

File Transfer Protocol

Το File Transfer Protocol (FTP), (στα ελληνικά Πρωτόκολλο Μεταφοράς Αρχείων) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο για τη μεταφορά αρχείων σε δίκτυα αρχιτεκτονικής TCP/IP. Η εφαρμογή αποτελείται από δύο κομμάτια, αυτό του εξυπηρετητή (server) και αυτό του πελάτη (client). Ο υπολογιστής που τρέχει την εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κ.ο.κ. Το πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα.

1. Τρόπος λειτουργίας

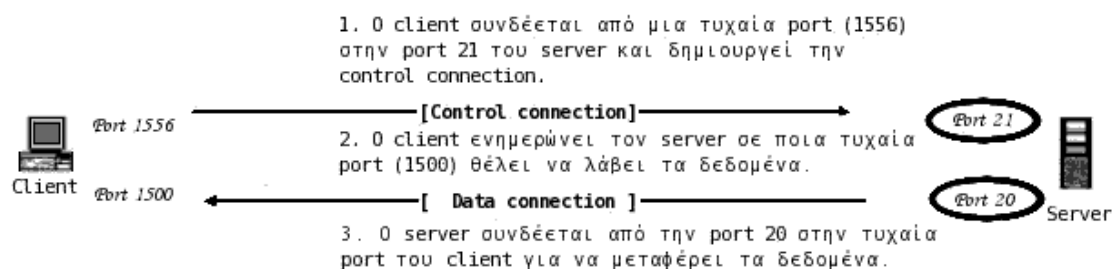
Αρχικά ο FTP server ανοίγει την θύρα (port) 21 περιμένοντας έναν FTP client να συνδεθεί. Στη συνέχεια ο client ξεκινά μια νέα σύνδεση από μια τυχαία θύρα προς την θύρα 21 του server. Μόλις γίνει η σύνδεση παραμένει ανοιχτή για όλη τη διάρκεια της συνόδου FTP. Η συγκεκριμένη σύνδεση ονομάζεται σύνδεση ελέγχου (control connection) και χρησιμοποιείται για τη μεταφορά εντολών.

Ακολουθεί η δημιουργία της σύνδεσης δεδομένων (data connection), δηλ. της σύνδεσης με την οποία μεταφέρονται τα δεδομένα των αρχείων. Υπάρχουν δύο τρόποι για να δημιουργηθεί μια τέτοια σύνδεση: με χρήση της ενεργητικής λειτουργίας (active mode) ή με χρήση της παθητικής λειτουργίας (passive mode).

1.1. Active mode

Στην ενεργητική λειτουργία (active mode) ο FTP client διαλέγει μια τυχαία θύρα στην οποία δέχεται τα δεδομένα της σύνδεσης. Ο client στέλνει τον αριθμό της θύρας, στην οποία επιθυμεί να "ακούει" (listen) για εισερχόμενες συνδέσεις. Ο FTP server δημιουργεί μια σύνδεση από την θύρα 20 στην ανοιχτή θύρα του client για τη μεταφορά των δεδομένων.

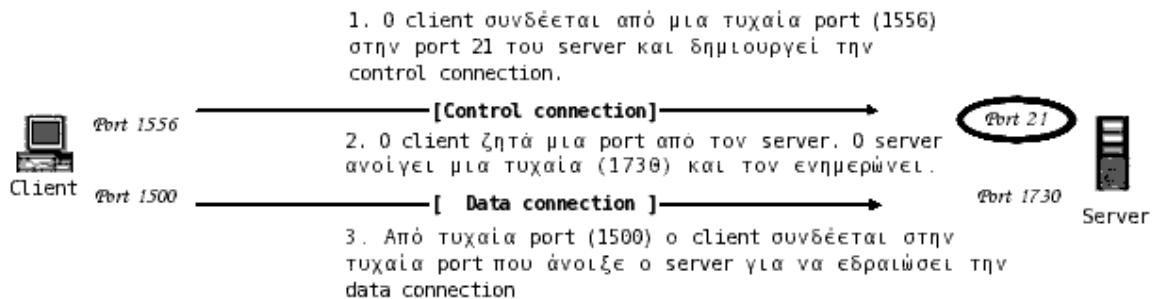
Οποιαδήποτε πληροφορία ζητήσει ο client, ανταλλάσσεται με βάση αυτή τη σύνδεση, που βασίζεται στο TCP. Όταν η μεταφορά ολοκληρωθεί ο server κλείνει τη σύνδεση. Κάθε φορά που ο client ζητάει δεδομένα, δημιουργείται κατά παρόμοιο τρόπο μια σύνδεση δεδομένων και η διαδικασία επαναλαμβάνεται.



Active mode

1.2. Passive mode

Στην παθητική λειτουργία (passive mode) ο client ζητά από τον server να διαλέξει μια τυχαία θύρα, στην οποία θα "ακούει" (listen) για την σύνδεση δεδομένων (data connection). Ο server ενημερώνει τον client για την θύρα την οποία έχει διαλέξει και ο client συνδέεται σε αυτή για τη μεταφορά των δεδομένων. Η μεταφορά ολοκληρώνεται όπως και στην ενεργητική λειτουργία (active mode), αφού η σύνδεση δεδομένων βασίζεται στο TCP. Η βασική δηλαδή διαφορά μεταξύ των δύο καταστάσεων λειτουργίας είναι ότι στην ενεργητική λειτουργία ο server δημιουργεί τη σύνδεση δεδομένων στον client, ενώ στην παθητική λειτουργία συμβαίνει το αντίστροφο.



Passive mode

2. Χρήση

Το FTP είναι ένα πρωτόκολλο πελάτη-εξυπηρετητή, ικανό να χειρίζεται οποιονδήποτε τύπο αρχείου χωρίς περαιτέρω επεξεργασία. Ωστόσο το FTP έχει εξαιρετικά υψηλή καθυστέρηση (latency). Αυτό σημαίνει ότι ο χρόνος μεταξύ του αιτήματος και της διαδικασίας παραλαβής του είναι αρκετά μεγάλος και για αυτό διότι μερικές φορές απαιτείται μεγάλη διαδικασία σύνδεσης.

