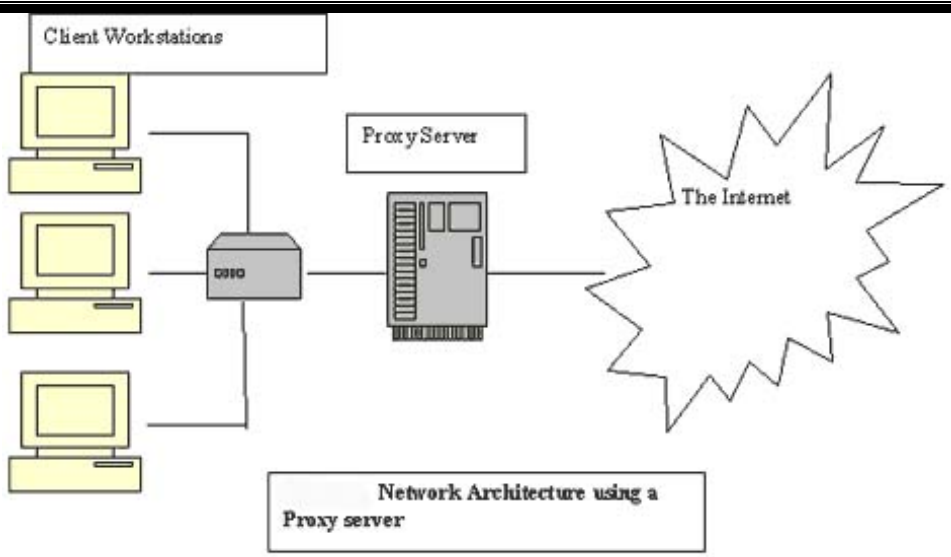
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Ηπείρου

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ ( Σ.Δ.Ο)
***ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ***

SCHOOL OF MANAGEMENT AND ECONOMICS
***DEPARTMENT OF COMMUNICATIONS, INFORMATICS AND MANAGEMENT***

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

## ΔΙΑΧΕΙΡΙΣΗ ΔΙΑΚΟΜΙΣΤΩΝ ΔΙΑΜΕΣΟΛΑΒΗΣΗΣ ΣΕ ΚΑΤΑΝΕΜΗΜΕΝΑ ΠΕΡΙΒΑΛΛΟΝΤΑ




**ΤΟΥ ΣΠΟΥΔΑΣΤΗ:**
***ΒΛΑΧΟΓΙΑΝΝΗΣ ΒΑΣΙΛΕΙΟΣ Α.Μ:3502***

**ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:**
ΒΑΣΙΛΕΙΑΔΗΣ ΔΗΜΗΤΡΙΟΣ

**ΔΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:**
ΡΙΖΟΣ ΓΕΩΡΓΙΟΣ
ΣΤΕΡΓΙΟΥ ΕΛΕΥΘΕΡΙΟΣ

## ΑΡΤΑ ΑΠΡΙΛΙΟΣ 2006

# ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

**ΠΕΡΙΕΧΟΜΕΝΑ**.....3

**ΠΡΟΛΟΓΟΣ**..... 5

**1.ΕΙΣΑΓΩΓΗ** ..... 6

**1.1 Τι είναι ένας proxy server;** ..... 6

**1.2 Τι προσφέρει ένας proxy server;** ..... 6

**1.3 Τι είναι ο ανώνυμος proxy server;**..... 7

**1.4 Ο proxy server που βρήκες είναι αληθινά ανώνυμος;** ..... 8

**1.4.1 Παράδειγμα 1 (απ΄ ευθείας σύνδεση)**..... 9

**1.4.2 Παράδειγμα 2 (transparent (=διαφανής) proxy)**..... 10

**1.4.3 Παράδειγμα 3 (ανώνυμος proxy+proxomitron 4.4)**..... 10

ΣΗΜΕΙΩΣΕΙΣ..... 10

**1.5 Reverse Proxy**..... 12

**2. Υπηρεσίες Proxy**..... 15

**2.1 Υπηρεσίες Proxy σε ένα Dual-homed Host.**..... 15

**2.2 Φιλτράρισμα πακέτων**..... 16

**2.2.1 ΦΙΛΤΡΑ ΠΕΡΙΟΧΗΣ** ..... 18

**2.3 ΧΡΗΣΗ ΚΡΥΦΗΣ ΜΝΗΜΗΣ**..... 19

**2.4 ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ WEB PROXY SERVER** ..... 20

**2.4.1 Χρήση κρυφής μνήμης του web proxy.**..... 20

**2.5 ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ**..... 21

**2.6 Ασφάλεια**..... 22

**3. Μετάφραση διεύθυνσης δικτύου** ..... 23

**3.1 IP διευθύνσεις και εσωτερικά δίκτυα** ..... 23

**4. PROXY SERVER** ..... 24

**4.1 Διακομιστές διαμεσολάβησης- Proxy Servers**..... 26

**4.2 Πώς λειτουργούν οι Proxy Servers και οι Transparent Proxy Servers** ..... 27

**4.3Παραδοσιακό Proxy**..... 27

**4.4 Διαφανής Proxy (Transparent proxy)**..... 27

**4.5 Χαρακτηριστικά ενός Caching Proxy Server**..... 28

**4.6 Authentication (Αυθεντικοποίηση)** ..... 28

**5. ΕΓΚΑΤΑΣΤΑΣΗ PROXY SERVER**..... 29

**5.1 Ρύθμιση του proxy server** ..... 31

**5.1.1 Διαμόρφωση του Internet Explorer** ..... 31

**5.2 ΔΙΑΧΕΙΡΙΣΗ PROXY SERVER** ..... 33
**5.3 Φιλτράρισμα αιτήσεων** ..... 34
**5.4 Φιλτράρισμα απαντήσεων** ..... 355
**5.5 Prefetching** ..... 366
**5.6 Μετάφραση και Μετατροπή κώδικα** ..... 37
**5.7 Σχηματισμός Κίνησης (Traffic Shaping)** ..... 37
**6. Κρυφός Αντιπρόσωπος (proxy cache)** ..... 38
**6.1 Transparent Caching** ..... 41
**6.2 Πλεονεκτήματα της διαφανούς Caching** ..... 41
**6.3 Μειονεκτήματα της διαφανούς caching** ..... 42
**6.4 Η Δρομολόγηση** ..... 43
**7. Σχετικές Μελέτες Πάνω σε Κρυφούς Αντιπροσώπους** ..... 44
**7.1 Συνεργαζόμενοι Κρυφοί Αντιπρόσωποι** ..... 41
**7.1.1 Ιεραρχίες Cache** ..... 44
**7.1.2 Ιεραρχικές Δομές** ..... 44
**7.1.3 Μη Ιεραρχικές Δομές** ..... 46
**7.2 Πλεονεκτήματα της ένταξης σε ιεραρχία** ..... 48
**7.3 Μειονεκτήματα της ένταξης σε ιεραρχία** ..... 49
**7.4 Intercache protocols** ..... 51
**7.5 ICP** ..... 51
**7.6 CARP (Cache Array Routing Protocol)** ..... 51
**7.7 Cache Cluster** ..... 52
**7.7.1 Εύρος Ζώνης (Bandwidth)** ..... 52
**7.7.2 Η "Ρεζέρβα"** ..... 53
**7.7.3 Ταχύτητα διεκπεραίωσης και Κατανομή Φόρτου** ..... 54
**8. Case Study** ..... 55
**8.1 CHAIN MESA-EXO** ..... 57
**8.2 Cache Proxy** ..... 59
**8.3 Εφαρμογή των δηλώσεων- μετατροπή τους σε κανόνες** ..... 62
**Συμπεράσματα** ..... 64
**ΑΚΡΩΝΥΜΙΑ** ..... 66
**ΒΙΒΛΙΟΓΡΑΦΙΑ** ..... 68

# ΠΡΟΛΟΓΟΣ

Ο σκοπός του συγκεκριμένου κειμένου είναι να δώσει πληροφορίες για την εγκατάσταση των διακομιστών την διαχείριση τους και την χρήση των υπηρεσιών που προσφέρουν.

Ο proxy server είναι μία πύλη που χωρίζει το εσωτερικό από το εξωτερικό δίκτυο, χωρίς να φαίνονται οι εσωτερικές διευθύνσεις στο εξωτερικό δίκτυο. Επιπλέον μπορεί να χρησιμοποιηθεί και ως case memory server δηλαδή να αποθηκεύει της σελίδες που έχουν κατεβάσει χρήστες και να της ξαναστέλνει αν ζητηθούν από άλλους χρήστες.

Το μοντέλο πελάτη – εξυπηρετητή (client-server), υπήρξε το βασικό για την κατασκευή κατανεμημένων συστημάτων (distributed systems) και υπηρεσιών λόγω της απλότητας της αρχής λειτουργίας του, που ήταν και η αιτία για την διαδεδομένη εμπορική χρήση του σε κατανεμημένα υπολογιστικά συστήματα για περισσότερο από μια δεκαετία. Όμως η εμφάνιση του internet computing και των εφαρμογών του, ανέδειξε κάποιες από τις εγγενείς αδυναμίες αυτού του μοντέλου, όπως είναι η ανάγκη κεντρικού ελέγχου της πληροφορίας και η διεξαγωγή της επεξεργασίας των δεδομένων σε ειδικευμένους υπολογιστικούς κόμβους (computing nodes), όπως είναι οι εξυπηρετητές, γεγονότα που είναι πολύ δεσμευτικά για μια σειρά από κατηγορίες υπολογιστικών εφαρμογών του Internet (internet computing application classes).

.

# 1.ΕΙΣΑΓΩΓΗ

## 1.1 Τι είναι ένας proxy server;

Proxy (=πληρεξούσιος) server λέγεται ένας server που παρεμβάλλεται μεταξύ του υπολογιστή σου και της διεύθυνσης του Διαδικτύου που θέλεις να πας (web σελίδα η ftp server) δρώντας σαν ενδιάμεσος. Κάθε αίτημα για σύνδεση που στέλνει ο υπολογιστής σου πηγαίνει πρώτα στον proxy server ο οποίος και το προωθεί στην τελική διεύθυνση εμφανιζόμενος αυτός σαν αποστολέας αντί για σένα. Στη συνέχεια τα δεδομένα που ζήτησες φτάνουν στον proxy server και αυτός τα προωθεί στον υπολογιστή σου.

Οι διάφοροι τύποι που μπορείς να συναντήσεις είναι:

- HTTP/HTTPS server με πρόσβαση στα ports 80, 8080 etc.
- Proxy Server με πρόσβαση στα ports 80, 8080, 3128 etc.
- FTP servers με πρόσβαση στο port 21
- SMTP servers με πρόσβαση στο 25
- NNTP servers με πρόσβαση στο 119
- PopD servers με πρόσβαση στο 110
- TelNet/Wingate servers με πρόσβαση στο port 23
- Socks servers με πρόσβαση στο port 1080

Τα νούμερα των βασικών ports είναι σημαντικό να τα γνωρίζεις έτσι ώστε όταν κάνεις ένα port scanning σε ένα server μπορείς να δεις ποια είναι ανοιχτά για το σκοπό που το θέλεις.

## 1.2 Τι προσφέρει ένας proxy server;

Συνήθως χρησιμοποιείς ένα proxy server για να αυξήσεις την ταχύτητα της σύνδεσης σου. Ένας proxy server διατηρεί αντίγραφα των σελίδων που επισκέπτεται σε μία βάση δεδομένων που λέγεται "cache". Το cache κάθε proxy server είναι συνήθως

τεράστιο σε μέγεθος και περιλαμβάνει τα αρχεία που έχουν ζητήσει εκατοντάδες, η και χιλιάδες χρήστες του Διαδικτύου. Αυτό έχει σαν αποτέλεσμα τα δεδομένα που ζητάς να βρίσκονται, πολλές φορές, ήδη στο cache δίνοντας τη δυνατότητα στον proxy να στα στείλει αμέσως (χωρίς να απαιτηθεί σύνδεση του με την πηγή των δεδομένων εκ νέου). Συχνά, η αύξηση της ταχύτητας είναι εντυπωσιακή. Μερικές φορές χρειάζεται να κάνεις RELOAD η REFRESH τη web σελίδα για να δεις μια πρόσφατη έκδοση μια και το αντίγραφο στο cache του proxy server μπορεί να είναι παλαιότερο.

Πολλές φορές, οι ιδιοκτήτες συγκεκριμένων τόπων του Διαδικτύου θέτουν γεωγραφικούς περιορισμούς στη σύνδεση. Για παράδειγμα, ο server μια ελληνικής web σελίδας μπορεί να είναι προγραμματισμένος να δέχεται συνδέσεις μόνο από το domain .gr. Σε αυτή την περίπτωση, βρισκόμενος σε κάποια άλλη χώρα, μπορείς να χρησιμοποιήσεις ένα ελληνικό proxy server και να συνδεθείς παρουσιαζόμενος σαν να είσαι από την Ελλάδα.

Ακόμα υπάρχουν χώρες όπου η κυβέρνηση λογοκρίνει τους Διαδικτυακούς τόπους στους οποίους οι πολίτες της χώρας μπορούν να συνδεθούν. Συνδεόμενοι με ένα proxy server μπορούν να ξεγελάσουν τους λογοκριτές και να αποκτήσουν πρόσβαση σε "απαγορευμένους τόπους" εμφανιζόμενοι ότι συνδέονται με τη διεύθυνση του proxy server και όχι την πραγματική τους. Σε ορισμένες χώρες πας φυλακή αν επισκεφτείς απαγορευμένες Διαδικτυακές διευθύνσεις! (βλ. αραβικές και ορισμένες ασιατικές χώρες)

Τέλος, χρησιμοποιώντας ορισμένους proxy servers μπορείς να προστατέψεις την ανωνυμία σου.

## 1.3 Τι είναι ο ανώνυμος proxy server;

Κάθε web σελίδα, σε όλο τον κόσμο, μπορεί να καταγράψει τις κινήσεις σου και να παρακολουθήσει τα ενδιαφέροντα σου χρησιμοποιώντας την διεύθυνσή IP σου, που είναι μοναδική. Ανάλογα με την πολιτική του κάθε Διαδικτυακού τόπου, ενδέχεται να μη μπορέσεις να έχεις πρόσβαση σε αυτό που θέλεις. Ακόμα, τα στοιχεία της επίσκεψης σου καταγράφονται και μπορεί να χρησιμοποιηθούν αργότερα.

Είναι ευρέως γνωστό ότι διάφορες κυβερνήσεις και οργανισμοί στήνουν web σελίδες δολώματα που αναφέρονται σε αμφισβητούμενα θέματα με στόχο την παρακολούθηση

των ενδιαφερομένων. Επιπρόσθετα αυτές οι πληροφορίες σε συνδυασμό με την διεύθυνση e- mail σου, μπορούν να χρησιμοποιηθούν για να σε βομβαρδίσουν οι Μικροεμπράκοι με κατευθυνόμενη διαφήμιση.

Με τη χρήση και μόνο της διεύθυνσης IP σου και τις πληροφορίες γύρω από το λειτουργικό σύστημα του υπολογιστή σου, μια web σελίδα μπορεί αυτόματα να εκμεταλλευτεί κάποια κενά ασφαλείας (security holes) του συστήματος σου με τη βοήθεια απλών προγραμμάτων που κυκλοφορούν έτοιμα και δωρεάν στο Διαδίκτυο. Τα πιο απλά από αυτά απλά θα παγώσουν τον υπολογιστή σου. Όμως υπάρχουν άλλα ισχυρότερα που μπορούν να αποκτήσουν πρόσβαση στα στοιχεία που έχεις αποθηκευμένα είτε στο σκληρό σου δίσκο είτε στη μνήμη RAM του υπολογιστή σου. Ένας ανώνυμος proxy server σε προστατεύει αποκρύπτοντας την διεύθυνση IP (ΣΗΜ. δεν την στέλνει μέσω HTTP), αποκλείοντας έτσι την πρόσβαση κάποιου τρίτου στον υπολογιστή σου. Συνήθως όμως, οι proxy servers ενημερώνουν με άλλο, παράλληλο τρόπο τον server-στόχο σχετικά με την διεύθυνση IP σου.

ΜΟΝΟ οι πραγματικά ανώνυμοι proxy servers δεν στέλνουν μέσω HTTP την διεύθυνση IP σου, και αποκρύπτουν αποτελεσματικά τις πληροφορίες γύρω από εσένα και τις συνήθειές σου. Κάποιοι από αυτούς έχουν την δυνατότητα να αποκρύπτουν ακόμα και το γεγονός ότι χρησιμοποιείς ένα proxy server! Τέλος, οι ανώνυμοι proxy servers μπορούν να χρησιμοποιηθούν για διάφορες υπηρεσίες του Διαδικτύου όπως Web-Mail (MSN Hot Mail, Yahoo mail), Web-chatrooms, αρχεία FTP, κτλ.

## 1.4 Ο proxy server που βρήκες είναι αληθινά ανώνυμος;

Υπάρχουν χιλιάδες "δημόσιοι" (=public) proxy servers σε πολλές χώρες που σου επιτρέπουν να συνδεθείς δωρεάν, όμως η πλειονότητα δεν είναι ανώνυμοι.

Στις διάφορες λίστες που θα βρεις υπάρχουν πολλοί που χαρακτηρίζονται σαν ανώνυμοι, μια και δεν ανακοινώνουν την διεύθυνση IP σου με τον συνήθη τρόπο (HTML), αλλά στην πραγματικότητα δεν είναι, μια και κοινοποιούν τα στοιχεία σου με άλλο τρόπο. Επιπλέον έχει παρατηρηθεί ότι ακόμα και ανώνυμοι proxy servers, κάποιες φορές κοινοποιούν τα στοιχεία σου. Ποτέ μη θεωρείς ένα proxy server σαν ανώνυμο χωρίς να τον τσεκάρεις εσύ ο ίδιος!

Ο απλούστερος τρόπος για να ελέγξεις τον βαθμό ανωνυμίας ενός proxy server είναι να συνδεθείς μέσω telnet. Αν δεν ξέρεις τι και πώς πήγαινε στη δεύτερη λύση.

Ας υποθέσουμε ότι το proxy που θες να τεστάρεις είναι το proxyx.com και το port το 8080:

```
telnet proxyx.com 8080 η telnet proxyx.com:8080 (ανάλογα με το σύστημα σου) GET http://smartsearch.hypermart.net/cgi-bin/chkip/senv2.cgi  ENTER (2 φορές)
```

1. Αν η απάντηση είναι connection refused τότε ο proxy server δεν είναι διαθέσιμος-ανοικτός. Σε αντίθετη περίπτωση θα δεις όλα τα στοιχεία που στέλνει ο browser σου προς τα έξω. Βέβαια αντί του http://smartsearch.hypermart.net/cgi-bin/chkip/senv2.cgi μπορείς να χρησιμοποιήσεις οποιαδήποτε άλλη διεύθυνση, όπως για παράδειγμα αυτές που θα βρεις στην λίστα με τα proxies (proxy list).
2. Αν δεν θες να ασχοληθείς με το telnet τότε μπορείς να χρησιμοποιήσεις απ΄ ευθείας τα διάφορα cgi η java scripts που είναι διαθέσιμα στο Διαδίκτυο για αυτή τη δουλειά.

Και στις δύο περιπτώσεις πρέπει να εξετάσεις με προσοχή το αποτέλεσμα. Ψάξε να βρεις αν η διεύθυνση IP σου παρουσιάζεται κάπου στα αποτελέσματα. Αν την δεις, τότε ο proxy server που τσεκάρεις δεν είναι ανώνυμος (δες παράδειγμα 2).

Ακολουθούν τρία παραδείγματα που θα σε βοηθήσουν να καταλάβεις το θέμα.

```
HTTP_USER_AGENT=Opera/6.05 (Windows 2000; U)en PATH=/usr/local/bin:/usr/bin:/bin  PATH_TRANSLATED=/home/cgi-bin/chkip/senv2.cgi  REMOTE_ADDR=200.203.2x.xxx REMOTE_HOST=200-203-2x-xxx-paemtx00x.dsl.telebrasilia.net.br REMOTE_PORT=65080
```

## 1.4.1 Παράδειγμα 1 (απ΄ ευθείας σύνδεση)

Σε αυτό το παράδειγμα η σύνδεση έγινε χωρίς την μεσολάβηση κάποιου proxy server ούτε άλλου φίλτρου. Βλέπεις καθαρά όχι μόνο τον browser που χρησιμοποίησα (Opera), το λειτουργικό μου σύστημα (Windows 2000) αλλά και την διεύθυνση IP μου φαρδιά-πλατιά (200-203-2x-xxx-paemtx00x.dsl.telebrasilia.net.br)

```
HTTP_CLIENT_IP=200.203.2x.xxx HTTP_CONNECTION=keep-alive HTTP_HOST=smartsearch.hypermart.net  HTTP_PRAGMA=no-cache HTTP_USER_AGENT=Opera/6.05 (Windows 2000; U) en HTTP_X_FORWARDED_FOR=148.233.111.232  PATH=/usr/local/bin:/usr/bin:/bin PATH_TRANSLATED=/home/cgi-bin/chkip/senv2.cgi
```

REMOTE_ADDR=200.64.191.50 REMOTE_HOST=dup-200-64-191-50.prodigy.net.mx REMOTE_PORT=50323

## 1.4.2 Παράδειγμα 2 (transparent (=διαφανής) proxy)

Εδώ η σύνδεση έγινε μέσω ενός διαφανούς proxy server. Βλέπεις πάλι τον browser (Opera) και το λειτουργικό σύστημα (Windows 2000), αφού δεν χρησιμοποίησα κάποιο φίλτρο. Αυτή τη φορά όμως η διεύθυνση IP μου εμφανίζεται σαν HTTP_CLIENT_IP (που δείχνει ότι η εντολή HTTP προήλθε από τη διεύθυνση 200-203-2x-xxx-paemtx00x.dsl.telebrasilia.net.br) μέσω των proxy servers 148.233.111.232 και dup-200-64-191-50.prodigy.net.mx (με αυτή ακριβώς τη σειρά).

HTTP_USER_AGENT=katsarola 4.78 PATH=/usr/local/bin:/usr/bin:/bin PATH_TRANSLATED=/home/cgi-bin/chkip/senv2.cgi REMOTE_ADDR=200.41.230.99 REMOTE_HOST=server.hcdiputados-ba.gov.ar REMOTE_PORT=3769

## 1.4.3 Παράδειγμα 3 (ανώνυμος proxy+proxomitron 4.4)

Εδώ η σύνδεση έγινε μέσω ενός ανώνυμου proxy server. Το μόνο που βλέπεις είναι η διεύθυνση του proxy server server.hcdiputados-ba.gov.ar χωρίς άλλα ίχνη προέλευσης. Αυτή τη φορά ο browser παρουσιάζεται σαν katsarola 4.78 ενώ το λειτουργικό σύστημα είναι άφαντο. Για το φιλτράρισμα έχω χρησιμοποιήσει το Proxomitron πού όσο γελοίο όνομα έχει τόσο αξιόλογο είναι. A must!

