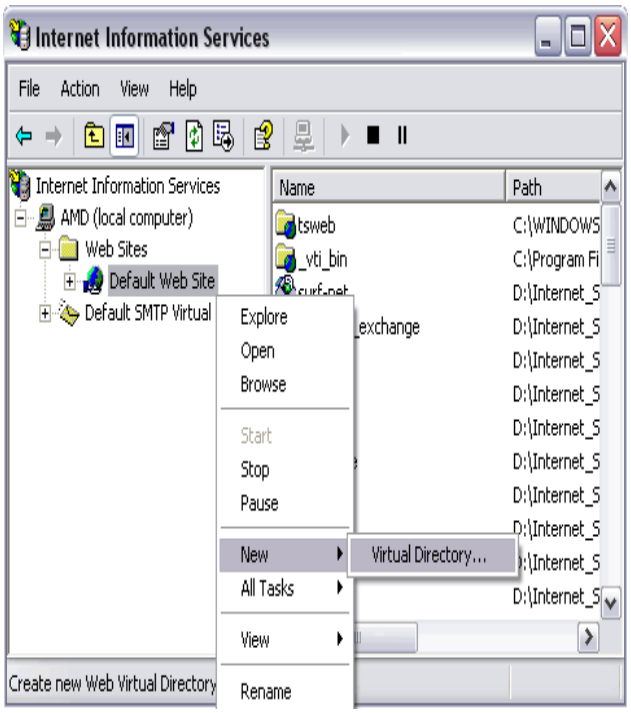
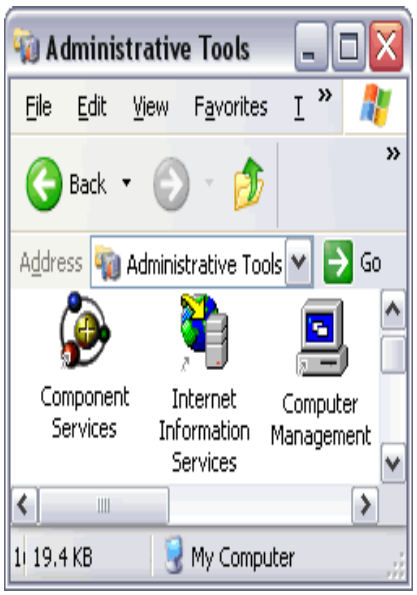
Τ.Ε.Ι. ΗΠΕΙΡΟΥ
T.E.I. OF EPIRUS

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

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

ΕΓΚΑΤΑΣΤΑΣΗ & ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ INTERNET INFORMATION SERVER (IIS) ΓΙΑ ΥΛΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ (WEB SERVICES)





ΣΠΟΥΔΑΣΤΡΙΑ: ΜΠΑΡΔΑ ΜΑΡΙΑ
ΕΙΣΗΓΗΤΗΣ: ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΑΡΤΑ 2006

ΠΕΡΙΕΧΟΜΕΝΑ

Η αλματώδης εξέλιξη του Διαδικτύου συντέλεσε στη διάδοση των υπηρεσιών με πιο δημοφιλή αυτή του Παγκόσμιου Ιστού. Το Internet αποτελεί πλέον ένα σημείο παρουσίας πολλών εκατομμυρίων χρηστών και οργανισμών μέσω των δικτυακών τους τόπων. Η δημοσίευση των ιστοσελίδων στο Διαδίκτυο καθώς και οι υπόλοιπες υπηρεσίες βασίζονται στην client - server αρχιτεκτονική. Οι εξυπηρετητές των υπηρεσιών Διαδικτύου, οι web servers αποτελούνται από ειδικά εργαλεία λογισμικού εγκατεστημένα σε σταθμούς του δημόσιου δικτύου για την αποστολή των περιεχομένων των δικτυακών τόπων. Στη συγκεκριμένη εργασία εξετάζουμε την εγκατάσταση και παραμετροποίηση ενός από τους πιο διαδεδομένους web servers, τον IIS server. Σκοπός είναι η λεπτομερής περιγραφή βήμα προς βήμα της εγκατάστασης και παραμετροποίησης καθώς επίσης και μιας αποτίμησης του εργαλείου.

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 ΤΟ ΔΙΑΔΙΚΤΥΟ

Το Internet ξεκίνησε τη δεκαετία του ’60 όταν εμφανίστηκαν στον στρατό των ΗΠΑ τα πρώτα δίκτυα υπολογιστών, δηλ. υπολογιστές που μπορούσαν να επικοινωνούν μεταξύ τους, ανταλλάσσοντας πληροφορίες. Καθώς η χρήση των δικτύων υπολογιστών γινόταν ολοένα και πιο απαραίτητη, άρχισε να αναπτύσσεται το 1969 από το Αμερικανικό Υπουργείο Άμυνας, ένα δίκτυο με το όνομα ARPANET με σκοπό να συμβάλλει στη διεξαγωγή των ακαδημαϊκών και στρατιωτικών ερευνών της χώρας.

Καθώς επεκτεινόταν, όμως, το ARPANET, συνδέονταν σ' αυτό όλο και περισσότερα ακαδημαϊκά και ερευνητικά δίκτυα, με στόχο να διευκολύνουν την ανταλλαγή πληροφοριών μεταξύ των διαφόρων οργανισμών.

Μέχρι το 1983, που έκανε την εμφάνισή του ο πρώτος προσωπικός υπολογιστής (PC - Personal Computer) της IBM, η χρήση των υπολογιστών ήταν προνόμιο των μεγάλων εταιριών, της ακαδημαϊκής κοινότητας και του στρατού. Οι προσωπικοί υπολογιστές γνώρισαν τεράστια τεχνολογική ανάπτυξη τις δεκαετίες του ’80 και του ’90 και επεκτάθηκαν σε κάθε ανθρώπινη δραστηριότητα. Το επόμενο μεγάλο βήμα ήταν η επικοινωνία των υπολογιστών μεταξύ τους και τελικά η δημιουργία του διαδικτύου, δηλ. του δικτύου που αποτελείται από διάφορα δίκτυα σε όλο τον κόσμο, του Internet.

Το Internet, με τη μορφή που το ξέρουμε σήμερα, ξεκίνησε με τη δημιουργία του NSFNet (National Science Foundation) το 1986, το οποίο αρχικά συνέδεσε υπολογιστικά κέντρα στις ΗΠΑ και αργότερα επεκτάθηκε διασυνδέοντας δίκτυα μεσαίου μεγέθους εκπαιδευτικών ιδρυμάτων, πανεπιστημίων και ερευνητικών κέντρων. Το NSFNet τελικά αντικατέστησε το ARPANET ενώ παρόμοια διεθνή δίκτυα, όπως το Ευρωπαϊκό EARN και το PACCOM των χωρών του Ειρηνικού Ωκεανού, άρχισαν να δημιουργούνται σ’ όλο τον κόσμο. Αυτά, συνδεόμενα μεταξύ τους, κατέληξαν στο σημερινό Internet .

1.2 ΥΠΗΡΕΣΙΕΣ ΤΟΥ INTERNET

Οι χρήστες του παγκόσμιου Διαδικτύου δηλ. του Internet μπορούν να χρησιμοποιούν ένα σύνολο από υπηρεσίες. Οι χρήστες συνδέονται από υπολογιστές-Πελάτες μέσω δικτύου ή μέσω τηλεφωνικών συνδέσεων με τους διακομιστές ή εξυπηρετητές των υπηρεσιών του Internet.

Οι πιο διαδεδομένες υπηρεσίες που προσφέρουν οι υπολογιστές-Εξυπηρετητές είναι οι εξής:

1.2.1 Το Ηλεκτρονικό Ταχυδρομείο (e-mail)

Με το ηλεκτρονικό ταχυδρομείο, ή απλά e-mail, οι χρήστες μπορούν να επικοινωνούν με μηνύματα στον υπολογιστή στα οποία επισυνάπτουν αρχεία όπως κείμενα, εικόνες και ηχητικά μηνύματα. Το e-mail είναι άμεσο και γρήγορο δίνοντας τη δυνατότητα της σχεδόν στιγμιαίας επικοινωνίας με αλληλογραφία μεταξύ πολλών χρηστών.

1.2.2 Ο Παγκόσμιος Ιστός (www).

Είναι το σύνολο των ιστοσελίδων που είναι διαθέσιμες στο Internet. Οι ιστοσελίδες είναι αρχεία τα οποία περιέχουν κείμενα, εικόνες, ήχο και video καθώς και υπερσυνδέσεις

προς άλλες θέσεις του ιστού. Τα κείμενα που περιέχουν υπερσυνδέσεις λέγονται υπερκείμενα ενώ τα μέσα που τις χρησιμοποιούν λέγονται υπερμέσα. Οι ιστοσελίδες είναι συνήθως οργανωμένες σε δικτυακούς τόπους. Για την εύρεση πληροφοριών μέσα στον Παγκόσμιο Ιστό υπάρχουν ειδικές τοποθεσίες που λειτουργούν σαν ευρετήρια και ονομάζονται μηχανές αναζήτησης*.

(*)Οι μηχανές αναζήτησης είναι βάσεις δεδομένων, όπου είναι καταχωρημένος ένας τεράστιος αριθμός πληροφοριών για τις υπάρχουσες ιστοσελίδες στους δικτυακούς τόπους (sites) του Internet και η αναζήτηση κρατάει μερικά μόνο δευτερόλεπτα.

1.2.3 Μηνύματα σε Κινητά Τηλέφωνα μέσω του Internet

Υπάρχει η δυνατότητα αποστολής και λήψης μηνυμάτων SMS από υπολογιστή σε συσκευές κυψελοειδούς τηλεφωνίας και το αντίστροφο.

1.2.4 Ομάδες Συζητήσεων (newsgroups)

Οι ομάδες συζητήσεων (newsgroups) είναι πίνακες ανακοινώσεων, όπου οι χρήστες μπορούν να δημοσιεύσουν απόψεις για κάποιο θέμα. Οι συζητήσεις είναι κατηγοριοποιημένες κατά θέμα. Οι χρήστες έχουν ακόμη τη δυνατότητα να απαντήσουν μέσω του πίνακα σε κάποιες δημοσιευμένες απόψεις.

1.2.5 Συνομιλία μέσω του Internet (Chat Rooms)

Με προγράμματα όπως το IRC (Internet Relay Chat) οι χρήστες μπορούν να στέλνουν γραπτά μηνύματα σε πραγματικό χρόνο όπως θα γινόταν σε μια συνομιλία και με κάρτα ήχου, ηχεία και μικρόφωνο, μπορούν να συνομιλούν με ελάχιστο κόστος με άτομα απ' όλο τον κόσμο.

1.2.6 Telnet

Με την υπηρεσία Telnet του Internet ένας χρήστης μπορεί να συνδεθεί μ' έναν απομακρυσμένο υπολογιστή και να μετατρέψει τον υπολογιστή του σε τερματικό έτσι ώστε να μπορεί να ελέγχει τις εφαρμογές και να έχει πρόσβαση σε δεδομένα και προγράμματα του απομακρυσμένου υπολογιστή. Ένας εξυπηρετητής Telnet μπορεί να είναι προσβάσιμος από όλους τους χρήστες ή μπορεί να απαιτεί τη χρήση ειδικού ονόματος χρήστη και κωδικού πρόσβασης. Κάθε σύνοδος Telnet μεταξύ του εξυπηρετητή και του υπολογιστή-πελάτη είναι διαφορετική και έχει τους δικούς της κανόνες και εξαρτάται από τον τύπο του συστήματος που έχει εγκατασταθεί στον άλλον υπολογιστή. Η ταχύτητα της υπηρεσίας Telnet εξαρτάται από το πόσο μεγάλη κίνηση

υπάρχει προς τον υπολογιστή-εξυπηρετητή και στον αριθμό των χρηστών που είναι συνδεδεμένοι εκείνη τη στιγμή.

1.2.7 Μεταφορά Αρχείων FTP (File Transfer Protocol)

Το πρωτόκολλο FTP χρησιμοποιείται για την μεταφορά των αρχείων από υπολογιστή σε υπολογιστή. Τα αρχεία που μεταφέρονται μπορεί να είναι είτε εκτελέσιμα αρχεία ή αρχεία δεδομένων. Τα αρχεία στέλνονται στον υπολογιστή παραλήπτη από έναν FTP - server που ανήκει συνήθως σε μεγάλες εταιρείες ή οργανισμούς, που παρέχουν υπηρεσίες στους χρήστες του Internet.

1.3 Πρωτόκολλο TCP/IP

Το Internet χρησιμοποιεί την τεχνολογία μεταγωγής πακέτων για τη μεταφορά των δεδομένων (τα δεδομένα κόβονται σε κομμάτια που ονομάζονται πακέτα). Ο χωρισμός των δεδομένων σε πακέτα επιτρέπει στο Internet να χρησιμοποιεί ταυτόχρονα τις ίδιες γραμμές επικοινωνίας για να εξυπηρετεί πολλούς χρήστες.

Όλα τα πακέτα περιέχουν βασικά στοιχεία όπως :

- Διεύθυνση προέλευσης
- Δεδομένα
- Διεύθυνση προορισμού
- Οδηγίες
- Πληροφορίες για την εκ νέου συναρμολόγηση του πακέτου δεδομένων
- Πληροφορίες ελέγχου σφαλμάτων

Τα παραπάνω στοιχεία βρίσκονται μέσα στα εξής τμήματα των πακέτων:

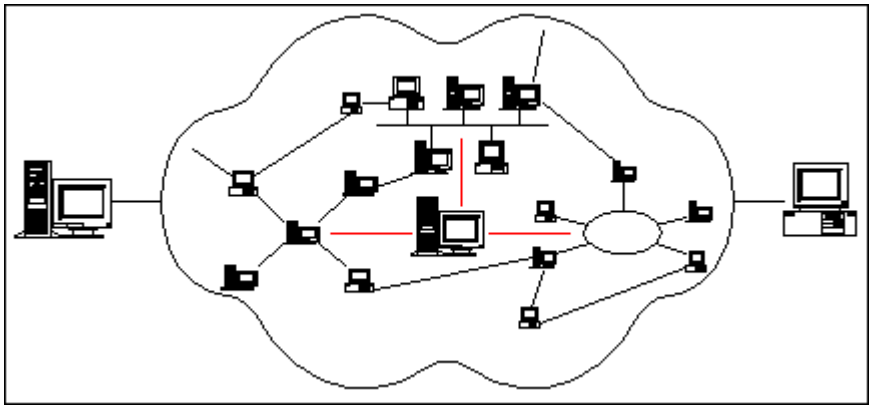
- Μια κεφαλίδα που περιέχει πληροφορίες χρόνου
- Τα δεδομένα
- Ένα επίμετρο που περιέχει στοιχεία έλεγχου σφαλμάτων

Κάθε υπολογιστής που συνδέεται στο Internet αντιστοιχίζεται με μία μοναδική διεύθυνση που ονομάζεται διεύθυνση **IP.**

Το ***πρωτόκολλο IP*** (*Internet Protocol - Πρωτόκολλο Διαδικτύωσης*) είναι υπεύθυνο για τη μεταφορά του πακέτου από υπολογιστή σε υπολογιστή μέσα από ένα πλέγμα

συνδέσεων. Καθώς το IP δρομολογεί το κάθε πακέτο μέσα στο δίκτυο, προσπαθεί να το παραδώσει, χωρίς να μπορεί να εγγυηθεί ότι το πακέτο θα φτάσει στον προορισμό του, ούτε κι ότι τα διάφορα πακέτα που αποτελούν τα αρχικά δεδομένα θα φτάσουν με τη σειρά με την οποία στάλθηκαν αλλά ούτε ότι το περιεχόμενο των πακέτων θα φτάσει αναλλοίωτο.

Το ***πρωτόκολλο TCP*** (*Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μετάδοσης*) είναι περισσότερο αξιόπιστο σε σχέση με το πρωτόκολλο IP. Εγγυάται ότι τα πακέτα θα παραδοθούν στον προορισμό τους, ότι θα φτάσουν με τη σειρά με την οποία στάλθηκαν και ότι τα περιεχόμενα των πακέτων θα φτάσουν αναλλοίωτα.



Εικόνα 1. Το Διαδίκτυο

Το ***TCP*** χρησιμοποιείται για τον έλεγχο των δεδομένων και το ***IP*** για την μεταφορά των δεδομένων από τον ένα υπολογιστή στον άλλον.

1.4 ΔΙΕΥΘΥΝΣΕΙΣ ΤΟΥ INTERNET & ΣΥΣΤΗΜΑ ΟΝΟΜΑΤΩΝ ΠΕΡΙΟΧΩΝ

Όπως είδαμε, κάθε σύνολο δεδομένων όπως αρχεία, κείμενα, αιτήσεις κλπ κατατέμνονται σε πακέτα και ταξιδεύουν μέσα από τις συνδέσεις των δικτύων προς έναν προορισμό. Ο αποστολέας και ο παραλήπτης του πακέτου ταυτοποιούνται ο καθένας από έναν μοναδικό αριθμό ή αλλιώς μια IP διεύθυνση. Η διαδικασία διευθυνσιοδότησης είναι πολύ σημαντική υπηρεσία του Internet, γιατί καθορίζει τις διευθύνσεις των z\συστημάτων κάθε σταθμού εργασίας (host) σε ολόκληρο τον κόσμο. Το πακέτο θα

φτάσει στον προορισμό του ακολουθώντας το μονοπάτι που του υποδεικνύει η IP διεύθυνση του παραλήπτη.

Οι IP διευθύνσεις του Internet είναι αριθμοί των 32 bits, που, συνήθως, για λόγους ευκολίας γράφεται ως τέσσερις τριάδες της μορφής xxx.xxx.xxx.xxx (dotted decimal notation). Κάθε τριάδα αριθμών μπορεί να πάρει τιμή 0 ως 255. Έτσι, η οποιαδήποτε διεύθυνση θα έχει τιμή μεταξύ 0.0.0.0 και 255.255.255.255.

Η διεύθυνση υποδεικνύει το δίκτυο και τον host υπολογιστή που βρίσκεται μέσα στο δίκτυο και η διαδικασία που ακολουθείται για να σταλεί ένα πακέτο στον προορισμό του, αναφέρεται σαν *δρομολόγηση* (routing).

Είναι προφανές ότι για να συνδεθούμε με κάποιο φορέα του Internet θα ήταν πολύ δύσκολο να θυμόμαστε τον δωδεκαψήφιο αριθμό τηςIP διεύθυνσης και θα έπρεπε να τηρούμε κατάλογο διευθύνσεων για τις εκατοντάδες ιστοσελίδες που θέλουμε να επισκεφτούμε.

Οι διευθύνσεις των διαφόρων παροχέων ή κόμβων μπορούν να αποδοθούν με κάποιο όνομα του οργανισμού ή της εταιρείας ή της υπηρεσίας που διαθέτει κόμβο στο Internet, με κάποια προθέματα ή κάποια επιθέματα που δηλώνουν ιδιότητα ή χώρα προέλευσης. Προκειμένου για διεύθυνση παροχέα ή φορέα, χρησιμοποιούμε όχι την IP διεύθυνση αλλά μια διεύθυνση της μορφής http://www.in.gr όπου το www.in.gr είναι το όνομα τομέα / περιοχής (Domain name).

Το πρώτο συνθετικό (http) δηλώνει το πρωτόκολλο με το οποίο έχουμε συνδεθεί με το συγκεκριμένο εξυπηρετητή (server) και δείχνει ότι έχουμε συνδεθεί για μεταφορά πληροφοριών με τη μορφή υπερκειμένου μέσω του Internet. Το πρόθεμα αυτό θα μπορούσε να ήταν ftp, αν είχαμε συνδεθεί με τον server για μεταφορά αρχείων. Είναι αυτονόητο ότι πρέπει ο server να υποστηρίζει την αντίστοιχη εργασία. Ακολουθεί ένα τυπικό διαχωριστικό με άνω κάτω τελεία και διπλή κάθετο (:///) και στη συνέχεια αναγράφεται η ένδειξη www (World Wide Web) που υποδηλώνει ότι πρόκειται για σελίδα του παγκόσμιου ιστού. Αμέσως μετά δηλώνεται το όνομα τομέα που αποτελείται από μια υποπεριοχή (Sub-domain) της διεύθυνσης (webdelivery), ενώ μπορεί και να υπάρχει και δεύτερο συνθετικό υποπεριοχής (π.χ. ee.auth).

Το τελευταίο συνθετικό – επίθεμα δηλώνει την ιδιότητα ή την εθνικότητα του παροχέα - φορέα, που είναι στην ουσία η κυρία περιοχή (domain) του.

Τα πιο γνωστά επιθέματα που δηλώνουν ειδικότητα είναι τα εξής:

- com: για εμπορική επιχείρηση (**com**mercial).

- edu: για εκπαιδευτικό ίδρυμα (**edu**cation).
- gov: για κυβερνητική υπηρεσία (**gov**ernment).
- mil: για στρατιωτική υπηρεσία (**mil**itary).
- org: για οργανισμό (**org**anization).

Στα επιθέματα εθνικοτήτων, τα γράμματα που αναγράφονται είναι συνήθως δύο και είναι χαρακτηριστικά του ονόματος της χώρας όπως αυτό αναφέρεται στα Αγγλικά. Για παράδειγμα μερικά είναι τα εξής: Ελλάδα (gr), Αίγυπτος (eg), Αυστραλία (au), Βέλγιο (be), Βραζιλία (br), Γερμανία (ge), Ιταλία (it), Ηνωμένο Βασίλειο (uk), Ηνωμένες Πολιτείες (us), Κίνα (cn), Τουρκία (tr), Ταϊβάν (tw), Ρωσία (ru), κλπ.

1.5 Web Servers

Όπως γνωρίζουμε η υλοποίηση των Υπηρεσιών του Internet στηρίζεται στη *client – server* αρχιτεκτονική. Οι υπηρεσίες αυτές όπως είναι ο *Παγκόσμιος Ιστός* (World Wide Web) ή το *Ηλεκτρονικό Ταχυδρομείο* (e-Mail) ή η *Μεταφορά Αρχείων* (File Transfer) προσφέρονται από Εξυπηρετητές (Servers) του Δικτύου οι οποίοι με το κατάλληλο λογισμικό μπορούν να εξυπηρετήσουν ταυτόχρονα πολλούς χρήστες. Οι χρήστες χρησιμοποιούν υπολογιστές ή συστήματα-Πελάτες (client) για να συνδεθούν με κάποιον εξυπηρετητή και να γίνουν αποδέκτες των υπηρεσιών.

Έτσι θα λέγαμε ότι η έννοια ***Web Server*** έχει δύο συστατικά: Το ένα αφορά των υπολογιστή ο οποίος έχει αναλάβει το ρόλο του διακομιστή ή αλλιώς εξυπηρετητή (server) για να απαντά συνήθως σε αιτήματα πελατών-υπολογιστών (client). Ταυτόχρονα όμως η έννοια αφορά και το λογισμικό, το οποίο είναι εγκατεστημένο σε ένα Εξυπηρετητή και αναλαμβάνει να εξυπηρετήσει τις client εφαρμογές που αιτούνται τις υπηρεσίες από τον Web Server.

Συνοπτικά, οι ***Web Server*** είναι προγράμματα εγκατεστημένα σε υπολογιστές – Εξυπηρετητές (servers) που αναλαμβάνουν συνήθως τις εξής λειτουργίες:

- Αναλαμβάνουν να απαντούν σε αιτήματα HTTP (Hyper Text Transfer Protocol). Οι Web Servers δέχονται αιτήματα HTTP από client εφαρμογές που είναι συνήθως οι φυλλομετρητές (web browsers) και στέλνουν μια HTTP απάντηση η οποία αποτελείται συνήθως από περιεχόμενο HTML (Hyper Text Markup Language), το οποίο μεταφράζεται και παρουσιάζεται στον client

υπολογιστή. Ο server αναλαμβάνει να στείλει και κάποιο μήνυμα λάθους σε περίπτωση που έχει γίνει κάποιο σφάλμα στην όλη διαδικασία.

- Διατήρηση Αρχείου Log (Logging). Οι Web Servers επίσης, αναλαμβάνουν τη διατήρηση ενός log αρχείου που περιέχει τις κινήσεις αιτημάτων και απαντήσεων από και προς του clients δίνοντας έτσι τη δυνατότητα ελέγχου και καταγραφής στατιστικών στους διαχειριστές τους.
- Παραμετροποίηση. Δίνουν τη δυνατότητα στους διαχειριστές τους με τα κατάλληλα περιβάλλοντα διεπαφής Χρήστη (user interface) να ελέγχουν και να παραμετροποιούν τον τρόπο λειτουργίας τους.
- Ταυτοποίηση. Δίνουν τη δυνατότητα στους διαχειριστές τους να ελέγχουν και καθορίζουν την πρόσβαση χρηστών προς τις υπηρεσίες που προσφέρουν.
- Διαχείριση μη στατικού περιεχομένου. Με την ανάπτυξη των δυναμικών σελίδων οι web servers απέκτησαν τη δυνατότητα μεταγλώττισης και αποστολής προς τις client εφαρμογές δυναμικού περιεχομένου. Έτσι σήμερα μπορούν και εξυπηρετούν ποικίλες πλατφόρμες δυναμικού προγραμματισμού όπως SSI, CGI, SCGI, FastCGI, PHP, ASP, ASP .NET, Server API κ.α.
- Υποστήριξη Module, έτσι ώστε να μπορούν να επεκταθούν οι δυνατότητες και οι υπηρεσίες που προσφέρουν. Για παράδειγμα η νέα έκδοση του IIS στηρίζεται σε αυτή την αρχιτεκτονική.
- Υποστήριξη πρωτοκόλλων ασφαλείας. Υποστηρίζουν πλέον την ασφαλή μετάδοση πληροφοριών με τη χρήση πρωτοκόλλων όπως το HTTPS (HTTP Secure).
- Συμπίεση δεδομένων για τη μετάδοση πληροφοριών με μεγαλύτερη ταχύτητα και καλύτερη διαχείριση του διαθέσιμου εύρους ζώνης.
- Virtual Hosting έτσι ώστε να εξυπηρετούνται πολύ δικτυακοί τόποι με μια IP διεύθυνση.

1.6 ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ΟΙ WEB SERVERS

Συνοπτικά, θα περιγράψουμε τη σύνδεση ενός χρήστη του Internet με έναν web server κατά την επίσκεψή του, για παράδειγμα, σε κάποιο δικτυακό τόπο που είναι

εγκατεστημένος στον server, για να έχουμε μια εικόνα του τρόπου που ο server εξυπηρετεί έναν επισκέπτη.

Η client – server αρχιτεκτονική υλοποιείται με τη σύνδεση ενός μηχανήματος client με έναν web server. Στον client υπολογιστή υπάρχει η αντίστοιχη web client εφαρμογή που στην πραγματικότητα είναι ένας Internet browser όπως ο Internet Explorer. Όταν ένας χρήστης του Internet πληκτρολογεί ή κάνει κλικ σε μια υπερσύνδεση στο URL (Unified Resource Location) μιας ιστοσελίδας π.χ. http://www.in.gr/index.htm τότε ακολουθούνται τα παρακάτω βήματα:

- Ο browser διαχωρίζει τη URL σε τμήματα, ξεχωρίζοντας το *πρωτόκολλο* (“http”), το *domain* (“www.in.gr”) και το *όνομα της ιστοσελίδας* (“index.htm”).
- Στη συνέχεια επικοινωνεί με κάποιον *DNS* (Domain Name Server) έτσι ώστε το όνομα domain που πληκτρολογήθηκε να μεταφραστεί σε IP διεύθυνση.
- Κατόπιν ο browser επικοινωνεί με τον server στην αντίστοιχη IP διεύθυνση και συγκεκριμένα στη θύρα 80 που είναι η προεπιλεγμένη για τον Παγκόσμιο Ιστό. Ο browser στέλνει μια αίτηση GET στον server ζητώντας από αυτόν να του αποστείλει το αρχείο index.htm.
- Στη συνέχεια ο web server στέλνει το περιεχόμενο σε μορφή HTML ιστοσελίδας χρησιμοποιώντας το πρωτόκολλο HTTP.
- Τέλος, ο browser παραλαμβάνει το περιεχόμενο σε μορφή αρχείου HTML και αναλαμβάνει να σχηματίσει την ιστοσελίδα στην οθόνη του χρήστη χρησιμοποιώντας τα HTML tags του αρχείου HTML.

Η διαδικασία αποστολής μιας αίτησης από την client εφαρμογή και απάντησης από τον server είναι κοινή και στην εξυπηρέτηση των υπόλοιπων υπηρεσιών του Internet.

ΚΕΦΑΛΑΙΟ 2

2.1 Internet Information Services – IIS

Ο IIS (Internet Information Server) της Microsoft αναφέρεται σε ένα σύνολο από υπηρεσίες του Internet που προσφέρονται από servers που είναι εγκατεστημένοι στο λειτουργικό σύστημα Microsoft Windows. Ο IIS Web Server της Microsoft είναι μαζί με τον Apache HTTP Server από τους πιο δημοφιλείς web servers.

