ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΤΕΙ ΗΠΕΙΡΟΥ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

# ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ

(Virtual Private Network)


ΟΝΟΜΑ:ΧΡΥΣΑΝΘΗ

ΕΠΙΘΕΤΟ:ΚΟΛΟΚΟΥΡΑ

Α.Μ 10749

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΣΤΕΡΓΙΟΥ ΕΛΕΥΘΕΡΙΟΣ

ΑΡΤΑ 2017

**Περίληψη**

Σύμφωνα με το Σύστημα Πληροφοριών Διοίκησης μιας επιχείρησης ( MIS) για να λειτουργήσει σωστά μια επιχείρηση θα πρέπει οι πληροφορίες που λαμβάνονται και αποστέλλονται να είναι πλήρης ,ακριβείς και κατάλληλες για την εργασία για την οποία προορίζονται και για το πρόσωπο που θα τις χρησιμοποιήσει, ενώ θα πρέπει παράλληλα να παρέχονται εγκαίρως και με ασφάλεια. Με ένα τέτοιο δίκτυο **(VPN )** το οποίο παρέχει τα περισσότερα απαιτούμενα των επιχειρήσεων σε θέματα ασφάλειας και ταχύτητας αποστολής των πληροφοριών θα ασχοληθούμε στην παρούσα εργασία. Θα κάνουμε μια μικρή ιστορική αναδρομή ,θα γνωρίσουμε τα χαρακτηριστικά του , τις αρχιτεκτονικές του καθώς και τα χαρακτηριστικά των πρωτοκόλλων που το απαρτίζουν.

**ΠΕΡΙΕΧΟΜΕΝΑ** **ΣΕΛ.**

**ΕΙΣΑΓΩΓΗ**

Είναι γεγονός ότι ζούμε σε μια διαδικτυακή εποχή όπου τόσο ο επιστημονικός όσο και ο επιχειρηματικός κόσμος συσχετίζεται με το διαδίκτυο . Η πληροφορική και οι τηλεπικοινωνίες βοηθούν καταλυτικά στην υποστήριξη της λειτουργίας μιας επιχείρησης. Ιδιαιτέρως σήμερα που οι απαιτήσεις των επιχειρήσεων ,ο ανταγωνισμός και οι συμμαχίες έχουν αυξηθεί σημαντικά.

Το διαδίκτυο εξαπλώνεται σε όλον τον κόσμο με ραγδαίους ρυθμούς δημιουργώντας άνεση ,ευκολία και ευελιξία στον τρόπο εξάπλωσης των επιχειρήσεων και ταυτόχρονα ανοίγοντάς τους νέους ορίζοντες στις προοπτικές και στις ανάγκες τους .

Οι απαιτήσεις όμως των επιχειρήσεων δεν σταματούν εκεί .Μπορεί το διαδίκτυο να τους εξασφαλίζει αύξηση της κερδοφορίας και της παραγωγικότητας γεννάει όμως κι άλλες ανάγκες ως προς την ασφάλεια και την ενδοαιτερική επέκταση και επικοινωνία.

Για το λόγο αυτό δημιουργήθηκαν τα VPNs ( Virtual Private Network ) . Είναι μια νέα τεχνολογία η οποία συνεχώς εξελίσσεται και προσπαθεί να δώσει λύσεις σε προβλήματα ασφάλειας, επέκτασης της υπάρχουσας υποδομής ,επικοινωνίας ,οργάνωσης , διαχείρισης και κατανομής πληροφοριών σε όλα τα τμήματα ή υποκαταστήματα μιας επιχείρησης όπου και αν βρίσκονται.

Την τεχνολογία αυτή θα προσπαθήσουμε να προσεγγίσουμε στην εργασία αυτή . Θα γνωρίσουμε τα χαρακτηριστικά της ,τον τρόπο που λειτουργεί , τις αρχιτεκτονικές της και τα πρωτόκολλα που την απαρτίζουν.

## ΚΕΦΑΛΑΙΟ 2: Γνωριμία με τα VPNs

### 2.1 Ορισμός και σημασιολογία VPN

Το **VPN είναι:** ο ασφαλής και αξιόπιστος τρόπος μεταφοράς μιας εμπιστευτικής και απόρρητης πληροφορίας μέσω ενός δημοσίου δικτύου. Πχ ( internet ).

Αναφέρει χαρακτηριστικά η υπεύθυνη IT του κέντρου βιώσιμης επιχειρηματικότητας εξέλιξης της τράπεζας Πειραιώς κ. Ουρανία Παντελίδου : « τα VPNs είναι ένα συνδυασμός πληροφορικής και τηλεπικοινωνιών ,με σκοπό να δημιουργήσουν ένα ασφαλές και οικονομικό τρόπο επικοινωνίας ανάμεσα σε απομακρυσμένα δίκτυα.»

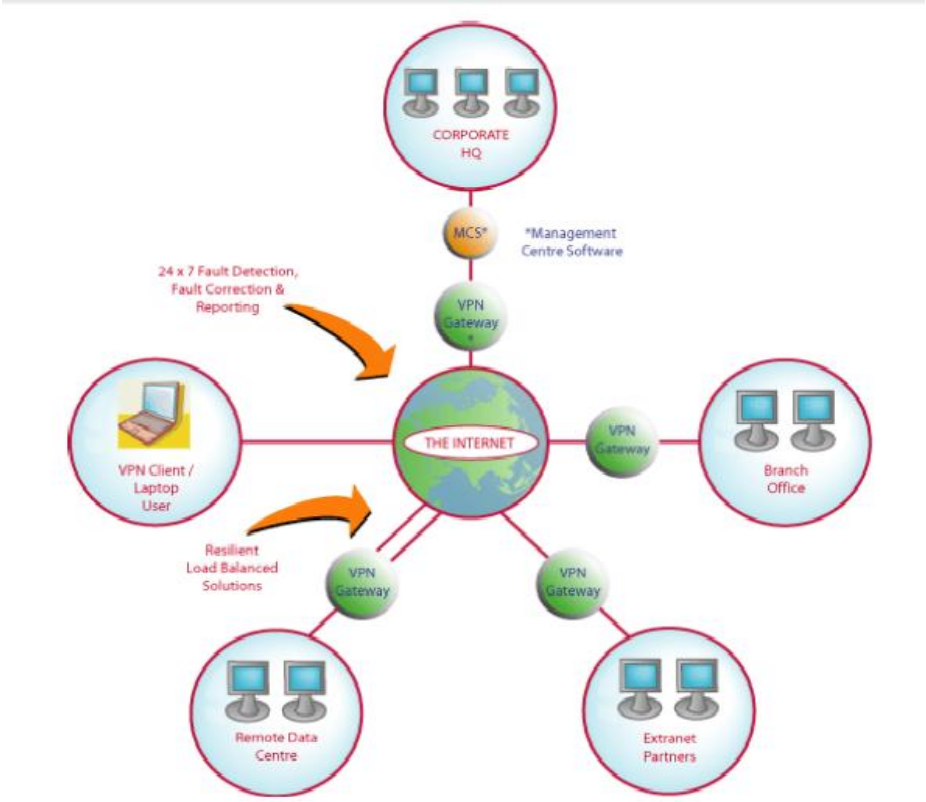
Σύμφωνα με την IETF ( Internet Engineering Task Force ), τα VPNs ορίζονται σαν την « εξομοίωση ενός προσωπικού Wide Area Network (WAN ) ,χρησιμοποιώντας κάποιο κοινόχρηστο ή δημόσια προσβάσιμο μέσω επικοινωνίας ,όπως το internet και τα IP δίκτυα.»

Ένας άλλος ορισμός που θα μπορούσε να αποδοθεί στα VPNs είναι : « τα VPNs είναι μια εναλλακτική λύση της υποδομής που παρέχουν τα WAN και που αντικαθιστούν ή επαυξάνουν τα υπάρχουσα ιδιωτικά δίκτυα που χρησιμοποιούν μισθωμένες γραμμές ή Frame Relay /ATM δίκτυα που ανήκουν στην επιχείρηση.»

**Virtual:** σημαίνει εικονικό κάτι το πλασματικό. Δηλαδή με τον όρο αυτό εννοούμε ότι το δίκτυο δεν υπάρχει σαν φυσική υπόσταση ,όμως μέσω της χρήσεις του internet μοιάζει με υπαρκτό .Το δίκτυο μπορεί να μορφοποιείτε ανάλογα με τις εγκαταστάσεις και το χρόνο που γίνεται η σύνδεση, χρησιμοποιώντας εξωτερικό εξοπλισμό (του ISP)και όχι αναγκαστικά της συγκεκριμένης επιχείρησης. Τα δεδομένα που στέλνουν κάθε φορά μπορούν να ακολουθούν διαφορετικές διαδρομές μέχρι να φτάσουν στον προορισμό τους.

**Private**: ο όρος αυτός δηλώνει πως το δίκτυο είναι ιδιωτικό. Δηλαδή ότι η δρομολόγηση της πληροφορίας και η διευθυνσιοδότηση των συσκευών μέσα στο δίκτυο είναι ανεξάρτητα από των υπόλοιπων δικτύων. Στην περίπτωση αυτή αναπτύσσετε μια ιδιωτική προσωπική σχέση μεταξύ των δύο σημείων(χρηστών) ανεξάρτητα αν χρησιμοποιείται κοινό δίκτυο ή αν αποστέλλονται ταυτόχρονα και άλλα δεδομένα τη συγκεκριμένη στιγμή. Ένα ακόμα χαρακτηριστικό των private δικτύων είναι η εξασφάλιση ασφάλειας και προστασίας από υποκλοπές εφόσον τα δεδομένα είναι απόρρητα.

**Network:** το VPN είναι ένα δίκτυο, αποτελούμενο από πολλές συσκευές συνδεδεμένες μεταξύ τους ελεύθερα και ηλεκτρονικά είτε μέσω καλωδίων είτε ασύρματα. Οι πληροφορίες μπορούν ν ’ αποστέλλονται και σε μεγάλες αποστάσεις χωρίς να δημιουργείτε πρόβλημα στην αποτελεσματικότητα ή στην αποδοτικότητα τους.




**Εικόνα 1 : εικονικά ιδιωτικά δίκτυα (VPNs )**

## 2.2.Ποιά η χρησιμότητα των δικτύων VPNs

Τα VPNs χρησιμοποιούνται συνήθως από μεγάλες εταιρίες για ασφαλή ηλεκτρονικό εμπόριο και επικοινωνία των συνεργατών, των προμηθευτών και των πελατών τους οι οποίοι μπορεί να βρίσκονται σε απομακρυσμένες περιοχές και να μην έχουν πρόσβαση.

Χωρίζονται σε 3$^{ης}$ κατηγορίες :

- Remote access (απομακρυσμένης πρόσβασης), επιτρέπει την σύνδεση σε μεμονωμένα στελέχη στο εταιρικό δίκτυο της επιχείρησης από το σπίτι ή σε κάποιο ταξίδι. Δίνεται η δυνατότητα ενδοεταιρικής τηλεφωνίας μέσω του προσωπικού υπολογιστή.
- Intranet VPNs, ασχολείται με την σύνδεση των γραφείων και των υποκαταστημάτων μιας εταιρίας. Σκοπός είναι να υπάρχει κεντρικός έλεγχος της υποδομής της εταιρείας ,δηλαδή να μπορούν χρήστες από απομακρυσμένα σημεία να χρησιμοποιούν την υποδομή της εταιρίας απευθείας από τα κεντρικά της γραφεία. Επιτρέπεται η ενδοεταιρική τηλεφωνίας.
- Extranet VPNs, επιτρέπουν στους εξωτερικούς συνεργάτες της επιχείρησης όπως προμηθευτές ή πελάτες να έχουν πρόσβαση στο δίκτυο της επιχείρησης για την ανταλλαγή πληροφοριών ανάλογα με τα δικαιώματα που επιθυμεί η επιχείρηση να αναθέσει.

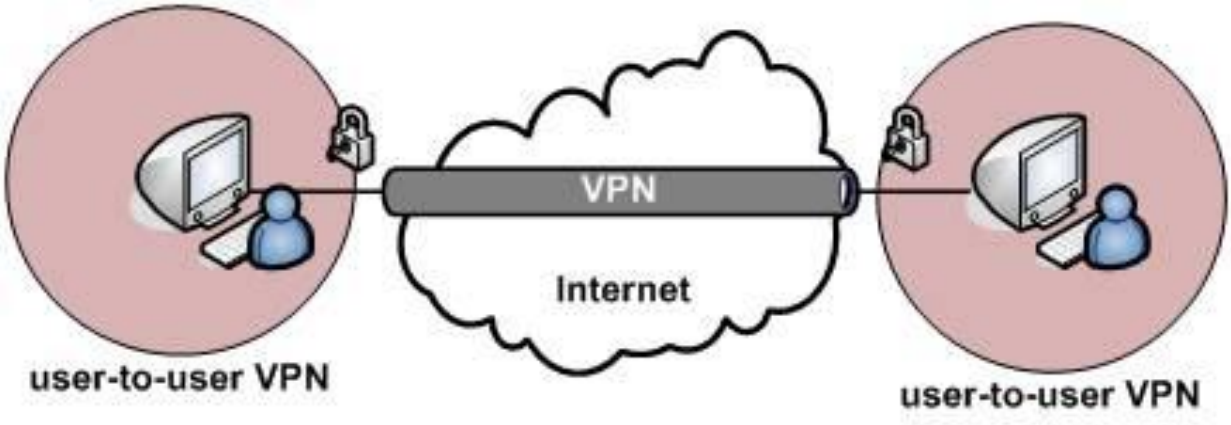
## 2.3.Ιστορική αναδρομή

Η δημιουργία VPNs δικτύων ξεκίνησε τη δεκαετία **1960.**

Τα πρώτα τηλεπικοινωνιακά δίκτυα που αναπτύχθηκαν, βασίστηκαν σε δύο τεχνολογίες:

- **γραμμές με διεπιλογή (dial-up lines ) ή Remote – access VPNs**

οι γραμμές αυτές εξυπηρετούσαν απαιτήσεις περιστασιακής συνδεσιμότητας και χρησιμοποιούνταν σε περιπτώσεις ανάγκης ύστερα από τηλεφωνική κλήση προς τον παροχέα. Πολλές φορές θα δούμε τις συνδέσεις αυτές να αποκαλούνται και ως virtual private dial-up network[VPDN].




**Εικόνα 2 :Σύνδεση dial -up**

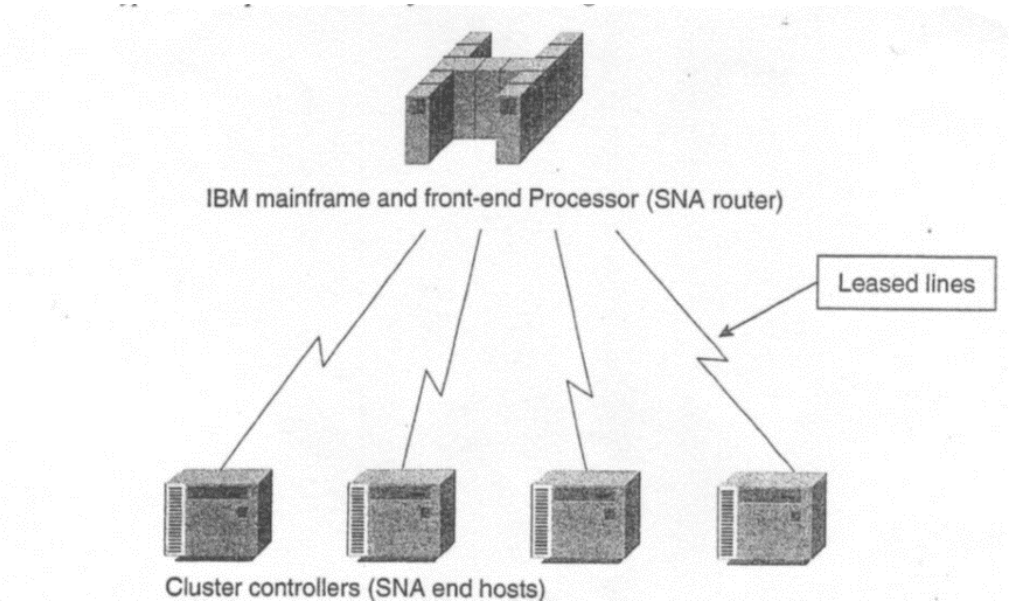
Στην αρχική τους έκδοση δεν χρησιμοποιούνταν το internet .

Π.χ αν ένας υπάλληλος επιθυμούσε να συνδεθεί από το σημείο στο οποίο βρισκόταν με το δίκτυο της επιχείρησης του το οποίο βρισκόταν σε απομακρυσμένο σημείο με τη χρήση dial-up modem έπρεπε να καλέσει στο τηλέφωνο στο άλλο σημείο .Με αυτόν τον τρόπο δημιουργούνταν μια point-to-point σύνδεση η οποία ήταν μεν μια ασφαλής απευθείας σύνδεση αφού δεν χρησιμοποιούνταν το internet και δεν επενέβαιναν στη γραμμή και άλλοι χρήστες. Όμως το κόστος ήταν αρκετά υψηλό και περιόριζε την ταχύτητα του PSTN δικτύου. Ειδικά αν η τοποθεσία του παροχέα ήταν στο εξωτερικό.

Στη συνέχεια εξελίχθηκαν σε Remote – access VPNs.

- **μισθωμένες γραμμές (leased-lines**)οι οποίες χρησιμοποιούνται μέχρι και σήμερα .

**Μισθωμένες Γραμμές:** είναι οι πρώτες τηλεπικοινωνιακές διασυνδέσεις οι οποίες εξασφάλιζαν την σύνδεση μεταξύ δύο σημείων με χρήση modem με προδιαγεγραμμένη ταχύτητα μετάδοσης δεδομένων 2.400 bps .Το εύρος ζώνης της ζεύξης ήταν διαθέσιμο μόνο στον πελάτη που το είχε εκμισθώσει .



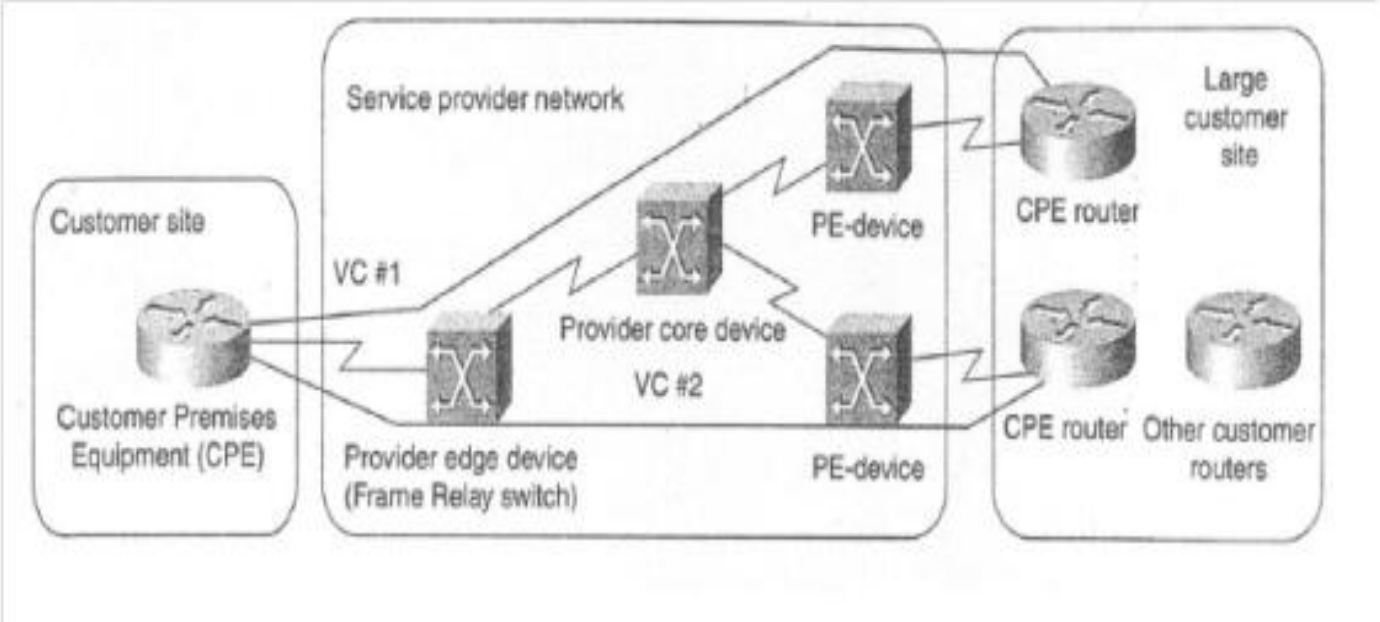

**Εικόνα 3 :Πρώτα τηλεπικοινωνιακά δίκτυα**

Βασικό μειονέκτημα των μισθωμένων γραμμών είναι πως η κίνηση των δεδομένων μεταξύ δύο τοποθεσιών διαφοροποιείτε ανάλογα την ώρα, τη μέρα ,το μήνα ,την εποχή. Λόγο του ότι η μισθωμένες γραμμές δεν παρέχουν ογκοχρέωση δηλαδή ο πάροχος προσφέρει σταθερό μηνιαίο μίσθωμα ανεξάρτητα από τον όγκο δεδομένων κατανάλωσης του χρήστη δημιουργούνται απαιτήσεις υψηλού εύρους ζώνης μεταξύ των τοποθεσιών.

Επίσης αντιμετωπίζουν δυσκολία στην ευελιξία δηλαδή δεν μπορούν να ανταποκριθούν εύκολα σε απαιτήσεις εξάπλωσης τους.

Για τους λόγους αυτούς οι ιδικοί προσπάθησαν να δώσουν λύσεις μέσω των νέων τεχνολογιών δημιουργώντας εξελισσόμενα **VPNs.**

Το πρώτο VPN βασίστηκε πάνω σε τεχνολογίες X.25, Frame relay και αργότερα SMDS, ATM.




**Εικόνα 4 : λύση VPN τεχνολογίας** Frame Relay

**Την δεκαετία του 1970** τα VPNs δίκτυα παρείχαν στους χρήστες υπηρεσίες ψηφιακών δεδομένων (Digital Data Service-DDS) με συνδέσεις 56 Kbps για ιδιωτικά δίκτυα και T1 υπηρεσίες με ταχύτητες 1.544 M bps.
**Το 1990** γεννήθηκε η ανάγκη για μετάδοση φωνής. Για το λόγο αυτό απευθύνθηκαν σε εταιρίες οι οποίες θα τους παρείχαν φτηνές φωνητικές κλήσεις. Οι εταιρίες προσέφεραν την T1 γραμμή. Η T1 είναι μια γραμμή η οποία είναι γρηγορότερη κ από την ποιο γρήγορη γραμμή του ADSL με ταχύτητα 1544kbps. Έτσι μειώθηκε το κόστος για τις τηλεφωνικές κλήσεις και αυξήθηκε η χρήση της T1 γραμμής . Όμως το κόστος της ήταν πολύ μεγάλο και η δυσκολία εκμίσθωσης της επίσης. Για το λόγο αυτό αυξήθηκαν ξανά οι συνδέσεις μετάδοσης δεδομένων.
Το 2000 το ADSL παρείχε τις υπηρεσίες του δοκιμαστικά .Η κυκλοφορία του στο εμπόριο άρχισε από το καλοκαίρι του 2003.
**Σήμερα** τα ποιο διαδεδομένα πρωτόκολλα που χρησιμοποιούνται είναι τα :

- **IP sec (Internet Protocol Security )**
- **SSL (Secure Socket Layer )**

ToIP sec είναι ίσως, το ποιό ισχυρό και το ποιό καλοσχεδιασμένο VPN πρωτόκολλο της εποχής μας .Αποτελείτε από 3 πρωτόκολλα όπου το καθένα από αυτά έχει το δικό του ρόλο είτε στην κρυπτογράφηση ,είτε στην ανταλλαγή πληροφοριών είτε στη διαχείριση ασφάλειας μεταξύ των δύο συνδεδεμένων άκρων.

### 2.3.1Τι παρείχαν τα πρώτα VPNs

Οι υπηρεσίες που παρείχαν οι τηλεπικοινωνιακές γραμμές που εκμίσθωνε ο πάροχος ήταν :

- Σύνδεση τηλεφωνικών κέντρων
- Τηλεφωνική επικοινωνία
- Τηλεομοιοτυπία (fax)
- Μετάδοση δεδομένων
- Σύνδεση με internet κ άλλα ιδιωτικά δίκτυα
- Σύνδεση εικονοτηλεφώνων και συστημάτων ασφαλείας
- Μετάδοση ραδιοφωνικών και τηλεπικοινωνιακών προγραμμάτων

### 2.3.2 Τι παρέχουν σήμερα τα VPNs σε σχέση με τα πρώτα VPNs

- Μικρότερο κόστος από αυτό των ιδιωτικών δικτύων
- Ανάπτυξη και ενίσχυση της οικονομίας του διαδικτύου
- Μείωση εξόδων σε θέματα διαχείρισης ιδιοκτησίας και λειτουργίας ιδιωτικού δικτύου
- Απλοποίηση διαδικτυακών τοπολογιών
- Μείωση φόρτου εργασίας

### 2.4 βασικές απαιτήσεις VPNs

Όταν μια εταιρία εγκαθιστά ένα VPN απαιτεί την αποφυγή κινδύνου εισβολής κακόβουλων χρηστών , την απαγόρευση πρόσβασης των συνεργατών σε πληροφορίες της εταιρίας πέραν των επιτρεπτών ,όπως επίσης και την εγγύηση ασφάλειας δεδομένων που διακινούνται μέσω διαδικτύου σε συνδέσεις απομακρυσμένης πρόσβασης.

Για να τα εξασφαλίσει όλα αυτά το VPN πρέπει οπωσδήποτε να πληρεί τις ποιο κάτω προϋποθέσεις :

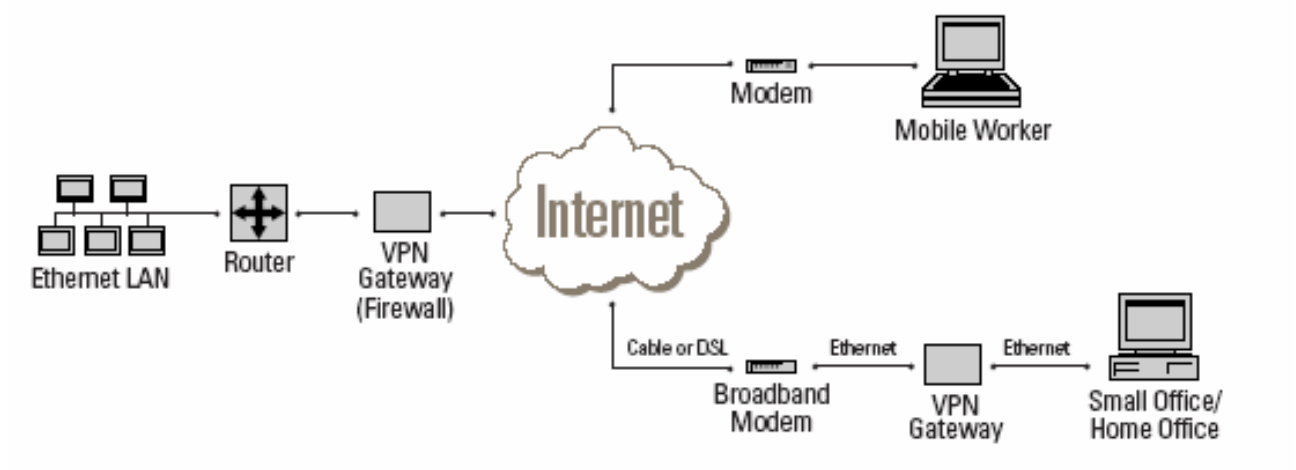
**User Authentication**: η επιχείρηση που θα επιλέξει αυτή τη λύση θα πρέπει να ελέγχει την ταυτότητα του χρήστη και να περιορίζει την πρόσβαση στο VPN μόνο σε χρήστες που εξουσιοδοτεί. Επίσης θα ελέγχονται και θα καταγράφονται οι επισκέψεις στις προσβάσιμες πληροφορίες.