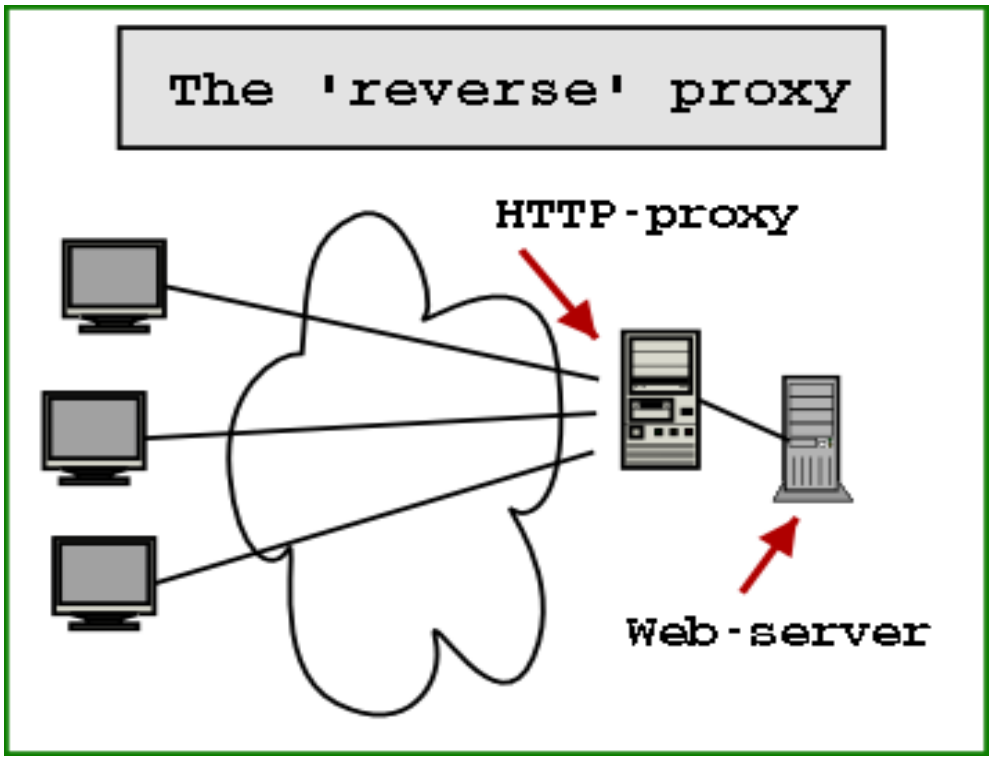
ΣΗΜΕΙΩΣΕΙΣ

Είναι αδύνατο να είσαι αόρατος η πραγματικά ανώνυμος στο Διαδίκτυο. Όποιος ισχυρίζεται το αντίθετο η δεν ξέρει τι λέει η έχει άλλους σκοπούς.

Μπορείς να ψάξεις και μόνος σου για proxy servers, αν και δεν στο συνιστώ. Χρησιμοποιώντας, για παράδειγμα προγράμματα όπως το wGateScan η το ProxyHunter, που είναι εύκολο να τα βρεις στο Διαδίκτυο. Δίνοντας τους ένα εύρος διευθύνσεων IP και το port που σε ενδιαφέρει, π.χ. 1080 και 23, η μόνο το port 23 στο wGateScan θα κάνουν scan μια-μια διεύθυνση και θα σου παρουσιάσουν τα αποτέλεσμα.

Όμως, λάβε υπ΄ όψη σου ότι αυτή η διαδικασία γνωστή σαν "Network Probing" ΑΠΑΓΟΡΕΥΕΤΑΙ από τους παροχείς σύνδεσης και αν το κάνεις συχνά μπορεί να χάσεις το λογαριασμό σου. Αν όμως επιμένεις τότε χρησιμοποίησε ένα η περισσότερους πραγματικά ανώνυμους proxy servers.

## 1.5 Reverse Proxy




Το *reverse proxy cache*, γνωστό και ως *Web Server Acceleration* (επιτάχυνση διακομιστεί ιστού), είναι ένας τρόπος να μειώνουμε το φόρτο ενός αρκετά φορτωμένου web server, βάζοντας ανάμεσα σε αυτόν και το Διαδίκτυο έναν proxy cache, το οποίο προσθέτει και επιπλέον ασφάλεια. Με σωστή χρήση του reverse proxy διευκολύνεται πολύ η δουλειά ενός web server ο οποίος παράγει στατικά και δυναμικά αντικείμενα. Τα στατικά μπορούν να αποθηκευτούν στην cache του reverse proxy, ενώ ο web server θα είναι πιο ελεύθερος να παράγει το δυναμικό περιεχόμενο.
Εφαρμόζοντας έναν reverse proxy παράλληλα με κάποιους web servers, το site μας μπορεί:

- Να αποφύγει περιττά έξοδα για την αγορά πρόσθετων web server, αυξάνοντας τις ικανότητες του υπάρχοντος. Θα εξυπηρετούν περισσότερες αιτήσεις για στατικό υλικό από τον web
- Θα εξυπηρετούν περισσότερες αιτήσεις για δυναμικό υλικό από τον web server
- Να αυξήσει το κέρδος της επιχείρησης, μειώνοντας τα λειτουργικά έξοδα συμπεριλαμβανομένου και τα έξοδα που απαιτούνται για το εύρος ζώνης που χρειάζεται.

- Επιτάχυνση του χρόνου απόκρισης των σελίδων και επιτάχυνση των download για τους εξωτερικούς χρήστες, μεταφέροντάς τους μια γρηγορότερη και καλύτερη εμπειρία της σελίδας και των υπηρεσιών μας.

Εάν η ιστοσελίδα μας δεν έχει γραφτεί με τρόπο να δουλεύει με κάποιο proxy, δε θα μπορεί να εκμεταλλευτεί όλες τις δυνατότητες ενός reverse proxy.

Σε κατάσταση reverse proxy, ο διακομιστής proxy συμπεριφέρεται κατά κύριο λόγο, σαν διακομιστής ιστού. Ενώ οι εσωτερικοί χρήστες χρειάζονται κάποιες ρυθμίσεις για να μπορούν να επικοινωνούν με τον proxy, οι εξωτερικοί δεν χρειάζονται καμία απολύτως. Το URL του site μας δρομολογεί τον πελάτη στον proxy σα να ήταν αυτός ο web server. Το αντιγραμμένο περιεχόμενο παραδίδεται από τον proxy cache στον εξωτερικό πελάτη χωρίς να εκτίθεται ο πραγματικός διακομιστής ή το ιδιωτικό μας δίκτυο που βρίσκονται πίσω από το firewall. Πολλαπλοί reverse proxy μπορούν να χρησιμοποιηθούν για την εξισορρόπηση του φόρτου (cache cluster).

Ένας reverse proxy cache διαφέρει από ένα συνηθισμένο ή έναν διαφανή proxy στο ότι μειώνει το φόρτο στον web server αντί να μειώνει το, προς τα έξω, εύρος ζώνης από την πλευρά των πελατών. Απαλλάσσουν τον web server από αιτήσεις πελατών για στατικό περιεχόμενο, αποτρέποντας έτσι την υπερφόρτωση του πραγματικού διακομιστή από απρόβλεπτες, απότομες αυξήσεις κίνησης. Ο proxy βρίσκεται ανάμεσα στο Διαδίκτυο και το site μας και χειρίζεται την κίνηση πριν φτάσει στον διακομιστή ιστού και αναχαιτίζει τις αιτήσεις προς τον διακομιστή ιστού και απαντά αντί γι' αυτόν από την εναποθήκευση που έχει κάνει στην cache του με προηγούμενες απαντήσεις. Αυτή η μέθοδος βελτιώνει την απόδοση μειώνοντας το ποσό των ιστοσελίδων που αναπαράγονται από τον web server.

Όταν ένας πελάτης-φυλλομετρητής δημιουργεί μια αίτηση HTTP, ο DNS θα δρομολογήσει την αίτηση προς τον proxy  ο proxy ελέγχει την cache του να δει αν περιέχει το ζητούμενο αντικείμενο. Εάν δεν το έχει, συνδέεται με τον web server και το κατεβάζει στην cache του. Ένας reverse proxy μπορεί να ικανοποιεί αιτήσεις για URL's τα οποία μπορεί να αποθηκεύσει στην cache του, όπως είναι οι σελίδες html και εικόνες.

Δυναμικό περιεχόμενο, όπως είναι τα cgi scripts, ASP, PHP δεν μπορούν να αποθηκευτούν στην cache. Ο proxy μπορεί να αποθηκεύσει στατικές σελίδες βασιζόμενος στις ετικέτες των κεφαλίδων HTTP (header tags) που επιστρέφει η ιστοσελίδα. Οι τέσσερις πιο σημαντικές ετικέτες είναι οι:

- Last-Modified. Πληροφορεί τον proxy για την τελευταία τροποποίηση της σελίδας.
- Expires. Πληροφορεί τον proxy για τον χρόνο που θα πρέπει να σβήσει την σελίδα από την cache του.
- Cache-Control. Πληροφορεί για το εάν πρέπει να αποθηκευτεί στην cache ή όχι
- Pragma. Παρόμοιο με το Cache-Control.

# 2. Υπηρεσίες Proxy

Οι υπηρεσίες *proxy* είναι εξειδικευμένες εφαρμογές ή προγράμματα διακομιστή τα οποία "τρέχουν" στο firewall το οποίο είναι είτε ένας dual-*homed host* με τη μία διεπαφή στο εσωτερικό δίκτυο και την άλλη στο εξωτερικό είτε ένας *bastion host* ο οποίος είναι προσπελάσιμος από τις εσωτερικές μηχανές του δικτύου και έχει πρόσβαση στο Διαδίκτυο. Αυτά τα προγράμματα υποκλέπτουν τις αιτήσεις των χρηστών για υπηρεσίες του
Διαδικτύου και τις προωθούν, καθώς αρμόζει σύμφωνα με την πολιτική ασφάλειας, προς τις πραγματικές υπηρεσίες. Τα proxy παρέχουν συνδέσεις αντικατάστασης και ενεργούν ως πύλες προς τις υπηρεσίες. Γι' αυτό το λόγο τα proxy είναι και γνωστά ως *πύλες επιπέδου εφαρμογής (application-level gateways).*

Οι υπηρεσίες proxy, άλλοτε αντιληπτές και άλλοτε όχι (transparent), βρίσκονται ανάμεσα στο χρήστη του εσωτερικού δικτύου και μιας υπηρεσίας έξω από αυτό (Διαδίκτυο). Αντί να μιλάνε κατ' ευθείαν ο ένας στον άλλον, μιλά ο καθένας σ 'έναν proxy. Οι proxy χειρίζονται όλες τις επικοινωνίες μεταξύ των εσωτερικών χρηστών και των υπηρεσιών του Διαδικτύου στο παρασκήνιο.

Η *διαφάνεια (transparency)* είναι το βασικό πλεονέκτημα των υπηρεσιών proxy. Στον πραγματικό server, ο proxy δίνει την ψευδαίσθηση ότι έχει να κάνει
μ' έναν χρήστη απ' ευθείας στον proxy host. Στον πραγματικό χρήστη, ο proxy δίνει την ψευδαίσθηση ότι μιλά απ 'ευθείας με τον πραγματικό server.

Οι υπηρεσίες proxy μπορούμε να πούμε ότι είναι αποτελεσματικές όταν χρησιμοποιούνται σε συνάφεια με κάποιο μηχανισμό ο οποίος αποτρέπει την άμεση επικοινωνία μεταξύ των εσωτερικών και εξωτερικών host. Οι dualhomed hosts και τα φίλτρα πακέτων είναι τέτοιοι μηχανισμοί. Εάν υπάρχει επικοινωνία άμεση του εσωτερικού με το εξωτερικό περιβάλλον, εξουδετερώνεται η ανάγκη χρήσης του proxy, οπότε και δε θα χρησιμοποιούν. Μία τέτοια παρακαμπτήρια οδός πιθανώς δεν είναι σύμφωνη με την πολιτική ασφάλειας του site μας.

## 2.1 Υπηρεσίες Proxy σε ένα Dual-homed Host.

Δύο είναι οι συνιστώσες μιας υπηρεσίας proxy: ο proxy server και ο proxy client. Στην περίπτωσή μας ο server βρίσκεται στον Dual-homed host. Ο πελάτης είναι μια ειδική

έκδοση ενός συνηθισμένου προγράμματος πελάτη (όπως είναι τα FTP, telnet, κλπ.) που μιλά στον proxy server αντί για τον πραγματικό server. Επιπρόσθετα, αν στους χρήστες έχουν δοθεί συγκεκριμένες οδηγίες, τα συνηθισμένα προγράμματα πελάτη μπορούν να χρησιμοποιηθούν ως proxy πελάτες. Ο proxy server εκτιμά τις αιτήσεις των πελατών και αποφαίνεται στο αν θα τις δεχτεί ή αν θα τις απορρίψει. Αν αποδεχτεί κάποια αίτηση, τότε επικοινωνεί με τον πραγματικό server εκ μέρους του πελάτη και προχωρεί στην αναμετάδοση της αίτησης προς τον πραγματικό server από τον πελάτη και τις απαντήσεις από τον πραγματικό server προς τον πελάτη.

## 2.2 Φιλτράρισμα πακέτων

Τα συστήματα φιλτραρίσματος πακέτων δρομολογούν πακέτα μεταξύ εσωτερικών και εξωτερικών host, αλλά το κάνουν επιλεκτικά. Επιτρέπουν ή αποτρέπουν την προσπέλαση ορισμένων ειδών πακέτα με τρόπο που αντανακλά την πολιτική ασφάλειας του site μας . Ο δρομολογητής ο οποίος χρησιμοποιείται από τα firewall φιλτραρίσματος πακέτων ονομάζεται screening *router*.

Κάθε πακέτο έχει ένα σύνολο από "κεφαλίδες" (headers), που περιέχουν συγκεκριμένες σημαντικές πληροφορίες, κάποιες από τις οποίες είναι: IP διεύθυνσης πηγής, IP διεύθυνσης προορισμού, το πρωτόκολλο (TCP, UDP ή ICMP), το TCP ή UDP port πηγής και προορισμού καθώς και τον τύπο του ICMP μηνύματος. Επιπρόσθετα ο δρομολογητής γνωρίζει κάποια πράγματα για τα πακέτα που εισέρχονται ή εξέρχονται από αυτόν τα οποία δεν αναφέρονται στις πληροφορίες των κεφαλίδων όπως για παράδειγμα το interface(η διεπαφή) απ' το οποίο μπήκε το ή αυτό απ το οποίο θα βγει.

Το γεγονός ότι χρησιμοποιούνται συγκεκριμένοι αριθμοί port στους server των υπηρεσιών Internet δίνει στον δρομολογητή τη δυνατότητα να επιτρέπει ή να αποτρέπει συγκεκριμένα είδη συνδέσεων απλά προσδιορίζοντας το κατάλληλο port (π.χ. TCP port 23 για συνδέσεις Telnet) στους κανόνες προσδιορισμού του φίλτρου πακέτων.

Εδώ παρουσιάζονται κάποια παραδείγματα με τον οποίο θα μπορούσαμε να

προγραμματίσουμε έναν screening router ώστε να δρομολογεί τα πακέτα επιλεκτικά από ή προς το site μας:

- Μπλοκάρισμα όλων των εισερχόμενων συνδέσεων από συστήματα έξω από το δίκτυο μας, εκτός από τις εισερχόμενες SMTP συνδέσεις ώστε να λαμβάνουμε αλληλογραφία.
- Μπλοκάρισμα των συνδέσεων σε ή από μη-έμπιστα συστήματα.
- Αποδοχή υπηρεσιών αλληλογραφίας και FTP, αλλά μπλοκάρισμα επικίνδυνων υπηρεσιών όπως TFTP, του συστήματος X Window, των υπηρεσιών *"r"* (rlogin, rsh, rcp κτλ)

Για να γίνει πιο σαφής και κατανοητή η διαδικασία του φιλτραρίσματος πακέτων θα εξηγήσουμε τη διαφορά μεταξύ ενός συνηθισμένου router και ενός screening router.

Ένας συνηθισμένος δρομολογητής απλά ελέγχει τη διεύθυνση προορισμού του πακέτου και επιλέγει τον καλύτερο τρόπο που γνωρίζει ώστε να κατευθύνει το πακέτο προς τον προορισμό του. Η απόφαση που εκλαμβάνεται για τη μοίρα του πακέτου βασίζεται αποκλειστικά από τον προορισμό του. Υπάρχουν δύο εκδοχές που αφορούν τη μοίρα του πακέτου: είτε γνωρίζει ο δρομολογητής πώς να το στείλει προς τον προορισμό του και το πράττει, είτε δε γνωρίζει και το επιστρέφει από όπου ήρθε στέλνοντας και ένα ICMP μήνυμα "destination unreachable" .

Από την άλλη ο screening router ρίχνει μια πιο προσεκτική ματιά στα πακέτα. Επιπρόσθετα, προσδιορίζοντας αν μπορεί ή όχι να δρομολογήσει το πακέτο προς τον προορισμό του, ένας screening router αποφαίνεται στο αν πρέπει ή όχι να το δρομολογήσει Το αν πρέπει ή όχι προσδιορίζεται από την πολιτική ασφάλειας του site μας η οποία του έχει επιβληθεί.

Παρόλο που είναι δυνατό να βρίσκεται ένας screening router μεταξύ του Internet και του εσωτερικού μας δικτύου, αυτό εναποθέτει τεράστια
ευθύνη σ' αυτόν. Όχι μόνο πρέπει να εκπληρώσει όλες τις διαδικασίες δρομολόγησης και λήψης αποφάσεων για τις δρομολογήσεις αλλά είναι και το μόνο σύστημα ασφάλειας. Εάν η ασφάλειά του αποτύχει ή καταρρεύσει από μια επίθεση το εσωτερικό δίκτυο μένει εκτεθειμένο. Επιπρόσθετα, ένας γνήσιος screening router δεν μπορεί να τροποποιεί υπηρεσίες. Μπορεί να επιτρέψει ή όχι μια υπηρεσία , αλλά δεν μπορεί να προστατεύσει μεμονωμένες λειτουργίες μιας υπηρεσίας. Α ν μια επιθυμητή υπηρεσία έχει κάποιες μη ασφαλής λειτουργίες ή αν η υπηρεσία συνήθως παρέχεται με έναν ανασφαλή server, το φιλτράρισμα πακέτων από μόνο του δε μπορεί να παρέχει την επιθυμητή ασφάλεια

Κάθε διερχόμενο πακέτο από ή προς το internet και στο εσωτερικό δίκτυο πρέπει

πρώτα να περάσει από τον proxy server, ο proxy server βρίσκεται στην κατάλληλη θέση για να παίξει το ρόλου του 'θυρωρού. Αυτό πετυχαίνετε με το να λειτουργεί ο proxy server σαν μεσολαβητής μεταξύ του internet και του intranet. Ο proxy server τοποθετείται σε ένα τμήμα του δικτύου που συνδέει το internet με το intranet. Δύο προσαρμοστές (κάρτες δικτύου) εγκαθίστανται στον proxy server. Ο πρώτος συνδέει το internet με τον proxy και δεύτερος το intranet με τον proxy. Αυτό σημαίνει ότι δεν υπάρχει απευθείας σύνδεση του intranet με το internet.

Με το λογισμικό proxy server 2 η Microsoft πρόσθεσε τη δυνατότητα φιλτραρίσματος των πακέτων (packet filtering) δίνοντας πολλές δυνατότητες αντιπυρικής ζώνης (firewall). Αυτό το φιλτράρισμα πακέτων λειτουργεί με την επιθεώρηση του κάθε πακέτου, ώστε να ελέγχει ποιο πρωτόκολλο 'χρησιμοποιεί και το αν πρόκειται για επιτρεπόμενη σύνδεση.

Ο proxy server μπορεί επίσης να χρησιμοποιηθεί για να φιλτράρει τις αίτησης από το εξωτερικό προς το εσωτερικό δίκτυο. Παράδειγμα μπορούμε να επιτρέπουμε συγκεκριμένες IP διευθύνσεις να συνδέονται στο εσωτερικό δίκτυο. Ή να φιλτράρουμε τις αιτήσεις από το εσωτερικό προς το εξωτερικό. Για παράδειγμα μπορούμε να αποτρέψουμε την πρόσβαση σε μία συγκεκριμένη ομάδα από web site.

Όταν έχει ενεργοποιηθεί το φιλτράρισμα πακέτων, μπορούμε να περιορίσουμε την πρόσβαση σε συγκεκριμένες εξωτερικές τοποθεσίες, ή να επιτρέψουμε να είναι ορατές μόνο ορισμένες εσωτερικές τοποθεσίες. Επιπλέον ορισμένα πρόσθετα προγράμματα μπορούν να προσθέσουν στο proxy server επιπλέον χαρακτηριστικά.

## 2.2.1 ΦΙΛΤΡΑ ΠΕΡΙΟΧΗΣ

Μπορούμε να διαχειριστούμε τη πρόσβαση των χρηστών σε συγκεκριμένες περιοχές ή IP διευθύνσεις στο Internet. Αυτό μας επιτρέπει να παρέχουμε περιορισμένη πρόσβαση σε τοποθεσίες κλειδιά ή να απαγορεύουμε την πρόσβαση από ορισμένες τοποθεσίες. Για να ενεργοποιήσουμε τα φίλτρα περιοχών ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε τον IIS και πατάμε δεξί κλικ στην επιλογή wed proxy.
Επιλέγουμε properties για να ανοίξει το παράθυρο wed proxy properties
2. Πατάμε το κουμπί Security και επιλέγουμε την καρτέλα Domain filter (φίλτρα περιοχών)
3. Ενεργοποιούμε το πλαίσιο ελέγχου Enable filtering
4. Για να επιλέξουμε τις περιοχές στις οποίες θα απαγορεύεται η πρόσβαση,

επιτρέποντας την πρόσβαση σε όλες τις άλλες ενεργοποιούμε την *ι* εΠ1λογή Granted. Για να επιτρέψουμε την πρόσβαση σε περιοχές και να την απαγορεύσουμε σε όλες τις άλλες ενεργοποιούμε την επιλογή Deny.

5. Για να προσθέσουμε μία περιοχή πατάμε το κουμπί AIt.

## 2.3 ΧΡΗΣΗ ΚΡΥΦΗΣ ΜΝΗΜΗΣ

Σε κάθε επιχείρηση υπάρχουν ορισμένες τοποθεσίες που ουσιαστικά επισκέπτονται τακτικά οι πάντες. Ακόμα και οι τοποθεσίες που είναι σχετικά δυναμικές έχουν πολλές πληροφορίες (όπως έγγραφα σε HTML, γραφικά κτλ.) οι οποίες δεν αλλάζουν συχνά. Ο proxy server μπορεί να αποθηκεύει στην κρυφή μνήμη (cache memory) πληροφορίες από τις τοποθεσίες όπου οι χρήστες επισκέπτονται συχνά, ώστε όταν οι χρήστες συνδεθούν στην τοποθεσία, μεγάλο μέρος από τις πληροφορίες παρέχεται από τον proxy server και όχι από τον απομακρυσμένο web server. Για παράδειγμα όταν δύο χρήστες Χ και Υ έχουν πρόσβαση στο WWW μέσω ενός κοινού proxy server. Ο πρώτος χρήστης Χ κατεβάζει μία σελίδα από τον απομακρυσμένο web server. Λίγη ώρα αργότερα ο χρήστης Υ ζητά την ίδια σελίδα. Αντί ο proxy server να προωθήσει ξανά την αίτηση στον web server όπου βρίσκεται η σελίδα που μπορεί να είναι χρονοβόρα διαδικασία ο proxy server απλά επιστρέφει την σελίδα που είχε κατεβάσει για τον χρήστη Χ.

Η χρήση της cache memory βελτιώνει σημαντικά την 'φαινόμενη' ταχύτητα της σύνδεσης του internet, επειδή παρέχει πληροφορίες τοπικά για κάποιες από τις πιο δημοφιλείς τοποθεσίες και αφού μειώνει την κίνηση στο Internet για αυτές της τοποθεσίες αυξάνεται το εύρος ζώνης για όλες της άλλες τοποθεσίες που επισκέπτονται οι χρήστες.

Ο proxy server μπορεί να χρησιμοποιεί τις ώρες μειωμένης κίνησης, όταν είναι συνδεδεμένοι λίγοι χρήστες στο internet για να ελέγχει τις τοποθεσίες που οι χρήστες επισκέπτονται συχνά για να εξασφαλίσει ότι είναι ενημερωμένες οι πληροφορίες που έχουν αποθηκευτεί για αυτές. Αυτή η παρακολούθηση βοηθά στην εξισορρόπηση και την εξομάλυνση των αιτήσεων μέσω της σύνδεσης μας στο internet μειώνοντας το κόστος και παρέχοντας διεκπεραιωτή ικανότητα κατά τη διάρκεια ωρών μεγαλύτερης κίνησης επειδή χρειάζεται να μεταφέρονται λιγότερες σελίδες και εικόνες.

