

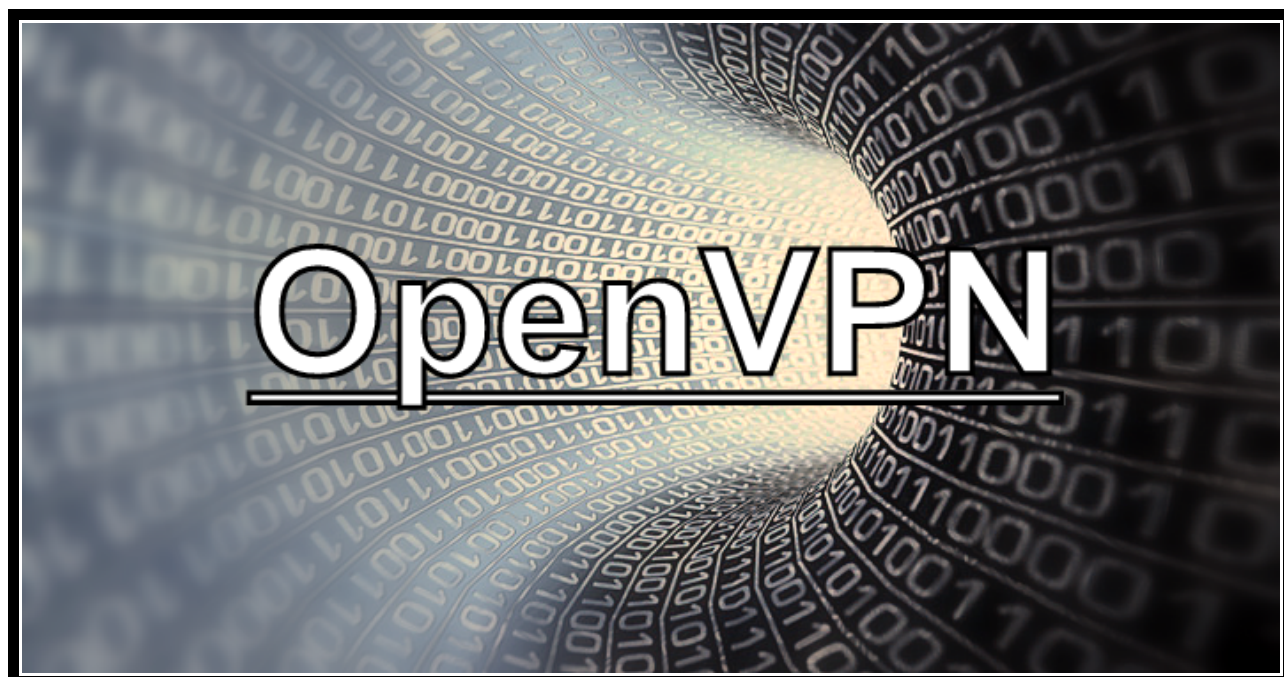


ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



Πτυχιακή εργασία

Δημιουργία υπηρεσίας VPN για το Τμήμα Πληροφορικής



Του φοιτητή :

Δημαρχόπουλου Δημήτριου

Αρ. Μητρώου : 1527

Επιβλέπων καθηγητής :

Χαρχαλάκης Στέφανος

Θεσσαλονίκη Ιούνιος 2010

Περιεχόμενα

ΠΕΡΙΛΗΨΗ.....	5
ABSTRACT.....	6
ΚΕΦΑΛΑΙΟ 1- Εισαγωγή.....	7
1.1 Εισαγωγή στα Ιδεατά Ιδιωτικά Δίκτυα.....	7
1.2 Προβλήματα Ασφάλειας και Internet.....	10
1.2.1 Θέματα και Τεχνικές Ασφάλειας (Δικτύων και Internet).....	11
1.2.2 Ασφάλεια και VPN.....	12
ΚΕΦΑΛΑΙΟ 2- Κατηγορίες VPN.....	13
2.1 Tunneling.....	14
2.2 IP in IP (Ενθυλάκωση – Tunneling).....	16
2.3 GRE (General Routing Encapsulation).....	18
2.4 PPP (Point To Point Protocol).....	19
ΚΕΦΑΛΑΙΟ 3- Πρωτόκολλα VPN.....	20
3.1 Πρωτόκολλα VPN επιπέδου Ζεύξης Δεδομένων (layer 2 OSI).....	20
3.1.1 Διαφορές L2F, PPTP και L2TP.....	22
3.2 Πρωτόκολλα VPN επιπέδου Δικτύου (layer 3 OSI).....	22
3.2.1 IPsec (IP Security).....	22
3.2.2 IPsec Αρχιτεκτονική.....	24
3.3 Πρωτόκολλα VPN επιπέδου Μεταφοράς (layer 4 OSI).....	27
3.3.1 SSL / TLS.....	27
3.3.2 SSL αρχιτεκτονική.....	28
3.3.3 SSL/TLS Κλειδιά και Κρυπτογράφηση.....	32
3.4 OpenVPN.....	32
3.4.1 OpenVPN Αρχιτεκτονική.....	33
3.4.2 OpenVPN L3 / L2 modes (Routing - Bridging).....	35
3.4.3 OpenVPN Ασφάλεια.....	36
ΚΕΦΑΛΑΙΟ 4- Υλοποίηση υπηρεσίας VPN.....	37
4.1 Δημιουργία υπηρεσίας VPN για το Τμήμα Πληροφορικής.....	37
4.1.1 Δυνατότητες – Περιορισμοί.....	38
4.2 Θέματα υλοποίησης- Λογισμικό.....	39
4.2.1 OpenVPN.....	39
4.2.1.1 Πλεονεκτήματα του OpenVPN.....	39
4.2.1.2 Σύγκριση του OpenVPN με το IPsec.....	42

4.2.2 Περιβάλλον GNU / Linux – Debian.....	44
4.2.3 Webmin - Διαχείριση μέσω Web.....	46
ΚΕΦΑΛΑΙΟ 5- Υλοποίηση Server.....	47
5.1 Εγκατάσταση OpenVPN Server.....	47
5.2 Ρύθμιση OpenVPN Server.....	49
5.3 Σενάρια (scripts).....	74
5.4 Αυθεντικοποίηση.....	75
5.5 Εκκίνηση OpenVPN Server.....	78
ΚΕΦΑΛΑΙΟ 6- Υλοποίηση Client.....	80
6.1 Ρύθμιση OpenVPN Client.....	80
6.2 Δημιουργία Πρόγραμματος Εγκαταστάτης (Windows Client).....	85
6.2.1 Αυτόματη Εγκατάσταση (Windows Client).....	87
6.3 Εγκατάσταση (Linux Client).....	89
6.4 Εγκατάσταση (Mac OS X Client).....	90
6.5 Υλοποίηση - Εγκατάσταση (PocketPC Client).....	92
ΚΕΦΑΛΑΙΟ 7- Διαχείριση - Παρατηρήσεις - Προβλήματα.....	96
7.1 Διαχείριση των VPN συνδέσεων.....	96
7.2 Παρατηρήσεις κατά την VPN σύνδεση.....	98
7.3 Προβλήματα κατά την VPN σύνδεση.....	99
ΚΕΦΑΛΑΙΟ 8- OpenVPN και Ασφαλές Σερφάρισμα.....	101
8.1 Φίλτρο ελέγχου περιεχομένων : “DansGuardian”	101
8.1.1 Εγκατάσταση του “DansGuardian”.....	104
ΚΕΦΑΛΑΙΟ 9- Δοκιμές Απόδοσης (Benchmarks).....	108
ΚΕΦΑΛΑΙΟ 10- Προτάσεις - Συμπεράσματα.....	113
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	114
ΠΑΡΑΡΤΗΜΑ.....	119

Ευρετήριο Σχημάτων

Σχήμα 1 : Οι φάσεις ανάπτυξης των VPN.....	9
Σχήμα 2 : Οι διάφορες κατηγορίες VPN.....	13
Σχήμα 3 : Tunneling.....	16
Σχήμα 4 : Ενθυλάκωση IP in IP.....	17
Σχήμα 5 : Διαδικασία ενθυλάκωσης.....	18
Σχήμα 6 : Χρήση του PPP, το οποίο λειτουργεί σε 3 στάδια.....	19
Σχήμα 7 : PPTP / Ενθυλάκωση GRE.....	21
Σχήμα 8 : Η δομή των IPv4 και IPv6 πακέτων με IPSec.....	23
Σχήμα 9 : Συστατικά του IPsec.....	25
Σχήμα 10 : IPsec Transport mode.....	26
Σχήμα 11 : IPsec Tunnel mode.....	27
Σχήμα 12 : SSL Protocol Stack.....	29
Σχήμα 13 : SSL/TLS handshake	30
Σχήμα 14 : Λειτουργίες του SSL Record Protocol.....	31
Σχήμα 15 : Αλγόριθμοι που χρησιμοποιούνται στο SSL Record Protocol.....	32
Σχήμα 16 : Λειτουργία του OpenVPN με TUN / TAP εικονική διασύνδεση.....	34
Σχήμα 17 : Σύγκριση του OpenVPN με το IPsec.....	44
Σχήμα 18 : Διάγραμμα Throughput Μέσω DSL πρόσβασης.....	109
Σχήμα 19 : Διάγραμμα Throughput Μέσω LAN πρόσβασης.....	109
Σχήμα 20 : Διάγραμμα Throughput Μέσω WLAN πρόσβασης.....	110
Σχήμα 21 : Διάγραμμα Throughput με διαφορετικές κρυπτογραφήσεις.....	110
Σχήμα 22 : Διάγραμμα Jitter Μέσω DSL πρόσβασης.....	111
Σχήμα 23 : Διάγραμμα Jitter Μέσω LAN πρόσβασης.....	112
Σχήμα 24 : Διάγραμμα Jitter Μέσω WLAN πρόσβασης.....	112

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία έχει ως θέμα τη δημιουργία υπηρεσίας VPN για το Τμήμα Πληροφορικής. Γίνεται μια συνοπτική παρουσίαση της εξέλιξης των Εικονικών Ιδιωτικών Δικτύων και των διαφορετικών τεχνολογιών στις οποίες βασίζεται. Στην συνέχεια παρατίθεται ένας πλήρης οδηγός για το πώς μπορεί κάποιος να εγκαταστήσει και να διαχειριστεί ένα VPN “server – client” σύστημα για το Τμήμα Πληροφορικής, βασιζόμενος στην εφαρμογή ανοιχτού κώδικα “OpenVPN” και πως να συνδεθεί μέσω αυτού, από οποιοδήποτε λειτουργικό σύστημα και αν διαθέτει, στο δίκτυο του Τμήματος Πληροφορικής. Τέλος, προτείνεται η δημιουργία μια υπηρεσίας “Ασφαλούς Σερφαρίσματος” μέσω του συνδυασμού της τεχνολογίας VPN κι ενός “Φίλτρου ελέγχου περιεχομένων” ιστοσελίδων.

ABSTRACT

The subject of the present thesis is the creation of VPN service for the Department of Information Technology. There is a concise presentation of the development of Virtual Private Networks together with the various technologies on which this is based. A complete 'how to' guide is given for the installation and management of a VPN "server - client" system for the I.T. Department and the way the user can be connected through this infrastructure to the I.T. Department. The installation is based on an open source application, "OpenVPN". At the end, the creation of a "Safe Surfing" service is proposed through a combination of VPN technology and a "Content Management Filter" for web sites.

1. ΚΕΦΑΛΑΙΟ 1- Εισαγωγή

Τα Ιδεατά η Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks ή VPN) αποτελούν σε λογικό επίπεδο, συνδέσεις δυο η περισσοτέρων τοποθεσιών (τοπικά δίκτυα ή μεμονωμένους χρήστες) ενός οργανισμού. Η φυσική τους διασύνδεση υλοποιείται πάνω από μια κοινόχρηστη δημόσια δικτυακή υποδομή, όπως το διαδίκτυο ή το τηλεφωνικό δίκτυο, με τρόπο που διασφαλίζεται το ιδιωτικό απόρρητο των διακινούμενων πληροφοριών.

“Η μεταφορά μέσω του Internet εμπιστευτικής πληροφορίας, με έναν αξιόπιστο και ασφαλή τρόπο, ονομάζεται Ιδεατό ή Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network).”

1.1 Εισαγωγή στα Ιδεατά Ιδιωτικά Δίκτυα

Τις τελευταίες δύο δεκαετίες ο κόσμος των υπολογιστών έχει αλλάξει σημαντικά. Πολλές επιχειρήσεις, αντί απλά ν' ασχολούνται με τοπικά ή εθνικά θέματα, στρέφονται σήμερα στην παγκόσμια αγορά και οικονομία. Έχοντας εγκαταστάσεις εκτός της μητρικής τους χώρας και σε πολλά άλλα μέρη του κόσμου, θέλοντας γρήγορη και ασφαλή επικοινωνία μεταξύ των γραφείων τους σε οποιοδήποτε σημείο και αν βρίσκονται αυτά, αντιμετωπίζουν πολύ συχνά προβλήματα επικοινωνίας ή λειτουργίας που απορρέουν από την γεωγραφική απόσταση που χωρίζει τα σημεία αυτά.

Αυτό είχε ως επακόλουθο, την χρήση μισθωμένων γραμμών (leased lines) με σκοπό την δημιουργία WAN (wide area network). Την δεκαετία του '90, οι μισθωμένες γραμμές είχαν εύρος (bandwidth) από απλή ISDN (integrated services digital network, 128 Kbps) ως και OC3 (Optical Carrier-3, 155 Mbps) και παρέιχαν την δυνατότητα στις εταιρίες, να μεγαλώσουν το ιδιωτικό δίκτυό τους

πέρα από πλαίσια μίας συγκεκριμένης γεωγραφικής περιοχής.

Υπάρχουν προφανή πλεονεκτήματα, ενός WAN μέσω μισθωμένων γραμμών, σε σύγκριση με ένα δημόσιο δίκτυο, όπως το Internet, όσον αφορά την ασφάλεια, την εγκυρότητα, τις επιδόσεις και την αποτελεσματικότητα. Όμως η ύπαρξη ενός σταθερού μισθώματος, ανεξάρτητα από τον όγκο των πληροφοριών που μεταφέρονται, αποτελεί βασικό μειονέκτημα των μισθωμένων γραμμών. Είναι μεγάλο έξοδο, το οποίο σταδιακά αυξάνεται όσο μεγαλώνει η απόσταση των γραφείων της επιχείρησης. Επίσης, δεν είναι αρκετά “ευέλικτα” δίκτυα, γιατί δεν είναι εύκολο ν' αναπροσαρμοστούν, όταν προκύπτει η ανάγκη εξάπλωσης τους. Μειονεκτήματα όπως αυτά, έδωσαν την ώθηση για την αναζήτηση νέων λύσεων, οδηγώντας σταδιακά στην ανάπτυξη των σημερινών VPN.

Οι εταιρίες στράφηκαν προς το διαδίκτυο, καθώς η δημοτικότητά του μεγάλωνε, με σκοπό την επέκταση του ιδιωτικού δικτύου τους. Πολλές επιχειρήσεις σήμερα, δημιουργούν το δικό τους VPN, προσαρμοσμένο στις ανάγκες των απομακρυσμένων υπαλλήλων και γραφείων της.

Ιστορικά, η τεχνολογία VPN πρώτο-υιοθετήθηκε από τις εταιρίες που θέλησαν να προσφέρουν ελεύθερα δοκιμαστικά προϊόντα (trials), για να ενημερώσουν έτσι το κοινό για την καινούρια αυτή τεχνολογία. Πολλοί εμπορικοί οίκοι ξεκίνησαν να χρησιμοποιούν τα VPN, επειδή η επιχειρηματική κοινωνία αναζητούσε έναν οικονομικό και ασφαλή τρόπο σύνδεσης των εταιρικών δικτύων και υπηρεσιών της. Με αργά βήματα επέκτειναν αυτήν την υποδομή, έχοντας στόχο να διευκολύνουν τους υπαλλήλους τους να συνδεθούν στο εταιρικό δίκτυο από το σπίτι ή κατά την διάρκεια ταξιδιών. Αυτό προετοίμασε τον δρόμο για την δεύτερη φάση της ανάπτυξης των VPN. Η τεχνολογία εφαρμόστηκε σε κάποιες όχι ιδιαίτερα κρίσιμες εφαρμογές και αργότερα σε άλλες κατεξοχήν σημαντικές, οι οποίες απαιτούσαν μεγαλύτερη ασφάλεια στις πληροφορίες που περιείχαν. Οι διάφορες φάσεις της ανάπτυξης της τεχνολογίας VPN παραθέτονται στον παρακάτω πίνακα :

ΧΡΟΝΙΚΟ ΠΛΑΙΣΙΟ	ΦΑΣΗ ΑΓΟΡΑΣ	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΓΟΡΑΣ
Πριν το 1998	ΠΡΩΙΜΟΙ ΕΝΣΤΕΡΝΙΣΤΕΣ	<ul style="list-style-type: none"> • Δοκιμαστικά υπηρεσιών • Τηλεταξιδευτές (Telecommuters) • Ad-hoc employment
1998	ΚΛΗΣΗ ΑΠΟ ΕΞΩΤΕΡΙΚΟΥΣ ΕΡΓΑΖΟΜΕΝΟΥΣ	<ul style="list-style-type: none"> • Εργαζόμενοι από το σπίτι • Κινητές μονάδες εργαζομένων • Παραδοσιακή κλήση για την δημιουργία αντιγράφων ασφαλείας
1999	ΔΙΑΚΛΑΔΩΣΗ ΚΛΗΣΗΣ ΕΞΩΤΕΡΙΚΩΝ ΕΡΓΑΖΟΜΕΝΩΝ	<ul style="list-style-type: none"> • Χρήση για ανεφοδιασμό και δημιουργία αντιγράφων ασφαλείας • Μερικά “tunnels”, πολύ χρήστες • Μη κρίσιμη LAN-to-LAN κίνηση δεδομένων
Από το 2000 και έπειτα	EXTRANETS	<ul style="list-style-type: none"> • End to end QoS & SLAs • Πολλά Tunnels, πολύ χρήστες • Μεγάλης κρισιμότητας LAN-to-LAN κίνηση δεδομένων • Ασφαλή Extranets

Σχήμα 1 : Οι φάσεις ανάπτυξης των VPN

Ένα VPN μπορεί να προσφέρει, με συγκεκριμένες εγγυήσεις, λύσεις σε θέματα οργάνωσης, επικοινωνίας, κατανομής και διαχείρισης πληροφοριών σε όλα τα τμήματα ή υποκαταστήματα ενός οργανισμού ή μιας επιχείρησης, όπου και αν βρίσκονται.

Με τα VPN επιτυγχάνονται σημαντικές μειώσεις, σε σχέση με τις παραδοσιακές λύσεις διασύνδεσης, στα τηλεπικοινωνιακά έξοδα μίας εταιρείας. Παράλληλα, εγγυώνται την ασφάλεια των επικοινωνιών αλλά και το ποιοτικό επίπεδο της παρεχόμενης υπηρεσίας (Service Level Agreement), κάτι που με τις κλασικές μεθόδους διασύνδεσης δεν είναι εύκολο.

1.2 Προβλήματα Ασφάλειας και Internet

Η διακίνηση δεδομένων μέσω τηλεπικοινωνιακών δικτύων δημιουργεί προβλήματα, καθώς αυτά καθίστανται ευπρόσβλητα σε κακόβουλες ενέργειες. Επίσης, η σύνδεση των ιδιωτικών δικτύων με το Internet καθώς και η διασύνδεση τους μέσω αυτού, δίνει τη δυνατότητα επιθέσεων προς τους υπολογιστές των ιδιωτικών δικτύων. Στις επικοινωνίες μέσω του διαδικτύου απαντώνται διάφοροι κίνδυνοι :

- Έλλειψη εμπιστευτικότητας, εφόσον τα δεδομένα που διακινούνται είναι χωρισμένα σε πακέτα, μπορούν εύκολα να κλαπούν και ν' αποκαλυφθεί το περιεχόμενό τους.
- Έλλειψη μηχανισμών για την ταυτοποίηση των χρηστών των συστημάτων. Όλα τα συστήματα που είναι συνδεδεμένα στο διαδίκτυο αναγνωρίζονται από την IP διεύθυνση τους. Το πρωτόκολλο IP όμως, δεν παρέχει από μόνο του κάποιο μηχανισμό αυθεντικοποίησης των χρηστών του συστήματος.
- Έλλειψη αξιόπιστων μέσων για σύνδεση με συγκεκριμένους υπολογιστές.
- Εκτεθειμένοι κωδικοί πρόσβασης. Εφόσον τα περισσότερα συστήματα χρησιμοποιούν κωδικούς για την ταυτοποίηση των χρηστών, οι οποίοι τις

περισσότερες φορές μεταφέρονται στο δίκτυο χωρίς να κρυπτογραφηθούν.

1.2.1 Θέματα και Τεχνικές Ασφάλειας (Δικτύων και Internet)

Τα βασικότερα θέματα και τεχνικές ασφάλειας που μπορούν να εφαρμοστούν, ώστε να επιτευχθεί η ασφάλεια των πληροφοριών που μεταδίδονται μέσω δικτύων και του διαδικτύου είναι :

- **Επιβεβαίωση ταυτότητας (Authentication)** : Αφορά την επιβεβαίωση της ταυτότητας του συνομιλητή, γιατί στις επικοινωνίες μέσω δικτύων έχει σημασία το πρόσωπο ή ο Η/Υ με τον οποίο υπάρχει επικοινωνία, να είναι όντως αυτός που υποτίθεται ότι είναι .
- **Εμπιστευτικότητα (Confidentiality)** : Εμπιστευτικότητα στην επικοινωνία, σημαίνει ότι κανείς μη εξουσιοδοτημένος δεν μπορεί να έχει πρόσβαση ώστε να διαβάσει τα δεδομένα που μεταφέρονται μέσω του δικτύου. Η κρυπτογράφηση είναι ένας αποτελεσματικός τρόπος αντιμετώπισης του κινδύνου αυτού.
- **Ακεραιότητα δεδομένων (Data Integrity)** : Σημαίνει ότι τα δεδομένα με κανένα τρόπο δεν έχουν τροποποιηθεί ή καταστραφεί κατά την μεταφορά τους μέσω του δικτύου.
- **Δικαιοδοσία πρόσβασης (Authorization)** : Τα συστήματα δικαιοδοσίας πρόσβασης επιτρέπουν την πρόσβαση μόνον σε εξουσιοδοτημένους χρήστες. Η μη αυστηρή τήρηση του Authorization και οι αδυναμίες των λειτουργικών συστημάτων, σε μεγάλα υπολογιστικά συστήματα που εξυπηρετούν πολυάριθμους χρήστες, μπορεί να επιτρέψουν την πρόσβαση εισβολέων σε μη επιτρεπτούς πόρους.
- **Απάρνηση ενέργειας ή πράξης (Non repudiation)** : Στην περίπτωση

αυτή το ένα από τα δύο συμβαλλόμενα μέρη στην επικοινωνία απαρνείται την συναλλαγή (π.χ. αποστολή ή λήψη μηνύματος που έκανε). Ένας τρόπος αντιμετώπισης αυτού του προβλήματος είναι η επιβεβαίωση της συναλλαγής από ένα τρίτο κοινά αποδεκτό φορέα (trusted party).

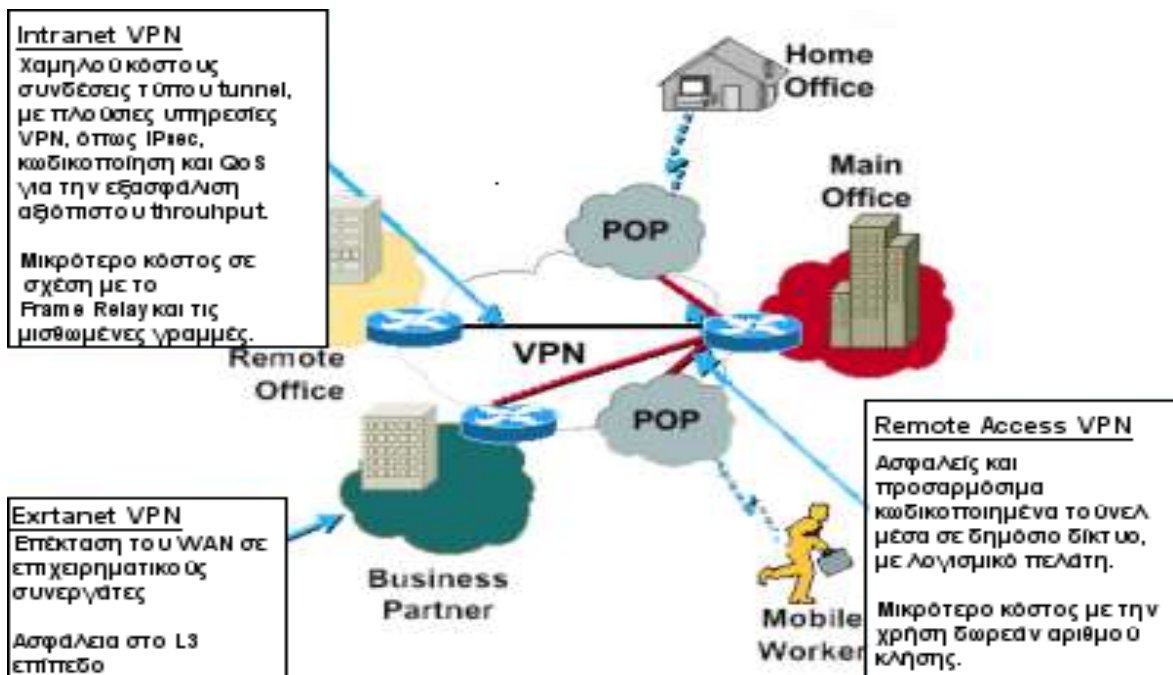
1.2.2 Ασφάλεια και VPN

Το διαδίκτυο από τη φύση του ως ένα ανοικτό δημόσιο δίκτυο παρουσιάζει προβλήματα ασφαλείας και απειλών. Τα VPN κάνουν χρήση μιας πληθώρας τεχνικών, διάφορων τεχνολογιών, εξασφαλίζοντας έτσι, για την κάθε περίπτωση, την προστασία των δεδομένων που μεταφέρουν. Τεχνικές που σχετίζονται με την αναγνώριση, τη διόρθωση και την παρεμπόδιση πιθανών επιθέσεων : Το τείχος προστασίας (firewall), η αυθεντικοποίηση (authentication), συμμετρική ή ασύμμετρη κρυπτογράφηση (encryption), οι ψηφιακές υπογραφές και τα πιστοποιητικά (ISO X.509), το γέμισμα των κυκλοφοριακών κενών, η αλυσίδωση των μηνυμάτων, η χρόνο-σφραγίδα (timestamp), η αναγνώριση εισβολών (intrusion detection), και το tunneling με χρήση πρωτοκόλλων όπως το IPsec, L2F, SSL/TLS (OpenVPN), PPTP, L2TP, κ.α. που αποτελούν ειδικά παραδείγματα τέτοιων τεχνικών.

2 ΚΕΦΑΛΑΙΟ 2- Κατηγορίες VPN

Υπάρχουν δύο ειδών Ιδεατά Ιδιωτικά Δίκτυα : Τα “απομακρυσμένης πρόσβασης” (Remote Access VPN), που επιτρέπουν σε μεμονωμένους χρήστες να συνδέονται στο τοπικό δίκτυο της εταιρείας (LAN) από απόσταση με ασφαλείς και κρυπτογραφημένες συνδέσεις και τα “σημείο-προς-σημείο” (Site-to-Site VPN), στα οποία ένας οργανισμός ή μια εταιρεία, μπορεί να συνδέσει πολλαπλά σημεία της με άλλα σημεία, άλλα τοπικά δίκτυα, ή ένα δημόσιο δίκτυο σαν το διαδίκτυο.

Αντίστοιχα, υπάρχουν δύο τύποι site-to-site VPN συνδέσεων, οι “Intranet-based”, μέσω των οποίων η εταιρεία, μπορεί να συνδέσει δύο δικά της απομακρυσμένα δίκτυα μεταξύ τους, ώστε να δημιουργήσουν ένα μοναδικό VPN και οι “Extranet-based”, όπου δύο διαφορετικές εταιρείες μπορούν να συνδέσουν τα τοπικά τους δίκτυα, δημιουργώντας έτσι ένα κοινό περιβάλλον εργασίας.



Σχήμα 2 : Οι διάφορες κατηγορίες VPN

Με βάση τον τρόπο λειτουργίας τους, τα VPN μπορούν να χωριστούν σε δύο κατηγορίες : Στα Ασφαλή Ιδεατά Ιδιωτικά Δίκτυα (Secure VPN) και στα Έμπιστα VPN (Trusted VPN).

1. Τα Ασφαλή VPN χρησιμοποιούν πρωτόκολλα κρυπτογράφησης και μεταφέρουν τα δεδομένα μέσω “τούνελ” πρωτοκόλλων (Tunneling), πράγμα που πρακτικά σημαίνει, ότι τα πακέτα ενθυλακώνονται μέσα σε άλλα πακέτα και στέλνονται έτσι μέσα στο δίκτυο με σκοπό την απόκρυψη του περιεχομένου τους και την επίτευξη της ιδιωτικότητας. Μερικά από αυτά τα πρωτόκολλα είναι : IPsec (IP security), SSL (Secure Sockets Layer), PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) τα οποία χρησιμοποιούν διαφορετικές τεχνικές για την ασφαλή μεταφορά των δεδομένων μέσω αναξιόπιστων δικτύων, όπως το Διαδίκτυο.
2. Τα Έμπιστα VPN από την άλλη πλευρά, δεν χρησιμοποιούν κρυπτογράφηση και “tunneling” τεχνικές, αλλά για να προστατέψουν τις επικοινωνίες τους, εμπιστεύονται την άμυνά τους στη χρησιμοποίηση του δικτύου ενός μόνο παρόχου. Τέτοια δίκτυα VPN είναι τα MPLS (Multi Protocol Label Switching) VPN και το L2F (Layer 2 Forwarding).

2.1 Tunneling

Το tunneling είναι η τεχνική που ενθυλακώνει ένα αρχικό πακέτο σε ένα νέο, διαφορετικού συνήθως πρωτοκόλλου και πρωτοεμφανίστηκε για να επιτρέψει τη μεταφορά δεδομένων μέσω δικτύων που χρησιμοποιούν διαφορετικά πρωτόκολλα.

Τα περισσότερα Εικονικά Ιδιωτικά Δίκτυα (VPN) στηρίζονται στο tunneling για

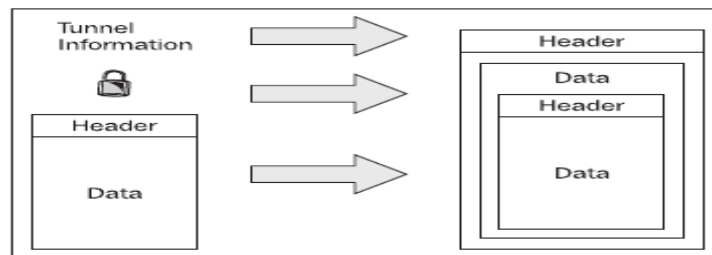
να δημιουργήσουν ένα ιδιωτικό δίκτυο το οποίο να μπορεί να διασχίσει το Internet. Οι δύο πλευρές του τούνελ αποκαλούνται tunnel interfaces. Το πρωτόκολλο του εξωτερικού πακέτου είναι κατανοητό από το δίκτυο, που με αυτό τον τρόπο καταλαβαίνει, τότε αυτό “εισέρχεται” ή “αποχωρεί”. Το tunneling απαιτεί τρία διαφορετικά πρωτόκολλα :

- **Carrier protocol** : Το πρωτόκολλο που χρησιμοποιείται από το δίκτυο επιβεβαιώνοντας πως η πληροφορία ταξιδεύει.
- **Encapsulating protocol** : Το πρωτόκολλο (GRE,IP / IP, IPSec, L2F, PPTP, L2TP) το οποίο είναι τυλιγμένο γύρω από τα αρχικά δεδομένα.
- **Passenger protocol** : Τα πραγματικά δεδομένα (IPX, NetBeui, IP) τα οποία μεταφέρονται.

Πολλές εφαρμογές του VPN χρησιμοποιούν “tunneling” για να δημιουργήσουν ένα εικονικό ιδιωτικό δίκτυο. Στην πραγματικότητα πολλά ιδιωτικά δίκτυα εταιρικού χαρακτήρα δεν χρησιμοποιούν πρωτόκολλο IP αλλά διαφορετικά πρωτόκολλα, για παράδειγμα το πρωτόκολλο IPX που χρησιμοποιούν μερικοί εξυπηρετητές της εταιρίας Novell.

Το πακέτο που ενθυλακώνεται μπορεί να είναι διαφορετικού ή του ίδιου πρωτοκόλλου. Χρησιμοποιώντας αυτήν την τεχνική μπορούν να σταλούν πακέτα τύπου IPX μέσω του Internet (το οποίο χρησιμοποιεί πρωτόκολλο TCP/IP) ώστε ο χρήστης να συνδεθεί απομακρυσμένα σε ένα υπολογιστικό σύστημα που χρησιμοποιεί το πρωτόκολλο IPX.

Στην περίπτωση του VPN, επειδή απαιτείται η μετάδοση δεδομένων ενός ασφαλούς εσωτερικού δικτύου μέσω του εξωτερικού ανοικτού δικτύου Internet, χρησιμοποιείται ενθυλάκωση για λόγους ασφαλείας, ακόμη και στην περίπτωση που τα δύο δίκτυα χρησιμοποιούν το ίδιο πρωτόκολλο IP. Δηλαδή με την τεχνική αυτή μπορεί κανείς να τοποθετήσει IP πακέτο μέσα σε ένα IP πακέτο.



Σχήμα 3 : Tunneling

Αυτό πρακτικά σημαίνει ότι μπορούν να σταλθούν μέσω του διαδικτύου πακέτα με ιδιωτικές διευθύνσεις αποστολέα και παραλήπτη, μέσα σε πακέτα που έχουν δημόσιες (διαδικτυακές) διευθύνσεις αποστολέα και παραλήπτη. Με αυτόν τον τρόπο γίνεται δυνατή η χρήση διευθύνσεων που είναι δεσμευμένες για ιδιωτική χρήση (μόνο για LAN) από την IANA (Internet Assigned Numbers Authority) για να αποκτηθεί πρόσβαση μέσω διαδικτύου.

Τα πρωτόκολλα που υλοποιούν VPN χωρίζονται σε κατηγορίες ανάλογα με το επίπεδο μοντέλου αναφοράς OSI που δημιουργούν το tunnel. Αναφορικά για το Επίπεδο 2 χρησιμοποιούνται τα PPTP, L2F και το L2TP, στο Επίπεδο 3. το IPsec και στο Επίπεδο 4 το SSL/TLS (OpenVPN).

2.2 IP in IP (Ενθυλάκωση – Tunneling)

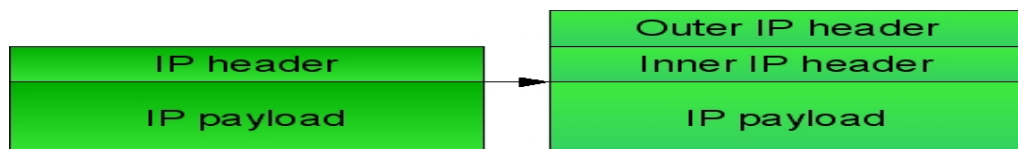
Μία “IP in IP” σύνδεση αποτελεί το απλούστερο τούνελ που μπορεί να δημιουργηθεί μεταξύ δύο κόμβων που επικοινωνούν με το TCP/IP πρωτόκολλο, χρησιμοποιώντας την τεχνική της ενθυλάκωσης πακέτου “IP in IP” που περιγράφεται στα RFC (Request for Comments) 1853 και 2003. Η τεχνική της ενθυλάκωση είναι αρκετά απλή, έχοντας μια εξωτερική IP επικεφαλίδα να προστίθεται πριν από την αρχική IP επικεφαλίδα και ενδιάμεσα τους τις υπόλοιπες επικεφαλίδες που περιέχουν πληροφορίες για τη διαδρομή, την ασφάλεια και

ειδικά για τη διαμόρφωση της σήραγγας. Η εξωτερική IP επικεφαλίδα περιέχει πληροφορίες όπως διεύθυνση “αποστολέα / παραλήπτη” για τον εντοπισμό και χαρακτηρισμό των “άκρων” της σήραγγας, ενώ η εσωτερική IP επικεφαλίδα περιλαμβάνει πληροφορίες διεύθυνσης “αποστολέα / παραλήπτη” για τον εντοπισμό του αρχικού αποστολέα και του τελικού παραλήπτη του IP πακέτου. Κάθε IP επικεφαλίδα συνδέεται με την επόμενη IP χρησιμοποιώντας τους μηχανισμούς του IP πρωτοκόλλου. Η πλέον γενική περίπτωση “IP in IP” τούνελ είναι:

Πηγή ----> Encapsulator ----> Decapsulator ----> Προορισμός

Με την πηγή, encapsulator, decapsulator, και τον προορισμό να αποτελούν ξεχωριστούς κόμβους. Ο κόμβος encapsulator θεωρείται το “σημείο εισόδου” της σήραγγας, ενώ ο κόμβος decapsulator θεωρείται το “σημείο εξόδου” από τη σήραγγα. Μπορεί να υπάρξουν πολλαπλά ζεύγη “πηγής - προορισμού” χρησιμοποιώντας την ίδια σήραγγα μεταξύ των encapsulator και decapsulator.

Το είδος των σηράγγων IP in IP έχει γενικά το χαμηλότερο φόρτο, αλλά μπορεί να ενθυλακώσει και να μεταφέρει μόνο IPv4 “unicast” κίνηση. Έτσι δεν είναι σε θέση να χρησιμοποιηθεί OSPF, RIP ή οποιαδήποτε άλλο πρωτόκολλο ή εφαρμογή που βασίζεται στο “multicast”. Μπορεί να ρυθμιστεί μόνο μία σήραγγα τη φορά για το μοναδικό ζεύγος απολήξεων της. Τέλος, το IP in IP υποστηρίζεται και μπορεί να λειτουργήσει με το FreeBSD, το IOS της Cisco, καθώς και σε περιβάλλον Linux μέσω του αρθώματος του πυρήνα “ipip”.

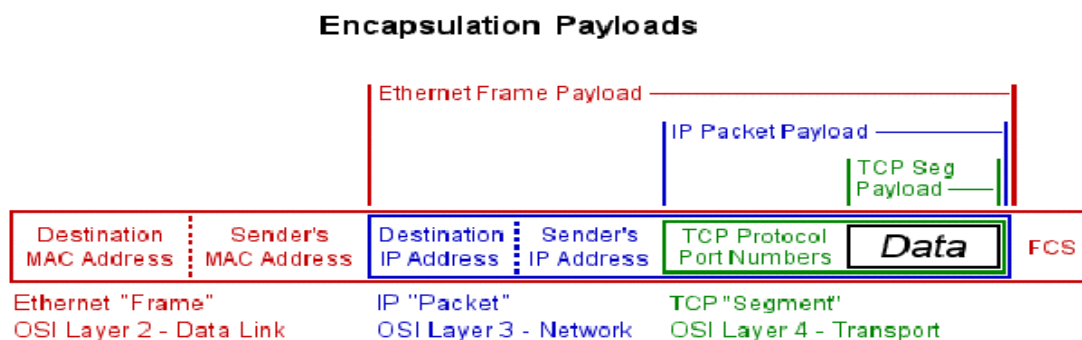


Σχήμα 4 : Ενθυλάκωση IP in IP

2.3 GRE (General Routing Encapsulation)

Το GRE είναι μια τεχνική ενθυλάκωσης που αναπτύχθηκε από τη Cisco και περιγράφεται στα RFC 1701 και 1702 τα οποία καθορίστηκαν το 1994. Σε ένα (Site-to-Site) VPN, αποτελεί τη βάση για τα άλλα πρωτόκολλα VPN και χρησιμοποιείται για “tunneling” ανάμεσα σε δρομολογητές πηγής και προορισμού (router-to-router). Τα GRE tunnels παρέχουν ένα ειδικό μονοπάτι κατά μήκος μίας διαμοιραζόμενης υποδομής WAN που δεν ανήκει μόνο σ' έναν χρήστη – πελάτη όπως το Internet. Ενθυλακώνουν την κίνηση με νέες επικεφαλίδες πακέτου, εξασφαλίζοντας έτσι τη διανομή τους σε ένα συγκεκριμένο προορισμό. Ένα GRE tunnel διαμορφώνεται ανάμεσα στο δρομολογητή πηγής και το δρομολογητή προορισμού. Τα πακέτα που πρόκειται να προωθηθούν κατά μήκος της διόδου ενθυλακώνονται με μία επικεφαλίδα GRE, μεταφέρονται κατά μήκος της διόδου και στο τέλος της αφαιρείται η επικεφαλίδα GRE.