2.1. Anonymous FTP

Το FTP εκτός από τους πιστοποιημένους χρήστες μπορεί να επιτρέψει και σε μια νέα κατηγορία χρηστών να συνδέονται στον FTP server. Οι χρήστες αυτοί δεν χρειάζεται να έχουν λογαριασμό, αντιθέτως χρησιμοποιούν έναν λογαριασμό γενικής χρήσης. Ο λογαριασμός αυτός ονομάζεται "anonymous FTP" και δεν απαιτεί κωδικό πρόσβασης, συνήθως όμως χρησιμοποιείται κατά σύμβαση ο κωδικός "guest" ή η διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail) του χρήστη.

Η σύνδεση "anonymous" χρησιμοποιείται κυρίως για αρχεία που είναι ανοιχτά στο κοινό, σαν αποθήκη πληροφοριών (όπως λογισμικό, έγγραφα, εικόνες κλπ.) Συνήθως, με αυτό τον τρόπο παρέχεται πρόσβαση σε αρχειοθετημένες mailing lists. Οι χρήστες που εισέρχονται ως "anonymous" πρέπει να έχουν περιορισμένα δικαιώματα πρόσβασης σε αρχεία του host. Διαφορετικά, εάν μπορούν να διαβάσουν οποιοδήποτε αρχείο ή να δημιουργήσουν νέα, δημιουργούνται προβλήματα ασφαλείας.

3. Ασφάλεια

Το FTP δεν σχεδιάστηκε με πρόνοια για ασφάλεια, με συνέπεια οι εφαρμογές να είναι ιδιαίτερα ευάλωτες και να εμφανίζονται ποικίλα προβλήματα κατά τη χρήση firewall ή NAT.

3.1. Προβλήματα NAT

Στην ενεργητική λειτουργία ο FTP server ξεκινά μια σύνδεση δεδομένων συνδεόμενος στην εξωτερική διεύθυνση IP της πύλης (gateway) NAT. Στην άλλη πλευρά, το μηχάνημα το οποίο είναι υπεύθυνο για τη "μετάφραση" των εσωτερικών διευθύνσεων IP του δικτύου στην εξωτερική, θα πάρει το πακέτο για τη δημιουργία της σύνδεσης. Όμως, στον πίνακα κατάστασης (state table) του NAT, στον οποίο διατηρείται το ιστορικό μεταφράσεων, δεν έχει καταγραφεί κανένα, με αποτέλεσμα το πακέτο να απορρίπτεται (γίνεται drop). Το πακέτο δεν φτάνει ποτέ στον client, δεν σχηματίζεται σύνδεση δεδομένων και η μεταφορά δεδομένων είναι αδύνατη.

Στην παθητική λειτουργία, επειδή η θύρα στην οποία συνδέεται ο server είναι τυχαία, είναι πιθανόν να μην επιτρέπεται σύνδεση προς τον αριθμό της από το λογισμικό - τείχος προστασίας (firewall). Σε αυτή την περίπτωση η σύνδεση δεδομένων δεν θα σχηματιστεί και, επομένως, δεν θα μεταφέρονται δεδομένα.

3.2. Έλλειψη κρυπτογράφησης

Τα δεδομένα που ανταλλάσσονται μέσω FTP δεν είναι κρυπτογραφημένα, με αποτέλεσμα οι εντολές που αποστέλλονται μέσω της control connection να είναι απλό κείμενο. Για το λόγο αυτό μπορούν εύκολα, με τη χρήση ενός sniffer, να αλιευθούν, να διαβασθούν και να ξανασταλούν ανάλογα με τη βούληση του επιτιθέμενου. Ανάμεσα σε αυτές, η εντολή που χρησιμοποιείται για να γίνει login σε ένα λογαριασμό FTP, με σύνταξη "PASS password", παρέχει στον επιτιθέμενο τον κωδικό του χρήστη. Αν συνδυαστεί με την εντολή "USER", με την οποία αποστέλεται το όνομα του χρήστη, ο επιτιθέμενος μπορεί να χρησιμοποιήσει τα στοιχεία για να εισέλθει στον ξένο λογαριασμό με τα ίδια δικαιώματα.

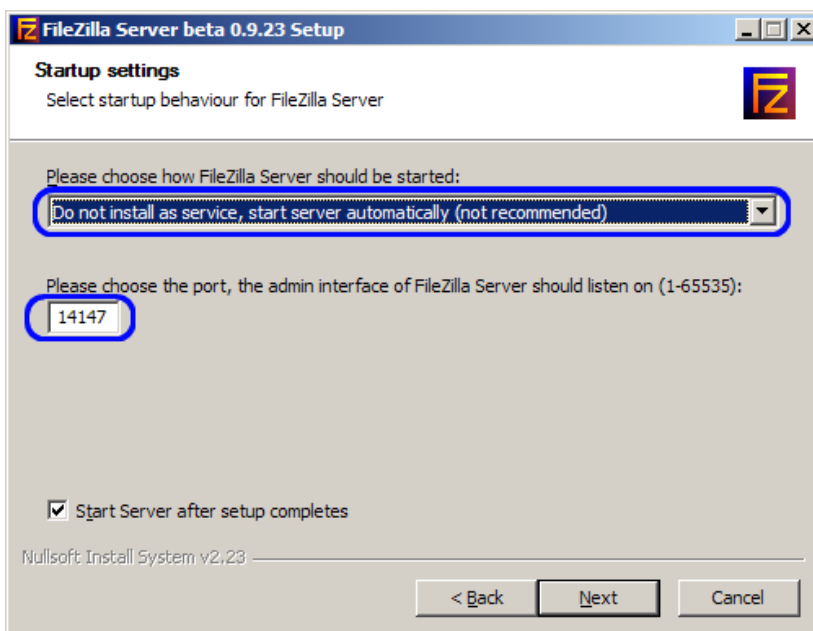
Επειδή οι περισσότεροι άνθρωποι τείνουν να επαναχρησιμοποιούν κωδικούς, ο επιτιθέμενος έχει αυξήσει τις πιθανότητες του σε μια brute-force attack. Με αυτό τον τρόπο, είναι πιθανό να αποκτήσει έλεγχο του συστήματος του χρήστη μόλις βρει τη διεύθυνση IP του, ανιχνεύοντας την έναρξη της συνόδου FTP (FTP session).