# 2.4 ΔΙΑΧΕΙΡΙΣΗ ΤΟΥ WEB PROXY SERVER

Εκτός από της γενικές παραμέτρους που μπορούμε να ρυθμίσουμε στον proxy server μπορούμε επίσης να ρυθμίσουμε και συγκεκριμένους παραμέτρους για τον web proxy όπως η χρήση της κρυφής μνήμης, η δρομολόγηση, η δημοσίευση στον ιστό και η καταγραφή ενεργειών.

## 2.4.1 Χρήση κρυφής μνήμης του web proxy.

Ο proxy server μπορεί να αποθηκεύσει web pages από απομακρυσμένους web server στις οποίες έχουμε συχνή πρόσβαση, ώστε να μειωθεί η ζήτηση εύρους ζώνης για το internet η χρήση της κρυφής μνήμης είναι ενεργοποιημένη από την εγκατάσταση. Για να ρυθμίσουμε την κρυφή μνήμη ακολουθούμε τα παρακάτω βήματα.

1. Ανοίγουμε τον IIS και πατάμε δεξί κλικ στην επιλογή wed proxy. Επιλέγουμε properties για να ανοίξει το παράθυρο wed proxy properties.

2. Επιλέγουμε την καρτέλα Caching.

3. Επιλέγουμε τις ρυθμίσεις και πατάμε το κουμπί OK για να αποθηκεύουμε τις αλλαγές και να κλείσουμε το παράθυρο.

Οι αλλαγές που μπορούμε να κάνουμε είναι:

- Enable cashing( ενεργοποίηση, απενεργοποίηση της κρυφής μνήμης).

Μπορούμε επίσης να αλλάξουμε τις ρυθμίσεις στη χρήση της κρυφής μνήμης. Οι επιλογές είναι:

- Updates are more important (πραγματοποιεί συχνότερα έλεγχο για την ενημέρωση ιστοσελίδων).
- Equal important ( ισορροπημένη συμπεριφορά)
- Fewer network accesses are more important (ο proxy server θα διατηρεί για περισσότερο χρόνο τα στοιχεία της κρυφής μνήμης, αυξάνοντας τον αριθμό προσπελάσεων).
- Enable active cashing (ενεργοποίηση ενεργούς χρήσης κρυφής μνήμης).

Μπορούμε να αλλάξουμε και τις ρυθμίσεις αυτής της λειτουργίας. Οι αλλαγές που μπορούμε να κάνουμε είναι:

- Faster user response is more important (σημαντικότερη είναι η πιο γρήγορη ανταπόκριση των χρηστών)
- Equal important (ισορροπημένη συμπεριφορά).
- Fewer network accesses are more important (ο proxy server κάνει λιγότερες λήψεις σελίδων για να μειώσει το εύρος ζώνης δικτύου).
- Cash size (το μέγεθος της κρυφής μνήμης). Μπορούμε να χρησιμοποιήσουμε οποιοδήποτε τοπικό δίσκο διαμορφωμένο σε NTFS για τη κρυφή μνήμη. Με αυτό το κουμπί μπορούμε να αλλάξουμε το μέγεθος και τη θέση της κρυφής μνήμης.
- Advanced (προχωρημένο). Μπορούμε να κάνουμε μικρό-ρυθμίσεις στις επιλογές του proxy server.

# 2.5 ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

Μπορούμε να ενεργοποιήσουμε άδειες ελέγχου πρόσβασης για διάφορα πρωτοκόλλα οι οποίες επιτρέπουν ή απαγορεύουν τη χρήση πρωτοκόλλων από χρήστες ή από ομάδες. Αυτή η επιλογή είναι χρήσιμη για τον έλεγχο της πρόσβασης από περιοχές του δικτύου προς το Internet.

Για να ενεργοποιήσουμε τον έλεγχο πρόσβασης για τον \Web proxy ακολουθούμε τα παρακάτω βήματα:

1. Ανοίγουμε τον IIS και πατάμε δεξί κλικ στην επιλογή "wed proxy. Επιλέγουμε properties για να ανοίξει το παράθυρο wed proxy properties.

2. Πατάμε στην καρτέλα Permission

3. Ενεργοποιούμε το πλαίσιο Enable access control (ενεργοποίηση ελέγχου πρόσβασης).

4. Επιλέγουμε από τον πτυσσόμενο κατάλογο Protocol το πρωτόκολλο που μας ενδιαφέρει.

5. Για να προσθέσουμε συγκεκριμένους χρήστες στους οποίους θα δώσουμε πρόσβαση στο πρωτόκολλο πατάμε το κουμπί Edit και επιλέγουμε το όνομα του

χρήστη

6. Αφού προσθέσουμε τους χρήστες που θέλουμε πατάμε το κουμπί Apply για να εφαρμοστούν οι αλλαγές.

## 2.6 Ασφάλεια

Ο Proxy server υποστηρίζει μία σειρά λειτουργιών που έχουν στόχο την ασφάλεια του δικτύου και να καθορίσει ποιοι χρήστες θα μπορούν να συνδέονται και σε ποιες τοποθεσίες. Μπορούμε να φιλτράρουμε πακέτα απαγορεύοντας την είσοδο ή την έξοδο ακατάλληλων πακέτων από το δίκτυο μας. Επιπλέον μπορούμε να ελέγχουμε την πρόσβαση στις διάφορες υπηρεσίες μεσολάβησης μέσω καταλόγων ελέγχου χρηστών και ομάδων.

Οι επιλογές ασφάλειας για τον Proxy server είναι οι εξής:

- Φιλτράρισμα πακέτων
- Έλεγχος πρόσβασης
- Φίλτρα περιοχής
- Ειδοποίηση
- Καταγραφή

# 3. Μετάφραση διεύθυνσης δικτύου

Η μετάφραση διεύθυνσης δικτύου (Network address translation, NA T ) αποκρύπτει την πραγματική διεύθυνση IP από μηχανήματα τα οποία βρίσκονται πέρα από το server που εκτελεί την μετάφραση. Η χρήση του proxy server δεν είναι ο μοναδικός τρόπος εκτέλεσης του NAT. NAT εκτελούν επίσης και τα windows 2000 server και από πολλούς δρομολογητές ή άλλες συσκευές δικτύου. Ο proxy server ) παρέχει ένα πλήρες πακέτο που υπερβαίνει την απλή μετάφραση διεύθυνσης. Όταν · εκτελείται το λογισμικό του proxy server ή μία άλλη μέθοδο NAT οι διευθύνσεις IP που έχουν εκχωρηθεί στους εσωτερικούς σταθμούς εργασίας και στους διακομιστές δεν χρειάζεται να είναι 'πραγματικές', επίσημες IP διευθύνσεις, αλλά μπορούν να είναι οποιεσδήποτε IP διευθύνσεις θέλουμε.

## 3.1 IP διευθύνσεις και εσωτερικά δίκτυα

Αν και θεωρητικά θα μπορούσαμε να χρησιμοποιήσουμε οποιεσδήποτε IP διευθύνσεις στο εσωτερικό δίκτυο σίγουρα δεν πρέπει να χρησιμοποιήσουμε διευθύνσεις που ανήκουν σε άλλους. Οπότε για να χρησιμοποιήσουμε τις NAT IP πρέπει να χρησιμοποιήσουμε τις IP διευθύνσεις που έχουν εκχωρηθεί για αυτό ειδικά το σκοπό. .

Όταν οι άνθρωποι αποφάσισαν πώς θα μοιράσουν τις IP ( πριν βρεθεί ο τρόπος εκτελέσεις της NA T) αποφάσισαν ότι επρόκειτο να παρουσιαστεί ανάγκη για διευθύνσεις οι οποίες θα μπορούσαν να χρησιμοποιηθούν για δοκιμαστικά δίκτυα ή άλλες καταστάσεις που δεν απαιτούσαν τη χρήση 'επίσημων' διευθύνσεων. Συνεπώς δημιούργησαν ένα ειδικό σύνολο IP διευθύνσεων που ονομάζονται διευθύνσεις ιδιωτικού δικτύου (private network addresses), όπως ορίζονται στο έγγραφο RFC

1918, ώστε να παρέχονται δίκτυα τάξης Α, τάξης Β και τάξης C για δοκιμή ή άλλα δίκτυα τα οποία δεν θα είναι φυσικά συνδεδεμένα στο internet.

Με τις private network addresses μπορούμε να έχουμε πολύ μεγαλύτερο χώρο διευθύνσεων από ότι αν έπρεπε να χρησιμοποιούμαι αποκλειστικά επίσημες IP διευθύνσεις, ενώ ταυτόχρονα προστατεύουμε την ακεραιότητα του internet. Αν ένα μηχάνημα με NAT διεύθυνση συνδεθεί στο internet, δεν θα προκαλέσει διένεξη με τα άλλα μηχανήματα γιατί οι NAT διευθύνσεις φιλτράρονται αυτόματα από τους δρομολογητές.

Οι παρακάτω IP διευθύνσεις έχουν σχεδιαστεί για ιδιωτικά δίκτυα που δεν θα έχουν άμεση σύνδεση στο internet. Μπορούν φυσικά να συνδεθούν στο internet μέσω ενός proxy server ή μίας άλλης μεθόδου που εκτελεί NA T.

10.0.0.0 έως 10.255:255.255 (ένα A class δίκτυο)
172.16.0.0 έως 172.31.255.255 (16 συνεχόμενα δίκτυα B class)
192.168.0.0 έως 192.163.255.255 (256 συνεχόμενα δίκτυα C class)

Ο proxy server συμπεριλαμβάνει αυτόματα αυτές τις διευθύνσεις στον τοπικό πίνακα διευθύνσεων (local address table, LAT) κατά την αρχική εγκατάσταση του προγράμματος.

Τ ο αποτέλεσμα της χρήσης του proxy server είναι ότι όλα τα μηχανήματα του εσωτερικού δικτύου φαίνονται να έχουνε την ίδια IP για τον εξωτερικό κόσμο η οποία είναι η εξωτερική διεύθυνση του proxy server. Πρόκειται για την μοναδική IP διεύθυνση που πρέπει να έχει εκχωρηθεί επίσημη δημόσια διεύθυνση IP.

# 4. PROXY SERVER

Ο proxy server (Διακομιστής μεσολαβητής) αποτελεί άριστη πύλη διαχωρισμού μεταξύ του εσωτερικού δικτύου και του Internet. Αποτελεί ένα ιδιαίτερα αποτελεσματικό εργαλείο για την απόκρυψη των εσωτερικών λεπτομερειών και διευθύνσεων IP του δικτύου. Ενώ αυξάνει τη συνολική ταχύτητα πρόσβασης στο internet και μειώνει τις απαιτήσεις σε εύρος ζώνης. (bandwidth).

Ο στόχος του proxy server είναι σχετικά απλός, απομονώνει το εσωτερικό δίκτυο από το Internet ενώ παρέχει πλήρη πρόσβαση και λειτουργικότητα στους χρήστες του εσωτερικού δικτύου που θέλουνε πρόσβαση στο internet. Είναι σαν ένα ειδικό φίλτρο που επιτρέπει την πρόσβαση στο internet αλλά δεν αφήνει κανέναν από το internet να έχει πρόσβαση στο εσωτερικό δίκτυο.

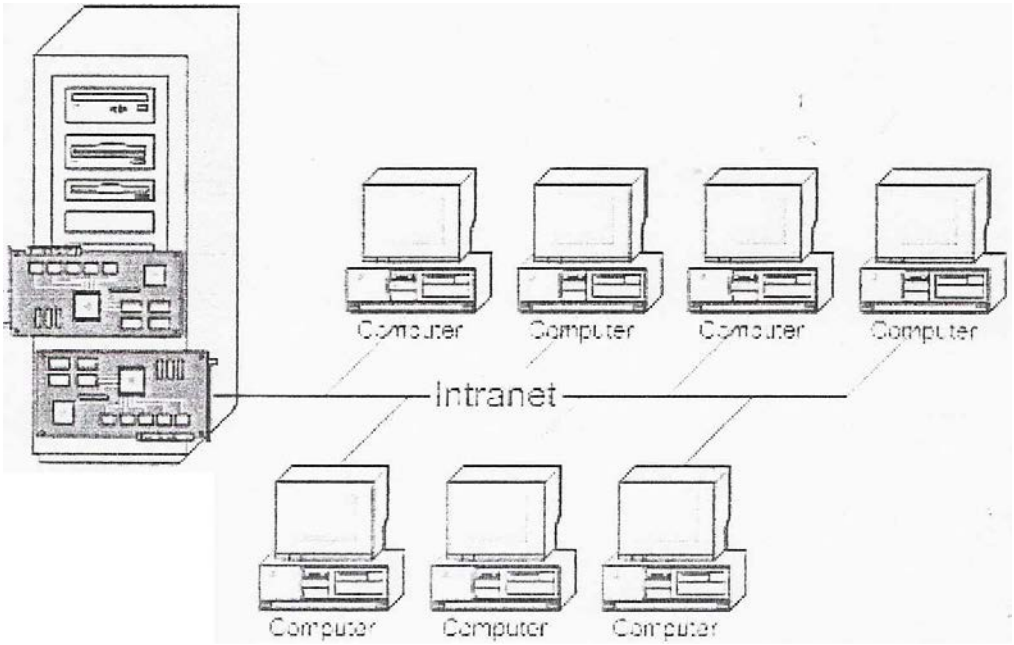
Ο proxy server απομονώνει το εσωτερικό δίκτυο από το internet, καθώς διαθέτει δύο (ή περισσότερες) εντελώς ξεχωριστές φυσικές συνδέσεις - μία με το internet και μία με το εσωτερικό δίκτυο. Κάθε δίκτυο συνδέεται με μία διαφορετική κάρτα δικτύου του proxy server, έτσι όλα τα πακέτα πρέπει να περάσουν από το λογισμικό του proxy server για να περάσουν από την μία σύνδεση στην άλλη.

Οι μηχανισμοί που χρησιμοποιεί ο proxy server για να επιτύχει αυτούς τους στόχους είναι:

. Μετάφραση διεύθυνσης δικτύου.

. Φιλτράρισμα πακέτων

. Χρήση κρυφής μνήμης



## 4.1 Διακομιστές διαμεσολάβησης- Proxy Servers

Ένας proxy είναι ένας μεσάζων σε μια διαδικτυακή συναλλαγή. Είναι μια εφαρμογή και βρίσκεται μεταξύ ένα πελάτη και έναν πραγματικό διακομιστή. Χρησιμοποιούνται πάρα πολύ συχνά και για firewalls για την παροχή ασφάλειας. Επιτρέπουν και μπορούν και να καταγράψουν αιτήσεις από το εσωτερικό μας δίκτυο προς το εξωτερικό δίκτυο.

Ένας proxy συμπεριφέρεται και σαν πελάτης, για τους εξωτερικούς διακομιστές, και σαν διακομιστής για τους εσωτερικούς πελάτες. Ο proxy δέχεται και επεξεργάζεται αιτήσεις από τους εσωτερικούς πελάτες και μετά τις προωθεί, σαν δικές του αιτήσεις προς τους εξωτερικούς διακομιστές. Όταν απαντήσει ένας εξωτερικός διακομιστής στον proxy, αυτός προωθεί τις απαντήσεις στον κατάλληλο πελάτη του δικτύου. Πολλές φορές οι proxy αναφέρονται και σαν "application layer gateways" (πύλες επιπέδου εφαρμογής). Αυτό το όνομα αντικατοπτρίζει το γεγονός ότι ο proxy βρίσκεται στο επίπεδο εφαρμογής του μοντέλου OSI , όπως και οι πελάτες -διακομιστές.

Οι proxy βρίσκουν πολλές εφαρμογές στον κόσμο των δικτύων. Μερικές από αυτές είναι:

- Logging. Η καταγραφή συμβάντων
- Access controls.
- Φιλτράρισμα
- Μετάφραση-μεταγλώτιση
- Έλεγχος για ιούς
- Caching
- Reverse proxy
- Reverse hosting
- Server proxying

Τα βασικότερα πλεονεκτήματα ενός proxy server είναι:

**1.** *Η ασφάλεια:* η δυνατότητα να επιτρέπεις ή να αποτρέπεις την πρόσβαση σε εξωτερικούς διακομιστές με την χρήση κάποιων "access list".

**2.** *Καταγραφή συμβάντων:* Η καταγραφή των κινήσεων των πελατών με πρόσβαση στο εξωτερικό δίκτυο. Αναφορές και στατιστικά μπορούν να γεννηθούν από τα *logs.*

**3.** *Caching:* ιστοσελίδες που ζητούνται πολύ συχνά από πελάτες του δικτύου, αποθηκεύονται τοπικά σε κάποιο κοινόχρηστο πόρο και είναι προσβάσιμες για όλους τους τοπικούς πελάτες.. Αυτό εξυπηρετεί διότι κάνουμε εξοικονόμηση του bandwidth (εύρους ζώνης) της σύνδεσης του Internet.

Υπάρχουν δύο τύποι proxy. Ο πρώτος είναι ο application-level proxy (επιπέδου εφαρμογής), ο οποίος καταλαβαίνει την υπηρεσία του επιπέδου εφαρμογής για την οποία κάνει την διαμεσολάβηση. Καταλαβαίνει και μπορεί και διερμηνεύει τις εντολές του πρωτοκόλλου του επιπέδου εφαρμογής που χρησιμοποιείται.

## 4.2 Πώς λειτουργούν οι Proxy Servers και οι Transparent Proxy Servers

Ας υποθέσουμε ότι έχουμε την εταιρία company.com. Έχουμε ένα εσωτερικό δίκτυο και μια σύνδεση για το Internet, την ppp στον proxy (proxy.company.com με εξωτερική διεύθυνση την 1.2.3.4 και εσωτερική την 192.168.0.1). έχουμε και έναν host που θα τον λέμε "εγώ" και έχει διεύθυνση 192.168.0.100.

## 4.3Παραδοσιακό Proxy

Σε αυτό το σενάριο τα πακέτα από το ιδιωτικό δίκτυο προς το Internet ποτέ δεν θα το διασχίσουν και το αντίθετο. . Οι διευθύνσεις του δικτύου πρέπει να είναι εσωτερικές (οι 192.168.*.*,10.*.*.*,172.16.*.* - 172.31.*.* δεν είναι πραγματικές διευθύνσεις του Internet). Ο μόνος τρόπος που βγαίνει κάποιο πακέτο προς το Internet είναι από τον proxy-firewall. Έχουμε εγκαταστήσει τον proxy μας στο port 8080. Ο "εγώ" έχει ρυθμίσει τον φυλλομετρητή του να χρησιμοποιεί τον proxy στο port 8080. Στο ιδιωτικό δίκτυο δεν χρειάζεται να ορίσουμε gateway.

Δίνουμε στο φυλλομετρητή του host την διεύθυνση http://www.teiep.gr. Ο φυλλομετρητής μας πηγαίνει στον proxy port 8080 χρησιμοποιώντας για τον εαυτό του το port 1100. Του ζητά την σελίδα. Εάν την έχει στην cache του την επιστρέφει. Αν όχι, τότε ψάχνει το www.teiep.gr και βρίσκει την διεύθυνση Α.Β.Γ.Δ Ανοίγει τότε μια σύνδεση προς αυτόν από το port 1123 στο port 80 του διακομιστή και ζητά την ιστοσελίδα. Καθώς την παραλαμβάνει, την κρατά στην cache και την προωθεί στη σύνδεση προς το φυλλομετρητή του "εγώ".

Από την πλευρά του teiep.gr, η σύνδεση γίνεται από το 1.2.3.4 της ppp

σύνδεσης του proxy με port 1123 προς το Α.Β.Γ.Δ στο port 80 του διακομιστή του. Από την πλευρά του "εγώ", η σύνδεση γίνεται από το 192.168.0.100 με port 1100 προς το 192.168.0.1, την εσωτερική διασύνδεση του proxy, στο port 8080.

## 4.4 Διαφανής Proxy (Transparent proxy)

Και σε αυτό το σενάριο, τα πακέτα από το ιδιωτικό δίκτυο προς το Internet ποτέ δεν θα το διασχίσουν και το αντίθετο. Οι διευθύνσεις του δικτύου μας είναι και εδώ ιδιωτικές. Ο μόνος τρόπος που βγαίνει κάποιο πακέτο προς το Internet είναι από τον proxy-firewall ο οποίος συνδέεται και στα δύο δίκτυα. Τρέχουμε ένα πρόγραμμα για transparent proxying (διαφανής διαμεσολάβηση) και τα πακέτα που εξέρχονται από αυτό το μηχάνημα αλλάζουν προορισμό και πηγαίνουν προς τον transparent proxy. Διαφανής διαμεσολάβηση (transparent proxy) σημαίνει ότι οι πελάτες δεν χρειάζεται ότι ανακατεύεται ένας proxy.

. Θα χρησιμοποιήσουμε ένα παρόμοιο παράδειγμα με το προηγούμενο. Οι διευθύνσεις του δικτύου είναι ίδιες με το παραπάνω παράδειγμα, καθώς και του "εγώ", του

transparent proxy-firewall και του www.teiep.gr. Ο proxy είναι

εγκατεστημένος στο port 8080. Ο πυρήνας κάνει ανακατεύθυνση του port πηγής 80 προς το port 8080 του proxy. Ο φυλλομετρητής μας είναι ρυθμισμένος να συνδέεται απ' ευθείας. Το gateway στο ιδιωτικό μας δίκτυο πρέπει να δείχνει στον proxy - firewall (gw: 192.168.0.1).

Δίνουμε στο φυλλομετρητή μας την διεύθυνση www.teiep.gr. Τότε ανοίγει μια σύνδεση προς αυτή τη διεύθυνση από το τοπικό port 1050 και ζητά από το διακομιστή την ιστοσελίδα (port 80). Καθώς τα πακέτα από το Εγώ(1Ο50) περνούν στο μηχάνημα με τον proxy (80), ανακατευθύνονται στον αναμένοντα proxy στο port 8080. Ο proxy ανοίγει μια σύνδεση από το port 1100 προς το Α.Β.Γ.Δ port 80 όπου πήγαιναν τα πρωτότυπα πακέτα. Καθώς ο proxy παίρνει τα δεδομένα από αυτή τη σύνδεση τα ανακατευθύνει προς τη σύνδεση με τον φυλλομετρητή ο οποίος και ανακατασκευάζει και προβάλλει την ιστοσελίδα.

Από την πλευρά του teiep.gr η σύνδεση γίνεται από το 1.2.3.4 (port 1100) προς το Α.Β.Γ.Δ στο port 80. Από την πλευρά του εγώ, η σύνδεση γίνεται από το 192.168.0.100 port 1050 προς το Α.Β.Γ.Δ στο port 80, αλλά στην πραγματικότητα μιλά με τον transparent proxy μας.

## 4.5 Χαρακτηριστικά ενός Caching Proxy Server

Το βασικότερο χαρακτηριστικό ενός caching proxy είναι η δυνατότητα να αποθηκεύει απαντήσεις άλλων διακομιστών για μετέπειτα χρήση, κάτι το οποίο μας γλιτώνει χρόνο και εύρος ζώνης. Συνήθως έχουν και πολλά άλλα πολύ χρήσιμα χαρακτηριστικά που μπορούν να φανούν πολύτιμα. Τα περισσότερα από αυτά είναι λίγο άσχετα με το caching αλλά μπορείς να τα κάνεις μόνο με έναν caching proxy. Για παράδειγμα αν θέλεις να αυθεντικοποιείς τους χρήστες σου αλλά δεν ενδιαφέρεσαι να κάνεις caching, είναι πολύ πιθανό να χρησιμοποιήσεις έναν caching proxy για αυτό το σκοπό.

## 4.6 Authentication (Αυθεντικοποίηση)

Ο proxy μπορεί να ζητά από τους χρήστες του να αυθεντικοποιούνται πριν εξυπηρετήσει οποιεσδήποτε αιτήσεις τους. Αυτό είναι πολύ χρήσιμο για proxy-firewall. Όταν ο κάθε χρήστης έχει το δικό του όνομα χρήστη και κωδικό πρόσβασης, μόνο εξουσιοδοτημένοι χρήστες μπορούν, π.χ. να δουν ιστοσελίδες από το www από το δίκτυό μας. Ακόμα, προσφέρει έναν ποιοτικότερο τρόπο παρακολούθησης πιθανών προβλημάτων.