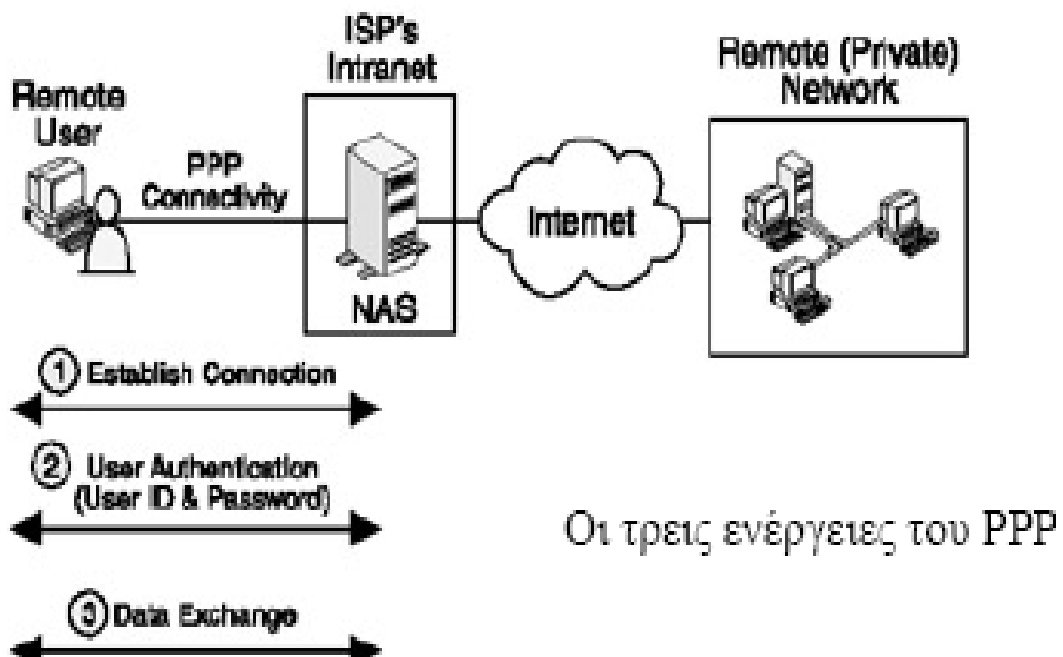
Το GRE αποτελεί συνήθως το πρωτόκολλο δημιουργίας της “κάψουλας” (**Encapsulating protocol**) που παρέχει το πλαίσιο εργασίας, για το πως θα δημιουργηθεί το πρωτόκολλο επιβάτη (**Passenger protocol**), για την μεταφορά του μέσω του πρωτοκόλλου μεταφοράς (**Carrier protocol**), που συνήθως βασίζεται στο IP. Αυτό συμπεριλαμβάνει πληροφορίες πάνω στο είδος του πακέτου που βάζουμε στην “κάψουλα” και πληροφορίες όσον αφορά την σύνδεση μεταξύ πελάτη και εξυπηρετητή.



Σχήμα 5 : Διαδικασία ενθυλάκωσης

2.4 PPP (Point To Point Protocol)

Σε ένα απομακρυσμένης πρόσβασης (Remote-Access) VPN, το tunneling συνήθως υλοποιείται με την βοήθεια του πρωτοκόλλου επικοινωνίας PPP (Point to Point Protocol) που περιγράφεται στο RFC 1661. Μέρος της σουίτας πρωτοκόλλων TCP/IP, είναι ένα πρωτόκολλο που μπορεί να χρησιμοποιηθεί πάνω σε πολλά φυσικά μέσα όπως δισύρματα χάλκινα καλώδια, οπτικές ίνες ή δορυφορική μετάδοση. Μια PPP σύνδεση μπορεί να μεταφέρει κυκλοφορία δεδομένων για πρωτόκολλα όπως το TCP/IP, AppleTalk, OSI, IPX. Τέλος το PPP μπορεί να διαχειριστεί συγχρονισμένη και ασύγχρονη μετάδοση δεδομένων χωρίς να περιορίζεται από την ταχύτητα μετάδοσης και έχει τρία στάδια λειτουργίας : (υλοποίηση σύνδεσης, αυθεντικοποίησης και μεταφοράς δεδομένων).



Σχήμα 6 : Χρήση του PPP, το οποίο λειτουργεί σε 3 στάδια

3 ΚΕΦΑΛΑΙΟ 3- Πρωτόκολλα VPN

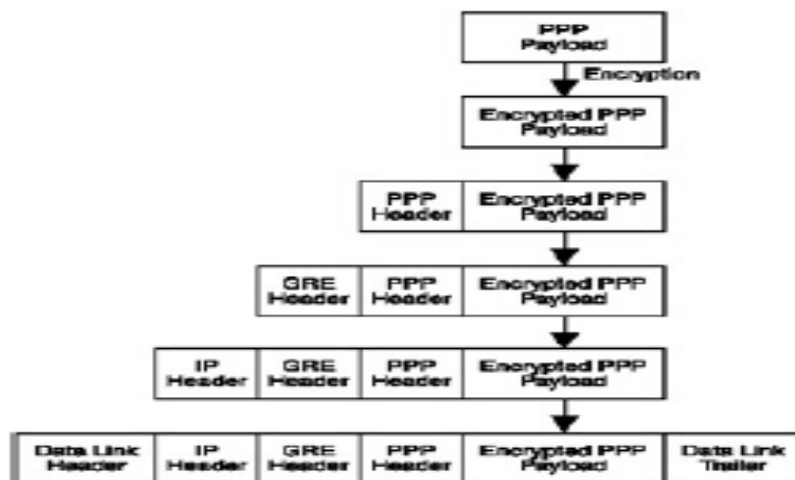
3.1 Πρωτόκολλα VPN επιπέδου Ζεύξης Δεδομένων (layer 2 OSI)

Τα Πρωτόκολλα που χρησιμοποιούνται από VPN εφαρμογές και βρίσκονται στο επίπεδο 2 του μοντέλου αναφοράς OSI, χρησιμοποιούν την τεχνική της ενθυλάκωσης και την βασική δομή του PPP για να υλοποιούν τα Remote-Access VPN και είναι :

- **L2F (Layer 2 Forwarding)** : Αναπτύχθηκε από την Cisco, έχει δικούς του μηχανισμούς για την ενθυλάκωση των πακέτων και δεν χρησιμοποιεί το GRE. Χρησιμοποιεί κάθε μέθοδο πιστοποίησης που υποστηρίζεται από το PPP.
- **PPTP (Point-to-Point Tunneling Protocol)** : Το PPTP δημιουργήθηκε από το PPTP Forum, μια διεθνής εταιρική συνεργασία των US Robotics, Microsoft, 3COM, Ascend και ECI Telematics. Είναι ευρέως διαδεδομένο μιας και αποτελεί το εξορισμού πρωτόκολλο δημιουργίας VPN στα λειτουργικά συστήματα της Microsoft. Χρησιμοποιεί το GRE ενθυλακώνοντας τα πακέτα δεδομένων IP σε πακέτα GRE πριν τα στείλει, διαμέσου των διαύλων επικοινωνίας, στον προορισμό τους. Υποστηρίζει κωδικοποίηση και χρησιμοποιεί τις μεθόδους πιστοποίησης που υποστηρίζονται από το PPP.
- **L2TP (Layer 2 Tunneling Protocol)** : Το L2TP αποτελεί το προϊόν συνεργασίας μεταξύ των μελών του PPTP Forum, Cisco και της IETF (Internet Engineering Task Force). Είναι το αποτέλεσμα της συγχώνευσης του PPTP και του L2F, ένας συνδυασμός των καλύτερων χαρακτηριστικών

τους, το οποίο ορίστηκε για λόγους συμβατότητας όλων των δικτύων μεταξύ τους. Παρέχει, ακόμη, συμπίεση βασισμένη σε λογισμικό. Επειδή υποστηρίζει πλήρως το IPSec και χρησιμοποιεί πολλά χαρακτηριστικά του για να επιτύχει μεγαλύτερη ασφάλεια, θεωρείται ότι παρέχει υπηρεσίες όχι μόνο δεύτερου αλλά και τρίτου επιπέδου και μπορεί να χρησιμοποιηθεί ως πρωτόκολλο tunneling είτε για Site-to-Site είτε για Remote-Access VPN.

Όλα αυτά τα πρωτόκολλα, ενσωματώνουν το 2ο επίπεδο (Data Link layer) στο πρωτόκολλο IP. Το πρωτόκολλο PPP λειτουργεί σε αυτό το επίπεδο και χρησιμοποιείται για να μεταφέρει το IP πρωτόκολλο και άλλα μέσω σειριακών και ψηφιακών συνδέσεων. Τυπικά οι συνδέσεις PPP πραγματοποιούνται μεταξύ ενός πελάτη και ενός κεντρικού υπολογιστή (host). Με παρόμοιο τρόπο τα PPTP, L2F και L2TP χρησιμοποιούνται για να “διασωληνώσουν” (tunneling) συνδέσεις τύπου PPP μέσω του διαδικτύου που τερματίζουν σε κάποιον κεντρικό υπολογιστή. Επειδή χρησιμοποιούν τη δομή του PPP πρωτοκόλλου, ενσωματώνουν κάποια χαρακτηριστικά του όπως δυναμική ανάθεση διεύθυνσης (DHCP), βασική αυθεντικοποίηση και συμπίεση.



Σχήμα 7 : PPTP / Ενθυλάκωση GRE

3.1.1 Διαφορές L2F, PPTP και L2TP

Με τα πρωτόκολλα PPTP και L2F μπορεί να χρησιμοποιηθεί όποια μέθοδος αυθεντικοποίησης χρησιμοποιεί και το PPP , συμπεριλαμβανομένων των PAP και CHAP. Στην διαδικασία της κρυπτογράφησης το PPTP χρησιμοποιεί τον αλγόριθμο RC4 με κλειδιά μήκους 40 και 128 bits , ενώ το L2F υποστηρίζει 40 ή 56 bit DES κρυπτογράφηση καθώς και το πρωτόκολλο IPSec. Το πρωτόκολλο L2TP μπορεί να χρησιμοποιηθεί στη θέση των PPTP και L2F και μπορεί να εφαρμόσει τις ίδιες μεθόδους αυθεντικοποίησης ενώ σαν μέθοδος κρυπτογράφησης προτιμάται το IPSec.

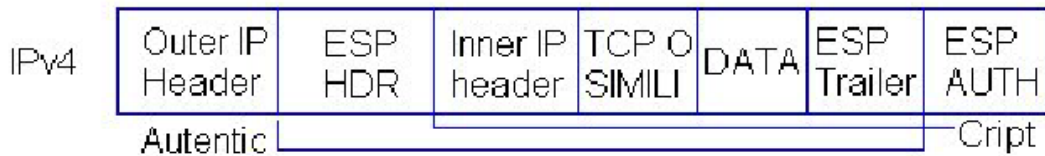
3.2 Πρωτόκολλα VPN επιπέδου Δικτύου (layer 3 OSI)

3.2.1 IPSec (IP Security)

Το πρωτόκολλο IPSec (Internet Security Protocol) δημιουργήθηκε για να καλύψει, τις έλλειψεις του TCP/IP σε διαδικασίες αυθεντικοποίησης και κωδικοποίησης, που το καθιστούν επισφαλές από την φύση του για οποιαδήποτε υπηρεσία ή εφαρμογή που βασίζεται πάνω του.

Το IPSec προτείνει σχεδιαστικές τεχνικές για μια υψηλού επιπέδου κατασκευαστική δομή, και όχι συγκεκριμένες μεθοδολογίες αλγορίθμων κωδικοποίησης ή μεθοδολογίες ανταλλαγής μυστικών κλειδιών.

Δημιουργήθηκε το 1995 και συντηρείται από μία ομάδα εργασίας του IETF. Σκοπός του είναι να παρέχει ασφάλεια σε επίπεδο πακέτων IP και συγκεκριμένα να καλύψει τα θέματα ασφαλείας του IPv6 με τα RFC 1825 – 1829, του οποίου και αποτελεί υποχρεωτικό μέρος. Λόγω όμως της αργής προώθησης του IPv6 και της αυξημένης ανάγκης για ασφάλεια στο κλασικό IPv4, το IPSec προσαρμόστηκε ώστε να είναι συμβατό και με το IPv4.



Σχήμα 8 : Η δομή των IPv4 και IPv6 πακέτων με IPSec.

Τα χαρακτηριστικά του IPSec ορίζονται από αρκετά RFC που προσδιορίζουν τις λεπτομέρειες για τα διαφορετικά τμήματα του πρωτοκόλλου, ενώ όλα ορίζουν πώς αυτά αλληλεπιδρούν μεταξύ τους. Πιο συγκεκριμένα, μια σειρά από RFC (2401 - 2412) ορίζουν τα πρωτόκολλα εκείνα που απαιτούνται για την δημιουργία VPN, π.χ. το RFC 2401 (IPSec), RFC 2402 (Authentication Header), RFC 2406 (Encapsulating Security Payload) και άλλα.

Οι υπηρεσίες που προσφέρει το IPSec παρέχουν ασφαλείς συνδέσεις, πράγμα που το επιτυγχάνει με :

- 1 Υπηρεσίες ακεραιότητας δεδομένων με πιστοποίηση αυθεντικότητας χωρίς σύνδεση (connectionless data integrity authentication).
- 2 Προαιρετική προστασία απέναντι στις επαναλήψεις (anti-replay).
- 3 Ταυτοποίηση προέλευσης δεδομένων (data origin authentication).
- 4 Εμπιστευτικότητα ροής δεδομένων (data flow confidentiality).

Οι υπηρεσίες αυτές εξασφαλίζονται στο επίπεδο IP και έτσι προσφέρεται

προστασία σ' αυτό και σε όλα τα παραπάνω επίπεδα, ανεξάρτητα από τα πρωτόκολλα που χρησιμοποιούνται σε αυτά.

Το IPSec σχεδιάστηκε για να χρησιμοποιηθεί σε μεγάλο εύρος εφαρμογών και όταν εφαρμοστεί σωστά, δεν επηρεάζει τα δίκτυα και τους υπολογιστές που δεν το υποστηρίζουν. Αποτελεί επίσης σημαντικό πλεονέκτημά του, ότι προστατεύει όλη τη κίνηση του δικτύου, μειώνοντας το συνολικό φόρτο “overhead” για τη δημιουργία ασφαλών καναλιών επικοινωνίας για τις εφαρμογές. Τέλος, απλοποιεί την υλοποίηση υπηρεσιών ασφάλειας, αφού συνήθως αυτή είναι πιο πολύπλοκη όταν οι υπηρεσίες υλοποιούνται σε υψηλότερο επίπεδο σε σχέση με τα χαμηλότερα.

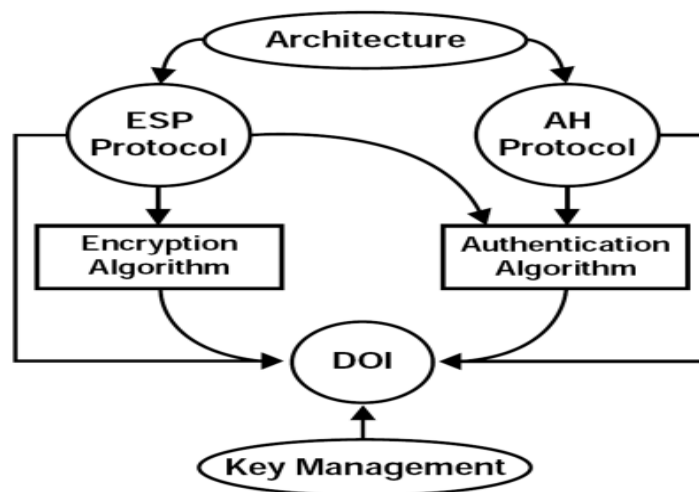
Ωστόσο, η υλοποίηση υπηρεσιών ασφάλειας σε επίπεδο δικτύου, δυσκολεύει τη διαχείριση τους στο επίπεδο εφαρμογής για πολυχρηστικά συστήματα. Παρά την ύπαρξη αυτής της αδυναμίας, μπορεί να υποθεθεί ότι με χρήση διάφορων μηχανισμών έλεγχου από τις εφαρμογές και διαχείρισης από τους χρήστες, επιτυγχάνεται η ισορροπία ασφάλειας και ευχρηστίας που απαιτεί κάθε σύστημα.

3.2.2 IPSec Αρχιτεκτονική

Το IPSec αποτελείται από τρεις συνιστώσες : Το Authentication Header (AH), το Encapsulating Security Payload (ESP) και το Internet Key Exchange (IKE) για τη προστασία των πακέτων IP. Οι συνιστώσες αυτές αποτελούν ένα σύνολο από επιπλέον επικεφαλίδες (headers) που υποστηρίζουν και υλοποιούν τα δύο πρωτόκολλα, το AH και το ESP.

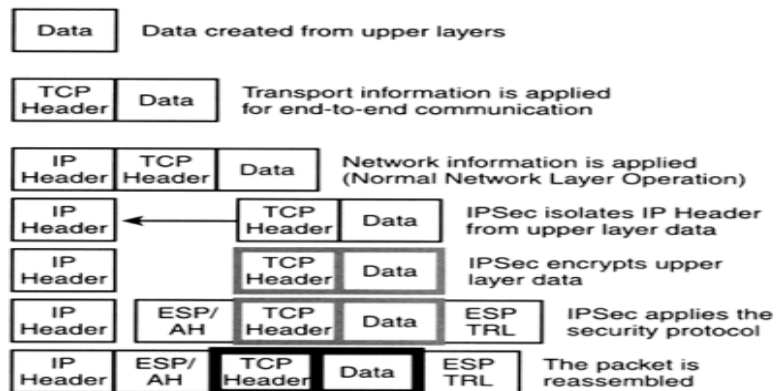
Το AH παρέχει ακεραιότητα δεδομένων, ταυτοποίηση προέλευσης δεδομένων και προστασία απέναντι στις επαναλήψεις. Το ESP παρέχει τα ίδια χαρακτηριστικά και επιπλέον εμπιστευτικότητα ροής δεδομένων. Τα AH και ESP δεν ορίζουν ποιοί ακριβώς αλγόριθμοι θα παρέχουν αυτές τις υπηρεσίες αλλά τον τρόπο που θα το κάνουν.

Το IPsec είναι ανεξάρτητο από τους τρέχοντες κρυπτογραφικούς αλγόριθμους και μπορεί να χρησιμοποιήσει καινούργιους όταν γίνουν διαθέσιμοι. Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται συνήθως για το AH είναι οι MD5 και SHA1 και για το ESP οι DES, 3DES και AES. Οι αλγόριθμοι αυτοί λειτουργούν με τρόπο που απαιτεί την ύπαρξη μυστικών κλειδιών τα οποία μπορούν είτε να δημιουργούνται δυναμικά κατά τη διαπραγμάτευση (negotiation) μιας σύνδεσης, είτε να είναι προ-μοιρασμένα (preshared). Η τελευταία λύση δεν είναι κατάλληλη για ευρεία εφαρμογή και συνήθως χρησιμοποιείται η διαδικασία ανταλλαγής μυστικών κλειδιών που χρησιμοποιεί δημόσια ψηφιακά πιστοποιητικά και βασίζεται στα πρωτόκολλα ISAKMP / Oakley / IKE (Internet Key Exchange) και στο πρότυπο πιστοποίησης X.509. Οι παράμετροι που απαιτούνται από τους αλγόριθμους που χρησιμοποιούνται για αυθεντικοποίηση, όπως ο MD5 και ο AES για κρυπτογράφηση, ορίζονται στο Domain of Interpretation (DOI). Το IPsec ορίζει, πώς αυτά τα διαφορετικά πρωτόκολλα αλληλεπιδρούν μεταξύ τους για να παρέχουν την επιθυμητή λειτουργικότητα. Το **σχήμα 9** δείχνει πως συνδέονται τα επιμέρους συστατικά του IPsec.



Σχήμα 9 : Συστατικά του IPsec.

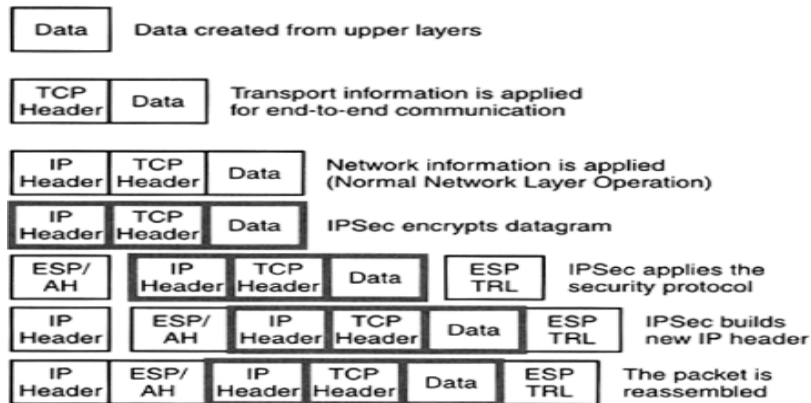
Το IPSec χρησιμοποιεί δύο βασικές μεθόδους για την υλοποίησή του, τις Συσχετίσεις Ασφάλειας (Security Associations - SA) και το Tunneling. Επίσης, έχει δύο καταστάσεις λειτουργίας (modes), Μεταφοράς (transport mode) και Σήραγγας (tunnel mode). Στην κατάσταση Μεταφοράς, οι αρχικές επικεφαλίδες του IP πακέτου μένουν ανέπαφες, έχοντας το πλεονέκτημα της προσθήκης μόνο μερικών bytes σε κάθε πακέτο. Ο βασικός περιορισμός του είναι ότι δεν είναι συμβατό με υπηρεσίες gateway, είναι κατάλληλο δηλαδή μόνο για end-to-end επικοινωνία που χρησιμοποιείται κυρίως για διασύνδεση μεταξύ δύο LAN ή για client-server εφαρμογές. Είναι ο τρόπος στην ουσία, με τον οποίο δύο συσκευές του δικτύου (και όχι οι χρήστες) μπορούν να επικοινωνήσουν. Αυτό συμβαίνει επειδή κατά την λήψη των πακέτων η επεξεργασία του IPSec γίνεται αφού έχει προηγηθεί η επεξεργασία του IP και πλέον δεν υπάρχει διαθέσιμη πληροφορία διευθυνσιοδότησης.



Σχήμα 10 : IPsec Transport mode

Στην κατάσταση Σήραγγας, όλο το αρχικό IP πακέτο, συμπεριλαμβανομένης και της αρχικής IP διεύθυνσης κρυπτογραφείται και γίνεται φορτίο (payload) ενός καινούριου IP πακέτου, που έχει μία νέα IP διεύθυνση. Το πακέτο έχει έτσι δύο IP headers που περιέχουν πληροφορίες διευθυνσιοδότησης και μπορεί να

χρησιμοποιηθεί για να παρέχει υπηρεσίες gateway .Αποτελεί τον πιο κοινό τρόπο λειτουργίας όσον αφορά τη σύνδεση μεταξύ δύο gateway συσκευών “network-to-network” ή μια σύνδεση μεταξύ μιας gateway συσκευής και ενός τερματικού σταθμού “host-to-network”.



Σχήμα 11 : IPsec Tunnel mode

3.3 Πρωτόκολλα VPN επιπέδου Μεταφοράς (layer 4 OSI)

3.3.1 SSL / TLS

Η χρήση “ανοιχτών” δικτύων, όπως το Internet, για μετάδοση κρίσιμων - προσωπικών δεδομένων οδήγησε στην ανάπτυξη ασφαλών δικτυακών πρωτοκόλλων για την κρυπτογράφηση και διασφάλιση αυτής της επικοινωνίας. Το SSL (Secure Socket Layer) είναι ένα πρωτόκολλο που ανήκει στην κατηγορία αυτή και παρέχει ασφάλεια πάνω από το TCP/IP. Αναπτύχθηκε, αρχικά, από την Netscape στις αρχές της δεκαετίας του 1990. Στη συνέχεια η Microsoft δημιούργησε παρόμοιο κώδικα και τελικά στα τέλη του '90 σχηματίστηκε στην IETF η ομάδα TLS, στα πλαίσια μιας προσπάθειας να συγχωνευτούν οι διαφορετικές προσεγγίσεις σ' ένα ενοποιημένο ανοιχτό πρότυπο το TLS (Transport Layer Security), το οποίο ουσιαστικά είναι το SSL version 3 με διάφορες διορθώσεις και

βελτιώσεις. Μέσω αυτού υλοποιούνται τα VPN επιπέδου Μεταφοράς. Ένα SSL/TLS VPN παρέχει στους τελικούς χρήστες εξουσιοδοτημένη και ασφαλή πρόσβαση σε εφαρμογές όπως HTTP, client/server και file sharing. Είναι ανεξάρτητο από το λειτουργικό σύστημα και επιτρέπει την κλιμάκωση στον έλεγχο πρόσβασης στις εφαρμογές, καθιστώντας το ιδανικό για χρήστες που μετακινούνται και επιθυμούν να έχουν απομακρυσμένη πρόσβαση από ένα μη ασφαλές σημείο.

3.3.2 SSL αρχιτεκτονική

Το SSL διαχειρίζεται την εμπιστευτικότητα και την ακεραιότητα του καναλιού μετάδοσης με κατάλληλη κρυπτογράφηση των δεδομένων, καθώς και την αυθεντικοποίηση του server αλλά και του client όταν αυτό είναι απαραίτητο. Οι υπηρεσίες που παρέχει είναι οι εξής :

- **Αμοιβαία αυθεντικοποίηση** : Ο server ταυτοποιείται στον client και αντίστροφα, μέσω των πιστοποιητικών δημόσιου κλειδιού (X.509) που ανταλλάσσουν κατά τη διάρκεια του SSL handshake.
- **Ιδιωτικότητα μηνύματος** : Εξασφαλίζεται μέσω κρυπτογράφησης με ιδιωτικό και δημόσιο κλειδί. Όλη η κίνηση ανάμεσα στον SSL server και client κρυπτογραφείται με τη χρήση ενός κλειδιού και ενός αλγόριθμου κρυπτογράφησης που διαπραγματεύονται κατά τη διάρκεια μιας SSL χειραψίας (handshake).
- **Ακεραιότητα μηνύματος** : Το SSL χρησιμοποιεί ένα συνδυασμό μυστικού κλειδιού και ειδικών hash συναρτήσεων (MAC - Message Authentication Code).

Το SSL απαιτεί ο κάτοχος του πιστοποιητικού να υπογράψει ψηφιακά κάποια δεδομένα, τα οποία ανταλλάσσονται κατά τη διάρκεια του handshake, αποδεικνύοντας έτσι ότι είναι ο νόμιμος ιδιοκτήτης του πιστοποιητικού. Τα δεδομένα αυτά συμπεριλαμβάνουν και το ίδιο το πιστοποιητικό, ούτως ώστε αποκλείεται κάποιος να υποκρίνεται κάποιον άλλον παρουσιάζοντας το πιστοποιητικό του. Το πιστοποιητικό δεν αυθεντικοποιεί από μόνο του, αλλά σε συνδυασμό με το σωστό ιδιωτικό κλειδί. Η όλη διαδικασία γίνεται “διάφανα” χωρίς να απαιτείται αλληλεπίδραση με τον χρήστη.

Η έκδοση SSL 2.0 υποστηρίζει μόνο αυθεντικοποίηση εξυπηρετητή (server authentication), ενώ η έκδοση SSL 3.0 παρέχει επιπλέον αυθεντικοποίηση πελάτη (client authentication).

Το SSL κάνει χρήση του TCP για την μεταφορά των δεδομένων και έχει σχεδιαστεί ώστε να παρέχει αξιόπιστη “end-to-end” ασφαλή και διάφανη “transparent” υπηρεσία, ανεξάρτητα από την εφαρμογή που χρησιμοποιείται από τον τελικό χρήστη.

Πιο συγκεκριμένα, το SSL δεν αποτελεί ένα, αλλά δύο επίπεδα πρωτοκόλλων, όπως φαίνεται στο παρακάτω **σχήμα 12**.

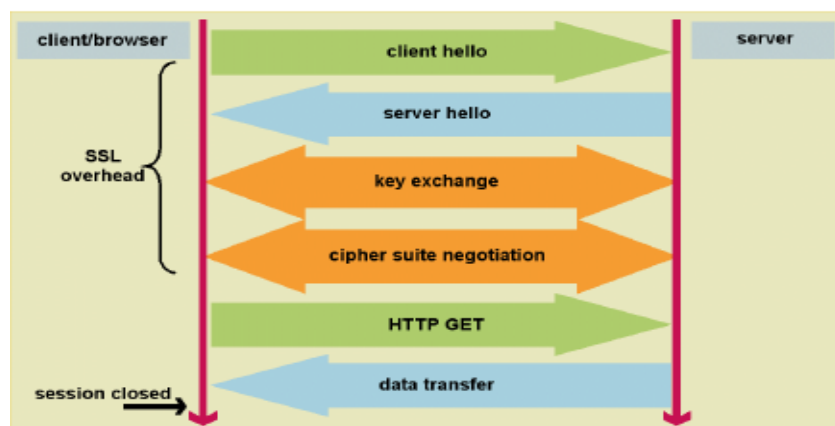
SSL Handshake Protocol	SSL Change Ciphert Spec Protocol	SSL Alert Protocol	HTTP
SSL Record Protocol			
TCP			
IP			

Σχήμα 12 : SSL Protocol Stack

Συνοπτικά, το SSL Record Protocol παρέχει βασικές υπηρεσίες ασφάλειας σε πρωτόκολλα υψηλότερων επιπέδων όπως το HTTP, υπηρεσίες εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων. Τα SSL πρωτόκολλα υψηλότερου επιπέδου που μπορούν να στρωματοποιούνται πάνω από το Record Protocol και χρησιμεύουν στη διαχείριση των SSL ανταλλαγών είναι: το Handshake Protocol, το Change Cipher Spec Protocol και το Alert Protocol.

Σημαντικότερο είναι το SSL Handshake Protocol, ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών, που διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και του client, εάν ζητηθεί. Η ανταλλαγή πληροφοριών, κατά την εφαρμογή του πρωτοκόλλου γίνεται ως εξής :

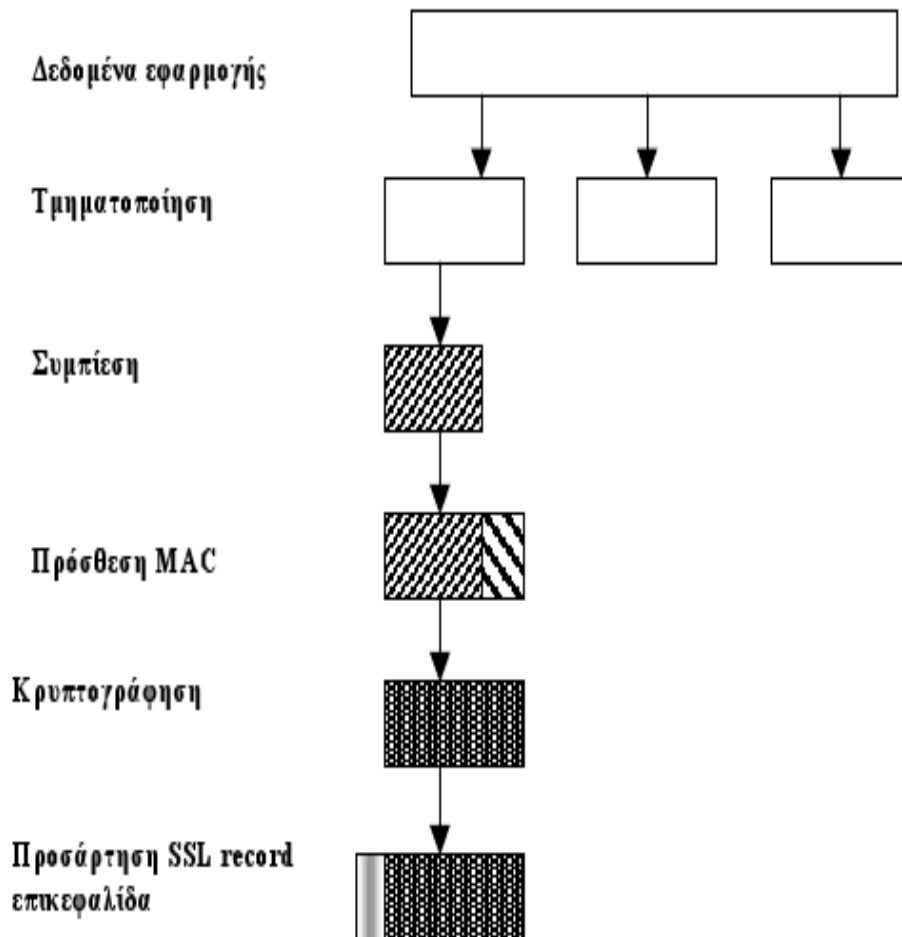
1. Ο client ξεκινά την σύνδεση.
2. Ο server απαντά, στέλνοντας στον πελάτη το digital ID του, και μπορεί να ζητήσει για ταυτοποίηση το digital ID του client.
3. Ο client επιβεβαιώνει το digital ID του server, και αν χρειαστεί στέλνει το δικό του digital ID για ταυτοποίηση στο server.
4. Η διαδικασία ταυτοποίησης ολοκληρώνεται. Ο client στέλνει το κλειδί συνεδρίας κρυπτογραφημένο με το δημόσιο κλειδί του server.
5. Ένα ασφαλές κανάλι επικοινωνίας δημιουργείται μεταξύ server και client.



Σχήμα 13 : SSL/TLS handshake

Μετά την ολοκλήρωση του SSL Handshake Protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL Record Protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας.

Συγκεκριμένα, το SSL Record Protocol λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και πραγματοποιεί κατακερματισμό “fragmentation”, συμπίεση “compression” και κρυπτογράφηση δεδομένων, σύμφωνα με την εκάστοτε μέθοδο συμπίεσης και τον αλγόριθμο κρυπτογράφησης που έχουν οριστεί από το Handshake Protocol.



Σχήμα 14 : Λειτουργίες του SSL Record Protocol

3.3.3 SSL/TLS Κλειδιά και Κρυπτογράφηση

Για την εφαρμογή του SSL/TLS χρησιμοποιείται ένας αριθμός από κλειδιά: το δημόσιο κλειδί του server “master key”, το server-write-key και το client-write-key που παράγονται μέσω μιας συνάρτησης hash από το “master key”, έναν τακτικό “ordinal” χαρακτήρα, την πρόκληση και το “id” της σύνδεσης

Για να εξασφαλιστεί η ασφαλής μετάδοση δεδομένων και μηνυμάτων χρησιμοποιείται η RSA κρυπτογράφηση δημόσιου κλειδιού, στην οποία μέσω ενός ζεύγους κλειδιών “δημόσιο και ιδιωτικό”, οποιαδήποτε πληροφορία κρυπτογραφείται με το ένα κλειδί, μπορεί ν’ αποκρυπτογραφηθεί μόνο με το άλλο. Σε κάθε σύνδεση client - server χρησιμοποιείται ένα διαφορετικό κλειδί συνόδου (session key), το οποίο λήγει μετά την συμπλήρωση κάποιας ώρας. Για την ανταλλαγή αυτού του κλειδιού καθώς και για την αμοιβαία ταυτοποίηση των συναλλασσόμενων μερών χρησιμοποιείται η κρυπτογραφία δημόσιου κλειδιού. Τέλος η συμμετρική κρυπτογραφία που είναι πιο γρήγορη, χρησιμοποιείται για την κρυπτογράφηση της συνόδου.

Block Cipher		Stream Cipher	
Αλγόριθμος	Μέγεθος κλειδιού	Αλγόριθμος	Μέγεθος κλειδιού
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

Σχήμα 15 : Αλγόριθμοι που χρησιμοποιούνται στο SSL Record Protocol.

3.4 OpenVPN

Το OpenVPN project δημιουργήθηκε το 2001 από τον James Yonan ο οποίος το

ονόμασε έτσι από σεβασμό στις βιβλιοθήκες και τα προγράμματα του OpenSSL project που χρησιμοποίησε για την υλοποίηση της εφαρμογής του, τονίζοντας έτσι, ότι πρόκειται για ένα λογισμικό ανοιχτού κώδικα (Open Source) και δωρεάν (Free Software).

Είναι μια SSL/TLS VPN εφαρμογή, που βασίζεται στην υποδομή του SSL/TLS για την δημιουργία των “tunnel” και την διαδικασία κρυπτογράφησης. Δημιουργεί την ίδια διασύνδεση δύο άκρων που εφαρμόζεται και από το IPSec, υλοποιώντας VPN συνδέσεις point-to-point, point-to-network και network-to-network (server-to-multiclient), οι οποίες είναι κρυπτογραφημένες συνδέσεις όπου παρέχεται υπηρεσία αυθεντικοποίησης. Επιτρέπει επίσης τη σύνδεση ακόμη και μέσα από firewall και NAT.

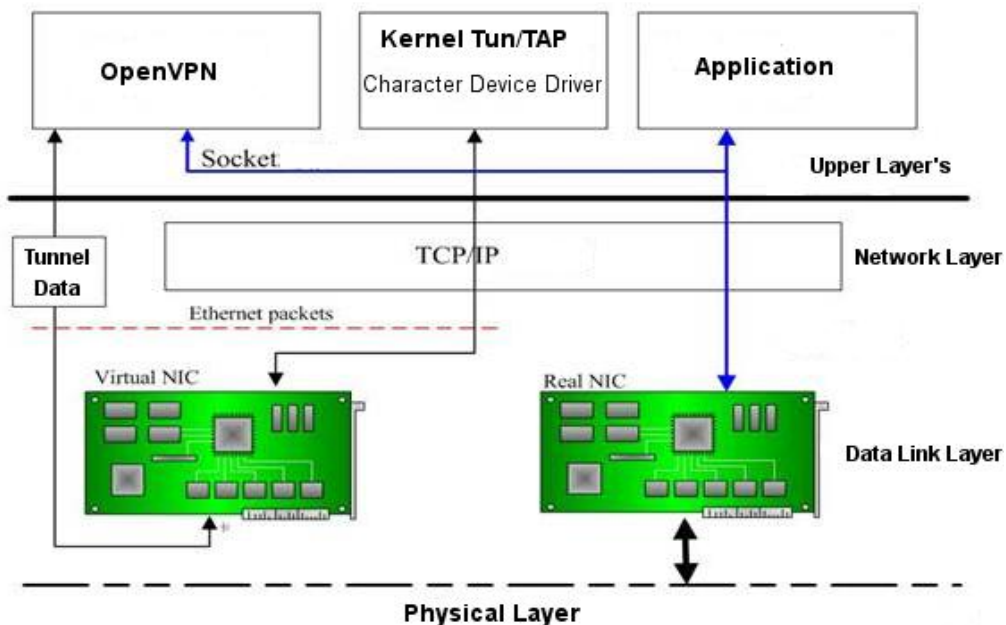
Μια εφαρμογή VPN, συνήθως πρέπει να επικοινωνήσει με τον πυρήνα (kernel) του λειτουργικού συστήματος για να εφαρμόσει κρυπτογράφηση σε μια διασύνδεση, επιτυγχάνοντας έτσι πρόσβαση χαμηλού επιπέδου με το υλικό, μέσω του οποίου γίνεται η διασύνδεση. Για να γίνει αυτό, πρέπει να γίνουν κάποιες εξεζητημένες αλλαγές στον πυρήνα λειτουργικού συστήματος. Το OpenVPN προορίζεται για απλούς χρήστες, αφού για να λειτουργήσει, δεν προαπαιτεί κάτι τέτοιο.

Σημαντικά πλεονεκτήματά του είναι η εύκολη προσαρμοστικότητα του στα λειτουργικά συστήματα, η ευκολία εγκατάστασης και ρύθμισης, η ευελιξία του όπως και το γεγονός ότι είναι λογισμικό ανοιχτού κώδικα που διανέμεται δωρεάν. Όλα τα παραπάνω, το καθιστούν μια πολύ καλή λύση δημιουργίας ασφαλών VPN tunnels, που γίνεται όλο και πιο δημοφιλής.

3.4.1 OpenVPN Αρχιτεκτονική

Το OpenVPN χρησιμοποιεί για τη δημιουργία “tunnel”, εικονικές συσκευές διασύνδεσης (virtual interfaces), στις οποίες ο έλεγχος και η προσβάσιμη γίνεται

από τον χρήστη (user space), χωρίς να εξαρτάται από τον πυρήνα του λειτουργικού συστήματος, παρέχοντας έτσι, ευκολία στην διαχείριση και μεγαλύτερη ευελιξία στην εγκατάσταση του, σε συστήματα διαφορετικών αρχιτεκτονικών. Με τον τρόπο αυτό καθίσταται πιο ασφαλές σε σχέση με το IPSec, με το οποίο είναι δυνατόν να συνυπάρχει χωρίς προβλήματα, στο ίδιο σύστημα. Σημαντικό μειονέκτημά του είναι ότι, η επικοινωνία και η διαχείριση των πακέτων γίνεται σε υψηλότερο επίπεδο σε σχέση με το IPSec, έχοντας ως αποτέλεσμα να διαρκεί περισσότερο η επεξεργασία τους.



Σχήμα 16 : Λειτουργία του OpenVPN με TUN / TAP εικονική διασύνδεση

Για τη δημιουργία ενός VPN tunnel, μπορεί να χρησιμοποιηθεί είτε το TCP, είτε το UDP πρωτόκολλο. Συνήθως όμως χρησιμοποιείται το UDP έναντι του TCP, γιατί υπάρχει πρόβλημα όταν δημιουργούνται tunnel TCP συνδέσεων πάνω από το TCP. Το πρόβλημα απορρέει από τον τρόπο λειτουργίας του TCP, που

παρακολουθεί τη συνέχεια των πακέτων και ζητάει επαναποστολή αυτών που χάνονται, μέσω μηχανισμών που προσαρμόζουν το χρόνο αναμονής αυτού του αιτήματος. Ωστόσο, όταν υπάρχει ένα μόνο στρώμα (TCP layer) είναι καλό και επιθυμητό να γίνεται. Όταν όμως τα πακέτα συνεχίζουν να αποτυγχάνουν, το χρονικό αυτό διάστημα αλλάζει και αυξάνεται εκθετικά, έτσι εάν δημιουργηθούν συνδέσεις TCP πάνω από το TCP, τότε θα υπάρξουν και δυο επίπεδα ελέγχου ροής των πακέτων που το καθένα θα έχει, διαφορετικούς χρόνους αιτήσεων επαναποστολής. Κάτι που μπορεί να έχει ως αποτέλεσμα την ραγδαία μείωση της απόδοσης του συστήματος, εάν οι χρόνοι αυτοί έχουν μεγάλη διαφορά μεταξύ τους , επιβραδύνοντας σημαντικά την σύνδεση.

3.4.2 OpenVPN L3 / L2 modes (Routing - Bridging)

Το OpenVPN έχει δύο καταστάσεις (routing ή bridging) και αναλόγως, χρησιμοποιεί τον αντίστοιχο οδηγό εικονικής συσκευής διασύνδεσης. Χρησιμοποιώντας τον οδηγό “TAP” γεφυρώνει διαφορετικά δίκτυα μεταξύ τους (bridging), ενώ με τη χρήση του οδηγού “TUN” δρομολογεί τα διαφορετικά δίκτυα μεταξύ τους (routing).