3.3. Επιθέσεις Man-in-the-middle

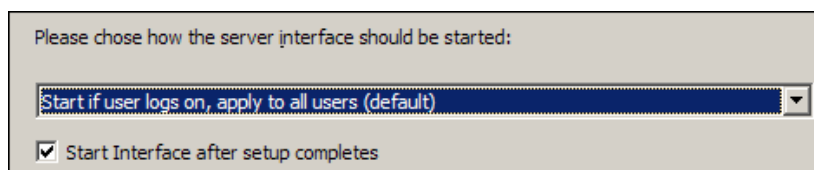
Με το File Transfer Protocol, ο server δεν εξασφαλίζει ότι ο client είναι αυτός που λέει, ούτε ο client αντίστοιχα για τον server. Ευκολονόητο, εφόσον το FTP δεν απαιτεί επαλήθευση των hosts και δεν ελέγχει αν τα δεδομένα προέρχονται από αυτούς, ούτε τα προστατεύει. Για αυτό το λόγο και τα δύο άκρα που ανταλλάσσουν δεδομένα, είναι ανοιχτά σε επιθέσεις man-in-the-middle από κάποιον επιτιθέμενο που συλλαμβάνει τα πακέτα του κάθε host, και στέλνει ψευδείς απαντήσεις. Σε ένα τέτοιο σενάριο θα μπορούσε κάποιος να εξαναγκάσει δύο server να επικοινωνήσουν απευθείας μεταξύ τους ανταλλάσσοντας μεγάλες ποσότητες δεδομένων (ο ένας download και ο άλλος upload) χωρίς αυτά να περνάν μέσα από κάποιον client. Η δημιουργία πολλών τέτοιων συνδέσεων μπορεί να έχει σαν αποτέλεσμα Άρνηση Παροχής Υπηρεσίας (Denial of Service – DDOS).

4. Εγκατάσταση του FileZilla Server

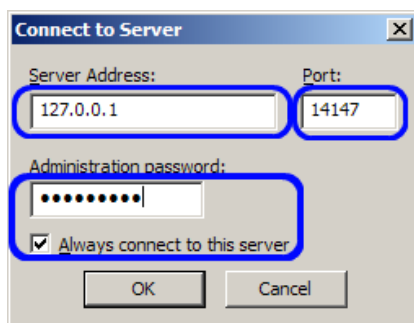
Τρέχουμε το εκτελέσιμο αρχείο της εγκατάστασης. Θα ερωτηθούμε σε κάποιο σημείο αν θέλουμε ο server να τρέχει ως service των Windows:



Η θύρα που φαίνεται σημειωμένη δεν έχει να κάνει με τον ίδιο τον server, αλλά είναι αυτή που θα χρησιμοποιεί το administration interface για να επικοινωνεί με τον server. Δε θα μας απασχολήσει κατά τη διαδικασία του port forwarding, αφού η επικοινωνία αυτή γίνεται τοπικά στο PC μας και η κίνηση δεν περνάει από τον router μας. Δίνουμε **Next**:

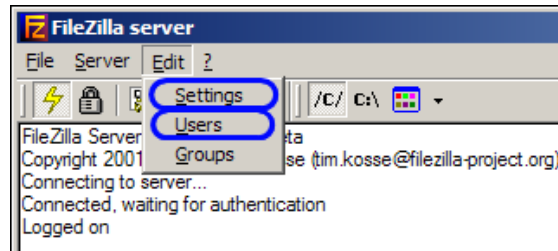


Εδώ αφήνουμε τα defaults και κλικ στο **Install**. Από εδώ και πέρα, όταν δεχόμαστε ερώτηση από το software firewall που έχουμε εγκατεστημένο σχετικά με τον FileZilla Server, θα πρέπει να επιτρέπουμε την κίνηση. Αμέσως θα φορτωθεί ο server και θα αντικρύσουμε την παρακάτω οθόνη:

