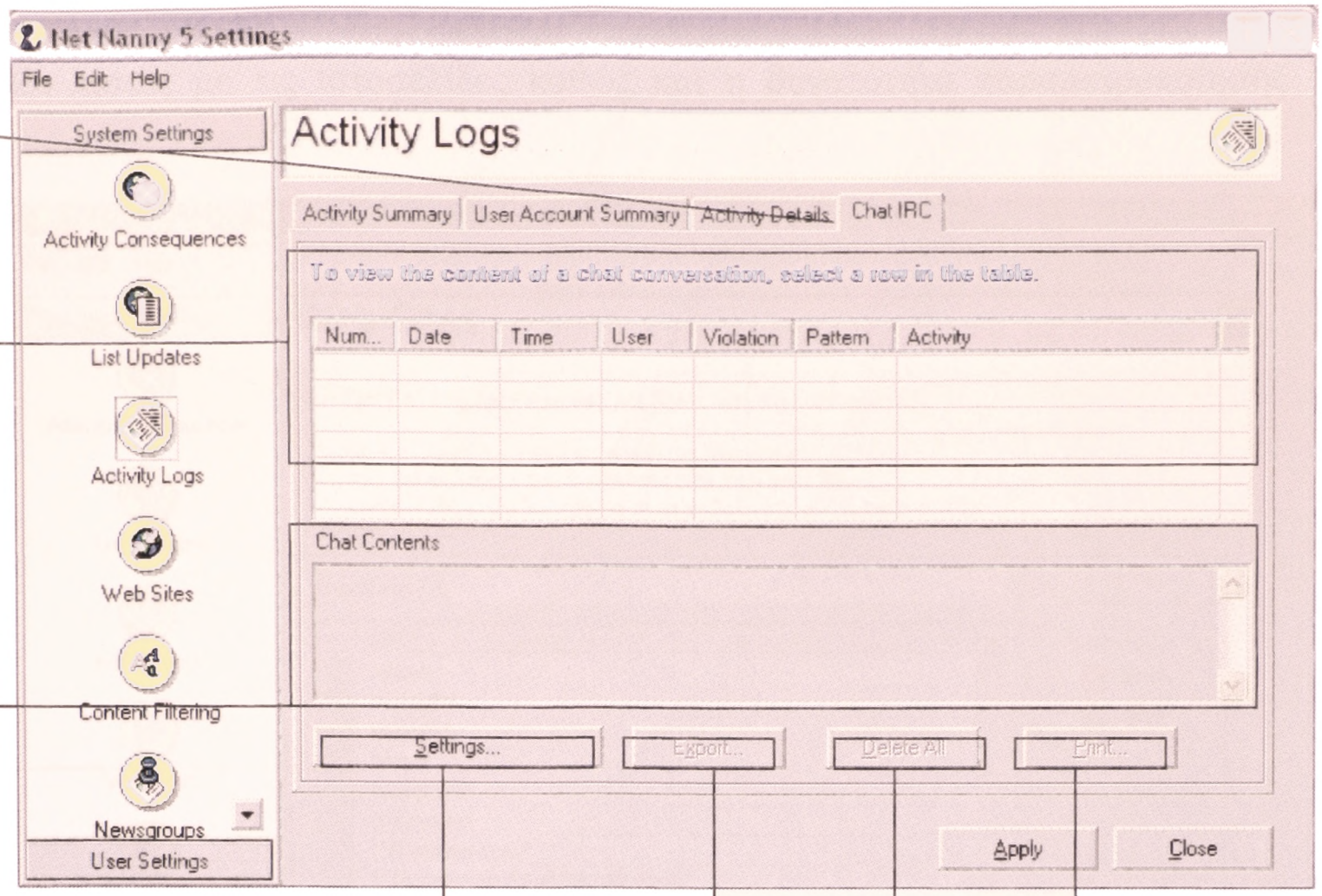

Στην περίπτωση που η παράβαση σχετίζεται με κάποια ιστοσελίδα μπορούμε να επιλέξουμε μεταξύ των: View Selected Website, Add to My Restricted List, Add to my Family-Friendly List, Send to Net Nanny Restricted List, Send to Net Nanny Family-Friendly List.

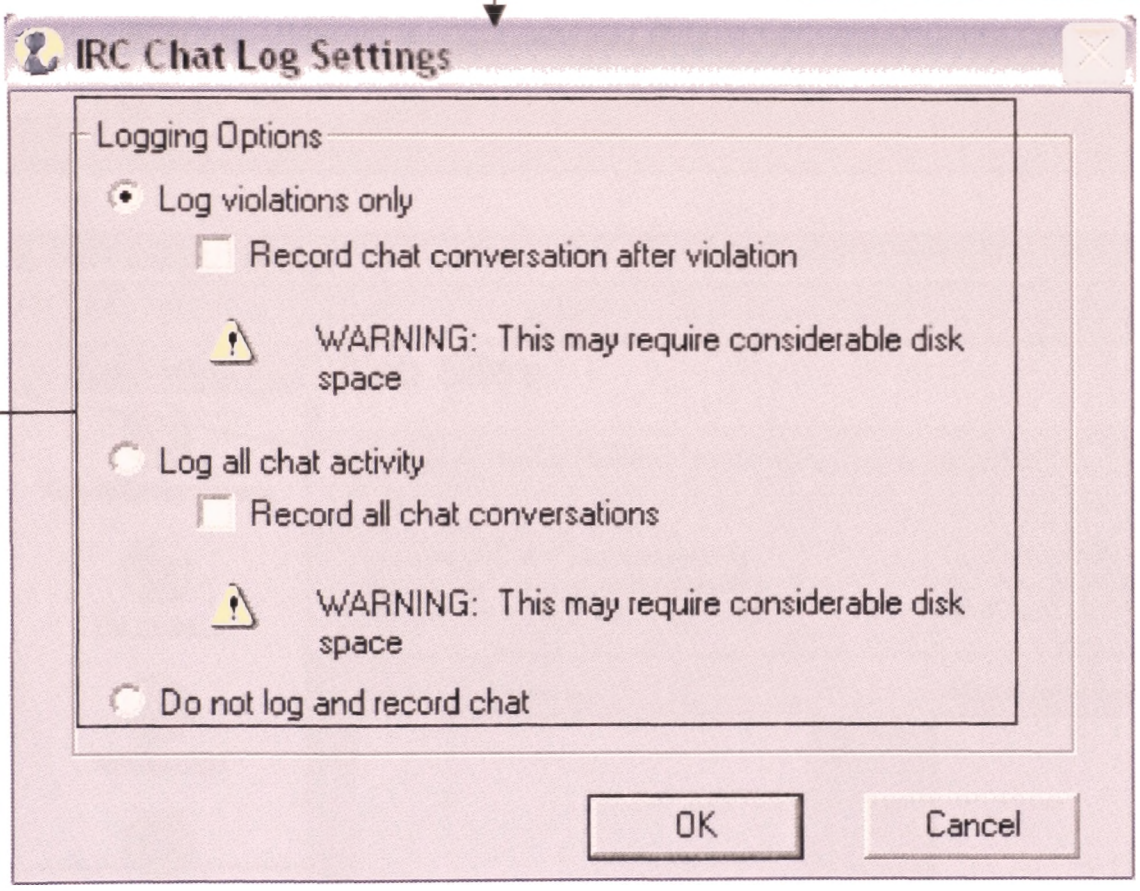
Chat IRC

Λεπτομερής ανάλυση όλων των ενεργειών / παραβάσεων που σχετίζονται με IRC chat. Αναλυτικά έχουμε: Α/Α της παράβασης, ημερομηνία, ώρα, χρήστη, είδος της παράβασης, μοτίβο σύμφωνα με το οποίο έγινε το μπλοκάρισμα και ενέργεια.

Μπορούμε να δούμε τα περιεχόμενα της συζήτησης ανάλογα με τις ρυθμίσεις που έχουμε κάνει

Ρυθμίσεις που σχετίζονται με το ποιες ενέργειες / παραβάσεις θα καταγράφονται. Αναλυτικά: 1) Να καταγράφει μόνο τις παραβάσεις. Μπορεί να καταγράφει και τη συζήτηση που ακολουθεί αμέσως μετά την παράβαση. 2) Να καταγράφει όλες τις ενέργειες. Μπορεί να καταγράφει όλη τη συζήτηση ανεξάρτητα εάν έχει σημειωθεί κάποια παράβαση. 3) Να μην γίνεται καμία καταγραφή.



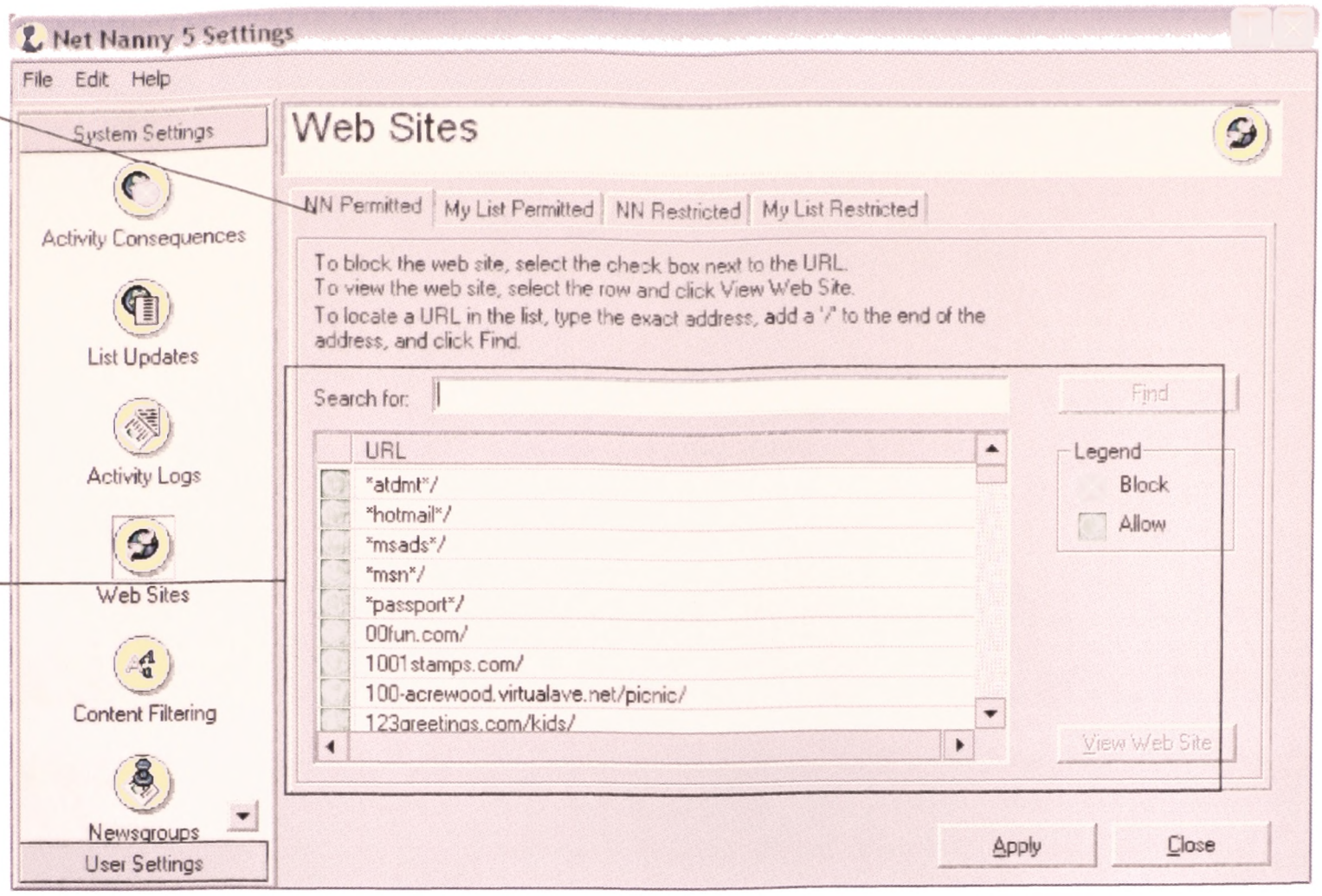

Διαγραφή, εξαγωγή σε μορφή αρχείου txt και εκτύπωση των εγγραφών.

4. Web Sites

Οι λίστες με τις ιστοσελίδες καθώς και η δυνατότητα παραμετροποίησής τους.

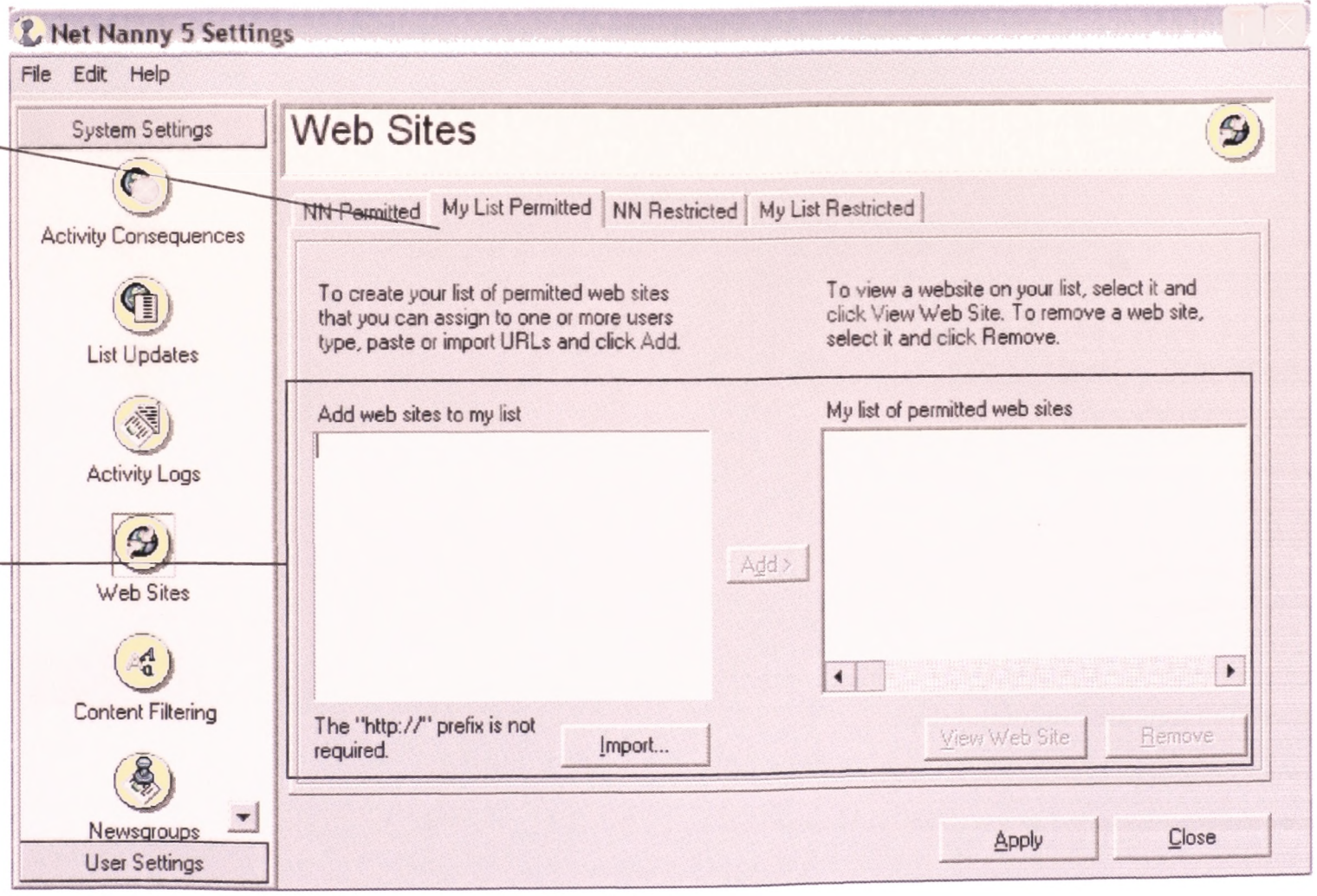
Net Nanny Permitted

Η λίστα με τις ιστοσελίδες που το Net Nanny επιτρέπει πάντα την πρόσβαση (white list). Μας δίνεται η δυνατότητα εύρεσης μιας ιστοσελίδας από τη λίστα καθώς επίσης να μπλοκάρουμε οποιαδήποτε θεωρούμε εμείς ακατάλληλη. Επίσης μπορούμε να επισκεφτούμε άμεσα μια ιστοσελίδα για να ελέγξουμε το περιεχόμενό της μόνοι μας.



