ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Αρχιτεκτονική
Εικονικών Ιδιωτικών Δικτύων

ΙΑΝΟΥΑΡΙΟΣ 2006

ΒΑΣΙΛΗΣ Ε. ΨΩΜΟΣ
mis0515@uom.gr
M.I.S. M.15/05

Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων
Καθηγητές: Α.Α. Οικονομίδης & Α. Πομπόρτσης

UNIVERSITY OF MACEDONIA

MASTER IN INFORMATION SYSTEMS

Architecture of Virtual Private Networks

JANUARY 2006

VASILIS. E. PSOMOS
mis0515@uom.gr
M.I.S. M.15/05

University of Macedonia
Master Information Systems
Networking Technologies
Professors: A.A. Economides & A. Pomportsis

Abstract

It is common knowledge that the Internet has rapidly expanded worldwide. It has already conquered not only the scientific but enterprising world as well. These developments , on one hand, increased their productivity and profitability, however simultaneously they created new demands. Thus the enterprises realised that answer in their problems was the utilisation of Virtual Private Networks (VPN) in order to supplement their existing infrastructure and overcome problems of communication, organisation, management and distribution of information in all the departments or their subsidiary companies, wherever they may be. This paper analyzes and organizes the basic categories VPNs and the different protocols that can be used. Finally conclusions are exported commenting on the advantages and disadvantages of each protocol

Περίληψη

Είναι πανθομολογούμενο ότι το διαδίκτυο έχει εξαπλωθεί με ραγδαίους ρυθμούς. Έχει κατακυριεύσει πλέον τον επιστημονικό αλλά και τον επιχειρηματικό κόσμο. Αυτές οι εξελίξεις έχουν μεν αυξήσει την παραγωγικότητα και την κερδοφορία τους, έχουν όμως ταυτόχρονα δημιουργήσει νέες απαιτήσεις. Έτσι οι επιχειρήσεις συνειδητοποίησαν ότι απάντηση στα προβλήματά τους ήταν η χρησιμοποίηση Εικονικών Ιδιωτικών Δικτύων (VPN) για να συμπληρώσουν την υπάρχουσα υποδομή τους και να ξεπεράσουν προβλήματα επικοινωνίας, οργάνωσης, διαχείρισης και κατανομής πληροφοριών σε όλα τα τμήματα ή τα υποκαταστήματά τους, όπου κι αν βρίσκονται. Στην παρούσα εργασία αναλύονται οι βασικές κατηγορίες VPN και περιγράφονται τα διαφορετικά πρωτόκολλα που μπορούν να χρησιμοποιηθούν. Τέλος εξάγονται και συμπεράσματα για τα πλεονεκτήματα και μειονεκτήματα κάθε πρωτοκόλλου.

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ 4

1.1 Εισαγωγή 4

2. ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ 6

2.1 Εικονικά Ιδιωτικά Δίκτυα 6

2.2 Δομικά Στοιχεία Εικονικών Ιδιωτικών Δικτύων 7

2.3 Πλεονεκτήματα Εικονικών Ιδιωτικών Δικτύων 9

2.4 Αρχιτεκτονικές Εικονικών Ιδιωτικών Δικτύων 10

3. ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΙΔΙΩΤΙΚΩΝ ΕΙΚΟΝΙΚΩΝΔΙΚΤΥΩΝ ΜΕ ΒΑΣΗ ΤΑ ΕΠΙΠΕΔΑ ΤΟΥ OSI 13

3.1.1 Εικονικά ιδιωτικά δίκτυα επιπέδου δικτύου βασισμένα στην τεχνολογία MPLS..... 13

3.1.2 Εικονικά ιδιωτικά δίκτυα επιπέδου δικτύου βασισμένα στο πρωτόκολλο IPSec 16

3.2.1 Εικονικά ιδιωτικά δίκτυα επιπέδου ζεύξης δεδομένων βασισμένα στο πρωτόκολλο PPTP 26

3.2.2 Εικονικά ιδιωτικά δίκτυα επιπέδου ζεύξης δεδομένων βασισμένα στο πρωτόκολλο L2TP 33

3.3 Εικονικά ιδιωτικά δίκτυα επιπέδου μεταφοράς βασισμένα στο πρωτόκολλο SSL..... 36

4. ΣΥΜΠΕΡΑΣΜΑΤΑ..... 41

ΒΙΒΛΙΟΓΡΑΦΙΑ 42

WHITE PAPERS 44

ΔΙΑΔΙΚΤΥΟ 45

ΠΕΡΙΕΧΟΜΕΝΑ

1. INRODUCTION 4

1.1 Introduction 4

2. VIRTUAL PRIVATE NETWORKS 6

2.1 Virtual private networks 6

2.2 Structural Components of virtual private networks 7

2.3 Advantages of Virtual private networks 9

2.4 Architectures of Virtual private networks 10

3. ARCHITECTURES OF VIRTUAL PRIVATE NETWORKS BASED ON OSI LAYERS 13

3.1.1 Network layer virtual private networks based on MPLS technology 13

3.1.2 Network layer virtual private networks based on IPSec protocol 16

3.2.1 Data link layer virtual private networks based on PPTP protocol 26

3.2.2 Data link layer virtual private networks based on L2TP protocol 33

3.3 Transport layer private networks based on SSL protocol 36

4. CONCLUSIONS 41

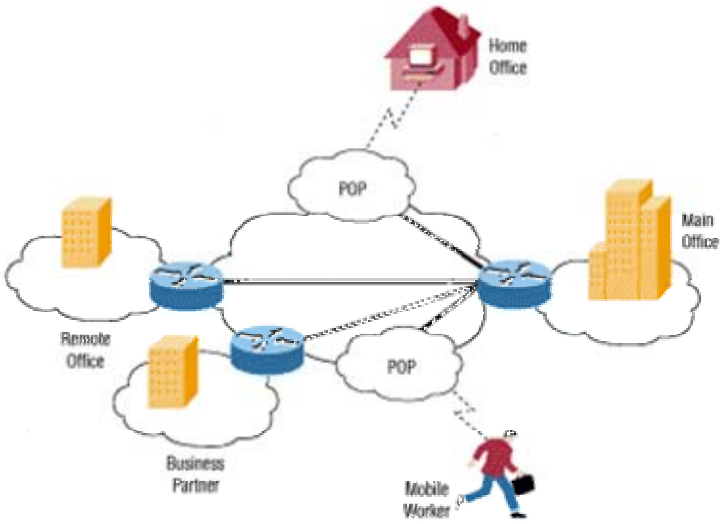
BOOK REFERENCES 42

WHITE PAPERS 44

WEB REFERENCES 45

1. ΕΙΣΑΓΩΓΗ

Είναι πανθομολογούμενο ότι το διαδίκτυο (Internet) έχει εξαπλωθεί με ραγδαίους ρυθμούς. Έχει κατακυριεύσει πλέον τον επιστημονικό αλλά και τον επιχειρηματικό κόσμο. Ο ανταγωνισμός έχει οδηγήσει τόσο σε συμμαχίες, αλλά και συνεταιρισμούς μεταξύ επιχειρήσεων. Αυτές οι εξελίξεις έχουν μεν αυξήσει την παραγωγικότητα και την κερδοφορία τους, έχουν όμως ταυτόχρονα δημιουργήσει νέες απαιτήσεις. Ένα δίκτυο που επικεντρώνεται στο να συνδέει με ευθείες/μισθωμένες γραμμές (leased lines) ή Frame Relay/ATM δίκτυα τα κεντρικά υποκαταστήματα/γραφεία των συνεργαζόμενων επιχειρήσεων δεν είναι πλέον αρκετό για πολλές επιχειρήσεις. Υπάρχει μεγάλος αριθμός απομακρυσμένων χρηστών του δικτύου των επιχειρήσεων, όπως για παράδειγμα οι εξωτερικοί συνεργάτες, που είναι απαραίτητο να έχουν πρόσβαση στους πόρους του δικτύου της επιχείρησης. Για παράδειγμα, θα πρέπει ένας εξωτερικός συνεργάτης μιας επιχείρησης να έχει τη δυνατότητα πρόσβασης σε δεδομένα και υπηρεσίες μέσα από το τοπικό δίκτυο μιας επιχείρησης, όχι μόνο από το σπίτι, αλλά και οπουδήποτε κι αν βρίσκεται, με τη χρήση του φορητού του υπολογιστή ή του PDA .



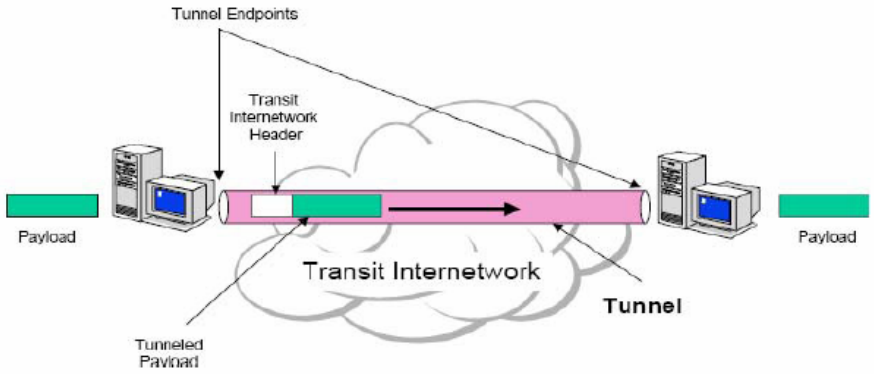
Εικόνα 1*: Οι επικοινωνιακές ανάγκες μιας σύγχρονης επιχείρησης την εποχή της παγκοσμιοποίησης*

Επιπρόσθετα η συντήρηση των μισθωμένων γραμμών (leased lines) ή Frame Relay/ATM δικτύων είναι όχι μόνο πολυδάπανη, αλλά και προβληματική πολλές φορές είτε εξαιτίας της γεωγραφικής απόστασης είτε εξαιτίας υπερφόρτωσης των γραμμών. Από την άλλη η εξέλιξη του Internet, του World Wide Web καθώς και η εμφάνιση της τεχνολογίας των Intranets, οδήγησαν τις επιχειρήσεις στο να συνειδητοποιήσουν ότι οι τεχνολογίες του Internet θα μπορούσαν να χρησιμοποιηθούν ώστε να επεκτείνουν ή να αντικαταστήσουν τις client/server εφαρμογές στα Ιδιωτικά τους Δίκτυα (Private Networks). Έτσι οι επιχειρήσεις συνειδητοποίησαν ότι απάντηση στα προβλήματά τους ήταν η χρησιμοποίηση Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks) για να συμπληρώσουν την υπάρχουσα υποδομή τους και να ξεπεράσουν προβλήματα επικοινωνίας, οργάνωσης, διαχείρισης και κατανομής πληροφοριών σε όλα τα τμήματα ή τα υποκαταστήματά τους, όπου κι αν βρίσκονται.

2.1 ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ

Ας ξεκινήσουμε με μια προσέγγιση του τι είναι ένα Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network). **Η μεταφορά μέσω του δημόσιου δικτύου (πχ. Internet) εμπιστευτικής πληροφορίας, με έναν αξιόπιστο και ασφαλή τρόπο, καλείται Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network)**. Ο όρος «Ιδιωτικό Δίκτυο» σημαίνει ότι πρόσβαση έχουν μόνο οι εξουσιοδοτημένοι χρήστες. Ο όρος «Εικονικό Δίκτυο» σημαίνει ότι οι δικτυακές συνδέσεις είναι ιδεατές, αφού τα δεδομένα ακολουθούν κάθε φορά διαφορετική διαδρομή για να φτάσουν στον προορισμό τους. Γενικά, το VPN είναι μια διαδικασία ή ρύθμιση τέτοια ώστε το Internet ή το δημόσιο δίκτυο να είναι ασφαλές και να λειτουργεί όπως ένα Ιδιωτικό Δίκτυο (Private Network). Με άλλα λόγια, την ιδιωτικότητα δεν την εξασφαλίζουν τα κυκλώματα (circuits) ή οι μισθωμένες γραμμές (leased lines), αλλά οι μηχανισμοί ασφαλείας και οι επεξεργασίες που, στα πλαίσια ενός VPN, επιτρέπουν μόνο σε συγκεκριμένους χρήστες την πρόσβαση σε εμπιστευτικά δεδομένα.

Τα Εικονικά Ιδιωτικά Δίκτυα μπορούν πολύ εύκολα να βρουν εφαρμογή είτε σε μεγάλες επιχειρήσεις είτε σε απομακρυσμένους χρήστες. Έτσι μια εταιρία ή ένας χρήστης ξεκινά μια ιδιωτική σύνδεση μέσω του ISP (Internet Service Provider), ο οποίος είναι ο αποκλειστικός υπεύθυνος για την περαιτέρω δρομολόγηση της μεταδιδόμενης πληροφορίας (πάνω στην υποδομή του Internet). Η ζεύξη για μία συγκεκριμένη επικοινωνία δύο «τελικών χρηστών» γίνεται δυναμικά: όταν ολοκληρωθεί η επικοινωνία, το εύρος ζώνης αποδεσμεύεται. Οι εικονικές ζεύξεις πραγματοποιούνται με ενθυλάκωση των πακέτων δεδομένων σε ειδικά IP πακέτα, κατάλληλων για μετάδοση σε δίκτυο Internet (πρωτοκόλλου IP). Στην ορολογία των VPN: αυτές οι εικονικές ζεύξεις ονομάζονται δίοδοι ή τούνελ (tunnels).



***Εικόνα 2**: Σχηματική αναπαράσταση ενός tunnel να μεταφέρει δεδομένα από ένα δίκτυο σε ένα άλλο μέσα από την λειτουργία ενός VPN*

2.2 ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΕΙΚΟΝΙΚΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ

Τα δομικά στοιχεία από τα οποία μπορεί να αποτελείται ένα VPN είναι το Internet, οι πύλες ασφαλείας, οι διακομιστές ασφάλειας (Security Police Servers), και οι υπηρεσίες πιστοποίησης (Certificate Authorities).

Το Internet είναι απαραίτητο για την μετάδοση των δεδομένων. Από ένα υπολογιστή μέσω μιας dial-up σύνδεσης (για παράδειγμα) πηγαίνουν στο Point Of Presence του Internet Service Provider και στην συνέχεια στο δίκτυο μέχρι να φτάσουν στο POP που βρίσκεται πλησιέστερα στον παραλήπτη.

Τα υπόλοιπα τρία στοιχεία είναι απαραίτητα για την ασφάλεια μετάδοσης των δεδομένων μας. Οι πύλες ασφαλείας υπάγονται σε 4 κατηγορίες.

- Δρομολογητές (routers)

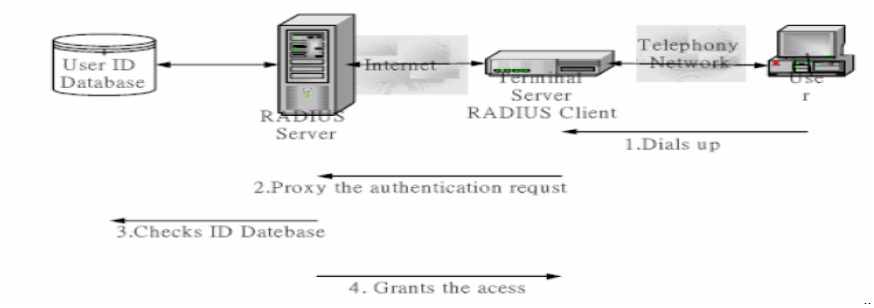
  Κάνουν κρυπτογράφηση των πακέτων που λαμβάνουν και προωθούν. Η κρυπτογράφηση μπορεί να γίνεται είτε με λογισμικό είτε με ξεχωριστό κύκλωμα για κρυπτογράφηση οπότε και η ταχύτητα είναι μεγαλύτερη. Ασφαλώς, όσο μεγαλύτερη είναι η απόδοση ενός δρομολογητή τόσο μεγαλύτερη θα είναι και η απόδοση όλου του VPN

- Τοίχοι Προστασίας (Firewalls)

  Φιλτράρουν τα δεδομένα με βάση τη διεύθυνση που αναγράφει το κάθε πακέτο. Επίσης κάνουν και κρυπτογράφηση. Σε μεγάλα όμως δίκτυα με μεγάλο φόρτο, αν τα firewalls πραγματοποιούν κρυπτογράφηση, πέφτει η συνολική απόδοση.