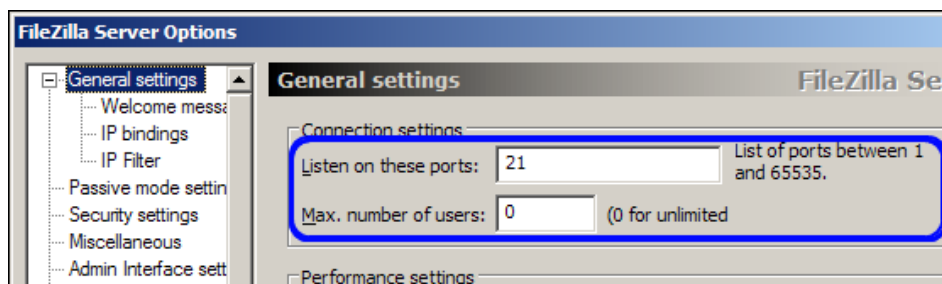


4.1. Ρυθμίσεις

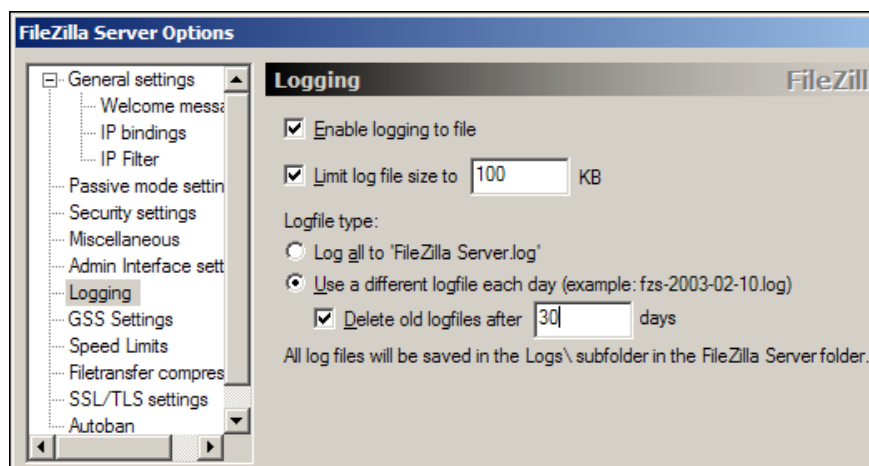
Εδώ γίνεται η σύνδεση του administration interface στον server. Ο server τρέχει τοπικά στο μηχάνημά μας, οπότε στο **Server Address** αφήνουμε τη διεύθυνση **127.0.0.1** (που είναι στα περισσότερα setups ισοδύναμη του **localhost**) και στη θύρα βάζουμε την ίδια τιμή με αυτήν που επιλέξαμε 2 οθόνες νωρίτερα. Συμπληρώνουμε με ένα password της αρεσκείας μας, βάζουμε tick στην από κάτω επιλογή και κλικ στο **OK**. Θα γίνει η σύνδεση και θα ανοίξει για πρώτη φορά το administration interface:



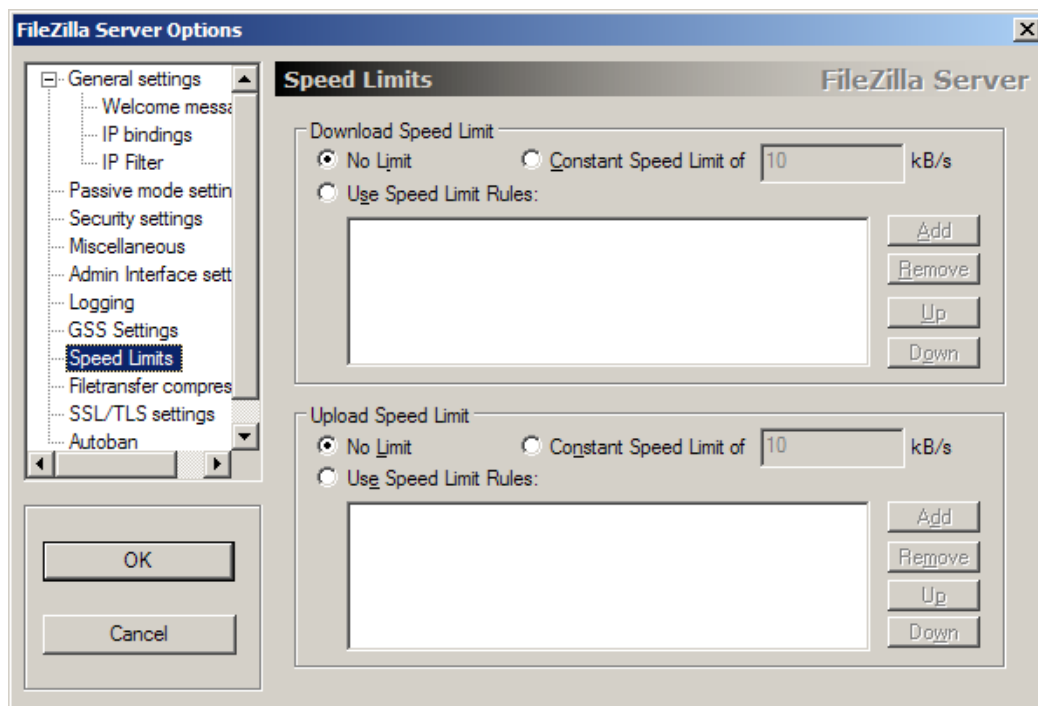
General Settings: Αφήνουμε τη θύρα 21 ως επιλογή και παρακάτω εισάγουμε το μέγιστο αριθμό χρηστών που θα μπορεί να εξυπηρετεί συγχρόνως ο FTP server. Εδώ πρέπει να ληφθεί υπ' όψιν η ταχύτητα της σύνδεσης Internet που έχουμε και συγκεκριμένα, ο ρυθμός **upload** αυτής. Ίσως είναι καλύτερα να μην επιτρέψουμε παραπάνω από 2-3 χρήστες, εκτός αν έχουμε γραμμή με upload > 512Kbps ή μία ακριβή **SDSL** σύνδεση. Συνεχίζουμε τις ρυθμίσεις:



Logging: Η σωστή καταγραφή είναι το ήμισυ του παντός στο system administration/security. Οπότε, κάνουμε τις ρυθμίσεις που φαίνονται παραπάνω. 3MB χώρος για να έχουμε τη δυνατότητα να ελέγξουμε τις συναλλαγές που έγιναν στον FTP server μας σε βάθος μηνός είναι μάλλον αμελητέα θυσία.

