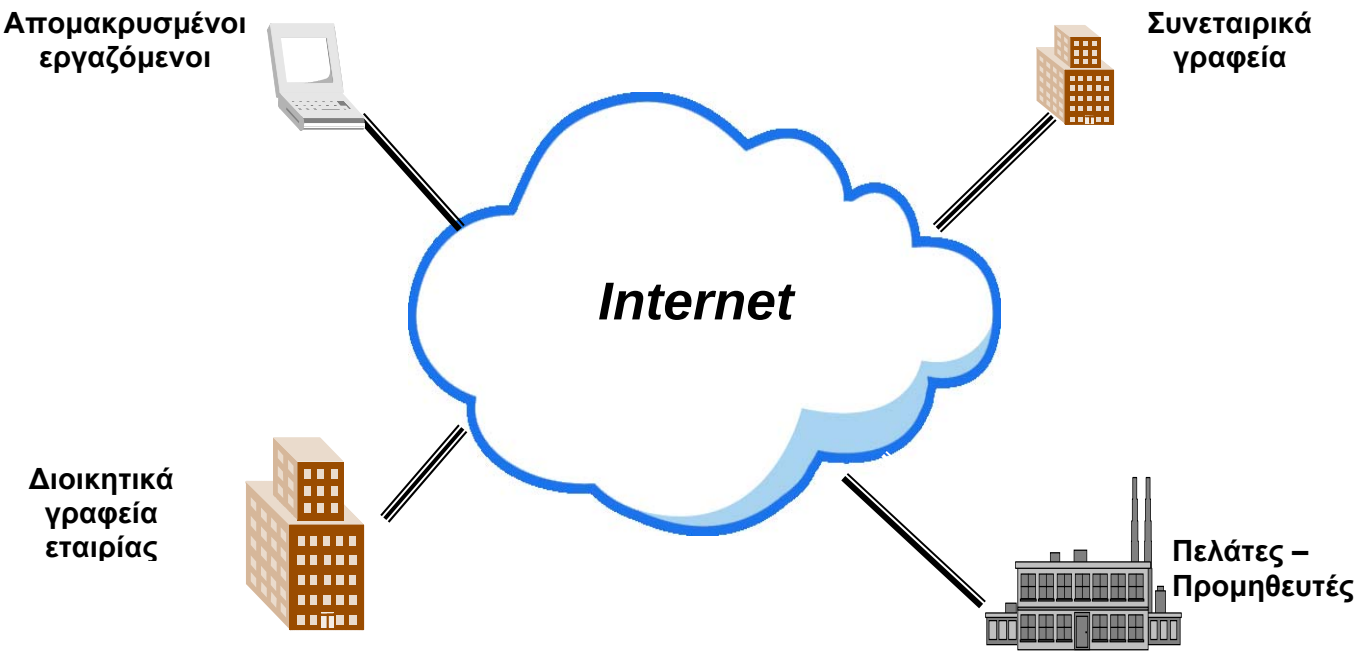
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΛΑΜΙΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΣΧΕΔΙΑΣΗ ΕΙΚΟΝΙΚΩΝ ΔΙΚΤΥΩΝ



Διδάσκων: Κώστας Λιμνιώτης

(Ακαδημαϊκό έτος 2005-2006)

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή

Η εξάπλωση της δικτυωμένης οικονομίας έχει επιφέρει ουσιαστικές αλλαγές στον τρόπο λειτουργίας των επιχειρήσεων. Ο ανταγωνισμός σε πολλές βιομηχανίες έχει οδηγήσει σε τόσο σε συμμαχίες αλλά και συνεταιρισμούς μεταξύ τους. Αυτές οι εξελίξεις έχουν μεν αυξήσει την παραγωγικότητα και την κερδοφορία πολλών επιχειρήσεων, έχουν όμως ταυτόχρονα δημιουργήσει νέες απαιτήσεις για τις επιχειρήσεις αυτές. Ένα δίκτυο που επικεντρώνεται στο να συνδέει απλά σταθερά σημεία των συνεργαζόμενων επιχειρήσεων δεν είναι πλέον αρκετό για πολλές επιχειρήσεις. Οι απομακρυσμένοι χρήστες του δικτύου των επιχειρήσεων, όπως για παράδειγμα οι εξωτερικοί συνεργάτες, απαιτούν πλέον πρόσβαση στους πόρους του δικτύου της επιχείρησης. Για παράδειγμα, θα πρέπει ένας εξωτερικός συνεργάτης μιας επιχείρισης να μπορεί να συνδεθεί στο τοπικό της δίκτυο από οπουδήποτε, μέσω του φορητού του υπολογιστή. Το κλασικό Δίκτυο Ευρείας Περιοχής (WAN) πρέπει λοιπόν να επεκταθεί ώστε να συμπεριλάβει και αυτού του τύπου τους εργαζόμενους. Ταυτόχρονα, οι επιχειρήσεις με περισσότερα από ένα παραρτήματα (καταστήματα, γραφεία) πολύ συχνά αντιμετωπίζουν προβλήματα επικοινωνίας ή λειτουργίας που απορρέουν από τη γεωγραφική απόσταση που τα χωρίζει. Συνεπώς, πολλές επιχειρήσεις στρέφονται προς τα **Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPNs)** για να συμπληρώσουν την υπάρχουσα WAN υποδομή τους και να επιλύσουν προβλήματα επικοινωνίας, οργάνωσης, διαχείρισης και κατανομής πληροφοριών σε όλα τα τμήματα ή τα υποκαταστήματα τους, όπου κι αν βρίσκονται.

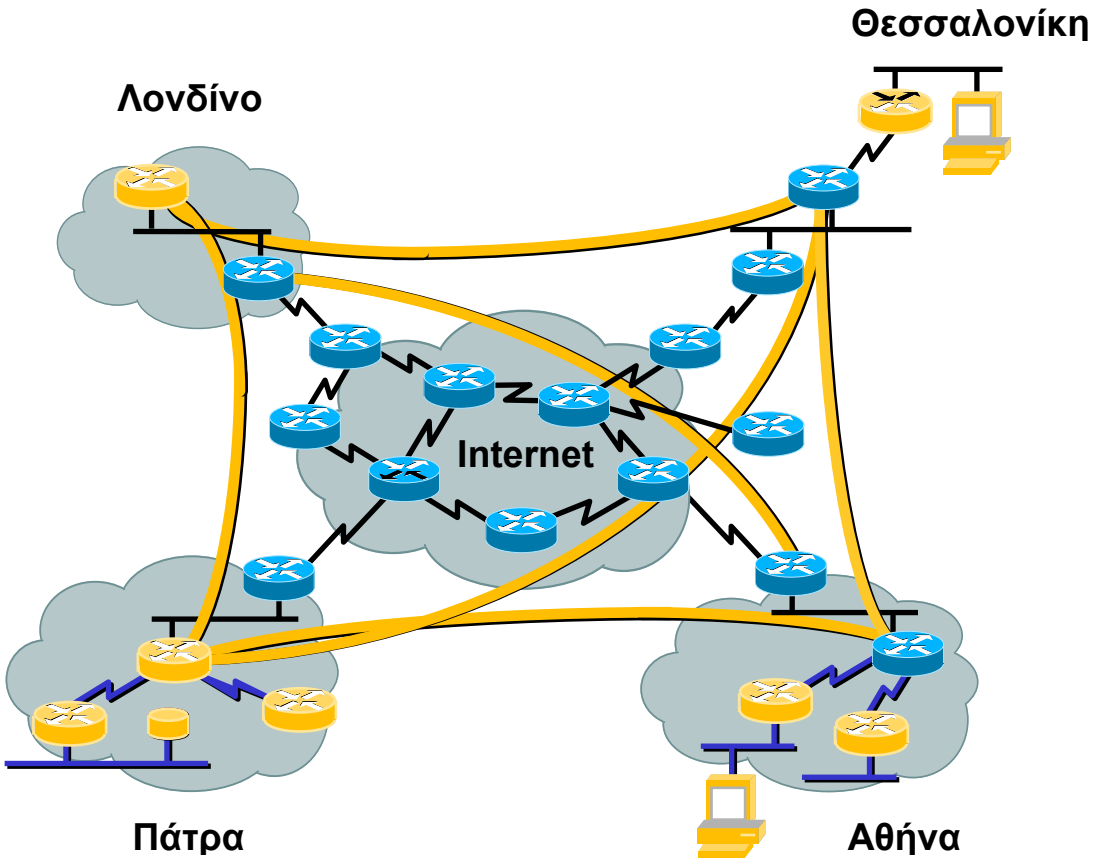
Το VPN είναι ένα δίκτυο εικονικών ζεύξεων ανεπτυγμένο σε μία υπάρχουσα δικτυακή υποδομή, με τη ιδιότητα ότι έχει την ίδια ασφάλεια, διαχείριση και υφίσταται την ίδια πολιτική σε όλο το μήκος του σαν να επρόκειτο για ιδιωτικό δίκτυο. Στην πραγματικότητα είναι μία εναλλακτική λύση της υποδομής που παρέχουν τα WAN και που αντικαθιστούν ή επαυξάνουν τα υπάρχοντα ιδιωτικά δίκτυα που χρησιμοποιούν μισθωμένες γραμμές ή Frame Relay/ATM δίκτυα που ανήκουν στην επιχείρηση. Οι απαιτήσεις των VPNs δεν είναι άλλες από αυτές των WAN: υποστήριξη πολλαπλών πρωτοκόλλων, υψηλή αξιοπιστία και εκτεταμένη διαβάθμιση. Ένα VPN μπορεί να αξιοποιήσει τις πιο γνωστές τεχνολογίες μεταφοράς που υπάρχουν σήμερα: το δημόσιο Internet (κατά κύριο λόγο), τα IP backbones διαφόρων παρόχων υπηρεσιών όπως επίσης και τα Frame Relay και ATM δίκτυά τους.

2. Ιστορική αναδρομή – Αρχιτεκτονικές των VPNs

Τα Εικονικά Ιδιωτικά Δίκτυα αποτελούν στις μέρες μας ένα σύγχρονο και εξελισσόμενο πεδίο και βρίσκουν εφαρμογή κυρίως σε μεγάλες εταιρίες αλλά και σε περιπτώσεις απομακρυσμένης πρόσβασης χρηστών με σκοπό να καλύψουν τις ανάγκες επικοινωνίας τους. Τα κλασικά ιδιωτικά δίκτυα βασίζονται σε μισθωμένες γραμμές όπου το κόστος τους είναι σημαντικό. Η λύση των VPNs προσπαθεί να επιλύσει αυτό το πρόβλημα αφού πλέον χρησιμοποιείται η δημόσια υποδομή, με τα οφέλη που αυτό συνεπάγεται σε θέματα κόστους. Επιπλέον εξακολουθεί να παρέχεται η ασφάλεια και η αξιοπιστία των μισθωμένων γραμμών. Γενικά, η τεχνολογία των Εικονικών Ιδιωτικών Δικτύων συγκεντρώνει πολλά πλεονεκτήματα, με κυριότερο το χαμηλότερο κόστος και την μεγαλύτερη ευελιξία στη διαχείριση.

Ο ακριβής ορισμός ενός Εικονικού Ιδιωτικού Δικτύου είναι «**ένα ιδιωτικό δίκτυο που κατασκευάζεται χρησιμοποιώντας την υπάρχουσα υποδομή ενός δημόσιου δικτύου, όπως για παράδειγμα το Internet ή το υπάρχον δίκτυο του παρόχου**». Ο όρος «ιδιωτικό δίκτυο» σημαίνει ότι πρόσβαση σε αυτό έχουν μόνο οι εξουσιοδοτημένοι χρήστες. Ο όρος «εικονικό δίκτυο» σημαίνει ότι οι δικτυακές συνδέσεις είναι ιδεατές, υπό την έννοια ότι τα δεδομένα που αποστέλλονται μεταξύ δύο χρηστών μπορεί να ακολουθούν κάθε φορά διαφορετική διαδρομή μέχρι να φτάσουν στον προορισμό τους.

Η δημιουργία ενός VPN είναι δυνατόν να βασίζεται στο πρωτόκολλο IP, όπου η προς μετάδοση πληροφορία διαμορφώνεται σε πακέτα IP και μεταδίδεται στο δίκτυο IP (σχήμα 1). Ένα IP VPN (η πιο συνηθισμένη περίπτωση Εικονικών Ιδιωτικών Δικτύων) είναι μία δικτυακή σύνδεση η οποία από την πλευρά των χρηστών συμπεριφέρεται σαν να ήταν μία ιδιωτική σύνδεση, παρόλο που χρησιμοποιείται κοινή διαμοιρασμένη δικτυακή υποδομή (shared communication infrastructure) για την πραγματοποίηση της σύνδεσης. Επιπλέον, η υλοποίηση των Εικονικών Ιδιωτικών Δικτύων είναι δυνατόν να βασίζεται στις τεχνολογίες ATM (Asynchronous Transfer Mode), Frame Relay ή MPLS (MultiProtocol Label Switching).



Σχήμα 1: VPN μιας επιχείρισης με πολλά παραρτήματα, πάνω στο IP

2.1. Τα πρώτα ιδιωτικά δίκτυα - Μισθωμένες Γραμμές

Οι μισθωμένες γραμμές υλοποιούν την τηλεπικοινωνιακή διασύνδεση δύο ή περισσότερων σημείων με προδιαγεγραμμένη ταχύτητα μετάδοσης δεδομένων. Ήταν για τη δεκαετία του 1960 ο μόνος τρόπος υλοποίησης ιδιωτικού δικτύου. Ένα τέτοιο δίκτυο δομείται όταν μία εταιρία μισθώνει κάποιες γραμμές επικοινωνίας για αποκλειστικά δική της ενδο-εταιρική χρήση. Οι γραμμές αυτές δεν ανήκουν στο δημόσιο τηλεφωνικό δίκτυο (PSTN), συνεπώς σε αυτά τα δίκτυα οι παρεχόμενες σημείο-προς-σημείο ("point-to-point") συνδέσεις πραγματοποιούνται χωρίς τη μεσολάβηση των διεπιλογικών κέντρων του τηλεπικοινωνιακού παρόχου. Οι τηλεπικοινωνιακές γραμμές που εκμισθώνει ο τηλεπικοινωνιακός πάροχος μπορούν να χρησιμοποιηθούν για:

- Σύνδεση Τηλεφωνικών Κέντρων
- Τηλεφωνική επικοινωνία
- Τηλεμοιοτυπία (fax)
- Μετάδοση δεδομένων
- Σύνδεση με το Internet και άλλα δημόσια ή ιδιωτικά δίκτυα

- Σύνδεση Εικονοτηλεφώνων και Συστημάτων Ασφαλείας
- Μετάδοση ραδιοφωνικών και τηλεοπτικών προγραμμάτων

Η χρήση των μισθωμένων γραμμών μεταξύ των διαφόρων σημείων μίας επιχείρησης επιτρέπει τη δημιουργία του δικού της δικτύου, με κύρια χαρακτηριστικά:

- Σταθερή χωρητικότητα
- Ταχύτητα μετάδοσης από 8Kbps, 64Kbps έως 2Mbps ανά γραμμή
  - Αναλογικές γραμμές κατάλληλες για μετάδοση φωνής, fax, δεδομένων σε χαμηλές ταχύτητες
  - Ψηφιακές γραμμές ταχυτήτων από 64 Kbps έως 2 Mbps ή 34Mbps, 155 Mbps
- **Ποιότητα και αξιοπιστία** (το βασικό πλεονέκτημα των μισθωμένων γραμμών)
- Πανελλαδική και διεθνής γεωγραφική κάλυψη

Βασικό μειονέκτημα των μισθωμένων γραμμών είναι ότι υπάρχει ένα σταθερό μίσθωμα ανεξάρτητα από τον όγκο των πληροφοριών που μεταφέρονται. Επίσης δεν είναι πολύ «ευέλικτα» δίκτυα, υπό την έννοια ότι δεν αναπροσαρμόζονται εύκολα όταν προκύπτει η ανάγκη εξάπλωσής τους. Αυτά τα μειονεκτήματα έδωσαν την ώθηση για την αναζήτηση νέων λύσεων, οδηγώντας σταδιακά στην ανάπτυξη των σημερινών VPNs.

Μια που οι βασικές τεχνολογίες πάνω στις οποίες δομούνται τα VPN είναι είτε το IP δίκτυο είτε το MPLS πρωτόκολλο, στις επόμενες δύο ενότητες θα περιγραφούν τα βασικά στοιχεία αυτών των τεχνολογιών.

2.2. Πρωτόκολλο IP

Το IP είναι πρωτόκολλο τρίτου επιπέδου και χρησιμοποιείται για διασύνδεση ηλεκτρονικών υπολογιστών που μπορούν να ανήκουν στο ίδιο ή σε διαφορετικά δίκτυα.

Η μετάδοση στο IP γίνεται με την τεχνική των πακέτων (datagrams). Το κάθε πακέτο του IP φθάνει στον παραλήπτη διασχίζοντας ένα ή περισσότερα διασυνδεδεμένα δίκτυα IP, χωρίς να εξαρτάται από άλλα προηγούμενα ή επόμενα πακέτα διατηρώντας έτσι την αυτονομία του μέσα στο δίκτυο.

Το IP ως πρωτόκολλο τρίτου επιπέδου δεν ασχολείται με τις φυσικές συνδέσεις ή τον έλεγχο των ενδιάμεσων ζεύξεων μεταξύ των κόμβων του δικτύου (που είναι αρμοδιότητα άλλων πρωτοκολλων χαμηλότερων επιπέδων όπως Ethernet, Frame Relay, PPP, κλπ). Στην ουσία ασχολείται με την διευθυνσιοδότηση, τον κατακερματισμό (fragmentation) μεγάλων πακέτων και την επανασυγκόλληση τους. Το πρωτόκολλο IP δεν θεωρείται αξιόπιστο καθώς δεν εξασφαλίζει την απ' άκρου εις άκρο ακεραιότητα των δεδομένων μέσω κάποιων τεχνικών επανεκπομπής, ελέγχου ροής κλπ. Οι λειτουργίες αυτές επιτυγχάνονται με το πρωτόκολλο TCP που είναι στο αμέσως ανώτερο επίπεδο. Το IP δεν απαιτεί την αποκατάσταση σύνδεσης μεταξύ δύο σημείων πριν την αναταλλαγή δεδομένων και γι' αυτό χαρακτηρίζεται ως χωρίς σύνδεση (connectionless).

Το IP παραλαμβάνει τα δεδομένα από το ανώτερο επίπεδο σε πακέτα με μέγιστο μέγεθος 64 Kbyte. Το IP διαιρεί το κάθε πακέτο σε περισσότερα τμήματα (fragments) (αν είναι απαραίτητο) και τα μεταδίδει μέσω του δικτύου. Ο κατακερματισμός αυτός γίνεται στις περιπτώσεις που τα πακέτα IP πρέπει να περάσουν από δίκτυα που έχουν περιορισμό στο μέγιστο μέγεθος πλαισίου (frame). Το Ethernet για παράδειγμα μπορεί να χειριστεί πλαίσια μεγέθους 64 έως 1500 Byte. Ενώ το έργο του κατακερματισμού μπορεί να γίνει από οποιαδήποτε ενδιάμεση συσκευή (π.χ. δρομολογητή) του δικτύου, η επανασυγκόλληση των IP πακέτων γίνεται από τον τελικό παραλήπτη.

Στο χειρισμό του πρωτοκόλλου IP συμμετέχουν μόνο οι δύο ακραίοι υπολογιστικοί σταθμοί και οι ενδιάμεσοι δρομολογητές. Την δρομολόγηση του IP πρωτοκόλλου αναλαμβάνουν οι δρομολογητές οι οποίοι γνωρίζουν την τοπολογία του δικτύου και διαθέτουν κατάλληλους πίνακες δρομολόγησης. Έτσι οι χρήστες αρκεί να γνωρίζουν μόνο την τελική διεύθυνση του αποδέκτη ώστε να δρομολογηθεί κατάλληλα το μήνυμά τους.

2.3. Τεχνολογία MPLS

Το MPLS (Multiprotocol Label Switching) είναι ένα πρωτόκολλο το οποίο δημιουργήθηκε από την IETF με στόχο να αυξήσει την ευελιξία και την απόδοση του παραδοσιακού IP και ταυτόχρονα να δώσει την δυνατότητα για την παροχή νέων

υπηρεσιών στο Διαδίκτυο. Το MPLS συνδυάζει την μεταγωγή με **ετικέτα (label)** και την παραδοσιακή δρομολόγηση του πρωτοκόλλου IP. Η τεχνική αυτή χρησιμοποιεί, εν γένει, 'ετικέτες' που κατασκευάζονται και τοποθετούνται κατά την εισαγωγή των πακέτων στο Δίκτυο Μεταγωγής / Κορμού, για την προώθηση τους στον τελικό προορισμό. Οι ετικέτες υποδεικνύουν τόσο τη δρομολόγηση των πακέτων όσο και τα χαρακτηριστικά ποιότητας των υπηρεσιών που παρέχονται από το δίκτυο.

Τα κύρια συστατικά της τεχνολογίας MPLS είναι τα εξής:

Ετικέτα (Label): Είναι η επικεφαλίδα/ετικέτα που χρησιμοποιείται από τους LSR (Label Switch Router) για την προώθηση των πακέτων. Οι LSRs διαβάζουν μόνο τις ετικέτες αυτού του τύπου, και όχι τις επικεφαλίδες IP των πακέτων. Οι ετικέτες έχουν νόημα μόνο σε τοπικό επίπεδο, δηλαδή μόνο μεταξύ δύο συσκευών που επικοινωνούν.

Δρομολογητής ετικέτας (Label Switch Router (LSR)): Αποτελεί την συσκευή κορμού του δικτύου που μετάγει πακέτα εφοδιασμένα με την κατάλληλη ετικέτα, σύμφωνα με τους προϋπολογισμένους πίνακες μεταγωγής.

Δρομολογητής ετικέτας άκρου (Edge Label Switch Router (Edge LSR)): Είναι η συσκευή που τοποθετείται στο άκρο του κυρίως δικτύου, η οποία εκτελεί την αρχική επεξεργασία και κατηγοριοποίηση του κάθε πακέτου και του αναθέτει την πρώτη ετικέτα.

Μονοπάτι ετικέτας (Label Switched Path (LSP)): Είναι το "μονοπάτι" που ορίζεται από τις ετικέτες που δημιουργούνται και ανατίθενται στο κάθε πακέτο, μεταξύ των τελικών σημείων του δικτύου. 'Ενα LSP μπορεί να είναι ορισμένο είτε στατικά είτε δυναμικά. Το τελευταίο προσδιορίζεται αυτόματα χρησιμοποιώντας πληροφορίες δρομολόγησης. Τα στατικά LSPs χρησιμοποιούνται σπανιότερα.

Πρωτόκολλο διανομής ετικετών (Label Distribution Protocol (LDP)): Είναι το πρωτόκολλο που έχει σαν ρόλο την απόδοση ετικετών στα πακέτα, καθώς και τη μετάφραση των πληροφοριών τους από τους LSRs. Αναθέτει ετικέτες στα πακέτα από τις δικτυακές συσκευές στις άκρες και στον πυρήνα του δικτύου, έτσι ώστε να καθοριστούν τα αναγκαία LSPs. Η απόδοση των ετικετών γίνεται σε συνδυασμό με κάποια πρωτόκολλα δρομολόγησης, όπως τα Open Shortest Path First (OSPF),

Intermediate System to Intermediate System (IS-IS), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) ή Border Gateway Protocol (BGP).

2.4. Αρχιτεκτονικές Εικονικών Ιδιωτικών Δικτύων

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

1. Με βάση την αντιστοιχία τους με τα επίπεδα του μοντέλου αναφοράς OSI, τα Εικονικά Ιδιωτικά Δίκτυα κατηγοριοποιούνται ως εξής:
    a. 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 MPLS δίκτυα.
    b. 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 MPLS.
    c. Στα Εικονικά Δίκτυα επιπέδου 4 (Μεταφοράς). Σε αυτήν την κατηγορία εμπίπτουν τα VPN στα οποία χρησιμοποιείται το πρωτόκολλο SSL.
2. Με βάση το είδος της διόδου (tunnel) που αναπτύσσεται (όπου με τον όρο δίοδο εννοούμε πρακτικά το νοητό κύκλωμα που σχηματίζεται, 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:
    a. οι «αυθόρμητες δίοδοι» (voluntary tunnels),
    b. οι «αναγκαστικές» δίοδοι (compulsory ή mandatory tunnels).
3. Με βάση το ποιοι είναι οι τελικοί χρήστες του VPN (δηλαδή ποια είναι τα δύο μέρη που συνομιλούν). Έτσι έχουμε:
    a. Τα VPN δομής «πελάτης-προς-δίκτυο» (client-to-LAN), όπου στην ουσία ένας απλός χρήστης συνδέεται με τον υπολογιστή του σε ένα

τοπικό δίκτυο. Αυτού του είδους τα VPN ονομάζονται επίσης και «Εικονικά Ιδιωτικά Δίκτυα Απομακρυσμένης Πρόσβασης»

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

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.

Η ανάλυση που θα υιοθετήσουμε βασίζεται στην πρώτη κατηγοριοποίηση – δηλαδή ως προς τα επίπεδα των χρησιμοποιούμενων πρωτοκόλλων, σε σχέση πάντα με τα επίπεδα αναφοράς του OSI. Μέσω όμως αυτής της ανάλυσης θα περιγραφούν όλα τα είδη Εικονικών Ιδιωτικών Δικτύων.