- Διακομιστές Ασφάλειας (Security Police Servers)

  Εξετάζουν τα δικαιώματα πρόσβασης των χρηστών και στέλνουν την κατάλληλη πληροφορία στις πύλες ασφαλείας. Σε πολλά συστήματα χρησιμοποιείται ένας RADIUS Server. Είναι επίσης υπεύθυνοι για τη διαχείριση του κλειδιού (IPsec πρωτόκολλο)



Εικόνα 3: RADIUS Server (Remote Authentication Dial-in User Service)

- Υπηρεσίες πιστοποίησης (Certificate Authorities)

Χρησιμοποιείται για τον έλεγχο της ορθότητας των στοιχείων ταυτότητας κάθε χρήστη που υπάρχουν στη βάση δεδομένων.

2.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΕΙΚΟΝΙΚΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ

Ένα Εικονικό Ιδιωτικό Δίκτυο χαρακτηρίζεται από ασφάλεια και από υψηλή ποιότητα υπηρεσιών. Ωστόσο οι λόγοι της εξάπλωσης των VPNs ήταν ένας συνδυασμός της πρακτικότητας και της οικονομικότητας τους.

Καταρχήν, η προσέγγιση των VPNs οδηγεί σε εντυπωσιακή μείωση του κόστους τηλεπικοινωνιών. Από τη μια το κόστος των μισθωμένων γραμμών απαιτούν μεγάλο μηνιαίο πάγιο και υψηλή χρέωση που γίνεται υψηλότερη ανάλογα με την απόσταση. Από την άλλη, εφόσον η «συνδεσιμότητα» (connectivity) στο Internet είναι καθολική, μια σύνδεση υψηλής ταχύτητας προϋποθέτει μόνο μία τοπική μισθωμένη γραμμή.

Επιπλέον, τα VPNs παρουσιάζουν «ευκαμψία» (flexibility) και προσαρμοστικότητα (scalability) χάρη στους μηχανισμούς δρομολόγησης στο Internet. Στα παραδοσιακά PN δίκτυα οι διαφορετικές τεχνολογίες που ενυπάρχουν στο εσωτερικό του δικτύου χρειάζονται ειδικό πρόσθετο εξοπλισμό προκειμένου να εξασφαλιστεί συμβατότητα. Αντίθετα στα VPNs όλες οι τεχνολογίες είναι συμβατές, αφού όλες μπορεί να τις χειριστεί ο ISP. Ακόμη στα παραδοσιακά PN δίκτυα, εάν επιθυμούσαμε να επεκτείνουμε το δίκτυο ώστε να περιλαμβάνει και ένα ακόμα σημείο (site), τότε θα έπρεπε να παραγγελθεί και να εγκατασταθεί μια επιπλέον μισθωμένη γραμμή. Σε ένα VPN όμως, αυτό που θα χρειάζονταν για την προσθήκη του επιπλέον σημείου (site) θα ήταν ένας επιπλέον δρομολογητής, και κατάλληλη διαμόρφωση των ήδη υπαρχόντων δρομολογητών –απλή εργασία για ένα διαχειριστή δικτύου. Έτσι επιτυγχάνουμε καλύτερη γεωγραφική επεκτασιμότητα του δικτύου, μιας και οποιοσδήποτε χρήστης από οποιοσδήποτε μέρος και αν βρίσκεται μπορεί να συνδεθεί στο VPN, αρκεί ο ISP να διαθέτει σημείο πρόσβασης στο Internet, POP (Point of Presence).

2.3 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΕΙΚΟΝΙΚΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ

Τα Εικονικά Ιδιωτικά Δίκτυα μπορούν να κατηγοριοποιηθούν με διάφορους τρόπους, ανάλογα με την οπτική γωνία που τα εξετάζει κανείς. Οι διάφοροι τρόποι κατηγοριοποίησης τους περιγράφονται παρακάτω:

1. Μια οπτική γωνία είναι με βάση την αντιστοιχία τους με τα επίπεδα του μοντέλου αναφοράς OSI. Οπότε τα Εικονικό Ιδιωτικά Δίκτυα κατηγοριοποιούνται ως εξής:

   - Στα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου 3 (Δικτύου). Σε αυτήν ανήκουν τα VPN που δομούνται πάνω σε IP δίκτυα και χρησιμοποιούν το πρωτόκολλο [IPSec, καθώς και τα VPN που δομούνται πάνω σε MLPS δίκτυα.

   - Στα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου 2 (Ζεύξης Δεδομένων). Σε αυτήν την κατηγορία εμπίπτουν τα VPN στα οποία χρησιμοποιείται κάποιο από τα πρωτόκολλα L2F, PPTP, L2TP. Επίσης VPN επιπέδου 2 μπορούν να αναπτυχθούν πάνω στην τεχνολογία MLPS.

   - Στα Εικονικά Δίκτυα επίπεδου 4 (Μεταφοράς). Σε αυτήν την κατηγορία εμπίπτουν τα VPN στα οποία χρησιμοποιείται το πρωτόκολλο SSL.

<table>
<tr><td>Application</td><td colspan="3">Application proxy server</td></tr>
<tr><td>Presentation</td><td colspan="3"></td></tr>
<tr><td>Session</td><td></td><td colspan="2">HTTPS</td></tr>
<tr><td>Transport</td><td>SOCKS</td><td colspan="2">SSL</td></tr>
<tr><td>Network</td><td>IPSec(IP Security)</td><td colspan="2">L2TP
(Layer 2 Tunneling Protocol)</td></tr>
<tr><td>Data Link</td><td>L2F(Layer 2 Forwarding)
PPTP(Point to Point Tunneling Protocol)</td><td colspan="2"></td></tr>
<tr><td>Physical</td><td colspan="3"></td></tr>
</table>

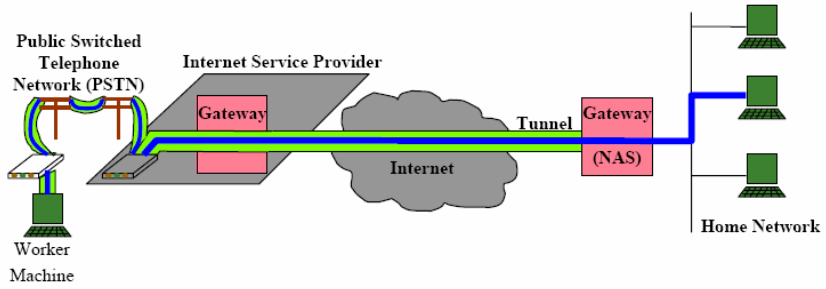
Εικόνα 4*: Στρωμάτωση των πρωτοκόλλων στα VPN και συσχέτισή τους με τα στρώματα OSI*

2. Με βάση το είδος της διόδου (tunnel) ,του νοητού κυκλώματος που σχηματίζεται και μέσω του οποίου γίνεται η μετάδοση των δεδομένων στο VPN). Υπάρχουν δύο είδη διόδων που προσδιορίζουν και την αντίστοιχη κατηγορία στην οποία εμπίπτει ένα VPN:

- Οι «αυθόρμητες» δίοδοι (voluntary tunnels),
- Οι «αναγκαστικές» δίοδοι (compulsory mandatory tunnels)

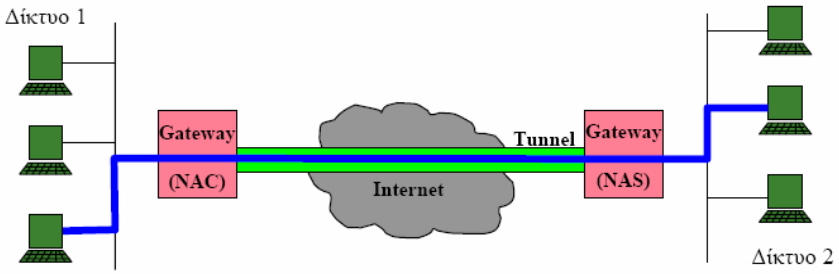
3. Με βάση το ποιοι είναι οι τελικοί χρήστες του VPN (δηλαδή ποια είναι τα δυο μέρη που συνομιλούν) Έτσι έχουμε:

- Τα VPN δομής «πελάτης-προς-δίκτυο» (client-to-LAN), όπου στην ουσία ένας απλός χρήστης συνδέεται με τον υπολογιστή του σε ένα τοπικό δίκτυο.



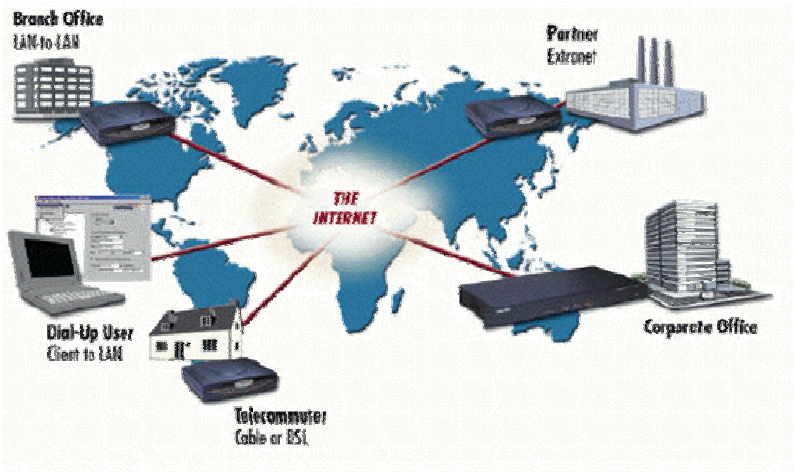
Εικόνα 5*: Σχηματική αναπαράσταση* client-to-LAN VPN

- Τα VPN δομής «δίκτυο -προς-δίκτυο» (LAN-to-LAN), όπου η δίοδος μεταφοράς των δεδομένων αναπτύσσεται μεταξύ δύο τοπικών δικτύων.



Εικόνα64*: Σχηματική αναπαράσταση* LAN-to-LAN VPN

Ένα Εικονικό Ιδιωτικό Δίκτυο περιγράφεται πλήρως αν αντιστοιχηθεί σε κάποιο είδος και για τις τρεις παραπάνω κατηγοριοποιήσεις. Για παράδειγμα, μπορούμε να αναφερθούμε σε ένα VPN ως εξής: χρησιμοποιεί το πρωτόκολλο L2TP, η δίοδος που αναπτύσσεται είναι αυθόρμητη και, τέλος, είναι απομακρυσμένης πρόσβασης.



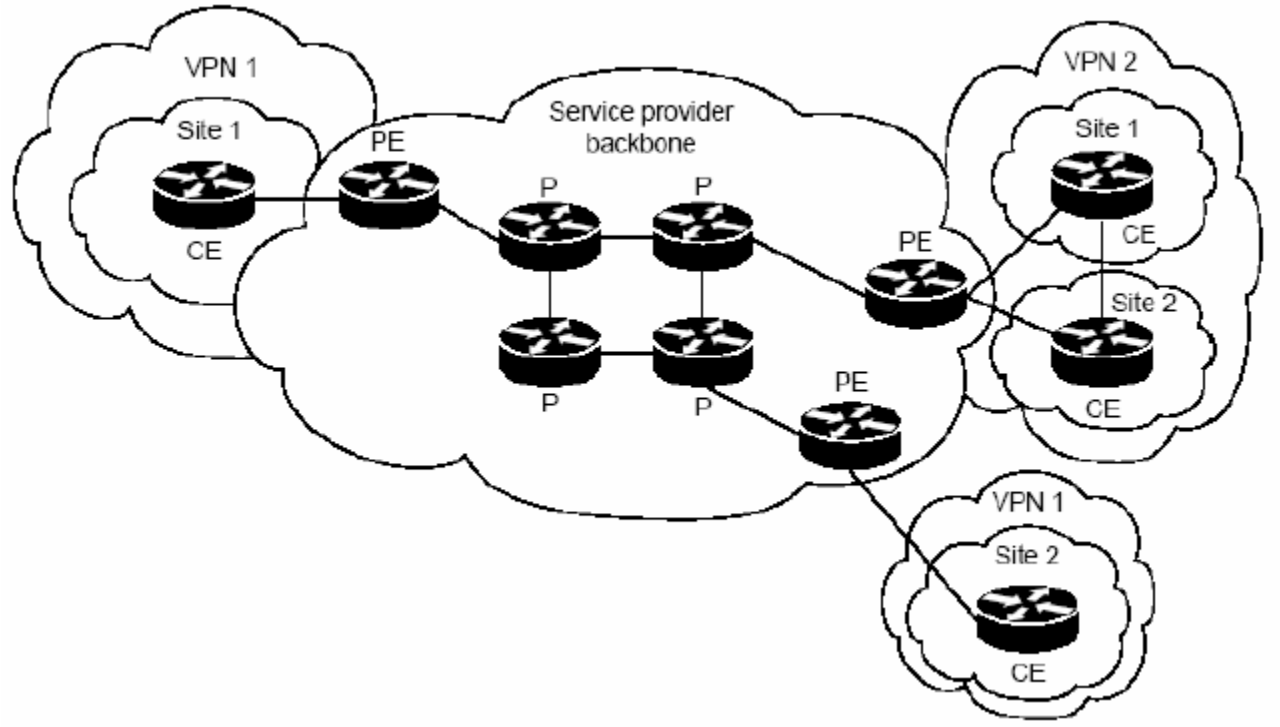
Εικόνα 7*: Η χρησιμότητα διαφορετικών* αρχιτεκτονικών *εφαρμογών* Εικονικών Ιδιωτικών Δικτύων σε μια επιχείρηση

3.1.1 ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ ΕΠΙΠΕΔΟΥ ΔΙΚΤΥΟΥ ΒΑΣΙΣΜΕΝΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ MPLS

Τα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου Δικτύου που βασίζονται στην τεχνολογία MPLS (Multiprotocol Label Switching) επιτρέπουν τη δημιουργία VPN κάνοντας χρήση του δικτύου κορμού MPLS του ISP. Τα VPN αυτά είναι σε επίπεδο IP και επομένως η μεταφορά της πληροφορίας γίνεται με τη χρήση αποκλειστικά του πρωτοκόλλου IP.

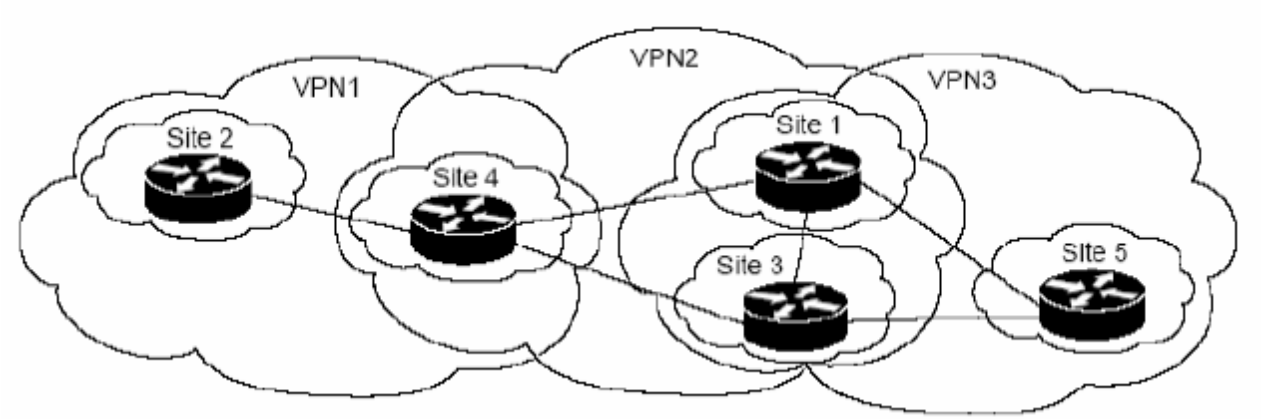
Τρία διαφορετικά είδη δρομολογητών συναντάμε στα MPLS VPNs:

- Δρομολογητές Customer Edge. Είναι οι δρομολογητές που τους διαχειρίζεται ο πελάτης και ανήκουν συνήθως σε αυτόν.
- Δρομολογητές Provider Edge . Είναι οι δρομολογητές που αποτελούν τα σημεία εισόδου και εξόδου των VPNs. Ανήκουν διαχειριστικά στον ISP.
- Δρομολογητές Provider. Είναι οι δρομολογητές που αποτελούν το δίκτυο κορμού του ISP και ανήκουν και αυτοί διαχειριστικά σε αυτόν. Ο κύριος σκοπός τους είναι η προώθηση των MPLS ετικετών προς τους Δρομολογητές Provider Edge.