# 5. ΕΓΚΑΤΑΣΤΑΣΗ PROXY SERVER

Για να εγκαταστήσουμε τον proxy server, χρειαζόμαστε δύο κάρτες δικτύου, μία για τις εσωτερικές συνδέσεις με τον proxy server και μία για τις εξωτερικές συνδέσεις. Η εξωτερική κάρτα πρέπει να είναι απευθείας συνδεδεμένη με την πύλη για το internet. Ο proxy server απαιτεί περίπου 12 MB στο σκληρό δίσκο για την εγκατάσταση και επιπλέον επαρκή χώρο στο δίσκο για να υποστηρίζει την τοπική αποθήκευση ιστοσελίδων στην κρυφή μνήμη (περιοχή προσωρινής αποθήκευσης.) Για μικρά δίκτυα ο χώρος αυτός πρέπει να είναι της τάξης τον 100 MB έως 200 MB, όμως για μεγαλύτερα. και πιο ενεργά δίκτυα ο χώρος αυτός πρέπει να είναι τουλάχιστον 1Ο φορές μεγαλύτερος.

Για λόγους ασφαλείας, η εσωτερική μας κάρτα δικτύου πρέπει να ανήκει σε ξεχωριστό φυσικό τμήμα του δικτύου από την εξωτερική κάρτα δικτύου. Πρέπει να εξασφαλιστεί ότι όλη η κίνηση θα παραμένει μόνο στο τμήμα στο οποίο ανήκει, και ότι τα πάντα θα διέρχονται από τον proxy server. Η εξωτερική κάρτα δικτύου πρέπει να έχει μία έγκυρη, επίσημη διεύθυνση IP που έχουμε καταχωρήσει επίσημα για το τοπικό μας δίκτυο. Η εσωτερική κάρτα δικτύου και όλα τα εσωτερικά μηχανήματα μπορούν είτε να έχουν έγκυρες, καταχωρημένες IP διευθύνσεις ,είτε μπορούν να χρησιμοποιούν διευθύνσεις IP από το φάσμα διευθύνσεων ιδιωτικών δικτύων όπως περιγράφονται στο έγγραφο RFC 1918. Στο εσωτερικό τμήμα ισχύουν οι κανόνες δρομολόγησης, όπου η εσωτερική διεύθυνση IP του proxy server είναι και η τελική πύλη.

Για να εγκαταστήσουμε το λογισμικό του proxy server σε ένα διακομιστή των windows 2000, πρέπει να χρησιμοποιήσουμε το αρχείο Msp2wizi.exe (Τον οδηγό εγκατάστασης τής Microsoft - Microsoft Proxy Server Setup wizard). Αυτός ο οδηγός θα προσθέσει κατά την εγκατάσταση μία ενημέρωση του κώδικα. Για την εγκατάσταση του Proxy server ακολουθούμε τα παρακάτω βήματα:

1. Κλείνουμε όλες τις εφαρμογές.

2. Ξεκινάμε την εφαρμογή Msp2wizi.exe για να φανεί η οθόνη άδειας χρήσης της Microsoft.

3. Αφού διαβάσουμε την άδεια χρήσης πατάμε το Yes για να συμφωνήσουμε με αυτήν. (Αν πατήσουμε το πλήκτρο No η εγκατάσταση θα τερματιστεί). Αν πατήσουμε το πλήκτρο Yes θα εμφανιστεί η κύρια οθόνη του οδηγού εγκατάστασης.

4. Τοποθετούμε το CD του Microsoft proxy server στη μονάδα του CD-ROM και πατάμε το Continue για να αρχίζει το πρόγραμμα εγκατάστασης του Microsoft proxy server. Πατάμε continue για να συνεχίσουμε.

5. Πληκτρολογούμε τον κωδικό αδείας του προϊόντος που είναι μαζί με το CD εγκατάστασης και πατάμε το πλήκτρο OK για να συνεχίσουμε. Θα εμφανιστεί η οθόνη (product ID). Πατάμε πάλι το πλήκτρο OK για να ανοίξει το πλαίσιο διαλόγου για την θέσης εγκατάστασης.

6. Εδώ μπορούμε να αλλάξουμε τη θέση όπου θα εγκατασταθεί ο proxy server πατώντας το πλήκτρο Change Folder και επιλέγοντας τη νέα διαδρομή. Αφού επιλέξουμε τη νέα θέση

πατάμε το κουμπί με το PC και το CD για να προορίσουμε και να αλλάξουμε τις επιλογές της εγκατάστασης πού θέλουμε.

7. Επιλέγουμε τις επιλογές που θέλουμε να εγκαταστήσουμε για τον proxy server. Η προεπιλογή πρόκειται να εγκαταστήσει όλες τις επιλογές, που απαιτούν περίπου 12 MB ελεύθερου χώρου στο δίσκο. Όταν κάνουμε τις επιλογές μας, πατάμε το κουμπί Continue για να συνεχίσουμε.

8. Το πρόγραμμα εγκαταστάσεων θα σταματήσει τις υπηρεσίες Ιστού για να εγκαταστήσει τον proxy server. Θα μας ζητηθεί να ενεργοποιήσουμε την κρυφή μνήμη και για να επιλέξουμε το μέγεθος και τη θέση της.

9. Ρυθμίζουμε το μέγεθος και τη θέση της κρυφής μνήμης. Η προεπιλογή είναι στα 100 MB. Μπορούμε να τοποθετήσουμε την μνήμη σε οποιαδήποτε μονάδα δίσκων που είναι διαμορφωμένη σε NTFS, καλό είναι να διανείμουμε τη μνήμή σε όσους το δυνατόν περισσότερους δίσκους. Πατάμε το OK για να συνεχίσουμε.

10. Θα εμφανιστεί το παράθυρο (Local Address Table Configuration).Εδώ μπορούμε να χτίσουμε τον τοπικό πίνακα διευθύνσεών μας. Αυτός ο πίνακας λέει στον proxy server ποιες διευθύνσεις είναι τοπικές και ποιες να αναμείνει να βρει στο έξω στο δίκτυο.

11. Στο πλαίσιο Edit, βάζουμε τις διευθύνσεις του τοπικού δικτύου. Δεν χρειάζεται να προσθέσουμε τις NAT IP γιατί θα μπουν μόνες τους όταν κατασκευάσουμε τον πίνακα. (Με το πλήκτρο Construct Table).

12. Όταν πατήσουμε το πλήκτρο Add θα μετακινήσουμε μια σειρά διευθύνσεων από το Edit πλαίσιο προς το Internal IP Ranges. Όταν προσθέσουμε όλες τις εσωτερικές IP διευθύνσεις. Πατάμε το πλήκτρο Construct Table για να πάμε στο παράθυρο Construct Local Address Table.

13. Για να προσθέσουμε τις NAT διευθύνσεις IP αυτόματα, επιλέγουμε Add the private ranges to the table. Εάν θέλουμε να φορτώσουμε τις IP διευθύνσεις από τις εσωτερικές κάρτες επιλέγουμε το Load known address ranges from all IP internal cards και για να επιλέξουμε συγκεκριμένες κάρτες επιλέγουμέ το load known address ranges from the following IP interface cards. Όταν κάνουμε τις επιλογές μας πατάμε OK.

14. Ένα μήνυμα θα εμφανιστεί, προειδοποιεί ότι ο τοπικός πίνακας διευθύνσεων μπορεί να περιλάβει και εξωτερικές διευθύνσεις. Πατάμε OK για να επιστρέψουμε στο παράθυρο Local Address Table Configuration.

15. Τώρα βλέπουμε το αυτόματα διευθετημένο πίνακα (Local Address Table LAT), όπως θα τον δημιουργήσει ο Proxy server. Μπορούμε να αναιρέσουμε οποιεσδήποτε εξωτερικές διευθύνσεις από τον πίνακα ή οποιαδήποτε άλλα λάθη. Εάν δεν φαίνονται οι τοπικές διευθύνσεις μπορούμε να τις προσθέσουμε μέσα, πατάμε OK για να πάμε στο παράθυρο

εγκατάστασης / διαμόρφωσης πελατών.

16. Στο παράθυρο Client Installation/Configuration, βάζουμε τις επιλογές που ελέγχουν πώς οι πελάτες θα συνδέουν με τον Proxy server. Γενικά, οι προεπιλογές είναι κατάλληλες για χρήση, εάν όμως έχουμε συγκεκριμένες ανάγκες, μπορούμε να αλλάξουμε τις ρυθμίσεις. Όταν ολοκληρώσουμε τις ρυθμίσεις, πατάμε OK για να ανοίξουμε το παράθυρο ελέγχου πρόσβασης (Access control).

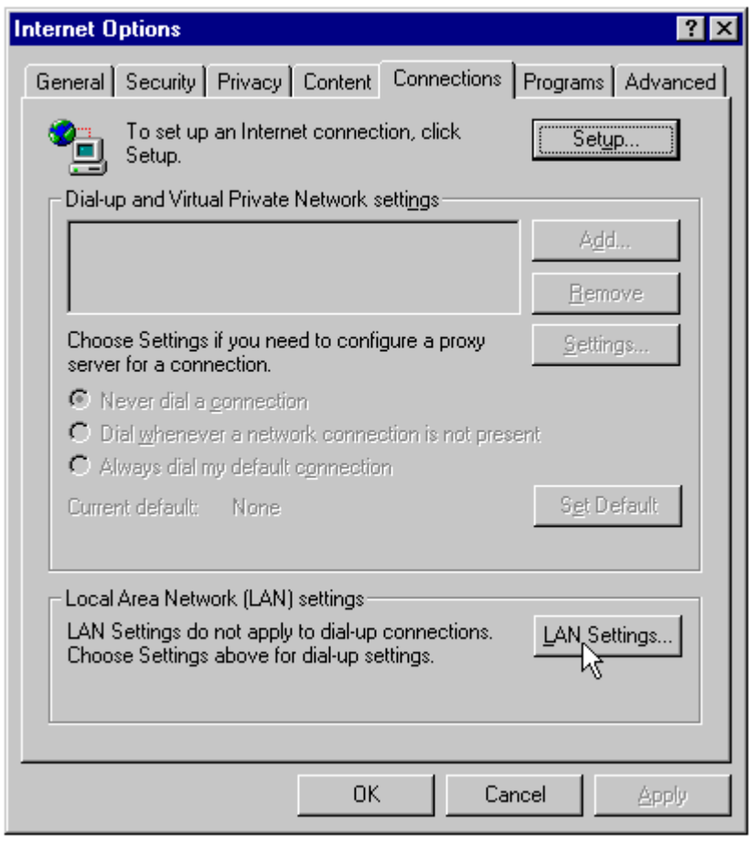
17. Εάν ενεργοποιήσουμε τον έλεγχο πρόσβασης στις υπηρεσίες WinSock και Web Proxy (ενεργοποιούνται στην εγκατάσταση), η πρόσβαση στο internet θα επιτρέπεται μόνο σε εκείνους τους πελάτες που έχουμε ορίσει ρητά την άδεια να χρησιμοποιούν αυτές τις εφαρμογές στον proxy server. Κανένας πελάτης δεν θα έχει πρόσβαση στο internet μέχρι να ρυθμίσουμε τον Proxy server. Εάν αλλάξουμε τα πλαίσια ελέγχου όλοι οι πελάτες θα έχουν πρόσβαση. Αυτές τις ρυθμίσεις μπορούμε να τις αλλάξουμε αργότερα από την διαχείριση του proxy server. Όταν τελειώσουμε τις ρυθμίσεις πατάμε OK.

18. Ένα μήνυμα θα εμφανιστεί που θα αναφέρει ότι το φιλτράρισμα πακέτων μπορεί να ενεργοποιηθεί αργότερα. Πατάμε το OK ώστε ο proxy server να τελειώσει την εγκατάσταση. Μετά πατάμε το πλήκτρο Finish και έχουμε τελειώσει με την εγκατάσταση. (Πρέπει να κάνουμε επανεκκίνηση του proxy server για να λειτουργούν οι νέες ρυθμίσεις).

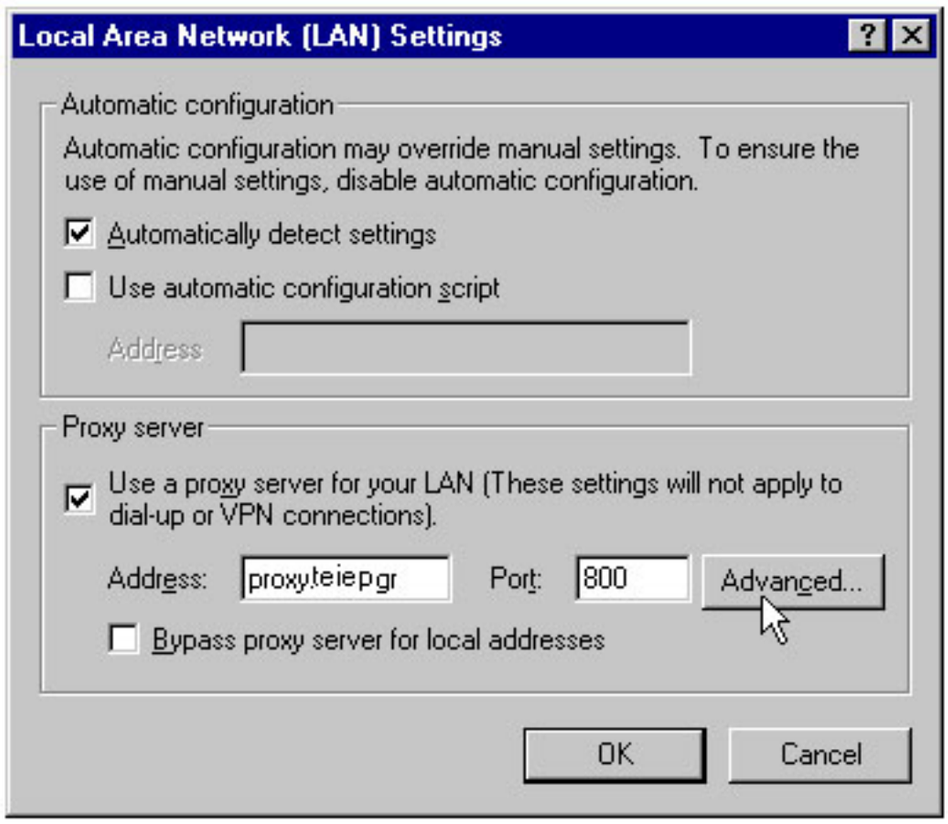
## 5.1 Ρύθμιση του proxy server

### 5.1.1 Διαμόρφωση του Internet Explorer

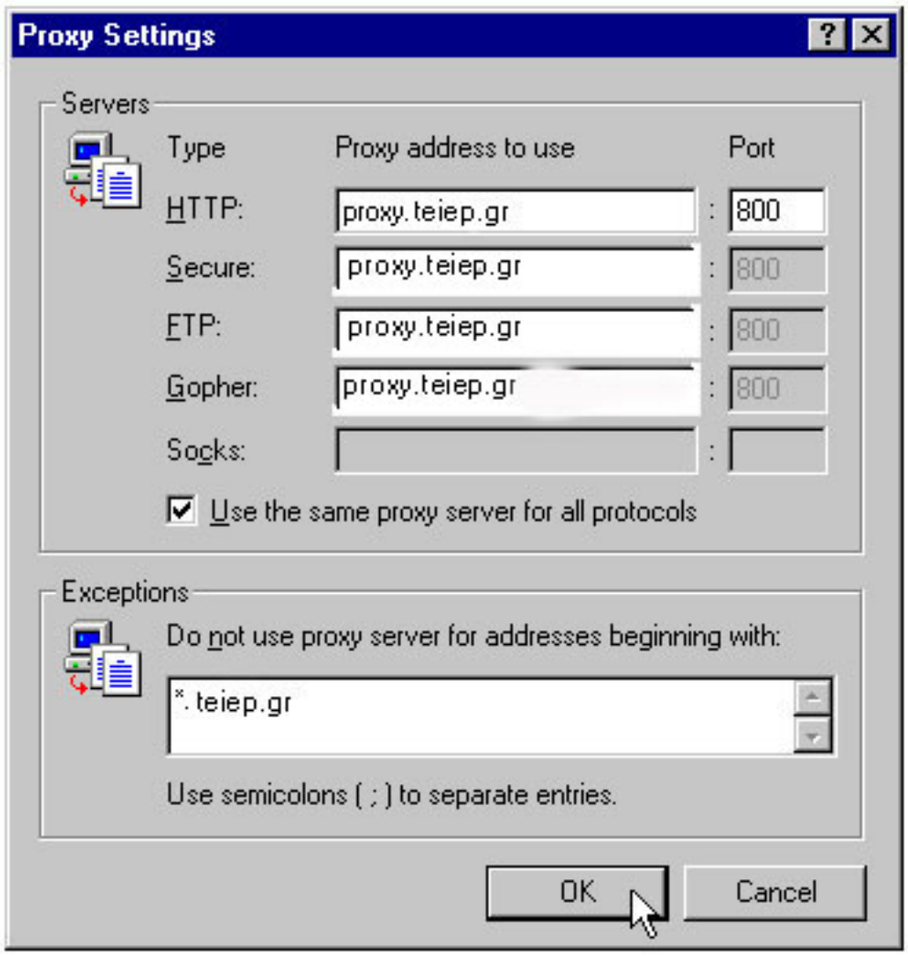
Από το μενού **Tools** επιλέγετε **Internet Options** και στο παράθυρο που θα εμφανιστεί την καρτέλα **Connections** και εν συνεχεία την επιλογή **LAN Settings...**




Συμπληρώνετε τα πεδία στην περιοχή Proxy server του παραθύρου **Local Area Network (LAN) Settings** όπως στην εικόνα



και επιλέγετε Advanced. Στο παράθυρο **Proxy Settings** συμπληρώνετε όπως παρακάτω:




Τερματίζετε τη διαδικασία επιλέγοντας OK.

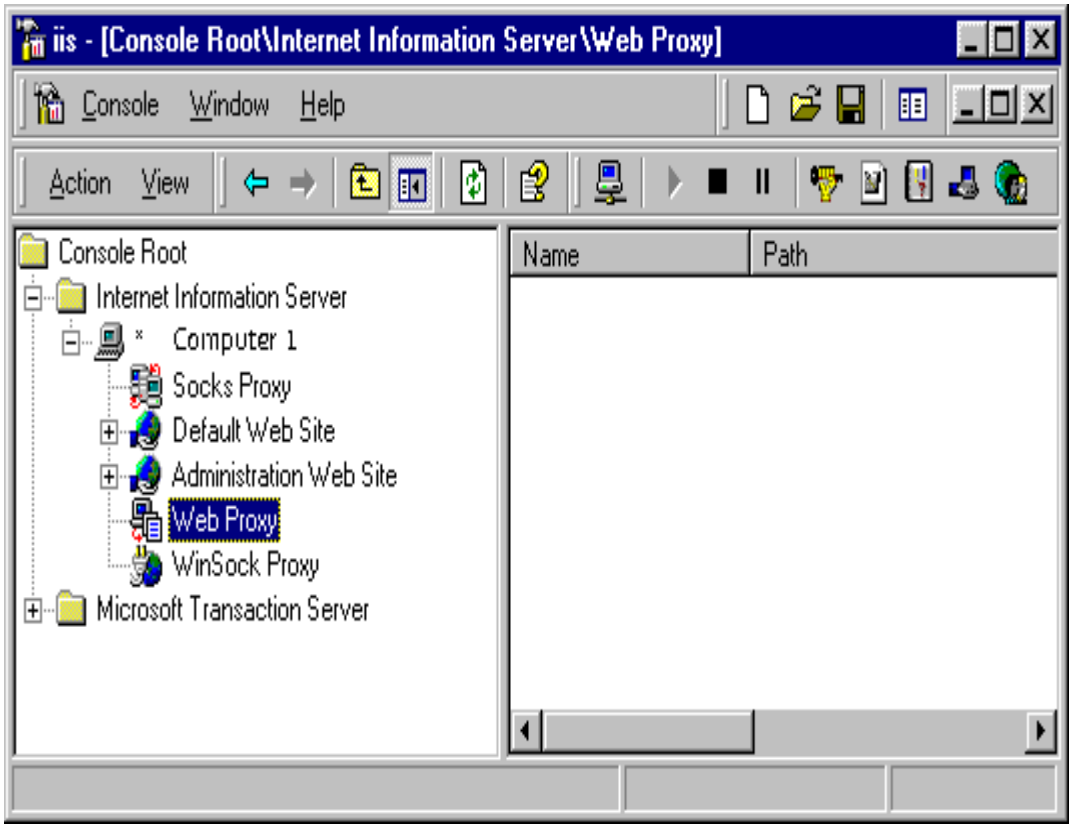
## 5.2 ΔΙΑΧΕΙΡΙΣΗ PROXY SERVER

Μετά την εγκατάσταση του Proxy Server οι περισσότερες Ρυθμίσεις έχουν ήδη καθοριστεί αν και είναι πιθανόν να χρειαστεί να αναθεωρήσουμε τις ρυθμίσεις εγκατάστασης ή τις ρυθμίσεις πρόσθετων επιλογών που δεν είναι διαθέσιμες στο πρόγραμμα εγκατάστασης.

Ο βασικός τρόπος διαχείρισης του Proxy Server γίνεται μέσω Internet Service Manager αν και μπορούμε και μέσω της γραμμής εντολών.
Σε περίπτωση που θέλουμε να κάνουμε τηλε-διαχείριση του Proxy Server ο υπολογιστής από τον οποίο διαχειριζόμαστε τον Proxy Server θα πρέπει να έχει την ίδια έκδοση Client με αυτή του Proxy Server. Για να διαχειριστούμε τον Proxy Server μέσω του Internet Service Manager θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

Ανοίγουμε το internet service manager από το μενού administrative tools.

1. Επιλέγουμε την επιλογή internet information services (IIS)στο δέντρο της κονσόλας και έπειτα επιλέγουμε την διαταγή connect..




2. Πατάμε το πλήκτρο Cancel αν είμαστε τοπικά συνδεδεμένοι στον proxy server. Σε περίπτωση που θέλουμε να συνδεθούμε σε απομακρυσμένο proxy server πληκτρολογούμε το όνομα του proxy server με το οποίο θέλουμε να συνδεθούμε.

3. Για να αλλάξουμε τις Ρυθμίσεις του web proxy ή του WinSock proxy ή και του socks proxy κάνουμε δεξί κλικ στο αντίστοιχο εικονίδιο του δέντρου και επιλέγουμε την διαταγή properties.

## 5.3 Φιλτράρισμα αιτήσεων

Οι caching proxy συχνά χρησιμοποιούνται για να φιλτράρουν αιτήσεις (Request Filtering) των χρηστών. Οι οργανισμοί. συνήθως έχουν κάποιες πολιτικές οι οποίες

απαγορεύουν στο προσωπικό την πρόσβαση πορνογραφικού υλικού τις ώρες εργασίας. Για την ενίσχυση της εφαρμογής αυτής της πολιτικής μπορεί να ρυθμιστεί ο proxy να απορρίπτει αιτήσεις προς γνωστές πορνογραφικές ιστοσελίδες. Αυτού του είδους το φιλτράρισμα είναι πολλές φορές αμφισβητήσιμο. Πολλοί το εξισώνουν με λογοκρισία και διευκρινίζουν, σωστά συχνά, ότι το φιλτράρισμα αιτήσεων δεν είναι και τέλειο.

## 5.4 Φιλτράρισμα απαντήσεων

Οι proxy μπορούν να φιλτράρουν απαντήσεις (response filtering). Αυτό συνήθως αναφέρεται στον έλεγχο των περιεχομένων ενός αντικειμένου που κατεβάζουμε. Ένα φίλτρο που ελέγχει για ιούς σε λογισμικό είναι ένα καλό παράδειγμα.