Στην κατάσταση γέφυρας “bridging”, τα διαφορετικά δίκτυα ενώνονται σε ένα κοινό υποδίκτυο “subnet”. Έτσι, δεν απαιτείται να ρυθμιστούν και να δηλωθούν τα διαφορετικά “routes” των δικτύων και μπορούν να μεταδοθούν μέσω του tunnel τα “network-broadcasts”, επιτρέποντας να δουλέψουν χωρίς πρόβλημα εφαρμογές που βασίζονται σε αυτά, όπως το “NetBIOS file sharing” και το “Network Neighbourhood Browsing” των Windows.

Η κατάσταση λειτουργίας γέφυρας, μπορεί να χρησιμοποιηθεί για να περάσει πάνω από την εικονική “Ethernet” διασύνδεση οποιουδήποτε πρωτόκολλο ανώτερου επιπέδου όπως τα IPv4, IPv6, IPX, AppleTalk, κ.α. Αν και δεν παρέχει την ευελιξία, την αποδοτικότητα και την μεταβλητότητα που έχουν τα

δρομολογούμενα (routed) δίκτυα, όταν δεν είναι απαραίτητη, προτιμάται τις περισσότερες φορές η κατάσταση λειτουργίας δρομολόγησης μεταξύ των δικτύων.

3.4.3 OpenVPN Ασφάλεια

Το OpenVPN, κάνοντας χρήση των δυνατοτήτων που προέρχονται από το SSL/TLS, (ανεξαρτήτως του αλγορίθμου κρυπτογράφησης), προσφέρει κρυπτογράφηση των VPN tunnel με δύο τρόπους. Ο πρώτος είναι με χρήση ενός σταθερού “κοινού” κλειδιού (static key) που είναι γνωστό και έχει μεταφερθεί και στα δύο άκρα του tunnel με κάποιο ασφαλές τρόπο (π.χ. Sftp). Αντίθετα, ο δεύτερος με τη χρήση δημόσιου και ιδιωτικού κλειδιού και τη δημιουργία πιστοποιητικών ασφαλείας (ISO X.509) για τον server και τους clients μέσω μιας CA (Certification Authority).

Η δεύτερη μέθοδος προσφέρει μεγαλύτερο βαθμό ασφαλείας και ισχυρότερη κρυπτογράφηση. Δεν παρέχει, ωστόσο, την ευκολία στην χρήση και την απλότητα του μηχανισμού του σταθερού κλειδιού που είναι προτιμότερο να χρησιμοποιείται, όταν υπάρχει κάποιος ασφαλής και εύκολος τρόπος για τη διαμοίραση του κοινού κλειδιού στα δύο άκρα του VPN tunnel. Η επιλογή της μεθόδου γίνεται αναλόγως της σημαντικότητας και του περιεχόμενου των δεδομένων που χρειάζεται να διαφυλαχθούν. Μεγαλύτερη ασφάλεια σε κάθε περίπτωση, σημαίνει και μεγαλύτερη πολυπλοκότητα.

Η αυθεντικοποίηση των clients από τον server μπορεί να γίνει είτε με την χρήση των πιστοποιητικών ασφαλείας είτε με τη χρήση τεχνολογιών όπως LDAP,RADIUS,κ.α. Παράλληλα παρέχετε η δυνατότητα οποιασδήποτε άλλης μεθόδου αυθεντικοποίησης μέσω σεναρίων (scripts) με χρήση “username – password“.

4 ΚΕΦΑΛΑΙΟ 4- Υλοποίηση υπηρεσίας VPN

4.1 Δημιουργία υπηρεσίας VPN για το Τμήμα Πληροφορικής

Η σχεδόν καθολική χρήση της τεχνολογίας DSL ως τρόπος πρόσβασης στο Internet και η γενικότερη αντικατάσταση της dial-up πρόσβασης από always-on υπηρεσίες έχουν αλλάξει τις ανάγκες σχετικά με τη δικτυακή πρόσβαση των φοιτητών αλλά και του προσωπικού του Τμήματος. Δεν είναι πλέον αποτελεσματικό και ρεαλιστικό το να παρέχεται πρόσβαση στο εσωτερικό δίκτυο του Τμήματος με χρήση dial-up συνδέσεων. Παράλληλα, οι ανάγκες για απομακρυσμένη πρόσβαση σε υπηρεσίες που αποτελούν μέρος της εκπαιδευτικής διαδικασίας ορισμένων μαθημάτων έχουν αυξηθεί.

Ταυτόχρονα με τα παραπάνω, εγκαταστάθηκε και λειτουργεί στο Τμήμα Πληροφορικής ασύρματο δίκτυο με ελεύθερη πρόσβαση. Λόγω των προβλημάτων ασφαλείας που παρουσιάζει ένα ασύρματο δίκτυο όταν παρέχεται ελεύθερη πρόσβαση σε αυτό, οι άμεσα διαθέσιμες υπηρεσίες μέσω αυτού είναι περιορισμένες.

Για τους παραπάνω λόγους και ως στόχος της εργασίας αυτής, εγκαταστάθηκε και λειτουργεί στο Τμήμα η υπηρεσία VPN, μέσω της οποίας είναι πλέον δυνατή η παροχή εκτεταμένης ασφαλούς δικτυακής πρόσβασης στα μέλη του προσωπικού και τους φοιτητές του Τμήματος.

Σκοπός της υπηρεσία VPN του Τμήματος Πληροφορικής είναι:

- Η παροχή πρόσβασης στις Ηλεκτρονικές Βιβλιοθήκες από χώρους εκτός του ΤΕΙ
- Η παροχή πρόσβασης σε μη δημόσιες υπηρεσίες του Τμήματος
- Η παροχή ασφαλούς εξωτερικής πρόσβασης στις υπηρεσίες του Τμήματος

- Η παροχή ασφαλούς πρόσβασης στο ασύρματο δίκτυο του Τμήματος
- Η γενικότερη διευκόλυνση - ενίσχυση των σπουδών και της εκπαιδευτικής διαδικασίας.

Πέρα από τα παραπάνω, η υπηρεσία VPN δεν έχει ως σκοπό την απόκρυψη της ταυτότητας των χρηστών ή την παροχή δυνατότητας λειτουργίας υπηρεσιών από μεριάς χρηστών.

Δόθηκε, επίσης, ιδιαίτερη σημασία στο να μην υπάρξουν κενά ασφάλειας στις δικτυακές υποδομές του Τμήματος και στη διαχείριση των λογαριασμών των χρηστών.

4.1.1 Δυνατότητες – Περιορισμοί

Η υπηρεσία αυτή υλοποιεί ένα κρυπτογραφημένο, ασφαλές, ιδεατό κανάλι επικοινωνίας μεταξύ του προσωπικού υπολογιστή του χρήστη και του εσωτερικού δικτύου του Τμήματος Πληροφορικής του Τ.Ε.Ι Θεσσαλονίκης. Κατά τον τρόπο αυτό, ο σταθμός εργασίας του χρήστη μεταφέρεται εικονικά "μέσα" στο δίκτυο του Τ.Ε.Ι Θεσσαλονίκης, ανεξάρτητα από την φυσική και δικτυακή του θέση.

Η υπηρεσία κρυπτογραφεί με ιδιαίτερα ισχυρό τρόπο οποιαδήποτε δικτυακή επικοινωνία, καθιστώντας έτσι ασφαλή, κάθε μετάδοση δεδομένων μέσω αυτής, ακόμη και κάτω από μη-ασφαλείς συνθήκες όπως τα ανοιχτά ασύρματα δίκτυα και τα δίκτυα τρίτων (πχ. με μη-φοιτητική σύνδεση ADSL, ή σε περίπτωση που ο υπολογιστής βρίσκεται σε οργανισμό / εταιρεία / πανεπιστήμιο εκτός Τ.Ε.Ι). Με αυτόν τον τρόπο καθίσταται εφικτή η πρόσβαση σε Ηλεκτρονικές Βιβλιοθήκες και εκπαιδευτικές υπηρεσίες του Τμήματος όπως βάσεις δεδομένων, Video Server κ.α.

Η συγκεκριμένη υπηρεσία παροχής VPN πρόσβασης υλοποιείται με τη χρήση του ελεύθερου λογισμικού OpenVPN. Πρόσβαση σε αυτή μπορούν να έχουν όσες συσκευές διαθέτουν σχετικό client λογισμικό, το οποίο και διατίθεται ελεύθερα για

Windows, Linux, MacOSX καθώς και για ορισμένα PDA.

Η δικτυακή VPN σύνδεση γίνεται μέσω του firewall του Τμήματος Πληροφορικής, το οποίο πραγματοποιεί τον έλεγχο της δικτυακής πρόσβασης. Η αυθεντικοποίηση γίνεται με βάση τους λογαριασμούς που παρέχονται στο προσωπικό και τους φοιτητές του Τμήματος. Κάθε χρήστης μπορεί να έχει μόνο μία ενεργή VPN σύνδεση σε συγκεκριμένη χρονική στιγμή.

Τέλος η χρήση της υπηρεσίας συνιστάται για πρόσβαση στις ηλεκτρονικές βιβλιοθήκες από χώρους εκτός του χώρου του ΤΕΙ, για χρήση του ασύρματου δικτύου του Τμήματος και σε περιπτώσεις που η ασφάλεια του δικτύου στο οποίο συμμετέχει ο χρήστης δεν είναι επιβεβαιωμένη.

4.2 Θέματα υλοποίησης- Λογισμικό

4.2.1 OpenVPN

Το OpenVPN αποτελεί έναν ασφαλή τρόπο δημιουργίας VPN tunnels που προορίζεται για απλούς χρήστες. Αυτό, σε συνδυασμό με την εύκολη προσαρμοστικότητα του στα λειτουργικά συστήματα και το γεγονός ότι είναι λογισμικό ανοιχτού κώδικα που διανέμεται δωρεάν, οδήγησε στην επιλογή του για την υλοποίηση της υπηρεσίας VPN για το Τμήμα Πληροφορικής.

4.2.1.1 Πλεονεκτήματα του OpenVPN

Το OpenVPN εισήγαγε μια νέα γενιά VPN. Ενώ άλλες λύσεις VPN χρησιμοποιούν συχνά “proprietary - κλειστούς” ή μη τυποποιημένους μηχανισμούς το OpenVPN έχει μια σπονδυλωτή “modular” αντιμετώπιση για την παροχή υπηρεσιών ασφάλειας και δικτύωσης. Χρησιμοποιεί τους μηχανισμούς αυθεντικοποίησης και κρυπτογράφησης που παρέχονται από το SSL / TLS οι οποίοι δεν χαρακτηρίζονται από την πολυπλοκότητα άλλων VPN εφαρμογών,

όπως το IPsec. Ταυτόχρονα, προσφέρει μοναδικά πλεονεκτήματα σε σχέση με άλλες υλοποιήσεις VPN εφαρμογών :

- **Layer 2 και Layer 3 VPN:** Το OpenVPN προσφέρει δύο βασικούς τρόπους λειτουργίας είτε ως Layer 2 ή Layer 3 VPN. Έτσι τα OpenVPN tunnels μπορούν να μεταφέρουν εκτός από IP πακέτα, Ethernet Frames, IPX καθώς και Windows Net Browsing πακέτα (NetBIOS), τα οποία αποτελούν πρόβλημα στις περισσότερες άλλες λύσεις VPN.
- **Προστασία των απομακρυσμένων client μέσω του εσωτερικού Firewall :** Στην περίπτωση που ένας απομακρυσμένος client που συνδέεται με το κεντρικό υποκατάστημα μιας εταιρείας μέσω VPN, του παρέχεται πλέον η δυνατότητα, να αλλάξει τις ρυθμίσεις δικτύου στον Η/Υ του, έτσι ώστε όλη η κίνηση του δικτύου, να αποστέλλεται μέσω του tunnel. Προστατεύεται έτσι από το εσωτερικό firewall και το εκάστοτε φιλτράρισμα, που διενεργείται στο εταιρικό proxy πχ (Content Filtering Internet Proxy).
- **Οι OpenVPN συνδέσεις μπορούν να “περάσουν” μέσα από firewall :** Εφόσον υπάρχει πρόσβαση στο Internet και σε HTTPS ιστοσελίδες, τότε και το OpenVPN θα πρέπει να συνδέεται χωρίς προβλήματα.
- **Υποστήριξη proxy και παραμετροποίηση :** Το OpenVPN έχει υποστήριξη για proxy και μπορεί να ρυθμιστεί ώστε να λειτουργεί ως TCP ή UDP υπηρεσία είτε ως server είτε ως client. Στην περίπτωση λειτουργίας ως server, το OpenVPN απλά περιμένει μέχρι να το ζητήσει ο πελάτης “client” μιας σύνδεσης, ενώ ως πελάτης προσπαθεί να δημιουργήσει μια σύνδεση με κάποιον server ανάλογα με την παραμετροποίηση που του έχει γίνει.
- **Μόνο μια πόρτα στο firewall πρέπει να ανοίξει για να επιτρέψει τις**

εισερχόμενες συνδέσεις : Από την έκδοση OpenVPN 2.0 και έπειτα, ο VPN διακομιστής “server” επιτρέπει πολλαπλές εισερχόμενες συνδέσεις για το ίδιο το πρωτόκολλο, TCP ή UDP μέσω μόνο μιας πόρτας, ενώ εξακολουθεί να χρησιμοποιεί διαφορετική παραμετροποίηση για κάθε σύνδεση.

- **Η Εικονική διασύνδεση (virtual interface) επιτρέπει πολύ συγκεκριμένες ρυθμίσεις δικτύωσης και κανόνες firewall** : Όλοι οι κανόνες, οι περιορισμοί, οι μηχανισμοί προώθησης, καθώς και εφαρμογές όπως το NAT μπορούν να χρησιμοποιηθούν με το OpenVPN.
- **Υψηλή ευελιξία με εκτεταμένες “scripting” δυνατότητες** : Το OpenVPN προσφέρει πολλά σημεία κατά τη διάρκεια της σύνδεσης για να ξεκινήσει επιμέρους σενάρια “scripts”. Αυτά τα σενάρια μπορούν να χρησιμοποιηθούν για λόγους αυθεντικότητας και πολλές ακόμα ενέργειες.
- **Διαφανής και υψηλής απόδοσης υποστήριξη για τα δυναμικά IP** : Με τη χρήση του OpenVPN δεν χρειάζεται πλέον να χρησιμοποιούνται στατικές διευθύνσεις IP στις δύο πλευρές της σήραγγας. Και οι δύο απολήξεις της σήραγγας μπορούν να έχουν φθηνή DSL πρόσβαση με δυναμικές IP και οι χρήστες σπάνια θα παρατηρήσουν αλλαγή της IP διεύθυνσης και στις δύο πλευρές. Ακόμη και σε μια τέτοια περίπτωση όμως, μια Windows Terminal server ή μια Secure Shell (SSH) συνεδρία για παράδειγμα, θα φαίνεται να κολλάει μόνο για μερικά δευτερόλεπτα, αλλά δεν θα τερματιστεί και θα συνεχίσει μετά από μια μικρή παύση.
- **Δεν έχει προβλήματα με το NAT** : Τόσο ο OpenVPN server όσο και οι πελάτες (clients) μπορούν να είναι μέσα σε ένα δίκτυο χρησιμοποιώντας μόνο ιδιωτικές διευθύνσεις IP. Κάθε firewall μπορεί με χρήση του NAT να

στέλνει την κυκλοφορία της σήραγγας από τη μια άκρη στην άλλη.

- **Απλή εγκατάσταση σε οποιαδήποτε πλατφόρμα:** Η εγκατάσταση και η χρήση του είναι εξαιρετικά απλή. Το OpenVPN είναι ιδιαίτερα ελκυστικό, ειδικότερα εάν κάποιος έχει προσπαθήσει να δημιουργήσει IPsec συνδέσεις με διαφορετικές εφαρμογές.
- **Αρθρωτή σχεδίαση “Modular Design” :** Με υψηλό βαθμό απλότητας, τόσο στον τομέα της ασφάλειας αλλά και της δικτύωσης. Δεν υπάρχει άλλη λύση VPN που μπορεί να προσφέρει το ίδιο φάσμα δυνατοτήτων σε αυτό το επίπεδο ασφάλειας.

4.2.1.2 Σύγκριση του OpenVPN με το IPsec

Αν και το IPsec αποτελεί το πιο διαδεδομένο, εξ' ορισμού πρότυπο για τη δημιουργία VPN, υπάρχουν ωστόσο πολλά επιχειρήματα υπέρ της χρήσης OpenVPN. Στον παρακάτω πίνακα φαίνεται γιατί μπορεί να προτιμηθεί το OpenVPN αντί του IPsec (με "+" αναφέρονται τα πλεονεκτήματα και με "-" τα μειονεκτήματα) :

IPsec VPN	OpenVPN
+ Η πρότυπη τεχνολογία VPN.	- Εξακολουθεί να είναι μάλλον άγνωστο και δεν είναι συμβατό με το IPsec.
+ Hardware πλατφόρμες (συσκευές, υλοποιήσεις).	- Μόνο σε υπολογιστές, αλλά σε όλα τα λειτουργικά συστήματα. Εξαιρέση οι συσκευές, όπου τρέχουν τα ενσωματωμένα UNIX σαν το OpenWrt και παρόμοια.

<ul style="list-style-type: none">+ Γνωστοί τεχνολογία.+ Πολλές GUI εφαρμογές για διαχείριση.- Περίπλοκη τροποποίηση του IP stack.- Αναγκαία η κρίσιμη τροποποίηση του πυρήνα “kernel”.- Δικαιώματα διαχειριστή είναι απαραίτητα.- Διαφορετικές IPsec υλοποιήσεις των διαφόρων κατασκευαστών μπορεί να είναι ασύμβατες μεταξύ τους- Πολύπλοκη παραμετροποίηση και τεχνολογία.- Χρειάζεται εμπειρία και προχωρημένες γνώσεις.- Πολλές θύρες και τα πρωτόκολλα είναι αναγκαία να παραμετροποιηθούν στο firewall- Προβλήματα με τις δυναμικές IP διευθύνσεις και των δύο πλευρών (server / client)- Προβλήματα ασφαλείας με τις	<ul style="list-style-type: none">- Νέα τεχνολογία Εξακολουθεί να διαδίδεται και η αυξάνεται.- Δεν υπάρχει κάποια επαγγελματική γραφική GUI εφαρμογή. Ωστόσο, υπάρχουν μερικά ενδιαφέροντα και πολλά υποσχόμενα έργα “projects”+ Απλή τεχνολογία.+ Τυποποιημένες διεπαφές δικτύου και πακέτα.+ Το OpenVPN μπορεί να τρέξει σε επίπεδο χρήστη “user space”, και μπορεί να τρέξει σε ψευδό-περιβάλλον “chroot-ed” για λόγους ασφαλείας+ Τυποποιημένες τεχνολογίες κρυπτογράφησης.+ Καλά δομημένη, αρθρωτή τεχνολογία με εύκολη παραμετροποίηση.+ Εύκολη εκμάθηση και γρήγορη επιτυχία για αρχάριους+ Μόνο μια πόρτα “port” στο firewall χρειάζεται.+ Το DynDNS λειτουργεί άψογα με ταχύτερες επανασυνδέσεις+ SSL / TLS ως πρότυπο
--	---

τεχνολογίες IPsec.	κρυπτογράφησης. + Διαμόρφωση της κίνησης των δεδομένων “Traffic Shaping” + Ταχύτητα (μέχρι και 20 Mbps σε μια μηχανή 1Ghz) + Η συμβατότητα με firewall και proxies + Δεν παρουσιάζει προβλήματα με το NAT (οι δύο πλευρές μπορούν να ανήκουν σε δίκτυα με NAT) + Δυνατότητες και ευκολίες για μετακινούμενους χρήστες “road warriors”
--------------------	--

Σχήμα 17 : Σύγκριση του OpenVPN με το IPsec

Λόγω των διαφορετικών προσεγγίσεων όσον αφορά την υλοποίηση, δεν υπάρχουν συγκρούσεις μεταξύ των δύο τεχνολογιών. Είναι πολύ σημαντικό το ότι οι δύο λύσεις VPN μπορούν να χρησιμοποιηθούν παράλληλα, τουλάχιστον εάν χρησιμοποιείται περιβάλλον Linux ή κάποια εφαρμογή που βασίζεται σε αυτό.

4.2.2 Περιβάλλον GNU / Linux – Debian

Περιβάλλον GNU / Linux – Debian Το GNU/Linux είναι ένα λειτουργικό σύστημα βασισμένο στο μοντέλο του UNIX και συμβατό σε μεγάλο βαθμό με το πρότυπο POSIX (**P**ortable **O**perating **S**ystem **I**nterface for **U**nix). Χρησιμοποιεί τα δομικά συστατικά του GNU Project και τον Linux kernel. Ιδρυτής του GNU Project είναι ο Richard Stallman και αρχικός σχεδιαστής και δημιουργός του Linux kernel ο Linus

Torvalds. Τα δομικά αυτά συστατικά ανήκουν στη κατηγορία του λογισμικού ανοιχτού κώδικα (Free Software / Open Source Software)

Το Linux συνήθως χρησιμοποιείται με τη μορφή μιας διανομής (distribution). Για τη δημιουργία της υπηρεσίας VPN για το Τμήμα Πληροφορικής χρησιμοποιήθηκε η διανομή Debian, μια από τις πρώτες διανομές Linux που υπήρξαν.

Το Debian σαν σχέδιο εργασίας άρχισε το 1993 από τον Ίαν Μέρντοκ, φοιτητή τότε του πανεπιστημίου Purdue, όταν έγραψε το Μανιφέστο Debian το οποίο καλούσε για τη δημιουργία μιας διανομής linux η οποία θα αναπτύσσονταν με τρόπο ανοιχτό και βασιζόμενο στο πνεύμα του GNU/Linux. Διάλεξε το όνομα συνδυάζοντας το όνομα της τότε φιλενάδας του Ντέμπρα (Debra) με το δικό του (Ian).

Αποτέλεσμα του Debian Project, είναι μια δημοφιλής διανομή Linux, ελεύθερο λογισμικό που αναπτύσσεται μέσω της συνεργασίας εθελοντών από όλο τον κόσμο. Βασίζεται στον πυρήνα linux και στην ομάδα βασικών εργαλείων του εγχειρήματος GNU.

Το Debian είναι γνωστό για την αφοσίωσή του στη φιλοσοφία του Unix και του ελεύθερου λογισμικού. Είναι επίσης γνωστό για το πλήθος επιλογών και δυνατοτήτων που προσφέρει: Η τρέχουσα έκδοση περιλαμβάνει πάνω από 25.000 πακέτα λογισμικού για δώδεκα αρχιτεκτονικές υπολογιστών που το φάσμα τους κυμαίνεται από ARM αρχιτεκτονική, που διαθέτουν συνήθως ενσωματωμένα συστήματα, IBM s390 αρχιτεκτονική κεντρικού υπολογιστή μέχρι τις πιο κοινές x86 και PowerPC αρχιτεκτονικές που υπάρχουν στους μοντέρνους προσωπικούς υπολογιστές.

Το Debian είναι επίσης πολύ γνωστό για το σύστημα διαχείρισης πακέτων και το APT Advanced Packaging Tool (προηγμένο εργαλείο πακέτων) που διαθέτει και πιο συγκεκριμένα, για τις αυστηρές πολιτικές που υιοθετεί ως προς την ποιότητα των πακέτων και των εκδόσεων του και την ανοιχτή διαδικασία ανάπτυξης και ελέγχου. Αυτές οι πρακτικές κάνουν πιο εύκολες τις αναβαθμίσεις και την

εγκατάσταση ή αφαίρεση πακέτων. Το Debian δεν υποστηρίζεται από κάποια εταιρία, αλλά από το Debian Project και τον οργανισμό Software in the Public Interest καθώς και από δωρεές που γίνονται μέσω οργανισμών που προωθούν το ελεύθερο λογισμικό

4.2.3 Webmin - Διαχείριση μέσω Web

Το Webmin είναι μια εφαρμογή που προορίζεται για διαχειριστές εξυπηρετητών “server” οι οποίοι θα πρέπει να γνωρίζουν τουλάχιστον τα βασικά της κάθε υπηρεσίας που υπάρχει στον server τους. Απλοποιεί την καθημερινή τους εργασία αποφεύγοντας την ενασχόληση με αρχεία ρυθμίσεων. Η ρύθμιση ενός server με το Webmin προϋποθέτει βασική γνώση των υπηρεσιών.

Το Webmin είναι μια web εφαρμογή η οποία μπορεί να χρησιμοποιηθεί για την πλήρη διαχείριση ενός Linux Server. Μέσα από ένα web περιβάλλον, αποφεύγοντας αρχεία ρυθμίσεων, υπάρχει ότι είναι απαραίτητο για την διαχείρισή του server ενώ είναι προσβάσιμο, είτε από τον ίδιο τον υπολογιστή, είτε από το τοπικό δίκτυο, είτε φυσικά μέσω ενός απομακρυσμένου υπολογιστή.

Μερικά παραδείγματα για το τι μπορεί να ρυθμιστεί είναι: fstab, iptables, postfix, disk quota, apache, mysql κ.α., τα οποία θα πρέπει να είναι ήδη εγκατεστημένα. Το Webmin είναι απλώς ένα εργαλείο ρυθμίσεων και όχι εγκατάστασης υπηρεσιών.

Στη περίπτωση του VPN για το Τμήμα Πληροφορικής, χρησιμοποιείται για την εύκολη διαχείριση τις υπηρεσίας OpenVPN (Server / Client), των αρχείων ρυθμίσεων καθώς και της διαχείρισης και δημιουργίας των κρυπτογραφικών κλειδιών που αυτή χρειάζεται. Η ρύθμιση αυτή γίνεται μέσω του **OpenVPN-admin** αρθρώματος “module” του.

5 ΚΕΦΑΛΑΙΟ 5- Υλοποίηση Server

5.1 Εγκατάσταση OpenVPN Server

Για την υλοποίηση του OpenVPN server χρησιμοποιήθηκε ένας Linux Virtual Server με εγκατεστημένο το βασικό Debian σύστημα. Το “host name” του server είναι το “openvpn.it.teithe.gr” με δημόσια IP διεύθυνση “195.251.123.180”. Παρακάτω περιγράφεται ο τρόπος και η διαδικασία που ακολουθήθηκε για την εγκατάσταση της OpenVPN server υπηρεσίας σε αυτόν.

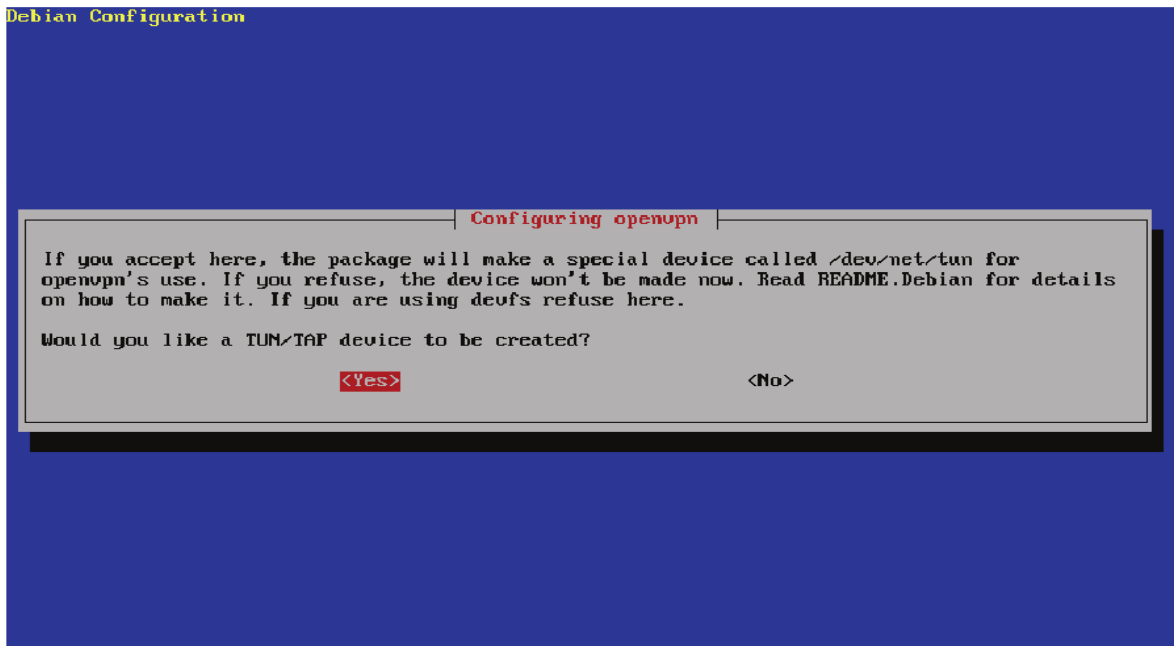
Έχοντας δικαιώματα διαχειριστή “root” στο σύστημα, χρησιμοποιήθηκε το έτοιμο πακέτο εγκατάστασης “deb” μέσω του συστήματος διαχείρισης πακέτων APT, καλώντας την εφαρμογή aptitude για να εγκατασταθεί και να ρυθμιστεί αυτόματα το OpenVPN και όλα τα προγράμματα και βιβλιοθήκες που αυτό χρειάζεται και προαπαιτεί : (OpenSSL βιβλιοθήκες, TUN / TAP εικονικούς οδηγούς και Lempel-Ziv-Oberhumer (LZO) βιβλιοθήκες συμπίεσης).

```
openvpn:~# aptitude install openvpn
```

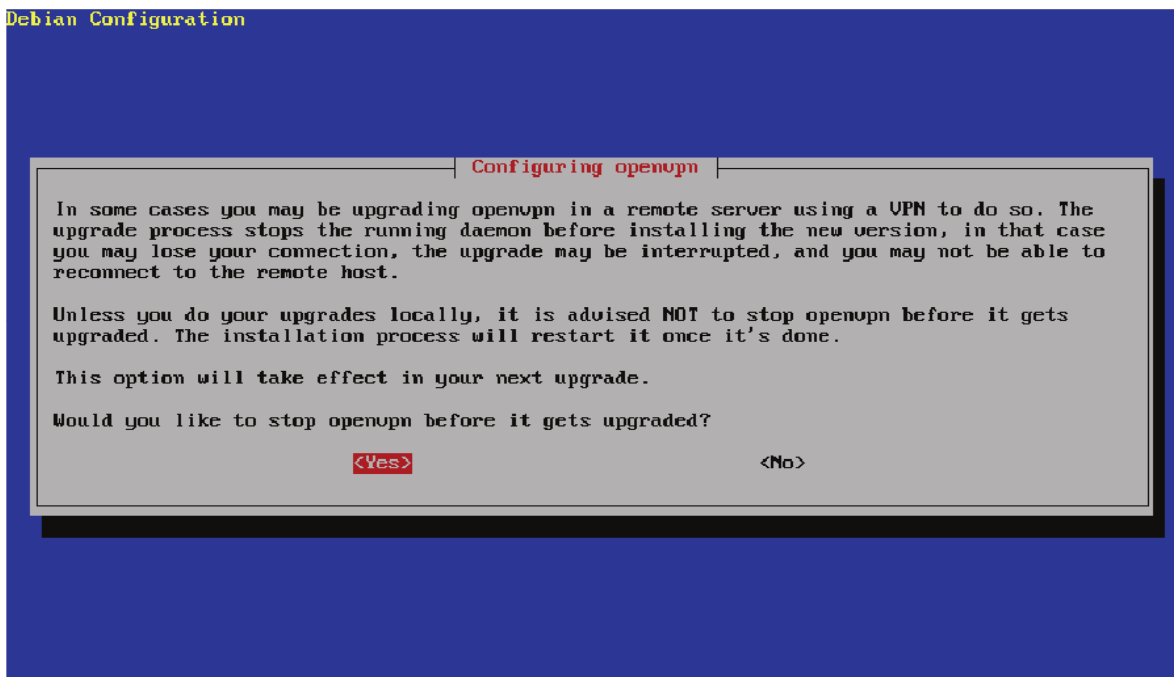
Το OpenVPN χρησιμοποιεί τους TAP και TUN εικονικούς οδηγούς για την δημιουργία των tunnel. Σε εκδόσεις του kernel άνω των 2.4 οι εικονικοί οδηγοί υπάρχουν ενσωματωμένοι στον πυρήνα του λειτουργικού, διαφορετικά πρέπει να εγκατασταθούν ξεχωριστά.

Κατά τη διαδικασία εγκατάστασης ζητείται να απαντηθούν τα ακόλουθα δύο ερωτήματα :

- Η επιλογή “Yes” στο aptitude δημιουργεί μια TUN / TAP συσκευή για χρήση από το OpenVPN. Η επιλογή “No” δεν επιτρέπει στο VPN να λειτουργήσει.



- Το δεύτερο ερώτημα θέτει ένα ζήτημα ασφαλείας, εάν, δηλαδή το OpenVPN πρέπει να διακοπεί κατά τη διάρκεια μιας ενημέρωσης. Η επιλογή "Yes" εξασφαλίζει την διακοπή του.



Η επιλογή αυτή διασφαλίζει ότι η υπηρεσία του OpenVPN θα σταματάει σε περίπτωση αναβάθμισης. Είναι ασφαλέστερο να υπάρχει ένα μικρό χρονικό διάστημα, κατά την διάρκεια του οποίου οι χρήστες δεν θα είναι σε θέση να συνδεθούν στο OpenVPN. Με τον τρόπο αυτό αποκλείεται η περίπτωση να παραμείνουν στο σύστημα παλαιότερες εκδόσεις λογισμικού και βιβλιοθήκες προκαλώντας ασυμβατότητες, πράγμα που μπορεί να συνέβαινε εάν υπήρχαν ενεργές συνδέσεις.

5.2 Ρύθμιση OpenVPN Server

Η ρύθμιση του OpenVPN όπως και οι περισσότερες Unix εφαρμογές έγινε χρησιμοποιώντας ένα αρχείο config. Το ότι το αρχείο config είναι σχεδόν ίδιο σε όλες τις πλατφόρμες, αποτελεί πλεονέκτημα που το καθιστά εύκολα προσαρμόσιμο σε όλα τα λειτουργικά συστήματα.

Στη συνέχεια εγκαταστάθηκε η εφαρμογή διαχείρισης Webmin και το OpenVPN-admin άρθρωμά του, ώστε να γίνει μέσω αυτού η βασική ρύθμιση του OpenVP. Αυτό γιατί το OpenVPN-admin δημιουργεί μια συγκεκριμένη δομή καταλόγων που χρειάζεται ώστε να διαχειρίζεται τα διάφορα config αρχεία (ιδιωτικά και δημόσια κλειδιά, αρχεία καταγραφής, κ.α) του OpenVPN server.

Μεταφορτώθηκε χειροκίνητα η τελευταία stable έκδοση “version 1.500” για Debian του webmin από την παρακάτω διεύθυνση <http://www.webmin.com>, διότι το webmin δεν διατίθεται πλέον στην επίσημη “stable” λίστα πακέτων του Debian έτσι ώστε να εγκατασταθεί μέσω του aptitude.

Μετά τη μεταφόρτωση εγκαταστάθηκε το webmin με την παρακάτω εντολή:

```
openvpn:~# dpkg -i webmin_1.500_all.deb
```

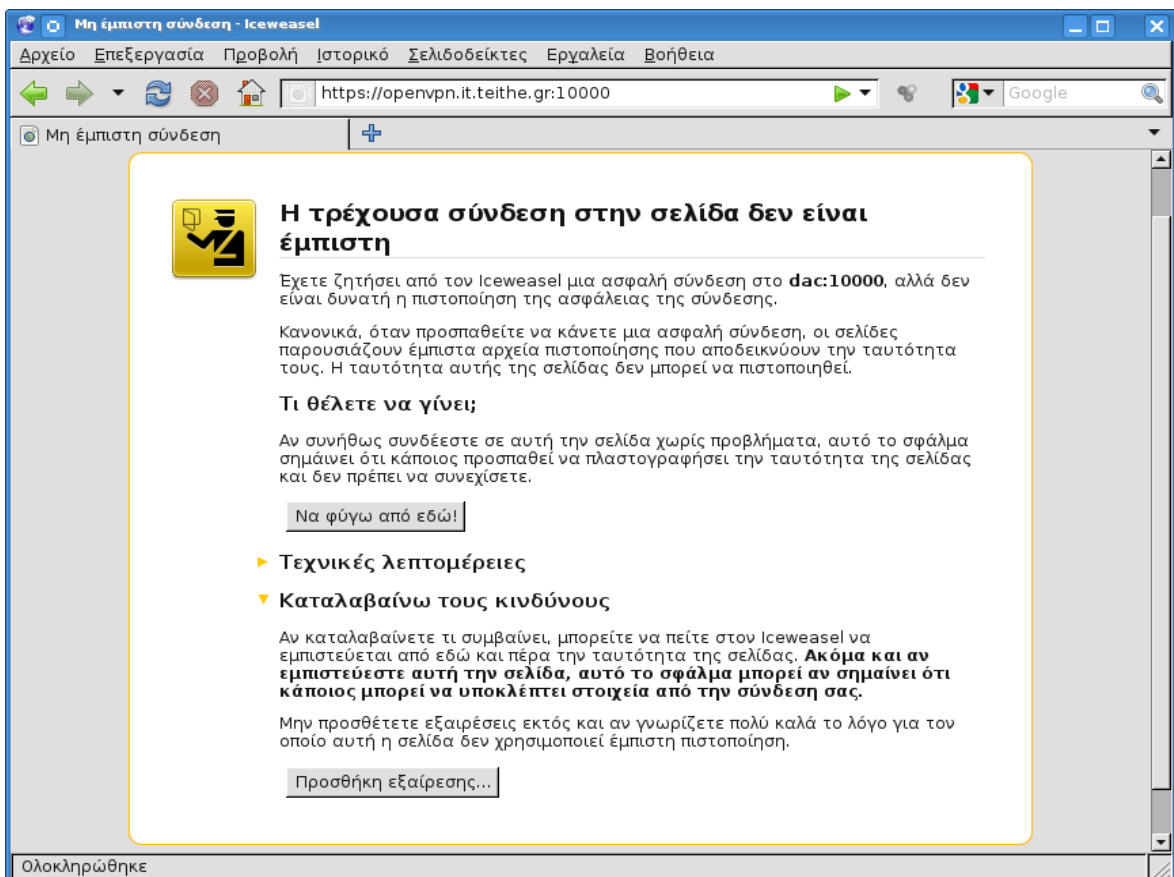
Με την οποία έγινε εγκατάσταση του Webmin στον κατάλογο: “/usr/

share/webmin” και των αρχείων ρυθμίσεών του, στον κατάλογο: “/etc/webmin”. Το αρχείο miniserv.conf περιέχει τις βασικές παραμέτρους για την πρόσβαση και τον έλεγχο ταυτότητας.

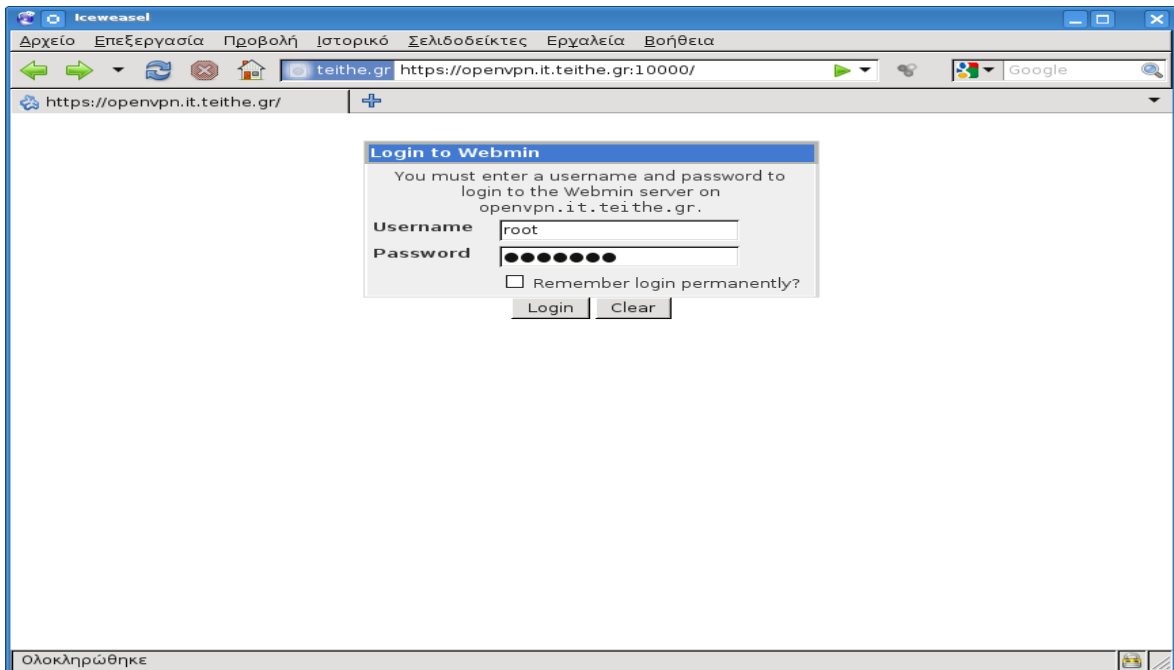
Ακολουθεί σύνδεση στην σελίδα διαχείρισης του webmin:

<https://openvpn.it.teithe.gr:10000>

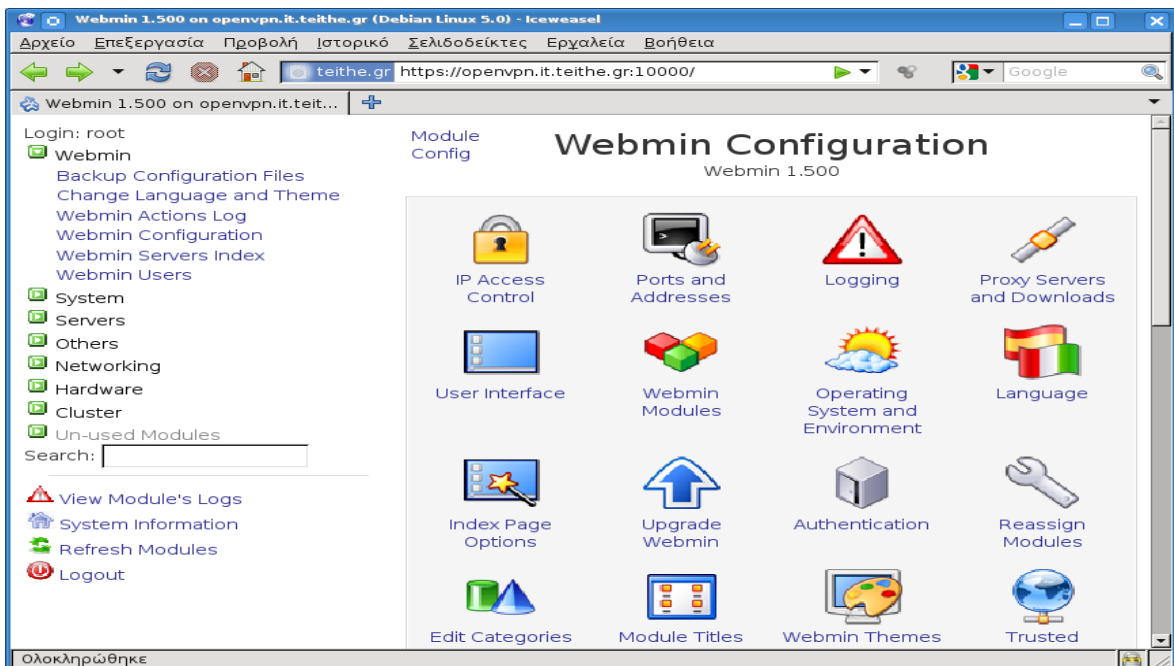
Από την σελίδα αυτή, γίνεται αποδοχή του πιστοποιητικού και προσθήκη εξαίρεσης για τη συγκεκριμένη διεύθυνση.