Εικόνα 8*: Ένα παράδειγμα* MPLS VPN, όπου CE (Δρομολογητές Customer Edge), PE (Δρομολογητές Provider Edge), P (Δρομολογητές Provider)

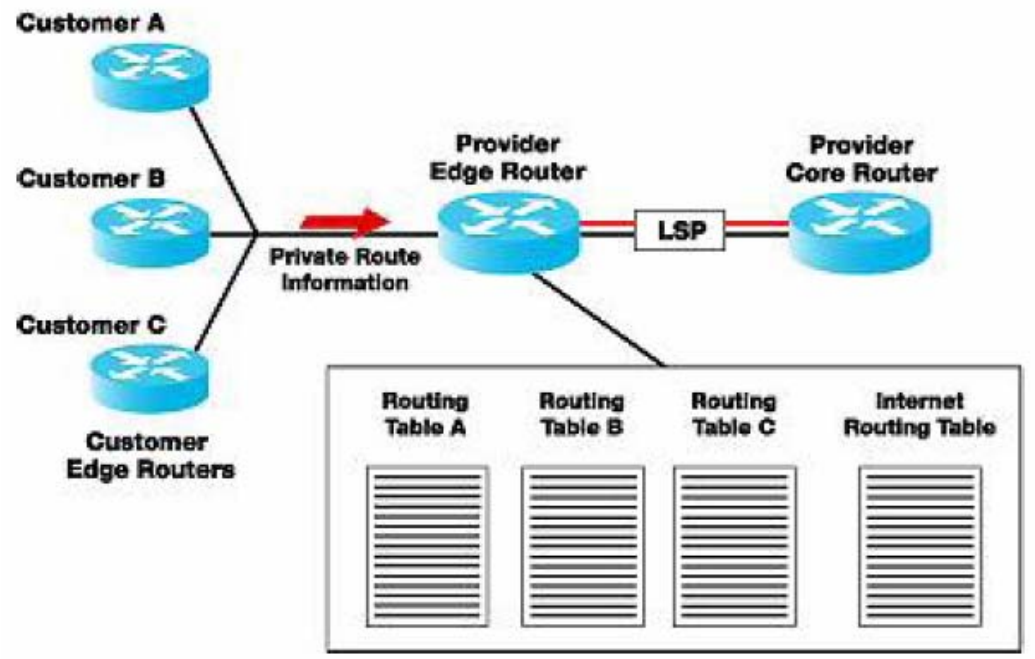
Όπως φαίνεται παραπάνω το δίκτυο του ISP αποτελείται από δρομολογητές τύπου Provider και Provider Edge. Στο δίκτυο κορμού του πάροχου συνδέονται τέσσερα sites, δύο από αυτά ανήκουν στο VPN και άλλα δύο sites ανήκουν στο VPN2 (όπου ένα site μπορεί να είναι ένα τοπικό δίκτυο Ethernet). Πρέπει να σημειωθεί πως δεν αποκλείεται ένα sites να ανήκει όχι μόνο σε ένα αλλά σε δύο VPN όπως φαίνεται και στο σχήμα που ακολουθεί:



***Εικόνα 9**: Ένα παράδειγμα* MPLS VPN όπου ένα site ανήκει σε περισσότερα από ένα VPN.

Οι Provider Edge δρομολογητές είναι αυτοί που διαμοιράζουν τις πληροφορίες δρομολόγησης των διαφόρων VPN και ενημερώνουν τους πίνακες δρομολόγησης που ανήκουν σε κάθε VPN. Η μεταφορά αυτής της πληροφορίας γίνεται με την χρήση του πρωτοκόλλου BGP (Borfer Gateway Protocol). Έτσι γίνεται δυνατή η επικοινωνία ανάμεσα στα «μέλη» ενός VPN. Επιπλέον είναι δυνατό, με πολιτική πρόσβασης BGP να επιτρέπεται ή να απαγορεύεται η πρόσβαση από/προς συγκεκριμένα «μέλη» ενός VPN. Παρέχεται έτσι μεγάλη ευελιξία αφού επιτρέπεται ή απαγορεύεται με διάφορους μηχανισμούς την ανταλλαγή μέρους ή όλου του πίνακα δρομολόγησης, ή επιλέγει μεταξύ διαφορετικών διαδρομών ποια θα είναι η κύρια και ποια η δευτερεύουσα.

Επίσης κάθε Provider Edge δρομολογητής μπορεί να συνδέεται με περισσότερους από ένα πελάτες. Έτσι σε κάθε Provider Edge δρομολογητή διατηρείται ένας «υποπίνακας» δρομολόγησης που περιέχει μόνο την πληροφορία που αφορά κάθε έναν συγκεκριμένο πελάτη, συμπεριφερόμενος σαν να είναι ένα σύνολο από εικονικούς δρομολογητές.



Εικόνα 10: *Πίνακας Δρομολόγησης* Provider Edge δρομολογητή

Κάθε πίνακας δρομολόγησης (routing table) αναφέρεται σε διαφορετικό πελάτη και αποτελεί έναν ανεξάρτητο εικονικό πίνακα δρομολόγησης που αποκαλείται VRF (Virtual Routing & Firewall Instance).

Η διεύρυνση ενός τέτοιου VPN είναι μια σχετικά απλή διαδικασία που χρειάζεται δυο βήματα για να επιτευχθεί.

1) να ενημερώσει τον Customer Edge δρομολογητή του νέου πελάτη για τον τρόπο σύνδεσης στο δίκτυο του παρόχου
2) να διαμορφώσει τον Provider Edge δρομολογητή έτσι ώστε να αναγνωρίζει την συμμετοχή του Customer Edge δρομολογητή του νέου πελάτη στο συγκεκριμένο VPN

3.1.2 ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ ΕΠΙΠΕΔΟΥ ΔΙΚΤΥΟΥ ΒΑΣΙΣΜΕΝΑ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ IPSec

Η ανάπτυξη του πρωτοκόλλου IPSec ξεκίνησε γιατί διαπιστώθηκε αδυναμία του TCP/IP στον τομέα της ασφάλειας, σε μια εποχή μάλιστα που η διάδοση των εμπορικών και εταιρικών εφαρμογών είχαν κατακλύσει το Internet και απαιτούσαν υψηλό βαθμό ασφάλειας. Είναι γνωστό ότι το πρωτόκολλο TCP/IP δεν παρέχει μηχανισμούς κρυπτογράφησης. Συνεπώς για την ασφαλή μετάδοση πάνω σε δίκτυο IP υπήρξε η ανάγκη νέου πρωτοκόλλου με μηχανισμούς κρυπτογράφησης, τα οποίο θα είναι εφαρμόσιμο σε IP δίκτυα. Το IPSec (IP Security) αποτελεί ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force (IETF) με στόχο την ασφαλή μετάδοση και ανταλλαγή δεδομένων μέσω του στρώματος IP. Το IPSec θεωρείται και είναι το πιο πλήρες πρωτόκολλο αφού τα άλλα (PPTP και L2TP) χρησιμοποιούν μέρη από το IPSec και σήμερα αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των δικτύων VPN.

Όσο αφορά τώρα τα θέματα ασφάλειας που ανακύπτουν με τη χρησιμοποίηση του Internet για τη πραγματοποίηση ιδιωτικών επικοινωνιών τα οποία το πρωτόκολλο IPSec αναπτύχθηκε για να αντιμετωπίσει είναι τα ακόλουθα.

- Απώλεια της Ιδιωτικότητας των Δεδομένων (Loss of Privacy). Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης που έχει καταφέρει να καταχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνηση τους στο Internet.
- Απώλεια Ακεραιότητας Δεδομένων (Loss of Data Integrity). Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης αλλάζει τα δεδομένα που μεταφέρονται στο δίκτυο (π.χ. τους αριθμούς ενός λογαριασμού καταθέσεων).
- Προσποίηση Ταυτότητας (Identity Spoofing): Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης παριστάνει ότι είναι ένας νόμιμος χρήστης του δικτύου και ζητά πληροφορίας που σε διαφορετική περίσταση δε θα μπορούσε να έχει.

- Άρνηση Υπηρεσιών (Denial-of-Service): Σ' αυτήν την περίπτωση γίνεται "επίθεση" σε κάποιον server του δικτύου. (π.χ. μαζική αποστολή e-mails)

Από την άλλη το πρωτόκολλο IPSec για την αντιμετώπιση αυτόν τον απειλών έχει παρέχει με μια σειρά από υπηρεσίες οι οποίες είναι:

- ✓ Ακεραιότητα τον δεδομένων (Integrity), που διασφαλίζει ότι τα πακέτα των δεδομένων κατά την διάρκεια της μεταφοράς τους δεν έχουν αλλοιωθεί ή παραποιηθεί, είτε από «εισβολείς» είτε από τυχόν σφάλματα επικοινωνίας
- ✓ Εξακρίβωση γνησιότητας της προέλευσης των δεδομένων (Authentication) ή πιστοποίηση ταυτότητας, που επαληθεύει ότι τα δεδομένα στάλθηκαν πράγματι από το χρήστη που ισχυρίζεται ότι τα έστειλε.
- ✓ Εμπιστευτικότητα (Confidentiality), που προσφέρει τη δυνατότητα αναγνώρισης και επεξεργασίας των δεδομένων μονό από εγκεκριμένους χρήστες.

Για να το πετύχει αυτό το πρωτόκολλο IPSec προσθέτει δύο κεφαλίδες. Την κεφαλίδα πιστοποίησης (IP Authentication Header - AH) για πιστοποίηση ταυτότητας και την κεφαλίδα ενθυλακωμένης ασφάλειας (Encapsulating Security Payload - ESP) για κρυπτογράφηση.

Αναλυτικότερα η κεφαλίδα πιστοποίησης (IP Authentication Header - AH) όταν προστίθεται σε ένα IP πακέτο, διασφαλίζει την ακεραιότητα, την πιστοποίηση ταυτότητας των δεδομένων, καθώς και την αποφυγή διπλότυπων πακέτων. Δεν παρέχει ασφάλεια εμπιστευτικότητας. Η ακεραιότητα και η πιστοποίηση πραγματοποιούνται και από τα δύο IPSec μέλη στις άκρες της διόδου (tunnel) εκτελώντας μία συνάρτηση κατακερματισμού στο IP πακέτο χρησιμοποιώντας ένα κοινό κλειδί (Message Authentication Code - MAC). Το αποτέλεσμα του υπολογισμού ο οποίος προκύπτει από τη συνάρτηση κατακερματισμού δεν κρυπτογραφείται και χρησιμοποιείται απλά από τον άλλο συμβαλλόμενο μέρος για να ελέγξει ότι τα στοιχεία δεν έχουν τροποποιηθεί. Το γεγονός αυτό καθ' αυτό της χρησιμοποίησης ενός κοινού μυστικού κλειδιού που είναι γνωστό και στα δύο μέρη (αποστολέας-δέκτης) εγγυάται την πιστοποίηση της ταυτότητας των συμβαλλομένων.

Η κεφαλίδα πιστοποίησης ταυτότητας αποτελείται από 5 πεδία

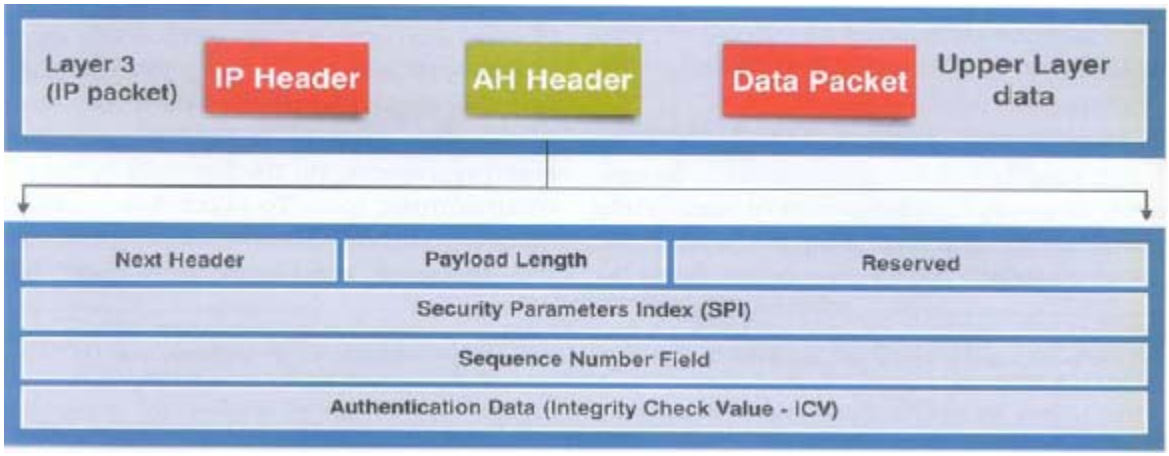
i. Πεδίο επόμενης κεφαλίδας (Next Header Field), όπου προσδιορίζει ποια είναι η επόμενη κεφαλίδα που είναι παρούσα στο IP πακέτο (π.χ. TCP, UDP, κ.ο.κ.)

ii. Μέγεθος του φορτίου (Payload Length)

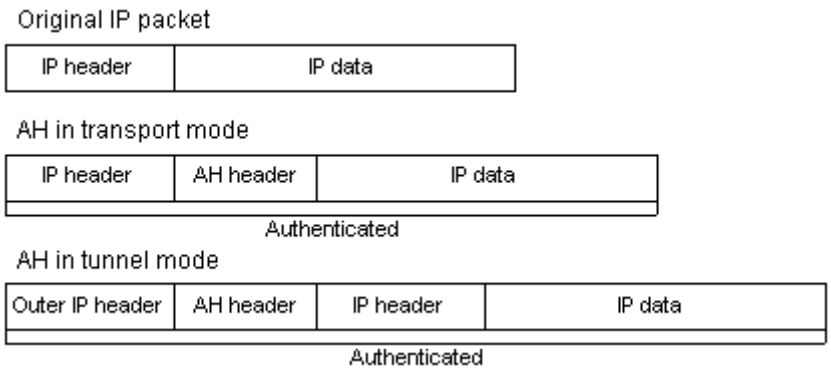
iii. Δείκτης παραμέτρων ασφαλείας (Security Parameter Index) προσδιορίζει στον παραλήπτη ποια πρωτόκολλα ασφαλείας χρησιμοποιήθηκαν από τον αποστολέα

iv. Ακολουθιακός αριθμός (Sequence Number): αυξάνεται κατά ένα για κάθε νέο πακέτο που καταφτάνει στον δέκτη από τον ίδιο αποστολέα και με το ίδιο δείκτη παραμέτρων ασφαλείας.

v. Δεδομένα Πιστοποίησης ταυτότητας (Authentication Data). Είναι το τμήμα εκείνο ου εξασφαλίζει την πιστοποίηση ταυτότητας. Όπως ήδη αναφέρθηκε, είναι το αποτέλεσμα μιας συνάρτησης κατακερματισμού (Integration Check Value).



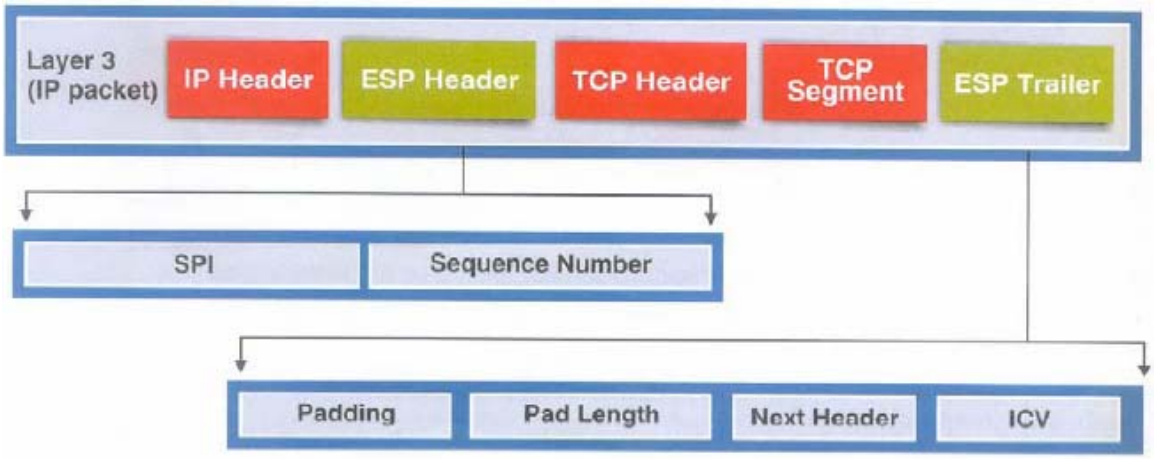
Εικόνα 11*: Τα* 5 *πεδία της κεφαλίδας πιστοποίησης* (IP Authentication Header - AH)



Εικόνα 12*: Η προσθήκη της κεφαλίδας πιστοποίησης* AH *σε* IP *πακέτο*

Η δεύτερη κεφαλίδα που προστίθεται είναι η κεφαλίδα ενθυλακωμένης ασφάλειας (Encapsulating Security Payload - ESP) για κρυπτογράφηση. Αυτή η κεφαλίδα παρέχει υπηρεσίες για την πιστοποίηση και ακεραιότητα των πακέτων IP που διαβιβάζονται μεταξύ δύο IPSec συστημάτων. Επιπρόσθετα παρέχει εμπιστευτικότητα μέσω μεθόδων κρυπτογράφησης. Η πιστοποίηση και η ακεραιότητα μπορούν να παρασχεθούν με τον ίδιο τρόπο που τα παρέχει και η κεφαλίδα AH. Το ESP παρέχει εμπιστευτικότητα με την κρυπτογράφηση ενός IP πακέτου. Το ESP υποστηρίζει ένα μεγάλο αριθμό συμμετρικών αλγορίθμων κρυπτογράφησης.