**Address management:** στην περίπτωση αυτή συνδέεται το VPNs server της διεύθυνσης του πελάτη με το τοπικό δίκτυο και εξασφαλίζεται το απόρρητο της διεύθυνσης.

**Key Management:** στην προϋπόθεση αυτή απαραίτητη είναι η παραγωγή και η ανανέωση encryption keys για τους client και service.

**Multiprotocol Support:** εδώ είναι αναγκαία η υποστήριξη κοινών πρωτοκόλλων που χρησιμοποιούνται στο διαδίκτυο όπως είναι το IP και το Internet Packet Exchange.

2.5 **Πως λειτουργεί και από τι απαρτίζεται ένα VPN δίκτυο**




**Εικόνα 5: Ένα VPN δίκτυο**

Σύμφωνα με την παραπάνω εικόνα ένας υπολογιστής αποστέλλει τα δεδομένα σε μια συσκευή VPN . Η συσκευή αυτή είναι τοποθετημένη στο σημείο που πραγματοποιείται η επικοινωνία μεταξύ του ιδιωτικού δικτύου και του δημόσιου δικτύου .Επεξεργάζεται τα δεδομένα που δέχτηκε και τα ελέγχει αν διαμορφώθηκαν σύμφωνα με τους κανόνες ασφαλείας που έχει ορίσει ο διαχειριστής του δικτύου. Στη συνέχεια καθιστά ασφαλή τα δεδομένα μέσω κάποιων αλγορίθμων ή δεν τα επεξεργάζεται καθόλου σε περίπτωση που είναι είδη ασφαλή.

Όταν επιβεβαιωθεί η ασφάλεια των δεδομένων η συσκευή **VPN** κρυπτογραφεί την πληροφορία επικολλώντας πάνω στο πακέτο δεδομένων που θα σταλθεί μια επικεφαλίδα και τις IP διευθύνσεις του αποστολέα και του παραλήπτη.

Στη συνέχεια επικολλά μια νέα επικεφαλίδα πάνω στα δεδομένα. Η επικεφαλίδα αυτή δίνει πληροφορίες για την συσκευή παραλήπτη που βρίσκεται στο τέλος της διαδρομής και οδηγίες για τον τρόπο προστασίας των δεδομένων . Ύστερα πραγματοποιεί ενθυλάκωση στο κρυπτογραφημένο πακέτο πληροφορίας με τις IPδιευθύνσεις της αντίστοιχης συσκευής ή συσκευών – παραλήπτη. Με τον τρόπο αυτό δημιουργείτε το ιδιωτικό tunnel μέσα στο οποίο μεταφέρονται τα δεδομένα ασφαλή μέσω του δημοσίου δικτύου. Τέλος όταν το πακέτο φτάσει στη συσκευή παραλήπτη γίνεται η αντίστροφη διαδικασία ενθυλάκωσης , η επικεφαλίδα ελέγχετε και το πακέτο αποκρυπτογραφείται

### 2.6 Δομικά στοιχεία ενός VPN

Ένα VPN αποτελείτε από :

- Το **internet** το οποίο χρησιμοποιείτε για τη μετάδοση των δεδομένων και
- Τις **πύλες ασφαλείας** ,οι οποίες χρησιμοποιούνται στην ασφαλή μετάδοση των δεδομένων και διακρίνονται σε τέσσερις κατηγορίες :
  - **Δρομολογητές (Routers)** ,κρυπτογραφούν είτε με λογισμικό είτε με ξεχωριστό κύκλωμα κρυπτογράφησης τα πακέτα που δέχονται και προωθούν. Η απόδοση όλου του VPN εξαρτάται σε μεγάλο βαθμό από την απόδοση του δρομολογητή .
  - **Τοίχος προστασίας (Firewalls ):** φιλτράρουν τα δεδομένα με βάση τη διεύθυνση του κάθε πακέτου. Μπορούν επίσης να κάνουν και κρυπτογράφηση αρκεί την ώρα της διαδικασίας το δίκτυο να μην είναι υπερφορτωμένο γιατί πέφτει η συνολική απόδοση.
  - **Υπηρεσίες πιστοποίησης (Certificate Authorities )** :ελέγχουν την εγκυρότητα των στοιχείων ταυτότητας του κάθε χρήστη που υπάρχει στη βάση δεδομένων.
  - **Διακομιστές ασφαλείας ( Security Police Servers ):** είναι υπεύθυνοι για τη διαχείριση του κλειδιού ,ελέγχουν τα δικαιώματα πρόσβασης των χρηστών και ενημερώνουν τις πύλες ασφαλείας με κατάλληλο μήνυμα.

## Κεφάλαιο 3$^{ο}$

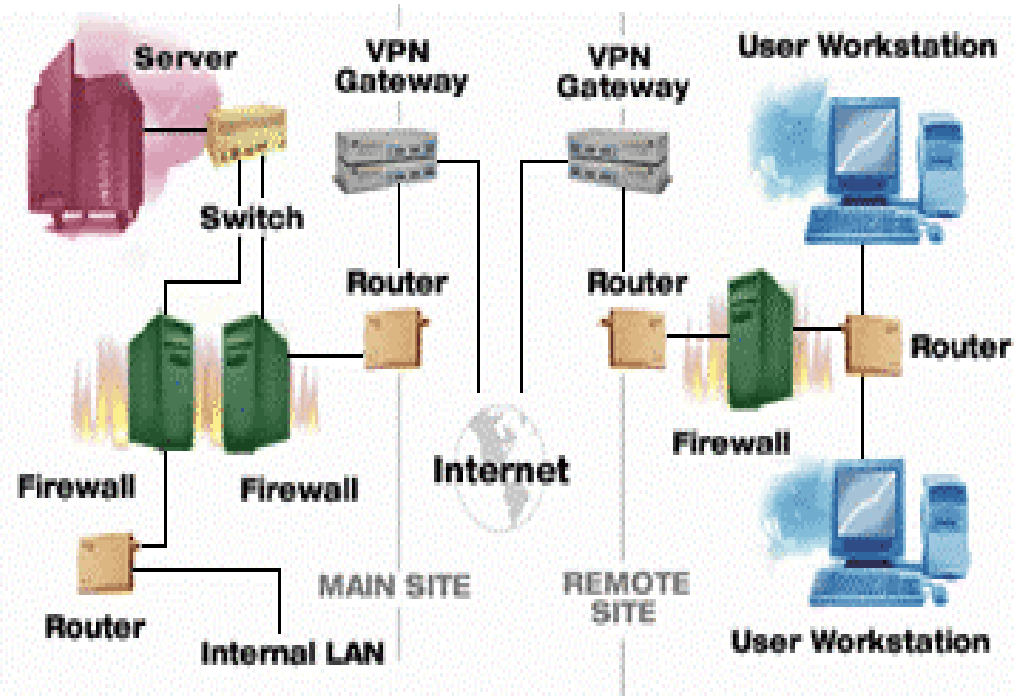
### Εξοπλισμός δικτύων VPNs

Για την υλοποίηση των VPNs χρησιμοποιούνται τα hardware και software . Για το πρώτο υπάρχουν εταιρείες όπως Cisco, Check Point ,Nokia ,Juniper που κατασκευάζουν VPN routers . Υπάρχουν όμως και τα DSL modem routers τα οποία παρέχουν κι αυτά δυνατότητες VPN.

Για υλοποίηση μέσω software υπάρχουν πολλές source λύσεις όμως η πολυπλοκότητα στην εγκατάσταση και στις ρυθμίσεις μπορεί να αποτελέσει πρόβλημα.

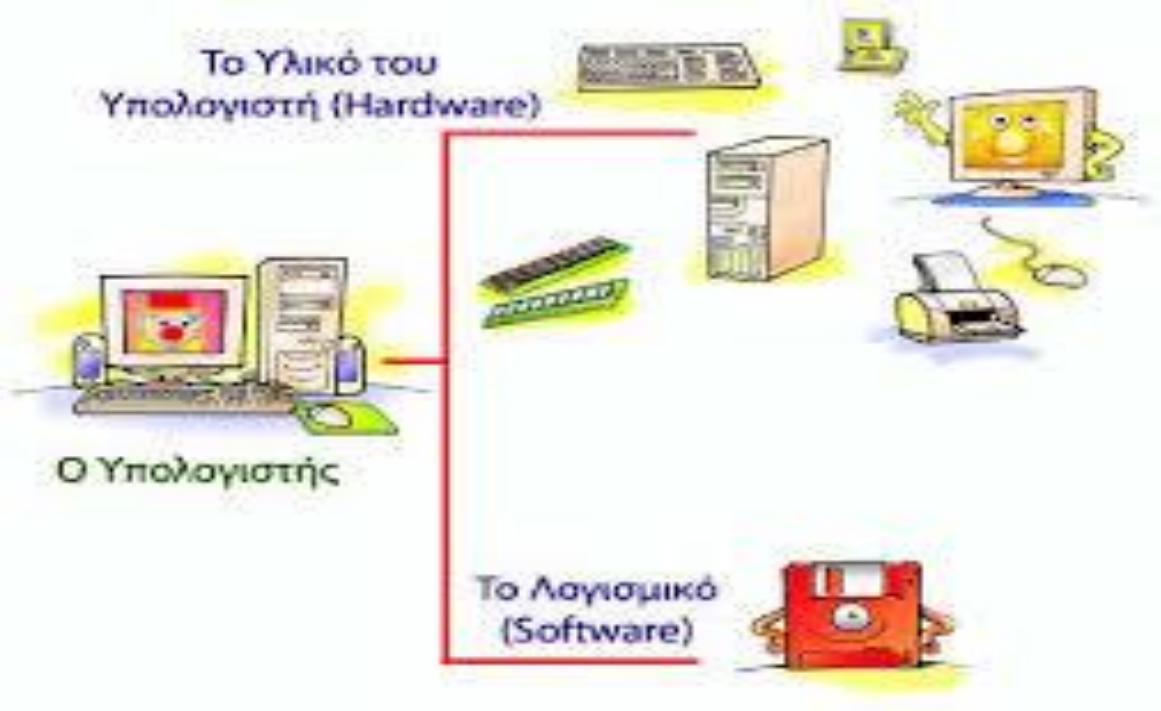
Ο εξοπλισμός που χρησιμοποιείτε στην υλοποίηση των VPNs διαφέρει από εταιρία σε εταιρία .

Το VPN software και hardware έχει την δυνατότητα να τοποθετηθεί σε διάφορα μέρη μέσα στο δίκτυο ,όπως πριν και μετά τους routers ή ανάμεσα στο ISP και το εταιρικό δίκτυο.

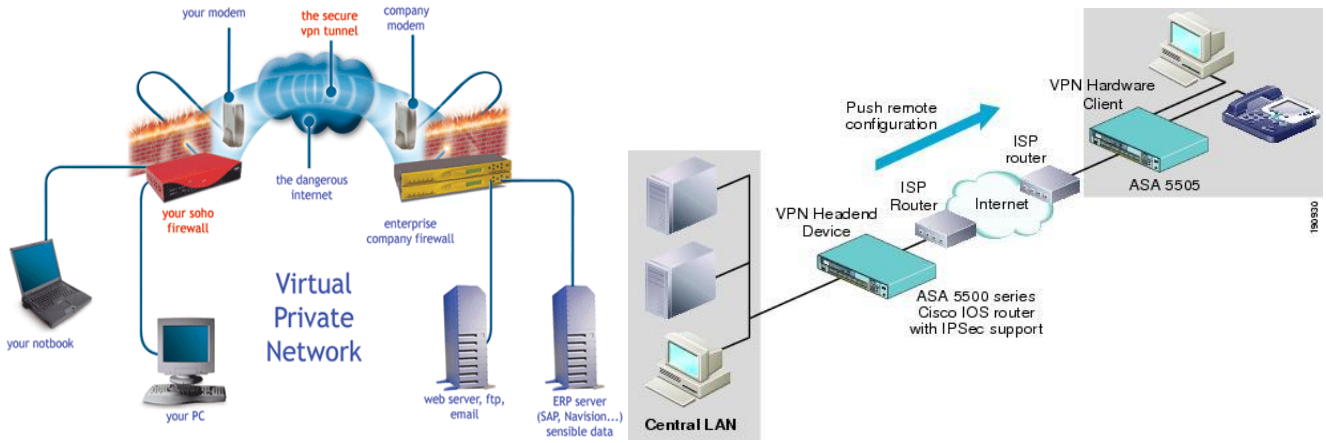



**Εικόνα 6: εξοπλισμός ενός VPN**

### 3.1 Το υλικό του υπολογιστή (hardware & **Software) VPN**



### 3.1.1 VPN hardware




Ένα VPN hardware είναι ένα εικονικό ιδιωτικό δίκτυο βασισμένο σε μια ενιαία αυτόνομη συσκευή. Η συσκευή αυτή ,η οποία παρέχει έναν ειδικό επεξεργαστή διαχειρίζεται τον έλεγχο ταυτότητας ,την κρυπτογράφηση και άλλες λειτουργίες VPN .

Για να στηθεί ένα VPN δίκτυο δεν αρκεί μόνο ο συνδυασμός hardware και software πρέπει να ενωθούν συσκευές με διαφορετικό προσανατολισμό , κατασκευαστή ακόμα και δυνατότητες .

Μερικές εξειδικευμένες συσκευές είναι οι routers firewall, DNS που προσφέρουν και αυτές με τη σειρά τους τις δικές τους υπηρεσίες.

Οι συσκευές αυτές χωρίζονται :

- Είτε με τον τρόπο δημιουργίας του tunnel και τον τρόπο πρόσβασης :
  - ✓ LAN –to –LAN
  - ✓ Dial –Up ή remote VPN gateways
- Είτε με τον τρόπο χρήσης της VPN συσκευής
  - ✓ Αν η συσκευή έχει φυσική σύνδεση στο δίκτυο τότε προσφέρετε και διαχείριση πόρων και bandwidth .
  - ✓ Αν η συσκευή έχει ως σκοπό μόνο τη διαχείριση δικτύου ,εφοδιάζετε με mail server και DNS caching .

Τα σημεία στα οποία θα πρέπει να δοθεί έμφαση καθώς χτίζεται ένα VPN δίκτυο είναι το tunneling , η κρυπτογράφηση και η πιστοποίηση χρηστών και διαχείριση. Ανάλογα με ποια από τις παραπάνω λειτουργίες θεωρούμε ποιο σημαντική επιλέγουμε και τα κατάλληλα πρωτόκολλα ( PPTP, L2TP,IP sec).

Ιδιαίτερη προσοχή πρέπει να δείξουμε στους remote users γιατί δημιουργούν για κάθε σύνδεση ένα tunnel . Πρέπει να υπολογίζεται ο αριθμός των ταυτόχρονων συνδέσεων δηλαδή των ταυτόχρονων ανοιχτών καναλιών γιατί παίζει ρόλο στην επιλογή συσκευής .

Αν και πρωτεύων πόλο παίζει το μέγεθος της επιχείρησης που θέλουμε να καλύψουμε.

### 3.1.2 VPN Software

Το Software γενικά, είναι όλο το άυλο υλικό του υπολογιστή είναι όλα τα προγράμματα που έχει μέσα του ή αν ακόμη δεν τα έχει τα εγκαθιστά ο χρήστης.

Στην περίπτωση όμως του VPN Software τα προϊόντα που του ανήκουν χωρίζονται σε δύο κατηγορίες

- Προϊόντα που χρησιμοποιούνται για συνδέσεις LAN to LAN και
- προϊόντα για συνδέσεις host to host tunneling τα οποία δεν είναι και τόσο εύχρηστα αφού καθυστερούν τους stand alone και μπορούν να αντικατασταθούν από τους Routers οι τα firewall για γρηγορότερη ασφάλεια και διαχείριση .

  Τα προϊόντα που χρησιμοποιούνται για διαδικασίες ενθυλάκωσης και Tunneling είναι το SOCKS v5 ή το Secure Shell (SSH ).

Γενικά τα σημεία στα οποία θα πρέπει να δίνουμε περισσότερη σημασία στα VAN Software είναι

- Τα πρωτόκολλα που υποστηρίζονται
- Η συνύπαρξη χωρίς προβλήματα με το υπάρχον λογισμικό
- Θέματα ασφαλείας, όπως κρυπτογράφηση και πιστοποίηση ταυτότητας των χρηστών .
- Διαχείριση (δυνατότητα για remote management )
- Auditing

Ποιο κάτω αναλύουμε δύο πολύ σημαντικά υλικά εξοπλισμού του VPN

## 3.2 Τοίχος ασφαλείας (firewalls)

Το firewalls είναι ένα λογισμικό ή ένα κομμάτι Hardware που λειτουργεί σαν προστατευτικό φράγμα μεταξύ του υπολογιστή και του υπόλοιπου ψηφιακού κόσμου παρέχοντας ασφάλεια από απειλές.

Κάθε ψηφιακή πληροφορία που εισέρχεται ή εξέρχεται από ένα δίκτυο περνάει μέσα από το firewall ,το οποίο με βάση συγκεκριμένα κριτήρια ασφαλείας θα επιτρέψει ή θα μπλοκάρει την είσοδο τους.

Τι κάνει το **firewall :**

- Αποτρέπει μη εξουσιοδοτημένους χρήστες ν αποκτήσουν πρόσβαση στον υπολογιστή και στο δίκτυο
- Παρακολουθεί την επικοινωνία του υπολογιστή του χρήστη με τους άλλους υπολογιστές στο internet.
- Δημιουργεί ένα τοίχος ασφαλείας που εμποδίζει τους κακόβουλους εισβολείς και προειδοποιεί το χρήστη για την προσπάθειά τους να συνδεθούν στον υπολογιστή.
- Προειδοποιεί αν κάποια εφαρμογή του υπολογιστή του χρήστη προσπαθεί να συνδεθεί με άλλους υπολογιστές στο internet .

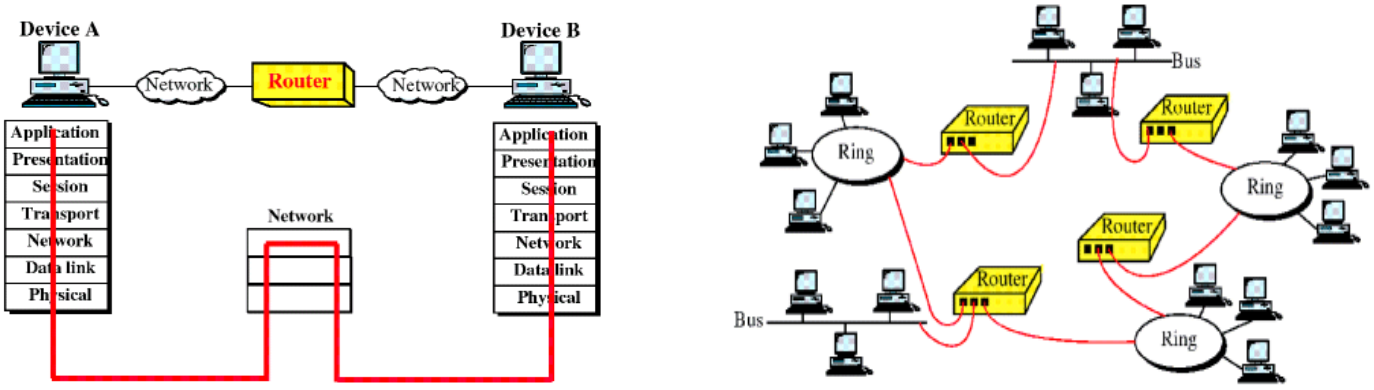
Οι firewalls παρόλο τη συμμετοχή τους σε θέματα ασφαλείας του δικτύου λόγω του ότι δεν μπορούν να ελέγξουν αν έχει γίνει στα πακέτα δεδομένων, κάποια αλλαγή κατά τη μεταφορά τους στο PSTN δεν μπορούμε να ισχυριστούμε ότι μπορούν από μόνοι τους να παρέχουν ασφάλεια στα VPNs. Αφού ο ρόλος τους είναι να έχουν γενική επίβλεψη του όλου δικτύου και προστατεύουν γενικά την επιχείρηση μπορούμε να πούμε ότι συμμετέχουν συμπληρωματικά στις όλες εφαρμογές ασφάλειας.

Στην εγκατάστασή τους εφιστούν μεγάλη προσοχή αφού είναι περίπλοκοι στο χειρισμό τους . Για καλύτερη διαχείριση προτείνεται να υπάρχει σε όλους τους firewalls που συμμετέχουν στο δίκτυο, το ίδιο configuration .

Μια ακόμη ιδιαιτερότητα των firewalls είναι πως είναι απαραίτητος ο εφοδιασμός των remote users με ιδικό software το οποίο να είναι συμβατό με το firewall. Γιατί υπάρχουν δύο περιπτώσεις. Στην πρώτη αν το VPN χρησιμοποιεί τα πρωτόκολλα PPTP και L2TP( που θα τα δούμε σε ποιο κάτω κεφάλαιο )τότε ο firewall αφήνει τα VPN πακέτα να περνούν αφού τα PPTP και L2TP τερματίζονται στο network service . Στη δεύτερη περίπτωση αν χρησιμοποιείτε το IP sec τότε είναι πολύ επικίνδυνος ο συνδυασμός των δύο γιατί υπάρχει πιθανότητα ασυμβατότητας των αλγορίθμων και των πρωτοκόλλων. Για τους λόγους αυτούς δεν προτείνετε η χρήση τους σε μεγάλα δίκτυα υψηλών απαιτήσεων.

### 3.3 Δρομολογητές (Routers )

Είναι συσκευές που σκοπό έχουν να ελέγχουν την κίνηση των πακέτων.




**Εικόνα 7: η θέση ενός δρομολογητή στο μοντέλο OSI και η μετάβαση πληροφοριών σε πολλά διασυνδεδεμένα δίκτυα.**

Γενικά ,

- Έχουν πρόσβαση σε όλα τα επίπεδα του δικτύου .
- Παρέχουν λογισμικό που τους επιτρέπει την επιλογή μονοπατιών δικτύου για την μετάδοση.
- Λειτουργούν στο επίπεδο διασύνδεσης δεδομένων.
- Μεταβιβάζουν πληροφορίες μεταξύ πολλών διασυνδεδεμένων δικτύων.
- Λαμβάνουν πακέτα από το δίκτυο και επιλέγουν την καλύτερη διαδρομή για την μετάδοσή τους μέσα στο δίκτυο.
- Δημιουργούν πίνακες δρομολόγησης ,οι οποίοι εμπεριέχουν τις διευθύνσεις όλων των συσκευών του δικτύου και προωθούν τα πακέτα σύμφωνα με αυτόν .
- Δεν μπορούν να συνδεθούν δίκτυα διαφορετικού τύπου . Για το λόγο αυτό χρησιμοποιούν πύλες (gateways ).
- Για την λειτουργία τους απαιτούν χρήση πρωτοκόλλων .
- Είναι συσκευές που μπορούν να εκπληρώσουν VPN λειτουργίες .

**Όμως πρέπει να πληρούν κάποια κριτήρια :**

- Να ενσωματώνουν δυνατότητα για ξεχωριστές ειδήσεις .
- Να υποστηρίζουν τους βασικούς IP sec ,PPTP και L2TP αλγορίθμους . Transport και tunnel IP sec mode, interplay και IPsec2 και τέλος κρυπτογραφικούς μηχανισμούς.
- Επιτρέπουν επεμβάσεις στο configuration .

Η αδυναμία τους είναι πως δεν παρέχουν πιστοποίηση ταυτότητας του χρήστη (authentication ) οπότε χρειάζονται συμπληρωματικά τα authentication server.

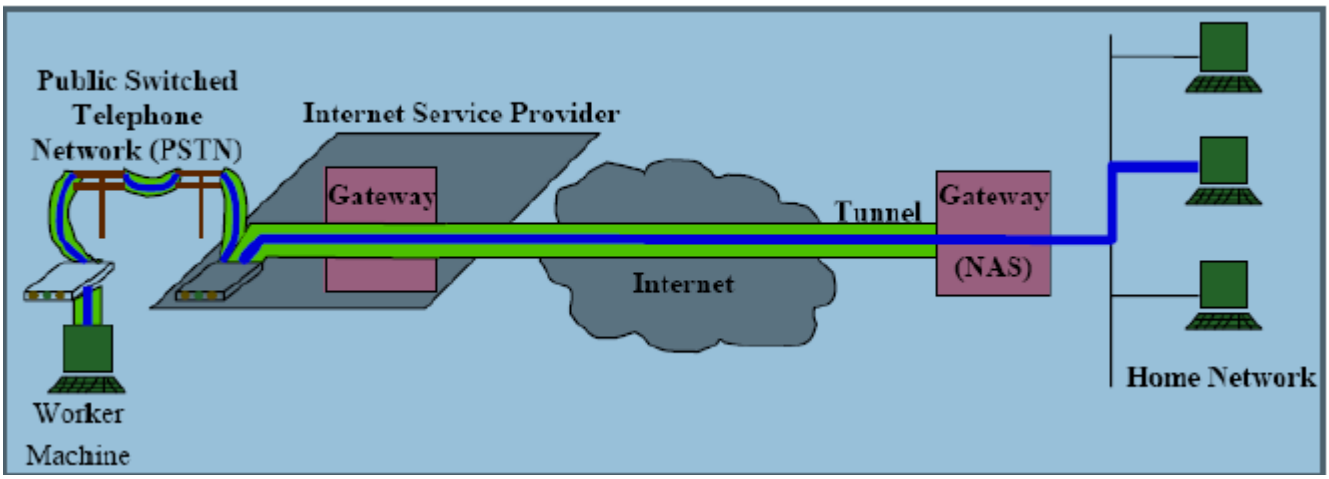
**Κεφάλαιο 4$^{ο}$ :Αρχιτεκτονικές Εικονικών Ιδιωτικών Δικτύων (VPNs)**

Οι τρόποι κατηγοριοποίησης των **VPNs** διαφέρουν κάθε φορά ,ανάλογα με την οπτική γωνία εξέτασης τους.

Μπορείς κανείς να τα κατηγοριοποιήσει είτε :

- Σύμφωνα **με την αντιστοιχία τους με το επίπεδο μεταφοράς OSI** . Όπου εδώ έχουμε 3ης υποκατηγορίες :
  - **VPNs επιπέδου 3 (Δικτύων )**
  - **VPNs επιπέδου 2 (Ζεύξης δεδομένων)**
  - **VPNs επιπέδου 4 (μεταφοράς)**
- Σύμφωνα **με τους χρήστες**
  - **VPN δομής <<πελάτη –προς- δίκτυο>> (client- to- LAN )**

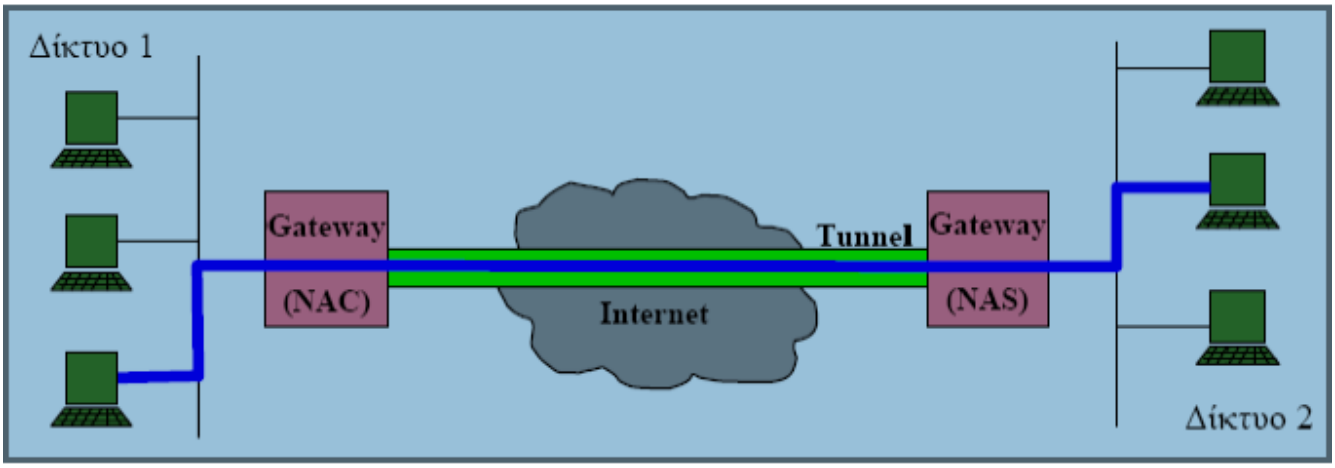
Η σύνδεσή του χρήστη γίνετε σ’ ένα τοπικό δίκτυο .