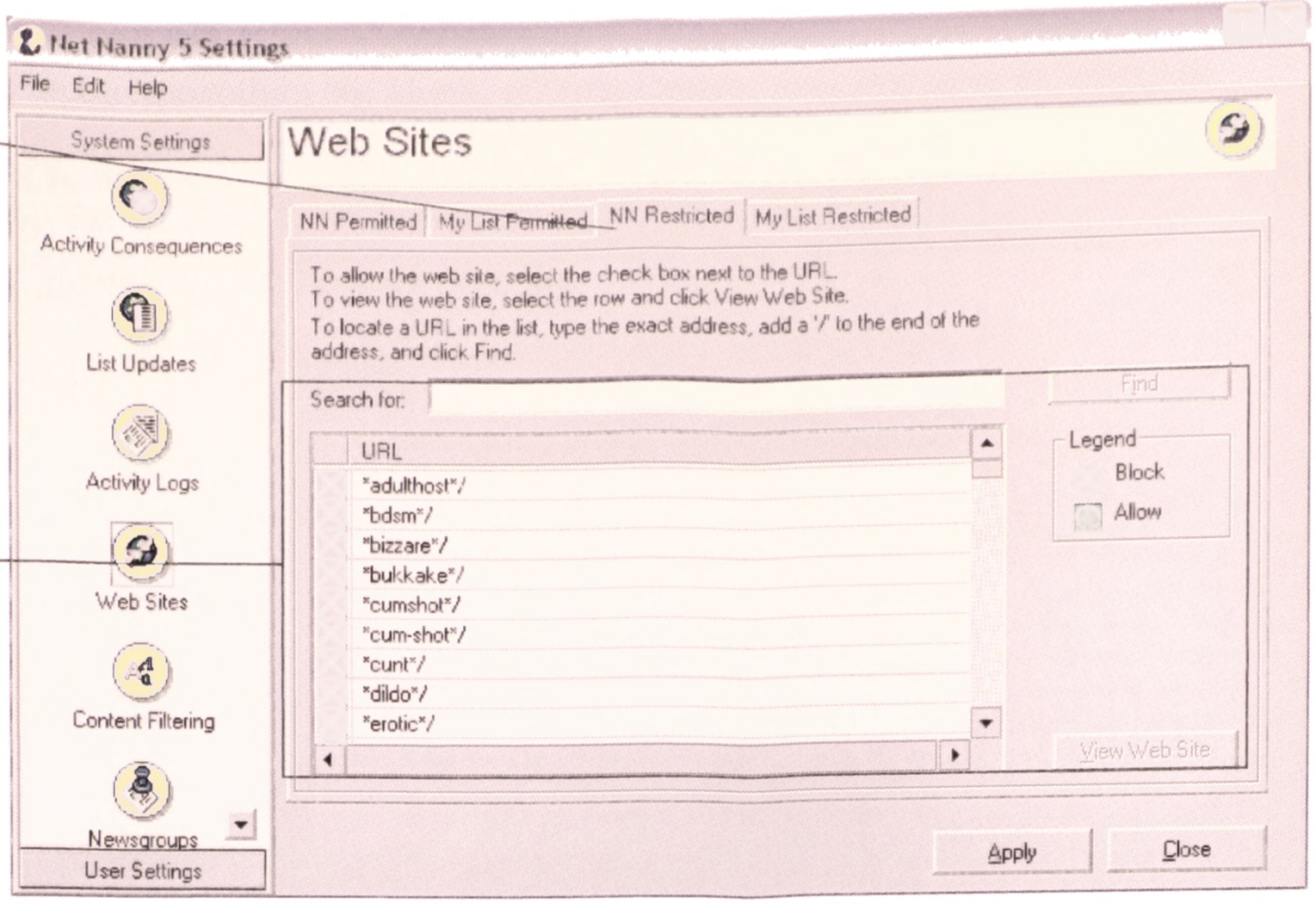

My List Permitted

Μπορούμε να δημιουργήσουμε τη δική μας λίστα με τις ιστοσελίδες που θεωρούμε εμείς ότι πρέπει πάντα να επιτρέπεται η πρόσβαση.



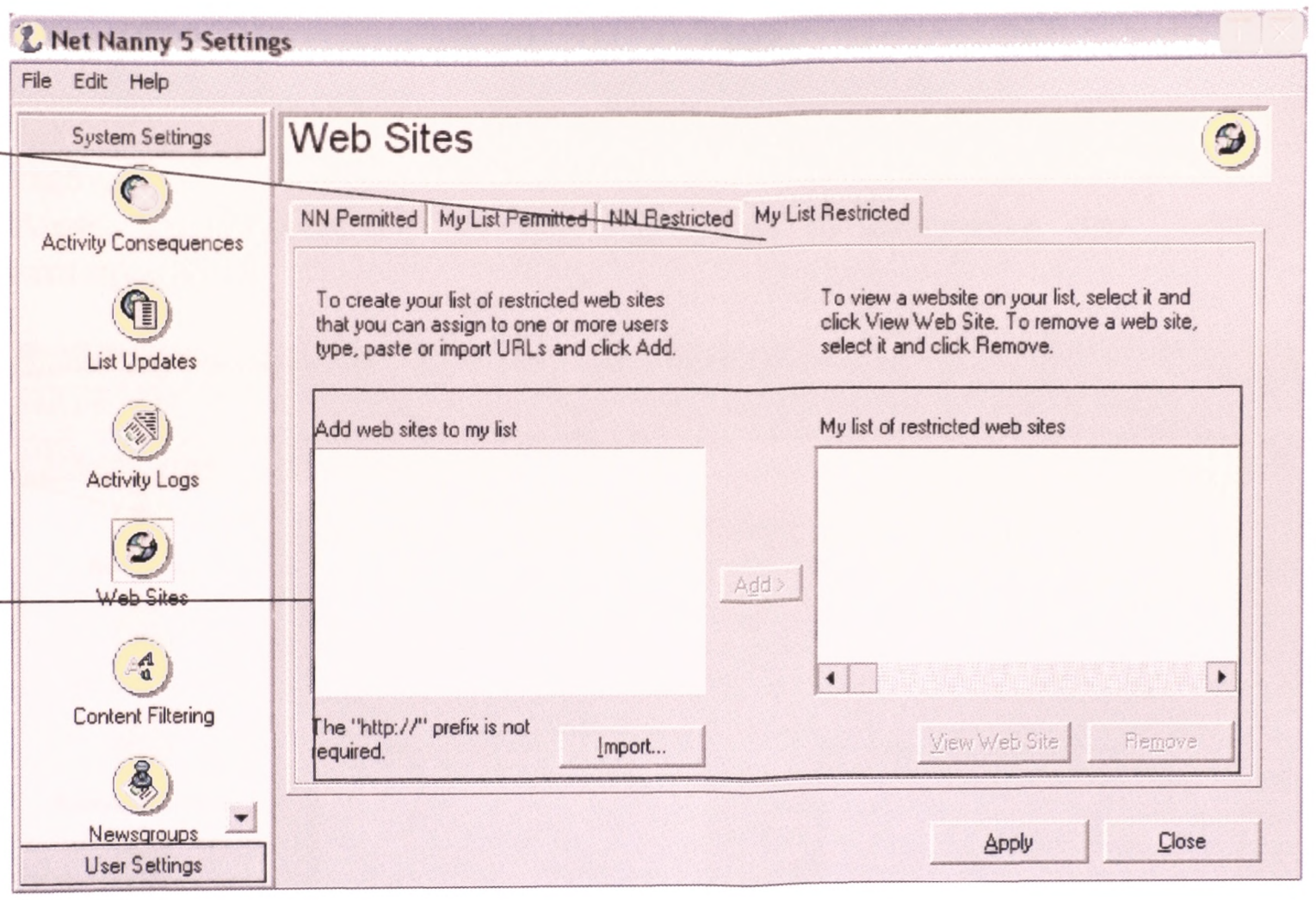
Net Nanny Restricted

Η λίστα με τις ιστοσελίδες που το Net Nanny μπλοκάρει πάντα την πρόσβαση (black list). Μας δίνεται η δυνατότητα εύρεσης μιας ιστοσελίδας από τη λίστα, καθώς επίσης να επιτρέψουμε την πρόσβαση σε οποιαδήποτε θεωρούμε εμείς κατάλληλη. Επίσης μπορούμε να επισκεφτούμε άμεσα μια ιστοσελίδα για να ελέγξουμε το περιεχόμενό της μόνοι μας.




My List Restricted

Μπορούμε να δημιουργήσουμε τη δική μας λίστα με τις ιστοσελίδες που θεωρούμε εμείς ότι πρέπει πάντα να μπλοκάρεται η πρόσβαση.

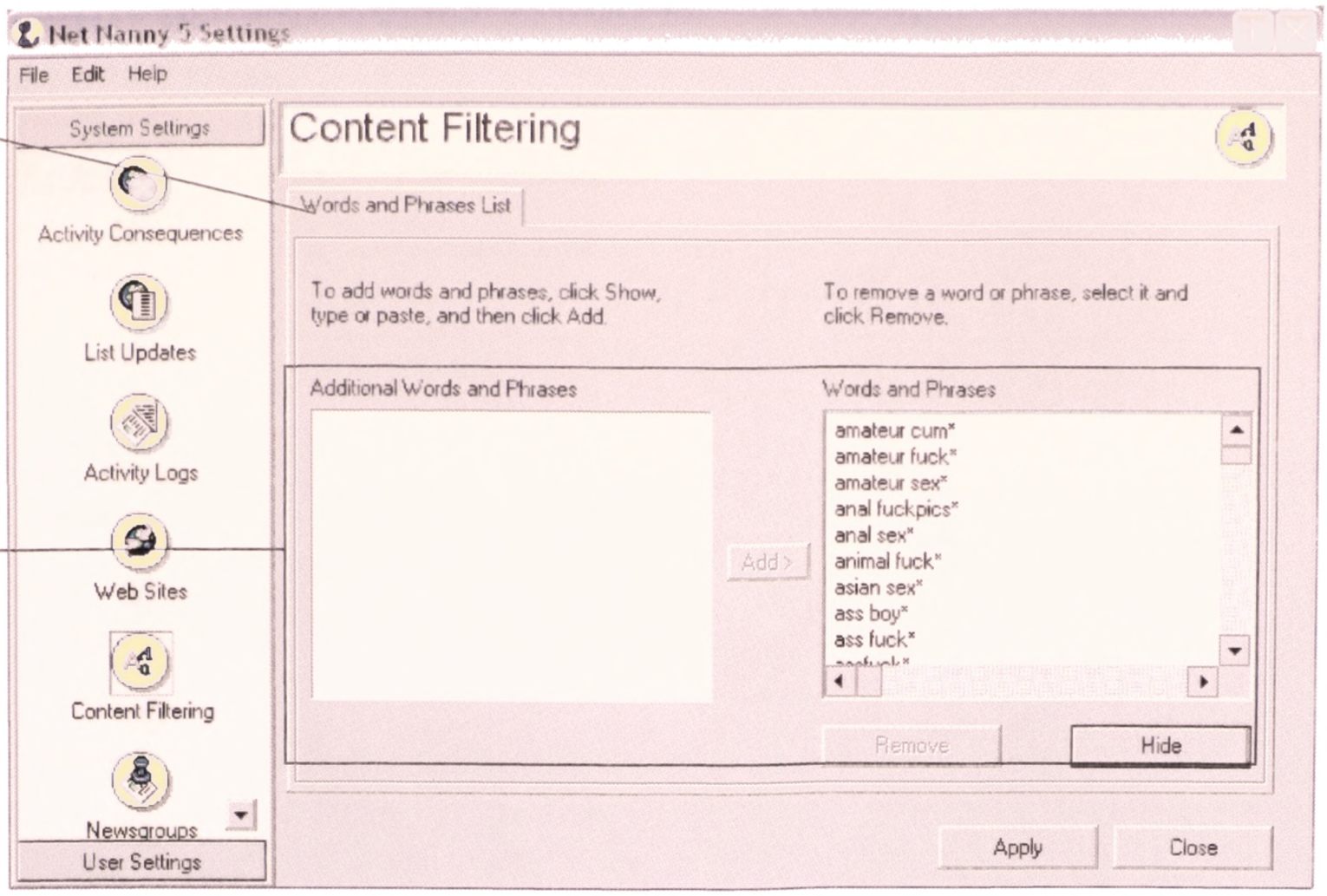


5. Content Filtering

Παραμετροποίηση της λίστας φιλτραρίσματος ανάλογα με το περιεχόμενο.

Words and Phrase List

Η λίστα με τις φράσεις και τις λέξεις που φιλτράρονται. Έχουμε τη δυνατότητα πρόσθεσης η αφαίρεσης οποιασδήποτε λέξης επιθυμούμε.