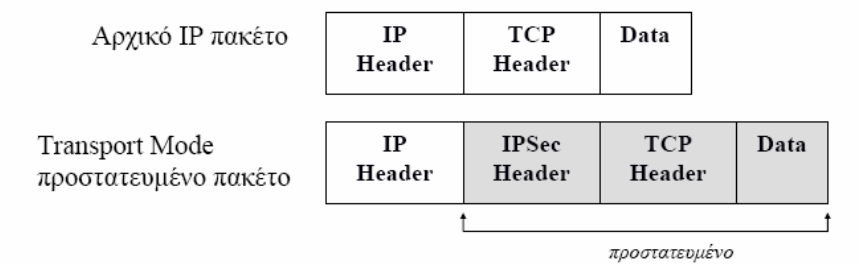
Τα πεδία της κεφαλίδας ESP είναι 6. Δύο από αυτά τοποθετούνται πριν το φορτίο του IP πακέτου (ESP Header) και τα υπόλοιπα τέσσερα μετά από αυτό (ESP Trailer). Τα πεδία SPI και Sequence Number του ESP Header έχουν την ίδια λειτουργία όπως στο AH. Το ίδιο ισχύει για τα πεδία Pad Length, Next Header και ICV του ESP Trailer. Το πεδίο Συμπλήρωσης (Padding) έχει μέγεθος το πολύ 255 bytes και χρειάζεται για να προσαρμόζεται το μέγεθος του IP πακέτου, ανάλογα με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται (αν αναλογιστούμε ότι κάποιοι αλγόριθμοι κρυπτογράφησης απαιτούν τα δεδομένα να είναι μήκους πολλαπλάσιου κάποιου συγκεκριμένου αριθμού bytes)



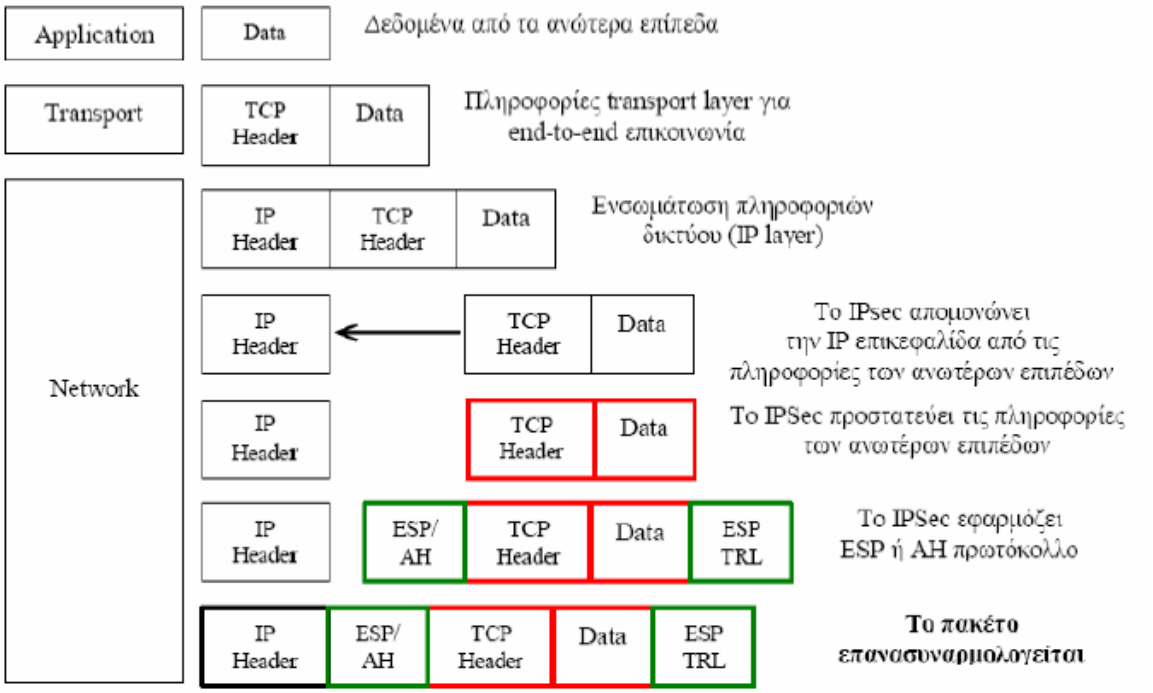
Εικόνα 12*: Τα* 6 πεδία της κεφαλίδας ενθυλακωμένης ασφάλειας (Encapsulating Security Payload - ESP)

Το IPSec έχει δυο τρόπους λειτουργίας (που σημαίνει δυο τρόπους με τους οποίους μπορούν να τοποθετηθούν οι κεφαλίδες AH και ESP).

Ο ένας είναι ο τρόπος μεταφοράς (transport mode).



Εικόνα 13: Ο τρόπος μεταφοράς (transport mode)

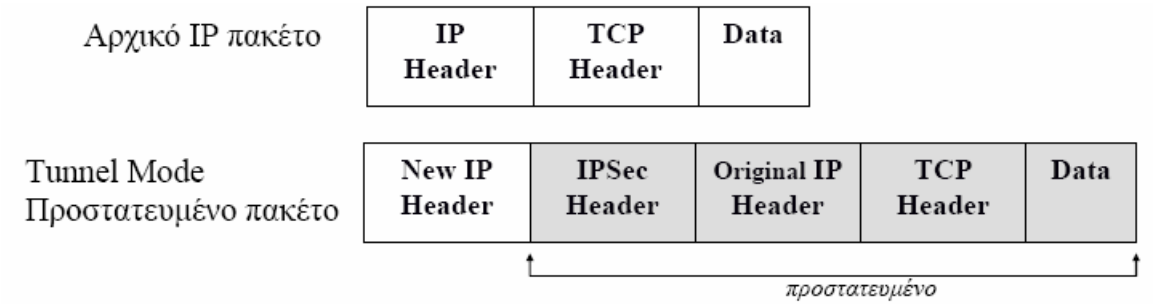


Εικόνα 14: IPSec σε κατάσταση μεταφοράς (transport mode)

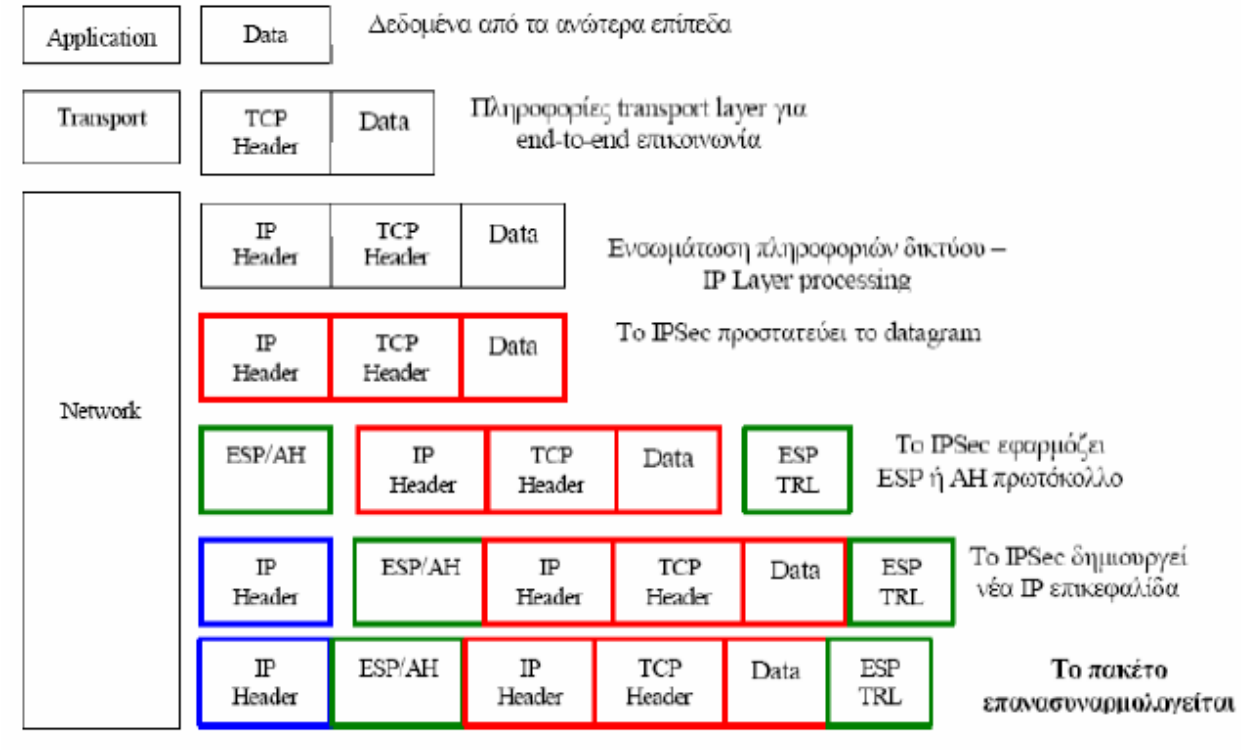
Κατά τον τρόπο μεταφοράς (transport mode) με ESP κρυπτογραφείται το αρχικό IP payload (όχι η κεφαλίδα). Με AH αυθεντικοποιείται το αρχικό IP payload καθώς και κάποια πεδία της IP κεφαλίδας. Χρησιμοποιείται για προστασία της επικοινωνίας από άκρο σε άκρο. Πλεονέκτημα του τρόπου είναι ότι σε κάθε πακέτο προστίθενται μόνο μερικά bytes (η νέα κεφαλίδα). Επίσης οι δρομολογητές βλέπουν τις διευθύνσεις πηγής και προορισμού και συνεπώς μπορούν να δρομολογήσουν κατά συγκεκριμένη QoS (Quality of

Service). Μειονέκτημα είναι ότι ανάλυση κίνησης μπορεί να γίνει από κακόβουλους.

Ο άλλος είναι ο τρόπος διόδου (tunnel mode).



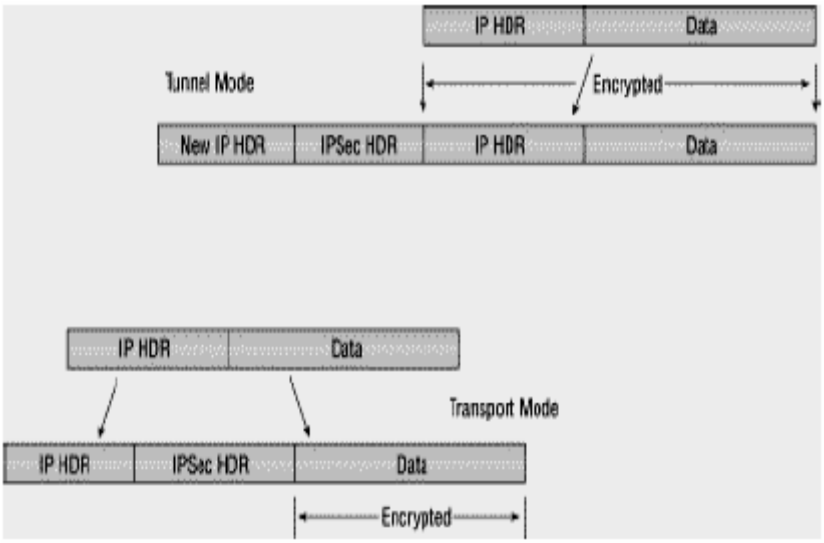
Εικόνα 15: Ο τρόπος διόδου (tunnel mode)



Εικόνα 16: IPSec σε κατάσταση διόδου (tunnel mode)

Κατά τον τρόπο διόδου (tunnel mode) το νέο IP πακέτο ταξιδεύει από τον έναν δρομολογητή στον άλλο χωρίς να μπορούν να διαβάσουν το αρχικό

πακέτο που βρίσκεται ενθυλακωμένο. Με ESP κρυπτογραφείται όλο το αρχικό IP πακέτο. Με AH αυθεντικοποιείται όλο το αρχικό IP πακέτο καθώς και κάποια πεδία της νέας IP κεφαλίδας. Επιτρέπεται στους δρομολογητές να λειτουργούν ως IPSec proxies, δηλαδή αυτό σημαίνει ότι το λειτουργικό του χρήστη δεν χρειάζεται τροποποίηση. Ακόμη προστατεύει από τον κίνδυνο ανάλυσης της κίνησης (αφού είναι κρυπτογραφημένα τα πάντα ακόμη και οι διευθύνσεις του αποστολέα και του παραλήπτη). Από την άλλη μεριά όμως απαιτείται επιπρόσθετη επεξεργασία στα πακέτα, από ότι στον τρόπο μεταφοράς (transport mode).



Εικόνα 17: Σύγκριση του τρόπου διόδου και του τρόπου μεταφοράς

Το IPSec περιλαμβάνει, εκτός από την επεξεργασία των πακέτων μέσω των κεφαλίδων AH και ESP, και πρωτόκολλα ανταλλαγής του κλειδιού. Μετά από εξέταση πολλών εναλλακτικών λύσεων για τη διαχείριση του κλειδιού, η IETF επέλεξε το IKE (Internet Key Exchange) σαν τον τρόπο ρύθμισης των συσχετίσεων ασφάλειας για το IPSec.

Το IKE δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι (tunnel) μετάξι δύο οντοτήτων και κατόπιν διαπραγματεύεται τις συσχετίσεις ασφάλειας για το IPSec. Αυτή η διαδικασία απαιτεί από τις δυο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν κλειδιά. Οι 5ύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσο μιας κατάλληλης διαδικασίας. Σε αυτή τη φάση υλοποιούνται συνήθως οι παρακάτω μηχανισμοί :

- Προ-Μοιρασμένα Κλειδιά. Το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας συνάρτησης κατακερματισμού) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.
- Κρυπτογράφηση Δημοσίων Κλειδιών-- Κάθε μηχανή παράγει έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το δημόσιο κλειδί (public key) της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια συνάρτηση κατακερματισμού του τυχαίου αριθμού, αποκρυπτογροφώντας με τα ιδιωτικά κλειδιά (private key) ό,τι λαμβάνουν από το συνομιλητή τους. Υποστηρίζεται μόνο η αλγόριθμος δημοσίων κλειδιών RSA.
- Ψηφιακές Υπογραφές Κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Ο αποστολέας χρησιμοποιεί το κρυφό του ιδιωτικό κλειδί για να υπογράψει ηλεκτρονικά τα δεδομένα του. Ο αποδέκτης του κειμένου χρησιμοποιεί το δημόσιο κλειδί του αποστολέα, το οποίο έτσι και αλλιώς γνωρίζει αφού είναι δημόσιο, για να ελέγξει την υπογραφή του αποστολέα. Αν αυτός ο έλεγχος είναι επιτυχής, αυτό σημαίνει ότι το κείμενο δεν έχει αλλαχθεί και έχει πιστοποιηθεί η ταυτότητα του αποστολέα. Υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

Μετά την πιστοποίηση της ταυτότητας του κάθε χρήστη, πρέπει να υπάρξει η ανταλλαγή του κλειδιού που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων που θα σταλούν μετέπειτα, κατά την επικοινωνία των δύο χρηστών. Ως βασικό αλγόριθμο ανταλλαγής κλειδιού το IKE. υποστηρίζει τον Diffie-Hellman (Μηχανισμός ανταλλαγής κλειδιών που αναπτύχθηκε από τους Diffie και Hellman το 1776. Επιτρέπει σε δύο χρήστες να ανταλλάσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές κανάλι. Είναι ένας κρυπτογραφικός αλγόριθμος δημοσίου κλειδιού), αν και μπορεί να υπάρξουν και άλλοι.