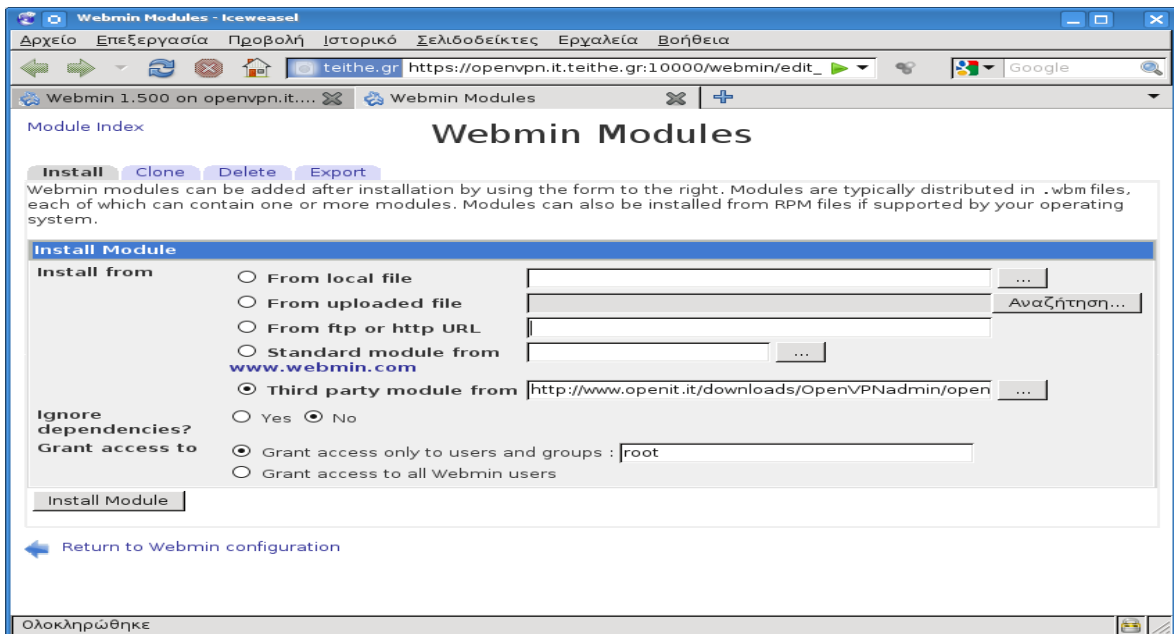
Στη συνέχεια ο χρήστης κάνει login στο σύστημα του webmin με το λογαριασμό του διαχειριστή “root” του συστήματος.



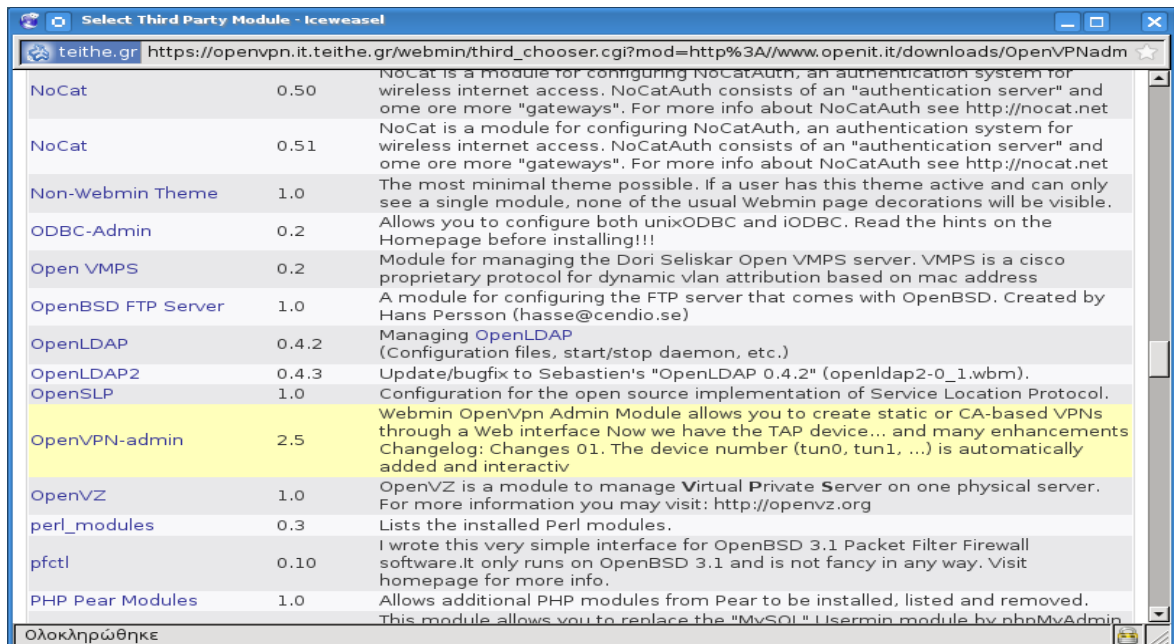
Μέσω του μενού Webmin > Webmin Configuration επιλέγεται το Webmin Modules :



Από τη σελίδα αυτή επιλέγεται το “Third party module from”.



Από τη λίστα που εμφανίζεται, επιλέγεται το OpenVPN-admin.



Επιλέγοντας το Module Config ο χρήστης βρίσκεται στην καρτέλα ρύθμισης του OpenVPN+CA “module” απ’ όπου ρυθμίζονται παράμετροι όπως οι διαδρομές στο σύστημα των διάφορων εκτελέσιμων, αρχεία ρυθμίσεων, αριθμοί εκδόσεων και πολλά άλλα που χρησιμοποιεί το OpenVPN+CA module για να λειτουργήσει.

Σε αυτό το σημείο, είναι επίσης σημαντικό ο χρήστης να ορίσει στην επιλογή **Server Hint for Clients** το hostname του server μας “openvpn.it.teithe.gr”.

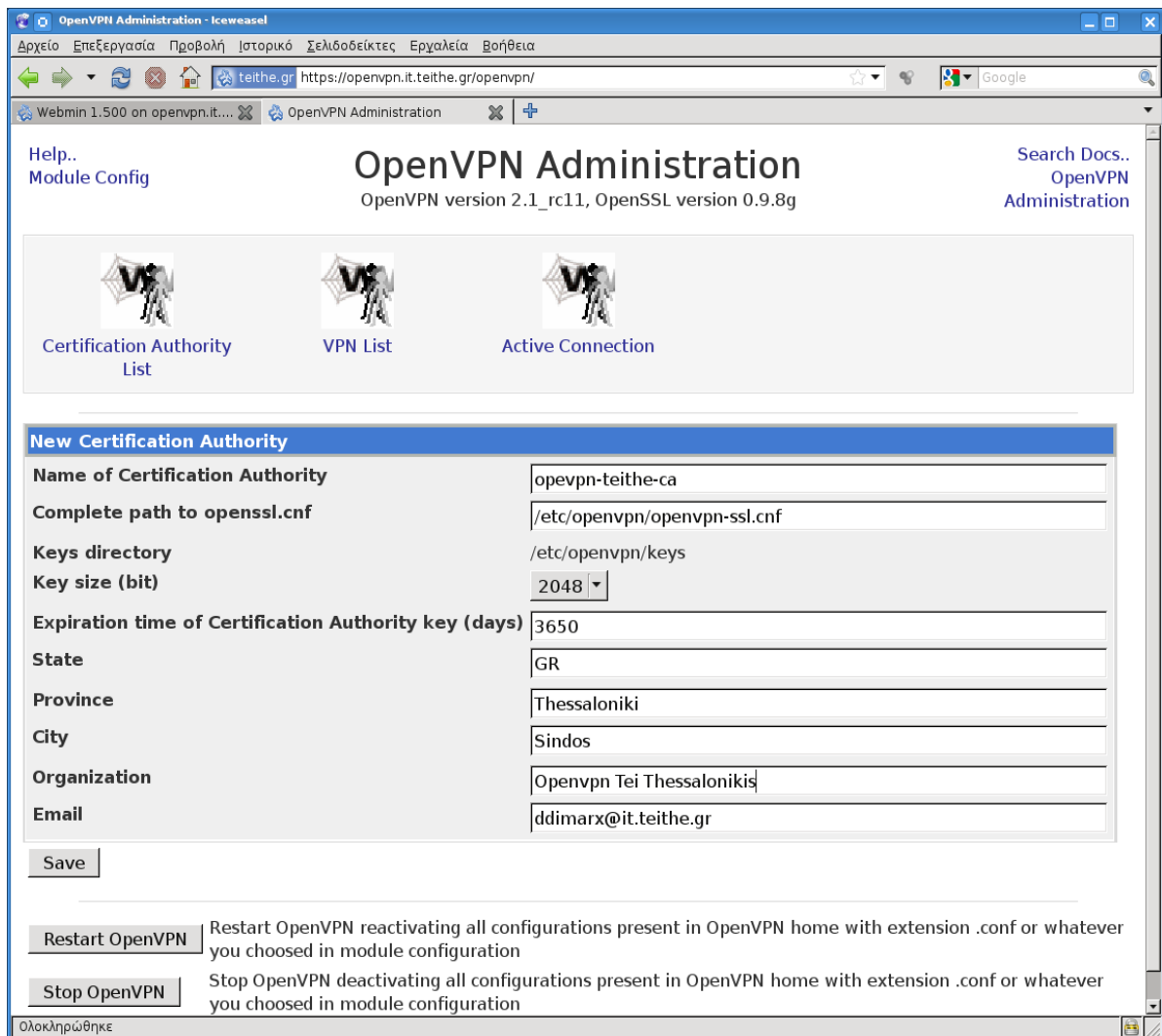
Παρακάτω φαίνονται τα πεδία και οι επιλογές που ορίστηκαν ώστε να συμβαδίζουν με τα στοιχεία του συστήματος στο οποίο εγκαθίσταται το OpenVPN+CA module:

The screenshot shows the 'Configuration' page for the OpenVPN + CA module. The browser window title is 'Configuration - Iceweasel'. The address bar shows 'https://openvpn.it.teithe.gr/config.cgi?openvpn'. The page content is as follows:

Configurable options for OpenVPN + CA	
System options	
OpenVPN Home (*)	/etc/openvpn
Server Hint for Clients (*)	openvpn.it.teithe.gr
Clients Subdir (relative to OpenVPN Home) (*)	clients
Servers Subdir (relative to OpenVPN Home) (*)	servers
Full path to openvpn (*)	/usr/sbin/openvpn
Keys Subdir (*)	keys
PID file path of running OpenVPN processes (*)	/var/run
OpenVPN version	2.1_rc11
OpenSSL cnf batch file (*)	/etc/openvpn/openvpn-ssl.cnf
Full path to ssl (*)	/usr/bin/openssl
SSL version	0.9.8g
Command to start OpenVPN (*)	/etc/init.d/openvpn start
Command to stop OpenVPN (*)	/etc/init.d/openvpn stop
Zip Command	/usr/bin/zip
Number of lines of log file to display	200
Seconds between log view refreshes	<input checked="" type="radio"/> Never <input type="radio"/> []
Tail command and arguments (LINES parameter required)	<input checked="" type="radio"/> Default (tail -n LINES) <input type="radio"/> []
If you use bridge device	
Command to start Bridge	/usr/share/webmin/openvpn/br_scripts/bridge_start
Command to stop Bridge	/usr/share/webmin/openvpn/br_scripts/bridge_end
Path to DOWN-ROOT-PLUGIN	/usr/lib/openvpn/openvpn-down-root.so
(*) Required fields	

At the bottom of the form, there is a 'Save' button and a 'Return to index' link. The status bar at the bottom of the browser window shows 'Ολοκληρώθηκε'.

Εφόσον αποθηκευτούν οι όποιες αλλαγές έχουν γίνει ο χρήστης επιστρέφει στην αρχική σελίδα του OpenVPN+CA module απ' όπου θα κατασκευάσει μια νέα αρχή πιστοποίησης “CA - Certification Authority”. Αργότερα, μέσω αυτής θα εκδώσει και θα διαχειριστεί τα δημόσια και ιδιωτικά κλειδιά του OpenVPN server και των clients που θα συνδέονται σε αυτόν.

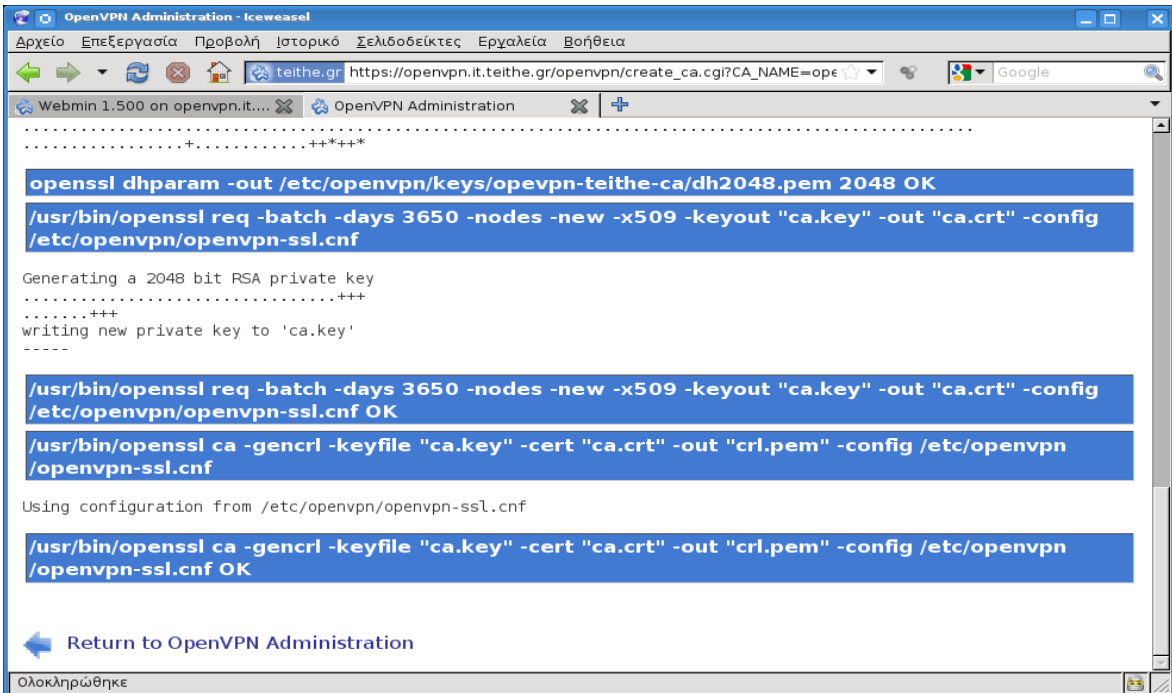
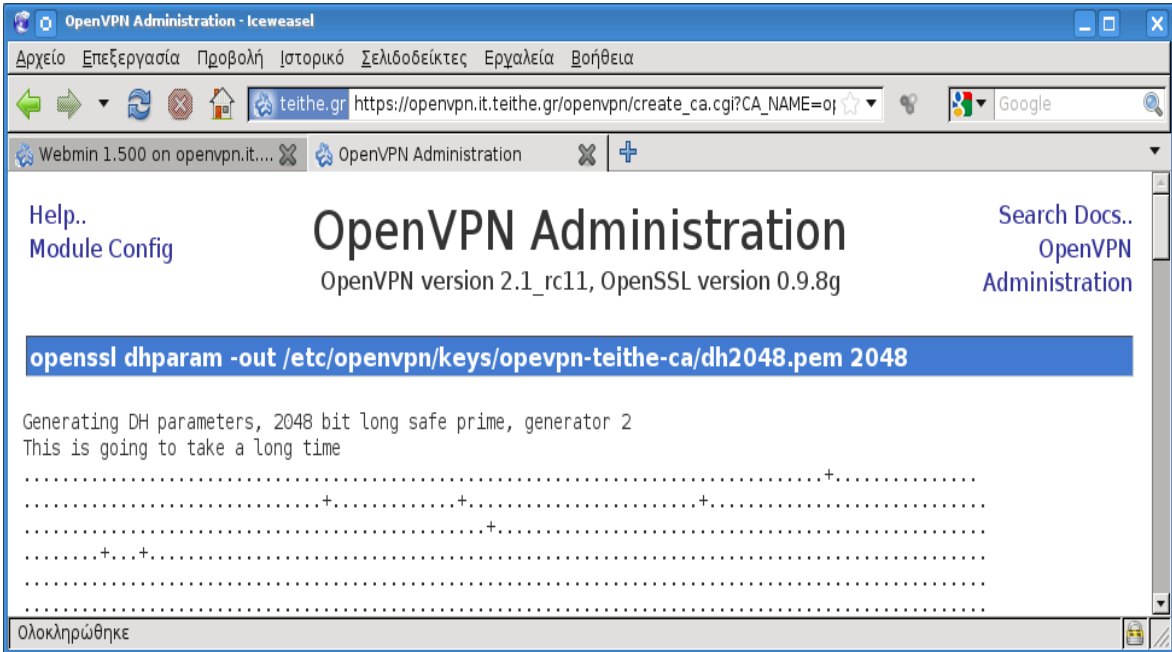


The screenshot shows the OpenVPN Administration web interface in a browser window. The page title is "OpenVPN Administration" and it displays the version information: "OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g". There are three main navigation buttons: "Certification Authority List", "VPN List", and "Active Connection". The "New Certification Authority" form is the primary focus, containing the following fields:

Name of Certification Authority	opevpn-teithe-ca
Complete path to openssl.cnf	/etc/openvpn/openvpn-ssl.cnf
Keys directory	/etc/openvpn/keys
Key size (bit)	2048
Expiration time of Certification Authority key (days)	3650
State	GR
Province	Thessaloniki
City	Sindos
Organization	Openvpn Tei Thessalonikis
Email	ddimarx@it.teithe.gr

Below the form, there are three buttons: "Save", "Restart OpenVPN", and "Stop OpenVPN". The "Restart OpenVPN" button has a tooltip that reads: "Restart OpenVPN reactivating all configurations present in OpenVPN home with extension .conf or whatever you choosed in module configuration". The "Stop OpenVPN" button has a tooltip that reads: "Stop OpenVPN deactivating all configurations present in OpenVPN home with extension .conf or whatever you choosed in module configuration". The status bar at the bottom of the browser window indicates "Ολοκληρώθηκε".

Μόλις αποθηκευτούν οι αλλαγές που έγιναν στην καρτέλα, το σύστημα αυτόματα, θα δημιουργήσει και θα αποθηκεύσει τα απαραίτητα κλειδιά για την υλοποίηση της αρχής πιστοποίησης με τις παρακάτω εντολές:



Στη συνέχεια από την κεντρική σελίδα του OpenVPN+CA module επιλέγεται το **Certification Authority List** και έπειτα το **Keys list** του **openvpn-teithe-ca**

Help..
Module Config

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

Certification Authority List				
Name	Notes	Info	Keys list	Remove
opevpn-teithe-ca		CA Info	Keys list	Remove

Στη σελίδα που ανοίγει, ορίζεται πρώτα στην επιλογή **Key name** το επιθυμητό όνομα του κλειδιού του OpenVPN server “opevpn-teithe-server”, θέτοντας και το **Key Server** σε **server**

Help..
Module Config

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

Keys list of Certification Authority opevpn-teithe-ca
No keys configured

New key to Certification Authority: opevpn-teithe-ca	
Key name	opevpn-teithe-server
Key password (min 4 chars)	
Key Server	server
Generate exportable PKCS#12 key	no
Password for exporting PKCS#12 (min 4 chars)	
Key expiration time (days)	3650
State	GR
Province	Thessaloniki
City	Sindos
Organization	Openvpn Tei Thessalonikis
Organization Unit	Office
Email	ddimarx@it.teithe.gr
<input type="button" value="Save"/>	

[Return to OpenVPN Administration](#)

Πατώντας το πλήκτρο για να αποθηκευθούν τα στοιχεία, το σύστημα θα δημιουργήσει αυτόματα και θα αποθηκεύσει όπως και προηγουμένως τα κλειδιά του server.

Help..
Module Config

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

```
openssl req -days 3650 -batch -new -keyout /etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.key
-out /etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.csr -nodes -extensions server -config
/etc/openvpn/openvpn-ssl.cnf
```

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.key'
-----
```

```
openssl req -days 3650 -batch -new -keyout /etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.key
-out /etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.csr -nodes -extensions server -config
/etc/openvpn/openvpn-ssl.cnf OK
```

```
openssl ca -days 3650 -batch -out /etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.crt -in
/etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.csr -extensions server -config /etc/openvpn
/openvpn-ssl.cnf
```

```
Using configuration from /etc/openvpn/openvpn-ssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'GR'
stateOrProvinceName :PRINTABLE:'Thessaloniki'
localityName      :PRINTABLE:'Sindos'
organizationName  :PRINTABLE:'Openvpn Tei Thessalonikis'
organizationalUnitName:PRINTABLE:'Office'
commonName        :PRINTABLE:'openvpn-teithe-server'
emailAddress      :IASSTRING:'ddimarx@it.teithe.gr'
Certificate is to be certified until Mar  7 18:39:17 2020 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

```
openssl ca -days 3650 -batch -out /etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.crt -in
/etc/openvpn/keys/opevpn-teithe-ca/openvpn-teithe-server.csr -extensions server -config /etc/openvpn
/openvpn-ssl.cnf OK
```

[Return to Keys list of Certification Authority opevpn-teithe-ca](#)

Αντίστοιχα η διαδικασία επαναλαμβάνεται για να δημιουργηθούν τα κλειδιά για τον client, με μόνη διαφορά ότι το **Key name** που θα επιλέξει ο χρήστης, είναι το “openvpn-teithe-client” και ότι στο Key Server θα είναι επιλεγμένο το **client**.

Σαφώς, και εφόσον αυτό είναι επιθυμητό, άλλες παράμετροι των κλειδιών αυτών όπως το **Key expiration time**, μπορούν να τροποποιηθούν, όπως επίσης μπορεί να τεθεί κάποιος κωδικός ασφαλείας χρήσης των κλειδιών αυτών στο **Key password**.

Virtual Private Network – OpenVPN – Δημαρχόπουλος Δημήτριος

Help..
Module Config

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

Keys list of Certification Authority opevpn-teithe-ca					
Name	Key Server	Verify	Export	Complete path of status log file	
opevpn-teithe-server	server	Verify	Export	active	Remove

New key to Certification Authority: opevpn-teithe-ca

Key name	opevpn-teithe-client
Key password (min 4 chars)	
Key Server	client
Generate exportable PKCS#12 key	no
Password for exporting PKCS#12 (min 4 chars)	
Key expiration time (days)	3650
State	GR
Province	Thessaloniki
City	Sindos
Organization	Openvpn Tei Thessalonikis
Organization Unit	Office
Email	ddimarx@it.teithe.gr

Save

[Return to OpenVPN Administration](#)

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Administration

```
openssl req -days 3650 -batch -new -keyout /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.key -out /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.csr -nodes -config /etc/openvpn/openvpn-ssl.cnf
```

```
Generating a 2048 bit RSA private key
..+++
.....+++
writing new private key to '/etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.key'
-----
```

```
openssl req -days 3650 -batch -new -keyout /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.key -out /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.csr -nodes -config /etc/openvpn/openvpn-ssl.cnf OK
```

```
openssl ca -days 3650 -batch -out /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.crt -in /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.csr -config /etc/openvpn/openvpn-ssl.cnf
```

```
Using configuration from /etc/openvpn/openvpn-ssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'GR'
stateOrProvinceName :PRINTABLE:'Thessaloniki'
localityName      :PRINTABLE:'Sindos'
organizationName  :PRINTABLE:'Openvpn Tei Thessalonikis'
organizationalUnitName:PRINTABLE:'Office'
commonName        :PRINTABLE:'opevpn-teithe-client'
emailAddress      :IA5STRING:'ddimarx@it.teithe.gr'
Certificate is to be certified until Mar  7 18:40:53 2020 GMT (3650 days)
```

```
Write out database with 1 new entries
Data Base Updated
```

```
openssl ca -days 3650 -batch -out /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.crt -in /etc/openvpn/keys/opevpn-teithe-ca/opevpn-teithe-client.csr -config /etc/openvpn/openvpn-ssl.cnf OK
```

[Return to Keys list of Certification Authority opevpn-teithe-ca](#)

Μόλις ολοκληρωθεί και η δημιουργία των κλειδιών του client μπορούν πλέον να δημιουργηθούν τα αρχεία ρυθμίσεων του OpenVPN server σε πρώτη φάση και έπειτα του client.

Help..
Module Config

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

Keys list of Certification Authority opevpn-teithe-ca					
Name	Key Server	Verify	Export	Complete path of status log file	
openvpn-teithe-server	server	Verify	Export	active	Remove
openvpn-teithe-client	client	Verify	Export	active	Remove

Για τη δημιουργία του OpenVPN server θα χρησιμοποιηθεί κατά αρχήν το webmin OpenVPN+CA άρθρωμα έτσι ώστε να δημιουργηθεί η κατάλληλη δομή φακέλων και αρχείων που χρειάζεται για την περαιτέρω διαχείριση του OpenVPN. Θα χρειαστεί και χειροκίνητη εισαγωγή κάποιων πιο εξειδικευμένων στοιχείων στο αρχείο ρυθμίσεων οι οποίες δεν μπορούν να γίνουν μέσω του webmin.

Από την αρχική σελίδα του OpenVPN+CA επιλέγεται το **VPN List** και έπειτα το **New VPN server** έχοντας υπόψη ότι στο **ca (Certification Authority)** είναι επιλεγμένη η αρχή πιστοποίησης “openvpn-teithe-ca” που είχε δημιουργηθεί προηγουμένως.

Help..
Module Config

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

VPN server list:

VPN List is empty

ca (Certification Authority): Creation of new VPN Server: select the Certification Authority and click New VPN server

VPN server list with simmetric key

VPN List is empty

Creation of new VPN Server with symmetrical key

[← Return to OpenVPN Administration](#)

Η επόμενη σελίδα περιέχει μια πληθώρα επιλογών και ρυθμίσεων σχετικά με τον τρόπο λειτουργίας που δύναται να έχει ο OpenVPN server. Οι βασικότερες επιλογές που πρέπει να γίνουν από εδώ είναι :

Name : Ορίζεται σαν “openvpn-teithe”

port (Port) : Αλλάζει σε “443” η port που θα περιμένει τις εισερχόμενες VPN συνδέσεις ο OpenVPN server. Αυτό γίνεται για μεγαλύτερη συμβατότητα με τα περισσότερα firewall που επιτρέπουν την “TCP” κίνηση δεδομένων σε αυτή διότι έτσι είναι η ορισμένη από την IANA το port για ασφαλείς “https” συνδέσεις.

proto (Protocol) : Για τον λόγο της συμβατότητας με τα firewall που αναφέρθηκε προηγουμένως επιλέγεται “tcp-server” ορίζοντας έτσι το “TCP” ως πρωτόκολλο επικοινωνίας για το OpenVPN παρόλο που η χρήση του “TCP” επιφέρει μείωση στην ταχύτητα μετάδοσης δεδομένων μέσω του VPN λόγω του overhead που έχουν από τη φύση τους οι TCP συνδέσεις. Θα μπορούσε να χρησιμοποιηθεί το “UDP” ως πρωτόκολλο επικοινωνίας κρατώντας την προεπιλεγμένη port “1194” του OpenVPN ή ορίζοντας την σε port “53” που είναι ορισμένο από την IANA για την υπηρεσία “DNS”.

management (Enable Management) : Η επιλογή αυτή ενεργοποιεί την υπηρεσία διαχείρισης του OpenVPN server σε κάποια συγκεκριμένη port του συστήματος που ορίζει ο χρήστης. Η διαχείριση μπορεί να γίνει μέσω telnet, μέσω του webmin OpenVPN+CA καθώς και άλλων γραφικών εργαλείων διαχείρισης της υπηρεσίας όπως το OpenVPN-Admin. Για το λόγο αυτό επιλέγεται :

Enable: Yes **IP:** 127.0.0.1 **Port:** 5702

enable TLS and assume server role during TLS handshake : Επιλέγοντας “Yes” ενεργοποιείται η επιλογή “tls-server” υποχρεώνοντας τον OpenVPN server να χρησιμοποιεί τα πιστοποιητικά του “SSL” και να λειτουργεί ως “TLS server” κατά την διαδικασία του “TLS handshake”

Local host name or IP address : Στο πεδίο αυτό ορίζεται σε ποια ή ποιες IP διευθύνσεις του server (εφόσον διαθέτει περισσότερες από μια συνδέσεις δικτύου) είναι επιθυμητό το OpenVPN να “περιμένει” για εισερχόμενες συνδέσεις.

Net IP assigns (option server) : Εδώ ορίζεται ο αριθμός του δικτύου - υποδικτύου που θα ανήκει το VPN (server και clients) : Ποιο συγκεκριμένα για το δίκτυο του τμήματος πληροφορικής ορίζεται το παρακάτω.

network : 192.168.15.64 **netmask** : 255.255.255.192

New VPN server	
Name	openvpn-teithe
port (Port)	443
proto (Protocol)	tcp-server
Device	tun
Bridge Device	
Network Device for Bridge	bond0
IP config for bridge	IP-Address/Gateway : <input type="text"/> Netmask : <input type="text"/>
IP-Range for Bridge-Clients	Start: <input type="text"/> End: <input type="text"/>
management (Enable Management)	Enable: <input checked="" type="checkbox"/> IP: 127.0.0.1 Port: <input type="text"/>
ca (Certification Authority)	openvpn-teithe-ca
Choose key	openvpn-teithe-server
Certificate Server	automatic
Key Server	automatic
Diffie-Hellman random file	dh2048.pem
enable TLS and assume server role during TLS handshake	<input checked="" type="checkbox"/>
Local host name or IP address	195.251.123.180
Net IP assigns (option server)	network <input type="text"/> netmask <input type="text"/>

Persist/unpersist ifconfig-pool data to file, at seconds intervals (default=600), as well as on program startup and shutdown (option ifconfig-pool-persist) : Θέτοντας “Yes” στην επιλογή αυτή, ρυθμίζεται ο OpenVPN server να κρατάει ένα αρχείο καταγραφής των IP διευθύνσεων που παραχωρεί δυναμικά στους clients, έτσι ώστε κάθε φορά που κάποιος client συνδέεται στο VPN να του εκχωρείται εάν είναι διαθέσιμη η ίδια IP διεύθυνση που του είχε ανατεθεί παλαιότερα.

Because the OpenVPN server mode handles multiple clients through a single tun or tap interface, it is effectively a router (option client-to-client) :

Για να επιτρέπεται η επικοινωνία μεταξύ των clients που συνδέονται στον OpenVPN server ορίζεται “Yes” σε αυτή την επιλογή.

Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks (option tls-auth) : Ενεργοποιώντας την επιλογή αυτή, “Yes”, παρέχεται μια βασική Denial of Service (DOS) προστασία. Το DOS είναι το είδος της επίθεσης, όπου κάποιος προσπαθεί να κατακλύσει το server με ψευδείς αιτήσεις σύνδεσης και ως εκ τούτου καθυστερεί τις πραγματικές συνδέσεις. Ενεργοποιώντας την επιλογή tls-auth ο OpenVPN server θα δέχεται μόνο κρυπτογραφημένα πακέτα με τη σωστή υπογραφή HMAC που παράγεται από το κλειδί που καθορίζεται στο αρχείο (π.χ. ta.key). Αυτή η επιλογή θα πρέπει πάντοτε να ενεργοποιείται όταν ο OpenVPN server δέχεται συνδέσεις από μη σταθερές - διαφορετικές IP διευθύνσεις.

Encrypt packets with cipher algorithm (option cipher) : Εδώ μπορεί να ορισθεί ο αλγόριθμος που θα χρησιμοποιείτε για την κρυπτογράφηση των πακέτων κατά την μεταφορά τους μέσα από το VPN. Ο προ επιλεγμένος αλγόριθμος που χρησιμοποιεί το OpenVPN είναι ο “BF-CBC 128 bit default key (variable)”. Βέβαια θα μπορούσαν να χρησιμοποιηθούν και πιο ισχυροί αλγόριθμοι, εάν αυτό είναι

επιθυμητό.

Float (Allow remote peer to change its IP address and/or port number) :

Η τελευταία αλλαγή που γίνεται με το να τεθεί “Yes” σε αυτή την επιλογή, επιτρέπει στους client να μπορούν να συνδεθούν στον server έχοντας διαφορετικές IP διευθύνσεις και χρησιμοποιώντας διαφορετικό port κάθε φορά.

Persist/unpersist ifconfig-pool data to file, at seconds intervals (default=600), as well as on program startup and shutdown (option ifconfig-pool-persist)	yes
Because the OpenVPN server mode handles multiple clients through a single tun or tap interface, it is effectively a router (option client-to-client)	yes
Allow multiple clients with the same common name to concurrently connect (option duplicate-cn)	no
Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks (option tls-auth)	yes
ccd-exclusive (Clients enabled only for this server)	yes
Encrypt packets with cipher algorithm (option cipher)	BF-CBC 128 bit default key (variable)
Use fast LZO compression (option comp-lzo)	yes
Limit server to a maximum of n concurrent clients (option max-clients)	100
User	nobody
Group	nogroup
Don't re-read key files (option persist-key)	yes
Don't close and reopen TUN/TAP device or run up/down scripts (option persist-tun)	yes
keepalive (A helper directive designed to simplify the expression of **ping** and **ping-restart** in server mode configurations)	Ping: 10 Ping-Restart: 120
Set output verbosity	2
Log at most n consecutive messages in the same category	20
Complete path of status log file	openvpn-status.log
Complete path of log file	openvpn.log
tun-mtu (Take the TUN device MTU to be n and derive the link MTU from it)	
fragment (Enable internal datagram fragmentation so that no UDP datagrams are sent which are larger than max bytes)	
mssfix (Announce to TCP sessions running over the tunnel that they should limit their send packet sizes such that after OpenVPN has encapsulated them, the resulting UDP packet size that OpenVPN sends to its peer will not exceed max bytes)	
float (Allow remote peer to change its IP address and/or port number)	yes

Έχοντας ολοκληρώσει με τις παραπάνω ρυθμίσεις, επιλέγεται το πλήκτρο “Save” για να αποθηκευθούν οι αλλαγές και να δημιουργηθούν αυτόματα στο σύστημα όλα τα απαραίτητα αρχεία του OpenVPN server. Τα υπόλοιπα πεδία που παραμένουν ως έχουν, περιγράφονται στην συνέχεια.

Αμέσως μετά, πρέπει να γίνουν κάποιες αλλαγές χειροκίνητα στο αρχείο ρυθμίσεων του OpenVPN server έτσι ώστε να συμπληρωθούν κάποια στοιχεία που δεν μπορεί να τα διαχειριστεί ο χρήστης μέσω webmin OpenVPN+CA όπως η μέθοδος αυθεντικοποίησης των client που θα συνδέονται στο OpenVPN server μέσω τον λογαριασμών που διαθέτουν στον κεντρικό server “aetos.it.teithe.gr” του τμήματος πληροφορικής.

Μπαίνοντας ως διαχειριστής “root” από ένα τερματικό και ανοίγοντας το βασικό αρχείο ρυθμίσεων του OpenVPN server με κάποιον επεξεργαστή κειμένου (πχ vim) γίνονται οι απαραίτητες αλλαγές έτσι ώστε το αρχείο να έχει την παρακάτω μορφή.

“/etc/openvpn/openvpn-teithe.conf”

```
port 443
proto tcp-server
dev tap0
ca keys/openvpn-teithe-ca/ca.crt
cert keys/openvpn-teithe-ca/openvpn-teithe-server.crt
key keys/openvpn-teithe-ca/openvpn-teithe-server.key
dh keys/openvpn-teithe-ca/dh2048.pem
server 192.168.15.64 255.255.255.192
crl-verify keys/openvpn-teithe-ca/crl.pem
ifconfig-pool-persist servers/openvpn-teithe/logs/ipp.txt
tls-auth servers/openvpn-teithe/ta.key 0
cipher BF-CBC
user nobody
group nogroup
status servers/openvpn-teithe/logs/openvpn-status.log
log-append servers/openvpn-teithe/logs/openvpn.log
```

```
verb 2
mute 20
max-clients 100
local 195.251.123.180
management 127.0.0.1 5207
keepalive 10 120
client-config-dir /etc/openvpn/servers/openvpn-teithe/ccd
tls-server
client-to-client
comp-lzo
persist-key
persist-tun
float
# Επιπλέον παράμετροι #####
ifconfig-noexec
port-share 195.251.123.180 10000
push "redirect-gateway def1"
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"
client-cert-not-required
username-as-common-name
auth-user-pass-verify servers/openvpn-teithe/bin/auth_aetos_user.sh "via-file"
script-security 2
up servers/openvpn-teithe/bin/create_vpn_tmp_dir.sh
tmp-dir /tmp/.openvpn/
```

Μια αλλαγή που πραγματοποιήθηκε είναι το “**dev tun0**” σε “**dev tap0**” γιατί προέκυψε κάποιο πρόβλημα λειτουργίας του εικονικού “TUN” δικτυακού οδηγού που χρησιμοποιείται για routing μεταξύ δικτύων “level 3” στο περιβάλλον του Linux

Virtual Server, ενώ το “TAP” που χρησιμοποιείται κυρίως για bridging “level 2” λειτουργεί χωρίς προβλήματα.

Αφαιρέθηκε επίσης η παράμετρος “**ccd-exclusive**” η οποία επιτρέπει συνδέσεις στον server μόνο για τους clients που έχουν ξεχωριστό αρχείο ρυθμίσεως (βάση του “login” ονόματος τους) στον κατάλογο ρυθμίσεων των client. Αυτό γιατί η συγκεκριμένη εγκατάσταση έχει σαν σκοπό να δημιουργήσει για όλους τους clients ένα κοινό αρχείο ρυθμίσεων όπου θα διαφοροποιούνται, όταν συνδέονται στον OpenVPN server, με το εκάστοτε “login” όνομα που έχει ο κάθε χρήστης στον server “aetos”.

Παρακάτω περιγράφεται συνοπτικά τι ορίζουν οι υπόλοιποι παράμετροι του αρχείου ρυθμίσεων του OpenVPN server.

- **port 443** : Το port που χρησιμοποιεί ο OpenVPN server.
- **proto tcp-server** : Το πρωτόκολλο που χρησιμοποιεί ο OpenVPN server.
- **dev tap0** : Η εικονική συσκευή που χρησιμοποιεί ο OpenVPN server
- **ca keys/opevpn-teithe-ca/ca.crt** : Ορίζει τη διαδρομή που βρίσκεται το πιστοποιητικό της αρχής πιστοποίησης και πρέπει να είναι διαθέσιμο στον server και στους client
- **cert keys/opevpn-teithe-ca/openvpn-teithe-server.crt** : Ορίζει τη διαδρομή που βρίσκεται το υπογεγραμμένο πιστοποιητικό της αρχής πιστοποίησης του OpenVPN server το οποίο πρέπει βρίσκεται μόνο στο server.
- **key keys/opevpn-teithe-ca/openvpn-teithe-server.key** : Ορίζει τη διαδρομή που βρίσκεται το ιδιωτικό RSA κλειδί του OpenVPN server και

πρέπει να βρίσκεται μόνο στο server.