3. Εικονικά Ιδιωτικά Δίκτυα Επιπέδου Δικτύου

3.1. Εικονικά Ιδιωτικά Δίκτυα βασισμένα στην τεχνολογία MPLS

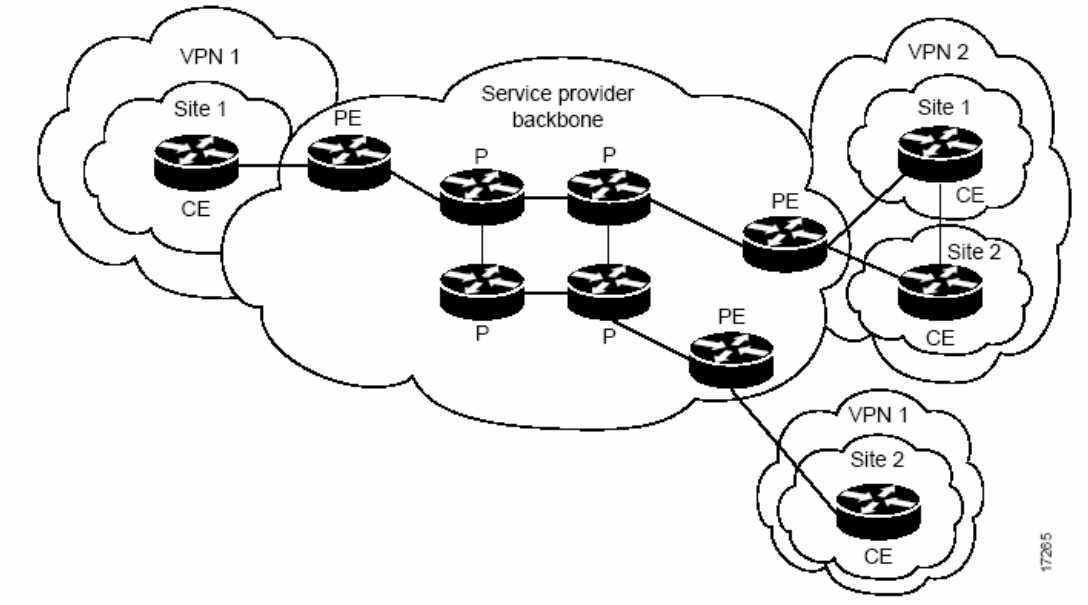
3.1.1. Γενική Περιγραφή

Τα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου Δικτύου που βασίζονται στην τεχνολογία MPLS (L3 MPLS VPNs) επιτρέπουν τη δημιουργία VPNs κάνοντας χρήση του δικτύου κορμού MPLS του ISP. Τα VPNs 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 CE (customer edge)**. Είναι οι δρομολογητές που τους διαχειρίζεται ο πελάτης και ανήκουν συνήθως σε αυτόν.
- **Δρομολογητές PE (provider edge)**. Είναι οι δρομολογητές που αποτελούν τα σημεία εισόδου και εξόδου των VPNs. Ανήκουν διαχειριστικά στον ISP. Αποτελούν το πιο σημαντικό τμήμα στη «λογική» των MPLS VPNs.
- **Δρομολογητές P (provider)**. Είναι οι δρομολογητές που αποτελούν το δίκτυο κορμού του ISP και ανήκουν και αυτοί διαχειριστικά σε αυτόν. Δεν συμμετέχουν στη λογική VPN - ο κύριος σκοπός τους είναι η προώθηση των MPLS ετικετών προς τους PE routers.

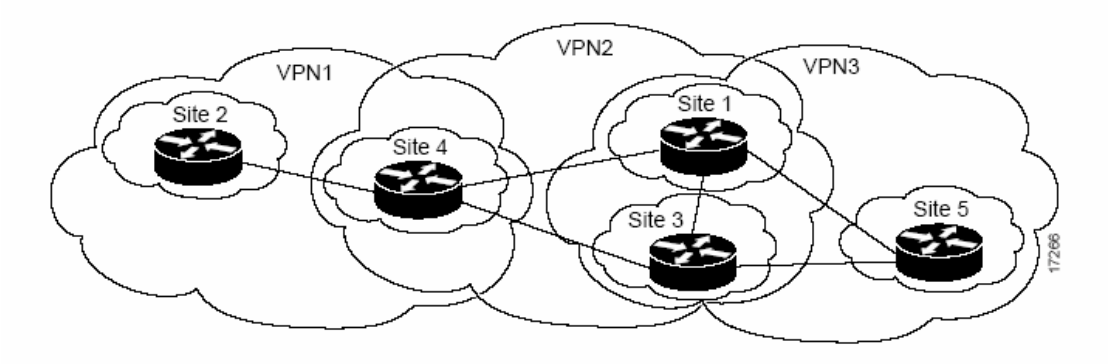
Χαρακτηριστικό είναι και το σχήμα που ακολουθεί:



Σχήμα 2: Ένα απλό παράδειγμα MPLS VPN

Όπως φαίνεται απο το παραπάνω σχήμα, το δίκτυο του πάροχου (Service Provider backbone) αποτελείται από δρομολογητές τύπου P και PE. Στο δίκτυο κορμού του πάροχου συνδέονται τέσσερα sites, δύο από αυτά ανήκουν στο VPN1 και άλλα δύο sites ανήκουν στο VPN2 (όπου ένα site μπορεί να είναι ένα τοπικό δίκτυο Ethernet).

Πρέπει να σημειωθεί πως τίποτε δεν αποκλείει ένα site να ανήκει όχι μόνο σε ένα αλλά σε δύο VPNs. Χαρακτηριστικό είναι το σχήμα που ακολουθεί:



Σχήμα 3: Παράδειγμα MPLS VPN όπου κάποια sites μπορεί να ανήκουν σε περισσότερα από ένα VPNs

Οι PE δρομολογητές είναι αυτοί που διαμοιράζουν τις πληροφορίες δρομολόγησης των διαφόρων VPNs και ενημερώνουν τους πίνακες δρομολόγησης που ανήκουν σε κάθε VPN. Οι PE δρομολογητές μεταφέρουν αυτή την πληροφορία μεταξύ τους με τη χρήση του πρωτόκολλου BGP (Border Gateway Protocol). Με τη χρήση του MPLS λοιπόν ανταλλάσουν MPLS ετικέτες και έτσι είναι δυνατό κάθε στιγμή, ένα «μέλος» ενός VPN που συνδέεται σε έναν συγκεκριμένο δρομολογητή PE να επικοινωνήσει με οποιοδήποτε άλλο «μέλος» του ίδιου VPN που συνδέεται σε κάποιον άλλο PE. Επιπλέον είναι δυνατό, μέσω πολιτικής πρόσβασης στο BGP, να επιτρέπεται ή να απαγορεύεται η πρόσβαση από/προς συγκεκριμένα «μέλη» ενός VPN. Γενικά, **το BGP είναι ένα αξιόπιστο και αποτελεσματικό πρωτόκολλο και το αποκλειστικό πρώτοκολλο ανταλλαγής πινάκων δρομολόγησης ανάμεσα σε παρόχους.** Παρέχει μεγάλη ευελιξία αφού επιτρέπει ή απαγορεύει 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 (backup).

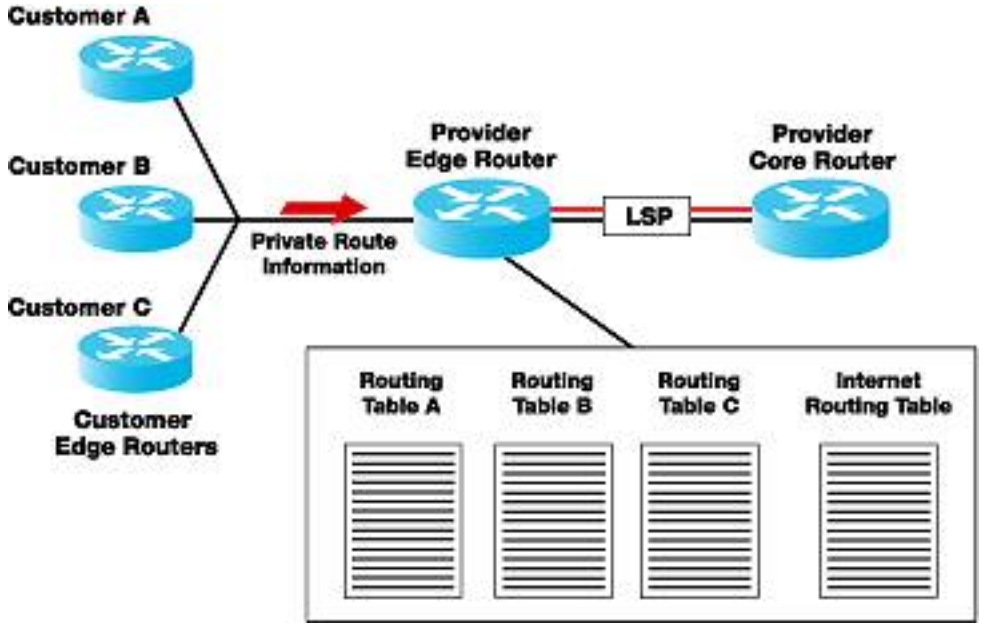
Οι P δρομολογητές δεν συμμετέχουν στην δρομολόγηση των VPNs. Συμμετέχουν μόνο στην ανταλλαγή ετικετών προκειμένου να δημιουργηθούν MPLS LSPs ανάμεσα στους δρομολογητές. Αυτά τα LSPs χρησιμοποιούν οι PEs προκειμένου να μεταφέρουν την κίνηση ανάμεσα στα «μέλη» των VPNs.

Αφού όλη η πληροφορία που διακινείται ανάμεσα στα διάφορα VPNs περνά «μέσα» από κοινό LSP (π.χ. το LSP που συνδέει τον P δρομολογητή της Αθήνας με τον P δρομολογητή της Θεσσαλονίκης), πώς γνωρίζει ο PE δρομολογητής που συνδέεται με τη σειρά του σε έναν P δρομολογητή σε ποιό VPN θα παραδώσει την πληροφορία του χρήστη (για την ακρίβεια, τα πακέτα του χρήστη); Σε αυτό το σημείο υπεισέρχεται ένα ακόμη label, το οποίο αναφέρεται σε συγκεκριμένο VPN. Άρα, τα MPLS πακέτα περιέχουν 2 ετικέτες – μία για τη δρομολόγηση του πακέτου μεταξύ των κόμβων του παρόχου και μία δεύτερη για την ταυτοποίηση ενός VPN.

Το BGP αποτελεί το πρωτόκολλο επιλογής για την μεταφορά της πληροφορίας δρομολόγησης στην υλοποίηση των MPLS VPNs. Με τη χρήση του BGP, οι δρομολογητές PE «γνωρίζουν» τους πίνακες δρομολόγησης των διαφόρων VPNs που συνδέονται σε άλλους PE δρομολογητές. Για παράδειγμα, αν το παράρτημα 1 (ας το ονομάσουμε site 1) κάποιας εταιρίας συνδέεται στο δρομολογητή PE1 του ISP ενώ το παράρτημα 2 της ίδιας εταιρίας συνδέεται στον PE2 τότε μέσω BGP, ο PE1 γνωρίζει ότι ο PE2 έχει συνδεδεμένο το site 2 και αντίστοιχα ο PE2 γνωρίζει ότι ο PE1 έχει συνδεδεμένο το site 1. Έτσι η εταιρία (και προφανώς τα παραρτήματά της) έχουν σύνδεση IP μέσω του δημόσιου δικτύου MPLS του πάροχου.

Είναι επίσης προφανές ότι σε κάθε PE δρομολογητή συνδέονται περισσότεροι από έναν πελάτες. Έτσι, κάθε PE δρομολογητής διατηρεί έναν «υποπίνακα» δρομολόγησης που περιέχει μόνο την πληροφορία δρομολόγησης που αφορά τον συγκεκριμένο πελάτη και μόνον αυτόν. Αυτό προσφέρει μέγιστη ασφάλεια αφού ο πίνακας δρομολόγησης ανήκει μόνο σε συγκεκριμένο πελάτη. Με άλλα λόγια, κάθε PE είναι σαν ένα σύνολο από εικονικούς δρομολογητές (virtual routers).

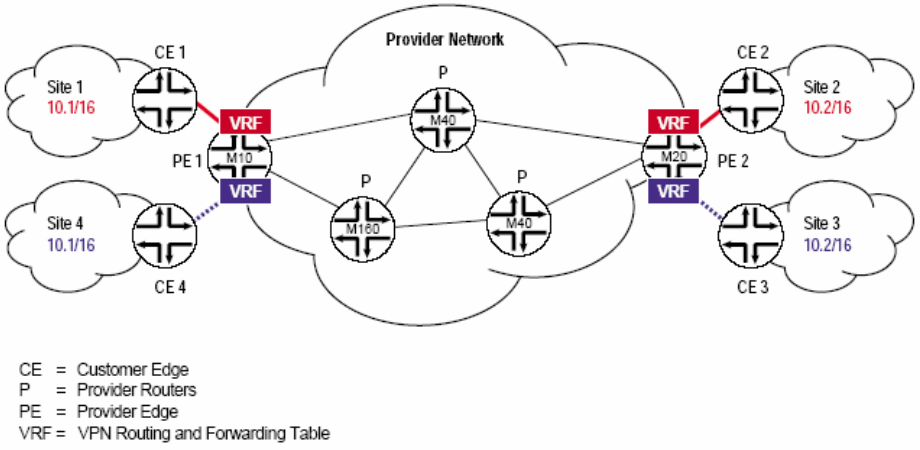
Χαρακτηριστικό είναι και το σχήμα που ακολουθεί:



Σχήμα 4: Τυπικό Routing Table σε έναν δρομολογητή PE

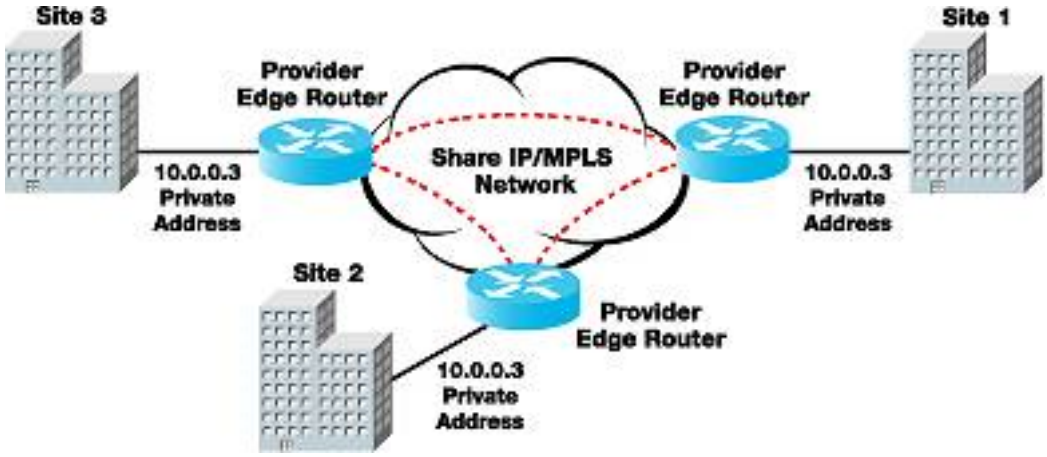
Όπως φαίνεται από το παραπάνω σχήμα, κάθε πίνακας δρομολόγησης (routing table) αναφέρεται σε διαφορετικό πελάτη **και αποτελεί έναν ανεξάρτητο εικονικό πίνακα δρομολόγησης που αποκαλείται VRF (Virtual Routing & Forwarding Instance)**.

Το σχήμα που ακολουθεί, δείχνει τα σημεία του δικτύου MPLS που υλοποιούνται τα διάφορα VRFs.



Σχήμα 5: Παράδειγμα τοπολογίας δικτύου BGP/MPLS VPN

Όταν σε κάθε ιδιωτικό δίκτυο χρησιμοποιούνται ιδιωτικές διευθύνσεις, αυτές δεν είναι μοναδικές ανά τον κόσμο και συνεπώς υπάρχει περίπτωση δύο υπολογιστές διαφορετικών δικτύων που θα θελήσουν να συνδεθούν μέσω ενός VPN να έχουν την ίδια διεύθυνση. (βλέπε σχήμα 6)



Σχήμα 6: Η χρήση ιδιωτικών διευθύνσεων μπορεί να προκαλέσει πρόβλημα (αλληλοεπικάλυψη διευθύνσεων)

Για τη γενικότερη λύση αυτού του προβλήματος υπάρχει το πρωτόκολλο NAT (Network Address Translator), που θα αναπτυχθεί σε άλλο κεφάλαιο. Ιδιαίτερα όμως όταν ο πάροχος έχει MPLS δομή, υπάρχει μια ειδική τεχνική που αναπτύσσει για να αντιμετωπίσει αυτό το πρόβλημα. Συγκεκριμένα, αναθέτει σε κάθε VPN ένα διαχωριστή δρομολόγησης που καλείται Route Distinguisher ή Route Descriptor (RD) και είναι διαφορετικός για κάθε πελάτη. Με αυτόν τον τρόπο «κατασκευάζονται» **μοναδικές διευθύνσεις** οι οποίες καλούνται VPN IP διεύθυνσεις και δημιουργούνται συνδέοντας τον RD με την IP διεύθυνση του πελάτη.

Σχήμα 7: VPN IP Διευθύνσεις

Επομένως, από την πλευρά της ασφάλειας, μέλη ενός VPN μπορούν να είναι μόνο όσοι έχουν το κατάλληλο διαχωριστή δρομολόγησης RD. Αυτή η ιδιότητα καθιστά την είσοδο μη εξουσιοδοτημένων χρηστών στα MPLS VPNs θεωρητικά αδύνατη.

Αν μια εταιρία θέλει να προσθέσει ένα νέο μέλος στο εταιρικό VPN (π.χ. ένα νέο παράρτημα), απλά ο πάροχος χρειάζεται να κάνει δύο ενέργειες:

- να ενημερώσει τον δρομολογητή CE του νέου παραρτήματος για τον τρόπο σύνδεσης στο δίκτυο του παρόχου,

- να διαμορφώσει τον PE δρομολογητή έτσι ώστε να αναγνωρίζει τη συμμετοχή του συγκεκριμένου CE στο συγκεκριμένο VPN.

Στη συνέχεια, το BGP που «τρέχει» στο συγκεκριμένο PE ενημερώνει αυτόματα όλους τους άλλους PEs για το νέο «μέλος».

Είναι σημαντικό να τονιστεί εν κατακλείδι ότι το υποδίκτυο της εταιρίας που δημιουργείται μέσα στο δίκτυο MPLS του ISP είναι ένα δίκτυο που, παρόλο που στηρίζεται σε ένα δημόσιο δίκτυο MPLS, αποτελεί ουσιαστικά ένα ιδιωτικό και απομονωμένο δίκτυο δεδομένων. Η ταχύτητα σε Mbps της σύνδεσης των διαφόρων πελατών εξαρτάται από την ταχύτητα της σύνδεσης μέσω CE & PE. Οι γραμμές αυτές στην Ελληνική δικτυακή πραγματικότητα θα μπορούσαν να είναι μισθωμένες γραμμές τύπου HellasCom.

3.2. Εικονικά Ιδιωτικά Δίκτυα βασισμένα στο πρωτόκολλο IPSec

3.2.1. Γενική Περιγραφή

Τα πρωτόκολλα TCP/IP δεν παρέχουν μηχανισμούς κρυπτογράφησης. Συνεπώς, για την ασφαλή μετάδοση πάνω σε δίκτυο IP υπήρξε η ανάγκη νέου πρωτοκόλλου με μηχανισμούς κρυπτογράφησης, το 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 (packets) μέσω του στρώματος IP. Το IPSec σήμερα αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των δικτύων VPN. Ως προς τα επίπεδα του OSI, αντιστοιχίζεται στο επίπεδο 3 (επίπεδο δικτύου).

Τα θέματα ασφάλειας που ανακύπτουν με τη χρησιμοποίηση του Διαδικτύου για τη πραγματοποίηση ιδιωτικών επικοινωνιών είναι τα ακόλουθα:

- *Απώλεια της Ιδιωτικότητας των Δεδομένων (Loss of Privacy):* Σ' αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνησή 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 πληροφορίες που σε διαφορετική περίπτωση δε θα μπορούσε να έχει.

- *Άρνηση Υπηρεσιών (Denial-of-Service)*: Σ' αυτήν την περίπτωση γίνεται "επίθεση" σε κάποιον server του δικτύου.

Ο βασικός στόχος στην ανάπτυξη του προτύπου IPSec είναι η αντιμετώπιση των παραπάνω απειλών χωρίς να απαιτείται πρόσθετος εξοπλισμός, ούτε να υπάρχει ανάγκη για ένα σύνολο τροποποιήσεων και αλλαγών σε διάφορες εφαρμογές.

Έτσι οι υπηρεσίες που προσφέρει το πρωτόκολλο IPSec είναι:

- **Ακεραιότητα των 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 μόνο από εγκεκριμένους χρήστες.

Το IPSec αναφέρεται σε μια σειρά πρωτοκόλλων όπως ορίζεται στα RFC 2401-2411 και RFC 2451. Αυτά τα πρωτόκολλα χωρίζονται σε δύο κύριες κατηγορίες:

► *Πρωτόκολλα σχετικά με την ασφάλεια*, τα οποία καθορίζουν την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι εμπιστευτικότητας, ακεραιότητας και πιστοποίησης ταυτότητας. Επίσης καθορίζεται και το πως πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου.

► *Πρωτόκολλα σχετικά με την ανταλλαγή κλειδιών*, τα οποία διαπραγματεύονται το συσχετισμό ασφάλειας μεταξύ των δυο υποψήφιων προς επικοινωνίας οντοτήτων (θα επεξηγηθεί παρακάτω).

3.2.2. Μηχανισμοί Ασφάλειας

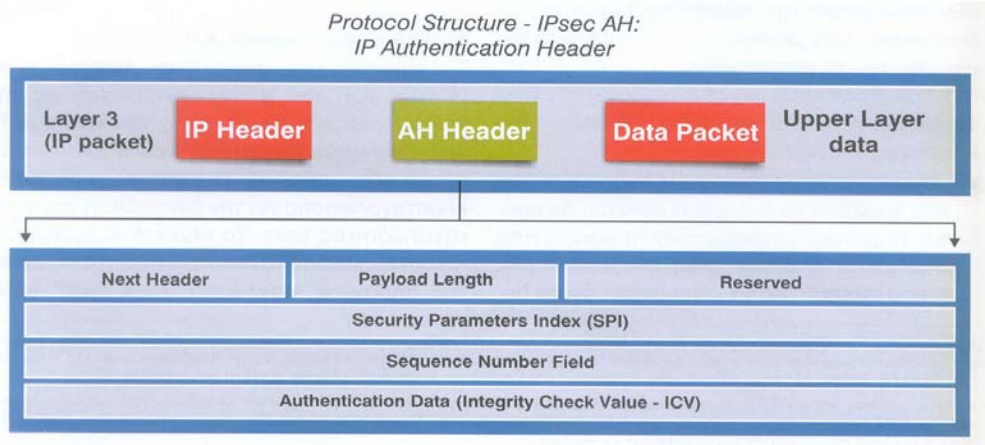
Το IPSec ορίζει ένα νέο σετ κεφαλίδων το οποίο προστίθεται στα IP πακέτα. Προκύπτουν έτσι καινούρια IP πακέτα μεγαλύτερα σε μέγεθος και άλλης δομής, που όμως επιτρέπουν τη διασφάλιση των απαιτήσεων ασφαλείας που περιγράφηκαν παραπάνω. Αυτές οι νέες κεφαλίδες, που διασφαλίζουν την ασφάλεια των IP πακέτων, αναλύονται παρακάτω:

- ✓ **Κεφαλίδα πιστοποίησης ταυτότητας (AH—Authentication Header)**: Αυτή η κεφαλίδα 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 του 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 το 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 (σχήμα 8):

  - 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.)
  - Μέγεθος του φορτίου (Payload length)
  - Δείκτης παραμέτρων ασφαλείας (Security Parameter Index (SPI)) – προσδιορίζει στον παραλήπτη ποια πρωτόκολλα ασφαλείας χρησιμοποιήθηκαν από τον αποστολέα
  - Ακολουθιακός αριθμός (Sequence number): αυξάνεται κατά ένα για κάθε νέο πακέτο που καταφτάνει στον δέκτη από τον ίδιο αποστολέα και με το ίδιο SPI.

- Δεδομένα πιστοποίησης ταυτότητας (Authentication data) – το τμήμα εκείνο που εξασφαλίζει την πιστοποίηση ταυτότητας. Όπως ήδη αναφέρθηκε, είναι το αποτέλεσμα μίας συνάρτησης κατακερματισμού (Integration Check Value – ICV).



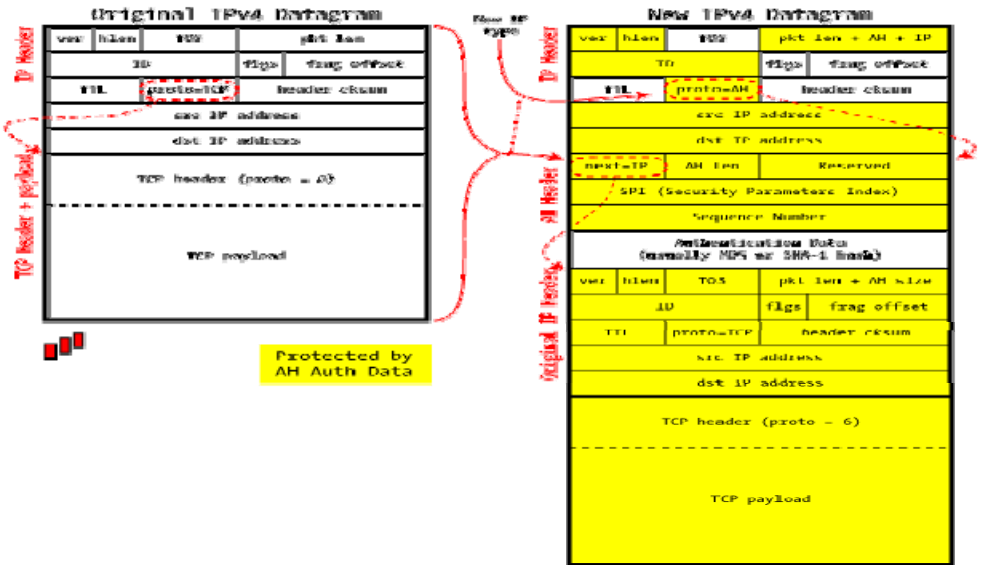
Σχήμα 8: Πεδία ενός AH Header.

Οι λειτουργίες ακεραιότητας και πιστοποίησης μέσω της κεφαλίδας πιστοποίησης εφαρμόζονται (σχήμα 9):

- Σε ολόκληρο το IP πακέτο, εκτός από εκείνα τα πεδία (IP header fields) που αλλάζουν κατά τη μεταφορά του όπως παραδείγματος χάριν το πεδίο TTL, που αλλάζει από τους δρομολογητές των διάφορων δικτύων (μειώνεται), κατά μήκος της πορείας που ακολουθεί το IP πακέτο.

- Σε όλο το AH header πλην του πεδίου του “Authentication Data” .

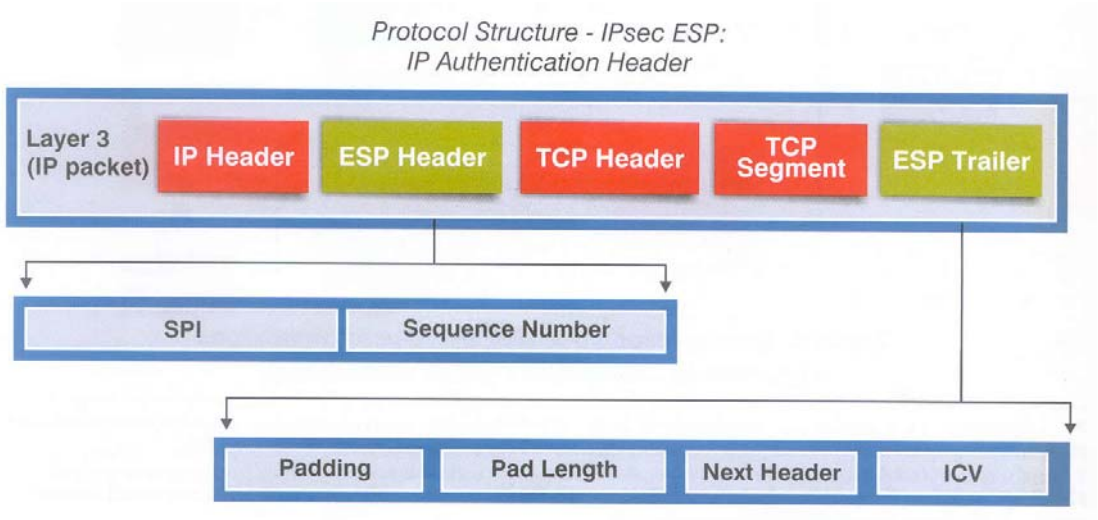
- Σε όλα τα δεδομένα των πάνω στρωμάτων της στοίβας πρωτοκόλλου (δεδομένα του IP πακέτου).