## 5.5 Prefetching

Prefetching είναι η διαδικασία ορισμένων δεδομένων προτού ζητηθεί.
Συστήματα δίσκων και μνημών συνήθως χρησιμοποιούν τη μέθοδο "Prefetching" επίσης γνωστό και ως "read ahead" (προ διάβασμα). Για τον ιστό συνήθως χρησιμοποιείται για να ανακτήσει υπέρ-συνδέσμους και εικόνες από ένα αρχείο HTML.

Είναι μια ανταλλαγή μεταξύ του χρόνου απόκρισης (latency) και του εύρους ζώνης. Ένας proxy επιλέγει αντικείμενα για το prefetch υποθέτοντας ότι κάποιος πελάτης θα τα ζητήσει. Σωστές προβλέψεις έχουν ως αποτέλεσμα μείωση του χρόνου απόκρισης. Λανθασμένες προβλέψεις ωστόσο χρησιμοποιούν άδικα το εύρος ζώνης.

Πέρα από την χρήση κρυφών αντιπροσώπων με σκοπό την μείωση του χρόνου απόκρισης που παρατηρούν οι χρήστες, ένας άλλος μηχανισμός που αποβλέπει στο ίδιο αποτέλεσμα, είναι η προώθηση των αντικειμένων στους χρήστες πριν ακόμα αυτοί τα ζητήσουν (prefetching). Η παράδοση των αντικειμένων γίνεται κατά το διάστημα όπου ο χρήστης βλέπει τα περιεχόμενα μίας ιστοσελίδας. Το ποια αντικείμενα πρόκειται να παραδοθούν στους χρήστες, καθορίζεται από το γεγονός ότι οι χρήστες ακολουθούν τους συνδέσμους (hyperlinks) μιας ιστοσελίδας σε συνδυασμό με την παρακολούθηση των ροών αιτήσεων από τους εξυπηρετητές που έχει σαν αποτέλεσμα τον εντοπισμό των δημοφιλών αντικειμένων.

Το σύστημα λοιπόν που αναλαμβάνει να υλοποιήσει τον παραπάνω μηχανισμό [31], αποτελείται από ένα σύνολο από διεργασίες (processes) που εκτελούνται τόσο στην πλευρά του εξυπηρετητή, όσο και στην πλευρά του χρήστη. Οι διεργασίες στην πλευρά του εξυπηρετητή αναλαμβάνουν να προβλέψουν την επόμενη αίτηση του χρήστη και να προωθήσουν το επόμενο αντικείμενο σε αυτόν. Οι διεργασίες στην πλευρά του χρήστη αναλαμβάνουν να παραδώσουν τα αντικείμενα στον χρήστη αλλά και να ενημερώσουν τις διεργασίες στον εξυπηρετητή για την συμπεριφορά του χρήστη.

Η χρήση κρυφών αντιπροσώπων σε συνδυασμό με την προώθηση αντικειμένων μπορεί να μειώσει ακόμα περισσότερο τον χρόνο που απαιτείται για να παραδοθεί ένα αντικείμενο στον χρήστη από την στιγμή που αυτό θα ζητηθεί [26]. Οι περισσότεροι κρυφοί αντιπρόσωποι είναι παθητικοί με την έννοια ότι αναλαμβάνουν δράση μόνο όταν γίνει η απαραίτητη αίτηση. Ενεργητικοί κρυφοί αντιπρόσωποι είναι αυτοί, που παράλληλα χρησιμοποιούν και ένα μηχανισμό προώθησης αντικειμένων (παρόμοιος με αυτόν που περιγράφτηκε πιο πριν), αποθηκεύοντας αντικείμενα στον δίσκο που

προβλέπεται ότι θα ζητηθούν στο μέλλον από τους χρήστες. Η προώθηση αντικειμένων μπορεί να χωριστεί σε δύο κατηγορίες με βάση τον "τόπο" όπου γίνεται η πρόβλεψη. Έτσι η πρώτη κατηγορία είναι τοπική προώθηση (local prefetching), όπου χρησιμοποιείται τοπική πληροφορία για την πρόβλεψη (δηλαδή μελετάται η ροή αιτήσεων του συνόλου των χρηστών που καλύπτει ο κρυφός αντιπρόσωπος). Η δεύτερη κατηγορία είναι η προώθηση με βάση τις υποδείξεις του εξυπηρετητή (server hint prefetching) όπου η πρόβλεψη γίνεται με βάση τις παρατηρήσεις από την πλευρά του εξυπηρετητή σχετικά με τα αντικείμενα και την ροή αιτήσεων προς αυτά.

## 5.6 Μετάφραση και Μετατροπή κώδικα

Η μετάφραση και η μετατροπή του κώδικα αναφέρονται στην επεξεργασία του περιεχομένου χωρίς τη σημαντική μετατροπή του νοήματος ή της εμφάνισης. Σαν παράδειγμα μπορούμε να φανταστούμε μια εφαρμογή η οποία μεταφράζει μια ιστοσελίδα από αγγλικά σε ελληνικά καθώς την κατεβάζει.

Η μετατροπή του κώδικα συνήθως αναφέρεται σε χαμηλού επιπέδου αλλαγές σε ψηφιακά δεδομένα παρά σε υψηλού επιπέδου ανθρώπινη γλώσσα. Η αλλαγή του format μιας εικόνας από gif σε jpeg είναι ένα καλό παράδειγμα. Το νόημα αυτής της διαδικασίας είναι ότι μια εικόνα σε jpeg είναι μικρότερη σε μέγεθος, άρα και μπορούμε να μειώσουμε το χρόνο μεταφοράς. Ένα ζεύγος proxy που συνεργάζονται, μπορούν να συμπιέσουν όλες τις μεταφορές μεταξύ τους και να τις αποσυμπιέσουν πριν φτάσουν στον πελάτη.

## 5.7 Σχηματισμός Κίνησης (Traffic Shaping)

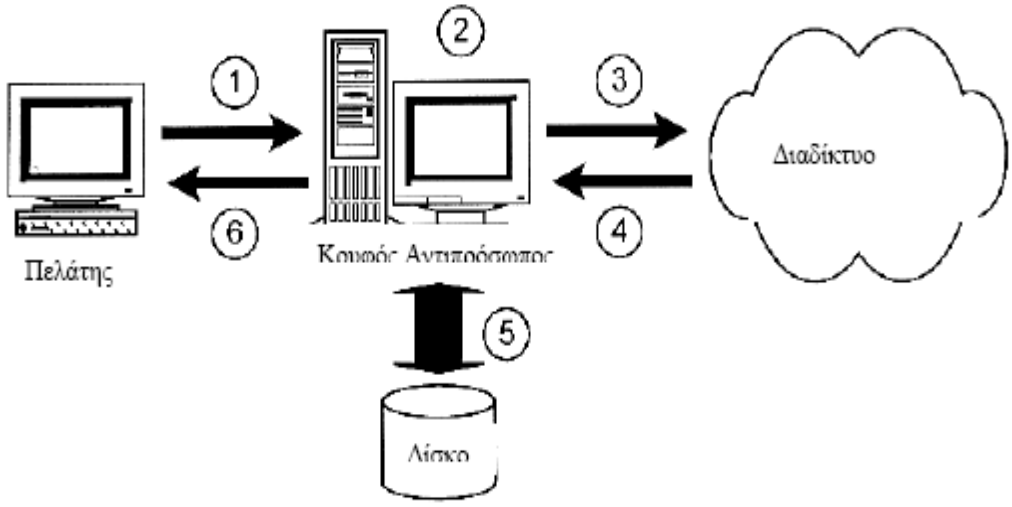
Ένας σημαντικός αριθμός οργανισμών χρησιμοποιούν proxy επιπέδου εφαρμογής για να ελέγχουν τη χρησιμοποίηση του εύρους ζώνης. Κατά μιαν έννοια, αυτή η διαδικασία γίνεται στο επίπεδο δικτύου όπου είναι δυνατόν ο έλεγχος της ροής των πακέτων, ωστόσο το επίπεδο εφαρμογής παρέχει πολύ χρήσιμες επιπλέον πληροφορίες.

Πριν συνεχίσουμε, πρέπει να εξηγήσουμε τι είναι cache hits και cache misses. Τα

"cache-hits" είναι οι αιτήσεις σελίδων ή αντικειμένων που βρέθηκαν στην cache και δεν χρειάσθηκε να γίνει καν σύνδεση με τον πραγματικό διακομιστή. Αυτό συνήθως γίνεται επειδή κάποιος χρήστης έχει νωρίτερα ζητήσει την σελίδα και αυτή έχει κρατηθεί στην cache. Αυτή είναι η πλέον επιθυμητή κατάσταση μιας cache-proxy. Τα "cache-misses" είναι οι αιτήσεις οι οποίες δεν ικανοποιήθηκαν από την cache μας και χρειάστηκε η επικοινωνία της cache με τον πραγματικό διακομιστή ώστε να πάρει απάντηση ο πελάτης. Τα ποσοστά αυτών των επιτυχιών και αποτυχιών, καθώς και άλλα στατιστικά στοιχεία μπορούμε να τα καταγράφουμε (logging).

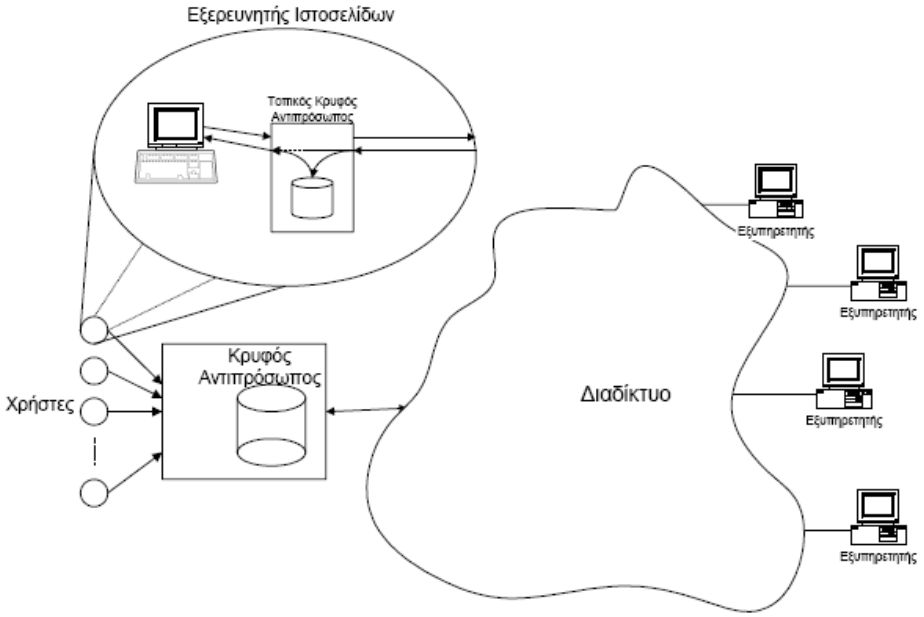
# 6. Κρυφός Αντιπρόσωπος (proxy cache)

Τα τελευταία χρόνια, πολύς λόγος έχει γίνει για τους κρυφούς αντιπροσώπους (proxy cache). Ένας κρυφός αντιπρόσωπος βρίσκεται ανάμεσα στο εξυπηρετητή και στον πελάτη. Συμπεριφέρεται σαν εξυπηρετητής για τους πελάτες και σαν πελάτης για τους εξυπηρετητές. Μπορούν να χρησιμοποιηθούν σαν συστήματα ελέγχου πρόσβασης, προστασίας τοπικού δικτύου κ.α. Η πιο διαδεδομένη χρήση τους είναι η προσωρινή αποθήκευση αντικειμένων με σκοπό την μείωση της κίνησης στο διαδίκτυο και την γρηγορότερη απόκριση στις αιτήσεις των πελατών.



Η Λειτουργία ενός κρυφού αντιπροσώπου, όταν ένας πελάτης στείλει μία αίτηση για ένα αντικείμενο 1 στον εξυπηρετητή, η αίτηση πρώτα επεξεργάζεται από τον κρυφό αντιπρόσωπο. Ο τελευταίος αναζητά το αντικείμενο στον αποθηκευτικό του χώρο (που μπορεί να είναι ο σκληρός δίσκο ή μνήμη RAM ή και τα δύο) 2. Εάν βρεθεί τότε στέλνεται πίσω στον πελάτη 6 χωρίς να χρειαστεί να επικοινωνήσει με τον απομακρυσμένο εξυπηρετητή. Σε αυτή την περίπτωση έχουμε τοπικό κτύπημα (hit) στα αποθηκευμένα αντικείμενα του αντιπροσώπου. Έτσι από τι μία ο πελάτης λαμβάνει πιο γρήγορα το αντικείμενο, ενώ από την άλλη αποφεύγεται η επιπλέον κίνηση στο διαδίκτυο και η επιβάρυνση του εξυπηρετητή που διαθέτει το αντικείμενο. Εάν δεν βρεθεί το αντικείμενο, τότε ο αντιπρόσωπος επικοινωνεί με τον εξυπηρετητή 3, λαμβάνει το αντικείμενο 4, και το προωθεί στον πελάτη 6 ενώ παράλληλα το αποθηκεύει στον αποθηκευτικό του χώρο για εξυπηρέτηση μελλοντικών αιτήσεων 5.

Παράλληλα με τους κρυφούς αντιπροσώπους στο διαδίκτυο, υπάρχουν και κρυφοί αντιπρόσωποι υλοποιημένοι μαζί με τους εξερευνητές ιστοσελίδων (browser cache) που σκοπό έχουν να αποθηκεύουν προσωρινά, τα αντικείμενα τα οποία ζητάει ένας μόνο χρήστης. Οι διαφορά τους από τους αντιπροσώπους του διαδικτύου είναι ότι οι τελευταίοι καλύπτουν ένα μεγαλύτερο αριθμό χρηστών όπως φαίνεται στο Σχήμα .




**Σχήμα 1-2. Κρυφός αντιπρόσωπος διαδικτύου και εξερευνητή ιστοσελίδων.**

Εν κατακλείδι, η χρήση των κρυφών αντιπροσώπων αποβλέπει στο να μειώσει το χρόνο

που απαιτείται για να εμφανιστούν τα περιεχόμενα μιας ιστοσελίδας που ζητάει ο χρήστης , να μειώσει την κατανάλωση του πολύτιμου εύρους ζώνης (bandwidth), μιας και η επικοινωνία με τον εξυπηρετητή γίνεται λιγότερο συχνά, και τέλος να μειώσει τον φόρτο εργασίας στον εξυπηρετητή . Για να είναι όμως αποτελεσματικό το εγχείρημα αυτό πρέπει από τη μια το κόστος παράδοσης του αντικειμένου μέσο του κρυφού αντιπροσώπου να είναι μικρότερο από το κόστος παράδοσης του αντικειμένου κατευθείαν από τον εξυπηρετητή (το κόστος μπορεί να εκφραστεί σαν την αποτελεσματικότητα του software και hardware που χρησιμοποιείται στον κρυφό αντιπρόσωπο, ο φόρτος εργασίας σε μια δεδομένη στιγμή κ.α.). Από την άλλη τα χαρακτηριστικά της ροής αιτήσεων (request streaming) πρέπει να είναι τέτοια ώστε να είναι ευνοεί την χρήση κρυφού αντιπροσώπου. Με άλλα λόγια πρέπει στο σύνολο των αιτήσεων να υπάρχουν και αιτήσεις για εξαιρετικά δημοφιλή αντικείμενα.

Τέτοια χαρακτηριστικά παρατηρούνται σήμερα στο διαδίκτυο αφού ένα μικρό σύνολο όλων των αντικειμένων τυγχάνουν ιδιαίτερης προσοχής από τους χρήστες. Τέτοια αντικείμενα είναι για παράδειγμα τα περιεχόμενα της ιστοσελίδας του CNN, του Yahoo κ.α.

Παρά το γεγονός ότι η χρήση κρυφών αντιπροσώπων φαίνεται να είναι ιδιαίτερα αποδοτική, παρουσιάζονται ορισμένα μειονεκτήματα. Αυτά, εν συντομία, είναι:

i) είναι δύσκολο να εγγυηθεί ότι το αντικείμενο που δίνεται στον χρήστη είναι και το ποιο πρόσφατο. Έτσι ενδέχεται αλλαγές που έχουν γίνει σε μια ιστοσελίδα να μην μπορεί να τις δει ο χρήστης.

ii) Εάν εξαιτίας του υπερβολικού φόρτου, ο κρυφός αντιπρόσωπος πάψει να λειτουργεί τότε η πρόσβαση στο διαδίκτυο θα είναι αδύνατη για όλους τους πελάτες που είναι συνδεδεμένοι σε αυτόν. Έτσι ο κρυφός αντιπρόσωπος είναι δυνατό να γίνει σημείο κατάρρευσης.

iii) Οι διαχειριστές των εξυπηρετητών πολλές φορές θέλουν να γνωρίζουν την καταγωγή των χρηστών που προσπελαύνουν τα αντικείμενα τους, ποια αντικείμενα ζητούν ποιοι και άλλα στατιστικά τα οποία τείνουν να θολώνουν οι κρυφοί αντιπρόσωποι αφού όλοι οι χρήστες έχουν το ίδιο ip.

iv) Ορισμένοι υποστηρίζουν ότι το δυναμικό – προσωπικό περιεχόμενο του διαδικτύου συνεχώς αυξάνεται σε σχέση με το στατικό και ανεξάρτητο από τον χρήστη. Τα δυναμικά αντικείμενα δεν πρέπει να αποθηκεύονται στους κρυφούς αντιπροσώπους, γιατί προορίζονται για ένα και μόνο χρήστη. Έτσι ενδέχεται στο μέλλον να μην είναι αποτελεσματική η χρήση κρυφών αντιπροσώπων.

## 6.1 Transparent Caching

Το transparent caching ή διαφανής caching, λέγεται έτσι γιατί αναχαιτίζει την δικτυακή κίνηση στον φυλλομετρητή. Σε αυτή την κατάσταση, η cache "βραχυκυκλώνει" την διαδικασία ανάκτησης εάν το επιθυμητό αρχείο βρίσκεται στην cache. Τα transparent caches είναι εξαιρετικά χρήσιμα για τις εταιρίες παροχής υπηρεσιών internet,οι φυλλομετρητές δεν χρειάζονται ρύθμιση. Αλλά είναι και ο πιο απλός τρόπος να χρησιμοποιούμε μία cache σ' ένα ιδιωτικό δίκτυο και αυτό επειδή δεν απαιτούν κάποιο σαφή συντονισμό με άλλες cache.Ο όρος διαφανής- transparent είναι υπερφορτωμένος, έχοντας διαφορετικές έννοιες κατά περίσταση. Κάποιες φορές εννοείται μια ρύθμιση η οποία παρεμβάλλεται στην κίνηση του port 80 προς εξωτερικούς διακομιστές από κάποιο χρήστη και την παρακάμπτει και κάποιες άλλες εννοείται ένας σημασιολογικά διαφανής proxy που δεν αλλάζει την σημασία ή το περιεχόμενο των αιτήσεων και απαντήσεων του πελάτη. Στην πραγματικότητα δεν υπάρχει πραγματική διαφάνεια, μόνο ημιδιαφάνεια και σίγουρα δεν υφίσταται διαφανής cache.

## 6.2 Πλεονεκτήματα της διαφανούς Caching

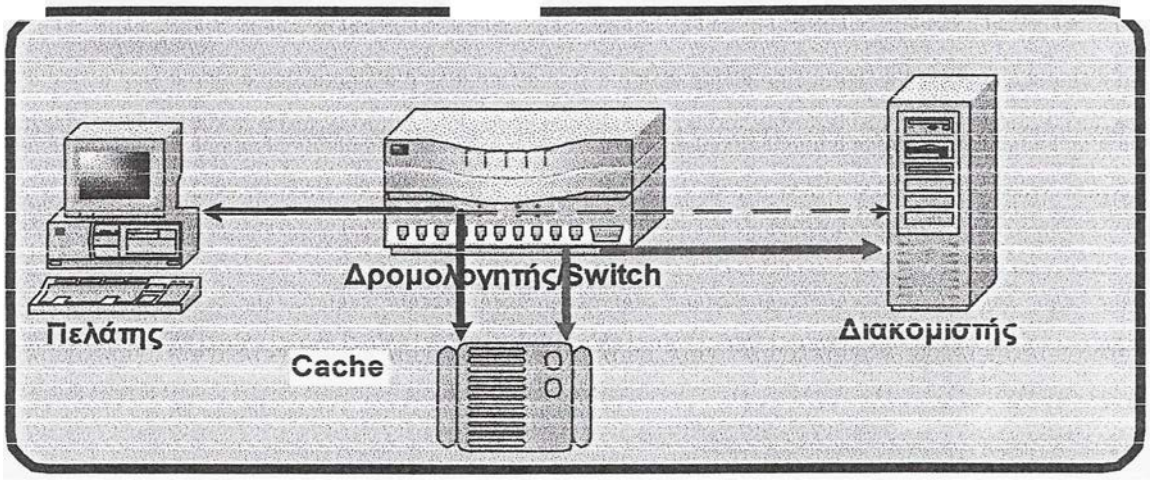
Τα πλεονεκτήματα της διαφανούς caching είναι περίπου τα αντίθετα από αυτά του proxy caching. Τα βασικότερα είναι:

- Εύκολη Διαχείριση- Ο φυλλομετρητής μας δεν χρειάζεται να είναι κατάλληλα ρυθμισμένος για να επικοινωνεί με την cache.
- Κεντρικός Έλεγχος- Ο χρήστης δεν μπορεί να αλλάξει τις ρυθμίσεις του φυλλομετρητή του ώστε να παρακάμψει τον proxy.

## 6.3 Μειονεκτήματα της διαφανούς caching

Κάποια από τα μειονεκτήματα που έχει η διαφανής caching είναι:

- Έλλειψη σταθερότητας- Λόγω του ότι βασίζεται στη σταθερή διαδρομή δρομολόγησης μεταξύ του πελάτη και του πραγματικού διακομιστή, η οποία τυγχάνει να περνά μέσα




από μια cached διαδρομή, είναι ευάλωτη σε αλλαγές δρομολόγησης στο Διαδίκτυο. Δηλαδή, αν μια γίνει σύνδεση ενός πελάτη με μια cache και συμβεί μια αλλαγή δρομολόγησης η οποία αναγκάζει τον πελάτη να πάρει μια διαδρομή η οποία δεν περνά από την συσκευή που έκανε την εκτροπή, η συνεδρία θα διακοπεί και ο χρήστης θα πρέπει να ξαναζητήσει την σελίδα. Αν, διαδρομές στο Διαδίκτυο αλλάζουν συνεχώς τότε τα αποτελέσματα θα είναι ακόμα πιο απρόβλεπτα.

- Έλεγχος χρηστών- Η διαφανής caching παίρνει τον έλεγχο από το χρήστη. Πολλοί χρήστες έχουν σοβαρές προκαταλήψεις σε ότι αφορά το caching και θα άλλαζαν παροχέα για να την αποφύγουν ή να την αποκτήσουν.

- Προαπαίτηση φυλλομετρητών- Πολλές διαφανής cache έχουν συγκεκριμένες απαιτήσεις από τους φυλλομετρητές των πελατών, δηλαδή στην κεφαλίδα του πακέτου να αναγράφεται το όνομα του host για τον οποίο προορίζεται και αυτό διότι οι cache αυτές δεν μπορούν να προσπελάσουν την IP διεύθυνση προορισμού από την IP διεύθυνση του πακέτου. Δηλαδή, σε περίπτωση που δεν υπάρχει η ζητούμενη στην cache, δεν μπορούν

να καταλάβουν ποιος είναι ο πραγματικός διακομιστής για να ζητήσουν από αυτόν τη σελίδα. Α ν και σήμερα, πάνω του 90% των φυλλομετρητών παρέχουν αυτό το χαρακτηριστικό.