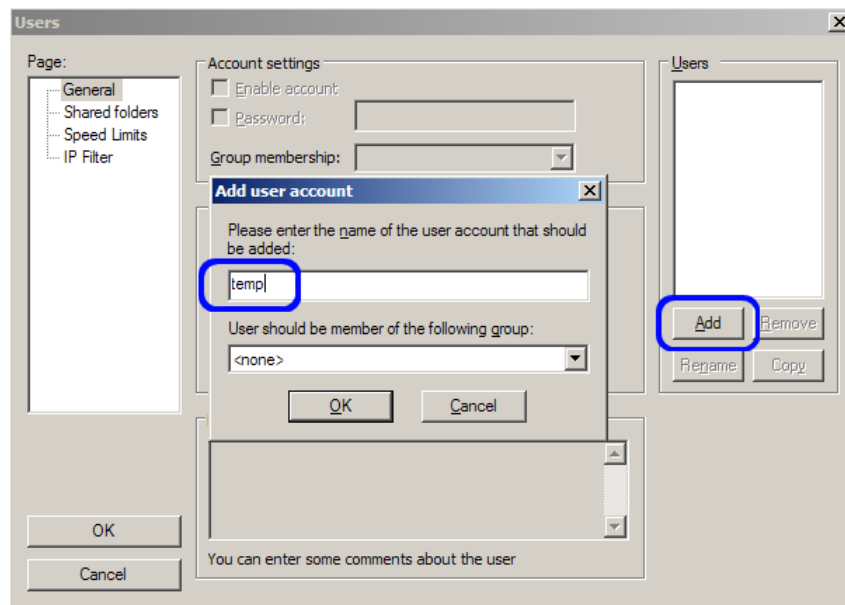


Speed Limits: Εδώ μπορούμε να ορίσουμε καθολικά speed limits. Παρακάτω θα δούμε όμως ότι μπορεί να γίνει ανά user account. Τα προβλήματα ταχύτητας των ADSL συνδέσεων στην Ελλάδα αυτήν τη στιγμή φαίνεται να έχουν να κάνουν κυρίως με το download rate μίας γραμμής και όχι με το upload. Π.χ. αν έχουμε σύνδεση 1024/256, άσχετα με τη μειωμένη ταχύτητα που μπορεί να κατεβάζουμε (ανάλογα και με τις ώρες της ημέρας), κατά πάσα πιθανότητα το upload rate της γραμμής (που καθορίζει την ταχύτητα με την οποία θα μπορούν να κατεβάσουν άλλοι από τον FTP server μας) θα είναι «καρφωμένο» στα $256 \text{ (Kbits/sec)} / 8 = 32 \text{ (Kbytes/sec)}$ - 10% περίπου (για το overhead) = 28 Kbytes/sec. Μπορούμε λοιπόν να βάλουμε μία εύλογη τιμή που θα επιτρέπει και το άνετο browsing την ώρα που κάποιος κατεβάζει από τον FTP server, π.χ. 20-24 ή ακόμη και unlimited αν δεν έχει πολλή κίνηση ο server. Φυσικά, αν κάποιος θέλει να ανεβάσει αρχεία στον server (πρέπει να του έχουμε δώσει και τα κατάλληλα δικαιώματα όπως θα δούμε παρακάτω), ρόλο παίζει το εκάστοτε download rate της γραμμής μας.

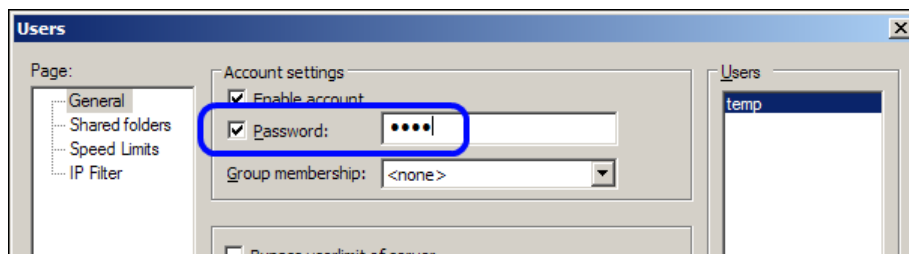


4.2. Δημιουργία Χρηστών

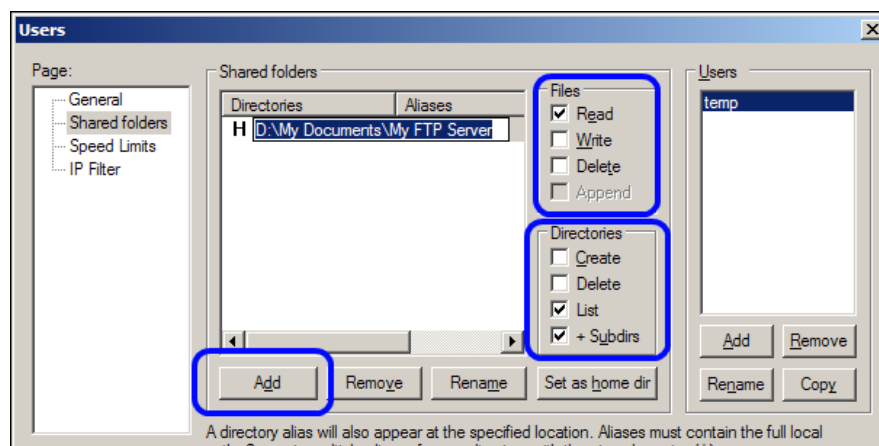
Θα δημιουργήσουμε μερικούς λογαριασμούς για άτομα στα οποία θέλουμε να δώσουμε πρόσβαση στον FTP server:



Κάνουμε κλικ στο Add, δίνουμε username και OK. Φυσικά, ορίζουμε και ένα password στη συνέχεια:



Εδώ από το Add ορίζουμε το home directory το οποίο θα βλέπουν οι χρήστες όταν συνδέονται στον server. Επίσης, μπορούμε να δώσουμε και δικαιώματα (ΠΡΟΣΟΧΗ!) εγγραφής/διαγραφής για αρχεία και δημιουργίας/διαγραφής directories. Για την επόμενη κατηγορία Speed Limits έγινε εκτενής ανάλυση πιο πάνω, οπότε κάνουμε τις ρυθμίσεις που θεωρούμε σωστές, ανάλογα με την ταχύτητα της γραμμής μας και πατάμε **OK**.