Σχήμα 9: Σύγκριση αρχικού IP πακέτου με το νέο, μετά την προσθήκη του AH.

✓**Ασφαλής Ενθυλάκωση της πληροφορίας** (**Encapsulating Security Payload – ESP**): 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 κρυπτογράφησης ενός IP πακέτου. Το ESP υποστηρίζει ένα μεγάλο αριθμό συμμετρικών αλγορίθμων κρυπτογράφησης, αλλά η εξ ορισμού συνηθισμένη προεπιλογή είναι ο αλγόριθμος AES (128-bit). Αυτό όμως δεν σημαίνει ότι δεν μπορούν να χρησιμοποιηθούν άλλοι αλγόριθμοι – όπως για παράδειγμα ο 3DES ή ο απλός DES.

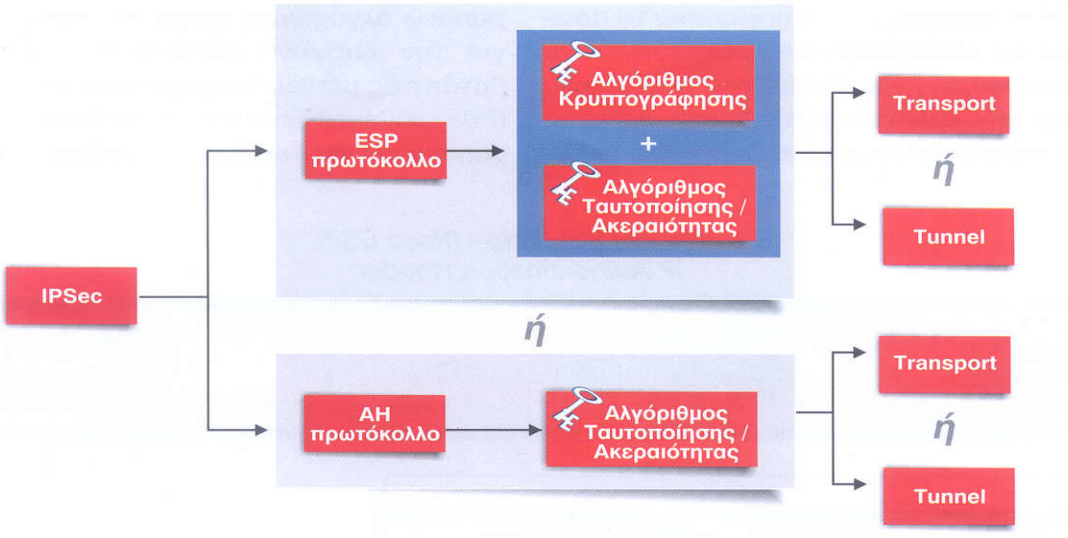
Τα πεδία της κεφαλίδας ESP είναι 6 – δύο από αυτά τοποθετούνται πριν το φορτίο του IP πακέτου (ESP Header) και τα υπόλοιπα τέσσερα μετά από αυτό (ESP Trailer) (σχήμα 10). Τα πεδία SPI και Sequence Number του ESP Header έχουν την ίδια λειτουργία όπως στο AH. Το ίδιο ισχύει για τα πεδία Pad Length, Next Header και ICV (το οποίο είναι προαιρετικό) 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 ανλογιστούμε ότι κάποιοι αλγόριθμοι κρυπτογράφησης απαιτούν τα δεδομένα να είναι μήκους πολλαπλάσιου κάποιου συγκεκριμένου αριθμού bytes).



Σχήμα 10: Πεδία ενός ESP Header και Trailer

3.2.3. Καταστάσεις ή τρόποι (modes) λειτουργίας

Το IPSec παρέχει δυο καταστάσεις (ή τρόπους) λειτουργίας (που σημαίνει δύο τρόπους με τους οποίους μπορούν τα τοποθετηθούν οι κεφαλίδες AH και ESP): **ο τρόπος μεταφοράς (transport mode)** και **ο τρόπος διόδου (tunnel mode)**, όπως φαίνεται στο σχήμα 11.

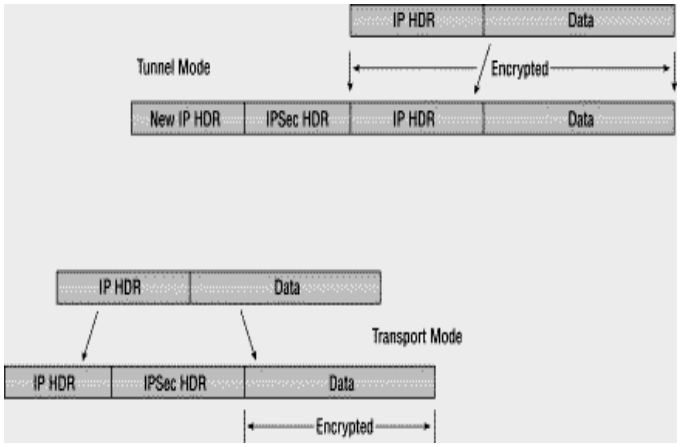


Σχήμα 11: Τρόπος καθορισμού ενός IPSec μετασχηματισμού (πρωτόκολλα-αλγόριθμοι-τρόποι υλοποίησης)

Στην κατάσταση λειτουργίας μεταφοράς (transport mode), οι αρχικές επικεφαλίδες του IP πακέτου μένουν ανέπαφες. Αυτή η κατάσταση λειτουργίας έχει το πλεονέκτημα της προσθήκης μόνο μερικών bytes σε κάθε πακέτο. Επιπλέον οι

συσκευές στο δημόσιο δίκτυο (όπως για παράδειγμα οι δρομολογητές) μπορούν να βλέπουν τον τελικό αποδέκτη του πακέτου, αφού οι IP διευθύνσεις μεταδίδονται ανέπαφες (μη κρυπτογραφημένες). Αυτή η δυνατότητα επιτρέπει ειδική επεξεργασία των πακέτων (για παράδειγμα δρομολόγηση με βάση την Ποιότητα Υπηρεσίας - QoS), βασισμένη στην πληροφορία που βρίσκεται στην IP επικεφαλίδα. Μειονέκτημα αυτού του τρόπου λειτουργία είναι το γεγονός ότι αφήνοντας την IP επικεφαλίδα χωρίς κρυπτογράφηση, ένας επιτιθέμενος μπορεί να κάνει ανάλυση κίνησης (traffic analysis). Για παράδειγμα, ο επιτιθέμενος θα μπορούσε να δει πότε ένας εργαζόμενος μίας εταιρίας έστειλε πολλά πακέτα σε έναν άλλο εργαζόμενο. Ωστόσο θα πρέπει να σημειωθεί ότι ο επιτιθέμενος θα γνώριζε μόνο την αποστολή των IP πακέτων και τίποτα άλλο: δεν θα ήταν στη θέση να καθορίσει αν π.χ. αυτά ήταν πακέτα e-mail ή κάποιας άλλης εφαρμογής.

Ο τρόπος λειτουργίας μεταφοράς χρησιμοποιείται κυρίως για διασύνδεση μεταξύ δύο LAN ή για εφαρμογές πελάτη-εξυπηρετητή (client-server). Στην ουσία, είναι ο τρόπος με τον οποίο δύο συσκευές του δικτύου (και όχι οι χρήστες) μπορούν να επικοινωνήσουν.



Σχήμα 12: Σύγκριση των πακέτων για τους δύο τρόπους λειτουργίας (tunnel και transport)

Στην κατάσταση λειτουργίας διόδου (tunnel mode), όλο το αρχικό IP πακέτο κρυπτογραφείται και γίνεται το φορτίο (payload) ενός καινούριου IP πακέτου. Αυτό σημαίνει ότι οι λειτουργίες κρυπτογράφησης, αυθεντικοποίησης κτλ. συντελούνται σε ολόκληρο το πακέτο, συμπεριλαμβανομένης και της αρχικής IP διεύθυνσης (βλέπε

σχήμα 12). Το καινούριο IP πακέτο που προκύπτει έχει μία νέα IP διεύθυνση (IPSec διεύθυνση). Αυτή η κατάσταση λειτουργίας επιτρέπει σε μια δικτυακή συσκευή, όπως ένας δρομολογητής, να ενεργήσει σαν ένας IPSec proxy. Αυτό σημαίνει ότι ο δρομολογητής είναι αυτός που πραγματοποιεί την κρυπτογράφηση για λογαριασμό των υπολογιστών του δικτύου: συγκεκριμένα, ο δρομολογητής-αποστολέας κρυπτογραφεί τα πακέτα και τα προωθεί στη IPSec δίοδο (tunnel). Ο αποδέκτης-δρομολογητής αποκρυπτογραφεί το αρχικό IP πακέτο και το προωθεί στον τελικό αποδέκτη. Το βασικό πλεονέκτημα λοιπόν είναι ότι τα ακραία συστήματα δεν χρειάζεται να έχουν απαραίτητες ρυθμίσεις έτσι ώστε να απολάβουν τα οφέλη από τη χρήση του IPSec. Με άλλα λόγια, το λειτουργικό σύστημα του χρήστη δεν χρειάζεται τροποποίηση. Άλλο πλεονέκτημα του τρόπου λειτουργίας διόδου είναι ότι προστατεύει το σύστημα από την διαδικασία της ανάλυσης κίνησης. Λόγω του ότι η αρχική IP διεύθυνση είναι «κρυμμένη», ο επιτιθέμενος μπορεί να προσδιορίσει μόνο τα ακραία σημεία του tunnel και όχι την πραγματική πηγή και τον προορισμό των πακέτων που κυκλοφορούν μέσα σε αυτό. Μειονέκτημα βέβαια είναι η μεγαλύτερη επεξεργασία πακέτων που απαιτείται.

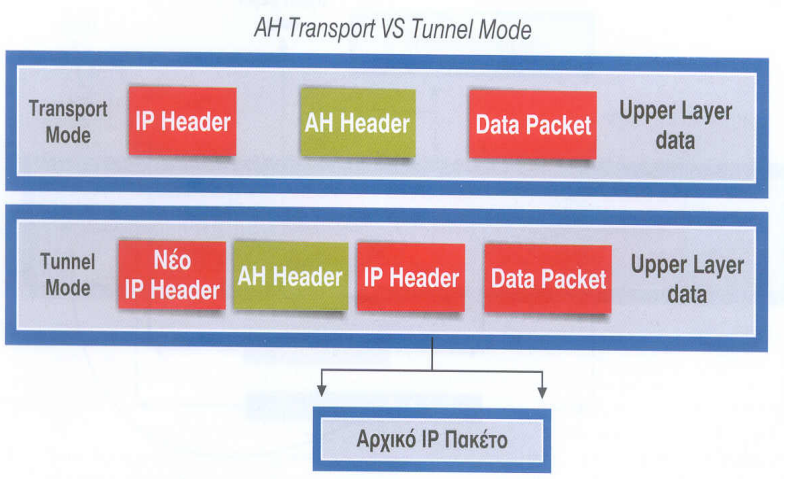
Η κατάσταση διόδου του IPSec αποτελεί τον πιο κοινό τρόπο λειτουργίας όσον αφορά τη σύνδεση μεταξύ δύο gateway συσκευών ή μια σύνδεση μεταξύ μιας gateway συσκευής και ενός τερματικού σταθμού. Ένα παράδειγμα αυτού του τρόπου υλοποίησης είναι ένας κινητός χρήστης που θέλει να συνδεθεί στο δίκτυο ενός οργανισμού για την απόκτηση πρόσβασης στο ηλεκτρονικό ταχυδρομείο ή σε διάφορα αρχεία κ.λ.π.

Ανάλογα με τον τρόπο υλοποίησης του IPSec (μεταφοράς ή διόδου) το τελικό IP πακέτο που δημιουργείται με την εφαρμογή της κεφαλίδας είτε της AH είτε της ESP, είναι διαφορετικό σε κάθε περίπτωση.

Στον *AH transport τρόπο υλοποίησης* οι υπηρεσίες ακεραιότητας και πιστοποίησης του AH πρωτοκόλλου προστατεύουν το αρχικό IP πακέτο. Η κεφαλίδα AH παρεμβάλλεται μετά από την αρχική IP κεφαλίδα και πριν από τα δεδομένα του IP πακέτου (που είναι τα περιεχόμενα των άνω στρωμάτων της στοίβας πρωτοκόλλου του μοντέλου OSI). Επειδή καμία κρυπτογράφηση δεν περιλαμβάνεται σε αυτό το

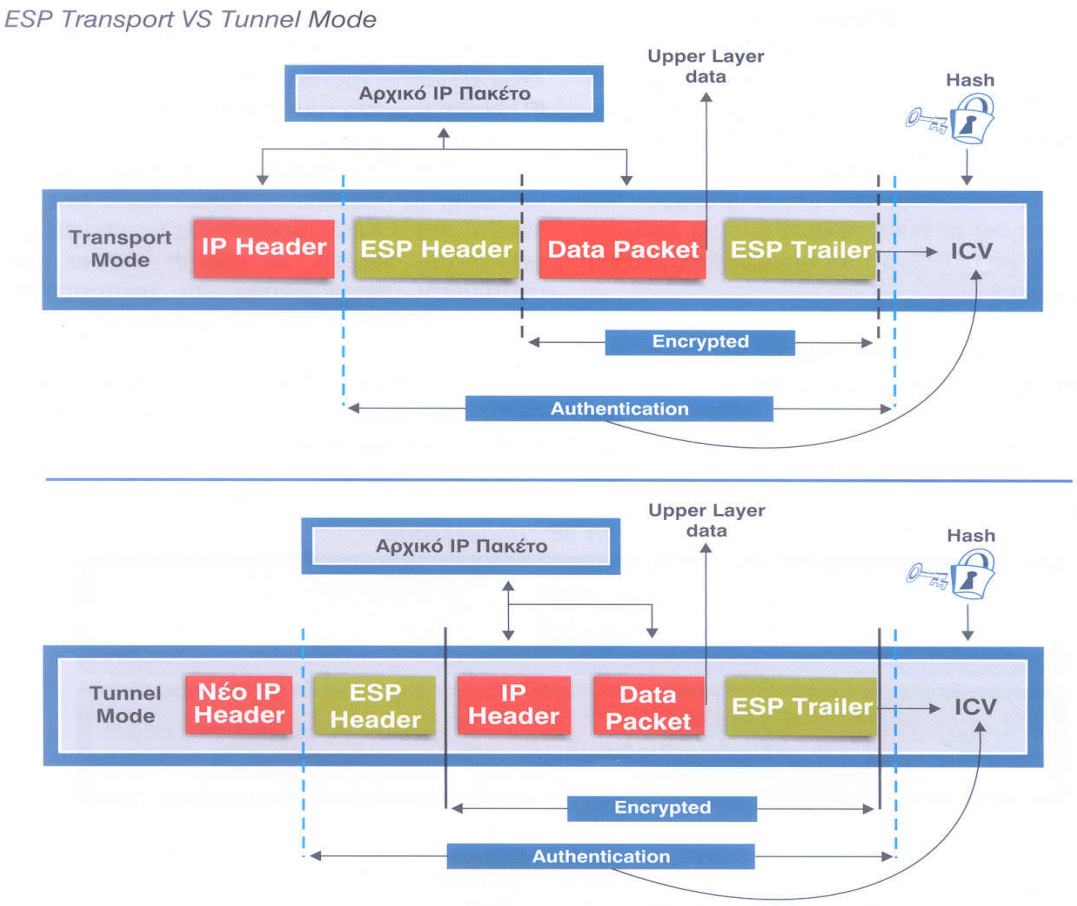
σημείο, η IP διεύθυνση προορισμού είναι αναγνώσιμη από οποιαδήποτε συσκευή του ανώτερου επιπέδου 3 - όπως π.χ. ένας δρομολογητής.

Στον *AH tunnel τρόπο υλοποίησης*, ολόκληρο το αρχικό IP πακέτο (κεφαλίδα και δεδομένα) γίνονται τα δεδομένα (φορτίο) για το νέο πακέτο. Μία νέα IP κεφαλίδα που περιλαμβάνει πληροφορίες για τα άκρα του tunneling (IP addresses) προστίθεται στο νέο πακέτο. Ολόκληρο το νέο πακέτο (νέο IP Header, AH Header, αρχικό IP Header, και αρχικό IP Payload) προστατεύεται από το πρωτόκολλο AH.



Σχήμα 13: Σύγκριση Transport και Tunnel τρόπων υλοποίησης του IPSec, όταν χρησιμοποιείται AH

Στον *ESP transport τρόπο υλοποίησης* το νέο ESP header τοποθετείται ανάμεσα στην καφαλίδα και τα δεδομένα του αρχικού πακέτου, ενώ το ESP trailer τοποθετείται μετά από τα δεδομένα του αρχικού IP πακέτου. Από την άλλη μεριά, στον *ESP tunnel τρόπο υλοποίησης* τα ESP header και trailer τοποθετούνται εκατέρωθεν του αρχικού IP πακέτου και επιπλέον προστίθεται ένα νέο IP header που περιλαμβάνει πληροφορίες για τα άκρα του tunneling (IP addresses).

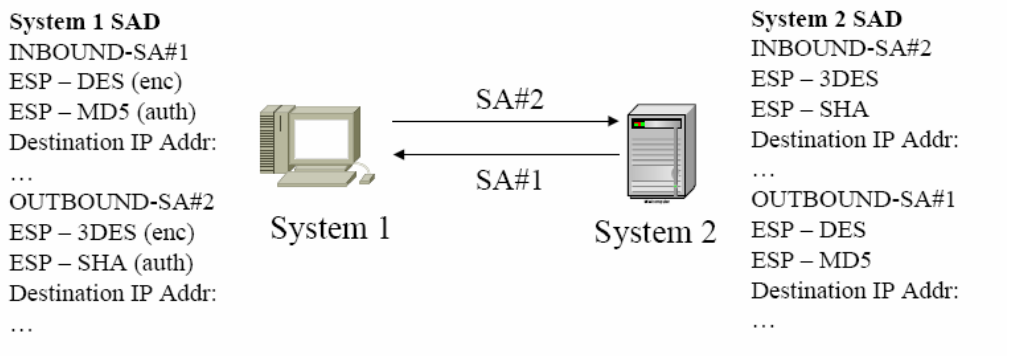


Σχήμα 14: Σύγκριση Transport και Tunnel τρόπων υλοποίησης του IPSec, όταν χρησιμοποιείται ESP

3.2.4. Συσχετίσεις Ασφάλειας

Το IPSec παρέχει πολλές επιλογές για την υλοποίηση κρυπτογράφησης και πιστοποίησης ταυτότητας στο δίκτυο. Κάθε IPSec σύνδεση μπορεί να παρέχει είτε κρυπτογράφηση (με ESP) είτε ακεραιότητα και πιστοποίηση ταυτότητας δεδομένων (με AH) ή και τα δύο (με ESP όπου υπάρχει και το αντίστοιχο πεδίο αυθεντικοποίησης των δεδομένων). Όταν η υπηρεσία ασφάλειας καθοριστεί, οι δυο επικοινωνούντες κόμβοι πρέπει να καθορίσουν ακριβώς ποιους αλγόριθμους θα χρησιμοποιήσουν (για παράδειγμα, AES ή 3DES για κρυπτογράφηση και MD5 ή SHA για ακεραιότητα δεδομένων). Αφού αποφασίσουν για τους αλγόριθμους οι δύο συσκευές πρέπει να μοιράσουν κλειδιά σύνδεσης. Η **συσχέτιση ασφάλειας** (**Security Association – SA**) είναι μια μέθοδος που χρησιμοποιείται από το IPSec για την παρακολούθηση όλων των λεπτομερειών που αφορούν μία δεδομένη IPSec επικοινωνία. Μια συσχέτιση ασφάλειας είναι η σχέση μεταξύ δυο ή περισσοτέρων

οντοτήτων που περιγράφει πως οι οντότητες θα χρησιμοποιήσουν τις υπηρεσίες ασφάλειας για να επικοινωνήσουν με ασφάλεια. Με άλλα λόγια, είναι η συμφωνία των δύο άκρων για τις παραμέτρους επικοινωνίας, όπως αλγόριθμοι κρυπτογράφησης και αυθεντικοποίησης, τρόπος ανταλλαγής κλειδιών, διάρκεια ισχύος τους κτλ.



Σχήμα 15: Συσχετίσεις Ασφάλειας IPSec

Οι συσχετίσεις ασφάλειας είναι μη κατευθυντικές που σημαίνει ότι για κάθε ζεύγος επικοινωνούντων συστημάτων υπάρχουν τουλάχιστον δυο συνδέσεις ασφάλειας—μια από το A στο B και μια από το B στο A (σχήμα 15). Η συσχέτιση ασφάλειας αναγνωρίζεται από έναν τυχαίως επιλεγμένο μοναδικό αριθμό ο οποίος λέγεται Δείκτης παραμέτρων ασφαλείας (*SPI - Security Parameter Index)* και από την *IP διεύθυνση του προορισμού*. Όταν μία συσκευή στέλνει ένα πακέτο το οποίο απαιτεί IPSec προστασία κοιτάει τη συσχέτιση ασφάλειας στη βάση δεδομένων του, εφαρμόζει τη συγκεκριμένη επεξεργασία και μετά εισάγει τον SPI από τη συσχέτιση ασφάλειας στην IPSec επικεφαλίδα. Όταν το αντίστοιχο μηχάνημα IPSec λαμβάνει το πακέτο κοιτάει με τη σειρά του τη συσχέτιση ασφάλειας στη βάση δεδομένων του (βάσει της διεύθυνσης προορισμού και του SPI) και μετά επεξεργάζεται το πακέτο όπως ορίζεται. Με λίγα λόγια, η συσχέτιση ασφάλειας είναι απλώς μια δήλωση της διαπραγματεύσιμης πολιτικής ασφάλειας μεταξύ δυο συσκευών.

Οι κύριες παράμετροι που προσδιορίζονται σε μία συσχέτιση ασφαλείας είναι:

- IP διεύθυνση πηγής και προορισμού
- Ένα ID χρήστη
- Πρωτόκολλο μεταφοράς (TCP ή UDP)

- Τον αλγόριθμο για έλεγχο πιστοποίησης ταυτότητας, καθώς και τα αντίστοιχα κλειδιά
- Τον αλγόριθμο που χρησιμοποιείται για κρυπτογράφηση, καθώς και τα κλειδιά
- Τρόπος λειτουργίας του IPSec (transfer ή tunnel mode)
- Διάρκεια ζωής μιας SA

3.2.5. Πρωτόκολλο Διαχείρισης Κλειδιών

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 (επέκταση του προϋπάρχοντος ISAKMP/Oakley πρωτοκόλλου) δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι (tunnel) μεταξύ δύο οντοτήτων και κατόπιν διαπραγματεύεται τις συσχετίσεις ασφάλειας για το IPSec. Αυτή η διαδικασία απαιτεί από τις δύο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν κλειδιά. Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω 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 κατακερματισμο) 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, αποκρυπτογραφώντας με τα ιδιωτικά κλειδιά (private keys) ό,τι λαμβάνουν από το συνομιλητή τους. Υποστηρίζεται μόνο ο 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 public key 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, αν και μπορεί να υπάρξουν και άλλοι.

Diffie-Hellman: Μηχανισμός ανταλλαγής κλειδιών που αναπτύχθηκε από τους Diffie και Hellman το 1976. Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές κανάλι. Είναι ένας κρυπτογραφικός αλγόριθμος δημοσίου κλειδιού. Το πρωτόκολλο έχει δύο παραμέτρους (αριθμούς): p και g. Το p είναι ένας πολύ μεγάλος πρώτος αριθμός και το g είναι ένας αριθμός με την ιδιότητα $g^k \neq 1 \bmod p$ για όλους τους k από 1 μέχρι p-2 (δηλαδή, στοιχείο-γεννήτορας (generator) στο σώμα των ακεραίων Modulo p). Τα p,g τα γνωρίζουν όλοι – είναι δημοσίως γνωστά. Ας υποθέσουμε τώρα ότι δύο χρήστες, ο A και ο B, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο A παράγει μία τυχαία τιμή x και ο B μία τυχαία τιμή y (όπου τα x,y είναι μικρότερα του p). Τα x,y κρατούνται μυστικά – μόνο ο A δηλαδή γνωρίζει το x και μόνο ο B το y. Στη συνέχεια ο A υπολογίζει τον αριθμό $x' = g^x \ mod \ p$ και ο B τον αριθμό $y' = g^y \ mod \ p$. Κατόπιν, ο ένας στέλνει στον άλλον τις τιμές αυτές. Τέλος, ο A κάνει τον υπολογισμό $(y')^x = g^{xy} \ mod \ p$ και ο B κάνει με την σειρά του τον υπολογισμό $(x')^y = g^{xy} \ mod \ p$. Συνεπώς και οι δύο υπολογίζουν τον ίδιο αριθμό – ο οποίος θα είναι το μυστικό κλειδί που θα χρησιμοποιήσουν. Η ασφάλεια του πρωτοκόλλου αυτού βασίζεται στο γεγονός ότι ένας επιτιθέμενος, ο οποίος παρακολουθεί το τι ανταλλάσσουν οι A και B, δεν μπορεί από τα x', y' να υπολογίσει το μυστικό κλειδί: για να το κάνει αυτό θα πρέπει να ξέρει είτε το x είτε το y. Όμως, όταν τα p και g είναι πολύ μεγάλα, το να ξέρει κανείς το x' ή το y' δεν του αρκεί για να βρει το x ή το y.

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 (σχήμα 16):

- **Ενεργοποίηση μιας IPSec συνόδου**. Στο βήμα αυτό καθορίζεται το σύνολο των IP πακέτων που πρόκειται να προστατευθούν μέσω του IPSec.