- **dh keys/opevpn-teithe-ca/dh2048.pem** : Ορίζει τη διαδρομή που βρίσκεται το Diffie-Hellman κλειδί που πρέπει να είναι διαθέσιμο και αυτό μόνο στο server.
- **server 192.168.15.64 255.255.255.192** : Ο αριθμός του δικτύου και υποδικτύου που ανήκει το VPN.
- **crl-verify keys/opevpn-teithe-ca/crl.pem** : Ορίζει τη διαδρομή που βρίσκεται το αρχείο με τη λίστα ανάκλησης πιστοποιητικών της αρχής πιστοποίησης και χρησιμεύει για να απαγορεύει την πρόσβαση σε clients που τους έχουν ανακληθεί τα πιστοποιητικά τους. Το αρχείο αυτό βρίσκεται μόνο στο server.
- **ifconfig-pool-persist servers/openvpn-teithe/logs/ipp.txt** : Ορίζει τη διαδρομή που βρίσκεται το αρχείο καταγραφής των IP διευθύνσεων που ο server παραχωρεί δυναμικά κάθε φορά στους clients.
- **tls-auth servers/openvpn-teithe/ta.key 0** : Ορίζει τη διαδρομή που βρίσκεται το κλειδί που χρησιμεύει στην προστασία έναντι των (DOS) επιθέσεων. Πρέπει να είναι διαθέσιμο στον server με την τιμή “0” και στους client με τιμή “1”.
- **cipher BF-CBC** : Ο αλγόριθμος που θα χρησιμοποιείται για την κρυπτογράφηση των πακέτων στην επικοινωνία μεταξύ server / client.
- **user nobody και group nogroup** : Οι επιλογές αυτές αποτελούν ένα ακόμα σημαντικό μέτρο ασφάλειας που δίνει την δυνατότητα ν' αλλάξουν τα

δικαιώματα χρήστη της διεργασίας του OpenVNP. Επίσης, έχουν ως αποτέλεσμα η διεργασία OpenVPN να αρχικοποιηθεί κανονικά και στη συνέχεια να υποπέσει στην κατηγορία χρήστη nobody και ομάδας nogroup με περιορισμένα δικαιώματα, αρκετά ώστε να μπορέσει να εκτελέσει την διεργασία του OpenVPN, αλλά χωρίς να έχει πρόσβαση σε άλλους πόρους του λειτουργικού συστήματος. Έτσι ακόμα και αν κάποιος καταφέρει και βρει κάποιο κενό ασφαλείας στο OpenVPN και καταφέρει να αποκτήσει έλεγχο της διεργασίας δεν θα έχει δικαιώματα για να κάνει κάποια αλλαγή στο σύστημα.

- **status servers/openvpn-teithe/logs/openvpn-status.log** : Ορίζει ένα αρχείο καταγραφής των συνδέσεων του OpenVPN server.
- **log-append servers/openvpn-teithe/logs/openvpn.log** : Ορίζει ένα αρχείο συνεχούς καταγραφής των μηνυμάτων λειτουργίας του OpenVPN server.
- **verb 2** : Ορίζει το πόσο αναλυτικές θα είναι οι πληροφορίες καταγραφής από “0” το ελάχιστο έως “11” το μέγιστο.
- **mute 20** : Ορίζει τον αριθμό των μηνυμάτων που θα εμφανίζονται και ανήκουν στην ίδια κατηγορία μηνύματος .
- **max-clients 100** : Ορίζει τον μέγιστο αριθμό ταυτόχρονων client συνδέσεων που μπορεί να εξυπηρετήσει ο OpenVPN server, αν και ο μέγιστος αριθμός host στο συγκεκριμένο υποδίκτυο είναι “62”.
- **local 195.251.123.180** : Ορίζει σε πια IP διεύθυνσης ο server θα “περιμένει” για εισερχόμενες συνδέσεις.

- **management 127.0.0.1 5207** : Ορίζει την υπηρεσία διαχείρισης του OpenVPN server μέσω telnet και άλλων προγραμμάτων διαχείρισης σε συγκεκριμένη port.
- **keepalive 10 120** : Η επιλογή αυτή συνδυάζει τα χαρακτηριστικά των παραμέτρων “ring” και “ring-restart” και ορίζει τους χρόνους που θα αποστέλλει ο server πακέτα ελέγχου της σύνδεσης των VPN τούνελ, έτσι ώστε ν’ αντιλαμβάνεται πότε μια σύνδεση δεν είναι πλέον ενεργή. Η επιλογή αυτή πρέπει να υπάρχει και στον server και στους client.
- **client-config-dir /etc/openvpn/servers/openvpn-teithe/ccd** : Ορίζει τον κατάλογο που το OpenVPN ελέγχει για εξειδικευμένα αρχεία ρυθμίσεων client όταν πραγματοποιείται μια νέα σύνδεση.
- **tls-server** : Ορίζει τον OpenVPN server να χρησιμοποιεί τα πιστοποιητικά του “SSL” και να λειτουργεί ως “TLS server” κατά την διαδικασία του “TLS handshake”.
- **client-to-client** : Επιτρέπει την επικοινωνία μεταξύ των clients που συνδέονται στον OpenVPN server.
- **comp-lzo** : Ορίζει το OpenVPN να χρησιμοποιεί την “Lzo” βιβλιοθήκη για συμπίεση της κυκλοφορίας των τούνελ.
- **persist-key** : Αυτή η παράμετρος θα εμποδίσει την εκ νέου ανάγνωση των κλειδιών σε περίπτωση επανεκκίνησης κάποιου τούνελ. Αυτό είναι αναγκαίο όταν το OpenVNP τρέχει ως μη προνομιούχος χρήστης (nobody – nogroup) που δεν έχει πρόσβαση στα αρχεία των κλειδιών.

- **persist-tun** : Αυτή η παράμετρος θα κράτηση ενεργές “up” της εικονικές συσκευές (TUN/TAP) σε περίπτωση επανεκκίνησης κάποιου τούνελ.
- **float** : Με την επιλογή αυτή επιτρέπεται στους client να μπορούν να συνδεθούν στον server έχοντας διαφορετικές IP διευθύνσεις και χρησιμοποιώντας διαφορετικό port κάθε φορά.

Είναι επίσης απαραίτητη η προσθήκη κάποιων επιπλέον παραμέτρων, που επιτρέπουν στον OpenVPN server να λειτουργεί χωρίς προβλήματα στον Linux Virtual Server , μεταδίδουν πληροφορίες στους client κατά την σύνδεση τους και ορίζουν τον τρόπο αυθεντικοποίησής τους μέσω του λογαριασμού που έχουν στον server “aetos” του τμήματος πληροφορικής.

Οι παράμετροι που προστίθενται είναι οι εξής :

- **ifconfig-noexec** : Η παράμετρος αυτή είναι απαραίτητη για να λειτουργήσει το OpenVPN στο Linux Virtual Server περιβάλλον και κάνει τον VPN server να μην εκτελέσει πραγματικά τις εντολές ifconfig / netsh και απλά να περάσει τις παραμέτρους “--ifconfig” στα σενάρια (scripts) που χρησιμοποιούν μεταβλητές περιβάλλοντος (environmental variables).
- **port-share 195.251.123.180 10000** : Όταν ο OpenVPN server χρησιμοποιεί το TCP πρωτόκολλο, τότε με την παράμετρο αυτή γίνεται ρύθμιση ώστε ο server να μοιράζεται την ίδια port (συγκεκριμένα την 443) με κάποια άλλη εφαρμογή, όπως ένα HTTPS server (συγκεκριμένα το webmin) που χρησιμοποιεί άλλο port. Αν ο OpenVPN server δεχθεί μια σύνδεση η οποία χρησιμοποιεί ένα μη-OpenVPN πρωτόκολλο, θα μεταβιβάσει τη σύνδεση αυτή στο “ip” και την port του server που το ορίστηκαν.

- **push “redirect-gateway def1” και push “dhcp-option DNS 208.67.222.222”**: Με την παράμετρο “push” ο OpenVPN server έχει την δυνατότητα να αποστέλλει στους clients πληροφορίες ρυθμίσεως κυρίως χαρακτηριστικών δρομολόγησης και δικτύου (πχ. Default Gateway, DNS κ.α.). Συγκεκριμένα η επιλογή “redirect-gateway” θα κάνει τους clients, (όταν συνδέονται στο VPN), να αναπροσανατολίσουν την προεπιλεγμένη πύλη δικτύου τους “Default Gateway” μέσω της σύνδεσης VPN, προκαλώντας όλη την δικτυακή IP κίνηση, όπως η περιήγηση στο Web και οι αναζητήσεις DNS να περνούν μέσα από το VPN τούνελ. Προκειμένου να λειτουργήσει σωστά αυτό θα πρέπει να εφαρμοστεί στο server η τεχνική NAT / bridge της TUN / TAP διασύνδεσης αντίστοιχα με το Internet. Η επιλογή “def1” χρησιμεύει για να παρακάμπτει και να μην διαγράφει την αρχική “Default Gateway” από τους clients, χρησιμοποιώντας τις διευθύνσεις “0.0.0.0/1” και “128.0.0.0/1” και όχι τη “0.0.0.0/0” έτσι ώστε να επαναφέρεται το αρχικό “Default Gateway” μετά το τέλος της VPN σύνδεσης ακόμα και σε περιπτώσεις που δεν τερματιστεί κανονικά η εφαρμογή του OpenVPN. Με τη παράμετρο “dhcp-option” ο OpenVPN server μπορεί να αποστέλλει, κυρίως σε Windows clients, συγκεκριμένες DHCP παραμέτρους. Ειδικότερα με την επιλογή “DNS” στέλνει την IP διεύθυνση του DNS server που θα χρησιμοποιούν οι clients κατά τη διάρκεια της VPN σύνδεσης. Προτείνεται η χρήση του OpenDNS “208.67.222.222 και 208.67.220.220” για να μην δημιουργηθούν προβλήματα προσπέλασης στον DNS server από το εκάστοτε δίκτυο του ISP κάθε χρήστη.
- **client-cert-not-required** : Με αυτή την παράμετρο απενεργοποιείται η χρήση των πιστοποιητικών για την αυθεντικοποίηση των client η οποία θα γίνεται με χρήση username / password. Αυτό γίνεται διότι έχει δημιουργηθεί μόνο ένα πιστοποιητικό που θα χρησιμοποιούν όλοι οι clients κυρίως για τη

κρυπτογράφηση του καναλιού επικοινωνίας των τούνελ.

- **username-as-common-name** : Για να λειτουργήσει σωστά η αυθεντικοποίηση μόνον με username / password προστίθεται και αυτή η παράμετρος η οποία κάνει τον OpenVPN server να χρησιμοποιεί το εκάστοτε username που δηλώνουν οι clients ως δείκτη σε λειτουργίες επισήμανσης και διαφοροποίησης των συνδέσεων, όπως σε αρχεία καταγραφής και όχι το “common-name” που υπάρχει στο πιστοποιητικό των clients.
- **auth-user-pass-verify servers/openvpn-teithe/bin/auth_aetos_user.sh "via-file"** : Με την επιλογή αυτή ενεργοποιείται ο μηχανισμός αυθεντικοποίησης στον OpenVPN server, η διαδρομή καταλόγου και το όνομα του script “auth_aetos_user.sh” που θα κάνει την αυθεντικοποίηση, καθώς και η μέθοδος (via-env / via-file) που θα χρησιμοποιηθεί για τον χειρισμό των username / password. Συγκεκριμένα για μεγαλύτερη ασφάλεια χρησιμοποιείται η μέθοδος μέσω αρχείου “via-file”.
- **script-security 2** : Το OpenVPN με την επιλογή αυτή παρέχει πολιτικές ελέγχου για το επίπεδο ασφάλειας χρήσης των εξωτερικών προγραμμάτων και σεναρίων (scripts). Χαμηλότερες τιμές είναι πιο περιοριστικές ενώ οι υψηλότερες πιο ανεκτικές, η τιμή “2” επιτρέπει την χρήση ενσωματωμένων προγραμμάτων καθώς και ανεξάρτητων scripts που καθορίζονται από το διαχειριστή.
- **tmp-dir /tmp/.openvpn/** : Ορίζεται ο κατάλογος που θα χρησιμοποιεί ο OpenVPN server για τα προσωρινά αρχεία όπως αυτά για την αυθεντικοποίηση . Η μέθοδος που έχει οριστεί προηγουμένως “via-file”, θα γράψει το όνομα χρήστη και κωδικό πρόσβασης στις δύο πρώτες γραμμές

ενός προσωρινού αρχείου. Στη συνέχεια τ' όνομα του αρχείου θα περάσει ως μεταβλητή στο (script) αυθεντικοποίησης και τέλος το αρχείο θα διαγραφεί αυτόματα μετά την ολοκλήρωση της διαδικασίας. Για μεγαλύτερη ασφάλεια, προτείνεται η δημιουργία προσωρινού φακέλου σε εικονικά “volatile” μέσα αποθήκευσης, όπως το “/dev/shm” εαν υπάρχουν, έτσι ώστε ν' αποφευχθεί η εγγραφή του αρχείου που περιέχει τα username / password σε κάποιο μόνιμο μέσο αποθήκευσης, όπως ο σκληρός δίσκος.

- **up servers/openvpn-teithe/bin/create_vpn_dir.sh** : Με την παράμετροι “up” ορίζουμε ένα σενάριο (script) που θα εκτελείται από τον OpenVPN server σε κάθε ξεκίνημα της υπηρεσίας. Το συγκεκριμένο script καλείται για ν' αρχικοποιήσει το προσωρινό φάκελο που ορίσαμε προηγουμένως.

5.3 Σενάρια (scripts)

Ένα από τα μεγαλύτερα προτερήματα του OpenVPN είναι η δυνατότητα που παρέχει στο χειρισμό και στην χρήση ανεξάρτητων εκτελέσιμων και σεναρίων (scripts) σε διάφορες στιγμές, όπως σύνδεσης - αποσύνδεσης κάποιου client κατά την ενεργοποίηση - απενεργοποίηση των εικονικών συσκευών (TUN/TAP) καθώς και για την αυθεντικοποίηση με username / password των client.

Στην περίπτωση του OpenVPN server του Τμήματος Πληροφορικής, έπρεπε να χρησιμοποιηθούν οι υπάρχοντες λογαριασμοί των χρηστών (φοιτητών και διδακτικού προσωπικού) του server “aetos”. Αυτό έγινε εφικτό με την δημιουργία σεναρίων κελύφους “bash” περιβάλλοντος UNIX, του προγράμματος ασφαλούς απομακρυσμένης πρόσβασης SSH και του εργαλείου “expect”.

Το expect είναι ένα πρόγραμμα που “μιλά” με άλλα διαδραστικά προγράμματα, σύμφωνα με ένα σενάριο. Με το σενάριο αυτό, το expect γνωρίζει τι μπορεί να αναμένει από ένα πρόγραμμα και ποια είναι η σωστή απάντηση σε έναν

ενδεχόμενο διάλογο. Παρέχει υψηλού επιπέδου δομές ελέγχου για να κατευθύνει το διάλογο αυτό και επιπλέον, ο χρήστης μπορεί να πάρει τον έλεγχο και να αλληλεπιδράσει άμεσα όταν χρειάζεται, ή να επιστρέψει τον έλεγχο στο σενάριο του expect.

Όλα τα σενάρια (scripts) τοποθετήθηκαν στον κατάλογο “servers/openvpn-teithe/bin/” που δημιουργήθηκε από το webmin OpenVPN+CA, μέσα στον εξορισμού κατάλογο με τα αρχεία ρυθμίσεως του OpenVPN “/etc/openvpn/”,

5.4 Αυθεντικοποίηση

Για την αυθεντικοποίηση των clients χρησιμοποιείται η παράμετρος “auth-user-pass-verify” στο αρχείο ρυθμίσεων του OpenVPN server για να καλέσει το σενάριο (script) **auth_aetos_user.sh**. Έπειτα μέσω της επιλογής “via-file” εισάγεται στο script το προσωρινό αρχείο με το username και password που δίνει κάθε φορά κάποιος client. Το script στη συνέχεια καλεί το “expect” σενάριο **auth_aetos_user.exp** περνώντας του σαν μεταβλητή με τη σειρά του το αρχείο με τα στοιχεία του client. Αυτό εκτελεί μια ασφαλή απομακρυσμένη ασφαλή σύνδεση SSH στον server “aetos.it.teithe.gr” με τα username και password που πήρε από το προσωρινά αποθηκευμένο αρχείο. Έπειτα εάν η προσπάθεια της σύνδεσης στον server “aetos” είναι επιτυχής επιστρέφει την τιμή “0” κατά την έξοδο του, αλλιώς επιστρέφει την τιμή “1”. Με τη σειρά του το script “auth_aetos_user.sh” επιστρέφει αντίστοιχα την τιμή “0” κατά την έξοδο του στον OpenVPN server επιτρέποντας έτσι την συνέχισή της σύνδεσης και τη δημιουργία του τούνελ για τον συγκεκριμένο χρήστη, αλλιώς επιστρέφει την τιμή “1”, όπου ο OpenVPN server τερματίζει άμεσα την σύνδεση με τον συγκεκριμένο client.

Τα αρχεία των σεναρίων (script) είναι τα εξής :

auth_aetos_user.sh

```
#!/bin/bash

pfile=$1

/etc/openvpn/servers/openvpn-teithe/bin/auth_aetos_user.exp $pfile >>
/dev/null

if [ $? -ne 0 ]; then
    exit 1
else
    exit 0
fi
```

auth_aetos_user.exp

```
#!/usr/bin/expect -f

set timeout 2
set host "aetos"
set file [lindex $argv 0]
set username [ string trim [ exec head -n1 $file ] ]
set password [ string trim [ exec tail -n1 $file ] ]

spawn ssh $username@$host echo OK
match_max 100000
expect "Are you sure you want to continue connecting (yes/no)? "
```

```
send -- "yes\r"  
expect "$username@$host's password: "  
send -- "$password\r"  
expect {  
    "OK\r" "exit 0"  
}  
  
exit 1
```

Το script που αρχικοποιεί (διαγράφει και δημιουργεί) με κατάλληλα δικαιώματα, τον κατάλογο που χρησιμοποιείται ως προσωρινό σημείο αποθήκευσης από τον OpenVPN server και καλείται κατά την εκκίνηση του με την παράμετρο “up” είναι :

create_vpn_dir.sh

```
#!/bin/bash  
  
rm -rf /tmp/.openvpn  
mkdir /tmp/.openvpn  
chown nobody.nogroup /tmp/.openvpn  
chmod 700 /tmp/.openvpn
```

Τέλος, αφού οριστεί η παράμετρος push “redirect-gateway def1”, ένα ενδεικτικό firewall script με τις απαραίτητες παραμέτρους NAT έτσι ώστε να είναι εφικτή η δρομολόγηση της IP κίνησης των client διαμέσου του VPN τούνελ προς το εσωτερικό δίκτυο του TEI καθώς και της πρόσβασης στο Internet μέσω αυτού, είναι το εξής :

vpn_firewall.sh

```
#!/bin/bash
#Ενεργοποίηση της IP προώθησης
echo "1" > /proc/sys/net/ipv4/ip_forward

#Για να επιτρέπεται η επικοινωνία με τις TUN/.TAP συσκευές
iptables -A INPUT -i tun+ -j ACCEPT
iptables -A FORWARD -i tun+ -j ACCEPT
iptables -A INPUT -i tap+ -j ACCEPT
iptables -A FORWARD -i tap+ -j ACCEPT

# Ενεργοποίηση NAT / Masquerade για το VPN subnet
iptables -t nat -A POSTROUTING -s 192.168.15.64/26 -j MASQUERADE
```

Το script πρέπει συγκεκριμένα να εκτελεστεί στο host περιβάλλον του Virtual Server.

5.5 Εκκίνηση OpenVPN Server

Εφόσον έχουν γίνει οι παραπάνω ενέργειες, μπορεί πλέον να ξεκινήσει η υπηρεσία του OpenVPN server μέσω του webmin OpenVPN+CA αρθρώματος από το μενού **VPN List**, στην καρτέλα **VPN server list**: του “openvpn-teithe” επιλέγοντας “Start” από το πεδίο “Action”.

VPN server list:										
Name	management	CA	proto	port	local	Logs	Client List	Status	Remove	Actions
openvpn-teithe	127.0.0.1 5207	openvpn-teithe-ca	tcp-server	443	195.251.123.180	Log	Client List	Disable	Remove	Start

Εναλλακτικός τρόπος για να ξεκινήσει η υπηρεσία είναι με την παρακάτω εντολή που δίνεται μέσω τερματικού, έχοντας δικαιώματα διαχειριστή “root”.

```
openvpn:~# /etc/init.d/openvpn start
```

6 ΚΕΦΑΛΑΙΟ 6- Υλοποίηση Client

6.1 Ρύθμιση OpenVPN Client

Το κυριότερο βήμα για την υλοποίηση του VPN τούνελ από την μεριά των client, είναι η δημιουργία του βασικού αρχείου ρυθμίσεων και κλειδιών του OpenVPN, που είναι το ίδιο για όλους τους OpenVPN clients, ανεξαρτήτως λειτουργικού συστήματος.

Η δημιουργία του αρχείου ρυθμίσεων OpenVPN client θα γίνει αρχικά όπως και για τον server με το webmin OpenVPN+CA άρθρωμα, έτσι ώστε να δημιουργηθεί η κατάλληλη δομή καταλόγων και αρχείων των client, αυτή τη φορά στον OpenVPN server. Θα χρειαστεί ξανά κάποια χειροκίνητη τροποποίηση (εισαγωγή και αφαίρεση) μερικών πιο εξειδικευμένων στοιχείων στο αρχείο ρυθμίσεων οι οποίες δεν μπορούν να γίνουν μέσω του webmin.

Από την αρχική σελίδα του OpenVPN+CA επιλέγεται το **VPN List** και έπειτα το **Client List** από τη γραμμή “openvpn-teithe” του **VPN server list**.

Help..
Module Config

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

VPN server list:										
Name	management	CA	proto	port	local	Logs	Client List	Status	Remove	Actions
openvpn-teithe	127.0.0.1 5207	openvpn-teithe-ca	tcp-server	443	195.251.123.180	Log	Client List	Disable		stop

ca (Certification Authority): openvpn-teithe-ca Creation of new VPN Server: select the Certification Authority and click New VPN server

VPN server list with simmetric key

VPN List is empty

Creation of new VPN Server with symmetrical key

[← Return to OpenVPN Administration](#)

Στην επόμενη σελίδα **VPN Client List openvpn-teithe** επιλέγεται το πλήκτρο “New VPN Client”.

Help..
Module
Config

OpenVPN Administration
OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

VPN Client List openvpn-teithe:
No client configured

New VPN Client Creation of NEW VPN client openvpn-teithe

Clients availables for OPENVPN GUI

[← Return to VPN server list](#)

Στην καρτέλα που ανοίγει έπειτα δεν χρειάζεται να γίνει καμία αλλαγή σε κάποιο από τα πεδία που περιέχει. Το μόνο που πρέπει να προστεθεί είναι στο πεδίο **Additional Configurations** η παράμετρος “auth-user-pass” που ενεργοποιεί στους OpenVPN clients την προτροπή για εισαγωγή username και password από τους χρήστες και αποθηκεύεται πατώντας το πλήκτρο “Save”.

New VPN Client openvpn-teithe

Name: openvpn-teithe-client

proto (Protocol): tcp-client

Device: tap

ca (Certification Authority): opevpn-teithe-ca

Choose key: automatic (= name)

cert (Client Certificate): automatic

key (Client Key): automatic

Diffie-Hellman random file: dh2048.pem

remote (Remote IP): IP server: openvpn.it.teithe. Port server: 443

Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks (option tls-auth): yes automatic (= server)

Encrypt packets with cipher algorithm (option cipher): BF-CBC

Use fast LZO compression (option comp-lzo): yes

User: nobody

Group: nogroup

Don't re-read key files (option persist-key): yes

Don't close and reopen TUN/TAP device or run up/down scripts (option persist-tun): yes

keepalive (A helper directive designed to simplify the expression of **ping** and **ping-restart** in server mode configurations): Ping: 10 Ping-Restart: 120

Set output verbosity: 2

Log at most n consecutive messages in the same category: 20

tun-mtu (Take the TUN device MTU to be n and derive the link MTU from it): automatic (= server)

fragment (Enable internal datagram fragmentation so that no UDP datagrams are sent which are larger than max bytes):

mssfix (Announce to TCP sessions running over the tunnel that they should limit their send packet sizes such that after OpenVPN has encapsulated them, the resulting UDP packet size that OpenVPN sends to its peer will not exceed max bytes): automatic (= server)

float (Allow remote peer to change its IP address and/or port number): yes

Additional Configurations: auth-user-pass

Στην συνέχεια από τη σελίδα **VPN Client List openvpn-teithe** με το πλήκτρο “Export” λαμβάνεται σε συμπιεσμένη μορφή το αρχείο “openvpn-teithe-client.zip”. Ταυτόχρονα δημιουργείται στον server ένας κατάλογος που περιλαμβάνει όλα τα αρχεία του client στην παρακάτω διαδρομή καταλόγου.

“/etc/openvpn/clients/openvpn-teithe/openvpn-teithe-client/”

[Help..](#)
[Module](#)
[Config](#)

OpenVPN Administration

OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

[Search Docs..](#)
[OpenVPN](#)
[Administration](#)

VPN Client List openvpn-teithe:					
Name	CA	proto	port	Export	Remove
openvpn-teithe-client	openvpn-teithe-ca	tcp-client		Export	Remove

New VPN Client

Creation of NEW VPN client openvpn-teithe

Clients availables for [OPENVPN GUI](#)

[← Return to VPN server list](#)

Μετά την αποσυμπίεση του, το “openvpn-teithe-client.zip” περιλαμβάνει ένα κατάλογο με το όνομα “openvpn-teithe-client”, όμοιο με τον κατάλογο που δημιουργήθηκε στον server, στον οποίο υπάρχουν τα εξής αρχεία : ca.crt, dh2048.pem, openvpn-teithe-client.conf, openvpn-teithe-client.crt, openvpn-teithe-client.key, openvpn-teithe-client.ovpn και ta.key

Το αρχείο openvpn-teithe-client.ovpn αποτελεί το βασικό αρχείο ρυθμίσεων για τον OpenVPN client σε περιβάλλον Microsoft Windows ενώ το αντίστοιχο για όλα τα υπόλοιπα λειτουργικά περιβάλλοντα είναι το openvpn-teithe-client.conf. Βασική διαφορά μεταξύ των δυο αρχείων είναι ότι στην ASCII κωδικοποίηση, το openvpn-teithe-client.ovpn περιέχει CRLF, LF χαρακτήρες και το ότι το openvpn-teithe-client.conf περιλαμβάνει τις παραμέτρους ασφαλείας δικαιωμάτων της διεργασίας του OpenVNP, **user nobody** και **group nogroup** που δεν έχουν χρηστική αξία σε

περιβάλλον Microsoft Windows. Συγκεκριμένα θα χρησιμοποιηθεί μόνο το αρχείο `openvpn-teithe-client.ovpn` το οποίο είναι συμβατό με όλα τα λειτουργικά συστήματα και τους υπάρχοντες OpenVPN clients.

Έπειτα, γίνεται επεξεργασία του `openvpn-teithe-client.ovpn` αρχείου με κάποιο επεξεργαστή κειμένου και αφαίρεση των περιττών πλέον παραμέτρων (`dh dh2048.pem`, `cert openvpn-teithe-client.crt`, `key openvpn-teithe-client.key`) αφού γι' αυθεντικοποίηση με τον OpenVPN server δεν θα χρησιμοποιηθούν τα X.509 πιστοποιητικά του client αλλά μόνο τα `username` και `password`.

Στην συνέχεια διαγράφονται τα αντίστοιχα περιττά, πλέον, αρχεία από τον κατάλογο (`dh2048.pem`, `openvpn-teithe-client.crt`, `openvpn-teithe-client.key` και `openvpn-teithe-client.conf`).

Μία επιπλέον αλλαγή είναι η επιλογή **“`resolv-retry infinite`”** σε **“`resolv-retry 60`”** που ορίζει ότι ο OpenVPN client θα προσπαθήσει για “60” δευτερόλεπτα ν' αντιστοιχίσει το `hostname` του OpenVPN server σε μια IP διεύθυνση και όχι επ' άπειρο.

Η τελική μορφή του αρχείου ρυθμίσεως είναι :

“`openvpn-teithe-client.ovpn`”

```
client
proto tcp-client
dev tap
ca ca.crt
remote openvpn.it.teithe.gr 443
tls-auth ta.key 1
cipher BF-CBC
verb 2
mute 20
keepalive 10 120
```

```
comp-lzo
persist-key
persist-tun
float
resolv-retry 60
nobind
auth-user-pass
```

Στη συνέχεια, περιγράφεται συνοπτικά το τι ορίζουν οι διαφορετικές παράμετροι που υπάρχουν στο αρχείο ρυθμίσεως των OpenVPN client σε σχέση με τις παραμέτρους του αρχείου ρυθμίσεων του OpenVPN server.

- **client** : Ορίζει το OpenVPN ότι πρόκειται να ενεργοποιηθεί ως υπηρεσία πελάτη “client”
- **proto tcp-client** : Ορίζει το πρωτόκολλο που χρησιμοποιεί ο OpenVPN client.
- **remote openvpn.it.teithe.gr 443** : Ορίζει το hostname του OpenVPN server και την πόρτα που θα προσπαθήσει να συνδεθεί ο client.
- **tls-auth ta.key 1** : Ορίζει τη σχετική διαδρομή και το όνομα του αρχείου που βρίσκετε το κλειδί που χρησιμεύει στην προστασία έναντι των (DOS) επιθέσεων από τον OpenVPN server και έχει την τιμή “1” στους clients.
- **nobind** : Η τελευταία αυτή παράμετρος που υπάρχει μόνο στο αρχείο ρυθμίσεων των OpenVPN clients, ορίζει ότι η διεργασία του OpenVPN θα δέσμευσει τυχαία μια port από την IP στοίβα ώστε να τη χρησιμοποιήσει για την αμφίδρομη επικοινωνία και ανταλλαγή IP

πακέτων με τον OpenVPN server κατά την διάρκεια της δημιουργίας του VPN τούνελ.

Έπειτα δημιουργείται ένα συμπιεσμένο αρχείο “openvpn-teithe-client.zip” με τα περιεχόμενα του φακέλου που έχουν επεξεργασθεί και μέσω sftp ανεβάζεται στον server “openvpn.it.teithe.gr”. Μέσω της βασικής ιστοσελίδας που κατασκευάστηκε, οι χρήστες μπορούν να το κατεβάσουν και να το εισάγουν χειροκίνητα, ανάλογα το λειτουργικό σύστημα που διαθέτουν και τους OpenVPN client που έχουν εγκαταστήσει, σύμφωνα με τις οδηγίες που δίνονται στη συνέχεια.

Μια διαφορετική και πιο εύκολη διαδικασία εγκατάστασης του OpenVPN client σε περιβάλλον Microsoft Windows γίνεται μέσω της δημιουργίας ενός προ-ρυθμισμένου προγράμματος εγκατάστασης που θα περιέχει και θα εγκαθιστά αυτόματα, εκτός από την εφαρμογή του OpenVPN, το παραπάνω αρχείο ρυθμίσεως και τα υπόλοιπα απαιτούμενα αρχεία για την δημιουργία της σύνδεσης με τον OpenVPN server, όπως περιγράφεται στη συνέχεια.

6.2 Δημιουργία Προγράμματος Εγκαταστάτης (Windows Client)

Για να αυτοματοποιηθεί η διαδικασία της εγκατάστασης του OpenVPN client δημιουργείται ένα πρόγραμμα εγκατάστασης με τη βοήθεια της Open Source εφαρμογής **Nullsoft Scriptable Install System** (NSIS). Το NSIS αποτελεί ένα σύστημα εγκατάστασης για Windows που βασίζεται σε σενάρια (scripts), έχει ελάχιστες απαιτήσεις και υποστηρίζεται από την Nullsoft, που είναι οι δημιουργοί του Winamp. Το NSIS χρησιμοποιείται ευρέως ως εναλλακτική λύση απέναντι σε εμπορικά προϊόντα όπως το InstallShield.

Η εγκατάσταση του NSIS συστήματος γίνεται έχοντας δικαιώματα διαχειριστή “root” και χρησιμοποιείται το έτοιμο πακέτο εγκατάστασης “deb” μέσω της εφαρμογής aptitude. Σημειώνεται ότι για λόγους αντιμετώπισης κάποιων

προβλημάτων συμβατότητας, πρέπει να εγκατασταθεί η testing “2.46-1” έκδοση του nsis .deb πακέτου.

```
openvpn:~# aptitude install -t testing nsis
```

Με βάση τις οδηγίες και τα παραδείγματα από NSIS script του “Mathias Sundman” που βρίσκονται στην ιστοσελίδα “<http://openvpn.se/>” και της γραφικής εφαρμογής διαχείρισης OpenVPN (openvpn-gui έκδοσης “1.0.3”) σε συνδυασμό με τις τελευταίες εκδόσεις “2.1.1” εκτελέσιμων του OpenVPN και του προγράμματος εγκατάστασης για Windows που υπάρχουν στην επίσημη ιστοσελίδα του OpenVPN “<http://openvpn.net/>”, δημιουργήθηκαν το NSIS script “openvpn-gui.nsi” (παρατίθεται στο παράρτημα) και τα αρχεία που αυτό χρειάζεται για τη παραγωγή του προρυθμισμένου προγράμματος εγκατάστασης OpenVPN client, συγκεκριμένα για τον OpenVPN server του Τμήματος Πληροφορικής.

Δημιουργήθηκε έπειτα το συμπιεσμένο αρχείο “openvpn_it_install_source-2.1.1-gui-1.0.3.tar.bz2” , το οποίο περιλαμβάνει τα αρχεία, τη δομή καταλόγων, καθώς και το openvpn-gui.nsi script και τοποθετήθηκε στην ιστοσελίδα “<http://openvpn.it.teithe.gr/pub/>.”

Αφού κατεβεί και αποσυμπιεστεί το παραπάνω αρχείο μέσα στον κατάλογο “openvpn_it_install_source-2.1.1-gui-1.0.3”, για να δημιουργηθεί το προρυθμισμένο εκτελέσιμο, καλείται ο NSIS compiler εκτελώντας την παρακάτω εντολή .(Δεν απαιτούνται δικαιώματα διαχειριστή)

```
openvpn:~$ makensis openvpn-gui.nsi
```

Μετά την ολοκλήρωση της διαδικασίας, δημιουργήθηκε το εκτελέσιμο αρχείο εγκατάστασης openvpn-it-2.1.1-gui-1.0.3-install.exe το οποίο τοποθετήθηκε για κατέβαση από τους χρήστες στην ιστοσελίδα “openvpn.it.teithe.gr”

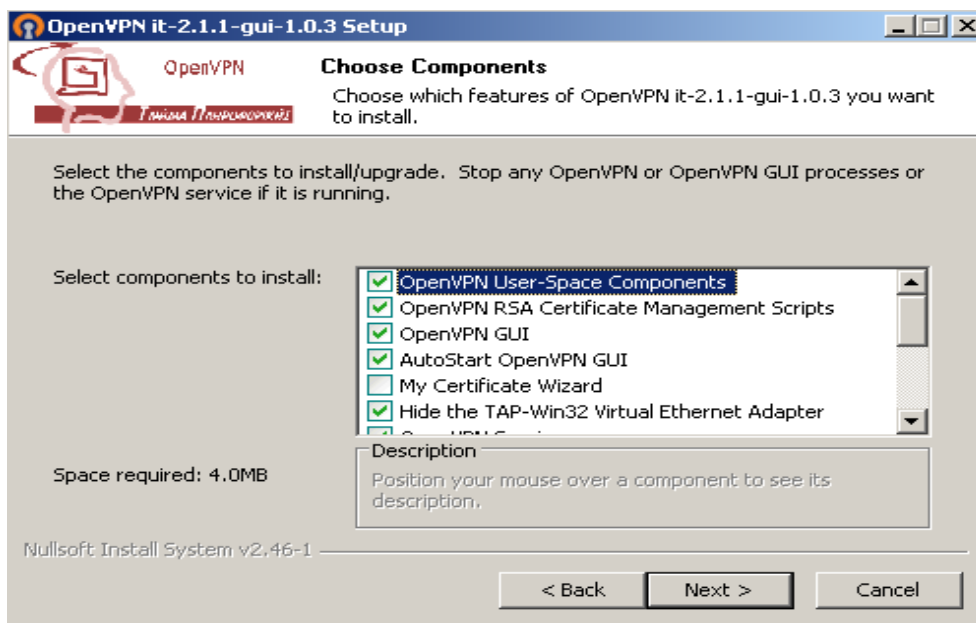
Τα προβλήματα που επιλύθηκαν με την τροποποίηση του `openvpn-gui.nsi` script και τη δημιουργία του `openvpn-it-2.1.1-gui-1.0.3-install.exe` είναι :


- Η αυτόματη εγκατάσταση του OpenVPN client στις πιο πρόσφατες εκδόσεις λειτουργικών συστημάτων Microsoft Windows (XP, Vista 32/64 και Windows 7 32/64)
- Η αυτόματη ρύθμιση του “User Account Control” (UAC) της εφαρμογής του OpenVPN να εκτελείται με δικαιώματα διαχειριστή στα Window Vista και Window 7.
- Η αυτόματη εγκατάσταση του αρχείου ρυθμίσεων “`openvpn-teithe-client.ovpn`” καθώς και των αρχείων `ca.crt` και `ta.key` που χρειάζονται για τη σύνδεση και δημιουργία του OpenVPN τούνελ.

6.2.1 Αυτόματη Εγκατάσταση (Windows Client)

Το μόνο που έχει να κάνει ο εκάστοτε χρήστης με λειτουργικό σύστημα Windows για να δημιουργήσει μια VPN σύνδεση με τον OpenVPN server του Τμήματος Πληροφορικής, είναι να κατεβάσει και να εγκαταστήσει το `openvpn-it-2.1.1-gui-1.0.3-install.exe` από τη ιστοσελίδα “`openvpn.it.teithe.gr`”.

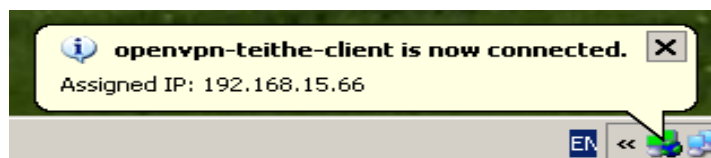
Ακολουθώντας τις οδηγίες του προγράμματος εγκατάστασης και μέσω μιας πληθώρας επιλογών, θα εγκαταστήσει το πρόγραμμα OpenVPN, τον εικονικό οδηγό TUN / TAP με την επιλογή “hide” προεπιλεγμένη, έτσι ώστε να μην εμφανίζεται στο μενού “Συνδέσεις Δικτύου” η εικονική συσκευή δικτύου και τέλος τα αρχεία ρυθμίσεων “`openvpn-teithe-client.ovpn`, `ca.cert` και `ta.key`”. (Η εικονική συσκευή δικτύου μπορεί να γίνει ορατή σε περίπτωση που κάποιος θέλει να γεφυρώσει “bridge” το VPN με κάποια άλλη συσκευή δικτύου)



Μετά την εγκατάσταση εμφανίζεται ένα νέο εικονίδιο  στη μπάρα εικονιδίων. Κάνοντας διπλό κλικ σε αυτό, ανοίγει το παράθυρο στο οποίο εισάγεται το username και το password, του αντίστοιχου λογαριασμού του server aetos.it.teithe.gr.



Αν η όλη διαδικασία εκτελέστηκε σωστά, τα παράθυρα θα εξαφανιστούν και θα επιβεβαιωθεί ότι έγινε σύνδεση.



Για ν' αποσυνδεθεί και να τερματιστεί το VPN χρησιμοποιείται το ίδιο εικονίδιο επιλέγοντας "Disconnect".

6.3 Εγκατάσταση (Linux Client)

Η εγκατάσταση του OpenVPN σε λειτουργικό σύστημα Linux εξαρτάται από την εκάστοτε διανομή. Για παράδειγμα στη Debian, όπως και στον server, εγκαθίσταται με την παρακάτω εντολή :

```
~# aptitude install openvpn
```

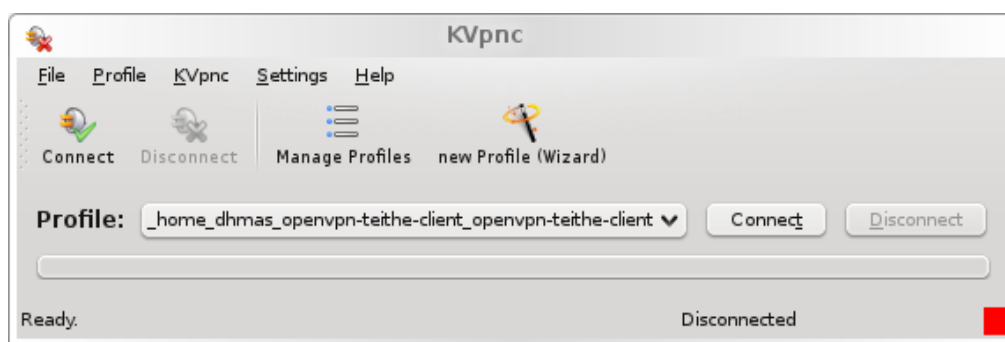
Μετά την ολοκλήρωση της εγκαταστάσεως του openvpn, πρέπει να μεταφορτωθεί το αρχείο ρυθμίσεων “openvpn-teithe-client.zip” από την ιστοσελίδα “<http://openvpn.it.teithe.gr>” και να αποσυμπιεστεί σε κάποιον κατάλογο. Έπειτα, με χρήση τερματικού μέσα στον κατάλογο αυτό, έχοντας δικαιώματα διαχειριστή “root”, ξεκινάει η διαδικασία σύνδεσης του OpenVPN client εκτελώντας την παρακάτω εντολή :

```
~# openvpn openvpn-teithe-client.ovpn
```

Εισάγεται στη συνέχεια, το username και το password που διαθέτουν στον server aetos.it.teithe.gr και γίνεται η σύνδεση, η οποία διαρκεί όσο παραμένει ανοιχτό το τερματικό.