Ο ακριβής ρόλος του IKE για τη διεκπαιρέωση μίας IPSec επικοινωνίας μεταξύ δυο ή περισσότερων συσκευών αντικατοπτρίζεται στην ακόλουθη διαδοχή βημάτων που λαμβάνουν χώρα σε μία IPSec ανταλλαγή δεδομένων.

a) Ενεργοποίηση μιας IPSec συνόδου. Στο βήμα αυτό καθορίζεται το σύνολο

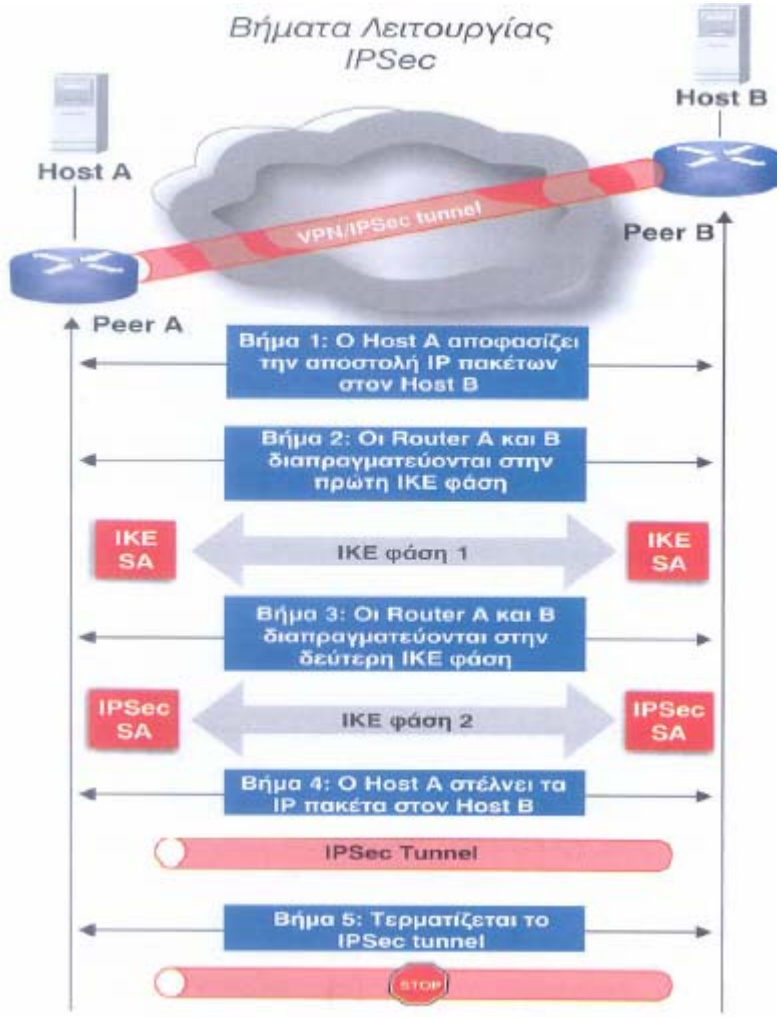
των IP πακέτων που πρόκειται να προστατευθούν μέσω του IPSec

b) IKE - Πρώτη φάση. Δημιουργία και λειτουργία της IKE Συσχέτισης Ασφαλείας,

c) IKE - Δεύτερη φάση. Δημιουργία και λειτουργία της AH/KKP Συσχέτισης Ασφαλείας

d) Μεταφορά Δεδομένων. Τα IP πακέτα που επιλέχθηκαν από το πρώτο βήμα μεταφέρονται.

e) Τερματισμός της IPSec συνόδου. Εφόσον ολοκληρωθεί η μεταφορά των IP πακέτων και δεν χρησιμοποιείται η παραπάνω σύνοδος, η τελευταία τερματίζεται.



Εικόνα 18*:* Βήματα λειτουργίας IPSec πρωτοκόλλου για ανταλλαγή δεδομένων

Τα δυο βασικά προβλήματα που καλείται να αντιμετωπίσει το IPSec είναι η αύξηση του μεγέθους των πακέτων (που σημαίνει μεγαλύτερος χρόνος επεξεργασίας τους) και η αδυναμία ή και αποτυχία καθορισμού καθολικών αλγορίθμων κρυπτογράφησης.

3.2.1 ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ ΕΠΙΠΕΔΟΥ ΖΕΥΞΗΣ ΔΕΔΟΜΕΝΩΝ ΒΑΣΙΣΜΕΝΑ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ PPTP

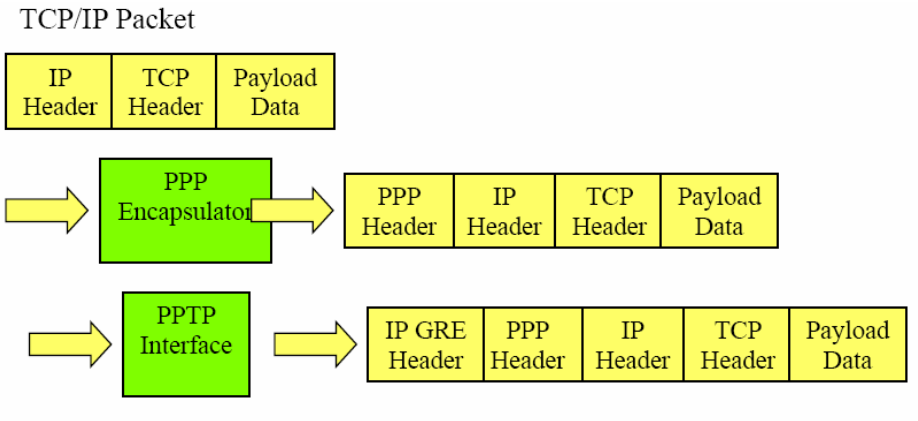
Το PPTP είναι ένας συνδυασμός του PPP (Point-to-Point Protocol) TCP/IP (Transmission Control Protocol / Internet Protocol). Δημιουργήθηκε από μια ομάδα εταιριών ανάμεσα στις οποίες οι 3Com, US Robotics, Microsoft, Ascend Communications παράλληλα με το L2F της Cisco. Το PPTP συνδυάζει τα χαρακτηριστικά του PPP (π.χ. εμπιστευτικότητα με ταυτόχρονη συμπίεση των πακέτων δεδομένων) και του TCP/IP (κυρίως τη δυνατότητα για δρομολόγηση των πακέτων στο Internet). Το PPTP μπορεί να πάρει πακέτα όπως IP, IPX, NetBios, SNA και να τα μετατρέψει σε ένα καινούριο IP πακέτο για μεταφορά. Για την πιστοποίηση της ταυτότητας του χρήστη χρησιμοποιεί τους μηχανισμούς PAP ή CHAP που παρέχονται από το PPP. Χρησιμοποιεί το Generic Routing Encapsulating Protocol (GRE) για μεταφορά των PPP πακέτων. Πραγματοποιεί επίσης κρυπτογράφηση για τα ενθυλακωμένα δεδομένα.

Δυο ειδών πακέτα χρησιμοποιούνται στο PPTP: πακέτα δεδομένων (data packets) και πακέτα ελέγχου (control packets). Τα πακέτα ελέγχου χρησιμοποιούνται για σηματοδοσία ενώ τα πακέτα δεδομένων για να μεταφέρουν τα δεδομένα του χρήστη. Τα πακέτα δεδομένων έχουν υποστεί πρώτα την διαδικασία της ενθυλάκωσης σύμφωνα με το Generic Routing Encapsulating Protocol .

Το PPTP αρχικά, χρησιμοποιεί αυτούσιο το PPP, από το οποίο εξασφαλίζει τα ακόλουθα:

- Εγκαθίδρυση της φυσικής ζεύξης
- Πιστοποίηση των χρηστών
- Δημιουργία PPP πλαισίων

Στη συνέχεια, τα PPP πλαίσια ενθυλακώνονται κατάλληλα σε μεγαλύτερα πακέτα με στόχο τη μετάδοση δεδομένων μέσω μιας διόδου. Στην ουσία δημιουργούνται IP πακέτα, με χρήση του πρωτοκόλλου ενθυλάκωσης GRE.

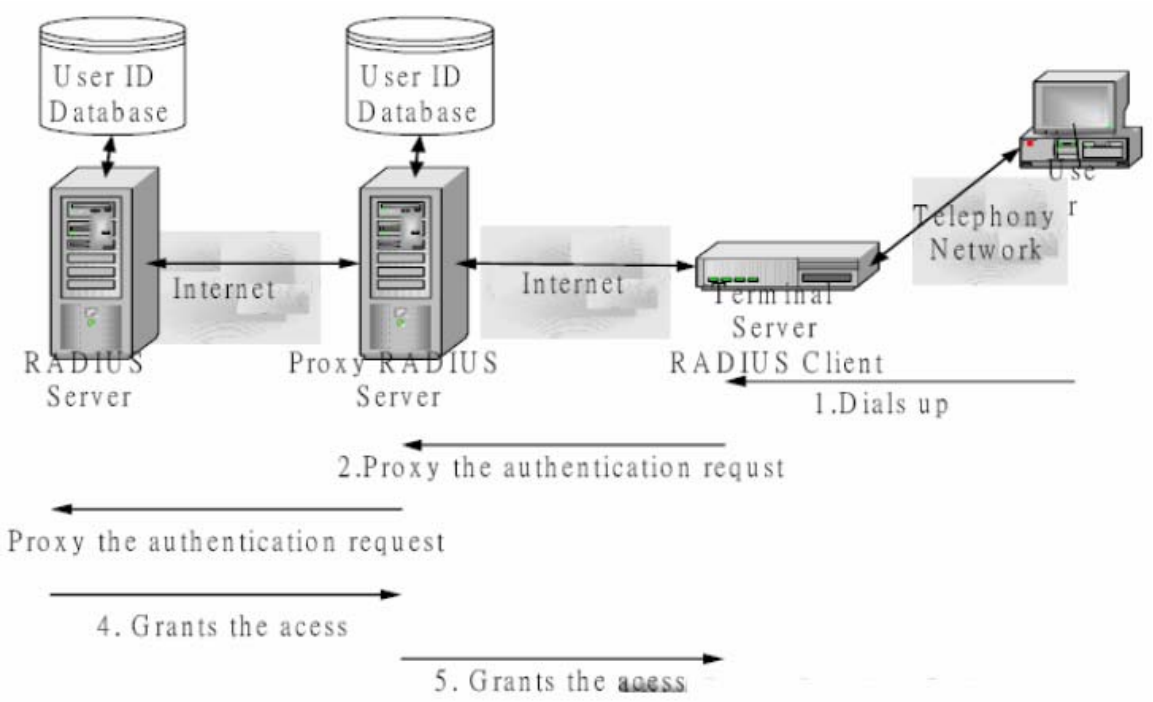


Εικόνα 19*: Ενθυλάκωση πακέτων στο PPTP*

Οι συσκευές στον ISP που είναι υπεύθυνες για λειτουργίες του πρωτοκόλλου PPTP ονομάζονται Remote Access Servers (RAS) ή Network Access Servers (NAS). Πρακτικά, ένας NAS ή RAS δεν είναι τίποτα άλλο παρά συλλογή modems με κατάλληλο λογισμικό. Μία από τις βασικές λειτουργίες του NAS είναι η πιστοποίηση ταυτότητας του χρήστη, δηλαδή ο έλεγχος του κατά πόσον ο χρήστης είναι εξουσιοδοτημένος στο να συνδεθεί στο δίκτυο. Αυτός ο έλεγχος ταυτότητας γίνεται μετά την αρχική αίτηση σύνδεσης στον ISP, κατά την οποία η ταυτότητα του χρήστη επικυρώθηκε με μηχανισμούς password που παρέχει το PPP (PAP ή CHAP). Με άλλα λόγια, η πιστοποίηση ταυτότητας του χρήστη που πραγματοποιεί ο NAS είναι η δεύτερη που λαμβάνει χώρα - έχει προηγηθεί είτε PAP είτε CHAP αυθενπκοποίηση. Ο RAS αυθεντικοποιεί τον χρήστη κυρίως με το πρωτόκολλο RADIUS.

Το πρωτόκολλο RADIUS έχει τη δομή μοντέλου client-server. Ο NAS δέχεται τις αιτήσεις των χρηστών, παίρνει ID και passwords από αυτούς, και τα προωθεί στον RADIUS server. Ο RADIUS server ενημερώνει για το αν εγκρίνει την πρόσβαση ή όχι, μια που διατηρεί μία κεντρική βάση δεδόμενων των χρηστών, τόσο με τα στοιχεία τους όσο και με τις αντίστοιχες υπηρεσίες που μπορεί να παρέχει σε καθέναν από αυτούς. Γενικότερα, ο RADIUS server διατηρεί στη βάση του διάφορα στοιχεία, όπως τη διεύθυνση του NAS (για πληροφορίες στατιστικής φύσεως της χρήσης της ζεύξης) καθώς και πληροφορίες χρέωσης των χρηστών (αν κάτι τέτοιο είναι πολιτική του παρόχου του δικτύου).

Συχνά υπάρχουν και RADIUS proxy server, οι οποίοι είναι εγκατεστημένοι στους ISPs και ενημερώνονται ανά περιοδικά διαστήματα από τον κεντρικό RADIUS server. Διατηρούν δηλαδή οι ίδιοι ένα αντίγραφο της βάσης δεδομένων, με βάση την οποία αυθεντικοποιουν το χρήστη

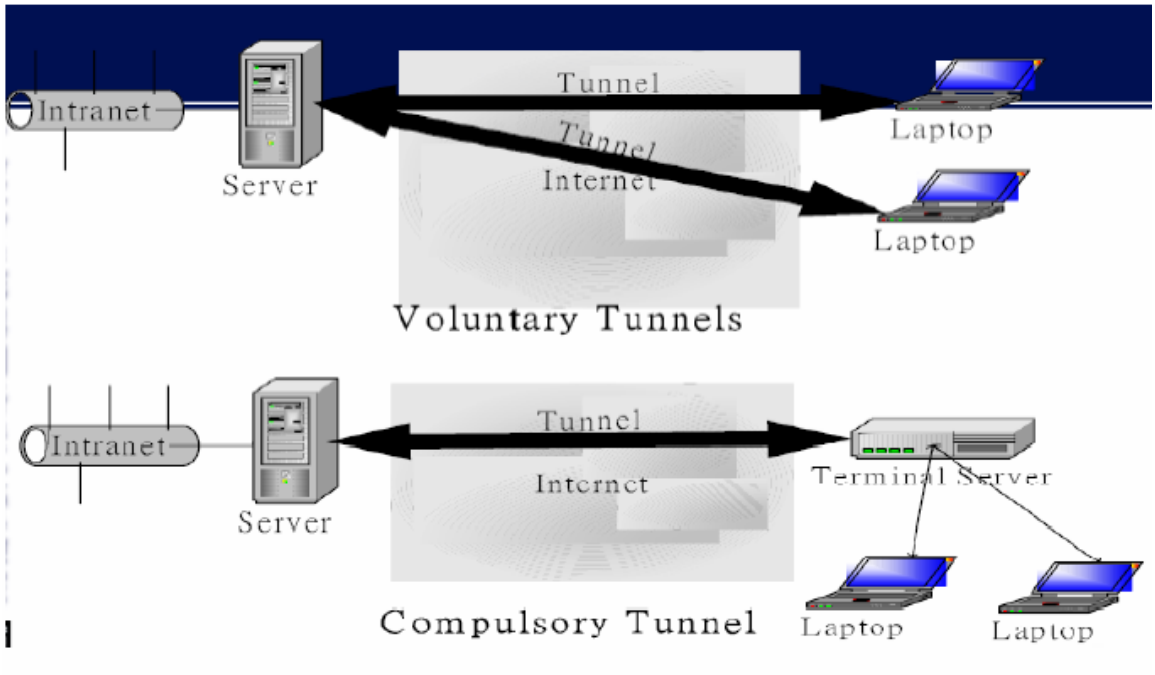


Εικόνα 20*: Λειτουργία του RADIUS με τον Proxy server*

Στο PPTP, οι ζεύξεις επικοινωνίας υλοποιούνται πάνω σε διόδους. Οι δυνατότητες του υπολογιστή του χρήστη καθορίζουν το άκρο της διόδου: αν ο υπολογιστής έχει PPTP software, τότε αυτός είναι το άκρο της διόδου. Διαφορετικά, αν υποστηρίζει μόνο PPP και όχι PPTP, τότε το άκρο της διόδου βρίσκεται στον ISP και συγκεκριμένα στον RAS.