Ο IIS ξεκίνησε αρχικά σαν ένα σύνολο επιπρόσθετων υπηρεσιών που αφορούσαν το Internet στην έκδοση των Windows NT 3.51. Στη συνέχεια ακολούθησε ο IIS 2.0 ο οποίος υποστηριζόταν από την έκδοση των Windows NT 4.0. Η έκδοση IIS 3.0 ήταν αυτή που υποστήριζε τη μεταγλώττιση δυναμικών ιστοσελίδων ASP (Active Server Pages - dynamic scripting environment). Στη συνέχεια καθώς η Microsoft κυκλοφορούσε τις νέες εκδόσεις των Windows, ενσωμάτωσε νέες εκδόσεις του IIS. Έτσι δημιουργήθηκε η έκδοση IIS 5.0 για τα Windows 2000 και IIS 5.1 για τα Windows XP Professional. Προς το παρόν, η τελευταία έκδοση του IIS είναι η έκδοση IIS 6.0 για το λειτουργικό σύστημα Windows Server 2003 .

Το επόμενο βήμα θα είναι η έκδοση IIS 7.0 η οποία θα είναι προεγκατεστημένη στα αναμενόμενα Windows Vista. Στην νέα του έκδοση οι περιορισμοί δεν θα εξαρτώνται από το πλήθος των ταυτόχρονων συνδέσεων αλλά από το φόρτο των αιτήσεων ανάλογα με τις ταυτόχρονες συνδέσεις.

Συνοπτικά λοιπόν η ιστορία των εκδόσεων είναι η εξής:

- IIS 1.0, Windows NT 3.51 Service Pack 3
- IIS 2.0, Windows NT 4.0
- IIS 3.0, Windows NT 4.0 Service Pack 3
- IIS 4.0, Windows NT 4.0 Option Pack
- IIS 5.0, Windows 2000

- IIS 5.1, Windows XP Professional
- IIS 6.0, Windows Server 2003 και Windows XP Professional x64 Edition
- IIS 7.0, Windows Vista

Οι βασικές υπηρεσίες του *IIS* συνοψίζονται ως εξής:

- WWW: Οι **IIS Web Server** αναλαμβάνουν τη φιλοξενία και διακομιδή Ιστοσελίδων και Δικτυακών Τόπων. Ο Web Server απαντάει στις εισερχόμενες αιτήσεις για αποστολή του περιεχομένου των ιστοσελίδων προς τους clients που στην περίπτωση του Παγκόσμιου Ιστού είναι οι Web Browsers. Επίσης οι Web Server έχουν τη δυνατότητα εκτέλεσης .dll προγραμμάτων με βάση το πρότυπο ISAPI - Internet Server Application Programming Interface. Επίσης έχει τη δυνατότητα μεταγλώττισης και εκτέλεσης ενσωματωμένου κώδικα σε σελίδες δυναμικού περιεχομένου ASP (Active Server Pages). Δεν έχει τη δυνατότητα εκτέλεσης CGI ή κώδικα Perl, των οποίων η εκτέλεση μπορεί να γίνει με την προσθήκη εξωτερικών προγραμμάτων. Επίσης έχει τη δυνατότητα διασύνδεσης με βάσεις δεδομένων με τη χρήση του προτύπου ODBC (Open DataBase Connectivity). Τέλος, έχει τη δυνατότητα φιλοξενίας και εξυπηρέτησης πολλών δικτυακών τόπων με τη χρήση ενός μόνο Server ενώ η προεπιλεγμένη θύρα αποδοχής HTTP αιτήσεων σε επίπεδο εφαρμογής είναι η θύρα 80.
- FTP (File Transfer Protocol): αναλαμβάνει την αποστολή αρχείων σε έναν client με τη χρήση του πρωτοκόλλου FTP. Για κάθε υπηρεσία FTP αντιστοιχεί μία μόνο IP διεύθυνση ενώ η προεπιλεγμένη θύρα για την υπηρεσία είναι η θύρα 21.
- SMTP (Simple Mail Transfer Protocol): Η υπηρεσία αυτή υλοποιεί την ανταλλαγή των γνωστών ηλεκτρονικών μηνυμάτων και εξυπηρετεί τη διαδεδομένη Ηλεκτρονική Αλληλογραφία (e-Mail). Ο IIS δε διαχειρίζεται λογαριασμούς χρηστών και η διαδικασία αυτή μπορεί να υλοποιηθεί από τον Microsoft Exchange ή κάποιον άλλον mail server. Η προεπιλεγμένη θύρα για την υπηρεσία αυτή είναι η 25.

- **NNTP (Network News Transport Protocol):** Πρόκειται για ένα πρωτόκολλο που δίνει τη δυνατότητα στον IIS να εξυπηρετεί ομάδες Συζητήσεων (newsgroups). Η υπηρεσία αυτή εξυπηρετείται από τη θύρα 119.
- **Index Server:** Η υπηρεσία αυτή επιτρέπει στους χρήστες να εκτελούν αναζητήσεις με τη χρήση Ευρετηρίων που διαχειρίζεται ο IIS. Ο server μπορεί να δημιουργήσει ευρετήρια για μια πληθώρα αρχείων όπως δυαδικών, HTML, Excel, PowerPoint , Word και απλά αρχεία κειμένου. Επίσης, μπορεί να αυξήσει τη δυνατότητα δημιουργίας ευρετηρίων και για άλλα format με τη χρήση add-ons. Η δημιουργία των ευρετηρίων είναι μη αντιληπτή και εκτελείται στο background.
- **Certificate Server:** Πρόκειται για μια υπηρεσία η οποία διασφαλίζει την ασφάλεια δεδομένων και την ταυτοποίηση χρηστών με τη χρήση Ψηφιακών Πιστοποιητικών. Τα πιστοποιητικά αυτά είναι είτε εσωτερικά ή εξωτερικά και προέρχονται από κάποιο φορέα όπως η VeriSign.
- **Site Server Express:**Χρησιμοποιείται για να παρέχει πληροφορίες για ένα δικτυακό τόπο που εξυπηρετείται από τον IIS. Περιλαμβάνει επίσης ένα γραφικό εργαλείο, τον Content Analyzer, για τον έλεγχο της ορθότητας της δομής του δικτυακού τόπου. Ο Report Writer είναι επίσης ένα εργαλείο που περιλαμβάνεται στον IIS για τη δημιουργία Αναφορών Σύνοψης με τη βοήθεια αρχείων log. Τέλος το εργαλείο Posting Acceptor επιτρέπει τη δημοσίευση περιεχομένου Web από απόσταση.
- **MTS - Microsoft Transaction Server:** Μια συναλλαγή (transaction) είναι μια διαδικασία η οποία αποτελείται από ένα σύνολο ενεργειών. Για να θεωρηθεί ότι μια συναλλαγή έχει ολοκληρωθεί θα πρέπει να έχουν εκτελεστεί όλες οι ενδιάμεσες ενέργειες. Σε αντίθετη περίπτωση ακυρώνονται όλες οι ενέργειες και η συναλλαγή ξεκινάει από την αρχή. Ο IIS πλέον υποστηρίζει την εκτέλεση ομάδας ενεργειών με τη μορφή transaction.

2.2 ΑΠΑΙΤΗΣΕΙΣ SOFTWARE-HARDWARE

Όπως αναφέραμε παραπάνω, ο IIS 5.0 μπορεί να εγκατασταθεί στις εκδόσεις των Windows 2000 Professional και σε μεταγενέστερες. Συνεπώς, στο μηχάνημα στο οποίο θα εγκατασταθεί, θα πρέπει να είναι ήδη εγκατεστημένη μια από τις server

εκδόσεις των Windows όπως είναι τα Windows 2000 Professional ή η έκδοση Microsoft Windows 2000 Professional ή για την έκδοση 5.1 τα Windows XP Professional.

Οι απαιτήσεις υλικού καθορίζονται από τις εκδόσεις των Windows που είναι εγκατεστημένες στον web server. Έτσι θα πρέπει τα χαρακτηριστικά του hardware να διασφαλίζουν την άνετη λειτουργία του server.

Οι ελάχιστες απαιτήσεις σε **hardware για τα *Microsoft Windows 2000 Professional*** περιλαμβάνουν τα εξής:

- Ταχύτητα: τουλάχιστον 133 MHz επεξεργαστή Pentium ή συμβατού με Pentium.
- Μνήμη: RAM 64 MB
- Σκληρός Δίσκος: 2 GB με ελεύθερο χώρο τουλάχιστον 650 MB.
- Λειτουργικό Σύστημα: Windows 2000 Professional.

Στην περίπτωση των ***Windows 2000 Server*** οι απαιτήσεις είναι περισσότερες:

- Ταχύτητα:τουλάχιστον 133 MHz επεξεργαστή Pentium ή συμβατού με Pentium.
- Μνήμη: RAM 256 MB
- Σκληρός Δίσκος: 2 GB με ελεύθερο χώρο τουλάχιστον 1 GB.
- Λειτουργικό Σύστημα: Windows 2000 Server.

Όπως θα δούμε, οι Internet υπηρεσίες που παρέχει ο IIS βασίζονται στο πρωτόκολλο TCP/IP. Συνεπώς το πρωτόκολλο θα πρέπει να είναι εγκατεστημένο και οι ρυθμίσεις του δικτύου, κατάλληλα παραμετροποιημένες.

ΚΕΦΑΛΑΙΟ 3

3.1 ΕΓΚΑΤΑΣΤΑΣΗ & ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ IIS

στα Windows XP Professional

ΒΗΜΑΤΑ ΕΓΚΑΤΑΣΤΑΣΗΣ

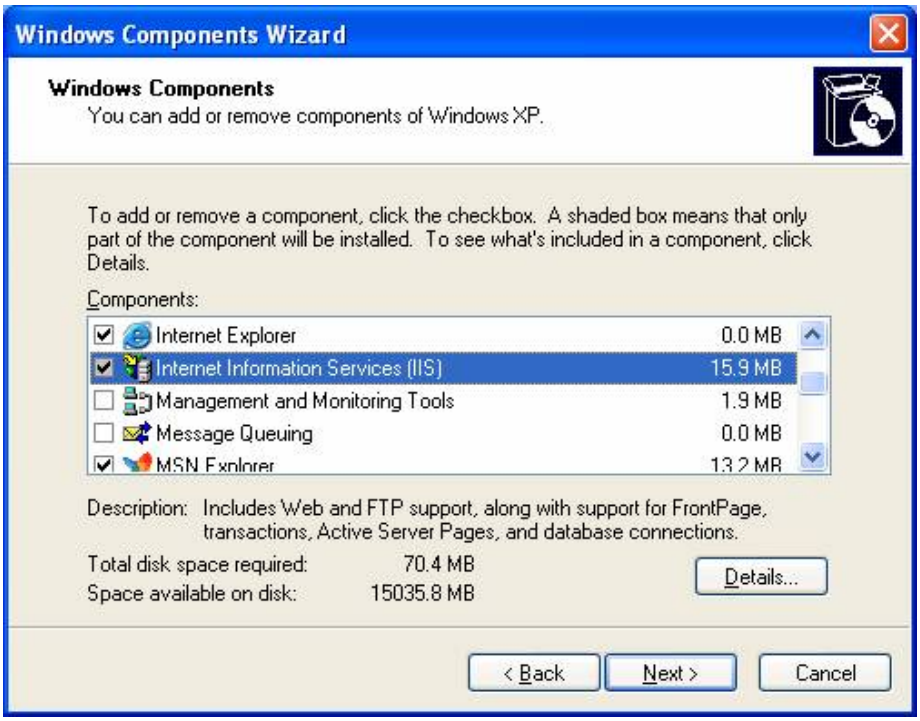
Τα Windows XP Professional κατά την εγκατάστασή τους δεν εγκαθιστούν τον IIS. Η έκδοση του IIS που εγκαθίσταται στα Windows XP Professional είναι η 5.1. Για να την εγκαταστήσουμε χρησιμοποιούμε το CD εγκατάστασης των Windows XP.

Εικόνα 2. Πίνακας Ελέγχου

Στον Πίνακα Ελέγχου και την Προσθαφαίρεση Προγραμμάτων επιλέγουμε την Προσθήκη Στοιχείων των Windows (Add/Remove Windows Components).

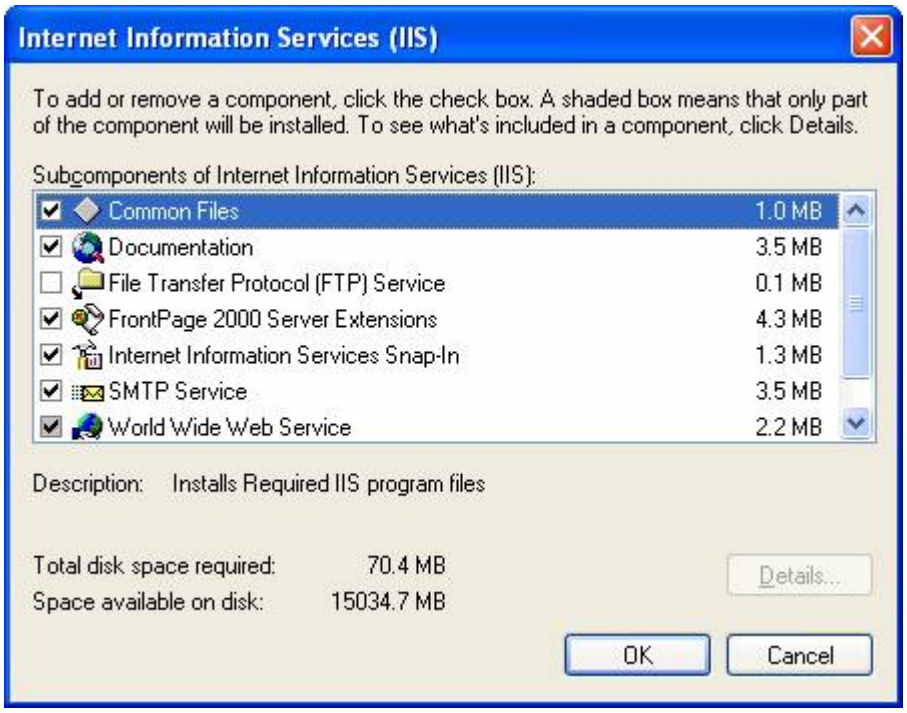
Εικόνα 3. Προσθαφαίρεση Στοιχείων

Ο Οδηγός Προσθήκης Στοιχείων των Windows (Windows Components) θα εμφανισθεί. Επιλέγουμε τον IIS.



Εικόνα 4. Στοιχεία των Windows

Στις λεπτομέρειες του Component (Details) επιλέγουμε τις υπηρεσίες που θα θέλουμε να εξυπηρετούνται από τον IIS όπως SMTP, FTP, WWW και άλλες.



Εικόνα 5. Λεπτομέρειες

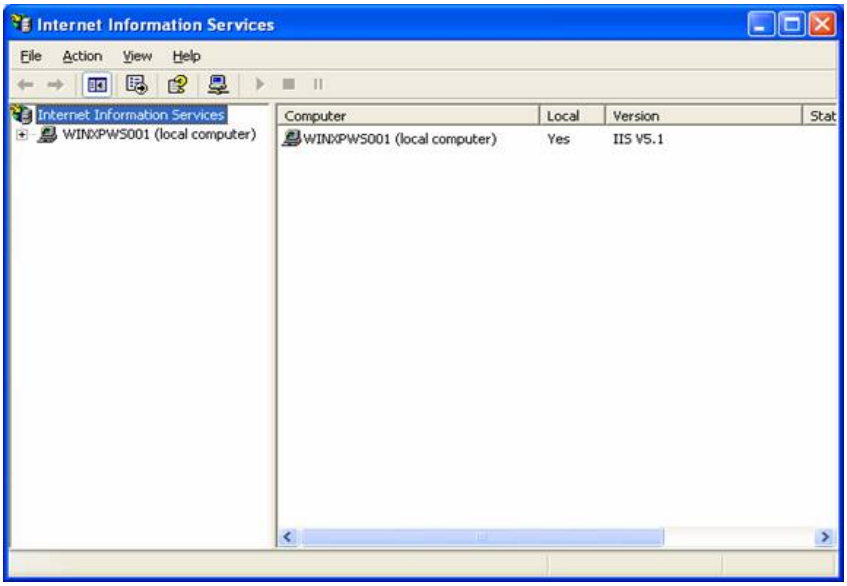
Πατώντας OK και Επόμενο (Next), ο IIS εγκαθίσταται σαν πρόγραμμα στον υπολογιστή – Server. Αφού ολοκληρωθεί η εγκατάστασή του, ο IIS είναι διαθέσιμος μέσα από τα Εργαλεία Διαχείρισης (Administrative Tools) του Πίνακα Ελέγχου (Control Panel).

Το εικονίδιο του IIS φαίνεται στην **Εικόνα 6**. Ανοίγοντας το εικονίδιο αυτό εμφανίζεται η εφαρμογή Διαχείρισης των IIS.

Εικόνα 6. Εικονίδιο στα Εργαλεία Διαχείρισης

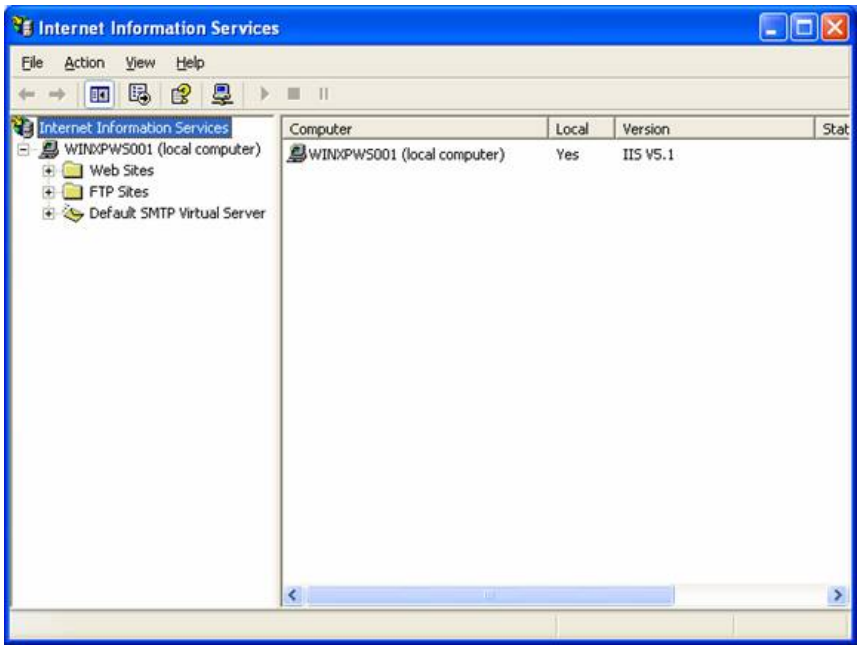
3.2 ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΤΟΥ IIS

Ο IIS, όπως είπαμε, διαχειρίζεται μέσα από ένα στάνταρτ MMC (Microsoft Management Console). Το περιβάλλον διεπαφής είναι παρόμοιο με κάθε άλλο περιβάλλον διαχείρισης ενός συστατικού των Windows XP Professional.



Εικόνα 7. Περιβάλλον Διαχείρισης MMC

Κάνοντας κλικ στο όνομα του υπολογιστή που στη συγκεκριμένη περίπτωση είναι WINXPWS001, θα εμφανιστεί το παρακάτω περιβάλλον όπως φαίνεται στην **Εικόνα 8.**



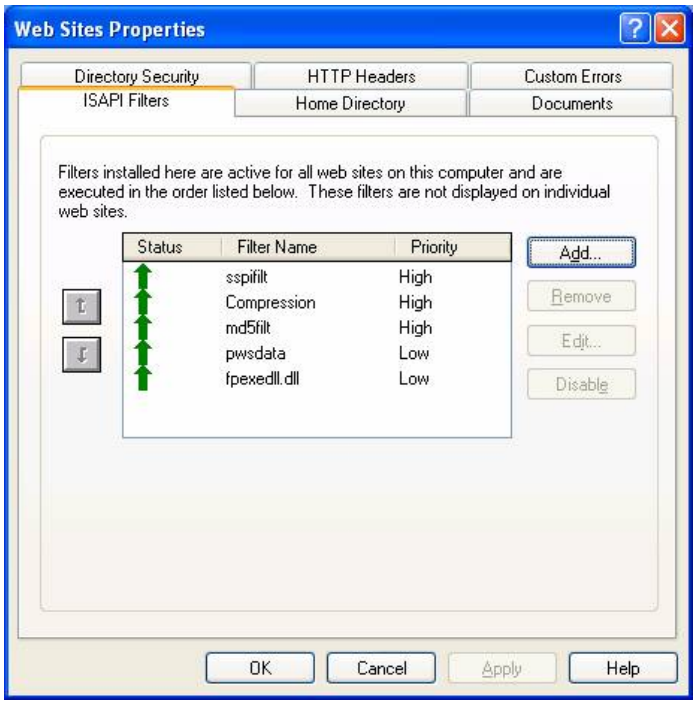
Εικόνα 8. Διαχείριση Τοπικού Server

Όπως φαίνεται μπορούμε να διαχειριστούμε τις υπηρεσίες **Web Sites, FTP Sites και SMTP server.**

3.3 Υπηρεσία Web Site(WWW)

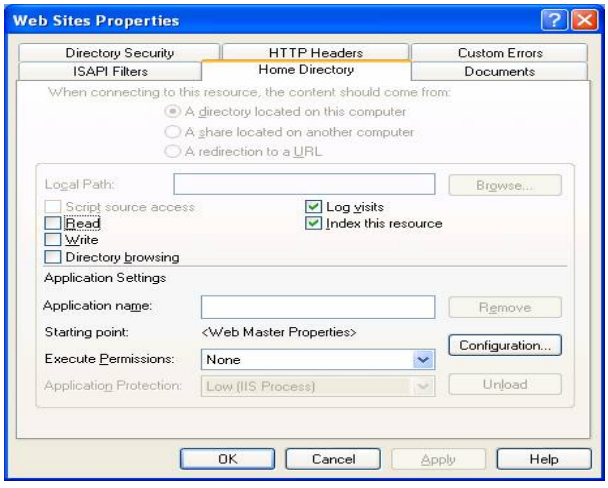
Για να μπορέσουμε να παραμετροποιήσουμε την υπηρεσία WWW, επιλέγουμε τοπικό server και στη συνέχεια τις *Ιδιότητες* (Properties). Οι παραμετροποιήσεις που γίνονται έχοντας επιλέξει τον web server, ισχύουν για όλους τους δικτυακούς τόπους που φιλοξενούνται.

3.3.1 Φίλτρα ISAPI: είναι μια λειτουργία του IIS με βάση την οποία τα έγγραφα πριν διακομιστούν στο Internet περνάνε μέσα από κάποια επεξεργασία. Έτσι για παράδειγμα ένα κείμενο μπορεί να περάσει μέσα από το φίλτρο Συμπίεσης (Compression filter) και να δοθεί συμπιεσμένο. Η σειρά με την οποία εφαρμόζονται τα φίλτρα στα εξυπηρετούμενα έγγραφα μπορεί να αλλάξει όπως και να προστεθούν επιπλέον φίλτρα.



Εικόνα 9. Φίλτρα ISAPI

3.3.2 Home Directory: Η καρτέλα Home Directory όπως φαίνεται και στην **Εικόνα 10**, περιέχει τα προεπιλεγμένα δικαιώματα για τους περιεχόμενους καταλόγους (directories) και επίσης επιτρέπει την παραμετροποίηση των εφαρμογών web.



Εικόνα 10. Home Directory

3.3.3 Δικαιώματα Πρόσβασης (Script Source Access): Η επιλογή Script source access επιτρέπει στους χρήστες να έχουν πρόσβαση στον πηγαίο κώδικα των

ιστοσελίδων. Αν η επιλογή Read είναι επιλεγμένη τότε ο κώδικας μπορεί να αναγνωστεί ενώ αν το Write είναι επιλεγμένο τότε ο κώδικας μπορεί να αλλαχτεί. Οι επιλογές αυτές αφορούν κυρίως τον κώδικα script που είναι εμφωλευμένος μέσα στις ιστοσελίδες και για λόγους ασφαλείας είναι προτιμότερο οι επιλογές αυτές να είναι απενεργοποιημένες εκτός των περιπτώσεων όπου ο κατασκευαστής των ιστοσελίδων που φιλοξενούνται επεξεργάζεται τον κώδικα από απόσταση.

3.3.3.1 Φυλλομέτρηση καταλόγου (Directory Browsing): Η επιλογή Directory Browsing δίνει τη δυνατότητα στους χρήστες να μπορούν να δουν μια λίστα με τους φακέλους και τα περιεχόμενα σε αυτούς αρχεία. Η λίστα αυτή εμφανίζεται πολλές φορές όταν δεν έχει οριστεί κάποια προεπιλεγμένη ιστοσελίδα για να εμφανίζεται κατά την εισαγωγή της διεύθυνσης του δικτυακού τόπου. Για λόγους ασφαλείας η επιλογή αυτή δεν πρέπει να είναι επιλεγμένη. Τέλος, η επιλογή Log visits δίνει τη δυνατότητα στον server να καταγράφει τις επισκέψεις τον αρχείο log.

3.3.3.2 Ρυθμίσεις εφαρμογής (Application Settings): Η επιλογή Application Settings επιτρέπει τη ρύθμιση των παραμέτρων που αφορούν την εφαρμογή (application) Με τον όρο αυτό, εννοούμε όλους τους καταλόγους και τα αρχεία που περιλαμβάνονται μέσα σε κάποιον κατάλογο που αποτελεί το σημείο εκκίνησης του ιστοτόπου.

3.3.3.3 Προστασία εφαρμογής (Application Protection): Η επιλογή Application Protection δίνει τη δυνατότητα στο διαχειριστή να απομονώσει την εκτέλεση μιας web -based εφαρμογής σε μια περιοχή μνήμης ξεχωριστή από την περιοχή μνήμης στην οποία εκτελείται ο IIS και άλλες εφαρμογές. Για μεγαλύτερη ασφάλεια η ρύθμιση αυτή θα πρέπει να είναι καθορισμένη στο Medium ή High και όχι στο Low.

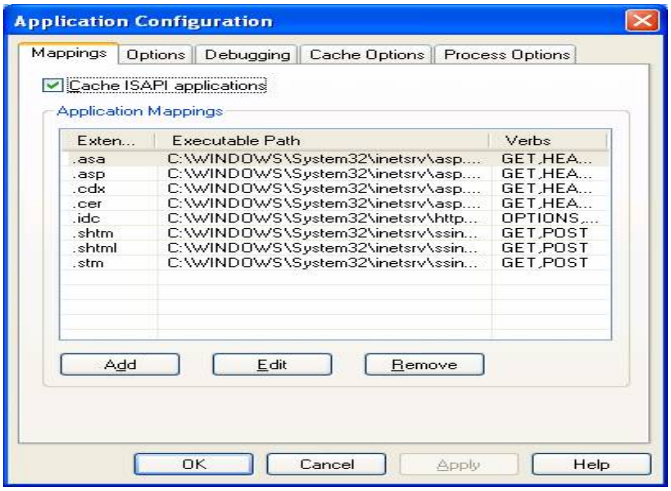
3.3.4 Δικαιώματα Εκτέλεσης (Execute Permission): Οι ρυθμίσεις Execute Permission δίνουν τη δυνατότητα εκτελέσεως προγραμμάτων ή κώδικα script μέσα στον κατάλογο του δικτυακού τόπου.

Οι δυνατές τιμές που μπορεί να έχει είναι οι εξής:

- None: Κανένα πρόγραμμα ή αρχείο script δεν επιτρέπεται να εκτελεστεί.

- Scripts: Επιτρέπει την εκτέλεση μόνο αρχείων script με επέκταση ονόματος που έχει συνδεθεί με κάποιο dll εκτέλεσης από τις ρυθμίσεις που περιγράφουμε παρακάτω (Mapping).
- Scripts and Executables: Επιτρέπει την εκτέλεση οποιουδήποτε εκτελέσιμου κώδικα που περιέχεται είτε σε αρχείο script ή σε binary μορφή όπως .exe και .dll. Η χρήση της επιλογής αυτής θα πρέπει να είναι πολύ προσεκτική γιατί μπορεί να προκαλέσει την εκτέλεση κώδικα από μη εξουσιοδοτημένους χρήστες. Ειδικά στην περίπτωση που στις προηγούμενες ρυθμίσεις έχει αποδοθεί Write permission στους χρήστες του ιστοτόπου, αυτοί θα έχουν τη δυνατότητα δημιουργίας κώδικα ή εκτελέσιμου αρχείου που πιθανώς να έχει επιβλαβείς σκοπούς στον web server.

Ενώ βρισκόμαστε στο παράθυρο Web Site Properties, επιλέγουμε το κουμπί *Configuration,* με αποτέλεσμα να εμφανιστούν οι επιλογές παραμετροποίησης.