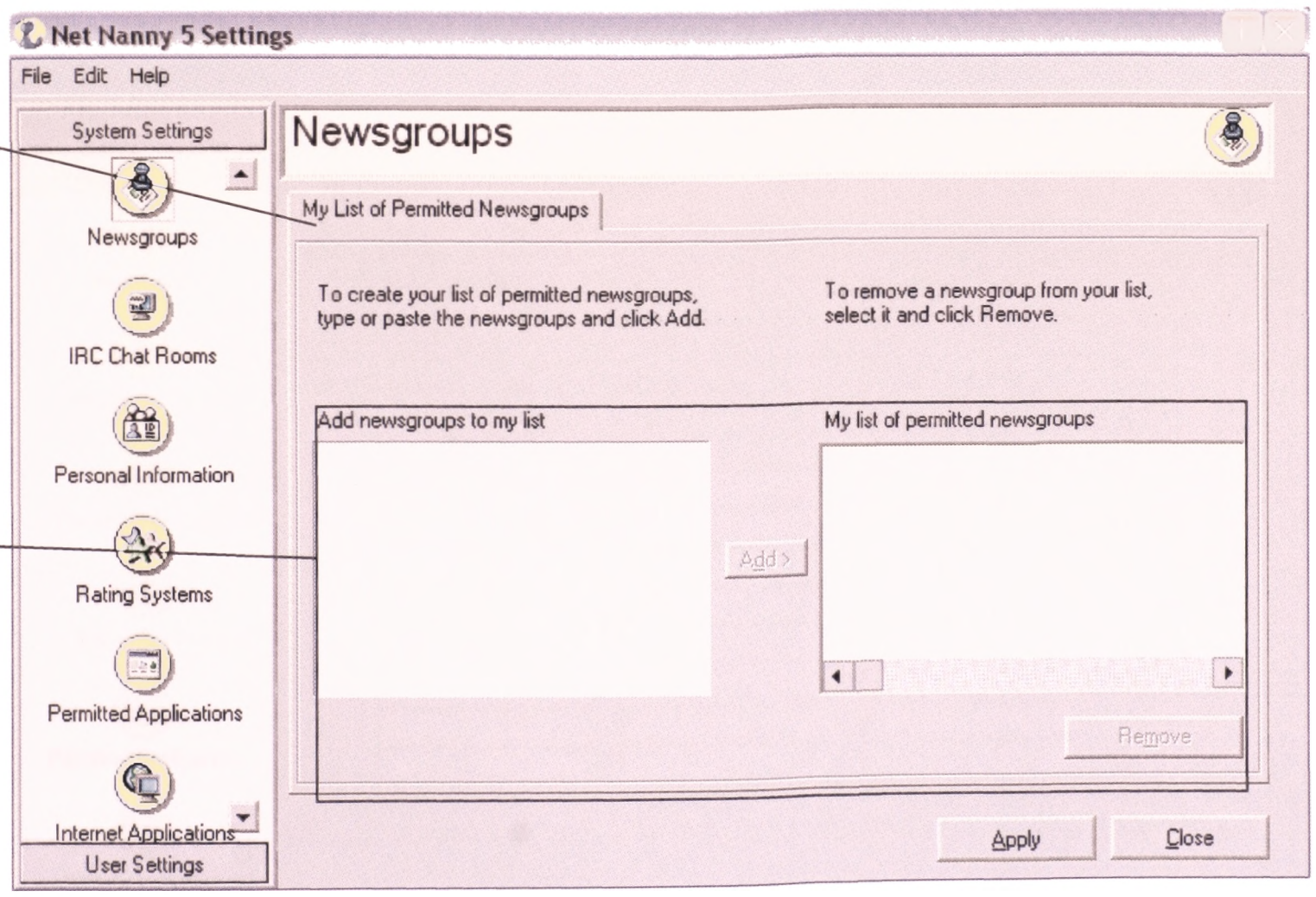



6. Newsgroups

Λίστα του διαχειριστή του Net Nanny με τα newsgroup στα οποία επιτρέπεται πρόσβαση.

My List of Permitted Newsgroups

Η προσωπική μας λίστα με τα Newsgroups στα οποία επιτρέπεται πάντα η πρόσβαση.

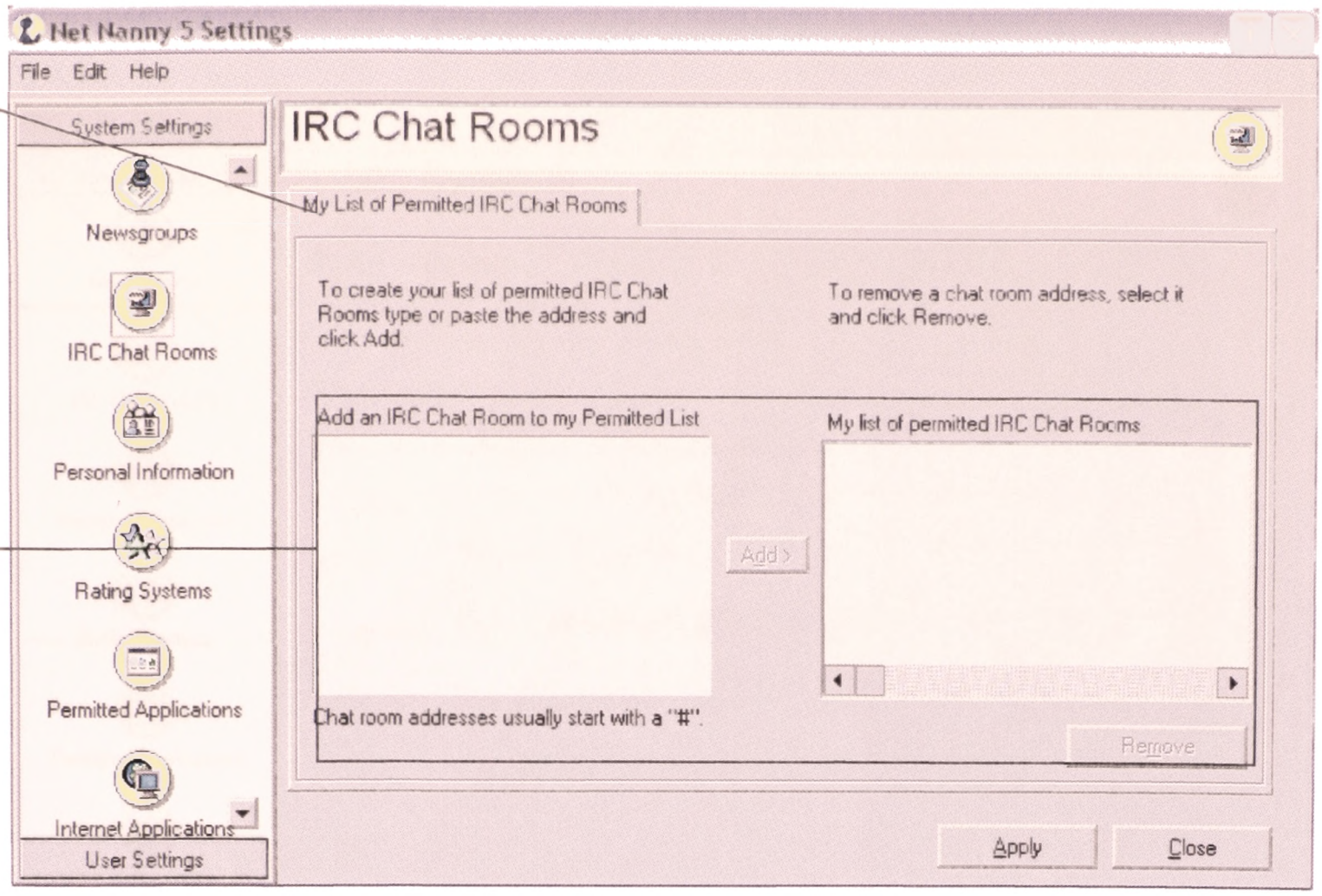


7. IRC chat rooms

Λίστα του διαχειριστή του Net Nanny με τα IRC chat rooms στα οποία επιτρέπεται πρόσβαση.

My List of Permitted IRC Chat Rooms

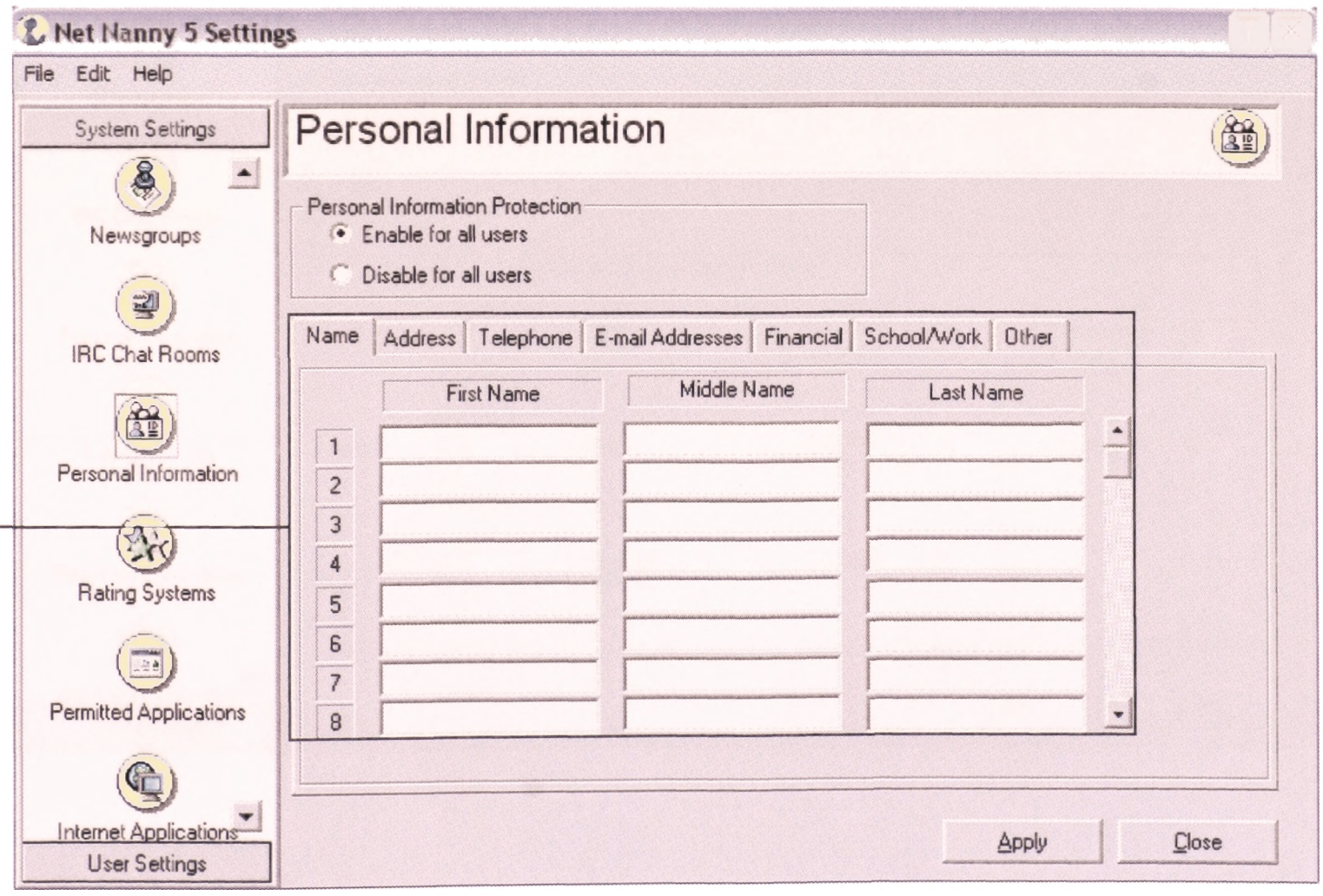
Η προσωπική μας λίστα με τα IRC chat rooms στα οποία επιτρέπεται πάντα η πρόσβαση.




8. Personal Information

Καταγραφή των προσωπικών πληροφοριών τις οποίες θέλουμε το Net Nanny να μπλοκάρει την εκπομπή τους και την αποθήκευσή τους σε Cookies.

Καταγραφή όλων των προσωπικών πληροφοριών που επιθυμούμε να προστατεύονται από το Net Nanny. Οι πληροφορίες αυτές όταν μεταδίδονται καλύπτονται από τον χαρακτήρα #. Το Net Nanny κατηγοριοποιεί τις πληροφορίες σε: Ονόματα, Διευθύνσεις, Τηλέφωνα, E-mail διευθύνσεις, Οικονομικά (πιστωτικές κάρτες), Σχολικά / Δουλειά και Άλλες. Το φιλτράρισμα ισχύει είτε για όλους τους χρήστες είτε για κανένα.



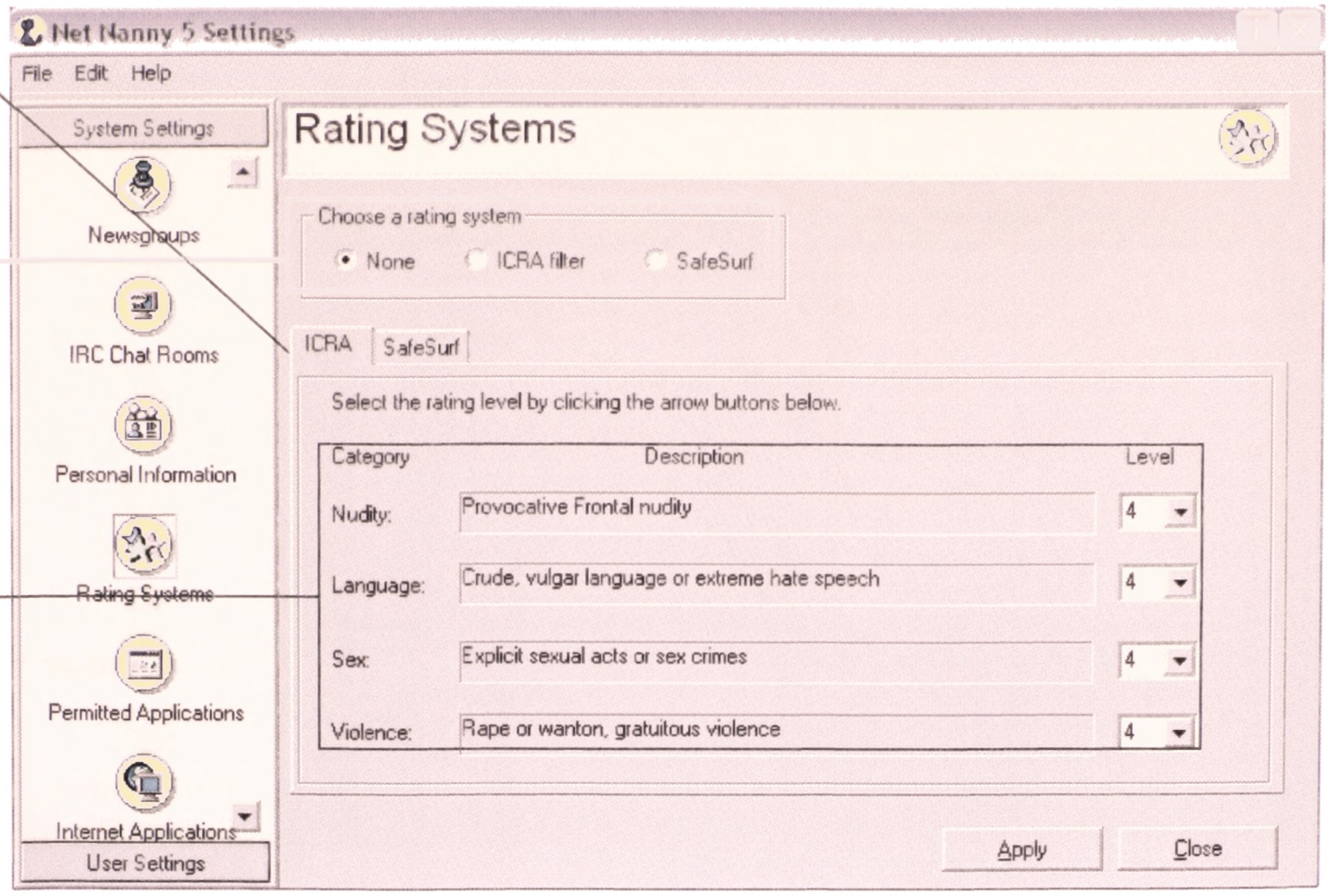
## 9. Rating Systems

Επιλέγουμε αν επιθυμούμε να χρησιμοποιήσουμε συστήματα βαθμονόμησης από τρίτους. Αυτά που προσφέρονται είναι το φίλτρο ICRA της Content Rating Association και το SafeSurf Rating Standard της SafeSurf.