Στο PPTP όπως είπαμε οι ζεύξεις γίνονται πάνω σε διόδους. Υπάρχουν τώρα δύο ειδών δίοδοι: οι «αυθόρμητες» δίοδοι (voluntary tunnels) και οι «αναγκαστικές» (compulsory ή mandatory tunnels). Οι πρώτες δημιουργούνται μετά από αίτηση του χρήστη, ενώ οι αναγκαστικές δίοδοι δημιουργούνται αυτόματα, χωρίς καμία παρεμβολή από τον χρήστη.

Μία αναγκαστική δίοδος έχει προκαθορισμένα ακραία σημεία (που είναι στην ουσία κάποιοι RAS), άρα ο έλεγχος πρόσβασης των χρηστών είναι πιο εύκολος. Δίνει επίσης τη δυνατότητα, αν η πολιτική της εταιρίας είναι τέτοια, οι εργαζόμενοι να μην έχουν πρόσβαση στο Internet, αλλά να χρησιμοποιούν τις Internet ζεύξεις αποκλειστικά και μόνο για το VPN. Επίσης στις αναγκαστικές διόδους πάνω σε μια δίοδο μπορούν να υπάρχουν πολλαπλές συνδέσεις. Ένα μειονέκτημα των αναγκαστικών διόδων είναι το γεγονός ότι η σύνδεση του υπολογιστή του χρήστη με τον RAS πραγματοποιείται έξω από τη δίοδο και, συνεπώς, είναι μη ασφαλής. Γενικά, οι αυθόρμητες δίοδοι προσφέρουν μεγαλύτερη ασφάλεια.



Εικόνα 21*: Σχηματική αναπαράσταση των δύο ειδών διόδων* «αυθόρμητες» δίοδοι (voluntary tunnels) και οι «αναγκαστικές» (compulsory ή mandatory tunnels)

Με τη σειρά τους οι αναγκαστικές δίοδοι χωρίζονται σε δύο υποκατηγορίες:

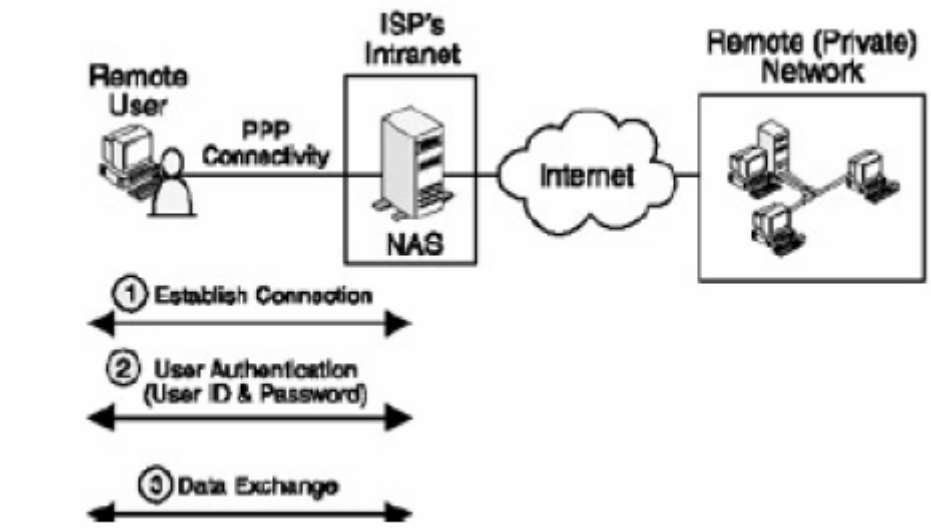
I. Στατικές αναγκαστικές δίοδοι (static compulsory tunnels).
   - Realm Based. ο RAS ελέγχει ένα τμήμα του ονόματος του χρήστη, τον τομέα (realm) και με βάση αυτό αποφασίζει τη δρομολόγηση της διόδου αυτού του χρήστη. Σε αυτές τις διόδους, όλοι οι χρήστες του ίδιου τομέα (π.χ. του ίδιου γραφείου) αντιμετωπίζονται με τον ίδιο τρόπο, δηλαδή, οι δίοδοι που δημιουργούνται προσφέρουν σε όλους την ίδια ποιότητα υπηρεσίας. Αυτό μειώνει την «ευλυγισία» του συστήματος.
   - Automatic. Υπάρχει προ-εγκατεστημένος εξοπλισμός. Ο χρήστης καλεί ένα συγκεκριμένο τηλεφωνικό αριθμό για να έχει πρόσβαση στο VPN (να ξεκινήσει μία δίοδος).

Γενικότερα, οι στατικές δίοδοι δεν προσφέρονται σε συστήματα όπου υπάρχει μεγάλο πλήθος χρηστών που αιτούνται πρόσβαση

II. Δυναμικές αναγκαστικές δίοδοι (dynamic compulsory tunnels):
   - Με βάση την αίτηση κάθε χρήστη, γίνεται σύνδεσή του με τον RAS. Χρειάζεται ένας RADIUS server για την εξουσιοδότηση του χρήστη.

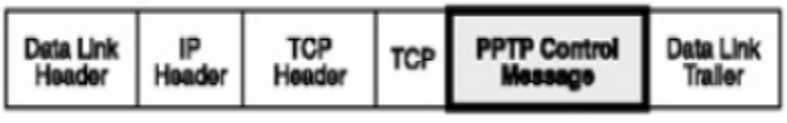
Η όλη λειτουργία του PPTP πραγματοποιείται σε τρεις φάσεις:

1. Πρώτη φάση: Το πρωτόκολλο χρησιμοποιεί το γνωστό πρωτόκολλο PPP για τη σύνδεση του χρήστη με τον ISP.



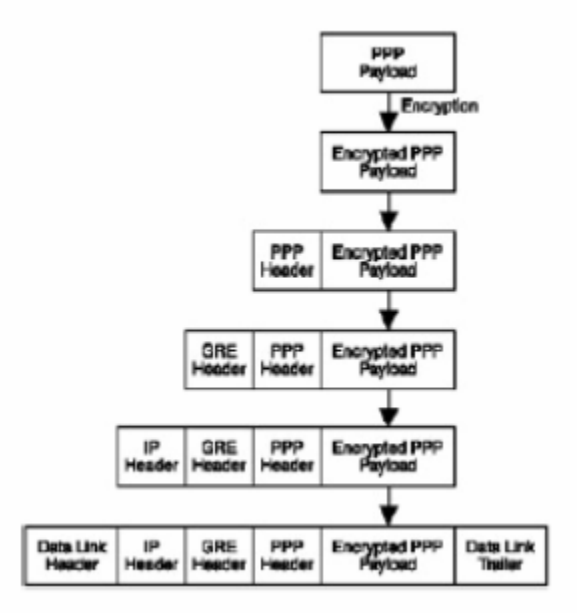
***Εικόνα 22**:Η πρώτη φάση του PPTP (χρήση του PPP, το οποίο λειτουργεί σε 3 στάδια)*

2. Δεύτερη φάση: Ανταλλάσσονται μηνύματα ελέγχου μεταξύ PPTP client και PPTP server (RAS) για τη διατήρηση αλλά και τον τερματισμό της διόδου. Τα μηνύματα αυτά ανταλλάσσονται με βάση τις IP διευθύνσεις τους.στην 1723 θύρα του RAS. Τα PPTP μηνύματα ελέγχου ενθυλακώνονται σε TCP/IP πακέτα.

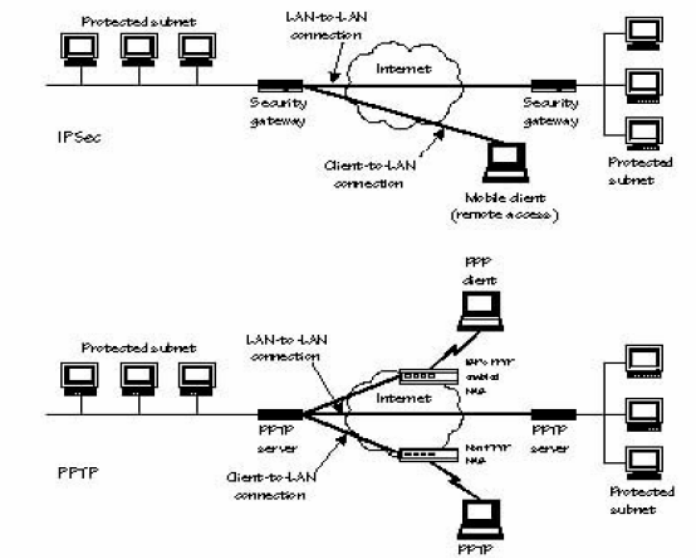


***Εικόνα 23**: `Η δεύτερη φάση του PPTP (*λογική εγκαθίδρυση του PPTP*)*

3. Τρίτη φάση: Τα πακέτα δεδομένων μεταφέρονται μέσω της διόδου που έχει υλοποιηθεί από την προηγούμενη (δεύτερη) φάση. Τα πακέτα είναι κρυπτογραφημένα. Ο βασικός αλγόριθμος κρυπτογράφησης που έχει χρησιμοποιηθεί για την υλοποίηση του PPTP πρωτοκόλλου είναι ο RC4. Το κλειδί κρυπτογράφησης προκύπτει από εφαρμογή μιας συνάρτησης κατακερματισμού στο password του. Η κρυπτογράφηση ξεκινά από τον υπολογιστή του χρήστη, κάτι που προσδίδει μεγαλύτερη ασφάλεια.



Εικόνα 24*: Η τρίτη φάση του PPTP (PPTP tunneling – μεταφορά δεδομένων)*



Εικόνα 25*: Σύγκριση δικτύων IPSec και PPTP*

Στα μειονεκτήματα του PPTP συγκαταλέγεται το γεγονός ότι οι PPTP servers δέχονται δεδομένα μόνη στην 1723 TCP θύρα, κάτι που αποτελεί σημαντική πληροφορία για κάποιον που θέλει να υποκλέψει την επικοινωνία. Επίσης, GRE πακέτα (που ενυπάρχουν στα PPTP πακέτα) δεν μπορούν να περάσουν από όλους τους τοίχους ασφαλείας (firewalls). Τέλος, τα VPNs που στηρίζονται στο PPTP εξαρτώνται από τα πρωτόκολλα που διαθέτει και μπορεί να υποστηρίξει ο ISP (σε αντίθεση με το IPSec).

ΣΥΓΚΡΙΣΗ ΠΡΩΤΟΚΟΛΛΩΝ

ΠΡΩΤΟΚΟΛΛΟ	ΘΕΤΙΚΑ	ΑΡΝΗΤΙΚΑ	ΘΕΣΗ ΣΤΟ ΔΙΚΤΥΟ
IPSec	• Παρέχει μεγάλη ασφάλεια	• Δύσκολο τη διαχείριση	• Ιδανικό για το domain network
	• Είναι μέρος του σχεδιασμού του Ipv6	• Όχι ευρέως χρησιμοποιούμενο	• Ιδανικό για τον client
	• Δουλεύει ανεξάρτητα από τις εφαρμογές	• Μικρή υποστήριξη στον client	• Ιδανικό για LAN to LAN με NT
PPTP	• Λειτουργεί με WIN NT,WIN.x	• Δεν μεγάλη ασφάλεια	
	• Προσφέρει end-to-end και node-to-node tunneling	• Δεν παρέχει ασφάλεια από remote access servers	• Ιδανικό για remote access servers
	• Ευρέως χρησιμοποιούμενο		
	• Παρέχει ασφάλεια μέσω των NT και RSA encryption		• Χρήση της πλατφόρμας των Win.x
	• Ανοιχτό σε άλλα πρωτόκολλα		
L2F	• Ανοιχτό σε άλλα πρωτόκολλα	• Δεν παρέχει encryption	• Ιδανικό για remote
	• Ευρέως χρησιμοποιούμενο	• Δεν παρέχει authentication	access σε POP
L2TP	• Συνδυάζει PPTP και L2F • Ανοιχτό σε άλλα πρωτόκολλα • Χρησιμοποιεί IPSec encryption	Μικρή διάδοση	• Ιδανικό για remote access σε POP

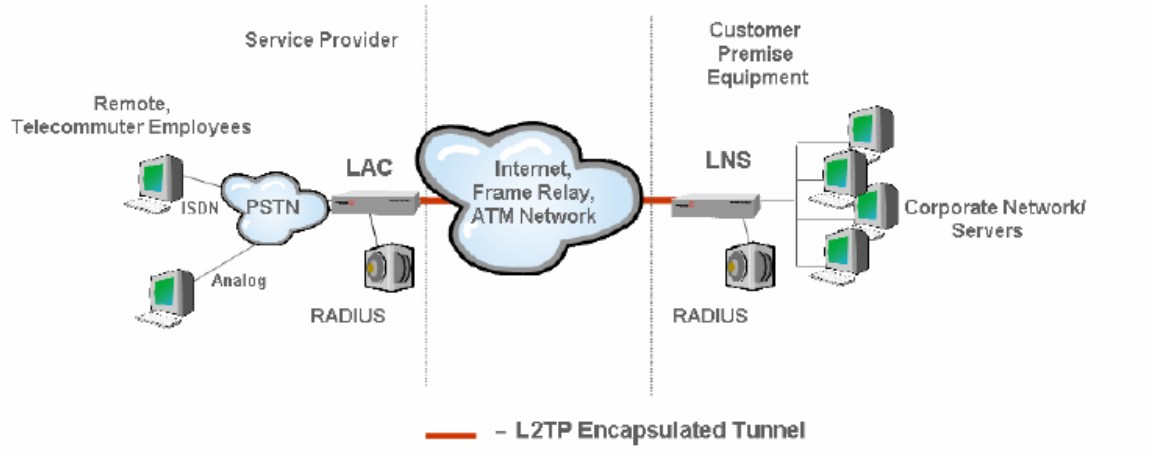
Πίνακας 1*. Σύγκριση πρωτοκόλλων των επιπέδων δικτύου και ζεύξης δεδομένων*

3.2.2 ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ ΕΠΙΠΕΔΟΥ ΖΕΥΞΗΣ ΔΕΔΟΜΕΝΩΝ ΒΑΣΙΣΜΕΝΑ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ L2TP

Το πρωτόκολλο L2TP είναι αποτέλεσμα συγχώνευσης του PPTP και του L2F. Ορίστηκε για λόγους συμβατότητας όλων των δικτύων μεταξύ τους. Το L2TP παρέχει συμπίεση βασισμένη σε λογισμικό. Ένας μικρός αριθμός τεχνικών συμπίεσης έχει προστεθεί στο επίπεδο της κρυπτογράφησης. Επειδή το L2TP χρησιμοποιεί πολλά χαρακτηριστικά του IPSec για να επιτύχει μεγαλύτερη ασφάλεια, θεωρείται ότι παρέχει υπηρεσίες όχι μόνο δεύτερου αλλά και τρίτου επιπέδου Το I.2TP χρησιμοποιεί δύο servers για τη σύνοδο.

i. τον LAC (L2TP Access Concentrator). Βρίσκεται στον ISP και χρησιμοποιείται για την εγκαθίδρυση μίας διόδου σε ένα δημόσιο δίκτυο η οποία τερματίζεται στον LNS του κόμβου προορισμού
ii. τον LNS (L2TP Network Server). Βρίσκεται στον προορισμό και χρησιμοποιείται για τον τερματισμό του tunnel. Αναλαμβάνει την αυθεντικοποίηση του χρήστη. Όταν ο LNS λάβει αίτηση για σύνδεση (δημιουργία διόδου) από έναν LAC αυθεντικοποιεί τον αιτούντα και εγκαθιδρύει το tunnel.