Εναλλακτικά, μπορεί να χρησιμοποιηθεί κάποια γραφική εφαρμογή όπως το KVRnc που εκτός των άλλων τύπων VPN client υποστηρίζει και το OpenVPN. Αφού γίνει εγκατάσταση με τον κατάλληλο τρόπο ανάλογα τη διανομή Linux, η εφαρμογή εκτελείται και πάλι έχοντας δικαιώματα διαχειριστή “root”. Στη συνέχεια γίνεται επιλογή από το μενού “Profile” του “Import OpenVPN config file”. Έπειτα επιλέγεται το αρχείο ρυθμίσεων “openvpn-teithe-client.ovpn” από τον κατάλογο όπου έχει αποσυμπιεστεί προηγουμένως. Επειδή το αρχείο ρυθμίσεων περιέχει τις σχετικές διαδρομές των αρχείων που απαιτούνται για την υλοποίηση της OpenVPN σύνδεσης, θα χρειαστεί να δηλωθεί η πλήρης διαδρομή αυτών των

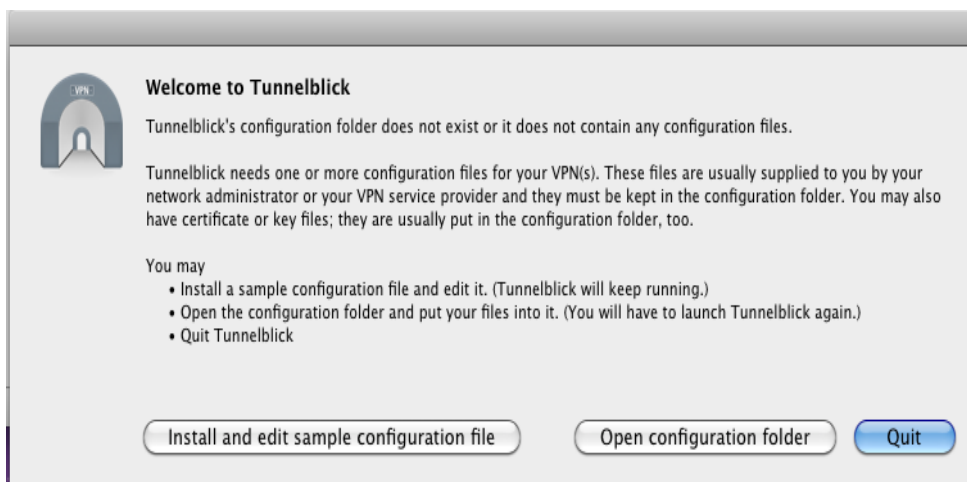
αρχείων. Αφού επιλεγθεί το “Manage Profiles”, στην καρτέλα “Authentication -> Certificate” πρέπει να εισαχθεί η πλήρης διαδρομή για το αρχείο ca.crt στο πεδίο “CA certificate path”, ενώ στην καρτέλα “Connection specific -> OpenVPN” η πλήρης διαδρομή για το αρχείο ta.key στο πεδίο “Use TLS auth”. Τέλος, έχοντας ολοκληρώσει τις παραπάνω αλλαγές γίνεται σύνδεση στον OpenVPN server, πατώντας “Connect” αφού εισαχθεί το αντίστοιχο username και password του server aetos.it.teithe.gr.




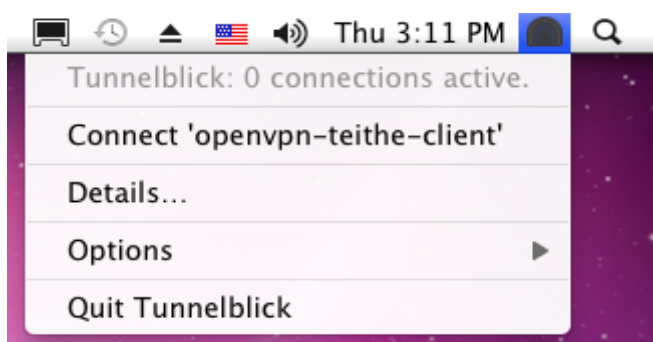
6.4 Εγκατάσταση (Mac OS X Client)

Για τη δημιουργία VPN σύνδεσης από το λειτουργικό σύστημα Mac OS X, οι χρήστες πρέπει να εγκαταστήσουν την open source γραφική εφαρμογή Tunnelblick που αναπτύχθηκε από τους Angelo Laub και Dirk Theisen, μεταφορτώνοντας το πακέτο εγκατάστασης “Tunnelblick_3.0.dmg” που βρίσκεται στην ιστοσελίδα “<http://code.google.com/p/tunnelblick/>”. Παράλληλα, πρέπει να κατεβάσουν το αρχείο “openvpn-teithe-client.zip” που περιλαμβάνει το αρχείο ρυθμίσεως και τα απαραίτητα αρχεία για την OpenVPN σύνδεση από την ιστοσελίδα “<http://openvpn.it.teithe.gr>”

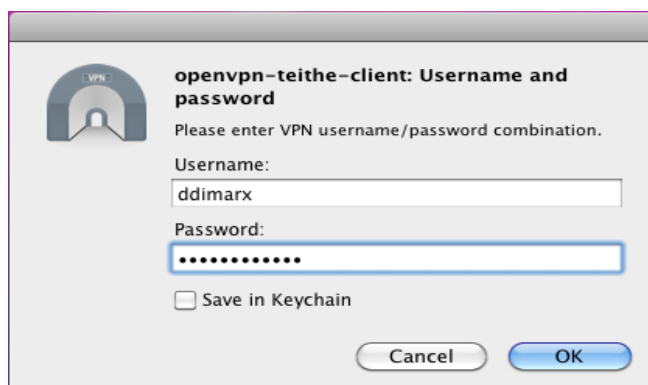
Μόλις ολοκληρωθεί η εγκατάσταση της εφαρμογής Tunnelblick από την καρτέλα που εμφανίζεται, επιλέγεται το “Open configuration folder”.



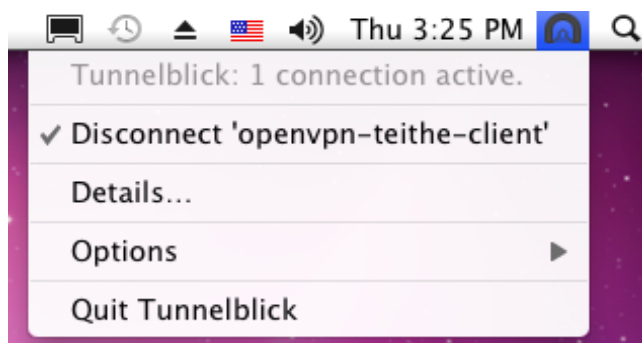
Έπειτα, αντιγράφεται μέσα σε αυτόν το κατάλογο : `"/Users/{User Home}/ApplicationSupport/Library/Tunnelblick/Configurations/"` το αρχείο ρυθμίσεως `openvpn-teithe-client.ovpn` καθώς και τα άλλα δυο αρχεία `ca.crt` και `ta.key`. Μετά από την αντιγραφή μπορεί ο χρήστης να ξεκινήσει την εφαρμογή Tunnelblick από το μενού Application. Κάνοντας κλικ στο εικονίδιο  που θα εμφανιστεί στη μπάρα εικονιδίων, επιλέγεται το `"Connect 'openvpn-teithe-client'"`.



Εισάγεται το `username / password` και με την επιλογή `"OK"` υλοποιείται η σύνδεση.



Για να γίνει αποσύνδεση επιλέγεται αντίστοιχα το “Disconnect” ή το “Quit Tunnelblick” ώστε να κλείσει η εφαρμογή :



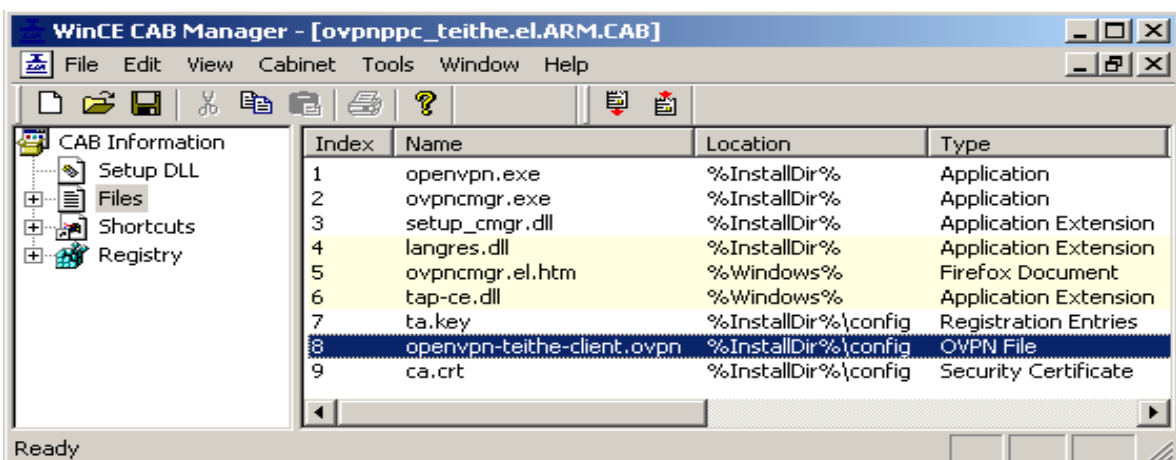
6.5 Υλοποίηση - Εγκατάσταση (PocketPC Client)


Είναι επίσης δυνατή η εγκατάσταση του OpenVPN σε συσκευές (PDA / PocketPC) που τρέχουν λειτουργικό σύστημα Windows CE. Βασιζόμενοι στο “OpenVPN PocketPC port” που βρίσκεται στη ιστοσελίδα “<http://ovpnppc.ziggurat29.com>”, χρησιμοποιήθηκε το αρχείο αυτόματης εγκατάστασης του OpenVPN έκδοσης “2.1.0” “ovpnppc.el.ARM.CAB” με ελληνικό μενού το οποίο μεταφορτώνεται από την διεύθυνση “<http://ovpnppc.ziggurat29.com/files/2.1.0/ovpnppc.el.ARM.CAB>”.

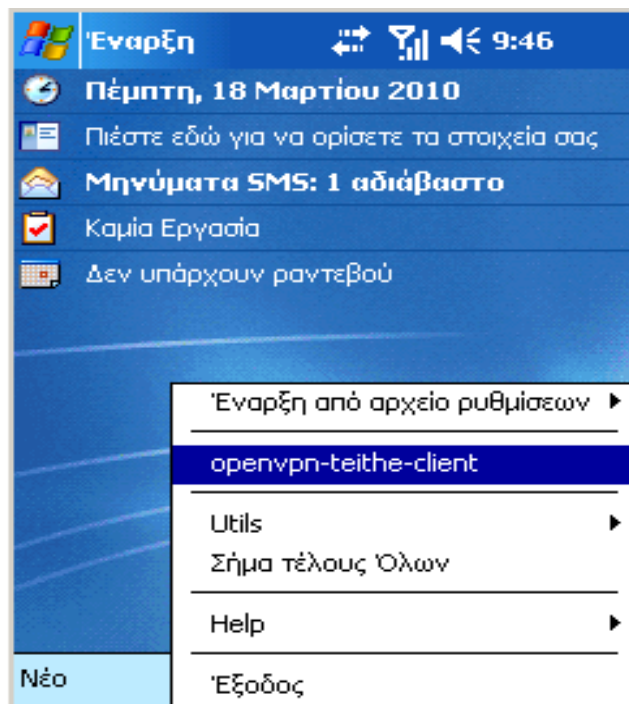
Επιπλέον χρησιμοποιήθηκε η εφαρμογή “WinCE CAB Manager” της εταιρίας “OCP Software”, η οποία διαχειρίζεται (διαβάζει και γράφει) τη μορφή αρχείου τύπου CAB που χρησιμοποιείται για την εγκατάσταση εφαρμογών σχεδιασμένων για το λειτουργικό σύστημα Windows CE.

Με την εφαρμογή “WinCE CAB Manager” δημιουργήθηκε το αρχείο “ovnpnppc_teithe.el.ARM.CAB” που υπάρχει και αυτό διαθέσιμο στην ιστοσελίδα “http://openvpn.it.teithe.gr”. Αυτό έγινε τροποποιώντας το αρχείο “ovnpnppc.el.ARM.CAB” στο οποίο εισήχθησαν τα αρχεία ca.crt και ta.key και το αρχείο ρυθμίσεως openvpn-teithe-client.ovpn. Το αρχείο ρυθμίσεως, αλλάχτηκε προηγουμένως έτσι ώστε να είναι συμβατό με την “σχετική διαδρομή” καταλόγων και αρχείων που απαιτείται από το λειτουργικό σύστημα Windows CE όπως φαίνεται παρακάτω. : **“openvpn-teithe-client.ovpn”**

```
(...)
dev tap
ca "\\Program Files\\OpenVPN\\config\\ca.crt"
remote openvpn.it.teithe.gr 443
tls-auth "\\Program Files\\OpenVPN\\config\\ta.key" 1
cipher BF-CBC
(...)
```



Οι κάτοχοι PocketPC με Windows CE, αφού κατεβάσουν το αρχείο “ονρηrrc_teithe.el.ARM.CAB” που δημιουργήθηκε από την ιστοσελίδα “http://openvpn.it.teithe.gr” και το αποθηκεύσουν σε κάποιο κατάλογο στη συσκευή τους ή σε κάποιας μνήμης επέκτασης (πχ.”SD memory”), μπορούν να εγκαταστήσουν αυτόματα το OpenVPN και τα προαπαιτούμενα αρχεία σύνδεσης με τον OpenVPN server του Τμήματος Πληροφορικής, απλά πατώντας επάνω στο όνομα του αρχείου μέσω της εφαρμογής “Διαχειρισή Αρχείων” των WindowsCE. Μετά την εγκατάσταση, το αρχείο “ονρηrrc_teithe.el.ARM.CAB” θα διαγραφεί αυτομάτως και θα εμφανιστεί το εικονίδιο . Κάνοντας κλικ επάνω του επιλέγεται “Έναρξη από αρχείο ρυθμίσεων” και στη συνέχεια “openvpn-teithe-client”. Έπειτα εισάγεται το username / password και με το “OK” ξεκινάει η σύνδεση. Αντίστοιχα για αποσύνδεση επιλέγεται το “Σήμα τέλους Όλων” και “Έξοδος” ώστε να κλείσει η εφαρμογή.



7 ΚΕΦΑΛΑΙΟ 7- Διαχείριση - Παρατηρήσεις - Προβλήματα

7.1 Διαχείριση των VPN συνδέσεων

Μετά την ολοκλήρωση της εγκατάστασης του OpenVPN server και την ενεργοποίηση της υπηρεσίας, μπορεί κάποιος να εμποτεύσει και να διαχειριστεί τις ενεργές συνδέσεις μέσω του webmin OpenVPN+CA αρθρώματος, επιλέγοντας “Active Connection” από την κύρια σελίδα του. Στη σελίδα αυτή υπάρχουν πληροφορίες όπως το όνομα του χρήστη, η πραγματική IP διεύθυνση και το port που χρησιμοποιεί, η εικονική (MAC ή IP) διεύθυνση που του έχει αποδοθεί, ο όγκος σε “Bytes” των δεδομένων που έχουν διακινηθεί μέσω του VPN καθώς και το πόσο έγινε η σύνδεση και πόση διάρκεια έχει. Προσφέρεται επίσης η δυνατότητα τερματισμού των ενεργών VPN συνδέσεων.

Help..
Module Config

OpenVPN Administration
OpenVPN version 2.1_rc11, OpenSSL version 0.9.8g

Search Docs..
OpenVPN
Administration

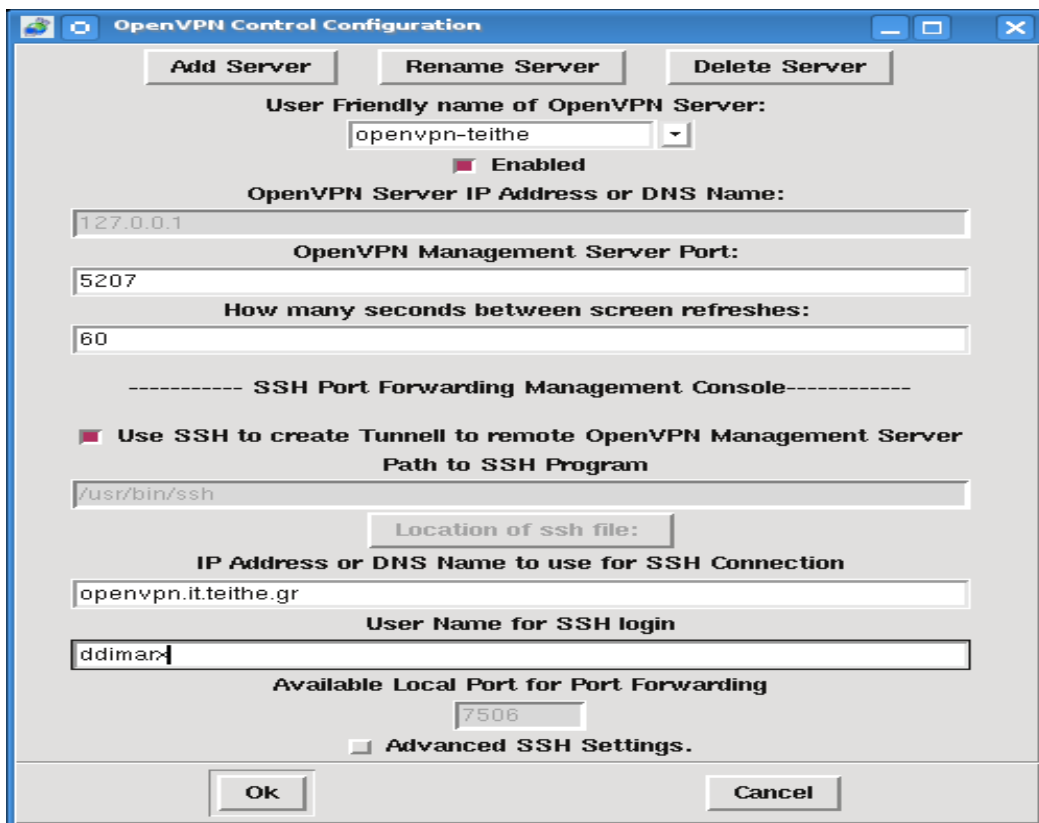
Active connection to VPN server						
Name	Virtual IP	Bytes received	Bytes sent	Real address	Connected since	remove key
VPN server: openvpn-teithe						
ddimarx	3a:5e:af:b6:06:be	36662	6802	79.107.224.233:35116	Sat Mar 20 17:24:15 2010	Stop and Disable

Active connection to VPN server with symmetrical key	
No VPN with management	

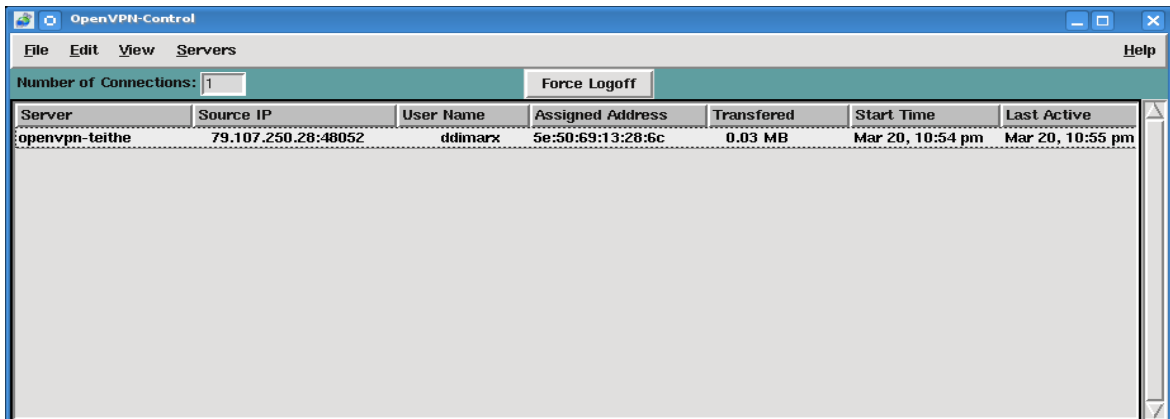
[Return to OpenVPN Administration](#)

Εναλλακτικά, ένας άλλος τρόπος διαχείρισης των συνδέσεων και του OpenVPN server είναι με τη χρήση του open source προγράμματος “**OpenVPN Control**” του Ron Dorn. Ανάλογα το λειτουργικό σύστημα που χρησιμοποιεί κανείς, μπορεί να κατεβάσει και να εγκαταστήσει το αντίστοιχο εκτελέσιμο από την ιστοσελίδα :
“<http://sourceforge.net/projects/openvpn-control/>”

Για να συνδεθεί το πρόγραμμα με το “management interface” του OpenVPN server, πρέπει, επιλέγοντας από το μενού “File -> Configure OpenVPN Control”, στην καρτέλα που θα εμφανιστεί, να οριστεί το “**OpenVPN Management Server Port**”, συγκεκριμένα “**5207**” και να επιλεγεί το “**Use SSH to create Tunnel to remote OpenVPN Management Server** “. Έπειτα εισάγονται στα αντίστοιχα πεδία το hostname του server “openvpn.it.teithe.gr” και το “login name” από κάποιο τοπικό user λογαριασμό.



Για να ολοκληρωθεί η διαδικασία της σύνδεσης, στο τερματικό παράθυρο που εμφανίζεται, πρέπει να εισαχθεί το σωστό password του χρήστη που δηλώθηκε προηγουμένως. Μόλις γίνει με επιτυχία μια ssh σύνδεση, ενεργοποιείται η διαχείριση του OpenVPN server προσφέροντας πληροφορίες και έλεγχο για τις OpenVPN ενεργές συνδέσεις.



The screenshot shows the OpenVPN-Control application window. At the top, there is a menu bar with 'File', 'Edit', 'View', 'Servers', and 'Help'. Below the menu bar, there is a 'Number of Connections' field set to '1' and a 'Force Logoff' button. The main area contains a table with the following data:

Server	Source IP	User Name	Assigned Address	Transferred	Start Time	Last Active
openvpn-teithe	79.107.250.28:48052	ddimarx	5e:50:69:13:28:6c	0.03 MB	Mar 20, 10:54 pm	Mar 20, 10:55 pm

7.2 Παρατηρήσεις κατά την VPN σύνδεση

Ο κάθε χρήστης με την έναρξη της VPN σύνδεσης αποκτά πρόσβαση στο Internet μέσω NAT με χρήση IP διευθύνσεων που του παρέχει ο OpenVPN server και ανήκουν στο εύρος διευθύνσεων του ΤΕΙ Θεσσαλονίκης. Εξαιτίας αυτού, αλλά και του τρόπου λειτουργίας της υπηρεσίας του OpenVPN παρατηρούνται τα εξής :

Πιθανή μείωση της ταχύτητας μεταφοράς δεδομένων, εφόσον ολόκληρη η κίνηση από και προς τον υπολογιστή του χρήστη γίνεται πλέον μέσω του VPN τούνελ το οποίο διενεργεί κρυπτογράφηση – αποκρυπτογράφηση των πακέτων που ανταλλάσσονται. Η τεχνική τις ενθυλάκωσις πακέτων μέσα σε άλλα IP πακέτα, επιφορτίζει την ροή δεδομένων με περισσότερα πακέτα, από ότι θα απαιτούνταν για την επικοινωνία εκτός του VPN τούνελ, όπως επίσης και το ότι παρεμβάλλονται ουσιαστικά περισσότεροι ενδιάμεσοι κόμβοι στην επικοινωνία δυο μερών.

Κλείσιμο των ενεργών ανοιχτών συνδέσεων που υπήρχαν κατά τη διάρκεια της έναρξης του VPN: Αυτό συμβαίνει κυρίως γιατί κατά την σύνδεση του VPN αλλάζει το Default Gateway του συστήματος του χρήστη. Έτσι όλα τα πακέτα που έχουν άγνωστο προς τον σταθμό εργασίας του χρήστη IP προορισμό,

αποστέλλονται πλέον από το καινούργιο Default Gateway, διακόπτοντας τις όποιες τυχών συνδέσεις δρομολογούνταν μέσω του παλαιού.

Αδυναμία χρήσης υπηρεσιών που παρέχονται από τους εκάστοτε ISP των χρηστών: Καθ' όλη τη διάρκεια της VPN σύνδεσης, ο υπολογιστής του χρήστη ανήκει πλέον σε δίκτυο ξένο, προς το αρχικό δίκτυο του ISP του, ο οποίος πιθανότατα, ν' απαγορεύει για παράδειγμα τη χρήση της αποστολής e-mail με τη χρήση του SMTP server του, καθώς και της υπηρεσίας DNS (πρόβλημα που παρακάμπτεται με την χρήση της επιλογής “push "dhcp-option DNS” στον OpenVPN server και τη χρησιμοποίηση του OpenDNS).

Όλα τα παραπάνω θέματα είναι γνωστά και οφείλονται κυρίως στην αλλαγή της IP διεύθυνσης των χρηστών κατά τη διάρκεια της VPN σύνδεσης, έπειτα από τον τερματισμό της οποίας, επανέρχονται όλα στην προηγούμενη, φυσιολογική κατάσταση πρόσβασης.

7.3 Προβλήματα κατά την VPN σύνδεση

Συχνά παρατηρούνται κάποια προβλήματα στην επίτευξη της σύνδεση VPN κάποιων client με τον OpenVPN server, τα οποία πιθανώς οφείλονται στη χρήση κάποιου firewall, χάρη στο οποίο, εμποδίζεται η επικοινωνία με την προεπιλεγμένη πόρτα επικοινωνίας του OpenVPN server (UDP 1194). Για το λόγο αυτό, στην παρούσα εγκατάσταση χρησιμοποιήθηκε η πόρτα TCP 443 που ανήκει στην υπηρεσία “https” και επιτρέπεται συνήθως από τα όλα τα firewall. Εάν παρόλα αυτά υπάρχει πρόβλημα, τότε θα πρέπει να δοκιμαστεί, η προσωρινή απενεργοποίηση του firewall ή να εισαχθούν σε αυτό κατάλληλοι κανόνες.

Επίσης, ένα σύνθητες πρόβλημα στη λειτουργία του OpenVPN σε συστήματα με Windows XP (Service Pack 2) σε συνδυασμό με κάποια firewalls ανεξάρτητων

κατασκευαστών, είναι το γεγονός ότι , ενώ φαίνεται ότι ο client έχει συνδεθεί με τον OpenVPN server, υπάρχει πρόβλημα κατά την ανάθεση της VPN IP διεύθυνσης και της IP επικοινωνίας με αυτόν. Λύση αυτού του είδους προβλημάτων, είναι η αναβάθμιση των Windows XP σε (Service Pack 3).

Τέλος, ένας άλλος λόγος που η σύνδεση δεν ολοκληρώνεται ποτέ, είναι η περίπτωση να είναι κλειστή για κάποιο λόγο η υπηρεσία “DHCP Client Service” των Windows (η οποία από προεπιλογή, πρέπει να είναι ενεργοποιημένη). Για το λόγο αυτό, το OpenVPN δεν μπορεί να αναθέσει στο σύστημα τις διάφορες παραμέτρους που αποστέλλει ο OpenVPN server όπως “VPN IP διεύθυνση, DNS, Default Gateway κ.α”.

8 ΚΕΦΑΛΑΙΟ 8- OpenVPN και Ασφαλές Σερφάρισμα

Με βάση τους μηχανισμούς κρυπτογράφησης (ασφάλειας, ακεραιότητας και εμπιστευτικότητας) που προσφέρει μια OpenVPN σύνδεση για τη μεταφορά δεδομένων από και προς το δίκτυο του τμήματος πληροφορικής και μέσω αυτού στο Internet, γεννήθηκε η ιδέα της δημιουργίας μιας πύλης ασφαλείας και της περαιτέρω αύξησης, μέσω αυτής, της ασφαλείας των δεδομένων που λαμβάνει ο κάθε χρήστης κυρίως κατά το “σερφάρισμα” ιστοσελίδων στο διαδίκτυο και το κατέβασμα αρχείων.

Η υλοποίηση αυτής της ιδέα μπορεί να γίνει με τη χρήση ενός φίλτρου ελέγχου περιεχομένου ιστοσελίδων “Web filtering” ή “Content filtering” .Το **DansGuardian** είναι ένα τέτοιο φίλτρο το οποίο διαθέτει μηχανισμούς ελέγχου του περιεχομένου μιας ιστοσελίδας προτού εμφανιστεί στον τελικό αποδέκτη που μπορεί να είναι και παιδιά μικρής ηλικίας. Μεταφορτώνει πριν τον τελικό χρήστη τα δεδομένα αυτά χρησιμοποιώντας έναν διακομιστή μεσολάβησης (**Proxy Server**) όπως ο Squid. Και χρησιμοποιεί το “ClamAV” antivirus για να ελέγχει για ιούς και άλλα επιβλαβή προγράμματα, δεδομένα και αρχεία που κατεβάζονται από το χρήστη.

Βασικό στην όλη διαδικασία είναι να λειτουργεί το σύστημα δίχως να χρειάζεται να κάνει κάποια ρύθμιση ή να το γνωρίζει ο τελικός χρήστης, δημιουργώντας έτσι, έναν διάφανο “**Transparent Proxy Server**”.

8.1 Φίλτρο ελέγχου περιεχομένων : “DansGuardian”

Το DansGuardian είναι ένα open source φίλτρο περιεχομένου ιστοσελίδων (web content filter), δημιουργοί του οποίου είναι οι Daniel Barron και Philip Allison. Φιλτράρει το πραγματικό περιεχόμενο των ιστοσελίδων, βασιζόμενο στην ταύτιση φράσεων ή λέξεων, στα μεταδεδομένα που συνδέονται με το περιεχόμενο του διαδικτύου και στα URL's των ιστοσελίδων. Σχεδιάστηκε κυρίως ώστε να

βοηθήσει εκπαιδευτικούς και γονείς να προσαρμόζουν την πρόσβαση παιδιών στο διαδικτυακό περιεχόμενο.

Οι βασικοί μηχανισμοί και οι μέθοδοι φιλτραρίσματος που διαθέτει και χρησιμοποιεί είναι:

Λευκές Λίστες : Οι “Whitelist”, ή αλλιώς οι λεγόμενες “περιφραγμένες τοποθεσίες” (walled gardens) είναι λίστες από ιστοσελίδες που είναι κατάλληλες γι’ ανηλίκους και επιτρέπουν στον χρήστη να έχει πρόσβαση αποκλειστικά σε αυτές.

Μαύρες Λίστες : Μία μαύρη λίστα “Blacklist” από ιστοσελίδες που πρέπει να αποφευχθούν (π.χ. με προσβλητικό, βίαιο ή ρατσιστικό περιεχόμενο), στις οποίες μπλοκάρεται η πρόσβαση, αν ο χρήστης προσπαθήσει να εισέλθει ηθελημένα ή μη.

Λίστες απαγορευμένων λέξεων : Μόλις βρεθεί κάποια από αυτές τις λέξεις – κλειδιά, σε κάποια ηλεκτρονική διεύθυνση ή στην ίδια την ιστοσελίδα, τότε μπλοκάρεται η πρόσβαση. Οι λίστες αυτές όπως και οι μαύρες λίστες αναβαθμίζονται συνεχώς.

Φιλτράρισμα βάσει αυτόματης ταξινόμησης του περιεχομένου : Τα συστήματα αυτόματης ταξινόμησης που διαθέτει αξιολογούν ολόκληρο το κείμενο που υπάρχει σε μια ιστοσελίδα. Χρησιμοποιώντας για αυτό γνωστές στατιστικές μεθόδους, όπως αυτές που εφαρμόζουν τα φίλτρα ανεπιθύμητης αλληλογραφίας.

Αυτοαξιολόγηση ιστοσελίδων : Οι Πάροχοι της διαδικτυακής πληροφορίας τοποθετούν εθελοντικά στον αντίστοιχο Ιστοχώρο μια ετικέτα “tag”, η οποία δείχνει αν και σε ποιο βαθμό η ιστοσελίδα αυτή περιέχει συγκεκριμένο επιβλαβές υλικό για τους χρήστες ανάλογος την ηλικία τους (π.χ. βία, γυμνό, σεξ, τζόγο, αλκοόλ,

χυδαία γλώσσα, κ.α). Οι ετικέτες και οι κατηγορίες έχουν δημιουργηθεί από την Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου ICRA (Internet Content Rating Association). Το φίλτρο διαβάζει αυτές τις ετικέτες και αποφασίζει αν θα επιτρέψει την πρόσβαση ή όχι , σύμφωνα με το επίπεδο ασφαλείας – ηλικίας που του έχει ορισθεί. Το πρόβλημα με αυτό το σύστημα είναι, ότι εξαρτάται από το αν οι ιδιοκτήτες των ιστοσελίδων θ' αξιολογήσουν εθελοντικά ή όχι,τις ιστοσελίδες τους.

Συνδυασμός μεθόδων φιλτραρίσματος : Το DansGuardian μπορεί να συνδυάσει όλες μαζί τις προσεγγίσεις στο φιλτράρισμα, (τεχνολογία επεξεργασίας κειμένου - γλώσσας, επεξεργασίας εικόνας και ανάλυσης του δικτυακού τόπου μεσώ των “tag”), ώστε να φτάσει σ' ένα θεωρητικό μοντέλο, το οποίο μπορεί να αποφανθεί εάν μία σελίδα έχει ακατάλληλο - επιβλαβές περιεχόμενο ή όχι, διαφοροποιώντας την προσβασιμότητα, ανάλογα την ηλικία των χρηστών. Συνεπώς, αναζητήσεις όρων, όπως “sex”, “έρωτας”, “ερωτισμός”, “σεξουαλικά μεταδιδόμενες ασθένειες”, δεν πρόκειται να ανακοπούν από το DansGuardian, το οποίο είναι αρκετά “έξυπνο”, ώστε να καταλάβει ότι αυτή η αναζήτηση, σύμφωνα με τα αποτελέσματα που επιστρέφει, δεν οδηγεί σε πορνογραφικό υλικό, αλλά αντίθετα οδηγεί σε γενικότερες πληροφορίες για τη σεξουαλικότητα, πράγμα που οι χρήστες μπορεί ν' αναζητήσουν είτε για προσωπικό τους ενδιαφέρον, είτε για να πραγματοποιήσουν κάποια εργασία.

Επέκτασης “Antivirus” : Τέλος το DansGuardian μπορεί να παρέχει προστασία από ιούς και κακόβουλα προγράμματα στα δεδομένα που μεταβιβάζει τελικός στους χρήστες, καλώντας ως επέκταση “plugins” αντί-υικά προγράμματα όπως το ClamAV που ελέγχουν τα δεδομένα αυτά.

8.1.1 Εγκατάσταση του “DansGuardian”

Η εγκατάσταση του dansguardian και των προαπαιτούμενων από αυτό εφαρμογών όπως το (ClamAV antivirus), μπορεί να γίνει καλώντας ως διαχειριστής “root” στο σύστημα την εφαρμογή aptitude.

```
openvpn:~# aptitude install dansguardian
```

Μετά την ολοκλήρωση της εγκατάστασης, για τη ρύθμιση και την παραμετροποίηση του, χρησιμοποιείται το webmin και το αντίστοιχο DansGuardian webmin module, η εγκατάσταση του οποίου γίνεται μέσω του μενού “Webmin -> Webmin Configuration” επιλέγοντας το “Webmin Modules”. Στη συνέχεια, επιλέγεται το “From ftp or http URL” στην καρτέλα “Install Module”, και εισάγεται στο διπλανό πεδίο η διεύθυνση της τελευταίας έκδοσης του module dgwebmin-0.7.0beta1b:”http://downloads.sourceforge.net/project/dgwebminmodule/dgwebmin-0.7.0beta1b/dgwebmin-0.7.0beta1b.wbm”, η οποία είναι συμβατή με την “stable” έκδοση του DansGuardian που εγκαταστάθηκε προηγουμένως. Επιλέγοντας το “Install Module” εγκαθίσταται.

[Module Index](#)

Webmin Modules

[Install](#) [Clone](#) [Delete](#) [Export](#)

Webmin modules can be added after installation by using the form to the right. Modules are typically distributed in .wbm files, each of which can contain one or more modules. Modules can also be installed from RPM files if supported by your operating system.

Install Module

Install from

From local file

From uploaded file

From ftp or http URL

Standard module from www.webmin.com

Third party module from

Ignore dependencies? Yes No

Grant access to

Grant access only to users and groups :

Grant access to all Webmin users

Μετά την ολοκλήρωση της εγκατάστασης, μπορεί να γίνει ρύθμιση και διαχείριση του DansGuardian επιλέγοντάς το από το μενού “Servers -> DansGuardian Web Content Filter”. Σημειώνεται ότι για να λειτουργήσει σωστά το module πρέπει να ρυθμιστούν από το “Module Config” κάποιες παράμετροι του συστήματος όπως η σωστή διαδρομή των καταλόγων και εκτελέσιμων του DansGuardian όπως “/usr/sbin/dansguardian”

Configuration

For module DansGuardian Web Content Filter

Configurable options for DansGuardian Web Content Filter	
Full path to DG config(etc) directory	/etc/dansguardian ...
Full path to DG pid file	/var/run/dansguardian.pid ...
Full path to DG binary	/usr/sbin/dansguardian ...
Full path to DG log directory	/var/log/dansguardian ...
Full path to DG messages file (or literal 'followDansGuardian')	followDansGuardian ...
Format of DG logfile	<input checked="" type="radio"/> followDansGuardian <input type="radio"/> force DG Native <input type="radio"/> force CSV <input type="radio"/> force Squid Native (no Log Analysis) <input type="radio"/> force TAB Delimited
Command to restart DG (if allowed)	<input type="radio"/> Module built-in -or- System <input checked="" type="radio"/> /etc/init.d/dansguardian rest
Auto restart DG as necessary (if allowed)	<input checked="" type="radio"/> explicit manual restart only <input type="radio"/> restart automatically
Command to start DG (if allowed)	<input type="radio"/> Module built-in -or- System <input checked="" type="radio"/> /etc/init.d/dansguardian star
Command to stop DG (if allowed)	<input type="radio"/> Module built-in -or- System <input checked="" type="radio"/> /etc/init.d/dansguardian sto
Auto reload DG groups as necessary (if allowed)	<input type="radio"/> explicit manual reload only <input checked="" type="radio"/> reload automatically
Include "fixed" lists (blacklists/phraselists/etc.) in displays	<input checked="" type="radio"/> exclude "fixed" lists from display <input type="radio"/> display "fixed" lists too

Save

Έπειτα, από την κεντρική σελίδα του module, είναι δυνατή η ρύθμιση μιας πληθώρας παραμέτρων που ορίζουν, από τον τρόπο που θα τρέχει η υπηρεσία (το port, τον proxy server που θα χρησιμοποιεί) έως το επίπεδο ασφαλείας και το είδος του φιλτραρίσματος που θα επιτελεί (ρύθμιση του antivirus, επιλογή των πεδίων της blacklist, το επίπεδο ηλικίας των χριστών και βαθμού ελέγχου του φίλτρου). Σημειώνεται ότι το DansGuardian παρέχει τη δυνατότητα ρύθμισης, έτσι ώστε να μην φιλτράρει την κίνηση, αλλά απλά να την καταγράφει και να λειτουργεί μόνο ως antivirus. Η τελική μορφή των βασικών αρχείων ρυθμίσεων του DansGuardian είναι “dansguardian.conf” και “dansguardianf1.conf” που βρίσκονται στον κατάλογο “/etc/dansguardian/”. Τέλος, το script “UpdateBL.sh” που εγκαθιστά

και ενημερώνει αυτόματα τις “Blacklist”, πρέπει να τοποθετείται στον κατάλογο “/etc/cron.daily” έτσι ώστε να εκτελείτε καθημερινά. (Τα αρχεία αυτά παρατίθενται στο παράρτημα.)

Login: root
Webmin
System
Servers
Apache Webserver
DansGuardian Web Content Filter
OpenVPN + CA
Read User Mail
SSH Server
Others
Networking
Hardware
Cluster
Un-used Modules
Search:
View Module's Logs
System Information
Refresh Modules
Logout

Help..
Module Config

DansGuardian
Version 2.9.9.4 (Webmin Module Version 0.7.0beta1b)

Stop-&-Restart DG
Stop DG
Reload DG Groups
Search Docs..