ICRA

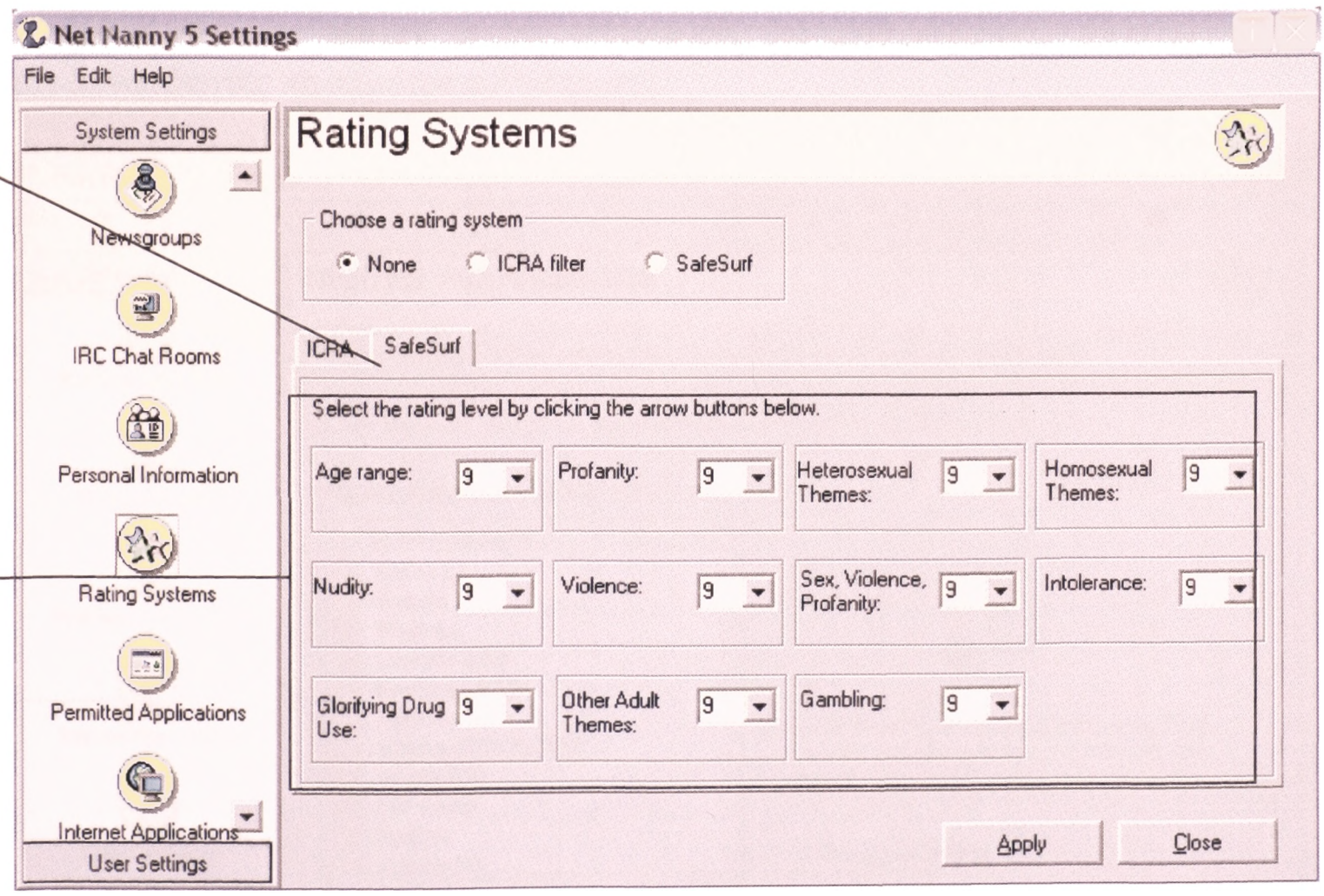
Επιλογή φίλτρου που θα χρησιμοποιήσουμε. Δεν μπορούμε να χρησιμοποιούμε παραπάνω από ένα μια δεδομένη στιγμή.

Δυνατότητα επιλογής του επιπέδου φιλτραρίσματος ανά κατηγορία. Το ICRA (www.icra.org) είναι ένα σύστημα βαθμονόμησης που χρησιμοποιεί το πρότυπο PICS (www.w3.org). Οι κατηγορίες που διαθέτει είναι περιορισμένες.




SafeSurf

Δυνατότητα επιλογής του επιπέδου φιλτραρίσματος ανά κατηγορία. Το SafeSurf (www.safesurf.com) είναι ένα σύστημα βαθμονόμησης που χρησιμοποιεί το πρότυπο PICS (www.w3.org). Οι κατηγορίες που διαθέτει είναι περισσότερες από του ICRA και καλύτερα δομημένες.

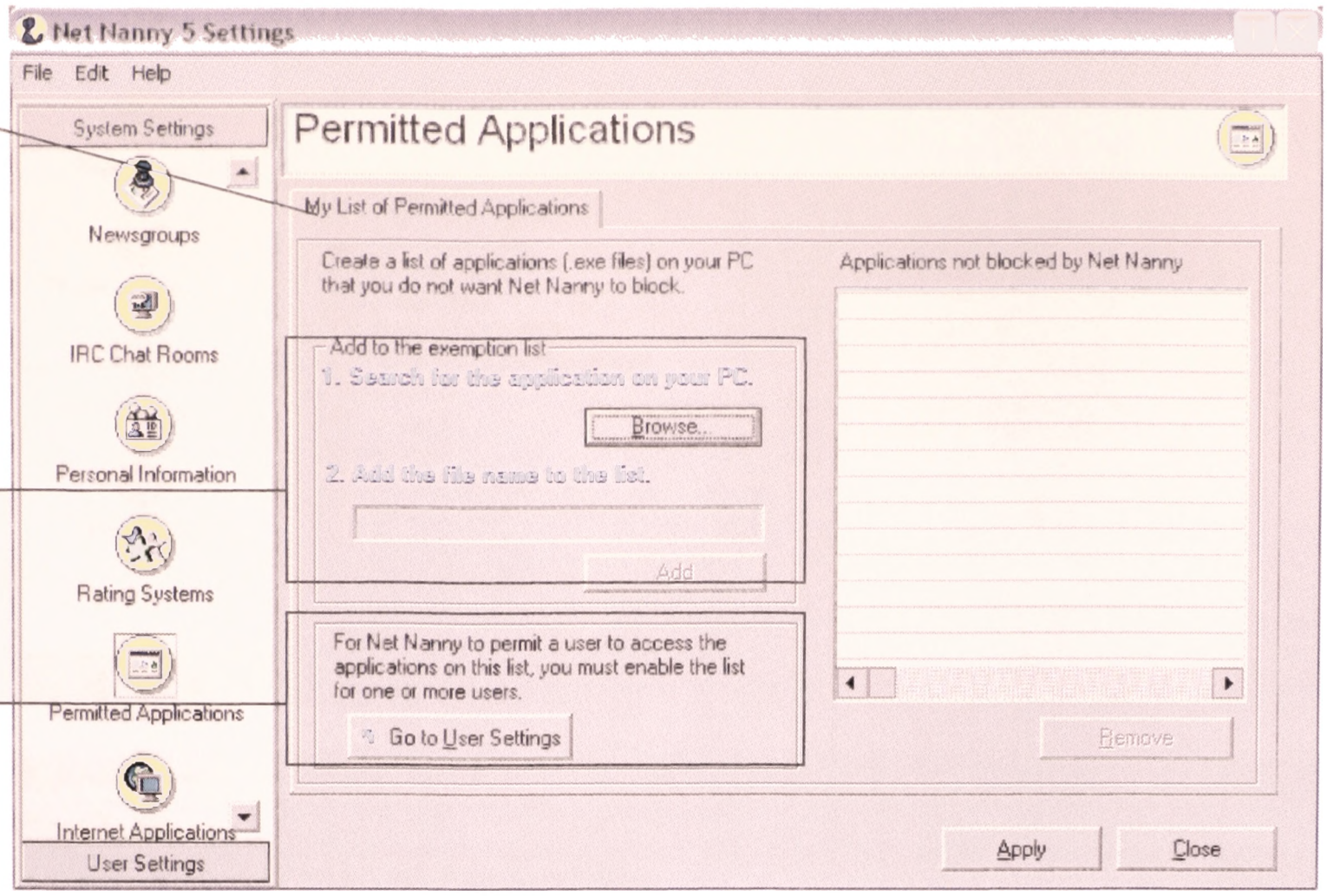


10. Permitted applications

Λίστα του διαχειριστή του Net Nanny με τις εφαρμογές οι οποίες δεν θα μπλοκάρονται.

My List of Permitted Applications

Δυνατότητα αναζήτησης εφαρμογών από τον προσωπικό μας υπολογιστή για τη δημιουργία προσωπικής λίστας με τις εφαρμογές οι οποίες δεν θα μπλοκάρονται. Οι εφαρμογές αυτές είναι προσβάσιμες από τον χρήστη εάν η λίστα είναι ενεργοποιημένη για τον εν λόγω χρήστη.

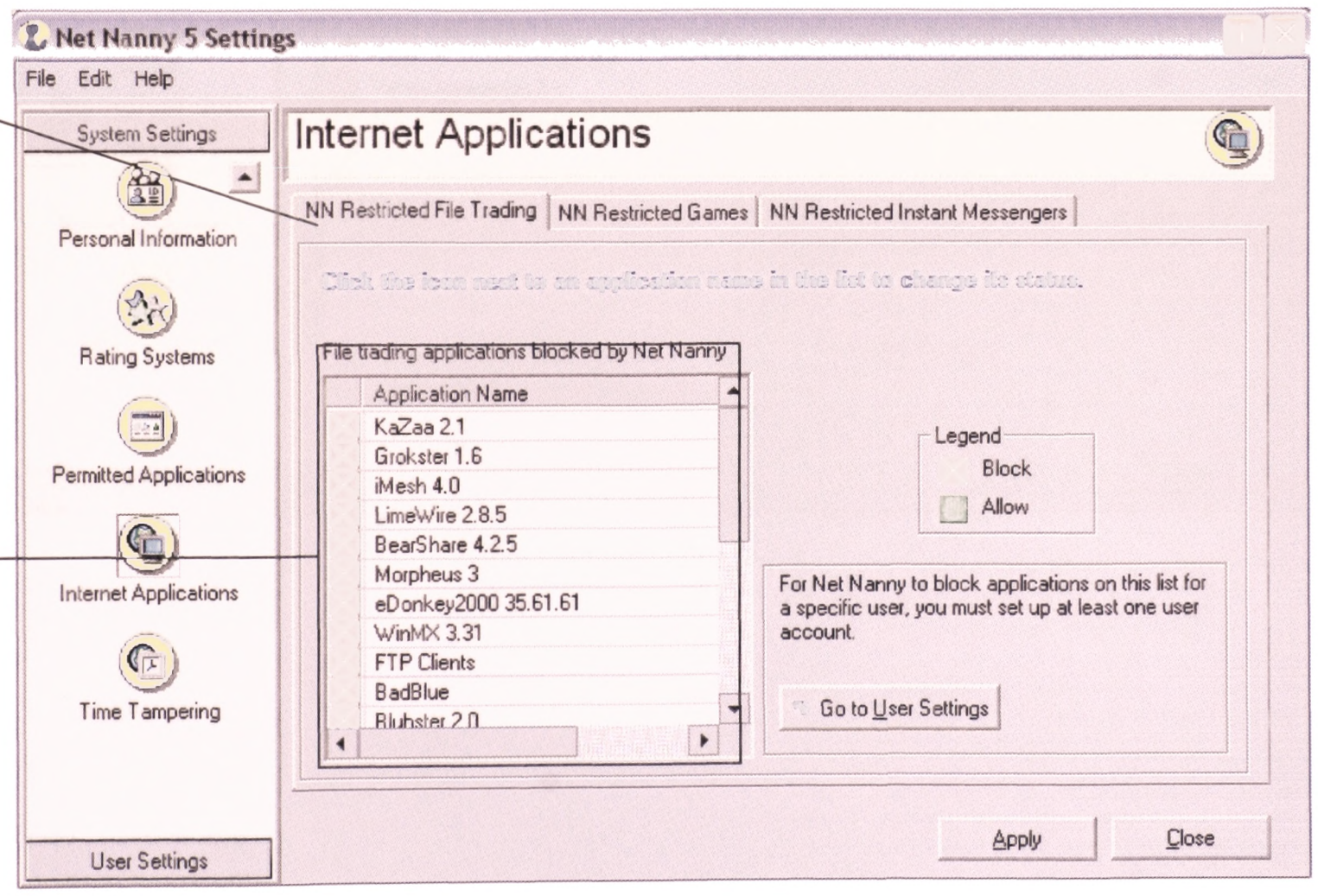



11. Internet Applications

Η λίστα του Net Nanny με τις εφαρμογές του internet που μπλοκάρονται καθώς και δυνατότητες παραμετροποίησης της.