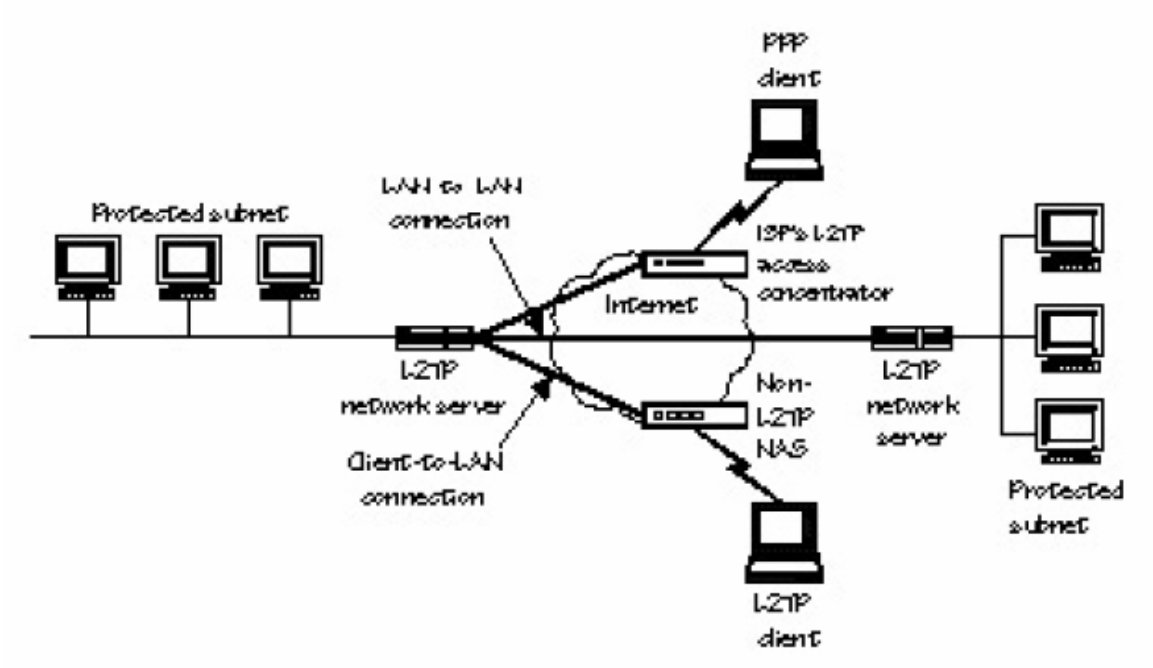
Όπως και στο PPTP, η αρχική σύνδεση του χρήστη με τον LAC (ο οποίος παίζει το ρόλο που έχει ο NAS στο PPTP γίνεται με χρήση του PPP, μέσω του οποίου ενθυλακώνονται διαφόρων ειδών πακέτα (Apple Tallk, IP, IPX και NETBEUI) και πραγματοποιείται μία πρώτη αυθεντικοποίηπη του χρήστη (με PAP ή CHAP). Μία δεύτερη πιστοποίηση της ταυτότητας του χρήστη λαμβάνει χώρα αμέσως μετά, με χρήση του RADIUS. Επίσης, μία άλλη αναλογία του L2TP μβ το PPTP είναι τα δύο είδη μηνυμάτων που μπορεί να ανταλλάσσονται: μηνύματα ελέγχου και μηνύματα δεδομένων. Τέλος, όπως και στο PPTP, ένα VPN που υλοποιείται με βάση το L2TP μπορεί να υποστηρίζει τόσο αυθόρμητες (voluntary) όσο και αναγκαστικές (compulsory) διόδους.



Εικόνα 26*: Σχηματική αναπαράσταση ενός VPN tunnel, βασισμένο σε L2TP*

Τα στάδια που ακολουθούνται για την δημιουργία μιας L2TP διόδου είναι τρία.

- Στάδιο 1: Ο απομακρυσμένος χρήστης συνδέεται με τον L2TP Access Concentrator (LAC) του ISP με χρήση του πρωτοκόλλου PPP. Ο LAC αυθεντικοποιεί τον χρήστη, με βάση το user name και password του. Στη συνεχεία, ο LAC προσδιορίζει την IP διεύθυνση του L2TP Network Server (LNS) που ανήκει στο LAN για το οποίο ο χρήστης αιτείται σύνδεση. Η σύνοδος L2TP ξεκινά μεταξύ LAC και LNS.
- Στάδιο 2: Μετά την εκκίνηση της L2TP συνόδου, ξεκινά η αυθεντικοποίηση του χρήστη στον LNS. Μπορεί να χρησιμοποιηθεί οποιοσδήποτε τυποποιημένος αλγόριθμος αυθεντικοποίησης (π.χ. CHAP). Όπως στα πρωτόκολλα PPTP και L2F, το L2TP δε θέτει περιορισμό για αλγόριθμο αυθεντικοποίησης. Ωστόσο, στην πράξη, έχει προτιμηθεί κυρίως η αυθεντικοποίηση με χρήση του RADIUS.
- Στάδιο 3: Μετά από επιτυχή αυθεντικοποίηση, μπορεί να δημιουργηθεί μια προστατευμένη δίοδος (tunnel) μεταξύ LAC και LNS. Το L2TP δεν προσδιορίζει ρητά μεθόδους για την κρυπτογράφηση (η οποία και παρέχει την ασφάλεια). Ωστόσο, για διόδους πάνω σε IP δίκτυα, μπορεί να χρησιμοποιηθεί το πρωτόκολλο IPSec. Τότε το L2TP ενθυλακώνεται σε UDP πακέτα που μεταφέρονται μεταξύ LAC και LNS μέσω IPSec tunnel. Για αυτό χρησιμοποιείται ως βασική η UDP πόρτα 1701 ωστόσο, μπορεί να χρησιμοποιηθεί εν γένει οποιαδήποτε άλλη UDP πόρτα.



Εικόνα 27*: Δομικά στοιχεία του L2TP*

Συγκρίνοντας το L2TP με το PPTP, το πρώτο λειτουργεί γενικά καλύτερα σε περιπτώσεις όπου τα πακέτα περνάνε από «τοίχους ασφαλείας», μια που δεν υπάρχει GRE ενθυλάκωση η οποία είναι αυτή που δημιουργεί το αντίστοιχο πρόβλημα στο PPTP. Επίσης, παρέχει μεγαλύτερη ασφάλεια ως προς την ανάλυση κίνησης (traffic analysis), λόγω του ότι η επικοινωνία δεν γίνεται μόνο μέσω μιας συγκεκριμένης UDP θύρας στον LNS (αν και υπάρχει μια προκαθορισμένη θύρα ως βασική, η 1701) οι διαχειριστές δικτύου μπορούν να αλλάζουν αυτήν τη θύρα, δυσκολεύοντας έτσι το έργο ενός επιτιθέμενου.

3.3 ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ ΕΠΙΠΕΔΟΥ ΜΕΤΑΦΟΡΑΣ ΒΑΣΙΣΜΕΝΑ ΣΤΟ ΠΡΩΤΟΚΟΛΛΟ SSL

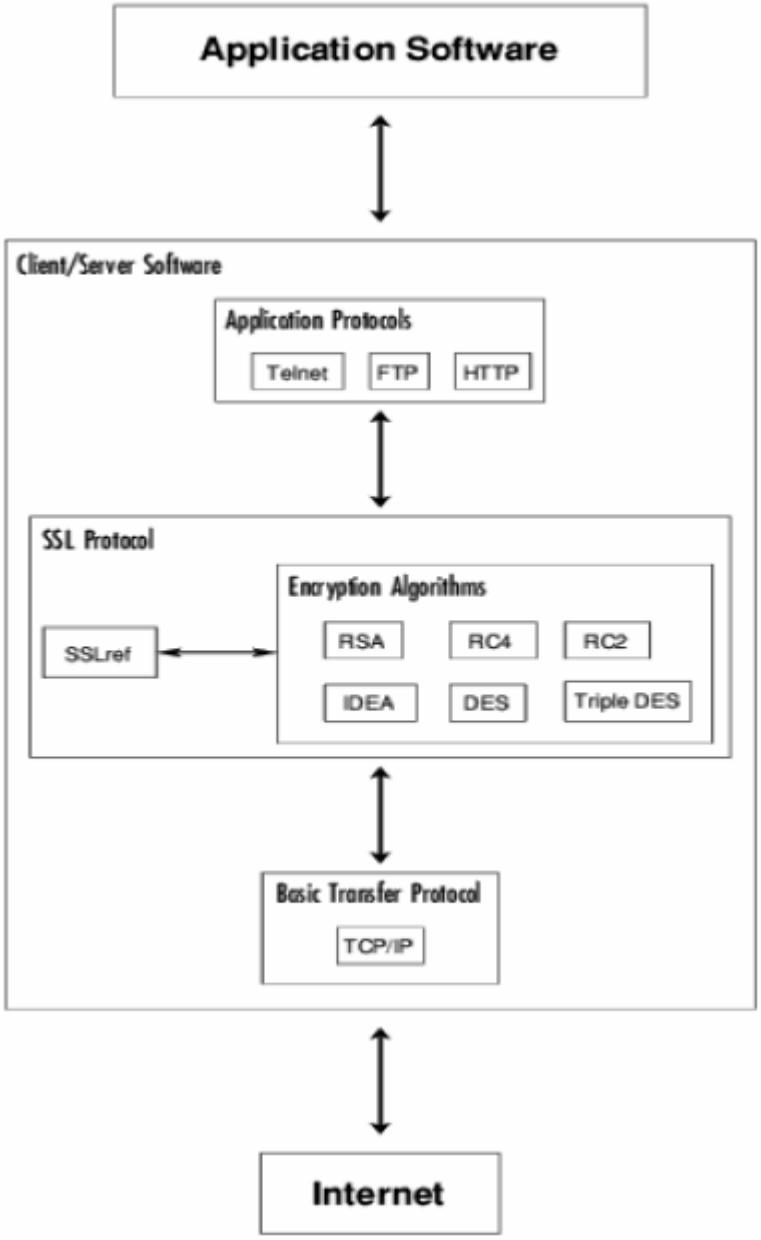
Το πρωτόκολλο SSL (Secure Socket Layer) αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών (π.χ. αριθμούς πιστωτικών καρτών). Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0). Τον Δεκέμβριο του 1994 εκδίδεται μια αναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0). Αναβαθμίστηκε σε SSL ν.3.0 με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία. Αυτή η νέα έκδοση του πρωτοκόλλου SSL τέθηκε επισήμως σε κυκλοφορία το Δεκέμβριο του 1995. Μετεξελίχτηκε στο TLS (Transport Layer Security). Βασικό του χαρακτηριστικό ότι παρέχει TCP/IP ασφάλεια μεταξύ δύο συστημάτων, όπου το ένα δρα σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server).

Το πρωτόκολλο SSL είναι οικείο στους περισσοτέρους χρήστες, ακόμα και σε εκείνους χωρίς ιδιαίτερο υπόβαθρο τεχνικών γνώσεων. Είναι είδη εγκατεστημένο σε οποιοδήποτε Η/Υ που είναι συνδεδεμένος στο Διαδίκτυο και χρησιμοποιεί έναν φυλλομετρητή (browser) χωρίς κάποια ιδιαίτερη ρύθμιση. Το SSL είναι ανεξάρτητο από το λειτουργικό σύστημα και επιτρέπει την κλιμάκωση στον έλεγχο πρόσβασης στις εφαρμογές, καθιστώντας το ιδανικό για «κινητούς» χρήστες που επιθυμούν να έχουν πρόσβαση από ένα μη «ασφαλές» άκρο (endpoint).

Το πρωτόκολλο SSL είναι δυνατόν να προσφέρει έλεγχο πρόσβασης σε extranet VPNs ή VPNs απομακρυσμένης πρόσβασης. Ο χρήστης, μέσω ενός SSL VPN, έχει πρόσβαση σε εφαρμογές Web από οπουδήποτε με την απλή χρήση ενός Web browser, μίας σύνδεσης στο Internet, και χωρίς την ανάγκη ύπαρξης κάποιου ιδιαίτερου λογισμικού στον υπολογιστή του. Τα SSL VPNs μπορούν να «περάσουν» πάνω από firewalls και να αντιμετωπίσουν θέματα NAT (Network Address Translation), ζητήματα τα οποία επιλύονται δύσκολα στην περίπτωση των VPNs.

Η ασφαλής σύνδεση που παρέχεται με το πρωτόκολλο SSL επιτυγχάνεται μέσω της πιστοποίησης της ταυτότητας των πλευρών που επικοινωνούν και της κρυπτογράφησης της κίνησης που πραγματοποιείται μεταξύ τους.

Το πρωτόκολλο SSL σωματοποιείται στην κορυφή μίας αξιόπιστης υπηρεσίας μεταφοράς όπως εκείνη που παρέχεται από το TCP/IP και είναι σε Θέση να παρέχει υπηρεσίες ασφάλειας για αυθαίρετες TCP/IP εφαρμογές. Στην πραγματικότητα, ένα σημαντικό πλεονέκτημα της ασφάλειας επιπέδου μεταφοράς γενικά και του SSL, ειδικότερο είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς (transparently) σε οποιαδήποτε TCP/IP εφαρμογή.

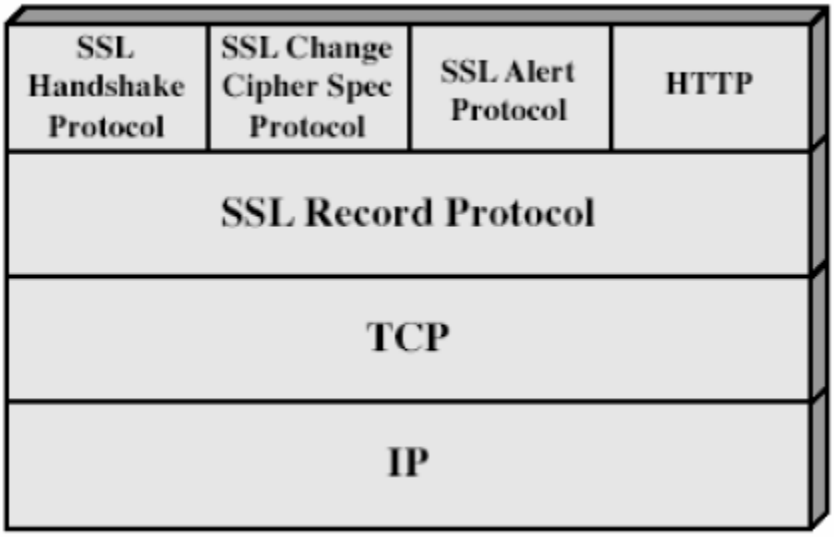


Εικόνα 28*: Σχηματική αναπαράσταση πρωτοκόλλου SSL*

Συνοπτικά. μπορεί να αναφερθεί ότι το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν server (εξυπηρετητής) και το άλλο σαν client (εξυπηρετούμενος). Αυτή η ασφάλεια έχει τρεις βασικές ιδιότητες:

1. Γίνεται πιστοποίηση ταυτότητας και των δύο χρηστών, μέσω κρυπτογραφίας δημόσιου κλειδιού.
2. Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων μέσω κρυπτογράφησης.
3. Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων με χρήση MACs

Γενικά, η ευθύνη του πρωτοκόλλου SSL να συντονίσει τις καταστάσεις συνόδου και σύνδεσης τόσο από την πλευρά του εξυπηρετούμενου όσο και από την πλευρά του εξυπηρετητή. Τα επικοινωνούντα μέρη μπορούν να έχουν πολλαπλές ταυτόχρονες συνόδους, καθώς επίσης και συνόδους με πολλαπλές συνδέσεις.