Manage DansGuardian - true web content filtering for all

Warning - running as root(superuser) risks new files not being readable by production DansGuardian

STATUS Display Status of Server(Daemon)	ANALYZE Analyze Logfiles	SEARCH Search for Phrase Words (or Domain or URL)	SYSCONF View/Edit System-Wide Base Config
PLUGINS View/Edit System-Wide Base Plugin Configs	SYSLISTS View/Edit System-Wide Lists	XLATE View/Edit System-Wide Messages(Translations)	ASSIGN View/Edit Filter Group Assignments
CONFS View/Edit A Filter Group's Base Config	LISTS View/Edit A Filter Group's Lists	MULTI View How Lists&Configs For Multiple Filter Groups Are Set Up	SETUP Set Up Lists&Configs For Multiple Filter Groups

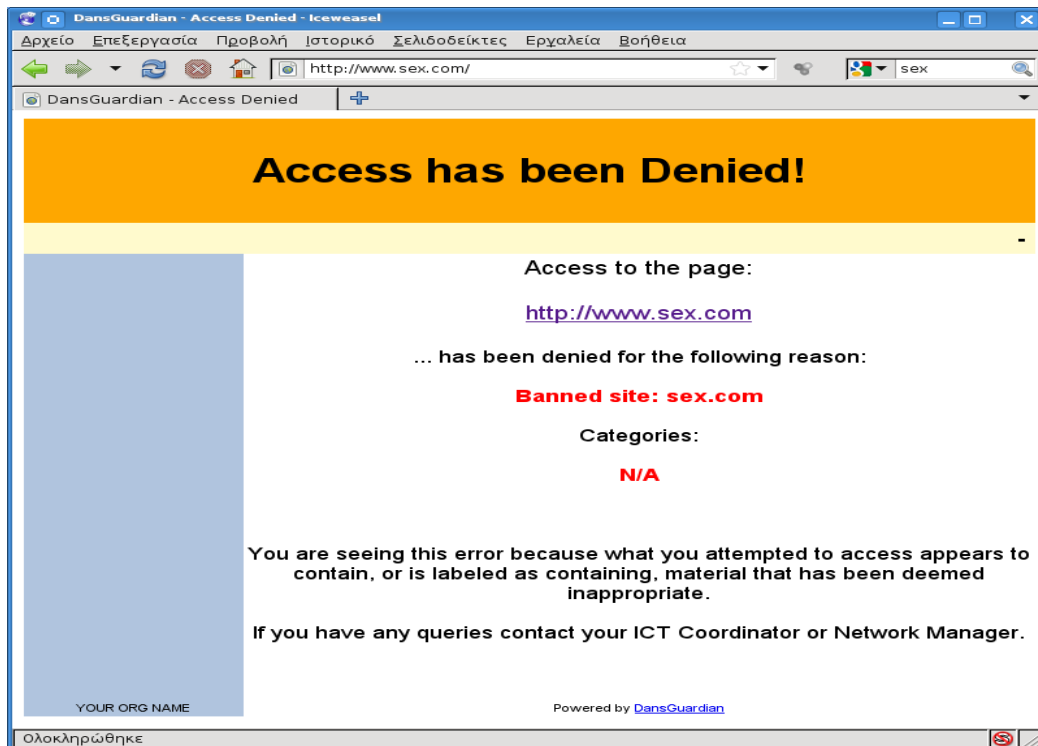
(Click To See Description Of Module Enhancements Since Previous Version)

Τέλος, εκτός από τη δυνατότητα έλεγχου της εκκίνησης, επανεκκίνησης και τερματισμού της υπηρεσίας, επιλέγοντας το “Analyze Logfiles”, παρέχεται η δυνατότητα προβολής και ανάλυσης του αρχείου καταγραφής των συνδέσεων και ιστοσελίδων που ζητήθηκαν από τους χρήστες καθώς και το είδος του φιλτραρίσματος που διενεργήθηκε σε αυτές.

Μετά την ολοκλήρωση της εγκατάστασης και της ρύθμισής του, για να λειτουργήσει το DansGaurdian ως “transparent proxy” καθολικά σε όλη την κίνηση web δεδομένων από και προς τους χρήστες του VPN, θα πρέπει επίσης να ρυθμιστεί κατάλληλα, το firewall στον server. Ποίο συγκεκριμένα στον host του Linux Virtual Server με την παρακάτω εντολή,

```
# iptables -A PREROUTING -p tcp -t nat -j REDIRECT --dport 80 --to-ports 1194
```

Έτσι όλα τα πακέτα που φτάνουν στον OpenVPN server από τους OpenVPN clients έχοντας προορισμό την port 80 (την εξ' ορισμού θύρα επικοινωνίας του πρωτοκόλλου "http" για την παροχή ιστοσελίδων) αναδρομολογούνται στην port 1194, στην οποία έχει οριστεί να δέχεται συνδέσεις το DansGuardian. Με αυτό τον τρόπο φιλτράρει τα δεδομένα πριν τα προωθήσει στους client, των οποίων οι χρήστες δεν χρειάζεται να κάνουν καμία ρύθμιση στον web browser που χρησιμοποιούν. Το φίλτρο ελέγχει για ιούς, ολόκληρη την Web κίνηση και απαγορεύει την πρόσβαση στις ιστοσελίδες, που εμπίπτουν σε κάποιον από τους κανόνες φιλτραρίσματός του, ενημερώνοντας τους χρήστες, με μια σελίδα που περιλαμβάνει τις σχετικές με την απαγόρευση αυτή πληροφορίες.



9 ΚΕΦΑΛΑΙΟ 9- Δοκιμές Απόδοσης (Benchmarks)

Σε αυτό το κεφάλαιο, παρουσιάζονται τ' αποτελέσματα των δοκιμών απόδοσης, που διενεργήθηκαν στο OpenVPN σύστημα του Τμήματος Πληροφορικής, σύμφωνα με τα RFC (1242, 2330, 2889, 3511) που προσδιορίζουν τα χαρακτηριστικά των κριτηρίων απόδοσης ενός δικτύου. Το βασικότερο χαρακτηριστικό που μετρήθηκε είναι ο ρυθμός διαμεταγωγής δεδομένων (throughput) και το (jitter).

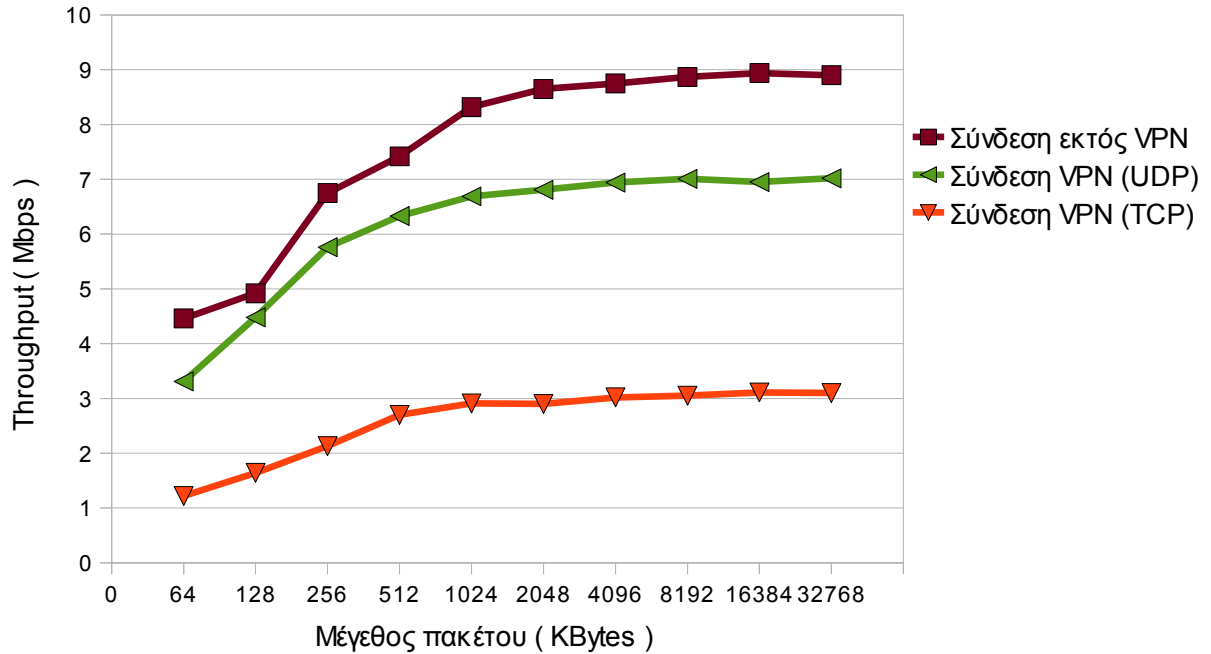
Το throughput είναι ο λόγος του συνολικού μεγέθους των δεδομένων που μεταφέρθηκαν σε ένα συγκεκριμένο χρονικό διάστημα, προς το διάστημα αυτό, μετρούμενος στο επίπεδο εφαρμογής, ενώ το jitter αποτελεί τη μέση τιμή της χρονικής καθυστέρησης κατά την μεταφορά των δεδομένων.

Για τις μετρήσεις αυτές χρησιμοποιήθηκε το “Iperf”, ένα διαδεδομένο πρόγραμμα μετρήσεως της απόδοσης δικτύων, που έχει το πλεονέκτημα, ότι παράγει μόνο του τα πακέτα που αποστέλλει κατά τη διάρκεια των δοκιμών. Γι' αυτό το λόγο, δεν δημιουργούνται κατά τη μέτρηση καθυστερήσεις από το δίσκο ή άλλο περιφερειακό του συστήματος.

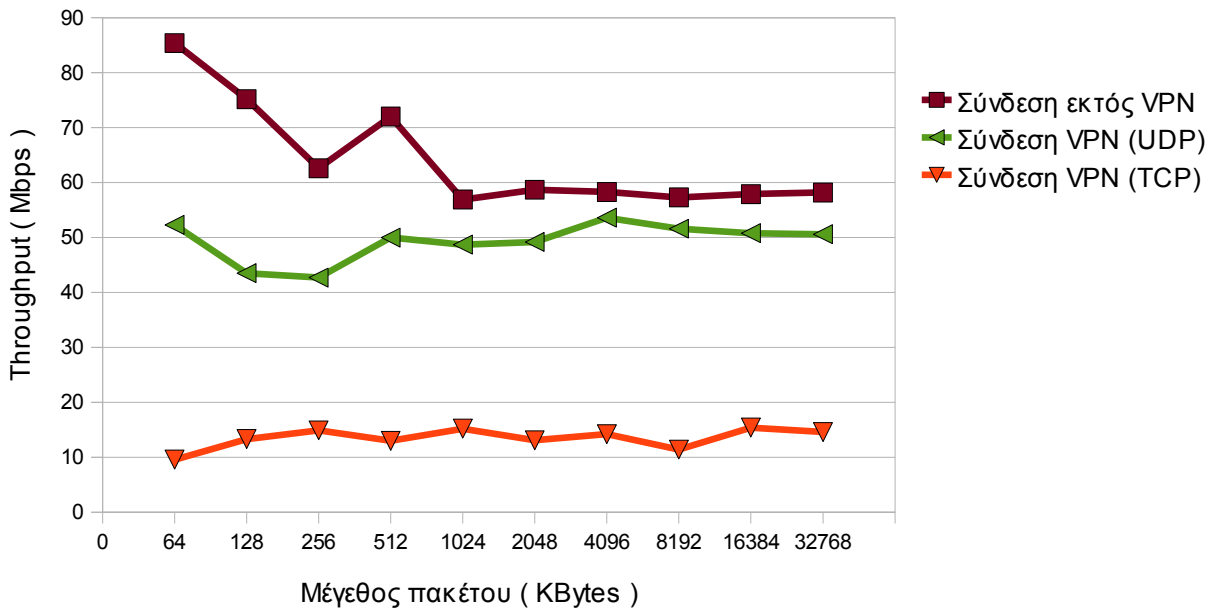
Οι μετρήσεις έγιναν σε πραγματικές συνθήκες λειτουργίας του συστήματος, και από τα τρία διαφορετικά σημεία πρόσβασης στο δίκτυο και σύνδεσης με τον OpenVPN server. (Μέσω DSL πρόσβασης “12Mbps Upload / 1Mbps Download”, Ασύρματου WLAN “48Mbps” και του τοπικού δικτύου LAN “100Mbps” του Τμήματος Πληροφορικής).

Τα χαρακτηριστικά και παράμετροι που διαφοροποιούνταν στις μετρήσεις αυτές ήταν, το είδος του πρωτοκόλλου επικοινωνίας (TCP ή UDP.) πάνω στο οποίο υλοποιήθηκαν οι VPN συνδέσεις και οι κρυπτογραφικοί αλγόριθμοι (ο εξορισμού “BF-CBC”, ο λιγότερο ισχυρός “DES-CBC” και ο ισχυρότερος “AES-256-CBC”), που αποτελούν την κύρια αιτία φόρτου “overhead” κατά την μεταφορά των δεδομένων μέσω των VPN συνδέσεων.

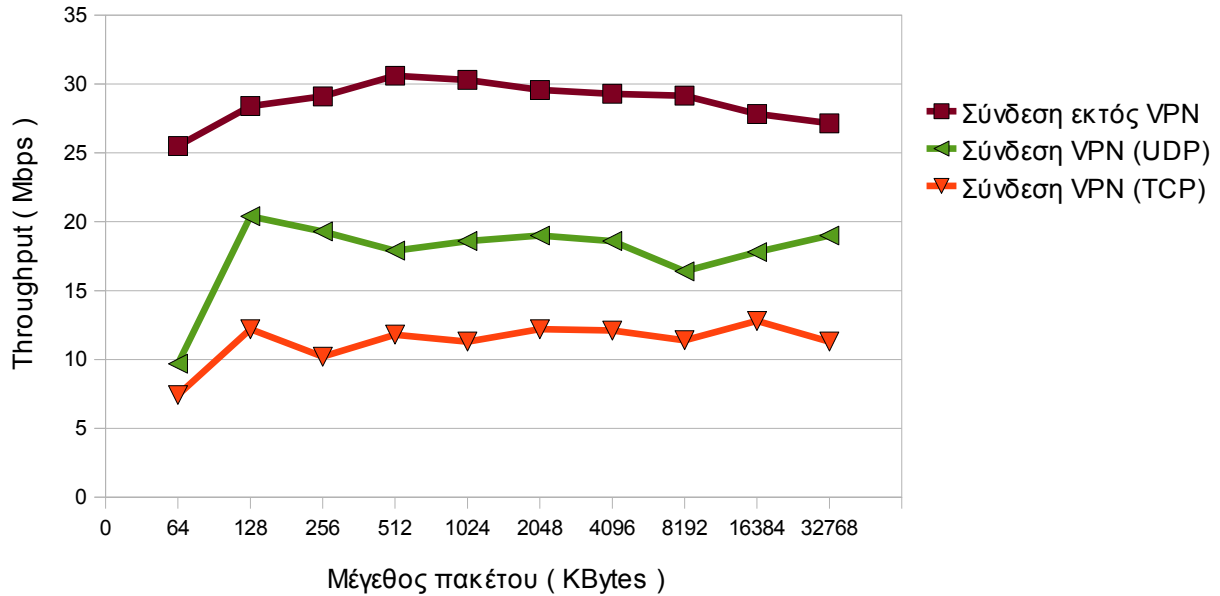
Σχήμα 18 : Διάγραμμα Throughput Μέσω DSL πρόσβασης



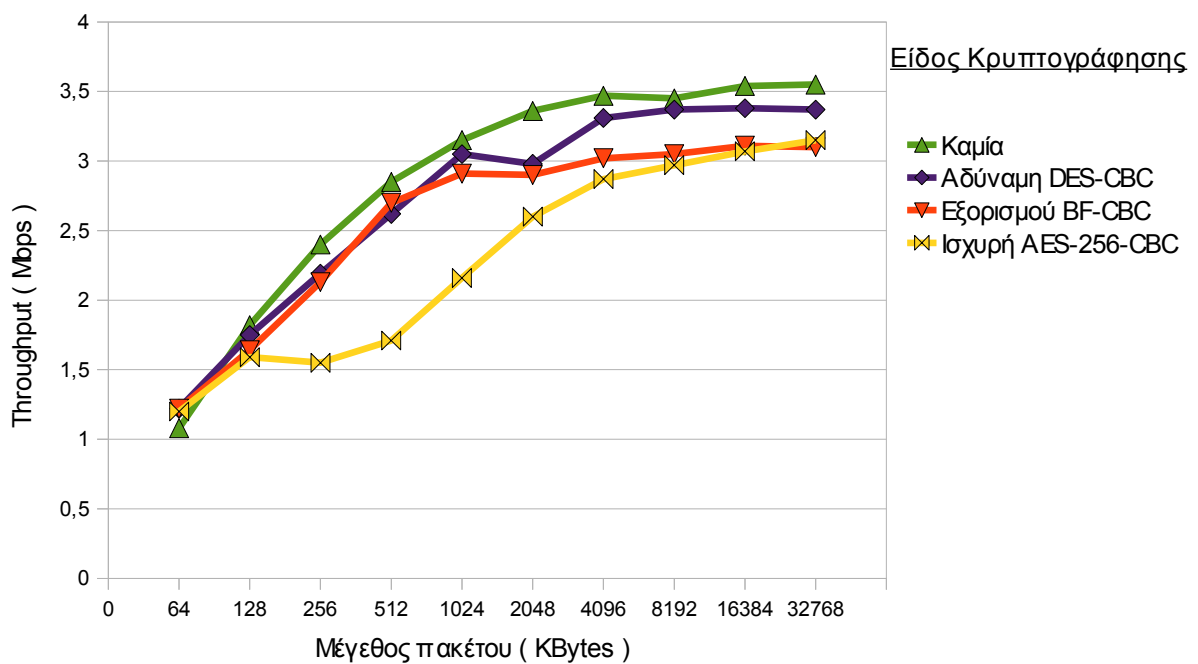
Σχήμα 19 : Διάγραμμα Throughput Μέσω LAN πρόσβασης



Σχήμα 20 : Διάγραμμα Throughput Μέσω WLAN πρόσβασης

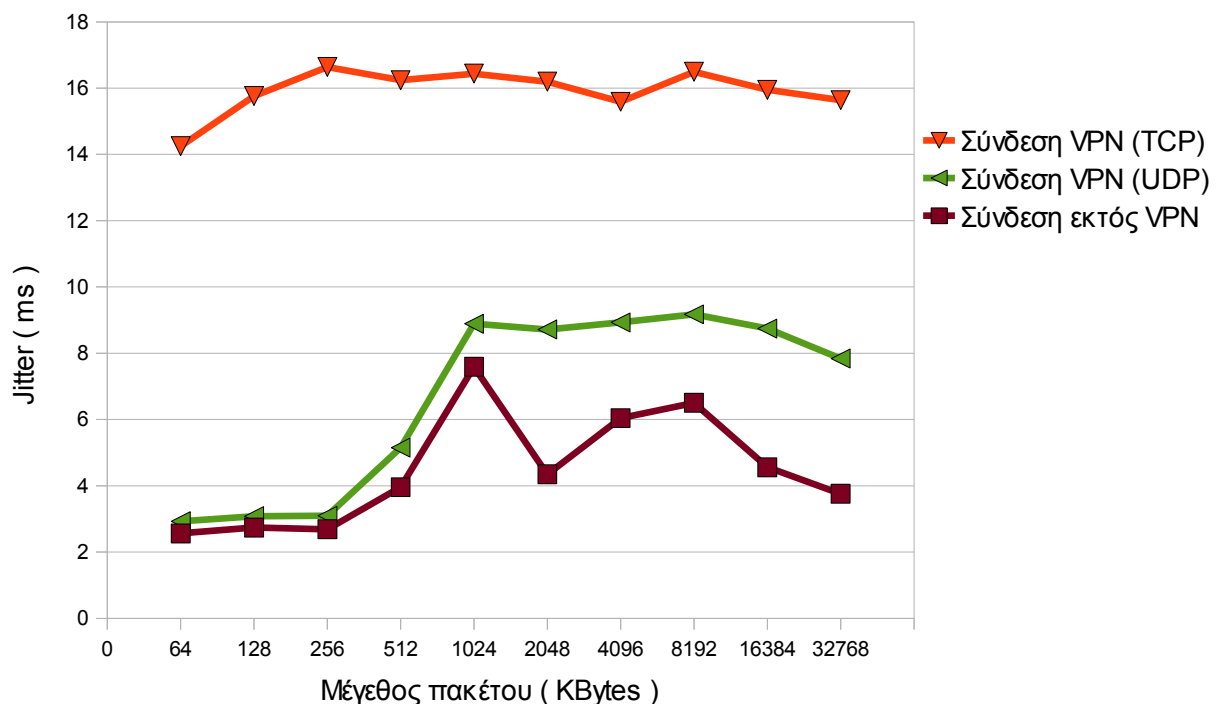


Σχήμα 21 : Διάγραμμα Throughput με διαφορετικές κρυπτογραφήσεις (Για VPN συνδέσεις μέσω TCP και DSL πρόσβασης)

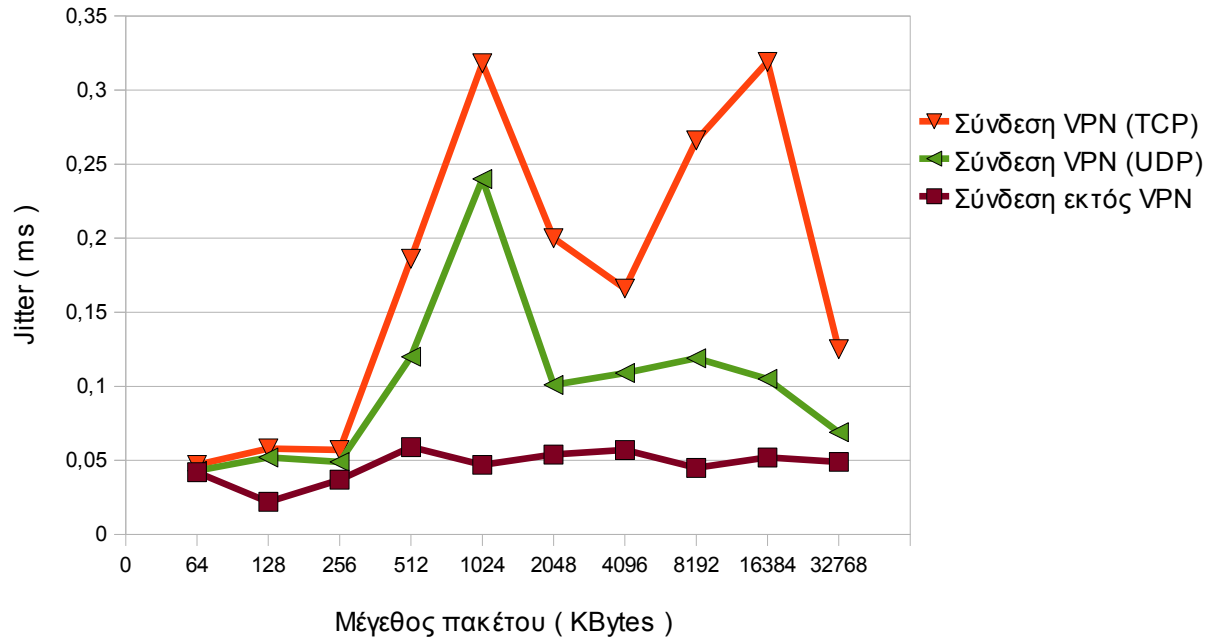


Βασιζόμενοι στη μελέτη των διαγραμμάτων που δημιουργήθηκαν από τα αποτελέσματα των διαφόρων δοκιμών και των μετρήσεων που έγιναν παρατηρείται, όπως ήταν αναμενόμενο, μείωση του ρυθμού διαμεταγωγής δεδομένων μέσω των VPN συνδέσεων σε σχέση με τις αντίστοιχες εκτός VPN συνδέσεις. Ιδιαίτερως μεγάλη είναι η διαφορά μεταξύ των UDP έναντι των TCP VPN συνδέσεων και χαρακτηριστική είναι η διαφοροποίηση του throughput εν αντιστοιχία με τους εκάστοτε κρυπτογραφικούς αλγόριθμους που χρησιμοποιήθηκαν. Παρόμοιες είναι και οι διαφοροποιήσεις των μετρήσεων του jitter, που έδειξαν ότι αυξάνετε στις VPN συνδέσεις σε σχέση με τις εκτός VPN συνδέσεις.

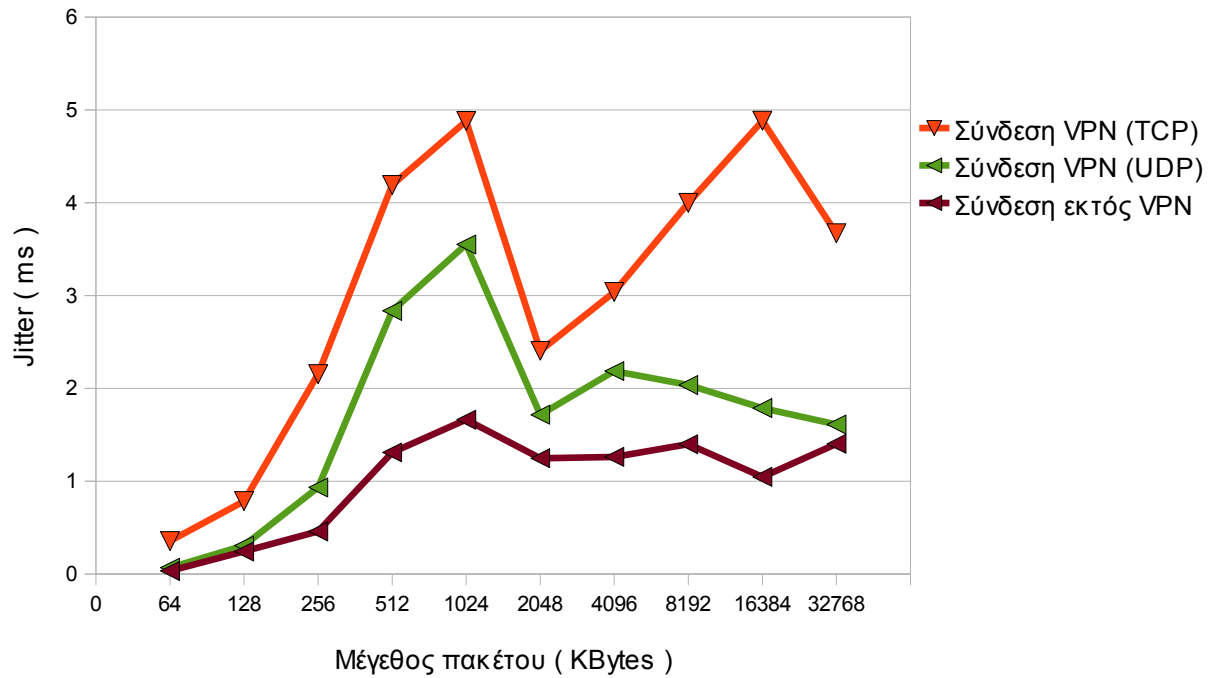
Σχήμα 22 : Διάγραμμα Jitter Μέσω DSL πρόσβασης



Σχήμα 23 : Διάγραμμα Jitter Μέσω LAN πρόσβασης



Σχήμα 24 : Διάγραμμα Jitter Μέσω WLAN πρόσβασης



10 ΚΕΦΑΛΑΙΟ 10- Προτάσεις - Συμπεράσματα

Η παρούσα πτυχιακή εργασία ασχολήθηκε με τη δημιουργία υπηρεσίας VPN για το Τμήμα Πληροφορικής. Αρχικά έγινε μία αναφορά στις διάφορες τεχνολογίες Εικονικών Ιδιωτικών Δικτύων που υπάρχουν, την εξέλιξη που είχαν και τα βασικά τους χαρακτηριστικά.

Έπειτα ασχολήθηκε με την δημιουργία μια μεθοδολογίας βάση της οποίας μπορεί κάποιος να εγκαταστήσει και να διαχειριστεί ένα VPN “server – client” σύστημα για το Τμήμα Πληροφορικής και παρουσίασή της ως οδηγού χρήσης. Τέλος αφορά τους τρόπους με τους οποίους μπορεί κάποιος να συνδεθεί μέσω του VPN στο δίκτυο του Τμήματος Πληροφορικής ανεξαρτήτως του λειτουργικού συστήματος που διαθέτει, βασιζόμενος στην εφαρμογή ανοιχτού κώδικα “OpenVPN”. Μια πρόταση, που υλοποιήθηκε είναι δημιουργία μιας υπηρεσίας “Ασφαλούς Σερφαρίσματος” μέσω του συνδυασμού της τεχνολογίας VPN κι ενός “Φίλτρο ελέγχου περιεχομένων” ιστοσελίδων.

Μια πρόταση που θα μπορούσε να γίνει, είναι να δοθεί η δυνατότητα ασφαλούς σύνδεσης και παροχής πρόσβασης στο Internet, με τη χρήση της υπηρεσίας VPN του Τμήματος Πληροφορικής, στους σπουδαστές και το προσωπικό του Τμήματος Πληροφορικής που έχουν πρόσβαση στο Ασύρματο Μητροπολιτικό Δίκτυο Θεσσαλονίκης μέσω του κόμβου του ΤΕΙ Θεσσαλονίκης που υπάρχει σε αυτό.

Τέλος, τα συμπεράσματα που εξήχθησαν για τη χρήση του VPN βάση των δοκιμών που έγιναν είναι ότι, η “ταχύτητα σύνδεσης” μέσω VPN υστερεί σημαντικά σε σύγκριση με μια εκτός VPN, πράγμα που επηρεάζεται από το πρωτόκολλο πάνω στο οποίο βασίζεται η εφαρμογή για να δημιουργήσει την σύνδεση (TCP – UDP) και το είδος της κρυπτογράφησης που χρησιμοποιείται για την διασφάλιση του καναλιού επικοινωνίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Αλεξόπουλος, Α., & Λογογιάννης, Γ. (2003). *Τηλεπικοινωνίες και Δίκτυα Υπολογιστών*. Αθήνα:
- [2] Παγκάλου, Γ., & Μαυρίδη, Ι. (2002). *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων*. Εκδόσεις Ανίκουλα.
- [3] Doraswamy, N., & Harkins, D. (1999). *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Prentice Hall PTR. NJ, USA: Upper Saddle River.
- [4] Douglas, C. E. *Διαδίκτυα με TCP/IP Αρχές, Πρωτόκολλα και Αρχιτεκτονικές Τόμος 1*. Εκδόσεις Κλειδάριθμος (4η Αμερικάνικη έκδοση).
- [5] Feilner, M. (April 2006). *OpenVPN Building and Integrating Virtual Private Networks*. BIRMINGHAM - MUMBAI: Packt Publishing
- [6] Kosiur, D. (1998). *Building and Managing Virtual Private Networks*. John Wiley & Sons.
- [7] Scott, C., Wolfe, P., & Erwin, M. (1999). *Virtual Private Networks – Second Edition*. O'Reilly.
- Request For Comments**
- [8] Atkinson, R. (aug 1995). *IP Authentication Header*. RFC 1826: IETF.
- [9] Atkinson, R. (aug 1995). *IP Encapsulating Security Payload (ESP)*. RFC 1827: IETF.
- [10] Atkinson, R. (aug 1995). *Security Architecture for the Internet Protocol*. RFC 1825: IETF.

[11] Bradner, S. (jul 1991). *Benchmarking Terminology for Network Interconnection Devices*. RFC 1242: IETF.

[12] Glenn, R., & Kent, S. (nov 1998). *The NULL Encryption Algorithm and Its Use With IPsec*. RFC 2410: IETF.

[13] Hanks, S., Li, T., Farinacci, D., & Traina, P. (oct 1994). *Generic Routing Encapsulation (GRE)*. RFC 1701: IETF.

[14] Hanks, S., Li, T., Farinacci, D., & Traina, P. (oct 1994). *Generic Routing Encapsulation over IPv4 networks*. RFC 1702: IETF.

[15] Harkins, D., & Carrel, D. (nov 1998). *The Internet Key Exchange (IKE)*. RFC 2409: IETF.

[16] Hickman, B., Newman, D., Tadjudin, S., & Martin, T. (apr 2003). *Benchmarking Methodology for Firewall Performance*. RFC 3511: IETF.

[17] Hoffman, P. (dec 2005). *Cryptographic Suites for IPsec*. RFC 4308: IETF

[18] Karn, P., Metzger, P., & Simpson, W. (aug 1995). *The ESP DES-CBC Transform*. RFC 1829: IETF.

[19] Kent, S., & Atkinson, R. (nov 1998). *IP Authentication Header*. RFC 2402: IETF.

[20] Kent, S., & Atkinson, R. (nov 1998). *IP Encapsulating Security Payload (ESP)*. RFC 2406: IETF.

[21] Kent, S., & Atkinson, R. (nov 1998). *Security Architecture for the Internet Protocol*. RFC 2401: IETF.

[22] Madson, C., & Doraswamy, N. (nov 1998). *The ESP DES-CBC Cipher*

Algorithm With Explicit IV. RFC 2405: IETF.

[23] Madson, C., & Glenn, R. (nov 1998). *The Use of HMAC-MD5-96 within ESP and AH*. RFC 2403: IETF.

[24] Madson, C., & Glenn, R. (nov 1998). *The Use of HMAC-SHA-1-96 within ESP and AH*. RFC 2404: IETF.

[25] Mandeville, R., & Perser, J. (aug 2000). *Benchmarking Methodology for LAN Switching Devices*. RFC 2889: IETF.

[26] Maughan, D., Schertler, M., Schneider, M., & Turner, J. (nov 1998). *Internet Security Association and Key Management Protocol (ISAKMP)*. RFC 2408: IETF.

[27] Metzger, P., & Simpson, W. (aug 1995). *IP Authentication using Keyed MD5*. RFC 1828: IETF.

[28] Orman, H. (nov 1998). *The OAKLEY Key Determination Protocol*. RFC 2412: IETF.

[29] Paxson, V., Almes, G., Mahdavi, J., & Mathis, M. (may 1998). *Framework for IP Performance Metrics*. RFC 2330: IETF.

[30] Pereira, R., & Adams, R. (nov 1998). *The ESP CBC-Mode Cipher Algorithms*. RFC 2451: IETF.

[31] Piper, D. (nov 1998). *The Internet IP Security Domain of Interpretation for ISAKMP*. RFC 2407: IETF.

[32] Schiller, J. (dec 2005). *Cryptographic Algorithms for Use in the Internet Key Exchange Version*. RFC 4307: IETF.

[33] Simpson, P. (jul 1994). *The Point-to-Point Protocol (PPP)*. RFC 1661: IETF.

[34] Simpson, W. (Oct.1995). *IP in IP Tunneling* . RFC 1853: IETF.

[35] Thayer, R., Doraswamy, N., & Glenn, R. (nov 1998). *IP Security Document Roadmap*. RFC 2411: IETF.

[36] Zweig, J., & Partridge, C. (feb 1990). *TCP alternate checksum options*. RFC 1145: IETF.

Ιστοσελίδες

[37] *DansGuardian - True Web Content Filtering for All*. Retrieved February 2, 2010, from : <http://dansguardian.org/>

[38] *Expect - Wikipedia, the free encyclopedia*:. Retrieved January 29, , from : <http://en.wikipedia.org/wiki/Expect>

[39] Sundman, M. *GUI for Windows*. Retrieved January 17, 2010, from : <http://openvpn.se/>

[40] *Internet Engineering Task Force*. Retrieved January 13, 2010, from : <http://www.ietf.org/>

[41] *Iperf - Wikipedia, the free encyclopedia*:. Retrieved January 19, 2010, from : <http://en.wikipedia.org/wiki/Iperf>

[42] *Iperf*. Retrieved February 5, 2010, from : <http://en.wikipedia.org/wiki/Iperf>

[43] *NSIS Wiki*. Retrieved January 25, , from : http://nsis.sourceforge.net/Main_Page

[44] *OpenVPN for PocketPC*. Retrieved January 24, 2010, from : <http://ovpnppc.ziggurat29.com/ovpnppc-main.htm>

[45] *SourceForge.net:OpenVPN Control - Project Web Hosting - Open Source Software*. Retrieved February 3, 2010, from : <http://openvpn-control.sourceforge.net/>

[46] *tunnelblick - Project Hosting on Code*. Retrieved January 23, 2010, from : <http://code.google.com/p/tunnelblick/>

[47] *Virtual private network - Wikipedia, the free encyclopedia*:. Retrieved January 15, 2010, from : http://en.wikipedia.org/wiki/Virtual_private_network

[48] *VPN Labs - VIRTUAL PRIVATE NETWORKS - Free VPN Software and Virtual Private Network News*. Retrieved January 20, 2010, from : <http://www.vpnlabs.com/>

[49] *Webmin*. Retrieved January 17, 2010, from : <http://www.webmin.com/>

[50] *Debian -- Το διεθνές λειτουργικό σύστημα*. Retrieved January 15, 2010, from : <http://www.debian.org/>

[51] Fsf, (2010). *The GNU Operating System*. Retrieved January 14, 2010, from : <http://www.gnu.org/>

[52] Iso - International Organization For, (2010). *International Organization for Standardization*. Retrieved January 20, 2010, from : <http://www.iso.org/iso/home.html>

[53] *The GNU Operating System*. Retrieved January 14, 2010, from <http://www.gnu.org/>

[54] Torvalds, L. *The Linux Kernel Archives*. Retrieved January 19, 2010, from <http://www.kernel.org/>

[55] *URLBlacklist.com*. Retrieved January 16, 2010, from <http://urlblacklist.com/>

[56] Yonan, J. *OpenVPN - Open Source VPN*. Retrieved January 19, 2010, from : <http://openvpn.net/>

ΠΑΡΑΡΤΗΜΑ

openvpn-gui.nsi

```

; *****
; * Copyright (C) 2002-2006 OpenVPN Solutions LLC *
; * 2004-2006 Updated by Mathias Sundman <mathias@openvpn.se> *
; * This program is free software; you can redistribute it and/or modify *
; * it under the terms of the GNU General Public License as published by *
; * the Free Software Foundation; either version 2 of the License, or *
; * (at your option) any later version. *
; *****
; Modified by ddimarx for openvpn.it.teithe.gr
; *****
; OpenVPN install script for Windows, using NSIS

!include "MUI.nsh"
!include "setpath.nsi"

!define HOME "openvpn"
!define BIN "${HOME}\bin"

!define PRODUCT_NAME "OpenVPN"
!define OPENVPN_VERSION "2.1.1"
!define GUI_VERSION "1.0.3"
!define MYCERT_VERSION "0.3.2b"
!define VERSION "it-${OPENVPN_VERSION}-gui-${GUI_VERSION}"

!define TAP "tap0901"
!define TAPDRV "${TAP}.sys"

!define TAPCAT "${TAP}.cat"

; something like "-DBG2"
!define OUTFILE_LABEL ""

; Default OpenVPN Service registry settings
!define SERV_CONFIG_DIR "$INSTDIR\config"
!define SERV_CONFIG_EXT "ovpn"
!define SERV_EXE_PATH "$INSTDIR\bin\openvpn.exe"
!define SERV_LOG_DIR "$INSTDIR\log"
!define SERV_PRIORITY "NORMAL_PRIORITY_CLASS"
!define SERV_LOG_APPEND "0"

; Default OpenVPN GUI registry settings
!define GUI_CONFIG_DIR "$INSTDIR\config"
!define GUI_CONFIG_EXT "ovpn"
!define GUI_EXE_PATH "$INSTDIR\bin\openvpn.exe"
!define GUI_LOG_DIR "$INSTDIR\log"
!define GUI_PRIORITY "NORMAL_PRIORITY_CLASS"
!define GUI_LOG_APPEND "0"
!define GUI_ALLOW_EDIT "1"
!define GUI_ALLOW_SERVICE "0"

```

```

!define GUI_ALLOW_PROXY "1"
!define GUI_ALLOW_PASSWORD "1"
!define GUI_SERVICE_ONLY "0"
!define GUI_PSW_ATTÉMPTS "3"
!define GUI_UP_TIMEOUT "15"
!define GUI_DOWN_TIMEOUT "10"
!define GUI_PRE_TIMEOUT "10"
!define GUI_SHOW_BALLOON "1"
!define GUI_SHOW_SCRIPT "1"
!define GUI_LOG_VIEWER "$WINDIR\notepad.exe"
!define GUI_EDITOR "$WINDIR\notepad.exe"
!define GUI_SUSPEND "1"
!define GUI_SILENT_CONN "0"

;-----
;Configuration

;General

OutFile "openvpn-${VERSION}${OUTFILE_LABEL}-install.exe"

SetCompressor bzip2

ShowInstDetails show
ShowUninstDetails show

;Folder selection page
InstallDir "$PROGRAMFILES\${PRODUCT_NAME}"

;Remember install folder
InstallDirRegKey HKCU "Software\${PRODUCT_NAME}" ""

!define SOURCE_ZIP_DEST "openvpn-${OPENVPN_VERSION}.zip"
!define SOURCE_ZIP_SRC "${HOME}\${SOURCE_ZIP_DEST}"

!define GUI_SOURCE_ZIP_DEST "openvpn-gui-${GUI_VERSION}.zip"
!define GUI_SOURCE_ZIP_SRC "${HOME}\${GUI_SOURCE_ZIP_DEST}"

!define MYCERT_SOURCE_ZIP_DEST "mycert-src-${MYCERT_VERSION}.zip"
!define MYCERT_SOURCE_ZIP_SRC "${HOME}\mycertwizard\${MYCERT_SOURCE_ZIP_DEST}"

# For testing only
#!define SOURCE_ZIP_SRC "c:\src\openvpn\install-win32\null.zip"

;-----
;Modern UI Configuration

Name "${PRODUCT_NAME} ${VERSION}"

!define MUI_COMPONENTSPAGE_SMALLDESC
!define MUI_FINISHPAGE_SHOWREADME "$INSTDIR\INSTALL-win32.txt"
!define MUI_FINISHPAGE_NOAUTOCLOSE

!define MUI_FINISHPAGE_SHOWREADME_NOTCHECKED
#!define MUI_FINISHPAGE_SHOWREADME_CHECKED
!define MUI_ABORTWARNING
!define MUI_ICON "${HOME}\install-win32\openvpn.ico"

```



```

!define MUI_UNICON "${HOME}\install-win32\openvpn.ico"
!define MUI_HEADERIMAGE

!define MUI_HEADERIMAGE_BITMAP "${HOME}\install-win32\vpn-tei.bmp"
!define MUI_UNFINISHPAGE_NOAUTOCLOSE

!define MUI_WELCOMEPAGE_TITLE "Welcome to the ${PRODUCT_NAME} Setup Wizard"

!define MUI_WELCOMEPAGE_TEXT "This wizard will guide you through the
installation of:\r\n\r\nOpenVPN - an Open Source VPN package by James
Yonan.\r\n\r\nOpenVPN GUI - A Graphical User Interface for OpenVPN by Mathias
Sundman\r\n\r\nMy Certificate Wizard - A tool to create a certificate request by
Vlada Macek\r\n\r\nNote that the Windows version of OpenVPN will only run on Win
2000, XP, or higher.\r\n\r\n\r\n"

!define MUI_COMPONENTSPAGE_TEXT_TOP "Select the components to install/upgrade.
Stop any OpenVPN or OpenVPN GUI processes or the OpenVPN service if it is
running."

!insertmacro MUI_PAGE_WELCOME
!insertmacro MUI_PAGE_LICENSE "${HOME}\install-win32\license.txt"
!insertmacro MUI_PAGE_COMPONENTS
!insertmacro MUI_PAGE_DIRECTORY
!insertmacro MUI_PAGE_INSTFILES
!insertmacro MUI_PAGE_FINISH

!insertmacro MUI_UNPAGE_CONFIRM
!insertmacro MUI_UNPAGE_INSTFILES
!insertmacro MUI_UNPAGE_FINISH

;-----
;Languages

!insertmacro MUI_LANGUAGE "English"

;-----
;Language Strings

LangString DESC_SecOpenVPNUserSpace ${LANG_ENGLISH} "Install OpenVPN user-space
components, including openvpn.exe."

LangString DESC_SecOpenVPNEasyRSA ${LANG_ENGLISH} "Install OpenVPN RSA scripts
for X509 certificate management."

LangString DESC_SecOpenSSLDLLs ${LANG_ENGLISH} "Install OpenSSL DLLs locally
(may be omitted if DLLs are already installed globally)."

LangString DESC_SecTAP ${LANG_ENGLISH} "Install/Upgrade the TAP-Win32 virtual
device driver. Will not interfere with CIPE."

LangString DESC_SecTAPHidden ${LANG_ENGLISH} "Install the TAP device as hidden.
The TAP device will not be visible under Network Connections."

LangString DESC_SecService ${LANG_ENGLISH} "Install the OpenVPN service wrapper
(openvpnserv.exe)"

LangString DESC_SecOpenSSLUtilities ${LANG_ENGLISH} "Install the OpenSSL