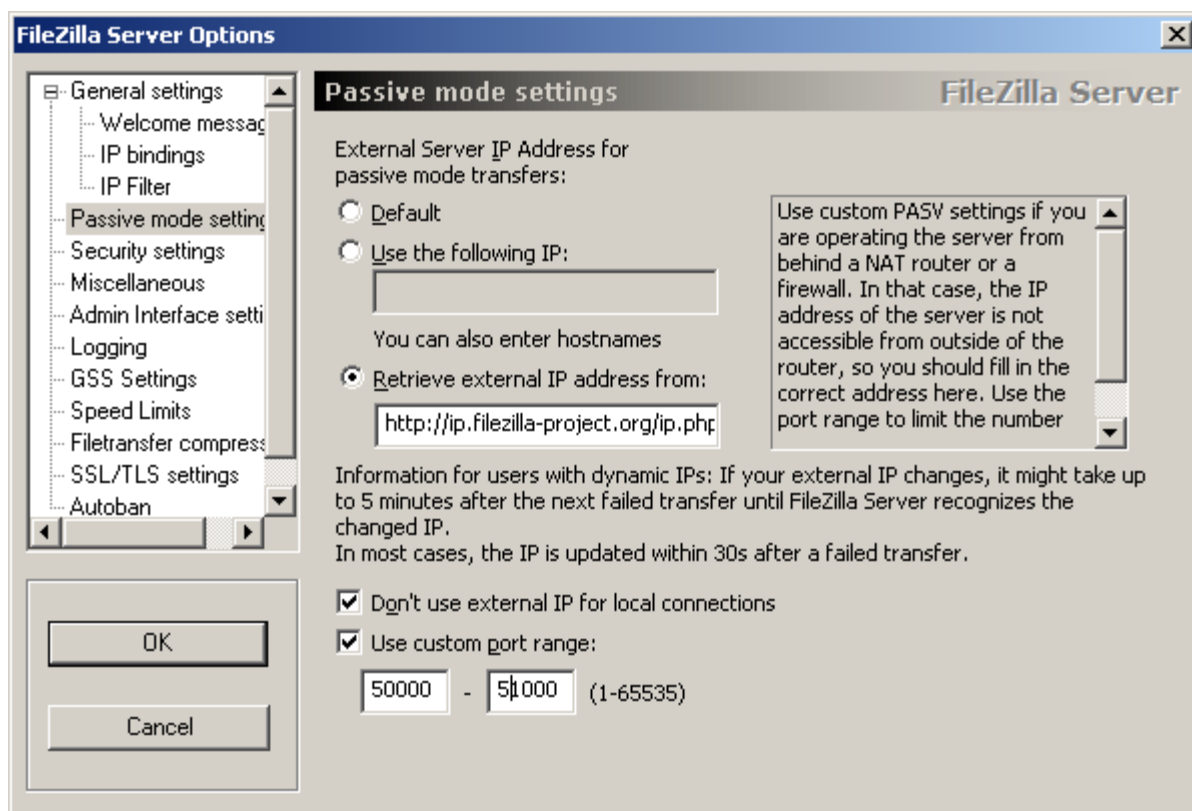
4.3. Active mode

Για να επιτρέψετε συνδέσεις σε Active Mode απλώς σιγουρέψτε ότι στον FileZilla Server επιτρέπεται να εγκαθιδρύει εξερχόμενες συνδέσεις σε τυχαίες θύρες, αφού ο πελάτης καθορίζει τη θύρα που θα χρησιμοποιηθεί.

Για το τοπικό άκρο της σύνδεσης, ο FileZilla Server προσπαθεί να χρησιμοποιήσει μία θύρα μικρότερη από αυτήν της σύνδεσης ελέγχου (π.χ. τη θύρα 20, αν ο server «ακούει» στη θύρα 21). Όμως, κάτι τέτοιο δεν είναι πάντα εφικτό και να μη βασίζεστε σε αυτό.

4.4. Passive mode

Σε passive mode, ο server ανοίγει ένα socket και περιμένει τον πελάτη να συνδεθεί σε αυτό. Εξ ορισμού, ο FileZilla Server ρωτά το λειτουργικό σύστημα για τη διεύθυνση IP του μηχανήματος και ζητά τον αριθμό μίας διαθέσιμης θύρας. Αυτή η ρύθμιση μπορεί να λειτουργήσει μόνο αν είστε συνδεδεμένοι στο Internet απευθείας χωρίς τη μεσολάβηση ενός NAT router και έχετε ορίσει στο firewall σας να επιτρέπει τις εισερχόμενες συνδέσεις σε όλες τις θύρες πάνω από την 1024.



Αν έχετε έναν NAT router, πρέπει να πείτε στον FileZilla Server την εξωτερική IP διεύθυνσή σας, ειδάλλως οι συνδέσεις passive mode με πελάτες εκτός του τοπικού σας δικτύου δε θα λειτουργούν:

- Αν έχετε στατική εξωτερική IP διεύθυνση, μπορείτε να την εισάγετε στο διάλογο παραμετροποίησης του FileZilla Server.
- Αν έχετε δυναμική διεύθυνση IP, μπορείτε να αφήσετε τον FileZilla να τη λαμβάνει αυτόματα από ένα ειδικό website. Εξαιρουμένου του αριθμού έκδοσης του FileZilla server, καμία άλλη πληροφορία δε μεταδίδεται προς αυτό το website

Αν δεν είστε σίγουροι, επιλέξτε το δεύτερο τρόπο. Αν δεν επιθυμείτε να επιτρέψετε τις εισερχόμενες συνδέσεις σε όλες τις θύρες ή αν έχετε έναν NAT router, πρέπει να πείτε στον