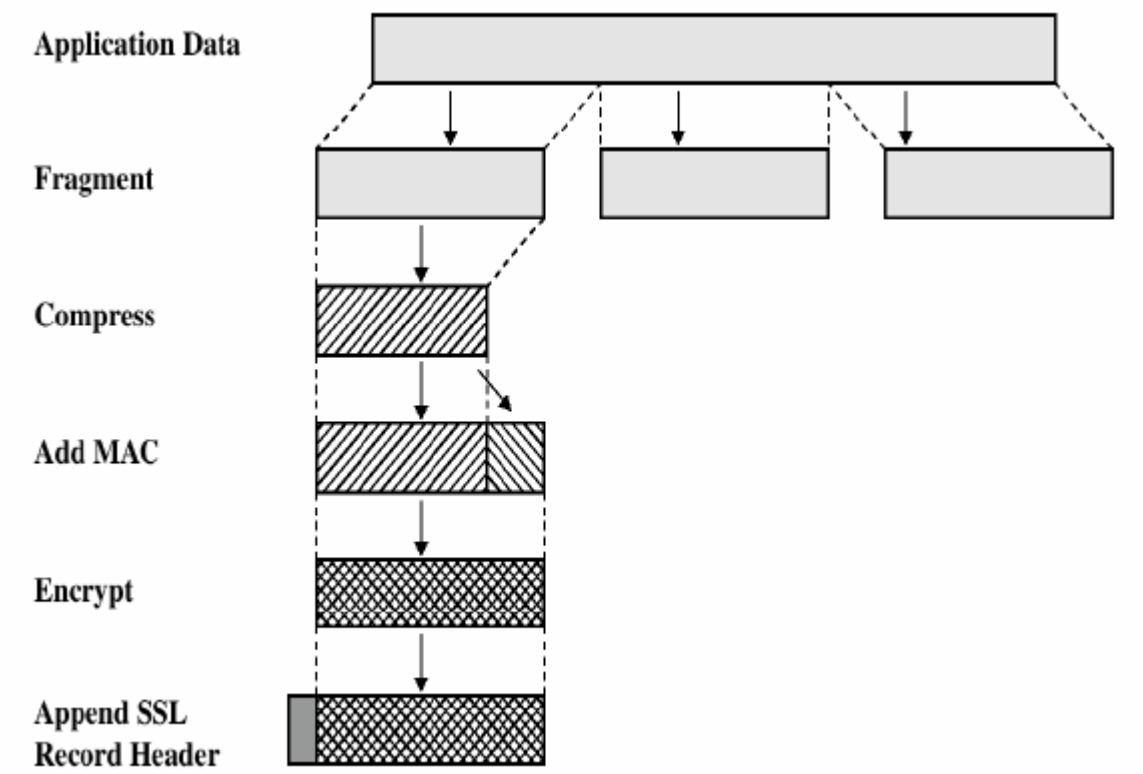
Εικόνα 28*: Αρχιτεκτονική του πρωτοκόλλου SSL*

Τα δύο βασικά πρωτόκολλα του SSL είναι το SSL Record Protocol και το SSL Handshake Protocol. Συνοπτικά, το SSL Record Protocol παρέχει υπηρεσίες εμπιστευτικότητας και ακεραιότητας δεδομένων καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων. Αρκετά πρωτόκολλα SSL, μπορούν να στρωματοποιούνται πάνω από το record protocol. Το σημαντικότερο από αυτά τα πρωτόκολλα είναι το SSL Handsake

Protocol, ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών το οποίο διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και εάν ζητηθεί και του client. Μετά την ολοκλήρωση του SSL Handshake Protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας.

Πιο συγκεκριμένα, το SSL Record Protocol λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και πραγματοποιεί κατακερματισμό (fragmentation), συμπίεση και κρυπτογράφηση δεδομένων. Κάθε ωφέλιμο φορτίο δεδομένων SSL Record Protocol μπορεί να συμπιέζεται και να κρυπτογραφείται σύμφωνα με την τρέχουσα μέθοδο συμπίεσης και τον αλγόριθμο κρυπτογράφησης.

Οι διαδικασίες που συντελούνται από το SSL Record Protocol απεικονίζονται αναλυτικά στην παρακάτω εικόνα.



Εικόνα 29*: Λειτουργίες* SSL Record Protocol

Το SSL Handshake Protocol έχει σκοπό να υποχρεώνει έναν πελάτη και έναν εξυπηρετητή (client) να καθιερώνουν τα πρωτόκολλα που θα χρησιμοποιηθούν κατά τη διάρκεια της επικοινωνίας, να επιλέγουν τη

μέθοδο συμπίεσης και την προδιαγραφή κρυπτογραφίας, να αυθεντικοποιούνται αμοιβαία και να δημιουργούν ένα κύριο μυστικό κλειδί (master secret key), από το οποίο προκύπτουν διάφορα κλειδιά συνόδου για αυθεντικοποίηση και κρυπτογράφηση μηνυμάτων.

Τελειώνοντας πρέπει να επισημάνουμε ότι το βασικό μειονέκτημα του SSL είναι οι περιορισμένες εφαρμογές που μπορεί να εξυπηρετήσει. Επιπλέον όλες αυτές οι εφαρμογές είναι απομακρυσμένης πρόσβασης μόνο (και όχι δίκτυο-προς-δίκτυο οι οποίες μπορούν να υποστηριχτούν από το IPSec). Θα λέγαμε λοιπόν ότι μεγάλη πληθώρα αναγκών που καλύπτει το IPSec δεν καλύπτονται από το SSL. Από την άλλη υπερτερεί ως προς το IPSec ως προς το κόστος αλλά και την πολυπλοκότητα υλοποίησης. Στον ακόλουθο πίνακα επιχειρείται μία σύγκριση των δύο πρωτοκόλλων:

	SSL	**IPSEC**
Εφαρμογές	Ο,τιδήποτε σχετικό με web, ανταλλαγή αρχείων ή email	Όλες όσες βασίζονται σε IP
Κρυπτογράφηση	Ισχυρή (128 bits)	Ισχυρή (128 bits, 168 bits)
Πιστοποίηση ταυτότητας	Ψηφιακά πιστοποιητικά	Ψηφιακά πιστοποιητικά
Κόστος	Χαμηλό	Υψηλό
Πολυπλοκότητα υλοποίησης	Χαμηλή	Υψηλή

***Πίνακας 2**: Σύγκριση SSL και IPSec πρωτοκόλλου.*

4.1 ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερασματικά μπορούμε να πούμε ότι τα IPSec VPNs, παρουσιάζουν αποδεκτή κλιμάκωση, υποστηρίζουν μηχανισμούς QoS. Αν υπάρχει ανάγκη διασύνδεσης μεταξύ sites όπως στη περίπτωση απομακρυσμένου γραφείου με τα κεντρικά γραφεία μιας εταιρίας τα IPSec VPNs είναι η καλύτερη επιλογή.

Αν από την άλλη η εταιρία ή ο πελάτης θέλει μια οικονομικότερη λύση για να προσθέσει πολλά περιφερειακά sites τότε τα MPLS VPNs είναι αυτό που χρειάζεται γιατί το κόστος προσθήκης τους είναι πολύ χαμηλότερο και δεν απαιτούν αγορά αδειών χρήσης.

Τα παρέχουν SSL VPNs μεγάλη ασφάλεια για τη διασύνδεση μεταξύ ενός εξυπηρετητή και ενός πελάτη. Χρησιμοποιούνται κυρίως για να συνδέουν χρήστες σε υπηρεσίες και εφαρμογές μέσω των δικτύων και υποστηρίζονται ευρέως από όλους τους εμπορικούς φυλλομετρητές.

	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…	Δεν απαιτείται. Βασίζεται στο Web browser.

Πίνακας 2*: Σύγκριση MPLS, IPSec και SSL VPNs.*

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Dave Kosiur "Building and Managing Virtual Private Networks"

Ο κ. Dave Kosiur εξηγεί τα VPNs, τη δυνατότητά τους για εξοικονόμηση χρημάτων και τα διάφορα μέσα ασφάλειας (συμπεριλαμβανομένης της κρυπτογράφησης, αλλά και λύσεων βασισμένων στο υλικό). Παρέχει επίσης λεπτομέρειες για όλα τα σημαντικά tunneling πρωτόκολλα, συμπεριλαμβανομένου του Internet Protocol Security Architecture (IPSec), του Point-to-Point Tunneling Protocol (PPTP), και Layer 2 Tunneling Protocol (L2TP).

2. Mike Erwin, Charlie Scott, Paul Wolfe "Virtual Private Networks", 2nd Edition (O'Reilly Nutshell)

Αυτό το βιβλίο εξηγεί πώς μπορεί να προγραμματισθεί και να δημιουργηθεί αποτελεσματικά ένα VPN. Ασχολείται αρχικά με γενικά ενδιαφέροντα πάνω στα VPN όπως δαπάνες, διαμόρφωση, και πώς ένα VPN ταιριάζει με άλλες τεχνολογίες δικτύωσης όπως τα firewalls. Συνεχίζει με λεπτομερείς περιγραφές για το πώς μπορεί να εγκατασταθούν και να χρησιμοποιηθούν τεχνολογίες VPN που είναι διαθέσιμες για τα WINDOWS NT και το Unix, όπως PPTP και L2TP, Altavista Tunnel, Cisco PIX, και το Secure Shell (SSH).

3. Dennis Fowler, "Virtual Private Networks: Making the Right Connection"

Ένας από τους πολύ καλύτερους τίτλους για αρχαρίους που επιδιώκουν να μάθουν για VPN «από το μηδέν». Διαπραγματεύεται τα οφέλη των VPNs και των προκλήσεων που περιλαμβάνονται στην εφαρμογή τους.

4. Ruixi Yuan and W. Timothy Strayer, "Virtual Private Networks: Technologies and Solutions"

Ασχολείται με τις τεχνολογίες VPN και καλύπτει την τεχνική του tunneling, της χρήσης του IPsec και άλλων πρωτοκόλλων, και του public key infrastructure (PKI). Τα VPN προσεγγίζονται τόσο από επιχειρηματική όσο και από τεχνική πλευρά

5. Κώστας Λιμνιώτης «Σχεδίαση Εικονικών Δικτύων»

Ο κ. Κώστας Λιμνιώτης εξηγεί τους λόγους εξάπλωσης της υιοθέτησης των VPN σήμερα. Αναλύει τις βασικές κατηγορίες VPN και περιγράφει τα διαφορετικά πρωτόκολλα που μπορούν να χρησιμοποιηθούν.

6. Κουρτής Παρασκευάς «Εικονικά Ιδιωτικά Δίκτυα»

Ο κ. Κουρτής Παρασκευάς επεξηγεί τι είναι τα VPN, τα πλεονεκτήματά τους, τα πρωτόκολλα υλοποίησής τους, αλλά και το υλικολογισμικό που απαιτείται για το σχεδιασμό τους.

7. Bruce Perlmutter, “Virtual Private Networking: A View From the Trenches”

Το βιβλίο καλύπτει τις βασικές αρχές της τεχνολογίας VPN και της επιχειρησιακής περίπτωσης των VPNs. Το βιβλίο περιέχει συνοπτικές περιγραφές VPN λύσεων από την ματιά των τελικών χρηστών, των φορέων παροχής υπηρεσιών, και της εταιρικής διαχείρισης.

WHITE PAPERS

8. **Understanding Virtual Private Networking, ADTRAN**

9. **IPsec overview, Cisco**

10. **IPSec Virtual Private Networks: Conformance and Performance Testing, Ixia**

11. **Microsoft Privacy Protected Network Access: Virtual Private Networking and Intranet Security, Microsoft**

12. **Security & Savings with Virtual Private Networks, NETGEAR**

13. **High Performance VPN Solutions Over Satellite Networks, Encore Networks**

14. **Preserving End-to-End Quality of Service For IP VPNs Over MPLS Satellite Networks, Encore Networks**

15. **Migration Of Legacy Systems & Applications to Broadband IP VPN Infrastructure, Encore Networks**

16. **Secure Remote Access with IPsec VPNs, Intoto**

17. **The Evolution of Mobile VPN and its Implications for Security, Nokia**

18. **11.Secure Remote Working: Are We Virtually There Yet?, AEP Networks**

ΔΙΑΔΙΚΤΥΟ

19. **http://about.com**
Διαδικτυακός τόπος με πρακτικές συμβουλές και λύσεις για σχεδόν οποιοδήποτε πρόβλημα.

20. **http://www.iec.org**
Η IEC είναι μια μη κερδοσκοπική οργάνωση που αφιερώνεται να βοηθήσει στην πρόοδο της τεχνολογίας και των επιχειρήσεων παγκοσμίως. Από το 1944, το IEC έχει παράσχει τις υψηλής ποιότητας εκπαιδευτικές ευκαιρίες για επαγγελματίες, ακαδημαϊκούς, και σπουδαστές.

21. **http://www.megaproxy.com**
Η Megaproxy είναι εταιρία παροχής ssl vpn λύσεων

22. **http://www.signal42.com**
Η Signal42 παρέχει πρόσφατες ειδήσεις σχετικά με το περιβάλλον Linux και άλλα σχετικά λειτουργικά συστήματα.

23. **http://www.infosyssec.net**
Μια περιεκτικότατη πηγή πληροφοριών σχετικά με θέματα ασφάλειας υπολογιστών και δικτύων στο διαδίκτυο. Περιέχει άρθρα, πληροφορίες και εκπαιδευτικό υλικό.

24. **http://computer.howstuffworks.com**
Μια περιεκτικότατη πηγή πληροφοριών σχετικά με το πώς λειτουργούν όλα τα επιτεύγματα της σύγχρονης τεχνολογίας των υπολογιστών και του διαδικτύου. Περιέχει άρθρα, πληροφορίες και εκπαιδευτικό υλικό.

25. **http://www.comptechdoc.org**
Διαδικτυακός τόπος μιας μη κερδοσκοπική οργάνωσης που σκοπός της είναι η κοινή χρήση πληροφοριών από ειδικούς σε διάφορα τεχνολογικά πεδία που οργανώνονται και παρουσιάζονται με τέτοιο τρόπο ώστε να είναι διδακτικά για να επιτρέψουν στους χρήστες να εξοικειωθούν και να μάθουν πιο γρήγορα τα αντικείμενα που τους ενδιαφέρουν.

26. **http://www.wkmn.com**
Η wkmn είναι εταιρία που παρέχει εκπαιδευτικά προϊόντα πάνω στις τεχνολογίες των υπολογιστών και των δικτύων.

27. **http://www.3com.com**
Η 3COM είναι εταιρία ολοκληρωμένων δικτυακών λύσεων που παρέχει προϊόντα, υπηρεσίες, αλλά και εκπαίδευση, σεμινάρια και πιστοποίηση.

28. **http://www.cisco.com**
Η CISCO είναι εταιρία ολοκληρωμένων δικτυακών λύσεων που παρέχει προϊόντα, υπηρεσίες, αλλά και εκπαίδευση, σεμινάρια και πιστοποίηση.

29. **http://www.intel.com**
Εταιρία που κατασκευάζει VPN προϊόντα

30. **http://www.microsoft.com**
Εταιρία που υποστηρίζει VPN λογισμικό.

31. **http://www.vpnc.org**
Η Virtual Private Network Consortium (Κοινοπραξία Εικονικών Ιδιωτικών Δικτύων) ανάμεσα στους σκοπούς της έχει και την προώθηση προϊόντων VPN, την βοήθεια του τύπου και πιθανών πελατών να καταλάβουν τις τεχνολογίες VPN και τα πρότυπα τους.

32. **http://www.vpnlabs.com**
Τα εργαστήρια VPN είναι μια ανοικτή κοινότητα για την έρευνα, τη δοκιμή, την ανασκόπηση, και τη συζήτηση των Εικονικών Ιδιωτικών Δικτύων.

33. **http://www.FindVPN.com**
Το FindVPN.com παρέχει οδηγούς και έρευνα για τα VPN ή VPN υπηρεσίες, αλλά και πληροφορίες.

34. **http://www.conta.uom.gr**
Το εργαστήριο **CONTA** (COmputer Networks & Telematics Applications) είναι ένα εργαστήριο έρευνας και ανάπτυξης. Τομείς ενδιαφέροντος: Πολυμεσικά Δίκτυα, Οπτικά Δίκτυα, Ποιότητα Υπηρεσιών, Σχεδίαση & Βελτιστοποίηση Δικτύων, Έλεγχος & Διαχείριση Ροής Πληροφορίας, Προσομοιώσεις Δικτύων, Ευφυείς Αλγόριθμοι σε Δίκτυα, Οικονομικά Δικτύων, Τιμολόγηση &Ανταγωνισμός, Τηλε-Εκπαίδευση, Ηλεκτρονικό Εμπόριο, Υπηρεσίες Παγκόσμιου Ιστού.

35. http://www.lcs.mit.edu
Δικτυακός τόπος του Εργαστηρίου Πληροφοριακών Συστημάτων του MIT (Massachusetts Institute of Technology).

36. http://www.wiley.com
Εκδοτικός Οργανισμός-Βιβλία για VPN και links σε προϊόντα, υπηρεσίες, VPN tests κλπ.

37. http://vpn.shmoo.com/
Η ομάδα Shmoo είναι μια μη κερδοσκοπική ομάδα ανταλλαγής και αποθήκευσης γνωμών και γνώσεων που αποτελείται από επαγγελματίες από όλο τον κόσμο που αφιερώνουν από τον ελεύθερους χρόνο και την ενέργειά τους στην έρευνα και την ανάπτυξη της ασφάλειας πληροφοριακών συστημάτων.