**Εικόνα 8 : <<πελάτη –προς- δίκτυο>> (client- to- LAN ) VAN**

- **VPN δομής << δίκτυο-προς –δίκτυο >> ( LAN -to- LAN)**

Η δίοδος μεταφοράς των δεδομένων αναπτύσσεται μεταξύ δύο τοπικών δικτύων .




**Εικόνα 9 : << δίκτυο-προς –δίκτυο >> ( LAN -to- LAN) VPN**

Και τέλος

➢ Σύμφωνα με το **είδος της διόδου (tunnel) ,του νοητού κυκλώματος που δημιουργείτε για την μετάδοση των δεδομένων .**

- << **αυθόρμητες δίοδοι** >>

Δημιουργούνται μετά από αίτηση του χρήστη .

- <<**αναγκαστικές δίοδοι** >>

Δημιουργούνται αυτόματα χωρίς επέμβαση του χρήστη .

Στο κεφάλαιο αυτό θα ασχοληθούμε εκτενέστερα με την πρώτη κατηγορία **VPNς επιπέδου μεταφοράς OSI.**

### 4.1 VPNs επιπέδου 3 (Δικτύου)

Στην κατηγορία των δικτύων επιπέδου 3 η πληροφορία που θα μεταδοθεί μετατρέπετε σε IP πακέτα και μεταδίδετε στο IP δίκτυο.

Το IP είναι πρωτόκολλο 3$^{ου}$ επιπέδου και δίνει τη δυνατότητα σε ηλεκτρονικούς υπολογιστές να διασυνδεθούν μεταξύ τους είτε ανήκουν στο ίδιο δίκτυο είτε όχι .

Τα πακέτα μεταδίδονται με την τεχνική datagram's .

Το κάθε πακέτο του IP φθάνει στον παραλήπτη περνώντας μέσα από ένα ή περισσότερα διασυνδεδεμένα δίκτυα IP ,διατηρώντας την αυτονομία του μέσα στο δίκτυο. Δηλαδή το κάθε πακέτο δεν εξαρτάται από το προηγούμενο ή το επόμενο πακέτο.

Το IP ασχολείται με την διευθυνσιοδότηση ,τον κατακερματισμό μεγάλων πακέτων και την ανασυγκόλληση τους .

Το κόστος τους είναι χαμηλό λόγο της αντικατάστασης των αφιερωμένων γραμμών από δημόσιες τοπικές συνδέσεις οι οποίες παρέχουν άνεση στις συνδέσεις εκτός δικτύου με άλλους χρήστες.

Η αξιοπιστία του όμως δεν είναι και τόσο μεγάλη εφόσον δεν εξασφαλίζει την ακεραιότητα των δεδομένων από την μια άκρη ως την άλλη μέσω κάποιων τεχνικών επανεκπομπής ή ελέγχου ροής .

Επίσης για την παροχή μέγιστης ασφάλειας των δεδομένων που κινούνται στο περιβάλλον δημοσίου δικτύου internet χρειάζεται η εφαρμογή τεχνικών κρυπτογράφησης.

#### 4.1.1 MPLS /VPNs Δικτύων

Λόγο της αδυναμίας των δρομολογητών να μην μπορούν να κρατήσουν πληροφορίες για τον τρόπο που δρομολογείτε ένα πακέτο, εφόσον μετά τη δρομολόγηση ο δρομολογητής επανέρχεται στην πρωταρχική του κατάσταση και δρομολογεί άλλα ανεξάρτητα πακέτα. Καθώς επίσης και το μειονέκτημα τους να προωθούν τα πακέτα με μοναδικό κριτήριο τον προορισμό τους μέσω μιας επαναλαμβανόμενης ενέργειας της μεταγωγής και της δρομολόγησης, γεννήθηκε η ανάγκη δημιουργίας μιας τεχνολογίας η οποία θα μπορεί να υποστηρίξει τα IP πρωτόκολλα και εφαρμογές σε συνδυασμό με την παροχή νέων υπηρεσιών.

Έτσι δημιουργήθηκε το πρωτόκολλο MPLS .

Το MPLS είναι δημιούργημα της IETF. Συνδυάζει την μεταφορά των πακέτων με ετικέτα(label) με την παραδοσιακή δρομολόγηση του IP .Στόχος είναι η αύξηση της ευελιξίας και της απόδοσης του πρωτοκόλλου IP καθώς και η δυνατότητα παροχής υπηρεσιών στο internet.Αυτό επιτεύχθηκε με τη συνεργασία γνωστών πρωτοκόλλων και του MPLS.

Για την υλοποίηση των **MPLS /VPNs** συνεργάζονται δύο τεχνολογίες οι **MPLS** και **BGP** όπου η πρώτη προωθεί τα πακέτα και η δεύτερη διανέμει τις διαδρομές ή τις ετικέτες.

Το **BGP** είναι πρωτόκολλο ανταλλαγής πινάκων δρομολόγησης μεταξύ των παρόχων. Είναι πολύ ευέλικτο. Επιτρέπει ή απαγορεύει την μορφοποίηση μέρους ή ολόκληρου του πίνακα δρομολόγησης. Επιτρέπει ή

απαγορεύει την πρόσβαση από /προς συγκεκριμένα <μέλη> ενός VPN. Επιλέγει ποια από τις διαδρομές θα είναι η κύρια και ποια η δευτερεύουσα και γενικότερα είναι εκείνο που επιλέγει τον τρόπο που θα μεταφερθεί η πληροφορία δρομολόγησης στην υλοποίηση των MPLS/VPNs.
Χρησιμοποιώντας το BGP γίνονται γνωστοί στους δρομολογητές PE οι πίνακες δρομολόγησης των VPNs που συνδέονται σε άλλους PE δρομολογητές

***Τι προσφέρει το MPLS πρωτόκολλο.***

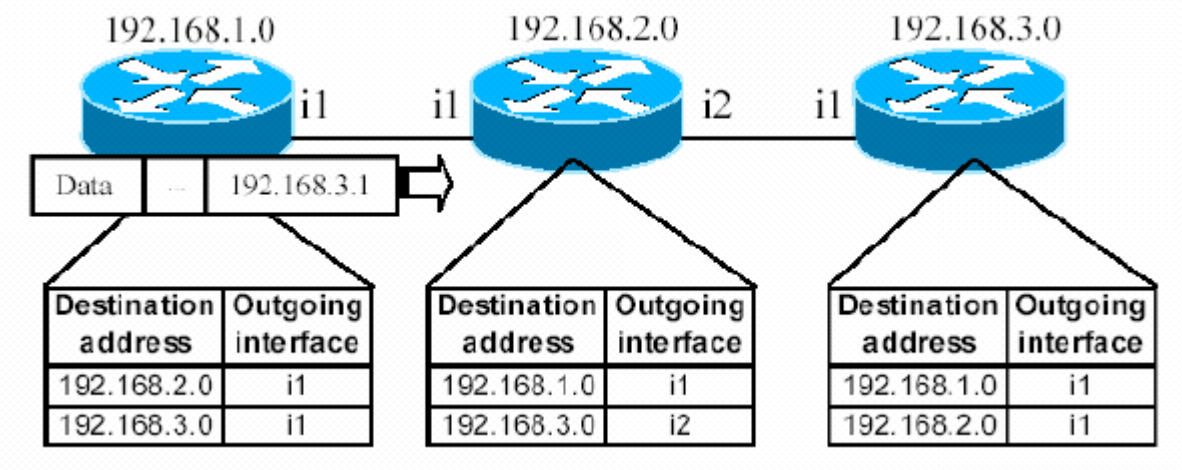
Αυτό που προσφέρει το **MPLS** πρωτόκολλο είναι ο διαχωρισμός των διαδικασιών της δρομολόγησης και της μεταγωγής σ ένα δρομολογητή. Η διαδικασία αυτή γίνεται μέσω του LSR (Label switching Router ) δρομολογητή ο οποίος προωθεί τα πακέτα μέσω μιας ετικέτας που υπάρχει στην κεφαλή του πακέτου.
Οι LSRs δρομολογητές χρησιμοποιούν το πρωτόκολλο **MPLS** δανειζόμενοι και χαρακτηριστικά των παραδοσιακών IP πρωτοκόλλων για να φτιάξουν πίνακες δρομολόγησης .Η μεταγωγή των πακέτων γίνεται μέσω του μεταγωγέα (ATM ).
( Το ATM μια μέθοδος για μεταφορά, πολυπλεξία και μεταγωγή πληροφορίας πολλών ειδών (data, video, audio) με υψηλές ταχύτητες μέσω ενός απλού μηχανισμού μετάδοσης και μεταγωγής.)

***Πως γίνεται η μεταγωγή των MPLS πακέτων***

Κατά την είσοδο κάθε πακέτου στο δίκτυο MPLS τοποθετείτε μια ετικέτα( label) από την οποία εξαρτάτε η απόφαση δρομολόγησης του πακέτου. Κατά την έξοδο του πακέτου από το δίκτυο MPLS η ετικέτα απομακρύνεται .Οι ετικέτες δείχνουν τόσο τη δρομολόγηση των πακέτων όσο και τα χαρακτηριστικά ποιότητας αυτών.

***Πως γίνεται η προώθηση των MPLS πακέτων***

Κατά την προώθηση των πακέτων σ ‘ ένα MPLS δίκτυο αρχικά εκτελούνται τα παραδοσιακά πρωτόκολλα δρομολόγησης IP,δημιουργώντας τους πίνακες δρομολόγησης με συγκεκριμένα πρωτόκολλα. Στη συνέχεια οι LSRs δρομολογητές για κάθε εγγραφή του πίνακα δρομολόγησης επικοινωνούν με τους γείτονες κόμβους για ν ‘ανταλλάξουν ετικέτες οι οποίες θα χρησιμοποιηθούν για την μεταγωγή των πακέτων . Τέλος τα δεδομένα στέλνονται σε πακέτα με την διεύθυνση προορισμού στην κεφαλή του καθ ‘ ενός πακέτου.




**Εικόνα 10: παραδοσιακός τρόπος δρομολόγησης**

***Διαφορές MPLS & IP ως προς τη δρομολόγηση***

Ενώ στη δρομολόγηση IP οι αποφάσεις για τη διαδρομή του πακέτου παίρνονται από τη διεύθυνση προορισμού. Στη MPLS δρομολόγηση υπολογίζονται κι άλλοι παράγοντες σχετικά με την τοπολογία δικτύου**.**

Επίσης, στη δρομολόγηση IP ο τρόπος που δημιουργούνται οι πίνακες δρομολόγησης και η ίδια η δρομολόγηση βασίζονται στην διερεύνηση των τριγύρω δικτύων βάση των IP διευθύνσεων , ενώ στη MPLS οι δύο αυτές διαδικασίες διαχωρίζονται σε forwarding plane και σε control plane προσφέροντας μεγαλύτερη ευελιξία .

**Από τι αποτελείτε ένα MPLS**

Ένα MPLS πρωτόκολλο αποτελείτε:

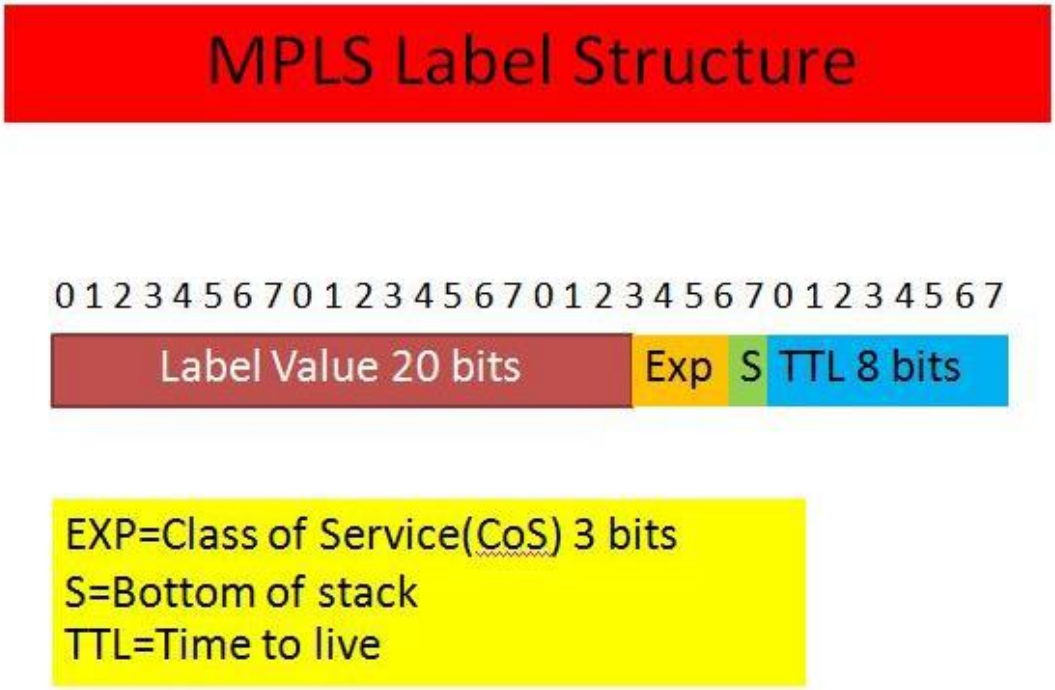
- από την **ετικέτα (Label)** την οποία χρησιμοποιούν οι δρομολογητές για την προώθηση των πακέτων.

Η τεχνολογία MPLS προσθέτει στα πακέτα μια επικεφαλίδα MPLS που περιέχει μια ή πολλές ετικέτες. Αυτή ονομάζεται ετικέτα σωρός και χρησιμοποιείτε από τους δρομολογητές ετικέτας LSRs την προώθηση των πακέτων.

Οι LSRs διαβάζουν μόνο τις ετικέτες αυτού του τύπου και όχι τις επικεφαλίδες των πακέτων IP. Επίσης οι ετικέτες έχουν νόημα μόνο όταν επικοινωνούν δύο συσκευές μεταξύ τους.

Η ετικέτα αποτελείτε από 32bit εκ των οποίων :

- ✓ Label (20 bits): όπου περιέχει την πληροφορία ετικέτας .
- ✓ QOS (Quality Of Service (3 bits)): περιέχει την πληροφορία για την ταξινόμηση ή την απόρριψη πακέτων.
- ✓ Bottom Of Stack Flag (1 bit): δείχνει αν η τρέχουσα ετικέτα είναι η τελευταία από το σωρό ετικετών.
- ✓ Time to Live –TTL(8 bits): χρόνος ζωής του πακέτου.




**Εικόνα 11:δομή ετικέτας**

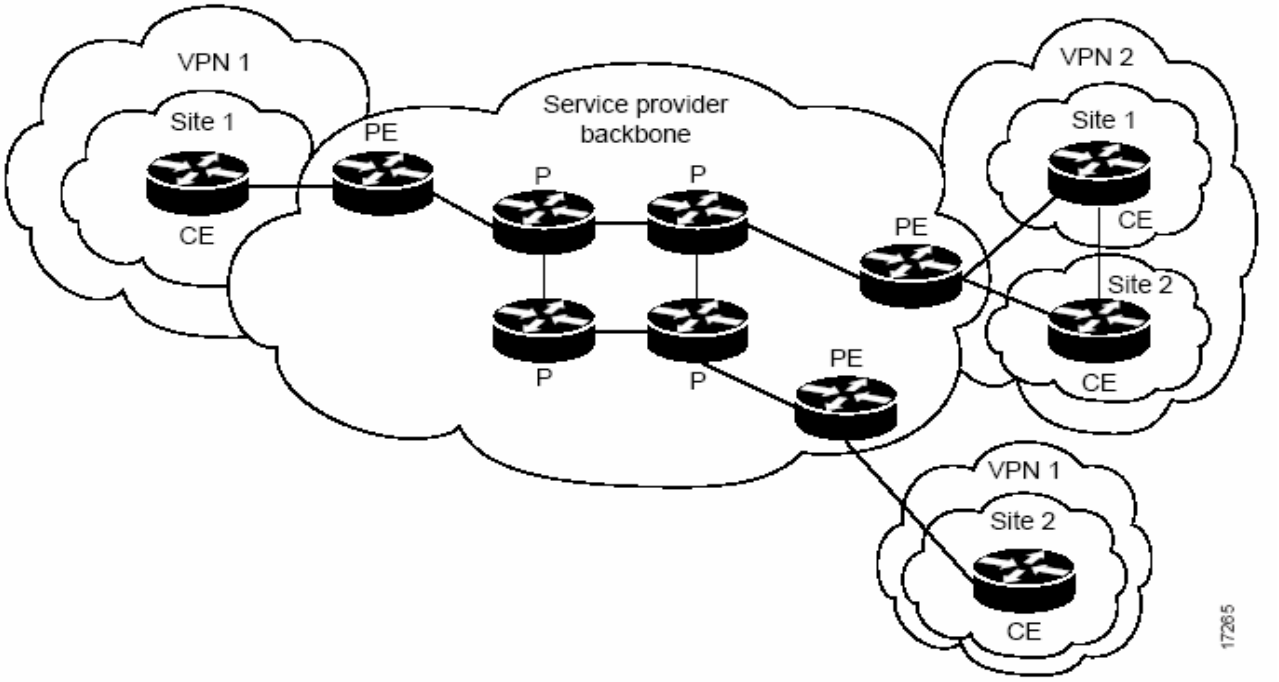
- Από τους **δρομολογητές ετικέτας (Ladel Switch Router (LSR))** .Είναι οι συσκευές κορμού του δικτύου MPLS που μεταφέρουν τα πακέτα εφοδιασμένα με την κατάλληλη ετικέτα όπως την καθορίζουν οι πίνακες μεταγωγής. Οι ετικέτες εδώ δεν είναι και τόσο χρήσιμες ,όμως τις διαβάζει ώστε να κάνει τη δρομολόγηση.

- Από τους **δρομολογητές ετικέτας άκρου(Edge Label Switch Router(Edge LRS**)). Είναι η συσκευή που βρίσκεται στο άκρο του κυρίως δικτύου MPLS και συγχρόνως κατηγοριοποιεί το κάθε IP πακέτο και του εκχωρεί την πρώτη ετικέτα. Στο τελικό άκρο του δικτύου ο Edge LRS αφαιρεί την ετικέτα και επαναφέρει το IP πακέτο στην αρχική του κατάσταση .

- Από το **μονοπάτι ετικέτας( Label Switch Path(LSP)).** Είναι η διαδρομή που ορίζεται από τις ετικέτες και δίνεται στο κάθε πακέτο ,μεταξύ των τελικών σημείων του δικτύου. Ένα μονοπάτι ετικέτας μπορεί να είναι είτε στατικό είτε δυναμικό. Τα δυναμικά LSPs προσδιορίζονται αυτόματα κάνοντας χρήση των πληροφοριών δρομολόγησης ενώ τα στατικά χρησιμοποιούνται ποιο σπάνια. **Το LSP πολλές φορές καλύπτει ανάγκες εύρους** ζώνης ,αποφυγή πιθανών σημείων συμφόρεσης ή ποιότητα υπηρεσίας.

- Και τέλος από το **πρωτόκολλο διανομής ετικετών(Label Distribution protocol (LDP))**. Αυτό αναθέτει ετικέτες στα πακέτα από τις δικτυακές συσκευές στις άκρες και στον πυρήνα του δικτύου έτσι ώστε να καθοριστούν τα αναγκαία LSPs και μεταφράζει τις πληροφορίες από τους LSRs. Η ανάθεση γίνεται σε συνδυασμό με άλλα πρωτόκολλα δρομολόγησης όπως είναι το RIP,BGP,IS-IS κτλπ.

**Είδη δρομολογητών στα MPLS/VPNs**




**Εικόνα 12: Δρομολογητές *MPLS/VPNs***

Τα είδη των δρομολογητών που συναντάμε στην τεχνολογία MPLS/VPNs είναι οι ***:***

- **CE (Customer Edge ).** Οι δρομολογητές αυτοί ανήκουν και διαχειρίζονται από τον πελάτη.
- **P (Provider**). Είναι οι δρομολογητές που δεν συντηρούν τα VPNs δρομολόγια. Αποτελούν το δίκτυο κορμού του ISP και διαχειρίζονται από αυτό . Ο ρόλος τους είναι να προωθούν τις MPLS ετικέτες προς τους δρομολογητή PE (Provider Edge ) Routers. Οι P δρομολογητές όπως είπαμε δεν συμμετέχουν στη δρομολόγηση των VPNs ανταλλάσουν μόνο ετικέτες για να δημιουργήσουν MPLS LSPs μεταξύ των δρομολογητών.

Οι PEs προκειμένου να μεταφέρουν την κίνηση μεταξύ των «μελών» των VPNs χρησιμοποιούν τα LSPs.

Για να γνωρίζει κάθε φορά ο PE δρομολογητής σε ποιο VPN θα παραδώσει το πακέτο του χρήστη δίνεται μια ακόμα ετικέτα η οποία αναφέρετε σε συγκεκριμένο VPN. Έτσι τα MPLS πακέτα παρέχουν δύο ετικέτες. Μια για τη δρομολόγηση του πακέτου μεταξύ των κόμβων του παρόχου ISP και άλλη μια για την ταυτοποίηση του VPN .

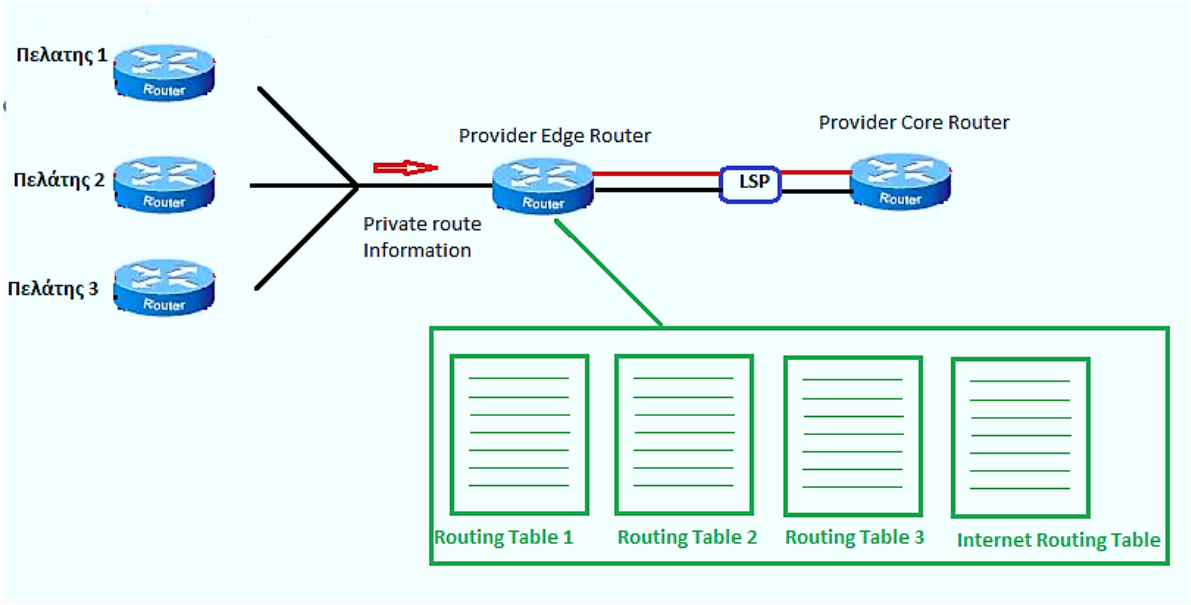
- **PE (Provider Edge). Οι** δρομολογητές αυτοί αποτελούν τα σημεία εισόδου και εξόδου των VPNs. Διαχειρίζονται από τον ISP και είναι το ποιο σημαντικό τμήμα ‘’λογικής ‘’των MPLS.

Κατανέμουν τις πληροφορίες δρομολόγησης των VPNs και προσανατολίζουν τους πίνακες δρομολόγησης που ανήκουν σε κάθε VPN. Η μετάδοση της πληροφορίας μεταξύ των δρομολογητών γίνεται μέσω του πρωτοκόλλου BGP.

Στους PE δρομολογητές λοιπόν με τη χρήση του MPLS ανταλλάσσονται MPLS ετικέτες δίνοντας την ευκαιρία να συνδεθούν και να επικοινωνήσουν μεταξύ τους <μέλη> ενός VPN με διαφορετικό όμως συνδεδεμένο PE.

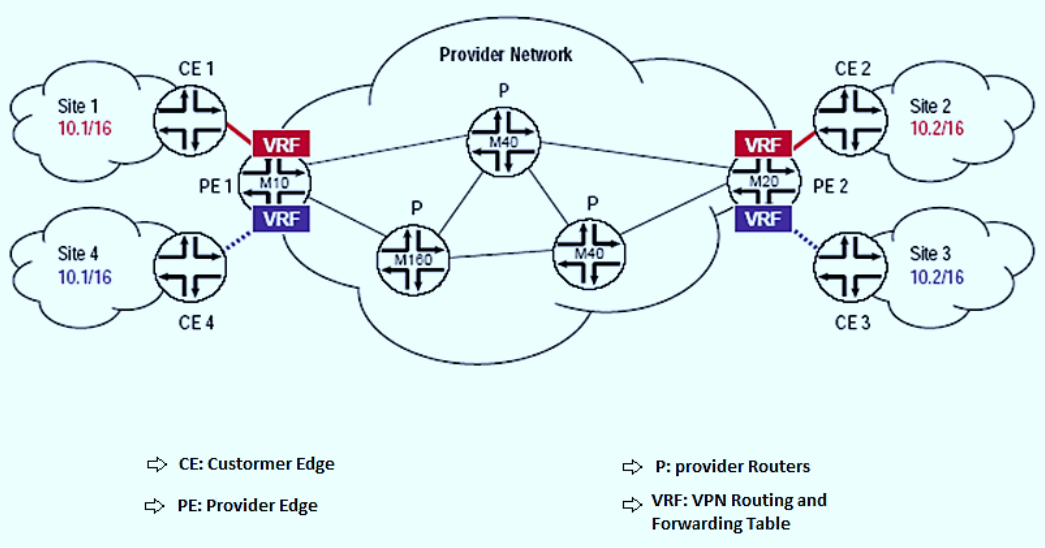
Κάθε PE συνδέεται με πολλούς πελάτες και διατηρεί έναν υποπίνακα δρομολόγησης που περιέχει την πληροφορία δρομολόγησης αποκλειστικά για κάθε έναν από αυτούς, προσφέροντας τους έτσι μέγιστη ασφάλεια.

Κάθε PE δρομολογητής είναι σαν ένα σύνολο από εικονικούς δρομολογητές (Virtual Routers)




**Εικόνα 13: πίνακας δρομολόγησης PE δρομολογητή .**

Κάθε πελάτης έχει το δικό του πίνακα δρομολόγησης ( Router table). Είναι ένας ανεξάρτητος εικονικός πίνακας δρομολόγησης και αποκαλείτε VRF(Virtual Routing & Firewall Instance ).