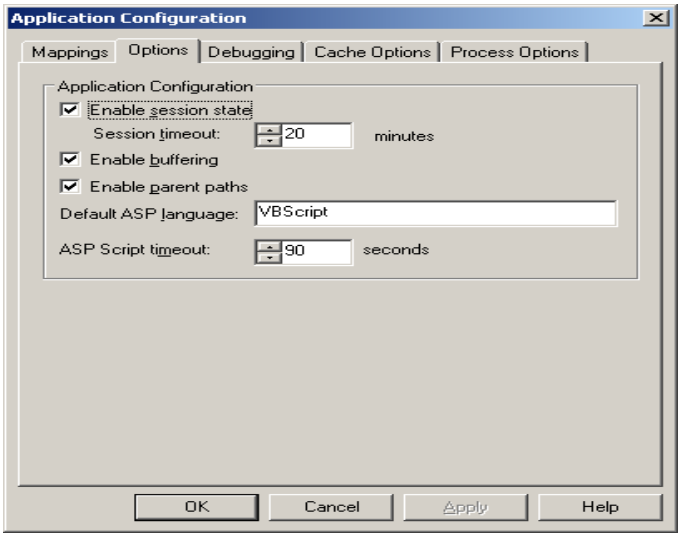
Εικόνα 11. Mapping

Στην καρτέλα **Mappings** προσδιορίζεται η εφαρμογή η οποία εξυπηρετεί τον κάθε τύπο εγγράφου. Έτσι μπορούμε να αντιστοιχίσουμε σε κάθε επέκταση ονόματος κάποιας σελίδας το αντίστοιχο DLL που θα εξυπηρετεί αυτό τον τύπο αρχείου. Για παράδειγμα οι σελίδες ASP (Active Server Pages) εξυπηρετούνται από το asp.dll, το οποίο εκτελεί τις εντολές και τον κώδικα που είναι ενσωματωμένος μέσα στις σελίδες.

Στην καρτέλα **Options** οι επιλογές που υπάρχουν είναι σημαντικές στην περίπτωση εξυπηρέτησης ASP ιστοσελίδων. Η επιλογή Enable session state θα πρέπει

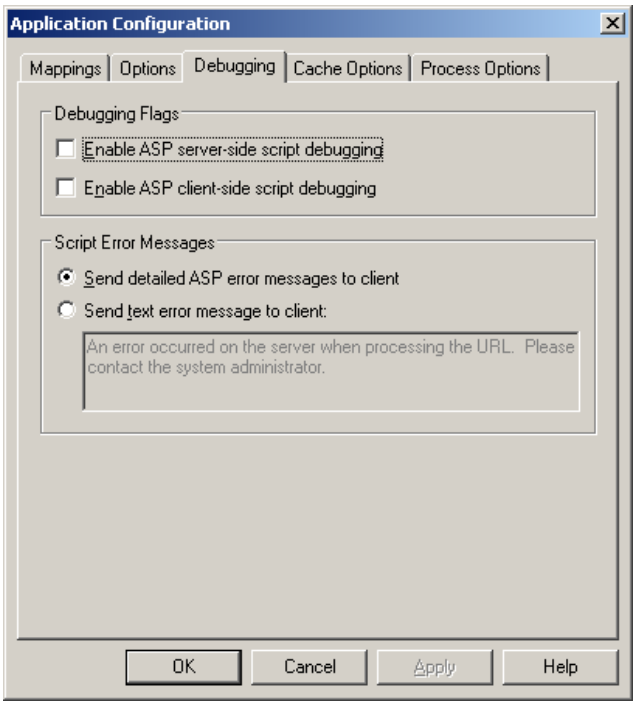
να είναι επιλεγμένη έτσι ώστε να δημιουργείται ένα Session (Σύνοδος) για κάθε χρήστη που συνδέεται με την ASP εφαρμογή. Ένα session μας επιτρέπει να παρακολουθούμε έναν χρήστη όσο αυτός περιηγείται στην εφαρμογή ενώ η επιλογή Session timeout προσδιορίζει σε πόσο χρόνο λήγει η σύνοδος από τη στιγμή που ο χρήστης αυτός δεν ζητάει μια νέα σελίδα ή δεν έχει κάνει ανανέωση της σελίδας. Η επιλογή “ASP Script timeout” επίσης καθορίζει πως αν κάποιο script δεν ολοκληρώθηκε, το γεγονός καταγράφεται στο Server Event Log των Windows και η εκτέλεση του script σταματάει. Οι ρυθμίσεις λήξης χρόνου και εκτέλεσης script είναι για λόγους ασφαλείας προτιμότερο να ενεργοποιούνται.

Επίσης, στις ρυθμίσεις μπορούμε να προσδιορίσουμε την προεπιλεγμένη γλώσσα script για τις ASP σελίδες. Η επιλογή "Enable parent paths" επιτρέπει τη χρήση καταλόγων που είναι γονείς του καταλόγου στον οποίο φιλοξενούνται οι ιστοσελίδες χρησιμοποιώντας τη σύνταξη ".." στον κώδικα των ASP σελίδων.



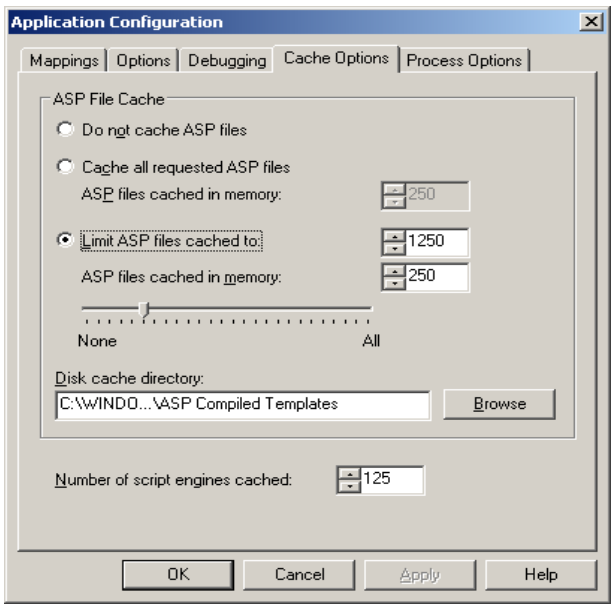
Εικόνα 12. Option

Στην καρτέλα **Debugging** μπορούμε να ενεργοποιήσουμε την επιλογή debugging και διόρθωση σφαλμάτων του κώδικα των ASP σελίδων από τον server ή και από τον client. Επίσης έχουμε τη δυνατότητα επιλογής του είδους του μηνύματος που θα σταλεί στον client σε περίπτωση σφάλματος που θα είναι είτε ένα προεπιλεγμένο μήνυμα λάθους των ASP σελίδων ή κάποιο κείμενο που θα πληκτρολογήσουμε.



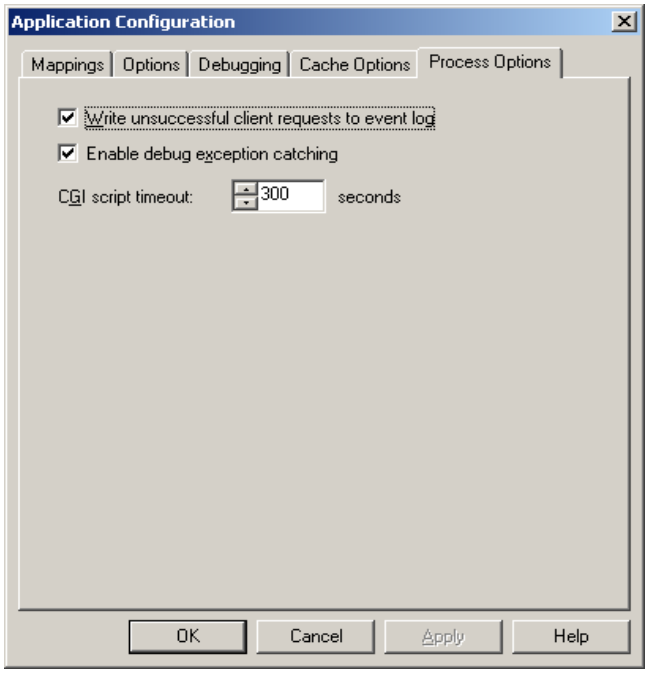
Εικόνα 13. Debugging

Η καρτέλα **Cache Options** μας δίνει τη δυνατότητα να ρυθμίσουμε τον τρόπο προσωρινής αποθήκευσης του περιεχομένου των ASP σελίδων. Οι σελίδες μπορούν να μην αποθηκεύονται καθόλου ή να αποθηκεύονται όλες ή μέχρι κάποιο όριο μνήμης. Επίσης, μπορούμε να προσδιορίσουμε και τη θέση στο δίσκο όπου αυτές οι ιστοσελίδες μπορούν να αποθηκευτούν προσωρινά.



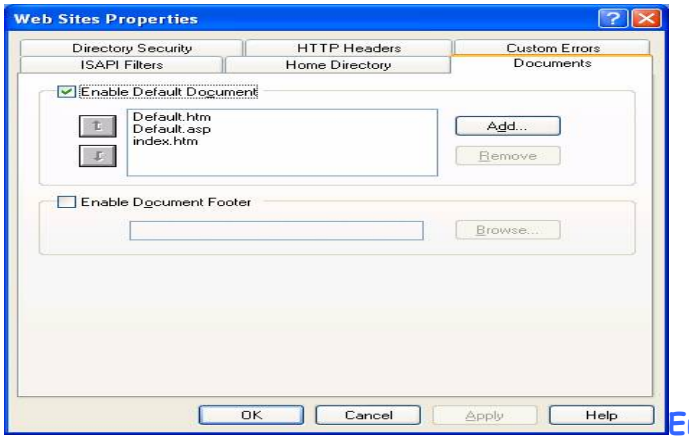
Εικόνα 14. Cache Option

Τέλος, στην καρτέλα **Process Options** μπορούμε να προσδιορίσουμε το αν μη επιτυχημένες κλήσεις από κάποιους clients θα καταγράφονται στο event log του server όπως επίσης και το αν θα γίνεται διαχείριση των τα exceptions. Επίσης προσδιορίζεται και ο χρόνος λήξης εκτέλεσης ενός CGI (Common Gateway Interface).



Εικόνα 15. Process Options

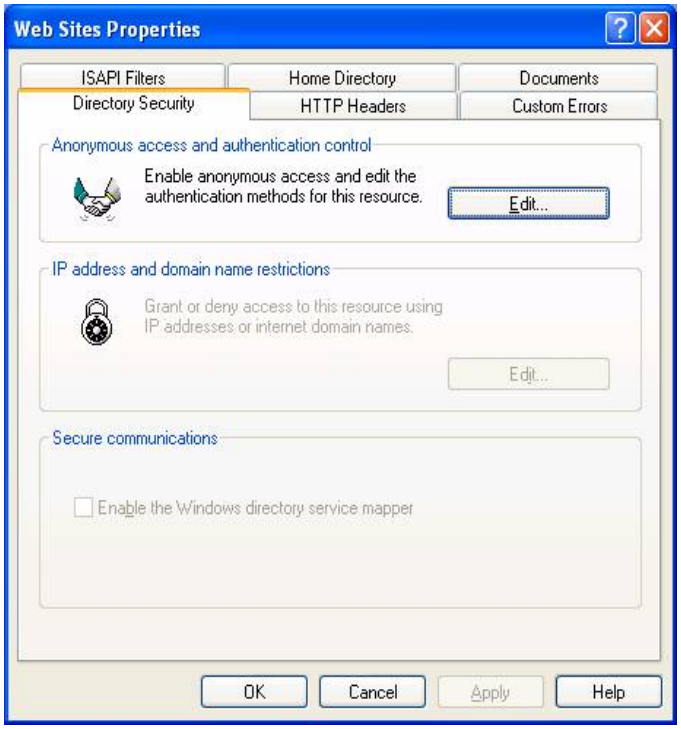
3.3.5 Documents: Στην καρτέλα **Documents** (του παραθύρου Web Site Properties) προσδιορίζονται τα ονόματα των αρχείων ή ιστοσελίδων τα οποία προεπιλεγμένα θα εξυπηρετούνται αν ο χρήστης δεν προσδιορίσει το όνομα της ιστοσελίδας αλλά πληκτρολογήσει μόνο το όνομα περιοχής (domain name) (π.χ. http://www.in.gr) ή μέχρι και τον κατάλογο (http://www.in.gr/weather/).



Εικόνα 16. Documents

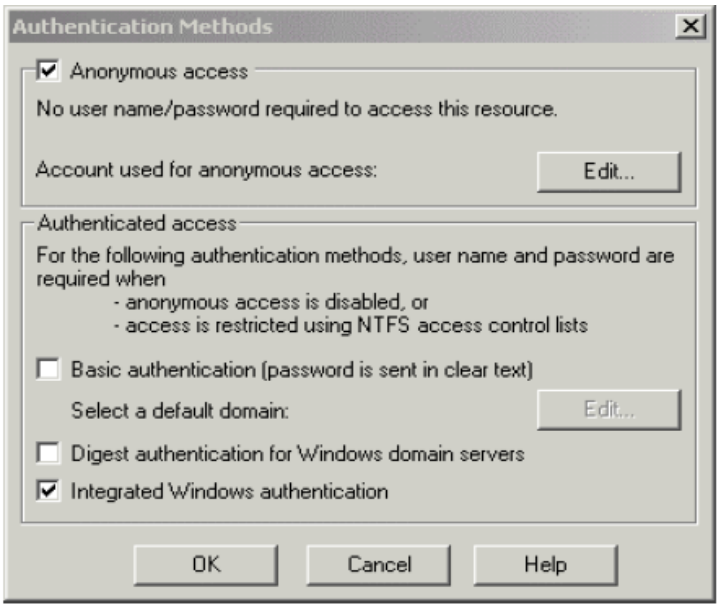
Το πρώτο από τα προεπιλεγμένα αρχεία που θα βρεθεί μέσα στον κατάλογο όπου τα αρχεία του δικτυακού τόπου περιέχονται, είναι αυτό που θα εμφανιστεί, στην περίπτωση που δεν προσδιοριστεί το όνομα της ιστοσελίδας. Η προτεραιότητα των προεπιλεγμένων αρχείων μπορεί να αλλάξει από αυτή την επιλογή. Συνήθως τα ονόματα που είναι προεπιλεγμένα είναι τα *index.asp*, *index.html* ή *default.html*.

3.3.6 Directory Security: Στην καρτέλα **Directory Security (Εικόνα 16)** περιέχονται οι ρυθμίσεις ασφαλείας για όλους τους καταλόγους δικτυακών τόπων που εξυπηρετεί ο IIS.



Εικόνα 17. Directory Security

Η επιλογή *Anonymous Access and Authentication Control* αφορά στον τρόπο με τον οποίο ένας χρήστης συνδέεται στον server και αποκτά πρόσβαση στο web περιεχόμενο. Με την επιλογή *Edit* εμφανίζεται το παράθυρο της **Εικόνας 18** όπου επιλέγεται ο τρόπος πρόσβασης.



Εικόνα 18. Μέθοδοι Ταυτοποίησης

3.3.7 Μέθοδος Anonymous Access: Ο πιο συνηθισμένος τρόπος πρόσβασης του Web Server είναι με την επιλογή Anonymous Access. Ο IIS Web Server δημιουργεί προεπιλεγμένα έναν λογαριασμό στον server, ο οποίος έχει όνομα IUSR_όνομαΥπολογιστή και IWAM_όνομαΥπολογιστή. Ο λογαριασμός αυτός έχει σαν δικαιώματα τοπικού logon (log on locally), πρόσβαση από το Δίκτυο (access this computer from the network) και Logon σαν batch διαδικασία (log on as a batch job). Κάθε φορά που κάποιος επισκέπτης του δικτυακού τόπου επισκέπτεται τον server για να ανακτήσει το περιεχόμενο του ιστοτόπου, κάνει αυτόματα loggon χρησιμοποιώντας αυτό το λογαριασμό. Τα δικαιώματα του λογαριασμού αυτού καθορίζουν το τι μπορεί να κάνει ο επισκέπτης. Τα δικαιώματα του συγκεκριμένου λογαριασμού μπορούν να παραμετροποιηθούν από την επιλογή *Edit.*

3.3.8 Μέθοδος Basic Authentication: Εκτός από την παραπάνω μέθοδο πρόσβασης, όλοι σχεδόν οι Web browsers υποστηρίζουν και τη μέθοδο Βασικής Ταυτοποίησης (Basic authentication). Με αυτή τη μέθοδο ο επισκέπτης θα πρέπει να εισάγει κάποιο όνομα και κωδικό χρήστη για να αποκτήσει πρόσβαση στο web περιεχόμενο. Οι πληροφορίες αυτές στέλνονται από το χρήστη προς τον server σε μορφή απλού κείμενου με αποτέλεσμα να μπορούν οι πληροφορίες αυτές να υποκλαπούν από κάποιο τρίτο που παρακολουθεί τη σύνδεση. Γι αυτό το λόγο η Βασική ταυτοποίηση θα πρέπει να χρησιμοποιείται σε συνδυασμό με το πρωτόκολλο SSL. Το πρωτόκολλο που περιγράφουμε στη συνέχεια επιτρέπει την ασφαλή μετάδοση εμπιστευτικών δεδομένων όπως είναι το Όνομα Χρήστη και ο Κωδικός Χρήστη.

Η εγκατάσταση Ταυτοποίησης με τη χρήση SSL ακολουθεί τα παρακάτω βήματα:

- **Απόκτηση ενός Server Certificate.**
- **Χρήση ενός ασφαλούς καναλιού κατά την πρόσβαση στο περιεχόμενο.**
- **Ενεργοποίηση της Βασικής Ταυτοποίησης και απενεργοποίηση των μεθόδων Ταυτοποίησης Anonymous και Intergrated Windows.**

3.3.9 Μέθοδος Digest Authentication For Windows Domain Servers: Η επιλογή αυτή προσφέρει τις ίδιες υπηρεσίες με την επιλογή Basic Authentication με τη διαφορά ότι χρησιμοποιεί μια διαφορετική μέθοδο αποστολής των πιστοποιητικών ταυτοποίησης.
Η διαδικασία είναι η εξής:

Ο server στέλνει κάποιες πληροφορίες στον client, ο οποίος συνδυάζοντας τες με το όνομα και κωδικό χρήστη καθώς επίσης και με κάποια data θα δημιουργήσει ένα hash κλειδί. Το κλειδί hash στέλνεται στον server συνοδευμένο από τα data σε μορφή απλού κειμένου. Ο server θα παραλάβει τα data και χρησιμοποιώντας το όνομα και κωδικό χρήστη θα δημιουργήσει ένα δικό του κλειδί hash. Αν τα δύο κλειδιά hash ταιριάζουν τότε σημαίνει ότι η ταυτοποίηση του χρήστη είναι επιτυχής.

Η ενεργοποίηση της επιλογή *Digest authentication* και η απενεργοποίηση των άλλων μεθόδων για να μπορέσει να λειτουργήσει απαιτεί την αποθήκευση των λογαριασμών χρηστών σε κρυπτογραφημένη μορφή σε συνδυασμό με την ενεργοποίηση της αντίστοιχης πολιτικής ασφαλείας στα Windows (Windows 2000 group policy : Computer Configuration->Windows Settings->Security Settings->Account Policies->Password Policy, “Store Passwords using reversible encryption for all users in the domain””).

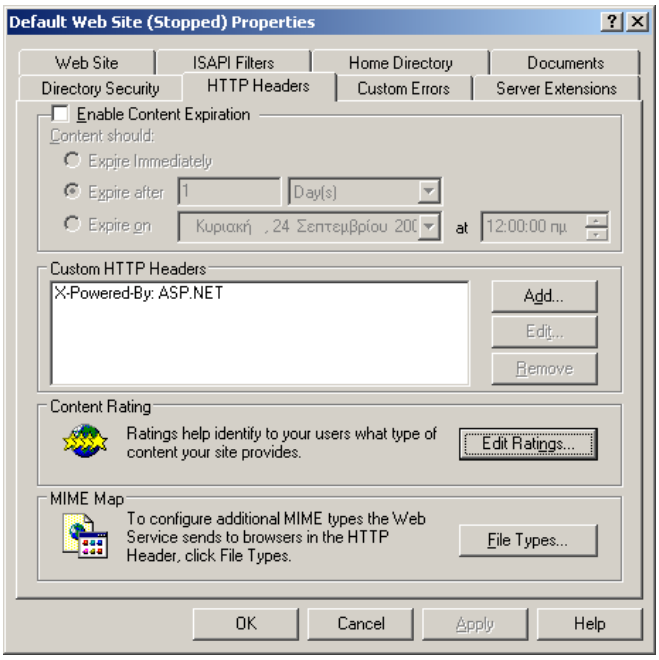
Παρά το γεγονός ότι η μέθοδος ασφαλούς ταυτοποίησης του χρήστη που συνδέεται με τον server για την ανάκτηση web περιεχομένου, δεν είναι η πιο ασφαλής, είναι σίγουρα πιο ασφαλής από τις απλούστερες μορφές ταυτοποίησης όπως η *Basic Authentication.*

3.3.10 Μέθοδος Intergrated Windows Authentication: Η επιλογή αυτή λεγόταν NTLM ή Windows NT Challenge/Response στις παλαιότερες εκδόσεις του IIS. Πρόκειται για μια μέθοδο ταυτοποίησης χρηστών οι οποίοι δεν επιθυμούν να εισάγουν το Όνομα και Κωδικό χρήστη σε μορφή απλού κειμένου και να το υποβάλλουν στο δίκτυο. Μια τεχνική κρυπτογράφησης που χρησιμοποιεί αλγόριθμο hash χρησιμοποιείται για τον

έλεγχο του κωδικού χρήστη. Το πραγματικό όνομα και ο κωδικός χρήστη δεν στέλνονται ποτέ μέσω του δικτύου αλλά στη θέση τους στέλνονται τα αντίστοιχα hash κλειδιά. Το πρωτόκολλο που χρησιμοποιείται μπορεί να είναι είτε το Kerberos v5 ή το πρωτόκολλο challenge / response. Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί μόνο αν ο χρήστης χρησιμοποιεί σαν web browser τον MS Internet Explorer.

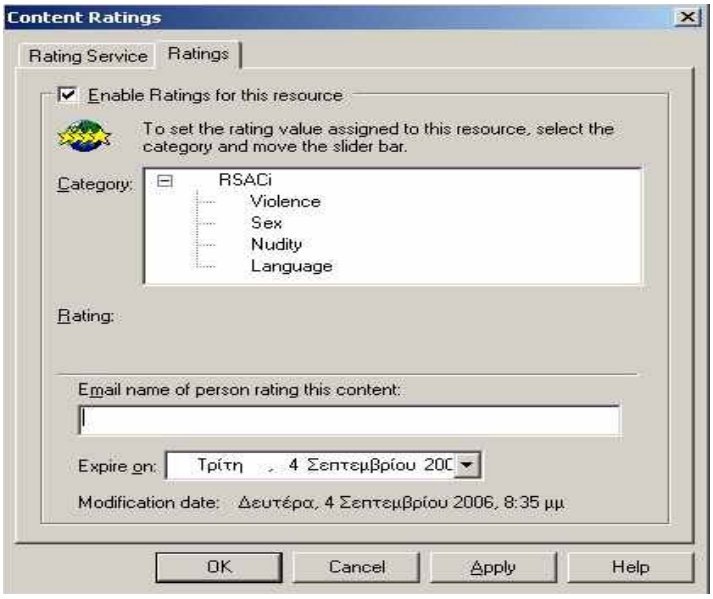
Ο IIS μπορεί να παραμετροποιηθεί έτσι ώστε να επιτρέπει το συνδυασμό όλων των μεθόδων ταυτοποίησης στον επισκέπτη στην προσπάθειά του να συνδεθεί με τον server. Για παράδειγμα, ο χρήστης μπορεί να επιχειρήσει να συνδεθεί με τον χρήστη χρησιμοποιώντας τη μέθοδο anonymous access. Ο χρήστης συνδέεται σε αυτή την περίπτωση με τη χρήση του λογαριασμού IUSR_όνομαΥπολογιστή. Αν η μέθοδος αυτή αποτύχει λόγω των δικαιωμάτων και της πολιτικής ασφαλείας του server, ο server στέλνει μια απάντηση στον web browser του χρήστη ειδοποιώντας τον ότι δεν έχει δικαίωμα πρόσβασης στον server. Επίσης στον client αποστέλλονται και όλες οι δυνατές μέθοδοι ταυτοποίησης που υποστηρίζονται από τον server. Ο web browser εμφανίζει στο χρήστη μια φόρμα εισαγωγής ονόματος και κωδικού χρήστη. Στη συνέχεια, αφού αυτά εισαχθούν, ο browser αναζητεί μια μέθοδο ταυτοποίησης που υποστηρίζεται και αποστέλλει στο server εκ νέου την αίτηση για ανάκτηση του περιεχομένου συνοδευμένη όμως από το όνομα και κωδικό χρήστη καθώς και τη μέθοδο ταυτοποίησης που έχει επιλεγεί. Χρησιμοποιώντας μια από τις δύο άλλες μεθόδους γίνεται η ταυτοποίηση του χρήστη.

3.3.11 HTTP Headers: Η καρτέλα **HTTP** Headers περιέχει της πληροφορίες επικεφαλίδας που στέλνονται από τον server προς τον web browser. Στο σημείο αυτό μπορούμε να προσδιορίσουμε τις παραμέτρους ημερομηνίας λήξης του περιεχομένου που στάλθηκε έτσι ώστε ανάλογα με τις ρυθμίσεις οι browsers των υπολογιστών-Πελατών να ξαναζητούν εκ νέου την αποστολή από τον server των ιστοσελίδων που έχουν λήξει. Από τη συγκεκριμένη καρτέλα μπορούν να προστεθούν επιπλέον πληροφορίες επικεφαλίδας. Έτσι μπορούν να προστεθούν ειδικοί τύποι επικεφαλίδων καθώς και πληροφορίες επικεφαλίδων ειδικών αρχείων MIME.



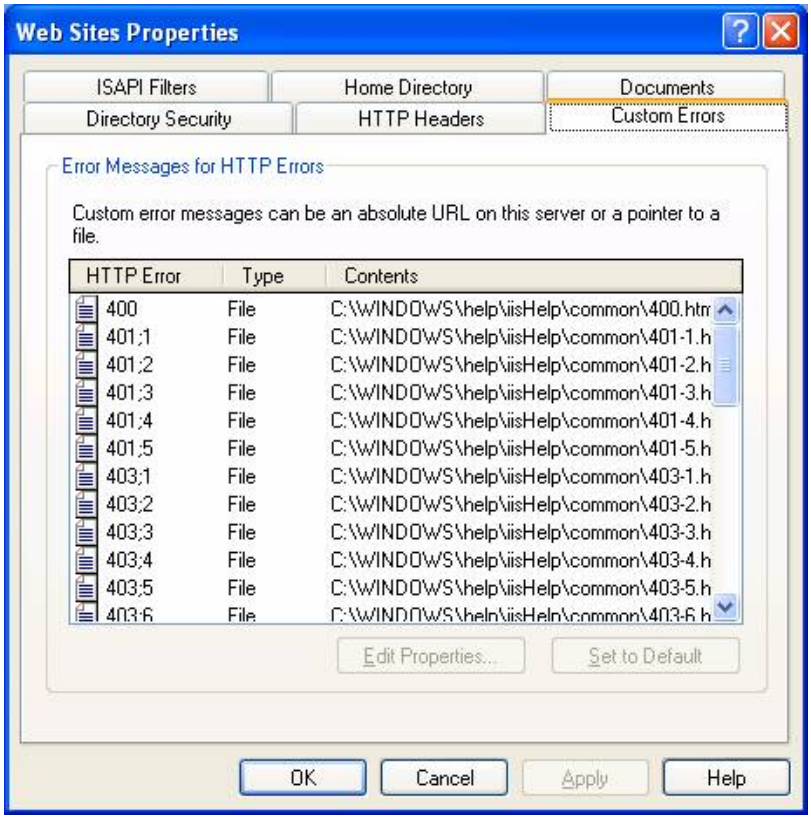
Εικόνα 19. HTTPS Headers

Επίσης, μπορεί να προσδιοριστεί το είδος του περιεχομένου που στέλνεται στον browser χρησιμοποιώντας την επικεφαλίδα για να μεταφέρει τη διαβάθμιση των πληροφοριών (Rating). Έτσι στην επιλογή Content Rating και στο αντίστοιχο παράθυρο μπορούμε να προσδιορίσουμε το είδος του περιεχομένου όπως φαίνεται και στην **Εικόνα 20.**



Εικόνα 20. Rating

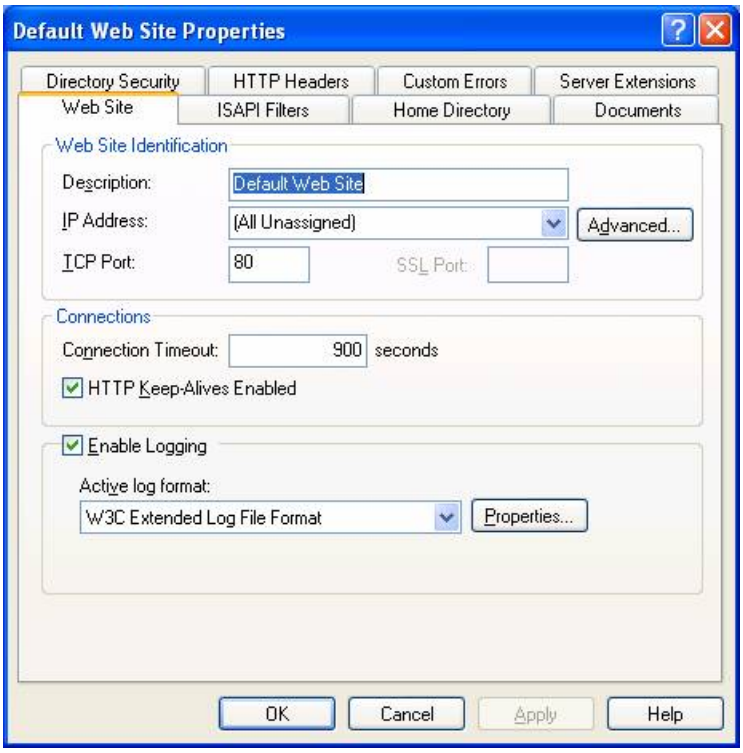
3.3.12 Custom Errors: Τέλος, η επιλογή Custom Errors μας δίνει τη δυνατότητα να αντιστοιχίσουμε σε κάθε HTTP σφάλμα που μπορεί να προκύψει, το αντίστοιχο μήνυμα σφάλματος με τη μορφή αρχείου. Συνήθως το αρχείο που εμφανίζεται στην οθόνη τους browser για να παρουσιάσει το σφάλμα είναι μια HTML σελίδα.