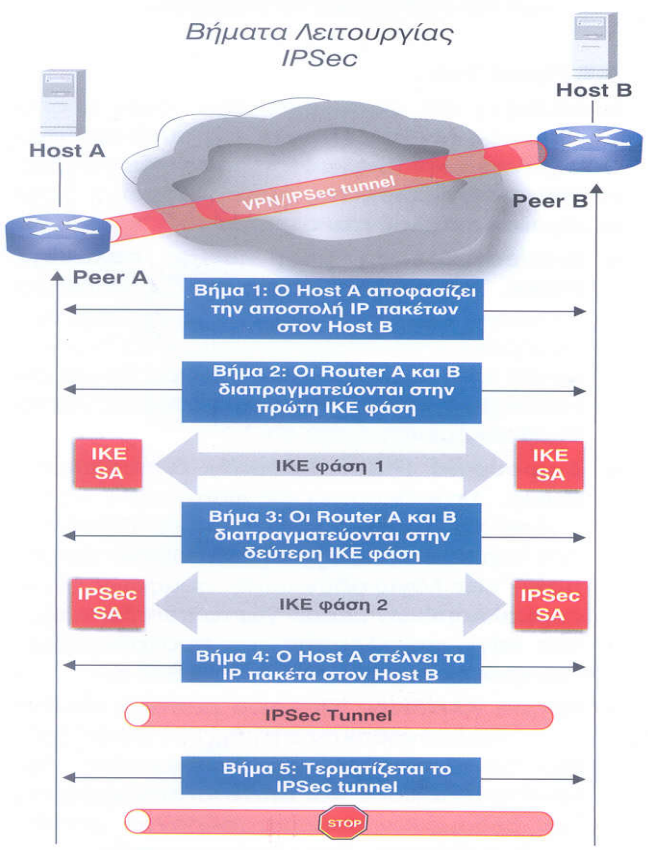
- **IKE - Πρώτη φάση**. Δημιουργία και λειτουργία της IKE Συσχέτισης Ασφαλείας.

- **IKE – Δεύτερη φάση**. Δημιουργία και λειτουργία της AH/ESP Συσχέτισης Ασφαλείας

- **Μεταφορά Δεδομένων**. Τα IP πακέτα που επιλέχθηκαν από το πρώτο βήμα μεταφέρονται.

- **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 SAs 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.

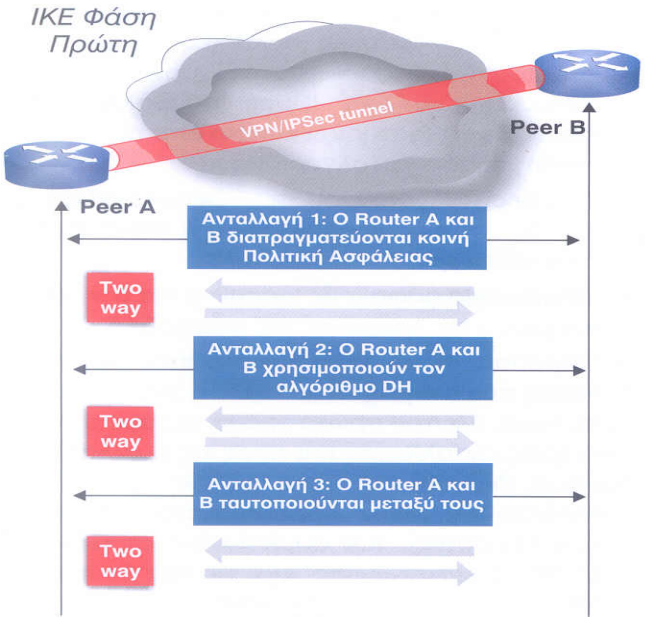


Σχήμα 16: Σύνολο βημάτων που πρέπει να πραγματοποιηθούν για την επιτυχή μετάδοση δεδομένων μέσω του IPSec πρωτοκόλλου

Οι κυριότερες λειτουργίες που συναντάμε στη πρώτη φάση του IKE είναι οι εξής:

- Πιστοποίηση των μελών που συμμετέχουν σε μια IPSec επικοινωνία.
- Ανάπτυξη μιας ή περισσότερων πολιτικών ασφάλειας IKE βασισμένες στη γενική πολιτική ασφάλειας ενός οργανισμού. Κάθε πολιτική απαιτεί την λήψη αποφάσεων για πέντε βασικές επιλογές ασφάλειας: *μέθοδος πιστοποίησης*, *αλγόριθμος κρυπτογράφησης*, *αλγόριθμος κατακερματισμού (για έλεγχο της ακεραιότητας δεδομένων)*, παράμετροι του *Diffie - Hellman αλγορίθμου (που προσδιορίζει το μέγεθος κλειδιού) και διάρκεια ζωής μίας SA*. Οι διαφορετικές πολιτικές μπορεί να απαιτούνται παραδείγματος χάριν στη περίπτωση που ένα IPSec συμβαλλόμενο μέρος δεν υποστηρίζει κάποια από τις παραπάνω μεθόδους ή αλγόριθμους.
- Εκτέλεση αλγόριθμου Diffie-Hellman για την δημιουργία ενός ή περισσοτέρων κοινών μυστικών κλειδιών.
- Δημιουργία ασφαλούς «διόδου» (tunneling) για την ολοκλήρωση της επόμενης (δεύτερης) IKE φάσης.

Η πρώτη φάση του IKE μπορεί να πραγματοποιηθεί με δυο τρόπους: είτε τον κύριο τρόπο (main) είτε τον επιθετικό (aggressive). Με τον πρώτο τρόπο έχουμε συνολικά τρεις ανταλλαγές μηνυμάτων και προς τις δυο κατευθύνσεις μεταξύ των συμβαλλόμενων μερών μιας IPSec επικοινωνίας (σχήμα 17), ενώ με τον δεύτερο τρόπο οι παραπάνω ανταλλαγές συμπτύσσονται σε μια μόνο ανταλλαγή με τρία στάδια (αποστολέας - δέκτης, δέκτης - αποστολέας, αποστολέας - δέκτης).



Σχήμα 17: Με ένα σύνολο τριών ανταλλαγών η πρώτη IKE φάση δημιουργεί ένα ασφαλές tunnel και ταυτοποιεί τα συμβαλλόμενα μέλη του

Οι ανταλλαγές μηνυμάτων που λαμβάνουν χώρα στην πρώτη φάση του IKE είναι οι εξής:

Πρώτη Ανταλλαγή. Σε αυτή καθορίζονται οι αλγόριθμοι ασφάλειας (κρυπτογράφησης) και πιστοποίησης ταυτότητας οι οποίοι πρόκειται να χρησιμοποιηθούν στα επόμενα βήματα. Για κάθε μια κατεύθυνση μία ξεχωριστή Συσχέτιση Ασφαλείας (SA) δημιουργείται με πληροφορίες που περιλαμβάνουν τους αλγόριθμους κρυπτογράφησης και πιστοποίησης που υποστηρίζονται από το κάθε άκρο της συνομιλίας, τον αλγόριθμο παραγωγής κοινού μυστικού κλειδιού (συμφωνία αρχικών παραμέτρων του Diffie-Hellman αλγορίθμου), τον χρόνο διάρκειας της πρώτης IKE φάσης, τον τρόπο πιστοποίησης που θα χρησιμοποιηθεί (π.χ. προμοιρασμένα κλειδιά) κ.ο.κ. Στο τέλος της παραπάνω διαδικασίας καθένας από τα IPSec «συνομιλούντες» διαθέτει μία κοινή IKE SA.

Δεύτερη Ανταλλαγή. Εφόσον επέλθει συμφωνία με τις προτεινόμενες παραμέτρους, εκτελείται ο αλγόριθμος παραγωγής κοινού μυστικού κλειδιού (Diffie-Hellman) μέσω του οποίου παράγεται ένα κλειδί που είναι κοινό και στα δύο μέρη. Ο εν λόγω αλγόριθμος είναι κρίσιμος στις διαδικασίες που αφορούν το IPSec πρωτόκολλο επειδή το κοινό μυστικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα χρησιμοποιώντας τους βασικούς αλγορίθμους κρυπτογράφησης που διευκρινίζονται στα IPSec SA (π.χ. στον DES).

Τρίτη Ανταλλαγή. Κάθε συμβαλλόμενο μέρος ταυτοποιεί το άλλο με χρήση των κατάλληλων αλγόριθμων (που έχουν οριστεί νωρίτερα).

Η **δεύτερη φάση IKE** πραγματοποιείται αμέσως μετά την ολοκλήρωση της πρώτης φάσης. Στην φάση αυτή εκτελούνται τα εξής:

- **Διαπραγμάτευση μιας κοινής πολιτικής IPSec**. Καθορίζονται οι τρόποι χρήσης των αλγόριθμων κρυπτογράφησης (π.χ. αν θα είναι τρόπος μεταφοράς (transport mode) ή διόδου (tunnel mode), αν θα χρησιμοποιηθεί AH ή ESP κ.ο.κ.)

- **Δημιουργία IPSec Συσχέτισης Ασφαλείας).** Στην δεύτερη IKE φάση κάθε στιγμή μπορεί να δημιουργηθεί ένα νέο IPSec SA στη περίπτωση που το προηγούμενο τερματιστεί, είτε λόγω αδυναμίας συμφωνίας των συμβαλλομένων μερών για τις παραμέτρους επικοινωνίας είτε λόγω παρέλευσης του προκαθορισμένου χρόνου λειτουργίας ενός IPSec SA.

- **Χρήση Κλειδιών**. Τα κοινά μυστικά κλειδιά που δημιουργήθηκαν στη πρώτη φάση χρησιμοποιούνται για τις λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων που μεταφέρονται μεταξύ των δύο IPSec συμβαλλομένων μερών.

3.2.6. Εφαρμογές

Το IPSec είναι ένα standard πρωτόκολλο για την υλοποίηση κρυπτογραφικών μηχανισμών σε δρομολογητές, τοίχους ασφαλείας (firewalls), αλλά και σε LANs ή μεμονωμένους κόμβους (hosts) που επικοινωνούν μέσω του Internet. Πιο συγκεκριμένα, υποστηρίζει την ασφαλή επικοινωνία μεταξύ δύο κόμβων, όπως επίσης και μεταξύ δύο LANs, εκτός από την client/server επικοινωνία που υποστηρίζουν τα άλλα πρωτόκολλα.

Επιπλέον, το IPSec είναι χρήσιμο για τη διασφάλιση της απομακρυσμένης πρόσβασης (μέσω dial-up) διασυνδέσεων VPN με απομακρυσμένα σημεία εντός εταιρικών ιδιωτικών δικτύων.

Γενικά, το IPSec χρησιμοποιείται για να προσφέρει τη μέγιστη δυνατή ασφάλεια σε περιπτώσεις χρηματοπιστωτικών ιδρυμάτων, χρηματιστηριακών εταιριών, και γενικά οπουδήποτε η μεταφερόμενη πληροφορία είναι ιδιαίτερα ευαίσθητη. Επιπλέον προσφέρει εκτός της κρυπτογράφησης, πιστοποίηση της ταυτότητας των μερών που λαμβάνουν μέρος σε ένα VPN (είτε πρόκειται για τοπικά δίκτυα, είτε για μεμονωμένους χρήστες), πιστότητα στη μετάδοση των δεδομένων, και προστασία των τοπικών δικτύων από κακόβουλες επιθέσεις. Με τον τρόπο που διαμορφώνονται σήμερα οι σύγχρονες επιχειρήσεις και με τις συνθήκες που απαιτούνται για την ασφαλή μετάδοση των πληροφοριών, είναι κατανοητό για ποιο λόγο οι τελευταίες

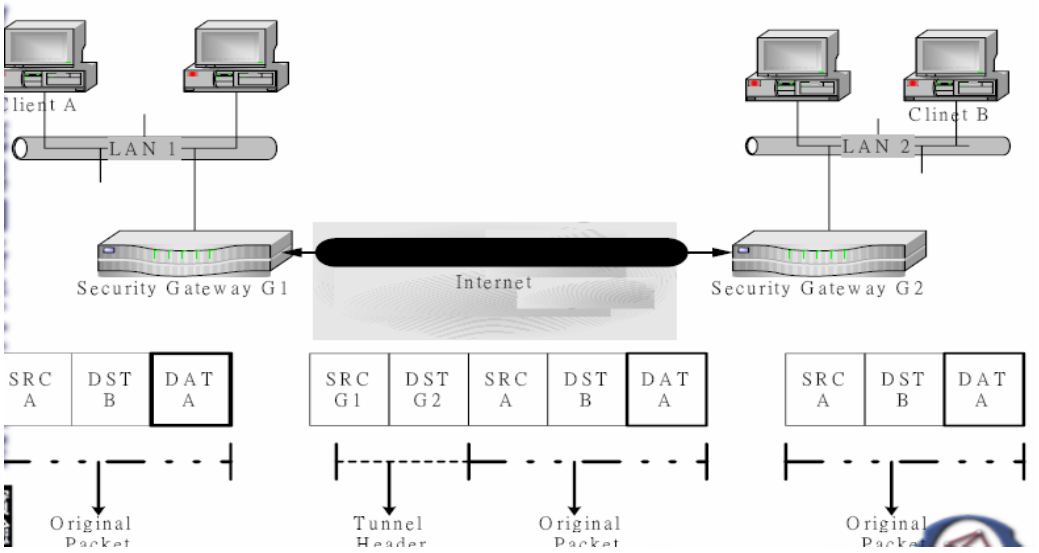
καταφεύγουν σε υλοποιήσεις όπως η IPSec τεχνολογία (και τα πρωτόκολλα που τη συνοδεύουν) προκειμένου να πετύχουν το στόχο τους. Αυτός δεν είναι τίποτα άλλο παρά η διασφάλιση της ακεραιότητας, πιστοποίησης και εμπιστευτικότητας των πληροφοριών που μεταδίδονται σήμερα ανά τον κόσμο σε ένα μεγάλο αριθμό δκτυών, είτε αυτά είναι εσωτερικά ενός οργανισμού είτε όχι. Η τεχνολογία IPSec στα VPN δίκτυα, έχει γίνει ευρέως αποδεκτή και αποδεικνύεται ιδιαίτερα επιτυχημένη, αφού αποτελεί μία από τις κυριότερες ασπίδες προστασίας των δεδομένων που μεταδίδονται σήμερα στο διαδίκτυο.

Προβλήματα που καλείται να αντιμετωπίσει το IPSec είναι η αύξηση του μεγέθους των πακετών (που σημαίνει μεγαλύτερος χρόνος επεξεργασίας τους), η μη δυνατότητα καθορισμού συγκεκριμένων καθολικών αλγορίθμων κρυπτογράφησης (λόγω νομοθετικών δυσκολιών που αντιμετωπίζουν πολλοί αλγόριθμοι και σε διάφορες χώρες), καθώς και το γεγονός ότι εφαρμόζεται μόνο σε IP δίκτυα (που σημαίνει ότι σε κάποια υπάρχοντα ιδιωτικά δίκτυα δεν μπορεί να εφαρμοστεί).

4. Εικονικά Ιδιωτικά Δίκτυα Επιπέδου Ζεύξης Δεδομένων

Τα Εικονικά Ιδιωτικά Δίκτυα με πρωτόκολλα επιπέδου 2 αναπτύχθηκαν κυρίως ως Δίκτυα Απομακρυσμένης Πρόσβασης: με άλλα λόγια, επιτρέπουν σε έναν απομακρυσμένο χρήστη να συνδεθεί μέσω μίας Internet γραμμής (π.χ. μέσω dial-up σύνδεσης) στο εσωτερικό δίκτυο μίας εταιρίας. Οι δίοδοι (tunnels) μπορούν να δημιουργηθούν είτε ανάμεσα σε ένα ζεύγος δρομολογητών (router-to-router) είτε μεταξύ δύο τερματικών κόμβων (host-to-host). Η εγκαθίδρυση διόδου μπορεί να υλοποιείται σε μία τοπολογία σημείου-προς-σημείο ή σημείου-προς-πολλά σημεία: η σημείου-προς-σημείου έχει λιγότερο διαχειριστικό φορτίο, από την άποψη της εγκαθίδρυσης και της συντήρησης.

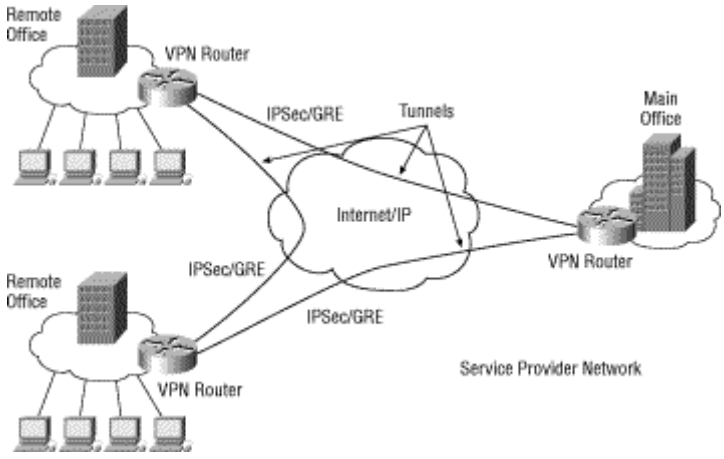
Η εγκαθίδρυση «διόδου» (tunneling) είναι η τεχνική ενθυλάκωσης ενός ολόκληρου πακέτου/πλαισίου δεδομένων σε ένα πακέτο/πλαίσιο διαφορετικού πρωτοκόλλου. Η επικεφαλίδα του tunneling πρωτοκόλλου προσαρτάται στο αρχικό πακέτο ενώ η μεταφορά/μετάδοση πραγματοποιείται με χρήση του νέου πρωτοκόλλου. Έτσι, όταν ένα τέτοιο πακέτο δρομολογείται προς τον κόμβο προορισμού, διατρέχει το δίκτυο μέσα από λογικό μονοπάτι, το οποίο αναφέρεται ως δίοδος (tunnel). Όταν ο κόμβος προορισμού λάβει το πακέτο, το μετατρέπει στην αρχική του μορφή. Σημειώνεται ότι η τεχνολογία tunneling μπορεί να αναπτυχθεί στο δεύτερο ή στο τρίτο επίπεδο του μοντέλου OSI.



Σχήμα 18: Ενθυλάκωση πακέτου σε νέο, για τη δημιουργία διόδου (tunnel)

Ένα από τα πλεονεκτήματα του tunneling είναι ότι τα διασυνδεδεμένα υποδίκτυα VPN δεν απαιτούν μοναδικές διευθύνσεις δικτύου. Αυτό είναι σημαντικό όταν η πλειοψηφία των οργανισμών σήμερα χρησιμοποιεί ιδιωτικές διευθύνσεις. Επίσης ένα VPN με τη χρήση του tunneling μπορεί να δημιουργηθεί με ή χωρίς τη γνώση του παρόχου δικτύου και θα μπορούσε να «περάσει» μέσα από διαδοχικούς παρόχους δικτύου.

Ο μηχανισμός της Cisco GRE (Generic Routing Encapsulation) χρησιμοποιείται για tunneling ανάμεσα σε δρομολογητές πηγής και προορισμού (router-to-router). Τα GRE tunnels παρέχουν ένα ειδικό μονοπάτι κατά μήκος μίας διαμοιραζόμενης υποδομής WAN που δεν ανήκει μόνο σε έναν χρήστη-πελάτη (π.χ. Internet) και ενθυλακώνουν την κίνηση με νέες επικεφαλίδες πακέτου για να εξασφαλίσουν τη διανομή σε ένα συγκεκριμένο προορισμό. Ένα GRE tunnel διαμορφώνεται ανάμεσα στο δρομολογητή πηγής και το δρομολογητή προορισμού. Τα πακέτα που πρόκεται να προωθηθούν κατα μήκος της διόδου ενθυλακώνονται με μία επικεφαλίδα GRE, μεταφέρονται κατα μήκος της διόδου και στο τέλος της αφαιρείται η επικεφαλίδα GRE.



Σχήμα 19: Υλοποίηση tunneling

Υπάρχουν τρία πρωτόκολλα επιπέδου 2: το πρωτόκολλο IETF Layer 2 Tunneling Protocol (L2TP), το πρωτόκολλο της Microsoft Point-to-Point Tunneling Protocol (PPTP) και το πρωτόκολλο της Cisco Layer 2 Forwarding Protocol (L2F). Τα δύο τελευταία αναπτύχθηκαν ανεξάρτητα, ωστόσο σύντομα γεννήθηκε η ανάγκη ύπαρξης ενός μόνο πρωτοκόλλου το οποίο να υιοθετείται από όλους (να αποτελεί πρότυπο

(standard) δηλαδή) και να συσχετίζει χαρακτηριστικά και από τα δύο προϋπάρχοντα. Έτσι, δημιουργήθηκε το L2TP.

4.1. Πρωτόκολλο L2F

Λόγω της μεγάλης ανάπτυξης των dial-up υπηρεσιών και την παροχή πολλών διαφορετικών πρωτοκόλλων χρειαζόταν ένας τρόπος για να δημιουργείται μία εικονική dial-up σύνδεση, όπου οποιοδήποτε από τα μη-IP πρωτόκολλα να μπορεί να χρησιμοποιεί τα πλεονεκτήματα που παρέχει το Internet. Μέσω του L2F, οι χρήστες έχουν τη δυνατότητα να κάνουν μία PPP (Point to Point) σύνδεση σε ένα dial-up πάροχο υπηρεσιών και, εν συνεχεία, να συνδεθούν στα υπολογιστικά συστήματα της εταιρίας τους. Το L2F έχει δικούς του μηχανισμούς για την ενθυλάκωση των πακέτων και δεν χρησιμοποιεί το GRE.
Ορισμένα από τα οφέλη που προσέφερε το L2F είναι :

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

Σε μία τυπική εγκατάσταση ο χρήστης κάνει μία PPP ή άλλη παρόμοια σύνδεση στον ISP και κατά την διάρκεια της αίτησης, ο NAS (Network Access Server), χρησιμοποιώντας το λογισμικό του L2F, αρχικοποιεί μία δίοδο προς τον προορισμό του χρήστη. Στη συνέχεια, ο προορισμός απαιτεί το password του χρήστη και αφού γίνει η πιστοποίηση ταυτότητας, παραχωρείται στο χρήστη η IP διεύθυνση σαν μία τυπική dial-up απομακρυσμένη πρόσβαση. Στην ουσία, η πιστοποίηση ταυτότητας γίνεται σε δύο επίπεδα: μία αρχικά από τον ISP (Internet Service Provider) στον οποίο συνδέεται ο χρήστης και μία μετέπειτα από την πύλη (gateway) που υπάρχει στο απομακρυσμένο δίκτυο που συνδέεται ο χρήστης.

4.2. Πρωτόκολλο PPTP

Το **PPTP** είναι ένας συνδυασμός του Point-to-Point Protocol (PPP) και του Transmission Control Protocol / Internet Protocol (TCP/IP). Αναπτύχθηκε από τις

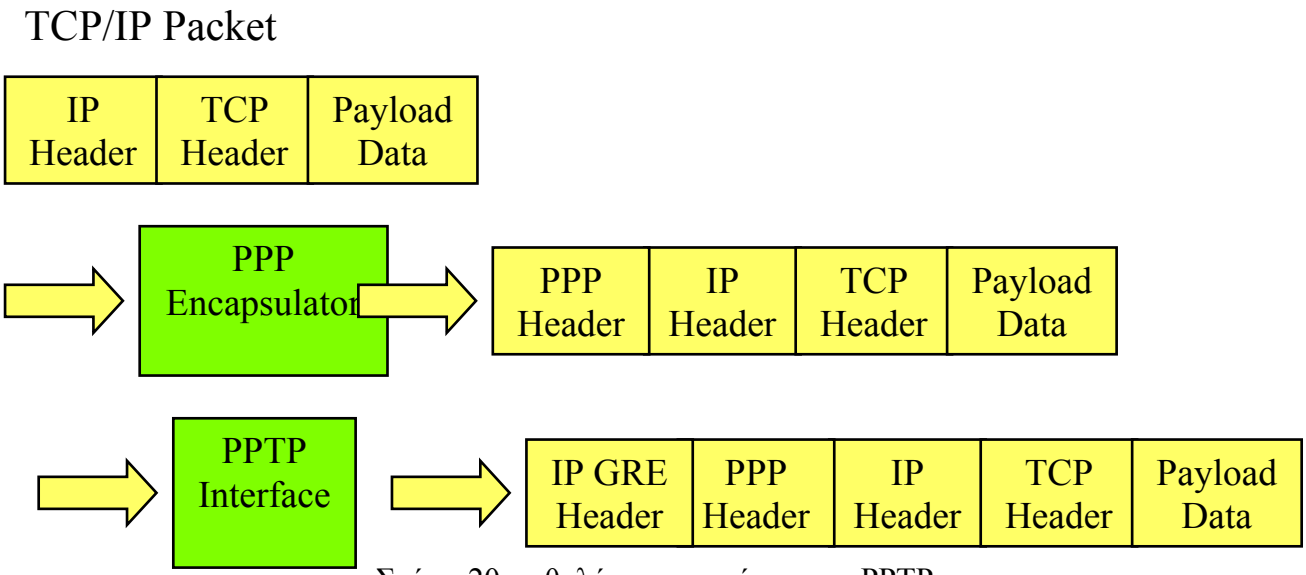
εταιρίες 3Com, Ascend Communications, Microsoft, ECI Telematics και US Robotics. Αναπτύχθηκε και λειτούργησε παράλληλα με το L2F της Cisco. Το PPTP συνδυάζει τα χαρακτηριστικά του PPP (π.χ εμπιστευτικότητα με ταυτόχρονη συμπίεση των πακέτων δεδομένων) και του TCP/IP (κυρίως τη δυνατότητα για δρομολόγηση 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 Protocol (GRE) για μεταφορά των PPP πακέτων. Πραγματοποιεί επίσης κρυπτογράφηση για τα ενθυλακωμένα δεδομένα.

Δύο 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 την διαδικασία της ενθυλάκωσης χρησιμοποιώντας το GRE v2.

Το PPTP λειτουργεί ως εξής: 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 ενθυλαώνονται κατάλληλα σε μεγαλύτερα πακέτα, με στόχο τη μετάδοση δεδομενων μέσω μιας διόδου. Στην ουσία δημιουργούνται IP πακέτα, με χρήση του πρωτοκόλλου ενθυλάκωσης GRE (σχήμα 20).