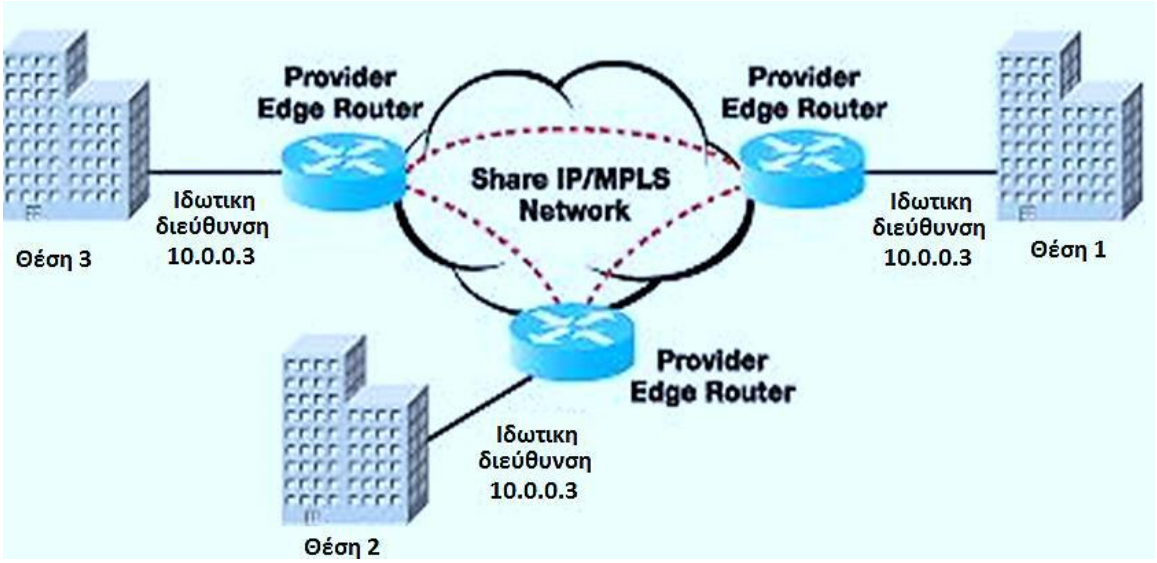



**Εικόνα 14: πίνακας δρομολόγησης VRF(Virtual Routing & Firewall Instance ).**

Για να προστεθεί ένα νέο μέλος στο VPN πχ. μιας εταιρίας χρειάζεται πρέπει ο πάροχος να ενημερώσει τον CE δρομολογητής του νέου πελάτη για το πώς θα συνδεθεί στο δίκτυο του παρόχου και να ανασχηματίσει τον PE δρομολογητή έτσι ώστε να του είναι γνωστός ο CE δρομολογητής του νέου πελάτη στο συγκεκριμένο VPN.

***VPN-IP διευθύνσεις***

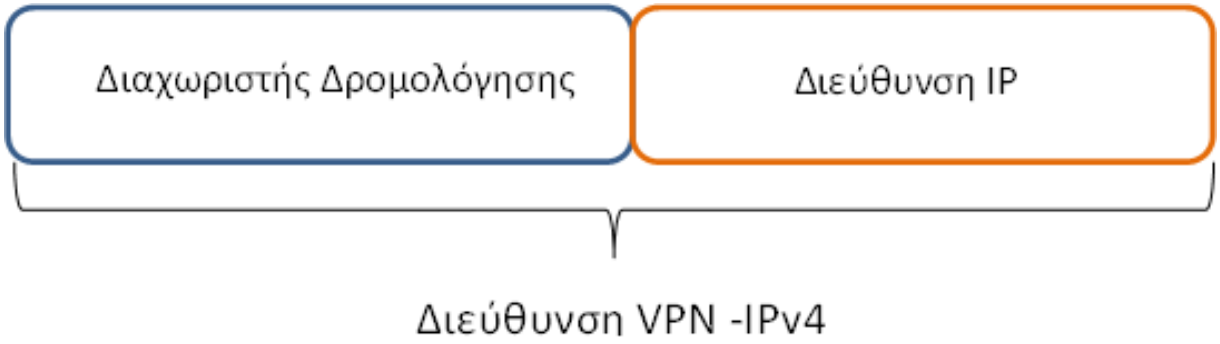
Οι διευθύνσεις που χρησιμοποιούνται στο ιδιωτικό δίκτυο δεν είναι μοναδικές. Έτσι είναι πολύ πιθανόν δύο υπολογιστές διαφορετικών δικτύων που θα συνδεθούν μέσω ενός VPN να έχουν κοινή διεύθυνση.




**Εικόνα 15: πρόβλημα κοινών διευθύνσεων**

Για το λόγο αυτό χρησιμοποιείτε το πρωτόκολλο NAT (Network Address Translator ).

Σε περίπτωση που ο πάροχος έχει MPLS δομή ,μπορεί να χρησιμοποιήσει τον διαχωριστή δρομολόγησης RD (Router Descriptor ). Αναθέτοντας σε κάθε VPN έναν RD ο οποίος είναι διαφορετικός για κάθε πελάτη και συνδέοντάς τον με την IP διεύθυνση του πελάτη δημιουργούνται IP διευθύνσεις οι οποίες είναι μοναδικές.




**Εικόνα 16 :μοναδικές διευθύνσεις**

***Τι προσφέρουν τα MPLS/VPNs***

- **Ανεξαρτησία από τη σύνδεση** .Τα MPLS/VPNs μπορούν να λειτουργήσουν και χωρίς σύνδεση.
- **Ευελιξία.** Η τεχνολογία MPLS/VPNs προσφέρει στους πελάτες της υπηρεσίες προστιθέμενης αξίας (values –added services) όπως( fax ,mms, φωνητικές κλείσεις ) καθώς και διαφορετικά επίπεδα ποιότητας υπηρεσιών (Quality of service )όπως (ποσοστά σφάλματος ,ρυθμός bit) για τη βελτίωση της συνολικής χρήσης του δικτύου . Επίσης λόγο της δυνατότητας που έχει να υλοποιείτε πάνω σε διαφορετικές αρχιτεκτονικές δικτύων μπορεί εύκολα να δημιουργηθεί VPN ανεξάρτητα από πόσες ή ποιες τεχνολογίες χρησιμοποιήθηκαν για τη φυσική σύνδεση των μελών.
- **Ευκολία εγκατάστασης**. Η αρχιτεκτονική του MPLS/VPNs δικτύου δίνει τη δυνατότητα σ ένα δίκτυο να κάνει αλλαγές στη δομή ή να αναδιαρθρωθεί με ευκολία. Αρκεί να κάνει αλλαγές στη διάταξη των δρομολογητών . επίσης δίνει τη δυνατότητα εύκολης εγκατάστασης τόσο στον πάροχο όσο και στον πελάτη.
- **Επεκτασιμότητα** . τα MPLS/VPNs προσαρμόζονται εύκολα στις αλλαγές που μπορεί να γίνουν στο δίκτυο μιας εταιρίας.
- **Κόστος υλοποίησης** . Αν ένας πελάτης θελήσει να προσθέσει στο δίκτυό του νέα περιφερειακά sites τα MPLS/VPNs προσφέρονται ως οι ποιο οικονομικές λύσεις εφόσον δεν απαιτούν αγορά αδειών χρήσης.
  Το κόστος τους είναι συνολικό κόστος χρήσης της μισθωμένης γραμμής και της διαχείρισης των VPNs από τον πάροχο.

- **Ασφάλεια** . στα MPLS/VPNs συνήθως δεν χρησιμοποιείτε η τεχνική κρυπτογράφησης .

  Ο πάροχος έχει τη δυνατότητα να διαμορφώσει το δίκτυο έτσι ώστε οι δρομολογητές του πελάτη να μην γνωρίζουν το δίκτυο κορμού του παρόχου και οι δρομολογητές κορμού να μην γνωρίζουν το δίκτυο του πελάτη.

  Στο MPLS δίκτυο τα πακέτα εισέρχονται μέσω PE router επομένως οτιδήποτε άλλο απορρίπτετε από το δίκτυο και η εισαγωγή τρίτων στο δίκτυο είναι σχεδόν αδύνατη.

### 4.1.2 Πρωτόκολλο IPSec

Επειδή τα TCP\ IP πρωτόκολλα δεν παρείχαν μηχανισμούς κρυπτογράφησης παρουσιάστηκε αδυναμία στην ασφάλεια μετάδοσης των δεδομένων πάνω σε IP δίκτυα. Έτσι δημιουργήθηκαν από την IEET τα αναπτυγμένα IPSec πρωτόκολλα που στόχευαν στην ασφαλή μετάδοση και ανταλλαγή δεδομένων μέσω του στρώματος IP χωρίς να χρειάζεται επιπλέον εξοπλισμό ούτε και τροποποίηση σε διάφορες εφαρμογές.

Το IPSec όπως είπαμε δημιουργήθηκε για να αντιμετωπίσει θέματα ασφάλειας όπως :

- **Απώλεια ιδιωτικότητας των δεδομένων ( Loss of privacy)**. Όταν ένας μη εξουσιοδοτημένος χρήστης έχει εισβάλει σε κάποιο δίκτυο και παρακολουθεί ιδιωτικά δεδομένα κατά τη μεταφορά τους στο internet.
- **Απώλεια ακεραιότητας δεδομένων (Loss of data integrity ).** Όταν ένας μη εξουσιοδοτημένος χρήστης τροποποιεί δεδομένα που μεταφέρονται στο internet.
- **Προσποίηση ταυτότητας (integrity spoofing ).** Όταν ένας μη εξουσιοδοτημένος χρήστης προσποιείτε ότι είναι νόμιμος χρήστης και αποσπά πληροφορίες .
- **Άρνηση υπηρεσιών ( Denial- of- service).** Όταν γίνεται επίθεση σε κάποιο server του δικτύου (π.χ. να αποστέλλονται ταυτόχρονα πολλά e-mails μαζί .)

Έτσι μπορούμε να πούμε ότι με την χρήση του IPSec πρωτοκόλλου προσφέρονται υπηρεσίες :

.

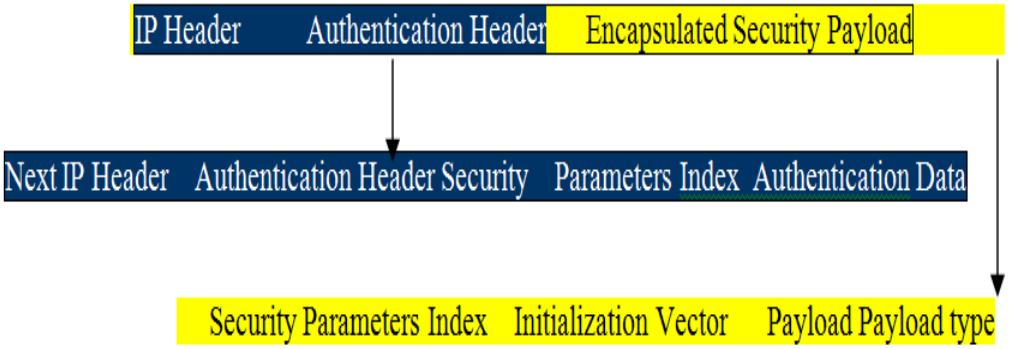
- **Ακεραιότητας δεδομένων (integrity):** εγγυάται την ασφαλή μεταφορά των πακέτων δεδομένων χωρίς τροποποιήσεις από «εισβολείς» ή από σφάλματα στην επικοινωνία .
- **Εξακρίβωση γνησιότητας προέλευσης των δεδομένων ( Authentication):** επαληθεύει και πιστοποιεί την ταυτότητα του αποστολέα των δεδομένων.
- **Εμπιστευτικότητα (confidentiality)** : δίνει τη δυνατότητα αναγνώρισης και τροποποίησης των δεδομένων μόνο σε συγκεκριμένους χρήστες.

  Για να εξασφαλίσει την επιτυχία προσφοράς των υπηρεσιών στις οποίες αναφερθήκαμε το IPSec , όρισε δύο νέα headers (επικεφαλίδες) σε κάθε IP πακέτο.

  - ***Της πιστοποίησης ( Authentication Header – AH ).***

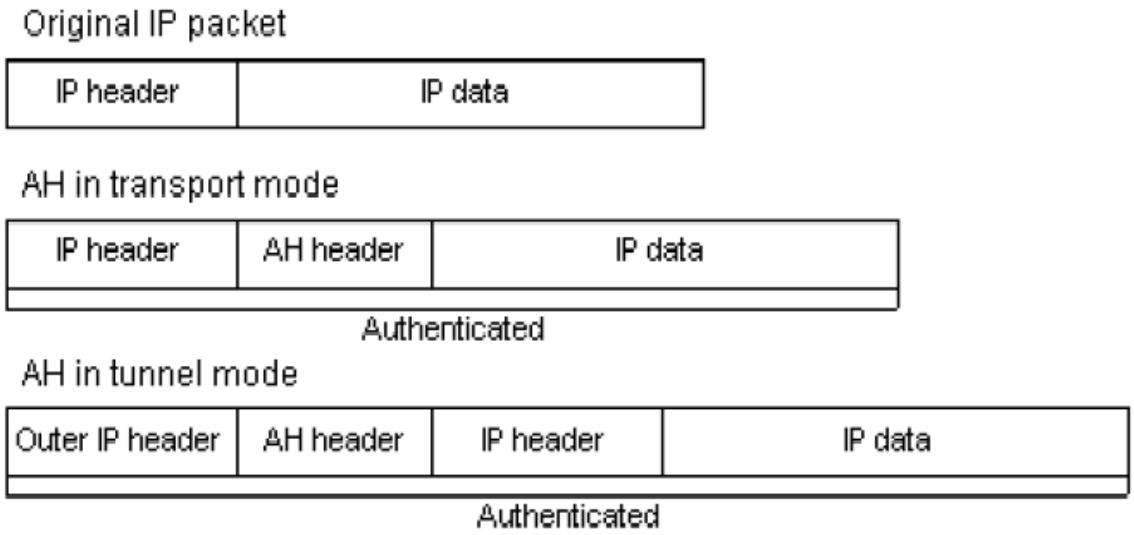
- ***Της ενθυλάκωσης ( Encapsulating security payload – ESP)***

Έτσι προέκυψαν νέα πακέτα IP μεγαλύτερα σε μέγεθος και με άλλη δομή.




**Εικόνα 17 : βασική δομή ενός IPsec πακέτου.**

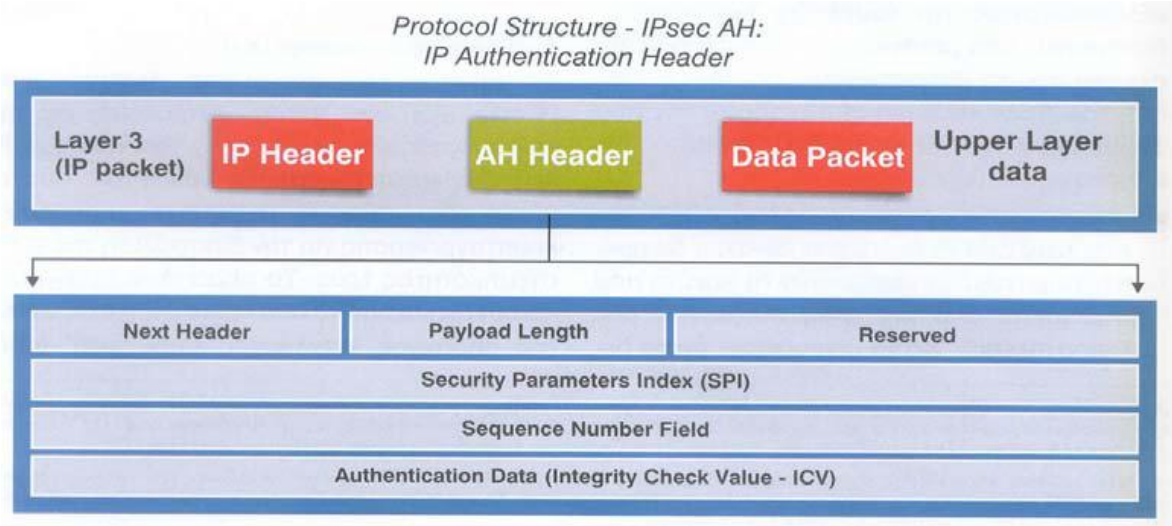
- ***Κεφαλίδα ποιστοποίησης ταυτότητας ( AH- Authentication Header)*** : εξυπηρετεί υπηρεσίες πιστοποίησης προέλευσης των δεδομένων ,αξιοπιστία δεδομένων και προστασία επανάληψης στα IP πακέτα και περιέχει ελέγχους κρυπτογράφισης με τη χρήση ενός κοινού κλειδιού(MAC) μεταξύ αποστολέα-δέκτη. Η κεφαλίδα αυτή μπαίνει μεταξύ των IP header και των πακέτων δεδομένων χωρίς να τα τροποποιεί .




**Εικόνα 18: προσθήκη κεφαλίδας πιστοποίησης AH σε IP πακέτο**

➢ ***Πεδία κεφαλίδας AH***

Η κεφαλίδα αποτελείτε από πέντε πεδία :




**Εικόνα 19 : πεδία IPsec AH**

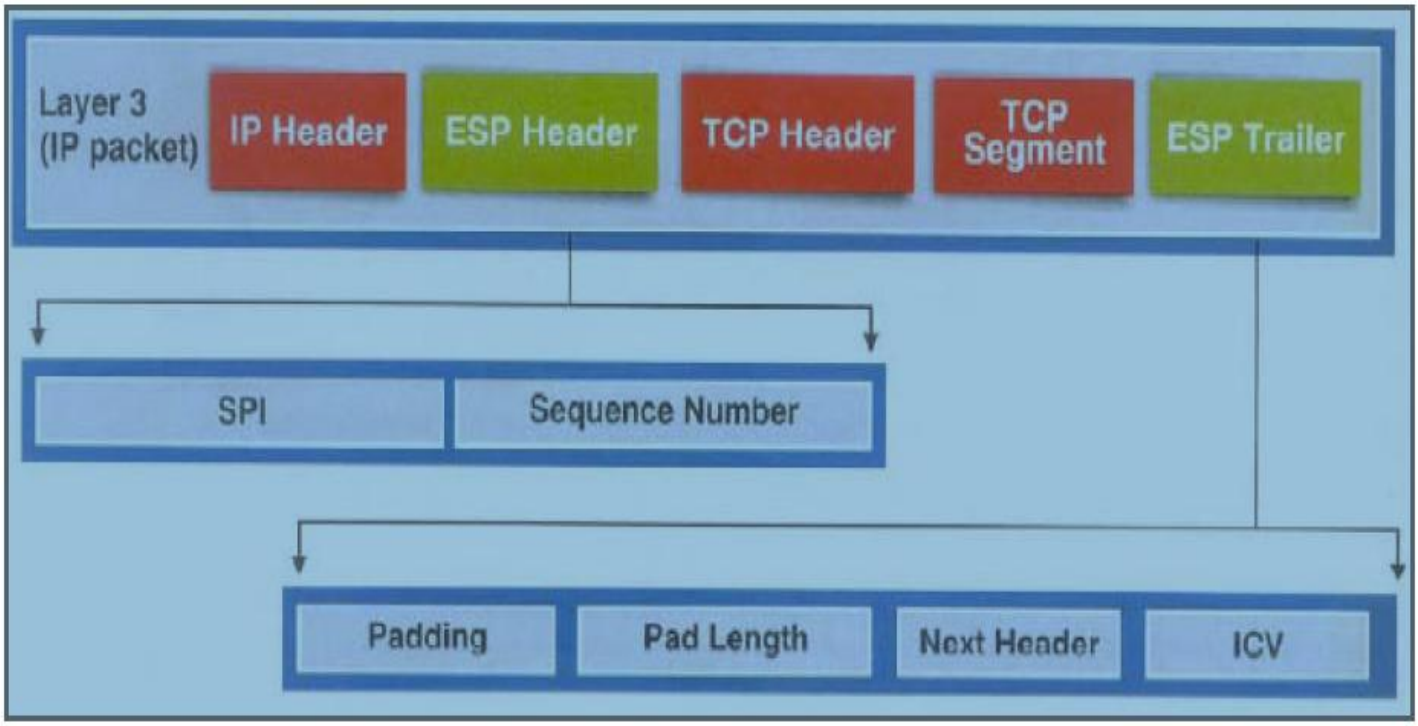
- **Πεδίο επόμενης κεφαλίδας ( Next header field).** Είναι ένα πεδίο 8bit που δίχνει ποια είναι η επόμενη κεφαλίδα που είναι παρούσα στο IP πακέτο .
- **Μήκος φορτίου ή μέγεθος φορτίου (Payload length).**
- **Δείκτη παραμέτρων ασφάλειας (security parameter index (SPI))** . ένας 32 bit αριθμός που πληροφορεί τον παραλήπτη για το ποια πρωτόκολλα ασφάλειας χρησιμοποιήσε ο αποστολέας.
- **Ακολουθειακός αριθμός.( Sequence numper).**Ένας 32 bit μετρητής ο οποίος αυξάνετε κατά ένα κάθε φορά που καταφτάνει ένα πακέτο στο δέκτη από τον ίδιο αποστολέα με το ίδιο SPI.
- **Δεδομένα πιστοποίησης ταυτότητας (Authentication data** ). Η ακεραιότητα και η πιστοποίηση πραγματοποιείτε από τα IPsec ακρέα μέλη του tunnel μέσω της συνάρτησης κατακερματισμού. Το μήκος του είναι μεταβλητό και μπορεί να είναι πολλαπλάσιο του μηκους 32 bit.

Τα ποιο σημαντικά πεδία είναι ο δείκτης παραμέτρων ασφάλειας που καθορίζει το είδος του πρωτοκόλλου που θα χρησιμοποιηθεί και η πιστοποίηση ταυτότητας των δεδομένων. Με τη χρήση του μηχανισμού interplay στο μετρητή πακέτων αποφεύγετε η υποκλοπή δεδομένων κατά τη διάρκεια αναμετάδοσης στο AH.

➢ ***Πεδία κεφαλίδας ESP***

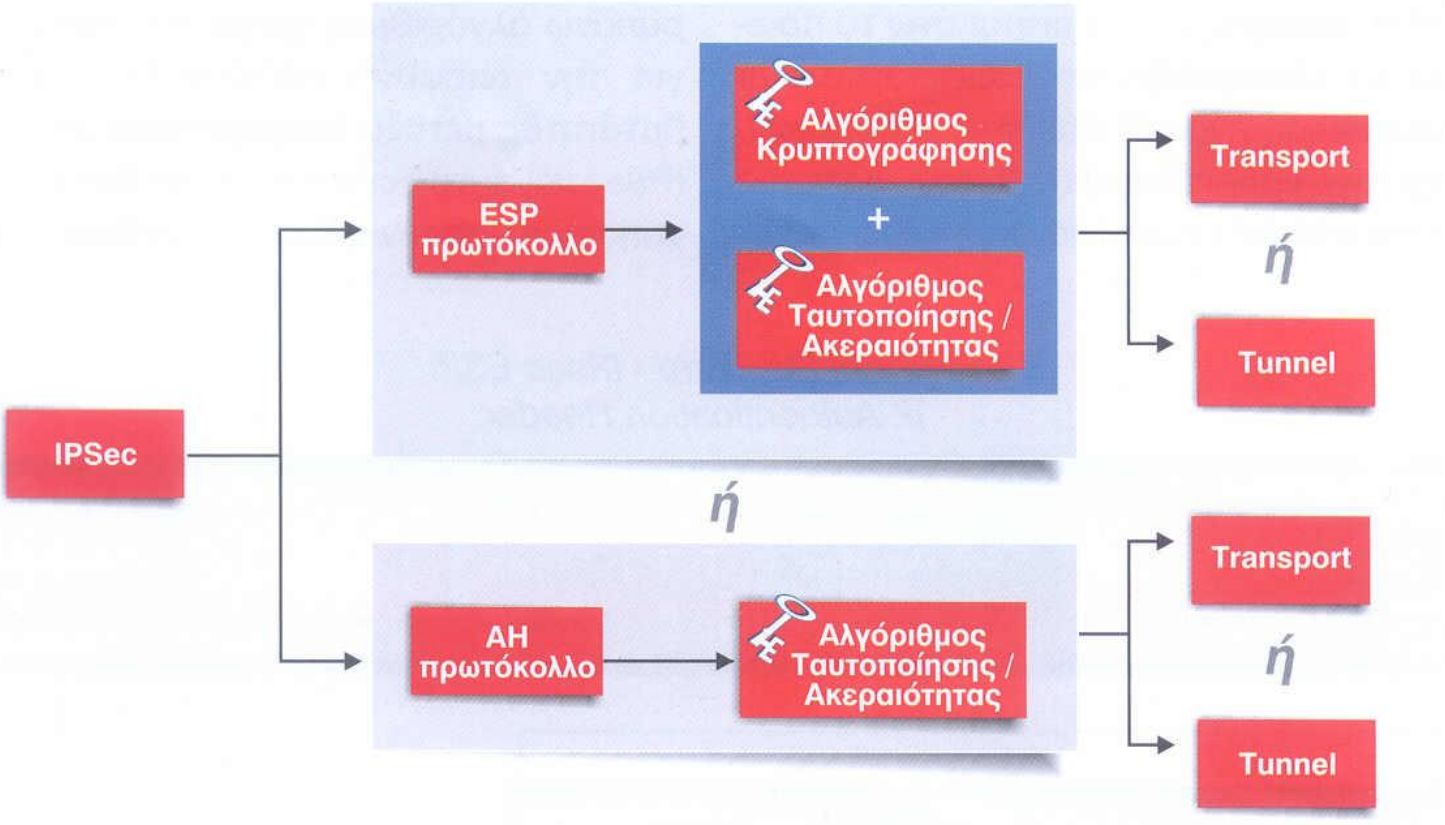
**Το ( Encapsulating security payload – ESP) αποτελείτε από έξι πεδία κεφαλίδας .** τα δύο τοποθετούνται πριν το φορτίο του IP πακέτου (ESP header )και τα τέσσερα επόμενα μετά (ESP trailer ) :

- **Πεδίο επόμενης κεφαλίδας ( Next header field).**
- **Μήκος φορτίου ή μέγεθος φορτίου (Payload length).**
- **Δείκτη παραμέτρων ασφάλειας (security parameter index (SPI)**
- **Ακολουθειακός αριθμός.( Sequence numper)**
- **Δεδομένα πιστοποίησης ταυτότητας (Authentication data )**
- **Padding .** Έχει μέγεθος 255 bytes το πολύ. Χρησιμοποιείτε για την προσαρμογή του μεγέθους του IP πακέτου ανάλογα με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιεί. Τα 5 πρώτα έχουν την ίδια λειτουργία όπως και στην AH κεφαλίδα.




**Εικόνα20: πεδία κεφαλίδας ESP.**

***Τρόποι λειτουργίας του IPsec***




**Εικόνα 21 :Τρόποι λειτουργίας IPSec**

Το IPSec λειτουργεί με δύο τρόπους (ανάλογα με τον τρόπο που θα τοποθετηθούν οι κεφαλίδες AH και ESP).