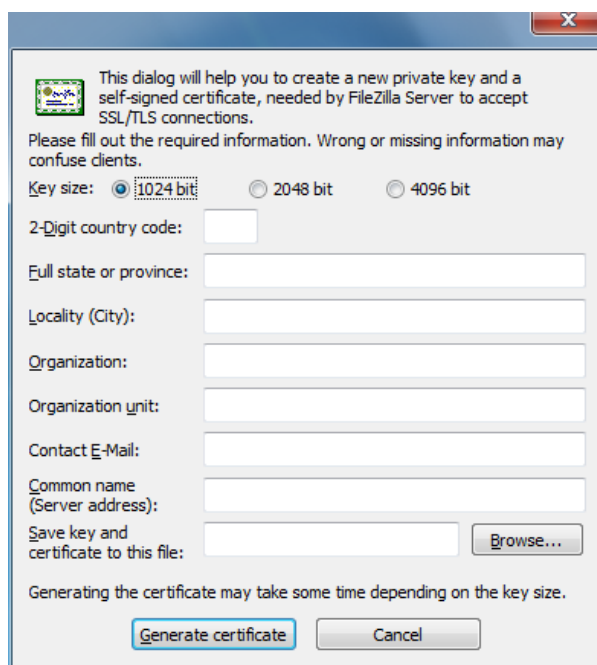
FileZilla Server να χρησιμοποιεί ένα συγκεκριμένο εύρος από θύρες για τις passive mode συνδέσεις. Θα πρέπει να ανοίξετε αυτές τις θύρες στο firewall σας. Αν έχετε έναν NAT router, θα πρέπει να προωθήσετε αυτές τις θύρες στο τοπικό μηχάνημα στο οποίο είναι εγκατεστημένος ο FileZilla Server. Αναλόγως του μοντέλου router, μπορείτε είτε να προωθήσετε ένα εύρος θυρών είτε θα πρέπει να τις προωθήσετε μία-μία χωριστά.

Οι έγκυρες πόρτες μπορεί να είναι από την 1 έως την 65535, όμως οι θύρες κάτω από την 1024 είναι συνήθως δεσμευμένες για άλλα πρωτόκολλα. Είναι καλό να επιλέξετε θύρες μεγαλύτερες από τη θύρα 50000 για passive mode FTP. Λόγω της φύσης του **TCP** (το υποκείμενο πρωτόκολλο μεταφοράς), μία θύρα δε μπορεί να επαναχρησιμοποιηθεί αμέσως μετά από κάθε σύνδεση. Γι' αυτό, το εύρος των θυρών δε θα πρέπει να είναι πολύ μικρό, ειδικά αν οι μεταφορές πολλών μικρών αρχείων θα αποτυγχάνουν. Ένα εύρος **50** θυρών θα πρέπει να είναι επαρκές στις περισσότερες των περιπτώσεων.

5. FTPS με χρήση SSL/TLS

5.1. Διαμόρφωση

Πρώτα θα χρειαστεί να δημιουργήσετε ένα πιστοποιητικό. Γι' αυτό μπορεί να χρησιμοποιηθεί η γεννήτρια Πιστοποιητικών του FileZilla server. Η γεννήτρια θα ζητήσει στοιχεία όπως ο κωδικός της χώρας, κράτος, πόλη, κλπ. .. Να είστε όσο πιο ειλικρινής γίνεται, καθώς μπορεί να πλήξετε την αξιοπιστία σας, αν εισάγετε λάθος πληροφορίες στο πιστοποιητικό.



Το μέγεθος για το πιστοποιητικό που το επιλέγετε στην κορυφή της γεννήτριας: 1024 bit, 2048 bit ή 4096 bit. Όσο μεγαλύτερο είναι το μέγεθος του κλειδιού το πιο ασφαλές το πιστοποιητικό, αλλά και η αρχική διαδικασία ανταλλαγής κλειδιών για κάθε σύνδεση. Υπάρχει, ωστόσο, ένα πράγμα που πρέπει να ληφθεί υπόψη, ο φόρτος της CPU κατά τη διάρκεια της εγκατάστασης της σύνδεσης. Όταν εφαρμόζετε κρυπτογράφηση για τον FileZilla server (FZS) σας η CPU θα πρέπει να κάνει πολλούς υπολογισμούς για την κρυπτογράφηση των δεδομένων που αποστέλλονται, αλλά και να αποκρυπτογραφήσει τα δεδομένα που λαμβάνονται. Το Bandwidth θα παίξει επίσης ρόλο στο πόσο θα επιβαρυνθεί η CPU. Εάν έχετε μια πιο αργή σύνδεση, ας πούμε γύρω από 1.5Mbps

upload, μπορεί να μη χρειάζεται να ανησυχείτε για την χρήση της CPU όσο. Ο καλύτερος τρόπος για να αποφασίσετε είναι να κάνετε δοκιμές.

Σημειώστε ότι ο FZS χρειάζεται τις διαδρομές για τα αρχεία πιστοποιητικών: Εάν έχετε δημιουργήσει το δικό του ιδιωτικό κλειδί και το πιστοποιητικό σας χωρίς να ορίσετε μια διαδρομή μπροστά από το όνομα του αρχείου, ο FZS βάζει μόνο το σκέτο όνομα αρχείου στο πεδίο πιστοποιητικό, χωρίς μήνυμα σφάλματος, αλλά αργότερα θα μπορεί να εμφανίσει ένα μήνυμα λάθους "Could not load certificate file" ("Δεν ήταν δυνατή η φόρτωση του πιστοποιητικού" όταν κάποιος προσπαθήσει να συνδεθεί μέσω FTPS).