Σχήμα 20: ενθυλάκωση πακέτων στο PPTP

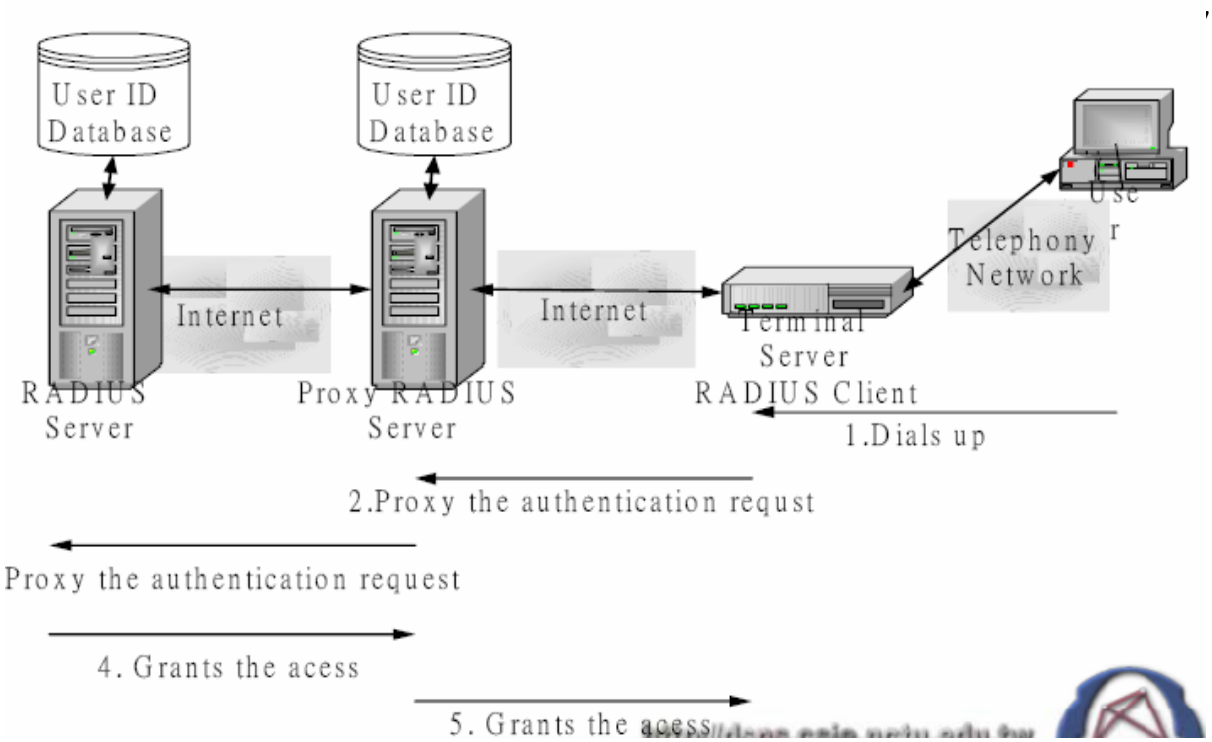
Οι συσκευές στον ISP που είναι υπεύθυνες για λειτουργίες του πρωτοκόλλου PPTP ονομάζονται είτε Remote Access Servers (RAS) είτε Network Access Servers (NAS) (το όνομα διαφοροποιείται ανάλογα με τον ακριβή ρόλο που έχει η συσκευή καθόλη τη διάρκεια υλοποίησης του πρωτοκόλλου). Πρακτικά, ένας NAS ή RAS 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 αυθεντικοποίηση. Ο RAS αυθεντικοποιεί τον χρήστη κυρίως με το πρωτόκολλο RADIUS (και σπανιότερα με το TACACS, το οποίο δεν θα αναλυθεί εδώ).

Το πρωτόκολλο RADIUS έχει τη δομή μοντέλου «πελάτη-εξυπηρετητή» (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 δεδομένων 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 servers, 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 αυθεντικοποιούν το χρήστη (σχήμα 21).

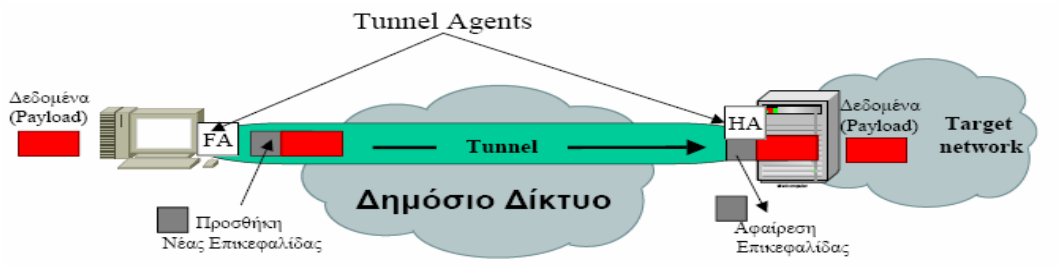
Στο PPTP, οι ζεύξεις επικοινωνίας υλοποιούνται πάνω σε διόδους (tunnels) (σχήμα 22). Οι δυνατότητες του υπολογιστή του χρήστη καθορίζουν το άκρο της διόδου: αν ο υπολογιστής έχει PPTP software, τότε αυτός είναι το άκρο της διόδου. Διαφορετικά, αν υποστηρίζει μόνο PPP και όχι PPTP, τότε το άκρο της διόδου βρίσκεται στον ISP και συγκεκριμένα στον RAS.



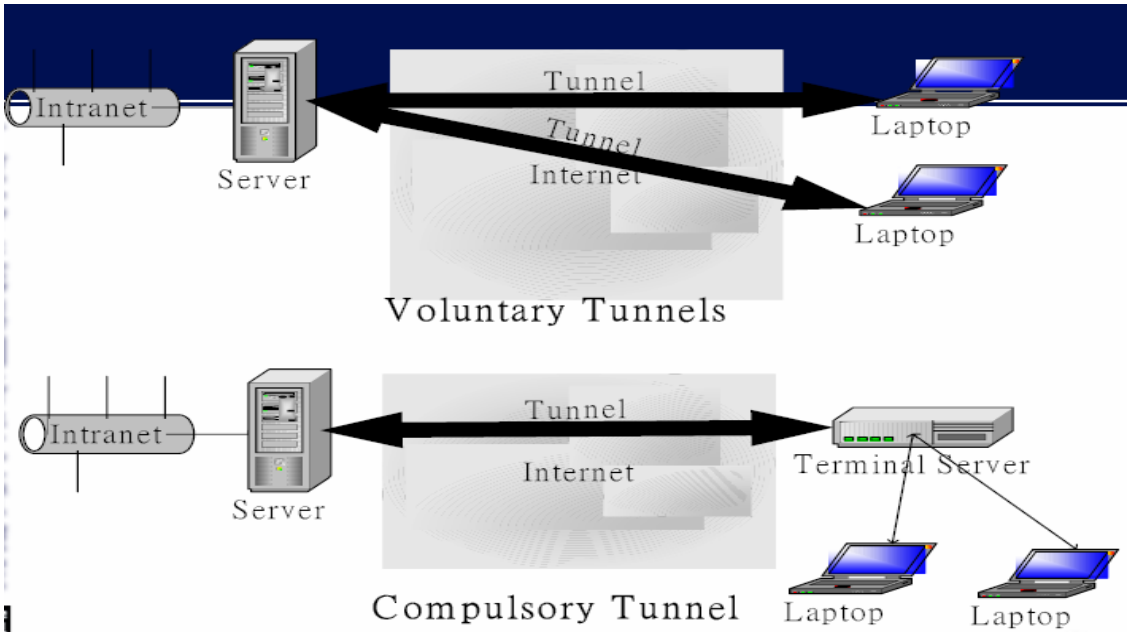
Σχήμα 21: Λειτουργία του RADIUS με Proxy Server

Υπάρχουν δύο ειδών δίοδοι: οι **«αυθόρμητες» δίοδοι (mandatory tunnels)** και οι **«αναγκαστικές» δίοδοι (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 μπορούν πολλαπλές συνδέσεις να υπάρχουν πάνω σε μία δίοδο. 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 (αφού δεν πραγματοποιούνται οι μηχανισμοί κρυπτογράφησης που η δίοδος επιβάλλει). Γενικά, οι αυθόρμητες δίοδοι προσφέρουν μεγαλύτερη ασφάλεια.



Σχήμα 22: Εγκαθίδρυση διόδου (tunnel)



Σχήμα 23: Σχηματική αναπαράσταση των δύο ειδών διόδων (αυθόρμητες και αναγκαστικές)

Οι αναγκαστικές δίοδοι χωρίζονται σε δύο υποκατηγορίες:

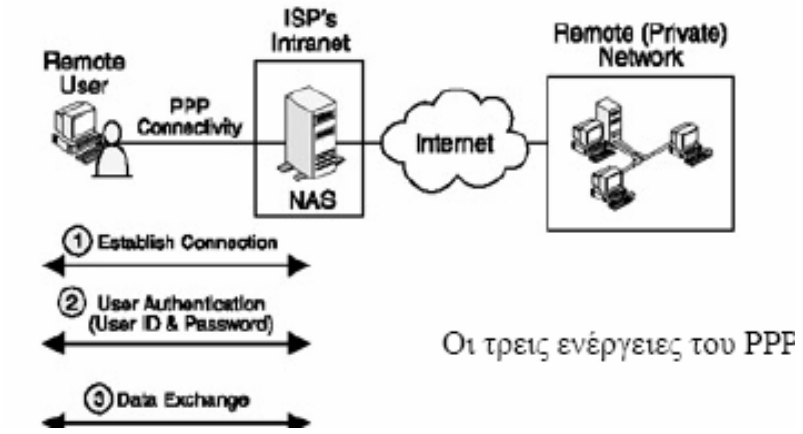
- Στατικές αναγκαστικές δίοδοι (static compulsory tunnels):
  - *Realm-based*: ο RAS ελέγχει ένα τμήμα του ονόματος του χρήστη, τον *τομέα (realm)* και με βάση αυτό αποφασίζει τη δρομολόγηση της διόδου αυτού του χρήστη. Σε αυτές τις διόδους, όλοι οι χρήστες του ίδιου τομέα (π.χ. του ίδιου γραφείου) αντιμετωπίζονται με τον ίδιο τρόπο – δηλαδή, οι δίοδοι που δημιουργούνται προσφέρουν σε όλους την ίδια ποιότητα υπηρεσίας. Αυτό μειώνει την «ευλυγισία» του συστήματος.
  - *Automatic:* Υπάρχει προεγκατεστημένος 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.

- 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.

Τα PPTP VPNs μπορούν να υποστηρίξουν όλα τα παραπάνω είδη διόδων.
Η όλη λειτουργία του PPTP πραγματοποιείται σε τρεις φάσεις:

- Πρώτη φάση: Εδώ το πρωτόκολλο χρησιμοποιεί το γνωστό πρωτόκολλο PPP για τη σύνδεση του χρήστη με τον ISP (σχήμα 24).
- Δεύτερη φάση: Ανταλλάσσονται μηνύματα ελέγχου μεταξύ PPTP client και PPTP Server (RAS) για τη διατήρηση αλλά και τον τερματισμό (στο τέλος) της διόδου. Τα μηνύματα αυτά ανταλλάσσονται με βάση τις IP διευθύνσεις τους, στην 1723 TCP θύρα του RAS. Τα PPTP μηνύματα ελέγχου ενθυλακώνονται σε TCP/IP πακέτα.
- 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 χρήστη (αφού το password το έχει, εκτός βέβαια από τον ίδιο το χρήστη, και το δίκτυο λόγω του RADIUS Server, δεν χρειάζεται ανταλλαγή κλειδιού). Η κρυπτογράφηση ξεκινά από τον υπολογιστή του χρήστη – κάτι που προσδίδει μεγαλύτερη ασφάλεια. (Η Microsoft έχει προτείνει και υλοποιήσει ένα σύστημα κρυπτογράφησης και αυθεντικοποίησης που ονομάζεται Microsoft Point-to-Point Encryption (MPPE): η κρυπτογράφηση σε αυτό γίνεται με RC4, ενώ η πιστοποίηση ταυτότητας με το πρωτόκολλο MS-CHAP.

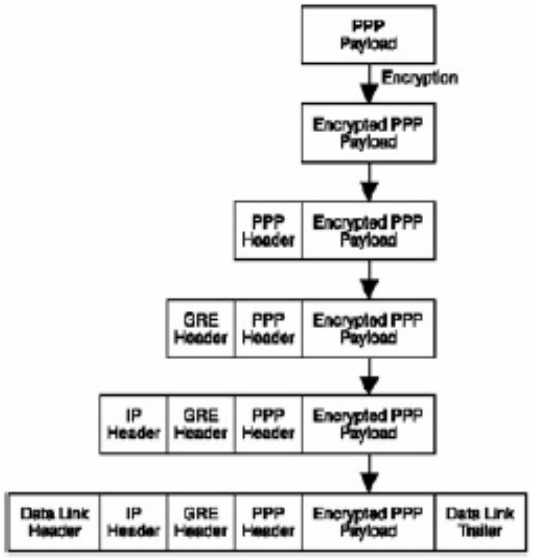


Σχήμα 24: Η πρώτη φάση του PPTP (χρήση του PPP, το οποίο λειτουργεί με 3 στάδια)

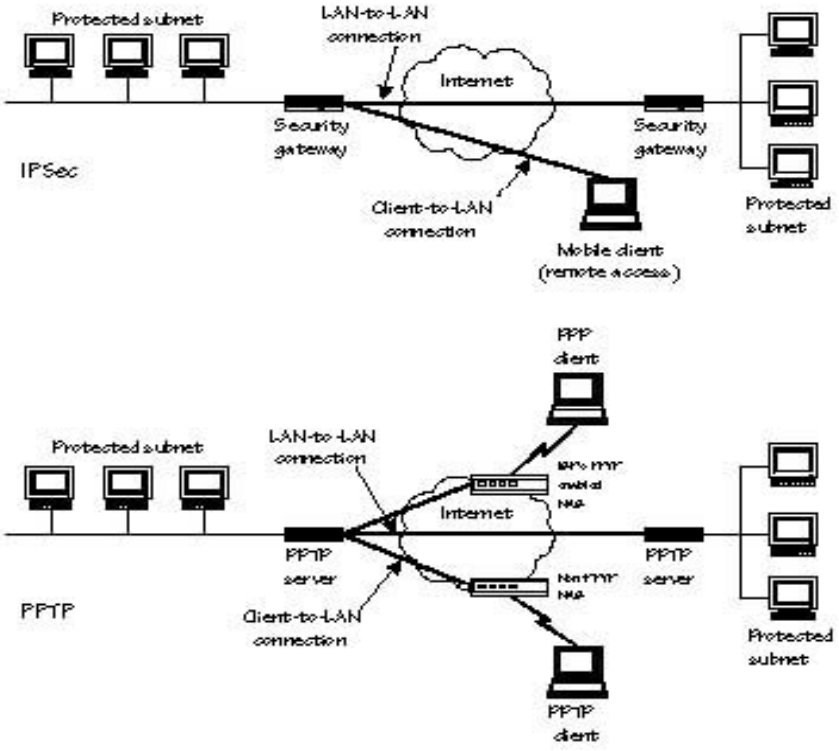
Η συνολική διαδικασία ενθυλάκωσης του PPTP απεικονίζεται στο σχήμα 19.

Μέχρι τώρα αναφερόμασταν, όσον αφορά τα Εικονικά Δίκτυα που βασίζονται στο PPTP, μόνο σε περιπτώσεις όπου ένας χρήστης συνδέεται με το PC του σε ένα δίκτυο. Αν και αυτό ήταν το αρχικό κίνητρο ανάπτυξης του PPTP, μπορεί παρόλα

αυτά να εξυπηρετήσει και περιπτώσεις σύνδεσης δικτύου με δίκτυο (LAN-to-LAN tunneling). Απλά ο server σε κάθε ένα από τα δύο δίκτυα που επικοινωνούν θα πρέπει να μπορεί να λειτουργεί άλλοτε ως server και άλλοτε ως client (σχήμα 25). Κατά τα άλλα, μία LAN-to-LAN PPTP υποδομή μοιάζει πολύ με μία LAN-to-LAN IPSec υποδομή, με εξαίρεση το ότι δεν υπάρχει το πρωτόκολλο ανταλλαγής κλειδιού IKE.



Σχήμα 25: Ενθυλάκωση ενός πακέτου δεδομένων στο PPTP



Σχήμα 26: Σύγκριση δικτύων IPSec και PPTP

Οι PPTP servers προωθούν πακέτα από και προς το αντίστοιχο LAN, έχοντας επίσης τη δυνατότητα να «φιλτράρουν» τα εισερχόμενα πακέτα. Όταν ο ISP διαθέτει PPTP server δεν χρειάζεται ο υπολογιστής του χρήστη να είναι εφοδιασμένος με ειδικό PPTP software – διαφορετικά, κάτι τέτοιο είναι απαραίτητο (και σε αυτήν την τελευταία περίπτωση το άκρο της διόδου είναι ο υπολογιστής και όχι ο PPTP server).
Στα μειονεκτήματα του PPTP συγκαταλέγεται το γεγονός ότι οι PPTP servers δέχονται δεδομένα μόνο 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 πολύ από τα πρωτόκολλα που διαθέτει και μπορεί να υποστηρίξει ο ISP (σε αντίθεση με το IPSec).

4.3. Πρωτόκολλο L2TP

Το αποτέλεσμα της συγχώνευσης του PPTP και του L2F είναι το πρωτόκολλο L2TP, το οποίο 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 L2TP χρησιμοποιεί δύο servers για τη σύνοδο:

- τον **LAC (L2TP Access Concentrator)** – Βρίσκεται στον ISP και χρησιμοποιείται για την εγκαθίδρυση μίας διόδου σε ένα δημόσιο δίκτυο π.χ. PSTN, ISDN, η οποία τερματίζεται στον LNS του κόμβου προορισμού

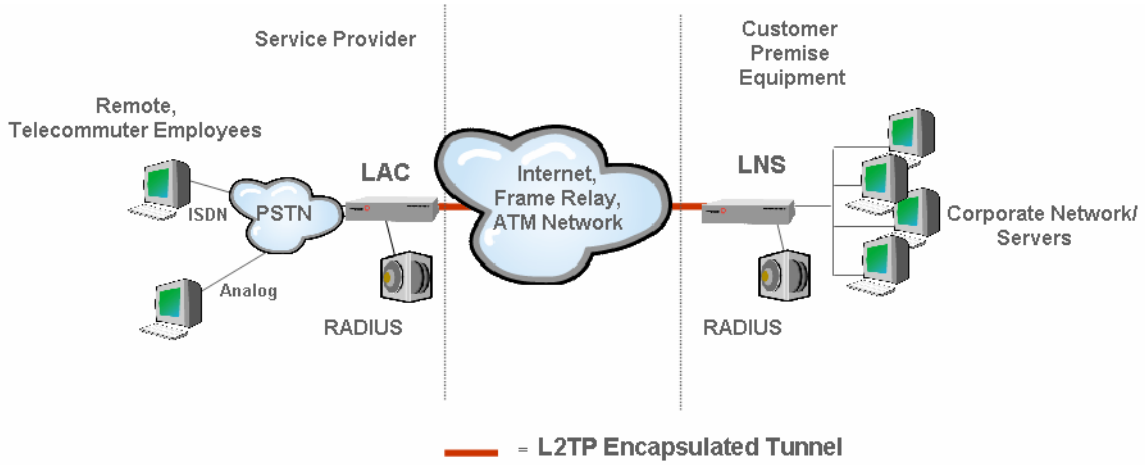
- τον **LNS (L2TP Network Server)** – Βρίσκεται στον προορισμό και χρησιμοποιείται για τον τερματισμό του tunnel. Αναλαμβάνει την αυθεντικοποίηση του χρήστη. Όταν ο LNS λάβει αίτηση για σύνδεση (δημιουργία διόδου) από έναν LAC, αυθεντικοποιεί τον αιτούντα και εγκαθιδρύει το tunnel.

Στη δίοδο που δημιουργείται μεταξύ του Access Concentrator και του Network Server μπορούν να υπάρχουν ταυτόχρονα πολλές σύνοδοι (επικοινωνίες): κάθε σύνοδος έχει ένα δικό της μοναδικό αριθμό Call ID, που υπάρχει στην επικεφαλίδα κάθε L2TP πακέτου. Μπορούν επίσης να υπάρχουν ταυτόχρονα

πολλές διαφορετικές δίοδοι μεταξύ του ίδιου Access Concentrator και του Access Server. Η κάθε μία τότε μπορεί να ικανοποιεί διαφορετικό QoS.

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 Talk, IP, IPX και NETBEUI) και πραγματοποιείται μία πρώτη αυθεντικοποίηση 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 με 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.

Ένα σχηματικό διάγραμμα ενός L2TP VPN (απομακρυσμένης πρόσβασης) απεικονίζεται στο σχήμα 27:



Σχήμα 27: Δίοδος που αναπτύσσεται σε L2TP VPN

Τα στάδια που ακολουθούνται για τη δημιουργία μίας L2TP διόδου είναι τα ακόλουθα:

Στάδιο 1: Ο απομακρυσμένος χρήστης συνδέεται με τον LAC του ISP με χρήση του πρωτοκόλλου PPP. Ο LAC αυθεντικοποιεί τον χρήστη, με βάση το user name και password του. Στη συνέχεια, ο LAC προσδιορίζει την IP διεύθυνση του LNS που ανήκει στο LAN για το οποίο ο χρήστης αιτείται σύνδεση. Μεταξύ LAC και LNS, η σύνοδος L2TP ξεκινά.

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 (Challenge Handshake Authentication Protocol). 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 ένα προστατευμένο 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.

Σε αναγκαστική δίοδο, ο χρήστης στέλνει PPP πακέτα στον LAC και η δημιουργία διόδου μεταξύ του LAC και του LNS του απομακρυσμένου δικτύου γίνεται ερήμην του – ο ίδιος ο χρήστης δεν κάνει καμία άλλη ενέργεια για τη δημιουργία αυτής της διόδου. Το IPSec λοιπόν είναι η καλύτερη επιλογή για τον χρήστη – στέλνει απευθείας κρυπτογραφημένα (και άρα ασφαλή) τα δεδομένα. Το AH προστίθεται από τον LAC του ISP. Το ESP προστίθεται μόνο όταν ο LNS στον προορισμό υποστηρίζει IPSec. Για την ανταλλαγή του συμμετρικού κλειδιού κρυπτογράφησης χρησιμοποιείται το IKE.
Σε αυθόρμητη δίοδο, το AH εφαρμόζεται στον υπολογιστή του χρήστη απευθείας (μια που ο υπολογιστής είναι το άκρο της διόδου – βλέπε σχήμα 17). Αν ο LNS στον προορισμό δεν υποστηρίζει IPSec, το ESP προστατεύει τα δεδομένα μόνο μέχρι να καταφτάσουν στον LNS.

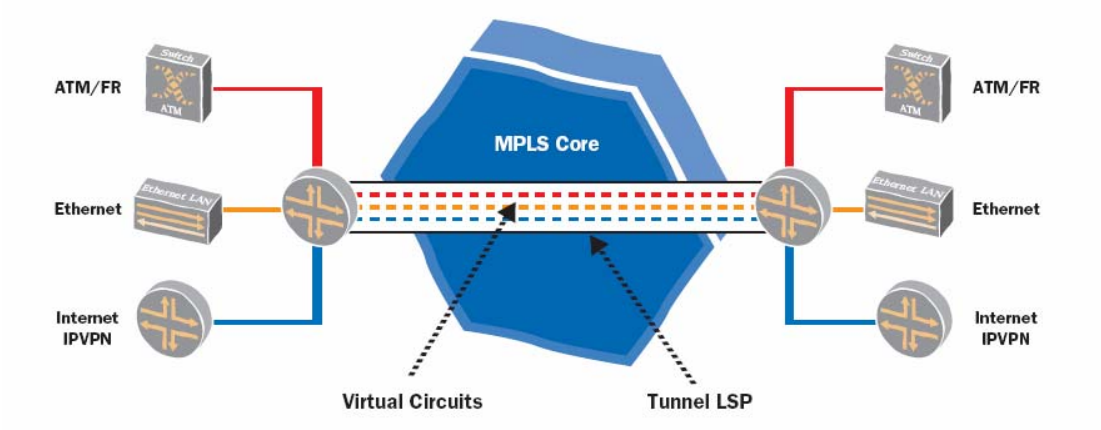
Από τα παραπάνω γίνεται φανερό ότι οι κύριες λειτουργίες που πρέπει να μπορεί να κάνει ο LNS (εκτός βέβαια της βασικής, που είναι η προώθηση των L2TP πακέτων που λαμβάνει στον αντίστοιχο υπολογιστή του δικτύου) είναι εκείνες που τον κάνουν συμβατό με το IPSec: με άλλα λόγια, πρέπει να μπορεί να υποστηρίζει τόσο μια μεγάλη ποικιλία αλγορίθμων κρυπτογράφησης όσο και να μπορεί να επεξεργάζεται

πακέτα που έχουν τις κεφαλίδες AH και ESP. Ένα χαρακτηριστικό του LNS είναι ότι δεν πραγματοποιεί φιλτράρισμα (σε αντίθεση με τον NAS στα PPTP δίκτυα).
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.
Τέλος, θα πρέπει να σημειωθεί ότι το L2TP πρωτόκολλο μπορεί να χρησιμοποιηθεί και για σύνδεση δίκτυο-προς-δίκτυο (LAN-to-LAN tunneling): ειδική μέριμνα πρέπει να υπάρξει ώστε κάθε άκρο της διόδου να μπορεί να δρα ταυτόχρονα και σαν LAC αλλά και σαν LNS.

4.4. Πρωτόκολλο MPLS

Η τεχνολογία MPLS επιτρέπει τη δημιουργία ιδεατών κυκλωμάτων (tunnels) κατά μήκος ενός δικτύου που βασίζεται στο πρωτόκολλο IP, με τρόπο τέτοιο ώστε να αναφερόμαστε σε MPLS VPNs επιπέδου 2 (L2 MPLS VPNs). Να σημειωθεί ότι και σε αυτή την περίπτωση (όπως άλλωστε και σε όλες τις εφαρμογές που στηρίζονται στο MPLS) οι αποφάσεις προώθησης των πακέτων λαμβάνονται με βάση την τιμή της ετικέτας και όχι με βάση την διεύθυνση προορισμού που βρίσκεται στην επικεφαλίδα ενός πακέτου. Στην περίπτωση βέβαια των L2 MPLS VPNs γίνεται μετάδοση πλαισίων του επιπέδου 2 (layer 2 frames) πάνω από MPLS. Για να γίνει πιο κατανοητή η όλη λογική, ας φανταστούμε π.χ. ένα πλαίσιο τεχνολογίας Ethernet (που είναι του δευτέρου επιπέδου του OSI/ISO). Τέτοια πλαίσια είναι δυνατό να μεταχθούν στο MPLS δίκτυο κορμού με τη χρήση ετικετών. Είναι λοιπόν αδιάφορο για το MPLS αν μετάγονται πακέτα IP ή πλαίσια επιπέδου 2. Το γεγονός αυτό σε συνδυασμό με την πιθανή ταυτόχρονη μετάδοση κίνησης IP που μπορεί να εξυπηρετεί άλλες συνδέσεις επιτρέπει τη διατήρηση και διαχείριση μίας κοινής υποδομής από τους ISPs.

Στην ουσία, όταν μιλάμε για L2 MPLS VPN, εννοούμε την ύπαρξη της ασφαλούς διόδου που δεν είναι τίποτα άλλο παρά το ιδεατό μονοπάτι LSP. Μέσω του MPLS πρωτοκόλλου, υπάρχει η δυνατότητα να ενθυλακωθούν πακέτα από διάφορα πρωτόκολλα (π.χ. ATM, Ethernet) σε ειδικά MPLS πακέτα έτσι να μεταφερθούν στην άλλη άκρη του δικτύου μέσω ενός LSP. Στο άκρο του δικτύου γίνεται η αντίστροφη διαδικασία δηλαδή η ανάκτηση του πακέτου στην αρχική του μορφή. Χαρακτηριστικό είναι και το σχήμα που ακολουθεί:



Σχήμα 28: Ενθυλάκωση ATM VCs, Ethernet frames, IP VPNs σε ένα LSP

Ολοένα και περισσότερες εταιρίες ζητούν διασύνδεση των εταιρικών παραρτημάτων τους, χρησιμοποιώντας την υποδομή που ήδη διαθέτουν (π.χ. Frame Relay switches, ATM switches, Ethernet switches). Από την άλλη πλευρά υπάρχει ο ISP επιθυμεί να διατηρεί ένα δίκτυο κορμού με ενιαία αρχιτεκτονική και όχι να είναι ένα συνοθύλευμα από διαφορετικές τεχνολογίες. Σε αυτήν την περίπτωση η τεχνολογία MPLS είναι άκρως δελεαστική. Έτσι «γεννήθηκαν» τα L2 MPLS VPNs.