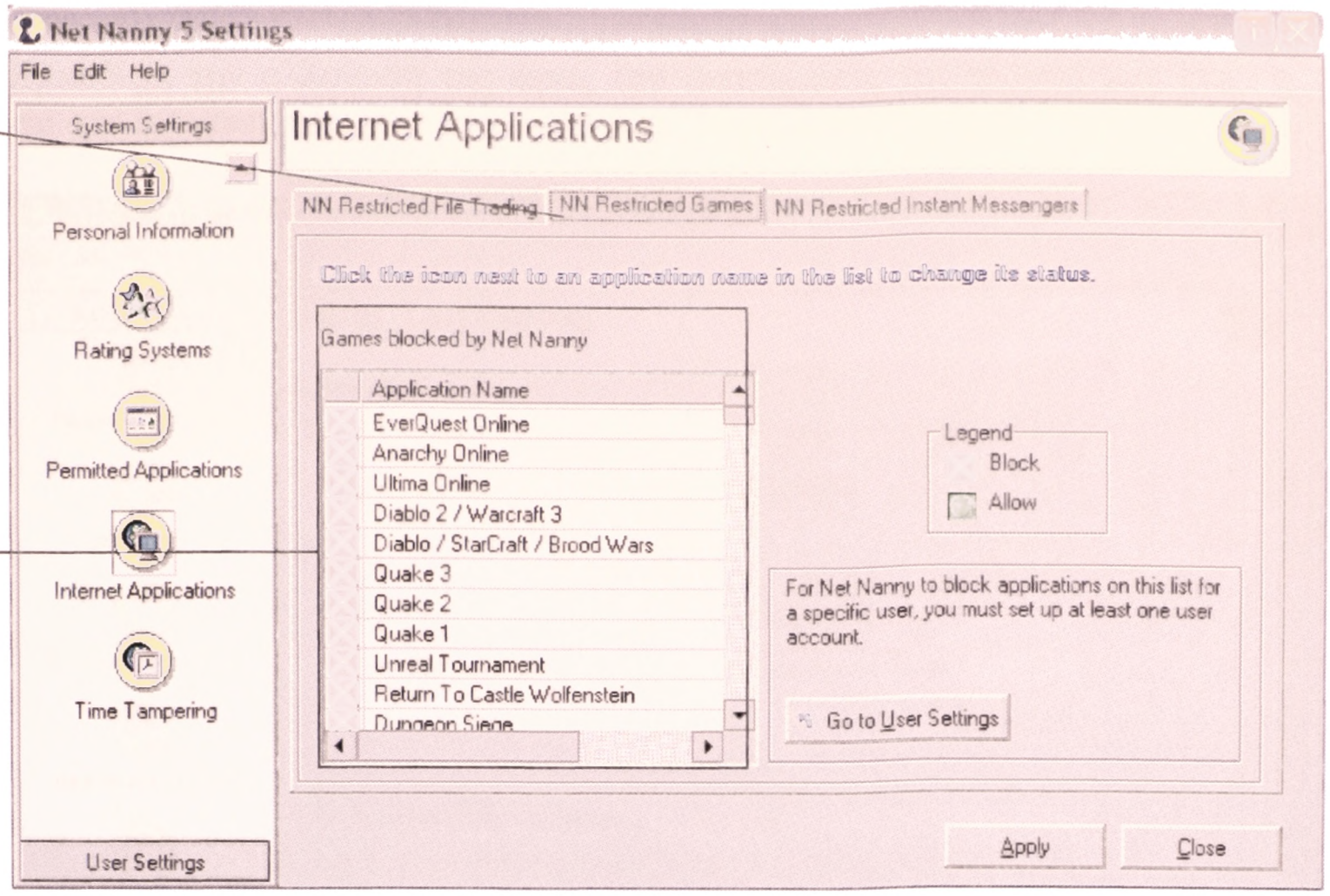
Net Nanny Restricted File Trading

Η λίστα του Net Nanny με τις εφαρμογές ανταλλαγής αρχείων οι οποίες πάντα μπλοκάρονται. Έχουμε τη δυνατότητα να επιτρέψουμε την πρόσβαση σε οποιαδήποτε από αυτές επιθυμούμε.



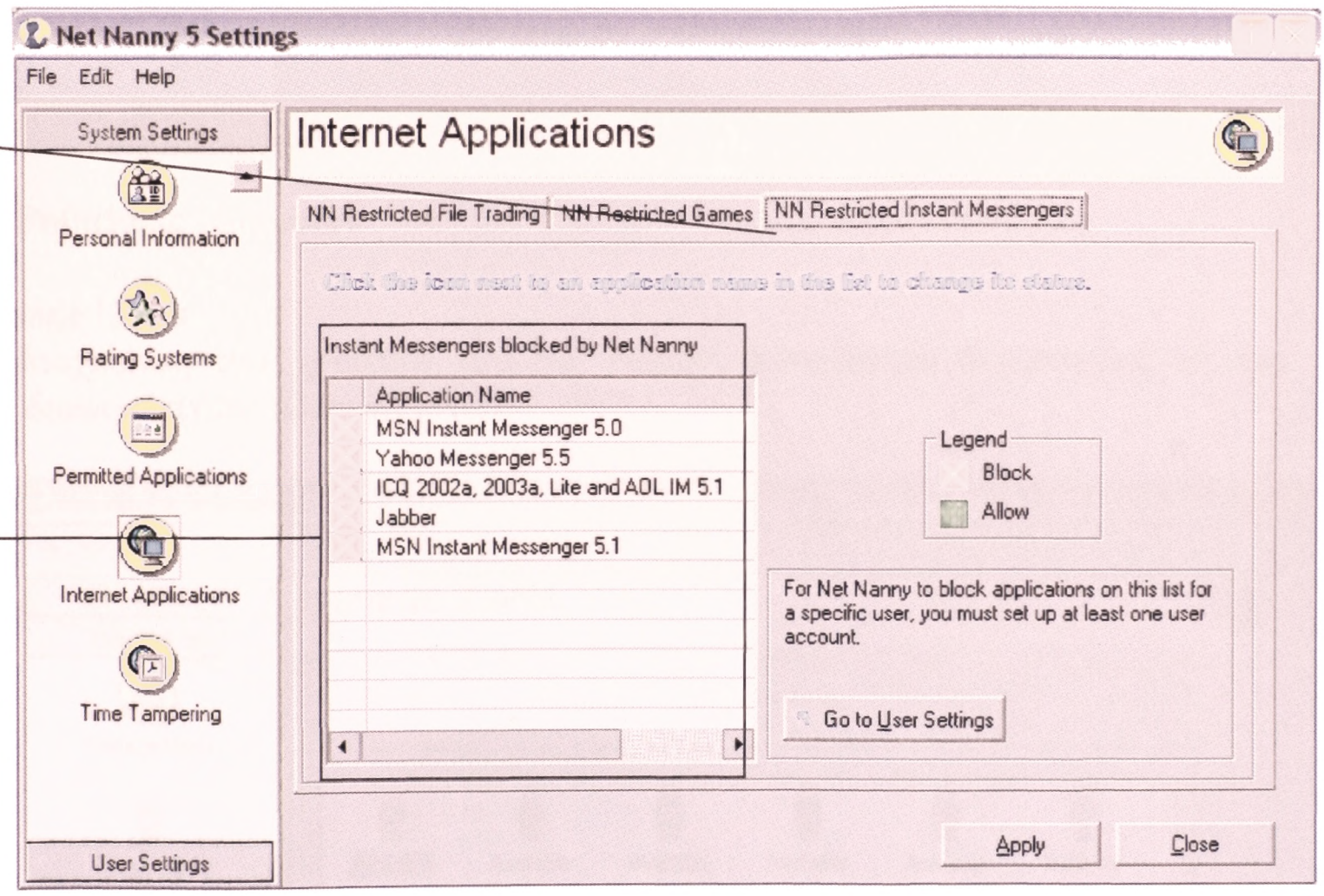
Net Nanny Restricted Games

Η λίστα του Net Nanny με τα διαδικτυακά παιχνίδια τα οποία πάντα μπλοκάρονται. Έχουμε τη δυνατότητα να επιτρέψουμε την πρόσβαση σε οποιαδήποτε από αυτά επιθυμούμε.




Net Nanny Restricted Instant Messengers

Η λίστα του Net Nanny με τις εφαρμογές ανταλλαγής μηνυμάτων οι οποίες πάντα μπλοκάρονται. Έχουμε τη δυνατότητα να επιτρέψουμε την πρόσβαση σε οποιαδήποτε από αυτές επιθυμούμε.

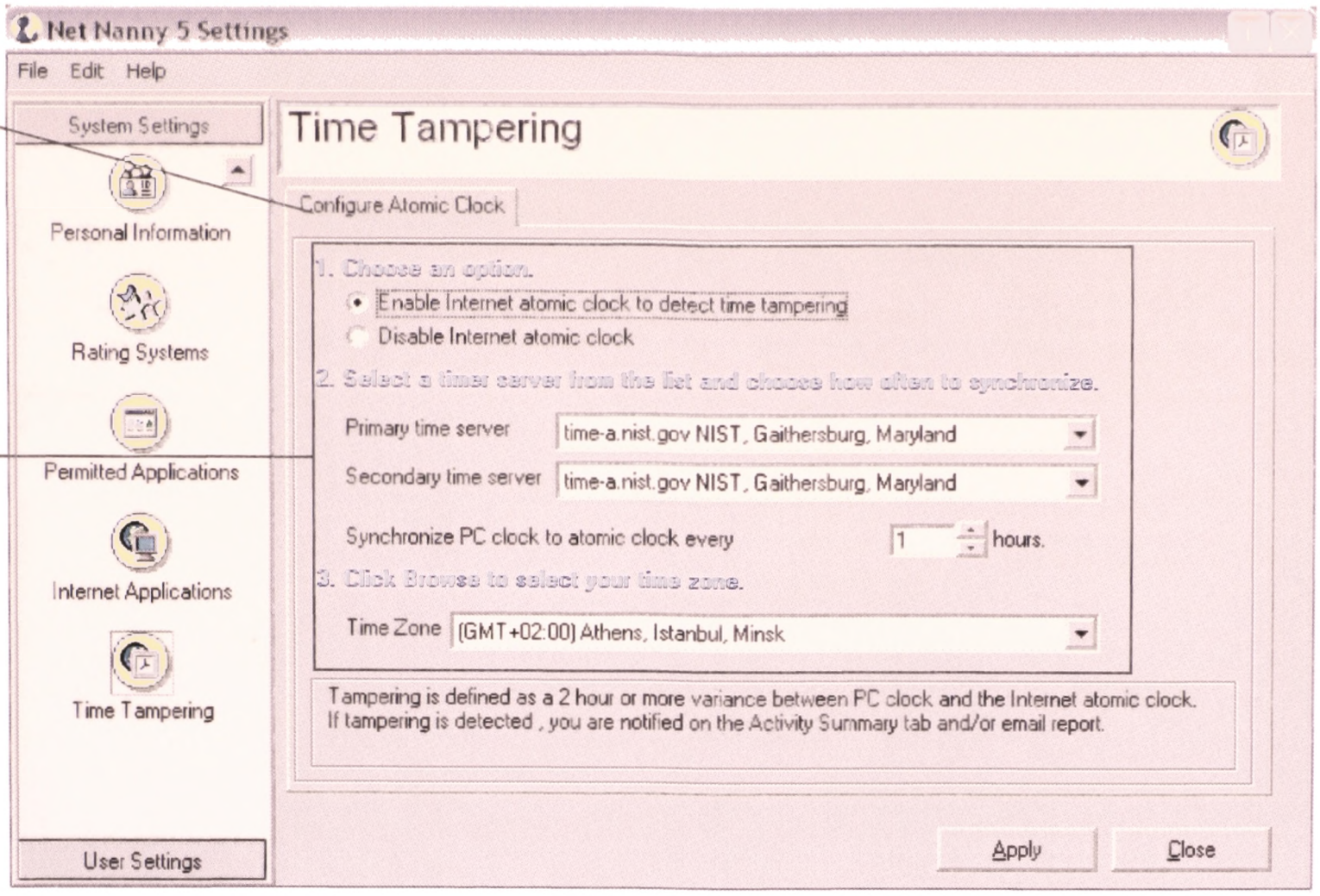


12. Time Tampering

Εμποδίζει την αλλοίωση της ώρας του συστήματος για περιπτώσεις όπου η πρόσβαση στο internet ενός χρήστη καθορίζεται με χρονοδιάγραμμα.

Configure Atomic Clock

Το Net Nanny χρησιμοποιεί κάποιον time server για να υπολογίσει την ώρα σύμφωνα με τη ζώνη ώρας που του έχουμε δώσει. Αν εντοπίσει διαφορά μεγαλύτερη των δυο ωρών τότε το καταγράφει και μας ενημερώνει. **Δεν** εμποδίζει την αλλοίωση της ώρας απλά καταγράφει την παράβαση.



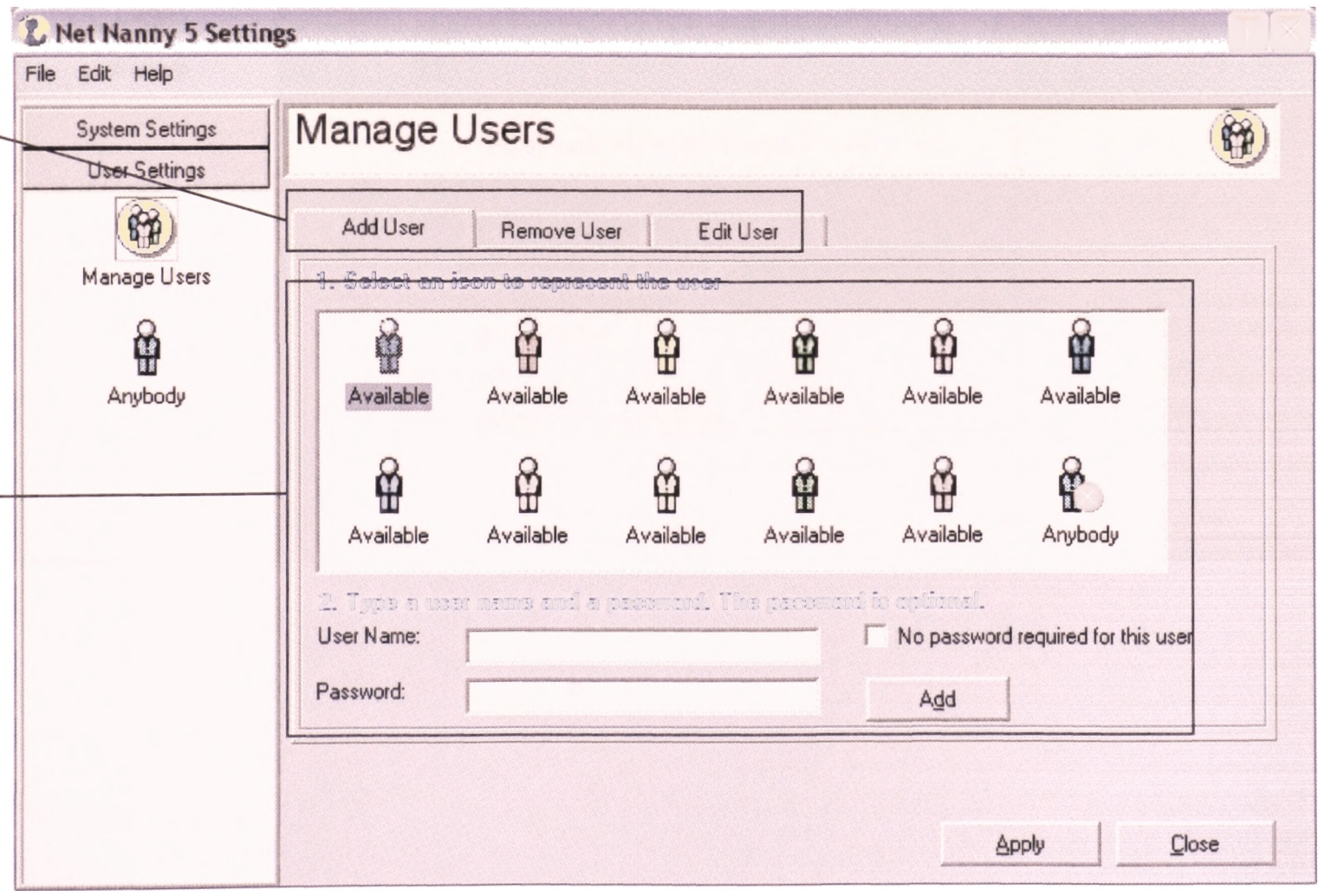

### 3.3.4.2 Ρυθμίσεις Χρηστών

1. Manage Users

Διαχείριση των χρηστών του Net Nanny. Δυνατότητα δημιουργίας ως και δώδεκα διαφορετικών ειδών χρηστών.