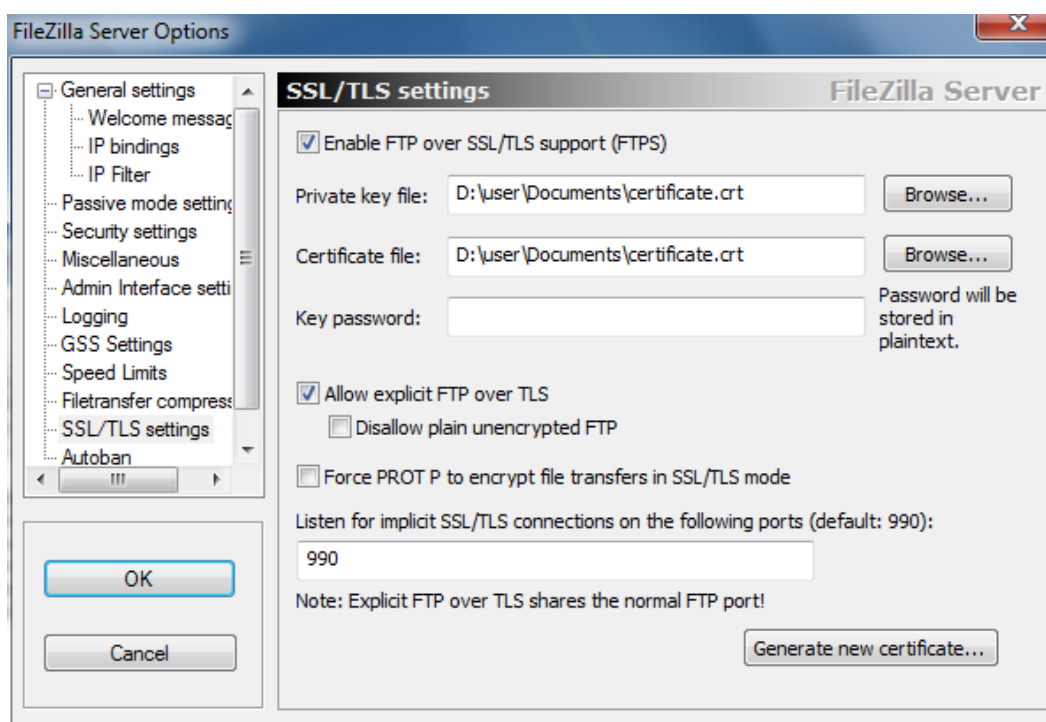
Συνεπώς, βάζετε πάντα την πλήρη διαδρομή προς τον ιδιωτικό κλειδί και τα αρχεία του πιστοποιητικού στα αντίστοιχα πεδία τους ώστε ο FZS να μπορεί να βρει τα αρχεία. Αφού έχετε δημιουργήσει το πιστοποιητικό γράψτε το όνομά του και την διαδρομή του φακέλου του στο πεδίο "Private key file".

5.2. Ενεργοποίηση SSL/TSL

Ενεργοποιείτε το "Enable FTP over SSL/TLS Support". Στις ρυθμίσεις SSL/TLS τσεκάρετε το "Allow explicit FTP over TLS." Συνιστάται επίσης να ελέγξετε "Disallow plain unencrypted FTP και το "Force PROT P to encrypt file transfers in SSL/TLS mode". Αυτό θα ενισχύσει περαιτέρω τις πολιτικές κρυπτογράφησης. Εδώ το PROT "P" σημαίνει "Ιδιωτικό" σε αντιδιαστολή με το "C" που σημαίνει απλό κείμενο.

Αν θέλετε μόνο ορισμένες ομάδες ή χρήστες να έχουν κρυπτογράφηση μπορείτε να το ορίσετε στις ρυθμίσεις του χρήστη ή της ομάδας. Αν υπάρχουν δεδομένα που θέλετε ακόμα να είναι διαθέσιμα στο ευρύ κοινό θα πρέπει να απενεργοποιήσετε τη ρύθμιση "Force".

Ρύθμιση του FTP server σας με αυτόν τον τρόπο σας επιτρέπει να κρυπτογραφήσετε τα δεδομένα σας και τις πληροφορίες σύνδεσης χωρίς να χρειάζεται να χρησιμοποιήσετε προγράμματα άλλων κατασκευαστών. Με ρητή SSL / TLS θα χρειαστείτε ένα FTP client, καθώς ο Internet Explorer και ο Firefox δεν υποστηρίζουν SSL/TLS χωρίς ειδικά plugins. Ο FileZilla client υποστηρίζει FTPS.



5.3. Διαφορά μεταξύ Explicit και Implicit FTPS

Explicit FTPS: Ο FTP client συνδέεται μέσω του καναλιού ελέγχου-εντολών (συνήθως στη θύρα 21), και στη συνέχεια μπορεί να διαπραγματευτεί τη χρήση SSL είτε για το κανάλι ελέγχου-εντολών ή (και) για κανάλι δεδομένων. Για να γίνει δηλαδή χρήση του SSL θα πρέπει ο πελάτης να το ζητήσει ρητά (explicitly).

Implicit FTPS: Το Implicit FTPS πηγαίνει ένα βήμα παραπέρα από την απαιτώντας πρώτα την αποστολή SSL εντολών πριν από οποιεσδήποτε άλλες FTP εντολές του πελάτη. Σε αντίθεση με το Explicit FTPS που επιτρέπει στον πελάτη αυθαίρετα να αποφασίσει εάν θα χρησιμοποιήσει SSL ή όχι, το Implicit FTPS απαιτεί το σύνολο της συνόδου FTP να είναι κρυπτογραφημένο. Βασικά ο τρόπος που λειτουργεί το Implicit FTPS είναι ότι ένα πρόγραμμα-πελάτης FTP συνδέεται με το κανάλι ελέγχου/εντολών, στην περίπτωση αυτή χρησιμοποιώντας τη θύρα 990, και αμέσως εκτελεί χειραψία SSL. Μετά από αυτό, μπορούν να σταλούν επιπλέον FTP εντολές από τον πελάτη. Στην περίπτωση αυτή πελάτες που δεν υποστηρίζουν SSL δεν μπορούν να συνδεθούν.

Πηγές:

http://www.insomnia.gr/wiki/_/internet/filezilla-server-howto-r48

http://www.insomnia.gr/wiki/_/internet/filezilla-και-δικτυακές-ρυθμίσεις-r49

[https://wiki.filezilla-project.org/FTPS_using_Explicit_SSL/TLS_howto_\(Server\)](https://wiki.filezilla-project.org/FTPS_using_Explicit_SSL/TLS_howto_(Server))

http://el.wikipedia.org/wiki/File_Transfer_Protocol