Εικόνα 21. Custom Errors

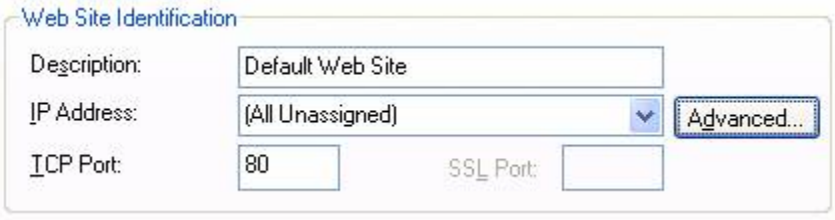
3.3.13 ΡΥΘΜΙΣΕΙΣ ΣΥΓΚΕΚΡΙΜΕΝΟΥ ΔΙΚΤΥΑΚΟΥ ΤΟΠΟΥ: Οι ρυθμίσεις που έχουμε περιγράψει μέχρι τώρα αφορούν όλους τους καταλόγους δικτυακών τόπων που φιλοξενούνται από τον IIS. Όπως είπαμε νωρίτερα υπάρχει η δυνατότητα ο IIS να εξυπηρετεί περισσότερους από έναν δικτυακούς τόπους. Οι ρυθμίσεις που περιγράψαμε θα αποτελούν τις προεπιλογές για κάθε δικτυακό τόπο. Παρ' όλα αυτά μπορούμε να παραμετροποιήσουμε τους επιμέρους δικτυακούς τόπους, ρυθμίζοντας τις ιδιότητες για κάθε έναν από αυτούς.

Επιλέγοντας έναν από τους δικτυακούς τόπους(καρτέλα **Web Site**) επιλέγουμε τις *Ιδιότητες* του.



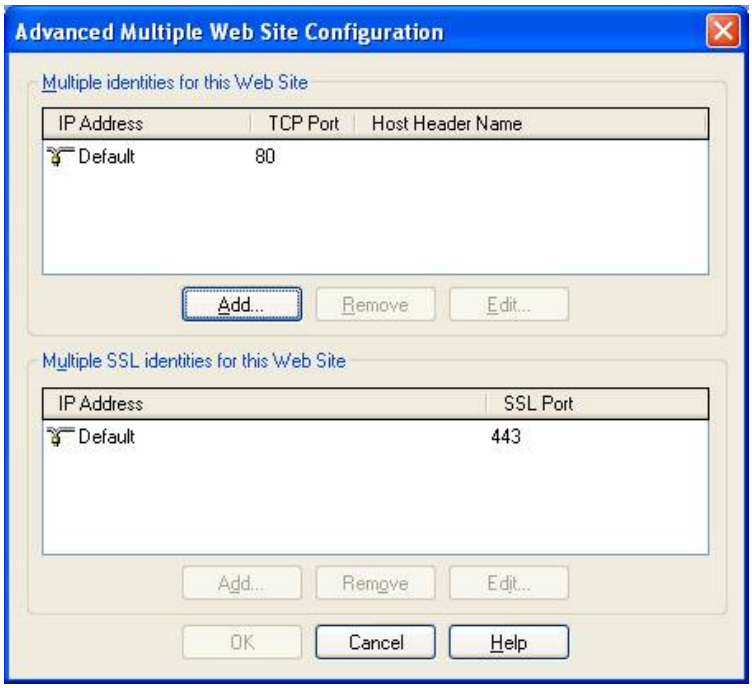
Εικόνα 22. Web Site

Πολλές από τις ρυθμίσεις είναι κοινές με αυτές που παραμετροποιούνται για όλους τους δικτυακούς τόπους. Οι αλλαγές που έγιναν στην προηγούμενη παραμετροποίηση εμφανίζονται σαν προεπιλεγμένες τιμές στις τρέχουσες ρυθμίσεις. Η καρτέλα **Web Site** μας δίνει τη δυνατότητα να προσδιορίσουμε την ταυτότητα του δικτυακού μας τόπου. Στο πεδίο *Description* εισάγουμε την περιγραφή του ενώ στο πεδίο *IP Address* προσδιορίζουμε τη διεύθυνση η οποία θα εξυπηρετεί το συγκεκριμένο δικτυακό τόπο στην περίπτωση που ο IIS server φιλοξενεί πολλούς ιστότοπους. Επίσης, προσδιορίζεται και η θύρα εξυπηρέτησης που όπως γνωρίζουμε είναι προεπιλεγμένα η 80.



Εικόνα 23. Identification

Με την επιλογή *Advanced* και ανοίγοντας το αντίστοιχο παράθυρο μπορούμε να προσδιορίσουμε παραπάνω από μια IP διεύθυνση που θα εξυπηρετεί τον ίδιο δικτυακό τόπο.



Εικόνα 24. IP Διεύθυνση

Πατώντας την επιλογή *Add* προσθέτουμε *μια νέα IP Address*. Επίσης από το ίδιο παράθυρο μπορούμε να προσθέσουμε μια νέα καταχώρηση για την ίδια IP Address αλλά με διαφορετικό όνομα Host Header Name. Η δυνατότητα αυτή μας επιτρέπει για τον ίδιο δικτυακό τόπο ο χρήστης να μπορεί να εισάγει περισσότερα από ένα ονόματα περιοχής.

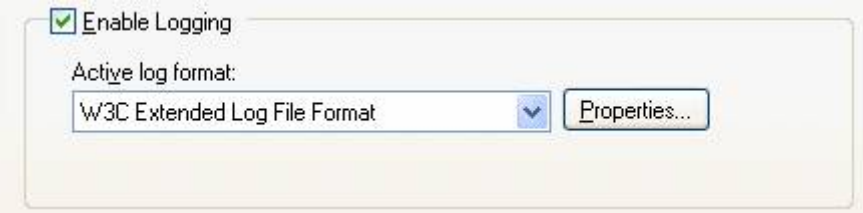
Εικόνα 25. Ρυθμίσεις Διεύθυνσης

Έτσι στο παράδειγμα της **Εικόνας 25** αν προστεθεί και μια ακόμα καταχώρηση με Host Header Name το www.yoursite.com, τότε οι χρήστες θα μπορούν να συνδεθούν χρησιμοποιώντας το νέο όνομα με τον ίδιο δικτυακό τόπο.

Επιστρέφοντας στο αρχικό παράθυρο μπορούμε να προσδιορίσουμε *το μέγιστο χρόνο* που μπορεί κάποιος χρήστης να είναι συνδεδεμένος με τον ιστότοπο.

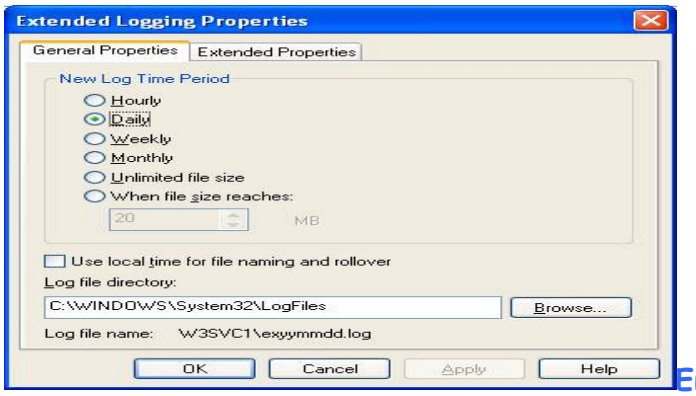
Εικόνα 26. Connections

Επίσης, μπορούμε να παραμετροποιήσουμε τις πληροφορίες που θα καταγράφει ο IIS για τους χρήστες που συνδέονται στον δικτυακό τόπο. Οι πληροφορίες αυτές καταγράφονται σε ένα log αρχείο στο δίσκο.



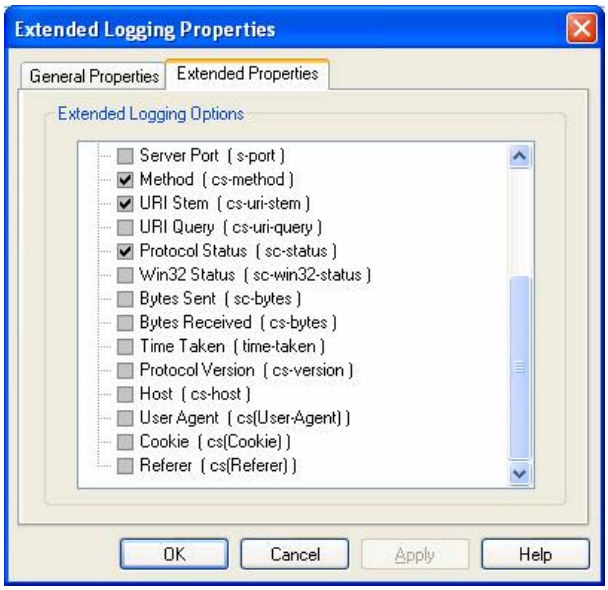
Εικόνα 27. Logging

Επιλέγοντας το κουμπί *Properties* και την καρτέλα **General Properties**, μπορούμε να ρυθμίσουμε τη συχνότητα με την οποία δημιουργείται ένα νέο log αρχείο και την τοποθεσία στο δίσκο όπου αποθηκεύεται. Για λόγους ασφαλείας μια καλή πρακτική είναι να αποθηκεύονται τα log αρχεία σε κάποιο δίσκο εκτός αυτού, που φιλοξενεί το δικτυακό τόπο.



Εικόνα 28. Ρυθμίσεις Logging

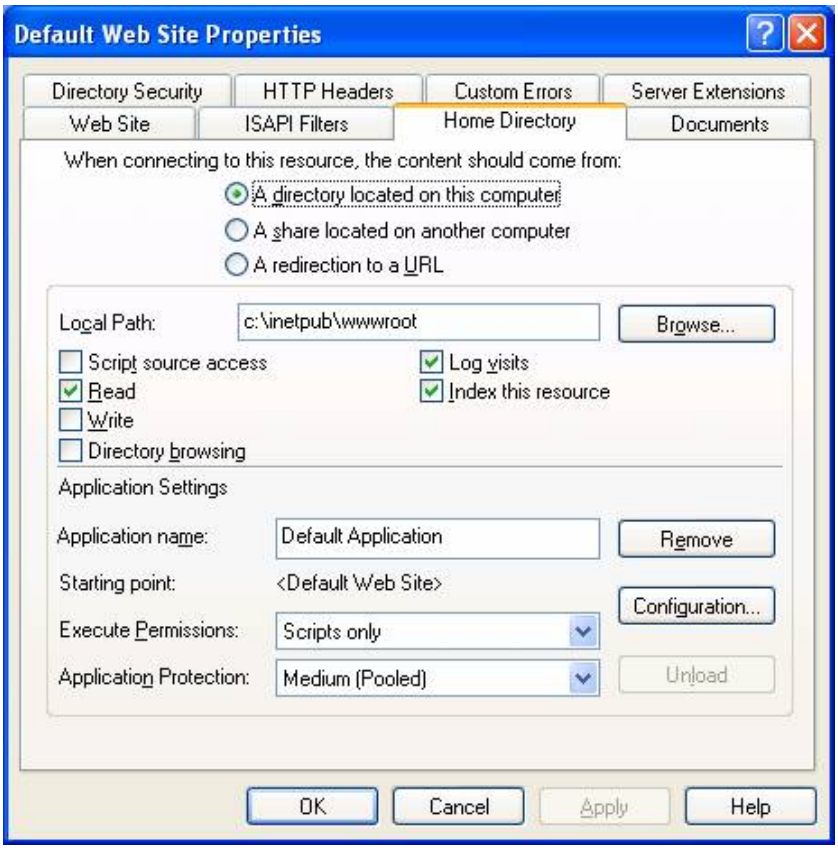
Επίσης, από την καρτέλα **Extended Properties,** (του παραθύρου Extended Logging Properties) επιλέγουμε τις πληροφορίες εκείνες οι οποίες θέλουμε να καταγράφονται σχετικά με τις επισκέψεις προς τον δικτυακό μας τόπο όπως φαίνεται και στην **Εικόνα.29**



Εικόνα 29.Προχωρημένες Ρυθμίσεις Logging

Επιστρέφοντας στις αρχικό παράθυρο ρυθμίσεων, η καρτέλα με τα *φίλτρα ISAPI* περιέχει τις προεπιλεγμένες τιμές που έχουμε δώσει νωρίτερα. Η λειτουργικότητα των ρυθμίσεων είναι αυτή που περιγράψαμε νωρίτερα και χρησιμοποιούμε την επιλογή σε περίπτωση που πρέπει να παραμετροποιήσουμε το συγκεκριμένο δικτυακό τόπο διαφορετικά από τις προεπιλεγμένες ρυθμίσεις.

3.3.14 Home Directory: Στην καρτέλα **Home Directory** μπορούμε να ρυθμίσουμε εκτός από τις παραμέτρους που ήδη περιγράψαμε για τον συγκεκριμένο δικτυακό τόπο, μπορούμε να ρυθμίσουμε την προέλευση από την οποία θα αποστέλλεται το περιεχόμενο στον browser του client. Έτσι συνήθως το περιεχόμενο του δικτυακού τόπου είναι αποθηκευμένο σε κάποια θέση του δίσκου του server υπολογιστή όπως επίσης μπορεί να είναι αποθηκευμένο σε κάποια κοινόχρηστη τοποθεσία ενός υπολογιστή που είναι συνδεδεμένος μέσω δικτύου με τον web server υπολογιστή.



Εικόνα 30. Home Directory

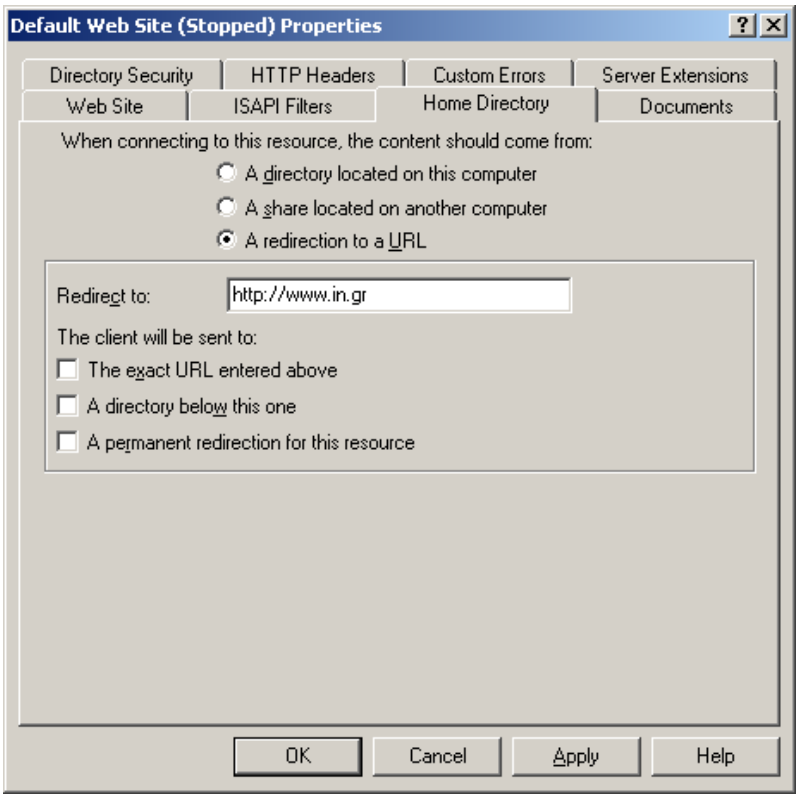
Και στις δύο αυτές περιπτώσεις η τοποθεσία προσδιορίζεται από το πεδίο Local Path κάτω από τις επιλογές προέλευσης του περιεχομένου. Στην **Εικόνα 30** βλέπουμε ότι ο δικτυακός τόπος είναι αποθηκευμένος στον τοπικό φάκελο inetpub\wwwroot στο δίσκο C.

Μια καλή πρακτική για περισσότερη ασφάλεια είναι να αλλάζουμε την τοποθεσία όπου αποθηκεύουμε το δικτυακό μας τόπο και να μην τον αποθηκεύουμε στην προεπιλεγμένη θέση inetpub\wwwroot αφού οι επίδοξοι hackers στην περίπτωση που επιχειρήσουν να αλλοιώσουν το περιεχόμενο του δικτυακού μας τόπου, θα επιχειρήσουν να εισβάλλουν στον συγκεκριμένο προεπιλεγμένο κατάλογο.

Με την τρίτη επιλογή προέλευσης *(Redirection),* θα μπορούσαμε να προσδιορίσουμε το URL (Unified Resource Location) ενός άλλου δικτυακού τόπου του Internet με αποτέλεσμα όταν κάποιος επισκέπτης συνδέεται με τον δικό μας δικτυακό τόπο, να ανακατευθύνεται η σύνδεσή του προς τον άλλο ιστότοπο.

Έτσι, στην περίπτωση που θα θέλαμε αντί του δικού μας δικτυακού τόπου να εμφανίζεται κάποιος τρίτος στον browser του επισκέπτη, θα επιλέγαμε την τρίτη επιλογή

και θα εισάγαμε το URL του άλλου ιστοτόπου, π.χ του www.in.gr, όπως φαίνεται και στην **Εικόνα 31**.

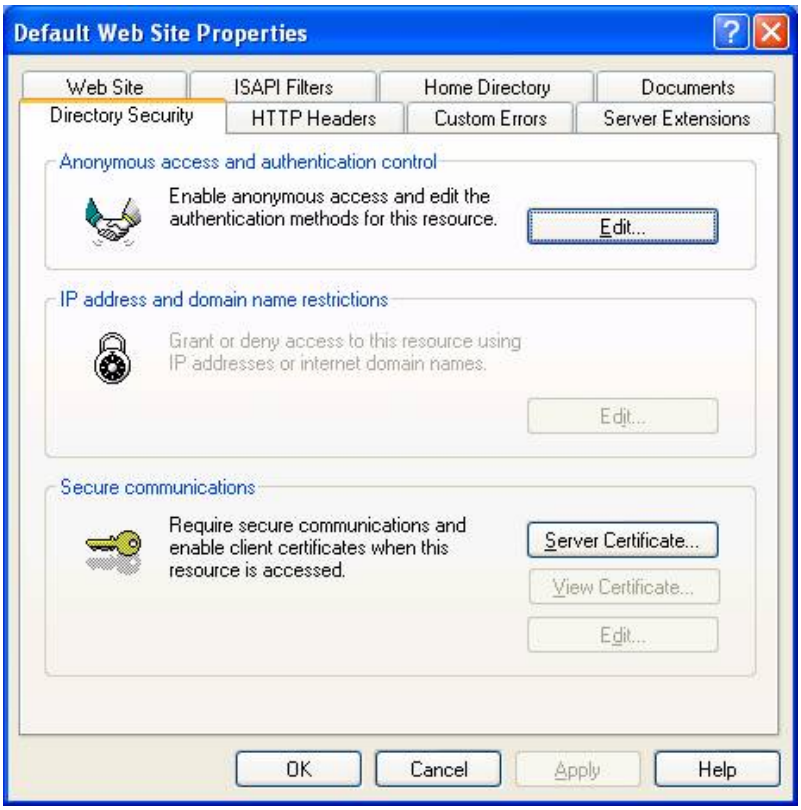


Εικόνα 31. Redirection

Οι επιλογές στο τμήμα *Application Settings* προσφέρουν την ίδια λειτουργικότητα με αυτή που περιγράφτηκε και νωρίτερα. Το ίδιο ισχύει και για την περίπτωση των ρυθμίσεων στην καρτέλα **Documents** όπου προσδιορίζονται για τον συγκεκριμένο ιστότοπο τα προεπιλεγμένα αρχεία που αποστέλλονται στον browser του client σε περίπτωση που δεν προσδιοριστεί το όνομα της σελίδας παρά μόνο το όνομα τομέα και ο φάκελος.

Ομοίως, η καρτέλα **HTTP Headers** προσδιορίζει το περιεχόμενο των επικεφαλίδων του περιεχομένου που αποστέλλει ο server στην περίπτωση επίσκεψης στο συγκεκριμένο ιστότοπο και ισχύουν οι ρυθμίσεις που προαναφέραμε. Τέλος, η καρτέλα **Custom Errors** προσδιορίζει με τον ίδιο τρόπο που περιγράφτηκε νωρίτερα τα μηνύματα σφαλμάτων που θα εμφανίζει ο συγκεκριμένος ιστότοπος σε περίπτωση σφάλματος.

3.3.15 Directory Security: Η καρτέλα **Directory Security** περιλαμβάνει τις ρυθμίσεις που έχουμε ήδη δει όσον αφορά την πρόσβαση των χρηστών στον server. Το τμήμα *Anonymous access* and Authentication Control μας δίνει τη δυνατότητα να επιλέξουμε τη μέθοδο με την οποία θα γίνεται η ταυτοποίηση του χρήστη πριν αυτός αποκτήσει πρόσβαση στο περιεχόμενο του δικτυακού τόπου, όπως φαίνεται και στην **Εικόνα 32** και περιγράφτηκε στην παράγραφο σχετικά με τις ιδιότητες όλων των δικτυακών τόπων.

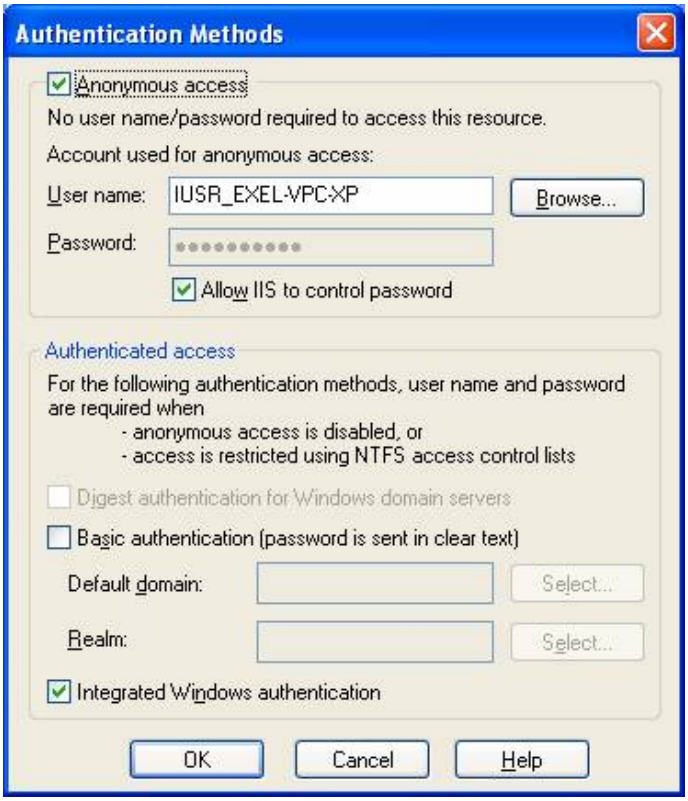


Εικόνα 32. Directory Security

Επίσης, η καρτέλα περιλαμβάνει το τμήμα IP address and domain name restrictions όπου δίνεται η δυνατότητα στον διαχειριστή του δικτυακού τόπου να δημιουργήσει μια λίστα διευθύνσεων ή ονομάτων domain τα οποία μπορούν να έχουν μόνο αυτοί πρόσβαση στον server ή αντίθετα να αποκλειστούν από τη δυνατότητα να συνδέονται με τον server.

Τέλος, υπάρχει και το τμήμα Secure Communications το οποίο αναφέρεται στη δυνατότητα απόκτησης και εγκατάστασης ψηφιακού πιστοποιητικού για την ασφαλή σύνδεση των χρηστών με τον web server. Η διαδικασία εγκατάστασης ενός ψηφιακού

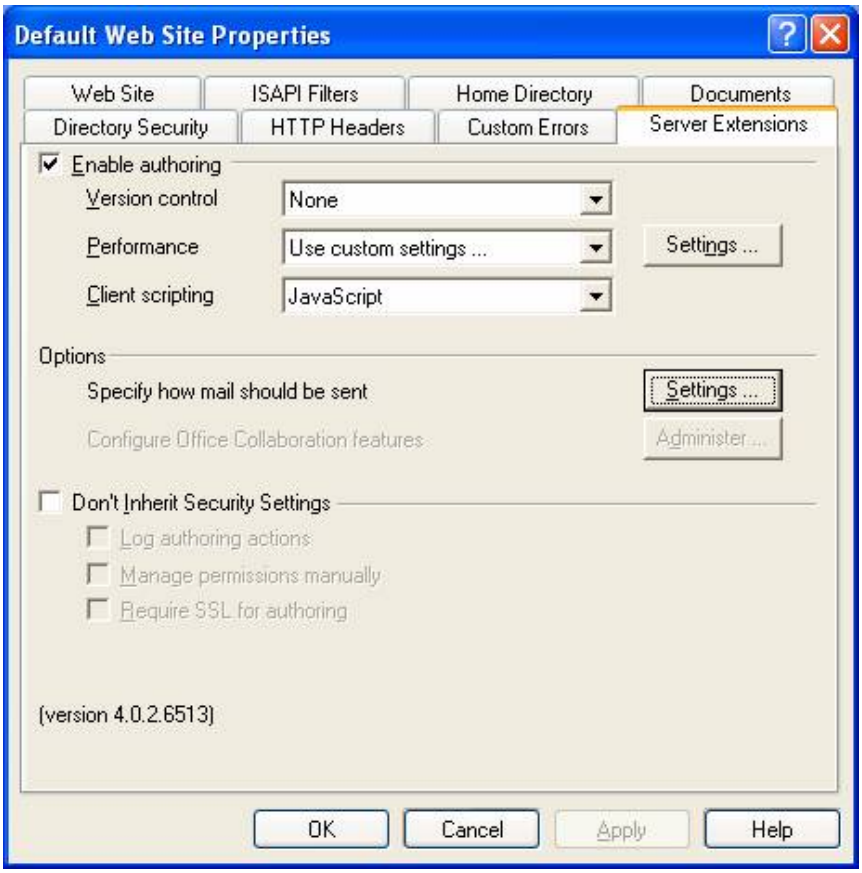
πιστοποιητικού αναλύεται στην σχετική παράγραφο ασφάλειας του web server με τη χρήση πιστοποιητικών.



Εικόνα 33. Μέθοδοι Ταυτοποίησης

Τέλος, η καρτέλα **Server Extensions** μας δίνει τη δυνατότητα ενεργοποίησης του ελέγχου έκδοσης καθώς επίσης και να παραμετροποιήσουμε τις ρυθμίσεις απόδοσης σε σχέση με την αναμενόμενη κίνηση και συχνότητα επισκέψεων στον server.

Επίσης μπορούμε να αλλάξουμε την προεπιλεγμένη γλώσσα script που χρησιμοποιείται από τον client από JavaScript σε VBScript, και αντίθετα. Τέλος, κάποιες φορές ο web server θα πρέπει να αποστέλλει e-mail σε επισκέπτες που είναι συνδεδεμένοι. Η παραμετροποίηση του τρόπου που στέλνει e-mail ο server γίνεται με την επιλογή *Settings* στην καρτέλα **Options** όπως φαίνεται στην **Εικόνα 34.**



Εικόνα 34. Server Extensions

Στη φόρμα που ανοίγει συμπληρώνουμε την e-mail διεύθυνση που θέλουμε να φαίνεται για τον αποστολέα server όπως επίσης και μια διεύθυνση επικοινωνίας, το όνομα του SMTP server και τον τρόπο κωδικοποίησης κειμένου του μηνύματος.