Add / Remove / Edit User

Μπορούμε να δούμε όλους τους χρήστες του Net Nanny. Έχουμε τη δυνατότητα να προσθέσουμε, να διαγράψουμε και να κάνουμε βασικές ρυθμίσεις (όνομα χρήστη, κωδικός πρόσβασης) ανά χρήστη.



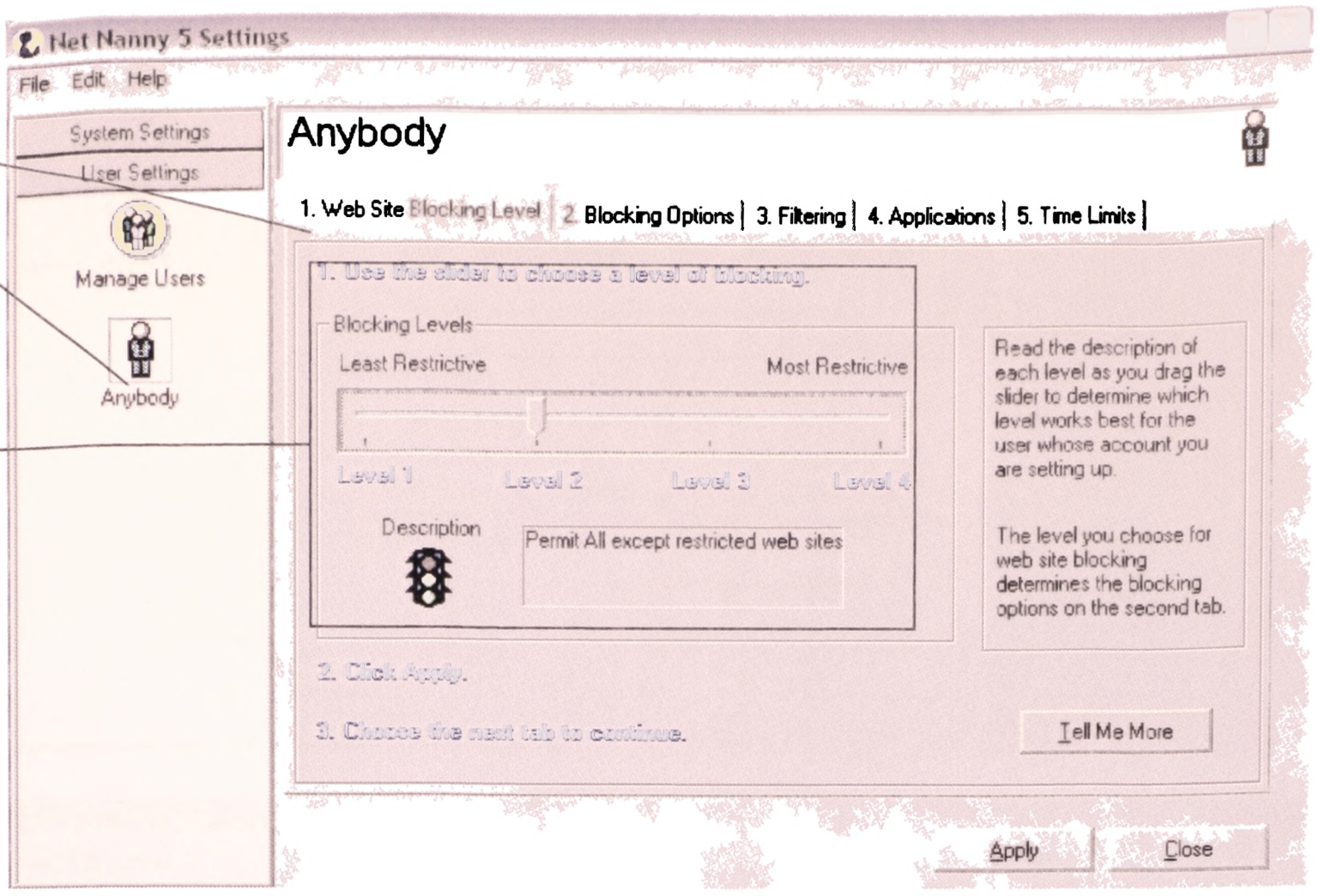
2. Users

Λεπτομερής παραμετροποίηση κάθε χρήστη.

Web Site Blocking Level

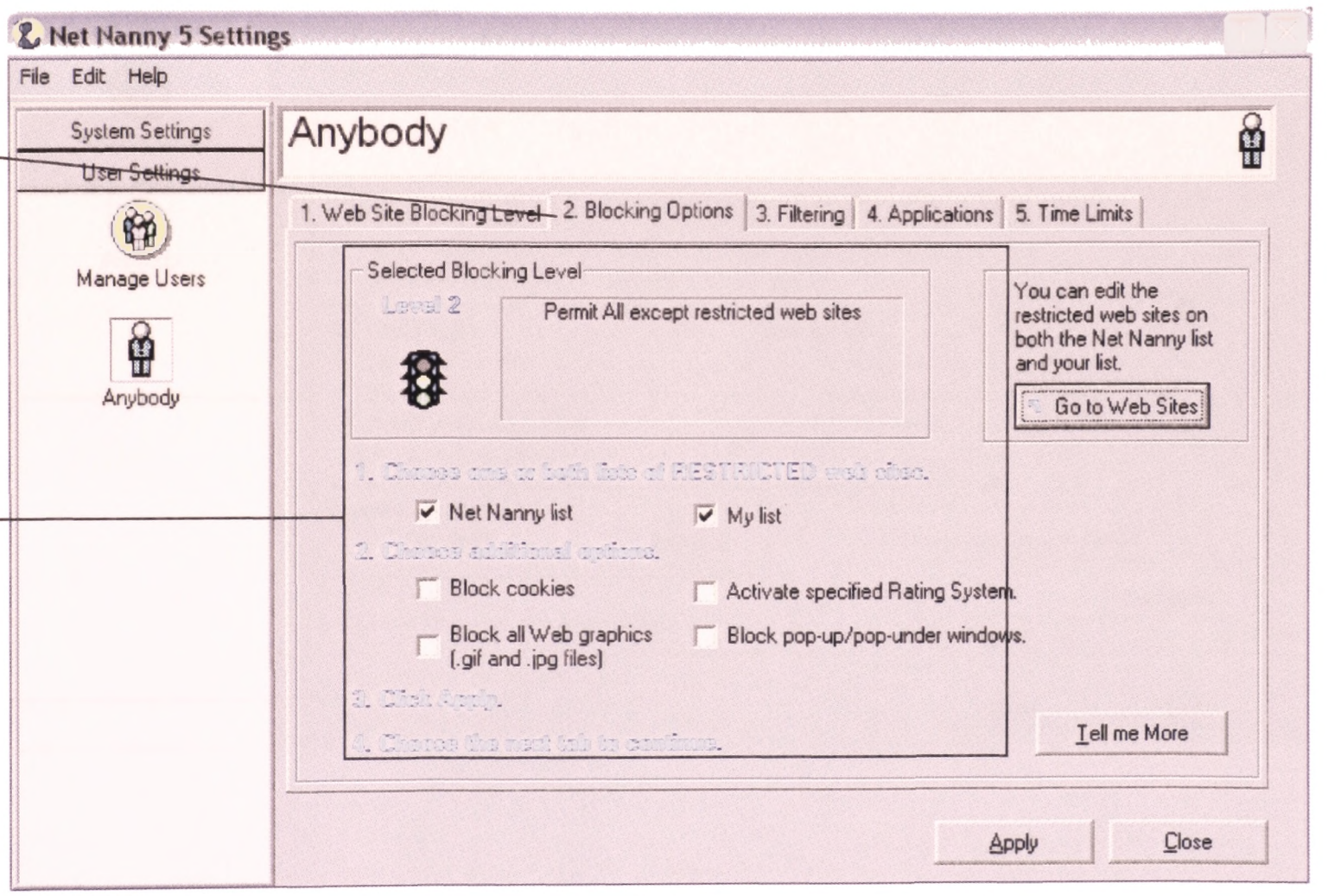
Χρήστης Anybody

Επιλέγουμε το επίπεδο αυστηρότητας με το οποίο μπλοκάρονται οι ιστοσελίδες. Τα επίπεδα είναι: Level 1: Permit all web sites, Level 2: Permit all except restricted web sites, Level 3: Block all except Family Friendly web sites, Level 4: Block all web sites.



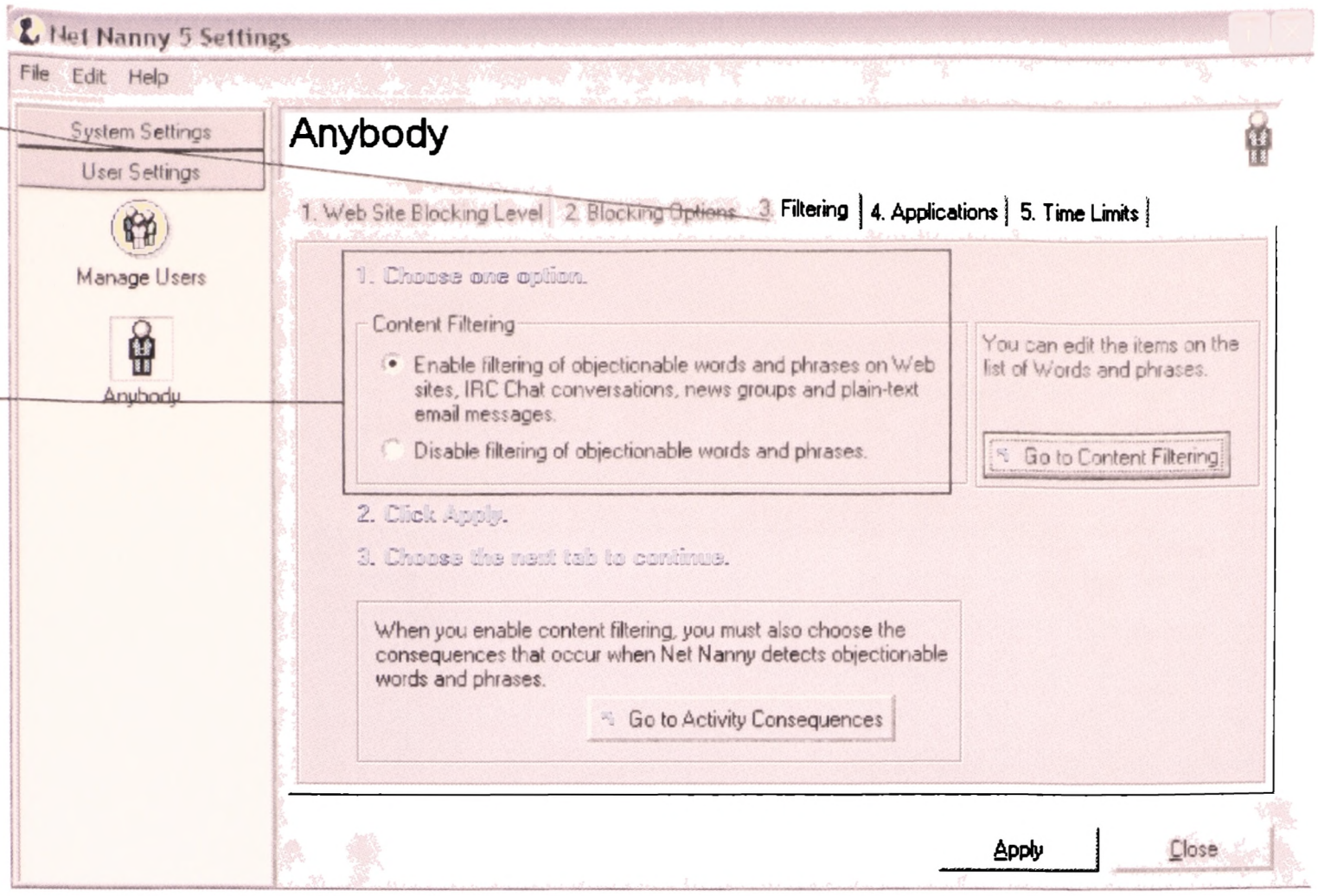

Blocking Options

Ρυθμίσεις μπλοκαρίσματος. Έχουμε τη δυνατότητα να επιλέξουμε ποιες λίστες θα χρησιμοποιούνται για το μπλοκάρισμα ιστοσελίδων (Net Nanny List, My List). Επίσης, αν θα μπλοκάρονται τα cookies, αν θα χρησιμοποιήσουμε κάποιο από τα δυο συστήματα βαθμονόμησης , αν θα μπλοκάρονται γραφικά (αρχεία .gif και .jpg) και αν θα μπλοκάρονται pop-up/pop-under παράθυρα. Κάποιες από αυτές τις ρυθμίσεις δεν είναι διαθέσιμες ανάλογα με το επίπεδο μπλοκαρίσματος που έχουμε επιλέξει για τον χρήστη (στην περίπτωση αυτή τον Anybody).



Filtering

Επιλέγουμε αν θέλουμε να φιλτράρονται λέξεις και φράσεις στις ιστοσελίδες, σε IRC Chat Rooms, σε Newsgroups και σε e-mail απλού κειμένου σύμφωνα με τη διαμορφωμένη λίστα του Net Nanny στο Content Filtering.