```

```

Utilities (used for generating public/private key pairs).
; LangString DESC_SecOpenVPNSource ${LANG_ENGLISH} "Install (but do not unzip)
the source code zip files."

LangString DESC_SecAddPath ${LANG_ENGLISH} "Add OpenVPN executable directory to
the current user's PATH."

LangString DESC_SecAddShortcuts ${LANG_ENGLISH} "Add shortcuts to the current
user's Start Menu and Desktop"

LangString DESC_SecFileAssociation ${LANG_ENGLISH} "Register OpenVPN config
file association (*.${SERV_CONFIG_EXT})"

LangString DESC_SecGUI ${LANG_ENGLISH} "Install OpenVPN GUI (A System tray
application to control OpenVPN)"

LangString DESC_SecGUIAuto ${LANG_ENGLISH} "Automatically start OpenVPN GUI at
system startup"

LangString DESC_SecMYCERT ${LANG_ENGLISH} "Install My Certificate Wizard - A
tool to create a certificate request."
;-----
;Data

; LicenseData "${HOME}\install-win32\license.txt"

;-----
;Reserve Files

;Things that need to be extracted on first (keep these lines before any File
command!)
;Only useful for BZIP2 compression

ReserveFile "${HOME}\install-win32\vpn-tei.bmp"

;-----
;Macros

!macro WriteRegStringIfUndef ROOT SUBKEY KEY VALUE
Push $R0
ReadRegStr $R0 "${ROOT}" "${SUBKEY}" "${KEY}"
StrCmp $R0 "" +1 +2
WriteRegStr "${ROOT}" "${SUBKEY}" "${KEY}" "${VALUE}'
Pop $R0
!macroend

!macro DelRegStringIfUnchanged ROOT SUBKEY KEY VALUE
Push $R0
ReadRegStr $R0 "${ROOT}" "${SUBKEY}" "${KEY}"
StrCmp $R0 "${VALUE}' +1 +2
DeleteRegValue "${ROOT}" "${SUBKEY}" "${KEY}"
Pop $R0
!macroend

!macro DelRegKeyIfUnchanged ROOT SUBKEY VALUE

```

```

Push $R0
ReadRegStr $R0 "${ROOT}" "${SUBKEY}" ""
StrCmp $R0 '${VALUE}' +1 +2
DeleteRegKey "${ROOT}" "${SUBKEY}"
Pop $R0
!macroend

!macro DelRegKeyIfEmpty ROOT SUBKEY
Push $R0
EnumRegValue $R0 "${ROOT}" "${SUBKEY}" 1
StrCmp $R0 "" +1 +2
DeleteRegKey /ifempty "${ROOT}" "${SUBKEY}"
Pop $R0
!macroend

;-----
;Set reboot flag based on tapinstall return

Function CheckReboot
  IntCmp $R0 1 "" noreboot noreboot
  IntOp $R0 0 & 0
  SetRebootFlag true
  DetailPrint "REBOOT flag set"
noreboot:
FunctionEnd

;-----
;Installer Sections

#!define SF_SELECTED 1
#!define SF_R0 16
!define SF_NOT_R0 0xFFFFFFFF

Section "OpenVPN User-Space Components" SecOpenVPNUserSpace

  SetOverwrite on
  SetOutPath "$INSTDIR\bin"

  File "${HOME}\openvpn.exe"

SectionEnd

Section "OpenVPN RSA Certificate Management Scripts" SecOpenVPNEasyRSA

  SetOverwrite on
  SetOutPath "$INSTDIR\easy-rsa"

  File "${HOME}\easy-rsa\openssl.cnf.sample"
  File "${HOME}\easy-rsa\vars.bat.sample"

  File "${HOME}\easy-rsa\init-config.bat"

  File "${HOME}\easy-rsa\README.txt"
  File "${HOME}\easy-rsa\build-ca.bat"
  File "${HOME}\easy-rsa\build-dh.bat"
  File "${HOME}\easy-rsa\build-key-server.bat"
  File "${HOME}\easy-rsa\build-key.bat"

```

```
File "${HOME}\easy-rsa\build-key-pkcs12.bat"
File "${HOME}\easy-rsa\clean-all.bat"
File "${HOME}\easy-rsa\index.txt.start"
File "${HOME}\easy-rsa\revoke-full.bat"
File "${HOME}\easy-rsa\serial.start"

SectionEnd

Section "OpenVPN GUI" SecGUI

SetOverwrite on
SetOutPath "$INSDIR\bin"
File "${HOME}\openvpn-gui.exe"

# Include your custom config file(s) here.
SetOutPath "$INSDIR\config"
File "${HOME}\config\openvpn-teithe-client.ovpn"

SetOutPath "$INSDIR\config"
File "${HOME}\config\ta.key"
File "${HOME}\config\ca.crt"

SetOutPath "$INSDIR"
File "${HOME}\install-win32\OpenVPN GUI ReadMe.txt"

CreateDirectory "$INSDIR\log"
CreateDirectory "$INSDIR\config"

SectionEnd

Section "AutoStart OpenVPN GUI" SecGUIAuto
SectionEnd

Section "My Certificate Wizard" SecMYCERT

SetOverwrite on
SetOutPath "$INSDIR\bin"
File "${HOME}\mycertwizard\mycert.exe"
File "${HOME}\mycertwizard\mycert.ini"

SectionEnd

Section "Hide the TAP-Win32 Virtual Ethernet Adapter" SecTAPHidden
SectionEnd

Section "OpenVPN Service" SecService

SetOverwrite on

SetOutPath "$INSDIR\bin"
File "${HOME}\service-win32\openvpnserv.exe"

FileOpen $R0 "$INSDIR\config\README.txt" w
FileWrite $R0 "This directory should contain OpenVPN configuration files\r$\n"
FileWrite $R0 "each having an extension of .${SERV_CONFIG_EXT}\r$\n"
FileWrite $R0 "\r$\n"
```

```

FileWrite $R0 "When OpenVPN is started as a service, a separate OpenVPN$\r$\n"
FileWrite $R0 "process will be instantiated for each configuration file.$\r$\n"
FileClose $R0

SetOutPath "$INSTDIR\sample-config"
File "${HOME}\sample-config\sample.${SERV_CONFIG_EXT}"
File "${HOME}\sample-config\client.${SERV_CONFIG_EXT}"
File "${HOME}\sample-config\server.${SERV_CONFIG_EXT}"

CreateDirectory "$INSTDIR\log"
FileOpen $R0 "$INSTDIR\log\README.txt" w
FileWrite $R0 "This directory will contain the log files for OpenVPN$\r$\n"
FileWrite $R0 "sessions which are being run as a service.$\r$\n"
FileClose $R0

SectionEnd

Section "OpenVPN File Associations" SecFileAssociation
SectionEnd

Section "OpenSSL DLLs" SecOpenSSLDLLs

SetOverwrite on
SetOutPath "$INSTDIR\bin"
File "${BIN}\libeay32.dll"
File "${BIN}\libssl32.dll"

File "${BIN}\libpkcs11-helper-1.dll"

SectionEnd

Section "OpenSSL Utilities" SecOpenSSLUtilities

SetOverwrite on
SetOutPath "$INSTDIR\bin"
File "${BIN}\openssl.exe"

SectionEnd

Section "TAP-Win32 Virtual Ethernet Adapter" SectAP

SetOverwrite on

FileOpen $R0 "$INSTDIR\bin\addtap.bat" w
FileWrite $R0 "rem Add a new TAP-Win32 virtual ethernet adapter$\r$\n"
FileWrite $R0 '"$INSTDIR\bin\tapinstall.exe" install
"$INSTDIR\driver\OemWin2k.inf" ${TAP}$\r$\n'
FileWrite $R0 "pause$\r$\n"
FileClose $R0

FileOpen $R0 "$INSTDIR\bin\deltapall.bat" w
FileWrite $R0 "echo WARNING: this script will delete ALL TAP-Win32 virtual
adapters (use the device manager to delete adapters one at a time)$\r$\n"
FileWrite $R0 "pause$\r$\n"
FileWrite $R0 '"$INSTDIR\bin\tapinstall.exe" remove ${TAP}$\r$\n'
FileWrite $R0 "pause$\r$\n"

```

```

FileClose $R0

; Check if we are running on a 64 bit system.
System::Call "kernel32::GetCurrentProcess() i .s"
System::Call "kernel32::IsWow64Process(i s, *i .r0)"
IntCmp $0 0 tap-win32

DetailPrint "We are running on a 64-bit system."

SetOutPath "$INSTDIR\bin"
File "${HOME}\tap-win64\i386\tapinstall.exe"
SetOutPath "$INSTDIR\driver"
File "${HOME}\tap-win64\i386\${TAPDRV}"

File "${HOME}\tap-win64\i386\${TAPCAT}"

SectionGetFlags ${SecTAPHidden} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" nohiddentap64 nohiddentap64

File "${HOME}\tap-win64-hiddentap\i386\OemWin2k.inf"
goto end

nohiddentap64:
File "${HOME}\tap-win64\i386\OemWin2k.inf"

goto end

tap-win32:

DetailPrint "We are running on a 32-bit system."

SetOutPath "$INSTDIR\bin"
File "${HOME}\tap-win32\i386\tapinstall.exe"
SetOutPath "$INSTDIR\driver"
File "${HOME}\tap-win32\i386\${TAPDRV}"

File "${HOME}\tap-win32\i386\${TAPCAT}"

SectionGetFlags ${SecTAPHidden} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" nohiddentap32 nohiddentap32

File "${HOME}\tap-win32-hiddentap\i386\OemWin2k.inf"
goto end

nohiddentap32:
File "${HOME}\tap-win32\i386\OemWin2k.inf"

end:

SectionEnd

Section "Add OpenVPN to PATH" SecAddPath

; remove previously set path (if any)

```

```

Push "$INSTDIR\bin"
Call RemoveFromPath

; append our bin directory to end of current user path
Push "$INSTDIR\bin"
Call AddToPath

SectionEnd

Section "Add Shortcuts to Start Menu" SecAddShortcuts

SetOverwrite on
CreateDirectory "$SMPROGRAMS\OpenVPN"
CreateDirectory "$SMPROGRAMS\OpenVPN\Documentation"
CreateShortCut "$SMPROGRAMS\OpenVPN\Documentation\OpenVPN Win32 README.lnk"
"$INSTDIR\INSTALL-win32.txt" ""
WriteINIStr "$SMPROGRAMS\OpenVPN\Documentation\OpenVPN HOWTO.url"
"InternetShortcut" "URL" "http://openvpn.net/howto.html"
WriteINIStr "$SMPROGRAMS\OpenVPN\Documentation\OpenVPN Manual Page.url"
"InternetShortcut" "URL" "http://openvpn.net/man.html"
WriteINIStr "$SMPROGRAMS\OpenVPN\Documentation\OpenVPN Web Site.url"
"InternetShortcut" "URL" "http://openvpn.net/"
WriteINIStr "$SMPROGRAMS\OpenVPN\Documentation\OpenVPN Windows Notes.url"
"InternetShortcut" "URL" "http://openvpn.net/INSTALL-win32.html"
CreateShortCut "$SMPROGRAMS\OpenVPN\Uninstall OpenVPN.lnk"
"$INSTDIR\Uninstall.exe"

SectionGetFlags ${SecGUI} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" nogui nogui

CreateShortCut "$SMPROGRAMS\OpenVPN\OpenVPN GUI.lnk" "$INSTDIR\bin\openvpn-
gui.exe"
CreateShortCut "$SMPROGRAMS\OpenVPN\Documentation\OpenVPN GUI ReadMe.lnk"
"$INSTDIR\OpenVPN GUI ReadMe.txt"
CreateShortCut "$DESKTOP\OpenVPN GUI.lnk" "$INSTDIR\bin\openvpn-gui.exe"

nogui:

SectionGetFlags ${SecMYCERT} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" nomycert nomycert

CreateShortCut "$SMPROGRAMS\OpenVPN\My Certificate Wizard.lnk"
"$INSTDIR\bin\mycert.exe"

nomycert:

SectionEnd

;Section "Source Code" SecOpenVPNSource
;
; SetOverwrite on
; SetOutPath "$INSTDIR"
; File "${SOURCE_ZIP_SRC}"
;

```

```

; SectionGetFlags ${SecGUI} $R0
; IntOp $R0 $R0 & ${SF_SELECTED}
; IntCmp $R0 ${SF_SELECTED} "" nogui nogui
; File "${GUI_SOURCE_ZIP_SRC}"
;
; nogui:
; SectionGetFlags ${SecMYCERT} $R0
; IntOp $R0 $R0 & ${SF_SELECTED}
; IntCmp $R0 ${SF_SELECTED} "" nomycert nomycert
;
; File "${MYCERT_SOURCE_ZIP_SRC}"
;
; nomycert:
;
;SectionEnd

;-----
;Post-install section

Section -post

; delete old devcon.exe
Delete "$INSTDIR\bin\devcon.exe"

;
; install/upgrade TAP-Win32 driver if selected, using tapinstall.exe
;
SectionGetFlags ${SecTAP} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" notap notap
; TAP install/update was selected.
; Should we install or update?
; If tapinstall error occurred, $5 will
; be nonzero.
IntOp $5 0 & 0
nsExec::ExecToStack "$INSTDIR\bin\tapinstall.exe" hwids ${TAP}'
Pop $R0 # return value/error/timeout
IntOp $5 $5 | $R0
DetailPrint "tapinstall hwids returned: $R0"

; If tapinstall output string contains "${TAP}" we assume
; that TAP device has been previously installed,
; therefore we will update, not install.
Push "${TAP}"
Call StrStr
Pop $R0

IntCmp $5 0 "" tapinstall_check_error tapinstall_check_error
IntCmp $R0 -1 tapinstall

;tapupdate:
DetailPrint "TAP-Win32 UPDATE"
nsExec::ExecToLog "$INSTDIR\bin\tapinstall.exe" update
"$INSTDIR\driver\OemWin2k.inf" ${TAP}'
Pop $R0 # return value/error/timeout
Call CheckReboot
IntOp $5 $5 | $R0

```



```

DetailPrint "tapinstall update returned: $R0"
Goto tapinstall_check_error

tapinstall:
DetailPrint "TAP-Win32 REMOVE OLD TAP"
nsExec::ExecToLog "$INSDIR\bin\tapinstall.exe" remove TAP'
Pop $R0 # return value/error/timeout
DetailPrint "tapinstall remove TAP returned: $R0"
nsExec::ExecToLog "$INSDIR\bin\tapinstall.exe" remove TAPDEV'
Pop $R0 # return value/error/timeout
DetailPrint "tapinstall remove TAPDEV returned: $R0"

DetailPrint "TAP-Win32 INSTALL (${TAP})"
nsExec::ExecToLog "$INSDIR\bin\tapinstall.exe" install
"$INSDIR\driver\OemWin2k.inf" ${TAP}'
Pop $R0 # return value/error/timeout
Call CheckReboot
IntOp $5 $5 | $R0
DetailPrint "tapinstall install returned: $R0"

tapinstall_check_error:
DetailPrint "tapinstall cumulative status: $5"
IntCmp $5 0 notap
MessageBox MB_OK "An error occurred installing the TAP-Win32 device driver."

notap:

; Store install folder in registry
WriteRegStr HKLM SOFTWARE\OpenVPN "" $INSDIR

; install as a service if requested
SectionGetFlags ${SecService} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" noserv noserv

; set registry parameters for openvpnserv
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN" "config_dir" "$
{SERV_CONFIG_DIR}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN" "config_ext" "$
{SERV_CONFIG_EXT}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN" "exe_path" "$
{SERV_EXE_PATH}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN" "log_dir" "$
{SERV_LOG_DIR}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN" "priority" "$
{SERV_PRIORITY}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN" "log_append" "$
{SERV_LOG_APPEND}"

; install openvpnserv as a service
DetailPrint "Previous Service REMOVE (if exists)"
nsExec::ExecToLog "$INSDIR\bin\openvpnserv.exe" -remove'
Pop $R0 # return value/error/timeout
DetailPrint "Service INSTALL"
nsExec::ExecToLog "$INSDIR\bin\openvpnserv.exe" -install'
Pop $R0 # return value/error/timeout

```

```

noserv:
; Store install folder in registry
WriteRegStr HKLM SOFTWARE\OpenVPN-GUI "" $INSTDIR

; Set registry keys for openvpn-gui if gui is requested
SectionGetFlags ${SecGUI} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" nogui nogui

; set registry parameters for openvpn-gui
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "config_dir"
"${GUI_CONFIG_DIR}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "config_ext"
"${GUI_CONFIG_EXT}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "exe_path"
"${GUI_EXE_PATH}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "log_dir"
"${GUI_LOG_DIR}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "priority"
"${GUI_PRIORITY}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "log_append"
"${GUI_LOG_APPEND}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "allow_edit"
"${GUI_ALLOW_EDIT}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"allow_service" "${GUI_ALLOW_SERVICE}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "allow_proxy"
"${GUI_ALLOW_PROXY}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"allow_password" "${GUI_ALLOW_PASSWORD}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "service_only"
"${GUI_SERVICE_ONLY}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "log_viewer"
"${GUI_LOG_VIEWER}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"passphrase_attempts" "${GUI_PSW_ATTEMPTS}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "editor"
"${GUI_EDITOR}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"connectscript_timeout" "${GUI_UP_TIMEOUT}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"disconnectscript_timeout" "${GUI_DOWN_TIMEOUT}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"preconnectscript_timeout" "${GUI_PRE_TIMEOUT}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"silent_connection" "${GUI_SILENT_CONN}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI" "show_balloon"
"${GUI_SHOW_BALLOON}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"show_script_window" "${GUI_SHOW_SCRIPT}"
!insertmacro WriteRegStringIfUndef HKLM "SOFTWARE\OpenVPN-GUI"
"disconnect_on_suspend" "${GUI_SUSPEND}"

#Set registry keys for openvpn-gui to Run As Administrator
#WriteRegStr HKLM "Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\layers" "$INSTDIR\bin\openvpn-gui.exe"

```

```

"RUNASADMIN"
  WriteRegStr HKCU "Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\layers" "$INSTDIR\bin\openvpn-gui.exe"
"RUNASADMIN"

; AutoStart OpenVPN GUI if requested
SectionGetFlags ${SecGUIAuto} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" nogui nogui

; set registry parameters for openvpn-gui
!insertmacro WriteRegStringIfUndef HKLM
"SOFTWARE\Microsoft\Windows\CurrentVersion\Run" "openvpn-gui"
"$INSTDIR\bin\openvpn-gui.exe"

nogui:
; Store README, license, icon
SetOverwrite on
SetOutPath $INSTDIR
File "${HOME}\install-win32\INSTALL-win32.txt"
File "${HOME}\install-win32\license.txt"
File "${HOME}\install-win32\openvpn.ico"

; Create file association if requested
SectionGetFlags ${SecFileAssociation} $R0
IntOp $R0 $R0 & ${SF_SELECTED}
IntCmp $R0 ${SF_SELECTED} "" noass noass
!insertmacro WriteRegStringIfUndef HKCR ".${SERV_CONFIG_EXT}" ""
"OpenVPNFile"
!insertmacro WriteRegStringIfUndef HKCR "OpenVPNFile" "" "OpenVPN Config
File"
!insertmacro WriteRegStringIfUndef HKCR "OpenVPNFile\shell" "" "open"
!insertmacro WriteRegStringIfUndef HKCR "OpenVPNFile\DefaultIcon" ""
"$INSTDIR\openvpn.ico,0"
!insertmacro WriteRegStringIfUndef HKCR "OpenVPNFile\shell\open\command" ""
'notepad.exe "%1"'
!insertmacro WriteRegStringIfUndef HKCR "OpenVPNFile\shell\run" "" "Start
OpenVPN on this config file"
!insertmacro WriteRegStringIfUndef HKCR "OpenVPNFile\shell\run\command" ""
'"$INSTDIR\bin\openvpn.exe" --pause-exit --config "%1"'

noass:
; ; Create start menu link to source distribution zip file
; IfFileExists "$SMPROGRAMS\OpenVPN" "" noshortcuts
; IfFileExists "$INSTDIR\${SOURCE_ZIP_DEST}" "" nosourcezip
; CreateShortCut "$SMPROGRAMS\OpenVPN\OpenVPN Source Code Distribution.lnk"
"$INSTDIR\${SOURCE_ZIP_DEST}" ""
;
; ; Create start menu shortcuts to addtap.bat and deltapall.bat
; nosourcezip:

CreateDirectory "$SMPROGRAMS\OpenVPN\Utilities"

IfFileExists "$INSTDIR\bin\addtap.bat" "" trydeltap
CreateShortCut "$SMPROGRAMS\OpenVPN\Utilities\Add a new TAP-Win32 virtual
ethernet adapter.lnk" "$INSTDIR\bin\addtap.bat" ""

```

```

trydeltap:
  IfFileExists "$INSDIR\bin\deltapall.bat" "" config_shortcut
  CreateShortcut "$SMPROGRAMS\OpenVPN\Utilities\Delete ALL TAP-Win32 virtual
  ethernet adapters.lnk" "$INSDIR\bin\deltapall.bat" ""

  ; Create start menu shortcuts for config and log directories

  CreateDirectory "$SMPROGRAMS\OpenVPN\Shortcuts"

config_shortcut:
  IfFileExists "$INSDIR\config" "" log_shortcut
  CreateShortcut "$SMPROGRAMS\OpenVPN\Shortcuts\OpenVPN configuration file
  directory.lnk" "$INSDIR\config" ""

log_shortcut:
  IfFileExists "$INSDIR\log" "" samp_shortcut
  CreateShortcut "$SMPROGRAMS\OpenVPN\Shortcuts\OpenVPN log file
  directory.lnk" "$INSDIR\log" ""

samp_shortcut:
  IfFileExists "$INSDIR\sample-config" "" genkey_shortcut
  CreateShortcut "$SMPROGRAMS\OpenVPN\Shortcuts\OpenVPN Sample Configuration
  Files.lnk" "$INSDIR\sample-config" ""

genkey_shortcut:
  IfFileExists "$INSDIR\bin\openvpn.exe" "" noshortcuts
  IfFileExists "$INSDIR\config" "" noshortcuts
  CreateShortcut "$SMPROGRAMS\OpenVPN\Utilities\Generate a static OpenVPN
  key.lnk" "$INSDIR\bin\openvpn.exe" "--pause-exit --verb 3 --genkey --secret
  "$INSDIR\config\key.txt" "$INSDIR\openvpn.ico" 0

noshortcuts:
  ; Create uninstaller
  WriteUninstaller "$INSDIR\Uninstall.exe"

  ; Show up in Add/Remove programs
  WriteRegStr HKLM "Software\Microsoft\Windows\CurrentVersion\Uninstall\OpenVPN"
  "DisplayName" "OpenVPN ${VERSION}"
  WriteRegExpandStr HKLM
  "Software\Microsoft\Windows\CurrentVersion\Uninstall\OpenVPN" "UninstallString"
  "$INSDIR\Uninstall.exe"

  ; Advise a reboot
  ;Messagebox MB_OK "IMPORTANT: Rebooting the system is advised in order to
  finalize TAP-Win32 driver installation/upgrade (this is an informational message
  only, pressing OK will not reboot)."

  WriteRegStr HKLM "Software\Microsoft\Windows\CurrentVersion\Uninstall\$
  {PRODUCT_NAME}" "DisplayIcon" "$INSDIR\openvpn.ico"
  WriteRegStr HKLM "Software\Microsoft\Windows\CurrentVersion\Uninstall\$
  {PRODUCT_NAME}" "DisplayVersion" "${VERSION}"

SectionEnd

;-----
;Descriptions

```

```

!insertmacro MUI_FUNCTION_DESCRIPTION_BEGIN
!insertmacro MUI_DESCRIPTION_TEXT ${SecOpenVPNUserSpace} $
(DESC_SecOpenVPNUserSpace)
!insertmacro MUI_DESCRIPTION_TEXT ${SecOpenVPNEasyRSA} $
(DESC_SecOpenVPNEasyRSA)
!insertmacro MUI_DESCRIPTION_TEXT ${SecGUI} $(DESC_SecGUI)
!insertmacro MUI_DESCRIPTION_TEXT ${SecGUIAuto} $(DESC_SecGUIAuto)
!insertmacro MUI_DESCRIPTION_TEXT ${SecMYCERT} $(DESC_SecMYCERT)
!insertmacro MUI_DESCRIPTION_TEXT ${SecTAP} $(DESC_SecTAP)
!insertmacro MUI_DESCRIPTION_TEXT ${SecTAPHidden} $(DESC_SecTAPHidden)
!insertmacro MUI_DESCRIPTION_TEXT ${SecOpenSSLUtilities} $
(DESC_SecOpenSSLUtilities)
!insertmacro MUI_DESCRIPTION_TEXT ${SecOpenSSLDLLs} $(DESC_SecOpenSSLDLLs)
; !insertmacro MUI_DESCRIPTION_TEXT ${SecOpenVPNSource} $(DESC_SecOpenVPNSource)
!insertmacro MUI_DESCRIPTION_TEXT ${SecAddPath} $(DESC_SecAddPath)
!insertmacro MUI_DESCRIPTION_TEXT ${SecAddShortcuts} $(DESC_SecAddShortcuts)
!insertmacro MUI_DESCRIPTION_TEXT ${SecService} $(DESC_SecService)
!insertmacro MUI_DESCRIPTION_TEXT ${SecFileAssociation} $
(DESC_SecFileAssociation)
!insertmacro MUI_FUNCTION_DESCRIPTION_END

Function .onInit
ClearErrors
UserInfo::GetName
IfErrors ok
Pop $R0
UserInfo::GetAccountType
Pop $R1
StrCmp $R1 "Admin" ok
Messagebox MB_OK "Administrator privileges required to install OpenVPN
[$R0/$R1]"
Abort
ok:

Push $R0
ReadRegStr $R0 HKLM SOFTWARE\OpenVPN-GUI ""
StrCmp $R0 "" goon

Messagebox MB_YESNO "It seems the package ${PRODUCT_NAME} (OpenVPN GUI) is
already installed.$\r$\nWe recommend you to uninstall it in the standard way
before proceeding. Continue installing?" IDYES goon
Abort

goon:
Pop $R0

Push $R0
Push $R1
FindWindow $R0 "openvpn-gui"
IntCmp $R0 0 donerun

Messagebox MB_YESNO|MB_ICONEXCLAMATION "OpenVPN GUI is currently running.
$\r$\nUntil you terminate it, all files that belong to it cannot be updated.
$\r$\nShall this program be killed now? If true, all existing connections will be
closed." IDNO donerun

SendMessage $R0 ${WM_DESTROY} 0 0 $R1 /TIMEOUT=7000

```

```

IntCmp $R1 0 donerun

    MessageBox MB_OK|MB_ICONEXCLAMATION "Trouble terminating OpenVPN GUI,
please close it and then click OK."

donerun:
Pop $R1
Pop $R0

;Disable My Certificate Wizard as default.
SectionSetFlags ${SecMYCERT} 0

; Don't install the TAP driver as hidden as default.
SectionSetFlags ${SecTAPHidden} 1

FunctionEnd

Function .onSelChange
    Push $0

    ;Check if Section OpenVPN GUI is selected.
    SectionGetFlags ${SecGUI} $0
    IntOp $0 $0 & ${SF_SELECTED}
    IntCmp $0 ${SF_SELECTED} "" noautogui noautogui

    ;GUI was selected so set GUIAuto to Not-ReadOnly.
    SectionGetFlags ${SecGUIAuto} $0
    IntOp $0 $0 & ${SF_NOT_RO}
    SectionSetFlags ${SecGUIAuto} $0
    goto CheckTAP

noautogui:
    SectionSetFlags ${SecGUIAuto} ${SF_RO}

CheckTAP:
    ;Check if Section Install-TAP is selected.
    SectionGetFlags ${SecTAP} $0
    IntOp $0 $0 & ${SF_SELECTED}
    IntCmp $0 ${SF_SELECTED} "" notap notap

    ;TAP was selected so set TAPHidden to Not-ReadOnly.
    SectionGetFlags ${SecTAPHidden} $0
    IntOp $0 $0 & ${SF_NOT_RO}
    SectionSetFlags ${SecTAPHidden} $0
    goto end

notap:
    SectionSetFlags ${SecTAPHidden} ${SF_RO}

end:
    Pop $0

FunctionEnd

Function .onInstSuccess
    IfFileExists "$INSTDIR\bin\openvpn-gui.exe" "" nogui
    ExecShell open "$INSTDIR\bin\openvpn-gui.exe"

```

```

nogui:
FunctionEnd
;-----
;Uninstaller Section
Function un.onInit
  ClearErrors
  UserInfo::GetName
  IfErrors ok
  Pop $R0
  UserInfo::GetAccountType
  Pop $R1
  StrCmp $R1 "Admin" ok
  Messagebox MB_OK "Administrator privileges required to uninstall OpenVPN
[$R0/$R1]"
  Abort
ok:
  Push $R0
  Push $R1
  FindWindow $R0 "openvpn-gui"
  IntCmp $R0 0 donerun

  Messagebox MB_YESNO|MB_ICONEXCLAMATION "OpenVPN GUI is currently running.
$r$\nUntil you terminate it, all files that belong to it cannot be removed.
$r$\nShall this program be killed now? If true, all existing connections will be
closed." IDNO donerun

  SendMessage $R0 ${WM_DESTROY} 0 0 $R1 /TIMEOUT=7000
  IntCmp $R1 0 donerun

  Messagebox MB_OK|MB_ICONEXCLAMATION "Trouble terminating OpenVPN GUI,
please close it and then click OK."

  donerun:
  Pop $R1
  Pop $R0

FunctionEnd
Section "Uninstall"

  DetailPrint "Service REMOVE"
  nsExec::ExecToLog '$INSTDIR\bin\openvpnserv.exe' -remove'
  Pop $R0 # return value/error/timeout

  Sleep 2000

  DetailPrint "TAP-Win32 REMOVE"
  nsExec::ExecToLog '$INSTDIR\bin\tapinstall.exe' remove ${TAP}'
  Pop $R0 # return value/error/timeout
  DetailPrint "tapinstall remove returned: $R0"

  Push "$INSTDIR\bin"
  Call un.RemoveFromPath

```

```

Delete "$DESKTOP\OpenVPN GUI.lnk"

RMDir /r "$SMPROGRAMS\OpenVPN"
RMDir /r "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\OpenVPN"
RMDir /r "$INSTDIR"

!insertmacro DelRegKeyIfUnchanged HKCR ".${SERV_CONFIG_EXT}" "OpenVPNFile"
DeleteRegKey HKCR "OpenVPNFile"
DeleteRegKey HKLM SOFTWARE\OpenVPN
DeleteRegKey HKLM SOFTWARE\OpenVPN-GUI
DeleteRegKey HKCU "Software\${PRODUCT_NAME}"
DeleteRegKey HKLM "Software\Microsoft\Windows\CurrentVersion\Uninstall\OpenVPN"
DeleteRegValue HKLM "Software\Microsoft\Windows\CurrentVersion\Run" "openvpn-
gui"
DeleteRegValue HKCU "Software\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\layers" "$INSTDIR\bin\openvpn-gui.exe"

SectionEnd

```

UpdateBL.sh.patch

UpdateBL_def : <http://urlblacklist.com/downloads/UpdateBL>

```

--- UpdateBL.def      2003-12-28 02:00:34.000000000 +0200
+++ UpdateBL.sh      2010-06-09 01:45:36.358534292 +0300
@@ -1,5 +1,7 @@
-#!/bin/bash
-###
+#!/bin/bash
+#
+#Modified by ddimarx for openvpn.it.teithe.gr and dansguardian 9.10
+#
# UpdateBL - refresh DansGuardian Blacklists
#
# Version: 0.9.2-Lince (Juan J. Prieto <jjprieto@eneotecnologia.com>)
@@ -70,19 +72,24 @@
#     DG_PATH - where the DansGuardian Binary is located
#
#
-export BL_URL=${BL_URL:="http://urlblacklist.com/cgi-bin/commercialdownload.pl?
type=download&file=smalltestlist"}
+#export BL_URL=${BL_URL:="http://urlblacklist.com/cgi-bin/commercialdownload.pl?
type=download&file=smalltestlist"}
+#export BL_URL_INFO=${BL_URL_INFO:="http://urlblacklist.com/cgi-
bin/commercialdownload.pl?type=information&file=bigblacklist"}
+export BL_URL=${BL_URL:="http://urlblacklist.com/cgi-bin/commercialdownload.pl?
type=download&file=bigblacklist"}
+
+#export BL_URL=${BL_URL:="http://urlblacklist.com/cgi-bin/commercialdownload.pl?
type=download&file=smalltestlist"}
export BL_URL_INFO=${BL_URL_INFO:="http://urlblacklist.com/cgi-

```



```

bin/commercialdownload.pl?type=information&file=bigblacklist"}
-#export BL_URL=${BL_URL:="http://urlblacklist.com/cgi-bin/commercialdownload.pl?
type=download&file=bigblacklist"}
+#export BL_URL=$
{BL_URL:="http://ftp.teledanmark.no/pub/www/proxy/squidGuard/contrib/blacklists.t
ar.gz"}

# IMPORTANT - The blacklist is COMMERCIAL. If you download without a
subscription you
# are stealing. You may try 1 download of the big list for free to
test.
# For details see: http://urlblacklist.com/

#
-export BL_INFO_FILE="/etc/dansguardian/blacklists/blacklists.info"
-export DB_PATH=${DB_PATH:="/etc/dansguardian/blacklists"}
+export BL_INFO_FILE="/etc/dansguardian/lists/blacklists/blacklists.info"
+export DB_PATH=${DB_PATH:="/etc/dansguardian/lists/blacklists"}
export HOME_DIR="/tmp"
-export SG_UGID=${SG_UGID:="nobody:nogroup"}
+#export SG_UGID=${SG_UGID:="nobody:nogroup"}
+export SG_UGID=${SG_UGID:="root:root"}
export DG_PATH=${DG_PATH:="/usr/sbin"}
export UNCOMP_CMD="/bin/gunzip"
export UNTAR_DIR="blacklists"
@@ -93,7 +100,7 @@
export BL_TAR_BASE="blacklists.tar.gz"
export BL_TAR_FULL="${HOME_DIR}/${BL_TAR_BASE}"
export TMP_DIR="/tmp/blacklists"
-export http_proxy="127.0.0.1:3128"
+export http_proxy="192.168.192.20:8080"

# We need to check for updates
export BL_URL_INFO='wget -q -Y on "${BL_URL_INFO}" -O - | head -n 1`
@@ -194,6 +201,10 @@
cd /tmp
rm -rf /tmp/blacklists

+#Unsortin the Blacklist by ddimarx
+ cd "${DB_PATH}" ; find . -type f -exec rl '{}' -o '{}'.tmp \; -exec
mv -f '{}'.tmp '{}' \;
+
+
# Change owner and permissions.
chown -R "${SG_UGID}" "${DB_PATH}"
chmod -R 755 "${DB_PATH}"
@@ -201,12 +212,19 @@
# Writting information in blacklists.info and blacklst.version
echo "DATE:${BL_DATE_NEW}" > ${BL_INFO_FILE}
echo "MD5SUM:${BL_MD5SUM_NEW}" >> ${BL_INFO_FILE}
- echo "${BL_DATE_NEW}" > /var/lib/lrpkg/blacklst.version
- chown root:root /var/lib/lrpkg/blacklst.version
- chmod 644 /var/lib/lrpkg/blacklst.version
+ #echo "${BL_DATE_NEW}" > /var/lib/lrpkg/blacklst.version
+ #chown root:root /var/lib/lrpkg/blacklst.version
+ #chmod 644 /var/lib/lrpkg/blacklst.version
+ echo "${BL_DATE_NEW}" > /etc/dansguardian/blacklists.info

```

```
+ #chown root:root /var/lib/lrpkg/blacklst.info
+ #chmod 644 /var/lib/lrpkg/blacklst.info

# Restarting Dansguardian.
- /etc/init.d/dansguardian restart >/dev/null 2>&1
+ #/etc/init.d/dansguardian restart >/dev/null 2>&1
+ /etc/init.d/dansguardian stop >/dev/null 2>&1
+ /etc/init.d/dansguardian restart >/dev/null 2>&1
+ #/etc/init.d/ttyRep stop >/dev/null 2>&1
+ #/etc/init.d/ttyRep start >/dev/null 2>&1

# Finished Blacklist update.
```

dansguardian.conf.patch

```
--- dansguardian_def.conf      2008-10-21 08:51:58.000000000 +0300
+++ dansguardian.conf 2010-06-09 01:23:23.175284371 +0300
@@ -1,8 +1,10 @@
+# Modified by ddimarx for openvpn.it.teithe.gr and dansguardian 9.10

# **NOTE** as of version 2.7.5 most of the list files are now in
dansguardianfl.conf

-UNCONFIGURED - Please remove this line after configuration
+#UNCONFIGURED - Please remove this line after configuration

# Web Access Denied Reporting (does not affect logging)
#
@@ -86,13 +88,28 @@
filterip =

# the port that DansGuardian listens to.
-filterport = 8080
+filterport = 1194

# the ip of the proxy (default is the loopback - i.e. this server)
-proxyip = 127.0.0.1
+proxyip = 192.168.192.20

# the port DansGuardian connects to proxy on
-proxyport = 3128
+proxyport = 8080
+
+# Whether to retrieve the original destination IP in transparent proxy
+# setups and check it against the domain pulled from the HTTP headers.
+#
+# Be aware that when visiting sites which use a certain type of round-
+robin
+# DNS for load balancing, DG may mark requests as invalid unless DG gets
+# exactly the same answers to its DNS requests as clients. The chances
```

```

of
+# this happening can be increased if all clients and servers on the same
LAN
+# make use of a local, caching DNS server instead of using upstream DNS
+# directly.
+#
+# See http://www.kb.cert.org/vuls/id/435052
+# on (default) | off
+#!! Not compiled !! originalip = on

# accessdeniedaddress is the address of your web server to which the cgi
# dansguardian reporting script was copied. Only used in reporting
levels 1 and 2.
@@ -106,7 +123,7 @@
#
# Individual filter groups can override this setting in their own
configuration.
#
-accessdeniedaddress = 'http://YOURSERVER.YOURDOMAIN/cgi-
bin/dansguardian.pl'
+accessdeniedaddress = 'http://195.251.123.180/cgi-bin/dansguardian.pl'

# Non standard delimiter (only used with accessdeniedaddress)
# To help preserve the full banned URL, including parameters, the
variables
@@ -413,8 +430,8 @@
# Some of the scanner(s) require 3rd party software and libraries eg
clamav.
# See the individual plugin conf file for more options (if any).
#
-#contentsscanner = '/etc/dansguardian/contentsscanners/clamav.conf'
-#!! Not compiled !! contentsscanner =
'/etc/dansguardian/contentsscanners/clamdscan.conf'
+contentsscanner = '/etc/dansguardian/contentsscanners/clamav.conf'
+#contentsscanner = '/etc/dansguardian/contentsscanners/clamdscan.conf'
#!! Unimplemented !! contentsscanner =
'/etc/dansguardian/contentsscanners/kavav.conf'
#!! Not compiled !! contentsscanner =
'/etc/dansguardian/contentsscanners/kavdscan.conf'
#contentsscanner = '/etc/dansguardian/contentsscanners/icapscan.conf'
@@ -437,7 +454,7 @@
# supposed to be trusted and will increase load.
# Correct use of grey lists are a better idea.
# (on|off) default = off
-contentscanexceptions = off
+contentscanexceptions = on

```

dansguardianf1.conf.patch

```
--- dansguardianfl_def.conf      2008-10-21 08:51:58.000000000 +0300
+++ dansguardianfl.conf 2010-06-09 01:27:07.415405511 +0300
@@ -1,5 +1,6 @@
-# DansGuardian filter group config file for version 2.9.9.4
+# DansGuardian filter group config file for version 2.10.1.1

+#Modified by ddimarx for openvpn.it.teithe.gr and dansguardian 9.10

# Filter group mode
# This option determines whether members of this group have their web access
@@ -94,7 +95,7 @@
# values. See the weightedphraselist file for examples.
# As a guide:
# 50 is for young children, 100 for old children, 160 for young adults.
-naughtynesslimit = 50
+naughtynesslimit = 180

# Category display threshold
# This option only applies to pages blocked by weighted phrase filtering.
@@ -129,7 +130,7 @@
#
# Defaults to disabled
# (on | off)
-enablepics = off
+enablepics = on

# Temporary Denied Page Bypass
# This provides a link on the denied page to bypass the ban for a few minutes.
To be
@@ -147,9 +148,6 @@
# '' = generate a random one (recommended and default)
# 'Mary had a little lamb.' = an example
# '76b42abc1cd0fdcaf6e943dcbc93b826' = an example
-#
-# Please note: manually entered keys are converted to all lowercase before use.
-#
bypasskey = ''

# Infection/Scan Error Bypass
```