Εικόνα 35. E-mail Settings

Στο τελευταίο τμήμα της καρτέλας **Server Extensions** δίνεται η δυνατότητα για απομακρυσμένο προγραμματισμό (Remote authoring) των ιστοσελίδων του δικτυακού τόπου. Επιλέγοντας να παρακαμφθούν οι ρυθμίσεις ασφαλείας *(Don't Inherit Security Settings)* μπορούμε να δώσουμε το δικαίωμα τροποποίησης των ιστοσελίδων από απομακρυσμένους χρήστες χρησιμοποιώντας μια από τις παρακάτω επιλογές ασφαλείας για την πρόσβαση στη δυνατότητα αυτή:

- Log authoring actions: Με την επιλογή αυτή ο IIS παρακολουθεί τις αλλαγές και τις ιστοσελίδες που γίνονται upload και προσθέτει τις σχετικές πληροφορίες όπως ώρα, όνομα χρήστη, όνομα απομακρυσμένου host κ.α. σε ένα αρχείο log.
- Manage permissions manually: Η επιλογή αυτή απενεργοποιεί τη δυνατότητα που έχουν κάποια εργαλεία διαχείρισης όπως τα εργαλεία του FrontPage (FrontPage MMC snap-in), να αλλάζουν τις ρυθμίσεις ασφαλείας του συγκεκριμένου δικτυακού τόπου.
- Require SSL for authoring: Με την επιλογή αυτή απαιτείται η χρήση του πρωτοκόλλου SSL για τον προγραμματισμό του δικτυακού τόπου.

3.4 FTP SERVER

Το FTP είναι ένα Πρωτόκολλο Μεταφοράς Αρχείων από υπολογιστή σε υπολογιστή και προήλθε από το Unix πριν την εμφάνιση της υπηρεσίας www. Η λήψη αρχείων λέγεται download ενώ η αποστολή αρχείων προς τον ιστό, λέγεται upload. Η σύνδεση γίνεται ανάμεσα σε έναν τοπικό υπολογιστή (local host), ενώ ο υπολογιστής με τον οποίο συνδέεται ονομάζεται μακρινός υπολογιστής (remote host).

Τα δύο είδη FTP είναι: *το ανώνυμο (anonymous) FTP* και *το κανονικό FTP*. Με το πρώτο μπορούμε να κατεβάσουμε (download) αρχεία από τον ιστό χωρίς να χρειαστεί κάποιο ειδικό συνθηματικό (password) χρησιμοποιώντας σαν όνομα χρήστη το anonymous. Με το anonymous FTP, έχουμε δικαίωμα πρόσβασης μόνο σε συγκεκριμένα αρχεία και καταλόγους. Για να ανεβάσουμε (upload), όμως, αρχεία στον ιστό, θα πρέπει να έχουμε πρόσβαση στον διακομιστή FTP με κάποιον κανονικό λογαριασμό και όχι τον ειδικό λογαριασμό anonymous. Συνήθως οι FTP servers έχουν

έναν δημόσιο (public) κατάλογο με το όνομα pub, όπου εκεί περιέχονται τα δημόσια αρχεία για download.

Παρά το γεγονός ότι μεγάλο μέρος των αρχείων ανταλλάσσεται μέσω της υπηρεσίας του Παγκόσμιου Ιστού, παραμένει μια πολύ διαδεδομένη υπηρεσία. Είναι προτιμότερο η υπηρεσία ανεβάσματος αρχείων στον FTP server να είναι απενεργοποιημένη ή στην περίπτωση που είναι ενεργοποιημένη, τα αρχεία να αποθηκεύονται σε έναν ξεχωριστό φάκελο που μπορεί να ονομάζεται "*Εισερχόμενα*". Ο φάκελος αυτός θα πρέπει να παρακολουθείται όσο γίνεται συχνότερα για την περίπτωση ανεβάσματος επικίνδυνων εκτελέσιμων αρχείων.

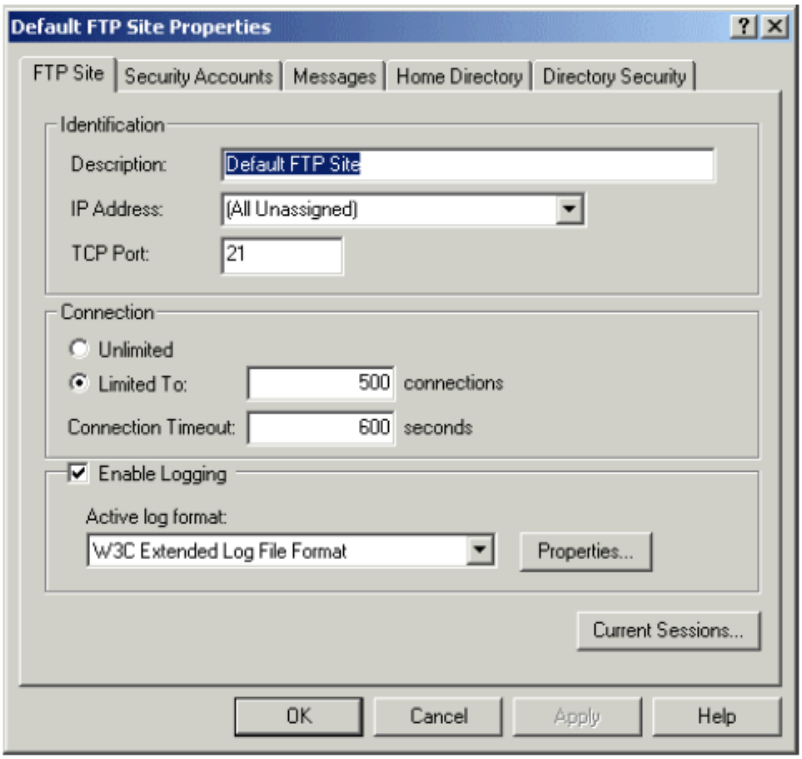
3.4.1 *Οργάνωση των FTP Φακέλων* :Οι FTP φάκελοι, όπου αποθηκεύονται τα αρχεία θα πρέπει να έχουν ονόματα σχετικά με το περιεχόμενό τους, π.χ multimedia αρχεία μπορούν να είναι αποθηκευμένα σε φακέλους ανά κατηγορία με ονόματα όπως video, images, mp3 κα. Για την ασφάλεια των περιεχομένων οι φάκελοι θα πρέπει να έχουν δικαίωμα χρήσης Read ONLY.

Επίσης, για την αντιγραφή αρχείων μέσω FTP στον server και τη δυνατότητα upload, θα πρέπει να δημιουργούνται ξεχωριστοί φάκελοι που όπως είπαμε θα πρέπει να ελέγχονται συχνά για την επικινδυνότητά τους και με δικαίωμα εγγραφής στον λογαριασμό anonymous User. Τα αρχεία αυτά είναι καλό να μεταφέρονται από το διαχειριστή του server σε φακέλους download. Η διαδικασία μπορεί να είναι λίγο πιο πολύπλοκη όμως προστατεύει τα αρχεία που διατίθενται για κατέβασμα από διαγραφή ή αλλοίωση. Επίσης, είναι μια καλή μέθοδος για έναν έλεγχο των αρχείων που διατίθενται από τον server για download αποφεύγοντας μη επιθυμητά αρχεία όπως πορνογραφικά, ιούς κα.

3.4.2 *FTP Site :* Η καρτέλα **FTP Site** περιέχει τις ίδιες επιλογές με την καρτέλα **Web Site** στην υπηρεσία WWW, οι οποίες αναφέρονται εδώ στην υπηρεσία FTP. Έτσι, ομοίως, με την WWW υπηρεσία μπορούμε να καθορίσουμε τις ιδιότητες του FTP όπως το όνομα περιγραφής του, την IP διεύθυνσή του και τη θύρα της συγκεκριμένης υπηρεσίας που στην περίπτωση του FTP είναι καθορισμένη παγκοσμίως με την τιμή 21.

Επίσης, καθορίζουμε τον αριθμό των ταυτόχρονων συνδέσεων καθώς και το χρόνο που πρέπει να παρέλθει για μια ανενεργή σύνδεση έτσι ώστε ο χρήστης αυτομάτως να αποσυνδεθεί.

Τέλος, για λόγους παρακολούθησης της κίνησης και των επισκεπτών του FTP site χρησιμοποιείται ένα αρχείο log με την ενεργοποίηση της επιλογής Enable Logging όπως φαίνεται και στην **Εικόνα 36.**

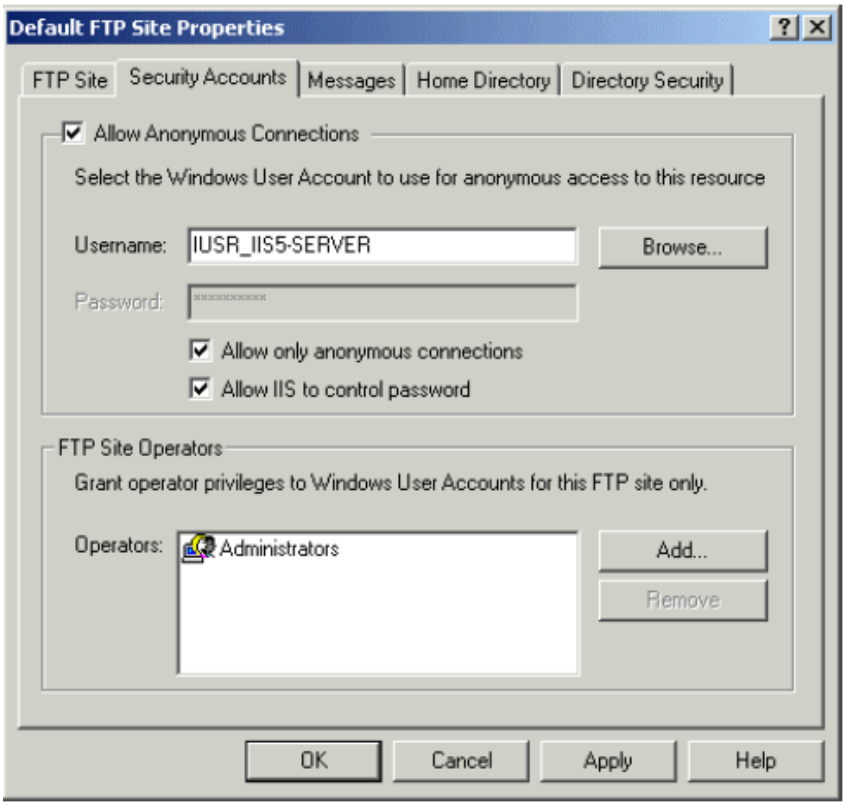


Εικόνα 36. FTP Site

3.4.3 Security Accounts: Η σελίδα αυτή χρησιμοποιείται για τον καθορισμό πρόσβασης με τη χρήση του λογαριασμού anonymous FTP καθώς και τον ορισμό των διαχειριστών του FTP site. Όταν η επιλογή *Allow only anonymous connections* είναι ενεργοποιημένη τότε οι χρήστες μπορούν να συνδεθούν με τον server μόνο με τη χρήση του λογαριασμού IUSR_ΌνομαΥπολογιστή και όχι με κάποιον άλλον στέλνοντας συγκεκριμένο όνομα και κωδικό χρήσης. Με αυτό τον τρόπο περιορίζεται ο κίνδυνος σύνδεσης με κάποιον λογαριασμό που μπορεί να έχει δικαιώματα διαχειριστή του server.

Στην περίπτωση λοιπόν της σύνδεσης *με Allow anonymous connections*, όταν ένας χρήστης συνδέεται χρησιμοποιεί το λογαριασμό IUSR_ΌνομαΥπολογιστή στον FTP server. Στην υπηρεσία FTP δεν υπάρχει η δυνατότητα της επιλογής *Integrated windows authentication.*

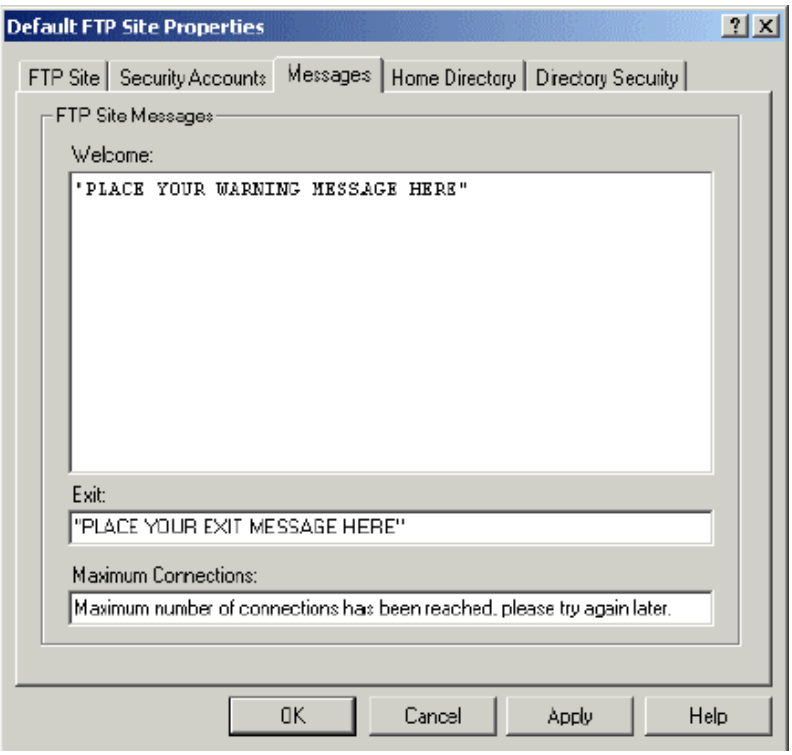
Στο κάτω μέρος της καρτέλας **(Εικόνα 37)** δίνεται η δυνατότητα καθορισμού των λογαριασμών χρηστών που μπορούν να διαχειρίζονται τον FTP server.



Εικόνα 37. Security Accounts.

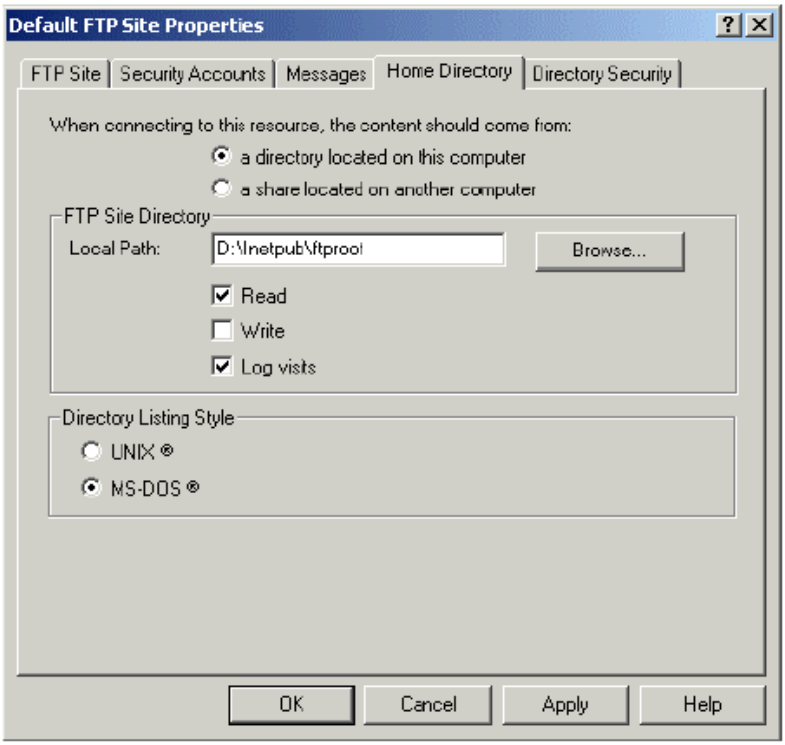
Η επιλογή *Allow IIS to control password* συνδέει τον λογαριασμό anonymous FTP που χρησιμοποιείται για logon και που είναι συνήθως ο IUSR_ΌνομαΥπολογιστή με τον αντίστοιχο λογαριασμό χρήστη που έχει δημιουργηθεί και χρησιμοποιείται στο τμήμα Computer Management.

3.4.4 Messages: Υπάρχουν τρεις τύποι μηνυμάτων που μπορούν να εμφανιστούν στον χρήστη όπως φαίνεται και στην **Εικόνα 38**, τα μηνύματα τύπου Welcome, Exit ή Maximum Connections. Ένα μήνυμα τύπου Welcome εμφανίζεται κατά τη σύνδεση του χρήστη στον FTP server. Αντίστοιχα, τα μηνύματα κατηγορίας Exit εμφανίζουν κάποια ειδοποίηση κατά τον τερματισμό της σύνδεσης. Τέλος, ένα μήνυμα εμφανίζεται και στην περίπτωση που οι συνδέσεις με τον FTP server έχουν φτάσει τον μέγιστο επιτρεπτό αριθμό.



Εικόνα 38. Messages

3.4.5 Home Directory: Αντίστοιχα με την ίδια επιλογή στην υπηρεσία WWW, μπορούμε να προσδιορίσουμε μέσα από αυτή τη φόρμα αν το περιεχόμενο δηλ. τα αρχεία για upload ή download θα βρίσκεται σε κάποιο φάκελο σε κάποιο δίσκο του server ή κάποιον υπολογιστή συνδεδεμένο με αυτόν, μέσω δικτύου. Όταν πρόκειται για τοπικό φάκελο μπορούμε να προσδιορίσουμε τη θέση του φακέλου στον server (Local Path) ενώ στην περίπτωση που το περιεχόμενο προέρχεται από άλλον υπολογιστή δικτύου τότε προσδιορίζουμε το όνομα του υπολογιστή και τη θέση του φακέλου μέσα σε αυτόν. Επίσης, μπορούμε να προσδιορίσουμε τα δικαιώματα πρόσβασης στους φακέλους του FTP site. Όπως ήδη αναφέραμε, είναι προτιμότερο όσον αφορά στην ασφάλεια του FTP site να δημιουργήσουμε δύο ξεχωριστούς φακέλους για την αποθήκευση αρχείων upload και download. Ο φάκελος που θα φιλοξενεί τα αρχεία για download, είναι ασφαλές να έχει μόνο δικαίωμα πρόσβασης Read ενώ ο φάκελος με τα αρχεία που έχουν γίνει upload μπορεί να έχει και Write **(Εικόνα 39)**. Ένας administrator του FTP site μπορεί να ελέγχει τι είδους αρχεία ανεβάζονται στον server και ποια από αυτά θα μπορούσαν να διανεμηθούν για download.



Εικόνα 39. Home Directory

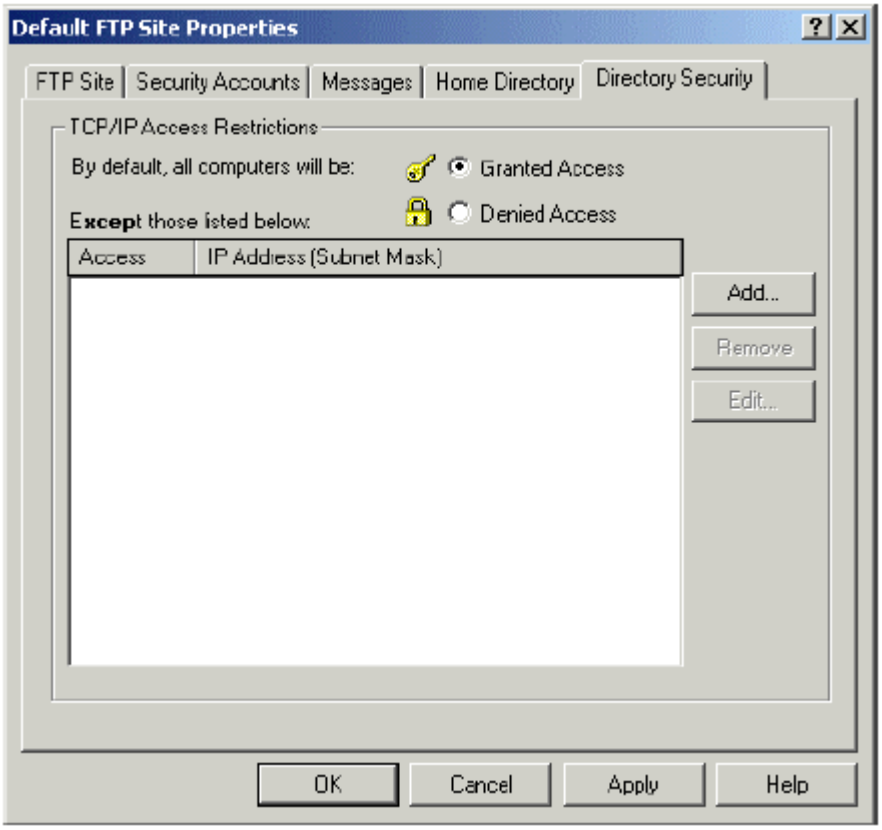
3.4.6 Directory Security: Σε αυτή τη φόρμα όπως φαίνεται και στην **Εικόνα 40** μπορούμε να προσδιορίσουμε ποιος μπορεί να συνδεθεί με το FTP site με βάση την IP διεύθυνση. Υπάρχουν οι επιλογές *Granted Access* και *Denied Access*. Η επιλογή *Granted Access* επιτρέπει την πρόσβαση στο FTP site όλων των υπολογιστών εκτός αυτών των οποίων η IP διεύθυνση περιλαμβάνεται στη λίστα που βρίσκεται στο κάτω μέρος της φόρμας.

Αντίθετα η επιλογή *Denied Access* επιτρέπει την πρόσβαση εκείνων μόνο των υπολογιστών που η IP διεύθυνση περιλαμβάνεται στη λίστα και αρνείται την πρόσβαση όλων των άλλων.

Υπάρχουν τρεις επιλογές κατά τον καθορισμό των IP διευθύνσεων που θα συμπεριληφθούν στη λίστα:

- Μεμονωμένος Υπολογιστής (single computer)
- Ομάδα Υπολογιστών (group of computers), που απαιτεί τον καθορισμό του *network ID* και της *μάσκας του υποδικτύου (subnet mask)*

- Όνομα Τομέα (Domain Name)



Εικόνα 40. Directory Security

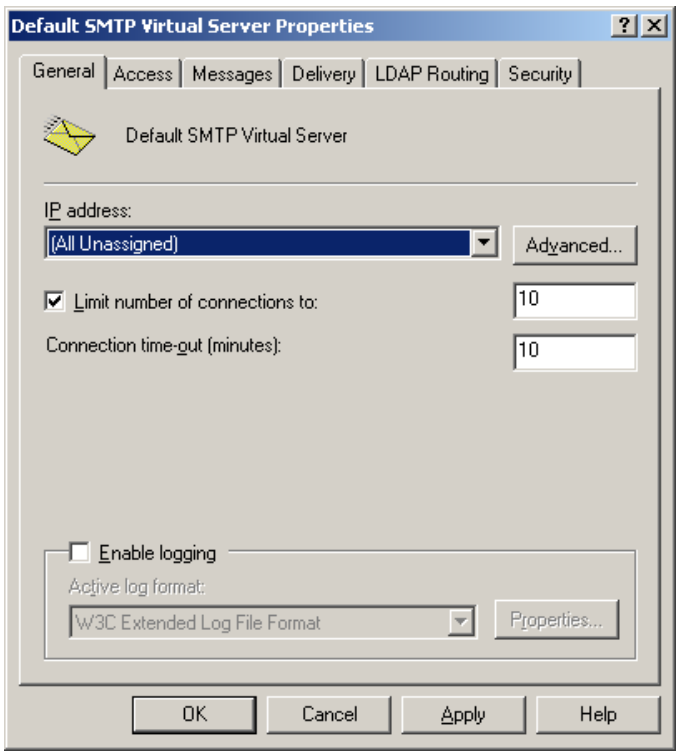
3.5 ΥΠΗΡΕΣΙΑ SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

Ο IIS 5.0 όπως είδαμε στις υπηρεσίες περιλαμβάνει και την υπηρεσία SMTP mail για τη μεταφορά μηνυμάτων του Internet μεταξύ διακομιστών. Η υπηρεσία δεν προσφέρει έναν POP server και γι' αυτό δε μπορεί να χρησιμοποιηθεί με κάποια εφαρμογή τελικού χρήστη (end – user programs) όπως είναι το Netscare Mail ή το Outlook Express. Η υπηρεσία είναι συμβατή με την πλειοψηφία των SMTP server και client. Χρησιμοποιείται κυρίως από εφαρμογές Internet που χρησιμοποιούν SMTP, όπως για παράδειγμα, για την αποστολή αυτομάτως ενός μηνύματος επιβεβαίωσης προς έναν πελάτη που συμπλήρωσε μια ηλεκτρονική φόρμα εγγραφής.

Επίσης, ένας web server μπορεί να λάβει μηνύματα. Αυτό μπορεί να χρησιμοποιηθεί στην περίπτωση που ο server αποστέλλει ένα μήνυμα σε κάποιον client και για κάποιο λόγο το μήνυμα δε φτάνει στον προορισμό του. Σε αυτή την περίπτωση ο server μπορεί να παραλάβει μια απόδειξη μη-παράδοσης του αρχικού μηνύματος, το οποίο θα ειδοποιεί τον διαχειριστή του server. Επίσης, μπορεί να δημιουργηθεί ένα mailbox που να παραλαμβάνει τα μηνύματα επισκεπτών ενός δικτυακού τόπου που φιλοξενείται στον server.

Επιλέγοντας το *SMTP site* και πατώντας τις Ι*διότητες* μπορούμε να παραμετροποιήσουμε την SMTP υπηρεσία.

3.5.1 *General:* Η καρτέλα αυτή είναι παρόμοια με την αντίστοιχη στις προηγούμενες υπηρεσίες. Εδώ μπορούμε, όπως φαίνεται και στην **Εικόνα 42,** να περιγράψουμε το όνομα του SMTP και να προσδιορίσουμε την IP διεύθυνση. Επίσης, μπορούμε να ενεργοποιήσουμε με τον ίδιο τρόπο την καταγραφή των συμβάντων σε ένα αρχείο log με την επιλογή *Enable Logging*, παραμετροποιώντας την από το κουμπί *Configuration*, όπως έχουμε δει μέχρι τώρα. Τέλος, παρόμοια και με τις άλλες υπηρεσίες καθορίζουμε το μέγιστο πλήθος και χρόνο σύνδεσης στον server.

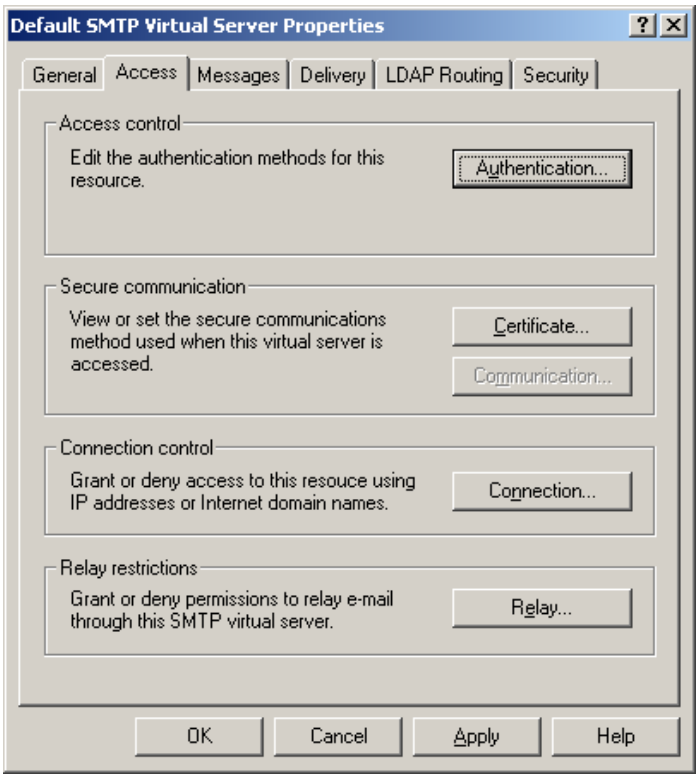


Εικόνα 41. SMTP

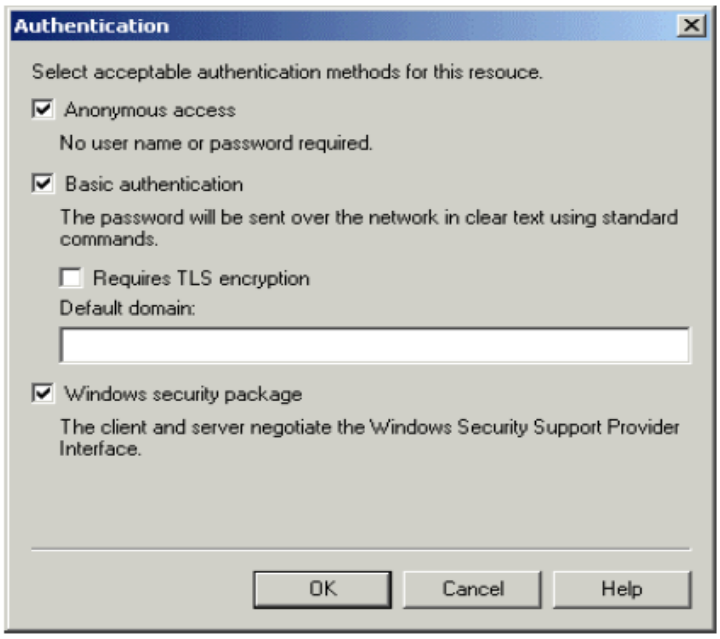
3.5.2 Access: Η καρτέλα Access περιέχει ένα πλήθος επιλογών όσον αφορά την πρόσβαση στον SMTP server. Με την επιλογή *Authentication* ανοίγει η φόρμα Authentication όπου μπορούμε να παραμετροποιήσουμε τις δυνατότητες ταυτοποίησης του χρήστη με παρόμοιο τρόπο με τις άλλες υπηρεσίες.