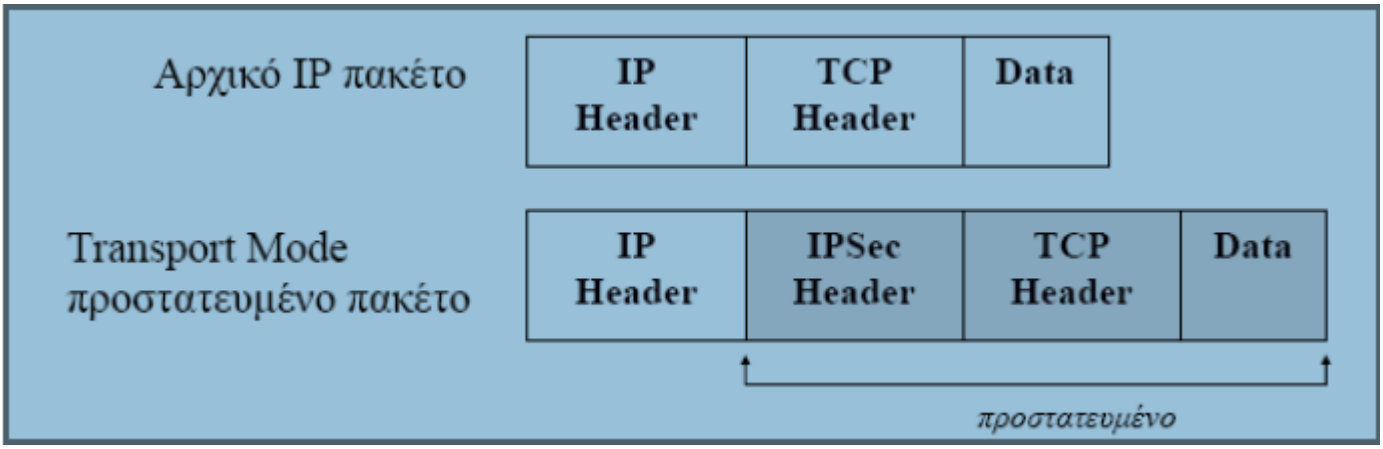
- ***Τρόπος μεταφοράς (transport mode )***
- ***Τρόπος διόδου (tunnel mode )***

- ***Τρόπος μεταφοράς (transport mode )***

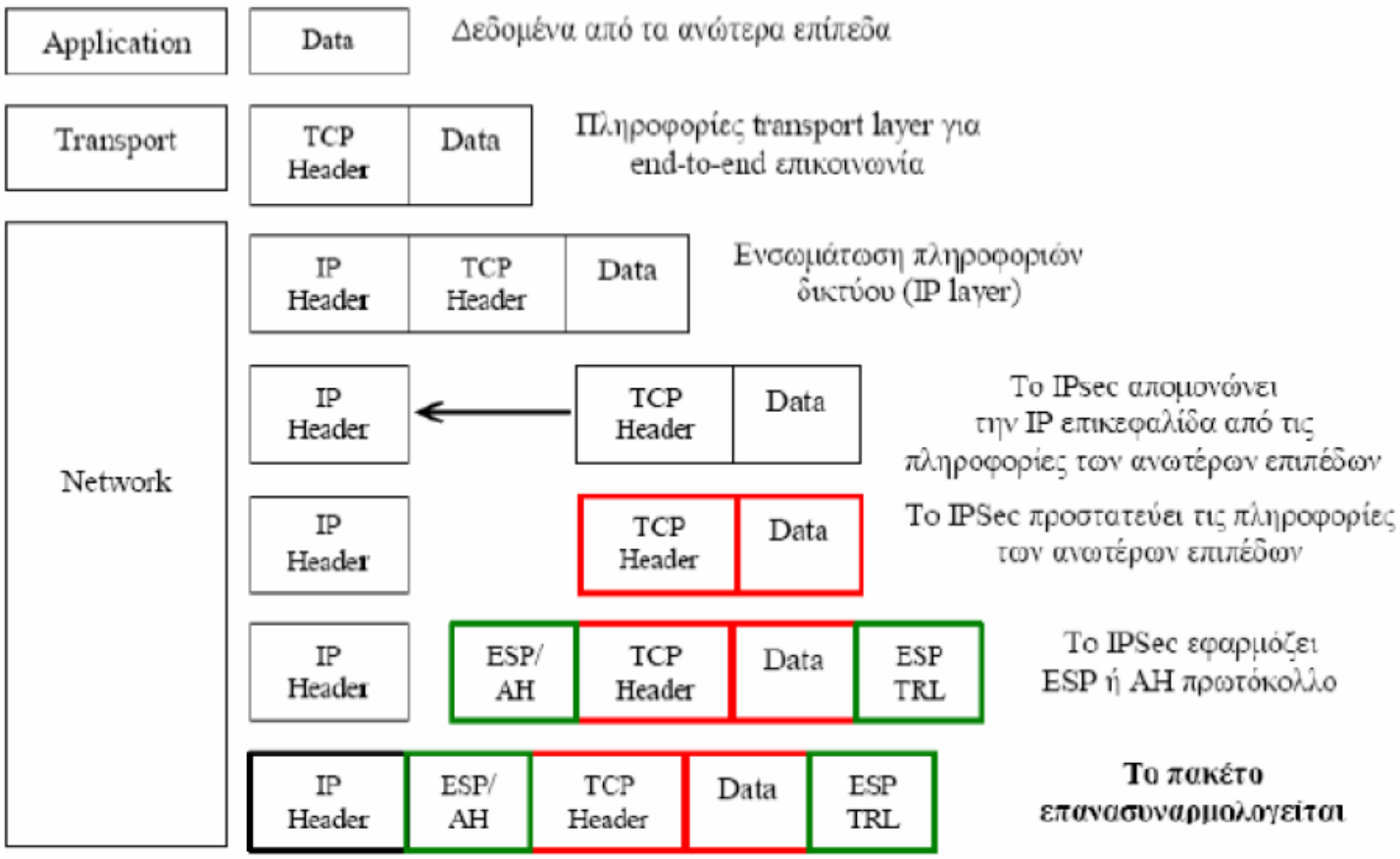
- Με ESP . Στην περίπτωση αυτή κρυπτογραφείται το αρχικό IP Payload και όχι η κεφαλίδα.
- Με AH. Εδώ αυθεντικοποιείται το αρχικό IP Payload και κάποια πεδία της IP κεφαλίδας, προσφέροντας από άκρο σε άκρο προστασία επικοινωνίας .Όμως η νέα επικεφαλίδα επιβαρύνει το κάθε πακέτο με bytes. Τέλος ,οι δρομολογητές δρομολογούν κατά συγκριμένο Qos (Quality of service) αφού μπορούν να δουν τις διευθύνσεις πηγής και προορισμού.

Μειονέκτημα του τρόπου αυτού είναι πως αφήνει την IP επικεφαλίδα χωρίς κρυπτογράφηση και οποιοσδήποτε κακόβουλος μπορεί να κάνει ανάλυση κίνησης.

Ο τρόπος αυτός χρησιμοποιείτε κυρίως για την σύνδεση μεταξύ δύο συσκευών δικτύων.




**Εικόνα 22 :τρόπος μεταφοράς (transport mode )**



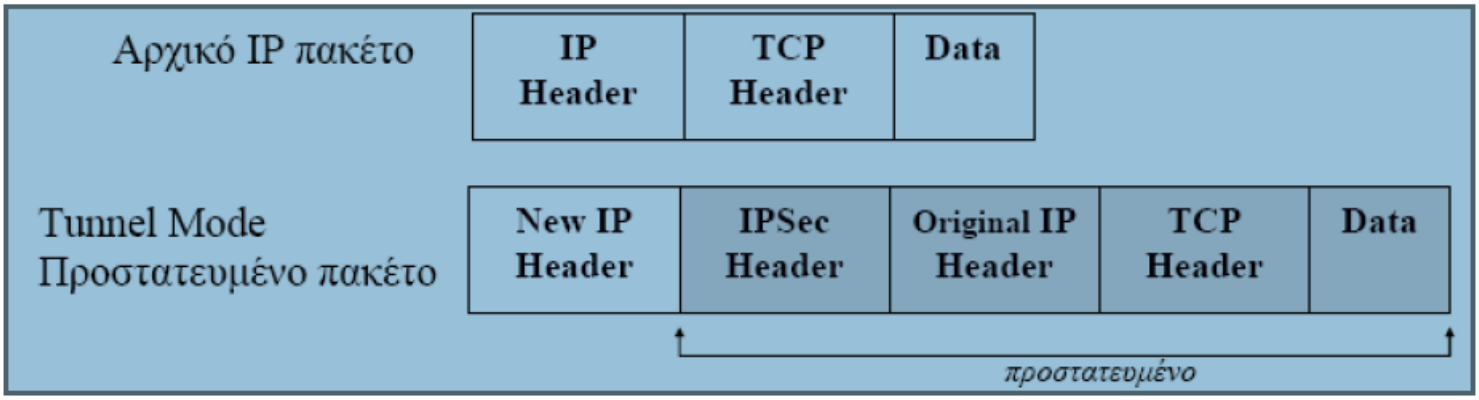

**Εικόνα 23 : Το IPsec σε κατάσταση μεταφοράς (transport mode )**

➢ ***Τρόπος διόδου( tunnel mode)***

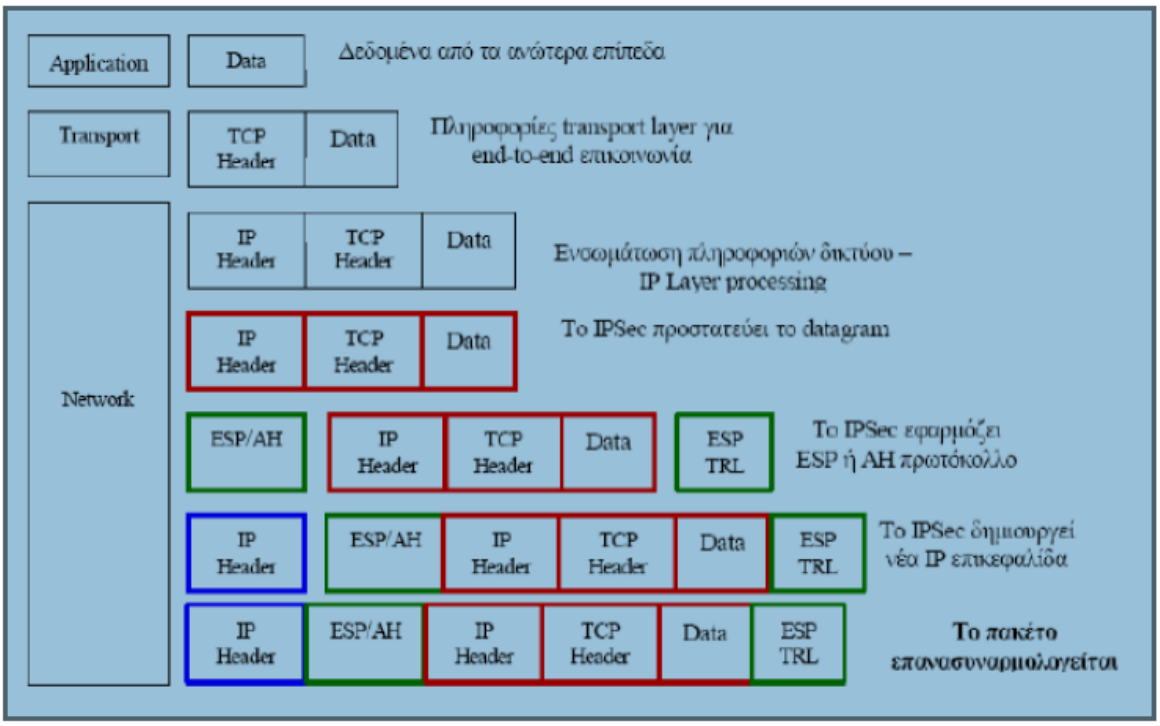
Στην περίπτωση αυτή το νέο IP πακέτο πηγαίνει από τον έναν δρομολογητή στον άλλον χωρίς να μπορούν να διαβάσουν το αρχικό πακέτο που βρίσκεται ενθυλακωμένο.

- Με ESP. Εδώ το αρχικό πακέτο κρυπτογραφείται ολόκληρο.
- Με AH . Αυθεντικοποιείται όλο το αρχικό IP πακέτο καθώς και κάποια πεδία της νέας κεφαλίδας. Οι δρομολογητές λειτουργούν ως IP proxies δηλαδή ,ο δρομολογητής –αποστολέας κρυπτογραφεί τα πακέτα και τα προωθεί στις IP sec διόδους (tunnel). Ο αποδέκτης δρομολογητής αποκρυπτογραφεί το αρχικό IP πακέτο και το προωθεί στον τελικό αποδέκτη.

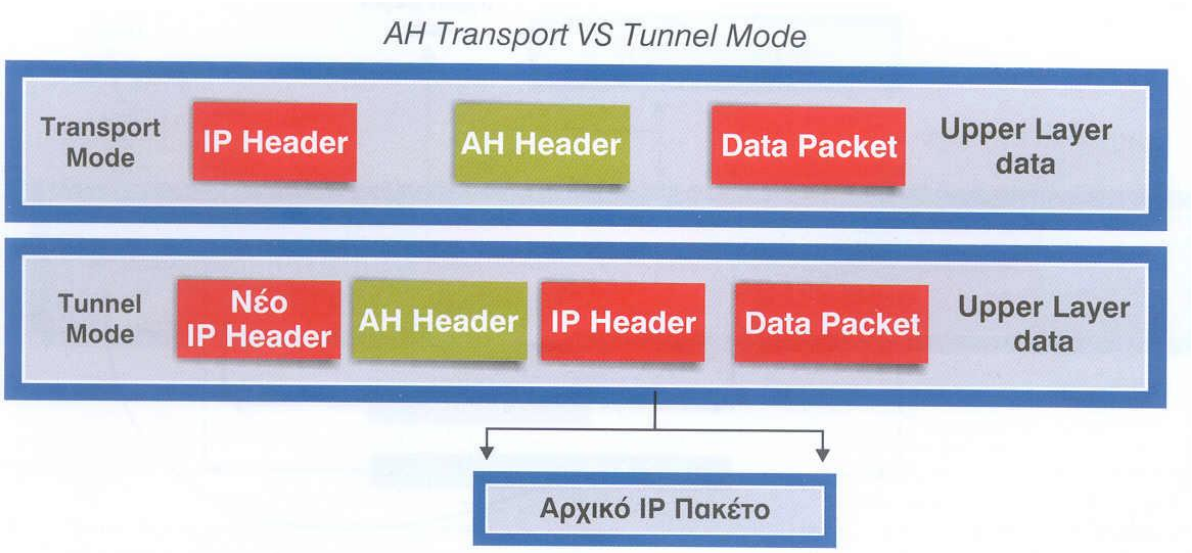
  Η διαδικασία αυτή προστατεύει από τον κίνδυνο ανάλυσης κίνησης όμως από την άλλη απαιτείτε επιπλέον επεξεργασία στα πακέτα απ ότι στον τρόπο μεταφοράς.



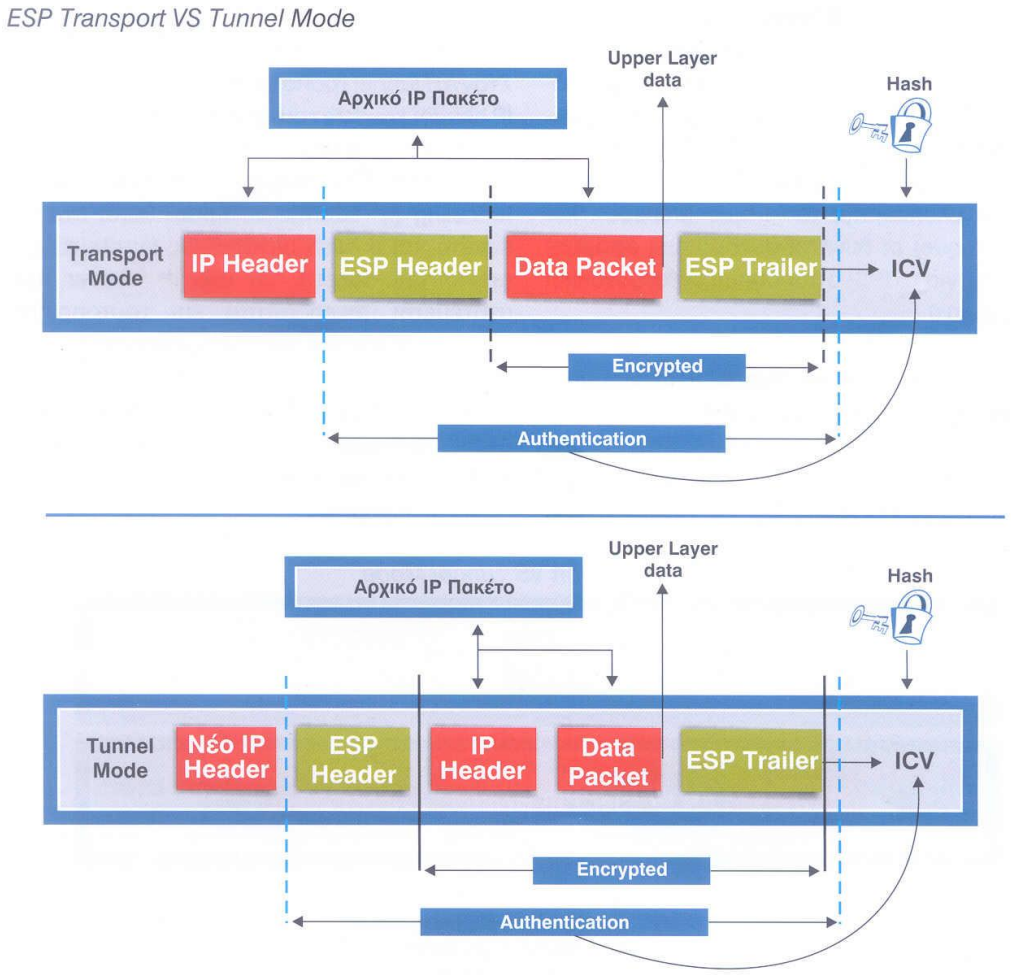

**Εικόνα 24 : τρόπος διόδου (tunnel mode)**




**Εικόνα 25 : Το IPSec σε κατάσταση διόδου (tunnel mode)**



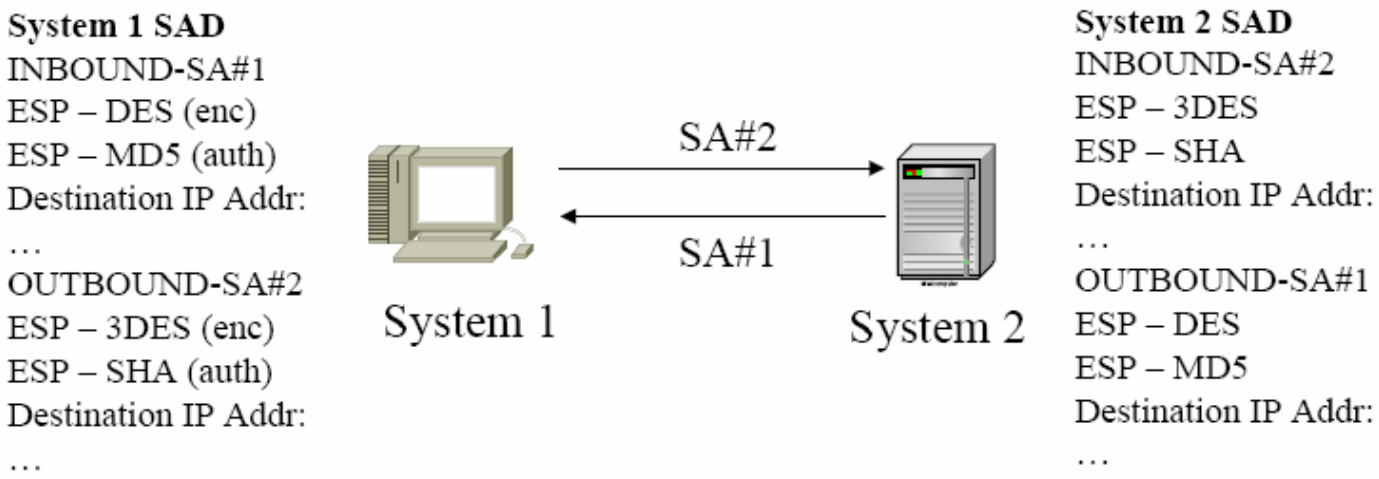

**Εικόνα 26: Σύγκριση Transport και Tunnel τρόπων υλοποίησης του IPsec , όταν χρησιμοποιείται AH**




**Εικόνα 27 :Σύγκριση Transport και Tunnel τρόπων υλοποίησης του IPSec, όταν χρησιμοποιείται ESP**

***Συσχέτιση ασφάλειας***

Είναι μια συμφωνία μεταξύ των δύο άκρων για την ασφαλή χρήση των υπηρεσιών ασφάλειας .




**Εικόνα 28 : συσχέτιση ασφαλείας**

Για κάθε ζευγάρι οντοτήτων που επικοινωνούν μεταξύ τους υπάρχουν δύο συνδέσεις ασφαλείας όπως βλέπουμε και στο παραπάνω σχήμα. Η συσχέτιση ασφάλειας αναγνωρίζεται από τον δείκτη παραμέτρων ασφάλειας SPI (Security parameter index) και από την IP διεύθυνση προορισμού.

**Οι κύριοι παράμετροι που προσδιορίζουν μια συσχέτιση ασφάλειας είναι :**

- IP διεύθυνση προορισμού
- Ένα ID χρήστη
- Πρωτόκολλο μεταφοράς (TCP ή UDP )
- Τον αλγόριθμο ελέγχου πιστοποίησης ταυτότητας και τα αντίστοιχα κλειδιά
- Τον αλγόριθμο κρυπτογράφησης και τα κλειδιά
- Τρόπος λειτουργίας του IPsec ( transfer / tunnel mode )
- Διάρκεια ζωής SA

***Μηχανισμοί κλειδιών***

**Το** IPSec εκτός από την επεξεργασία των πακέτων μέσω των ESP και AH κεφαλίδων περιλαμβάνει και πρωτόκολλα ανταλλαγής κλειδιού. Η IETF για να μπορέσει να ρυθμίσει τις συσχετίσεις ασφάλειας του IPSec επέλεξε το IKE (Internet key exchange ) κλειδί.

Το IKE σχηματίζει ένα ασφαλές κανάλι ( tunnel ) μεταξύ των δύο οντοτήτων και στη συνέχεια διαπραγματεύεται τις συσχετίσεις ασφάλειας για το IPSec.

Οι δύο οντότητες καλούνται να πιστοποιήσουν η μια την άλλη ,να μοιράσουν κλειδιά και μέσω μιας διαδικασίας να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης. Στην κατάσταση αυτή δημιουργούνται συνήθων οι παρακάτω μηχανισμοί:

- **Προ-μοιρασμένα κλειδιά.** Εδώ το κλειδί προ- εγκαθίσταται και στις δύο μηχανές. Το ίδιο κλειδί επεξεργασμένο πλέον με τη βοήθεια μιας συνάρτησης κατακερματισμού αποστέλλετε κατά την πιστοποίηση από τη μία μηχανή στην άλλη. Αν η μορφή που έχει το κλειδί είναι ίδια με αυτή που υπολογίζεται τοπικά σε κάθε μηχανή ,τότε ή διαδικασία πιστοποίησης είναι θετική.
- **Κρυπτογράφηση δημοσίων κλειδιών.** Στην περίπτωση αυτή κάθε μηχανή παράγει έναν ψευδο- τυχαίο αριθμό τον οποίο κρυπτογραφεί με το δημόσιο κλειδί της άλλης μηχανής . Οι μηχανές αποκρυπτογραφούν με τα ιδιωτικά κλειδιά ότι λαμβάνουν από το συνομιλητή τους και υπολογίζουν μια συνάρτηση κατακερματισμού του τυχαίου αριθμού. Με αυτό τον τρόπο γίνεται η πιστοποίηση. Υποστηρίζεται μόνο ο αλγόριθμος δημοσίων κλειδιών RSA.

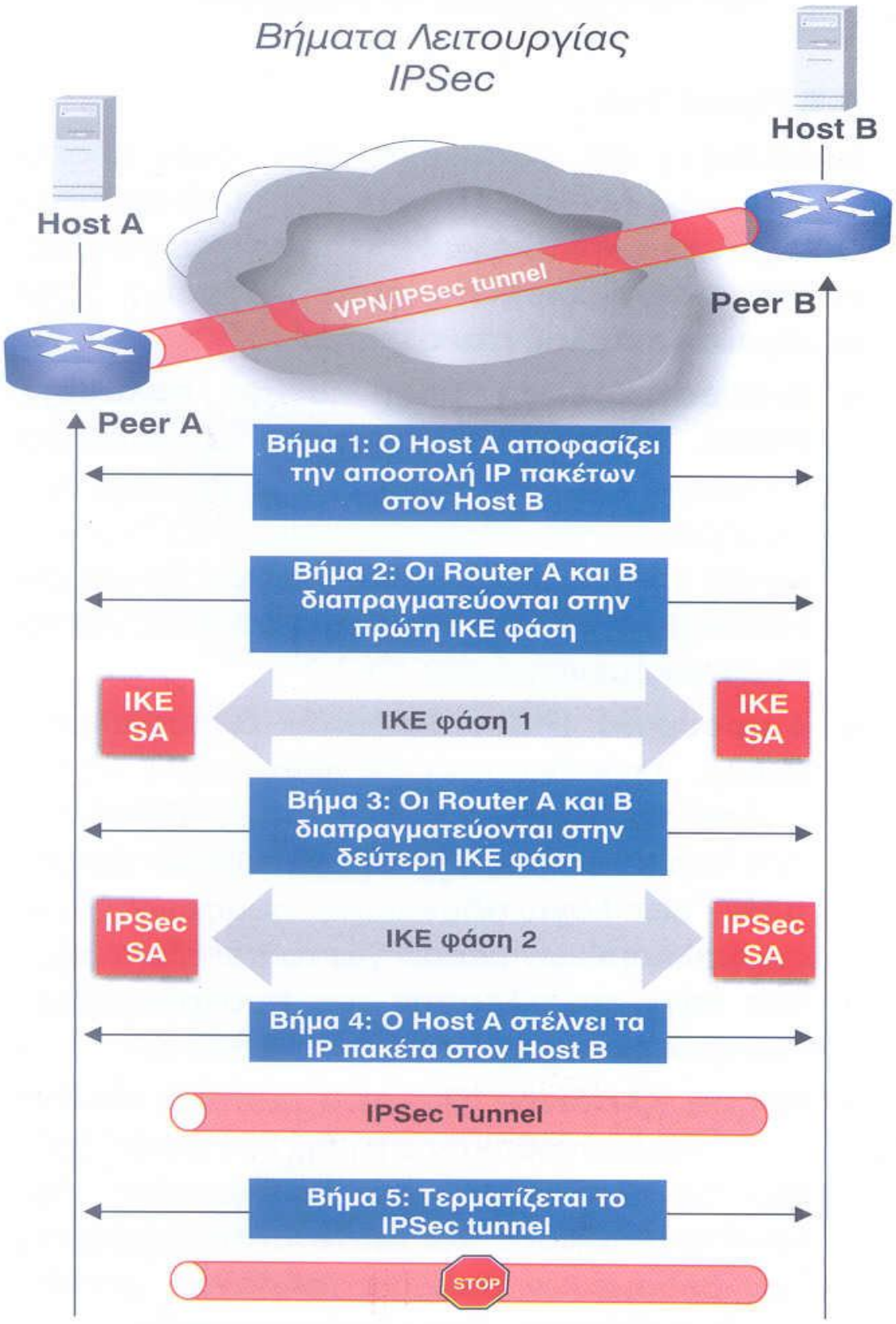
  **Ψηφιακές υπογραφές .** κάθε συσκευή στέλνει στην άλλη ψηφιακά υπογεγραμμένα δεδομένα . Η ηλεκτρονική υπογραφή των δεδομένων επιτυγχάνετε με τη χρήση του κρυφού ιδιωτικού κλειδιού από τον αποστολέα. Ο αποδέκτης πιστοποιεί την υπογραφή του αποστολέα μέσω του δημοσίου κλειδιού. Αν

ο έλεγχος αυτός επιτευχθεί τότε το κείμενο δεν έχει υποστεί αλλαγές και πιστοποιείτε η ταυτότητα του αποστολέα. Μετά την πιστοποίηση της ταυτότητας του κάθε χρήστη είναι απαραίτητη η ανταλλαγή του κλειδιού που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων που θα αποσταλούν στη συνέχεια κατά την επικοινωνία των δύο χρηστών.

Το IKE ως βασικό αλγόριθμος ανταλλαγής κλειδιού υποστηρίζει το Diffie-Hellman. Όμως μπορεί να υπάρξουν κ άλλοι όπως :

- Το κλειδί Diffie-Hellman για ανταλλαγή δύο σημείων
- Ψηφιακή πιστοποίηση για δημόσια κλειδιά
- Διάφορους αλγόριθμους hash
- Data encryption standard (DES)

Για να πραγματοποιηθεί μια IPSec επικοινωνία μεταξύ δύο ή περισσότερων συσκευών ακολουθούνται μια σειρά βημάτων όπως παρακάτω.