Υπάρχουν δύο προσεγγίσεις όσον αφορά τα L2 MPLS VPNs:

1. *Layer 2 MPLS-based VPN: Draft-Martini*

Αυτού του είδους τα VPNs ορίζονται από ένα σύνολο από Internet drafts που καθορίζουν με λεπτομέρεια τόσο τον τρόπο της ενθυλάκωσης σε L2, αλλά και τους τρόπους μεταφοράς της σηματοδοσίας (για τους οποίους χρησιμοποιείται το LDP). Η προσέγγιση του Draft-Martini αποκαλείται επίσης Pseudo Wire Emulation, γιατί υλοποιούνται ουσιαστικά συνδέσεις σημείου προς σημείο που θεωρούνται ως pseudo wires (αφού δεν υπάρχει πραγματική σύνδεση σημείο-προς-σημείο αλλά μόνο LSPs δημιουργημένα στο δίκτυο κορμού).

Το πλεονέκτημα του Draft-Martini VPN είναι ότι μπορεί να υποστηρίξει ένα ευρύ σύνολο από διαφορετικές τεχολογίες (Ethernet, Frame Relay, ATM, High-Level Data Link Control (HDLC) και Point-to-Point Protocol (PPP)). Το μειονέκτημα του Draft-Martini VPN είναι ότι δεν είναι είναι κλιμακούμενο. Σε περιπτώσεις δηλαδή που απαιτούνται πολλά τέτοια VPNs πρέπει να δημιουργηθούν ανεξάρτητα το ένα από το άλλο.

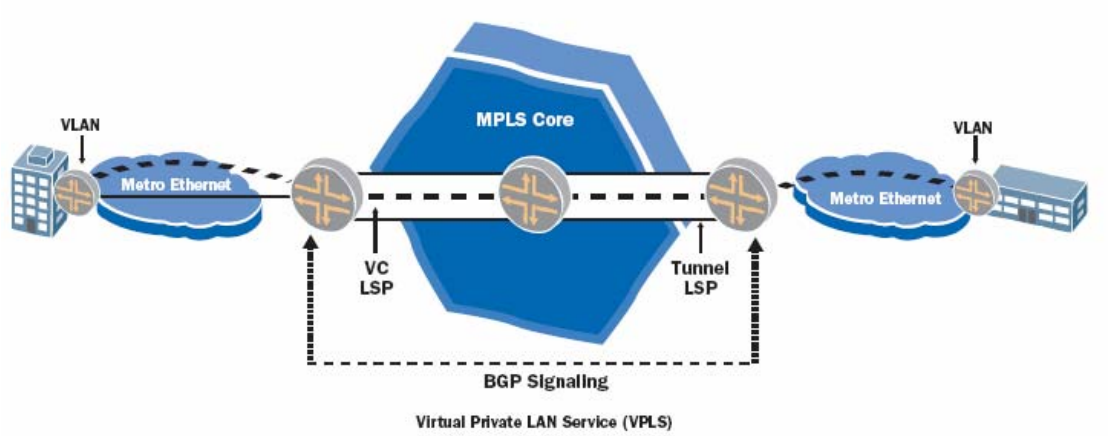
2. *Layer 2 MPLS-based VPN: Draft-Kompella*

Τα Draft-Kompella VPNs σχεδιάστηκαν για να επιλύσουν τα προβλήματα των Draft-Martini VPNs. Πιο συγκεκριμένα, τα Draft-Kompella VPN χρησιμοποιούν το πρωτόκολλο BGP και όχι το LDP για τη δημιουργία των διόδων. Το πλεονέκτημα είναι ότι το BGP ήδη χρησιμοποιείται και για την υλοποίηση των L3 VPNs που μπορεί να συνυπάρχουν στο δίκτυο κορμού - επομένως δεν απαιτείται η εισαγωγή ενός ακόμη πρωτοκόλλου όπως είναι το LDP.

Ένα ακόμα πλεονέκτημα των Draft-Kompella VPNs είναι ότι απαιτούν ελάχιστη προσπάθεια από το διαχειριστή του δικτύου MPLS για τη δημιουργία τους. Κι αυτό γιατί το BGP είναι ένα επαρκώς αυτοματοποιημένο πρωτόκολλο που απαιτεί μικρή παρέμβαση απο το διαχειριστή.

Αξίζει να σημειωθεί ότι ένα Draft-Kompella VPN εξακολουθεί να μπορεί να υποστηρίζει ένα μεγάλο πλήθος ενθυλακώσεων, όπως το Draft-Martini. Συνεπώς, είναι η λύση που υιοθετούν οι περισσότερες εταιρίες για την κατασκευή προϊόντων που θα παρέχουν αυτές τις υπηρεσίες.

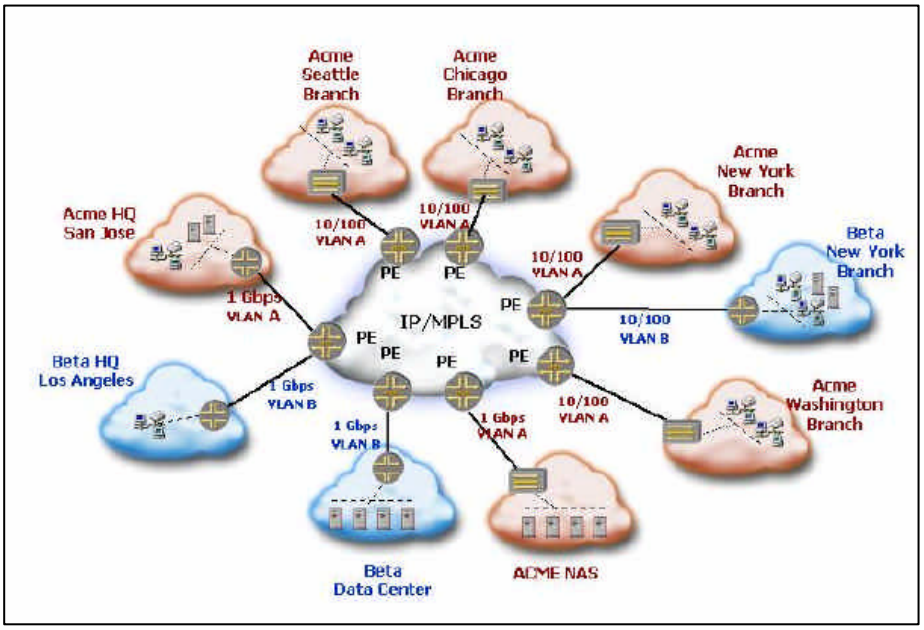
Εκτός από L2 VPNs, γίνεται - όλο και πιο συχνά τώρα τελευταία – αναφορά στα δίκτυα VPLS (Virtual Private LAN Services) τα οποία ουσιαστικά υλοποιούν μία τοπολογία Ethernet και η οποία εκτείνεται σε περισσότερα από ένα μητροπολιτικά δίκτυα. Για παράδειγμα θα μπορούσαμε να αναφερθούμε σε μια εταιρία η οποία έχει ήδη αναπτύξει στην Αθήνα και στη Θεσσαλονίκη από ένα μητροπολιτικό δίκτυο. Στην περίπτωση που ένα μέλος του μητροπολιτικού δικτύου της Αθήνας χρειάζεται να υλοποιήσει μία Ethernet σύνδεση με ένα μέλους του μητροπολιτικού δικτύου της Θεσσαλονίκης είναι εφικτό να γίνει αυτό με τη χρήση της τεχνολογίας VPLS.
Χαρακτηριστικό είναι και το σχήμα που ακολουθεί:



Σχήμα 29: Τεχνολογία VPLS

Ένα από τα πλεονεκτήματα της τεχνολογίας VPLS είναι ότι οι πελάτες που το επιθυμούν συνδέονται με τη χρήση Ethernet interfaces – δηλαδή, με απλά λόγια, κάθε χρήστης αντιλαμβάνεται τους υπολογιστές του απομακρυσμένου μητροπολιτικού δικτύου σαν να βρίσκονται στο δικό του Ethernet.

Το σχήμα που ακολουθεί απεικονίζει τον τρόπο με τον οποίο μία εταιρία μπορεί με ασφαλή τρόπο να χρησιμοποιήσει την δημόσια υποδομή του ISP που στηρίζεται στο πρωτόκολλο MPLS έτσι ώστε να δημιουργήσει το ιδιωτικό της Ethernet δίκτυο το οποίο εκτείνεται σε περισσότερες από μία πόλεις, με μεγάλες αποστάσεις μεταξύ τους.



Σχήμα 30: VPLS τοπολογία για μια εταιρία, προκειμένου να δομήσει Ethernet δίκτυο μεταξύ διαφορετικών πόλεων

Ένα σημαντικό ζήτημα της τεχνολογίας VPLS είναι επίσης ο τρόπος με τον οποίο «ανακαλύπτονται» νέοι κόμβοι πελατών που εισάγονται στο δίκτυο. Υπάρχουν δύο προσεγγίσεις: ο αυτοματοποιημένος τρόπος (auto-discovery) και «χειροκίνητη» ένταξή του από τον διαχειριστή του δικτύου MPLS.

5. Εικονικά Ιδιωτικά Δίκτυα Επιπέδου Μεταφοράς

Τα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου 4 (Μεταφοράς) υλοποιούνται μέσω του πρωτοκόλλου SSL (Secure Sockets Layer) (σε αυτήν την κατηγορία εντάσσεται επίσης και το πρωτόκολλο SOCKS, που δεν θα αναλυθεί εδώ). Στη συνέχεια περιγράφεται η τεχνολογία SSL VPN, αναλύονται οι μηχανισμοί ασφάλειας και αναφέρονται ενδεικτικές εφαρμογές τους.

5.1. Γενική Περιγραφή SSL

Τα Εικονικά Ιδιωτικά Δίκτυα (VPN) Επιπέδου Εφαρμογής χρησιμοποιούν το πρωτόκολλο SSL (Secure Sockets Layer) ώστε να υλοποιούν επικοινωνίες μέσω επισφαλών καναλιών του Internet, διαφυλάσσοντας κάποιο συγκεκριμένο επίπεδο ασφάλειας. Στην πραγματικότητα, ένα SSL VPN παρέχει στους τελικούς χρήστες εξουσιοδοτημένη και ασφαλή πρόσβαση σε εφαρμογές όπως HTTP, client/server και file sharing.

Το πρωτόκολλο SSL είναι οικείο στους περισσότερους χρήστες, ακόμα και σε εκείνους χωρίς ιδιαίτερο υπόβαθρο τεχνικών γνώσεων. Είναι ήδη εγκατεστημένο σε οποιοδήποτε Η/Υ που είναι συνδεδεμένος στο Διαδίκτυο και χρησιμοποιεί έναν standard 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. Επίσης 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 IPSec VPNs.

Η ασφαλής σύνδεση που παρέχεται με το πρωτόκολλο SSL επιτυγχάνεται μέσω:

α) της πιστοποίησης της ταυτότητας των πλευρών που επικοινωνούν και
β) της κρυπτογράφησης της κίνησης που πραγματοποιείται μεταξύ τους.

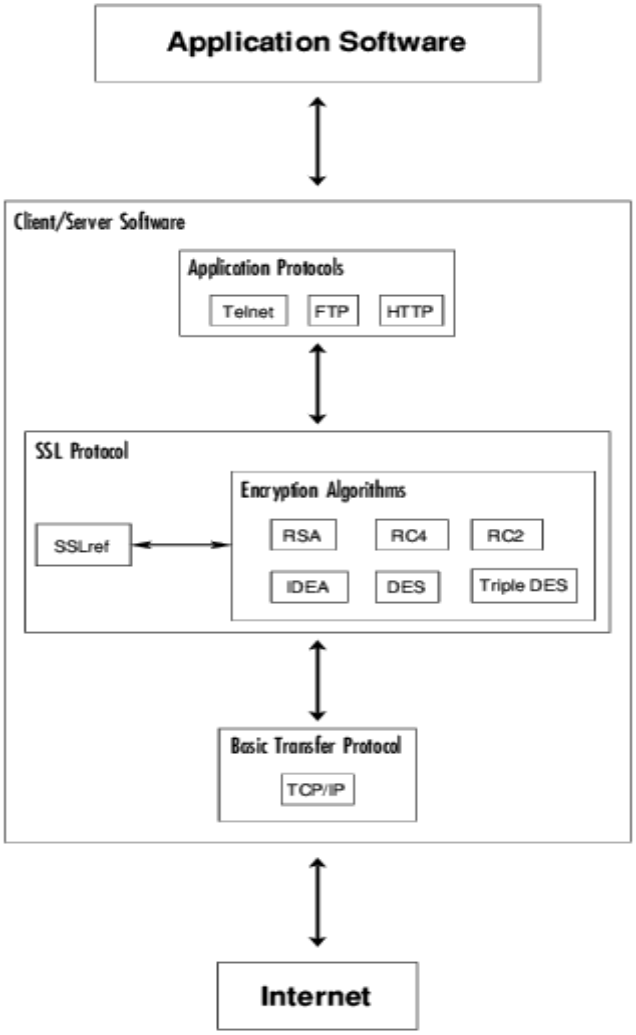
Διευκρινίζεται ότι τα SSL VPNs αφορούν εφαρμογές που υποστηρίζουν το πρωτόκολλο SSL, όπως για παράδειγμα Web browsers και Web-based e-mail.

5.2. Μηχανισμοί Ασφάλειας στο SSL

Η ασφάλεια των SSL VPNs βασίζεται στους μηχανισμούς ασφάλειας του πρωτοκόλλου SSL. Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0) και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή RFC (Request For Comments). Τον Δεκέμβριο του 1994 εκδίδεται μια επαναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0). Ωστόσο, το SSL version 2.0 είχε αρκετούς περιορισμούς τόσο ως προς την κρυπτογραφική ασφάλεια όσο και ως προς τη λειτουργικότητά του. Έτσι το πρωτόκολλο αναβαθμίστηκε σε SSL v.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. Το τελευταίο Internet Draft που προσδιορίζει το SSL v.3.0 κυκλοφόρησε το Νοέμβριο του 1996. Η περιγραφή του SSL βασίζεται σε αυτές τις τελευταίες προδιαγραφές του πρωτοκόλλου. Η τελευταία έκδοση του SSL μετεξελίχτηκε στο TLS (Transport Layer Security).

Το πρωτόκολλο SSL στρωματοποιείται 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 ειδικότερα είναι η ανεξαρτησία από την εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς (transparently) σε οποιαδήποτε

TCP/IP εφαρμογή στρωματοποιείται στην κορυφή του. Μια αναπαράσταση του πρωτοκόλλου SSL βλέπουμε στη συνέχεια.



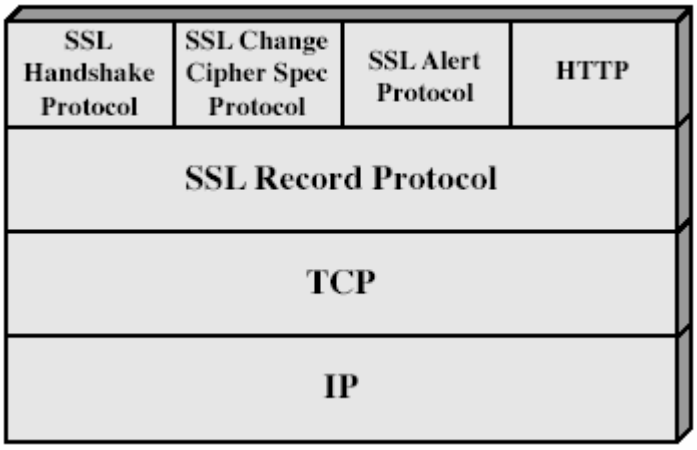
Σχήμα 31: Αναπαράσταση του πρωτοκόλλου SSL

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

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

Γενικά, μία σύνοδος του SSL πρωτοκόλλου εξελίσσεται αξιοποιώντας γνώση από διαδοχή προγενέστερων καταστάσεων και είναι η ευθύνη του πρωτοκόλλου SSL, και συγκεκριμένα του SSL handshake protocol που θα δούμε στη συνέχεια, να συντονίσει τις καταστάσεις συνόδου και σύνδεσης τόσο από την πλευρά του εξυπηρετούμενου όσο και από την πλευρά του εξυπηρέτη. Τα επικοινωνούντα μέρη μπορούν να έχουν πολλαπλές ταυτόχρονες συνόδους, καθώς επίσης και συνόδους με πολλαπλές συνδέσεις.

Η στρωμάτωση των πρωτοκόλλων του SSL απεικονίζεται στο σχήμα 32:



Σχήμα 32: Αρχιτεκτονική του SSL

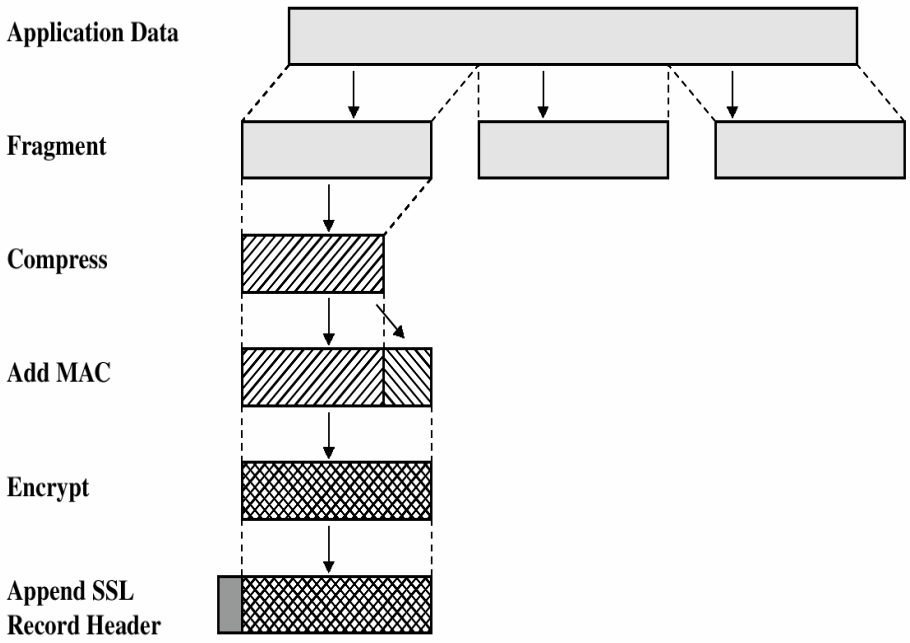
Τα δύο βασικά πρωτόκολλα του SSL είναι το **SSL Record Protocol** και το **SSL Handshake Protocol**. Συνοπτικά, το SSL Record Protocol παρέχει υπηρεσίες εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων. Αρκετά πρωτόκολλα SSL μπορούν να στρωματοποιούνται πάνω από το record protocol. Το σημαντικότερο από αυτά τα πρωτόκολλα είναι το SSL Handshake 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 μπορεί να συμπιέζεται και να κρυπτογραφείται σύμφωνα με την τρέχουσα μέθοδο συμπίεσης και τον αλγόριθμο κρυπτογράφησης (που έχουν οριστεί από το Handshake Protocol). Οι αλγόριθμοι που χρησιμοποιούνται στο SSL Record Protocol φαίνονται στον ακόλουθο πίνακα.

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		

Όταν η ασφάλεια είναι πολύ κρίσιμη, το μέγεθος του κλειδιού πρέπει να είναι τουλάχιστον 128 bits.

Οι διαδικασίες που συντελούνται από το SSL Record Protocol απεικονίζονται αναλυτικά στο σχήμα 33.



Σχήμα 33: Λειτουργίες του SSL Record Protocol

Το *SSL Handshake Protocol* είναι το κυριότερο πρωτόκολλο από αυτά που βρίσκονται ένα στρώμα ψηλότερα από το SSL Record Protocol. Σκοπός του SSL Handshake protocol είναι να 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 και να δημιουργούν ένα κύριο μυστικό κλειδί (master secret key), από το οποίο προκύπτουν διάφορα κλειδιά συνόδου για αυθεντικοποίηση και κρυπτογράφηση μηνυμάτων.

Τα βήματα της διαδικασίας SSL Handshake είναι τα ακόλουθα:

Βήμα 1: Ο SSL client συνδέεται με τον SSL server και ζητά να τον πιστοποιήσει. Επίσης ο client ενημερώνει για το ποιους αλγορίθμους κρυπτογράφησης υποστηρίζει. Ο server από την πλευρά του επιβεβαιώνει το αν μπορεί να υποστηρίξει τους αλγορίθμους αυτούς, ενώ επίσης αποδίδει και έναν μοναδικό αριθμό (coonection id) στη σύνδεση που έχει δημιουργηθεί.

Βήμα 2: Ο server αποδεικνύει την ταυτότητά του με την αποστολή του ψηφιακού του πιστοποιητικού. Τα πιστοποιητικά επαληθεύονται με τον έλεγχο των ημερομηνιών εγκυρότητας, καθώς και από το γεγονός ότι το πιστοποιητικό φέρει την υπογραφή μίας διαπιστευμένης αρχής πιστοποιητικού. Υπάρχει η δυνατότητα, προαιρετικά, ο server να ζητήσει πιστοποίηση ταυτότητας από τον client.

Βήμα 3: Εάν ο server έχει ζητήσει πιστοποιητικό γνησιότητας από τον client, αυτός το αποστέλλει. Επίσης πραγματοποιείται η διαπραγμάτευση για τον αλγόριθμο κρυπτογράφησης μηνύματος, καθώς και για τη συνάρτηση κατακερματισμού. Συνήθως ο server επιλέγει την πιο ισχυρή κρυπτογραφική μέθοδο από αυτές που του πρότεινε ο client. Ταυτόχρονα, ο client και ο server παράγουν τα κλειδιά συνόδου σύμφωνα με τα ακόλουθα βήματα:

α) 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).
β) Ο server απαντά με περισσότερα τυχαία δεδομένα (κρυπτογραφημένα με το δημόσιο κλειδί του client, αν είναι διαθέσιμο. Αλλιώς, στέλνει τα δεδομένα μη κρυπτογραφημένα - cleartext).
γ) Τα κλειδιά κρυπτογράφησης παράγονται από όλα αυτά τα τυχαία δεδομένα με τη χρήση των συναρτήσεων κατακερματισμού.

Βήμα 4: Ανταλλάσσονται μηνύματα τερματισμού των διαδικασιών του Handshake Protocol.

Σήμερα, το πρωτόκολλο SSL είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το Internet. Μειονέκτημα της χρήσης του αποτελεί το γεγονός ότι επιβραδύνεται η επικοινωνία του browser του client με τον HTTPS server. Η καθυστέρηση οφείλεται

στις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με ασύμμετρο κρυπτοσύστημα κατά την αρχικοποίησης της SSL συνόδου. Πρακτικά, οι χρήστες αντιλαμβάνονται μικρή καθυστέρηση λίγων δευτερολέπτων μεταξύ της έναρξης σύνδεσης με το HTTPS εξυπηρέτη και της ανάκτησης της πρώτης HTML σελίδας από αυτόν. Επειδή κατά τη σχεδίαση του SSL αποθηκεύεται το κύριο μυστικό κλειδί, η καθυστέρηση επηρεάζει μόνον την πρώτη SSL επικοινωνία μεταξύ browser και HTTPS server. Συγκριτικά με την εγκατάσταση συνόδου, ο επιπλέον φόρτος από τη λειτουργία αλγορίθμων όπως οι DES, RC2, RC4, είναι πρακτικά ασήμαντος.

5.3. Αντοχή του πρωτοκόλλου SSL σε επιθέσεις

Στη συνέχεια θα αναφερθεί η «αντοχή» του πρωτοκόλλου SSL σε κάποια είδη επιθέσεων καθώς επίσης και οι αδυναμίες του. Αξίζει να σημειωθεί ότι το SSL πρωτόκολλο δεν παρέχει προστασία έναντι επιθέσεων ανάλυσης κυκλοφορίας (traffic analysis). Για παράδειγμα, ένας αναλυτής κυκλοφορίας εξετάζοντας τις μη κρυπτογραφημένες IP διευθύνσεις αποστολέα και παραλήπτη, καθώς και τους TCP αριθμούς θυρών, μπορεί τελικά να καταγράψει ποια μέρη αλληλεπιδρούν ή ποιοι τύποι υπηρεσιών χρησιμοποιούνται.

Επίθεση *Dictionary Attack:* Μπορεί να εφαρμοστεί από έναν «επιτιθέμενο» όταν ένα μέρος του μη κρυπτογραφημένου κειμένου είναι στην κατοχή του. Τότε το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί. Το SSL δεν απειλείται από αυτήν την επίθεση όταν τα κλειδιά των αλγορίθμων του είναι μεγέθους 128 bit.

Επίθεση *Brute Force Attack*: 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. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι χωρίς νόημα (τα 2^{128} κλειδιά που καλείται να υπολογίσει κανείς είναι απίστευτα μεγάλος αριθμός).

Επίθεση *Replay Attack:* Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί ξανά να χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση *replay attack*. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνοδο (κάθε σύνοδος έχει το δικό της id, που ορίζεται κατά την έναρξη των διαδικασιών του Handshake πρωτοκόλλου). Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.

Επίθεση *Man-In-The-Middle:* Συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τα τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα. Όμως όπως ήδη είδαμε το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατη. Συνεπώς, ο επιτιθέμενος δεν μπορεί να πείσει τον client ότι είναι ο server.

Η μεγαλύτερη αδυναμία του πρωτοκόλλου είναι η ευαισθησία των αλγόριθμων που χρησιμοποιούν μικρά κλειδιά. Συγκεκριμένα, οι RC4-40, RC2-40 και DES-56 εισάγουν σοβαρά προβλήματα ασφάλειας και θα πρέπει να αποφεύγονται.

Επιπλέον, από τη στιγμή που μία σύνδεση δημιουργηθεί, το ίδιο master key χρησιμοποιείται καθ' όλη την διάρκεια της. Όταν το SSL χρησιμοποιείται πάνω από μια μακρόχρονη σύνδεση (π.χ. μιας TELNET εφαρμογής), η αδυναμία αλλαγής του master key γίνεται επικίνδυνη. Η καλύτερη μέθοδος επίλυσης αυτού του προβλήματος είναι η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα, μειώνοντας έτσι την πιθανότητα μιας επιτυχούς Brute Force Attack.