Έτσι αναλυτικά έχουμε τις εξής επιλογές ταυτοποίησης:

- Anonymous Access: Η μέθοδος είναι παρόμοια με προηγούμενες υπηρεσίες.
- Basic Authentication: Ομοίως, είναι παρόμοια με προηγούμενες υπηρεσίες.
- Requires TLS encryption: Με την επιλογή αυτή, τα εισερχόμενα μηνύματα κρυπτογραφούνται με βάση το πρωτόκολλο TLS (Transport Layer Security). Για τη χρησιμοποίηση της Βασικής Ταυτοποίησης (Basic Authentication), ορίζεται ένα προεπιλεγμένο domain.
- Windows Security Package: Για να χρησιμοποιηθεί η επιλογή αυτή ταυτοποίησης θα πρέπει να υποστηρίζεται από την client εφαρμογή του mail όπως το Microsoft Outlook Express. Η ταυτοποίηση γίνεται με μεγαλύτερο βαθμό ασφάλειας χρησιμοποιώντας μια τεχνική κρυπτογράφησης έτσι ώστε να μην μεταδίδονται μέσω δικτύου οι πραγματικοί κώδικες χρήσης.



Εικόνα 42. Access



Εικόνα 43. Authentication

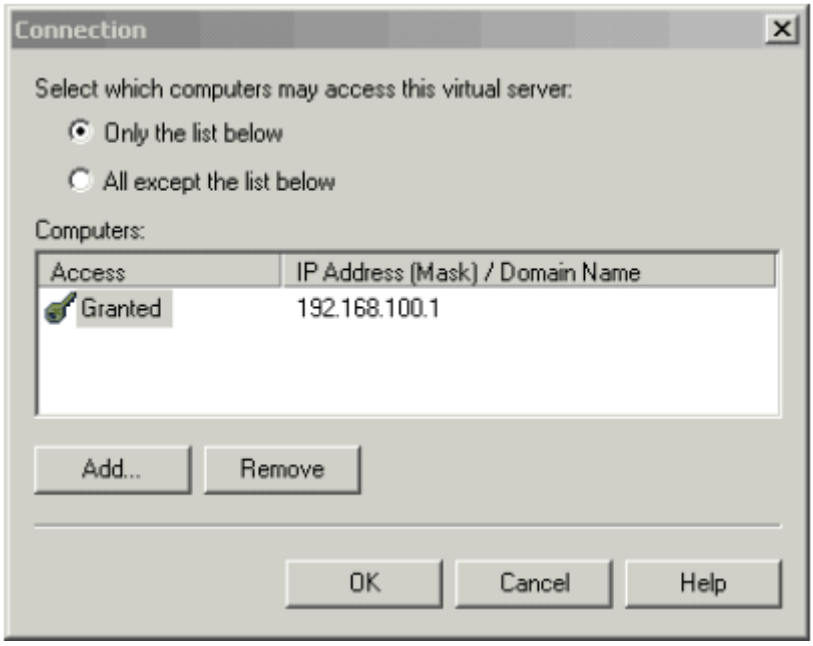
Η υπηρεσία Microsoft SMTP όπως είπαμε, υποστηρίζει το πρωτόκολλο **T**ransport **L**ayer **S**ecurity (TLS) για την μετάδοση μηνυμάτων σε κρυπτογραφημένη

μορφή. Η χρήση του TLS μπορεί να εφαρμοστεί σε όλες τις εισερχόμενες συνδέσεις με την χρήση του τμήματος Secure Communication στην καρτέλα **Access**. Το πρωτόκολλο TLS βασίζεται στη χρήση ζεύγους κλειδιών και ψηφιακών πιστοποιητικών. Για την απόκτηση των πιστοποιητικών, με την επιλογή Certificate δημιουργείται μια αίτηση για ψηφιακό πιστοποιητικό από κάποιο Φορέα Πιστοποίησης (CA – Certificate Authority).

Η χρήση του πιστοποιητικού για την κρυπτογράφηση των μηνυμάτων ορίζεται από τη φόρμα **Security** η οποία ανοίγει από την επιλογή Communication στο τμήμα Secure Communication της καρτέλας. Για τη μέγιστη δυνατή ασφάλεια, επιλέγοντας τη δυνατότητα *Require 128-bit encryption,* όπως φαίνεται και στην **Εικόνα 44,** χρησιμοποιείται κωδικοποίηση των 128 bits, εφόσον αυτή υποστηρίζεται από τον υπολογιστή.

Εικόνα 44. Security

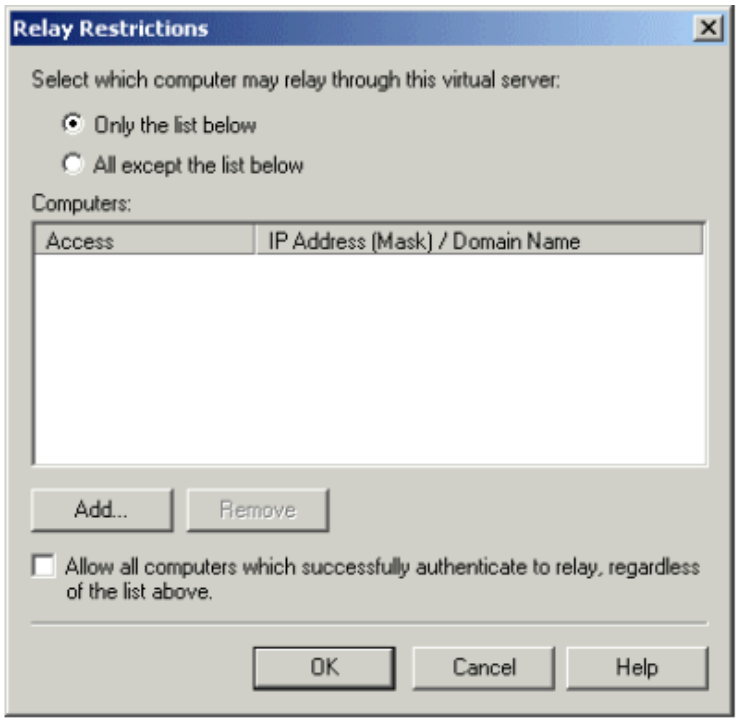
Η επιλογή Connection στο αντίστοιχο τμήμα της καρτέλας **Access** λειτουργεί παρόμοια με την αντίστοιχη επιλογή στις υπηρεσίες WWW και FTP. Μπορούμε να προσδιορίσουμε τις IP διευθύνσεις των υπολογιστών που θέλουμε να έχουν πρόσβαση στην υπηρεσία θέτοντας την επιλογή *Only the list below* στη φόρμα Connection **(Εικόνα 45)** ή να αποκλείσουμε την πρόσβαση στους συγκεκριμένους υπολογιστές χρησιμοποιώντας την επιλογή *All except the list below*.



Εικόνα 45. Δικαίωμα Σύνδεσης

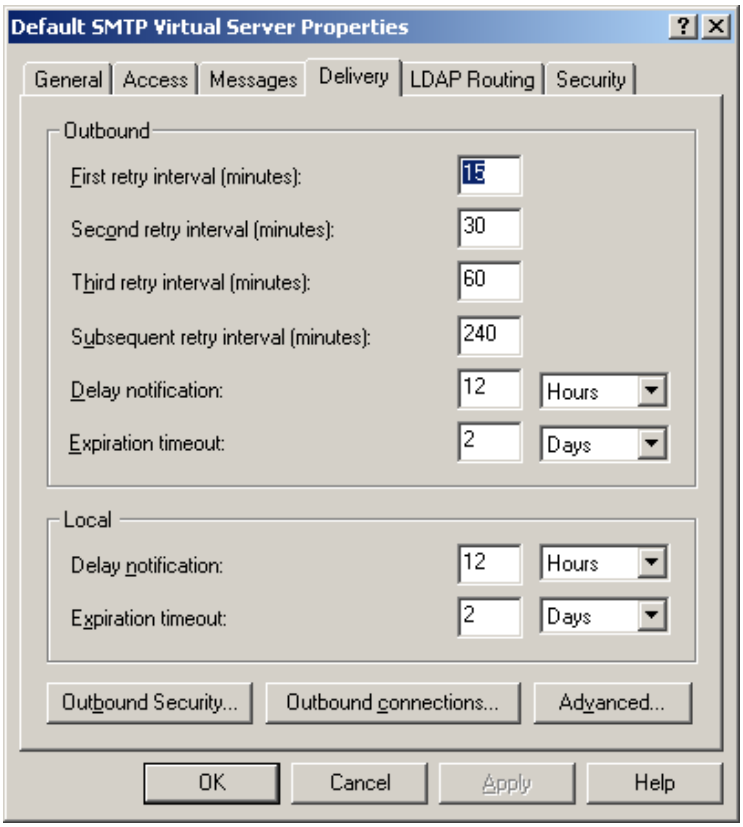
Στην καρτέλα **Access,** τέλος, υπάρχει το τμήμα *Relay Restrictions* με την επιλογή *Relay.* Με την επιλογή αυτή μπορούμε να ορίσουμε ποιοι υπολογιστές μπορούν να στέλνουν μηνύματα στο δικό μας server για αναμετάδοση προς άλλους SMTP servers.

Ομοίως, έχουμε δύο επιλογές για τον ορισμό του δικαιώματος αυτού σε υπολογιστές. Είτε να ορίσουμε τις IP διευθύνσεις αυτών που έχουν δικαίωμα για *Relay* με την επιλογή *Only the list below* είτε να αποκλείσουμε κάποιους με την επιλογή *All except the list below.* Η συγκεκριμένη επιλογή θα πρέπει να χρησιμοποιείται με μεγάλη προσοχή διότι μπορεί να δοθεί η ευκαιρία σε τρίτους να την χρησιμοποιήσουν για την αποστολή spam mail μέσω του δικού μας server έτσι ώστε να φαίνεται ότι προέρχονται από τον δικό μας server. Τέλος, υπάρχει και η επιλογή *Allow all computers which successfully authenticates to relay, regardless of the list* με την οποία όλοι όσοι έχουν κάνει ταυτοποίηση με την χρήση ονόματος και κωδικού χρήστη μπορούν να χρησιμοποιούν την παραπάνω δυνατότητα ανεξάρτητα με την λίστα υπολογιστών που έχουν οριστεί πρωτύτερα όπως φαίνεται και στην **Εικόνα 46.**



Εικόνα 46. Αναμετάδοση

3.5.3 Delivery : Στην καρτέλα αυτή μπορούμε να παραμετροποιήσουμε τις ρυθμίσεις για την εξερχόμενη αλληλογραφία. Στο τμήμα Outbound μπορούμε να ορίσουμε τα χρονικά διαστήματα κατά τα οποία θα προσπαθεί ο server να αποστείλει την εξερχόμενη αλληλογραφία μέχρι και την τρίτη προσπάθεια και για κάθε προσπάθεια μετά από την τρίτη μπορούμε να ορίσουμε και το χρόνο στον οποίο θα λάβουμε ειδοποίηση ότι η αλληλογραφία έχει καθυστερήσει να αποσταλεί και το μέγιστο χρόνο για τον οποίο θα σταματήσει να προσπαθεί για την αποστολή των εξερχόμενων μηνυμάτων.

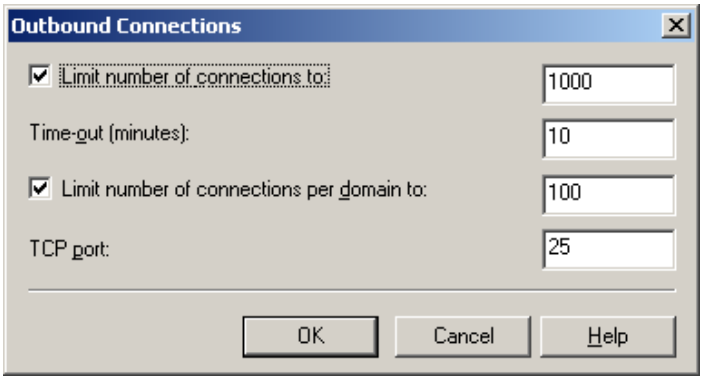


Εικόνα 47. Delivery

Για τον ορισμό των παραμέτρων ασφαλείας των εξερχόμενων μηνυμάτων επιλέγουμε το κουμπί *Outbound Security*. Για τα μηνύματα που είναι να αποσταλούν μπορούμε στη φόρμα *Outbound Security* να ορίσουμε το είδος της ταυτοποίησης που απαιτείται από τον SMTP server που θα παραλάβει την αλληλογραφία και το αν θα χρησιμοποιηθεί κρυπτογράφηση TLS. Βασική προϋπόθεση είναι ο server – παραλήπτης να υποστηρίζει τη μέθοδο ταυτοποίησης που έχουμε ορίσει για τα αποστελλόμενα μηνύματα. Οι επιλογές όπως φαίνεται και στην **Εικόνα 48** είναι παρόμοιες με τις επιλογές που έχουμε ήδη αναφέρει και σε προηγούμενες παραμετροποιήσεις ταυτοποίησης όπως η Anonymous Access ή η Basic Access με κρυπτογράφηση TLS.

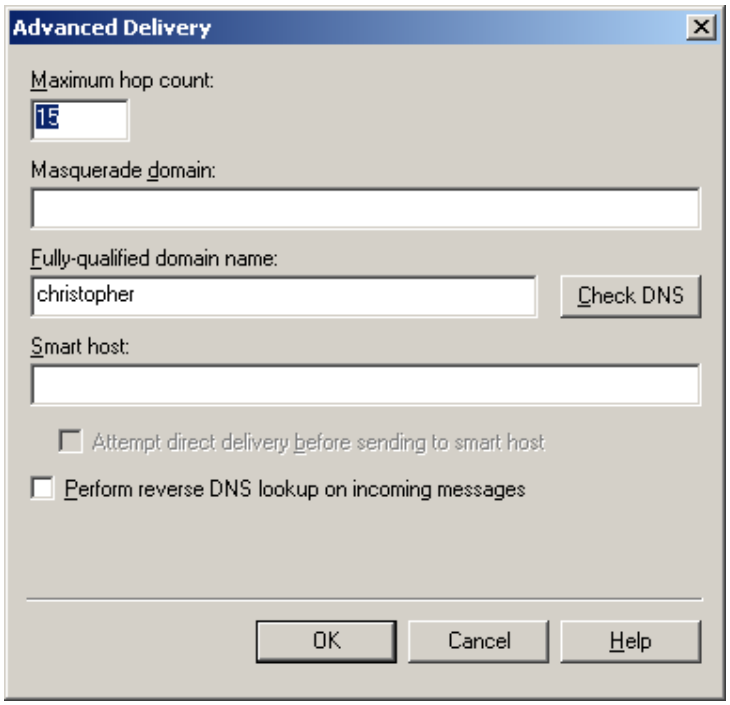
Εικόνα 48. Outbound Security

Επίσης η επιλογή *Outbound Connections* στην καρτέλα **Delivery** μας δίνει τη δυνατότητα παραμετροποίησης του μέγιστου αριθμού συνδέσεων εξερχόμενης Αλληλογραφίας συνολικά και ανά απομακρυσμένο domain, το χρόνο λήξης μιας ανενεργούς σύνδεσης καθώς και τη θύρα που θα χρησιμοποιηθεί για την αποστολή των εξερχόμενων μηνυμάτων και η οποία έχει προεπιλεγμένη τιμή το 25 όπως καθορίζεται από το πρωτόκολλο TCP και φαίνεται και στην **Εικόνα 49.**



Εικόνα 49. Outbound Connections

Τέλος, η επιλογή *Advanced* ανοίγει την αντίστοιχη φόρμα παραμετροποίησης. Η πρώτη ρύθμιση είναι η Maximum hop count. Όταν ένα μήνυμα αποστέλλεται μπορεί να περάσει από κάποιο πλήθος ενδιάμεσων server μέχρι να φτάσει στον τελικό του προορισμό. Με τη ρύθμιση αυτή μπορούμε να εισάγουμε το μέγιστο αριθμό ενδιάμεσων server. Αν το πλήθος των ενδιάμεσων servers ξεπεράσει τον αριθμό, αυτό το μήνυμα επιστρέφεται πίσω στον server μας με μια ειδοποίηση μη παραλαβής.



Εικόνα 50. Advanced Delivery

Με την επιλογή *Masquerade domain* μπορούμε να αλλάξουμε το όνομα του domain που εμφανίζεται στη στήλη "Από" (Mail From) στα απεσταλμένα μηνύματα. Επίσης υπάρχει το πεδίο Fully-qualified domain name. Για να ταυτοποιηθεί και να επικυρωθεί ένας υπολογιστής σε ένα TCP/IP δίκτυο απαιτείται μια εγγραφή του Mail Exchanger η οποία αποτελείται από το όνομα domain και το όνομα του host. Το όνομα FQDN (Fully-Qualified Domain Name) χρησιμοποιείται από την υπηρεσία DNS (Domain Name Server) για να προσδιορίσει τον host server για ένα domain. Το όνομα FQDN χρησιμοποιείται από την υπηρεσία SMTP. Είναι το ίδιο με αυτό που έχει προσδιοριστεί στο πεδίο Computer Identification στις Ιδιότητες Συστήματος του Υπολογιστή και μπορεί να αλλαχτεί είτε από εκεί είτε από τη συγκεκριμένη φόρμα.

Η επιλογή *Smart host* μας δίνει τη δυνατότητα να προσδιορίσουμε έναν host server στον οποίο θα δρομολογηθούν όλα τα εξερχόμενα μηνύματα αντί να σταλούν απευθείας στο απομακρυσμένο domain. Αυτό μας επιτρέπει να δρομολογήσουμε τα μηνύματα μέσω μιας σύνδεσης που μπορεί να είναι πιο γρήγορη ή πιο οικονομική. Για να προσδιορίσουμε τον smart host μπορούμε να πληκτρολογήσουμε είτε το όνομα FQDN ή την IP διεύθυνσή του μέσα σε αγκύλες [ ]. Έχοντας ενεργοποιημένη την επιλογή *Attempt direct delivery before sending to smart host* η υπηρεσία SMTP επιχειρεί να αποστείλει τα μηνύματα πρώτα απευθείας στον απομακρυσμένο domain πριν επιχειρήσει να τα στείλε μέσω του smart host.

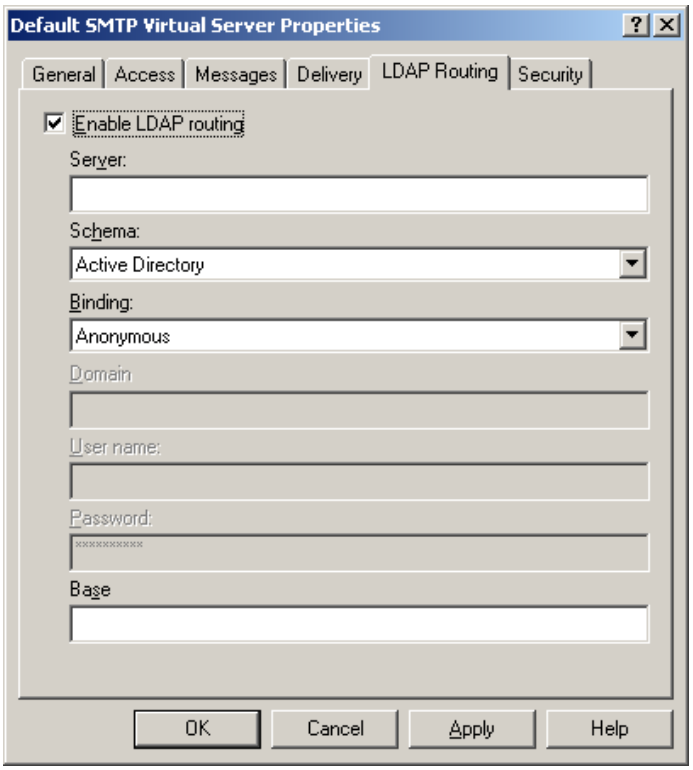
Τέλος, η Επιλογή *Perform reverse DNS lookup on incoming messages* ενεργοποιεί μια διαδικασία επικύρωσης από την υπηρεσία SMTP. Γίνεται ένας έλεγχος για το αν η IP διεύθυνση του Client ταιριάζει με το όνομα host/domain που υποβάλλεται από τον Client κατά την εντολή EHLO/HELO. Αν ο έλεγχος είναι επιτυχής τότε η επικεφαλίδα RECEIVED παραμένει ως έχει αλλιώς παίρνει την τιμή "unverified".

3.5.4 LDAP Routing: Η καρτέλα LDAP Routing χρησιμοποιείται για να παραμετροποιήσουμε τις ιδιότητες ενός server Υπηρεσίας Καταλόγων (Directory Services Server) που θα χρησιμοποιείται από τον SMTP server και όπου θα αποθηκεύονται πληροφορίες για τους mail clients και τα mailboxes. Το πρωτόκολλο επικοινωνίας του SMTP server με τον server Υπηρεσίας Καταλόγων είναι το Lightweight Directory Access Protocol (LDAP). Ο SMTP Server μπορεί να παραμετροποιηθεί έτσι ώστε να χρησιμοποιεί έναν LDAP server για τη διαχείριση αποστολέων και παραληπτών των μηνυμάτων.

Για να ενεργοποιηθεί το πρωτόκολλο LDAP ενεργοποιούμε την επιλογή Enable LDAP. Το πρώτο πεδίο το οποίο ρυθμίζουμε είναι ο Server όπου συμπληρώνουμε το όνομα του υπολογιστή στον οποίο είναι εγκατεστημένη η υπηρεσία LDAP. Το πεδίο Schema αφορά τον τύπο της υπηρεσίας καταλόγου που θέλουμε να χρησιμοποιηθεί.

Οι δυνατές επιλογές είναι:

- Active Directory. Με την επιλογή αυτή χρησιμοποιείται ο Windows 2000 Active Directory σαν LDAP server.
- Site Server Membership Directory. Η επιλογή αυτή αφορά το Microsoft LDAP Service σαν τμήμα του Microsoft Commercial Internet System 2.0 Mail.
- Exchange LDAP Service. Με την επιλογή αυτή χρησιμοποιείται ο Microsoft Site Server 3.0 ή νεότερη έκδοση σαν LDAP server.



Εικόνα 51. LDAP Routing

Με την επιλογή *Binding* καθορίζουμε τον τρόπο ταυτοποίησης του SMTP server από τον LDAP server.

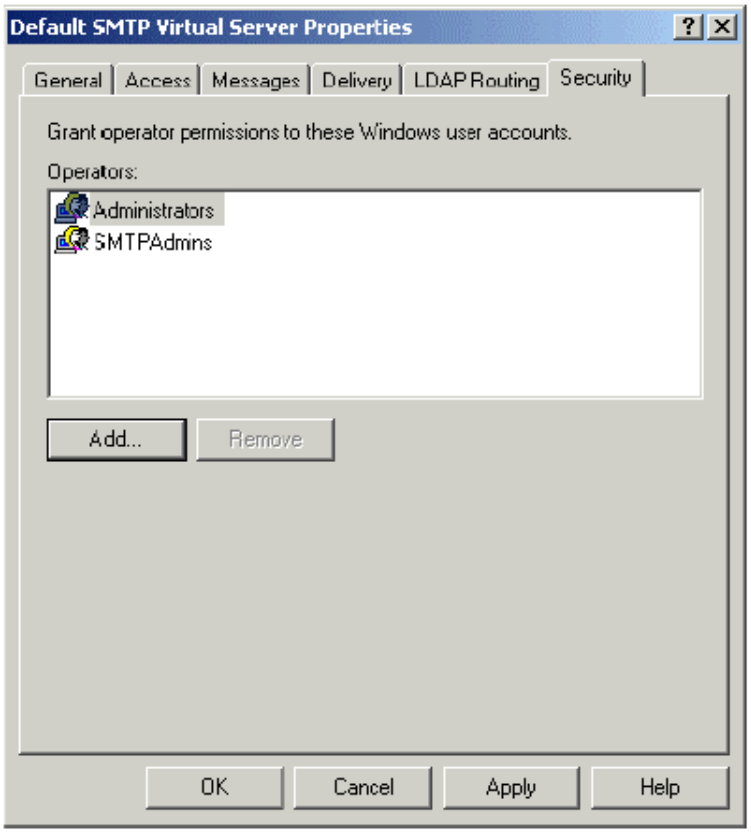
Οι δυνατοί τρόποι είναι οι εξής:

- Anonymous. Δεν στέλνεται όνομα ή κωδικός χρήστη.
- Plain text. Το όνομα και κωδικός χρήστη στέλνονται σαν απλό κείμενο στον LDAP server.
- Windows SSPI. Το όνομα και κωδικός χρήστη στέλνονται σε κρυπτογραφημένη μορφή.
- Service accounts. Χρησιμοποιούνται οι πληροφορίες του λογαριασμού με τον οποίο ο SMTP Server λειτουργεί.

Το πεδίο Domain καθορίζει το domain του λογαριασμού χρήστη που θα χρησιμοποιηθεί για τη σύνδεση με τον LDAP server. Το όνομα χρήστη για τη σύνδεση με τον LDAP server ορίζεται από το πεδίο User name ενώ ο κωδικός χρήστη στο πεδίο

Password. Οι παραπάνω ρυθμίσεις λειτουργούν μόνο για τους τύπους σύνδεσης Plain text ή Windows SSPI. Τέλος, στο πεδίο Base προσδιορίζουμε το όνομα ενός container στην υπηρεσία directory από όπου η υπηρεσία SMTP θα ξεκινήσει την αναζήτηση στον LDAP server.

3.5.5 Security: Στην καρτέλα **Security** προσδιορίζουμε τους χρήστες ή τις ομάδες χρηστών που θα είναι διαχειριστές της υπηρεσίας SMTP. Υπάρχει η δυνατότητα δημιουργίας ομάδων χρηστών τοπικά στο μηχάνημα για τη διαχείριση λογαριασμών χρηστών οι οποίοι θα αποτελούν διαχειριστές της υπηρεσίας SMTP, όπως φαίνεται και στην **Εικόνα 52** .

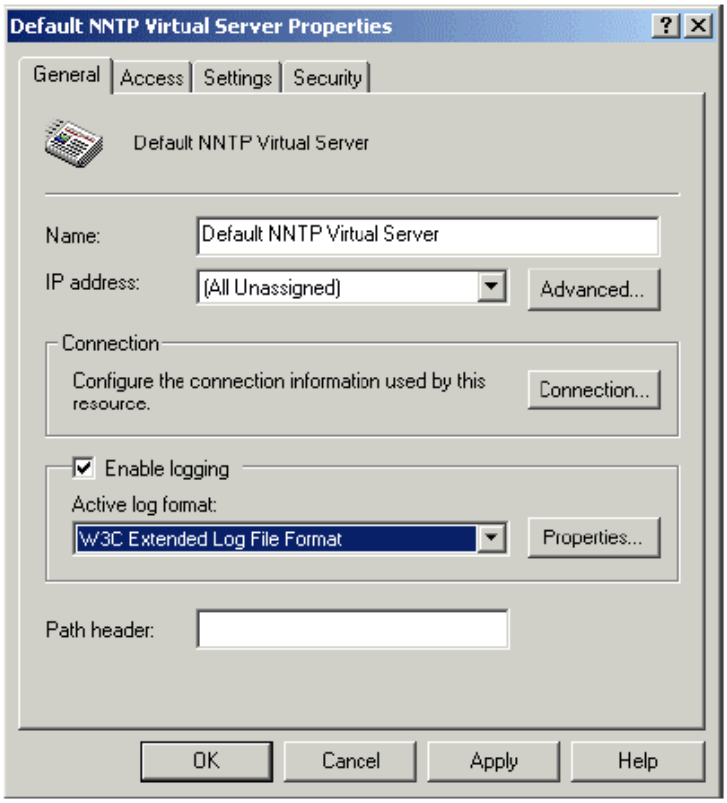


Εικόνα 52. Security

3.6 NETWORK NEWS TRANSFER PROTOCOL (NNTP)

Ο IIS 5.0 όπως είδαμε στην εισαγωγή συμπεριλαμβάνει και την υπηρεσία NNTP (Network News Transfer Protocol), η οποία χρησιμοποιείται για τη φιλοξενία ομάδων συζητήσεων τύπου USENET σε ένα εσωτερικό ή εξωτερικό δίκτυο. Ο server υποστηρίζει πολλές μεθόδους ταυτοποίησης, αποκλεισμό IP διευθύνσεων ή domain και κατέβασμα νέων ειδήσεων. Για την παραμετροποίηση του NNTP server, τον επιλέγουμε και κατόπιν ανοίγουμε τις Ιδιότητές του.