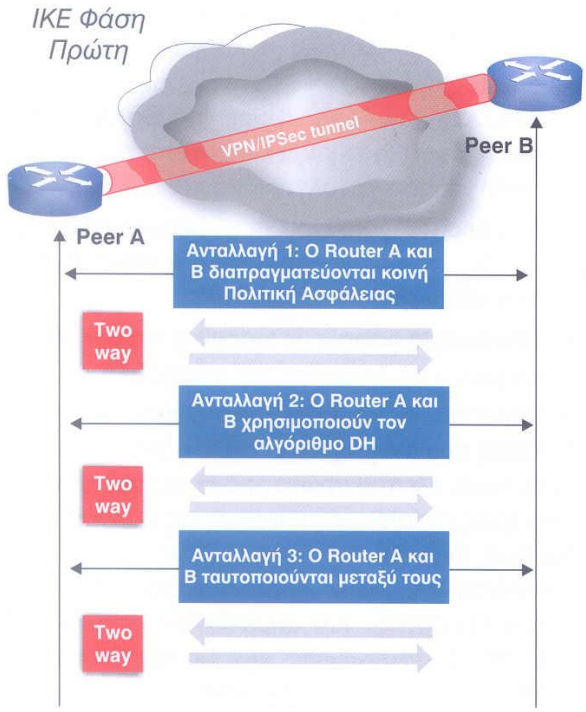

**Εικόνα 29 : βήματα λειτουργίας IPSec**

- **Ενεργοποίηση μιας IPSec συνόδου** . Στο βήμα αυτό προσδιορίζονται τα IP πακέτα που θα προστατευθούν μέσω του IPSec.
- **IKE- πρώτη φάση**. Δημιουργείτε και λειτουργεί η IKE Συσχέτιση ασφαλείας .
- **IKE – Δεύτερη φάση**. Δημιουργείτε και λειτουργεί η AH/ESP Συσχέτισης Ασφαλείας
- **Μεταφορά Δεδομένων**. Μεταφέρονται τα IP πακέτα που επιλέχθηκαν από το πρώτο βήμα .
- **Τερματισμός της IPSec συνόδου**. Εφόσον ολοκληρωθεί η μεταφορά των IP πακέτων και δεν χρησιμοποιείται η παραπάνω σύνοδος, η τελευταία τερματίζεται.

➢ Στην **πρώτη φάση IKE** μέσω των IKE SA προετοιμάζεται το έδαφος για την επόμενη διαπραγμάτευση των άλλων πρωτοκόλλων ασφάλειας του IPSec (όπως το AH και το ESP πρωτόκολλο). Στην πραγματικότητα υλοποιείται η διαχείριση των κλειδιών μέσω του IKE.

Η πρώτη φάση μπορεί να υλοποιηθεί με δύο τρόπους :

- Κύριος τρόπος (main): εδώ γίνονται τρείς ανταλλαγές μηνυμάτων και προς τις 2 κατευθύνσεις των συμβαλλόμενων μερών.
- Επιθετικός (aggressive) :οι ανταλλαγές συμπτύσσονται σε μια με τρία στάδια (αποστολέα- δέκτη, δέκτη –αποστολέα ,αποστολέα – δέκτη ).




**Εικόνα 30 : IKE πρώτη φάση**

**Πρώτη ανταλλαγή** :καθορίζονται οι αλγόριθμοι ασφάλειας και πιστοποίησης ταυτότητας . Δημιουργείτε μια ξεχωριστή συσχέτιση ασφαλείας (SA) για κάθε κατεύθυνση και μια κοινή IKE SA για καθ έναν από τους IPSec «συν ομιλούντες »

**Δεύτερη ανταλλαγή** : γίνεται συμφωνία παραμέτρων και εκτελείτε ο αλγόριθμος παραγωγής κοινού μυστικού κλειδιού μέσω του οποίου παράγετε ένα κοινό κλειδί και για τα δύο μέρη. Το κλειδί αυτό θα κρυπτογραφήσει στη συνέχεια τα δεδομένα.

**Τρίτη ανταλλαγή** : κάθε συμβαλλόμενο μέρος ταυτοποιεί το άλλο με τους κατάλληλους αλγορίθμους που ορίστηκαν νωρίτερα.

- **Στη δεύτερη φάση IKE** : πραγματοποιείτε μετά το τέλος της πρώτης φάσης και εκτελεί τα εξής:
  - **Διαπραγμάτευση κοινής πολιτικής IPSec**. Εδώ καθορίζονται οι τρόποι κρυπτογράφησης( AH/ESP, Transport mode / Tunnel mode )
  - **Δημιουργία IPSec Συσχέτιση Ασφαλείας**. Στην περίπτωση που το IPSec SA τερματίσει δημιουργείτε ένα νέο.
  - **Χρήση κλειδιών** . τα κοινά μυστικά κλειδιά που δημιουργήθηκαν στην πρώτη φάση χρησιμοποιούνται στην κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που μεταφέρονται μεταξύ των δύο IPSec συμβαλλόμενων μερών.

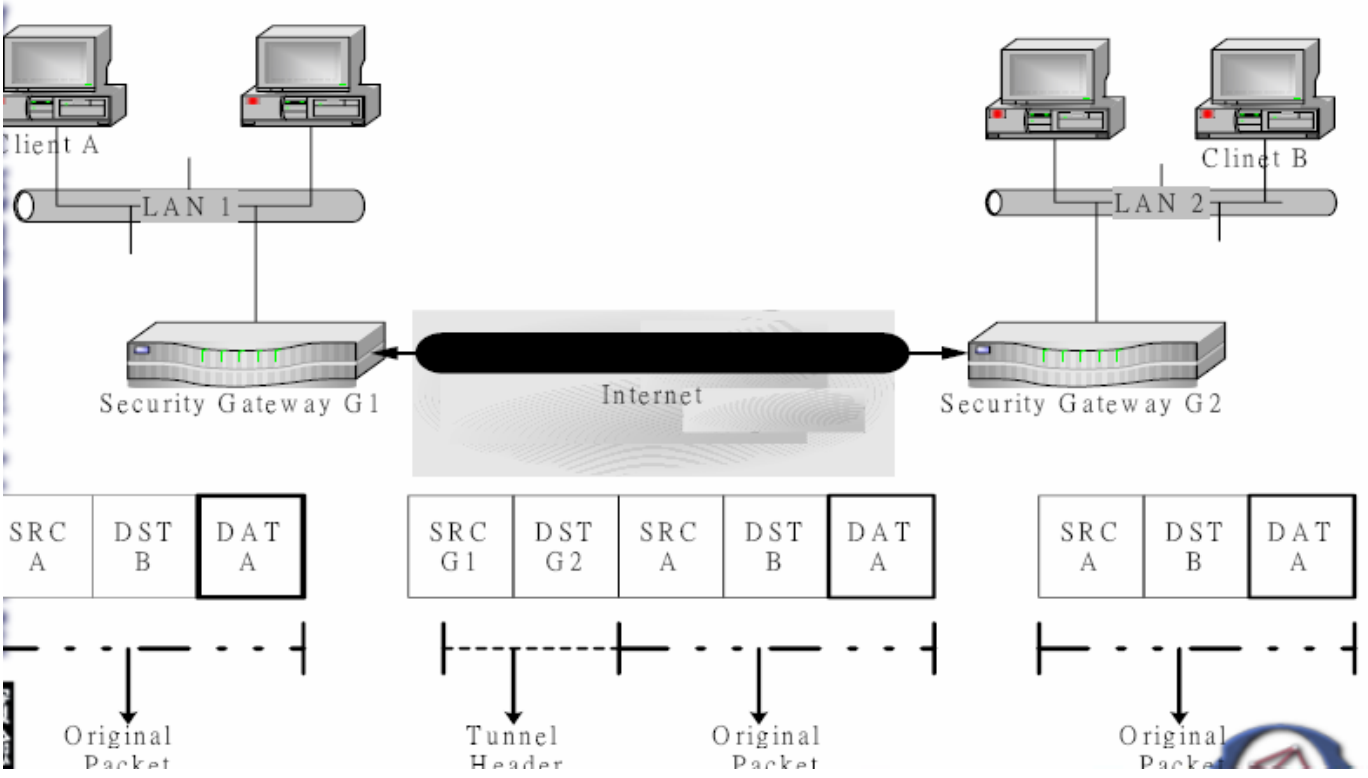
### 4.2 VPNs επιπέδου 2 (Ζεύξης δεδομένων)

Τα VPNs επιπέδου 2 Ζεύξης δεδομένων αναπτύχθηκαν σε δίκτυα απομακρυσμένης πρόσβασης. Τα δίκτυα αυτά επιτρέπουν σ ένα απομακρυσμένο χρήστη να συνδεθεί στο εσωτερικό δίκτυο μιας εταιρίας μέσω μιας γραμμής internet . Στη σύνδεση αυτή δημιουργούνται δίοδοι (tunnels ) ανάμεσα στους δρομολογητές ( router –to – router ) ή μεταξύ των δύο τερματικών κόμβων ( host- to –host ). Η τοπολογία στην οποία γίνεται εγκαθίδρυση της διόδου μπορεί να είναι είτε σημείου προς σημείο ,είτε σημείου προς πολλά σημεία.

Όταν μιλάμε για **εγκαθίδρυση διόδου (tunnel)** αναφερόμαστε στην τεχνική ενθυλάκωσης ενός πακέτου δεδομένων σ' ένα πακέτο διαφορετικού πρωτοκόλλου. Στο αρχικό πακέτο προσκολλάτε η επικεφαλίδα του tunneling και γίνεται η μεταφορά μέσω του νέου πρωτοκόλλου.

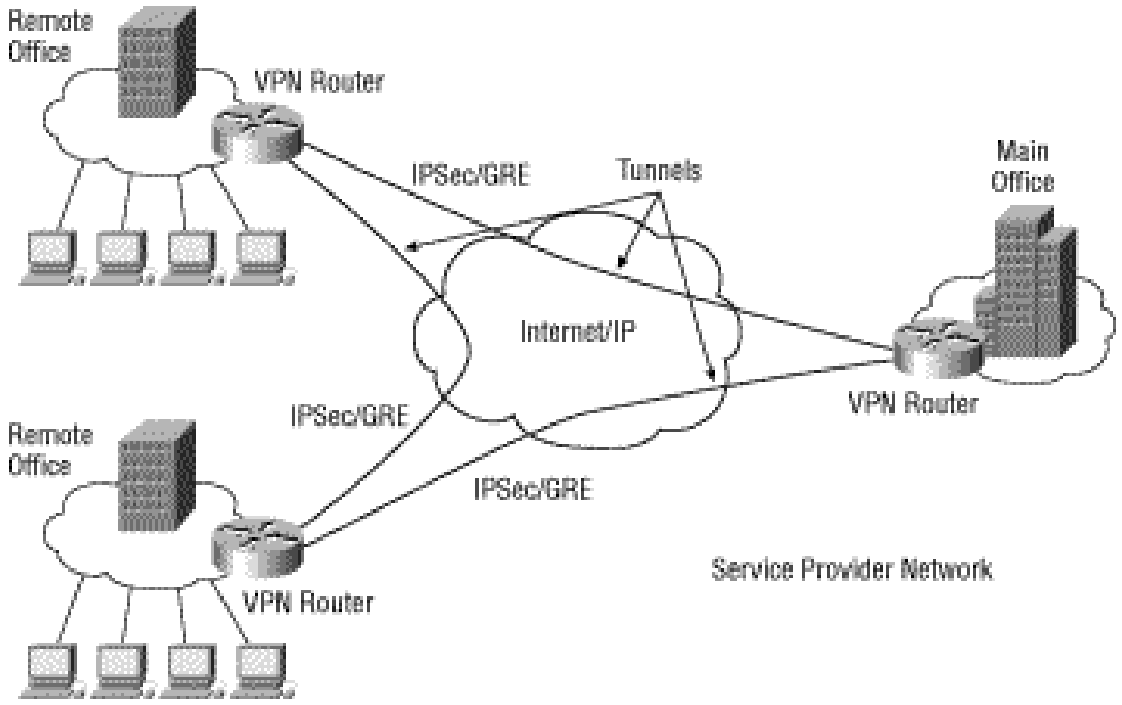
**Δίοδος** είναι το μονοπάτι του δικτύου μέσα από το οποίο περνάει το πακέτο ,κατευθυνόμενο προς τον κόμβο. Όταν το πακέτο φτάσει στον κόμβο παίρνει ξανά την αρχική του μορφή. Η τεχνολογία tunneling αναπτύσσεται στο $2^{ο}$ ή στο $3^{ο}$ επίπεδο του μοντέλου OSI.

.




**Εικόνα 31 : ενθυλάκωση πακέτου σε νέο ,για τη δημιουργία tunnel**

**Tunneling** είναι η διαδικασία κατά την οποία δημιουργείτε μια σύνδεση μεταξύ δύο σημείων (end - points). Με τη χρήση ιδικού εξοπλισμού ο αποστολέας συγχωνεύει τα IP πακέτα σε άλλα πακέτα τα οποία ταξιδεύουν μέσω του internet. Τα πακέτα αυτά παίρνουν νέο IP header και κρυπτογράφηση. Κατά την άφιξη των πακέτων στον προορισμό τους τα παραλαμβάνει ο παραλήπτης αφαιρείτε η πρόσθετη επικεφαλίδα ,γίνεται η αποκρυπτογράφηση και παραδίδεται το αρχικό πακέτο.




**Εικόνα 32 : υλοποίηση Tunneling**

***Πρωτόκολλα επιπέδου 2***

**Τρία είναι τα είδη πρωτοκόλλου ζεύξης δεδομένων :**

- IETF Layer 2 Tunneling Protocol (L2TP)
- Point to point Tunneling Protocol (PPTP)
- Layer 2 Forwarding Protocol ( L2F)

Το PPTP κατασκεύασμα της Microsoft και το L2F της Cisco αναπτύχθηκαν ανεξάρτητα. Όμως αυτό που ήταν αναγκαίο ήταν να χρησιμοποιείται ένα πρωτόκολλο από όλους το οποίο να έχει τα χαρακτηριστικά και των δύο. Έτσι δημιουργήθηκε το L2TP.

### 4.2.1 Το πρωτόκολλο Layer 2 Forwarding Protocol (L2F)

Το πρωτόκολλο L2F είναι κι αυτό πρόταση της Cisco . Για να υλοποιηθεί χρειάζεται να υπάρχει access server και router καθώς επίσης να υποστηρίζεται από τον εξοπλισμό του ISP. Επιτρέπει πάνω από μία ταυτόχρονες συνδέσεις κατά τη δημιουργία του tunnel και προσφέρει στους χρήστες τη δυνατότητα να κάνουν μια PPP ( point to point) σύνδεση σε Dial-up πάροχο υπηρεσιών και να έχουν πρόσβαση στα υπολογιστικά συστήματα της εταιρίας . Επίσης εμπεριέχει δικούς του μηχανισμούς ενθυλάκωσης των πακέτων και δεν κάνει χρήση των GRE.

Ο GRE είναι ένας μηχανισμός που χρησιμοποιείτε για Tunneling ανάμεσα σε δρομολογητές πηγής και προορισμού( router to router ). Τα GRE Tunnels δημιουργούν ένα ειδικό μονοπάτι ανάμεσα στο δρομολογητή προορισμού και το δρομολογητή πηγής όπου προωθούνται τα ενθυλακωμένα με μια GRE επικεφαλίδα πακέτα και μεταφέρονται κατά μήκος της διόδου. Όταν φτάσουν στο τέλος αφαιρείτε η επικεφαλίδα.

***Πως γίνεται μια τυπική εγκατάσταση:***

- Ο χρήστης κάνει μια PPP ή άλλη σύνδεση στο ISP .
- Κατά τη διάρκεια της αίτησης ο NAS μέσω του L2F αρχικοποιεί μια δίοδο προς τον προορισμό του χρήστη.
- Ο προορισμός ζητάει password του χρήστη .
- Γίνεται πιστοποίηση ταυτότητας
  - ✓ Μία από τον ISP στον οποίο συνδέεται ο χρήστης .
  - ✓ Μία από την πύλη (gateway) του απομακρυσμένου δικτύου που συνδέεται ο χρήστης.
- Παραχωρείτε στο χρήστη IP διεύθυνση σαν μια τυπική Dial-up απομακρυσμένη πρόσβαση.

***Τι προσφέρει το L2F πρωτόκολλο***

- Ανεξαρτησία πρωτοκόλλων (IPX, SNA)
- Αυθεντικοποίηση (PPP, CHAP, TACACS ή RADIUS)
- Διαχείριση διευθύνσεων
- Δυναμικά και ασφαλή tunnels
- Υπηρεσίες χρέωσης (accounting)
- Έλεγχος ροής

### 4.2.2 Το πρωτόκολλο Point to point Tunneling Protocol (PPTP )

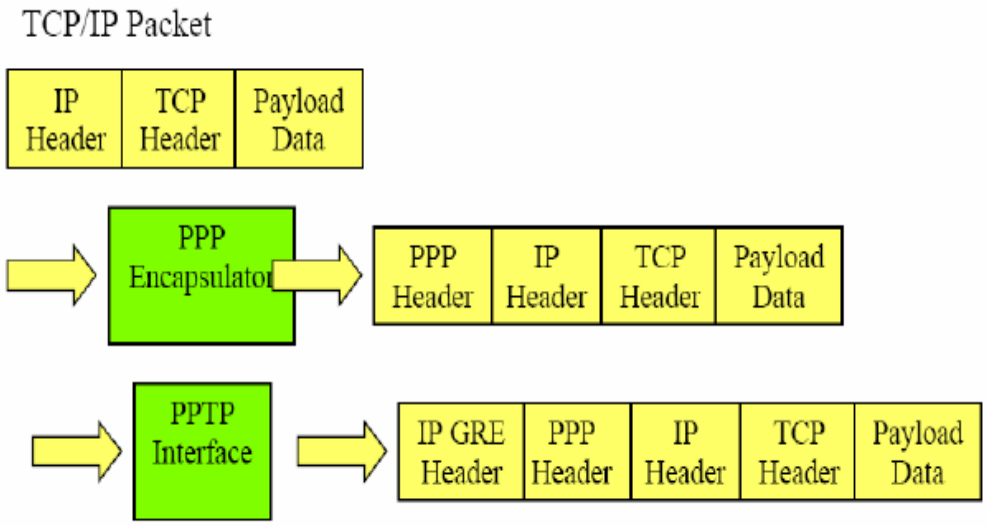
Το point to point Tunneling Protocol είναι δημιούργημα μιας ομάδας εταιριών η οποία ονομάστηκε PPTP Forum. Οι εταιρίες αυτές ήταν η Microsoft , η 3Com, η US Robotics και η Ascend Communications . Η βασική τους ιδέα ήταν η δημιουργία προϋποθέσεων για εύκολη και ασφαλή πρόσβαση απομακρυσμένων χρηστών με τα εταιρικά τους δίκτυα μέσω τοπικού ISP. Το PPTP είναι ένας συνδυασμός του PPP και του TCP/IP .Δηλαδή το PPTP προσπαθεί να συνδυάσει την εμπιστευτικότητα με ταυτόχρονη συμπίεση των δεδομένων του PPP και την δυνατότητα δρομολόγησης των πακέτων στον internet του TCP/IP. Ουσιαστικά παίρνει πακέτα όπως το IP,IPX, Net Bios SNA και τα μετατρέπει σ' ένα καινούργιο IP πακέτο για μεταφορά. Πιστοποιεί την ταυτότητα του χρήστη μέσω των μηχανισμών PAP και CHAP που του τα παρέχει το PPP . Η μεταφορά των PPP πακέτων ,η κρυπτογράφηση και η ενθυλάκωση .γίνεται μέσω του GRE .

Στο PPTP χρησιμοποιούνται δύο ειδών πακέτα :

- Πακέτα δεδομένων (data packets ) ,τα οποία χρησιμοποιούνται για σηματοδοσία και έχουν ενθυλακωθεί μέσω του GRE v2.
- Πακέτα ελέγχου ( control packets), τα οποία χρησιμοποιούνται για τη μεταφορά δεδομένων του χρήστη .

***Πως λειτουργεί το PPTP***

Στην αρχή χρησιμοποιείτε αυτούσιο το PPP για να εξασφαλιστεί η εγκαθίδρυση της φυσικής ζεύξης ,η πιστοποίηση των χρηστών και η δημιουργία PPP πλαισίων. Στη συνέχεια τα PPP πλαίσια ενθυλακώνονται σε μεγαλύτερα πακέτα για να μεταδοθούν τα δεδομένα μέσω μιας διόδου. Με την χρήση του GRE δημιουργούνται IP πακέτα.



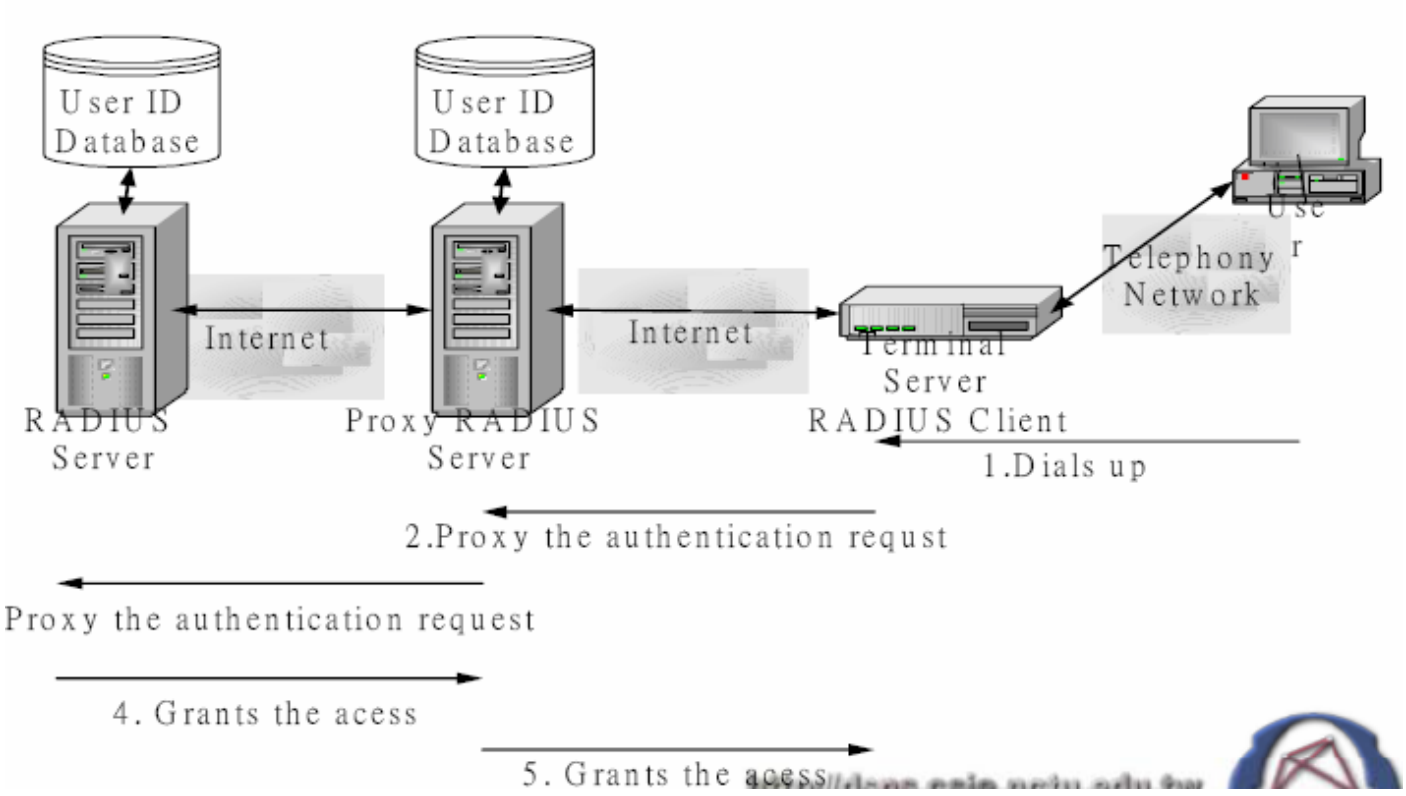

**Εικόνα 33: ενθυλάκωση πακέτων στο PPTP**

Για τη σωστή λειτουργία του PPTP είναι υπεύθυνες οι συσκευές του ISP :RAS(Remote Access Server ) και NAS (Network Access Servers ) οι οποίες είναι μια συλλογή modems με κατάλληλο λογισμικό**.**

- NAS (Network Access Servers). Είναι η πιστοποίηση ταυτότητας του χρήστη η οποία γίνεται μέσω της αίτησης σύνδεσης στον ISP και επικυρώνεται με μηχανισμούς password που παρέχει το PPP .
- RAS (Remote Access Server ). Εδώ η αυθεντικοποίηση του χρήστη η οποία γίνεται κυρίως μέσω του πρωτοκόλλου RADIUS.

Η δομή του RADIUS πρωτοκόλλου είναι αυτή του «πελάτη –εξυπηρετητή». Ο RADIUS Server δέχεται από το NAS αιτήσεις ,ID ,και passwords χρηστών και με τη σειρά του ενημερώνει αν θα εγκριθεί η πρόσβαση ή όχι αφού διατηρεί μια κεντρική βάση δεδομένων με τα στοιχεία τους, τις υπηρεσίες που παρέχονται στον καθένα απ αυτούς καθώς και πληροφορίες για τις χρεώσεις τους .

Υπάρχουν επίσης και οι RADIUS proxy servers όπου είναι εγκατεστημένοι στο ISPs . Αυτοί ενημερώνονται συχνά από το κεντρικό RADIUS Server και έχουν στην κατοχή τους ένα αντίγραφο της βάσης δεδομένων για να μπορούν κι αυτοί να αυθεντικοποιούν το χρήστη.



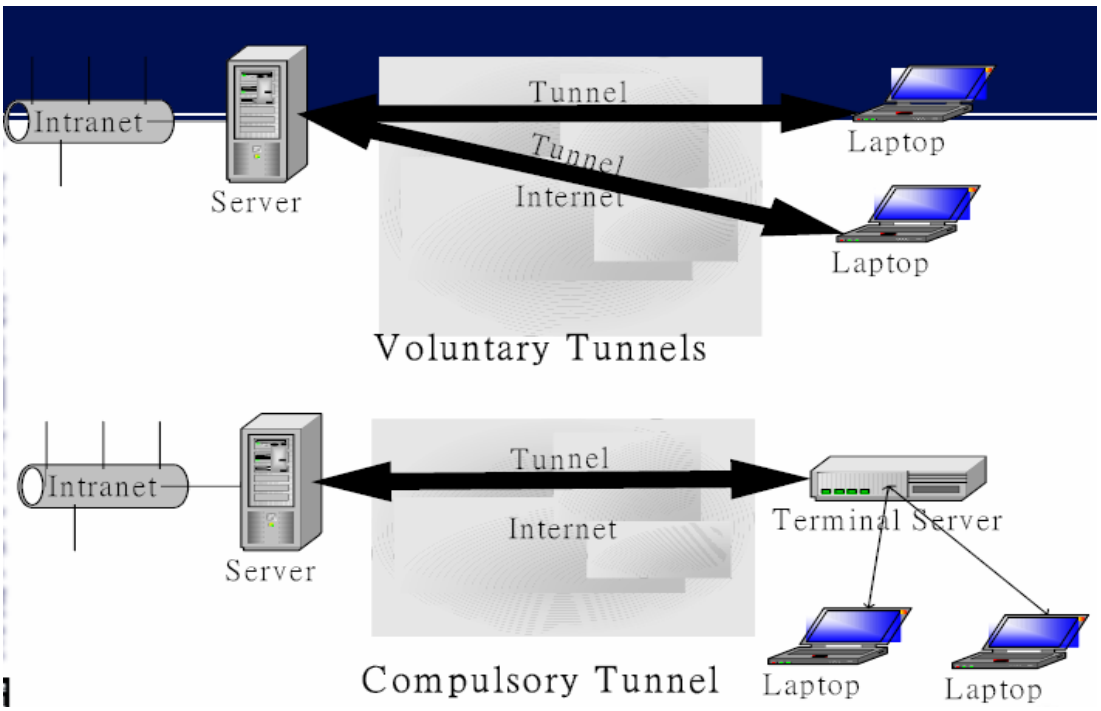

**Εικόνα 34 :λειτουργία RADIUS με proxy servers**

Οι ζεύξεις επικοινωνίας στο PPTP πραγματοποιούνται πάνω σε διόδους. Το άκρο της διόδου καθορίζεται κάθε φορά από τις δυνατότητες που έχει ο υπολογιστής του χρήστη. Αν ο υπολογιστής έχει PPTP software, τότε αυτός γίνεται άκρο της διόδου διαφορετικά αν χρησιμοποιεί PPP τότε άκρο της διόδου βρίσκεται στο RAS του ISP .

Υπάρχουν δύο ειδών δίοδοι:

- οι **«αυθόρμητες» δίοδοι** οι οποίες δημιουργούνται μετά από αίτηση του χρήστη.
- οι **«αναγκαστικές» δίοδοι** δημιουργούνται αυτόματα χωρίς την παρέμβαση του χρήστη.