## 6.4 Η Δρομολόγηση

Η διαδικασία της "απαγωγής" των πακέτων ξεκινά στο επίπεδο δικτύου (IP), όπου όλα τα IP πακέτα δρομολογούνται μεταξύ κόμβων. Σε αυτό το επίπεδο ένας δρομολογητής ή ένα switch αναγνωρίζει πακέτα HTTP και τα εκτρέπει προς μια cache αντί να τα προωθήσει στον αρχικό προορισμό. Υπάρχουν αρκετοί τρόποι για να πετύχουμε την απαγωγή.

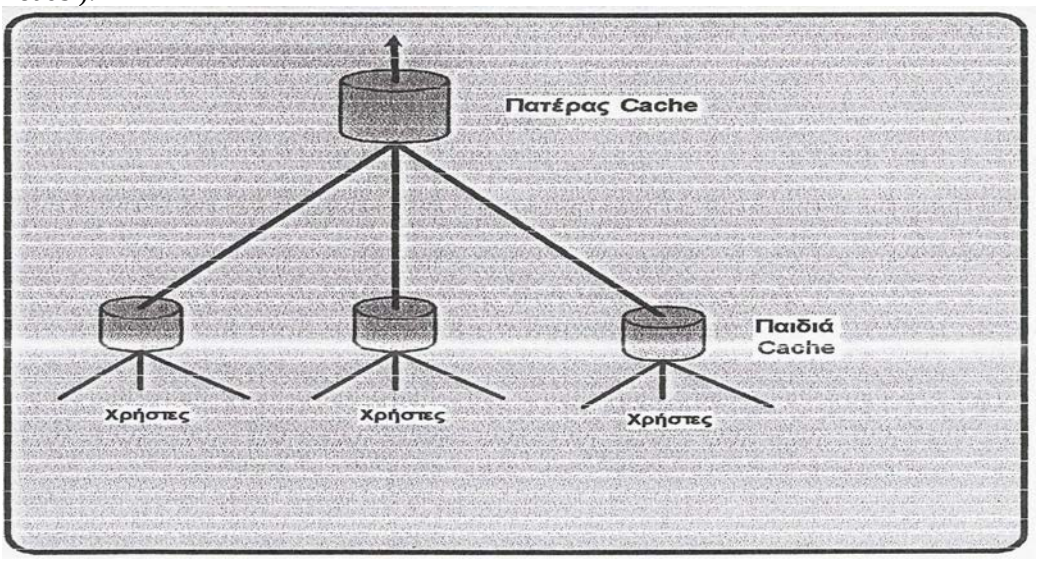
- **inline-** Ένα Inline cache είναι μια συσκευή η οποία συνδυάζει δρομολόγηση (ή και γεφύρωμα δικτύων-bridge) και caching ιστού σε ένα κομμάτι υλικού. Ένα παράδειγμα μπορεί να είναι ένας υπολογιστής με δύο ή περισσότερες κάρτες δικτύου το οποίο έχει για λειτουργικό σύστημα Linux ή unix και σε αυτό τρέχει ο Squid cache-proxy.
- *Επιπέδου* 4 switch - Το switch δουλεύει συνήθως στο επίπεδο 2 (επίπεδο σύνδεσης δεδομένων). Ένα switch επιπέδου 4 μπορεί να παίρνει και αποφάσεις προώθησης βασιζόμενο στα χαρακτηριστικά του επιπέδου 4 ( επίπεδο μεταφοράς), όπως είναι οι διευθύνσεις IP και αριθμοί port του TCP. Χρησιμοποιούνται επίσης και για εξισορρόπηση του φόρτου του διακομιστή.
- *Web Cache Coordination Protoco/* - Το WCCP είναι ένα πρωτόκολλο της CISCO SYSTEMS που απαιτεί την υλοποίησή του σ' ένα δρομολογητή (ή ακόμα και ένα switch) και στην cache. Αποτελείται από δύο συστατικά μέρη. Το πρώτο είναι το πρωτόκολλο ελέγχου και το δεύτερο είναι ο μηχανισμός ανακατεύθυνσης της κίνησης.
- *Cisco Policy Routing* - Η πολιτική δρομολόγησης (policy routing) αναφέρεται στην ικανότητα ενός δρομολογητή να παίρνει αποφάσεις για την προώθηση βασιζόμενο όχι μόνο στην διεύθυνση προορισμού του πακέτου. Μπορούμε να το χρησιμοποιήσουμε αυτό για να ανακατευθύνουμε πακέτα βασιζόμενοι στους αριθμούς port προορισμού.

# 7. Σχετικές Μελέτες Πάνω σε Κρυφούς Αντιπροσώπους

## 7.1 Συνεργαζόμενοι Κρυφοί Αντιπρόσωποι

### 7.1.1 Ιεραρχίες Cache

Μια ιεραρχία από cache είναι μια διευθέτηση από cache που συνεργάζονται μεταξύ τους. Σε μια τέτοια ιεραρχία, οι cache των κατώτερων επιπέδων προωθούν αποτυχίες (cache misses) της cache προς τα ανώτερα επίπεδά ώσπου να αποδεχτεί την αίτηση κάποια άλλη cache ή να προωθηθεί στον πραγματικό διακομιστη. Οι ιεραρχίες είναι ελκυστικές γιατί μπορούν να προσφέρουν βελτιώσεις της αποδοτικότητας. Κάποιες αποτυχίες της cache μας θα είναι επιτυχίες σε κάποιες από τις ανώτερες cache με αποτέλεσμα την μείωση του εύρους ζώνης του δικτύου και βελτιώνει την ταχύτητα του κατεβάσματος (downloads ).




Το παιδί-cache προωθεί τις αποτυχίες του (cache misses) σ' έναν πατέρα cache. Τότε ο πατέρας του παρέχει μια απάντηση από τη δική του cache, τον πραγματικό διακομιστή ή μια άλλη cache. Ένας πατέρας μπορεί να χρησιμοποιεί bandwidth προς τους πραγματικούς διακομιστές ώστε να ικανοποιήσει την αίτηση της cache του παιδιού.

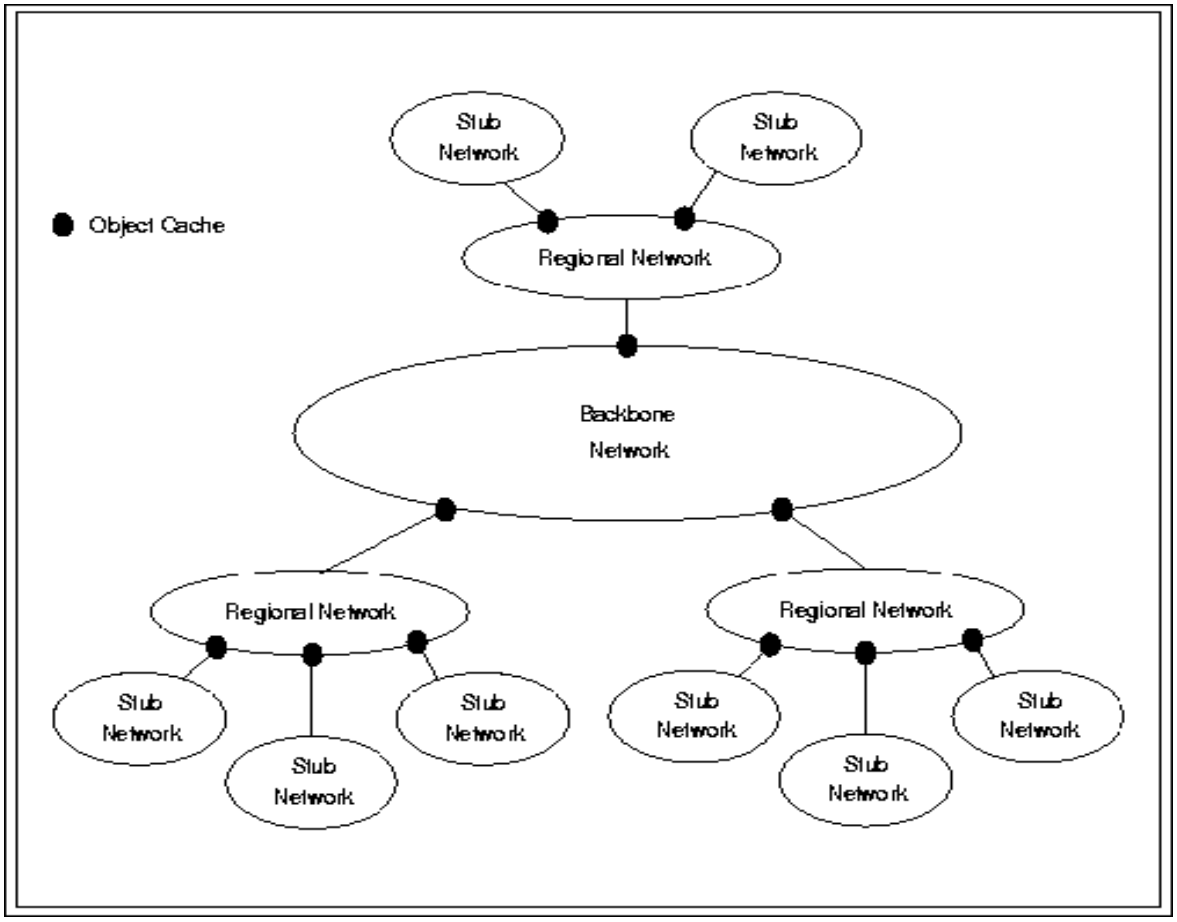
Οι σχέσεις των αδερφών-cache είναι σχεδιασμένες ώστε να αποτρέπουν μια cache να επιβαρύνει με κάποιο τίμημα μια άλλη cache. Όλες οι αιτήσεις που στέλνονται προς έναν αδερφό-cache θα πρέπει να είναι επιτυχίες (cache hits). Ένας αδερφός δε θα πρέπει ποτέ

να δώσει ένα αντικείμενο που έχει ζητηθεί από έναν πατέρα-cache και δεν υπάρχει στην cache του. Αν δεν υπάρχει επιστρέφει ένα μήνυμα ότι αρνείται να προωθήσει την αίτηση. Μια cache επικοινωνεί με τα παιδιά-cache χρησιμοποιώντας ένα από τα πρωτόκολλα *"Intercache"* . Αυτά τα πρωτόκολλα επιτρέπουν στις cache να μαθαίνουν εάν μια γειτονική cache έχει κάποιο συγκεκριμένο αντικείμενο στην cache τους. Μια αίτηση πρέπει να σταλθεί μόνο σ' έναν αδερφό εάν το πρωτόκολλο intercache προβλέπει ότι θα είναι επιτυχία cache.

Αυτές οι σχέσεις δεν είναι δεδομένες. Μια cache μπορεί να είναι πατέρας για κάποιες cache και αδερφός για άλλες. Αυτή είναι η πιο χρησιμοποιημένη μορφή ιεραρχίας από τους παροχείς Internet. Μια απεικόνιση αυτής της ιεραρχίας φαίνεται στην εικόνα 4.4.1.

## 7.1.2 Ιεραρχικές Δομές

Η βασική ιδέα είναι ότι οι αιτήσεις σε αντικείμενα τα οποία δεν βρίσκονται σε ένα κρυφό αντιπρόσωπο, μπορούν να εξυπηρετηθούν από ένα γειτονικό (κοντινό) αντιπρόσωπο ο οποίος ενδέχεται να έχει το αντικείμενο. Έτσι πολλοί κρυφοί αντιπρόσωποι συνεργάζονται, σχηματίζοντας μια ιεραρχική δομή (ένα δέντρο).
Αιτήσεις που δεν μπορούν να εξυπηρετηθούν από τον δίσκο ενός κρυφού αντιπροσώπου, διαβιβάζονται είτε στον πατέρα του είτε στα αδέρφια του. Η διαδικασία αυτή συνεχίζεται μέχρι η αίτηση να φτάσει στην ρίζα του δέντρου όπου τελικά αν δεν βρεθεί ούτε εκεί το αντικείμενο τότε διοχετεύεται στον απομακρυσμένο εξυπηρετητή. Πολλές μελέτες έχουν γίνει πάνω σε αυτό το μοντέλο και κατά καιρούς έχουν παρουσιαστεί ορισμένες παραλλαγές, όπως για παράδειγμα να προωθείται η αίτηση μέχρι το σημείο στο οποίο θεωρείται ότι είναι πιο αποδοτικό, σε σύγκριση με την απευθείας ανάκτηση του αντικειμένου από τον εξυπηρετητή. Μερικά από τα προϊόντα τα οποία εκμεταλλεύονται την ιεραρχική δομή είναι τα Harvest , Squid , Apache. Στο Σχήμα φαίνεται η ιεραρχική δομή των κρυφών αντιπροσώπων.




## 7.1.3 Μη Ιεραρχικές Δομές

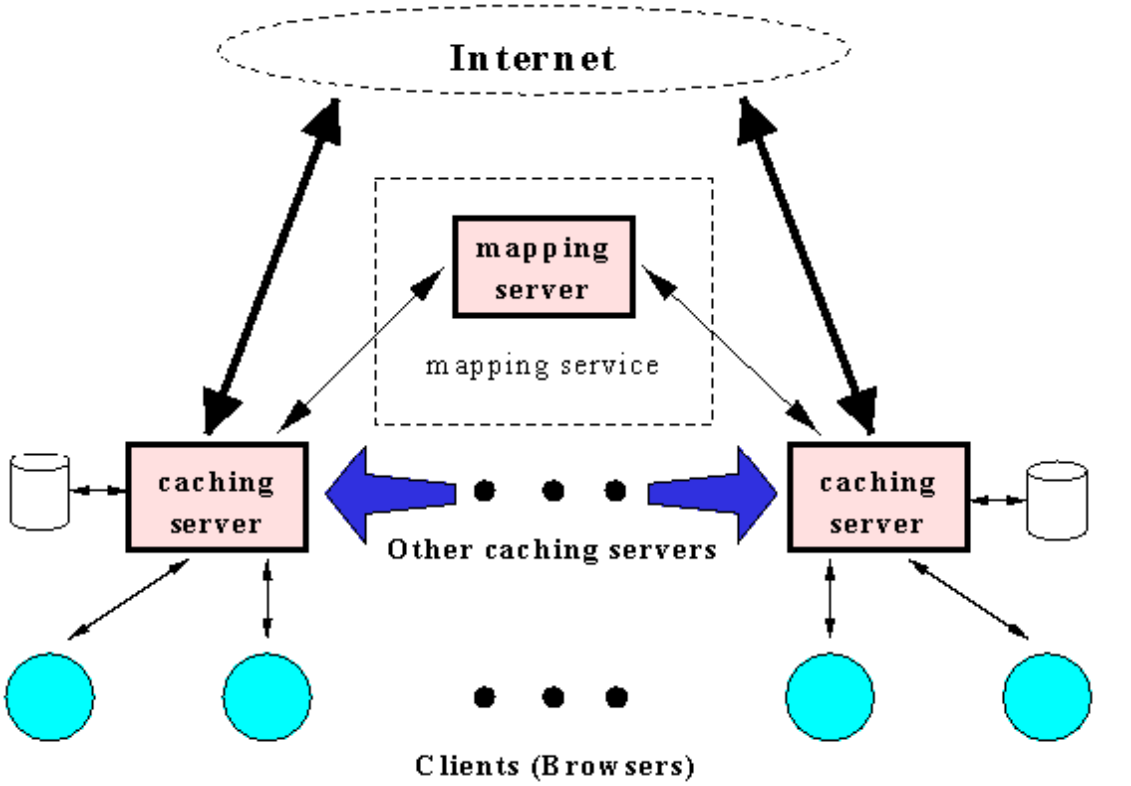
Οι ιεραρχικές δομές παρουσιάζουν ορισμένα προβλήματα πράγμα το οποίο οδήγησε στην κατανεμημένη προσέγγιση του προβλήματος. Ένα από τα προβλήματα είναι ότι παρά την καλή απόδοση του συστήματος όσον αναφορά το hit ratio (το hit ratio ορίζεται σαν τον λόγο των αιτήσεων που εξυπηρετήθηκαν από τον κρυφό αντιπρόσωπο προς το σύνολο των αιτήσεων) ο χρόνος απόκρισης που παρατηρούν οι χρήστες είναι αρκετά μεγάλος εξαιτίας των πολλών επιπέδων στο δέντρό, του υπερβολικού φόρτου που παρουσιάζεται στους κρυφούς αντιπροσώπους και της απόστασης αυτών από τους χρήστες.

Υπάρχουν τρεις βασικές σχεδιαστικές επιλογές οι οποίες πρέπει να ακολουθηθούν σε κατανεμημένη προσέγγιση [10]:

i) τα αντικείμενα πρέπει να εντοπίζονται και να παραδίνονται στους χρήστες με βάση την ελάχιστη απόσταση από αυτούς,

ii) τα αντικείμενα πρέπει να διαμοιράζονται ανάμεσα σε πολλούς αντιπροσώπους και σε πολλούς χρήστες και

iii) οι αντιπρόσωποι πρέπει να είναι όσο το δυνατόν πιο κοντά στους χρήστες.




Το σύστημα το οποίο παρουσιάζεται , υποστηρίζει μια υπηρεσία βαθμωτής εύρεσης αντικειμένων η οποία ονομάζεται ιεραρχία υποδείξεων (hint hierarchy) η οποία επιτρέπει σε κάθε κρυφό αντιπρόσωπο να εντοπίσει ποιος (κρυφός αντιπρόσωπος ‘η εξυπηρετητής) κατέχει το κάθε αντικείμενο που ζητείται από τους χρήστες και βρίσκεται στην κοντινότερη απόσταση (αριθμός hops). Εδώ παρουσιάζεται ένα σύστημα “Summary Cache” το οποίο επιτρέπει τον διαμοιρασμό αντικειμένων μεταξύ αρκετών κρυφών αντιπροσώπων.

Μια πρώτη απόπειρα κατανεμημένου συστήματος κρυφών αντιπροσώπων έχει γίνει από το CRISP (Caching and Replication for Internet Service Performance) . Η βασική ιδέα, όπως φαίνεται στο Σχήμα, κρύβεται πίσω από την έννοια του συμβουλευτικού εξυπηρετητή (directory server ή mapping server) ο οποίος διατηρεί πληροφορία με το τι είναι αποθηκευμένου και που. Στην περίπτωση που μία αίτηση δεν μπορεί να εξυπηρετηθεί από ένα αντιπρόσωπο, ρωτάται ο συμβουλευτικός εξυπηρετητής ο οποίος

γνωρίζει τι είναι αποθηκευμένο σε όλους τους αντιπροσώπους που απαρτίζουν το κατανεμημένο σύστημα. Σε περίπτωση που το αντικείμενο είναι κάπου αποθηκευμένο στο σύστημα, η αίτηση κατευθύνεται στον αντιπρόσωπο που το έχει, διαφορετικά η αίτηση κατευθύνεται στον απομακρυσμένο εξυπηρετητή. Ένα παρόμοιο με το CRISP σύστημα το οποίο όμως υποστηρίζει και δυναμικού τύπου αντικείμενα όπως βίντεο και μουσική είναι το MiddleMan και παρουσιάζεται στο [16].

Το ότι υπάρχει μία κεντρική υπηρεσία που αναλαμβάνει να απαντήσει στις ερωτήσεις των αντιπροσώπων μπορεί να οδηγήσει στην κατάρρευση του συστήματος όταν ο συμβουλευτικός εξυπηρετητής πάψει να λειτουργεί. Μία εναλλακτική προσέγγιση είναι ο κατακερματισμός του καταλόγου των αντικειμένων που είναι αποθηκευμένα στους αντιπροσώπους σε N υποκαταλόγους τους οποίους διαχειρίζονται N συμβουλευτικοί εξυπηρετητές [29]. Έτσι ο φόρτος στον συμβουλευτικό εξυπηρετητή τώρα κατανέμεται. Μία πιθανή βλάβη σε ένα από τους συμβουλευτές επηρεάζει μόνο τον υποκατάλογο που έχει αναλάβει να διαχειρίζεται. Αυτό μειώνει την πιθανότητα καθολικής βλάβης του συστήματος. Ένα βήμα παραπέρα μας οδηγεί στην απουσία συμβουλευτικών εξυπηρετητών. Σε αυτή την περίπτωση ο κατάλογος των αντικειμένων που είναι αποθηκευμένα στο σύστημα αντιγράφεται σε όλους τους κρυφούς αντιπροσώπους του συστήματος. Έτσι ανά πάσα στιγμή, οι κρυφοί αντιπρόσωποι γνωρίζουν που να προωθήσουν την αίτηση για αντικείμενο το οποίο δεν έχουν οι ίδιοι. Εξαιτίας του ότι με την πάροδο του χρόνου ο κατάλογος των αντικειμένων μπορεί να γίνει ιδιαίτερα μεγάλος, πράγμα το οποίο οδηγεί σε αυξημένες ανάγκες αποθηκευτικού χώρου, αλλά και διαχείρισης του καταλόγου, οδηγούμαστε στην χρήση τμήματος του καταλόγου. Έτσι αντιγράφεται στους αντιπροσώπους το τμήμα του καταλόγου που προβλέπεται να παράγει τα περισσότερα χτυπήματα (hits, εξυπηρέτηση των αιτήσεων από τον δίσκο του κρυφού αντιπροσώπου) στο σύστημα. Μια προσέγγιση είναι να αποθηκεύεται πληροφορία θέσης για τα αντικείμενα αυτά τα οποία είναι ιδιαίτερα δημοφιλή.

## 7.2 Πλεονεκτήματα της ένταξης σε ιεραρχία

- Αποδοτικότητα. Κλειδιά στο αν η ένταξη σε μια ιεραρχία cache θα είναι αποδοτική, είναι η επιτυχία σε μια γειτονική cache σε περίπτωση που είναι αποτυχία στη δική μας cache, η γειτονική επιτυχία cache να φτάνει σε εμάς πιο γρήγορα από ότι θα έφτανε αν ήταν αποτυχία και ερχόταν από τον πραγματικό διακομιστή. Ακόμα, οι αποτυχίες των

ανωτέρων cache δεν θα πρέπει να είναι αισθητά πιο αργές από ότι θα ήταν η απάντηση από τον πραγματικό διακομιστή.

- Μη προεπιλεγμένη δρομολόγηση. Οι πατέρες-cache είναι χρήσιμοι όταν πρέπει να επιβάλλεις την ροή της κίνησης μέσω μιας συγκεκριμένης διαδρομής στο δίκτυο. Ένα διάσημο παράδειγμα είναι όταν έχεις ένα firewall. Θέλεις να περνά όλη η κίνηση του δικτύου μέσω αυτού. Είναι πολύ συνηθισμένο πλέον πολλοί οργανισμοί και πολλές εταιρίες να χρησιμοποιούν ένα διαφανή (transparent) proxy. Οι HTTP συνδέσεις των πελατών ανακατευθύνονται προς έναν caching proxy σε αυτές τις περιπτώσεις και δεν απορρίπτονται. Αν σε μια τέτοια περίπτωση πελάτης είναι ο caching proxy, το firewall proxy είναι ένας πατέρας-cache και ας μην το καταλαβαίνει το παιδί. Ακόμα, μπορούν να χρησιμοποιηθούν πολλαπλοί πατέρες-cache για πολλαπλές συνδέσεις προς τα εξωτερικά δίκτυα όπου το φόρτο μοιράζεται αναλόγως με τις απαιτήσεις.

## 7.3 Μειονεκτήματα της ένταξης σε ιεραρχία

Πριν αποφασίσουμε την ένταξη σε μια ιεραρχία θα πρέπει να γνωρίζουμε και κάποια από τα μειονεκτήματά της.