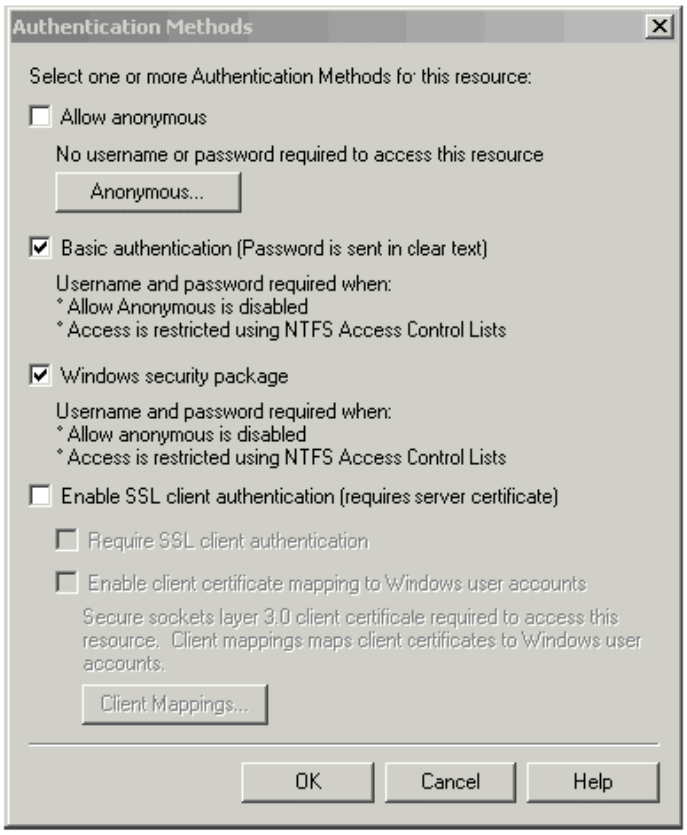
Στην φόρμα που εμφανίζεται η πρώτη καρτέλα είναι η **General**. Οι επιλογές στη συγκεκριμένη φόρμα είναι ίδιες με αυτές που έχουμε παραμετροποιήσει σε όλες τις άλλες υπηρεσίες όπως φαίνεται και στην **Εικόνα 53**.



Εικόνα 53. General

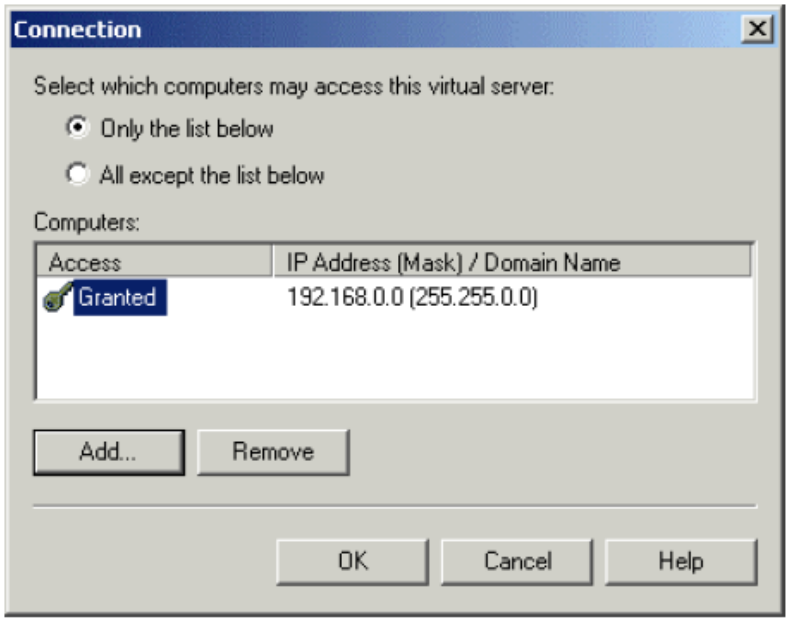
Στην καρτέλα **Access** υπάρχουν επίσης οι ρυθμίσεις πρόσβασης στον NNTP server από τους χρήστες. Με την επιλογή *Authentication* ανοίγει η φόρμα με τις ρυθμίσεις ταυτοποίησης όπου καθορίζουμε τις μεθόδους με τις οποίες θα γίνει η

ταυτοποίηση κατά τη σύνδεση των χρηστών για τη δημοσίευση ειδήσεων. Οι επιλογές που είναι δυνατές είναι παρόμοιες με τις υπόλοιπες υπηρεσίες που έχουμε προαναφέρει. Μία από αυτές είναι η *Anonymous Authentication*, η οποία ενεργοποιείται με την επιλογή *Allow anonymous.* Η επιλογή αυτή δεν συνίσταται στη συγκεκριμένη υπηρεσία διότι δίνεται το δικαίωμα έτσι σε οποιονδήποτε χρήστη που συνδέεται με τον server, να δημοσιεύει οποιαδήποτε πληροφορία. Αν η υπηρεσία δεν περιορίζεται στα πλαίσια ενός ενδοδικτύου (intranet) τότε η καλύτερη επιλογή θα ήταν η χρήση της ταυτοποίησης με τη χρήση του πρωτοκόλλου SSL και των ψηφιακών πιστοποιητικών.



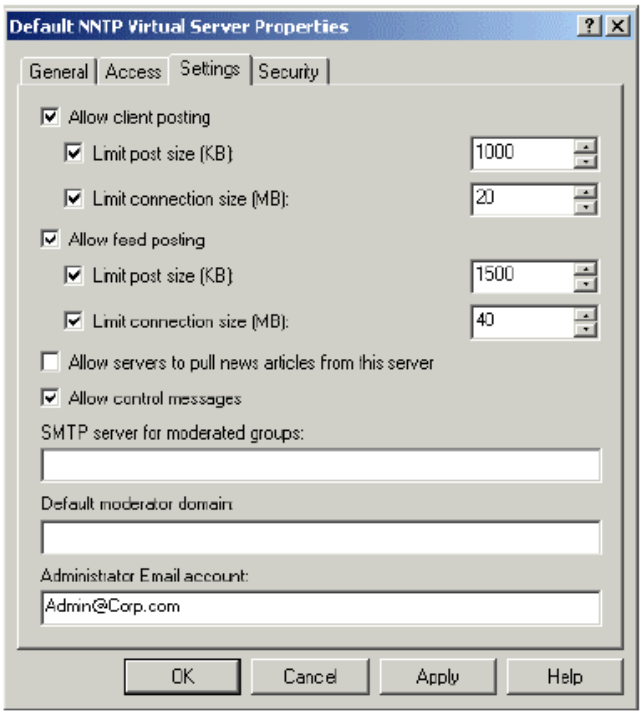
Εικόνα 54. Μέθοδοι Ταυτοποίησης

Στην ίδια καρτέλα υπάρχει επίσης η επιλογή *Connection*, η οποία ανοίγει το παράθυρο *Connection*, όπως φαίνεται και στην **Εικόνα 55.** Στο παράθυρο μπορούμε να αποκλείσουμε μια λίστα χρηστών ενεργοποιώντας την επιλογή *All except the list below* και ορίζοντας τις ανεπιθύμητες IP διευθύνσεις ή να επιτρέψουμε σε αυτή τη λίστα την πρόσβαση με την επιλογή *Only the list below.*



Εικόνα 55. Σύνδεση

3.6.1 Settings: Όπως φαίνεται και στην **Εικόνα 56** υπάρχουν διάφορες ρυθμίσεις που αφορούν σε περιορισμούς της υπηρεσίας NNTP. Εδώ δηλώνεται η δυνατότητα των χρηστών να δημοσιεύουν στον server μηνύματα και επίσης ο μέγιστος αριθμός μηνυμάτων που μπορεί να δημοσιεύσει ένας χρήστης και το μέγιστο μέγεθος ανά σύνδεση. Μια επίσης σημαντική επιλογή είναι η *Allow servers to pull news articles from this server*, η οποία δίνει τη δυνατότητα σε μηνύματα τα οποία έχουν δημοσιευθεί στον server να διαδοθούν σε άλλους NNTP servers. Η επιλογή αυτή είναι προτιμότερο να είναι απενεργοποιημένη στην περίπτωση που χρησιμοποιείται για ομάδες ειδήσεων εσωτερικά σε ένα δίκτυο. Η επιλογή *Allow control messages*, δίνει τη δυνατότητα σε χρήστες να σβήνουν ομάδες συζητήσεων ή μηνύματα.



Εικόνα 56. Settings

3.6.2 Security: Στην καρτέλα Security, προσδιορίζουμε τους χρήστες ή τις ομάδες χρηστών που θα είναι διαχειριστές της υπηρεσίας NNTP με τον ίδιο τρόπο που έχει παρουσιαστεί και σε προηγούμενες υπηρεσίες. Υπάρχει η δυνατότητα δημιουργίας ομάδων χρηστών τοπικά στο μηχάνημα για τη διαχείριση λογαριασμών χρηστών οι οποίοι θα αποτελούν διαχειριστές της υπηρεσίας NNTP.

3.7 Certificate Server

Μια από τις σημαντικότερες δυνατότητες που παρέχει ο IIS είναι η ταυτοποίηση χρηστών με τη χρήση του πρωτοκόλλου Secure Socket Layer (SSL). Για τη χρήση του πρωτοκόλλου απαιτείται η έκδοση ενός *ψηφιακού πιστοποιητικού* (Digital Certificate). Το ψηφιακό πιστοποιητικό εκδίδεται από έναν ανεξάρτητο Φορέα Πιστοποίησης (Certificate Authority) όπως η VeriSign, ο οποίος εγγυάται για την εταιρία ή τον δικτυακό τόπο που αιτείται. Το πιστοποιητικό αποστέλλεται, εγκαθίσταται στον web server και χρησιμοποιείται για την ασφάλεια των Διαδικτυακών υπηρεσιών όσον αφορά την ταυτοποίηση χρηστών και την κρυπτογράφηση δεδομένων. Αν και στο παρελθόν οι web

browsers υποστήριζαν πιστοποιητικά ασφαλείας των 40 bits σήμερα υποστηρίζεται κρυπτογράφηση των 128 bits που παρέχει τη μέγιστη δυνατή ασφάλεια. Μερικοί από τους φορείς πιστοποίησης είναι οι εξής:

- http://www.baltimore.com/servercert/index.asp
- http://www.entrust.com
- http://www.geotrust.com
- http://www.instantssl.com/
- http://www.verisign.com/products/site/

Το πρωτόκολλο SSL είναι ένα πρωτόκολλο αίτησης / απάντησης που βασίζεται στη χρήση της μεθόδου Δημόσιου και Ιδιωτικού κλειδιού.

Η διαδικασία ταυτοποίησης με τη χρήση του πρωτοκόλλου είναι η εξής:

- Αρχικά ο Client συνδέεται με τον Server
- Στη συνέχεια ο Server αποστέλλει το ψηφιακό πιστοποιητικό μαζί με το Δημόσιο κλειδί.
- Ο Client και ο Server συμφωνούν στο βαθμό κρυπτογράφησης (40 ή 128 bits).
- Ο Client δημιουργεί ένα Κλειδί Συνόδου (session key) το οποίο κρυπτογραφεί με τη χρήση του Δημοσίου Κλειδιού του server και το αποστέλλει στον Server.
- Τέλος, ο Server αποκρυπτογραφεί το Κλειδί Συνόδου με τη χρήση του δικού του Ιδιωτικού Κλειδιού.

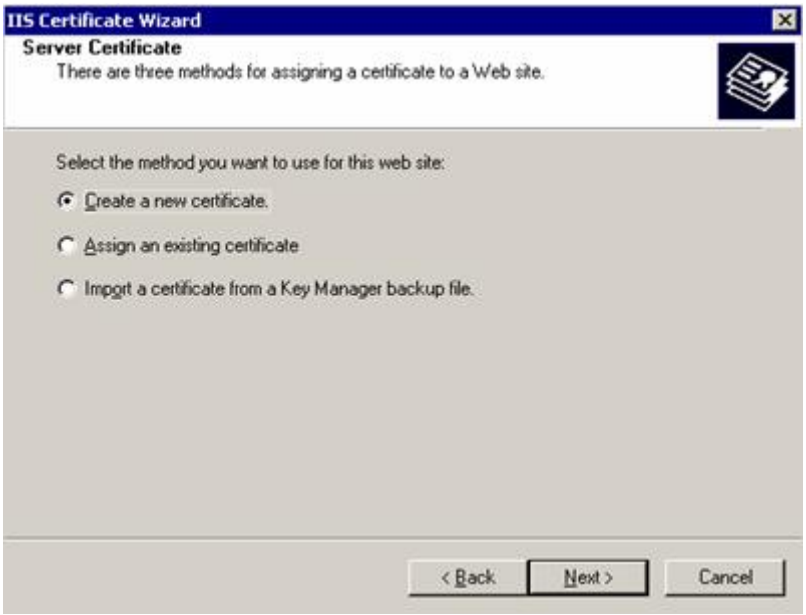
Στη συνέχεια, θα περιγράψουμε τον τρόπο με τον οποίο ένας web server αιτείται για την έκδοση ενός ψηφιακού πιστοποιητικού και την εγκατάστασή του για τη χρήση του μέσα από την επιλογή Server Certificate στο τμήμα Secure Communications στην καρτέλα Directory Security.

3.7.1 Έκδοση Πιστοποιητικού

Για την απόκτηση ενός ψηφιακού πιστοποιητικού πρέπει να δημιουργηθεί και αποσταλλεί μια αίτηση CSR (Certificate Signing Request). Πατώντας την επιλογή Server Certificate στο τμήμα Secure Communications στην καρτέλα Directory Security, ξεκινάει ο οδηγός έκδοσης ψηφιακού πιστοποιητικού όπως φαίνεται και στη **Εικόνα 57.**

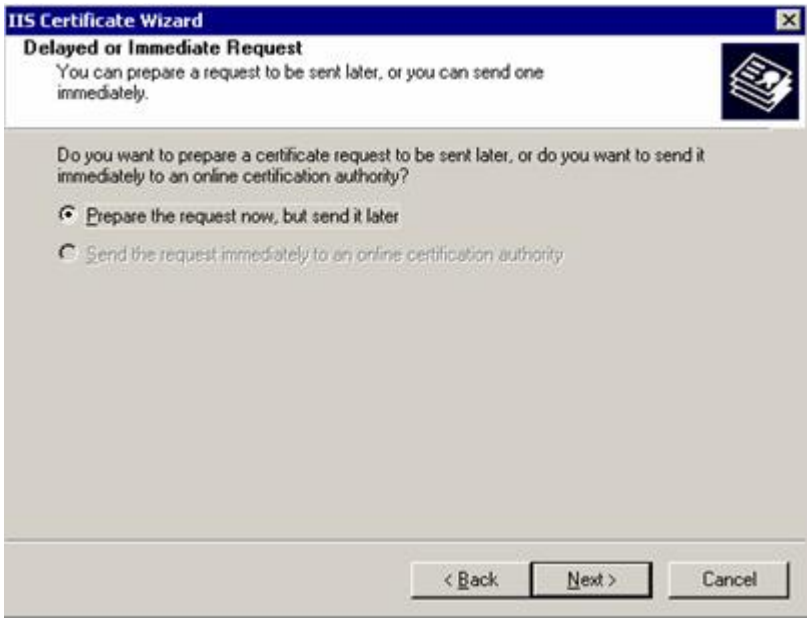
Εικόνα 57. *Οδηγός Πιστοποιητικού*

Πατώντας το κουμπί Next εμφανίζεται η φόρμα της **Εικόνας 58** όπου επιλέγουμε τη δημιουργία νέου πιστοποιητικού με την επιλογή *Create a new certificate* και πατάμε το Next.



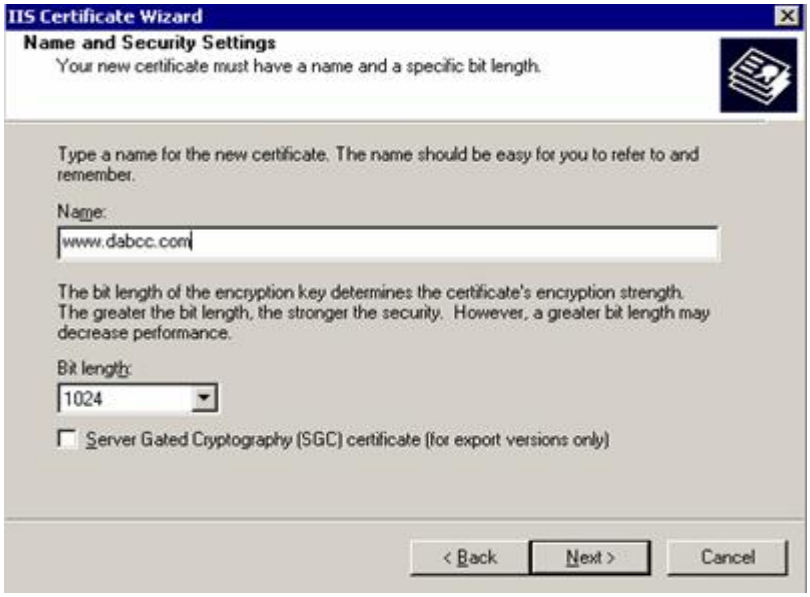
Εικόνα 58.

Στο επόμενο Βήμα **(Εικόνα 59)** επιλέγουμε την προετοιμασία της αίτησης και αποστολή της αργότερα με την επιλογή *Prepare the request now, but send it later* και πατάμε Next.



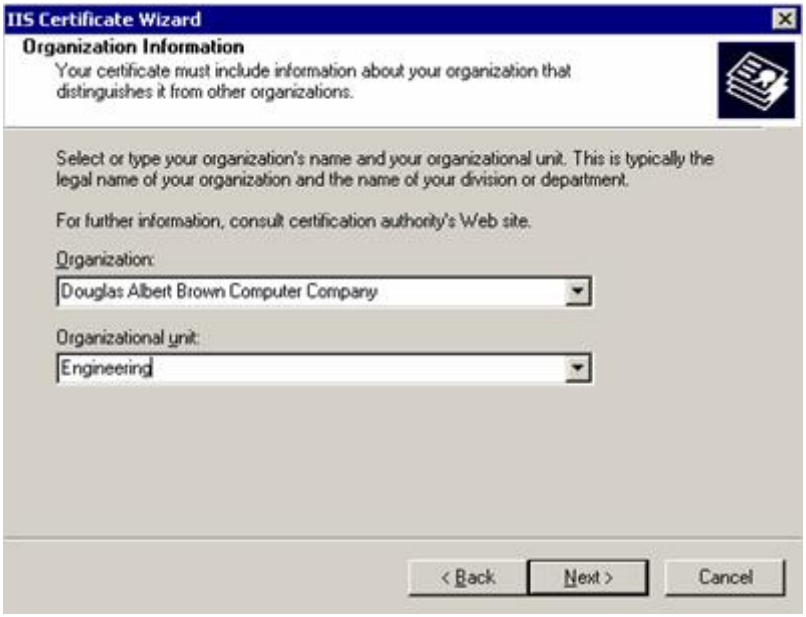
Εικόνα 59.

Στη φόρμα που ακολουθεί στην **Εικόνα 60** και στο πεδίο Name and Security Settings πληκτρολογούμε ένα όνομα για το νέο πιστοποιητικό και το μήκος του από το οποίο εξαρτάται και ο βαθμός ασφαλείας και πατάμε την επιλογή Next.



Εικόνα 60.

Στην συνέχεια όπως φαίνεται και στην **Εικόνα 61** εισάγουμε το ακριβές όνομα του οργανισμού που αιτείται το ψηφιακό πιστοποιητικό και το τμήμα και στη συνέχεια πατάμε το Next

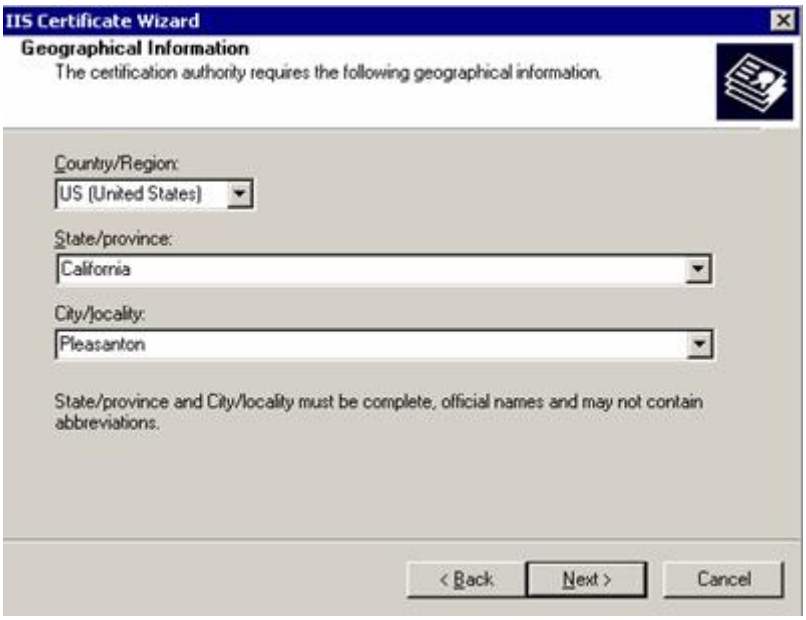


Εικόνα 61.

Στο παράθυρο της **Εικόνας 62** εισάγουμε το ακριβές όνομα του domain του δικτυακού μας τόπου στο πεδίο Common Name.

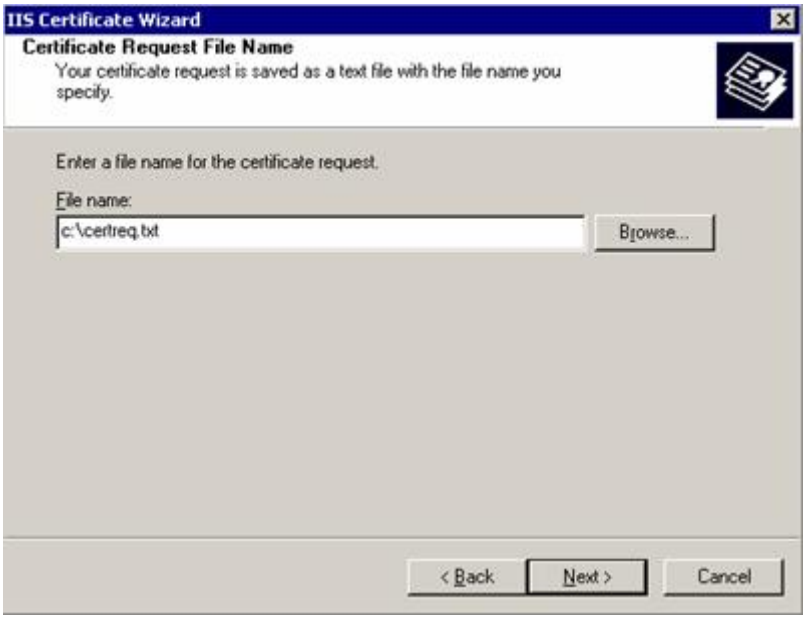
Εικόνα 62.

Στην επόμενη φόρμα **(Εικόνα 63)** εισάγουμε τη διεύθυνσή μας στα πεδία Country/Region , State/province, και City/locality και στη συνέχεια πατάμε *Next.*



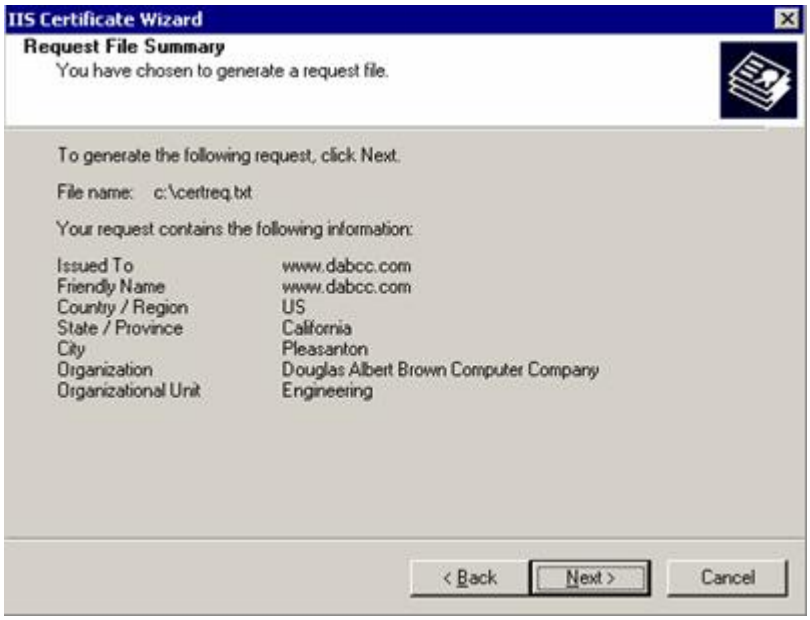
Εικόνα 63.

Στη φόρμα της **Εικόνας 64** πληκτρολογούμε τη διαδρομή και το όνομα στον τοπικό δίσκο του server όπου θα αποθηκευτεί η αίτηση CSR.



Εικόνα 64.

Τέλος, όπως φαίνεται και στην **Εικόνα 65** λαμβάνουμε μια επιβεβαίωση της αίτησης που είναι αποθηκευμένη στο δίσκο και πατάμε Next.



Εικόνα 65.

Στην τελευταία οθόνη του Οδηγού **(Εικόνα 66)** πατάμε Finish για να ολοκληρωθεί η διαδικασία.

Εικόνα 66. Ολοκλήρωση Οδηγού

3.7.2 Εγκατάσταση Πιστοποιητικού

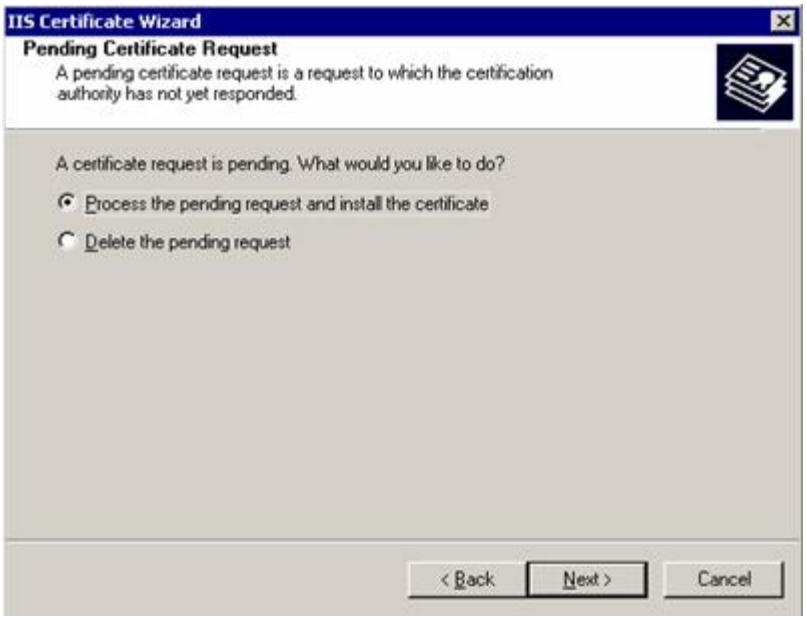
Για την παραλαβή και εγκατάσταση του πιστοποιητικού υπάρχουν δύο τρόποι:

- Αποστολή του αρχείου CSR σε ένα δημόσιο Φορέα Πιστοποίησης (CA)
- Χρήση του Microsoft Certificate Server του IIS 5.0

Στην πρώτη περίπτωση αποστέλλουμε το αρχείο CSR στο δημόσιο Φορέα Πιστοποίησης (CA) που επιθυμούμε και αυτός με τη σειρά του μας αποστέλλει ένα email με το πιστοποιητικό το οποίο είναι μια ακολουθία χαρακτήρων μήκους 1024 bits. Αντιγράφουμε την ακολουθία αυτή και κατόπιν την επικολλούμε σε ένα αρχείο κειμένου σε μια συγκεκριμένη θέση στο δίσκο. Στη συνέχεια, ξεκινάμε την διαδικασία εγκατάστασης του πιστοποιητικού. Στη συνέχεια μέσα από τον IIS και από την καρτέλα **Directory Security** πατάμε το κουμπί *Server Certificate* και ξεκινάμε τον Οδηγό Εγκατάστασης του πιστοποιητικού όπως φαίνεται και στην **Εικόνα 67**.