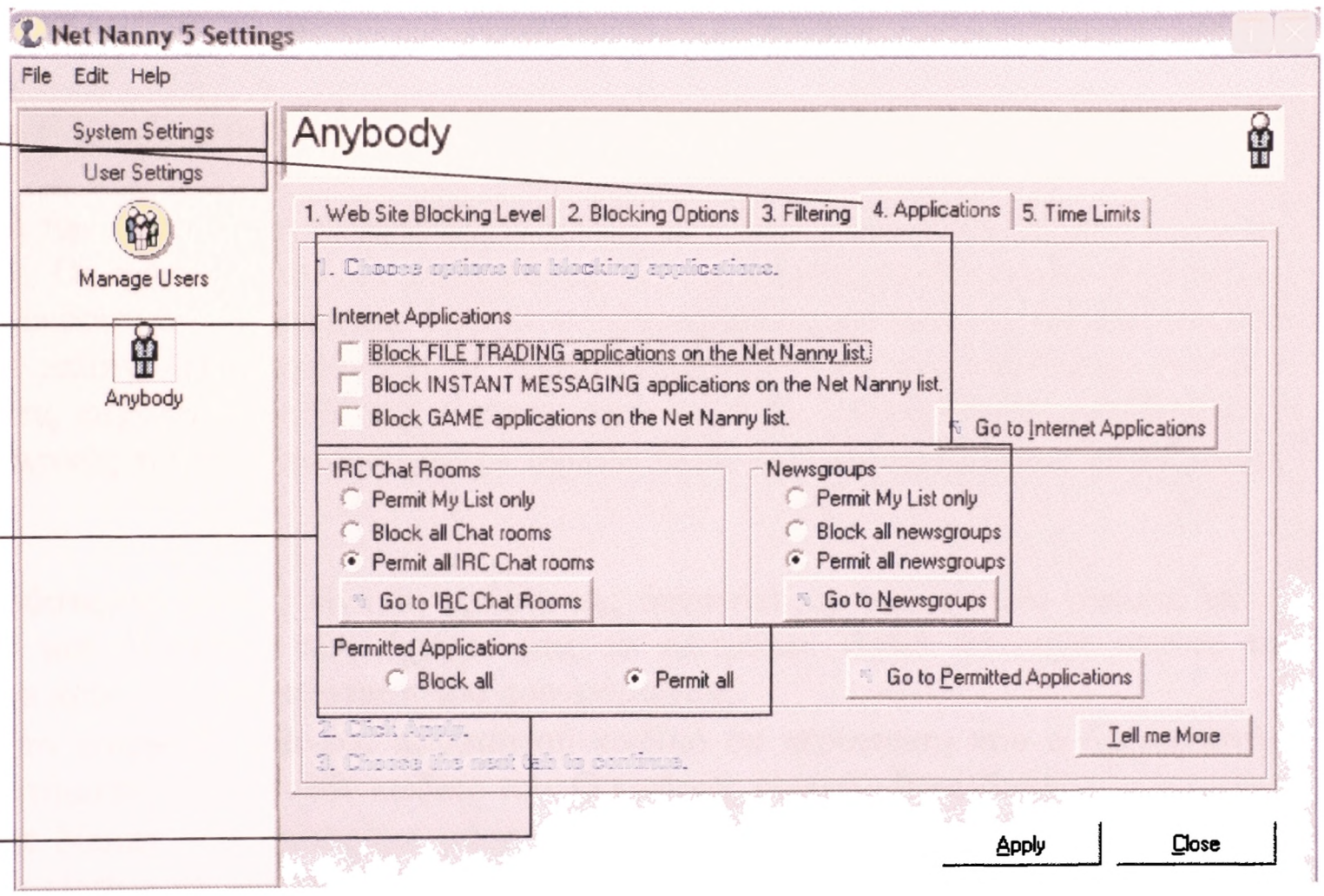


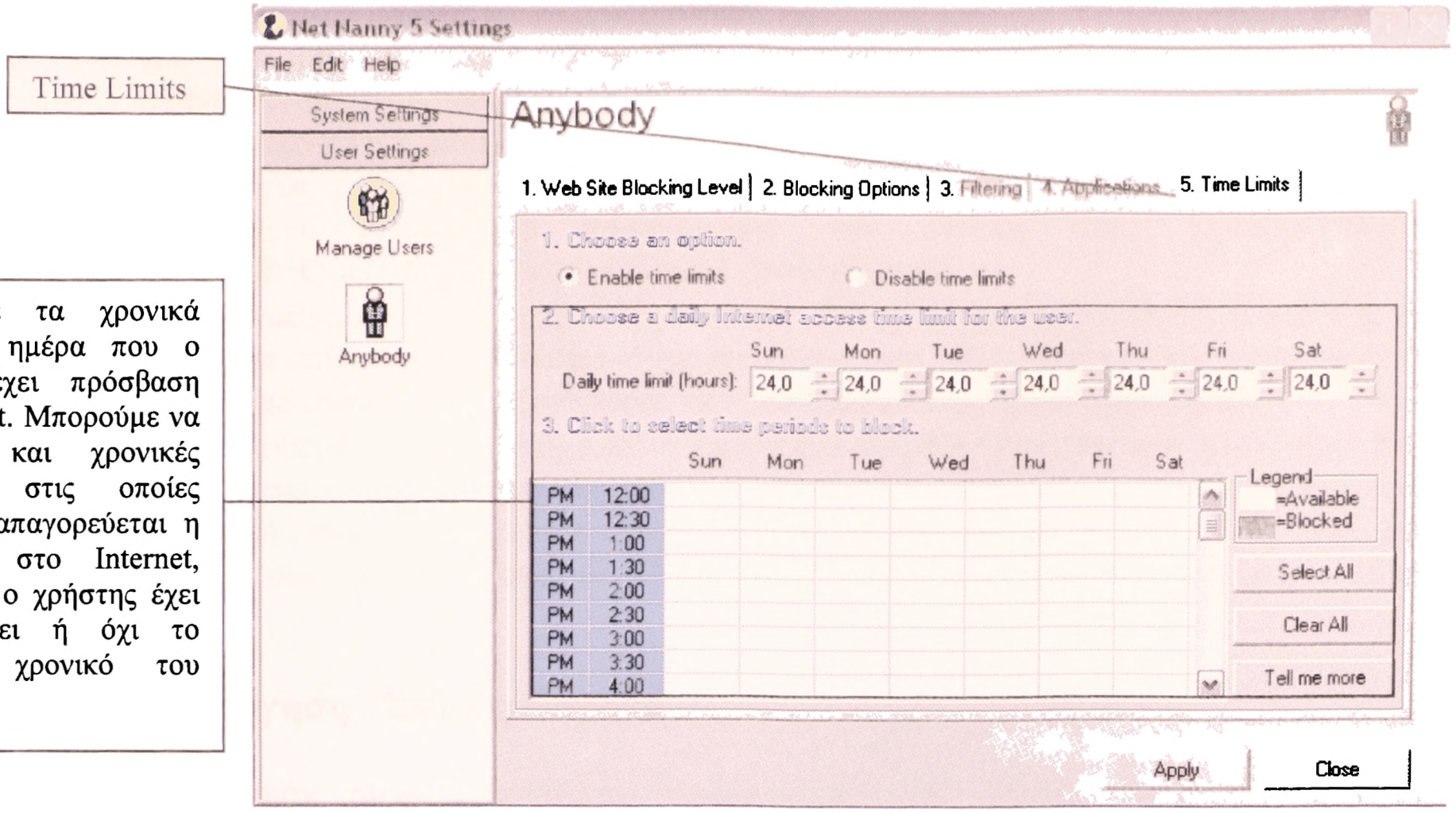

Applications

Επιλέγουμε ποιες κατηγορίες διαδικτυακών εφαρμογών επιθυμούμε να μπλοκάρονται.

Επιλέγουμε σε ποια IRC Chat Rooms και Newsgroups θα επιτρέπεται η πρόσβαση στον χρήστη

Επιλέγουμε αν η λίστα με τις επιτρεπόμενες εφαρμογές θα είναι διαθέσιμη σε αυτόν τον χρήστη.






## 3.3.5 Τρόποι Εξουδετέρωσης

Σε αυτή την ενότητα θα αναφερθούμε στους πιο γνωστούς τρόπους εξουδετέρωσης του Net Nanny. Οι τρόποι αυτοί δεν είναι πάντα το ίδιο αποτελεσματικοί και εξαρτώνται άμεσα από την έκδοση του λειτουργικού μας συστήματος καθώς και από την έκδοση του Net Nanny. Πολλοί επίσης λειτουργούν και σε εκδόσεις λειτουργικών και Net Nanny που δεν αναφέρονται στις παρακάτω μεθόδους. Επίσης, στην ενότητα 3.4 αναφέρεται αναλυτικά ο πιο αποτελεσματικός τρόπος «παράκαμψης» σχεδόν όλων των προγραμμάτων λογοκρισίας στο Internet.

- Ο απλούστερος τρόπος είναι η χρήση της δυνατότητας του system restore, αν η έκδοση των Windows που έχουμε μας το επιτρέπει. Απλά κάνουμε restore το σύστημα πριν την εγκατάσταση του προγράμματος.
- Υπάρχουν αναφορές για ένα πασπαρτού κωδικό σε περίπτωση που ο διαχειριστής του συστήματος ξεχάσει τον κωδικό του. Ο κωδικός είναι ο **~frontdoor**.
- Στα Net Nanny 4.0 μπορούμε μέσα από το msconfig να αφαιρέσουμε από την καρτέλα startup τα nntray.exe και NNSvsc. Μετά από επανεκκίνηση το Net Nanny έχει απενεργοποιηθεί. Αν έχουμε Windows XP και Net Nanny 5.0 τότε στην καρτέλα services βλέπουμε μόνο το NNSvc. Αφαιρώντας το δεν επιτυγχάνουμε τίποτα καθώς το Net Nanny μετά την επανεκκίνηση αντιλαμβάνεται την αλλαγή και τη διορθώνει, δηλαδή "Net Nanny Service is not running. To rectify the problem, Net Nanny Starter will try re-activating Net Nanny now. This may take a few minutes. Thank you for your patienc. System Code: 10003". Ανοίγουμε με Alt+Ctrl+Del τον Task Manager, πάμε στην καρτέλα processes και τερματίζουμε τις nntray.exe και NNSvc.exe, έτσι απενεργοποιούμε την λειτουργία του Net Nanny για το session μας.
- Στα Windows 95 πατάμε Alt+Ctrl+Del για να ανοίξουμε την λίστα με τα προγράμματα που είναι φορτωμένα στη μνήμη. Ανάλογα από την έκδοση του Net Nanny που έχουμε τα OCRAWARE ή Wnldr32 θα φαίνονται στην λίστα. Τερματίζουμε τη λειτουργία τους για να απενεργοποιήσουμε το Net Nanny για το session σας.

- Ανοίγουμε το αρχείο c:\windows\system.ini. Κάτω από την ετικέτα [boot] υπάρχει μια γραμμή με όνομα "drivers=". Αφαιρούμε το wndrv16.dll και κάνουμε επανεκκίνηση στον υπολογιστή.
- Για υπολογιστές που χρησιμοποιούν ακόμη το αρχείο config.sys (κυρίως σε συστήματα με dos και windows 3.x), ανοίγουμε το αρχείο και στη γραμμή DEVICE=C:\nn\nndrv.sys προσθέτουμε την εντολή rem. Δηλαδή REM DEVICE=C:\nn\nndrv.sys και κάνουμε επανεκκίνηση.
- Για να καθαρίσουμε το ημερολόγιο του Net Nanny σβήνουμε το αρχείο Wnn3.log, το οποίο θα πρέπει να βρίσκεται στον κατάλογό του (Net Nanny). Δεν μπορούμε να σβήσουμε συγκεκριμένες εγγραφές γιατί το αρχείο είναι κρυπτογραφημένο.
- Στην περίπτωση που τίποτα από τα παραπάνω δεν δουλέψει για τον συνδυασμό του λειτουργικού μας συστήματος και Net Nanny μπορούμε να δοκιμάσουμε κάτι πιο δραστικό όπως να σβήσουμε κάποια αρχεία επιλεκτικά από τον κατάλογο του Net Nanny όπως το nntray.exe, το NNSvc.exe ή και ακόμα όλο τον κατάλογο του Net Nanny.

### 3.3.6 Αξιολόγηση / Συμπεράσματα

Το προϊόν αυτό απευθύνεται αποκλειστικά για ιδιωτικά περιβάλλοντα, μη επαγγελματικά και κυρίως οικογενειακά. Είναι πολύ απλό στην εγκατάσταση και χρήση, οι αναφορές του είναι ολοκληρωμένες και έχει συμφέρουσα τιμή. Ένα από τα σημαντικότερα πλεονεκτήματά του αλλά, συγχρόνως και μειονέκτημα είναι οι ελεύθερες σε πρόσβαση λίστες του. Το Net Nanny καταφέρνει με αυτό τον τρόπο κάτι για το οποίο αυτά τα προϊόντα κατακρίνονται· την απαλοιφή των κρυπτογραφημένων λιστών, των οποίων ο διαχειριστής του προγράμματος δεν βλέπει τα περιεχόμενά τους, αφαιρώντας από αυτόν ένα από τα σημαντικότερα δικαιώματα του ατόμου, τη συμμετοχή του στην απρόσκοπτη και πολυμερή πληροφόρηση. Από την άλλη, η λίστα του Net Nanny με τις μπλοκαρισμένες ιστοσελίδες δεν ξεπερνάει τις 5000, όταν οι ανταγωνιστές του πλησιάζουν και πολλές φορές ξεπερνάνε τις 100.000. Επειδή η δημιουργία αυτών των λιστών είναι αποτέλεσμα πολλών ωρών εργασίας η κάθε εταιρία θεωρεί ότι πρέπει να προστατεύει τη λίστα που με μεγάλο κόπο και κόστος συντάσσει καθημερινά και ενημερώνει τα προϊόντα της. Στην περίπτωση του Net Nanny η μικρή σε μήκος λίστα σε συνδυασμό με το γεγονός ότι καλύπτεται σχεδόν πλήρως από τους ανταγωνιστές του κάνει την Bionet Systems να μην έχει κανένα λόγο να κρυπτογραφήσει την λίστα της καθώς αποτελεί προϊόν ελάχιστου χρόνου, κόπου και κόστους.

Οι κατηγορίες στις οποίες διαχωρίζει το περιεχόμενο των ιστοσελίδων είναι οι εξής 5: Sexual Explicitness, Hate, Violence, Crime και Drugs. Σημαντικό είναι το γεγονός ότι μόνο η αγγλική γλώσσα υποστηρίζεται, ενώ σε δοκιμές που έγιναν προσθέσαμε μια Ελληνική λέξη στην λίστα η οποία πέρναγε το φίλτρο ανενόχλητη.