- Εμπιστοσύνη. Όταν ενταχθούμε σε μια ιεραρχία είναι σαν να λέμε ότι εμπιστευόμαστε όλα τα μέλη της ιεραρχίας απόλυτα. Πιστεύουμε ότι τα δεδομένα που μας δίνει είναι έγκυρα, δεν έχουν τροποποιηθεί με κάποιο τρόπο. Εμπιστευόμαστε σε όλα τα μέλη την ιδιωτικότητα των αιτήσεών μας.
- Χαμηλά ποσοστά επιτυχίας (Low Hit Ratio). Τα ποσοστά επιτυχιών από πατέρες και αδερφούς-cache είναι συνήθως πολύ χαμηλά σε σύγκριση με μια cache η οποία εξυπηρετεί απ' ευθείας τελικούς χρήστες.
- Επιπτώσεις στις δρομολογήσεις. Όσο η απόσταση μεταξύ των δρομολογητών αυξάνεται (hops), αυξάνονται και οι επιπτώσεις στις διαφοροποιήσεις της δρομολόγησης. Αν για παράδειγμα ένας πατέρας έχει πολλές συνδέσεις για το Intenet και κάποια από αυτές διακόπτει ενώ το παιδί-cache έχει και αυτό μια σύνδεση Internet, αν μια απ' τις συνδέσεις του πατέρα κοπεί δεν θα μπορεί να επικοινωνήσει με κάποιους πραγματικούς διακομιστές και θα στέλνει στα παιδιά-cache μηνύματα σφαλμάτων. Όμως, εφόσον υπάρχει και η άλλη σύνδεση του παιδιού, ίσως αυτό να θελήσει να χρησιμοποιήσει αυτήν.
- Η διατήρηση της συνέπειας και της εγκυρότητας, από χρονικής άποψης, μιας σελίδας

μεταξύ των μελών της ιεραρχίας είναι δύσκολη διαδικασία. Σε μια περίπτωση όπου ένα παιδί έχει δύο πατέρες-cache και έχουν και οι δύο μια απάντηση πως θα μπορούμε να ξέρουμε ποια απάντηση είναι πιο έγκυρη; Το καλύτερο που μπορούμε να κάνουμε είναι να χρησιμοποιήσουμε μια διαδικασία ακύρωσης αντικειμένων (object invalidation process). Ορισμένα από τα πρωτόκολλα cache έχουν τέτοια χαρακτηριστικά.

- Μεγάλες οικογένειες. Τα πολλά επίπεδα στην ιεραρχία πολλές φορές προκαλούν προβλήματα. ειδικά στα ανώτερα επίπεδά της και αυτό λόγω των πολλών αιτήσεων που δέχονται από τους εκατοντάδες ή και χιλιάδες πελάτες που βρίσκονται από κάτω.
- Όποτε ένας proxy προωθεί μια αίτηση προς έναν πραγματικό διακομιστή καταγράφει τη σύνδεση από την **IP** του proxy. Όταν ένας παροχέας υπηρεσιών ή ο ιδιοκτήτης της σελίδας πιστεύει ότι γίνεται κάποια κατάχρηση ή κακομεταχείριση επικοινωνεί με τον υπεύθυνο της **IP** από όπου έρχονται οι αιτήσεις (proxy) για τα παράπονα.
- Πολλές φορές δεν επιστρέφουν σωστά ή έγκυρα μηνύματα σφαλμάτων. Ένα παράδειγμα είναι ότι ένας proxy δεν μπορεί να καταλάβει τη διαφορά μεταξύ ενός ονόματος DNS που πραγματικά δεν υπάρχει ή απλά δεν δουλεύει η υπηρεσία προσωρινά.
- Μεταξύ μιας σχέσης αδερφών-cache υπάρχει ένας μηχανισμός πρόβλεψης επιτυχίας (cache hit) η οποία γίνεται από τα πρωτόκολλα cache. Στην περίπτωση που η πρόβλεψη δεν είναι σωστή, δηλαδή όταν μια αίτηση προβλέπεται να είναι επιτυχία στην cache του αδερφού άλλά τελικά δεν είναι, το αποκαλούμε *λανθασμένη επιτυχία (false hit)*.
- Βρόχος προώθησης. Ένας βρόχος προώθησης παρουσιάζεται όταν μια αίτηση στέλνεται πάνω - κάτω μεταξύ δύο ή παραπάνω κόμβων της ιεραρχίας. Αυτό μπορεί να συμβεί μεταξύ δυο cache όταν στον καθένα είναι δηλωμένος ο άλλος ως πατέρας-cache.
- Βλάβες και άρνηση υπηρεσίας (Service Denial). Υπάρχουν κάποια προβλήματα, που είναι πιο δύσκολα να εντοπιστούν, από ότι μια ολοκληρωτική, μηχανική βλάβη σε έναν πατέρα-cache όπως είναι η υπερφόρτωση με κίνηση του πατέρα, το οποίο έχει σαν αποτέλεσμα την αύξηση του χρόνου των αποκρίσεων. Μια πιθανή αιτία άρνησης υπηρεσίας είναι κάποιο πρόβλημα με τον διακομιστή DNS του πατέρα-cache. Αυτές οι ενδείξεις βέβαια δεν είναι σίγουρο ότι οφείλονται σε κάποιο σφάλμα.

## 7.4 Intercache protocols

Αυτά τα πρωτόκολλα χρησιμοποιούνται μεταξύ συνεργαζόμενους cache proxy για πολλούς λόγους, ο βασικότερος εκ των οποίων είναι να βοηθούν σε αποφάσεις ζήτησης, δηλαδή δεδομένου κάποιων στοιχείων, προς ποια κατεύθυνση να στείλει την αίτηση;

## 7.5 ICP

Είναι το αυθεντικό πρωτόκολλο intercache. Πρωταρχικός του σκοπός είναι να μαθαίνει εάν κάποια γειτονική cache έχει πιο φρέσκο αντίγραφο ενός
συγκεκριμένου αντικειμένου. Οι γείτονες-cache απαντούν είτε με ένα ναι (HIT),
είτε με ένα όχι (MISS). Η cache συλλέγει ένα συγκεκριμένο αριθμό από απαντήσεις ICP και παίρνει μια απόφαση προώθησης. Ακόμα και αν όλοι οι γείτονες απαντήσουν με MISS, το ICP μπορεί να παρέχει πρόσθετες υποδείξεις που βοηθούν στο να διαλέξει τον καλύτερο πατέρα-cache.
Το ICP είναι πέραν του τέλειου, όμως χρησιμοποιείται ακόμα ευρέως.

## 7.6 CARP (Cache Array Routing Protocol)

Το CARP δεν είναι ένα πρωτόκολλο αυτό καθεαυτό. Σχεδιάστηκε για να επιλύσει ένα πολύ συγκεκριμένο πρόβλημα. Το πώς να επιτύχουμε αποδοτικά και κλιμακωτά την εξισορρόπηση του φόρτου ενώ αυξάνουμε τα ποσοστά επιτυχιών (hit ratios) και μειώνουμε το χρόνο αδράνειας. Είναι πολύ χρήσιμο σε περιπτώσεις που η cache μας αποτελείται από πολλά μηχανήματα (cache *C/uster).*
Για κάθε αίτηση, το CARP υπολογίζει ένα βαθμό για κάθε proxy cache. Η αίτηση προωθείται στον proxy με το μεγαλύτερο βαθμό. Εάν αυτό αποτύχει, τότε δοκιμάζεται η cache με το δεύτερο μεγαλύτερο βαθμό. Ο βαθμός είναι ένας
υπολογισμός βασιζόμενος σ' ένα hash του URL, ένα hash του ονόματος της cache, και τα ειδικό βάρος που έχει ανατεθεί στην κάθε cache. Το σημαντικότερο χαρακτηριστικό αυτής της διαδικασίας είναι ότι εάν προστεθεί άλλη μια μηχανή για την cache δεν αλλάζει την ιεραρχία των βαθμών των υπολοίπων cache, αλλά δημιουργεί νέες βαθμολογίες. Στατιστικά, οι νέοι βαθμοί θα είναι μεγαλύτεροι από τους προηγούμενους για το μέρος

των URL που είναι ανάλογο στο βάρος της cache στο cIuster.
Το CARP καθορίζει και έναν τύπο αρχείων για ένα *Proxy Array Membership Table.* Έναν πίνακα δηλαδή, ο οποίος επιτρέπει σε πελάτες να διαπιστώσουν ποιες cache ανήκουν σε μια ομάδα, σε ένα *group.* Ο αλγόριθμος του CARP μπορεί να χρησιμοποιηθεί σε οποιοδήποτε πελάτη ιστού, όπως είναι ένας φυλλομετρητής ή έναν proxy cache. Το CARP δουλεύει μόνο για σχέσεις νέων- παιδιών γιατί προβλέπει cache hits.

## 7.7 Cache Cluster

Ένα *Cache cluster* είναι μια ομάδα από ξεχωριστούς proxy cache που είναι ρυθμισμένοι να ενεργούν σαν να ήταν ένας διακομιστής. Δηλαδή, οι χρήστες και οι πελάτες τους αντιλαμβάνονται ως μια μονάδα.

Μια συστάδα διαφέρει από την ιεραρχία σε κάποιες λεπτομέρειες. Αρχικά, τα μέλη της συστάδας βρίσκονται το ένα κοντά στο άλλο, φυσικά και τοπολογικά, δηλαδή βρίσκονται στο ίδιο δωμάτιο και ανήκουν στο ίδιο υποδίκτυο. Πολλοί Οργανισμοί χρησιμοποιούν cache clusters για να εξυπηρετούν ή να παρέχουν περισσότερες σελίδες και περίσσιες υπηρεσίες. Αν σε έναν οργανισμό υπάρχει ένας proxy, αλλά η κίνηση αυξάνεται και επιβαρύνονται, με αποτέλεσμα να γίνονται αργές οι υπηρεσίες τότε μια καλή λύση, χωρίς να χαθεί το υπάρχον προϊόν cache και τα περιεχόμενα της, είναι να πάρει άλλη μια μηχανή και να φτιάξει ένα μικρό cluster.

Βέβαια, υπάρχουν και άλλοι λόγοι για να χρησιμοποιήσει ένας Οργανισμός συστάδες. Αναφέρω τρεις:

### 7.7.1 Εύρος Ζώνης (Bandwidth)

Μια απλή διαμόρφωση για κατανομή φόρτου αποτελεί χαμένο χώρο στο αποθηκευτικό μέσο και σπατάλη του εύρους ζώνης. Λέμε χαμένος χώρος γιατί η ίδια απάντηση μπορεί να αποθηκευτεί σε πολλές cache και λέμε σπατάλη του εύρους ζώνης γιατί δεν χρειάζεται πάντα να προωθούμε ένα "cache miss" προς τον πραγματικό διακομιστή εάν γνωρίζουμε

ότι ένα άλλο μέλος της συστάδας έχει ήδη την απάντηση αποθηκευμένη.

Υπάρχουν δύο τρόποι να βελτιώσουμε την χρήση των δίσκων και του εύρους ζώνης. Ο ένας είναι να διανεμηθούν οι αιτήσεις πριν μπουν στη συστάδα, δηλαδή κάποια συσκευή ή κάποιος αλγόριθμος φροντίζει ώστε η ίδια αίτηση να πηγαίνει προς το ίδιο μέλος της συστάδας. Ο δεύτερος τρόπος είναι να δημιουργήσουμε "αδερφικές σχέσεις" μεταξύ των cache-μελών της συστάδας και να χρησιμοποιήσουμε ένα πρωτόκολλο intercache να εντοπίζουμε απαντήσεις που βρίσκονται ήδη στην cache μας. Σε αυτή την περίπτωση δεν μας ενδιαφέρει ποια cache παρέλαβε την αρχική αίτηση.
Υπάρχουν αρκετές τεχνικές και προϊόντα που διανέμουν αιτήσεις και τις αναθέτουν σε συγκεκριμένα μέλη της συστάδας. Κάποια από αυτά είναι το WCCP, τα switch επιπέδου 4 και επιπέδου 7 και το πρωτόκολλο CARP

## 7.7.2 Η "Ρεζέρβα"

Ένας τρόπος να παρέχουμε πλεονάζουσες υπηρεσίες είναι να έχουμε σε αναμονή μια δεύτερη cache. Σε κανονική λειτουργία, όλες οι αιτήσεις πηγαίνουν στην πρωταρχική cache. Αν αυτή αποτύχει αναλαμβάνει η δεύτερη.
Αυτή η διαρρύθμιση δεν είναι ακριβώς μια συστάδα, μιας και μόνο μία εκ των δύο cache λειτουργεί σε μια χρονική στιγμή. Οι τεχνικές όμως είναι παρόμοιες.

Κάποια γνωστά προϊόντα (Switch Επιπέδου 4 και 7) μπορούν να ρυθμιστούν να δουλεύουν ως transparent proxy ή με μια εικονική διεύθυνση διακομιστή (virtual server). Μπορούμε να πούμε στο switch τις πραγματικές IP διευθύνσεις για την πρωταρχική cache και την cache - ρεζέρβα. Κανονικά προωθεί όλες τις συνδέσεις στην πρωταρχική . Αν το switch διαπιστώσει ότι η πρωταρχική έχει πέσει, τότε χρησιμοποιεί τη ρεζέρβα. Εφόσον οι χρήστες μιλούν στον εικονικό διακομιστή, δεν υπάρχουν προβλήματα με DNS και ARP timeouts

### 7.7.3 Ταχύτητα διεκπεραίωσης και Κατανομή Φόρτου

Ένα cache cluster με κατανομή φόρτου (load sharing) μπορεί να βελτιώσει την ταχύτητα διεκπεραίωσης και την αξιοπιστία. Η ταχύτητα διεκπεραίωσης αυξάνεται διότι πολλές cache μπορούν να χειριστούν περισσότερη κίνηση από ότι μία. Η αξιοπιστία αυξάνεται γιατί όταν παρουσιαστεί κάποιο πρόβλημα σε μία cache, οι άλλες απορροφούν τον αυξημένο φόρτο.

Ο πιο φτηνό ς τρόπος για να πετύχουμε κατανομή του φόρτου είναι με το DNS Server, να δηλώσουμε το ίδιο όνομα host σε όλα τα μέλη της συστάδας, δηλαδή η μέθοδος *round-robin,* κατά την οποία ο DNS server θα ανακυκλώνει τις IP των μελών και θα δίνει άλλη IP σε κάθε Iookup.

Μια πιο ρωμαλέα προσέγγιση, αν και πιο ακριβή, είναι η χρήση ενός switch επιπέδου 4 ή κάποια γνωστά προϊόντα για εξισορρόπηση φόρτου. Με αυτή την προσέγγιση η κατανομή του φόρτου γίνεται αρκετά πιο ισορροπημένα από ότι στην προσέγγιση round-robin και δεν έχουμε μεγάλες καθυστερήσεις.

Σε πολλές περιπτώσεις όπου υπάρχει cache cluster και στον πραγματικό διακομιστή (ιστού) με ένα switch επιπέδου 4 μπροστά από αυτό, το οποίο διανέμει τις αιτήσεις με βάση τη διεύθυνση lP. Όταν η επικοινωνία όμως περιέχει πληροφορίες συνεδρίας ( session inforn1ation, π.χ. χρήση "cookies"),και κάποια ακόλουθα πακέτα πάνε σε κάποιον άλλον διακομιστή του cluster, απορρίπτονται Αυτό λύνεται με τη χρήση των switch επιπέδου 7 τα οποία καταλαβαίνουν πληροφορίες όπως τα cookies.

# 8. Case Study

Στο case study θα αναφέρουμε τη δομή της ασφάλειας ενός δικτύου μιας επιχείρησης η οποία αποτελείται από δύο βασικά τμήματα. Το τμήμα πωλήσεων, όπου ασχολείται με την προώθηση και την αγορά προϊόντων για την επιχείρηση και το τεχνικό τμήμα, το οποίο ασχολείται με τεχνικά θέματα της ίδιας της επιχείρησης και τεχνικά θέματα που αφορούν πελάτες της.

Θα χρησιμοποιηθεί η αρχιτεκτονική της *αποστρατικοποιημένης ζώνης* (De-Militarized Zone, DMZ). Η επιχείρηση έχει στη διάθεσή της ένα C class δίκτυο. Θα υποθέσουμε ότι οι διευθύνσεις 192.168.0.0/ 255.255.255.0 είναι πραγματικές διευθύνσεις δημοσιευμένες στο Διαδίκτυο και όχι ιδιωτικού δικτύου. Για ιδιωτικού δικτύου διευθύνσεις θα χρησιμοποιήσουμε τις διευθύνσεις 10.0.1.0/24 και 10.0.2.0/24. Χρησιμοποιούμε για στάση αποτυχίας την στάση defauIt deny.

Για εξωτερικό δρομολογητή χρησιμοποιούμε έναν H/Y με Linux (kerneI 2.2.19) για λειτουργικό σύστημα ο οποίος έχει μια κάρτα δικτύου (ethO) και μια μόνιμη σύνδεση point-to-point Αυτός είναι και ο δρομολογητής μας. Μέσα στο περιμετρικό δίκτυο, το οποίο χρησιμοποιεί πραγματικές διευθύνσεις, έχουμε:

- Έναν maiI server για την επιχείρησή μας με διεύθυνση 192.168.0.5
- Έναν δημόσιο FTP Server με διεύθυνση 192.168.0.3
- Έναν δημόσιο DNS Server με διεύθυνση 192.168.0.6
- Έναν δημόσιο Web Server με διεύθυνση 192.168.0.2, ο οποίος
  δημοσιεύεται μέσω ενός cache-proxy accelerator.
- Ένας cache proxy accelerator με διεύθυνση 192.168.0.4 ο οποίος
  εξυπηρετεί τον Web Server μας.

Τέλος, ένας ιδιωτικός proxy-cache server με διεύθυνση 192.168.0.7,
σε H/Y με Linux (kernel 2.2.19) και Squid 2.3 ST ABLE 5 ο οποίος
εξυπηρετεί τα ιδιωτικά μας δίκτυα.

Στον εξωτερικό μας firewall χρησιμοποιούμε ipchains. Κάνουμε τον έλεγχο των πακέτων στην αλυσίδα "input". Τα ipchains έχουν τρεις αλυσίδες που δεν μπορούν να

σβηστούν, την αλυσίδα input, την αλυσίδα output, την αλυσίδα forward. Πάνω σε αυτές βασίζονται οι αλυσίδες των χρηστών. Όλες οι αλυσίδες έχουν και μια πολιτική ασφαλείας. Εξ' ορισμού οι τρεις προαναφερθέντες έχουν default ACCEPT. Εδώ θα χρησιμοποιήσουμε και αλυσίδες χρηστών.

1. ipchains -N exo-mesa

2.ipchains -N mesa-exo

3.ipchains -A input -allo -s 127.0.0.0/8 -l-j DENY

4.ipcains -A input -ílo -j ACCEPT

5. ipchains -A input -í ρρρO -j exo-mesa

6.ipchains -A input -í ethO -j mesa-exo

7.ipchains -A exo-mesa -s 192.168.0.0/24 -l-j DENY

8.ipchains -A exo-mesa -ρ icmp -d 192.168.0.7 --icmp-type echo-request -j DENY

9.ipcllains -A exo-mesa -ρ icmp -d 192.168.0.2 --icmp-type echo-request -j DENY

*/O.* ipchains -A exo-mesa -ρ tcp -d 192.168.0.5 smtp -j ACCEPT

*11.* ipchains -A exo-mesa -ρ udp -d 192.168.0.6 domain -j ACCEPT

*12.* ipchains -A exo-mesa -ρ tcp -d 192.168.0.6 domain -j ACCEPT

*13.* ipchains -A exo-mesa -ρ tcp -d 192.168.0.4 www -j ACCEPT

*14.* ipchains -A exo-mesa -ρ tcp -d 192.168.0.3 ftp -j ACCEPT

*15.* ipchains -A exo-mesa -ρ tcp -d 192.168.0.3 ftp-data -j ACCEPT

/6. ipchains -A exo-mesa -ρ tcp ! -Y -d 192.168.0.7 1024:65535 -j ACCEPT /7.

ipchains -A exo-mesa -ρ icmp -j ACCEPT

18. ipchains -A exo-mesa -I-j OENν

# 8.1 CHAIN MESA-EXO

1. ipchains -A mesa-exo -s ! 192.168.0.0/24 -l-j OENY
2.ipchains -A mesa-exo -ρ tcp -s 192.168.0.5 smtp -j ACCEPT
3.ipchains -A mesa-exo -ρ tcp -s 192.168.0.6 domain -j ACCEPT
4.ipchains -A mesa-exo -ρ udp -s 192.168.0.6 domain -j ACCEPT
5.ipchains-Amesa-exo-ptcp! -y-s 192.168.0.4www-j ACCEPT
6.ipchains -A mesa-exo -ρ tcp ! -y -s 192.168.0.3 ftp-j ACCEPT
7.ipchains -A mesa-exo -ρ tcp ! -y -s 192.168.0.3 ftp-data-j ACCEPT
8.ipchains -A mesa-exo -ρ tcp -s 192.168.0.7 1024:65535 -j ACCEPT 9.ipchains -A mesa-exo -p icmp -j ACCEPT
*10.* ipchains -A mesa-exo -l-j REJECT
Στους κανόνες 1 και 2 δημιουργούμε τις αλυσίδες mesa-exo και exo-mesa.
Στους κανόνες 3 και 4 γίνεται έλεγχος για IP spoofing της loopback στην αλυσίδα input. Αν διαπιστωθεί τέτοια περίπτωση, τότε το πακέτο απορρίπτεται. Αν όχι, επιτρέπεται.

Κανόνες 5,6. Αν εισέλθει πακέτο από το interface της εξωτερικής σύνδεσης, τότε να ελεγχθεί στην αλυσίδα exo-mesa που δημιουργήσαμε. Αντίστοιχα, αν εισέλθει πακέτο από το interface της κάρτας δικτύου (ethO) να ελεγχθεί στην αλυσίδα mesa-exo που δημιουργήσαμε.
Από τον κανόνα 7 ξεκινούν οι κανόνες για την αλυσίδα χρήστη exo-mesa.
Κανόνας 7. Έλεγχος για IP Spoofing. Αν το πακέτο που εισήλθε από το interface ppp έχει διεύθυνση πηγής κάποια διεύθυνση του δικτύου μας, τότε απορρίπτεται.

Κανόνας 8 και 9. Έλεγχος αν το πακέτο είναι τύπου icmp echo.-request, δηλαδή αν κάποιος από έξω κάνει ping στον cache server (192.168.0.7) και στην πραγματική διεύθυνση του web server μας (192.168.0.2) και αν ναι, τότε απορρίπτεται (και κατ' επέκταση δεν δίνεται απάντηση από αυτούς)

. Στους κανόνες 10,12,13,14 και 15 ελέγχεται το πακέτο με βάση το πρωτόκολλο (εδώ TCP), τη διεύθυνση προορισμού και το ροή προορισμού. Εάν κάποιο αντιστοιχεί στον web server, ftp server, dns server, maiI server και στο αντίστοιχο port, τότε το πακέτο περνά.

Στον κανόνα 11 γίνεται η ίδια διαδικασία για τον dns server μας, μόνο που εδώ το πρωτόκολλο που ελέγχεται είναι το udp. Εάν ταιριάξει ο κανόνας, τότε και πάλι το πακέτο περνά.

Στον κανόνα 16 ελέγχεται το πακέτο, αν είναι tcp το πρωτόκολλο, αν δεν είναι πακέτο που ζητά να ανοίξει σύνδεση tcp και πηγαίνει στον cache-proxy στην διεύθυνση 192.168.0.7 σε port μεγαλύτερα του 1023. αυτό σημαίνει ότι το πακέτο θα είναι κάποια απάντηση σε κάποια αίτηση του cache-proxy μας. Αν ταιριάξει, τότε περνά.

Στον κανόνα 17 ελέγχεται το πρωτόκολλο του πακέτου εάν είναι icmp και αν είναι περνά.

Στον κανόνα 18 απορρίπτονται και καταγράφονται στα Iog fiIes όλα τα υπόλοιπα πακέτα.

Εδώ τελειώνουν οι κανόνες της αλυσίδας exo-mesa και αρχίζουν οι κανόνες της άλλης αλυσίδας χρήστη, η mesa-exo.