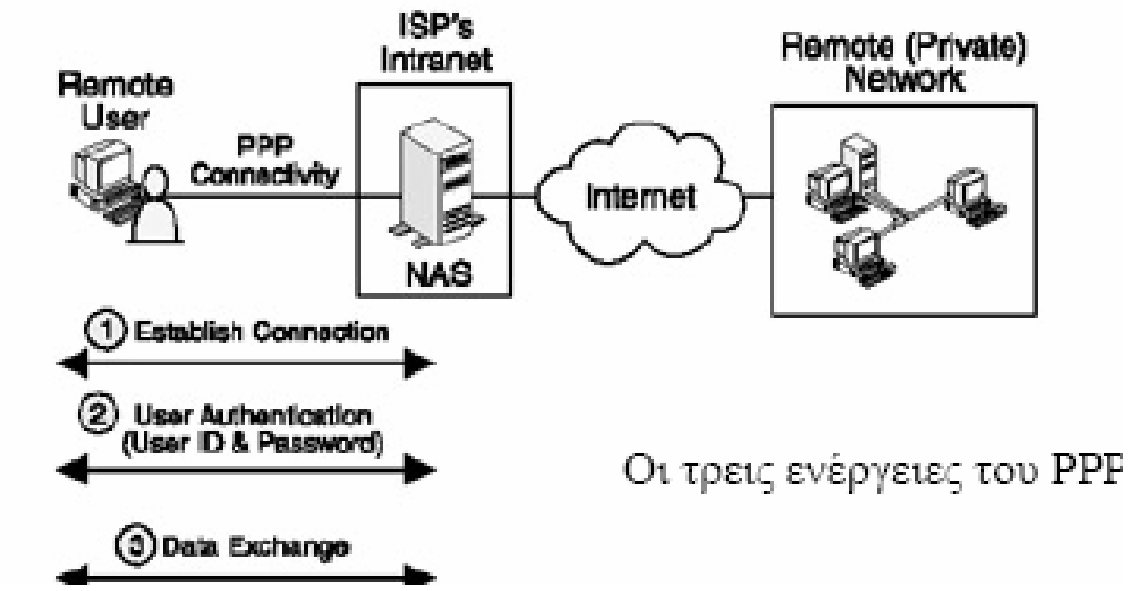
Η αναγκαστική δίοδος έχει προκαθορισμένα ακραία σημεία (που είναι στην ουσία κάποιοι RAS), και έτσι μπορεί ποιο εύκολα να γίνει έλεγχος πρόσβασης των χρηστών. Επίσης παρέχει τη δυνατότητα στις εταιρίες που δεν επιθυμούν οι εργαζόμενοι τους να έχουν πρόσβαση στο Internet να χρησιμοποιούν τις Internet ζεύξεις αποκλειστικά για το VPN. Στις αναγκαστικές διόδους μπορούν πολλαπλές συνδέσεις να υπάρχουν πάνω σε μια δίοδο. Μειονέκτημα τους είναι ότι δεν είναι και τόσο ασφαλείς αφού η σύνδεση του υπολογιστή του χρήστη με τον RAS πραγματοποιείται έξω από τη δίοδο με αποτέλεσμα να μην πραγματοποιούνται οι μηχανισμοί κρυπτογράφησης που η δίοδος επιβάλλει.




**Εικόνα 35: Σχηματική αναπαράσταση των αυθόρμητων και των αναγκαστικών διόδων.**

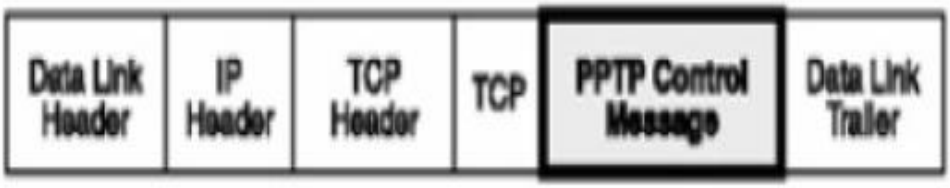
Ας συνεχίσουμε όμως με τη λειτουργία του PPTP βήμα –βήμα :

- **Πρώτη φάση . Στη φάση αυτή χρησιμοποιείτε το πρωτόκολλο** PPP για τη σύνδεση χρήστη και ISP.




**Εικόνα 36 :πρώτη φάση λειτουργίας του PPTP**

- **Δεύτερη φάση :γίνεται ανταλλαγή μηνυμάτων ελέγχου μεταξύ** PPTP client και PPTP server (RAS) έτσι ώστε να διατηρηθεί ή δίοδος και να τερματίσει .Η ανταλλαγή αυτή γίνεται τις IP διευθύνσεις τους ,στην 1723 TCP θύρα του RAS. Τα PPTP μηνύματα ελέγχου ενθυλακώνονται σε TCP/IP πακέτα.

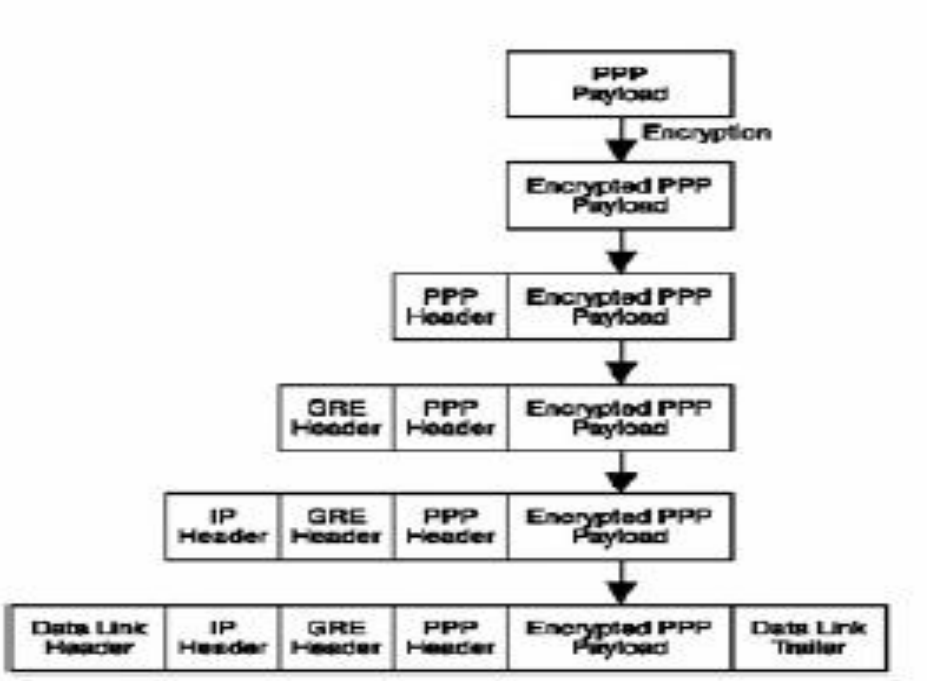



**Εικόνα 37 : δεύτερη φάση** PPTP (λογική εγκαθίδρυση του PPTP)

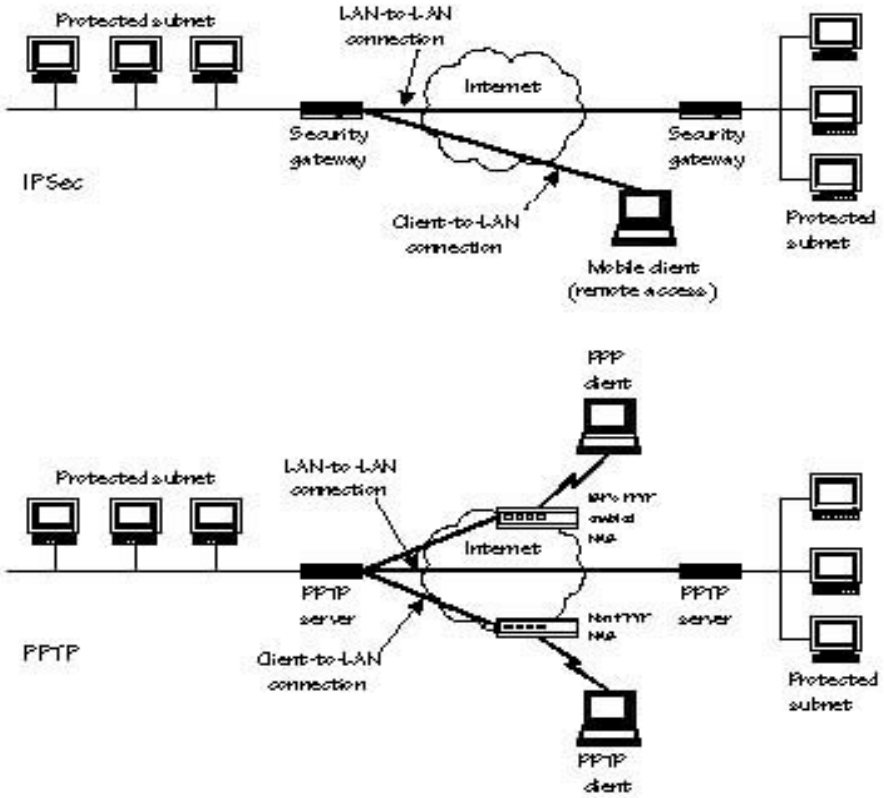
- **Τρίτη φάση :** τα πακέτα δεδομένων κρυπτογραφούνται μέσω του πρωτοκόλλου RC4 και μεταφέρονται μέσω της διόδου που δημιουργήθηκε στην προηγούμενη φάση. Το κλειδί κρυπτογράφησης προκύπτει απ την συνάρτηση κατακερματισμού στο password του χρήστη. Για μεγαλύτερη ασφάλεια η κρυπτογράφηση ξεκινάει από τον υπολογιστή του χρήστη.

  Όλα αυτά που καταγράψαμε μέχρι τώρα αφορούσαν το PPTP όπου η σύνδεση σε δίκτυο γινόταν μεταξύ του χρήστη και του υπολογιστή του. Υπάρχουν όμως και περιπτώσεις σύνδεσης δικτύου με δίκτυο (LAN –to –LAN tunneling ) . Το οποίο μοιάζει πολύ με την LAN - to - LAN IP sec υποδομή με την διαφορά ότι δεν υπάρχει το IKE(πρωτόκολλο ανταλλαγής κλειδιού) .

Στην περίπτωση (LAN –to –LAN tunneling) ο server παίζει διπλό ρόλο . Σε κάθε ένα από τα δύο δίκτυα που επικοινωνούν άλλοτε λειτουργεί ως server και άλλοτε ως client




**Εικόνα 38 : Τρίτη φάση του PPTP( PPTP tunneling- μεταφορά δεδομένων )**




**Εικόνα 39:σύγκριση δικτύων IPsec και PPTP .**

Οι PPTP server φιλτράρουν τα εισερχόμενα πακέτα και τα προωθούν από και προς τα αντίστοιχα LAN. Όταν το ISP διαθέτει PPTP server ο υπολογιστής δεν χρειάζεται PPTP software .

***Μειονεκτήματα του PPTP***

Ένα μειονέκτημα του PPTP είναι πως οι PPTP server δέχονται δεδομένα μόνο στη θήρα 1723 TCP με αποτέλεσμα να υπάρχει ενδεχόμενο υποκλοπής δεδομένων . Επίσης τα DRE πακέτα που υπάρχουν είδη στα PPTP πακέτα δεν μπορούν να περάσουν μέσα από από όλους τους τοίχους ασφαλείας . τέλος τα VPNs που στηρίζονται στο PPTP εξαρτώνται σε μεγάλο βαθμό από τα πρωτόκολλα που διαθέτει και μπορεί να υποστηρίξει ο ISP.

### 4.2.3 Το πρωτόκολλο Layer 2 Tunneling Protocol (L2TP)

Για λόγους συμβατότητας όλων των δικτύων έγινε συγχώνευση του PPTP πρωτοκόλλου και του L2F με αποτέλεσμα να δημιουργηθεί ένα νέο πρωτόκολλο το L2TP ,το οποίο παρέχει συμπίεση βασισμένη σε λογισμικό. Ένα μικρό μέρος από τις τεχνικές συμπίεσης προστέθηκε στο επίπεδο της κρυπτογράφησης.
Το L2TP παρέχει υπηρεσίες $2^{ου}$ και $3^{ου}$ επιπέδου λόγο της εκμετάλλευσης πολλών χαρακτηριστικών του IPSec εξασφαλίζοντας έτσι μεγαλύτερη ασφάλεια**.**

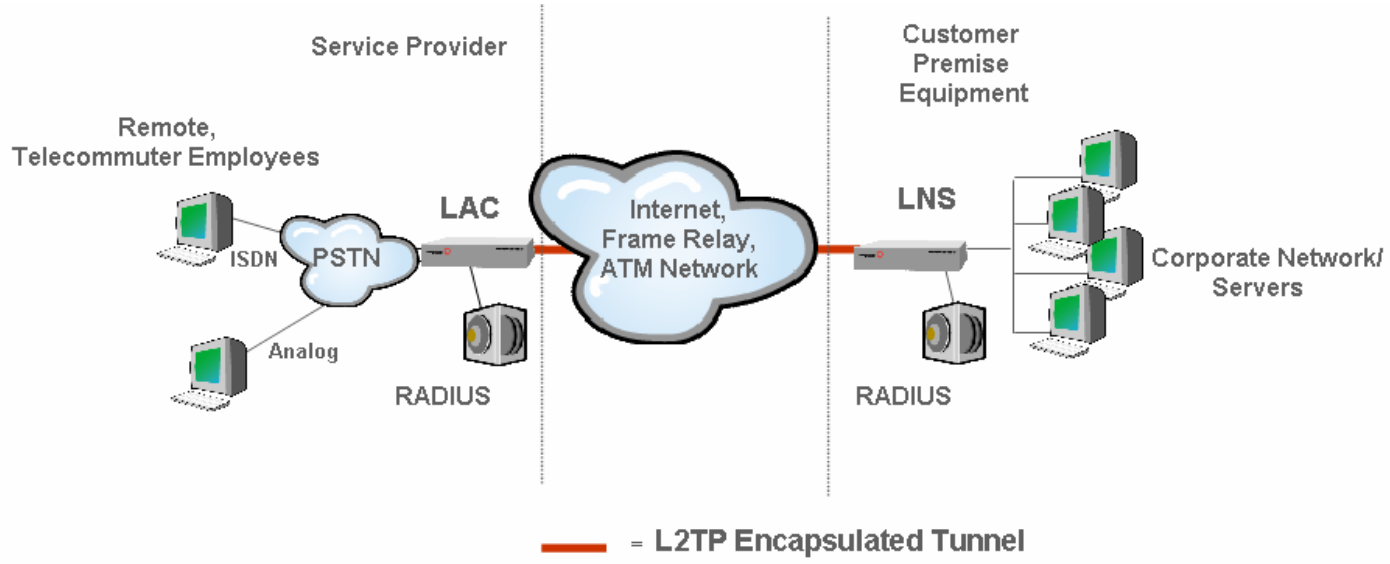
**Το πρωτόκολλο αυτό χρησιμοποιεί δύο server για τη σύνοδο :**

- Τον **LAC ( L2TP Access Concentrator )**, ο οποίος βρίσκεται στο ISP και εγκαθιδρύει μια δίοδο σένα δημόσιο δίκτυο όπου η δίοδος αυτή τερματίζει στο LNS του κόμβου προορισμού και
- Τον **LNS (L2TP Network Server ),** ο οποίος βρίσκεται στον προορισμό και χρησιμοποιείτε για να τερματίσει το tunnel . Ο LNS δέχεται αίτηση σύνδεσης από ένα LAC , κάνει την αυθεντικοποίηση του αιτούντα- χρήστη και εγκαθιδρύει το tunnel.

  Μεταξύ του Access Concentrator και του Network Server δημιουργείτε μια δίοδος με πολλές συνόδους (επικοινωνίας ) όπου η κάθε μία έχει ένα μοναδικό αριθμό call ID ,που βρίσκεται στην επικεφαλίδα του L2TP πακέτου. Υπάρχει όμως περίπτωση να δημιουργηθούν πολλές διαφορετικές δίοδοι όπου η κάθε μία θα ικανοποιεί διαφορετικό QOS . Η αρχική σύνδεση του LAC με το χρήστη γίνεται μέσω του PPP. Εκείνος ενθυλακώνει διάφορα είδη πακέτων και κάνει μια αρχική αυθεντικοποίηση του χρήση. Στη συνέχεια ο RADIUS κάνει μια δεύτερη αυθεντικοποίηση της ταυτότητας του χρήστη.

  Το L2TP όπως και το PPTP είναι δύο είδη μηνυμάτων που μπορούν να ανταλλάσσονται : μηνύματα ελέγχου και μηνύματα δεδομένων.

Όταν δημιουργείτε VPN βασισμένο πάνω στο L2TP πρωτόκολλο μπορεί να υποστηρίξει και αυθόρμητες και αναγκαστικές διόδους.




**Εικόνα 40 :δίοδος με βάση L2TP VPN**

***Πως δημιουργείτε μια L2TP δίοδος* :**

**Βήμα 1$^{ο}$** : με τη χρήση του PPP ο απομακρυσμένος χρήστης ζητάει σύνδεση με τον LAC του ISP .

Ο LAC αυθεντικοποιεί τον χρήστη ζητώντας του user name και password και προσδιορίζει την IP του LNS που ανήκει στον LAN για το οποίο ο χρήστης ζητάει σύνδεση. Αμέσως μετά ξεκινάει L2TP σύνοδος μεταξύ LAC και LNS .

**Βήμα 2$^{ο}$ :** εδώ γίνεται η αυθεντικοποίηση του χρήστη από το LNS μέσω οποιουδήποτε τυποποιημένου αλγορίθμου αυθεντικοποίησης . Δεν υπάρχει κάποιος περιορισμός στην επιλογή του αλγορίθμου , ωστόσο συνήθως χρησιμοποιείται ο RADIUS.

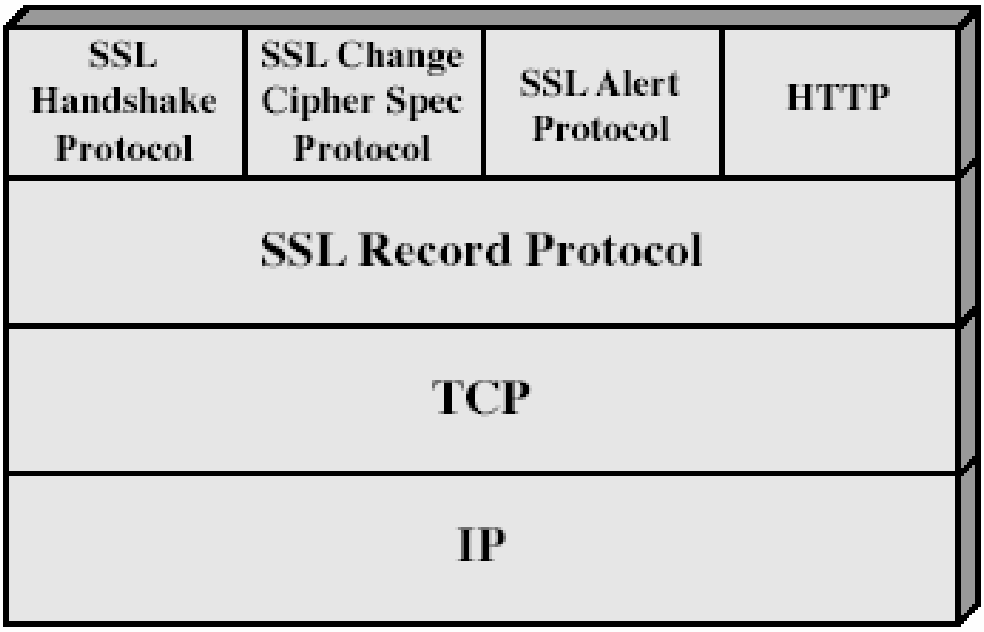
**Βήμα 3$^{ο}$ :** στη συνέχεια δημιουργείτε ένα προστατευόμενο tunnel μεταξύ LAC και LNS και γίνεται η κρυπτογράφηση. Δεν επιβάλλεται μια συγκεκριμένη μέθοδος κρυπτογράφησης όμως για διόδους πάνω σε IP δίκτυα μπορεί να χρησιμοποιηθεί το IPSec πρωτόκολλο . Τότε γίνεται στο L2TP ενθυλάκωση σε UDP πακέτα τα οποία μεταφέρονται μέσω IPSec tunnel μεταξύ LAC και LNS . Η βασική θήρα που χρησιμοποιείτε είναι η UDP 1701 όμως δεν αποκλείεται η χρήση οποιασδήποτε άλλης UDP θήρας**.**

Στην αναγκαστική δίοδο ο χρήστης στέλνει PPP πακέτα στον LAC. Χωρίς να το γνωρίζει και χωρίς να κάνει καμία άλλη ενέργεια δημιουργείτε μια δίοδος μεταξύ του LAC και του LNS του απομακρυσμένου δικτύου. Το IPsec στέλνει απευθείας κρυπτογραφημένα τα δεδομένα . Το LACτου ISP προσθέτει το AH. Το ESP προστίθεται μόνο όταν ο LNS υποστηρίζει IPSec στον προορισμό του. Για την ανταλλαγή κλειδιού χρησιμοποιείτε το IKE .

Στην αυθόρμητη δίοδο τώρα το AH εγκαθίσταται απευθείας στον υπολογιστή του χρήστη. Αν ο LNS δεν υποστηρίζει IPSec στον προορισμό του ,το ESP προστατεύει προσωρινά τα δεδομένα μέχρι να καταφτάσουν στο LNS.

Ανακεφαλαιώνοντας τις λειτουργίες του LNS διαπιστώνουμε ότι υποστηρίζει μια μεγάλη ποικιλία αλγορίθμων κρυπτογράφησης και επεξεργάζεται πακέτα που έχουν τις κεφαλίδες AH και ESP . Ακόμη παρέχει μεγάλη ασφάλεια ως προς την ανάλυση κίνησης λόγω της ευελιξίας χρήσης UDP θηρών. Τέλος μπορεί να χρησιμοποιηθεί για σύνδεση δίκτυο – προς- δίκτυο (LAN to LAN tunneling ). Ένα αρνητικό του LNS είναι ότι δεν πραγματοποιεί φιλτράρισμα.

### 4.3 VPNs επιπέδου 4 (μεταφοράς )




Η υλοποίηση των εικονικών δικτύων επιπέδου μεταφοράς γίνεται μέσω του πρωτοκόλλου **SSL** ( Secure Sockets Layer ) .

#### 4.3.1 Πρωτόκολλο SSL

Το **SSL** γνωστό και ως ηλεκτρονικό πιστοποιητικό δημιουργεί μια ασφαλή σύνδεση μεταξύ μιας ιστοσελίδας και του φυλλομετρητή του χρήστη( browser ). Το SSL εξασφαλίζει την ασφαλή ανταλλαγή δεδομένων ανάμεσα στις δύο πλευρές αυτή του εξυπηρετητή (server) και του εξυπηρετούμενου (client). Χρησιμοποιείται από ιστοσελίδες που ασχολούνται με ηλεκτρονικές συναλλαγές. Γι ‘αυτό και τις περισσότερες φορές ζητείτε από τον επισκέπτη να εισάγει προσωπικά στοιχεία και δεδομένα. Αντιλαμβανόμαστε ότι μια ιστοσελίδα χρησιμοποιεί **SSL** πρωτόκολλα ,αρκεί να παρατηρήσουμε το εικονίδιο που παριστά ένα λουκέτο ή το πρόθεμα https μπροστά από τη διεύθυνση της ιστοσελίδας.

Το πρωτόκολλο **SSL** δημιουργήθηκε από την εταιρία Netscape communications corporation. Η πρώτη σχεδίαση του πρωτοκόλλου εκδόθηκε για πρώτη φορά τον Οκτώβρη του 1994 με τη μορφή RFC ( Request

For Comments ) (version 1.0). Το Δεκέμβριο της ίδιας χρονιάς επανεκδόθηκε μια βελτιωμένη έκδοση.( version 2.0 ). Το 1995 κυκλοφόρησε η αναβαθμισμένη έκδοση SSL ( version 3.0) και άρχισε να εφαρμόζεται από τις βιομηχανίες. Αργότερα μετεξελίχθηκε στο TLS (Transport Layer Security ).

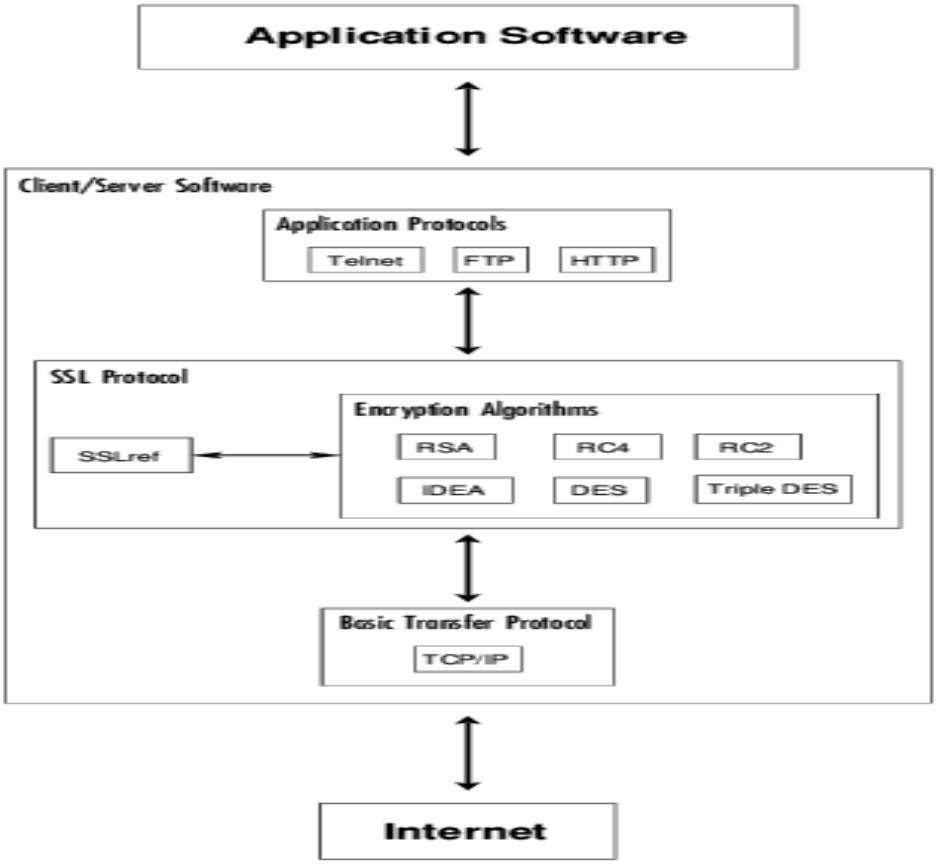
***Παροχή ασφάλειας από το SSL***

Το SSL σχεδιάστηκε για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων . όπου το ένα λειτουργεί σαν server και το άλλο σαν client.

Για να επιτευχθεί εξασφάλιση απορρήτου :

- Γίνεται κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol.
- Πιστοποιείτε υποχρεωτικά μέσω έγκυρων πιστοποιητικών η ταυτότητα του server και προαιρετικά του client.
- Υποστηρίζονται πολλοί μηχανισμοί κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση κάθε είδους ανάγκης.
- Με τη χρήση MACs τεχνικής γίνεται αντιληπτός οποιοσδήποτε προσπαθήσει να αλλοιώσει πληροφορίες. Έτσι εξασφαλίζεται η ακεραιότητα των δεδομένων.

Το SSL πρωτόκολλο μπορεί να τοποθετηθεί στην κορυφή οπουδήποτε αξιόπιστου πρωτοκόλλου μεταφοράς. Είναι ανεξάρτητο από TCP/ IP όπου αυτό σημαίνει ότι παρέχει ασφάλεια αδιαφανώς σε οποιαδήποτε TCP/ IP εφαρμογή στρωματοποιείτε στην κορυφή. Τρέχει κάτω από τα πρωτόκολλα εφαρμογών όπως είναι το HTTP , FTP, TELNET.