## 3.4 Γενικά συμπεράσματα / Συγκριτική αξιολόγηση

### 3.4.1 Γενικά συμπεράσματα

Είναι κοινά αποδεκτό, λαμβάνοντας υπόψη μελέτες και έρευνες, ότι το Διαδίκτυο αποτελεί το ισχυρότερο και δημοφιλέστερο επικοινωνιακό μέσο στη σύγχρονη εποχή. Στις μέρες μας, όλο και περισσότερα άτομα, προερχόμενα από διαφορετικά πολιτιστικά, οικονομικά και κοινωνικά υπόβαθρα, αλλά και διαφορετικών ηλικιακών επιπέδων, γίνονται μέτοχοι της δικτυακής κοινωνίας, μέσω της χρήσης του Internet.

Η αύξηση του αριθμού των χρηστών του Διαδικτύου, σε ποσοτικό αλλά και ποιοτικό επίπεδο, σε συνδυασμό με το γεγονός ότι η προστασία των ατομικών δικαιωμάτων και ο σεβασμός της ανθρώπινης αξιοπρέπειας αποτελεί αναγκαιότητα της σύγχρονης εποχής,

οδηγεί όλο και περισσότερο τις εταιρείες να παράγουν προγράμματα που στόχο έχουν να διασφαλίζουν την προστασία των «ευπαθών ομάδων» από την έκθεσή τους σε ακατάλληλα και επιβλαβή περιεχόμενα πληροφοριών. Τα προγράμματα αυτά τείνουν να μεταμορφώνονται με την πάροδο του χρόνου και την αύξηση των απαιτήσεων σε ολοκληρωμένες λύσεις λειτουργικότητας και ασφάλειας δικτύων. Με άλλα λόγια φροντίζουν όχι μόνο για τον έλεγχο του περιεχομένου αλλά και για την προστασία του δικτύου από άγνωστες απειλές, επιβλαβείς σελίδες και ιομορφικό λογισμικό. Επίσης παρατηρούν και ενημερώνουν τον διαχειριστή του δικτύου με σκοπό την επίτευξη της αποτελεσματικότερης και ασφαλέστερης χρήσης των πόρων του.

Στις παραπάνω ενότητες παρουσιάστηκαν μερικά από τα βασικότερα προγράμματα λογοκρισίας που κυκλοφορούν στην αγορά μέχρι σήμερα, ενώ πιο κάτω θα επιχειρήσουμε μια συγκριτική αξιολόγησή τους.

### 3.4.2 Συγκριτική Αξιολόγηση

Από τα προγράμματα που προαναφέρθηκαν, το Net Nanny 5.0 δεν μπορεί να συγκριθεί αναλογικά με τα άλλα δύο (Websense Enterprise v5.0, MIMEsweeper for Web 5.0), για το λόγο ότι το συγκεκριμένο απευθύνεται σε ιδιωτικά και κυρίως οικογενειακά περιβάλλοντα, ενώ τα υπόλοιπα σε μεγάλα επιχειρησιακά περιβάλλοντα. Παρ'όλα αυτά το Net Nanny 5.0 αποτελεί μια ολοκληρωμένη και αρκετά αποτελεσματική εφαρμογή λογοκρισίας. Είναι απλό στην εγκατάσταση και στη χρήση του, με ολοκληρωμένες αναφορές και αρκετά συμφέρουσα τιμή.

Από την πλευρά τους τα Websense Enterprise v5.0 και MIMEsweeper for Web 5.0 είναι εφαρμογές που χρησιμοποιούνται από μεγάλα επιχειρησιακά δίκτυα, αποτελούμενα από έως και 10.000 χρήστες. Αν επιχειρήσουμε μια σύγκριση μεταξύ των δύο αυτών προγραμμάτων, θα τολμήσουμε να πούμε ότι το Websense Enterprise v5.0 υπερέχει του MIMEsweeper for Web 5.0. Η υπεροχή του Websense Enterprise v5.0 έγκειται κυρίως στο γεγονός ότι αποτελεί μια πιο σύνθετη και πολύπλοκη εφαρμογή, τόσο ως προς την εγκατάσταση, τον εξοπλισμό και το υλικό του, όσο και ως προς τις δυνατότητές του με ένα μηχανισμό φιλτραρίσματος που ενσωματώνεται σε όλους τους τύπους δικτύου, ώστε να μπορεί να εφαρμόζει τις πιο πολύπλοκες πολιτικές φιλτραρίσματος με απόλυτη επιτυχία.

Παρ΄όλα αυτά δεν θα πρέπει να υποτιμήσουμε το MIMEsweeper for Web 5.0., καθώς η βάση δεδομένων του, τα εργαλεία αναφορών του και οι πολιτικές που χρησιμοποιεί, είναι αρκετά αποτελεσματικές, χωρίς ωστόσο να φτάνουν απόλυτα το επίπεδο του Websense Enterprise v5.0. Αυτό σημαίνει ότι ο μηχανισμός ανανέωσης της βάσης δεδομένων του Websense Enterprise v5.0 φαίνεται να είναι πιο δυναμικός με τη χρήση του WebCatcher και τα εργαλεία των αναφορών πιο λειτουργικά με τη βοήθεια του Explorer.

Συμπερασματικά, θα μπορούσαμε να πούμε ότι η πλήρης ανάπτυξη της πλατφόρμας Websense Enterprise v5.0 προσφέρει τη βέλτιστη προστασία με μηχανισμούς παρακολούθησης και βελτίωσης της απόδοσης του δικτύου. Για την επίτευξη όμως αυτού του αποτελέσματος το κόστος σε υλικό και σχεδιασμό είναι σαφώς μεγαλύτερο από του MIMEsweeper for Web 5.0. Από την άλλη πλευρά, αν και το MIMEsweeper for Web 5.0. λειτουργεί και ενσωματώνεται στο δίκτυο σαν ένας proxy server, οι δυνατότητές του περιορίζονται σε HTTP και browser FTP κίνηση, με αποτέλεσμα να καθίσταται αναγκαία η ύπαρξη και των υπολοίπων εφαρμογών της Clearswift για ολοκληρωμένο φιλτράρισμα. Τέλος, όταν χρησιμοποιείται μόνο ένας MIMEsweeper proxy server για το φιλτράρισμα παρατηρούνται φαινόμενα αυξημένης κίνησης και δημιουργείται ένα σημείο δυνητικής αποτυχίας της ολοκληρωμένης λειτουργίας του δικτύου.

## 3.5 Cencoware Circumventor

**Πηγή: peacefire.org**

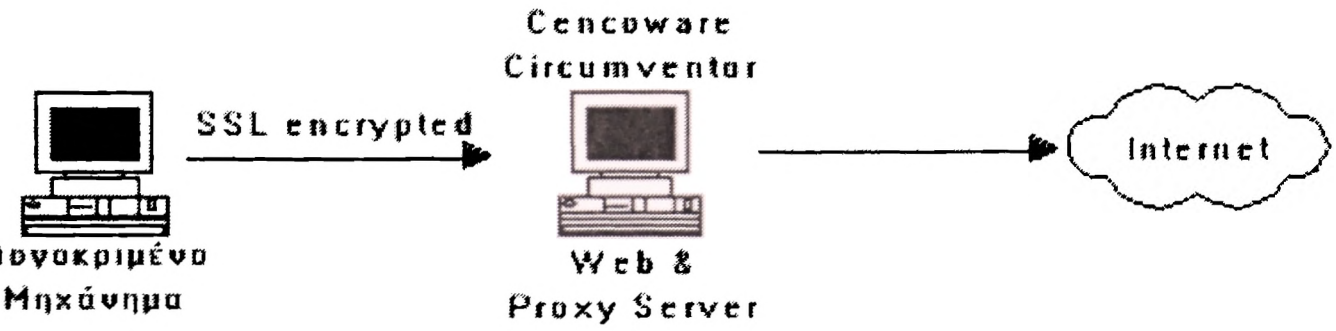
Πρόκειται για μια μικρή ομάδα προγραμμάτων που μας επιτρέπει να παρακάμπτουμε όλα τα γνωστά είδη προγραμμάτων και τεχνολογιών λογοκρισίας. Είναι ίσως ο πιο ολοκληρωμένος και αποτελεσματικός τρόπος και δεν επιφέρει καμία αλλαγή ή επιβάρυνση στο σύστημά μας.

### 3.5.1 Παράμετροι

Ο Circumventor πρέπει να εγκατασταθεί σε ένα υπολογιστικό σύστημα το οποίο δεν λογοκρίνεται με κανένα τρόπο. Δηλαδή αν πρόκειται για τον προσωπικό μας υπολογιστή π.χ. να μην έχει εγκατεστημένο κάποιο από τα Net Nanny / Cyber Patrol / CYBERsitter, να μην βρισκόμαστε μέσα σε κάποιες από τις χώρες που λογοκρίνουν το περιεχόμενο των ιστοσελίδων που επιτρέπεται να βλέπουν οι κάτοικοί τους, π.χ. Κίνα και Σαουδική Αραβία και τέλος να μην ανήκουμε σε δίκτυο στο οποίο λειτουργεί κάποιο πρόγραμμα λογοκρισίας, όπως π.χ. σε σχολεία ή και επαγγελματικά περιβάλλοντα. Επίσης, το μηχάνημα στο οποίο θα εγκατασταθεί πρέπει να έχει Windows Xp ή 2000, να έχει μια συνεχή σύνδεση στο Intrenet, όπως DSL ή μισθωμένο κύκλωμα και είναι θετικό να έχει και στατική IP διεύθυνση.

### 3.5.2 Λειτουργία

Ο Circumventor μετατρέπει έναν υπολογιστή σε Web Server ο οποίος λειτουργεί και σαν proxy. Όταν ολοκληρωθεί η εγκατάσταση μας δίνεται ένα URL με το οποίο μπορούμε να επισκεφτούμε τον Server μας. Αυτό το URL χρησιμοποιούμε από ένα λογοκριμένο μηχάνημα για να επισκεφτούμε την ιστοσελίδα στον server μας η οποία τρέχει ένα script το οποίο διαθέτει ένα κενό πεδίο. Μέσα σε αυτό το πεδίο συμπληρώνουμε την διεύθυνση της σελίδας στην οποία ως εκείνη την στιγμή δεν είχαμε πρόσβαση. Τα υπόλοιπα τα αναλαμβάνει ο Circumventor για να μας φέρει τη σελίδα. Επίσης εγκαθιστούμε και ένα SSL πιστοποιητικό για να κρυπτογραφείται η επικοινωνία μας με τον server σε περίπτωση που μεταφέρονται ευαίσθητες πληροφορίες.




εικ. 1 Σχηματική δομή

### 3.5.3 Εγκατάσταση

1. Εγκαθιστούμε την Active Perl στο μηχάνημα (www.perl.com)
2. Εγκαθιστούμε το OpenSA – Open Server Architecture. Πρόκειται για έναν Open Source Web Server βασισμένο στον Apache. (www.opensa.org)
3. Τέλος, εγκαθιστούμε ένα Perl script με όνομα CGIProxy και το SSL πιστοποιητικό. Για τη διευκόλυνση μας και τα δυο εγκαθίστανται με το αρχείο circumventor-setup.exe, το οποίο βρίσκεται στο www.peacefire.org.

# ΕΠΙΛΟΓΟΣ

Το Διαδίκτυο (Internet), είναι ένα δυνατό επικοινωνιακό μέσο, που μπορεί να χρησιμοποιηθεί για να προάγει την αμερόληπτη ανάπτυξη και να προστατέψει τα ανθρώπινα δικαιώματα παντού. Λαμβάνοντας υπόψη την αυξανόμενη δύναμη και επιρροή που αποκτά συνεχώς, θα πρέπει να είναι ένα εργαλείο, που να συντελεί στην πρόοδο της ανθρώπινης γνώσης και επιστήμης και στην προαγωγή του κοινού καλού των κοινωνικών συνόλων .

Για την επίτευξη των πιο πάνω βασικό παράγοντα αποτελεί η προστασία των χρηστών από την ανεξέλεγκτη έκθεσή τους σε επιβλαβή περιεχόμενα. Η λογοκρισία λοιπόν, αν και σαν έννοια παραπέμπει αλλού, στο χώρο του Διαδικτύου μοιάζει να είναι απαραίτητο στοιχείο, προκειμένου να γίνεται σωστή χρήση των πόρων του από κάθε είδους κοινό. Το παραπάνω είναι εφικτό βέβαια, μόνο αν η λογοκρισία εφαρμόζεται κατά τέτοιο τρόπο, ώστε να προωθεί τα κοινωνικά συμφέροντα, να μην περιορίζει τις ατομικές και κοινωνικές ελευθερίες και να προστατεύει τις «ευπαθείς ομάδες». Επιπλέον, σημαντικό είναι ο χρήστης του Διαδικτύου να είναι ενήμερος για το πού και για ποιους λόγους εφαρμόζεται η λογοκρισία στις συγκεκριμένες πληροφορίες. Τέλος, απαραίτητη προϋπόθεση για την επιτυχή εφαρμογή τέτοιων πολιτικών είναι να αποτελούν αυτές οι πολιτικές προϊόν διαλόγου και συνεργασίας μεταξύ όλων των δημόσιων και κοινωνικών φορέων, είτε πρόκειται για την πολιτεία και τα νομικά όργανα, είτε για εκπαιδευτικούς φορείς, ή ακόμα και για τους απλούς πολίτες των εκάστοτε πραγματικών και διαδικτυακών κοινωνιών.

Η λογοκρισία στο Διαδίκτυο αποτελεί μια δικλείδα ασφαλείας των ηθικών αξιών των ατόμων και των κοινωνιών. Παρ΄όλα αυτά όμως, παρατηρούμε ότι οι εφαρμογές υψηλών δυνατοτήτων που κυκλοφορούν στην αγορά και σχετίζονται με αυτό το αντικείμενο απευθύνονται σε μεγάλα επιχειρησιακά περιβάλλοντα. Το γεγονός αυτό θέτει προβληματισμούς όσον αφορά τις αιτίες για τις οποίες χρησιμοποιούνται αυτές οι εφαρμογές, οι οποίες παύουν να είναι μόνο ηθικής προέλευσης, αλλά επεκτείνονται και στο οικονομικό επίπεδο.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


McCrea P., Smart B., Andrews M.. "*Blocking Contenet on the Internet: A Technical Perspective*", Report prepared for the Australian National Office for the Information Economy, http://www.cmis.csiro.au/reports/blocking.pdf, June 1998

Resnick P., Miller J., "*PICS: Internet Access Controls Without Censorship*", Communications of the ACM, Vol.39, No 10, pp.87-93, October 1996

Paul Greenfield, Phillip McCrea. "*Shuping Ran-Access Preventation Techniques for Internet Content Filtering*", http://www.cmis.csiro.au/reports/filtering.pdf

http://www.epe.org.gr/showarticle.jsp?articleid=67, "Πρακτικά Μέτρα Προστασίας από τις «Κακοτοπιές» στο Internet", Μάρτιος 2003

http://www.anthropos.gr/show_news.asp?Id=1351, "*Silenced: an international report on sensorship and control of the Internet*", September 2003

http://www.w3.org/PICS

http://www.websense.com

http://www.clearswift.com

http://www.peacefire.org

http://www.perl.com

http://www.opensa.org

http://www.netnanny.com