Στον κανόνα 1 γίνεται έλεγχος για IP Spoofing στα πακέτα που εισέρχονται από την κάρτα δικτύου μας. Αν το πακέτο δεν έχει διεύθυνση πηγής κάποια διεύθυνση του εσωτερικού μας δικτύου, τότε καταγράφεται και απορρίπτεται.

Στον κανόνα 2, 3 γίνεται έλεγχος για το αν το πρωτόκολλο είναι tcp και αν το πακέτο κατευθύνεταί προς τον MaiI server ή τον DNS server στα αντίστοιχα port του καθενός και αν ταιριάξει, τότε το πακέτο περνά.

Στον κανόνα 4 γίνεται ότι και στον κανόνα 2, μόνο που ελέγχεται αν το πρωτόκολλο είναι udp.

Στους κανόνες 5,6,7 γίνεται έλεγχος για το αν το πρωτόκολλο είναι tcp, αν είναι ήδη ανοιχτεί tcp σύνδεση (δεν είναι πακέτο που ζητά να γίνει σύνδεση), και προορίζεται για τον cache accelerator, ή τον ftp server στα αντίστοιχα port και αν ταιριάξει τον κανόνα το πακέτο περνά.

Στον κανόνα 8 γίνεται έλεγχος του πακέτου με βάση το πρωτόκολλο ( tcp), και η πηγή του πακέτου, αν είναι ο cache-proxy μας και αν το port είναι μεγαλύτερο του 1023.

Ο κανόνας 9 επιτρέπει τη διέλευση του πακέτου αν το πρωτόκολλο είναι icmp.

Στον τελευταίο κανόνα απορρίπτονται και καταγράφονται όλα τα άλλα πακέτα. Η απόρριψη REJECT στέλνει απάντηση icmp ότι για κάποιο λόγο δεν έφτασε το πακέτο ώστε να μην συνεχιστεί η προσπάθεια μέχρι το timeout.

## 8.2 Cache Proxy

Ο cache-proxy είναι εγκατεστημένος σε Η/Υ με λειτουργικό Linux (kernel 2.2.19) ο οποίος δεν προωθεί τα πακέτα παρά σε μια περίπτωση, όπως θα δούμε και πιο κάτω. Έχει τρεις κάρτες δικτύου, τις ethO, eth1, eth2. Η ethO αντιστοιχεί στην πραγματική διεύθυνση 192.168.0.7 του περιμετρικού δικτύου μας. Οι άλλες δύο αντιστοιχούν στα δύο εσωτερικά, ιδιωτικά δίκτυα του τεχνικού τμήματος (με IP 10.0.1.1/24) και του, τμήματος πωλήσεων ( με IP 10.0.2.1/24). Έχουμε εγκαταστήσει και τον Squid Cache Proxy 2.3 STABLE 5.

Χρησιμοποιούμε ipchains για την προστασία των ιδιωτικών δικτύων από το περιμετρικό και γενικά τα εξωτερικά. Επειδή ο proxy μας θα εξυπηρετεί τις αιτήσεις από μέσα προς διακομιστές www, ftp θα πρέπει να χρησιμοποιήσουμε NAT ή Masquerading για τις υπόλοιπες υπηρεσίες που θέλουμε να παρέχουμε, συγκεκριμένα, ηλεκτρονική αλληλογραφία. Οπότε οι κανόνες ορίζονται ως εξής:

1) ipchains -A ínput -í ethO -s 10.0.0.0/16 -j DENY -I

2) ipchains -A input -í ethl -s ! 10,.0.1.0/24 -j DENY -1

3) ipchains -A íηput -í eth2 -s ! 10.0.2.0/24 -j DENY -1

Σε αυτούς τους τρεις κανόνες γίνεται η αντιμετώπιση του IP Spoofing στα τρία interface.

4) ipchains -A ínput -í ethO -ρ tcp ! -Y -s 192.168.0.6 domain -j ACCEPT

5) ipchains -A íηput -í ethO -ρ udp -s 192.168.0.6 domain -j ACCEPT

6) ipchains -A input -í ethO -ρ tcp ! -Y --dport 1024:65535 -j ACCEPT

7) ipchains -A ínput -í ethO -ρ icmp -s 192.168.0.0/24 -j ACCEPT

8) ipchains -A input -í ethO -j DENY -1

Εδώ γίνονται έλεγχος του eth0 στην αλυσίδα εισόδου (ínput). Ο κανόνας 5 είναι λίγο ρίσκο γιατί δεν μπορούμε να ελέγξουμε αν η σύνδεση έχει γίνει λόγω του πρωτοκόλλου udp όμως πολλές φορές απαιτείται για τα DNS lookups. Οι κανόνες 4 και 6 ελέγχουν την σύνδεση, αν έχει γίνει δηλαδή, για τον κανόνα 4 επιτρέπει το πακέτο αν έρχεται από τον DNS server μας. Ο κανόνας 6 επιτρέπει το πακέτο αν το port προορισμού είναι μεγαλύτερο του 1024 και έχει το γίνει σύνδεση. Ο καν. 7επιτρέπει όλα τα ICMP από το DMZ. Ο καν. 8 απορρίπτει όλα τα άλλα πακέτα που εισέρχονται από το ethO.

9) ipchains -A ínput -í eth 1 -ρ icmp -j ACCEPT

1O)ipchains -A ínput -í ethl -ρ tcp -d 192.168.0.5 smtp -j ACCEPT

11) ipchains -A input -í eth 1 -ρ tcp -d 192.168.0.5 ρορ3 -j ACCEPT

12) ipchains -A input -í eth 1 -ρ tcp -dport 3129 -j ACCEPT

13) ipchains -A inρυt -i eth 1 -j REJECT -I

Εδώ γίνεται έλεγχος του eth 1 στην αλυσίδα inρυt- εισόδου. Επιτρέπουμε τα icmp πακέτα και αιτήσεις για αποστολή και λήψη αλληλογραφίας και αιτήσεις tcp προς το port του proxy. Όποιο άλλο πακέτο εισέλθει στο ethl απορρίπτεται

και σου στέλνεται ενημερωτικό icmp μήνυμα, καθώς και καταγράφεται.

14) ipchains -A inρυt -í eth2 -p icmp -j ACCEPT

15) ipchains -A inρυt -í eth2 -ρ tcp -d 192.168.0.5 smtp -j ACCEPT

16) ipchains -A inρυt -i eth2 -ρ tcp -d 192.168.0.5 ρορ3 -j ACCEPT

17) ipchains -A inρυt -í eth2 -P tcp --dport 3129 -j ACCEPT

18) ipchains -A inρυt -í eth2 -j REJECT -I

Εδώ γίνεται ότι ακριβώς έγινε για το eth1 στους κανόνες 9-13, αλλά γίνεται

για το eth2 τώρα.

Επειδή τα πακέτα που περνούν από τα εσωτερικά δίκτυα προς το εξωτερικό

περιμετρικό μας δίκτυο δεν έχουν πραγματικές διευθύνσεις πρέπει να υποστούν "Masquerading" . Αυτό γίνεται στην αλυσίδα forward ως εξής

19) ipchains -A forward -ρ tcp -d 192.168.0.5 -j MASQ

20) ipchains -A forward -ρ tcp -s 192.168.0.5 -j MASQ

Δηλαδή οποιοδήποτε πακέτο φτάσει σε αυτή την αλυσίδα και έχει πηγή ή

προορισμό τον mail server μας περνά και υφίσταται Masquerading.

21)ipchains -A output -ρ tcp -d 192.168.0.5 smtp -j ACCEPT

22) ipchains -A output -ρ tcp -d 192.168.0.5 ρορ3 -j ACCEPT

23) ipchains -A output -ρ tcp -s 192.168.0.5 smtp -j ACCEPT

24) ipchains -A output -ρ tcp -s 192.168.0.5 ρορ3 -j ACCEPT

25) ipchains -A output -í ethO -ρ tcp -s 192.168.0.6 domain -j ACCEPT

26) ipchains -A output -í ethO -ρ tcp --sport 1024:65535 -j ACCEPT

27) i~chains -A ουtρυt -í ethO -ρ icmp -j ACCEPT

28) ipchains -A ουtρυt -í ethO -l -j REJECT

Στους κανόνες 21-24 επιτρέπουμε την έξοδο από οποιοδήποτε interface πακέτων που προορίζονται ή προέρχονται από τον MaiI server μας. Στον κανόνα 25 επιτρέπουμε να εξέλθουν από το ethO πακέτα προς τον DNS Server μας. Στον κανόνα 26 επιτρέπουμε όλα τα πακέτα από το ethO να βγουν αν έχουν port πηγής μεγαλύτερο του 1024. Στον κανόνα

27 αφήνουμε να εξέλθουν από το ethO όλα τα πακέτα icmp και τέλος δεν επιτρέπουμε και καταγράφουμε οποιοδήποτε άλλο πακέτο αποπειραθεί να βγει από το ethO.

## Squid Cache Proxy.

Ο proxy μας τρέχει στο port 3129. Πρόσβαση στην cache έχουν χρήστες από τα δύο ιδιωτικά μας δίκτυα καθώς και ο Iocalhost, ο ίδιος ο Η/Υ όπου τρέχει ο squid cache proxy.

Στον Squid φτιάχνουμε τα Access Control Lists (ACL's) και τα ενεργοποιούμε με τα acl operator, δηλαδή τα : http_access για http αιτήσεις και τα icp_access τα οποία είναι για επικοινωνία της cache μας με άλλες cache, κάτι το οποίο δεν γίνεται εδώ.

1) acl texniko src 1O.0.1.0/255.255.255.0
2)acl poliseis src 10.0.2.0/24
3)acl private_nets src 10.0.0.0/16

# Δήλωση των ιδιωτικών μας δικτύων. Πρώτα δηλώσαμε το τεχνικό τμήμα,
#έπειτα το τμήμα πωλήσεων και, τέλος, όλα τα πιθανά υποδίκτυα με Subnet
#Mask 255.255.0.0.

4) acl bad_domains dstdomain hack.com intruder.com
#δήλωση των domain που θεωρούμε μη έμπιστα. Αυτά είναι το hack.com και το intruder.com.

5) acl weekends time SA
# δήλωση των ημερών Κυριακή και Σάββατο

6) acl badsites url_regex -í sex χχχ porn
# δήλωση των url που περιέχουν τις
#λέξεις XXX, sex και porn. Case insensitive (-í).

7) acl downloads url_regex -í \.avi$ \.mpeg$ \.mpg$
#δήλωση των url τα οποία #τελειώνουν με .mpeg , .mpg , .avi ώστε να επιτραπούν ή να αποτραπούν τα download τέτοιων αρχείων.

8) acl all src 0.0.0.0/0.0.0.0
#δήλωση όλων των διευθύνσεων IP

9) acI manager proto cache _ object
#δήλωση αντικειμένων cache

10) acllocall10st src 127.0.0.1/255.255.255.255
#δήλωση του locall1ost

11) acl SSL -ports port 443 563
#δήλωση των γνωστών port για το SSL

12)acI Safe_ports80 21 443 563 70 210 1024-65535
#δήλωση των port που φαίνονται

13)acI Connect method CONNECT
#δήλωση της μεθόδου CONNECT που χρησιμοποιείται σε συνδέσεις SSL αντί για το GET.

## 8.3 Εφαρμογή των δηλώσεων- μετατροπή τους σε κανόνες

Οι κανόνες πρέπει να μπουν με μια σειρά Ελέγχονται ο ένας μετά τον άλλον.
Αν ταιριάξει κάποιος γίνεται αποδεκτή η αίτηση ή απορρίπτεται Αυτό που θέλουμε να κάνουμε είναι:

1) Να επιτρέψουμε το πρωτόκολλο cache_object μόνο από τον H/Y που τρέχει τον proxy.
2) Να επιτρέψουμε την πρόσβαση στον IocaIhost
3) Να απορρίψουμε αιτήσεις CONNECT σε μη ασφαλή SSL port
4) Να απορρίψουμε την πρόσβαση στους τεχνικούς τα σαββατοκύριακα
5) Να απορρίψουμε την πρόσβαση στους πωλητές στα site πορνογραφικού περιεχομένου καθώς και το κατέβασμα αρχείων βίντεο τύπου avi, mpeg και mpg
6) Να επιτρέψουμε την πρόσβαση στα υποδίκτυά μας και σε άλλα υποδίκτυα που πιθανώς

να υπάρξουν σε κάθε άλλη περίπτωση και
7) Να αποτρέψουμε την πρόσβαση σε οποιονδήποτε άλλον.

Ακόμα, θέλουμε οι αιτήσεις του υποδικτύου των τεχνικών προς των web server που βρίσκεται σε αυτό το υποδίκτυο να μην περνούν από την cache, να πηγαίνουν απ' ευθείας.
.
Έτσι, συντάσσουμε τους εξής κανόνες με τη σειρά που είπαμε:
1) http_access allow manager localhost
2) http_access allow localhost
3) http_access deny manager
4) http_access deny ! Safe_ports
5) http_access deny Connect ! SSL_ports
6) http_access deny texniko weekends
7) http_access deny poliseis downloads
8) http_access deny poliseis badsites
9) http_access allow private_nets
10) http_access deny all
Και για απ’ευθείας πρόσβαση στον web server του texniko από τους τεχνικούς:
11)always_direct allow texniko
12)never_direct allow all.

# Συμπεράσματα

Ο proxy server αποτελεί την καλύτερη πύλη διαχωρισμού του εσωτερικού δικτύου από το Intenet. Ο proxy server μπορεί να χρησιμοποιηθεί σαν ένα είδος firewall που θα φιλτράρει τα εισερχόμενα και τα εξερχόμενα πακέτα του δικτύου. Μπορεί επίσης από την στιγμή που θα εγκατασταθεί να κάνει όλο το εσωτερικό δίκτυο να φαίνεται ότι χρησιμοποιεί την εξωτερική IP του proxy server. Μία άλλη εργασία που εκτελεί ο proxy server είναι η χρήση κρυφής μνήμης όταν κάποιος εσωτερικός χρήστης κατεβάζει μία ιστοσελίδα από έναν απομακρυσμένο Web server ο proxy server αποθηκεύει την ιστοσελίδα και σε περίπτωση που κάποιος άλλος χρήστης ζητήσει την ίδια σελίδα ο proxy server του την στέλνει χωρίς να χρειάζεται να την ξανακατεβάσει από τον απομακρυσμένο web server.

Χάρη στην υπηρεσία πανδικτυακού proxy , όσες εταιρείες μετακινούν μεγάλο όγκο ή αριθμό αρχείων, καθώς και audio ή video έχουν τη δυνατότητα να προσφέρουν καλύτερη ποιότητα περιεχομένου στο ευρύ κοινό, επιτυγχάνοντας παράλληλα μια σημαντική εξοικονόμηση χρημάτων. Γι' αυτό και στο εξωτερικό οι υπηρεσίες αυτές είναι εξαιρετικά διαδεδομένες, ενώ πρόσφατα άρχισαν να κάνουν ορατή την παρουσία τους και στη χώρα μας. Σύντομα λοιπόν πολλοί μεγάλοι Έλληνες παραγωγοί δικτυακού περιεχομένου θα γίνουν πελάτες τους, ενώ όλοι μας θα απολαμβάνουμε καλύτερες υπηρεσίες χάρη σε αυτή την εξαιρετικά απλή στη σύλληψη, αλλά περίπλοκη στην υλοποίηση τεχνολογία. (Οι αλγόριθμοι κατανομής φόρτου εργασίας μεταξύ των servers που χρησιμοποιούν εταιρείες όπως η Akamai αποτελούν έναν από τους δυναμικότερους κλάδους της μαθηματικής ανάλυσης.)

Η χρήση διακομιστών μεσολάβησης (proxy servers) είναι ευρύτατη στο internet για πολλούς λόγους. Σχεδόν όλοι οι οργανισμοί ανά τον κόσμο, οι οποίοι χρησιμοποιούν εσωτερικά τοπικά δίκτυα τα οποία παρέχουν πρόσβαση στο internet, χρησιμοποιούν proxy servers. Τα πλεονεκτήματα είναι πολλά, είναι όμως σκόπιμο να αναφέρουμε ότι με τους proxy επιτυγχάνουμε κατά βάση τα εξής:

- **Επιτάχυνση της περιήγησης στο διαδίκτυο.** Ο proxy server σε όλα τα δίκτυα είναι εγκατεστημένος σε σημείο κατάλληλο ώστε να έχει την ταχύτερη πρόσβαση στο internet. Όταν ένας χρήστης χρησιμοποιεί τον proxy, ζητάει με το πρόγραμμά του την αναμετάδοση του

περιεχομένου που επιθυμεί. Ο proxy πραγματοποιεί τη σύνδεση για λογαριασμό του χρήστη και αναμεταδίδει το περιεχόμενο σε αυτόν, χωρίς να πρέπει να συνδεθεί ο χρήστης με τον απομακρυσμένο τόπο μέσω γραμμών χαμηλής ταχύτητας.

- **Αποθήκευση των δημοφιλών σελίδων.** Ο proxy όταν αναμεταδίδει ένα δικτυακό τόπο, τον αποθηκεύει και τοπικά. Έτσι, ο επόμενος χρήστης που θα θελήσει να δει την ίδια σελίδα, την διαβάζει κατευθείαν από τον proxy server και δεν χρειάζεται να την ξαναζητήσει μέσω του internet. Ο διακομιστής μεσολάβησης ταυτόχρονα ελέγχει σε τακτά χρονικά διαστήματα για νεώτερες εκδόσεις των σελίδων. Έτσι πέραν της επιτάχυνσης, επιτυγχάνεται και απελευθέρωση της γραμμής με το internet από άσκοπες μεταφορές δεδομένων. Ένας καλός proxy server σε ένα τυπικό δίκτυο επιτυγχάνει βελτίωση μέχρι και 40%.
- **Αύξηση ασφάλειας από ιούς.** Ο διακομιστής μεσολάβησης πέρα από την αναμετάδοση μπορεί να χρησιμοποιεί και προγράμματα ελέγχου για ιούς. Έτσι αποφεύγεται η μεταφορά επικίνδυνου περιεχομένου στους χρήστες.
- **Αύξηση ασφάλειας δικτύου.** Οι διακομιστές μεσολάβησης είναι ισχυροί υπολογιστές με ασφαλή και σταθερά λειτουργικά συστήματα, τα οποία μέσω της λειτουργίας τους σαν proxy εμποδίζουν την απευθείας σύνδεση των χρηστών με το internet.
- **Έλεγχος ροής.** Με τους διακομιστές μεσολάβησης, μπορούν να εφαρμοστούν πολιτικές που δίνουν προτεραιότητα στην περιήγηση στο διαδίκτυο, έναντι άλλων υπηρεσιών λιγότερο σημαντικών. Έτσι μπορεί να βελτιωθεί ακόμα περισσότερο η όλη ταχύτητα περιήγησης.

Όλα τα παραπάνω, κάνουν τους proxy servers πολύ δημοφιλείς και απαραίτητους σε όλα τα σύγχρονα δίκτυα.

# ΑΚΡΩΝΥΜΙΑ

**Active Directory:**Ενεργός κατάλογος**.**Ο ενεργός κατάλογος χρησιμοποιείται για την διαχείρηση των λογαριασμών των πόρων και την ασφάλεια του δικτύου.

**Cache Memory**:Κρυφή μνήμη.Είναι η μνημη που χρησιμοποίει ο proxy server για την αποθήκευση των ιστοσελίδων που θα χρησιμοποιήσει για να τις ξαναστείλει στους χρήστες του εσωτερικού δικτύου.

**DHCP SERVER**:Dynamic Host Configuration Protocol.Πρωτόκολλο για την απόδοση IP διευθήνσεων σε Η/Υ με δυναμικό τρόπο.

**Domain Controller**:Ελεγκτής περιοχής.Διακομιστής στον οποίο τρέχει ο ενεργός κατάλογος(Active Directory) ή είναι ο ελεγκτής περιοχής.

**Firewall**: Ένα εικονίκο τοίχος προστασίας που δεν επιτρέπει τυην παράνομη πρόσβαση στο δίκτυο.

**FTP Server**:File Transfer Protocol.Πρωτόκολλο για την μεταφορά αρχείων από Η/Υ σε Η/Υ ανεξάρτητα από το λειτουργικό σύστημα που χρησιμοποιούν.

**HTML**:Hypertext Transfer Protocol.Πρωτόκολλο που καθορίζει τον τρόπο με τον οποίο ο πελάτης ζητά από τον server να του στείλει τις ιστοσελίδες

**IIS**: Internet information Services.Εφαρμογή των Windows 2000 Server για την διαχείριση των υπηρεσιών των δικτύων και των διαδικτύων.

**Intranet**: Εσωτερικό δίκτυο ,το δίκτυο μιας επιχείρησης.

**IP Διεύθυνση**: Η 32bit διεύθυνση του κάθε Η/Υ σε ένα δίκτυο.

**LAT**:Local Address Table.Ο πίνακας διευθύνσεων ενός τοπικού δικτύου.

**MS DOS**:Λειτουργικό σύστημα

**Msp2wizi.exe**:Microsoft Proxy Server Setup Wizard.Το αρχείο για την εγκατάσταση του proxy server για Windows 2000 server.

**NAT IP**:Network address translation. IP διευθύνσεις που έχουν καταχωρηθεί για δοκιμαστικά δίκτυα και είναι ελεύθερες στη χρήση τους από τον καθένα.

**NTFS**: New Technology File System.Σύστημα διαμέρησεις δίσκων.

**Proxy Server**: Διακομιστής Μεσολαβητής .Έιναι ο διακομιστής που χωρίζει το εσωτερικό από το εξωτερικό δίκτυο και προσφέρει και υπηρεσίες cache memory.

**Server**: Διακομιστής .Ο Η/Υ που έχει ρυθμιστεί να προσφέρει υπηρεσίες και διαδυκτύων.

**TCP/IP**:Transfer Communication Protocol.Πρωτόκολλο για την επικοινωνία Η/Υ σε δίκτυα.

**Web Server**:Διακομιστής Ιστού. Ο Διακομιστής που προσφέρει υπηρεσίες ιστοσελίδων.

**Web Site**:Ιστοσελίδα.

**Δομές Περιοχών**: Δίκτυα που χωρίζονται σε περιοχές για την καλύτερη διαχείρισή τους.

**Κλάσης Δικτύων**: Ο χωρισμός των δικτύων σε κλάσης με βάση την IP διεύθυνσή τους.

**Κώδικας ASCII**:Ο κώδικας που αντιστοιχεί τον κάθε χαρακτήρα σε δυαδικά ψηφία.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ”Builting Internet Firewalls”
D.Brent Chapman & Elizabeth D. Zwicky
O’Reilly, First Edition, November 2000

2. ”X RAM , Firewalls, τα αντιπυρικά τείχη
Θ.Μότσιος
“Τεύχος 6 Μάιος 2001. Ειδική έκδοση του RAM , εκδόσεις Λαμπράκης”

3. ”Web Caching”
Duane Wessels
O’Reilly & Accociates, Inc-2001

4. ”Squid. A user’s Guide”
Oskar Pearson
Copyright © 2000 by Oskar Pearson

5. ”Linux Firewall and Proxy Server HOWTO, http://www.tldp.org”
Mark Grennan

6. ”Microsoft® Proxy Server 2.0 MCSE Study System”
Simmons Curt
IDG Books Worldwide, Inc-2000

7. “Hacker Proof”
Lars Klander
Jamsa Press 2002

8. Pure Sight of Squid : http://www.icognito.com/PDF/PureSight_Squid.pdf

9. Adv-Routing-HOWTO:
http://sunsite.ui.ac.id/pub/linux/docs/HOWTO/Adv-Routing-HOWTO.html

10. Εγχειρίδιο διαχειριστή δικτύου των Microsoft Windows 2000 Server
Charlie Russel-Sharon Crawford
Εκδόσεων Κλειδάριθμος© 2000

11. Ο Βοηθός του διαχειριστή δικτύου των Microsoft Windows 2000 Server & Professional
William R. Stanek
Εκδόσεων Κλειδάριθμος © 2000

12. Δίκτυα Υπολογιστών
Andrew S. Tanenbaum
Εκδόσεις Παπασωτηρίου © 2001