5.4. Σύγκριση του SSL με το IPSec

Όπως ήδη είδαμε, το βασικό μειονέκτημα ενός Εικονικού Ιδιωτικού Δικτύου που βασίζεται στο 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

5.5. Εφαρμογές

Η πιο κοινή εφαρμογή του πρωτοκόλλου SSL είναι η διασφάλιση HTTP επικοινωνιών μεταξύ του browser και του web server. Η ασφαλής έκδοση του HTTP χρησιμοποιεί URLs που ξεκινούν με "https" αντί του κανονικού "http" και διαφορετική πόρτα (port) που είναι η προκαθορισμένη «πόρτα» 443. Το πρωτόκολλο SSL παρέχει κρυπτογράφηση σε επίπεδο εφαρμογής για Web browsers και άλλες εφαρμογές. Χρησιμοποιείται διεθνώς για μεταφορά ευαίσθητων οικονομικά δεδομένων. Πιο συγκεκριμένα, το SSL χρησιμοποιείται γενικά σε διακομιστές Web για την υποστήριξη εφαρμογών ηλεκτρονικού εμπορίου, ηλεκτρονικών τραπεζικών υπηρεσιών και άλλων εφαρμογών που απαιτούν ασφάλεια των επικοινωνιών.

Για παράδειγμα, κατά τη διάρκεια ηλεκτρονικών τραπεζικών συναλλαγών, η τεχνολογία SSL χρησιμοποιείται για την κρυπτογράφηση των προσωπικών στοιχείων του χρήστη πριν απομακρυνθούν από τον υπολογιστή του, κατά τέτοιο τρόπο ώστε να μην είναι εφικτή η ανάγνωση από τρίτα άτομα. Το SSL εμποδίζει την υποκλοπή ευαίσθητων πληροφοριών (π.χ. αριθμοί πιστωτικών καρτών, υπόλοιπο λογαριασμών και άλλα οικονομικά και προσωπικά στοιχεία) που στέλνονται μέσω Internet μεταξύ

του browser του χρήστη και ενός διακομιστή web κατά τη διάρκεια ηλεκτρονικών συναλλαγών.

Σύμφωνα με όσα αναφέρθηκαν παραπάνω, το πρωτόκολλο SSL υλοποιεί χαρακτηριστικά VPN αφού παρέχει κρυπτογράφηση δεδομένων, πιστοποίηση του server και προαιρετικά της ταυτότητας του client και εξασφαλίζει την ακεραιότητα των δεδομένων. Τα SSL VPNs είναι κατάλληλα για να παρέχουν ασφάλεια σε εφαρμογές απομακρυσμένης πρόσβασης, όπως εφαρμογές Web, εφαρμογές client/server και εφαρμογές file sharing.

6. «Μεταγλώττιση διεθύνσεων» (Network Address Translation)

6.1. Διατύπωση προβλήματος

Είναι γνωστό ότι όταν κάποιος υπολογιστής είναι συνδεδεμένος στο Internet (ή σε οποιοδήποτε IP δίκτυο), του έχει αποδοθεί μία μοναδική IP διεύθυνση (ένας 32-bit αριθμός). Το πρωτόκολλο που εκτελείται για την απόδοση IP διευθύνσεων είναι το DHCP (Dynamic Host Control Protocol. Γενικά δεν μπορεί να αποδοθεί αυθάιρετα ένας οποιοσδήποτε 32-bit αριθμός σε έναν υπολογιστή – υπάρχουν διάφορες κλάσεις IP διευθύνσεων και ο κάθε υπολογιστής μπορεί να έχει ως διεύθυνση κάποιον αριθμό της κλάσης στην οποία ανήκει μόνο.

Ειδικά για τα ιδιωτικά δίκτυα, όπου ο αριθμός τους ανά τον κόσμο είναι συντριπτικά μεγάλος (ας αναλογιστούμε για παράδειγμα ότι σε κάθε απλό εργαστήριο Πληροφορικής σε ένα σχολείο υπάρχει ένα τοπικό ιδιωτικό δίκτυο), οι IP διεθύνσεις που μπορούν να έχουν οι υπολογιστές μπορούν να ανήκουν μόνο σε κάποια από τις τρεις επόμενες κλάσεις:

- 10.0.0.0 - 10.255.255.255 (Class A)
- 172.16.0.0 - 172.31.255.255 (Class B)
- 192.168.0.0 - 192.168.255.255 (Class C)

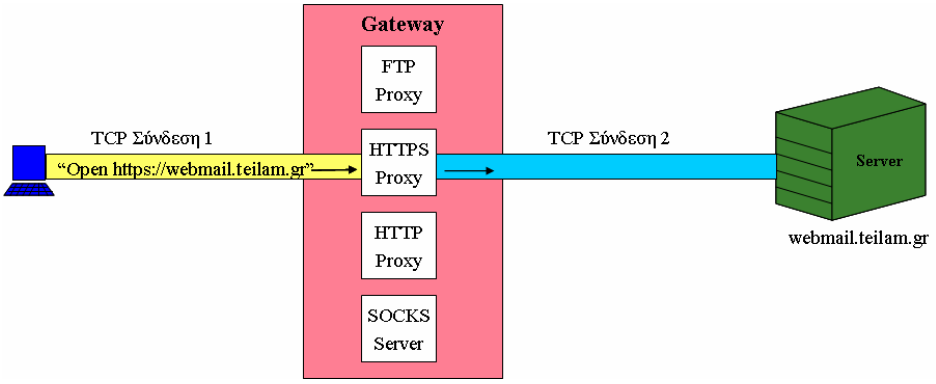
Έτσι, μπορούν ταυτόχρονα δύο διαφορετικοί υπολογιστές που ανήκουν σε διαφορετικά δίκτυα να έχουν την ίδια IP διεύθυνση (στο τοπικό ιδιωτικό του δίκτυο ο καθένας). Αυτό είναι απόλυτα θετικό – θα ήταν αδύνατον κάθε φορά που δημιουργούσαμε ένα τοπικό δίκτυο και αποδίδαμε διευθύνσεις στους υπολογιστές του, να εξετάζαμε αν σε κάποιο άλλο δίκτυο στον κόσμο υπάρχει κάποια κοινή διεύθυνση. Από την άλλη πλευρά όμως, αυτό το χαρακτηριστικό γίνεται μειονέκτημα όταν χρειαστεί να συνδεθούν δύο τέτοια δίκτυα – στο νέο μεγαλύτερο δίκτυο που δημιουργείται, είναι πιθανό να βρεθούν δύο υπολογιστές με την ίδια IP διεύθυνση - αυτό βέβαια δεν πρέπει να επιτραπεί να συμβεί. Το παραπάνω λοιπόν είναι ένα πρόβλημα που συναντά κανείς κατά τη διασύνδεση δύο τοπικών δικτύων για την

υλοποίηση ενός μεγαλύτερου VPN. Δύο είναι οι βασικοί τρόποι να αντιμετωπιστεί: η χρήση proxy server ή το πρωτόκολλο Network Address Translation (NAT).

6.2. Χρήση proxy server

Όταν σε ένα τοπικό δίκτυο υπάρχει ένας proxy server, τότε κάθε πακέτο που στέλνει ένας υπολογιστής του δικτύου στον «έξω κόσμο» γίνεται μέσω ενός Proxy server. Είναι ειδική «συσκευή» που αναλαμβάνει να προωθεί κάθε πακέτο που στέλνει ένας υπολογιστής του δικτύου και του οποίου ο προορισμός είναι εκτός δικτύου. Όταν υπάρχει ένας proxy server, το πακέτο που τελικά απομακρύνεται από το τοπικό δίκτυο έχει σαν IP διεύθυνση αποστολέα όχι την πραγματική IP διεύθυνση του υπολογιστη-αποστολέα, αλλά την IP διεύθυνση του Proxy server. Δημιουργείται λοιπόν μια νέα TCP σύνδεση (βλέπε σχήμα 34). Έτσι, αποφεύγεται το προαναφερθέν πρόβλημα σχετικά με την επαναχρησιμοποίηση IP διευθύνσεων.

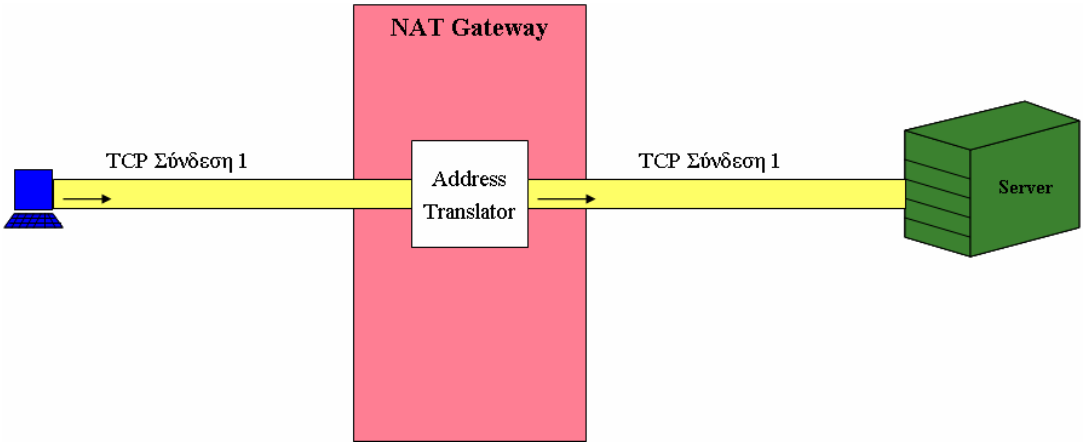
Μειονέκτημα αυτής της προσέγγισης αποτελεί το γεγονός ότι δεν είναι γενικού τύπου: δεν μπορεί να χρησιμοποιηθεί σε όλες τις περιπτώσεις. Κατ' αρχήν, υπάρχει ειδικός proxy server για κάθε εφαρμογή και όχι ένας καθολικός proxy server (π.χ. άλλος proxy server θα προωθήσει μία αίτηση για σύνδεση σε μια ιστοσελίδα και άλλος proxy server θα προωθήσει μία αίτηση ftp). Συνεπώς, αν χρειαστεί κάποια στιγμή να χρησιμοποιηθεί μία εφαρμογή για την οποία δεν έχει ληφθεί μέριμνα να υπάρχει ο κατάλληλος Proxy, υπάρχει πρόβλημα. Επίσης, οι proxy servers δεν μπορούν να επεξεργαστούν εύκολα περιπτώσεις που το υλοποιούμενο πρωτόκολλο του στρώματος δικτύου δεν είναι το TCP αλλά το UDP.



Σχήμα 34: Παράδειγμα λειτουργίας του Proxy Server

6.3. Πρωτόκολλο NAT

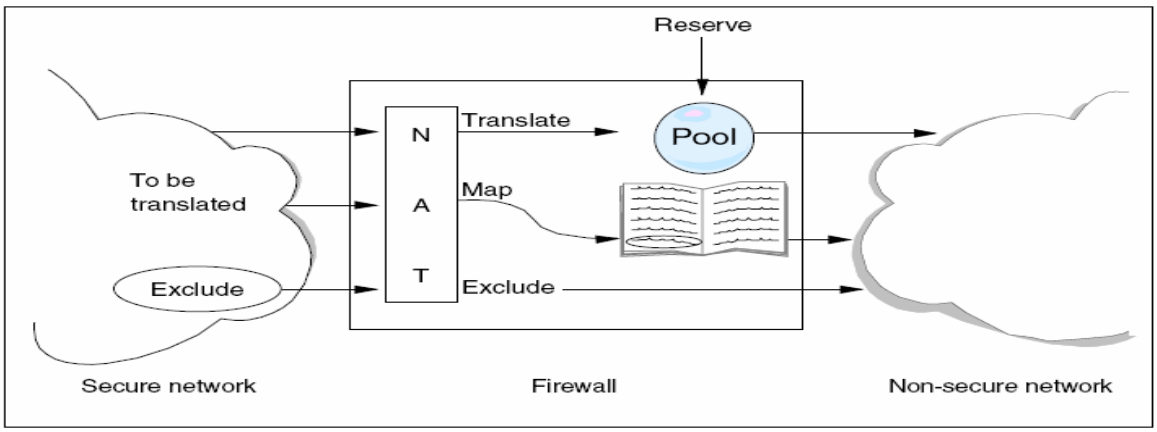
Το NAT (Network Address Translation) είναι ειδικό πρωτόκολλο που εκτελούν οι πύλες (gateways) και έχει σαν αποτέλεσμα να αλλάζει την IP διεύθυνση ενός πακέτου που ξεκινά από έναν υπολογιστή εντός του τοπικού δικτύου και προωθείται εκτός του δικτύου. Δεν δημιουργείται μία νέα TCP σύνδεση από τον Network Translator – βλέπε το ακόλουθο σχήμα:



Σχήμα 35: Σχηματική αναπαράσταση του NAT

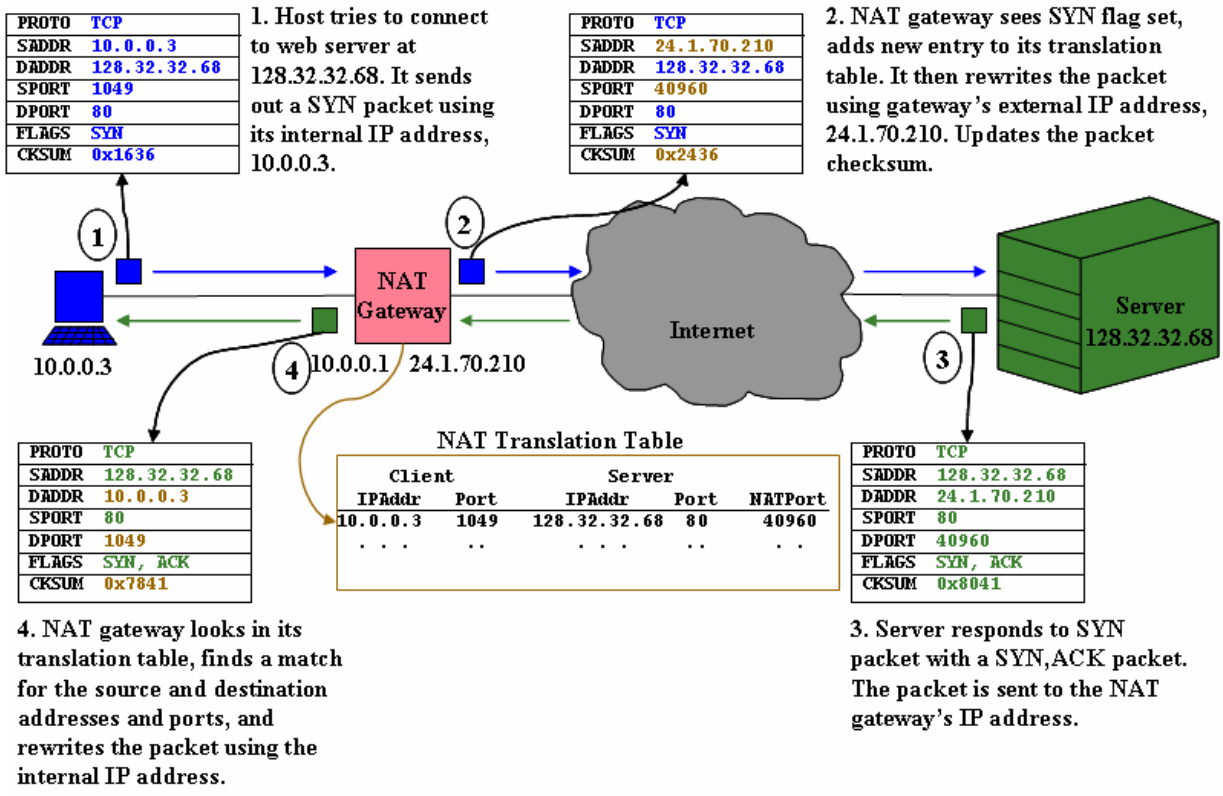
Πιο συγκεκριμένα, το NAT δουλεύει ως εξής: Κάθε υπολογιστής ενός ιδιωτικού δικτύου που ζητάει να συνδεθεί με κάποιον εκτός δικτύου, κάνει αίτηση στον Network Address Translator (που υπάρχει στην πύλη (gateway ή firewall)) για να πάρει μία νέα διεύθυνση. Ο NAT διαθέτει ένα σύνολο διαθέσιμων IP διευθύνσεων («address pool») και μία από αυτές τις αναθέτει στον υπολογιστή. Ταυτόχρονα, κρατάει μία βάση δεδομένων στην οποία καταγράφει τη διεύθυνση που απέδωσε σε κάθε υπολογιστή (διαδικασία MAP). Έτσι, κάθε πακέτο που φεύγει από τον υπολογιστή του ιδιωτικού δικτύου και «ταξιδεύει» στο Internet έχει σαν διεύθυνση αποστολέα τη νέα αυτή διεύθυνση. Αντίστροφα, κάθε υπολογιστής που θέλει να στείλει δεδομένα στον συγκεκριμένο υπολογιστή του ιδιωτικού δικτύου, στέλνει πακέτα με διεύθυνση παραλήπτη τη νέα διεύθυνση. Ο NAT είναι πάλι υπεύθυνος σε αυτήν την περίπτωση για να παραλάβει ο υπολογιστής τα πακέτα που προορίζονται για αυτόν: συγκεκριμένα, ο NAT κοιτάει τη βάση δεδομένων και βλέπει ποια είναι η πραγματική IP διεύθυνση του υπολογιστή (δηλαδή η διεύθυνση που έχει στο ιδιωτικό του δίκτυο) και, με βάση αυτήν την πληροφορία, δρομολογεί τα εισερχόμενα πακέτα. Τα παραπάνω απεικονίζονται στο σχήμα 36 – όπου η διαδικασία Exlude υποδηλώνει

το γεγονός ότι κάποιες διευθύνσεις κάποιες φορές δεν χρειάζεται να αλλάξουν (να «μεταγλωτιστούν») σε κάποια άλλη (π.χ. αν αντιστοιχούν σε κάποιον mail server).



Σχήμα 36: Λειτουργία του NAT

Για να γίνει ακόμα πιο σαφής η διαδικασία του NAT, ας δούμε αναλυτικά το ακόλουθο παράδειγμα:



Σχήμα 37: Ένα παράδειγμα της NAT διαδικασίας

Ας παρακολουθήσουμε τη διαδικασία που συντελείται στο παραπάνω σχήμα.

- **Στάδιο 1**. Ένας υπολογιστής εντός ιδιωτικού δικτύου με διεύθυνση 10.0.0.3 θέλει να συνδεθεί με ένα απομακρυσμένο υπολογιστή (server – π.χ ένας ftp server) που έχει διεύθυνση 128.32.32.68. Παρακολουθούμε τα πεδία από το TCP/IP πλαίσιο που μας ενδιαφέρουν: τα SADDR, DADDR είναι οι διευθύνσεις αποστολέα και προορισμού αντίστοιχα. Τα SPORT, DPORT είναι οι TCP θύρες αποστολέα και προορισμού αντίστοιχα και σχετίζονται κυρίως με την εφαρμογή που αιτείται ο χρήστης (τα νούμερα στο σχήμα είναι τυχαία). Το CKSUM είναι το πεδίο εκείνο του TPC/IP πλαίσιου που υπολογίζεται με σκοπό την ανίχνευση σφάλματος – δηλαδή εκτελεί μια συνάρτηση κατακερματισμού πάνω σε όλο το υπόλοιπο πακέτο και η τιμή που υπολογίζεται είναι αυτή που μπαίνει στο CKSUM (επίσης τυχαία η τιμή που αναγράφεται στο σχήμα).

- **Στάδιο 2**. Ο NAT μεταβάλλει τη διεύθυνση του υπολογιστή. Στο συγκεκριμένο παράδειγμα την κάνει 24.1.70.210 (οπότε και αλλάζει η τιμή του πεδίου SADDR στο TCP/IP πακέτο). Αντίστοιχα αλλάζει και η τιμή του SPORT (επίσης τυχαία η τιμή του σχήματος), ενώ προφανώς, αφού 2 πεδία του πακέτου έχουν μεταβληθεί, αναγκαστικά θα αλλάξει και η τιμή του CKSUM. Ταυτόχρονα, ο NAT ενημερώνει τον πίνακά του σχετικά με την αλλαγή στη IP διεύθυνση που πραγματοποίησε (διαδικασία MAP, όπως αναφέρθηκε νωρίτερα). Η νέα καταχώρηση που τοποθετείται στον πίνακα περιέχει την αρχική IP διεύθυνση και TCP θύρα του υπολογιστή, την IP διεύθυνση και TCP θύρα του υπολογιστή-προορισμού, καθώς και την TPC θύρα του NAT.

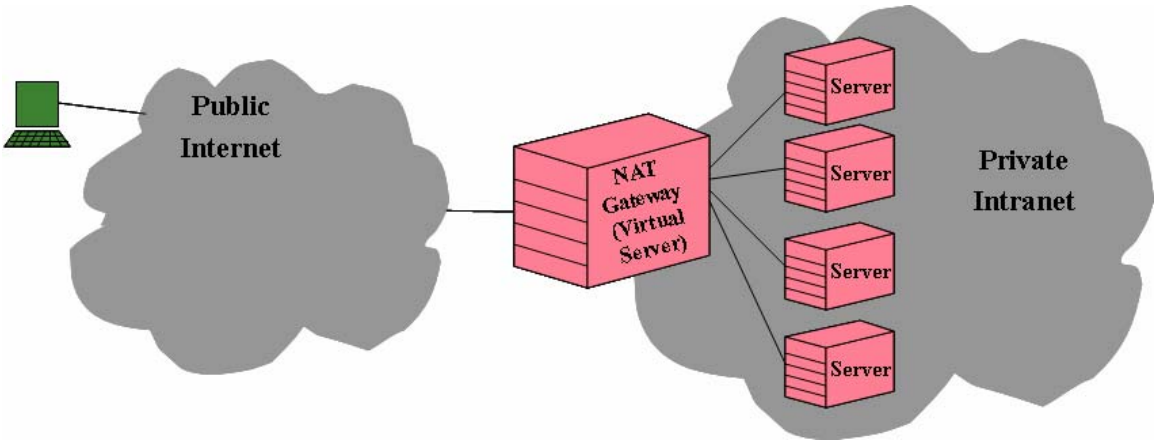
- **Στάδιο 3.** Παρατηρούμε τώρα το TCP/IP πακέτο-απάντηση που στέλνει ο απομακρυσμένος υπολογιστής. Προφανώς, η τιμή του SADDR είναι η διεύθυνση του υπολογιστή αυτού – δηλαδή 128.32.32.68. Η τιμή του DADDR είναι η διεύθυνση του αρχικού υπολογιστή που «βλέπει» ο 128.32.32.68 – δηλαδή, η νέα διεύθυνση 24.1.70.210. Οι τιμές του SPORT και DPORT είναι προφανώς 80 και 40960 – δηλαδή, εναλλάσονται οι αντίστοιχες τιμές του πακέτου που είχαμε στο στάδιο 2. Και, τέλος, επισημαίνεται ότι φυσικά η τιμή του CKSUM είναι διαφορετική από όλες τις προηγούμενες (αφού το εν λόγω IP πακέτο δεν είναι ίδιο με κανένα από τα προηγούμενα).

- **Στάδιο 4.** Ο NAT κοιτάει το πακέτο που λαμβάνει (αυτό του σταδίου 3) και ψάχνει τον πίνακά του να βρει καταχώρηση που να έχει ως NAT θύρα τη 40960 (δηλαδή το DPORT του πακέτου που έλαβε), ως διεύθυνση προορισμού την 128.32.32.68 (που είναι η SADDR του πακέτου που έλαβε) και ως θύρα προορισμού την 80. Στο συγκεκριμένο παράδειγμα βρίσκει την καταχώρηση, η οποία σαν διεύθυνση και TCP θύρα αποστολέα έχει τις 10.0.0.3 και 1049 αντίστοιχα. Άρα, ξέρει σε ποιον υπολογιστή εντός του ιδιωτικού δικτύου να προωθήσει το πακέτο. Προσέξτε τα πεδία του προωθημένου αυτού πακέτου: πρέπει ο ο υπολογιστής 10.0.0.3 να μην αντιλαμβάνεται τον NAT, συνεπώς δεν φαίνεται πουθενά ούτε η διεύθυνση που απέδωσε ο NAT ούτε η θύρα του. Με άλλο λόγια, οι τιμές των πεδίων του πακέτου 4 είναι οι αντίστροφες αυτών του σταδίου 1 (δηλαδή η DADDR του σταδίου 1 γίνεται SADDR του σταδίου 4 κ.ο.κ). Και, βέβαια, πάλι έχουμε μια διαφορετική τιμή του CKSUM, σε σχέση με όλες τις προηγούμενες.

Όταν σε έναν υπολογιστή ανατίθεται πάντα μία νέα συγκεκριμένη IP διεύθυνση, μιλάμε για **στατική** μεταγλώττιση διεύθυνσης – διαφορετικά, αν κάθε φορά του αποδίδεται διαφορετική διεύθυνση, τότε αναφερόμαστε σε **δυναμική** μεταγλώττιση (που είναι και η συνηθέστερη περίπτωση). Πρέπει να σημειωθεί ότι το NAT, όπως περιγράφηκε παραπάνω, έχει τον ίδιο περιορισμό με τον Proxy server ως προς το ότι λειτουργεί μόνο πάνω σε TCP.

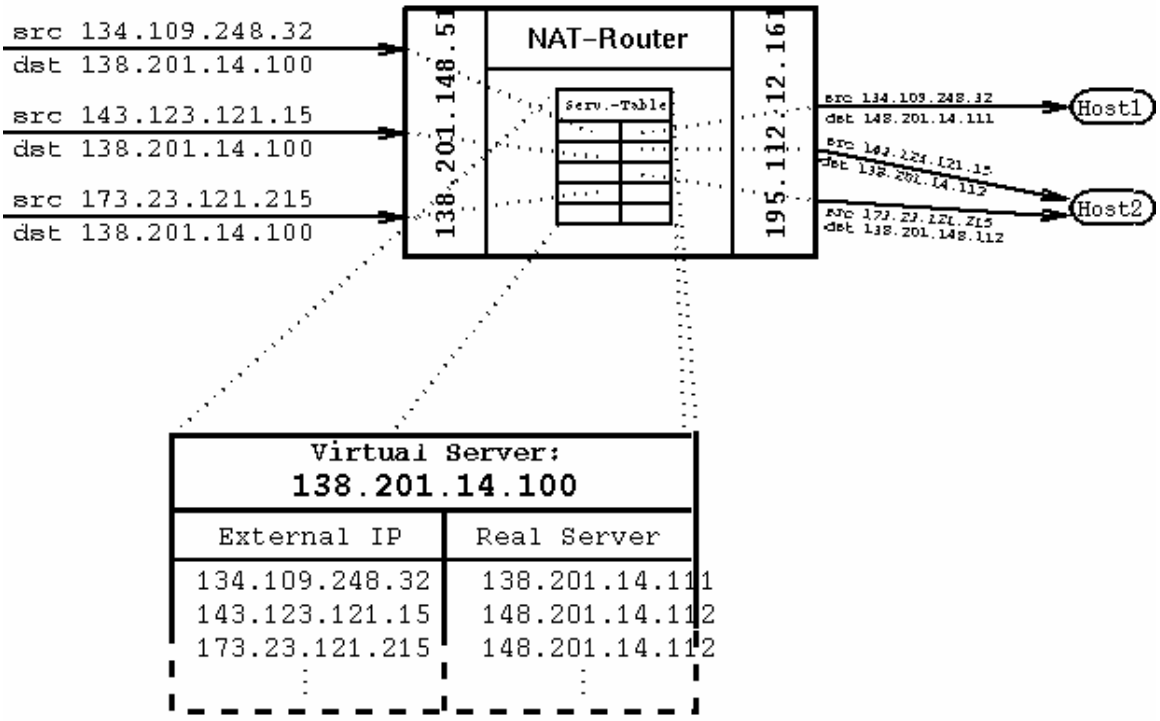
6.3.1. Ειδική περίπτωση NAT – Ιδεατός εξυπηρετητής (virtual server)

Το NAT πρωτόκολλο έχει και έναν δεύτερο τρόπο λειτουργίας, για τις περιπτώσεις που ένας απομακρυσμένος υπολογιστής θέλει να συνδεθεί με έναν υπολογιστή εντός ενός VPN (ή γενικότερα εντός ενός οποιουδήποτε ιδιωτικού δικτύου). Η προσέγγιση αυτή έχει την εξής φιλοσοφία: ως διεύθυνση προορισμού των πακέτων που στέλνει ο απομακρυσμένος υπολογιστής δεν είναι η πραγματική διεύθυνση του υπολογιστή στον οποίον θέλει να συνδεθεί αλλά μια ιδεατή διεύθυνση. Τι σημαίνει αυτό?? Δεν υπάρχει πραγματική συσκευή με αυτή τη διεύθυνση – απλά ο NAT όταν λαμβάνει πακέτο με διεύθυνση προορισμού την ιδεατή, καταλαβαίνει ότι κάποιος ζητά σύνδεση εντός του VPN και προωθεί το πακέτο σε κάποιον server εντός του δικτύου (βλέπε σχήμα 38). Ο NAT πάλι κρατάει μία βάση δεδομένων, στη οποία κρατείται πληροφορία για ποιος πραγματικός εξυπηρετητής έχει τελικά αναλάβει την εξυπηρέτηση της αίτησης του απομακρυσμένου υπολογιστή.