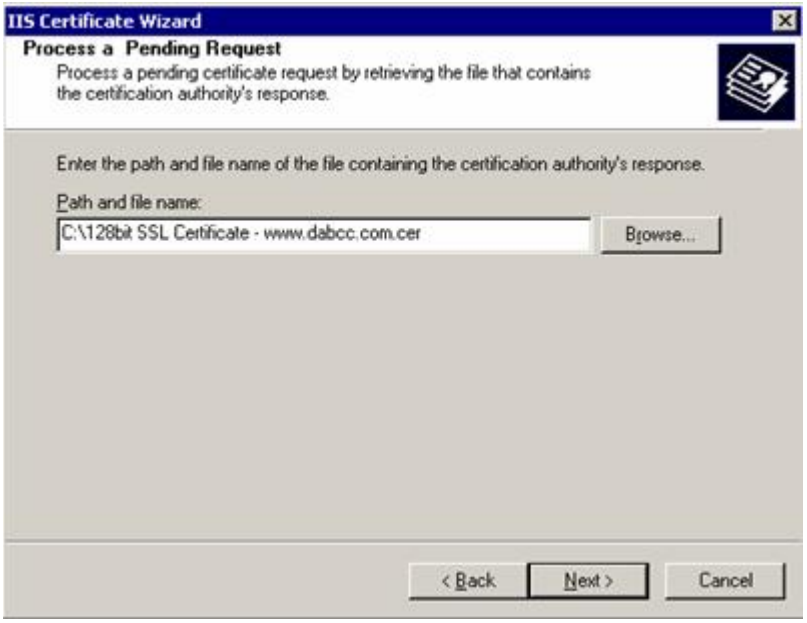
Εικόνα 67. Οδηγός Παραλαβής Πιστοποιητικού

Πατώντας Next προχωράμε στην επόμενη οθόνη **(Εικόνα 68)** όπου επιλέγουμε *Process the pending request and install the certificate* και πατάμε Next.



Εικόνα 68.

Τέλος, εισάγουμε τη θέση στην οποία αποθηκεύσαμε το αρχείο κειμένου με την ακολουθία του πιστοποιητικού και πατάμε Next.



Εικόνα 69.

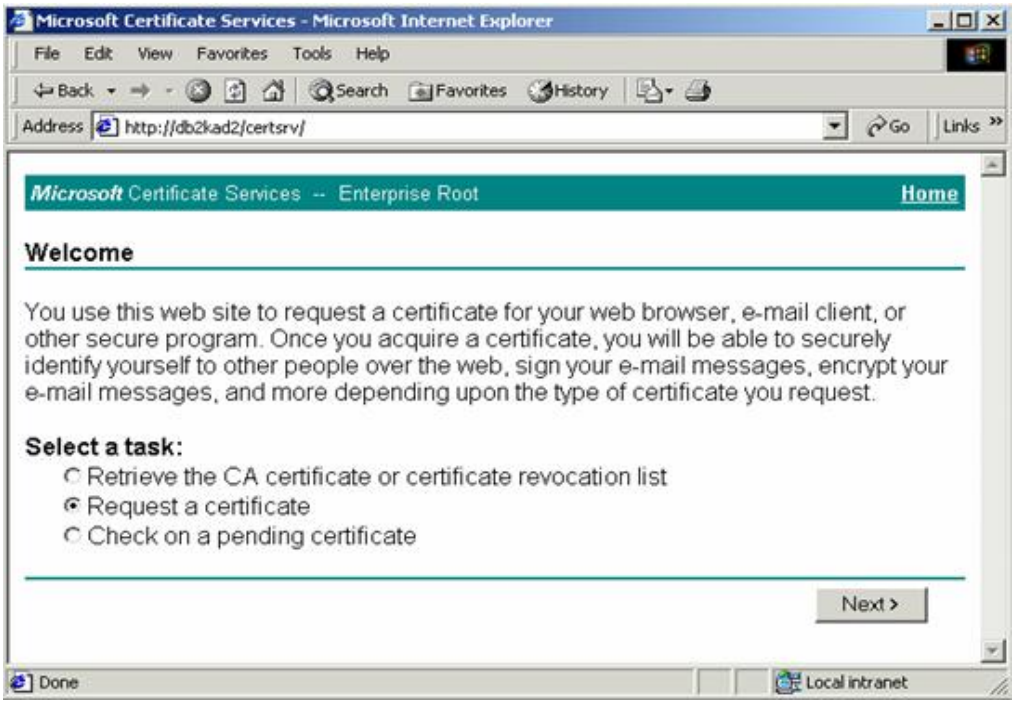
Τέλος, εμφανίζεται μια αναφορά επικύρωσης και πατώντας Next εμφανίζεται η τελική οθόνη του Οδηγού όπου πατάμε Finish για να ολοκληρωθεί η διαδικασία. Το πιστοποιητικό έχει ήδη εγκατασταθεί και μπορεί να χρησιμοποιηθεί είτε για την

ταυτοποίηση χρηστών ή για τη χρήση του πρωτοκόλλου HTTPS ασφαλούς σύνδεσης με τον server.

Όπως ήδη είπαμε, το πιστοποιητικό μπορεί εναλλακτικά να παραληφθεί και να εγκατασταθεί με τη χρήση του Microsoft Certificate Server. Η υπηρεσία αυτή που είναι μέρος του IIS 5.0 μας δίνει τη δυνατότητα να εγκαταστήσουμε το ψηφιακό πιστοποιητικό μέσα από τον web browser του υπολογιστή και στην τοποθεσία http://servername/certserv , όπου servername είναι το domain όνομα του δικτυακού μας τόπου.

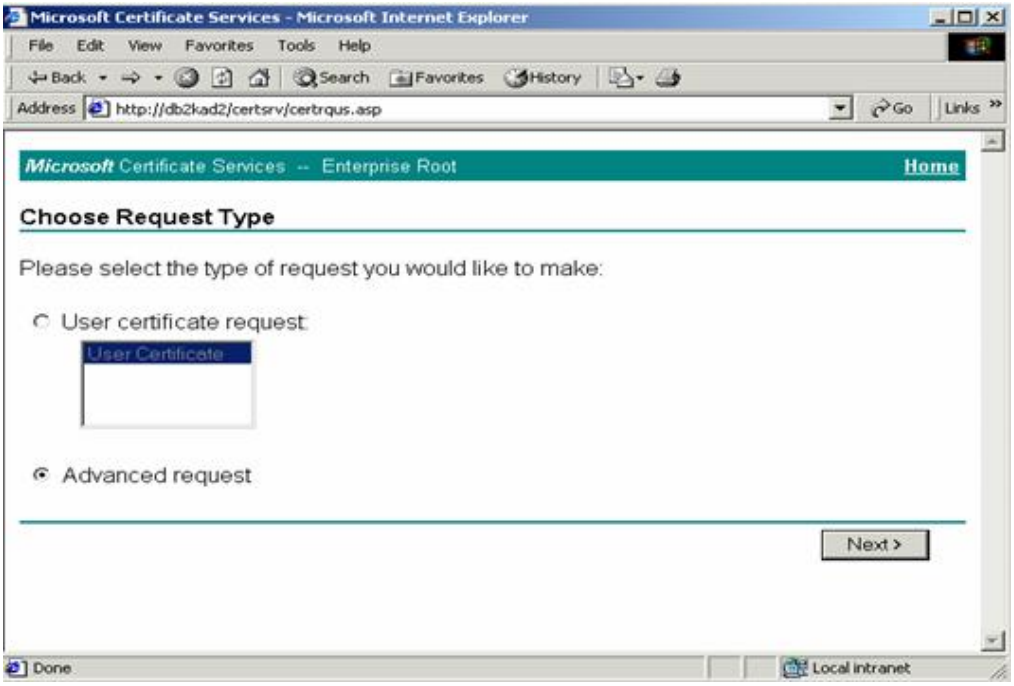
Συνεπώς αντί να αποστείλουμε την CSR αίτηση προς το Φορέα Πιστοποίησης ακολουθούμε την εξής διαδικασία:

Αρχικά, ανοίγουμε τον Internet Explorer και πληκτρολογούμε τη διεύθυνση του Certificate Server (http://mywebserver/certserv). Στη συνέχεια, εμφανίζεται η οθόνη της **Εικόνας 70** όπου επιλέγουμε *Request a certificate* και πατάμε Next



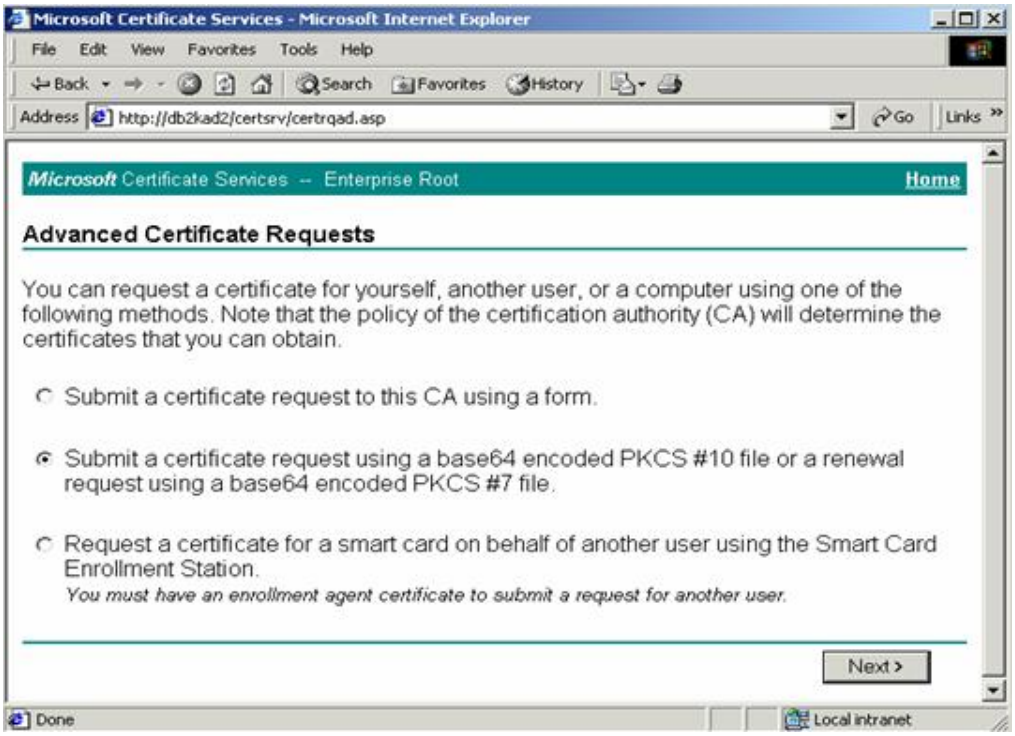
Εικόνα 70.

Στη συνέχεια, **(Εικόνα 71)** επιλέγουμε *Advanced request* και πατάμε *Next*



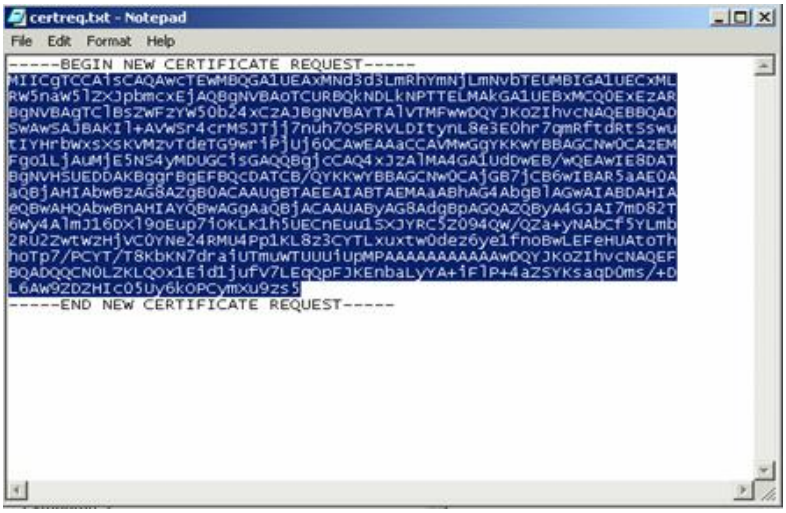
Εικόνα 71.

Επιλέγουμε, *Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file* **(Εικόνα 72)** και πατάμε Next.



Εικόνα 72.

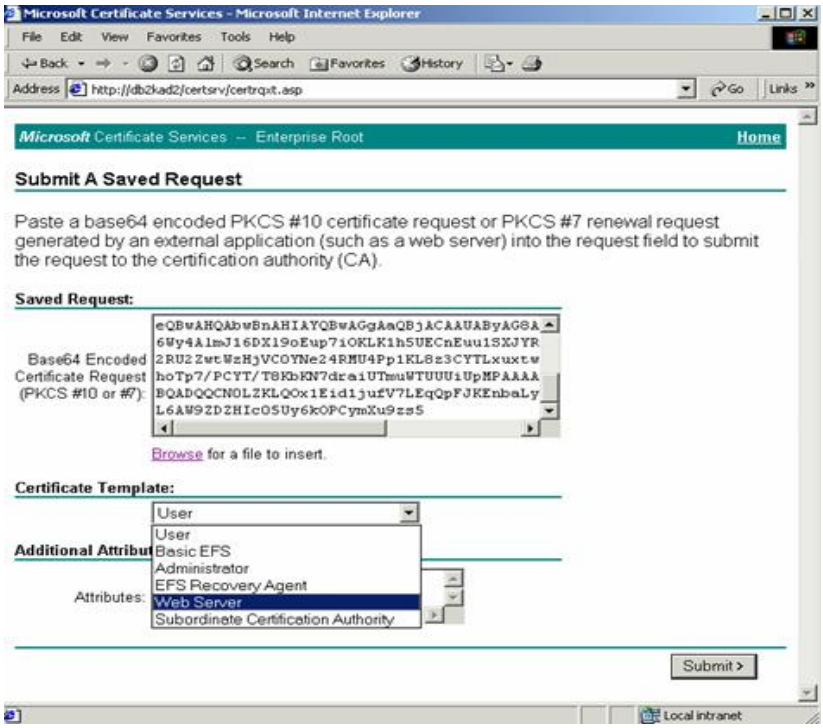
Στη συνέχεια, ανοίγουμε το αρχείο της αίτησης CSR (certreq.txt) που είχαμε αποθηκεύσει κατά τη διαδικασία δημιουργίας της αίτησης στον τοπικό δίσκο και αντιγράφουμε την ακολουθία των χαρακτήρων μέσα από το αρχείο.



Εικόνα 73.

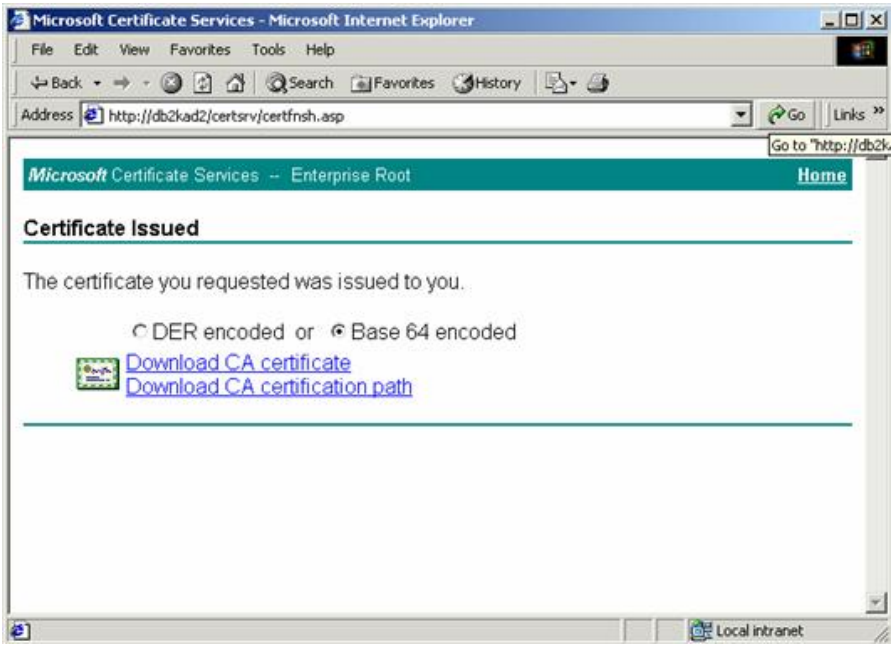
Στην οθόνη που έχει εμφανιστεί στον web browser και στο πεδίο Base64 Encoded Certificate Request κάνουμε επικόλληση του κειμένου και επιλέγουμε την τιμή Web Server από το μενού Certificate Template όπως φαίνεται και στην Εικόνα.74

Στη συνέχεια πατάμε Submit.



Εικόνα 74.

Στην οθόνη που εμφανίζεται επιλέγουμε την κωδικοποίηση που θα χρησιμοποιηθεί από την επιλογή *Base 64 encoded* και στη συνέχεια πατάμε *Download CA certificate* για την απόκτηση του πιστοποιητικού όπως φαίνεται και στην **Εικόνα 75.**



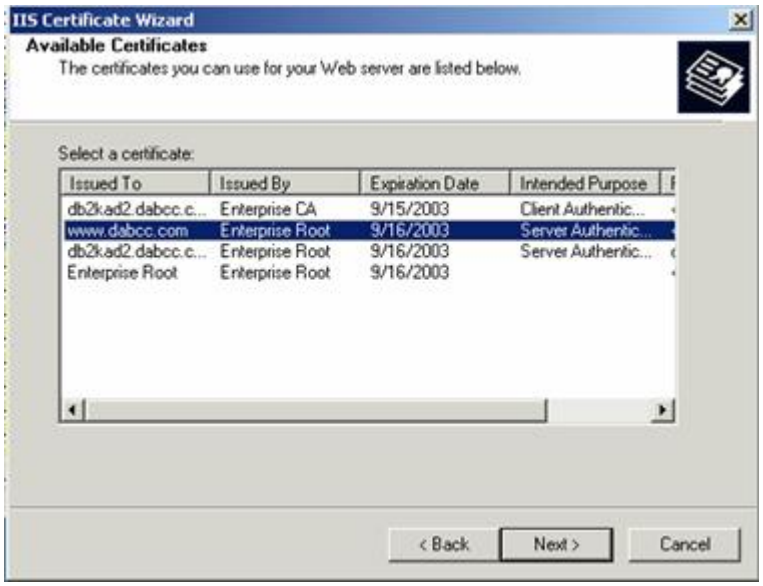
Εικόνα 75.

Αποθηκεύουμε το πιστοποιητικό όπως φαίνεται και στην **Εικόνα 76** με το όνομα του web server μας σε κάποια θέση στον δίσκο.

Εικόνα 76.

Τέλος, κάνοντας δεξί κλικ στο αποθηκευμένο πιστοποιητικό επιλέγουμε *Install Certificate* για την εγκατάστασή του.

Από την επιλογή *Server Certificate* στο τμήμα Secure Communications στην καρτέλα **Directory Security** μέσα από τον IIS, όπως φαίνεται και στην Εικόνα επιλέγουμε *Assign an existing certificate* και πατάμε Next. Στη συνέχεια από τη λίστα των πιστοποιητικών που εμφανίζεται **(Εικόνα 77)** επιλέγουμε το πρόσφατα εγκατεστημένο και πατάμε *Next*.



Εικόνα 77.

Η διαδικασία ολοκληρώνεται και το πιστοποιητικό είναι έτοιμο προς χρήση. Ο έλεγχος της ενεργοποίησης του πρωτοκόλλου SSL μπορεί να γίνει μέσα από τον web server μας με έλεγχο της https επικοινωνίας. Για τον έλεγχο αυτό δημιουργούμε μια απλή ιστοσελίδα HTML ή ASP (π.χ. test.htm) και την αποθηκεύουμε στον κατάλογο του δικτυακού μας τόπου.

Στη συνέχεια ανοίγοντας τον web browser πληκτρολογούμε τη διεύθυνση της ιστοσελίδας που συνήθως είναι www.myserver.com/test.html όπου myserver.com είναι το όνομα του δικτυακού μας τόπου και test.htm είναι το όνομα της ιστοσελίδας. Αντί όμως της χρήσης του πρωτοκόλλου http:// πληκτρολογούμε το πρωτόκολλο https:// το οποίο κοινοποιεί στον web server ότι η επικοινωνία πρέπει να γίνει με τη χρήση ασφαλούς σύνδεσης SSL. Αν το πιστοποιητικό έχει εγκατασταθεί επιτυχώς τότε στη γραμμή κατάστασης του web browser θα εμφανιστεί η χαρακτηριστική κλειδαριά που αντιστοιχεί στην ασφαλή σύνδεση.

ΕΠΙΛΟΓΟΣ

Ο IIS είναι όπως είπαμε ένας από τους πιο διαδεδομένους web servers ο οποίος εξελίσσεται συνέχεια. Νέα στοιχεία προστίθενται στις καινούριες εκδόσεις και σε πολλά σημεία η Microsoft έχει προχωρήσει σε ριζικές αλλαγές στην αρχιτεκτονική του web server της. Ο ανταγωνισμός με τον επίσης πολύ διαδεδομένο Apache server έχει οδηγήσει σε βελτίωση των χαρακτηριστικών και της σχεδίασής του.

ΜΕΙΟΝΕΚΤΗΜΑΤΑ & ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥ IIS

Τα βασικά **μειονεκτήματα** των εκδόσεων του IIS 5.1 και προγενέστερων είχαν να κάνουν με τη σχεδίαση του server όσον αφορά στην αρχιτεκτονική του. Σε σύγκριση με την αρχιτεκτονική του Apache server που παρουσίαζε στο παρελθόν πολλά μειονεκτήματα.

Ο Apache server στηριζόταν στην τμηματική αρχιτεκτονική (modular) όπου οι υπηρεσίες και οι δυνατότητες προσθέτονταν πάνω σε μια κύρια εφαρμογή σαν ξεχωριστά modules. Το μοντέλο αυτό υλοποιήθηκε στην περίπτωση του IIS από την έκδοση 6.0 και μετά. Το μεγάλο *πλεονέκτημα* του Apache είναι ότι βασίζεται σε μια κεντρική εφαρμογή η οποία καλεί ένα τμήμα της εφαρμογής για την εξυπηρέτηση των εισερχομένων κλήσεων από τους clients. Σε περίπτωση που κάτι συμβεί στην εξυπηρέτηση από το συγκεκριμένο τμήμα και αυτή διακοπεί τότε μια νέα διαδικασία δημιουργείται για να εξυπηρετήσει τελικά τον client.

Σε εκδόσεις προηγούμενες του IIS 6.0 αυτό το μοντέλο πολλαπλής εξυπηρέτησης δεν ήταν δυνατό να υλοποιηθεί με αποτέλεσμα αν για κάποιο λόγο σταματούσε η εξυπηρέτηση των client , ο web server έβγαινε εκτός λειτουργίας.

Το βασικό πρόβλημα του IIS είναι ότι η υλοποίησή του στηρίζεται σε μεγάλο βαθμό στην αρχιτεκτονική του λειτουργικού συστήματος και κυρίως στον πυρήνα αυτού (kernel) κάτι που δεν ισχύει για τον Apache ο οποίος είναι σε μεγάλο βαθμό υλοποιημένος ανεξάρτητα με τη λειτουργία τους συστήματος, μπορεί πολύ εύκολα να επεκταθεί.

Τέλος, το μεγαλύτερο και πιο σοβαρό πρόβλημα που είχαν να αντιμετωπίσουν οι παλαιότερες εκδόσεις του IIS ήταν οι αδυναμίες του στο θέμα της ασφάλειας. Ο IIS και γενικότερα τα Windows αντιμετώπισαν στο παρελθόν πολύ μεγάλα προβλήματα

από διάφορες επιθέσεις όπως ιούς, hackers, υποκλοπές μεταδόσεων κα. Ο Apache server ήταν ανέκαθεν πιο ασφαλής και παρουσίαζε λιγότερα προβλήματα ασφαλείας από ότι ο IIS.

Το βασικό **πλεονέκτημα** του IIS είναι ότι αποτελεί ένα προϊόν της Microsoft απόλυτα συμβατό με τα Windows. Εκμεταλλεύεται την καθολική διάδοση του λειτουργικού συστήματος Windows στους υπολογιστές παγκοσμίως με αποτέλεσμα να είναι εύκολα προσβάσιμος και να βρίσκεται εγκατεστημένος, αν και όχι προεπιλεγμένα, στην πλειοψηφία των server εκδόσεων των Windows. Προσφέρει επίσης ένα γραφικό περιβάλλον διαχείρισης φιλικό προς τους διαχειριστές και ειδικότερα προς αυτούς που είναι εξοικειωμένοι με την πλατφόρμα των Windows.

Είναι γεγονός ότι στο παρελθόν αντιμετώπισε αρκετά προβλήματα ειδικά στον τομέα της ασφάλειας αλλά από την νέα έκδοση του IIS, την έκδοση 6.0 για τα Windows Server 2003 και Windows XP Professional x64 Edition καθώς και την αναμενόμενη έκδοση 7.0 των Windows Vista έχουν γίνει σημαντικές βελτιώσεις σε όλους τους τομείς. Όπως και σε παλαιότερες εκδόσεις έτσι και στην έκδοση 6.0 η αρχιτεκτονική του IIS δεν ήταν τμηματική αλλά όλες οι δυνατότητες υλοποιούνταν από ένα dll. Ουσιαστικά η νέα έκδοση 6.0 είχε σημαντικές αλλαγές στη σχεδίαση του γραφικού περιβάλλοντος παρά στην αρχιτεκτονική του λογισμικού.

ΜΕΛΛΟΝΤΙΚΕΣ ΒΕΛΤΙΩΣΕΙΣ

Στο **μέλλον** οι νέες εκδόσεις του IIS θα στηρίζονται περισσότερο στο μοντέλο ανάπτυξης τμημάτων στο οποίο στηρίζεται και ο Apache. Χαρακτηριστικά όπως η Βασική Ταυτοποίηση (Basic Authentication) και η συμπίεση θα υλοποιούνται από ξεχωριστά modules τα οποία θα μπορούν να προστεθούν ή να αφαιρεθούν αυξάνοντας ή αντίστοιχα μειώνοντας τη λειτουργικότητα. Επίσης η αρχιτεκτονική αυτή μπορεί να δώσει τη δυνατότητα σε προγραμματιστές να δημιουργήσουν τμήματα του server που θα επεκτείνουν τις δυνατότητες του όπως συμβαίνει και στον Apache.

Όσον αφορά την **ασφάλεια,** οι βελτιώσεις που έγιναν στην έκδοση 6.0 ήταν σημαντικές. Παρ' όλα αυτά στο μέλλον υπάρχουν πολλές σημαντικές βελτιώσεις στην ασφάλεια εκτέλεσης .NET εφαρμογών. Ο IIS 6.0 χειρίζεται τις ASP.net εφαρμογές σαν μια επέκταση ISAPI ενώ η αντιμετώπισή του στη μελλοντική έκδοση IIS 7.0 θα είναι πιο άμεση δίχως να αφήνει λιγότερα κενά σε θέματα ασφαλείας. Επίσης, η ταχύτητα του server αναμένεται να αυξηθεί σημαντικά ειδικά στις http υπηρεσίες του

παγκόσμιου ιστού. Μια άλλη σημαντική αλλαγή είναι η δυνατότητα εξυπηρέτησης περισσότερων από έναν δικτυακών τόπων, πρόβλημα που αντιμετώπιζε ο IIS 5.1.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερασματικά θα μπορούσαμε να πούμε ότι ο IIS είναι ένα πλήρες εργαλείο εξυπηρέτησης υπηρεσιών Διαδικτύου και φιλοξενίας δικτυακών τόπων που όμως στο παρελθόν αντιμετώπισε αρκετά προβλήματα λόγω της κακής σχεδίασής του αλλά που συνεχώς βελτιώνεται από έκδοση σε έκδοση. Η επιλογή του IIS 5.1 για την εγκατάσταση και παραμετροποίηση του, έγινε με βάση το γεγονός ότι αποτελεί την πιο διαδεδομένη έκδοση του IIS.

Το μεγάλο πλεονέκτημά του είναι ότι είναι το περιβάλλον διεπαφής με το χρήστη είναι πολύ φιλικό και η πλειοψηφία των χρηστών είναι πολύ εξοικειωμένοι με αυτό, λόγω της προηγούμενης εμπειρίας τους στη χρήση των MMC εργαλείων και γενικότερα του περιβάλλοντος των Windows. Η χρήση του είναι πολύ εύκολη ακόμα και για έναν αρχάριο διαχειριστή ο οποίος μπορεί να θέσει σε λειτουργία την υπηρεσία WWW χωρίς να έχει προηγούμενη γνώση και με τις ελάχιστες οδηγίες χρήσης. Παρ' όλα αυτά η ευκολία αυτή εγκυμονεί πολλούς κινδύνους όσον αφορά στην ασφάλεια του συστήματος και των δεδομένων. Και αυτό γιατί οι προεπιλογές κατά την απλή εγκατάσταση του IIS αφήνουν πολλά κενά στην ασφάλεια του server και δίνουν τη δυνατότητα σε τρίτους για κακόβουλες επιθέσεις κατά του δικτυακού μας τόπου. Η σωστή και προσεκτική παραμετροποίηση του server λαμβάνοντας σοβαρά υπόψη κάποιο πλαίσιο κανόνων ασφαλείας μπορεί να εγγυηθεί την ασφαλή δημοσίευση των δεδομένων και των περιεχομένων του web server στο Διαδίκτυο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- www.google.gr
- http//:www.microsoft.com
- Andrew Tanenbaum "Computer Network", εκδόσεις ΚΛΕΙΔΑΡΕΙΘΜΟΣ
- Joe Casad, 'Μάθετε το TCP / IP σε 24 Ώρες", εκδόσεις Μ. Γκιούρδας
- William E. Walker IV, Sheila M. Christman, "Guide to the secure Configuration and Afdministration of Microsoft Internet Information Services 5.0"