**Εικόνα 41 : Το πρωτόκολλο SS**

***Υποστηριζόμενοι αλγόριθμοι***

Υπάρχουν δύο είδη αλγόριθμων κρυπτογράφησης οι stream cipher και οι block cipher .

| 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 | | |

**Εικόνα 42: αλγόριθμοι κρυπτογράφησης**

Οι αλγόριθμοι για την παραγωγή των hash και digest values για τα MACs είναι :

- MD5 (128-bit hash ) και
- SHA (160-bit hash).

Οι τεχνικές διαχείρισης των κλειδιών ( key management ) είναι :

- η ασύμμετρη κρυπτογραφία με RSA
- η τεχνική Diffie – Hellman.

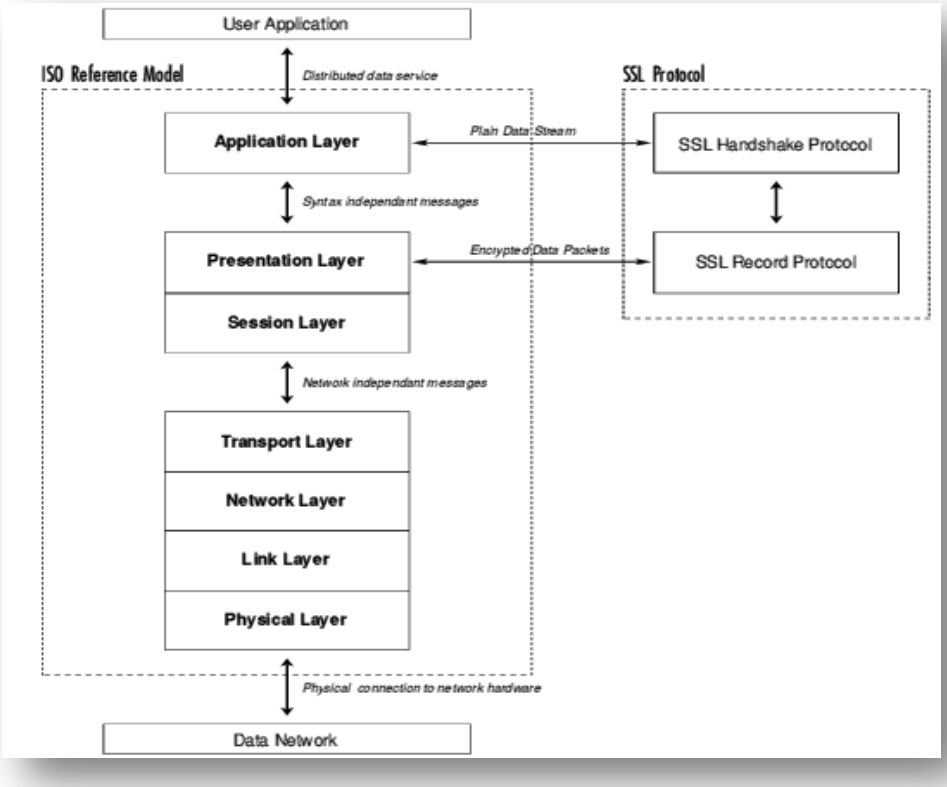
Τα πιστοποιητικά είναι της μορφής X.509.

Ο RSA μαζί με τον DSS και τον Fortezza μπορούν να χρησιμοποιηθούν για την ψηφιακή υπογραφή των κλειδιών κρυπτογράφησης.

***Το SSL Και το OSI μοντέλο***

Κάθε νέο πρωτόκολλο είναι πολύ σημαντικό να μπορεί να ταιριάζει με το μοντέλο OSI. Γιατί θα μπορεί να παρέχει δυνατότητες αντικατάστασης κάποιου υπάρχοντος μοντέλου ή ενσωμάτωση στην υπάρχουσα δομή του πρωτοκόλλου.

Το SSL βλέπουμε στο παρακάτω σχήμα ότι δεν αντικαθιστά κάποιο άλλο πρωτόκολλο αλλά αποτελεί ένα επιπρόσθετο στρώμα το οποίο δεν εμποδίζει την λειτουργία και άλλου μηχανισμού ασφάλειας σε υψηλότερο επίπεδο.



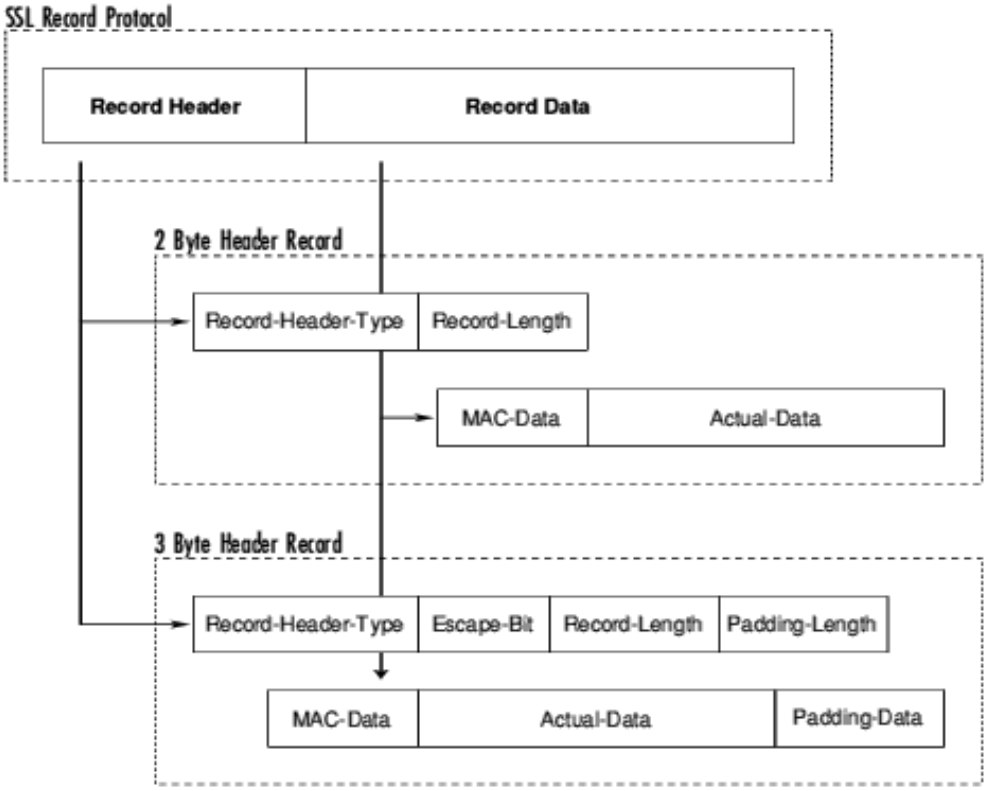

**Εικόνα 43 : *SSL Και το OSI μοντέλο***

Το SSL αποτελείτε από δύο μέρη:

- Το SSL Handshake Protocol (SSLHP) ,το οποίο διαπραγματεύεται τους αλγορίθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πιστοποιεί την ταυτότητα του server και του client αν ζητηθεί.
- Το SSL Record Protocol (SSLRP), το οποίος συγκεντρώνει τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει και συνεχίζει με την αποκρυπτογράφηση των υπόλοιπων πακέτων που παραλαμβάνει.

*Λειτουργία του SSL με :*

- **Record Protocol (SSLRP)**




**Εικόνα 44: SSL Record Protocol (SSLRP)**

Ένα πακέτο αποτελείται από την επικεφαλίδα και τα δεδομένα.

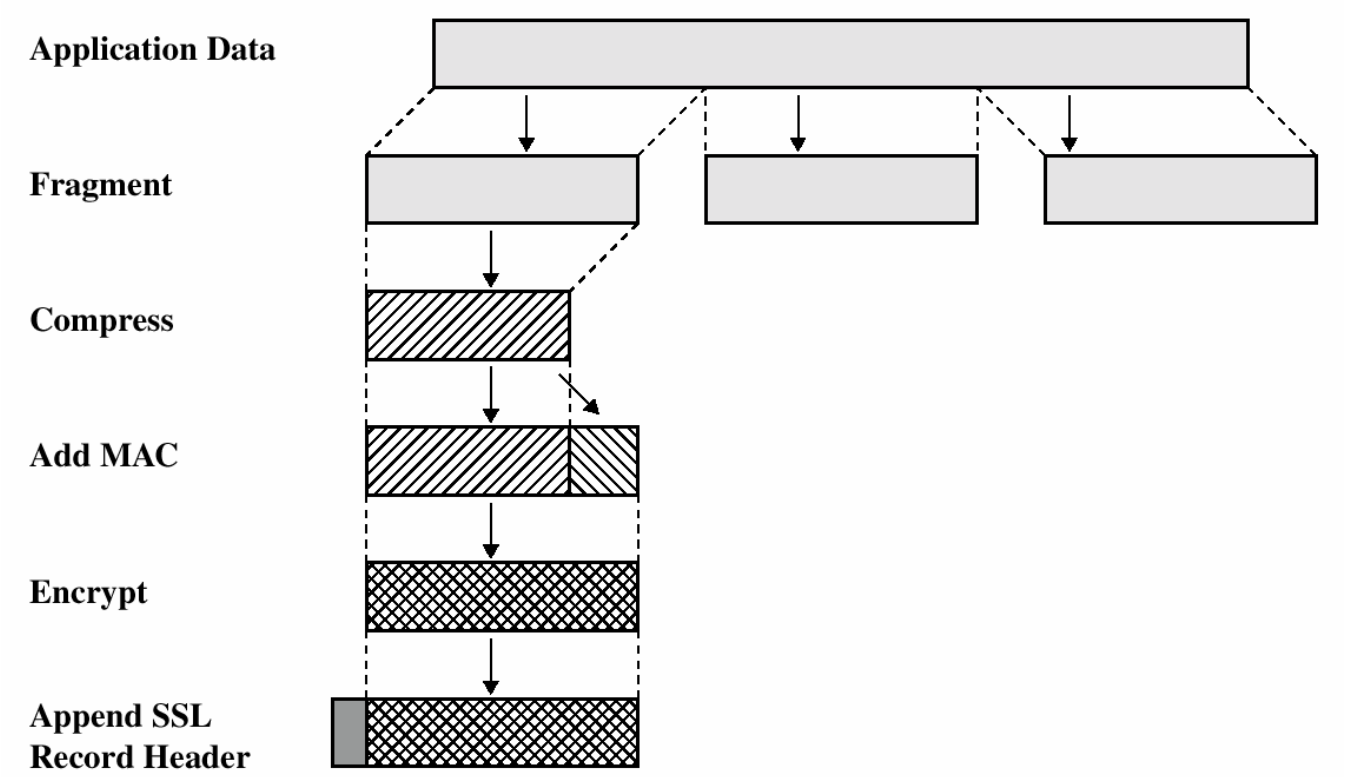
Η επικεφαλίδα μπορεί να είναι 3 bytes ή 2 bytes , από αν τα δεδομένα χρειάζονται συμπλήρωμα (padding).Για την επικεφαλίδα των 2 bytes το μέγεθος του πακέτου είναι 32767 bytes, ενώ για την επικεφαλίδα των 3 bytes το μέγεθος είναι 16383 bytes.

Το πεδίο escape bit είναι 3 bytes.

Το κομμάτι των δεδομένων αποτελείται από ένα MAC, τα πραγματικά δεδομένα και τα δεδομένα συμπλήρωσης, εάν χρειάζονται. Αυτό το κομμάτι είναι που κρυπτογραφείται κατά την μετάδοση. Όταν οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται είναι τύπου block cipher τότε απαιτούνται συμπληρωματικά δεδομένα και ο ρόλος τους είναι να συμπληρώνουν τα πραγματικά δεδομένα ώστε το μέγεθος τους είναι πολλαπλάσιου του μεγέθους που δέχεται σαν είσοδο ο block cipher .

Εάν χρησιμοποιούνται stream cipher τότε δεν απαιτείται συμπλήρωμα και μπορεί αν χρησιμοποιηθεί η επικεφαλίδα των 2 bytes.

Το SSL Record Protocol (SSLRP) εξασφαλίζει εμπιστευτικότητα ,ακεραιότητα δεδομένων και προστασία από επιθέσεις. Δέχεται δεδομένα υψηλότερων επιπέδων κάνει κατακερματισμό (Fragmentation ), συμπίεση και κρυπτογράφηση δεδομένων.




**Εικόνα 45: λειτουργίες του SSL Record Protocol**

- **Με Handshake Protocol (SSLHP)**

Το SSL **Handshake Protocol** υποχρεώνει έναν πελάτη ( client ) και έναν εξυπηρετητή (server)

- να καθιερώνουν τα πρωτόκολλα που θα χρησιμοποιηθούν κατά τη διάρκεια της επικοινωνίας
- να επιλέγουν τη μέθοδο συμπίεσης και την προδιαγραφή κρυπτογραφίας
- να αυθεντικοποιούνται αμοιβαία
- να δημιουργούν ένα κύριο μυστικό κλειδί (master secret key )από το οποίο προκύπτουν διάφορα κλειδιά συνόδου για αυθεντικοποίηση και κρυπτογράφηση μηνυμάτων.

Το πρωτόκολλο SSL **Handshake χωρίζεται** σε δύο φάσεις:

- στην πρώτη φάση επιλέγονται οι αλγόριθμοι γίνεται η ανταλλαγής master secret key και πιστοποιείτε η ταυτότητα του server.
- Στη δεύτερη φάση γίνεται η διαχείριση της πιστοποίησης της ταυτότητας του client (εάν ζητηθεί) και ολοκληρώνεται η διαδικασία του handshaking . Μετά την ολοκλήρωση των δύο φάσεων το στάδιο handshaking τελειώνει και η μεταφορά μεταξύ των δύο άκρων αρχίζει.

***Η διαδικασία SSL Handshake βήμα προς βήμα***

**βήμα 1$^{ο}$** : Ο SSL client συνδέεται με τον SSL server και ζητά πιστοποίηση. Ο client ενημερώνει για τους αλγορίθμους κρυπτογράφησης που υποστηρίζει. Ο server επιβεβαιώνει ότι μπορεί να υποστηρίξει τους αλγορίθμους αυτούς και ορίζει ένα μοναδικό αριθμό (connection id) στη σύνδεση που έχει δημιουργηθεί.
**Βήμα 2$^{ο}$** : Ο server πιστοποιεί την ταυτότητά του με την αποστολή του ψηφιακού του πιστοποιητικού. Η επαλήθευση των πιστοποιητικών γίνεται με τον έλεγχο των ημερομηνιών εγκυρότητας και με το γεγονός ότι το πιστοποιητικό φέρει την υπογραφή μίας διαπιστευμένης αρχής πιστοποιητικού. Υπάρχει περίπτωση ο server να ζητήσει πιστοποίηση ταυτότητας από τον server.
**Βήμα 3$^{ο}$ :** Εάν ο server έχει ζητήσει πιστοποιητικό γνησιότητας από τον client, αυτός το αποστέλλει. Στη συνέχεια πραγματοποιείται διαπραγμάτευση για τον αλγόριθμο κρυπτογράφησης μηνύματος και για τη συνάρτηση κατακερματισμού. Συνήθως ο server επιλέγει την πιο ισχυρή κρυπτογραφική μέθοδο από αυτές που του πρότεινε ο client. Παράλληλα ο client και ο server παράγουν τα κλειδιά συνόδου με την ακόλουθη διαδικασία :

- Αρχικά ο client παράγει έναν τυχαίο αριθμό τον οποίο στέλνει στο server , κρυπτογραφημένο με το δημόσιο κλειδί του server (που έχει αποκτηθεί από το πιστοποιητικό του server).
- Στη συνέχεια ο server απαντά με περισσότερα τυχαία δεδομένα κρυπτογραφημένα με το δημόσιο κλειδί του client, αν είναι διαθέσιμο. Αλλιώς, στέλνει τα δεδομένα μη κρυπτογραφημένα – clear text.
- Και τέλος με τη χρήση των συναρτήσεων κατακερματισμού παράγονται από τα τυχαία δεδομένα τα κλειδιά κρυπτογράφησης.

**Βήμα 4$^{ο}$** :Ανταλλάσσονται μηνύματα τερματισμού των διαδικασιών του **Handshake Protocol.**

***Επιθέσεις που δέχεται το SSL πρωτόκολλο***

- **Επίθεση Dictionary Attack** : η επίθεση γίνεται από κάποιον επιτήδειο ο οποίος έχει στην κατοχή του ένα μέρος μη κρυπτογραφημένου κειμένου. Στην περίπτωση αυτή γίνεται κρυπτογράφηση του μέρους αυτού χρησιμοποιώντας κάθε πιθανό κλειδί . η έρευνα συνεχίζεται σε όλο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί το κομμάτι που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Η έρευνα είναι επιτυχής όταν βρεθεί το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος . Το SSL δεν εκτελείτε όταν τα κλειδιά του αλγορίθμου έχουν μέγεθος 128 bit.
- **Επίθεση Brute Force Attack :** Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Δεν έχει νόημα η επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits.

- **Επίθεση Replay Attack : η επίθεση αυτή πραγματοποιείτε** όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server. Το SSL όμως χρησιμοποιεί το connection – id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν γίνεται να υπάρχουν δυο ίδια connection – id, και ο server δεν δέχεται το σύνολο των είδη χρησιμοποιημένων μηνυμάτων . Το connection – id, έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.
- **Επίθεση Man In The Middle :** στην περίπτωση αυτή ένας τρίτος παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αυτό που κάνει είναι να προωθεί μηνύματα στο server αφού πρώτα επεξεργαστεί τα μηνύματα του client και τα τροποποιήσει όπως αυτός επιθυμεί. Το ίδιο κάνει και για τα μηνύματα που προέρχονται από τον server. Προσποιείται στον client ότι είναι ο server και αντίστροφα. Όμως το SSL ζητάει ταυτοποίηση της ταυτότητάς του server την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατη. Συνεπώς, ο επιτιθέμενος δεν μπορεί να πείσει τον client ότι είναι ο server.
-

***Πλεονεκτήματα SSL***

- Είναι εύκολα διαχειρίσημο από τους χρήστες και δεν απαιτεί ιδιαίτερες τεχνικές γνώσεις.
- Είναι εγκατεστημένο σε κάθε υπολογιστή που έχει συνδεθεί μέσω του standard browser στο διαδίκτυο και δεν χρειάζεται ιδιαίτερες ρυθμίσεις.
- Είναι ανεξάρτητο από το λειτουργικό σύστημα .
- Προσφέρει έλεγχο πρόσβασης σε εφαρμογές VANs extranet ή VPNs απομακρυσμένης πρόσβασης.
- Δίνει τη δυνατότητα πρόσβασης στο χρήστη σε εφαρμογές web από οπουδήποτε με τη χρήση web browser,μιας σύνδεσης στο internet και χωρίς να έχει κάποιο λογισμικό στον υπολογιστή.
- Αντιμετωπίζουν θέματα NAT περνώντας πάνω από τείχους προστασίας (firewalls) .

***Μειονεκτήματα SSL***

- Το βασικό μειονέκτημα της χρήσης του SSL πρωτοκόλλου είναι η επιβράδυνση που δημιουργείτε στην επικοινωνία του browser του client με τον HTTPS server.
- Άλλη μεγάλη αδυναμία του SSL είναι η ευαισθησία των αλγορίθμων που χρησιμοποιούν μικρά κλειδιά. Οι RC4-49, RC2-40 και DES-56 θα πρέπει ν αποφεύγονται γιατί εισάγουν σοβαρά προβλήματα στην ασφάλεια.
- Επίσης η μακροχρόνια χρήση του SSL σε μια σύνδεση (π.χ εφαρμογή TELNET ) δημιουργεί αδυναμία στην αλλαγή του master key το οποίο χρησιμοποιείται καθ' όλη τη διάρκεια της σύνδεσης. Το γεγονός αυτό δημιουργεί επικινδυνότητα επιθέσεων . Για το λόγο αυτό κρίνετε απαραίτητη η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα.

Ανακεφαλαιώνοντας γίνεται μια σύγκριση μεταξύ των πρωτοκόλλων όλων των επιπέδων .

**Σύγκριση πρωτοκόλλων**

| | MPLS VPNs | IPSec VPNs | SSL VPNs |
|---|---|---|---|
| **Πιστοποίηση ταυτότητας χρήστη (δηλαδή έλεγχος της πρόσβασης στη δίοδο)** | Βασίζεται στη χρήση των μοναδικών route distinguishers. Παρέχεται πρόσβαση στην ομάδα που χρησιμοποιεί την υπηρεσία και απορρίπτεται κάθε άλλου είδους μη εξουσιοδοτημένη πρόσβαση | Μέσω ψηφιακού πιστοποιητικού ή προ-διαμοιρασμένου κλειδί | Μέσω ψηφιακού πιστοποιητικού |
| **Εμπιστευτικότητα** | Διαχωρισμός κίνησης μέσω των RDs | Μηχανισμοί κρυπτογράφησης στο επίπεδο δικτύου IP | Μηχανισμοί κρυπτογράφησης |
| **Κλιμάκωση** | Υψηλή. Ικανό να υποστηρίζει δεκάδες χιλιάδες VPNs πάνω από το ίδιο δίκτυο | Αποδεκτή. Μπορεί να απαιτεί επιπρόσθετο σχεδιασμό για τη διανομή κλειδιού, τη διαχείριση κλειδιού, | Δεν τίθεται ζήτημα κλιμάκωσης. Το δίκτυο του ISP δε γνωρίζει την κίνηση SSL |
| **Εξοπλισμός** | Απαιτούνται στοιχεία του δικτύου MPLS του δικτύου κορμού του ISP | Μπορεί να αναπτυχθεί πάνω από τα υπάρχοντα δίκτυα IP ή το Internet | Δεν απαιτείται. Το δίκτυο του ISP δε γνωρίζει την κίνηση SSL |
| **QoS** | Υποστηρίζουν SLAs παρέχοντας μηχανισμούς QoS, με εγγυημένο bandwidth, | Δεν υποστηρίζουν. | Δεν υποστηρίζουν. Το δίκτυο του ISP δε γνωρίζει την κίνηση SSL |
| **VPN client** | Δεν απαιτείται διότι το MPLS VPN είναι μία υπηρεσία που υλοποιείται στο επίπεδο δικτύου και οι χρήστες δε χρειάζονται VPN clients για να αλληλεπιδράσουν με το δίκτυο. | Απαιτείται για απομακρυσμένη πρόσβαση ενός χρήστη μέσω IPSec VPN. (Π.χ. το λογισμικό Cisco VPN Client, το οποίο υποστηρίζεται από τα λειτουργικά συστήματα Microsoft Windows, Solaris, Linux και Macintosh) | Δεν απαιτείται. Βασίζεται στο Web browser. |

## Κεφάλαιο 5ο

### Συμπεράσματα

Συνοψίζοντας λοιπόν ,βλέπουμε ότι τα VPNs αποτελούν βασικό κομμάτι των IP δικτύων του Internet και μια πολύ καλή επιλογή για τις επιχειρήσεις εφόσον τους προσφέρει ασφάλεια και υψηλής ποιότητας υπηρεσίες(ανάλογα την ποιότητα του δικτύου πάνω στο οποίο υλοποιούνται ) συνδυάζει πρακτικότητα και οικονομία ,μειώνεται το κόστους τηλεπικοινωνιών ,παρουσιάζει ευκαμψία και προσαρμοστικότητα χάρη στους μηχανισμούς δρομολόγησης στο internet,οι τεχνολογίες είναι συμβατές αφού μπορούν να διαχειριστούν από το ISP , αυξάνεται απεριόριστα η χωρητικότητας και τέλος το δίκτυο επεκτείνεται σε πολλές και διαφορετικές περιοχές με μεγάλη ευελιξία .

Το τηλεπικοινωνιακό κόστος είναι χαμηλό εφόσον χρησιμοποιείτε το δημόσιο δίκτυο .

Το κόστος υλοποίησης εξαρτάτε από τον αριθμό των σημείων σύνδεσης την χωρητικότητα σύνδεσής του ,τα κανάλια φωνής που υποστηρίζει ,την επιλογή ταχύτητας πρόσβασης στο internet ,τον αριθμό απομακρυσμένων χρηστών που θα καλύπτουν τηλεφωνικά ,την κοινή χρήση εφαρμογών και τα τηλεπικοινωνιακά έξοδα σύνδεσης των σημείων .

Ο εξοπλισμός υλοποίησης των VPNs συνήθως περιλαμβάνεται στην τιμή διάθεσης τους, με την μορφή ενοικίασης. Τα εφεδρικά κυκλώματα ( ISDN γραμμές) περιλαμβάνονται κ αυτά στο συνολικό σχεδιασμό και κόστος με τον παροχέα των VPNs να αναλαμβάνει την εγκατάσταση, την συντήρηση ,την παρακολούθηση ,την επέμβαση σε περιπτώσεις προβλημάτων του δικτύου VPN και την ενεργοποίησή τους.

**Βιβλιογραφία**


1.Patrick J.Montana & Bruce H. Charnov, Μάνατζμεντ σειρά οικονομία και επιχείρηση, εκδόσεις Κλειδάριθμος 2002.

2. JoAnne Woodcock, Εισαγωγή στα δίκτυα υπολογιστών, εκδόσεις κλειδάριθμος 2000.

3. Σπυριδούλα Μαργαρίτη & Στεργίου Ελευθέριος ,Τοπικά και αστικά δίκτυα ,εκδόσεις νέων τεχνολόγων 2007.

4. Πτυχιακή εργασία ,Ασφαλής μεταφορά δεδομένων με τη χρήση ιδεατών ιδιωτικών δικτύων ,Σκορδά Χριστίνα & Γιαννακουδάκης Νικόλαος ,2006.

5. Διπλωματική εργασία ,Διαχείριση κινητικότητας και ασφάλειας σε ασύρματα εικονικά ιδιωτικά δίκτυα ,Κωσταντινίδης Χ.Αριστοτέλης ,2004.

6. Πτυχιακή εργασία ,Εικονικά Ιδιωτικά Δίκτυα , Κουτρουμπής Μιχάλης & Ελευθεριάδου Ευμορφύλη ,2006 .

7. http://openclass.teiwm.gr/modules/document/file.php/INFORMATIC105/SSL%20-TLS.pdf

8. http://www.forwww.gr/sites/default/files/epikoinonies_dedomenon_-_diktua.pdf

9. http://www.excelixi.org/el/Knowledge-Base/e-Business/Virtual-Private-Networks

10. http://www.uniquelife.gr/ti-ine-vpn-ke-giati-chriazomaste/

11. http://openclass.teiwm.gr/modules/document/file.php/INFORMATIC105/SSL%20-TLS.pdf

12. http://openclass.teiwm.gr/modules/document/file.php/INFORMATIC105/VPN.pdf

13 . http://docplayer.gr/4749190-Shediasmos-eikonikon-diktyon-enotita-5-eikonika-idiotika-diktya-epipedoy-zeyxis-dedomenon-layer-2-vpns.html

14. http://openclass.teiwm.gr/modules/units/?course=INFORMATIC105&id=196

15. https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjC4ejs87nQAhWL6xQKHZEzB80QFghAMAM&url=http%3A%2F%2Fwww.pyxida.aueb.gr%2Fgetfile.php%3Fobject_id%3Diid%3A3510%26ds_id%3DPDF1&usg=AFQjCNFjj-5kknqc3OIoobgGfW6zucRruw&sig2=9WWpPBA1YZ-zRCpq-DCYEQ

16. https://eclass.upatras.gr/modules/document/file.php/CEID1064/%CE%94%CE%B9%CE%B1%CE%BB%CE%AD%CE%BE%CE%B5%CE%B9%CF%82%202014-15/06_MPLS.pdf

17. http://www.excelixi.org/el/Knowledge-Base/e-Business/Virtual-Private-Networks

18. http://searchnetworking.techtarget.com/definition/hardware-VPN

19. https://www.techopedia.com/definition/15237/hardware-virtual-private-network-hardwarevpn

20. http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2004-0206/DT2004-0206.doc

21. http://www.ekoletsou.gr/pdfFiles/VPN.pdf

22. http://conta.uom.gr/conta/ekpaideysh/seminaria/M_NetworkTech/chilasvpn.pdf

23. https://www.pcsteps.gr/1376-vpn-technology-explained/#__

24. http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4081/Plessas.pdf?sequence=2

25. http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2005/VPN%20ARCHITECTURES.pdf