Σχήμα 38: NAT με ιδεατό server

Ένα παράδειγμα φαίνεται στο ακόλουθο σχήμα:



Σχήμα 39: Παράδειγμα NAT με ιδεατό server

Στο παραπάνω παράδειγμα υπάχουν τρεις χρήστες (με διευθύνσεις 134.109.248.32, 143.123.121.15 και 173.23.121.215) που θέλουν να συνδεθούν στο VPN. Ο κάθε ένας στέλνει στην ιδεατή διεύθυνση 138.201.14.100. Μέσα στο VPN υπάρχουν δύο πραγματικοί servers με διεθύνσεις 138.201.14.111 και 148.201.14.112. Ο κάθε χρήστης εξυπηρετείται τελικά από έναν από τους δύο server. Διατηρείται μία βάση δεδομένων με τις ενεργές κάθε στιγμή συνδέσεις. (στον Host1 το πακέτο έχει σαν διεύθυνση αποστολέα την 134.109.248.32, ενώ στον Host2 τα δύο πακέτα έχουν σαν διεύθυνση αποστολέα τις 143.121.121.15 και 173.23.121.215 αντίστοιχα).

Υπάρχουν αλγόριθμοι που εκτελούνται από τον NAT και καθορίζουν τον πραγματικό server στον οποίο θα προωθηθεί κάθε εισερχόμενο πακέτο. Οι αλγόριθμοι αυτοί αποσκοπούν στη λεγόμενη εξισσορόπηση του φορτίου, έτσι ώστε να μην είναι ένας server πιο «φορτωμένος» από άλλους.

7. «Τοίχοι ασφαλείας» (Firewalls)

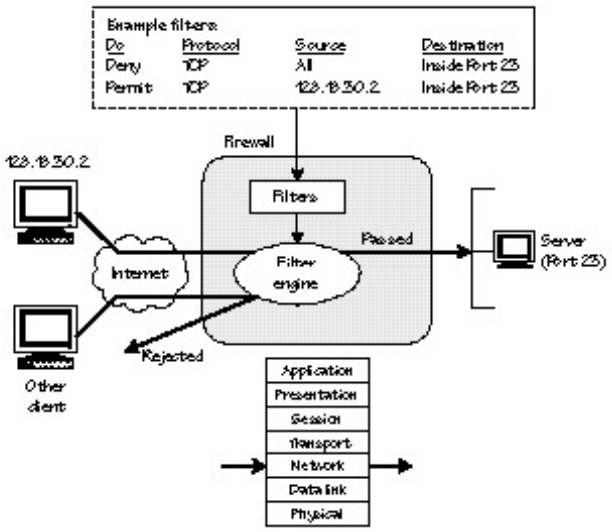
Οι τοίχοι ασφαλείας (firewalls) χρησιμοποιούνταν ανέκαθεν για να προστατεύουν τα LANs από «εισβολή» μη εξουσιοδοτημένων πακέτων. Με απλά λόγια, πραγματοποιούν φιλτράρισμα σε κάθε πακέτο, το οποίο φιλτράρισμα βασίζεται σε κάποια κριτήρια, όπως το είδος του πακέτου, η εφαρμογή στην οποία ανήκει ή η IP διεύθυνση.

Υπάρχουν τριών ειδών τοίχοι ασφαλείας:

- Φίλτρα πακέτων (Packet filters)
- Πύλες ασφαλείας (security gateways (proxies))
- Έξυπνα φίλτρα (Smart filters ή stateful inspections firewalls)

7.1. Φίλτρα πακέτων

Ένα φίλτρο πακέτων εξετάζει στα εισερχόμενα πακέτα τις IP διευθύνσεις πηγής και προορισμού και επιτρέπουν τη διέλευση, με βάση κάποιους κανόνες που έχει θέσει ο διαχειριστής του δικτύου. Για παράδειγμα, στο σχήμα 40, επιτρέπεται η είσοδος μόνο σε πακέτα που προέρχονται από υπολογιστή με IP διεύθυνση 128.18.30.2.



Σχήμα 40: Παράδειγμα ενός Packet filter

Σημαντικά πλεονεκτήματα των πακέτων φίλτρων είναι η εύκολη υλοποίησή τους, καθώς και το γεγονός ότι είναι διαφανή στον χρήστη. Ωστόσο, η πολυπλοκότητά τους μεγαλώνει όσο αυξάνονται οι κανόνες φιλτραρίσματος. Επίσης η τακτική του να επιλέγεται ή όχι πρόσβαση με βάση την IP διεύθυνση δεν είναι η καλύτερη λύση, μια που η IP διεύθυνση από μόνη της σε καμιά περίπτωση δεν εξασφαλίζει αυθεντικοποίηση του αποστολέα. Μια καλύτερη λύση θα ήταν να υπάρχει πιστοποίηση ταυτότητας του χρήστη που στέλνει τα πακέτα. Μία επιπρόσθετη αδυναμία των πακέτων φίλτρων, που απορρέει από τα παραπάνω, είναι το ότι δεν προστατεύουν από επιθέσεις ‘ man-in-the-middle’. Τέλος, πρέπει να συνυπολογιστεί το γεγονός ότι πολλές εφαρμογές δεν έχουν σταθερές θύρες (ports) στις οποίες στέλνουν πακέτα, έτσι ειναι δύσκολο να υπάρξουν στατικοί κανόνες φιλτραρίσματος.

7.2. Πύλες ασφαλείας

Οι πύλες ασφαλείας επιτρέπουν στους χρήστες να χρησιμοποιούν έναν proxy server προκειμένου να επικοινωνήσουν με ασφαλή συστήματα. Ο proxy server δέχεται μία σύνδεση από τη μία πλευρά και, αν η σύνδεση επιτρέπεται, δημιουργεί μια δεύτερη σύνδεση με τον προορισμό από την άλλη πλευρά (Σχήμα 34). Ο χρήστης που ζητά τη σύνδεση δεν συνδέεται ποτέ κατευθείαν με τον προορισμό. Ένας Proxy server, προκειμένου να εξυπηρετεί διάφορα είδη κίνησης, πρέπει να περιέχει πολλούς proxy agents.

Οι πύλες ασφαλείας διαχωρίζονται σε δύο υποκατηγορίες, ανάλογα το είδος του proxy server: σε circuit proxies και application proxies.

7.2.1. Circuit Proxies

Ένας Circuit proxy τοποθετείται ανάμεσα στον δρομολογητή δικτύου (network router) και στο Internet. Στο Internet δεν μεταδίδονται οι πραγματικές IP διευθύνσεις, παρά μόνο η διεύθυνση του proxy. Ένας circuit proxy δεν εξετάζει ποτέ το είδος της εφαρμογής στην οποία υπάγονται τα πακέτα που δέχεται.

Μειονέκτημά τους έναντι των πακέτων φίλτρων είναι το γεγονός ότι είναι πιο αργοί από τα φίλτρα πακέτων, γιατί δομούν εκ νέου την IP διεύθυνση κάθε πακέτου. Επίσης δεν είναι διαφανείς προς τον χρήστη, μια που απαιτείται ειδικό λογισμικό στο PC του.

Ένα πρότυπο για circuit proxy είναι το λεγόμενο SOCKS. Είναι ειδικό firewall που επιτρέπει την πρόσβαση μόνο σε κατάλληλα SOCKS πακέτα. Απαιτείται συνεπώς κατάλληλο software για να μετατρέπει κάθε πακέτο στην κατάλληλη μορφή. Οι περισσότεροι browsers υποστηρίζουν το SOCKS. Υποστηρίζει τόσο TCP όσο και UDP εφαρμογές.

7.2.2. Application Proxies

Η κύρια διαφορά τους από τους circuit proxies είναι ότι εξετάζουν ολόκληρο το πακέτο (δουλεύουν δηλαδή στο επίπεδο 7 και όχι στο 3). Αποθαρρύνουν συνεπώς το IP spoofing. Χρειάζεται ένας agent για κάθε IP υπηρεσία (π.χ. HTTP, FTP, SMTP κ.α.) για την οποία θέλουμε να ελέγχουμε την πρόσβαση. Άρα για κάθε νέα υπηρεσία δεν μπορεί να χρησιμοποιηθεί κάποιος υπάρχων agent. Η πιστοποίηση ταυτότητας είναι πιο ασφαλής. Ωστόσο, είναι πιο αργοί από τους circuit proxies.

7.3. Έξυπνα φίλτρα

Αυτά τα firewalls βασίζονται στην τεχνική Stateful Multi-Layer Inspection (SMLI). Στόχος της, εκτός της μεγίστης δυνατής ασφάλειας, είναι και η βέλτιστη δυνατής απόδοση. Τα έξυπνα φίλτρα μοιάζουν με τους Application proxies, υπό την έννοια ότι εξετάζουν όλο το πακέτο (δηλαδή τις κεφαλίδες όλων των επιπέδων OSI). Χρησιμοποιούν όμως ειδικούς αλγορίθμους (traffic-screening) για να καθορίζουν ή μη τη διέλευση των εισερχόμενων πακέτων. Κάθε πακέτο συγκρίνεται με άλλα «φιλικά» πακέτα.

Ένα έξυπνο φίλτρο κλείνει όλες τις TCP θύρες και τις ανοίγει δυναμικά, όταν κάποιες συνδέσεις τις χρειάζονται. Υποστηρίζει επίσης και UDP πακέτα. Λόγω της μεγάλης ασφάλειας που παρέχουν χρησιμοποιούνται κατά κόρον στα VPN – αν και συνδυάζονται και με proxies, για αυθεντικοποίηση.

8. Συγκριτικά στοιχεία των διαφόρων τεχνολογιών - Συμπεράσματα

Στο παρόν κείμενο πραγματοποιήθηκε μία επισκόπηση των βασικών τεχνολογιών που χρησιμοποιούνται για την υλοποίηση Εικονικών Ιδιωτικών Δικτύων. Σαν κατακλείδα, θα επιχειρηθεί μία σύνοψη, καθώς και μια προσπάθεια σύγκρισης των διάφορων τεχνολογιών.

8.1. Ασφάλεια

Όσον αφορά την ασφάλεια, τα **MPLS VPNs** προωθούν την κίνηση με βάση τις ετικέτες. Η τεχνολογία MPLS, όπως έχει ήδη αναφερθεί, επιτρέπει τον διαχωρισμό κίνησης ανάμεσα σε διαφορετικα VPNs στο ίδιο δίκτυο κορμού με τη χρήση των route distinguishers (RD). Όταν υλοποιείται ένα VPN, καθορίζονται αυτόματα μοναδικοί route distinguishers και τοποθετούνται στις επικεφαλίδες του πακέτου. Η διασφάλιση των δεδομένων του χρήστη στα MPLS VPNs είναι παρόμοια με τη διασφάλιση που παρέχεται από τις παραδοσιακές WAN υποδομές (δηλαδή Frame Relay και ATM): με άλλα λόγια, ο πάροχος υπηρεσιών μπορεί να σχεδιάσει το δίκτυο έτσι ώστε οι δρομολογητές του πελάτη να μην γνωρίζουν το δίκτυο κορμού του παρόχου, και οι δρομολογητές κορμού να μη γνωρίζουν το δίκτυο του πελάτη.

Τα **IPSec VPNs** παρέχουν μεγάλη ασφάλεια για μία επιχείρηση. Η ασφάλεια τους έγκειται στο ότι πραγματοποιούνται λειτουργίες πιστοποίησης ταυτότητας του χρήστη, εμπιστευτικότητας και ακεραιότητας των δεδομένων. Οι χρήστες αυθεντικοποιούνται με ψηφιακά πιστοποιητικά ή προ-μοιρασμένα κλειδιά. Τα πακέτα που δεν είναι σύμφωνα με την πολιτική ασφάλειας απορρίπτονται. Επιπλέον τα IPSec VPNs χρησιμοποιούν μηχανισμούς κρυπτογράφησης και δημιουργίας διόδου (tunneling) στο επίπεδο δικτύου. Πιο συγκεκριμένα το IPSec περιλαμβάνει:

- Δημιουργία διόδου (με AH ή ESP),
- Κρυπτογράφηση (112- ή 168-bit 3DES, 128-, 192, ή 256-bit AES, …)
- Πιστοποίηση ταυτότητας του χρήστη (είτε με Username/Password είτε με RADIUS, είτε με X.509 ψηφιακά πιστοποιητικά)

Τα **SSL VPNs** παρέχουν ασφαλή διασύνδεση μεταξύ ενός εξυπηρετητή (server) και ενός πελάτη (client). Η ασφάλεια στην επικοινωνία επιτυγχάνεται μέσω της πιστοποίησης της ταυτότητας των πλευρών που επικοινωνούν καθώς και της κρυπτογράφησης της κίνησης που πραγματοποιείται μεταξύ τους. Τα SSL VPNs παρέχουν κρυπρογράφηση δεδομένων με τη χρήση των αλγορίθμων είτε RC4 είτε Triple-DES είτε AES. Επιπλέον το SSL χρησιμοποιεί τον αλγόριθμο RSA για την ανταλλαγή του κλειδιού κρυπτογράφησης μεταξύ των δύο πλευρών. Πιο συγκεκριμένα, τα SSL VPNs υλοποιούν:

- Κρυπτογράφηση (40-bit ή 128-bit RC4, 168-bit 3DES, 128-bit AES)
- Πιστοποίηση (Username/Password ή X.509 ψηφιακά πιστοποιητικά)

8.2. Κλιμάκωση

Σχετικά με την κλιμάκωση ή διαβαθμισιμότητα, τα **MPLS VPNs** κλιμακώνονται εύκολα - δηλαδή προσαρμόζονται εύκολα σε αλλαγές που πιθανώς να συμβαίνουν στο δίκτυο μίας εταιρίας. Για παράδειγμα, όταν προστίθεται ένας υπολογιστής ή ένα ολόκληρο LAN στο VPN, ο πάροχος υπηρεσιών χρειάζεται να κάνει τα εξής:

- να ενημερώσει τον δρομολογητή CE του νέου παραρτήματος για τον τρόπο σύνδεσης στο δίκτυο του παρόχου,
- να διαμορφώσει τον PE δρομολογητή έτσι ώστε να αναγνωρίζει τη συμμετοχή του συγκεκριμένου CE στο συγκεκριμένο VPN.
- Στη συνέχεια, το BGP που «τρέχει» στο συγκεκριμένο PE ενημερώνει αυτόματα όλους τους άλλους PEs για το νέο «μέλος».

Με άλλα λόγια, δεν απαιτείται επαναδιαμόρφωση στα άλλα υπάρχοντα sites και έτσι υπάρχει σημαντικό κέρδος σε λειτουργικά κόστη.

Αντίστοιχα, τα **IPSec VPNs** παρουσιάζουν αποδεκτή κλιμάκωση (όχι όμως τόσο καλή όσο τα MPLS). Σε μία μεγάλη υλοποίηση ενός full-mesh IPSec VPN (δηλαδή όλοι επικοινωνούν με όλους) απαιτείται επιπλέον σχεδιασμός για τη διανομή κλειδιού και τη διαχείριση κλειδιού.

Τέλος, στην περίπτωση των **SSL VPNs** δεν υπάρχει ανάγκη για κλιμάκωση (λόγω της client-server φιλοσοφίας που έχουν, καθώς και για το ότι εξυπηρετούν μόνο συγκεκριμένες εφαρμογές, όπως mail και ftp).

8.3. Μηχανισμοί QoS

Όσον αφορά την υποστήριξη μηχανισμών QoS, πρεπει να αναφερθεί ότι τα **MPLS VPNs** υποστηρίζουν μηχανισμούς QoS που εξασφαλίζουν εγγυημένο bandwidth, οι οποίες βελτιώνουν τη συνολική χρήση του δικτύου.

Τα **IPSec VPNs** δεν παρέχουν μηχανισμούς QoS.

Επίσης, στα **SSL VPNs** δεν τίθεται ζήτημα για υλοποίηση QoS και SLAs αφού το υφιστάμενο δίκτυο δε γνωρίζει ότι την ύπαρξη κίνησης SSL.

8.4. Απαίτηση ειδικού software για VPN client

Ένα χαρακτηριστικό των VPNs είναι το κατά πόσον, προκειμένου να συνδεθεί ένας απομακρυσμένος υπολογιστής σε αυτό, απαιτείται η ύπαρξη ειδικού software (VPN client software). Τα **MPLS VPNs** λειτουργούν στο επίπεδο δικτύου και δεν απαιτούν τη χρήση VPN client – οι δρομολογητές (LSRs) είναι υπεύθυνοι για τη δημιουργία των διόδων.

Αντίθετα, στην περίπτωση της απομακρυσμένης πρόσβασης ενός χρήστη σε ένα VPN μέσω του **IPSec**, ο χρήστης χρησιμοποιεί ένα VPN software client και επιλέγει τον κατάλληλο προορισμό (με βάση το συμβολικό όνομα ή τη διεύθυνση IP). Αφού επιτευχθεί η πιστοποίηση ταυτότητας, εγκαθιδρύεται ένα IPSec tunnel. Για τη διασύνδεση LAN-to-LAN μέσω IPSec, οι χρήστες δε χρειάζονται να έχουν κάποιο λογισμικό client στον Η/Υ τους. Ένας IPSec VPN δρομολογητής σε ένα παράρτημα μίας εταιρίας αρχίζει αυτομάτως μία IPSec δίοδο με τα κεντρικά γραφεία της.

Τα **SSL VPNs** συνδέουν χρήστες σε υπηρεσίες και εφαρμογές μέσω των δικτύων και υποστηρίζονται ευρέως από όλους τους εμπορικούς browsers. Συνεπώς παρέχουν

πρόσβαση στους χρήστες οπουδήποτε κι αν βρίσκονται χωρίς την απαίτηση κάποιου ειδικού VPN client.

8.5. Κόστος Υλοποίησης

Το κόστος εγκατάστασης και χρήσης ενός VPN αποτελεί έναν σημαντικό παράγοντα για την επιλογή της κατάλληλης τεχνολογίας υλοποίησης ενός Εικονικού Ιδιωτικού Δικτύου. Αρχικά ας δούμε τα επιμέρους κόστη που χαρακτηρίζουν την δημιουργία ενός VPN.

Το σημαντικότερο κόστος που υπεισέρχεται στην υλοποίηση ενός VPN είναι ο σχεδιασμός του. Το κόστος αυτό το αναλαμβάνει ο πάροχος υπηρεσιών (ISP) – πρέπει να πραγματοποιηθεί μελέτη της κίνησης του δικτύου της εταιρίας του πελάτη έτσι ώστε να σχεδιαστεί το δίκτυο κατά τρόπο τέτοιο ώστε να ικανοποιεί τόσο τις υπάρχουσες ανάγκες όσο και τις απαιτήσεις για περαιτέρω υπηρεσίες. Παράλληλα η εταιρία πρέπει να λάβει σοβαρά υπόψη την ύπαρξη δευτερεύουσας σύνδεσης με το Internet, ώστε να μπορεί να έχει κάποιες εναλλακτικές επιλογές σε περίπτωση που η κύρια σύνδεση παρουσιάζει προβλήματα. Το κόστος μιας ενδεχόμενης απομόνωσης από το Internet μπορεί να είναι μεγαλύτερο σε σχέση με αυτό που απαιτείται για τη συντήρηση της σύνδεσης αυτής.

Η απόκτηση του εξοπλισμού VPN και των αδειών χρήσης του λογισμικού είναι ένας ακόμη παράγοντας που προστίθεται στο κόστος του VPN. Πρέπει να υπάρχουν οι συσκευές που θα κάνουν πιστοποίηση της ταυτότητας των χρηστών καθώς και οι συσκευές που θα επιτρέπουν πρόσβαση σε απομακρυσμένους χρήστες με ασφαλή τρόπο (VPN clients).

Ένας τρίτος παράγοντας κόστους είναι η ανάγκη συντήρησης και διαχείρισης του δικτύου. Η συντήρηση αφορά αναβάθμιση συσκευών ή λογισμικού που προσφέρουν νέες δυνατότητες στο VPN (π.χ. νέοι αλγόριθμοι κρυπτογράφησης). Αρκετές φορές το κόστος αναβάθμισης συμπεριλαμβάνεται στην αγορά των αδειών χρήσης των μερών που συνιστούν το VPN. Η διαχείριση συνήθως ανατίθεται στον ISP που έχει αναλάβει και την εγκατάσταση του VPN.

Επομένως, το κόστος είναι ένα σημαντικό θέμα όταν πρέπει να αποφασιστεί ποια τεχνολογία VPN θα επιλεγεί. Αν υπάρχει η ανάγκη για διασύνδεση μεταξύ sites, όπως στην περίπτωση ενός απομακρυσμένου γραφείου με τα κεντρικά γραφεία της εταιρίας, τα IPSec VPNs είναι η πιο κατάλληλη επιλογή. Οι χρήστες θα έχουν την εμπειρία «on-the-LAN», δηλαδή της απευθείας σύνδεσης στο τοπικό δίκτυο, χωρίς να πρέπει να διαχειριστούν clients. Αν υπάρχει η ανάγκη διασύνδεσης για απομακρυσμένους/κινητούς χρήστες, συνεργάτες της επιχείρησης ή πελάτες, όπου οι συσκευές και τα δίκτυα από τα οποία πραγματοποιείται η πρόσβαση κάθε φορά αλλάζουν, τότε τα SSL VPNs είναι η πιο κατάλληλη επιλογή (αν και υπάρχει πάντα ο περιορισμός των συγκεκριμένων εφαρμογών που μπορούν να εξυπηρετηθούν).

Το αρχικό κόστος για την υλοποίηση ενός IPSec VPN είναι μικρότερο από το κόστος που απαιτείται για ένα SSL VPN, αφού ένα IPSec VPN μπορεί να υλοποιηθεί πάνω από το υφιστάμενο δίκτυο IP χωρίς να υπάρχει ανάγκη για σχεδιασμό και δημιουργία ενός νέου δικτύου. Πάντως, όταν οι εταιρίες υπολογίζουν τα κόστη, το return on investment (ROI) για ένα SSL VPN είναι πολύ μεγαλύτερο: κι αυτό γιατί τα SSL VPNs δεν απαιτούν υλοποίηση και διαχείριση κάποιου client και, συνεπώς, τα τρέχοντα κόστη για διαχείριση και υποστήριξη είναι πολύ χαμηλότερα. Επιπλέον, οι χρήστες έχουν τη δυνατότητα πρόσβασης στους δικτυακούς πόρους της επιχείρησης από οπουδήποτε και συνεπώς η συνολική παραγωγικότητα αυξάνει.

Τέλος, τα MPLS VPNs αποτελούν τη λύση επιλογής στην περίπτωση εκείνη που οι απαιτήσεις του πελάτη είναι προς την κατεύθυνση της εύκολης προσθήκης νέων περιφερειακών sites. Αν η εταιρία δηλαδή, έχει αυξημένες ανάγκες διασύνδεσης πολλών παραρτημάτων, το κόστος προσθήκης τους είναι χαμηλότερο από εκείνο της τεχνολογίας IPSec. Παράλληλα, τα MPLS VPNs δεν απαιτούν αγορά αδειών χρήσης όπως στην περίπτωση των IPSec VPNs ενώ και αυτά εξασφαλίζουν την εμπειρία «on-the-LAN» αφού υπάρχει μία μόνιμη σύνδεση με τους πόρους του δικτύου. Το κόστος στα MPLS VPNs είναι το αθροιστικό κόστος χρήσης της μισθωμένης γραμμής και της διαχείρισης των VPNs από τον πάροχο. Η μισθωμένη γραμμή είναι τυπική ψηφιακή ευθεία HellasCom σε ταχύτητες που μπορεί να κυμαίνονται από 64Kbps μέχρι 2Mbps.

Συνοψίζοντας, λοιπόν, θα λέγαμε ότι η υλοποίηση ενός Εικονικού Ιδιωτικού Δικτύου εξαρτάται αφενός από τις ανάγκες της εταιρίας-πελάτη, αφετέρου από το κόστος εγκατάστασης και χρήσης του VPN. Είναι δύο παράγοντες που καθορίζουν την τεχνολογία VPN που επιλέγει κάθε εταιρία για να υλοποιήσει το ιδιωτικό της δίκτυο πάνω από μία κοινώς διανεμημένη υποδομή.

8.6. Συγκριτικός Πίνακας

Στη συνέχεια παρατίθεται ένας πίνακας που παρουσιάζει συνοπτικά τα πλεονεκτήματα και τους περιορισμούς των τριών αρχιτεκτονικών VPNs MPLS, IPSec, και SSL σύμφωνα με όσα αναλύθηκαν παραπάνω.

	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.

Βιβλιογραφικές πηγές

1. Dave Kosiur, “Building and Managing Virtual Private Networks”, John Wiley & Sons, 1998.
2. Gordon Chaffee , “Διαλέξεις από το Πανεπιστήμιο του Berkeley” (2005)
3. Charlie Scott, Paul Wolfe and Mike Erwin, “Virtual Private Networks – Second Edition”, O’Reilly, 1999.
4. Πληθώρα διαλέξεων και σημειώσεων που είναι διαθέσιμες στο Internet